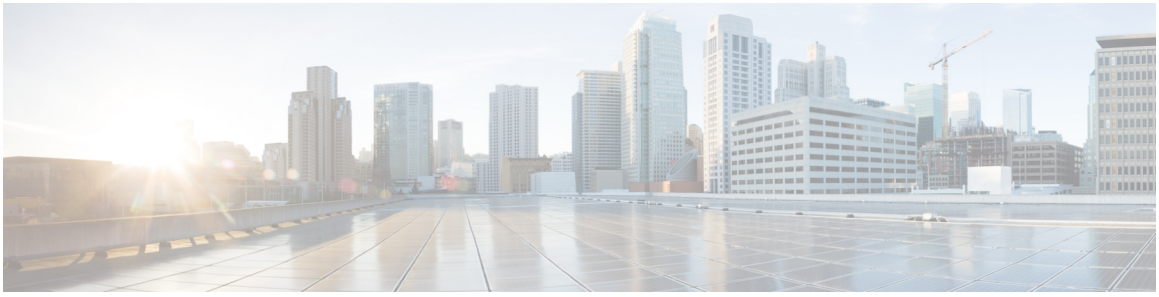


Design and Deployment of Cisco NFVIS SD-Branch using Cisco Catalyst SD-WAN Manager, Release 26.x and Later

First Published: 2026-03-10

Last Modified: 2026-04-24

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



CONTENTS

Short Description ?

CHAPTER 1 **Overview of Cisco NFVIS SD-Branch Solution** 1

Cisco SD-Branch Solution Components 2

Key Tasks Before you Begin 4

CHAPTER 2 **Define Cisco NFVIS SD-Branch Solution** 5

Create Authorized Device List 5

Identity, Trust and Whitelist 7

Create VNF Image Packages 7

Discover and Deploy Devices 12

CHAPTER 3 **Design Cisco NFVIS SD-Branch Solution** 15

Wan Edge Onboarding Methods 15

Automated Deployment 15

Plug-and-Play Process 16

Staging 18

Zero-Trust Model 18

Network Firewall Requirements 19

Network Design 19

Configure Network Design Elements 20

Configure Circuits 21

Configure Branch Sites 21

Configure Global Parameters 25

Configure Device Profiles 28

ENCS Device Profile and Additional Services 33
CLI Add-On Feature Templates 41
Single IP Address Sharing between NFVIS and Router VM 47
Configure Single IP Address Sharing 48
Verify Single IP Address Sharing 49

CHAPTER 4 **Deploy Cisco NFVIS SD-Branch Solution 51**
Prerequisites for NFVIS WAN Edge Onboarding 51
Prerequisites to Onboard NFVIS WAN Edge Devices using PnP Process 52
Onboarding NFVIS device using Plug-and-Play process 53

CHAPTER 5 **Operate Cisco NFVIS SD-Branch Solution 61**
Monitor and Manage the Status of Cisco Catalyst SD-WAN Control Components using Cisco SD-WAN Manager 61
Monitor the Cisco Catalyst SD-WAN Control Components Through Device Pane 61
View WAN Edge Device Details and Statistics Through Device Pane 62
Monitor WAN Edge Device Through Cisco SD-WAN Manager SSH Server Dashboard using CLI Commands 64
Start, Stop, and Restart WAN Edge Devices 65
Troubleshooting Device Onboarding 67
Diagnosing Onboarding Issues 67
Missing root ca certificate on the WAN Edge device 70

CHAPTER 6 **Support for Making Day N Changes to Profiles Attached to a Device 73**
Restrictions for Day N Changes in Network Design 73
Information About Day N Changes in Network Design 74
Configure Day N Changes for Network Profiles 74
Modify Device Name and Branch Name 74
Modify Global Parameters 75
Modify Device Profiles 75
Migrating from Insecure to Secure Configuration, Release 26.1.1 77

CHAPTER 7 **Upgrade Cisco NFVIS Software 79**
Cisco NFVIS Software Upgrade Workflow 79

Support Matrix For Upgrading Cisco NFVIS 80
Information about Cisco NFVIS Software Upgrade Workflow 81
Prerequisites for Using the Cisco NFVIS Software Upgrade Workflow 81
Restrictions for Cisco NFVIS Software Upgrade Workflow 82
Benefits of NFVIS Software Upgrade Workflow 82
Upgrade Cisco NFVIS Using the Software Upgrade Workflow 82
Add the Remote Server 82
Add the Upgrade Software Image 83
Access the NFVIS Software Upgrade Workflow 83
Delete Downloaded Software Image 84
Schedule Software Upgrade Workflow 84
Cisco NFVIS Software Upgrade Using the CLI 85
Verify Software Upgrade Using CLI 87

CHAPTER 8 **Cisco SD-Branch ThousandEyes Support 89**
Information About Cisco SD-Branch ThousandEyes Support 89
Benefits of Cisco SD-Branch ThousandEyes Support 89
Prerequisites for Cisco SD-Branch ThousandEyes Support 90
Restrictions for Cisco SD-Branch ThousandEyes Support 90
Deploy ThousandEyes 90
Monitor Cisco SD-Branch ThousandEyes Support 92

CHAPTER 9 **Manage Cisco Catalyst 8300 Series Edge uCPE using Cisco SD-WAN Manager via NFV Config Group Workflow 93**
Overview of Onboarding Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager 93
Define Cisco Catalyst 8300 Series Edge uCPE In Cisco SD-WAN Manager 94
Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager 96
Deploy Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager 98
Operate Cisco Catalyst 8300 Series Edge uCPE Using Cisco SD-WAN Manager 99

CHAPTER 10 **Manage Cisco NFVIS Devices Using NFV Config Group Workflow 101**
Overview of Onboarding Cisco NFVIS Devices to Cisco SD-WAN Manager 101
Supported Devices 102
Define Cisco NFVIS Devices In Cisco SD-WAN Manager 102

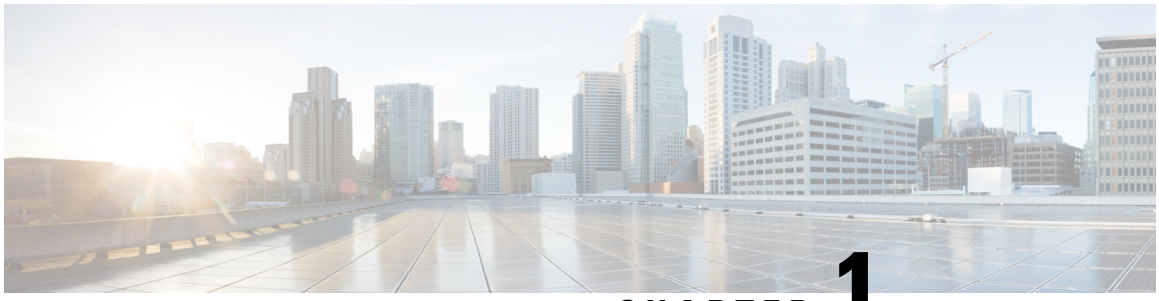
Create a Device List 102
Sync Smart Account Using Cisco SD-WAN Manager 102
Register a Remote Server 103
Upload a VNF QCOW2 103
Use the Quick Connect Workflow 103
Upload .CSV Files 104
Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager 105
Access NFV Configuration Group Workflow 105
Create Add on CLI configuration 106
Associate Cisco NFVIS Devices with Cisco SD-WAN Manager 106
Create a Switch Feature Profile For Cisco ENCS 107
Deploy Cisco NFVIS Devices to Cisco SD-WAN Manager 107
Operate Cisco NFVIS Devices Using Cisco SD-WAN Manager 108

CHAPTER 11 **Onboard Cisco UCS C-Series M6 Devices Using Cisco SD-WAN Manager via NFV Config Group Workflow** 109
Overview of Onboarding Cisco UCS C-Series M6 Devices to Cisco SD-WAN Manager 109
Benefits of Cisco SD-WAN Manager Workflows 110
Supported Devices 110
Define Cisco UCS C-Series M6 Devices in Cisco SD-WAN Manager 111
Create Add on CLI Configuration 113
Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager 113
Deploy Cisco UCS C-Series M6 Devices to Cisco SD-WAN Manager 115
Operate Cisco UCS C-Series M6 Devices Using Cisco SD-WAN Manager 115

CHAPTER 12 **Appendix** 117
NFVIS Deployment in Sites with Low WAN Bandwidth 117
Single IP Address Sharing Between NFVIS and the Router VM 118

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026–2026 Cisco Systems, Inc. All rights reserved.



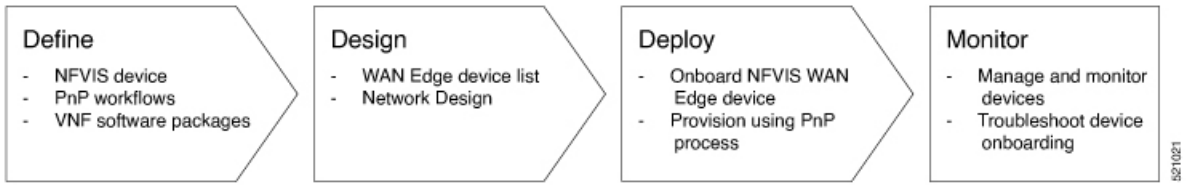
CHAPTER 1

Overview of Cisco NFVIS SD-Branch Solution

Enterprise and service providers, are consolidating network services from dedicated hardware appliances into virtualized on-demand applications. These applications run on branch office softwares with a centralized orchestration and management. The branch office softwares eliminates the dependency on hardware for each function at the branch, simplifies configurable tasks, reduces time and centralizes operations and management. This increases the ability of operators to deploy Network Function Virtualization (NFV) services with greater speed and flexibility.

Cisco Software-Defined Branch (SD-Branch) solution is a combination of simplified hardware, software and virtualized services that can be deployed in a short time. Cisco SD-Branch solution allows you to select from a list of cisco validated designs templates and deploy full-service branch in a matter of minutes.

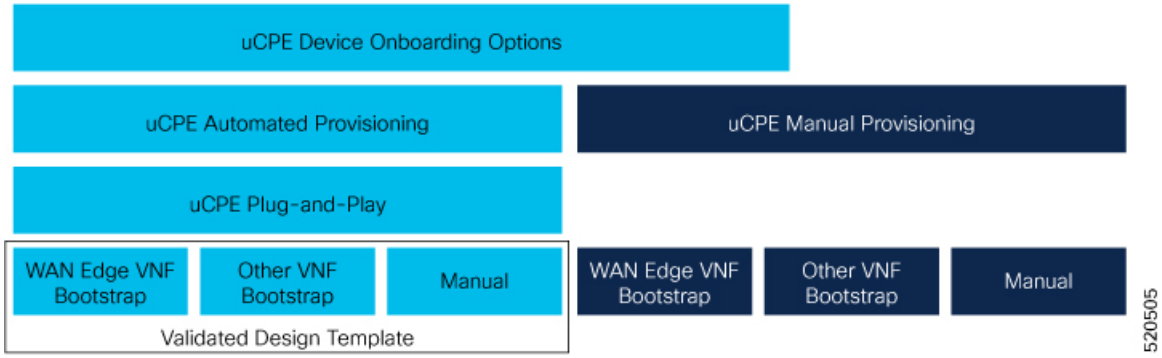
With centralized orchestration and WAN network management, Cisco SD-Branch solution provides the ability to configure and manage initial deployment, change and add new services to your IT environment from a single location, and eliminates the time taken to visit each individual branch office. The orchestration manages existing SD-Branch services, new network service on-boarding, virtual network function (VNF) packages, network services lifecycle management, global resource management, and validation and authorization of SD-Branch infrastructure resource requests, from a single point.



Cisco SD-Branch solution includes the following orchestration functions:

- Service coordination and instantiation: The orchestration software communicates with the underlying Cisco SD-Branch platform to instantiate a service, creating the virtual instance of a service on the platform.
- Service chaining: Connects network services like routing, firewalls and WAN optimization in a virtual chain and optimizes the use of network resources while improving the application performance.
- Scaling services: Manages sufficient resources to deliver the service when there is an increase in the number of services.
- Service monitoring: Tracks the performance of the platform and resources to ensure that they are adequate to provide a good service.

This document provides design and deployment instructions for NFVIS SD-Branch solution and focuses on how to deploy ENCS 5400 uCPE WAN Edge device and other virtualized network services or applications in a branch environment.



- Cisco SD-Branch Solution Components, on page 2
- Key Tasks Before you Begin, on page 4

Cisco SD-Branch Solution Components

The various components of Cisco SD-branch solution are:

- **Hardware Components**:
  - **Cisco 5000 Enterprise Network Compute System** - The Cisco 5000 Enterprise Network Compute System (ENCS) is a line of compute appliances designed for the Cisco SD-Branch and Enterprise Network Functions Virtualization (ENFV) solution. The 5000 ENCS is a hybrid platform that combines the best attributes of a traditional router and a traditional server and offers the same functionality with a smaller infrastructure footprint. Offered with the Cisco Integrated Services Virtual Router (ISRv) and NFV Infrastructure Software (NFVIS) as the hosting layer, the platform offers a complete solution for a simplified deployment.

    NFVIS 4.2.1, Cisco vManage 20.3.1 and later releases on ENCS 5400 devices are supported on Cisco SD-Branch solution.

  - **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.

    NFVIS 4.4.1, Cisco vManage 20.4.1 and later releases on Catalyst 8200-UCPE Edge Series devices are supported on Cisco SD-Branch solution.

  - **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.

Note When you use Cisco Catalyst Edge uCPE 8300 for high throughput requirements, we recommend that you use NVME based storages (M.2 NVME or U.2 NVME) or E1.S based.

- **Cisco Network Function Virtualization Infrastructure Software** - The Cisco Network Function Virtualization Infrastructure Software (NFVIS) software is used as the base virtualization infrastructure software running on the x86 compute platform. The Cisco NFVIS software provides VM lifecycle management, VM service chaining, VM image management, platform management, PNP for bootstrapping a device, AAA features, syslog, and SNMP server. The NFVIS software provides programmable REST and netconf APIs for all the mentioned functionalities.
- **Virtual Network Functions** - The Cisco SD-branch solution supports both Cisco-developed and third-party Virtual Network Functions (VNFs). The following table includes the validated VNFs and their versions:

Cisco Virtual Network Functions (VNFs)	Versions
Cisco ISRv	17.2.1 16.12.1a 16.11.1b
Cisco ASAv	9.13.1
Cisco vWAAS	6.4.3c-b-42
Cisco vEdge	20.1 19.2.1

Third Party Virtual Network Functions (VNFs)	Versions
Fortinet®	v5.4.1,build9317,161003
PaloAlto®	8.1.3
Riverbed®	9
CheckPoint®	77.30
SilverPeak®	7.3.9.0

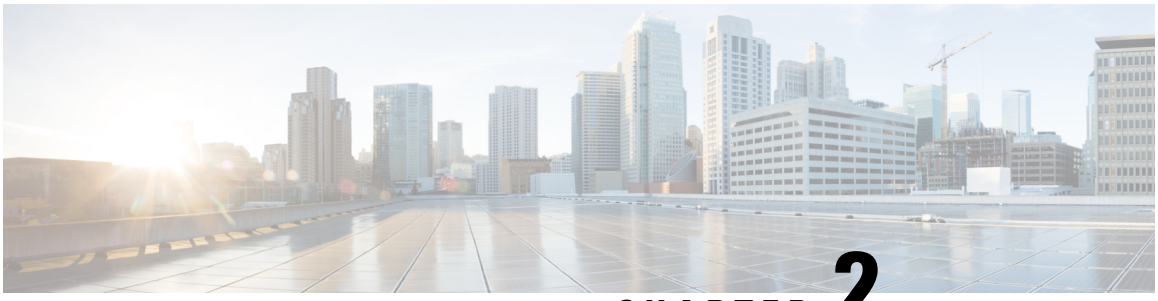
- **Orchestration through Cisco SD-WAN Manager** - The Cisco SD-WAN Manager is used for orchestrating the Cisco SD-branch solution. Cisco SD-WAN Manager and Cisco SD-WAN Validator version 20.1.1 or later are supported on Cisco SD-branch solution. The orchestrator provides the following functionalities:
  - Cisco SD-WAN Validator—The Cisco SD-WAN Validator provides Cisco SD-WAN Manager information to the network elements that may be running behind Network Address Translation (NAT). It performs initial authentication and authorizes the network elements to provide the Session Traversal Utilities for NAT (STUN) server functionality.

- Cisco SD-WAN Manager—Cisco SD-WAN Manager is an SDN controller that provides centralized configuration management, monitoring, and troubleshooting of the SD-branch solution.

Key Tasks Before you Begin

Ensure that the following prerequisites are met before you get started:

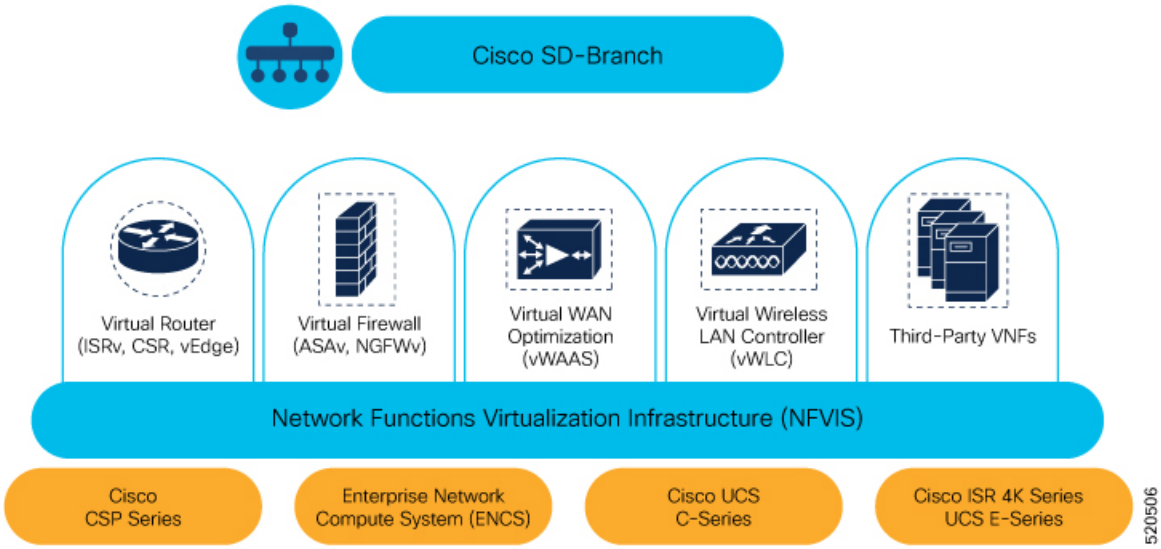
- Cisco SD-WAN Control Components like Cisco SD-WAN Manager, Cisco SD-WAN Validator, and Cisco SD-WAN Controller are already deployed with valid certificates in cloud or on-prem.
- NFVIS WAN Edge device has reachability to the Cisco SD-WAN Validator and other Cisco SD-WAN Control Components which are reachable through public IP addresses across the WAN transports.



CHAPTER 2

Define Cisco NFVIS SD-Branch Solution

Cisco SD-Branch solution is a full stack solution that delivers enterprise grade network and application services. You can choose from a variety of compute platforms that fits your design requirements. All the supported platforms has NFVIS as the host OS, for life cycle management of the SD-Branch device. The architecture allows zero touch provisioning of services in branch network compute devices using Cisco SD-WAN Manager.



Note NFVIS SD-Branch solution currently supports only ENCS 5400 devices.

- Create Authorized Device List, on page 5
- Create VNF Image Packages, on page 7
- Discover and Deploy Devices, on page 12

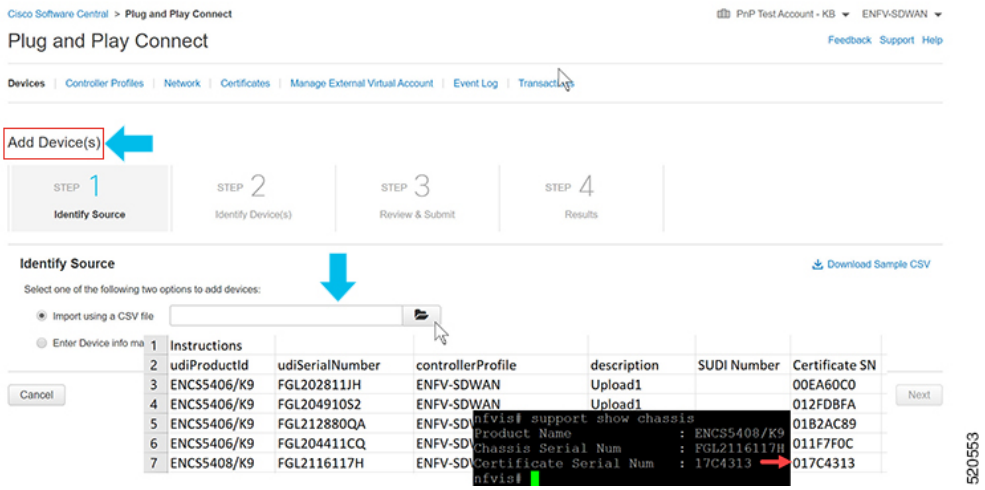
Create Authorized Device List

ENCS device serial numbers are uploaded into the customer specific Cisco Smart Account and virtual account. This is an automated process but, sometimes, you might have to manually create a virtual account and upload

ENCS device serial numbers. The following steps show you how to redirect a device at customer location to customer specific controller.

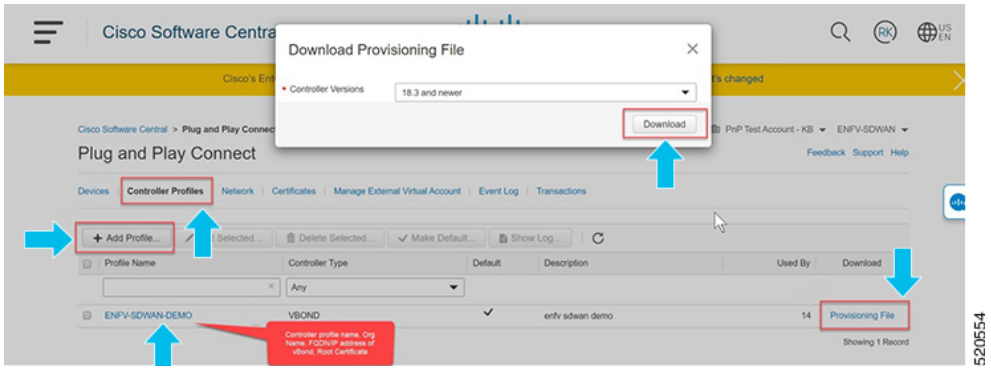
1. Add controller information to virtual account.

   - In PnP Connect server, select **Devices**, click **+ Add Devices** and upload a CSV file with information about PID, serial number and controller. You can upload a certificate issued by Symantec or upload enterprise root cert.



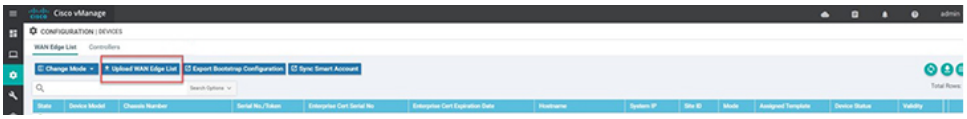
Note Starting from Cisco vManage 20.4, if the ENCS device certificate serial number is not available, the device serial number can be used to authenticate the device by populating the device serial number in the SUDI Number column. Cisco SD-WAN Manager smart sync uses the device serial number to authenticate the device.

   - Select **Controller Profiles** and click **+Add Profiles**. Enter details related to the controller to create a profile. Select **Provisioning File** and download it.



2. Add the device list to Cisco SD-WAN Manager.

   - Upload the authorized device list from virtual account to Cisco SD-WAN Manager.



Identity, Trust and Whitelist

Identity of the NFVIS WAN Edge device is uniquely identified by the chassis ID and certificate serial number. The following certificates are provided depending on the WAN Edge device:

- ENCS hardware device certificate is stored in the on-board SUDI chip installed during manufacturing. ENCS hardware is shipped with Cisco NFVIS software.
- Cisco Catalyst SD-WAN virtual devices do not have root certificates pre-installed on the device. For these devices, a One-Time Password (OTP) is provided by Cisco SD-WAN Manager to authenticate the device with the Cisco SD-WAN Control Components.

Trust of the WAN Edge devices is done using the root chain certificates that are pre-loaded in manufacturing, loaded manually, distributed automatically by Cisco SD-WAN Manager, or installed during Plug and Play (PnP) or Zero-Touch Provisioning (ZTP), the automated deployment provisioning process.

The Cisco SD-Branch solution uses a whitelist model, which means that the NFVIS WAN Edge devices that are allowed to join the SD-Branch overlay network need to be known by all the SD-Branch controllers before hand. This is done by adding the WAN Edge devices in the PnP connect portal. The added WAN Edge devices are attached to the Cisco SD-WAN Validator profile contained in the PnP portal (associated with the SD-Branch overlay organization-name) to create a provisioning file. This file is imported into the SD-Branch Cisco SD-WAN Control Components, which then automatically shares the device whitelist with the rest of SD-Branch controllers (Cisco SD-WAN Validator). The provisioning file containing the device whitelist can also be synced directly from the PnP connect portal to Cisco SD-WAN Manager through a secure SSL connection using REST APIs.

Note The Cisco SD-WAN Control Components such as Cisco SD-WAN Manager, Cisco SD-WAN Validator and Cisco SD-WAN Controller and WAN Edge devices, should all be configured with the same organization-name to join the same SD-Branch overlay network.

Create VNF Image Packages

Table 1: Feature History Table

Feature Name	Release Information	Description
Support for Uploading Different VNF Image Packages	NFVIS 4.6.1 Cisco vManage Release 20.6.1	This feature allows you to register a VNF image by uploading seperate VNF packages for image package, scaffold, and disk image.

Uploading a prepackaged Cisco VM image, tar.gz is supported on Cisco SD-WAN Manager. You can also package the VM image by providing a root disk image in any of the supported formats (qcow2). Use the linux

command-line NFVIS VM packaging tool, nfvpt.py to package the qcow2 or create a customized VM image for Cisco SD-WAN Manager.

Note

- Download the prepackaged Cisco VM image from the ISRv Software Download Page and the scaffold files for third party VMs from the Scaffold Files for Third Party VMs Software Download Page.
- Each VM type such as a firewall can have multiple VM images that are uploaded to Cisco SD-WAN Manager from same or different vendors being added to the catalog. Also, different versions that are based on the release of the same VM can be added to the catalog. However, ensure that the VM name is unique.
- When you upload a Cisco Catalyst 8000V Edge Software image to Cisco SD-WAN Manager, you might see a failure message that says **Image type missing in image properties file**. To add the missing image properties, extract the compressed tar.gz file, open the **image_properties.xml** file, add **`<imageType>virtualmachines</imageType>`** to the code and save the file.

The Cisco VM image format can be bundled as *.tar.gz and can include:

- Root disk images to boot the VM.
- Package manifest for checksum validation of the file listing in the package.
- Image properties file in XML format that lists the VM meta data.
- (Optional) Day-0 configuration, other files that are required to bootstrap the VM.
- System generated properties file in XML format that lists the VM system properties

The VM images can be hosted on both HTTP server local repository that Cisco SD-WAN Manager hosts or the remote server.

If the VM is in NFVIS supported VM package format such as, tar.gz, Cisco SD-WAN Manager performs all the processing and you can provide variable key and values during VNF provisioning.

Upload Different Image Types

Starting from NFVIS release 4.6.1, the process of image registration is decoupled from the process of uploading image properties. You can register the VNF image by uploading it in any supported image format. The following image formats are supported:

- Image package: .tar.gz file for the complete image package.
- Scaffold: .tar.gz file comprising of only the metadata (image properties and day 0 configuration files).
- Disk image: .qcow2 disk image.

To upload the image types:

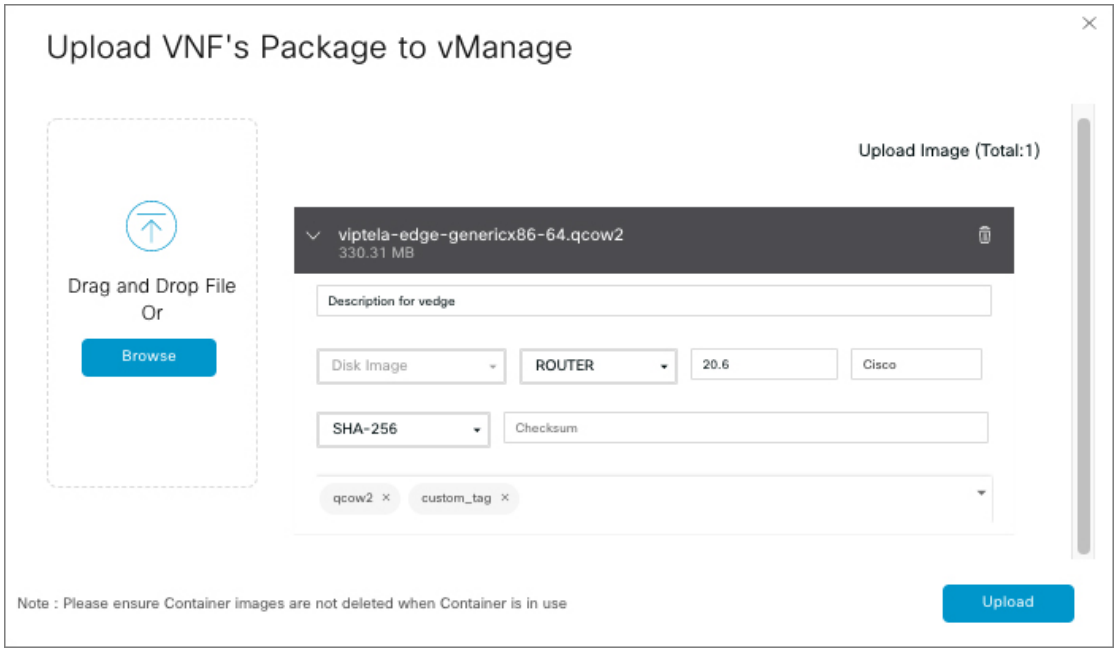
1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. From the **Upload Virtual Image** drop-down list, choose **vManage**.
4. In the **Upload VNF's Package to SD-WAN Manager** window upload your tar.gz or qcow2 file.

Note

- While uploading a Cisco Catalyst 8000V Edge Software image to Cisco SD-WAN Manager, you may encounter a failure message that says **Image type missing in image properties file**. To add the missing image properties, extract the compressed tar.gz file, open the **image_properties.xml** file, add **`<imageType>virtualmachines</imagetype>`** to the code and save the file.
- While uploading multiple VNF package files to Cisco SD-WAN Manager, you may encounter an error that states **failed to upload**. Uploading multiple VNF package files to Cisco SD-WAN Manager fails when the disk space allocated for the upload is less than 20% of the total partition size of the disk. Ensure to free up some disk space to upload multiple images.

5. From the **File Type** drop-down list, choose the image type (Image Package, Scaffold or Disk Image).
6. (Optional) Add descriptions and tags to help identify your image. You can either use the default tags available or create your own custom tags.
7. If you are uploading a disk image, choose values for **VNF Type**, **Version** and **Vendor**

   .

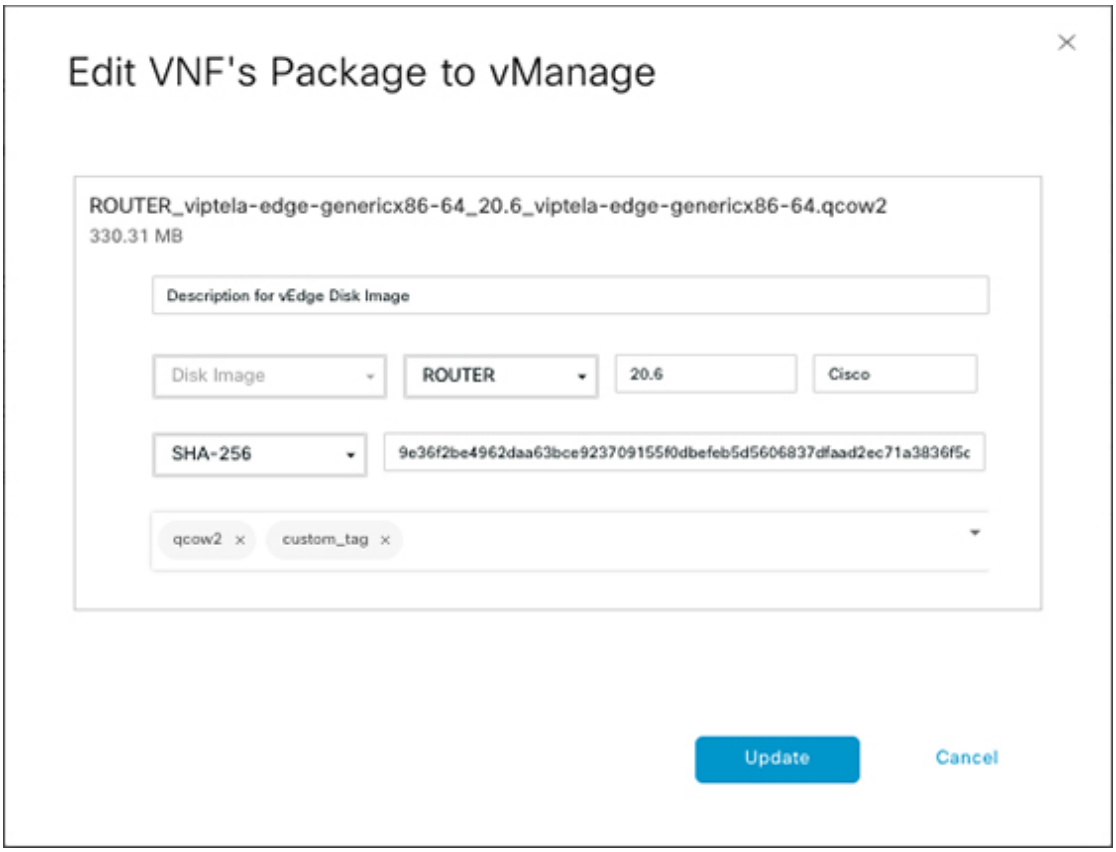


8. Click **Upload**

   .

To edit the VNF package:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. For the desired image, click **…** and choose **Edit**.



4. After making the desired changes, click **Update**.

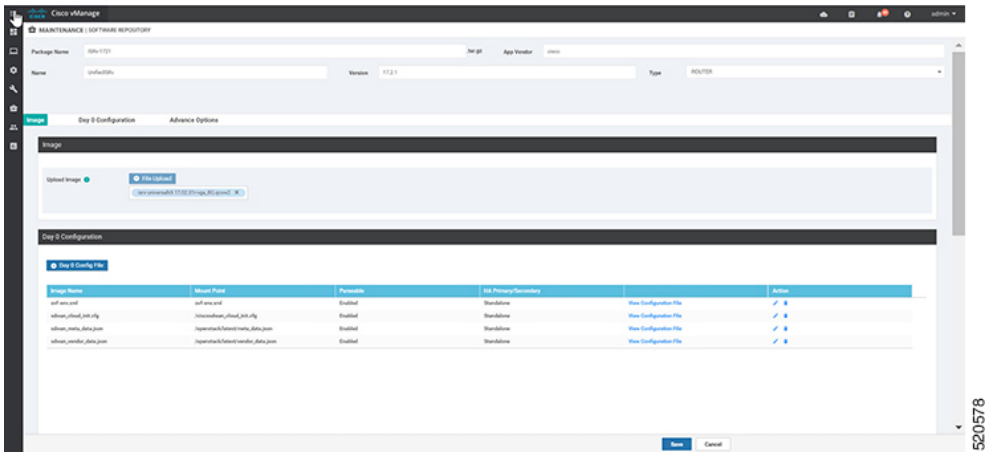
Note Cisco SD-WAN Manager only manages the Cisco VNFs, whereas Day-1 and Day-N configurations within VNF are not supported for other VNFs. See the NFVIS Configuration Guide, VM Image Packaging for more information about VM package format and content, and samples on image_properties.xml and manifest (package.mf).

To upload multiple packages for the same VM, same version, Communication Manager (CM) type, ensure that one of the three values (name, version, VNF type) are different. Then, you can repackage the VM *.tar.gz to be uploaded.

The following is an example of how to build an ISRv package:

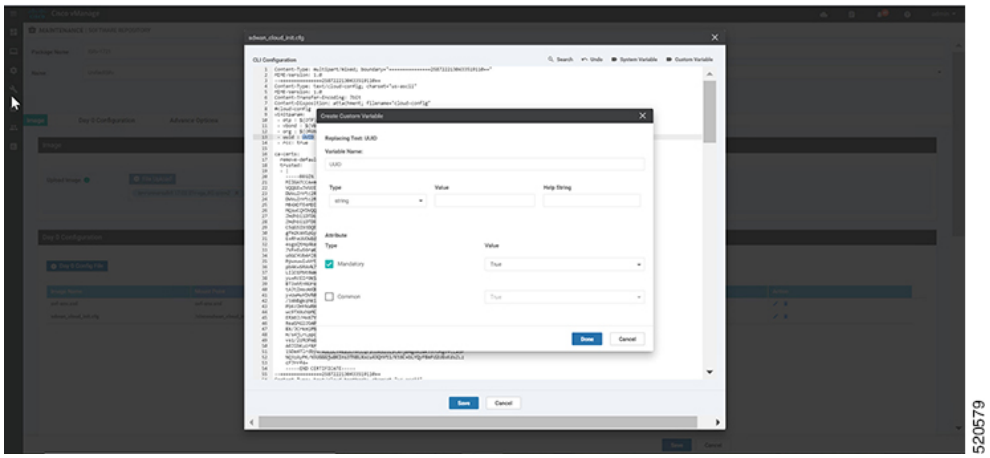
1. Upload the root disk image for bootstrap configurations.

   Click on **View Configuration File** next to the image.



2. Select a variable and click on **Custom Variable**. In the pop-up window, select the variable type from the drop down menu.

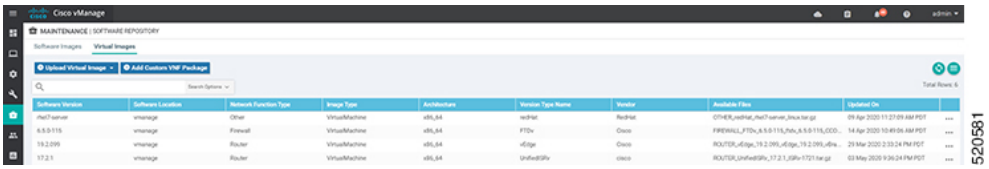
   Click **Done** and then click **Save**.



3. You can select the image properties as per your requirements.



4. You can see the image package is created and added in the list of virtual images.



Discover and Deploy Devices

The WAN Edge device contacts the Cisco SD-WAN Validator on bootup, to establish a secure transient DTLS control connection. The Cisco SD-WAN Validator information can be configured manually through CLI on the WAN Edge device, using an IP address or resolvable domain-name FQDN, or it can be obtained automatically through the PnP or ZTP process.

The SD-Branch controllers (Cisco SD-WAN Validator, Cisco SD-WAN Manager and Cisco SD-WAN Controller) and WAN Edge devices need to mutually authenticate and trust each other before establishing the secure control connections. When the SD-Branch controllers authenticate each other and WAN Edge devices, they:

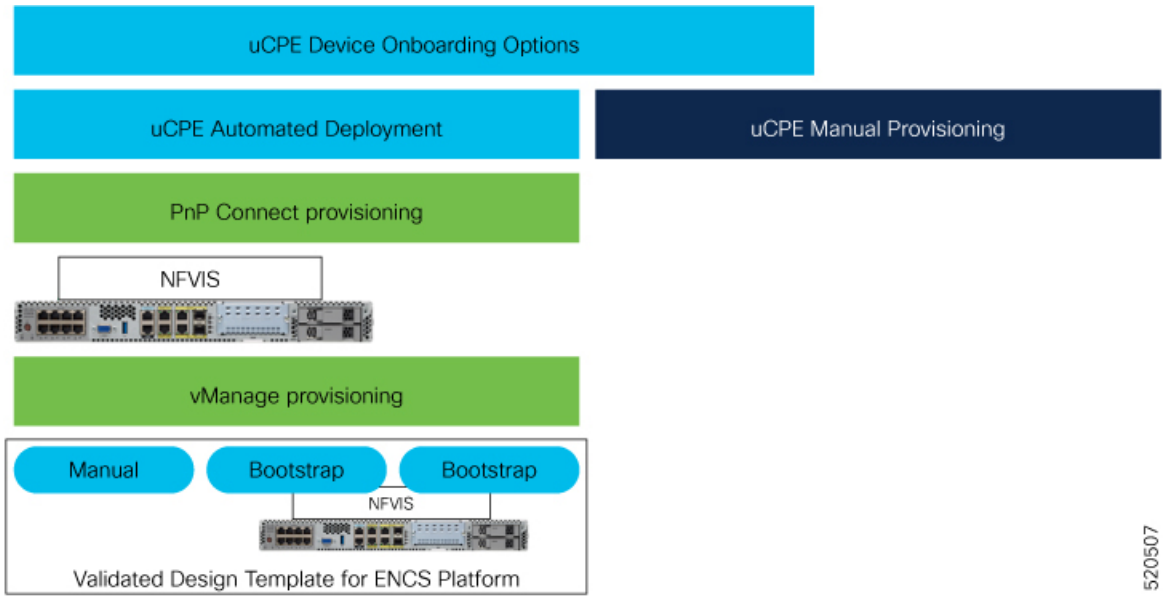
- Validate the root of trust for the certificate root CA
- Compare the organization-name of the received certificate Organization Unit (OU) against the locally configured
- Compare the certificate serial number against the authorized whitelist

When the WAN Edge devices authenticate the controllers, they:

- Validate the root of trust for the certificate root CA
- Compare the organization-name of the received certificate OU against the locally configured.

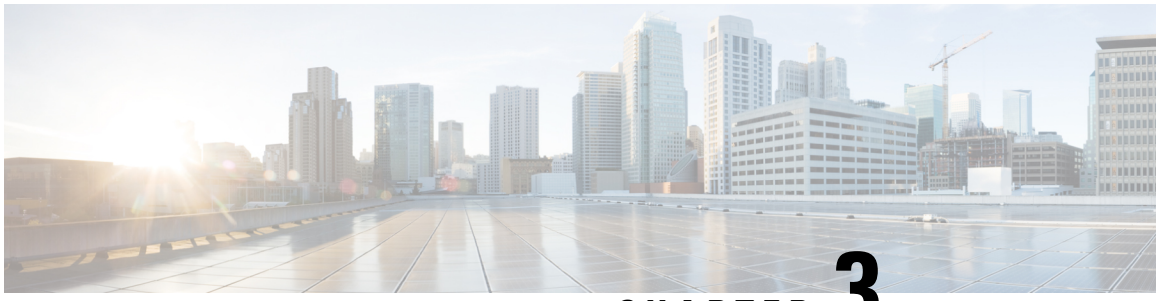
After successful authentication, the Cisco SD-WAN Validator establishes a secure transient DTLS control connection and then shares the Cisco SD-WAN Manager IP addresses. At this time, the Cisco SD-WAN Validator informs the other SD-branch controllers (Cisco SD-WAN Manager and Cisco SD-WAN Controller) to expect a control connection request from the WAN Edge device. ENCS device, unlike Cisco Catalyst SD-WAN devices does not maintain a control connection with Cisco SD-WAN Controller.

NFVIS WAN Edge device, upon learning the Cisco SD-WAN Manager information, initiates a control connection to the Cisco SD-WAN Manager server. After a successful authentication, a separate secure persistent DTLS/TLS connection is established. Cisco SD-WAN Manager provisions the configuration using the NETCONF protocol based on the device template attached to the WAN Edge device.



Default behavior of the NFVIS WAN Edge device is to establish:

- Secure transient DTLS control connection to Cisco SD-WAN Validator across one WAN transport, only during the onboarding process.
- Secure permanent DTLS/TLS control connection to Cisco SD-WAN Manager across a single WAN transport.



CHAPTER 3

Design Cisco NFVIS SD-Branch Solution

The NFVIS SD-Branch solution provides Zero Touch Provisioning (ZTP) of branch devices with a full service capability. Configuring WAN circuit type, network IP addresses and topology create unique consideration in provisioning ENCS network compute WAN-Edge platforms.

- Wan Edge Onboarding Methods, on page 15
- Network Design, on page 19

Wan Edge Onboarding Methods

Automated Deployment

Automated deployment automates the day-zero experience of securely onboarding and deploying the NFVIS WAN Edge device, with default factory shipped settings, into the Cisco Catalyst SD-WAN network.

Automated deployment discovers the Cisco SD-WAN Validator IP address dynamically using the PnP process for the ENCS physical platform.

The following are the primary requirements to use this onboarding option:

- The NFVIS WAN Edge device must be connected to a WAN transport that can provide a dynamic IP address, default-gateway and DNS information.

  If you have a static IP address, you must configure the IP address using the following configuration example:

```
configure terminal
bridges bridge wan-br
no dhcp
bridges bridge wan-br
no dhcp
system settings wan ip address 10.1.1.1 255.255.255.0
system settings default-gw 10.1.1.2
system settings dns-server 172.16.10.10
pnp automatic dhcp disable
pnp automatic dns disable
pnp automatic cco enable
commit
```

- The NFVIS WAN Edge device can DNS resolve devicehelper.cisco.com for the Plug-and-Play Connect server.

- In Cisco SD-WAN Manager, a device configuration must be built and attached to the WAN Edge device to successfully onboard the device.

Use the **show pnp status** command to view the progress of PnP redirection to Cisco SD-WAN Validator.

```
Device# show pnp status

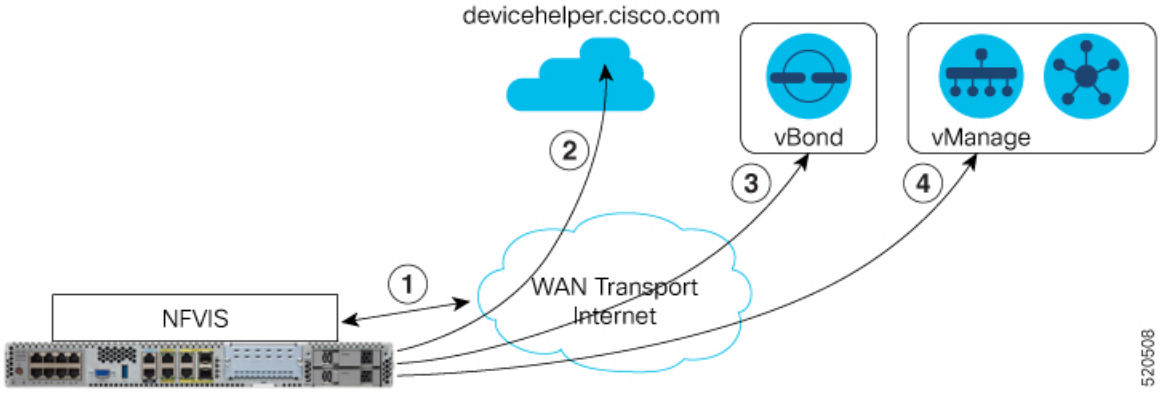
pnp status response PnP Agent is not running
server-connection
status: Success
time: 22:22:20 Dec 09
device-info
status: Success
time: 22:09:19 Dec 09
capability
status: Success
time: 22:06:17 Dec 09
redirection
status: Success
time: 22:25:46 Dec 09
certificate-install
status: Success
time: 22:51:26 Dec 09
device-auth
status: Success
time: 22:01:29 Dec 09

pnp status ip-address ""
pnp status ipv6-address ""
pnp status port ""
pnp status transport ""
pnp status cafile ""
pnp status created_by user
pnp status dhcp_opt43 0
pnp status dns_discovery 0
pnp status cco_discovery 0
pnp status dhcp-ipv6 0
pnp status dns-ipv6 0
pnp status cco-ipv6 0
pnp status timeout 0
```

In case of any failure, you can use the **pnp action command stop**, **pnp action command start** or **pnp action command restart** command to start, stop or restart the process.

Plug-and-Play Process

The day-zero automated Plug-and-Play (PnP) process provides a simple, secure procedure to discover, install and provision the NFVIS WAN Edge device to join the Cisco Catalyst SD-WAN overlay network.



The steps involved during the PnP onboarding process is as follows:

1. The NFVIS WAN Edge device on boot up, obtains IP address, default gateway and DNS information through DHCP on the supported device's PnP interface that is connected to the WAN transport (typically Internet).
2. The NFVIS WAN Edge device attempts to reach the Cisco-hosted PnP connect server. The router attempts to resolve the name of the PnP server at devicehelper.cisco.com and uses an HTTPS connection to gather information about the Cisco SD-WAN Validator, including the organization-name.

Note

- For an ENCS deployment using enterprise root-ca certificates, the WAN Edge device receives the root certificates, along with the Cisco SD-WAN Validator and organization-name information from the PnP Connect portal.
- If an enterprise root-ca certificate is expected as a result of devicehelper.cisco.com, use the **show certificate root-ca-cert** command to verify that the certificate is received.
- Starting from Cisco NFVIS Release 4.9.1, establishing a control connection to the management plane via the management port is supported. The management port needs to be connected with Cisco Catalyst SD-WAN for a successful connection to the control plane.

3. The WAN Edge device authenticates with the Cisco SD-WAN Validator using its chassis or serial number and root certificate. After a successful authentication, the Cisco SD-WAN Validator provides the device with the Cisco SD-WAN Manager.
4. The WAN Edge device initiates and establishes secure connections with the Cisco SD-WAN Manager and downloads the configuration using NETCONF from Cisco SD-WAN Manager and joins the Cisco Catalyst SD-WAN overlay network.

Note When the vDaemon service is started within the Cisco NFVIS environment for SD-Branch deployments, the **hostAction** operations for backup and restore, as well as **vmExportAction** and **vmImportAction**, are disabled.

Staging

NFVIS WAN Edge devices can be staged through the certificate status, controlled from Cisco SD-WAN Manager. Certificates for devices can be placed in staging state before deployment. During staging state, the WAN Edge devices can only establish secure control connections with the Cisco SD-WAN Control Components. The data plane connections are not created.

You can use the WAN Edge devices in the staged state to prepare the device, which may involve upgrading the software and configuring the device, before fully integrating it into the Cisco Catalyst SD-WAN overlay network by changing the certificate status from **Staging** to **Valid** from the Cisco SD-WAN Manager GUI.

NFVIS WAN Edge Certificate Status

The NFVIS WAN Edge device certificate in Cisco SD-WAN Manager, can be configured to be in one of the below states:

- **Invalid** – In this state, the WAN Edge device is not authorized to join the Cisco SD-WAN Control Components and the overlay network. The device does not form control plane or data plane connections to any of the Cisco Catalyst SD-WAN components.
- **Staging** – In this state, the WAN Edge device establishes secure control plane connections to the Cisco SD-WAN Control Components (Cisco SD-WAN Validator, Cisco SD-WAN Manager) only. It is important to note that no data plane connections are established with other WAN Edge devices in the overlay network.
- **Valid** – In this state, the WAN Edge device is fully onboarded onto the Cisco Catalyst SD-WAN network. The device establishes secure control plane connections with the controllers and secure data plane connections with all the other WAN Edge routers in the Cisco Catalyst SD-WAN overlay network.

Zero-Trust Model

The NFVIS SD-Branch solution is a Zero-Trust model. Trusting a WAN Edge device includes WAN device whitelist and the root certificate. The device certificate must also be in a **Valid** state to be authorized on the network.

WAN Edge devices have to be known and authorized by all the Cisco SD-WAN Control Components before allowing the device onto the network. Authorizing the device can be done by:

- Adding the device in Plug-and-Play connect portal and associating it with the Cisco SD-WAN Validator profile.
- Synchronizing the device list to Cisco SD-WAN Manager or manually downloading and importing the provisioning file to Cisco SD-WAN Manager.



Note WAN Edge network devices can be added automatically and associated with the Cisco SD-WAN Validator profile in the Plug-and-Play connect portal by assigning the smart account and virtual account details.

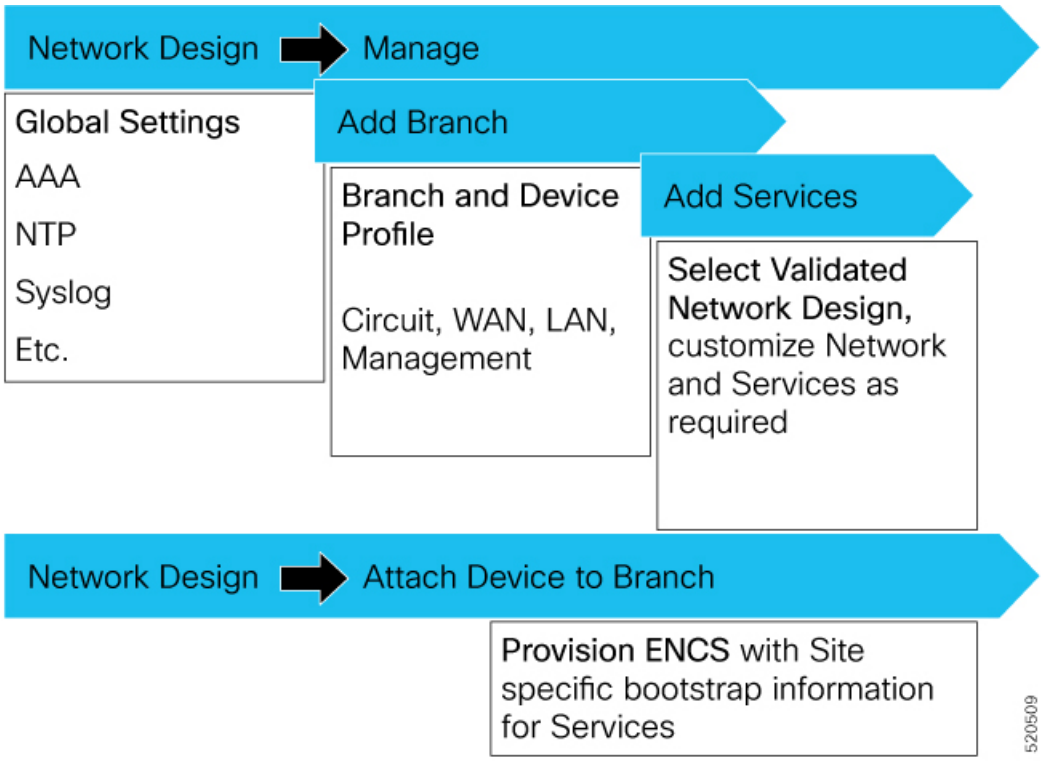
Network Firewall Requirements

To deploy WAN Edge devices behind a firewall, ensure that the appropriate ports are opened for the Cisco SD-WAN Control Components to securely establish connections.

- By default, all the Cisco SD-WAN Control Components attempt to use DTLS, UDP base port 12346 to establish connections.
- If the WAN Edge device is unable to establish control connections with the Cisco SD-WAN Control Components using the default base port or if multiple WAN Edge devices are placed behind a NAT device, the WAN Edge device can port hop through 5 base ports. Port hopping is done sequentially on ports 12346, 12366, 12386, 12406, and 12426 before returning to port 12346. Port hopping is enabled by default on the WAN Edge device.
- A port-offset can be configured to uniquely identify each WAN Edge device placed behind a NAT device and to prevent attempts from using the same base ports. A port offset is a number from 0 to 19, 0 being the default. If a port-offset is configured, the default base port is incremented with the port-offset value and the subsequent ports are incremented by 20. For example, in a deployment with a port-offset value set to 1, then the WAN Edge initiates the connection with port 12347 (12346+1) and then subsequently port hopping is done sequentially on ports 12347, 12367, 12387, 12407, 12427 before returning to port 12347.
- The WAN Edge device uses the same base ports to establish data plane connections, such as IPsec connections and BFD sessions, with other WAN Edge devices in the overlay network.
- The Cisco SD-WAN Validator always uses DTLS, UDP source port 12346, to establish control connections with the Cisco SD-WAN Control Components. The default port can be changed with a configuration change.

Network Design

Use the Network Design feature on Cisco SD-WAN Manager to create and manage an overlay network topology. You can add circuits, data centers, and branch sites to a network topology, configure LAN, WAN, and management interfaces for elements in the topology, review the topology, and perform related tasks. The network design operations are particularly useful for small-scale deployments that include data centers and branch sites.



Network design consists of these major workflows:

- Create network topology—Create circuits, data centers, and branch sites, in this order. A network topology must include at least one circuit and one data center.
- Configure device profiles—Configure global parameters and options for LAN, WAN, and management settings.
- Attach devices profiles—Attach device profiles to devices.
- Ongoing management—Add elements to the network topology and modify the configuration settings for elements as needed.

Configure Network Design Elements

With the network design feature, you can create a new overlay network topology and modify existing elements in a topology. You can perform these activities from the **Network Design** page on Cisco SD-WAN Manager.

Creating a new network topology involves performing the following procedures in the order shown:

Table 2:

Procedure	Description	Reference
1	Add circuits.	See Configure Circuits .
3	Add branch sites.	See Configure Branch Sites.

Procedure	Description	Reference
4	Configure global parameters.	See Configure Global Parameters.
5	Configure device profiles.	See Configure Device Profiles.

A network topology must include at least one circuit. After a network topology is created, you can modify its elements directly.

Configure Circuits

Each network topology must have at least 1 circuit and can have up to 18 circuits. NFVIS can use only one circuit for establishing control connection. In case of failure of the configured circuit, alternate circuits cannot be used.

To configure circuits for a network topology, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Choose **Create Network Design** (which is displayed if you have not yet created a network topology) or **Manage Network Design** (which is displayed if you have created a network topology).
3. Choose **Circuits**.

   A screen for configuring circuits is displayed. If any circuits have been created, this screen lists them. You can remove a circuit by clicking its corresponding delete icon.
4. Click **Add New**.
5. Choose the **Private** or the **Public** radio button to indicate whether the circuit is private or public.
6. From the **Circuit Color** drop-down list, choose a predefined color to uniquely identify the transport location (TLOC) in a circuit.

   The color you choose cannot be used for a TLOC in any other circuit in the topology.
7. To add more circuits, repeat steps 2 through 5.
8. To remove a circuit that you added, click its corresponding **Delete** icon.
9. Click **Finish**.
10. Click **Save** on the Network Design screen.

    Or, if you do not want to save the updates that you made, click **Cancel**.

Configure Branch Sites

Configuring a branch site involves assigning a name and adding device profiles and segments to the branch site. Each network topology must have at least one branch site.

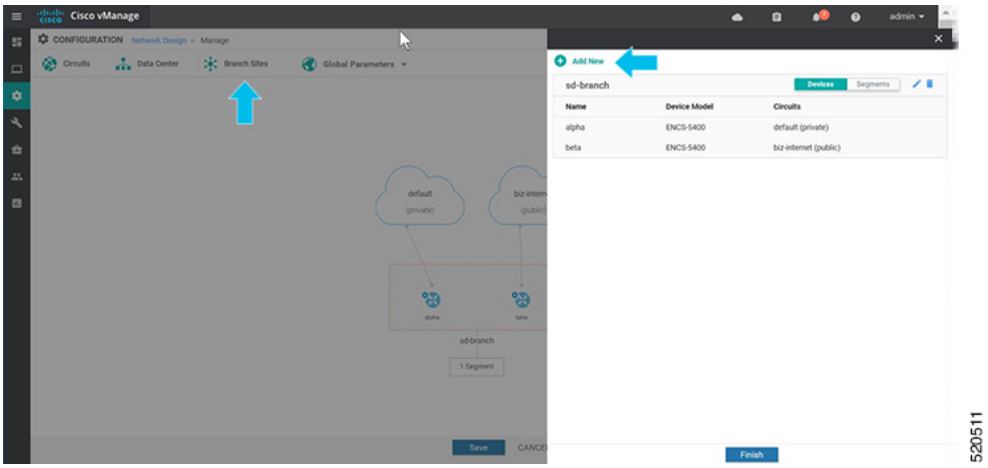
To configure branch sites for a network topology:

1. Frome the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Choose **Create Network Design** (which is displayed if you have not yet created a network topology) or **Manage Network Design** (which is displayed if you have created a network topology).

Click **Branch Sites**. This option is dimmed out if you have not added at least one circuit.

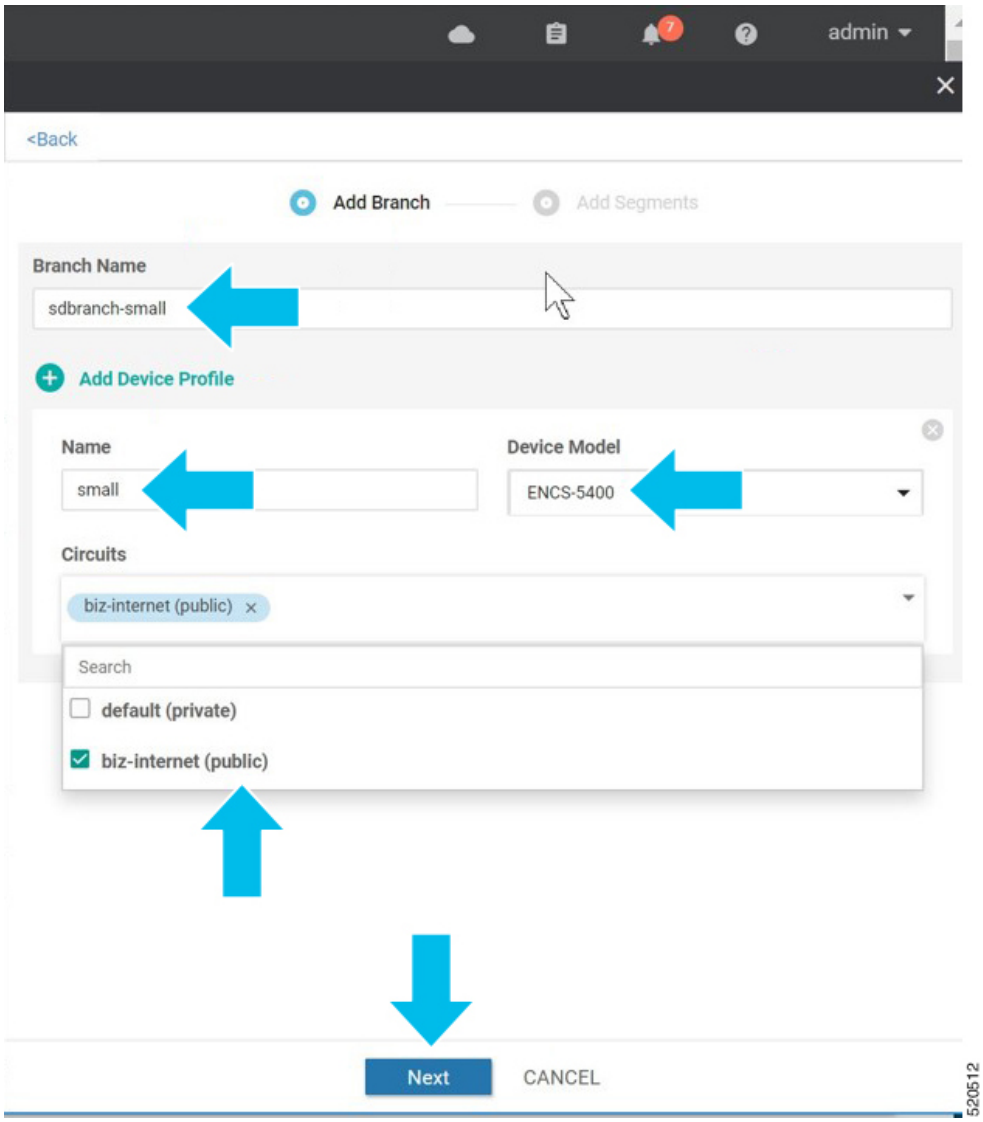
Configuring branch sites page appears. If any branch sites have already been created, this page lists them.

To add a branch site, click **Add new**.



3. To add a branch:
   a. Enter a unique name for the branch site in **Branch Name**. This name cannot be used for any other data center, branch site, or device profile in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.
   b. To add a new device profile, click **Add Device Profile**.

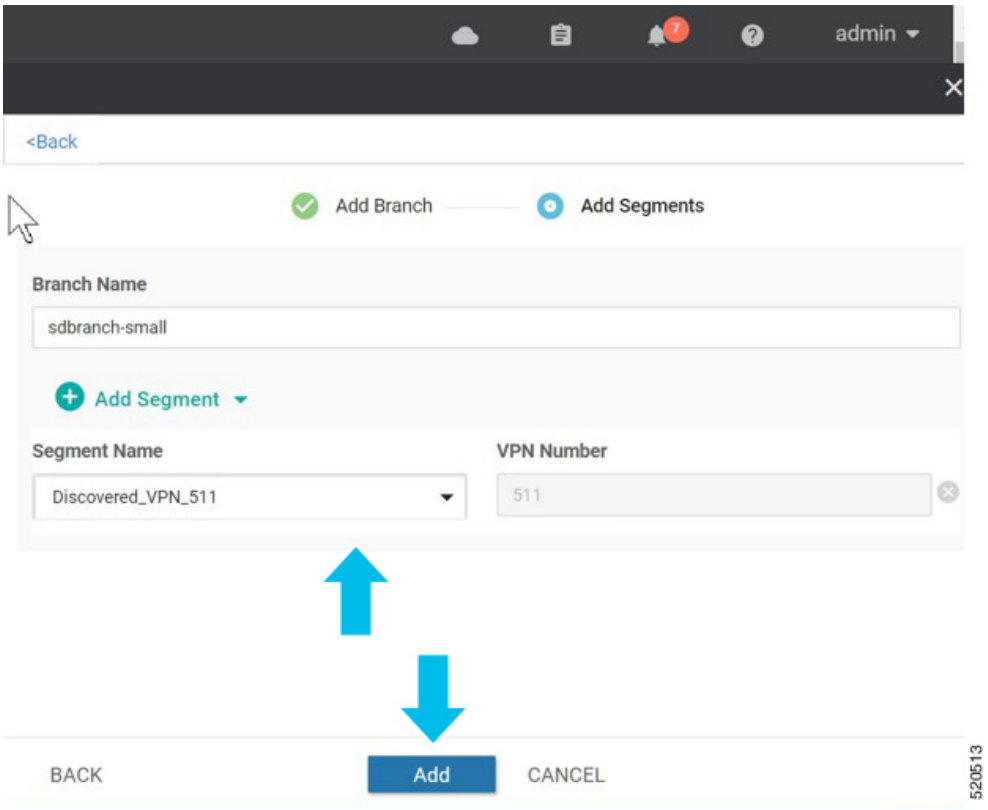
      Each branch site must have at least one device profile. A device profile is associated with a specific device type in the branch site and provides configuration settings that are pushed to those device types.
   c. Enter **Name** to enter a name for the device profile
   d. From the **Device Model** drop-down list, choose the device type to associate with the device profile.
   e. Choose **Circuits** to display a list of circuits that you have created and then check the box next to each circuit that the device profile should be associated with.
   f. Click **Next**.



4. A segment is a service side VPN that is associated with all device profiles in the branch site. Each branch site must have at least one segment. You can use the same segment in multiple branch sites.To add one or more segments:

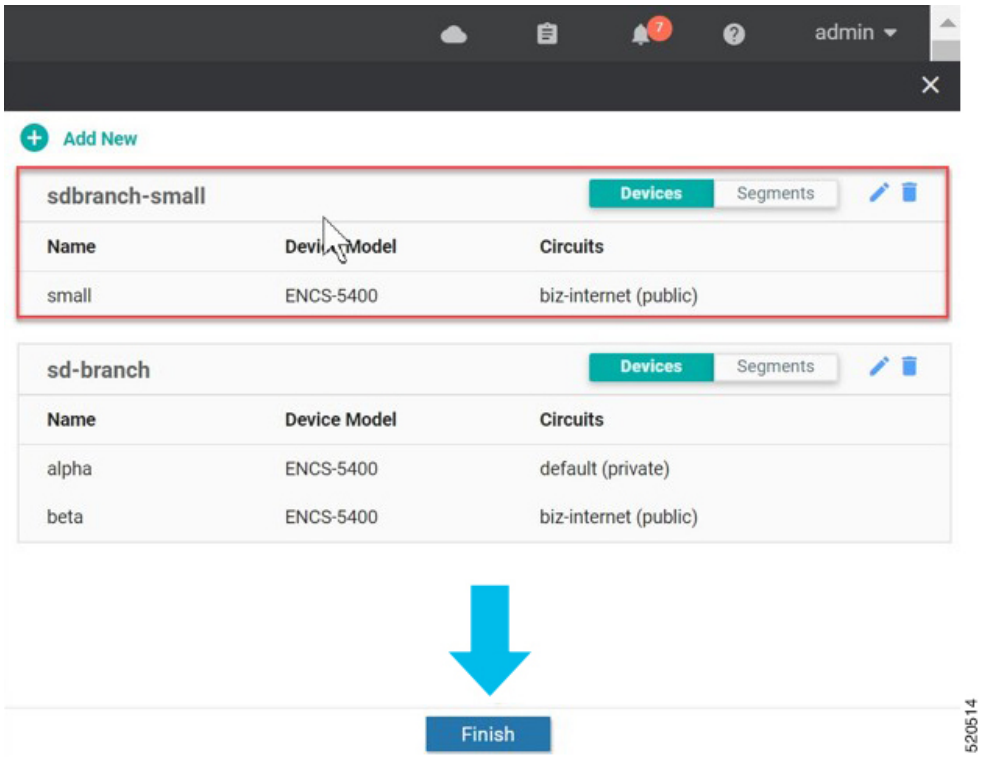
   a. Click **Add Segment**. Choose a segment from the drop-down list. The VPN Number populates automatically with the VPN ID that was configured for the segment.

   b. Click **Add**.

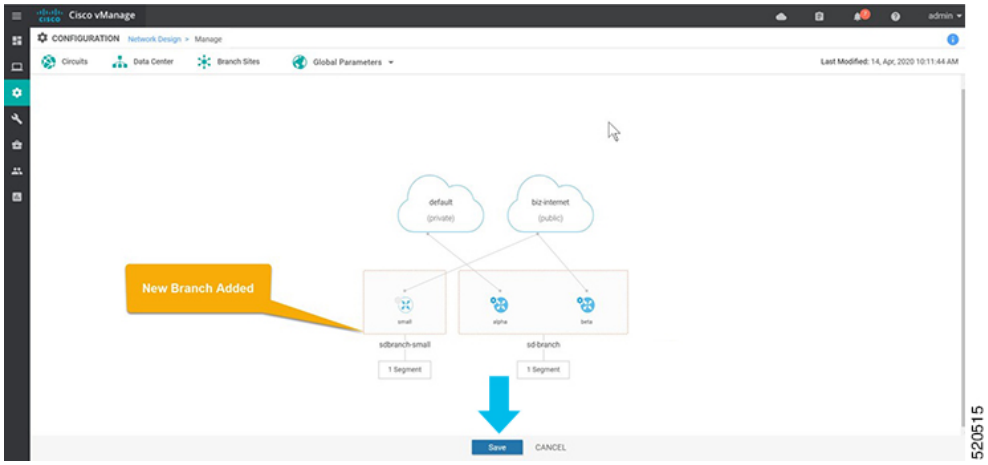


The system displays a list of branch sites.

5. Click **Finish**.



6. Click **Save** on the **Network Design** page.



Configure Global Parameters

Global parameters are configuration settings that are used in all device profiles in a network topology. If you do not configure global parameters, factory default configuration settings are used for device profiles.

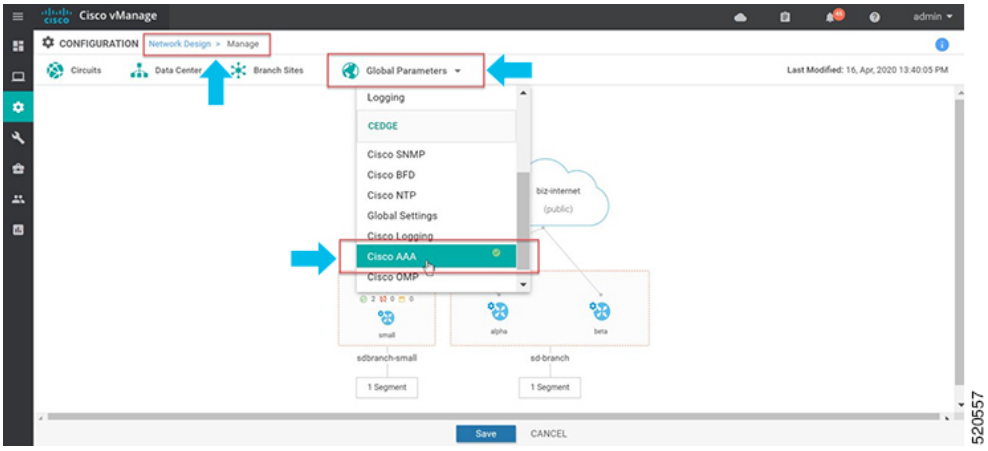
SD-Branch currently supports NTP, AAA and logging parameters only.

To configure global parameters:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.

2. Choose **Create Network Design** (which is displayed if you have not yet created a network topology) or **Manage Network Design** (which is displayed if you have created a network topology).

   Choose **Global Parameters** and choose the desired template from the drop-down list.

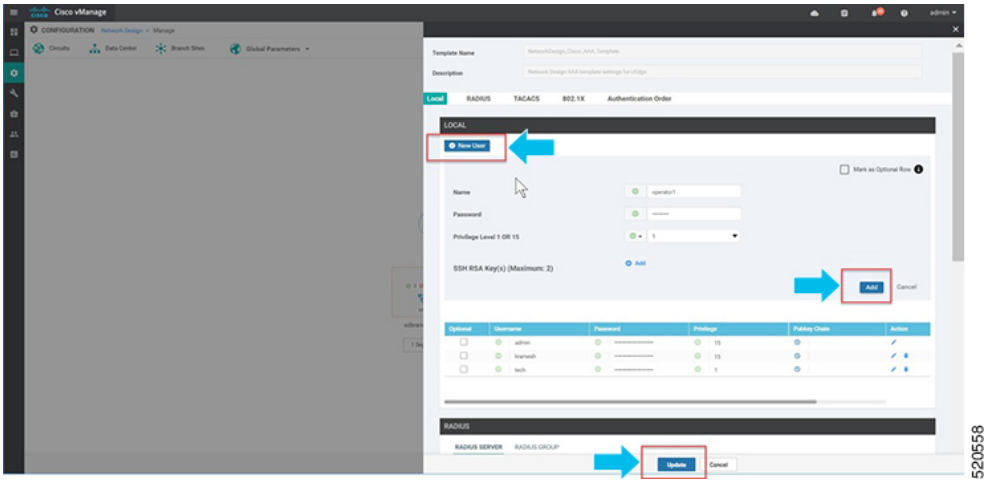


3. Configure the template.

   The template name and description is automatically populated and cannot be changed. You cannot select a device type as the template is used for all devices throughout your network.

   To add a new user, select **+ New User**, and enter the details. Click **Add**.

   Click **Update** to complete the configuration.



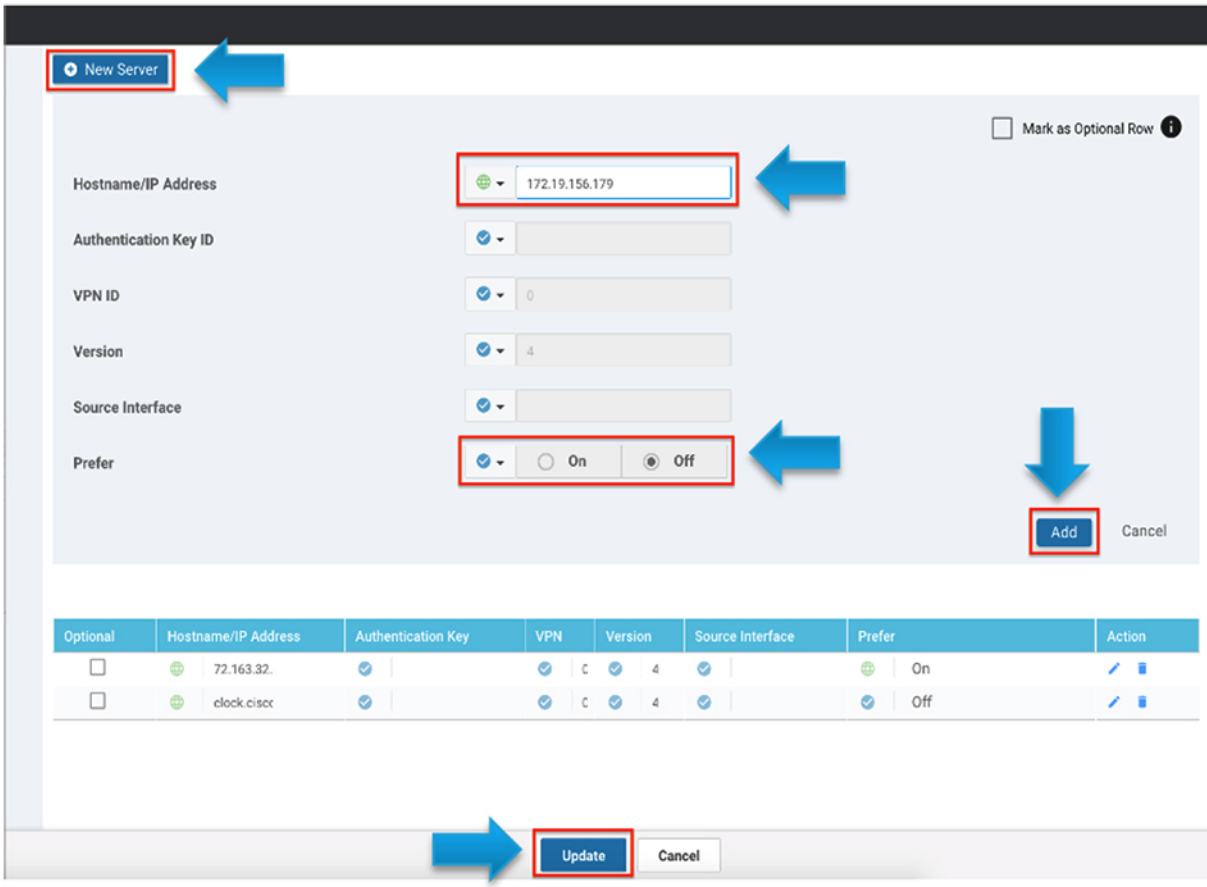
   Cisco vManage 20.1 and 20.3 releases support only AAA global parameters on local users. You can update TACACS and RADIUS settings through the Add-on CLI feature configuration on the device.

4. Add NTP server.

   To add a new server, choose **+ New Server** and enter **Hostname/IP Address**.

5. Choose **Prefer** options and click **Add**.

   Click **Update** to complete the configuration.

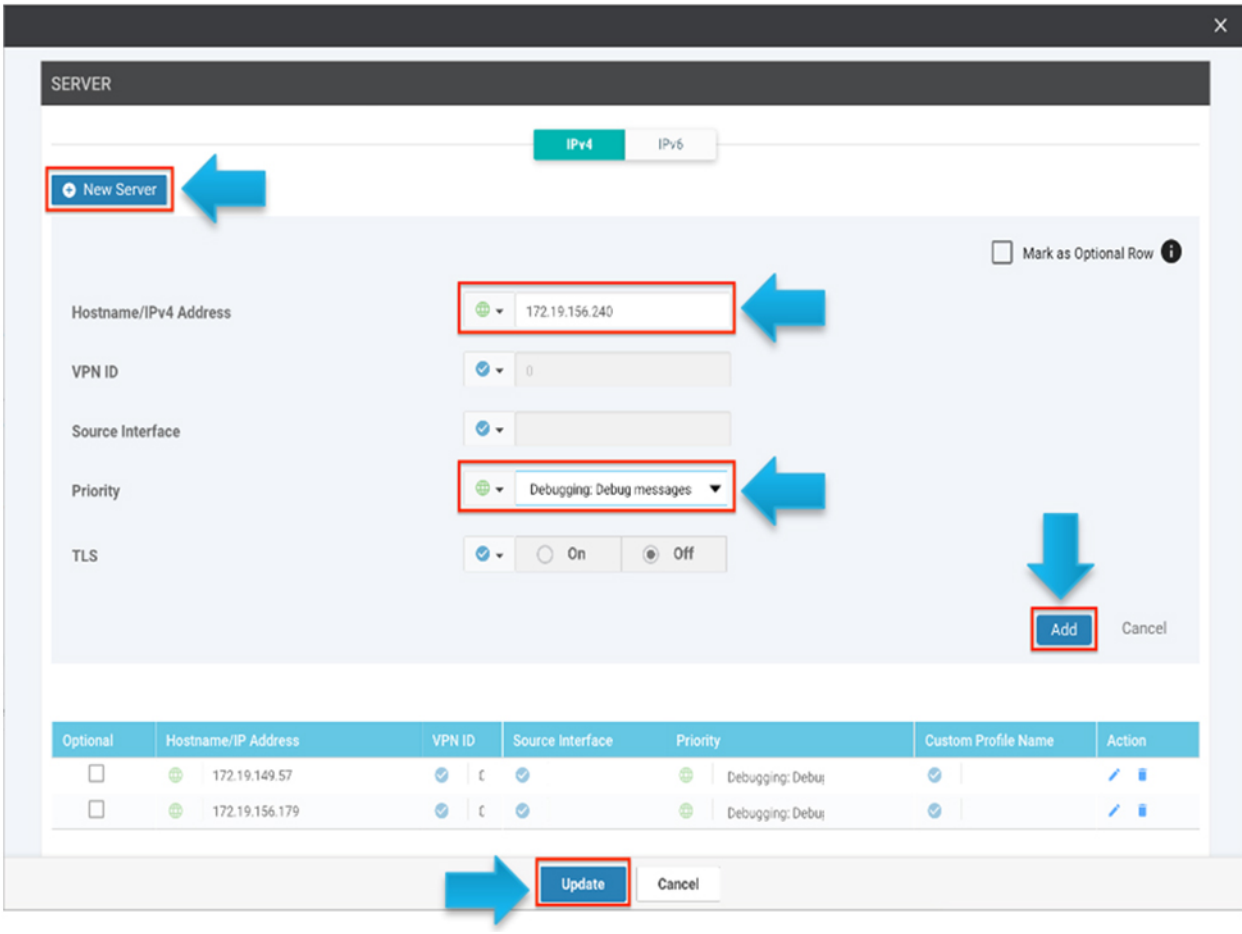


Authentication Key ID, **VLAN ID**, **Version** and **Source Interface** is not applied to NFVIS platforms. NFVIS platforms supports only one preferred and one backup NTP servers.

6. Add logging server.

   To add a new server, select **+ New Server** and enter **Hostname/IP Address**. Choose **Priority** options and click **Add**.

   Click **Update** to complete the configuration.



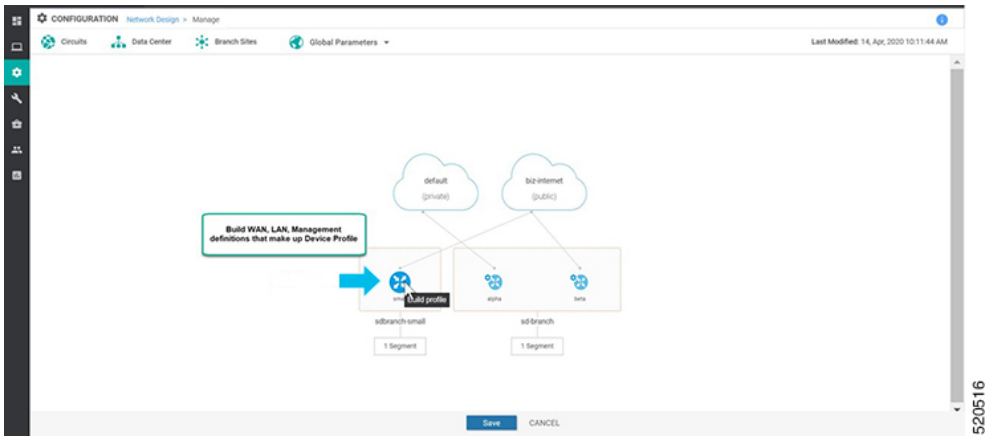
VPN ID and **Source Interface** is not applied to NFVIS platforms. The maximum number of logging servers supported is four. Ensure that **Priority** is using the same setting. NFVIS platforms support only one priority or logging severity as a globlal configuration.

Configure Device Profiles

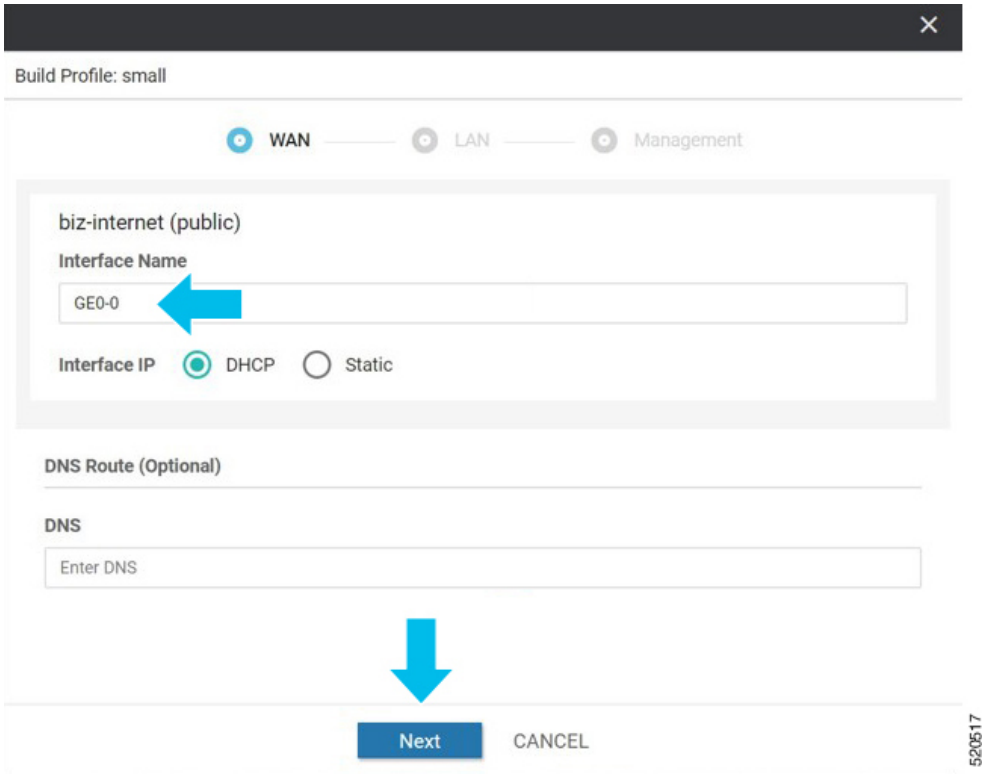
You must configure a device profile for each router in a data center or a branch site before the device profile can be attached to the router.

To configure a device profile for a router in a network topology:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. A network diagram is displayed on the **Network Design** page. When you hover your mouse over the image representation of the device, choose **Build profile**.



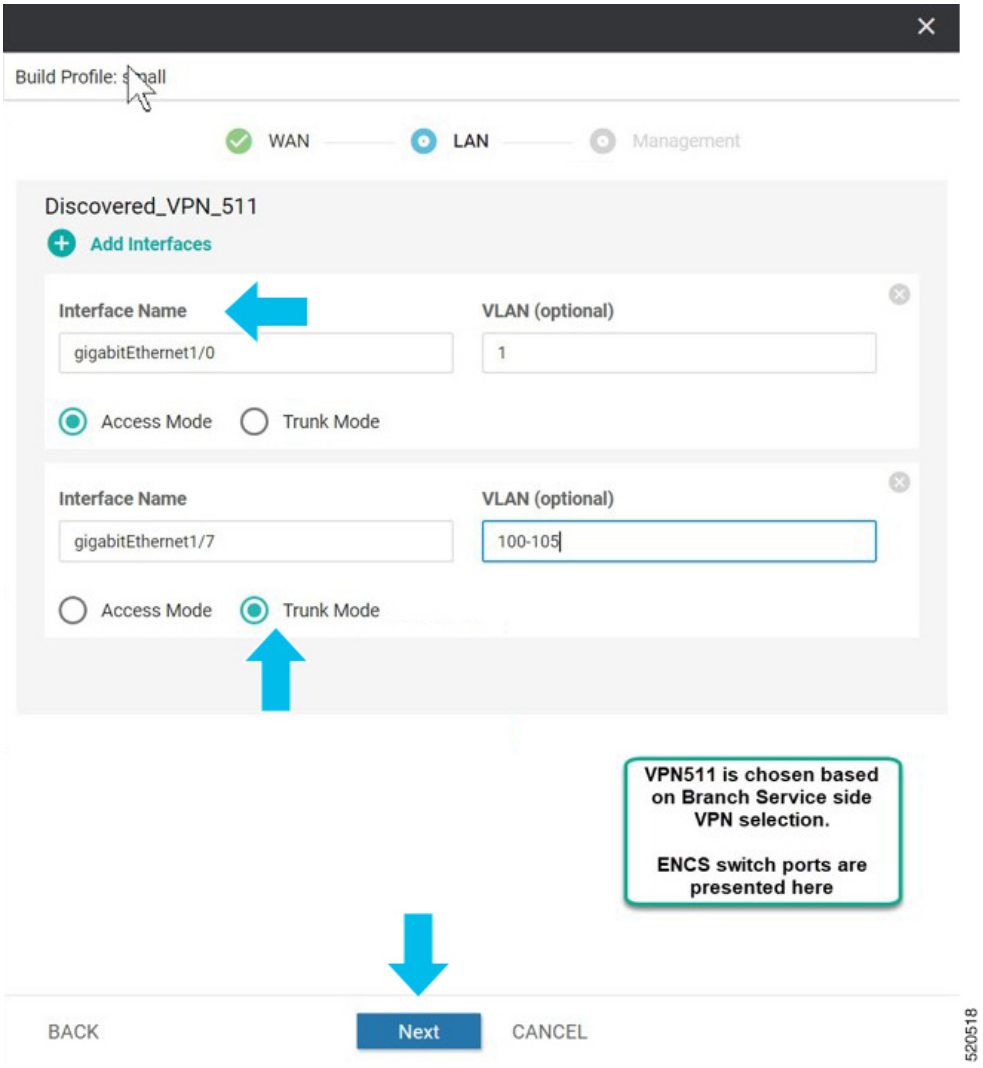
3. To build a device profile, enter the WAN interface details for the profile:
   - Enter the name of a TLOC interface to associate it with the a circuit that is associated with this router, in **Interface Name**.
   - Choose one of the radio buttons, **DHCP** or **Static**.
   - (Optional) Enter the IP address of the primary DNS server in the network in **DNS server**.
   - Click **Next**.



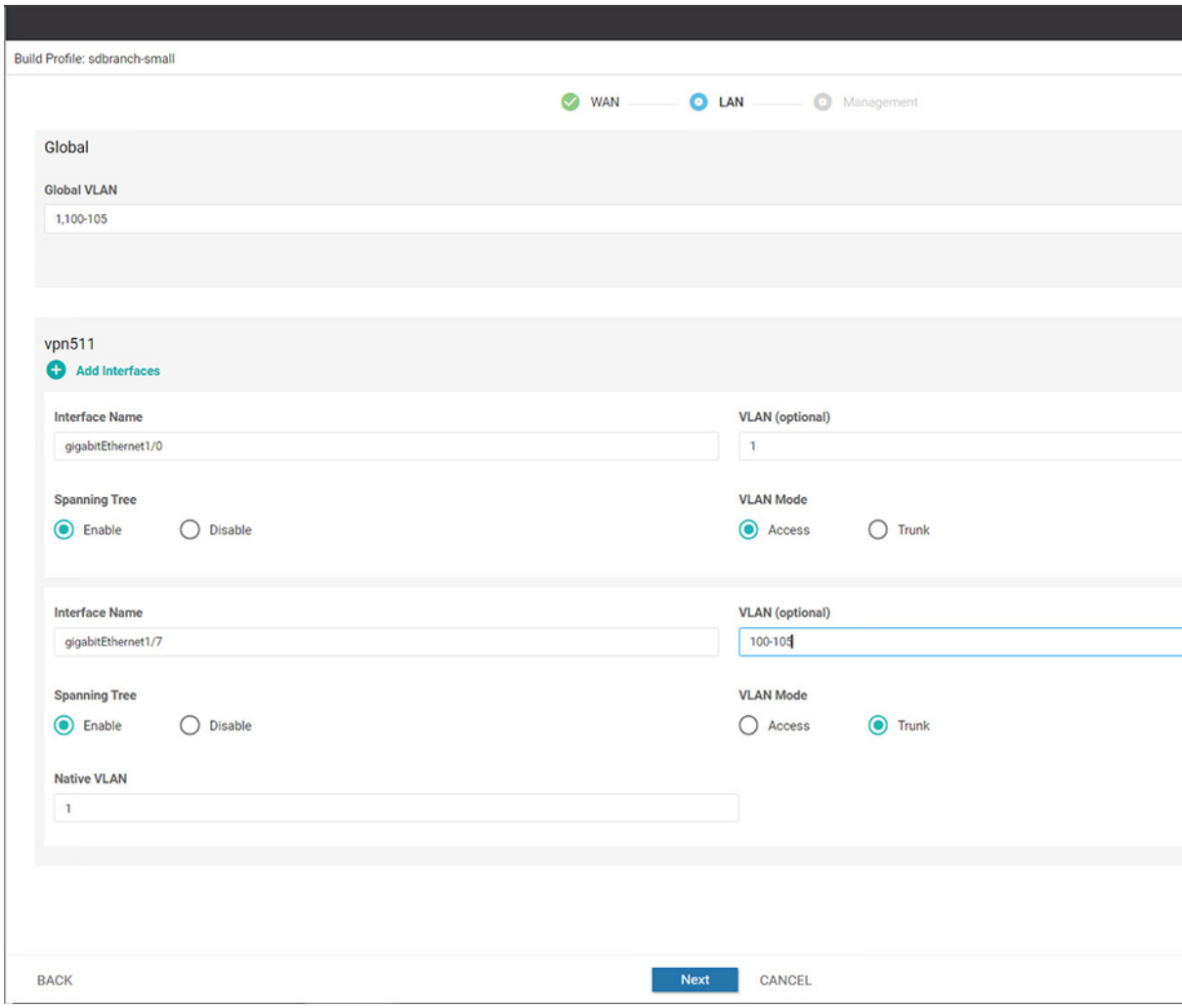
4. Enter the LAN interface details for the profile:
   - Enter the name of a LAN side interface in **Interface Name** to associate with the segment .

- (Optional) Enter a sub-interface in **VLAN** if needed for your deployment.
- Choose one of the radio buttons, **Access Mode** or **Trunk Mode**.
- Click **Next**.

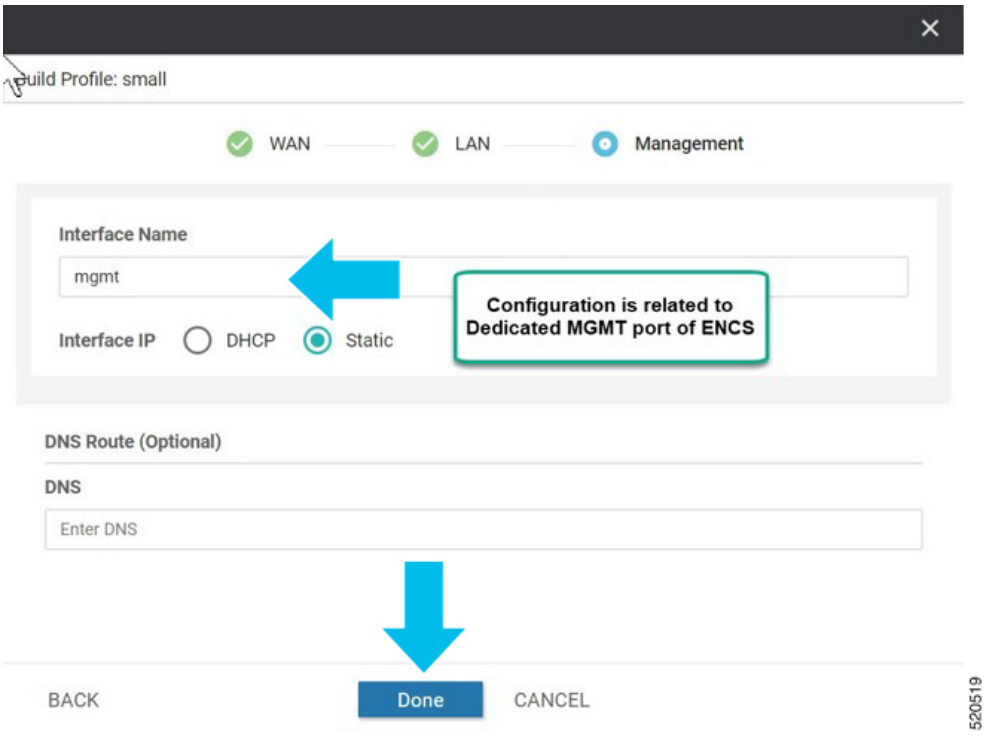
Global VLANs must be defined using addon CLI template. Global VLANs are a collection of all VLANs used in the ENCS switch ports.



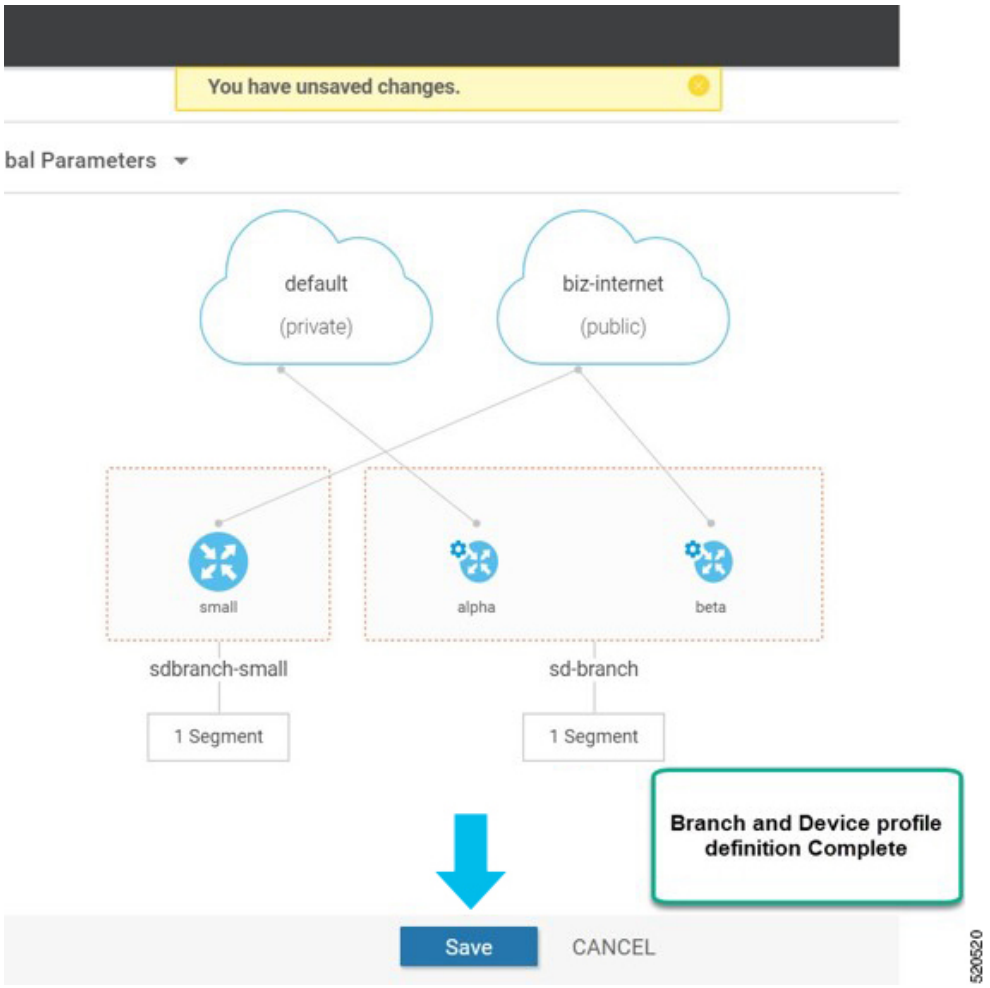
Starting from NFVIS 4.4 release, you can set some additional LAN interface details from Cisco SD-WAN Manager.



5. Enter the management interface details for the profile:
   - Enter the name for the management interface in **Interface Name** to associate with the device.
   - Choose one of the radio buttons, **DHCP** or **Static**.
   - Click **Done**.



6. Click **Save** on the Network Design screen.



ENCS Device Profile and Additional Services

For ENCS 5400 device, you have to configure both device profile and addon services. After you configure a device profile, continue with adding services on the ENCS branch design.

VNF image package for services, virtual networks and associated virtual switch or bridge are part of the ENCS network design. Virtual NICs (VNICs) are part of the VNF services and the order of the VNICs must be configured correctly for continuous traffic flow through the different services, in the intended order. To simplify the user experience, there are a set of prescriptive Cisco validated designs that you can choose and complete the network design. You can also customize the network topology if required, to delete and modify, services or networks.

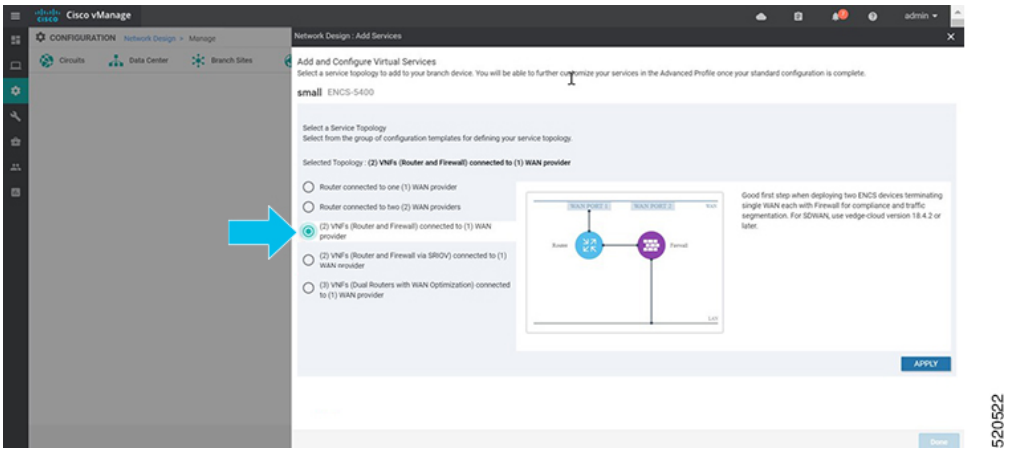
In the following example, Cisco Catalyst SD-WAN router and Cisco NGFW based network topology is created. This procedure can be applied to other Cisco validated network design templates.

To add services and create network topology template for a group of sites:

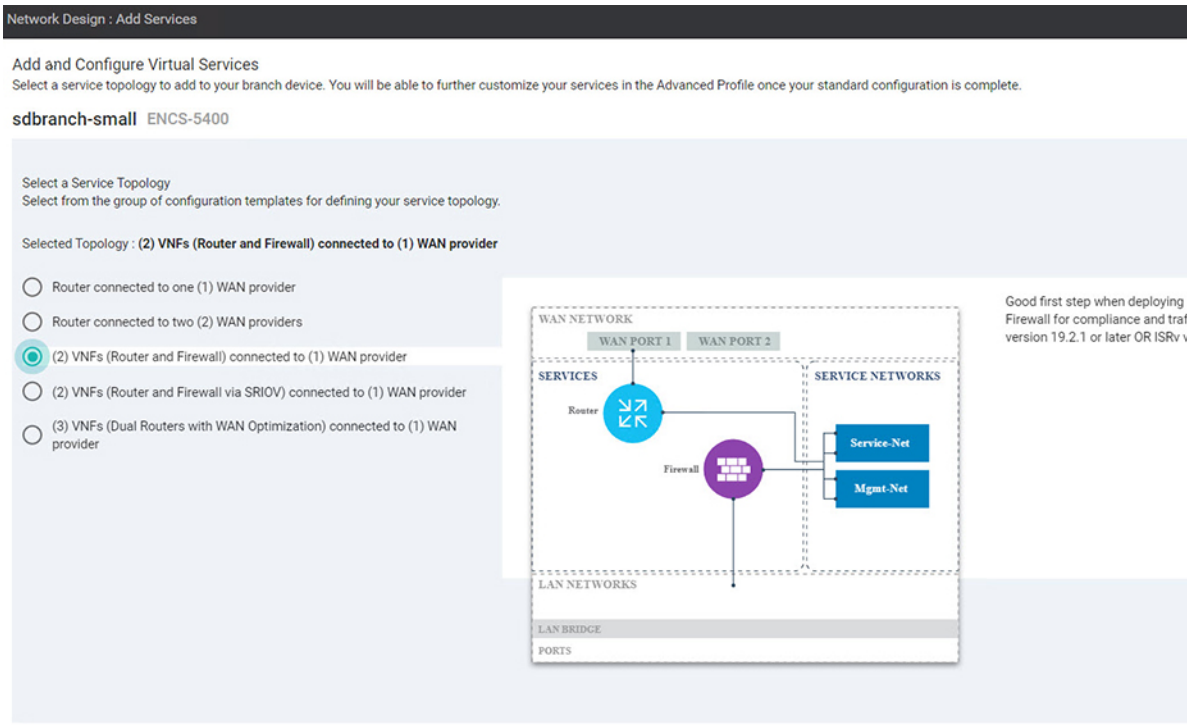
1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. A network diagram is displayed on the **Network Design** page. Hover your mouse over the image representation of the branch device and choose **Add services**.



3. In the **Add services** page, choose a service topology from the list of available configuration templates. Click **Apply**.



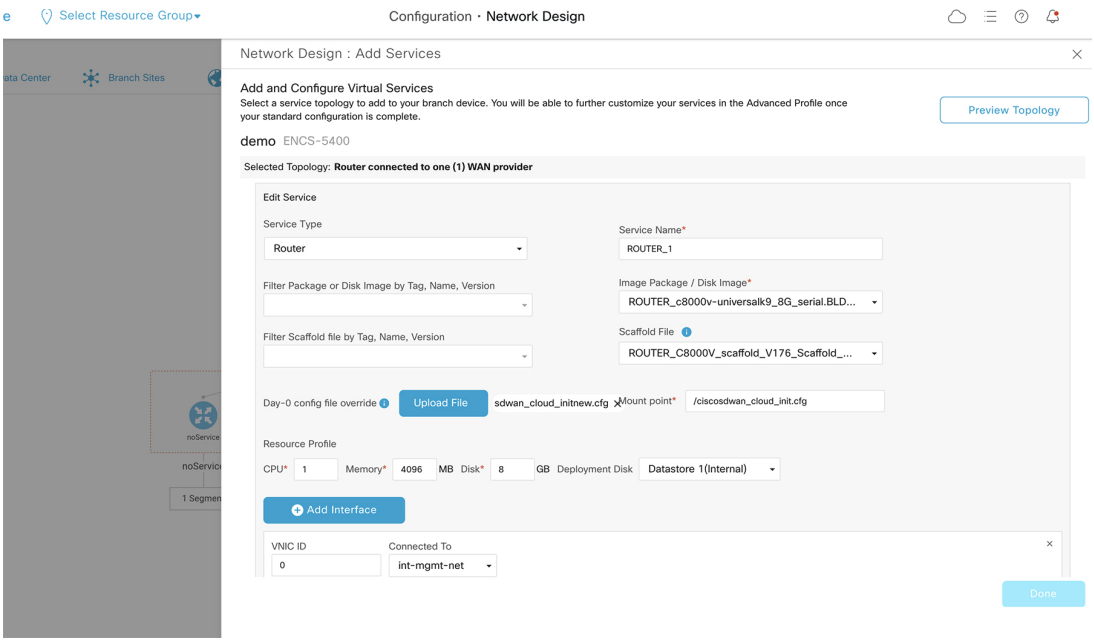
Starting from NFVIS 4.4 release, a graphical view of the topology is available for the listed templates.



4. Starting from NFVIS 4.6.1 release, you can upload either a tar.gz file or a qcow2 file when registering your image and you can tag the image with keywords to help identify it. You can also upload a scaffold file.

   (Optional) To upload a Day 0 configuration file, that overrides any settings in the scaffold or tar.gz files or an existing Day 0 configuration in the package or scaffold file, ensure the following:

   - Variables are represented within "{{" "}}". Example: **`{{SAMPLE_VARIABLE}}`**
   - Passwords are represented within "$${" and "}". Example : **`$${SAMPLE_PASSWORD}`**
   - Variables to be ignored are represented within "${" and "}". Example: **`${NICID_0}`**



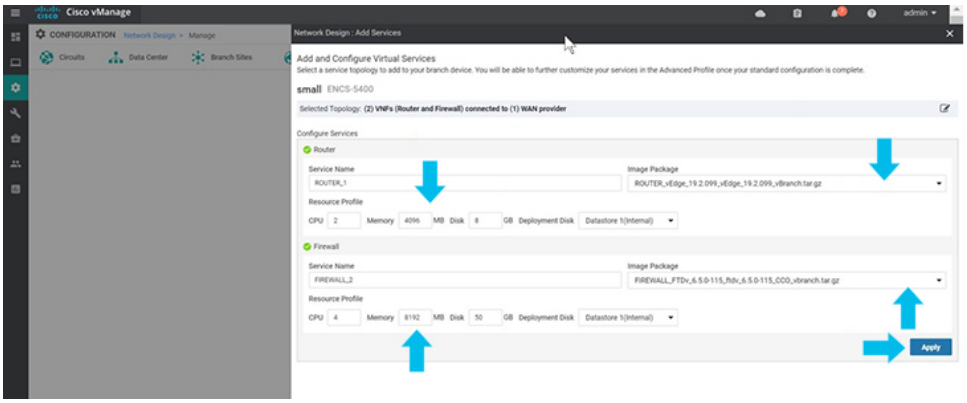
Note The mount point value varies with the VNF. The different mount point values are as follows:

- For C8000v and ISRv in controller/ Cisco SD-WAN Manager mode: ciscosdwan_cloud_init.cfg
- For C8000v and ISRv in autonomous/non-Cisco SD-WAN Manager mode: iosxe_config.txt
- For vEdge Cloud: /openstack/latest/user_data
- For ASAv and FTDv: day0-config

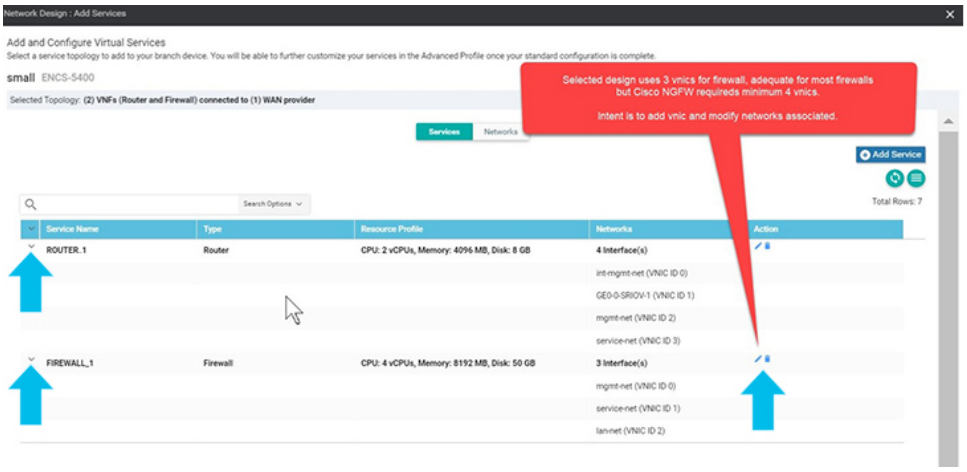
5. To add and configure the virtual services, enter the details of the virtual services:
   - Choose the **Image Package** from the drop-down list, and enter details to the resource profiles.

Note When you deploy the device in a remote site, verify if the image is available on your local system to skip the image download over WAN. For more information see, NFVIS Deployment in Sites with Low WAN Bandwidth, on page 117

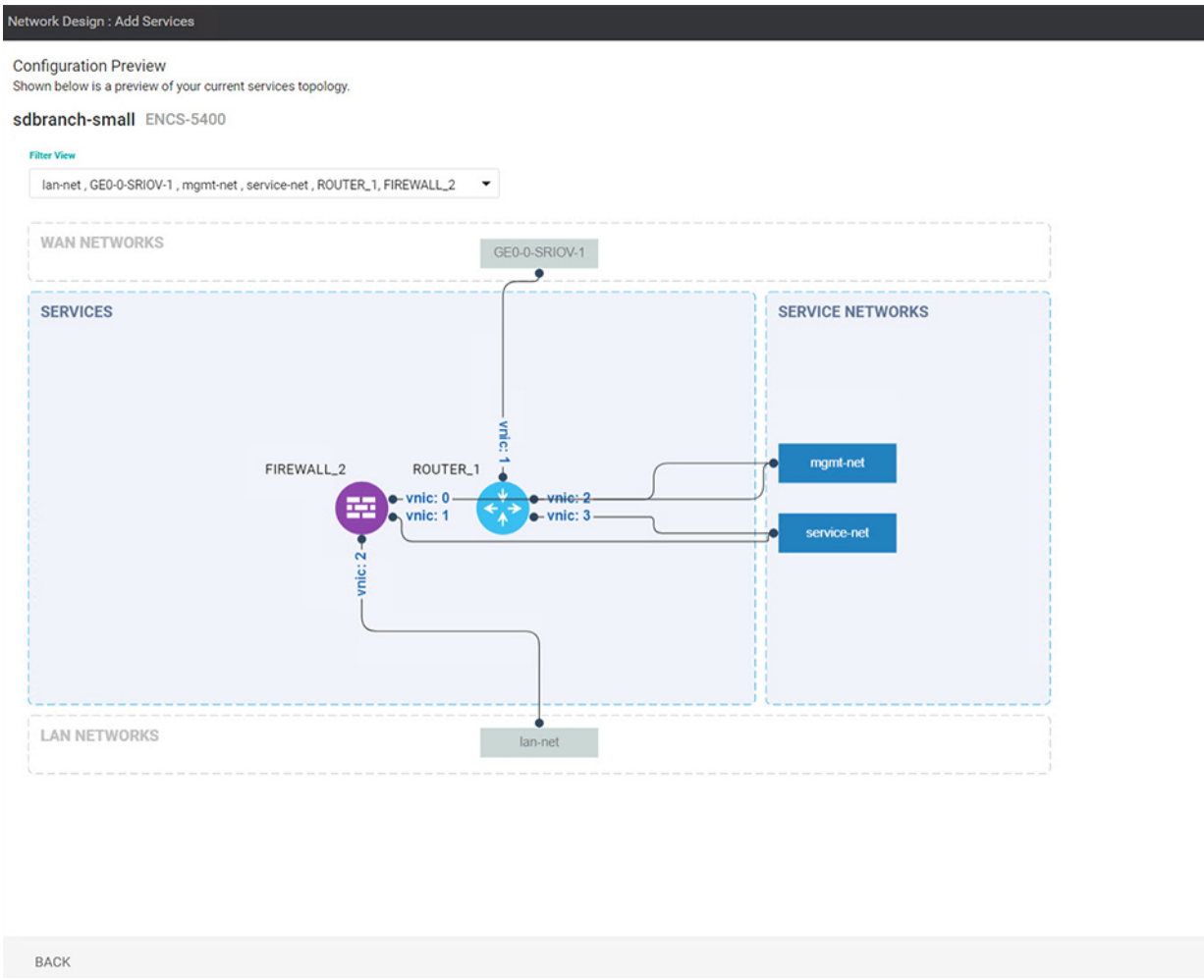
   - Click **Apply**.



6. The list of services added in the previous step are displayed on this page. You can add or modify networks associated with each device.



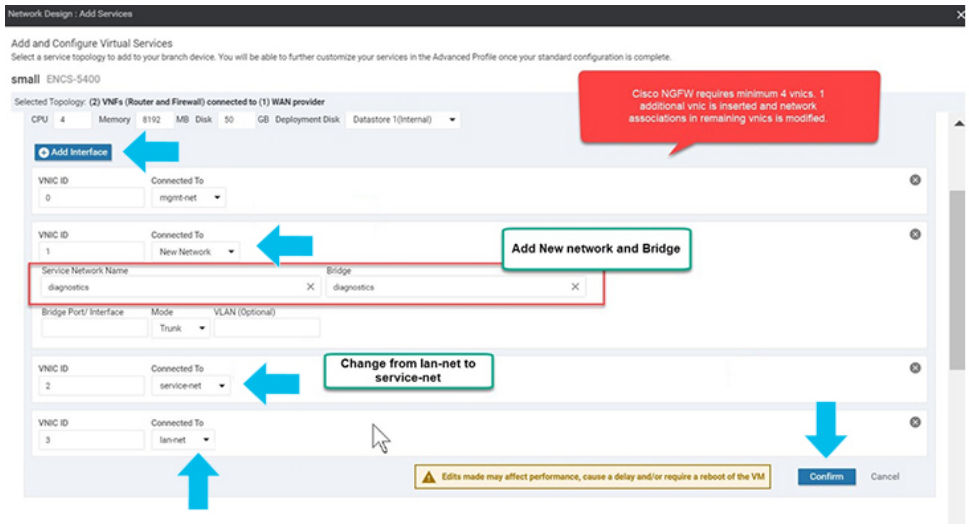
Starting from NFVIS 4.4, you can click **Preview Topology** to view the topology of the added services along with the associated networks. You can use the drop down menu to **Filter View** and view only the services that you want.



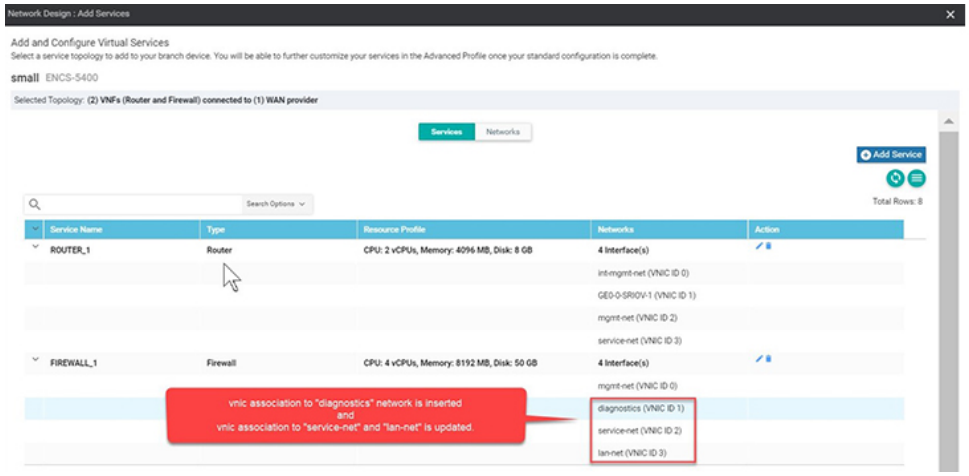
7. Click **+ Add Interface** to add a new network. Enter the network details associated with the new network.

   Modify the details related to the exisitng interfaces

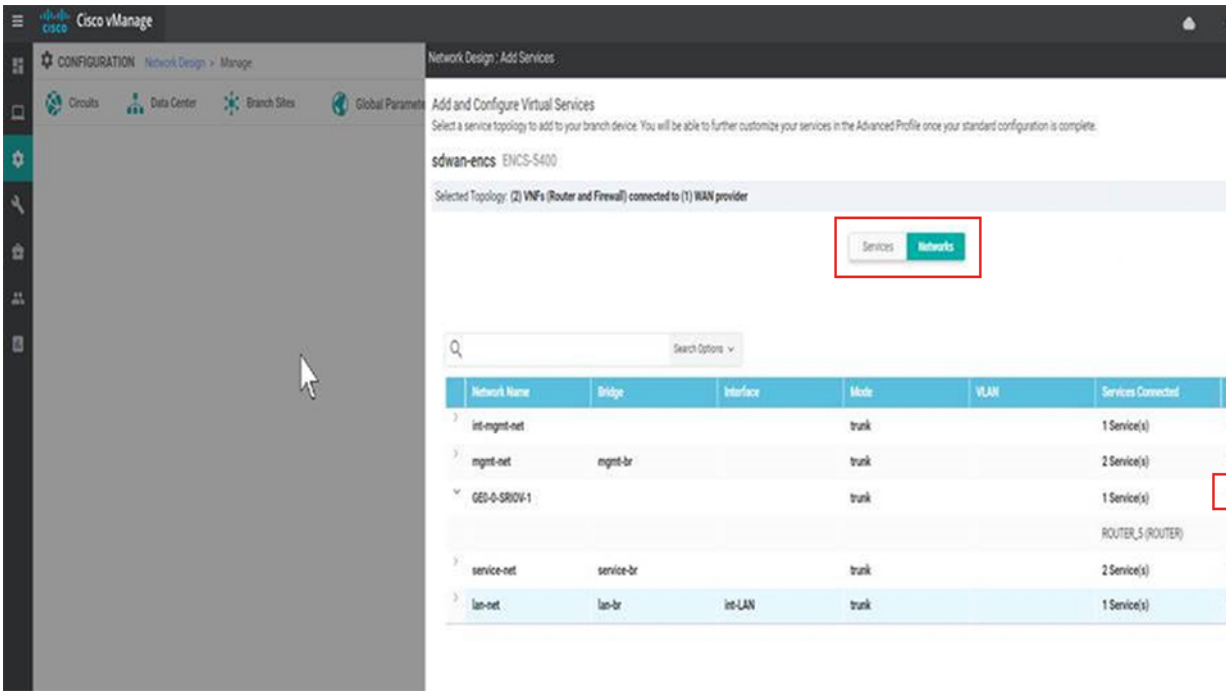
   Click **Confirm**.



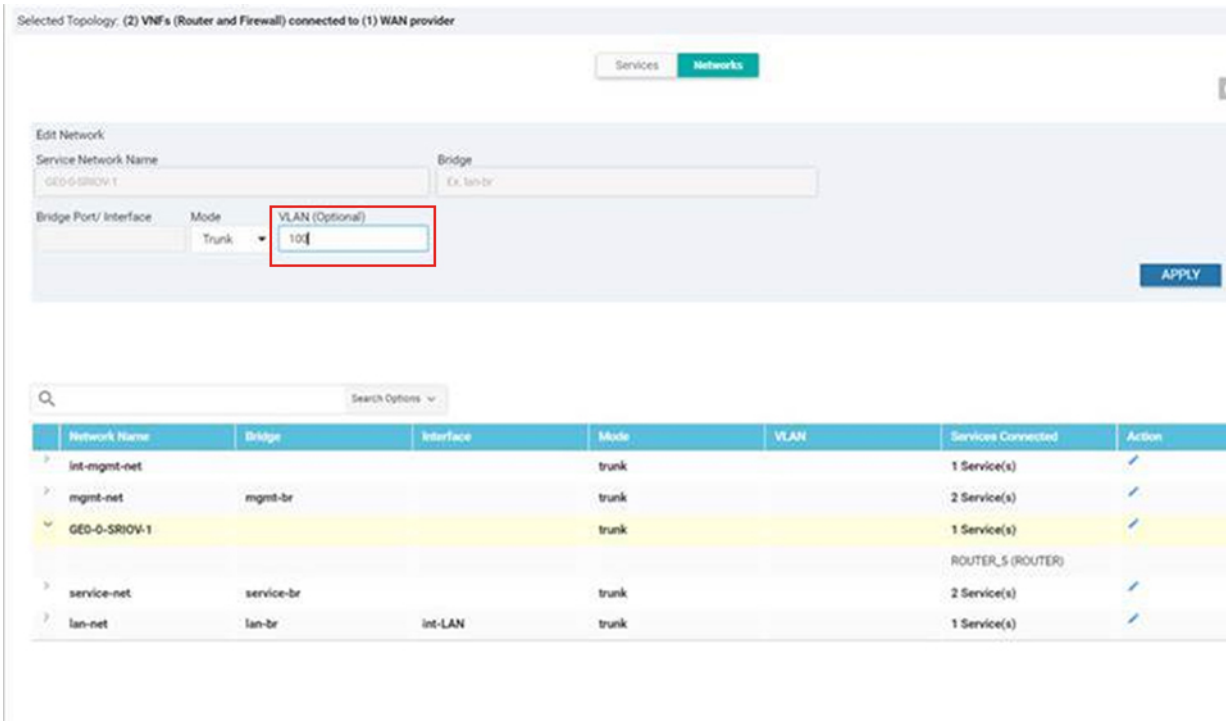
8. You can see the new and modified interfaces in the **Services** page.



9. To define VLAN for the SRIOV networks, select **Networks**. In the list of networks displayed you can add or modify the networks.



10. For WAN side network, by default all VLANs in trunk mode are allowed. If you have set the Dot1q in ISRv, VLAN passes through the network.



Note There is a known race condition defect that leads to VNF deployment failure when VLANs are configured in networks using NFVIS 4.2.1. You can upgrade to NFVIS 4.4.1 along with Cisco vManage 20.4.1 or above to resolve this issue.

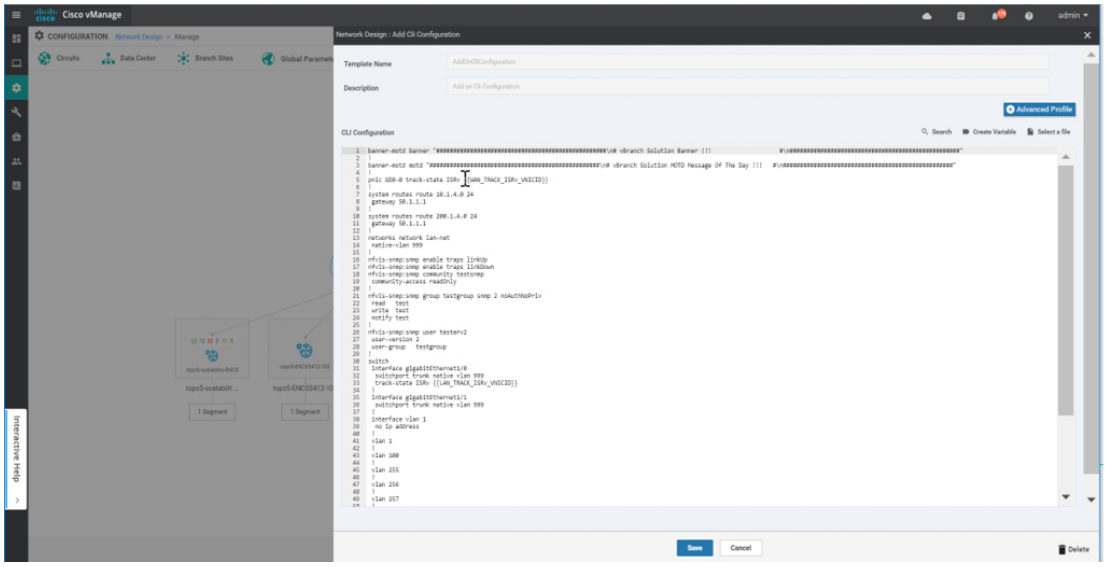
CLI Add-On Feature Templates

You can use CLI add-on feature templates to attach specific CLI configurations to a device. CLI add-on feature templates must be used in conjunction with Network Design. It is recommended to use this feature only for configurations that are not natively supported in Network Design.

To create a CLI add-on feature template:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Create Network Design** (which is displayed if you have not yet created a network topology) or **Manage Network Design** (which is displayed if you have created a network topology).

   Hover your mouse over the image representation of the branch device and choose **Add CLI Configuration**.



This section lists the supported add-on CLI configurations for the following features in NFVIS. For more information, see Cisco Enterprise Network Function Virtualization Infrastructure Software Configuration Guide

Boot-up time	`vm_lifecycle tenants tenant admin deployments deployment deployment-ROUTER_1 vm_group deployment-ROUTER_1 bootup_time 600`
Port tracking	`pnic GE0-0 track-state ROUTER_1 1`

ACL	system settings ip-receive-acl 0.0.0.0/0 service [scpd] action accept priority 0 ! system settings ip-receive-acl 10.31.40.24/32 service [scpd] action accept priority 5 !
Static route	system routes route 192.168.10.10 24 gateway 192.168.0.2
TACACS+	aaa authentication tacacs tacacs-server host 172.19.156.179 key 7 encrypted-shared-secret cisco123 admin-priv 15 oper-priv 14 !
Banner	banner-motd banner "Banner for vBranch"
Message of the Day (MOTD).	banner-motd motd "MOTD for vBranch"

SNMP	nfvis-snmp:snmp enable traps linkUp nfvis-snmp:snmp enable traps linkDown nfvis-snmp:snmp community testsnmp community-access readOnly ! nfvis-snmp:snmp group snmpgroupv1 snmp 1 noAuthNoPriv read test write test notify test ! nfvis-snmp:snmp group snmpgroupv2 snmp 2 noAuthNoPriv read test write test notify test ! nfvis-snmp:snmp group snmpgroupv3 snmp 3 authPriv read test write test notify test ! nfvis-snmp:snmp user testerv1 user-version 1 user-group snmpgroupv1 ! nfvis-snmp:snmp user testerv2 user-version 2 user-group snmpgroupv2 ! nfvis-snmp:snmp user testerv3 user-version 3 user-group snmpgroupv3 auth-protocol sha passphrase cisco123 priv-protocol aes passphrase cisco123 ! nfvis-snmp:snmp host SNMP-SERVER-57 host-port 161 host-ip-address 172.19.149.57 host-version 3 host-security-level authPriv host-user-name testerv3 ! nfvis-snmp:snmp host SNMP-SERVER-179 host-port 161 host-ip-address 172.19.156.179 host-version 1 host-security-level noAuthNoPriv host-user-name testerv1 ! nfvis-snmp:snmp host SNMP-SERVER-229 host-port 161 host-ip-address 172.25.221.229 host-version 2 host-security-level noAuthNoPriv host-user-name testerv2 !
Default gateway	system settings default-gw 172.25.217.1

Configure VLAN range instead of individual VLAN CLI for ENCS switch. VLAN range value can be parameterized which is useful in configuring site specific VLAN range variations. **Note** This command is supported only for NFVIS 4.4 and newer versions.	`switch vlan-range 1,100,200,300-305`

ENCS switch configurations: global VLAN, access vlan, trunk vlan, native vlan, spanning tree, port-channel, track-state, speed, duplex and QoS	

	switch interface gigabitEthernet1/0 track-state ISRv 3 ! interface gigabitEthernet1/1 speed 100 duplex full ! interface gigabitEthernet1/2 channel-group 1 mode auto ! interface gigabitEthernet1/3 channel-group 1 mode auto ! interface gigabitEthernet1/4 speed 100 switchport mode access switchport access vlan 100 ! interface gigabitEthernet1/5 spanning-tree disable ! interface gigabitEthernet1/6 speed 1000 duplex full switchport mode trunk switchport trunk native vlan 101 no switchport trunk allowed switchport trunk allowed vlan vlan-range 8,113-114,130 ! interface gigabitEthernet1/7 qos cos 3 switchport mode trunk switchport trunk native vlan 999 no switchport trunk allowed switchport trunk allowed vlan vlan-range 255-257,999 ! interface port-channel1 spanning-tree mst 1 cost 200000000 spanning-tree mst 2 cost 200000000 switchport mode trunk no switchport trunk allowed switchport trunk allowed vlan vlan-range 100,126-128 ! vlan 1 ! vlan 8 ! vlan 100 ! vlan 101 ! vlan 113 ! vlan 114 ! vlan 126 ! vlan 127

	! vlan 128 ! vlan 130 ! vlan 255 ! vlan 256 ! vlan 257 ! vlan 996 ! vlan 997 ! vlan 998 ! vlan 999 ! qos port ports-trusted qos trust cos-dscp spanning-tree mode mst spanning-tree mst 2 priority 61440 spanning-tree mst configuration name mst_LAN instance 1 vlan 996-998 instance 2 vlan 100,126-128 ! !
Single IP Address Sharing between NFVIS and the Router VM	single-ip-mode vm-name deployment-name-of-ROUTER

Single IP Address Sharing between NFVIS and Router VM

Table 3: Feature History

Feature Name	Release Information	Description
Support for Single IP Address for NFVIS and the Router VM	NFVIS 4.5 Cisco vManage Release 20.5.1 and later	This release extends the support for using a single public IP address between NFVIS and the router VM to the SD-Branch solution.

Overview of Single IP Address Sharing

Typically, in a virtual branch deployment, two public IP addresses are needed for each branch site, one for the NFVIS and the other for the router VM. With the support for sharing a single IP address, a single public IP address that is assigned to a branch site, can be shared between NFVIS and the router VM deployed on NFVIS. This feature limits the number of public IP addresses required to just one, and also ensures that the branch site is reachable even if the router is in failure state.

Use the CLI Add-on feature template in Cisco SD-WAN Manager to configure this feature.

How Single IP Address Sharing Works

- NFVIS in a branch site has a public IP address assigned. The required single IP address configuration is configured using the Add-on CLI feature template in Cisco SD-WAN Manager.
- Cisco SD-WAN Manager pushes this configuration to NFVIS. NFVIS then releases its WAN IP address to the router VM that is being deployed.
- The deployed VM acts as the gateway for NFVIS.
- NFVIS periodically pings the NFVIS Internet gateway, through the deployed VM, to verify NFVIS-to-Cisco SD-WAN Manager connectivity. If NFVIS is unable to connect to the Internet gateway, it does the following:
  1. Shuts down the router VM deployed on NFVIS
  2. Reclaims the IP address it assigned to the VM
  3. Tries to reestablish the control connection with Cisco SD-WAN Manager

Supported VMs

Single IP address sharing between NFVIS and router VMs is only supported for the following router VMs:

- Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V)
- Cisco Integrated Services Virtual Router (ISRv)
- Cisco vEdge Cloud router

Configure Single IP Address Sharing

Step 1: Configure Router VM

The following example shows the SDWAN NAT DIA configuration that must be included on the router VM. In this example, GigabitEthernet1 is the MGMT interface connected through int-mgmt-net on NFVIS. GigabitEthernet2 is the VPN 0 WAN interface connected through GE0-0 on NFVIS.



Note Ensure that **`int-mgmt-net subnet`** mask is consistent across all the Cisco NFVIS devices. When you deploy a single IP topology and provide different **`int-mgmt-net subnet`** masks, the Cisco NFVIS devices loses the control connection.

```
Interface Gigabitethernet1
ip nat inside
Interface Gigabitethernet2
ip nat outside

ip nat inside source list NAT interface GigabitEthernet2 overload
ip access-list standard NAT permit ip 10.20.0.0 0.0.0.255

vrf definition 500
!
address-family ipv4
exit-address-family
```

```
!
address-family ipv6
exit-address-family
!

interface Gigabitethernet1
 vrf forwarding 500

interface Gigabitethernet2
 ip nat outside

ip nat route vrf 500 0.0.0.0 0.0.0.0 global
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
!
```

Note VRF 500 is an example and can be changed to any allowed SDWAN VPN number (range: 0 to 65527) other than 0 and 512.

Note For end-to-end configuration example, see *Appendix*.

Step 2: Configure Single IP Address Sharing

The following is the sample configuration that must be included in the CLI Add-on feature template to enable single IP address sharing between NFVIS and the router VM. In this example, deployment-ROUTER_1.deployment-ROUTER_1 is the deployment name of the router VM.

```
single-ip-mode vm-name deployment-ROUTER_1.deployment-ROUTER_1
```

Note For end-to-end configuration example, see the *Appendix* chapter.

Verify Single IP Address Sharing

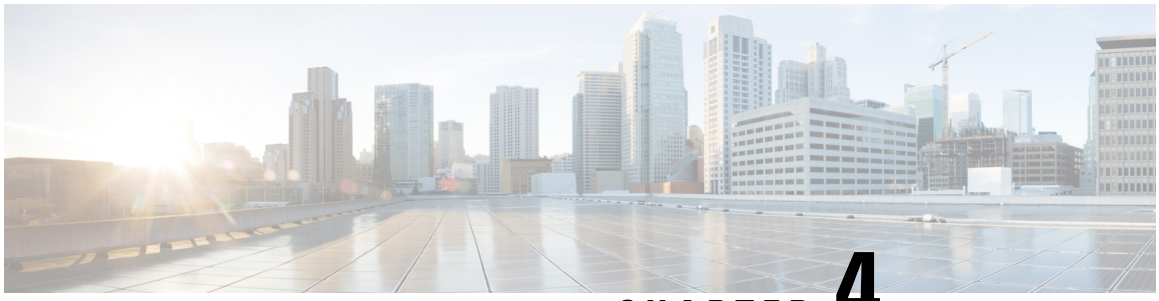
The following is sample output from the **show single-ip-mode** command, which is used to verify the status of single IP mode..

```
Device# show single-ip-mode
single-ip-mode state active
single-ip-mode state-details "VM alive"
```

The following is sample output from the **show control connections** command, which is used to verify Cisco NFVIS to Cisco SD-WAN Manager control connection.

```
Device# show control connections
                          PEER                                                PEER
                 CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                    PRIV
  PEER                                     PUB
                 GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP        PORT  PUBLIC IP      PORT
  LOCAL COLOR     PROXY STATE UPTIME      ID
--------------------------------------------------------------------------------------------------------------------------------
```

```
vmanage dtls 10.10.10.29     101        0      172.19.156.234    12846 172.19.156.234 12846
       bronze    No    up     0:01:41:22  0
```



CHAPTER 4

Deploy Cisco NFVIS SD-Branch Solution

The deployment section covers the prerequisites to onboard NFVIS WAN Edge devices, followed by the different on-boarding options and on-boarding verification.

- Prerequisites for NFVIS WAN Edge Onboarding, on page 51
- Prerequisites to Onboard NFVIS WAN Edge Devices using PnP Process, on page 52
- Onboarding NFVIS device using Plug-and-Play process, on page 53

Prerequisites for NFVIS WAN Edge Onboarding

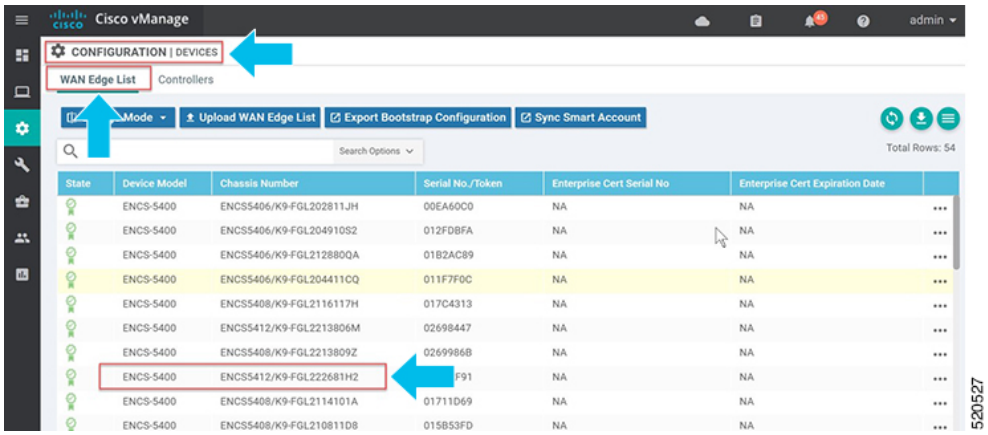
Ensure that the following prerequisites are met before proceeding with the WAN Edge onboarding process:

- The NFVIS WAN Edge device has reachability to the Cisco SD-WAN Validator and Cisco SD-WAN Manager.
- The authorized WAN Edge device whitelist is uploaded on all Cisco SD-WAN Control Components by adding and associating the WAN edge devices with a Cisco SD-WAN Validator profile in the PnP portal. The whitelist provision file can be downloaded from the PnP portal and uploaded to Cisco SD-WAN Manager or synchronized to Cisco SD-WAN Manager using the **Sync Smart Account** option. Cisco SD-WAN Manager later distributes this whitelist to the additional controllers.

Note Software WAN Edge devices deployed in virtual environment do not have chassis or serial number. For such devices, PnP server generates a unique serial number when the software device is added in the PnP portal.

- The WAN Edge device must be in **Valid** or **Staging** certificate state.

  In Cisco SD-WAN Manager, navigate to **Configuration** > **Devices** > **WAN Edge List**, identify the WAN Edge device. Under the **Validity** column, verify the device is in either **Valid** or **Staging** state.



Note A WAN Edge device within **Staging** state will establish only control connections with the Cisco Catalyst SD-WAN Control Components. Data plane connections are not established across WAN Edge devices. To fully onboard the device, the device state must be moved from **Staging** to **Valid**. In Cisco SD-WAN Manager, under **Configuration** > **Certificates** > **WAN Edge List**, select the WAN Edge device(s) and change the state to **Valid** under the **Validity** column and click **Send to Controllers**.

- The WAN Edge device must be running NFVIS software.

Prerequisites to Onboard NFVIS WAN Edge Devices using PnP Process

Ensure that the following prerequisites are met for onboarding NFVIS WAN Edge devices using PnP process:

- The factory default ENCS NFVIS device should be able to resolve FQDN devicehelper.cisco.com and reach the Cisco cloud-hosted Plug-and-Play Connect server to retrieve the Cisco SD-WAN Validator information, organization-name and enterprise root-ca certificates (if using enterprise root-ca certificates).
- The WAN Edge must be factory defaulted before onboarding using bootstrap option.

Note ENCS NFVIS devices can be factory defaulted if needed using the CLI command on the device **factory-default-reset all**.

- The Cisco PnP Connect server at http://software.cisco.com must have the ENCS NFVIS WAN Edge added and the device associated with the Cisco SD-WAN Validator profile.

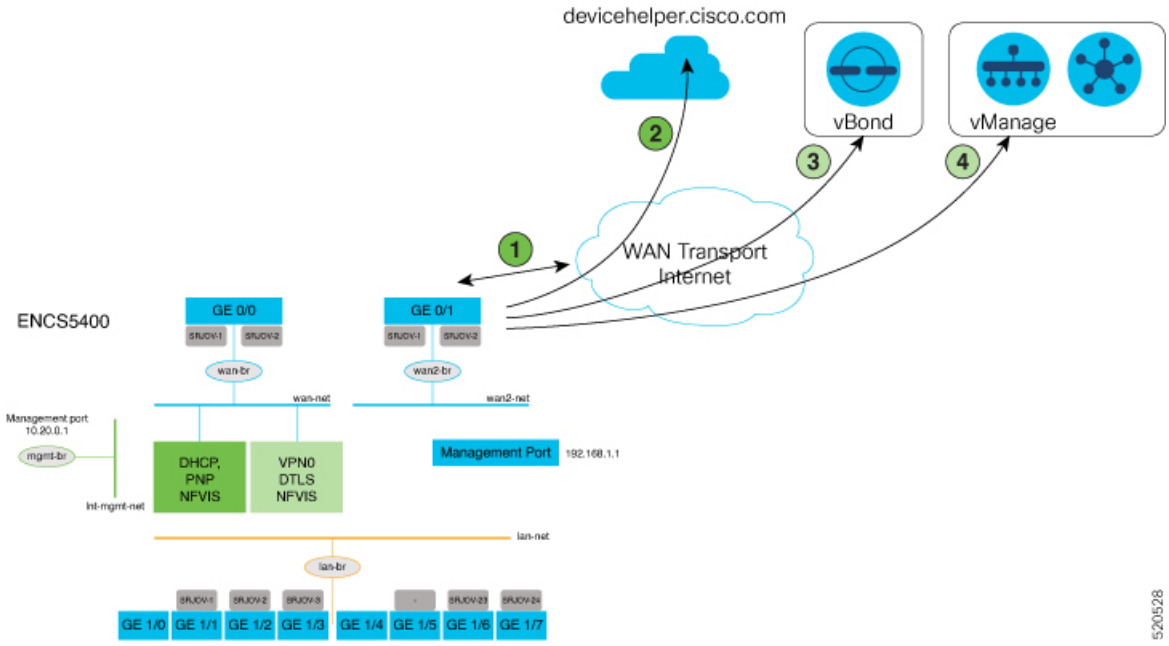
  Navigate to **Cisco Software Central** > **Network Plug and Play** > **Plug and Play Connect** > **Devices**, verify the device is available with **Controller** profile associated to it.

Onboarding NFVIS device using Plug-and-Play process

The NFVIS WAN Edge is initially onboarded into the Cisco Catalyst SD-WAN overlay network through the PnP process.

Note The factory default NFVIS WAN Edge device has preconfigured PnP supported interfaces. The device dynamically procures an IP address and registers itself with the Cisco SD-WAN Control Components.

1. Connect the PnP supported interface to the internet WAN transport.



The steps involved in the image above is explained in detail below:

a. Power on the ENCS device and connect the WAN Interface to GE0-0.

b. ENCS connects to devicehelper.cisco.com. ENCS gets a root certificate from the PnP Connect server.

c. ENCS is redirected to Cisco SD-WAN Validator. The PnP Connect server changes the ENCS device state from **Pending** to **Redirected**.

d. ENCS is automatically registered to Cisco SD-WAN Manager at this step.

Note Starting from Cisco NFVIS Release 4.9.1, establishing a control connection to the management plane via the management port is supported. The management port needs to be connected with Cisco SD-WAN Manager for a successful connection to the control plane.

If the management port is used to establish the control connection, you should preserve the control connection by adding a CLI add-on feature template under VPN 0 to the ENCS device in Cisco SD-WAN Manager. For more information on CLI add-on feature templates, see CLI Add-on Feature Templates. Here's the sample management CLI add-on CLI template:

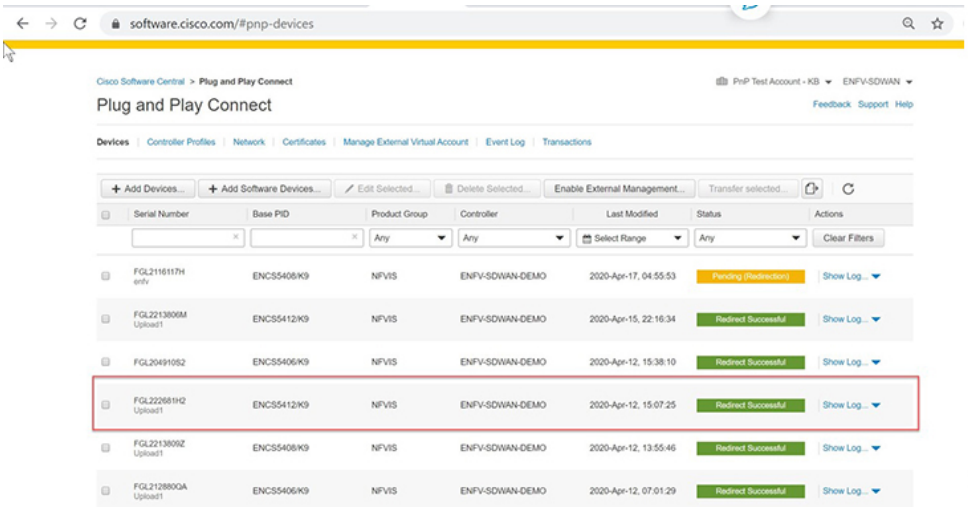
```
vpn 0
 interface MGMT
  no shutdown
  tunnel-interface
   color red
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   encapsulation ipsec
  !
 !
!
```

2. Connect GE0/0 port to WAN and power on the ENCS device
   - After bootup, the device dynamically obtains IP address, default gateway, and DNS information through the DHCP process from the upstream WAN transport device.
   - The WAN Edge device makes a DNS request to connect devicehelper.cisco.com to the ZTP server.
   - The WAN Edge device reaches the Cisco cloud hosted PnP Connect server and presents its chassis and serial number in order to authenticate with the server.
   - After authentication, the PnP Connect portal provides information about the Cisco SD-WAN Validator, organization-name and root certificates.

Note For deployments using enterprise root-ca certificate, device downloads the enterprise root CA certificate, along with the Cisco SD-WAN Validator IP address or DNS and organization-name using the HTTPS protocol. This information is used by the WAN Edge device to initiate control connections with the Cisco SD-WAN Validator.

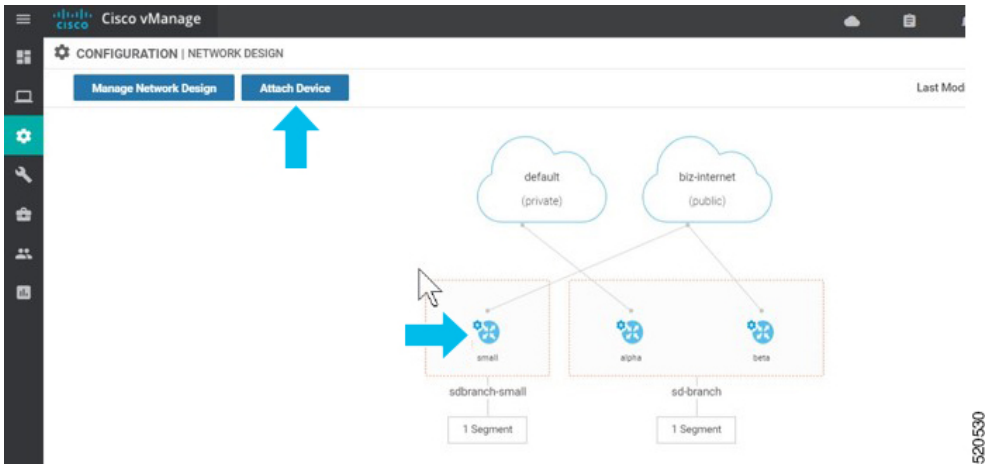
   - At this stage, the PnP portal indicates a **Redirect Successful** status when the WAN Edge device is redirected through PnP to the Cisco SD-WAN Validator controller.

     The following is an example of ENCS 5412 being redirected successfully:

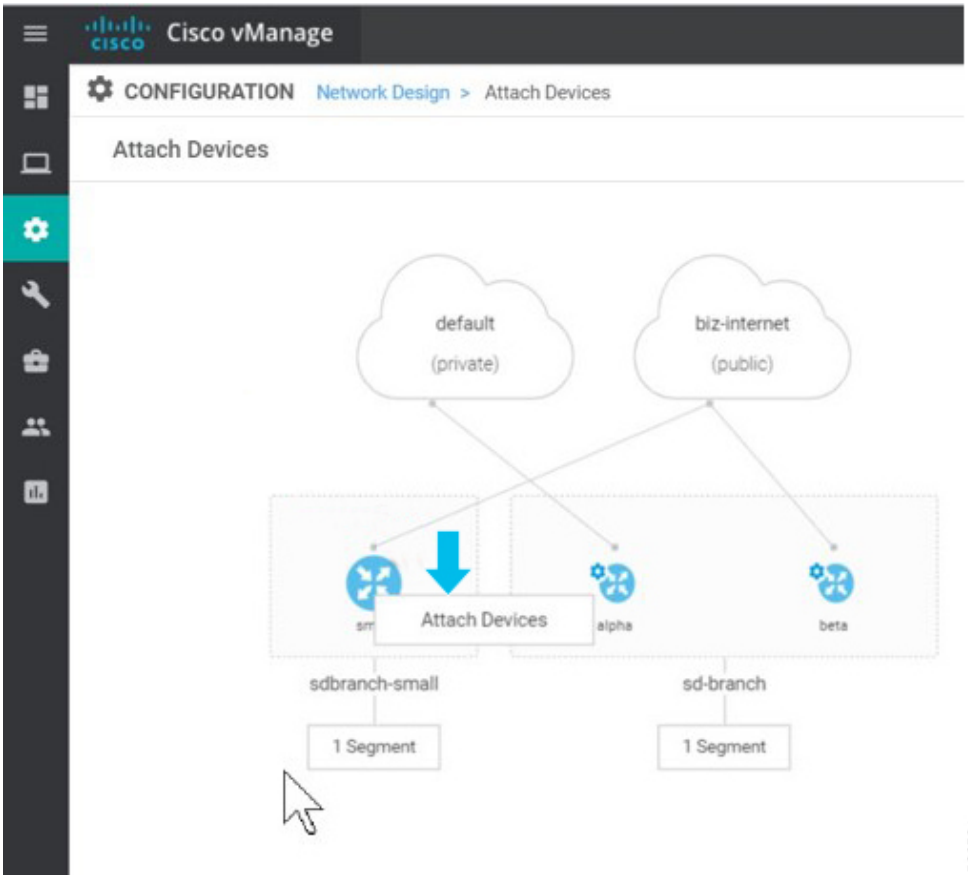


3. After authentication with the Cisco SD-WAN Validator, Cisco SD-WAN Manager information is available to the NFVIS WAN Edge device to register and establish a secure connection.

   - The device then attempts to establish a secure control connection with Cisco SD-WAN Manager. The device has no configuration and to build the connection it uses 0.0.0.0 as the system IP address to bring up the initial control connection with the Cisco SD-WAN Manager.
   - Attaching a device profile to WAN Edge devices makes the devices available to be controlled and configured through the Cisco SD-WAN Manager. To attach a device:
     - From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
     - Click **Attach Devices** and then select the device on the network topology.

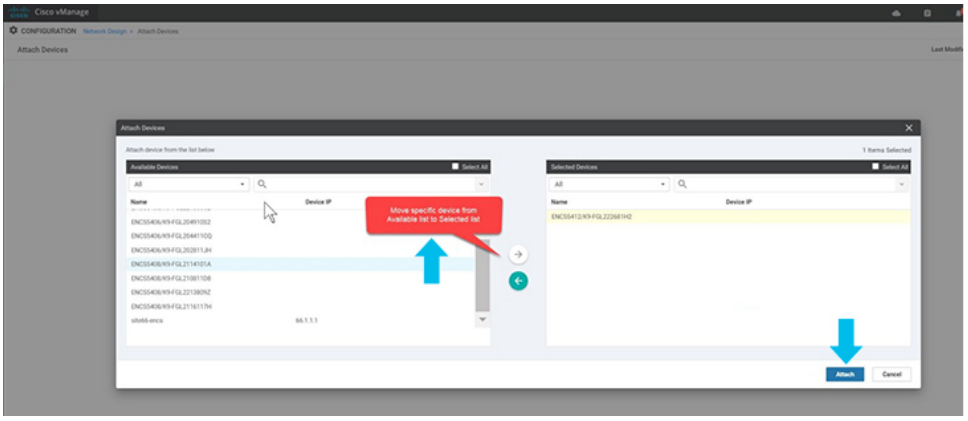


     - Click **Attach Devices**.



- A list of available devices appears on a pop up window. Select the specific device under the available list and move it to the selected list using the arrow.

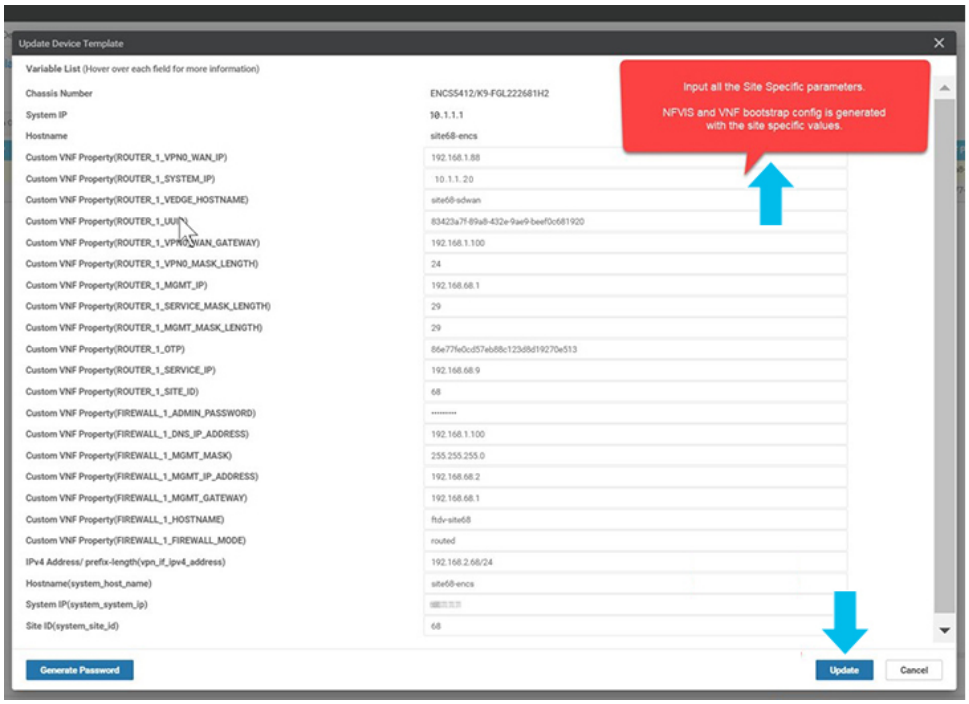
  Click **Attach**.



- The selected device can be modified using **Edit Device Template**.



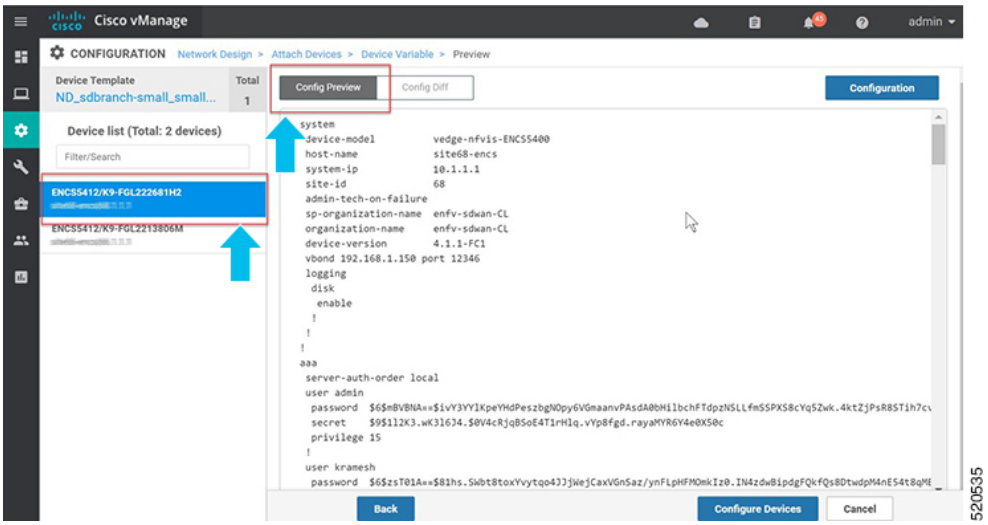
- You can update all the site specific parameters and the click **Update**.



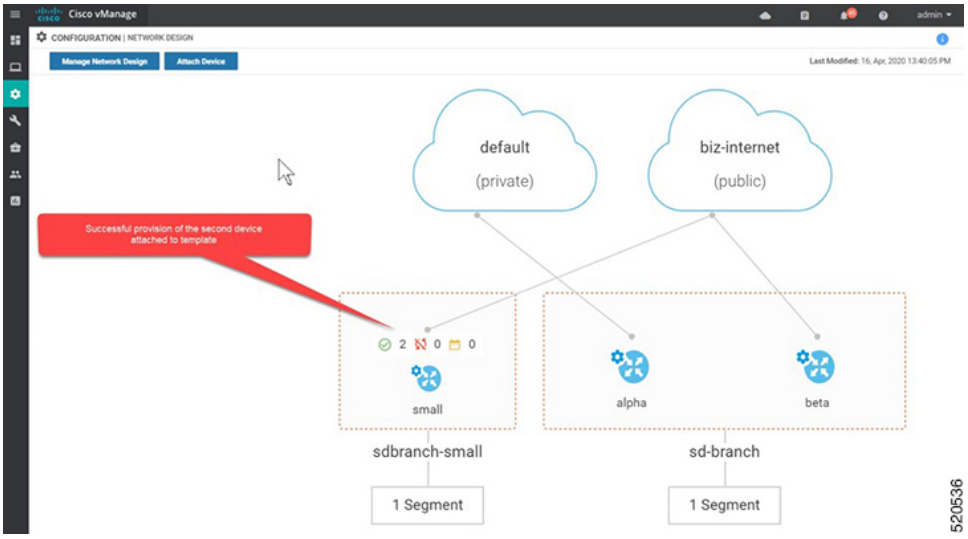
- Click on the name of the device and choose **config preview**. You can preview the configuration associated to the selected device.

  If you attach a device template containing the new CLI add-on feature template here, the configurations are merged and is visible here.

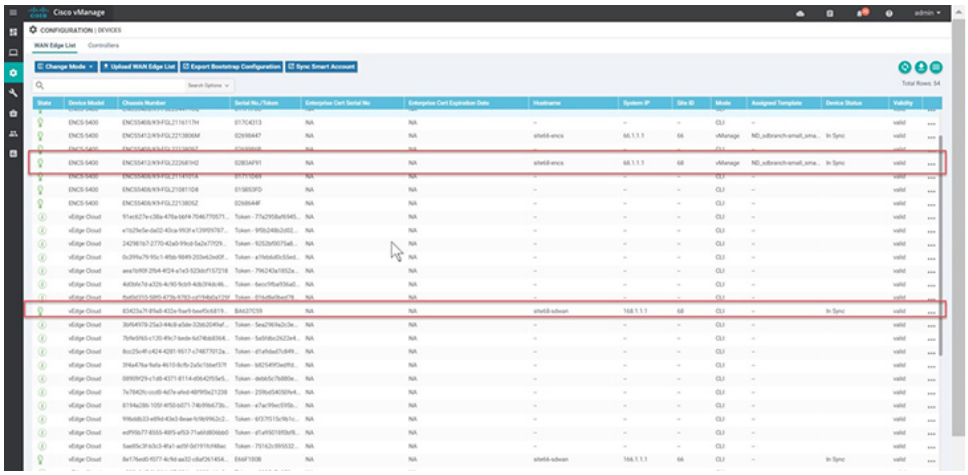
  Click **Configure Devices** to push the configuration to the devices.



- After you configure the devices, the **Network Design** screen displays the successful provision of the second device to the topology. The configuration updates are pushed to the selected devices.



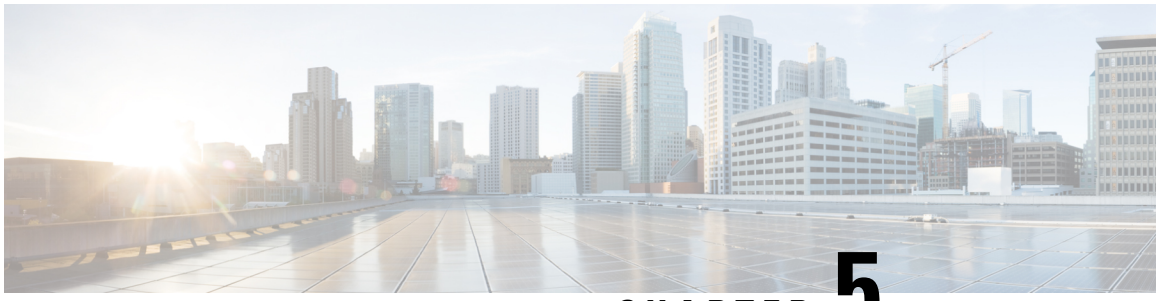
- You can check the **Validity** of the attached device in **WAN Edge List**.



- After authentication and **Attach Device** provisioning flow, Cisco SD-WAN Manager responds to NFVIS with the system IP address of the device and forces the device to reauthenticate using the shared system IP address.



- The WAN Edge device then re-initiates control connections to all the Cisco SD-WAN Control Components (Cisco SD-WAN Validator, Cisco SD-WAN Manager controllers) using the configured system IP address to join the Cisco Catalyst SD-WAN overlay network.



CHAPTER 5

Operate Cisco NFVIS SD-Branch Solution

You can monitor, troubleshoot and manage the WAN Edge devices using Cisco SD-WAN Manager. Some of the common troubleshooting and monitoring steps are covered in this section.

- Monitor and Manage the Status of Cisco Catalyst SD-WAN Control Components using Cisco SD-WAN Manager, on page 61
- Troubleshooting Device Onboarding , on page 67

Monitor and Manage the Status of Cisco Catalyst SD-WAN Control Components using Cisco SD-WAN Manager

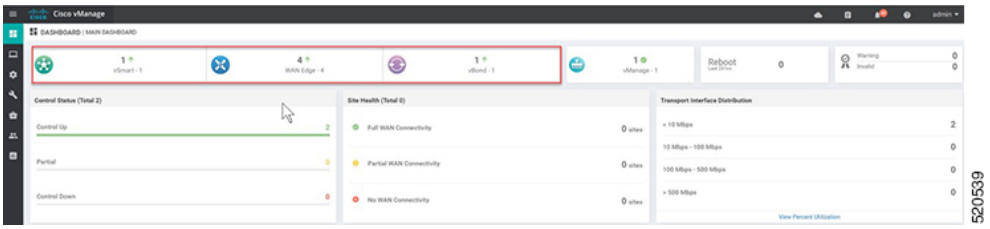
From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**, to monitor the overall health of the Cisco Catalyst SD-WAN overlay network.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard** to monitor the overall health of the Cisco Catalyst SD-WAN overlay network.

Monitor the Cisco Catalyst SD-WAN Control Components Through Device Pane

From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**, to view the **Hero Bar** with five panes, which runs across the top of the dashboard screen that displays all the control connections from Cisco SD-WAN Manager to the Cisco SD-WAN Controller, vEdge routers, and Cisco SD-WAN Validator in the overlay network. The pane also displays the status of the Cisco SD-WAN Manager in the network. Ensure that the connections for all the Cisco SD-WAN Control Components are up.

Note In Cisco vManage Release 20.6.x and earlier releases, the **Device Pane** is part of the **Dashboard** > **Main Dashboard** page.

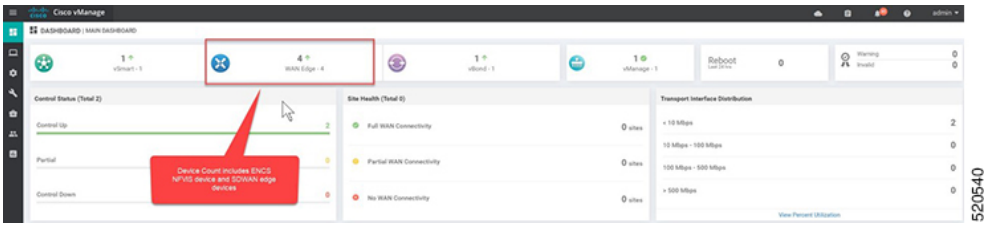


View WAN Edge Device Details and Statistics Through Device Pane

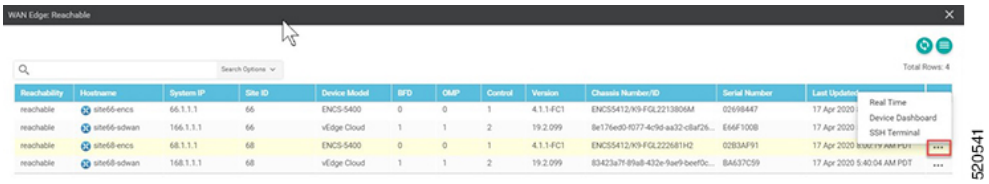
1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

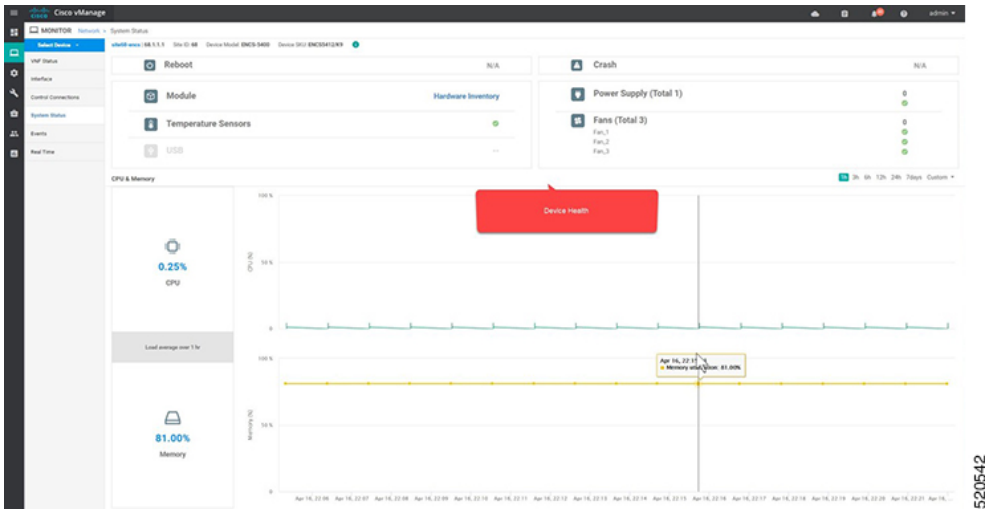
2. To view device statistics, click on the number, to display a table with detailed information for each connection.



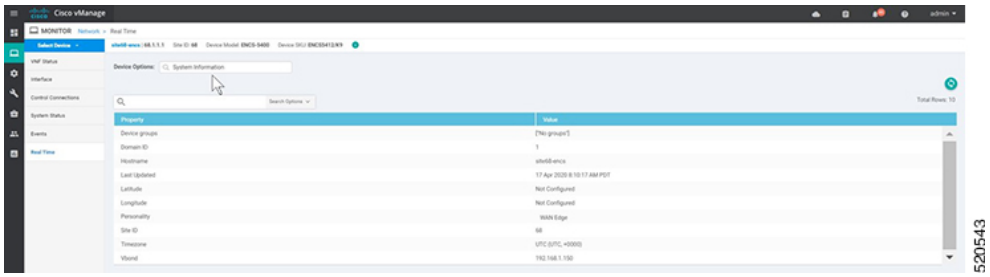
3. The table lists **System IP**, **Site ID**, **Device Model**, **Software Version** and more. For more device-specific information, click **…** at the end of each row. From here you can access **Device Dashboard**, **Real Time data**, or the **SSH Terminal**.



The **Device Dashboard** displays the **System Status** of the device, the device **Module Hardware Inventory** information, **CPU & Memory** real time statistics.

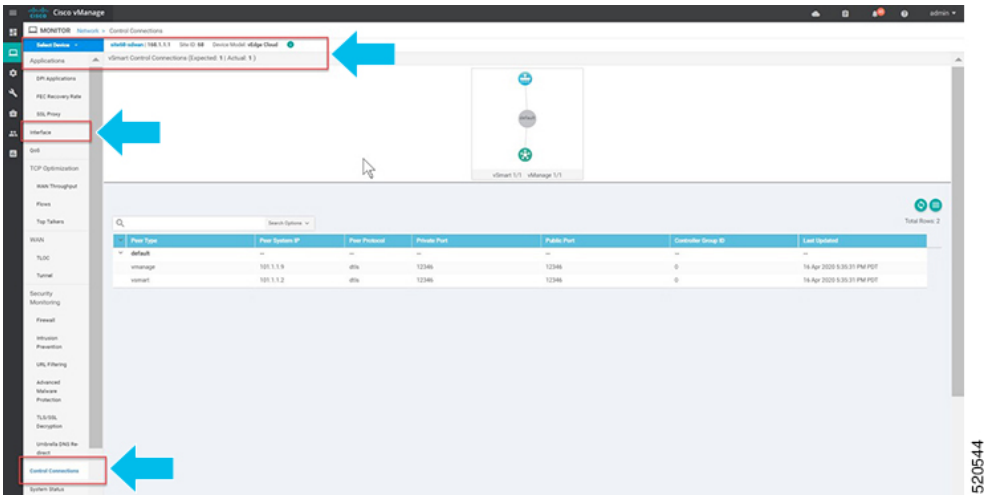


Real Time displays the basic system information of the device such as **Site ID**, **Vbond**, **Hostname**, **Latitude**, **Longitude** and more.



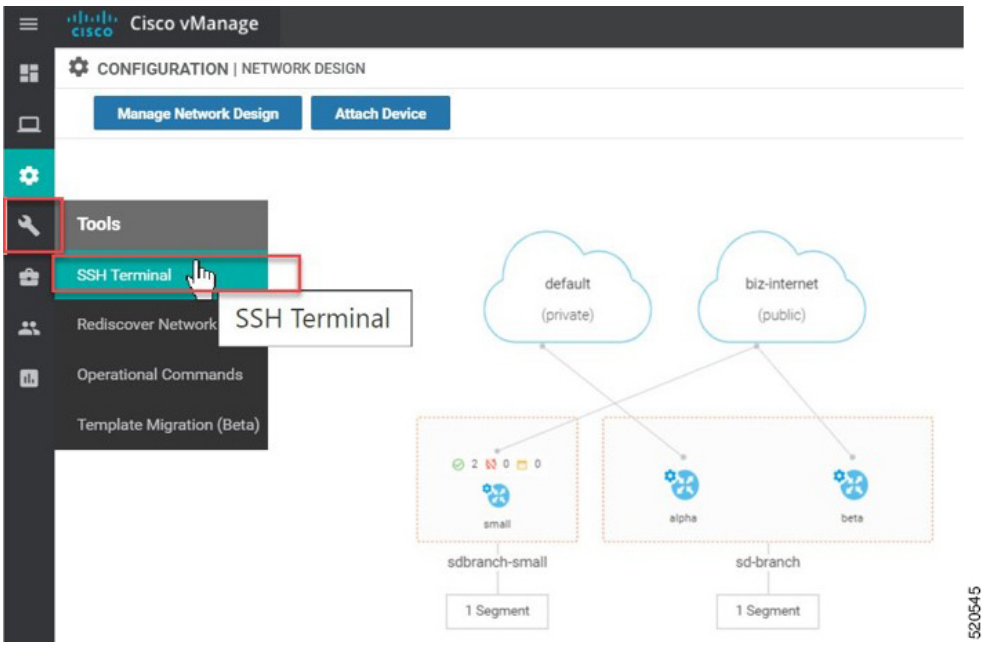
4. Additional information such as **Control Connections** over the interfaces of the WAN Edge device can be viewed from Cisco SD-WAN Manager. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.Choose the device from the list and look for device information from the left-side panel.

Note In Cisco vManage Release 20.6.x and earlier releases, device information is available in the **Monitor** > **Network** page.



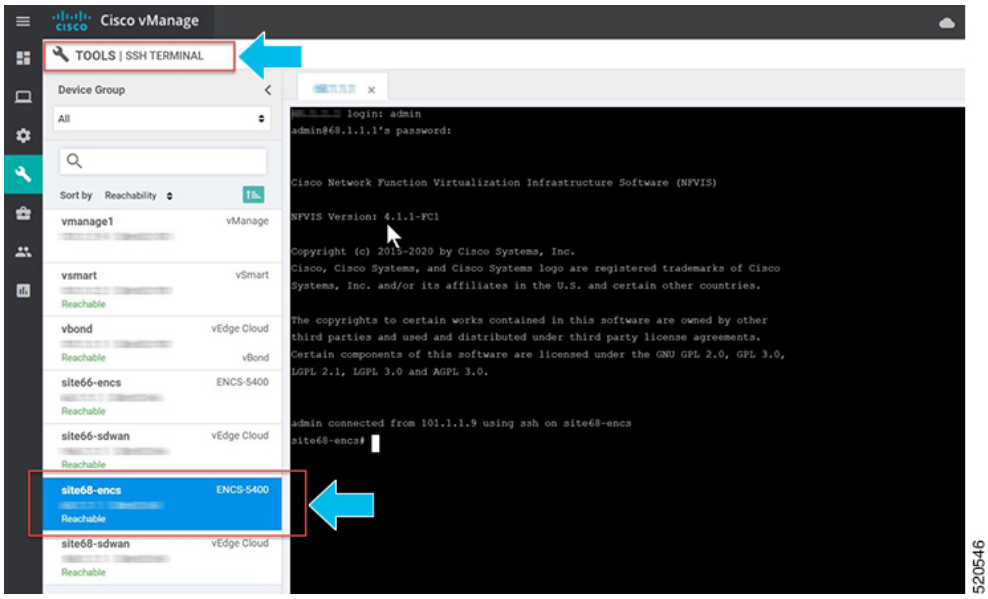
Monitor WAN Edge Device Through Cisco SD-WAN Manager SSH Server Dashboard using CLI Commands

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.



2. Choose the WAN Edge from the **Device Group**.

   To verify if the WAN Edge device has established secure control connections with the Cisco SD-WAN Control Components, enter the **show control connections** command.



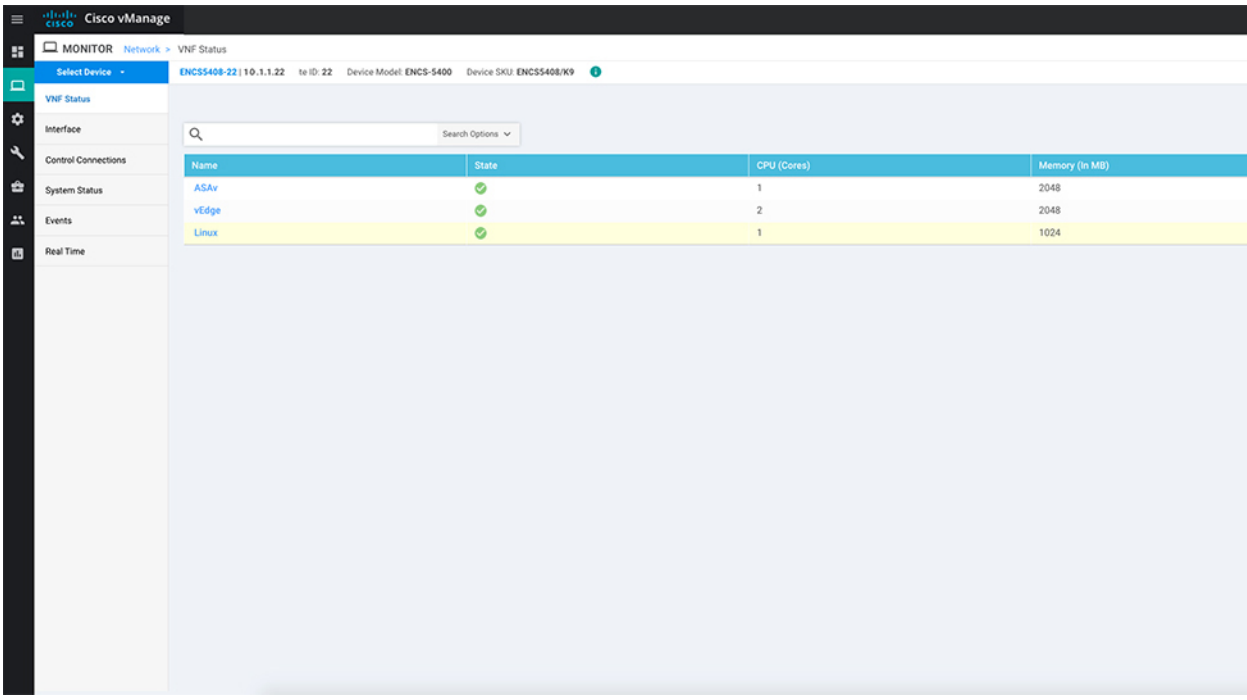
Start, Stop, and Restart WAN Edge Devices

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

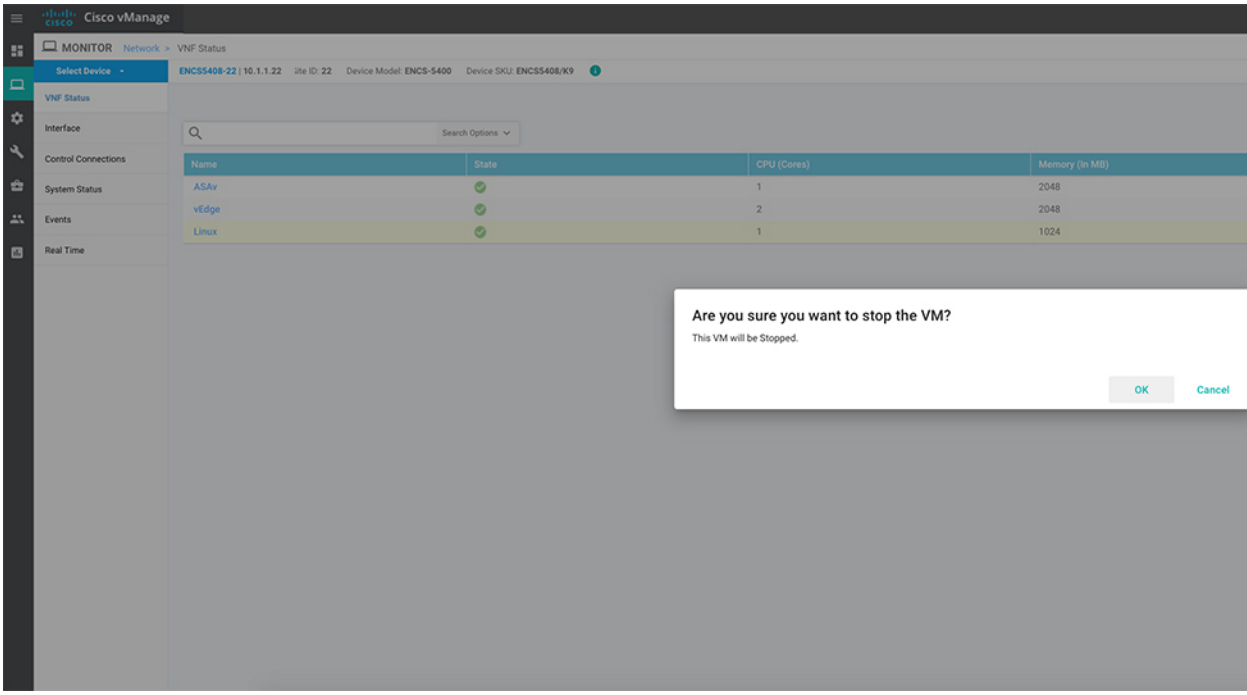
   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose the WAN Edge device.

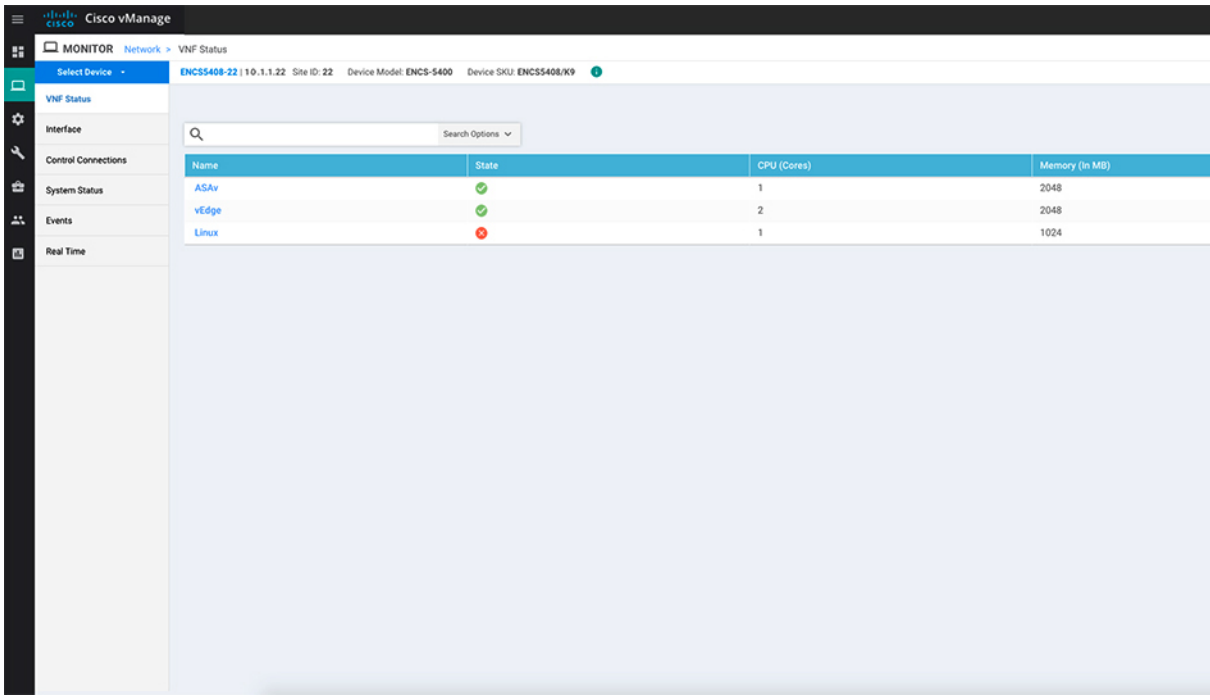
3. A list of deployed VMs for the device appears on screen. Click **…** next to the VM to start, stop or restart the device.



The following examples show how to stop a VM and the change in status of the VM.



Note You can view the VM status by choosing **Tools** > **Discover Network** from the Cisco SD-WAN Manager menu. Choose the **Device** and click **Rediscover** to sync the latest status.



You can also start, stop or restart the VM using the **vmAction vmName Linux actionType STOP/START/REBOOT** command. To view the status of the VMs, use the **show system:system deployments** or **show vm_lifecycle deployments all** command.

```
Device# vmAction vmName Linux actionType STOP

Device# show system:system deployments
NAME    ID  STATE
--------------------
ASAv    1   running
vEdge   2   running
Linux   -   shut
```

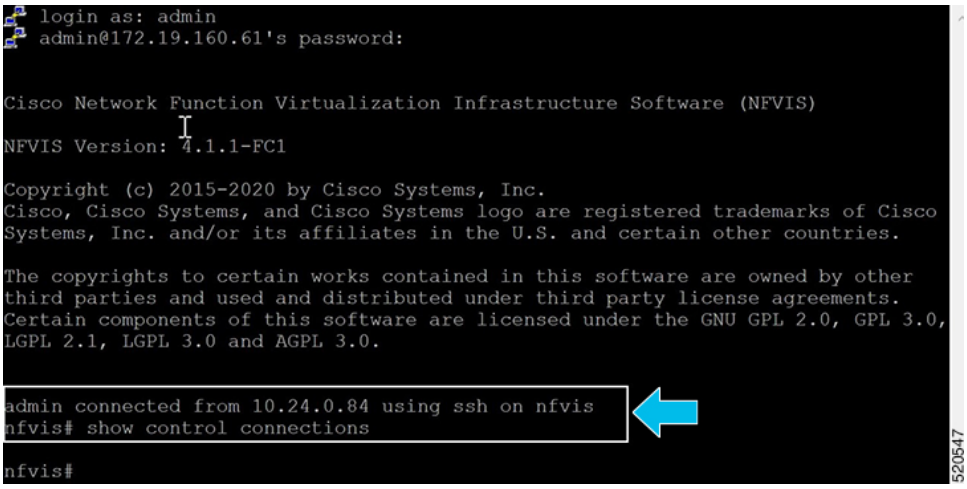
Troubleshooting Device Onboarding

This section explains some of the common troubleshooting procedures.

Diagnosing Onboarding Issues

This section covers the most common issues that could be encountered during the WAN Edge device onboarding process and recommended resolution to resolve the issues.

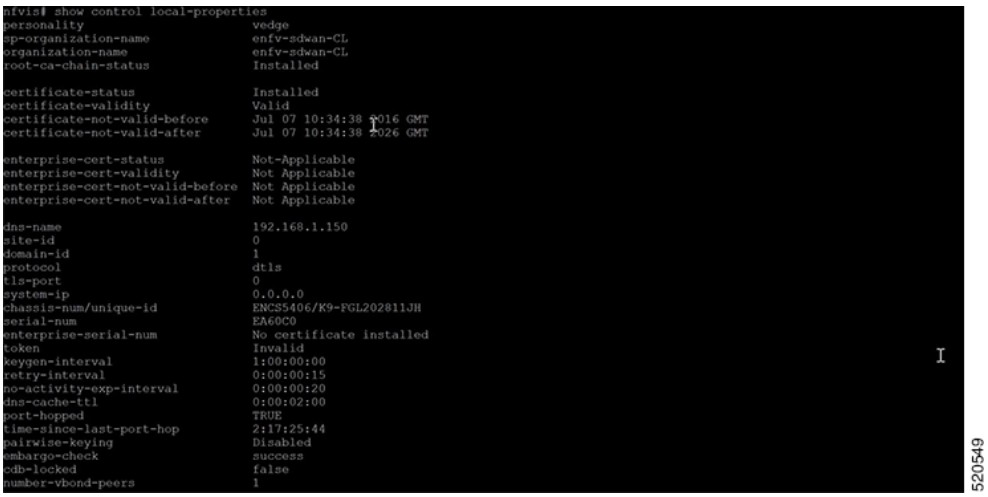
1. To verify the WAN Edge device has established a secure control connection with the Cisco SD-WAN Control Components, enter the **show control connections** command.

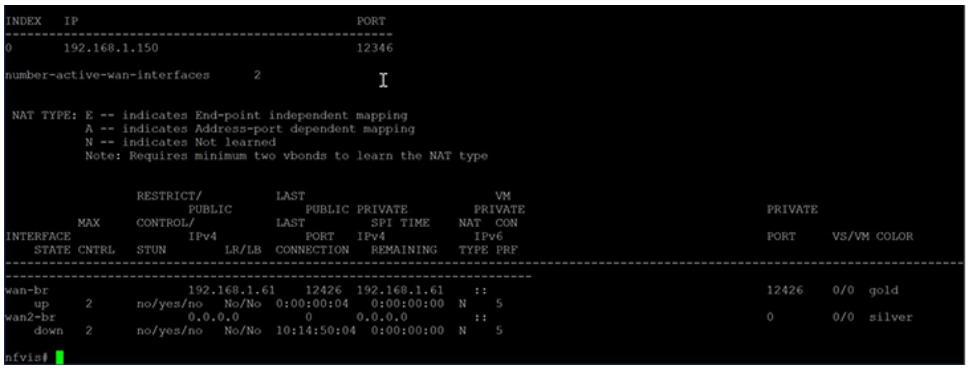


2. To verify the device properties used to authenticate WAN Edge devices, enter the **show control local-properties** command.



In the output, ensure that:

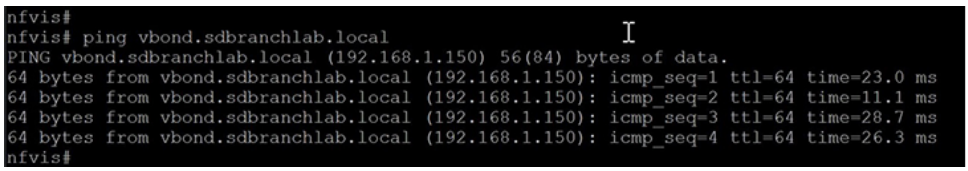




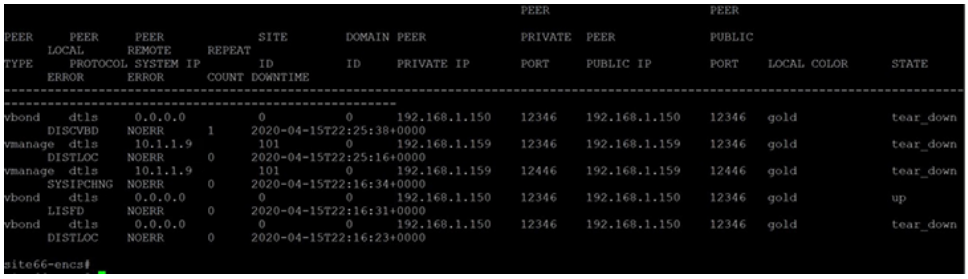
- system parameters are configured to include organization-name and site-id
- certificate-status and root-ca-chain-status are installed
- certificate-validity is Valid
- dns-name is pointing to Cisco SD-WAN Validator IP address/DNS
- system-ip is configured and chassis-num/unique-id and serial-num/token is available on the device

The above parameters must be available on the WAN Edge device to mutually authenticate with the Cisco SD-WAN Control Componentsbefore establishing the connections.

3. To verify the reachability of the Cisco SD-WAN Validator from the WAN Edge device:



4. If a WAN Edge device fails to establish connection with the Cisco SD-WAN Control Components, enter the **show control connections-history** command to view the reason for failure. View the LOCAL ERROR and REMOTE ERROR column to gather error details.



Some of the reasons for the WAN Edge device failure to establish control connections with the Cisco SD-WAN Control Components are listed below:

CRTVERFL – the error state indicates the WAN Edge device authentication is failing because of a root-ca certificate mismatch between the WAN device and the Cisco SD-WAN Control Components. Use the show certificate root-ca-cert on vEdge devices or show sdwan certificate root-ca-cert on IOS-XE Catalyst SD-WAN devices to confirm the same certificates are installed on the WAN Edge device and the Cisco SD-WAN Control Components.

CTORGNMMIS - the error state indicates the WAN Edge device authentication is failing because of a mismatch organization-name, compared with the organization-name configured on the Cisco SD-WAN Control Components. Use show sdwan control local-properties on vEdge devices and show sdwan control local-properties on IOS-XE Catalyst SD-WAN devices to confirm all the Cisco SD-WAN Control Components are configured with same organization-name across the Cisco Catalyst SD-WAN environment.

NOZTPEN – the error state indicates the onboarding vEdge device is not part of the authorized whitelist device on the ZTP server. Use show ztp entry on the on-prem ZTP server to verify the device whitelist.

NOVMCFG – the error status indicates the WAN Edge device has not been attached with a device template in Cisco SD-WAN Manager. This status is seen when onboarding the device using automated deployment options, which is the PnP or ZTP process.

VB_TMO, VM_TMO, VP_TMO, VS_TMO – the error indicates the WAN Edge device has lost reachability to the Cisco SD-WAN Control Components.

5. Use the following show commands to verify control connections on the WAN Edge device:
   - **show control connections**
   - **show control connections-history**
   - **show control connections-info**
   - **show control local-properties**
   - **show control statistics**
   - **show control summary**
   - **show control valid-vmanage-id**

Missing root ca certificate on the WAN Edge device

If the root-ca-chain certificates for the onboarding platform is missing, device authentication will fail. A failure in device authentication cannot establish control connection to the Cisco SD-WAN Control Components. The following steps shows how to install root-ca certificate on the device components:

Login into the device and view the root-ca-chain status from the **show control local-properties** command. The following example is a sample output that shows the root-ca-chain-status is in **Not-Installed** state.

```
show control local-properties
personality                     vedge
sp-organization-name            ENB-Solutions -21615
organization-name               ENB-Solutions -21615
root-ca-chain-status            Not-Installed
```

The following is an example of how to upload the root certificate in NFVIS:

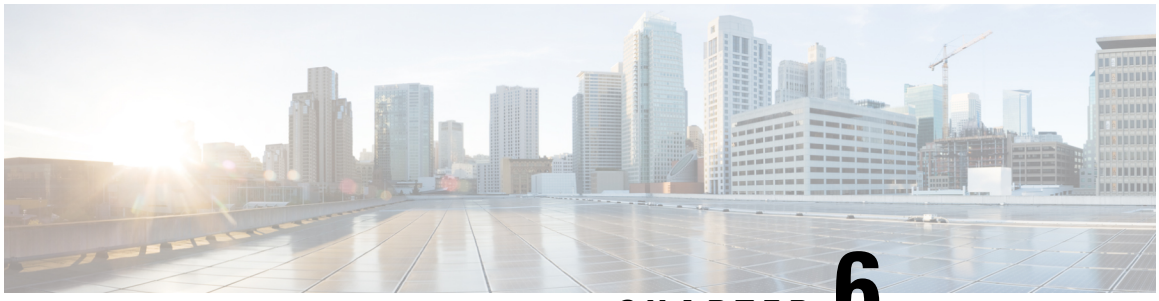
```
nfvis# request root-cert-chain install scp://admin@10.28.13.168
Uploading root-ca-cert-chain via VPN 0
Enter directory of root CA certificate file : /ws/admin-sjc/
Enter root CA certificate file name (default: root-ca.crt) : TPMRootChain.pem
Copying ... admin@10.28.13.168:/ws/admin-sjc//TPMRootChain.pem via VPN 0
Warning: Permanently added '10.28.13.168' (ECDSA) to the list of known hosts.

WARNING!!!
READ THIS BEFORE ATTEMPTING TO LOGON
```

```
This System is for the use of authorized users only. Individuals
using this computer without authority, or in excess of their
authority, are subject to having all of their activities on this
system monitored and recorded by system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored. Anyone using this system expressly
consents to such monitoring and is advised that if such
monitoring reveals possible criminal activity, system personnel
may provide the evidence of such monitoring to law enforcement
officials.

Cisco Acceptable Use Policy:
http://wwwin.cisco.com/c/cec/organizations/security-trust/infosec/policies.html

admin@10.28.13.168's password:
TPMRootChain.pem 100% 7651 1.8MB/s 00:00
Updating the root certificate chain..
Successfully installed the root certificate chain
nfvis#
```



CHAPTER 6

Support for Making Day N Changes to Profiles Attached to a Device

Table 4:

Feature Name	Release Information	Description
Support for Making Day N Changes to Profiles Attached to a Device	NFVIS 4.6.1 Cisco vManage Release 20.6.1	This feature allows you to make changes to Network Design profiles even after they are attached to a device.

- Restrictions for Day N Changes in Network Design, on page 73
- Information About Day N Changes in Network Design, on page 74
- Configure Day N Changes for Network Profiles, on page 74

Restrictions for Day N Changes in Network Design

- Update from dual WAN to single WAN is not supported.
- Control connections from NFVIS to Cisco SD-WAN Manager can only be established through one path. You can configure either wan-br or wan2-br.
- The SRIOV and OVS interfaces cannot be swapped. This is because the interface MAC addresses are changed.
- Physical ports cannot be removed from the default mapping.
- Only one physical port can be assigned to one OVS-bridge.
- Network mapping swap that results in a MAC address change is not allowed. For instance, changing the VNIC type from virtio to SRIOV is not allowed, as it causes a change in the MAC address.
- Only the CPU and Memory values can be updated in the flavor. We recommend to update the flavor through Cisco SD-WAN Manager.
- We recommend that you first apply the DPDK enabling command alone, to the Day N configuration changes, and after that is successful and the VMs are up and running, then apply the flavor configuration update. This is because, enabling DPDK requires a VM reboot, but when the VM is booting, the VM

flavor cannot be updated. Hence, we recommend that you separate out the DPDK enabling configuration changes from the rest of the configuration changes.

Information About Day N Changes in Network Design

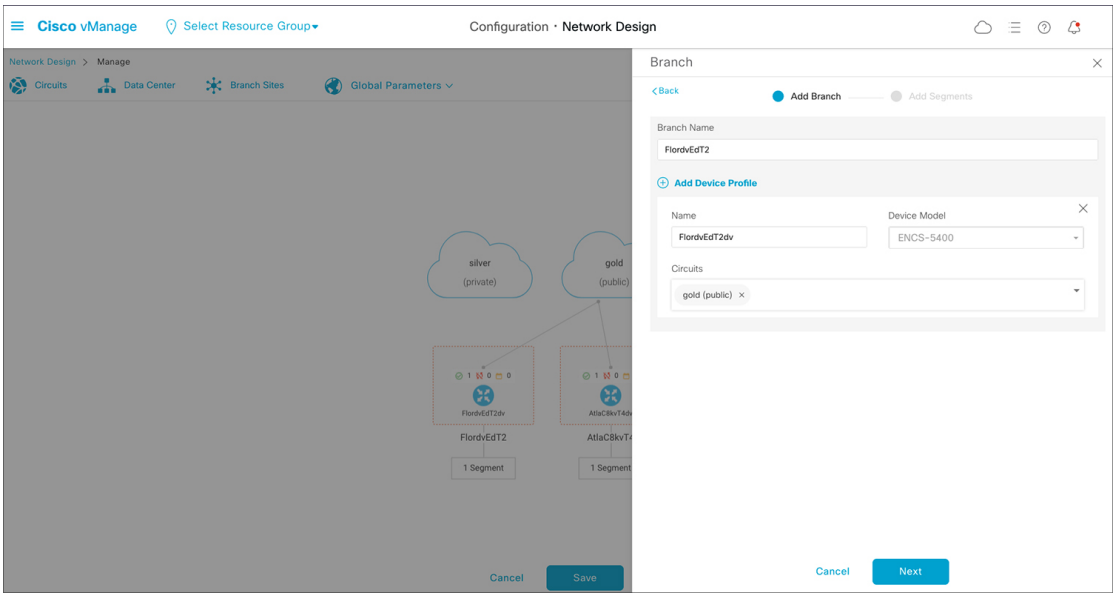
This feature enables you to make changes to the Network Design profiles even after they are attached to one or more devices. You can make changes to the global parameters, edit the services and networks settings, and make changes to the WAN and LAN settings. You can also modify the CLI configuration.

Configure Day N Changes for Network Profiles

Modify Device Name and Branch Name

To change the name of a device that is attached to the network:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Manage Network Design**.
3. Click **Branch Sites**.
4. Find the device that you want to edit and click the edit symbol.
5. In the **Branch Name** field, enter a name if you want to change the branch name.



6. Click **Next**.
7. If a segment name is not chosen, click the **Segment Name** drop down list and choose a segment name.
8. Click **Add**, and then click **Finish**.

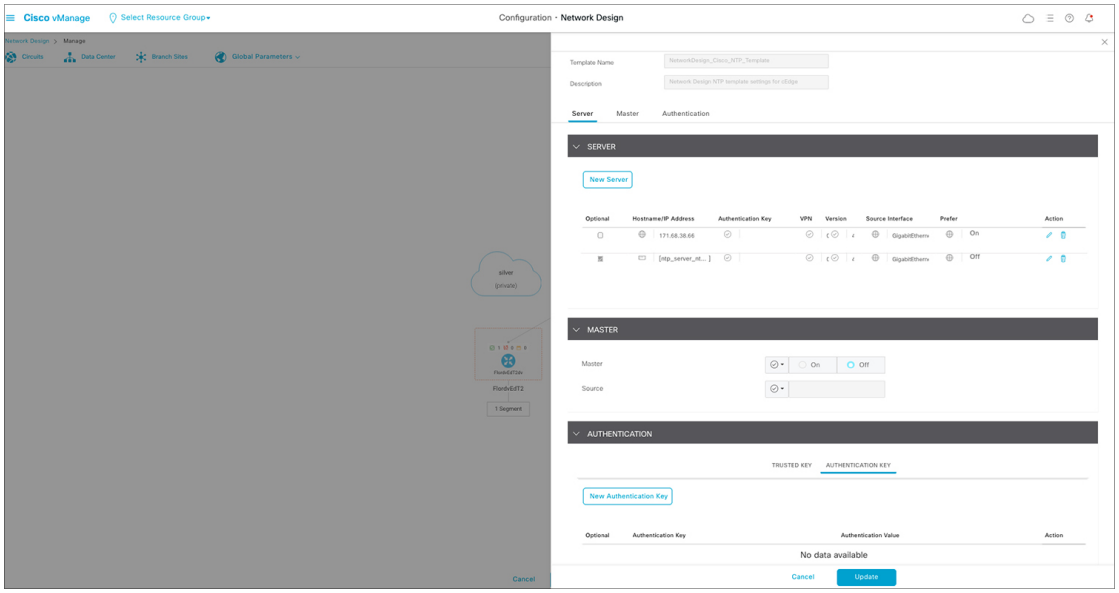
9. Click **Save**. In the dialog box that appears, click **Proceed**.

Modify Global Parameters

Changes in Global Parameters affect all the devices in the network globally. Starting from NFVIS 4.6 release global parameters can be modified even with the devices attached to the network.

To make Day N changes to the global parameters:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Manage Network Design**.
3. Click **Global Parameters**.
4. From the drop-down list, choose the Cisco IOS XE Catalyst SD-WAN device parameter that you want to modify. You can make Day N changes to these parameters—Cisco NTP, Cisco AAA and Cisco Logging.
5. To add a new server to the profile, click **New Server**, and to add a new authentication key, click **New Authentication Key**. You can modify the existing server and authentication key parameters.
6. You can also modify the **Master** and **Source** parameters.



7. Click **Update**.

Note To configure any NFVIS device changes, use the Cisco IOS XE Catalyst SD-WAN device parameters.

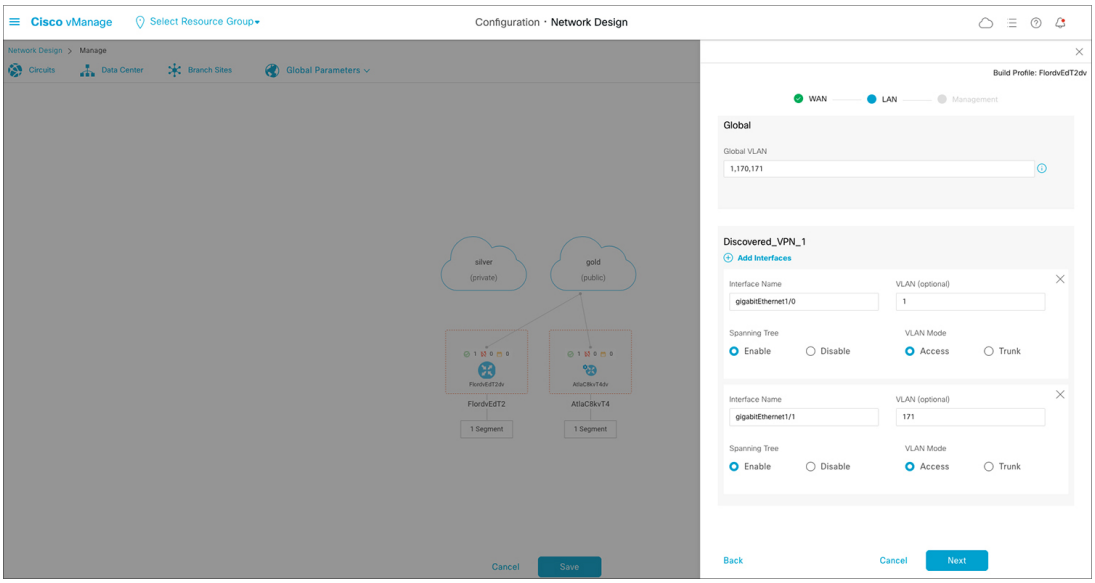
Modify Device Profiles

To make Day N changes to the device profiles:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Manage Network Design**.
3. Click the device on which you want to make the Day N change.
4. Choose **Edit Profile**.
5. Click the edit symbol to make changes to the parameters.
6. Under **WAN**, set the interface IP to either **DHCP** or **Static**.

Note If you choose the interface IP as static, you need to configure the IP default gateway using the CLI Add-on Feature template.

7. Click **Next**.
8. Under **LAN**, enter the **Global VLAN** value.
9. To add new interfaces, click **Add Interfaces**.
10. To modify settings for the spanning tree, VLAN (VLAN ID), and VLAN mode for the new interface, use the **Spanning Tree**, **VLAN (optional)**, and **VLAN Mode** fields respectively. You can also make these changes for existing interfaces.



11. Click **Next**.
12. Under **Management**, you can set the interface IP to either **DHCP** or **Static** based on your selection in the WAN profile. If you set the interface IP as **DHCP** in the WAN profile, then you need to choose **Static** for the management profile and vice versa.

Note The interface name should not be modified for any of the profiles. The default interface names are:

- For the WAN profile- GE0-0 or GE0-1
- For the LAN profile- gigabitEthernet1/0 through gigabitEthernet1/7
- For the Management profile- mgmt

13. Click **Done**.

Migrating from Insecure to Secure Configuration, Release 26.1.1

Starting from Cisco Catalyst SD-WAN Manager Release 26.1.1.1, Cisco introduces the **system mode insecure** CLI command. This command is required if your configuration contains insecure features (such as SNMPv1/v2, HTTP, or weak ciphers). To move a device to a fully secure state, you must correct the insecure configurations and then transition the device mode from "Insecure" to "Secure." For more information, see Resilient Infrastructure.

Due to system limitations, this transition cannot be completed in a single configuration push from Cisco SD-WAN Manager. It requires a two-step configuration push process.

Prerequisites

- The device must be running NFVIS and Cisco Catalyst SD-WAN Manager Release 26.1.1.1.
- You must have an existing Network Design for the branch site.
- A **CLI Add-On Feature Template** must be available to manage the **system mode insecure** command.

Secure the Features (First Configuration Push)

In this step, you update all feature configurations to secure standards to allow the transition.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design**.
2. Click **Manage Network Design**.
3. Hover your mouse over the image representation of the branch device and choose **Add CLI Configuration**
4. In the CLI Add-On template, add the **system mode insecure** command.
5. Click **Attach Devices** and select the device on the network topology.
6. Choose the specific device from the **Available Devices** list and move it to the **Selected Devices** list using the arrow.
7. Click **Attach**.
8. Click **Config Preview** to verify that both the **system mode insecure** command and all your new secure feature configuration are included.
9. Click **Configure Devices** to push the configuration.

   The configuration updates are pushed to the device. The device features are now secure. However, the device reports the system mode status as `system mode status Insecure`.

Use the **show system mode** command to verify the current system status. To transition the device to a secure status, you must complete the second configuration push to remove the **system mode insecure** command. For more information, see the **Finalize Secure Mode (Second Configuration Push)** section.

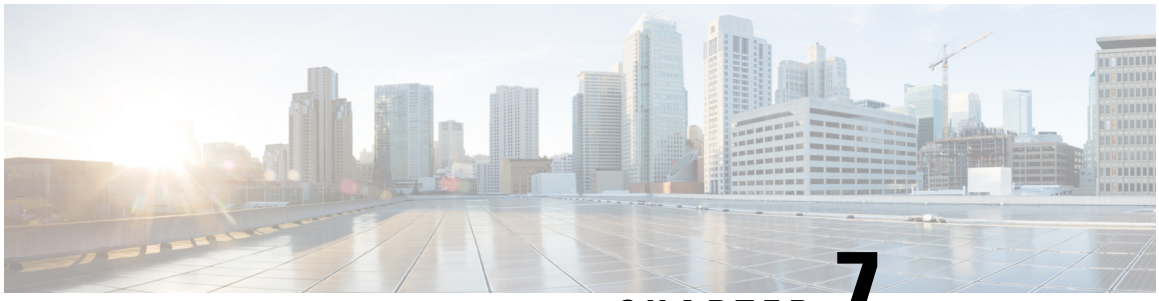
Finalize Secure Mode (Second Configuration Push)

To make the device status as Secure, perform the following steps as part of the second configuration push from Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Design** > **Manage Network Design**.
2. Hover your mouse over the image representation of the branch device and choose **Edit CLI Configuration**
3. Remove the **system mode insecure** command from the template. Alternatively, you may remove the CLI template entirely if it only contains the **system mode insecure** command.
4. Click **Attach Devices** and select the device on the network topology.
5. Choose the specific device from the **Available Devices** list and move it to the **Selected Devices** list using the arrow.
6. Click **Attach**.
7. Click **Config Preview** to that the **system mode insecure** command is no longer present in the configuration.
8. Click **Configure Devices** to push the updated configuration.

   The configuration updates are pushed to the device. This removes the **system mode insecure** command from the device.

   Use the **show system mode** command to verify the current system status. Confirm that the output displays `system mode status secure`. The status will only transition to secure after the second configuration push has successfully removed the **system mode insecure** command.



CHAPTER 7

Upgrade Cisco NFVIS Software

- Cisco NFVIS Software Upgrade Workflow, on page 79
- Support Matrix For Upgrading Cisco NFVIS, on page 80
- Information about Cisco NFVIS Software Upgrade Workflow, on page 81
- Prerequisites for Using the Cisco NFVIS Software Upgrade Workflow, on page 81
- Restrictions for Cisco NFVIS Software Upgrade Workflow, on page 82
- Benefits of NFVIS Software Upgrade Workflow, on page 82
- Upgrade Cisco NFVIS Using the Software Upgrade Workflow, on page 82
- Schedule Software Upgrade Workflow, on page 84
- Cisco NFVIS Software Upgrade Using the CLI, on page 85
- Verify Software Upgrade Using CLI, on page 87

Cisco NFVIS Software Upgrade Workflow

Table 5: Feature History

Feature Name	Release Information	Description
Cisco NFVIS Software Upgrade Workflow	Cisco NFVIS Release 4.8	This feature introduces a guided workflow that enables you to upgrade Cisco NFVIS using the .iso file. You can skip a release and upgrade to two releases after.
Schedule the Software Upgrade Workflow	Cisco NFVIS Release 4.9.1	This feature introduces a scheduler in the software upgrade workflow using which you can schedule the upgrade of the software images on Cisco NFVIS at your convenience.

Support 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.
- Since NFVIS version 4.9, the SD-Branch NFVIS ISO upgrade support matrix is the same as that for standalone upgrades. For more information, see the Upgrade Matrix for Upgrading Cisco NFVIS.

Running Version	Supported Upgrade Version	Supported Upgrad
4.13.1	4.14.1 (future release)	iso
4.12.1	4.13.1	iso
4.11.1	4.12.1	iso
4.10.1	4.11.1	iso
4.9.3	4.11.1	iso
4.9.2	4.11.1	iso
	4.10.1	iso
	4.9.3	iso
4.9.1	4.11.1	iso
	4.10.1	iso
	4.9.3	iso
	4.9.2	iso
4.8.1	4.9.3	iso
	4.9.2	iso
	4.9.1	iso
4.7.1	4.8.1	nfvispkg
4.6.3	4.7.1	nfvispkg
4.6.2	4.7.1	nfvispkg
	4.6.3	nfvispkg
4.6.1	4.7.1	nfvispkg
	4.6.3	nfvispkg
	4.6.2	nfvispkg
4.5.1	4.6.1	nfvispkg
4.4.2	4.5.1	nfvispkg

4.4.1	4.5.1	nfvispkg
	4.4.2	nfvispkg

Information about Cisco NFVIS Software Upgrade Workflow

Using this workflow, you can download and upgrade .iso software images on Cisco NFVIS with an option to schedule the upgrade process at your convenience. The workflow also shows you the status of the software upgrade. This workflow provides you with two options to perform the software upgrade and they are: **Download and Upgrade** and **Dowload Only**. You can also skip a software version and upgrade to two release after, using an .iso file.

Note The Cisco NFVIS upgrade image (.nfvispkg) can be hosted on either the Cisco SD-WAN Manager local repository or a remote server.

Prerequisites for Using the Cisco NFVIS Software Upgrade Workflow

- The remote server, either FTP or HTTP, must be set to host the Cisco NFVIS upgrade (.nfvispkg and .iso) image.

Note Performing a software upgrade using the .nfvispkg upgrade image is supported only till Cisco NFVIS Release 4.9. In the upcoming releases, only .iso image will be published for both fresh and existing upgrades of Cisco NFVIS.

- The Cisco NFVIS devices need to run Cisco NFVIS Release 4.8 for using the Software Upgrade Workflow and run Cisco NFVIS Release 4.9 for using the scheduler option.

Timeout settings

Set the download timeout and activate timeout as follows:

1. In Cisco SD-WAN Manager, click **Administration** > **Settings** > **Software Install Timeout**.
2. Click **Edit** and configure the following parameters:
   - Download timeout: 120 minutes
   - Activate timeout: 180 minutes

Note The download timeout setting may vary depending on the actual network bandwidth and quality.

Restrictions for Cisco NFVIS Software Upgrade Workflow

- The .iso upgrade image cannot be hosted on the Cisco SD-WAN Manager repository. It must be hosted on the remote server, either as FTP or HTTP file.

Benefits of NFVIS Software Upgrade Workflow

- The software upgrade workflow helps you prevent various device software upgrade failures by displaying device upgrade status. For example, if the upgrade process fails at any particular stage, the workflow flags it as **failed**.
- With this workflow, you can choose to download and upgrade the NFVIS devices with the new software image.

Benefits of Schedule a Software Upgrade Workflow

The software upgrade workflow scheduler helps you prevent various device downtime occurring due to the software upgrade process. For example, you can schedule the software upgrade workflow during your non-business hours which won't affect your employees or customers.

Upgrade Cisco NFVIS Using the Software Upgrade Workflow

Add the Remote Server



Note Starting from Cisco NFVIS Release 4.9, You can also add a remote server using **Create New** option in the **Select remote server** drop-down in the Software Upgrade Workflow.

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** .
2. Click **Add Remote Server**.
3. Enter the **Server Name** and the **Server IP or DNS Name**.
4. From the **Select Protocol** drop-down list, choose either the FTP or HTTP protocol.
5. Enter the **Port** number.
6. (Optional) Enter your **User ID** and **Password**.
7. (Optional) Enter the **Image Location Prefix**.
8. Enter **VPN** as 0.
9. Click **Add**.

Note If the VPN field is left blank or empty, the NFVIS upgrade will fail with an unknown error. Ensure the VPN field is populated.

Add the Upgrade Software Image

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** .
2. Click **Software Images**.
3. From the **Add New Software** drop-down list, choose **Remote Server (preferred)**.
4. From the **Remote Server Name** drop-down list, choose the server.
5. Enter the **Image Filename**.
6. Click **Save**.

Note While downloading the upgrade image, the FTP/HTTP path string including the username, password and file name, can only contain these characters: [a-zA-Z0-9_/ ?*.:@+=%-]

Access the NFVIS Software Upgrade Workflow

Before You Begin

Note Only one software upgrade workflow is executed at a time. If you schedule a workflow while another work flow is in progress, the scheduled workflow is only executed after the in-progress workflow is completed.

To check if there is an in-progress software upgrade workflow:

From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon. Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

Access the Software Upgrade Workflow

1. In the Cisco SD-WAN Manager Menu, click **Workflows** > **Workflow Library**

   or

   Starting from Cisco vManage Release 20.9.1, click **Workflows** > **Software Upgrade.**.

Note In the Cisco vManage Release 20.8.1, the **Workflow Library** is titled **Launch Workflows**.

2. Start a new software upgrade workflow: **Workflow Library** > **Software Upgrade**.

OR

Alternatively, resume an in-progress software upgrade workflow: **In-progress** > **Software Upgrade**.

3. Follow the on-screen instructions to schedule a new software upgrade workflow.



Note Click **Exit** to exit from an in-progress software upgrade workflow. You can resume the in-progress workflow at your convenience.

Verify the Status of the Software Upgrade Workflow

To check the software upgrade workflow status:

1. From the Cisco SD-WAN Manager toolbar, click the **Task-list** icon.

   Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.

2. Click the + icon to view the details of a task.

   Cisco SD-WAN Manager opens a pane displaying the status of the task and details of the device on which the task was performed.

Delete Downloaded Software Image

To delete downloaded software images from Cisco NFVIS:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**.
3. Click **Delete Downloaded Images**
4. In the **Delete Downloaded Images** dialogue box, choose the appropriate image or images to delete.
5. Click **Delete**.

Schedule Software Upgrade Workflow

Introduced in the Cisco vManage 20.9.1, you can schedule the software upgrade workflow at your convenience and avoid any downtime due to the software upgrade process. A scheduler enables you to schedule the upgrade workflow for a later time. You can enter the **Start Date**, **Start time**,and **Select Timezone**.

Schedule Software Upgrade Workflow

Use the following steps to schedule a software upgrade workflow:

1. In the Cisco SD-WAN Manager Menu, click **Workflows** > **Workflow Library**

   OR

   Starting from Cisco vManage Release 20.9.1, click **Workflows** > **Popular Workflows** > **Software Upgrade.**.

2. Start a new software upgrade workflow: **Workflow Library** > **Software Upgrade**.

   OR

   Alternatively, resume an in-progress software upgrade workflow: **In-progress** > **Software Upgrade**.

3. In the **Scheduler** section, choose **Later**.



Note Use the **Now** option to perform the software upgrade for the selected devices immediately.

4. Choose the **Start Date**, **Start Time**, and **Select Timezone**.



Note Ensure that the **Start time** is at least two minutes greater than the current time of schedule.

5. Click **Next**.
6. The software upgrade workflow is scheduled.

Cisco NFVIS Software Upgrade Using the CLI

Download the Software Image

Minimum supported releases: Cisco NFVIS Release 4.9, Cisco vManage Release 20.9.1

To download the software image from the remote server, use the following steps:

1. Request to download the software image from the remote server.

   ```
   nfvis# request software download
   ```

2. Enter the file path of the software image.

   ```
   nfvis# request software download <ip-address>/image/<image-name>
   ```

Example:

```
nfvis# request software download
nfvis# request software download
http://172.25.221.219/image/Cisco_NFVIS-4.9.1-72-20220804_032636.iso
```

Download and Activate the Software Image

Minimum supported releases: Cisco NFVIS Release 4.9, Cisco vManage Release 20.9.1

To download and activate the software image from the remote server, use the following steps:

1. Request to download the software image from the remote server.

   ```
   nfvis# request software download <ip-address>/image/<image-name>
   ```

2. Install the software image.

   ```
   nfvis# request software install <image-name>
   ```

3. Activate the software image.

```
nfvis# request software activate <image-name>
```

4. The node reboots with the activated version.

Example:

```
nfvis# request software download
http://172.25.221.219/image/Cisco_NFVIS-4.9.1-72-20220804_032636.iso
nfvis# request software install Cisco_NFVIS-4.9.1-72-20220804_032636.iso
nfvis# request software activate 4.9.1-72-20220804_032636
```

Remove the Software Image

Minimum supported releases: Cisco NFVIS Release 4.9, Cisco vManage Release 20.9.1

To remove the downloaded image, use the following command:

Request to remove the software image from the remote server.

```
nfvis# request software delete-image <image-name>
```

Example:

```
nfvis# request software delete-image Cisco_NFVIS-4.9.1-72-20220804_032636.iso
```

Install the Software Image

Minimum supported releases: Cisco NFVIS Release 4.8, Cisco vManage Release 20.8.1

To install the downloaded image, use the following command:

Request to install the software image from the remote server.

```
nfvis# request software image install <image-name>
```

Example:

```
nfvis# request software image install Cisco_NFVIS-4.8.1-FC4.iso
```

Activate the Software Image

Minimum supported releases: Cisco NFVIS Release 4.8, Cisco vManage Release 20.8.1

To install the downloaded image, use the following command:

Request to activate the software image from the remote server.

```
nfvis# request software activate <image-name>
```

Example:

```
nfvis# request software activate 4.8.1-FC4
```

Install and Activate the Software Image

Minimum supported releases: Cisco NFVIS Release 4.8, Cisco vManage Release 20.8.1

To install and activate the downloaded image, use the following command:

Request to download and activate the software image from the remote server.

```
nfvis# request software image install <image-name> reboot
```

Example:

```
nfvis# request software image install Cisco_NFVIS-4.8.1-FC4.iso reboot
```

Download, Install And Activate the Software Image

Minimum supported releases: Cisco NFVIS Release 4.8, Cisco vManage Release 20.8.1

To download, install and activate the software image from the remote server, use the following command:

Request to download, install and activate the software image from the remote server.

```
nfvis# request software install http://<ip-adress>/path/<image-name> reboot
```

Example:

```
nfvis# request software install http:/10.0.0.1/path/Cisco_NFVIS-4.8.1-FC4.iso reboot
```

Remove the Software Image

Minimum supported releases: Cisco NFVIS Release 4.8, Cisco vManage Release 20.8.1

To remove the downloaded image, use the following command:

Request to remove the software image from the remote server.

```
nfvis# request software image remove <image-name>
```

Example:

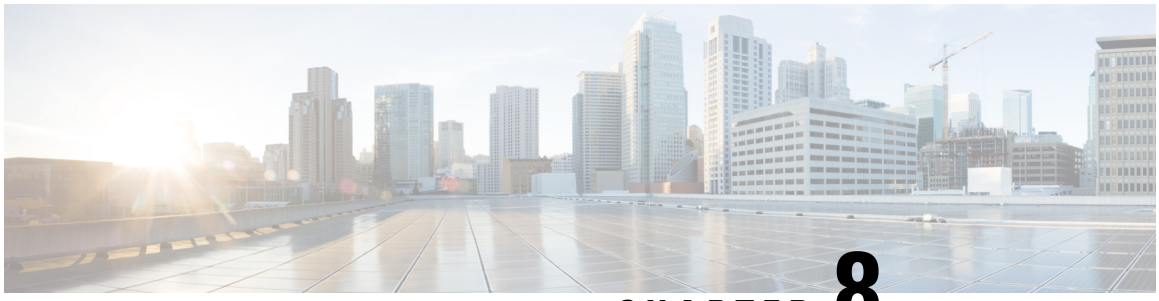
```
nfvis# request software image remove Cisco_NFVIS-4.8.1-FC4.iso
```

Verify Software Upgrade Using CLI

The following is a sample output from the **show software** command:

```
nfvis# show software
software 4.9.1-59
active    true
default   true
timestamp 2022-07-23T02:12:15-00:00
software 4.9.1-72-20220804_032636
active   false
default  false
previous false
```

In this output, **software 4.9.1-59** indicates that your device is upgraded with the latest software.



CHAPTER 8

Cisco SD-Branch ThousandEyes Support

Table 6: Feature History

Feature Name	Release Information	Description
Cisco NFVIS ThousandEyes Container Support	Cisco SD-Branch Release 20.15.2	This feature adds support to use Cisco ThousandEyes as a container within Cisco SD-WAN Manager. This feature also adds support for ThousandEyes Docker Container Upgrade using the NFVIS VM Lifecycle Workflow. It also introduces support for using new NFVIS-specific Docker images provided by ThousandEyes.

- Information About Cisco SD-Branch ThousandEyes Support, on page 89
- Benefits of Cisco SD-Branch ThousandEyes Support, on page 89
- Prerequisites for Cisco SD-Branch ThousandEyes Support, on page 90
- Restrictions for Cisco SD-Branch ThousandEyes Support, on page 90
- Deploy ThousandEyes, on page 90
- Monitor Cisco SD-Branch ThousandEyes Support, on page 92

Information About Cisco SD-Branch ThousandEyes Support

Cisco SD-WAN Manager supports a preintegrated solution that allows deploying ThousandEyes Enterprise Agent as a container on Cisco NFVIS devices. Experience ThousandEyes network monitoring and testing capabilities directly on your Cisco SD-Branch network infrastructure. The feature provides visibility into the performance of the underlying network infrastructure.

Benefits of Cisco SD-Branch ThousandEyes Support

- Gain complete visibility into your network performance, including network infrastructure, cloud providers, WAN links, and internal data center networks within Cisco NFVIS.

- Reduce Mean Time To Repair (MTTR) for network issues, improve network reliability, and optimize application performance.

Prerequisites for Cisco SD-Branch ThousandEyes Support

- Ensure that the minimum software version for Cisco NFVIS devices is Cisco NFVIS Release 4.15.2 and your Cisco SD-WAN Manager is running Cisco Catalyst SD-WAN Manager Release 20.15.2.
- You require a minimum of two CPU cores, memory of 2048 MB, and a disk size of 8192 MB to enable a ThousandEyes container.

Restrictions for Cisco SD-Branch ThousandEyes Support

- Add **`TEAGENT_ACCOUNT_TOKEN`** and **`TEAGENT_INET`** to the bootstrap configuration file to deploy the ThousandEyes container.
- Monitoring charts aren't supported for Cisco ThousandEyes container.

Deploy ThousandEyes

Deploy ThousandEyes Container in Cisco SD-WAN Manager Using a CLI Add-On Profile

Create a CLI Add-On Profile

For NFVIS devices managed by Cisco SD-WAN Manager, follow these steps to deploy the ThousandEyes container:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Adjacent to a configuration group, click **…** and choose **Edit**.
3. In the **Feature Profiles - Unconfigured** area, locate **CLI Profile**.



Note If the configuration group already has a CLI profile configured, this option will not appear.

4. On the **CLI Profile** card, click **Start Configuration**.

   An **Edit Config Feature** pane opens.
5. Enter a name and, optionally, a description for a new CLI add-on profile.
6. Enter configuration commands in the **CLI Configuration** area or click **Import Config File** to import a configuration.

   Use the following sample CLI configuration for image registration and deployment:

```
vm_lifecycle images image thousandeyes-enterprise-agent-0.33.0
 src
```

```
https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-0.33.0-nfvis.docker

 locator vim_id container
 properties property vnf_type
  value THOUSANDEYES
 !
!

vm_lifecycle flavors flavor thousandeyes-flavor vcpus 2 memory_mb 1024 root_disk_mb 20480
!
vm_lifecycle tenants tenant admin
 deployments deployment THOUSANDEYES-DEMO
  vm_group THOUSANDEYES-DEMO
   locator vim_id container
   image              thousandeyes-enterprise-agent-0.33.0
   flavor             thousandeyes-flavor
   vim_vm_name        THOUSANDEYES-DEMO
   bootup_time        -1
   config_data configuration bootstrap_config
    data            "{ \"env_variables\" : { \"TEAGENT_ACCOUNT_TOKEN\" :
\"${TEAGENT_ACCOUNT_TOKEN}\", \"TEAGENT_INET\" : \"${TEAGENT_INET}\"} }"
    template_engine VELOCITY
    variable TEAGENT_ACCOUNT_TOKEN
     val [ 53rettywagbuouhw06hu65767rtyuyyui ]
    !
    variable TEAGENT_INET
     val [ 4 ]
   !   !
 !
```

7. To convert a configuration value to a variable, select the value and click **Create Variable**.

   Enter the variable name, and click **Create Variable**. You can also type a variable name directly, in the format {{variable-name}}. Example: {{hostname}}

   Variables enable you to enter values for the variables individually for each device when you deploy a configuration group to devices. During the deployment, you can enter values manually or using a CSV file.

8. To encrypt a plain-text password using type 6 encryption, select the password and click **Encrypt Type 6**.

   In the example below, you can select the password, ABCD, and click **Encrypt Type 6** to encrypt the password.

   ```
   server-private 10.0.0.1 key 0 ABCD
   ```

   For more information about type 6 encryption, see Type 6 passwords.



Note Encrypt only passwords. Encrypting a CLI command may cause a failure when deploying the configuration group to devices.

9. Click **Save** and proceed to associate and deploy the device to the appropriate Configuration Group.

Upgrade ThousandEyes Agent Container in Cisco SD-WAN Manager Using a CLI Add-On Profile

Edit the Existing Add-On CLI Profile:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

2. In the CLI add-on profile, adjacent to the config feature, click **…** and choose **Edit Feature**.
3. Modify the deployment payload to replace the existing image path with the path of the new version of the ThousandEyes image in the **CLI Configuration** area or click **Import Config File** to import a configuration.

   Use the following sample CLI configuration for updating the image version:

   ```
   vm_lifecycle tenants tenant admin
    deployments deployment THOUSANDEYES-DEMO
     vm_group THOUSANDEYES-DEMO
      locator vim_id container
      image
   https://downloads.stg.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-0.34.0-nfvis.docker
   ```

4. To convert a configuration value to a variable, select the value and click **Create Variable**.

   Enter the variable name, and click **Create Variable**. You can also type a variable name directly, in the format {{variable-name}}. Example: {{hostname}}

   Variables enable you to enter values for the variables individually for each device when you deploy a configuration group to devices. During the deployment, you can enter values manually or using a CSV file.
5. To encrypt a plain-text password using type 6 encryption, select the password and click **Encrypt Type 6**.

   In the example below, you can select the password, ABCD, and click **Encrypt Type 6** to encrypt the password.

   ```
   server-private 10.0.0.1 key 0 ABCD
   ```

   For more information about type 6 encryption, see Type 6 passwords.



Note Encrypt only passwords. Encrypting a CLI command may cause a failure when deploying the configuration group to devices.

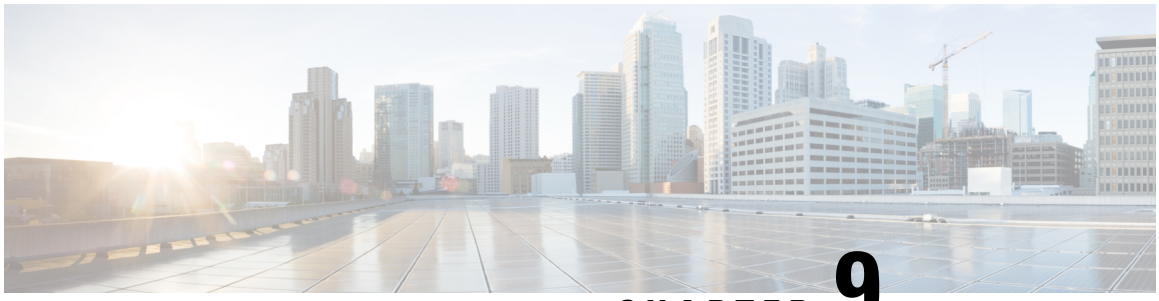
6. Click **Save** to complete the update process.

Monitor Cisco SD-Branch ThousandEyes Support

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. From the list of devices, select the Cisco NFVIS device to monitor the system status, device health and interface packet statistics. View the CPU utilization for the guest VNF as well.
3. You can start, stop, or restart ThousandEyes container.



Note Monitoring charts for ThousandEyes container isn't supported.



CHAPTER 9

Manage Cisco Catalyst 8300 Series Edge uCPE using Cisco SD-WAN Manager via NFV Config Group Workflow

Table 7: Feature History

Feature Name	Release Information	Description
Manage Cisco Catalyst 8300 Series Edge uCPE using Cisco SD-WAN Manager via **Create NFV Config Group Workflow**	Cisco NFVIS Release 4.12.1 Cisco Catalyst SD-WAN Manager Release 20.12.1	You can manage the lifecycle of Cisco Catalyst 8300 Series Edge uCPE using Cisco SD-WAN Manager. You can seamlessly provision and monitor Cisco Catalyst 8300 Series Edge uCPE. You can deploy Cisco Catalyst 8300 Series Edge uCPE in bulk.

- Overview of Onboarding Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager, on page 93
- Define Cisco Catalyst 8300 Series Edge uCPE In Cisco SD-WAN Manager, on page 94
- Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager, on page 96
- Deploy Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager, on page 98
- Operate Cisco Catalyst 8300 Series Edge uCPE Using Cisco SD-WAN Manager, on page 99

Overview of Onboarding Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager

With **Create NFV Configuration Group** Workflows, Cisco SD-WAN Manager provides an enhanced and intuitive user interface to manage and operate Cisco Catalyst 8300 Series Edge uCPE more efficiently. The workflow is designed to streamline and simplify the management tasks related to Cisco NFVIS using Cisco SD-WAN Manager.

You can now easily onboard and provision Cisco Catalyst 8300 Series Edge uCPE into the Cisco SD-WAN Manager system using a simplified user interface and guided workflows. Create **Create NFV Configuration Group** for Day 0, enabling efficient deployment and setup of Cisco Catalyst 8300 Series Edge uCPE according

to specific service requirements. You can also modify configuration group parcels for Day N design customization. Cisco SD-WAN Manager offers the capability to manage software images for uCPE (Universal Customer Premises Equipment) platforms and VNF (Virtual Network Function) services, allowing administrators to source NFVIS and VNF images from external repositories. The workflows provide monitoring tools and insights to ensure the health and performance of both Cisco Catalyst 8300 Series Edge uCPE and virtualized network functions. Cisco SD-WAN Manager, with its modular and rich set of APIs, facilitates automation and integration with external systems. This allows for enhanced network orchestration and operational efficiency.

Key Tasks Before you Begin

- Your Cisco SD-WAN Manager should run Cisco Catalyst SD-WAN Manager Release 20.12.1 and later to onboard Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager using workflows.
- Ensure Cisco NFVIS WAN Edge device has reachability to the Cisco SD-WAN Validator and other Cisco SD-WAN Control Components which are reachable through public IP addresses across the WAN transports.
- Cisco NFVIS WAN Edge device has reachability to the remote server.

Define Cisco Catalyst 8300 Series Edge uCPE In Cisco SD-WAN Manager

Create a Device List

Create the device list in Cisco Smart Account and make it available in Cisco SD-WAN Manager. For more information see, Cisco Plug and Play Support Guide for Cisco SD-WAN products.

Sync Smart Account Using Cisco SD-WAN Manager

1. In the Cisco SD-WAN Manager Menu, click **Configuration** > **Devices**.
2. Click **Sync Smart Account**.
3. In the **Sync Smart Account** pane, enter the **Username** and **Password**. Choose whether you want to sync the WAN edge list with other Cisco SD-WAN Control Components using the **Sent to Controllers** drop-down list.
4. Click **Sync**.

   After the device has been successfully added to Cisco SD-WAN Manager, you should see the Cisco Catalyst 8300 Series Edge uCPE in the devices list.



Note The device will reach out to the Plug and Play Connect portal to receive the control components information. Do not interrupt the PnP boot-up process or the redirection to control components will fail.

Add a Remote Server

Cisco SD-WAN Manager uses the remote repository to source the vnf-disk-image, and auto-generate the files required by Cisco Catalyst 8300 Series Edge uCPE. For more information on adding a remote server see, Register Remote Server.

Upload a VNF Package

Uploading VNF QCOW2 to Cisco SD-WAN Manager is a three step process:

1. Download VNF package from the CCO.
2. Modify and repack Cisco SD-Branch VNF package (optional).
3. In the Cisco SD-WAN Manager Menu, navigate to **Maintenance** > **Software Repository** > **Virtual Images** > **Upload Virtual Image** > **Remote Server (preferred)** to upload VNF package into Cisco SD-WAN Manager.
4. In the pop-up window, enter the QCOW image file name (including the extension) and other required/optional fields to add remote server virtual image.

Use the Quick Connect Workflow

Quick Connect Workflow provides an alternative, guided method in Cisco SD-WAN Manager to onboard supported WAN edge devices into the Cisco Catalyst SD-WAN overlay network. This workflow adds Cisco Catalyst 8300 Series Edge uCPE to the WAN transport and establishes data plane and control plane connections.

The behavior of the Quick Connect workflow depends on how you upload devices to Cisco SD-WAN Manager. You can upload your devices in one of the following ways, either as part of the Quick Connect workflow or independently.

- Using the auto sync option, where your Smart Account is synced with Cisco SD-WAN Manager. This option requires Cisco SD-WAN Manager to be able to connect with the Cisco Plug n Play (PnP) portal.
- Using the manual upload method, where you download the authorized serial number file of devices from the Cisco PnP portal and upload it to Cisco SD-WAN Manager.



Note

- You can upload a file with the serial numbers: upload a signed file (.viptela file) from Cisco Plug and Play or upload an un-signed file (.csv file) and the sample CVS file can be downloaded directly from the link.
- Typical virtual branch deployment requires authorized list of devices and image packages for the services to be deployed. Also, the VNF images must be made available in Cisco SD-WAN Manager image repository.

Access the Quick Connect Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows**.
2. **Start a new Quick Connect workflow:** Under the **Popular Workflows** area, choose **Quick Connect Workflow**.

Note Ensure that you have the following configured before you get started:

- Organization's name
- Certificate Authorization
- Cisco SD-WAN Control Components including Cisco SD-WAN Controllers and Cisco SD-WAN Validators as per your requirement

3. Import device serial numbers from Cisco Plug and Play or upload device files manually using serial numbers.

Note Choose **Skip for now** if you already have Cisco Catalyst 8300 Series Edge uCPE configured in Cisco SD-WAN Manager.

4. Once, you see the Cisco Catalyst 8300 Series Edge uCPE in the device list, select the device and click **Next**.
5. Add and review Cisco Catalyst 8300 Series Edge uCPE settings that you want to configure and click **Next**.
6. You can tag Cisco Catalyst 8300 Series Edge uCPE to respective keywords (optional) to better group and identify the Cisco Catalyst 8300 Series Edge uCPE.

Note
- In Cisco SD-WAN Manager Release 20.12.1, device tagging is not supported for Cisco Catalyst 8300 Series Edge uCPE.

7. In the summary page, review the configuration of Cisco Catalyst 8300 Series Edge uCPE for one last time and click **Onboard**.
8. Your Cisco Catalyst 8300 Series Edge uCPE is now defined as a supported device in Cisco SD-WAN Manager.

Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager

The **Create NFV Configuration group** workflow provides a simple, reusable, and structured approach for the configurations in Cisco Catalyst SD-WAN and NFVIS environments. You can create a configuration group, that is, a logical grouping of features or configurations that can be applied to one or more devices in the network. You can also create profiles based on features that are required, recommended, or uniquely used, and then combine the profiles to complete a device configuration.

The configuration group workflow in Cisco SD-WAN Manager provides a guided method to create configuration groups and feature profiles. For more information see, Overview of Configuration Group Workflows.

Access NFV Configuration Group Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create NFV Configuration Group**.
2. **Start a new NFV Configuration workflow:** Under the **Popular Workflows** area, choose **Create NFV Configuration Group**.

Note You can perform site-wise configurations and tweak the site settings based on your requirement.

3. Enter a name for your NFV Configuration group and click **Next**.
4. Define the NFV device system settings and WAN circuits using the **Site Configurations** step.

Table 8: Site Configurations

Field	Description
Site Type	The configuration group type is **Single NFV Device** by default. **Note** Only single NFV device configuration group type is supported in Cisco SD-WAN Manager Release 20.12.1.
Site Settings	Enter site specific values that maybe common to other devices in Cisco SD-WAN Manager. Configure two different banner text strings, one to be displayed before the login prompt login banner. The other to be displayed after a successful login to the device-message-of-the-day (MOTD).
WAN Interfaces	Configure the WAN interfaces required. **Note** Maximum 4 WAN interfaces can be added.
WAN Routing	Click **Add Routes** to add WAN routing details to the configuration.

5. Define VNF services in the **VNF Services** step. You can either pick a pre-defined topology or you create your own custom topology.
6. Review and edit the NFV Config Group design if required and click **Create Configuration Group**.
7. Once you are done creating a NFV configuration group workflow, in the success page, click **Associate Devices to NFV-Router-Firewall** to associate the NFVIS devices to the intended configuration group.

Note You can edit the configuration group and add Day N modifications to the configuration group.

Create Add on CLI configuration

Create Add on CLI configuration with a user defined Feature Profile. For more information see, Configuration Groups and Feature Profiles.

Associate Cisco Catalyst 8300 Series Edge uCPE with Cisco SD-WAN Manager

1. Once the NFVIS Config group is successfully created, in the **What's Next** area, click **Associate Devices to NFV-Router-Firewall**.
2. Choose and review the list of devices.
3. Click **Next**.
4. Choose the respective device from the **Available Devices** screen.

Note You can perform site-wise configurations and tweak the site settings based on your requirement.

5. Click **Next**.
6. The devices are added to the configuration group. In the device added success pop-up, click **Provision Devices** to check all the site parameters, connectivity and check if the device is ready for configuration. Click **No, I Will Do It Later** if you want to skip provisioning your devices.

Deploy Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager

1. In the Cisco SD-WAN Manager, click **Workflows** > **Deploy Configuration Group**.
2. Choose the configuration group you created and click **Next**.
3. Select the devices from the particular site and click **Next**.
4. Add and review device configuration.

Note Cisco Catalyst SD-WAN autogenerates minimal configurations to make it easier for you to bring up your Cisco Catalyst 8300 Series Edge uCPE. Modify them as needed and directly edit the table to add System IP and Site IDs as per the requirement.

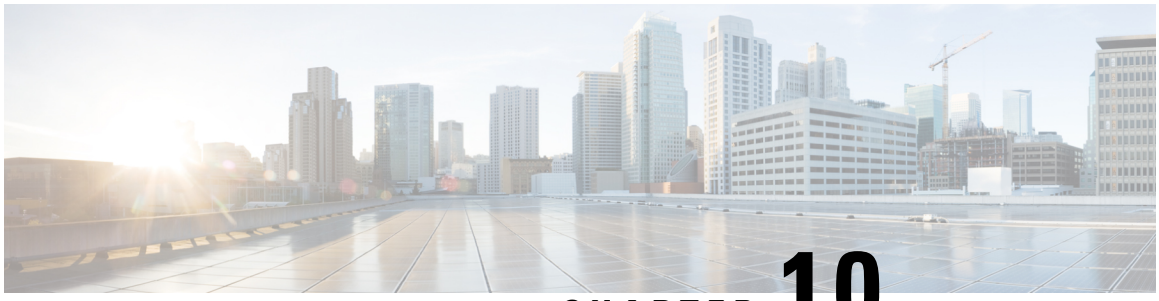
5. In the **Summary** page, review the configuration group and the selected device.
6. Click **Deploy**.

You've succesfully deployed your Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager.

Operate Cisco Catalyst 8300 Series Edge uCPE Using Cisco SD-WAN Manager

Monitor and operate Cisco Catalyst 8300 Series Edge uCPE using Cisco SD-WAN Manager.

1. In the Cisco SD-WAN Manager menu, click **Monitor** > **Devices**.
2. In the list of devices appearing, select Cisco Catalyst 8300 Series Edge uCPE to monitor the system status, device health and interface packet statistics. You can view the CPU utilization for the guest VNF as well.



CHAPTER 10

Manage Cisco NFVIS Devices Using NFV Config Group Workflow

Table 9: Feature History

Feature Name	Release Information	Description
Manage Cisco NFVIS devices using Cisco SD-WAN Manager via **Create NFV Config Group Workflow**	Cisco NFVIS Release 4.14.1 Cisco Catalyst SD-WAN Manager Release 20.14.1	Using this feature, manage the lifecycle of Cisco ENCS and Cisco Catalyst Edge uCPE 8200 devices using Cisco SD-WAN Manager. You can seamlessly provision and monitor Cisco ENCS and Cisco Catalyst Edge uCPE 8200 devices. You can deploy multiple Cisco ENCS and Cisco Catalyst Edge uCPE 8200 devices in bulk.

- Overview of Onboarding Cisco NFVIS Devices to Cisco SD-WAN Manager, on page 101
- Supported Devices, on page 102
- Define Cisco NFVIS Devices In Cisco SD-WAN Manager, on page 102
- Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager, on page 105
- Create a Switch Feature Profile For Cisco ENCS, on page 107
- Deploy Cisco NFVIS Devices to Cisco SD-WAN Manager, on page 107
- Operate Cisco NFVIS Devices Using Cisco SD-WAN Manager, on page 108

Overview of Onboarding Cisco NFVIS Devices to Cisco SD-WAN Manager

With **Create NFV Configuration Group** Workflows, Cisco SD-WAN Manager provides an enhanced and intuitive user interface to manage and operate Cisco ENCS more efficiently. The workflow is designed to streamline and simplify the management tasks related to Cisco NFVIS using Cisco SD-WAN Manager.

You can now easily onboard and provision Cisco NFVIS devices into the Cisco SD-WAN Manager system using a simplified user interface and guided workflows. Create an NFV Configuration Group for Day 0 to enable efficient deployment and setup of Cisco NFVIS devices according to specific service requirements.

You can also modify configuration group parcels for Day N design customization. Cisco SD-WAN Manager offers the capability to manage software images for uCPE (Universal Customer Premises Equipment) platforms and VNF (Virtual Network Function) services, allowing administrators to source NFVIS and VNF images from external repositories.

Benefits of Cisco SD-WAN Manager Workflows

- The workflows provide monitoring tools and insights to ensure the health and performance of both Cisco ENCS and virtualized network functions.
- The Cisco SD-WAN Manager, with its modular and rich set of APIs, facilitates automation and integration with external systems. This allows for enhanced network orchestration and operational efficiency.

Key Tasks Before you Begin

- Ensure that your Cisco SD-WAN Manager is running Cisco Catalyst SD-WAN Manager Release 20.14.1 and later to onboard Cisco ENCS to Cisco SD-WAN Manager using workflows.
- Ensure Cisco NFVIS WAN Edge device has reachability to the Cisco SD-WAN Validator and other Cisco SD-WAN Control Components which are reachable through public IP addresses across the WAN transports.
- Ensure that Cisco NFVIS WAN Edge device has rechability to the remote server.

Supported Devices

- Cisco ENCS
- Cisco Catalyst Edge uCPE 8200

Define Cisco NFVIS Devices In Cisco SD-WAN Manager

Create a Device List

Create a device list in the Cisco Smart Account and make it available in Cisco SD-WAN Manager. For more information see, Cisco Plug and Play Support Guide for Cisco SD-WAN products.

Sync Smart Account Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Click **Sync Smart Account**.
3. In the **Sync Smart Account** pane, enter the **Username** and **Password**. To sync the WAN edge list, with other Cisco SD-WAN Control Components, use the **Send to Controllers** drop-down list.
4. Click **Sync**.

After the device is successfully added to Cisco SD-WAN Manager, you should see the Cisco ENCS in the devices list.



Note The device reaches out to the Cisco Plug and Play (PNP) Connect portal to receive the control components information. Don't interrupt the PnP boot-up process or the redirection to control components fails.

Register a Remote Server

Cisco SD-WAN Manager uses the remote repository to source the vnf-disk-image, and auto generate the files required by Cisco ENCS. For more information on adding a remote server,see Register Remote Server.

Upload a VNF QCOW2

Uploading VNF QCOW2 to Cisco SD-WAN Manager is a three-step process:

1. Download the VNF QEMU Copy On Write version 2 (QCOW2) from CCO.
2. In the Cisco SD-WAN Manager Menu, navigate to **Maintenance** > **Software Repository** > **Virtual Images** > **Upload Virtual Image** > **Remote Server (preferred)** to upload VNF QCOW2 to Cisco SD-WAN Manager.
3. In the pop-up window, enter the QCOW image file name (including the extension) and other required/optional fields to add a remote server virtual image.

Use the Quick Connect Workflow

A Quick Connect Workflow provides an alternative, guided method in Cisco SD-WAN Manager to onboard supported WAN edge devices into the Cisco Catalyst SD-WAN overlay network. This workflow helps you configure Cisco NFVIS devices to establish data plane and control plane connections.

The behavior of the Quick Connect workflow depends on how you upload devices to Cisco SD-WAN Manager. You can upload your devices in one of the following ways, either as part of the Quick Connect workflow or independently.

- Auto-sync option: Your Smart Account is in sync with the Cisco SD-WAN Manager. This option requires Cisco SD-WAN Manager to be able to connect with the Cisco PNP portal.
- Manual upload: Download the authorized serial number file of devices from the Cisco PnP portal and upload it to Cisco SD-WAN Manager.

Use the following instructions to use the quick connect workflow:

1. From the Cisco SD-WAN Manager menu, choose **Workflows**.
2. To start a new quick connect workflow: Under the **Popular Workflows** area, choose **Quick Connect Workflow**.

Note Ensure that you have the following configured before you get started:

- Organization's name
- Certificate Authorization
- Cisco SD-WAN Control Components including Cisco SD-WAN Controllers and Cisco SD-WAN Validators as per your requirement

3. Import device serial numbers from Cisco Plug and Play or upload device files manually using serial numbers.

Note Choose **Skip for now** if you already have Cisco NFVIS devices configured in Cisco SD-WAN Manager.

4. Once you see the Cisco NFVIS devices in the device list, select the device from the device list, and click **Next**.
5. Add and review the Cisco NFVIS devices settings that you want to configure and click **Next**.
6. (Optional) You can tag Cisco NFVIS devices to respective keywords (optional) to better group and identify the Cisco NFVIS devices.

Note In Cisco SD-WAN Manager Release 20.12.1, device tagging isn't supported for Cisco NFVIS device. The device tagging is supported for Cisco NFVIS devices starting from Cisco SD-WAN Manager Release 20.13.1.

7. In the summary page, review the configuration of Cisco NFVIS device for one last time and click **Onboard**.

   Your Cisco NFVIS device is defined as a supported device in Cisco SD-WAN Manager.

Upload .CSV Files

- To upload a file with the serial numbers: Download the sample CSV file and upload a signed file (.viptela file) from Cisco Plug and Play or upload an unsigned file (.csv file). For more information, see Plug and Play Connect Service.

Note The **Chassis number** and either the **Cert Serial Number** or **SUDI Serial Number** are mandatory field to onboard Cisco ENCS onto Cisco SD-WAN Manager.

- Typical virtual branch deployment requires an authorized list of devices and VNF images for the services to deploy. Also, the VNF images should be made available in the remote server(s).

Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager

The **Create NFV Configuration group** workflow provides a simple, reusable, and structured approach for the configurations in Cisco Catalyst SD-WAN and NFVIS environments. You can create a configuration group, that is, a logical grouping of features or configurations that is applied to one or more devices in the network. Create profiles based on features that are required, recommended, or uniquely used, and then combine the profiles to complete a device configuration.

The configuration group workflow in Cisco SD-WAN Manager provides a guided method to create configuration groups and feature profiles. For more information see, Overview of Configuration Group Workflows.

Access NFV Configuration Group Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create NFV Configuration Group**.
2. Start a new NFV Configuration workflow: Under the **Popular Workflows** area, choose **Create NFV Configuration Group**.

Note You can perform site-wise configurations and tweak the site settings based on your requirement.

3. Enter a name for your NFV Configuration group and click **Next**.
4. Define the NFV device system settings and WAN circuits using the **Site Configurations** step.

Table 10: Site Configurations

Field	Description
Site Type	The configuration group type is **Single NFV Device** by default. This is the only option available.
Site Settings	Enter site-specific values that maybe common to other devices in Cisco SD-WAN Manager. Configure two different banner text strings, one to be displayed before the login banner. The other to be displayed after a successful login to the device-message-of-the-day (MOTD).
WAN Interfaces	Configure the WAN interfaces required. **Note** Only one DHCP and a maximum of four WAN interfaces are supported. The Cisco ENCS device supports only two WAN interfaces.

Field	Description
WAN Routing	Click **Add Routes** to add WAN routing details to the configuration.

5. Define VNF services in the **VNF Services** step. You can either pick a predefined topology or you create your own custom topology.
6. Review and edit the NFV Config Group design if required and click **Create Configuration Group**.
7. Once you create an NFV configuration group workflow, in the success page, click **Associate Devices to the NFV config group** to associate the NFVIS devices to the intended configuration group.

Note You can edit the configuration group and add Day N modifications to the configuration group.

Create Add on CLI configuration

Create an Add on CLI configuration with a user-defined Feature Profile. For more information see, Configuration Groups and Feature Profiles.

Note

- In the **Add and Review Device Configuration** page, enter `GEO-2` in the field for the LAN interface, where the default variable name is `lan_1_intf_name`.
- Enter the **LAN IP address** and **Subnet Mask**. The Cisco SD-WAN Manager configures these settings under the MGMT interface on the Cisco ENCS platform.

Associate Cisco NFVIS Devices with Cisco SD-WAN Manager

1. Once the NFVIS Config group is sucessfully created in the **What's Next** area, click **Associate Devices to the NFV config group**.
2. Choose and review the list of devices.
3. Click **Next**.
4. Choose the respective device from the **Available Devices** screen.

Note

- You can perform site-wise configurations and tweak the site settings based on your requirement.
- If you intend to use ENCS LAN-SRIOV networks for the VM interfaces, enter `GEO-2` in the **Interface Name Variable**.

5. Click **Next**.

6. The devices are added to the configuration group. In the device added success pop-up, click **Provision Devices** to check all the site parameters, connectivity, and check if the device is ready for configuration. Click **No, I Will Do It Later** if you want to skip provisioning your devices.

Create a Switch Feature Profile For Cisco ENCS

Cisco ENCS devices are built-in with a hardware switch, by default. Configure the switch within Cisco ENCS using Cisco SD-WAN Manager using the **Switch** feature profile.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **...** in the **Actions** column adjacent to the NFV configuration group you created and click **Edit**.
3. Expand the **Network Profile** and navigate to the **Switch** tab.



Note The NFV configuration groups, by default, creates **System Profile** and **Network Profile** as associated profiles.

4. Click **Add Switch**.
5. In the **Add Feature** page, enter a **Name** and **Description** (optional) for the switch profile.
6. In the **Basic Settings** tab, click **+ Add Interfaces** and add the switch parcel configuration.

Field	Description
Interface Name	Choose an interface from the interface name drop-down list.
VLAN	Enter a VLAN value.
VLAN Mode	Choose between Access or Trunk VLAN modes.
Native VLAN	In case of trunk mode, add a native VLAN value.
Action	Click the delete icon to delete the switch profile.

Deploy Cisco NFVIS Devices to Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Deploy Configuration Group**.
2. Choose the configuration group you created and click **Next**.
3. Select the devices from the particular site and click **Next**.
4. Add and review device configuration.

Note Cisco Catalyst SD-WAN autogenerates minimal configurations to make it easier for you to bring up your Cisco NFVIS device. Modify them as needed and edit the configuration fields to add System IP and Site IDs as per the requirement.

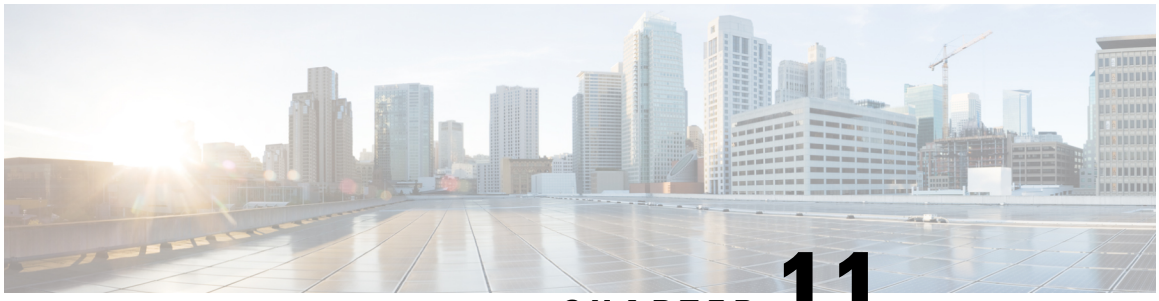
5. In the **Summary** page, review the configuration group and the selected device.
6. Click **Deploy**.

   You've succesfully deployed your Cisco NFVIS device to Cisco SD-WAN Manager.

Operate Cisco NFVIS Devices Using Cisco SD-WAN Manager

Monitor and operate Cisco NFVIS devices using Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. In the list of devices appearing, select the Cisco NFVIS device to monitor the system status, device health and interface packet statistics. View the CPU utilization for the guest VNF as well.



CHAPTER 11

Onboard Cisco UCS C-Series M6 Devices Using Cisco SD-WAN Manager via NFV Config Group Workflow

Table 11: Feature History

Feature Name	Release Information	Description
Manage Cisco UCS C-Series M6 Devices using Cisco SD-WAN Manager via **Create NFV Config Group Workflow**	Cisco NFVIS Release 4.15.2 Cisco Catalyst SD-WAN Manager Release 20.15.2	With this feature, you can manage the lifecycle of Cisco UCS C-Series M6 devices using Cisco SD-WAN Manager. This enables seamless provisioning and monitoring of these devices, and supports bulk deployment, which is ideal for large-scale operations.

- Overview of Onboarding Cisco UCS C-Series M6 Devices to Cisco SD-WAN Manager, on page 109
- Supported Devices, on page 110
- Define Cisco UCS C-Series M6 Devices in Cisco SD-WAN Manager, on page 111
- Create Add on CLI Configuration, on page 113
- Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager, on page 113
- Deploy Cisco UCS C-Series M6 Devices to Cisco SD-WAN Manager, on page 115
- Operate Cisco UCS C-Series M6 Devices Using Cisco SD-WAN Manager, on page 115

Overview of Onboarding Cisco UCS C-Series M6 Devices to Cisco SD-WAN Manager

With **Create NFV Configuration Group** Workflows, Cisco SD-WAN Manager provides an enhanced and intuitive user interface to manage and operate Cisco UCS C-Series M6 devices more efficiently. The workflow is designed to streamline and simplify the management tasks related to Cisco NFVIS using Cisco SD-WAN Manager.

Onboarding and Provisioning Cisco UCS C-Series M6 Devices

You can now easily onboard and provision Cisco UCS C-Series M6 devices into Cisco SD-WAN Manager using a simplified user interface and guided workflows. Create an NFV Configuration Group for Day 0, enabling efficient deployment and setup of Cisco UCS C-Series M6 devices according to specific service requirements. You can also modify configuration group parcels for Day N design customization. Cisco SD-WAN Manager offers the capability to manage software images for UCS C-Series M6 platforms and VNF (Virtual Network Function) services,allowing administrators to source NFVIS and VNF images from external repositories.

Cisco UCS C-Series M6 Support for Smart Licensing

Cisco UCS C-Series M6 devices with NFVIS support smart licensing. You can configure smart licensing using the CLI Add-on profile in Cisco SD-WAN Manager. For more information see, Create Add on CLI Configuration, on page 113.

Key Tasks Before you Begin

- Your Cisco SD-WAN Manager should run Cisco Catalyst SD-WAN Manager Release 20.15.2 and later to onboard Cisco UCS C-Series M6 devices with NFVIS to Cisco SD-WAN Manager using workflows.
- Ensure Cisco NFVIS WAN Edge device has reachability to the Cisco SD-WAN Validator and other Cisco SD-WAN Control Components which are reachable through public IP addresses across the WAN transports.
- Cisco NFVIS WAN Edge device has reachability to the remote server.

Benefits of Cisco SD-WAN Manager Workflows

- The workflows provide monitoring tools and insights to ensure the health and performance of both Cisco UCS C-Series M6 devices and virtualized network functions.
- Cisco SD-WAN Manager, with its modular and rich set of APIs, facilitates automation and integration with external systems. This allows for enhanced network orchestration and operational efficiency.

Supported Devices

The following devices are supported by Cisco SD-WAN Manager:

- Cisco UCS C220 M6S Rack Server
- Cisco UCS C240 M6S Rack Server
- .Cisco UCS C240 M6SX Rack Server

Define Cisco UCS C-Series M6 Devices in Cisco SD-WAN Manager

Create a Device List

Create the device list in Cisco Smart Account and make it available in Cisco SD-WAN Manager. For more information see, Cisco Plug and Play Support Guide for Cisco SD-WAN products.

Sync Smart Account Using Cisco SD-WAN Manager

Starting from Cisco Catalyst SD-WAN Manager Release 20.15.2, the **Sync Smart Account** option is available from the Quick Connect workflow. For more information, see the **Access the Quick Connect Workflow** section.

The following workflow to sync a smart account is applicable for Cisco vManage Release 20.9.1 and earlier.

1. From the Cisco SD-WAN Manager menu, click **Configuration** > **Devices**.
2. Click **Sync Smart Account**.
3. In the **Sync Smart Account** pane, enter the **Username** and **Password**. Choose whether you want to sync the WAN edge list with other Cisco SD-WAN Control Components using the **Sent to Controllers** drop-down list.
4. Click **Sync**.

   After the device has been successfully added to Cisco SD-WAN Manager, you should see the Cisco UCS C-Series M6 devices list.



Note The device will reach out to the Plug and Play Connect portal to receive the control components information. Do not interrupt the PnP boot-up process or the redirection to control components will fail.

Add a Remote Server

Cisco SD-WAN Manager uses the remote repository to source the vnf-disk-image, and auto-generate the files required by Cisco UCS C-Series M6 devices. For more information on adding a remote server see, Register Remote Server.

Upload a VNF Package

Uploading VNF QCOW2 to Cisco SD-WAN Manager is a three step process:

1. Download VNF package from the CCO.
2. Modify and repack Cisco SD-Branch VNF package (optional).
3. In the Cisco SD-WAN Manager Menu, navigate to **Maintenance** > **Software Repository** > **Virtual Images** > **Upload Virtual Image** > **Remote Server (preferred)** to add VNF package into Cisco SD-WAN Manager.

4. In the pop-up window, enter the QCOW2 image file name (including the extension, .qcow2), ThousandEyes Container TAR image file name (including the extension .tar), and other required/optional fields to add remote server virtual image.

Use the Quick Connect Workflow

Quick Connect Workflow provides an alternative, guided method in Cisco SD-WAN Manager to onboard supported WAN edge devices into the Cisco Catalyst SD-WAN overlay network. This workflow adds Cisco UCS C-Series M6 devices to the WAN transport and establishes data plane and control plane connections.

The behavior of the Quick Connect workflow depends on how you upload devices to Cisco SD-WAN Manager. You can upload your devices in one of the following ways, either as part of the Quick Connect workflow or independently.

- Using the auto sync option, where your Smart Account is synced with Cisco SD-WAN Manager. This option requires Cisco SD-WAN Manager to be able to connect with the Cisco Plug n Play (PnP) portal.
- Using the manual upload method, where you download the authorized serial number file of devices from the Cisco PnP portal and upload it to Cisco SD-WAN Manager.



Note

- You can upload a file with the serial numbers: upload a signed file (.viptela file) from Cisco Plug and Play or upload an un-signed file (.csv file) and the sample CVS file can be downloaded directly from the link.
- Typical virtual branch deployment requires authorized list of devices and image packages for the services to be deployed. Also, the VNF images must be made available in Cisco SD-WAN Manager image repository.

Access the Quick Connect Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows**.
2. **Start a new Quick Connect workflow:** Under the **Popular Workflows** area, choose **Quick Connect Workflow**.



Note Ensure that you have the following configured before you get started:

- Organization's name
- Certificate Authorization
- Cisco SD-WAN Control Components including Cisco SD-WAN Controllers and Cisco SD-WAN Validators as per your requirement

Starting from Cisco Catalyst SD-WAN Manager Release 20.15.2, you can sync smart account from the quick connect workflow.

3. Click **Log into your Smart Account**.
4. Enter your user name and password for your smart account, and **Next**.

5. Import device serial numbers from Cisco Plug and Play or upload device files manually using serial numbers.



Note Choose **Skip for now** if you already have Cisco UCS C-Series M6 devices configured in Cisco SD-WAN Manager.

6. Once, you see the Cisco UCS C-Series M6 devices in the device list, select the device and click **Next**.
7. Add and review Cisco UCS C-Series M6 devices settings that you want to configure and click **Next**.
8. You can tag Cisco UCS C-Series M6 devices to respective keywords (optional) to better group and identify the Cisco UCS C-Series M6 devices.
9. In the summary page, review the configuration of Cisco UCS C-Series M6 devices for one last time and click **Onboard**.
10. Your Cisco UCS C-Series M6 devices is now defined as a supported device in Cisco SD-WAN Manager.

Create Add on CLI Configuration

Using a CLI add-on profile, you can specify CLI commands to execute on devices. For more information see CLI Add-On Profile.

Change Smart Licensing Mode

To change the licensing mode from Cisco Smart Licensing Utility (CSLU), which is the default mode, to Smart or vice versa from the Cisco SD-WAN Manager, you can use the add-on CLI. For more information, see Configure Cisco NFVIS Support For Cisco UCS C-Series M6 Rack Servers.

Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager

The **Create NFV Configuration group** workflow provides a simple, reusable, and structured approach for the configurations in Cisco Catalyst SD-WAN and NFVIS environments. You can create a configuration group, that is, a logical grouping of features or configurations that can be applied to one or more devices in the network.You can also create profiles based on features that are required, recommended, or uniquely used, and then combine the profiles to complete a device configuration.

The configuration group workflow in Cisco SD-WAN Manager provides a guided method to create configuration groups and feature profiles. For more information see, Overview of Configuration Group Workflows.

Access NFV Configuration Group Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create NFV Configuration Group**.
2. **Start a new NFV Configuration workflow:** Under the **Popular Workflows** area, choose **Create NFV Configuration Group**.

Note You can perform site-wise configurations and tweak the site settings based on your requirement.

3. Enter a name for your NFV Configuration group and click **Next**.
4. Define the NFV device system settings and WAN circuits using the **Site Configurations** step.

Table 12: Site Configurations

Field	Description
Site Type	The configuration group type is **Single NFV Device** by default.
Site Settings	Enter site specific values that maybe common to other devices in Cisco SD-WAN Manager. Configure two different banner text strings, one to be displayed before the login prompt login banner. The other to be displayed after a successful login to the device-message-of-the-day (MOTD).
WAN Interfaces	Configure the WAN interfaces required. **Note** Maximum 4 WAN interfaces can be added.
WAN Routing	Click **Add Routes** to add WAN routing details to the configuration.

5. Define VNF services in the **VNF Services** step. You can either pick a pre-defined topology or you create your own custom topology.
6. Review and edit the NFV Config Group design if required and click **Create Configuration Group**.
7. Once you are done creating a NFV configuration group workflow, in the success page, click **Associate Devices to NFVirtual Configuration Group** to associate the NFVIS devices to the intended configuration group.

Note You can edit the configuration group and add Day N modifications to the configuration group.

Associate Cisco UCS C-Series M6 devices with Cisco SD-WAN Manager

1. Once the NFVIS Config group is successfully created, in the **What's Next** area, click **Associate Devices to NFVirtual Configuration Group**.
2. Choose and review the list of devices.
3. Click **Next**.
4. Choose the respective device from the **Available Devices** screen.

Note You can perform site-wise configurations and tweak the site settings based on your requirement.

5. Click **Next**.
6. The devices are added to the configuration group. In the device added success pop-up, click **Provision Devices** to check all the site parameters, connectivity and check if the device is ready for configuration. Click **No, I Will Do It Later** if you want to skip provisioning your devices.

Deploy Cisco UCS C-Series M6 Devices to Cisco SD-WAN Manager

1. In the Cisco SD-WAN Manager, click **Workflows** > **Deploy Configuration Group**.
2. Choose the configuration group you created and click **Next**.
3. Select the devices from the particular site and click **Next**.
4. Add and review device configuration.

Note Cisco Catalyst SD-WAN autogenerates minimal configurations to make it easier for you to bring up your Cisco UCS C-Series M6 devices. Modify them as needed and directly edit the table to add System IP and Site IDs as per the requirement.

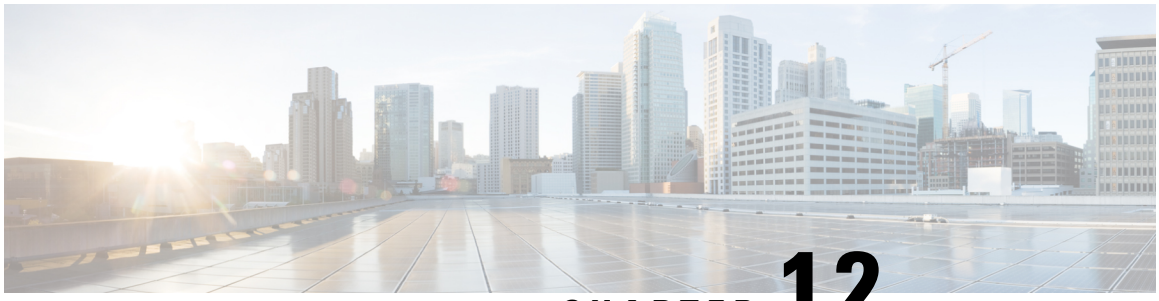
5. In the **Summary** page, review the configuration group and the selected device.
6. Click **Deploy**.

   You've succesfully deployed your Cisco UCS C-Series M6 devices to Cisco SD-WAN Manager.

Operate Cisco UCS C-Series M6 Devices Using Cisco SD-WAN Manager

Monitor and operate Cisco UCS C-Series M6 devices using Cisco SD-WAN Manager.

1. In the Cisco SD-WAN Manager menu, click **Monitor** > **Devices**.
2. In the list of devices appearing, select Cisco UCS C-Series M6 devices to monitor the system status, device health and interface packet statistics. You can view the CPU utilization for the guest VNF as well.



CHAPTER 12

Appendix

- NFVIS Deployment in Sites with Low WAN Bandwidth, on page 117
- Single IP Address Sharing Between NFVIS and the Router VM, on page 118

NFVIS Deployment in Sites with Low WAN Bandwidth

The VNF images are downloaded from Cisco SD-WAN Manager onto NFVIS device during provisioning. Across low bandwidth WAN uplinks, the image download can be time consuming. In this case, there is an option to make the large image files available in the local repository of NFVIS device and the device is instructed to use the local image during provisioning.

The following steps shows how you can create and upload VNF images in NFVIS.

1. Upload the image package in Cisco SD-WAN Manager image repository.

   For example:

   vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz

2. SCP copy the VNF image onto NFVIS device. Cisco SD-WAN Manager then skips downloading the package. Ensure that you rename the package when you SCP and upload the same package into Cisco SD-WAN Manager.

   ```
   scp<username>@<SCP_SERVER_IP>:/<package_name>
   intdatastore:<vnf_typ>_<name>_<version>_<package_name>
   ```

   Example:

   ```
   scp admin@172.19.156.240:/vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz

   intdatastore:/ROUTER_vEdge_20.3.904-9_vEdge_20.3.904-9_vBranch_Cisco_ENB_Viptela_monitor_EFT.tar.gz
   ```

   Add <vnf_typ>_<name>_<version>_ prefix in front of the original package name which is based on the information from the image_properties.xml file inside the package.

   ```
   <image_properties>
           <vnf_type>ROUTER</vnf_type>
           <name>vEdge</name>
           <version>20.3.904-9</version>
   ……
   ……
   ```

```
.....
</image_properties>
```

3. Use the **show system:system file-list** command to verify that the image is copied successfully.

You can then go ahead with the rest of the Network Design template workflow and Cisco SD-WAN Manager skips the download VNF step. Ensure that you select the correct package in the Network Design template.

Single IP Address Sharing Between NFVIS and the Router VM

This topic contains the end-to-end configuration example to configure the single IP address sharing feature between NFVIS and the router VM.

Step 1: Configure HTTP Host for Day 0 Configuration

The following examples show how to set up the HTTP server to host the day 0 configuration file for Cisco Catalyst 8000V and Cisco vEdge devices respectively.

Example: Host Day 0 Configuration File for Cisco Catalyst 8000V

```
Content-Type: multipart/mixed; boundary="==========2587222130433519110=="
MIME-Version: 1.0
--==========2587222130433519110==
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config"
#cloud-config
vinitparam:
 - otp : ${EX_OTP}
 - vbond : ${EX_VBOND}
 - org : ${EX_ORGNAME}
 - uuid : ${EX_UUID}

--==========2587222130433519110==
Content-Type: text/cloud-boothook; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
 filename="config-default.txt"
#cloud-boothook
system
   host-name             ${EX_HOSTNAME}
   system-ip             ${EX_SYSTEM_IP}
   overlay-id            1
   site-id               ${EX_SITE_ID}
   port-offset           0
   control-session-pps   300
   admin-tech-on-failure
   sp-organization-name  "${EX_ORGNAME}"
   organization-name     "${EX_ORGNAME}"
   port-hop
   track-transport
   track-default-gateway
   console-baud-rate     115200
   vbond ${EX_VBOND} port 12346
   logging
    disk
     enable
    !
```

```
 !
!
bfd app-route multiplier 6
bfd app-route poll-interval 600000
sslproxy
 no enable
 rsa-key-modulus      2048
 certificate-lifetime 730
 eckey-type           P256
 ca-tp-label          PROXY-SIGNING-CA
 settings expired-certificate  drop
 settings untrusted-certificate drop
 settings unknown-status       drop
 settings unsupported-protocol-versions drop
 settings unsupported-cipher-suites drop
 settings failure-mode         close
 settings minimum-tls-ver      TLSv1
!
no tcpproxy enable
!
sdwan
 interface GigabitEthernet2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color default
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
  exit
 exit
 appqoe
  no tcpopt enable
 !
 omp
  no shutdown
  send-path-limit  4
  ecmp-limit       4
  graceful-restart
  no as-dot-notation
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
```

```
    address-family ipv4
     advertise connected
     advertise static
    !
    address-family ipv6
     advertise connected
     advertise static
    !
   !
  !
  security
   ipsec
    rekey               86400
    replay-window       512
    authentication-type sha1-hmac ah-sha1-hmac
   !
  !
  no service pad
  service tcp-keepalives-in
  service tcp-keepalives-out
  no service tcp-small-servers
  no service udp-small-servers
  username admin privilege 15 secret 0 admin
  vrf definition Mgmt-intf
   description Transport VPN
   rd          1:512
   address-family ipv4
    route-target export 1:512
    route-target import 1:512
    exit-address-family
   !
   address-family ipv6
    exit-address-family
   !
  !
vrf definition 500
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
 !
!
vrf definition ${EX_DATA_VPN_NUMBER}
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition ${EX_MGMT_VPN_NUMBER}
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
hostname ${EX_HOSTNAME}
username ${EX_SSH_USERNAME} privilege 15 secret 0 ${EX_SSH_PASSWORD}
enable password ${EX_ENABLE_PASSWORD}
!
ip name-server ${EX_DNS_IP}
```

```
!
  ip arp proxy disable
  no ip finger
  no ip rcmd rcp-enable
  no ip rcmd rsh-enable
  no ip dhcp use class
  ip multicast route-limit 2147483647
  ip bootp server
  no ip source-route
  no ip http server
  no ip http secure-server
  no ip http ctc authentication
  no ip igmp ssm-map query dns
  interface GigabitEthernet1
   vrf forwarding 500
   description MGMT
   no shutdown
   arp timeout 1200
   ip address ${NICID_0_IP_ADDRESS} ${NICID_0_NETMASK}
   ip redirects
   ip mtu    1500
   mtu         1500
   negotiation auto
  exit
  interface GigabitEthernet2
   description Transport
   no shutdown
   arp timeout 1200
   ip address ${EX_VPN0_WAN_IP_ADDRESS} ${EX_VPN0_WAN_NETMASK}
   ip nat outside
   ip redirects
   ip mtu    1500
   mtu         1500
   negotiation auto
  exit
interface GigabitEthernet3
 vrf forwarding ${EX_MGMT_VPN_NUMBER}
 ip address ${EX_MGMT_IP_ADDRESS} ${EX_MGMT_NETMASK}
 no shutdown
 exit
!
interface GigabitEthernet4
 vrf forwarding ${EX_DATA_VPN_NUMBER}
 ip address ${EX_LAN_IP_ADDRESS} ${EX_LAN_NETMASK}
 no shutdown
 exit
!
  interface Tunnel2
   no shutdown
   ip unnumbered GigabitEthernet2
   no ip redirects
   ipv6 unnumbered GigabitEthernet2
   no ipv6 redirects
   tunnel source GigabitEthernet2
   tunnel mode sdwan
  exit
  clock timezone UTC 0 0
  logging persistent size 104857600 filesize 10485760
  logging buffered 512000
  no logging rate-limit
  logging persistent
  aaa authentication login default local
  aaa authorization exec default local
  aaa session-id common
```

```
  no crypto ikev2 diagnose error
  no crypto isakmp diagnose error
  snmp-server ifindex persist
  line con 0
   login authentication default
   speed    115200
   stopbits 1
  !
  line vty 0 4
   transport input ssh
  !
  line vty 5 80
   transport input ssh
  !
  lldp run
  nat64 translation timeout tcp 60
  nat64 translation timeout udp 1
 !
!
ip route 0.0.0.0 0.0.0.0 ${EX_VPN0_WAN_GATEWAY}
!
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat route vrf 500 0.0.0.0 0.0.0.0 global
!

--===============2587222130433519110==
```

Example: Host Day 0 Configuration File for a Cisco vEdge Device for version 20.5

```
#cloud-config
write_files:
- path: /etc/viptela/otp
  content: "${OTP}"
- path: /etc/viptela/uuid
  content: "${UUID}"
- path: /etc/default/personality
  content: "vedge"
- path: /etc/default/inited
  content: "1"
- path: /etc/viptela/cdb_init_done
  content: "1"
- path: /etc/viptela/vdaemon_gen_id
  content: "0"
- path: /etc/confd/init/cloud-init.xml
  content: |
    <config xmlns="http://tail-f.com/ns/config/1.0">
      <omp xmlns="http://viptela.com/omp">
        <advertise>
          <protocol>ospf</protocol>
          <route>external</route>
        </advertise>
        <advertise>
          <protocol>connected</protocol>
        </advertise>
        <advertise>
          <protocol>static</protocol>
        </advertise>
      </omp>
      <security xmlns="http://viptela.com/security">
        <ipsec>
          <authentication-type>ah-sha1-hmac</authentication-type>
          <authentication-type>sha1-hmac</authentication-type>
        </ipsec>
      </security>
      <system xmlns="http://viptela.com/system">
```

```
    <personality>vedge</personality>
    <rootcert-installed>true</rootcert-installed>
    <host-name>${HOSTNAME}</host-name>
    <system-ip>${SYSTEM_IP}</system-ip>
    <site-id>${SITE_ID}</site-id>
    <organization-name>${ORGNAME}</organization-name>
    <vbond>
      <remote>${VBOND}</remote>
    </vbond>
    <aaa>
      <auth-order>local</auth-order>
      <auth-order>radius</auth-order>
      <auth-order>tacacs</auth-order>
      <usergroup>
        <name>basic</name>
        <task>
          <mode>system</mode>
          <permission>read</permission>
          <permission>write</permission>
        </task>
        <task>
          <mode>interface</mode>
          <permission>read</permission>
          <permission>write</permission>
        </task>
      </usergroup>
      <usergroup>
        <name>netadmin</name>
      </usergroup>
      <usergroup>
        <name>operator</name>
        <task>
          <mode>system</mode>
          <permission>read</permission>
        </task>
        <task>
          <mode>interface</mode>
          <permission>read</permission>
        </task>
        <task>
          <mode>policy</mode>
          <permission>read</permission>
        </task>
        <task>
          <mode>routing</mode>
          <permission>read</permission>
        </task>
        <task>
          <mode>security</mode>
          <permission>read</permission>
        </task>
      </usergroup>
      <user>
        <name>admin</name>
<password>$6$siwKBQ==$wI2lUa9BSreDPI6gB8sl4E6PAJoVXgMogv/whJ8F1C6sWdRazdxorYYTLrL6syiG6qnIABTnrE96HJiKF6QRq1</password>
      </user>
    </aaa>
  </system>
  <vpn xmlns="http://viptela.com/vpn">
    <vpn-instance>
      <vpn-id>0</vpn-id>
      <dns>
```

```
      <dns-addr>${DNS_IP}</dns-addr>
    </dns>
    <interface>
      <if-name>ge0/0</if-name>
      <ip>
        <dhcp-client>true</dhcp-client>
      </ip>
      <nat/>
      <tunnel-interface>
        <encapsulation>
          <encap>ipsec</encap>
        </encapsulation>
        <allow-service>
          <all>true</all>
        </allow-service>
      </tunnel-interface>
      <shutdown>false</shutdown>
    </interface>
    <interface>
      <if-name>ge0/3</if-name>
      <ip>
        <address>${NICID_4_IP_ADDRESS}/${NICID_4_CIDR_PREFIX}</address>
      </ip>
      <shutdown>false</shutdown>
    </interface>
  </vpn-instance>
  <vpn-instance>
    <vpn-id>${DATA_VPN_NUMBER}</vpn-id>
    <interface>
      <if-name>ge0/2</if-name>
      <ip>
        <address>${SERVICE_IP}/${SERVICE_MASK_LENGTH}</address>
      </ip>
      <shutdown>false</shutdown>
    </interface>
  </vpn-instance>
  <vpn-instance>
    <vpn-id>${MANAGEMENT_VPN_NUMBER}</vpn-id>
    <interface>
      <if-name>ge0/1</if-name>
      <ip>
        <address>${MGMT_IP}/${MGMT_MASK_LENGTH}</address>
      </ip>
      <shutdown>false</shutdown>
    </interface>
  </vpn-instance>
  <vpn-instance>
    <vpn-id>512</vpn-id>
    <interface>
      <if-name>eth0</if-name>
      <shutdown>false</shutdown>
    </interface>
  </vpn-instance>
 </vpn>
</config>
```

Step 2: Configure Single IP Address Sharing

This example shows how to configure single IP address sharing between NFVIS and the router VMs using the CLI Add-on feature template in Cisco SD-WAN Manager.

Sample Configuration for Cisco Catalyst 8000V Using CLI Add-on Feature Template

In this example NFVIS uses the int-mgmt-net-br interface in VPN 0 to establish control connection with Cisco SD-WAN Manager. The configuration also includes the VM lifecyle configuration for the day 0 configuration. NFVIS gets this information from HTTP server included in the configuration.

```
vm_lifecycle tenants tenant admin
 description      "Built-in Admin Tenant"
 managed_resource true
 vim_mapping      true
 deployments deployment deployment-ROUTER_1
  vm_group deployment-ROUTER_1
   image
ROUTER_C8000V_V175-Serial_C8Kv_175_LATEST_20201115_122120-serial_vBranch_Ubaid_Sdwan3.tar.gz

   flavor             ROUTER_1
   vim_vm_name        ROUTER_1
   bootup_time        900
   recovery_wait_time 5
   recovery_policy action_on_recovery REBOOT_ONLY
   !
   config_data configuration ciscosdwan_cloud_init.cfg
    file "http://172.25.221.219/config/UBAID_SDWAN_CLOUD_INITnew.cfg"
    variable EX_UUID
     val [ {{EX_UUID}} ]
    !
    variable EX_OTP
     val [ {{EX_OTP}} ]
    !
    variable EX_ORGNAME
     val [ "{{EX_ORGNAME}}" ]
    !
    variable EX_VBOND
     val [ {{EX_VBOND}} ]
    !
    variable EX_SYSTEM_IP
     val [ {{EX_SYSTEM_IP}} ]
    !
    variable EX_SITE_ID
     val [ {{EX_SITE_ID}} ]
    !
    variable EX_VPN0_WAN_GATEWAY
     val [ {{EX_VPN0_WAN_GATEWAY}} ]
    !
    variable EX_VPN0_WAN_IP_ADDRESS
     val [ {{EX_VPN0_WAN_IP_ADDRESS}} ]
    !
    variable EX_VPN0_WAN_NETMASK
     val [ {{EX_VPN0_WAN_NETMASK}} ]
    !
    variable EX_DNS_IP
     val [ {{EX_DNS_IP}} ]
    !
    variable EX_SSH_USERNAME
     val [ {{EX_SSH_USERNAME}} ]
    !
    variable EX_SSH_PASSWORD
     val [ "{{EX_SSH_PASSWORD}}" ]
    !
    variable EX_ENABLE_PASSWORD
     val [ "{{EX_ENABLE_PASSWORD}}" ]
    !
    variable EX_HOSTNAME
     val [ {{EX_HOSTNAME}} ]
    !
    variable EX_LAN_IP_ADDRESS
```

```
     val [ {{EX_LAN_IP_ADDRESS}} ]
    !
    variable EX_LAN_NETMASK
     val [ {{EX_LAN_NETMASK}} ]
    !
    variable EX_MGMT_IP_ADDRESS
     val [ {{EX_MGMT_IP_ADDRESS}} ]
    !
    variable EX_MGMT_NETMASK
     val [ {{EX_MGMT_NETMASK}} ]
    !
    variable EX_DATA_VPN_NUMBER
     val [ {{EX_DATA_VPN_NUMBER}} ]
    !
    variable EX_MGMT_VPN_NUMBER
     val [ {{EX_MGMT_VPN_NUMBER}} ]
    !
   !
  !
 !
!
single-ip-mode vm-name deployment-ROUTER_1.deployment-ROUTER_1
!
vpn 0
interface int-mgmt-net-br
  no shutdown
  tunnel-interface
   color bronze
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   encapsulation ipsec
  !
!
```

Sample Configuration for a Cisco vEdge Cloud Router Using CLI Add-on Feature Template

In this example NFVIS uses the int-mgmt-net-br interface in VPN 0 to establish control connection with Cisco SD-WAN Manager. The configuration also includes the VM lifecyle configuration for the day 0 configuration. NFVIS gets this information from HTTP server included in the configuration.

```
vm_lifecycle tenants tenant admin
 description      "Built-in Admin Tenant"
 managed_resource true
 vim_mapping      true
 deployments deployment deployment-ROUTER_1
  vm_group deployment-ROUTER_1
   bootup_time        600
   recovery_wait_time 5
   recovery_policy action_on_recovery REBOOT_ONLY
   !
   kpi_data kpi VM_ALIVE
     metric_collector type ICMPPing
     metric_collector nicid 4
     !

   config_data configuration /openstack/latest/user_data
```

```
    file "http://172.25.221.219/config/20.5-vedge-single-ip-dhcp.cfg"
    variable EX_UUID
     val [ {{EX_UUID}} ]
    !
    variable EX_OTP
     val [ {{EX_OTP}} ]
    !
    variable EX_ORGNAME
     val [ "{{EX_ORGNAME}}" ]
    !
    variable EX_VBOND
     val [ {{EX_VBOND}} ]
    !
    variable EX_SYSTEM_IP
     val [ {{EX_SYSTEM_IP}} ]
    !
    variable EX_SITE_ID
     val [ {{EX_SITE_ID}} ]
    !
    variable EX_DNS_IP
     val [ {{EX_DNS_IP}} ]
    !
    variable EX_SSH_USERNAME
     val [ {{EX_SSH_USERNAME}} ]
    !
    variable EX_SSH_PASSWORD
     val [ "{{EX_SSH_PASSWORD}}" ]
    !
    variable EX_ENABLE_PASSWORD
     val [ "{{EX_ENABLE_PASSWORD}}" ]
    !
    variable EX_HOSTNAME
     val [ {{EX_HOSTNAME}} ]
    !
    variable EX_SERVICE_IP
     val [ {{EX_SERVICE_IP}} ]
    !
    variable EX_SERVICE_MASK_LENGTH
     val [ {{EX_SERVICE_MASK_LENGTH}} ]
    !
    variable EX_MGMT_IP
     val [ {{EX_MGMT_IP}} ]
    !
    variable EX_MGMT_MASK_LENGTH
     val [ {{EX_MGMT_MASK_LENGTH}} ]
    !
    variable EX_DATA_VPN_NUMBER
     val [ {{EX_DATA_VPN_NUMBER}} ]
    !
    variable EX_MANAGEMENT_VPN_NUMBER
     val [ {{EX_MANAGEMENT_VPN_NUMBER}} ]
    !
   !
  !
 !
!
single-ip-mode vm-name deployment-ROUTER_1.deployment-ROUTER_1
!
vpn 0
interface int-mgmt-net-br
  no shutdown
  tunnel-interface
   color bronze
   no allow-service bgp
```

```
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
    allow-service https
    encapsulation ipsec
   !
!
```