

Deployment planning

Objective

Consult the Release Notes for the version of NFVIS you will deploy: https://www.cisco.com/c/en/us/support/routers/enterprise-nfv-infrastructure-software/products-release-notes-list.html.

- Architecture, topology and management interfaces, on page 1
- Hardware support & readiness, on page 2
- Host system requirements, on page 3
- NFVIS licensing readiness, on page 4
- NFVIS networking readiness, on page 4
- Application support & readiness, on page 6
- Security readiness, on page 8
- Install readiness, on page 8

Architecture, topology and management interfaces

Objective

Cisco NFVIS is deployed as a standalone virtualization host for local virtual machine workloads.

Host topology and management interfaces

Additional hosts may be deployed to provide hardware/workload redundancy, additional capacity for application scale, geographic coverage or other customer requirements.

Each Cisco NFVIS host may be managed via multiple interfaces:

- NFVIS Portal (GUI), accessed through a web browser using the local ethernet management network connection
- NFVIS CLI, access through SSH. One host may access the CLI of another host.
- NFVIS NETCONF/RESTCONF APIs (see https://developer.cisco.com/docs/nfvis/, these can be used to build centralized management dashboards for multiple hosts)

Before you can use any of these management interfaces, you will need to complete installation, then configure management network access.

Hardware support & readiness

Cisco NFVIS is only supported on specific hardware platforms with specific configurations. NFVIS is only supported on the Cisco Calling Appliances listed in Table 1 below, along with the minimum required NFVIS release for each appliance model/generation. If you are doing a fresh install on an appliance, or a rebuild of a supported appliance, see their install guides below:

- Cisco Business Edition 6000 Install and Upgrade Guides at https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/products-installation-guides-list.html
- Cisco Business Edition 7000 Install and Upgrade Guides at https://www.cisco.com/c/en/us/support/unified-communications/business-edition-7000/products-installation-guides-list.html
- Cisco Expressway CE1400V Appliance Installation Guide at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/install_guide/CE1400V/exwy_b_cisco-expressway-ce1400v-appliance-installation-guide.html

Supported appliances require UCS BIOS and CIMC settings compatible with NFVIS. See the Supported Hardware section of the Release Notes for the NFVIS version you are deploying.

Expect installation problems and other issues if you attempt to install NFVIS on unsupported hardware. The only fix will be to get onto a supported calling appliance hardware configuration.

Table 1: Supported Calling Appliance Models

Cisco Calling Appliances	Models / Generations	Supported Base PIDs	First introduced in this NFVIS Release
Cisco Business Edition 6000	BE6000M (M7)	BE6K-M7-K9 BE6K-M7-XU	4.18.2a
Cisco Business Edition 6000	BE6000M (M6)	BE6K-M6-K9 BE6K-M6-XU	4.18.2a
Cisco Business Edition 6000	BE6000M (M5)	BE6M-M5-K9 BE6M-M5-XU	4.18.2a
Cisco Business Edition 6000	BE6000H (M5)	BE6H-M5-K9 BE6H-M5-XU	4.18.2a
Cisco Business Edition 7000	BE7000M (M7)	BE7M-M7-K9 BE7M-M7-XU	4.18.2a
Cisco Business Edition 7000	BE7000M (M6)	BE7M-M6-K9 BE7M-M6-XU	4.18.2a
Cisco Business Edition 7000	BE7000M (M5)	BE7M-M5-K9 BE7M-M5-XU	4.18.2a

Cisco Calling Appliances	Models / Generations	Supported Base PIDs	First introduced in this NFVIS Release
Cisco Business Edition 7000	BE7000H (M7)	BE7H-M7-K9 BE7H-M7-XU	4.18.2a
Cisco Business Edition 7000	BE7000H (M6)	BE7H-M6-K9 BE7H-M6-XU	4.18.2a
Cisco Business Edition 7000	BE7000H (M5)	BE7H-M5-K9 BE7H-M5-XU	4.18.2a
Expressway CE1400V	CE1400V (M7)	CE1400V-M7-K9	4.18.2a

Host system requirements

Objective

These resources are required for a standalone Cisco NFVIS. A summary quick-reference table by calling appliance model is in the Virtualization Guide for On-premises Calling at Cisco Virtualization Guide for Cisco On-premises Calling Applications.

NFVIS host resource requirements

Total Cores	NFVIS 4.18.2a and later Releases
16 or less	1 + (1 core per socket applicable to DPDK systems)
More than 16	2 cores in NUMA-0 1 core in NUMA-1 (if Multi-NUMA node system*) (1 core per socket applicable to DPDK systems)

* Indicates that Multi-NUMA node systems require an additional CPU core system reserved. This additional core is helpful in processing the cross NUMA nodes, indirectly improving the performance of Cisco NFVIS functions on the system cores.

Table 2: CPU allocation

Reserved System Memory	Up to 16 GB	Up to 32 GB	Up to 64 GB	Up to 128 GB	Greater than 128 GB	Greater than 256 GB
Reserved for NFVIS	7 GB/ 8 GB*	11 GB/ 12 GB*	11 GB/ 12 GB*	11 GB/ 12 GB*	11 GB/ 13 GB*	16 GB/ 20 GB*

If hyper-threading is enabled on the device, each core reflects two logical CPUs.

* Indicates the memory allocation is applicable only for Multi-NUMA node systems. In case of single node systems, the memory allocation values without * is applicable.

Table 3: Memory allocation

Total System Memory	Additional memory required for DPDK support per NUMA node
Upto 63 GB	1
64 GB - 127 GB	2
128 GB - 256 GB	4

NFVIS licensing readiness

Cisco NFVIS is a paid product and requires an active subscription for entitlement to use the product, receive technical support from Cisco TAC and gain access to feature/maintenance releases.

- To ensure this required subscription is in order, Cisco Partners can consult the Cisco Business Edition 6000/7000 Ordering Guide.
- A valid, active subscription will appear in Cisco Commerce Subscriptions & Services as a Subscription ID with product name A-NFVIS-COLLAB, with a quantity of L-LIC-COLLAB Items matching the quantity of calling appliances in the deployment.

Cisco NFVIS uses Cisco Smart Licensing to manage entitlement to product usage, support, upgrades and updates.

- To license NFVIS, you require an active Cisco Smart Account. For more information on Smart Account, see, How to Request a Smart Account
- NFVIS only supports certain Smart Licensing modes.
- NFVIS enforces licensing, including a Grace Period and Compliance Mode (where admin goes read-only).
- For more details on Cisco Smart Licensing for NFVIS, see details in Chapter 6 –Cisco Smart Licensing for NFVIS.

NFVIS networking readiness

NFVIS connects virtual network functions (VNFs) to one another and to physical network ports. It does this by attaching each VNF's virtual NIC to a network configured in NFVIS. Only two ways to provide that connectivity are Open vSwitch (OVS) and SR-IOV.

Open vSwitch (OVS)

OVS is a software switch running on the NFVIS host. It forwards traffic between virtual machine virtual NICs and, through bridges, physical NICs or port channels. NFVIS uses bridges as virtual switches and networks to define which connections a virtual machine can use, including options such as VLAN settings.

For example, two virtual machines attached to the same OVS network can communicate through the bridge. A bridge connected to a physical port can also carry their traffic to or from the external network. Because NFVIS handles this switching, OVS is flexible for connecting virtual machines and applying network configuration.

SR-IOV concepts

Objective

SR-IOV lets a supported physical NIC expose multiple Virtual Functions (VFs). NFVIS can assign a VF to a virtual machine, giving it a more direct path to NIC hardware. The NIC's Physical Function (PF) provides and manages those VFs.

OVS and SR-IOV networking behavior

This direct path can improve throughput and reduce latency and host CPU work, which can suit virtual machines with demanding traffic requirements. It depends on a compatible NIC and VNF driver, and the number of available VFs is limited by the hardware. NFVIS lets you enable SR-IOV on a physical NIC and create SR-IOV networks for VNF assignment.

In short, OVS is the general-purpose virtual switching path; SR-IOV gives a virtual machine a more direct hardware networking path when performance is the priority. Some deployments use both—for example, SR-IOV for a virtual machine's external-facing interface and OVS networks for its connections to other virtual machines.

Default system configuration

Default system configuration is a network setup that

- configures networks in Cisco NFVIS to allow inbound and outbound traffic
- creates default networks and bridges that cannot be deleted.

This diagram illustrates the default network configuration:

Figure 1. Default network configuration



These networks and bridges are created by default and cannot be deleted. You can configure more as required:

- A LAN network (LAN-net) and a LAN bridge (LAN-br)—The default static management IP address (192.168.1.1) for the NFVIS host is configured on the LAN bridge. One of the ports for inbound and outbound traffic are associated with the LAN bridge. Any LAN port can be used to access the default static IP address. By default, the hostname is set to "NFVIS".
- A WAN network (WAN-net) and a WAN bridge (WAN-br)—This is created with the "eth0" port, and is configured to enable the DHCP connection.

By default, the first port on the device is associated with the WAN bridge. One of the other ports on the device are associated with the LAN bridge.

Application support & readiness

Objective

This reference groups information about Application Support & Readiness, including Supported Applications, Finding Application Files, VM Placement Planning.

Supported applications

Objective

Cisco NFVIS only supports select Cisco Collaboration workloads in the Table below, which lists the first release when support for that application was added. For compatibility of applications with subsequent releases, see the document indicated by the table.

Supported applications and release compatibility

Unlisted applications/workloads are not supported for hosting on NFVIS (and are not expected to install / boot / operate properly due to lack of enablement in NFVIS for their particular software contents).

See the Release Notes for NFVIS 26.2 for which applications are supported.

Table 4: Supported Applications/Workloads

Category	Application /Workload	First i ntroduced in this NFVIS Release	Check here for Application / NFVIS compatibility matrix
On-premises Calling	Cisco Unified Communications Manager (CUCM)	4.18.2a **Note** not supported on 26.2.1 at this time.	c
On-premises Calling	Cisco Unified CM Session Management Edition (SME)	4.18.2a **Note** not supported on 26.2.1 at this time.	c
On-premises Calling	Cisco Unified CM – IM & Presence Service (IMP)	4.18.2a **Note** not supported on 26.2.1 at this time.	c
On-premises Calling	Cisco Unity Connection (CUC)	4.18.2a **Note** not supported on 26.2.1 at this time.	c

Category	Application /Workload	First i ntroduced in this NFVIS Release	Check here for Application / NFVIS compatibility matrix
On-premises Calling	Cisco Emergency Responder (CER)	4.18.2a **Note** not supported on 26.2.1 at this time.	c
On-premises Calling	Cisco Expressway (Expwy)	4.18.2a **Note** not supported on 26.2.1 at this time.	c
On-premises Meetings	Cisco Meeting Server (CMS)	26.2.1	Virtualization for Cisco Meeting Server at
On-premises Meetings	Cisco Meeting Management (CMM)	26.2.1	Virtualization for Cisco Meeting Server at
On-premises Contact Center	Unified Contact Center Express suite (UCCX)	26.2.1	Virtualization for Cisco Unified Contact Center Express at
On-premises Contact Center	Cisco Customer Collaboration Platform (CCP)	26.2.1	Cisco Customer Collaboration Platform Installation and Upgrade Guide, Release 15.0 SU1 or later at
Webex Calling	Cisco Webex Calling Dedicated Instance Enhanced Survivability Node (DI ESN)	4.18.2a **Note** not supported on 26.2.1 at this time.	Enhanced Survivability prerequisites, Virtualization specification
Webex Edge	Cisco Webex Edge Video Mesh Node (VMN)	26.2.1	Deployment Guide for Video Mesh at

Category	Application /Workload	First i ntroduced in this NFVIS Release	Check here for Application / NFVIS compatibility matrix
Webex Key Management Service (KMS)	Cisco Webex Hybrid Data Security (HDS)	26.2.1	Virtual Host Requirements, Deployment guide for Webex Hybrid Data Security

Finding application files

Objective

NFVIS requires Images and Profiles to create and deploy virtual machines. For the files each application provides for use with NFVIS, see their Installation Guides (Cisco Virtualization Guide for Cisco On-premises Calling Applications and other documents).

VM placement planning

Objective

An NFVIS host will have a system requirements holdback on physical hardware capacity for its needs. Cisco Collaboration applications also have “rules” for VM placement and minimum hardware specs to be supported.

VM placement planning considerations

Note “vcpu” term usage may differ in NFVIS monitoring screens vs. as used in application VM specs definitions and VM Placement rules.

Security readiness

At a minimum, after fresh install, you will immediately be prompted to change default login credentials

To review NFVIS credential policies, and other security-related items you may want to handle immediately after install, see NFVIS security considerations

Install readiness

Install is dependent upon:

1. Location of the NFVIS software image on the network, relative to where the destination calling appliance is located. For example, uploading NFVIS image remotely via staging NFVIS on a server on the same LAN as the calling appliance may have drastically different durations.
2. Storage and network speed of whatever is hosting the NFVIS software image. E.g. your laptop may be slower than a server.

Depending on above factors, NFVIS fresh installation can take 30-120 minutes before the system is ready for first-time-setup and configuration. For fastest install, stage the NFVIS image on the same LAN as the calling appliance, on a server with fast storage and fast network.