



# Release Note for Cisco Wide Area Application Services Software Version 6.2.3x

---

July 31, 2019



Note

---

The most current Cisco documentation for released products is available on [Cisco.com](http://Cisco.com).

---

## Contents

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

- 6.2.3e
- 6.2.3d
- 6.2.3c
- 6.2.3b
- 6.2.3a
- 6.2.3

For information on Cisco WAAS features and commands, see the Cisco WAAS documentation located at [http://www.cisco.com/en/US/products/ps6870/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html).

This Release Note contains the following sections:

- [New and Changed Features](#)
- [Interoperability and Support](#)
- [Upgrading from a Release Version to Version 6.2.3x](#)
- [Downgrading from Version 6.2.3x to a Previous Version](#)
- [Cisco WAE and WAVE Appliance Boot Process](#)
- [Operating Considerations](#)
- [Software Version 6.2.3x 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 6.2.3x:

- [Cisco Software Version 6.2.3x New and Changed Features](#)
- [Cisco Software Version 6.2.3x Filenames](#)
- [Cisco WAAS Appliance System Firmware Update](#)
- [Configuring ICA over Socket Secure \(SOCKS\) Server](#)

## Cisco Software Version 6.2.3x New and Changed Features

This section contains the following topics:

- [WAAS Version 6.2.3e New and Changed Features](#)
- [WAAS Version 6.2.3d New and Changed Features](#)
- [WAAS Version 6.2.3b New and Changed Features](#)

### WAAS Version 6.2.3e New and Changed Features

- Unique alarm identifier support—WAAS Central manager now identifies every device alarm instance with a unique identifier. This allows for better tracking of raised and cleared alarms and link notifications with GUI outputs.

### WAAS Version 6.2.3d New and Changed Features

- Alarm Email Notification- With release 6.2.3d, the WAAS software supports an email notification mechanism, that is triggered whenever the WAAS Central Manager receives an alarm notification for a raised or cleared alarm. To configure the alarm email notification feature:
  - From the WAAS Central Manager menu go to **Devices > Configure > Monitoring > Email Notification** to configure the email server settings.
  - From the WAAS Central Manager go to **Home > Admin > Alarm Email Notification > Configure** to configure the email notification settings.

You can enable the email notification for Raised and Cleared alarms, depending on the severity level. After you have configured this, you are notified of all alarms for the devices that are registered with the WAAS Central Manager.
- Easy detection and resolution of configuration conflicts between WAAS Central Manager and WAAS Devices.

To identify the configuration conflict pages, from the WAAS Central Manager navigate to **Home > Admin > Force Device Group > View Pages** to see the impacted Device Name, Device Group Name and Page Name. You can click on the page link to navigate to the corresponding page to correct the configuration conflict.

## WAAS Version 6.2.3b New and Changed Features

- **Configuring ICA over Socket Secure (SOCKS) Server**—For WAAS Version 6.2.3b and later, WAAS software supports optimizing ICA traffic redirected over SOCKS proxy servers. For details on how to configure ICA over SOCKS for WAAS, see [Configuring ICA over Socket Secure \(SOCKS\) Server](#).
- **SMART-SSL**, an encryption service that enables L7 application network services (such as FTP, HTTP, DNS) to optimize traffic on SSL/TLS encrypted applications. SMART-SSL enables content caching for SSL/TLS applications (HTTP object cache for HTTPS traffic) in single-sided deployment.

For how to configure and use this feature, see “Configuring SMART-SSL” in the “Configuring Application Acceleration” chapter of the [Cisco Wide Area Application Services Configuration Guide](#).

- Cisco WAAS Version 6.2.3 with Akamai Connect Version 1.4.2
- vWAAS new and changed features:
  - vWAAS in KVM on CentOS

For a list of CLI commands added to or changed for WAAS Version 6.2.3x, see [Cisco WAAS Software Version 6.2.3 Command Changes](#).

## Cisco Software Version 6.2.3x Filenames

This section describes the Cisco WAAS Software Version 6.2.3x 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 the [Cisco Virtual Wide Area Application Services Installation and Configuration Guide](#).

### Standard Image Files

Cisco WAAS Software Version 6.2.3x includes the following standard primary software image files for use on Cisco WAAS appliances and modules:

- `waas-universal-6.2.3.x-k9.bin`—Universal software image that includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade a device operating in any device mode.
- `waas-accelerator-6.2.3.x-k9.bin`—Application Accelerator software image that includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator 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-6.2.3.x-k9.iso`—Cisco WAAS software recovery CD image.
- `waas-sre-installer-6.2.3.x-k9.zip`—Image for SRE installer.



**Note** From software version 6.2.3d, separate software images for the SRE installer are not supported. If you want to upgrade your existing SRE deployments, you need to use the standard software image file WAAS-6.2.3.x-k9.bin.

For EOS announcement of select Cisco Services-Ready Engine Modules, please refer to the [EOS document](#) on cisco.com.

- waas-x86\_64-6.2.3.x-k9.sysimg—Flash memory recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- waas-6.2.3.x-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- waas-kdump-6.2.3.x-k9.bin—Kdump analysis component that you can install and use with the Application Accelerator software image. The Kdump analysis component is intended for troubleshooting specific issues and should be installed following the instructions provided by Cisco TAC.
- waas-alarm-error-books-6.2.3.x.zip—Contains the alarm and error message documentation.

## No Payload Encryption Image Files

Cisco WAAS Software Version 6.2.3x 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-6.2.3.x-npe-k9.bin—Universal NPE software image that includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade a device operating in any device mode.
- waas-accelerator-6.2.3.x-npe-k9.bin—Application Accelerator NPE software image that includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator 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-6.2.3.x-npe-k9.zip—SM-SRE install .zip file that includes all the NPE files necessary to install Cisco WAAS on the SM-SRE module.

The following additional files are also included:

- waas-rescue-cdrom-6.2.3.x-npe-k9.iso—Cisco WAAS NPE software recovery CD image.
- waas-x86\_64-6.2.3.x-npe-k9.sysimg—Flash memory NPE recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- waas-6.2.3.x-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-alarm-error-books-6.2.3.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.



Note

---

AppNav IOM is not supported in WAAS Software version 6.1.x and later.

---

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

If you 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.

For the specific BIOS version required for WAVE-594/694 models, WAVE-7541/7571/8541 models, and WAVE-294 models or if a BIOS firmware update is needed, you can download it from [cisco.com](http://cisco.com) at the [Cisco Wide Area Application Service \(WAAS\) Firmware](#) download page ([registered](#) customers only). The firmware binary image for WAVE-294/594/694/7541/7571/8541 appliances is named `waas6-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 waas6-bmc-installer-49a-49a-27a-k9.bin
```

Use the appropriate BIOS installer file for your appliance model.

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

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

## BMC Firmware Update

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

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

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

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

```

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

```

If a BMC firmware update is needed, you can download it from [cisco.com](http://cisco.com) at the [Cisco Wide Area Application Service \(WAAS\) Firmware](#) download page (registered customers only). For example, if the firmware binary image is named `waas-bmc-installer-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 waas6-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](http://cisco.com) at the [Cisco Wide Area Application Service \(WAAS\) Firmware](#) download page ([registered](#) customers only). The firmware differs depending on your hardware platform:

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

The firmware binary image is named `waas6-raid-fw-installer-12.12.0-0060-k9.bin`. Instructions on how to apply the firmware update are posted on [cisco.com](http://cisco.com) together with the firmware in the file named `M2_0060_FIRMWARE.pdf`, which you can see when you hover the mouse over the firmware file.

## Configuring ICA over Socket Secure (SOCKS) Server

This section contains the following topics:

- [About ICA over SOCKS Optimization](#)
- [Limitations of ICA over SOCKS Optimization](#)
- [Configuration Procedure for Optimizing ICA over SOCKS](#)

### About ICA over SOCKS Optimization

In a typical deployment where NetScaler is deployed as a SOCKS proxy, the connections from the client go to the SOCKS server instead of the XenApp server.

Since the ICA optimizer accepts and intercepts only ICA and CGP packets, the packets with SOCKS headers are not recognized and the connection is handed off. The ICA traffic does not get optimized in such scenarios.

For WAAS Version 6.2.3b and later, the WAAS software supports optimizing ICA traffic redirected over SOCKS proxy servers.

### Limitations of ICA over SOCKS Optimization

ICA over SOCKS optimization has the following limitations:

- The NetScaler gateway does not support non-default ports configured with Multi-Port Policy on XenApp for Multi-Stream ICA (MSI).
- The NetScaler gateway does not support SOCKS with ICA over SSL.

Additionally, the NetScaler gateway does not support SOCKS v4. so the current functionality supports only SOCKS v5.

### Configuration Procedure for Optimizing ICA over SOCKS

To support optimizing ICA over SOCKS, perform the following steps:

- 
- Step 1** Make the necessary changes in the NetScaler Gateway to enable the SOCKS proxy (Cache redirection server) and also make the equivalent/required changes on the StoreFront server along with updates to the `default.ica` file. Refer to Citrix NetScaler documentation for more information.

- Step 2** From the WAAS Central Manager menu, choose **Devices** > device-name (or **Device Groups** > device-group-name). Next choose **Configure** > **Acceleration** > **Optimization Class-Map**.
- Step 3** Edit the class-map named **Citrix** and add the required port number using the **Add Match Condition** option.  
The port number added in the class-map should be the same as the one configured for the SOCKS proxy, on the NetScaler gateway. Note that in case the SOCKS proxy port is running on ICA or CGP ports i.e. 1494 or 2498, then the existing configuration need not be modified.
- Step 4** Select the branch device and make the necessary changes for the port number.  
Alternately use the **class-map type match-any citrix** global configuration command to make these changes.
- 

## 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](#)
- [Citrix ICA Interoperability](#)
- [WAAS Application Accelerators Interoperability with Third-Party Load Balancers](#)
- [Cipher Support for SSL Acceleration](#)

## Hardware, Client, and Web Browser Support

This section contains the following topics:

- [Platforms Supported by WAAS](#)
- [Browsers Supported by WAAS](#)

### Platforms Supported by WAAS

The Cisco WAAS software operates on these hardware platforms:

- WAVE-294, 594, 694, 7541, 7571, 8541
- 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 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 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. For WAAS Version 6.2.3x and later, vWAAS is supported on KVM on CentOS and Microsoft Azure.

For more information on vWAAS for RHEL KVM, KVM on CentOS, and vWAAS on Microsoft Azure, see the [Cisco Virtual Wide Area Application Services Installation and Configuration Guide](#).

- 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).

You must deploy the Cisco WAAS Central Manager on a dedicated device.

## Browsers Supported by WAAS

The Cisco WAAS Central Manager GUI requires Internet Explorer Version 11, Windows Version 7 or later, 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.



**Note** For best results for Windows-based systems with WAAS, we recommend using FireFox as your browser.

- 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.



**Note** A known issue in Chrome Version 44.0 may prevent some WAAS Central Manager pages—including Device Listing, Reports, Software Update pages—from loading properly. In all other Chrome versions, earlier and later than Chrome Version 44.0, all WAAS Central Manager pages work as expected.

## Cisco WAAS Version Interoperability

Consider the following guidelines when operating a Cisco WAAS network that mixes Software Version 6.2.3x 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 5.1.x or later.

- **Cisco WAAS system interoperability:**

Cisco WAAS Version 6.2.3x 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 5.1.x. Directly upgrading a device from a version earlier than Version 5.5.3 to 6.2.3x is not supported.

## Cisco WAAS and vWAAS Interoperability

[Table 1](#) shows the default number of CPUs, memory capacity, disk storage and supported ISR platforms for ISR models. [Table 2](#) shows the default number of CPUs, memory capacity and disk storage for vWAAS models.

**Table 1** *ISR Models: CPUs, Memory, Disk Storage and Supported ISR Platforms*

ISR Model	CPUs	Memory	Disk Storage	Supported ISR Platform
ISR-WAAS-200 (for WAAS 5.x and 6.2.1)	1	3 GB	151 GB	ISR-4321
ISR-WAAS-200 (for WAAS 6.2.3x)	1	4 GB	151 GB	ISR-4321
ISR-WAAS-750	2	4 GB	151 GB	ISR-4351, ISR-4331, ISR-4431, ISR-4451
ISR-WAAS-1300	4	6 GB	151 GB	ISR-4431, ISR-4451
ISR-WAAS-2500	6	8 GB	338 GB	ISR-4451



**Note**

For vWAAS with WAAS Version 6.2.3c or later, for ISR-4321 with profile ISR-WAAS-200, the ISR-WAAS RAM is increased from 3 GB to 4 GB. For this increase in ISR-WAAS RAM to be implemented, you must complete a new OVA deployment of WAAS version 6.2.3c or later. The increase in ISR-WAAS RAM is not automatically implemented with an upgrade to WAAS Version 6.2.3c or later.

**Table 2** *vWAAS Models: CPUs, Memory and Disk Storage*

vWAAS Model	CPUs	Memory	Disk Storage
vWAAS-150 (for WAAS Version 6.x)	1	3 GB	160 GB
vWAAS-200 (for WAAS Version 5.x through 6.2.1)	1	3 GB	260 GB
vWAAS-200 (for WAAS Version 6.2.3x)	1	4 GB	260 GB
vWAAS-750	2	4 GB	500 GB
vWAAS-1300	2	6 GB	600 GB
vWAAS-2500	4	8 GB	750 GB
vWAAS-6000	4	11 GB	900 GB
vWAAS-12000	4	12 GB	750 GB
vWAAS-50000	8	48 GB	1500 GB

Consider the following guidelines when using Cisco vWAAS with WAAS:



Note

For vWAAS for WAAS Version 6.2.x with Cisco Enterprise NFVIS, the vWAAS must run as an unmanaged VM.

- For vWAAS with WAAS Version 6.2.3x, ISR-4321 with profile ISR-WAAS-200, ISR-WAAS RAM is increased from 3 GB to 4 GB. For this increase in ISR-WAAS RAM to be implemented, you must complete a new OVA deployment of WAAS version 6.2.3x; the increase in ISR-WAAS RAM is not automatically implemented with an upgrade to WAAS 6.2.3x.
- 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.
- vWAAS and DRE partitions:
  - *When you deploy vWAAS using OVAs older than the 6.2.3d version, DRE's **ackq** and **plz** partitions are not created as expected for vWAAS-6000, 12000, and 50000 models (they are created of lesser size and no alarms will be displayed to indicate the mismatch in partition sizes). Because of this, the connection flow for vWAAS will not be optimized by DRE after a certain period. To ensure DRE optimization for vWAAS, after deployment you must use the **disk delete-data-partitions** command to re-create these partitions for vWAAS.*



Note

If the vWAAS device is downgraded in the following scenarios:

- from vWAAS for WAAS Version 6.4.1a to WAAS Version 6.2.3x, or
- from vWAAS for WAAS Version 6.x to 5.x

the WAAS alarm `filesystem_size_mismatch` is displayed; it indicates that the partition was not created as expected. To clear the alarm, use the `disk delete-data-partitions` command to re-create the DRE partitions.

- *If you deploy vWAAS with WAAS version 6.2.3d or later, an issue will not be seen. Here, partitions will be created as expected.*



Note

The `disk delete-data-partitions` command will re-create the partition and leads to cache loss.

For more information on the **disk delete-data-partitions** command, see the [Cisco Wide Area Application Services Command Reference](#). For more information on DRE compression, see the [Cisco Wide Area Application Services Configuration Guide](#).

- 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.



Caution

Multiple deployments of vWAAS on the same Hyper-V host *in parallel* may cause unexpected results, due to availability of free space when creating VHDs. We recommend that you do *not* deploy multiple vWAAS on Hyper-V in parallel, unless you have verified that you have enough free disk space required for the respective vWAAS models.

- 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 the [Cisco Virtual Wide Area Application Services Installation and Configuration Guide](#).
- To ensure reliable throughput with the following configuration—**vWAAS on Windows Server 2012 R2 Hyper-V in Cisco UCS-E Series 160S-M3**—we recommend that you do the following:
  - Upgrade to the latest UCS-E firmware (Version 3.1.2), available on the [Cisco Download Software Page for UCS E-Series Software, UCS E160S M3 Software](#).
  - Verify that you have installed the critical Windows Server updates, available on the [Microsoft Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update Rollup](#) page. You can also obtain the standalone update package through the Microsoft Download Center by searching for **KB2887595**.

**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 st of vWAAS image files, see the [Cisco Virtual Wide Area Application Services Installation and Configuration Guide](#).

**Note**

For a vCM-100 model used with the RHEL KVM or KVM on CentOS hypervisor, with the default memory size of 2 GB:

When you upgrade to WAAS Version 6.2.3x from an earlier version, or downgrade from WAAS Version 6.2.3x to an earlier version, and use either the **restore factory-default** command or the **restore factory-default preserve basic-config** command, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

**CAUTION:** *The **restore factory-default** command erases user-specified configuration information stored in the flash image, including the starting configuration of the device, and also removes data from the disk, user-defined partitions, and the entire Central Manager database.*

To resolve this situation, follow these steps:

1. Power down the vWAAS using the **virsh destroy *vmname*** command or the virt manager.
2. Power up the vWAAS using the **virsh start *vmname*** command or the virt manager.

This upgrade/downgrade scenario does not occur for vCM-100 models whose memory size is upgraded to 4 GB.

## Cisco WAAS, ISR-WAAS and IOS-XE Interoperability

Table 3 shows Cisco WAAS, ISR-WAAS and IOS-XE Interoperability.

**Table 3** 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 and later 16.3.x and later

### Operating Guidelines for Cisco WAAS, ISR-WAAS and IOS-XE Interoperability

- ISR4321-B/K9 is not supported for ISR-WAAS installation.
- **Activating ISR-WAAS after formatting the Cisco 4000 Series ISR-router bootflash:**  
After you format the Cisco 4000 Series ISR-router bootflash, you must reload the router to ensure a successful activation of ISR-WAAS. If you do not reload the ISR router after formatting the bootflash, you will be unable to activate ISR-WAAS. For more information on formatting the Cisco 4000 Series ISR router bootflash, see the [Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco 4000 Series ISRs](#).
- **For ISR-4321 with IOS-XE, used with WAAS Version 6.2.3x:**  
You must complete a new OVA deployment of WAAS version 6.2.3x for this configuration to work successfully. This configuration will not automatically work after an upgrade to WAAS Version 6.2.3x from WAAS Version 5.x or 6.x.
- **Using the intrusion detection and prevention system Snort with ISR-WAAS and ISR-4000 Series, with a hard disk less than or equal to 200 GB:**  
To ensure a successful WAAS installation of ISR-WAAS and Snort on an ISR router, you must install ISR-WAAS *before* you install Snort. If you do not follow this installation order, ISR-WAAS will not install and a disk error will be displayed.
- **VRF restriction for VirtualPortGroup31 on ISR-WAAS:**  
When you configure ISR-WAAS with EZConfig—VirtualPortGroup31, the WAAS service/router interface, is automatically created, and you can then add or modify specific parameters for it.



**Note** Do not add Virtual Routing and Forwarding (VRF) to VirtualPortGroup31. VRF will cause VirtualPortGroup31 to lose its IP address and will disable AppNav. To re-establish these, you must uninstall and reinstall ISR-WAAS without VRF.

For more information on VirtualPortGroup31, see the [Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco 4000 Series ISRs](#).

## 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.
- 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 4 shows Cisco WAAS, ASR/CSR and IOS-XE Interoperability.

**Table 4** 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
5.5.5x	ASR-1000x/CSR-1000V	3.13-3.17
5.5.7x	ASR-1000x/CSR-1000V	3.12-3.17

WAAS Version	ASR/CSR Series	IOS-XE Version Supported
6.1.1a, 6.2.1x	ASR-1000x/CSR-1000V	3.15.2, 3.16.01a, 3.16.2, 3.17
6.2.3x	ASR-1000x/CSR-1000V	3.13.8, 3.15.2, 3.16.01a, 3.16.2, 3.16.3, 3.16.6, 3.16.8, 3.17, 3.17.03, 3.17.04, 16.3.4, 16.3.5, 16.4.2, 16.5.1, 16.5.2, 16.6.1, 16.7.1

## Cisco WAAS Express Interoperability

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



Note

When Cisco WAAS Express is used on the Cisco Integrated Services Router Generation 2 (ISR G2) with the Cisco VPN Internal Service Module (VPN-ISM) or with Group Encrypted Transport (GETVPN) enabled, the WAAS Express does not optimize FTP data.

To ensure that FTP data is optimized when WAAS Express is used with the Cisco ISR G2, use the ISR G2's IOS crypto map software.

- For a Cisco WAAS device running WAAS Version 6.x and a Cisco WAAS Express peer device running Cisco IOS Release 15.6(3)M, 15.6(2)T1 or later, TLS1 is supported, but SSL3 is removed. Before upgrading WAAS Express to one of these IOS releases, configure TLS1 in the WAAS Express Device Group > Peering Service page, and then upgrade the WAAS Express device to the specified IOS release.
- 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 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 5](#) lists the Cisco WAAS, WAAS Express and IOS Interoperability

**Table 5** 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.x	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.
- If you use Microsoft System Center Configuration Manager with Preboot Execution Environment (SCCM/PXE), we recommend the following configurations for the ports that carry SCCM/PXE traffic: port 80, port 443, and port 445:
  - port 80—Communicates with the distribution point. Configure for **pass-through traffic**.
  - port 443—Communicates with the distribution point. Configure for **pass-through traffic**.
  - port 445—Used for software package distribution data transfer. Configure for **traffic optimization**.

Without these configurations you may see the error message “PXE error code 80070056.”

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 6.2.3x can manage WAEs running software Versions 5.x and later. However, we recommend that all WAEs in a given WCCP service group be running the same version.



**Note** All WAEs in a WCCP service group must have the same mask.

To upgrade the WAEs in your WCCP service group, follow these steps:

- 
- Step 1** You must disable WCCP redirection on the Cisco IOS router first. To remove the global WCCP configuration, use the following **no ip wccp** global configuration commands:
- ```
Router(config)# no ip wccp 61
Router(config)# no ip wccp 62
```
- Step 2** Perform the Cisco WAAS software upgrade on all WAEs using the Cisco WAAS Central Manager GUI.
- Step 3** Verify that all WAEs have been upgraded in the Devices pane of the Central Manager GUI. Choose **Devices** to view the software version of each WAE.
- Step 4** If mask assignment is used for WCCP, ensure that all WAEs in the service group are using the same WCCP mask value.
- Step 5** Reenable WCCP redirection on the Cisco IOS routers. To enable WCCP redirection, use the **ip wccp** global configuration commands:
- ```
Router(config)# ip wccp 61
Router(config)# ip wccp 62
```
- 

## NTLM Interoperability

Cisco WAAS Version 5.1 and later do not support Windows domain login authentication using the NTLM protocol. Therefore, upgrading from a Cisco WAAS Version earlier than 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.

## 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

## WAAS Application Accelerators Interoperability with Third-Party Load Balancers

A load balancer is used to balance network and application traffic across a set of servers, The resulting evenly-distributed traffic improves the response rate of network traffic, increases the availability of applications, and minimizes the risk of a single server becoming overloaded.

[Table 6](#) shows the interoperability between WAAS application accelerators and the F5 load balancer. For more information about WAAS load balancing, see the “Configuring Traffic Interception” chapter of the [Cisco Wide Area Application Services Configuration Guide](#) and also see the [Server Load-Balancing Guide vA5\(1.0\)](#), [Cisco ACE Application Control Engine](#).



**Note** WAAS does not currently support Citrix NetScaler load balancer.

**Table 6** WAAS Application Accelerators Interoperability with Load Balancers

WAAS Status	Load Balancer Status	Authentication Method	WAAS AO Supported/ Not Supported
WAAS enabled	F5 enabled	Kerberos	<ul style="list-style-type: none"> <li>EMAPI not supported</li> <li>SSL not supported</li> </ul>
WAAS disabled	F5 enabled	Kerberos	<ul style="list-style-type: none"> <li>EMAPI supported</li> <li>SSL supported</li> </ul>
WAAS enabled	F5 disabled	Kerberos	<ul style="list-style-type: none"> <li>EMAPI supported</li> <li>SSL supported</li> </ul>
WAAS enabled	F5 enabled	NTLM	<ul style="list-style-type: none"> <li>EMAPI supported</li> <li>SSL not supported</li> </ul>

## Cipher Support for SSL Acceleration

No new cipher support is available for SSL Acceleration (Legacy SSL Acceleration) other than those listed in “Configuring SSL Management Services” of the [Cisco Wide Area Application Services Configuration Guide](#). For additional ciphers supported, please see the supported cipher list for SMART-SSL Acceleration.

## Upgrading from a Release Version to Version 6.2.3x

Upgrading to WAAS Version 6.2.3x is supported from WAAS Version 4.2.1 and later. For information on upgrade paths, see [Upgrade Paths and Considerations for Version 6.2.3x](#).

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 6.2.3xx, see [Workflow: Upgrading from a Release Version to Version 6.2.3x](#).

This section contains the following topics:

- [Upgrade Paths and Considerations for Version 6.2.3x](#)
- [Workflow: Upgrading from a Release Version to Version 6.2.3x](#)
  - [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 6.2.3x

This section contains the following topics:

- [Upgrade Paths for WAAS Version 6.2.3x](#)
- [Upgrading from Cisco WAAS Version 5.x and Later to Version 6.2.3x](#)
- [Upgrading from Cisco WAAS Version 4.2.x to Version 6.2.3x](#)

### Upgrade Paths for WAAS Version 6.2.3x

Upgrading to WAAS Version 6.2.3x is supported from WAAS Version 4.2.x and later. [Table 7](#) shows the upgrade path for each of these versions.

**Table 7** Upgrade Paths to WAAS Version 6.2.3x

Current WAAS Version	WAAS CM Upgrade Path	WAAS Upgrade Path
5.5.3 and later	<ul style="list-style-type: none"> <li>• Upgrade directly to 6.2.3x</li> </ul>	<ul style="list-style-type: none"> <li>• Upgrade directly to 6.2.3x</li> </ul>
4.3.x through 5.5.1	<ol style="list-style-type: none"> <li>1. Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7</li> <li>2. Upgrade to 6.2.3x</li> </ol>	<ol style="list-style-type: none"> <li>1. Upgrade to 5.5.3 or 5.5.5x</li> <li>2. Upgrade to 6.2.3x</li> </ol>
4.2.x	<ol style="list-style-type: none"> <li>1. Upgrade to version 4.3.x through 5.4.x</li> <li>2. Upgrade to 5.5.3 or 5.5.5x (5.5.5, 5.5.5a), or 5.5.7</li> <li>3. Upgrade to 6.2.3x</li> </ol>	<ol style="list-style-type: none"> <li>1. Upgrade to version 4.3.x through 5.4.x</li> <li>2. Upgrade to 5.5.3 or 5.5.5x</li> <li>3. Upgrade to 6.2.3x</li> </ol>



#### Note

When you upgrade from WAAS Software Version 5.5.x to 6.2.3b, the expired SSL certificates do not get removed automatically and show up in the alarms.

### Upgrading from Cisco WAAS Version 5.x and Later to Version 6.2.3x

This section contains the following topics:

- [WAAS Version 5.1 and Later: NTLM](#)
- [WAAS Version 5.2 and Later: Usernames](#)
- [WAAS Version 5.3 and Later: Name and Description Fields](#)
- [WAAS Version 6.2.3x: vWAAS](#)
- [WAAS Version 6.2.3x: vCM-100 with RHEL KVM or KVM on CentOS](#)

## WAAS Version 5.1 and Later: NTLM

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

## WAAS Version 5.2 and Later: Usernames

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*—Change usernames in the Central Manager **Admin > AAA > Users** page.

*For remotely authenticated users*—Change 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.

## WAAS Version 5.3 and Later: Name and Description Fields

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 Centralized Management System (CMS) logs.

## WAAS Version 6.2.3x: vWAAS

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.

## WAAS Version 6.2.3x: vCM-100 with RHEL KVM or KVM on CentOS

If you upgrade to WAAS Version 6.2.3x, or downgrade from WAAS Version 6.2.3x to an earlier version, and use a vCM-100 model with the following parameters, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

- vCM-100 has default memory size of 2 GB
- vCM-100 uses the RHEL KVM or KVM on CentOS hypervisor

- You use either the **restore factory-default** command or the **restore factory-default preserve basic-config** command



**Note** The **restore factory-default** command erases user-specified configuration information stored in the flash image, including the starting configuration of the device, and also removes data from the disk, user-defined partitions, and the entire Central Manager database.

To resolve this situation, follow these steps:

- Power down the vWAAS using the **virsh destroy *vmname*** command or the virt manager.
- Power up the vWAAS using the **virsh start *vmname*** command or the virt manager.

This upgrade/downgrade scenario does not occur for vCM-100 models whose memory size is upgraded to 4 GB.

## Upgrading from Cisco WAAS Version 4.2.x to Version 6.2.3x

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 7](#).

## Workflow: Upgrading from a Release Version to Version 6.2.3x

To upgrade from a Release Version to Version 6.2.3x, complete the tasks listed in [Table 8](#).

**Table 8** *Workflow: Upgrading from a Release Version to Version 6.2.3x*

Workflow Task	Description
<ul style="list-style-type: none"> <li><a href="#">Upgrade Part 1: Create a Backup of the Primary WAAS CM Database</a></li> </ul>	<ul style="list-style-type: none"> <li><i>Before you start the upgrade process</i> from a release version to Version 6.2.3x, create a backup of the primary WAAS CM database and save it to a remote location.</li> </ul>
<ul style="list-style-type: none"> <li><a href="#">Upgrade Part 2: Upgrade the Standby WAAS CM</a></li> </ul>	<ul style="list-style-type: none"> <li>If your WAAS system has a standby WAAS CM, upgrade the standby WAAS CM <i>before</i> you upgrade the primary WAAS CM.</li> </ul>
<ul style="list-style-type: none"> <li><a href="#">Upgrade Part 3: Upgrade the Primary WAAS CM</a></li> </ul>	<ul style="list-style-type: none"> <li>Upgrade the primary WAAS CM, including verifying that the new WAAS image is loaded correctly, verifying connectivity between WAAS CM and all WAE devices, and verifying that all WAE devices are online.</li> </ul>
<ul style="list-style-type: none"> <li><a href="#">Upgrade Part 4: Upgrade the Branch WAE Devices</a></li> </ul>	<ul style="list-style-type: none"> <li>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.</li> </ul>
<ul style="list-style-type: none"> <li><a href="#">Upgrade Part 5: Upgrade the Data Center WAAS Software</a></li> </ul>	<ul style="list-style-type: none"> <li>Upgrade the data center WAAS software, including upgrading each data center WAE device.</li> </ul>

Workflow Task	Description
<ul style="list-style-type: none"> <li>• <a href="#">Upgrade Part 6: Upgrade Each Data Center WAE</a></li> </ul>	<ul style="list-style-type: none"> <li>• Upgrade each data center WAE device, including disabling and re-enabling WCCP</li> </ul>
<ul style="list-style-type: none"> <li>• <a href="#">Upgrade Part 7: WCCP and Migration Processes</a></li> </ul>	<ul style="list-style-type: none"> <li>• 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>.</li> </ul>
<ul style="list-style-type: none"> <li>• <a href="#">Upgrade Part 8: Post-Upgrade Tasks</a></li> </ul>	<ul style="list-style-type: none"> <li>• <i>After you complete the WAAS system upgrade to Version 6.2.3x, perform tasks including clearing your browser cache, verifying licenses, and verifying proper configuration of applications accelerators, policies, and class maps.</i></li> </ul>

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

This section contains the following topics:

- [Prerequisite for Primary WAAS CM Database Backup](#)
- [Creating a Primary WAAS CM Database Backup](#)

### Prerequisite for Primary WAAS CM Database Backup

Note the following different CMS database backup scenarios, depending on the size of /sw and /swstore:

- If you are upgrading your vCM, vWAAS, ISR-WAAS, or SRE device from an earlier WAAS version to WAAS Version 6.2.3x, *and the /sw and /swstore partition size is less than 2GB*, you must back up the CMS database *before* creating a backup of the primary WAAS CM database, following the instructions described in the [Caution](#) note.
- *For devices using WAAS Version 5.x*, the /sw and /swstore partition size is 1GB, so you must back up the CMS database, you must back up the CMS database *before* creating a backup of the primary WAAS CM database, following the instructions described in the [Caution](#) note.
- *For devices using WAAS Version 6.x*, the /sw and /swstore partition size is 2GB, so you do not need to create a backup of the CMS database before creating a backup of the primary WAAS CM database.



#### Caution

If you are upgrading your WAAS device from an earlier WAAS version to WAAS Version 6.2.3x, *and the /sw and /swstore partition size is less than 2 GB*, 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 6.2.3x.

The upgrade process on this type of configuration will automatically clear system and data partition, which will erase the WAAS CM database.

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



## Creating a Primary WAAS CM Database Backup

Before upgrading to WAAS Version 6.2.3x, follow these steps to create a backup of the WAAS CM database:

- 
- Step 1** Use Telnet or SSH to access the primary WAAS 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** Use Telnet or SSH to access the standby WAAS CM IP address:
- Step 2** Copy the new software image to the standby WAAS CM with the WAAS CLI **copy ftp** command.
- The following example shows the file in the root directory. Provide the correct path on your WAAS system, if different from the root directory path.
- ```
wae# copy ftp install ftpserver / waas-image.bin
```
- 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** Use Telnet or SSH to access the primary WAAS CM IP address:
- Step 2** Copy the new software image to the primary WAAS CM, either from the WAAS CM or the CLI.
- From the WAAS CM:
- In the Standby WAAS CM, navigate to **Admin > Versioning > Software Update**.
  - From the Software Files listing, select the new software version.
  - Click **Submit**.
- From the CLI:
- Use the **copy ftp** command.
- The following example shows the file in the root directory. Provide the correct path on your WAAS system, if different from the root directory path.
- ```
wae# copy ftp install ftpserver / waas-image.bin
```
- Step 3** Copy the new Version 6.2.3x 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 4** Reload the primary WAAS CM, using the **reload** command
- Step 5** Verify that the new Version 6.2.3x image is loaded correctly, using the **show version** command.
- Step 6** To confirm connectivity, ping the standby WAAS CM (if present in your WAAS system) and branch WAE devices.
- Step 7** Confirm that the CMS services are running, using the **show cms info** command.
- Step 8** Choose **Devices > All Devices** and verify that all WAE devices are online.
- Step 9** 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 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:8443`
- Step 2** Verify that all WAE devices are online (displaying green).
- Step 3** Resolve any alarm conditions that may exist.
- Step 4** Copy the new software image to the branch WAE, either from the WAAS CM or the CLI.  
 From the WAAS CM:
- In the branch WAE, navigate to **Admin > Versioning > Software Update**.
  - From the Software Files listing, select the new software version.
  - Click **Submit**.
- From the CLI:
- Use the **copy ftp** command. You can use either Universal or Accelerator-only images.  
 The following example shows the file in the root directory. Provide the correct path on your WAAS system, if different from the root directory path.  

```
wae# copy ftp install ftpserver / waas-image.bin
```
- Step 5** Reload the WAE using the **reload** command.
- Step 6** Verify that the new Version 6.2.3x software image has installed correctly, using the **show version** command.
- Step 7** Verify that the correct licenses are installed, using the **show license** command.
- Step 8** If you have purchased an Enterprise license and have enabled it, proceed to [Step 10](#).  
 If you have purchased an Enterprise license and have not yet enabled it, perform the following tasks:
- Clear the Enterprise license, using the **clear license transport** command.
  - Add the Enterprise license, using the **license add enterprise** command.
- Step 9** Save the changed configuration, using the **copy running-config startup-config** command.
- Step 10** From the primary WAAS CM, choose **Devices > branchWAE**, to verify that the WAE device is online and has a *green* status.
- Step 11** 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 12](#).  
 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.
  - Save the changed configuration, using the **copy running-config startup-config** command.

- Step 12** The branch WAE devices within the active WAAS network are now upgraded to the current WAAS Version 6.2.3x.

## 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:8443`
- 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:
- Disable WCCP with the **no wccp tcp-promiscuous service-pair serviceID serviceID** global configuration command.
  - Wait until the countdown expires, or use CTL-C to skip the countdown.
  - Verify that WCCP is disabled, using the **show wccp status** command.
  - 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:
- Step 5** Copy the new software image to the data center WAE, either from the WAAS CM or the CLI.
- From the WAAS CM:
- In the data center WAE, navigate to **Admin > Versioning > Software Update**.
  - From the Software Files listing, select the new software version.
  - Click **Submit**.
- From the CLI:
- Use the **copy ftp** command. You can use either Universal or Accelerator-only images.  
The following example shows the file in the root directory. Provide the correct path on your WAAS system, if different from the root directory path.
- ```

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

```
- Step 6** Reload the WAE using the **reload** command.
- Step 7** Verify that the new Version 6.2.3x software image has installed correctly, using the **show version** command.
- Step 8** Verify that WCCP is disabled, using the **show wccp status** command.
- Step 9** Save the changed configuration, using the **copy running-config startup-config** command.
- Step 10** From the primary WAAS CM, choose **Devices > branchWAE**, to verify that the WAE device is online and has a *green* status.
- Step 11** (Optional) Enable WCCP on all intercepting routers or switches in the list, if you have used [Step 2](#).
- Telnet to each core router or switch.
  - 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 12** Verify the following WAE device functionalities:
- 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.
  - Verify that redirecting router IDs are seen, using the **show wccp routers** command.
  - Verify that all WAEs in the cluster are seen, using the **show wccp clients** command.
  - Verify that the packet count to the WAE is increasing and no loops are detected, using the **show wccp statistics** command.
  - 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.
  - Verify that flows are being optimized, using the **show statistics connection** command.
  - If you are using WCCP for traffic interception, verify that WCCP is working properly, using the **show running -config wccp** command.

- Step 13** Each data center WAE within the active WAAS network is now upgraded to the current WAAS Version 6.2.3x.
- 

## 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 6.2.3x:

- 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 6.2.3x, 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 6.2.3x, 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 6.2.3x, 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 6.2.3x, 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 6.2.3x:

- 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 6.2.3x. 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 6.2.3x to a Previous Version

This section contains the following topics:

- [Downgrading the WAAS System from Version 6.2.3x to a Previous Version](#)
- [Downgrading the WAAS CM from Version 6.2.3x to a Previous Version](#)

## Downgrading the WAAS System from Version 6.2.3x to a Previous Version

This section contains the following topics:

- [Downgrade Path Considerations](#)

- [Downgrade Component and Data Considerations](#)

## Downgrade Path Considerations

- Downgrading from 6.2.3x is supported to 6.2.1x, 6.1.1a, 6.1.1, 5.5.7, 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 6.2.3x 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 6.2.3x, 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 6.2.3x 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 from 6.2.3x WAAS CM directly to a version earlier than Version 5.5.3 is blocked.
- If the 6.2.3x WAAS CM 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 6.2.3x 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** All Cisco WAAS nodes in an AppNav deployment must be running Cisco WAAS version 5.0 or later.

## 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 6.2.3x:

- 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 6.2.3x, 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.

## Software Version 6.2.3x Resolved and Open Caveats, and Command Changes

This section contains the resolved caveats, open caveats, and command changes in Software Version 6.2.3x, fixed and known and contains the following topics:

- [Cisco WAAS Software Version 6.2.3e Resolved Caveats](#)
- [Cisco WAAS Software Version 6.2.3e Open Caveats](#)
- [Cisco WAAS Software Version 6.2.3d Resolved Caveats](#)
- [Cisco WAAS Software Version 6.2.3d Open Caveats](#)
- [Cisco WAAS Software Version 6.2.3c Resolved Caveats](#)
- [Cisco WAAS Software Version 6.2.3c Open Caveats](#)
- [Cisco WAAS Software Version 6.2.3b Resolved Caveats](#)
- [Cisco WAAS Software Version 6.2.3b Open Caveats](#)
- [Cisco WAAS Software Version 6.2.3a Resolved Caveats](#)
- [Cisco WAAS Software Version 6.2.3a Open Caveats](#)
- [Cisco WAAS Software Version 6.2.3 Resolved Caveats](#)
- [Cisco WAAS Software Version 6.2.3 Open Caveats](#)
- [Cisco WAAS Software Version 6.2.3 Command Changes](#)
- [Using Previous Client Code](#)

### Cisco WAAS Software Version 6.2.3e Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.2.3e.

| Caveat ID Number           | Description                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvk03838</a> | Optimization not working between 623e and other released versions.                                   |
| <a href="#">CSCvf28759</a> | Need to restrict the upgrade of vwaas6k on 960 GB SSD                                                |
| <a href="#">CSCvg61872</a> | Azure vWAAS-6K showing the Model as Reduced-DC                                                       |
| <a href="#">CSCvg76146</a> | Unable to do SSH to Azure WAAS after downgrading to 6.2.1-b11 from 6.4.0 image                       |
| <a href="#">CSCvf55876</a> | Input Packet Drops, Consuming too much resources causing network down                                |
| <a href="#">CSCvg29766</a> | Waasnet process restarts when removing bridgegroup from interface and assigning IP                   |
| <a href="#">CSCvg56020</a> | Continuous waasnet service restart observed with Mix AO traffic profile                              |
| <a href="#">CSCvf24960</a> | Frequently SSL replumbing error messages seen while connection closing immediately after open        |
| <a href="#">CSCvh88834</a> | SSLAO service restart when peer SSL AO information is not available in AOIM.                         |
| <a href="#">CSCul14659</a> | SSL/TLS use of weak RC4 cipher port 8443/tcp over SSL CVE-2013-2566                                  |
| <a href="#">CSCvg99470</a> | SSL accelerator enabled back after box reload while it was disabled before reload                    |
| <a href="#">CSCvg33919</a> | Svcdisabled alarm raised by ssl_itps when ASVC is configured with chained cert                       |
| <a href="#">CSCvf25027</a> | WAAS fix CVE-2017-3167, CVE-2017-3169, CVE-2017-7679, and CVE-2017-9788.                             |
| <a href="#">CSCvf01245</a> | Cluster went to down Due to "TFO accelerator load level has been set to 0" in SN                     |
| <a href="#">CSCvi40884</a> | Apache Traffic Server host header and line folding                                                   |
| <a href="#">CSCvi82153</a> | Traffic is Dropped at The SN when cma process is restarted                                           |
| <a href="#">CSCvg40834</a> | Traffic_server core with Akamai cache                                                                |
| <a href="#">CSCvh23590</a> | Unwanted warning message displayed after enabling Akamai config                                      |
| <a href="#">CSCvc83974</a> | Akamai process restarts unexpectedly, leaves a dump file                                             |
| <a href="#">CSCvj25184</a> | Akamai process restarts unexpectedly and leaves a dump file while accessing sites with curl command. |
| <a href="#">CSCvg76284</a> | httpcache service has been disabled with akamai enabled                                              |
| <a href="#">CSCvf84769</a> | Inadequate monitoring of http object cache component                                                 |
| <a href="#">CSCvg81918</a> | object cache partitions created with wrong sizes after partition delete                              |
| <a href="#">CSCvh96772</a> | exec_pkt_cap process memory dump file got generated                                                  |
| <a href="#">CSCve72132</a> | test_stat process memory dump gets generated when FG_DUMP debug command is run.                      |
| <a href="#">CSCvi06590</a> | Perf degradation with HTTPS/Live Streaming in 641 when compared to 623d                              |
| <a href="#">CSCuw17054</a> | MAPI AO gets disabled and MAPI Core observed for RPC-HTTPS with Kerberos                             |
| <a href="#">CSCvf01746</a> | WAAS HTTP AO process httpmuxd consumes more memory causing multiple AO keepalive timeouts            |
| <a href="#">CSCvi40799</a> | Timeout observed at 180 seconds                                                                      |
| <a href="#">CSCvj06770</a> | Connection timeout at 180 seconds, despite origin not responding for over 6 minutes                  |
| <a href="#">CSCvg38704</a> | HTTPAO should raise an alarm when split header limit reached and traffic is dropped                  |
| <a href="#">CSCvh51200</a> | Bypass server configuration with wild cards are not working in HTTPAO                                |
| <a href="#">CSCvb08476</a> | WAAS: ICA AO service restart observed in device                                                      |

| Caveat ID Number            | Description                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCve65800</a>  | Device registration to CM fails when management flow goes via inline data-path                       |
| <a href="#">CSCvf97803</a>  | Router registration to 6.x of CM : "enable password" not supported                                   |
| <a href="#">CSCvd78539</a>  | Device hung and unavailable on network due to TX Hung                                                |
| <a href="#">CSCvh07778</a>  | Replacement device gets assigned to group for newly activated devices                                |
| <a href="#">CSCvg97531</a>  | log file size is growing beyond 48MB, WAAS device will run out of disk space                         |
| <a href="#">CSCvg74712</a>  | Inline interfaces were down post reload in interception mode                                         |
| <a href="#">CSCvf09323</a>  | Multiple Vulnerabilities in ntp                                                                      |
| <a href="#">CSCvd94539</a>  | Timestamps missing after negotiated in single sided scenario                                         |
| <a href="#">CSCvf82199</a>  | WCCP flaps and WAASNET memory dump observed while restoring policies after WAE reload                |
| <a href="#">CSCvf55664</a>  | fda service triggers reload while waasnet restarts                                                   |
| <a href="#">CSCve81510</a>  | Rarely seeing waasnet service restart with interface flap in Inline interception                     |
| <a href="#">CSCvf79425</a>  | WAASNET process memory dump gets generated when SMB AO service restarts multiple times               |
| <a href="#">CSCvg18237</a>  | Connections are pending for PT APP CFG flows.                                                        |
| <a href="#">CSCva80599</a>  | NGSSL : Stuck connection when HTTP AO is restarted                                                   |
| <a href="#">CSCvf38574</a>  | NGSSL : Stuck connection when HTTP AO is restarted - DDTS to track fix from AOSHELL                  |
| <a href="#">CSCvg08380</a>  | TsDL stuck on Edge and Core while running ngssl dual sided traffic                                   |
| <a href="#">CSCvg73808</a>  | THsDL/Ts stuck on Edge and Core with ngssl real time traffic                                         |
| <a href="#">CSCCuy82470</a> | Connection reset seen while sending mails with large attachments                                     |
| <a href="#">CSCvf58933</a>  | THDL unresponsive connections observed while running http/ssl traffic                                |
| <a href="#">CSCvh07373</a>  | Observing more number of PT connections and connections are not scaling while running akc perf test  |
| <a href="#">CSCvh10643</a>  | Connection is getting pushed down from windows to Netapp server after the password change            |
| <a href="#">CSCvh49517</a>  | Connection reset with Win10 client when SMB 2.1-Mute config is set                                   |
| <a href="#">CSCvg85350</a>  | Security Keys not getting invalidated upon failure at EDGE and connection being reset continuously   |
| <a href="#">CSCve68201</a>  | Permanent connectivity issue on virtual ethernet                                                     |
| <a href="#">CSCvi05071</a>  | Multiple notifications of the same alarm                                                             |
| <a href="#">CSCva96382</a>  | eth_bypass alarm gets generated without reason                                                       |
| <a href="#">CSCve21589</a>  | WAAS SR_DRS_CRACK_NAME alarm occurring frequently.                                                   |
| <a href="#">CSCvf29847</a>  | Raised alarm counter not updated in Email when alarms raised and cleared within the polling interval |
| <a href="#">CSCvf71387</a>  | AlarmEMailNotification page,mail is not triggered for the combination of valid and dummy addresses   |
| <a href="#">CSCvf55798</a>  | Email notification is not triggered for CM based alarms like CMS-Secure-store , clock mismatch       |



| Caveat ID Number           | Description                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------|
| <a href="#">CSCvh13100</a> | Unwanted alarm raised while starting http object-cache                                       |
| <a href="#">CSCvf58311</a> | Documentation : snmp remote engine ID mandatory for snmp notify inform trap for v3 user      |
| <a href="#">CSCvg90211</a> | WAVE-294-K9 does not respond with CDP Neighborhood Table details when polled via SNMP        |
| <a href="#">CSCvf18223</a> | WAE reload got stuck with stopping pid, can't proceed until connect to console               |
| <a href="#">CSCvf62979</a> | Rarely device goes offline or Central manager fails to contact device                        |
| <a href="#">CSCvf58709</a> | SMBAO process restarted unexpectedly with dbo 2.1 traffic pattern.                           |
| <a href="#">CSCvg63085</a> | SMB Digital Key not refreshing digital Key with account password change                      |
| <a href="#">CSCvg19496</a> | WAAS:623d:SMBAO Core after receiving partial leasekey from server                            |
| <a href="#">CSCvg24312</a> | Branch SMBAO memory usage goes above the expected limit                                      |
| <a href="#">CSCvf58745</a> | SMB Object-Cache: obj_entry and transaction statistics showing improper values               |
| <a href="#">CSCvg24344</a> | SMBAO memory leak seen on the DC device with high signed traffic                             |
| <a href="#">CSCvg25861</a> | SMBV3 signed pushdown connections result in SMBAO memory leak on branch WAE                  |
| <a href="#">CSCvg03370</a> | Reducing the SMB Object Cache memory which it takes at start up                              |
| <a href="#">CSCvh10339</a> | SMB connection not optimized when security keys fail at Branch box                           |
| <a href="#">CSCvg26443</a> | CM Chart update fail with collecting statistics of the application: SMB failuer              |
| <a href="#">CSCvf20884</a> | Tacacs+ command authorization failed for user unknown and keep pushing the config from CM    |
| <a href="#">CSCvf81284</a> | Optimization stops silently upon flow table overflow                                         |
| <a href="#">CSCvh24158</a> | Fault response from server for request opnum 65535                                           |
| <a href="#">CSCvh60335</a> | Disk SMART warning not reported to user                                                      |
| <a href="#">CSCvg47760</a> | Handle the raid controller's OCR event                                                       |
| <a href="#">CSCvh55089</a> | RAID1 missing disk is not reported                                                           |
| <a href="#">CSCvg23772</a> | Statistics to check the load by pass failures due to usage and disk latency                  |
| <a href="#">CSCvi54862</a> | packet capture processing does not stop when the ssh session timeouts                        |
| <a href="#">CSCvh22217</a> | Inline module is dropping icmp packets                                                       |
| <a href="#">CSCvg50517</a> | GPO update failed due to guest bit set in session setup response                             |
| <a href="#">CSCvj13159</a> | Zero Mac is getting programmed in WAAS when gateway interface is flapped in Apnnav-xe setup  |
| <a href="#">CSCvg20842</a> | WAAS Command Authorization fails when sending commands with multiple arguments to ACS server |
| <a href="#">CSCvd32072</a> | Failed to generate sysreport in SN while running more than 30k connection                    |
| <a href="#">CSCvf57958</a> | Restart of bash process                                                                      |
| <a href="#">CSCvf23058</a> | Segmentation fault related to xargs in in__libc_start_main ()                                |
| <a href="#">CSCve71066</a> | FTP connection failure with WAAS after FTP client "MLSD" request.                            |
| <a href="#">CSCvg34336</a> | ISR-WAAS is blocking traffic when there is a MTU change in packet path                       |

| Caveat ID Number           | Description                                                                           |
|----------------------------|---------------------------------------------------------------------------------------|
| <a href="#">CSCvg35976</a> | Getting authentication prompt when WAAS in place the proxy attempts to negotiate NTLM |
| <a href="#">CSCvi37887</a> | Lower DRE error 'Invalid frame version received from peer' to trace level             |

## Cisco WAAS Software Version 6.2.3e Open Caveats

The following caveats are open in Software Version 6.2.3e. Note that there might be additional open caveats from previous releases that are applicable to this release, unless they are specifically listed as resolved.

| Caveat ID Number           | Description                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvk30565</a> | Observed SMBAO Single Client Performance degradation for large file download                         |
| <a href="#">CSCvj53057</a> | HTTP/S connections with DNS failures lock HTTP AO resources (httpmuxd64)                             |
| <a href="#">CSCvi36270</a> | Connection not hitting correct classifier although correct accelerators are applied                  |
| <a href="#">CSCvj16852</a> | In Device status page, Router alarms count not in sync with Device status & AlarmPanel               |
| <a href="#">CSCvj07016</a> | WAASNet process going pending state and not handling traffic in a scenario                           |
| <a href="#">CSCvj32470</a> | waasnet process restart and memory dump observed with MAX flows                                      |
| <a href="#">CSCvj30270</a> | WAASNET process memory dump gets generated in WAAS 6.4.1a                                            |
| <a href="#">CSCvj51761</a> | WAASNet service restart with a core file with wn_dft_thread and DP handler                           |
| <a href="#">CSCvi84306</a> | WAASNET service restart seen in SN in a scenario during high load test                               |
| <a href="#">CSCvi73822</a> | SSL Accelerated service & Certificate expiry Alarms observed in GUI but not in CLI                   |
| <a href="#">CSCvj21786</a> | SMB AO office files are failing to open after save via SMBv1                                         |
| <a href="#">CSCvi94691</a> | SMBAO memory increasing gradually during high load and pushdown scenarios                            |
| <a href="#">CSCvj53621</a> | SMBAO created a core dump due to handling non existent Negotiate Response                            |
| <a href="#">CSCvi71814</a> | SMB AO:Rarely Last Write timestamp is changed during file copy and paste                             |
| <a href="#">CSCvj41880</a> | Observed SMBAO Single Client Performance degradation with normalise buffer check                     |
| <a href="#">CSCvh96699</a> | Unusually large amount of memory Consumed by SMBAO on the DC device longevity test on rare condition |
| <a href="#">CSCvi97288</a> | FTP data transfer failed from branch wave when management interface configured                       |
| <a href="#">CSCvh47298</a> | SNMP service poll returns unknown username in a scenario                                             |
| <a href="#">CSCvi02645</a> | SNMP service restart seen in WAE device in a scenario                                                |
| <a href="#">CSCvi73273</a> | Akamai proxy configuration differs from CM GUI                                                       |
| <a href="#">CSCvh03423</a> | Connections not getting redirect to SN WAE device in a scenario                                      |

| Caveat ID Number           | Description                                                                       |
|----------------------------|-----------------------------------------------------------------------------------|
| <a href="#">CSCvh96906</a> | Force device group setting need to be applied multiple time to fix local override |
| <a href="#">CSCvh51119</a> | Throughput fluctuation seen with ESXI-vWAAS-6K with UCS-E160D-M2 and UCS-E180D-M2 |

## Cisco WAAS Software Version 6.2.3d Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.2.3d.

| Caveat ID Number           | Description                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------|
| <a href="#">CSCvd81077</a> | httpcache service died multiple times                                                           |
| <a href="#">CSCvf21935</a> | httpcache service has been disabled with akamai enabled                                         |
| <a href="#">CSCve79892</a> | Observed HTTP traffic-interruption in Branch due to malformed http request                      |
| <a href="#">CSCvf53563</a> | Traffic_server process restarted while accessing corrupted gzip file                            |
| <a href="#">CSCvf42490</a> | Flow segment is not released by HTTP AO while running single-sided Https traffic via Proxy      |
| <a href="#">CSCve59122</a> | HTTP AO restarted while running sharepoint traffic                                              |
| <a href="#">CSCvf35961</a> | HTTP AO service died due to http traffic run                                                    |
| <a href="#">CSCve20802</a> | Stuck connections observed due to sendsocket event                                              |
| <a href="#">CSCve71887</a> | SCCM/PXE traffic interrupted while WAAS is in the path                                          |
| <a href="#">CSCve74457</a> | Core dump seen in ICA AO and restarted                                                          |
| <a href="#">CSCve72253</a> | Rarely Core dump generated for MAPI AO with RPCHTTP(s) traffic                                  |
| <a href="#">CSCva52094</a> | SR-Server CORE observed reactivating ISR WAAS with Hostname change                              |
| <a href="#">CSCvd08821</a> | Stuck Connection with TM, under load conditions for MAPI-RPCHTTP Traffic                        |
| <a href="#">CSCve05349</a> | Akamai status going to ERROR state while clicking on override group settings button from CM GUI |
| <a href="#">CSCvd68640</a> | Akamai Status to added in GUI as "Pending with reload" when reload is required manually         |
| <a href="#">CSCvd87574</a> | Cisco Wide Area Application Services Central Manager Information Disclosure Vulnerability       |
| <a href="#">CSCvd78045</a> | CM GUI shouldn't allow to create trigger with invalid mib name in interop                       |
| <a href="#">CSCve15397</a> | CM-AppNav polling sessions get stuck and result in AppNav remaining offline forever             |
| <a href="#">CSCvd77681</a> | DG configurations are not pushed to WAE when SSL AO is disabled in WAE                          |
| <a href="#">CSCvd81462</a> | DG dropdown "select a device group" option is not working in SSL global settings page           |
| <a href="#">CSCve64337</a> | DG- Remove Settings is throwing error messages                                                  |

| Caveat ID Number           | Description                                                                                        |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvd48873</a> | Force device group appears due to config not sync for Securestore page while register fresh device |
| <a href="#">CSCvd61131</a> | ForceDeviceGroup appears when device automatically assign to DeviceGroup if DiskEncryption enabled |
| <a href="#">CSCva54052</a> | NTP server CM GUI configuration push is failed for vWAAS deployed in KVM                           |
| <a href="#">CSCvc12651</a> | Remote Authentication user without privileges to be deleted during Upgrade                         |
| <a href="#">CSCvd82891</a> | SNMP host community/ user special char restriction should be parity with CLI                       |
| <a href="#">CSCvb78641</a> | TACACS authentication failing after upgrade                                                        |
| <a href="#">CSCve53942</a> | WCM AppNavXE statistics collection thread may freeze for a while                                   |
| <a href="#">CSCve91472</a> | In some cases Object Cache Server (ocserver) process stopped and restarted                         |
| <a href="#">CSCve78125</a> | OC process stopped and restarted when garbage collector failed to update db                        |
| <a href="#">CSCvd89141</a> | SMB AO restarted due to "oc_client_ipc_send_error_response_msg" function                           |
| <a href="#">CSCuz29040</a> | SMBAO load test resulting in OC_Open Pending counter remaining constant                            |
| <a href="#">CSCve29588</a> | SMBAO Object cache Rename file descriptor leak observed during load condition                      |
| <a href="#">CSCvc23114</a> | Looped Packets from 2 RTRS with lesser mtu goes with invalid checksum                              |
| <a href="#">CSCvf47948</a> | Client sending kerberos security blob in two session setup requests cause reset                    |
| <a href="#">CSCve16092</a> | encryption-service process reloaded unexpectedly while optimizing SMBv3 signed connections         |
| <a href="#">CSCve49142</a> | Failure processing split server response with non success status                                   |
| <a href="#">CSCve11987</a> | Object cache File descriptor leaks due to "current open file handles" are closed by smbao          |
| <a href="#">CSCvc06665</a> | Observed connection resets observed in DBO cache eviction scenario                                 |
| <a href="#">CSCve74033</a> | Process restarted due to DirBrowsingResource while running the long load test                      |
| <a href="#">CSCvf56703</a> | SMB AO FD leak while running heavy directory browsing traffic                                      |
| <a href="#">CSCvf77875</a> | SMB AO service restarts when accessing security layer in unsigned session setup packet.            |
| <a href="#">CSCve47337</a> | SMB Core Files due to windows-domain encryption-service, on Upgrading WAAS                         |
| <a href="#">CSCvf47958</a> | SMBAO client denial list is not getting updated for SMB AO generated reset                         |
| <a href="#">CSCvf58709</a> | SMBAO process restarted unexpectedly with dbo 2.1 traffic pattern.                                 |
| <a href="#">CSCvf41079</a> | SMBAO restarted with OC memory corruption                                                          |
| <a href="#">CSCve19211</a> | SMBAO Unexpected restart while handling Lib Crypto                                                 |
| <a href="#">CSCvd91293</a> | ASVC_Transport core seen on 623c while running Mixed AO traffic                                    |
| <a href="#">CSCva95837</a> | NGSSL: ASVC with server-name does not get configured in ASVCStore                                  |
| <a href="#">CSCvd73314</a> | Stuck Connections observed in Single sided NGSSL traffic via proxy                                 |
| <a href="#">CSCve75509</a> | DRE partition is full and getting lot of 'No space left on device' logs                            |
| <a href="#">CSCva45688</a> | Shutdown CLI need to shutdown the vWAAS instance                                                   |
| <a href="#">CSCve58163</a> | vWAAS Never Powers Down VM                                                                         |
| <a href="#">CSCvd32072</a> | Failed to generate sysreport in SN while running more than 30k connection                          |

| Caveat ID Number           | Description                                                                          |
|----------------------------|--------------------------------------------------------------------------------------|
| <a href="#">CSCvd62595</a> | Top command showing Garbage value with AppNav Interception                           |
| <a href="#">CSCve86619</a> | Cannot SSH to WAAS By Using InlineGroup Interface                                    |
| <a href="#">CSCve70447</a> | ISR-WAAS becomes unreachable after upgrade to 623c on 4321                           |
| <a href="#">CSCvc67937</a> | lowmem_reserve and memory allocation failure                                         |
| <a href="#">CSCve00712</a> | Multiple AO service got disabled on multiple SN's while mixed AO traffic is running  |
| <a href="#">CSCvc10545</a> | Need to show interface details when receiving SNMP Link up/ down traps               |
| <a href="#">CSCvd50984</a> | SNMP restarts unexpectedly leaving a core file                                       |
| <a href="#">CSCuz56155</a> | WAAS SR server failed in Key retrieval                                               |
| <a href="#">CSCvd90139</a> | PMD memory leak occurs while configuring bulk class map policy                       |
| <a href="#">CSCvf04748</a> | PMD service restarted after WAASNET Restart                                          |
| <a href="#">CSCvd88250</a> | Processing time is more after configuring class-map having 800+ entries              |
| <a href="#">CSCva00161</a> | TFO:capped on speed: low latency between WAAS and server in Cloud                    |
| <a href="#">CSCve82523</a> | HTTPS stuck connections on Core and Edge both                                        |
| <a href="#">CSCve29255</a> | Observed THSDL stuck connections while accessing http/https websites via squid proxy |
| <a href="#">CSCvd02911</a> | Waasnet core in fg_endp_close_ext function in ICA traffic during load test           |
| <a href="#">CSCvf05107</a> | Waasnet error logging when timestamp option not found                                |
| <a href="#">CSCve53939</a> | waasnet service restarted when enabling InlineGroup                                  |
| <a href="#">CSCvd38216</a> | WNDFT core file seen in WAAS when serving mixed AO traffic.                          |

## Cisco WAAS Software Version 6.2.3d Open Caveats

The following caveats are open in Software Version 6.2.3d. Note that there might be additional open caveats from previous releases that are applicable to this release, unless they are specifically listed as resolved.

| Caveat ID Number           | Description                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvf58933</a> | THDL stuck connection observed while running http/ssl traffic                                        |
| <a href="#">CSCvf50909</a> | HTTP Stuck connections and sysreport could not be generated                                          |
| <a href="#">CSCvf51154</a> | THs stuck connection observed intermittently when sending HTTPs traffic via proxy                    |
| <a href="#">CSCvf71387</a> | AlarmEMailNotification page,mail is not triggered for the combination of valid and dummy addresses   |
| <a href="#">CSCvf55798</a> | Email notification is not triggered for CM based alarms like CMS-Secure-store , clock mismatch       |
| <a href="#">CSCvf26917</a> | ForceDeviceGroup seen in port channel page for round-robin option                                    |
| <a href="#">CSCvf29847</a> | Raised alarm counter not updated in Email when alarms raised and cleared within the polling interval |

| Caveat ID Number           | Description                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------|
| <a href="#">CSCvf83883</a> | SSH enable failed only 1st time from GUI if device upgraded without SSH and without Key     |
| <a href="#">CSCva58191</a> | SMB AO restarted during eviction of object cache at load condition.                         |
| <a href="#">CSCvd96948</a> | SMB AO restarted during object cache file invalidation                                      |
| <a href="#">CSCvf51931</a> | SIA Invalid Pkt Alarms seen on 7571                                                         |
| <a href="#">CSCvf58709</a> | SMBAO process restarted unexpectedly with dbo 2.1 traffic pattern.                          |
| <a href="#">CSCvf55876</a> | SMBAO: Consuming too much resources causing network down                                    |
| <a href="#">CSCve21589</a> | WAAS SR_DRS_CRACK_NAME alarm occurring frequently.                                          |
| <a href="#">CSCvf83563</a> | ISR-WAAS goes to ActivateFailed state on multiple events                                    |
| <a href="#">CSCve68201</a> | Permanent connectivity issue on virtual ethernet                                            |
| <a href="#">CSCvf02875</a> | Reducing the memory utilized by ISR-WAAS-200                                                |
| <a href="#">CSCve43393</a> | Non encoded messages are sent to DRE decoder after disabled by AO                           |
| <a href="#">CSCvd93324</a> | SO_DRE service restarted due to segmentation fault seen on 623c while running Mixed Traffic |
| <a href="#">CSCvf58729</a> | Stuck connection observed while running load test                                           |
| <a href="#">CSCvf01245</a> | Cluster went to down Due to "TFO accelerator load level has been set to 0" in SN            |
| <a href="#">CSCvf58746</a> | Device going unresponsive due to delay in processing IO waits                               |
| <a href="#">CSCvd78539</a> | Device hung and unavailable on network due to TX Hung                                       |
| <a href="#">CSCvf32228</a> | Device was unreachable for a brief period                                                   |
| <a href="#">CSCvf55664</a> | fda service triggers reload while waasnet restarts                                          |
| <a href="#">CSCve71066</a> | FTP connection failure with WAAS after FTP client "MLSD" request.                           |
| <a href="#">CSCve53302</a> | Name Service Cache Daemon restarted in WAAS                                                 |
| <a href="#">CSCve81510</a> | Rarely seeing waasnet service restart with interface flap in Inline interception            |
| <a href="#">CSCvf51307</a> | WAAS Packet Capture command failed to work                                                  |
| <a href="#">CSCvc80702</a> | Losing connectivity to WAAS after changing the NTP Server IP with traffic                   |
| <a href="#">CSCvf82199</a> | Ocasionally wn_dft0 core file generated while restoring policies after reload               |
| <a href="#">CSCvf81284</a> | Optimization stops silently upon flow table overflow                                        |
| <a href="#">CSCvd94539</a> | Timestamps missing after negotiated in single sided scenario                                |
| <a href="#">CSCva11610</a> | Waasnet terminated during negative test conditions                                          |

## Cisco WAAS Software Version 6.2.3c Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.2.3c.

| Caveat_ID_Number            | Headline                                                                                 |
|-----------------------------|------------------------------------------------------------------------------------------|
| <a href="#">CSCvd94539</a>  | Timestamps missing after negotiated in single sided scenario                             |
| <a href="#">CSCvd76202</a>  | Connection stuck seen with HTTP traffic- dual sided                                      |
| <a href="#">CSCvd06515</a>  | WAAS box raising TFO limit alarm due to stuck connections in TH state                    |
| <a href="#">CSCvd44988</a>  | 'TFO: Statistics server not running' message is displayed with show stat tfo cli         |
| <a href="#">CSCvb81972</a>  | Improve memory resource in CE                                                            |
| <a href="#">CSCvd46295</a>  | Memory leaks in policy engine module during class-policy config push                     |
| <a href="#">CSCva65775</a>  | SMB accelerator and OC server process reloaded unexpectedly after 4 days of soak test    |
| <a href="#">CSCvc13956</a>  | SMB AO restarted while clearing object cache                                             |
| <a href="#">CSCvd75610</a>  | SMB AO restarted due to "smb2ReadLaunchOCRead ()" in Mega profile soak                   |
| <a href="#">CSCve06332</a>  | SMBAO : Directories Disappearing on Remote Files Shares                                  |
| <a href="#">CSCva33283</a>  | connection reset for SMB2 connections while doing file upload                            |
| <a href="#">CSCvc76036</a>  | Connections stuck for SMB due to failuer between WAASNET and SMBAO                       |
| <a href="#">CSCvc84457</a>  | smb connection consuming time in sessionsetup due to key-retrieval wait                  |
| <a href="#">CSCvc49776</a>  | Slow SMBAO Performance with oc_mgr: IO_BUSY: and write queue messages in logs            |
| <a href="#">CSCvc59105</a>  | SMB AO coredump or deadlocked when evicting the front LRU node                           |
| <a href="#">CSCvc17688</a>  | Core file alarm may raise for Object Cache Server or SMB Accelerator.                    |
| <a href="#">CSCCuy81194</a> | Core generated by smbao                                                                  |
| <a href="#">CSCvc97114</a>  | Key failure resets while running unsigned smbv3 soak profile                             |
| <a href="#">CSCva55682</a>  | SMB accelerator's Object Cache not disabled when config is pushed from CM's device group |
| <a href="#">CSCvd10188</a>  | Object-cache initialization stuck with 70% inodes and 90% cache size fill                |
| <a href="#">CSCvd53303</a>  | Akamai process restarted in accessing cached headers in stale/POST txn                   |
| <a href="#">CSCvc12602</a>  | Core file dumped when Akamai connect is enabled                                          |
| <a href="#">CSCvd00762</a>  | SMB accelerator reloads unexpectedly in soak run due to a conditional assert failure     |
| <a href="#">CSCvd54413</a>  | Traffic Server core                                                                      |
| <a href="#">CSCvd25445</a>  | Http object-cache traffic_server stops                                                   |
| <a href="#">CSCvd70864</a>  | event_base_loop core dump observed during Mega profile soak test                         |
| <a href="#">CSCvc29189</a>  | vwaas partitions missing after upgrade in one scenario                                   |
| <a href="#">CSCvd28998</a>  | WAAS devices unable to retrieve key and mark identity as blacklist.                      |
| <a href="#">CSCvc14370</a>  | SNMP Trigger not removed after downgrade from 623a to 557 in CM                          |
| <a href="#">CSCvd34739</a>  | SNMP Configuration not in sync with WCM and FDG appears in SNMP-DG                       |
| <a href="#">CSCvd39567</a>  | snmp sub-agent ccore file detected                                                       |
| <a href="#">CSCvc64841</a>  | Level 3 messages related to classifier name not found while querying snmp WAN opt mib    |

| Caveat_ID_Number           | Headline                                                                                                                                                                                                                                                                                  |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CSCvc95550</a> | Failures seen with polling snmp mibs iFTable, iFXTable on inline device                                                                                                                                                                                                                   |
| <a href="#">CSCvd53336</a> | Inline interface delays link propagation                                                                                                                                                                                                                                                  |
| <a href="#">CSCvd45642</a> | Restrict number of ssl_request_log.date and access_log.date logs files to 5                                                                                                                                                                                                               |
| <a href="#">CSCvc94792</a> | Logs in service_logs folder are not getting rolled over and compressed causing disk full                                                                                                                                                                                                  |
| <a href="#">CSCvd81787</a> | System message in Video Acceleration Transaction Log CM GUI and exceptions are seen in WCM cms_logs                                                                                                                                                                                       |
| <a href="#">CSCvb60453</a> | monitoring log file not logging any details in sysreport                                                                                                                                                                                                                                  |
| <a href="#">CSCvc67819</a> | Unexpected reload of smb accelerator process during long soak test.                                                                                                                                                                                                                       |
| <a href="#">CSCvb88945</a> | External SN blocks traffic when jumbo MTU is enabled                                                                                                                                                                                                                                      |
| <a href="#">CSCvc15749</a> | Empty server reply in a specific scenario with appnav interception                                                                                                                                                                                                                        |
| <a href="#">CSCvc66013</a> | Unable to change/ edit nested policy in Appnav cluster policies                                                                                                                                                                                                                           |
| <a href="#">CSCvc74609</a> | sn_unreachable between AppNav and Service Node causing network outage                                                                                                                                                                                                                     |
| <a href="#">CSCvc44940</a> | Unknown frame type from peer -- WAAS-RE-3-690412                                                                                                                                                                                                                                          |
| <a href="#">CSCvc83156</a> | Missing ability to determine reasons for AO keepalive failure                                                                                                                                                                                                                             |
| <a href="#">CSCvc99271</a> | Policy configuration fails programming into engine                                                                                                                                                                                                                                        |
| <a href="#">CSCvb48643</a> | Evaluation of waas for Openssl September 2016<br>CVE-2016-6304 CVE-2016-6305 CVE-2016-2183 CVE-2016-6303<br>CVE-2016-6302 CVE-2016-2182 CVE-2016-2180 CVE-2016-2177<br>CVE-2016-2178 CVE-2016-2179 CVE-2016-2181 CVE-2016-6306<br>CVE-2016-6307 CVE-2016-6308 CVE-2016-6309 CVE-2016-7052 |
| <a href="#">CSCvc23536</a> | Evaluation of waas for NTP November 2016<br>CVE-2016-9311 CVE-2016-9310 CVE-2016-7427 CVE-2016-7428<br>CVE-2016-9312 CVE-2016-7431 CVE-2016-7434 CVE-2016-7429<br>CVE-2016-7426 CVE-2016-7433                                                                                             |
| <a href="#">CSCva62833</a> | Disk encryption does not enable with AAA accounting enabled                                                                                                                                                                                                                               |
| <a href="#">CSCvc55023</a> | Scheduled reports do not get generated on the required date                                                                                                                                                                                                                               |
| <a href="#">CSCvd36676</a> | After fresh device Registration, Enabled features page is getting overridden                                                                                                                                                                                                              |
| <a href="#">CSCvd45107</a> | cms_cdm service will be restarted in WCM when primary int of WAE is removed in a scenario                                                                                                                                                                                                 |
| <a href="#">CSCvc58689</a> | Central manager fails to generate config for waas express routers                                                                                                                                                                                                                         |
| <a href="#">CSCvc57012</a> | WAAS CM API showing 0 for passthroughpeerin and passthroughpeerout                                                                                                                                                                                                                        |
| <a href="#">CSCvc51740</a> | packet-capture command does not work                                                                                                                                                                                                                                                      |
| <a href="#">CSCvc53678</a> | Waasnet service restart while running single sided HTTP/HTTPs traffic                                                                                                                                                                                                                     |
| <a href="#">CSCvc69416</a> | http accelerator dumps core file rarely                                                                                                                                                                                                                                                   |
| <a href="#">CSCvc76621</a> | core.httpmuxd while sharepoint prefetch                                                                                                                                                                                                                                                   |
| <a href="#">CSCvc07847</a> | Sharepoint prefetch is not working for word document with xml extension                                                                                                                                                                                                                   |
| <a href="#">CSCvc95534</a> | DRE cored during WAE shutdown                                                                                                                                                                                                                                                             |
| <a href="#">CSCvc97255</a> | Enable/Disable of AO based on dependency to be notified during upgrade                                                                                                                                                                                                                    |



| Caveat_ID_Number           | Headline                                                                       |
|----------------------------|--------------------------------------------------------------------------------|
| <a href="#">CSCvd03489</a> | rserverd64 Core file when clearing blacklist for domain not part of blacklist. |
| <a href="#">CSCvd26805</a> | Not able to enable SSH service from Device group                               |
| <a href="#">CSCvd39655</a> | sysmon process terminated unexpectedly                                         |

## Cisco WAAS Software Version 6.2.3c Open Caveats

The following caveats are open in Software Version 6.2.3c. Note that there might be additional open caveats from previous releases that are applicable to this release, unless they are specifically listed as resolved.

| Caveat_ID_Number           | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCUw60169</a> | http object-cache does not validate server IP address BB509                                        |
| <a href="#">CSCve29255</a> | Observed THSDL stuck connections while accessing http/https websites via squid proxy               |
| <a href="#">CSCve29588</a> | SMBAO Object cache Rename file descriptor leak observed during soak profile execution              |
| <a href="#">CSCve11987</a> | Object cache File descriptor leaks due to "current open file handles" are closed by smbao          |
| <a href="#">CSCve15397</a> | CM-AppNav polling sessions get stuck and result in AppNav remaining offline forever                |
| <a href="#">CSCvd65317</a> | File descriptors not getting released while executing "show stats conn" command                    |
| <a href="#">CSCuz29040</a> | SMBAO SOAK run resulting in OC_Open Pending counter remaining constant                             |
| <a href="#">CSCve28074</a> | SMB AO restarted with function "oc_server_ipc_read".                                               |
| <a href="#">CSCvd89141</a> | SMB AO restarted due to "oc_client_ipc_send_error_response_msg" function                           |
| <a href="#">CSCve20802</a> | Stuck connections observed due to sendsocket event                                                 |
| <a href="#">CSCvd73314</a> | Stuck Connections observed in Single sided NGSSL traffic via proxy                                 |
| <a href="#">CSCva80599</a> | NGSSL : Stucks are in HTTP when restarted HTTP AO on the flow-THs (-ve)                            |
| <a href="#">CSCvd48873</a> | Force device group appears due to config not sync for Securestore page while register fresh device |
| <a href="#">CSCvd61131</a> | ForceDeviceGroup appears when device automatically assign to DeviceGroup if DiskEncryption enabled |
| <a href="#">CSCvd97120</a> | Rescue doesn't work with 623c image.                                                               |
| <a href="#">CSCva52094</a> | SR-Server CORE observed reactivating ISR WAAS with Hostname change                                 |
| <a href="#">CSCvd46635</a> | Solution TB : Stuck connections on THs and Ts - 623c                                               |
| <a href="#">CSCvd81077</a> | Solution TB-httpcache service died multiple times                                                  |
| <a href="#">CSCvd69827</a> | Device got Hung while running ICA Traffic                                                          |
| <a href="#">CSCvd88250</a> | Processing time is more after configuring class-map having 800+ entries                            |
| <a href="#">CSCvd90139</a> | PMD memory leak occurs while configuring bulk class map policy                                     |
| <a href="#">CSCvd39397</a> | Major delays in DNS Query initiated by WAAS                                                        |

| Caveat_ID_Number           | Headline                                                 |
|----------------------------|----------------------------------------------------------|
| <a href="#">CSCvc83974</a> | Akamai process restarts unexpectedly, leaves a dump file |
| <a href="#">CSCvd35983</a> | wget for preposition should handle the space in URL      |

## Cisco WAAS Software Version 6.2.3b Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.2.3b.

| Caveat_ID_Number           | Headline                                                                                            |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvc27623</a> | Waaasnet service restart while running continuous soak test                                         |
| <a href="#">CSCvc33933</a> | SMB preposition not starting with host logging enabled                                              |
| <a href="#">CSCvc21161</a> | Waaasnet core while running singled sided HTTPs/HTTP traffic                                        |
| <a href="#">CSCvc26500</a> | “Identity not configured” alarm clears and raises several time.                                     |
| <a href="#">CSCvb81704</a> | Observed Waaasnet core”Wn_dft” file after upgrading from 5.x to 6.3.x                               |
| <a href="#">CSCuz15911</a> | SMB AO office files are failing to open after save via SMBv2                                        |
| <a href="#">CSCvc56666</a> | SMB File operation is getting failed due to OC “write queue” is getting stuck                       |
| <a href="#">CSCvc39906</a> | HTTPS connections are stuck on data center resulting in tfo overload                                |
| <a href="#">CSCvc41636</a> | SMB AO coredump due to inconsistency of read bytes state                                            |
| <a href="#">CSCvc43363</a> | Coredump created by SMB AO when trying to access data from packet content not present               |
| <a href="#">CSCvb69383</a> | snmpv3 not working on 6.2.1 Waaas in a specific scenario                                            |
| <a href="#">CSCvc50650</a> | Appnav Intercept:pkts received for the flows that are in FTM_WAAS_FLOW_STATE_HISTORICAL are dropped |
| <a href="#">CSCvc19814</a> | Wrong Counter getting updated in auto-discovery stats.                                              |

## Cisco WAAS Software Version 6.2.3b Open Caveats

The following caveats are open in Software Version 6.2.3b. Note that there might be additional open caveats from previous releases that are applicable to this release, unless they are specifically listed as resolved.

| Caveat_ID_Number           | Headline                                                           |
|----------------------------|--------------------------------------------------------------------|
| <a href="#">CSCvc24763</a> | WAAS version 5.5.7 noticed Core dump for smb.                      |
| <a href="#">CSCvc57012</a> | WAAS CM API showing 0 for passthroughpeerin and passthroughpeerout |
| <a href="#">CSCvc55023</a> | Scheduled reports do not get generated on the required date        |
| <a href="#">CSCvc58689</a> | Central manager fails to generate config for waaas express routers |
| <a href="#">CSCva33283</a> | connection reset for SMB2 connections while doing file upload      |
| <a href="#">CSCva62833</a> | Disk encryption does not enable with AAA accounting enabled        |
| <a href="#">CSCvb56318</a> | WAAS Corrupted chard after modifying available report.             |

| Caveat_ID_Number            | Headline                                                                   |
|-----------------------------|----------------------------------------------------------------------------|
| <a href="#">CSCvb69139</a>  | regular database maintenance not performed in all device-modes             |
| <a href="#">CSCvb78641</a>  | TACACS authentication failing after upgrade                                |
| <a href="#">CSCvc53678</a>  | Waasnet service restart while running single sided HTTP/HTTPs traffic      |
| <a href="#">CSCvc67819</a>  | Unexpected reload of smb accelerator process during long soak test.        |
| <a href="#">CSCvc21298</a>  | Memory leak seen during the DBO SOAK profile execution                     |
| <a href="#">CSCvc59481</a>  | OC server core while running smbv3sign & smbv3 encryption large file cases |
| <a href="#">CSCCuy17271</a> | oc core malloc_printerr while running SMB Regression                       |

## Cisco WAAS Software Version 6.2.3a Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.2.3a.

| Caveat_ID_Number           | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCvb30731</a> | Waasnet service terminates and generates a core file                                               |
| <a href="#">CSCva59805</a> | Device going to offline in a scenario                                                              |
| <a href="#">CSCva96691</a> | SMBAO Core when Authentication fails and Server downgrade the Authentication from Kerberos to NTLM |
| <a href="#">CSCvb42434</a> | SMB AO coredump created in a specific situation                                                    |
| <a href="#">CSCvb49052</a> | DRE disk_full "Cache disk is full" alarm on WAVE-694 after upgrade to WAAS 6.2.3                   |
| <a href="#">CSCvb52967</a> | WAAS - AppNav communication issue with ServiceNodes                                                |
| <a href="#">CSCvb55927</a> | SMB timeout alarm is raised and the accelerator remains in timeout state forever                   |
| <a href="#">CSCvb45413</a> | HTTPS (443) connections stuck on core long after closed on edge                                    |
| <a href="#">CSCvb10628</a> | ISR-WAAS can ignore updates of name- or ntp-server from IOS                                        |
| <a href="#">CSCvb25141</a> | Local Device config is getting pushed every PCM config from CM                                     |
| <a href="#">CSCva26420</a> | WAAS Edge is dropping packets when it gets multi-packet 407 response                               |
| <a href="#">CSCuh86284</a> | Issue with daily consolidation hour system property                                                |
| <a href="#">CSCvb17887</a> | WAAS CM will show changes in data on the HTTP bandwidth savings chart                              |
| <a href="#">CSCvb25734</a> | Mon API TrafficStats.retrieveCPUUtilization fails to retrieve stats                                |
| <a href="#">CSCvb41805</a> | SMBAO process cores due to internal mismatch in URL names                                          |
| <a href="#">CSCvb40281</a> | Outlook pst files are not bypassed by WAAS                                                         |
| <a href="#">CSCva95254</a> | WAAS CM removing crypto certificates on WAAS Express routers                                       |
| <a href="#">CSCva84398</a> | Alarm raised about user space core file created of process pidof                                   |
| <a href="#">CSCvb59314</a> | Connections to particular websites may fail through WAAS in a specific situation                   |
| <a href="#">CSCvb44718</a> | Unable to use underscore in trap host community via GUI                                            |
| <a href="#">CSCvb40213</a> | Sorting of device groups is not possible                                                           |

| Caveat_ID_Number           | Headline                                                                                   |
|----------------------------|--------------------------------------------------------------------------------------------|
| <a href="#">CSCvb55730</a> | Connections fail hitting the expected class-map and policy                                 |
| <a href="#">CSCvb57872</a> | WAAS device goes Offline in CM GUI                                                         |
| <a href="#">CSCvb38240</a> | SNMP configuration from DG is not reflecting in device                                     |
| <a href="#">CSCvb70443</a> | Core WAAS with ASVC causes extra rDNS queries for proxy CONNECT SSL requests               |
| <a href="#">CSCvb57207</a> | Unable to install Akamai License                                                           |
| <a href="#">CSCvb63549</a> | smbao core with smb2LeaseAckCleanup Function                                               |
| <a href="#">CSCvb81006</a> | SMBAO terminates in bufferCreateView                                                       |
| <a href="#">CSCvb76604</a> | Optimized traffic on port 23 fills disk with debug output                                  |
| <a href="#">CSCvb53474</a> | SNMP: No space left on device while querying iso mib during stress                         |
| <a href="#">CSCvb58833</a> | sn_sia_invl_d_pkt alarm seen on ANC with traffic                                           |
| <a href="#">CSCva92135</a> | waasnet process restarted with single sided TLS 1.2 connections running ECDHE cipher       |
| <a href="#">CSCvb81995</a> | HTTP: Traffic server stopped working during tar/zip/Microsoft update                       |
| <a href="#">CSCvb58618</a> | HTTP: Traffic server stopped working while downloading Windows update                      |
| <a href="#">CSCva77075</a> | HTTP: Traffic server stopped working while handling TSContMutexGet                         |
| <a href="#">CSCva92728</a> | Unexpected reload while running SSL traffic on Nextgen SSL                                 |
| <a href="#">CSCvb97356</a> | Directory browsing optimization causes deadlock when we hit the max nodes SMB AO can cache |
| <a href="#">CSCvb92954</a> | SMB preposition config does not get pushed out to ISR-WAAS                                 |
| <a href="#">CSCuz55920</a> | Empty server response found in Web-Pages in a specific scenario                            |
| <a href="#">CSCvb43838</a> | snmp-server mib persist event cli is failing while configuring                             |
| <a href="#">CSCvb86397</a> | Modification of SNMP host is not happening from CLI                                        |
| <a href="#">CSCvb86429</a> | Modification of SNMP Trigger is not happening from CLI.                                    |
| <a href="#">CSCvc04836</a> | Looped Packets from SN to SC going out with Invalid IP Checksum                            |
| <a href="#">CSCvb58171</a> | SMB AO restarts with coredump in particular scenario                                       |

## Cisco WAAS Software Version 6.2.3a Open Caveats

The following caveats are open in Software Version 6.2.3a. Note that there might be additional open caveats from previous releases that are applicable to this release, unless they are specifically listed as resolved.

| Caveat_ID_Number           | Headline                                                                        |
|----------------------------|---------------------------------------------------------------------------------|
| <a href="#">CSCva52094</a> | SR-Server CORE observed reactivating ISR WAAS with Hostname change              |
| <a href="#">CSCva00161</a> | TFO:capped on speed: low latency between WAAS and server in Cloud               |
| <a href="#">CSCvb95306</a> | After upgrade from 5.5.3 to 6.3.0 able to see FDG in SNMP general settings page |
| <a href="#">CSCvb88945</a> | External SN blocks traffic when jumbo MTU is enabled                            |

| Caveat_ID_Number           | Headline                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCva54052</a> | NTP server configuration push is failed for KVM-vWAAS from CM GUI                                  |
| <a href="#">CSCva80599</a> | NGSSL: Stucks are in HTTP when restarted HTTP AO on the flow-THs (-ve)                             |
| <a href="#">CSCvc29774</a> | Few stuck connections seen rarely on BR WAE after long duration of browsing internet               |
| <a href="#">CSCvc21161</a> | Waasnet core while running single sided HTTPs/HTTP traffic                                         |
| <a href="#">CSCvc27623</a> | Waasnet service restart while running continuous soak test                                         |
| <a href="#">CSCvc27941</a> | "SSL accelerator overloaded " alarm raised on vWAAS-50k during SOAK test                           |
| <a href="#">CSCvc26500</a> | "Identity not configured" alarm clears and raises several time.                                    |
| <a href="#">CSCvc26475</a> | Crash at SO_DRE while running SSL traffic in NGSSL dual-sided topo - TsDL                          |
| <a href="#">CSCvb81704</a> | Observed waasnet core"Wn_dft" file after upgrading from 5.x to 6.3.x                               |
| <a href="#">CSCvb83252</a> | SSL AO's operational status doesn't come up after "Restore factory-default preserve basic-config " |
| <a href="#">CSCvc12079</a> | Unable to create snmp trigger in 5.x from device level when cm is in 6.3.x                         |

## Cisco WAAS Software Version 6.2.3 Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.2.3.

| Caveat_ID_Number            | Headline                                                                 |
|-----------------------------|--------------------------------------------------------------------------|
| <a href="#">CSCva30228</a>  | WAAS cons are retransmitting packets very quickly and are getting reset. |
| <a href="#">CSCCuy06186</a> | Lan devices are not accessible after shutting port-channel mem interface |
| <a href="#">CSCCuy06942</a> | ISR-WAAS: SMB accelerator gets disabled upon ISR router upgrade/reload   |
| <a href="#">CSCCuz10327</a> | File transfer failed in a specific scenario in Azure vWAAS               |
| <a href="#">CSCCuz22537</a> | SMB Preposition tasks with multiple domains fail when run in parallel    |
| <a href="#">CSCva18411</a>  | cms server logfiles not cleaned up                                       |
| <a href="#">CSCCuz34038</a> | ISR-WAAS goes offline after long duration traffic                        |
| <a href="#">CSCCuz41637</a> | Rarely policy engine doesn't push connection to HTTP AO during upgrade   |
| <a href="#">CSCCuz47571</a> | Akamai:Object-Cache top-hosts counters are not getting incremented       |
| <a href="#">CSCCuz49231</a> | ssh login to Azure vWAAS not working                                     |
| <a href="#">CSCCut83135</a> | core.dispatcher.x.x.x created while configuring machine account identity |
| <a href="#">CSCCux30779</a> | SMB Preposition task status shows completed if connection not optimized  |
| <a href="#">CSCCux76467</a> | Outlook not connect to exchange with Wan secure interoperable mode       |
| <a href="#">CSCCuy46644</a> | Interception access-list not working                                     |
| <a href="#">CSCCuy55846</a> | WAAS 6.1.1a SMB AO restart generating core file                          |
| <a href="#">CSCCuy59549</a> | WAAS 6.1.1a SMB AO core file on DC device                                |
| <a href="#">CSCCuy73435</a> | SMB preposition task may get fail when running more than 15 in parallel  |
| <a href="#">CSCCuz11211</a> | AO Timeouts seen during longevity test                                   |

| Caveat_ID_Number           | Headline                                                                  |
|----------------------------|---------------------------------------------------------------------------|
| <a href="#">CSCuz12323</a> | Force device group not pushing enable feature config in specific scenario |
| <a href="#">CSCuz18876</a> | snmp core file observed in SM-SRE devices while query Host Resources MIB  |
| <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="#">CSCuz55707</a> | All devices cannot use CM as proxy for http object cache                  |
| <a href="#">CSCuz59552</a> | Akamai: Preposition logging missing, PP-IMS sometimes doesn't happen.     |
| <a href="#">CSCva02503</a> | serial-to-IP converter packets dropped by WAAS 6.1 with inline            |
| <a href="#">CSCva14731</a> | Unable to login with Radius user configured in Cisco ACS 5.x              |
| <a href="#">CSCva39357</a> | CM-WAE connectivity impacted in inline interception                       |
| <a href="#">CSCuc52663</a> | System property edit page shown after submit                              |
| <a href="#">CSCuu71549</a> | Central manager not responsive due to no space on /state                  |
| <a href="#">CSCux74907</a> | Network unreachable warning message in cms_httpd server log               |
| <a href="#">CSCuz47444</a> | WAAS 6.1.1a show statistic tfo detail output is showing incorrect value   |
| <a href="#">CSCup30376</a> | Error messages are seen for /dev/ceflash during SRE image upgrade         |
| <a href="#">CSCus80217</a> | Apache HTTP Server upgrade in WAAS                                        |
| <a href="#">CSCux25652</a> | Need dedicated thread in PMD to handle Keep alive request from AO         |
| <a href="#">CSCuy46947</a> | Move to stronger crypto certificates                                      |
| <a href="#">CSCva00437</a> | Move to stronger crypto certificates                                      |

## Cisco WAAS Software Version 6.2.3 Open Caveats

The following caveats are open in Software Version 6.2.3.

| Caveat_ID_Number           | Headline                                                                 |
|----------------------------|--------------------------------------------------------------------------|
| <a href="#">CSCuw17054</a> | MAPI AO gets disabled and MAPI Core observed for RPC-HTTPS with Kerberos |
| <a href="#">CSCuy82470</a> | New connection established while sending mail with attachments           |
| <a href="#">CSCuz34303</a> | Processor P0 CATERR error in BMC event log                               |
| <a href="#">CSCuz94568</a> | WAAS appliance not responding to SNMP                                    |
| <a href="#">CSCva26420</a> | WAAS Edge is dropping packets when it gets multi-packet 407 response     |
| <a href="#">CSCva40790</a> | Central manager reporting insufficient data from WAAS Express routers    |
| <a href="#">CSCuy30007</a> | SMB Preposition does not support Extended Unicode Characters             |
| <a href="#">CSCuz15000</a> | vWAAS-Azure pending Development from Microsoft                           |
| <a href="#">CSCuz61982</a> | SMBAO preposition is not working with NetApp filer with SMBv2 Signing    |
| <a href="#">CSCva56509</a> | High CPU on WAAS for process httpcache-akamai traffic_server             |

| Caveat_ID_Number           | Headline                                                         |
|----------------------------|------------------------------------------------------------------|
| <a href="#">CSCva59451</a> | WCM reporting inconsistencies when different timezone configured |
| <a href="#">CSCvb30731</a> | WAASnet service terminates and generates a core file             |

## Cisco WAAS Software Version 6.2.3 Command Changes

This section lists the new and modified commands in Cisco WAAS Software Version 6.2.3.

[Table 9](#) lists the commands and options that have been added or changed in Cisco WAAS Software Version 6.2.3.

**Table 9** CLI Commands Added or Modified in Version 6.2.3

| Mode                 | Command                                    | Description                                                                                                                                                |
|----------------------|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Global configuration | <b>crypto encryption-service enable</b>    | Enables and configures encryption services on a WAAS device.                                                                                               |
| EXEC                 | <b>show accelerator</b>                    | New <b>interposer-ssl</b> parameter added, which displays the status for the SSL Interposer accelerator.                                                   |
|                      | <b>show statistics encryption-services</b> | Displays encryption-services general statistics for a WAE, including SSL Interposer statistics and Security Assistant Key Escrow (SAKE) server statistics. |

## Using Previous Client Code

If you have upgraded to Cisco WAAS Version 6.2.3x 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 `ADBeanTemplate.xml` 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.