

# Release Notes for Cisco Enterprise Network Function Virtualization Infrastructure Software, Release 3.12.x

---

**First Published:** 2020-01-31

**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 3.12.3

- Secure Tunnel enhancements for PKI and EAP
- APC UPS support
- SNMP support for CPU usage
- AAA auth-order
- Console login when NFVIS down

### New and Enhanced Features for Cisco Enterprise NFVIS Release 3.12.2

- ENCS 5400 supports 24 LAN SRIOV networks.

### New and Enhanced Features for Cisco Enterprise NFVIS Release 3.12.1

- DPDK enhancements
  - ENCS PMD driver support
  - Migration for VMs with PNIC associated to DPDK bridge
  - Service bridge extension to platforms: UCSC, UCSE, CSP
  - Non-ENCS DPDK PMD driver support
- Dynamic SR-IOV support on UCSC-M5, UCSE-M3, and CSP platforms
- ENCS 5400 supports 12 LAN SRIOV networks.

## 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.

### Open Bugs for Cisco Enterprise NFVIS Release 3.12.3

Caveat ID Number	Description
<a href="#">CSCvr49551</a>	PNIC track state does not sustain after Power cycle
<a href="#">CSCvr64064</a>	NFVIS AAA AUTH-ORDER: same user id can login to NFVIS with either local or tacacs password.
<a href="#">CSCvr83044</a>	NFVIS: "factory-reset all" failed if we have VM added volume on NFS
<a href="#">CSCvr93504</a>	ERROR: Class:3000000; Subclass:50000; Operation: D

Caveat ID Number	Description
<a href="#">CSCvs44341</a>	All configs for s/w on ENCS is intact after factory reset(except images and connectivity)
<a href="#">CSCvs45600</a>	NFVIS - 3.12.3 RC5 - SPAN stops working after reboot the VM
<a href="#">CSCvs57164</a>	Traffic fail on lan-net with dpdk enabled after upgrade
<a href="#">CSCvs70784</a>	3.12.3-FC1: Upgrade Status Invalid
<a href="#">CSCvs71064</a>	3.12.3-FC1 - vnic not coming up when there is an error in track-state configuration
<a href="#">CSCvs79898</a>	Unable to do pnp on ENCS 3.12.3 RC9 using MSX to set admin password, potential Confid issue

### Resolved Bugs for Cisco Enterprise NFVIS Release 3.12.2

Caveat ID Number	Description
<a href="#">CSCvq66963</a>	Change in NFVIS 3.12.1 platform-detail API cause NFVIS Devices 'Partial Collection Failure' on DNAC
<a href="#">CSCvq82509</a>	Handle TACACS encrypted shared-secret with \\
<a href="#">CSCvq86428</a>	PNIC ALLMULTI is changed to off when PNIC SRIOV switchmode VEB is configured.
<a href="#">CSCvq91412</a>	Increase LAN-SRIOV network number to 24 on encs
<a href="#">CSCvq93639</a>	Switch daemon - Restart failed due to unclosed socket
<a href="#">CSCvq94002</a>	NFVIS SNMPTrap is not generated
<a href="#">CSCvq94855</a>	Application error after performing "factory-default-reset all" action post NFVIS 3.12.1 FCS upgrade

### Open Bugs for Cisco Enterprise NFVIS Release 3.12.1

Caveat ID Number	Description
<a href="#">CSCvo84097</a>	Frame errors on some ENCS5400 units that causes OS2BMC channel to be DOWN
<a href="#">CSCvq35365</a>	Cannot Disable/Enable SRIOV on interface eth2-1 to eth2-4 with driver i40e on UCS-CM5
<a href="#">CSCvq48983</a>	Getting error when dragging the VM and connecting the links too quickly
<a href="#">CSCvq49883</a>	ISRv with SRIOV goes to ERROR state after VM restart, reboot, or upgrade if pnic is admin down
<a href="#">CSCvq51263</a>	Portal Switch page takes up to 20 seconds to load or refresh
<a href="#">CSCvq56915</a>	ping fail after update vnic from lan-sriov to lan-br on encs

Caveat ID Number	Description
<a href="#">CSCvq59803</a>	Factory Reset Except-Images gives error after enabling sriov with maxvfs and cant login after that
<a href="#">CSCvq65951</a>	Delete rbac user "administrator" (role:admin) and cause vbmd service NOT OK after NFVIS reboot

## Limitations with Host Driver on ENCS Platforms

When the interface is shutdown in an ISRv VM the input packet count increases. This is an Intel firmware and host driver defect. When the interface is shutdown on the ISRv VM, the i40e VF driver sends a message to the i40e PF host driver to delete the MAC filters. This stops the shutdown interface from receiving unicast traffic. However for ISRv, if the multicast and broadcast promiscuous mode is set on the VF, it allows the multicast and broadcast packets to be received on the VF. Since there is no specific command to the firmware from the host driver which indicates to the firmware that the VF is shutdown, the system continues to receive multicast and broadcast packets.

## Software Upgrade

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

For more details on the software upgrade, see the Upgrading Cisco Enterprise NFVIS section in the [Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide](#).




---

**Note** NFVIS 3.12.3 supports upgrade from NFVIS 3.11.x.

---

## 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_2.9.SPA
	CIMC	CIMC_3.2.9.bin
	WAN Port Driver	1.63-0x80000e2f
	LAN Port Driver	5.04-0x80004abc
ENCS 5104	BIOS	V010
	MCU	1.1
	WAN Port Driver	5.2.20-k/1.63, 0x80000f76
UCS-E160S-M3/K9	BIOS	UCSEM3_2.6
	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_2.6
	CIMC	3.2(8.20190624114303)
UCS-E1120D-M3/K9	BIOS	UCSEDM3_2.6
	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	4.0(4c)
CSP-5436	BIOS	C240M5.4.0.1c.0.0627180945
	CIMC	4.0(1a)

## Supported VMs

The following table lists the verified versions of supported VMs for NFVIS 3.12.x release:

VM	Version
Cisco ISRv	16.10.2
	16.11.1b
	16.12.1
Cisco ASA v	9.12.1
Cisco vWAAS	6.4.3b-b-53
Cisco NGFWv	6.3.0-83
Viptela vEdge	18.4.1
cEdge	16.10.2
eWLC	16.10.1
ThousandEyes	Agent 1.27.4
Fortinet	Fortigate 5.6.2
PaloAlto	PAN-OS 8.0.5
InfoVista	Ipanema VNF vipe_kvm v9.1.6.6
CTERA	6.0.4



**Note** Windows and Linux VMs are also supported.

## 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](#)

