Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 4.9.x

First Published: 2023-03-30

Last Modified: 2024-02-29

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 4.9.3

Feature	Description
Change in default system memory for CSP devices	Starting from Cisco NFVIS 4.9.3 release, 8 GB is allocated to Cisco NFVIS in a CSP device with 64 GB memory space.
A new command to clear cache memory	The **`support flush cache memory`** command is introduced to clear cache memory using the CLI, that clears up some system memory to enable Cisco NFVIS to perform better. Clearing caches using support flush cache command can help resolve issues related to outdated or corrupted cache data. For example, clearing the cache in a web browser can help resolve issues such as slow page load times of Cisco NFVIS portal.

New and Enhanced Features for Cisco Enterprise NFVIS Release 4.9.1

Feature	Description
Cisco NFVIS Kubernetes Support	This feature enables you to deploy and operate Kubernetes as a VM using Cisco Enterprise NFVIS. You can download the NFVIS Kubernetes.tar.gz file, upload it to the Cisco Enterprise NFVIS and deploy the Kubernetes VM to leverage Kubernetes related technologies within Cisco Enterprise NFVIS.
VM Image Packaging Tool	The VM image packaging tool provides the UI for you to generate a full VM package, generate a scaffold package, and repackage. The tool works separately from the Cisco NFVIS system.

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 4.9.5

Resolved Bugs for Cisco Enterprise NFVIS Release 4.9.5

Identifier	Headline
CSCvo10155	Cisco NFVIS: TACACS+ session timeout is hardcoded and not user configrable
CSCwf50202	Cisco ENCS: Block transfer communication for TAM/sudi in SD-WAN Manager use case.

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.9.4

Resolved Bugs for Cisco Enterprise NFVIS Release 4.9.4

Identifier	Headline
CSCwe78888	Critical CVE in component spring-framework. Upgrade to latest version.
CSCwe21793	Duplicate Packets seen on CSP5400 Colo Cisco vManage Deployment

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.9.3

Resolved Bugs for Cisco Enterprise NFVIS Releases 4.9.3

Identifier	Headline
CSCwe10069	Cisco NFVIS flush built up cache/buffer
CSCwe13663	The Support RMA of devices on CSP.
CSCwe13710	New CLI to change default system memory

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.9.2

Resolved Bugs for Cisco Enterprise NFVIS Releases 4.9.2

Identifier	Headline
CSCwc66537	Cisco NFVIS SD-Branch: After "factory-default-reset all", the hostname shows "factory-reset"
CSCwc82388	Cisco NFVIS Release 4.9.1 CSP Call Trace i40e 0000:af:00.1: Unable to configure VFs, other operation is pending
CSCwc73891	Cisco NFVIS tech supprt generation caused disk space to rapidly fill up
CSCwc87753	Upgrade fail: Cisco NFVIS 4.6.3 to 4.9.1
CSCwd21993	VNF status is throwing an error, however VNF is up and running

Resolved and Open Bugs for Cisco Enterprise NFVIS Release 4.9.1

Resolved Bugs for Cisco Enterprise NFVIS Release 4.9.1

Bug ID	Description
CSCwc87753	Upgrade fail : NFVIS 4.6.3 to 4.9.1
CSCwd04322	Cisco Catalyst 8000V bin upgrade to 17.9.1a from 17.6.3a cause traffic fail on iavf interface while virtio works
CSCvz74003	Cisco Enterprise NFV Infrastructure Software Improper Signature Verification Vulnerability

Important Notes

- In Cisco NFVIS 4.6.1, backup with GE0-1-SRIOV-3 cannot be restored on ENCS 5400. For more details, see CSCvz82738.
- Cisco NFVIS 4.7.1 is the last release in which the **`system settings dns-server`** command is supported. We recommend that you use the **`system settings name-server`** command (supported

from NFVIS 4.4.1) instead of **system settings dns-server**, starting from NFVIS 4.8.1 and later releases.

- Cisco NFVIS 4.7.1 is the last release in which the **route-distribute** command is supported. We recommend that you use the **router bgp** command, instead of **route-distribute**, starting from Cisco NFVIS 4.8.1 and later releases. For more information on the **router bgp** command, see Configure BGP on NFVIS.
- Starting from Cisco NFVIS 4.7.1 and later releases, we recommend that you use the .iso file upgrade method to upgrade NFVIS. For more information on upgrading Cisco NFVIS, see Upgrade Cisco NFVIS.
- Starting from Cisco NFVIS 4.9.1 release, The memory reserved for Multi-NUMA node systems with more than 128 GB is increased to 20 GB in total. The memory reserved for Multi-NUMA node systems with more than 64 GB is increased to 10 GB in total.
- Cisco NFVIS 4.8.1 is the last release in which .nfvispkg file is published for upgrading the Cisco NFVIS devices.
- Starting from Cisco NFVIS 4.9.1 and later releases, use the .iso file upgrade method to upgrade NFVIS. For more information on upgrading Cisco NFVIS, see Upgrade Cisco NFVIS.
- If your Cisco NFVIS devices are running Cisco NFVIS Release 4.6.x and you are looking to upgrade to NFVIS Release 4.9.x using direct upgrade, we recommend that you use the Cisco-4.9.1-FC3.iso software image instead of Cisco-4.9.1-FC2.iso software image for a stable user experience.
- If your Cisco NFVIS devices are running Cisco NFVIS Release 4.9.1, upgraded using the Cisco-4.9.1-FC2.iso image, we recommend that you upgrade to Cisco-4.9.1-FC3.iso version of the software for a stable experience.
- Cisco NFVIS 4.9.x is the last supported Cisco NFVIS release for the following device platforms:
  - CSP-5216
  - CSP-5228
  - CSP-5436, CSP-5444, and CSP-5456
- Starting from Cisco NFVIS 4.9.3 release, 8 GB is allocated to Cisco NFVIS in a CSP device with 64 GB memory space.
- 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:

- 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

Platform	Firmware	Version
C8200-UCPE-1N8	BIOS	C8200-UCPE_1.04.103020201614
	MCU	240.52

Platform	Firmware	Version
ENCS 5406, ENCS 5408, and ENCS 5412	BIOS	ENCS54_3.06
		ENCS54_BIOS_3.06.SPA (Cisco NFVIS Release 4.9.4)
		ENCS54_BIOS_3.06.SPA (Cisco NFVIS Release 4.9.5)
	CIMC	CIMC_3.2.14.2.bin
		CIMC_3.2.14.6.bin (Cisco NFVIS Release 4.9.4)
		CIMC_3.2.14.13.bin (Cisco NFVIS Release 4.9.5)
	WAN Port Driver	ENCS54_BIOS_3.06.SPA
	LAN Port Driver	1.4.22.7-11-ciscocsx
CSP-5216 (last supported release)	BIOS	Use HUU 4.2(2a)
	CIMC	Use HUU 4.2(2a)
CSP-5228 (last supported release)	BIOS	Use HUU 4.2(2a)
	CIMC	Use HUU 4.2(2a)
CSP-5436, CSP-5444, and CSP-5456 (last supported release)	BIOS	Use HUU 4.2(2a)
	CIMC	Use HUU 4.2(2a)

Guest VNFs

This section provides support statements for different guest Virtual Network Functions (VNFs) that you can run on Cisco Routing virtual platforms enabled by the NFVIS 4.9.x release.

Cisco Router VNFs

Note

- Cisco provides support for deployment and configuration of the VNF versions listed below, when deployed on Cisco Routing virtual platforms, enabled by this release of NFVIS.
- Cisco provides support on a case-by-case basis for unlisted combinations of NFVIS release + VNF version.

Product homepage	Software download
Cisco Catalyst 8000V Edge Software	17.9.3 17.9.2 17.9.1 17.8.1 17.7.1 17.6.3
Cisco ISRv	17.3.5
Cisco vEdge	20.9.3 20.9.2 20.9.1 20.8.1 20.7.1 20.6.3 20.3.5

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.

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
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