Release Note for Cisco Wide Area Application Services Software Version 6.4.3x

June 18, 2021

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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

Contents

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

- 6.4.3f
- 6.4.3e
- 6.4.3d
- 6.4.3c
- 6.4.3b
- 6.4.3a
- 6.4.3

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.

This Release Note contains the following sections:

Cisco Software Version 6.4.3x New and Changed Features

This section has the following topics:

Cisco Software Version 6.4.3f New and Changed Features

No new features were added in this release. A few commands have been modified that are documented in Table 10Cisco WAAS CLI Commands Added or Modified in Cisco WAAS Version 6.4.3f, page 47 and the resolved caveats are listed in the Cisco Software Version 6.4.3f Resolved Caveats, page 49, below.

Cisco Software Version 6.4.3e New and Changed Features

- **SNMPv3 with Advanced Encryption Standard (AES) encryption**: For Cisco WAAS Version 6.4.3e and later, AES encryption provides strong encryption capability for SNMPv3 messages. AES encryption for Cisco WAAS uses the Cipher Feedback (CFB) mode with encryption key sizes of 128, 192, or 256 bits.
- **Strong software password enforcement**: For Cisco WAAS Version 6.4.3e and later, users must change the default password for the **admin** user after initial login. This applies to the following:

  - default administrator account for Cisco WAAS Central Manager and Cisco WAAS CLI on Cisco WAAS devices.
  - default NFVIS administrator account for Cisco Enterprise Network Compute System 5400-W Series (Cisco ENCS 5400-W Series) appliances.
  - default NFVIS administrator account for Cisco Cloud Services Platform 5000-W Series (Cisco CSP 5000-W Series) appliances.
- **Shared LAN on Motherboard (LOM) support**: The shared LOM feature helps to re-use existing on-board Ethernet LAN interfaces on Cisco ENCS 5400-W series appliances by providing IP connectivity to Cisco Integrated Management Controller (CIMC) for remote management and health monitoring though SNMP and Syslog, while the same interfaces configured for traffic optimization.
  - Shared LOM works with the **Standby interface** in Cisco WAAS, but does not work with the P**ort-channel interface** in Cisco WAAS.
  - Shared LOM support is available for vWAAS on the ENCS 5400-W series. For more information, see the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series" in the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.
- **Apache HTTP Server upgrade**: For Cisco WAAS Version 6.4.3e and later, Cisco WAAS uses Apache HTTP Server Apache 2.4.41

Cisco Software Version 6.4.3d New and Changed Features

- **Support for Windows Hypervisor 2016**: Cisco vWAAS in Cisco WAAS Version 6.4.3d and later supports Windows Hypervisor 2016 Standalone deployments.
- **Support for RHEL/ CentOS Linux KVM Hypervisor**: Cisco vWAAS in Cisco WAAS Version 6.4.3d and later supports:
  - RHEL Server 7.5 and RHEL Server 7.6
  - CentOS Linux 7.5.1804 (Core) and CentOS Linux 7.6.1810 (Core)

Cisco Software Version 6.4.3c New and Changed Features

- **Support for VMware ESXi 6.7**: Cisco vWAAS in Cisco WAAS Version 6.4.3c and later supports VMware ESXi 6.0, VMware ESXi 6.5 and VMware ESXi 6.7 (only via web client using vCenter).

Cisco Software Version 6.4.3b New and Changed Features

- **Support for VMware ESXi 6.5**: Cisco vWAAS in Cisco WAAS 6.4.3b and later supports VMware ESXi 6.5.
- **Support for VMware vCenter Server**: Cisco vWAAS in Cisco WAAS 6.4.3b supports Web Client of VMware vCenter Server 6.0 version.
- **App ID Support**: Application based classification is now supported on Cisco WAAS Version 6.4.3b. This classification can be integrated with existing pre-defined AppNav class-maps and matched with the NBAR protocol for further application optimization. You can also use Nested class-maps to match conditions for the Applications.

- **SMBv311 Encryption**: This release supports Layer 7 optimization for encrypted SMBv311 connections. This optimization is by default and no extra configuration is required for existing SMB configurations.

For a list of CLI commands added or changed for Cisco WAAS Version 6.4.3b, see Cisco Software Version 6.4.3x Command Changes, page 46.

Cisco Software Version 6.4.3a New and Changed Features

- **Cisco Cloud Services Platform for WAAS (Cisco CSP 5000-W)**: An open x86 hardware platform for deployment of Cisco datacenter network functions virtualization (VNFs). The Cisco CSP 5000-W Series contains an embedded Linux KVM hypervisor, and enables you to monitor and manage the life cycle of vWAAS on NFVIS.

  There are three CSP 5000-W models:

  – CSP 5228-W (12,000 connections): for vWAAS-12000

  – CSP 5228-W (50,000 connections): for vWAAS-50000

  – CSP 5436-W (150,000 connections): for vWAAS-150000

- Cisco WAAS Central Manager and CLI support to configure pass-through connections that are not optimized by NGSSL accelerators.
- **Alarm features**:
  – Alarm details are displayed in the WAAS Central Manager device dashboard page.
  – Alarm sorting is available based on the alarm time raised in the Alerts page.

Cisco Software Version 6.4.3 New and Changed Features

This section contains the following topics:

Cisco WAAS 6.4.3 New and Changed Features

Cisco WAAS Software Version 6.4.3 includes the following WAAS new and changed features:

- **SMART-SSL support** is enhanced to include the following:
  – Ability to configure DSCP Remarking of LAN and WAN values.
  – Ability to configure multiple accelerated services to use any server for SSL acceleration.
  – New SaaS optimization and reporting- Support for acceleration of ServiceNow and Salesforce.
- **Smart Licensing**: Support for devices to automate manual licensing tasks by simplifying the core functions of purchasing, managing and reporting of licenses.
- **SMB 311 Pre-authentication Integrity Support**: Pre-authentication is one of the new SMB 3.1.1 security improvements in Windows 10 and Windows Server 2016. It protects against any tampering with SMB2's connection establishment and authentication messages by leveraging cryptographic security functions.

- **SMB DFS Preposition**: DFS Distributed file system (DFS) consists of software residing on network servers and clients that transparently links shared folders located on different file servers into a single namespace for improved load sharing and data availability. DFS preposition allows you to fetch configured DFS shares in a specific time, cache it and use later whenever required.
- **Admission control**: SMB acceleration has been enhanced with admission control properties for managing memory issues on the device. These enhancements monitor/control the over-utilization of RAM by SMB optimizers.
- **SMB Acceleration Performance Improvement**: Ensures that you can configure the minimum file size to bypass for SMB optimization.
- **DC Level 7 Support**: WAAS supports optimization of traffic to/from Domain Controllers with domain/forest level 7 (DC 7) like Windows Server 2016.
- **MAPI over HTTP**: MAPI accelerator now provides improved support for Outlook and Exchange connections by optimizing MAPI over HTTP traffic.
- **ITD support for WAAS**: for traffic distribution, load balancing, and redirection.
- **Catena support for WAAS**: provides selective traffic chaining using security policies for traffic redirection in a routed mode.

For a list of CLI commands added or modified changed for WAAS Version 6.4.3, see Cisco Software Version 6.4.3x Command Changes, page 46.

Cisco vWAAS in Cisco WAAS Version 6.4.3 New and Changed Features

Cisco vWAAS in Cisco WAAS Version 6.4.3 includes the following vWAAS new and changed features:

- SR-IOV: Cisco vWAAS with SR-IOV is supported on RHEL KVM, KVM on CentOS, and VMware ESXi for the following vWAAS and vCM models:
  - vWAAS-150
  - vWAAS-200
  - vWAAS-750
  - vWAAS-1300
  - vWAAS-2500
  - vWAAS-6000
  - vWAAS-12000
  - vWAAS-50000
  - vCM-100
  - vCM-500
  - vCM-1000
  - vCM-2000

  Cisco vWAAS with SR-IOV on VMware ESXi is supported for vWAAS 150000.

  This expands SR-IOV support for vWAAS: vWAAS for WAAS 6.4.1 supports vWAAS with SR-IOV on RHEL KVM for the following models only:
  - vWAAS-150
  - vWAAS-200
  - vWAAS-750

  - vWAAS-1300
  - vWAAS-2500
  - vWAAS-6000
  - vCM-100
  - vCM-500
  - vCM-1000
  - vCM-2000
- Fail-To-Wire (FTW): FTW is supported for Cisco vWAAS on Cisco ENCS 5400-W, with features that include traffic interception (inline and WCCP) and failure handling.

Cisco Software Version 6.4.3x Filenames

This section describes the Cisco WAAS Software Version 6.4.3x software image files for use on Cisco WAAS appliances and modules and contains the following topics:

Cisco WAAS Standard Image Files

Cisco WAAS Software Version 6.4.3x includes the following standard primary software image files for use on Cisco WAAS appliances and modules:

- **Cisco_NFVIS_4.1.2-FCx_WAAS-APPLIANCE-6.4.3x-bx.iso**: Unified Cisco WAAS image package for ENCS 5400-W Series appliances and for CSP 5000-W Series appliances.
- **waas-universal-6.4.3x.*x*-k9.bin**: Universal software image that includes Cisco WAAS 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-6.4.3x.*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-6.4.3x.x-k9.iso**: Cisco WAAS software recovery CD image.
- **waas-x86_64-6.4.3x.x-k9.sysimg**: Flash memory recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- **waas-6.4.3x.*x*-k9.sysimg**: Flash memory recovery image for 32-bit platforms (all other devices).
- **waas-kdump-6.4.3x.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-6.4.3x.x.zip**: Contains the alarm and error message documentation.

No Payload Encryption Image Files

Cisco WAAS Software Version 6.4.3x 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:

- **Cisco_NFVIS_4.1.2-FCx_WAASNPE-APPLIANCE-6.4.3x-bx.iso**: Unified Cisco WAAS image package for ENCS 5400-W Series appliances and for CSP 5000-W Series appliances.
- **waas-universal-6.4.3x.*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-6.4.3x.*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.

The following additional files are also included:

- **waas-rescue-cdrom-6.4.3x.*x*-npe-k9.iso**: Cisco WAAS NPE software recovery CD image.
- **waas-x86_64-6.4.3x.*x*-npe-k9.sysimg**: Flash memory NPE recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- **waas-6.4.3x.*x*-npe-k9.sysimg**: Flash memory NPE recovery image for 32-bit platforms (all other devices).

Cisco vWAAS Image Files

This section contains the following topic:

- Platforms Supported by Cisco WAAS, page 12

Hypervisor-wise Unified OVA Package Format for Cisco vWAAS in Cisco WAAS Version 6.4.3x

Each unified OVA package file provides an option to choose a Cisco vWAAS or Cisco vCM model and other required parameters to launch Cisco vWAAS or Cisco vCM in Cisco WAAS in the required configuration.

Table 1 shows the unified OVA filename formats supported for hypervisors, appliances, Cisco vWAAS models, and Cisco vCM models.

Note On VMware ESXi, the OVA deployment for Cisco WAAS Version 6.4.1 and later must be done only through VMware vCenter. For more information on deployment, see *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

For a listing of current hypervisor-wise NPE and non-NPE OVA files for Cisco vWAAS or Cisco vCM, see the Cisco Wide Area Application Services (WAAS) Download Software Page and select the WAAS software version for your Cisco vWAAS instance.

Table 1 Cisco Unified OVA Filename Format Supported for Hypervisors, Appliances, vWAAS and vCM Models

Hypervisor or Appliance	Sample Cisco Unified OVA Filename Format	Supported Cisco vWAAS Models	Supported Cisco vCM Models
VMware ESXi	• Cisco-WAAS-Unified-6.4.3f-b-46.ova • Cisco-WAAS-Unified-6.4.3f-npe-b-46.ova	• vWAAS-150 • vWAAS-200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000 • vWAAS-6000R • vWAAS-12000 • vWAAS-50000 • vWAAS-150000	• vCM-100 • vCM-500 • vCM-1000 • vCM-2000
Microsoft Hyper-V	• Cisco-HyperV-vWAAS-unified-6.4.3f-b-46.zip • Cisco-HyperV-vWAAS-unified-6.4.3f-b-46-npe.zip	• vWAAS-150 • vWAAS- 200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000 • vWAAS-6000R • vWAAS-12000 • vWAAS-50000	• vCM-100 • vCM-500 • vCM-1000 • vCM-2000
KVM CentOS	• Cisco-KVM-vWAAS-Unified-6.4.3f-b-46.tar.gz • Cisco-KVM-vWAAS-Unified-6.4.3f-b-46-npe.tar.gz	• vWAAS-150 • vWAAS- 200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000 • vWAAS-6000R • vWAAS-12000 • vWAAS-50000	• vCM-100 • vCM-500 • vCM-1000 • vCM-2000

Hypervisor or Appliance	Sample Cisco Unified OVA Filename Format	Supported Cisco vWAAS Models	Supported Cisco vCM Models
Cisco NFVIS vBranch	• Cisco-KVM-vWAAS-Unified-6.4.3f-b-46.tar.gz • Cisco-KVM-vWAAS-Unified-6.4.3f-b-46-npe.tar.gz	• vWAAS-150 • vWAAS-200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000 • vWAAS-6000R	• N/A
Cisco ISR-WAAS	• ISR-WAAS-6.4.3f-b-46.ova • ISR-WAAS-6.4.3f-b-46-npe.ova	• vWAAS-200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500	• N/A
Cisco ENCS 5400-W	• Cisco_NFVIS_4.1.2-FC2_WAAS-APPLIANCE-6.4.3f-b-46.iso • Cisco_NFVIS_4.1.2-FC2_WAASNPE-APPLIANCE-6.4.3f-b-46.iso	• vWAAS-200 • vWAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000R	• N/A
Cisco CSP 5000-W	• Cisco_NFVIS_4.1.2-FC2_WAAS-APPLIANCE-6.4.3f-b-46.iso • Cisco_NFVIS_4.1.2-FC2_WAASNPE-APPLIANCE-6.4.3f-b-46.iso	• vWAAS-12000 • vWAAS-50000 • vWAAS-150000	• N/A

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

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.

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

If you install a Cisco AppNav Controller Interface Module in a device that requires a BIOS update, the bios_support_seiom major alarm is raised, "I/O module may not get the best I/O performance with the installed version of the system BIOS firmware."

To determine if a device has the correct BIOS version, use the **show hardware** command. The last three characters of the Version value, for example, "20a," show the BIOS version installed on the device.

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

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

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

Use the appropriate BIOS installer file for your appliance model.

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

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

BMC Firmware Update

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

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

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

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

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

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

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

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

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

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

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

RAID Controller Firmware Update

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

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

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

Interoperability and Support

This section contains the following topics:

Hardware, Client, and Web Browser Support

This section contains the following topics:

Platforms Supported by Cisco WAAS

The Cisco WAAS software operates on these hardware platforms:

- ENCS-W-5406, ENCS-W-5408, ENCS-W-5412
- CSP-W-5228, CSP-W-5436
- WAVE-294, 594, 694, 7541, 7571, 8541
- ISR-WAAS-200, 750, 1300, 2500
- ISR-44xx Series Routers

Hypervisors Supported by Cisco vWAAS

Table 2 shows the operating systems and supported hypervisors, hardware platforms, and Cisco vCM and vWAAS models.

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

Table 2 Operating Systems and Supported Hypervisors, Platforms, vCM and vWAAS Models

Operating System	Hypervisor	Recommended Cisco Hardware	Supported Versions for Cisco vWAAS 6.4.3x	Cisco vWAAS and Cisco vCM Models Supported
VMware	ESXi 6.0	UCS-C or UCS-E Series	ESXi 6.0 (U3h) (Build 9313334) vCenter 6.0.0 (Build 9154154)	vWAAS-150 vWAAS- 200 vWAAS-750 vWAAS-1300 vWAAS-2500 vWAAS-6000 vWAAS-12000 vWAAS-50000 vWAAS-150000 vCM-100 vCM-500 vCM-1000 vCM-2000
	ESXi 6.5	UCS-C or UCS-E Series	ESXi 6.5 (U2) (Build 8294253) vCenter Version 6.5.0.20000 (Build 8307201)	
	ESXi 6.7	UCS-C or UCS-E Series	ESXi 6.7 (U1) (Build 10302608) vCenter Version 6.7.0.30000 (Build 13007145)	
Microsoft Windows	SCVMM	UCS-C or UCS-E Series	Windows Server 2012R2 Standard - Microsoft System Center 2012 R2 - Version 3.2.7510.0	vWAAS-150 vWAAS-200 vWAAS-750 vWAAS-1300 vWAAS-2500 vWAAS-6000 vWAAS-12000 vWAAS-50000 vCM-100 vCM-500 vCM-1000 vCM-2000
	Hyper-V	UCS-C or UCS-E Series	Windows Server 2012R2 Standard - Version 6.3 (Build 9600)	
	Hyper-V	UCS-C or UCS-E Series	Windows Server 2016 Standard - Version 1607 (Build 14393.0)	

Operating System	Hypervisor	Recommended Cisco Hardware	Supported Versions for Cisco vWAAS 6.4.3x	Cisco vWAAS and Cisco vCM Models Supported
RHEL Linux	KVM	UCS-C or UCS-E Series	Red Hat Enterprise Linux (RHEL) Server 7.1 RHEL Server 7.5 RHEL Server 7.6	vWAAS-150 vWAAS-200 vWAAS-750 vWAAS-1300 vWAAS-2500 vWAAS-6000 vWAAS-12000 vWAAS-50000 vCM-100 vCM-500 vCM-1000 vCM-2000
CentOS Linux	KVM	UCS-C or UCS-E Series	CentOS Linux 7.2.1511 (Core) CentOS Linux 7.5.1804 (Core) CentOS Linux 7.6.1810 (Core)	
SUSE Linux	KVM	UCS-C or UCS-E Series	SUSE Linux Enterprise Server-12-SP3	
NFVIS	---	ENCS 5400-W Series	NFVIS 3.7.1 and later	vWAAS 200, 750, 1300, 2500, 6000-R
ISR-WAAS	---	ISR-44xx Series	IOS-XE 16.x and later	vWAAS 200, 750, 1300, 2500,
Azure (Standard/ Premium)	Hyper-V	Microsoft Azure Cloud	---	vWAAS models that are supported on Microsoft Hyper-V: vWAAS-200, 750, 1300, 2500, 6000, 12000
OpenStack (CentOS)	KVM	UCS-C Series	---	vWAAS models that are supported on KVM on CentOS: vWAAS-150 vWAAS- 200 vWAAS-750 vWAAS-1300 vWAAS-2500 vWAAS-6000 vWAAS-12000 vWAAS-50000

For more information, see *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

Browsers Supported by Cisco 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 Cisco WAAS, we recommend using FireFox as your browser.

- 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, and 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 6.4.3x devices with devices running earlier software versions:

- **Cisco WAAS Central Manager interoperability**:

  In a mixed version Cisco WAAS network, the Cisco WAAS Central Manager must be running the latest version of the Cisco WAAS software (6.4.3x), and associated Cisco WAAS devices must be running Cisco WAAS Version 5.1.x- 5.5.7xor later.

- **Cisco WAAS system interoperability**:

  Cisco WAAS Version 6.4.3x 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 Cisco WAAS version 5.5.3 to 6.4.3 is not supported.

Cisco WAAS and Cisco vWAAS Interoperability

This section contains the following topics:

Cisco ISR-WAAS Models and Supported Cisco ISR Platforms

Table 3 ISR-WAAS Models: CPUs, Memory, Disk Storage and Supported ISR Platforms

Cisco ISR-WAAS Model	CPUs	Memory	Disk Storage	Cisco ISR Platform Supported	Cisco WAAS Version Supported
ISR-WAAS-200	1	3 GB	151 GB	ISR-4321	6.2.3 and later
ISR-WAAS-200	1	4 GB	151 GB	ISR-4321	6.2.3 and later
ISR-WAAS-750	2	4 GB	151 GB	ISR-4351, ISR-4331, ISR-4431, ISR-4451	6.2.3 and later
ISR-WAAS-750	2	4 GB	151 GB	ISR-4461	6.2.3 and later
ISR-WAAS-1300	4	6 GB	151 GB	ISR-4431, ISR-4451	6.2.3 and later
ISR-WAAS-1300	4	6 GB	151 GB	ISR-4461	6.4.1b and later
ISR-WAAS-2500	6	8 GB	338 GB	ISR-4451	6.2.3 and later
ISR-WAAS-2500	6	8 GB	338 GB	ISR-4461	6.4.1b and later

Operating guidelines for Cisco ISR-WAAS:

- 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.
  - For ISR-WAAS-200 in ISR-4321 with IOS-XE 16.x, 4 GB of memory is mandatory.
  - For ISR-WAAS-200 in ISR-4321 with IOX-XE 3.x, 3 GB of memory is recommended; 4 GB of memory is optional.

Cisco vWAAS Resizing in Cisco WAAS Version 6.4.1 and Later

Cisco vWAAS in Cisco WAAS Version 6.4.1x and later requires additional resources, so we highly recommend that you resize CPU and memory resources, as shown in Table 4. Resizing Cisco vWAAS on the recommended platforms enables Cisco vWAAS to scale to optimized TCP connections for the associated device, and to optimize CPU and RAM utilization.

Caution Resizing CPU and memory resources is highly recommended, although optional, for Cisco vWAAS models on all hypervisors. For Cisco vWAAS in Cisco WAAS Version 6.4.1b and later, options are provided during Cisco vWAAS deployment for you to choose either original or resized resources.

Note Cisco ISR-WAAS and Cisco vCM are not resized for Cisco vWAAS in Cisco WAAS Version 6.4.1a and later.

Note For optimum performance, we recommend you use the SSD disk with the Cisco UCS models listed in Table 4.

Table 4 Resized vWAAS CPU and Memory Specifications for WAAS Version 6.4.1a and Later

Cisco vWAAS Model	Old CPU	Resized CPU	Tested CPU Clock Speed	Old Memory	Resized Memory	Disk Storage	Minimum Recommended Cisco Platform
vWAAS-150	1 CPU	2 CPUs	1.7 GHz	3 GB	4 GB	160 GB	UCS-E140N-M2
vWAAS-200	1 CPU	2 CPUs	1.8 GHz	3 GB	4 GB	260 GB	UCS-E140S-M2
vWAAS-750	2 CPUs	4 CPUs	1.8 GHz	4 GB	8 GB	500 GB	UCS-E140S-M2
vWAAS-1300	2 CPUs	4 CPUs	1.9 GHz	6 GB	12 GB	600 GB	UCS-E160S-M3
vWAAS-2500	4 CPUs	6 CPUs	1.9 GHz	8 GB	16 GB	750 GB	UCS-E160S-M3
vWAAS-6000	4 CPUs	8 CPUs	2.0 GHz	11 GB	24 GB	900 GB	UCS-E180D-M3
vWAAS-6000R	4 CPUs	8 CPUs	2.0 GHz	11 GB	24 GB	875 GB	UCS-E180D-M3
vWAAS-12000	4 CPUs	12 CPUs	2.6 GHz	12 GB	48 GB	750 GB	UCS-C220 or UCS-C240
vWAAS-50000	8 CPUs	16 CPUs	2.6 GHz	48 GB	72 GB	1500 GB	UCS-C220 or UCS-C240
vWAAS-150000	24 CPU	---	3.0 GHz	96 GB	---	2999 GB	UCS-C220 or UCS-C240

Guidelines for Using Cisco vWAAS with Cisco WAAS

This section contains the following topics:

Operating Guidelines for Cisco vWAAS in Cisco WAAS

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

Caution Before installing new Cisco vWAAS instances along with existing Cisco vWAAS instance in any host, ensure that there is sufficient CPU, Memory, and Storage for all the instances planned.

- For Cisco vWAAS in Cisco WAAS Version 6.1.x and later, the Cisco vWAAS and Cisco vCM devices require *both* virtual (network) interfaces to be present, but both need not be active. The virtual interface 1/0 of Cisco vWAAS will come up in **no shutdown** state and will be sending DHCP request for IP address request from DHCP server. The virtual interface 2/0 will be in 'shutdown' state and can be configured as required. In case of Cisco vCM, by default, both the virtual interfaces will come up with **shutdown** state. For more information, see the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

Upgrade and Downgrade Guidelines for Cisco vWAAS in Cisco WAAS

- 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 Cisco UCS-E firmware, 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 Cisco vWAAS, upgrade one Cisco vWAAS node at a time in any Cisco UCS device. Considering the resized options selection, ensure that there is enough available disk space, before and after the upgrade. Upgrades done without sufficient space makes the Cisco vWAAS device go offline and in diskless mode.

- If the virtual host was created using an OVA file of Cisco vWAAS in Cisco WAAS Version 5.0 or earlier, and you have upgraded Cisco vWAAS within Cisco WAAS, you must verify that the SCSI Controller Type is set to **VMware Paravirtual**. Otherwise, Cisco 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 Cisco 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 Cisco vWAAS, in Cisco WAAS Version 6.1.x or later.

  For more information on setting the SCSI Controller Type and on the Cisco vWAAS VM installation procedure, see the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

Note If the Cisco vWAAS device is downgraded in the following scenarios:

—from Cisco vWAAS in Cisco WAAS Version 6.4.3x to Cisco WAAS Version 6.2.3x, or
—from vWAAS in Cisco WAAS Version 6.x to 5.x

the Cisco 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.

Cisco WAAS, ISR and IOS-XE Interoperability

This section contains the following topics:

Cisco WAAS, ISR and IOS-XE Interoperability

Table 5 Cisco WAAS, ISR and IOS-XE Interoperability

Cisco ISR-Platform	Cisco WAAS Version Supported	Cisco IOS-XE Version Supported
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451	• 6.4.3	• 3.16.4a, 3.16.7b, • 16.3.6, 16.3.7, 16.6.3, 16.6.4, 16.5.2, 16.8.1, 16.3.5, 16.6.2, 16.9.1
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451	• 6.4.3a	• 16.9.2, 16.9.3
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451	• 6.4.3b	• 16.3.8, 16.6.5, 16.6.6, 16.9.3, 16.11.1
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451	• 6.4.3c	• 16.3.8, 16.6.6, 16.9.3, 16.11.1, 16.11.2
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451	• 6.4.3d	• 16.3.9, 16.6.7, 16.9.4*, 16.12.2, 17.1.1
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451	• 6.4.3e	• 16.6.8, 16.9.5*, 16.12.03s
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451	• 6.4.3f	• 16.3.11,16.6.8,16.9.5,16.9.6* ,16.12.4,17.3.1a

* In the table column **Cisco IOS-XE Version Supported**, this is the recommended release version.

Note ISR Platforms running software version 17.4 or later do not support the WAAS software. We recommend that you use IOS version 17.3 or earlier if you want to continue using the WAAS software.

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

- Cisco ISR-4321-B/K9 is not supported for Cisco ISR-WAAS installation.
- Activating Cisco ISR-WAAS after formatting the Cisco 4000 Series Cisco ISR-router bootflash:

  After you format the Cisco 4000 Series ISR-router bootflash, you must reload the router to ensure a successful activation of Cisco ISR-WAAS. If you do not reload the Cisco ISR router after formatting the bootflash, you will be unable to activate Cisco 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*.
- Using the intrusion detection and prevention system Snort with Cisco ISR-WAAS and Cisco ISR-4000 Series, with a hard disk less than or equal to 200 GB:

  To ensure a successful Cisco WAAS installation of Cisco ISR-WAAS and Snort on a Cisco ISR router, you must install Cisco ISR-WAAS *before* you install Snort. If you do not follow this installation order, Cisco ISR-WAAS will not install and a disk error will be displayed.
- VRF restriction for **VirtualPortGroup31** on Cisco ISR-WAAS:

When you configure Cisco ISR-WAAS with EZConfig: **VirtualPortGroup31**, the Cisco 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 Cisco 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*.

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

Cisco AppNav and AppNav-XE Interoperability

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

Note AppNav Controller functionality is available for Cisco WAAS Version 6.4.1 and later. However, configuration of the AppNav Controller function and Cisco WAAS node function on the same device is not supported.

- All Cisco WAAS nodes in an AppNav deployment must be running Cisco WAAS version 5.0 or later.
- Cisco WAAS Version 6.4.1 and later ensure porting of AppNav to the Cisco WAASNet infrastructure.

Note Cisco WAAS Version 6.4.1 and later supports Cisco AppNav IOM.

- All Cisco AppNav devices in a single cluster must be of the same exact type. This includes Cisco 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 Cisco Cloud Services Router (Cisco CSR) 1000V Series or the Cisco Integrated Services Router (Cisco ISR) 4000 series. For example, you cannot have a Cisco ISR-4451 and a Cisco ISR-4321 in the same AppNav-XE cluster.
- If you are connecting an AppNav Controller (ANC) to a Cisco 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 Cisco Catalyst 6500 series switch.

Note Although a Cisco IOS router can have a dot (".") in the hostname, this special character is not allowed in a Cisco 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 '.'**.

- If you have configured NBAR protocols and nested class maps on an AppNav-XE cluster (AppNav-XE device running software version Cisco IOS-XE version 16.10 and later) and want to downgrade the AppNav-XE device to a lower version, we recommend that you remove the NBAR protocol and nested class map configurations from the Cisco WAAS Central Manager AppNav-XE cluster first, otherwise the AppNav-XE cluster gets into the **Force Device Group** settings mode.

Cisco WAAS, ASR/CSR and IOS-XE Interoperability

Table 6 Cisco WAAS, ASR/CSR, and IOS-XE Interoperability

Cisco WAAS Version	Cisco ASR/CSR Series	Cisco 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
6.1.1a, 6.2.1x	ASR-1000x/CSR-1000V	3.15.2, 3.16.01a, 3.16.2, 3.17
6.2.3	ASR-1000x/CSR-1000V	• 3.13.8,3.15.2, 3.16.01a, 3.16.2, 3.16.3, 3.16.6, 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
6.4.1x	ASR-1000x/CSR-1000V	• 3.13.8, 3.16.06, 3.17.04, • 16.04.01, 16.3.3, 16.4.2, 16.3.5, 16.6.1, 16.6.2, 16.7.1
6.4.3, 6.4.3a	ASR-1000x/CSR-1000V	• 3.16.4a,3.16.7b • 16.3.6, 16.3.7, 16.6.3, 16.6.4, 16.5.2, 16.8.1, 16.3.5, 16.6.2, 16.9.1, 16.9.2, 16.9.3
6.4.3b	ASR-1000x/CSR-1000V	16.3.8, 16.6.5, 16.6.6, 16.9.3, 16.11.1
6.4.3c	ASR-1000x/CSR-1000V	16.3.8, 16.6.6, 16.9.3, 16.11.1, 16.11.2

Cisco WAAS Version	Cisco ASR/CSR Series	Cisco IOS-XE Version Supported
6.4.3d	ASR-1000x/CSR-1000V	16.6.7, 16.9.4, 17.1.1, 16.12.2, 16.3.9
6.4.3e	ASR-1000x/CSR-1000V	16.6.8, 16.9.5, 16.12.03s
6.4.3f	ASR-1000x/CSR-1000V	16.3.11,16.6.8,16.9.5,16.9.6,16.12.4,17.3.1a

Traffic Interception Interoperability

This section contains the following topics:

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) and Catena. For Cisco WAAS Version 5.5.1 and earlier, Cisco WAAS supports WCCP, AppNav, and vPATH.

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

- Cisco ISR-WAAS devices support only the AppNav Controller interception method. For more information on Cisco AppNav, see Cisco AppNav and AppNav-XE Interoperability, page 20.
- For Cisco vWAAS in Microsoft Azure, the supported traffic interception method is PBR (Police-Based Routing); Cisco vWAAS in Microsoft 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 Interception Interoperability

Cisco WAAS Central Managers running Cisco WAAS Version 6.4.3 and later can manage WAEs running Cisco WAAS Software Version 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 To perform the Cisco WAAS software upgrade on all WAEs, use the Cisco WAAS Central Manager GUI.

Step 3 Verify that all WAEs have been upgraded in the **Devices** pane of the Cisco WAAS Central Manager GUI. To view the software version of each WAE, choose **Devices**.

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
```

Citrix ICA Interoperability

Consider the following guidelines for 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**
- Citrix NetScaler/HDX insight version used for test validation:
  - **NetScaler VPX 12.1.51.19** (HDX insight 12.1.50.43), DDC 7.18 VDA 7.18 (Windows Server 2k16), Windows Client 2007, 2010, Citrix Receiver 14.1,14.5,14.9,14.12.
  - **XenApp & Desktop DDC 7.18, VDA 7.18** (Windows server 2k16), Windows Client 2007, 2010, Citrix Receiver 14.1,14.5,14.9,14.12.
  - **XenApp & Desktop DDC 7.15.300LTSR, VDA 7.15.300LTSR** (Windows server 2k16), Windows Client 2007, 2010, Citrix Receiver 14.1,14.5,14.9,14.12.
  - **XenApp & Desktop DDC 7.6, VDA 7.6** (Windows server 2k12r2), Windows Client 2007, 2010, Citrix Receiver 14.1,14.5,14.9,14.12.
  - **XenApp & Desktop 6.5** (Windows server 2008r2), Windows Client 2007, 2010, Citrix Receiver 14.1,14.5,14.9,14.12.

Cisco 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.

Step 6 Table 7 shows the interoperability between Cisco WAAS application accelerators and the F5 load balancer. For more information about Cisco WAAS load balancing, see the sections "About Traffic Interception Methods" and "Configuring Policy-Based Routing" in the *Cisco Wide Area Application Services Configuration Guide*, and see the *Server Load-Balancing Guide vA5(1.0), Cisco ACE Application Control Engine*.

Table 7 Cisco WAAS Application Accelerators Interoperability with Load Balancers

Cisco WAAS Status	Load Balancer Status	Authentication Method	Cisco WAAS Application Accelerator Supported or Not Supported
WAAS enabled	F5 enabled	Kerberos	• EMAPI not supported • SSL not supported
WAAS disabled	F5 enabled	Kerberos	• EMAPI supported • SSL supported
WAAS enabled	F5 disabled	Kerberos	• EMAPI supported • SSL supported
WAAS enabled	F5 enabled	NTLM	• EMAPI supported • SSL not supported

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 Cisco WAAS Version 6.4.3x

This section contains the following topics:

For additional upgrade information and detailed procedures, see the *Cisco Wide Area Application Services Upgrade Guide*.

Guidelines for Upgrading from a Release Version to Cisco WAAS Version 6.4.3x

Consider these guidelines to upgrade from a release version to Cisco WAAS Version 6.4.3x:

- Upgrading to Cisco WAAS Version 6.4.3 is supported from Cisco WAAS Version 4.2.1 and later. For information on upgrade paths, see Upgrade Paths and Considerations for Cisco WAAS Version 6.4.3x, page 25.
- 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 Cisco WAAS Version 6.4.3x, see Migrating a Cisco WAAS Central Manager from an Unsupported to a Supported Platform, page 36.

Note When you perform a software upgrade via the Cisco WAAS Central Manager, there is only a limited system check to verify the support of the target Cisco WAAS version. To ensure that you have a successful Cisco WAAS upgrade, use Table 8, “Upgrade Paths to Cisco WAAS Version 6.4.3,”to verify that the target version is supported for your system.

Upgrade Paths and Considerations for Cisco WAAS Version 6.4.3x

This section contains the following topics:

Upgrade Paths for Cisco WAAS Version 6.4.3x

Upgrading to WAAS Version 6.4.3x is supported from WAAS Version 4.2.x and later. Table 8 shows the upgrade path for each of these versions.

Note When you perform a software upgrade via the WAAS Central Manager, there is only a limited system check to verify the support of the target WAAS version. To ensure that you have a successful WAAS upgrade, use Table 8, to verify that the target version is supported for your system.

Table 8 Upgrade Paths to Cisco WAAS Version 6.4.3x

Current Cisco WAAS Version	Cisco WAAS Central Manager CM Upgrade Path	Cisco WAAS Upgrade Path
5.5.3 and later	• Upgrade directly to 6.4.3x	• Upgrade directly to 6.4.3x

Current Cisco WAAS Version	Cisco WAAS Central Manager CM Upgrade Path	Cisco WAAS Upgrade Path
4.3.x through 5.5.1	1. Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x 2. Upgrade to 6.4.3x	1. Upgrade to 5.5.3, 5.5.5x, or 5.5.7x 2. Upgrade to 6.4.3x
4.2.x	1. Upgrade to version 4.3.x through 5.4.x 2. Upgrade to 5.5.3 or 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x 3. Upgrade to 6.4.3x	1. Upgrade to version 4.3.x through 5.4.x 2. Upgrade to 5.5.3, 5.5.5x, or 5.5.7x 3. Upgrade to 6.4.3x

Upgrading from Cisco WAAS Version 5.x and Later to Cisco WAAS Version 6.4.3x

This section contains the following topics:

Cisco 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 Citrix ICA Interoperability, page 23. If no application is using the unsupported configurations on the device, then remove the unsupported configurations to upgrade.

Cisco WAAS Version 5.2 and Later: 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 Cisco WAAS Central Manager **Admin > AAA > Users** page.

For remotely authenticated users: Change usernames on the remote authentication server.

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

Cisco WAAS Version 5.3 and Later: 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.

Cisco WAAS Version 6.4.3x: vWAAS

- When upgrading Cisco vWAAS, do not upgrade more than five Cisco vWAAS nodes at the same time on a single Cisco UCS device box. Upgrading more than five Cisco vWAAS nodes at the same time may cause the Cisco vWAAS devices to go offline and diskless mode.
- Cisco vWAAS for Cisco WAAS 6.4.3 requires additional resources before upgrading from Cisco WAAS 6.2.3d to Cisco WAAS 6.4.3x:
  - **Upgrading from the Cisco WAAS Central Manager**: If you initiate and complete the upgrade from the Cisco WAAS Central Manager without increasing resources for Cisco vWAAS, alarms (CPU & RAM) to indicate insufficient resource allocation will be displayed on the Cisco WAAS Central Manager *after* the upgrade process is completed. No alarms are displayed at the beginning of the upgrade process.
  - **Upgrading from the WAAS CLI**: If you initiate an upgrade to Cisco WAAS 6.4.3x with the Cisco WAAS CLI, a warning on insufficient resources is displayed at the *start* of the upgrade process.
- Upgrading the ENCS 5400-W Series appliances and CSP 5000-W appliances to Cisco WAAS Version 6.4.3e is not supported. To run Cisco WAAS 6.4.3e version on these devices, you must do a fresh installation with the required version of the Cisco WAAS Unified Package for ENCS 5400-W and CSP 5000-W appliances.

Cisco WAAS Version 6.4.3x: vCM-100 with RHEL KVM or KVM on CentOS

If you upgrade to Cisco WAAS Version 6.4.3, or downgrade from Cisco WAAS Version 6.4.3 to an earlier version, and use a Cisco vCM-100 model with the following parameters, the Cisco vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

- Cisco vCM-100 has default memory size of 2 GB
- Cisco 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 Cisco WAAS Central Manager database.

To resolve this situation, follow these steps:

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

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

Upgrading from Cisco WAAS Version 4.2.x to Cisco WAAS Version 6.4.3x

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 8.

Workflow: Upgrading from a Release Version to Cisco WAAS Version 6.4.3x

To upgrade from a Release Version to Cisco WAAS Version 6.4.3x, complete the tasks listed in Table 9.

Table 9 Workflow: Upgrading from a Release Version to Cisco WAAS Version 6.4.3x

Workflow Task	Description
• Upgrade Part 1: Create a Backup of the Primary Cisco WAAS Central Manager Database	• Before you start the upgrade process from a release version to Version 6.4.3x, create a backup of the primary Cisco WAAS Central Manager database and save it to a remote location.
• Upgrade Part 2: Upgrade the Standby Cisco WAAS Central Manager	• If your Cisco WAAS system has a standby Cisco WAAS Central Manager, upgrade the standby Cisco WAAS Central Manager *before* you upgrade the primary Cisco WAAS Central Manager.
• Upgrade Part 3: Upgrade the Primary Cisco WAAS Central Manager	• Upgrade the primary Cisco WAAS Central Manager, including verifying that the new Cisco WAAS image is loaded correctly, verifying connectivity between Cisco WAAS Central Manager and all Cisco WAE devices, and verifying that all Cisco WAE devices are online.
• Upgrade Part 4: Upgrade the Branch Cisco WAE Devices	• Upgrade the branch Cisco WAE devices, including verifying that new Cisco WAAS image is loaded correctly, verifying that correct licenses are installed, and saving the new configuration.
• Upgrade Part 5: Pre-Upgrade Task for the Data Center Cisco WAAS Software	• Upgrade the data center Cisco WAAS software, including upgrading each data center Cisco WAE device.
• Upgrade Part 6: Upgrade Each Data Center Cisco WAE	• Upgrade each data center Cisco WAE device, including disabling and re-enabling WCCP
• 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	• After you complete the Cisco WAAS system upgrade to Version 6.4.3x, perform tasks including clearing your browser cache, verifying licenses, and verifying proper configuration of applications accelerators, policies, and class maps.

Upgrade Part 1: Create a Backup of the Primary Cisco WAAS Central Manager Database

This section contains the following topics:

Prerequisite for the Primary Cisco WAAS Central Manager Database Backup

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

- If you are upgrading your Cisco vCM, Cisco vWAAS or Cisco ISR-WAAS device from an earlier Cisco WAAS version to Cisco WAAS Version 6.4.3x, *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 Cisco WAAS CM database, following the instructions described in the Caution note.
- For devices using Cisco WAAS Version 5.x: The **/sw** and **/swstore** partition size is 1 GB, so you must back up the CMS database, you must back up the CMS database *before* creating a backup of the primary Cisco WAAS Central Manager database, following the instructions described in the Caution note.
- For devices using Cisco WAAS Version 6.x: The **/sw** and **/swstore** partition size is 2 GB, so you do not need to create a backup of the CMS database before creating a backup of the primary Cisco WAAS Central Manager database.

Caution If you are upgrading your Cisco WAAS device from an earlier Cisco WAAS version to Cisco WAAS Version 6.4.3x, and the **/sw** and **/swstore** partition size is less than 2 GB, it is crucial that you create a backup of the Cisco WAAS Central Manager database and save it to an external file (FTP/SFTP) *before* you upgrade to Cisco WAAS Version 6.4.3.

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

After upgrade is complete, restore the saved Cisco WAAS Central Manager database to your system.

Creating a Primary Cisco WAAS Central Manager Database Backup

Before upgrading to Cisco WAAS Version 6.4.3x, follow these steps to create a backup of the Cisco WAAS Central Manager database:

Step 1 Use Telnet or SSH to access the primary Cisco WAAS Central Manager 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 Cisco WAAS Central Manager

Follow these steps to upgrade the standby Cisco WAAS Central Manager, if present in your Cisco WAAS system.

Step 1 Use Telnet or SSH to access the standby Cisco WAAS Central Manager IP address:

Step 2 Copy the new software image to the standby Cisco WAAS Central Manager with the **copy ftp** command.

The following example shows the file in the root directory. Provide the correct path on your Cisco WAAS system, if different from the root directoy path.

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

Step 3 Reload the standby Cisco WAAS Central Manager 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 Cisco WAAS Central Manager and branch Cisco 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 Cisco WAAS Central Manager, confirm that the status indicator for the standby Cisco WAAS Central Manager is **online** and **green**.

Upgrade Part 3: Upgrade the Primary Cisco WAAS Central Manager

Perform the following tasks *before* you upgrade the primary Cisco WAAS Central Manager:

- Before upgrading the primary Cisco WAAS Central Manager, create a backup copy of the primary Cisco WAAS Central Manager database. For more information, see Upgrade Part 1: Create a Backup of the Primary Cisco WAAS Central Manager Database, page 29.
- If your Cisco WAAS system has a standby Cisco WAAS Central Manager, you must upgrade the standby Cisco WAAS Central Manager before you upgrade the primary Cisco WAAS Central Manager. For more information, see Upgrade Part 2: Upgrade the Standby Cisco WAAS Central Manager, page 30.

Follow these steps to upgrade the primary Cisco WAAS Central Manager.

Step 1 Use Telnet or SSH to access the primary Cisco WAAS Central Manager IP address:

Step 2 Copy the new software image to the primary Cisco WAAS Central Manager, either from the Cisco WAAS Central Manager or the Cisco WAAS CLI.

From the Cisco WAAS Central Manager:

a. In the Standby Cisco WAAS Central Manager, navigate to **Admin** > **Versioning** > **Software Update**.

b. From the **Software Files** listing, select the new software version.

c. Click **Submit**.

From the Cisco WAAS CLI:

a. Use the **copy ftp** command.

The following example shows the file in the root directory. Provide the correct path on your Cisco WAAS system, if different from the root directoy path.

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

Step 3 Copy the new Cisco WAAS Version 6.4.3 software image to the primary Cisco WAAS Central Manager, 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 Cisco WAAS system, if different from the root directory path.

Step 4 Reload the primary Cisco WAAS Central Manager, using the **reload** command

Step 5 Verify that the new Cisco WAAS Version 6.4.3x image is loaded correctly, using the **show version** command.

Step 6 To confirm connectivity, ping the standby Cisco WAAS Central Manager (if present in your Cisco WAAS system) and branch Cisco 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 Cisco WAE devices are online.

Step 9 Choose **Device Groups** > **AllWAASGroups** > **Assign Devices** and verify that each Cisco WAE device is listed with a green check mark.

Upgrade Part 4: Upgrade the Branch Cisco WAE Devices

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

- Created a backup copy of the primary Cisco WAAS Central Manager database. For more information, see Upgrade Part 1: Create a Backup of the Primary Cisco WAAS Central Manager Database, page 29.
- Upgraded the standby Cisco WAAS Central Manager, if one is present on your Cisco WAAS system. For more information, see Upgrade Part 2: Upgrade the Standby Cisco WAAS Central Manager, page 30.
- Upgraded the primary Cisco WAAS Central Manager. For more information, see Upgrade Part 3: Upgrade the Primary Cisco WAAS Central Manager, page 31.

Follow these steps to upgrade the branch Cisco WAE devices.

Step 1 Access the primary Cisco WAAS Central Manager GUI:

```
https://cm-ip-address:8443
```

Step 2 Verify that all Cisco 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 Cisco WAE, either from the Cisco WAAS Central Manager or the CLI.

From the Cisco WAAS Central Manager:

a. In the branch Cisco WAE, navigate to **Admin** > **Versioning** > **Software Update**.

b. From the **Software Files** listing, select the new software version.

c. Click **Submit**.

From the Cisco WAAS CLI:

a. 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 Cisco WAAS system, if different from the root directoy path.

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

Step 5 Reload the Cisco WAE using the **reload** command.

Step 6 Verify that the new Cisco WAAS Version 6.4.3x 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:

a. Clear the Enterprise license, using the **clear license transport** command.

b. 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 Cisco WAAS Central Manager, choose **Devices** > *branchWAE*, to verify that the Cisco WAE device is online and has a **green** status.

Step 11 Verify the following Cisco WAE device functionalities:

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

b. (Optional) Confirm that flows are being optimized, using the **show statistics connection** command.

c. 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:

   1. Clear the Transport license, using the **clear license transport** command.
   2. Add the Enterprise license, using the **license add enterprise** command.
   3. Save the changed configuration, using the **copy running-config startup-config** command.

Step 12 The branch Cisco WAE devices within the active Cisco WAAS network are now upgraded to the current Cisco WAAS Version 6.4.3x.

Upgrade Part 5: Pre-Upgrade Task for the Data Center Cisco WAAS Software

Follow these steps to upgrade the data center Cisco WAAS software.

Step 1 Access the primary Cisco WAAS Central Manager GUI:

```
https://cm-ip-address:8443
```

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

Step 3 Resolve any alarm conditions that may exist.

Step 4 Upgrade each data center Cisco WAE (Upgrade Part 6: Upgrade Each Data Center Cisco WAE, page 34).

Note For deployments using WCCP as the traffic interception method, each data center Cisco 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 Cisco 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 Cisco WAE in the cluster, then shut down the interfaces on the optimizing Cisco WAE in the cluster.

Upgrade Part 6: Upgrade Each Data Center Cisco WAE

Follow these steps to upgrade each data center WAE.

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

a. Disable WCCP with the **no wccp tcp-promiscuous service-pair** *serviceID serviceID* global configuration command.

b. Wait until the countdown expires, or use CTL-C to skip the countdown.

c. Verify that WCCP is disabled, using the **show wccp status** command.

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

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

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

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

Step 4 Upgrade the data center Cisco WAE software:

Step 5 Copy the new software image to the data center WAE, either from the Cisco WAAS Central Manager or the CLI.

From the Cisco WAAS Central Manager:

a. In the data center Cisco WAE, navigate to **Admin > Versioning > Software Update**.

b. From the **Software Files** listing, select the new software version.

c. Click **Submit**.

From the CLI:

a. 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 directoy path.

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

Step 6 Reload the Cisco WAE using the **reload** command.

Step 7 Verify that the new Cisco WAAS Version 6.4.3x 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 Cisco WAAS Central Manager, choose **Devices** > *branchWAE*, to verify that the Cisco 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.

a. Telnet to each core router or switch.

b. Enable WCCP, using the **ip wccp 61 redirect-list** *acl-name* command and the **ip wccp 62 redirect-list** *acl-name* command.

- **WCCP Service ID 61: Source IP address**. The WCCP Service ID (service group) is applied closest to the LAN interface.
- **WCCP Service ID 62: Destination IP address**. The WCCP Service ID (service group) is applied closest to the WAN interface.
- You can change the WCCP redirect list as needed by changing the redirect in/out statement.

Step 12 Verify the following Cisco WAE device functionalities:

a. Enable WCCP, using the **wccp tcp-promiscuous service-pair** *serviceID serviceID* global configuration command. If you are using WCCP single-service, use the **wccp tcp-promiscuous** *serviceID* global configuration command.

b. Verify that redirecting router IDs are seen, using the **show wccp routers** command.

c. Verify that all Cisco WAEs in the cluster are seen, using the **show wccp clients** command.

d. Verify that the packet count to the WAE is increasing and no loops are detected, using the **show wccp statistics** command.

e. Verify that the buckets assigned for **Service Group 61** match those of **Service Group 62**, and are assigned to the WAE, using the **show wccp flows tcp-promiscuous detail** command.

f. Verify that flows are being optimized, using the **show statistics connection** command.

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

Step 13 Each data center Cisco WAE within the active Cisco WAAS network is now upgraded to the current Cisco WAAS Version 6.4.3x.

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 Cisco WAAS Version 6.4.3x:

- After upgrading a Cisco WAAS Central Manager, you must clear your browser cache, close the browser, and restart the browser before reconnecting to the Cisco WAAS Central Manager.
- After upgrading application accelerator Cisco 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 Cisco 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 Cisco WAAS Version 6.4.3x, 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 Cisco WAAS Central Managers that have secure store enabled and you have switched primary and standby roles between the two Cisco WAAS Central Managers, before upgrading the Cisco WAAS Central Managers to Version 6.4.3x, you must reenter all passwords in the primary Cisco WAAS Central Manager GUI. The passwords that need to be reentered include user passwords. If you do not reenter the passwords, after upgrading to Cisco WAAS Version 6.4.3x, the Central Manager fails to send configuration updates to Cisco WAEs and the standby Cisco WAAS Central Manager until after the passwords are reentered.
- If you use the setup utility for basic configuration after upgrading to Cisco WAAS Version 6.4.3x, 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 Cisco WAAS Central Manager 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 Cisco WAE-274, WAE-474, WAE-574, WAE-674, WAE-7341, or WAE-7371), you are not allowed to upgrade the device to Version 6.1 or later. You must migrate the Cisco WAAS Central Manager to a supported platform by following the procedure in this section, which preserves all of the Cisco WAAS Central Manager configuration and database information.

Caution Database backup is intended for recovery of the current Cisco WAAS Central Manager 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 Cisco WAAS Central Manager first, and then change its role after database synchronization.

Follow these steps to migrate a primary Cisco WAAS Central Manager from an unsupported platform to a platform that is supported for Cisco WAAS Version 6.4.3x:

Step 1 From the primary Cisco WAAS 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-01-23-2018-15-08_5.0.1.0.15.dump
Backup file backup/cms-db-01-23-2018-15-08_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-01-23-2018-15-08_5.0.1.0.15.dump
```

Step 2 Display and write down the IP address and netmask of the Cisco WAAS 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 Cisco WAAS Central Manager.

```
CM# configure
CM(config)# interface GigabitEthernet 1/0 shutdown
```

Step 4 Replace the existing Cisco WAAS Central Manager device with a new hardware platform that can support Cisco WAAS Version 6.1. Ensure that the new Cisco WAAS Central Manager device is running the same software version as the old Cisco WAAS Central Manager.

Step 5 Configure the new Cisco WAAS Central Manager with the same IP address and netmask as the old Cisco WAAS 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 Cisco WAAS Central Manager.

```
newCM# copy ftp disk 10.11.5.5 / cm-backup.dump cms-db-01-23-2018-15-08_5.0.1.0.15.dump
```

Step 7 Restore the database backup on the new Cisco WAAS Central Manager by using the **cms database restore** command. Use **Option 1** to restore all CLI configurations.

```
newCM# cms database restore backup/cms-db-01-23-2018-15-08_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-01-23-2018-15-08_5.0.1.0.15.dump'
```

Step 8 Enable the CMS service.

```
newCM# configure
newCM(config)# cms enable
```

Step 9 Verify that the Cisco WAAS 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 Cisco WAAS Central Manager that is running on unsupported hardware and is registered to the primary Cisco WAAS Central Manager, deregister the standby Cisco WAAS Central Manager.

```
standbyCM# cms deregister
```

Step 11 Upgrade the primary Cisco WAAS Central Manager to Cisco WAAS Version 6.4.3x. You can use the **Central Manager Software Update** window or the **copy ftp install** command.

Step 12 Verify that the Cisco WAAS 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 Cisco WAAS 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 Cisco WAAS Central Manager role to standby, and register the standby Cisco WAAS Central Manager to the primary Cisco WAAS 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 Primary Cisco WAAS Central Manager to a Cisco vCM

Follow these steps to migrate a physical appliance being used as a primary Cisco WAAS Central Manager to a Cisco vCM:

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

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

Step 3 Ensure that the Primary Cisco WAAS Central Manager and Standby Cisco WAAS Central Manager updates are working.

Step 4 Switch over Cisco WAAS Central Manager roles so that Cisco vCM works as Primary Cisco WAAS Central Manager. 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 Cisco 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** EXEC command. 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 Cisco WAAS 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** or **Journal commit I/O error** or **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 Cisco WAE device and wait until the RAID rebuild finishes normally.

Using Previous Client Code

If you have upgraded to Cisco WAAS Version 6.4.3x and are using the WSDL2Java tool to generate client stubs that enforce strict binding, earlier version client code (prior to Cisco WAAS Version 4.3.1) may return unexpected exceptions due to new elements added in the response structures in Cisco WAAS Version 4.3.1 and later releases. The observed symptom is an exception related to an unexpected subelement because of the new element (for example, a **deviceName** element) in the XML response.

To work around this problem, we recommend that you patch the WSDL2Java tool library to silently consume exceptions if new elements are found in XML responses and then regenerate the client stubs. This approach avoids future problems if the API is enhanced with new elements over time.

You must modify the ADBBeanTemplate.xsl file in the **axis2-adb-codegen-*version*.jar** file.

To apply the patch, follow these steps:

Step 1 List the files in the **axis2-adb-codegen**-*version*.**jar** file:

```
# jar tf axis2-adb-codegen-1.3.jar
```

```
META-INF/
META-INF/MANIFEST.MF
org/
org/apache/
org/apache/axis2/
org/apache/axis2/schema/
org/apache/axis2/schema/i18n/
org/apache/axis2/schema/template/
org/apache/axis2/schema/typemap/
org/apache/axis2/schema/util/
org/apache/axis2/schema/writer/
org/apache/axis2/schema/i18n/resource.properties
org/apache/axis2/schema/i18n/SchemaCompilerMessages.class
org/apache/axis2/schema/template/ADBDatabindingTemplate.xsl
org/apache/axis2/schema/template/CADBBeanTemplateHeader.xsl
org/apache/axis2/schema/template/CADBBeanTemplateSource.xsl
org/apache/axis2/schema/template/PlainBeanTemplate.xsl
org/apache/axis2/schema/template/ADBBeanTemplate.xsl
org/apache/axis2/schema/c-schema-compile.properties
org/apache/axis2/schema/schema-compile.properties
org/apache/axis2/schema/typemap/JavaTypeMap.class
org/apache/axis2/schema/typemap/TypeMap.class
org/apache/axis2/schema/typemap/CTypeMap.class
org/apache/axis2/schema/util/PrimitiveTypeWrapper.class
org/apache/axis2/schema/util/PrimitiveTypeFinder.class
org/apache/axis2/schema/util/SchemaPropertyLoader.class
org/apache/axis2/schema/SchemaConstants$SchemaPropertyNames.class
org/apache/axis2/schema/SchemaConstants$SchemaCompilerArguments.class
org/apache/axis2/schema/SchemaConstants$SchemaCompilerInfoHolder.class
org/apache/axis2/schema/SchemaConstants.class
org/apache/axis2/schema/ExtensionUtility.class
org/apache/axis2/schema/CompilerOptions.class
org/apache/axis2/schema/writer/BeanWriter.class
org/apache/axis2/schema/writer/JavaBeanWriter.class
org/apache/axis2/schema/writer/CStructWriter.class
org/apache/axis2/schema/SchemaCompilationException.class
org/apache/axis2/schema/BeanWriterMetaInfoHolder.class
org/apache/axis2/schema/SchemaCompiler.class
org/apache/axis2/schema/XSD2Java.class
META-INF/maven/
META-INF/maven/org.apache.axis2/
META-INF/maven/org.apache.axis2/axis2-adb-codegen/
META-INF/maven/org.apache.axis2/axis2-adb-codegen/pom.xml
META-INF/maven/org.apache.axis2/axis2-adb-codegen/pom.properties
```

Step 2 Change the **ADBBeanTemplate.xsl** file by commenting out the following exceptions so that the generated code consumes the exceptions:

```
<xsl:if test="$ordered and $min!=0">
  else{
    // A start element we are not expecting indicates an invalid parameter was passed
    // throw new org.apache.axis2.databinding.ADBException("Unexpected subelement " +
reader.getLocalName());
  }
</xsl:if>

.
.
.

  while (!reader.isStartElement() &amp;&amp; !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.

Downgrading from Cisco WAAS Version 6.4.3x to a Previous Version

This section contains the following topics:

Downgrading the Cisco WAAS System from Cisco WAAS Version 6.4.3x to a Previous Version

This section contains the following topics:

Downgrade Path Considerations

- Downgrading from Cisco WAAS Version 6.4.3x is supported to Cisco WAAS Version 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 Cisco WAAS Version 6.x to a version earlier than Cisco WAAS Version 5.5.3 is not supported.
- On the Cisco 4451-X Integrated Services Router running Cisco ISR-WAAS, downgrading to a version earlier than Cisco WAAS Version 5.2.1 is not supported.
- On the Cisco UCS E-Series Server Module installed in a Cisco ISR G2 Router and running Cisco vWAAS, downgrading to a version earlier than Cisco WAAS Version 5.1.1 is not supported. On the Cisco UCS E-Series Server Module installed in the Cisco 4451-X Integrated Services Router and

running Cisco vWAAS, downgrading to a version earlier than Cisco WAAS Version 5.2.1 is not supported. On other Cisco vWAAS devices you cannot downgrade to a version earlier than Cisco WAAS Version 4.3.1.

- On Cisco WAVE-294, WAVE-594, WAVE-8541 models with solid state drives (SSDs) you cannot downgrade to a version earlier than Cisco WAAS Version 5.2.1.
- On Cisco WAVE-694 model with solid state drives (SSDs), you cannot downgrade to a version earlier than 5.5.1.
- On Cisco vCM-500 or Cisco vCM-1000, you cannot downgrade to a version earlier than Cisco WAAS Version 5.5.1.

Downgrade Component and Data Considerations

- For Cisco WAAS on devices on the Cisco ENCS 5400-W Series:
  - You cannot downgrade a Cisco vWAAS device on Cisco ENCS-W to a version earlier than WAAS Version 6.4.3, if it is connected with inline FTW card and configured with portchannel and standby or if configured with inline interception.
  - You cannot downgrade a Cisco vWAAS device on Cisco ENCS-W to a version earlier than Cisco WAAS Version 6.4.1.
  - The Cisco WAAS Central Manager supports upgrade and downgrade of all *applicable* device types in a device group.

    For example, if you are downgrading a device group that has a physical Cisco WAE, a Cisco vWAAS, and appliances like the Cisco ENCS 5400-W Series or the Cisco CSP 5000-W Series to a version earlier than their respective supported version, the Cisco WAAS Central Manager will initiate the downgrade process only for the physical and virtual Cisco WAEs, but not for appliances like Cisco ENCS 5400-W Series or Cisco CSP 5000-W Series.
- For Cisco ENCS 5400-W Series appliances and Cisco CSP 5000-W Series appliances: To run a Cisco WAAS version earlier than Cisco WAAS Version 6.4.3e, you must do a fresh installation. A downgrade from Cisco WAAS Version 6.4.3e to an earlier Cisco WAAS version is not supported.
- 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 Cisco WAAS Version 5.0 are maintained.
- If you have configured disk cache for Cisco ISR-WAAS device, downgraded from Cisco WAAS Version 6.4.3 to Cisco WAAS Version 5.5.3, and then restore rollback to Cisco WAAS Version 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 Cisco WAAS Version 6.4.3, 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 Cisco WAAS Central Manager from Cisco WAAS Version 6.4.3x to an Earlier Version

This section contains the following topics:

Cisco WAAS Central Manager Downgrade Path Considerations

- Downgrading from Cisco WAAS Version 6.4.3x Cisco WAAS Central Manager directly to a version earlier than Cisco WAAS Version 5.5.3 is blocked.
- If the Cisco WAAS Version 6.4.3x Cisco WAAS Central Manager is downgraded to a version earlier than Cisco WAAS Version 5.2.1, it can no longer manage Cisco AppNav-XE clusters and devices and all related configuration records are removed.
- When downgrading a Cisco WAAS Version 6.4.3x Cisco WAAS Central Manager to a version earlier than Cisco WAAS Version 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.

Cisco WAAS Central Mangaer Downgrade Procedure Considerations

- As it applies to your Cisco WAAS Central Manager and the current version of your Cisco WAAS system, perform the following tasks *before* a Cisco WAAS Central Manager downgrade:
  - If you have a standby Cisco WAAS Central Manager, it must be registered to the primary Cisco WAAS Central Manager *before* the downgrade.
  - Prior to downgrading the Cisco WAAS Central Manager to a version up to Cisco WAAS Version 5.2.1, you must remove **Backup WNG** from the Cisco AppNav-XE cluster and verify that the Cisco WAAS Central Manager and Cisco AppNav-XE device are in sync.
- If you have configured App ID and nested class-map in the Cisco AppNav XE cluster, you should not downgrade the Cisco WAAS Central Manager (running Cisco WAAS Version 6.4.3b and later) to a lower version that does not support the App ID configurations from the CLI. To downgrade, you should first remove the AppID and nested class-map configurations from AppNav XE cluster and then proceed with the downgrade. If you try to downgrade the Cisco WAAS Central Manager from the Cisco WAAS Central Manager GUI, an error message prompts you to remove the App ID and nested class map configuration before proceeding with the downgrade.
- Each of the following Cisco WAAS Central Manager downgrade procedures requires a particular task sequence:
  - If the Cisco WAAS Central Manager is downgraded to a version up to Cisco WAAS Version 5.2.1 and if the Cisco AppNav-XE cluster has more than 32 Cisco WAAS nodes: Prior to downgrade, we recommend that you reduce the number of Cisco WAAS nodes to a maximum of 32 Cisco WAAS nodes.
  - When downgrading Cisco WAAS devices, first downgrade application accelerator Cisco WAEs, then the standby Cisco WAAS Central Manager (if you have one), and lastly the primary Cisco WAAS Central Manager.
- When downgrading a Cisco AppNav Controller device to a version earlier than 5.0.1, you must perform the following tasks:
  1. Deregister the device from the Cisco WAAS Central Manager.
  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 Cisco WAAS Central Manager to a Previous Version

To downgrade the Cisco WAAS Central Manager (not required for Cisco WAE devices), follow these steps:

Step 1 (Optional) From the Cisco WAAS 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 Cisco WAAS Central Manager, you must clear your browser cache, close the browser, and restart the browser before reconnecting to the Cisco WAAS Central Manager.

Step 3 Reload the device.

Note Downgrading the database may trigger full updates for registered devices. In the Cisco WAAS Central Manager GUI, ensure that all previously operational devices come online.

Cisco WAE and Cisco WAVE Appliance Boot Process

To monitor the boot process on Cisco WAE and Cisco WAVE appliances, connect to the serial console port on the appliance as directed in the Hardware Installation Guide for the respective Cisco WAE and Cisco WAVE appliance.

Cisco WAE and Cisco 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 Guidelines

This section contains the following operating guidelines for Cisco WAAS Version 6.4.3x:

Report Scheduling and Policy Changes

- Cisco WAAS 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.

Device Group Default Settings

When you create a device group in Cisco WAAS Version 6.4.3x, 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 Cisco WAAS 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 Cisco WAAS Central Manager GUI Cisco WAAS 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. To continue to the Cisco WAAS Central Manager login window, click **OK** or **Cancel** in the certificate dialog. To avoid this prompt, remove the installed personal certificates or use a different browser.

- Default settings with mixed versions

  If a Cisco WAAS 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 Cisco WAAS Central Manager to apply the default setting for a feature to mixed devices in a device group, the default for the Cisco WAAS Central Manager version is applied to all devices in the group.

Cisco Software Version 6.4.3x Command Changes

This section lists the new and modified commands in Cisco Software Version 6.4.3x.

- Table 10 lists the commands and options that have been added or changed in Cisco Software Version 6.4.3f.
- Table 11 lists the commands and options that have been added or changed in Cisco Software Version 6.4.3e.
- Table 12 lists the commands and options that have been added or changed in Cisco Software Version 6.4.3b.
- Table 13 lists the commands and options that have been added or changed in Cisco Software Version 6.4.3.

Table 10 Cisco WAAS CLI Commands Added or Modified in Cisco WAAS Version 6.4.3f

Mode	Command	Description
Global Configuration	**(config)# disk encrypt enable {0 | 1| 3}**	Enhanced to include the option for disk sanitation. The default option is 1. 0 -Skip disk sanitization 1 -Pass disk sanitization 3 -Pass disk sanitization as per DOD standards
	config# nfvis mgmt-port shutdown	Enhanced to include the option to shutdown the NFVIS management port, only on the ENCS-W and CSP-W platforms. To enable the management port, run the **no** form of the command. **config# no nfvis mgmt-port shutdown** Note: By default, the NFVIS management port is always enabled (**Admin UP** state).

Table 11 Cisco WAAS CLI Commands Added or Modified in Cisco WAAS Version 6.4.3e

Mode	Command	Description
Global Configuration	**(config)# snmp-server user name group**	Enhanced to include the parameter **protocol AES {128 | 192 | 256} | DES**. Used to specify the encryption method and key length.

Table 12 Cisco WAAS CLI Commands Added or Modified in Cisco WAAS Version 6.4.3b

Mode	Command	Description
Global Configuration	**router(config)# class-map type appnav match-any xxx** **router(config-cmap)# match nbar-protocol yyy**	Used to configure an AppNav class map based on Application ID and match it with the NBAR Protocol
	router(config-cmap)# match nbar-protocol **router(config-cmap)# match nbar-protocol attribute xxx**	Used to configure an AppNav class map based on Application ID and match it with the NBAR Protocol attribute
	router(config-cmap)# match nbar-protocol **router(config-cmap)# match nbar-protocol attribute sub-category <sub-category-name>**	Used to configure an AppNav class map based on Application ID and match it with the NBAR Protocol attribute and sub-attribute
	router(config-cmap)# match class xxx **router(config-cmap)# APPNAV-ACL-HTTP dstPort {80, 8080, 8088, 8000, 3128} xxx AppIds {yyy, zzz, aaa}**	Used to configure an AppNav class map based on Application ID and match it with another class-map
	accelerator http object-cache add-memory	Used to configure additional memory in RAM for Akamai caching.
EXEC	**show statistics accelerator smb**	Enhanced to include optimization statistics for SMBv311 encrypted optimization.

Mode	Command	Description
	show alarms core	Used to display details for core files
	show alarms crash	Used to display details for crash files

Table 13 Cisco WAAS CLI Commands Added or Modified in Cisco WAAS Version 6.4.3

Mode	Command	Description
Global Configuration	**accelerator smb bypass-file-size min-file-size <value>**	Use to configure the minimum file size for bypass by SMB optimization for better performance
	accelerator smb highest-dialect 3-11	Used to configure SMB version 3.11 to be the highest dialect.
	accelerator smb preposition server	Used to set the server name for the directive. To preposition a DFS shares, dfs workspace name should be entered in the format domain_name/namepace_name .
	(config-ssl-accelerated) dscp-lan	Used to specify the dscp-lan value to be used by the SSL protocol for the accelerated service.
	(config-ssl-accelerated) dscp-wan	Used to specify the dscp-wan value to be used by the SSL protocol for the accelerated service.
	(config-ssl-accelerated) asvc	Used to configure the accelerated service as secondary.
	(config-ssl-accelerated)#application-name)	Enhanced to configure applications like Salesforce and ServiceNow.
EXEC	**show statistics accelerator smb detail**	Added new field descriptions for SMB 3_11 flows.
	show statistics accelerator mapi detail	Added new field descriptions for MAPI HTTP flows.
	sh statistics application saas	Enhanced to display statistics for ServiceNow and Salesforce.
	debug accelerator LogShrink enable	Used to compress the detailed SMB accelerator logs.

Cisco Software Version 6.4.3x Resolved and Open Caveats

This section contains the resolved caveats, open caveats, and command changes in Cisco Software Version 6.4.3, fixed and known and contains the following topics:

Cisco Software Version 6.4.3f Resolved Caveats

The following caveats, impacting earlier software versions of Cisco WAAS, were resolved in Cisco Software Version 6.4.3f.

Caveat ID Number	Description
CSCvt65620	In some cases, WAAS device shows cpu utilization exceeded threshold alarm
CSCvu10236	Stale alarm is not clearing in central manager GUI
CSCvu45497	Apache HTTP server multiple vulnerabilities CVE-2020-1934 CVE-2020-1927
CSCvu47501	data partitions to be erased when disk-encrypt config is toggled
CSCvu66900	Time delay occurs while shut/unshut portchannel member interface virtual 1/0 and 2/0 on ENCS-W
CSCvu67537	Key not retrieved after domain controller connectivity flap
CSCvu81926	MAPI AO crash in normal operations
CSCvu83391	Memory Dump noticed while accessing youtube from a Windows 10 client
CSCvv07189	Traffic is not optimizing in NFVIS vbranch solution
CSCvv09089	Traffic blockhole at WAAS after an unexpected reload in waasnet process
CSCvv09104	Debugging with matching ACL doesn't work as expected.
CSCvv20003	Unable to change SNMPv3 user from AES to DES from WCM
CSCvv42489	Key retrieval failed on DC WAAS nodes
CSCvv72081	print operation is taking much time to process the jobs due to connection reset by WAAS for SMB311
CSCvv75759	Apache HTTP Server Multiple Vulnerabilities CVE-2020-9490 CVE-2020-11993 CVE-2020-11984
CSCvv77629	Changes made to Appnav Policies are applied in reverse order
CSCvv88592	The acc_proxy service has been disabled alarm is raised on Central Manager
CSCvv97567	route conflict observed in ENCS-W platform
CSCvw04680	Unexpected reload of waasnet process (dft thread)
CSCvs32581	Central manager audit trail is not logging user action of "restore-default" in device-group policy

Cisco Software Version 6.4.3f Open Caveats

The following caveats are open in Cisco Software Version 6.4.3f. 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
CSCvv39433	Onepclient crash in ISR-WAAS
CSCvv71375	Optimized traffic is greater than the original traffic
CSCvw32663	waasnet service restarting frequently while handling malformed packet
CSCvw32862	snmpwalk gets timed out with Remote SNMP ID and notify inform enabled
CSCvu99806	Model is Undefined and ISR-WAAS not accessible through Internal IP with other Issues-ISR4K
CSCvw12367	Kernel core (kernel.rp_ISR4300_0_20201014193026.core) in ISR4321 (BLD_V174_THROTTLE_LATEST_20201014)
CSCvw04694	Unexpected restart of WAASNET process in connection closure
CSCvw14129	Default Gateway Mac Programed as Zero In WAASNET
CSCvw20914	Unexpected restart of SNMP process in WAAS.
CSCvv99718	waasnet coredump during insertion of ssl in http proxy connection
CSCvv34901	SMB 2.0 connections pushdown in a specific scenario
CSCvw34112	CSR1000v router moving to offline state with 16.3.11 CCO image

Cisco Software Version 6.4.3e Resolved Caveats

The following caveats, impacting earlier software versions of Cisco WAAS, were resolved in Cisco Software Version 6.4.3e.

Caveat ID Number	Description
CSCvu15994	Object cache increased more than 100%
CSCvu14020	After windows domain join observed "sh run" "wr mem" slowness issue on few devices
CSCvu23511	SMB AO in timeout state
CSCvu17002	Need to Mask SNMP Community String in SysReport
CSCvu23479	Sysreport generation issue
CSCvu24267	One of the WAN port link gets negotiated to 10Mbps speed in ENCS
CSCvs76822	mingetty process constantly restarting
CSCvt37725	SMB AO restarts when signed session and unsigned anonymous share session established in single flow
CSCvu32618	AD password sync issue

Caveat ID Number	Description
CSCvk39673	Apache httpd server upgrade to 2.4.x version in WAAS
CSCvo42233	Interface details doesn't show up in link up/down traps in snmp
CSCvr82367	CIMC resets ENCS inline group when show tech-support executed via serial console
CSCvs58970	Multiple times WAASNET process abnormal restart
CSCvs67178	Slow upgrade WCM with many ssl accelerated services
CSCvs77728	syslog is flooding with Emergency Thaw messages
CSCvt07671	DFT memory dump occurred in WAASNET
CSCvt47018	waasnet memory dump occurred with SSL traffic
CSCvt55260	slowness observed in "show run" or "write mem" commands post WAAS device domain-join
CSCvt62215	SSL connections are breaking due to incomplete packet exchange between waas devices
CSCvu29388	Need to Mask SNMP Community String in "sh tech-support" CLI

Cisco Software Version 6.4.3e Open Caveats

The following caveats are open in Cisco Software Version 6.4.3e. 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
CSCvv07189	Traffic is not optimizing in NFVIS vbranch solution
CSCvt65620	In some cases, WAAS device shows cpu utilization exceeded threshold alarm
CSCvu67594	Proxy based HTTPS Application access issue
CSCvu67537	Key not retrieved after domain controller connectivity flap
CSCvu66900	Time delay occurs while shut/unshut portchannel member interface virtual 1/0 and 2/0 on ENCS-W
CSCvu47501	All data partitions to be erased(deep-format) when disk-encrypt config is toggled
CSCvu17773	unwanted nsNotify traps received even when not configured

Cisco Software Version 6.4.3d Resolved Caveats

The following caveats, impacting earlier software versions of Cisco WAAS, were resolved in Cisco Software Version 6.4.3d.

Caveat ID Number	Description
CSCvq71094	Core seen in ISR when removing the service-insertion config and committing it back
CSCvo05022	Unexpected system reload observed in ISR-WAAS in a scenario
CSCvm93197	Device becoming low on available system memory and swap gets used.
CSCvo56976	In some cases SNMP Process stopped working after code upgrade
CSCvq31968	TCP handshake packets are not captured for both tx and rx with packet-capture option in WAAS
CSCvq46172	WAAS device becomes unresponsive due to CPU spike.
CSCvq57545	Observing "No space left on device" error log in Azure device
CSCvi09138	TFO accelerator set to Zero in SN after upgrade in a scenario
CSCvn49079	Rarely Ts pending connections observed with proxy connect traffic
CSCvq79786	T pending connections at SDH read shut in term side observed with proxy connect webtraffic
CSCvr03978	SMBAO restarted in Session setup Response for unsigned 2.02 connection
CSCvq63401	More than 40% memory is used by waasnet process after traffic is stopped
CSCvr20271	Memory consumed by waasnet process is not released even after the traffic is stopped
CSCvr38859	TCP connections are getting reset in ISR-WAAS
CSCvs01400	SNMP user's passwords are stored as clear text
CSCvc89685	SMBAO: decodeVfnCompoundResponse api results in assert failure
CSCvq77784	WAAS (Inline interception) drops fragmented IP packets with padding in Ethernet header
CSCvr25509	WAAS in Appnav interception doesn't handle fragmentation packet properly.
CSCvr44928	WCM manage devices list is not showing correctly under devices tab with latest chrome update
CSCvr46293	WAASNET memory dump observed due to mismatch SSL config
CSCvr66404	Office365 connection is breaking with waas and proxy in environment
CSCvr70166	Core dump seen core.wn_dft0.6.4.3c.b902.cnbuild
CSCvr73697	Stale connections observed for HTTP flows to port 8080 on branch WAE
CSCvr74057	WAAS interface drops packets in a specific scenario.
CSCvs01692	WAAS shows user password, snmp community, windows-domain machine password in clear text in logs
CSCvs03892	snmp_subagent_start_log grows in size and take a lot of spaces on a disk ~3Gb
CSCvq81547	Configuring class-map with match "0.0.0.0 255.255.255.255" in CM GUI triggers FDG.
CSCvq85624	Back out split header alarm code changes
CSCvr04561	WCM: Unable to configure AppNav-XE cluster, after router re-registration.

Caveat ID Number	Description
CSCvq66195	HTTP object-cache whitelist-optimization feature is not working after branch waas reload
CSCvq71603	wn_dft3 memory dump generated while optimizing SSL traffic with proxy
CSCvr07847	win2k19 shares are not accessible from SMB 2.1 unsigned dalect
CSCvs17368	Downloading internet files failed when interposer ssl is enabled

Cisco Software Version 6.4.3d Open Caveats

The following caveats are open in Cisco Software Version 6.4.3d. 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
CSCvo42233	Interface details doesn't show up in link up/down traps in snmp
CSCvp43864	SCP : TFO only throughput drop observed with single client
CSCvr96854	Crash in Kerberos connection of SMB2.1 (Session setup request in DC) dialect with SMBV3 client.
CSCvs10071	Identity added into the black list while doing downgrade from 643d to 641c
CSCvs11495	Device not re-joining WCCP cluster in rare scenario due to wn_ioctl issue after wn restart
CSCvs32581	Central manager audit trail is not logging user action of "restore-default" in device-group policy.
CSCvs38725	CLI output missing newlines with unknown TERM variable
CSCvs41538	Resource reservation failed for proxy connect connections
CSCvr63877	Duplicate policy entries under Cluster config in CM

Cisco Software Version 6.4.3c Resolved Caveats

The following caveats, impacting earlier software versions of Cisco WAAS, were resolved in Cisco Software Version 6.4.3c.

Caveat ID Number	Description
CSCvd65975	Outdated monitoring data not deleted from database
CSCvn17306	Fix WAAS HTTP broken bypass configuration for Akamai feature
CSCvn31929	Upgrade ESXi Virtual Hardware Version to 9 or higher
CSCvo41787	Windows-domain join fails after downgrade and upgrade (643b to 641c ,641c to 643b)

Caveat ID Number	Description
CSCvo77026	Some times WAVE devices report Power Supply Unit (PSUx) reports AC lost
CSCvo91779	ENCS: Deleting a Standby over port channel interface not happening properly
CSCvp04247	DG conf of T+ page can't be pushed to device when cmdauth is enabled at DG, but not at device level
CSCvp19547	cms log entries not logged with GMT but local time
CSCvp25913	Not able to deploy vwaas on KVM using Launch.sh script
CSCvp28818	Virtual waas deployment does not verify supported platform
CSCvp36703	HTTP Object cache restarts when handling HTTP TRACE request
CSCvp36850	Device offline alarm timestamp to be retained after WCM restart
CSCvp47341	Unnecessary client DNS lookup
CSCvp59602	WAAS Unable to configure SW upgrade image on CM
CSCvp64259	Unexpected reload of SNMP Daemon
CSCvp64604	Central Manager traffic for Appnav IOM/WAAS gets optimized with Jumbo MTU fails in 6.x
CSCvp71881	Clients accessing Office 365 are seeing connections failed or delayed causing latency.
CSCvp79527	Cloud Services: Optamization failed due to hostname mismatch with SAN certificate & wildcard config
CSCvp85139	After upgrade to 6.4.3 a seeing high disk utilization Alarm is seen
CSCvp95017	When AkamaiWhitelist enable in Branch and HTTPAO disable in DC:HTTP sites are not loading in browser
CSCvq03096	CE is not handling the traffic for newly added url into Akamai whitelist urls
CSCvq07050	ENCS: Inline Failover timeout value 1 need to remove from supported value list in GUI
CSCvq20794	High disk utilization Alarm is seen, logfiles not rotated
CSCvq31232	WAAS dropping packets with PT Internal error when there is no space to add Auto-Discovery options
CSCvq43344	Appnav report total passthrough traffic is not matched with total appnav traffic passthrough traffic

Cisco Software Version 6.4.3c Open Caveats

The following caveats are open in Cisco Software Version 6.4.3c. 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	Description
CSCvn49079	Ts pending connections observed with proxy connect traffic
CSCvj80301	Akamai: Pending HTTP connections observed during long duration test with Akamai enabled
CSCvm93197	Device becoming low on available system memory and swap gets used.
CSCvn51289	ENCS-W-5406: vWAAS-200 F2W 4 port port channel 50% decode Spirent throughput dropping every 15 mins
CSCvo05022	Unexpected system reload observed in ISR-WAAS in a scenario
CSCvo56936	Akamai: MSFT OTT need to be tweaked to include more varieties of http requests/responses
CSCvo56942	Akamai: Apple iTunes need to be processed through another OTT
CSCvo56976	In some cases SNMP Process stopped working after code upgrade
CSCvp30904	Transfer speed might be impacted if we use Dual ANC/SN combo setup with portchannel interface
CSCvp43864	SCP : TFO only throughput drop observed with single client
CSCvp55629	WAAS optimization breaking SMB sessions when DFS share accessed with url
CSCvp84279	Physical wae device went to rescue image while doing upgrade
CSCvp84394	CMS logs are flooded with "Duplicate Match condition exists" when duplicate match condition is added
CSCvq00349	SN device of Appnav-Inline interception goes unreachable during reload
CSCvq41688	False alarms reporting on the Central Manager
CSCvq46172	WAAS device becomes unresponsive due to CPU spike.
CSCvq58179	WAAS HTTP AO gradually consume all memory and require device reload.
CSCvi09138	TFO accelerator set to Zero in SN after upgrade in a scenario
CSCvp29053	Observing Failure while Registering CSR Router with WAAS central manager
CSCvo98703	NFVIS mgmt ip becomes unreachable after upgrading nfvis from 3.10 to 3.11
CSCvp68819	T pending connections at SDH segment observed with proxy connect webtraffic
CSCvo05022	Unexpected system reload observed in ISR-WAAS in a scenario
CSCvq66195	HTTP object-cache whitelist-optimization feature is not working after branch waas reload
CSCvq70152	Identity lost after upgrade from 623e-b45 to 64b/643c
CSCvq68123	so_dre_nonia service restarted while running ngssl traffic in DC device

Cisco Software Version 6.4.3b Resolved Caveats

The following caveats, impacting earlier software versions of Cisco WAAS, were resolved in Cisco Software Version 6.4.3b.

Caveat ID Number	Description
CSCvc85758	Unexpected termination of login process with a memory dump file
CSCvh12112	Device-Id & DRE-Peer-ID calculated using the Internal Interface MAC Address on ENCS WAAS
CSCvi02645	SNMP service restart seen in WAE device in a scenario
CSCvi48755	WAN Throughput drop observed in 694,594,SUSE-6k,Centos-6k devices
CSCvi55394	Device is unreachable after restarting WAASnet service followed by IMD service
CSCvk32347	Traffic blockhole in only SC/SN combo device with 6.4.1 a image after any waasnet core.
CSCvm31772	MAPI AO shutdown unexpectedly after creating memory dump during server load
CSCvm65210	Need configurable option for SMBv3 client blacklist timeout
CSCvm71218	EOT check error logs get flooding in DRE and syslog errorlogs in WAE syslog
CSCvm77984	windows authentication fail-over server-unreachable is not working as expected
CSCvm94646	WAAS Central Manager login will fail for users during user Password expiry
CSCvn06748	Rarely ICA memory dump observed during NPRM restart
CSCvn11087	Observed system dump during the MAPI performance test in 641c
CSCvn16168	WAAS does not send Remote Address for TACACS+ Enable Authentication
CSCvn20627	vmtool log directed to limited and temporary storage
CSCvn31957	WAAS BIOS is not updating after install on WAAS version 6.4.3b171
CSCvn41476	Observed oclite_timer system dump while running the long soak
CSCvn41523	Gateway not pinging after restart of WAASNET
CSCvn61519	HTTPAO service restart seen in WAE after 643a upgrade in a scenario
CSCvn68230	Wassnet DFT memory dump occurs when it's handling ICA over SSL traffic.
CSCvn68409	Parse buffer in NG-SSL may not terminate with null results memory dump during string operations
CSCvn72347	SN ACL based packet-capture with "swap src-ip" enabled not working in IOM environment
CSCvn75690	DRE statistics files saved to RAM drive leading to memory leak.
CSCvn80759	HTTP black listing for split header request and response
CSCvn85351	smb bypass-file-size min-file-size command to view in startup-config
CSCvn93202	Waasnet memory dump (wn_dft1) occurs after waasnet process restart.
CSCvo10273	ISM core files generating Waas stops passing traffic

Caveat ID Number	Description
CSCvo20585	ISR-WAAS: Onepclient exit unexpectedly at random time after 6.4.3 upgrade
CSCvo34082	Waas SNMP v2 traps not Primarly link up link down but additional alerts also
CSCvo39703	SMB AO Restarted during the scal performance test in 643b
CSCvo43659	Appnav / WAAS node devices goes offline with Central manager after upgrade from 5.5.7b to 6.4.1b
CSCvo47904	SNMP v2 config Traps are not working
CSCvo60134	Incorrect "log index id" in log leads to memory dump
CSCvn39853	SMB 3.1.1 Encryption support by SMBAO
CSCvn68993	WCCP mask assignment not consistent, some local frames corrupted
CSCvn62443	Policy configuration removed while waasnet process restarted

Cisco Software Version 6.4.3b Open Caveats

- The following caveats are open in Cisco Software Version 6.4.3b. Note that there might be additional open caveats from previous releases that are applicable to this release, unless they are specifically listed as resolved.
- For NFVIS open caveats that affect Cisco WAAS, see the *Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.11.x*.

Caveat ID Number	Description
CSCvk59131	Many missed NP keepalive logs seen in waasnet logs
CSCvm54741	Akamai: More WAN and LAN TP fluctuations observed with Akamai Performance in high end VWAAS models
CSCvm59747	ENCS-W port-channel member interface operational state stays Down on a specific scenario
CSCvm93197	Device becoming low on available system memory and swap gets used.
CSCvn05452	Traffic Drop observed on shutdown of standby primary interface in SE+OE combo
CSCvn29696	"T" pending connection at SDH segment while Running webtraffic via DC proxy
CSCvn33962	CSP-W:vWAAS WAN throughput fluctuation observed and WAN TP ~22% less compared with physical WAE
CSCvn51289	ENCS-W-5406: vWAAS-200 F2W 4 port port channel 50% decode Spirent throughput dropping every 15 mins
CSCvn55860	CSPW: Interface lose connectivity when the configurations moved from TenGig copper to Fiber port
CSCvn81520	Uploading Akamai license creating new CusgtomerID

Caveat ID Number	Description
CSCvo05022	SIT: Unexpected system reload observed in ISR-WAAS in a scenario during soak test
CSCvo33162	CSPW: unexpected system reload seen in vWAAS, when peer device is having LLDP enabled
CSCvo34944	CM Appnav XE CLI query for suite license needs to be corrected since not available polaris 16.10
CSCvo45520	Packet-capture appnav-controller CLI keeps on flushing logs even-after executing stop command
CSCvo55751	SRIOV vWAAS gets crashed after mtu configuration
CSCvo56936	Akamai: MSFT OTT need to be tweaked to include more varieties of http requests/responses
CSCvo56942	Akamai: Apple iTunes need to be processed through another OTT
CSCvo56976	In some cases SNMP Process stopped working after code upgrade
CSCvo71759	Selection of non-editable tunnels to be prevented in AppNav cluster wizard
CSCvo73542	Both ANCs show the flow as AC owned
CSCvo85872	SN device of Appnav-Inline interception goes unreachable during U/D in a specific scenario
CSCvo91779	ENCS: Deleting a Standby over port channel interface not happening properly
CSCvp00574	Expired CA certificate need to remove from "Well Known CA"
CSCvp03025	Unexpected system reload of traffic server (Akamai connect)
CSCvp04247	DG conf of T+ page can't be pushed to device when cmdauth is enabled at DG, but not at device level
CSCvp06167	SMBAO Memory configurations are not reflecting the resized values
CSCvp21067	Device is not recovered correctly after shutdown of the device and showing System is not initialized
CSCvp27019	ext4 option to be made as default for better 694 performance
CSCvo41787	Windows-domain join fails after downgrade and upgrade (643b to 641c ,641c to 643b)
CSCvo33543	Physical device falls back to rescue mode in UG/DG in some scenarios
CSCvp50219	Device unreachable while flapping the standby & PC interfaces in ANC

Cisco Software Version 6.4.3a Resolved Caveats

The following caveats, impacting earlier software versions of Cisco WAAS, were resolved in Cisco Software Version 6.4.3a.

Caveat ID Number	Description
CSCvj62798	Remote authenticated users - Tacacs+/Radius unable to login via SSH
CSCvm73619	PIDOF memory dump seen in the WAAS device in a scenario
CSCvk47432	Traffic server system/memory dump is observed during long duration mixed AO soak testing
CSCvm04946	NgSSL Single Sided- Connections getting optimized for non-whitelisted URLs in HTTP connect enabled
CSCvm27185	svcdisabled httpcache alarm raised while running the akamai load test
CSCvm44361	es_ism process memory dump created during overnight web traffic testing
CSCvj82965	ENCS-F2W:vWAAS-port channel 99% decode test throughput is ~40% less compare with Tahoe port-channel
CSCvm10007	F2W: Need new WAAS command for on-demand firmware/FPGA upgrade
CSCvm10763	ENCS vWAAS virtual 2/0 interface getting down after restart waasnet without F2W
CSCvk73391	SMBAO restarted multiple times during file upload/download in 643
CSCvn15406	ICA system/memory dump file seen on the WAAS
CSCvm19178	Alarm Unique ID is resetting for the new alarms
CSCvm31582	Multiple TFO alarms are displayed in UI for same device
CSCvm50802	Device Type filtering is not happening in Device List Page
CSCvn28051	IOS Credentials used for Registration are retained in WCM GUI
CSCvn35355	Traffic blackholed in SE OE Combo when ANC of Combo device1 and SN of combo device 2 is selected
CSCvn45401	Shutdown the interfaces from WCM is not working for both physical and logical interfaces
CSCvh96906	Force device group setting need to be applied multiple time to fix local override
CSCvj66784	Device unresponsive when user login with fail-over authentication with debug auth user enabled
CSCvj88714	WAAS sends TCP timestamp options in the ACK to server even if the server does not send TS options
CSCvj21179	Unable to configure IP for device in BRIDGE mode
CSCvk48179	WAASNET Memory Dump Happens when restarting the waasnet service
CSCvk69680	F2W Inline: Unable to reach default gateway after shut/unshut inlinegrp + disable/enable inline
CSCvm17139	Policy and class-map configuration missed, during continues WAASNET restart.
CSCvm24540	Unexpected system reload observed in ISR-WAAS

Caveat ID Number	Description
CSCvm31772	MAPI AO shutdown unexpectedly after creating memory dump during server load
CSCvm35205	Overlapping FQDN in HTTPAO Whitelist and SSL Accelerated service cause TFO only connection
CSCvm35640	WAASNet process restarts after power outage
CSCvm41942	Unexpected SMB restart upon handling rare smbv1 request
CSCvm41943	SMB Connections will get Reset in SMBV3 Unsigned Client Vs SMBV2 Signed Server in few scenarios
CSCvm45611	waasnet crash at lwssl
CSCvm48362	WAASNet memory dump file generated under certain conditions
CSCvm71236	Domain join status lost after WAAS upgrade to 643

Cisco Software Version 6.4.3a Open Caveats

- The following caveats are open in Cisco Software Version 6.4.3a. Note that there might be additional open caveats from previous releases that are applicable to this release, unless they are specifically listed as resolved.
- For NFVIS open caveats that affect Cisco WAAS, see the *Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.10.x*.

Caveat ID Number	Description
CSCvn68993	WCCP mask assignment not consistent
CSCvn25459	TFO limit set to zero in vWAAS-12k and DRE cache size reduced in vWAAS-50K with 6.2.3e image
CSCvm77984	windows authentication fail-over server-unreachable is not working as expected
CSCvm85956	Unexpected FTP process restart during translog export to server
CSCvm93197	Device becoming low on available system memory and swap gets used.
CSCvn12138	ISR-WAAS console becomes unresponsive.
CSCvn16168	WAAS does not send Remote Address for TACACS+ Enable Authentication
CSCvn20627	vmtool log directed to limited and temporary storage
CSCvn61519	HTTPAO service restart seen in WAE after 643a upgrade in a scenario
CSCvh12112	Device-Id & DRE-Peer-ID calculated using the Internal Interface MAC Address on ENCS WAAS
CSCvm59747	ENCS-W port-channel member interface operational state stays Down on a specific scenario
CSCvn33962	CSP-W:vWAAS WAN throughput fluctuation observed and WAN TP ~22% less compared with physical WAE

Caveat ID Number	Description
CSCvn40316	CSP-5228:vWAAS-50K TFO only test throughput ~46% less compare with 7571
CSCvn43391	CSPW: Unable to connect vWAAS after multiple power-cycle issued from CIMC gui
CSCvn51289	ENCS-W-5406: vWAAS-200 F2W 4 port port channel 50% decode Spirent throughput dropping every 15 mins
CSCvn55860	CSPW: Interface lose connectivity when the configurations moved from TenGig copper to Fiber port
CSCvi48755	WAN Throughput drop observed in 694,594,SUSE-6k,Centos-6k devices
CSCvj80301	Pending HTTP connections observed during long duration test with Akamai enabled
CSCvm54741	More WAN and LAN TP fluctuations observed with Akamai Performance in high end VWAAS models
CSCvn39384	Traffic server Memory dump observed with HTTP traffic and akamai enabled
CSCvk59131	Many missed NP keepalive logs seen in waasnet logs
CSCvm85913	Duplex errors on interfaces that are shut down
CSCvn05452	Traffic Drop observed on shutdown of standby primary interface in SE+OE combo
CSCvn08731	Under rare conditions in SE+OE combo mode connections are not seen in the SN
CSCvm94646	WAAS Central Manager login will fail for users during user Password expiry
CSCvn61273	Duplicate unique ID is observed for alarms in Alarm panel after upgrading the central manager
CSCvn47477	Statistics are not getting cleared in WAAS devices
CSCvn61736	vWAAS-SRIOV interface: With WCCP enabled, gateway is not reachable after WAASnet service restart
CSCvi55394	Device is not unreachable after restarting WAASnet service followed by IMD service
CSCvk32347	Traffic blockhole in only SC/SN combo device with 6.4.1 a image after any waasnet core.
CSCvn29696	"T" pending connection at SDH segment while Running webtraffic via DC proxy
CSCvn31957	WAAS BIOS is not updating after install on WAAS version 6.4.3b171
CSCvn37133	CSP-vWAAS12k: WAASnet-dft memory dump, while WAASnet service is restarted with jumbo MTU configured
CSCvn41523	Gateway not pinging after restart of WAASNET on CSP vWAAS.
CSCvn62443	Policy-Map deletion in Appnav-XE device

Cisco Software Version 6.4.3 Resolved Caveats

The following caveats, impacting earlier software versions of Cisco WAAS, were resolved in Cisco Software Version 6.4.3.

Caveat ID Number	Description
CSCvj63315	Unexpected process reload during large webcast using Akamai Connect
CSCvi98993	THDL & TH Pending Connection seen in BR SN after high load
CSCvc21656	SMB: disable alarm "No active domain identity configured for domain" when identity not necessary
CSCvc83974	Akamai process restarts unexpectedly, leaves a dump file
CSCvd49006	Upgrading the Likewise from 6.1 to 8.5
CSCve71066	FTP connection failure with WAAS after FTP client "MLSD" request.
CSCvf20884	Tacacs+ command authorization failed for user unknown and keep pushing the config from CM
CSCvg25312	SIA Invalid error messages to be displayed
CSCvg30904	Support for DFS with SMB Prepositioning
CSCvg95232	ANC did not stop wccp participation while cluster was not operational.
CSCvh47298	SNMP service poll returns unknown username in a scenario
CSCvh51200	Bypass server configuration with wild cards are not working in HTTPAO
CSCvh54169	SMBAO missing Admission Control accepts connections leading to overload
CSCvh62274	WAAS CM Activation page showing outdated information
CSCvh90104	Disable SSH CBC Mode Ciphers in WAAS
CSCvh94469	Evaluation of WAAS for OpenSSL CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738
CSCvh96699	Unusually large amount of memory Consumed by SMBAO on the DC device during longevity test
CSCvh96772	exec_pkt_cap process memory dump file got generated
CSCvi03102	SMBAO Should raise an alarm when latency parameters are lower then needed
CSCvi05071	Multiple notifications of the same alarm
CSCvi06590	Perf degradation with HTTPS/Live Streaming in 641 when compared to 623d
CSCvi12337	Central manager can have out of sync status of http object cache component
CSCvi17620	Waasnet service restarted while sending single sided https traffic
CSCvi28879	6.2.3d: Update local user details throw error with remote_user field empty

Caveat ID Number	Description
CSCvi37887	Lower DRE error 'Invalid frame version received from peer' to trace level
CSCvi40799	Timeout observed at 180 seconds
CSCvi44283	SMB v3.1.1 Preauth support for SMBAO
CSCvi48375	SMB AO: Duplicate folders wiill show up when User renames a folder
CSCvi54862	packet capture processing does not stop when the ssh session timeouts
CSCvi65520	WCM not updating Policy configuration changed under AppNav Cluster
CSCvi68416	Cms service failing to start after database restored
CSCvi70287	False alarm seen in console and WAE device not optimizing connections in a scenario
CSCvi71814	SMB AO:Rarely Last Write timestamp is changed during file copy and paste
CSCvi73273	Akamai proxy configuration differs from CM GUI
CSCvi74692	WAASNET Process RAM Dump Happens Repeatedly
CSCvi76855	Connection stats pending to increment for RDP traffic in WAE device in a scenario
CSCvi79251	WAE device is being deleted after some time from WAAS group in WCM
CSCvi81780	ICA process generated a memory/system dump in CGP reconnect scenario
CSCvi82129	ASVC memory dump when user disables Interposer-ssl immediately after disabling an ASVC.
CSCvi82153	Traffic is Dropped at The SN when cma process is restarted
CSCvi92383	PT policy for a IP matching ASVC configured and interposer-ssl makes the website inaccessible
CSCvi93462	SSL : Handle delays originated due to client side behavior (Proxy Connect)
CSCvi97202	Gateway unreachable after WN service restart observed in vWAAS device
CSCvj06223	Service Restart Of WAASNET During Intializing Interface
CSCvj07016	WAASNet process going pending state and not handling traffic in a scenario
CSCvj13159	Zero Mac is getting programmed in WAAS when gateway interface is flapped in Apnnav-xe setup
CSCvj21786	SMB AO office files are failing to open after save via SMBv1
CSCvj25184	Akamai process restarts unexpectedly and leaves a dump file while accessing sites with curl command.
CSCvj26521	Correct AO Plumb / Chaining behavior in WAAS 6.x code
CSCvj37681	AppNav Routers Registration failure and offline on CM

Caveat ID Number	Description
CSCvj44598	Webpage fail to open, when HTTPAO is in half close connection state (proxy connect)
CSCvj51761	WAASNet service restart with a core file with wn_dft_thread and DP handler
CSCvj53621	SMBAO created a core dump due to handling non existent Negotiate Response
CSCvj65381	Inconsistent operation of debug commands
CSCvj73342	Connection broken and download fail for long connection download
CSCvj78487	Traffic server memory dump created when sub_trans/ACC connect with no uds_session and address-check
CSCvj97610	The unknown command when interpreted by the WAAS unable to parse the packet
CSCvj98884	SSL AO stats process stuck interrupting stats reproted to WCM
CSCvk03700	unknown NTLMVersion from windows client breaks smb communication
CSCvk03838	Optimization not working between 623e and other released versions.
CSCvk07808	Encryption Services Failed to initialized, unable to configure identity for MAPI / SMB
CSCvk25931	Random SNMP polling failure
CSCvk45500	ICA accelerator restarts in a rare case
CSCvk45904	In some cases, WAASNet Process creates memory dump and impacts traffic
CSCvk47607	False alarms reporting on the Central Manager
CSCvk50234	ICA vs ICA OVER SSL graph is not populating records in the CM GUI
CSCvk66495	Closing ICAoverSSL connections after exceeding the ICA session-limit.
CSCvk76419	ISM Core file during SSL HANDSHAKE causing IsmFlowmgr issue
CSCvm04854	SMBAO Restarts while parsing SMB1 error response
CSCvj00003	Add 6.2.3e TCP buffer changes to 6.4.1b to improve performance
CSCvj96874	header_max_limit alarm does not clear until HTTP accelerator is restarted
CSCvk30256	Self clean up support for alarm mismatch data between Central Manager and WAE
CSCvi53371	SSL version not inheriting from SSL global settings for peering Services.
CSCve04030	Application ID for MAPI traffic showing as Citrix in AppNav XE device
CSCvh03423	Connections not getting redirect to SN WAE device in a scenario
CSCvh47471	SNMP View cannot be modified/removed after downgrade from 6.x to 5.x

Caveat ID Number	Description
CSCvh65545	Observed intermittent traffic issue after nprm restart
CSCvi02659	Gateway unreachable in standalone inline device after reload
CSCvi53407	SSL cipher not inheriting from SSL global settings for peering Services.
CSCvi62624	Alarm details are not visible for few alarms in WCM
CSCvi68396	Alarms are not shown when device change from inactive to active state
CSCvi73822	SSL Accelerated service & Certificate expiry Alarms observed in GUI but not in CLI
CSCvi76910	Older Unique id persists for alarms while downgrade and upgrade of CM
CSCvj10858	Need to remove Failover timeout option from Inlinegroup interface settings for physical devices
CSCvj13242	Connection reset seen for TFO traffic with 750ms latency and 1% drops combination
CSCvj16852	In Device status page, Router alarms count not in sync with Device status & AlarmPanel
CSCvj41888	SIA Invalid Alarm not displaying under "show alarm" CLI
CSCvj42839	Cipher is not inheriting from global settings page while submitting the peering service page.
CSCvj50878	Need to remove Failover timeout option from Inline settings in Network interface page
CSCvj62798	Remote authenticated users - Tacacs+/Radius unable to login via SSH
CSCvj74332	Not able to deploy ISR-WAAS in ISR-4321 router installed with IOS-XE-16.9.x version
CSCvj76737	Custom user is having secure store privileges in device group.
CSCvk20194	SMB AO: Duplicate folder appears after User renames a folder
CSCvk36872	SNMP Asset TAG CLI command failures observed in cms logs
CSCvk44861	TFO Pending connections observed with web traffic via proxy connect
CSCvk62762	SMBAO Memory leaks observed while running soak test with all SMB dialect traffic

Cisco Software Version 6.4.3 Open Caveats

- The following caveats are open in Cisco Software Version 6.4.3. Note that there might be additional open caveats from previous releases that are applicable to this release, unless they are specifically listed as resolved.
- For NFVIS open caveats that affect Cisco WAAS, see the *Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.9.x*.

Caveat ID Number	Description
CSCvh96906	Force device group setting need to be applied multiple time to fix local overide
CSCvi48755	WAN Throughput drop observed in 694,594,SUSE-6k,Centos-6k devices
CSCvj02769	Appnav keeps redirect traffic to waas node (SN) when waas node is in pending state
CSCvj63315	WAAS crashed during large webcast useing Akamai Connect
CSCvj66784	Device unresponsive when user login with fail-over authentication with debug auth user enabled
CSCvj82965	ENCS-F2W:vWAAS-port channel 99% decode test throughput is ~40% less compare with Tahoe port-channel
CSCvj88714	WAAS sends TCP timestamp options in the ACK to server even if the server does not send TS options
CSCvj21179	Unable to configure IP for device in BRIDGE mode
CSCvk11492	Connection Reset seen in ENCS vWAAS instance after clearing DRE cache
CSCvk18039	CSP-W:50% Encode test lot of throughput fluctuation seen and LAN TP ~44% less compare with vWAAS-12K
CSCvk24383	Traffic Server memory dump generated immediately after WAAS startup
CSCvk33903	Traffic stopped optimizing after assigning the IP from on-board to iom interace
CSCvk48179	WAASNET Memory Dump Happens when restarting the waasnet service
CSCvk52145	httpcache process restarts and leaves coredump
CSCvk59179	Azure: vWAAS doesn't forward packet after reboot/clear ARP cache.
CSCvk64584	Memory dump observed in srserverd64 with DC 8541 WAE
CSCvk69680	Unable to reach default gateway while shut/unshut inlinegrp + disable/enable inline mode
CSCvm02178	DLT Memory Dump In WAASNET In Certain Conditions
CSCvm17139	Policy and class-map configuration missed, during continues WAASNET restart.
CSCvm24540	Unexpected system reload observed in ISR-WAAS
CSCvm27998	Ts pending connections observed with dual sided webtraffic via proxy connect
CSCvm31772	MAPI AO shutdown unexpectedly after creating memory dump during load test
CSCvm35205	Overlapping FQDN in HTTP AO Whitelist and SSL Accelerated service cause TFO only connection
CSCvm35640	WAASNet crash is seen after power outage
CSCvm41942	Unexpected SMB restart upon handling rare smbv1 request
CSCvm41943	SMB AO set guest bit in sessionsetup response for signed connection
CSCvm44361	es_ism process memory dump created during overnight web traffic testing
CSCvm45611	waasnet crash at lwssl
CSCvm48362	WAASNet memory dump file generated under certain conditions
CSCvm71236	Domain join status lost while device upgrading to 643

Cisco WAAS Documentation Set

In addition to this document, the WAAS documentation set includes the following publications:

- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Monitoring Guide*
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *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*
- *Installing the Cisco ENCS-INLN-GE-4T (FTW-NIM) in a Cisco ENCS 5400-W Series Device*

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.