

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

Table 1: 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 1
- Define Cisco Catalyst 8300 Series Edge uCPE In Cisco SD-WAN Manager, on page 2
- Design Cisco NFVIS Service Chain Using Cisco SD-WAN Manager, on page 4
- Deploy Cisco Catalyst 8300 Series Edge uCPE to Cisco SD-WAN Manager, on page 6
- Operate Cisco Catalyst 8300 Series Edge uCPE Using Cisco SD-WAN Manager, on page 7

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 2: 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.