

Cisco vWAAS with Cisco Enterprise NFVIS

This section describes Cisco vWAAS with Cisco Enterprise Network Functions Virtualization Infrastructure Software (Cisco Enterprise NFVIS). It contains the following sections:

- Cisco Enterprise NFVIS, page 9-1
- Cisco vWAAS with Cisco Enterprise NFVIS, page 9-2
- Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later, page 9-3
- Firmware Upgrade for Cisco Enterprise NFVIS, page 9-5
- Traffic Interception for Cisco vWAAS with Cisco Enterprise NFVIS, page 9-6
- Upgrade Guidelines for Cisco Enterprise NFVIS, page 9-8

Cisco Enterprise NFVIS

Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) is a Linux-based software-hosting layer with embedded KVM hypervisor.

Cisco Enterprise NFVIS contains the following features:

- Cisco vWAAS with Cisco Enterprise NFVIS is deployed on the Cisco ENCS 5400-W Series. For more information on the ENCS 5400-W Series, see the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series".
- Cisco Enterprise Network Functions Virtualization (NFV): Extends Linux by packaging additional functions for Virtual Network Functions (VNF) that support lifecycle management, monitoring, device programmability, service chaining, and hardware acceleration.

Cisco Enterprise NFV also provides local network management capabilities that enable you to dynamically deploy virtualized network functions such as a virtual router, firewall, and WAN acceleration on a supported Cisco device, eliminating the need to add a physical device for every network function.

- Monitoring: Monitors all the parameters of the deployed Cisco vWAAS, including memory, storage, and CPU, and monitors memory, storage, and CPU utilization of the Cisco vWAAS.
- Traffic verification: Verifies traffic flows through Cisco vWAAS by monitoring the VNF interface statistics.
- Add-On Capability: Ability to add vCPU, memory, and storage, to modify the networking option and add a virtual interface, to configure the virtual networking port and connect it to a VLAN.

Cisco vWAAS with Cisco Enterprise NFVIS

This section contains the following topics:

- About Cisco vWAAS with Cisco Enterprise NFVIS, page 9-2
- Operating Guidelines for Cisco vWAAS with Cisco Enterprise NFVIS, page 9-2
- Platforms and Software Versions Supported for Cisco vWAAS with Cisco Enterprise NFVIS, page 9-2

About Cisco vWAAS with Cisco Enterprise NFVIS

Cisco vWAAS with Cisco Enterprise NFVIS enables Cisco WAAS to run Cisco vWAAS as a standalone VM on the Cisco ENCS 5400-W Series platform to provide WAN application optimization, and, optionally, application optimization with Akamai Connect.

Operating Guidelines for Cisco vWAAS with Cisco Enterprise NFVIS

For guaranteed performance, the Cisco ENCS 5400-W Series, Cisco UCS-C Series, Cisco UCS-E Series, Cisco ENCS 5100, Cisco CSP-2100, and Cisco ISR configurations listed in the Cisco WAAS sizing guides and specifically noted in Cisco WAAS, Cisco vWAAS user guides, and Cisco WAAS Release Notes are the only devices we recommend for use with Cisco vWAAS.

Caution

Although Cisco vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

For more information about supported platforms for Cisco Enterprise NFV, see the Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.11.x.

Platforms and Software Versions Supported for Cisco vWAAS with Cisco Enterprise NFVIS

Table 9-1 shows the platforms and software versions supported for Cisco vWAAS with Cisco Enterprise NFVIS.

PID and Device Type	Earliest Cisco WAAS Version Supported	Host Platforms	Earliest Host Version Supported	Disk Type
 PID: OE-VWAAS-ENCS Device Type: OE-VWAAS-ENCS 	• 6.4.1	Cisco ENCS 5400-W Series	Cisco Enterprise NFVIS 3.7.1	• virtio
 PID: OE-VWAAS-KVM Device Type: OE-VWAAS-KVM 	• 6.2.x	Cisco UCS-E Series	Cisco Enterprise NFVIS 3.7.1	• virtio

Table 9-1 Platforms and Software Versions Supported for Cisco vWAAS with Cisco NFVIS

Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W provides the following capabilities:

- Enterprise Application Optimization: Branch to branch, and branch to data center optimization of application traffic, either within or outside of a Cisco iWAN solution. This includes traditional WAAS WAN optimization functions, as well as the deployment of other iWAN solution features that are inherent in Cisco IOS-XE platforms.
- Everything as a Service (XaaS) Optimization: For single-sided use cases in cloud deployments, where you have control of one side of the connection, for example, branch to cloud, and data center to cloud (for backup and recovery purposes). Optimizations are applied in a unilateral fashion, without reliance on a peer.
- Service Nodes: A service node is a Cisco WAAS application accelerator that optimizes and accelerates traffic according to the optimization policies configured on the device. It can be a Cisco vWAAS instance or a Cisco ENCS 5400-W device.



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

• Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W is part of Cisco iWAN: A suite of components that brings together WAN optimization, performance routing, and security levels of leased lines and MPLS VPN services to the Internet. For more information on Cisco Enterprise NFVIS and Cisco NFV, see the *Cisco Intelligent WAN - An SD-WAN Solution*.

Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later

This section contains the following topics:

- About the Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later, page 9-4
- Operating Guidelines for the Unified OVA Package Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later, page 9-4

About the Unified OVA Package for Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later

In Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.x, Cisco vWAAS is deployed in a RHEL KVM hypervisor on a Cisco ENCS 5400-W Series device.

In Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.x and later, Cisco provides a single, unified OVA or NPE OVA package for each hypervisor type, which can be used with all Cisco vWAAS models for that hypervisor.

Each unified OVA package file is a preconfigured VM image that is ready to run on a particular hypervisor. The launch script for each unified OVA package provides the model and other required parameters to launch Cisco vWAAS in Cisco WAAS in the required configuration.

Here are examples of the unified OVA and NPE OVA package filenames for Cisco vWAAS on RHEL KVM:

- OVA: Cisco-KVM-vWAAS-Unified-6.4.3c-b-42.tar
- NPE OVA: Cisco-KVM-vWAAS-Unified-6.4.3c-b-42-npe.tar

The unified OVA package for Cisco vWAAS on RHEL KVM/KVM on CentOS contains the following files.

- Flash disk image
- Data system disk
- Akamai disk
- **INSTRUCTIONS.TXT**: Describes the procedure for deploying the virtual instance and using the **launch.sh** file.
- package.mf template file and bootstrap-cfg.xml—These two files work together on the Cisco Enterprise NFVIS platform with the image_properties.xml file as day-zero configuration template.
- ezdeploy.sh: The script used to deploy vWAAS on UCS-E.
- exdeploy_qstatus.exp: The dependent file for ezdeploy.sh script.
- **image_properties.xml**: A VM configuration template file used on the Cisco Enterprise NFVIS platform.
- launch.sh: The launch script to deploy Cisco vWAAS on Linux KVM.
- **vm_macvtap.xml**: Configuration file for Cisco vWAAS deployment using host machine interfaces with the help of the **mactap** driver.
- **vm_tap.xml**: Configuration file for Cisco vWAAS deployment using the virtual bridge or OVS present in the host machine.

Operating Guidelines for the Unified OVA Package Cisco vWAAS with Cisco Enterprise NFVIS in Cisco WAAS Version 6.4.1 and Later

The Cisco ENCS 5400-W Series, Cisco UCS-C Series, Cisco UCS-E Series, Cisco ENCS 5100, Cisco CSP-2100, and Cisco ISR configurations listed in the Cisco WAAS Sizing Guides and specifically noted in Cisco WAAS and Cisco vWAAS user guides and Cisco WAAS Release Notes are the only devices we recommend for use with Cisco vWAAS.

I



Although Cisco vWAAS models may be able to operate with other Cisco or third-party hardware, successful performance and scale for those configurations is not guaranteed.

For more information about supported platforms for Cisco Enterprise NFV, see the Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software.

Firmware Upgrade for Cisco Enterprise NFVIS

To upgrade the Complex Programmable Logic Device (CPLD) and scp fw-upgradend the Field Programmable Gate Array (FPGA) for Cisco Enterprise NFVIS to the latest version, follow these steps:

- **Step 1** Ensure that your system is running the following:
 - Cisco WAAS Version 6.4.3b
 - Cisco Enterprise NFVIS 3.11.1
- Step 2 Download the Cisco WAAS Firmware image for ENCS-W Appliance from the Cisco Wide Area Application Services (WAAS) Software 6.4.3x Download Page.
- Step 3 To upgrade the FPGA, use the **nfvis scp fw-upgrade** command:

ENCS-W# nfvis scp fw-upgrade server-IP RemoteFileDirectory RemoteFileName

Example:

ENCS-W# nfvis scp fw-upgrade 172.19.156.179 ./ Cisco_ENCS_firmware-3.11.1.fwpkg



After you upgrade the firmware package, you must power-cycle the entire chassis to ensure that the FPGA takes effect.

- Step 4 To verify the CPLD and FPGA version, use the CIMC GUI or the CLI.
 - To verify the CPLD and FPGA version from the CIMC GUI, choose Chassis > Summary (Figure 9-1).

Premiust Kanie ENCO Serial Kumber TOL21243172 PD ENCOS400-POL2124072 PD ENCOS400-BOD0-BSTR-2EA01064000 BIOS Version BL0004-02-B-0000-BSTR-2EA01064000 BIOS Version CPLD Version 17 Oescription CPLD Version 17 Asset Tag Unit trans Current Time (UTC) Bal Out 6 07:07:40 2018 Local Tame Brow et 07:07:40 2018 UTC -0000 Timederee UTC Balent Timederee	cito Cisco	o Integrated Management Controller		÷ 🔍 🛛 👔	400000111204-ENCISH06F0(2124811E
Preduct Kanne EVC0 Heathere EVC05400-20L21241718 Serial Kumber F02.2525578 IP Address 5.1.1.31 PD EVC05400-4020-4020-4000-4879-258-510540000 IP Address 5.1.1.31 INDE F0009000-4020-4020-40000-4879-258-510540000 IP Address 5.0.000 E870-26.000 BI03 Version BI03 Version EVC0510_2.24 (Public Date 01-10.000) IP Address 5.0.000 E870-26.000 BI03 Version BI03 Version EVC0510_2.24 (Public Date 01-10.000) IP address Version 2.0.000 E870-26.000 BI03 Version BI03 Version EVC0510_2.24 (Public Date 01-10.000) IP address Version 2.0.000 E870-26.000 BI03 Version Evect File Evec 10000 Early Version 2.0.000 E870-26.000 Asset Tag University Evec 10000 Evec 10000 Evec 10000 Evec 10000 Chassis Status © Overal Dates Evec 10000 Evec 10000 Evec 10000 Evec 10000 Overal Dates © Overal Dates © Overal Dates Evec 10000 Evec 10000 Overal Dates © Overal Dates © Overal Dates Evec 100000 Evec 100000	Ohassis / Sum	imary 🚊		Hamach Ho	atteor [same coll] tog takes O
Seriel Rumber 7012124117E IP Address: \$11.131 PD: Tx0084024-02A80000487F+02EA510050000 MAC Address: \$12.0204001410+145130 BitDis Version: BitDis Version: BitDis Version: \$12.0204001410+1242130 Description:	Server Proper	rties	Cisco Integrated I	Management Controller (Cis	sco IMC) Information
PD: ENC 54406x8 NUR: TODB0004024604600004876-0284506000000 BIO 3 Version: BIO 3 Version: Description: Immune Asset Tag: Immune Unit: Current Time (UTC) Satisfies Status: Current Time (UTC) Prevent Status: Current Time (UTC) Overall Servery Status: Current Time (UTC) Overall Servery Status: Current Time (UTC)	Product Name:	EVCE	Hasthama	ENC05405-F012124017g	
UURD 100090004-02x8-00000-8179-2Ex5-00600000 BIOR Version BVCR14_2.4 flaue Desc. 0710202161 Overrighter Immuner Asset Tag Immuner UVRD Sci 001 50127 40 2018 Corrent Time (UTC) Sci 001 50127 40 2018 UTC -0000 Timestere UTC Reset Flats: Immuner Overall Strever Status: Immuner Overall Dimwiner Immuner	Serial Number	PGL21248178	IP Address:	8.5.5.521	
BIOL Version BIOL	PID	ENC88406×0	MAC Address	70 DB 00 C4 02 A8	
Oversit joints Interface Asset Tag: Universe Asset Tag: Universe Universe Sar Out 65 00 14 00 15 01 27 40 00 15 UT 0 -0000 Taxestract UTC Rewer Status Interface Overall Server Status Interface Overall Server Status Interface	NVID:	75089804-0248-0200-8879-2E4510E99300	Firmware Version:	8 218 20130817145818)	
Asset Tage Universal Stratus Provert Status Provert Status Provert Sta	BIG'S Version.	8NG814_2.4 (Bure Delle 0712/2218)	CPLD Version	17 .	
Least Tame Set Ger 6 01 21 43 32/18 UTC -0000 Taxastee UTC Extent Taxastee UTC Extent	Overrightion:		Handware Version:	1	
Timessee UTC ElectTimesee	Asset Tag	Unkrown .	Current Time (UTC)	Set Out 8 07.07.40 2018	
Chassis Status Power Statu:			Local Time	\$41 Oct 8 01 01 40 2018 UTC +0000	
Power State: Co Created Server State: Co Overall Server State: Co			Timptone	uto.	Balant Torquerre
Overal Server Status: Cont	Chassis Statu	5			Labort Tomparty
Overall Server Status: Status: Status: Status					
Overal DIMM Status.					
Overall Storage Status: 🚰 Comm	Overall DIMM	Statut. Const			
	Overail Storage	Status: Sal Court			

Figure 9-1 Using the CIMC Console to Verify CPLD/FPGA Version

• To verify the CPLD and FPGA version from the CIMC CLI, use the following command:

```
ENCS-W# scope cimc
ENCS-W# /cimc # show firmware detail
Firmware Image Information:
Update Stage: NONE
Update Progress: 0%
Current FW Version: 3.2(6.20180817145819)
FW Image 1 Version: 3.2(6.20180817145819)
FW Image 1 State: RUNNING ACTIVATED
FW Image 2 Version: 3.2(3.20171215104530)
FW Image 2 State: BACKUP INACTIVATED
Boot-loader Version: 3.2(6.20180817145819).36
CPLD Version: 1.7
Hardware Version: 2
```

Traffic Interception for Cisco vWAAS with Cisco Enterprise NFVIS

Cisco vWAAS with Cisco Enterprise NFVIS on Cisco ENCS 5400-W supports WCCP traffic interception.

WCCP specifies interactions between one or more routers and one or more Cisco WAEs, to establish and maintain the transparent redirection of selected types of traffic in real time. The selected traffic is redirected to a group of Cisco WAEs with the aim of optimizing resource usage and lowering response times. A WCCP-enabled router and a Cisco WAE exchange WCCP protocol packets and negotiate membership of WCCP service groups.

For Cisco vWAAS on Cisco ENCS 5400-W with WCCP, there are two Ethernet Gigabit ports that can be configured to intercept the traffic. With the NIM card, the ports can be used to intercept the WCCP traffic (configure port channel with LAN and WAN interface) if the inline interception method is not configured.

ſ

For detailed information on configuring WCCP, see the chapter "Configuring Traffic Interception" in the *Cisco Wide Area Application Services Configuration Guide*.

Table 9-2 shows the CLI commands used to configure WCCP traffic interception for Cisco vWAAS with Cisco Enterprise NFVIS.

Mode	Command	Description
Global configuration	interception method wccp	Configures the WCCP traffic interception method.
	wccp access-list	Configures an IP access list on a WAE for inbound WCCP GRE-encapsulated traffic.
	wccp flow-redirect	Redirects moved flows.
	wccp router-list	Configures a router list for WCCP Version 2.
	wccp shutdown	Sets the maximum time interval after which the WAE will perform a clean shutdown of the WCCP.
	wccp tcp-promiscuous	Configures the WCCP Version 2 TCP promiscuous mode service.
	wccp tcp-promiscuous service-pair serviceID serviceID+1	Configures the WCCP Version 2 TCP promiscuous mode service and specifies a pair o IDs for the WCCP service on devices configured as application accelerators.
user-level	show statistics wccp	Displays WCCP statistics for a WAE.
EXEC and privileged-level	show wccp clients	Displays which WAEs are seen by which routers.
EXEC	show wccp egress	Displays the WCCP egress method—IP forwarding, generic GRE, WCCP GRE, or L2.
	show wccp flows tcp-promiscuous summary	Displays WCCP packet flows and TCP-promiscuous service information.
	show wccp masks tcp promiscuous	Displays WCCP mask assignments and TCP-promiscuous service information.
	show wccp routers [detail]	Displays details of routers seen and not seen by the specified WAE.
	show wccp services [detail]	Displays the configured WCCP services.
	show wccp statistics	Displays WCCP generic routing encapsulation packet-related information.
	show wccp status	Displays the enabled state of WCCP and the configured service IDs.

 Table 9-2
 CLI Commands for WCCP Interception Mode

For more information on these commands, see the *Cisco Wide Area Application Services Command Reference*.

Upgrade Guidelines for Cisco Enterprise NFVIS

This section contains the following topics:

- Upgrading to Cisco Enterprise NFVIS 3.9.1 for Cisco WAAS Version 6.4.3, page 9-8
- Upgrading to Cisco Enterprise NFVIS 3.10.1 for Cisco WAAS Version 6.4.3a, page 9-9
- Upgrading to Cisco Enterprise NFVIS 3.11.1 for Cisco WAAS Version 6.4.3b, page 9-10

Upgrading to Cisco Enterprise NFVIS 3.9.1 for Cisco WAAS Version 6.4.3

Cisco Enterprise NFVIS 3.9.1 is supported for Cisco vWAAS in Cisco WAAS Version 6.4.3.

- This section provides general guidelines. For detailed upgrade information:
 - For the full procedure to upgrade to Cisco Enterprise NFVIS 3.9.1, see the chapter Upgrading Cisco Enterprise NFVIS in the Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide, Release 3.9.1.
 - For more information on Cisco Enterprise NFVIS upgrade procedures and Cisco Enterprise NFVIS image files, see the Cisco Enterprise NFVIS Configuration Guides Page
- If you are running **nfvis-371-waas-641a** or **nfvis-371-waas-641b** on a Cisco ENCS 5400-W device, before upgrading Cisco Enterprise NFVIS, upgrade to Cisco WAAS Version 6.4.3. For more information on Cisco Enterprise NFVIS and ENCS 5400-W devices, see the section Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W in the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series,"
- Table 9-3 shows the supported upgrade paths for Cisco Enterprise NFVIS 3.9.1.

Current Cisco Enterprise NFVIS Version	Cisco Enterprise NFVIS Upgrade Path	
3.7.1	1. Upgrade to Cisco Enterprise NFVIS 3.8.1	
	2. Upgrade to Cisco Enterprise NFVIS 3.9.1	
3.8.1	Upgrade directly to Cisco Enterprise NFVIS 3.9.1	

Table 9-3 Upgrade Paths for Cisco Enterprise NFVIS 3.9.1

• After you upgrade your system from an earlier to a later version of Cisco Enterprise NFVIS, the newly upgraded Cisco Enterprise NFVIS version automatically upgrades BIOS and CIMS for the Cisco ENCS 5400-W platform. Table 9-4 shows the Cisco Enterprise NFVIS 3.9.1 automatic BIOS and CIMC upgrades for the Cisco ENCS 5400-W series.

Table 9-4	Cisco Enterprise NFVIS 3.9.1 Automatic CIMC and BIOS Upgrades for Cisco ENCS 5400-W
-----------	---

Cisco Enterprise NFVIS Upgrade	Automatic Upgrade for BIOS for Cisco ENCS 5400-W	Automatic Upgrade for CIMC for Cisco ENCS 5400-W
From Cisco Enterprise NFVIS 3.7.1 to Version 3.8.1	Upgraded to BIOS 2.5	Upgraded to CIMC 3.2.4
From Cisco Enterprise NFVIS 3.8.1 to Version 3.9.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6



Each upgrade may take about 90 minutes. Do not interrupt the upgrade process.

Upgrading to Cisco Enterprise NFVIS 3.10.1 for Cisco WAAS Version 6.4.3a

Cisco Enterprise NFVIS 3.10.1 is supported for Cisco vWAAS in Cisco WAAS Version 6.4.3a.

- This section provides general guidelines. For detailed upgrade information:
 - For the procedure to upgrade to Cisco Enterprise NFVIS 3.10.1, see the chapter Upgrading Cisco Enterprise NFVIS in the Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide, Release 3.10.1.
 - For more information on Cisco Enterprise NFVIS upgrade procedures and Cisco Enterprise NFVIS image files, see the Cisco Enterprise NFVIS Configuration Guides Page.
 - If you are running **nfvis-371-waas-641a** or **nfvis-371-waas-641b** on a Cisco ENCS 5400-W device: Before upgrading Cisco Enterprise NFVIS, upgrade to Cisco WAAS Version 6.4.3. For more information on Cisco Enterprise NFVIS and Cisco ENCS 5400-W devices, see the section Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W in the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series,"
- Table 9-5 shows the supported upgrade paths for Cisco Enterprise NFVIS 3.10.1.

Current Cisco Enterprise NFVIS Cisco Enterprise NFVIS Upgrade Path Version		
3.7.1	1. Upgrade to Cisco Enterprise NFVIS 3.8.1	
	2. Upgrade to Cisco Enterprise NFVIS 3.10.1	
3.8.1	Upgrade directly to Cisco Enterprise NFVIS 3.10.1	
3.9.1	Upgrade directly to Cisco Enterprise NFVIS 3.10.1	

Table 9-5Upgrade Paths for Cisco Enterprise NFVIS 3.10.1

• After you upgrade your system from an earlier to a later version of Cisco Enterprise NFVIS, the newly upgraded Cisco Enterprise NFVIS version automatically upgrades BIOS and CIMS for the Cisco ENCS 5400-W platform. Table 9-6 shows the Cisco Enterprise NFVIS 3.10.1 automatic BIOS and CIMC upgrades for the Cisco ENCS 5400-W series.

Table 9-6	Cisco Enterprise NFVIS 3.10.1 Automatic CIMC and BIOS Upgrades for Cisco ENCS 5400-W

Cisco Enterprise NFVIS Upgrade	Automatic Upgrade for BIOS for Cisco ENCS 5400-W	Automatic Upgrade for CIMC for Cisco ENCS 5400-W
From Cisco Enterprise NFVIS 3.7.1 to Version 3.8.1	Upgraded to BIOS 2.5	Upgraded to CIMC 3.2.4
From Cisco Enterprise NFVIS 3.8.1 to Version 3.9.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6
From Cisco Enterprise NFVIS 3.9.1 to Version 3.10.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6



Each upgrade may take about 90 minutes. Do not interrupt the upgrade process.

Upgrading to Cisco Enterprise NFVIS 3.11.1 for Cisco WAAS Version 6.4.3b

Cisco Enterprise NFVIS 3.11.1 is supported for Cisco vWAAS in Cisco WAAS Version 6.4.3b.

- This section provides general guidelines. For detailed upgrade information:
 - For the procedure to upgrade to Cisco Enterprise NFVIS 3.11.1, see the chapter "UpUpgrading Cisco Enterprise NFVIS" in the Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide, Release 3.11.1.
 - For more information on Cisco Enterprise NFVIS upgrade procedures and Cisco Enterprise NFVIS image files, see the Cisco Enterprise NFVIS Configuration Guides page
- If you are running nfvis-371-waas-641a or nfvis-371-waas-641b on a Cisco ENCS 5400-W device: Before upgrading Cisco Enterprise NFVIS, upgrade to Cisco WAAS Version 6.4.3. For more information on Cisco Enterprise NFVIS and Cisco ENCS 5400-W devices, see the section Upgrade and Downgrade Guidelines for Cisco vWAAS on Cisco ENCS 5400-W in the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series,"
- Table 9-7 shows the supported upgrade paths for Cisco Enterprise NFVIS 3.11.1.

Current Cisco Enterprise NFVIS Version	Cisco Enterprise NFVIS Upgrade Path	
3.7.1	1. Upgrade to Cisco Enterprise NFVIS 3.8.1	
	2. Upgrade to Cisco Enterprise NFVIS 3.10.1	
3.8.1	1. Upgrade to Cisco Enterprise NFVIS 3.10.1	
	2. Upgrade to Cisco Enterprise NFVIS 3.11.1	
3.9.1	Upgrade directly to Cisco Enterprise NFVIS 3.11.1	
3.10.1	Upgrade directly to Cisco Enterprise NFVIS 3.11.1	

Table 9-7Upgrade Paths for Cisco Enterprise NFVIS 3.11.1

• After you upgrade your system from an earlier to a later version of Cisco Enterprise NFVIS, the newly upgraded Cisco Enterprise NFVIS version automatically upgrades BIOS and CIMS for the Cisco ENCS 5400-W platform. Table 9-8 shows the NFVIS 3.11.1 automatic BIOS and CIMC upgrades for the Cisco ENCS 5400-W series.

Table 9-8	Cisco Enterprise NFVIS 3.11.1 Automatic CIMC and BIOS Upgrades for Cisco ENCS 5400-W

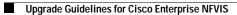
Cisco Enterprise NFVIS Upgrade	Automatic Upgrade for BIOS for Cisco ENCS 5400-W	Automatic Upgrade for CIMC for Cisco ENCS 5400-W
From Cisco Enterprise NFVIS 3.7.1 to Version 3.8.1	Upgraded to BIOS 2.5	Upgraded to CIMC 3.2.4
From Cisco Enterprise NFVIS 3.8.1 to Version 3.9.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6

Cisco Enterprise NFVIS Upgrade	Automatic Upgrade for BIOS for Cisco ENCS 5400-W	Automatic Upgrade for CIMC for Cisco ENCS 5400-W
From Cisco Enterprise NFVIS 3.9.1 to Version 3.10.1	Upgraded to BIOS 2.6	Upgraded to CIMC 3.2.6
From Cisco Enterprise NFVIS 3.10.1 to Version 3.11.1	Upgraded to BIOS 2.7	Upgraded to CIMC 3.2.7

Note

Γ

Each upgrade may take about 90 minutes. Do not interrupt the upgrade process.



1

