

Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 4.4.1, 4.4.2

First Published: 2020-12-18

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 4.4.1

Feature	Description	Where Documented
Cisco Catalyst 8200 Series Edge Universal CPE Support	The Cisco Catalyst 8200 Series is the next generation of Cisco Enterprise Network Compute System platform that combines routing, switching and application hosting into a compact one rack unit device. These platforms are designed to allow customers to run virtualized network functions and other applications as virtual machines on the same hardware platform powered by Cisco NFVIS hypervisor software.	Supported Hardware Platforms On NFVIS Cisco Catalyst 8200 Series Edge uCPE Hardware Installation Guide

Feature	Description	Where Documented
SNMP VM Monitoring MIB	SNMP VM monitoring MIBs support added.	SNMP MIB Support
Live Export Support	Supports VM backup process without shutting down the VM.	VM Action APIs
VM Export with Selective Disk	You can exclude certain disks or volumes from a VM export.	VM Export with Selective Disk
BGP Support on NFVIS	This feature allows NFVIS system to learn routes announced from the remote BGP neighbor and apply the learnt routes to NFVIS system. This feature also allows you to announce or withdraw NFVIS local routes to the remote BGP neighbor.	BGP Support on NFVIS
Enhancements to Secure Overlay Feature	The secure overlay feature has been enhanced to allow an active or standby headend model by allowing FQDN for remote public IP address, and multiple sets of remote headend parameters. NFVIS can also learn local private tunnel IP address from the headend router. Secure overlay combined with BGP feature allows encryption to many learned remote subnets.	Secure Overlay and Single IP Configuration
DNS Name Server Configuration Enhancement	NFVIS allows configuring upto three nameservers which can be used by DNS resolvers in the order specified by the user. New command introduced to configure DNS nameservers: system settings name-server .	DNS Name Servers
CIMC Secure Overlay Support	This is a disaster recovery feature to recover an unresponsive NFVIS. CIMC periodically monitors NFVIS health and when NFVIS health check fails, CIMC establishes a secure tunnel to the remote. At remote site, you can login to CIMC and do the necessary troubleshooting to recover NFVIS.	CIMC Secure Overlay Support

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 4.4.2

Caveat ID Number	Description
CSCvw95411	Add support for NFVIS ISO upgrade from base version 4.2.2
CSCvx02516	Add a command to Clear the BIOS password for C8200-UCPE-1N8

Open Bugs for Cisco Enterprise NFVIS Release 4.4.1

Caveat ID Number	Description
CSCvw33608	4.2 to 4.4 upgrade : system is not accessible via customer bridge
CSCvw70486	4.4.1-FC2 iso_upgrade Caught exception for reboot Command '/usr/sbin/reboot' failed.Exit status:-15
CSCvv21961	BGP path attribute AS-Path not correct
CSCvw01593	C8200-UCPE-1N8 and CSP5444 SNMPv2-SMI::mib-2.47.1.1.1.1.2.1 = STRING: "Unsupported
CSCvs16513	C8200-UCPE-1N8 doesn't allow to create VRRP group for interface GE0/2~GE0/5
CSCvs90718	C8200-UCPE-1N8 LTE:show cell network shows wrong info for some areas and need enhancement for others

Caveat ID Number	Description
CSCvs96939	C8200-UCPE-1N8 LTE:when have SIM in both slots, show cell status shows SIM in slot 1 as Not inserted
CSCvr15262	C8200-UCPE-1N8 LTE PIM: show cellular output takes some time to display
CSCvr33531	C8200-UCPE-1N8 LTE PIM: When IP address changes, show cellular sometimes shows stale IP address info
CSCvt22057	C8200-UCPE-1N8 LTE PIM: Wrong FW version message displayed when FW upgrade was successful
CSCvw60648	C8200-UCPE-1N8 watchdog timer does not work
CSCvw29857	CSP5444 Dynamic SRIOV on i40e problem
CSCvw65247	CSP5444 lldp doesn't return hostname unlike other platform ENCS Tabei
CSCvw72019	CSP5444 undeploying c8kv took 5 hours.
CSCvw52857	CSP5444 vmExport to usb failure
CSCvw55682	ENCS : vEdge20.4-206: traffic failure post pnic GE0-0 down/up as ARP failed on GE0-0-SRIOV
CSCvw76861	FC2 image: SS - LTE PIM cannot ping out upon fresh install - impacts PnP and Console Connection
CSCvw89859	Machine goes into endless cycle of reboots if upgraded from NFVIS-4.2 to NFVIS-4.4
CSCvw37603	ND template stay in DB when no branch associated to and cause image delete failure
CSCvw76910	NFVIS: occasional VMMIB walk failure wile system under high CPU load
CSCvw73924	NFVIS4.4.1-FC2 vmExport/vmImport with NGIO enabled will make VM Error
CSCvw95039	NFVIS 4.4.1 - nginx error on pnp certificate install - 502 Bad Gateway
CSCvw37290	NFVIS B&R: host restore failed to register raw disk format
CSCvw80381	NFVIS-ESC-LITE: B&R failure caused due to backup'ed image include other image disk
CSCvw76005	NFVIS-ESC-LITE: Virtual disk size is not equal to provisioned for thick provisioned VM
CSCvv35838	NFVIS-ESC-LITE: vmExportAction create folder under / for invalid exportPath
CSCvx19599	NFVIS-ESC-LITE: VM is not recoverable after vmExportAction due to lack of disk space
CSCvw75228	NFVIS PORTAL: Portal did not prevent VM backup with the identical name as VM name

Caveat ID Number	Description
CSCvw74089	NFVIS PORTAL: Portal did not show error msg if two vmExport runs in parallel for same VM
CSCvw49216	NFVIS Upgrade traceback: [FIRMWARE-UPDATE:] Error=upgrade_302 Caught Exception in Upgrade Apply
CSCvr86873	No syslog generated for VM_BACKUP_XXX notifications
CSCvw83479	Out of memory (oom-killer): Stopping strobe of WDT monitoring BMC. Reset coming
CSCvw74071	OVS error: "could not open network device GE0-1_I11 (No such device)"
CSCvw77135	OVS error: error: "could not open network device vnic1 (No such device)"
CSCvw77197	PIM LTE Port can be removed but can't be added
CSCvw68443	pnic track in ENCS port channel is not accepted
CSCvw07747	Portal is accessible w/o providing username/password more than 5 hours later
CSCvw44371	port channel doesn't allow to join pnic member when link status is not same
CSCvw49508	removing member from port channel doesn't reflect
CSCvw66744	SecureOverlay: Default Route lost in table 220 after failover
CSCvv49034	Secure Overlay: Tunnel in error when parameters list out of order
CSCvv59694	secure overlay default route solution does not work with system routes
CSCvv50300	secure overlay restoration failed via hostaction restore
CSCvw49143	show port-channel doesn't return correct output
CSCvv16807	SNMP Error=snmp_104 Unexpected value sensor_values
CSCvw50644	snmpwalk Error=nfvis_101 snmp_ifmib_walk Caught Exception:: Issue due to upgrade
CSCvw51160	snmpwalk Error=nfvis_101 snmp_ifmib_walk Caught Exception due to port-channel
CSCvw32055	system reboot twice after upgrade applied with traffic and subsystem stop issue for 12 hours
CSCvv86089	VM cannot detect LLDP packets coming from external network when connected through OVS bridge
CSCvv94066	VMs became paused post 4.4.1 upgrade when remaining NFVIS system disk space is marginal.
CSCvw31738	ZTP vBranch Solution: Tabei PIM LTE fail on PnP redirect when wan-br/wan2-br get DHCP IP and gateway

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.

ISO File Upgrade

- NFVIS 4.4.1 supports upgrade from NFVIS 4.2.x using *.nfvispkg* file. If the NFVIS 4.2.x is newly installed, then it supports upgrade to NFVIS 4.4.1 using *.iso* file.
- Newly installed NFVIS 4.4.1 supports upgrade to a later version of NFVIS 4.5 or NFVIS 4.6 using a *.iso* file.
- Skipped version upgrade with baseline NFVIS 4.4 to NFVIS 4.6 is only supported with a *.iso* file, not a *.nfvispkg* file.
- The *.iso* file upgrade requires an extra space of 8 GB, for rollback. The following table shows the amount of space required for rollback for the corresponding installation disk space:

Installation Disk Space	Space Required for Rollback
<32 GB	6.75 GB
32 GB - 128 GB	9.5 GB
>128 GB	11 GB

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_2.12.SPA
	CIMC	CIMC_3.2.11.4
	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
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(8.20190624114303)
UCS-E1120D-M3/K9	BIOS	UCSEDM3_2.10
	CIMC	3.2(8.20190624114303)
UCS-C220-M4	BIOS	3.0.3a
	CIMC	3.0(3c)

Platform	Firmware	Version
CSP-2100-X1	BIOS	3.0.3a
	CIMC	3.0(3a)
UCS-C220-M5	BIOS	C220M5.3.1.3c.0.0307181404
	CIMC	3.1(3a)
CSP-5228	BIOS	C220M5.4.0.4c.0.0506190754
	CIMC	4.1(1c)
CSP-5436 and CSP-5444	BIOS	Use HUU 4.1(1c)
	CIMC	Use HUU 4.1(1c)

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 4.4.1 and NFVIS 4.4.2 releases.

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	17.4.1b
Cisco ISRv	17.3.2
	17.3.1a
	17.2.1r
	16.12.4
	16.12.5
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)	6.6.0-90 6.5
Cisco ASAv	9.14.1 9.12.1
WAN Optimization VNFs	
Cisco vWAAS	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](#)

