Release Note for Cisco Wide Area Application Services Software Version 6.4.5x

August 17, 2020

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:

- 6.4.5a
- 6.4.5

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 Systems, Inc.
www.cisco.com

- Obtaining Documentation and Submitting a Service Request

Cisco Software Version 6.4.5x New and Changed Features

This section contains the following topics:

- Cisco Software Version 6.4.5a New and Changed Features
- Cisco Software Version 6.4.5 New and Changed Features

Cisco Software Version 6.4.5a New and Changed Features

- Cisco WAAS Central Manager Failover and Recovery: If your Primary Cisco WAAS Central Manager becomes inoperable, a Standby Central Manager automatically continues connectivity with Cisco vManage.

Cisco Software Version 6.4.5 New and Changed Features

- Flow sync of passthrough sessions for AppNav XE connections: Configuration support to disable passthrough flow synchronization to other AppNav-XE devices in a cluster has been provided in this release.
- WAAS Central Manager support for revocation and reimport of certificates for vManage Registration.
- WAAS Central Manager support for latest vManage Template status: This template is pushed from vManage to the SDWAN device, whenever a SDWAN AppNav cluster is created, configured or deleted.

Cisco Software Version 6.4.5x Filenames

This section describes the Cisco WAAS Software Version 6.4.5 software image files for use on Cisco WAAS appliances and modules and contains the following topics:

- Cisco WAAS Standard Image Files
- No Payload Encryption Image Files
- Cisco vWAAS Unified OVA Package Formats by Hypervisor

Cisco WAAS Standard Image Files

Cisco WAAS Software Version 6.4.5x includes the following standard primary software image files for use on Cisco WAAS appliances and modules:

- **Cisco_NFVIS_4.1.2-FC5_WAAS-APPLIANCE-6.4.5x-x.iso**: Unified Cisco WAAS image package for ENCS-W-5400 Platform device and for CSP-W-5000 Platform device.
- **waas-universal-6.4.5x.x-k9.tar:** 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-6.4.5x.x-k9.tar**: 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-6.4.5x.x-k9.tar**: Cisco WAAS software recovery CD image.
- **waas-6.4.5x.x-k9.sysimg.tar**: Flash memory recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- **waas-kdump-addon-6.4.5x.*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-6.4.5x.*x*.zip**: Contains the alarm and error message documentation.

No Payload Encryption Image Files

Cisco WAAS Software Version 6.4.3 includes No Payload Encryption (NPE) primary software image files that have the disk encryption feature disabled. These images are suitable for use in countries where disk encryption is not permitted. NPE primary software image files include the following:

- **Cisco_NFVIS_4.1.2-FC5_WAASNPE-APPLIANCE-6.4.5x-x.iso**: Unified Cisco WAAS image package for ENCS-W-5400 Platform device and for CSP-W-5000 Platform device.
- **waas-universal-6.4.5.x-npe-k9.tar**: 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-6.4.5.x-npe-k9.tar**: 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-6.4.5.x-npe-k9.tar**: Cisco WAAS NPE software recovery CD image.
- **waas-6.4.5.x-npe-k9.sysimg.tar**: Flash memory NPE recovery image for 32-bit platforms (all other devices).

Cisco vWAAS Unified OVA Package Formats by Hypervisor

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 6.4.5 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 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	Cisco Unified OVA Filename Format	Supported Cisco vWAAS Models	Supported Cisco vCM Models
VMware ESXi	• Cisco-WAAS-Unified-6.4.5a-b-50.tar • Cisco-WAAS-Unified-6.4.5a-npe-b-50.tar	• 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
	• Cisco-WAAS-Unified-6.4.5-b-75.tar • Cisco-WAAS-Unified-6.4.5-npe-b-75.tar		
Microsoft Hyper-V	• Cisco-HyperV-vWAAS-unified-6.4.5a-b-50.tar • Cisco-HyperV-vWAAS-unified-6.4.5a-b-50-npe.tar	• 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
	• Cisco-HyperV-vWAAS-unified-6.4.5-b-75.tar • Cisco-HyperV-vWAAS-unified-6.4.5-b-75-npe.tar		
KVM CentOS	• Cisco-KVM-vWAAS-Unified-6.4.5a-b-50.tar • Cisco-KVM-vWAAS-Unified-6.4.5a-b-50-npe.tar	• 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
	• Cisco-KVM-vWAAS-Unified-6.4.5-b-75.tar • Cisco-KVM-vWAAS-Unified-6.4.5-b-75-npe.tar		

Hypervisor or Appliance	Cisco Unified OVA Filename Format	Supported Cisco vWAAS Models	Supported Cisco vCM Models
Cisco NFVIS vBranch	• Cisco-KVM-vWAAS-Unified-6.4.5a-b-50.tar • Cisco-KVM-vWAAS-Unified-6.4.5a-b-50-npe.tar	• vWAAS-150 • vWAAS-200 • WAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000 • vWAAS-6000R	• N/A
	• Cisco-KVM-vWAAS-Unified-6.4.5-b-75.tar • Cisco-KVM-vWAAS-Unified-6.4.5-b-75-npe.tar		
Cisco ISR-WAAS	• ISR-WAAS-6.4.5a-50.tar • ISR-WAAS-6.4.5a-50-npe.tar	• vWAAS-200 • WAAS-750 • vWAAS-1300 • vWAAS-2500	• N/A
	• ISR-WAAS-6.4.5-75.tar • ISR-WAAS-6.4.5-75-npe.tar		
Cisco ENCS-W/K9	• Cisco_NFVIS_4.1.2-FC5_WAAS-APPLIANCE-6.4.5a-b50.iso • Cisco_NFVIS_4.1.2-FC5_WAASNPE-APPLIANCE-6.4.5a-b50.iso	• vWAAS-200 • WAAS-750 • vWAAS-1300 • vWAAS-2500 • vWAAS-6000R	• N/A
	• Cisco_NFVIS_4.1.2-FC5_WAAS-APPLIANCE-6.4.5-b75.iso • Cisco_NFVIS_4.1.2-FC5_WAASNPE-APPLIANCE-6.4.5-b75.iso		
CSP-W-5000	• Cisco_NFVIS_4.1.2-FC5_WAAS-APPLIANCE-6.4.5a-b50.iso • Cisco_NFVIS_4.1.2-FC5_WAASNPE-APPLIANCE-6.4.5a-b50.iso	• vWAAS-12000 • vWAAS-50000 • vWAAS-150000	• N/A
	• Cisco_NFVIS_4.1.2-FC5_WAAS-APPLIANCE-6.4.5-b75.iso • Cisco_NFVIS_4.1.2-FC5_WAASNPE-APPLIANCE-6.4.5-b75.iso		

Interoperability and Support

This section contains the following topics:

- Hardware, Client, and Web Browser Support
- Cisco WAAS Version Interoperability
- Cisco WAAS and Cisco vWAAS Interoperability
- Cisco WAAS, ISR and IOS-XE Interoperability
- Cisco AppNav and AppNav-XE Interoperability
- Cisco WAAS, ASR/CSR and IOS-XE Interoperability
- Traffic Interception Interoperability
- NTLM Interoperability
- Citrix ICA Interoperability
- Cisco WAAS Application Accelerators Interoperability with Third-Party Load Balancers
- Cipher Support for SSL Acceleration

Hardware, Client, and Web Browser Support

This section contains the following topics:

- Platforms Supported by Cisco WAAS
- Browsers Supported by Cisco WAAS
- Hypervisors Supported by Cisco vWAAS

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 6.4.5	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 6.4.5	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-W-5400 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 6.4.5 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 (6.4.5), 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 6.4.5 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 6.4.5 is not supported.

Cisco WAAS and Cisco vWAAS Interoperability

This section contains the following topics:

- Cisco ISR-WAAS Models and Supported Cisco ISR Platforms
- Cisco vWAAS Resizing in Cisco WAAS Version 6.4.1 and Later
- Guidelines for Using Cisco vWAAS with Cisco WAAS

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	5.5.7 and later 6.2.1
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	5.5.7 and later
ISR-WAAS-750	2	4 GB	151 GB	ISR-4461	6.4.1b and later
ISR-WAAS-1300	4	6 GB	151 GB	ISR-4431, ISR-4451	5.5.7 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	5.5.7 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 6.4.1 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
- Upgrade and Downgrade Guidelines for Cisco vWAAS in Cisco WAAS

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

Consider the following guidelines for Cisco WAAS, ISR and IOX-XE interoperability:

- The following table shows Cisco WAAS and Cisco IOX-XE versions supported for Cisco ISR platforms:

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, ISR-4461	6.4.5	16.9.5, 16.12.2, 16.12.3, 17.1.1, 17.2.1
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451, ISR-4461	6.4.5a	16.9.5*, 16.12.4, 17.2.1, 17.3.1a

*Suggested version

- 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*.
- We recommend you to use vManage version 20.1 for SDWAN Appnav deployments.

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.
- If you have configured PaasThrough Flow synchronization on an AppNav XE Cluster (AppNavXE device running software version Cisco IOS-XE version 17.2 and later) and want to downgrade the AppNav-XE device to a non-supported version, we recommend that you disable PT Flow synch from the Cisco WAAS Central Manager AppNav-XE cluster first. Otherwise the AppNav-XE cluster gets into the Force Device Group settings mode.
- If vManage/SDWAN devices are registered with WCM and SDWAN clusters are configured in WCM in 6.4.5x, we recommend that you delete the SDWAN AppNav Cluster, de-register the SDWAN device and de-register vManage from the WCM before downgrading it to a version lower than 645.

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, 3.16.1a, 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, 3.16.1a, 3.16.2, 3.17
6.2.3	ASR-1000x/CSR-1000V	• 3.13.8,3.15.2, 3.16.1a, 3.16.2, 3.16.3, 3.16.6, 3.17, 3.17.3, 3.17.4 • 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, 3.16.6, 3.17.4, • 16.4.1, 16.3.3, 16.4.2, 16.3.5, 16.6.1, 16.6.2, 16.7.1
6.4.5, 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
6.4.3d	ASR-1000x/CSR-1000V	16.6.7, 16.9.4, 17.1.1, 16.12.2, 16.3.9
6.4.5	ASR-1000x/CSR-1000V	16.6.7, 16.9.5, 16.12.2, 16.12.3, 17.1.0., 17.2.1,
6.4.5a	ASR-1000x/CSR-1000V	16.6.8, 16.9.5, 16.12.4, 17.2.1,17.3.1a

Traffic Interception Interoperability

This section contains the following topics:

- General Traffic Interception Interoperability
- WCCP Interception Interoperability

General Traffic Interception Interoperability

Cisco WAAS uses the following traffic interception methods: Web Cache Communications Protocol (WCCP), WCCP Version 2, AppNav, Inline, Policy-Based Routing (PBR) and ITD (advanced version of PBR) 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.
- 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 6.4.5 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
```

NTLM Interoperability

Cisco WAAS Versions 5.1 and later do not support Windows domain login authentication using the NTLM protocol. Therefore, upgrading from a Cisco WAAS Version earlier than Version 5.1 with the device configured with Windows domain login authentication using the NTLM protocol is blocked. You must change the Windows domain authentication configuration to use the Kerberos protocol before proceeding with the upgrade.

To change from NTLM to Kerberos Windows domain login authentication, follow these steps:

Step 1 Unconfigure Windows domain login authentication. To do this, use the Cisco WAAS Central Manager **Configure** > **Security** > **AAA** > **Authentication Methods** window.

Step 2 Change the Windows domain configuration setting to use the Kerberos protocol. To do this, use the Cisco WAAS Central Manager **Configure** > **Security** > **Windows Domain** > **Domain Settings** window.

For more information, see “Configuring Windows Domain Server Authentication Settings” in the “Configuring Administrative Login Authentication, Authorization, and Accounting” chapter of the *Cisco Wide Area Application Services Configuration Guide*.

Step 3 Perform the Windows domain join again from the Cisco WAAS Central manager in the **Configure** > **Security** > **Windows Domain** > **Domain Settings** window.

Step 4 Configure Windows domain login authentication from the Cisco WAAS Central manager **Configure** > **Security** > **AAA** > **Authentication** Methods window.

Step 5 Upgrade your device.

Consider the following guidelines for upgrading your device:

- If you are upgrading the Central Manager itself from the GUI and the Windows domain login authentication on the Central Manager is configured to use the NTLM protocol, the upgrade fails with the following error logged in the device log:
  - **Error code107: The software update failed due to unknown reason. Please contact Cisco TAC.**
- To view the device log for the Cisco WAAS Central Manager, choose the Cisco WAAS Central Manager device and then choose **Admin** > **Logs** > **Device Logs**. If you see this error, follow the steps above to change the Cisco WAAS Central Manager device Windows domain login authentication from NTLM to Kerberos.
- If you upgrade the Cisco WAAS Central Manager itself from the Cisco WAAS CLI and the upgrade fails due to NTLM being configured, you will get an appropriate error message. After the Cisco WAAS Central Manager is upgraded to Cisco WAAS Version 5.1, it can detect and display the reason for any upgrade failures for other devices.

Note Cisco WAAS Version 5.1 and later do not support the Kerberos protocol running with a nonstandard port (other than port 88). Upgrading from a Cisco WAAS Version earlier than 5.1 with the device configured with the Kerberos protocol on a nonstandard port is blocked. You must change the Kerberos server on your network to listen on port 88 and change the Kerberos configuration on the device to use port 88. To do this, use the Cisco WAAS Central Manager **Configure** > **Security** > **Windows Domain** > **Domain Settings** window.

If you try to upgrade your device from the Cisco WAAS CLI and the upgrade fails due to NTLM configuration, then the **kerberos_validation.sh** script is installed on your device. This script can be used to verify that your network supports the Kerberos protocol before changing from NTLM to Kerberos. This script is not available if you are using the Cisco WAAS Central Manager to upgrade the device.

To run the **kerberos_validation.sh** script, follow these steps:

Step 1 (Optional) Run the Kerberos validation script command with the **-help** option to display the usage:

```
CM# script execute kerberos validation.sh -help

Help:
This script does basic validation of Kerberos operation, when device is using NTLM
protocol for windows-domain login authentication.
It can be used as a pre-validation before migrating from NTLM to Kerberos authentication
method.

It does following tests:
1. Active Directory reachability test
2. LDAP server and KDC server availability test
3. KDC service functionality test
   For this test to succeed device must have to join the domain before this test, if not
have joined already.
4. Test for time offset between AD and Device (should be < 300s)

Script Usage:
kerberos_validation.sh [windows-domain name]
For example if Device has joined cisco.com then you need to enter: kerberos_validation.sh
cisco.com
```

Step 2 Run the Kerberos validation script to verify that your network supports the Kerberos protocol before migrating from NTLM to Kerberos:

```
CM# script execute kerberos validation.sh windows_domain_name

WARNING: For windows authentication operation in 5.1.1, Device will use service on
following ports.
         Please make sure they are not blocked for outbound traffic.
==========================================================================================
53 UDP/TCP, 88 UDP/TCP, 123 UDP, 135 TCP, 137 UDP, 139 TCP, 389 UDP/TCP, 445 TCP,
464 UDP/TCP, 3268 TCP

Performing following tests on this device.
Test 1: Active Directory reachability test
Test 2: LDAP server and KDC server availability test
Test 3: KDC service functionality test
        For this test to succeed device must have to join the domain before this test, if
not have joined already.
Test 4: Test for time offset between AD and Device (should be < 300s)

Tests are in progress. It may take some time, please wait...
```

```
Test 1: Active Directory reachability test : PASSED
Test 2: LDAP server and KDC server availability test : PASSED
Test 3: KDC service functionality test : PASSED
Test 4: Test for time offset between AD and Device (should be < 300s) : PASSED

Validation completed successfully!
```

Step 3 Change the device Windows domain login authentication from NTLM to Kerberos and upgrade your device, as described in the first procedure in this section.

Citrix ICA Interoperability

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 versions used for test validation for Cisco WAAS Version 6.4.3x and earlier (interoperability for Citrix and Cisco WAAS is unchanged for Cisco WAAS Version 6.4.5x):
  - **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.

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 6.4.5x

This section contains the following topics:

- Guidelines for Upgrading from a Release Version to Cisco WAAS Version 6.4.5x
- Upgrade Support Matrix for Platforms
- Workflow: Upgrading from a Release Version to Cisco WAAS Version 6.4.5x
- Migrating a Cisco WAAS Central Manager from an Unsupported to a Supported Platform
- Migrating a Physical Appliance Being Used as a Primary Cisco WAAS Central Manager to a Cisco vCM
- Ensuring a Successful RAID Pair Rebuild
- Using Previous Client Code

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 6.4.5x

Consider these guidelines to upgrade from a release version to Cisco WAAS Version 6.4.5:

- Upgrading to Cisco WAAS Version 6.4.5 is supported from Cisco WAAS Version 4.2.1 and later. For information on upgrade paths, see Upgrade Support Matrix for Platforms.

- 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 6.4.5x, see Workflow: Upgrading from a Release Version to Cisco WAAS Version 6.4.5x.

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 , “Upgrade Paths to Cisco WAAS Version 6.4.3,”to verify that the target version is supported for your system.

Upgrade Support Matrix for Platforms

Table 8 provides recommendations for Cisco ENCS 5400-W, Cisco CSP 5000-W and other platforms when you upgrade from an earlier Cisco WAAS version to Cisco WAAS 6.4.5a.

Table 8 Upgrade Support Matrix for Platforms

Earlier Cisco WAAS Version	New Cisco WAAS Version	Cisco ENCS 5400-W Cisco CSP 5000-W	Other Supported Platforms
6.4.3d	6.4.5a	Needs fresh installation	Upgrade supported
6.4.3e	6.4.5a	Upgrade supported	Upgrade supported
6.4.5	6.4.5a	Needs fresh installation	Upgrade supported
6.4.5a	6.4.5a	Upgrade supported	Upgrade supported

Upgrade Paths and Considerations for Cisco WAAS Version 6.4.5x

This section contains the following topics:

- Upgrade Paths for Cisco WAAS Version 6.4.5x
- Upgrading from Cisco WAAS Version 5.x and Later to Cisco WAAS Version 6.4.5x
- Upgrading from Cisco WAAS Version 4.2.x to Cisco WAAS Version 6.4.5x

Upgrade Paths for Cisco WAAS Version 6.4.5x

Upgrading to WAAS Version 6.4.5x is supported from WAAS Version 4.2.x and later. 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 , to verify that the target version is supported for your system.

Table 9 Upgrade Paths to Cisco WAAS Version 6.4.5

Current Cisco WAAS Version	Cisco WAAS Central Manager CM Upgrade Path	Cisco WAAS Upgrade Path
5.5.3 and later	• Upgrade directly to 6.4.5	• Upgrade directly to 6.4.5
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 6.4.5	1. Upgrade to 5.5.3, 5.5.5x, or 5.5.7x 2. Upgrade to 6.4.5
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 6.4.5x	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 6.4.5x

Upgrading from Cisco WAAS Version 5.x and Later to Cisco WAAS Version 6.4.5x

Consider the following guidelines for upgrading Cisco WAAS Version 5.x and Later to Cisco WAAS Version 6.4.5x

- **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 NTLM Interoperability. If no application is using the unsupported configurations on the device, then remove the unsupported configurations to upgrade.

- **Cisco WAAS Version 5.2 and Later: 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 6.4.5x: 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 6.4.5x 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 6.4.5x with the Cisco WAAS CLI, a warning on insufficient resources is displayed at the *start* of the upgrade process.
- Cisco WAAS Version 6.4.5x: vCM-100 with RHEL KVM or KVM on CentOS

  If you upgrade to Cisco WAAS Version 6.4.5, or downgrade from Cisco WAAS Version 6.4.5 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:

  a. Power down the Cisco vWAAS using the **virsh destroy** *vmname* command or the virt manager.

  b. 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 6.4.5x

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 .

Workflow: Upgrading from a Release Version to Cisco WAAS Version 6.4.5x

To upgrade from a Release Version to Cisco WAAS Version 6.4.5, complete the tasks listed in Table 10.

Table 10 Workflow: Upgrading from a Release Version to Cisco WAAS Version 6.4.5x

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 6.4.5x, 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 6.4.5x, 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

Before you begin:

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 6.4.5, *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 6.4.5x, 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 6.4.5.

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.

Before upgrading to Cisco WAAS Version 6.4.5x, 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.
- 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.

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 6.4.5 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 6.4.5x 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.
- 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.
- Upgraded the primary Cisco WAAS Central Manager. For more information, see Upgrade Part 3: Upgrade the Primary Cisco WAAS Central Manager.

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 6.4.5x 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 6.4.5x.

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).

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 6.4.5x 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 6.4.5x.

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 6.4.5:

- 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 6.4.5, 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 6.4.5, 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 6.4.5, 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 6.4.5, 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 6.4.5:

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 6.4.5. 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 6.4.5 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 6.4.5x to a Previous Version

This section contains the following topics:

- Downgrade Support Matrix for Platforms
- Downgrading the Cisco WAAS System from Cisco WAAS Version 6.4.5x to a Previous Version
- Downgrading the Cisco WAAS Central Manager from Cisco WAAS Version 6.4.5x to an Earlier Version

Downgrade Support Matrix for Platforms

Table 11provides recommendations for Cisco ENCS 5400-W, Cisco CSP 5000-W and other platforms when you downgrade from Cisco WAAS version 6.4.5a to an earlier Cisco WAAS version.

Table 11 Downgrade Support Matrix for Supported Platforms

Earlier Cisco WAAS Version	New Cisco WAAS Version	Cisco ENCS 5400-W Cisco CSP 5000-W	Other Supported Platforms
6.4.5a	6.4.3d	Needs fresh installation	Downgrade supported
6.4.5a	6.4.3e	Downgrade supported	Downgrade supported
6.4.5a	6.4.5	Needs fresh installation	Downgrade supported
6.4.5a	6.4.5a	Downgrade supported	Downgrade supported

Downgrading the Cisco WAAS System from Cisco WAAS Version 6.4.5x to a Previous Version

This section contains the following topics:

- Downgrade Path Considerations
- Downgrade Component and Data Considerations

Downgrade Path Considerations

- Downgrading from Cisco WAAS Version 6.4.5x 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 a Cisco ENCS-W and Cisco CSP-W platform to a version earlier than Cisco WAAS Version 6.4.1, the Cisco WAAS Central Manager will initiate the downgrade process only for the physical and virtual Cisco WAEs, but not for the Cisco ENCS-W and Cisco CSP-W platform.
- 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 6.4.5 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 6.4.5, 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 6.4.5x to an Earlier Version

This section contains the following topics:

- Cisco WAAS Central Manager Downgrade Path Considerations
- Cisco WAAS Central Manager Downgrade Procedure Considerations
- Procedure for Downgrading the Cisco WAAS Central Manager to a Previous Version

Cisco WAAS Central Manager Downgrade Path Considerations

- Downgrading from Cisco WAAS Version 6.4.5 Cisco WAAS Central Manager directly to a version earlier than Cisco WAAS Version 5.5.3 is blocked.
- If the Cisco WAAS Version 6.4.5 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 6.4.5 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 Manager 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
- Device Group Default Settings
- CIFS Support of FAT32 File Servers
- Using the HTTP Accelerator with the Cisco ASR 1000 Series Router and WCCP

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 6.4.5, 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 6.4.5a Resolved Caveats

The following caveats, impacting earlier software versions of Cisco WAAS, were resolved in Cisco Software Version 6.4.5a.

Caveat ID Number	Description
CSCvt67356	After Primary & secondary CM fail over, SDWAN AppNav configs removed

Cisco Software Version 6.4.5a Open Caveats

The following caveats are open in Cisco Software Version 6.4.5a. 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
CSCvs74062	AppNav Policy Pass through data mismatches in AppNav report pass through reasons chart
CSCvs88120	SDWAN Support: SN movement between SNGs Fails
CSCvu45497	Apache HTTP server multiple vulnerabilities CVE-2020-1934 CVE-2020-1927
CSCvu46011	SDWAN AppNav Report shows double the actual data after PCM/SCM fail over

Cisco Software Version 6.4.5 Open Caveats

The following caveats are open in Cisco Software Version 6.4.5. 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 3.12.x*.

Caveat ID Number	Description
CSCvk39673	Apache httpd server upgrade to 2.4.x version in WAAS
CSCvs41538	Resource reservation failed for proxy connect connections
CSCvs58970	Multiple times WAASNET process abnormal restart
CSCvs67178	Slow upgrade WCM with many ssl accelerated services
CSCvs76822	mingetty process constantly restarting
CSCvs77728	syslog is flooding with Emergency Thaw messages
CSCvt07671	DFT memory dump occurred in WAASNET

Caveat ID Number	Description
CSCvt08991	syslog rate-limit does not work well
CSCvt11217	CM:Latest raised alarm not cleared from DB until new alarm raised
CSCvt37613	MAPI AO is not optimizing few haader pattern of MAPI over HTTPS traffic.
CSCvt37725	SMB AO restarts when signed session and unsigned anonymous share session established in single flow
CSCvs74062	AppNav Policy Pass through data mismatches in AppNav report pass through reasons chart
CSCvt32855	Invalid extension of vmanage certificate is accepted
CSCvs88120	SDWAN Support: SN movement between SNGs Fails
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
CSCvt65620	In some cases, WAAS device shows cpu utilization exceeded threshold alarm
CSCvt67356	After Primary & secondary CM fail over, SDWAN AppNav configs removed
CSCvt37725	SMB AO restarts when signed session and unsigned anonymous share session established in single flow
CSCvt62215	SSL connections are breaking due to incomplete packet exchange between waas devices

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.

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