Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 4.5.1

First Published: 2018-03-01

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 4.5.1

Feature	Description	Where Documented
ENCS Switch Monitoring	This feature allows you to calculate the data rate for ENCS switch ports based on the data collected from the ENCS switch.	ENCS Switch Monitoring
Authentication Cache for External Authentication Server	This feature supports TACACS authentication through OTP on NFVIS portal	Authentication Cache for External Authentication Server

Feature	Description	Where Documented
BGP Route Annoucement over MPLS or IPSec	This feature allows you to configure NFVIS to announce routes through BGP over MPLS or in conjunction with secure overlay to announce routes over IPSec tunnel.	BGP Route Annoucement over MPLS or IPSec
Simplified Remote ID Configuration using EAP authentication	Remote ID configuration using EAP authentication is simplified. If the added security using a distinguished name is not required when using EAP authentication, then an FQDN can be configured on NFVIS to simplify the remote ID configuration and reduce authentication complexity.	Simplified Remote ID Configuration

NFVIS Portal Enhancements

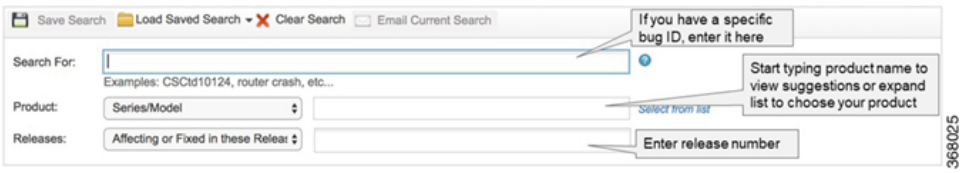
- The NFVIS portal pages are made consistent in terms of design.
- The menu is divided into different sections: **Configuration, Monitoring, Operations,** and **Notifications**.
- The time taken to reload a page is reduced. If you make changes in a page and reload the page, the previous existing details are displayed first and then the new changes are reflected.
- You can filter, sort and search for relevant information in all the tables. The entries in the table are sequentially arranged and can be refreshed at a tabular level.
- The **Network Design** canvas can be customized by rearranging the nodes.
- The pages on the portal can adapt to different screen sizes.

Open Bugs

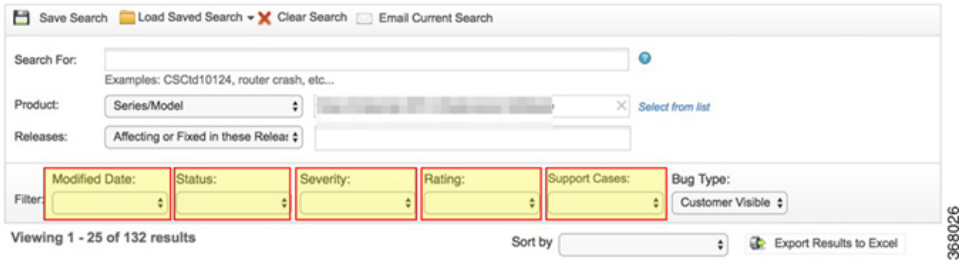
About the Cisco Bug Search Tool

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.



Open Bugs for Cisco Enterprise NFVIS Release 4.5.1

Caveat ID Number	Description
CSCvw44371	port channel doesn't allow to join pnic member when link status is not same
CSCvw84935	Portal shows non-existing VM objects in deploy page
CSCvx29111	NFVIS GUI session expires while image upload is still in progress
CSCvx42188	Restored system showed GE0-0 ARP failure cauing commnucation failure to headend
CSCvx52651	System-monitoring support for DPDK ports
CSCvx58175	show secure overlay command is not based on current actual status causing discrepancy
CSCvx66107	cpu usage causing huge packet drop over port channel (for non-hyperthreaded platform)
CSCvx70684	Multiple default SRIOV networks not seen after Factory reset
CSCvx72066	CSCP5456 i40 sometime down when dual mode 10G/1G Intel SFP connect to 1G Cisco SFP
CSCvx74858	Error=nfvis_105 Failed to update Error - cannot add non SRIOV physical NICs to non DPDK bridges
CSCvx79871	Error in Importing Images because of CDB lock by pnp with wan dhcp-ipv6 configuration.
CSCvx84761	ntpd NOT OK post upgrade from 4.4.2-FC2 4.5.1-FC1 on ENCS
CSCvx84899	4.5.1 upgrade fail with exception iso file missing mounting
CSCvx86101	DPDK custom bridge network access fail as bridge down

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.

Note NFVIS 4.5.1 supports incremental upgrade from NFVIS 4.4.x using .nfvispkg file.

NFVIS 4.5.1 supports direct one-step upgrade from NFVIS 4.2.x or NFVIS 4.4.x using .iso file.

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_2.13.SPA
	CIMC	CIMC_3.2.12.4
	WAN Port Driver	1.4.22.7-10-ciscocsx
	LAN Port Driver	5.4.0-3-k CISCO
ENCS 5104	BIOS	V010
	MCU	1.1
	WAN Port Driver	5.4.0-1-k, 0x80000f76

Platform	Firmware	Version
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
CSP-5228	BIOS	C220M5.4.0.4c.0.0506190754
	CIMC	4.1(1c)
CSP-5436, CSP-5456, and CSP-5444	BIOS	Use HUU 4.1(1c)
	CIMC	Use HUU 4.1(1c)
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 4.5.1 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	17.5.1 17.4.1b
Cisco ISRv	17.3.3 17.3.2 17.3.1a 17.2.1r 16.12.4
Cisco vEdge	20.4.1 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