Cisco Network Function Virtualization Infrastructure Software Getting Started Guide

First Published: 2020-09-01

Last Modified: 2024-01-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

About Cisco Enterprise NFVIS

Cisco Enterprise Network Function Virtualization Infrastructure Software (Cisco Enterprise NFVIS) is a Linux-based infrastructure software designed to help service providers and enterprises to design, deploy and manage network services. Cisco Enterprise NFVIS helps dynamically deploy virtualized network functions, such as a virtual router, firewall, and WAN accelerator on supported Cisco devices. Such virtualized deployments of VNFs also leads to device consolidation. You no longer need separate devices. Automated provisioning and centralized management also eliminates costly truck rolls.

Cisco Enterprise NFVIS provides a Linux-based virtualization layer to the Cisco Enterprise Network Function Virtualization (ENFV) solution.

Cisco ENFV Solution Overview

The Cisco ENFV solution helps convert your critical network functions into a software which can deploy network services across dispersed locations in minutes. It provides a fully integrated platform that can run on top of a diverse network of both virtual and physical devices with the following primary components:

- Cisco Enterprise NFVIS
- VNFs
- Unified Computing System (UCS) and Enterprise Network Compute System (ENCS) hardware platforms
- Digital Network Architecture Center (DNAC)

Benefits of Cisco Enterprise NFVIS

- Consolidates multiple physical network appliances into a single server running multiple virtual network functions.
- Deploys services quickly and in a timely manner.
- Cloud based VM life cycle management and provisioning.
- Life cycle management to deploy and chain VMs dynamically on the platform.

- Programmable APIs.

Supported Hardware Platforms

Depending on your requirement, you can install Cisco Enterprise NFVIS on the following Cisco hardware platforms:

- Cisco 5100 Series Enterprise Network Compute System (Cisco ENCS)
- Cisco 5400 Series Enterprise Network Compute System (Cisco ENCS)
- Cisco Catalyst 8200 Series Edge Universal CPE
- Cisco Catalyst 8300 Series Edge Universal CPE
- Cisco UCS C220 M4 Rack Server
- Cisco UCS C220 M5Rack Server
- Cisco UCS C M6 Rack Servers (UCSC-C220-M6S, UCSC-C240-M6SX, and UCSC-C240-M6S)
- Cisco Cloud Services Platform 2100 (CSP 2100)
- Cisco Cloud Services Platform 5228 (CSP-5228), 5436 (CSP-5436) and 5444 (CSP-5444 Beta)
- Cisco ISR4331 with UCS-E140S-M2/K9
- Cisco ISR4351 with UCS-E160D-M2/K9
- Cisco ISR4451-X with UCS-E180D-M2/K9
- Cisco UCS-E160S-M3/K9 Server
- Cisco UCS-E180D-M3/K9
- Cisco UCS-E1120D-M3/K9

Cisco ENCS

The Cisco 5100 and 5400 Series Enterprise Network Compute System combines routing, switching, storage, processing, and a host of other computing and networking activities into a compact one Rack Unit (RU) box. This high-performance unit achieves this goal by providing the infrastructure to deploy virtualized network functions and acting as a server that addresses processing, workload, and storage challenges.

Cisco Catalyst 8200 Series Edge Universal CPE

The Cisco Catalyst 8200 Edge uCPE is the next generation of Cisco Enterprise Network Compute System 5100 Series that combines routing, switching and application hosting into a compact one rack unit device for the small and Medium Virtualized Branch. 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. These devices are 8 Core x86 CPUs with HW Acceleration for IPSec crypto traffic with higher number of WAN ports. They have a NIM slot and a PIM slot to choose different WAN, LAN and LTE/5G modules for the Branch.

Cisco Catalyst 8300 Series Edge Universal CPE

The Cisco Catalyst 8300 Series Edge Universal Customer Premises Equipment (uCPE) is a purpose-built x86 platform that is designed for branch virtualization. It enables device consolidation across network and security functions, improves operational flexibility and service agility, simplifies network operations, and results in reduced deployment times and fewer truck rolls for delivery of add-on services.

Cisco UCS C220 M4/M5 Rack Server

The Cisco UCS C220 M4 Rack Server is a high-density, general-purpose enterprise infrastructure and application server that delivers world class performance for a wide range of enterprise workloads, including virtualization, collaboration, and bare-metal applications.

Cisco UCS C M6 Rack Server

The Cisco UCS C220 M6 Rack Server is the most versatile general-purpose infrastructure and application server in the industry. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications.

Cisco CSP 2100-X1, 5228, 5436 and 5444 (Beta)

Cisco Cloud Services Platform is a software and hardware platform for data center network functions virtualization. This open kernel virtual machine (KVM) platform is designed to host networking virtual services. Cisco Cloud Services Platform devices enables network, security, and load balancer teams to quickly deploy any Cisco or third-party network virtual service.

Note CSP 5000 series devices support ixgbe drivers.

Caution If CSP platforms are running NFVIS, Return Material Authorization (RMA) is not supported.

Cisco UCS E-Series Server Modules

The Cisco UCS E-Series Servers (E-Series Servers) are the next generation of Cisco UCS Express servers. E-Series Servers are a family of size, weight, and power efficient blade servers that are housed within the Generation 2 Cisco Integrated Services Routers (ISR G2), Cisco 4400, and Cisco 4300 Series Integrated Services Routers. These servers provide a general-purpose compute platform for branch office applications deployed either as bare metal on operating systems, such as Microsoft Windows or Linux; or as virtual machines on hypervisors.

Supported VMs

Currently, Cisco Enterprise NFVIS supports the following Cisco VMs and third-party VMs:

- Cisco Catalyst 8000V Edge Software
- Cisco Integrated Services Virtual (ISRv)
- Cisco Adaptive Security Virtual Appliance (ASAv)

- Cisco Virtual Wide Area Application Services (vWAAS)
- Linux Server VM
- Windows Server 2012 VM
- Cisco Firepower Next-Generation Firewall Virtual (NGFWv)
- Cisco vEdge
- Cisco XE SD-WAN
- Cisco Catalyst 9800 Series Wireless Controller
- ThousandEyes
- Fortinet
- Palo Alto
- CTERA
- InfoVista

Key Tasks You can Perform Using Cisco Enterprise NFVIS

- Perform VM image registration and deployment
- Create new networks and bridges, and assign ports to bridges
- Perform service chaining of VMs
- Perform VM operations
- Verify system information including CPU, port, memory, and disk statistics
- SR-IOV support on all interfaces of all platforms, with the exception of UCS-E backplane interface

The APIs for performing these tasks are explained in the API Reference for Cisco Enterprise NFVIS.

Note NFVIS can be configured through Netconf interface, REST APIs and command-line interface as all the configurations are exposed through YANG models.

From a Cisco Enterprise NFVIS command-line interface, you can connect to another server and VMs remotely using the SSH client.

CHAPTER 2

Set Up Cisco Enterprise NFVIS

This chapter provides provides information to unbox and configure Enterprise Network Compute System (ENCS) 5400 series platform devices to be accessed remotely over the WAN. You will provision a router VNF (Virtual Network Function) instance and further configure it to enable traffic flow from LAN to WAN.

This chapter covers the following use cases to set up the initial configuration:

- Set up using console serial cable.
- Set up using ethernet cable.

You should be able to complete the entire setup in 60 minutes.

Introduction to ENCS 5400 Platform Devices

Cisco Enterprise Network Compute System (ENCS) 5000 series is a family of compute appliances designed for a virtualized software-defined branch network architecture. ENCS is a purpose-built hybrid platform with a small infrastructure footprint that combines the functionality of a traditional router with a traditional server. It allows you to deploy network services, Virtual Network Functions (VNFs), within minutes. For more information on ENCS features and datasheet see, Cisco 5000 Series Enterprise Network Compute System.

This chapter introduces you to ENCS 5400 series devices and its key components. This series includes the following models:

- ENCS 5406
- ENCS 5408
- ENCS 5412

Installation Prerequisites

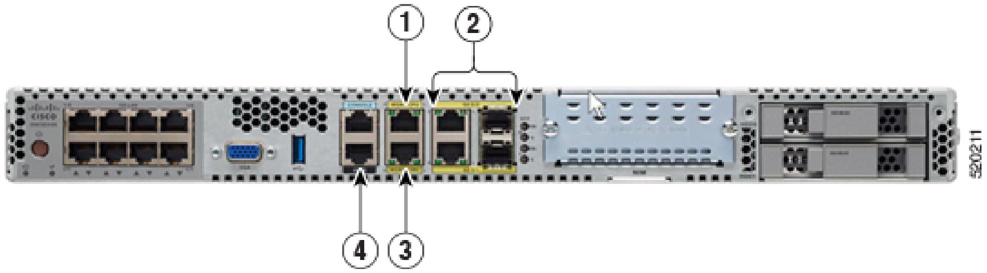
As a prerequisite, ensure that you have the following before getting started on the setup of the device:

- ENCS 5400 device with supporting power cables
- One console serial cable or two ethernet cables of suitable length
- Windows or Mac Laptop with Terminal software that supports serial port connections
- One available LAN IP address (`10.29.43.84`) to access the ENCS device on the LAN at this address for administration purposes.
- Subnet mask (`255.255.255.0`) and Gateway IP address (`10.29.43.1`) to manage the ENCS device on your LAN. Ask your local LAN administrator for your environment.

Components of ENCS 5400 Series

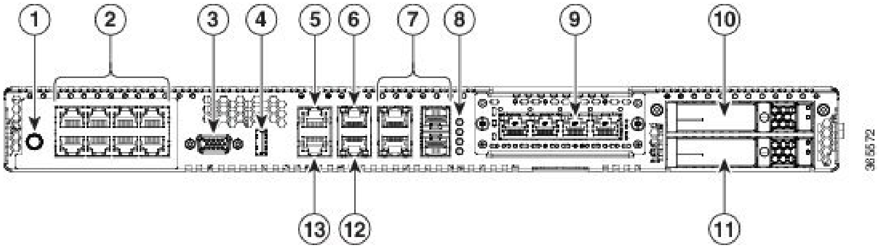
Hardware

Figure 1: Install hardware ports



1	Ethernet management port Manage network hypervisor (NFVIS) IP/virtual serial consol access to VNF	2	NFVIS and VNF Management through copper or fiber WAN port Physical port shared between NFVIS and VNF services
3	CIMC ethernet connection CLI access to NFVIS through CIMC-KVM	4	CIMC serial connection CLI access to NFVIS through CIMC

Figure 2: Front Panel of the Cisco 5400 ENCS



1.	Power on/off switch	2	Integrated LAN ports - optional PoE support is available for some models
3	VGA connector	4	USB port
5	Serial console port for CPU	6	Ethernet management port for CPU
7	Front panel Gigabit Ethernet ports	8	LEDs for front panel Gigabit Ethernet ports
9	Network Interface Module (NIM)	10	Drive bay 0
11	Drive bay 1	12	Ethernet management port for CIMC
13	Serial console port for CIMC		

Cisco IMC

Cisco Integrated Management Controller (CIMC) is an out-of-band embedded management service that runs natively on the device. You can access Cisco IMC console either through serial console cable, or an ethernet cable. It supports multiple interfaces, including a web user interface, a command-line interface (CLI), and an XML API.

You can perform firmware upgrade, BIOS upgrade, install and upgrade operating system and so on from Cisco IMC. For more information see, CIMC Access Control.

Note In this guide we will not be using Cisco IMC to complete the minimal setup.

NFVIS

Cisco Network Function Virtualization Infrastructure Software (NFVIS) is an operating system software for software-defined branch network virtualization deployments. NFVIS is the operating system for all ENCS series of devices. NFVIS is based on open source Kernel-based Virtual Machine (KVM) hypervisor.

NFVIS enables you to run one or more network services like router, firewall and so on as Virtual Machines (VMs) also known as Virtual Network Functions (VNFs) on a single hardware platform.

You can access NFVIS through:

- Serial console port using a serial console cable, or
- Dedicated NFVIS management ethernet port which gives you access to the web-based GUI console, or

- Cisco IMC.

This chapter includes instructions to setup an ENCS device using the GUI console.

For more information on NFVIS see, Enterprise NFV Infrastructure Software.

VNFs

Virtual Network Functions (VNFs), is a collective term used to describe virtualized network services such as a virtual router, a virtual firewall, a virtual load balancer and so on. VNF is synonymous to Virtual Machine (VM).

Every ENCS device comes pre-installed with a virtual appliance image file of Cisco virtual Integrated Services Router (ISRv). This chapter describes how to use this image file to create a router VNF instance and then configure it to enable traffic on the LAN to flow towards the WAN.

Unpacking and Cabling ENCS 5400

Unpacking the Device

The device, accessory kit, publications, and any optional units may be shipped in more than one container. When you unpack the containers, check the packing list to ensure that you have received all the items on the list.

Only unpack the product when you are ready to install it. This will help prevent accidental damage.

Remove the ENCS device from the shipping box and rack it up as per the instructions in the box.

Cabling

The device will automatically power-on when you connect the power cable to the device. Configure NFVIS management IP address on the device, so that it can be managed remotely over the LAN.

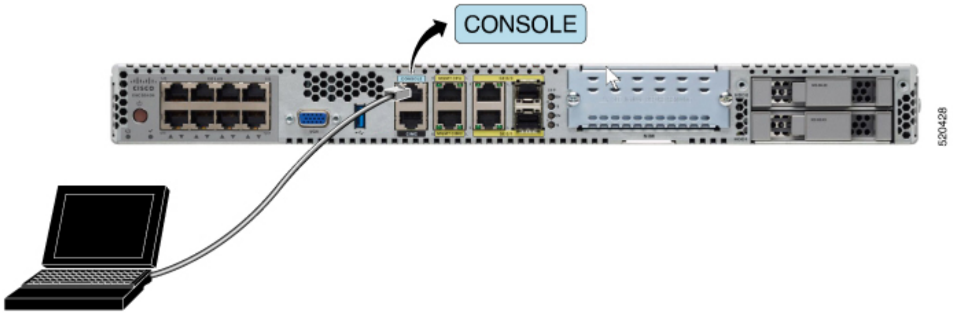
You can configure NFVIS management IP address on the device using:

- Serial console cable: Connect your laptop to the serial port on the device using a serial console cable and set up the NFVIS IP address. Also use the Ethernet cable to connect the device management Ethernet port to local management network and then access the device remotely for further configurations.

  To access the device over a dedicated management Ethernet port use the serial console cable to setup the device management IP address. You can then access the NFVIS portal using the configured device management IP address for the installation procedure.

  Connect one end of the serial console cable to the port labeled **CONSOLE** on the ENCS device and the other end to your laptop serial port or USB port.

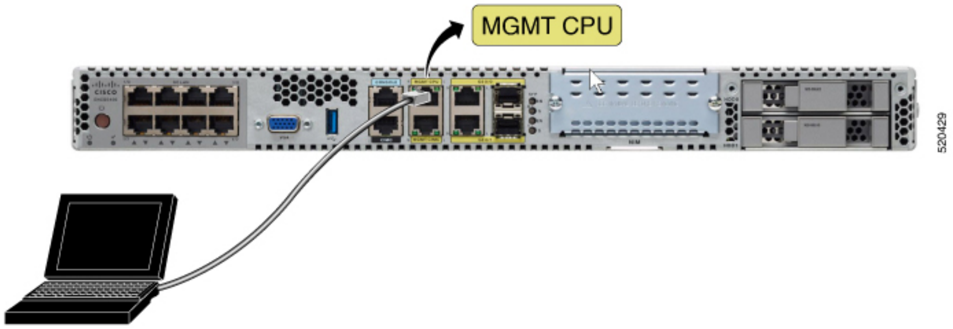
Figure 3: Serial Concole Cable connection



- Ethernet cable: Connect your laptop to the management Ethernet port on the device using an Ethernet cable and set up the NFVIS IP address. To manage the device remotely over the management network, reconnect the management port to the local management network.

  Connect one end of the Ethernet cable to the **MGMT CPU** port on the ENCS device and the other end to your laptop Ethernet port or local switch.

Figure 4: Ethernet Cable connection



Install NFVIS on ENCS 5400 Platforms

After unboxing and cabling the ENCS device:

1. Set up the NFVIS management IP address to access the device remotely over LAN.
2. Create a VNF instance using Cisco ISRv router on NFVIS web-based GUI console.
3. Configure ISRv router to enable LAN to WAN connectivity.
4. Validate LAN to WAN connectivity.

Access NFVIS

1. For initial NFVIS login, the default username is **`admin`** and the default password is **`Admin123#`**.

```
NFVIS Version: 3.12.3
```

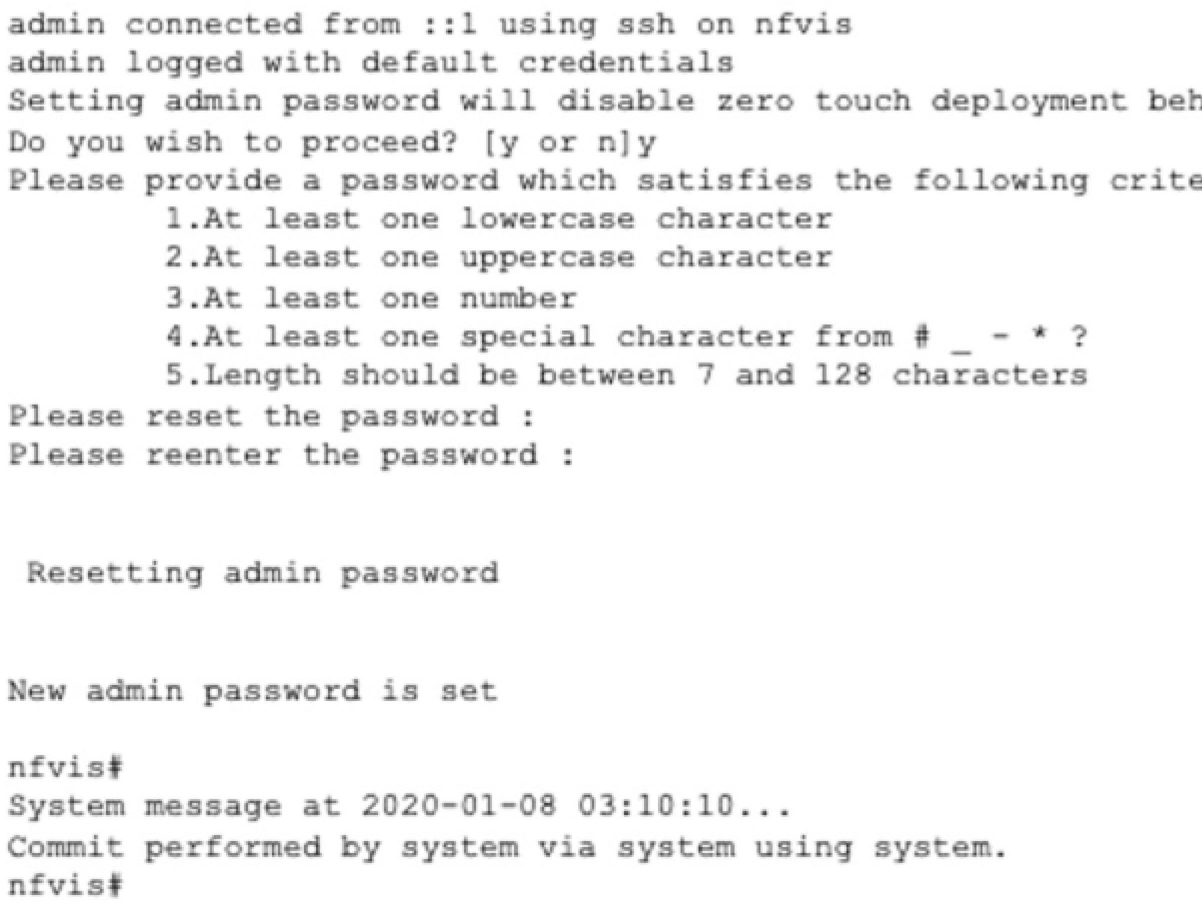
```
Copyright (c) 2015-2020 by Cisco Systems, Inc.
Cisco, Cisco Systems, and Cisco Systems logo are registered trademarks of Cisco
Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

The copyrights to certain works contained in this software are owned by other
third parties and used and distributed under third party license agreements.
Certain components of this software are licensed under the GNU GPL 2.0, GPL 3.0,
LGPL 2.1, LGPL 3.0 and AGPL 3.0.
```

2. Immediately after the initial login, the system prompts you to change the default password. All other operations are blocked until default password is changed.

   You must adhere to the following rules to create a strong password:

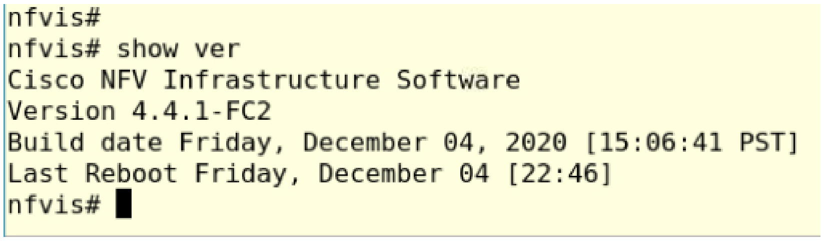
   - Must contain at least one upper case and one lower case letter.
   - Must contain at least one number and one special character (# _ - * ?).
   - Must contain seven characters or greater. Length should be between 7 and 128 characters.

3. After you change the password you will be at the nfvis prompt.



```
admin connected from ::1 using ssh on nfvis
admin logged with default credentials
Setting admin password will disable zero touch deployment beh
Do you wish to proceed? [y or n]y
Please provide a password which satisfies the following crite
        1.At least one lowercase character
        2.At least one uppercase character
        3.At least one number
        4.At least one special character from # _ - * ?
        5.Length should be between 7 and 128 characters
Please reset the password :
Please reenter the password :


 Resetting admin password



New admin password is set

nfvis#
System message at 2020-01-08 03:10:10...
Commit performed by system via system using system.
nfvis#
```

4. After you login to NFVIS, you can see the information about NFVIS version. You can then decide if you want to install or upgrade to a newer version.



```
nfvis#
nfvis# show ver
Cisco NFV Infrastructure Software
Version 4.4.1-FC2
Build date Friday, December 04, 2020 [15:06:41 PST]
Last Reboot Friday, December 04 [22:46]
nfvis#
```

Configure the Device Management IP Address

1. Configure the device management IP address.

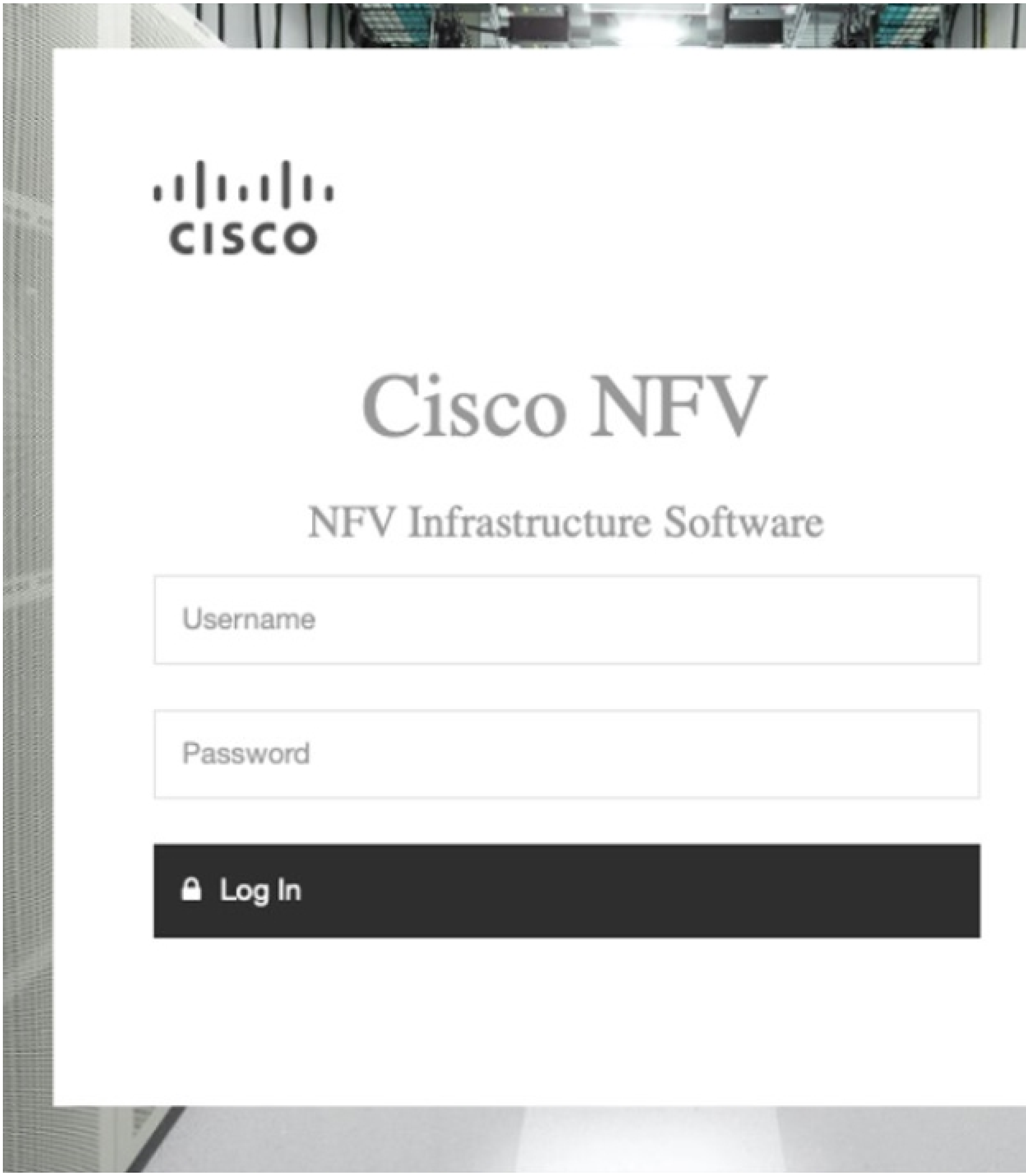
```
configure terminal
system settings mgmt ip address 10.29.43.84 255.255.255.0
bridges bridge wan-br no dhcp
bridges bridge wan2-br no dhcp
system settings default-gw 10.29.43.1
commit
end
```

2. The device management IP address is now set to 10.29.43.84 and you can access NFVIS remotely at this address.
3. Use the **show system settings-native** command to confirm the settings and display the current values.
4. To logout from the system enter **`Exit`**.

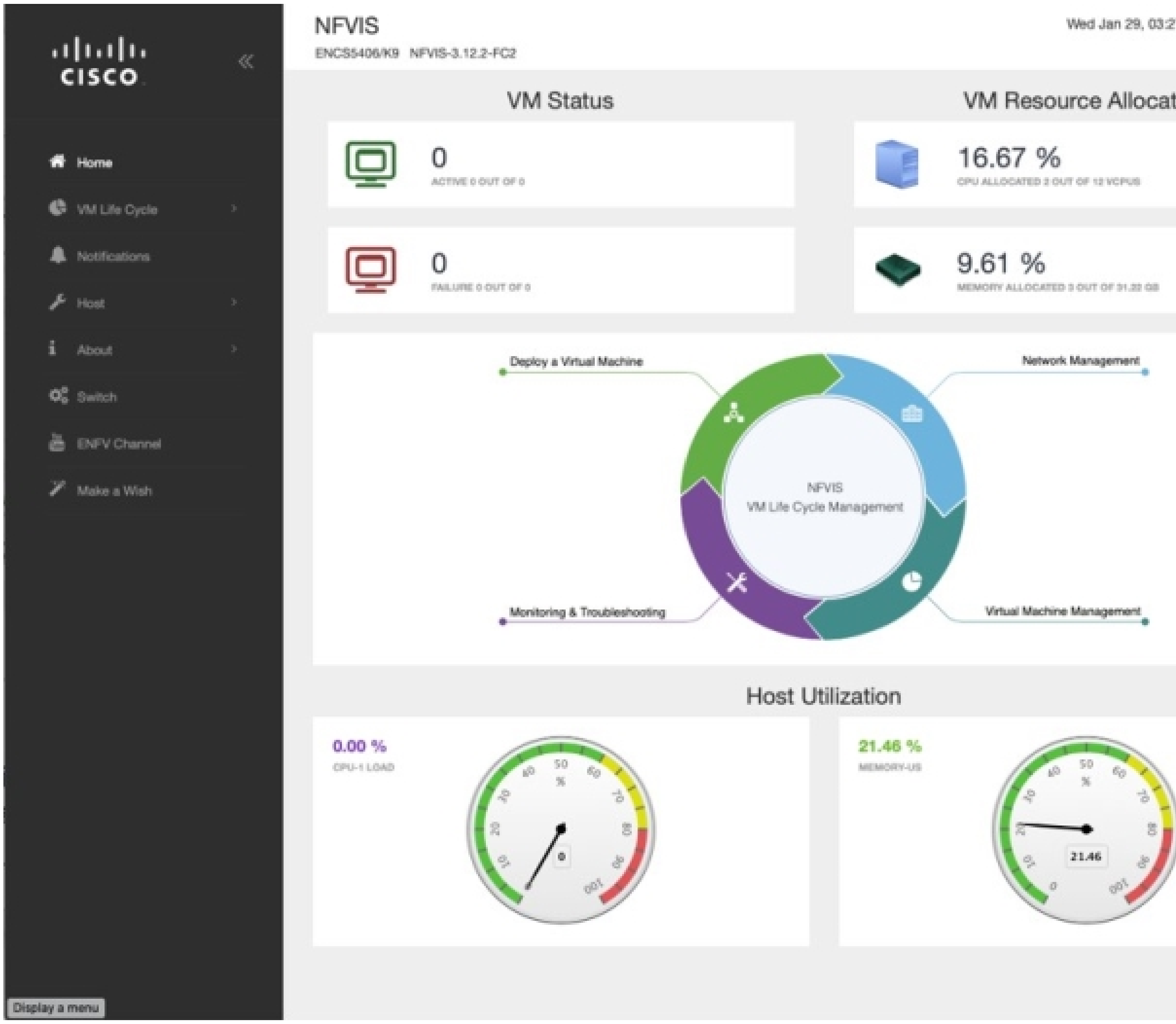
Access NFVIS Portal

To access NFVIS portal:

1. Connect your laptop to the local ethernet management network. Enter https://10.29.43.84 in your web browser's address bar. We recommend that you use Google Chrome.



2. To login to NFVIS portal, the username is **`admin`** and password is the new generated password. You will see the NFVIS dashboard which provides a summary of activities on the device.

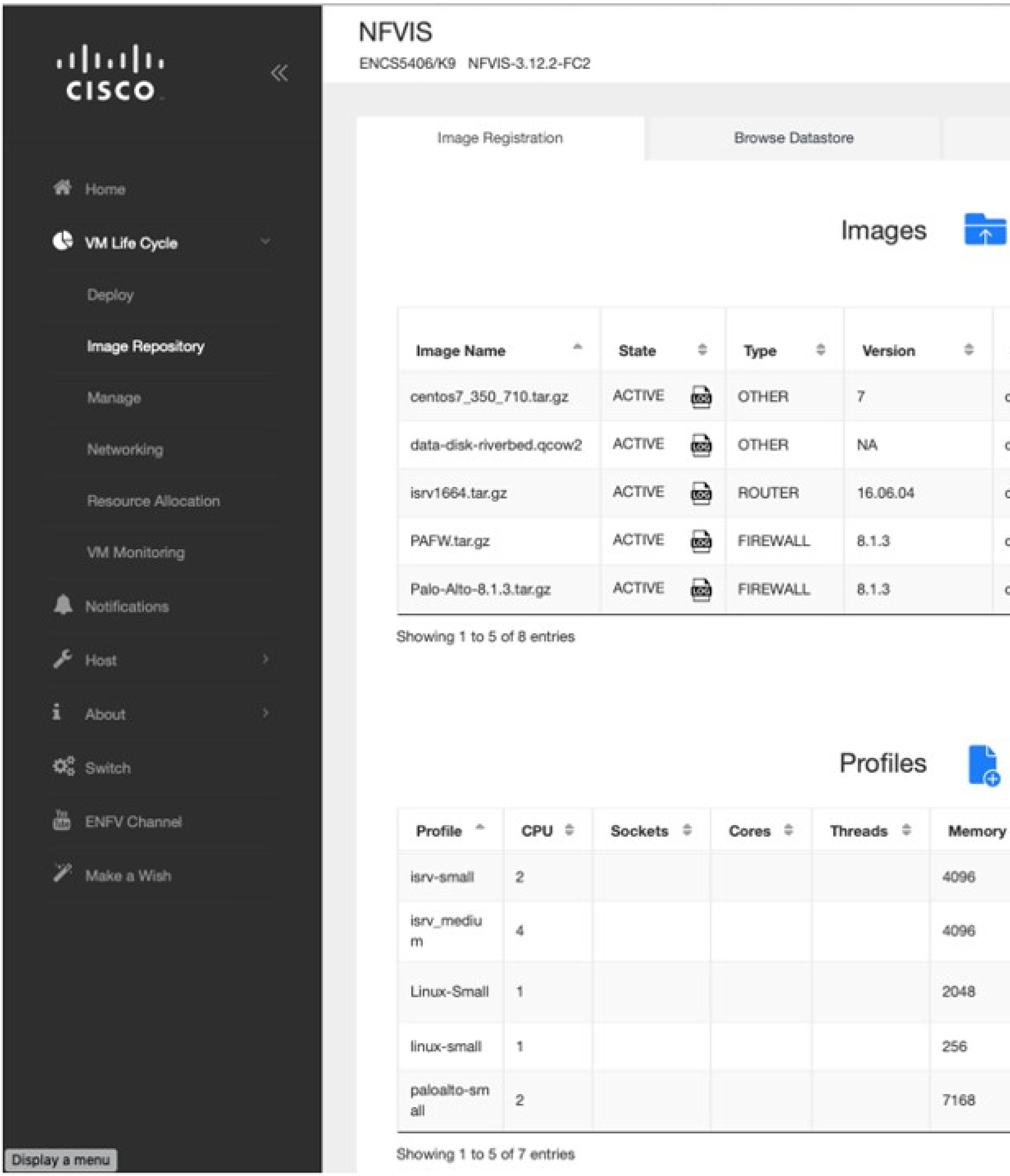


Create and Deploy a Virtual Router

To deploy a virtual router on a factory shipped ENCS 5400 device:

1. Chose **VM Life Cycle** > **Image Repository** from the navigation tree on the left of the interface. Here you will see all the previously uploaded images in the device.

   For a factory shipped ENCS 5400 device, in **Images**, the only available image is `isrv.tar.gz` and in **Profiles**, you can see `isrv-mini`, `isrv-small` and `isrv-medium` or `C8000V-mini`, `C8000V-small` and `C8000V-medium`.



NFVIS

ENCS5406/K9 NFVIS-3.12.2-FC2

Images

Image Name	State	Type	Version
centos7_350_710.tar.gz	ACTIVE	OTHER	7
data-disk-riverbed.qcow2	ACTIVE	OTHER	NA
isrv1664.tar.gz	ACTIVE	ROUTER	16.06.04
PAFW.tar.gz	ACTIVE	FIREWALL	8.1.3
Palo-Alto-8.1.3.tar.gz	ACTIVE	FIREWALL	8.1.3

Showing 1 to 5 of 8 entries

Profiles

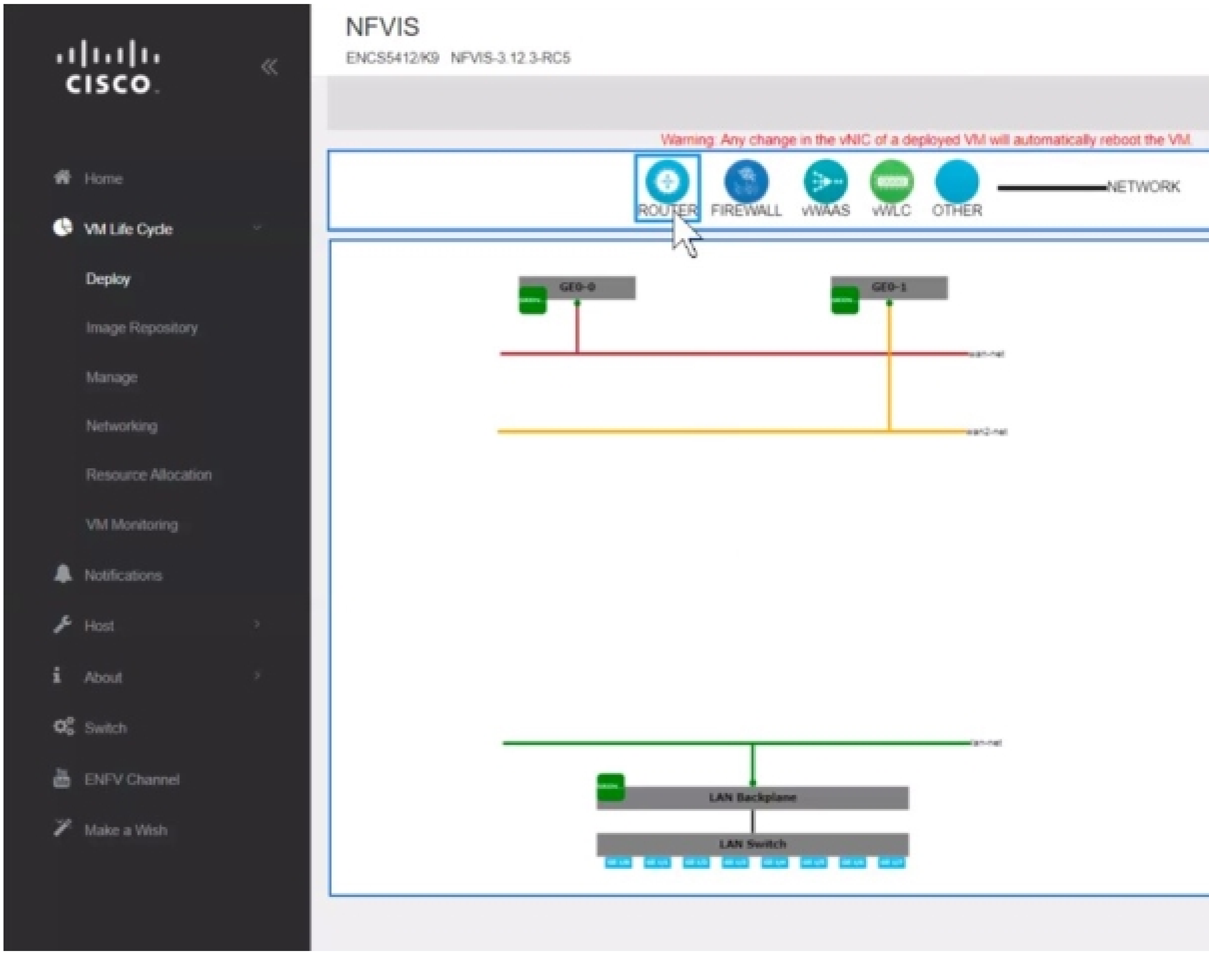
Profile	CPU	Sockets	Cores	Threads	Memory
isrv-small	2				4096
isrv_medium	4				4096
Linux-Small	1				2048
linux-small	1				256
paloalto-small	2				7168

Showing 1 to 5 of 7 entries

In **Images** you can see information about the available images and make a note of the version for an upgrade if required. The **ACTIVE** state of the image indicates that the image is registered and ready for deployment.

2. Chose **VM Life Cycle** > **Deploy**.

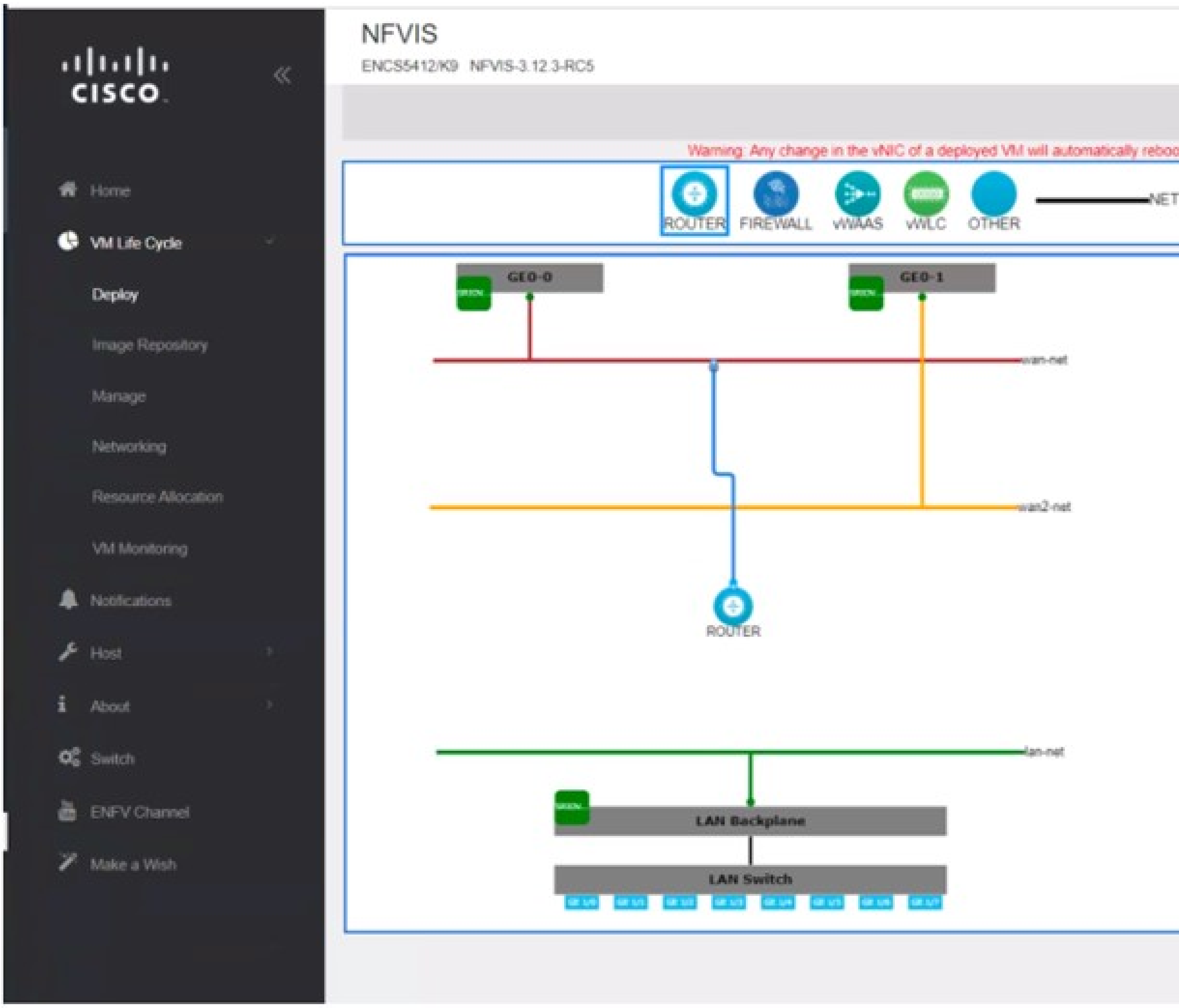
You can a catalog of various VNFs at the top of the page. The default configuration of the device at the center of the page has LAN, WAN, and WAN2 networks.



Warning: Any change in the vNIC of a deployed VM will automatically reboot the VM.

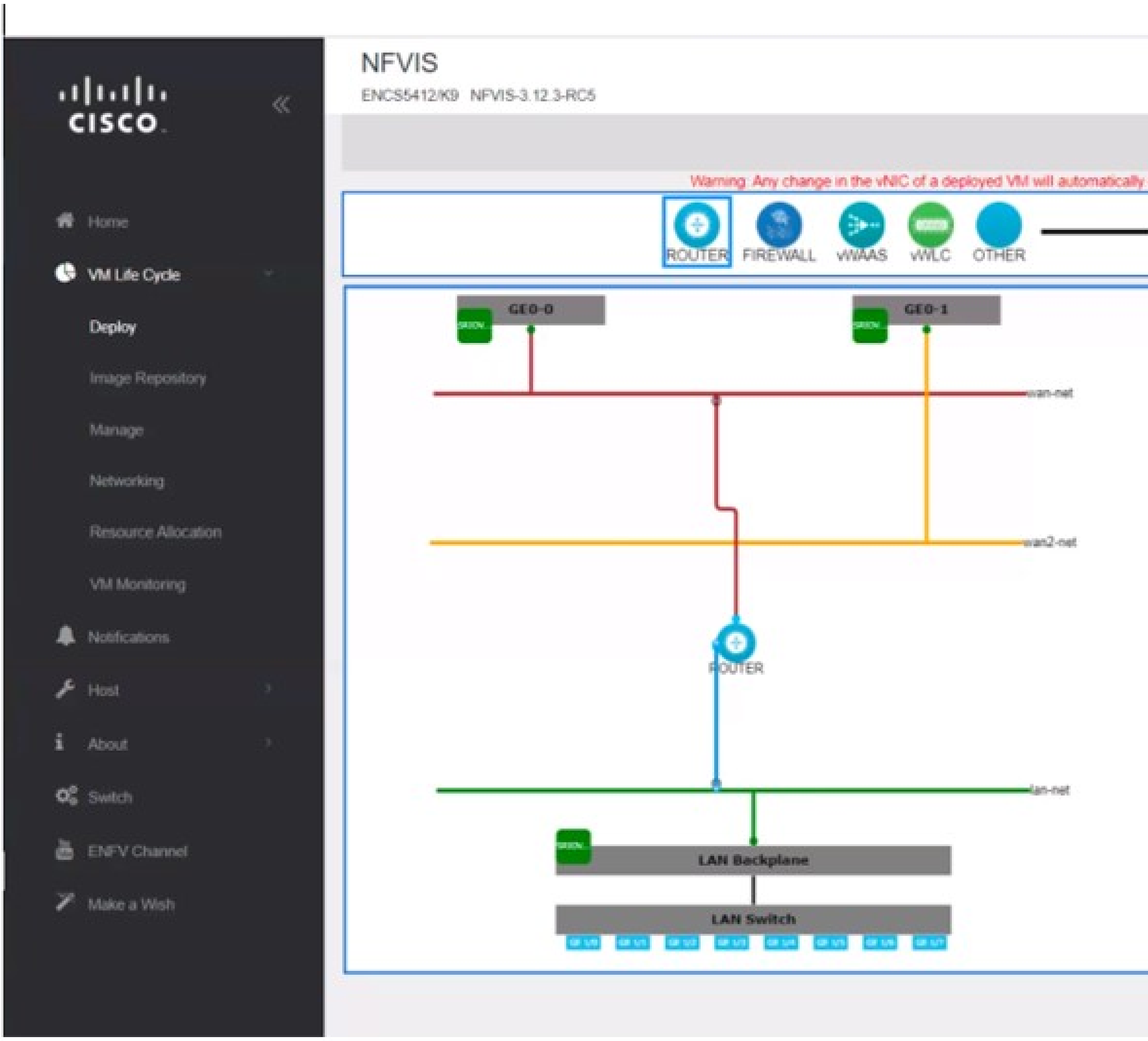
3. To create a router instance with a LAN and WAN connection click and drag **ROUTER** to the center of the page. To configure a connection to the WAN, click **ROUTER** on the page and drag it to the `wan-net` line.

   Select the connected line to view the details. In the vNIC details pane you will see that the interface `GigabitEthernet2` is associated with the WAN (`wan-net`). Record this interface name to use the same name to configure the WAN subnet later.



To configure a LAN connection, click **ROUTER** again and this time drag it to the `lan-net` line.

Select the connected line to view the details. In the vNIC details pane you will see that interface `GigabitEthernet3` is associated with the LAN (`lan-net`). Record this interface name to use this same name to configure the local subnet later.

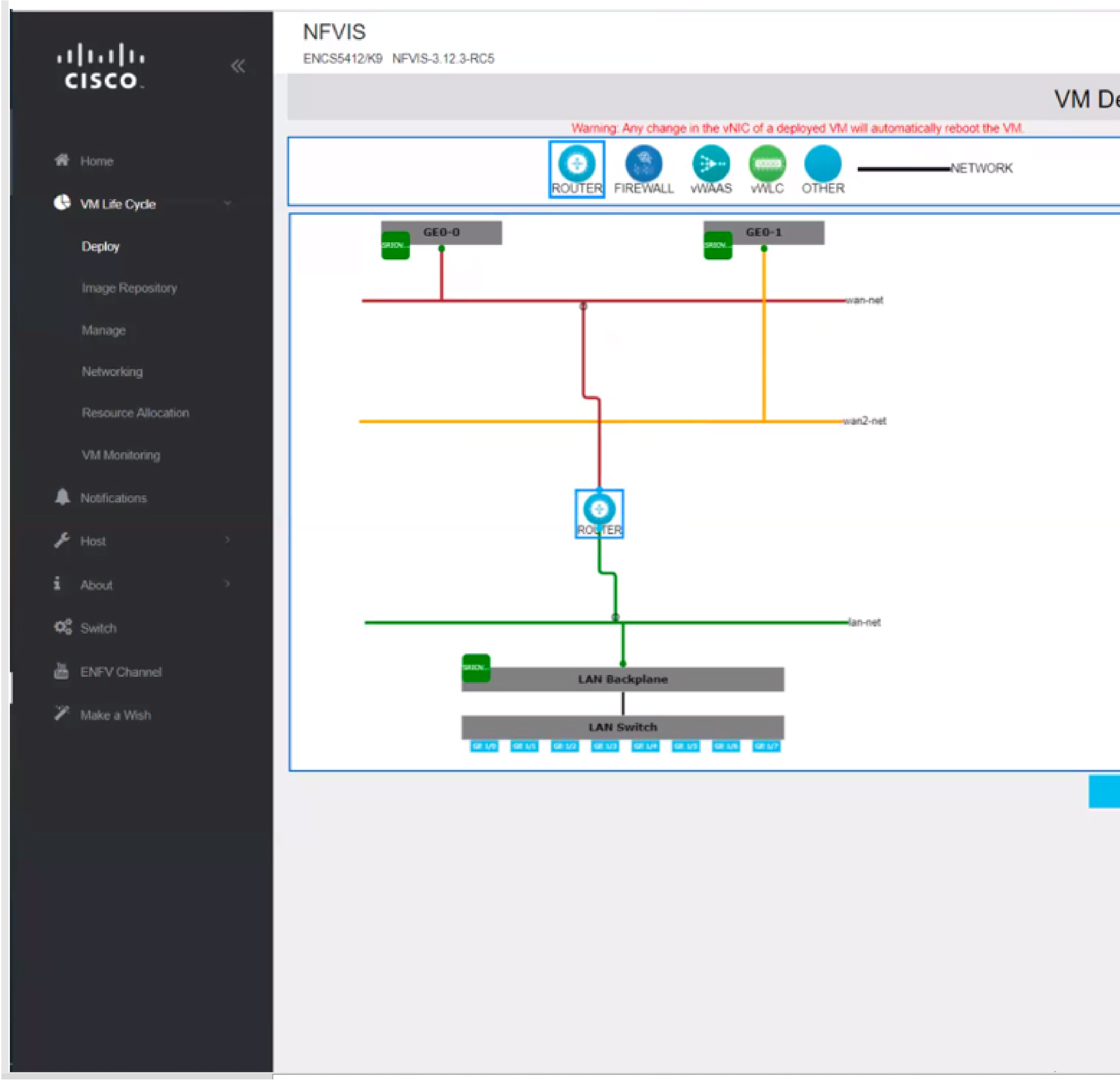


Warning: Any change in the vNIC of a deployed VM will automatically

4. Click on **ROUTER** and enter the **VM Details**:

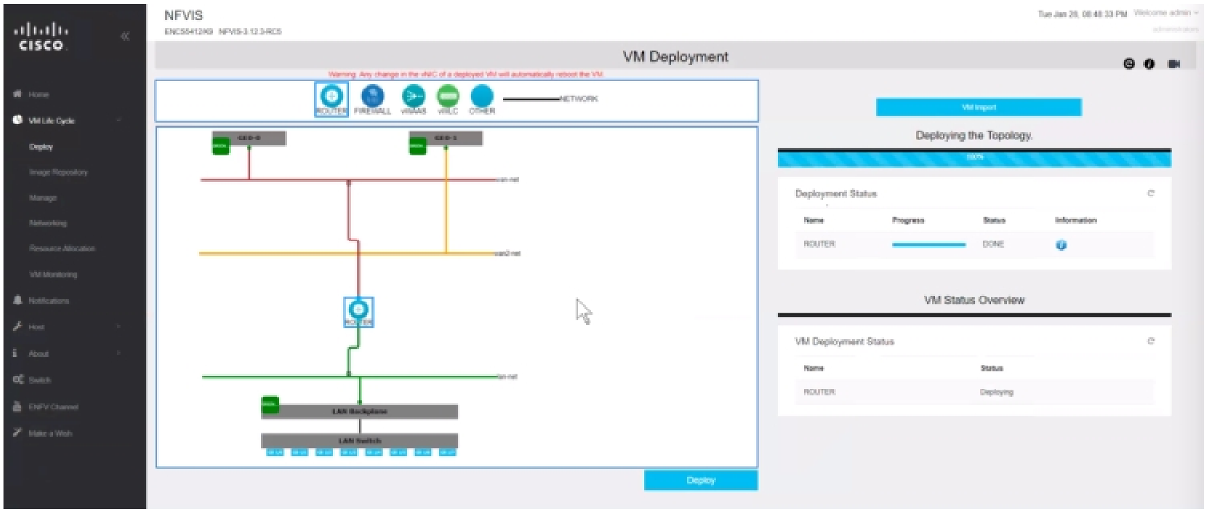
```
Profile: isrv-small
SSH USERNAME: admin
SSH PASSWORD: time44Fun
Port Number: 22
External Port Range: 2001
Source Bridge: MGMT
Deployment Disk: datastore1(internal)
```

These values indicate that the VM uses **`isrv-small`** profile which is has 2 CPUs, 4 GB of memory, and 8 GB of disk space. You can remotely login to this VM through SSH with the credentials specified in **SSH USERNAME** and **SSH PASSWORD**. The **Port Number** and **External Port Range** values maps port 2001 on the management network IP address to port number 22 in the VM, as required for SSH connectivity into the VM over the management network (Source Bridge = MGMT). This VNF will be stored in the default datastore named as datastore1(internal).



Warning: Any change in the vNIC of a deployed VM will automatically reboot the VM.

5. Click **Deploy** to deploy the VM and see the progress of the deployment on the right side of the page. A successful deployment is indicated through a pop-up message on the corner of the page.



VM Deployment

Warning: Any change in the vNIC of a deployed VM will automatically reboot the VM.

Deploying the Topology.

Deployment Status

Name	Progress	Status	Information
ROUTER		DONE	

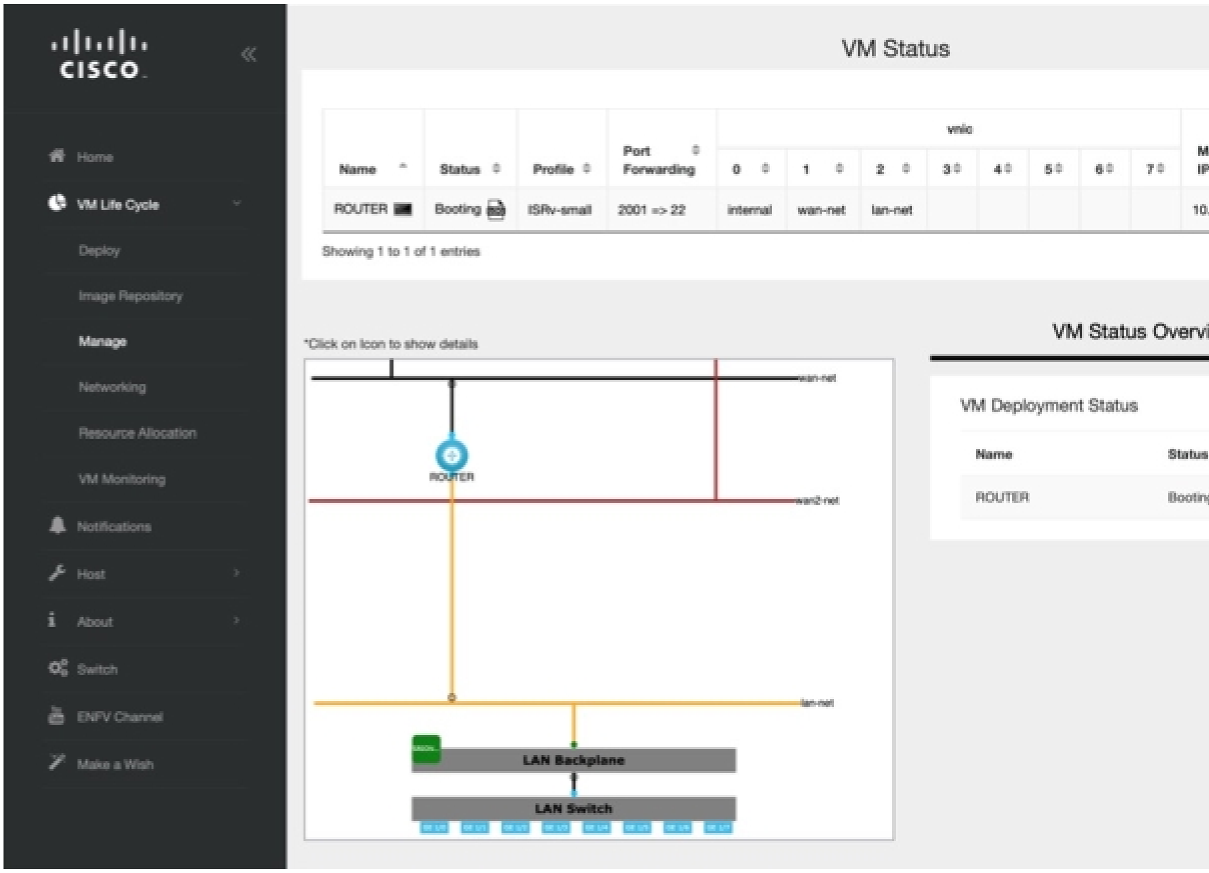
VM Status Overview

VM Deployment Status

Name	Status
ROUTER	Deploying

6. To monitor the progress of the router VNF booting, chose **VM Life Cycle** > **Manage**.

   The status of the deployment is displayed in **VM Status Overview**. Click on the refresh button to get the latest status.



VM Status

Name	Status	Profile	Port Forwarding	vnic 0	1	2	3	4	5	6	7	M IP
ROUTER	Booting	ISRv-small	2001 => 22	internal	wan-net	lan-net						10.

Showing 1 to 1 of 1 entries

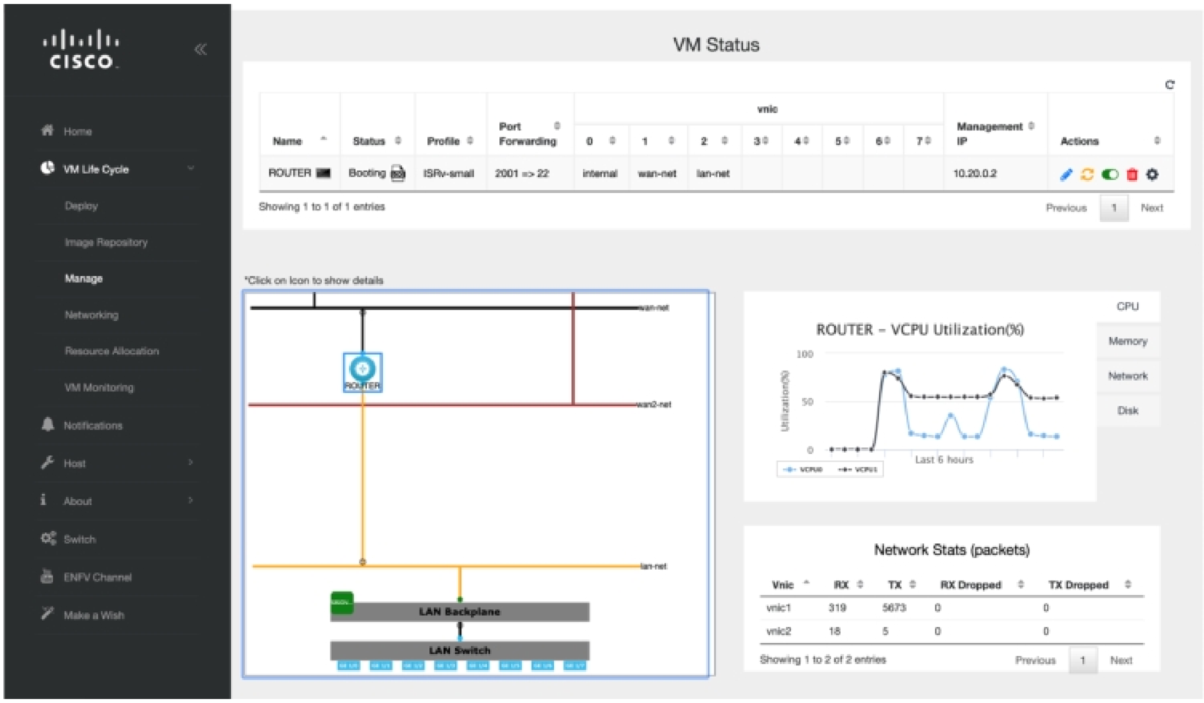
*Click on Icon to show details

VM Status Overvi

VM Deployment Status

Name	Status
ROUTER	Bootin

7. When the router VNF is ready you can see all the data related to it.



VM Status

Name	Status	Profile	Port Forwarding	vnic 0	vnic 1	vnic 2	vnic 3	vnic 4	vnic 5	vnic 6	vnic 7	Management IP	Actions
ROUTER	Booting	ISRv-small	2001 => 22	internal	wan-net	lan-net						10.20.0.2	

Showing 1 to 1 of 1 entries

Previous 1 Next

*Click on Icon to show details

Network Stats (packets)

Vnic	RX	TX	RX Dropped	TX Dropped
vnic1	319	5673	0	0
vnic2	18	5	0	0

Showing 1 to 2 of 2 entries

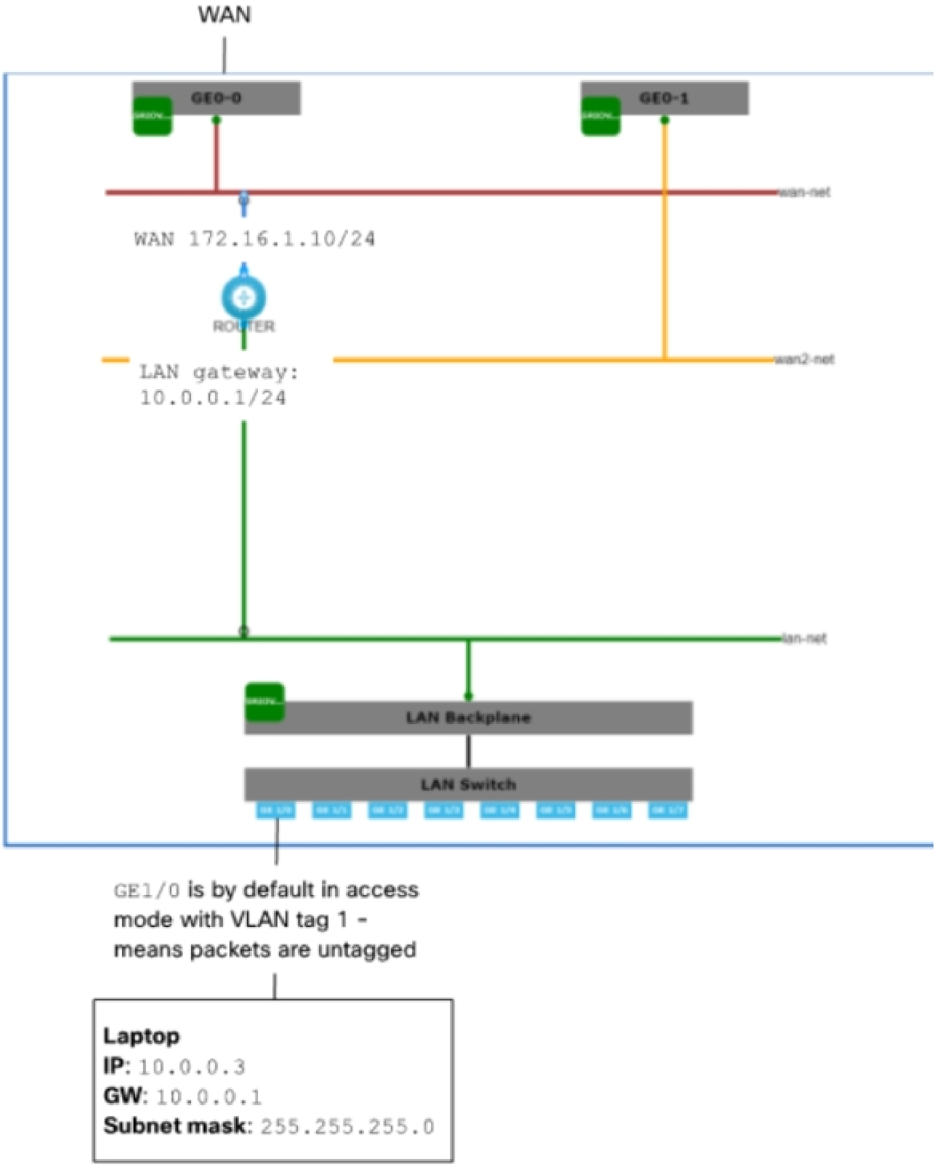
Previous 1 Next

You have now completed the creation and deployment of ISRv router VNF instance.

LAN to WAN Connectivity

After successfully creating and deploying the virtual router, configure the virtual router to enable traffic flow from the LAN network to the WAN. The following image shows the LAN to WAN connectivity through a virtual router:

Figure 5: LAN and WAN Connection Through Virtual Router



The traffic flow from the laptop to WAN is through the physical 8-port embedded switch in ENCS and the OVS virtual switch lan-net. The laptop is connected to port GE1/0 on the embedded 8-port switch with an Ethernet cable. The laptop has `10.0.0.3` as static IP address, `10.0.0.1` as gateway IP address and subnet mask as `255.255.255.0`.

By default, GE1/0 port is configured to be in access mode with VLAN tag 1, the internal virtual lan-net OVS switch is in trunk mode and the virtual router is configured to accept the untagged traffic.

The gateway IP address `10.0.0.1` is configured on the virtual router. The virtual router is connected to the external WAN port that enables traffic to flow to and from the WAN.

During the router VNF deployment, you need to set external port, and source-bridge pointing out same bridge that is used to provide access to the system, such as wan-br or lan-br. Now you should be able to SSH to this router VNF from your laptop on the management network. To login:

```
ssh admin@10.29.43.84:2001
```

Use the same password as what you had specified while creating the VNF instance:

```
time44Fun
```

Configure the LAN facing interface of the router to 10.0.0.1/24 subnet:

```
interface GigabitEthernet3
ip address 10.0.0.1 255.255.255.0
```

Configure the WAN side of the router:

```
interface GigabitEthernet2
ip address 172.16.1.10 255.255.255.0
```

Set the default route:

```
ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

Now from the laptop you should be able to reach any destination on the WAN.

You have now successfully deployed a virtual router on a factory shipped ENCS 5400 device. For further configurations, see Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide.

CHAPTER 3

Install Cisco Enterprise NFVIS Using CIMC

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

Install NFVIS Through CIMC

Install Cisco Catalyst 8300 Series Edge uCPE Using CIMC

Minimum supported releases: Cisco NFVIS Release 4.12.2 and Cisco SD-Branch Release 20.12.2.

1. **Access the CIMC Interface**: Login to CIMC using your administrator credentials.

2. Load the Cisco NFVIS operating system installation disk into vKVM-mapped vDVD, or copy the disk image files to your computer. Launch the console from the CIMC Home page, click **Launch vKVM** from the Toolbar.

   Ensure that the vKVM-mapped vDVD is in boot order.

   Reboot the server. When the server reboots, it begins the installation process from the vKVM-mapped vDVD.

3. **Prepare the Installation Media**: You can download, map, unmap, or delete a host image. Download a host image, such as Linux from a remote FTP or HTTP server onto the CIMC internal repository and then map the image onto the virtual drive of a USB controller in the Cisco Catalyst 8300 Series Edge uCPE. After you map the image, set the boot order to make the virtual drive, in which the image is mounted, as the first boot device, and then reboot the server. The host image must have .iso as the file extension. For example,

   For more detailed information on host image mapping see, Host Image Mapping.

4. **Map the host Image**: In the CIMC interface, navigate to the **Compute** menu and click **Host Image Mapping** tab. Browse to the location of your ISO image, and upload. You see the ISO image listed in the **Host Image Mapping Information** tab and click **Map Selected Image**. Reboot the server.

Note Set the boot order to make the virtual drive in which the image is mounted as the first boot device.

5. **Manage Server Power**: In the Navigation pane, click the **Chassis** > **Summary** > **Host Power Link**.

Click **Hard Reset** to reboot the server.

6. **Follow Installation Prompts**: After the system reboots, continue to monitor the KVM window with regards to the booting process. Follow the prompts you see to complete the installation process. Follow the prompts, providing the required information as requested.
7. **Confirm Installation**: Once the installation is complete, the system reboots again. You can confirm the installation by logging into the Cisco NFVIS and checking the system status.

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

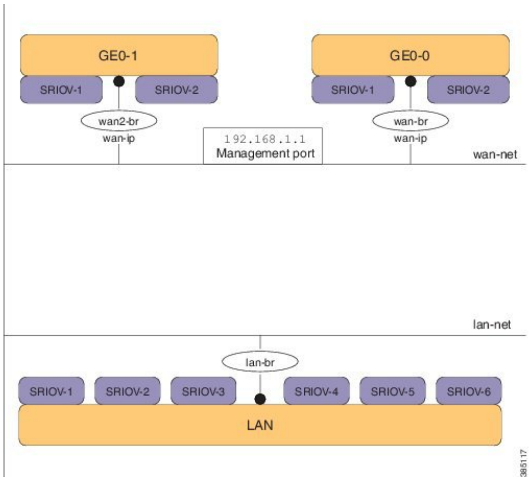
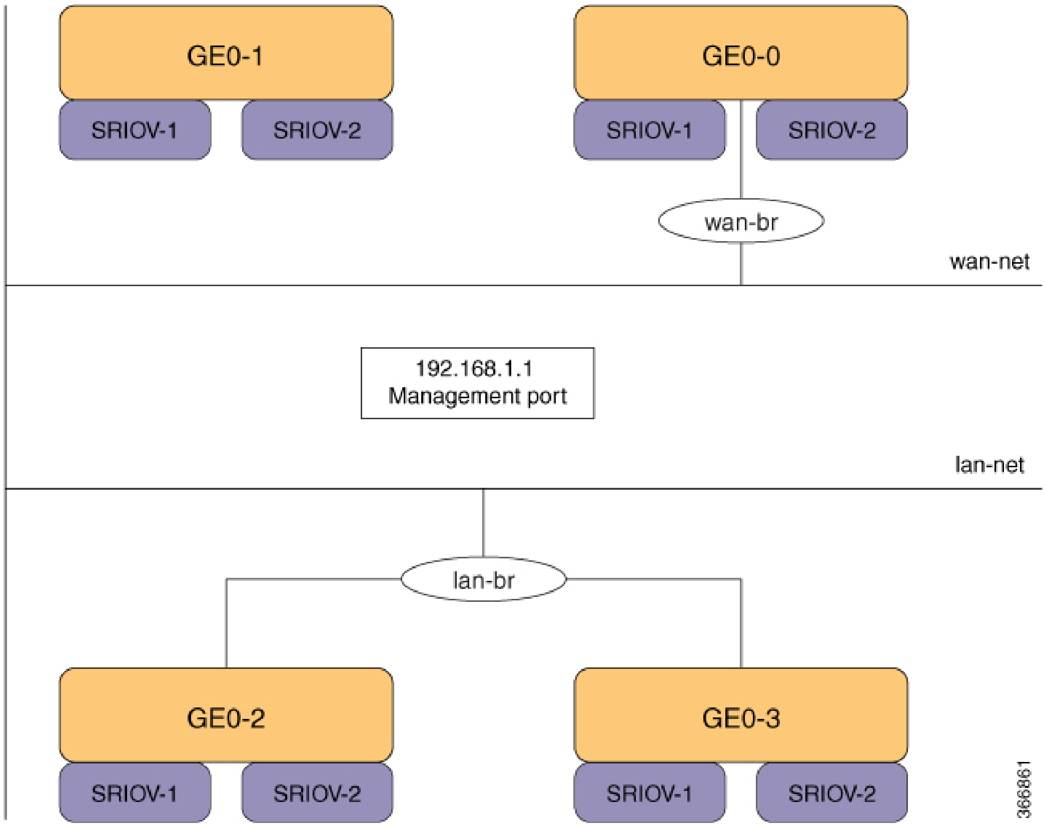


Figure 7: Default Network Configuration of Cisco Enterprise NFVIS with the Cisco ENCS 5100



- 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 Cisco NFVIS 4.6.1 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.
- Starting from Cisco NFVIS release 4.8.1 till Cisco NFVIS release 4.12.1, installing Cisco NFVIS on Cisco UCS C-Series Servers aren't supported.
- Starting from Cisco NFVIS release 4.13.1, install Cisco NFVIS on Cisco UCS C-Series Servers including Cisco UCS C-M6 Rack servers using Cisco NFVIS Smart Licensing feature.
- Starting from Cisco NFVIS 4.10.1, Cisco NFVIS can't be installed on Cisco CSP platforms.

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.

The recommended CIMC version for Cisco UCS-C Series Rack Servers is 4.3(2) or later versions.

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.

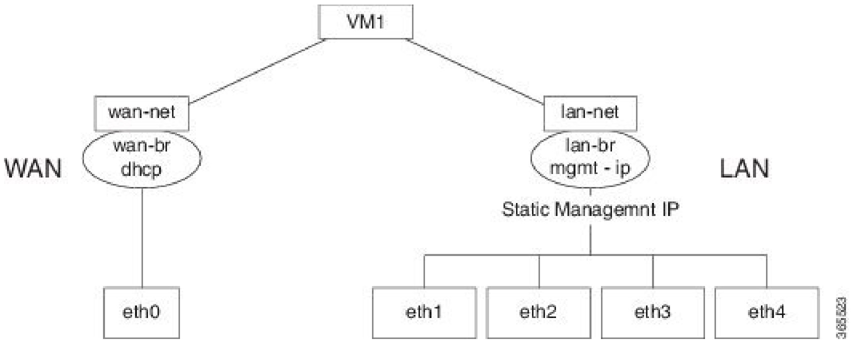
Note The system prompts you to change the default password at the first login attempt. You must set a strong password as per the on-screen instructions to proceed with the application. You cannot run API commands or proceed with any tasks unless you change the default password at the first login. The 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 8: 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.

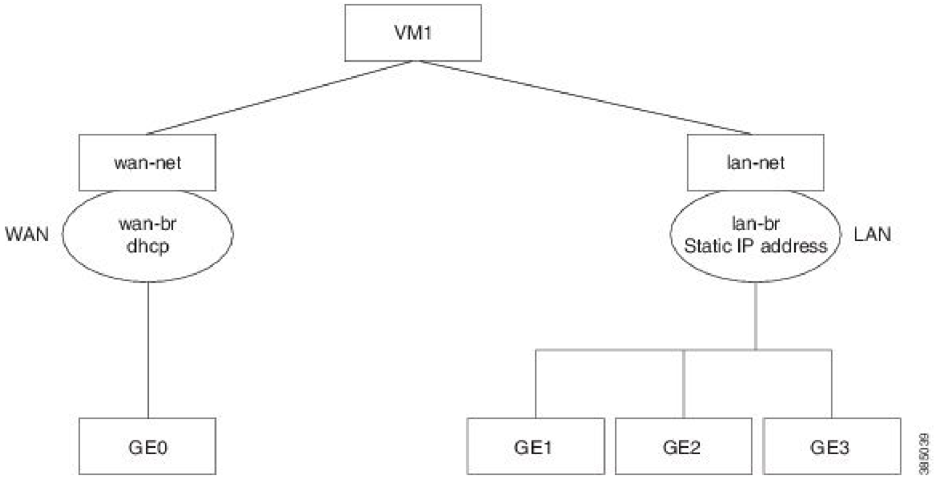
Use **admin** as the login name and **Admin123#** as the default password.

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 9: 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.

CHAPTER 4

Install Cisco Enterprise NFVIS Using USB

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.

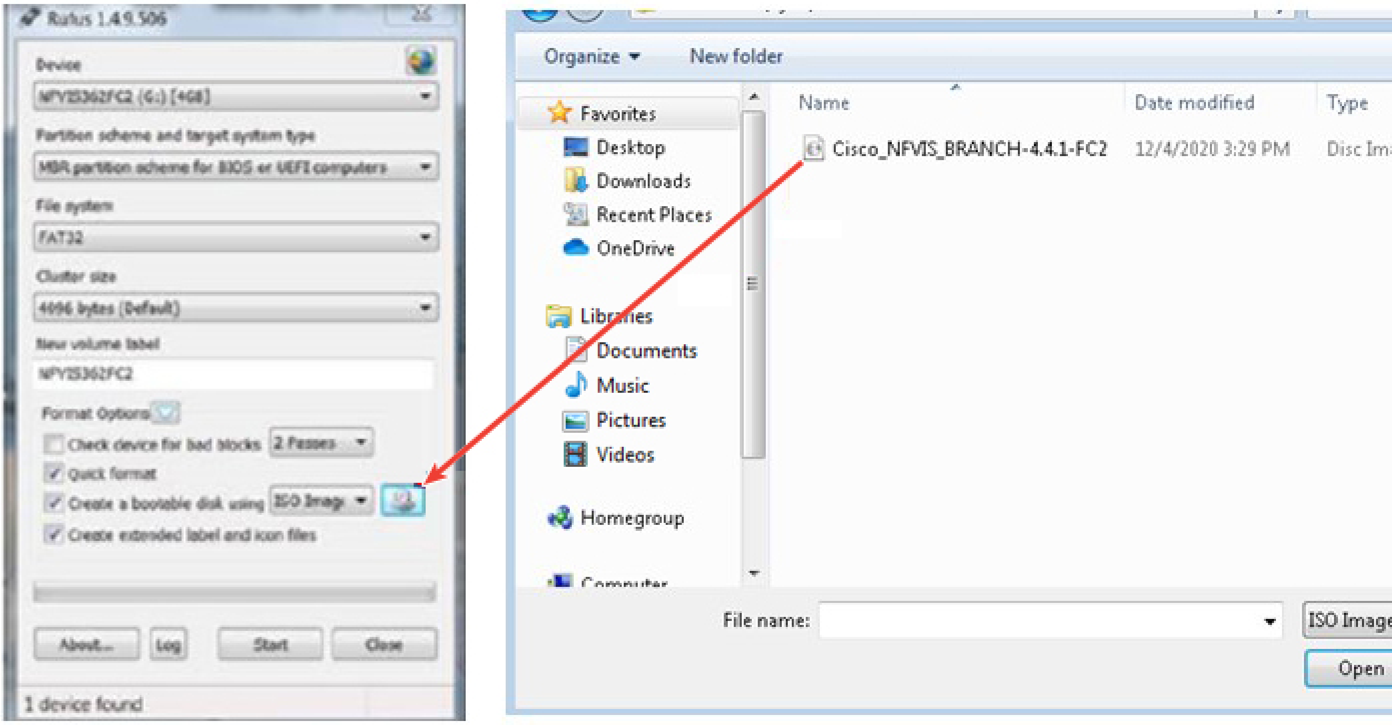
Step 1 Create bootable USB with NFVIS image.

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



Rufus 1.4.9.506

Device: NFVIS362FC2 (G:) [4GB]

Partition scheme and target system type: MBR partition scheme for BIOS or UEFI computers

File system: FAT32

Cluster size: 4096 bytes (Default)

New volume label: NFVIS362FC2

Format Options

□ Check device for bad blocks 2 Passes

☑ Quick format

☑ Create a bootable disk using ISO Image

☑ Create extended label and icon files

1 device found

Name	Date modified	Type
Cisco_NFVIS_BRANCH-4.4.1-FC2	12/4/2020 3:29 PM	Disc Im

File name: ISO Image

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

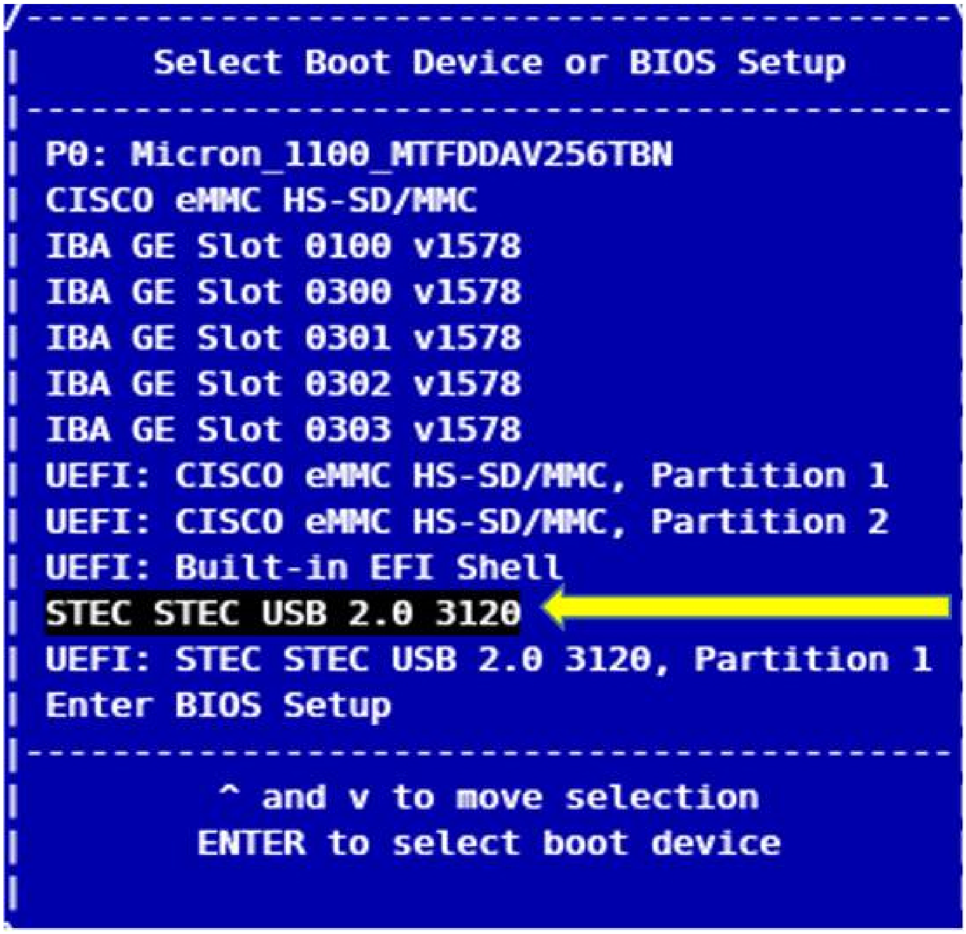
Step 3 Power on system.

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.



```
/----------------------------------------
|       Select Boot Device or BIOS Setup
|----------------------------------------
| P0: Micron_1100_MTFDDAV256TBN
| CISCO eMMC HS-SD/MMC
| IBA GE Slot 0100 v1578
| IBA GE Slot 0300 v1578
| IBA GE Slot 0301 v1578
| IBA GE Slot 0302 v1578
| IBA GE Slot 0303 v1578
| UEFI: CISCO eMMC HS-SD/MMC, Partition 1
| UEFI: CISCO eMMC HS-SD/MMC, Partition 2
| UEFI: Built-in EFI Shell
| STEC STEC USB 2.0 3120
| UEFI: STEC STEC USB 2.0 3120, Partition 1
| Enter BIOS Setup
|----------------------------------------
|         ^ and v to move selection
|          ENTER to select boot 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.

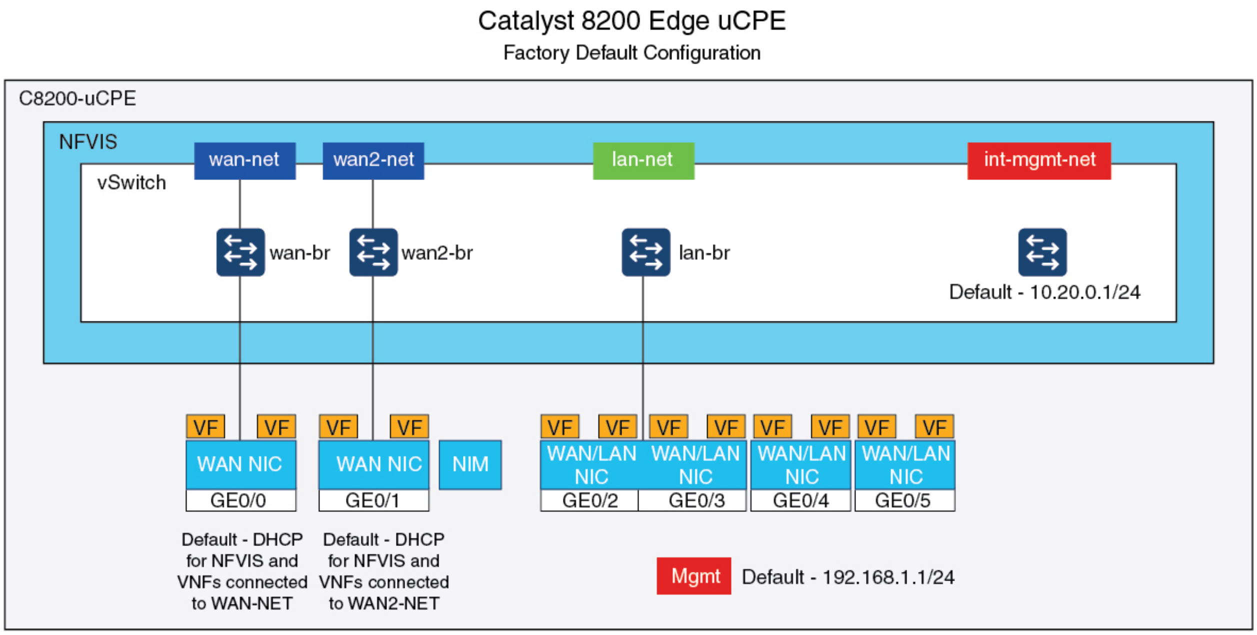
What to do next

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, on page 37

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.

CHAPTER 5

Upgrade Cisco NFVIS

The Cisco NFVIS enabled hardware comes preinstalled with Cisco NFVIS version. Follow the steps below to upgrade it to the latest version of the release.

The Cisco Enterprise NFVIS upgrade image is available as a `.iso` and `.nfvispkg` file. Currently, downgrade is not supported. All RPM packages in the Cisco Enterprise NFVIS upgrade image are signed to ensure cryptographic integrity and authenticity. In addition, all RPM packages are verified during Cisco Enterprise NFVIS upgrade.

Ensure that you copy the image to the Cisco NFVIS server before starting the upgrade process. Always specify the exact path of the image when registering the image. Use the **scp** command to copy the upgrade image from a remote server to your Cisco Enterprise NFVIS server. When using the **scp** command, you must copy the image to the "`/data/intdatastore/uploads`" folder on the Cisco Enterprise NFVIS server.

Note

- In Cisco NFVIS release 4.2.1 and earlier releases, you can upgrade Cisco NFVIS from one release to the very next release using the .nfvispkg file. For example, you can upgrade your NFVIS from Cisco NFVIS release 3.5.2 to Cisco NFVIS release 3.6.1.
- Starting from Cisco NFVIS release 4.4.1, you can upgrade NFVIS using .iso file.
- 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.

Upgrade Matrix for Upgrading Cisco NFVIS

Note

- Use the following table to upgrade from your current version of Cisco NFVIS software to the latest supported upgrade versions only. If you upgrade to an unsupported version, the system might crash.
- Upgrading using .iso file is recommended if the supported upgrade image type is both .iso and .nfvispkg.

Table 1: Upgrade Matrix for Upgrading Cisco NFVIS from Cisco NFVIS Release 4.6.1 and later

Running Version	Supported Upgrade Version	Supported Upgrad
4.14.1	4.15.1 (future release)	iso
4.13.1	4.15.1 (future release) 4.14.1	iso
4.12.3	4.15.1 (future release) 4.14.1	iso
4.12.2	4.15.1 (future release) 4.14.1 4.13.1 4.12.3	iso
4.12.1	4.15.1 (future release) 4.14.1 4.13.1 4.12.3	iso
4.11.1	4.12.3	iso
4.10.1	4.11.1 4.12.3	iso
4.9.5	4.12.3	
4.9.4	4.12.3	
	4.9.5	
4.9.3	4.12.3	iso
	4.11.1	
	4.9.4 and 4.9.5	

4.9.2	4.12.3	iso
	4.11.1	
	4.9.3, 4.9.4, and 4.9.5	
4.9.1	4.12.3	iso
	4.11.1	
	4.10.1	
	4.9.5, 4.9.4, 4.9.3, and 4.9.2	
4.8.1	4.9.4	iso
	4.9.3	
	4.9.2	
	4.9.1	
4.7.1	4.9.4	iso
	4.9.3	
	4.9.2	
	4.9.1	
	4.8.1	iso, nfvispkg
4.6.3	4.9.4	iso
	4.9.3	
	4.9.2	
	4.9.1	
	4.8.1	
	4.7.1	nfvispkg
4.6.2	4.9.1 or 4.9.2 or 4.9.3 or 4.9.4	iso
	4.8.1	
	4.7.1	
	4.6.3	

4.6.1	4.9.1 or 4.9.2 or 4.9.3 or 4.9.4	iso
	4.8.1	
	4.7.1	iso, nfvispkg
	4.6.3	iso

Table 2: Upgrade Matrix for Upgrading Cisco NFVIS from Cisco NFVIS Release 4.5.1 and earlier

Running Version	Supported Upgrade Version	Supported Upgrade Image Type(s)
4.5.1	4.7.1	iso
	4.6.3	iso, nfvispkg
	4.6.2	iso, nfvispkg
	4.6.1	iso, nfvispkg
4.4.2	4.6.3	iso
	4.6.2	iso
	4.6.1	iso
	4.5.1	iso, nfvispkg
4.4.1	4.6.3	iso
	4.6.2	iso
	4.6.1	iso
	4.5.1	iso, nfvispkg
	4.4.2	iso, nfvispkg
4.2.1	4.4.2	nfvispkg
	4.4.1	nfvispkg
4.1.2	4.2.1	nfvispkg
4.1.1	4.2.1	nfvispkg
	4.1.2	nfvispkg
3.12.3	4.1.1	nfvispkg
3.11.3	3.12.3	nfvispkg
3.10.3	3.11.3	nfvispkg
3.9.2	3.10.3	nfvispkg
3.8.1	3.9.2	nfvispkg

Restrictions for Cisco NFVIS ISO File Upgrade

- Cisco NFVIS supports .iso upgrade only from version N to versions N+1, N+2 and N+3 starting from Cisco NFVIS release 4.6.x (except Cisco NFVIS releases 4.7.x and 4.8.x). NFVIS does not support .iso upgrade from version N to version N+4 and above.
- Image downgrade using .iso file is not supported.

Note In case of an error while upgrading from version N to N+1 or N+2, Cisco NFVIS rolls back to the image version N.

Upgrade Cisco NFVIS 4.8.1 and Later Using ISO File

The following example shows how to use the **scp** command to copy the upgrade image:

- To copy the upgrade image, use the **scp** command from Cisco NFVIS CLI:

```
nfvis# scp
admin@192.0.2.9:/NFS/2022-01-23/13/nfvis/iso/Cisco_NFVIS-4.8.0-13-20220123_020232.iso
intdatastore:Cisco_NFVIS-4.8.0-13-20220123_020232.iso
```

- To copy the upgrade image, use the **scp** command from remote linux:

```
config terminal
system settings ip-receive-acl 0.0.0.0/0
service scpd action accept
commit

scp -P22222 Cisco_NFVIS-4.8.0-13-20220123_020232.iso
admin@172.27.250.128:/data/intdatastore/uploads/Cisco_NFVIS-4.8.0-13-20220123_020232.iso
```

Alternatively, you can upload the image to the Cisco Enterprise NFVIS server using the **System Upgrade** option from the Cisco Enterprise NFVIS portal.

Note When the NFVIS upgrade is in progress, ensure that the system is not powered off. If the system is powered off during the NFVIS upgrade process, the system may become inoperable and you may need to reinstall the system.

The upgrade process comprises of two tasks:

1. Register the image using the **system upgrade image-name** command.
2. Upgrade the image using the **system upgrade apply-image** command.

Register an Image

To register an image, use the following command:

```
config terminal
system upgrade image-name Cisco_NFVIS-4.8.0-13-20220123_020232.iso location
/data/intdatastore/uploads/Cisco_NFVIS-4.8.0-13-20220123_020232.iso
commit
```

Note You must verify the image registration status before upgrading the image using the **system upgrade apply-image** command. The package status must be valid for the registered image.

To verify the image registration status, use the following command:

```
nfvis# show system upgrade

                 PACKAGE
NAME                                     LOCATION
                 VERSION   STATUS  UPLOAD DATE
------------------------------------------------------------------------------------------
Cisco_NFVIS-4.8.0-13-20220123_020232.iso
/data/upgrade/register/Cisco_NFVIS-4.8.0-13-20220123_020232.iso  4.8.0-13  Valid
2022-01-24T02:40:29.236057-00:00


nfvis# show system upgrade reg-info

                 PACKAGE
NAME                                     LOCATION
                 VERSION   STATUS  UPLOAD DATE
------------------------------------------------------------------------------------------
Cisco_NFVIS-4.8.0-13-20220123_020232.iso
/data/upgrade/register/Cisco_NFVIS-4.8.0-13-20220123_020232.iso  4.8.0-13  Valid
2022-01-24T02:40:29.236057-00:00
```

Upgrade the Registered Image

To upgrade the registered image, use the following command:

```
config terminal
system upgrade apply-image Cisco_NFVIS-4.8.0-13-20220123_020232.iso scheduled-time 5
commit
```

To verify the upgrade status, use the **show system upgrade apply-image** command in the privileged EXEC mode.

```
nfvis# show system upgrade
                                                    UPGRADE  UPGRADE
NAME                                      STATUS     FROM     TO
-----------------------------------------------------------------------
Cisco_NFVIS-4.8.0-13-20220123_020232.iso  SCHEDULED  -        -


                 PACKAGE
NAME                                     LOCATION
```

```
                 VERSION   STATUS  UPLOAD DATE
------------------------------------------------------------------------------------------
Cisco_NFVIS-4.8.0-13-20220123_020232.iso
/data/upgrade/register/Cisco_NFVIS-4.8.0-13-20220123_020232.iso  4.8.0-13  Valid
2022-01-24T02:40:29.236057-00:00
```

Upgrade APIs and Commands

The following table lists the upgrade APIs and commands:

Upgrade APIs	Upgrade Commands
• /api/config/system/upgrade • /api/config/system/upgrade/image-name • /api/config/system/upgrade/reg-info • /api/config/system/upgrade/apply-image	• system upgrade image-name • system upgrade apply-image • show system upgrade reg-info • show system upgrade apply-image

Upgrade Cisco NFVIS 4.7.1 and Earlier Using a .nvfispkg File

The following example shows how to use the **scp** command to copy the upgrade image:

scp command from NFVIS CLI:

```
nfvis# scp admin@192.0.2.9:/NFS/Cisco_NFVIS_BRANCH_Upgrade-351.nfvispkg
intdatastore:Cisco_NFVIS_BRANCH_Upgrade-351.nfvispkg
```

scp command from remote linux:

```
config terminal
system settings ip-receive-acl 0.0.0.0/0
service scpd action accept
commit

scp -P 22222 nfvis-351.nfvispkg admin@192.0.2.9:/data/intdatastore/uploads/nfvis-351.nfvispkg
```

Alternatively, you can upload the image to the Cisco Enterprise NFVIS server using the **System Upgrade** option from the Cisco Enterprise NFVIS portal.

Note When the NFVIS upgrade is in progress, ensure that the system is not powered off. If the system is powered off during the NFVIS upgrade process, the system may become inoperable and you may need to reinstall the system.

The upgrade process comprises two tasks:

- Registering the image using the **system upgrade image-name** command.
- Upgrading the image using the **system upgrade apply-image** command.

Register an Image

To register an image:

```
config terminal
system upgrade image-name nfvis-351.nfvispkg location
/data/intdatastore/uploads/<filename.nfvispkg>
commit
```

Note You must verify the image registration status before upgrading the image using the **system upgrade apply-image** command. The package status must be valid for the registered image.

Verify the Image Registration

Use the **show system upgrade reg-info** command in the privileged EXEC mode to verify the image registration.

```
nfvis# show system upgrade reg-info
PACKAGE
NAME             LOCATION                                       VERSION        STATUS UPLOAD DATE
------------------------------------------------------------------------------------------
nfvis-351.nfvispkg /data/upgrade/register/nfvis-351.nfvispkg 3.6.1-722 Valid
2017-04-25T10:29:58.052347-00:00
```

Upgrade the Registered Image

To upgrade the registered image:

```
config terminal
system upgrade apply-image nfvis-351.nfvispkg scheduled-time 5
commit
```

Verify the Upgrade Status

Use the **show system upgrade apply-image** command in the privileged EXEC mode

```
nfvis# show system upgrade apply-image
UPGRADE
NAME   STATUS     FROM     UPGRADE TO
------------------------------------------------------------------------------------------
nfvis-351.nfvispkg SUCCESS 3.5.0 3.5.1
```

The only upgrade supported when BIOS secured boot (UEFI mode) is enabled on ENCS 5400 platform is:

NFVIS 3.8.1 + BIOS 2.5(legacy) --> NFVIS 3.9.1 + BIOS 2.6(legacy)

The following upgrade requires re-installation of NFVIS in UEFI mode:

NFVIS 3.8.1 + BIOS 2.5(legacy) --> NFVIS 3.9.1 + BIOS 2.6(UEFI)

NFVIS 3.9.1 + BIOS 2.6(legacy) --> NFVIS 3.9.1 + BIOS 2.6(UEFI)

Upgrade APIs and Commands

The following table lists the upgrade APIs and commands:

Upgrade APIs	Upgrade Commands
• /api/config/system/upgrade • /api/config/system/upgrade/image-name • /api/config/system/upgrade/reg-info • /api/config/system/upgrade/apply-image	• system upgrade image-name • system upgrade apply-image • show system upgrade reg-info • show system upgrade apply-image

Firmware Upgrade

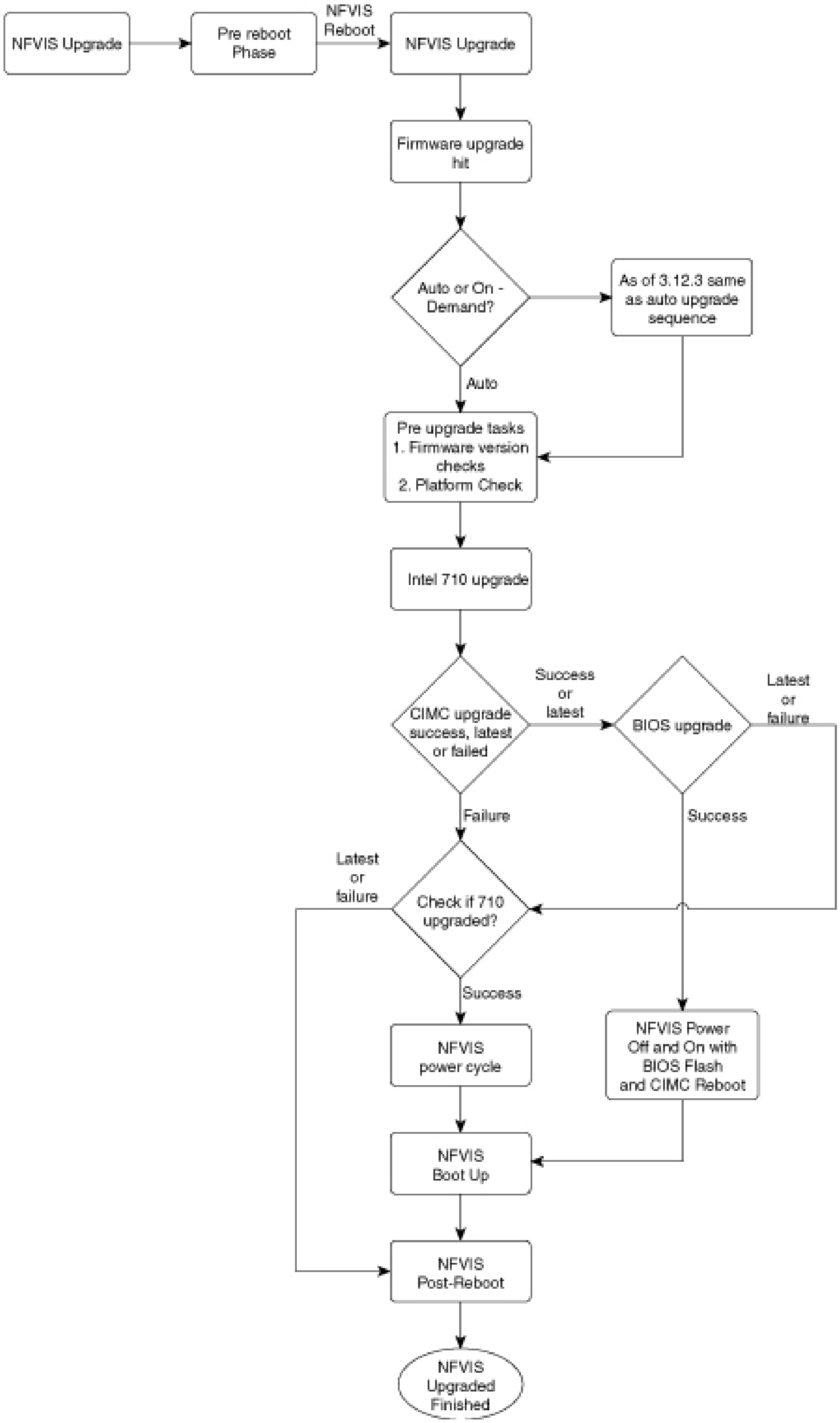
Note Firmware upgrade is supported only on ENCS 5400 series devices.

This feature was introduced in NFVIS 3.8.1 release as part of NFVIS auto-upgrade and it supports upgrade of selected firmwares on ENCS 5400 series devices. Firmware upgrade is triggered during NFVIS upgrade as part of the post reboot phase. To trigger the firmware upgrade refer to the NFVIS upgrade feature.

Starting from NFVIS 3.9.1 release, an on demand upgrade is supported which provides a separate firmware package (.fwpkg extension) to be registered and applied through NFVIS CLI. You can also upgrade to the latest firmware through a fresh installation of NFVIS.

The following firmwares can be upgraded:

- Cisco Integrated Management Controller (CIMC)
- BIOS
- Intel 710
- FPGA


NFVIS Upgrade
Pre reboot Phase
NFVIS Reboot
NFVIS Upgrade
Firmware upgrade hit
Auto or On - Demand?
As of 3.12.3 same as auto upgrade sequence
Auto
Pre upgrade tasks
1. Firmware version checks
2. Platform Check
Intel 710 upgrade
CIMC upgrade success, latest or failed
Success or latest
BIOS upgrade
Latest or failure
Failure
Success
Latest or failure
Check if 710 upgraded?
Success
NFVIS power cycle
NFVIS Power Off and On with BIOS Flash and CIMC Reboot
NFVIS Boot Up
NFVIS Post-Reboot
NFVIS Upgraded Finished

Starting from NFVIS 3.12.3 release, the firmware upgrade script is changed from executable to module format. The code is modularized and each firmware can be individually upgraded. The shell commands are called with subprocess instead of os.system() calls. Each firmware upgrade call is monitored with a time limit. If the call is stuck, the process is killed and execution control will return back to the code flow with appropriate message.

The following table shows the sequence of firmware upgrade:

NFVIS Upgrade	Fresh Install	On Demand Upgrade
Intel 710		
1. NFVIS upgrade **2.** Reboot **3.** Login **4.** Firmware upgrade 710 **5.** NFVIS power cycle **6.** Login	**1.** Install **2.** Reboot **3.** Login **4.** Firmware upgrade 710 **5.** NFVIS power cycle **6.** Login	**1.** Firmware upgrade 710 **2.** NFVIS power cycle **3.** Login
Intel 710 and BIOS		
1. NFVIS upgrade **2.** Reboot **3.** Login **4.** Firmware upgrade 710 and BIOS **5.** NFVIS power off/on due to BIOS **6.** Login	**1.** Install **2.** Reboot **3.** Login **4.** Firmware upgrade 710 and BIOS **5.** NFVIS power off/on due to BIOS **6.** Login	**1.** Firmware upgrade 710 and BIOS **2.** NFVIS power off/on due to BIOS **3.** Login
Intel 710 and CIMC		
1. NFVIS upgrade **2.** Reboot **3.** Login **4.** Firmware upgrade 710 and CIMC **5.** CIMC reboot **6.** NFVIS power cycle due to 710 **7.** Login	**1.** Install **2.** Reboot **3.** Login **4.** Firmware upgrade 710 and CIMC **5.** CIMC reboot **6.** NFVIS power cycle due to 710 **7.** Login	**1.** Firmware upgrade 710 and CIMC **2.** CIMC reboot **3.** NFVIS power cycle due to 710 **4.** Login
CIMC		

NFVIS Upgrade	Fresh Install	On Demand Upgrade
1. NFVIS upgrade 2. Reboot 3. Login 4. Firmware upgrade CIMC 5. CIMC reboot 6. Login	1. Install 2. Reboot 3. Login 4. Firmware upgrade CIMC 5. CIMC reboot 6. Login	1. Firmware upgrade CIMC 2. CIMC reboot 3. Login
CIMC and BIOS		
1. NFVIS upgrade 2. Reboot 3. Login 4. Firmware upgrade CIMC and BIOS 5. NFVIS power off 6. CIMC reboot 7. BIOS flash 8. NFVIS power on 9. Login	1. Install 2. Reboot 3. Login 4. Firmware upgrade CIMC and BIOS 5. NFVIS power off 6. CIMC reboot 7. BIOS flash 8. NFVIS power on 9. Login	1. Firmware upgrade CIMC and BIOS 2. NFVIS power off 3. CIMC reboot 4. BIOS flash 5. NFVIS power on 6. Login
BIOS		
1. NFVIS upgrade 2. Reboot 3. Login 4. Firmware upgrade BIOS 5. NFVIS power off 6. BIOS flash 7. NFVIS power on 8. Login	1. Install 2. Reboot 3. Login 4. Firmware upgrade BIOS 5. NFVIS power off 6. BIOS flash 7. NFVIS power on 8. Login	1. Firmware upgrade BIOS 2. NFVIS power off 3. BIOS flash 4. NFVIS power on 5. Login
Intel 710, CIMC and BIOS		

NFVIS Upgrade	Fresh Install	On Demand Upgrade
1. NFVIS upgrade 2. Reboot 3. Login 4. Firmware upgrade 710, CIMC and BIOS 5. NFVIS power off 6. CIMC reboot 7. BIOS flash 8. NFVIS power on 9. Login	1. Install 2. Reboot 3. Login 4. Firmware upgrade 710, CIMC and BIOS 5. NFVIS power off 6. CIMC reboot 7. BIOS flash 8. NFVIS power on 9. Login	1. Firmware upgrade 710, CIMC and BIOS 2. NFVIS power off 3. CIMC reboot 4. BIOS flash 5. NFVIS power on 6. Login