

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 1
- Prerequisites to Onboard NFVIS WAN Edge Devices using PnP Process, on page 2
- Onboarding NFVIS device using Plug-and-Play process, on page 3

Prerequisites for NFVIS WAN Edge Onboarding

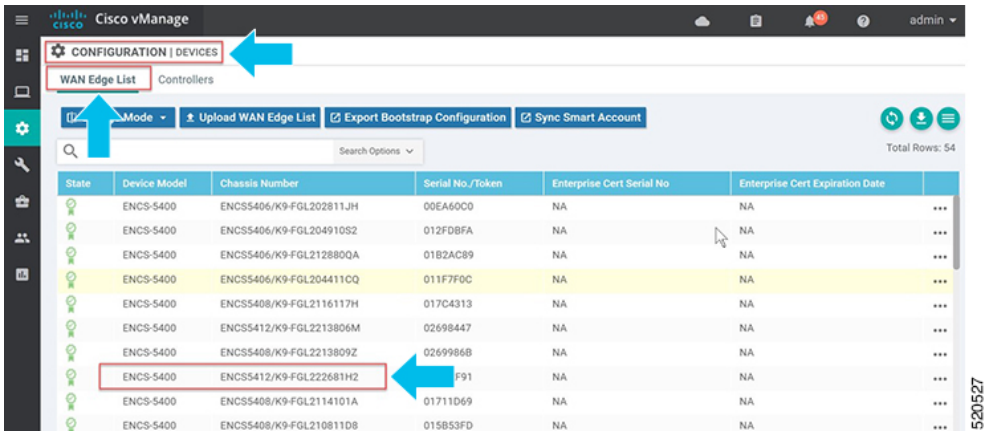
Ensure that the following prerequisites are met before proceeding with the WAN Edge onboarding process:

- 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.

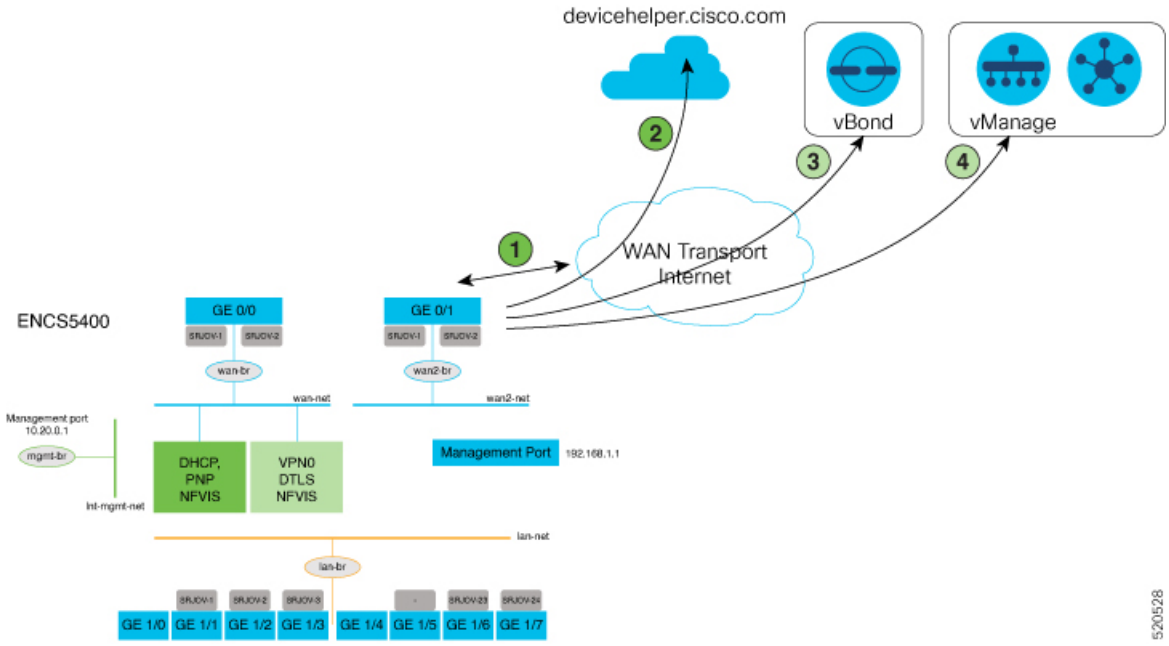
  Navigate to **Cisco Software Central** > **Network Plug and Play** > **Plug and Play Connect** > **Devices**, verify the device is available with **Controller** profile associated to it.

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:

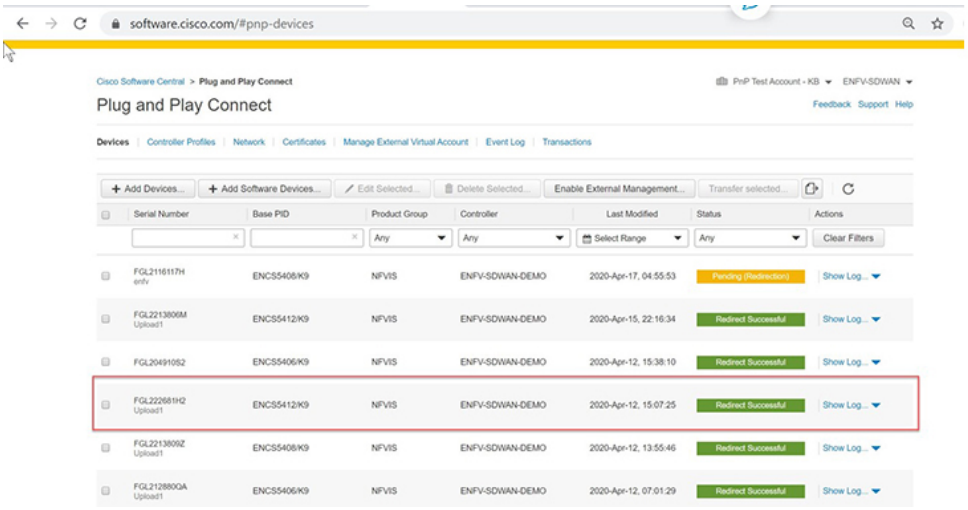
```
vpn 0
 interface MGMT
  no shutdown
  tunnel-interface
   color red
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service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

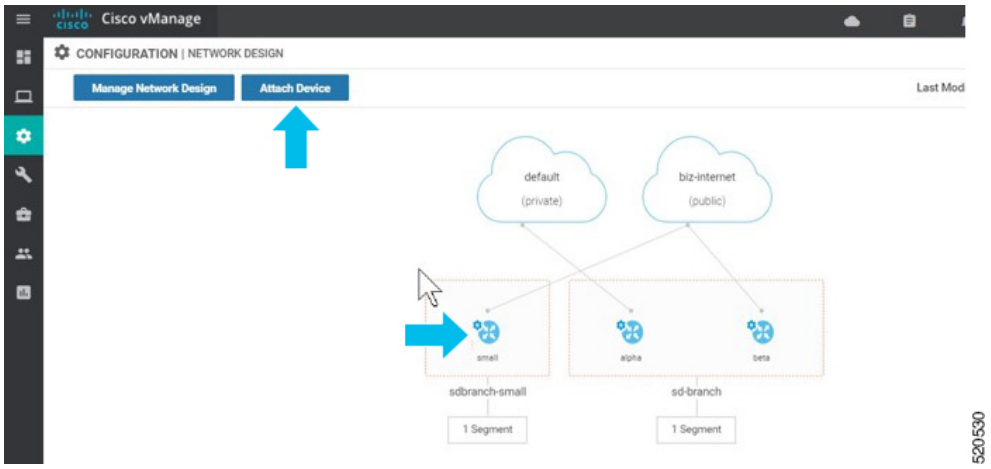
   - At this stage, the PnP portal indicates a **Redirect Successful** status when the WAN Edge device is redirected through PnP to the Cisco SD-WAN Validator controller.

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

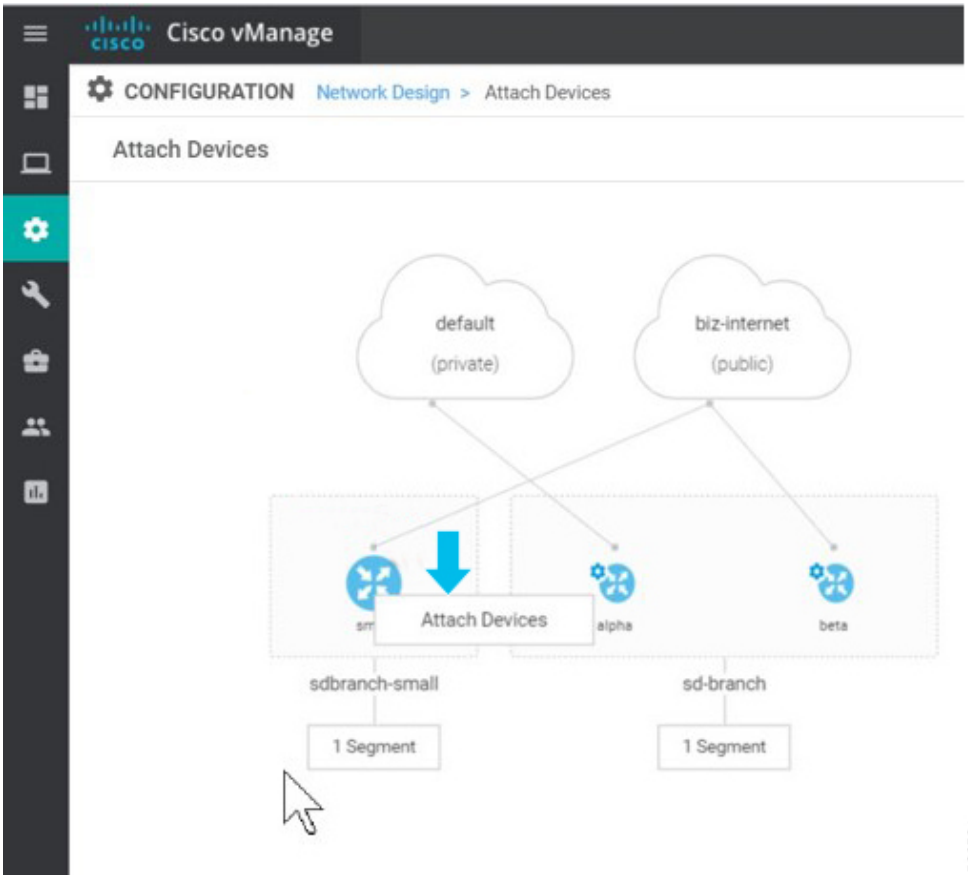


3. After authentication with the Cisco SD-WAN Validator, Cisco SD-WAN Manager information is available to the NFVIS WAN Edge device to register and establish a secure connection.

   - 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.

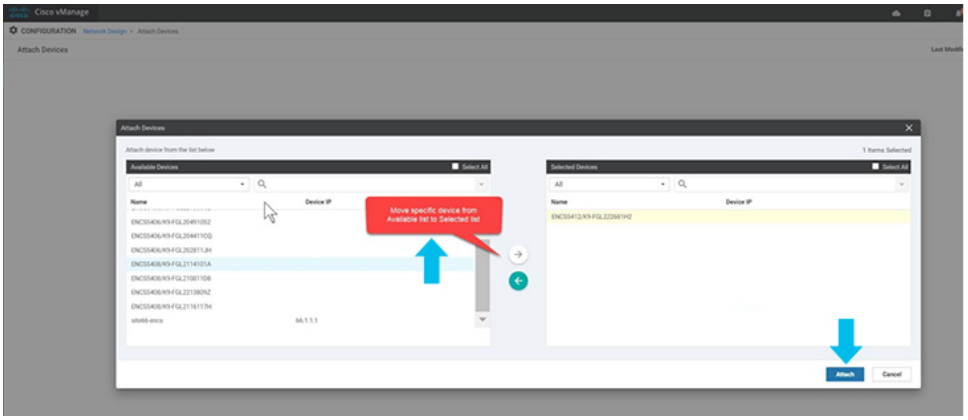


     - Click **Attach Devices**.



- 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.

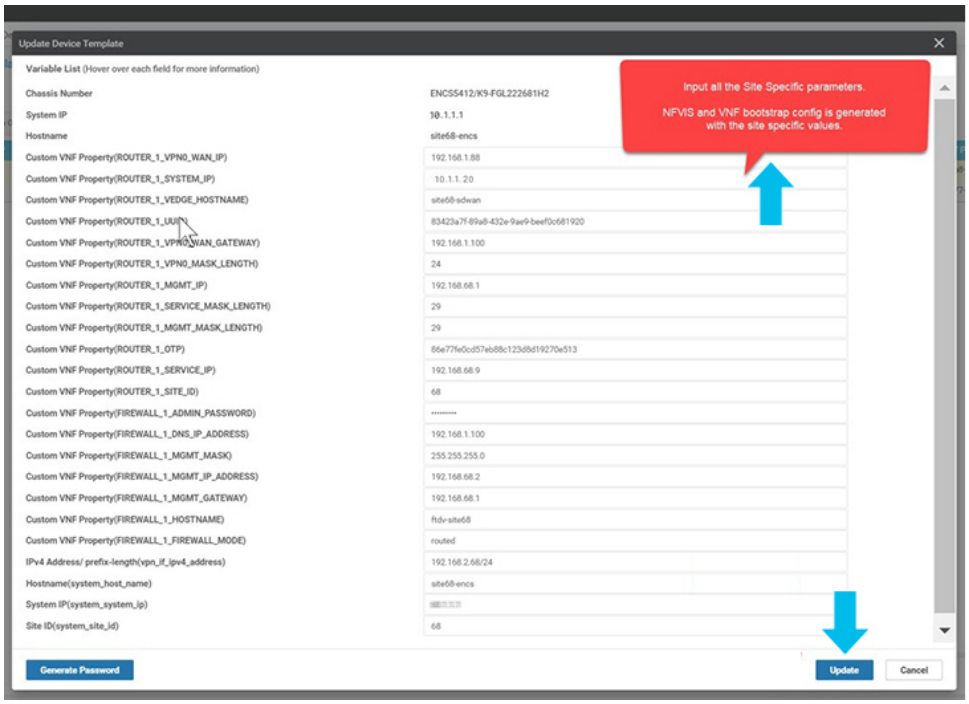
  Click **Attach**.



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



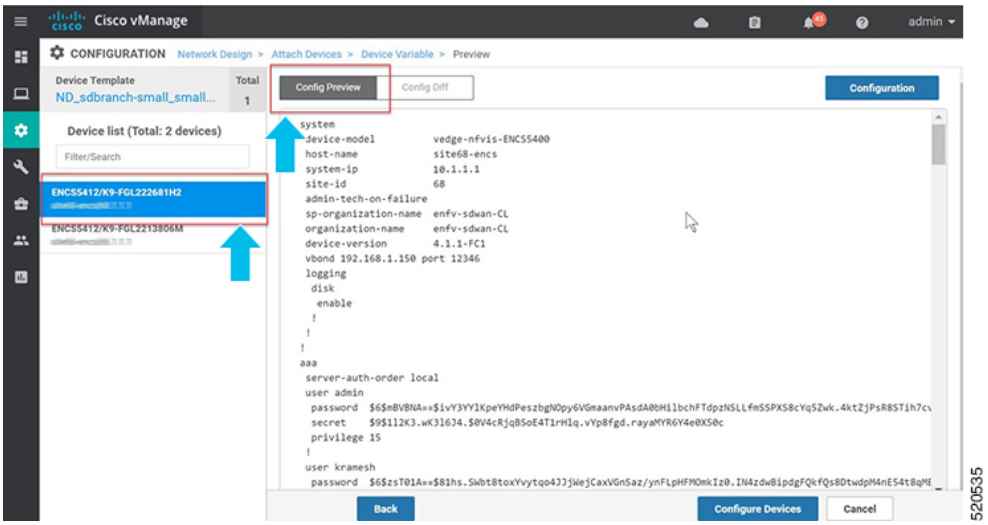
- You can update all the site specific parameters and the click **Update**.



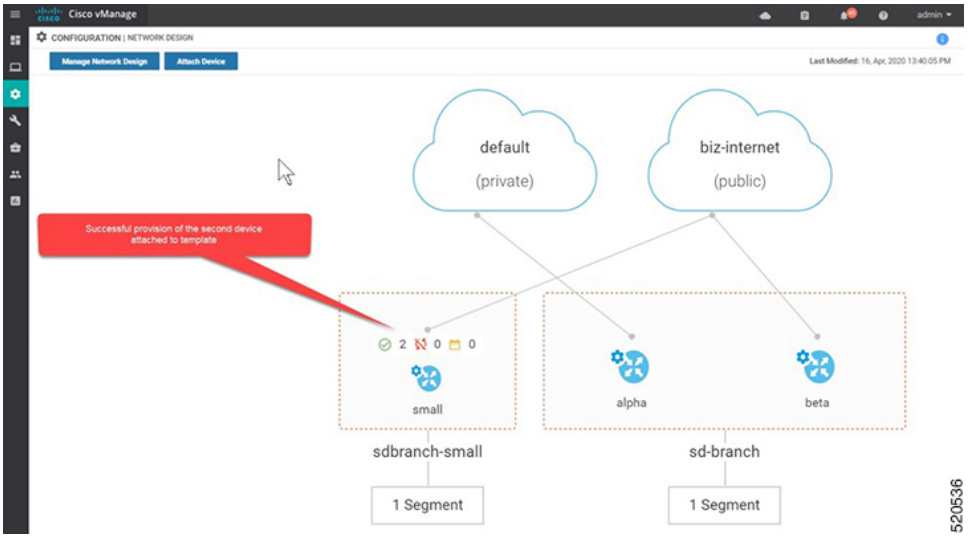
- Click on the name of the device and choose **config preview**. You can preview the configuration associated to the selected device.

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

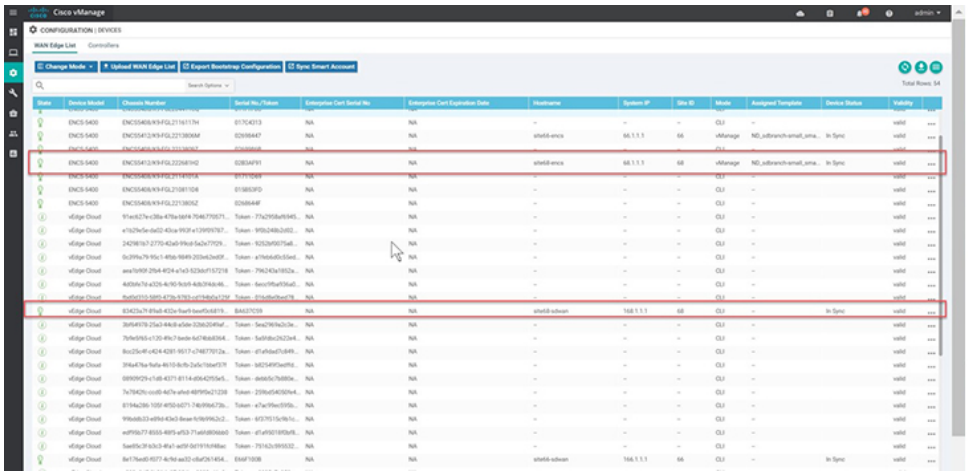
  Click **Configure Devices** to push the configuration to the devices.



- 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.