



Installing Cisco Enterprise NFVIS Using the KVM Console

- [Installation Prerequisites](#) , on page 1
- [Installing Cisco Enterprise NFVIS on the Cisco UCS C220 M4 Rack Server](#), on page 2
- [Installing Cisco Enterprise NFVIS on Cisco UCS E-Series Servers](#), on page 4
- [Installing Cisco Enterprise NFVIS on a Cisco ENCS](#), on page 8

Installation Prerequisites

- Ensure that you have the IP address configured for Cisco Integrated Management Controller (CIMC) as well as a login account with administrative privileges.
- Ensure that you have the installation media for Cisco Enterprise NFVIS as an ISO image.
- The IP address of the system (required for remote access) is available.
- Ensure that hyper-threading is enabled in BIOS. By default, hyper-threading is enabled in BIOS on the UCS-C, UCS-E and ENCS platforms.



Note The installation steps are slightly different for Cisco UCS and Cisco ENCS platforms. See the following sections for details:

[Installing Cisco Enterprise NFVIS on the Cisco UCS C220 M4 Rack Server](#), on page 2

[Installing Cisco Enterprise NFVIS on Cisco UCS E-Series Servers](#), on page 4

[Installing Cisco Enterprise NFVIS on a Cisco ENCS](#), on page 8

Assumptions

- The user is familiar with the supported hardware device, CIMC, Cisco Network Plug and Play, and Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM).
- The initial setup of the hardware device is complete, and the device is ready for loading Cisco Enterprise NFVIS.

- The user is familiar with general Linux installation.

For more details on the supported hardware devices, see respective documentation available on Cisco.com.

Installing Cisco Enterprise NFVIS on the Cisco UCS C220 M4 Rack Server

This section provides information about a series of tasks you need to perform in order to install Cisco Enterprise NFVIS on a Cisco UCS C220 M4 Rack Server.

Logging Into the CIMC GUI

Before you begin

- Make sure that you have configured the IP address to access CIMC.
- If not installed, install Adobe Flash Player 10 or later on your local system.

For details on how to configure an IP address for CIMC, see the [Set up CIMC for UCS C-Series Server](#) guide on cisco.com.

-
- Step 1** In your web browser, enter the IP address that you configured to access CIMC during initial setup.
- Step 2** If a security dialog box displays, do the following:
- a) **Optional:** Select the check box to accept all content from Cisco.
 - b) Click **Yes** to accept the certificate and continue.
- Step 3** In the log in window, enter your username and password.
- When logging in for the first time to an unconfigured system, use **admin** as the username and **password** as the password.
- Step 4** Click **Log In**.
- The **Change Password** dialog box only appears the first time you log into CIMC.
- Step 5** Change the password as appropriate and save.
- The CIMC home page is displayed.
-

Activating a Virtual Device

You will have to launch the KVM Console to activate virtual devices.

Before you begin

Ensure that you have the Java 1.6.0_14 or a higher version installed on your local system.

-
- Step 1** Download the Cisco Enterprise NFVIS image from a prescribed location to your local system.
- Step 2** From CIMC, select the **Server** tab, and click **Launch KVM Console**.
- Note** A JNLP file will be downloaded to your system. You must open the file immediately after it is downloaded to avoid the session timeout.
- Step 3** Open the renamed *.jnlp* file. When it prompts you to download Cisco Virtual KVM Console, click **Yes**. Ignore all security warnings and continue with the launch.
- The KVM Console is displayed.
- Step 4** From the **Virtual Media** menu on the KVM Console, select **Activate Virtual Devices**.
- If prompted with an unencrypted virtual media session message, select **Accept this session**, and click **Apply**. The virtual devices are activated now.
-

Mapping the Cisco Enterprise NFVIS Image

-
- Step 1** From the **Virtual Media** menu on the KVM Console, select **Map CD/DVD...**
- Step 2** Browse for the installation file (ISO) on your local system, and select it .
- Step 3** Click **Map Device**.
- The ISO image file is now mapped to the CD/DVD.
-

Booting the Device

After mapping the image, you will have to boot the device using the KVM console. First, you have to boot from the DVD source, and then reboot from the hard drive.

-
- Step 1** From CIMC, select the **Server** tab and click **BIOS**.
- Step 2** From the **BIOS Actions** area, select **Configure Boot Order**.
- If any boot order is listed in the **Configure Boot Order** dialog box, proceed to **Step 3** to delete the boot order. If no boot order is listed, skip **Step 3**, and proceed to **Step 4**.
- Step 3** Select the boot order listed, and click **Delete**.
- Step 4** Select **Add Virtual Media** from the **Add Boot Device** section in the **Configure Boot Order** dialog box. The **Add Virtual Media** dialog box appears.
- Step 5** In the **Name** field, enter the boot device name (for example, KVM-DVD).
- Step 6** In the **Sub Type** field, select **KVM Mapped DVD**.
- Step 7** In the **State** field, ensure that **Enabled** is selected.
- Step 8** Enter **1** in the **Order** field.
- Step 9** Click **Add Device**. Click **Save**, and then click **Close** to close the **Configure Boot Order** dialog box.

The boot order is now configured.

Step 10 From the **Power** menu on the KVM Console, select **Power Cycle System (cold boot)**.

The KVM console will automatically install Cisco Enterprise NFVIS. The entire installation might take minimum 30 minutes to one hour to complete.

Step 11 After the installation is complete, the system is automatically rebooted from the hard drive. Log into the system when the command prompt changes from "localhost" to "nfvis" after the reboot. Wait for some time for the system to automatically change the command prompt. If it does not change automatically, press **Enter** to manually change the command prompt from "localhost" to "nfvis". 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 12 You can verify the installation using the System API or by viewing the system information from the Cisco Enterprise NFV portal.

What to do next

You can verify the default configuration, and set up initial IP configuration to launch the Cisco Enterprise NFV portal. For details, see [Performing Initial System Configuration](#).

Installing Cisco Enterprise NFVIS on Cisco UCSE-Series Servers

Before you begin

- Configure the UCS E interface on the Cisco ISR router.
- Configure the Gigabit Ethernet interface on the Cisco ISR router.
- Ensure that you have the IP address configured for CIMC access as well as a login account with administrative privileges.
- Ensure that the Cisco UCS E server has one of the following supported firmware versions or above:
 - 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

For more details on how to perform the basic configuration on the Cisco ISR routers, see the following guides:

- [Sample Configuration on the Cisco ISR Router to Bring Up a Cisco UCS E Server](#), on page 6
- [Getting Started Guide for Cisco UCS E-Series Servers, Release 1.0\(2\) Installed in the Cisco ISR 4451-X](#)
- [Getting Started Guide for Cisco UCS E-Series Servers, Release 1.0](#)

-
- Step 1** Log into CIMC.
For details, see [Logging Into the CIMC GUI , on page 2](#)
- Step 2** From the **Server** tab, click **Launch KVM Console**.
The KVM Console opens in a separate window.
- Step 3** From the KVM console, click the **Virtual Media** tab.
- Step 4** In the **Virtual Media** tab, map the virtual media using either of the following methods:
- Select the **Mapped** check box for the CD/DVD drive containing the operating system.
 - Click **Add Image**, browse, and select the Cisco Enterprise NFVIS ISO image, click **Open** to mount the image, and then select the **Mapped** check box for the mounted image.
- You must keep the **Virtual Media** tab open during the installation process. Closing the tab unmaps all virtual media.
- Step 5** From the **Server** tab, select **BIOS**.
- Step 6** From the **BIOS Actions** area, select **Configure Boot Order**.
The **Configure Boot Order** dialog box appears.
- Step 7** From the **Device Types** area, select **CD/DVD Linux Virtual CD/DVD**, and then click **Add**.
- Step 8** Select **HDD PCI RAID Adapter**, and then click **Add**.
- Step 9** Set the boot order sequence using the **Up** and **Down** options. The **CD/DVD Linux Virtual CD/DVD** boot order option must be the first choice.
- Step 10** Click **Apply** to complete the boot order setup.
- Step 11** Reboot the server by selecting the **Power Off Server** option from the **Server Summary** page in CIMC.
- Step 12** After the server is down, select the **Power On Server** option in CIMC.

When the server reboots, the KVM console will automatically install Cisco Enterprise NFVIS from the virtual CD/DVD drive. The entire installation might take 30 minutes to one hour to complete.
- Step 13** After the installation is complete, the system is automatically rebooted from the hard drive. Log into the system when the command prompt changes from "localhost" to "nfvis" after the reboot.
Wait for some time for the system to automatically change the command prompt. If it does not change automatically, press **Enter** to manually change the command prompt from "localhost" to "nfvis". 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 14** You can verify the installation using the System API or by viewing the system information from the Cisco Enterprise NFV portal.
-

What to do next

You can verify the default configuration, and set up initial IP configuration to launch the Cisco Enterprise NFV portal. For details, see [Performing Initial System Configuration](#).

Sample Configuration on the Cisco ISR Router to Bring Up a Cisco UCS E Server

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
```

Installing Cisco Enterprise NFVIS on a Cisco ENCS



Note Software or hardware RAID controller setup is not supported with Cisco ENCS in Cisco Enterprise NFVIS Release 3.5.1.

Before you begin

- Make sure that you have configured the IP address to access CIMC.
- If not installed, install Adobe Flash Player 10 or later on your local machine.

For details on how to configure an IP address for CIMC, see the [Set up CIMC for UCS C-Series Server](#) guide on cisco.com.

-
- Step 1** In your web browser, enter the IP address that you configured to access CIMC during initial setup.
- Step 2** If a security dialog box displays, do the following:
- Optional:** Select the check box to accept all content from Cisco.
 - Click **Yes** to accept the certificate and continue.
- Step 3** In the **Log in** window, enter your username and password.
- When logging in for the first time to an unconfigured system, use **admin** as the username and **password** as the password.
- Step 4** Click **Log In**.
- The **Change Password** dialog box only appears the first time you log into CIMC.
- Step 5** Change the password as appropriate and save.
- The CIMC home page is displayed.
- Step 6** From the CIMC **Server** tab, select **Summary**, and click **Launch KVM Console**.
- The KVM Console opens in a separate window.
- Step 7** From the **Virtual Media** menu on the KVM Console, select **Activate Virtual Devices**.
- If prompted with an unencrypted virtual media session message, select **Accept this session**, and click **Apply**. The virtual devices are activated now.
- Step 8** From the **Virtual Media** menu on the KVM Console, select **Map CD/DVD**.
- Step 9** Browse for the installation file (ISO) on your local system, and select it.
- Step 10** Click **Map Device**.
- The ISO image file is now mapped to the CD/DVD.
- Step 11** From the CIMC **Server** tab, select **BIOS**.

- Step 12** From the **BIOS Actions** area, select **Configure Boot Order**. The **Configure Boot Order** dialog box appears.
- Step 13** From the **Device Types** area, select **CD/DVD Linux Virtual CD/DVD**, and then click **Add**.
- Step 14** Select **HDD**, and then click **Add**.
- Step 15** Set the boot order sequence using the **Up** and **Down** options. The **CD/DVD Linux Virtual CD/DVD** boot order option must be the first choice.
- Step 16** Click **Apply** to complete the boot order setup.
- Step 17** Reboot the server by selecting the **Power Off Server** option from the **Server Summary** page in CIMC.
- Step 18** After the server is down, select the **Power On Server** option in CIMC.
- When the server reboots, the KVM console will automatically install Cisco Enterprise NFVIS from the virtual CD/DVD drive. The entire installation might take 30 minutes to one hour to complete.
- Step 19** After the installation is complete, the system is automatically rebooted from the hard drive. Log into the system when the command prompt changes from "localhost" to "nfvis" after the reboot.
- Wait for some time for the system to automatically change the command prompt. If it does not change automatically, press **Enter** to manually change the command prompt from "localhost" to "nfvis". 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. 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 20** You can verify the installation using the System API or by viewing the system information from the Cisco Enterprise NFVIS portal.

What to do next

You can verify the default configuration, and set up initial IP configuration to launch the Cisco Enterprise NFV portal. For details, see [Performing Initial System Configuration](#).

