Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 4.12.x

First Published: 2023-08-20

Last Modified: 2024-08-14

About Cisco Enterprise NFVIS

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Find all the information you need about this release—new features, known behavior, resolved and open bugs, and related information.

What's New

New and Enhanced Features for Cisco Enterprise NFVIS Release 4.12.1

Feature	Description
DHCP Support for Internal Management Network	Cisco NFVIS uses the IP address assigned by a DHCP server for monitoring the VNF deployment.
VM Image Registration Using FTP and SCP Servers	In addition to already existing support to register a VM image using a http or https servers, you can register the VM images using FTP and SCP servers.

Resolved and Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.12.8

Resolved Bugs for Cisco NFVIS Release 4.12.8

Bug ID	Description
CSCwr58936	NFVIS: Missing Default Route when Using Single-IP Mode

Open Bugs for Cisco NFVIS Release 4.12.8

There are no open defects captured for Cisco NFVIS Release 4.12.8.

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.12.7

Resolved Bugs for Cisco NFVIS Release 4.12.7

Bug ID	Description
CSCwr77187	NFVIS: Issues with system_disk impact ability to access filesystem.
CSCwr33022	NFVIS: Guest VMs in VM_ERROR_STATE post upgrade due to "Cannot allocate memory".
CSCws02936	C8200-UCPE: NFVIS Fails to boot following Power-Cycle.
CSCwr43787	dhcp-ipv6 enabled in wan-br even though no running config explicitly enables it.
CSCwq54601	uCPE8300-1n20 NFVIS 4.12.4 upgrade to 4.15.4 fail.

Open Bugs for Cisco NFVIS Release 4.12.7

There are no open defects captured for Cisco NFVIS Release 4.12.7.

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.12.6

Resolved Bugs for Cisco NFVIS Release 4.12.6

Bug ID	Description
CSCwp25909	hugepages lost after Upgrading from 4.9 to 4.12
CSCwj45350	When rebooting cimc, it triggers to reboot NFVIS4.12.3 too

Bug ID	Description
CSCwq36748	ENCS5412 4.9.5 to 4.12.6 upgrade stuck

Open Bugs for Cisco NFVIS Release 4.12.6

There are no open defects captured for Cisco NFVIS Release 4.12.6.

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.12.5

Resolved Bugs for Cisco NFVIS Release 4.12.5

Bug ID	Description
CSCwf08895	c8200-uCPE: ENTROPY-0-ENTROPY_ERROR causing to constantly reboots

Open Bugs for Cisco NFVIS Release 4.12.5

Bug ID	Description
CSCwj45350	When rebooting CIMC, it triggers to reboot NFVIS 4.12.3 too

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.12.4

Resolved Bugs for Cisco NFVIS Release 4.12.4

Bug ID	Description
CSCwi43001	Cisco IMC Web-Based Management Interface Command Injection Vulnerability.
CSCwk24416	allocate_hugepages service crashes with a ZeroDivisionError.
CSCwj12469	NFVIS | CSR generation fails with invalid path when using it in vmanage mode.
CSCwi29799	Cisco Integrated Management Controller Command Injection Vulnerability for UCS E-Series M6.
CSCwj89223	NFVIS: "show system file-list disk usb" shows no files.
CSCwj16653	uCPE8300: VM went into ERROR after backup -> FDR -> Restore.
CSCwk76995	nfvis4.12.4 FAILED: maapi_delete(ms, mtid, argv[0]), Error: item does not exist (1): /nacm:nacm/

Bug ID	Description
CSCwj40609	ENCS NFVIS upgrade stuck [4.5->4.6->4.7->4.8->4.9.1->4.9.3->4.9.5-FC1 ok; stuck going to 4.12.3-FC4].
CSCwk77001	ucpe8300 with 4.12.4-24 core.lldpad.3226.TM1-c8kv-Artemis-medium.1721241090.gz
CSCwj01836	NFVIS4.12.3 ENCS missing extdatastore1 and extdatastore2 after upgrade from 4.9.5.
CSCwc81026	ENCS nfvis4.9.1 hostaction change-cimc-password failed.
CSCwi61297	ENCS5412 NFVIS 4.9.4-ES7 silent reboot.
CSCwi98689	ENCS upgrade from 4.9.5 to 4.12.3 caused all VMs shut.
CSCwk08549	NFVIS-4.12.4-12: System usb-mount mount failed on Tabei_M.
CSCwi19991	uCPE8300-1in20 GUI->Monitor->Port Statistics doese't display anything.
CSCwk76993	nfvis_operational log reports system setting error.
CSCwj76335	ENCS LAN-SRIOV over VLAN failed to pass ARP packet to c8kv.

Open Bugs for Cisco NFVIS Release 4.12.4

Bug ID	Description
CSCwm03901	vm restoration fail Crypto device is not available for this deployment.

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.12.3

Resolved Bugs for Cisco NFVIS Release 4.12.3

Bug ID	Description
CSCwi67312	Cisco ENCS: Automatic renewal of self signed certificate
CSCwi02497	Mount USB devices as part of Cisco NFVIS bootup

Open Bugs for Cisco NFVIS Release 4.12.3

Bug ID	Description
CSCwj45350	When rebooting CIMC, it triggers to reboot NFVIS4.12.3 too
CSCwj45343	Cisco NFVIS 4.12.3-FC4 NIM-2GE-CU-SFP is missing from Cisco Catalyst 8000V

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.12.2

Resolved Bugs for Cisco Enterprise NFVIS Release 4.12.2

Identifier	Headline
CSCwh44401	Restore fail with port channel
CSCwh30633	Cisco NFVIS 4.12.1 GUI portal forced password length 9 or more during VM deployment when first 8 only works
CSCwh07195	Cisco Catalyst Edge uCPE 8200 4.9.3-FC5 CCO to 4.12.1-FC upgrade fail

Open Bugs for Cisco Enterprise NFVIS Release 4.12.2

Identifier	Headline
CSCwh89691	UX 2.0 : CG Push fail: Failed to notify device after 3 attempts
CSCwf40904	QAT support not updated when multiple VM profiles are changed together
CSCwh93399	Cisco NFVIS should not allow users to configure via CLI command manually when device is in vManage mode

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.12.1

Resolved and Open Bugs for Cisco NFVIS Release 4.12.1

Resolved Bugs for Cisco NFVIS Release 4.12.1

Identifier	Headline
CSCwh30633	NFVIS4.12.1 GUI portal forced password length 9 or more during VM deployment when first 8 only works.
CSCwf97011	NFVIS CG deploy, Rollback failing because of the internet connectivity being temporarily down.

Open Bugs for Cisco NFVIS Release 4.12.1

There are no defect fixes in this Cisco NFVIS Release 4.12.1.

Important Notes

- Starting from Cisco NFVIS Release 4.10.1, the guest VNF settings are automatically preserved from the previous release version, when you upgrade to a newer release version. You don't have to reinstall NFVIS to update the guest VNF settings. For more information see, Upgrade Cisco NFVIS.
- Starting from Cisco NFVIS Release 4.10.1, Cisco NFVIS is based on open source AlmaLinux distribution. In Cisco NFVIS Release 4.9.x and earlier releases, Cisco NFVIS was based on CentOS Linux distribution which is now end-of-life. The support for CentOS Linux distribution will be discontinued in June 2024.
- If you are using I-350 based Network Interface Cards (NICs) that use IGB drivers, the Virtual Router Redundancy Protocol (VRRP) is not supported due to a limitation of MAC addresses that can be used in your network.

Software Upgrade

The Cisco Enterprise NFVIS upgrade image is available as *.iso* file. Currently, downgrades are not supported.

For more details on the software upgrade, see the Upgrading Cisco Enterprise NFVIS section in the Cisco Network Function Virtualization Infrastructure Software Getting Started Guide.

System Requirements

The following resources are required for a standalone Cisco Enterprise NFVIS:

- NFVIS needs 5GB of system memory.
- For a system that has 16 or less CPU cores, one CPU core is reserved for NFVIS. For a system that has more than 16 CPU cores, 2 CPU cores are reserved for NFVIS.
- For a system that has 32 GB or less of RAM, 3 GB is reserved for NFVIS. For a system that has more than 32 GB of RAM, 4 GB is reserved for NFVIS.
- 20 GB storage.
- For NFVIS portal, the minimum supported version of browsers are:
  - Mozilla Firefox 66
  - Google Chrome 71
  - Windows 10 Edge
  - MacOS 10.15 Safari



Note More memory and disk space are required to be added to the system, depending on VM deployments.

Supported Programs and Platforms

Supported Programs

The Cisco Meraki vMX solution is supported on Cisco's Enterprise NFV Infrastructure Software (NFVIS). For more information see, vMX Setup Guide for NFVIS.

Supported Platforms

The following table lists the only supported platforms and firmware for Cisco ENFV

Table 1:

Platform	Firmware	Version
C8200-UCPE-1N8	BIOS	C8200-UCPE_1.04.103020201614
	MCU	240.52
ENCS 5406, ENCS 5408, and ENCS 5412	BIOS	ENCS54_BIOS_3.06.SPA(Cisco NFVIS 4.12.1/4.12.2/4.12.3./4.12.4
	CIMC	CIMC 3.2.14.2.bin(Cisco NFVIS Release 4.12.1)
		CIMC 3.2.14.9.bin(Cisco NFVIS Release 4.12.2)
		CIMC 3.2.14.14.bin(Cisco NFVIS Release 4.12.3)
		CIMC_3.2.14.19.bin(Cisco NFVIS Release 4.12.4)
	WAN Port Driver	5.4.0-5-k CISCO
	LAN Port Driver	1.4.22.7-11-ciscocsx
C8300-UCPE-1N20	BIOS	C83uCPE_BIOS_1.00.SPA (Cisco NFVIS Release 4.12.1)
		C83uCPE_BIOS_1.03.SPA (Cisco NFVIS Release 4.12.2/4.12.3 /4.12.4)
	CIMC	CIMC_4.12.0.284R.bin (Cisco NFVIS Release 4.12.1
		CIMC_4.12.0.296R.bin (Cisco NFVIS Release 4.12.2/4.12.3)
		CIMC_4.12.0.302R.bin (Cisco NFVIS Release 4.12.4)

Guest VNFs

This section provides support statements for different guest Virtual Network Functions (VNFs) that you can run on Cisco Routing virtual platforms that are enabled by the Cisco NFVIS Release 4.12.1.

Cisco Router VNFs

Note

- Cisco provides deployment and configuration support for the VNF versions listed below, when these VNFs are deployed on Cisco Routing virtual platforms that are enabled by Cisco NFVIS Release 4.12.1.
- Cisco provides support on a case-by-case basis for unlisted combinations of Cisco NFVIS releases and VNF version combinations.

Table 2: Software Download Links

Product Homepage	Software Download
Cisco Catalyst 8000V Edge Software	17.12.8 17.12.7 17.12.6 17.12.5 17.12.4 17.12.3 17.12.2 17.12.1 17.11.1 17.10.1 17.9.3 17.9.1 17.8.1 17.7.1 17.6.3
Cisco vEdge	20.9.1 20.9.3 20.8.1 20.7.1 20.6.5 20.6.3

Table 3: Supported Linux Drivers for SR-IOV Acceleration

Platform	NIC	NIC Driver in NFVIS	Linux (Ubuntu/Alma) Drivers for SROV Interop
Cisco ENCS	Intel XL710 for chassis backplane switch	i40e Recommended Version: 1.4.22.7-12-ciscocsx	i40evf /iavf Recommended Version: 5.19.0-21-generic
	Intel I350 for GE0-0 and GE0-1 ports	igb Recommended Version: 4.18.0-372.9.1.el8.x86_64	igbvf Recommended Version: 5.19.0-21-generic
Cisco Catalyst 8200 Series Edge uCPE	Intel X553 1GbE - for GE0-0 and GE0-1 ports	ixgbe Recommended Version: 5.3.7-2 CISCO	ixgbevf Recommended Version: 5.19.0-21-generic
	Intel I350 - for GE0-2 to GE0-5 ports	igb Recommended Version: 4.18.0-372.9.1.el8.x86_64	igbvf Recommended Version: 5.19.0-21-generic
Cisco Catalyst 8300 Series Edge uCPE	Intel E810GE0-3 to GE0-64 x 10 G SFP+ ports	ice Version: 1.11.14	iavf Version: 5.15.64

Other Cisco Owned VNFs

Note

- Limited testing is done to ensure you can create a guest VM instance using the software download image for these versions, as posted on Cisco Software download page.
- For full-support statement see the individual product release documentation.

The following section provides information about generic Linux Distro Images (Ubuntu 22.10 & Alma 8.6 or similar) that can be deployed on Cisco NFVIS Release 4.12.1. See the above table for details on the SRIOV driver that is required on the guest Linux VM based on the platform.

Table 4: Software Download Links

Product Homepage	Software Download
Security VNFs	
Cisco NGFW (FTDv)	6.6.1-91 6.6.0-90
Cisco ASAv	9.14.2 9.14.1

Product Homepage	Software Download
WAN Optimization VNFs	
Cisco vWAAS	6.4.5a-b-50 6.4.5-b-75 6.4.3c-b-42

Non-Cisco Vendor Owned VNFs

You can run VNFs owned by various vendors on Cisco's NFV platforms enabled by NFVIS . Formal support for these VNFs requires a joint effort between Cisco and the VNF vendor.

Cisco offers VNF vendors a "for-fee" NFVIS 3rd-party certification program to test and certify their VNFs on Cisco's virtualized platforms. After testing and certification is complete, the results are published on this page- Cisco Enterprise NFV Open Ecosystem and Qualified VNF Vendors.

For more specific support details about VNF versions and test compatibility matrix with NFVIS releases, see the VNF release documentation on the vendor support site.

As a NFVIS customer, if you need a unique combination of NFVIS release and a specific VNF version, you may submit your certification request to Cisco at nfv-ecosystem@cisco.com or reach out to the VNF vendor support team asking them to initiate a certification on the Cisco platform.

Related Documentation

- Cisco Network Function Virtualization Infrastructure Software Getting Started Guide
- API Reference for Cisco Enterprise Network Function Virtualization Infrastructure Software
- Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide, Release 4.x
- Cisco Enterprise Network Function Virtualization Infrastructure Software Command Reference
- Release Notes for Cisco NFV SD-Branch features in Cisco vManage Release 20.12.x
- Design and Deployment Guide of Cisco NFVIS SD-Branch using Cisco SD-WAN Manager
- Cisco Catalyst 8200 Series Edge uCPE Data Sheet
- Cisco Cloud Services Platform 5000 Series Data Sheet
- Cisco 5400 Enterprise Network Compute System Hardware Installation Guide
- Cisco 5400 Enterprise Network Compute System Data Sheet
- Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM, Release 1.5.x
- Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources, Cisco SD-WAN Release 20.12.x

© 2023–2024 Cisco Systems, Inc. All rights reserved.