Release Note for Cisco Wide Area Application Services Software Version 6.4.1x

August 2, 2019

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

Contents

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

- 6.4.1c
- 6.4.1b
- 6.4.1a
- 6.4.1

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

New and Changed Features

The following sections describe the new and changed features in Software Version 6.4.1x:

Cisco Software Version 6.4.1c New and Changed Features

Cisco WAAS Software Version 6.4.1c includes the following new features and changes:

- Support for Device Alarm Status on the Device Dashboard of the WAAS Central Manager GUI.
- Enhancements to the WAAS Central Manager Alarm panel – You can now sort alarms based on Alarm Raised Time.
- WAAS Central Manager and CLI support to configure pass-through connections that are not optimized by NGSSL accelerators.
- Support for TLSv1.2 - You can additionally configure TLSv1.2 for management service apart from the existing SSLv3.0 and TLSv1.0. We recommend this configuration only if there are no 5.x devices managed by CM in your setup.

Cisco Software Version 6.4.1b New and Changed Features

Cisco WAAS Software Version 6.4.1b includes the following new features and changes:

- **ISR-4461**—ISR-4461 is supported for vWAAS models vWAAS-750, vWAAS-1300, and vWAAS-2500, and supports ISR-WAAS models ISR-WAAS-750, ISR-WAAS-1300, and ISR-WAAS-2500.
- **SUSE Linux**—vWAAS in SUSE Linux is supported for all vWAAS and vCM models that are supported on KVM on CentOS.
- **OpenStack**—vWAAS in OpenStack is supported for all vWAAS and vCM models that are supported on KVM on CentOS.
- **TLS v1.1/v1.2**—Dual-sided Transport Layer Security (TLS) Version 1.1/1.2 is supported for additional communications security.

  In addition to TLS v1.0, the WAAS Central Manager can establish an SSL connection with TLS v1.1 and TLS v1.2 protocol to a Cisco IOS Router (AppNav-XE) for HTTP/S communication.

Cisco Software Version 6.4.1a New and Changed Features

Cisco WAAS Software Version 6.4.1a includes the following new features and changes:

- **vWAAS-150000** – The vWAAS-150000 supports 150,000 connections and is used with the ESXi hypervisor, Version 5.5 or 6.0. The vWAAS-150000 replaces WAVE-8541, which has EOS/EOL dates.

- **vWAAS Resizing** – For vWAAS with WAAS Version 6.4.1a and later, you can optionally increase vCPU and memory to enable vWAAS models to scale to optimized TCP connections for their associated device. For more information, see vWAAS Resizing for WAAS Version 6.4.1a and Later.
- **Satellite Optimization**- From release 6.4.1a, WAAS supports traffic optimization for better throughput in high latency, low bandwidth, satellite networks that are used by WAAS peer devices on the Satellite WAN link.
- **RAID-1 array for ENCS 5400-W Series** (Optional)– For WAAS Release 6.4.1a and later, you can include an optional RAID-1 array and an SSDs (960 GB SSD) for ENCS-5400 Series models ENCS-5406/K9, ENCS-5408/K9, and ENCS-5412/K9.

⚠ **Caution** vWAAS is designed to run in appliance mode or as a Virtualized Network Function (VNF) in three Cisco ENCS 5400-W series models (ENCS 5406-W, ENCS 5408-W, and ENCS 5412-W) and three Cisco PIDs (ENCS 5406-K9, ENCS 5408-K9, and ENCS 5412-K9).

For guaranteed performance, the ENCS 5400 Series, UCS-C Series, UCS-E Series, and ISR configurations listed in the WAAS Sizing Guides and specifically noted in WAAS and vWAAS user guides and WAAS Release Notes are the only devices we recommend for use with vWAAS. Although vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

Cisco Software Version 6.4.1 New and Changed Features

This section contains the following topics:

- vWAAS New and Changed Features
- WAAS New and Changed Features
- Discontinued Features

vWAAS New and Changed Features

Cisco WAAS Software Version 6.4.1 includes the following vWAAS new and changed features:

- ENCS 5400 Series—ENCS 5406-W, ENCS 5408-W, ENCS 5412-W—for WAAS and vWAAS

⚠ **Caution** vWAAS is designed to run in appliance mode or as a Virtualized Network Function (VNF) in three Cisco ENCS 5400-W series models (ENCS 5406-W, ENCS 5408-W, and ENCS 5412-W) and three Cisco PIDs (ENCS 5406-K9, ENCS 5408-K9, and ENCS 5412-K9).

For guaranteed performance, the ENCS 5400 Series, UCS-C Series, UCS-E Series, and ISR configurations listed in the WAAS Sizing Guides and specifically noted in WAAS and vWAAS user guides and WAAS Release Notes are the only devices we recommend for use with vWAAS. Although vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

- RMA Process for Cisco EOS/EOL WAVE devices
- Unified OVA for vWAAS hypervisors—Cisco provides a single, unified OVA for NPE and non-NPE version of WAAS image for all the vWAAS models for that hypervisor.

Note Unified OVA for vWAAS hypervisors requires VMWare vCenter to deploy Unified OVA files. Deployment of Unified OVA files does not work using vSphere client.

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

- vWAAS in Cisco Enterprise Network Functions Virtualization (NFV)—Virtualizes WAN optimization on top of four different host platforms: Cisco UCS C-Series server, Cisco UCS E-Series server, Cisco 4000 series Integrated Services Routers (ISR), or Cisco ENCS 5400 series
- vWAAS with NFVIS on ENCS—Installation procedure for vWAAS with NFVIS on the Cisco ENCS 5400 Series.
- vWAAS with Single-Root I/O Virtualization (SR-IOV)—Enables the vWAAS instance to share the I/O device in a virtualized environment. SR-IOV provides independent memory space, interrupts, and DMA streams for each virtual machine, and allows a device to support multiple virtual functions.

WAAS New and Changed Features

Cisco WAAS Software Version 6.4.1 includes the following WAAS new and changed features:

- SMART-SSL—Encryption service that enables L7 application network services (e.g. ftp, http, dns) to optimize traffic on SSL/TLS encrypted applications. It enables content caching for SSL/TLS applications (http object cache for https traffic) in both single-sided and dual-sided deployment. With the evolution of cloud services, there is a critical need to provide application optimization. Starting with release 6.4.1, SMART-SSL optimization, is enabled using both single-sided and dual-sided mode.
- WAAS Central Manager Monitor API and Enhancements
- SSH management access by default
- AppNav controller— AppNav is a combination of hardware and software solutions that simplifies network integration of WAN optimization. Release 6.4.1 and later ensure porting of AppNav to the WAASNet infrastructure.

Note AppNav Controller functionality was re-introduced to WAAS with WAAS Version 6.4.1. However, configuration of the AppNav Controller function and WAAS node function on the same device is not supported.

For more information on AppNav, see the “Configuring AppNav” chapter of the *Cisco Wide Area Application Services Configuration Guide*.

- SMB object cache enhancements—Using the existing interfaces, OCLite enables faster cache lookups using in-memory directory instead of using external databases.
- ICA over SOCKS—Support for optimizing ICA traffic redirected over SOCKS proxy servers.
- Image Signing capability- For WAAS Version 6.4.1 and later, the WAAS image files are digitally signed to assure code authenticity and integrity. After downloading the image, you need to verify the image before loading it onto your devices. To facilitate this, each WAAS image is posted in TAR file format. For example, the waas-universal-6.4.1 image TAR file contains the following files.
  - cisco_x509_verify_release.py

- WAAS-CCO_RELEASE.cer
- waas-universal-6.4.1.36-k9.bin
- waas-universal-6.4.1.36-k9.bin.signature
- waas-universal-6.4.1.36-k9.bin_README

Details of the verification process are provided in the waas-universal-6.4.1.36-k9.bin_README file. After extracting the TAR file, follow the instruction provided in waas-universal-6.4.1.36-k9.bin_README to verify the image authenticity before loading the image on to the device.

Discontinued Features

Cisco WAAS Software Version 6.4.1 includes the following discontinued features:

- Network Analysis Module (NAM) support discontinued—For WAAS Version 6.4.1 and later, NAM is no longer supported in WAAS.
- SM-SRE network module support discontinued—For WAAS Version 6.4.1 and later, the SM-SRE network module is no longer supported for WAAS.

For a list of CLI commands added to or changed for WAAS Version 6.4.1x, see Cisco Software Version 6.4.1x Command Changes.

Cisco Software Version 6.4.1x Filenames

This section describes the Cisco WAAS Software Version 6.4.1x software image files for use on Cisco WAAS appliances and modules and contains the following topics:

- Standard Image Files
- No Payload Encryption Image Files
- For a list of vWAAS image files, see the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

Standard Image Files

Cisco WAAS Software Version 6.4.1x includes the following standard primary software image files for use on Cisco WAAS appliances and modules:

- Cisco_NFVIS_3.7.1-160_WAAS-6.4.1-b36-20180117_020900.iso.tar—Unified WAAS image package for ENCS Platform device.
- waas-universal-6.4.1x.*x*-k9.bin—Universal software image that includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade a device operating in any device mode.
- waas-accelerator-6.4.1x.*x*-k9.bin—Application Accelerator software image that includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator device. This software image file is significantly smaller than the Universal image. Kdump analysis functionality is not included in the Accelerator-only image.

The following additional files are also included:

- waas-rescue-cdrom-6.4.1x.x-k9.iso—Cisco WAAS software recovery CD image.
- waas-x86_64-6.4.1x.x-k9.sysimg—Flash memory recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).

- waas-6.4.1x.*x*-k9.sysimg—Flash memory recovery image for 32-bit platforms (all other devices).
- waas-kdump-6.4.1x.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-6.4.1x.x.zip—Contains the alarm and error message documentation.

No Payload Encryption Image Files

Cisco WAAS Software Version 6.4.1x includes No Payload Encryption (NPE) primary software image files that have the disk encryption feature disabled. These images are suitable for use in countries where disk encryption is not permitted. NPE primary software image files include the following:

- Cisco_NFVIS_3.7.1-160_WAASNPE-6.4.1-b36-20180117_022026.iso.tar—Unified WAAS NPE image package for ENCS Platform devices.
- waas-universal-6.4.1x.*x*-npe-k9.bin—Universal NPE software image that includes Central Manager and Application Accelerator functionality. You can use this type of software file to upgrade a device operating in any device mode.
- waas-accelerator-6.4.1x.*x*-npe-k9.bin—Application Accelerator NPE software image that includes Application Accelerator functionality only. You can use this type of software file to upgrade only an Application Accelerator device. This software image file is significantly smaller than the Universal image. Kdump analysis functionality is not included in the Accelerator-only image.

The following additional files are also included:

- waas-rescue-cdrom-6.4.1x.*x*-npe-k9.iso—Cisco WAAS NPE software recovery CD image.
- waas-x86_64-6.4.1x.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 64-bit platforms (WAVE-294/594/694/7541/7571/8541).
- waas-6.4.1x.*x*-npe-k9.sysimg—Flash memory NPE recovery image for 32-bit platforms (all other devices).
- waas-alarm-error-books-6.4.1x.*x*-npe.zip—Contains the NPE alarm and error message documentation.

Cisco WAAS Appliance System Firmware Update

On Cisco Wide Area Application Engine (WAE) and Cisco Wide Area Application Virtualization Engine (WAVE) appliances, we recommend that you update the following three types of system firmware to the latest version to best support new Cisco WAAS features.

This section contains the following topics:

- BIOS Update
- BMC Firmware Update
- RAID Controller Firmware Update

BIOS Update

The latest BIOS is required for AppNav operation with a Cisco AppNav Controller Interface Module in WAVE-594/694/7541/7571/8541 models. WAVE-294 models may also need a BIOS update.

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

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

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

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

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

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

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

Use the appropriate BIOS installer file for your appliance model.

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

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

BMC Firmware Update

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

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

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

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

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

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

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

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

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

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

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

RAID Controller Firmware Update

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

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

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

Interoperability and Support

This section contains the following topics:

Hardware, Client, and Web Browser Support

This section contains the following topics:

Platforms Supported by WAAS

The Cisco WAAS software operates on these hardware platforms:

- ENCS 5406-W, ENCS 5408-W, ENCS-5412-W

Caution vWAAS is designed to run in appliance mode or as a Virtualized Network Function (VNF) in three Cisco ENCS 5400-W series models (ENCS 5406-W, ENCS 5408-W, and ENCS 5412-W) and three Cisco PIDs (ENCS 5406-K9, ENCS 5408-K9, and ENCS 5412-K9).

For guaranteed performance, the ENCS 5400 Series, UCS-C Series, UCS-E Series, and ISR configurations listed in the WAAS Sizing Guides and specifically noted in WAAS and vWAAS user guides and WAAS Release Notes are the only devices we recommend for use with vWAAS. Although vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

- WAVE-294, 594, 694, 7541, 7571, 8541
- ISR-WAAS-200, 750, 1300, 2500
- vWAAS-150, 200, 750, 1300, 2500, 6000, 12000, 50000 on ESXi. For information on minimum ESXi version supported for each vWAAS model, see the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.

- vWAAS-150, vWAAS-200, 750, 1300, 2500, 6000, 12000, 50000 on Microsoft Hyper-V. For information on the version of Windows supported for each vWAAS model on Microsoft Hyper-V, see the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.
- For WAAS Version 6.2.1 and later, vWAAS is supported on RHEL KVM. For WAAS Version 6.4.1x and later, vWAAS is supported on KVM on CentOS and Microsoft Azure.

  For more information on vWAAS for RHEL KVM, KVM on CentOS, and vWAAS on Microsoft Azure, see the *Cisco Virtual Wide Area Application Services Installation and Configuration Guide*.
- Additionally, Cisco 880 Series, 890 Series, and ISR G2 routers running Cisco WAAS Express are supported on the branch side (Cisco WAAS Version 5.0.x or later is required on the data center side).

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

Browsers Supported by WAAS

The Cisco WAAS Central Manager GUI requires Internet Explorer Version 11, Windows Version 7 or later, Firefox Version 4 or later, Chrome Version 10 or later, or Safari version 5.x (only on Apple OS X) and the Adobe Flash Player browser plug-in.

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

- For WAAS version 5.4.1 and later, you are no longer prompted to install the Google Frame plug-in when you access the Central Manager GUI using Internet Explorer. However, if Google Frame plug-in has already been installed earlier, IE will continue using it.
- When using Internet Explorer, ensure that the **Tools** > **Internet Options** > **Advanced tab** > **Do not save encrypted pages to disk** check box (under Security) is checked. If this box is unchecked, some charts will not display.

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

Cisco WAAS Version Interoperability

Consider the following guidelines when operating a Cisco WAAS network that mixes Software Version 6.4.1x devices with devices running earlier software versions:

- **Cisco WAAS CM interoperability**:

  In a mixed version Cisco WAAS network, the Central Manager must be running the highest version of the Cisco WAAS software, and associated Cisco WAAS devices must be running Version 5.1.x or later.

- **Cisco WAAS system interoperability**:

  Cisco WAAS Version 6.4.1x is not supported running in a mixed version Cisco WAAS network in which any Cisco WAAS device is running a software version earlier than Version 5.1.x. Directly upgrading a device from a version earlier than Version 5.5.3 to 6.4.1x is not supported.

Cisco WAAS and vWAAS Interoperability

This section contains the following topics:

- ISR-WAAS Models and Supported ISR Platforms
- vWAAS Models: CPUs, Memory and Disk Storage
- vWAAS Resizing for WAAS Version 6.4.1a and Later
- Guidelines for Using Cisco vWAAS with Cisco WAAS

ISR-WAAS Models and Supported ISR Platforms

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

ISR Model	CPUs	Memory	Disk Storage	ISR Platform Supported	WAAS Version Supported
ISR-WAAS-200	1	3 GB	151 GB	ISR-4321	5.2.1 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	5.2.1 and later
ISR-WAAS-750	4	6 GB	151 GB	ISR-4461	6.4.1b and later
ISR-WAAS-1300	4	6 GB	151 GB	ISR-4431, ISR-4451	5.2.1 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	5.2.1 and later
ISR-WAAS-2500	6	8 GB	338 GB	ISR-4461	6.4.1b and later

Operating Guidelines for 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.

vWAAS Models: CPUs, Memory and Disk Storage

Table 2 vWAAS Models: CPUs, Memory and Disk Storage

vWAAS Model	CPUs	Memory	Disk Storage
vWAAS-150 (for WAAS Version 6.x)	1	3 GB	160 GB
vWAAS-200 (for WAAS Version 5.x through 6.2.1)	1	3 GB	260 GB
vWAAS-200 (for WAAS Version 6.2.3x and 6.4.1)	1	4 GB	260 GB
vWAAS-750	2	4 GB	500 GB
vWAAS-1300	2	6 GB	600 GB
vWAAS-2500	4	8 GB	750 GB
vWAAS-6000	4	11 GB	900 GB
vWAAS-6000-R	4	11 GB	875 GB
vWAAS-12000	4	12 GB	750 GB
vWAAS-50000	8	48 GB	1500 GB

vWAAS Resizing for WAAS Version 6.4.1a and Later

vWAAS for WAAS Version 6.4.1a requires additional resources, so we highly recommend that you resize CPU and memory resources, as shown in Table 3. Resizing vWAAS on the recommended platforms enables vWAAS to scale to optimized TCP connections for the associated device, and to reduce CPU and RAM utilization.

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

For vWAAS for WAAS Version 6.4.1b, you cannot deploy vWAAS-12000 or vWAAS-50000 in Microsoft Hyper-V with the original resources. For a successful deployment of vWAAS 12000 or vWAAS-50000 in Microsoft Hyper-V with original resources, do a new deployment with WAAS Version 6.4.1 or earlier, and then perform the bin upgrade to WAAS Version 6.4.1b.

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

Note For optimum performance, we recommend you use the SSD disk with the UCS models listed in Table 3.

Table 3 Resized vWAAS CPU and Memory Specifications for WAAS Version 6.4.1a and Later

vWAAS Model	Old CPU	Resized CPU	Tested CPU Clock Speed	Old Memory	Resized Memory	Minimum Recommended Platform
vWAAS-150	1 CPU	2 CPUs	1.7 GHz	3 GB	4 GB	UCS-E140N-M2
vWAAS-200	1 CPU	2 CPUs	1.8 GHz	3 GB	4 GB	UCS-E140S-M2
vWAAS-750	2 CPUs	4 CPUs	1.8 GHz	4 GB	8 GB	UCS-E140S-M2
vWAAS-1300	2 CPUs	4 CPUs	1.9 GHz	6 GB	12 GB	UCS-E160S-M3
vWAAS-2500	4 CPUs	6 CPUs	1.9 GHz	8 GB	16 GB	UCS-E160S-M3
vWAAS-6000	4 CPUs	8 CPUs	2.0 GHz	11 GB	24 GB	UCS-E180D-M3
vWAAS-6000R	4 CPUs	8 CPUs	2.0 GHz	11 GB	24 GB	UCS-E180D-M3
vWAAS-12000	4 CPUs	12 CPUs	2.6 GHz	12 GB	48 GB	UCS-C220 or UCS-C240
vWAAS-50000	8 CPUs	16 CPUs	2.6 GHz	48 GB	72 GB	UCS-C220 or UCS-C240

Guidelines for Using Cisco vWAAS with Cisco WAAS

This section contains the following topics:

- Operating Guidelines for vWAAS with WAAS
- Upgrade and Downgrade Guidelines for vWAAS with WAAS

Operating Guidelines for vWAAS with WAAS

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

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

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

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

Caution vWAAS is designed to run in appliance mode or as a Virtualized Network Function (VNF) in three Cisco ENCS 5400-W series models (ENCS 5406-W, ENCS 5408-W, and ENCS 5412-W) and three Cisco PIDs (ENCS 5406-K9, ENCS 5408-K9, and ENCS 5412-K9).

For guaranteed performance, the ENCS 5400 Series, UCS-C Series, UCS-E Series, and ISR configurations listed in the WAAS Sizing Guides and specifically noted in WAAS and vWAAS user guides and WAAS Release Notes are the only devices we recommend for use with vWAAS. Although vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

Upgrade and Downgrade Guidelines for vWAAS with 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 UCS-E firmware (Version 3.1.2), available on the Cisco Download Software Page for UCS E-Series Software, UCS E160S M3 Software.
  - Verify that you have installed the critical Windows Server updates, available on the Microsoft Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update Rollup page. You can also obtain the standalone update package through the Microsoft Download Center by searching for **KB2887595**.

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

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

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

  a. Power down the vWAAS.

  b. From the VMware vCenter, navigate to **vSphere Client** > **Edit Settings** > **Hardware**.

  c. Choose **SCSI controller 0**.

  d. From the Change Type drop-down list, verify that the SCSI Controller Type is set to **VMware Paravirtual**. If this is not the case, choose **VMware Paravirtual**.

  e. Click **OK**.

  f. Power up the vWAAS, with WAAS Version 6.1.x or later.

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

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

When you upgrade to WAAS Version 6.4.1x from an earlier version, or downgrade from WAAS Version 6.4.1x to an earlier version, and use either the **restore factory-default** command or the **restore factory-default preserve basic-config** command, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

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

To resolve this situation, follow these steps:

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

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

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

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

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

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

Cisco WAAS, ISR and IOS-XE Interoperability

This section contains the following topics:

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

Cisco WAAS, ISR and IOS-XE Interoperability.

Table 4 Cisco WAAS, ISR and IOS-XE Interoperability

ISR-Platform	WAAS Version Supported	IOS-XE Version Supported
ISR-4461	• 6.4.1b and later	• 16.9.1 and later
ISR-4451	• 5.2.1 and later • 6.1.1 and later	• 3.10 and later • 16.3.1 and later
ISR-4431, 4351, 4331	• 5.4.1 and later • 6.1.1 and later	• 3.13 and later • 16.3.1 and later
ISR-4321 with 4 GB memory	• 6.2.3 and later	• 16.3.1 and later
ISR-4321 with 3 GB memory	• 5.4.1 and later • 6.2.1	• 3.13 and later • 16.3.1 and later

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

- ISR-4321-B/K9 is not supported for ISR-WAAS installation.

- **Activating ISR-WAAS after formatting the Cisco 4000 Series ISR-router bootflash:**

  After you format the Cisco 4000 Series ISR-router bootflash, you must reload the router to ensure a successful activation of ISR-WAAS. If you do not reload the ISR router after formatting the bootflash, you will be unable to activate ISR-WAAS. For more information on formatting the Cisco 4000 Series ISR router bootflash, see the *Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco 4000 Series ISRs*.

- **For ISR-4321 with IOS-XE, used with WAAS Version 6.2.3c or 6.4.1:**

  You must complete a new OVA deployment of WAAS version 6.2.3c or 6.4.1 for this configuration to work successfully. This configuration will not automatically work after an upgrade to WAAS Version 6.2.3c or 6.4.1 from WAAS Version 5.x or 6.x.

- **Using the intrusion detection and prevention system Snort with ISR-WAAS and ISR-4000 Series, with a hard disk less than or equal to 200 GB:**

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

- **VRF restriction for VirtualPortGroup31 on ISR-WAAS:**

  When you configure ISR-WAAS with EZConfig—VirtualPortGroup31, the WAAS service/router interface, is automatically created, and you can then add or modify specific parameters for it.

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

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

Cisco AppNav and AppNav-XE Interoperability

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

Note AppNav Controller functionality was re-introduced to WAAS with WAAS Version 6.4.1. However, configuration of the AppNav Controller function and 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 Express devices cannot operate as Cisco WAAS nodes in an AppNav deployment.
- Release 6.4.1 and later ensure porting of AppNav to the WAASNet infrastructure.

Note WAAS Version 6.4.1 and later supports AppNav IOM. However, prior versions of 6.x do not support AppNav IOM.

- All AppNav devices in a single cluster must be of the same exact type. This includes IOS-XE devices, down to memory and ESP configuration.

  - All Cisco ASRs (Aggregation Services Routers) in an AppNav Controller Group need to be the same model, with the same ESP (Embedded Services Processor) rate (in Gbps). For example, in an AppNav Controller Group, you cannot have one ASR-1006 40-Gbps ESP and one ASR-1006 100-Gbps ESP.
  - The same principle is true for using the CSR (Cloud Services Router) 1000V Series or the ISR (Integrated Services Router) 4000 series. For example, you cannot have an ISR-4451 and an ISR-4321 in the same AppNav-XE cluster.
- If you are connecting an AppNav Controller (ANC) to a Catalyst 6500 series switch and you have configured the ANC to use the Web Cache Communication Protocol (WCCP) with the L2 redirect method, do not deploy the ANC on the same subnet as the client computers. This configuration can cause packet loss due to a limitation of the Catalyst 6500 series switch.

Note Although an IOS router can have a dot (".") in the hostname, this special character is not allowed in a WAAS device hostname. If you try to import an AppNav-XE device that has a dot in the hostname, the import will fail and the following error message is displayed: **Registration failed for the device devicename ConstraintException; Invalid AppNav-XE name: X.X since name includes invalid character '.'**.

Cisco WAAS, ASR/CSR and IOS-XE Interoperability

Table 5 Cisco WAAS, ASR/CSR, and IOS-XE Interoperability

WAAS Version	ASR/CSR Series	IOS-XE Version Supported
5.2.1	ASR-1000x/CSR-1000V	3.9
5.3.1, 5.3.3, 5.3.5a	ASR-1000x/CSR-1000V	3.9-3.12
5.3.5f	ASR-1000x/CSR-1000V	3.15.2, 3.16.01a, 3.16.2, 3.17
5.4.x	ASR-1000x/CSR-1000V	3.13
5.5.1	ASR-1000x/CSR-1000V	3.13-3.15
5.5.3	ASR-1000x/CSR-1000V	3.13-3.16
5.5.5x	ASR-1000x/CSR-1000V	3.13-3.17
5.5.7x	ASR-1000x/CSR-1000V	3.12-3.17
6.1.1a, 6.2.1x	ASR-1000x/CSR-1000V	3.15.2, 3.16.01a, 3.16.2, 3.17
6.2.3	ASR-1000x/CSR-1000V	3.13.8,3.15.2, 3.16.01a, 3.16.2, 3.16.3, 3.16.6, 3.17, 3.17.03, 3.17.04, 16.3.4, 16.3.5, 16.4.2, 16.5.1, 16.5.2, 16.6.1, 16.7.1
6.4.1x	ASR-1000x/CSR-1000V	3.13.8, 3.16.06, 3.17.04, 16.04.01, 16.3.3, 16.4.2, 16.3.5, 16.6.1, 16.6.2, 16.7.1

Cisco WAAS Express Interoperability

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

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

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

- For a Cisco WAAS device running WAAS Version 6.x and a Cisco WAAS Express peer device running Cisco IOS Release 15.6(3)M, 15.6(2)T1 or later, TLS1 is supported, but SSL3 is removed. Before upgrading WAAS Express to one of these IOS releases, configure TLS1 in the WAAS Express Device Group > Peering Service page, and then upgrade the WAAS Express device to the specified IOS release.
- When using a Cisco WAAS device running version 5.x and a Cisco WAAS Express peer device running Cisco IOS Release 15.2(2)T or earlier, connections originating from the Cisco WAAS device and sent to the Cisco WAAS Express peer are passed through instead of being optimized. We recommend upgrading to Cisco WAAS Express in Cisco IOS Release 15.2(3)T or later to take advantage of the latest enhancements.

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

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

Table 6 lists the Cisco WAAS, WAAS Express and IOS Interoperability

Table 6 Cisco WAAS, WAAS Express and IOS Interoperability

WAAS Version	WAAS Express Platform	IOS Version Supported
5.2.1	89x,19xx, 29xx, 39xx	15.2(4)M, 15.3(1)T
5.3.1 5.3.5x 5.4.1 5.5.x 6.1.x 6.2.x 6.4.1	89x,19xx, 29xx, 39xx	15.2(4)M, 15.3(1)T, 15.3(3)M, 15.4(2)T, 15.5(1)T, 15.5(2)T, 15.5(3)M, 15.6(1)T, 15.6(2)T

Note 39xxE series routers do not support WAAS Express.

Traffic Interception Interoperability

This section contains the following topics:

- General Traffic Interception Interoperability
- WCCP 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). For WAAS Version 5.5.1 and earlier, WAAS supports WCCP, AppNav, and vPATH.

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

- ISR-WAAS devices support only the AppNav Controller interception method. For more information on AppNav, see Cisco AppNav and AppNav-XE Interoperability.
- For vWAAS in Azure, the supported traffic interception method is PBR (Police-Based Routing); vWAAS in Azure does not support WCCP or AppNav interception methods.
- Pass-through traffic does not benefit from optimization. For example, SSH port 22 has minimal traffic volume, so would not benefit by optimizing TCP flows.
- If you use Microsoft System Center Configuration Manager with Preboot Execution Environment (SCCM/PXE), we recommend the following configurations for the ports that carry SCCM/PXE traffic: port 80, port 443, and port 445:
  - port 80—Communicates with the distribution point. Configure for **pass-through traffic**.
  - port 443—Communicates with the distribution point. Configure for **pass-through traffic**.
  - port 445—Used for software package distribution data transfer. Configure for **traffic optimization**.

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

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

WCCP Interception Interoperability

Central Managers running Version 6.4.1x can manage WAEs running software Versions 5.x and later. However, we recommend that all WAEs in a given WCCP service group be running the same version.

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

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

Step 1 You must disable WCCP redirection on the Cisco IOS router first. To remove the global WCCP configuration, use the following **no ip wccp** global configuration commands:

```
Router(config)# no ip wccp 61
Router(config)# no ip wccp 62
```

Step 2 Perform the Cisco WAAS software upgrade on all WAEs using the Cisco WAAS Central Manager GUI.

Step 3 Verify that all WAEs have been upgraded in the Devices pane of the Central Manager GUI. Choose **Devices** to view the software version of each WAE.

Step 4 If mask assignment is used for WCCP, ensure that all WAEs in the service group are using the same WCCP mask value.

Step 5 Reenable WCCP redirection on the Cisco IOS routers. To enable WCCP redirection, use the **ip wccp** global configuration commands:

```
Router(config)# ip wccp 61
Router(config)# ip wccp 62
```

NTLM Interoperability

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

Follow these steps to change from NTLM to Kerberos Windows domain login authentication:

Step 1 Unconfigure Windows domain login authentication. You can do this from the Central manager in the **Configure** > **Security** > **AAA** > **Authentication Methods** window.

Step 2 Change the Windows domain configuration setting to use the Kerberos protocol. You can do this from Central manager in the **Configure** > **Security** > **Windows Domain** > **Domain Settings** window. For more information, see “Configuring Windows Domain Server Authentication Settings” in the “Configuring Administrative Login Authentication, Authorization, and Accounting” chapter of the *Cisco Wide Area Application Services Configuration Guide*.

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

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

Step 5 Upgrade your device.

Note If you are upgrading the Central Manager itself from the GUI and the Windows domain login authentication on the Central Manager is configured to use the NTLM protocol, the upgrade fails with the following error logged in the device log:
Error code107: The software update failed due to unknown reason. Please contact Cisco TAC.

To view the device log for the Central Manager, choose the Central Manager device and then choose **Admin > Logs > Device Logs**. If you see this error, follow the steps above to change the Central Manager device Windows domain login authentication from NTLM to Kerberos.

If you upgrade the Central Manager itself from the CLI and the upgrade fails due to NTLM being configured, you will get an appropriate error message. Once the Central Manager is upgraded to Version 5.1, it can detect and display the reason for any upgrade failures for other devices.

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

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

To run the script, follow these steps:

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

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

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

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

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

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

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

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

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

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

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

Validation completed successfully!
```

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

Citrix ICA Interoperability

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

- Adaptive Display: Disabled
- Legacy Graphic Mode: Enabled

WAAS Application Accelerators Interoperability with Third-Party Load Balancers

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

Step 4 Table 7 shows the interoperability between WAAS application accelerators and the F5 load balancer. For more information about WAAS load balancing, see the sections “About Traffic Interception Methods” and “Configuring Policy-Based Routing” 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 WAAS Application Accelerators Interoperability with Load Balancers

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

WAAS Status	Load Balancer Status	Authentication Method	WAAS Application Accelerator Supported/ Not 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 Version 6.4.1x

This section contains the following topics:

- Guidelines for Upgrading from a Release Version to Version 6.4.1x
- Upgrade Paths and Considerations for Version 6.4.1x
- Workflow: Upgrading from a Release Version to Version 6.4.1x
  - Upgrade Part 1: Create a Backup of the Primary WAAS CM Database
  - Upgrade Part 2: Upgrade the Standby WAAS CM
  - Upgrade Part 3: Upgrade the Primary WAAS CM
  - Upgrade Part 4: Upgrade the Branch WAE Devices
  - Upgrade Part 5: Pre-Upgrade Task for the Data Center WAAS Software
  - Upgrade Part 6: Upgrade Each Data Center WAE
  - Upgrade Part 7: WCCP and Migration Processes
  - Upgrade Part 8: Post-Upgrade Tasks
- Migrating a WAAS CM from an Unsupported to a Supported Platform
- Migrating a Physical Appliance Being Used as a WAAS CM to a vCM
- Ensuring a Successful RAID Pair Rebuild

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

Guidelines for Upgrading from a Release Version to Version 6.4.1x

Consider these guidelines to upgrade from a release version to WAAS Version 6.4.1x:

- Upgrading to WAAS Version 6.4.1x is supported from WAAS Version 4.2.1 and later. For information on upgrade paths, see Upgrade Paths and Considerations for Version 6.4.1x.
- To take advantage of new features and bug fixes, we recommend that you upgrade your entire deployment to the latest version. For an overview of the upgrade process from a release version to Version 6.4.1x, see Workflow: Upgrading from a Release Version to Version 6.4.1x.

Note When you perform a software upgrade via the WAAS Central Manager, there is only a limited system check to verify the support of the target WAAS version. To ensure that you have a successful WAAS upgrade, use Table 8, "Upgrade Paths to WAAS Version 6.4.1x,"to verify that the target version is supported for your system.

Upgrade Paths and Considerations for Version 6.4.1x

This section contains the following topics:

- Upgrade Paths for WAAS Version 6.4.1x
- Upgrading from Cisco WAAS Version 5.x and Later to Version 6.4.1x
- Upgrading from Cisco WAAS Version 4.2.x to Version 6.4.1x

Upgrade Paths for WAAS Version 6.4.1x

Upgrading to WAAS Version 6.4.1x is supported from WAAS Version 4.2.x and later. Table 8 shows the upgrade path for each of these versions.

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

Table 8 Upgrade Paths to WAAS Version 6.4.1x

Current WAAS Version	WAAS CM Upgrade Path	WAAS Upgrade Path
5.5.3 and later	• Upgrade directly to 6.4.1x	• Upgrade directly to 6.4.1x
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 6.4.1x	1. Upgrade to 5.5.3, 5.5.5x, or 5.5.7x 2. Upgrade to 6.4.1x
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 6.4.1x	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 6.4.1x

Upgrading from Cisco WAAS Version 5.x and Later to Version 6.4.1x

This section contains the following topics:

- WAAS Version 5.1 and Later: NTLM
- WAAS Version 5.2 and Later: Usernames
- WAAS Version 5.3 and Later: Name and Description Fields
- WAAS Version 6.4.1x: vWAAS
- WAAS Version 6.4.1x: vCM-100 with RHEL KVM or KVM on CentOS

WAAS Version 5.1 and Later: NTLM

Cisco WAAS Version 5.1 and later do not support NTLM Windows domain authentication or use of a nonstandard port (other than port 88) for Kerberos authentication.

- Upgrading from a Cisco WAAS Version earlier than 5.1 is blocked if either of these configurations are detected. You must change these configurations and ensure that your domain controller is configured for Kerberos authentication before proceeding with the upgrade.
- A script is provided to verify that your network supports Kerberos protocol before migrating from NTLM. For more information, see NTLM Interoperability. If no application is using the unsupported configurations on the device, then remove the unsupported configurations to upgrade.

WAAS Version 5.2 and Later: Usernames

Cisco WAAS Version 5.2 and later restrict the characters used in usernames to letters, numbers, period, hyphen, underscore, and @ sign, and a username must start with a letter or number.

Any username not meeting these guidelines is prevented from logging in. Prior to upgrading the Central Manager to Version 5.2 or later, we recommend that you change any such usernames to valid usernames to allow login.

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

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

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

WAAS Version 5.3 and Later: Name and Description Fields

Cisco WAAS Version 5.3 and later restricts the use of characters in the name and description field to alphanumeric characters, periods (.), hyphens (-), underscores (), and blank spaces when you create custom reports. When you upgrade from Cisco WAAS Version 4.x and you have custom reports that have special characters in the name or description field, Cisco WAAS automatically removes the special characters from the report name and description, and logs the modification in the Centralized Management System (CMS) logs.

WAAS Version 6.4.1x: vWAAS

- When upgrading vWAAS, do not upgrade more than five vWAAS nodes at the same time on a single UCS box. Upgrading more than five vWAAS nodes at the same time may cause the vWAAS devices to go offline and diskless mode.
- vWAAS for WAAS 6.4.1x requires additional resources before upgrading from WAAS 6.2.3d to WAAS 6.4.1x.
  - *Upgrading from the WAAS Central Manager:* If you initiate and complete the upgrade from the WAAS Central Manager without increasing resources for vWAAS, alarms (CPU & RAM) to indicate insufficient resource allocation will be displayed on the 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 WAAS 6.4.1 with the CLI, a warning on insufficient resources is displayed at the *start* of the upgrade process.

WAAS Version 6.4.1x: vCM-100 with RHEL KVM or KVM on CentOS

If you upgrade to WAAS Version 6.4.1x, or downgrade from WAAS Version 6.4.1x to an earlier version, and use a vCM-100 model with the following parameters, the vCM-100 may not come up due to GUID Partition Table (GPT) boot order errors.

- vCM-100 has default memory size of 2 GB
- vCM-100 uses the RHEL KVM or KVM on CentOS hypervisor
- You use either the **restore factory-default** command or the **restore factory-default preserve basic-config** command

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

To resolve this situation, follow these steps:

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

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

Upgrading from Cisco WAAS Version 4.2.x to Version 6.4.1x

When you upgrade from Cisco WAAS Version 4.x, you must reconfigure the custom EPM policy for a device or device group. You must first restore the default policy setting by selecting the **Restore default Optimization Policies** link for the device group in the Modifying Device Group window and then reconfigure your custom policy rules for the device. For more information on upgrade paths, see Table 8.

Workflow: Upgrading from a Release Version to Version 6.4.1x

To upgrade from a Release Version to Version 6.4.1x, complete the tasks listed in Table 9.

Table 9 Workflow: Upgrading from a Release Version to Version 6.4.1x

Workflow Task	Description
• Upgrade Part 1: Create a Backup of the Primary WAAS CM Database	• *Before you start the upgrade process* from a release version to Version 6.4.1x, create a backup of the primary WAAS CM database and save it to a remote location.
• Upgrade Part 2: Upgrade the Standby WAAS CM	• If your WAAS system has a standby WAAS CM, upgrade the standby WAAS CM *before* you upgrade the primary WAAS CM.

Workflow Task	Description
• Upgrade Part 3: Upgrade the Primary WAAS CM	• Upgrade the primary WAAS CM, including verifying that the new WAAS image is loaded correctly, verifying connectivity between WAAS CM and all WAE devices, and verifying that all WAE devices are online.
• Upgrade Part 4: Upgrade the Branch WAE Devices	• Upgrade the branch WAE devices, including verifying that new WAAS image is loaded correctly, verifying that correct licenses are installed, and saving the new configuration.
• Upgrade Part 5: Pre-Upgrade Task for the Data Center WAAS Software	• Upgrade the data center WAAS software, including upgrading each data center WAE device.
• Upgrade Part 6: Upgrade Each Data Center WAE	• Upgrade each data center 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 WAAS system upgrade to Version 6.4.1x*, perform tasks including clearing your browser cache, verifying licenses, and verifying proper configuration of applications accelerators, policies, and class maps.

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

This section contains the following topics:

- Prerequisite for Primary WAAS CM Database Backup
- Creating a Primary WAAS CM Database Backup

Prerequisite for Primary WAAS CM Database Backup

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

- If you are upgrading your vCM, vWAAS or ISR-WAAS device from an earlier WAAS version to WAAS Version 6.4.1x, *and the /sw and /swstore partition size is less than 2GB*, you must back up the CMS database *before* creating a backup of the primary WAAS CM database, following the instructions described in the Caution note.
- *For devices using WAAS Version 5.x*, the /sw and /swstore partition size is 1GB, so you must back up the CMS database, you must back up the CMS database *before* creating a backup of the primary WAAS CM database, following the instructions described in the Caution note.
- *For devices using WAAS Version 6.x*, the /sw and /swstore partition size is 2GB, so you do not need to create a backup of the CMS database before creating a backup of the primary WAAS CM database.

Caution If you are upgrading your WAAS device from an earlier WAAS version to WAAS Version 6.4.1x, *and the /sw and /swstore partition size is less than 2 GB*, it is crucial that you create a backup of the WAAS CM database and save it to an external file (FTP/SFTP) *before* you upgrade to WAAS Version 6.4.1x.

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

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

Creating a Primary WAAS CM Database Backup

Before upgrading to WAAS Version 6.4.1x, follow these steps to create a backup of the WAAS CM database:

Step 1 Use Telnet or SSH to access the primary WAAS CM IP address.

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

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

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

```
creating backup file with label 'backup'
```

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

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

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

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

Upgrade Part 2: Upgrade the Standby WAAS CM

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

Step 1 Use Telnet or SSH to access the standby WAAS CM IP address:

Step 2 Copy the new software image to the standby WAAS CM with the WAAS CLI **copy ftp** command.

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

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

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

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

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

Step 6 Wait at least five minutes.

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

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

Upgrade Part 3: Upgrade the Primary WAAS CM

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

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

Follow these steps to upgrade the primary WAAS CM.

Step 1 Use Telnet or SSH to access the primary WAAS CM IP address:

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

From the WAAS CM:

a. In the Standby WAAS CM, 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.

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 3 Copy the new Version 6.4.1x software image to the primary WAAS CM, using the **copy ftp** command:

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

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

Step 4 Reload the primary WAAS CM, using the **reload** command

Step 5 Verify that the new Version 6.4.1x image is loaded correctly, using the **show version** command.

Step 6 To confirm connectivity, ping the standby WAAS CM (if present in your WAAS system) and branch WAE devices.

Step 7 Confirm that the CMS services are running, using the **show cms info** command.

Step 8 Choose **Devices** > **All Devices** and verify that all WAE devices are online.

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

Upgrade Part 4: Upgrade the Branch WAE Devices

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

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

Follow these steps to upgrade the branch WAE devices.

Step 1 Access the primary WAAS CM GUI:

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

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

Step 3 Resolve any alarm conditions that may exist.

Step 4 Copy the new software image to the branch WAE, either from the WAAS CM or the CLI.

From the WAAS CM:

a. In the branch 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 5 Reload the WAE using the **reload** command.

Step 6 Verify that the new Version 6.4.1x 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 WAAS CM, choose **Devices** > *branchWAE*, to verify that the WAE device is online and has a *green* status.

Step 11 Verify the following WAE device functionalities:

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 WAE devices within the active WAAS network are now upgraded to the current WAAS Version 6.4.1x.

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

Follow these steps to upgrade the data center WAAS software.

Step 1 Access the primary WAAS CM GUI:

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

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

Step 3 Resolve any alarm conditions that may exist.

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

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

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

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

Upgrade Part 6: Upgrade Each Data Center WAE

Follow these steps to upgrade each data center WAE.

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

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

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

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

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

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

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

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

Step 4 Upgrade the data center WAE software:

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

From the WAAS CM:

a. In the data center 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 WAE using the **reload** command.

Step 7 Verify that the new Version 6.4.1x software image has installed correctly, using the **show version** command.

Step 8 Verify that WCCP is disabled, using the **show wccp status** command.

Step 9 Save the changed configuration, using the **copy running-config startup-config** command.

Step 10 From the primary WAAS CM, choose **Devices** > *branchWAE*, to verify that the WAE device is online and has a *green* status.

Step 11 (Optional) Enable WCCP on all intercepting routers or switches in the list, if you have used Step 2.

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 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 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 optmized, 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 WAE within the active WAAS network is now upgraded to the current WAAS Version 6.4.1x.

Upgrade Part 7: WCCP and Migration Processes

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

Upgrade Part 8: Post-Upgrade Tasks

Perform the following tasks after you have completed the upgrade to WAAS Version 6.4.1x:

- After upgrading a Central Manager, you must clear your browser cache, close the browser, and restart the browser before reconnecting to the Central Manager.
- After upgrading application accelerator WAEs, verify that the proper licenses are installed by using the **show license** EXEC command. The Transport license is enabled by default. If any of the application accelerators were enabled on the device before the upgrade, you should enable the Enterprise license. Configure any additional licenses as needed by using the **license add** EXEC command. For more information on licenses, see the “Managing Software Licenses” section in the *Cisco Wide Area Application Services Configuration Guide*.
- After upgrading application accelerator WAEs, verify that the proper application accelerators, policies, and class maps are configured. For more information on configuring accelerators, policies, and class maps, see the “Configuring Application Acceleration” chapter in the *Cisco Wide Area Application Services Configuration Guide*.
- If you use the setup utility for basic configuration after upgrading to 6.4.1x, WCCP router list 7 is used. Because the setup utility is designed for use on new installations, any existing configuration for WCCP router list 7 is replaced with the new configuration.
- If you have two Central Managers that have secure store enabled and you have switched primary and standby roles between the two Central Managers, before upgrading the Central Managers to Version 6.4.1x, you must reenter all passwords in the primary Central Manager GUI. The passwords that need to be reentered include user passwords. If you do not reenter the passwords, after upgrading to Version 6.4.1x, the Central Manager fails to send configuration updates to WAEs and the standby Central Manager until after the passwords are reentered.
- If you use the setup utility for basic configuration after upgrading to 6.4.1x, WCCP router list 7 is used. Because the setup utility is designed for use on new installations, any existing configuration for WCCP router list 7 is replaced with the new configuration.

Migrating a WAAS CM from an Unsupported to a Supported Platform

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

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

Follow these steps to migrate a primary WAAS CM from an unsupported platform to a platform that is supported for WAAS Version 6.4.1x:

Step 1 From the primary Central Manager CLI, create a database backup by using the **cms database backup** EXEC command. Move the backup file to a separate device by using the **copy disk ftp** command.

```
CM# cms database backup
Creating database backup file backup/cms-db-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 Central Manager.

```
CM# show running-config interface
primary-interface GigabitEthernet 1/0
!
interface GigabitEthernet 1/0
 ip address 10.10.10.25 255.255.255.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
```

Step 3 Shut down all the interfaces on the primary Central Manager.

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

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

Step 5 Configure the new Central Manager with the same IP address and netmask as the old Central Manager. You can do this in the setup utility or by using the **interface** global configuration command.

```
newCM# configure
newCM(config)# interface GigabitEthernet 1/0 ip address 10.10.10.25 255.255.255.0
```

Step 6 Copy the backup file created in Step 1 from the FTP server to the new Central Manager.

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

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

```
newCM# cms database restore backup/cms-db-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 Central Manager GUI is accessible and all Cisco WAAS devices are shown in an online state in the Devices window.

Step 10 (Optional) If you have a standby Central Manager that is running on unsupported hardware and is registered to the primary Central Manager, deregister the standby Central Manager.

```
standbyCM# cms deregister
```

Step 11 Upgrade the primary Central Manager to Cisco WAAS Version 6.4.1x. You can use the Central Manager Software Update window or the **copy ftp install** command.

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

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

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

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

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

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

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

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

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

Step 3 Ensure that the Primary CM and Standby CM updates are working.

Step 4 Switch over CM roles so that vCM works as Primary CM. For more information, see the “Converting a Standby Central Manager to a Primary Central Manager” section of the *Cisco Wide Area Application Services Configuration Guide*.

Ensuring a Successful RAID Pair Rebuild

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

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

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

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

- The device is offline in the Central Manager GUI.
- CMS cannot be loaded.
- Error messages say that the file system is read-only.
- The syslog contains errors such as “Aborting journal on device md2,” “Journal commit I/O error,” “Journal has aborted,” or “ext3_readdir: bad entry in directory.”
- Other unusual behaviors occur that are related to disk operations or the inability to perform them.

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

Downgrading from Version 6.4.1x to a Previous Version

This section contains the following topics:

- Downgrading the WAAS System from Version 6.4.1x to a Previous Version
- Downgrading the WAAS CM from Version 6.4.1x to a Previous Version

Downgrading the WAAS System from Version 6.4.1x to a Previous Version

This section contains the following topics:

- Downgrade Path Considerations
- Downgrade Component and Data Considerations

Downgrade Path Considerations

- Downgrading from 6.4.1x is supported to 6.2.1x, 6.1.1a, 6.1.1, 5.5.7, 5.5.5a, 5.5.5 and 5.5.3. Downgrading directly from 6.x to a version earlier than 5.5.3 is not supported.
- On the Cisco 4451-X Integrated Services Router running ISR-WAAS, downgrading to a version earlier than 5.2.1 is not supported.
- On the UCS E-Series Server Module installed in a Cisco ISR G2 Router and running vWAAS, downgrading to a version earlier than 5.1.1 is not supported. On the UCS E-Series Server Module installed in the Cisco 4451-X Integrated Services Router and running vWAAS, downgrading to a version earlier than 5.2.1 is not supported. On other vWAAS devices you cannot downgrade to a version earlier than 4.3.1.
- On WAVE-294/594/8541 models with solid state drives (SSDs) you cannot downgrade to a version earlier than 5.2.1.
- On WAVE-694 model with solid state drives (SSDs), you cannot downgrade to a version earlier than 5.5.1.
- On vCM-500/vCM-1000, you cannot downgrade to a version earlier than 5.5.1.

Downgrade Component and Data Considerations

- For WAAS on devices on the ENCS 5400 Series:
  - You cannot downgrade a WAAS device on ENCS to a version earlier than WAAS Version 6.4.1.

    If you try to downgrade a WAAS device on ENCS to a version earlier than WAAS Version 6.4.1, the WAAS Central Manager displays the following warning message:

    Device Group has unsupported devices *ENCS-DeviceName* to the selected version. The image installation will not be applied on such devices.

    Do you still want to proceed with the downgrade?
  - The 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 WAE, a virtual WAE, and an ENCS platform to a version earlier than WAAS Version 6.4.1, the Central Manager will initiate the downgrade process only for the physical and virtual WAEs, but not for the ENCS 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 5.0 are maintained.

- When downgrading to a version earlier than 4.4.1, the DRE cache is cleared and the DRE caching mode for all application policies is changed to bidirectional (the only available mode prior to 4.4.1). Before downgrading a WAE, we recommend that you use the Central Manager GUI to change all policies that are using the new Unidirectional or Adaptive caching modes to the Bidirectional caching mode.
- Current BMC (Baseboard Management Controller) settings are erased and restored to factory default settings when you downgrade Cisco WAAS to a version earlier than 4.4.5.
- If you have configured disk cache for ISR-WAAS device, downgraded from 6.4.1x to 5.5.3, and then restore rollback to 6.1.1x, you must reload the disk cache configuration for the new configuration to take effect. If you do not perform a reload after the rollback to 6.4.1x, the new configuration will not take effect, and output from the show disks cache-details command will display the error message **Disk cache has been configured. Please reload for the new configuration to take effect**.
- If the vWAAS device is downgraded from vWAAS for WAAS Version 6.4.1a to WAAS Version 6.2.3x, the WAAS alarm filesystem_size_mismatch is displayed; it indicates that the partition was not created as expected. To clear the alarm, use the disk delete-data-partitions command to re-create the DRE partitions.

Downgrading the WAAS CM from Version 6.4.1x to a Previous Version

This section contains the following topics:

- WAAS CM Downgrade Path Considerations
- WAAS CM Downgrade Procedure Considerations
- Procedure for Downgrading the WAAS CM to a Previous Version

WAAS CM Downgrade Path Considerations

- Downgrading from 6.4.1x WAAS CM directly to a version earlier than Version 5.5.3 is blocked.
- If the 6.4.1x WAAS CM is downgraded to a version earlier than 5.2.1, it can no longer manage AppNav-XE clusters and devices and all related configuration records are removed.
- When downgrading a 6.4.1x WAAS CM to a version earlier than 4.4.1, and secure store is in auto-passphrase mode, the downgrade is blocked. You must switch to user-passphrase mode before you can downgrade to a software version that does not support auto-passphrase mode.

WAAS CM Downgrade Procedure Considerations

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

    ——Change service IDs back to their default values of 61 and 62.

    ——Change the failure detection timeout back to the default value of 30 seconds.

Note Only these WCCP default values are supported in versions prior to 4.4.1; any other values are lost after the downgrade. If a WAE is registered to a Central Manager, it is configured with the default service IDs of 61 and 62 after it is downgraded and comes back online.

- Each of the following WAAS CM downgrade procedures requires a particular task sequence:
  - If the WAAS CM is downgraded to a version up to 5.2.1 and if the AppNav-XE cluster has more than 32 WAAS nodes: prior to downgrade, we recommend that you reduce the number of WAAS nodes to a maximum of 32 WAAS nodes.
  - When downgrading Cisco WAAS devices, first downgrade application accelerator WAEs, then the standby Central Manager (if you have one), and lastly the primary Central Manager.
- When downgrading an AppNav Controller device to a version earlier than 5.0.1, you must perform the following tasks:
  1. Deregister the device from the WAAS CM.
  2. Change the device mode to application-accelerator.
  3. Downgrade the device.
  4. Re-register the device (or, alternatively, you can reregister the device before downgrading).

  If you do not deregister the device before downgrading, the device goes offline and the device mode is not set correctly. In that case, use the **cms deregister force** EXEC command to deregister the device and then reregister it by using the **cms enable** global configuration command.

  Note All Cisco WAAS nodes in an AppNav deployment must be running Cisco WAAS version 5.0 or later.

Procedure for Downgrading the WAAS CM to a Previous Version

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

Step 1 (Optional) From the Central Manager CLI, create a database backup by using the **cms database backup** EXEC command. Move the backup file to a separate device by using the **copy disk ftp** command.

```
CM# cms database backup
Creating database backup file backup/cms-db-03-18-2016-15-08_5.0.1.0.15.dump
Backup file backup/cms-db-02-18-2016-15-08_5.0.1.0.15 is ready.
Please use `copy' commands to move the backup file to a remote host.
CM# cd /local1/backup
CM# copy disk ftp 10.11.5.5 / 06-28-backup.dump cms-db-03-18-2016-15-08_5.0.1.0.15.dump
```

Step 2 Install the downgrade Cisco WAAS software image by using the **copy ftp install** EXEC command.

```
CM# copy ftp install 10.11.5.5 waas/4.4 waas-universal-4.4.5c.4-k9.bin
```

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

Step 3 Reload the device.

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

Cisco WAE and WAVE Appliance Boot Process

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

Cisco WAE and WAVE appliances may have video connectors that should not be used in a normal operation. The video output is for troubleshooting purposes only during BIOS boot and stops displaying output as soon as the serial port becomes active.

Operating Considerations

This section includes operating considerations that apply to Cisco WAAS Software Version 6.4.1x:

- **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 WAAS Version 6.4.1xx, the Configure > Acceleration > DSCP Marking page is automatically configured for the group, with the default DSCP marking value of copy.

- **Using Autoregistration with Port-Channel and Standby Interfaces**

  Autoregistration is designed to operate on the first network interface and will not work if this interface is part of a port-channel or standby. Do not enable the auto-register global configuration command when the interface is configured as part of a port-channel or standby group.

CIFS Support of FAT32 File Servers

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

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

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

- **Disabling WCCP from the Central Manager**

  If you use the Central Manager to disable WCCP on a Cisco WAAS device, the Central Manager immediately shuts down WCCP and closes any existing connections, ignoring the setting configured by the **wccp shutdown max-wait** global configuration command (however, it warns you). If you want to gracefully shut down WCCP connections, use the **no enable** WCCP configuration command on the Cisco WAAS device.

- **Changing Device Mode To or From Central Manager Mode**

  If you change the device mode to or from Central Manager mode, the DRE cache is erased.

- **TACACS+ Authentication and Default User Roles**

  If you are using TACACS+ authentication, we recommend that you do not assign any roles to the default user ID, which has no roles assigned by default. If you assign any roles to the default user, external users that are authenticated by TACACS+ and who do not have the waas_rbac_groups attribute defined in TACACS+ (meaning they are not assigned to any group) can gain access to all the roles that are assigned to the default user.

- **Internet Explorer Certificate Request**

  If you use Internet Explorer to access the Central Manager GUI Version 4.3.1 or later and Internet Explorer has personal certificates installed, the browser prompts you to choose a certificate from the list of those installed in the personal certificate store. The certificate request occurs to support Cisco WAAS Express registration and is ignored by Internet Explorer if no personal certificates are installed. Click **OK** or **Cancel** in the certificate dialog to continue to the Central Manager login page. To avoid this prompt, remove the installed personal certificates or use a different browser.

- **Default Settings with Mixed Versions**

  If a Central Manager is managing Cisco WAAS devices that have different versions, it is possible that a feature could have different default settings in those different versions. If you use the Central Manager to apply the default setting for a feature to mixed devices in a device group, the default for the Central Manager version is applied to all devices in the group.

Software Version 6.4.1x Resolved and Open Caveats and Command Changes

This section contains the resolved caveats, open caveats, and command changes in Software Version 6.4.1x, fixed and known and contains the following topics:

- Cisco Software Version 6.4.1c Resolved Caveats
- Cisco Software Version 6.4.1c Open Caveats
- Cisco Software Version 6.4.1b Resolved Caveats
- Cisco Software Version 6.4.1b Open Caveats
- Cisco Software Version 6.4.1a Resolved Caveats

- Cisco Software Version 6.4.1a Open Caveats
- Cisco Software Version 6.4.1 Resolved Caveats
- Cisco Software Version 6.4.1 Open Caveats
- Cisco Software Version 6.4.1x Command Changes
- Using Previous Client Code

Cisco Software Version 6.4.1c Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.4.1c.

Caveat ID Number	Description
CSCvf01746	WAAS HTTP AO process httpmuxd consumes more memory causing multiple AO keepalive timeouts
CSCvh07373	Observing more number of PT connections and connections are not scaling while running akc perf test
CSCvh96772	exec_pkt_cap process memory dump file got generated
CSCvi02645	SNMP service restart seen in WAE device in a scenario
CSCvi36270	Connection not hitting correct classifier although correct accelerators are applied
CSCvi74692	WAASNET Process RAM Dump Happens Repeatedly
CSCvi98993	THDL & TH Pending Connection seen in BR SN after high load
CSCvj37681	AppNav Routers Registration failure and offline on CM
CSCvk41395	RPC over HTTPS fails with Appnav-XE interception.
CSCvk41478	SNMPv2 not polling "TfoStats" information after waasnet Memory Dump
CSCvk47607	False alarms reporting on the Central Manager
CSCvk48179	WAASNET Memory Dump Happens when restarting the waasnet service
CSCvk59104	Traffic not seeing in SN after nprm restart in ANC
CSCvk62115	TFO pending connection due to SDH did not propagate FIN
CSCvk62762	SMBAO Memory leaks observed while running soak test with all SMB dialect traffic
CSCvk65184	641b:fresh deployment of vWAAS 12k and 50k with non-resized resources is not successful with Hyper-V
CSCvm52188	Devices are not listed in report central page while generating Device Dashboard (AppNav-XE) report.
CSCvm84282	Session Resumption behavior with Interposer SSL in WAAS may cause problem with SSL traffic
CSCvm50860	WAAS should Pass through connections which are not getting Optimized by NGSSL
CSCvi68416	Cms service failing to start after database restored

Caveat ID Number	Description
CSCvm35205	Overlapping FQDN in HTTPAO Whitelist and SSL Accelerated service cause TFO only connection
CSCvk66495	Closing ICAoverSSL connections after exceeding the ICA session-limit.
CSCvh53271	VWAAS-150K : WAN throughput 12% and LAN throughput 2% less compared with 8541
CSCvm76240	Support for configuring WAAS pass through connections which are not getting Optimized by NGSSL
CSCvf02875	Reducing the memory utilized by ISR-WAAS-200

Cisco Software Version 6.4.1c Open Caveats

The following caveats are open in Software Version 6.4.1c. 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
CSCvf72849	Less Throughput observed with 44xx ISR waas using 16.7.1 image in ISR Router
CSCvh12112	Device-Id & DRE-Peer-ID calculated using the Internal Interface MAC Address on ENCS WAAS
CSCvh63293	IMD goes down after restart and SYSMON errors observed after WAASNET , PMD restart
CSCvh78904	T Pending connections observed with web traffic via proxy
CSCvk32347	Traffic blockhole in only SC/SN combo device with 6.4.1 a image after any waasnet core.
CSCvk52162	waasnet process restarts and leave memory dump
CSCvk53862	Pending connections observed while running webtraffic via dc proxy
CSCvk59131	Many missed NP keepalive logs seen in waasnet logs
CSCvk59179	Azure: vWAAS doesn't forward packet after reboot/clear ARP cache.
CSCvm19178	Alarm Unique ID is resetting for the new alarms
CSCvm27998	Ts pending connections observed with dual sided webtraffic via proxy connect
CSCvm31582	Multiple TFO alarms are displayed in UI for same device
CSCvm44361	es_ism process memory dump created during overnight web traffic testing
CSCvm76487	System Level TCP Summary Report (Traffic Volume and Reduction chart) rarely shows incorrect value
CSCvm80594	Unable to add match conditions for the class-maps in appnav-cluster
CSCvm85913	Duplex errors on interfaces that are shut down
CSCvm93197	Device becoming low on available system memory and swap gets used.
CSCvm99487	SMB connections are reset then pushdown due to key failure

Caveat ID Number	Description
CSCvm99718	exec_show_runni system dump seen in service-node during long duration traffic test
CSCvn00333	%IOSXE-4-PLATFORM: SIP0: kernel: skbuff: bad partial csum: csum=65535/65535 len=80
CSCvn05452	Traffic Drop observed on shutdown of standby primary interface in SE+OE combo
CSCvn06748	ICA memory dump observed during NPRM restart
CSCvn08731	In SE+OE combo,connections are not seen in the SN
CSCvn12138	ISR-WAAS console becomes unresponsive.
CSCvn14320	WAAS product being affected by CVE-2018-15473
CSCvn15406	ICA system/memory dump file seen on the WAAS
CSCvn16168	WAAS does not send Remote Address for TACACS+ Enable Authentication
CSCvn20627	vmtool log directed to limited and temporary storage
CSCvn35355	Traffic blackholed in SE OE Combo when ANC of Combo device1 and SN of combo device 2 is selected
CSCvn11087	Observed system dump during the MAPI performance test in 641c
CSCvn29696	"T" pending connection at SDH segment while Running webtraffic via DC proxy
CSCvi73273	Akamai proxy configuration differs from CM GUI

Cisco Software Version 6.4.1b Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.4.1b.

Caveat ID Number	Description
CSCvk03838	Optimization not working between 623e and other released versions.
CSCvf20884	Tacacs+ command authorization failed for user unknown and keep pushing the config from CM
CSCvi65520	WCM not updating Policy configuration changed under AppNav Cluster
CSCvi79251	WAE device is being deleted after some time from WAAS group in WCM
CSCvh94469	Evaluation of WAAS for OpenSSL CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738
CSCvj74332	Not able to deploy ISR-WAAS in ISR-4321 router installed with IOS-XE-16.9.x version
CSCvh72553	Mark KVM as default hypervisor for virtual WAAS
CSCvi93462	SSL : Handle delays originated due to client side behavior (Proxy Connect)
CSCvi40137	Cisco Wide Area Application Services Software Static SNMP Credentials Vulnerability
CSCvc83974	Akamai process restarts unexpectedly, leaves a dump file

Caveat ID Number	Description
CSCvk45500	ICA accelerator restarts in a rare case
CSCvk50234	ICA vs ICA OVER SSL graph is not populating records in the CM GUI
CSCvi81780	ICA process generated a memory/system dump in CGP reconnect scenario
CSCvj13159	Zero Mac is getting programmed in WAAS when gateway interface is flapped in Apnnav-xe setup
CSCvj26521	Correct AO Plumb / Chaining behavior in WAAS 6.x code
CSCvj73342	Connection broken and download fail for long connection download
CSCvj44598	Webpage fail to open, when HTTPAO is in half close connection state (proxy connect
CSCvi82153	Traffic is Dropped at The SN when cma process is restarted
CSCvi40884	Apache Traffic Server host header and line folding
CSCvi94691	SMBAO memory increasing gradually during high load and pushdown scenarios
CSCvk45904	In some cases, WAASNet Process creates memory dump and impacts traffic
CSCvi17620	Waasnet service restarted while sending single sided https traffic
CSCvj07016	WAASNet process going pending state and not handling traffic in a scenario
CSCvk03700	unknown NTLMVersion from windows client breaks smb communication
CSCvh96699	Unusually large amount of memory Consumed by SMBAO on the DC device longevity test
CSCvi54862	packet capture processing does not stop when the ssh session timeouts
CSCvj97610	The unknown command when interpreted by the WAAS unable to parse the packet
CSCvi40799	Timeout observed at 180 seconds
CSCvi70287	False alarm seen in console and WAE device not optimizing connections in a scenario
CSCvi86162	Error message throwing while adding match condition with same source and destination ip
CSCvj51761	WAASNet service restart with a core file with wn_dft_thread and DP handler
CSCvk07808	Encryption Services Failed to initialized, unable to configure identity for MAPI / SMB

Cisco Software Version 6.4.1b Open Caveats

The following caveats are open in Software Version 6.4.1b. 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
CSCvk59104	Traffic not seeing in SN after nprm restart in ANC
CSCvk32347	Traffic blockhole in only SC/SN combo device with 6.4.1 a image after any waasnet core.
CSCvk59179	Azure: vWAAS doesn't forward packet after reboot/clear ARP cache.
CSCvj97528	Unexpected reload of NSCD leads to Preposition failure
CSCvj13488	TLS 1.1/1.2 support for CM to Router communication after router registration
CSCvk47607	False alarms reporting on the Central Manager
CSCvj37681	AppNav Routers are going to offline state in WAAS Central Manager after registration
CSCvk52145	httpcache process restarts and leaves coredump
CSCvh96906	Force device group setting need to be applied multiple time to fix local overide
CSCvj84675	WAAS device not responding to ping or ssh/telent while the disk utilization is high.
CSCvi36270	Connection not hitting correct classifier although correct accelerators are applied
CSCvi98993	THDL & TH Pending Connection seen in BR SN after high load
CSCvk51962	Occasionally web page does not load and DRE resets the connection
CSCvk53700	SMB object cache-lite unexpected reload during SMB file read/write operations in a certain scenario
CSCvk30565	Observed SMBAO Single Client Performance degradation for large file download
CSCvk39110	SMBAO Memory leak observed in Branch WAE while executing the Longevity tests
CSCvk62762	SMBAO Memory leaks observed while running soak test with all SMB dialect traffic
CSCvk53799	Connections pushdown due to "IOBuff_threshold_reached" during SMB performance test in 641b
CSCvk53862	Pending connections observed while running webtraffic via dc proxy
CSCvk55916	T pending connections observed with single-sided webtraffic via proxy connect
CSCvk62115	TFO pending connection due to SDH did not propagate FIN
CSCvi72673	Cisco Wide Area Application Services Software Disk Check Tool Privilege Escalation Vulnerability
CSCvi74692	WAASNET Process RAM Dump Happens Repeatedly
CSCvj30270	WAASNET process memory dump gets generated in WAAS 6.4.1a
CSCvk52162	waasnet process restarts and leave memory dump
CSCvk48179	WAASNET Memory Dump Happens when restarting the waasnet service
CSCvj06223	Service Restart Of WAASNET During Intializing Interface

Caveat ID Number	Description
CSCvj83232	Application change not reflected in Policy Map CLI
CSCvk16278	Rarely Webpage fails to load with message "Site can't be reached" and Error code "ERR_TIMED_OUT"
CSCvk41395	RPC over HTTPS fails with Appnav-XE interception.
CSCvk41478	SNMPv2 not polling "TfoStats" information after waasnet Memory Dump
CSCvj02769	Appnav keeps redirect traffic to waas node (SN) when waas node is in pending state
CSCvj69356	NPRM Restarted & default-gw not reachable in Appnav in Max Cluster.
CSCvk65629	File download from OBIEE failed on WAAS when http object cache is enabled
CSCvk65184	641b:fresh deployment of vWAAS 12k and 50k with non-resized resources is not successful with Hyper-V

Cisco Software Version 6.4.1a Resolved Caveats

The following caveats, impacting earlier software versions of WAAS, were resolved in Software Version 6.4.1a.

Caveat ID Number	Description
CSCuy82470	Connection reset seen while sending mails with large attachments
CSCva42612	"sh wccp ?" options all appear twice
CSCva96382	eth_bypass alarm can get generated without reason
CSCvb08476	WAAS: ica_ao64 core generated on device
CSCve86008	Akamai status "Required reload" need to be intimated in device list page
CSCve94135	SAR service utility restart appearing in the WAAS accelerator
CSCvg24312	Branch SMBAO memory usage goes above the expected limit
CSCvg29766	Waasnet process restart observed rarely when removing bridgegroup from interface and assiging IP
CSCvg34336	ISR-WAAS is blocking traffic when there is a MTU change in packet path
CSCvg38704	HTTPAO should raise an alarm when split header limit reached and traffic is dropped
CSCvg63085	SMB Digital Key not refreshing digital Key with account password change
CSCvg74531	Filtering options in device list are limited
CSCvg74712	Inline interfaces were down post reload in interception mode
CSCvg76284	httpcache service has been disabled with akamai enabled
CSCvg77509	Force settings on all Devices in Group icon showing in Optimization Policies page in a scenario
CSCvg85350	Security Keys not getting invalidated upon failure at EDGE and connection being reset continuously
CSCvg88235	Stuck connections "T" seen in soak

Caveat ID Number	Description
CSCvg90211	WAVE-294-K9 does not respond with CDP Neighborship Table details when polled via SNMP
CSCvg97531	log file size is growing beyond 48MB, DUT will run out of disk space
CSCvg99470	SSL accelerator enabled back after box reload while it was disabled before reload
CSCvh07778	Replacement device gets assigned to group for newly activated devices
CSCvh10339	SMB connection not optimized when security keys fail at Branch box
CSCvh13100	Unwanted alarm raised while starting http object-cache
CSCvh20136	Stuck connection T seen in NGSSL dual side
CSCvh21193	Observed cli failure and corresponding errorlogs during nprm nodemgr restart in ANC
CSCvh22217	Inline module is dropping icmp packets
CSCvh23590	Unwanted warning message displayed after enabling Akamai config
CSCvh24158	Fault response from server for request opnum 65535
CSCvh49517	Connection reset with Win10 client when SMB 2.1-Mute config is set
CSCvh51200	Wildcard support for Bypass mode in HTTPAO
CSCvh55089	RAID1 missing disk is not reported
CSCvh60335	Disk SMART warning not reported to user
CSCvh63504	ENCS-vWAAS6K inaccessible after disk partition delete
CSCvh65545	Observed intermittent traffic issue after nprm restart
CSCvh67554	Unable to create new device group after deleting default WAAS and Waas Express device groups
CSCvg50056	Need to remove TCP related configuration in CM device from GUI
CSCvg81918	object cache partitions created with wrong sizes after partition delete
CSCvh69369	Wildcard support for bypaas mode in CM.
CSCvg72476	Observing less wan TP with 4351 vwaas performance in 641 with more than 10% degradation
CSCvg86605	vBranch: Observing rmd service disabled alarm while downgrading waas from 6.4.1 to 6.2.3d

Cisco Software Version 6.4.1a Open Caveats

The following caveats are open in Software Version 6.4.1a. 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
CSCvc12656	TCAM entries are affected when repopulated after NPRM restart.
CSCvd69827	Device got Hung while running ICA Traffic
CSCvf39448	High CPU usage of 50% seen without traffic

Caveat ID Number	Description
CSCvf57314	"Pending with reload" status should be updated for 7571 in specific scenario
CSCvf58933	THDL stuck connection observed while running http/ssl traffic
CSCvg25864	SN SIA Invalid Packet alarm rarely seen in ANC during high load test
CSCvg91871	Httpao service disabled during high load test
CSCvg95232	ANC did not stop wccp participation while cluster was not operational.
CSCvh03423	Service Node is not returning packets to network after random change on the interface configs in SN
CSCvh07373	Observing more number of PT connections and connections are not scaling while running akc perf test
CSCvh12491	Maximum CPU utilization and throughput fluctuations are seen in few instances in 641 with 594-ICA
CSCvh13904	Observing Cluster degrade and ARP entry in DELAY/INCOMPLETE state in ANC on random interface changes
CSCvh14162	packet capture on ANC interface with "number-of-files' option is not working as expected
CSCvh22986	Rarely T,TDL warm process taking more time in a specific scenario
CSCvh47298	SNMPv3 polling returns Unknown UserName after reload of WAAS
CSCvh50791	WN_DFT core file seen in vWAAS150K while change egress method
CSCvh51119	Throughput fluctuation seen with ESXI-vWAAS-6K with UCS-E160D-M2 and UCS-E180D-M2
CSCvh54169	SMB missing Admission Control accepts connections leading to overload
CSCvh63244	Wan Secure core seen after downgrade the SN
CSCvh63924	WAAS HTTPAO: Bad deletion from fd table cause core
CSCvh78904	T stuck connection observed with web traffic via proxy
CSCvh86313	Invalid pointer error when trying to stop the packet capture
CSCvh96699	Abnormal memory consumed by SMBAO on the DC device longevity test
CSCvh96772	core.exec_pkt_capture core file generated
CSCvi02645	SNMP restarts with a core dump
CSCvi09138	TFO accelerator set to Zero in SN after upgrade in a scenario
CSCvi18247	unable to stop packet capture on ANC using "packet-capture stop" command
CSCvh53271	VWAAS-150K : WAN throughput 12% and LAN throughput 2% less compared with 8541
CSCvf01746	WAAS HTTP AO process httpmuxd consumes more memory causing multiple AO keepalive timeouts
CSCvi48375	SMB AO: Duplicate folders will show up when User renames a folder
CSCvi36270	Connection not hitting correct classifier although correct accelerators are applied
CSCvm52188	Devices are not showing in report central page while generating Device Dashboard (AppNav-XE) report

Cisco Software Version 6.4.1 Resolved Caveats

The following caveats were resolved in Software Version 6.4.1.

Caveat ID Number	Headline
CSCve74457	Cisco Wide Area Application Services ICA Accelerator Denial of Service Vulnerability
CSCve82472	Cisco Wide Area Application Services (WAAS) Denial-of-Service (DoS) Vulnerability
CSCvf27051	WAAS Akamai Cache not support wildcards for server bypass
CSCvg40834	Traffic_server core with Akamai cache
CSCvg35976	Getting authentication prompt when WAAS in place the proxy attempts to negotiate NTLM
CSCvf21935	httpcache service has been disabled with akamai enabled
CSCve72253	Rarely MAPI AO restarted unexpectedly with RPCHTTP(s) traffic
CSCve82523	HTTPS stuck connections on Core and Edge both
CSCve79892	Observed HTTP traffic-interruption in Branch due to malformed http request
CSCvh01870	Stuck conns observed on branch device for http traffic
CSCvh22843	Errors seen in http logs for http connect requests with policy changes in wae
CSCve68201	Permanent connectivity issue on virtual ethernet
CSCve71066	FTP connection failure with WAAS after FTP client "MLSD" request.
CSCvg18237	Stuck connections for PT APP CFG flows.
CSCuy82470	Connection reset seen while sending mails with large attachments
CSCvf32228	Device was unreachable for a brief period
CSCvd94539	Timestamps missing after negotiated in single sided scenario
CSCvf09323	Multiple Vulnerabilities in ntp
CSCvc67937	lowmem_reserve and memory allocation failure
CSCvf04748	PMD service restarted after WAASNET Restart
CSCvf55664	fda service triggers reload while waasnet restarts
CSCvf82199	waasnet wn_dft0 and wccp flaps are seen
CSCvf05107	Waasnet error logging when timestamp option not found
CSCve53939	waasnet service restarted when enabling InlineGroup
CSCve86619	Cannot SSH to WAAS By Using InlineGroup Interface
CSCvc95550	Failures seen with polling snmp mibs iFTable, iFXTable on inline device
CSCvf25027	WAAS fix CVE-2017-3167, CVE-2017-3169, CVE-2017-7679, and CVE-2017-9788.
CSCvf81284	Optimization stops silently upon flow table overflow
CSCvf57958	Restart of bash process
CSCvf97803	Router registration to 6.x of CM : "enable password" not supported

Caveat ID Number	Headline
CSCvg20842	WAAS Command Authorization fails when sending commands with multiple arguments to ACS server
CSCvg47760	Handle the raid controller's OCR event
CSCve16092	encryption-service process reloaded unexpectedly while optimizing SMBv3 signed connections
CSCve19211	SMBAO Unexpected restart while handling Lib Crypto
CSCve47337	SMB Core Files due to windows-domain encryption-service, on Upgrading WAAS
CSCvf41079	smbao restarted with OC memory corruption
CSCvf47948	Client sending kerberos security blob in two session setup requests cause reset
CSCvf47958	SMBAO client denial list is not getting updated for SMB AO generated reset
CSCvg26443	CM Chart update fail with collecting statistics of the application: SMB failure
CSCvg50517	GPO update failed due to guest bit set in session setup response
CSCuz56155	WAAS SR server failed in Key retrieval
CSCvd38216	WNDFT core file seen in WAAS when serving mixed AO traffic.
CSCvf01245	Cluster went to down Due to "TFO accelerator load level has been set to 0" in SN
CSCvd78539	Device hung and unavailable on network due to TX Hung
CSCve15397	CM-AppNav polling sessions get stuck and result in AppNav remaining offline forever
CSCve21589	WAAS SR_DRS_CRACK_NAME alarm occurring frequently.
CSCve49142	Failure processing split server response with non success status
CSCve65800	Device registration failing inline deployment while management flow going via inline data-path
CSCuy17130	Invalid stats value getting displayed for active ANC egress control cnt
CSCvd34222	NGSSL:DUAL SIDE: Auto Discovery Interop Support for negotiation of SSLAOv1 and SSLAOv2

Cisco Software Version 6.4.1 Open Caveats

The following caveats are open in Software Version 6.4.1.

Caveat ID Number	Headline
CSCvh51200	Bypass server configuration with wild cards are not working in HTTPAO
CSCvg97531	log file size is growing beyond 48MB, WAAS device will run out of disk space
CSCvd69827	Device got Hung while running ICA Traffic
CSCvg95232	ANC did not stop wccp participation while cluster was not operational.
CSCva42612	"sh wccp ?" options all appear twice
CSCve94135	SAR utility core file appearing in the WAAS accelerator
CSCvf72849	Less Throughput observed with 44xx ISR waas using 16.7.1 image in ISR Router

Caveat ID Number	Headline
CSCvh47298	SNMPv3 polling returns Unknown UserName after reboot of WAAS
CSCvh55089	RAID1 missing disk is not reported
CSCvh60335	Disk SMART warning not reported to user
CSCvh63504	ENCS-vWAAS6K inaccessible after disk partition delete
CSCvf58933	THDL stuck connection observed while running http/ssl traffic
CSCvh13100	Unwanted alarm raised while starting http object-cache
CSCvg25864	SN SIA Invalid Packet alarm rarely seen in ANC during high load test
CSCvg29766	Waasnet process restart observed rarely when removing bridgegroup from interface and assiging IP
CSCvh03423	Service Node is not returning packets to network after random change on the interface configs in SN
CSCvh07373	Observing more number of PT connections and connections are not scaling while running akc perf test
CSCvh13904	Observing Cluster degrade and ARP entry in DELAY/INCOMPLETE state in ANC on random interface changes
CSCvf34294	In a specific scenario, NHM keepalive alarm seen during AKC soak
CSCvg34336	ISR-WAAS is blocking traffic when there is a MTU change in packet path
CSCvh22217	Inline module is dropping icmp packets
CSCvh65545	Observed intermittent traffic issue after nprm restart
CSCvh22986	Rarely T,TDL warm process taking more time in a specific scenario
CSCvh49517	Connection reset with Win10 client when SMB 2.1-Mute config is set
CSCvh58009	SMBAO restarted while running mega soak in 6.4.1
CSCvb08476	WAAS: ica_ao64 core generated on device
CSCvg77509	Force settings on all Devices in Group icon showing in Optimization Policies page in a scenario
CSCvh23590	Unwanted warning message displayed after enabling Akamai config
CSCvh52624	XE router registration to Central Manager not working with 16.8.1(TP) dev branch image

Cisco Software Version 6.4.1x Command Changes

This section lists the modified commands in Cisco WAAS Software Version 6.4.1x.

Table 10 lists the commands and options that have been added or changed in Cisco WAAS Software Version 6.4.1x.

Table 10 CLI Commands Added or Modified in Version 6.4.1x

Mode	Command	Description
Global Configuration	**accelerator http object-cache validate-address bypass**	Adds bypass server IP addresses to a whitelist for Server Address Validation for the Akamai Connect cache.
	accelerator http object-cache validate-address enable	Validates the server IP address configuration for the Akamai Connect cache.
	interface virtual	Used for communication between the NFVIS host and the WAAS guest. The IP address associated with this interface (virtual 1/0) is assigned automatically by NFVIS while booting up, and cannot be modified.
EXEC	**show statistics accelerator smb debug**	Added field descriptions for OCLite.

Using Previous Client Code

If you have upgraded to Cisco WAAS Version 6.4.1x and are using the WSDL2Java tool to generate client stubs that enforce strict binding, earlier version client code (prior to 4.3.1) may return unexpected exceptions due to new elements added in the response structures in 4.3.1 and later releases. The observed symptom is an exception related to an unexpected subelement because of the new element (for example, a deviceName element) in the XML response.

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

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

To apply the patch, follow these steps:

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

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

META-INF/
META-INF/MANIFEST.MF
org/
org/apache/
org/apache/axis2/
org/apache/axis2/schema/
org/apache/axis2/schema/i18n/
org/apache/axis2/schema/template/
org/apache/axis2/schema/typemap/
org/apache/axis2/schema/util/
org/apache/axis2/schema/writer/
org/apache/axis2/schema/i18n/resource.properties
org/apache/axis2/schema/i18n/SchemaCompilerMessages.class
org/apache/axis2/schema/template/ADBDatabindingTemplate.xsl
org/apache/axis2/schema/template/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.

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

Cisco WAAS Documentation Set

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

- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Monitoring Guide*
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*
- *Configuring WAAS Express*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 294 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 594 and 694 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 7541, 7571, and 8541 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Installing the Cisco WAE Inline Network Adapter*

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the "Cisco WAAS Documentation Set" section.

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.