Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 4.7.1

First Published: 2021-11-26

Last Modified: 2024-03-26

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 4.7.1

Feature	Description	Where Documented
Granular Role Based Access Control	This feature introduces a new resource group policy that manages the VM and VNF. You can now assign users to a group to control VNF access, during VNF deployment.	Granular Role Based Access Control
Enforce Setting of BIOS and CIMC Passwords	This feature enforces the user to change the default password for CIMC and BIOS.	Enforce Setting of BIOS and CIMC Passwords

Feature	Description	Where Documented
Support for 40G Dual Port and Quad-Split NICs in Cisco Cloud Services Platforms	Starting from this release, the 40G network interface card (NIC) supports dual port modes on Cisco Cloud Services Platform (CSP).	Support for 40G Dual Port and Quad-Split NICs in Cisco Cloud Services Platforms

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 Bugs for Cisco Enterprise NFVIS Release 4.7.1

Bug ID	Description
CSCvz09517	Out of memory (oom-killer): Stopping strobe of WDT monitoring BMC. Reset coming
CSCwa18012	VM remain shut post upgrade to 4.7 EFT
CSCwa04732	Portal Packaging UI: OIB when create VM package, show "Unknown" status and no further notification
CSCwa04530	Portal Packaging UI does not allow to specify mount point for bootstrap file
CSCwa04779	Portal OIB: when click Download Tech Support button, no further progress/status info. Kind of stuck.
CSCwa06000	Portal Packaging UI: "invalid value for: custom-property-key" error is seen when create VM package

Open Bugs for Cisco Enterprise NFVIS Release 4.7.1

Bug ID	Description
CSCwa25328	CSP port channel failure
CSCwa22991	Tabei: 4.6 to 4.7.0-78 cause error: "could not open network device int-CELL-1-0 (No such device)
CSCvz61055	SFP insertion/removal syslog request
CSCwa23058	switch ports and lan interface on ENCS failed to comeup after NFVIS upgrade.
CSCwa48902	The order to add remote user to resource group when local system having same user name

Important Notes

- In NFVIS 4.6.1, backup with GE0-1-SRIOV-3 cannot be restored on ENCS 5400. For more details, see CSCvz82738.
- 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.
- 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 NFVIS 4.8.1 and later releases. For more information on the **router bgp** command, see Configure BGP on NFVIS.
- Starting from NFVIS 4.7.1 and later releases, we recommend that you use the .iso file upgrade method to upgrade NFVIS.

Software Upgrade

The Cisco Enterprise NFVIS upgrade image is available as a *.nfvispkg* or *.iso* file. Currently, downgrade is not supported.

For more details on the software upgrade, see the Upgrading Cisco Enterprise NFVIS section in the https://www.cisco.com/c/en/us/td/docs/routers/nfvis/get_started/nfvis-getting-started-guide/m-upgrade-nfvis.html.

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 Platforms and Firmware

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

Platform	Firmware	Version
ENCS 5406, ENCS 5408, and ENCS 5412	BIOS	ENCS54_BIOS_3.04.SPA
	CIMC	CIMC_3.2.13.8
	WAN Port Driver	5.4.0-5-k CISCO
	LAN Port Driver	1.4.22.7-11-ciscocsx
ENCS 5104	BIOS	V010
	MCU	1.1
	WAN Port Driver	5.4.0-1-k, 0x80000f76
UCS-E160S-M3/K9	BIOS	UCSEM3_2.10
	CIMC	3.2(8.20190624114303)
UCS-E140S-M2/K9	BIOS	UCSES_1.5.0.8
	CIMC	3.2(8.20190624114303)
UCS-E160D-M2/K9	BIOS	UCSED_3.5.0.1
	CIMC	3.2(8.20190624114303)
UCS-E180D-M2/K9	BIOS	UCSED_3.5.0.1
	CIMC	3.2(8.20190624114303)
UCS-E180D-M3/K9	BIOS	UCSEDM3_2.10
	CIMC	3.2.11.5
UCS-E1120D-M3/K9	BIOS	UCSEDM3_2.10
	CIMC	3.2.11.5
UCSC-C220-M4S	BIOS	Use HUU 4.1(2f)
	CIMC	Use HUU 4.1(3d)
UCSC-C220-M5SX	BIOS	Use HUU 4.1(3b)
	CIMC	Use HUU 4.1(3b)
CSP-5216	BIOS	Use HUU 4.1(3d)
	CIMC	Use HUU 4.1(3d)

Platform	Firmware	Version
CSP-5228	BIOS	Use HUU 4.1(3d)
	CIMC	Use HUU 4.1(3d)
CSP-5436, CSP-5456, and CSP-5444	BIOS	Use HUU 4.1(3d)
	CIMC	Use HUU 4.1(3d)
C8200-UCPE-1N8	BIOS	C8200-UCPE_1.04.103020201614
	MCU	240.52

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 4.7.1 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	17.6.1a 17.5.1 17.4.1b
Cisco ISRv	17.3.3 17.3.2 17.3.1a 17.2.1r 16.12.4
Cisco vEdge	20.6.1 20.4.1 19.2.3

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