Install Cisco Enterprise NFVIS

This chapter describes how to install Cisco NFVIS through Cisco IMC and USB for the supported hardware platforms.

Install NFVIS Through CIMC

Install NFVIS on ENCS 5400 Platform

Software or hardware RAID controller setup is not supported on Cisco ENCS 5400 platform devices. NFVIS is not installed on RAID disk group. RAID disk group on ENCS 5400 platform devices is used for extdatastore only.

Step 1 Log in to CIMC.

The recommended CIMC version for ENCS 5400 platforms is 3.2(7) or later version.

Step 2 To launch KVM Console, Select **Launch KVM** from the CIMC homepage.

You can choose Java or HTML based KVM. It is recommnded to use HTML based KVM. Ensure that the pop-up blocker is disabled as KVM Console opens in a separate window.

Step 3 To map virtual media from the KVM Console:

a) To know if a downloaded file is safe to install, it is essential to compare the file's checksum before using it. Verifying the checksum helps ensure that the file was not corrupted during network transmission, or modified by a malicious third party before you downloaded it. For more information see, Virtual Machine Security.

b) Select **Virtual Media** and then **Activate Virtual Devices**.

c) Select **Virtual Media** again and then **Map CD/DVD**. Browse and select the Cisco Enterprise NFVIS ISO image. Click **Open** and Map Drive to mount the image.

d) Select **Virtual Media** again to ensure the NFVIS ISO image is now mapped to CD/DVD.

Step 4 To configure Boot Order:

a) From the **CIMC Compute**, select **BIOS**.

b) Select **Configure Boot Order** and the **Configure Boot Order** dialog box appears.

c) From the **CD/DVD** page, select **Cisco vKVM-Mapped vDVD**, and select **Add**.
d) From **HDD**, select **RAID Adapter**, and then click **Add**.
a) Set the boot order sequence using the **Up** and **Down** options. The **Cisco vKVM-Mapped vDVD** boot order must be the first choice. **Save Changes** to complete the boot order setup.

Note To configure Boot Order for UEFI through CIMC, the supported BIOS version is 2.10 or later. If any other BIOS version is used, you must configure UEFI Boot Order through the BIOS setup menu and set **BootOrderRules** to **Loose**.

To configure Boot Order for UEFI:

a) From the **CIMC Compute**, select **BIOS**.
b) Select **Configure Boot Order** and the **Configure Boot Order** dialog box appears.
c) Use >>, <<, **up** and **down** buttons to make **UEFI Image Map** as the first option in the right-hand column of the user interface.
d) Use the >>, <<, **up** and **down** buttons again to make **UEFI OS** as the second option in the right-hand column of the user interface.
e) Click **Save changes**.

You can also configure Boot Order for UEFI using CLI. The following is an example to configure Boot Order for UEFI using CLI:

```
Server# scope bios
Server /bios # set boot-order uefimap,uefios
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
- If a specified device type is not seen by the BIOS, it will be removed
  from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
  The configured list will be appended by the additional device types
  seen by the BIOS
Server /bios *# commit
Server /bios #
Server /bios # show detail
BIOS:
    BIOS Version:"UCSEDM3.2.10b5 (Build Date:02/27/2020)"
    Boot Order: UEFIMAP,UEFIOS
    FW Update/Recovery Status: None, OK
    Active BIOS on next reboot: main
    UEFI Secure Boot: enabled
```

Step 5 Power cycle server to start the installation:

From CIMC homepage, select **Host Power**. Reboot the server by selecting the **Power Off** option. After the server is down, select the **Power On** option.

When the server reboots, the KVM console automatically installs Cisco Enterprise NFVIS from the virtual CD/DVD drive. The entire installation might take 30 minutes to one hour to complete.

Step 6 For ENCS 5400 platforms, auto-upgrade the firmware.

Starting from NFVIS 3.8.x release, firmware auto-upgrade is supported. After the NFVIS installation is complete, BIOS or CIMC is upgraded to the corresponding versions automatically. CIMC and NFVIS is rebooted multiple times. The firmware upgrade might take 30 minutes to one hour to complete. Do not use the system during the firmware upgrade.

Step 7 After the installation is complete, the system automatically reboots from the hard drive. Log into the system when the command prompt **nfvis login** is displayed after the reboot.

Use **admin** as the login name and **Admin123#** as the default password.

Note The system prompts you to change the default password at the first login attempt. You must set a strong password as per the on-screen instructions to proceed with the application. You cannot run API commands or proceed with any tasks unless you change the default password at the first login. API returns a 401 unauthorized error if the default password is not reset.

Step 8 Verify the installation using the System API, CLI, or by viewing the system information from the Cisco Enterprise NFV portal.

Step 9 Configure hostname and assign a management IP address to access NFVIS.

Connect ethernet management port to the network for management access. To enable IP address based access over ethernet for NFVIS, use the serial console connection port.

Default System Configuration on the Cisco ENCS

The diagram below illustrates the default network configuration of Cisco Enterprise NFVIS with the Cisco ENCS.

Figure 1: Default Network Configuration of Cisco Enterprise NFVIS with the Cisco ENCS 5400

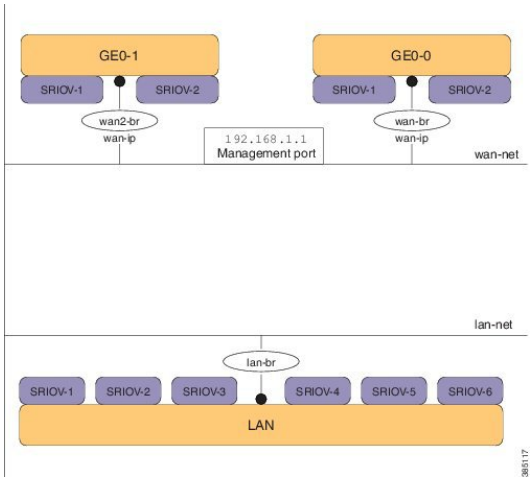
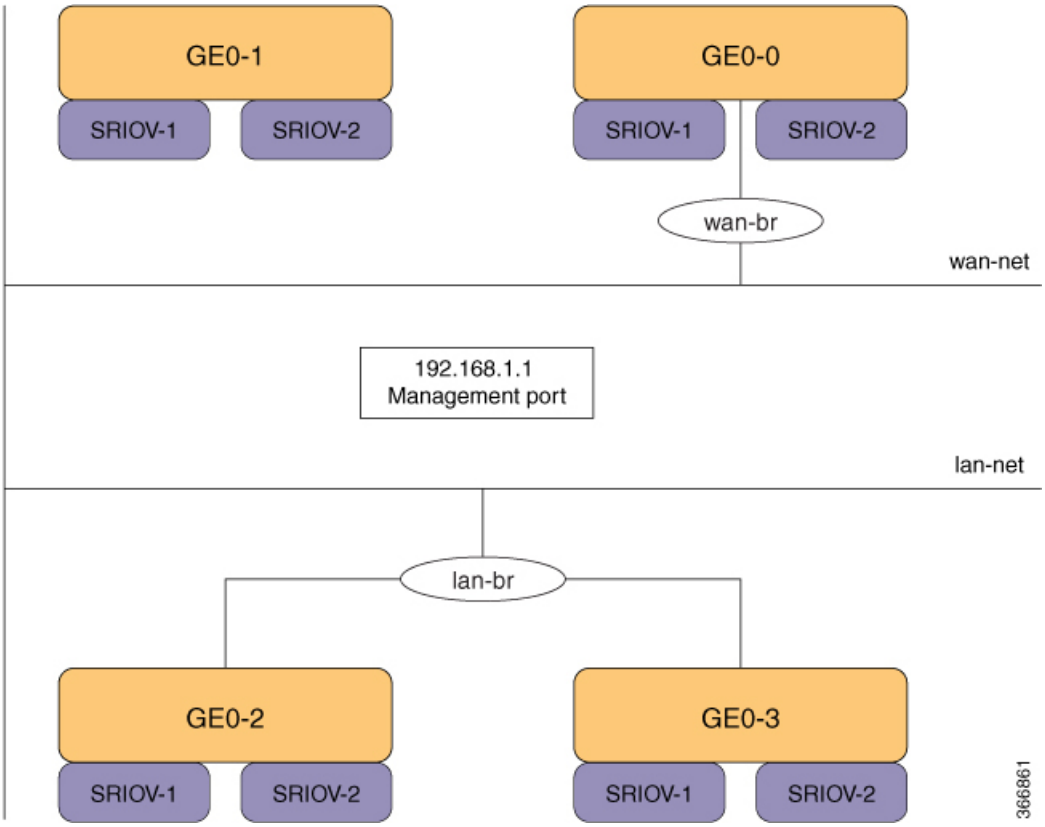


Figure 2: Default Network Configuration of Cisco Enterprise NFVIS with the Cisco ENCS 5100



- LAN ports—Eight physical Gigabit Ethernet ports for inbound and outbound traffic.
- WAN port—You can use one of the dual media Ethernet ports (wan-br and wan2-br) for DHCP connection.
- Bridges—They form a Layer 2 domain between virtual network interface controllers (vNICs) of VMs. A vNIC is used by a virtual machine to provide virtual network interfaces by defining a range of MAC addresses. The default management IP address (192.168.1.1) for the NFVIS host is configured on the management port. Multiple VMs can use the same LAN port for local connectivity.
- Network—It is a segment Layer 2 bridge domain where only the specific VLAN traffic is allowed.
- Reserved VLANs in the LAN network on the ENCS 5400 platform—The VLAN range 2350-2449 is reserved for internal use and should not be used on the external switch ports and for virtual machines in the LAN ports". Note that this limitation doesn't apply to the WAN ports.
- Internal 192.168.10.00/24 and 192.168.50.0/24 networks—The IP subnet 192.168.10.0/24 and 192.168.50.0/24 are used for the ENCS-5400 internal networks. A user should not use this IP subnet on the NFVIS management network. In the future NFVIS releases, this internal subnet will be isolated so that users can use this for NFVIS management.

Note The following networks and bridges are automatically configured. You can configure more as required.

- A LAN network (lan-net) and a LAN bridge (lan-br)
- A WAN network (wan-net) and a WAN bridge (wan-br)

wan2-net and wan2-br are the default configurations for ENCS 5400 and ENCS 5100.

The default networks and bridges cannot be deleted.

Install NFVIS on USC C-Series Servers and CSP Platforms

UCS-C series devices has to configure RAID disk group before installing NFVIS. UCS-C supports only single RAID disk group for fresh installation.

Note Starting from NFVIS 4.6 release, USC C-Series Servers and CSP Platforms support upto 3 RAID groups. The first raid group is reserved for OS installation and the other RAID groups can be used as external storage drives.

Step 1 Log in to CIMC.

The recommended CIMC version for USC-C Series Servers and Cisco CSP platforms is 3.0(3c) or later version.

Step 2 To launch KVM Console, Select **Launch KVM** from the CIMC homepage.

You can choose Java or HTML based KVM. It is recommnded to use HTML based KVM. Ensure that the pop-up blocker is disabled as KVM Console will open in a separate window.

Step 3 To map virtual devices from the KVM Console:

a) To know if a downloaded file is safe to install, it is essential to compare the file's checksum before using it. Verifying the checksum helps ensure that the file was not corrupted during network transmission, or modified by a malicious third party before you downloaded it. For more information see, Virtual Machine Security.
b) Select **Virtual Media** and then **Activate Virtual Devices**.
c) Select **Virtual Media** again and then **Map CD/DVD**. Browse and select the Cisco Enterprise NFVIS ISO image. Click **Open** and Map Drive to mount the image.
d) Select **Virtual Media** again to ensure the NFVIS ISO image is now mapped to CD/DVD.

Step 4 To configure boot order:

a) From the **CIMC Compute**, select **BIOS**.
b) Select **Configure Boot Order** and the **Configure Boot Order** dialog box appears.
c) Select **Advanced**.
d) The **Add Boot Device** page appears. Select **Add Virtual Media**, and the **Add Virtual Media** dialog box appears.
e) Enter a name and select **KVM Mapped DVD**. Set state to **Enabled** and order as 1, and **Save Changes**.
f) The **Add Boot Device** page appears again, select **Add Local HDD**, and **Add Virtual Media** dialog box appears.
g) Enter a name, set state to **Enabled** and order as 2, and **Save Changes**.
h) Click **Close**.

Step 5 Power cycle server to start the installation:

From CIMC homepage, select **Host Power**. Reboot the server by selecting the **Power Off** option. After the server is down, select the **Power On** option.

When the server reboots, the KVM console automatically installs Cisco Enterprise NFVIS from the virtual CD/DVD drive. The entire installation might take 30 minutes to one hour to complete.

Step 6 After the installation is complete, the system automatically reboots from the hard drive. Log into the system when the command prompt **nfvis login** is displayed after the reboot.

Use **admin** as the login name and **Admin123#** as the default password.

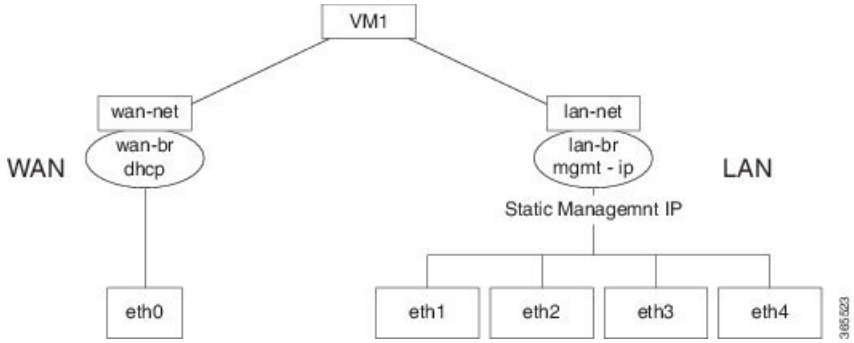
Note The system prompts you to change the default password at the first login attempt. You must set a strong password as per the on-screen instructions to proceed with the application. You cannot run API commands or proceed with any tasks unless you change the default password at the first login. The API commands will return 401 unauthorized error if the default password is not reset.

Step 7 Verify the installation using the System API, CLI, or by viewing the system information from the Cisco Enterprise NFV portal.

Default System Configuration on the Cisco UCS C220 M4 Server and Cisco CSP 2100

Configuring the networks in Cisco Enterprise NFVIS allows inbound and outbound traffic and VMs to be service chained. The following diagram illustrates the default network configuration:

Figure 3: Default Network Configuration with Cisco UCS C220 M4 and Cisco CSP 2100



The following 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.

For more details about the initial setup, see the Installing the Server chapter in the *Cisco UCS C220 M4 Server Installation and Service Guide* or *Cisco Cloud Services Platform 2100 Hardware Installation Guide*.

Install NFVIS on UCS-E Series Servers

- UCS-E Single-Wide supports only single RAID disk group for fresh installation. UCS-E Double-Wide series supports single or dual RAID disk groups for NFVIS 4.1 fresh installation, or one RAID disk group for NFVIS 3.X fresh installation.
  - Single disk group (4 disks): RAID0/RAID1/RAID10/RAID5. If FDE disks are used, you can also enable Secured RAID0/RAID1/RAID10/RAID5.
  - Dual disk groups (2 disks each): RAID0/RAID1 or Secured RAID0/RAID1 if FDE disks are used. NFVIS installation does not support any configuration with JBOD disk.

  For more information, see Managing Storage Using RAID for UCS-E devices
- Configure the Gigabit Ethernet interface on the Cisco ISR router.
- Configure the UCS E interface on the Cisco ISR router. The following sample configuration shows the basic configuration performed on the Cisco ISR 4451 router with DHCP enabled.

```
Last configuration change at 02:36:37 UTC Thu Feb 18 2016
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname NFVIS-ISR4451
!
boot-start-marker
boot system bootflash:isr4300-universalk9.03.16.01a.S.155-3.S1a-ext.SPA.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
no aaa new-model
!
!
!
ip domain name cisco.com
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
!
!
```

```
license udi pid ISR4331/K9 sn FDO192207MN
!
!
ucse subslot 1/0
 imc access-port shared-lom console
 imc ip address 172.19.183.172 255.255.255.0 default-gateway 172.19.183.1
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
vlan internal allocation policy ascending
!
!
!
interface GigabitEthernet0/0/0
 ip address 172.19.183.171 255.255.255.0
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/2
 no ip address
 shutdown
 negotiation auto
!
interface ucse1/0/0
 ip unnumbered GigabitEthernet0/0/0
 negotiation auto
 switchport mode trunk
 no mop enabled
 no mop sysid
!
interface ucse1/0/1
 no ip address
 no negotiation auto
 switchport mode trunk
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
interface Vlan1
 no ip address
 shutdown
!
ip default-gateway 172.19.183.1
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
ip route 0.0.0.0 0.0.0.0 172.19.183.1
```

```
ip route 172.19.183.172 255.255.255.255 ucse1/0/0
ip ssh version 2
!
!
!

control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login local
 transport input all
 transport output all
!
!
end
```

Note Ensure that following supported firmware versions or above are available:

- BIOS UCSED.2.5.0.3 or later for UCS-E160D-M2/K9 and UCS-E180D-M2/K9
- BIOS UCSES.1.5.0.5 or later for UCS-E140S-M2/K9
- BIOS UCSEM3_2.5 or later for UCS-E160S-M3
- BIOS UCSEDM3_2.5 or later for UCS-E180D-M3 and UCS-E1120D-M3

Step 1 Log in to CIMC.

Note The recommended CIMC version for USC-E Series Servers is 3.2(7) or later version.

Step 2 To launch KVM Console, Select **Launch KVM** from the CIMC homepage.

You can choose Java or HTML based KVM. It is recommnded to use HTML based KVM. Ensure that the pop-up blocker is disabled as KVM Console will open in a separate window.

Step 3 To map virtual media from the KVM Console:

a) To know if a downloaded file is safe to install, it is essential to compare the file's checksum before using it. Verifying the checksum helps ensure that the file is not corrupted during network transmission, or modified by a malicious third party before you downloaded it. For more information see, Virtual Machine Security.

b) Select **Virtual Media** and then **Activate Virtual Devices**.

c) Select **Virtual Media** again and then **Map CD/DVD**. Browse and select the Cisco Enterprise NFVIS ISO image. Click **Open** and Map Drive to mount the image.

d) Select **Virtual Media** again to ensure the NFVIS ISO image is now mapped to CD/DVD.

Step 4 Configure boot order.

a) From the **CIMC Compute**, select **BIOS**.

b) Select **Configure Boot Order** and the **Configure Boot Order** dialog box appears.
c) From the **CD/DVD** page, select **Cisco vKVM-Mapped vDVD**, and select **Add**.
d) From **HDD**, select **RAID Adapter**, and then select **Add**.
e) Set the boot order sequence using the **Up** and **Down** options. The **Cisco vKVM-Mapped vDVD** boot order must be the first choice. **Save Changes** to complete the boot order setup.

Note To configure Boot Order for UEFI through CIMC, the supported BIOS version is 2.10 or later. If any other BIOS version is used, you must configure UEFI Boot Order through the BIOS setup menu and set **BootOrderRules** to **Loose**.

To configure Boot Order for UEFI:

a) From the **CIMC Compute**, select **BIOS**.
b) Select **Configure Boot Order** and the **Configure Boot Order** dialog box appears.
c) Use >>, <<, **up** and **down** buttons to make **UEFI Image Map** as the first option in the right-hand column of the user interface.
d) Use the >>, <<, **up** and **down** buttons again to make **UEFI OS** as the second option in the right-hand column of the user interface.
e) Click **Save changes**.

Step 5 Power cycle server to start the installation:

From CIMC homepage, select **Host Power**. Reboot the server by selecting the **Power Off** option. After the server is down, select the **Power On** option.

When the server reboots, the KVM console automatically installs Cisco Enterprise NFVIS from the virtual CD/DVD drive. The entire installation might take 30 minutes to one hour to complete.

Step 6 For ENCS 5000 series platforms, auto-upgrade the firmware.

Starting from NFVIS 3.8.x release, firmware auto-upgrade is supported. After the NFVIS installation is complete, BIOS or CIMC is upgraded to the corresponding versions automatically. CIMC and NFVIS is rebooted multiple times. The firmware upgrade might take 30 minutes to one hour to complete. Do not use the system during the firmware upgrade.

Step 7 After the installation is complete, the system automatically reboots from the hard drive. Log into the system when the command prompt **nfvis login** is displayed after the reboot.

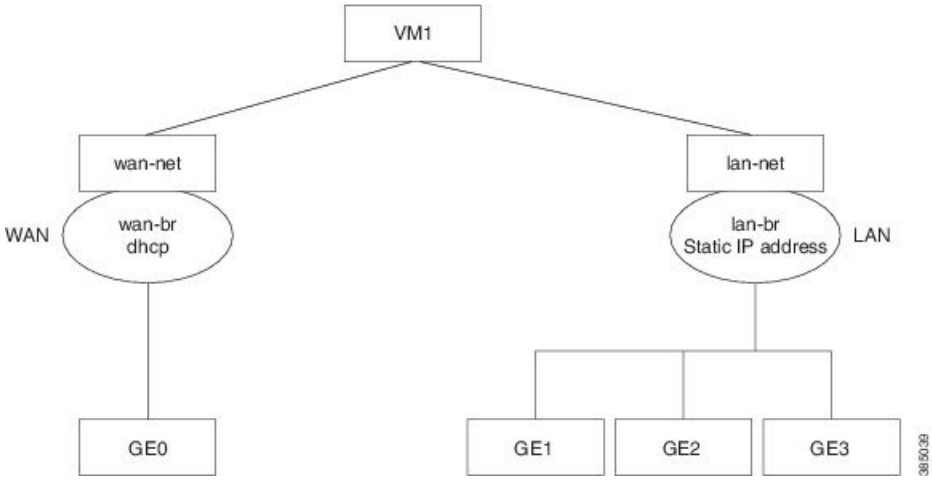
Use **admin** as the login name and **Admin123#** as the default password.

Note The system prompts you to change the default password at the first login attempt. You must set a strong password as per the on-screen instructions to proceed with the application. You cannot run API commands or proceed with any tasks unless you change the default password at the first login. API will return 401 unauthorized error if the default password is not reset.

Step 8 Verify the installation using the System API, CLI, or by viewing the system information from the Cisco Enterprise NFV portal.

Default System Configuration on the Cisco UCS E-Series Servers

Figure 4: Default Network Configuration with a Cisco UCS E-Series Server



The following 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. All other ports for inbound and outbound traffic are associated with the LAN bridge. By default, the hostname is set to "nfvis".
- A WAN network (wan-net) and a WAN bridge (wan-br)— The physical WAN ports are on the Cisco ISR module. They are not externally available on the Cisco UCS E server. The WAN traffic comes from the ISR WAN ports, and goes through the backplane to the Cisco UCS-E server. The backplane has one internal WAN interface (GE0) to establish connection with the Cisco UCS-E server. By default, the "GE0" interface is enabled for the DHCP connection.

For more details on the initial setup, see the Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine.

Install NFVIS Through USB

Install Cisco Enterprise NFVIS on Cisco ENCS 5104 and Cisco Catalyst 8200 UCPE

Before you begin

For Cisco Catalyst 8200 UCPE installation ensure that you install NFVIS only on one drive and only that drive be present at the time of installation.

For Cisco Catalyst 8200 UCPE, it is recommended to set the BIOS password after you log in to NFVIS.

To set the BIOS password, use the **hostaction change-bios-password** command. Without this step, you will not be able to select the device to install NFVIS.

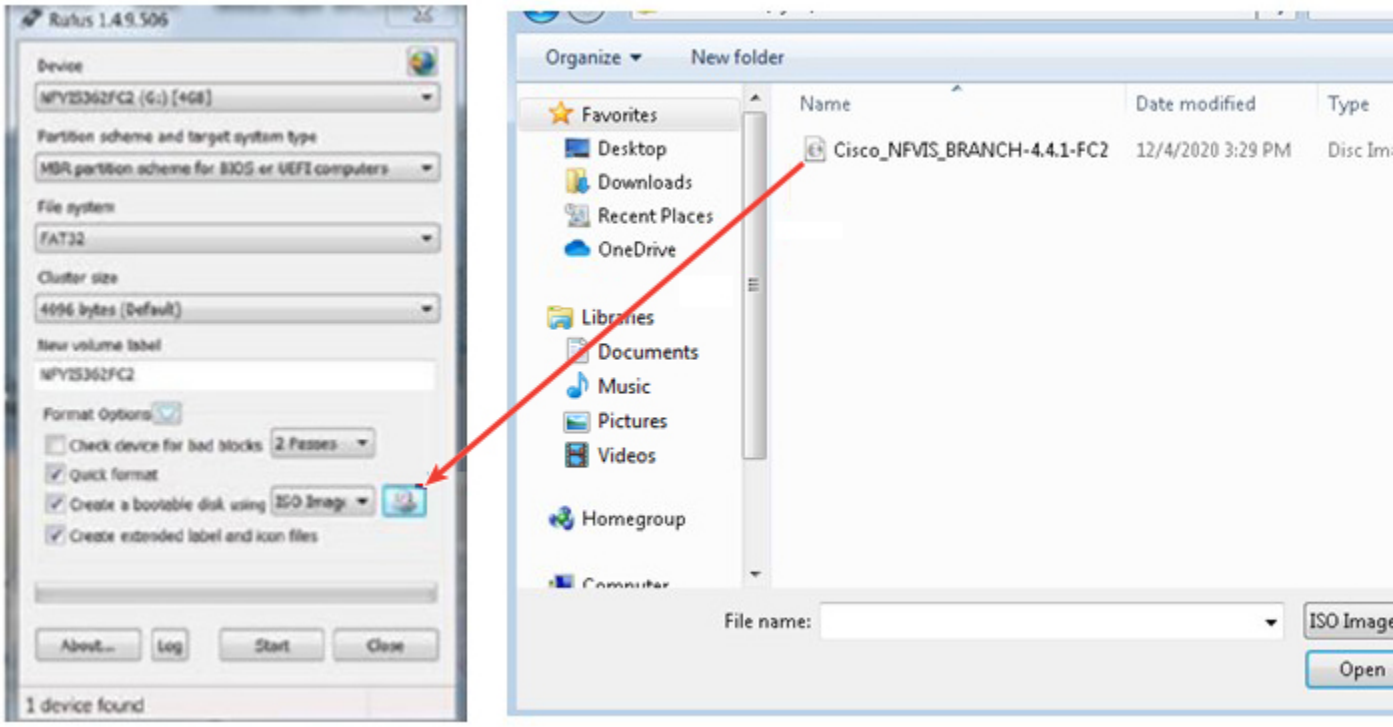
Step 1 Create bootable USB with NFVIS image.

In this example, we used rufus utility in Windows environment. Rufus utility can be downloaded https://rufus.akeo.ie/. For this example, following parameters were used to burn bootable NFVIS USB device:

- Device: USB stick
- Partition scheme: MBR
- Filesystem: FAT32
- Cluster size: use default
- Volume label: use default
- Quick format: checked
- Create bootable: select "ISO Image" and click next icon then choose NFVIS image.
- Create extended label: checked

Press **Start** and wait for completion.

Eject USB thumb drive



Step 2 Insert USB device in one of USB slot in ENCS5104.

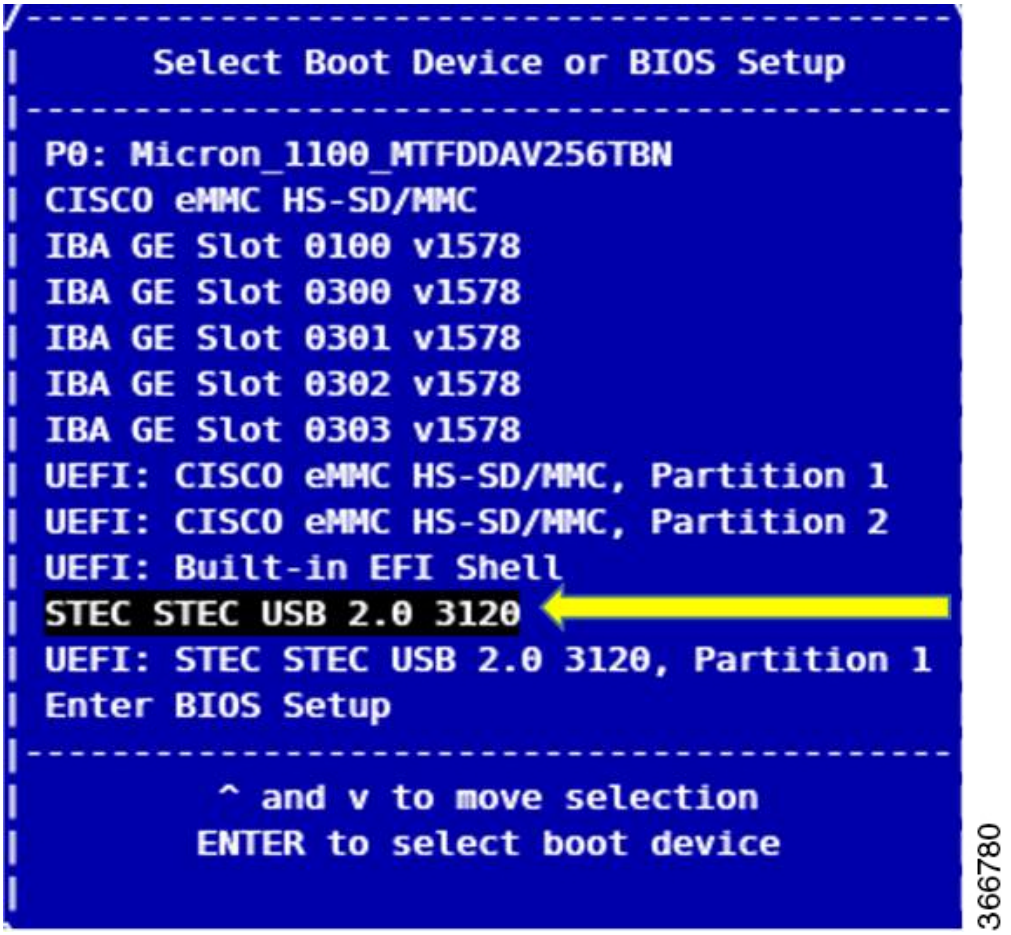
Step 3 Power on system.

Step 4 During system boot up, press F6 key.

```
Press <DEL> or <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot in 5 seconds or press any key
 to continue.
```

Step 5 Once you press F6, you will see the following screenshot to select which device you want to boot from. Select your USB device.

In the following screenshot example, there is STEC USB being used. That display will vary depending on your usb device vendor. Use the arrow key to select that device.



Step 6 Wait until installation is completed. System will be rebooted once installation is done.

Step 7 Log into the system with username **admin** and **Admin123#** as a default password

Step 8 You will be prompted and asked to change password at the first login. You must set a strong password per the on-screen instruction to proceed.

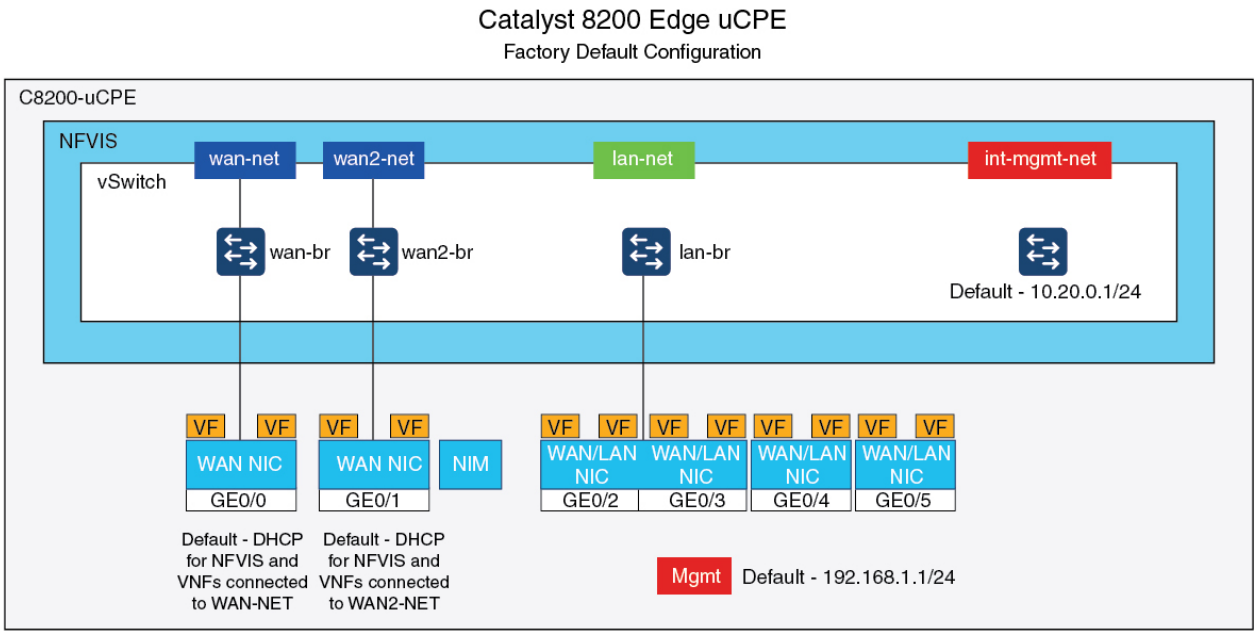
Step 9 You can verify the installation status using the System API or command line interface per the NFVIS user guide.

What to do next

You can verify the default configuration, and set up initial IP configuration to launch the Cisco Enterprise NFV portal.

Default System Configuration on Cisco Catalyst 8200 UCPE

The diagram below illustrates the default network configuration of Cisco Enterprise NFVIS with the Cisco ENCS.



- NFVIS can be accessed by default through the WAN port or GE0/2 LAN port for management.
- WAN network (wannet and wan2net) and WAN bridge (wanbr and wan2br) are set to enable DHCP by default. GE0 is associated to WAN bridge and WAN2 bridge by default.
- The management IP address 192.168.1.1 on Cisco Catalyst 8200 UCPE is accessible through GE0/2.
- GE0/2 is associated to LAN bridge.
- An internal management network (int-mgmt-net) and bridge (int-mgmt-br) is created and internally used for system monitoring.