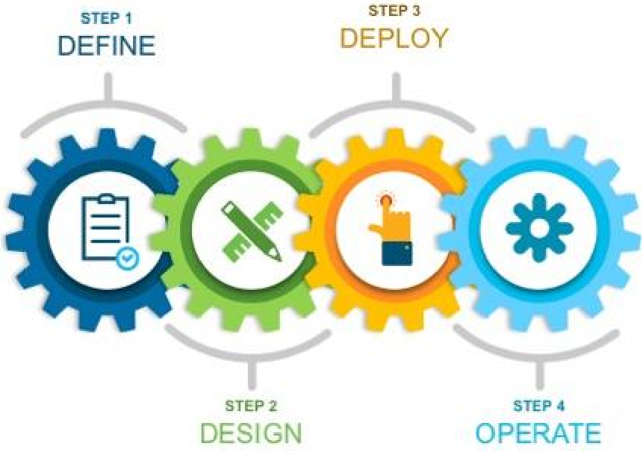
Validated Profile: Wireless Automation Deployment Using Cisco DNA Center

Revised: January 23, 2024

Solution Overview

This guide explains how to use Cisco DNA Center 2.3.5.5 to deploy and manage a legacy wireless local area network (WLAN) within an enterprise network, using Cisco Catalyst 9800 Series Wireless Controllers, Cisco IOS XE Cupertino 17.9.4a.

This guide provides technical guidance to design, deploy, and operate a Cisco WLAN using Cisco DNA Center.



This guide contains the following main sections:

- *Define the wireless network* presents a high-level overview of the campus, remote office, and cloud-based WLAN that is designed and deployed through Cisco DNA Center.
- *Design the wireless network* discusses the integration of Cisco DNA Center with Cisco Identity Services Engine (Cisco ISE); creation of the site hierarchy—including the importing of floor maps—within Cisco DNA Center; configuration of various network services necessary for network operations, such as AAA, DNS, DHCP, NTP, SNMP, and Syslog servers; and configuration of wireless settings, including WLANs/SSIDs, VLANs, and RF profiles for the WLAN deployment.
- *Deploy the wireless network* discusses discovery of the wireless controllers, managing the software images running on the wireless controllers, configuring HA SSO redundancy on the wireless controllers, provisioning the enterprise and guest wireless controllers within Cisco DNA Center, joining APs to the enterprise wireless controller HA SSO pair, provisioning the APs within Cisco DNA Center, and positioning the APs on the floor maps within Cisco DNA Center.
- *Monitor and operate the wireless network* discusses how to use Cisco DNA Assurance to monitor and troubleshoot the WLAN deployment.

The audience for this guide includes network design engineers and network operations personnel who want to use Cisco DNA Center to deploy a Cisco WLAN within their wireless networks.

Prerequisites

Before you can deploy and manage a legacy WLAN within an enterprise network, Cisco DNA Center must be installed and properly configured. For more information about installing and configuring Cisco DNA Center, see the *Cisco DNA Center Installation Guide*.

The following table displays the round-trip time (RTT) requirements between Cisco DNA Center and the specified network elements.

The latency between the Cisco DNA Center appliance and a managed device should be ~100 milliseconds RTT or less. After 100 milliseconds, longer execution times could be experienced for certain events, such as inventory collection, provisioning, and image update (SWIM). Cisco does not support an RTT of more than 300 milliseconds. For more details on RTT and supported scale, see the *Cisco DNA Center Data Sheet*.

Table 1: Cisco Recommended RTT

Source Device	Target Device	Maximum RTT Supported
Cisco DNA Center Node	Cisco DNA Center Node	10 milliseconds
Cisco DNA Center Node	Cisco ISE	300 milliseconds
Cisco DNA Center Node	Wireless Controller	200 milliseconds
Wireless Controller	Access Points	20 milliseconds (local mode)
Wireless Controller	Access Points	300 milliseconds (flex mode)
Wireless Controller	Cisco ISE	100 milliseconds

Table 2: Cisco Supported Scale Numbers for Wireless Controller Models

Wireless Controller Model	Maximum Number of APs	Maximum Number of Clients
Catalyst 9800-L	250	5000
Catalyst 9800-40	2000	32,000
Catalyst 9800-80	6000	64,000
Catalyst 9800-CL (4 CPU/8 GB RAM)	1000	10,000
Catalyst 9800-CL (6 CPU/16 GB RAM)	3000	32,000
Catalyst 9800-CL (10 CPU/32 GB RAM)	6000	64,000

Table 3: Cisco DNA Center 1-Node System Scale

SKU	DN-SW-APL	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
Legacy Devices (switch, router, wireless controller)	1000	1000	2000	5000
Legacy Wireless Access Points	4000	4000	6000	13,000
Wireless Sensors	600	600	800	1600
Concurrent Endpoints	25,000	25,000	40,000	100,000
Transient Endpoints (over a 14-day period)	75,000	75,000	120,000	250,000

SKU	DN-SW-APL	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
Ratio of Endpoints to Wired	Any	Any	Any	Any
Ratio of Endpoints to Wireless	Any	Any	Any	Any
Site Elements	2500	2500	5000	10,000
Wireless Controller	500	500	1000	2000
Ports	48,000	48,000	192,000	768,000
API Rate Limit (APIs/minute)	50	50	50	50
NetFlow (flows/second)	30,000	30,000	48,000	120,000
Concurrent Software Image Updates	100	100	100	100

Table 4: Scale for 3-Node DN2-HW-APL-XL Cluster

Description	Supported Scale
Devices (switch, router, wireless controller)	10,000
Wireless Access Points	25,000
Concurrent Endpoints	300,000
Transient Endpoints (over a 14-day period)	750,000
NetFlow (flows/second)	250,000
Number of Floors (per wireless controller)	1000

Required Network Ports

Cisco DNA Center requires that specific ports are open for traffic flows to and from the appliance, whether you open them using firewall settings or a proxy gateway. For more information, see the "Required Network Ports" topic in the *Cisco DNA Center Second-Generation Appliance Installation Guide*.

Certificate Management for Cisco DNA Center

By default, Cisco DNA Center uses self-signed certificates, but you can use a certificate that is signed by your internal certificate authority during deployment. To replace the default certificate, see the "Manage Certificates" topic in the *Cisco DNA Center Security Best Practices Guide*.

Define the Wireless Network

This section presents a high-level overview of the campus, remote office, and cloud-based WLAN that is designed and deployed through Cisco DNA Center.

There are three scenarios that outline three types of typical, legacy wireless deployments. In the first scenario, a campus wireless deployment with APs in local mode uses wireless controllers in a high availability (HA) configuration; the wireless controllers are located in the same campus building. In the second scenario, a remote office wireless deployment with APs in flex mode uses wireless controllers in an N+1 configuration; the wireless controllers are located in the data center. In the third scenario, a wireless network for a corporate event uses a wireless controller that is hosted in a cloud environment, such as Amazon Web Services (AWS).

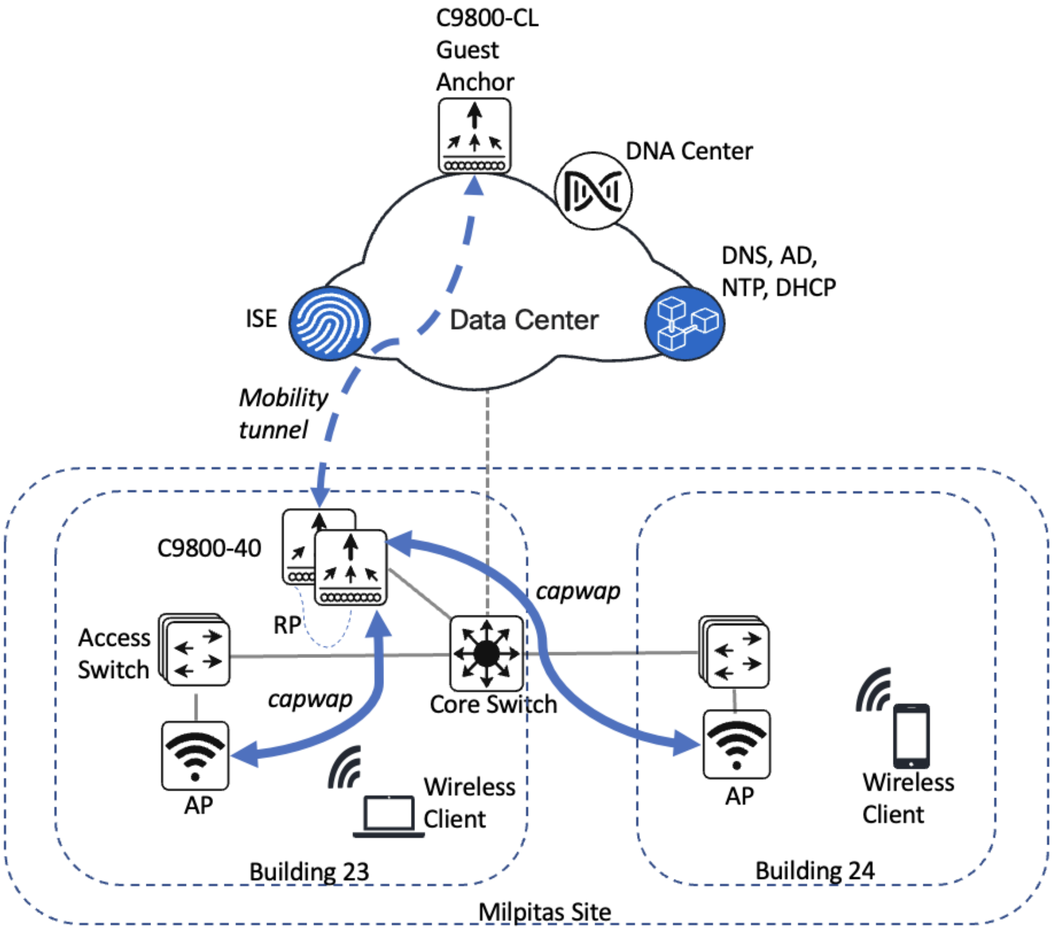
Campus Wireless Deployment

The campus wireless deployment uses a pair of Cisco Catalyst 9800-40 Wireless Controllers in a high availability (HA) SSO configuration. Located on multiple floors within multiple buildings of the campus, the wireless controller pair functions as the enterprise wireless controller for access points (APs) in local mode. Wireless guest access is provided through a separate Cisco Catalyst 9800-CL Wireless Controller, which functions as a traditional guest wireless controller and is anchored to the enterprise (foreign) wireless controller.

The design and deployment of the WLAN is fully automated, utilizing intent-based networking (IBN). Cisco DNA Center is designed for IBN and provides a level of abstraction from the device-level user interface.

Note In the production environment, the guest anchor wireless controller is typically connected to a DMZ segment off of a firewall to separate guest wireless traffic from internal employee traffic. In such designs, the firewall policy must be configured to allow the necessary traffic between the enterprise foreign wireless controller and the guest anchor wireless controller.

Figure 1: High-Level Design for Campus Wireless Deployment



The campus wireless deployment includes the following features:

- Site hierarchy consisting of a single area (**Milpitas**) and multiple buildings (**Building 23** and **Building 24**), each with multiple floors (**Floor 1** and **Floor 2**)
- Legacy, centralized campus wireless deployment in which all wireless traffic is backhauled to the wireless controller
- Enterprise SSID and guest SSID
- A single pair of enterprise Catalyst 9800-40 Wireless Controllers in an HA SSO configuration
- Guest wireless access through a dedicated guest Catalyst 9800-CL Wireless Controller, which is auto-anchored to the enterprise HA SSO wireless controller pair

Note The Cisco DNA Center CLI templates can be used to configure anything that cannot be configured through the intent-based profiles and/or the model config. This guide discusses the specific wireless controller features that can be configured in Cisco DNA Center.

Wireless controllers must be assigned to sites during the Cisco DNA Center provisioning process. For this deployment guide, a Catalyst 9800-40 Wireless Controller HA SSO pair (**C9800-40**) will be assigned to **Building 23** within the **Milpitas** area. There can only be one primary enterprise (nonguest) wireless controller for the APs on a floor at a given time, meaning that only one enterprise wireless controller can be provisioned per floor within Cisco DNA Center. The APs on **Floor 1** and **Floor 2** within **Building 23** and the APs on **Floor 1** within **Building 24** will be provisioned to **C9800-40** through Cisco DNA Center.

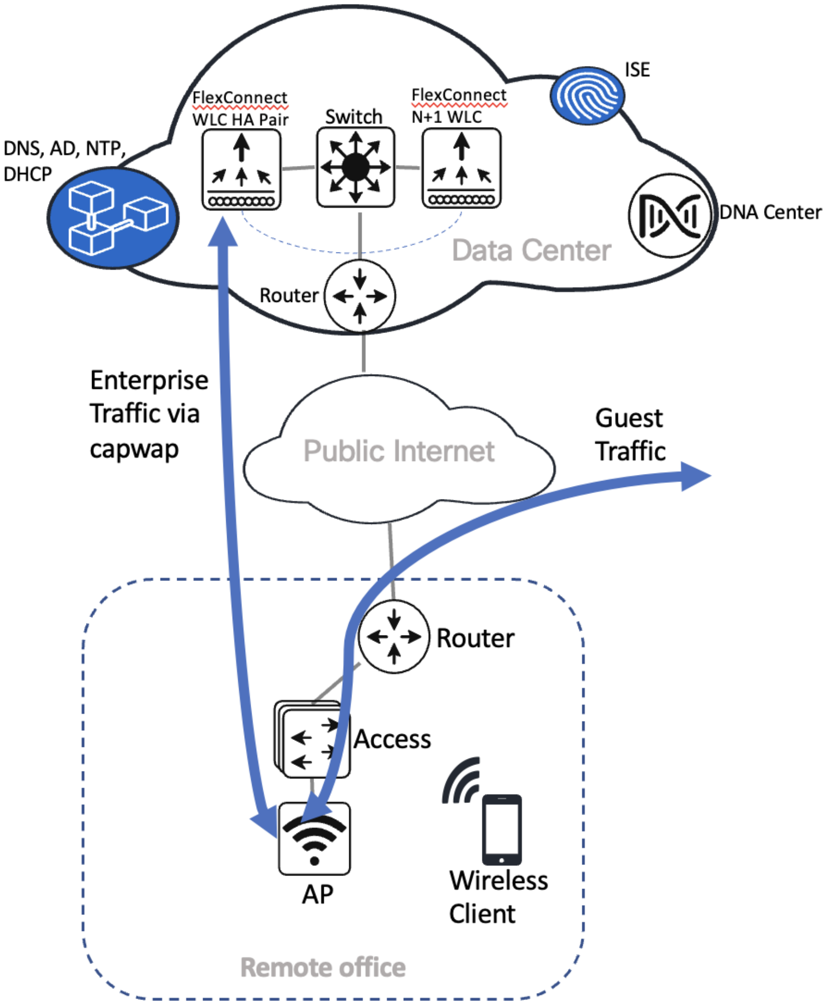
Remote Office Wireless Deployment

The remote office wireless deployment uses a pair of Cisco Catalyst 9800-40 Wireless Controllers in a high availability (HA) N+1 configuration. Located on multiple floors within a remote office building, the wireless controller pair functions as the enterprise wireless controller for access points (APs) in flex mode. Wireless guest access is locally switched, and employee (nonguest) wireless traffic is centrally switched. All authentication, whether for employee (WPA2/802.1X) or guest (WebAuth) wireless traffic, is centrally performed through Cisco ISE, highlighting the use of Cisco ISE as both a AAA server and a guest portal.

The design and deployment of the WLAN is fully automated, utilizing intent-based networking (IBN). Cisco DNA Center is designed for IBN and provides a level of abstraction from the device-level user interface.

Note Alternate designs for guest wireless traffic, including local termination with Direct Internet Access (DIA) at the remote office, may be implemented when combining WLAN functionality with Cisco SD-WAN. For more information, see *Cisco SD-WAN: Enabling Direct Internet Access*.

Figure 2: High-Level Design for Remote Office Wireless Deployment



The remote office wireless deployment includes the following features:

- Site hierarchy consisting of a single area (**New York**) and a single building (**Branch 5**) with multiple floors (**Floor 1**, **Floor 2**, and **Floor 3**)
- Legacy, flex mode in which data traffic is centrally switched for the enterprise SSID and locally switched for the guest SSID
- Enterprise SSID and guest SSID
- A single pair of enterprise Catalyst 9800-40 Wireless Controllers in an HA N+1 configuration

Note The Cisco DNA Center CLI templates can be used to configure anything that cannot be configured through the intent-based profiles and/or the model config.

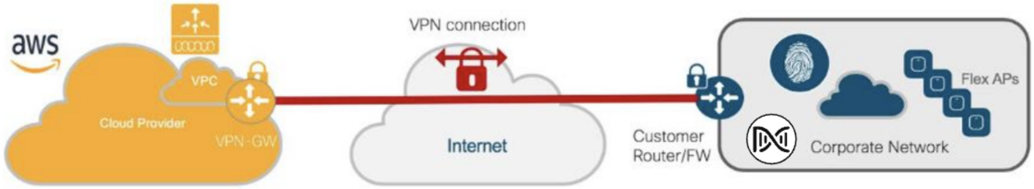
The wireless controllers must be assigned to sites during the Cisco DNA Center provisioning process. For this deployment guide, a Catalyst 9800-40 Wireless Controller HA SSO pair (**C9800-40**) will be assigned to **Branch 5** within the **New York** area, even though the pair is physically located in the data center. There can be only one primary enterprise (nonguest) wireless controller for the APs on a floor at a given time, meaning only one enterprise wireless controller can be provisioned per floor within Cisco DNA Center. The APs on **Floor 1** and **Floor 2** within **Branch 5**, **New York** will be provisioned to **C9800-40** through Cisco DNA Center.

Wireless Controller Hosted on AWS Deployment

This wireless deployment uses a Cisco Catalyst 9800-CL Wireless Controller hosted on Amazon Web Services (AWS). Located on an event center floor, the wireless controller is configured as the enterprise wireless controller for access points (APs) in flex mode. All authentication, whether for employee (WPA2/802.1X) or guest (WebAuth) wireless traffic, is centrally performed through Cisco ISE and located in the data center.

Cisco DNA Center is designed for IBN and provides a level of abstraction from the device-level user interface.

Figure 3: High-Level Design for Cisco Catalyst 9800-CLWireless Controller Hosted on AWS



This wireless deployment includes the following features:

- Site hierarchy consisting of a single area (**San Jose**) with an event center (**Eventcenter**) that has a single floor (**Eventcenterfloor**)
- Legacy, flex wireless deployment where all wireless traffic is backhauled to the wireless controller
- Flex mode in which data traffic is locally switched
- Enterprise SSID and corporate special event SSID
- A Catalyst 9800-CL Wireless Controller hosted on AWS

Note The Cisco DNA Center CLI templates can be used to configure anything that cannot be configured through the intent-based profiles and/or the model config.

The wireless controllers must be assigned to sites during the Cisco DNA Center provisioning process. For this deployment guide, a Catalyst 9800 Wireless Controller (**C9800-CL**) on AWS will be assigned to **Eventcenter** within the **San Jose** area. There can be only one primary enterprise (nonguest) wireless controller for the APs on a floor at a given time, meaning only one enterprise wireless controller can be provisioned per floor within Cisco DNA Center. The APs on **Eventcenterfloor** within **Eventcenter** will be provisioned to **C9800-CL** on AWS through Cisco DNA Center.

Migration from the Legacy Network

This section provides an overview of the following migrations from the legacy network, using Cisco AireOS Wireless Controller or Cisco Prime Infrastructure:

- Legacy Cisco AireOS Wireless Controller to Cisco Catalyst 9800 Series Wireless Controller

- Cisco Prime Infrastructure to Cisco DNA Center

Migrate APs from a Legacy Cisco AireOS Wireless Controller to a Cisco Catalyst 9800 Series Wireless Controller

This section explains how to migrate access points (APs) from a legacy Cisco AireOS Wireless Controller to a Cisco Catalyst 9800 Series Wireless Controller. For this migration, the minimum AireOS version that is required is 8.5, with support for IRCM.

Procedure

Step 1 Add a temporary floor to the legacy site, which is managed by the Cisco AireOS Wireless Controller.

Step 2 Discover the Catalyst 9800 Series Wireless Controller and provision the wireless controller to the legacy site that manages the newly added floor.

Step 3 Enter the interface details, such as VLAN for legacy flow.

Step 4 Configure a mobility tunnel between the Cisco AireOS Wireless Controller and the Catalyst 9800 Series Wireless Controller.

Step 5 Migrate the APs to the Catalyst 9800 Series Wireless Controller using one of the following methods:

Note The APs will be migrated to a new wireless controller using the AP config workflow, which will configure the new wireless controller as the primary wireless controller.

a) Iterative migration: Only specific APs on a floor are migrated (Milpitas/Building 23/Floor2).

1. On a single floor, identify *some* of the APs that need to be moved from the Cisco AireOS Wireless Controller to the Catalyst 9800 Series Wireless Controller.

   Do not select all the APs on a single floor.

2. Create a new temporary floor (Floor 2_1) that is managed by the Catalyst 9800 Series Wireless Controller.

3. Move the subset of APs to the Catalyst 9800 Series Wireless Controller using the AP config workflow.

   Through the workflow, the Catalyst 9800 Series Wireless Controller will be configured as the primary wireless controller.

4. Once the subset of APs join the Catalyst 9800 Series Wireless Controller, provision the APs to Catalyst 9800 Series Wireless Controller, which is a part of Floor 2_1.

   At this point, a subset of APs are now managed by the Catalyst 9800 Series Wireless Controller, and the remaining APs are managed by the Cisco AireOS Wireless Controller. As a result, service is not disrupted on that floor.

5. Iteratively move the remaining APs from the floor to the Catalyst 9800 Series Wireless Controller.

b) Floor-by-floor migration: An entire set of APs on a floor are migrated to the Catalyst 9800 Series Wireless Controller.

1. Create a new temporary floor (Floor 2_1) that is managed by the Catalyst 9800 Series Wireless Controller.

2. Move all the APs on a single floor to the Catalyst 9800 Series Wireless Controller.

3. Provision the APs to the Catalyst 9800 Series Wireless Controller, which is a part of Floor 2_1.

4. Provision the Catalyst 9800 Series Wireless Controller to manage Floor 2.

5. Either iteratively or by entire floor, provision the APs to Floor 2.

6. Delete the temporary floor, Floor 2_1.

7. Repeat the first six steps in substep b for your desired sites, buildings, and floors.

8. Delete the temporary floor created in Step 1.

Step 6 (Optional) Remove the Cisco AireOS Wireless Controller from the inventory using the config cleanup option.

Migrate from Cisco Prime Infrastructure to Cisco DNA Center

Before you begin

- Using the *Cisco Prime Infrastructure and Cisco DNA Center Compatibility Matrix*, identify the Prime Data Migration Tool (PDMT) release that is compatible with your version of Cisco DNA Center.
- Download the compatible PDMT release using the Cisco Software Download Tool.

Procedure

Step 1 Perform a readiness check using the Cisco Prime Infrastructure Cisco DNA Center Assessment and Readiness Tool (PDART).

For more information about using PDART, see Use PDART - a Cisco DNA Center Readiness Tool.

Step 2 Once you have assessed the readiness of the migration, use the PDMT to migrate your sites and devices from Cisco Prime Infrastructure to Cisco DNA Center.

Design the Wireless Network

Ensure that the prerequisites are met, as described in Prerequisites.

This section contains the following topics and processes:

- Integrate Cisco Identity Services Engine (ISE) with Cisco DNA Center
- Cisco ISE and third-party AAA server
- Configure the site hierarchy in Cisco DNA Center
- Configure network services for network operation
- Campus wireless deployment settings
- Remote office wireless deployment settings
- Design the Cisco Catalyst 9800-CL Wireless Controller hosted on AWS

Integrate Cisco ISE with Cisco DNA Center

The integration of Cisco Identity Services Engine (ISE) with Cisco DNA Center enables the sharing of information between the two platforms, including device and group information. Specific to this guide, the integration allows you to create a guest portal in Cisco

ISE through a workflow in Cisco DNA Center. The guest portal is created when the guest wireless network is defined within a wireless profile in Cisco DNA Center. For more information, see Campus Wireless Deployment Settings, on page 30.

Use the following procedures to integrate Cisco ISE with Cisco DNA Center:

- Configure Cisco ISE as an authentication policy server

  See Configure Cisco ISE as an Authentication and Policy Server to Cisco DNA Center, on page 12.

- Allow pxGrid connectivity from Cisco DNA Center into Cisco ISE

  See the "Cisco pxGrid Cloud and Cisco ISE Integration" topic in the *Cisco pxGrid Cloud Solution Guide*.

Cisco ISE and Third-Party AAA Server

Even though Cisco DNA Center supports third-party AAA servers for RADIUS and TACACS+ authentications, Cisco ISE provides additional analytics for endpoints.

Configure Cisco ISE as an Authentication and Policy Server to Cisco DNA Center

Before you begin

To complete this action, your user profile must be assigned the SUPER-ADMIN-ROLE or the NETWORK-ADMIN-ROLE.

Procedure

Step 1 Log in to the Cisco DNA Center web console using an IP address or a fully qualified domain name.

Example:

https://<*Cisco_DNA_Center_IPaddr_or_FQDN*>

Step 2 From the top-left corner, click the menu icon and choose **System** > **Settings**.

Step 3 In the left pane, from the **External Services** drop-down list, choose **Authentication and Policy Servers**.

Step 4 From the **Add** drop-down list, choose **ISE**.

The **Add ISE server** slide-in pane is displayed.

Step 5 Enter the server details in the required fields.

The following table describes the fields in the **Add ISE server** slide-in pane.

Field	Settings	Description
Server IP Address	Text Field	IP address of the Cisco ISE server. If multiple IP addresses are configured, ensure this IP address is shown on the Cisco ISE deployment instance.
Shared Secret	Text Field	The shared secret used by network devices for communicating with the Cisco ISE server. Within the IOS XE device configuration, this is known as the PAC key.
Username	Text Field	The username of the default super admin account, which you created during Cisco ISE installation.

Field	Settings	Description
Password	Text Field	The password of the default super admin account, which you created during Cisco ISE installation.
FQDN	Text Field	The fully qualified domain name of the Cisco ISE server.
Virtual IP Address	Text Field	One or more Policy Services Nodes (PSNs) may be behind a single load balancer. When this happens, you can add the load balancer IP(s) in the **Virtual IP** field.
Advanced Settings > Protocol	Multiple Choice Radio Button	Determines the authentication protocol(s). You can choose from the following protocol options: • RADIUS: The default setting, which uses the RADIUS protocol. • TACACS: Uses the TACACS protocol.
Advanced Settings > Authentication Port	Text Field	When RADIUS is selected, the default port is 1812.
Advanced Settings > Accounting Port	Text Field	When RADIUS is selected, the default port is 1813.
Advanced Settings > Port	Text Field	This field appears only when TACACS is selected. The default port is 49.
Retries	Number	The number of authentication retries before failure. The default is 3 retries.
Timeout (seconds)	Number	The number of seconds before an attempt times out. The default is 4 seconds.

For this design and deployment guide, the following information was entered.

Field	Value
Server IP Address	172.23.240.152
Shared Secret	—
Cisco ISE Server	On
Username	admin
Password	—
FQDN	cvdise31.cagelab.local
Subscriber Name	admin
SSH Key	—
Virtual IP Address	—

Field	Value
Advanced Settings > Protocol	RADIUS
Advanced Settings > Authentication Port	1812
Advanced Settings > Accounting Port	1813
Retries	3
Timeout (seconds)	4

Note Before adding Cisco ISE, confirm that the following prerequisites are met:

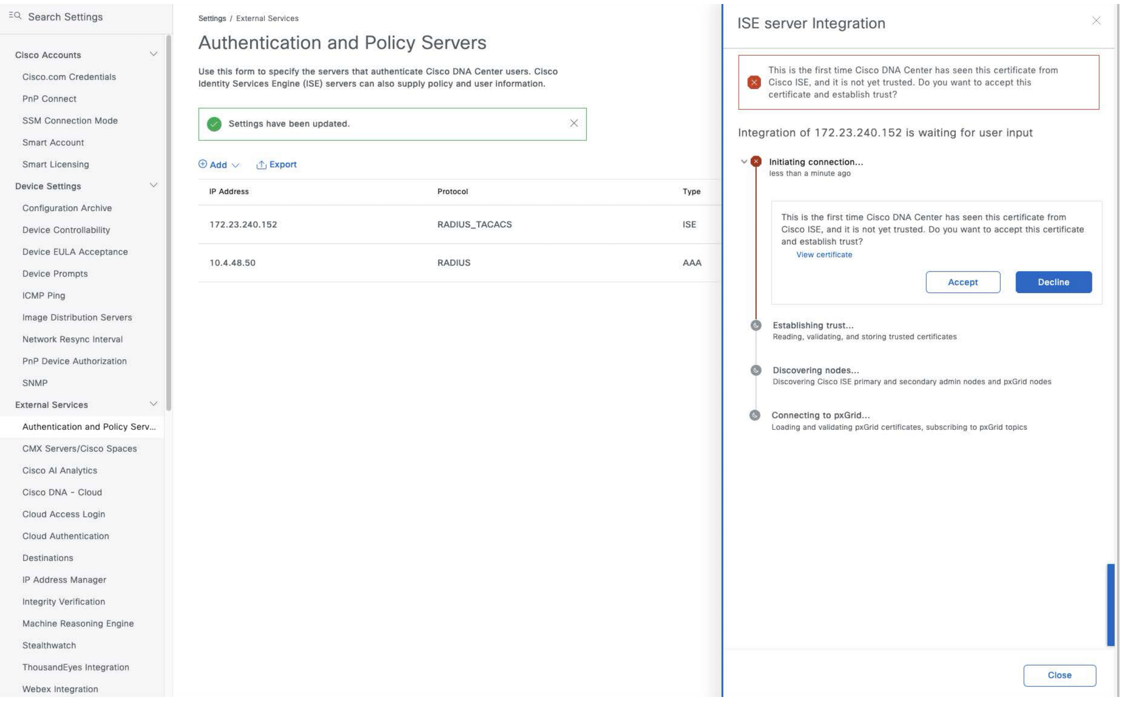
- Your version of Cisco ISE is compatible with your version of Cisco DNA Center.

  For more information, see the *Cisco DNA Center* Compatibility Matrix.

- The Cisco ISE GUI password matches the Cisco ISE CLI password.
- PxGrid is enabled for the Cisco ISE deployment instance.
- The ERS on the Cisco ISE server is enabled for read/write.

Step 6 Click **Add** to create the Cisco ISE server within Cisco DNA Center.

The **ISE server Integration** slide-in pane displays a message about accepting the Cisco ISE certificate and establishing trust.



Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

Settings have been updated.

IP Address	Protocol	Type
172.23.240.152	RADIUS_TACACS	ISE
10.4.48.50	RADIUS	AAA

ISE server Integration

This is the first time Cisco DNA Center has seen this certificate from Cisco ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?

Integration of 172.23.240.152 is waiting for user input

Initiating connection...
less than a minute ago

This is the first time Cisco DNA Center has seen this certificate from Cisco ISE, and it is not yet trusted. Do you want to accept this certificate and establish trust?
View certificate

Establishing trust...
Reading, validating, and storing trusted certificates

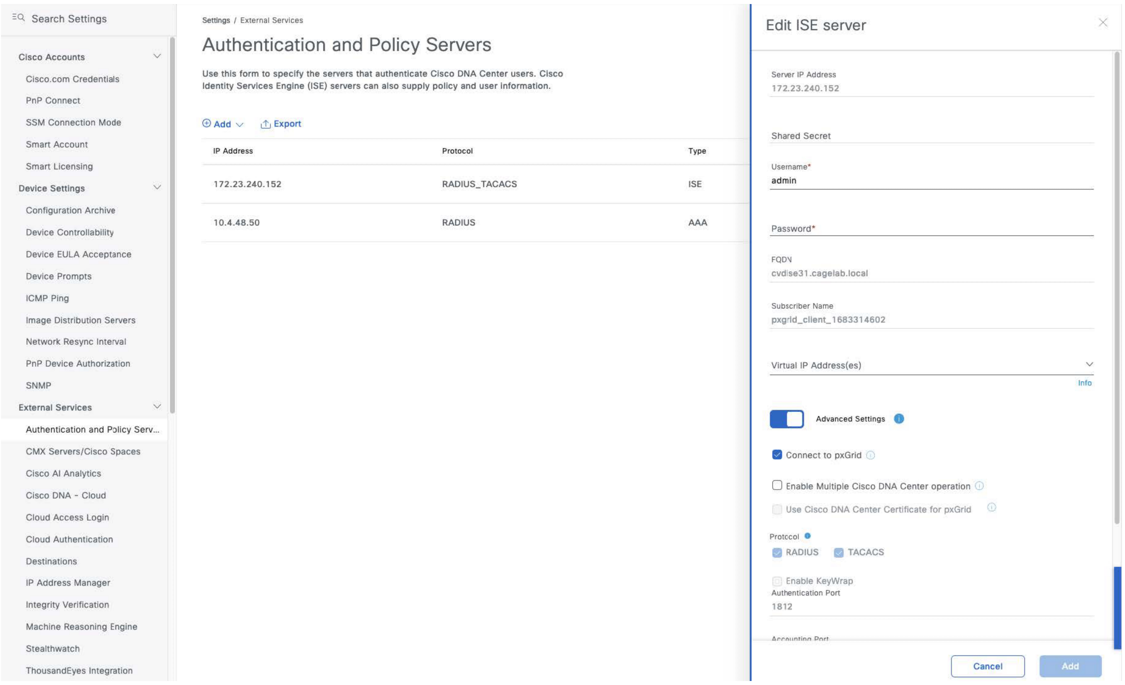
Discovering nodes...
Discovering Cisco ISE primary and secondary admin nodes and pxGrid nodes

Connecting to pxGrid...
Loading and validating pxGrid certificates, subscribing to pxGrid topics

Step 7 Click **Accept**.

After the integration is complete, the **Authentication and Policy Servers** window is displayed. The new Cisco ISE server should display an **ACTIVE** status.

If you want to change any server settings, hover your cursor over the ellipsis icon (•••) in the **Actions** column and choose **Edit**.



Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

IP Address	Protocol	Type
172.23.240.152	RADIUS_TACACS	ISE
10.4.48.50	RADIUS	AAA

Server IP Address: 172.23.240.152

Shared Secret

Username*: admin

Password*

FQDN: cvdise31.cagelab.local

Subscriber Name: pxgrid_client_1683314602

Virtual IP Address(es)

Advanced Settings

☑ Connect to pxGrid

□ Enable Multiple Cisco DNA Center operation

□ Use Cisco DNA Center Certificate for pxGrid

Protocol: ☑ RADIUS ☑ TACACS

□ Enable KeyWrap

Authentication Port: 1812

Accounting Port

Configure Site Hierarchy and Import Floor Maps

The configuration of the site hierarchy includes defining the network sites for deployment and defining the hierarchical relationships of the network sites, which consist of areas, buildings, and floors. Child sites automatically inherit certain attributes from parent sites, but you can override the attributes within the child site.

The following table summarizes the site hierarchy for this guide. A single area (**Milpitas**) is provisioned, containing multiple buildings (**Buildings 23** and **Building 24**) with multiple floors (**Floor 1** and **Floor 2**).

Name	Type of Site	Parent	Additional Information
Milpitas	Area	Global	—
Building 23	Building	Milpitas	Address: 560 McCarthy Boulevard, Milpitas, California 95035
Building 24	Building	Milpitas	Address: 510 McCarthy Boulevard, Milpitas, California 95035
Floor 1	Floor	Building 23	Dimensions: 200 ft. x 274 ft. x 10 ft. APs on this floor are provisioned to the Cisco Catalyst 9800 Series Wireless Controller HA pair.

Name	Type of Site	Parent	Additional Information
Floor 2	Floor	Building 23	Dimensions: 200 ft. x 274 ft. x 10 ft. APs on this floor are provisioned to the Cisco Catalyst 9800 Series Wireless Controller HA pair.
Floor 1	Floor	Building 24	Dimensions: 200 ft. x 250 ft. x 10 ft. APs on this floor are provisioned to the Cisco Catalyst 9800 Series Wireless Controller HA pair.
Floor 2	Floor	Building 24	Dimensions: 200 ft. x 250 ft. x 10 ft. APs on this floor are provisioned to the Cisco Catalyst 9800 Series Wireless Controller HA pair.

This section contains the following processes:

- Create an area
- Create a building within an area
- Create a floor in a building
- Create and position a planned AP by using the Cisco DNA Center GUI or by importing from Cisco Prime Infrastructure or Ekahau

Create an Area

Before you begin

To complete this action, your user profile must be assigned the SUPER-ADMIN-ROLE or the NETWORK-ADMIN-ROLE.

Procedure

Step 1 Login to the Cisco DNA Center web console using an IP address or a fully qualified domain name.

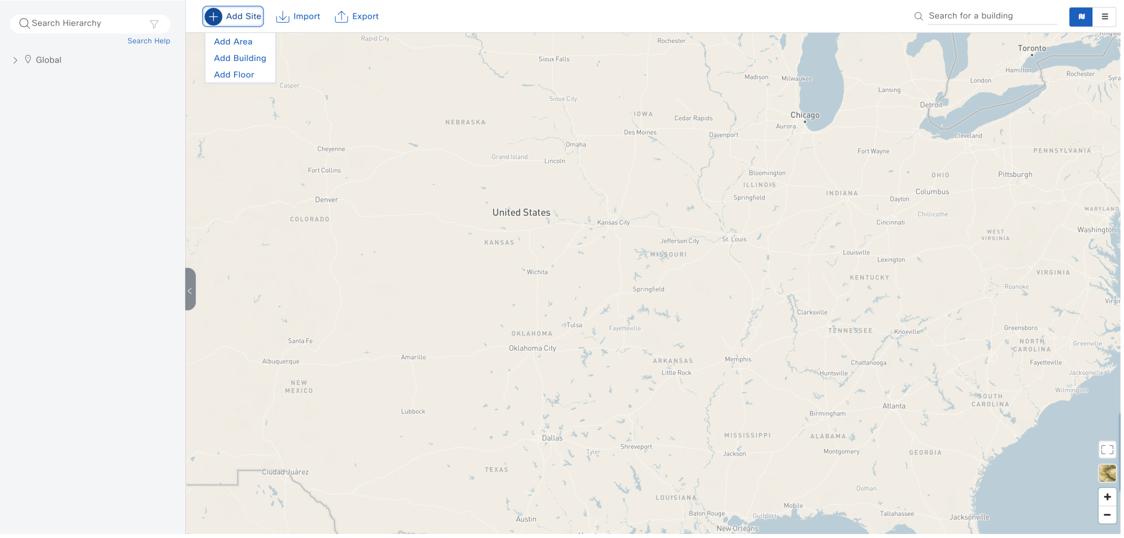
Example:

https://<Cisco_DNA_Center_IPaddr_or_FQDN>

Step 2 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

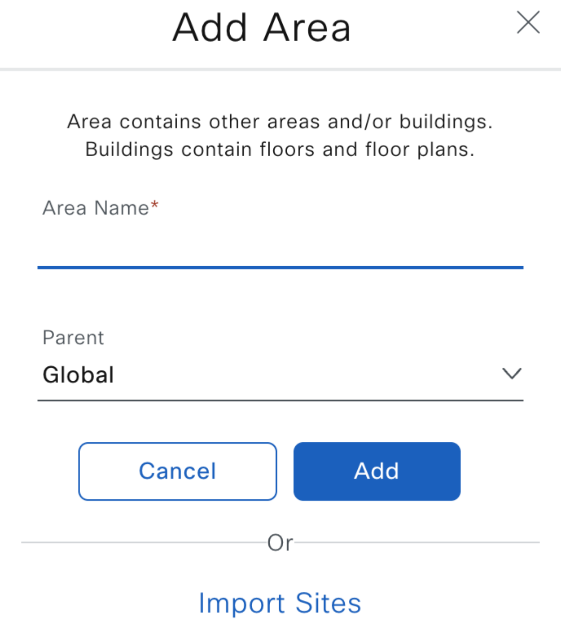
The **Network Hierarchy** window is displayed.

If this is the first time you have configured the network hierarchy, the left hierarchy pane may only display a single **Global** entry.



Step 3 Click **+ Add Site** > **Add Area**.

The **Add Area** dialog box is displayed.



Add Area

Area contains other areas and/or buildings.
Buildings contain floors and floor plans.

Area Name*

Parent
Global

Step 4 In the **Add Area** dialog box, from the **Parent** drop-down list, enter the **Area Name** and choose the desired parent.

For this deployment guide, choose **Global** for the **Parent** and create an area named **Milpitas** within an area named **US**.

Step 5 Click **Add**.

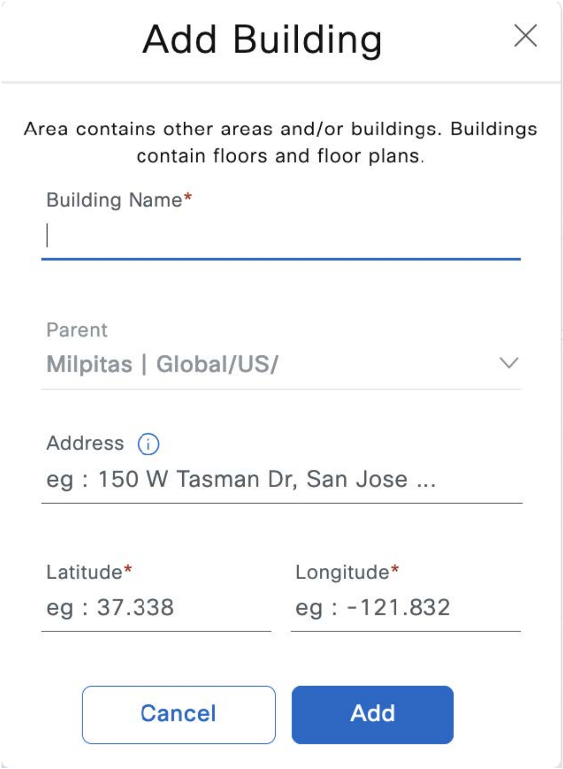
Create a Building Within an Area

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

Step 2 Click **+ Add Site** > **Add Building**.

The **Add Building** dialog box is displayed.



Add Building ×

Area contains other areas and/or buildings. Buildings contain floors and floor plans.

Building Name*

Parent

Milpitas | Global/US/

Address ⓘ

eg : 150 W Tasman Dr, San Jose ...

Latitude*

eg : 37.338

Longitude*

eg : -121.832

Cancel Add

Step 3 In the **Add Building** dialog box, enter the **Building Name** and choose the desired area from the **Parent** drop-down list.

For this deployment guide, enter **Building 23** for the **Building Name**. For the **Parent**, choose **Milpitas | Global/US**.

Step 4 Enter the building address or GPS coordinates using one of the following methods:

- In the **Address** field, enter the building address and choose the correct address from the list of available options. Latitude and longitude will be automatically entered in the **Latitude** and **Longitude** fields for the chosen address.
- Enter the GPS coordinates of the building in the **Latitude** and **Longitude** fields. If you use this method, you do not need to enter an address.

For this deployment guide, enter the address **560 McCarthy Boulevard, Milpitas, California 95035**, which is configured for **Building 23**.

Step 5 Click **Add**.

For this deployment guide, repeat Step 1 through Step 5 to add a second building, **Building 24**, to the **Milpitas** area.

Create a Floor in a Building

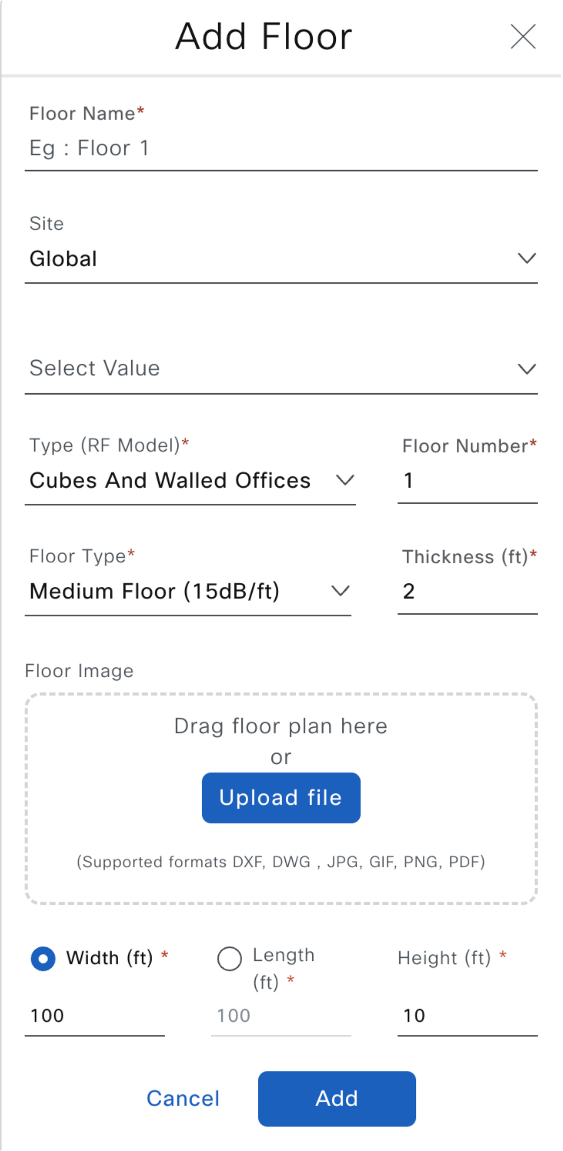
AP locations and wireless coverage (heatmaps) can be displayed from the floor maps. Floors are referenced during wireless provisioning.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

Step 2 Click + **Add Site** > **Add Floor**.

The **Add Floor** dialog box is displayed.



Add Floor

Floor Name*: Eg : Floor 1

Site: Global

Select Value

Type (RF Model)*: Cubes And Walled Offices

Floor Number*: 1

Floor Type*: Medium Floor (15dB/ft)

Thickness (ft)*: 2

Floor Image

Drag floor plan here
or

(Supported formats DXF, DWG , JPG, GIF, PNG, PDF)

● Width (ft) *: 100

○ Length (ft) *: 100

Height (ft) *: 10

Step 3 In the **Add Floor** dialog box, enter the **Floor Name** and choose the desired area from the **Site** drop-down list.

For this deployment guide, enter **Floor 1** for the **Floor Name**. For the **Site**, choose **Milpitas | Global/US**, and for the **Building**, choose **Building 23 | Global/US/Milpitas/**.

Step 4 Choose the appropriate space type from the **Type (RF Model)** drop-down list and enter the associated **Floor Number**.

Step 5 Choose the appropriate floor type from the **Floor Type** drop-down list and enter the associated **Thickness (ft)**.

Step 6 Add the floor plan to the **Floor Image** area using one of the following methods:

- Drag and drop the floor plan file into the **Floor Image** area.
- Click **Upload file** and choose the floor plan file that you want to upload.

Note If you have floor map diagrams in DXF, DWG, JPG, GIF, or PNG formats you can add them to any defined floors. If you import a map archive that has been exported from Cisco Prime Infrastructure, ensure that the site hierarchy configured in Cisco DNA Center is identical to the site hierarchy configured in Cisco Prime Infrastructure.

Step 7 Click the **Width (ft)** radio button and enter the floor width in feet.

Step 8 Click the **Length (ft)** radio button and enter the floor length in feet.

Step 9 In the **Height (ft)** field, enter the ceiling height in feet.

Note Adding the floor width, floor length, and ceiling height allows you to scale the floor plan correctly, impacting wireless coverage (heatmaps) and AP positioning.

For this deployment guide, enter **200** for the **Width (ft)**. For the **Length (ft)**, enter **275**, and for the **Height (ft)**, enter **10**.

Step 10 Click **Add**.

For this deployment guide, repeat Step 1 through Step 10 three times to add **Floor 2** to **Building 23**, **Floor 1** to **Building 24**, and **Floor 2** to **Building 24**.

Create and Position a Planned AP in Cisco DNA Center

There are three ways to get a planned AP on a floor map:

- Create a planned AP in Cisco DNA Center UI
- Import a map that has been exported from Cisco Prime Infrastructure
- Import a map that has been exported from Ekahau

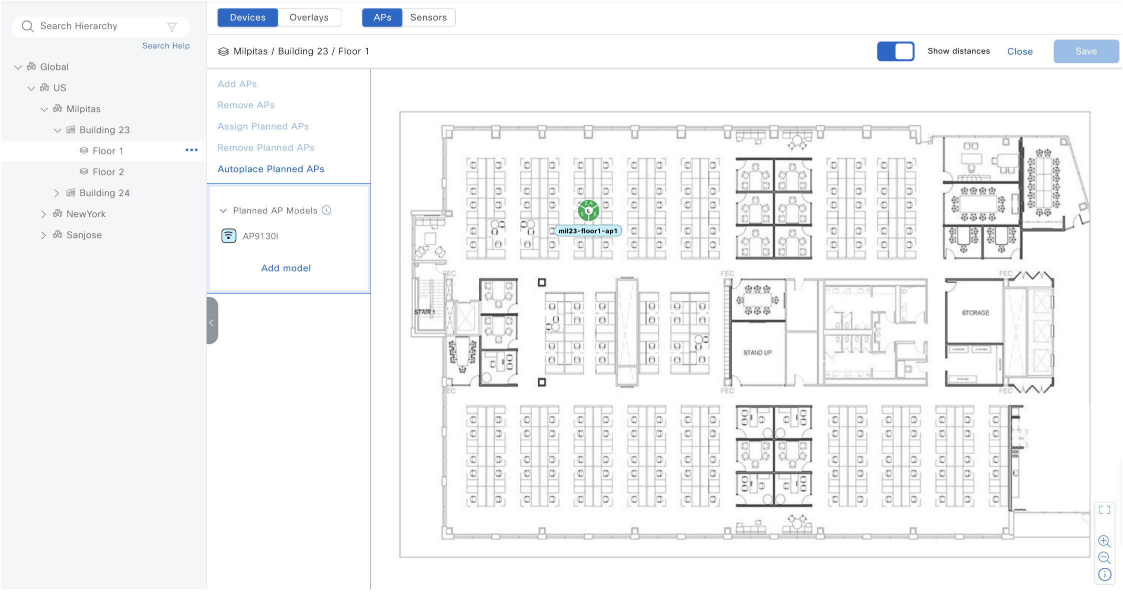
Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

Step 2 In the left hierarchy pane from the **Global** drop-down list, choose the desired floor for the AP.

Step 3 Click **Add/Edit**.

Step 4 From the **Planned AP Models** drop-down list, click **Add model**.



Step 5 In the **Select AP models to add** dialog box, choose the AP model from the drop-down list.

Step 6 Click **Add AP models**.

Step 7 From the **Planned AP Models** drop-down list, choose the desired AP model.

Step 8 In the floor map, move your cursor to the desired location of the AP and click the location.

Step 9 In the **Edit Planned AP** slide-in pane, ensure the **Planned AP Name** matches the real AP host name.

If a red octagon with an X is displayed, choose an **Antenna** from the **Antenna** drop-down list.

Step 10 Click **Save**.

Import a Map from Cisco Prime Infrastructure

Before you begin

This section assumes that the map has already been exported from Cisco Prime Infrastructure. For more information, see the "Export Maps Archive" topic in the *Cisco Prime Infrastructure 3.10 User Guide*.

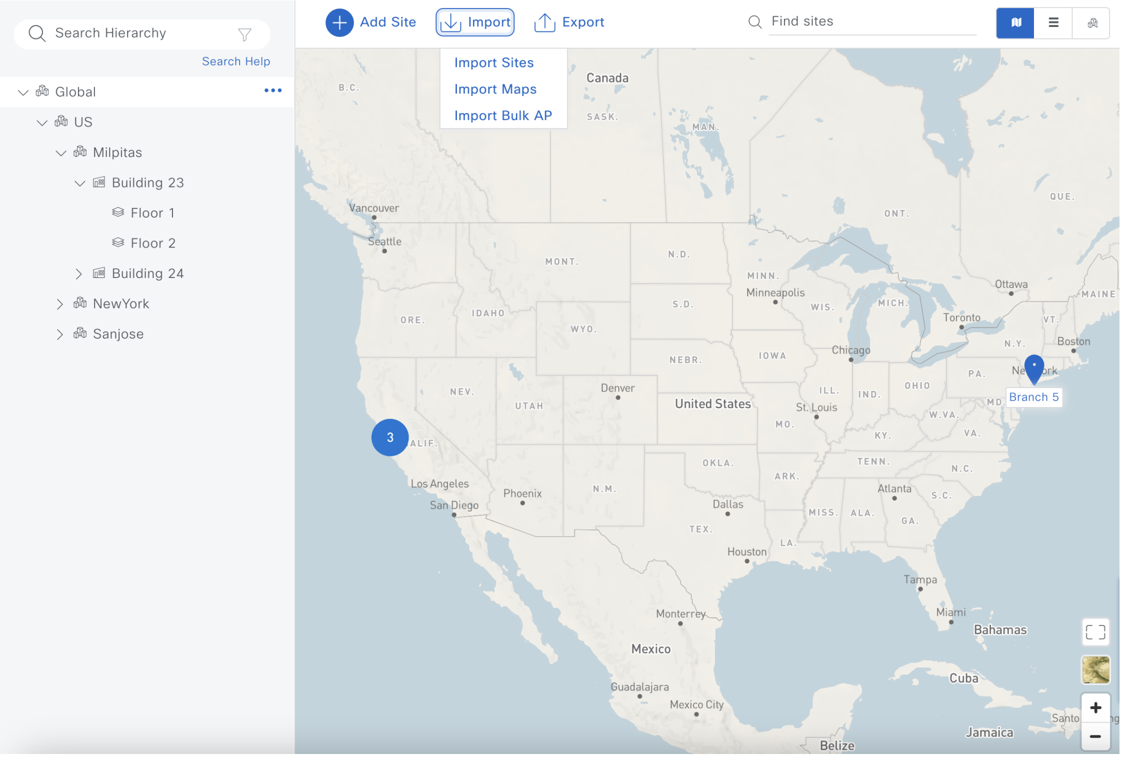
Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

Step 2 In the left hierarchy pane, choose **Global**.

Cisco Prime Infrastructure maps can be imported at the **Global** level.

Step 3 Click **Import** > **Import Maps**.



Step 4 In the **Import Maps** dialog box, import the map using one of the following methods:

- Click **Choose a file** and choose the map file that you want to upload.
- Drag and drop the map file into the **Import Maps** upload area.

Step 5 Click **Import**.

Export a Map from Cisco DNA Center as an Ekahau Project File

To create and position a planned AP using Ekahau, first create the sites in Cisco DNA Center and export the sites as an Ekahau project. Then, create the planned AP in Ekahau and save the AP as an Ekahau project. Finally, import the Ekahau project back into Cisco DNA Center.

Note You can only export an Ekahau project file at a non-nested site level, which means there can be only one site with buildings within the chosen site.

The following steps explain this process:

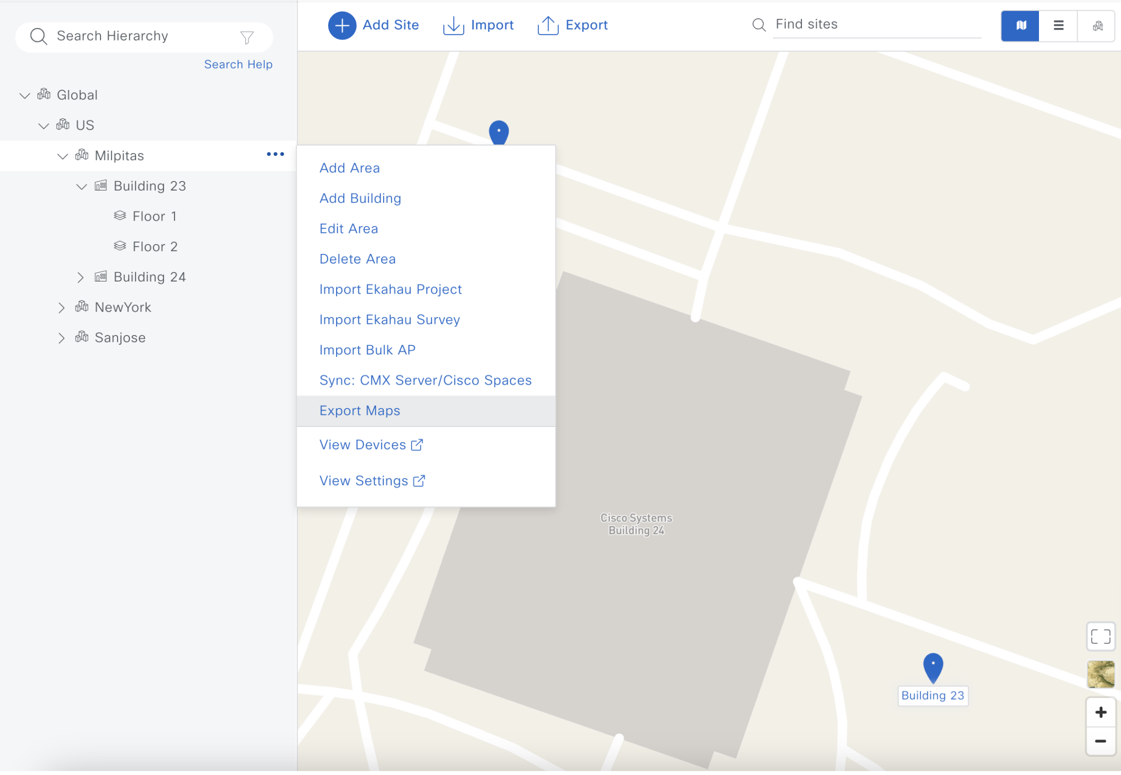
Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

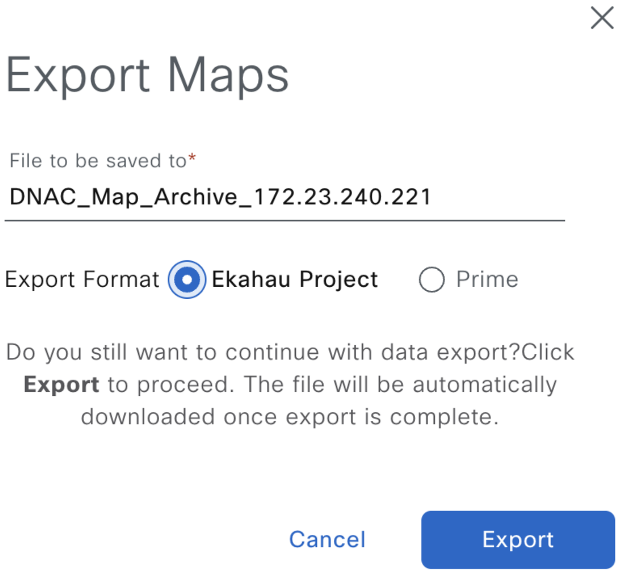
Step 2 In the left hierarchy pane, choose the appropriate site for your map.

For this deployment guide, choose **Milpitas**.

Step 3 Hover your cursor over the ellipsis icon (•••) and choose **Export Maps**.



Step 4 In the **Export Maps** dialog box, enter the desired file name and click the **Ekahau Project** radio button.



Export Maps

File to be saved to*

DNAC_Map_Archive_172.23.240.221

Export Format ● Ekahau Project ○ Prime

Do you still want to continue with data export?Click **Export** to proceed. The file will be automatically downloaded once export is complete.

Step 5 Click **Export**.

Import a Map from Ekahau

Before you begin

The maps imported from Ekahau are in Ekahau project file format. Ensure that the map is imported from the same site level at which the map was exported. For example, if the map was exported from the **Milpitas** site, you must import the map from **Milpitas**.

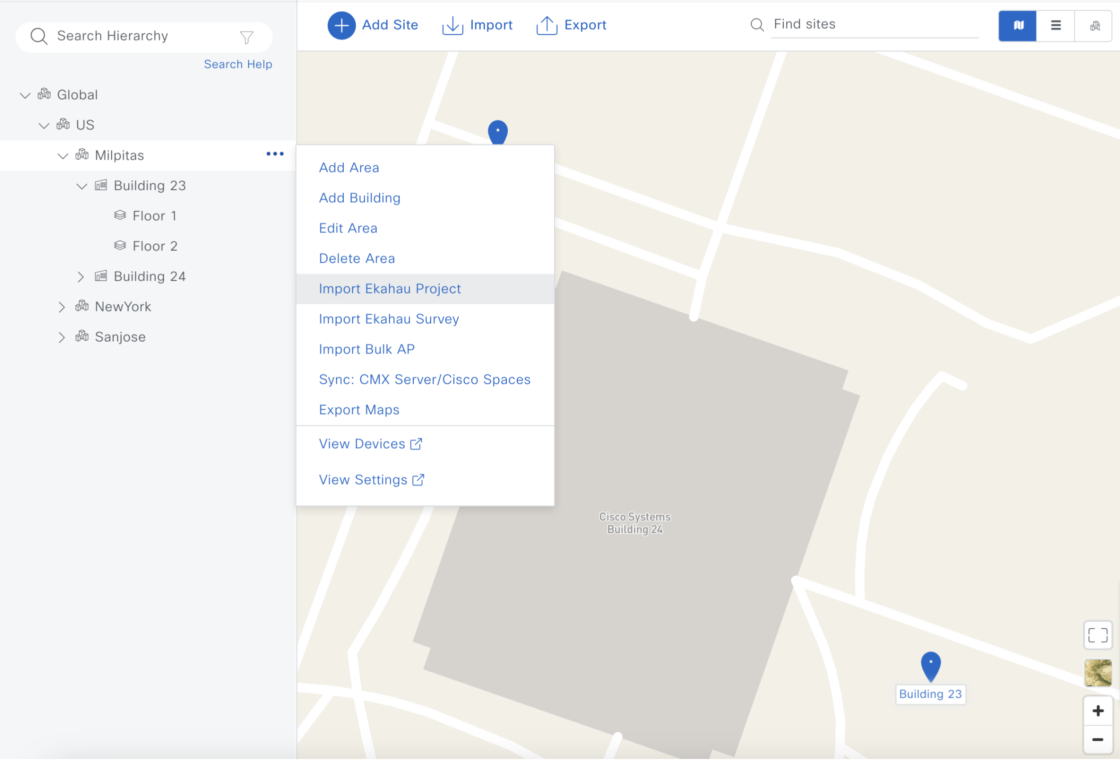
Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

Step 2 In the left hierarchy pane, choose the appropriate site for your map.

For this deployment guide, choose **Milpitas**.

Step 3 Hover your cursor over the ellipsis icon (•••) and choose **Import Ekahau Project**.



Step 4 In the **Import Ekahau Project** dialog box, import the map using one of the following methods:

- Click **Choose a file** and choose the project file that you want to upload.
- Drag and drop the map file into the **Import Ekahau Project** upload area.

Step 5 Click **Import**.

Configure Network Services for Network Operation

This section explains how to configure AAA, DHCP, DNS, NTP, SNMP, and syslog services that align with the site hierarchy in Cisco DNA Center. If the services use the same servers across the entire site hierarchy, you can configure the services globally. The inheritance properties of the site hierarchy allow global settings to be available to all sites. Differences for individual sites can then be applied on a site-by-site basis. This guide shows the network services created globally.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Network**.

Step 2 In the left hierarchy pane, choose **Global**.

Step 3 Click **+ Add Servers**.

Step 4 In the **Add Servers** dialog box, check the **AAA** check box and the **NTP** check box.

This guide does not require the deployment of **Image Distribution** or **Stealthwatch Flow Destination**, so do not check the **Image Distribution** check box or the **Stealthwatch Flow Destination** check box.

Step 5 Click **OK**.

An AAA server and an NTP server are now displayed in the **Network** window.

Step 6 Configure the relevant fields for the **AAA Server**.

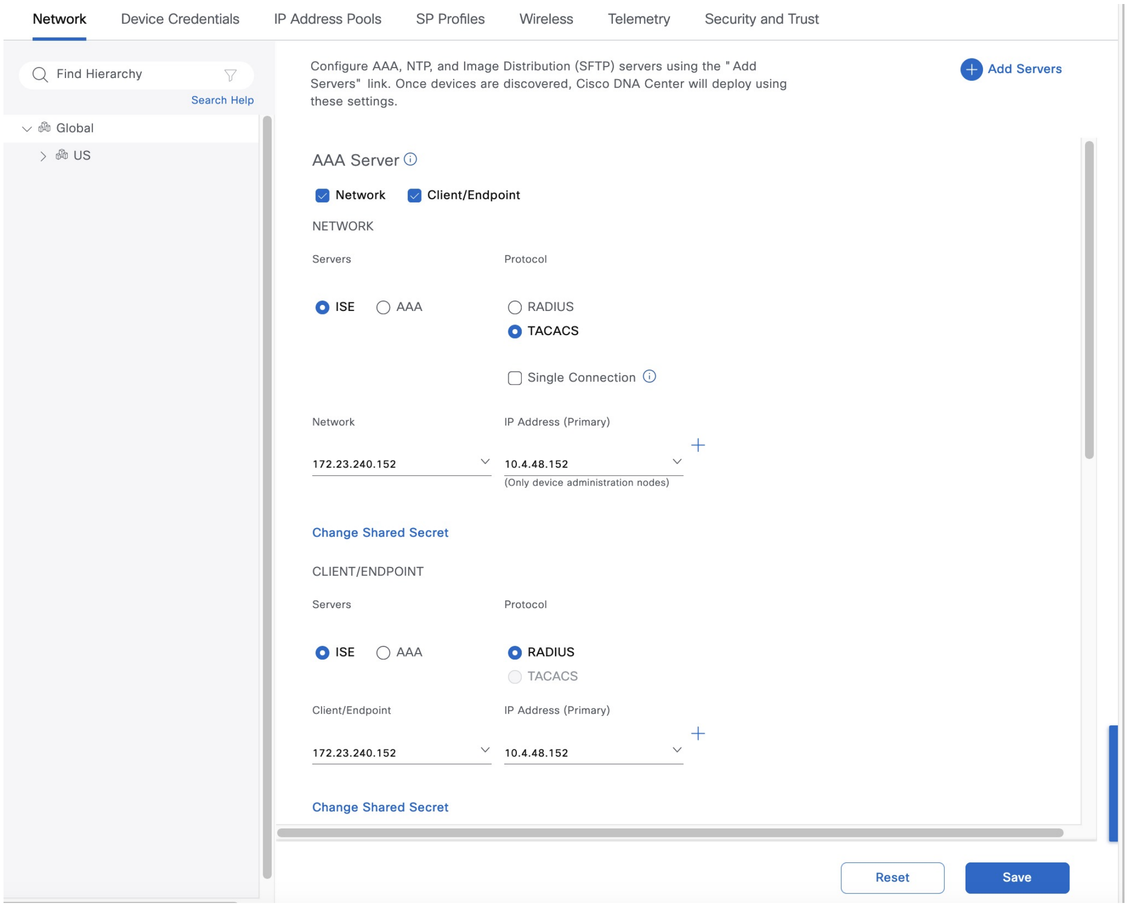
For both network devices and wireless clients, this design and deployment guide uses Cisco ISE as the AAA server (which uses the RADIUS protocol). For this guide, the following fields were configured for the **AAA Server**.

Table 5: AAA Server Configuration

Field	Value
Network	Checked
Client/Endpoint	Checked
Network > Servers	ISE
Network > Protocol	TACACS
Network > Network	172.23.240.152
Network > IP Address (Primary)	10.4.48.152
Network > Shared Secret	—
Client/Endpoint > Servers	ISE
Client/Endpoint > Protocol	RADIUS
Client/Endpoint > Network	172.23.240.152
Client/Endpoint > IP Address (Primary)	10.4.48.152

Field	Value
Client/Endpoint > Shared Secret	—

Figure 4: AAA Server Configuration in Cisco DNA Center



Configure AAA, NTP, and Image Distribution (SFTP) servers using the " Add Servers" link. Once devices are discovered, Cisco DNA Center will deploy using these settings.

AAA Server

☑ Network ☑ Client/Endpoint

NETWORK

Servers: ● ISE ○ AAA

Protocol: ○ RADIUS ● TACACS

□ Single Connection

Network: 172.23.240.152

IP Address (Primary): 10.4.48.152 (Only device administration nodes)

Change Shared Secret

CLIENT/ENDPOINT

Servers: ● ISE ○ AAA

Protocol: ● RADIUS ○ TACACS

Client/Endpoint: 172.23.240.152

IP Address (Primary): 10.4.48.152

Change Shared Secret

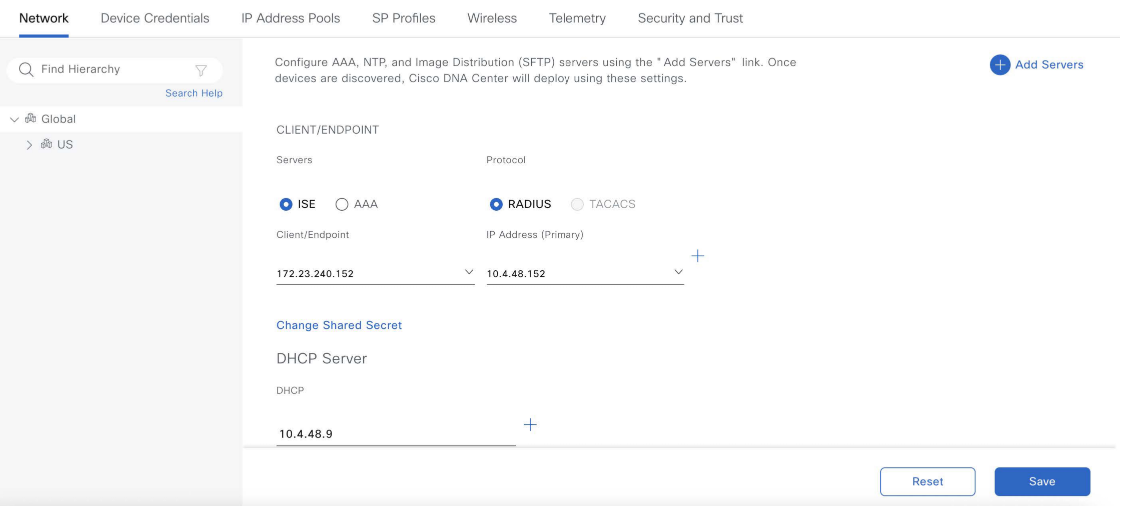
Step 7 Configure the relevant fields for the **DHCP Server**.

This design and deployment guide uses a single Microsoft Active Directory (AD) server, which functions as both the DNS and DHCP servers for the network. For this guide, the following field was configured for the **DHCP Server**.

Table 6: DHCP Server Configuration

Field	Value
DHCP	10.4.48.9

Figure 5: DHCP Server Configuration in Cisco DNA Center



Configure AAA, NTP, and Image Distribution (SFTP) servers using the " Add Servers" link. Once devices are discovered, Cisco DNA Center will deploy using these settings.

CLIENT/ENDPOINT

Servers: ● ISE ○ AAA

Protocol: ● RADIUS ○ TACACS

Client/Endpoint: 172.23.240.152

IP Address (Primary): 10.4.48.152

DHCP Server

DHCP: 10.4.48.9

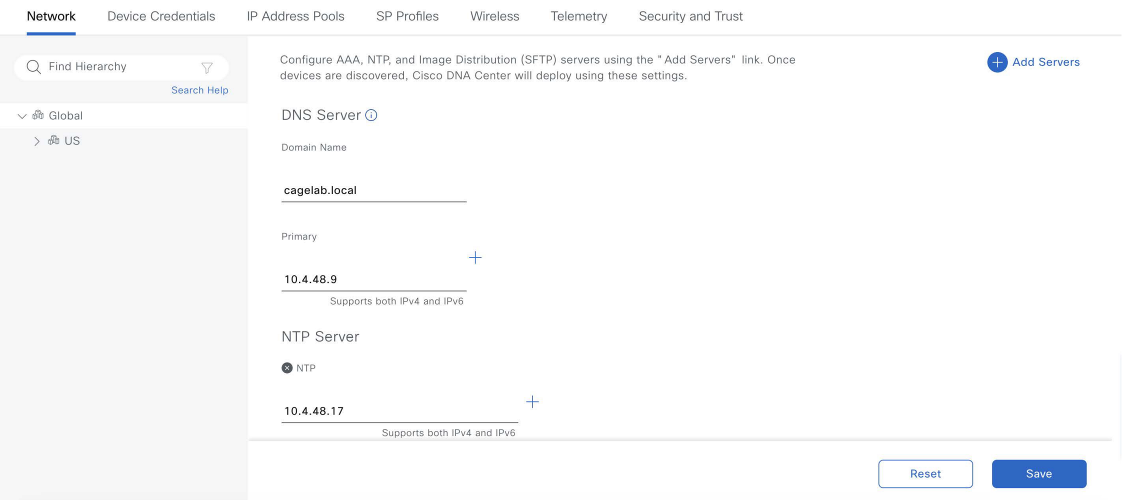
Step 8 Configure the relevant fields for the **DNS Server**.

Because this design and deployment guide uses a lab network, the **DNS Server** configuration only used a single DNS domain. For this guide, the following fields were configured for the **DNS Server**.

Table 7: DNS Server Configuration

Field	Value
Domain Name	cagelab.local
Primary	10.4.48.9

Figure 6: DNS Server Configuration in Cisco DNA Center



Configure AAA, NTP, and Image Distribution (SFTP) servers using the " Add Servers" link. Once devices are discovered, Cisco DNA Center will deploy using these settings.

DNS Server

Domain Name: cagelab.local

Primary: 10.4.48.9

Supports both IPv4 and IPv6

NTP Server

NTP: 10.4.48.17

Supports both IPv4 and IPv6

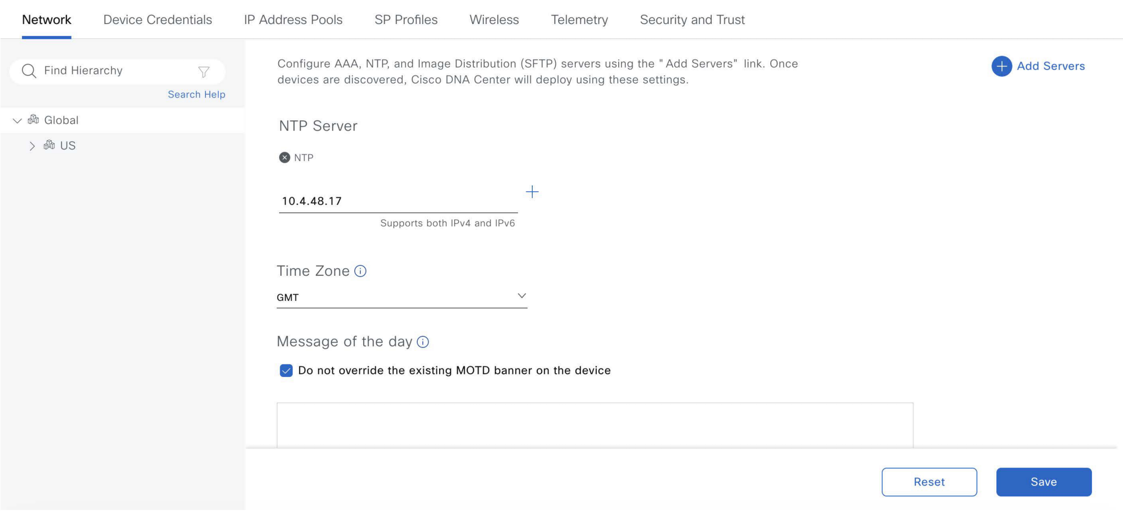
Step 9 Configure the relevant fields for the **NTP Server**.

For production networks, multiple NTP servers can be added for resiliency and accuracy. Time synchronization within a network is essential for any logging functions, as well as secure connectivity such as SSH. Because this design and deployment guide uses a lab network, the **NTP Server** configuration only used a single NTP server. For this guide, the following fields were configured for the **NTP Server**.

Table 8: NTP Server Configuration

Field	**Value**
IP Address	10.4.48.17
Time Zone	GMT

Figure 7: NTP Server Configuration in Cisco DNA Center



Configure AAA, NTP, and Image Distribution (SFTP) servers using the " Add Servers" link. Once devices are discovered, Cisco DNA Center will deploy using these settings.

NTP Server

NTP

10.4.48.17

Supports both IPv4 and IPv6

Time Zone: GMT

Message of the day

☑ Do not override the existing MOTD banner on the device

Step 10 Choose the desired time zone from the **Time Zone** drop-down list.

Because this design and deployment guide uses a lab network, a single time zone is used for the site hierarchy. In a production network, each site within the site hierarchy would reflect the time zone of the location.

Step 11 For the **Message of the day**, check the **Do not overwrite the existing MOTD banner on the device** check box or enter your desired message in the text box.

The **Message of the day** field controls the message displayed when logging in to the network device. This setting is not applicable to this design and deployment guide, so for this guide, the check box was checked for **Do not overwrite the existing MOTD banner on the device**.

Step 12 Click **Save**.

Step 13 At the top of the window, click **Telemetry**.

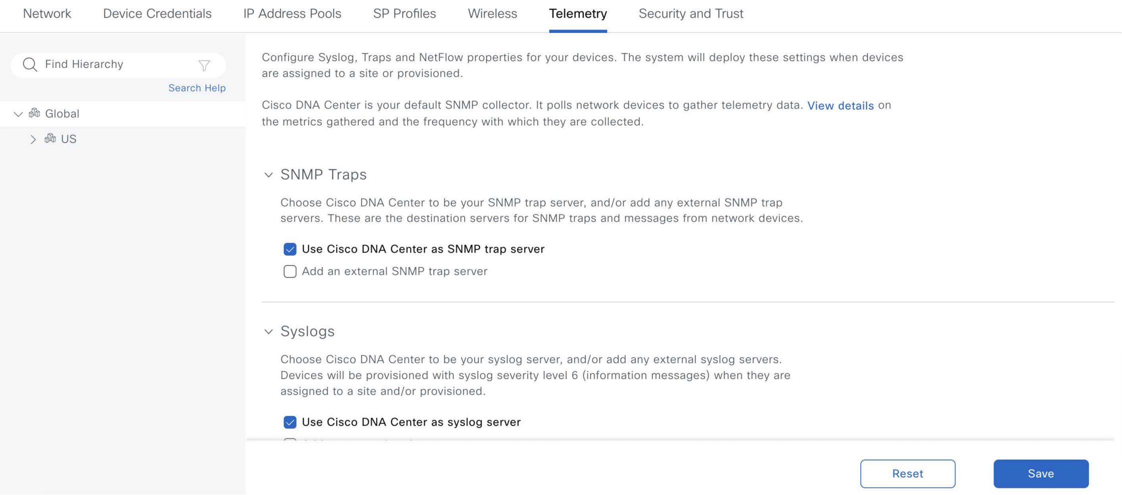
Step 14 From **SNMP Traps**, configure the SNMP trap server.

This design and deployment guide uses Cisco DNA Center as the SNMP server. If you check the **Use Cisco DNA Center as SNMP server** check box, SNMP trap information will be sent to Cisco DNA Center for Cisco AI Network Analytics. For this guide, the following fields were configured for the SNMP server.

Table 9: SNMP Server Configuration

Field	Value
Use Cisco DNA Center as SNMP server	Checked
SNMP > IP Address	—

Figure 8: SNMP Server Configuration in Cisco DNA Center



Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.

Cisco DNA Center is your default SNMP collector. It polls network devices to gather telemetry data. View details on the metrics gathered and the frequency with which they are collected.

SNMP Traps

Choose Cisco DNA Center to be your SNMP trap server, and/or add any external SNMP trap servers. These are the destination servers for SNMP traps and messages from network devices.

☑ Use Cisco DNA Center as SNMP trap server

□ Add an external SNMP trap server

Syslogs

Choose Cisco DNA Center to be your syslog server, and/or add any external syslog servers. Devices will be provisioned with syslog severity level 6 (information messages) when they are assigned to a site and/or provisioned.

☑ Use Cisco DNA Center as syslog server

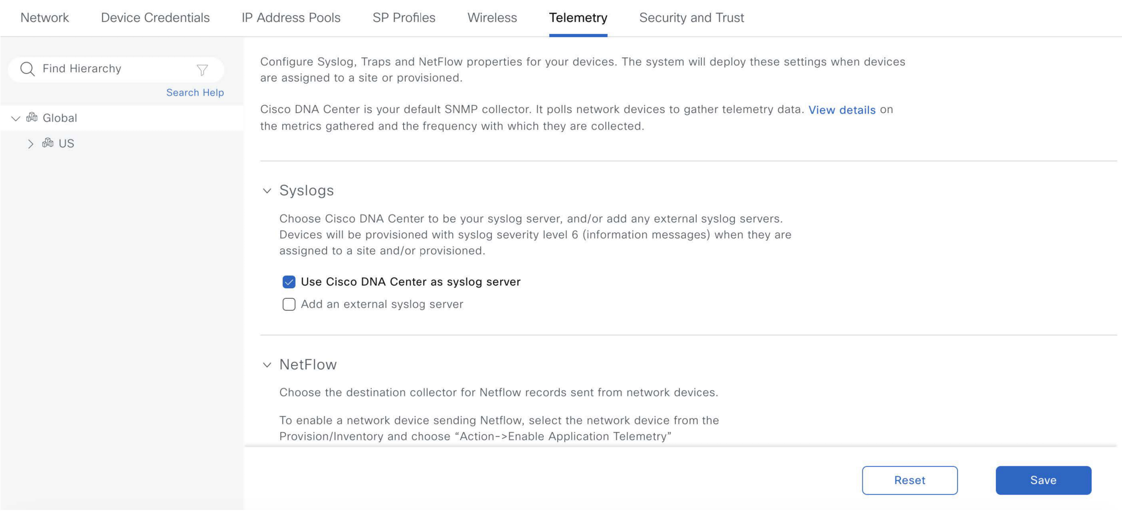
Step 15 From **Syslogs**, configure the syslog server.

This design and deployment guide uses Cisco DNA Center as the syslog server. If you check the **Use Cisco DNA Center as syslog server** check box, syslog information will be sent to Cisco DNA Center for Cisco AI Network Analytics. For this guide, the following fields were configured for the syslog server.

Table 10: Syslog Server Configuration

Field	Value
Use Cisco DNA Center as syslog server	Checked
Syslog > IP Address	—

Figure 9: Syslog Server Configuration in Cisco DNA Center



Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.

Cisco DNA Center is your default SNMP collector. It polls network devices to gather telemetry data. View details on the metrics gathered and the frequency with which they are collected.

Syslogs

Choose Cisco DNA Center to be your syslog server, and/or add any external syslog servers. Devices will be provisioned with syslog severity level 6 (information messages) when they are assigned to a site and/or provisioned.

☑ Use Cisco DNA Center as syslog server

□ Add an external syslog server

NetFlow

Choose the destination collector for Netflow records sent from network devices.

To enable a network device sending Netflow, select the network device from the Provision/Inventory and choose "Action->Enable Application Telemetry"

Step 16 Click **Save**.

Campus Wireless Deployment Settings

To configure the campus wireless deployment settings, you need to create the following in Cisco DNA Center:

- Wireless interfaces: The Ethernet interfaces (VLANs) that are used for terminating wireless traffic.
- Enterprise wireless networks: Consist of the nonguest WLANs/SSIDs for the deployment.
- Guest wireless networks: Consist of the guest WLANs/SSIDs for the deployment.
- Wireless radio frequency (RF) profiles: Includes the radio frequency profiles for the deployment.
- Wireless sensor settings: Wireless sensors provide the ability to run diagnostic tests on the WLAN and perform packet captures. For information about wireless sensors, see Monitor and Operate the Wireless Network, on page 189.
- CMX servers: Integration with CMX servers allows the location of wireless clients to be displayed on floor maps. For information about integration with CMX servers, see Monitor and Operate the Wireless Network, on page 189.
- Native VLAN: The native VLAN configuration is specific to FlexConnect Access Point (AP) deployments.

Note This deployment guide describes a wireless network with APs that operate in the centralized (local) mode.

Recommendations

When configuring the campus wireless deployment settings, consider the following recommendations:

- Similar to any production deployment, you must place the APs in a VLAN that is different from the Wireless Management Interface (WMI). If you must configure the APs in the same VLAN as the WMI for staging or testing purposes, Cisco recommends that you limit the number of APs to less than 100.

- For APs in local mode, the round-trip latency must not exceed 20 milliseconds between the access point and the controller.
- Use PortFast on AP switch ports for APs in local mode, supporting only the central switched WLANs. To configure the switch port for PortFast, set the port to be connected as a host port, using the switch port host command or the PortFast command. This configuration allows for a faster AP join process. There is no risk of loops, as the local mode APs never directly bridge traffic between VLANs. You can set the port directly on access mode.
- For APs in Flex mode and local switching, the switch port needs to be in trunk mode for most scenarios. In such cases, use spanning-tree portfast trunk on the switch port.
- To optimize the TCP client traffic encapsulation in CAPWAP, Cisco recommends that you always enable the TCP Maximum Segment Size (MSS) feature, as it can reduce the overall amount of CAPWAP fragmentation, thereby improving the overall wireless network performance. You must adjust the MSS value depending on the traffic type and Maximum Transmission Unit (MTU) of the Cisco Wireless Controller-to-AP path.
- In the Cisco Catalyst 9800 Series Wireless Controller, TCP MSS adjust is enabled by default, with a value of 1250 bytes, which is considered an acceptable value for most deployments. You can further optimize the value depending on your setup. You must configure directly on the wireless controller or via the Template Hub.

Configure Wireless Interfaces

In Cisco DNA Center, the enterprise and guest WLANs terminate on the Ethernet VLAN interfaces. For this design and deployment guide, the following table shows the wireless interfaces created for the enterprise and guest WLANs.

Table 11: Wireless Interfaces

Name	VLAN	Usage
employee	160	Employee voice and data VLAN
guest-dmz	125	Guest data VLAN
flex	180	Flex client VLAN

Procedure

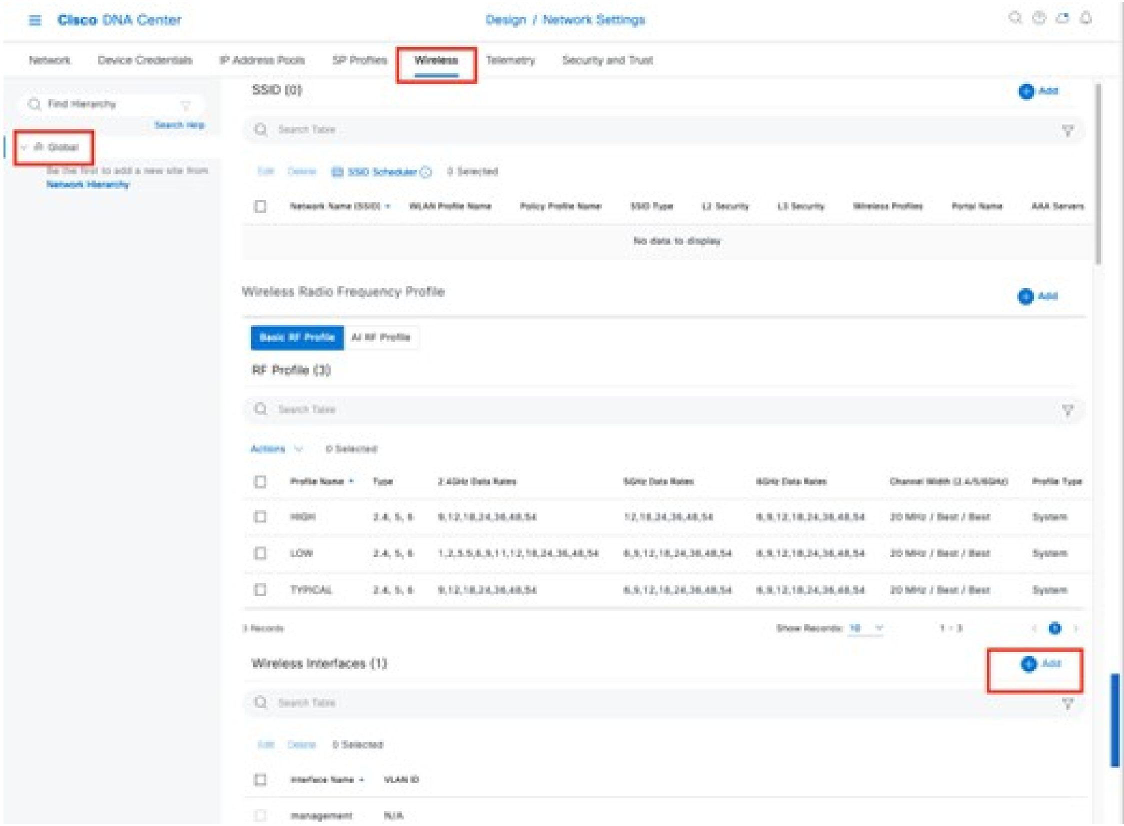
Step 1 Log in to Cisco DNA Center using the IP address or the fully qualified domain name of your instance.

For example: https://<Cisco_DNA_Center_IPaddr_or_FQDN>. The credentials (user ID and password) you enter must have SUPER-ADMIN-ROLE or NETWORK-ADMIN-ROLE privileges.

Step 2 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

The **Wireless Network Settings** dashboard is displayed.

Figure 10: Wireless Network Settings Dashboard



SSID (0)

0 Selected

□	Network Name (SSID)	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers

No data to display

Wireless Radio Frequency Profile

RF Profile (3)

0 Selected

□	Profile Name	Type	2.4GHz Data Rates	5GHz Data Rates	6GHz Data Rates	Channel Width (2.4/5/6GHz)	Profile Type
□	HIGH	2.4, 5, 6	9,12,18,24,36,48,54	12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System
□	LOW	2.4, 5, 6	1,2,5.5,6,9,11,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System
□	TYPICAL	2.4, 5, 6	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System

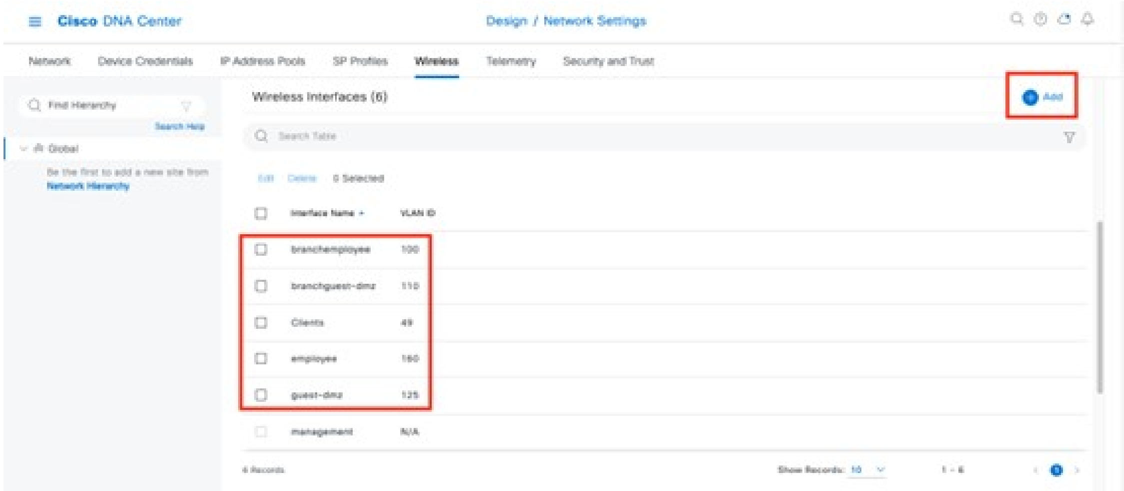
3 Records   Show Records: 10   1 - 3

Wireless Interfaces (1)

0 Selected

□	Interface Name	VLAN ID
□	management	N/A

Figure 11: Wireless Interfaces Window



Wireless Interfaces (6)

0 Selected

□	Interface Name	VLAN ID
□	branchemployee	100
□	branchguest-dmz	110
□	Clients	49
□	employee	160
□	guest-dmz	125
□	management	N/A

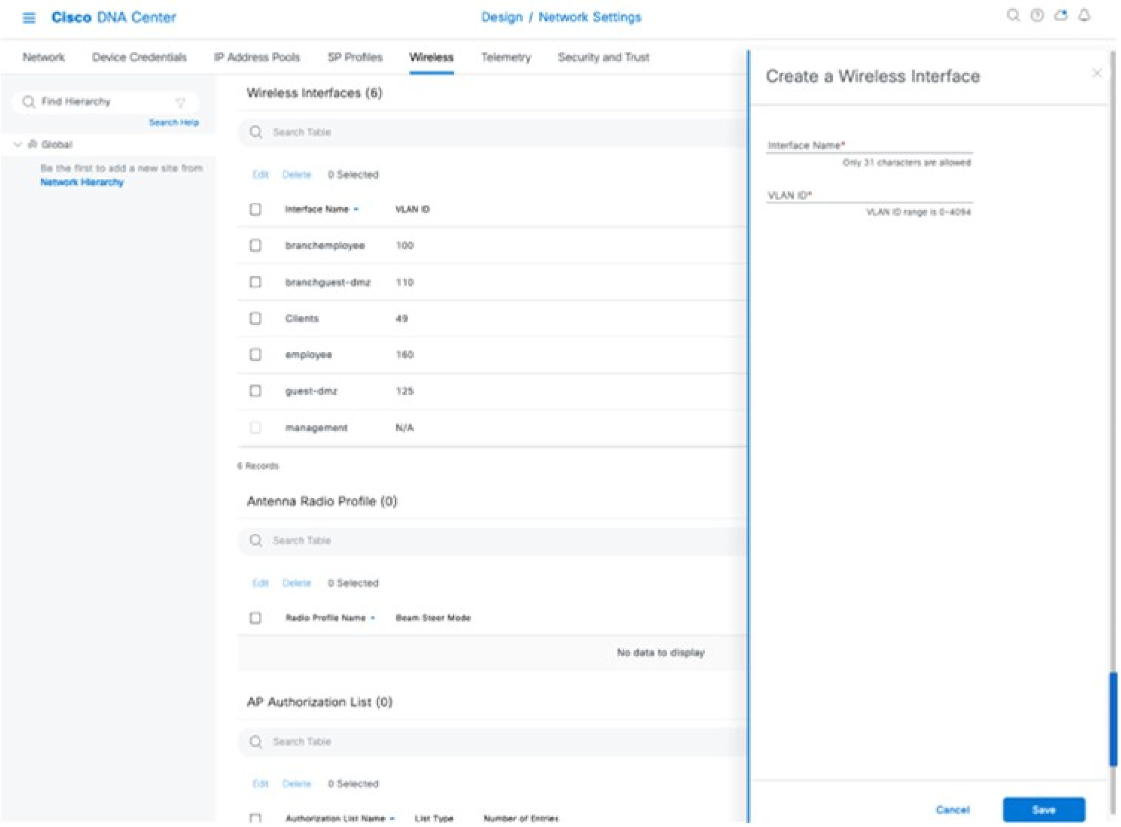
6 Records   Show Records: 10   1 - 6

Note Wireless settings are hierarchical. Settings defined at lower levels of the site hierarchy override the settings defined in higher levels. By default, you are taken to the global level, which is the highest level of the site hierarchy. You must define the wireless interfaces at the global level of the site hierarchy.

Step 3 Click **Add** next to **Wireless Interfaces**.

The **New Wireless Interface** slide-in pane is displayed.

Figure 12: New Wireless Interface Slide-in Pane



Wireless Interfaces (6)

Interface Name	VLAN ID
branchemployee	100
branchguest-dmz	110
Clients	49
employee	160
guest-dmz	125
management	N/A

Antenna Radio Profile (0)

Radio Profile Name	Beam Steer Mode
No data to display	

AP Authorization List (0)

Authorization List Name	List Type	Number of Entries

Create a Wireless Interface

Interface Name*

Only 31 characters are allowed

VLAN ID*

VLAN ID range is 0-4094

Step 4 Enter the **Interface Name** and **VLAN ID** for the wireless interface corresponding to the enterprise VLAN (employee), and then click **Add**.

Repeat this procedure to add the wireless interface for the guest VLAN (guest-dmz). The two new wireless interfaces are displayed in the **Wireless Network Settings** dashboard.

Configure Enterprise Wireless SSID

Enterprise wireless networks are the nonguest WLANs/SSIDs that are available for broadcast across the deployment, and you must define these wireless networks at the global level of the site hierarchy. Once defined, you can apply the enterprise wireless networks to wireless profiles, and then you can assign wireless profiles to one or more sites within the hierarchy.

Note Cisco recommends limiting the number of Service Set Identifiers (SSIDs) configured on the controller. You can configure 16 simultaneous WLANs/SSIDs (per radio on each AP). Each WLAN/SSID needs separate probe responses and beaconing transmitted at the lowest mandatory rate, and the RF pollution increases as more SSIDs are added.

Some smaller wireless stations such as PDAs, Wi-Fi phones, and barcode scanners cannot cope with a high number of Basic SSIDs (BSSIDs) over the air, resulting in lockups, reloads, or association failures. Cisco recommends that you have one to three SSIDs for an enterprise and one SSID for high-density designs. By using the AAA override feature, you can reduce the number of WLANs/SSIDs while assigning individual per user VLAN/settings in a single SSID scenario.

For this deployment guide, a single enterprise WLAN/SSID named **lab3employee** is provisioned.

Procedure

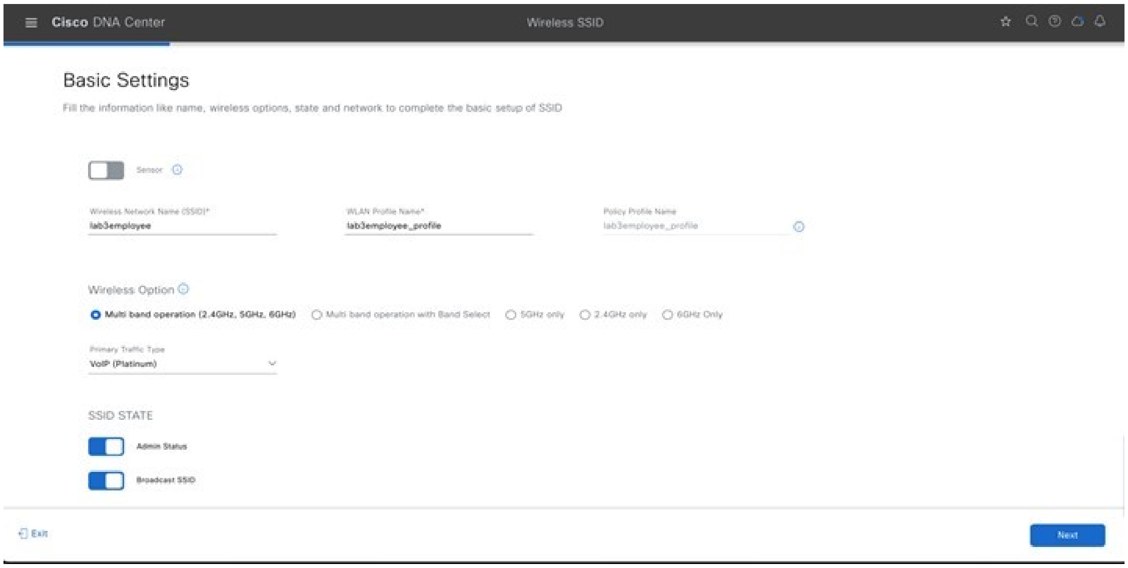
Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Click **SSIDs**.

Step 3 Hover your cursor over **+ Add** and choose **Enterprise**.

The **Basic Settings** window is displayed.

Figure 13: Basic Settings Window to Create an Enterprise Wireless SSID



Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID

Sensor: off

Wireless Network Name (SSID)*: lab3employee

WLAN Profile Name*: lab3employee_profile

Policy Profile Name: lab3employee_profile

Wireless Option

● Multi band operation (2.4GHz, 5GHz, 6GHz) ○ Multi band operation with Band Select ○ 5GHz only ○ 2.4GHz only ○ 6GHz Only

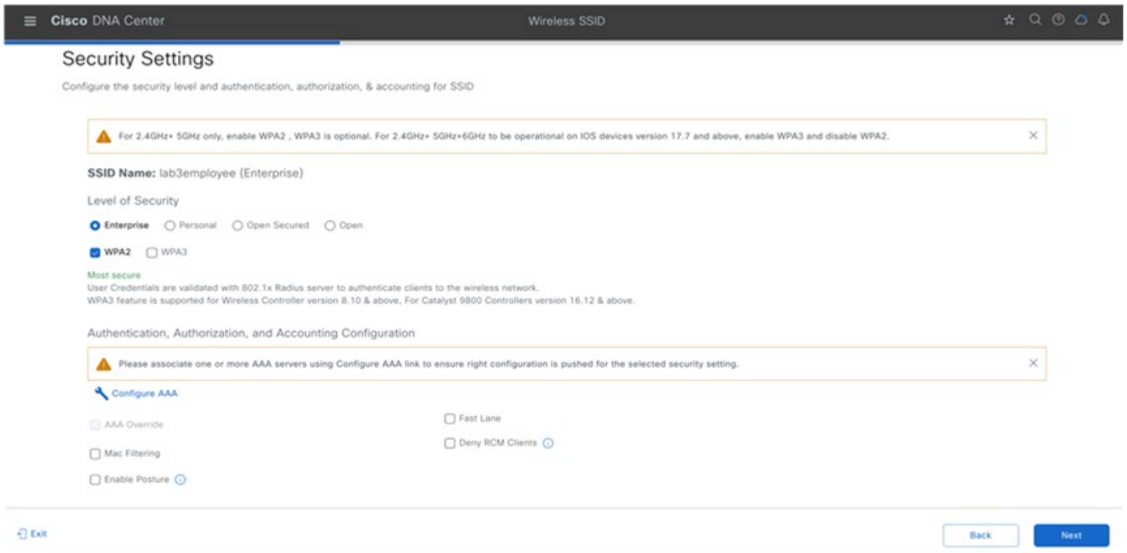
Primary Traffic Type: VoIP (Platinum)

SSID STATE

Admin Status: on

Broadcast SSID: on

Figure 14: Security Settings for the Enterprise SSID



Security Settings

Configure the security level and authentication, authorization, & accounting for SSID

For 2.4GHz+ 5GHz only, enable WPA2 , WPA3 is optional. For 2.4GHz+ 5GHz+6GHz to be operational on IOS devices version 17.7 and above, enable WPA3 and disable WPA2.

SSID Name: lab3employee (Enterprise)

Level of Security

● Enterprise ○ Personal ○ Open Secured ○ Open

☑ WPA2 □ WPA3

Most secure
User Credentials are validated with 802.1x Radius server to authenticate clients to the wireless network.
WPA3 feature is supported for Wireless Controller version 8.10 & above, For Catalyst 9800 Controllers version 16.12 & above.

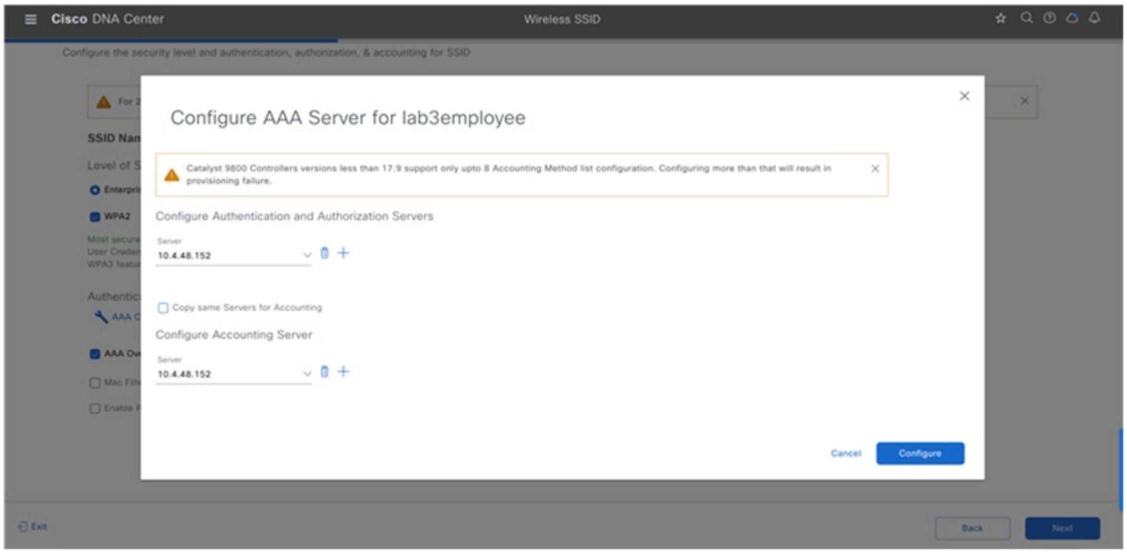
Authentication, Authorization, and Accounting Configuration

Please associate one or more AAA servers using Configure AAA link to ensure right configuration is pushed for the selected security setting.

Configure AAA

□ AAA Override
□ Mac Filtering
□ Enable Posture
□ Fast Lane
□ Deny RCM Clients

Figure 15: AAA Server for the Enterprise SSID



Configure AAA Server for lab3employee

Catalyst 9800 Controllers versions less than 17.9 support only upto 8 Accounting Method list configuration. Configuring more than that will result in provisioning failure.

Configure Authentication and Authorization Servers

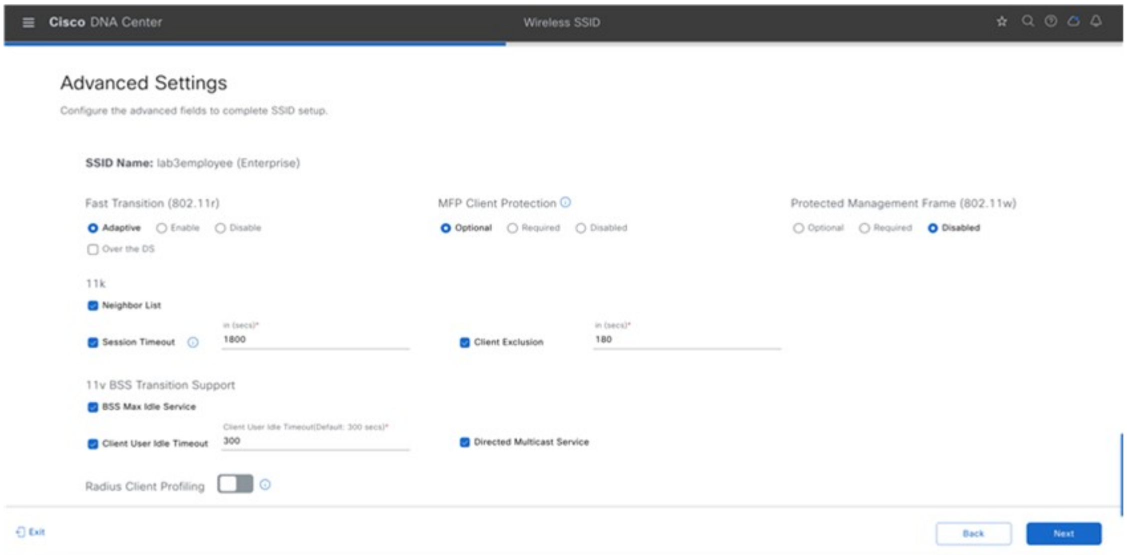
Server: 10.4.48.152

□ Copy same Servers for Accounting

Configure Accounting Server

Server: 10.4.48.152

Figure 16: Advanced Settings for the Enterprise SSID



Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: lab3employee (Enterprise)

Fast Transition (802.11r)
● Adaptive ○ Enable ○ Disable
□ Over the DS

MFP Client Protection
● Optional ○ Required ○ Disabled

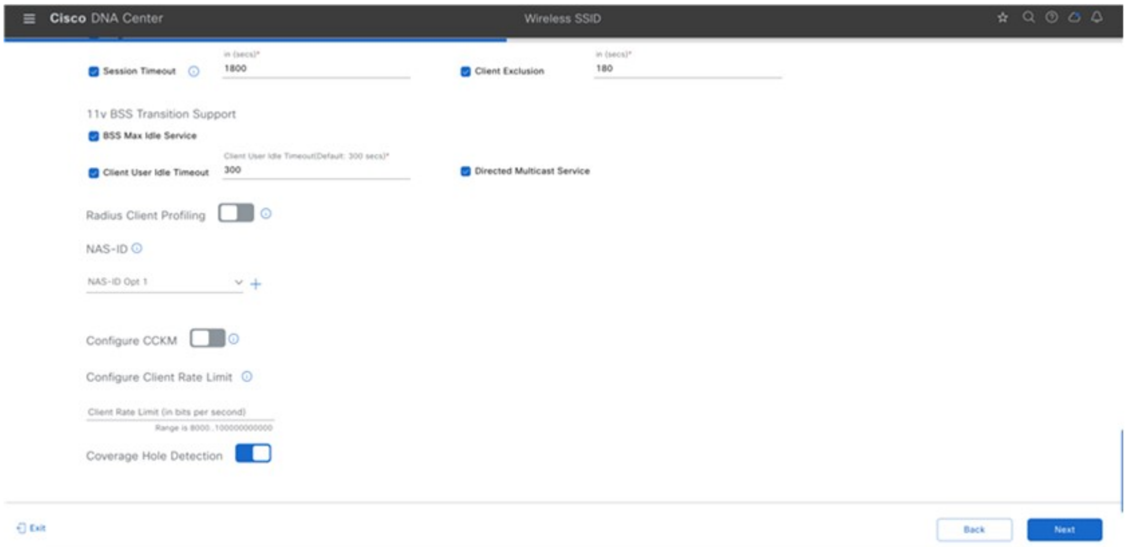
Protected Management Frame (802.11w)
○ Optional ○ Required ● Disabled

11k
☑ Neighbor List
☑ Session Timeout — in (secs)*: 1800
☑ Client Exclusion — in (secs)*: 180

11v BSS Transition Support
☑ BSS Max Idle Service
☑ Client User Idle Timeout — Client User Idle Timeout(Default: 300 secs)*: 300
☑ Directed Multicast Service

Radius Client Profiling

Figure 17: Additional Advanced Settings for the Enterprise SSID



☑ Session Timeout — in (secs)*: 1800
☑ Client Exclusion — in (secs)*: 180

11v BSS Transition Support
☑ BSS Max Idle Service
☑ Client User Idle Timeout — Client User Idle Timeout(Default: 300 secs)*: 300
☑ Directed Multicast Service

Radius Client Profiling

NAS-ID
NAS-ID Opt 1

Configure CCKM

Configure Client Rate Limit
Client Rate Limit (in bits per second)
Range is 8000..100000000000

Coverage Hole Detection

Note Enabling the neighbor list (802.11k) may cause some legacy devices to react incorrectly to unknown information. Most devices will ignore the 802.11k information (even if they do not support it), but a disconnection or a failure to associate may occur for some devices. It is advisable to test before enabling this option.

In scenarios where clients would move in and out of coverage areas or when the client is battery operated and may go to sleep frequently, you may consider increasing the idle time out to 3600 seconds (60 minutes) to reduce the likelihood of client deletion.

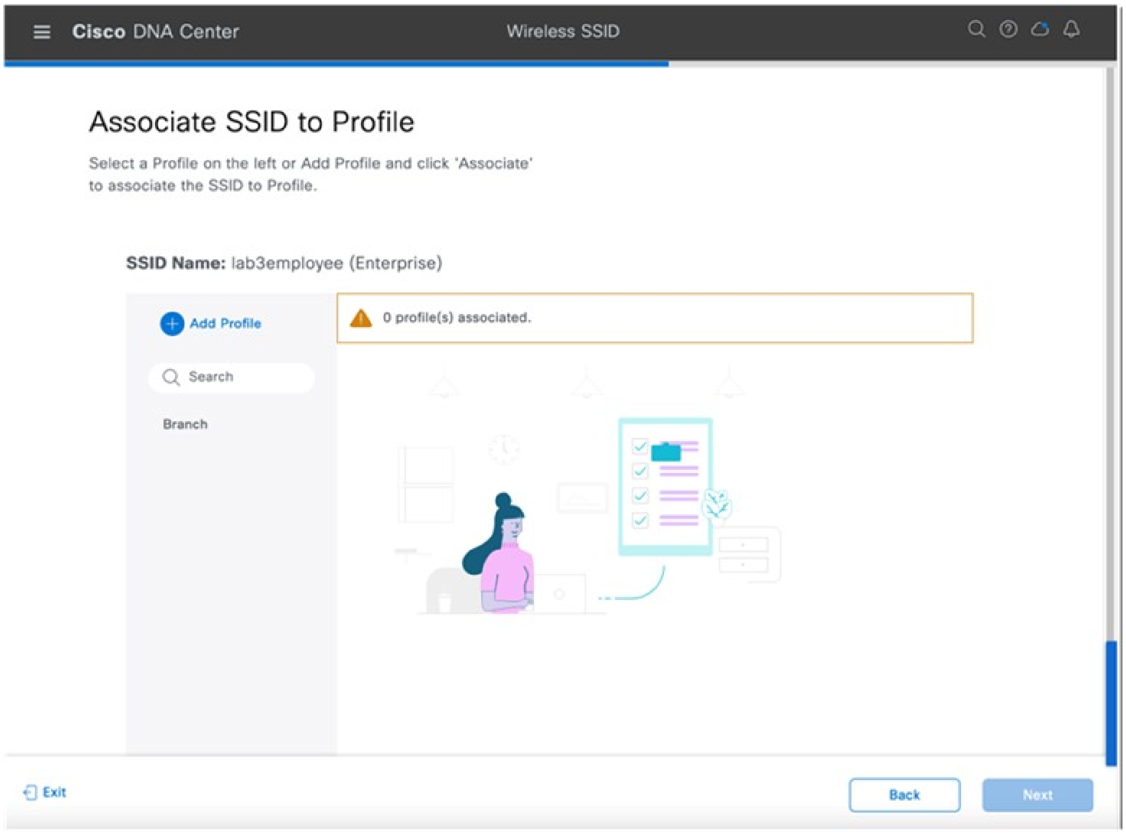
For information about features that can be configured for enterprise wireless networks via Cisco DNA Center, see Enterprise Wireless Network Features Configurable via Cisco DNA Center, on page 39.

Step 4 Enter the information for the **Basic Settings** and click **Next**.

The next screen in the workflow is displayed. You can either attach the enterprise wireless network to an existing wireless profile, or you can create a new wireless profile and attach the enterprise wireless network.

Note For information about the settings for the enterprise wireless network configured for this deployment guide, see Enterprise Wireless Network Settings Configured in the Deployment Guide, on page 49.

Figure 18: Associate SSID to Profile



Associate SSID to Profile

Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile.

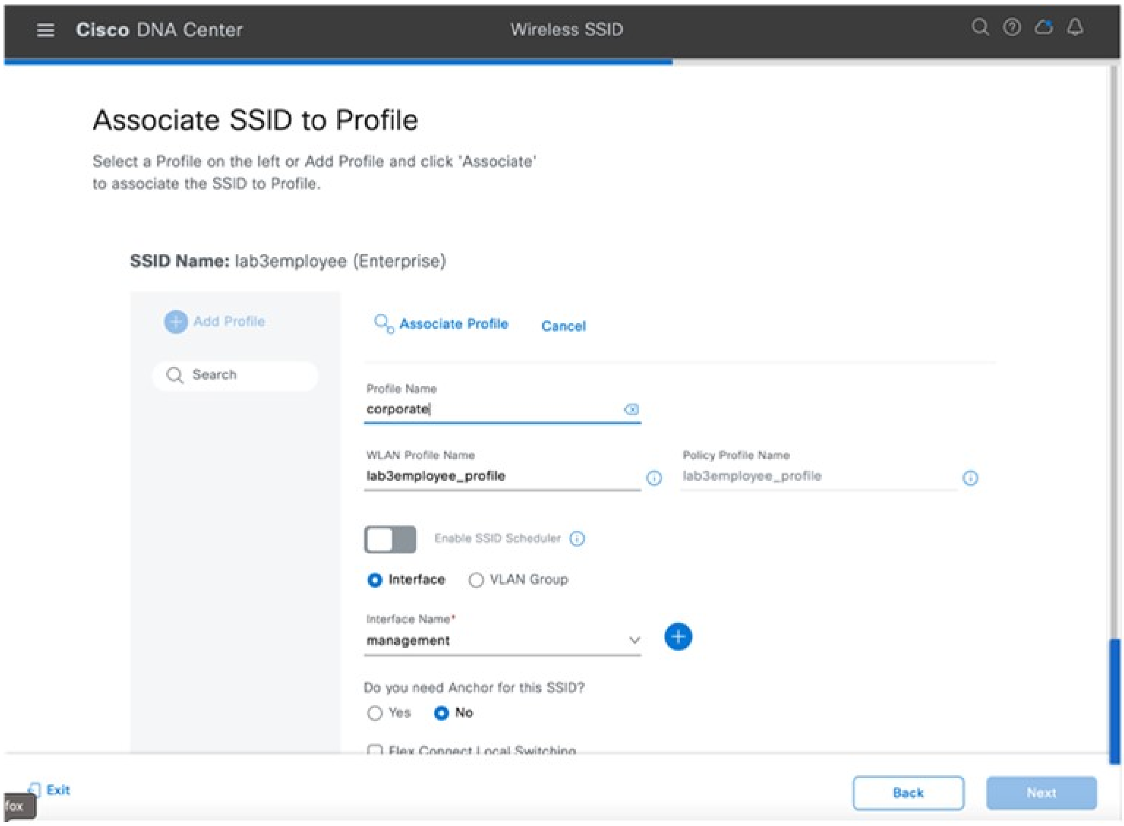
SSID Name: lab3employee (Enterprise)

0 profile(s) associated.

Step 5 Click **+ Add Profile** to create and add a new wireless profile.

The **Create a Wireless Profile** side panel is displayed.

Figure 19: Create a New Wireless Profile



Associate SSID to Profile

Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile.

SSID Name: lab3employee (Enterprise)

Profile Name: corporate

WLAN Profile Name: lab3employee_profile

Policy Profile Name: lab3employee_profile

Enable SSID Scheduler

● Interface ○ VLAN Group

Interface Name*: management

Do you need Anchor for this SSID?

○ Yes ● No

□ Flex Connect Local Switching

Step 6 In **Profile Name**, enter the name of the new wireless profile, and then click **Associate Profile**.

For this deployment guide, create a wireless profile named **Corporate**.

Step 7 Click the newly created profile and select the interface to be associated with this profile.

Step 8 Click **Save**, and then click **Next**.

Step 9 (Skip this step if SD-Access App is not deployed.) Under **Fabric**, select **No**.

The **Select Interface** field is displayed. This deployment guide only discusses non-SDA wireless deployments using Cisco DNA Center.

Step 10 From the **Select Interface** drop-down menu, select the employee to terminate the lab3Employee SSID onto the employee VLAN (VLAN 160) created in the previous procedure.

Step 11 Under **Guest Anchor** option, choose **No**.

Step 12 Uncheck the **Flex Connect Local Switching** check box, and then click **Save** to save an existing profile.

If a profile does not already exist, create a new profile, and click **Save**.

Step 13 Click **Next**.

Step 14 Review the summary for the **Network Profile**, and click **Save**.

Step 15 From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**.

Step 16 In the **Wireless Profiles** table, from the **Sites** column, click **Assign Site** for your desired profile.

For this deployment guide, click **Assign Site** for the newly created wireless profile, **Corporate**.

Step 17 In the **Global** section, click > to display the Milpitas area.

Step 18 Choose the **Milpitas** area.

All of the child site locations are automatically selected: **Building 23** with **Floor 1**, **Floor 2**, and **Floor 3** and **Building 24** with **Floor 1**, **Floor 2**, and **Floor 3**.

Step 19 Click **OK** to close the site hierarchy side panel.

Step 20 Click **Edit** under summary of **Network Profiles Attach Template(s)** to add CLI-based templates to the enterprise wireless network configuration.

Note You must define all the templates within the **Template Editor** dashboard of Cisco DNA Center. This design and deployment guide will not discuss the addition of templates because the guide does require knowledge of the CLI syntax for the specific Cisco Wireless Controller platform. The Cisco DNA Center CLI templates can be used to configure anything that cannot be configured through the intent-based profiles and/or the model config.

Step 21 Click **Save**.

The wireless profile named **Corporate** is assigned to the Milpitas area. The wireless profile contains the **lab3employee** SSID, so when wireless controllers and APs are assigned to the Milpitas area, the APs will broadcast the lab3employee SSID.

Step 22 Click **Finish** to add the **lab3employee** enterprise wireless network.

The new enterprise wireless network displays in the **Wireless Network Settings** dashboard.

For information about configuring overrides, see Define Site Override Support, on page 50.

Enterprise Wireless Network Features Configurable via Cisco DNA Center

Table 12: Enterprise Wireless Network Features Configurable via Cisco DNA Center

Feature	Type	Description
Wireless Network Name (SSID)	Text Field	The SSID for the WLAN.
WLAN Profile Name	Text Field	Cisco DNA Center considers SSID_Profile to be the default, which is based on the SSID name. You can change the WLAN profile name as per your requirements.
Policy Profile Name	Non Editable	Policy Profile Name is the same as the WLAN Profile Name and is not editable. Based on the WLAN profile name, Cisco DNA Center automatically generates the policy profile name for the Cisco Catalyst 9800 Series Wireless Controller.
BROADCAST SSID	On/Off Toggle	Determines whether the SSID will be broadcast in wireless beacons and probe responses.

Feature	Type	Description
SSID STATE	On/Off Toggle	Use the toggle button to turn on or turn off the radios on the APs. When the Admin Status is disabled, the APs remain associated with the wireless controller and are accessible, but the APs still require licenses.
Sensor	On/Off Toggle	Ensure that Sensor is disabled.
WIRELESS OPTION	Radio Button	Determines in which RF bands the SSID will be broadcast. The following wireless options are available: • Multiband operation (2.4 GHz, 5 GHz, and 6 GHz). • Multiband operation with band select. Band selection enables client radios that are capable of operating in both the 2.4 GHz and 5 GHz band to move to the typically less congested 5 GHz band by delaying probe responses on the 2.4 GHz channels. • 5 GHz only. • 2.4 GHz only. • 6 GHz only.

Feature	**Type**	**Description**
LEVEL OF SECURITY	Radio Button	

Feature	Type	Description
		Determines the Layer 2 (L2) security settings for the WLAN. Choose the encryption and authentication type for the network. The sites, buildings, and floors inherit settings from the global hierarchy. You can override the level of security at the site, building, or floor level. The following choices are available: • **Enterprise**: You can configure both WPA2 and WPA3 security authentication by checking the respective check boxes. **Note** Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). WPA3 is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher-grade security protocols for sensitive data networks. For multiband operation using only 2.4 GHz and 5 GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4 GHz, 5 GHz, and 6 GHz bands, you must enable WPA3 and disable WPA2 for the 6 GHz band to be operational on the devices running Cisco IOS Release 17.7 and later. • **Personal**: You can configure both WPA2 and WPA3 security authentication by checking the respective check boxes. By default, the WPA2 check box is enabled. If you choose Personal, enter the passphrase key in the Passphrase field. This key is used as the pairwise master key (PMK) between the clients and authentication server. **Note** WPA3-Personal brings better protection to individual users by providing more robust password-based authentication, making the brute-force dictionary attack much more difficult and time-consuming. For WPA2-Personal, you can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floors inherit the new settings. For information, see Preshared Key Override. For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4 GHz, 5 GHz, and 6 GHz bands, you must enable WPA3 and disable WPA2 for the 6 GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.

Feature	Type	Description
		(Optional) For WPA2-Personal, do the following to configure multi-preshared key (MPSK) support: **1.** Click **Configure MPSK**. **2.** In the **Configure MPSK** dialog box, click **Add to an MPSK**. You can add up to five MPSKs. **3.** From the **Priority** drop-down list, choose a priority. **Note** If the priority 0 key is not configured in central web authentication (CWA) flex mode, client connection to the WLAN may fail. From the **Passphrase Type** drop-down list, choose a passphrase type. **4.** In the **Passphrase** field, enter a passphrase. **5.** Click **Save**. MPSK applies to Layer 2 security configuration for WPA2-Personal. • **Open Secured**: From the **Assign Open SSID** drop-down list, choose an open SSID to redirect the clients to an open-secured SSID. The open-secured policy provides the least security. **Note** Fast Transition is not applicable for open-secured SSID. • **Open**: The open policy provides no security. It allows any device to connect to the wireless network without any authentication.

Feature	**Type**	**Description**
Primary Traffic Type	Drop Box	For Catalyst 9800 Series Wireless Controllers, the setting applies a precious metals QoS SSID policy in both the upstream and downstream direction for the WLAN/SSID. Precious metals policies control the maximum DSCP marking within the CAPWAP header as traffic is tunneled between the AP and the Cisco Wireless Controller in centralized (local mode) designs. The following choices are available: • VoIP (Platinum): QoS on the wireless network is optimized for wireless voice and data traffic. • Video (Gold): QoS on the wireless network is optimized for video traffic. • Best Effort (Silver): QoS on the wireless network is optimized for wireless data traffic only. • Non-real Time (Bronze): QoS on the wireless network is optimized for low-bandwidth usage.
Fastlane	Check Box	You can check this check box only when the type of Enterprise Network is Voice and Data. For the Catalyst 9800 Series Wireless Controller, the Fastlane check box enables Auto QoS in Fastlane mode. Auto QoS in Fastlane mode configures the Fastlane EDCA profile for both the 5 GHz and 2.4 GHz bands. However, no precious metals QoS SSID policy is applied to the WLAN/SSID when the Fastlane check box is selected.

Feature	Type	Description
Configure AAA	Link	Click **Configure AAA** to add and configure the AAA servers for the enterprise wireless network SSID. Select the **Authentication, Authorization, and Accounting server** from **Drop Box**. Click **+** to add a server. **Note** You can configure a maximum of six AAA servers for an SSID of an enterprise wireless network for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches. From the **Additional Server** drop-down list, choose the server IP address. To use the AAA server for accounting, check the **Copy Same Servers for Accounting** check box. To configure a different accounting server for an SSID, do the following: **1.** From the **Configure Accounting Server** drop-down list, you can either search for a server IP address by entering its name in the Search field or choose the accounting server IP address. **2.** Click **+** to add a server. **Note** You can configure a maximum of six accounting servers for an SSID of enterprise wireless network for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches. **3.** From the **Additional Server** drop-down list, choose the server IP address. Cisco DNA Center allows you to override the set of AAA server configurations for the SSID at the site level. For each set of overridden AAA settings per SSID, Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Cisco DNA Center creates the new WLAN profiles equal to the number of floors. You must reprovision the device to override the AAA servers at the site level.
Deny RCM Clients	Check Box	Check the check box to deny clients with randomized MAC addresses.
Mac Filtering	Check Box	This is an additional L2 security settings that applies MAC address filtering for the WLAN.

Feature	Type	Description
AAA Override	Check Box	Check box to enable the AAA override functionality. By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.
Enable Posture	Check Box	Check this check box to enable posture assessment. The **Pre-Auth ACL List Name** drop-down list appears when you enable posture. Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients' access to protected areas of a network.
Pre-Auth ACL List Name	Drop Box	Choose the ACL list name that you already created to map with the SSID. **Note** AAA configuration is mandatory for posturing. Click **Configure AAA** to add AAA servers for the enterprise wireless network SSID.
Advanced Settings – FAST TRANSITION (802.11r)	Radio Button and Check Box	Additional L2 security settings for the WLAN that controls 802.11r Fast Transition (FT). The following radio button choices are available: • Adaptive: This setting allows devices that support 802.11r Fast Transition to use it, as well as other 802.11r and non-802.11r devices to associate in a non-Fast Transition state. This is the default setting. • Enable: This setting enables 802.11r Fast Transition. • Disable: This setting disables 802.11r Fast Transition. Over the DS: Check box that enables Over-the-DS (Distribution System) Fast Transition. With Over-the-DS Fast Transition, the wireless station communicates with the target AP through the current AP, which is then forwarded through the wireless controller. The Cisco-Apple best practice is to disable Over-the-DS, even though the default is enabled.
Advanced Settings – Protected Management Frame (802.11w)	Radio Button	The options available under Protected Management Frame (802.11w) vary based on the settings that you chose under Level of Security. The following options may be available: • Optional • Required • Disabled The Required option is mandatory for WPA3.

Feature	Type	Description
Advanced Settings – Session timeout	Check Box and Integer Field	Configures the maximum time for a client session to remain active before requiring reauthorization. The range is between 300 and 86,400 seconds (5 minutes and 24 hours). The default is enabled with a time of 1800 seconds (30 minutes).
Advanced Settings – Client Exclusion	Check Box and Integer Field	Configures the amount of time a wireless client is excluded from attempting to authenticate after the maximum number of authentication failures has been exceeded. The default is enabled with a time of 180 seconds (3 minutes).
Advanced Settings – MFP CLIENT PROTECTION	Radio Button	Additional security setting that controls the use of 802.11w Protected Management Frames for the WLAN. The following radio button choices are available: • Optional: This setting allows wireless stations to use the 802.11w Protected Management Frames that they support and allows other wireless stations that do not support PMFs to coexist on the WLAN. This is the default setting. • Required: The wireless client is required to use Protected Management Frames on the WLAN. • Disabled: Protected Management Frames are disabled on the WLAN.
Advanced Settings – 11k Neighbor List	Check Box	Controls the use of 802.11k Assisted Roaming neighbor lists for the WLAN, which can limit the need for passive and active scanning by the wireless client. The default setting is enabled for the band (5 GHz or 2.4 GHz) with which the client is associated.
Advanced Settings – Client User Idle Timeout	Check box	Client User Idle Timeout: Check this check box to set the user idle timeout for a WLAN. **Note** If the data sent by the client is more than the threshold quota specified as the user idle timeout, the client is considered to be active and the wireless controller begins another timeout period. By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

Feature	Type	Description
NAS-ID	Drop-down list	NAS-ID Opt drop-down list, choose the required type of network access server identifier (NAS ID). To specify a custom script for the NAS ID, choose **Custom Option** from the **NAS-ID Opt** drop-down list and enter the custom script in the corresponding **Custom Script for Opt** field. You can enter up to 31 alphanumeric characters, special characters, and spaces for the custom script. Cisco DNA Center does not support the special characters ?, ", < , and trailing spaces for the custom script. **Note** Cisco DNA Center supports NAS ID with custom script only for Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.7 or later. (Optional) Click **+** to add another NAS ID. You can add up to three NAS IDs.
Advanced Settings – Coverage Hole Detection	Toggle button	Use the **Coverage Hole Detection** toggle button to enable or disable the coverage hole detection functionality.
Advanced Settings – Client Rate Limit	Integer Field	Configure Client Rate Limit: Enter a value for the client rate limit in bits per second. The valid range is from 8000 through 100,000,000,000. The value must be a multiple of 500. The following are the valid ranges for client rate limit on Cisco IOS XE devices: • The valid range for the Cisco Catalyst 9800-L Wireless Controller, the Cisco Catalyst 9800-40 Wireless Controller, and the Cisco Catalyst 9800-80 Wireless Controller is from 8000 through 67,000,000,000 bits per second. • The valid range for the Cisco Catalyst 9800-CL Wireless Controller is from 8000 through 10,000,000,000 bits per second. • The valid range for the Cisco Embedded Wireless Controller on Catalyst Access Points is from 8000 through 2,000,000,000 bits per second. • The valid range for the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches is from 8000 through 100,000,000,000 bits per second.

Feature	Type	Description
Advanced Settings – Directed Multicast Service	Check box	Directed Multicast Service: Check this check box to enable directed multicast service. **Note** By default, Directed Multicast Service (DMS) is enabled. Using the DMS, the client requests APs to transmit the required multicast packets as unicast frames, which allows clients to sleep for a longer time and saves the battery power.
Advanced Settings – Radius Client Profiling	Toggle button	For RADIUS Client Profiling, use this toggle button to enable or disable RADIUS profiling on a WLAN. **Note** At least one AAA or PSN server is required to enable this feature.
Advanced Settings – CCKM	Toggle button	Configure CCKM: Use this toggle button to enable CCKM as the authentication key management option in Cisco DNA Center. Timestamp Tolerance: This field is visible only if you enable CCKM. Enter the CCKM tolerance level. **Note** You can configure CCKM only if SSID has Layer 2 security as Enterprise in WPA2 or WPA2+WPA3.
Advanced Settings – 11v BSS TRANSITION SUPPORT	Multiple Check Boxes and Integer Field	Additional settings for support of 802.11v Wireless Network Management (WNM) for the WLAN. The following settings are available: BSS Max Idle Service: Check box that enables the maximum idle service for the WLAN. Allows APs to send the timeout value to the wireless client within association and reassociation response frames. The default setting is enabled.

Enterprise Wireless Network Settings Configured in the Deployment Guide

Table 13: Enterprise Wireless Network Settings Configured in the Deployment Guide

Feature	Settings
Wireless Network Name (SSID)	lab3employee
Broadcast SSID	On
Admin Status	On
Wireless Option	Multi band operation (2.4 GHz, 5 GHz, 6 GHz)
Primary Traffic Type	VoIP (platinum)
Configure AAA	AAA configured
Level of Security	WPA2

Feature	Settings
AAA Override	Enabled
Enable Posture	Unchecked
Deny RCM Clients	Unchecked
Advanced Security Options - Mac Filtering	Unchecked
Advanced Security Options - Fast Transition	Adaptive
Type of Enterprise Network	Voice and Data
Fastlane	Unchecked
Advanced Settings – FAST TRANSITION (802.11r)	Adaptive, Over the DS Checked
Advanced Settings – Mac Filtering	Checked
Advanced Settings – Session timeout	Checked, 1800 seconds
Advanced Settings – Client Exclusion	Checked, 180 seconds
Advanced Settings – MFP CLIENT PROTECTION	Optional
Advanced Settings –Protected Management Frame	Disabled
Advanced Settings – 11k Neighbor List	Checked
Advanced Settings – Radius Client Profiling	Unchecked
Advanced Settings – Configure Client Rate Limit	Blank
Advanced Settings – Coverage Hole Detection	Checked
Configure CCKM	Unchecked
NAS-ID	Blank
Advanced Settings – 11v BSS TRANSITION SUPPORT	BSS Max Idle Service – Checked Client Idle User Timeout – Checked, 300 seconds Directed Multicast Service - Checked

Define Site Override Support

WLAN profiles created with different AAA settings can be assigned at different site levels. Site level overrides will push a new WLAN profile to the wireless controller. You can override the global SSID with the settings based on area, buildings and floor levels. Perform the following procedure to configure the overrides.

Procedure

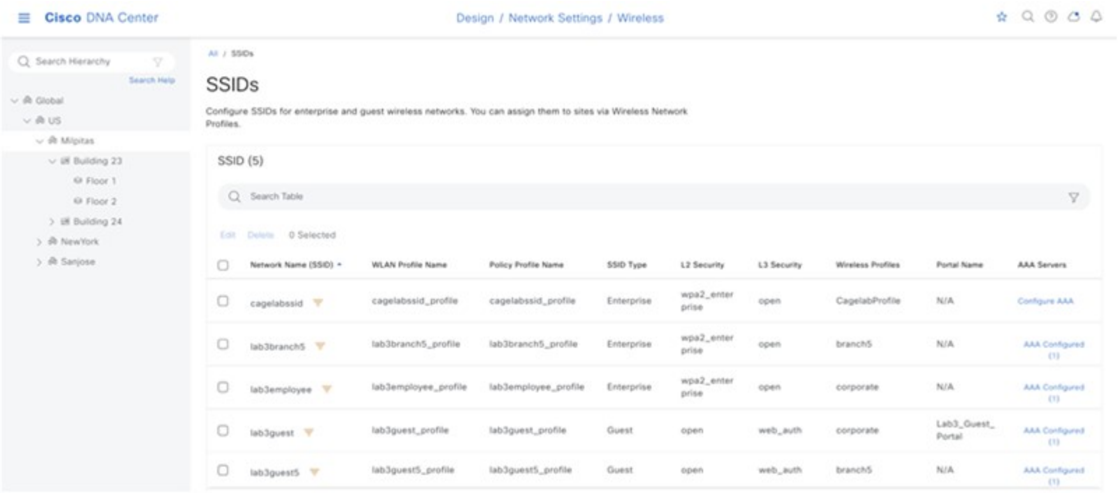
Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Click **SSIDs**.

Step 3 Expand the sites, and then click on the desired site in the left pane.

Step 4 Select **lab3employee** SSID, and then click **Edit**.

Figure 20: SSID Site Override Settings



SSIDs

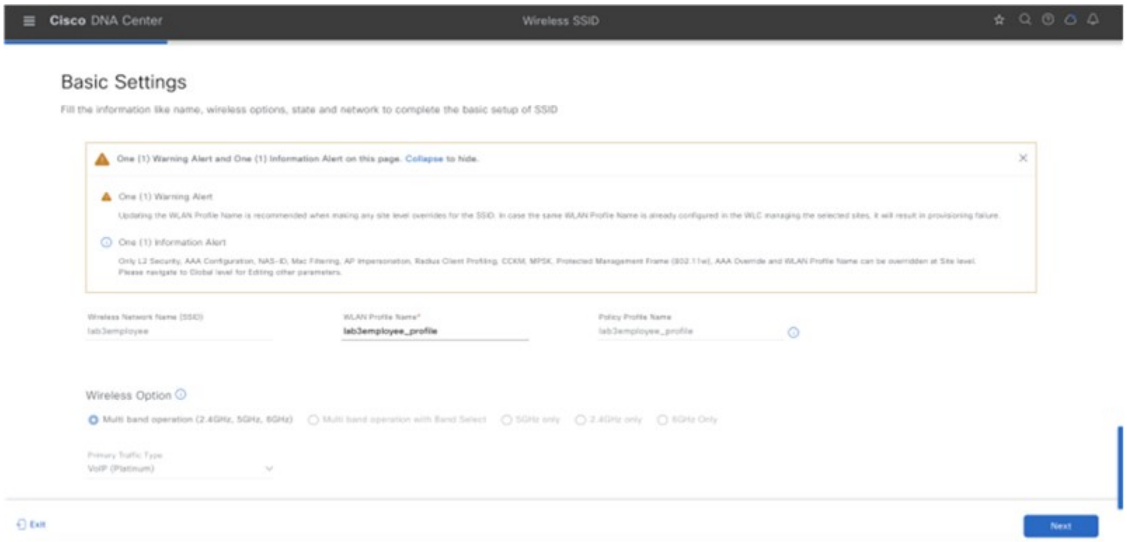
Configure SSIDs for enterprise and guest wireless networks. You can assign them to sites via Wireless Network Profiles.

SSID (5)

Network Name (SSID)	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
cagelabssid	cagelabssid_profile	cagelabssid_profile	Enterprise	wpa2_enterprise	open	CagelabProfile	N/A	Configure AAA
lab3branch5	lab3branch5_profile	lab3branch5_profile	Enterprise	wpa2_enterprise	open	branch5	N/A	AAA Configured (1)
lab3employee	lab3employee_profile	lab3employee_profile	Enterprise	wpa2_enterprise	open	corporate	N/A	AAA Configured (1)
lab3guest	lab3guest_profile	lab3guest_profile	Guest	open	web_auth	corporate	Lab3_Guest_Portal	AAA Configured (1)
lab3guest5	lab3guest5_profile	lab3guest5_profile	Guest	open	web_auth	branch5	N/A	AAA Configured (1)

Step 5 Click **Next** and configure the override settings for the selected site.

Figure 21: Override Settings for a Site



Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID

One (1) Warning Alert and One (1) Information Alert on this page. Collapse to hide.

One (1) Warning Alert

Updating the WLAN Profile Name is recommended when making any site level overrides for the SSID. In case the same WLAN Profile Name is already configured in the WLC managing the selected sites, it will result in provisioning failure.

One (1) Information Alert

Only L2 Security, AAA Configuration, NAS-ID, Mac Filtering, AP Impersonation, Radius Client Profiling, CCKM, MPSK, Protected Management Frame (802.11w), AAA Override and WLAN Profile Name can be overridden at Site level. Please navigate to Global level for Editing other parameters.

Wireless Network Name (SSID): lab3employee

WLAN Profile Name*: lab3employee_profile

Policy Profile Name: lab3employee_profile

Wireless Option

● Multi band operation (2.4GHz, 5GHz, 6GHz) ○ Multi band operation with Band Select ○ 5GHz only ○ 2.4GHz only ○ 6GHz Only

Primary Traffic Type: VoIP (Platinum)

Step 6 Click **Save** in the last page to assign the profile to the site.

The next time the wireless controller is provisioned, the configuration will be pushed to the wireless controller managing that site.

Note

Cisco recommends updating the WLAN Profile Name when making any site level overrides for the SSID. If the same WLAN profile name is already configured in the wireless controller that manages the selected sites, a provisioning failure will occur.

Only L2 Security, AAA Configuration, NAS-ID, Mac Filtering, AP Impersonation, Radius Client Profiling, CCKM, MPSK, Protected Management Frame (802.11w), AAA Override, and WLAN Profile Name can be overridden at the site levels. To edit other parameters, navigate to the global level.

Configure Guest Wireless SSID

Guest wireless networks must be defined at the global level of the site hierarchy. Once defined, you can apply guest wireless networks to wireless profiles. You can then assign wireless profiles to one or more sites within the hierarchy.

For this deployment guide, a single guest wireless network (SSID) named **lab3guest** is provisioned.

Procedure

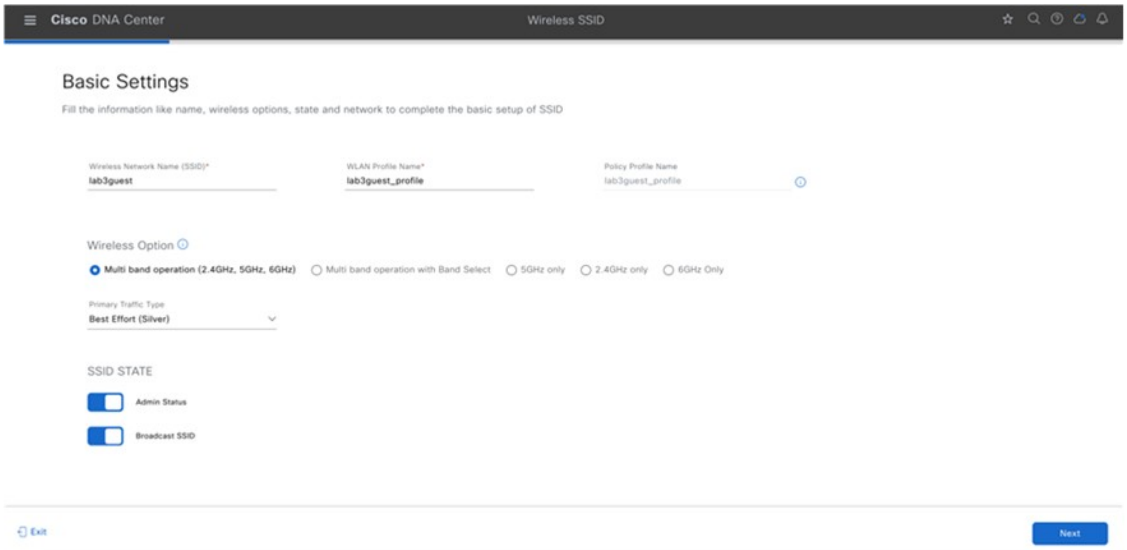
Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Click **SSIDs**.

Step 3 Hover your cursor over **+ Add** and choose **Guest**.

The **Basic Settings** window is displayed.

Figure 22: Basic Settings Window to Create a Guest Wireless SSID



Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID

Wireless Network Name (SSID)* lab3guest

WLAN Profile Name* lab3guest_profile

Policy Profile Name lab3guest_profile

Wireless Option

● Multi band operation (2.4GHz, 5GHz, 6GHz) ○ Multi band operation with Band Select ○ 5GHz only ○ 2.4GHz only ○ 6GHz Only

Primary Traffic Type Best Effort (Silver)

SSID STATE

Admin Status

Broadcast SSID

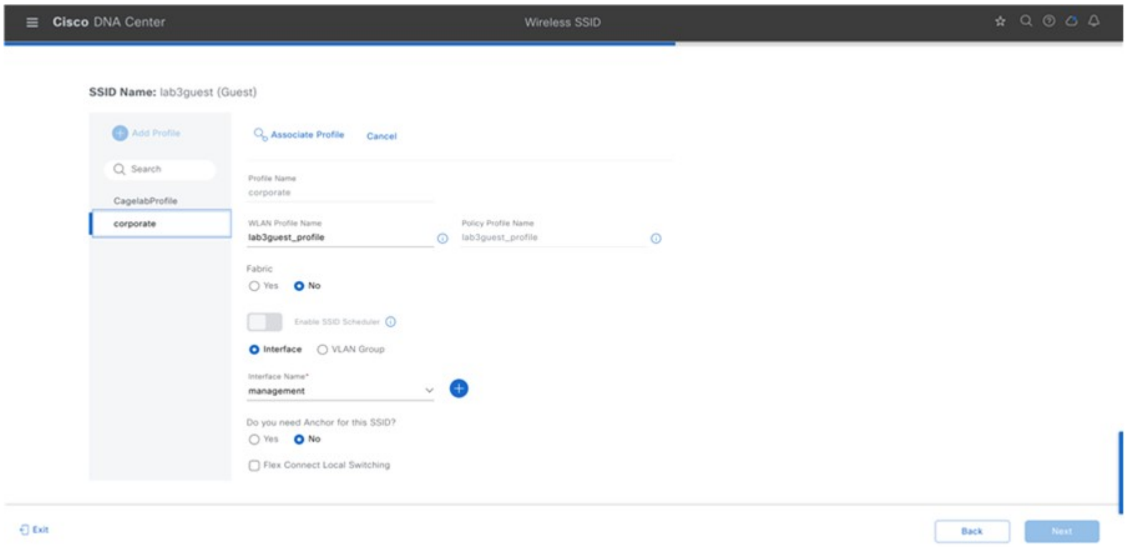
For information about the features that can be configured for guest wireless networks via Cisco DNA Center, see Guest Wireless Network Features Configurable via Cisco DNA Center, on page 57.

Step 4 Enter the information for the **Basic Settings** and click **Next**.

The next screen in the workflow is displayed. Here, you can attach the guest wireless network to the existing corporate wireless profile.

For information about the settings for the guest wireless network configured for this deployment guide, see Guest Wireless Network Settings Configured in the Deployment Guide, on page 68.

Figure 23: Create a Guest Wireless Profile



SSID Name: lab3guest (Guest)

Profile Name
corporate

WLAN Profile Name
lab3guest_profile

Policy Profile Name
lab3guest_profile

Fabric
○ Yes ● No

Enable SSID Scheduler

● Interface ○ VLAN Group

Interface Name*
management

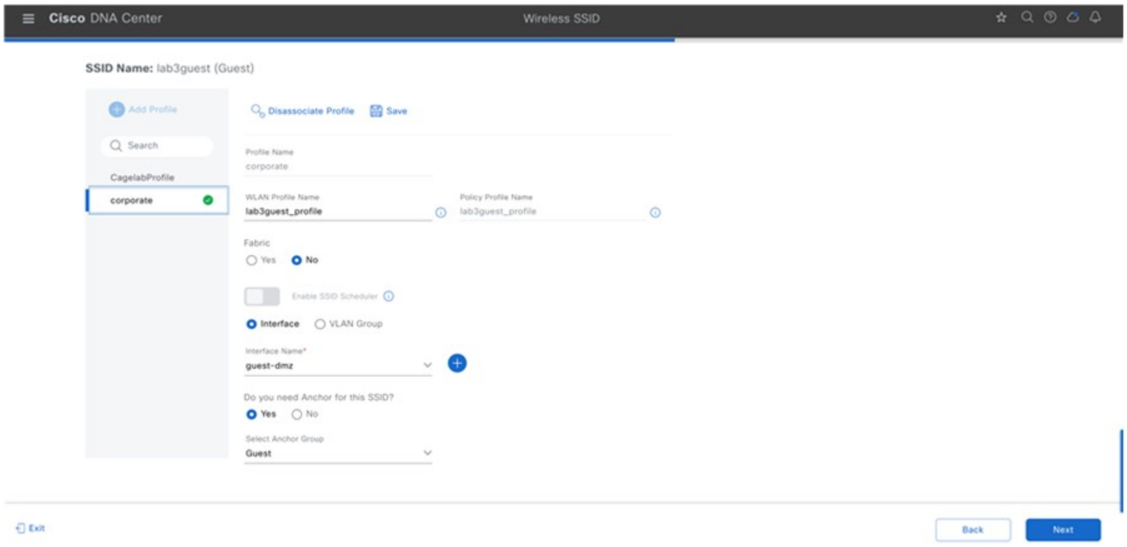
Do you need Anchor for this SSID?
○ Yes ● No

□ Flex Connect Local Switching

Step 5 Choose the **Corporate Wireless** profile.

Step 6 Click **Edit** in the **Wireless Profile** side panel to add the guest wireless network.

Figure 24: Edit a Wireless Profile Side Panel



SSID Name: lab3guest (Guest)

Profile Name
corporate

WLAN Profile Name
lab3guest_profile

Policy Profile Name
lab3guest_profile

Fabric
○ Yes ● No

Enable SSID Scheduler

● Interface ○ VLAN Group

Interface Name*
guest-dmz

Do you need Anchor for this SSID?
● Yes ○ No

Select Anchor Group
Guest

Step 7 Under **Fabric**, choose **No**.

Selecting **No** will automatically cause additional fields to appear.

This deployment guide only discusses non-SDA wireless deployments using Cisco DNA Center.

Step 8 Select **Yes** next to **Do you need a Guest Anchor for this Guest SSID**.

This will configure a traditional autoanchor relationship between the enterprise (foreign) and the guest (anchor) wireless controller. Typically, the guest (anchor) wireless controller is located within an Internet Edge DMZ segment of the campus network. If you choose **Yes**, from the **Select Anchor Group** drop-down list, choose an anchor group for the SSID.

To create an anchor group, do the following:

a) From the top-left corner, click the menu icon and choose **Design** > **Network Settings**.
b) Click the **Wireless** tab.
c) From the left hierarchy tree, choose **Global**.
d) Click **Anchor Groups**.

   The **Anchor Groups** window opens.

e) In the **Anchor Group** table, click **Add**.
f) In the **Anchor Group Name** field of the **Anchor Group** slide-in pane, enter the anchor group name.
g) To add a managed wireless controller as an anchor, click **Add Managed WLC** and do the following in the **Add Managed WLC** dialog box:

   1. Check the check box next to the name of the devices that you want to add as anchors.

      To search for a device, in the **Search Table** search field, enter either the partial name or the full name of the device and press **Enter**.

   2. Click **Add**.

h) (Optional) To add an external wireless controller as an anchor, click **Add External WLC** and do the following in the **Add External WLC** dialog box:

   1. In the **Device Name** field, enter the device name.
   2. From the **Device Series** drop-down list, choose a device series.
   3. In the **Peer IP Address** field, enter the peer IP address.
   4. (Optional) In the **NAT IP Address** field, enter the Network Address Translation (NAT) IP address.
   5. In the **MAC Address** field, enter the MAC address of the device.
   6. In the **Mobility Group Name** field, enter the mobility group name.
   7. (Optional) In the **Hash** field, enter the hash for the Cisco Catalyst 9800 Series Wireless Controller.

      Note This field is available for only the Cisco Catalyst 9800-CL Wireless Controllers.

   8. Click **Add**.

i) (Optional) To add an existing external wireless controller as an anchor, click **Add Existing External WLC** and do the following in the **Add Existing External WLC** dialog box:

   1. Check the check box next to the name of the devices that you want to add as anchors.

      To search for a device, in the **Search Table** search field, enter either the partial name or the full name of the device and press **Enter**.

   2. Click **Add**.

j) (Optional) To set the priority for an anchor, from the **Priority Order** drop-down list, choose the priority for the anchor wireless controller.

k) Click **Save**.

For more information, see the "Create an Anchor Group" topic in the *Cisco DNA Center User Guide*.

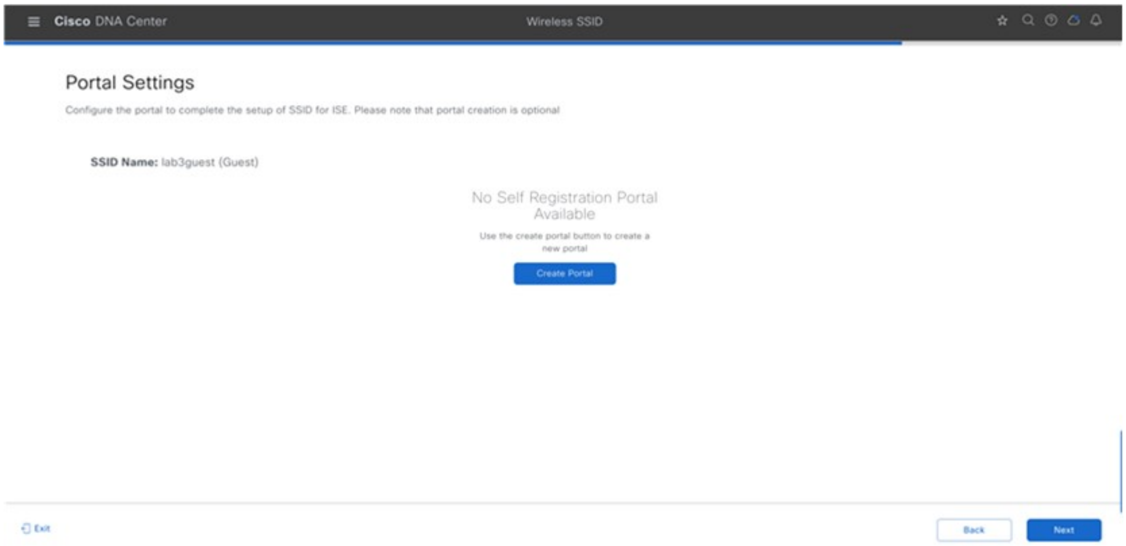
Step 9 From the **Select Interface** drop-down menu, select **guest-dmz**.

This will terminate guest traffic on the guest-dmz VLAN (VLAN 125).

Step 10 Click **Next**.

The **Portal Customization** page is displayed.

Figure 25: Create a Guest Wireless Network Portal Customization



Portal Settings

Configure the portal to complete the setup of SSID for ISE. Please note that portal creation is optional

SSID Name: lab3guest (Guest)

No Self Registration Portal Available

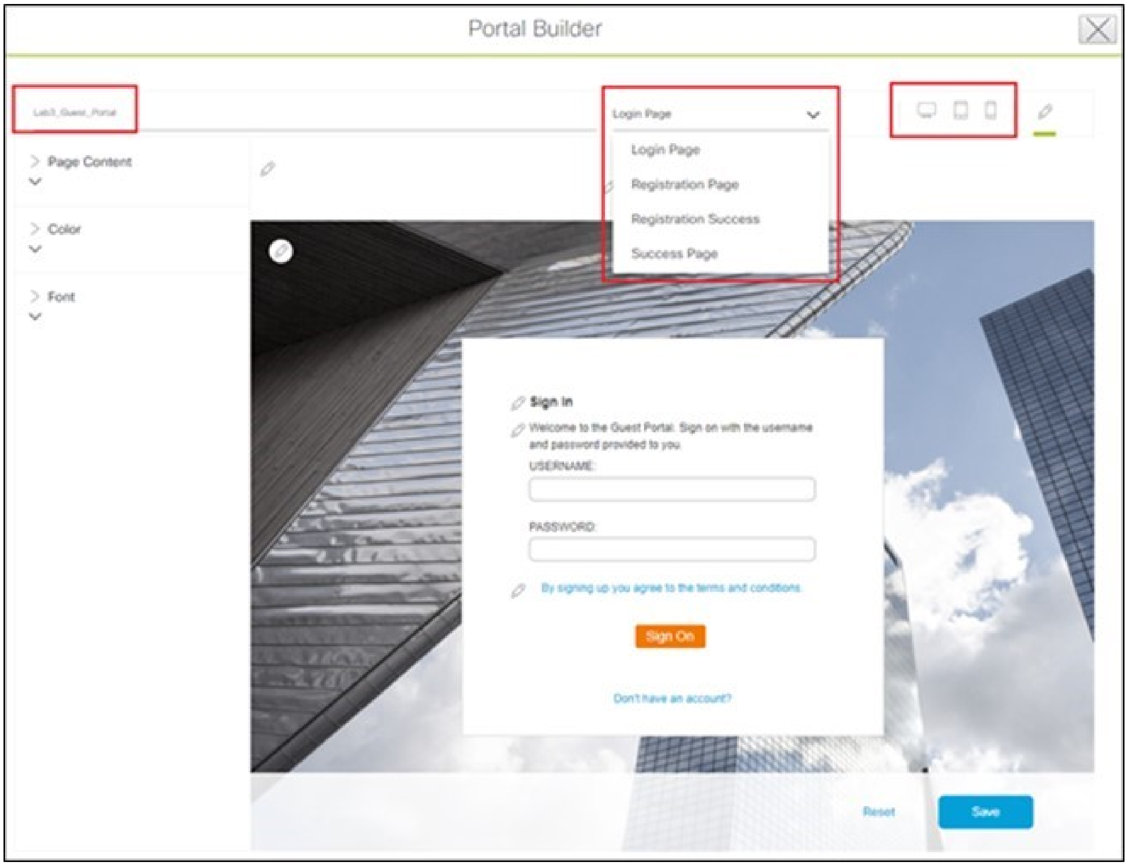
Use the create portal button to create a new portal

Step 11 To add a new guest portal within Cisco ISE, click **Create Portal**.

The **Portal Builder** page is displayed.

You have the option to leave without portal creation.

Figure 26: Portal Builder Screen



Welcome to the Guest Portal. Sign on with the username and password provided to you.

By signing up you agree to the terms and conditions

Step 12 Enter the necessary information. You must at least name the guest portal.

For this deployment guide, the portal has been named **Lab3_Guest_Portal**. The drop-down menu in the top center of the **Portal Builder** allows you to customize the Login Page, Registration Page, Registration Success, and Success Page of the portal. You can customize the color scheme, fonts, page content, logo, and background for the web portal. You can also preview the portal to see what it will look like on a smart phone, tablet, and computer.

Step 13 Click **Save** to create the new guest portal on the Cisco ISE server and return to the guest wireless network workflow.

The new guest portal is now displayed.

Step 14 Click **Next**.

The **Summary** page of Guest SSID Configuration is displayed.

Step 15 Click **Save**.

The guest wireless SSID (lab3guest) is displayed in the **Wireless Network Settings** dashboard.

Step 16 Click **Sites** in network profile summary page to bring up a panel displaying the site hierarchy.

Step 17 Under **Global**, click the >to display the Milpitas area.

Step 18 Select the Milpitas area.

The child site locations, **Building 23 - Floor 1**, **Floor 2**, and **Floor 3** and **Building 24 - Floor 1**, **Floor 2**, and **Floor 3**, are automatically selected.

Note It is best practice to only select floors in a wireless network profile assignment. Selecting floors helps you to make changes, like removing a floor from network hierarchy or applying a different wireless network profile for a particular set of floors without significant disruption. If you have different SSIDs on different floors or enable 6E with a different profile per floor, different network profiles might be necessary. If you create different sets of SSIDs on the same floor, you will have to split the floor into multiple, different network profiles.

Step 19 Click **OK** to close the site hierarchy side panel.

Step 20 Click **+ Add** under **Attach Template(s)** to add the CLI-based templates to the enterprise wireless network configuration.

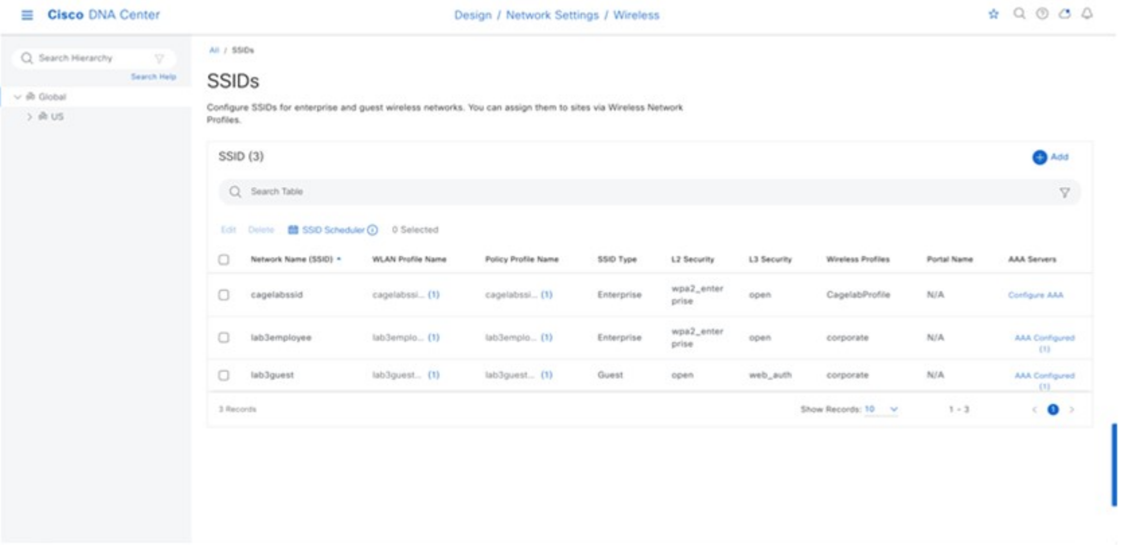
You must define all the templates within the **Template Editor** dashboard of Cisco DNA Center. This design and deployment guide will not discuss the addition of templates because the guide does not require knowledge of the CLI syntax for the specific Cisco Wireless Controller platform. Wireless features not supported by the web-based graphical user interface of Cisco DNA Center may be added through templates.

Step 21 Click **Save** in the **Edit a Wireless Profile** side panel to save the edits to the corporate wireless profile.

lab3guest SSID is added to the corporate wireless profile. This ensures that when wireless controllers and APs are assigned to the Milpitas area, the APs will broadcast the **lab3guest** SSID.

Step 22 Click **Save** to add the **lab3guest** guest wireless network to the corporate wireless profile.

Figure 27: Wireless Network Settings Dashboard with Enterprise and Guest SSIDs



SSIDs

Configure SSIDs for enterprise and guest wireless networks. You can assign them to sites via Wireless Network Profiles.

SSID (3)

Network Name (SSID)	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
cagelabssid	cagelabssi... (1)	cagelabssi... (1)	Enterprise	wpa2_enterprise	open	CagelabProfile	N/A	Configure AAA
lab3employee	lab3emplo... (1)	lab3emplo... (1)	Enterprise	wpa2_enterprise	open	corporate	N/A	AAA Configured (1)
lab3guest	lab3guest... (1)	lab3guest... (1)	Guest	open	web_auth	corporate	N/A	AAA Configured (1)

3 Records   Show Records: 10   1 - 3

For information about provisioning ISE Settings from Cisco DNA Center, see Provision Cisco ISE Settings from Cisco DNA Center, on page 69.

Guest Wireless Network Features Configurable via Cisco DNA Center

Table 14: Guest Wireless Network Features Configurable via Cisco DNA Center

Feature	Type	Description
Wireless Network Name (SSID)	Text Field	The SSID for the WLAN.

Feature	Type	Description
WLAN Profile Name	Text Field	Cisco DNA Center will take SSID_Profile as default based on SSID Name. You can change the WLAN profile name as per your requirements.
Policy Profile Name	Non Editable	Policy Profile Name is the same as the WLAN Profile Name and is not editable. Based on the WLAN profile name, Cisco DNA Center automatically generates the policy profile name for the Cisco Catalyst 9800 Series Wireless Controller.
WIRELESS OPTION	Radio Button	Determines in which RF bands the SSID will be broadcast. The following choices are available: • Multiband operation (2.4 GHz, 5 GHz, and 6 GHz) • Multiband operation with band select. Band selection enables client radios that are capable of operating in both the 2.4 GHz and 5 GHz band to move to the typically less congested 5 GHz band by delaying probe responses on the 2.4 GHz channels. • 5 GHz only. • 2.4 GHz only. • 6 GHz only.
Primary Traffic Type	Drop Box	For Catalyst 9800 Series Wireless Controllers, this setting applies a precious metals QoS SSID policy in both the upstream and downstream direction for the WLAN/SSID. Precious metals policies control the maximum DSCP marking within the CAPWAP header, as traffic is tunneled between the AP and the Cisco Wireless Controller in centralized (local mode) designs. For Cisco AireOS Wireless Controllers, this setting applies the Platinum QoS profile to the WLAN/SSID. Application Visibility is enabled on the WLAN/SSID, but no AVC profile is applied. The Fastlane EDCA profile is set for both the 802.11a/n/ac (5 GHz) and the 802.11b/g/n (2.4 GHz) radios. • VoIP (Platinum): QoS on the wireless network is optimized for wireless voice and data traffic. • Video (Gold): QoS on the wireless network is optimized for video traffic. • Best Effort (Silver): QoS on the wireless network is optimized for wireless data traffic only. • Nonreal Time (Bronze): QoS on the wireless network is optimized for low-bandwidth usage.
Broadcast SSID	On/Off Toggle	Determines whether the SSID will be broadcast in wireless beacons and probe responses. The default setting is on.
SSID STATE	On/Off Toggle	Use this toggle button to turn on or turn off the radios on the APs. When the Admin Status is disabled, the APs remain associated with the wireless controller and are accessible, but the APs still require licenses.

Feature	Type	Description
LEVEL OF SECURITY L2 Security	Radio Button	

Feature	Type	Description
		Determines the Layer 2 (L2) security settings for the WLAN. Choose the encryption and authentication type for the network. The sites, buildings, and floors inherit settings from the global hierarchy. You can override the level of security at the site, building, or floor level. The following choices are available: • **Enterprise**: You can configure both WPA2 and WPA3 security authentication by checking the respective check boxes. **Note** Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). WPA3 is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher-grade security protocols for sensitive data networks. For multiband operation using only 2.4 GHz and 5 GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4 GHz, 5 GHz, and 6 GHz bands, you must enable WPA3 and disable WPA2 for the 6 GHz band to be operational on the devices running Cisco IOS Release 17.7 and later. • **Personal**: You can configure both WPA2 and WPA3 security authentication by checking the respective check boxes. By default, the WPA2 check box is enabled. If you choose Personal, enter the passphrase key in the Passphrase field. This key is used as the pairwise master key (PMK) between the clients and authentication server. **Note** WPA3-Personal brings better protection to individual users by providing more robust password-based authentication, making the brute-force dictionary attack much more difficult and time-consuming. For WPA2-Personal, you can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floors inherit the new settings. For information, see Preshared Key Override. For multiband operation using only 2.4 GHz and 5 GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4 GHz, 5 GHz, and 6 GHz bands, you must enable WPA3 and disable WPA2 for the 6 GHz band to be operational on the devices running Cisco IOS Release 17.7 and later. (Optional) For WPA2-Personal, do the following to configure multi-preshared key (MPSK) support: 1. Click **Configure MPSK**.

Feature	Type	Description
		2. In the **Configure MPSK** dialog box, click **Add to an MPSK**. You can add up to five MPSKs. **3.** From the **Priority** drop-down list, choose a priority. **Note** If the priority 0 key is not configured in central web authentication (CWA) flex mode, the client connection to the WLAN may fail. From the **Passphrase Type** drop-down list, choose a passphrase type. **4.** In the **Passphrase** field, enter a passphrase. **5.** Click **Save**. MPSK is not supported on Cisco AireOS Wireless Controllers. MPSK applies to Layer 2 security configuration for WPA2- Personal. • **Open Secured**: From the **Assign Open SSID** drop-down list, choose an open SSID to redirect the clients to an open-secured SSID. The open-secured policy provides the least security. **Note** Fast Transition is not applicable for open-secured SSID. • **Open**: The open policy provides no security. It allows any device to connect to the wireless network without any authentication.
LEVEL OF SECURITY L3 security	Radio Button	Determines the Layer 3 security settings for the WLAN. The following options are available: • Web Auth: Specifies Web Authentication, where guest devices are redirected to a web portal for authentication. This is the default setting. • Open: Specifies an open SSID with no authentication.

Feature	Type	Description
AUTHENTICATION SERVER	Drop Box	This selection is only available if Web Auth is selected within LEVEL OF SECURITY. Determines the web portal and authentication server for Web Auth. • Central Web Authentication: This setting configures Central Web Authentication (CWA), where the Cisco ISE server defined under **System Settings** > **Settings** > **Authentication and Policy Servers** is both the web portal and the authentication server. This is the default setting. • Web Authentication Internal: Web authentication or Web Auth is a Layer 3 security method that allows a client to pass Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) traffic only until the client has passed some form of authentication. For web authentication internal, the client is redirected to a page that is constructed by the Cisco Wireless Controller. • Web Authentication External: The client is redirected to the specified URL. Enter a redirect URL in the Web Auth URL field. • Web Passthrough Internal: Web passthrough is a solution that is used for guest access and requires no authentication credentials. In web passthrough authentication, wireless users are redirected to the usage policy page when they use the internet for the first time. After accepting the policy, the clients are allowed to use the internet. • Web Passthrough External: The client is redirected to the specified URL. Enter a redirect URL in the Web Auth URL field. • Open: There is no security at layer 3 level and any device can connect to SSID.
AUTHENTICATION SERVER > ISE Authentication > What kind of portal are you creating today?	Drop-down Menu	The selection is only available if ISE Authentication is chosen. Determines the type of guest portal that will be created within the Cisco ISE server. The following options are available: • Self Registered: With this type of portal, guests onboard themselves to the network. This is the default setting. • Hotspot: This configures an 802.11u hotspot portal.

Feature	Type	Description
AUTHENTICATION SERVER > ISE Authentication > Where will your guests redirect after successful authentication?	Drop-down Menu	This selection is only available if ISE Authentication is selected. Determines what web page is displayed after guests have successfully authenticated to the network. The following options are available: • Success Page: A dedicated page you create that indicates authentication was successful. From there, the guest would need to retype the original URL that they were attempting to reach. • Original URL: Once authentication is successful, the guest is automatically redirected to the original URL that they were attempting to reach. This is the default setting. • Custom URL: Once authentication is successful, the guest is automatically redirected to a URL of your choice.
AUTHENTICATION SERVER > External Authentication > Web Auth URL?	Text Field	This selection is only available if External Authentication is selected. Specifies the URL of the Web Auth server. The guest will be redirected to this URL to be authenticated to the network.

Feature	Type	Description
Configure AAA	Link	Click **Configure AAA** to add and configure the AAA servers for the enterprise wireless network SSID. Choose **Authentication, Authorization, and Accounting server** from **Drop Box**. Click **+** to add a server. **Note** You can configure a maximum of six AAA servers for an SSID of enterprise wireless network for the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches. From the **Additional Server** drop-down list, choose the server IP address. To use the AAA server for accounting, check the **Copy Same Servers for Accounting** check box. To configure a different accounting server for an SSID, do the following: **1.** From the **Configure Accounting Server** drop-down list, you can either search for a server IP address by entering the name in the **Search** field or choose the accounting server IP address. **2.** Click **+** to add a server. **Note** You can configure a maximum of six accounting servers for an SSID of enterprise wireless network for the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches. **3.** From the **Additional Server** drop-down list, choose the server IP address. Cisco DNA Center allows you to override the set of AAA server configurations for the SSID at the site level. For each set of overridden AAA settings per SSID, Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Cisco DNA Center creates the new WLAN profiles equal to the number of floors. You must reprovision the device to override the AAA servers at the site level.
Mac Filtering	Check Box	Check this check box to enable MAC-based access control or security in the wireless network. **Note** When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.
AAA Override	Check Box	Check box to enable the AAA override functionality. By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.

Feature	Type	Description
Timeout Settings for Sleeping Clients	Select radio button	If you choose Web Authentication Internal, Web Authentication External, Web Passthrough Internal, or Web Passthrough External for Timeout Settings for sleeping clients, choose one of the following authentication options: Always authenticate: Enables authentication for sleeping clients. Authenticate after: Enter the duration for which sleeping clients are to be remembered before reauthentication becomes necessary. The valid range is from 10 minutes through 43,200 minutes, and the default duration is 720 minutes. **Note** Clients with guest access and web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered before reauthentication becomes necessary. The valid range is from 10 minutes through 43,200 minutes, and the default is 720 minutes. You can configure the duration on a WLAN and on a user group policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is less than the time configured on the sleeping timer of the WLAN, the lifetime of the client is used as the sleeping time.
Deny RCM Clients	Check Box	Check this check box to deny clients with randomized MAC addresses.
Pre-Auth ACL List Name	Drop Box	Choose the ACL list name that you already created to map with the SSID.
Fastlane	Check Box	This box can only be checked when the **Type of Enterprise Network** has been chosen as Voice and Data. For Catalyst 9800 Series Wireless Controllers, the **Fastlane** check box enables Auto QoS in Fastlane mode. Auto QoS in Fastlane mode configures the Fastlane EDCA profile for both the 5 GHz and 2.4 GHz bands. However, no precious metals QoS SSID policy is applied to the WLAN/SSID when the **Fastlane** check box is selected. For Cisco AireOS Wireless Controllers, this setting enables the Fastlane macro for the WLAN/SSID. The Fastlane macro applies the Platinum QoS profile to the WLAN/SSID. Application Visibility is enabled on the WLAN/SSID with the AVC profile named AUTOQOS-AVC-PROFILE. The QoS Map is modified to trust DSCP in the upstream direction. In the downstream direction, Cisco best practices are implemented when mapping DSCP-to-UP values.
Advanced Settings – Session timeout	Check Box and Integer Field	Configures the maximum time for a client session to remain active before requiring reauthorization. The range is between 300 and 86,400 seconds (5 minutes and 24 hours). The default is enabled with a time of 1800 seconds (30 minutes).
Advanced Settings – Client Exclusion	Check Box and Integer Field	Configures the amount of time a wireless client is excluded from attempting to authenticate after maximum authentication failures has been exceeded. The default is enabled with a time of 180 seconds (3 minutes).

Feature	Type	Description
Advanced Settings – MFP CLIENT PROTECTION	Radio Button	Additional security setting that controls the use of 802.11w Protected Management Frames for the WLAN. The following options are available: • Optional: This setting allows wireless stations to use the 802.11w Protected Management Frames that they support and allows other wireless stations that do not support PMFs to coexist on the WLAN. This is the default setting. • Required: The wireless client is required to use Protected Management Frames on the WLAN. • Disabled: Protected Management Frames are disabled on the WLAN.
Advanced Settings – 11k Neighbor List	Check Box	Controls the use of 802.11k Assisted Roaming neighbor lists for the WLAN, which can limit the need for passive and active scanning by the wireless client. The default setting is enabled for the band (5 GHz or 2.4 GHz) with which the client is associated.
Advanced Settings – 11v BSS TRANSITION SUPPORT	Multiple Check Boxes and Integer Field	Additional settings for support of 802.11v Wireless Network Management (WNM) for the WLAN. The following settings are available: • BSS Max Idle Service: Check box that enables the maximum idle service for the WLAN. Allows APs to send the timeout value to the wireless client within association and reassociation response frames. The default setting is enabled. • Client User Idle Timeout: Check box with bounded integer field that specifies the maximum amount of time an AP keeps a wireless client associated without receiving any frames from the client for the WLAN. This allows the client to sleep longer and conserve battery usage for mobile devices. The default setting is enabled with a time of 300 seconds. • Directed Multicast Service: Check box that allows the client to request that multicast streams be sent as unicast streams to the client from the AP. By default, this setting is enabled.

Feature	Type	Description
NAS-ID	Drop-down List	From the **NAS-ID Opt** drop-down list, choose the required type of network access server identifier (NAS ID). To specify a custom script for the NAS ID, choose Custom Option from the NAS-ID Opt drop-down list and enter the custom script in the corresponding Custom Script for Opt field. You can enter up to 31 alphanumeric characters, special characters, and spaces for the custom script. Cisco DNA Center does not support the special characters ?, ", < , and trailing spaces for the custom script. **Note** Cisco DNA Center supports NAS ID with custom script only for Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.7 or later. (Optional) Click **+** to add another NAS ID. You can add up to three NAS IDs. Cisco DNA Center applies only one NAS ID for Cisco AireOS Wireless Controllers. You can overwrite the NAS ID at the site level from **Design** > **Network Settings** > **Wireless**.
Advanced Settings – Coverage Hole Detection	Toggle button	Coverage Hole Detection toggle button to enable or disable the coverage hole detection functionality.
Advanced Settings – Client Rate Limit	Integer Field	To configure the Client Rate Limit, enter a value for the client rate limit in bits per second. The valid range is from 8000 through 100,000,000,000. The value must be a multiple of 500. **Note** This configuration is not applicable for Cisco AireOS Wireless Controllers. To configure client rate limit for Cisco AireOS Wireless Controllers, click the menu icon and choose **Tools** > **Model Config Editor** > **Wireless** > **Advanced SSID Configuration**. For more information, see Create a Model Config Design for Advanced SSID. The following are the valid ranges for a client rate limit on Cisco IOS XE devices: • The valid range for the Cisco Catalyst 9800-L Wireless Controller, the Cisco Catalyst 9800-40 Wireless Controller, and the Cisco Catalyst 9800-80 Wireless Controller is from 8000 through 67,000,000,000 bits per second. • The valid range for the Cisco Catalyst 9800-CL Wireless Controller is from 8000 through 10,000,000,000 bits per second. • The valid range for the Cisco Embedded Wireless Controller on Catalyst Access Points is from 8000 through 2,000,000,000 bits per second. • The valid range for the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches is from 8000 through 100,000,000,000 bits per second.

Feature	Type	Description
Advanced Settings – Radius Client Profiling	Toggle button	For Radius Client Profiling, use this toggle button to enable or disable RADIUS profiling on a WLAN. **Note** At least one AAA or PSN server is required to enable this feature.
Advanced Settings – CCKM	Toggle button	Configure CCKM: Use this toggle button to enable CCKM as the authentication key management option in Cisco DNA Center. Timestamp Tolerance: This field is visible only if you enable CCKM. Enter the CCKM tolerance level. The CCKM tolerance level is not applicable for the Cisco AireOS Wireless Controller platform. **Note** You can configure CCKM only if SSID has Layer 2 security as Enterprise in WPA2 or WPA2+WPA3.
Advanced Settings – Protected Management Frame (802.11w)	Radio Button	The options available under Protected Management Frame (802.11w) vary based on the settings that you chose under Level of Security. The following options may be available: • Optional • Required • Disabled

Guest Wireless Network Settings Configured in the Deployment Guide

Table 15: Guest Wireless Network Settings Configured in the Deployment Guide

Feature	Settings
Wireless Network Name (SSID)	lab3guest5
Broadcast SSID	On
Admin Status	On
Wireless Option	Multi band operation (2.4 GHz, 5 GHz, 6 GHz)
Primary Traffic Type	Best Effort (Silver)
LEVEL OF SECURITY	Web Auth
AUTHENTICATION SERVER	ISE Authentication
AUTHENTICATION SERVER > ISE Authentication > What kind of portal are you creating today?	Self Registered
AUTHENTICATION SERVER > ISE Authentication > Where will your guests redirect after successful authentication?	Original URL
Configure AAA	AAA configured

Feature	**Settings**
AAA Override	Enabled
Mac Filtering	Checked
Fastlane	Unchecked
Deny RCM Clients	Unchecked
Pre Auth ACL	Select configured Pre auth ACL
Advanced Settings – FAST TRANSITION (802.11r)	Disabled
Advanced Settings – MFP CLIENT PROTECTION	Optional
Advanced Settings –Protected Management Frame	Disabled
Advanced Settings – Session timeout	Checked, 1800 seconds
Advanced Settings – Client Exclusion	Checked, 180 seconds
Advanced Settings – MFP CLIENT PROTECTION	Optional
Advanced Settings – 11k Neighbor List	Checked
Advanced Settings – Radius Client Profiling	Unchecked
Advanced Settings – Configure Client Rate Limit	Blank
Advanced Settings – Coverage Hole Detection	Checked
Configure CCKM	Unchecked
NAS-ID	Blank
Advanced Settings – 11v BSS TRANSITION SUPPORT	BSS Max Idle Service – Checked Client Idle User Timeout – Checked, 300 seconds Directed Multicast Service - Checked

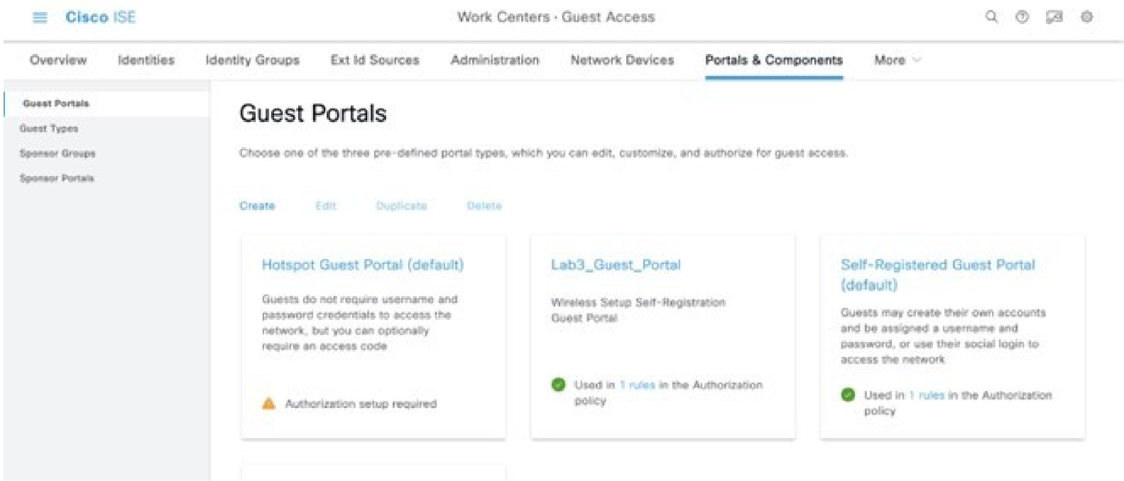
Provision Cisco ISE Settings from Cisco DNA Center

When a guest SSID profile is assigned to a site, Cisco DNA Center will push the required authentication, authorization, and guest portal configurations to Cisco ISE according to the settings in the guest SSID profile.

Procedure

Step 1 Choose **Lab3_Guest_Portal** to verify the portal details.

Figure 28: Guest Portal in Cisco ISE



Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Hotspot Guest Portal (default)

Guests do not require username and password credentials to access the network, but you can optionally require an access code

Authorization setup required

Lab3_Guest_Portal

Wireless Setup Self-Registration Guest Portal

Used in 1 rules in the Authorization policy

Self-Registered Guest Portal (default)

Guests may create their own accounts and be assigned a username and password, or use their social login to access the network

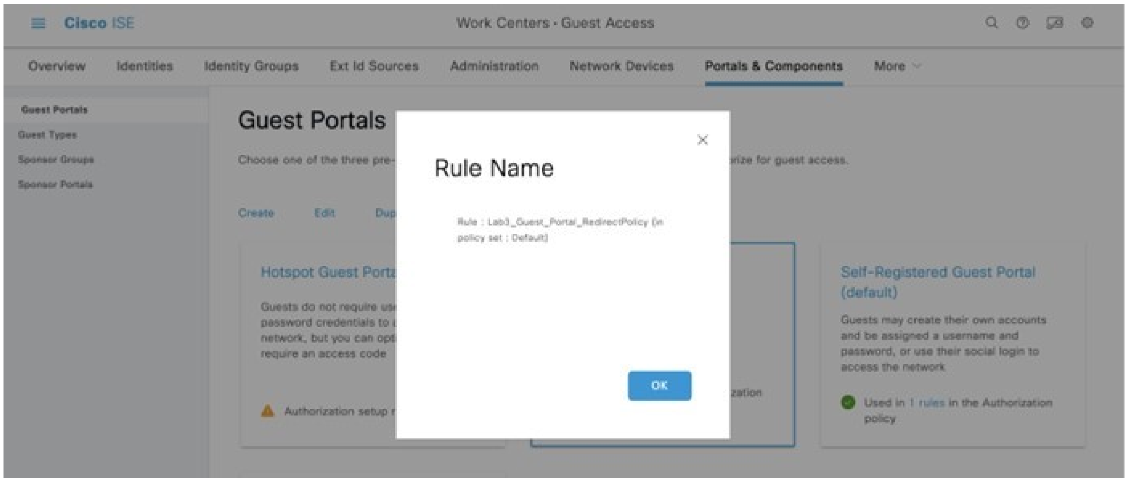
Used in 1 rules in the Authorization policy

ISE will display a new guest portal named **Lab3_Guest_Portal**.

.

Step 2 Click the **1 rules** link to check the authorization policy created by Cisco DNA Center.

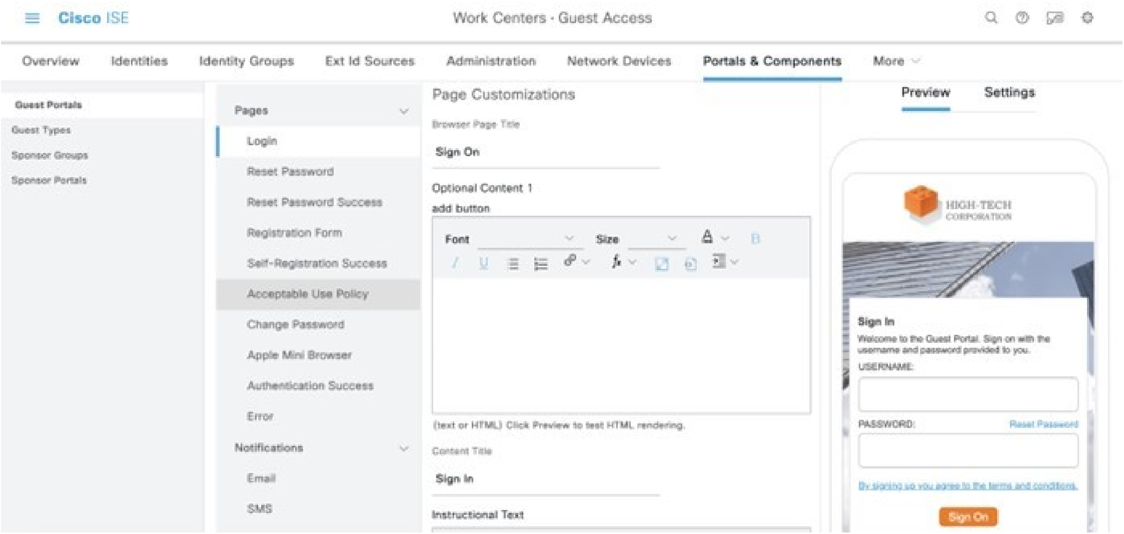
Figure 29: Guest Portal Redirect Policy



Rule Name

Rule : Lab3_Guest_Portal_RedirectPolicy (in policy set : Default)

Figure 30: Guest Portal Preview



Page Customizations

Browser Page Title: Sign On

Optional Content 1

add button

(text or HTML) Click Preview to test HTML rendering.

Content Title: Sign In

Instructional Text

Sign In

Welcome to the Guest Portal. Sign on with the username and password provided to you.

USERNAME:

PASSWORD: Reset Password

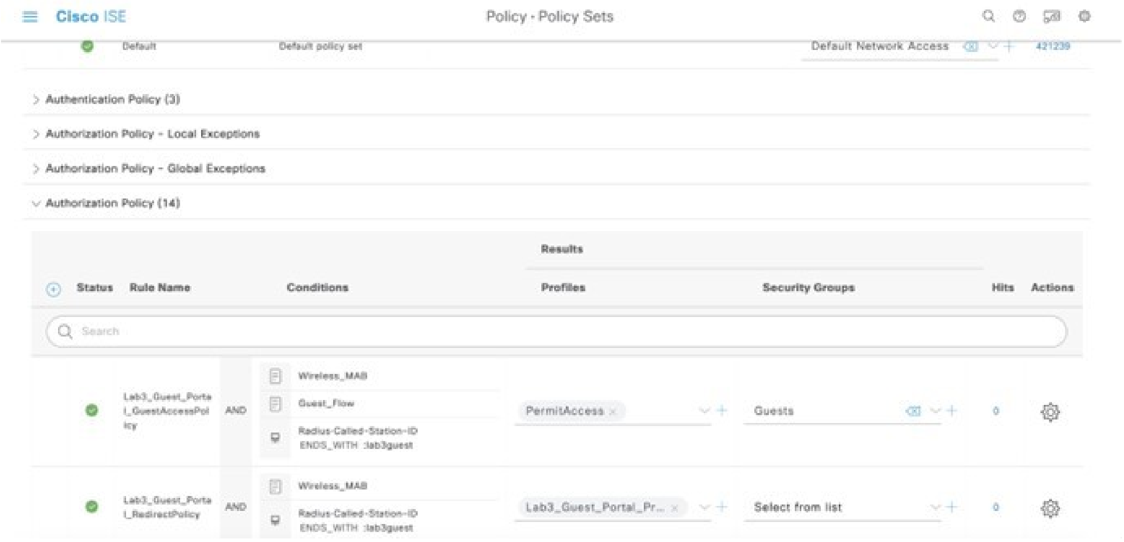
By signing up you agree to the terms and conditions.

Step 3 From the top-left corner, click the menu icon and choose **Policy** > **Policy sets**.

Step 4 Click **Default**.

Step 5 Go to **Authorization Policy** to verify the authorization policy pushed by Cisco DNA Center.

Figure 31: Guest SSID Authorization Policy



Default | Default policy set | Default Network Access | 421239

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (14)

				Results			
Status	Rule Name		Conditions	Profiles	Security Groups	Hits	Actions
●	Lab3_Guest_Portal_GuestAccessPolicy	AND	Wireless_MAB Guest_Flow Radius-Called-Station-ID ENDS_WITH :lab3guest	PermitAccess	Guests	0	⚙
●	Lab3_Guest_Portal_RedirectPolicy	AND	Wireless_MAB Radius-Called-Station-ID ENDS_WITH :lab3guest	Lab3_Guest_Portal_Pr...	Select from list	0	⚙

Remote Office Wireless Deployment Settings

This section provides an overview of a remote office wireless network using APs in FlexConnect mode, which will be provisioned using Cisco DNA Center.

The site hierarchy consists of the following:

- A branch area (**New York**) with a building (**Branch 5**) and multiple floors (**Floor 1**, **Floor2**, and **Floor 3**).
- An SSID for employee traffic (**lab3branch5**) and an SSID for guest traffic (l**ab3guest5**), both advertised by the APs within the branch.
- A non-Cisco SDA (legacy) remote office wireless deployment, in which all employee branch wireless traffic is centrally switched.

The guest wireless traffic within the branch is locally switched. Cisco Wireless Controllers will be in N+1 HA mode and must be assigned to sites during the Cisco DNA Center provisioning process.

Note For this deployment guide, both Catalyst 9800-40 wireless controllers (C9800-Flex-CVD and C9800-CVD-Nplus1) will be assigned to building **Branch 5** within the **New York** area.

Within Cisco DNA Center, sites (areas, buildings, or floors) containing APs are assigned as either primary managed AP locations or secondary managed AP locations. There can be only one primary enterprise wireless controller assigned to a site at a given time, meaning that a site can only be assigned as a primary managed AP location for one enterprise wireless controller at a time. For this deployment guide, APs on **Floor 1** within **Branch 5**, will be provisioned to C9800-Flex-CVD through Cisco DNA Center.

Cisco DNA Center supports the configuration of AP high availability, in which the AP tries to associate with primary and secondary wireless controllers and form a CAPWAP control connection. If the primary wireless controller is unavailable, the AP will attempt to establish a CAPWAP control connection to the secondary wireless controller. In Cisco DNA Center, this is accomplished by configuring sites containing APs as secondary managed AP locations.

Note For this design and deployment guide, wireless controller C9800-Flex-CVD will be provisioned so that **Floor 1** of **Branch 5** is a primary managed AP location. For the APs within **Branch 5**, wireless controller C9800-CVD-Nplus1 will serve as the secondary wireless controller in an N+1 wireless controller redundancy configuration.

Recommendations

When configuring the remote office wireless deployment settings, consider the following recommendations:

- Use PortFast on AP switch ports for APs in FlexConnect mode, supporting only the central switched WLANs. To configure the switch port for PortFast, set the port to be connected as a host port, using the switch port host command or the PortFast command. This configuration allows for a faster AP join process. There is no risk of loops, as the local mode APs never directly bridge traffic between VLANs. You can set the port directly on access mode.
- For APs in FlexConnect mode, when using locally switched WLANs mapped to different VLANs (the AP switch port is in trunk mode), prune or limit the VLANs present on the port to match the AP-configured VLANs.

Configure Wireless Interface

In Cisco DNA Center, the enterprise and guest WLANs terminate on the wireless interfaces known as Ethernet VLAN interfaces. The following table shows the wireless interfaces created for this design and deployment guide for the enterprise and guest WLANs.

Table 16: Wireless Interfaces

Name	VLAN	Usage
branchemployee	100	VLAN for centrally switched employee traffic.

Name	VLAN	Usage
branchguest-dmz	110	VLAN for guest traffic locally switched on a VLAN on switch.

Note The native VLAN (AP VLAN) configuration is specific to FlexConnect AP deployments. The FlexConnect locally switched traffic terminates on a specific VLAN, which is configured in the wireless profile for this design and deployment guide. Therefore, the field will be left blank.

The following steps explain how to configure wireless interfaces within Cisco DNA Center.

Before you begin

To complete this action, you must have SUPER-ADMIN-ROLE or the NETWORK-ADMIN-ROLE privileges.

Procedure

Step 1 Login to Cisco DNA Center web console using the IP address or fully qualified domain name of your instance.

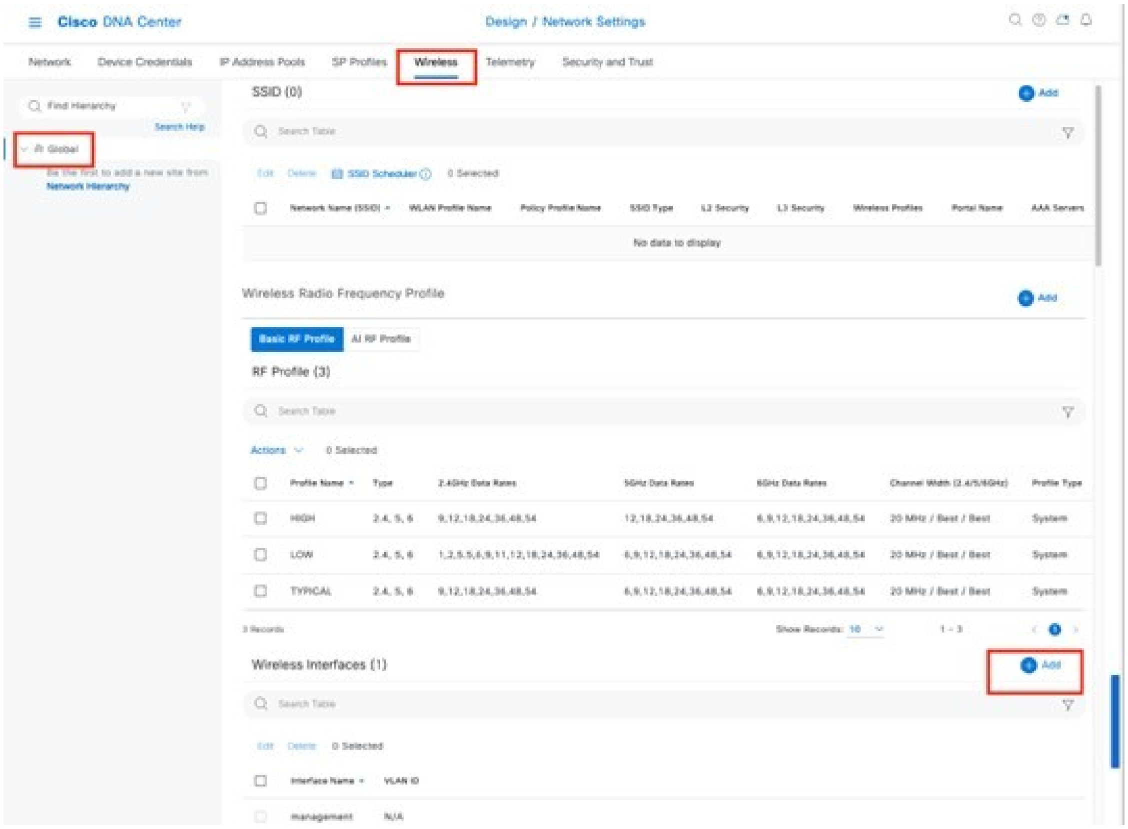
Example:

https://<Cisco_DNA_Center_IPaddr_or_FQDN>

Step 2 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

The **Wireless Network Settings** dashboard is displayed. An example is shown in the following figure.

Figure 32: Adding Wireless Interface



SSID (0)

0 Selected

Network Name (SSID)	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers

No data to display

Wireless Radio Frequency Profile

RF Profile (3)

0 Selected

Profile Name	Type	2.4GHz Data Rates	5GHz Data Rates	6GHz Data Rates	Channel Width (2.4/5/6GHz)	Profile Type
HIGH	2.4, 5, 6	9,12,18,24,36,48,54	12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System
LOW	2.4, 5, 6	1,2,5.5,6,9,11,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System
TYPICAL	2.4, 5, 6	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System

3 Records

Wireless Interfaces (1)

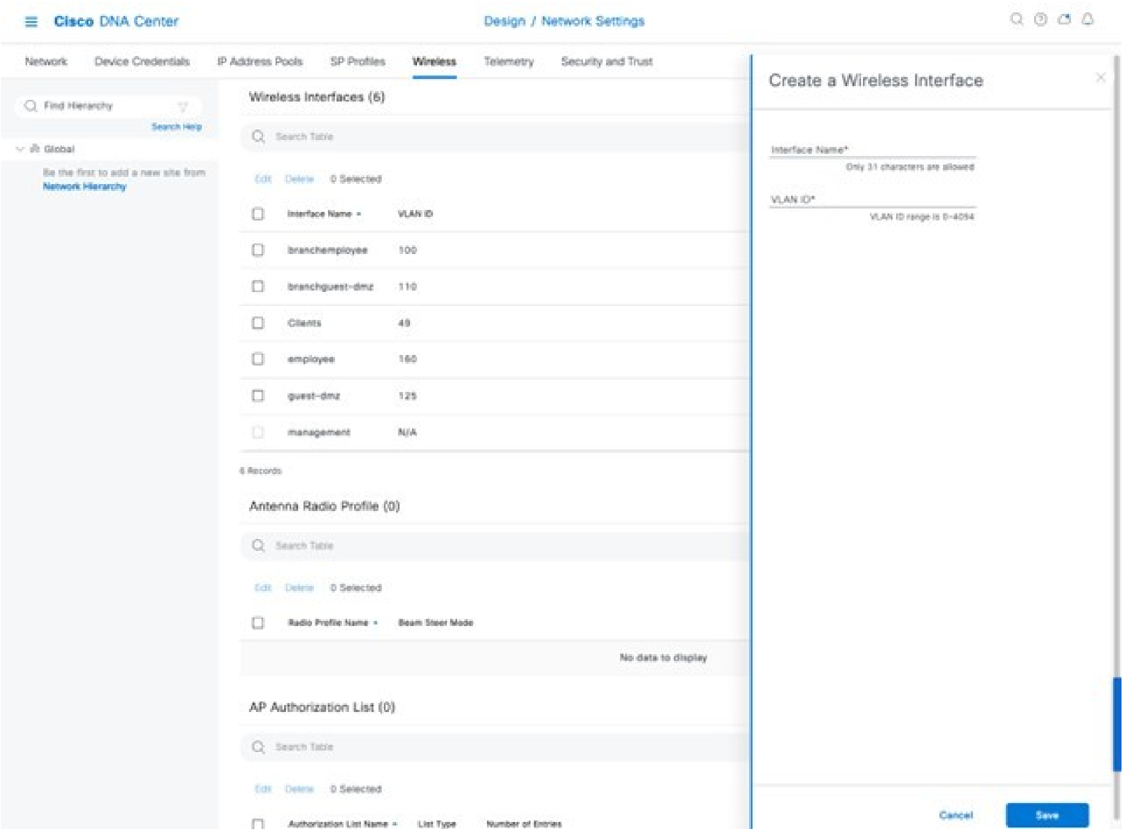
0 Selected

Interface Name	VLAN ID
management	N/A

Step 3 Enter the **Interface Name** and **VLAN ID** for the wireless interface corresponding to the enterprise VLAN (**branchemployee**).

Step 4 Click **Add**.

Figure 33: Interface and VLAN Under Wireless Interfaces



Wireless Interfaces (6)

Interface Name	VLAN ID
branchemployee	100
branchguest-dmz	110
Clients	49
employee	160
guest-dmz	125
management	N/A

Antenna Radio Profile (0)

Radio Profile Name	Beam Steer Mode

AP Authorization List (0)

Authorization List Name	List Type	Number of Entries

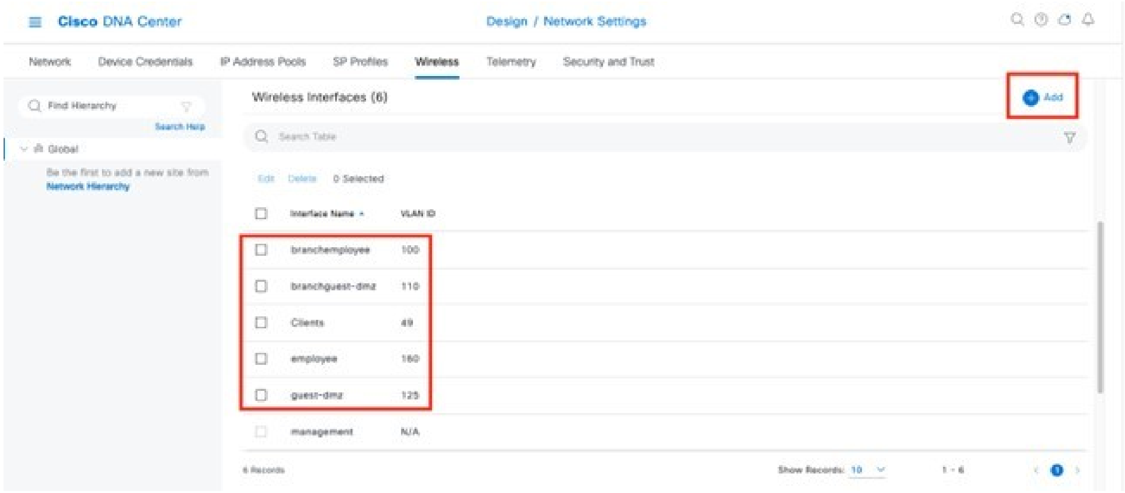
Create a Wireless Interface

Interface Name*
Only 31 characters are allowed

VLAN ID*
VLAN ID range is 0-4094

Repeat the procedure to add the wireless interface for the guest VLAN (**guest-dmz**). When completed, the two new wireless interfaces should appear in the **Wireless Network Settings** dashboard, as shown in the figure below:

Figure 34: Created Wireless Interfaces



Wireless Interfaces (6)

Interface Name	VLAN ID
branchemployee	100
branchguest-dmz	110
Clients	49
employee	160
guest-dmz	125
management	N/A

Configure Enterprise Wireless SSID

Enterprise wireless networks are the nonguest WLAN/SSIDs that are available for broadcast across the deployment. You must define them at the global level of the site hierarchy. Once defined, you can apply the enterprise wireless networks to wireless profiles and assign wireless profiles to one or more sites within the hierarchy.

For the design and deployment guide, a single enterprise WLAN SSID named **lab3branch5** is provisioned.

Procedure

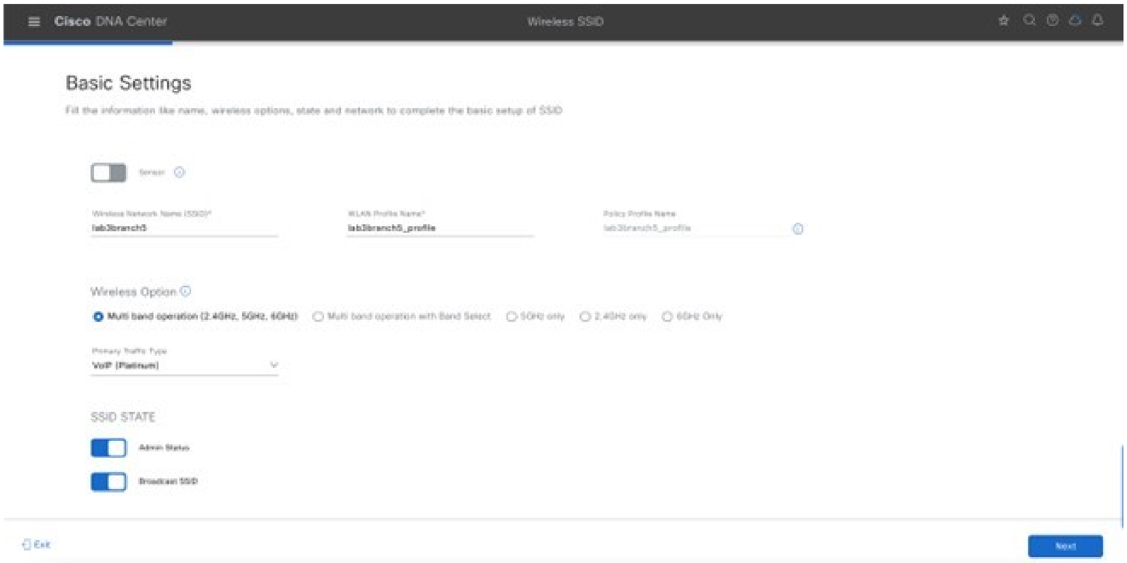
Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 2 Click **SSIDs**.

Step 3 Hover your cursor over **+ Add** and choose **Enterprise**.

The **Basic Settings** window is displayed.

Figure 35: Basic Settings Window to Create a New Enterprise SSID



Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID

Sensor

Wireless Network Name (SSID)*: lab3branch5

WLAN Profile Name*: lab3branch5_profile

Policy Profile Name: lab3branch5_profile

Wireless Option

● Multi band operation (2.4GHz, 5GHz, 6GHz) ○ Multi band operation with Band Select ○ 5GHz only ○ 2.4GHz only ○ 6GHz Only

Primary Traffic Type: VoIP (Platinum)

SSID STATE

Admin Status

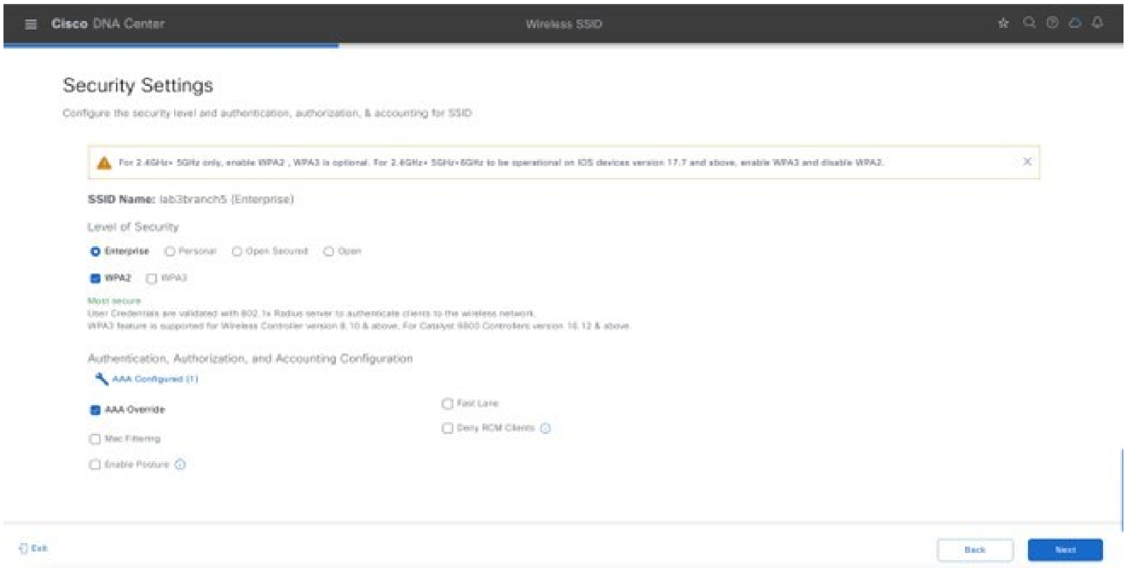
Broadcast SSID

For information about features that can be configured for enterprise wireless networks via Cisco DNA Center, see Enterprise Wireless Network Features Configurable via Cisco DNA Center, on page 39.

Step 4 Enter the information for the **Basic Settings** and click **Next**.

Note For information about the settings for the enterprise wireless network configured for this deployment guide, see Enterprise Wireless Network Settings Configured in the Deployment Guide, on page 49.

Figure 36: Security Setting for the Enterprise SSID



Security Settings

Configure the security level and authentication, authorization, & accounting for SSID

For 2.4GHz+ 5GHz only, enable WPA2 , WPA3 is optional. For 2.4GHz+ 5GHz+6GHz to be operational on IOS devices version 17.7 and above, enable WPA3 and disable WPA2.

SSID Name: lab3branch5 (Enterprise)

Level of Security

● Enterprise ○ Personal ○ Open Secured ○ Open

☑ WPA2 □ WPA3

Most secure
User Credentials are validated with 802.1x Radius server to authenticate clients to the wireless network.
WPA3 feature is supported for Wireless Controller version 8.10 & above. For Catalyst 9800 Controllers version 16.12 & above.

Authentication, Authorization, and Accounting Configuration

AAA Configured (1)

☑ AAA Override

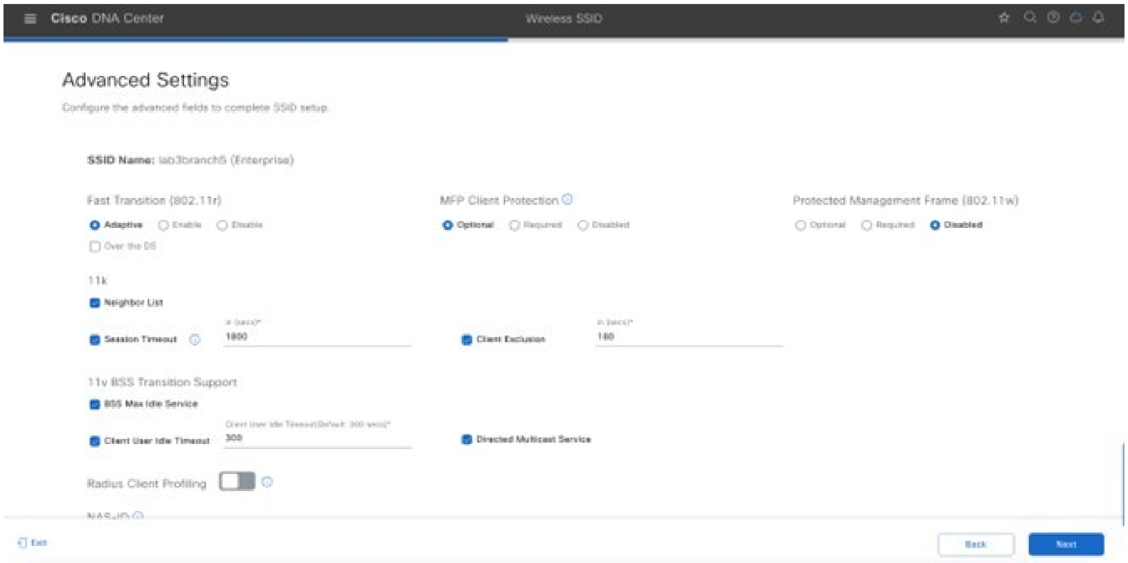
□ Mac Filtering

□ Enable Posture

□ Fast Lane

□ Deny RCM Clients

Figure 37: Advanced Settings for the Enterprise SSID



Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: lab3branch5 (Enterprise)

Fast Transition (802.11r)

● Adaptive ○ Enable ○ Disable

□ Over the DS

MFP Client Protection

● Optional ○ Required ○ Disabled

Protected Management Frame (802.11w)

○ Optional ○ Required ● Disabled

11k

☑ Neighbor List

☑ Session Timeout — in (secs)*: 1800

☑ Client Exclusion — in (secs)*: 180

11v BSS Transition Support

☑ BSS Max Idle Service

☑ Client User Idle Timeout — Client User Idle Timeout(Default: 300 secs)*: 300

☑ Directed Multicast Service

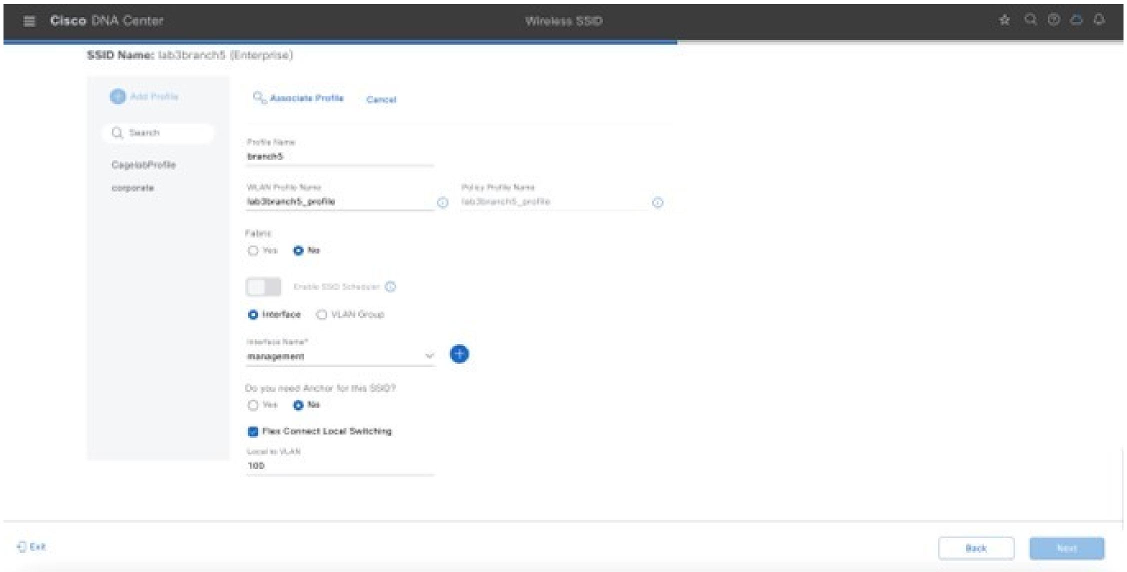
Radius Client Profiling

NAS-ID

Step 5 Click **+ Add** to add a new wireless profile.

Note You can either attach the enterprise wireless network to an existing wireless profile, or you can create a new wireless profile and attach the enterprise wireless network.

Figure 38: Attach Enterprise Wireless Network to Wireless Profile



SSID Name: lab3branch5 (Enterprise)

Profile Name: branch5

WLAN Profile Name: lab3branch5_profile

Policy Profile Name: lab3branch5_profile

Fabric: ○ Yes ● No

Enable SSID Scheduler

● Interface ○ VLAN Group

Interface Name*: management

Do you need Anchor for this SSID? ○ Yes ● No

☑ Flex Connect Local Switching

Local to VLAN: 100

Step 6 Enter the **Wireless Profile Name**.

For this deployment guide, create a wireless profile named **branch5**.

Step 7 (Skip this step if SD-Access App is not deployed.) Under **Fabric**, select **No**.

The **Select Interface** field is displayed. This deployment guide only discusses non-SDA wireless deployments using Cisco DNA Center.

Step 8 From the **Select Interface** drop-down menu, choose **branchemployee**.

Step 9 Check the box next to **FlexConnect Local Switching**.

Step 10 Enter VLAN ID 100 in **Local to VLAN**.

For terminating branch employee traffic, you have selected the **branchemployee** interface on the enterprise wireless controller, but all branch employee traffic will be locally switched onto VLAN 100 of the branch switch.

Step 11 Click **Next**.

The **Summary** page displays SSID basic settings, security, advanced settings, and network profiles.

Step 12 Click **Save**.

Note Even though Cisco DNA Center allows multiple network profiles to be associated with a single SSID, be sure to avoid associating a single SSID with network profiles that have both flex and nonflex profiles. Each of these profiles require the APs to be in different modes, flex and local respectively.

Step 13 Click **Configure Network Profiles**.

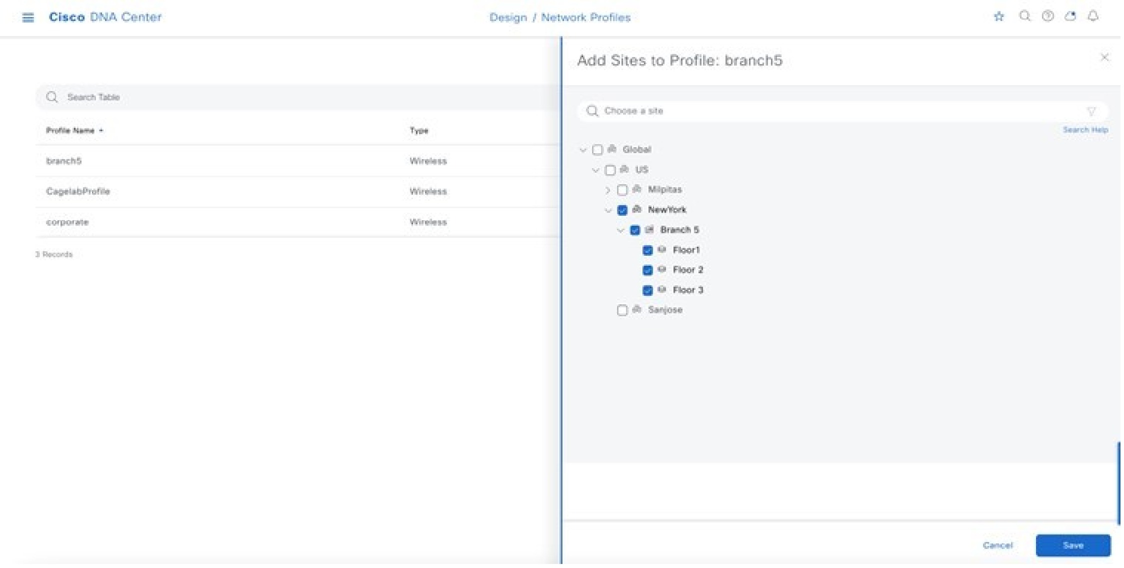
Step 14 Click **Assign Sites** in branch network profiles.

Step 15 Select the **New York** area.

All of the child site locations are automatically selected: **Building 23** with **Floor 1**, **Floor 2**, and **Floor 3** and **Building 24** with **Floor 1**, **Floor 2**, and **Floor 3**.

Step 16 Click **OK** to close the site hierarchy side panel and return to the **Create a Wireless Profile** side panel.

Figure 39: Assign Site in Branch Network Profile



Profile Name	Type
branch5	Wireless
CagelabProfile	Wireless
corporate	Wireless

3 Records

- □ Global
  - □ US
    - □ Milpitas
    - ☑ NewYork
      - ☑ Branch 5
        - ☑ Floor1
        - ☑ Floor 2
        - ☑ Floor 3
    - □ Sanjose

Step 17 Click **+ Add** under **Attach Template(s)** to add the CLI-based templates to the enterprise wireless network configuration.

Note You must have defined all the templates within the **Template Editor** dashboard of Cisco DNA Center. This design and deployment guide will not discuss the addition of templates because the guide does require knowledge of the CLI syntax for the specific Cisco Wireless Controller platform. However, you can add the wireless features that are not supported by the web-based GUI of Cisco DNA Center through templates.

The new enterprise wireless network, **lab3branch5**, appears in the **Wireless Network Settings** dashboard.

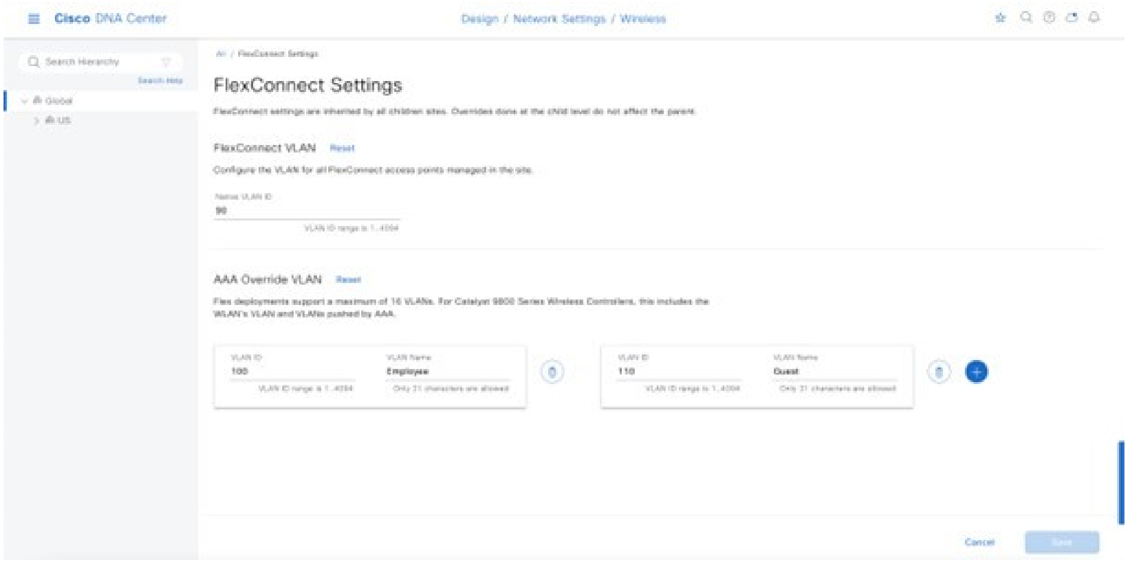
Configure FlexConnect Settings

The following procedure describes the steps to configure the FlexConnect settings using Cisco DNA Center, which is where the native VLAN and the client VLAN can be set.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless** > **FlexConnect Settings**.

Figure 40: FlexConnect Settings Page



FlexConnect Settings

FlexConnect settings are inherited by all children sites. Overrides done at the child level do not affect the parent.

FlexConnect VLAN

Configure the VLAN for all FlexConnect access points managed in the site.

Native VLAN ID: 90

VLAN ID range is 1..4094

AAA Override VLAN

Flex deployments support a maximum of 16 VLANs. For Catalyst 9800 Series Wireless Controllers, this includes the WLAN's VLAN and VLANs pushed by AAA.

VLAN ID: 100 (VLAN ID range is 1..4094) VLAN Name: Employee (Only 31 characters are allowed)

VLAN ID: 110 (VLAN ID range is 1..4094) VLAN Name: Guest (Only 31 characters are allowed)

Step 2 Configure **Native VLAN** and **AAA override VLAN** in the global settings.

Note In global settings, you can override native VLAN and AAA override VLAN at the area, building, and floor levels.

Configure FlexConnect in the Model Config Editor

Model configs are a set of model-based, discoverable, and customizable configuration capabilities, which you can deploy on your network devices with high-level service intent and device-specific CLI templates. The following procedure describes the steps to perform a model config for FlexConnect.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

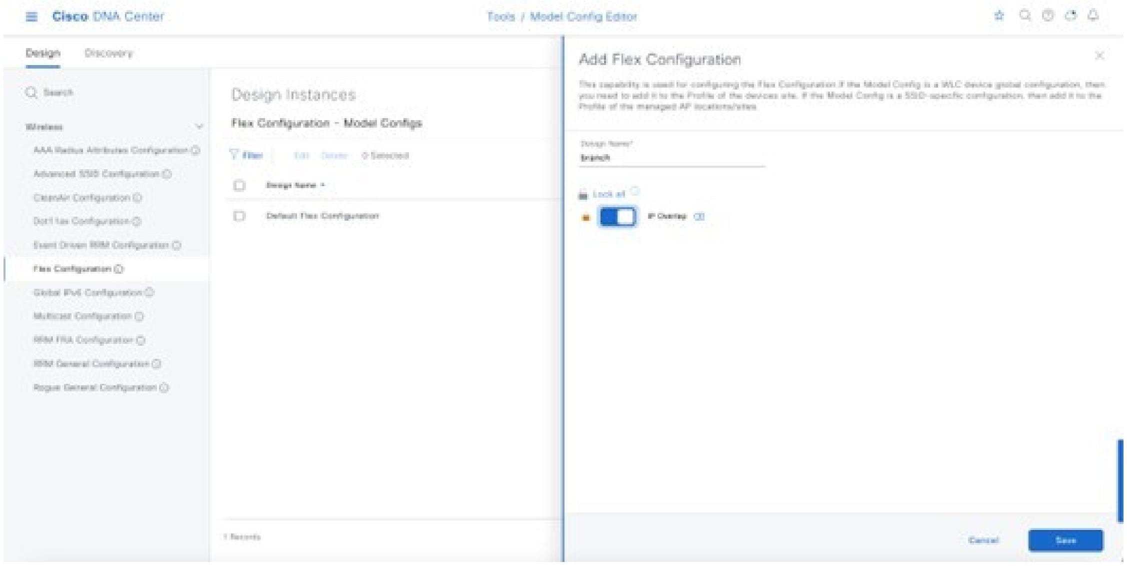
Step 2 Click **Flex Configuration**.

Step 3 Click **Add** and enter the design name.

For example, enter **branch** as the design name.

Step 4 Enable **IP Overlap**.

Figure 41: Model Config for Flex Configuration



Add Flex Configuration

This capability is used for configuring the Flex Configuration. If the Model Config is a WLC device global configuration, then you need to add it to the Profile of the devices site. If the Model Config is a SSID-specific configuration, then add it to the Profile of the managed AP locations/sites.

Design Name*: branch

IP Overlap: ●

Cisco DNA Center
Tools / Model Config Editor
Design
Discovery
Search
Wireless
AAA Radius Attributes Configuration
Advanced SSID Configuration
CleanAir Configuration
Dot11ax Configuration
Event Driven RRM Configuration
Flex Configuration
Global IPv6 Configuration
Multicast Configuration
RRM FRA Configuration
RRM General Configuration
Rogue General Configuration
Design Instances
Flex Configuration - Model Configs
Filter
Edit
Delete
0 Selected
Design Name
Default Flex Configuration
1 Records
Lock all
Cancel
Save

Map FlexConnect Model Config to Network Profiles

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Profiles**.

Step 2 Click **Edit branch5** network profile.

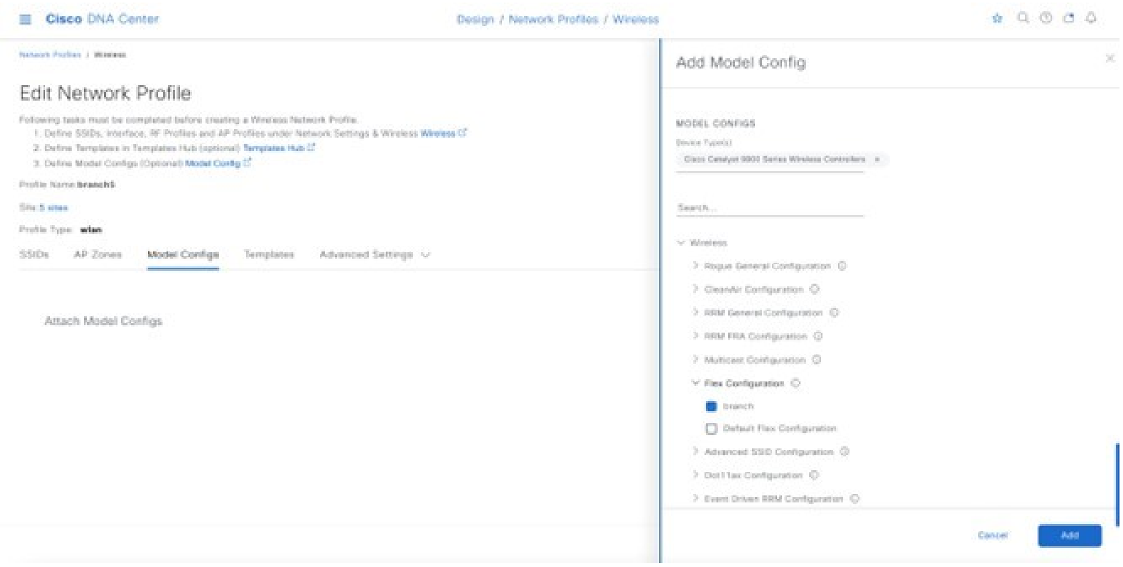
Step 3 Click the **Model Config** tab, and then click **Add Model Config**.

Step 4 Choose **Wireless Controller** as the Device Type.

Step 5 Click **Wireless** > **Flex Configuration**, and then select the configured model config.

Step 6 Click **Add** and save the changes.

Figure 42: Add Model Config to Flex Network Profile



Cisco DNA Center
Design / Network Profiles / Wireless
Network Profiles / Wireless

Edit Network Profile

Following tasks must be completed before creating a Wireless Network Profile.

1. Define SSIDs, Interface, RF Profiles and AP Profiles under Network Settings & Wireless Wireless
2. Define Templates in Templates Hub (optional) Templates Hub
3. Define Model Configs (Optional) Model Config

Profile Name: branch5

Site: 5 sites

Profile Type: wlan

Device Type(s): Cisco Catalyst 9800 Series Wireless Controllers

- ☑ branch
- □ Default Flex Configuration

Configure Guest Wireless SSID

Guest wireless networks must be defined at the global level of the site hierarchy. Once defined, guest wireless networks are applied to wireless profiles. Wireless profiles are then assigned to one or more sites within the hierarchy. For this deployment guide, a single guest wireless network (SSID) named **lab3guest5** is provisioned.

Procedure

Step 1

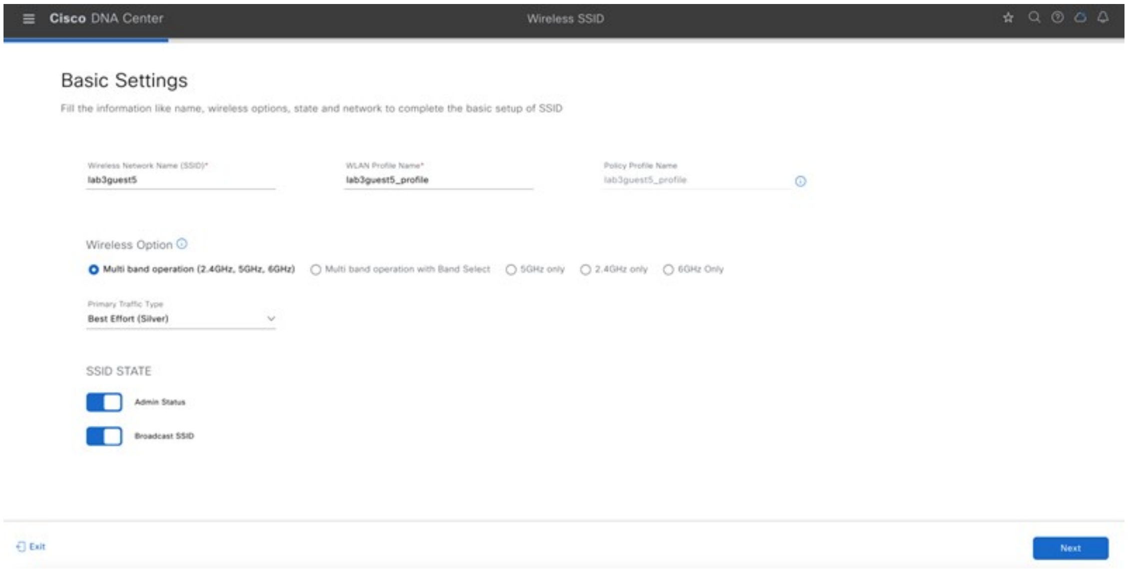
Step 2 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 3 Click **SSIDs**.

Step 4 Hover your cursor over **+ Add** and choose **Guest**.

The **Basic Settings** window is displayed.

Figure 43: Basic Settings Window to Create a Guest Wireless SSID



Basic Settings

Fill the information like name, wireless options, state and network to complete the basic setup of SSID

Wireless Network Name (SSID)*: lab3guest5

WLAN Profile Name*: lab3guest5_profile

Policy Profile Name: lab3guest5_profile

Wireless Option

● Multi band operation (2.4GHz, 5GHz, 6GHz) ○ Multi band operation with Band Select ○ 5GHz only ○ 2.4GHz only ○ 6GHz Only

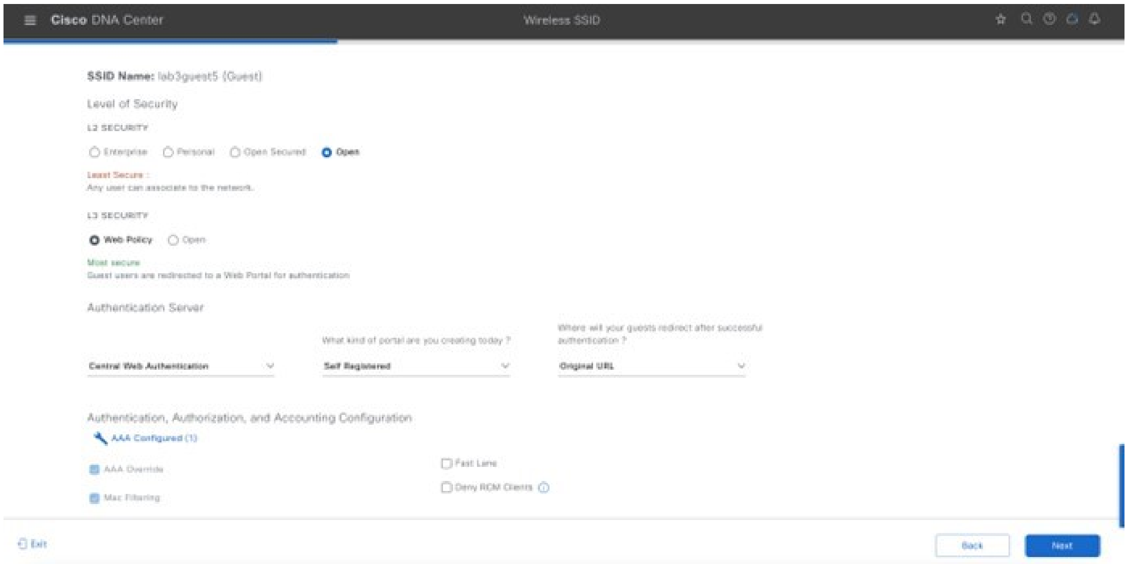
Primary Traffic Type
Best Effort (Silver)

SSID STATE

Admin Status

Broadcast SSID

Figure 44: Security Settings for Guest SSID



SSID Name: lab3guest5 (Guest)

Level of Security

L2 SECURITY

○ Enterprise ○ Personal ○ Open Secured ● Open

Least Secure :
Any user can associate to the network.

L3 SECURITY

● Web Policy ○ Open

Most secure
Guest users are redirected to a Web Portal for authentication

Authentication Server: Central Web Authentication

What kind of portal are you creating today ?: Self Registered

Where will your guests redirect after successful authentication ?: Original URL

Authentication, Authorization, and Accounting Configuration

AAA Configured (1)

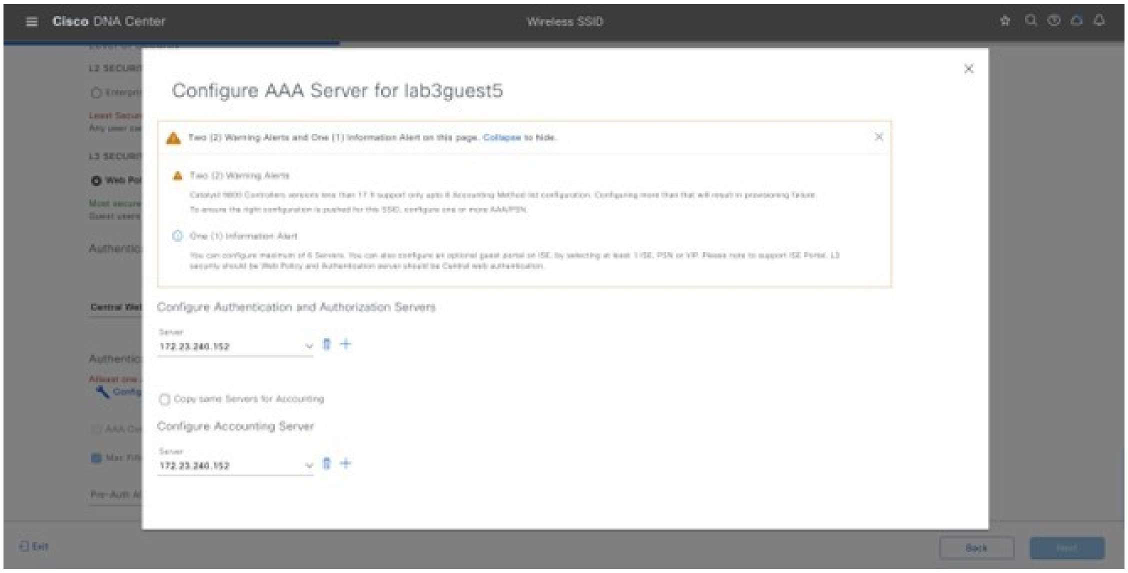
☑ AAA Override

☑ Mac Filtering

□ Fast Lane

□ Deny RCM Clients

Figure 45: AAA Settings for Flex Guest SSID



Configure AAA Server for lab3guest5

Two (2) Warning Alerts and One (1) Information Alert on this page. Collapse to hide.

Two (2) Warning Alerts

Catalyst 9800 Controllers versions less than 17.9 support only upto 8 Accounting Method list configuration. Configuring more than that will result in provisioning failure.

To ensure the right configuration is pushed for this SSID, configure one or more AAA/PSN.

One (1) Information Alert

You can configure maximum of 6 Servers. You can also configure an optional guest portal on ISE, by selecting at least 1 ISE, PSN or VIP. Please note to support ISE Portal, L3 security should be Web Policy and Authentication server should be Central web authentication.

Configure Authentication and Authorization Servers

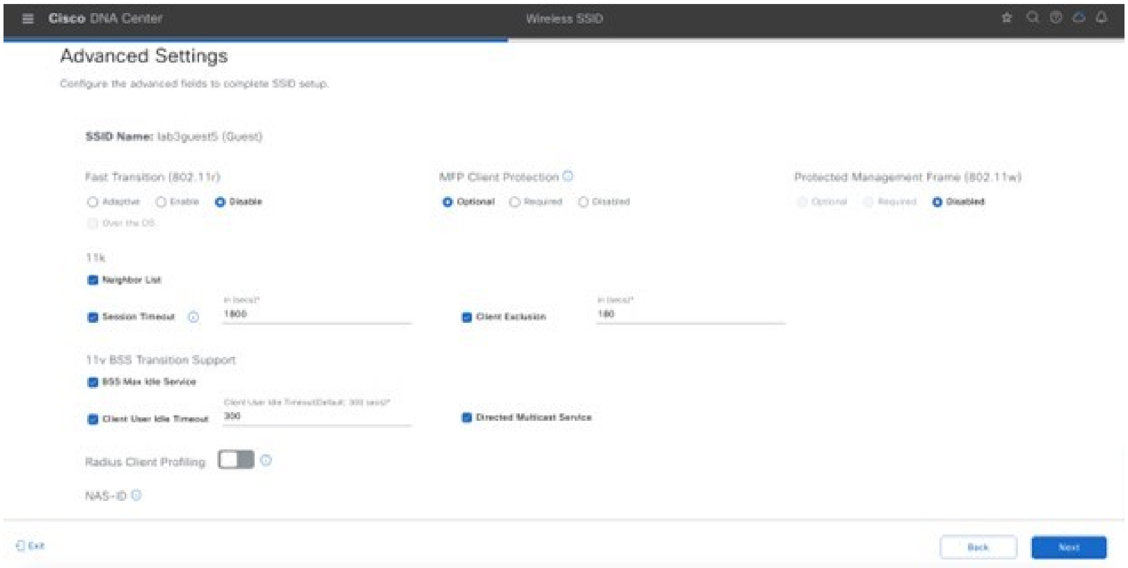
Server: 172.23.240.152

□ Copy same Servers for Accounting

Configure Accounting Server

Server: 172.23.240.152

Figure 46: Advanced Settings for Flex Guest SSID



Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: lab3guest5 (Guest)

Fast Transition (802.11r): ○ Adaptive ○ Enable ● Disable
□ Over the DS

MFP Client Protection: ● Optional ○ Required ○ Disabled

Protected Management Frame (802.11w): ○ Optional ○ Required ● Disabled

11k

☑ Neighbor List

☑ Session Timeout — in (secs)*: 1800

☑ Client Exclusion — in (secs)*: 180

11v BSS Transition Support

☑ BSS Max Idle Service

☑ Client User Idle Timeout — Client User Idle Timeout(Default: 300 secs)*: 300

☑ Directed Multicast Service

Radius Client Profiling: off

NAS-ID

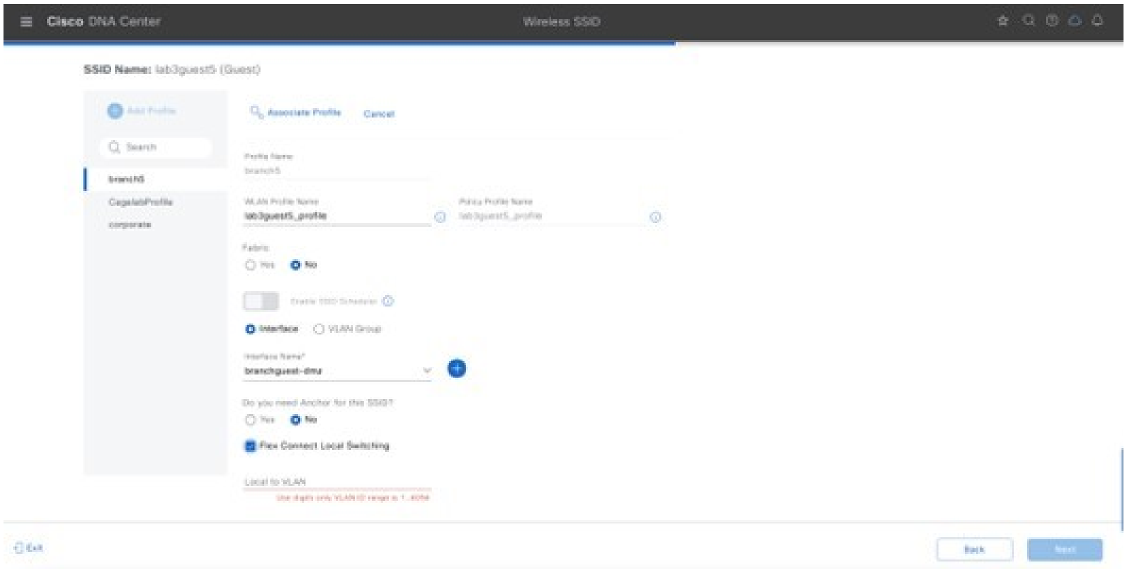
For information about features that can be configured for guest wireless networks via Cisco DNA Center, see Guest Wireless Network Features Configurable via Cisco DNA Center, on page 57.

Step 5 Enter the information for the relevant fields and click **Next**.

Note For information about the settings for the enterprise wireless network configured for this deployment guide, see Guest Wireless Network Settings Configured in the Deployment Guide, on page 68.

Step 6 Attach the guest wireless network to the existing **branch5** wireless profile.

Figure 47: Attach Wireless Profile to Flex Guest SSID



SSID Name: lab3guest5 (Guest)

Profile Name: branch5

WLAN Profile Name: lab3guest5_profile

Policy Profile Name: lab3guest5_profile

Fabric: ○ Yes ● No

Enable SSID Scheduler

● Interface ○ VLAN Group

Interface Name*: branchguest-dmz

Do you need Anchor for this SSID? ○ Yes ● No

☑ Flex Connect Local Switching

Local to VLAN

Use digits only. VLAN ID range is 1 - 4094

Step 7 From the **Select Interface** drop-down menu, choose **branchguest-dmz**.

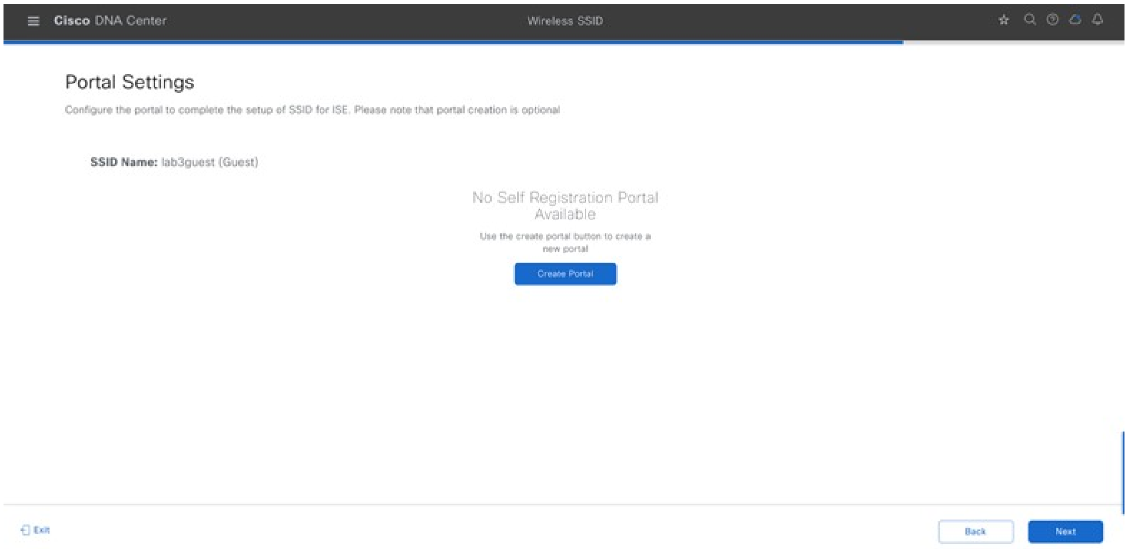
The guest traffic on the **branchguest-dmz** VLAN (VLAN 110) will be terminated.

Step 8 Click **FlexConnect Local switching** and enter **Local Vlan 110**.

Step 9 Click **Next**.

The **Portal Customization** page is displayed.

Figure 48: Guest Portal Customization for Flex Guest Wireless SSID



Portal Settings

Configure the portal to complete the setup of SSID for ISE. Please note that portal creation is optional

SSID Name: lab3guest (Guest)

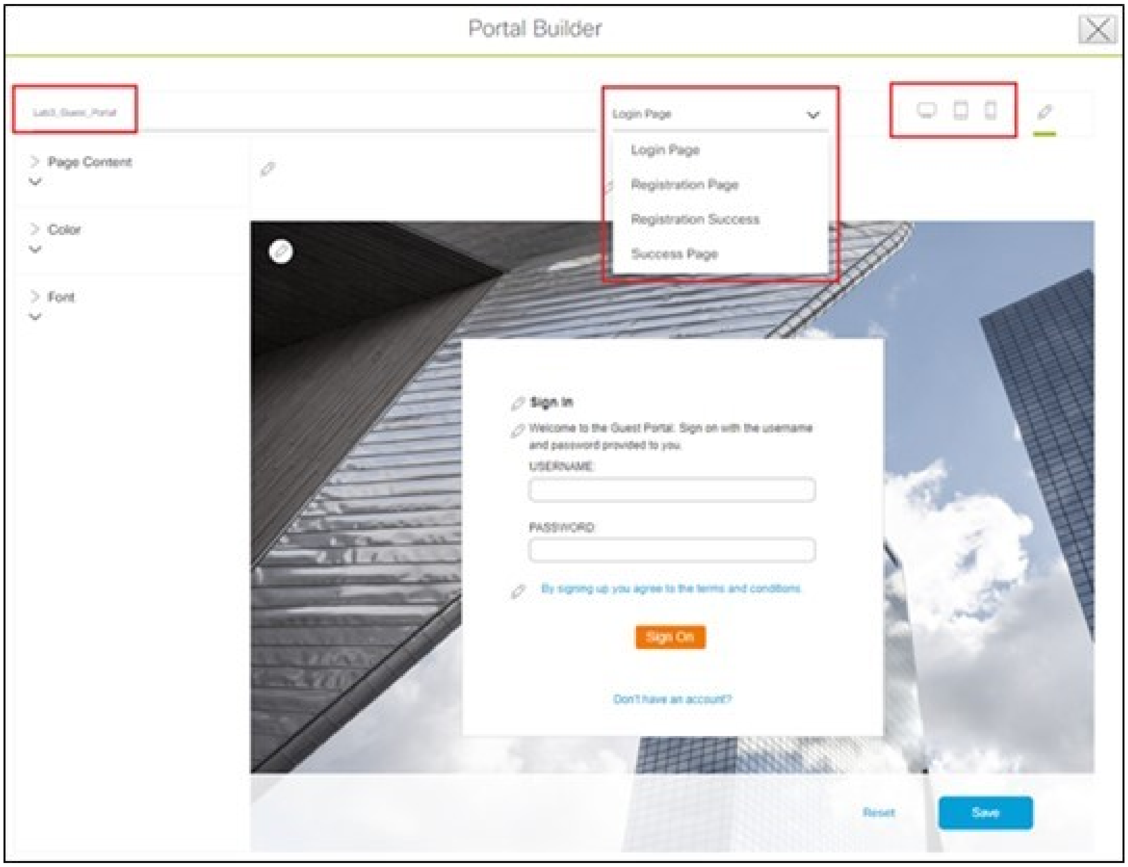
No Self Registration Portal Available

Use the create portal button to create a new portal

Step 10 Click **Create Portal** to add a new guest portal in Cisco ISE.

The **Portal Builder** page is displayed. You have the option to leave without portal creation.

Figure 49: Flex Guest SSID Portal Builder Screen



Lab3_Guest_Portal

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Step 11 Enter the relevant information.

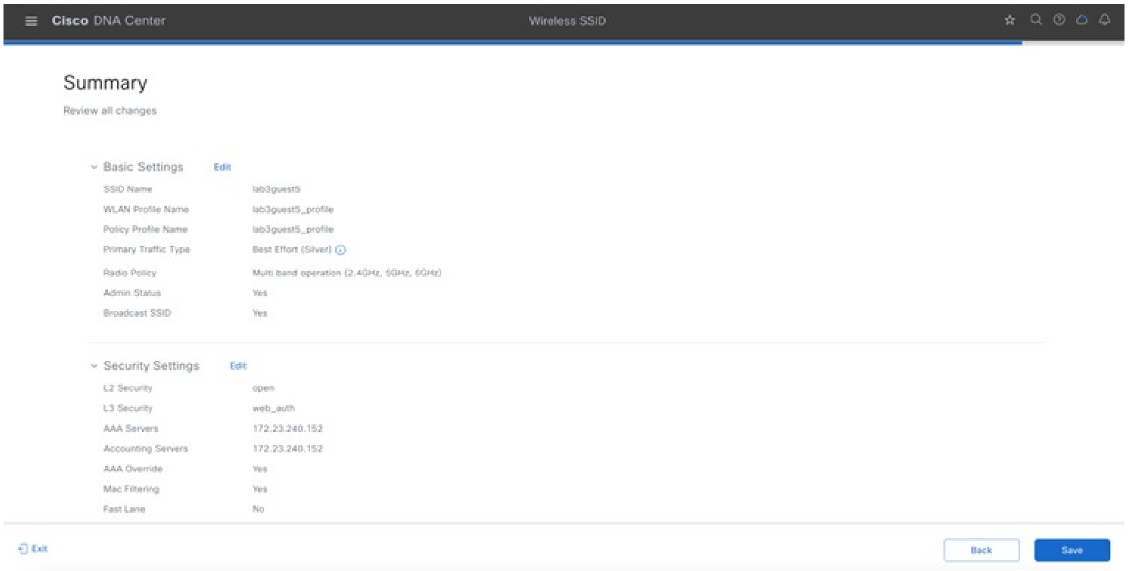
You must at least name the guest portal. For this deployment guide, the portal has been named **Lab3_Guest_Portal**. The drop-down menu in the **Portal Builder** allows you to customize the Login Page, Registration Page, Registration Success, and Success Page of the portal. You can customize the color scheme, fonts, page content, logo, and background for the web portal. You can also preview the portal to see what it will look like on a smart phone, tablet, and computer.

Step 12 Click **Save** to create the new guest portal on the Cisco ISE server and return to the guest wireless network workflow.

Step 13 Click **Next**.

The summary page will show SSID basic settings, security, advanced settings, and network profiles.

Figure 50: Flex Guest SSID Summary Page



Summary

Review all changes

Basic Settings Edit

SSID Name	lab3guest5
WLAN Profile Name	lab3guest5_profile
Policy Profile Name	lab3guest5_profile
Primary Traffic Type	Best Effort (Silver)
Radio Policy	Multi band operation (2.4GHz, 5GHz, 6GHz)
Admin Status	Yes
Broadcast SSID	Yes

Security Settings Edit

L2 Security	open
L3 Security	web_auth
AAA Servers	172.23.240.152
Accounting Servers	172.23.240.152
AAA Override	Yes
Mac Filtering	Yes
Fast Lane	No

Step 14 Click **Save**.

Step 15 Click **Configure Network Profiles**.

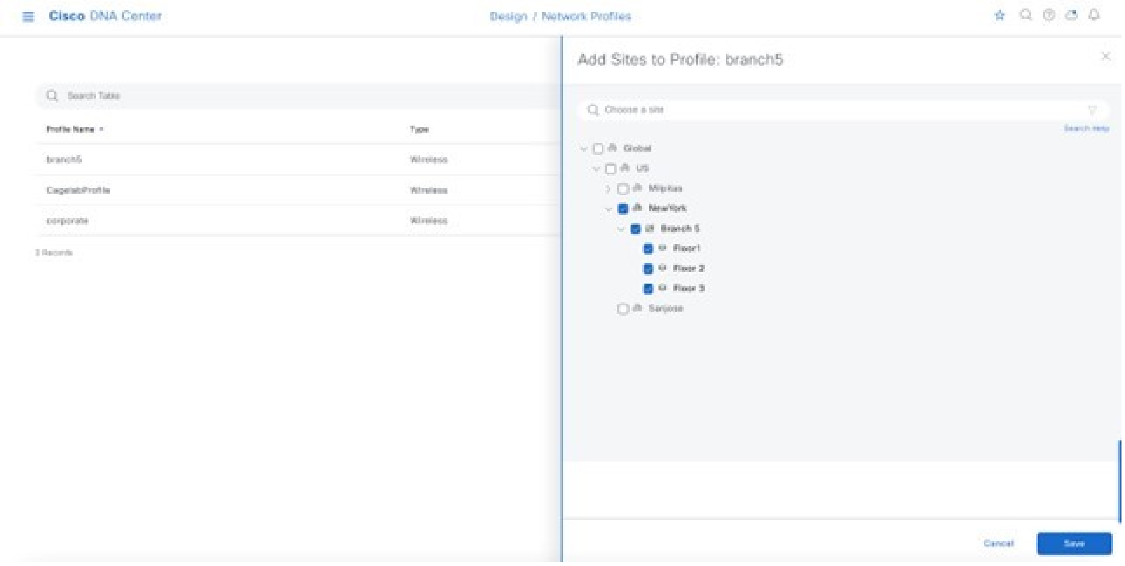
Step 16 Click **Assign Sites** in **Branch Network Profiles**.

Step 17 Select the New York area. This should automatically check the child site locations: **Branch 5** with **Floor 1**, **Floor 2**, and **Floor 3**.

Automatically, the child site locations are selected: **Branch 5** with **Floor 1**, **Floor 2**, and **Floor 3**.

Step 18 Click **OK** to close the site hierarchy side panel and return to the **Create a Wireless Profile** side panel.

Figure 51: Site Assignment to Flex Guest Profile



Profile Name	Type
branch5	Wireless
CagelabProfile	Wireless
corporate	Wireless

3 Records

Add Sites to Profile: branch5

- □ Global
  - □ US
    - □ Milpitas
    - ☑ NewYork
      - ☑ Branch 5
        - ☑ Floor1
        - ☑ Floor 2
        - ☑ Floor 3
    - □ Sanjose

Step 19 Click **+ Add** under **Attach Template(s)** to add the CLI-based templates to the enterprise wireless network configuration.

Note You must have defined all the templates within the **Template Editor** window of Cisco DNA Center. This design and deployment guide will not discuss the addition of templates because the guide does require knowledge of the CLI syntax for the specific Cisco Wireless Controller platform. However, you can add the wireless features that are not supported by the web-based GUI of Cisco DNA Center through templates.

The new enterprise wireless network, **lab3branch5**, is displayed in the **Wireless Network Settings** window.

Note WLAN profiles created with different AAA settings can be assigned at different site levels. Site level overrides will push a new WLAN profile to the wireless controller. You can override the Global SSID with the settings based on area, buildings, and floor levels.

Cisco recommends updating the WLAN Profile Name when making any site level overrides for the SSID. If the same WLAN profile name is already configured in the wireless controller that manages the selected sites, a provisioning failure will occur.

Only L2 Security, AAA Configuration, NAS-ID, Mac Filtering, AP Impersonation, Radius Client Profiling, CCKM, MPSK, Protected Management Frame (802.11w), AAA Override, and WLAN Profile Name can be overridden at site levels. To edit other parameters, navigate to the global level.

Configure FlexConnect Settings for Guest SSID

The following procedure describes how to configure the FlexConnect settings for a guest SSID.

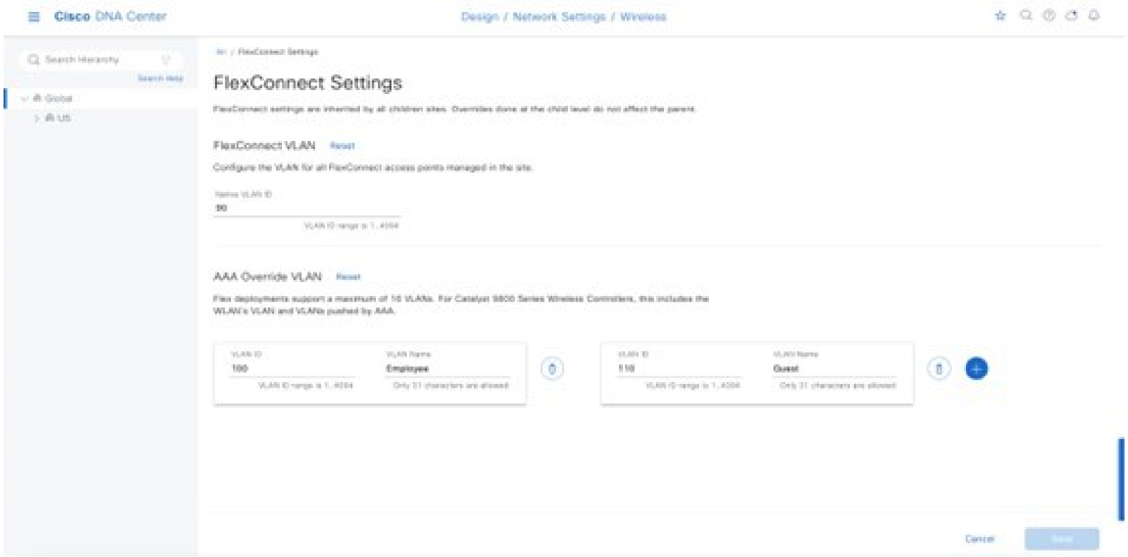
Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network settings** > **Wireless Flex connect settings**.

Step 2 Configure native VLAN and AAA override VLAN in global settings.

Note You can override the native VLAN and AAA override VLAN in global settings at the area, building, and floor levels.

Figure 52: FlexConnect Settings for Flex Guest SSID Image



Cisco DNA Center
Design / Network Settings / Wireless
Search Hierarchy
Search Help
Global
US
All / FlexConnect Settings

FlexConnect Settings

FlexConnect settings are inherited by all children sites. Overrides done at the child level do not affect the parent.

FlexConnect VLAN

Configure the VLAN for all FlexConnect access points managed in the site.

Native VLAN ID: 90

VLAN ID range is 1..4094

AAA Override VLAN

Flex deployments support a maximum of 16 VLANs. For Catalyst 9800 Series Wireless Controllers, this includes the WLAN's VLAN and VLANs pushed by AAA.

VLAN ID	VLAN Name
100	Employee
110	Guest

VLAN ID range is 1..4094

Only 31 characters are allowed

Configure Model Config Editor for Flex Guest SSID

This section describes the procedure to configure the model config for a flex guest SSID.

Procedure

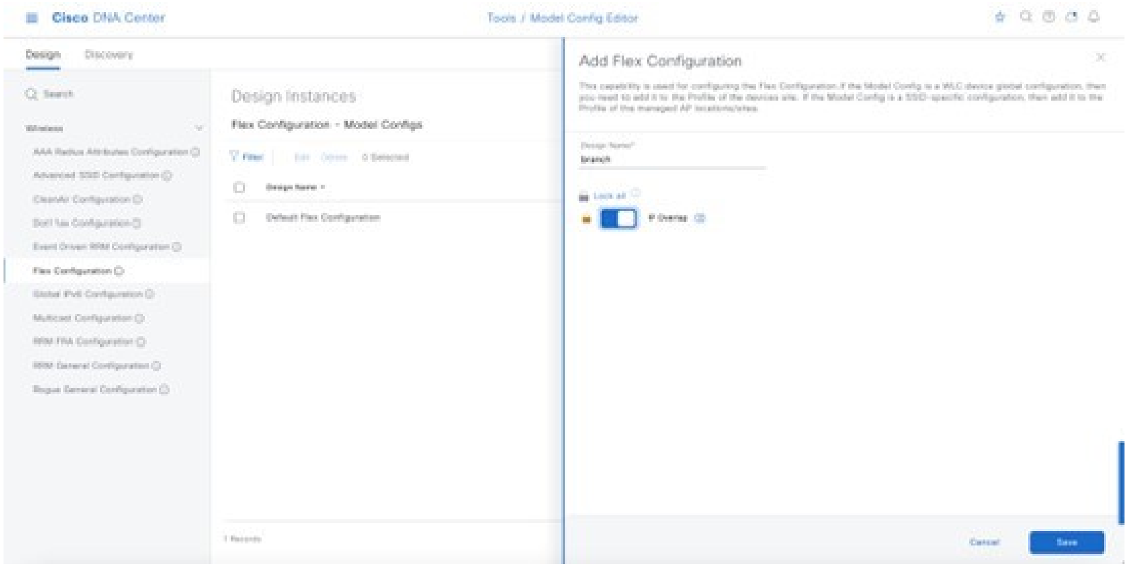
Step 1 From the top-left corner, click the menu icon and choose **Tools** > **Model Config Editor**.

Step 2 Click **Flex Configuration**.

Step 3 Click **Add** and provide design name as branch.

Step 4 Enable **IP Overlap**.

Figure 53: Model Config for Flex Guest SSID


Cisco DNA Center
Tools / Model Config Editor
Design
Discovery
Search
Wireless
AAA Radius Attributes Configuration
Advanced SSID Configuration
CleanAir Configuration
Dot11ax Configuration
Event Driven RRM Configuration
Flex Configuration
Global IPv6 Configuration
Multicast Configuration
RRM FRA Configuration
RRM General Configuration
Rogue General Configuration
Design Instances
Flex Configuration - Model Configs
Filter
Edit
Delete
0 Selected
Design Name
Default Flex Configuration
1 Records
Add Flex Configuration
Lock all
Cancel
Save

This capability is used for configuring the Flex Configuration. If the Model Config is a WLC device global configuration, then you need to add it to the Profile of the devices site. If the Model Config is a SSID-specific configuration, then add it to the Profile of the managed AP locations/sites.

Design Name*: branch

IP Overlap: on

Map Flex Guest SSID Model Config to Network Profiles

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Profile**.

Step 2 Choose the **Edit branch5** network profile.

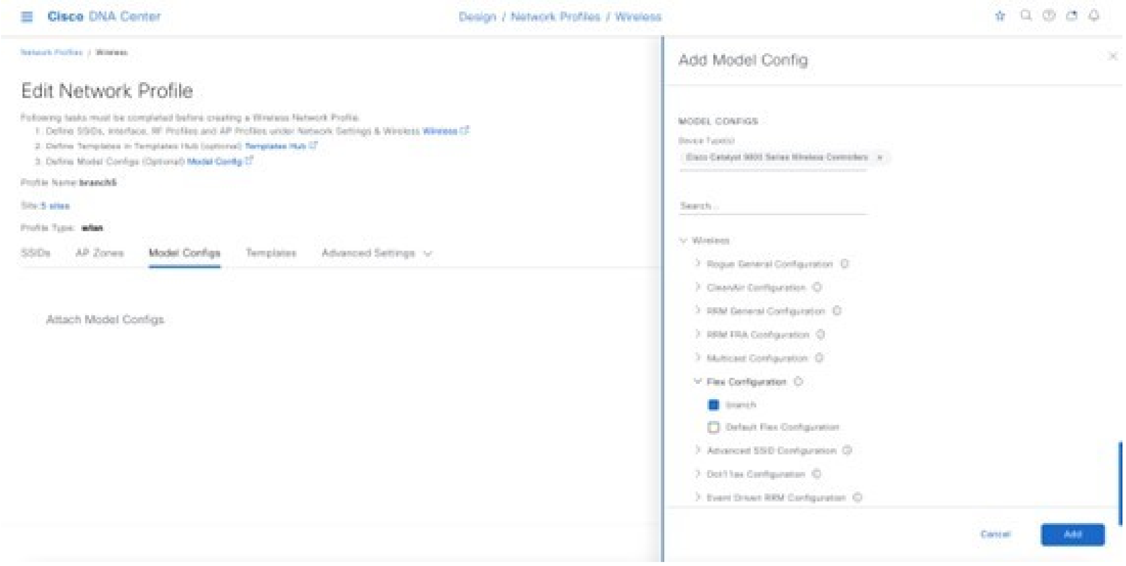
Step 3 Click **Model Config** and add a model config.

Step 4 For **Device Type**, choose wireless controller.

Step 5 Click **Wireless** > **Flex Configuration** and choose the configured model config.

Step 6 Click **Add** and save the changes.

Figure 54: Map FlexConnect Model Config to Guest Network Profile



Cisco DNA Center

Design / Network Profiles / Wireless

Network Profiles / Wireless

Edit Network Profile

Following tasks must be completed before creating a Wireless Network Profile.

1. Define SSIDs, Interface, RF Profiles and AP Profiles under Network Settings & Wireless Wireless
2. Define Templates in Templates Hub (optional) Templates Hub
3. Define Model Configs (Optional) Model Config

Profile Name: branch5

Site: 5 sites

Profile Type: wlan

Add Model Config

MODEL CONFIGS

Device Type(s): Cisco Catalyst 9800 Series Wireless Controllers

- Wireless
  - Rogue General Configuration
  - CleanAir Configuration
  - RRM General Configuration
  - RRM FRA Configuration
  - Multicast Configuration
  - Flex Configuration
    - ☑ branch
    - □ Default Flex Configuration
  - Advanced SSID Configuration
  - Dot11ax Configuration
  - Event Driven RRM Configuration

Customize Wireless RF Profiles

The **Wireless Radio Frequency Profile** section of the **Wireless Settings** dashboard allows you to do the following:

- Visually inspect the settings for each of the three preconfigured RF profiles within Cisco DNA Center. These RF profiles are also preconfigured within the Cisco Catalyst 9800 Series Wireless Controller.
- Create custom RF profiles in which you can fine tune various RF aspects of your wireless deployment.
- Choose either a preconfigured or custom RF profile as the default RF profile that is assigned to APs within Cisco DNA Center.

When provisioning APs in Cisco DNA Center, the default RF profile configured within the **Wireless Settings** dashboard will be applied. However, you can also override this setting for each AP.

The following preconfigured RF profiles are available:

- LOW: This profile tunes the RF attributes in both bands (2.4 GHz and 5 GHz) for low client density deployments.
- TYPICAL: This profile tunes the RF attributes in both bands (2.4 GHz and 5 GHz) for medium client density deployments.
- HIGH: This profile tunes the RF attributes in in both bands (2.4 GHz and 5 GHz) for high client density deployments, such as stadiums, auditoriums, etc.

Note Appendix D explains the specific settings within each of the three preconfigured RF profiles within Cisco DNA Center.

Set the desired TPC threshold on the RF group, based on the AP density and installed height. For large deployments, there can be significant variations in the RF environment, so it is important to properly adjust TPC to ensure optimal coverage in each location.

Together with transmit power, data rates are the primary mechanism to influence the client roaming behavior. Changing data rates to the lowest mandatory rate can modify when the client may trigger a new roam, which is especially important for large open spaces that suffer from sticky client problems.

When setting up RF profiles, try to avoid configuring adjacent AP groups and RF profiles with different DCA channel sets, as this can negatively impact DCA calculations.

Users can add a nonsupported channel to the RF profile DCA list, even if the channel is not supported in the configured regulatory domain. The recommendation is to always check if the configured channels are allowed in the country domain. There is no impact on network operations because the DCA would not assign the unsupported channels to the APs. However, starting in release 17.5, the C9800 has a validation to check if the added channels are allowed.

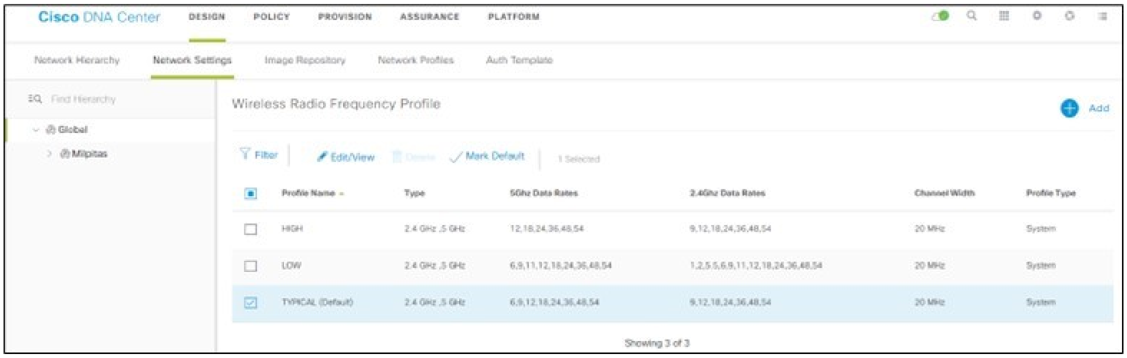
Procedure

Step 1 From the **Wireless Network Settings** dashboard, locate the **Wireless Radio Frequency Profile** section.

The **Wireless Radio Frequency Profile** section of the **Wireless Settings** dashboard can only be accessed at the global level of the site hierarchy.

Step 2 By default, the TYPICAL RF profile is set as the default RF profile. You will know this because it will appear as **TYPICAL (Default)** as shown in the following figure. To change the RF profile, check the check box next to the name of one of the available profiles, and then click the ✓ default button.

Figure 55: Wireless Radio Frequency Profile



Wireless Radio Frequency Profile

■	Profile Name	Type	5Ghz Data Rates	2.4Ghz Data Rates	Channel Width	Profile Type
□	HIGH	2.4 GHz ,5 GHz	12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz	System
□	LOW	2.4 GHz ,5 GHz	6,9,11,12,18,24,36,48,54	1,2,5.5,6,9,11,12,18,24,36,48,54	20 MHz	System
☑	TYPICAL (Default)	2.4 GHz ,5 GHz	6,9,12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz	System

Showing 3 of 3

For this design and deployment guide, the TYPICAL RF profile was selected, indicating that the deployment is meant for an environment with medium client density.

The FlexConnect design for a remote office is now complete.

Design the Cisco Catalyst 9800-CL Wireless Controller Hosted on AWS

This section describes the wireless controller hosted on AWS deployment, which uses a cloud-based Cisco Catalyst 9800-CL Wireless Controller hosted on AWS. For more information, see Deployment guide for Cisco Catalyst 9800 Wireless Controller for Cloud (C9800-CL) on Amazon Web Services (AWS).

Launching a Cisco Catalyst 9800 Amazon Machine Image (AMI) occurs directly from the AWS Marketplace. The Cisco Catalyst 9800 Series Wireless Controller will be deployed on an Amazon EC2 in an Amazon Virtual Private Cloud (VPC).

Cisco supports the following instance type for the first release of the Cisco Catalyst 9800 Series Wireless Controller on the cloud:

C5.xlarge: 4 vCPUs, 8 GB RAM, 8GB Disk with 1 vNIC.

The allocated resources will allow the instance to scale to 1000 APs and 10,000 clients.

Prerequisites for Deploying the Cisco Catalyst 9800-CL Wireless Controller on AWS

- Create a managed VPN connection from the corporate network to the VPC.
- Create a VPC with the desired subnet for the wireless management interface on the Catalyst 9800 Series Wireless Controller.
- Catalyst 9800 Series Wireless Controller CloudFormation template: You do not have to configure the CloudFormation template because the template is automatically integrated in the launching procedure. If desired, you can download and view the CloudFormation template file from the AWS Marketplace page for the product.
- Amazon Machine Instance ID (AMI-ID) for the desired Catalyst 9800 Series Wireless Controller software release: The AMI will be available in the AWS marketplace.
- AP access can be restricted to your instance for security reasons. For example, CAPWAP from a single, specific IP range can be allowed so that only those APs are able to register to the controller. The following table shows the ports that need to be opened in the firewall to allow the AP to communicate with the wireless controller on AWS.

Table 17: Ports Required to be Opened in Firewall

Ports	Protocol
UDP 5246/5247/5248	CAPWAP
TCP 22	SSH, SCP
TCP 21	FTP
ICMP	Ping
UDP 161, 162	SNMP/SNMP Traps
TCP 443/80	HTTPs/HTTP
TCP/UDP 49	TACACS+
UDP 53	DNS Server
UDP 1812/1645/1813/1646	Radius
UDP 123	NTP Server
UDP 514	Syslog

Install the Cisco Catalyst 9800-CL Wireless Controller on AWS

Procedure

Step 1 Navigate to the AWS Marketplace.

Step 2 Locate the Cisco Catalyst 9800-CL Wireless Controller product page by searching the AWS Marketplace for "C9800-CL."

Step 3 Choose the **Cisco Catalyst 9800-CL Wireless Controller for Cloud** and click **Continue to Subscribe**.

Step 4 Choose the fulfillment option: **Cloud Formation Template** (recommended) or **Amazon Machine Image (AMI)**.

If you choose AMI, you can use the AWS Console or the AWS Marketplace interface.

For both fulfillment options, you will be guided through the steps to launch a new Catalyst 9800-CL Wireless Controller instance.

Step 5 During the installation process, you will be prompted to select the following:

- The desired AWS region.
- The VPC (custom or default) and installation location for the Catalyst 9800-CL Wireless Controller.
- The desired IP subnet for the Catalyst 9800-CL Wireless Controller management and wireless management interface.
- The security group associated with the VPC.
- The key pair for SSH connection.

Step 6 Click **Review and Launch** and ensure that the information is accurate.

Step 7 Click **Launch Instances**.

Step 8 Go to **AWS Console** > **EC2** services and wait for your instance to indicate a state of **running**. You will have to wait a few minutes before you can connect to your Catalyst 9800-CL Wireless Controller instance.

Step 9 Connect to the IP address assigned to your Catalyst 9800-CL Wireless Controller instance and use the WebUI wizard for Day 0 configuration and setup.

Step 10 Alternatively, connect to your instance using an SSH client, providing the necessary credentials or the private SSH key selected during setup.

For example: `ssh -i mykeypair.pem ec2-user@<IP of the instance>`

Step 11 Once SSH has connected, you should see the IOS XE command prompt on the Catalyst 9800-CL Wireless Controller. You may now begin configuring your instance.

Configure Enterprise Wireless Networks (SSIDs)

Wireless settings are hierarchical. Settings at lower levels of the site hierarchy can override settings defined in higher levels. By default, you are taken to the global level, which is the highest level of the site hierarchy.

Enterprise wireless networks are the nonguest WLANs/SSIDs that are available for broadcast across the deployment, and these networks must be defined at the global level of the site hierarchy. Once defined, enterprise wireless networks are applied to wireless profiles, which are assigned to one or more sites within the hierarchy. For this design and deployment guide, a single enterprise WLAN/SSID named **corpevent** is provisioned. The following steps explain how to configure the enterprise wireless network within Cisco DNA Center.

Before you begin

To complete this action, your user profile must be assigned the SUPER-ADMIN-ROLE or the NETWORK-ADMIN-ROLE.

Procedure

Step 1 Log in to the Cisco DNA Center web console using an IP address or a fully qualified domain name.

Example:

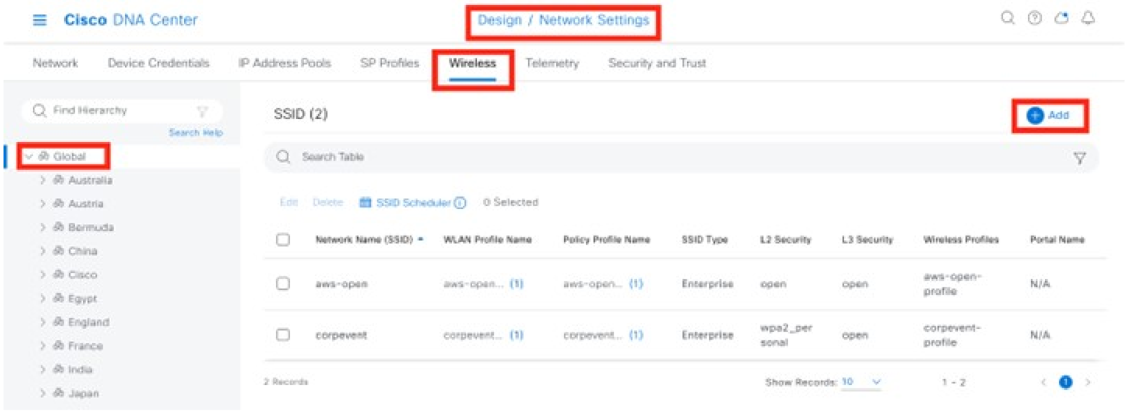
http://<Cisco_DNA_Center_IPaddr_or_FQDN>

Step 2 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 3 From the **Wireless Network Settings** dashboard, hover your cursor over **+ Add** and choose **Enterprise**.

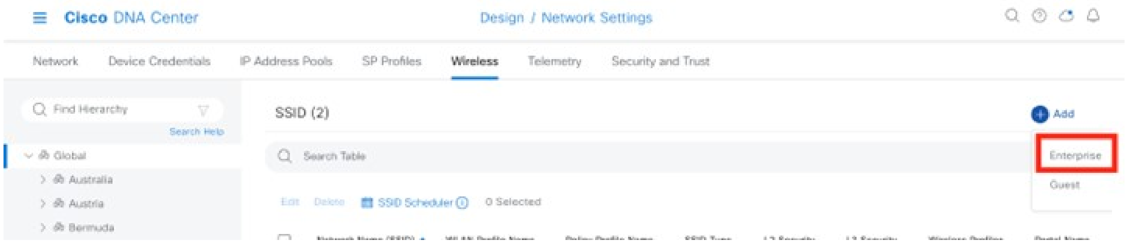
The **Create an Enterprise Wireless Network** dialog box is displayed.

Figure 56: Wireless Network Settings



Network Name (SSID)	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name
aws-open	aws-open... (1)	aws-open... (1)	Enterprise	open	open	aws-open-profile	N/A
corpevent	corpevent... (1)	corpevent... (1)	Enterprise	wpa2_personal	open	corpevent-profile	N/A

Figure 57: Selecting an Enterprise for Wireless Network Settings



Step 4 Enter the necessary information and click **Next**.

The settings used in this deployment are provided in the following table.

Table 18: Settings for Enterprise SSID

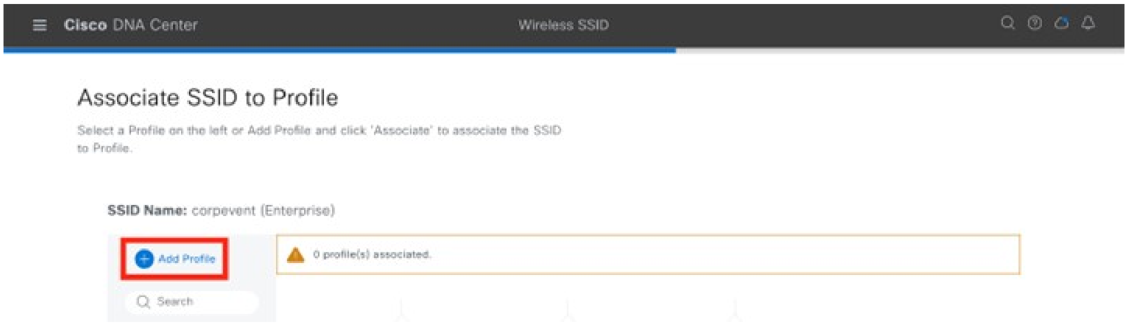
Feature	Settings
Wireless Network Name (SSID)	Corpevent
Broadcast SSID	On

Feature	Settings
Wireless Option	Multiband operation (2.4GHz, 5GHz, 6GHz)
Primary Traffic Type	VoIP (Platinum)
Level of Security	Personal, WPA2
Advanced Security Options - Mac Filtering	Unchecked
Passphrase Type	<Enter passphrase>
Fastlane	Unchecked
Identify PSK	Unchecked
Deny RCM clients	Unchecked
Advanced Settings – FAST TRANSITION (802.11r)	Adaptive, Over the DS Unchecked
Advanced Settings – MFP Client Protection	Optional
Advanced Settings – Protected Management Frame (802.11w)	Disabled
Advanced Settings – Session timeout	Checked, 1800 seconds
Advanced Settings – Client Exclusion	Checked, 300 seconds
Advanced Settings – MFP CLIENT PROTECTION	Optional
Advanced Settings – 11k Neighbor List	Checked
Advanced Settings – 11v BSS TRANSITION SUPPORT	BSS Max Idle Service – Checked
	Client Idle User Timeout – Checked, 300 seconds
	Directed Multicast Service - Checked

Step 5 The next page in the workflow is displayed. You can attach the enterprise wireless network to an existing wireless profile, or you can create a new wireless profile and attach the enterprise wireless network.

Step 6 Click **Add** to add a new wireless profile.

Figure 58: Associate SSID to Network Profile



Associate SSID to Profile

Select a Profile on the left or Add Profile and click 'Associate' to associate the SSID to Profile.

SSID Name: corpevent (Enterprise)

0 profile(s) associated.

Step 7 In the **Wireless Profile Name** field, enter the name of the new wireless profile. For this deployment guide, a wireless profile named **corpevent-profile** was created.

Step 8 From **Fabric**, click the **No** radio button.

This deployment guide only discusses non-SDA wireless deployments using Cisco DNA Center. When you choose **No**, the **Select Interface** field is automatically displayed.

Step 9 From the **Select Interface** drop-down list, choose **Management**.

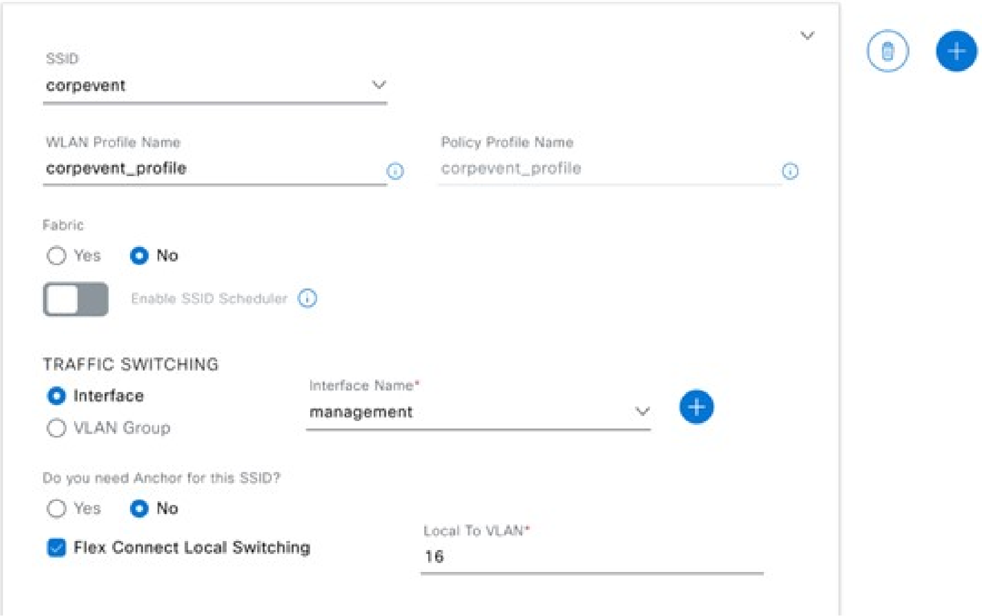
> **Note** The AWS wireless controller does not support layer 2 VLAN because it is not needed for a publicly deployed wireless controller, and the AWS wireless controller is never in use. When doing manual config on an AWS or Azure wireless controller, you can skip this step. However, with Cisco DNA Center provisioning, the FlexConnect flow requires a VLAN to be pushed, even though the VLAN is not in use on an AWS or Azure wireless controller. These wireless controllers only support flex local switching. To avoid Cisco DNA Center from provisioning a VLAN, choose **Management** for the interface.

Step 10 Check the **FlexConnect Local Switching** check box.

Step 11 In the **Local to VLAN** field, enter VLAN ID 16.

All branch employee traffic will be locally switched onto VLAN 16 of the branch switch.

Figure 59: Assign VLAN for Enterprise SSID



SSID
corpevent

WLAN Profile Name
corpevent_profile

Policy Profile Name
corpevent_profile

Fabric
○ Yes ● No

Enable SSID Scheduler

TRAFFIC SWITCHING
● Interface
○ VLAN Group

Interface Name*
management

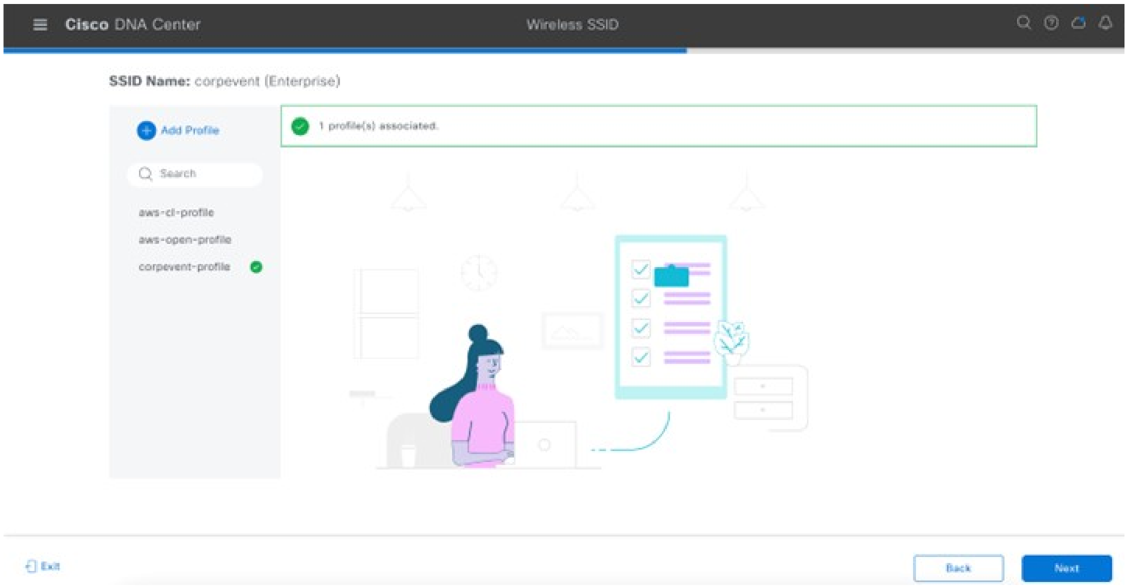
Do you need Anchor for this SSID?
○ Yes ● No

☑ Flex Connect Local Switching

Local To VLAN*
16

Step 12 Click **Associate Profile** to attach the profile to wireless SSID.

Figure 60: Successful Association of SSID to Network Profile



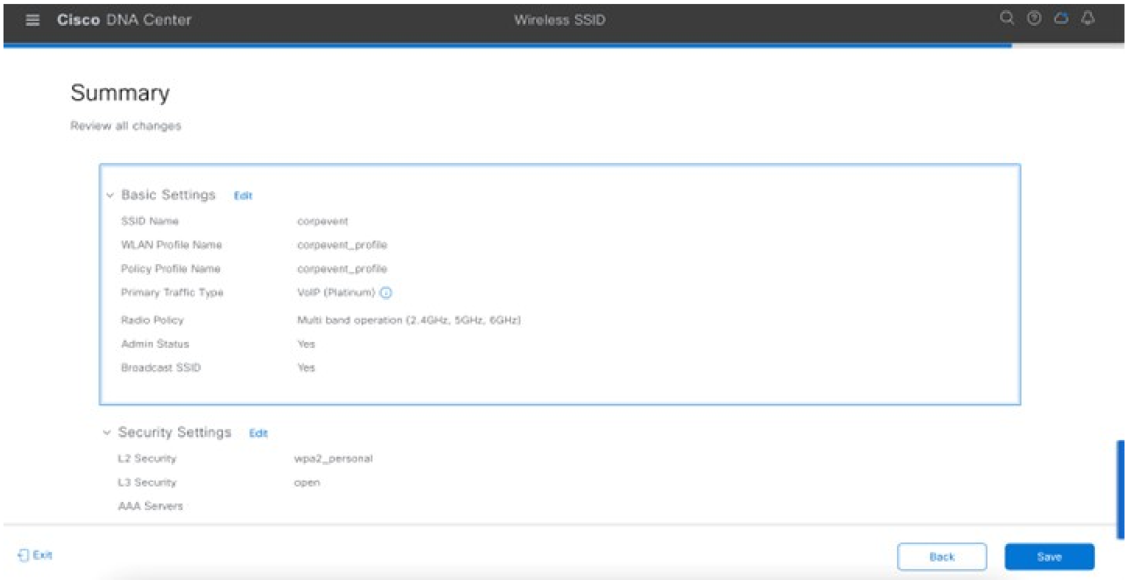
SSID Name: corpevent (Enterprise)

1 profile(s) associated.

- aws-cl-profile
- aws-open-profile
- corpevent-profile ✓

Step 13 Click **Next** to review the summary, and then click **Save**.

Figure 61: Summary Page for Reviewing Enterprise SSID Configuration



Summary

Review all changes

Basic Settings

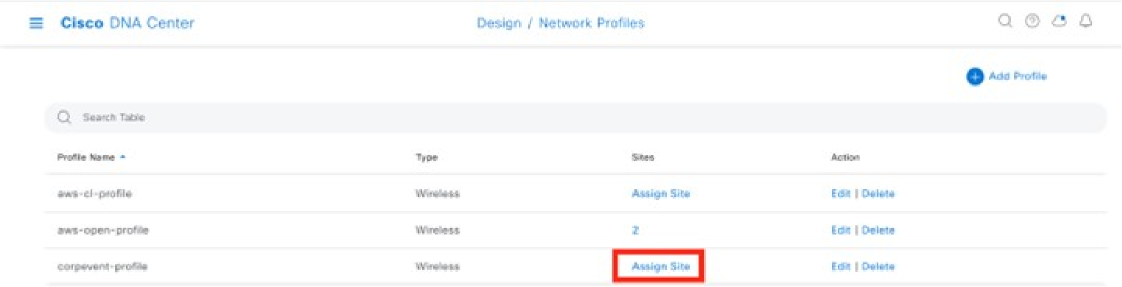
SSID Name	corpevent
WLAN Profile Name	corpevent_profile
Policy Profile Name	corpevent_profile
Primary Traffic Type	VoIP (Platinum)
Radio Policy	Multi band operation (2.4GHz, 5GHz, 6GHz)
Admin Status	Yes
Broadcast SSID	Yes

Security Settings

L2 Security	wpa2_personal
L3 Security	open
AAA Servers	

Step 14 Click **Configure Network Profile** to go to the **Network Profiles** page to assign the site for the wireless profile.

Figure 62: Site Assignment for Network Profile



Profile Name	Type	Sites	Action
aws-cl-profile	Wireless	Assign Site	Edit | Delete
aws-open-profile	Wireless	2	Edit | Delete
corpevent-profile	Wireless	Assign Site	Edit | Delete

Step 15 Click **Assign Site**.

Step 16 In the left hierarchy tree, choose Global > Milpitas area.

The child site locations are automatically selected: **Branch 5** and **Floor 1** and **Floor 2**.

Step 17 Click **OK** to close the site hierarchy side panel and return to **Create a Wireless Profile**.

The design of the wireless controller on AWS is complete, and you can go to the *Deploy the wireless network* section.

Deploy the Wireless Network

This section of the design and deployment guide implements the use case discussed in the *Solution Overview* section of this document. Cisco DNA Center is used to automate the deployment of the wireless profile created in the *Design the wireless network* section of this document to a Cisco Catalyst 9800-40 enterprise wireless controller HA SSO pair (WLC-9800-2) and a Cisco Catalyst 9800-CL guest wireless controller (WLC-9800-CL).

This section contains the following topics and processes:

- Discover and manage the Catalyst 9800 Series Wireless Controllers
- Manage software images for the Catalyst 9800 Series Wireless Controllers
- Use software image management (SWIM) to update the Catalyst 9800 Series Wireless Controller software
- Configure high availability (HA) stateful switch-over (SSO) on the Catalyst 9800-40 enterprise wireless controllers
- Provision the Catalyst 9800-40 enterprise wireless controller HA SSO pair
- Provision the Catalyst 9800-CL guest anchor wireless controller
- Join the new APs to the enterprise wireless controller HA SSO pair
- Provision the new APs
- Position the new APs on the floor map
- Local RRM Vs cloud-based RRM
- Enable cloud-based RRM
- Template programmer for additional wireless configurations

Enterprise WLAN for Campus Wireless Deployment

This section explains how to provision the campus wireless deployment for the Milpitas site. For this scenario, the wireless controllers are discovered, and their images are updated and provisioned. These procedures are explained in the following sections.

Discover and Manage the Cisco Catalyst 9800 Series Wireless Controller

This deployment guide uses IP address ranges for discovery of both of the Cisco Catalyst 9800-40 Wireless Controllers deployed as enterprise wireless controllers and the Cisco Catalyst 9800-CL Wireless Controller deployed as the guest wireless controller. Before initiating the discovery, IP connectivity must be enabled to the devices. When using IP address ranges, you can reduce the range to just the wireless controllers to speed the discovery.

Note Alternatively, you can supply an initial device for discovery and direct Cisco DNA Center to use Cisco Discovery Protocol (CDP) to find connected neighbors.

The following assumptions are made for this procedure:

- The two Catalyst 9800-40 Wireless Controllers (WLC-9800-1 and WLC-9800-2) are connected to the network as standalone wireless controllers. Configuration of the two Catalyst 9800-40 Wireless Controllers into an HA SSO pair will be done within Cisco DNA Center in a later process.
- NETCONF is enabled on all of the Cisco Catalyst 9800 Series Wireless Controllers (WLC-9800-1, WLC-9800-2, and WLC-9800-CL).
- All Catalyst 9800 Series Wireless Controllers are on the network, with management IP addresses configured for reachability.
- SSH access is enabled on all of the Catalyst 9800 Series Wireless Controllers, with a user ID and password configured within the local user database.
- All Catalyst 9800 Series Wireless Controllers have hostnames configured (WLC-9800-1, WLC-9800-2, and WLC-9800-CL), which will allow the devices to be identified by their hostnames within the Cisco DNA Center inventory after discovery.

For this design and deployment guide, the following table shows the hostnames, platform models, and IP addresses for Cisco DNA Center.

Table 19: Hostnames, Platform Models, and IP Addresses for Cisco DNA Center

Hostname	Platform Model	IP Address
WLC-9800-1	Cisco Catalyst 9800-40 Wireless Controller	10.4.50.2
WLC-9800-2	Cisco Catalyst 9800-40 Wireless Controller	10.4.50.22
WLC-9800-CL	Cisco Catalyst 9800-CL Wireless Controller	10.4.48.153

This section contains the following processes:

- Discover the two Catalyst 9800-40 Wireless Controllers, which serve as the enterprise HA SSO pair for the WLAN deployment.
- Discover the Catalyst 9800-CL Wireless Controller, which serves as the guest anchor wireless controller for the WLAN deployment.

Discover and Manage the Cisco Catalyst 9800-CL Wireless Controller Deployed on AWS

The discovery process is the same for other Cisco Catalyst 9800-CL Wireless Controllers.

Discover the Cisco Catalyst 9800-40 Wireless Controllers Serving as the Enterprise HA SSO Pair for WLAN Deployment

The following steps explain how to discover the Cisco Catalyst 9800-40 Wireless Controllers (WLC-9800-1 and WLC-9800-2).

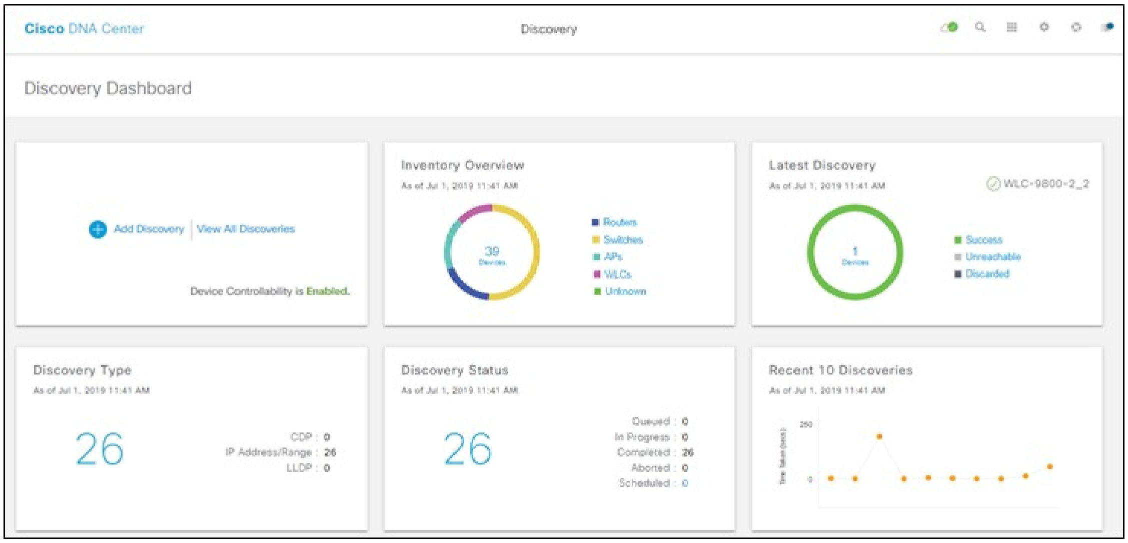
Procedure

Step 1 Navigate to the main Cisco DNA Center dashboard.

Step 2 From the top-left corner, click the menu icon and choose **Tools** > **Discovery**.

The **Discovery Dashboard** is displayed.

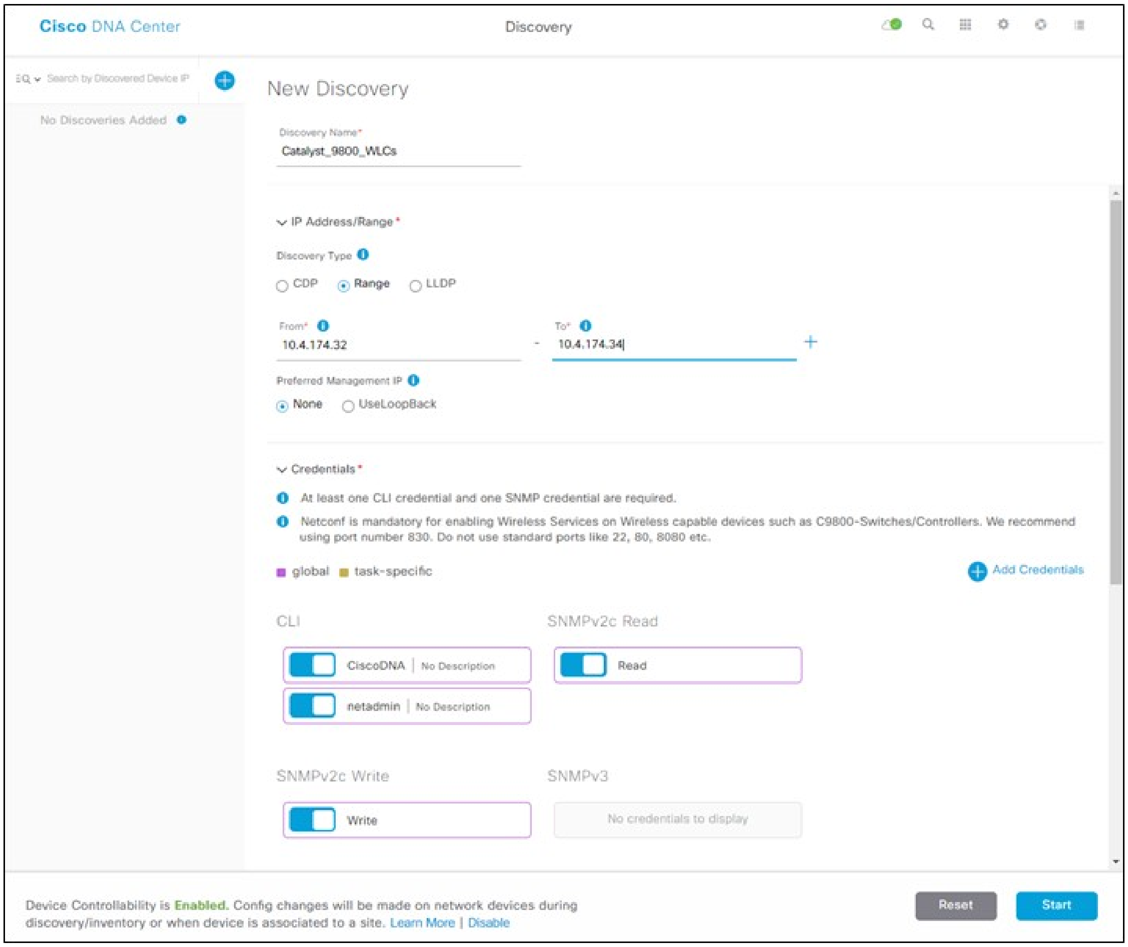
Figure 63: Discovery Dashboard



Step 3 Click **+ Add Discovery** to create a new discovery.

The **New Discovery** window is displayed.

Figure 64: New Discovery Window



New Discovery

Discovery Name*: Catalyst_9800_WLCs

IP Address/Range*

Discovery Type: ○ CDP ● Range ○ LLDP

From*: 10.4.174.32 - To*: 10.4.174.34

Preferred Management IP: ● None ○ UseLoopBack

Credentials*

At least one CLI credential and one SNMP credential are required.

Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers. We recommend using port number 830. Do not use standard ports like 22, 80, 8080 etc.

■ global ■ task-specific

CLI: CiscoDNA | No Description; netadmin | No Description

SNMPv2c Read: Read

SNMPv2c Write: Write

SNMPv3: No credentials to display

Device Controllability is Enabled. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

Step 4 From **IP Address/Range**, for **Discovery Type**, click the **Range** radio button.

Step 5 In the **From** field, enter the beginning IP address, and in the **To** field, enter the ending IP address.

The range configured is 10.4.50.2 - 10.4.50.22, which is sufficient to discover the two Catalyst 9800-40 Wireless Controllers (WLC-9800-1 and WLC-9800-2).

Step 6 For **Preferred Management IP**, if a device has a loopback interface used for management, click the **Use Loopback** radio button. Otherwise, click the **None** radio button.

For this deployment, the VLAN 174 interface is configured as the wireless management interface, so **Preferred Management IP** is set to **None**.

Step 7 Make sure the **CLI**, **SNMP**, and **NETCONF** credential toggle buttons are set to **On**.

All Catalyst 9800 Series Wireless Controllers require **NETCONF** for discovery and provisioning. The user ID and password used for NETCONF access to the wireless controllers is the same as the SSH password.

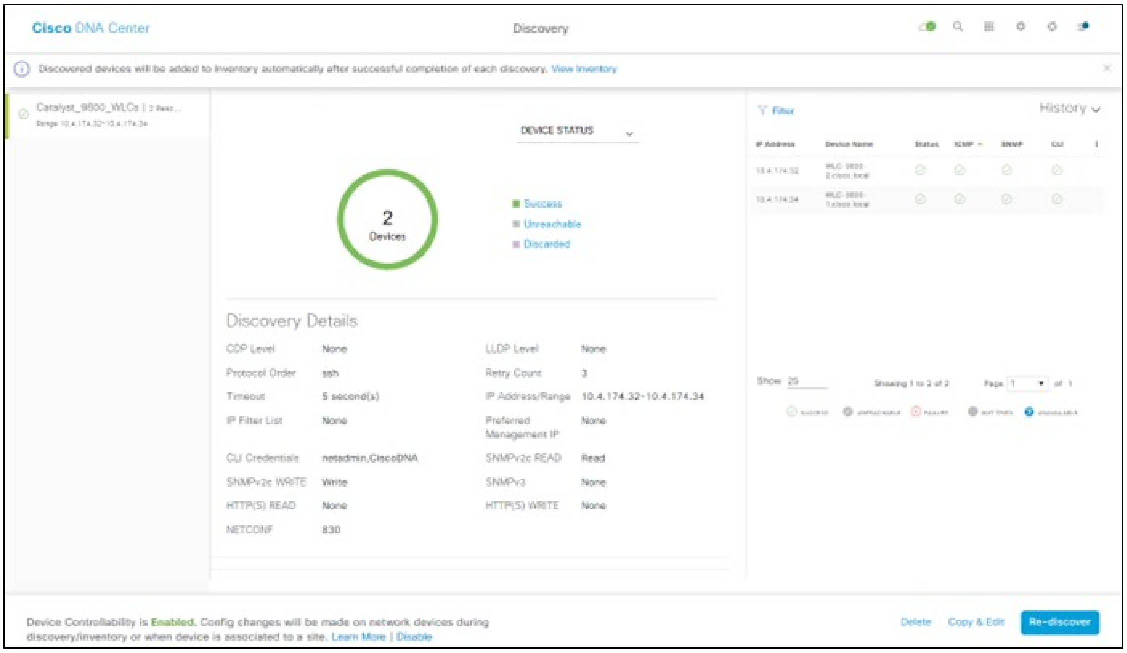
Step 8 From the **Advanced** section, for **Protocol Order**, check the **SSH** check box.

It is not recommended to enable Telnet because Telnet traffic is sent in clear text across the network, which could pose a security vulnerability.

Step 9 Click **Start** to begin the discovery.

The discovery details are displayed while the discovery runs. After discovery is complete, the discovery details are displayed.

Figure 65: Discovery Details



Discovered devices will be added to Inventory automatically after successful completion of each discovery. View Inventory

IP Address	Device Name	Status	ICMP	SNMP	CLI
10.4.174.32	WLC-9800-2.cisco.local	✓	✓	✓	✓
10.4.174.34	WLC-9800-1.cisco.local	✓	✓	✓	✓

Discovery Details

CDP Level	None	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Address/Range	10.4.174.32-10.4.174.34
IP Filter List	None	Preferred Management IP	None
CLI Credentials	netadmin,CiscoDNA	SNMPv2c READ	Read
SNMPv2c WRITE	Write	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	830		

Device Controllability is Enabled. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. Learn More | Disable

Step 10 After the discovery process is complete, navigate to the main Cisco DNA Center dashboard.

Step 11 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The list of devices known to Cisco DNA Center will be displayed, including the two Catalyst 9800-40 Wireless Controllers (WLC-9800-1 and WLC-9800-2) that were discovered. The Catalyst 9800-40 Wireless Controllers should show a **Last Sync Status** of **Managed**.

Cisco DNA Center can now access the devices, synchronize the inventory, and make configuration changes on the devices.

Discover the Cisco Catalyst 9800-CL Wireless Controller Serving as the Guest Anchor Wireless Controller for WLAN Deployment

To discover the Cisco Catalyst 9800-40 Wireless Controller for the Cisco Catalyst 9800-CL guest Wireless Controller (WLC-9800-CL), repeat the steps in Discover the Cisco Catalyst 9800-40 Wireless Controllers Serving as the Enterprise HA SSO Pair for WLAN Deployment.

For this deployment guide, the IP address range for discovery of the Catalyst 9800-CL guest Wireless Controller (WLC-9800-CL) is a single IP address: 10.4.174.36 - 10.4.174.36.

Note Optionally, you can discover all the wireless controllers in a single discovery that includes the IP address range of both the Catalyst 9800-40 enterprise Wireless Controllers (WLC-9800-1 and WLC-9800-2) and the Catalyst 9800-CL guest Wireless Controller (WLC-9800-CL).

Manage Software Images for the Cisco Catalyst 9800 Series Wireless Controllers

This process is used to upload the latest software images for the Cisco Catalyst 9800 Series Wireless Controllers to the Cisco DNA Center software image repository. The following table shows the platforms and software images uploaded for this deployment.

Table 20: Software Images for Catalyst 9800 Series Wireless Controller

Platform	Software Version	Software Image
Cisco Catalyst 9800-40 Wireless Controller	IOS XE Release 17.9.4a	C9800-40-universalk9_wlc.17.09.04a.SPA.bin
Cisco Catalyst 9800-CL Wireless Controller	IOS XE Release 17.9.4a	C9800-CL-universalk9.17.09.04a.SPA.bin

A minimum of IOS XE release 16.10.1 is required for operability between the Catalyst 9800 Series Wireless Controllers and Cisco DNA Center.

The following procedures are included in this process:

- Upload the software image for the Cisco Catalyst 9800-40 Wireless Controller.
- Upload the software image for the Cisco Catalyst 9800-CL Wireless Controller.

Upload the Software Image for the Cisco Catalyst 9800-40 Wireless Controllers

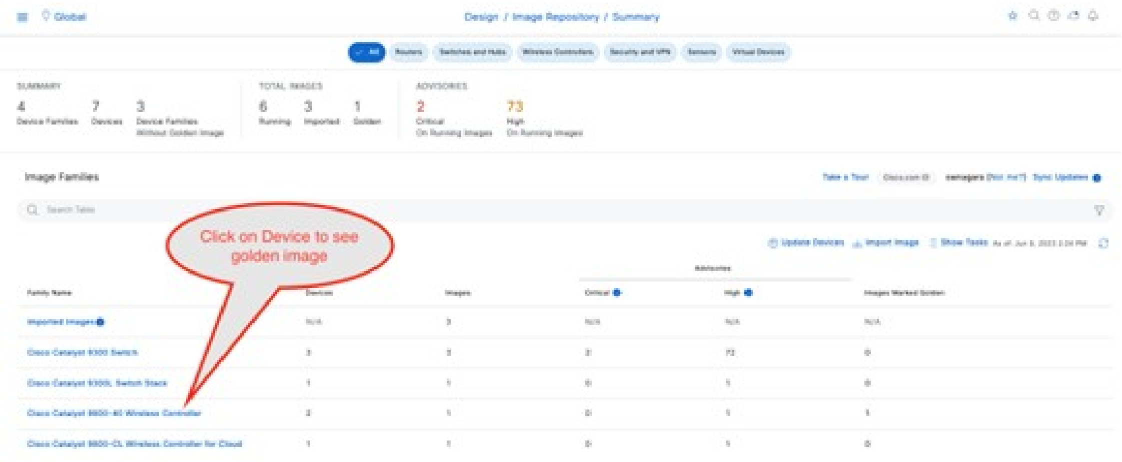
The following steps discuss the image upload process for the Cisco Catalyst 9800-40 Wireless Controllers (WLC-9800-1 and WLC-9800-2).

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Image Repository**.

The **Image Repository** window is displayed in the following figure.

Figure 66: Image Repository



SUMMARY			TOTAL IMAGES			ADVISORIES	
4 Device Families	7 Devices	3 Device Families Without Golden Image	6 Running	3 Imported	1 Golden	2 Critical On Running Images	73 High On Running Images

Image Families

Click on Device to see golden image

			Advisories		
Family Name	Devices	Images	Critical	High	Images Marked Golden
Imported Images	N/A	3	N/A	N/A	N/A
Cisco Catalyst 9300 Switch	3	3	2	72	0
Cisco Catalyst 9300L Switch Stack	1	1	0	1	0
Cisco Catalyst 9800-40 Wireless Controller	2	1	0	1	1
Cisco Catalyst 9800-CL Wireless Controller for Cloud	1	1	0	1	0

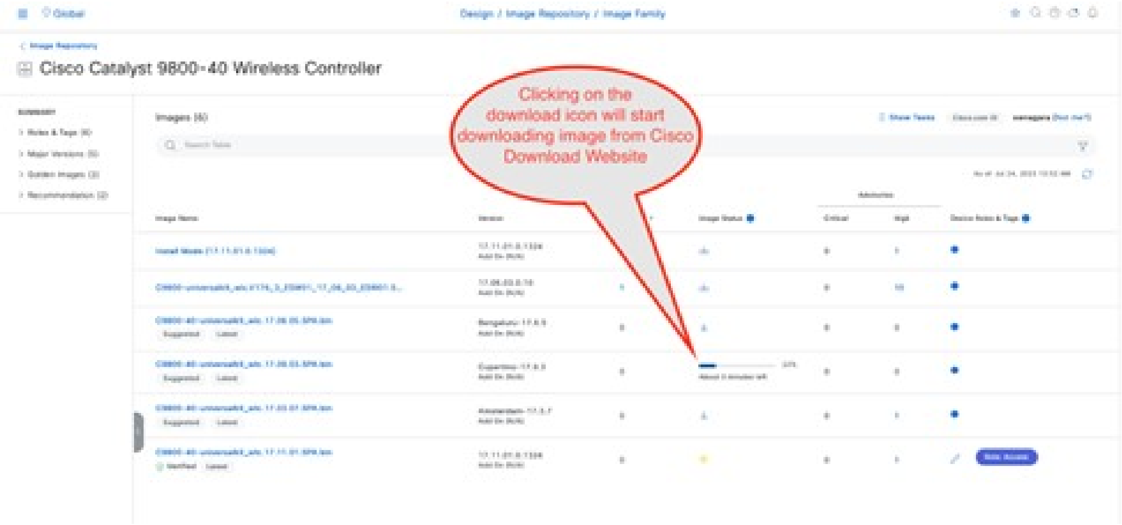
Step 2 You can get a new image into the Cisco DNA Center image repository by doing one of the following:

- Download the image from the Cisco website.
- Import the image from your local machine.

Step 3 For your desired image, click download image icon. The image will begin to download from the Cisco website.

For this deployment guide, image 17.9.4a was downloaded.

Figure 67: Download Image

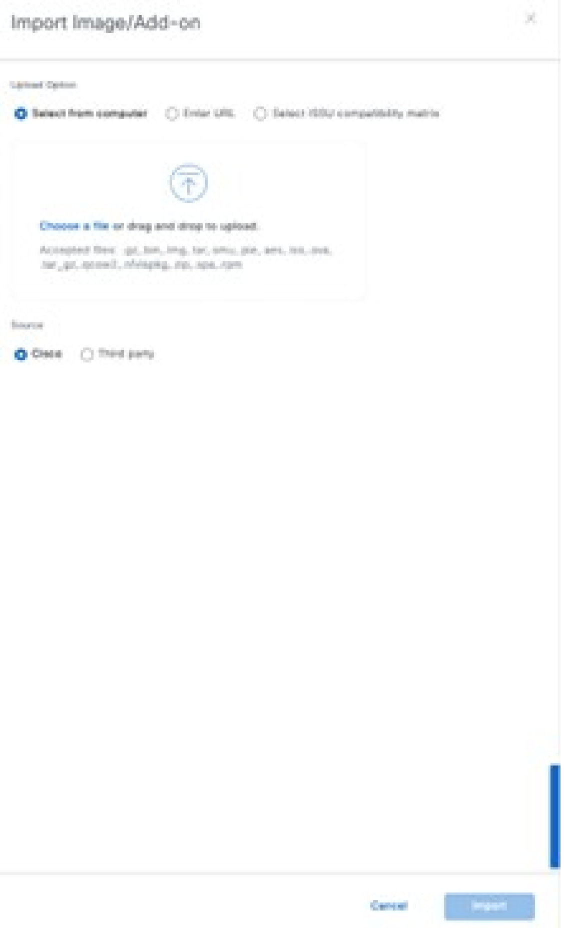


Clicking on the download icon will start downloading image from Cisco Download Website

Step 4 Alternatively, click **Import** to import a new image.

The **Import Image/Add-on** dialog box is displayed.

Figure 68: Import Image



Import Image/Add-on

Upload Option

● Select from computer ○ Enter URL ○ Select ISSU compatibility matrix

Choose a file or drag and drop to upload.

Accepted files: .gz, .bin, .img, .tar, .smu, .pie, .aes, .iso, .ova, .tar.gz, .qcow2, .nfvispkg, .zip, .spa, .rpm

Source

● Cisco ○ Third party

Step 5 Click **Choose File**.

Step 6 Navigate to the Catalyst 9800-40 software image on your computer and choose the desired image.

For this deployment guide, C9800-40-universalk9_wlc.17.09.04a.SPA.bin was chosen.

Step 7 Under **Source**, click the **Cisco** radio button because this is a Cisco software image.

Step 8 Click **Import** to upload the image to the Cisco DNA Center image repository.

A status bar shows the progress of the upload. Once the upload is complete, the main **Image Repository** window is displayed.

Step 9 Click **Show Tasks** to verify that the image was imported successfully.

The **Recent Tasks (Last 50)** side panel is displayed. The new image transitions are shown in yellow. The tasks that are completed successfully are shown with a green check mark.

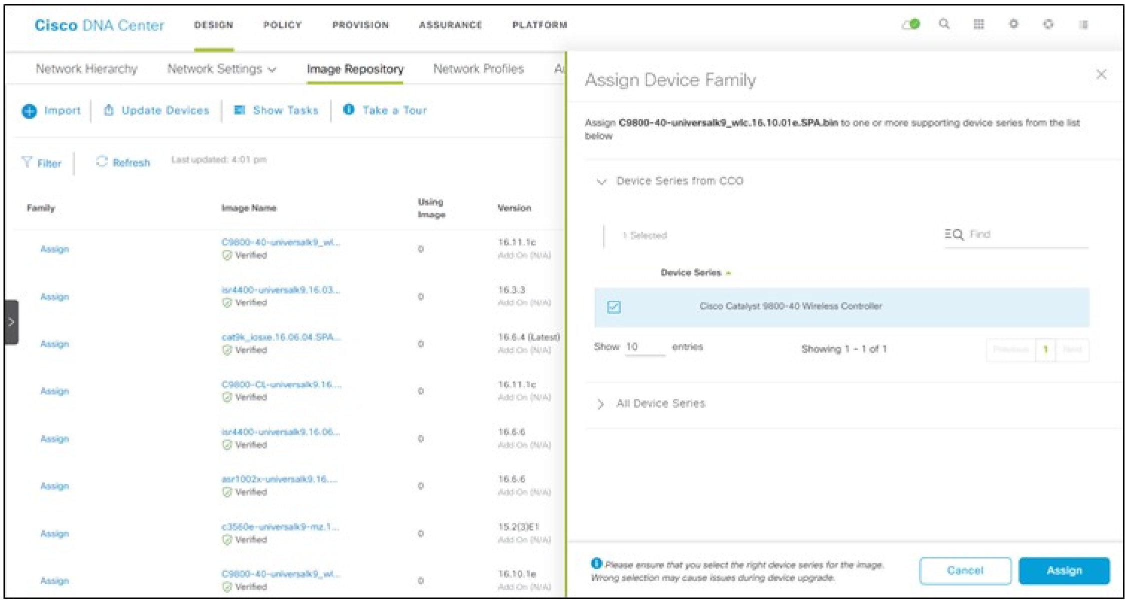
Step 10 Close the **Recent Tasks (Last 50)** side panel.

Step 11 From the **Image Repository** window, click > next to Imported Images to expand the list of imported images.

Step 12 Click **Assign** next to the image file you just uploaded.

The **Assign Device Family** side-in pane is displayed.

Figure 69: Assign Device Family



Last updated: 4:01 pm

Family	Image Name	Using Image	Version
Assign	C9800-40-universalk9_wl... Verified	0	16.11.1c Add On (N/A)
Assign	isr4400-universalk9.16.03... Verified	0	16.3.3 Add On (N/A)
Assign	cat9k_iosxe.16.06.04.SPA... Verified	0	16.6.4 (Latest) Add On (N/A)
Assign	C9800-CL-universalk9.16.... Verified	0	16.11.1c Add On (N/A)
Assign	isr4400-universalk9.16.06... Verified	0	16.6.6 Add On (N/A)
Assign	asr1002x-universalk9.16.... Verified	0	16.6.6 Add On (N/A)
Assign	c3560e-universalk9-mz.1... Verified	0	15.2(3)E1 Add On (N/A)
Assign	C9800-40-universalk9_wl... Verified	0	16.10.1e Add On (N/A)

Assign Device Family

Assign **C9800-40-universalk9_wlc.16.10.01e.SPA.bin** to one or more supporting device series from the list below

Device Series from CCO

1 Selected

Find

	Device Series
☑	Cisco Catalyst 9800-40 Wireless Controller

Show 10 entries

Showing 1 - 1 of 1

All Device Series

Please ensure that you select the right device series for the image. Wrong selection may cause issues during device upgrade.

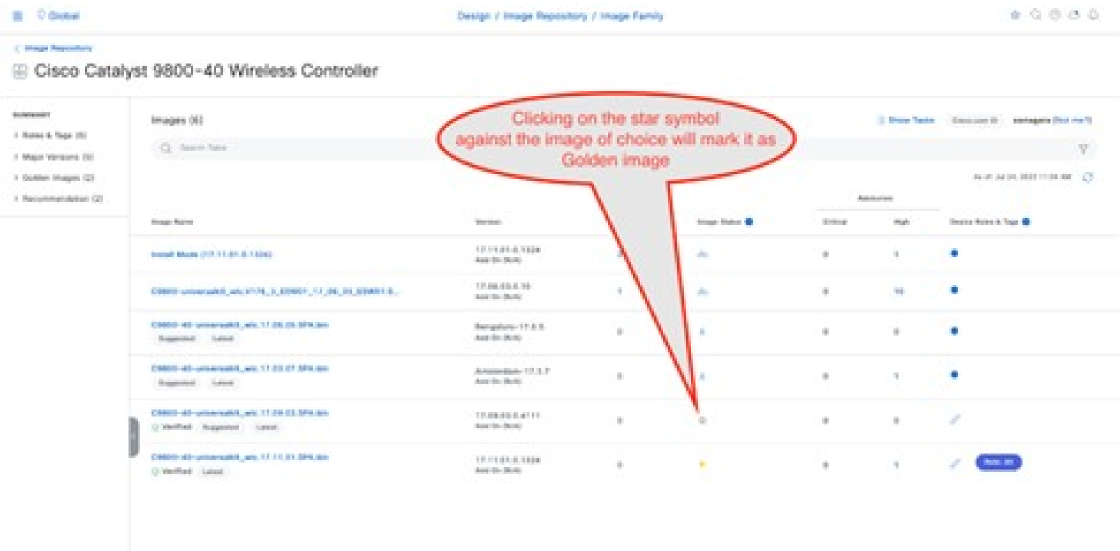
Step 13 Choose the **Cisco Catalyst 9800-40 Wireless Controller** and click **Assign** to assign this image to its device family.

Step 14 Under the **Family** column in the list of devices in the main repository window, locate the Catalyst 9800-40 Wireless Controllers and expand the list of available images for the device.

You should now see the new image you just uploaded in the list of images available for the device family.

Step 15 Click the star for **Golden Image** to mark the image as the preferred one for the Catalyst 9800-40 Wireless Controller platform.

Figure 70: Mark Golden Image


Global
Design / Image Repository / Image Family
Image Repository
Cisco Catalyst 9800-40 Wireless Controller
Images (6)

Clicking on the star symbol against the image of choice will mark it as Golden image

Repeat the entire procedure for the Catalyst 9800-CL guest Wireless Controller (WLC-9800-CL). For this deployment guide, the Catalyst 9800-CL guest Wireless Controller upload image name is C9800-CL-universalk9.17.09.04a.SPA.bin.

Update the Software Image for the Cisco Catalyst 9800-CL Wireless Controller

This section outlines the procedure for updating the wireless controller image after the image is marked as golden.

Use Software Image Management (SWIM) to Update the Catalyst 9800 Series Wireless Controller Software

This process is used for the following purposes:

- Distribute (download) the software image from the Cisco DNA Center image repository to the wireless controllers.
- Upgrade the software images running on the wireless controllers.

Both steps can be run immediately, or the steps can be scheduled to run at a specified date and time to comply with existing network change schedules.

Cisco DNA Center runs a compliance check, which compares the devices in the inventory with images marked as a golden images. Devices that are out of compliance with the golden image are marked as **Outdated** in the inventory. Before you can update an image to the version marked as golden, the inventory collection must be successfully completed, and the device must be in a **Managed** state.

The following procedures are included in this process:

- Upgrade the software images for the Catalyst 9800-40 Wireless Controllers.
- Upgrade the software image for the Catalyst 9800-CL Wireless Controller.

Upgrade the Software Image for the Cisco Catalyst 9800-40 Wireless Controllers

The following procedure explains how to upgrade the software images for the Cisco Catalyst 9800-40 Wireless Controllers (WLC-9800-1 and WLC-9800-2).

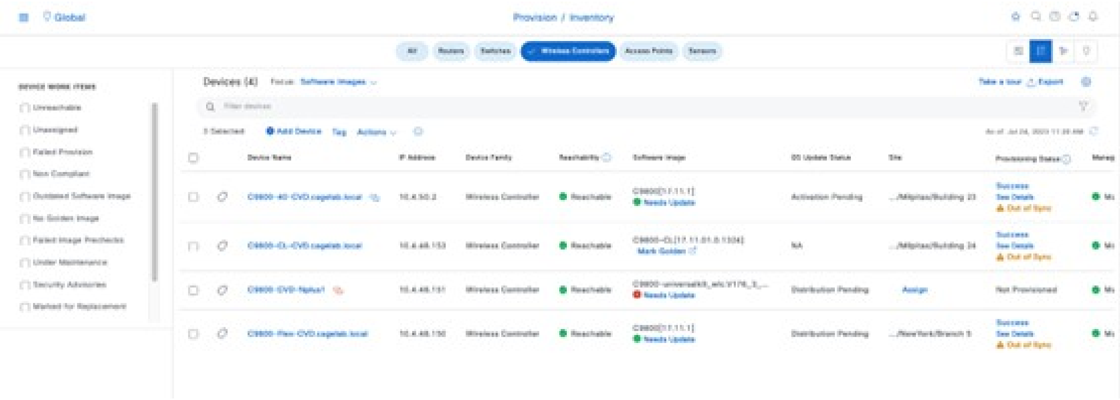
Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

Step 2 From the **Focus** drop-down list, choose **Software Images**.

The window displays the software image running on each device in the inventory.

Figure 71: Inventory Window



	Device Name	IP Address	Device Family	Reachability	Software Image	OS Update Status	Site	Provisioning Status	Manag
□	C9800-40-CVD.cagelab.local	10.4.50.2	Wireless Controller	● Reachable	C9800[17.11.1] ● Needs Update	Activation Pending	.../Milpitas/Building 23	Success See Details ⚠ Out of Sync	● M
□	C9800-CL-CVD.cagelab.local	10.4.48.153	Wireless Controller	● Reachable	C9800-CL[17.11.01.0.1324] Mark Golden	NA	.../Milpitas/Building 24	Success See Details ⚠ Out of Sync	● M
□	C9800-CVD-Nplus1	10.4.48.151	Wireless Controller	● Reachable	C9800-universalk9_wlc.V176_1_... ● Needs Update	Distribution Pending	Assign	Not Provisioned	● M
□	C9800-Flex-CVD.cagelab.local	10.4.48.150	Wireless Controller	● Reachable	C9800[17.11.1] ● Needs Update	Distribution Pending	.../NewYork/Branch 5	Success See Details ⚠ Out of Sync	● M

Step 3 From the list of devices, locate one of the Catalyst 9800-40 Wireless Controllers (WLC-9800-1 or WLC-9800-2).

Step 4 Under the **Software Image** column for the Catalyst 9800-40 Wireless Controller, click **Needs Update**.

The **Image Update Readiness Check** slide-in pane is displayed.

Figure 72: Image Update Readiness Check Window

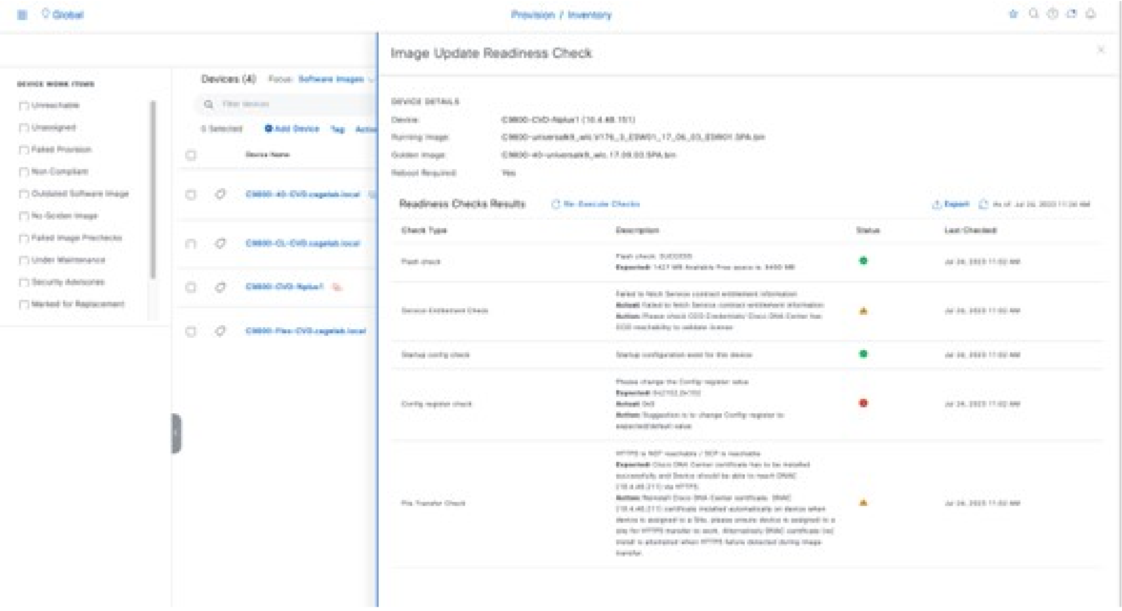


Image Update Readiness Check

DEVICE DETAILS

Device: C9800-CVD-Nplus1 (10.4.48.151)

Running Image: C9800-universalk9_wlc.V176_3_ESW01_17_06_03_ESW01.SPA.bin

Golden Image: C9800-40-universalk9_wlc.17.09.03.SPA.bin

Reboot Required: Yes

Readiness Checks Results Re-Execute Checks Export As of: Jul 26, 2023 11:26 AM

Check Type	Description	Status	Last Checked
Flash check	Flash check: SUCCESS **Expected:** 1427 MB Available Free space is: 8450 MB	●	Jul 26, 2023 11:02 AM
Service Entitlement Check	Failed to fetch Service contract entitlement information **Actual:** Failed to fetch Service contract entitlement information **Action:** Please check CCO Credentials/ Cisco DNA Center has CCO reachability to validate license	▲	Jul 26, 2023 11:02 AM
Startup config check	Startup configuration exist for the device	●	Jul 26, 2023 11:02 AM
Config register check	Please change the Config register value **Expected:** 0x2102,0x102 **Actual:** 0x0 **Action:** Suggestion is to change Config register to expected/default value	●	Jul 26, 2023 11:02 AM
File Transfer Check	HTTPS is NOT reachable / SCP is reachable **Expected:** Cisco DNA Center certificate has to be installed successfully and Device should be able to reach DNAC (10.4.48.211) via HTTPS. **Action:** Reinstall Cisco DNA Center certificate. DNAC (10.4.48.211) certificate installed automatically on device when device is assigned to a Site, please ensure device is assigned to a site for HTTPS transfer to work. Alternatively DNAC certificate (re) install is attempted when HTTPS failure detected during image transfer.	▲	Jul 26, 2023 11:02 AM

Ensure that the **Status** column shows either a green icon indicating success or a yellow icon indicating a warning. If any of the checks show a red icon indicating failure, the image on the platform was not upgraded. In this deployment guide, the **Config register check** shows a red icon because the config register value needs to be 0x2102 or 0x102, but the device is using a value of 0x0.

If necessary, correct any issues on the wireless controller which result in a failure.

Step 5 Click **Re-Execute Check** to rerun the readiness assessment.

> **Note** Configuring a time zone in IOS XE devices through the `clock timezone` IOS CLI command may cause a warning to appear in the **Image Update Readiness Check** slide-in pane, indicating that the time is significantly different between your device and Cisco DNA Center. You may be able to clear this warning by removing the `clock timezone` command from the device, resyncing the device in the inventory, and clicking **Re-Execute Check** to run the readiness assessment again. As a result, the time format of the device will be displayed in UTC time rather than the local time zone.

Step 6 When you have corrected all checks which indicate a failure, close the **Image Update Readiness Check** slide-in pane.

Step 7 Repeat Step 1 through Step 6 for the other Catalyst 9800-40 Wireless Controller.

Step 8 Check the check boxes for both of the Catalyst 9800-40 Wireless Controllers (Wireless Controller-9800-1 and Wireless Controller-9800-2).

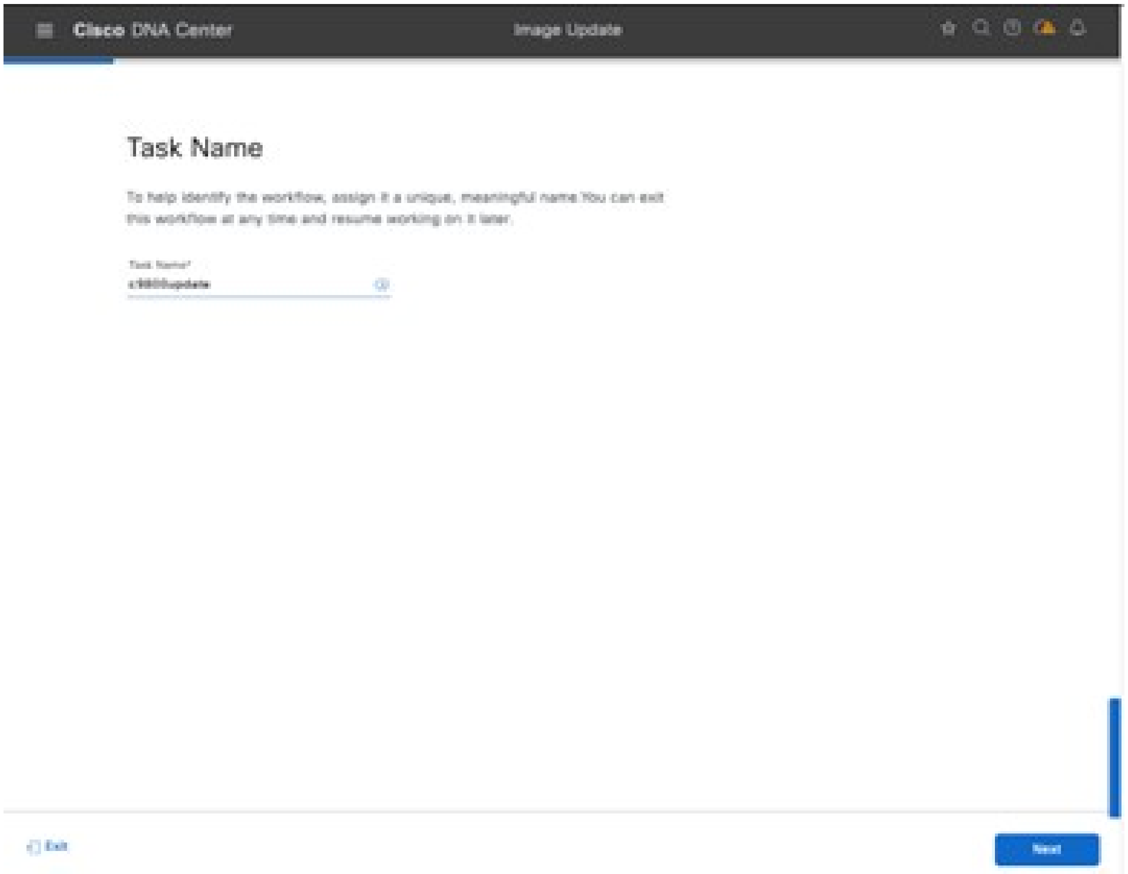
Step 9 From the **Actions** drop-down list, choose **Software Image** > **Image Update**.

The **Image Update** slide-in pane is displayed.

a) Enter a unique name in the **Task Name** field.

For this deployment guide, the name is entered as **c9800update**.

Figure 73: Enter Task Name



Task Name

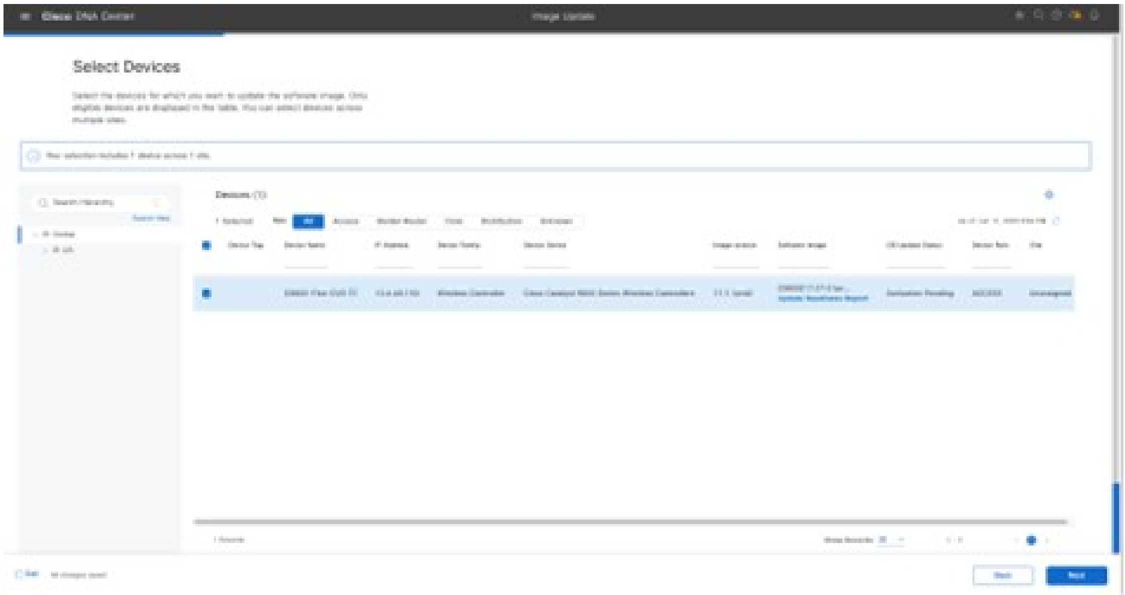
To help identify the workflow, assign it a unique, meaningful name You can exit this workflow at any time and resume working on it later.

Task Name*
c9800update

b) Click **Next**.

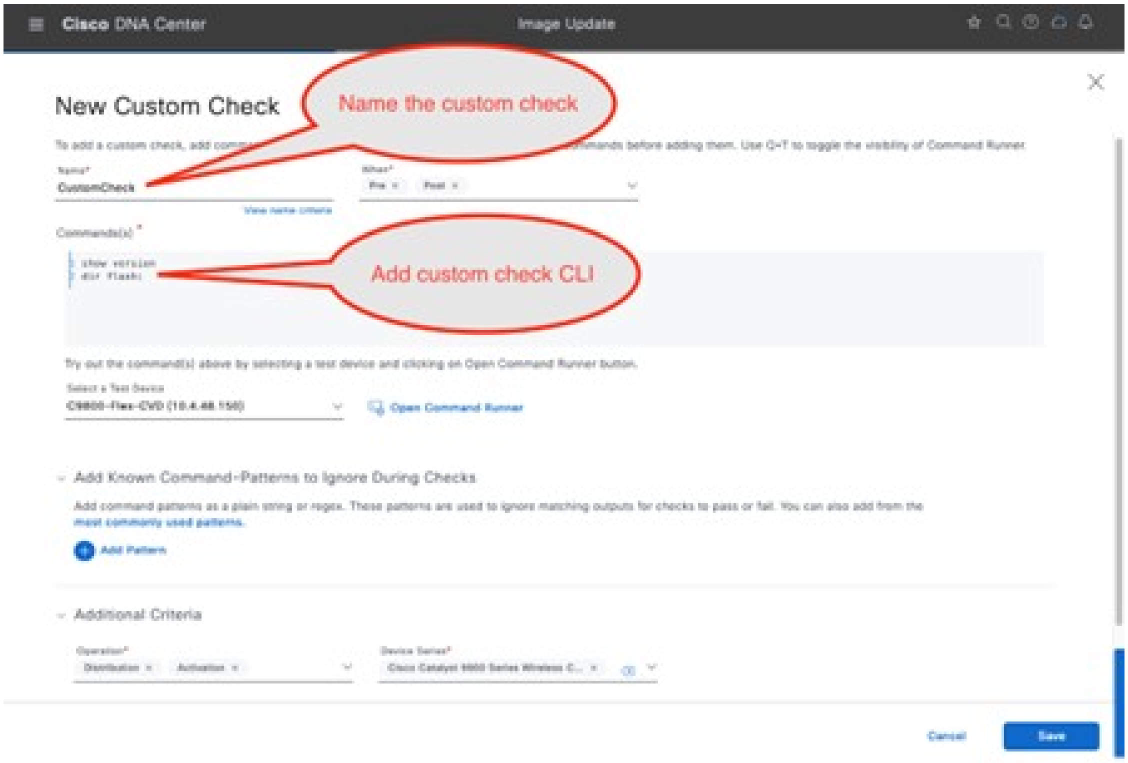
c) Check the check box for the device name to choose the device.

Figure 74: Select Devices Window



d) Click **Next** to proceed to the customized software distribution checks.

Figure 75: Custom Distribution Check



New Custom Check

To add a custom check, add comm… ommands before adding them. Use Q+T to toggle the visibility of Command Runner.

Name*: CustomCheck

When*: Pre × Post ×

View name criteria

Commands(s) *

```
show version
dir flash:
```

Try out the command(s) above by selecting a test device and clicking on Open Command Runner button.

Select a Test Device: C9800-Flex-CVD (10.4.48.150)

Add Known Command-Patterns to Ignore During Checks

Add command patterns as a plain string or regex. These patterns are used to ignore matching outputs for checks to pass or fail. You can also add from the most commonly used patterns.

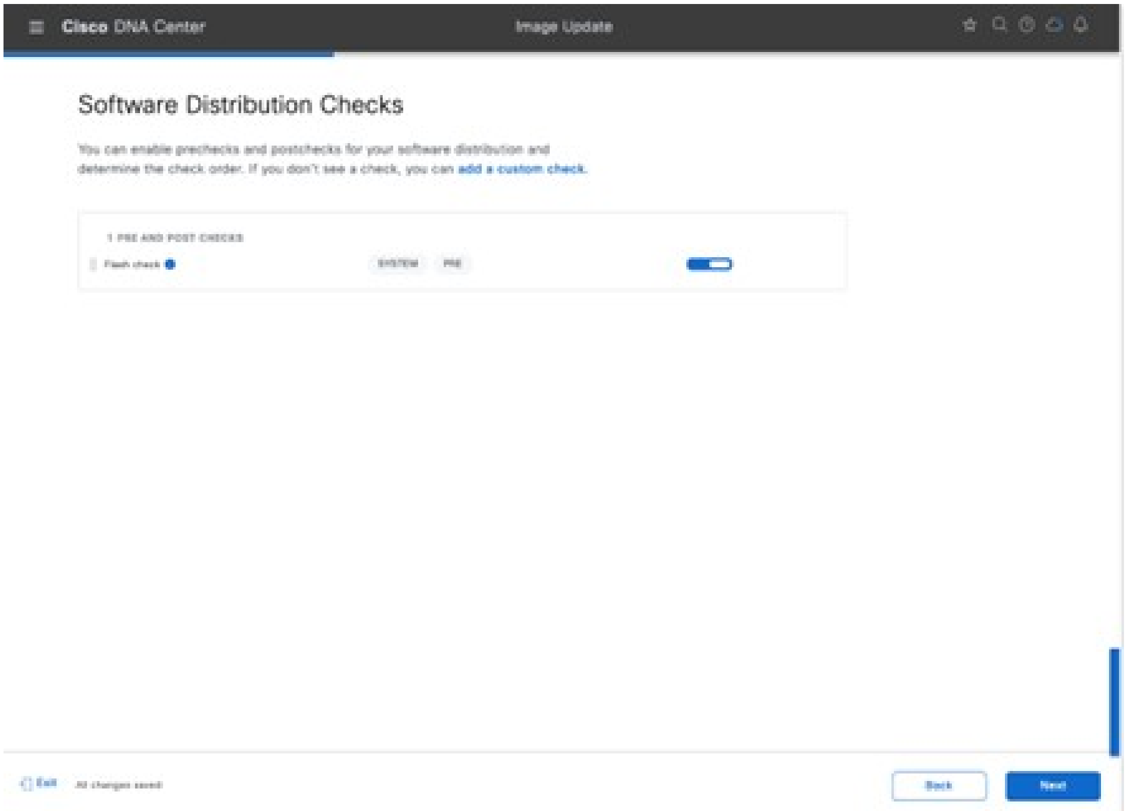
Additional Criteria

Operation*: Distribution × Activation ×

Device Series*: Cisco Catalyst 9800 Series Wireless C… ×

e) If customization is not needed, choosing the default **Flash check** is optional.

Figure 76: Update Image Distribution



Software Distribution Checks

You can enable prechecks and postchecks for your software distribution and determine the check order. If you don't see a check, you can add a custom check.

1 PRE AND POST CHECKS

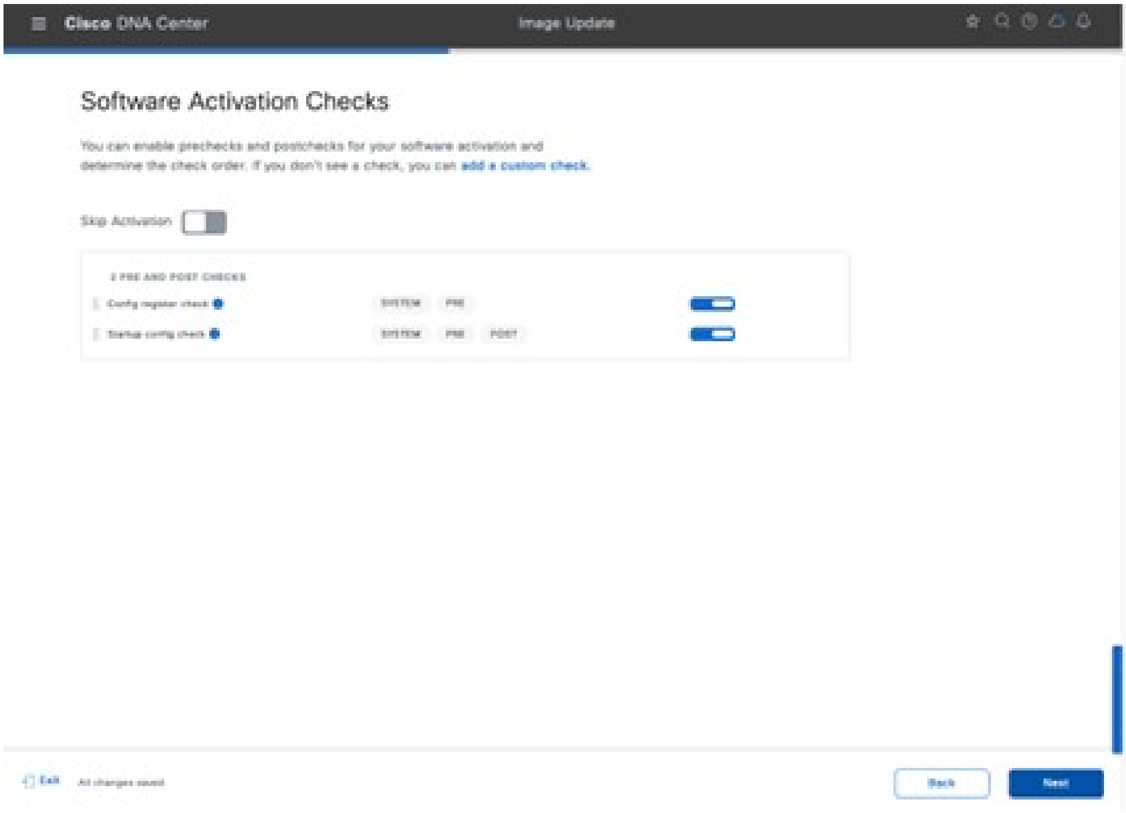
Flash check SYSTEM PRE

f) Click **Next** to proceed to **Software Activation Checks**. By default, **Config register check** and **Startup config check** are chosen.

g) Click **Add a custom check** to add additional custom checks.

For this guide, only the default checks are chosen.

Figure 77: Software Activation Checks



Software Activation Checks

You can enable prechecks and postchecks for your software activation and determine the check order. If you don't see a check, you can add a custom check.

Skip Activation

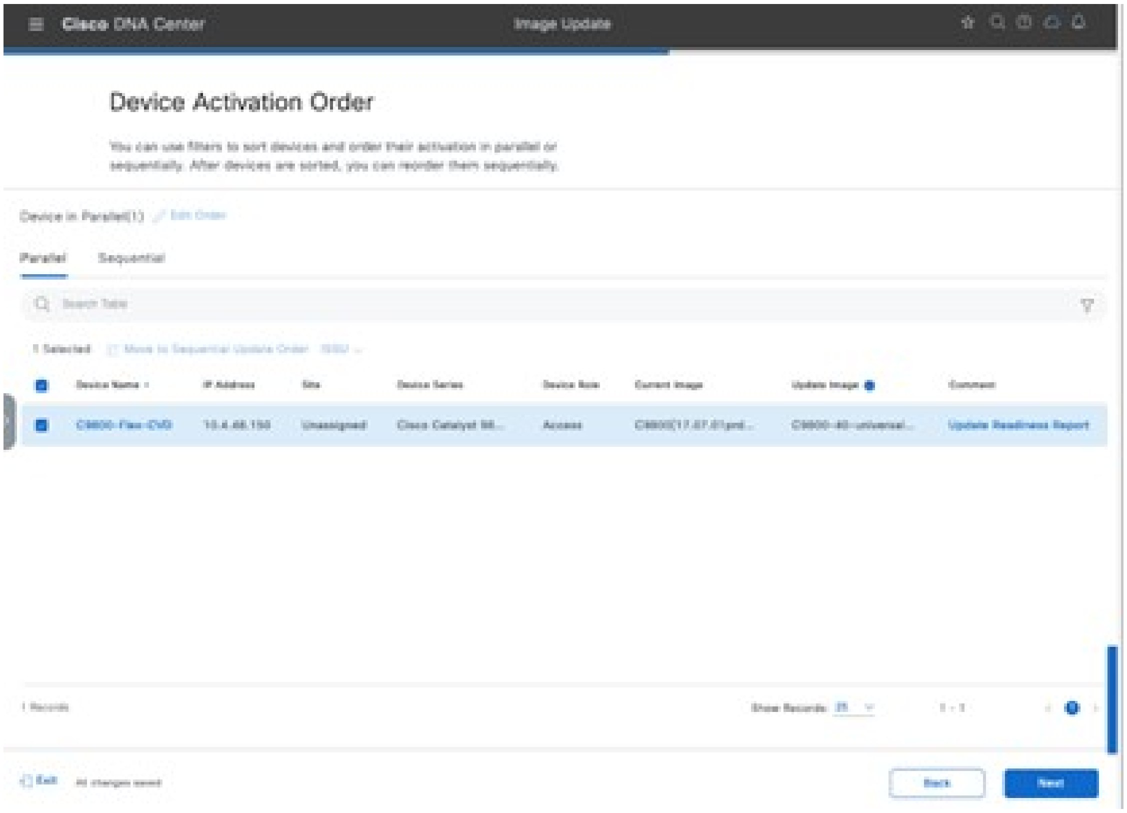
2 PRE AND POST CHECKS

Config register check	SYSTEM	PRE		
Startup config check	SYSTEM	PRE	POST	

h) Click **Next** and choose the **Device Activation order** if there is more than one device.

For this guide, there is only one device, so only that device is chosen.

Figure 78: Device Activation Order



Device Activation Order

You can use filters to sort devices and order their activation in parallel or sequentially. After devices are sorted, you can reorder them sequentially.

Device in Parallel(1) Edit Order

1 Selected Move to Sequential Update Order ISSU

☑	Device Name	IP Address	Site	Device Series	Device Role	Current Image	Update Image	Comment
☑	C9800-Flex-CVD	10.4.48.150	Unassigned	Cisco Catalyst 98...	Access	C9800(17.07.01prd...	C9800-40-universal...	Update Readiness Report

1 Records Show Records: 25 1 - 1

i) Click **Next** to schedule the distribution and activation for a later time. To execute the distribution and activation immediately, click **Now**.

If the software has not been distributed (downloaded from the Cisco DNA Center repository to the wireless controllers) you cannot choose the **Now** option. However, you can schedule the software to be activated immediately after the software distribution is complete, or you can schedule the software activation for a later date and time. If you schedule the activation time to be too close to the distribution time, you will receive a warning that the update may fail because the distribution of the image to the devices may not complete before the scheduled activation time.

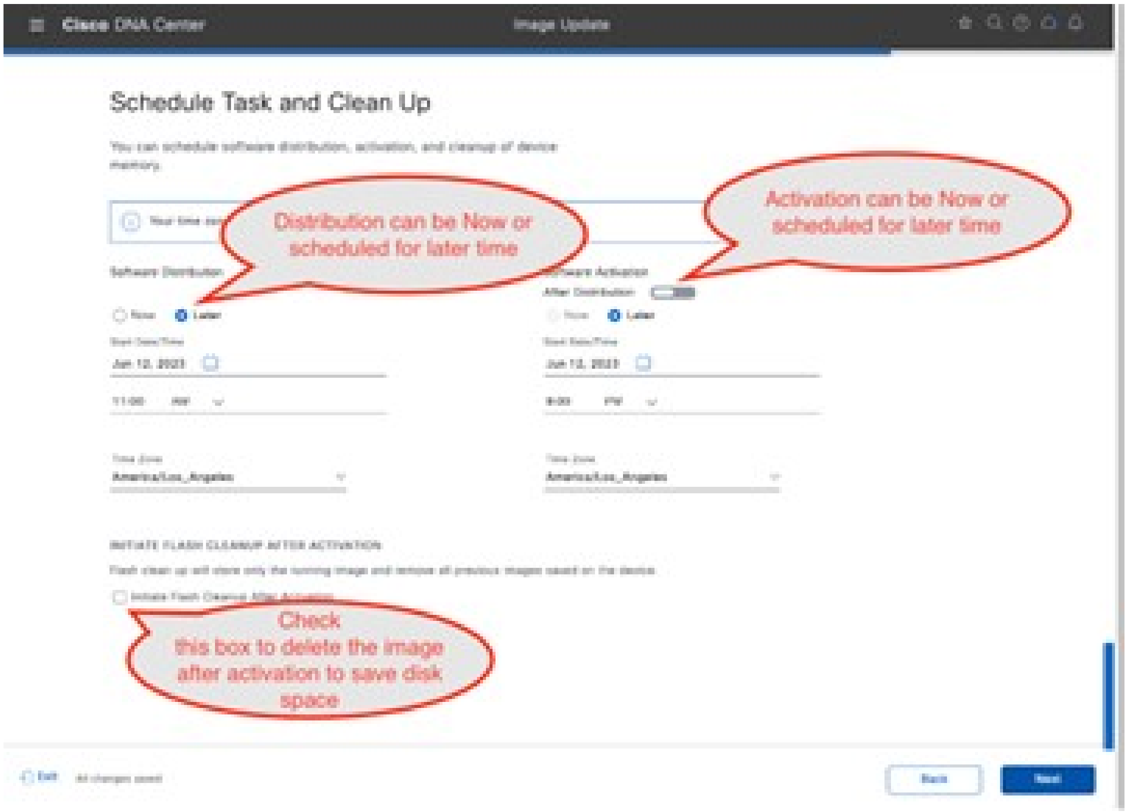
Note It is always recommended to upgrade software images only during scheduled network operations change windows.

Step 10 Enable **Software Activation After Distribution**.

Alternatively, click the **Later** radio button and adjust the date and time for the image distribution.

Enabling **Software Activation After Distribution** will activate the image immediately after it is distributed. This action combines the download and activation of the image into a single scheduled process, rather than scheduling download and activation separately.

Figure 79: Distribution and Activation Window



Schedule Task and Clean Up

You can schedule software distribution, activation, and cleanup of device memory.

Your time zo

Software Distribution

○ Now ● Later

Start Date/Time

Jun 12, 2023

11:00 AM

Time Zone

America/Los_Angeles

Software Activation

After Distribution

○ Now ● Later

Start Date/Time

Jun 12, 2023

9:00 PM

Time Zone

America/Los_Angeles

INITIATE FLASH CLEANUP AFTER ACTIVATION

Flash clean up will store only the running image and remove all previous images saved on the device.

□ Initiate Flash Cleanup After Activation

All changes saved

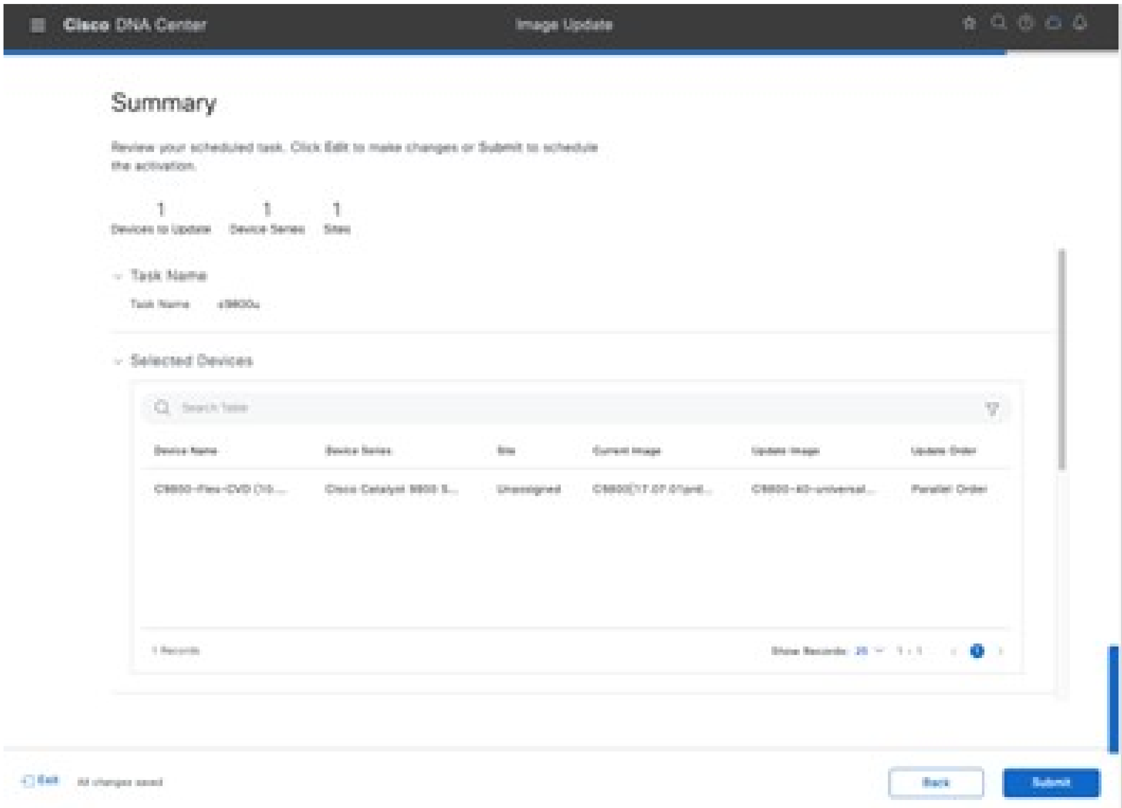
Distribution can be Now or scheduled for later time

Activation can be Now or scheduled for later time

Check this box to delete the image after activation to save disk space

a) Click **Next** to proceed to the **Summary** window and review your selections before submitting the task to update the device image.

Figure 80: Review Summary Before Submitting Upgrade Task



Cisco DNA Center

Image Update

Summary

Review your scheduled task. Click Edit to make changes or Submit to schedule the activation.

1 Devices to Update

1 Device Series

1 Sites

Task Name

Task Name c9800u

Selected Devices

Device Name	Device Series	Site	Current Image	Update Image	Update Order
C9800-Flex-CVD (10....	Cisco Catalyst 9800 S...	Unassigned	C9800[17.07.01prd...	C9800-40-universal...	Parallel Order

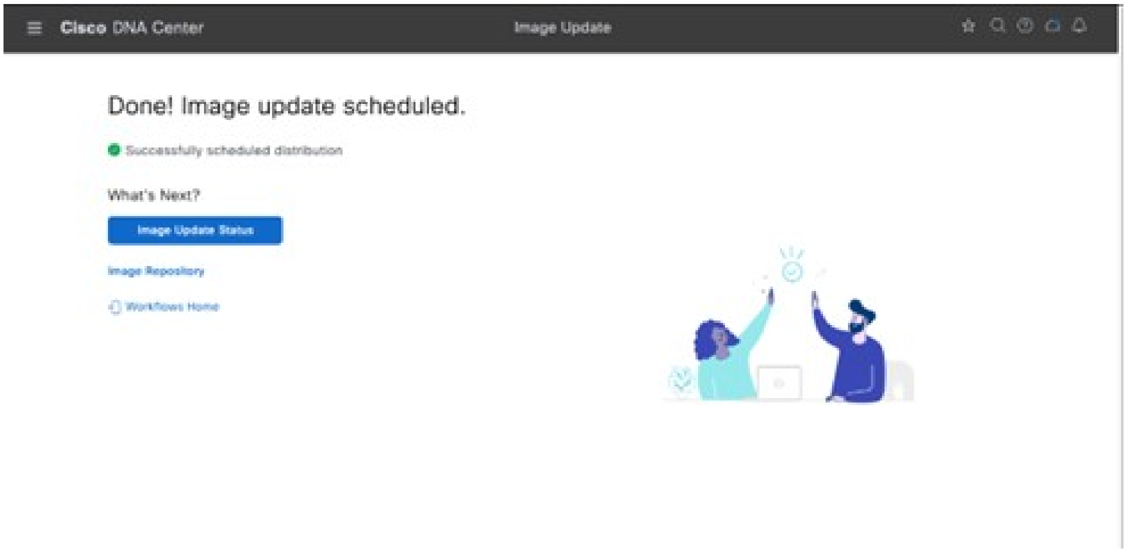
1 Records

Show Records: 25 1 - 1

b) Click **Submit**.

The status window is displayed, showing the progress of the update.

Figure 81: Image Update Status



Cisco DNA Center

Image Update

Done! Image update scheduled.

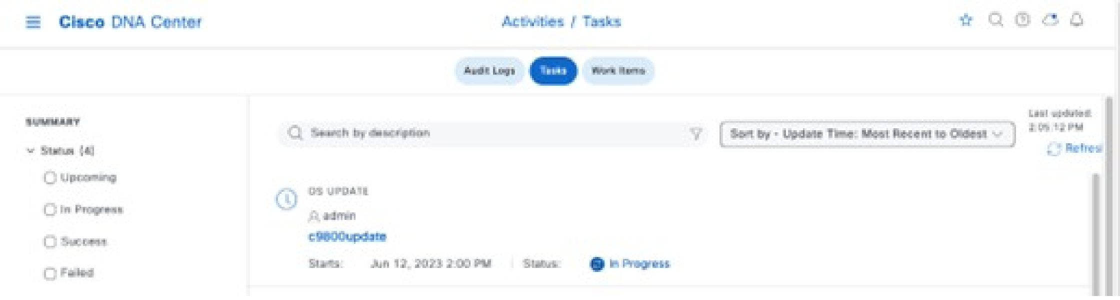
● Successfully scheduled distribution

What's Next?

Step 11 Click **Image Update Status**, which takes you to the update progress window.

Alternatively, click the menu icon and choose **Activities** > **Tasks**. The scheduled task window is displayed.

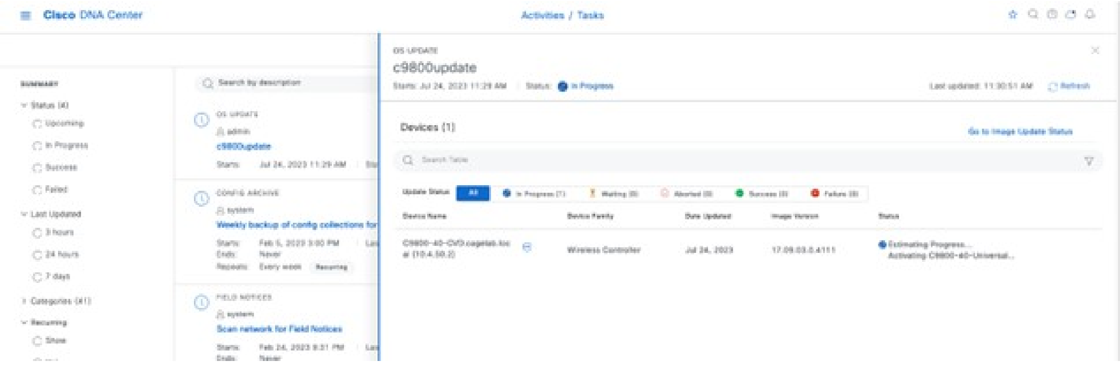
Figure 82: Scheduled Tasks Window



OS UPDATE
admin
c9800update
Starts: Jun 12, 2023 2:00 PM | Status: In Progress

You can expand the task to see the details regarding the distribution and activation of the image.

Figure 83: Operating System Update in Progress



OS UPDATE
admin
c9800update
Starts: Jul 24, 2023 11:29 AM

CONFIG ARCHIVE
system
Weekly backup of config collections for
Starts: Feb 6, 2023 3:00 PM
Ends: Never
Repeats: Every week Recurring

FIELD NOTICES
system
Scan network for Field Notices
Starts: Feb 24, 2023 8:31 PM
Ends: Never

OS UPDATE
c9800update
Starts: Jul 24, 2023 11:29 AM | Status: In Progress
Last updated: 11:30:51 AM

Device Name	Device Family	Date Updated	Image Version	Status
C9800-40-CVD.cagelab.local (10.4.50.2)	Wireless Controller	Jul 24, 2023	17.09.03.0.4111	Estimating Progress... Activating C9800-40-Universal...

On successful completion of the task, an icon is displayed next to the task, indicating that the update was successful. Again, you can expand the task to see the details regarding the distribution and activation of the image.

Step 12 Close the scheduled tasks slide-in pane.

Step 13 From the top-left corner, click the menu icon and choose **Provision** > **Inventory** to go back to the inventory list in the main provisioning window.

The image for the Catalyst 9800-40 Wireless Controller now shows that it has updated to the chosen IOS version.

Repeat the entire procedure for the Catalyst 9800-CL Guest Wireless Controller (Cisco Catalyst 9800 Series Wireless Controller-CL).

Configure HA SSO on the Cisco Catalyst 9800-40 Enterprise Wireless Controllers

Cisco Catalyst 9800 Series Wireless Controllers support the ability to be configured in an active or standby high availability (HA) stateful switch-over (SSO) pair. Cisco DNA Center supports the ability to take two controllers of the same model, running the same operating system version, and configure them as an HA SSO pair.

Note

- Before you turn on HA SSO, the RP ports are connected, either directly or through a dedicated L2 network. You can connect either the fiber SFP or Ethernet RJ-45 port. The fiber SFP HA connectivity takes priority over RJ-45. If SFP is connected when RJ-45 HA is up and running, the HA pair reloads.
- When connecting the RP ports directly, back-to-back, Cisco recommends using a copper cable with a length less than 30 meters (100 feet). If you need to go beyond 30 meters (100 feet), it is recommended to connect the RP ports using a fiber cable.
- Both the boxes are running the same software and are in the same boot mode (install mode is the recommended boot mode).
- For physical appliances, use the same hardware type (for example, you cannot pair a C9800-L-C with a C9800-L-F).
- For the Catalyst 9800-CL Wireless Controller, pick the same scale template (large, medium, or small) on both virtual machines.
- Before forming an HA pair, it is recommended to delete the existing certificates and keys in each of the Catalyst 9800 Series Wireless Controllers that were previously deployed as standalone. Doing this avoids the risk of the same trustpoint being present on both wireless controllers with different keys, which would cause issues after a switchover.
- Set the keep-alive retries to 5 (the default for release 17.1).
- Set the higher priority (2) on the chassis that you want to be the active wireless controller.

The following steps explain how to configure the Catalyst 9800-40 Wireless Controllers (WLC-9800-1 and WLC-9800-2) as an HA SSO pair.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The main provisioning window displays the devices. By default, the **Focus** is set for **Inventory**.

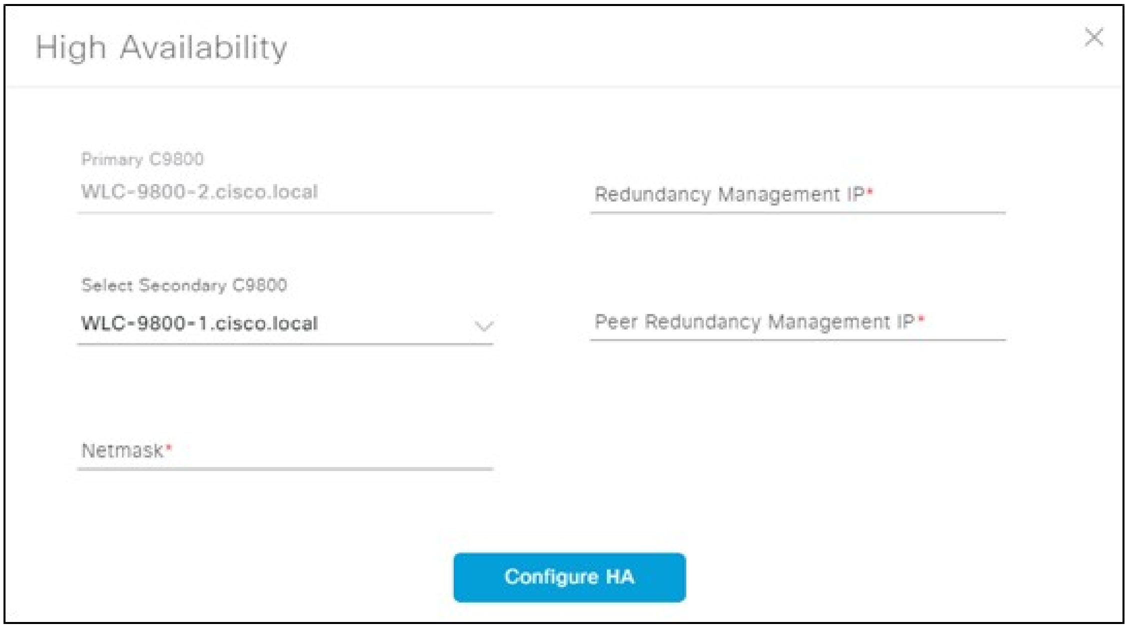
Step 2 Locate and check the check box for the Catalyst 9800-40 Wireless Controller which will be the primary wireless controller of the HA SSO wireless controller pair.

For this design and deployment guide, **WLC-9800-2** was selected as the primary wireless controller.

Step 3 From the **Actions** drop-down list, select **Provision** > **Configure WLC HA**.

The **High Availability** slide-in pane is displayed.

Figure 84: High Availability Window



High Availability

Primary C9800
WLC-9800-2.cisco.local

Redundancy Management IP*

Select Secondary C9800
WLC-9800-1.cisco.local

Peer Redundancy Management IP*

Netmask*

Step 4 Enter the required information in the respective fields and click **Configure HA**.

The following table shows the high availability information for this deployment guide:

Table 21: High Availability Settings

Field	Value
Primary Cisco Catalyst 9800 Series Wireless Controller	WLC-9800-1.cisco.local
Redundancy Management IP	`10.4.174.132`
Select Secondary Cisco Catalyst 9800 Series Wireless Controller	WLC-9800-2.cisco.local
Peer Redundancy Management IP	`10.4.174.134`
Netmask	24

Note The **Redundancy Management IP** and the **Peer Redundancy Management IP** addresses must be in the same IP subnet as the wireless management interface.

A dialog box is displayed, notifying you that the wireless controllers will be rebooted when they are placed in the high availability mode.

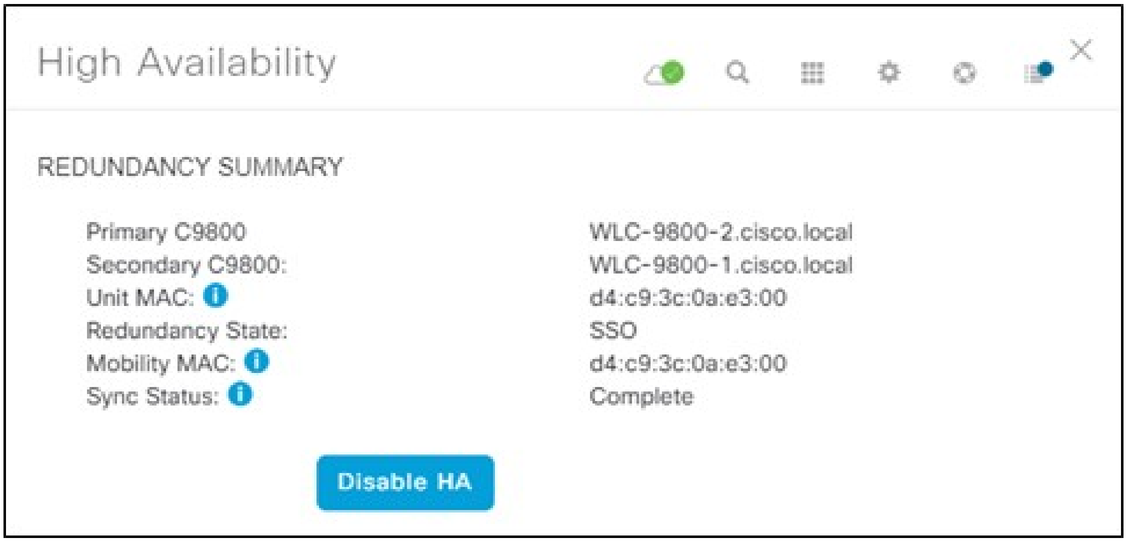
Step 5 Click **OK** to accept and put the two Catalyst 9800-40 Wireless Controllers in HA SSO mode.

It will take several minutes for the wireless controllers to reboot and display in HA SSO mode. All configurations from the primary Catalyst 9800-40 Wireless Controller, including the IP address of the management interface, will be copied to the secondary Catalyst 9800-40 Wireless Controller. Cisco DNA Center will no longer show two wireless controllers in the inventory. Instead, only a single Wireless Controller HA SSO pair with two serial numbers will appear in the inventory.

For this deployment guide, the wireless controller HA SSO pair is WLC-9800-2.

Step 6 If you choose the wireless controller (WLC-9800-2), and from the **Actions** drop-down list, choose **Provision** > **Configure WLC HA**, you can see additional information about the Catalyst 9800-40 Wireless Controller HA SSO pair.

Figure 85: Catalyst 9800-40 Wireless Controller HA SSO Pair Details



High Availability

REDUNDANCY SUMMARY

Primary C9800	WLC-9800-2.cisco.local
Secondary C9800:	WLC-9800-1.cisco.local
Unit MAC:	d4:c9:3c:0a:e3:00
Redundancy State:	SSO
Mobility MAC:	d4:c9:3c:0a:e3:00
Sync Status:	Complete

Note If you click **Disable HA**, both Catalyst 9800-40 Wireless Controllers will revert to standalone mode, with the secondary wireless controller reset to factory settings. It is recommended that you establish console access to the wireless controllers before disabling HA. You will need to change the IP address and hostname of one of the wireless controllers to rediscover the controller in Cisco DNA Center after disabling HA.

Provision the Cisco Catalyst 9800-40 Enterprise Wireless Controller HA SSO Pair

The following steps explain how to provision the corporate wireless profile to the Cisco Catalyst 9800-40 enterprise Wireless Controller HA SSO pair, known as Cisco Catalyst 9800-40-CVD.cagelab.local.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The main provisioning window displays the devices in the inventory. By default, **Inventory** is chosen from the **Focus** drop-down list.

Step 2 Locate and check the check box for **C9800-40-CVD.cagelab.local**.

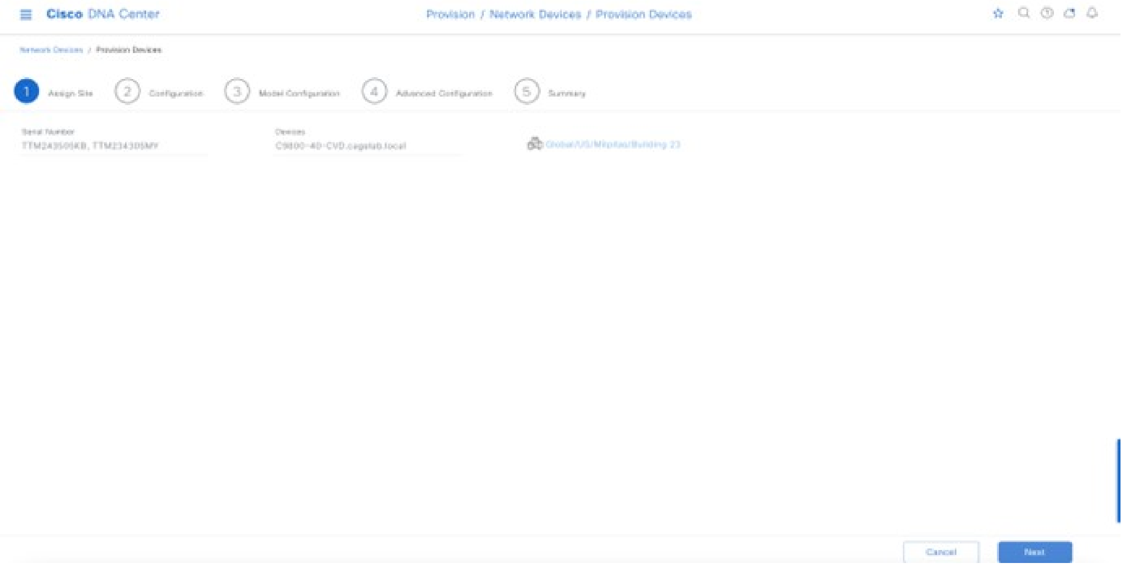
Step 3 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

You are taken through a four-step workflow for provisioning the enterprise wireless controller HA SSO pair (C9800-40-CVD.cagelab.local), starting with **Assign Site**.

Step 4 In the **Assign Site** window, click **Choose a Site**. A slide-in pane is displayed, which shows the site hierarchy configured for Cisco DNA Center.

For this deployment guide, the enterprise wireless controller HA SSO pair (**C9800-40-CVD.cagelab.local**) is assigned to the building level.

Step 5 Expand the site hierarchy for **Milpitas** and choose **Building 23**.



Serial Number: TTM243505KB, TTM234305MY

Devices: C9800-40-CVD.cagelab.local

Global/US/Milpitas/Building 23

Figure 86: Assign Site to Building Level

Note

- The enterprise wireless controller HA SSO pair (**C9800-40-CVD.cagelab.local**) must be assigned to a building or floor within the Cisco DNA Center site hierarchy. It cannot be assigned to Milpitas area or to the global level of the site hierarchy, even though **C9800-40-CVD.cagelab.local** is assigned to **Building 23** in this deployment guide. APs located on floors in other buildings are supported by the wireless controller.
- When the wireless controller is assigned to a site, the wireless controller is added as a device to Cisco ISE.

Step 6 Click **Save** to assign **C9800-40-CVD.cagelab.local** to **Building 23**.

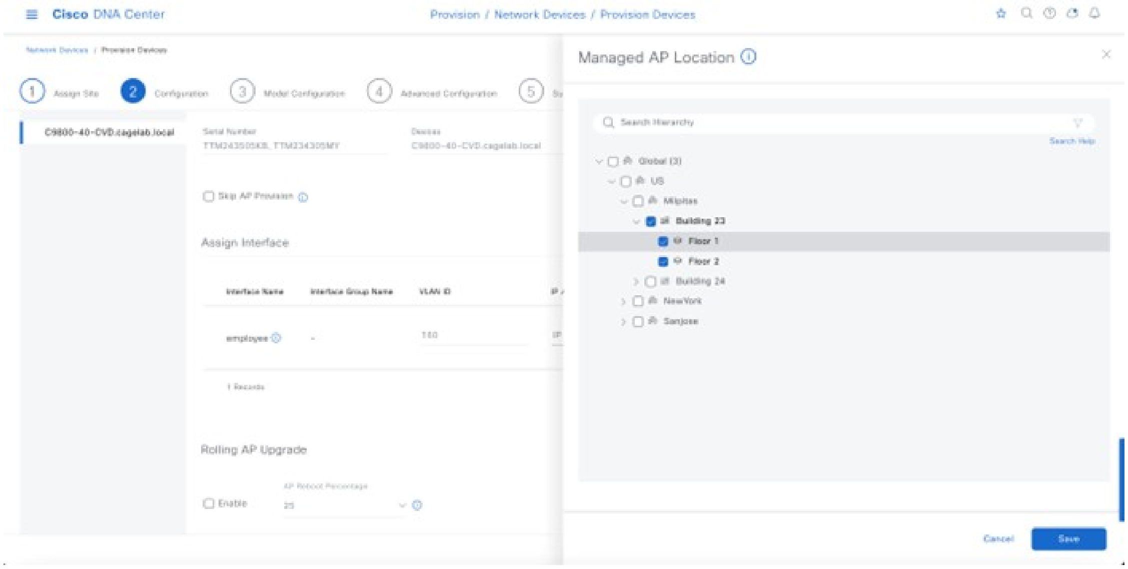
Step 7 Click **Next**.

The **Configuration** window is displayed.

Step 8 In the **Configuration** window, choose **Active Main** for the wireless controller **Role**.

Step 9 Click **Select Primary Managed AP locations**.

The **Managed AP Location** slide-in pane is displayed, showing the site hierarchy for Cisco DNA Center.



C9800-40-CVD.cagelab.local

Serial Number: TTM243505KB, TTM234305MY

Devices: C9800-40-CVD.cagelab.local

□ Skip AP Provision

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP A
employee	-	160	IP

1 Records

Rolling AP Upgrade

□ Enable   AP Reboot Percentage: 25

- □ Global (3)
  - □ US
    - □ Milpitas
      - ☑ Building 23
        - ☑ Floor 1
        - ☑ Floor 2
      - □ Building 24
    - □ NewYork
    - □ Sanjose

Cisco DNA Center supports the ability to configure N+1 redundancy for APs and HA SSO for a wireless controller. As a result, you can configure both primary and secondary managed AP locations. Primary managed AP locations are sites that include buildings and/or floors, where the wireless controller will serve as the primary wireless controller within the AP high availability configuration. Secondary managed AP locations are sites where the wireless controller will serve as the secondary wireless controller within the AP high availability configuration. If the primary wireless controller or wireless controller HA SSO pair fail, APs will reestablish CAPWAP connections to the wireless controller.

For this guide, the Catalyst 9800-40 Wireless Controller HA SSO pair (**C9800-40-CVD.cagelab.local**) will be the primary wireless controller, managing APs on **Floors 1** and **Floor 2** of **Building 23** and **Building 24**. No secondary managed AP locations will be configured because the wireless controller HA SSO pair already provides redundancy in a campus network, where all the APs are operating in a centralized mode deployment.

Step 10 Expand the site hierarchy and choose **Floors 1** and **Floor 2** for **Building 23** and **Floors 1** and **Floor 2** for **Building 24**.

Step 11 Click **Save**.

Because you have selected this wireless controller to be an Active Main wireless controller, additional fields are displayed. The corporate wireless profile has defined the enterprise SSID as **lab3employee** and the wireless interface on which the SSID terminates as **employee on VLAN ID 160**, so this enterprise SSID and wireless interface will be automatically displayed. Likewise, because the corporate wireless profile has defined the guest SSID as **lab3guest** and the wireless interface on which the SSID terminates as **guest-dmz on VLAN ID 125**, this information will also be automatically displayed.

Step 12 Enter the values for IP address, Gateway IP address, LAG/Port Number, and Subnet Mask (in bits) for each SSID.

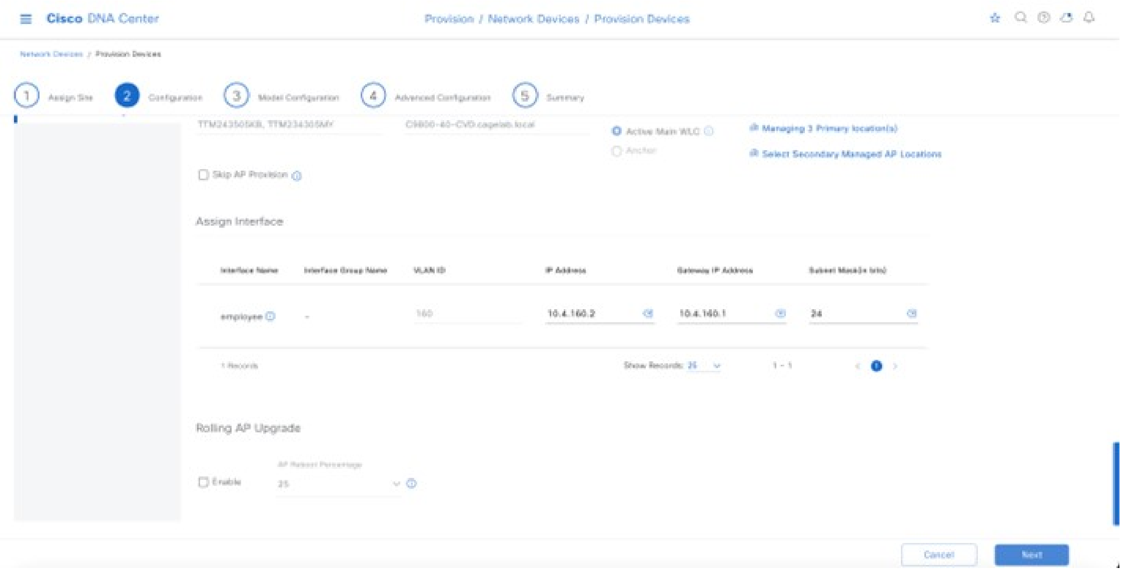
The following table shows the values entered for this deployment guide.

Table 22: Enterprise Wireless Controller Settings

Field	Value
SSID Name	lab3employee
Interface Name	employee
VLAN ID	160

Field	Value
IP Address	10.4.160.2
Gateway IP Address	10.4.160.1
LAG/Port Number	1
Subnet Mask (in bits)	24
SSID Name	lab3guest
Interface Name	Guest-dmz
VLAN ID	125
IP Address	10.4.125.2
Gateway IP Address	10.4.125.1
LAG/Port Number	1
Subnet Mask (in bits)	24

Figure 87: Enterprise Wireless Controller Settings in Cisco DNA Center



TTM2435050KB, TTM234305MY C9800-40-CVD.cagelab.local

● Active Main WLC
○ Anchor

Managing 3 Primary location(s)

Select Secondary Managed AP Locations

☐ Skip AP Provision

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
employee	-	160	10.4.160.2	10.4.160.1	24

1 Records Show Records: 25 1 - 1

Rolling AP Upgrade

☐ Enable AP Reboot Percentage 25

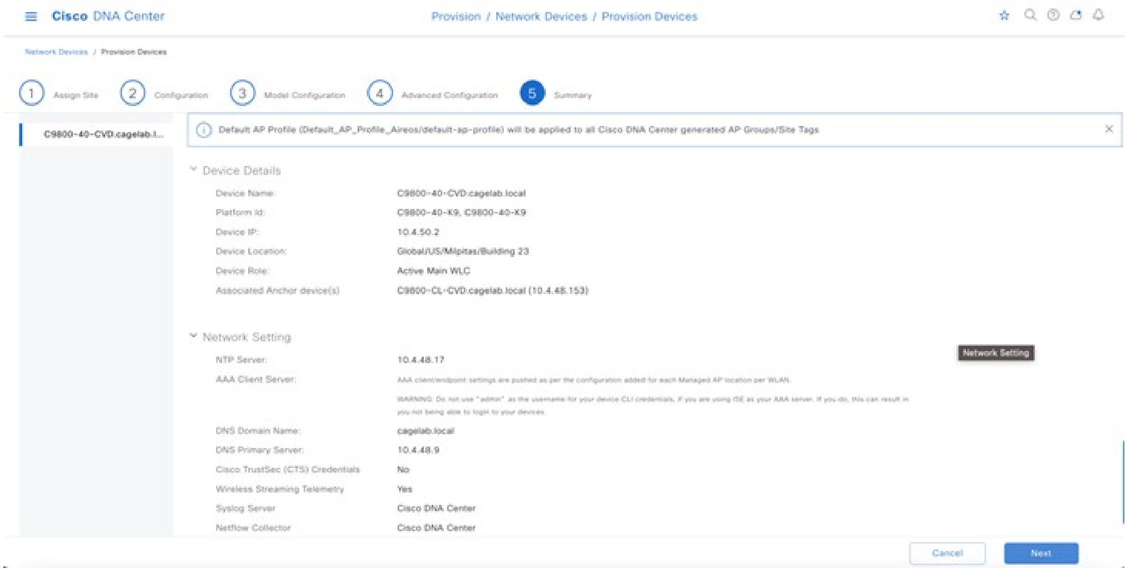
Note The guest-dmz interface is defined on the enterprise foreign wireless controller. When the anchor tunnel is up between the enterprise foreign wireless controller and the guest anchor wireless controller, guest wireless traffic is automatically terminated on the guest-dmz interface of the guest anchor wireless controller. However, if the anchor tunnel is down, guest wireless traffic is terminated on the guest-dmz interface of the enterprise foreign wireless controller. It is a best practice to specify an isolated Layer 2 VLAN for the guest-dmz interface on the enterprise foreign wireless controller, with no DHCP server to supply IP addresses to guest wireless devices. By doing so, if the anchor tunnel is down, guest wireless devices are isolated to a Layer 2 subnet with no network access.

Step 13 Click **Next**.

The **Advanced Configuration** window is displayed. If you have configured a template within the Template Editor for the device type and the site, you can apply the template here. This deployment guide does not discuss the use of templates for advanced configuration of the Catalyst 9800-40 wireless controller HA SSO pair (**C9800-40-CVD.cagelab.local**).

Step 14 Click **Next**.

The **Summary** window is displayed. This window provides a summary of the configuration which will be provisioned to the Catalyst 9800-40 Wireless Controller HA SSO pair (WLC-9800-2). You can expand each section to see the details of the configuration, which is based on the corporate wireless profile created in the *Design the wireless network* section of this deployment guide.



Default AP Profile (Default_AP_Profile_Aireos/default-ap-profile) will be applied to all Cisco DNA Center generated AP Groups/Site Tags

Device Details

Device Name: C9800-40-CVD.cagelab.local

Platform Id: C9800-40-K9, C9800-40-K9

Device IP: 10.4.50.2

Device Location: Global/US/Milpitas/Building 23

Device Role: Active Main WLC

Associated Anchor device(s) C9800-CL-CVD.cagelab.local (10.4.48.153)

Network Setting

NTP Server: 10.4.48.17

AAA Client Server: AAA client/endpoint settings are pushed as per the configuration added for each Managed AP location per WLAN.

WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

DNS Domain Name: cagelab.local

DNS Primary Server: 10.4.48.9

Cisco TrustSec (CTS) Credentials No

Wireless Streaming Telemetry Yes

Syslog Server Cisco DNA Center

Netflow Collector Cisco DNA Center

Step 15 Click **Deploy** to deploy the configuration to the Catalyst 9800-40 Wireless Controller HA SSO pair (**C9800-40-CVD.cagelab.local**). A slide-in pane is displayed, asking if you wish to deploy the configuration now or schedule the configuration for later.

Note It is best practice to make configuration changes and provision new devices in your network only during scheduled network operation change windows.

Step 16 Click the **Now** radio button and click **Apply** to apply the configuration. You will be redirected to the **Inventory** window in **Provisioning**. The provisioning status of the device will temporarily show **Provisioning**, but the status should change to **Success** after a few minutes. Click **See Details** below the provisioning status of the device for more information.

Cisco DNA Center will dynamically create two new WLAN profiles within the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (**C9800-40-CVD.cagelab.local**). Each WLAN profile has a dynamically generated name based on the SSID name specified in the corporate wireless profile. The following table shows the names of the WLAN profiles and their respective SSIDs, automatically generated by Cisco DNA Center during the provisioning of **C9800-40-CVD.cagelab.local** for this deployment guide.

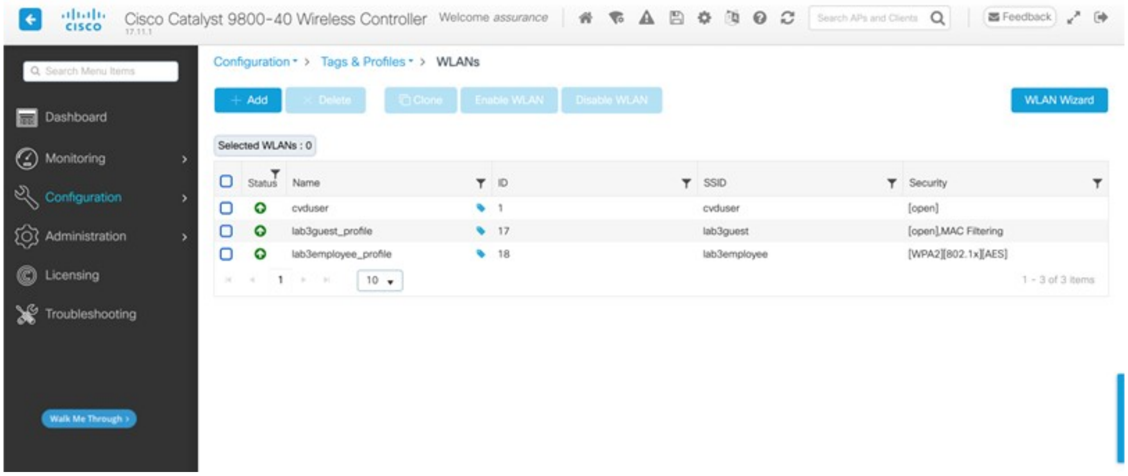
Table 23: WLAN Profiles Dynamically Generated by Cisco DNA Center

WLAN Profile Name	SSID	WLAN ID
lab3guest_profile	lab3guest	17

WLAN Profile Name	SSID	WLAN ID
lab3employee_profile	lab3employee	18

Note It is best practice to create a custom profile for a site and create policy tags with user configured profile names to make the cross-verification process easier on the wireless controller. If default profiles are used, Cisco DNA Center will prefix the name with SSID.

An example of the WLAN configuration, as seen from the web-based GUI of **C9800-40-CVD.cagelab.local** is shown in the following figure.



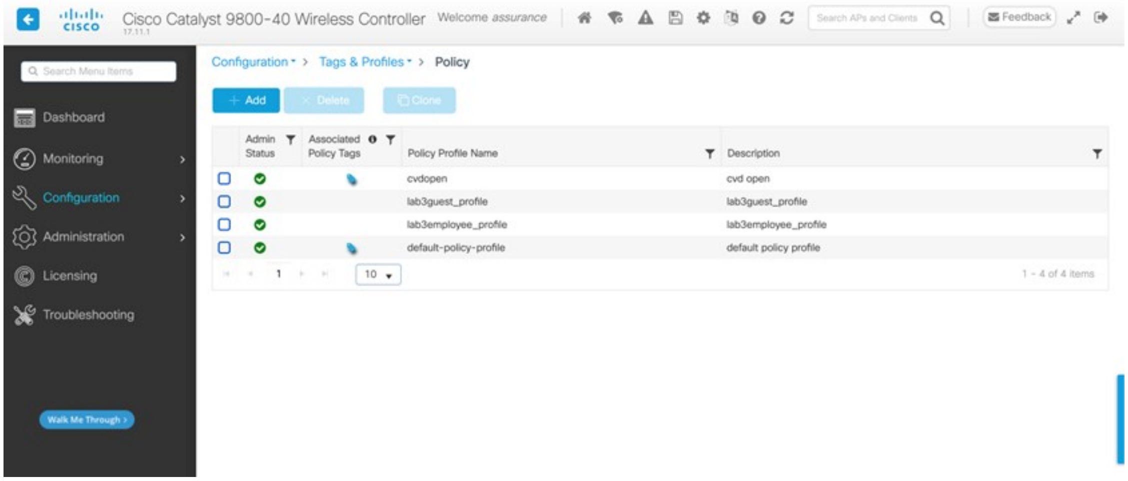
Selected WLANs : 0

Status	Name	ID	SSID	Security
●	cvduser	1	cvduser	[open]
●	lab3guest_profile	17	lab3guest	[open],MAC Filtering
●	lab3employee_profile	18	lab3employee	[WPA2][802.1x][AES]

1 - 3 of 3 items

The WLAN IDs corresponding to the two SSIDs, **lab3guest** and **lab3employee**, are 17 and 18, respectively. When APs are assigned the policy tag **default-policy-tag**, APs joined to Cisco Catalyst 9800 Series Wireless Controller will broadcast SSIDs of WLANs with IDs from 1 to 16. In order to avoid creating WLAN IDs which are broadcast with the **default-policy-tag**, Cisco DNA Center creates WLANs and SSIDs starting with a WLAN ID of 17 and higher.

During provisioning, Cisco DNA Center also creates two new policy profiles within the **C9800-40-CVD.cagelab.local**. The names of the new policy profiles match the names of the created WLAN profiles. An example of the configuration, as seen from the web-based GUI of **C9800-40-CVD.cagelab.local** is shown in the following figure.



Admin Status	Associated Policy Tags	Policy Profile Name	Description
✓	●	cvdopen	cvd open
✓		lab3guest_profile	lab3guest_profile
✓		lab3employee_profile	lab3employee_profile
✓	●	default-policy-profile	default policy profile

1 - 4 of 4 items

At this point in the provisioning process, the policy profiles and the WLAN profiles are not mapped to any policy tag that has been applied to any AP.

Provision the Cisco Catalyst 9800-CL Guest Anchor Wireless Controller

Use the following procedure to provision the corporate wireless profile to the Cisco Catalyst 9800-CL guest anchor Wireless Controller, known as **C9800-CL-CVD.cagelab.local**.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The main provisioning screen displays the devices in the inventory. By default, **Inventory** is chosen from the **Focus** drop-down list.

Step 2 Locate and check the check box for **C9800-CL-CVD.cagelab.local**.

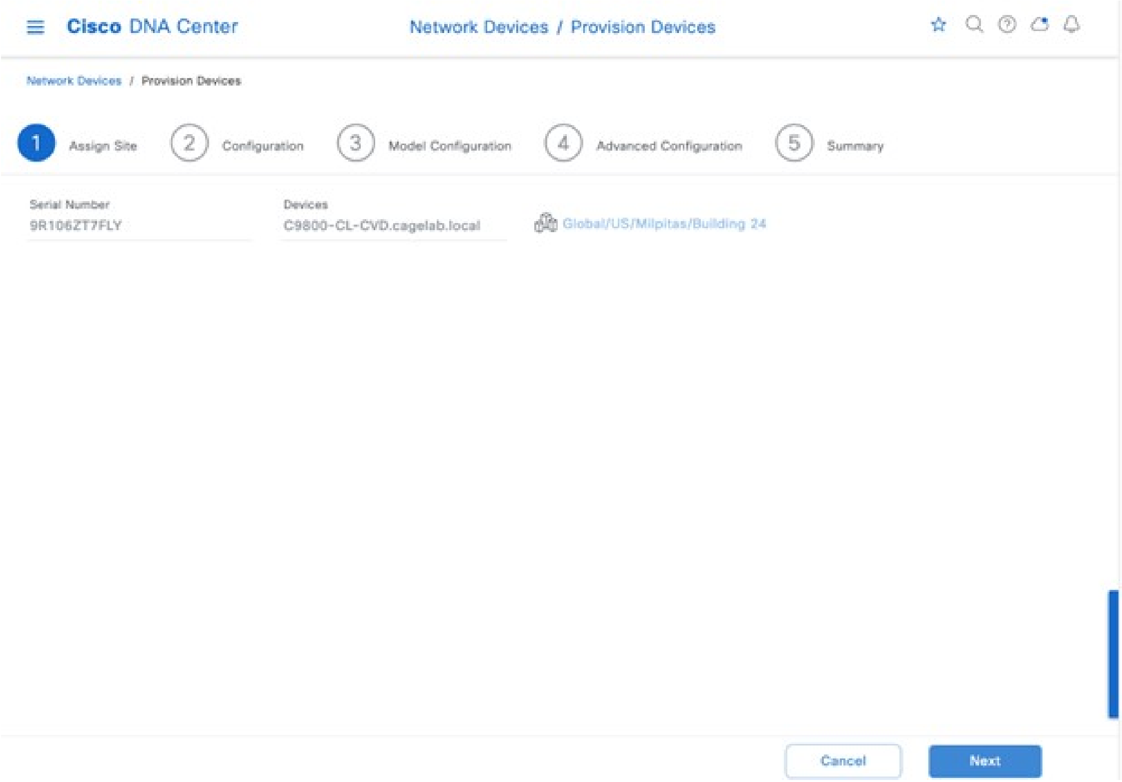
Step 3 From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

You are taken through a four-step workflow for provisioning the guest wireless controller (C9800-CL-CVD), starting with **Assign Site**.

Step 4 In the **Assign Site** window, click **Choose a Site**.

A slide-in pane is displayed, showing the site hierarchy configured for Cisco DNA Center. For this deployment guide, the guest anchor wireless controller (**C9800-CL-CVD.cagelab.local**) is assigned to the building level.

Step 5 Expand the site hierarchy for **Milpitas** and select **Building 23**.



Serial Number: 9R106ZT7FLY
Devices: C9800-CL-CVD.cagelab.local
Global/US/Milpitas/Building 24

Note The guest wireless controller (**C9800-CL-CVD.cagelab.local**) must be assigned to a building or floor in the Cisco DNA Center site hierarchy. The controller cannot be assigned to Milpitas or to the global level of the site hierarchy, even though **C9800-CL-CVD.cagelab.local** is assigned to **Building 23** in this deployment guide. APs located on floors in other buildings are supported by the wireless controller.

Step 6 Click **Save** to assign **C9800-CL-CVD.cagelab.local** to **Building 23**.

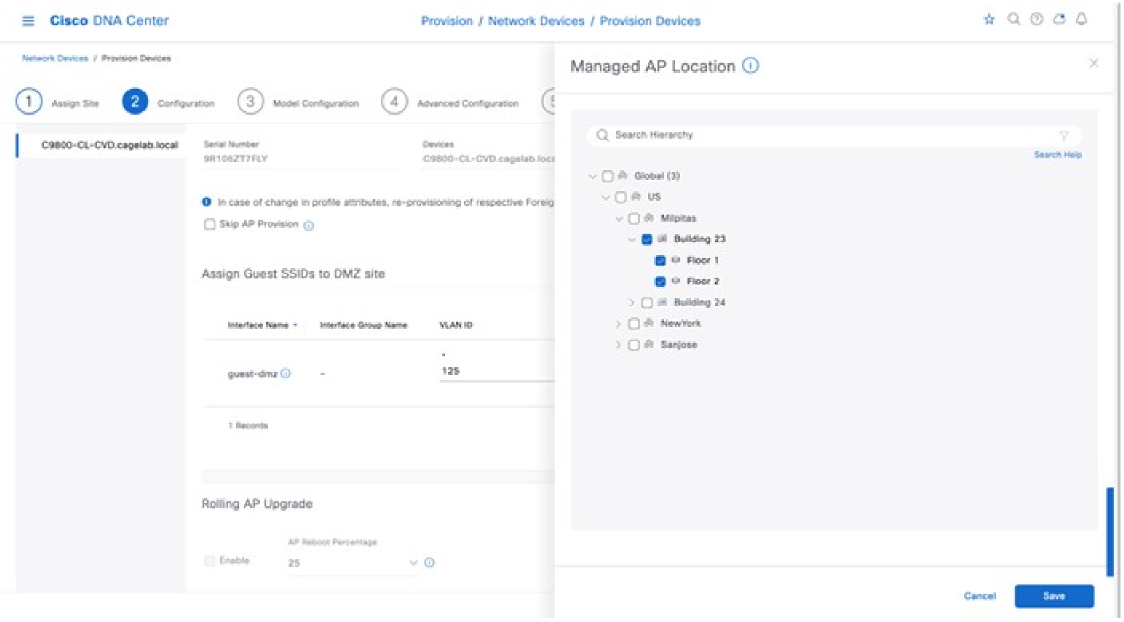
Step 7 Click **Next**.

The **Configuration** window is displayed.

Step 8 In the **Configuration** window, choose **Guest Anchor** for the wireless controller **Role**.

Step 9 Click **Select Primary Managed AP locations**.

The **Managed AP Location** slide-in pane is displayed, showing the site hierarchy for Cisco DNA Center.



C9800-CL-CVD.cagelab.local

Serial Number: 9R106ZT7FLY

Devices: C9800-CL-CVD.cagelab.loca

In case of change in profile attributes, re-provisioning of respective Foreig

□ Skip AP Provision

Assign Guest SSIDs to DMZ site

Interface Name	Interface Group Name	VLAN ID
guest-dmz	-	125

1 Records

Rolling AP Upgrade

□ Enable

AP Reboot Percentage: 25

- □ Global (3)
  - □ US
    - □ Milpitas
      - ☑ Building 23
        - ☑ Floor 1
        - ☑ Floor 2
      - □ Building 24
    - □ NewYork
    - □ Sanjose

For this deployment guide, the guest anchor wireless controller (**C9800-Flex-CVD.cagelab.local**) will manage APs on **Floor 1**, **Floor 2**, and **Floor 3** in building **branch5**.

Step 10 Expand the site hierarchy and choose the desired sites within the site hierarchy.

Step 11 Click **Save**.

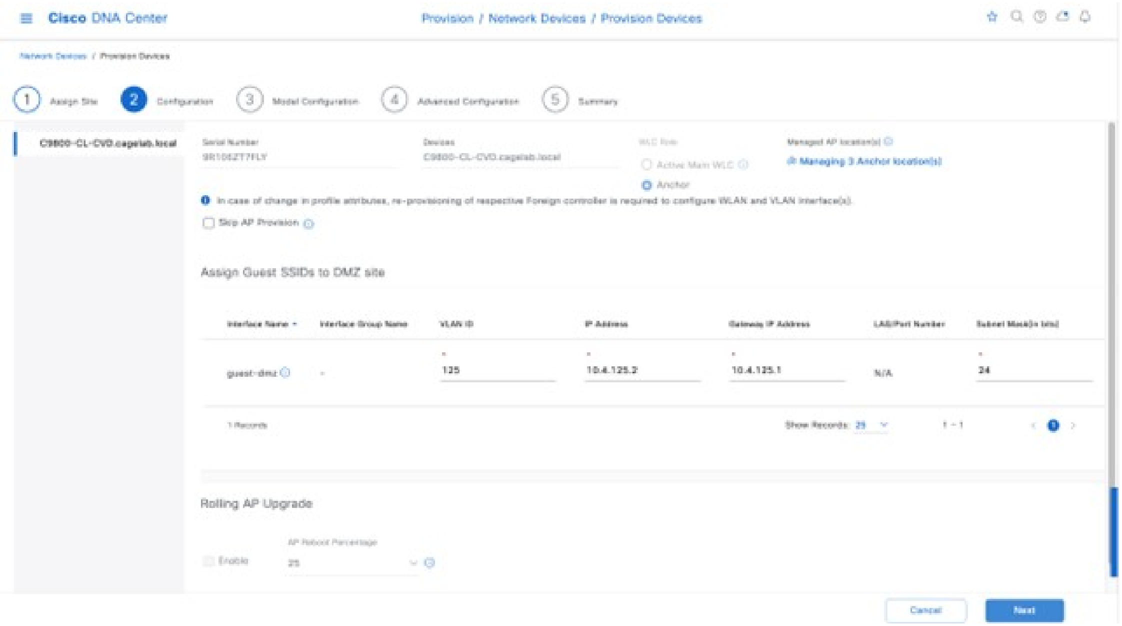
The **Managed AP Location** slide-in pane will close. Because you have selected this wireless controller to be a Guest wireless controller, additional fields are displayed. The corporate wireless profile has defined the enterprise SSID as **lab3guest** and the wireless interface on which the SSID terminates as **branchguest-dmz on VLAN ID 110**, so this enterprise SSID and wireless interface will be automatically displayed.

Step 12 Enter the values for IP address, Gateway IP address, LAG/Port Number, and Subnet Mask (in bits) for the SSID. The following table shows the values entered for this deployment guide.

Table 24: Guest Wireless Controller Settings

Field	Value
SSID Name	lab3guest
Interface Name	guest-dmz
VLAN ID	125
IP Address	10.4.125.2
Gateway IP Address	10.4.125.1
LAG/Port Number	1
Subnet Mask (in bits)	24

Figure 88: Guest Wireless Controller Settings in Cisco DNA Center



C9800-CL-CVD.cagelab.local

Serial Number: 9R1062T7FLY

Devices: C9800-CL-CVD.cagelab.local

WLC Role: ○ Active Main WLC ● Anchor

Managed AP location(s): Managing 3 Anchor location(s)

In case of change in profile attributes, re-provisioning of respective Foreign controller is required to configure WLAN and VLAN interface(s).

□ Skip AP Provision

Assign Guest SSIDs to DMZ site

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	LAG/Port Number	Subnet Mask(in bits)
guest-dmz	-	125	10.4.125.2	10.4.125.1	N/A	24

1 Records   Show Records: 25   1 - 1

Rolling AP Upgrade

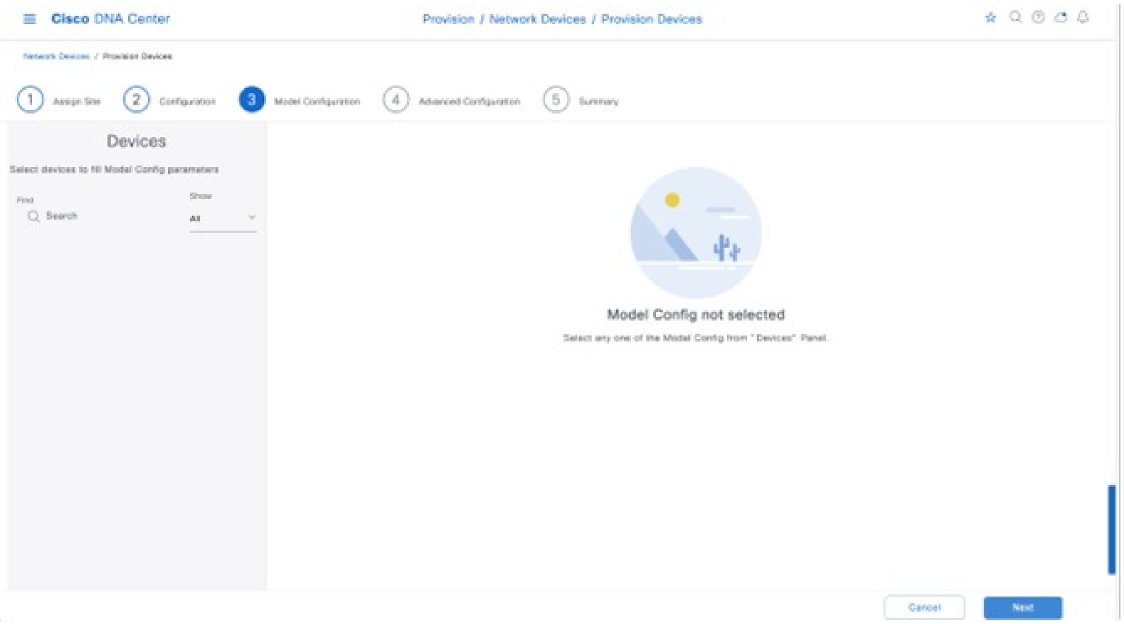
□ Enable   AP Reboot Percentage: 25

Step 13 Click **Next**.

The **Model Configuration** window is displayed. If you have configured a template within the model configs for the device type and the site, you can apply the template here, and you can edit and view the model configuration. In the campus wireless deployment, no model config is used.

Step 14 Click **Next**.

The **Summary** window is displayed.



Select devices to fill Model Config parameters

Model Config not selected

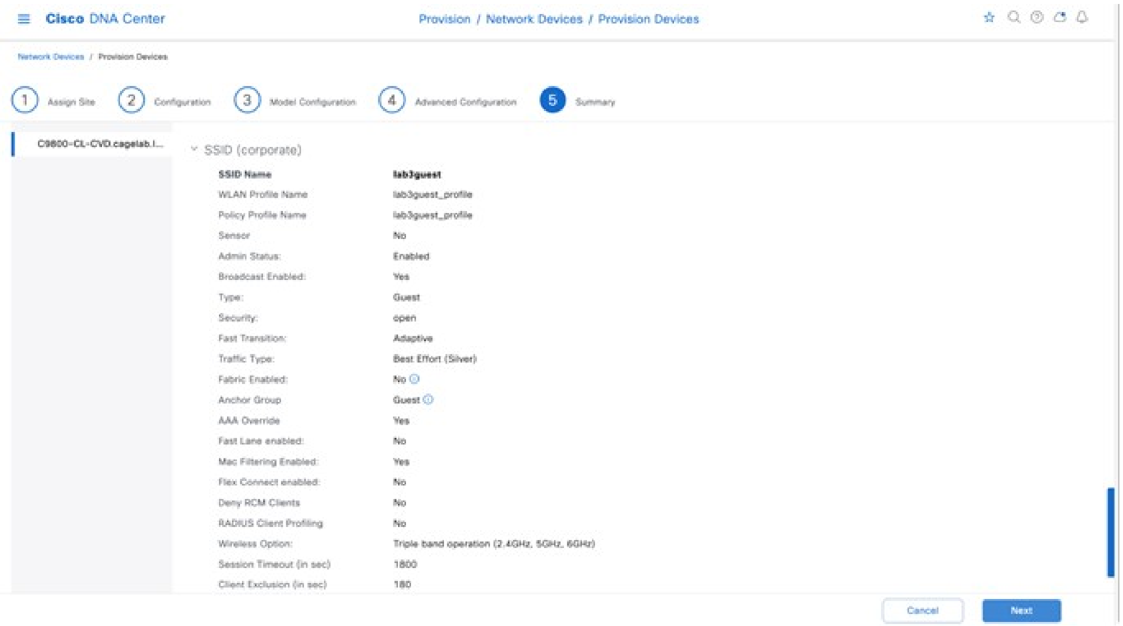
Select any one of the Model Config from " Devices" Panel.

Step 15 Click **Next** in the device provisioning workflow.

The **Advanced Configuration** window is displayed. If you have configured a template within the Template Editor for the device type and the site, you can apply the template here. This deployment guide does not discuss the use of templates for advanced configuration of the Catalyst 9800-CL guest Wireless Controller.

Step 16 Click **Next** in the device provisioning workflow.

The **Summary** window is displayed. This screen provides a summary of the configuration which is provisioned to C9800-CL-CVD.



SSID Name	**lab3guest**
WLAN Profile Name	lab3guest_profile
Policy Profile Name	lab3guest_profile
Sensor	No
Admin Status:	Enabled
Broadcast Enabled:	Yes
Type:	Guest
Security:	open
Fast Transition:	Adaptive
Traffic Type:	Best Effort (Silver)
Fabric Enabled:	No
Anchor Group	Guest
AAA Override	Yes
Fast Lane enabled:	No
Mac Filtering Enabled:	Yes
Flex Connect enabled:	No
Deny RCM Clients	No
RADIUS Client Profiling	No
Wireless Option:	Triple band operation (2.4GHz, 5GHz, 6GHz)
Session Timeout (in sec)	1800
Client Exclusion (in sec)	180

Step 17 You can expand each section to see the details of the configuration, which is based on the corporate wireless profile created in the *Design the wireless network* section of this deployment guide.

Step 18 Click **Next** to deploy the configuration to C9800-CL-CVD. A slide-in pane is displayed, asking if you want to deploy the configuration now or schedule the configuration for later.

Note It is best practice to make configuration changes and provision new devices in your network only during scheduled network operation change windows.

Step 19 Click the **Now** radio button, and click **Apply** to apply the configuration. You will be redirected back to the **Inventory** window within **Provisioning**. The provisioning status of the device will temporarily show **Provisioning**, but the status will change to **Success** after a few minutes. Click **See Details** below the provisioning status of the device for more information.

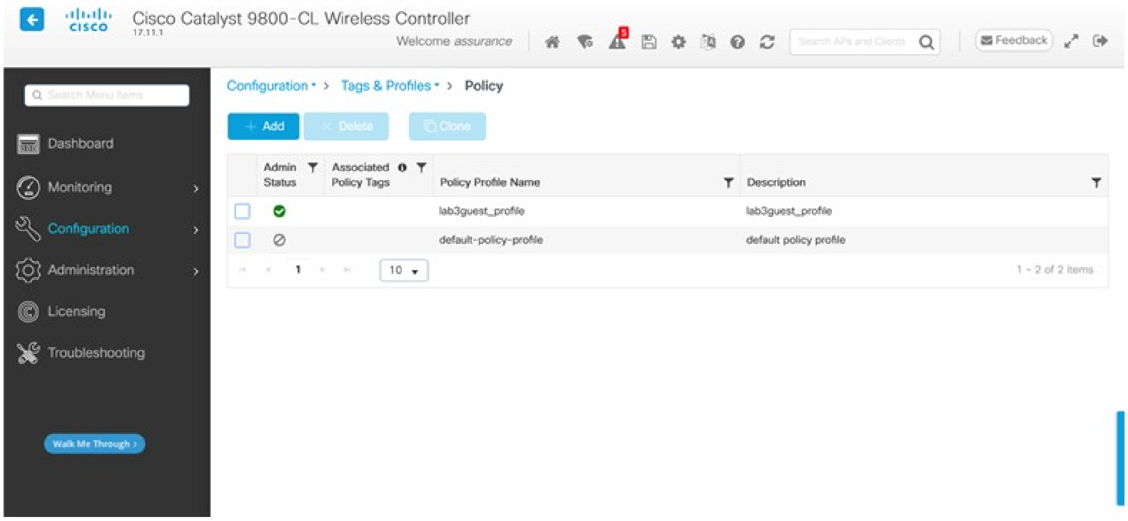
Cisco DNA Center will dynamically create a new WLAN profile within the Catalyst 9800-CL guest Wireless Controller (**C9800-CL-CVD.cagelab.local**). The following table shows the name of the WLAN profile and respective SSID generated by Cisco DNA Center during the provisioning of **C9800-CL-CVD.cagelab.local** for this deployment guide.

Table 25: WLAN Profiles for the Guest Anchor Wireless Controller

WLAN Profile Name	SSID	WLAN ID
lab3guest5_profile	lab3guest	17

The WLAN profile name is based on the SSID name, specified within the corporate wireless profile and created during the *Design the wireless network* section of this deployment guide.

An example of the WLAN configuration, as seen from the web-based GUI of **C9800-CL-CVD.cagelab.local**, is shown in the following figure.



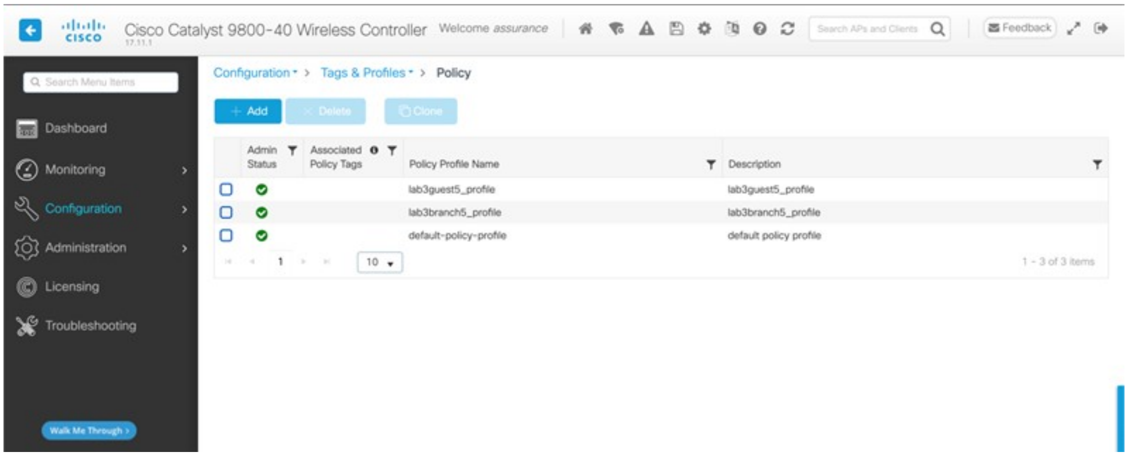
Configuration › Tags & Profiles › Policy

	Admin Status	Associated Policy Tags	Policy Profile Name	Description
□	✓		lab3guest_profile	lab3guest_profile
□	⊘		default-policy-profile	default policy profile

1 - 2 of 2 items

The WLAN ID corresponding to the lab3guest SSID is 17. When APs are assigned the policy tag **default-policy-tag**, the APs joined to Cisco Catalyst 9800 Series Wireless Controller will broadcast SSIDs of WLANs that have IDs from 1 to 16. To avoid creating WLAN IDs which are broadcast with the **default-policy-tag**, Cisco DNA Center creates WLANs or SSIDs starting with a WLAN ID of 17 and higher.

During provisioning, Cisco DNA Center also creates a new policy profile within the **C9800-40-CVD.cagelab.local**. The name of the new policy profile matches the name of the created WLAN profiles. An example of the configuration, as seen from the web-based GUI of **C9800-40-CVD.cagelab.local**, is shown in the following figure.



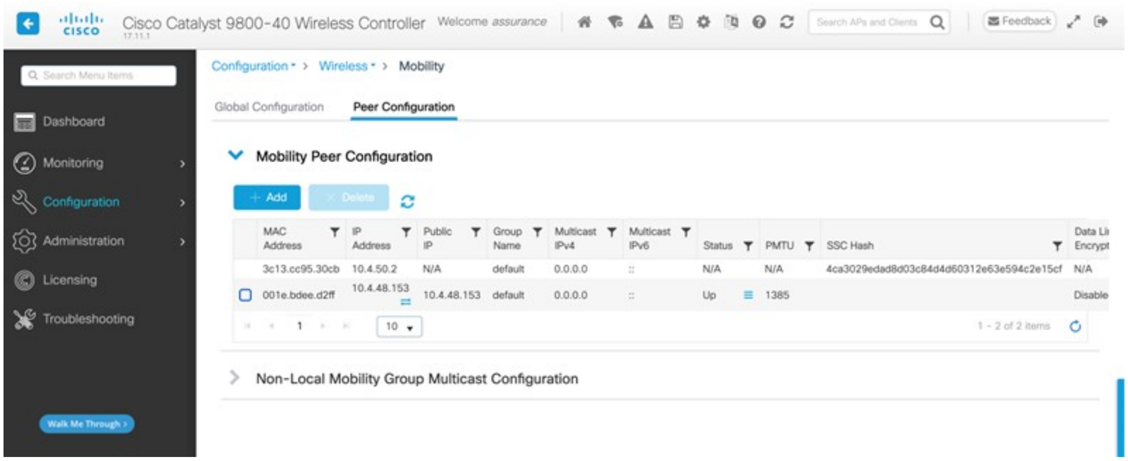
Configuration › Tags & Profiles › Policy

	Admin Status	Associated Policy Tags	Policy Profile Name	Description
□	✓		lab3guest5_profile	lab3guest5_profile
□	✓		lab3branch5_profile	lab3branch5_profile
□	✓		default-policy-profile	default policy profile

1 - 3 of 3 items

Cisco DNA Center will provision the mobility tunnel between the enterprise wireless controller HA SSO pair (**C9800-40-CVD.cagelab.local**) that functions as the foreign controller and the guest wireless controller (C9800-CL-CVD.cagelab.local) that functions as the anchor controller. The mobility tunnel is shown in the following figures.

Figure 89: Mobility Tunnel on the Foreign Controller (C9800-40-CVD.cagelab.local)



Configuration > Wireless > Mobility

Global Configuration | Peer Configuration

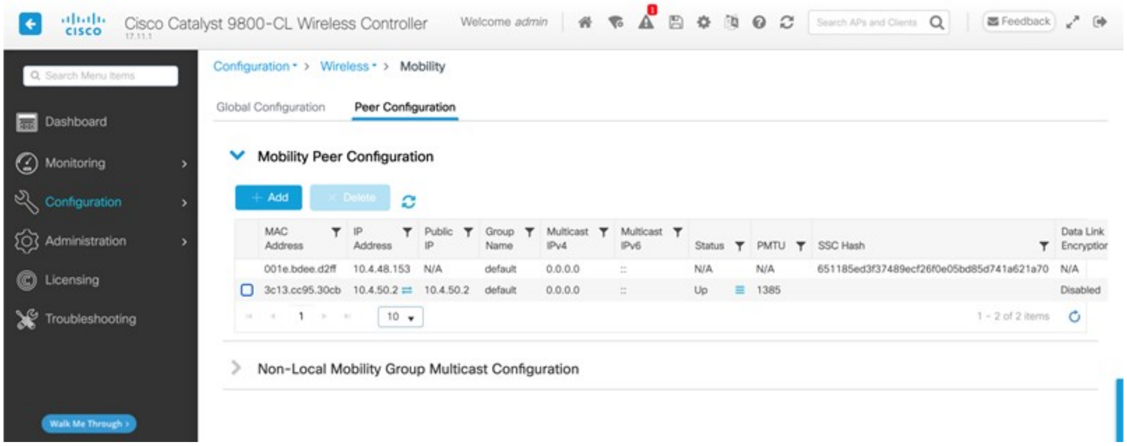
Mobility Peer Configuration

	MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Li Encrypt
	3c13.cc95.30cb	10.4.50.2	N/A	default	0.0.0.0	::	N/A	N/A	4ca3029edad8d03c84d4d60312e63e594c2e15cf	N/A
□	001e.bdee.d2ff	10.4.48.153	10.4.48.153	default	0.0.0.0	::	Up	1385		Disable

1 - 2 of 2 items

Non-Local Mobility Group Multicast Configuration

Figure 90: Mobility Tunnel on the Anchor Controller (C9800-CL-CVD.cagelab.local)



Configuration > Wireless > Mobility

Global Configuration | Peer Configuration

Mobility Peer Configuration

	MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryptior
	001e.bdee.d2ff	10.4.48.153	N/A	default	0.0.0.0	::	N/A	N/A	651185ed3f37489ecf26f0e05bd85d741a621a70	N/A
□	3c13.cc95.30cb	10.4.50.2	10.4.50.2	default	0.0.0.0	::	Up	1385		Disabled

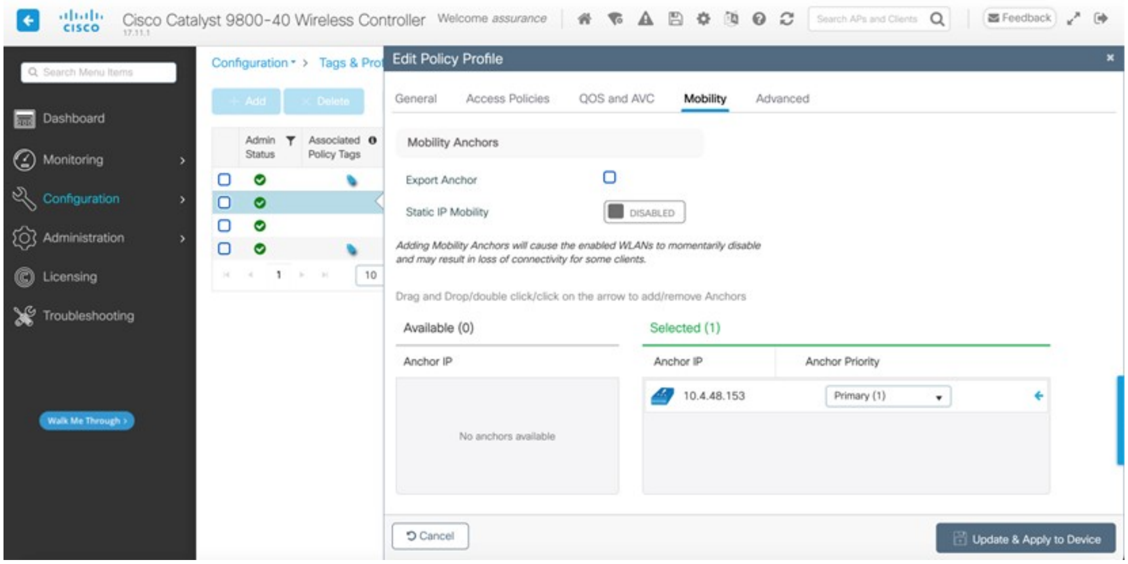
1 - 2 of 2 items

Non-Local Mobility Group Multicast Configuration

Step 20 Click the **lab3guest_Profile** policy profile in the foreign controller (**C9800-40-CVD.cagelab.local**) and navigate to the **Mobility** window, which displays the mapping of the anchor controller to the policy profile.

These settings are automatically configured by Cisco DNA Center during provisioning.

Figure 91: Foreign Controller (C9800-40-CVD.cagelab.local) Guest Policy Profile with Mobility Settings



Edit Policy Profile

Mobility Anchors

Export Anchor □

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)	Selected (1)	
Anchor IP	Anchor IP	Anchor Priority
No anchors available	10.4.48.153	Primary (1)

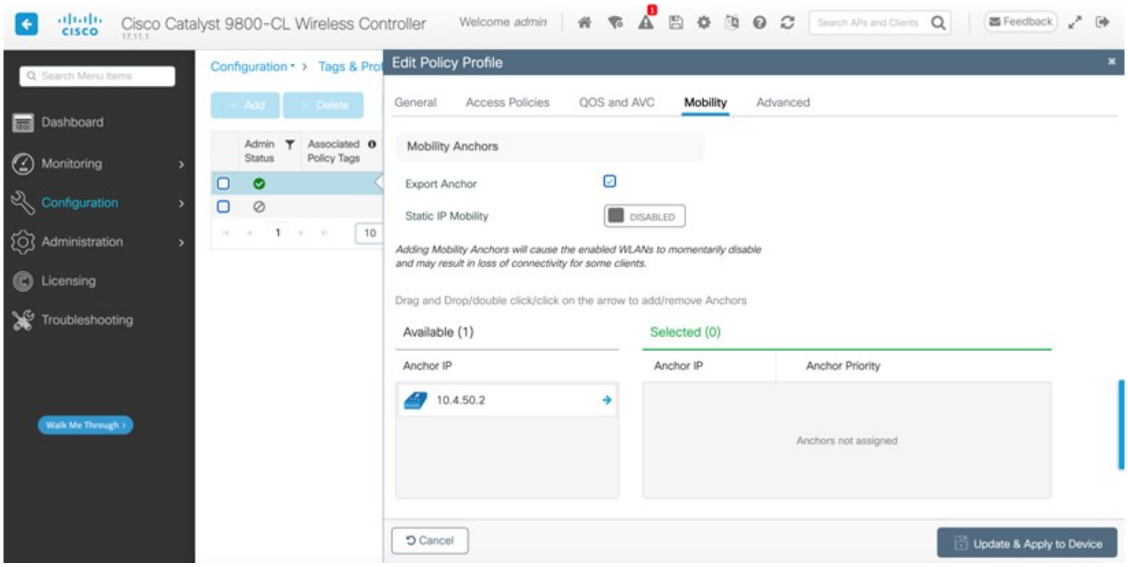
Cancel

Update & Apply to Device

Step 21 Click the **lab3guest_profile** policy profile in the anchor controller (**C9800-CL-CVD.cagelab.local**) and navigate to the **Mobility** window, which displays the export of the anchor controller within the policy profile (similar to the configuration of the anchor and foreign controllers within the Cisco AireOS Wireless Controllers).

These settings are automatically configured by Cisco DNA Center during provisioning.

Figure 92: Anchor Controller (WLC-9800-CL) Policy Profile with Mobility Settings



Edit Policy Profile

Mobility Anchors

Export Anchor ☑

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (0)	
Anchor IP	Anchor IP	Anchor Priority
10.4.50.2	Anchors not assigned	

Cancel

Update & Apply to Device

Join New APs to the Enterprise Cisco Catalyst 9800 Series Wireless Controller

The following steps explain how to discover and join the APs to the enterprise Catalyst 9800 Series Wireless Controller.

Before you begin

For this procedure in the deployment guide, assume that new APs will use IP DHCP discovery to discover the Cisco Catalyst 9800 Series Wireless Controller. Also assume that the new APs have never been primed. A Cisco AP has been primed when it has previously joined (established a CAPWAP tunnel) a wireless controller and cached the IP address of the wireless controller in NVRAM; or when primary, secondary, or tertiary wireless controller management IP addresses have been configured within the AP. In such scenarios, the AP will give preference to the primary, secondary, or tertiary wireless controller configuration over IP DHCP discovery.

With IP DHCP discovery, DHCP servers use Option 43 to provide one or more wireless controller management IP addresses to the APs. When an AP learns the management IP address of the Catalyst 9800 Series Wireless Controller, the AP sends a CAPWAP join request message to the wireless controller. Once joined, the wireless controller manages the APs configuration, firmware, control transactions, and data transactions.

Procedure

Step 1 Configure the necessary VLANs on the Layer 2 access switches that support the Cisco APs joining the Catalyst 9800 Series Wireless Controller.

This deployment guide assumes that APs are connected to Layer 2 access switches. A dedicated VLAN is on the switches for APs that are separate from end-user devices, such as PCs and IP phones. The use of a dedicated VLAN for APs and switch management is generally regarded as a design best practice, but this method does result in additional VLANs being deployed on the switches.

The management VLAN (VLAN 64) is used for establishing CAPWAP tunnels to branch APs and for managing connectivity to the branch switch. The branch employee VLAN (VLAN 16) is used for locally terminating wireless traffic from the corporate event SSID on the branch switch.

Step 2 Configure VLAN 64 and VLAN 16 on the branch switch.

Step 3 Configure the switch port to which the AP is connected to be a trunk port, with VLANs 64 and 16 allowed and VLAN 16 as the native VLAN. Make sure the switch port is not shut down. An example is shown in the following configuration.

```
interface GigabitEthernet1/0/1
switchport trunk native vlan 64
switchport trunk allowed vlan 16,64
switchport mode trunk logging event trunk-status load-interval 30
no shutdown
spanning-tree portfast trunk
ip dhcp snooping trust
```

For this deployment guide, a Microsoft Active Directory (AD) server with IP address `10.4.48.9` functions as the IP DHCP server. The IPv4 address of the Catalyst 9800 Series Wireless Controller (C9800-CL deployed on AWS) configured within DHCP Option 43 is `172.38.0.10`. Configuration of the DHCP within the Microsoft AD server is outside the scope of this document.

The following example depicts the configuration of a Layer 3 switch using a VLAN switched virtual interface (SVI):

```
interface Vlan64
ip address 10.5.64.1
255.255.255.0
ip helper-address 10.4.48.10
```

```
interface Vlan16
ip address 10.5.16.1
255.255.255.0
ip helper-address 10.4.48.10
```

Step 4 Connect the Cisco AP(s) to the switch port(s) on the Layer 2 access switches.

The APs should get IP addresses and automatically join the Catalyst 9800 Series Wireless Controller. Once the new APs register with the wireless controller, a resync on Cisco DNA Center is automatically triggered. After the resync is complete, the new APs will show up in the inventory. Alternatively, you can manually resync the inventory for the wireless controller using the following steps:

a. From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

b. Check the check box for the device name.

c. From the **Actions** drop-down list, choose **Inventory** > **Resync Device**.

d. Click **Ok** in the warning window to confirm the resync.

After you have resynced the Catalyst 9800-40 wireless controller HA SSO pair (WLC-9800-2), the APs that are joined to the wireless controller should appear within the inventory.

Provision the New APs

Once the access points (APs) have been joined to the Cisco Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (**C9800-40-CVD.cagelab.local**), the APs must be provisioned. Provisioning with Cisco DNA Center is necessary for the APs to receive the correct configuration to advertise the **lab3employee** and **lab3guest** SSIDs.

The following table lists the APs that are provisioned in this deployment guide, including their locations:

AP Name	AP Model	Location
mil23-floor1-ap1	C9130AXI-B	Building 23, Floor 1
mil23-floor1-ap2	C9130AXI-B	Building 23, Floor 1
mil23-floor2-ap1	C9130AXI-B	Building 23, Floor 2
mil24-floor1-ap1	C9124AXD-B	Building 24, Floor 1
mil24-floor2-ap1	C9124AXD-B	Building 24, Floor 2
AP1416.9D7C.16FC	C9130AXI-B	Branch 5, Floor 1
AP1416.9D7C.16F8	C9130AXI-B	Branch 5, Floor 2

Note In this deployment guide, a mixture of APs deployed across the buildings and floors shows the provisioning of different AP models in different locations, all controlled by the same Catalyst 9800 Series HA SSO Wireless Controller pair. In a typical deployment, the same AP model would be deployed for a floor and across the entire deployment.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The main provisioning screen displays the devices within the inventory. By default, the **Focus** will be set for **Inventory**.

Step 2 Check the box for each of the APs to be provisioned.

Step 3 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

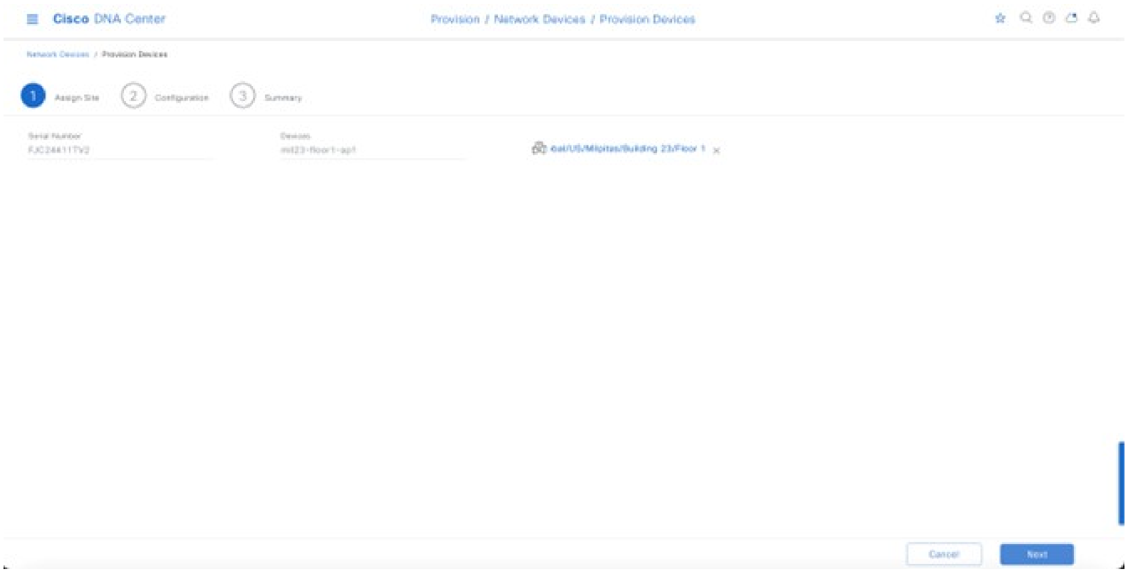
You are taken through a workflow for provisioning the APs, starting **Assign Site**.

Step 4 For each of the APs, click **Choose a Site**.

A side panel is displayed, showing the site hierarchy configured for Cisco DNA Center.

Expand the site hierarchy for Milpitas, and then choose the building (**Building 23** or **Building 24**) and the floor (**Floor 1** or **Floor 2**) for each AP.

Figure 93: AP Provisioning Step 1 – Assign Site


Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
Cancel
Next

Serial Number: FJC24411TV2

Devices: mil23-floor1-ap1

Global/US/Milpitas/Building 23/Floor 1

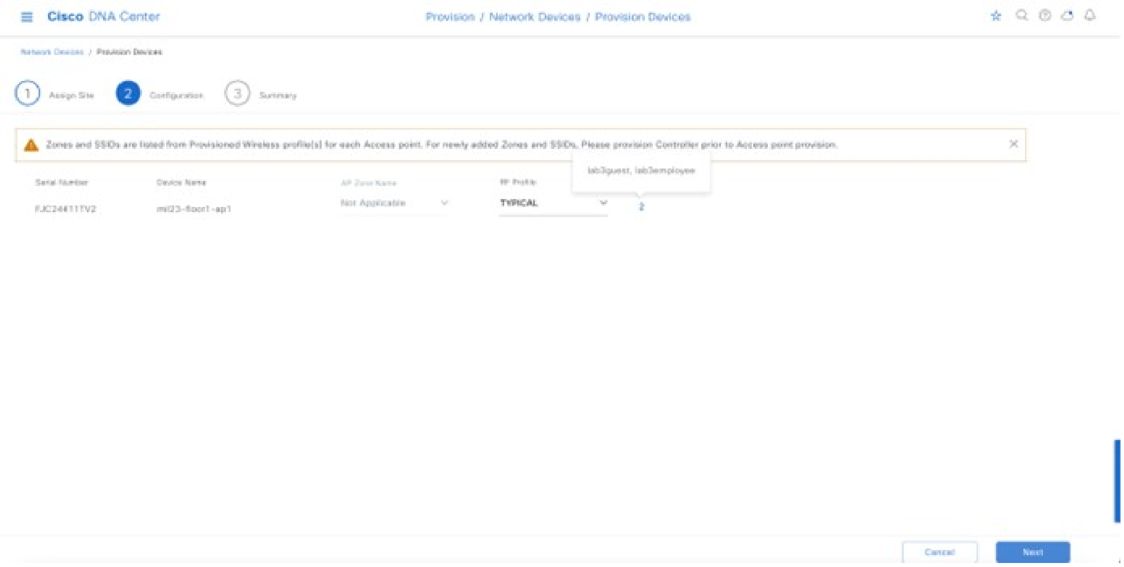
Step 5 Click **Save**.

Step 6 Click **Next** to set up the configuration.

Step 7 From the drop-down menu, for **RF Profile**, choose the RF profile that you want to assign to each of the APs.

For this deployment guide, the TYPICAL RF profile was chosen. This RF profile was also chosen as the default RF profile in *Design the wireless network*.

Figure 94: AP Provisioning Step 2 – Configuration



Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
Cancel
Next

Zones and SSIDs are listed from Provisioned Wireless profile(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision.

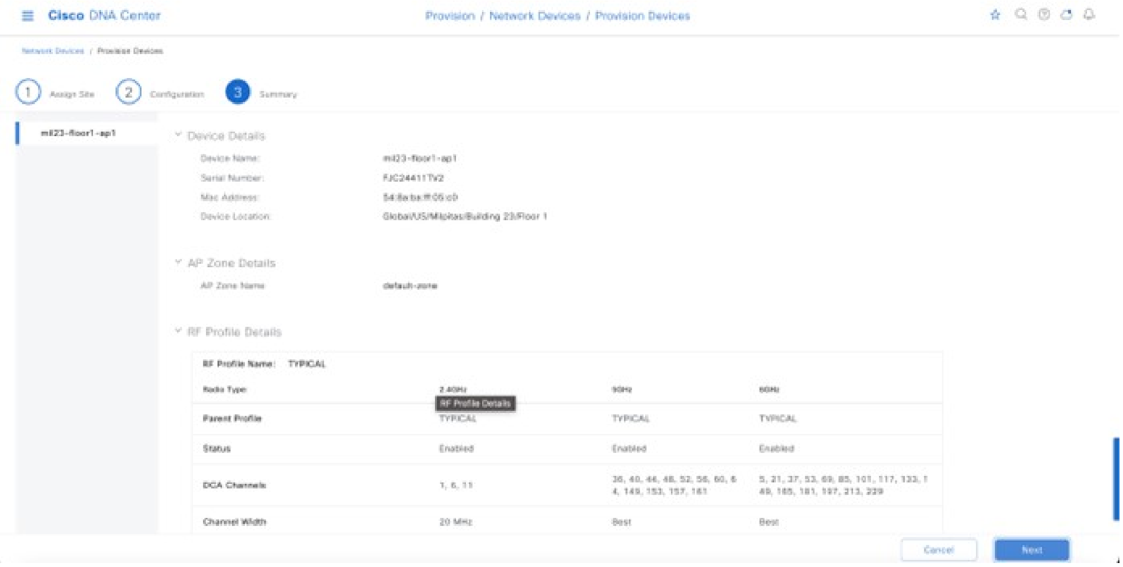
Serial Number	Device Name	AP Zone Name	RF Profile	
FJC24411TV2	mil23-floor1-ap1	Not Applicable	TYPICAL	2

lab3guest, lab3employee

Step 8 Click **Next**.

The **Summary** screen is displayed with details of the configuration that will be provisioned to each AP.

Figure 95: AP Provisioning Step 3 – Summary



Device Details

Device Name: mil23-floor1-ap1

Serial Number: FJC24411TV2

Mac Address: 54:8a:ba:ff:05:c0

Device Location: Global/US/Milpitas/Building 23/Floor 1

AP Zone Details

AP Zone Name: default-zone

RF Profile Details

RF Profile Name: TYPICAL

Radio Type	2.4GHz	5GHz	6GHz
Parent Profile	TYPICAL	TYPICAL	TYPICAL
Status	Enabled	Enabled	Enabled
DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213, 229
Channel Width	20 MHz	Best	Best

Step 9 Click **Deploy** to provision the APs.

A slide-in pane is displayed. You can choose to deploy the configuration now, or you can schedule the configuration for later.

The best practice is to make configuration changes and provision new devices in your network only during scheduled network operation change windows.

The following metrics describe the recommended scale limits. Outside of these recommended numbers, the wireless controller will work, but the controller will operate below its optimal performance.

Table 26: Recommended Maximum Number of APs per Site Tag for Local Mode

Platform	Number of APs
C9800-90	1600 APs/tag
C9800-40	800 APs/tag
C9800-CL (medium and large)	1600 APs/tag
Any other C9800 platform	500 APs/tag

Table 27: Recommended Maximum Number of APs per Site Tag for Flex Mode

Platform	Number of APs
All	100 APs/tag

Table 28: Recommended Number of Site Tags

Platform	Number of Site Tags
C9800-80	8
C9800-40	5
C9800-CL (medium)	3
C9800-CL (large)	7

Step 10 Choose **Now** and then click **Apply** to apply the configuration.

The **Success** dialog box is displayed, indicating that after provisioning, the APs will reboot.

Step 11 Click **OK**.

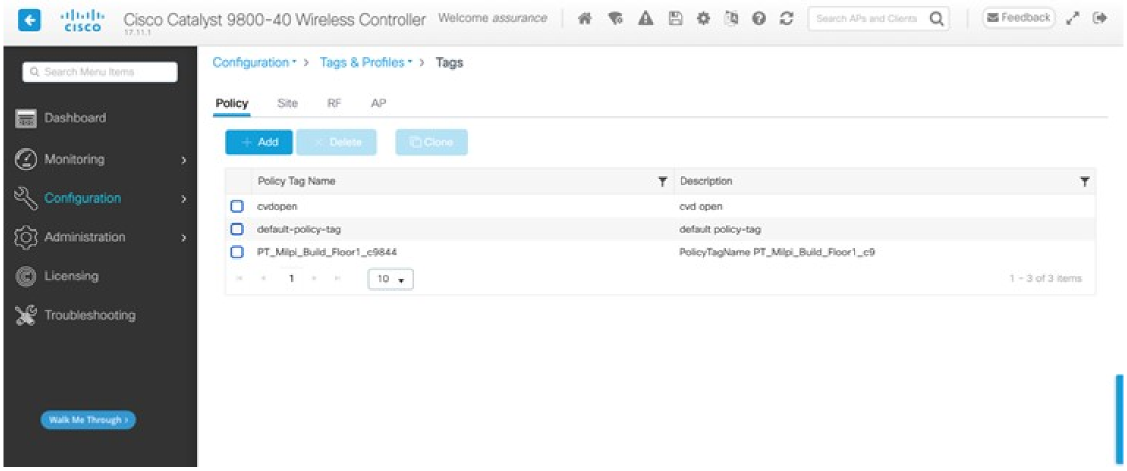
The main **Provisioning** window displays the list of inventories.

The provisioning status of the APs will temporarily show as **Provisioning**, but the status will transition to **Success** after a few minutes. For more information, you can click **See Details** directly below the provisioning status of each AP.

Cisco DNA Center creates a new policy tag within the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (**C9800-40-CVD.cagelab.local**) for each floor that contains provisioned APs.

For example, in the following figure, three new policy tags are created, corresponding to the APs provisioned on **Floor 1** of **Building 23**. Each policy tag is unique to a site, indicating a specific floor in a building. Policy tags for a floor will be created by Cisco DNA Center when APs are provisioned to the floor.

Figure 96: Policy Tags Created by Cisco DNA Center in the Catalyst 9800-40 Enterprise Wireless Controller



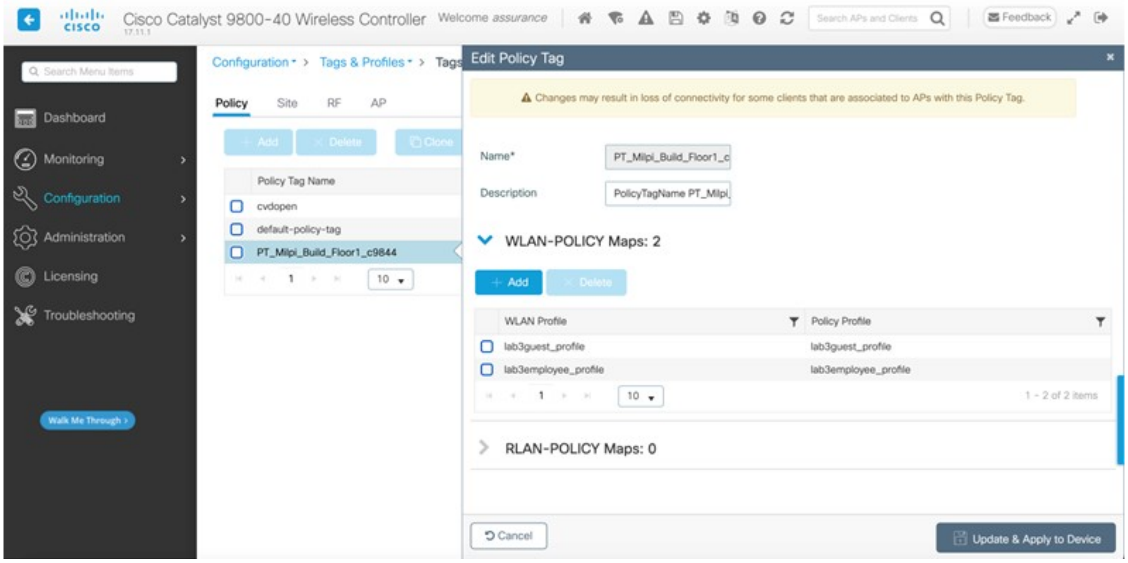
	Policy Tag Name	Description
□	cvdopen	cvd open
□	default-policy-tag	default policy-tag
□	PT_Milpi_Build_Floor1_c9844	PolicyTagName PT_Milpi_Build_Floor1_c9

1 · 10 · 1 - 3 of 3 items

Click on any of the policy tags to display the policy profiles and the WLAN profiles that have been added to the new policy tag by Cisco DNA Center.

The WLAN profiles and the policy profiles created during the provisioning of the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair have been added to each of the policy tags, which are controlled by the corporate WLAN profile created in Cisco DNA Center in *Design the wireless network*. The corporate WLAN profile specified the **lab3employee** and **lab3guest** SSIDs to be broadcast throughout the Milpitas area (**Floor 1** in **Buildings 23**).

Figure 97: Policy Tag Details



Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*: PT_Milpi_Build_Floor1_c

Description: PolicyTagName PT_Milpi

WLAN-POLICY Maps: 2

+ Add × Delete

	WLAN Profile	Policy Profile
□	lab3guest_profile	lab3guest_profile
□	lab3employee_profile	lab3employee_profile

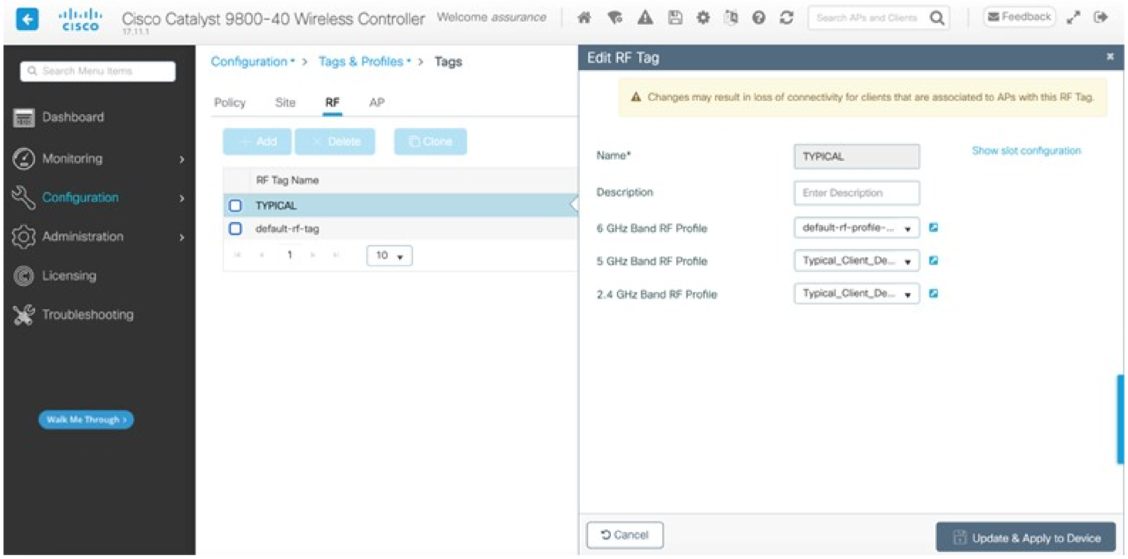
1 · 10 · 1 - 2 of 2 items

RLAN-POLICY Maps: 0

Cancel · Update & Apply to Device

During the AP provisioning process, the TYPICAL RF profile was chosen. Cisco DNA Center creates a new RF tag named TYPICAL within the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (WLC-9800-2).

Figure 98: TYPICAL RF Tag created by Cisco DNA Center



Edit RF Tag

⚠ Changes may result in loss of connectivity for clients that are associated to APs with this RF Tag.

Name* TYPICAL

Show slot configuration

Description Enter Description

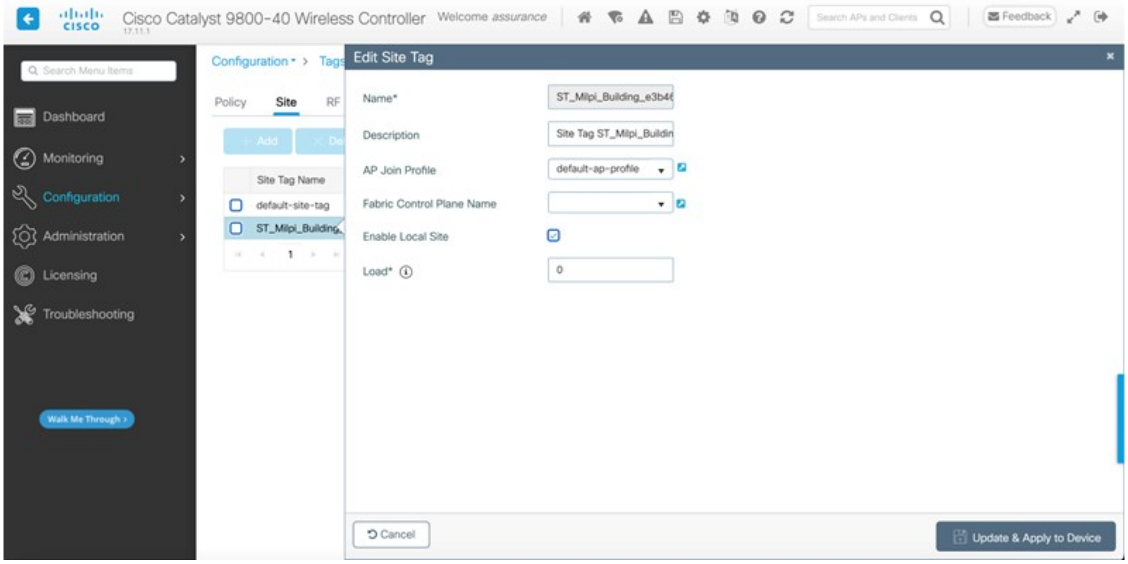
6 GHz Band RF Profile default-rf-profile-...

5 GHz Band RF Profile Typical_Client_De...

2.4 GHz Band RF Profile Typical_Client_De...

Finally, Cisco DNA Center statically assigns a policy tag (specific to each floor), an RF tag (named TYPICAL since this was the only RF Profile specified during AP provisioning), and a site tag (named ST_Milpi_Building_e3b46_0) to each AP within the Catalyst 9800-40 enterprise wireless controller HA SSO pair (C9800-40-CVD.cagelab.local). The site tag ST_Milpi_Building_e3b46_0 contains the default AP join profile named default-ap-profile.

Figure 99: Site Tag Created by Cisco DNA Center



Edit Site Tag

Name* ST_Milpi_Building_e3b4(

Description Site Tag ST_Milpi_Buildin

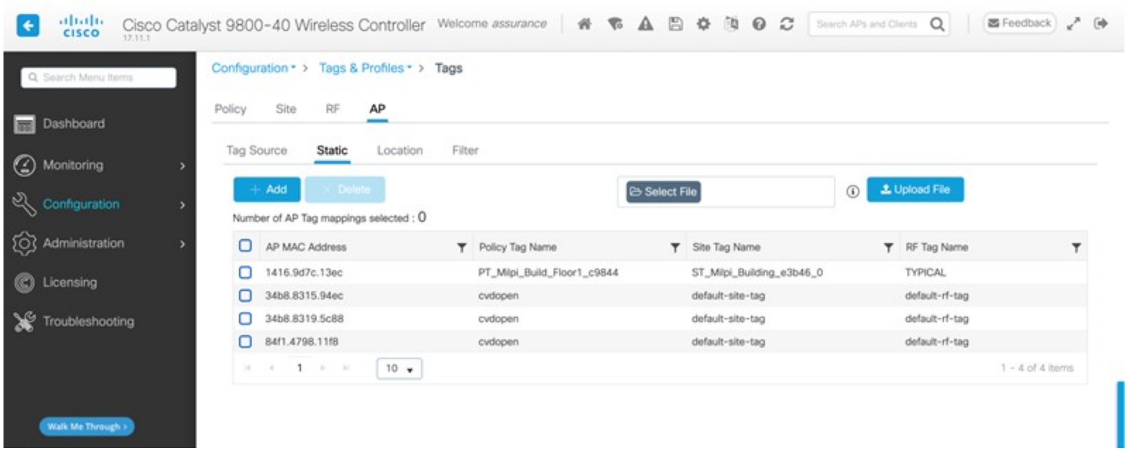
AP Join Profile default-ap-profile

Fabric Control Plane Name

Enable Local Site ☑

Load* ⓘ 0

Figure 100: Static Assignment of Tags to APs by Cisco DNA Center



Number of AP Tag mappings selected : 0

☐	AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
☐	1416.9d7c.13ec	PT_Milpi_Build_Floor1_c9844	ST_Milpi_Building_e3b46_0	TYPICAL
☐	34b8.8315.94ec	cvdopen	default-site-tag	default-rf-tag
☐	34b8.8319.5c88	cvdopen	default-site-tag	default-rf-tag
☐	84f1.4798.11f8	cvdopen	default-site-tag	default-rf-tag

The assignment of the policy tag to the AP causes the **lab3employee** and **lab3guest** SSIDs to be broadcast by the AP provisioned on the floor. At this point, wireless clients should be able to associate with the **lab3employee** and/or **lab3guest** SSIDs and authenticate to the network.

Position New APs on a Floor Map with No Planned AP

You must position the newly discovered APs on the floor maps if there is no corresponding AP planned for each of the buildings and floors within Cisco DNA Center. When a planned AP matches the hostname of the new AP, the new AP is automatched with the planned AP and positioned as per the planned AP.

Note Automatching only happens when browsing to the floor in the network hierarchy.

At this point in the deployment, the AP in local mode should be broadcasting the SSID on the floors for Milpitas, Building 23.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy**.

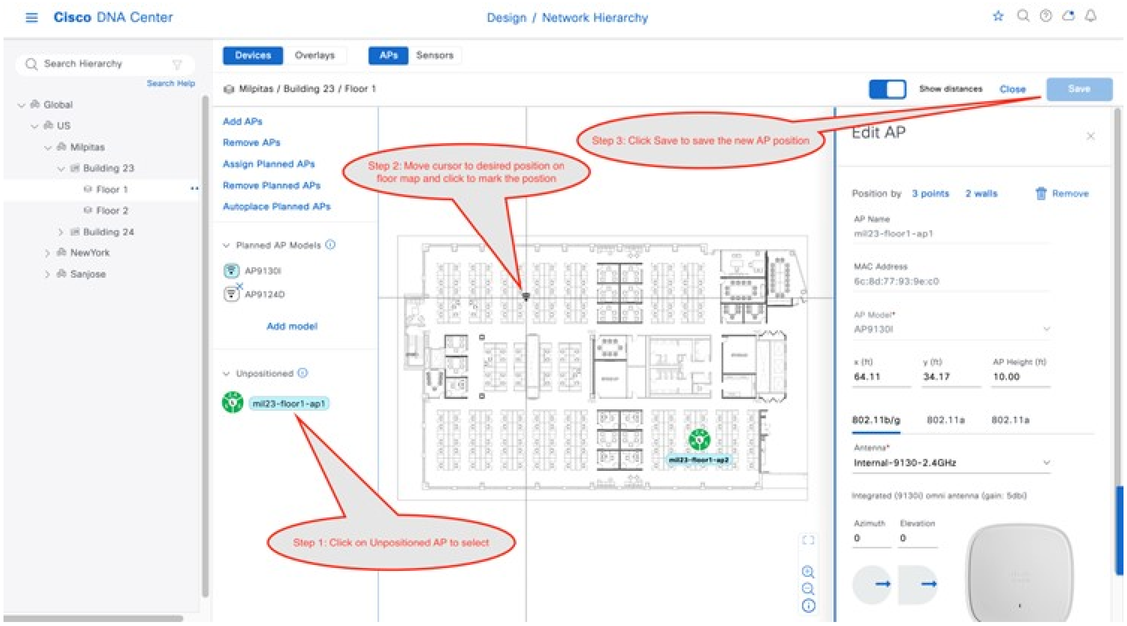
Step 2 Expand the network hierarchy in left hierarchy tree and choose Milpitas > Building 23 > Floor 1.

The floor plan for Floor 1 is displayed.

Step 3 Click **Add/Edit** to edit the floor plan.

The unpositioned APs are displayed, allowing you to edit various aspects of the floor plan.

Figure 101: Edit the Floor Plan



Step 1: Click on Unpositioned AP to select

Step 2: Move cursor to desired position on floor map and click to mark the postion

Step 3: Click Save to save the new AP position

AP Name: mil23-floor1-ap1

MAC Address: 6c:8d:77:93:9e:c0

AP Model*: AP9130I

x (ft): 64.11

y (ft): 34.17

AP Height (ft): 10.00

Antenna*: Internal-9130-2.4GHz

Integrated (9130I) omni antenna (gain: 5dbi)

Azimuth: 0

Elevation: 0

Step 4 Choose an unpositioned AP, move your cursor to the correct location on the floor map, and then click to choose the desired position.

The floor map will change, showing additional details about the position of the AP on the floor map. You may need to select the antenna for the AP, depending on the model of AP that you are positioning. If you need to select the antenna, a red warning will be displayed.

Step 5 (Optional) Click on the **802.11a/b/g/n** tab to display the antenna, azimuth, and elevation settings.

Step 6 From the **Antenna** drop-down list, choose the antenna type for the AP being positioned.

For the design and deployment guide, internal antennas were used on all APs.

Step 7 Repeat the Step 1 through Step 6 for the **802.11a** tab.

You can fine tune the position and adjust the AP height, once the AP is placed on the floor map. The default AP height will be based on the height of the floor that you specified when you imported the floor map. You can adjust the azimuth and elevation settings of the antennas, or for APs with integrated antennas, you can adjust the azimuth and elevation of the AP.

Step 8 Repeat Step 1 through Step 7 for the remaining unpositioned APs on the floor.

Step 9 Click **Save**.

The positioning of the APs on the floor map is saved. Once you have positioned the APs on the floor map, you should see heat maps. By default, the heat maps display AP RSSI values, which provide a rough estimate of the coverage area of each of the APs on the floor. The heat maps can be displayed for 2.4 GHz coverage, 5 GHz coverage, or both 2.4 and 5 GHz coverage.

Step 10 (Optional) Click **Add/Edit** again, to edit the floor plan.

Step 11 In the **Overlays** section, you have the option to add coverage areas, openings, location regions, walls, shelving units, markers, GPS markers, and align points to make the floor plan more accurately reflect the RF characteristics of the actual floor.

At this point in the deployment, the AP in local mode should be broadcasting the SSID on the floors for Milpitas, Building 23.

Enterprise WLAN for Remote Office Wireless Deployment

This section describes how to provision an AP in flex mode for the **New York** site.

Use this procedure to provision the **branch5** wireless profile to the Cisco Catalyst 9800-40 enterprise Wireless Controller (**C9800-Flex-CVD**). For information about the **branch5** wireless profile, see Define the Wireless Network, on page 5.

Before you begin

Make sure that the wireless controller has been discovered, the software image has been updated, and the high availability (HA) wireless controller has been configured.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The main provisioning window displays the devices. By default, the **Focus** will be set to **Inventory**.

Step 2 Check the check box for the Cisco Catalyst 9800-40 enterprise Wireless Controller (**C9800-Flex-CVD**).

Step 3 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

You are taken through a workflow for provisioning the enterprise wireless controller (**C9800-Flex-CVD**), starting with **Assign Site**.

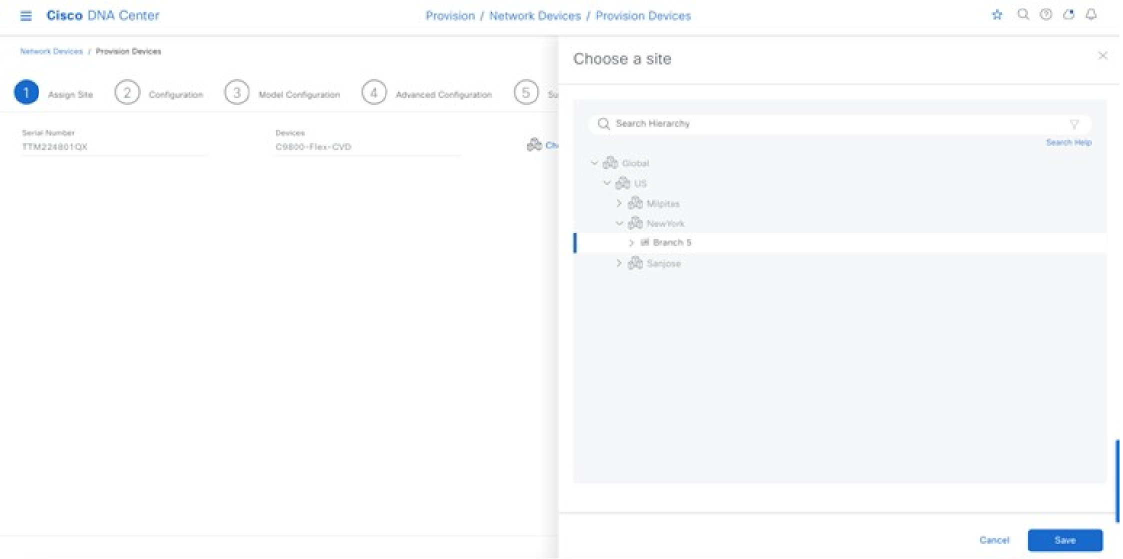
Step 4 Click **Choose a Site** in the **Assign Site** window. A slide-in pane is displayed, showing the site hierarchy configured for Cisco DNA Center.

The enterprise wireless controller (**C9800-Flex-CVD**) must be assigned at the building level.

Do the following in the **Choose a Site** slide-in pane:

a) Expand the site hierarchy for **New York** and choose **Branch 5**.

Figure 102: Enterprise Wireless Controller Provisioning – Assign Site



Serial Number: TTM224801QX

Devices: C9800-Flex-CVD

Note The enterprise wireless controller (**C9800-Flex-CVD**) must be assigned to a building or floor within the Cisco DNA Center site hierarchy. It cannot be assigned to an area (like **New York**) or to the global level of the site hierarchy. Although **C9800-Flex-CVD** is assigned to a building (**Branch 5** for this guide), APs located on floors in other buildings are supported by the wireless controller.

b) Click **Save** to assign **C9800-Flex-CVD** to building **Branch 5**.

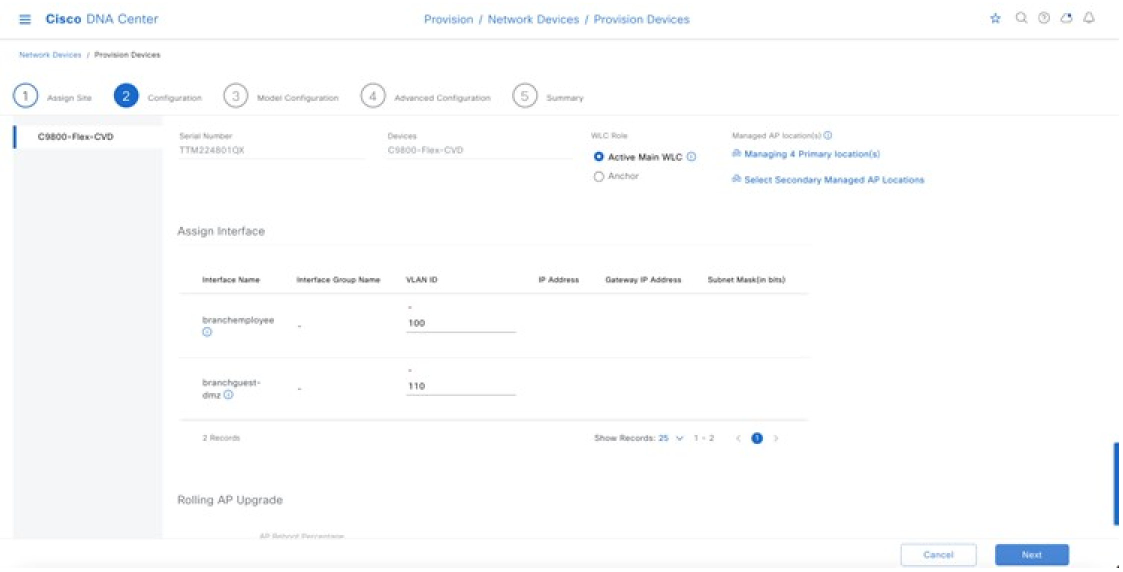
Step 5 Click **Next**.

Step 6 In the **Configuration** window, do the following:

a) For the **WLC Role**, choose **Active Main WLC**.

b) Click **Select Primary Managed AP locations**. The **Managed AP Location** slide-in pane is displayed, showing the site hierarchy for Cisco DNA Center.

Figure 103: Enterprise Wireless Controller Provisioning – Configuration



C9800-Flex-CVD

Serial Number: TTM224801QX

Devices: C9800-Flex-CVD

WLC Role: ● Active Main WLC ○ Anchor

Managed AP location(s): Managing 4 Primary location(s)

Select Secondary Managed AP Locations

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
branchemployee	-	100			
branchguest-dmz	-	110			

2 Records   Show Records: 25   1 - 2

Cisco DNA Center 2.3.5.5 release supports the ability to configure N+1 redundancy for APs and HA SSO for wireless controllers. This means you can configure both primary and secondary managed AP locations. Primary managed AP locations are sites (buildings and/or floors) where the wireless controller serves as the primary wireless controller within the AP high availability configuration. Secondary managed AP locations are sites where the wireless controller serves as the secondary wireless controller within the AP high availability configuration. If the primary wireless controller or the wireless controller HA SSO pair fails, APs will reestablish CAPWAP connections to the wireless controller.

For this deployment guide, the Catalyst 9800-40 Series Wireless Controller (**C9800-Flex-CVD**) will be the primary wireless controller managing APs within **Floor 1**, **Floor 2**, and **Floor 3** on **Branch 5**. No secondary managed AP locations will be configured because the wireless controller HA SSO pair already provides redundancy in a campus network, where all the APs are operating in a centralized (local) mode deployment.

c) Expand the site hierarchy and choose **Floor 1**, **Floor 2**, and **Floor 3** in **Branch 5** and **Floor 1**, **Floor 2**, and **Floor 3**.

d) Click **Save**.

The **Managed AP Location** slide-in pane will close. Because you have selected the wireless controller to be an **Active Main WLC**, additional fields are displayed within the window. Since the **branch5** wireless profile has defined the enterprise SSID as **lab3branch5** and the wireless interface on which the SSID terminates as **branchemployee** on VLAN ID 100, both the SSID and the wireless interface will be automatically displayed. Likewise, because the **corporate** wireless profile has defined the guest SSID as **lab3guest** and has defined the wireless interface on which the SSID terminates as **guest-dmz** on VLAN ID 125, these will also be automatically displayed.

e) Enter the values in IP address, Gateway IP Address, LAG/Port Number, and Subnet Mask (in bits) for each SSID.

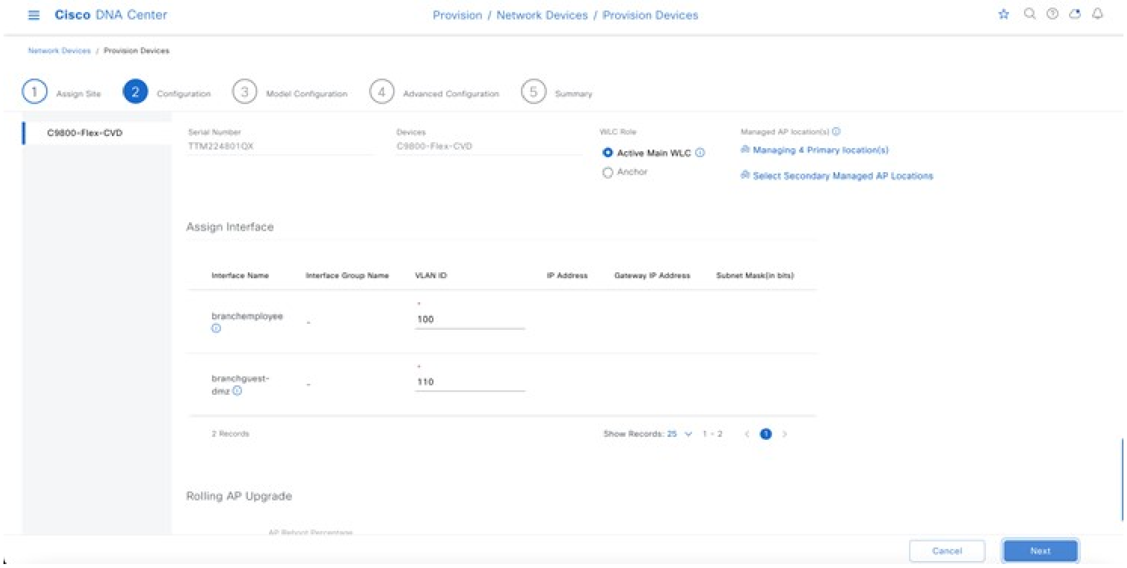
The following table shows the values entered for this deployment guide.

Table 29: Enterprise Wireless Controller Settings

Field	Value
SSID Name	lab3branch5

Field	Value
Interface Name	branchemployee
VLAN ID	100
IP Address	**10.4.160.2**
Gateway IP Address	**10.4.160.1**
LAG/Port Number	1
Subnet Mask (in bits)	24
SSID Name	lab3guest5
Interface Name	branchguest-dmz
VLAN ID	110
IP Address	**10.4.125.2**
Gateway IP Address	**10.4.125.1**
LAG/Port Number	1
Subnet Mask (in bits)	24

Figure 104: Enterprise Wireless Controller Settings in Cisco DNA Center



Serial Number: TTM224801QX

Devices: C9800-Flex-CVD

WLC Role: ● Active Main WLC ○ Anchor

Managed AP location(s): Managing 4 Primary location(s)

Select Secondary Managed AP Locations

Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
branchemployee	-	100			
branchguest-dmz	-	110			

2 Records   Show Records: 25   1 - 2

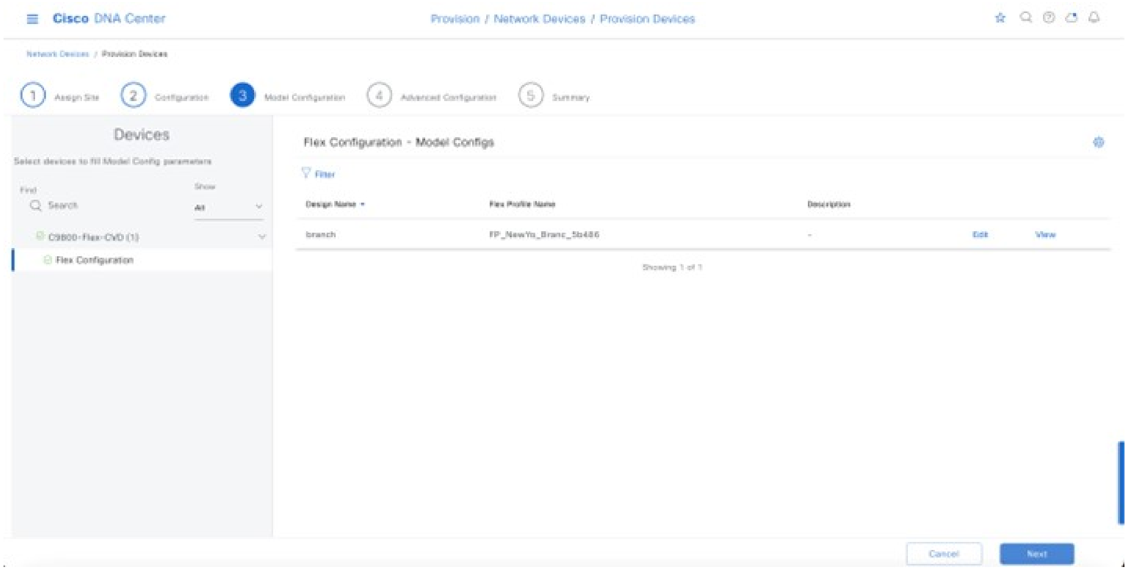
Rolling AP Upgrade

AP Reboot Percentage

f) Click **Next**.

Step 7 The **Model Configuration** window is displayed. If you have configured a template within the **Model configs** for the device type and the site, you can apply the model config here, and you can edit and view the model config of the flex configuration.

Figure 105: Flex Mode Model Config



Flex Configuration - Model Configs

Design Name	Flex Profile Name	Description		
branch	FP_NewYo_Branc_5b486	-	Edit	View

Showing 1 of 1

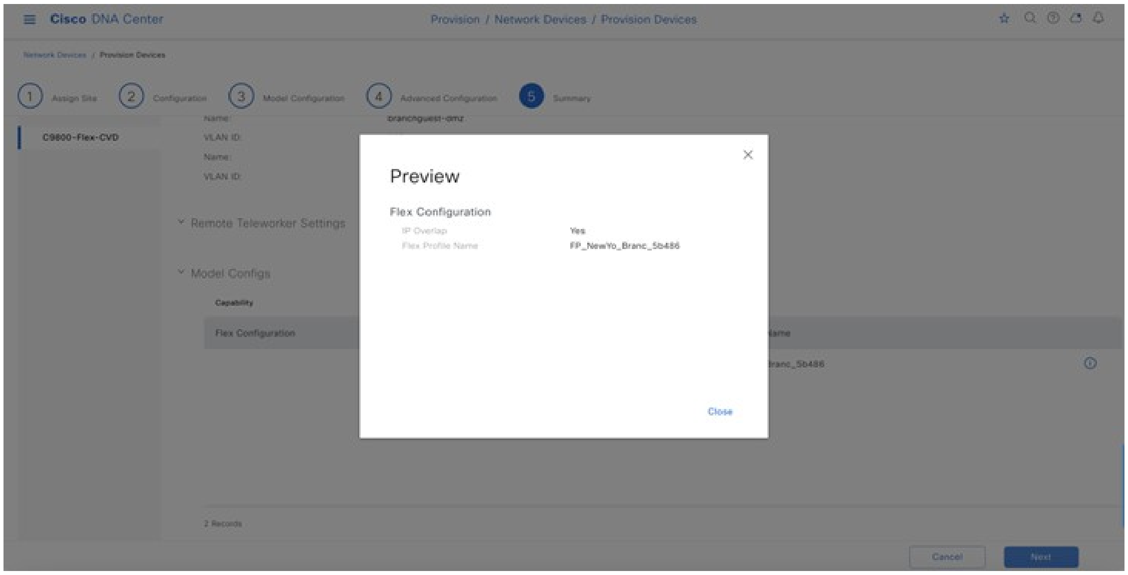
Step 8 Click **Next**.

Step 9 The **Advanced Configuration** window is displayed. If you have configured a template in the **Tools** > **Template Hub** window for the device type and for the site, you can apply the template here. This deployment guide does not discuss the use of templates for advanced configuration of the Catalyst 9800-40 Series Wireless Controller (**C9800-Flex-CVD**).

Step 10 Click **Next**.

Step 11 The **Summary** window is displayed. This window provides a summary of the configuration that will be provisioned to the Catalyst 9800-40 Series Wireless Controller (**C9800-Flex-CVD**).

Figure 106: Flex Mode Device Provisioning Summary



Preview

Flex Configuration

IP Overlap	Yes
Flex Profile Name	FP_NewYo_Branc_5b486

You can expand each area to see the details of the configuration. The configuration is based on the **branch5** wireless profile created during the *Design the wireless network* section of this guide.

Step 12 Click **Deploy** to deploy the configuration to the Catalyst 9800-40 Series Wireless Controller HA SSO pair (**C9800-40-CVD.cagelab.local**).

Note It is best practice to make configuration changes and provision new devices in your network only during scheduled network operation change windows. It is also best practice to preview the configs before they are deployed onto the device.

Step 13 Click **Now** to deploy the configuration immediately or click **Later** to schedule the deployment for a later time.

Step 14 Click **Apply**.

You will be taken back to the **Inventory** window within provisioning.

After the devices are deployed successfully, the provision status changes from **Provisioning** to **Success**.

Step 15 For more information, click **See Details** below the provisioning status of the device.

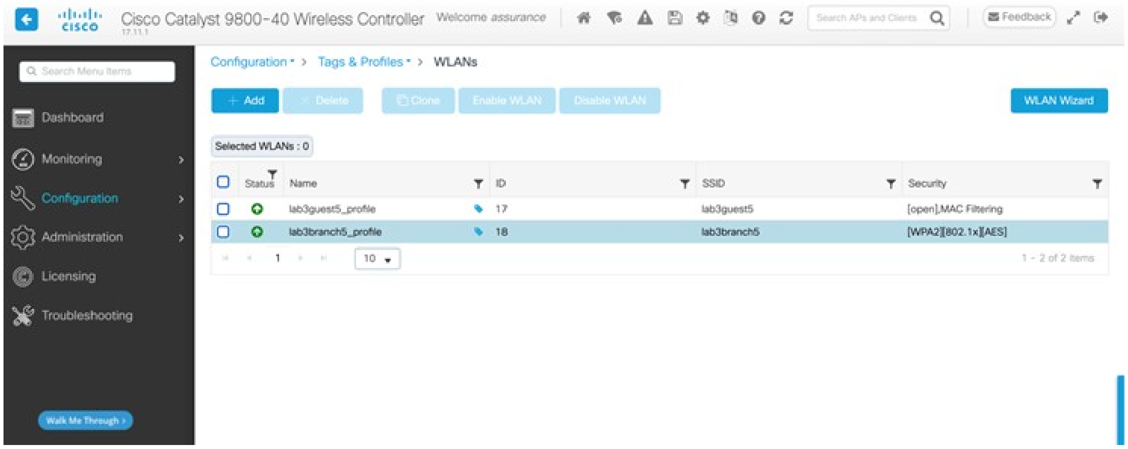
Cisco DNA Center will dynamically create two new WLAN profiles within the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (**C9800-Flex-CVD**). Each WLAN profile has a dynamically generated name, based on the SSID name specified within the **branch5** wireless profile and created during the *Design the wireless network* section of this deployment guide. The following table shows the names of the WLAN profiles and their respective SSIDs, automatically generated by Cisco DNA Center during the provisioning of **C9800-40-CVD.cagelab.local** for this deployment guide.

Table 30: WLAN Profiles Generated by Cisco DNA Center

WLAN Profile Name	SSID	WLAN ID
lab3guest5_profile	lab3guest5	17
lab3branch5_profile	lab3branch5	18

An example of the WLAN configuration in the web-based GUI of **C9800-Flex-CVD.cagelab.local** is shown in the following figure.

Figure 107: Flex WLANs/SSIDs Created by Cisco DNA Center



Selected WLANs : 0

Status	Name	ID	SSID	Security
●	lab3guest5_profile	17	lab3guest5	[open],MAC Filtering
●	lab3branch5_profile	18	lab3branch5	[WPA2][802.1x][AES]

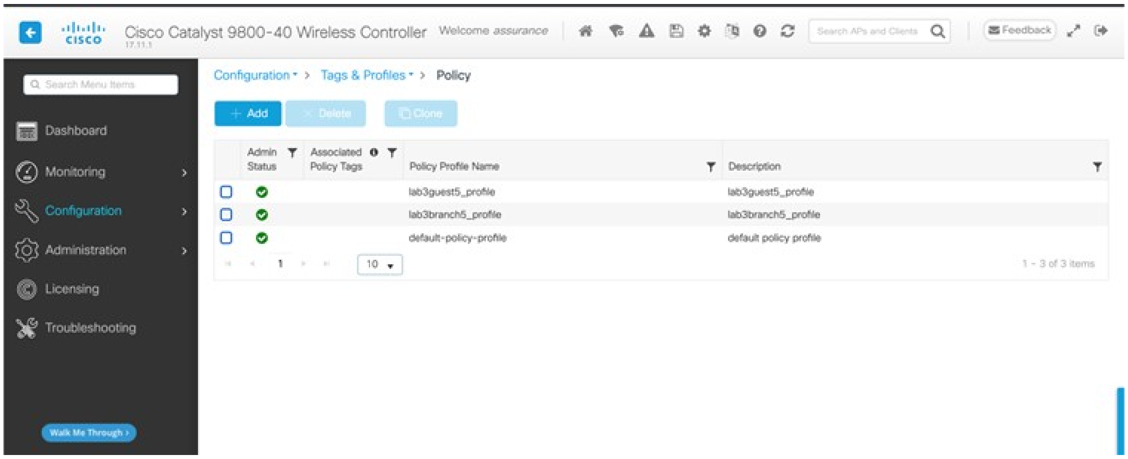
1 10 1 - 2 of 2 items

Note The WLAN IDs corresponding to the two SSIDs, lab3guest5, and lab3branch5 are 17, 18, and 18, respectively. When the APs are assigned the policy tag named **default-policy-tag**, Catalyst 9800 Series Wireless Controllers will broadcast the SSIDs of the WLANs, which have IDs from 1 to 16. To avoid creating WLAN IDs which are broadcast with **default-policy-tag**, Cisco DNA Center creates WLANs/SSIDs beginning with WLAN ID 17 and higher.

During provisioning, Cisco DNA Center also creates two new policy profiles within **C9800-Flex-CVD**. The names of new policy profiles match the names of the created WLAN profiles.

An example of the configuration in the web-based GUI of **C9800-Flex-CVD** is shown in the following figure.

Figure 108: Catalyst 9800 Wireless Controller Policy Profiles Created by Cisco DNA Center for Flex



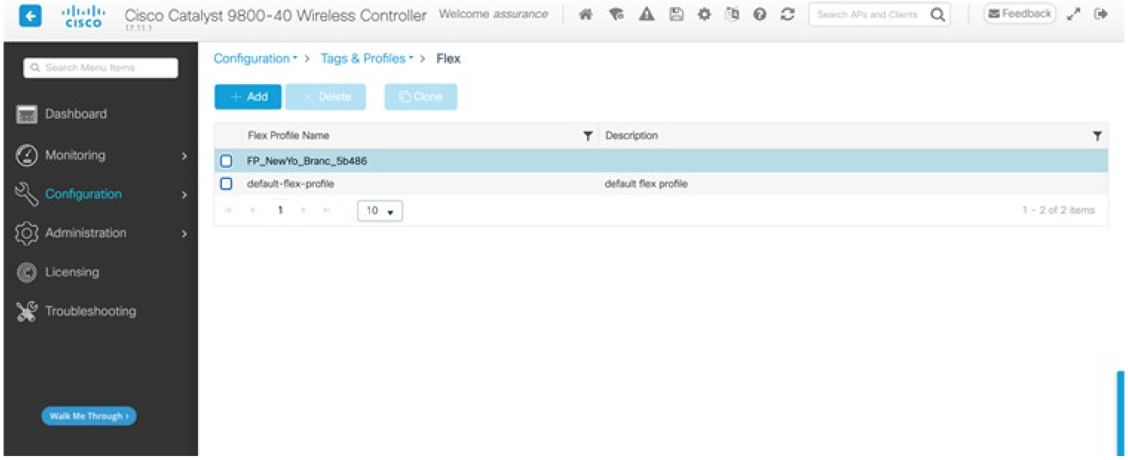
Configuration > Tags & Profiles > Policy

Admin Status	Associated Policy Tags	Policy Profile Name	Description
✓		lab3guest5_profile	lab3guest5_profile
✓		lab3branch5_profile	lab3branch5_profile
✓		default-policy-profile	default policy profile

1 - 3 of 3 items

At this point in the provisioning process, the policy profiles and the WLAN profiles are not mapped to any policy tag that has been applied to any AP. On the controller, Cisco DNA Center creates flex profiles with names generated by Cisco DNA Center.

Figure 109: Flex Profile Window

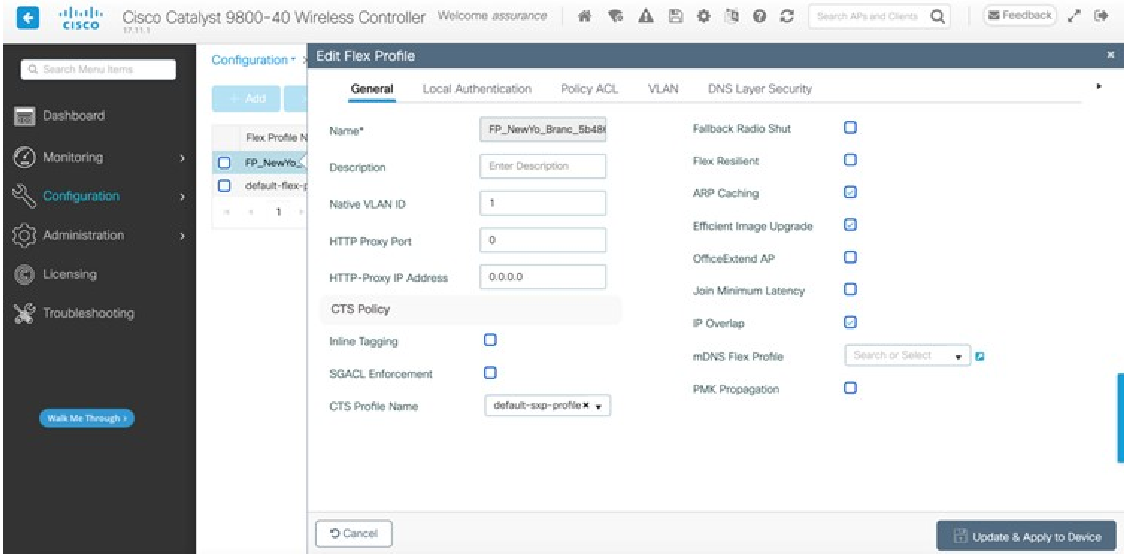


Configuration > Tags & Profiles > Flex

Flex Profile Name	Description
FP_NewYo_Branc_5b486	
default-flex-profile	default flex profile

1 - 2 of 2 items

Figure 110: Edit Flex Profile Dialog Box



Name* FP_NewYo_Branc_5b48

Description Enter Description

Native VLAN ID 1

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

CTS Policy

Inline Tagging □

SGACL Enforcement □

CTS Profile Name default-sxp-profile

Fallback Radio Shut □

Flex Resilient □

ARP Caching ☑

Efficient Image Upgrade ☑

OfficeExtend AP □

Join Minimum Latency □

IP Overlap ☑

mDNS Flex Profile Search or Select

PMK Propagation □

Provision an AP for the N+1 Wireless Controller

The following steps explain how to provision an AP associated with the N+1 wireless controller.

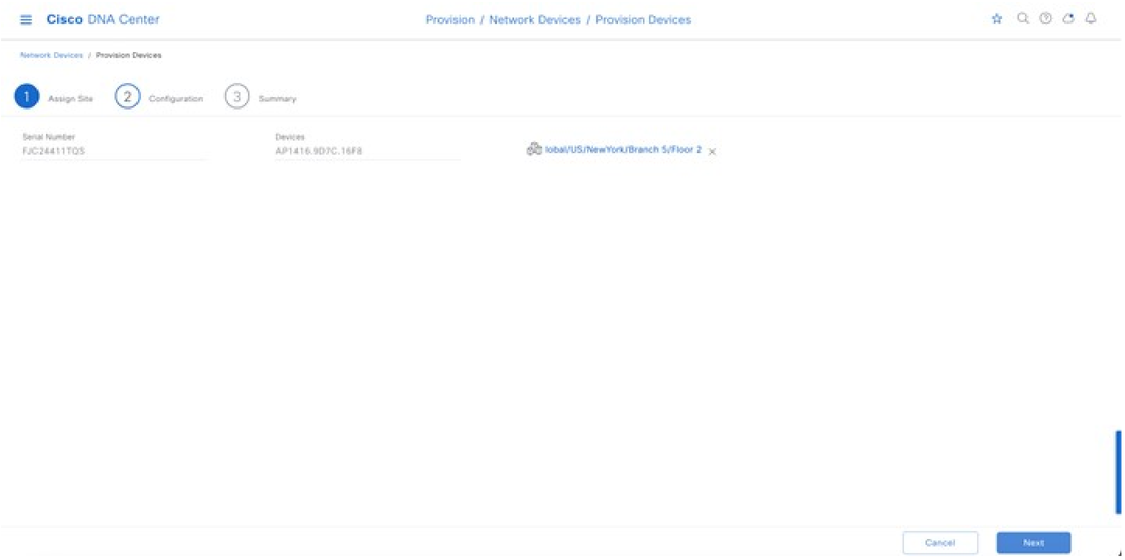
Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

Step 2 Choose the desired AP, and from the **Actions** drop-down list, choose **Provision** > **Provision Device**.

Step 3 Choose **Assign Site** for the AP.

Figure 111: N+1 AP Floor Assignment


Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
Cancel
Next

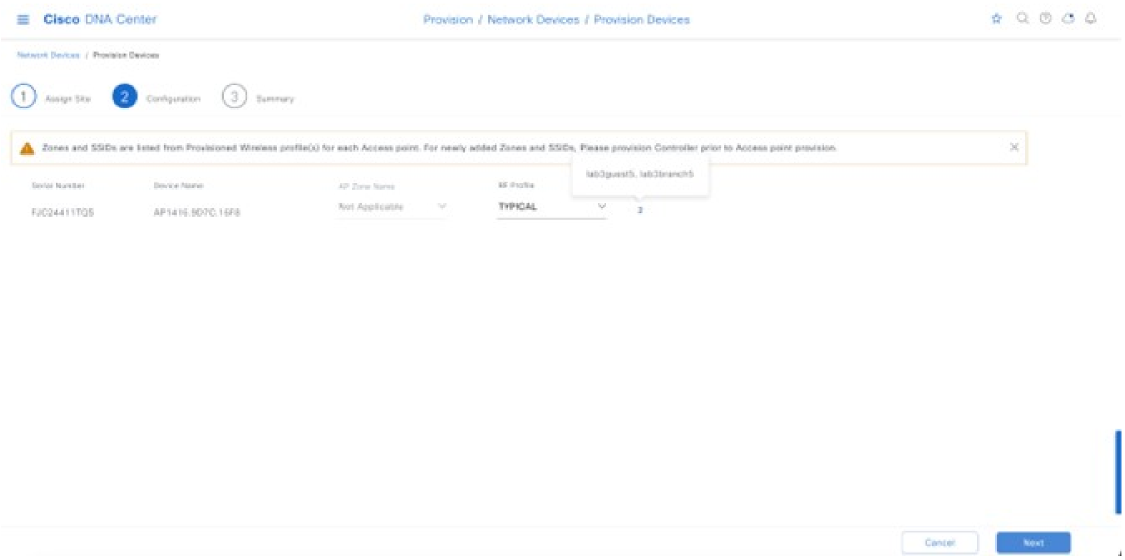
Serial Number: FJC24411TQS

Devices: AP1416.9D7C.16F8

lobal/US/NewYork/Branch 5/Floor 2

The **Configuration** window shows the SSID to be provisioned to the AP.

Figure 112: N+1 AP SSID Based on Wireless Profile


Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
Cancel
Next

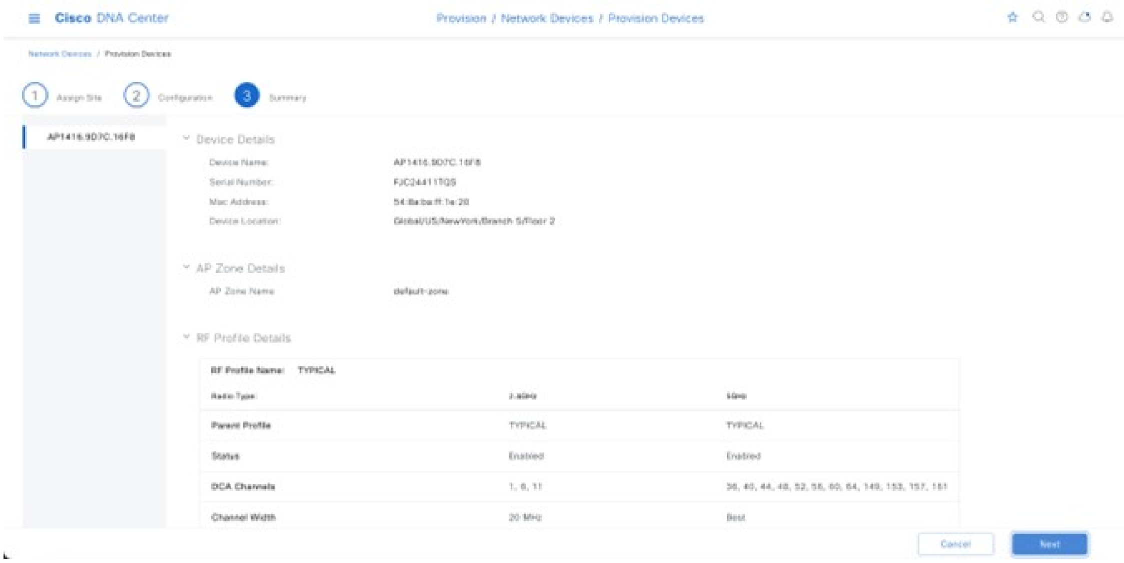
Zones and SSIDs are listed from Provisioned Wireless profile(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision.

Serial Number	Device Name	AP Zone Name	RF Profile	
FJC24411TQS	AP1416.9D7C.16F8	Not Applicable	TYPICAL	2

lab3guest5, lab3branch5

Cisco DNA Center shows the AP summary details before provisioning.

Figure 113: N+1 AP Provision Summary



Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
AP1416.9D7C.16F8
Cancel
Next

Device Details

Device Name: AP1416.9D7C.16F8

Serial Number: FJC24411TQS

Mac Address: 54:8a:ba:ff:1e:20

Device Location: Global/US/NewYork/Branch 5/Floor 2

AP Zone Details

AP Zone Name default-zone

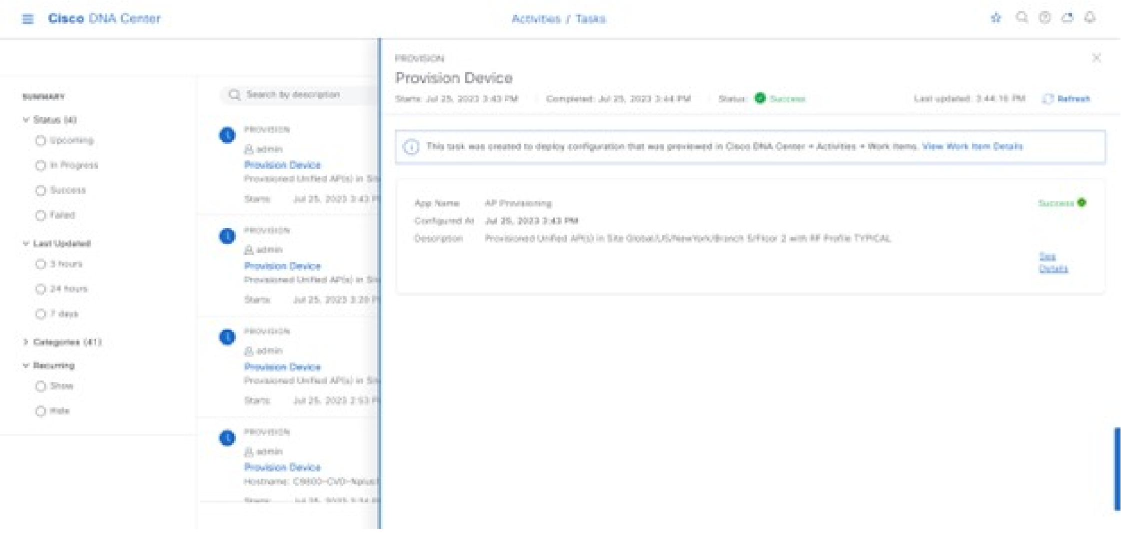
RF Profile Details

RF Profile Name: TYPICAL

Radio Type:	2.4GHz	5GHz
Parent Profile	TYPICAL	TYPICAL
Status	Enabled	Enabled
DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
Channel Width	20 MHz	Best

Step 4 Go to **Activities** > **Tasks** to view the provision status of the AP.

Figure 114: N+1 AP Provision Status



Provisioned Unified AP(s) in Si

Starts: Jul 25, 2023 3:43 P

Provisioned Unified AP(s) in Si

Starts: Jul 25, 2023 3:20 P

Provisioned Unified AP(s) in Si

Starts: Jul 25, 2023 2:53 P

Hostname: C9800-CVD-Nplus1

PROVISION

Provision Device

Starts: Jul 25, 2023 3:43 PM | Completed: Jul 25, 2023 3:44 PM | Status: ● Success | Last updated: 3:44:16 PM

This task was created to deploy configuration that was previewed in Cisco DNA Center > Activities > Work Items. View Work Item Details

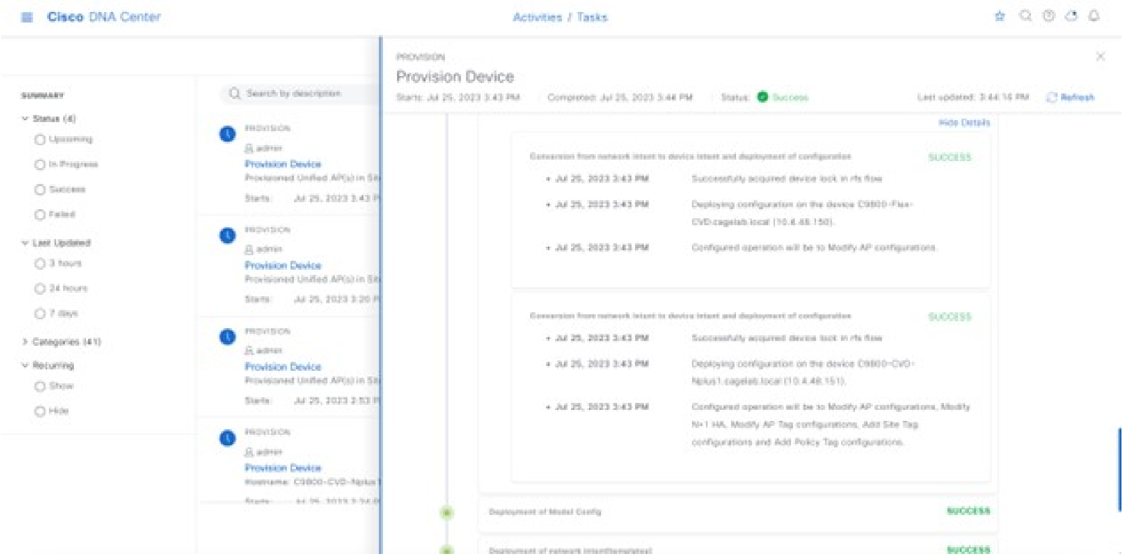
App Name AP Provisioning — Success ●

Configured At Jul 25, 2023 3:43 PM

Description Provisioned Unified AP(s) in Site Global/US/NewYork/Branch 5/Floor 2 with RF Profile TYPICAL

Step 5 After provisioning, check the AP configuration details.

Figure 115: N+1 AP Provision Details



Provision Device

Starts: Jul 25, 2023 3:43 PM | Completed: Jul 25, 2023 3:44 PM | Status: Success | Last updated: 3:44:16 PM | Refresh

Hide Details

Conversion from network intent to device intent and deployment of configuration — SUCCESS

- Jul 25, 2023 3:43 PM — Successfully acquired device lock in rfs flow
- Jul 25, 2023 3:43 PM — Deploying configuration on the device C9800-Flex-CVD.cagelab.local (10.4.48.150).
- Jul 25, 2023 3:43 PM — Configured operation will be to Modify AP configurations.

Conversion from network intent to device intent and deployment of configuration — SUCCESS

- Jul 25, 2023 3:43 PM — Successfully acquired device lock in rfs flow
- Jul 25, 2023 3:43 PM — Deploying configuration on the device C9800-CVD-Nplus1.cagelab.local (10.4.48.151).
- Jul 25, 2023 3:43 PM — Configured operation will be to Modify AP configurations, Modify N+1 HA, Modify AP Tag configurations, Add Site Tag configurations and Add Policy Tag configurations.

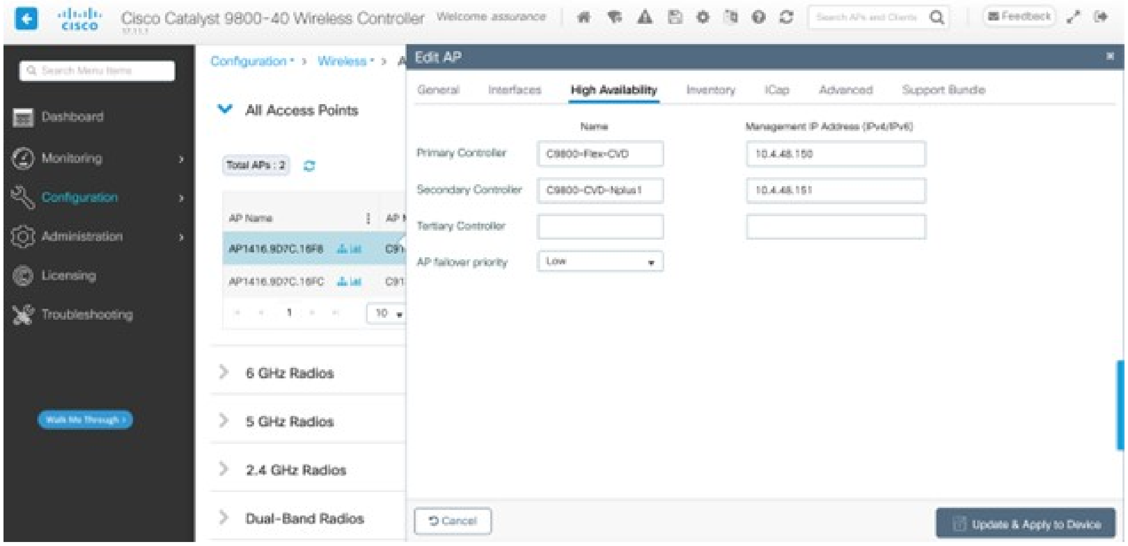
Deployment of Model Config — SUCCESS

Deployment of network intent(templates) — SUCCESS

Step 6 Check the AP configuration on the wireless controller. The AP should correctly show high availability of the primary and secondary controllers.

The AP joins the primary controller after the reboot, and the AP will be able to join the secondary controller if the primary controller is unreachable. Included in the N+1 controller provision and the AP-joined primary controller, the primary controller and the secondary controller details were changed in the high availability of the AP.

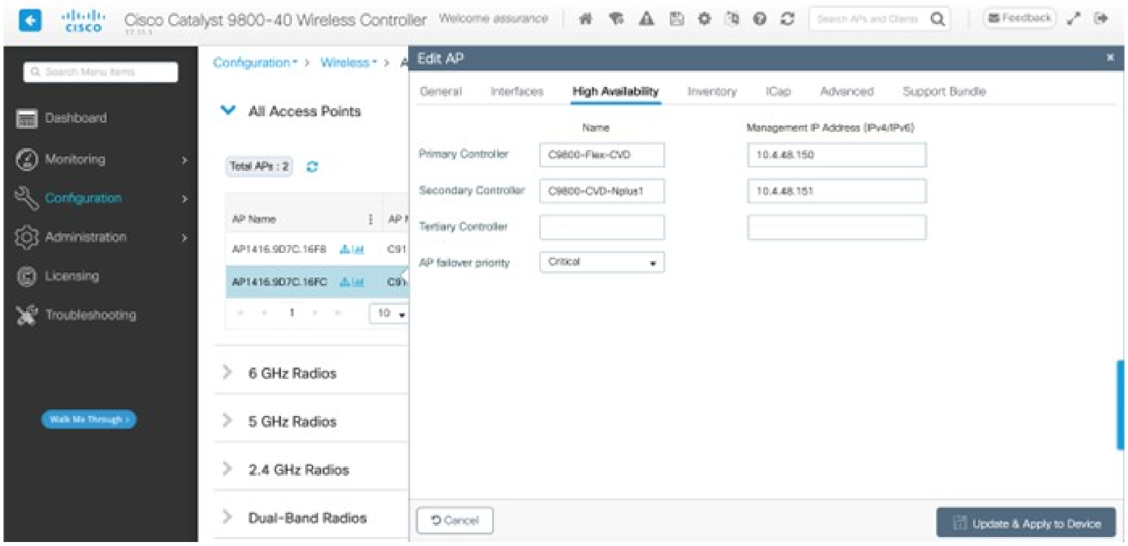
Figure 116: N+1 AP Showing the Primary and Secondary Wireless Controllers



	Name	Management IP Address (IPv4/IPv6)
Primary Controller	C9800-Flex-CVD	10.4.48.150
Secondary Controller	C9800-CVD-Nplus1	10.4.48.151
Tertiary Controller		
AP failover priority	Low	

Step 7 Repeat the procedure to provision the second AP on **Floor 2** of **Branch 5** and verify that the primary and secondary wireless controllers are configured correctly, as shown in following figure.

Figure 117: N+1 AP Assigned Primary and Secondary Wireless Controllers for Second AP



Total APs : 2

AP Name
AP1416.9D7C.16F8
AP1416.9D7C.16FC

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	C9800-Flex-CVD	10.4.48.150
Secondary Controller	C9800-CVD-Nplus1	10.4.48.151
Tertiary Controller		

AP failover priority: Critical

Configure the N+1 Wireless Controller for FlexConnect

For this guide, the Cisco Catalyst 9800-40 Wireless Controller is named Cisco Catalyst 9800-CVD-Nplus1.cagelab.local, serving as the N+1 controller (secondary controller) for Cisco Catalyst 9800-Flex-CVD.cagelab.local (primary controller).

Perform the following steps to deploy the N+1 controller, assuming the N+1 controller is present in the same site as the primary controller.

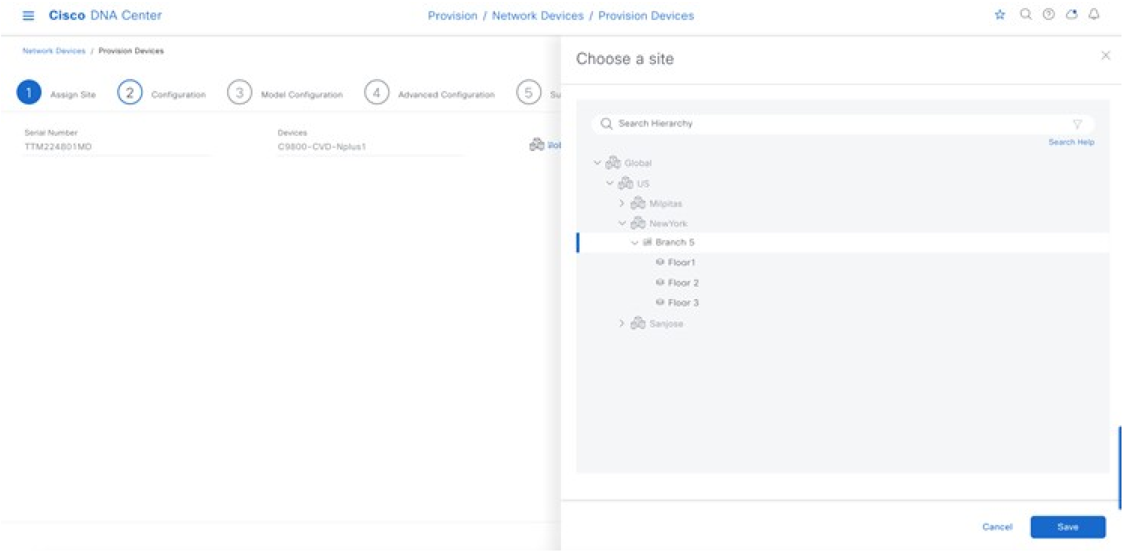
Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory** and choose the N+1 controller.

Step 2 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

Step 3 In the **Assign Site** window, assign the site to N+1 controller and to the **Branch 5** building location, as shown in the following figure.

Figure 118: Assign the Site to the N+1 Controller

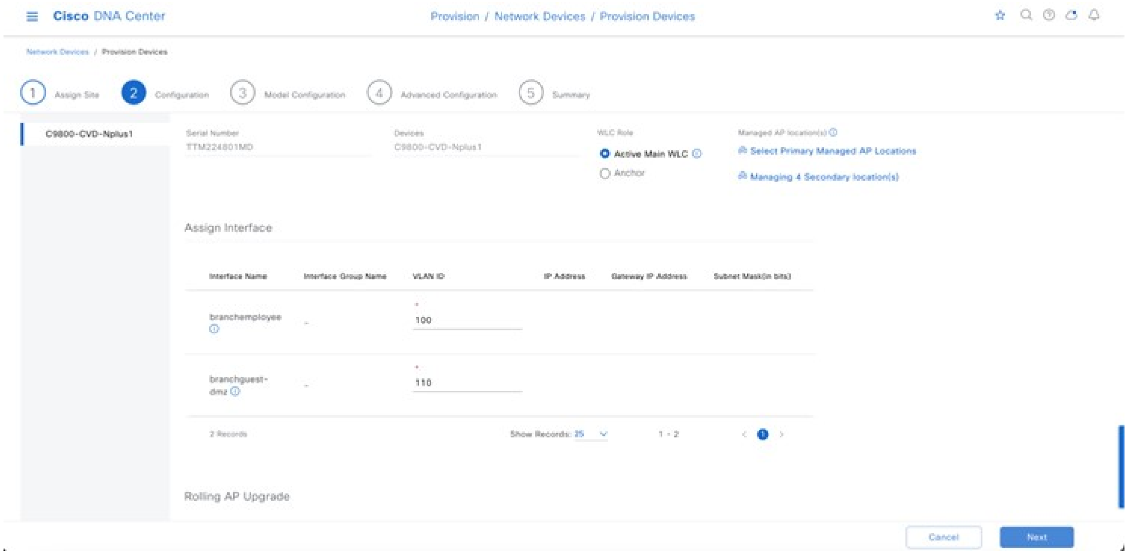


Serial Number: TTM224801MD

Devices: C9800-CVD-Nplus1

Step 4 In the **Configuration** window, click **Managing Secondary Locations**, which manages the primary controller AP.

Figure 119: Configuration for N+1 Controller


Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Model Configuration
4 Advanced Configuration
5 Summary
C9800-CVD-Nplus1
Select Primary Managed AP Locations
Managing 4 Secondary location(s)
Rolling AP Upgrade
Cancel
Next

Serial Number: TTM224801MD

Devices: C9800-CVD-Nplus1

WLC Role: ● Active Main WLC ○ Anchor

Managed AP location(s)

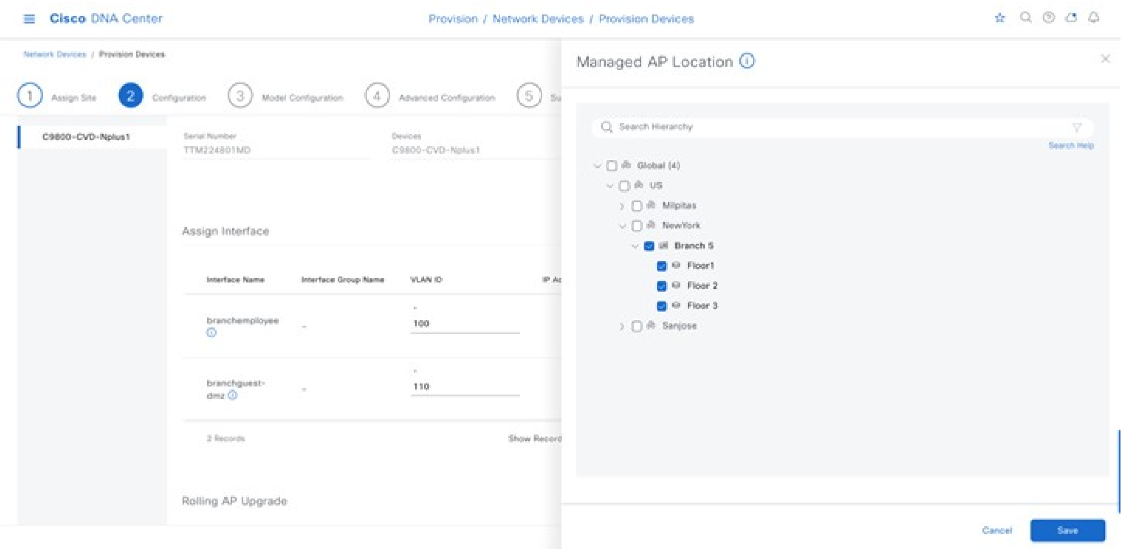
Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
branchemployee	-	100			
branchguest-dmz	-	110			

2 Records Show Records: 25 1 - 2

Step 5 Choose the floors managed by the primary controller.

Figure 120: Managed AP Location Selection



Serial Number: TTM224801MD

Devices: C9800-CVD-Nplus1

Interface Name	Interface Group Name	VLAN ID	IP Ac
branchemployee	-	100	
branchguest-dmz	-	110	

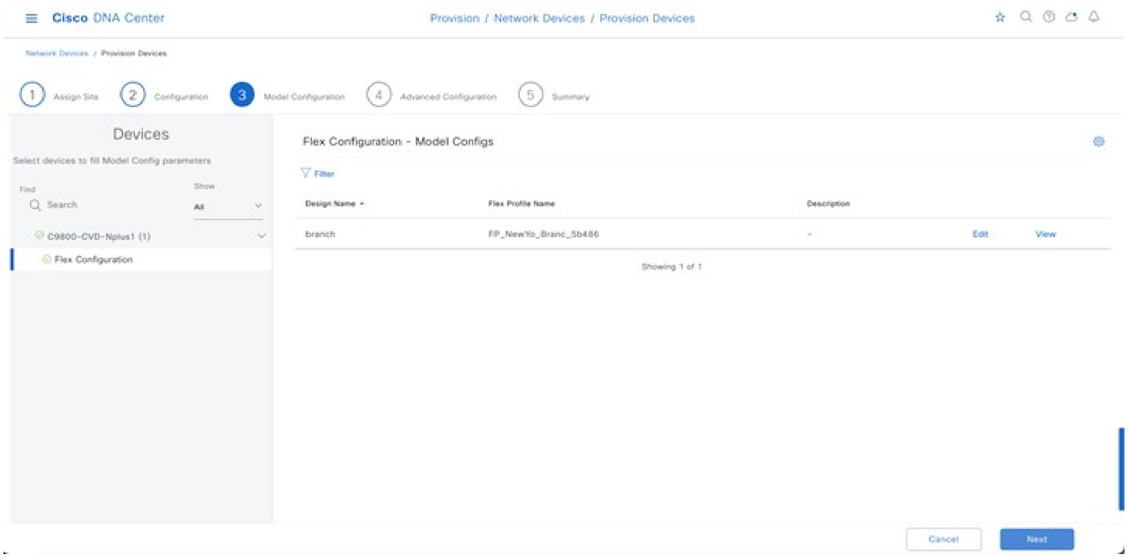
2 Records

Show Record

- ☐ Global (4)
  - ☐ US
    - ☐ Milpitas
    - ☐ NewYork
      - ☑ Branch 5
        - ☑ Floor1
        - ☑ Floor 2
        - ☑ Floor 3
    - ☐ Sanjose

Cisco DNA Center will automatically recognize the model config with the flex configuration as a part of the primary controller.

Figure 121: N+1 Wireless Controller with Flex Model Configuration

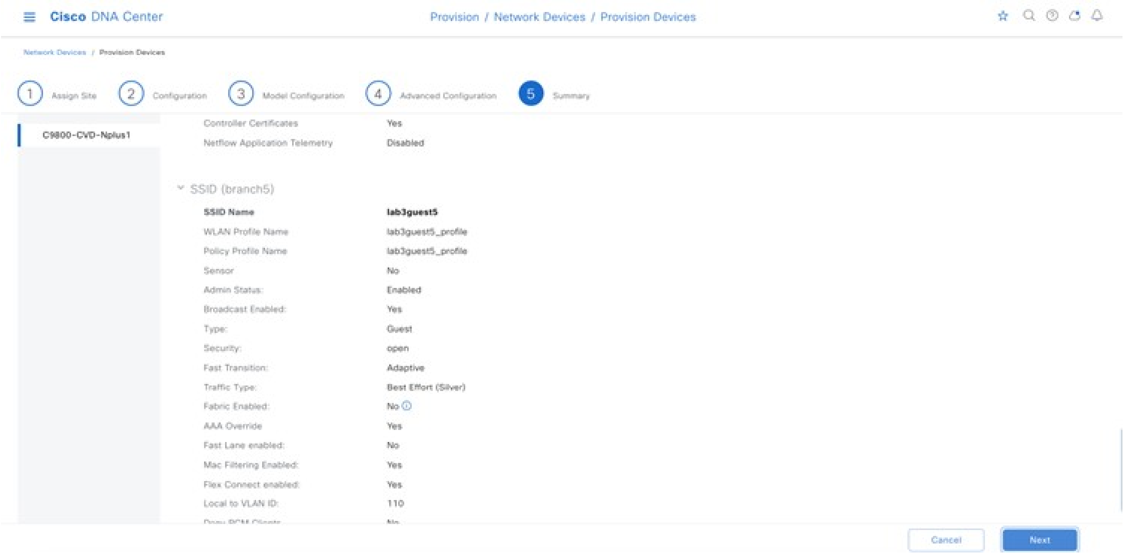


Design Name	Flex Profile Name	Description		
branch	FP_NewYo_Branc_5b486	-	Edit	View

Showing 1 of 1

Step 6 In the **Summary** window, you can review the details of the SSID, sites, and network settings configuration before deployment.

Figure 122: N+1 Wireless Controller Provision Summary Window



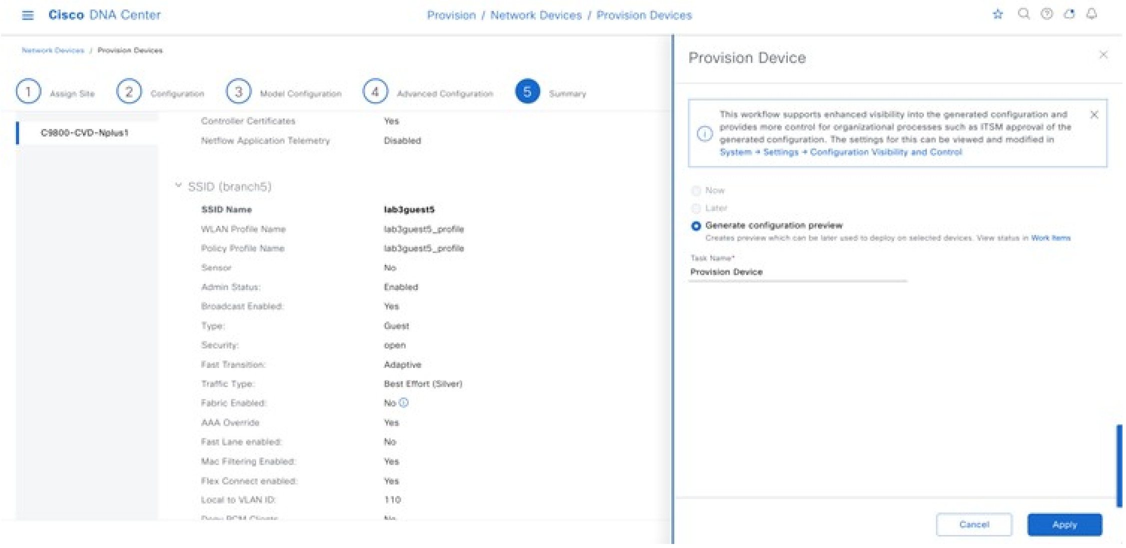
Controller Certificates	Yes
Netflow Application Telemetry	Disabled

˅ SSID (branch5)

SSID Name	**lab3guest5**
WLAN Profile Name	lab3guest5_profile
Policy Profile Name	lab3guest5_profile
Sensor	No
Admin Status:	Enabled
Broadcast Enabled:	Yes
Type:	Guest
Security:	open
Fast Transition:	Adaptive
Traffic Type:	Best Effort (Silver)
Fabric Enabled:	No ⓘ
AAA Override	Yes
Fast Lane enabled:	No
Mac Filtering Enabled:	Yes
Flex Connect enabled:	Yes
Local to VLAN ID:	110
Deny RCM Clients:	No

Step 7 Choose the **Generate Configuration Preview** radio button to review the configuration before deployment.

Figure 123: N+1 Wireless Controller Config Preview



Controller Certificates	Yes
Netflow Application Telemetry	Disabled

˅ SSID (branch5)

SSID Name	**lab3guest5**
WLAN Profile Name	lab3guest5_profile
Policy Profile Name	lab3guest5_profile
Sensor	No
Admin Status:	Enabled
Broadcast Enabled:	Yes
Type:	Guest
Security:	open
Fast Transition:	Adaptive
Traffic Type:	Best Effort (Silver)
Fabric Enabled:	No ⓘ
AAA Override	Yes
Fast Lane enabled:	No
Mac Filtering Enabled:	Yes
Flex Connect enabled:	Yes
Local to VLAN ID:	110
Deny RCM Clients:	No

This workflow supports enhanced visibility into the generated configuration and provides more control for organizational processes such as ITSM approval of the generated configuration. The settings for this can be viewed and modified in System → Settings → Configuration Visibility and Control

○ Now

○ Later

● Generate configuration preview

Creates preview which can be later used to deploy on selected devices. View status in Work Items

Task Name*

Provision Device

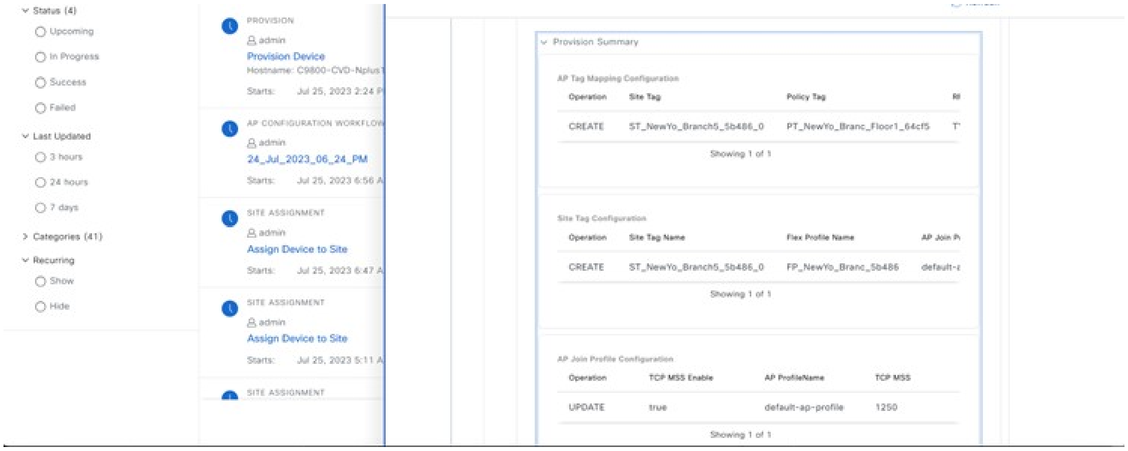
Step 8 Click **Apply**.

Step 9 Choose **Activities** > **Task**.

Cisco DNA Center should provision the controller successfully.

Cisco DNA Center applies the same configurations from the primary controller to the N+1 controller. The following figures show the provision summary.

Figure 124: N+1 Provision Status - Part 1



- Status (4)
  - ○ Upcoming
  - ○ In Progress
  - ○ Success
  - ○ Failed
- Last Updated
  - ○ 3 hours
  - ○ 24 hours
  - ○ 7 days
- Categories (41)
- Recurring
  - ○ Show
  - ○ Hide

PROVISION
admin
Provision Device
Hostname: C9800-CVD-Nplus1
Starts: Jul 25, 2023 2:24 P

AP CONFIGURATION WORKFLOW
admin
24_Jul_2023_06_24_PM
Starts: Jul 25, 2023 6:56 A

SITE ASSIGNMENT
admin
Assign Device to Site
Starts: Jul 25, 2023 6:47 A

SITE ASSIGNMENT
admin
Assign Device to Site
Starts: Jul 25, 2023 5:11 A

SITE ASSIGNMENT

Provision Summary

AP Tag Mapping Configuration

Operation	Site Tag	Policy Tag	Rf
CREATE	ST_NewYo_Branch5_5b486_0	PT_NewYo_Branc_Floor1_64cf5	T'

Showing 1 of 1

Site Tag Configuration

Operation	Site Tag Name	Flex Profile Name	AP Join P
CREATE	ST_NewYo_Branch5_5b486_0	FP_NewYo_Branc_5b486	default-:

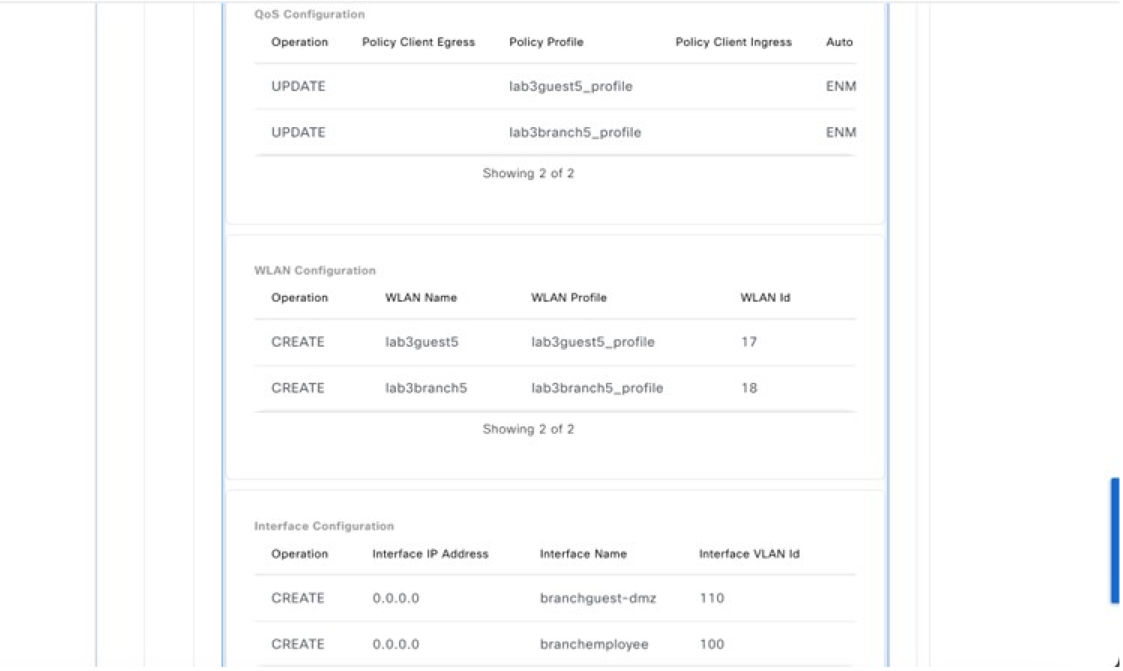
Showing 1 of 1

AP Join Profile Configuration

Operation	TCP MSS Enable	AP ProfileName	TCP MSS
UPDATE	true	default-ap-profile	1250

Showing 1 of 1

Figure 125: N+1 Provision Status - Part 2



QoS Configuration

Operation	Policy Client Egress	Policy Profile	Policy Client Ingress	Auto
UPDATE		lab3guest5_profile		ENM
UPDATE		lab3branch5_profile		ENM

Showing 2 of 2

WLAN Configuration

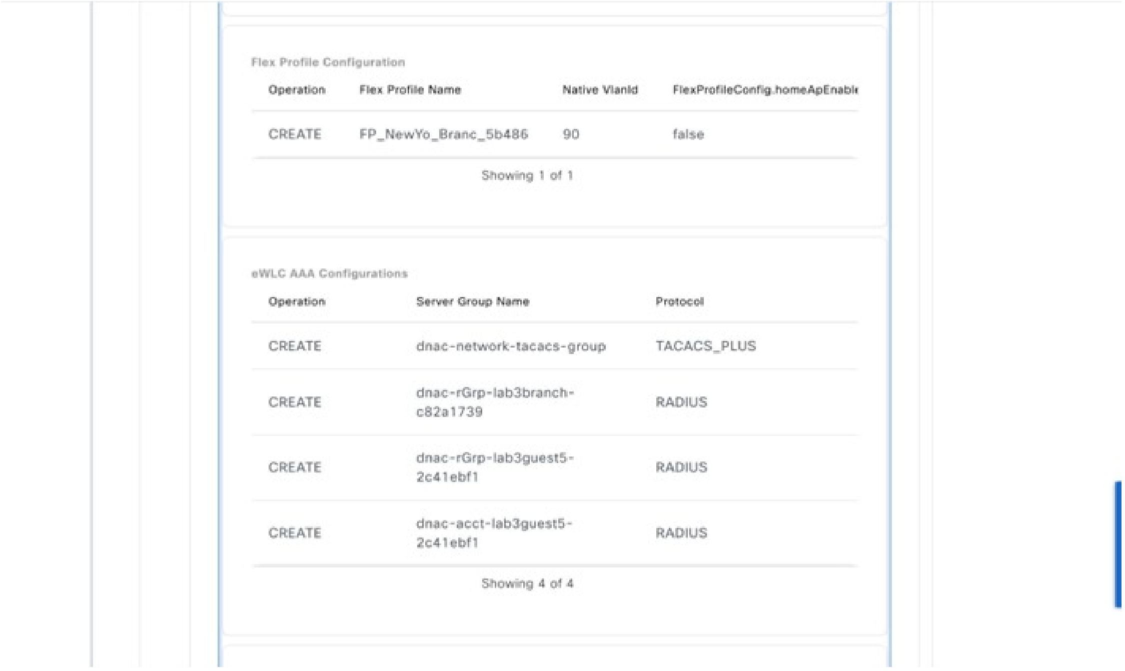
Operation	WLAN Name	WLAN Profile	WLAN Id
CREATE	lab3guest5	lab3guest5_profile	17
CREATE	lab3branch5	lab3branch5_profile	18

Showing 2 of 2

Interface Configuration

Operation	Interface IP Address	Interface Name	Interface VLAN Id
CREATE	0.0.0.0	branchguest-dmz	110
CREATE	0.0.0.0	branchemployee	100

Figure 126: N+1 Provision Status - Part 3



Flex Profile Configuration

Operation	Flex Profile Name	Native VlanId	FlexProfileConfig.homeApEnabl
CREATE	FP_NewYo_Branc_5b486	90	false

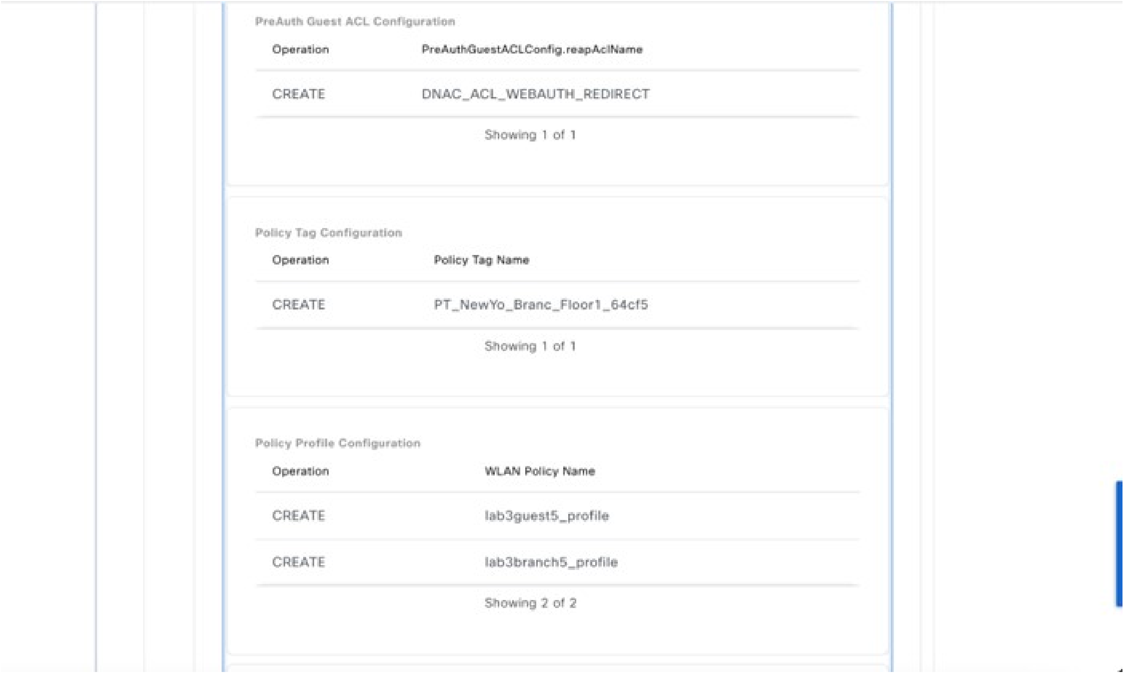
Showing 1 of 1

eWLC AAA Configurations

Operation	Server Group Name	Protocol
CREATE	dnac-network-tacacs-group	TACACS_PLUS
CREATE	dnac-rGrp-lab3branch-c82a1739	RADIUS
CREATE	dnac-rGrp-lab3guest5-2c41ebf1	RADIUS
CREATE	dnac-acct-lab3guest5-2c41ebf1	RADIUS

Showing 4 of 4

Figure 127: N+1 Provision Status - Part 4



PreAuth Guest ACL Configuration

Operation	PreAuthGuestACLConfig.reapAclName
CREATE	DNAC_ACL_WEBAUTH_REDIRECT

Showing 1 of 1

Policy Tag Configuration

Operation	Policy Tag Name
CREATE	PT_NewYo_Branc_Floor1_64cf5

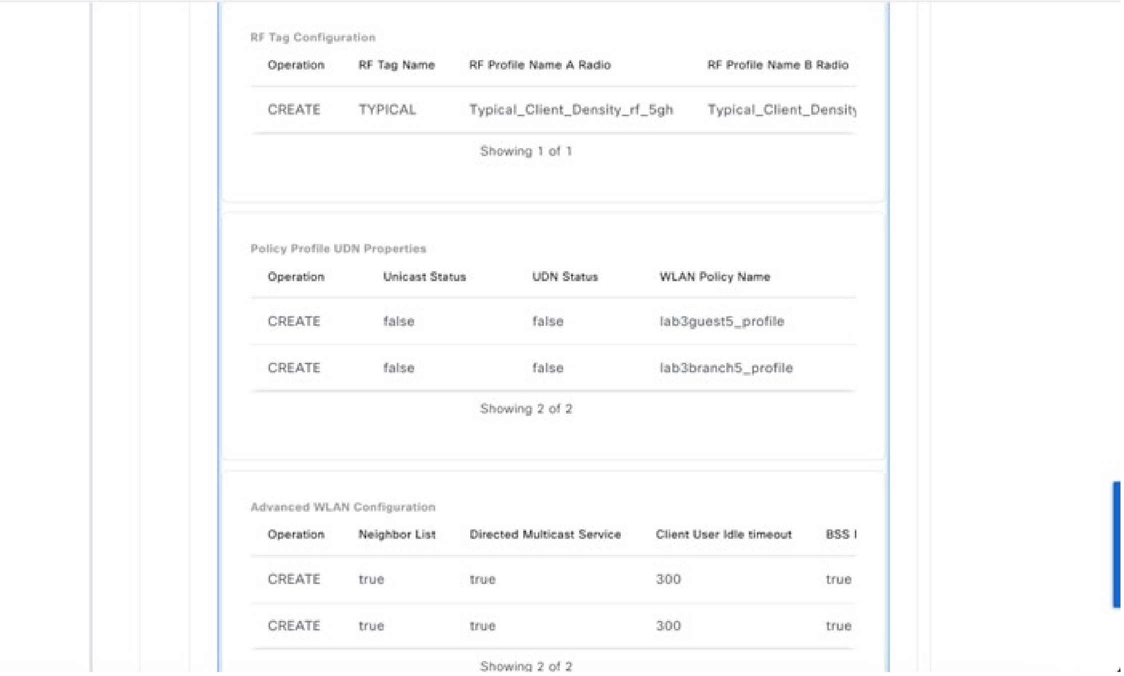
Showing 1 of 1

Policy Profile Configuration

Operation	WLAN Policy Name
CREATE	lab3guest5_profile
CREATE	lab3branch5_profile

Showing 2 of 2

Figure 128: N+1 Provision Status - Part 5



RF Tag Configuration

Operation	RF Tag Name	RF Profile Name A Radio	RF Profile Name B Radio
CREATE	TYPICAL	Typical_Client_Density_rf_5gh	Typical_Client_Density

Showing 1 of 1

Policy Profile UDN Properties

Operation	Unicast Status	UDN Status	WLAN Policy Name
CREATE	false	false	lab3guest5_profile
CREATE	false	false	lab3branch5_profile

Showing 2 of 2

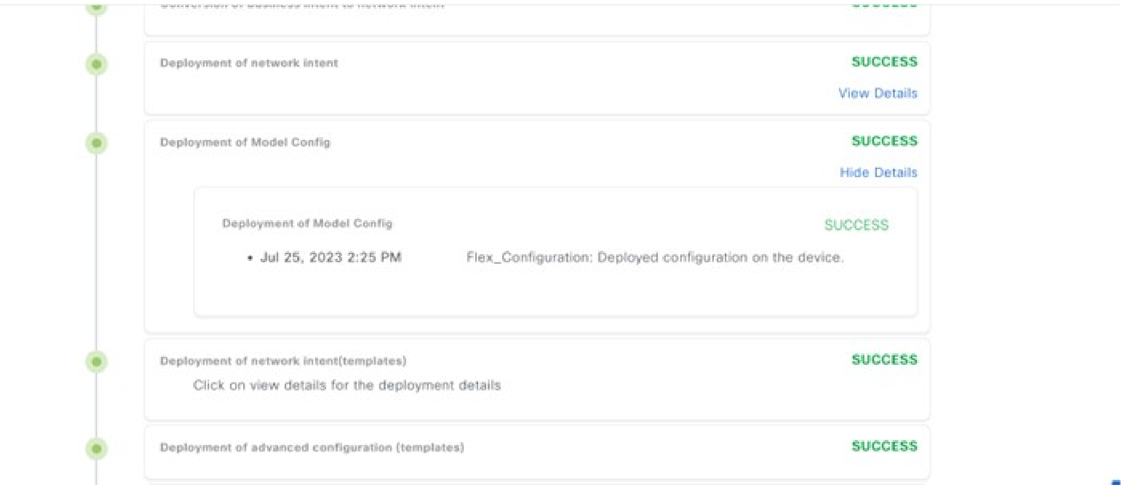
Advanced WLAN Configuration

Operation	Neighbor List	Directed Multicast Service	Client User Idle timeout	BSS I
CREATE	true	true	300	true
CREATE	true	true	300	true

Showing 2 of 2

The following figure displays the flex configuration using a model config.

Figure 129: N+1 Model Provision Status



Deployment of network intent — SUCCESS — View Details

Deployment of Model Config — SUCCESS — Hide Details

Deployment of Model Config — SUCCESS

- Jul 25, 2023 2:25 PM Flex_Configuration: Deployed configuration on the device.

Deployment of network intent(templates) — SUCCESS

Click on view details for the deployment details

Deployment of advanced configuration (templates) — SUCCESS

Create AP Zones for Onboarding Two SSIDs with Different Sets of APs on the Same Floor

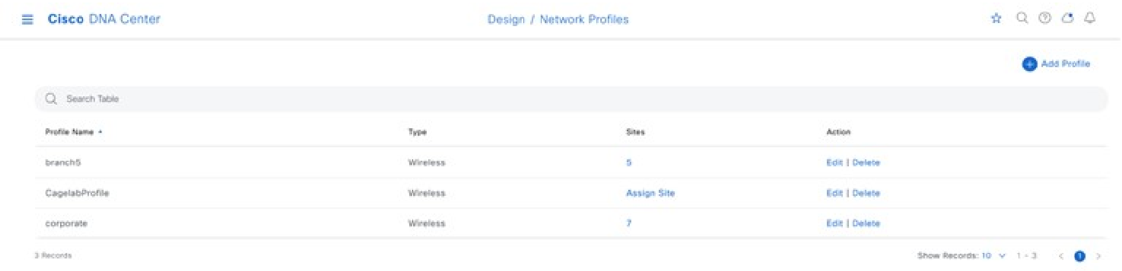
An AP zone allows you to associate different SSIDs and RF profiles for a set of APs on the same site. You can use device tags to identify the APs for which you want to apply the AP zone. From the **AP Zones** tab within the wireless profile, you can create separate AP zones with a subset of SSIDs configured in the network profile for a device tag. Cisco DNA Center applies the AP zone configurations to APs during provisioning.

In this guide, two zones will be created in New York, building Branch 5, Floor 1. There will be two APs on the floor: one AP will be in zone1 broadcasting corporate SSID, and the other AP will be in zone2 broadcasting the guest SSID.

The following steps explain how to create two AP zones and provision the APs to be configured with these zones:

1. From the top-left corner, click the menu icon and choose **Design** > **Network Profiles** and click **Edit** for the **Corporate** network profile.

Figure 130: AP Zone: Network Profile Window



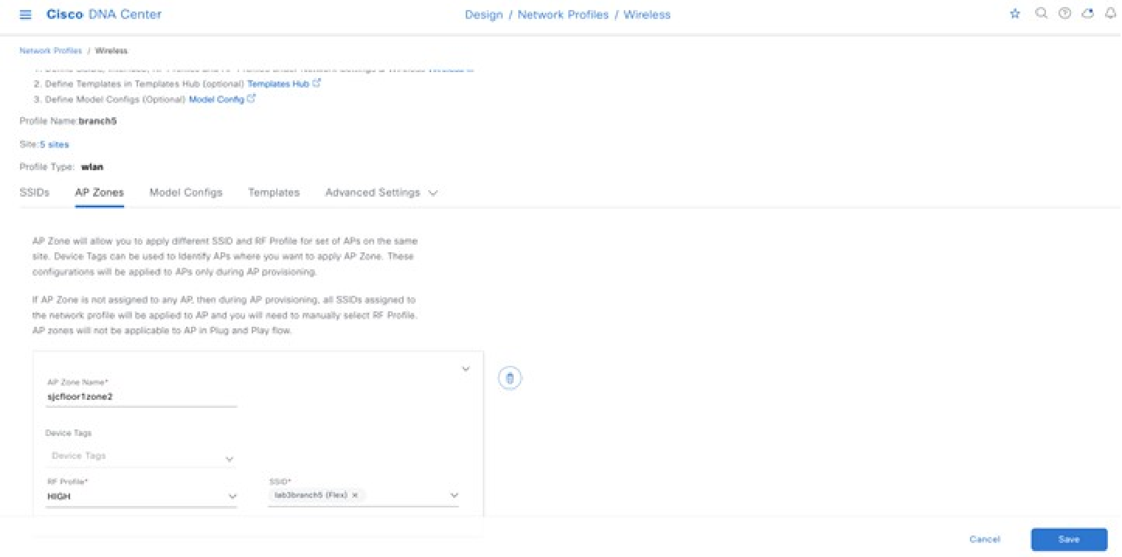
Profile Name	Type	Sites	Action
branch5	Wireless	5	Edit | Delete
CagelabProfile	Wireless	Assign Site	Edit | Delete
corporate	Wireless	7	Edit | Delete

3 Records

Show Records: 10 1 - 3

2. Click the **AP Zones** tab, and create two AP zones. Name the first zone sjcfloor1zone2 for lab3branch5 SSID with RF profiles: High, and name the other AP zone sjcfloor1zone1 for lab3guest5 SSID with RF Profiles: Low.

Figure 131: AP Zone1 Created Under Network Profile



2. Define Templates in Templates Hub (optional) Templates Hub
3. Define Model Configs (Optional) Model Config

Profile Name: branch5

Site: 5 sites

Profile Type: wlan

AP Zone will allow you to apply different SSID and RF Profile for set of APs on the same site. Device Tags can be used to Identify APs where you want to apply AP Zone. These configurations will be applied to APs only during AP provisioning.

If AP Zone is not assigned to any AP, then during AP provisioning, all SSIDs assigned to the network profile will be applied to AP and you will need to manually select RF Profile. AP zones will not be applicable to AP in Plug and Play flow.

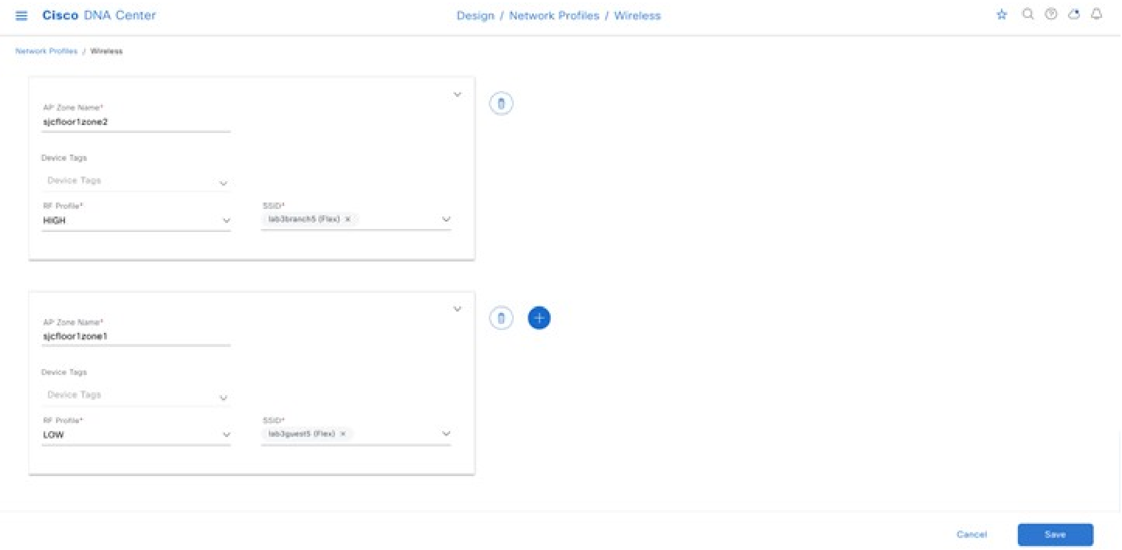
AP Zone Name*: sjcfloor1zone2

Device Tags: Device Tags

RF Profile*: HIGH

SSID*: lab3branch5 (Flex)

Figure 132: AP Zone2 Created Under Network Profile



Cisco DNA Center
Design / Network Profiles / Wireless
Network Profiles / Wireless

AP Zone Name*: sjcfloor1zone2
Device Tags: Device Tags
RF Profile*: HIGH
SSID*: lab3branch5 (Flex) ×

AP Zone Name*: sjcfloor1zone1
Device Tags: Device Tags
RF Profile*: LOW
SSID*: lab3guest5 (Flex) ×

3. Click **Save**.

Note Cisco DNA Center does not apply AP zone configurations to the APs claimed from the Plug and Play (PnP) process.

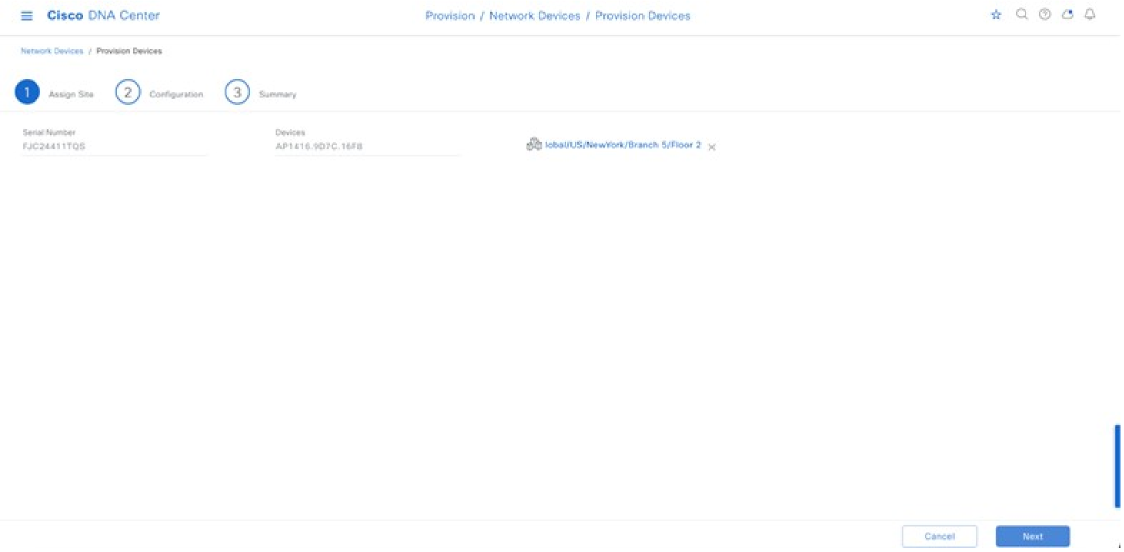
If an AP zone is already provisioned on an AP and if an AP zone configuration is later updated, the wireless controller must be reprovisioned to apply the updates. Reprovisioning the AP is not necessary.

During AP provisioning, based on the device tag and site of the AP, Cisco DNA Center chooses the corresponding AP zone and automatically assigns the RF profile. If two AP zones are configured for an AP, you can choose the required AP zone. If there are no AP zones for an AP, you can choose the required RF profile. Before creating an AP zone, ensure that you have created wireless SSIDs under the **Design** > **Network Settings** > **Wireless** tab. To apply the AP zone configuration to an AP, reprovision the wireless controller.

Provision One AP to Zone Named sjcfloor1zone1 for lab3guest5 SSID with RF Profiles: Low

1. From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.
2. Choose the AP and from the **Actions** drop-down menu, and choose **Provision** > **Provision Devices**.
3. Choose the site for the AP and click **Next**.

Figure 133: AP Zone Provision – Site Selection


Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
Cancel
Next

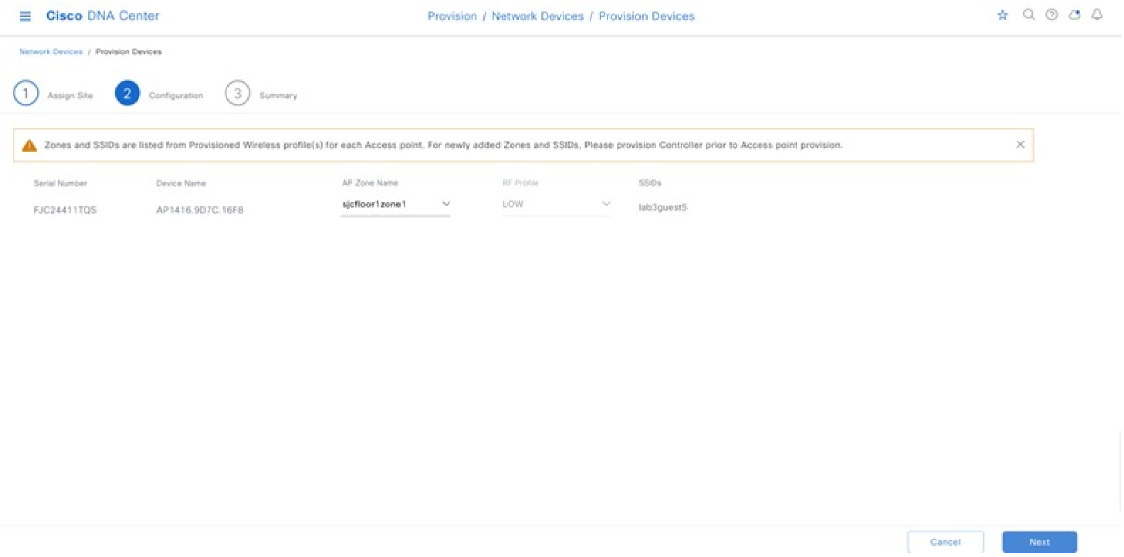
Serial Number: FJC24411TQS

Devices: AP1416.9D7C.16F8

lobal/US/NewYork/Branch 5/Floor 2

4. Choose the AP zone from the drop-down list.

Figure 134: AP Zone Provision – Zone Selection

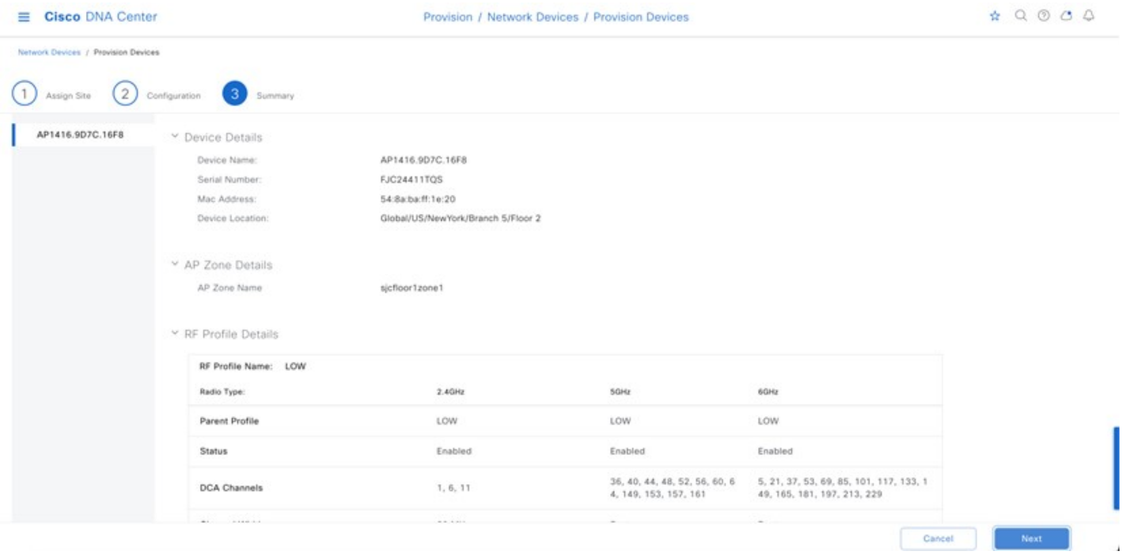

Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
Cancel
Next

Zones and SSIDs are listed from Provisioned Wireless profile(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision.

Serial Number	Device Name	AP Zone Name	RF Profile	SSIDs
FJC24411TQS	AP1416.9D7C.16F8	sjcfloor1zone1	LOW	lab3guest5

5. Review the details in the **Summary** window and click **Next**.

Figure 135: AP Zone Provision Summary



≡ Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
AP1416.9D7C.16F8
Cancel
Next

Device Details

Device Name: AP1416.9D7C.16F8
Serial Number: FJC24411TQS
Mac Address: 54:8a:ba:ff:1e:20
Device Location: Global/US/NewYork/Branch 5/Floor 2

AP Zone Details

AP Zone Name sjcfloor1zone1

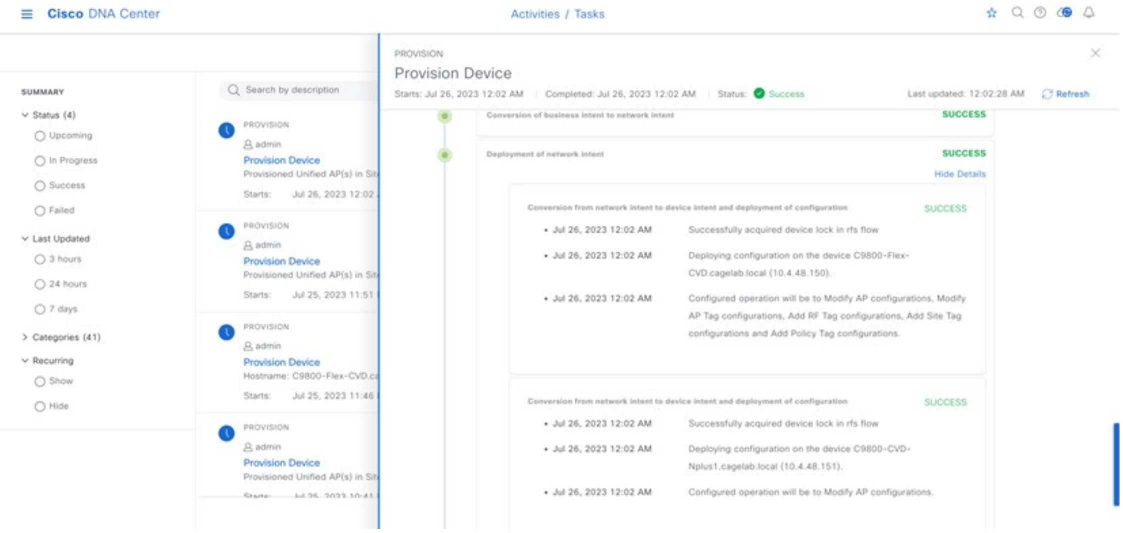
RF Profile Details

RF Profile Name: LOW

Radio Type:	2.4GHz	5GHz	6GHz
Parent Profile	LOW	LOW	LOW
Status	Enabled	Enabled	Enabled
DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213, 229

6. Go to **Activities** > **Tasks** and verify that the AP zone is successfully provisioned to the AP.

Figure 136: AP Zone Provision Status



PROVISION
admin
Provision Device
Provisioned Unified AP(s) in Sit
Starts: Jul 26, 2023 12:02

PROVISION
admin
Provision Device
Provisioned Unified AP(s) in Sit
Starts: Jul 25, 2023 11:51

PROVISION
admin
Provision Device
Hostname: C9800-Flex-CVD.c
Starts: Jul 25, 2023 11:46

PROVISION
admin
Provision Device
Provisioned Unified AP(s) in Sit

PROVISION

Provision Device

Starts: Jul 26, 2023 12:02 AM | Completed: Jul 26, 2023 12:02 AM | Status: Success | Last updated: 12:02:28 AM

Conversion of business intent to network intent SUCCESS

Deployment of network intent SUCCESS

Conversion from network intent to device intent and deployment of configuration SUCCESS

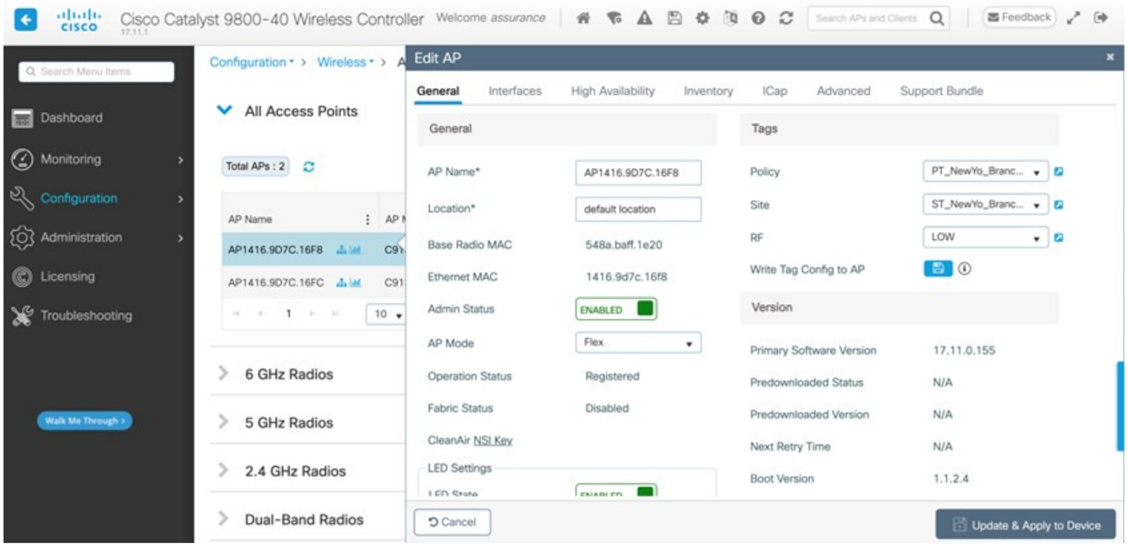
- Jul 26, 2023 12:02 AM Successfully acquired device lock in rfs flow
- Jul 26, 2023 12:02 AM Deploying configuration on the device C9800-Flex-CVD.cagelab.local (10.4.48.150).
- Jul 26, 2023 12:02 AM Configured operation will be to Modify AP configurations, Modify AP Tag configurations, Add RF Tag configurations, Add Site Tag configurations and Add Policy Tag configurations.

Conversion from network intent to device intent and deployment of configuration SUCCESS

- Jul 26, 2023 12:02 AM Successfully acquired device lock in rfs flow
- Jul 26, 2023 12:02 AM Deploying configuration on the device C9800-CVD-Nplus1.cagelab.local (10.4.48.151).
- Jul 26, 2023 12:02 AM Configured operation will be to Modify AP configurations.

7. Check the AP configuration on the Cisco Wireless Controller GUI. The AP configuration shows RF tag, site tag, and policy tag correctly in the wireless controller.

Figure 137: AP1 SSIDs Provisioned through Cisco DNA Center



Total APs : 2

AP Name	AP M
AP1416.9D7C.16F8	C9
AP1416.9D7C.16FC	C91

General

AP Name*: AP1416.9D7C.16F8

Location*: default location

Base Radio MAC: 548a.baff.1e20

Ethernet MAC: 1416.9d7c.16f8

Admin Status: ENABLED

AP Mode: Flex

Operation Status: Registered

Fabric Status: Disabled

CleanAir NSI Key

LED Settings

LED State: ENABLED

Tags

Policy: PT_NewYo_Branc...

Site: ST_NewYo_Branc...

RF: LOW

Write Tag Config to AP

Version

Primary Software Version: 17.11.0.155

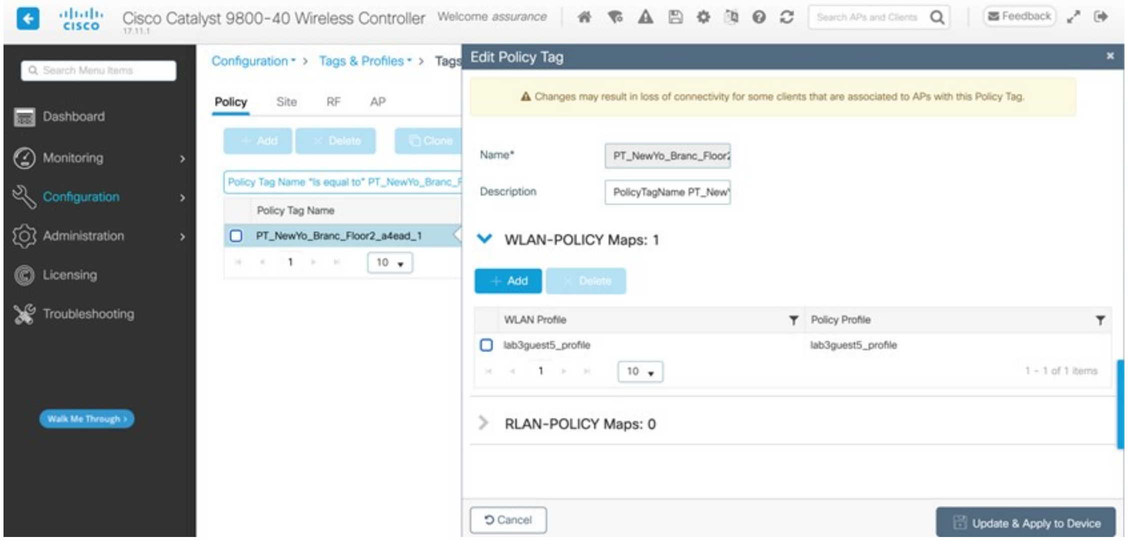
Predownloaded Status: N/A

Predownloaded Version: N/A

Next Retry Time: N/A

Boot Version: 1.1.2.4

Figure 138: Policy Tag1 Provisioned through Cisco DNA Center



Policy Tag Name "is equal to" PT_NewYo_Branc_F

Policy Tag Name
PT_NewYo_Branc_Floor2_a4ead_1

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*: PT_NewYo_Branc_Floor2

Description: PolicyTagName PT_NewY

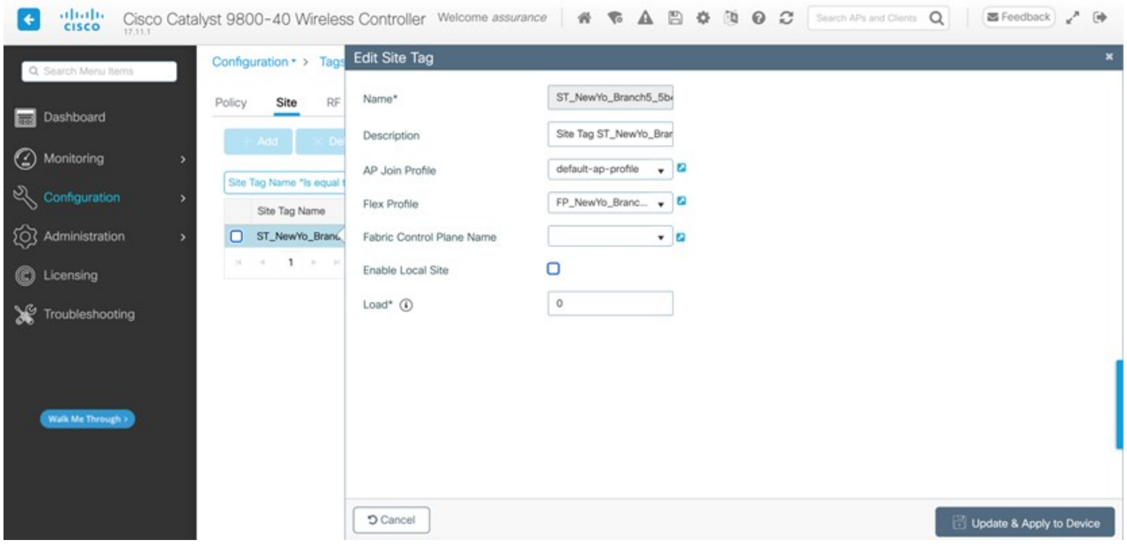
WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
lab3guest5_profile	lab3guest5_profile

1 - 1 of 1 items

RLAN-POLICY Maps: 0

Figure 139: Site Tag1 Provisioned through Cisco DNA Center



Edit Site Tag

Name*: ST_NewYo_Branch5_5b

Description: Site Tag ST_NewYo_Bran

AP Join Profile: default-ap-profile

Flex Profile: FP_NewYo_Branc...

Fabric Control Plane Name:

Enable Local Site: □

Load*: 0

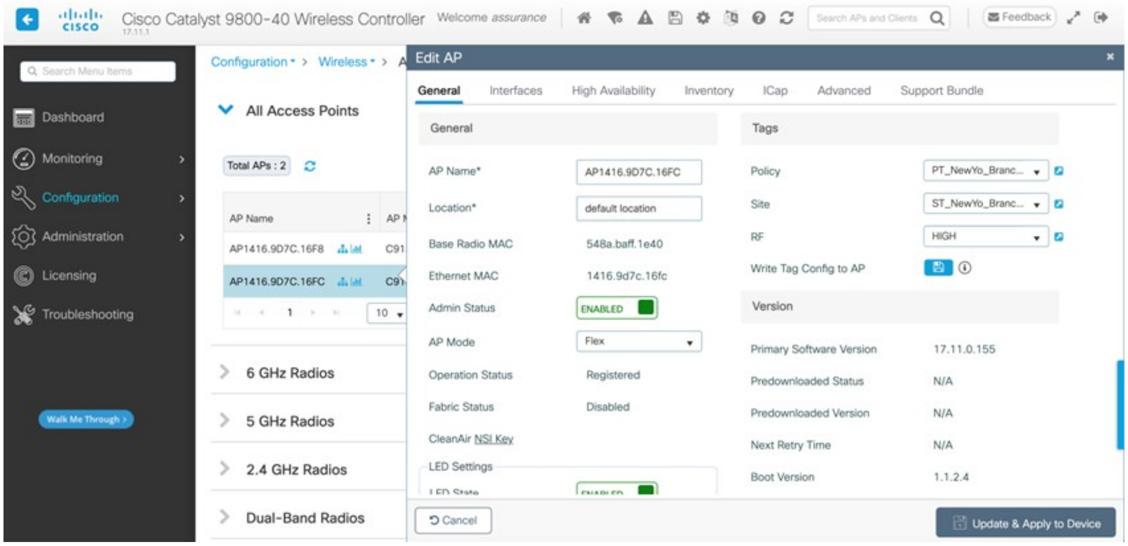
Cancel

Update & Apply to Device

8. Repeat Step 1 through Step 7 to provision the AP named sjcfloor1zone2 for lab3branch5 SSID with RF Profiles: High.

9. Check the AP configuration for second AP in the wireless controller GUI. The AP configuration shows RF tag, site tag, and policy tag correctly in the controller.

Figure 140: AP2 SSIDs Provisioned through Cisco DNA Center



Edit AP

General | Interfaces | High Availability | Inventory | ICap | Advanced | Support Bundle

General

AP Name*: AP1416.9D7C.16FC

Location*: default location

Base Radio MAC: 548a.baff.1e40

Ethernet MAC: 1416.9d7c.16fc

Admin Status: ENABLED

AP Mode: Flex

Operation Status: Registered

Fabric Status: Disabled

CleanAir NSI Key

LED Settings

LED State: ENABLED

Tags

Policy: PT_NewYo_Branc...

Site: ST_NewYo_Branc...

RF: HIGH

Write Tag Config to AP

Version

Primary Software Version: 17.11.0.155

Predownloaded Status: N/A

Predownloaded Version: N/A

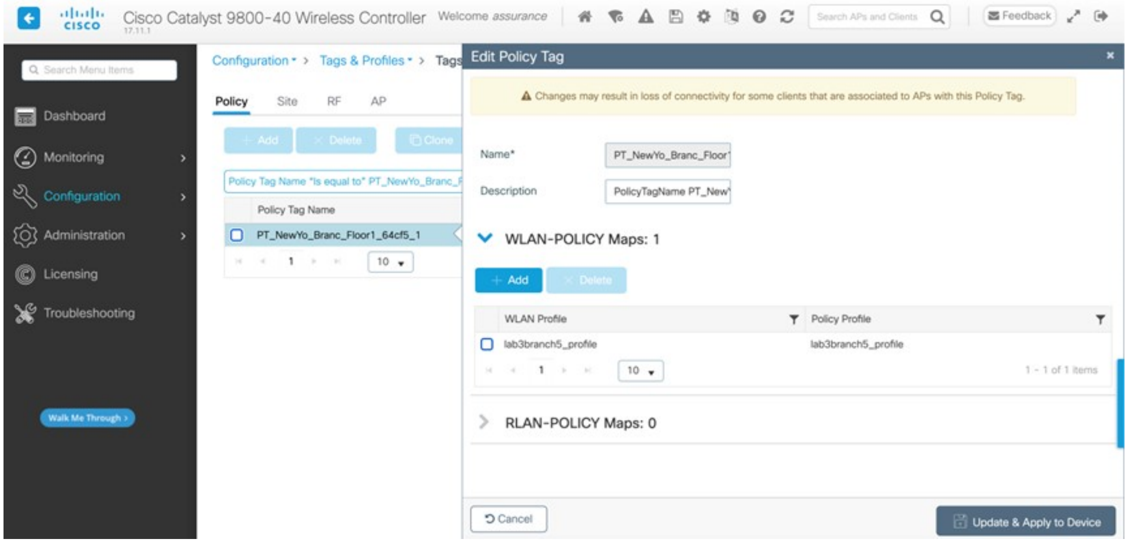
Next Retry Time: N/A

Boot Version: 1.1.2.4

Cancel

Update & Apply to Device

Figure 141: Policy Tag2 Provisioned through Cisco DNA Center



Policy Tag Name "Is equal to" PT_NewYo_Branc_F

	Policy Tag Name
□	PT_NewYo_Branc_Floor1_64cf5_1

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name* PT_NewYo_Branc_Floor1

Description PolicyTagName PT_New

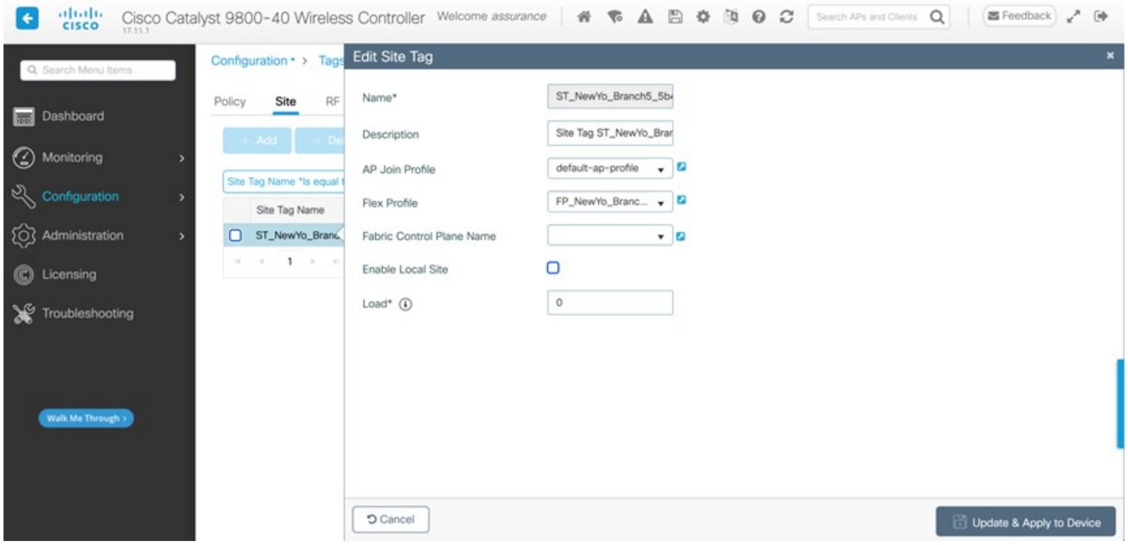
WLAN-POLICY Maps: 1

	WLAN Profile	Policy Profile
□	lab3branch5_profile	lab3branch5_profile

1 - 1 of 1 items

RLAN-POLICY Maps: 0

Figure 142: Site Tag2 Provisioned through Cisco DNA Center



Site Tag Name "Is equal t

	Site Tag Name
□	ST_NewYo_Branc

Name* ST_NewYo_Branch5_5b

Description Site Tag ST_NewYo_Brar

AP Join Profile default-ap-profile

Flex Profile FP_NewYo_Branc...

Fabric Control Plane Name

Enable Local Site □

Load* 0

Join New APs to the Enterprise Cisco Catalyst 9800 Series Wireless Controller HA SSO Pair (WLC-9800-2)

This deployment guide assumes that new APs use IP DHCP Discovery to discover the Cisco Catalyst 9800-40 Wireless Controller HA SSO pair (WLC-9800-2) and that the new APs have never been primed. A Cisco AP has been primed when it has previously joined (established a CAPWAP tunnel) to a wireless controller and cached the IP address of the wireless controller in NVRAM; or when primary, secondary, or tertiary wireless controller management IP addresses have been configured within the AP. In such scenarios, the AP will give preference to the primary, secondary, or tertiary wireless controller configuration over IP DHCP Discovery.

With IP DHCP Discovery, DHCP servers use Option 43 to provide one or more wireless controller management IP addresses to the APs. When an AP learns the management IP address of the Catalyst 9800-40 Wireless Controller HA SSO pair (WLC-9800-2), it will send a CAPWAP join request message to the wireless controller. When joined, the wireless controller manages the APs configuration, firmware, control transactions, and data transactions.

The following steps explain how to discover and join the APs to the enterprise wireless controller HA SSO pair (WLC-9800-2).

Procedure

Step 1 Configure the necessary VLANs on the Layer 2 access switches that support the Cisco APs, which join the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (WLC-9800-2).

This deployment guide assumes that APs are connected to Layer 2 access switches. A dedicated VLAN is on the switches for APs that are separate from end-user devices, such as PCs and IP phones. The use of a dedicated VLAN for APs is generally regarded as a design best practice, but this method does result in additional VLANs being deployed on the switches.

The following example shows the configuration on a Layer 2 access switch:

```
vlan 102
name AP_management
```

Step 2 Configure the switch ports to which the APs will be connected to be part of the configured VLAN. Ensure that the switch ports are not shut down.

The following example shows the interface configuration:

```
interface TenGigabitEthernet1/0/45
description AIR-AP2802I-B-K9 AP00F6.6313.B796
switchport access vlan 102
switchport mode access
no shutdown
```

In a deployment scenario with Layer 2 access switches, the upstream Layer 3 device (switch or router), that is associated with the VLAN connected to the AP, must be configured to relay DHCP requests to a centralized DHCP server. The relay function is enabled through the **ip helper-address** interface-level command.

Step 3 Configure the necessary DHCP relay commands on the upstream Layer 3 devices that support APs, which join the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (WLC-9800-2).

The following example shows the configuration on a Layer 3 switch using a VLAN switched virtual interface (SVI):

```
interface Vlan102
ip address 10.4.2.1 255.255.255.0
ip helper-address 10.4.48.10
```

Step 4 Configure the DHCP scopes within the IP DHCP server to return the management IP address of the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (WLC-9800-2) in Option 43.

For this deployment guide, a Microsoft Active Directory (AD) server with IP address **10.4.48.10** functions as the IP DHCP server. The IPv4 address of the enterprise wireless controller HA SSO pair (WLC-9800-2) configured within DHCP Option 43 is **10.4.74.32**. Configuration of the DHCP within the Microsoft AD server is outside the scope of this document.

Step 5 Connect the Cisco AP(s) to the switch port(s) on the Layer 2 access switches.

The APs should get IP addresses and automatically join the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (WLC-9800-2). When the inventory resync interval for WLC-9800-2 passes, the new APs should be displayed in the Cisco DNA Center inventory. Alternatively, you can manually resync the inventory for the wireless controller using the following steps:

a. From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The main provisioning window displays the devices in the inventory. By default, the **Focus** is set for **Inventory**.

b. Check the check box for **WLC-9800-2**.

c. From the **Actions** drop-down menu, choose **Inventory** > **Resync Device**. A warning dialog box asks you to confirm the resync.

d. Click **OK** to confirm the resync and close the dialog box.

After you have resynced the Catalyst 9800-40 Wireless Controller HA SSO pair (WLC-9800-2), the APs that are joined to the wireless controller should be displayed in the **Inventory** window.

Provision the New APs

Once the APs have been joined to the Cisco Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (C9800-40-CVD.cagelab.local), they must be provisioned. Provisioning with Cisco DNA Center is necessary for the APs to receive the correct configuration to advertise the **lab3employee** and **lab3guest** SSIDs. The following table lists the APs that were provisioned for this deployment guide, including their locations.

Table 31: APs Provisioned in Cisco DNA Center

AP Name	AP Model	Location
AP1416.9D7C.16FC	C9130AXI-B	Branch 5, Floor 1

Note The mixture of APs deployed across the buildings and floors within this design and deployment guide is simply to show the provisioning, through Cisco DNA Center, of different models of APs in different locations, all controlled by the same Catalyst 9800 Series HA SSO Wireless Controller pair. In a typical deployment, the same AP model would tend to be deployed within a floor, and often across the entire deployment.

The following are the steps for provisioning APs within Cisco DNA Center.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Inventory** > **Provision**.

The main provisioning window displays the devices. By default, the **Focus** will be set for **Inventory**.

Step 2 Locate and check the check box for each of the APs to be provisioned.

Step 3 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

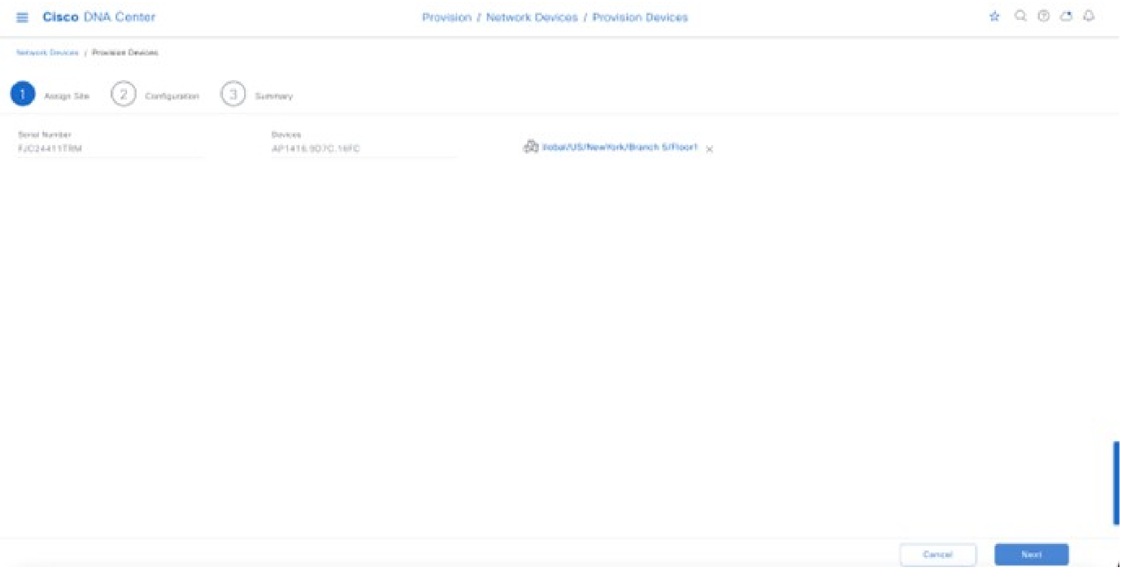
You are taken through a workflow for provisioning the APs, starting with **Assign Site**.

Step 4 For each of the APs listed, click **Choose a Site**.

A slide-in pane is displayed, showing the site hierarchy that is configured for Cisco DNA Center.

Step 5 Expand the site hierarchy for **New York**, choose the building (**Branch 5**) and the floor (**Floor 1**) for each AP.

Figure 143: AP Provisioning Step 1 – Assign Site



Cisco DNA Center — Provision / Network Devices / Provision Devices

Network Devices / Provision Devices

1 Assign Site — 2 Configuration — 3 Summary

Serial Number: FJC24411TRM

Devices: AP1416.9D7C.16FC

Global/US/NewYork/Branch 5/Floor1

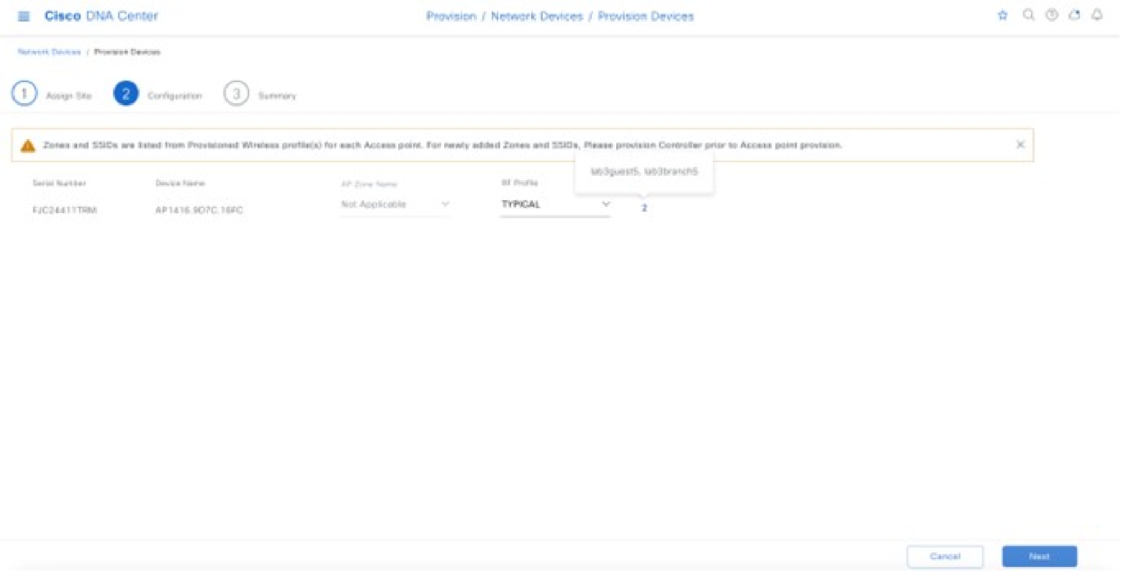
Step 6 Click **Save** to save the site assignments for the APs.

Step 7 Click **Next** to advance to the next in the provisioning workflow, **Configuration**.

Step 8 From the **RF Profile** drop-down list, choose the RF profile to assign to each of the APs.

For this deployment guide, the TYPICAL RF profile was chosen. The TYPICAL RF profile was also chosen as the default RF profile in *Design the wireless network*.

Figure 144: AP Provisioning Step 2 – Configuration



Cisco DNA Center — Provision / Network Devices / Provision Devices

Network Devices / Provision Devices

1 Assign Site — 2 Configuration — 3 Summary

Zones and SSIDs are listed from Provisioned Wireless profile(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision.

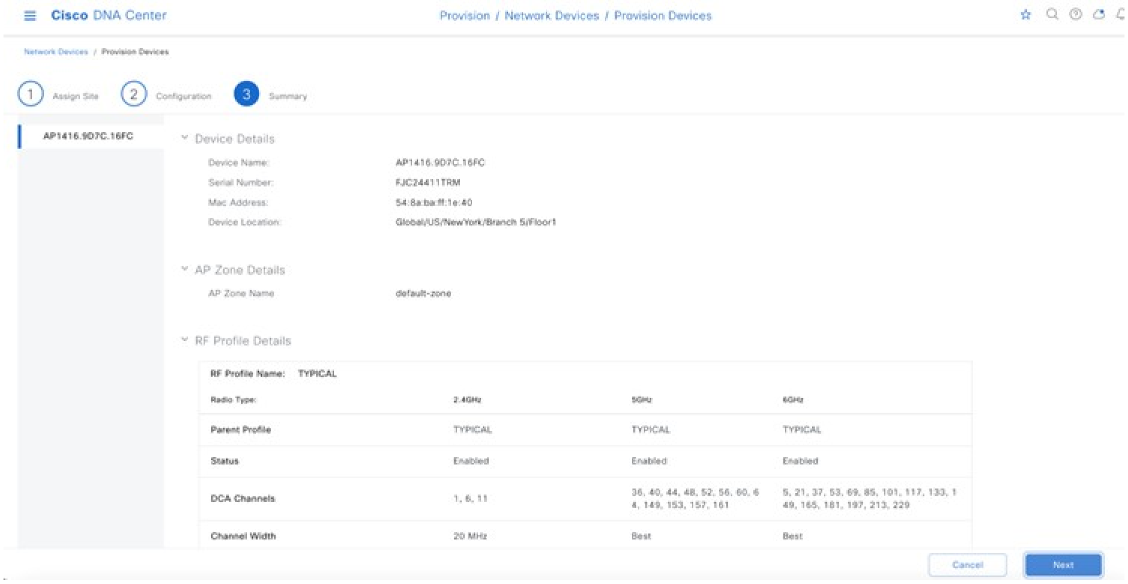
Serial Number	Device Name	AP Zone Name	RF Profile	
FJC24411TRM	AP1416.9D7C.16FC	Not Applicable	TYPICAL	2

lab3guest5, lab3branch5

Step 9 Click **Next** to advance to the next step in the provisioning workflow, **Summary**.

The **Summary** window provides a summary of the configuration that will be provisioned to each of the APs.

Figure 145: AP Provisioning Step 3 – Summary



Cisco DNA Center
Provision / Network Devices / Provision Devices
Network Devices / Provision Devices
1 Assign Site
2 Configuration
3 Summary
AP1416.9D7C.16FC

Device Details

Device Name:	AP1416.9D7C.16FC
Serial Number:	FJC24411TRM
Mac Address:	54:8a:ba:ff:1e:40
Device Location:	Global/US/NewYork/Branch 5/Floor1

AP Zone Details

AP Zone Name	default-zone

RF Profile Details

RF Profile Name: TYPICAL

Radio Type:	2.4GHz	5GHz	6GHz
Parent Profile	TYPICAL	TYPICAL	TYPICAL
Status	Enabled	Enabled	Enabled
DCA Channels	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213, 229
Channel Width	20 MHz	Best	Best

Step 10 Click **Deploy** to provision the APs. A slide-in pane is displayed. You can deploy the configuration now, or you can schedule the configuration to be deployed later.

Note It is best practice to make configuration changes and provision new devices in your network only during scheduled network operation change windows.

In this scenario, the flex profile is provisioned to the AP, changing the AP mode from local to flex. As a result, an AP reboot is required, leading to a disruption in service for wireless clients.

Step 11 Click the **Now** radio button.

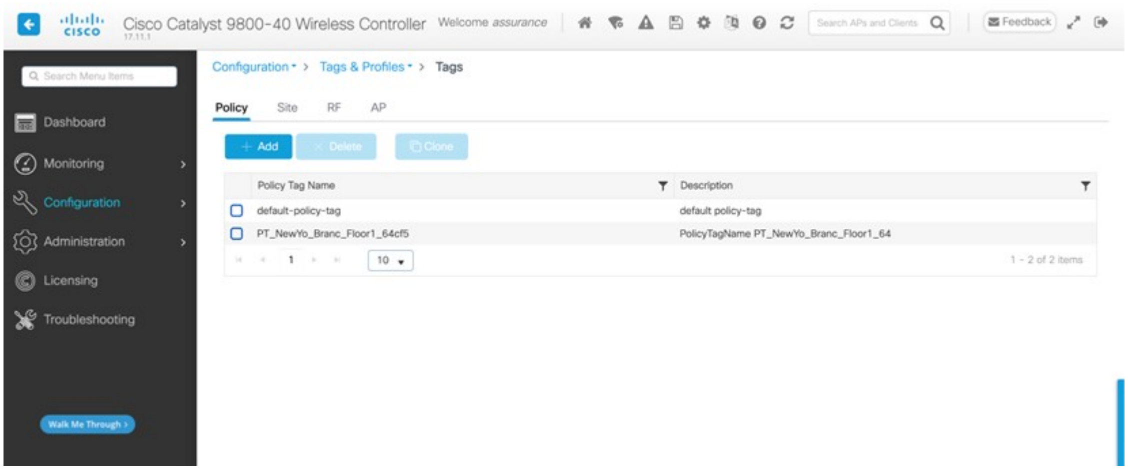
Step 12 Click **Apply** to apply the configuration.

A **Success** dialog box is displayed, with a message indicating that after provisioning, the APs will reboot, and the AP mode will change from local to flex.

Step 13 Click **OK** to confirm. The list of inventories in the main provisioning window is displayed. The provisioning status of the APs will temporarily show **Provisioning**, but the status will change to **Success** after a few minutes. For more information, you can click **See Details** below the provisioning status of each AP.

For each floor that contains the provisioned APs, Cisco DNA Center creates a new policy tag in the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (C9800-Flex-CVD).

Figure 146: Policy Tags Created by Cisco DNA Center in the Catalyst 9800-40 Enterprise Wireless Controller



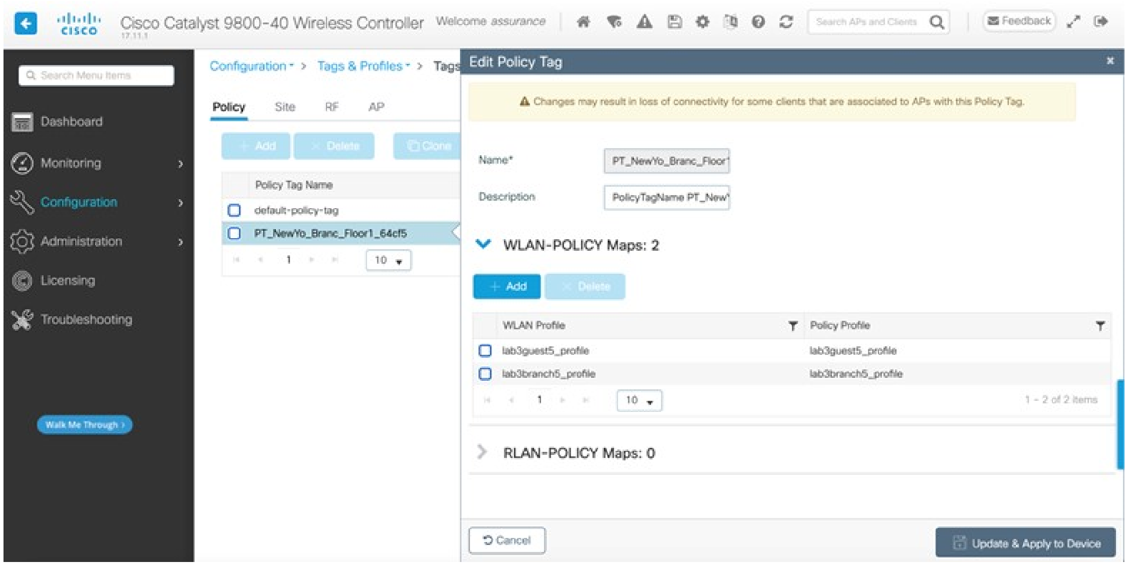
Policy Tag Name	Description
default-policy-tag	default policy-tag
PT_NewYo_Branc_Floor1_64cf5	PolicyTagName PT_NewYo_Branc_Floor1_64

1 - 2 of 2 items

Three new policy tags have been created, corresponding to the APs provisioned on **Floor 1** of building **Branch 5**. Each policy tag is unique to a site, indicating a specific floor within a building. Policy tags for a floor will only be created by Cisco DNA Center when APs are provisioned to the floor.

By clicking on any of the policy tags, you can display the policy profiles and the WLAN profiles that are added to the new policy tag by Cisco DNA Center.

Figure 147: Policy Tag Details



Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name* PT_NewYo_Branc_Floor

Description PolicyTagName PT_New

WLAN-POLICY Maps: 2

WLAN Profile	Policy Profile
lab3guest5_profile	lab3guest5_profile
lab3branch5_profile	lab3branch5_profile

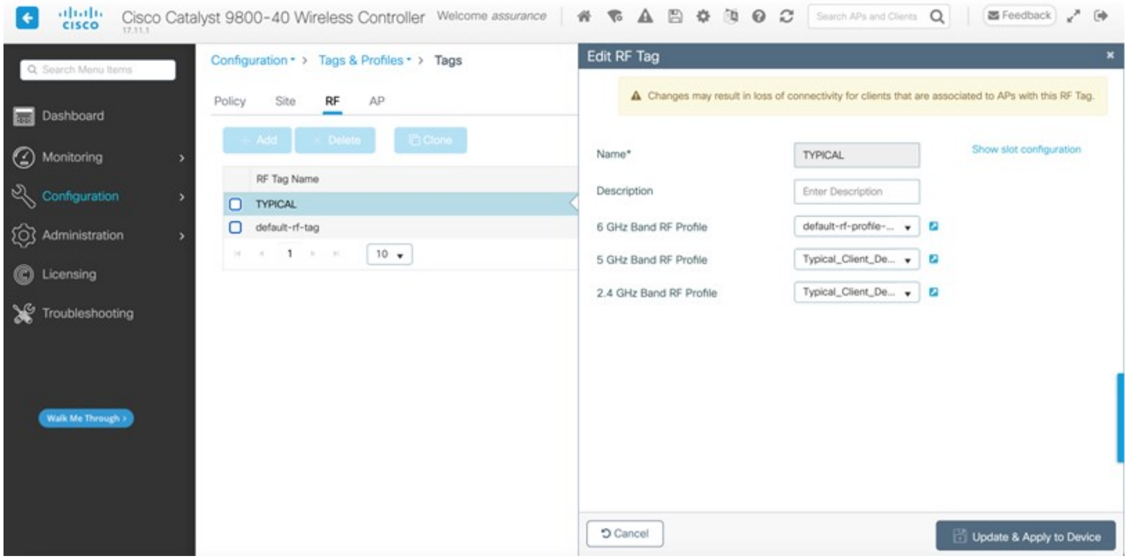
1 - 2 of 2 items

RLAN-POLICY Maps: 0

The WLAN profiles and the policy profiles that are created during the provisioning of the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair have been added to each of the policy tags. This process is controlled by the **branch5** WLAN profile that is created in Cisco DNA Center within *Design the wireless network*. The **branch5** WLAN profile specified the **lab3branch5** and **lab3guest5** SSIDs to be broadcast throughout the **New York** area (**Floor 1** of building **Branch 5**).

During the AP provisioning process, the TYPICAL RF profile was chosen. Cisco DNA Center creates a new RF tag named TYPICAL within the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (C9800-Flex-CVD).

Figure 148: TYPICAL RF Tag Created by Cisco DNA Center



Edit RF Tag

⚠ Changes may result in loss of connectivity for clients that are associated to APs with this RF Tag.

Name*: TYPICAL

Show slot configuration

Description: Enter Description

6 GHz Band RF Profile: default-rf-profile-...

5 GHz Band RF Profile: Typical_Client_De...

2.4 GHz Band RF Profile: Typical_Client_De...

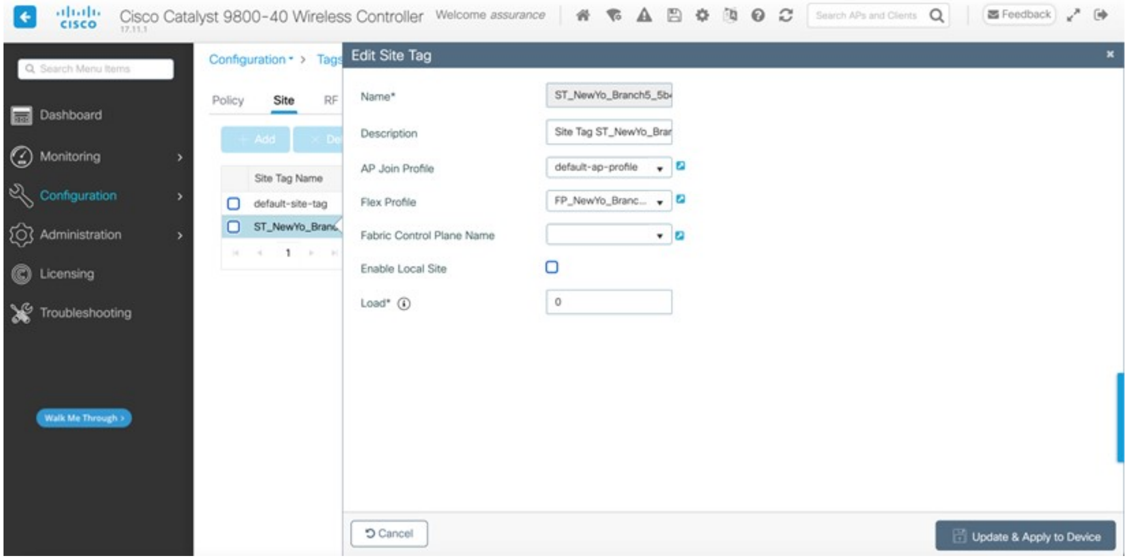
Cancel

Update & Apply to Device

Finally, Cisco DNA Center statically assigns a policy tag (specific to each floor), the RF tag (named TYPICAL), and the site tag (named ST_NewYo_Branch5_5b486_0) to each AP in the Catalyst 9800-40 enterprise Wireless Controller HA SSO pair (C9800-Flex-CVD). The site tag ST_NewYo_Branch5_5b486_0 contains the default AP join profile named **default-ap-profile**.

An example of the static assignment of the policy tag, site tag, and RF tag to each AP is shown in the following figure.

Figure 149: Assignment of Site Tag Seen on Wireless Controller GUI



Edit Site Tag

Name*: ST_NewYo_Branch5_5b

Description: Site Tag ST_NewYo_Brar

AP Join Profile: default-ap-profile

Flex Profile: FP_NewYo_Branc...

Fabric Control Plane Name:

Enable Local Site: □

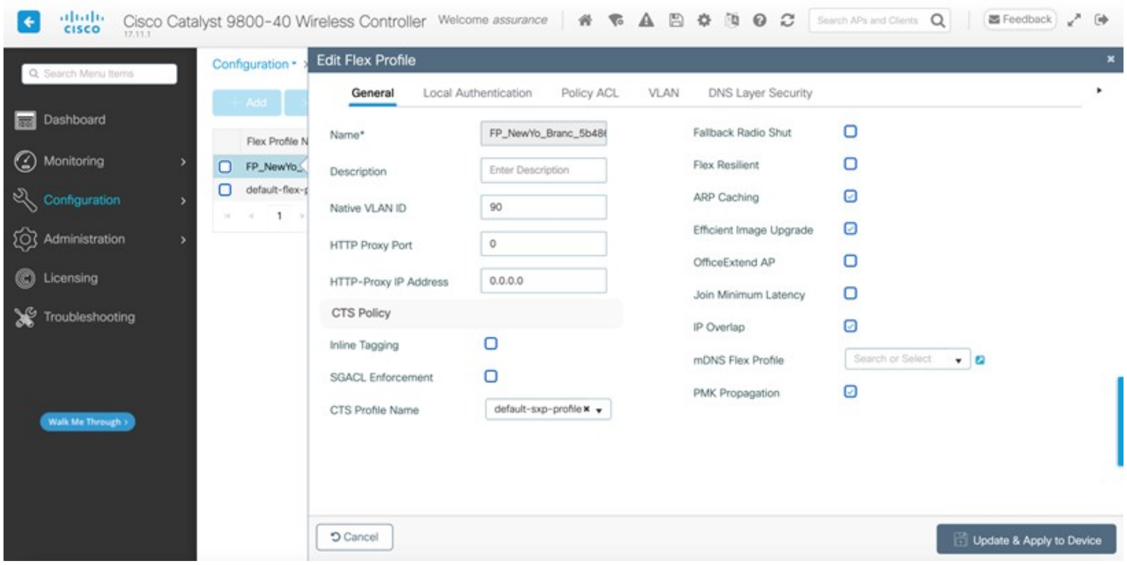
Load*: 0

Cancel

Update & Apply to Device

The flex profile was mapped to the site tag, with the local site being disabled. After the AP provision with VLAN 90, the flex profile was correctly updated with the native VLAN ID.

Figure 150: Flex Profile Seen in Wireless Controller GUI



Name* FP_NewYo_Branc_5b48(

Description Enter Description

Native VLAN ID 90

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

CTS Policy

Inline Tagging □

SGACL Enforcement □

CTS Profile Name default-sxp-profile

Fallback Radio Shut □

Flex Resilient □

ARP Caching ☑

Efficient Image Upgrade ☑

OfficeExtend AP □

Join Minimum Latency □

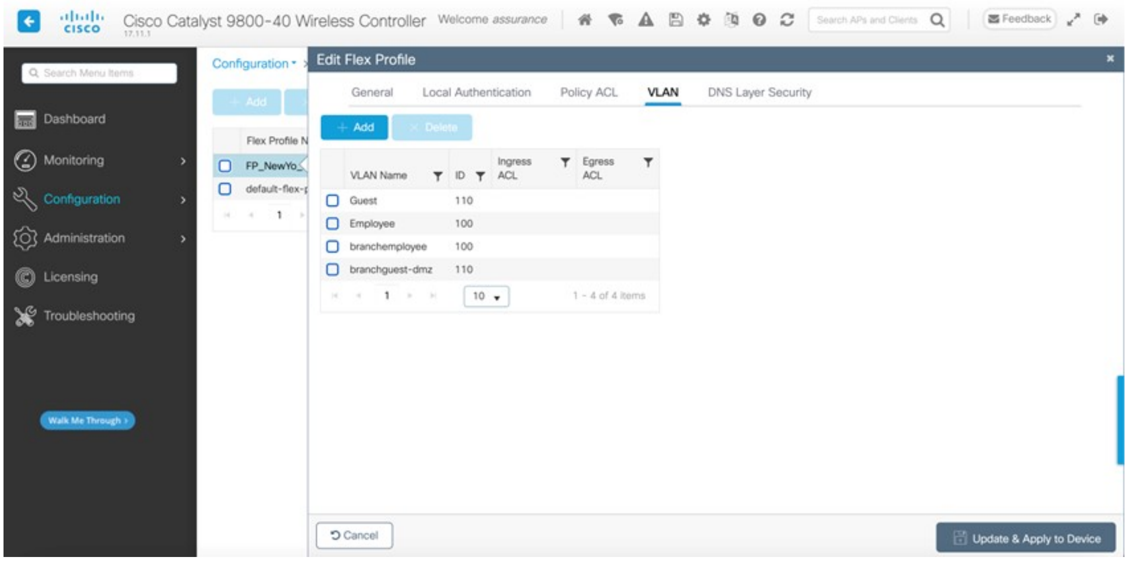
IP Overlap ☑

mDNS Flex Profile Search or Select

PMK Propagation ☑

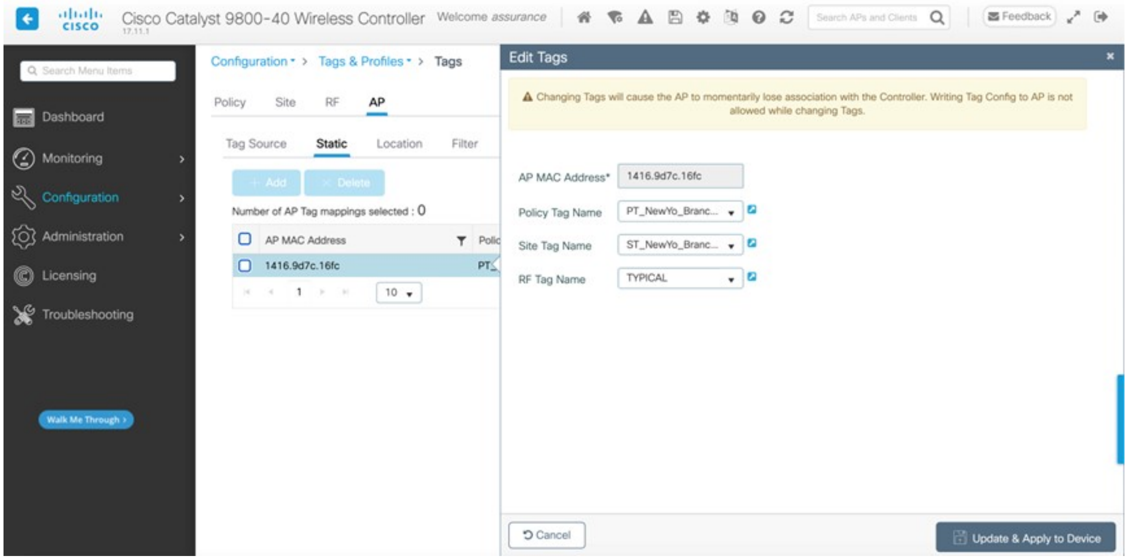
To view the flex profile local VLAN mapped to the flex profiles, click the VLAN tab for the flex profile.

Figure 151: Flex Profile Seen in Wireless Controller GUI



VLAN Name	ID	Ingress ACL	Egress ACL
Guest	110		
Employee	100		
branchemployee	100		
branchguest-dmz	110		

Figure 152: Static Assignment of Tags to APs by Cisco DNA Center



Number of AP Tag mappings selected : 0

☐	AP MAC Address	Polic
☐	1416.9d7c.16fc	PT

1 10

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

AP MAC Address* 1416.9d7c.16fc

Policy Tag Name PT_NewYo_Branc...

Site Tag Name ST_NewYo_Branc...

RF Tag Name TYPICAL

The assignment of the policy tag to the AP causes the **lab3branch5** and **lab3guest5** SSIDs to be broadcasted by the AP provisioned on the floor. At this point, wireless clients should be able to associate with the **lab3branch5** and/or **lab3guest5** SSIDs and authenticate to the network.

Note When APs are provisioned without provisioning the wireless controller, it is best practice to go to the **Inventory** window and change the focus to **Provision**. Monitor the provisioning status column to see if any wireless controllers show up as “Out of Sync.” If so, provision the wireless controller to get back in sync.

Cisco DNA Center continues to add support for additional wireless features in the newer releases, and these features can be provisioned through Cisco DNA Center. If the newer features are provisioned through a template programmer or through other tools, it is best practice to preview the config and resolve conflicts before provisioning the wireless controller and the AP from Cisco DNA Center.

When Cisco DNA Center is upgraded to a newer release, Cisco recommends upgrading the wireless controller to the recommended version that is compatible with the newer Cisco DNA Center release.

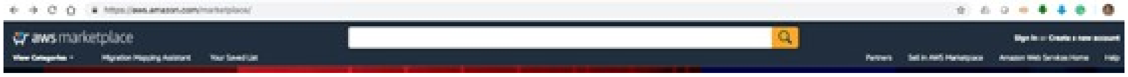
WLAN for Wireless Controller Hosted on AWS Deployment

The following steps explain how to launch a Cisco Catalyst 9800-CL Wireless Controller (C9800-CL) from the AWS Marketplace with the CloudFormation template.

Procedure

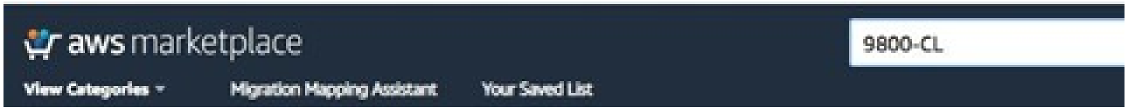
Step 1 Log in to the AWS Marketplace.

Figure 153: AWS Marketplace Window



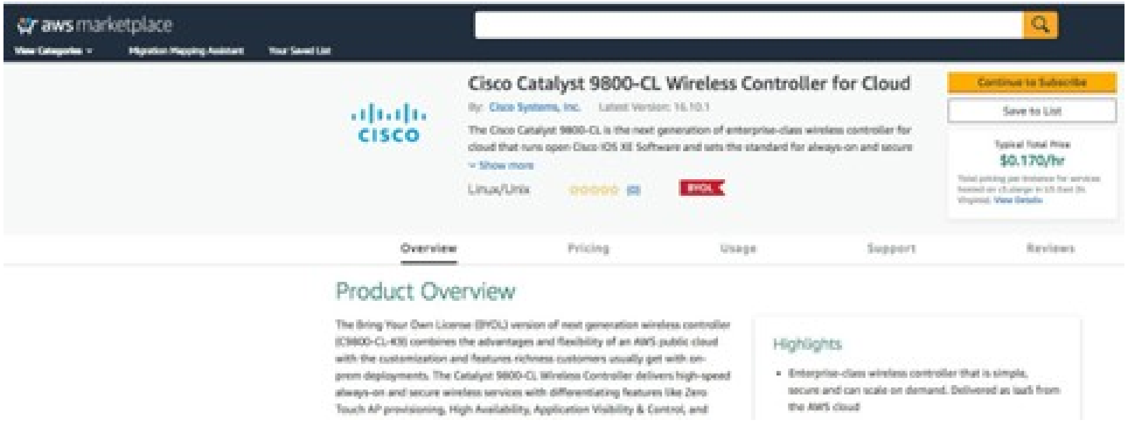
Step 2 Search for Catalyst 9800 or C9800-CL and from the search results, click the Cisco Catalyst 9800-CL Wireless Controller for Cloud window.

Figure 154: Search for C9800-CL



Step 3 The product overview window is displayed:

Figure 155: Product Overview



Cisco Catalyst 9800-CL Wireless Controller for Cloud

By: Cisco Systems, Inc. Latest Version: 16.10.1

The Cisco Catalyst 9800-CL is the next generation of enterprise-class wireless controller for cloud that runs open Cisco IOS XE Software and sets the standard for always-on and secure

Show more

Linux/Unix (0) BYOL

Typical Total Price

$0.170/hr

Total pricing per instance for services hosted on c5.large in US East (N. Virginia). View Details

Product Overview

The Bring Your Own License (BYOL) version of next generation wireless controller (C9800-CL-K9) combines the advantages and flexibility of an AWS public cloud with the customization and features richness customers usually get with on-prem deployments. The Catalyst 9800-CL Wireless Controller delivers high-speed always-on and secure wireless services with differentiating features like Zero Touch AP provisioning, High Availability, Application Visibility & Control, and

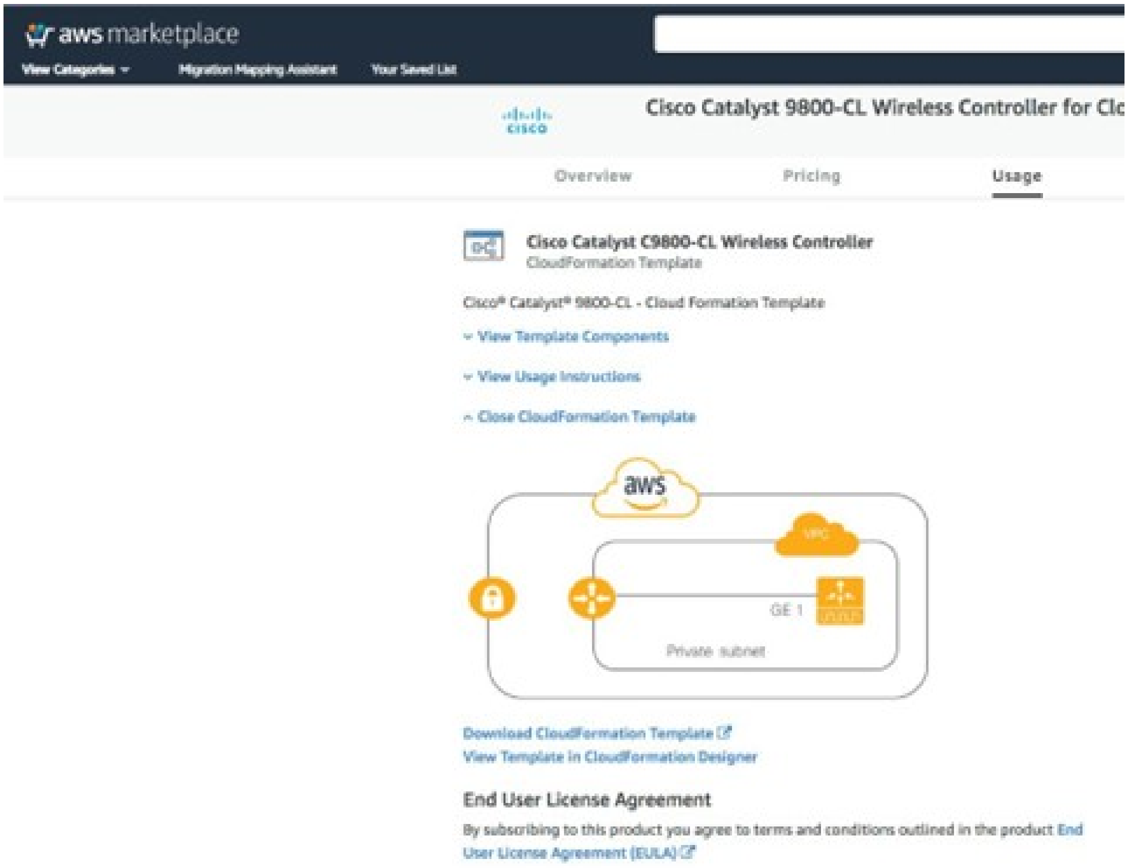
Highlights

- Enterprise-class wireless controller that is simple, secure and can scale on demand. Delivered as IaaS from the AWS cloud

You can read all the information about the product, support, licensing, and cost estimate for deploying the C9800-CL in the different AWS regions.

If you scroll down in this window, you will be able to get information about the topology and the CloudFormation template, as shown in the following figure.

Figure 156: CloudFormation Template



Cisco Catalyst 9800-CL Wireless Controller for Clo

Cisco Catalyst C9800-CL Wireless Controller

CloudFormation Template

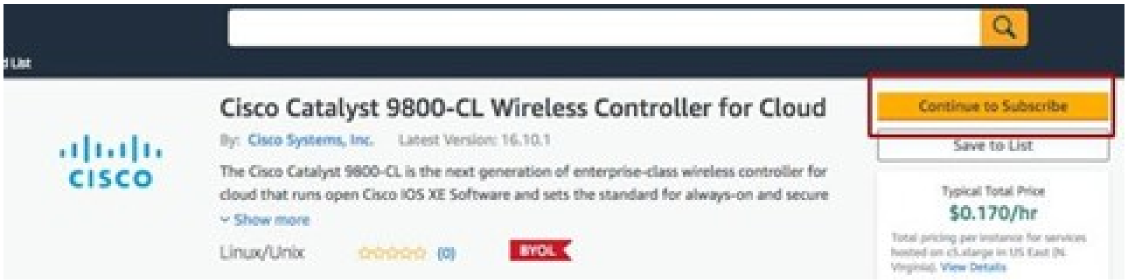
Cisco® Catalyst® 9800-CL - Cloud Formation Template

End User License Agreement

By subscribing to this product you agree to terms and conditions outlined in the product End User License Agreement (EULA)

Step 4 In the top-right corner, click **Continue to Subscribe**.

Figure 157: Subscription Window



Cisco Catalyst 9800-CL Wireless Controller for Cloud

By: Cisco Systems, Inc. Latest Version: 16.10.1

The Cisco Catalyst 9800-CL is the next generation of enterprise-class wireless controller for cloud that runs open Cisco IOS XE Software and sets the standard for always-on and secure

Linux/Unix

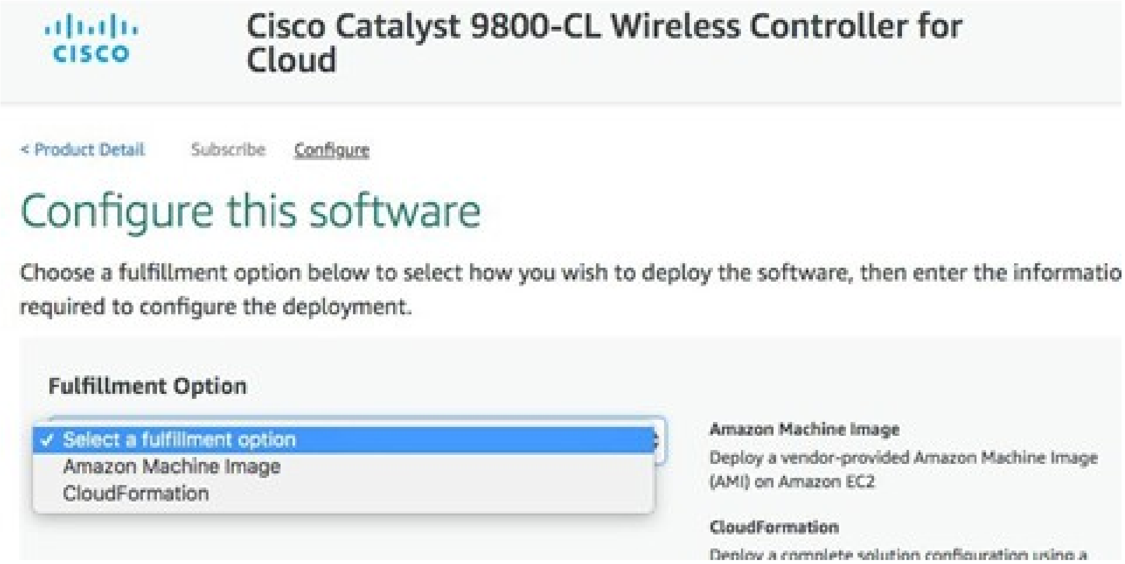
Typical Total Price

$0.170/hr

Total pricing per instance for services hosted on c5.xlarge in US East (N. Virginia).

Step 5 Choose **CloudFormation** as the **Fulfilment Option**.

Figure 158: Configure the Software



Cisco Catalyst 9800-CL Wireless Controller for Cloud

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the informatio required to configure the deployment.

Fulfillment Option

Amazon Machine Image

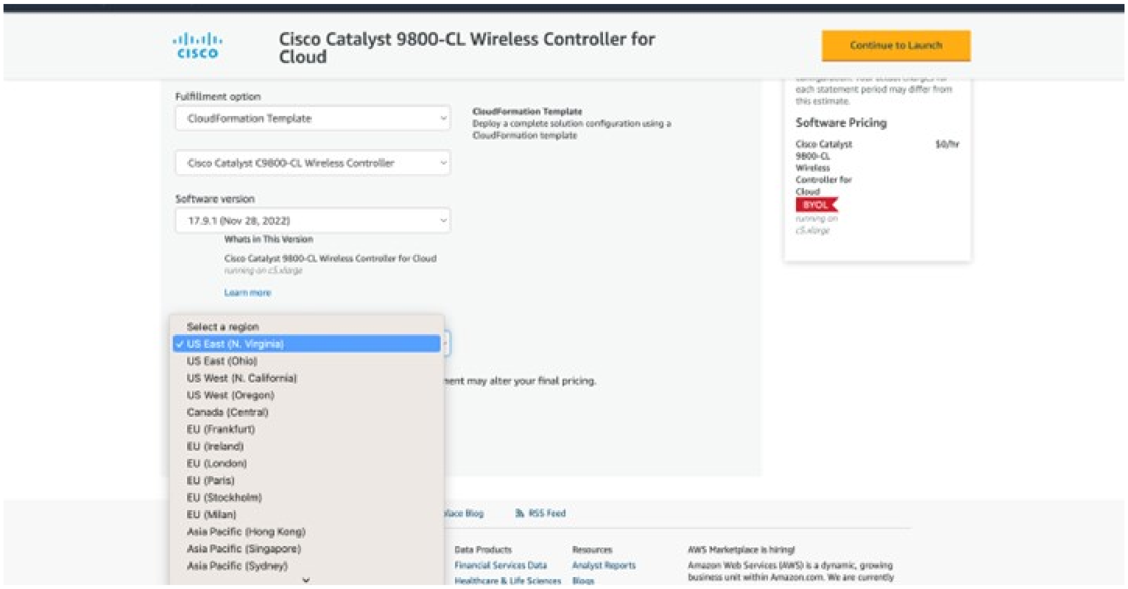
Deploy a vendor-provided Amazon Machine Image (AMI) on Amazon EC2

CloudFormation

Deploy a complete solution configuration using a

Step 6 Scroll down and choose the **Region** where you want to create the C9800-CL instance.

Figure 159: Select a Region



Cisco Catalyst 9800-CL Wireless Controller for Cloud

Fulfillment option: CloudFormation Template

Cisco Catalyst C9800-CL Wireless Controller

CloudFormation Template

Deploy a complete solution configuration using a CloudFormation template

Software version: 17.9.1 (Nov 28, 2022)

Whats in This Version

Cisco Catalyst 9800-CL Wireless Controller for Cloud

running on c5.xlarge

ment may alter your final pricing.

each statement period may differ from this estimate.

Software Pricing

Cisco Catalyst 9800-CL Wireless Controller for Cloud BYOL running on c5.xlarge	$0/hr

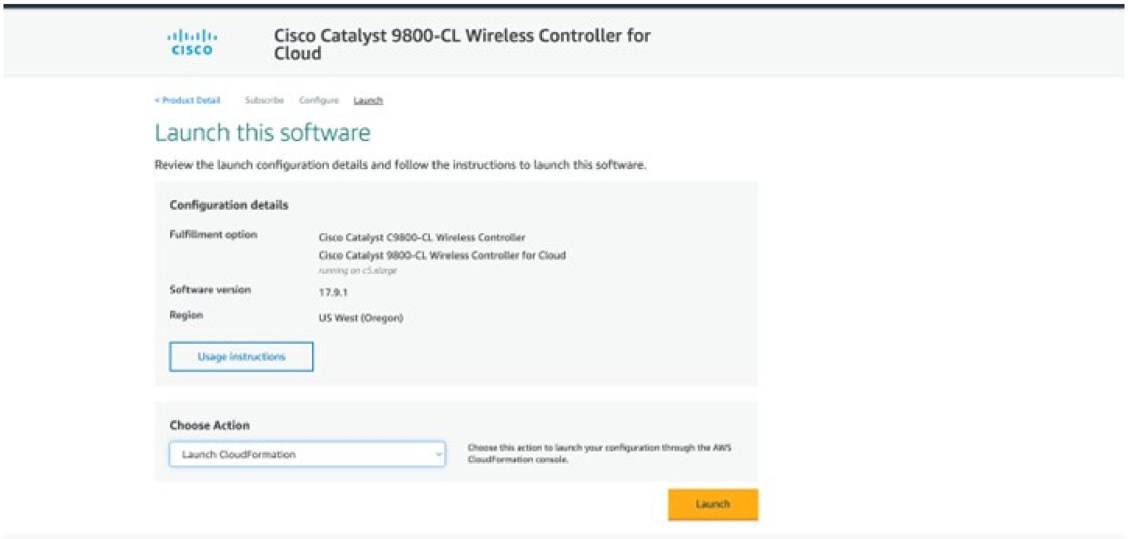
AWS Marketplace is hiring!

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently

Step 7 Click **Continue to Launch**.

Step 8 Click **Launch**.

Figure 160: Launch the Software



Cisco Catalyst 9800-CL Wireless Controller for Cloud

< Product Detail   Subscribe   Configure   Launch

Launch this software

Review the launch configuration details and follow the instructions to launch this software.

Configuration details

Fulfillment option: Cisco Catalyst C9800-CL Wireless Controller
Cisco Catalyst 9800-CL Wireless Controller for Cloud
running on c5.xlarge

Software version: 17.9.1

Region: US West (Oregon)

Usage instructions

Choose Action

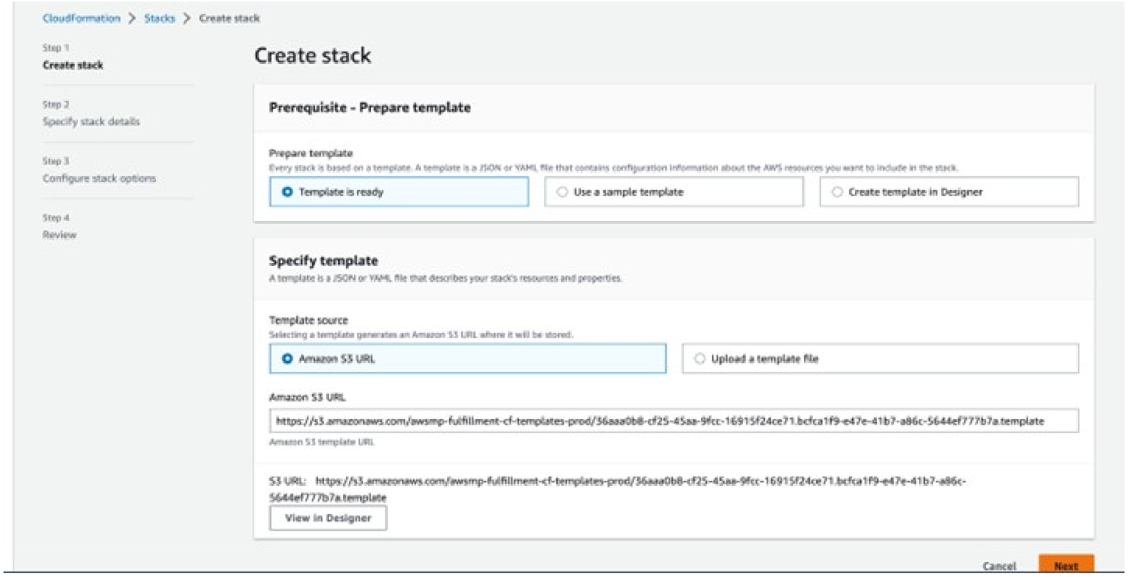
Launch CloudFormation

Choose this action to launch your configuration through the AWS CloudFormation console.

Launch

You will be automatically redirected to the CloudFormation service in the AWS console, and the following window will be displayed.

Figure 161: Create Stack Window



CloudFormation > Stacks > Create stack

Step 1
Create stack

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

● Amazon S3 URL ○ Upload a template file

Amazon S3 URL
https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/36aaa0b8-cf25-45aa-9fcc-16915f24ce71.bcfca1f9-e47e-41b7-a86c-5644ef777b7a.template
Amazon S3 template URL

S3 URL: https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/36aaa0b8-cf25-45aa-9fcc-16915f24ce71.bcfca1f9-e47e-41b7-a86c-5644ef777b7a.template

View in Designer

Cancel   Next

Step 9 Click **Next**.

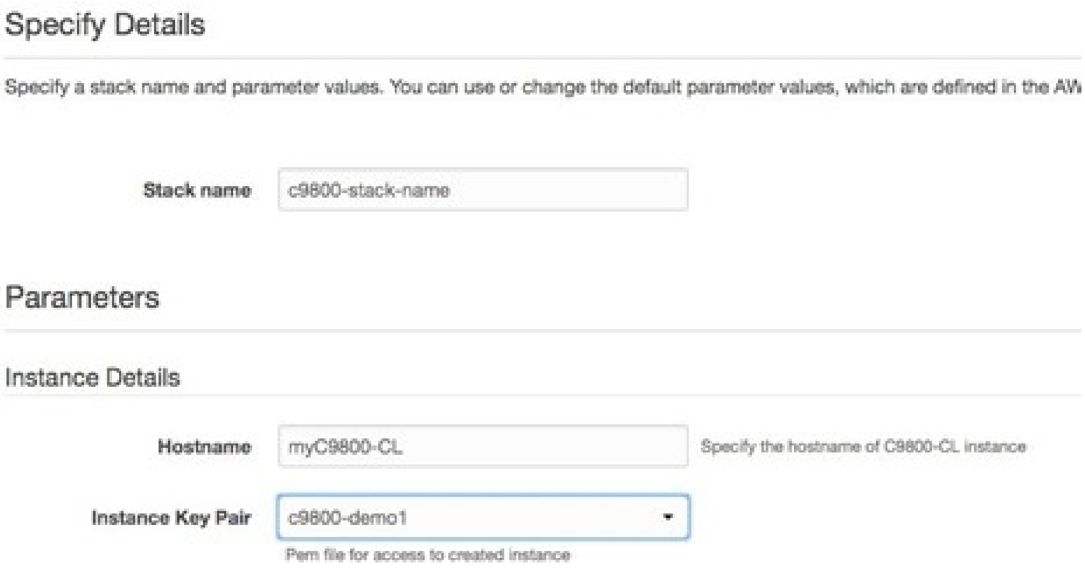
The template has been automatically chosen.

Note If you have specifications that require a change to the default template, you can upload a different template by clicking the **Upload a template to Amazon S3** radio button and choosing the relevant file.

Step 10 Enter the **Stack name** and the **Instance Details**.

Step 11 Enter the C9800 **Hostname** and choose the previously created key pair.

Figure 162: Specify Details



Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AW

Stack name: c9800-stack-name

Parameters

Instance Details

Hostname: myC9800-CL — Specify the hostname of C9800-CL instance

Instance Key Pair: c9800-demo1 — Pem file for access to created instance

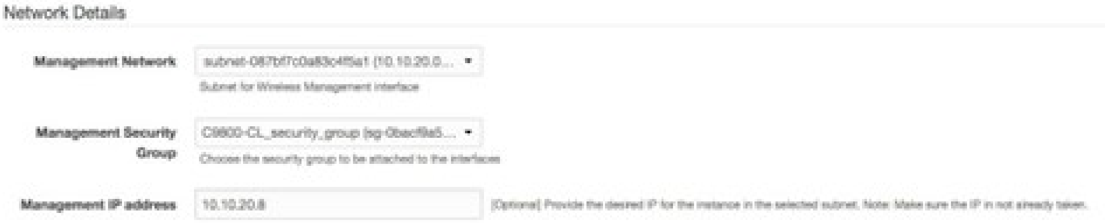
Step 12 Enter the **Network Details**.

a. From the drop-down list, choose the subnet and security group that you want to assign to the wireless management interface.

Note Make sure that the chosen subnet and security group belongs to the same VPC.

b. Within the chosen subnet, you can enter the IP address that will be assigned to the C9800 instance. Make sure that the specific IP belongs to the chosen subnet and that the IP is not already in use, or else the stack creation will fail.

Figure 163: Network Details



Network Details

Management Network: subnet-087bf7c0a83c4f5a1 (10.10.20.0... — Subnet for Wireless Management interface

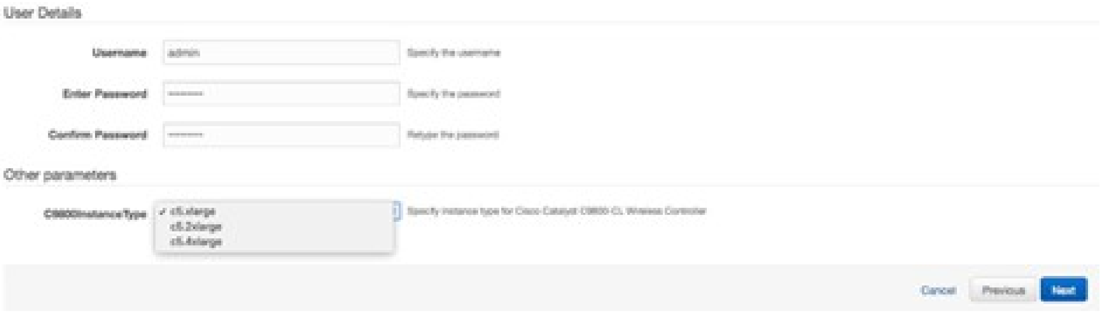
Management Security Group: C9800-CL_security_group (sg-0bacf9a5... — Choose the security group to be attached to the interfaces

Management IP address: 10.10.20.8 — [Optional] Provide the desired IP for the instance in the selected subnet. Note: Make sure the IP in not already taken.

Step 13 (Optional) Enter the username and password to remotely connect to the instance.

If you don’t configure the username and password, you will be able to log in through SSH using the default AWS user (ec2-user) and the instance key pair. Choose the instance type according to the scale. Cisco only supports c5.xlarge (the default value), which corresponds to the supported scale: 1000 APs and 10,000 clients.

Figure 164: User Details



User Details

Username: admin — Specify the username

Enter Password: ——— — Specify the password

Confirm Password: ——— — Retype the password

Other parameters

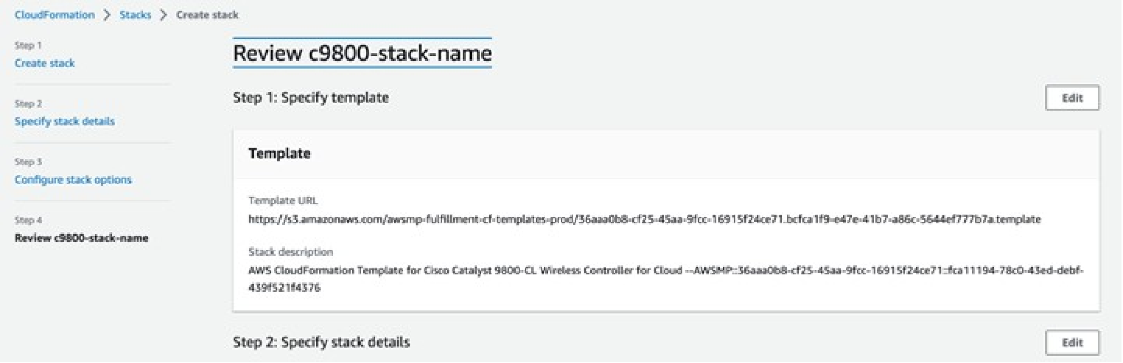
C9800InstanceType: ✓ c5.xlarge, c5.2xlarge, c5.4xlarge — Specify instance type for Cisco Catalyst C9800-CL Wireless Controller

Step 14 Click **Next**.

Step 15 For the option window, use the default settings and click **Next**.

Step 16 Review the settings and click **Submit**.

Figure 165: Review the Settings - Part 1



CloudFormation > Stacks > Create stack

Step 1
Create stack

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review c9800-stack-name

Review c9800-stack-name

Step 1: Specify template

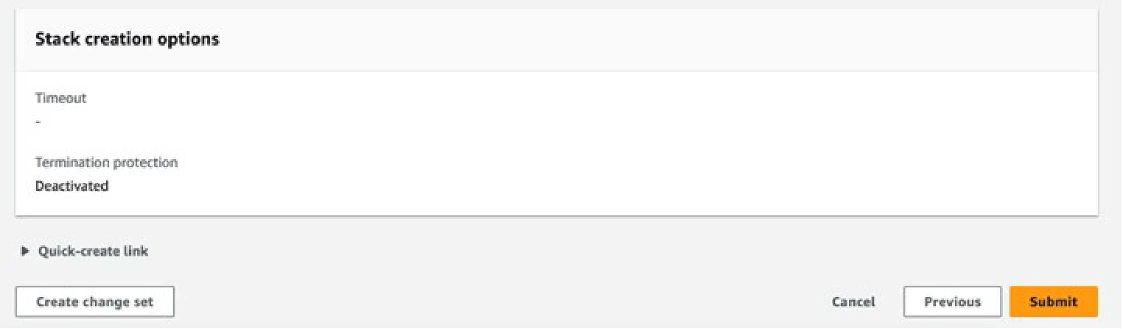
Template

Template URL
https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/36aaa0b8-cf25-45aa-9fcc-16915f24ce71.bcfca1f9-e47e-41b7-a86c-5644ef777b7a.template

Stack description
AWS CloudFormation Template for Cisco Catalyst 9800-CL Wireless Controller for Cloud --AWSMP::36aaa0b8-cf25-45aa-9fcc-16915f24ce71::fca11194-78c0-43ed-debf-439f521f4376

Step 2: Specify stack details

Figure 166: Review the Settings - Part 2



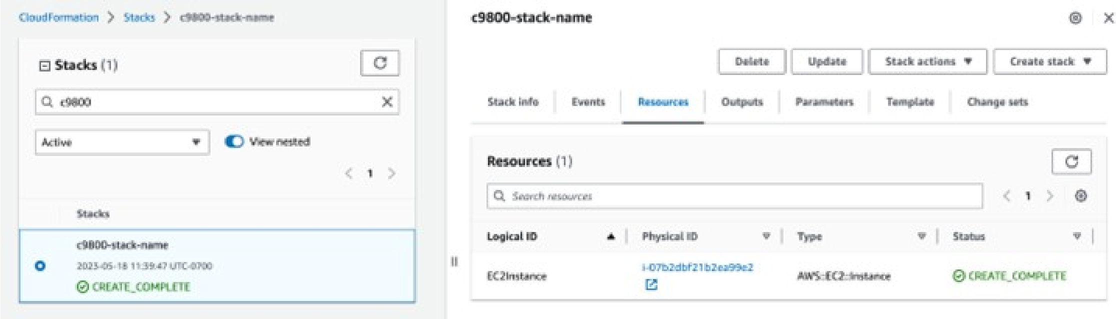
Stack creation options

Timeout
-

Termination protection
Deactivated

Step 17 Wait a few seconds for the status to change from **CREATE_IN_PROGRESS** to **CREATE_COMPLETE**.

Figure 167: Configuration Completion Status



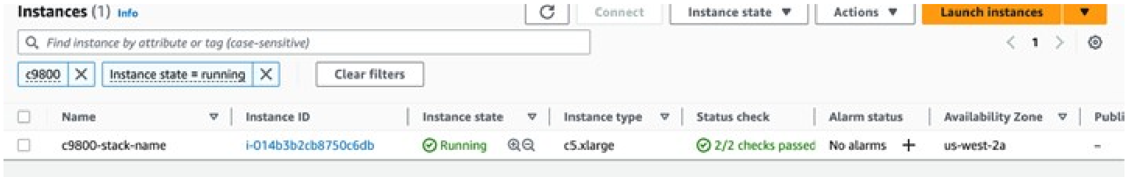
Stacks: c9800-stack-name, 2023-05-18 11:39:47 UTC-0700, CREATE_COMPLETE

Resources (1)

Logical ID	Physical ID	Type	Status
EC2Instance	i-07b2dbf21b2ea99e2	AWS::EC2::Instance	CREATE_COMPLETE

Step 18 Go to the **EC2** dashboard and click **Running Instances**.

Figure 168: EC2 Dashboard



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Publi
c9800-stack-name	i-014b3b2cb8750c6db	Running	c5.xlarge	2/2 checks passed	No alarms	us-west-2a	–

Configure the Cisco Catalyst 9800-CL Wireless Controller Using CLI Commands

The day zero web-based guided workflow can be skipped when configuring the CLI commands for the basic settings. After these steps, you can access the GUI for day one configuration. For the Cisco Catalyst 9800-CL Wireless Controller (C9800-CL) on AWS cloud, GigabitEthernet 1 is the only available interface and has the following characteristics:

- Uses a Layer 3 interface (AWS only supports this type of interface).
- Gets the IP address using DHCP.
- Does not have a wireless CLI wizard for the Catalyst 9800-CL Wireless Controller.

Procedure

Step 1 Access the CLI commands through SSH. Use the .pem file to authenticate using the certificate, `chmod 400 <file>.pem`

```
ssh -i “file name.pem” ec2-user@<c9800-CL IP>
```

Step 2 (Optional) Set the hostname to the following:

```
WLC(config)#hostname C9800
```

Step 3 Enter the config mode, and add the login credentials using the following command:

```
C9800(config)#username <name> privilege 15 password <yourpwd>
```

Step 4 Verify the GigabitEthernet 1 configuration and IP address. The following interface is configured for DHCP.

```
c9800#sh run int gig 1
Building configuration...
Current configuration : 99 bytes
!
```

```
interface GigabitEthernet1
ip address dhcp
negotiation auto
no mop enabled
no mop sysid
end

C9800#show ip int brief

Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet1       172.38.0.10     YES DHCP   up                    up

Vlan1                  unassigned      YES unset  administratively down down

C9800#
```

Step 5 Disable the wireless network to configure the country code.

```
C9800(config)#ap dot11 5ghz shutdown
Disabling the 802.11a network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
C9800(config)#ap dot11 24ghz shutdown
Disabling the 802.11b network may strand mesh APs.
Are you sure you want to continue? (y/n)[y]: y
```

Step 6 Configure the AP country domain. This configuration triggers the GUI to skip the day zero workflow because the Catalyst 9800 Series Wireless Controller needs a country code to be operational.

```
C9800(config)# c9800-10-30(config)#ap country ?
WORD Enter the country code (e.g. US,MX,IN) upto a maximum of 20 countries

C9800(config)#ap country US
```

Changing a country code could reset the channel and RRM grouping configuration. After implementing this command, check the customized APs for valid channel values and if the wireless controller is running in RRM One-Time mode, reassign the channels.

```
Are you sure you want to continue? (y/n)[y]: y
```

```
C9800(config)#
```

Step 7 A certificate is needed for the AP to join the virtual Catalyst 9800 Series Wireless Controller. The certificate can be created automatically through the day zero workflow or manually using the following commands:

Specify the interface to be the wireless management interface.

```
C9800(config)#wireless management interface gig 1In exec mode, issue the following command:
C9800#wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 <pwd>
Configuring vWLC-SSC…
Script is completed
This is a script the automates the whole certificate creation:Verifying Certificate
Installation:C9800#show wireless management trustpoint
Trustpoint Name : ewlc-default-tp
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : e55e61b683181ff0999ef317bb5ec7950ab86c9e
Private key Info : Available
```

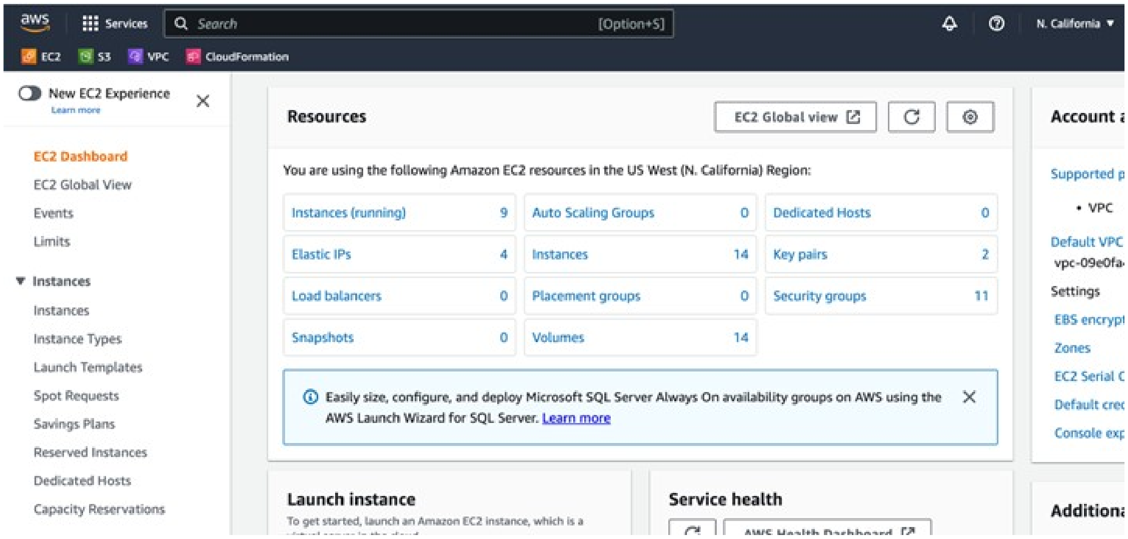
Note You can skip the certificate or trustpoint configuration, but doing so will not allow the APs to join. Instead, you would have to configure the certificate from the GUI by importing the desired certificate.

Step 8 To access the main dashboard, use https://<IP of the wireless management interface> and the credentials that you entered earlier. Because the box has a country code that is configured, the GUI skips the day zero window, and you can access the main dashboard for day one configuration.

Step 9 For provisioning the Catalyst 9800-CL Wireless Controller from Cisco DNA Center, change the management interface from DHCP to static using the following steps:

a) Navigate to the AWS console and find the **EC2 Dashboard**.

Figure 169: EC2 Dashboard



Resources

You are using the following Amazon EC2 resources in the US West (N. California) Region:

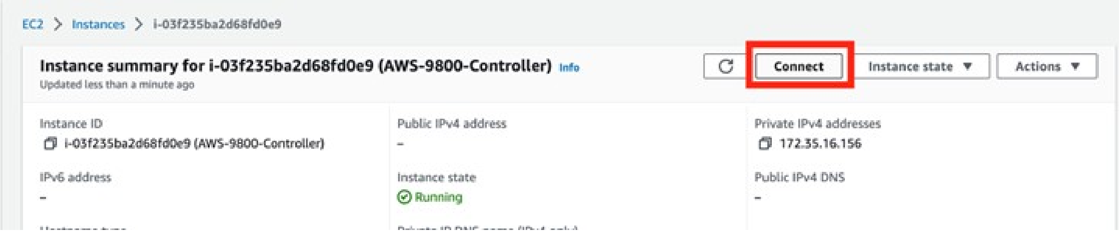
Instances (running)	9	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	4	Instances	14	Key pairs	2
Load balancers	0	Placement groups	0	Security groups	11
Snapshots	0	Volumes	14		

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

b) Click **Instances** and choose the Catalyst 9800-CL Wireless Controller instance.

Figure 170: EC2 Instance



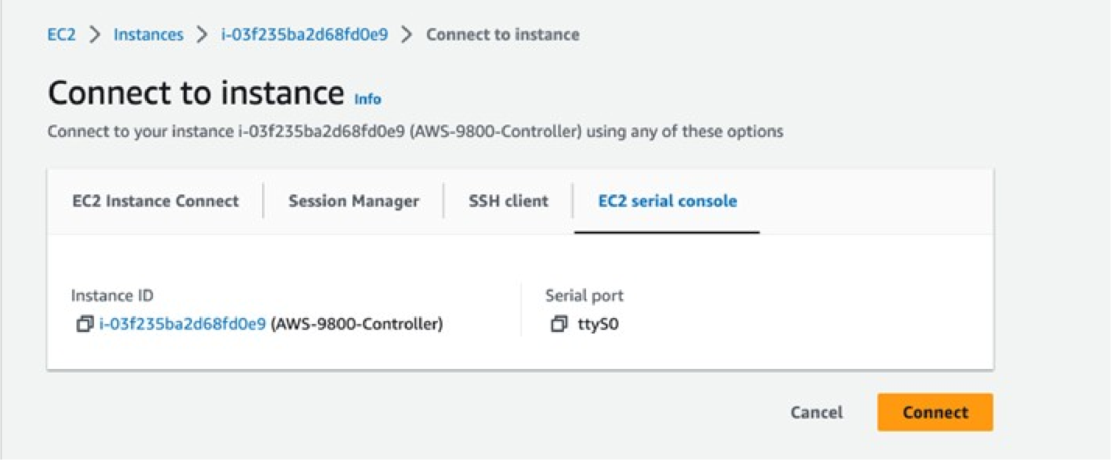
Instance summary for i-03f235ba2d68fd0e9 (AWS-9800-Controller)

Updated less than a minute ago

Instance ID i-03f235ba2d68fd0e9 (AWS-9800-Controller)	Public IPv4 address –	Private IPv4 addresses 172.35.16.156
IPv6 address –	Instance state Running	Public IPv4 DNS –

Step 10 Click **Connect**.

Figure 171: Connect to Instance Window



EC2 > Instances > i-03f235ba2d68fd0e9 > Connect to instance

Connect to instance Info

Connect to your instance i-03f235ba2d68fd0e9 (AWS-9800-Controller) using any of these options

Instance ID: i-03f235ba2d68fd0e9 (AWS-9800-Controller)

Serial port: ttyS0

Step 11 Unconfigure `ip address dhcp` under `interface gig 1` and configure the static IP address `ip address 172.38.0.10`.

Discover and Manage the Cisco Catalyst 9800-CL Wireless Controller Deployed on AWS

The discovery process is the same for other Cisco Catalyst 9800-CL Wireless Controllers.

Provision the Cisco Catalyst 9800-CL Wireless Controller Deployed on AWS

Provision the Catalyst 9800 Series Wireless Controller so that the San Jose area is the primary managed AP location for the wireless controller.

The following steps explain how to provision the **corpevent-profile** wireless profile (defined in *Define the wireless network*) to the Catalyst 9800-CL Wireless Controller.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The **Inventory** window displays the devices. By default, the **Focus** is set to **Default**.

Step 2 Locate and check the check box for the Catalyst 9800 Series Wireless Controller.

Step 3 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

Step 4 Click **Choose a Site**.

A slide-in pane is displayed, showing the site hierarchy configured for Cisco DNA Center. For this deployment guide, the Catalyst 9800 Series Wireless Controller is assigned to the building level.

Step 5 Expand the site hierarchy for San Jose and choose Eventcenter.

Step 6 Click **Save** to assign Catalyst 9800 Series Wireless Controller to San Jose/Eventcenter.

Step 7 Click **Next** to move to the next step in the device provisioning workflow.

Step 8 In the **Configuration** window, choose **Active Main WLC** for the **WLC Role**.

Step 9 Continue clicking **Next** until you reach the **Summary** window.

The **Summary** window provides a summary of the configuration that will be provisioned to the Catalyst 9800 Series Wireless Controller.

You can expand each section to see the details of the configuration. The configuration is based on the **branch5** wireless profile, created in the *Design the wireless network* section of this deployment guide.

Step 10 Click **Deploy** to deploy the configuration to the Catalyst 9800-40 Wireless Controller. A slide-in pane is displayed. You can deploy the configuration now; you can schedule the configuration to be deployed later; or you can generate a configuration preview. If you choose to generate a preview, a preview is created, which can be deployed later on selected devices. If a site assignment is invoked during a configuration preview, the device controllability configuration will be pushed to the corresponding device(s). You can view the status in **Work Items**.

Note It is best practice to make configuration changes and provision new devices in your network only during scheduled network operation change windows.

Step 11 Click the **Now** radio button and click **Apply** to apply the configuration.

You will be taken back to the **Inventory** window within the provisioning dashboard. The provisioning status of the device will temporarily be set to **Configuring**, but the status should change to **Success** after a few minutes. For more information about provisioning, you can click **See Details** directly below the provisioning status of the device.

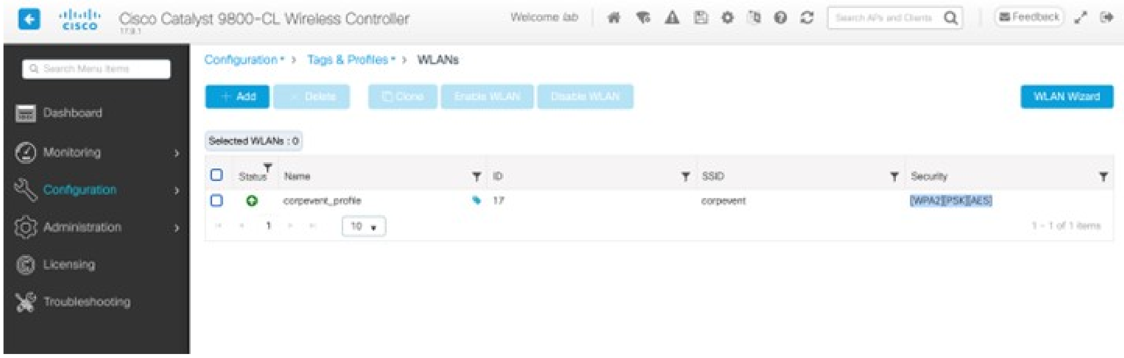
The following table shows the names of the WLAN profiles and their respective SSIDs, automatically generated by Cisco DNA Center during the provisioning of Catalyst 9800 Series Wireless Controller for this deployment guide.

Table 32: WLAN Profiles Dynamically Generated by Cisco DNA Center

WLAN Profile Name	SSID	WLAN ID	Security
corpevent_profile	corpevent	17	[WPA2][PSK][AES]

An example of the WLAN configuration, as seen from the web-based GUI of Catalyst 9800 Series Wireless Controller-1, is shown in the following figure.

Figure 172: WLANs/SSIDs Dynamically Created by Cisco DNA Center



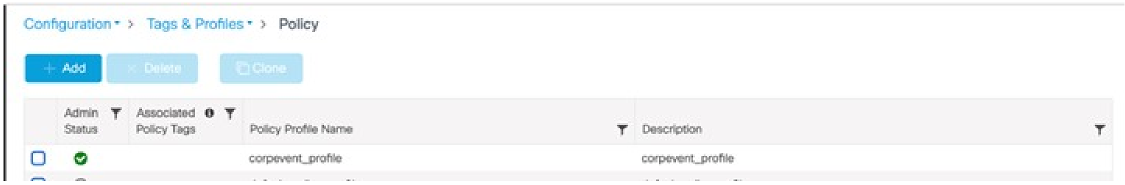
Selected WLANs : 0

□	Status	Name	ID	SSID	Security
□	●	corpevent_profile	17	corpevent	[WPA2][PSK][AES]

1 | 10 | 1 - 1 of 1 items

During provisioning, Cisco DNA Center creates a new policy profile in the Catalyst 9800 Series Wireless Controller. The names of the new policy profiles match the names of the created WLAN profiles. An example of the configuration, as seen from the web-based GUI of Catalyst 9800 Series Wireless Controller is shown in the following figure.

Figure 173: Policy Tag Created by Cisco DNA Center



	Admin Status	Associated Policy Tags	Policy Profile Name	Description
□	✓		corpevent_profile	corpevent_profile

At this point in the provisioning process, the policy profiles and the WLAN profiles are not mapped to any policy tag applied to any AP. Likewise, no flex profiles have been created.

Join New APs to the Enterprise Cisco Catalyst 9800 Series Wireless Controller

The following steps explain how to discover and join the APs to the enterprise Catalyst 9800 Series Wireless Controller.

Before you begin

For this procedure in the deployment guide, assume that new APs will use IP DHCP discovery to discover the Cisco Catalyst 9800 Series Wireless Controller. Also assume that the new APs have never been primed. A Cisco AP has been primed when it has previously joined (established a CAPWAP tunnel) a wireless controller and cached the IP address of the wireless controller in NVRAM; or when primary, secondary, or tertiary wireless controller management IP addresses have been configured within the AP. In such scenarios, the AP will give preference to the primary, secondary, or tertiary wireless controller configuration over IP DHCP discovery.

With IP DHCP discovery, DHCP servers use Option 43 to provide one or more wireless controller management IP addresses to the APs. When an AP learns the management IP address of the Catalyst 9800 Series Wireless Controller, the AP sends a CAPWAP join request message to the wireless controller. Once joined, the wireless controller manages the APs configuration, firmware, control transactions, and data transactions.

Procedure

Step 1 Configure the necessary VLANs on the Layer 2 access switches that support the Cisco APs joining the Catalyst 9800 Series Wireless Controller.

This deployment guide assumes that APs are connected to Layer 2 access switches. A dedicated VLAN is on the switches for APs that are separate from end-user devices, such as PCs and IP phones. The use of a dedicated VLAN for APs and switch management is generally regarded as a design best practice, but this method does result in additional VLANs being deployed on the switches.

The management VLAN (VLAN 64) is used for establishing CAPWAP tunnels to branch APs and for managing connectivity to the branch switch. The branch employee VLAN (VLAN 16) is used for locally terminating wireless traffic from the corporate event SSID on the branch switch.

Step 2 Configure VLAN 64 and VLAN 16 on the branch switch.

Step 3 Configure the switch port to which the AP is connected to be a trunk port, with VLANs 64 and 16 allowed and VLAN 16 as the native VLAN. Make sure the switch port is not shut down. An example is shown in the following configuration.

```
interface GigabitEthernet1/0/1
switchport trunk native vlan 64
switchport trunk allowed vlan 16,64
switchport mode trunk logging event trunk-status load-interval 30
no shutdown
```

```
spanning-tree portfast trunk
ip dhcp snooping trust
```

For this deployment guide, a Microsoft Active Directory (AD) server with IP address `10.4.48.9` functions as the IP DHCP server. The IPv4 address of the Catalyst 9800 Series Wireless Controller (C9800-CL deployed on AWS) configured within DHCP Option 43 is `172.38.0.10`. Configuration of the DHCP within the Microsoft AD server is outside the scope of this document.

The following example depicts the configuration of a Layer 3 switch using a VLAN switched virtual interface (SVI):

```
interface Vlan64
ip address 10.5.64.1
255.255.255.0
ip helper-address 10.4.48.10
```

```
interface Vlan16
ip address 10.5.16.1
255.255.255.0
ip helper-address 10.4.48.10
```

Step 4 Connect the Cisco AP(s) to the switch port(s) on the Layer 2 access switches.

The APs should get IP addresses and automatically join the Catalyst 9800 Series Wireless Controller. Once the new APs register with the wireless controller, a resync on Cisco DNA Center is automatically triggered. After the resync is complete, the new APs will show up in the inventory. Alternatively, you can manually resync the inventory for the wireless controller using the following steps:

a. From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

b. Check the check box for the device name.

c. From the **Actions** drop-down list, choose **Inventory** > **Resync Device**.

d. Click **Ok** in the warning window to confirm the resync.

After you have resynced the Catalyst 9800-40 wireless controller HA SSO pair (WLC-9800-2), the APs that are joined to the wireless controller should appear within the inventory.

Provision the New APs

Once the APs have joined to the Cisco Catalyst 9800 Series Wireless Controller, they must be provisioned. Provisioning with Cisco DNA Center is necessary for the APs to receive the correct configuration to advertise the **corpevent** SSIDs.

Use the following steps to provision APs within Cisco DNA Center.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The main provisioning window displays the devices. By default, the **Focus** will be set for **Inventory**.

Step 2 Locate and check the check box for each of the APs to be provisioned.

Step 3 From the **Actions** drop-down menu, choose **Provision** > **Provision Device**.

You are taken through a workflow for provisioning the APs, starting with **Assign Site**.

Step 4 For each of the APs, click **Choose a Site**.

A slide-in pane is displayed, showing the site hierarchy configured for Cisco DNA Center. Expand the site hierarchy for Milpitas and choose the building (**Branch 5**) and the floor (**Floor 1** or **Floor 2**) for each AP.

The following table lists the APs that are provisioned in this deployment guide, including their locations:

AP Name	AP Model	Location
mil23-floor1-ap1	C9130AXI-B	Building 23, Floor 1
mil23-floor1-ap2	C9130AXI-B	Building 23, Floor 1
mil23-floor2-ap1	C9130AXI-B	Building 23, Floor 2
mil24-floor1-ap1	C9124AXD-B	Building 24, Floor 1
mil24-floor2-ap1	C9124AXD-B	Building 24, Floor 2
AP1416.9D7C.16FC	C9130AXI-B	Branch 5, Floor 1
AP1416.9D7C.16F8	C9130AXI-B	Branch 5, Floor 2

Step 5 Click **Save** to save the site assignments for the APs.

Step 6 Click **Next** to advance to the next step in the provisioning workflow, **Configuration**.

Step 7 From the **RF Profile** drop-down list, choose the RF profile to assign to each of the APs.

For this deployment guide, the TYPICAL RF profile was chosen. This RF profile was also selected as the default RF profile in *Design the wireless network*.

Step 8 Click **Next** to advance to the next step in the provisioning workflow, **Summary**.

The **Summary** window provides a summary of the configuration that will be provisioned to each of the APs.

Step 9 Click **Deploy** to provision the APs.

A slide-in pane is displayed. You can choose to deploy the configuration now, or you can schedule the configuration for later.

Note The best practice is to make configuration changes and provision new devices in your network only during scheduled network operation change windows.

Step 10 Click the **Now** radio button and click **Apply** to apply the configuration.

A **Success** dialog box should be displayed, indicating that after provisioning, the APs will reboot.

Step 11 Click **OK** to confirm.

The policy, site, and RF tags provisioned through Cisco DNA Center can be verified on the wireless controller GUI.

At this point, wireless clients should be able to associate with the **corpevent** SSIDs and authenticate the network.

Monitor and Operate the Wireless Network

This section describes daily monitoring and operations on the wireless network via Cisco DNA Center, which has already deployed the network.

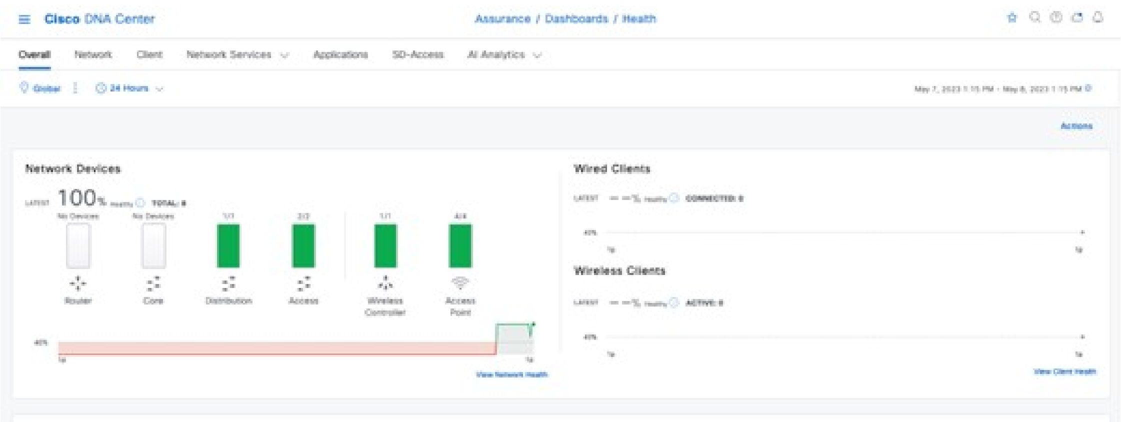
Monitor Wireless Network Health

Cisco DNA Center monitors network health by calculating the score using critical Key Performance Indicators (KPIs). Device health is calculated using KPIs collected for each device. Each device type uses different KPIs to compute health. For example, APs use RF parameters such as interference, utilization, air quality, and noise, while wireless controllers use link errors, free Mbuf, packet pools, free timers, and WQE pools. Device health is presented in Cisco DNA Center at the **Global** site, and individual device levels under the **Assurance** section.

Global-Level Network Health

From the top-left corner, click the menu icon and choose **Assurance** > **Health**. The **Overall** health window is displayed, showing the global-level network health defined by the ratio of healthy devices to the total number of devices.

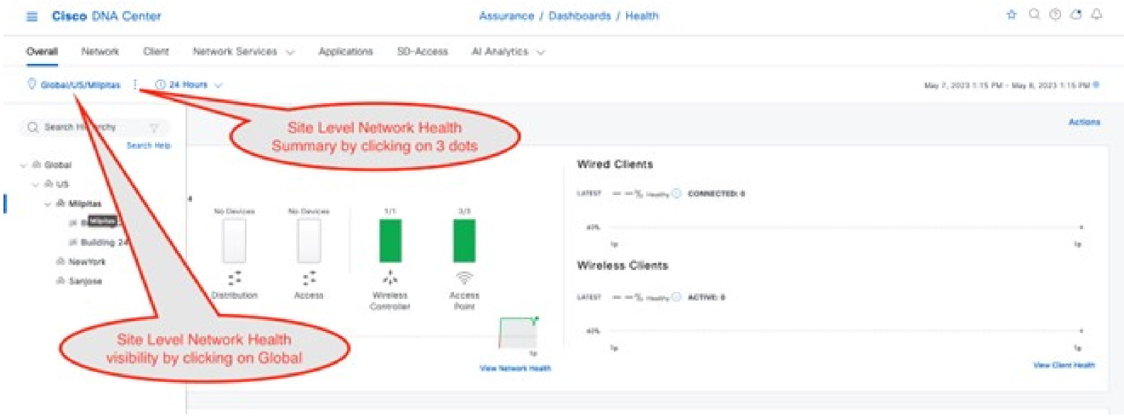
Figure 174: Overall Window



Site-Level Network Health

Click Global ⋮ to view the site-level network health, or click ⋮ to view the site-level network health summary.

Figure 175: Site-Level Network Health



Site Level Network Health Summary by clicking on 3 dots

Site Level Network Health visibility by clicking on Global

Device-Level Health

Click the **Network** tab. In the **Network Devices** dashboard, click a device name in the **Device Name** column.

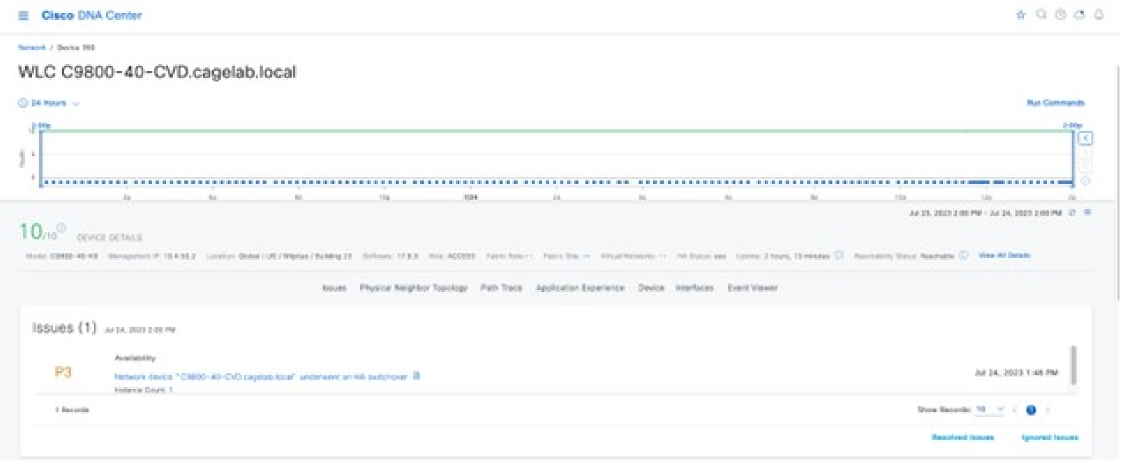
The **Device 360** window displays a 360-degree view of the network device, which shows the health change over a period of time. Hover your cursor over the timeline slider to view the health and events information about the network device over a period of time.

Wireless Controller 360

The health timeline is displayed at the top of the **Device 360** window. The device-level details, such as model, management IP, location, current software version, and high availability status, are displayed in the **Device Details** area. Hover your cursor over the timeline to view more information. You can view statistics for the last 3 hours, 24 hours, or 7 days by choosing the required time from the drop-down list in the top-left corner. The health plot is available for a maximum of 30 days.

Note Make sure to assign the wireless controller to a site in order to view the wireless controller health.

Figure 176: Device 360 Window

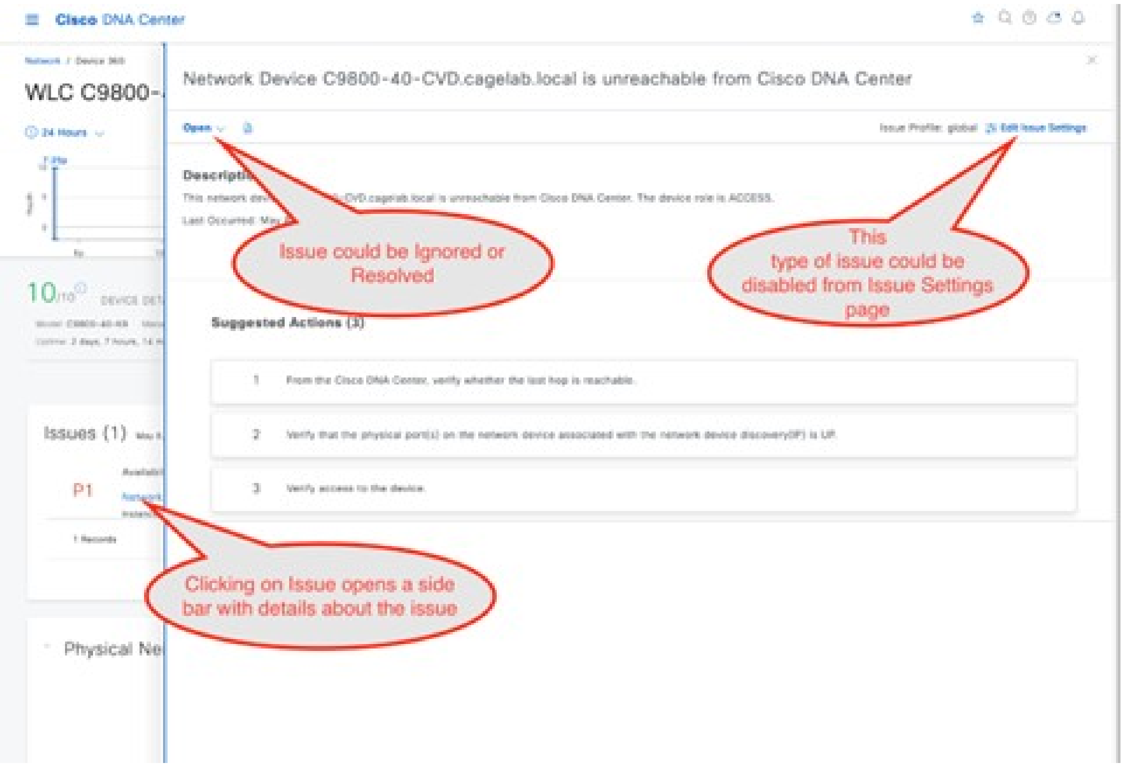


Network device "C9800-40-CVD.cagelab.local" underwent an HA switchover

Jul 24, 2023 1:48 PM

The **Issues** section displays major issues (if any) with a brief title of the issue. Click the corresponding issue title to view additional details about the issue. Choose **Assurance** > **Issue Settings**, where you can enable or disable a particular category of issue and its thresholds.

Figure 177: Example of a Wireless Controller Issue



Network Device C9800-40-CVD.cagelab.local is unreachable from Cisco DNA Center

Open · Issue Profile: global · Edit Issue Settings

Description

This network dev[illegible]-CVD.cagelab.local is unreachable from Cisco DNA Center. The device role is ACCESS.

Last Occurred: May [illegible]

Suggested Actions (3)

1 From the Cisco DNA Center, verify whether the last hop is reachable.

2 Verify that the physical port(s) on the network device associated with the network device discovery(IP) is UP.

3 Verify access to the device.

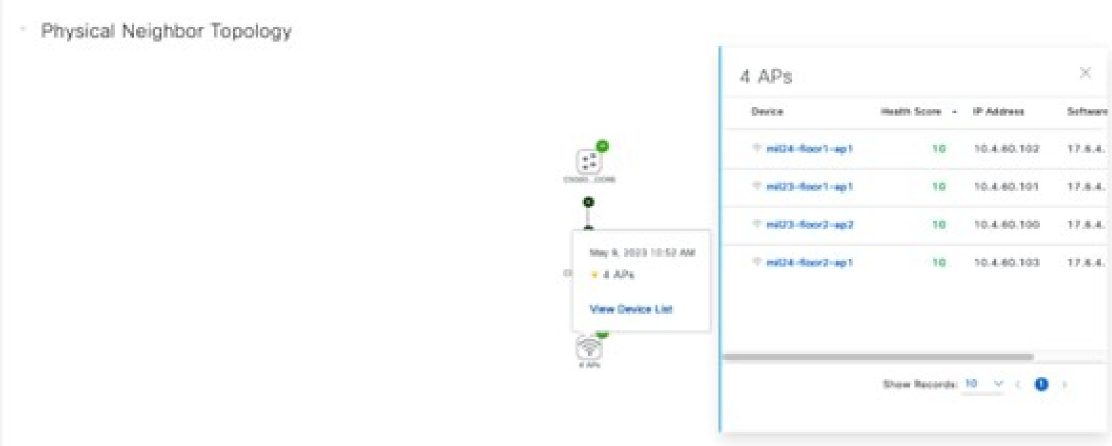
Issue could be Ignored or Resolved

This type of issue could be disabled from Issue Settings page

Clicking on Issue opens a side bar with details about the issue

The **Physical Neighbor Topology** section provides a visualization of the connectivity with the next-hop devices. Hover over your cursor over a device or click a device to view additional details. The chart provides the total number of APs and clients associated with the wireless controller.

Figure 178: Physical Neighbor Topology



May 9, 2023 10:52 AM

4 APs

Device	Health Score	IP Address	Software
mil24-floor1-ap1	10	10.4.60.102	17.6.4.
mil23-floor1-ap1	10	10.4.60.101	17.6.4.
mil23-floor2-ap2	10	10.4.60.100	17.6.4.
mil24-floor2-ap1	10	10.4.60.103	17.6.4.

Show Records: 10

The **Event viewer** section consolidates the events for the wireless controller in a table format. The events associated with a syslog message can be created into an issue that is generated and shown in the **Issues** section. To create this custom issue, choose **Assurance** > **Issue Settings** > **User Defined** and click **Create an Issue**.

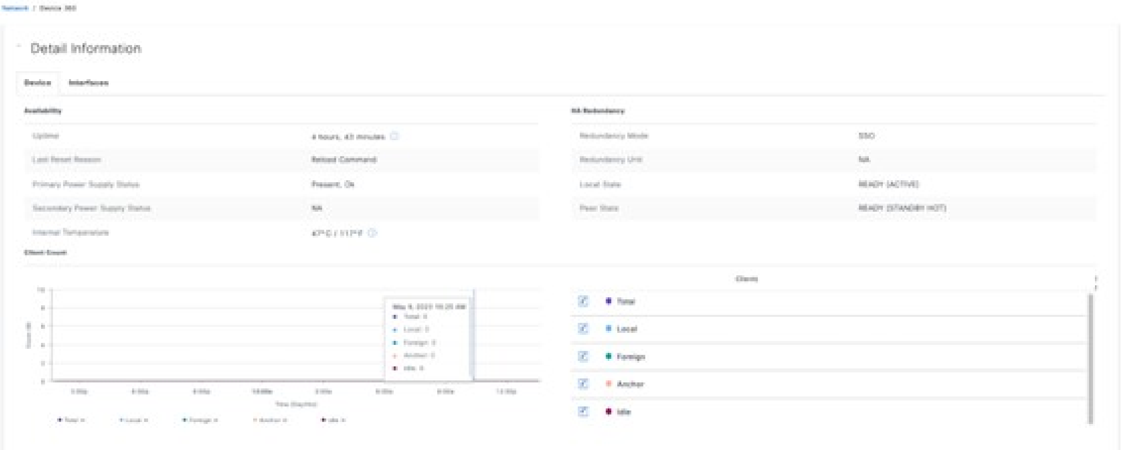
The **Path Trace** section helps to identify routing issues between the wireless controller and the destination device. Path trace only works if all the devices leading up to the destination device are discovered in Cisco DNA Center.

Note To use **Live Traffic**, you must enable wired endpoint data collection from **Design** > **Network Settings** > **Telemetry**. Also, all the associated devices must be provisioned from the inventory page.

The **Application Experience** section shows the application traffic from wireless clients seen by the wireless controller. If the APs are in local mode, the wireless controller can be the application traffic exporter. If the APs are in flex mode, any of the switches or routers carrying the traffic must export application traffic information to Cisco DNA Center. After 17.10.1 for wireless controllers, the APs in flex mode can still send application traffic to Cisco DNA Center via wireless controllers.

The **Detail Information** section has **Device** and **Interfaces** subsections. The **Device** section has information on the wireless controller uptime, temperature, HA, and last reload reason. The charts have CPU, memory, temperature, and AP count over a period of time. The client count chart shows local, foreign, anchor, and idle information.

Figure 179: Device Details



Network / Device 360

Detail Information

Device Interfaces

Availability

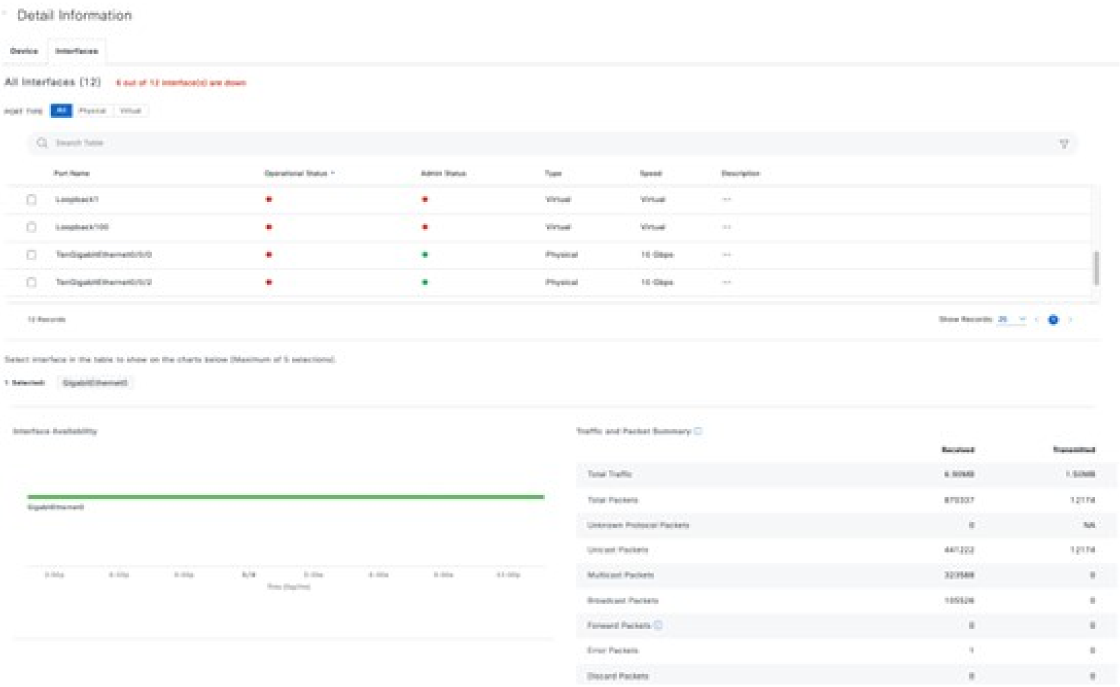
Uptime	4 hours, 43 minutes
Last Reset Reason	Reload Command
Primary Power Supply Status	Present, Ok
Secondary Power Supply Status	NA
Internal Temperature	47°C / 117°F

HA Redundancy

Redundancy Mode	SSO
Redundancy Unit	NA
Local State	READY (ACTIVE)
Peer State	READY (STANDBY HOT)

Client Count

Figure 180: Device Interface Details



Detail Information

Device | Interfaces

All Interfaces (12) 6 out of 12 interface(s) are down

Intf Type: All | Physical | Virtual

Search Table

	Port Name	Operational Status	Admin Status	Type	Speed	Description
□	Loopback1	🔴	🔴	Virtual	Virtual	--
□	Loopback100	🔴	🔴	Virtual	Virtual	--
□	TenGigabitEthernet0/0/0	🔴	🟢	Physical	10 Gbps	--
□	TenGigabitEthernet0/0/2	🔴	🟢	Physical	10 Gbps	--

12 Records

Show Records: 25

Select interface in the table to show on the charts below (Maximum of 5 selections).

1 Selected: GigabitEthernet0

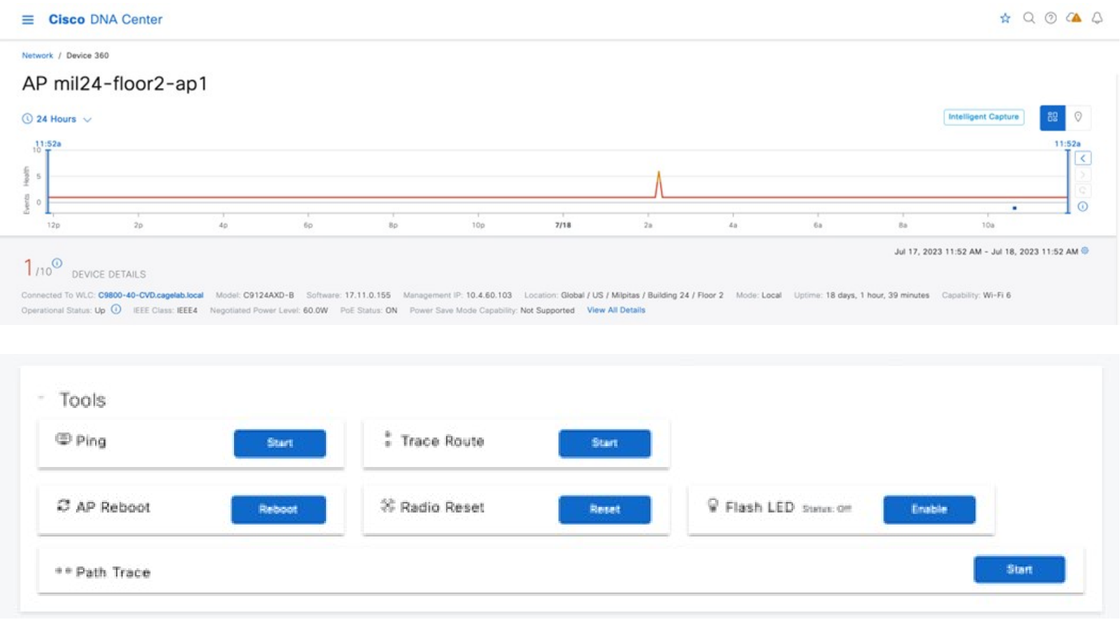
Interface Availability

Traffic and Packet Summary

	Received	Transmitted
Total Traffic	6.90MB	1.50MB
Total Packets	875337	12174
Unknown Protocol Packets	0	NA
Unicast Packets	441222	12174
Multicast Packets	323588	0
Broadcast Packets	105526	0
Forward Packets	0	0
Error Packets	1	0
Discard Packets	0	0

The **AP 360** window has most of the charts that the wireless controller has, such as the health timeline, issues, physical neighbor topology, event viewer, and detail information sections. The **AP 360** window also has AP-specific sections, such as tools to check connectivity, reload the AP, reset the radio, and control the flash LED. Under the **Detail** section, additional subsections exist for RF and POE that are specific to AP 360.

Figure 181: AP 360 Health Timeline



Jul 17, 2023 11:52 AM - Jul 18, 2023 11:52 AM

1 /10 DEVICE DETAILS

Connected To WLC: C9800-40-CVD.cagelab.local Model: C9124AXD-B Software: 17.11.0.155 Management IP: 10.4.60.103 Location: Global / US / Milpitas / Building 24 / Floor 2 Mode: Local Uptime: 18 days, 1 hour, 39 minutes Capability: Wi-Fi 6

Operational Status: Up IEEE Class: IEEE4 Negotiated Power Level: 60.0W PoE Status: ON Power Save Mode Capability: Not Supported View All Details

The following figure shows an example of the AP assigned to a valid policy profile, allowing the SSID starts to broadcast from the AP. After the AP starts broadcasting SSID, the memory usage interference and channel utilization increase, as shown in the following trend charts.

Figure 182: AP 360: CPU and Memory Charts

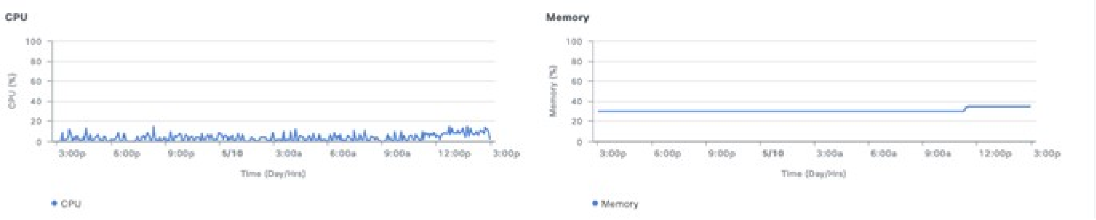


Figure 183: AP 360: Channel Utilization over Time

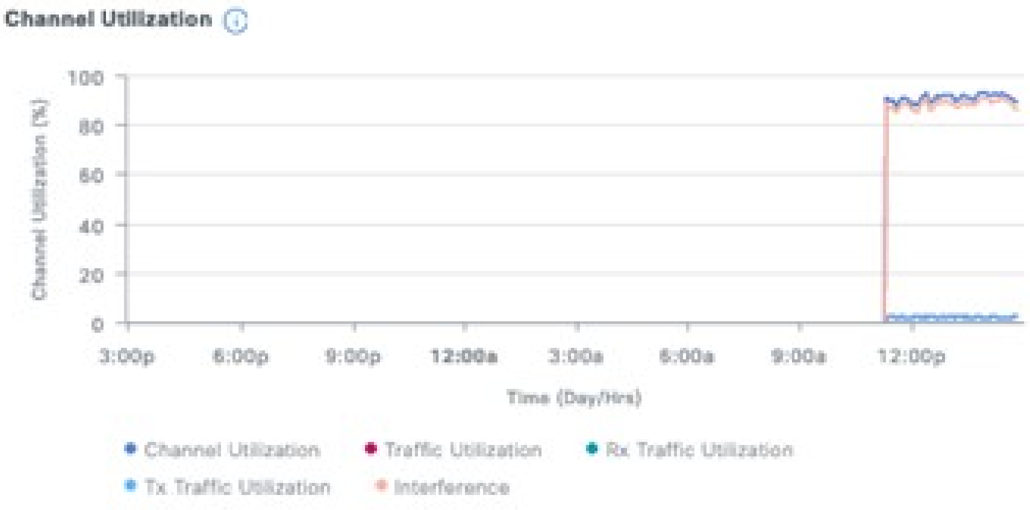
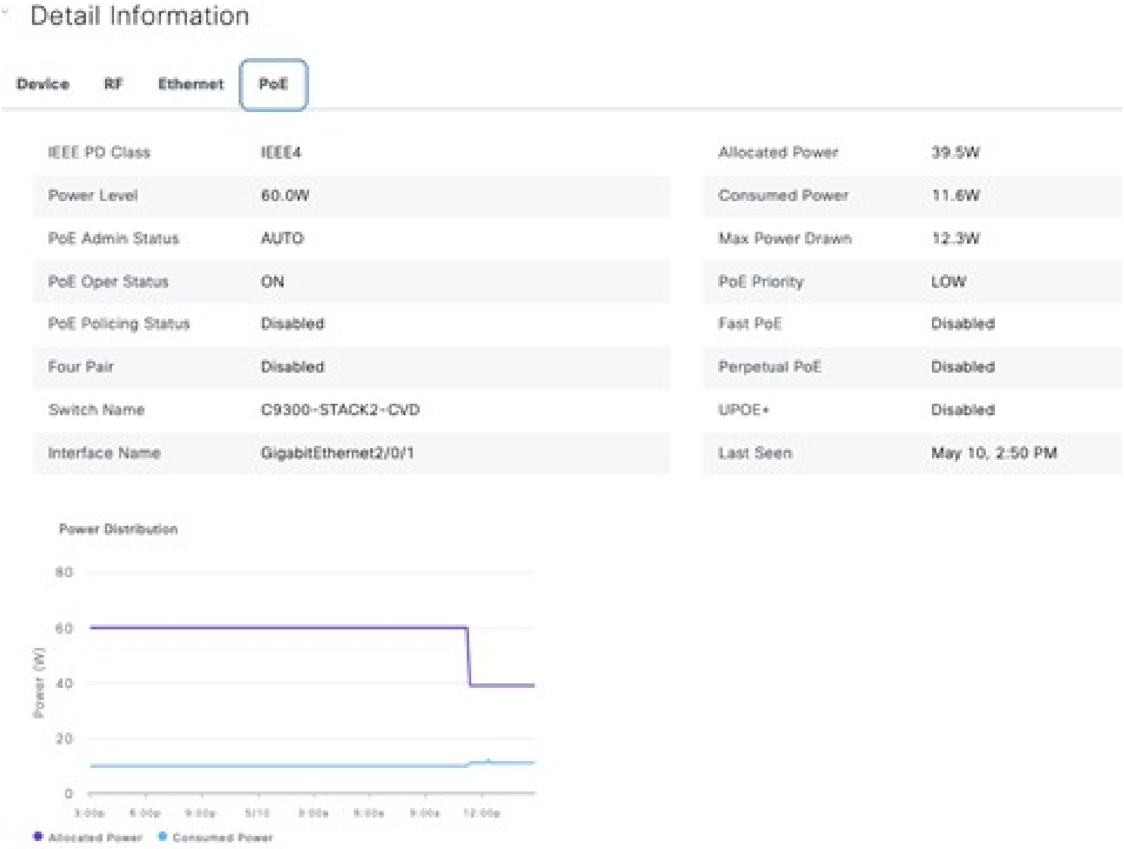


Figure 184: AP 360: PoE Information



Detail Information

Device RF Ethernet PoE

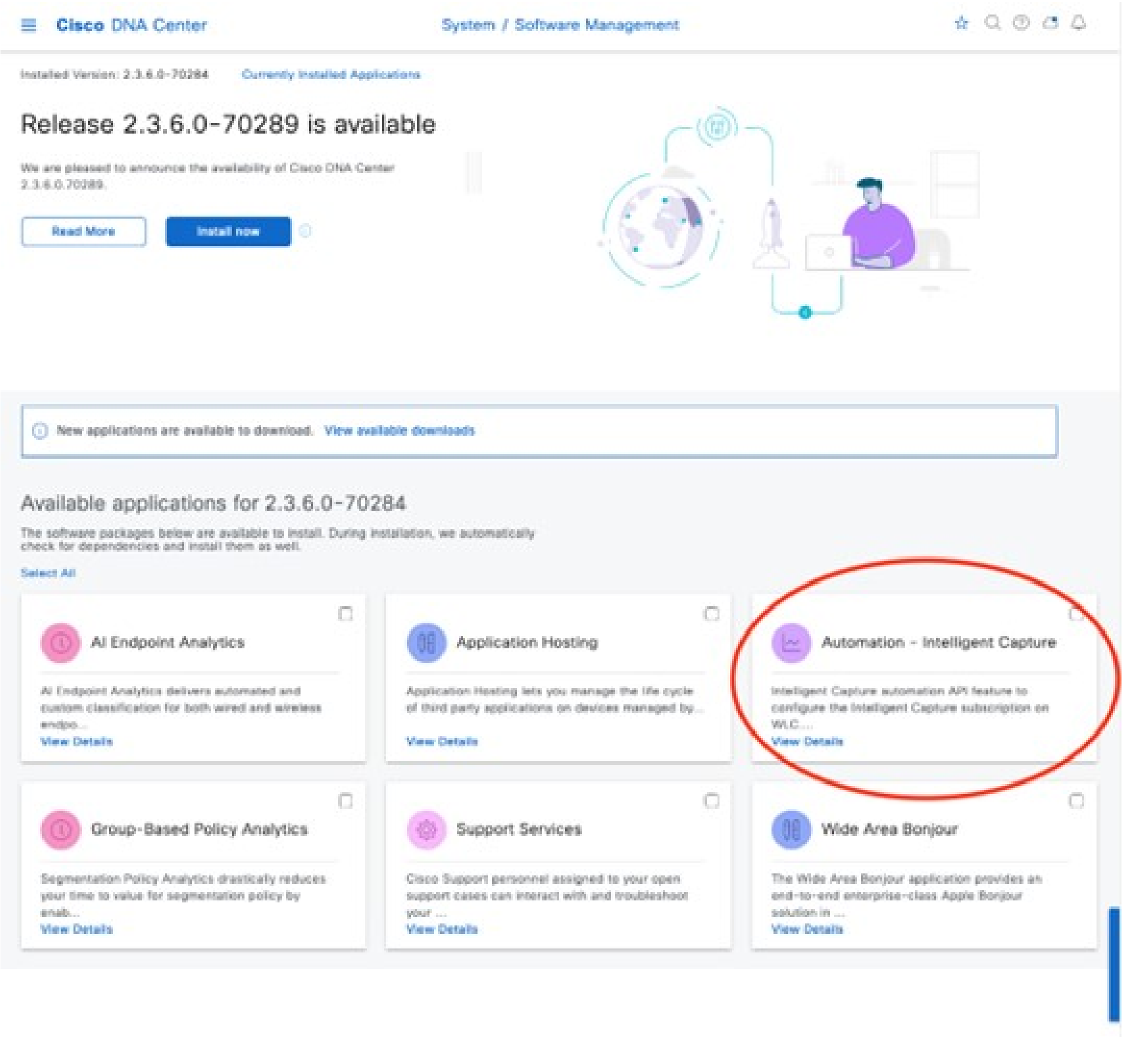
IEEE PD Class	IEEE4	Allocated Power	39.5W
Power Level	60.0W	Consumed Power	11.6W
PoE Admin Status	AUTO	Max Power Drawn	12.3W
PoE Oper Status	ON	PoE Priority	LOW
PoE Policing Status	Disabled	Fast PoE	Disabled
Four Pair	Disabled	Perpetual PoE	Disabled
Switch Name	C9300-STACK2-CVD	UPOE+	Disabled
Interface Name	GigabitEthernet2/0/1	Last Seen	May 10, 2:50 PM

Intelligent Capture

Intelligent Capture and APs

Intelligent Capture (ICAP) allows APs to capture packets and stream statistics directly from the APs to Cisco DNA Center via a gRPC tunnel. This feature requires the AP to be able to reach Cisco DNA Center directly via port 32626. If there is a firewall between the AP and Cisco DNA Center, this traffic needs to be allowed via the 32626 port. Up to the latest release Cisco DNA Center of 2.3.5.0, there is a scale limit of 1000 APs that can be enabled for statistics. By default, the ICAP application is not installed when shipped from the factory, so you must install the package from the **Software Management** window. The following figure shows that the Intelligent Packet Capture package is not yet installed as shipped from the factory.

Figure 185: Install Intelligent Packet Capture Package



Cisco DNA Center

System / Software Management

Installed Version: 2.3.6.0-70284 Currently Installed Applications

Release 2.3.6.0-70289 is available

We are pleased to announce the availability of Cisco DNA Center 2.3.6.0.70289.

New applications are available to download. View available downloads

Available applications for 2.3.6.0-70284

The software packages below are available to install. During installation, we automatically check for dependencies and install them as well.

Select All

□ AI Endpoint Analytics

AI Endpoint Analytics delivers automated and custom classification for both wired and wireless endpo...
View Details

□ Application Hosting

Application Hosting lets you manage the life cycle of third party applications on devices managed by...
View Details

□ Automation - Intelligent Capture

Intelligent Capture automation API feature to configure the Intelligent Capture subscription on WLC...
View Details

□ Group-Based Policy Analytics

Segmentation Policy Analytics drastically reduces your time to value for segmentation policy by enab...
View Details

□ Support Services

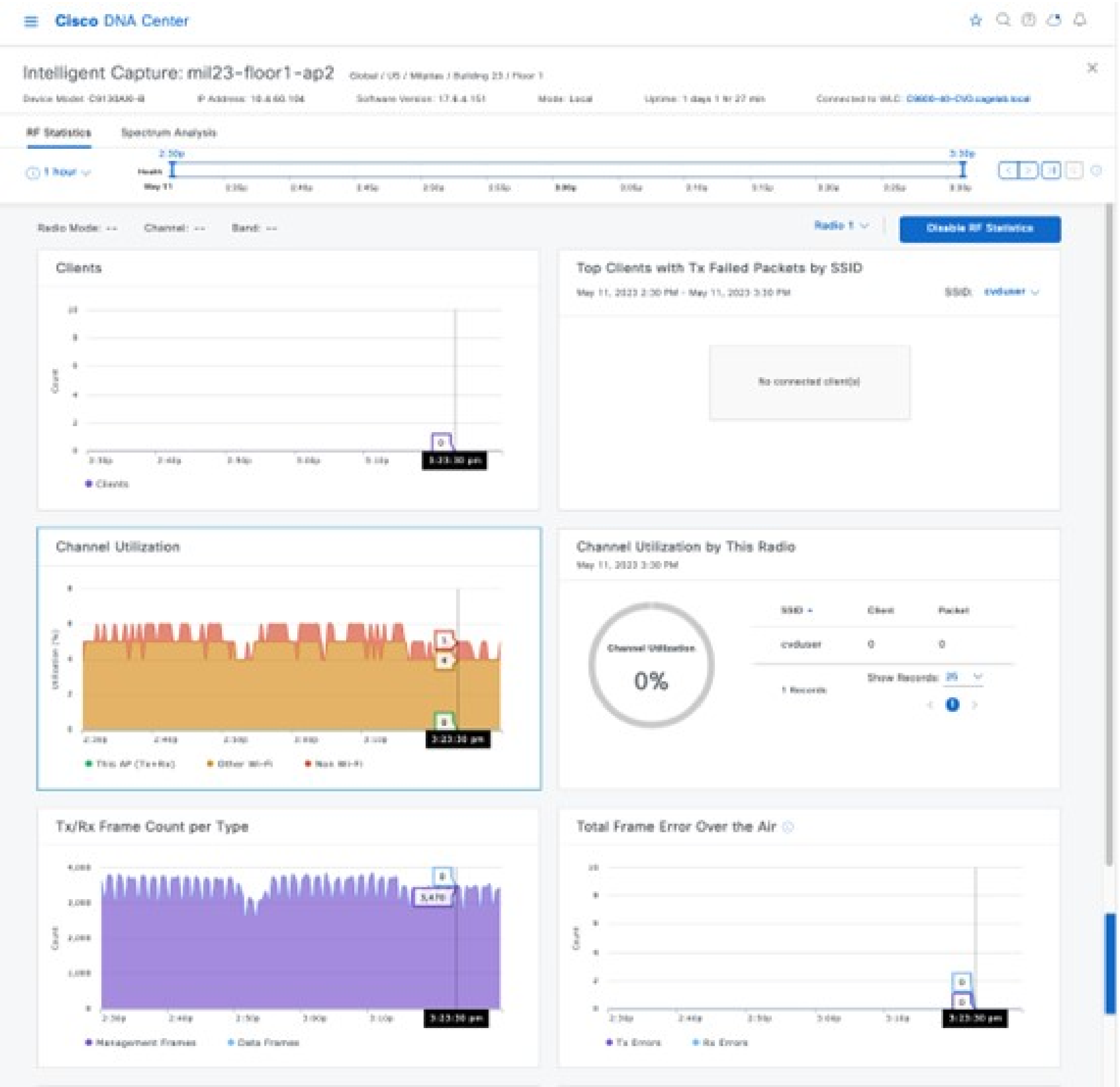
Cisco Support personnel assigned to your open support cases can interact with and troubleshoot your ...
View Details

□ Wide Area Bonjour

The Wide Area Bonjour application provides an end-to-end enterprise-class Apple Bonjour solution in ...
View Details

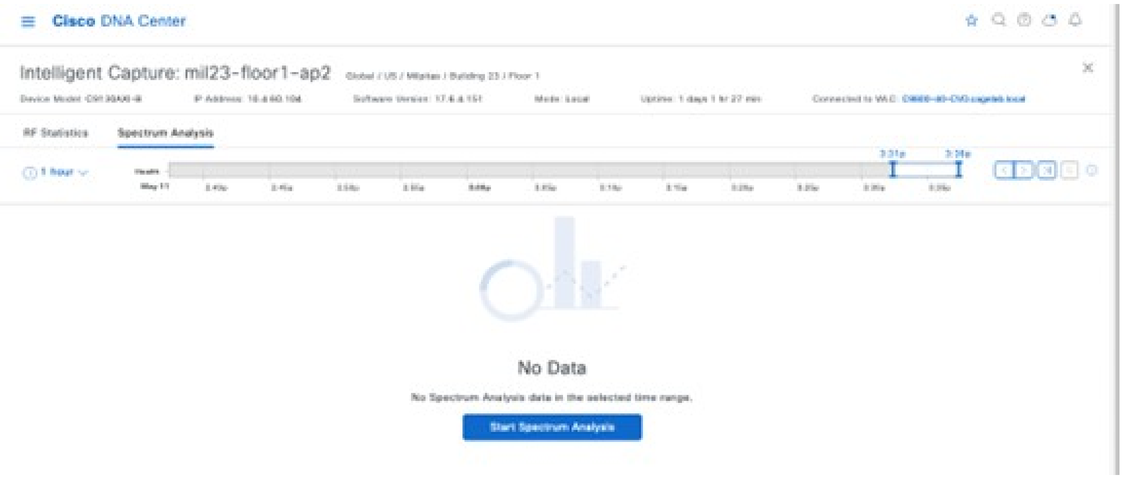
Choose the **Automation – Intelligent Capture** package and click **Install** to install the application. Once it is installed, the AP 360 page displays the **Intelligent Capture** button at the top right of the 360 page. Click the **Intelligent Capture** button to open a side bar. Click **Enable RF Statistics** at the top-right corner of the page to enable RF statistics. Alternatively, you can enable the RF statistics from the **Intelligent Capture Settings** page by navigating to **Assurance** > **Settings** > **Intelligent Capture Settings** > **Access Points**. Enabling the RF statistics takes a few minutes, based on the scale on the Cisco DNA Center. Once enabled, the charts in the **Intelligent Capture** window display statistics for clients, channel utilization, Tx/RX frame count, frame errors, Tx power, and multicast or broadcast counts as shown in the following figure. The statistics are updated every 30 seconds. Click either **Enable RF Statistics** or **Disable RF Statistics** to change the band of the AP.

Figure 186: Intelligent Capture for AP after RF Statistics is Enabled



Click the **Spectrum Analysis** tab to enable an AP. Click **Start Spectrum Analysis** to configure an AP to start capturing spectrum analysis data and stream it to the Cisco DNA Center, as shown in following figure. The spectrum analysis can only run for 10 minutes at a time.

Figure 187: Intelligent Capture Spectrum Analysis Window



Cisco DNA Center

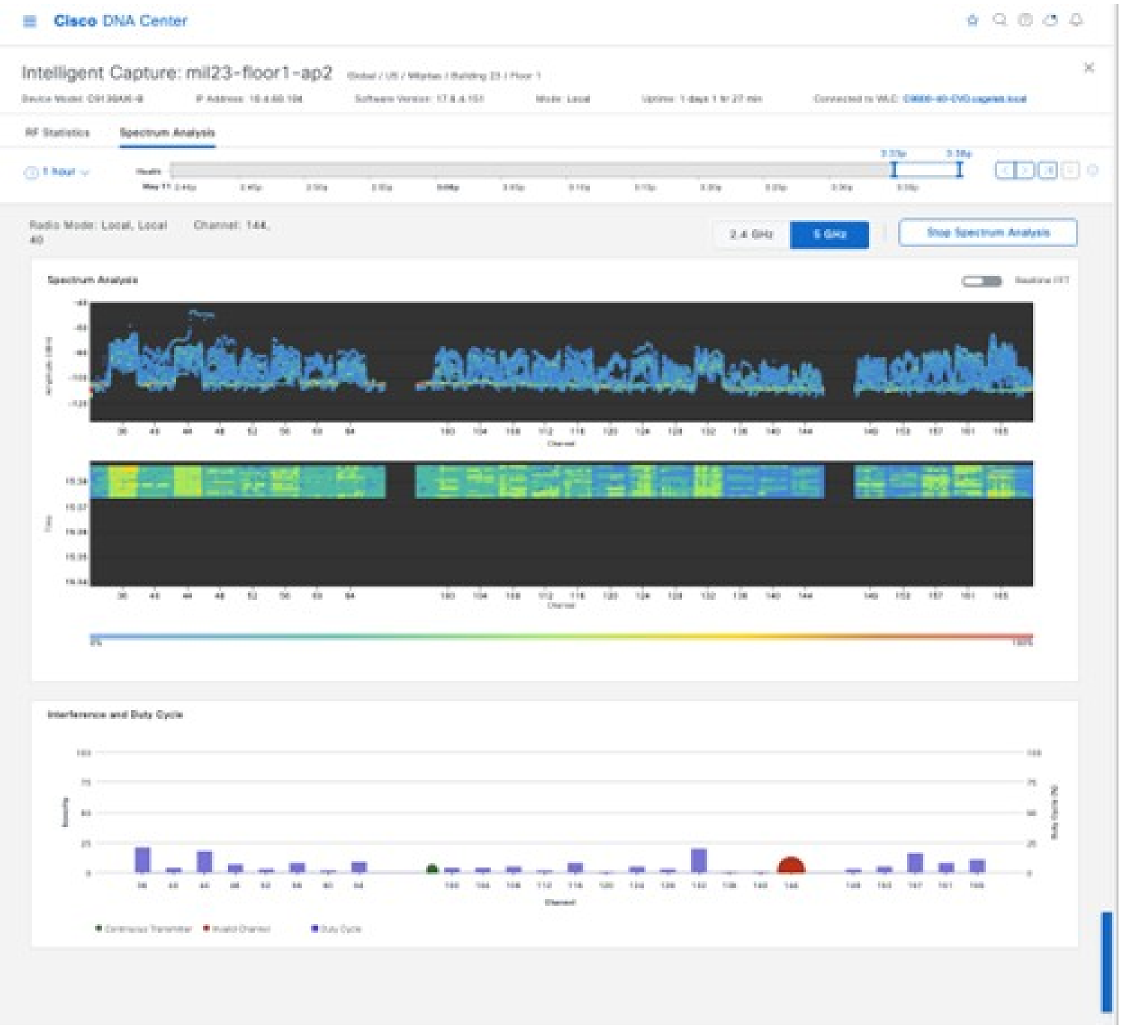
Intelligent Capture: mil23-floor1-ap2 Global / US / Milpitas / Building 23 / Floor 1

Device Model: C9130AXI-B IP Address: 10.4.60.104 Software Version: 17.6.4.151 Mode: Local Uptime: 1 days 1 hr 27 min Connected to WLC: C9800-40-CVO.cagelab.local

No Data

No Spectrum Analysis data in the selected time range.

Figure 188: AP Spectrum Analysis for 5G Band



Cisco DNA Center

Intelligent Capture: mil23-floor1-ap2 Global / US / Milpitas / Building 23 / Floor 1

Device Model: C9130AXI-B IP Address: 10.4.60.104 Software Version: 17.6.4.151 Mode: Local Uptime: 1 days 1 hr 27 min Connected to WLC: C9800-40-CVO.cagelab.local

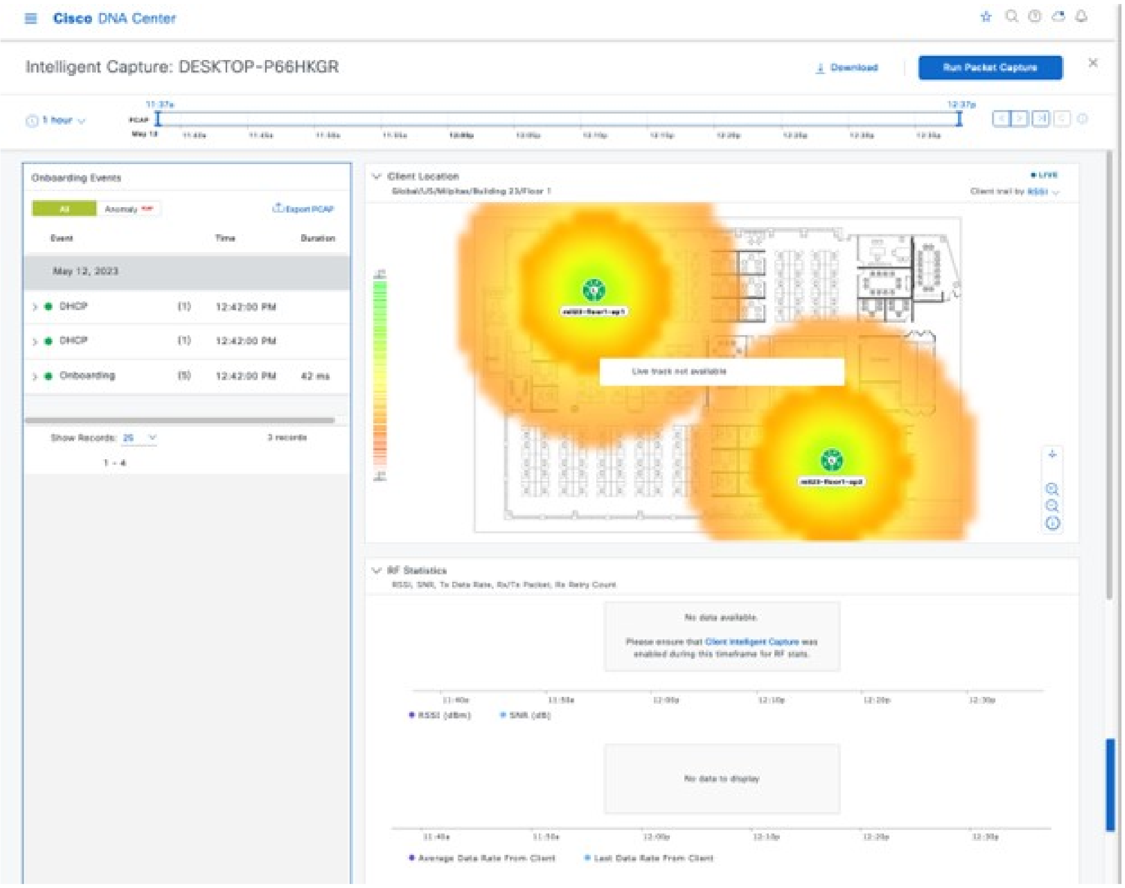
Radio Mode: Local, Local Channel: 144, 40

Once **Spectrum Analysis** is enabled and shown in Cisco DNA Center, it stays for 30 days and can be revisited by choosing that time frame and a duration (1, 3, or 5 hours), using the left or right arrow buttons. This feature is designed to be used live during a short period to capture RF conditions when an interference event is happening.

Intelligent Capture and Wireless Clients

ICAP enables live or scheduled packet capture for any wireless client that associates with an AP that is discovered by Cisco DNA Center. An ICAP page in the **Client 360** window also provides additional live statistics about the client, such as RF statistics, average data rate, and packet count over a period of time. The window also provides the events associated with client onboarding and a maps section showing the location of the client on the floor map if CMX/Cisco Spaces is integrated into Cisco DNA Center. The following figure shows the ICAP page for a wireless client before the onboarding packet capture is enabled.

Figure 189: Intelligent Capture for a Wireless Client Before Enabling ICAP



Intelligent Capture: DESKTOP-P66HKGR

Onboarding Events

Event		Time	Duration
May 12, 2023			
DHCP	(1)	12:42:00 PM	
DHCP	(1)	12:42:00 PM	
Onboarding	(5)	12:42:00 PM	42 ms

Show Records: 25 — 3 records — 1 - 4

Client Location — Global/US/Milpitas/Building 23/Floor 1

Live track not available

RF Statistics — RSSI, SNR, Tx Data Rate, Rx/Tx Packet, Rx Retry Count

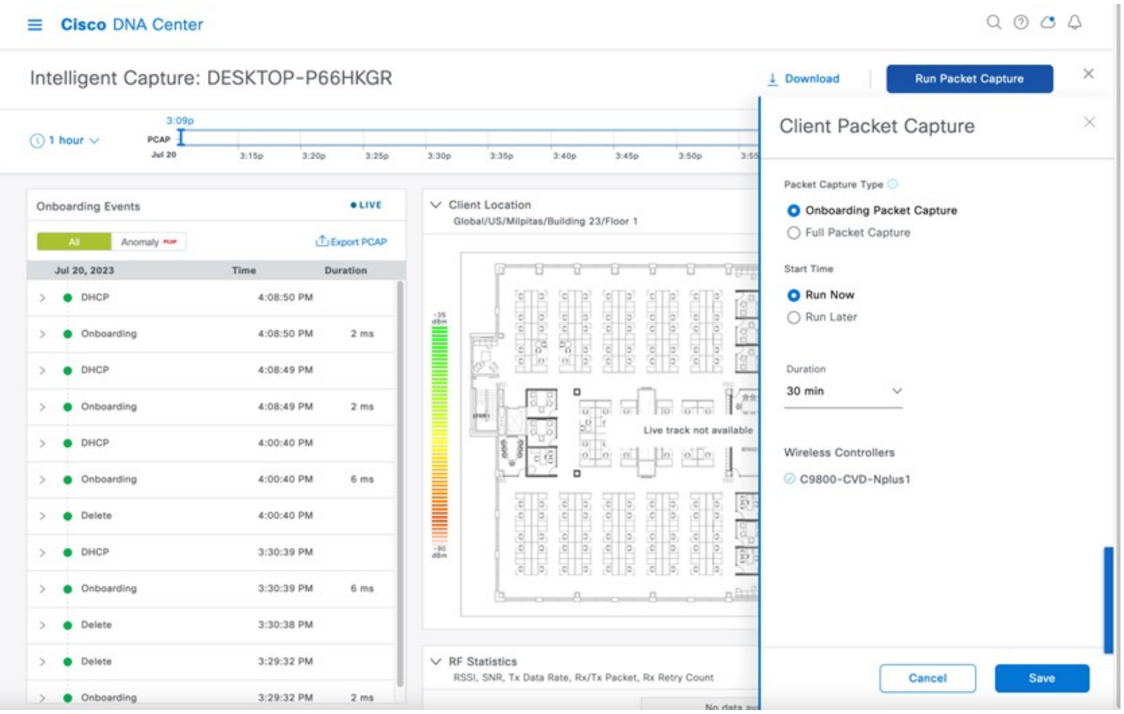
No data available.

Please ensure that Client Intelligent Capture was enabled during this timeframe for RF stats.

No data to display

Click **Run Packet Capture** in the top-right corner of the window to enable the onboarding packet capture. You can schedule this capture by clicking **Client Intelligent Capture**, which will bring you to the ICAP settings page. While enabling the onboarding packet capture, you can choose the desired wireless controller. A selected wireless controller will show a green check mark to the left of the wireless controller name. By default, the wireless controller where the client is currently associated will be selected, as shown in the following figure.

Figure 190: Packet Capture for Onboarding Events of Wireless Clients



Jul 20, 2023	Time	Duration
DHCP	4:08:50 PM	
Onboarding	4:08:50 PM	2 ms
DHCP	4:08:49 PM	
Onboarding	4:08:49 PM	2 ms
DHCP	4:00:40 PM	
Onboarding	4:00:40 PM	6 ms
Delete	4:00:40 PM	
DHCP	3:30:39 PM	
Onboarding	3:30:39 PM	6 ms
Delete	3:30:38 PM	
Delete	3:29:32 PM	
Onboarding	3:29:32 PM	2 ms

Client Packet Capture

Packet Capture Type

● Onboarding Packet Capture

○ Full Packet Capture

Start Time

● Run Now

○ Run Later

Duration

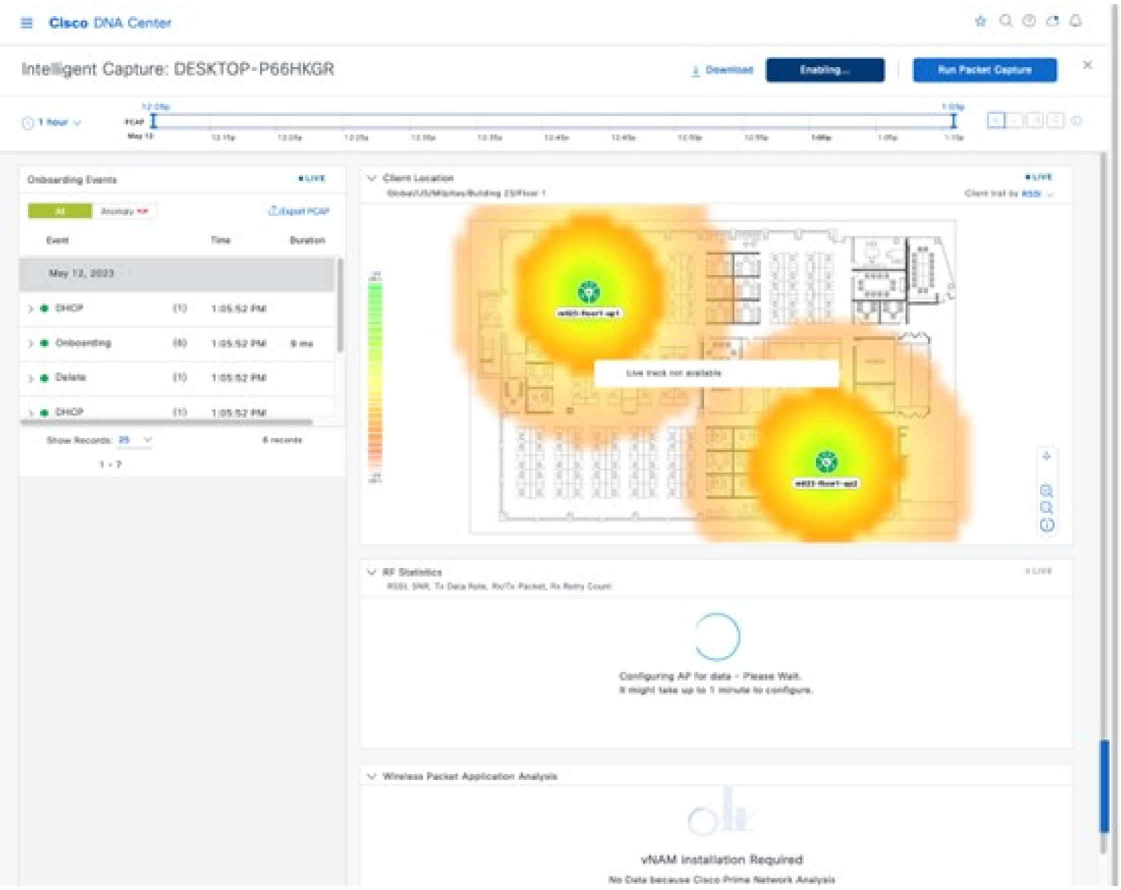
30 min

Wireless Controllers

C9800-CVD-Nplus1

Once you click **Save**, it will take several minutes to configure the wireless controller and AP to send the live packet capture for the wireless client, as shown in the following figure.

Figure 191: Configuring ICAP for Wireless Clients



Event		Time	Duration
May 12, 2023			
DHCP	(1)	1:05:52 PM	
Onboarding	(6)	1:05:52 PM	9 ms
Delete	(1)	1:05:52 PM	
DHCP	(1)	1:05:52 PM	

Show Records: 25 6 records

1 - 7

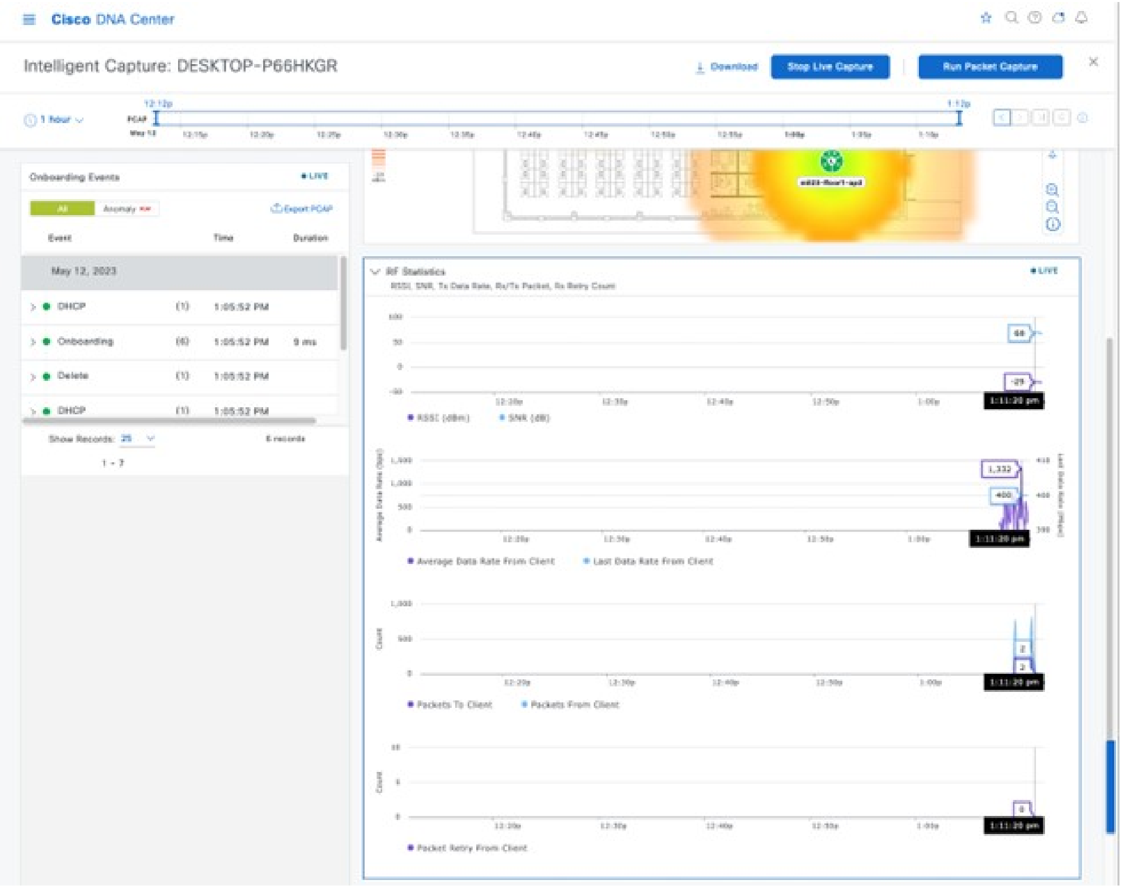
Configuring AP for data - Please Wait.
It might take up to 1 minute to configure.

vNAM Installation Required

No Data because Cisco Prime Network Analysis

After the wireless controller and APs are configured, live statistics about the client are displayed in the charts, as shown in following figure.

Figure 192: Live Onboarding Events and Statistics Shown in Intelligent Capture Window



Event		Time	Duration
May 12, 2023			
DHCP	(1)	1:05:52 PM	
Onboarding	(6)	1:05:52 PM	9 ms
Delete	(1)	1:05:52 PM	
DHCP	(1)	1:05:52 PM	

Show Records: 25 6 records

1 - 7

On the wireless controller and the AP, the configured settings can be verified using the following CLI:

- **C9800-40-CVD#show ap icap serviceability detail**

```
AP name          : mil23-floor1-ap1AP serviceability
gRPC server status
  WLC timestamp                   : 05/12/2023 13:29:55
  AP timestamp                    : 05/12/2023 13:29:54
  Status                          : ready
  Last success timestamp          : 05/12/2023 13:29:54
  Last failure timestamp          : 12/31/1969 16:00:00
  Last failure status             : idle
  Last JWT success timestamp      : 05/12/2023 13:27:35
  Last JWT failure timestamp      : 12/31/1969 16:00:00
  Last JWT failure reason         : Unknown
  Packet transmit attempts        : 53
  Packet transmit failures        : 0
  Packet receive count            : 1061
  Packet receive failures         : 0
Full packet-trace stats
  AP timestamp                    : 05/12/2023 13:29:54
  Packets received                : 0
  Packets sent                    : 0
  Packets filtered                : 0
  Packets dropped                 : 0
  Packets dropped while disabled : 0
  Packets dropped without JWT     : 0
```

```
Partial packet-trace stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 1061
  Packets sent                   : 262
  Packets filtered               : 799
  Packets dropped                : 0
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 0
Anomaly detection event stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 0
  Packets sent                   : 0
  Packets filtered               : 0
  Packets dropped                : 0
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 0
Anomaly detection packet stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 0
  Packets sent                   : 0
  Packets filtered               : 0
  Packets dropped                : 0
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 0
Statistics stats
  AP timestamp                   : 05/12/2023 13:29:54
  Packets received               : 0
  Packets sent                   : 15165
  Packets filtered               : 0
  Packets dropped                : 2
  Packets dropped while disabled : 0
  Packets dropped without JWT    : 2
```

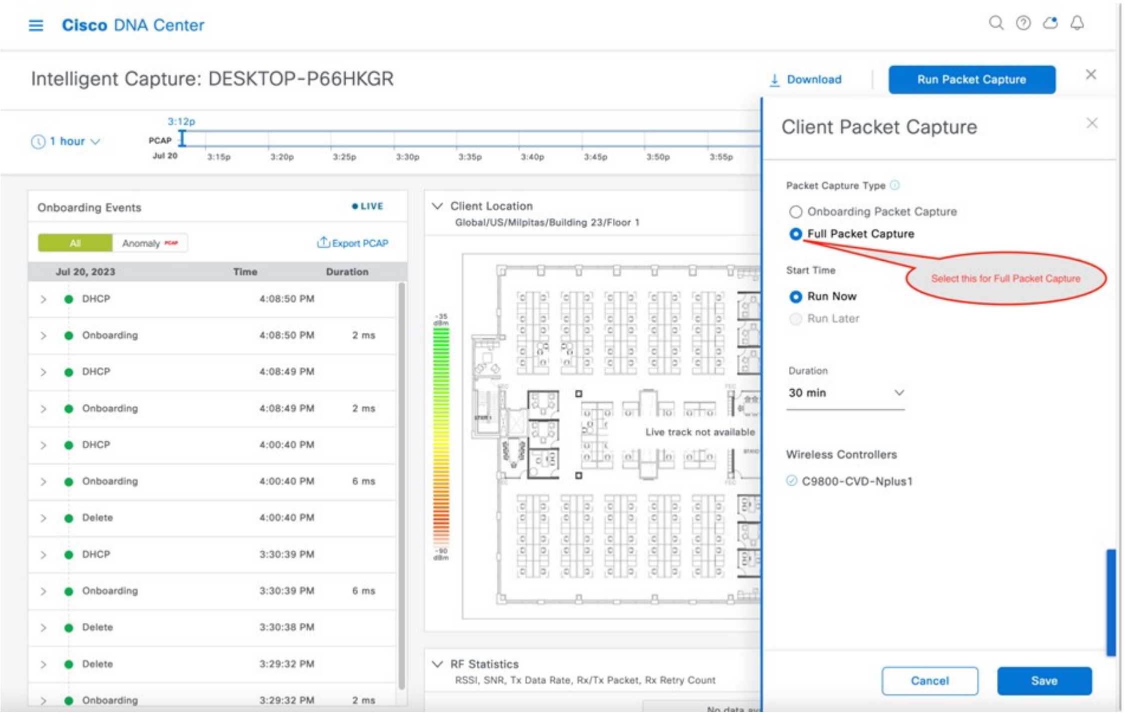
- **mil23-floor1-ap1#show ap icap subscription**

```
Subscription list
-----------------
 Full Pkt Capture      : Disabled
 Partial Pkt Capture   : Enabled
 Anomaly Event         : Disabled
 Debug                 : Disabled
 Stats                 : Enabled
 Ap Operational Data   : Disabled
       Sensor Message        : Disabled
 RRM Operational Data  : Disabled
 Client Events         : Disabled
 MMAP Packets          : Disabled
 aWIPS Forensic Pkts   : Disabled
MAC and Filters subscription list
---------------------------------
Full-packet-trace: None
Partial-packet-trace: 1C:1B:B5:1F:C0:F7
 Filters: assoc auth probe arp dhcp eap icmp dhcpv6 icmpv6 dns ndp
Anomaly Detection: None

Client Stats
------------
MAC Address Table:
  1C:1B:B5:1F:C0:F7

RF Spectrum
-----------
Radio Slot(s): NONE
mil23-floor1-ap1#
```

Once ICAP for onboarding events is enabled and the client is deauthenticated and reauthenticated, the packets are captured during those events and sent to Cisco DNA Center. The events with captured packets will have a PCAP icon to the right side of the event name in the onboarding events section. Once you select an event, it will show the analysis of the captured packets in a visual format. The captured packets can be downloaded as a PCAP file by clicking **Download Packets** in the top-right corner of the **Auto Packet Analyzer** section. The captured packets of a group of events can be downloaded by clicking **Export PCAP** in the **Onboarding Events** section. **Export PCAP** is intended for the full set of events, and **Download Packets** should be used for subevents.

In order to capture the data packets from clients, the full packet capture needs to be enabled as shown in the following figure.

Figure 193: Full Packet Capture Configuration



Intelligent Capture: DESKTOP-P66HKGR

Onboarding Events

Jul 20, 2023	Time	Duration
DHCP	4:08:50 PM	
Onboarding	4:08:50 PM	2 ms
DHCP	4:08:49 PM	
Onboarding	4:08:49 PM	2 ms
DHCP	4:00:40 PM	
Onboarding	4:00:40 PM	6 ms
Delete	4:00:40 PM	
DHCP	3:30:39 PM	
Onboarding	3:30:39 PM	6 ms
Delete	3:30:38 PM	
Delete	3:29:32 PM	
Onboarding	3:29:32 PM	2 ms

Client Location
Global/US/Milpitas/Building 23/Floor 1

RF Statistics
RSSI, SNR, Tx Data Rate, Rx/Tx Packet, Rx Retry Count

Client Packet Capture

Packet Capture Type
○ Onboarding Packet Capture
● Full Packet Capture

Select this for Full Packet Capture

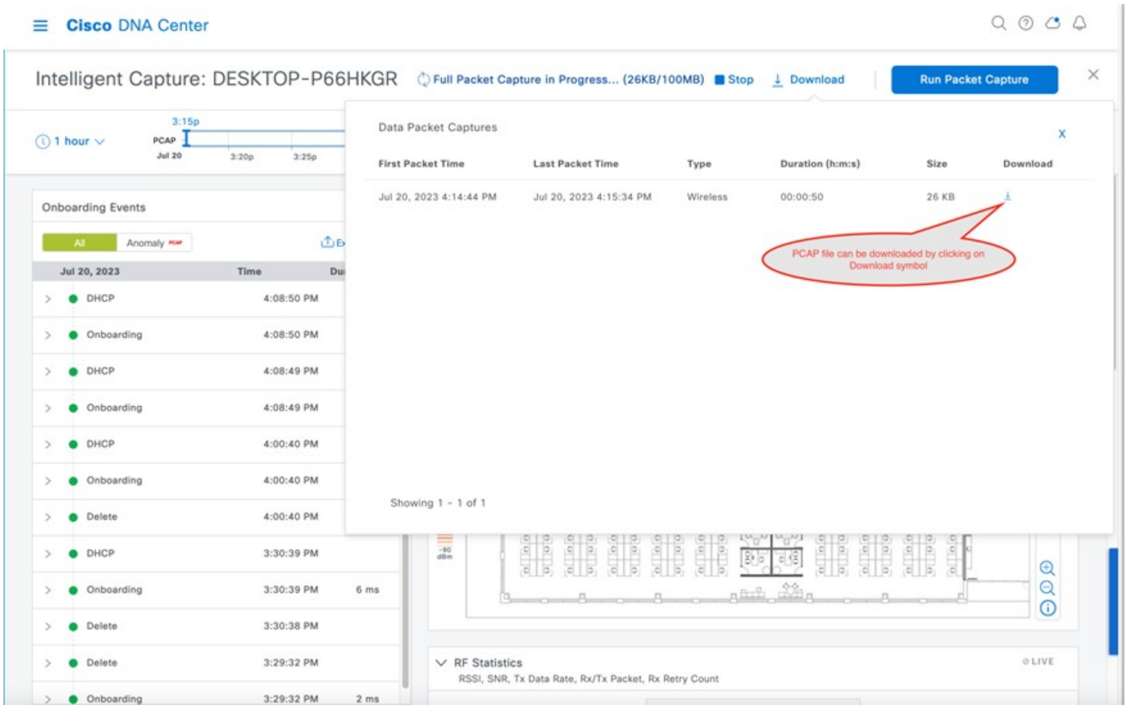
Start Time
● Run Now
○ Run Later

Duration
30 min

Wireless Controllers
C9800-CVD-Nplus1

Click **Save** to enable the full packet capture. Click the download icon to download the packets as a PCAP file, as shown in the following figure.

Figure 194: Downloading the Full Packet Capture



Intelligent Capture: DESKTOP-P66HKGR

Data Packet Captures

First Packet Time	Last Packet Time	Type	Duration (h:m:s)	Size	Download
Jul 20, 2023 4:14:44 PM	Jul 20, 2023 4:15:34 PM	Wireless	00:00:50	26 KB	⤓

PCAP file can be downloaded by clicking on Download symbol

Showing 1 - 1 of 1

Onboarding Events

Jul 20, 2023	Time	Du
DHCP	4:08:50 PM	
Onboarding	4:08:50 PM	
DHCP	4:08:49 PM	
Onboarding	4:08:49 PM	
DHCP	4:00:40 PM	
Onboarding	4:00:40 PM	
Delete	4:00:40 PM	
DHCP	3:30:39 PM	
Onboarding	3:30:39 PM	6 ms
Delete	3:30:38 PM	
Delete	3:29:32 PM	
Onboarding	3:29:32 PM	2 ms

RF Statistics

RSSI, SNR, Tx Data Rate, Rx/Tx Packet, Rx Retry Count

Rogue and Adaptive Wireless Intrusion Prevention

Rogue Management

The Rogue Management application in Cisco DNA Center detects and classifies threats and enables network administrators, network operators, and security operators to monitor network threats. Cisco DNA Center helps to quickly identify the highest-priority threats and allows you to monitor these threats in the **Rogue and aWIPS** dashboard within Cisco DNA Assurance.

A rogue device is an unknown AP or client that is detected by the managed APs in your network. A rogue AP can disrupt wireless LAN operations by hijacking legitimate clients. A hacker can use a rogue AP to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of clear-to-send (CTS) frames. This action mimics an AP informing a particular client to transmit, while instructing all the others to wait, which results in legitimate clients not being able to access network resources. As a result, wireless LAN service providers have a strong interest in banning rogue APs from the air space.

Cisco DNA Center constantly monitors all the nearby APs and automatically discovers and collects information about rogue APs.

When Cisco DNA Center receives a rogue event from a managed AP, it responds in the following ways:

- If the unknown AP is not managed by Cisco DNA Center, Cisco DNA Center applies the rogue classification rules.
- If the unknown AP is not using the same SSID as your network, Cisco DNA Center verifies whether the AP is connected to the corporate wired network and extends to the wired network. If the rogue AP is physically connected to the switch port of the corporate network, Cisco DNA Center classifies the AP as **Rogue on wire**.

  Cisco switches managed by Cisco DNA Center are required for rogue on wire to work.
- If the AP is unknown to Cisco DNA Center, and is using the same SSID as your network, Cisco DNA Center classifies the AP as a **Honeypot**.

- If the unknown AP is not using the same SSID as your network and is not connected to the corporate network, Cisco DNA Center verifies whether it is causing any interference. If it is, Cisco DNA Center classifies the AP as **Interferer** and marks the rogue state as **Potential Threat**. The threshold level for classifying the interferers on the network is greater than -75 dBm.
- If the unknown AP is not using the same SSID as your network, and is not connected to the corporate network, Cisco DNA Center verifies whether it is a neighbor. If it is a neighbor, Cisco DNA Center classifies the AP as **Neighbor** and marks the rogue state as **Informational**. The threshold level for classifying the rogue AP as a neighbor AP is less than or equal to -75 dBm.

Adaptive Wireless Intrusion Prevention

The Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is a wireless intrusion threat detection and mitigation mechanism. aWIPS uses an advanced approach to wireless threat detection and performance management. An AP detects threats and generates alarms. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver complete and highly accurate wireless threat prevention.

With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both wired and wireless networks and use that network intelligence to analyze attacks from many sources. You are able to accurately pinpoint attacks and proactively prevent attacks, rather than wait until damage or exposure has occurred.

Because the aWIPS functionality is integrated into Cisco DNA Center, aWIPS can configure and monitor aWIPS policies and alarms and report threats.

aWIPS supports the following capabilities:

- Static signatures
- Standalone signature detection
- Alarms
- Static signature file packaged with controller and AP image

Cisco DNA Center supports the following signatures that detect various denial of service (DoS) attacks:

- **Authentication flood**: A form of DoS attack that floods an AP's client-state table (association table) by imitating many client stations (MAC address spoofing) and sending authentication requests to the AP. Upon reception of each individual authentication request, the target AP creates a client entry in State 1 of the association table. If open system authentication is used for the AP, the AP returns an authentication success frame and moves the client to State 2. If Shared Key Authentication (SHA) is used for the AP, the AP sends an authentication challenge to the attacker's imitated client, which does not respond, and the AP keeps the client in State 1. In either of these scenarios, the AP contains multiple clients hanging in either State 1 or State 2, which fills up the AP association table. When the table reaches its limit, legitimate clients are not able to authenticate and associate with this AP.
- **Association flood**: A form of DoS attack that aims to exhaust an AP's resources, particularly the client association table, by flooding the AP with many spoofed client associations. An attacker using such a vulnerability can emulate many clients to flood a target AP's client association table by creating many clients. When the client association table overflows, legitimate clients cannot get associated.
- **CTS Flood**: A form of DoS attack when a specific device sends a bulk Clear To Send (CTS) control packet to wireless devices sharing the same radio frequency (RF) medium. This kind of attack blocks wireless devices from using the RF medium until the CTS flood stops.
- **RTS Flood**: A form of DoS attack when a specific device sends a bulk RTS control packet to an AP for blocking wireless bandwidth, which leads to performance disturbance for the clients on that AP.
- **Broadcast Probe**: A form of DoS attack when a specific device tries to flood a managed AP with broadcast probe requests.

- **Disassociation Flood**: A form of DoS attack that aims to send an AP to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the AP to a client. With client adapter implementations, this form of attack is effective in immediately disrupting wireless services against this client. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep the client out of service.
- **Disassociation Broadcast**: A form of DoS attack when a specific device triggers a disassociation broadcast to disconnect all the clients.

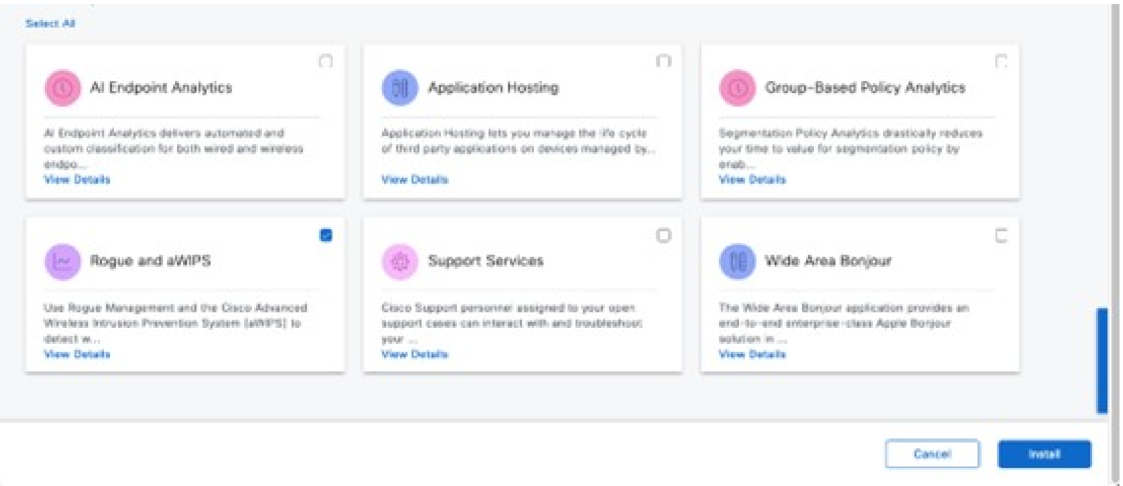
  This attack aims to send an AP's client to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the AP to the broadcast address of all the clients. With current client adapter implementations, this form of attack immediately disrupts wireless services against multiple clients. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep all the clients out of service.
- **Deauthentication flood**: A form of DoS attack that aims to send an AP's client to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the AP to the client unicast address. With the current client-adapter implementations, this form of attack immediately disrupts wireless services against the client. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame. An attacker repeatedly spoofs the deauthentication frames to keep all the clients out of service.
- **Deauthentication broadcast**: A form of DoS attack that sends all the clients of an AP to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the AP to the broadcast address. With client adapter implementation, this form of attack immediately disrupts wireless services against multiple clients. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame.
- **EAPOL logoff flood**: A form of DoS attack when a specific device tries to send Extensible Authentication Protocol over LAN (EAPOL) logoff packets, which are used in the WPA and WPA2 authentication for (DoS).

  Because the EAPOL logoff frame is not authenticated, an attacker can potentially spoof this frame and log out a user from an AP, thus committing a DoS attack. The fact that the client is logged out from the AP is not obvious until the client attempts communication through the WLAN. Typically, the disruption is discovered and the client reassociates and authenticates automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-logoff frames.

Basic Setup Workflow

To install the Rogue and aWIPS application in Cisco DNA Center, click the menu icon and choose **System** > **Software Management**. Choose the **Rogue and aWIPS** package, and click **Install** in the bottom-right corner, as shown in the figure below.

Figure 195: Installing Rogue and aWIPS Application



□ AI Endpoint Analytics

AI Endpoint Analytics delivers automated and custom classification for both wired and wireless endpo...

□ Application Hosting

Application Hosting lets you manage the life cycle of third party applications on devices managed by...

□ Group-Based Policy Analytics

Segmentation Policy Analytics drastically reduces your time to value for segmentation policy by enab...

☑ Rogue and aWIPS

Use Rogue Management and the Cisco Advanced Wireless Intrusion Prevention System (aWIPS) to detect w...

□ Support Services

Cisco Support personnel assigned to your open support cases can interact with and troubleshoot your ...

□ Wide Area Bonjour

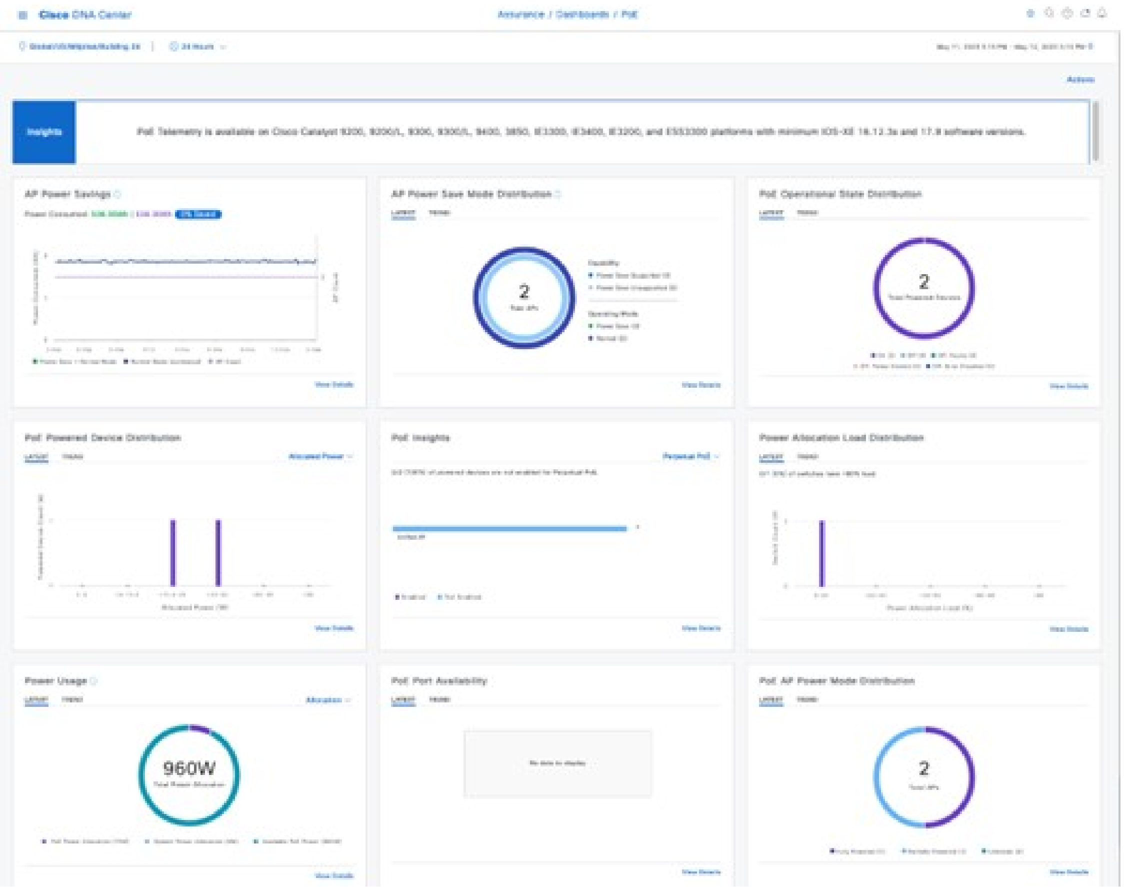
The Wide Area Bonjour application provides an end-to-end enterprise-class Apple Bonjour solution in ...

After installing the package, navigate to **Assurance** > **Rogue and aWIPS**.

For more information on how to configure Rogue and aWIPS in Cisco DNA Center, see the Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide.

POE Charts

Figure 196: PoE Charts in Cisco DNA Center


Cisco DNA Center
Assurance / Dashboards / PoE
Actions
Insights
AP Power Savings
AP Power Save Mode Distribution
2
PoE Operational State Distribution
2
PoE Powered Device Distribution
PoE Insights
Power Allocation Load Distribution
Power Usage
960W
PoE Port Availability
PoE AP Power Mode Distribution
2
View Details

PoE Telemetry is available on Cisco Catalyst 9200, 9200/L, 9300, 9300/L, 9400, 3850, IE3300, IE3400, IE3200, and ESS3300 platforms with minimum IOS-XE 16.12.3s and 17.9 software versions.

POE charts are available in the **AP 360** window, which provides a timeline view of the power consumed by the AP over the selected period of time.

Cisco Aironet 1800S Network Sensors

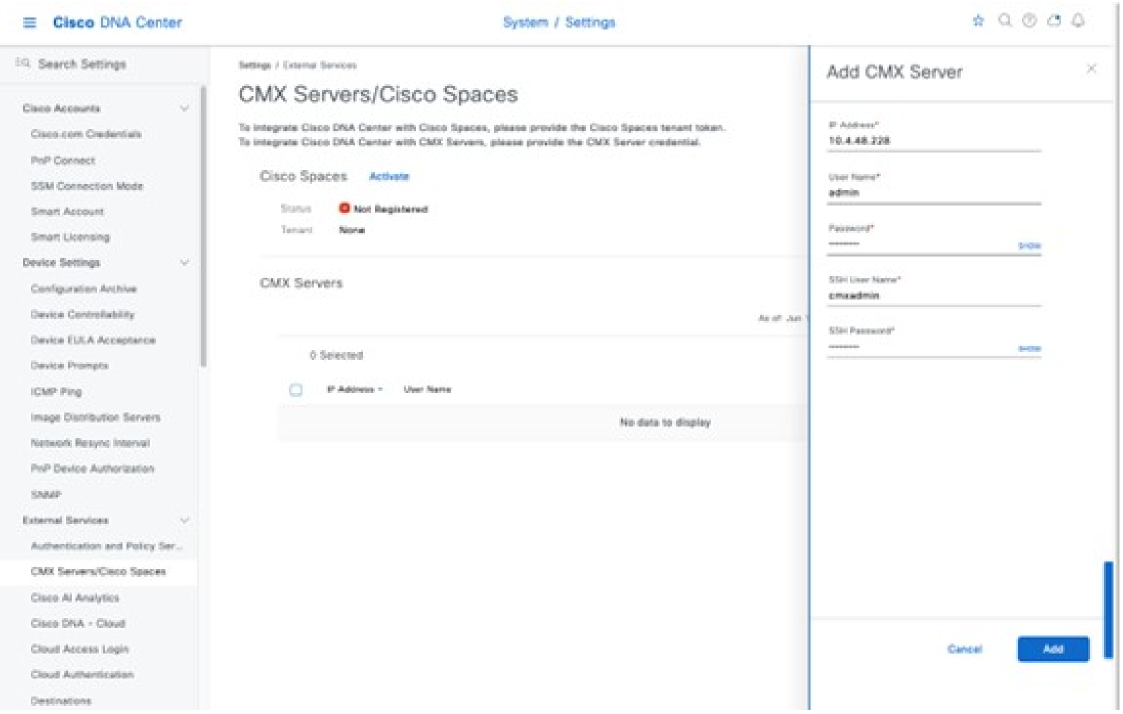
As wireless networks grow, it is imperative that wireless issues are identified proactively and resolved. Network sensors are small form factor devices that can be deployed in office spaces, such as conference rooms, work areas, where wireless coverage is critical and does not require an on-site IT technician. These sensors act as wireless clients, which can run on-demand or scheduled synthetic tests. For more information, see the Cisco Aironet Active Sensor Deployment Guide.

Cisco Spaces and CMX Integration

CMX On-premise Integration

To integrate the on-premise CMX, click the menu icon and choose **System** > **Settings** > **CMX Servers/Cisco Spaces**. Click **Add** under CMX Servers, and in the **Add CMX Server** slide-in pane, enter the requested values, as shown in figure below. After entering the values, click **Add**.

Figure 197: Integrate On-premise CMX into Cisco DNA Center



CMX Servers/Cisco Spaces

To integrate Cisco DNA Center with Cisco Spaces, please provide the Cisco Spaces tenant token.
To integrate Cisco DNA Center with CMX Servers, please provide the CMX Server credential.

Cisco Spaces

Status: Not Registered
Tenant: None

CMX Servers

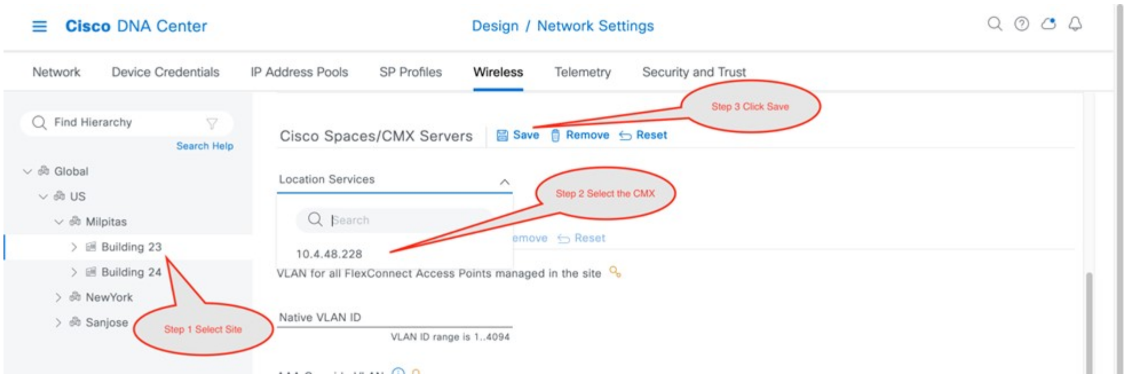
No data to display

Add CMX Server

IP Address*: 10.4.48.228
User Name*: admin
Password*: --------
SSH User Name*: cmxadmin
SSH Password*: --------

To assign CMX to a site, navigate to **Design** > **Network Settings**, and click the **Wireless** tab. Click the **Cisco Spaces/CMX Servers** tab, as shown in the following figure.

Figure 198: Assigning CMX to a Site

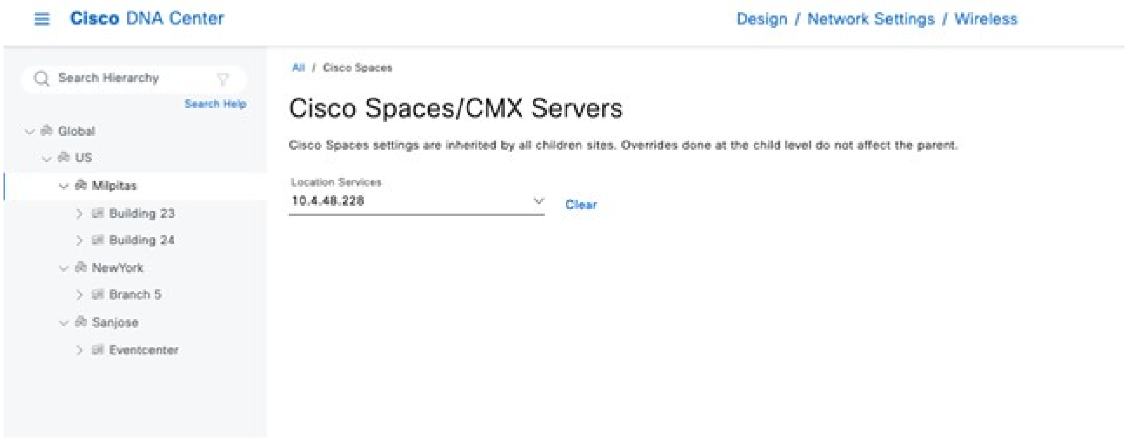


Location Services: 10.4.48.228

VLAN for all FlexConnect Access Points managed in the site

From the left hierarchy tree, select the desired site. From the **Location Services** drop-down list, choose the CMX server. The following figure shows an example CMX server for the selected Milpitas site.

Figure 199: CMX Site Assignment via Cisco DNA Center



Cisco Spaces/CMX Servers

Cisco Spaces settings are inherited by all children sites. Overrides done at the child level do not affect the parent.

Location Services: 10.4.48.228

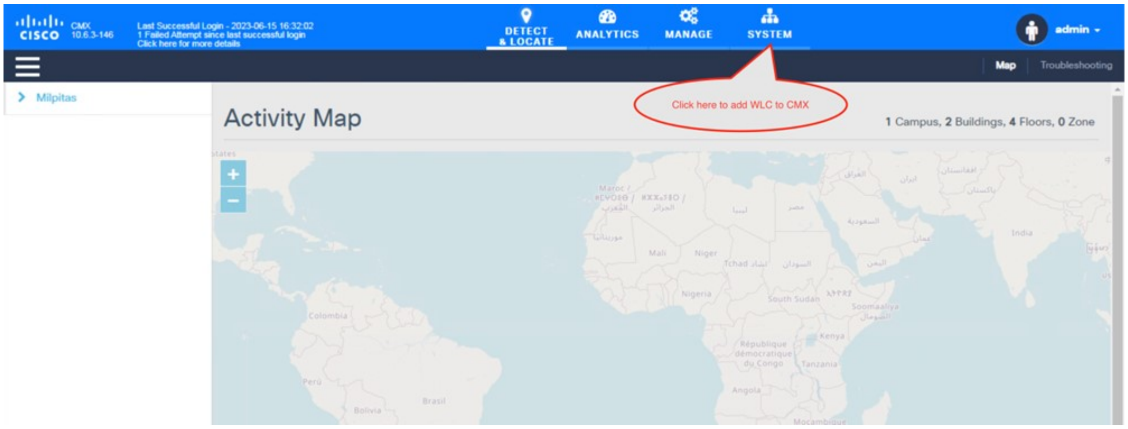
Once the location is assigned for the CMX, the site hierarchy related to that site, the APs in that site, and the AP position information will be synced with CMX.

Note Integrating CMX with Cisco DNA Center will not automatically add the wireless controller to the CMX. You must add the wireless controller manually on the CMX using the CMX GUI interface.

Use the following steps to add the wireless controller to the CMX.

1. Login to CMX GUI interface and navigate to **SYSTEM**, as shown in the following figure.

   Figure 200: CMX GUI to Add Wireless Controller

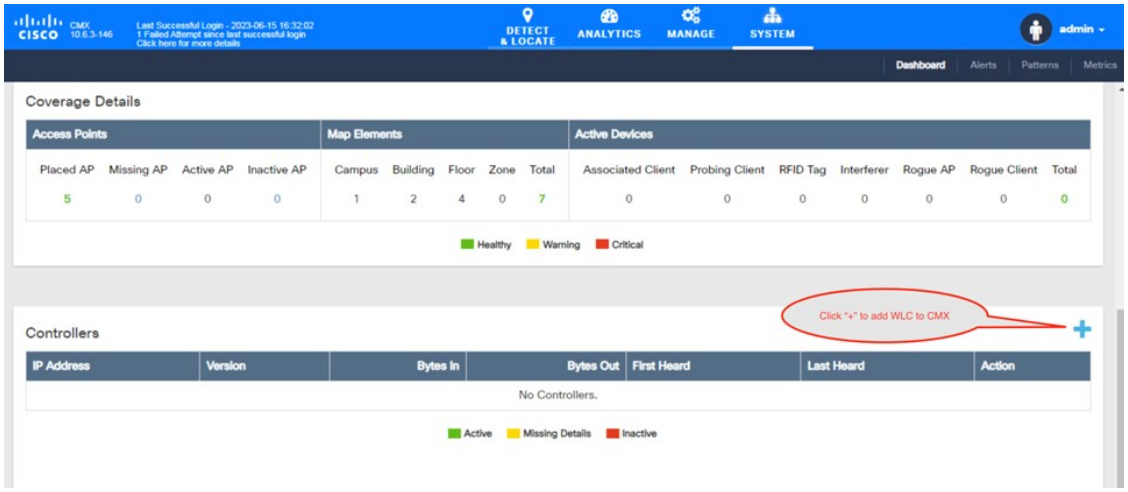
   

   Last Successful Login - 2023-06-15 16:32:02
   1 Failed Attempt since last successful login
   Click here for more details

   Click here to add WLC to CMX

2. Click + to add the wireless controller to the CMX.

Figure 201: Adding Wireless Controller within the SYSTEM in CMX



Last Successful Login - 2023-06-15 16:32:02
1 Failed Attempt since last successful login
Click here for more details

Coverage Details

Access Points				Map Elements					Active Devices						
Placed AP	Missing AP	Active AP	Inactive AP	Campus	Building	Floor	Zone	Total	Associated Client	Probing Client	RFID Tag	Interferer	Rogue AP	Rogue Client	Total
5	0	0	0	1	2	4	0	7	0	0	0	0	0	0	0

🟩 Healthy 🟨 Warning 🟥 Critical

Controllers

Click "+" to add WLC to CMX

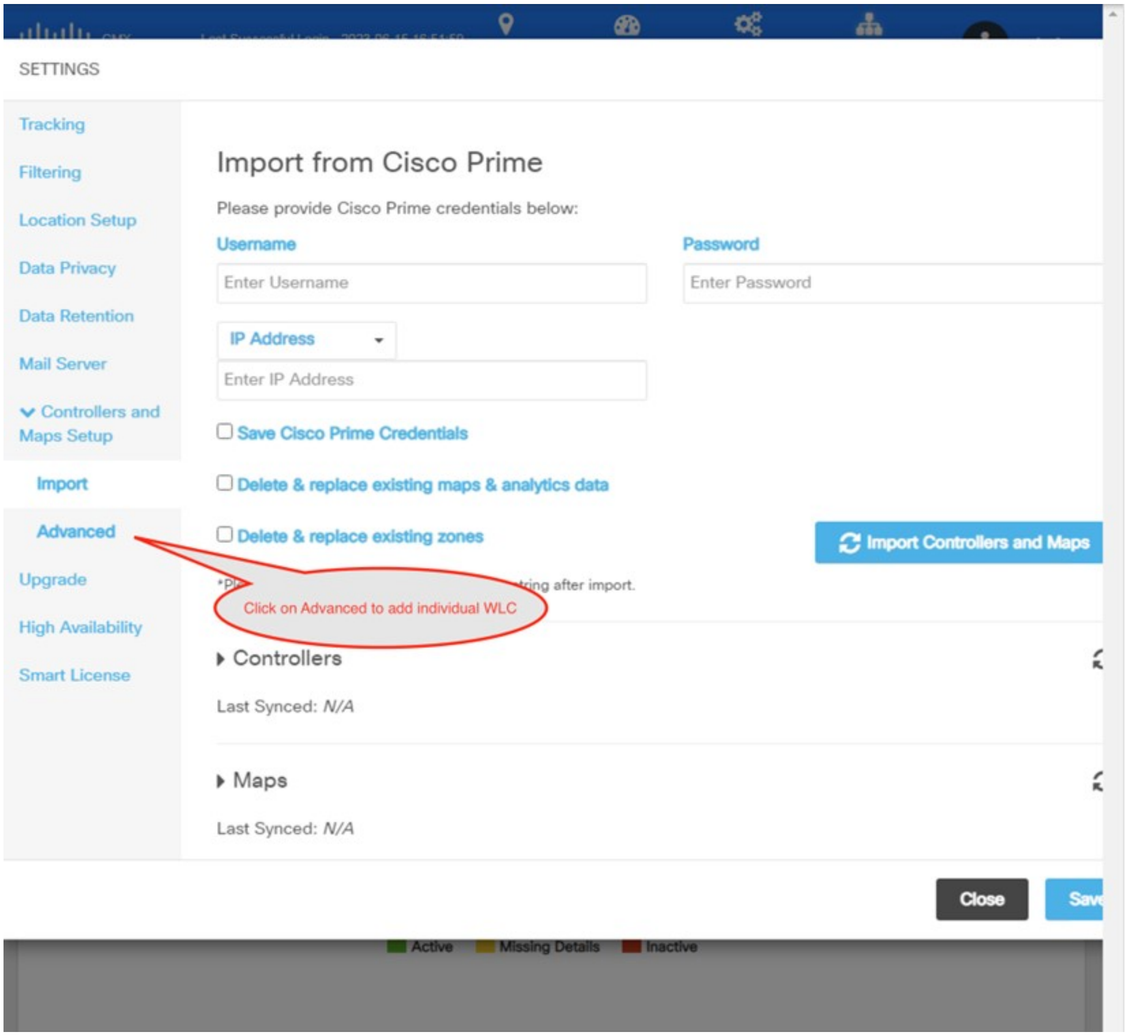
IP Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
No Controllers.						

🟩 Active 🟨 Missing Details 🟥 Inactive

3. From **Settings** > **Controllers and Map Setup**, click **Advanced** to add an individual wireless controller.

   The **Import from Cisco Prime** dialog box is displayed.

Figure 202: Add an Individual Wireless Controller to the CMX



SETTINGS

- Tracking
- Filtering
- Location Setup
- Data Privacy
- Data Retention
- Mail Server
- Controllers and Maps Setup
  - Import
  - Advanced
- Upgrade
- High Availability
- Smart License

Import from Cisco Prime

Please provide Cisco Prime credentials below:

Username: Enter Username

Password: Enter Password

IP Address: Enter IP Address

□ Save Cisco Prime Credentials

□ Delete & replace existing maps & analytics data

□ Delete & replace existing zones

Import Controllers and Maps

*Pl ring after import.

Click on Advanced to add individual WLC

Controllers

Last Synced: *N/A*

Maps

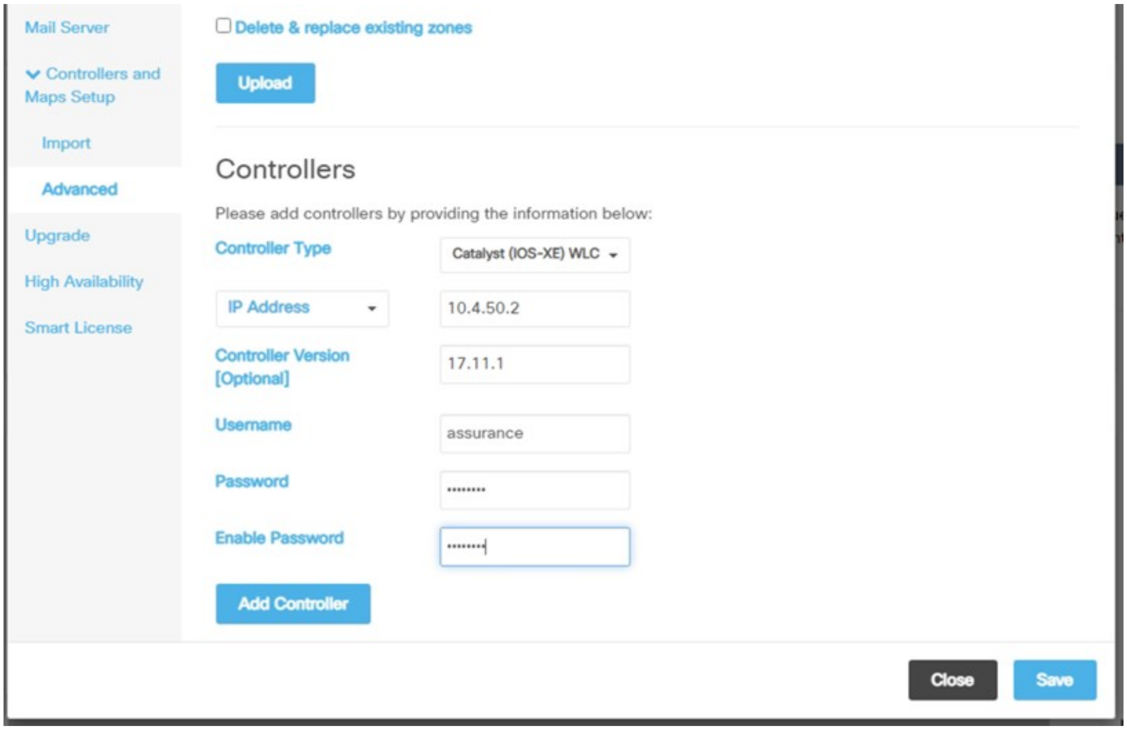
Last Synced: *N/A*

Close

Sav

4. Scroll down and click **Add Controller** to add the wireless controller to the CMX, as shown in the following figure.

Figure 203: Add Individual Wireless Controller Information



☐ Delete & replace existing zones

Controllers

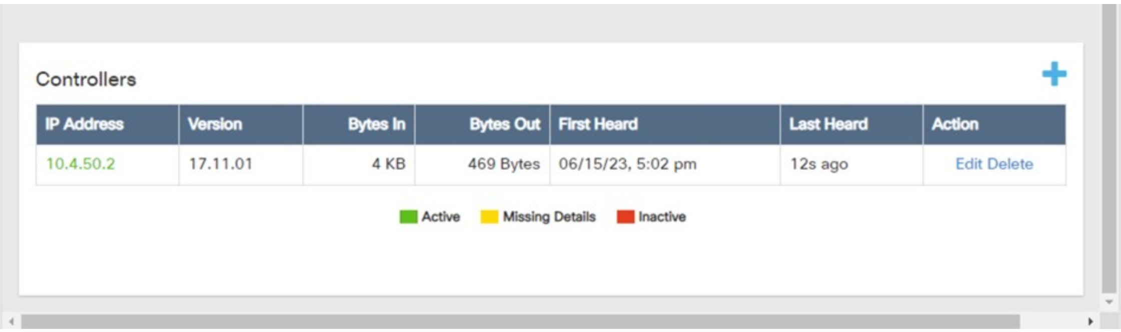
Please add controllers by providing the information below:

Controller Type	Catalyst (IOS-XE) WLC
IP Address	10.4.50.2
Controller Version [Optional]	17.11.1
Username	assurance
Password	••••••••
Enable Password	••••••••

5. Click **Save**.

   The list of wireless controllers is displayed.

Figure 204: List of Wireless Controllers



Controllers

IP Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
10.4.50.2	17.11.01	4 KB	469 Bytes	06/15/23, 5:02 pm	12s ago	Edit Delete

🟩 Active 🟨 Missing Details 🟥 Inactive

Integrate Cisco Spaces with Cisco DNA Center

Use this procedure to activate your Cisco Spaces account and integrate it with Cisco DNA Center. For more information, see the Cisco Spaces Configuration Guide.

Before you begin

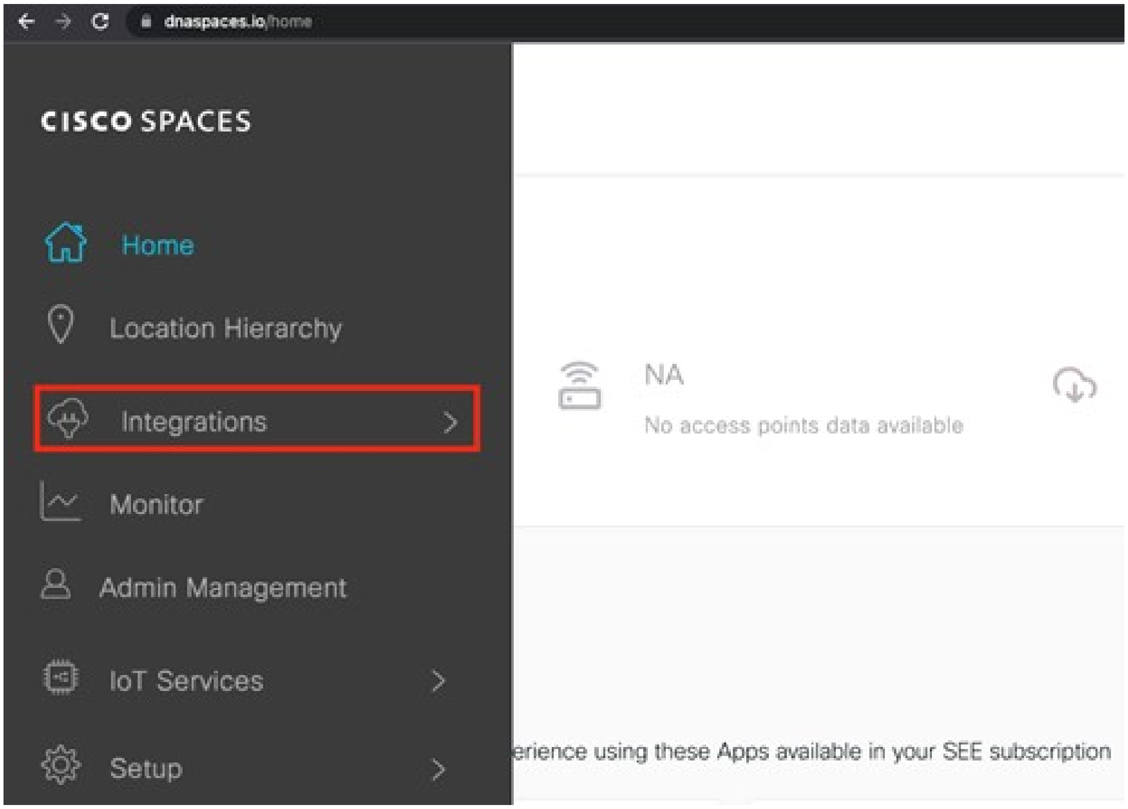
To integrate Cisco Spaces with Cisco DNA Center, you must have a Cisco Spaces account.

Procedure

Step 1 To activate your account in dnaspace.io, send an email to cisco-dnaspace-support@external.cisco.com. An activation link will be sent to the email address that you used to request the activation.

Step 2 Generate a token from dnaspaces.io for Cisco DNA Center integration and copy the token.

Figure 205: Token Generation for Cisco DNA Center Integration in dnaspaces.io



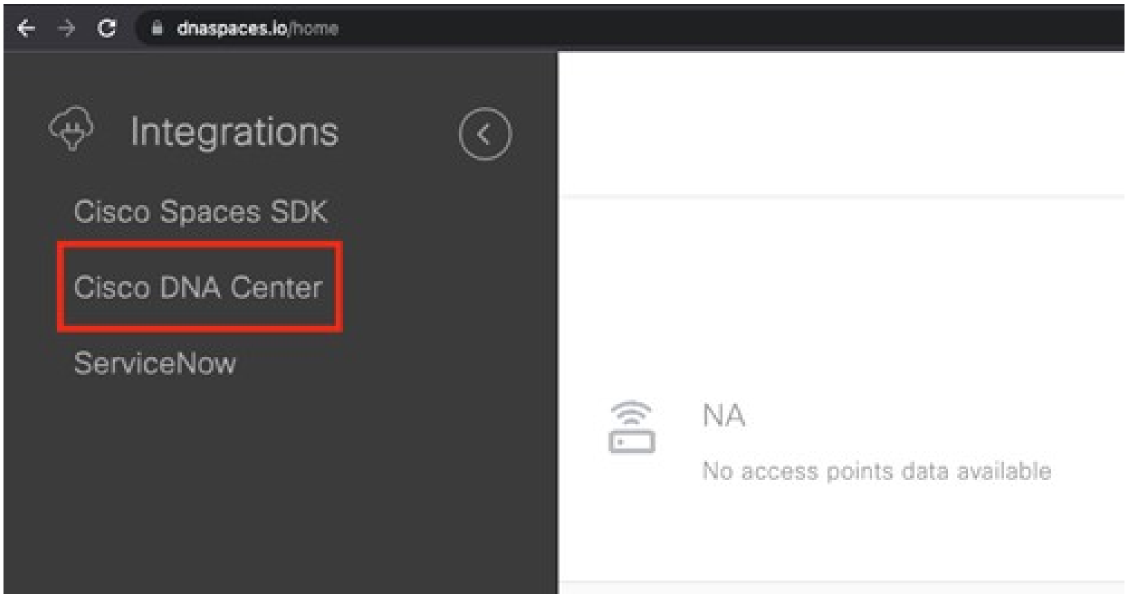
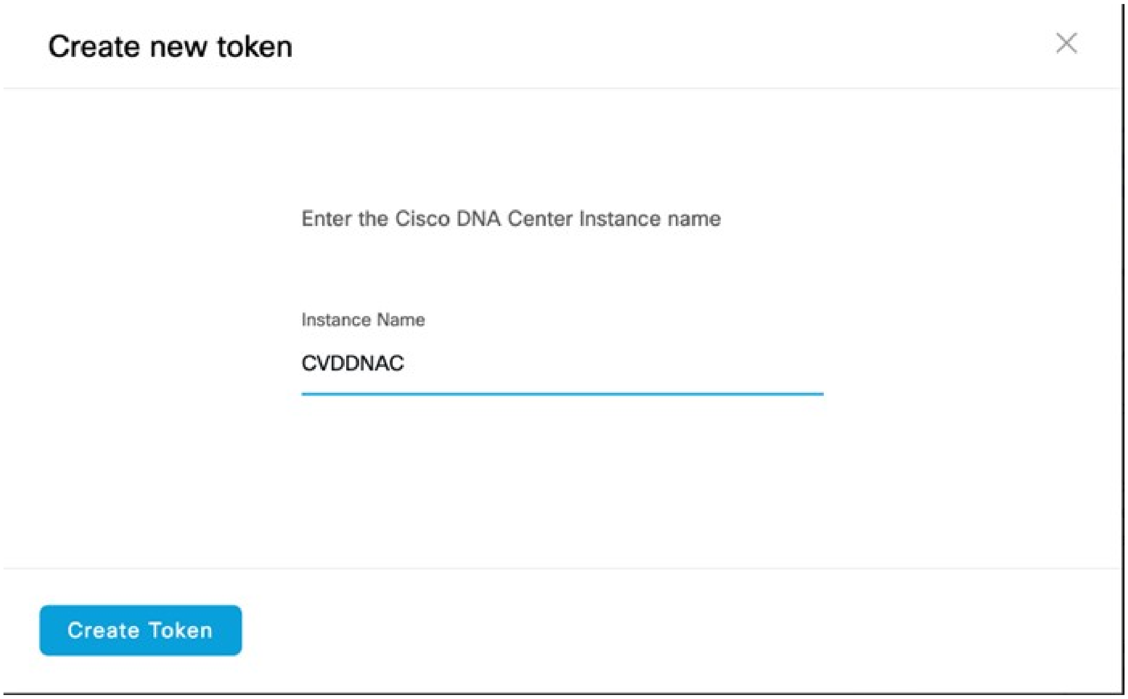


Figure 206: Create New Token



Enter the Cisco DNA Center Instance name

Instance Name: CVDDNAC

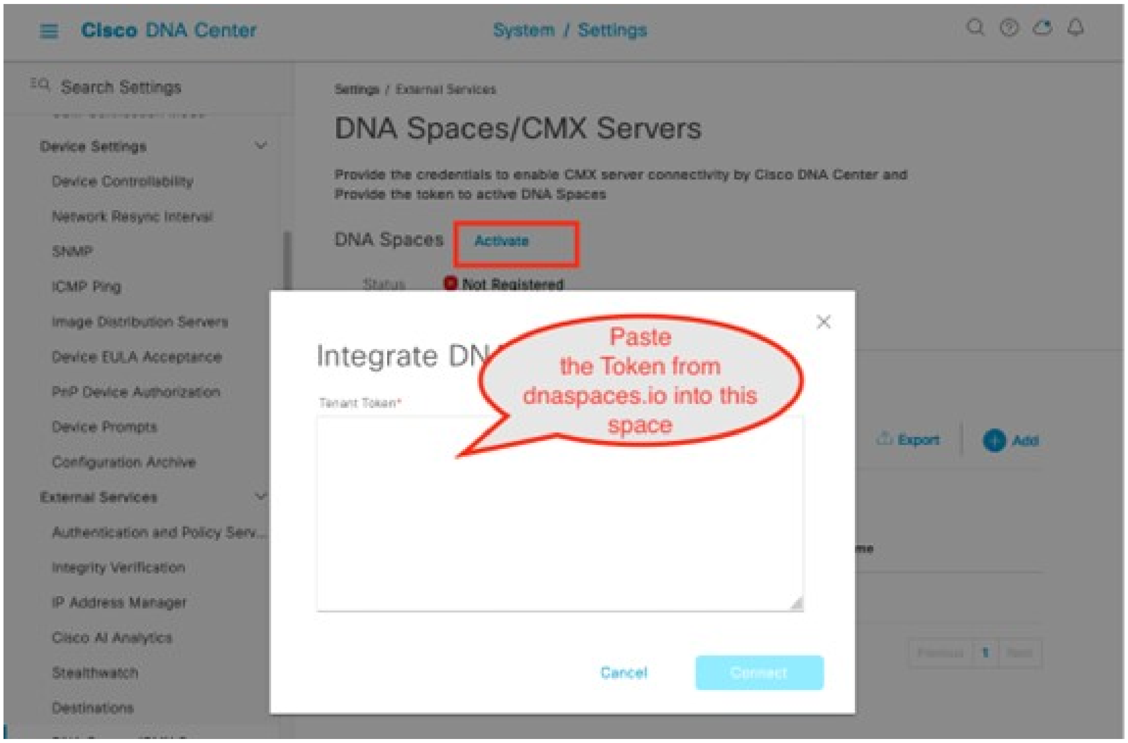
Step 3 Log in to the Cisco DNA Center UI.

Step 4 From the top-left corner, click the menu icon and choose **System** > **Settings** > **CMX Servers/Cisco Spaces**.

Step 5 Click **Activate** next to Cisco Spaces.

Step 6 In the dialog box, paste the token that was copied from dnaspaces.io.

Figure 207: Provide the Cisco Spaces Tenant Token



DNA Spaces/CMX Servers

Provide the credentials to enable CMX server connectivity by Cisco DNA Center and Provide the token to active DNA Spaces

DNA Spaces: Activate

Status: Not Registered

Integrate DN

Tenant Token*

Paste the Token from dnaspaces.io into this space

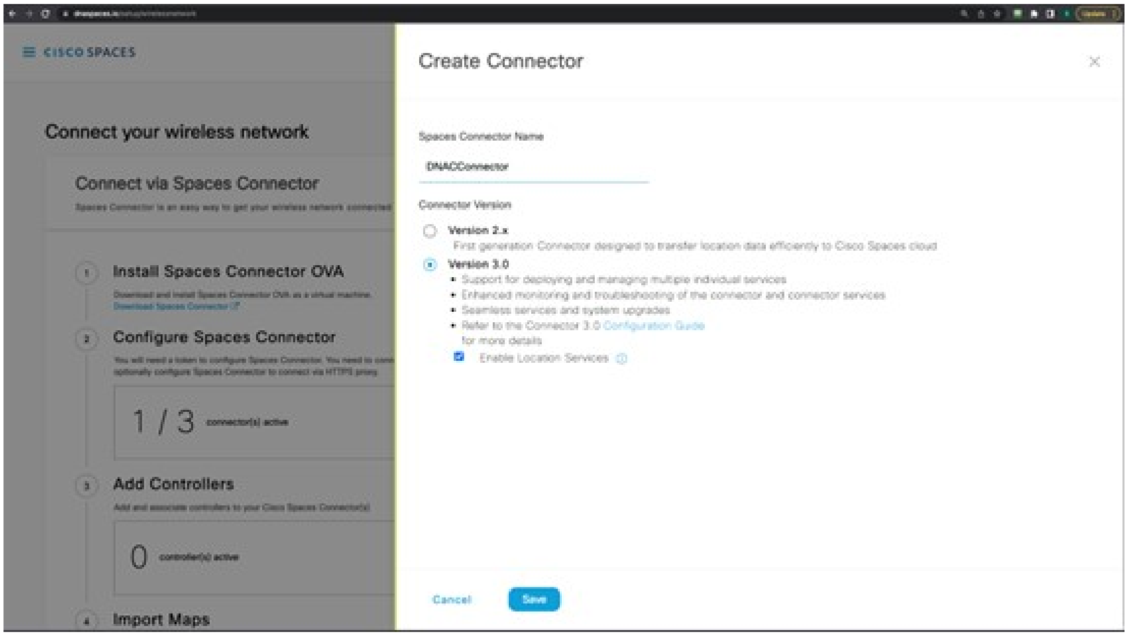
Step 7 If the wireless controller cannot reach dnaspaces.io, download a Cisco Spaces connector and deploy it on premises where it can reach both the wireless controller and dnaspaces.io. This process requires the dual interface version of the Cisco Spaces connector. For more information, see the "Retrieving a Token for a Connector from Cisco Spaces (Wireless)" topic in the Cisco Spaces: Connector Configuration Guide.

Primary interface information will be requested the first time the connector is powered on. The secondary interface values have to be entered via the CLI, as provided in the document. If the connector requires a proxy to reach dnaspaces.io, it has to be added via the connector UI interface.

Step 8 Log in to dnaspaces.io and click the menu icon and choose **Setup** > **Wireless Networks** > **Connect via Spaces**.

Step 9 Click **Create Connector** and enter a name for the connector.

Figure 208: Create Connector



CISCO SPACES
Connect your wireless network
Connect via Spaces Connector
Spaces Connector is an easy way to get your wireless network connected
1 Install Spaces Connector OVA
Download and install Spaces Connector OVA as a virtual machine.
Download Spaces Connector
2 Configure Spaces Connector
You will need a token to configure Spaces Connector. You need to conn
optionally configure Spaces Connector to connect via HTTPS proxy
1 / 3 connector(s) active
3 Add Controllers
Add and associate controllers to your Cisco Spaces Connector(s)
0 controller(s) active
4 Import Maps

Create Connector

Spaces Connector Name: DNACConnector

Connector Version

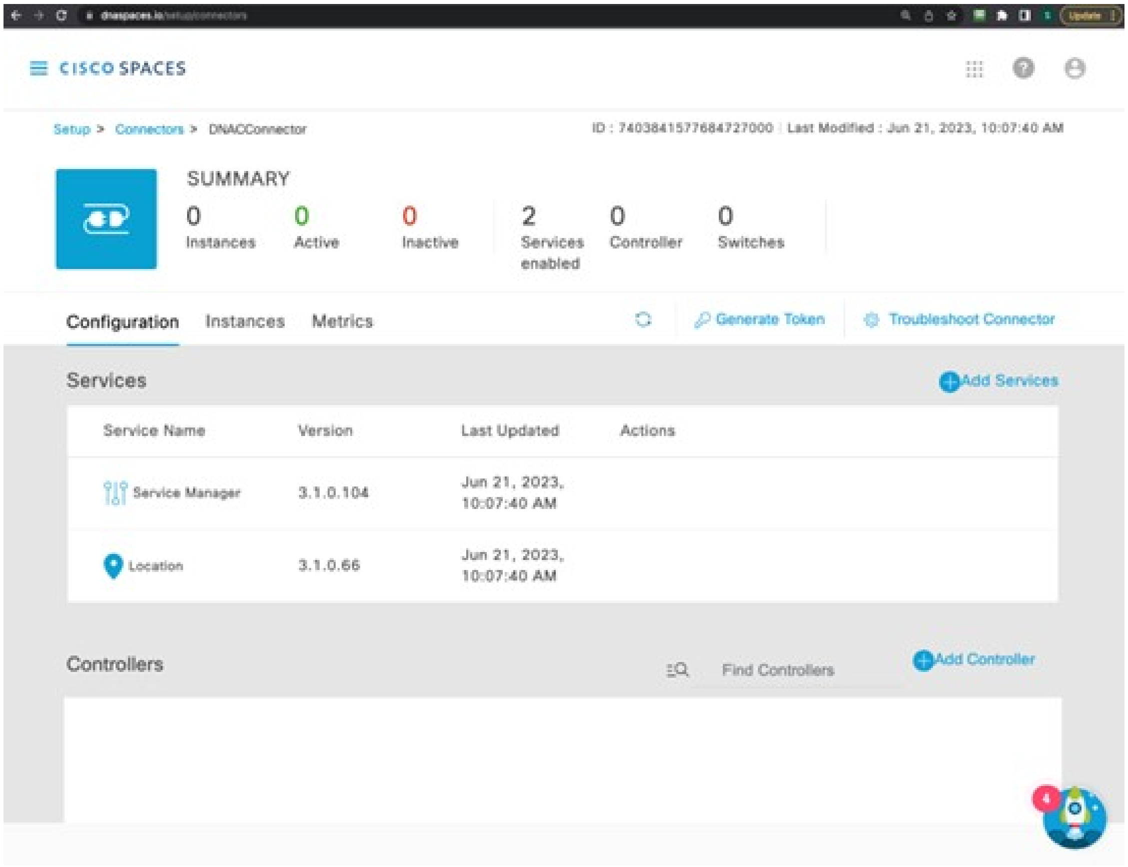
○ **Version 2.x**
First generation Connector designed to transfer location data efficiently to Cisco Spaces cloud

● **Version 3.0**
- Support for deploying and managing multiple individual services
- Enhanced monitoring and troubleshooting of the connector and connector services
- Seamless services and system upgrades
- Refer to the Connector 3.0 Configuration Guide for more details

☑ Enable Location Services

Step 10 Choose the connector that was recently created and click **Generate Token**.

Figure 209: Summary Window


dnaspaces.io/setup/connectors
CISCO SPACES
Setup > Connectors > DNACConnector

ID : 7403841577684727000 | Last Modified : Jun 21, 2023, 10:07:40 AM

SUMMARY

0	0	0	2	0	0
Instances	Active	Inactive	Services enabled	Controller	Switches

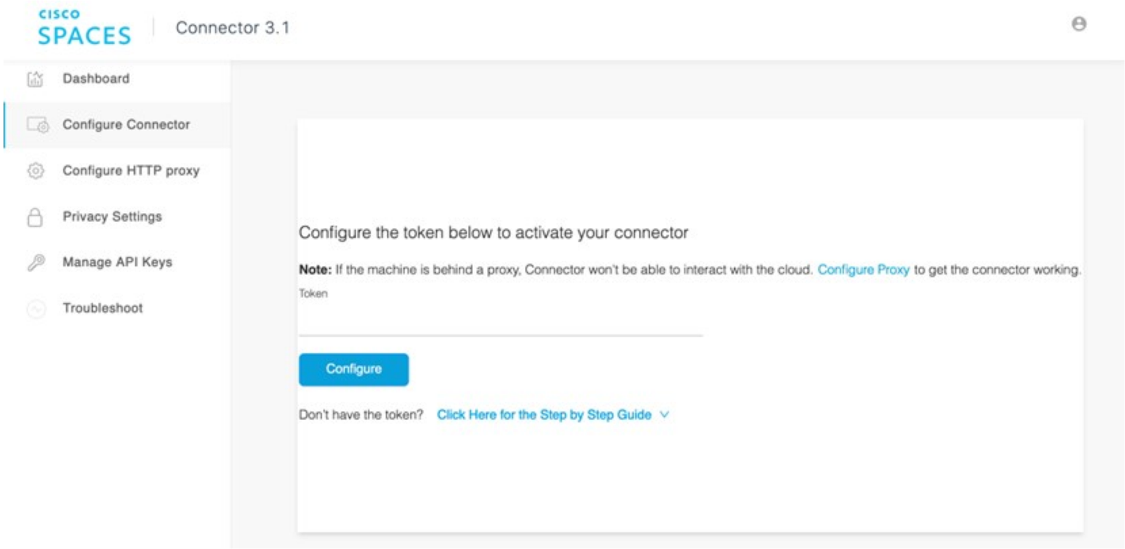
Services

Service Name	Version	Last Updated	Actions
Service Manager	3.1.0.104	Jun 21, 2023, 10:07:40 AM	
Location	3.1.0.66	Jun 21, 2023, 10:07:40 AM	

Controllers

Step 11 Log in to the Cisco Spaces connector GUI and enter the token to register this deployed connector with dnaspaces.io.

Figure 210: Activate Connector



Configure the token below to activate your connector

Note: If the machine is behind a proxy, Connector won't be able to interact with the cloud. Configure Proxy to get the connector working.

Token

Don't have the token? Click Here for the Step by Step Guide

Step 12 After the connector is registered with dnaspaces.io successfully, the wireless controller can be added from the connector instance in dnaspace.io.

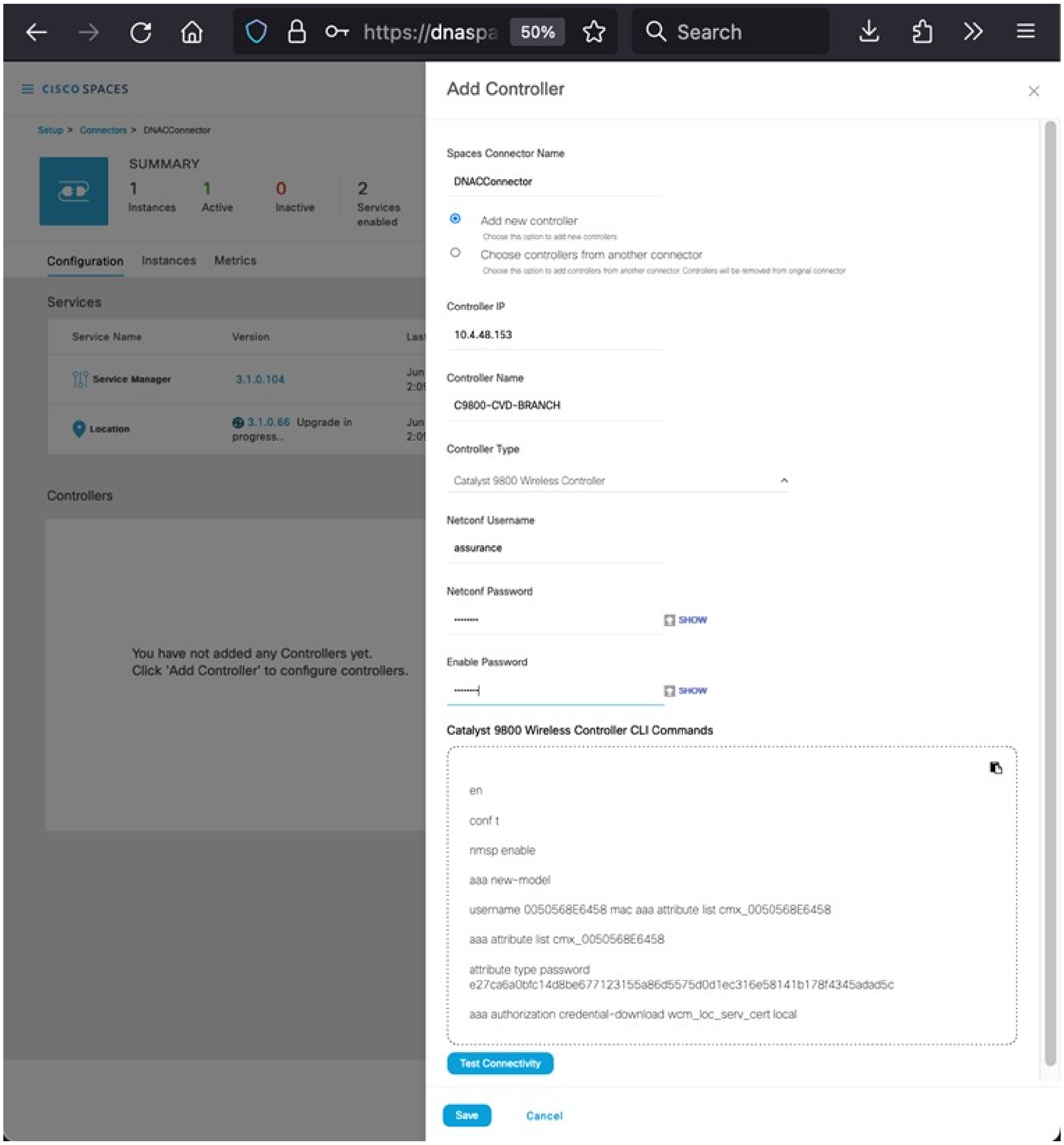
Step 13 Log in to dnaspaces.io and click the menu icon and choose **Setup** > **Wireless Networks** > **View Connectors**.

Step 14 Click **Add Controller**.

Step 15 Choose **Catalyst 9800 Wireless Controller** for the **Controller Type**.

Step 16 Enter the username and password and click **Save**.

Figure 211: Add Connector



Service Name	Version	Las
Service Manager	3.1.0.104	Jun 2:0
Location	3.1.0.66 Upgrade in progress..	Jun 2:0

You have not added any Controllers yet.
Click 'Add Controller' to configure controllers.

Spaces Connector Name: DNACConnector

● Add new controller
Choose this option to add new controllers

○ Choose controllers from another connector
Choose this option to add controllers from another connector. Controllers will be removed from original connector

Controller IP: 10.4.48.153

Controller Name: C9800-CVD-BRANCH

Controller Type: Catalyst 9800 Wireless Controller

Netconf Username: assurance

Netconf Password: ········

Enable Password: ········

Catalyst 9800 Wireless Controller CLI Commands

```
en

conf t

nmsp enable

aaa new-model

username 0050568E6458 mac aaa attribute list cmx_0050568E6458

aaa attribute list cmx_0050568E6458

attribute type password
e27ca6a0bfc14d8be677123155a86d5575d0d1ec316e58141b178f4345adad5c

aaa authorization credential-download wcm_loc_serv_cert local
```

Step 17 Wait several minutes for the wireless controller to show as **Active** in dnaspace.io.

Step 18 Navigate to the Cisco DNA Center UI.

Step 19 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 20 Click **Cisco Spaces/CMX Servers**.

Step 21 Choose your account from the **Location Services** drop-down list.

Step 22 From the left hierarchy tree, expand **Global** and choose the site that will use Cisco Spaces to track the client location.

Step 23 Click **Save**.

> **Note** After making changes on the sites assigned to Cisco Spaces, a resync may be required. To perform the resync, click the menu icon and choose **Design** > **Network Settings** > **Wireless**. Click the three dots for the site or floor and choose **Sync CMX Server/Cisco Spaces**.

Integrate On-Premise Cisco CMX with Cisco DNA Center

Use this procedure to integrate the on-premise Cisco Connected Mobile Experiences (CMX) with Cisco DNA Center.

Procedure

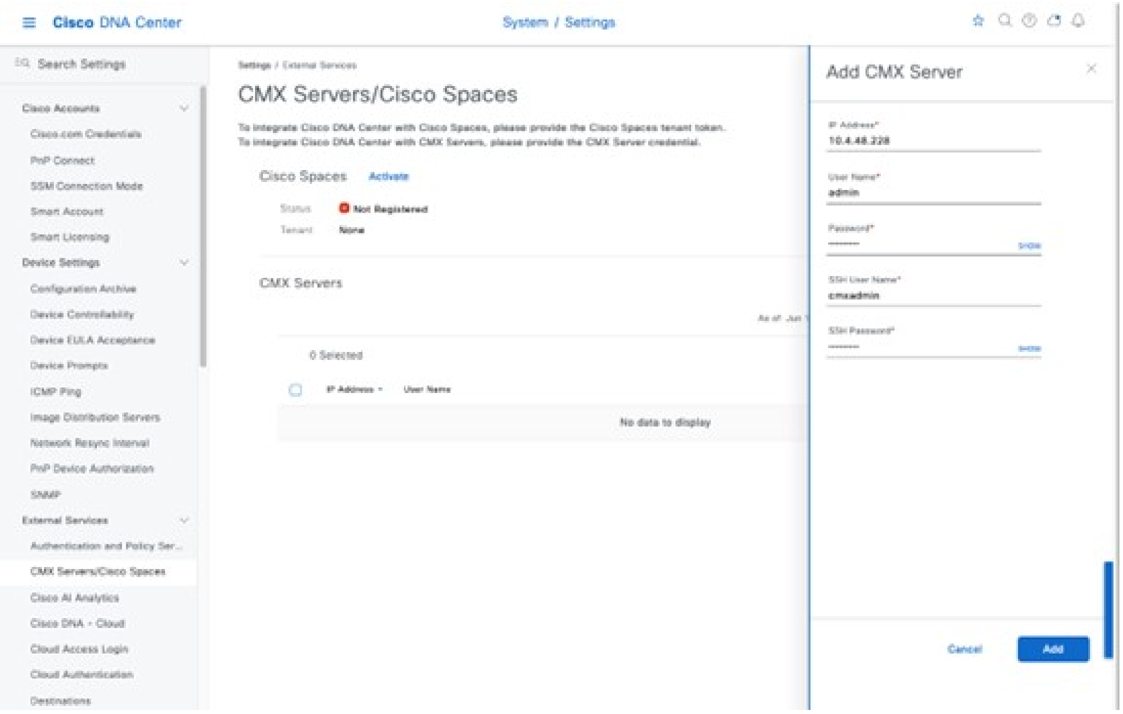
Step 1 From the top-left corner, click the menu icon and choose **System** > **Settings** > **CMX Servers/Cisco Spaces**.

Step 2 From **CMX Servers**, click **Add**.

The **Add CMX Server** slide-in pane is displayed.

Step 3 Enter the requested information into the relevant fields.

Figure 212: Integrate On-Premise CMX with Cisco DNA Center



To integrate Cisco DNA Center with Cisco Spaces, please provide the Cisco Spaces tenant token.
To integrate Cisco DNA Center with CMX Servers, please provide the CMX Server credential.

Status: Not Registered
Tenant: None

No data to display

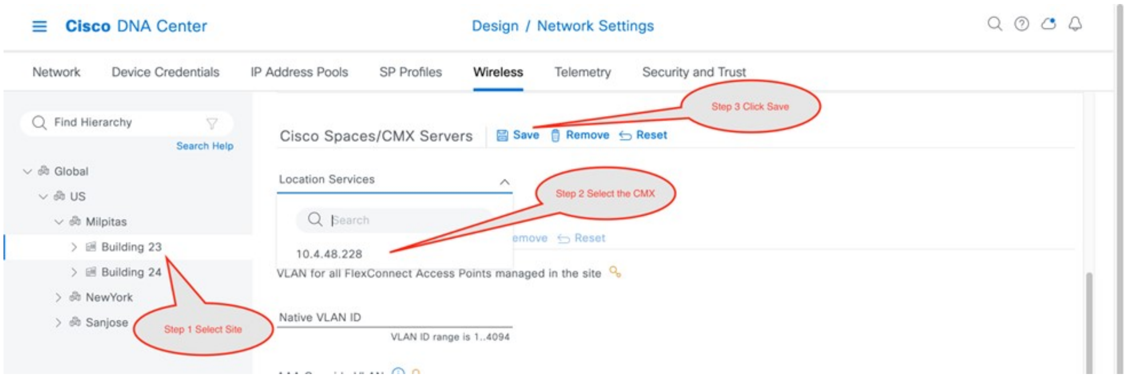
IP Address*: 10.4.48.228
User Name*: admin
Password*: ---------
SSH User Name*: cmxadmin
SSH Password*: ---------

Step 4 Click **Add**.

Step 5 To assign CMX to a site(s), click the menu icon and choose **Design** > **Network Settings** > **Wireless**.

Step 6 Click **Cisco Spaces/CMX Servers**.

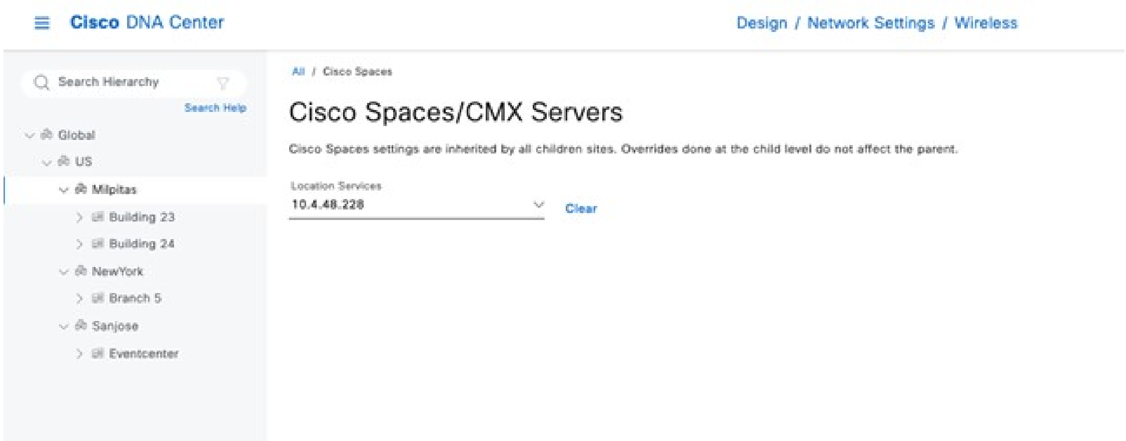
Figure 213: Assigning CMX to Site(s)



Step 7 From the **Location Services** drop-down list, select the CMX server.

The following figure shows an example CMX server 10.4.48.228 for the Milpitas site.

Figure 214: CMX Site Assignment via Cisco DNA Center



Cisco Spaces settings are inherited by all children sites. Overrides done at the child level do not affect the parent.

Location Services: 10.4.48.228

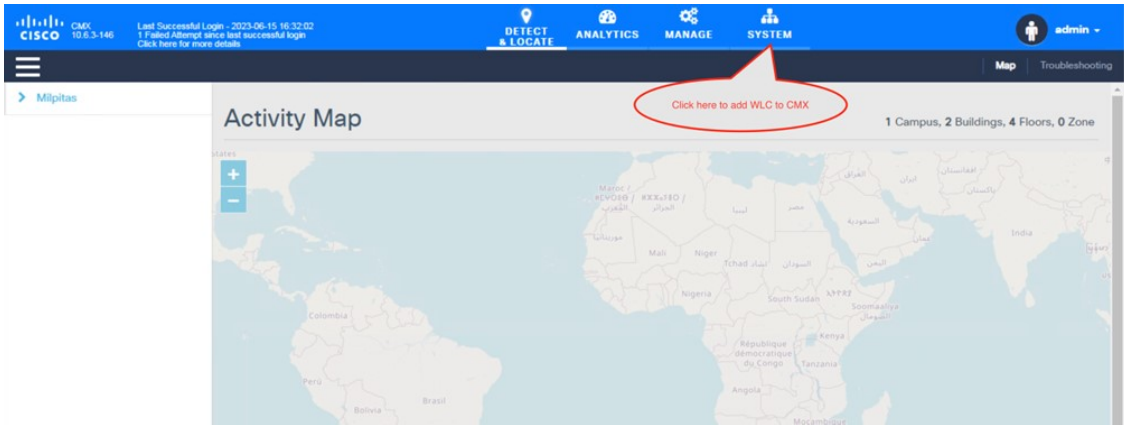
Once the location is assigned for the CMX server, the site hierarchy related to that site, the APs in that site, and the AP position information will be synced with the CMX server.

Note

Integrating the CMX with Cisco DNA Center will not automatically add the wireless controller to the CMX server. To manually add the wireless controller to the CMX using the CMX GUI interface, perform the following steps:

a. Log in to the CMX GUI interface and navigate to **SYSTEM**.

Figure 215: CMX GUI to Add Wireless Controller



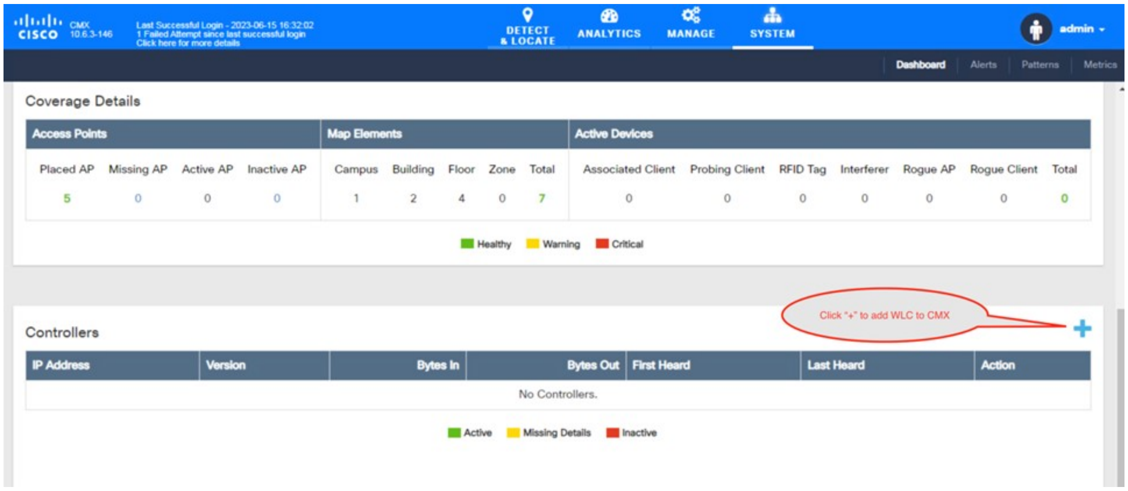
Last Successful Login - 2023-06-15 16:32:02
1 Failed Attempt since last successful login
Click here for more details

Click here to add WLC to CMX

1 Campus, 2 Buildings, 4 Floors, 0 Zone

b. Click **+** to add the wireless controller to the CMX.

Figure 216: Add the Wireless Controller to the CMX



Last Successful Login - 2023-06-15 16:32:02
1 Failed Attempt since last successful login
Click here for more details

Coverage Details

Access Points				Map Elements					Active Devices						
Placed AP	Missing AP	Active AP	Inactive AP	Campus	Building	Floor	Zone	Total	Associated Client	Probing Client	RFID Tag	Interferer	Rogue AP	Rogue Client	Total
5	0	0	0	1	2	4	0	7	0	0	0	0	0	0	0

🟩 Healthy 🟨 Warning 🟥 Critical

Click "+" to add WLC to CMX

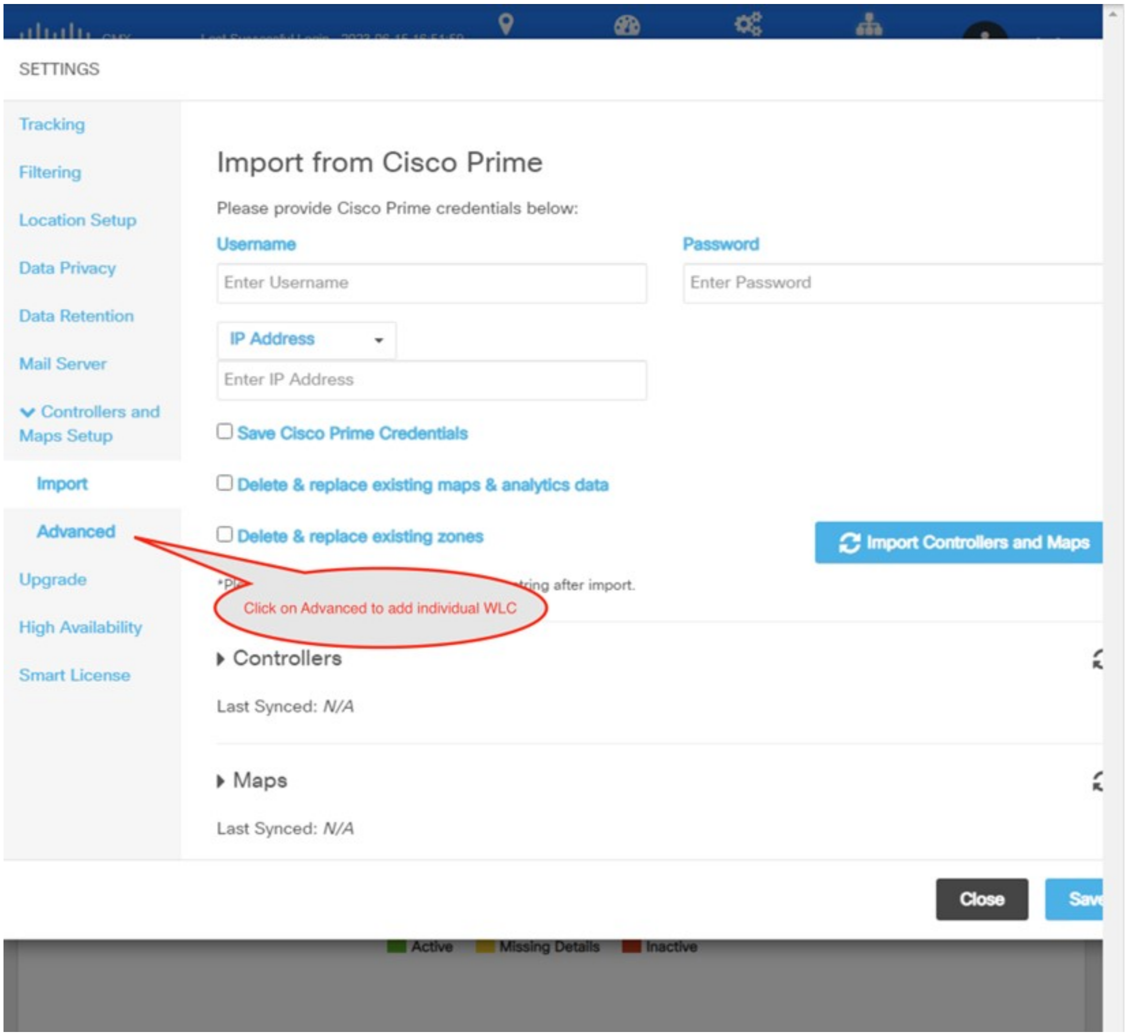
Controllers

IP Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
No Controllers.						

🟩 Active 🟨 Missing Details 🟥 Inactive

c. From **Controllers and Maps Setup**, click **Advanced**.

Figure 217: Controllers and Maps Setup: Advanced



Import from Cisco Prime

Please provide Cisco Prime credentials below:

Username: Enter Username

Password: Enter Password

IP Address ▾

Enter IP Address

□ Save Cisco Prime Credentials

□ Delete & replace existing maps & analytics data

□ Delete & replace existing zones

*Pl … tring after import.

Click on Advanced to add individual WLC

Controllers

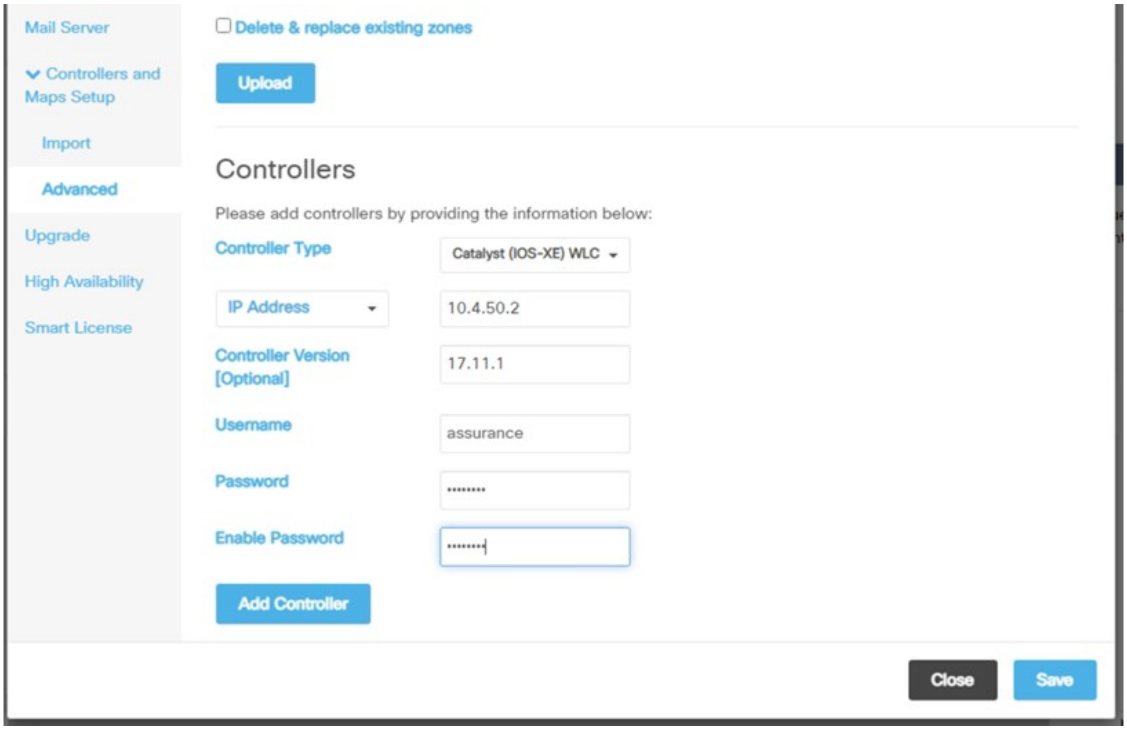
Last Synced: *N/A*

Maps

Last Synced: *N/A*

d. From **Controllers**, click **Add Controller** to add the wireless controller to the CMX, as shown in the following figure.

Figure 218: Individual Wireless Controller Information



□ Delete & replace existing zones

Controllers

Please add controllers by providing the information below:

Controller Type: Catalyst (IOS-XE) WLC

IP Address: 10.4.50.2

Controller Version [Optional]: 17.11.1

Username: assurance

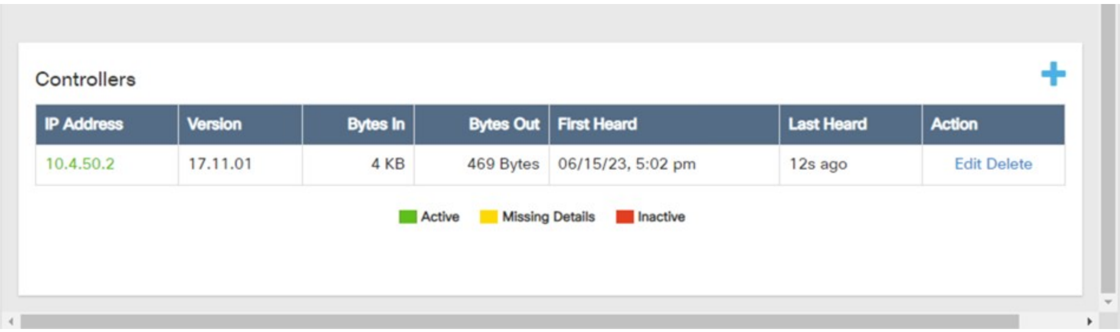
Password: ••••••••

Enable Password: ••••••••

e. Click **Save**.

The list of wireless controllers is displayed.

Figure 219: List of Wireless Controllers



Controllers

IP Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
10.4.50.2	17.11.01	4 KB	469 Bytes	06/15/23, 5:02 pm	12s ago	Edit Delete

🟩 Active 🟨 Missing Details 🟥 Inactive

Hardware Upgrade, Refresh, and Replacement

Replace Cisco Wireless Controller

Cisco DNA Center does not support a workflow to replace the wireless controller, but the replacement needs to be directly performed on the wireless controller. If one of the boxes in a SSO pair fails and must be replaced, Cisco recommends that you follow this procedure to put the device back in the cluster while avoiding any disruptions to the wireless network.

Procedure

Step 1 Physically disconnect the failed box and send the box in for Return Material Authorization (RMA).

Step 2 Make sure that the active wireless controller is configured with a higher chassis priority (= 2).

Step 3 When you receive the new box, before you connect it to the network and to the existing Cisco Catalyst 9800 Series Wireless Controller, configure the basic parameters offline: login credentials, IP connectivity, and redundancy configuration, including RMI (if applicable). Remember to set the chassis priority to 1, so when SSO pair is formed, this box will become the standby and will not disrupt the existing active wireless controller.

Step 4 Save the configuration on the new box and power it off.

Step 5 Physically connect the new Cisco Catalyst 9800 Series Wireless Controller to the network (uplink and RP ports).

Step 6 Power on the new box.

Step 7 The box will boot up, and the SSO pair will be formed again, with the new box going to standby hot state.

Replace an AP

Use the following procedure to replace the AP hardware. Cisco DNA Center provides an AP hardware replacement guided workflow for reasons such as hardware failure.

Before you begin

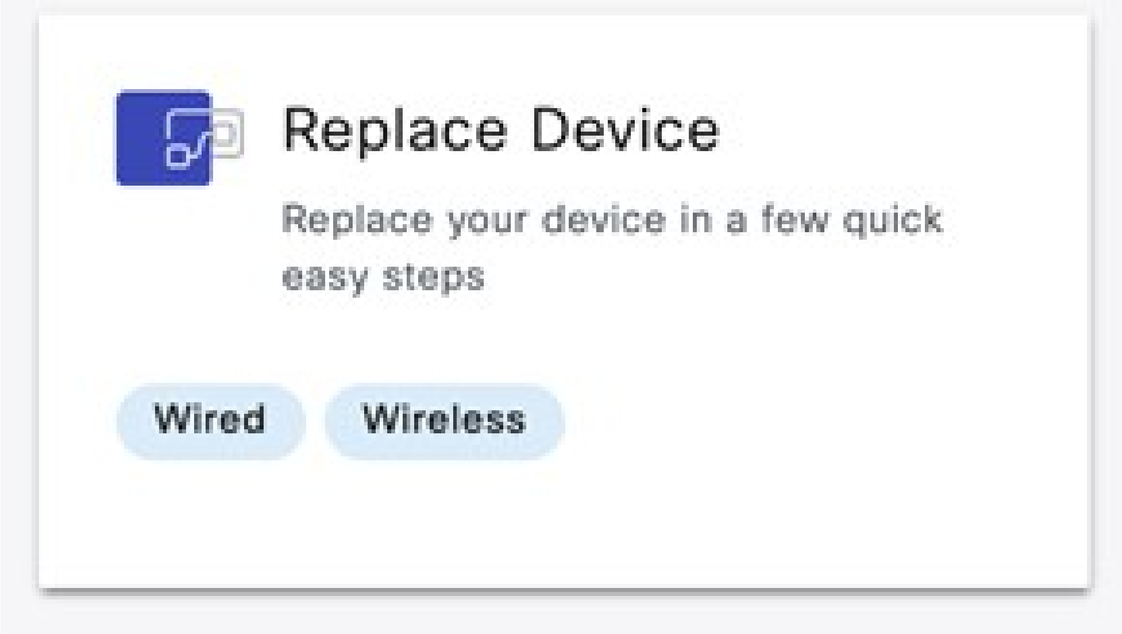
- Cisco DNA Center should have provisioned the AP to be replaced.
- The AP to be replaced should be in unreachable state.
- The new AP is registered with the wireless controller where the older AP was registered.
- The new AP is visible in Cisco DNA Center inventory window.

When replacing the AP, the old AP and the new AP have to be the same model. If you are replacing the old AP with a different model, use the **Access Point Refresh** workflow that is explained in the following subsection.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Workflows** > **Replace Device**.

Figure 220: Replace Device

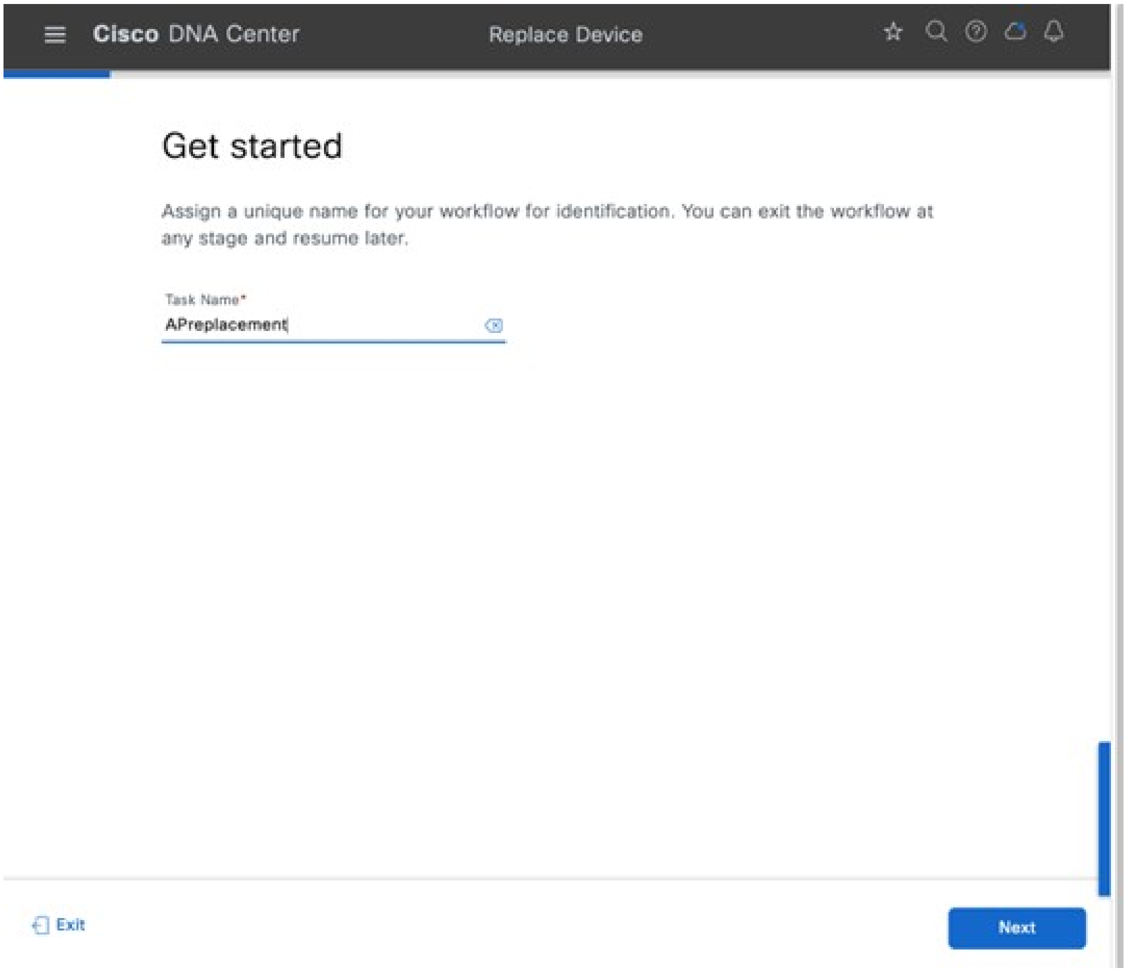


Replace Device

Replace your device in a few quick easy steps

Step 2 In the **Get started** window, enter a unique **Task Name** for your workflow.

Figure 221: Get Started



Get started

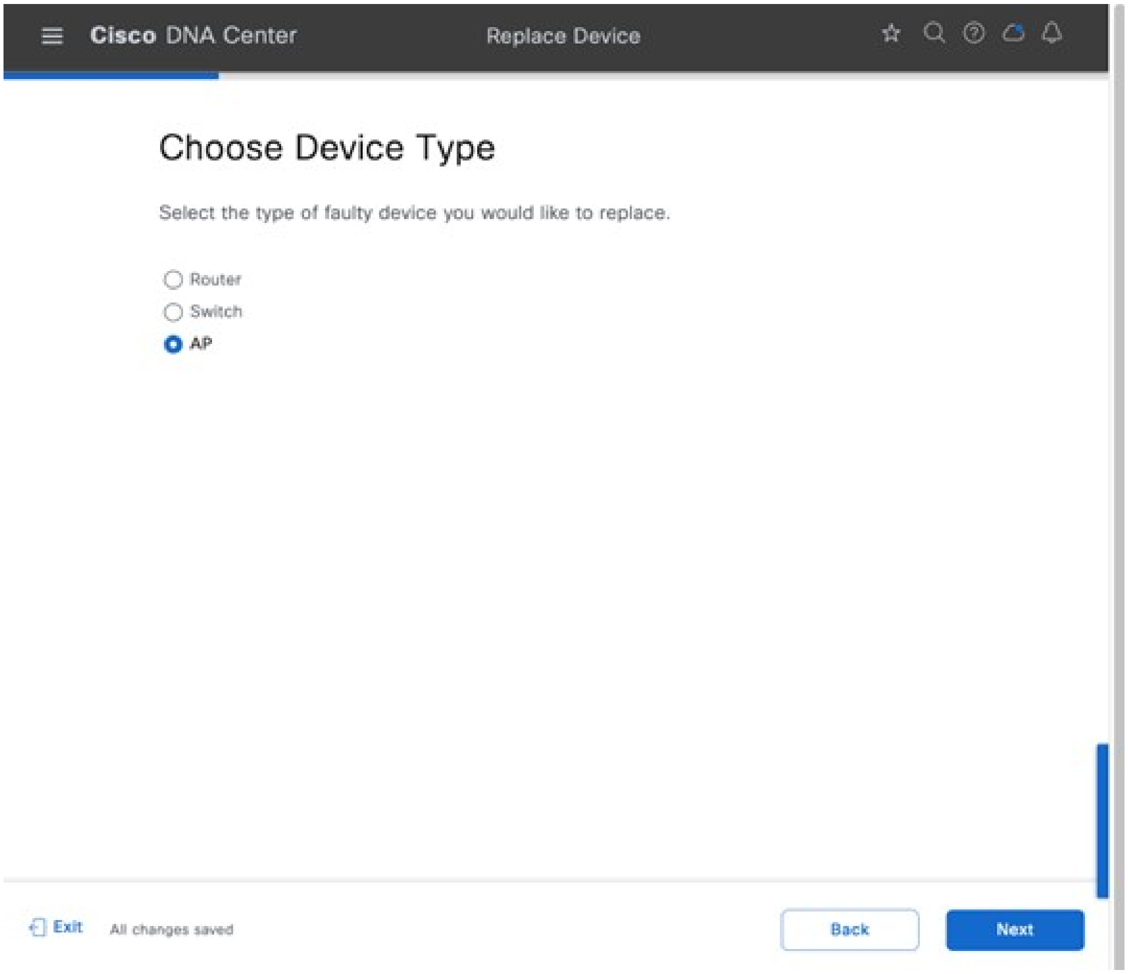
Assign a unique name for your workflow for identification. You can exit the workflow at any stage and resume later.

Task Name*

APreplacement

Step 3 In the **Choose Device Type** window, choose **AP**.

Figure 222: Choose Device Type



Choose Device Type

Select the type of faulty device you would like to replace.

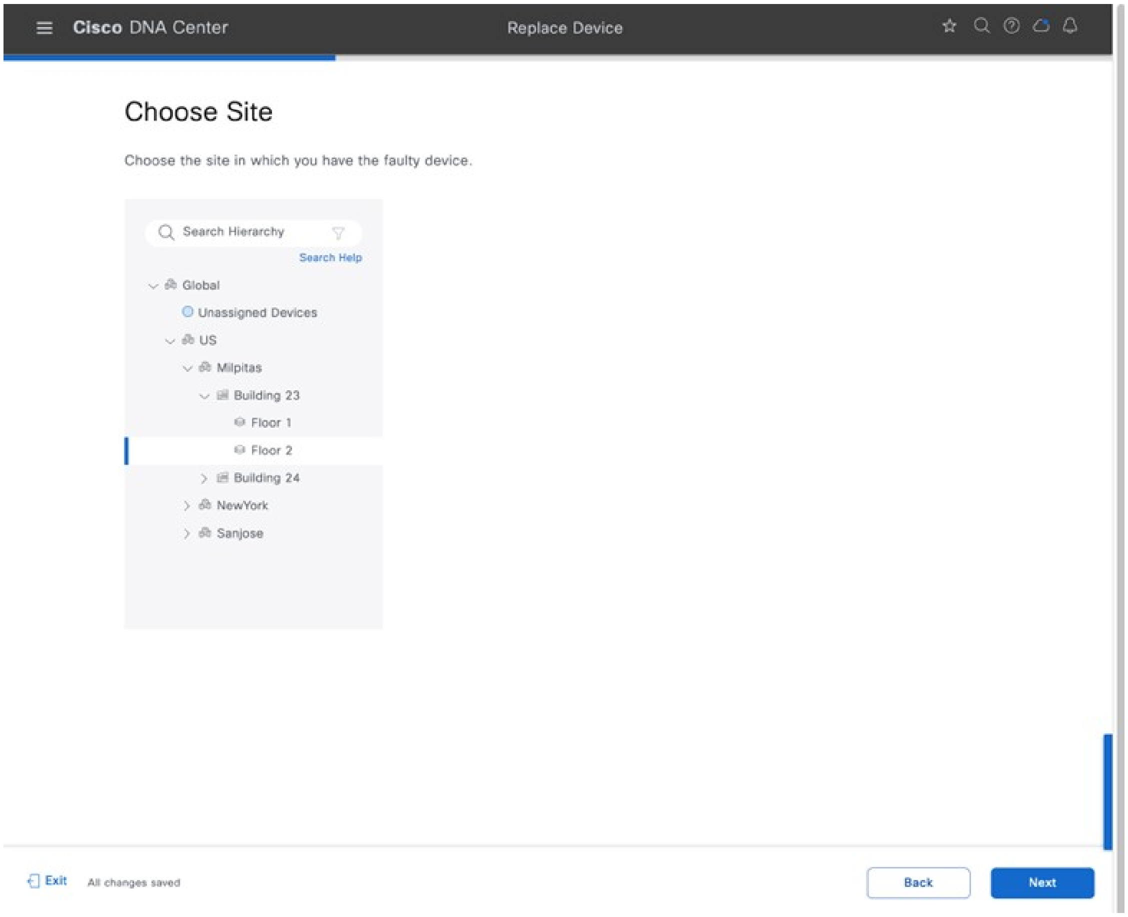
○ Router

○ Switch

● AP

Step 4 In the **Choose Site** window, choose the site in which AP needs to be replaced.

Figure 223: Choose Site



Choose Site

Choose the site in which you have the faulty device.

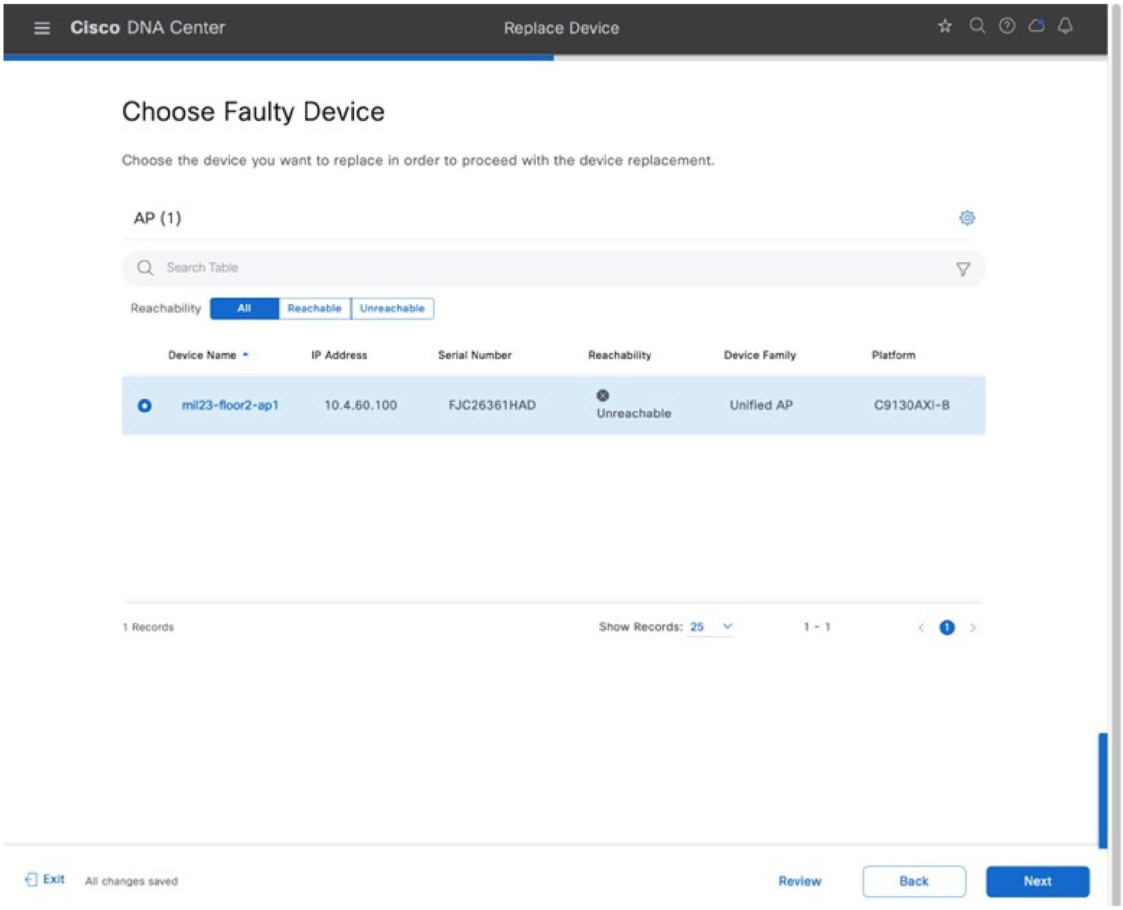
Step 5 In the **Choose Faulty Device** window, if you don't find an AP, do the following:

a) Click **Add Faulty Device**.

b) Choose the faulty device and click **Next**.

c) In the **Mark for Replacement** window, click **Mark**.

Figure 224: Choose Faulty Device



Choose Faulty Device

Choose the device you want to replace in order to proceed with the device replacement.

AP (1)

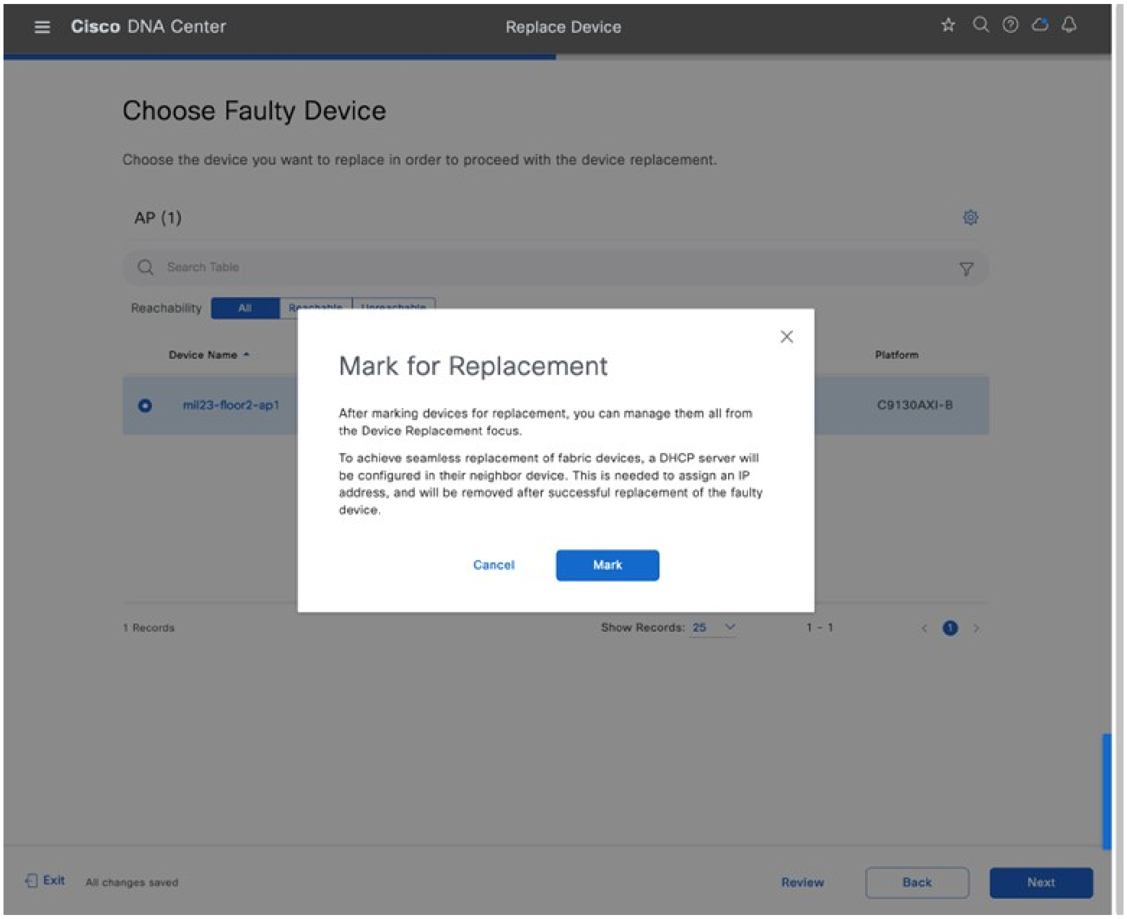
	Device Name	IP Address	Serial Number	Reachability	Device Family	Platform
●	mil23-floor2-ap1	10.4.60.100	FJC26361HAD	Unreachable	Unified AP	C9130AXI-B

1 Records

Show Records: 25

1 - 1

Figure 225: Mark for Replacement



Choose Faulty Device

Choose the device you want to replace in order to proceed with the device replacement.

Device Name	Platform
● mil23-floor2-ap1	C9130AXI-B

1 Records   Show Records: 25   1 - 1

Mark for Replacement

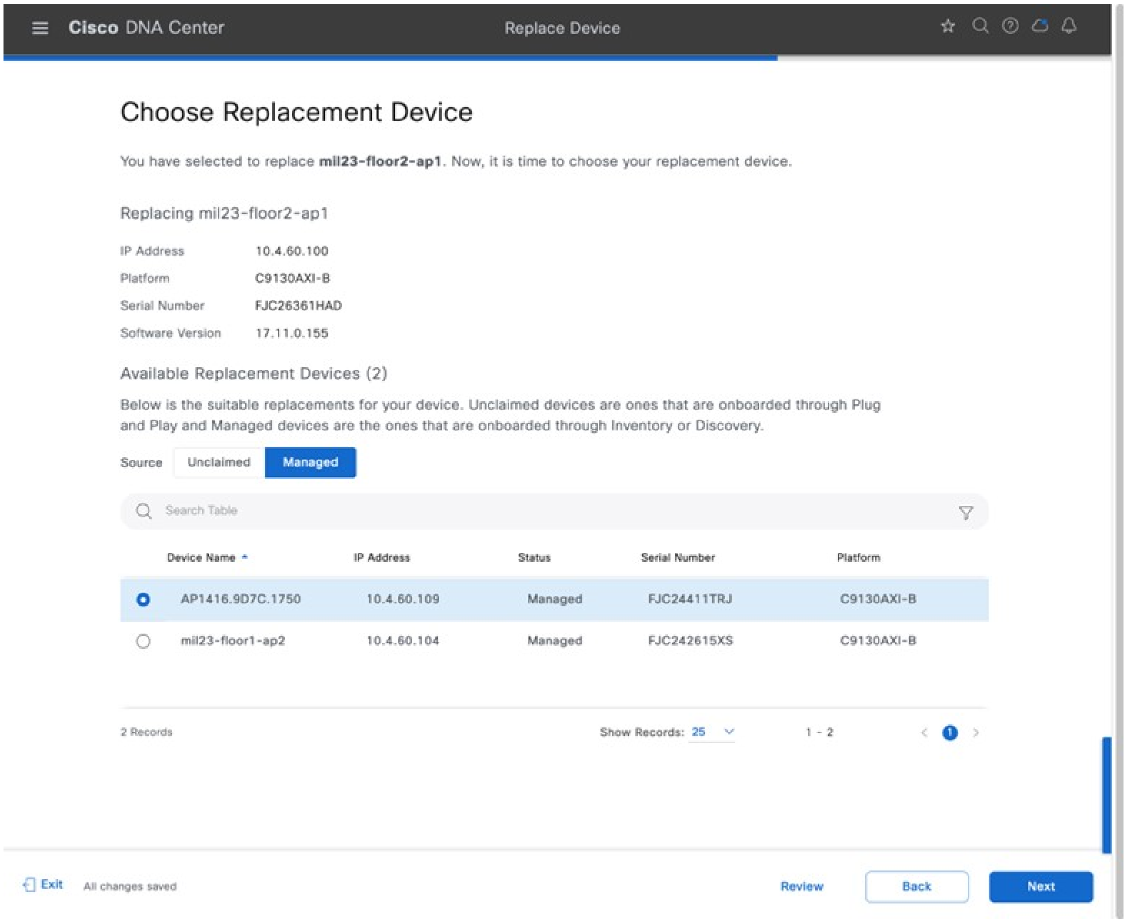
After marking devices for replacement, you can manage them all from the Device Replacement focus.

To achieve seamless replacement of fabric devices, a DHCP server will be configured in their neighbor device. This is needed to assign an IP address, and will be removed after successful replacement of the faulty device.

Step 6 In the **Choose Replacement Device** window, choose a replacement device from the **Unclaimed** tab or **Managed** tab.

The **Unclaimed** tab shows the devices that are onboarded through PnP. The **Managed** tab shows the devices that are onboarded either through inventory or the discovery process.

Figure 226: Choose Replacement Device



Choose Replacement Device

You have selected to replace **mil23-floor2-ap1**. Now, it is time to choose your replacement device.

Replacing mil23-floor2-ap1

IP Address	10.4.60.100
Platform	C9130AXI-B
Serial Number	FJC26361HAD
Software Version	17.11.0.155

Available Replacement Devices (2)

Below is the suitable replacements for your device. Unclaimed devices are ones that are onboarded through Plug and Play and Managed devices are the ones that are onboarded through Inventory or Discovery.

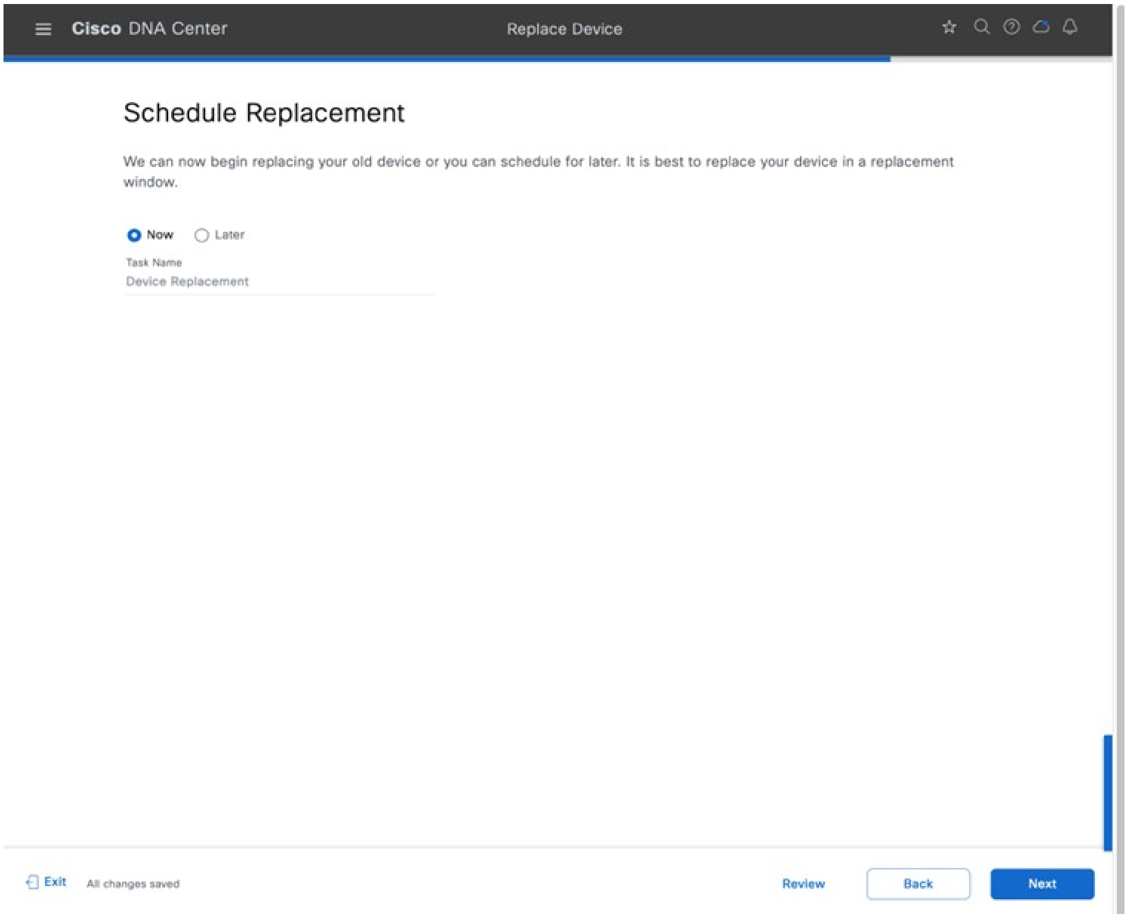
Source: Unclaimed | Managed (selected)

	Device Name	IP Address	Status	Serial Number	Platform
●	AP1416.9D7C.1750	10.4.60.109	Managed	FJC24411TRJ	C9130AXI-B
○	mil23-floor1-ap2	10.4.60.104	Managed	FJC242615XS	C9130AXI-B

2 Records   Show Records: 25   1 - 2

Step 7 In the **Schedule Replacement** window, click **Now** to start device replacement immediately, or click **Later** to schedule device replacement at a specific time.

Figure 227: Schedule Replacement



Schedule Replacement

We can now begin replacing your old device or you can schedule for later. It is best to replace your device in a replacement window.

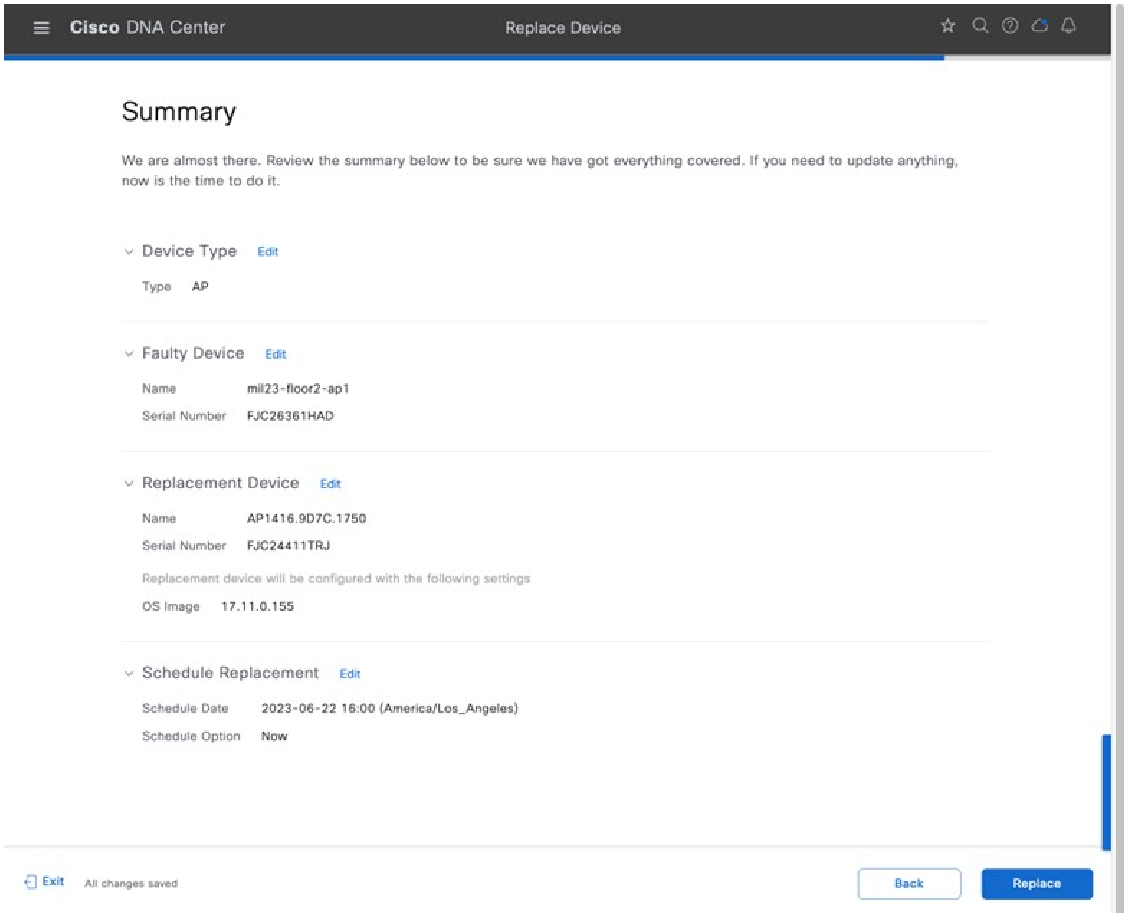
● Now ○ Later

Task Name
Device Replacement

All changes saved

Step 8 In the **Summary** window, review the configuration settings.

Figure 228: Summary Window



Summary

We are almost there. Review the summary below to be sure we have got everything covered. If you need to update anything, now is the time to do it.

Device Type Edit

Type AP

Faulty Device Edit

Name mil23-floor2-ap1

Serial Number FJC26361HAD

Replacement Device Edit

Name AP1416.9D7C.1750

Serial Number FJC24411TRJ

Replacement device will be configured with the following settings

OS Image 17.11.0.155

Schedule Replacement Edit

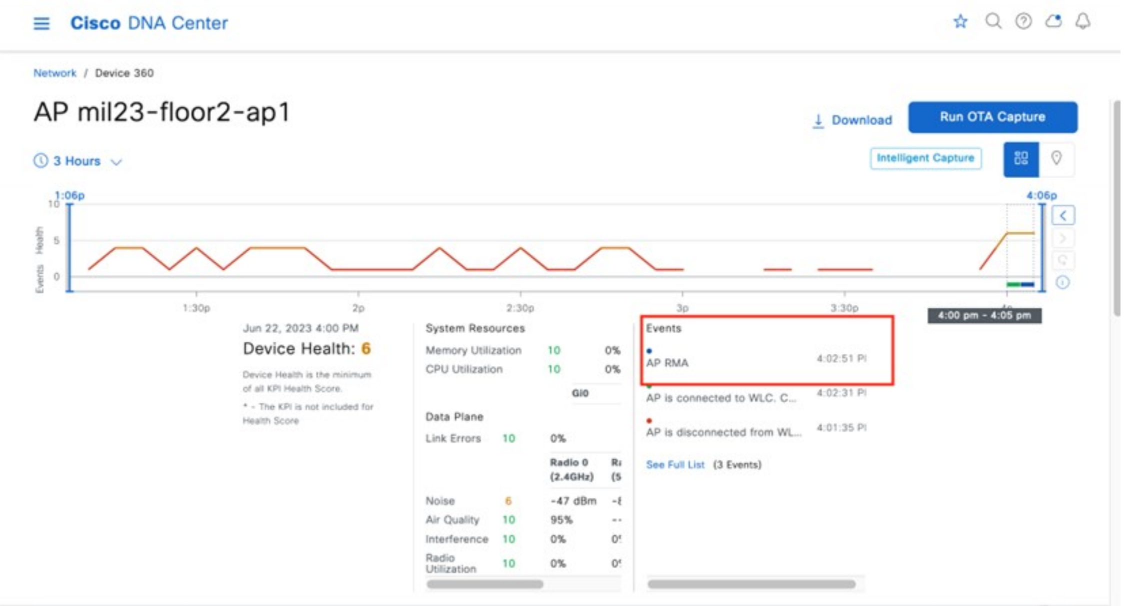
Schedule Date 2023-06-22 16:00 (America/Los_Angeles)

Schedule Option Now

Step 9 Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** window.

Step 10 **Device 360** window displays the RMA in the timeline and the **Event** table.

Figure 229: Device 360 Window



Jun 22, 2023 4:00 PM

Device Health: 6

Device Health is the minimum of all KPI Health Score.

* - The KPI is not included for Health Score

System Resources

Memory Utilization	10	0%
CPU Utilization	10	0%

Data Plane

			Gi0
Link Errors	10		0%

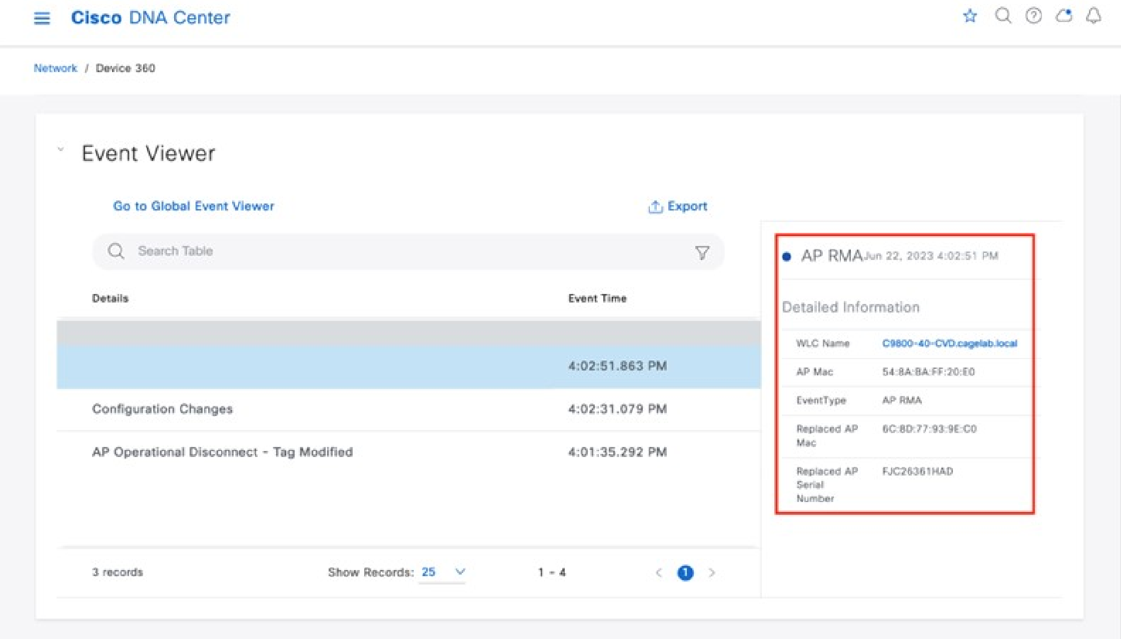
		Radio 0 (2.4GHz)	Ra (5
Noise	6	-47 dBm	-8
Air Quality	10	95%	--
Interference	10	0%	0'
Radio Utilization	10	0%	0'

Events

AP RMA	4:02:51 PI
AP is connected to WLC. C...	4:02:31 PI
AP is disconnected from WL...	4:01:35 PI

See Full List (3 Events)

Figure 230: Event Viewer



Details	Event Time
	4:02:51.863 PM
Configuration Changes	4:02:31.079 PM
AP Operational Disconnect - Tag Modified	4:01:35.292 PM

3 records Show Records: 25 1 - 4 1

AP RMA Jun 22, 2023 4:02:51 PM

Detailed Information

WLC Name	C9800-40-CVD.cagelab.local
AP Mac	54:8A:BA:FF:20:E0
EventType	AP RMA
Replaced AP Mac	6C:8D:77:93:9E:C0
Replaced AP Serial Number	FJC26361HAD

AP Refresh

Cisco DNA Center provides the AP hardware refresh guided workflow. You can use the following procedure to replace old APs with new ones in Cisco DNA Center.

Before you begin

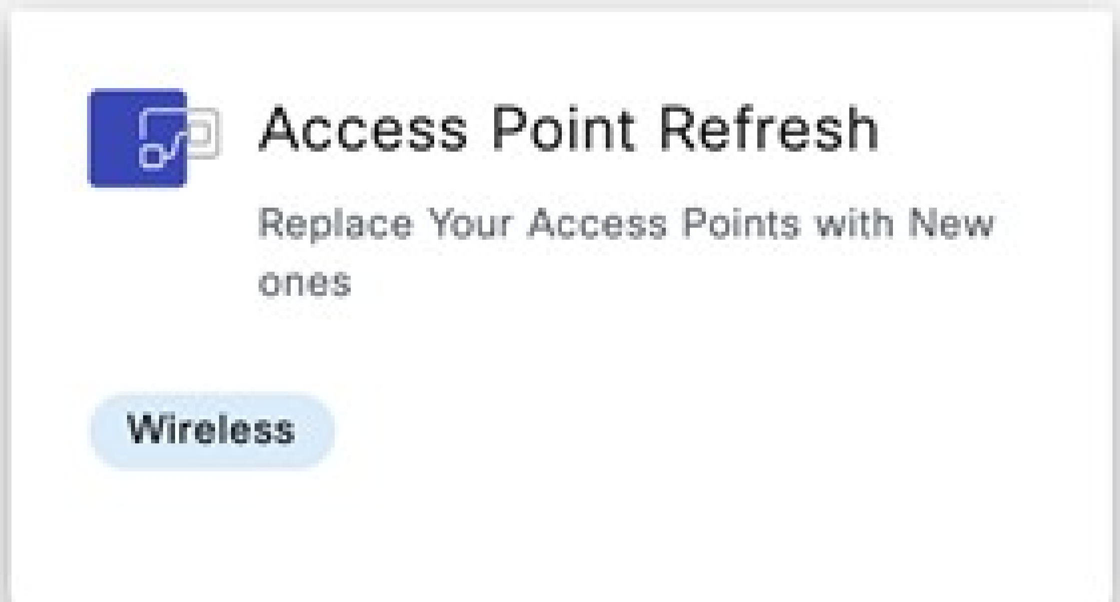
- The old AP site must be provisioned.
- Ensure that the old AP is in the unreachable state.
- The new AP must be registered with the wireless controller where the old AP is registered.
- The new AP must be available in the Cisco DNA Center inventory.

When replacing an AP with an internal antenna with an AP with an external antenna, the angles of the external antenna are to be manually set and vice versa.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Workflows** > **Access Point Refresh**.

Figure 231: Access Point Refresh

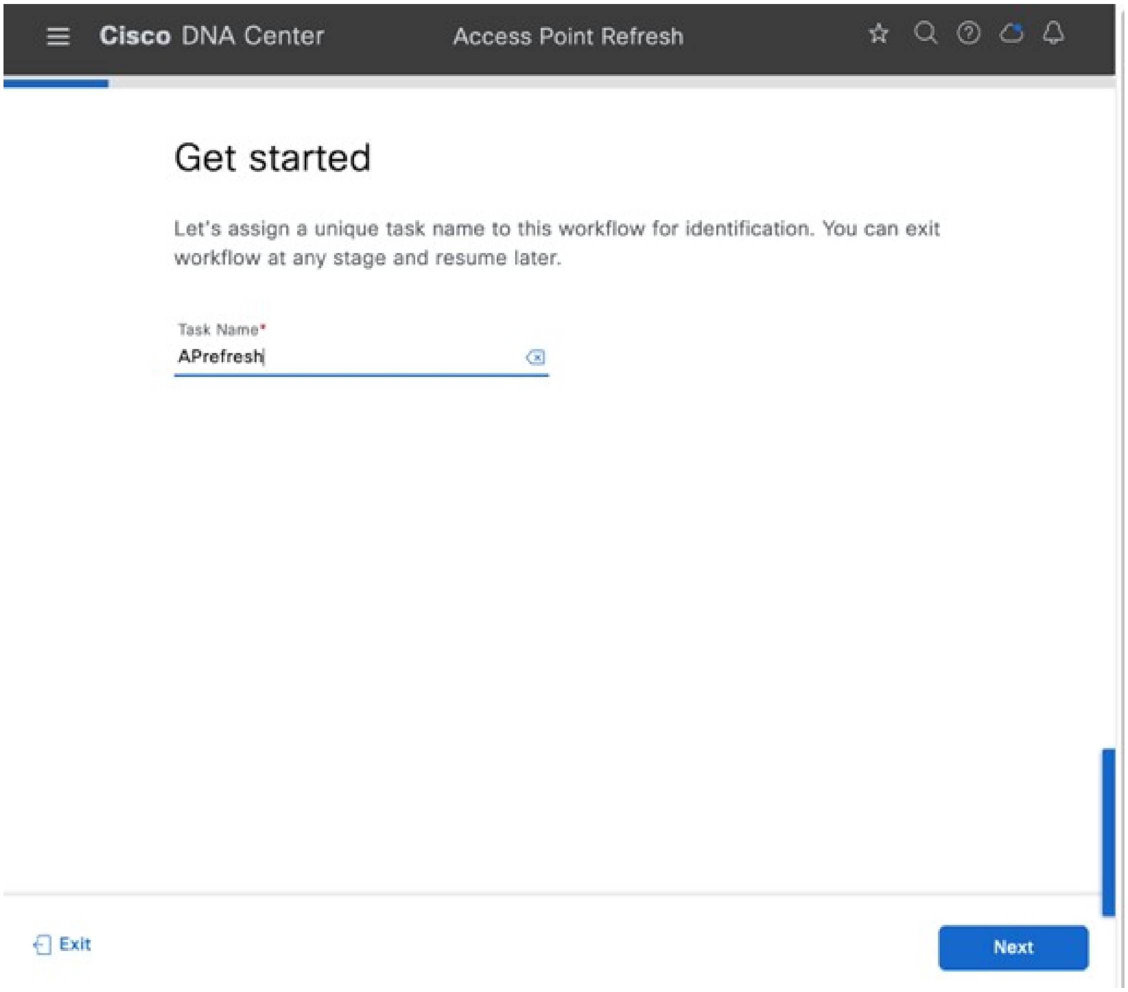


Access Point Refresh

Replace Your Access Points with New ones

Step 2 In the **Get Started** window, enter a unique name for the task, and click **Next**.

Figure 232: Get Started



Get started

Let's assign a unique task name to this workflow for identification. You can exit workflow at any stage and resume later.

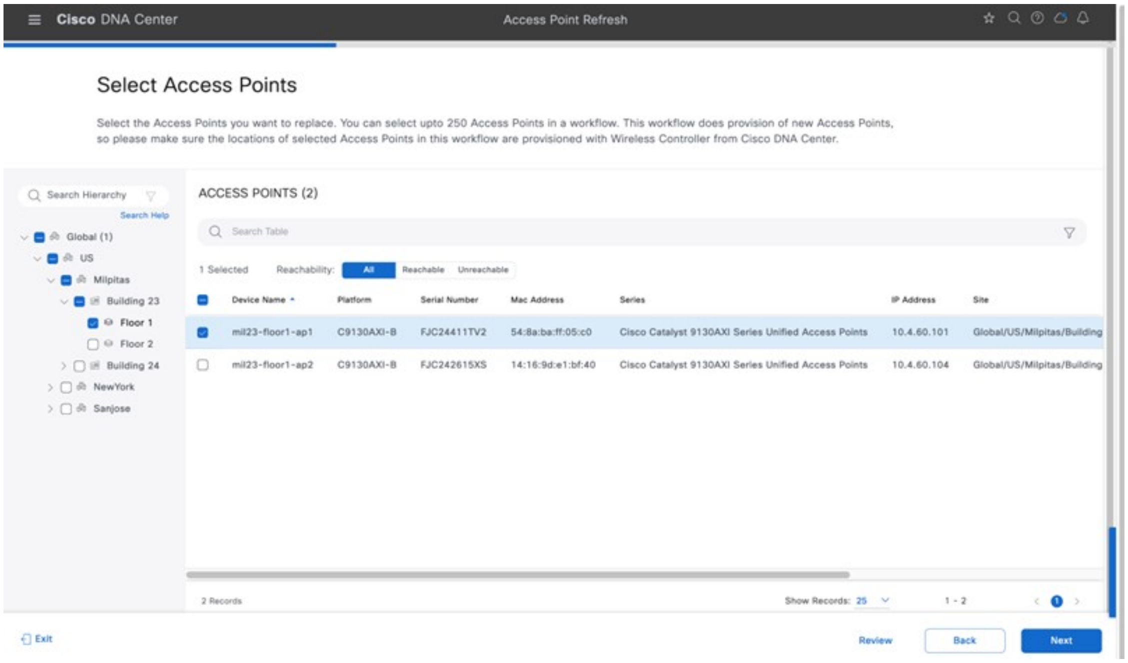
Task Name*
APrefresh

Step 3 In the **Select Access Points** window, do the following:

a. In the left pane, check the check box next to the floor where you want to refresh the AP.

b. In the right pane, check the check box next to the device name that you want to replace.

Figure 233: Select Access Points



Select Access Points

Select the Access Points you want to replace. You can select upto 250 Access Points in a workflow. This workflow does provision of new Access Points, so please make sure the locations of selected Access Points in this workflow are provisioned with Wireless Controller from Cisco DNA Center.

	Device Name	Platform	Serial Number	Mac Address	Series	IP Address	Site
☑	mil23-floor1-ap1	C9130AXI-B	FJC24411TV2	54:8a:ba:ff:05:c0	Cisco Catalyst 9130AXI Series Unified Access Points	10.4.60.101	Global/US/Milpitas/Building
□	mil23-floor1-ap2	C9130AXI-B	FJC242615XS	14:16:9d:e1:bf:40	Cisco Catalyst 9130AXI Series Unified Access Points	10.4.60.104	Global/US/Milpitas/Building

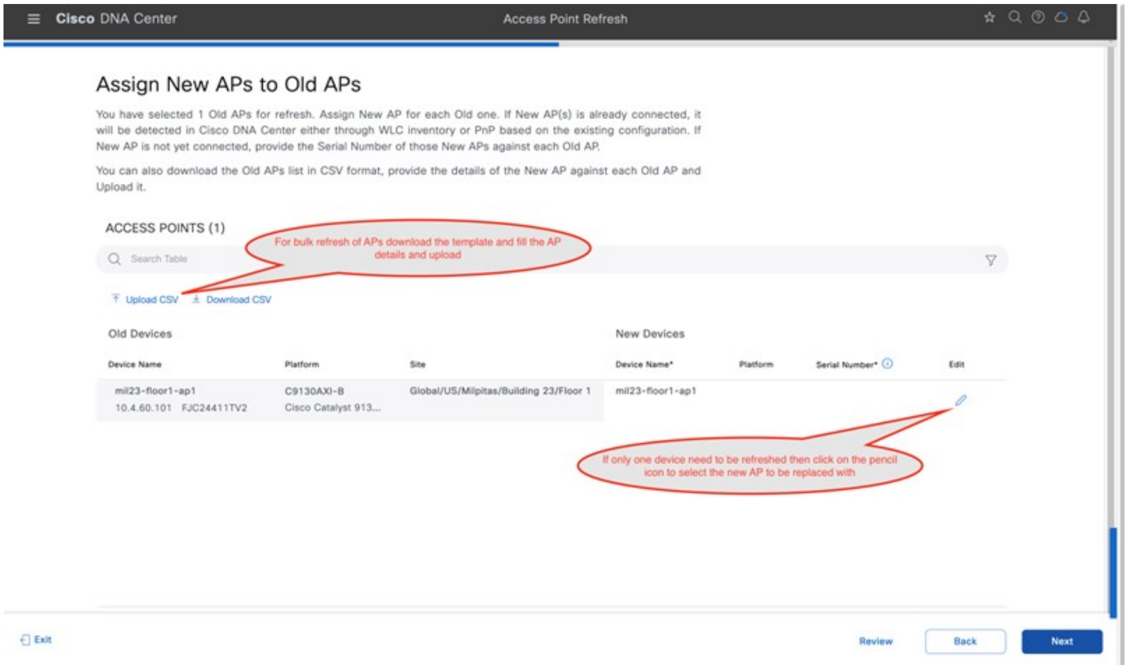
Step 4 In the **Assign New APs to Old APs** window, to add the new AP details using comma-separated value (CSV) file, do the following:

a. Click **Download CSV**. The downloaded CSV template file contains the old AP details. Update the device name and add the serial number of the new AP.

b. To import the CSV file, click **Upload CSV**.

Step 5 To add the new AP details using the GUI, click the edit icon (✎) for the AP, and in the **Edit details**, make necessary changes as shown in the following figures.

Figure 234: Assign New APs to Old APs



Assign New APs to Old APs

You have selected 1 Old APs for refresh. Assign New AP for each Old one. If New AP(s) is already connected, it will be detected in Cisco DNA Center either through WLC inventory or PnP based on the existing configuration. If New AP is not yet connected, provide the Serial Number of those New APs against each Old AP.

You can also download the Old APs list in CSV format, provide the details of the New AP against each Old AP and Upload it.

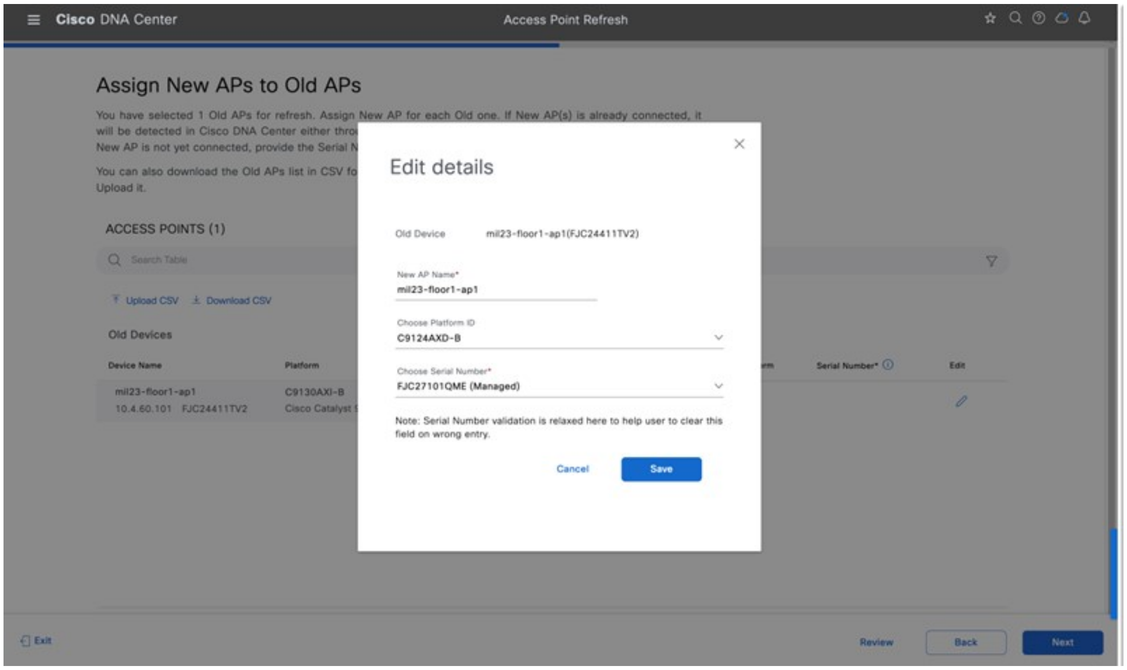
ACCESS POINTS (1)

For bulk refresh of APs download the template and fill the AP details and upload

Old Devices			New Devices			
Device Name	Platform	Site	Device Name*	Platform	Serial Number*	Edit
mil23-floor1-ap1 10.4.60.101 FJC24411TV2	C9130AXI-B Cisco Catalyst 913...	Global/US/Milpitas/Building 23/Floor 1	mil23-floor1-ap1			

If only one device need to be refreshed then click on the pencil icon to select the new AP to be replaced with

Figure 235: Edit Details



Edit details

Old Device mil23-floor1-ap1(FJC24411TV2)

New AP Name*
mil23-floor1-ap1

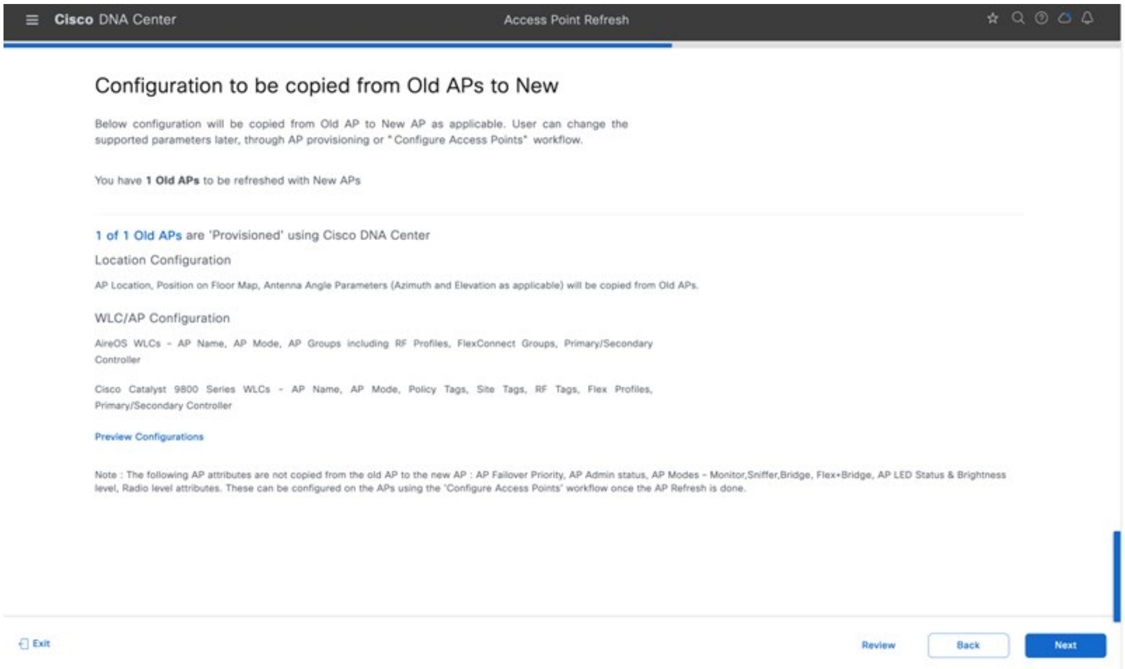
Choose Platform ID
C9124AXD-B

Choose Serial Number*
FJC27101QME (Managed)

Note: Serial Number validation is relaxed here to help user to clear this field on wrong entry.

Step 6 Click **Save**, and click **Next** to view the refresh summary.

Figure 236: Copy Configurations from Old APs to New



Configuration to be copied from Old APs to New

Below configuration will be copied from Old AP to New AP as applicable. User can change the supported parameters later, through AP provisioning or " Configure Access Points" workflow.

You have **1 Old APs** to be refreshed with New APs

1 of 1 Old APs are 'Provisioned' using Cisco DNA Center

Location Configuration

AP Location, Position on Floor Map, Antenna Angle Parameters (Azimuth and Elevation as applicable) will be copied from Old APs.

WLC/AP Configuration

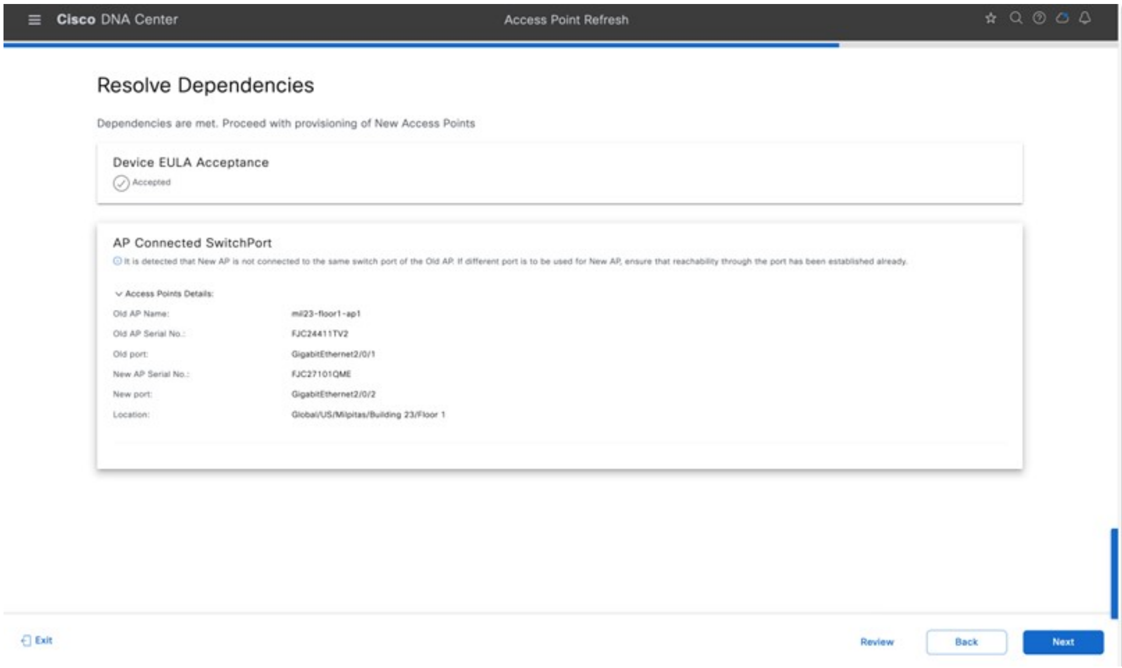
AireOS WLCs - AP Name, AP Mode, AP Groups including RF Profiles, FlexConnect Groups, Primary/Secondary Controller

Cisco Catalyst 9800 Series WLCs - AP Name, AP Mode, Policy Tags, Site Tags, RF Tags, Flex Profiles, Primary/Secondary Controller

Preview Configurations

Note : The following AP attributes are not copied from the old AP to the new AP : AP Failover Priority, AP Admin status, AP Modes - Monitor,Sniffer,Bridge, Flex+Bridge, AP LED Status & Brightness level, Radio level attributes. These can be configured on the APs using the 'Configure Access Points' workflow once the AP Refresh is done.

Figure 237: Resolve Dependencies



Resolve Dependencies

Dependencies are met. Proceed with provisioning of New Access Points

Device EULA Acceptance

✓ Accepted

AP Connected SwitchPort

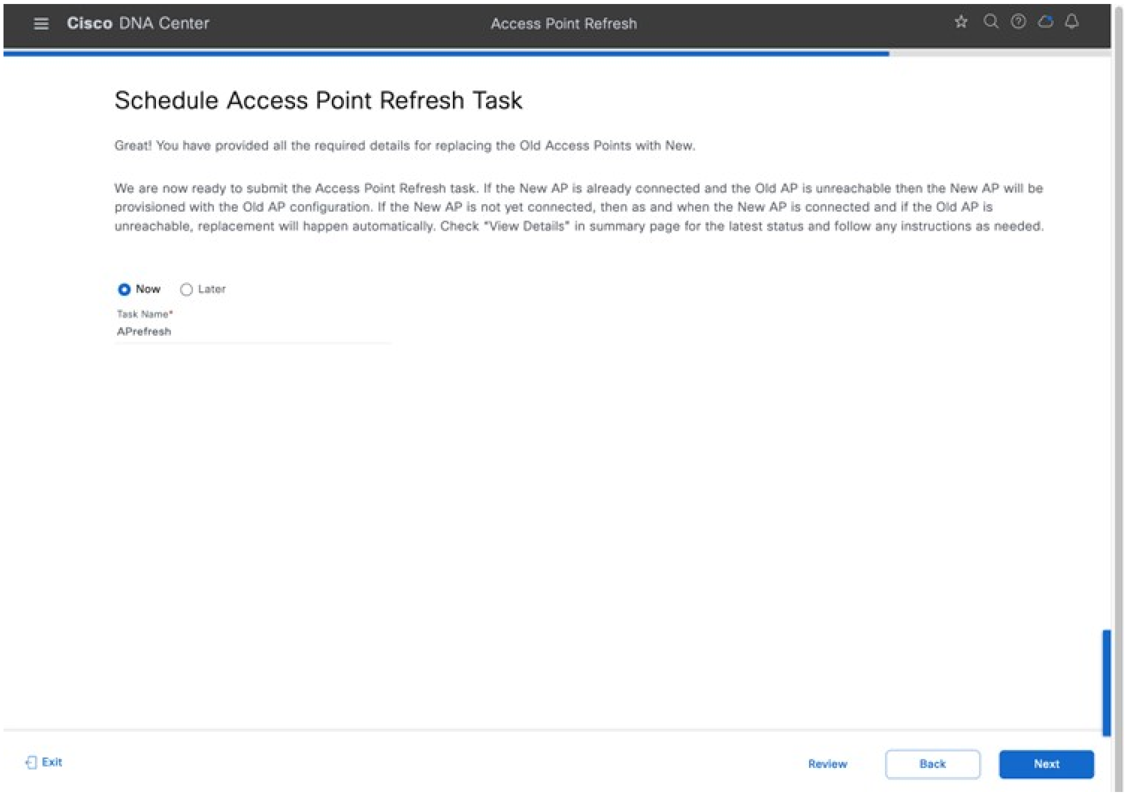
It is detected that New AP is not connected to the same switch port of the Old AP. If different port is to be used for New AP, ensure that reachability through the port has been established already.

Access Points Details:

Old AP Name:	mil23-floor1-ap1
Old AP Serial No.:	FJC24411TV2
Old port:	GigabitEthernet2/0/1
New AP Serial No.:	FJC27101QME
New port:	GigabitEthernet2/0/2
Location:	Global/US/Milpitas/Building 23/Floor 1

Step 7 In the **Schedule Access Point Refresh Task** window, click **Now** to start AP refresh immediately, or click **Later** to schedule AP refresh at a specific time.

Figure 238: Schedule AP Refresh Task



Schedule Access Point Refresh Task

Great! You have provided all the required details for replacing the Old Access Points with New.

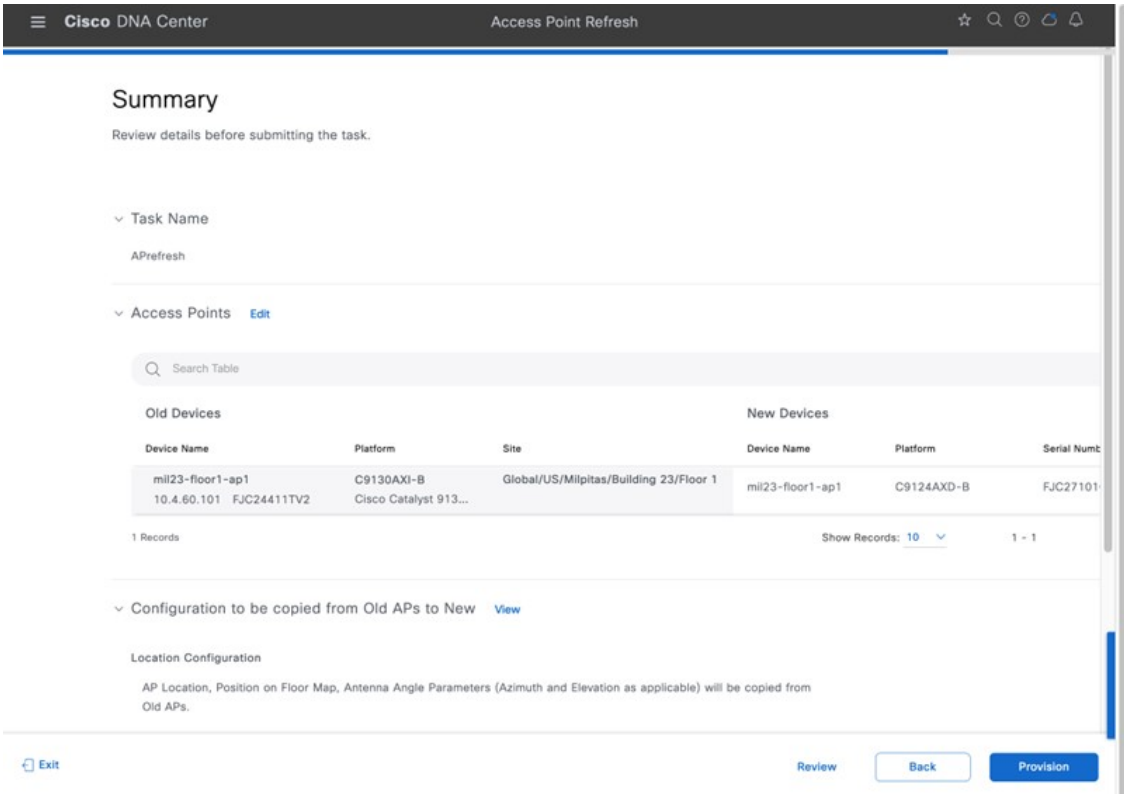
We are now ready to submit the Access Point Refresh task. If the New AP is already connected and the Old AP is unreachable then the New AP will be provisioned with the Old AP configuration. If the New AP is not yet connected, then as and when the New AP is connected and if the Old AP is unreachable, replacement will happen automatically. Check "View Details" in summary page for the latest status and follow any instructions as needed.

● Now ○ Later

Task Name*
APrefresh

Step 8 In the **Summary** window, review the configuration settings.

Figure 239: Summary Window



Summary

Review details before submitting the task.

Task Name

APrefresh

Access Points

Old Devices			New Devices		
Device Name	Platform	Site	Device Name	Platform	Serial Numb
mil23-floor1-ap1 10.4.60.101 FJC24411TV2	C9130AXI-B Cisco Catalyst 913...	Global/US/Milpitas/Building 23/Floor 1	mil23-floor1-ap1	C9124AXD-B	FJC27101

1 Records

Show Records: 10

1 - 1

Configuration to be copied from Old APs to New

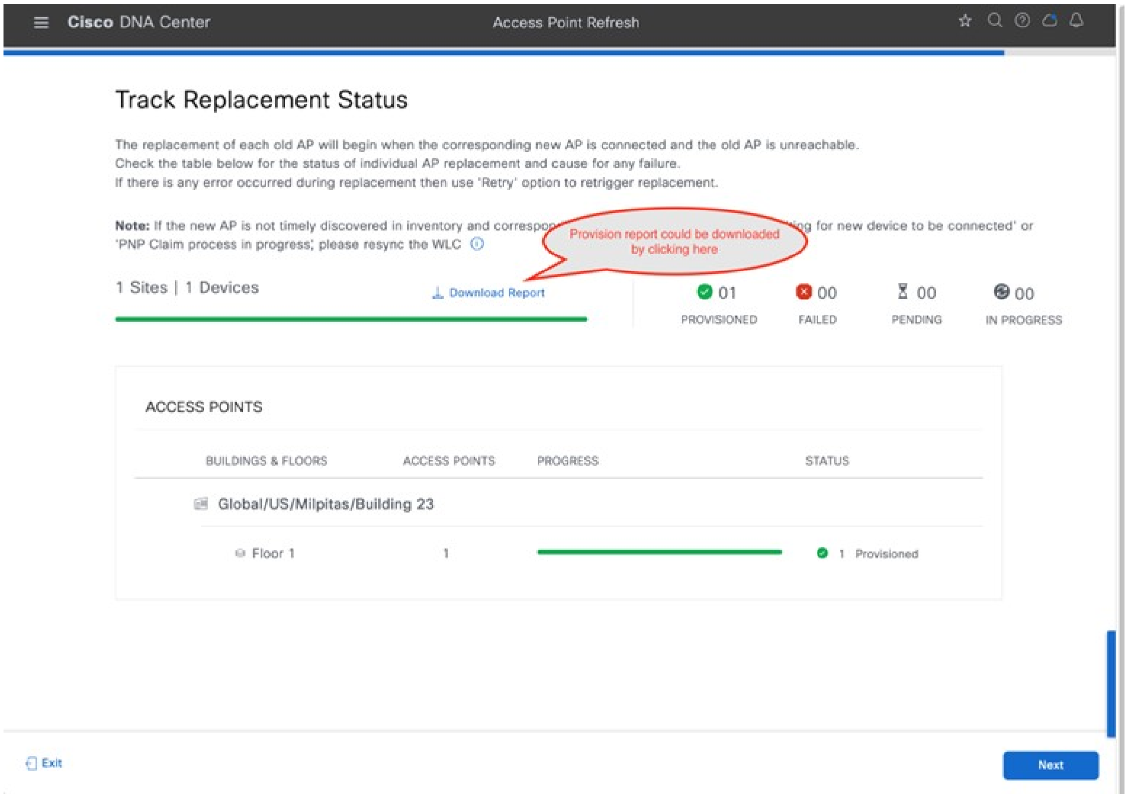
Location Configuration

AP Location, Position on Floor Map, Antenna Angle Parameters (Azimuth and Elevation as applicable) will be copied from Old APs.

Step 9 Click **Provision** to start the provisioning.

Step 10 In the **Track Replacement Status** window, click **Download Report** to download the provisioning status report.

Figure 240: Track Replacement Status



Track Replacement Status

The replacement of each old AP will begin when the corresponding new AP is connected and the old AP is unreachable.
Check the table below for the status of individual AP replacement and cause for any failure.
If there is any error occurred during replacement then use 'Retry' option to retrigger replacement.

Note: If the new AP is not timely discovered in inventory and correspon ing for new device to be connected' or 'PNP Claim process in progress', please resync the WLC

Provision report could be downloaded by clicking here

1 Sites | 1 Devices

Download Report

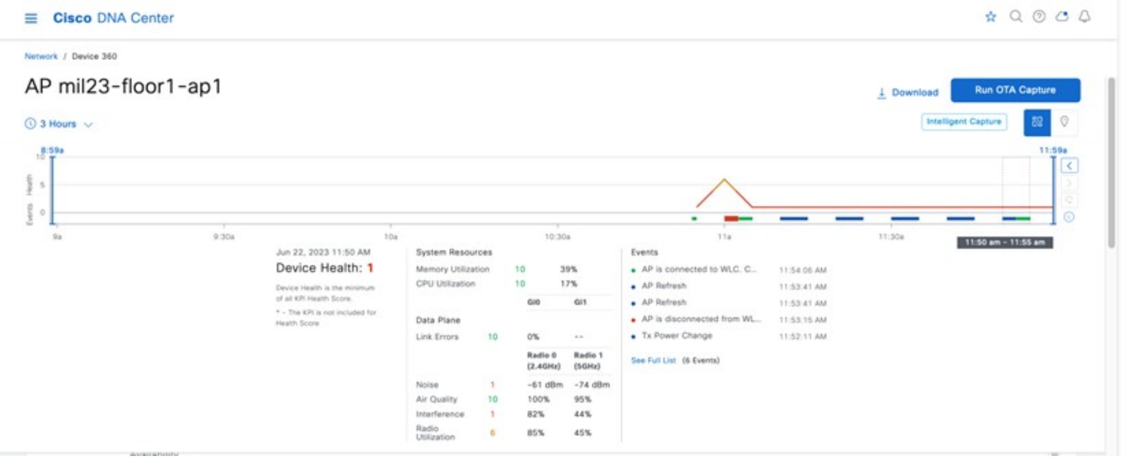
01	00	00	00
PROVISIONED	FAILED	PENDING	IN PROGRESS

ACCESS POINTS

BUILDINGS & FLOORS	ACCESS POINTS	PROGRESS	STATUS
Global/US/Milpitas/Building 23			
Floor 1	1		1 Provisioned

Step 11 An Assurance AP 360 page displays the AP refresh timeline in the time travel and **Events** table as shown in the following figures.

Figure 241: Device 360



AP mil23-floor1-ap1

Jun 22, 2023 11:50 AM

Device Health: 1

Device Health is the minimum of all KPI Health Score.

* - The KPI is not included for Health Score

System Resources

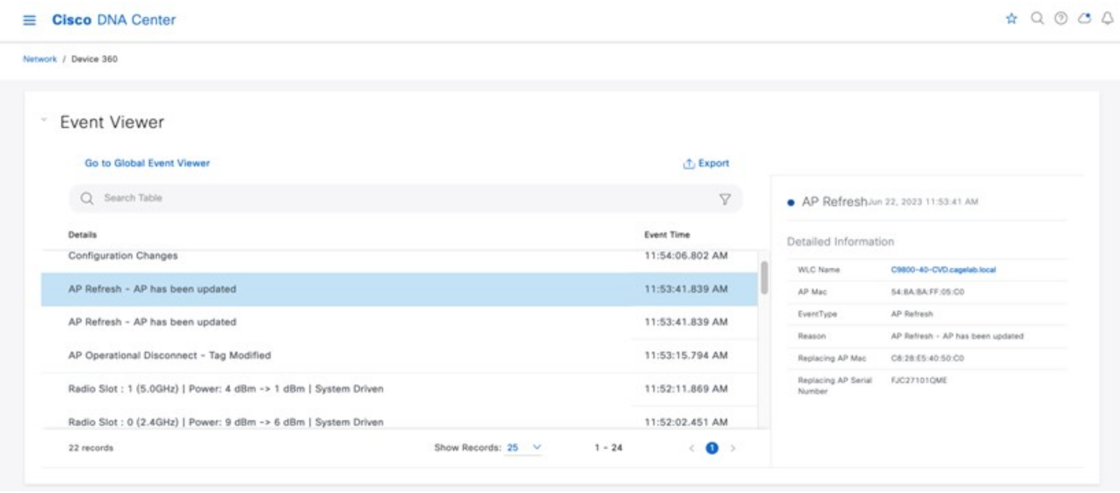
Memory Utilization	10	39%	
CPU Utilization	10	17%	
		Gi0	Gi1
Data Plane			
Link Errors	10	0%	--
		Radio 0 (2.4GHz)	Radio 1 (5GHz)
Noise	1	-61 dBm	-74 dBm
Air Quality	10	100%	95%
Interference	1	82%	44%
Radio Utilization	6	85%	45%

Events

AP is connected to WLC. C...	11:54:06 AM
AP Refresh	11:53:41 AM
AP Refresh	11:53:41 AM
AP is disconnected from WL...	11:53:15 AM
Tx Power Change	11:52:11 AM

See Full List (6 Events)

Figure 242: Event Viewer



Details	Event Time
Configuration Changes	11:54:06.802 AM
AP Refresh - AP has been updated	11:53:41.839 AM
AP Refresh - AP has been updated	11:53:41.839 AM
AP Operational Disconnect - Tag Modified	11:53:15.794 AM
Radio Slot : 1 (5.0GHz) | Power: 4 dBm -> 1 dBm | System Driven	11:52:11.869 AM
Radio Slot : 0 (2.4GHz) | Power: 9 dBm -> 6 dBm | System Driven	11:52:02.451 AM

22 records Show Records: 25 1 - 24

AP Refresh Jun 22, 2023 11:53:41 AM

Detailed Information

WLC Name	C9800-40-CVD.cagelab.local
AP Mac	54:8A:BA:FF:05:C0
EventType	AP Refresh
Reason	AP Refresh - AP has been updated
Replacing AP Mac	C8:28:E5:40:50:C0
Replacing AP Serial Number	FJC27101QME

Cloud-Based AI Enhancements

Cisco DNA Center has AI-based enhancements that leverage the power of machine learning (ML) and machine reasoning (MR) to provide accurate insights that are specific to your network deployment. The AI-based features include Radio Resource Management (RRM) and broadly AI-based Analytics, which provides network insights and deviations from the baseline.

Cisco AI RRM

AI-enhanced RRM integrates the power of artificial intelligence (AI) and ML into the reliable and trusted Cisco RRM product family algorithms in the cloud. AI-enhanced RRM is coordinated through Cisco DNA Center (an on-premises appliance) as a service. Existing Cisco Catalyst 9800 RRM sites can transition seamlessly to an intelligent, centralized service. As with other Cisco DNA Center services, AI-enhanced RRM brings a host of new features with it. Learn more here.

Cisco AI Analytics

Cisco AI Analytics provides insights and charts that help network administrators troubleshoot network issues and conduct long-term capacity planning. Learn more here.

Mesh Networks

Cisco outdoor APs can be operated with a wired network for backhaul, or with a mesh network using a 5-GHz or 2.4-GHz radio as the backhaul. In a Cisco wireless mesh network, multiple mesh APs form a network that provides secure, scalable wireless LAN. APs in a mesh network operate through root access point (RAP) or mesh access point (MAP). RAPs are connected to the wired network at each location. All downstream APs operate as MAPs and communicate using wireless links. All APs are configured and shipped as mesh APs. To use an AP as a RAP, any MAP must be reconfigured as RAP. All mesh networks must contain at least one RAP.

Details on how to use Cisco DNA Center to configure a mesh network are available here. After Cisco DNA Center 2.3.6, the **Wireless Settings** window organizes the workflows under different tiles. You create the AP authorization list under **Security Settings**, and then click **AP Authorization List**. You create the mesh AP profile under the **AP Profiles** tile, and then click **Add**. Choose the wireless controller type to be the AP Profile for IOS-XE. In the profile window, click **Mesh** to configure the mesh parameters.

Hardware and Software Specifications

The solution is tested with the hardware and software listed in the following table.

Functional Area	Product	Software Version
Enterprise Wireless Controllers	Cisco Catalyst 9800-40 Wireless Controllers	17.09.04a
Guest Wireless Controller	Cisco Catalyst 9800-CL Cloud Controller	17.09.04a
Enterprise SDN Controller	Cisco DNA Center	2.3.5.5
AAA Server	Cisco Identity Services Engine	3.2

Settings in Each Preconfigured RF Profile

The following tables list the settings for each of the default wireless RF profiles (low, typical, high) in Cisco DNA Center.

You cannot change the default RF profile settings. To change any setting, you must create a custom profile and assign it as the default RF profile.

Table 33: Settings for the Low Wireless RF Profile

Feature	Type	Description
Profile Name	Text field	LOW
PROFILE TYPE > 2.4 GHz	On/off toggle	Enables or disables the 2.4-GHz band for the RF profile. Set to On.
PROFILE TYPE > 2.4 GHz > Parent Profile	Radio button	This is the parent profile from which this RF profile is derived. This field only applies when creating custom RF profiles, because custom RF profiles can be based on a preconfigured RF profile. For the Low RF profile, this is set to Low. Available options: • High: High client density RF profile. • Medium (Typical): Medium client density RF profile. • Low: Low client density RF profile. • Custom: Custom RF profile.
PROFILE TYPE > 2.4 GHz > DCA Channel	Multiple choice radio button	Selects the channels in which Dynamic Channel Assignment (DCA) operates in automatic mode within the 2.4-GHz band. Choices are channels 1 to 14. The default setting is channels 1, 6, and 11. This field is not visible in the 2.4-GHz band when editing one of the preconfigured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 2.4-GHz band. Note that it is generally not recommended to implement channels other than 1, 6, and 11 in the 2.4-GHz band.

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > Supported Data Rates	Single direction slider with multiple positions	Slider with multiple positions to indicate the range of data rates supported in the 2.4-GHz band. Rates are as follows from lowest to highest: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. For the Low RF profile, this is set for all data rates, allowing maximum device compatibility. The Low RF profile is designed for wireless environments of low client density. In these environments, wireless clients may connect to APs at potentially farther distances and lower data rates.
PROFILE TYPE > 2.4 GHz > Supported Data Rates > Enable 802.11b Data Rates	Check box	This check box works with the preceding slider. Checking the box enables the 802.11b data rates 1, 2, 5.5, 6, 9, and 11 Mbps on the slider. For the Low RF profile, this check box is checked.
PROFILE TYPE > 2.4 GHz > Mandatory Data Rates	Multiple choice radio button	This is used to select the data rates that the wireless client must support to be able to associate with the wireless network in the 2.4-GHz band. Choices are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. For the Low RF profile, the following data rates are mandatory: 1, 2, 5.5, and 11 Mbps.
PROFILE TYPE > 2.4 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	This slider determines the minimum and maximum power levels that Transmit Power Control (TPC) can configure on 2.4-GHz radios in APs associated with this RF profile. The full range of the slider is from –10 to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based on RSSI from neighboring APs. For the Low RF profile, the sliders are set so that the full range of power levels (–10 to 30 dBm) is available to TPC. For environments of low client density, APs may be farther spaced, and therefore may need to transmit at higher power levels for complete coverage. This setting allows TPC to adjust the 2.4-GHz radios across the full range of power levels.
PROFILE TYPE > 2.4 GHz > TX Power Configuration > RX SOP	Drop-down menu	The Receiver Start of Packet Detection Threshold (RX-SOP) determines the RF signal level at which the 2.4-GHz radio demodulates and decodes a wireless packet. Lower RX-SOP levels increase the sensitivity of the 2.4-GHz radio to wireless clients. Wireless client traffic with lower Received Signal Strength Indication (RSSI) values is decoded by the AP. Because lower RSSI is often due to the wireless client being farther from the AP, this has the effect of increasing the cell size (coverage) of the AP. This is beneficial for environments of low client density, where APs may be spaced farther apart. For the Low RF profile, this is set to Low (–80 dBm).

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and therefore the coverage behavior of the system. The TPC Power Threshold ranges from –80 to –50 dBm. Wireless deployments of low client density typically have fewer APs. Increasing the TPC Power Threshold value can result in higher transmit power levels of the radios of individual APs, increasing the overall coverage of each AP. For the Low RF profile, this is set to –65 dBm for the 2.4-GHz radio.
PROFILE TYPE > 5 GHz	On/off toggle	Enables or disables the 5-GHz band for the RF profile. Set to On.
PROFILE TYPE > 5 GHz > Parent Profile	Radio button	This is the parent profile from which this RF profile is derived. This field only applies when creating custom RF profiles, because custom RF profiles can be based on a preconfigured RF profile. For the Low RF profile, this is set to Low. Available options: • High: High client density RF profile. • Medium (Typical): Medium client density RF profile. • Low: Low client density RF profile. • Custom: Custom RF profile.
PROFILE TYPE > 5 GHz > Channel Width	Drop-down menu	Selects the channel width for the 5-GHz band. Choices are 20, 40, 80, and 160 MHz or Best. Best allows DCA to select the optimal channel width for the environment. For the Low RF profile, channel width is set to 20 MHz.
PROFILE TYPE > 5 GHz > DCA Channel	Multiple choice radio button	Selects the channels in which DCA operates in automatic mode within the 5-GHz band. Choices vary based on regulatory domain: UNII-1 channels 36 – 48, UNII-2 channels 52 – 144, and UNII-3 channels 149 – 165. This field is not visible in the 5-GHz band when editing one of the preconfigured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 5-GHz band.
PROFILE TYPE > 5GHz > Supported Data Rates	Single direction slider with multiple positions	Slider with multiple positions to indicate the range of data rates supported in the 5-GHz band. Rates are as follows from lowest to highest: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. For the Low RF profile, this is set for all data rates. The Low RF profile is designed for wireless environments of low client density. In these environments, wireless clients may connect to APs at potentially farther distances and lower data rates.

Feature	Type	Description
PROFILE TYPE > 5 GHz > Mandatory Data Rates	Multiple choice radio button	This is used to select the data rates that the wireless client must support to be able to associate with the wireless network in the 5-GHz band. Choices are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. For the low RF profile, the following data rates are mandatory: 6, 12, and 24 Mbps.
PROFILE TYPE > 5 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	This slider determines the minimum and maximum power levels that TPC can configure on 5-GHz radios in APs associated with this RF profile. The full range of the slider is from –10 to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based on RSSI from neighboring APs. For the low RF profile, the sliders are set so that the full range of power levels (–10 to 30 dBm) is available to TPC. For environments of low client density, APs may be farther spaced, and therefore may need to transmit at higher power levels for complete coverage. This setting allows TPC to adjust the 5-GHz radios across the full range of power levels.
PROFILE TYPE > 5 GHz > TX Power Configuration > RX SOP	Drop-down menu	The RX-SOP determines the RF signal level at which the 5-GHz radio demodulates and decodes a wireless packet. Lower RX-SOP levels increase the sensitivity of the 5-GHz radio to wireless clients. Wireless client traffic with lower RSSI values is decoded by the AP. Because lower RSSI is often due to the wireless client being farther from the AP, this has the effect of increasing the cell size (coverage) of the AP. This is beneficial for environments of low client density, where APs may be spaced farther apart. For the Low RF profile, this is set to Low (–80 dBm).
PROFILE TYPE > 5 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and therefore the coverage behavior of the system. The TPC Power Threshold ranges from –80 to –50 dBm. Wireless deployments of low client density typically have fewer APs. Increasing the TPC Power Threshold value can result in higher transmit power levels of the radios of individual APs, increasing the overall coverage of each AP. For the Low RF profile, this is set to –60 dBm for the 5-GHz radio.

Table 34: Settings for the Typical Wireless RF Profile

Feature	Type	Description
Profile Name	Text field	TYPICAL
PROFILE TYPE > 2.4 GHz	On/off toggle button	Enables or disables the 2.4-GHz band for the RF profile. Set to On.

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > Parent Profile	Radio button	This is the parent profile from which this RF profile is derived. This field only applies when creating custom RF profiles, because custom RF profiles can be based on a preconfigured RF profile. For the Typical RF profile, this is set to Medium (Typical). Available options: • High: High client density RF profile. • Medium (Typical): Medium client density RF profile. • Low: Low client density RF profile. • Custom: Custom RF profile.
PROFILE TYPE > 2.4 GHz > DCA Channel	Multiple choice radio button	Selects the channels in which DCA operates in automatic mode within the 2.4-GHz band. Choices are channels 1 to 14. The default setting is channels 1, 6, and 11. This field is not visible in the 2.4-GHz band when editing one of the preconfigured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 2.4-GHz band. Note that it is generally not recommended to implement channels other than 1, 6, and 11 in the 2.4-GHz band.
PROFILE TYPE > 2.4 GHz > Supported Data Rates	Single direction slider with multiple positions	Slider with multiple positions to indicate the range of data rates supported in the 2.4-GHz band. Rates are as follows from lowest to highest: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. For the Typical RF profile, this is set to rates of 9 Mbps and higher. The Typical RF profile is designed for wireless environments of medium client density. In these environments, having wireless clients connecting to APs at lower speeds decreases the overall throughput of the wireless network. Sufficient AP density should be deployed such that the clients can connect and transmit at higher rates.
PROFILE TYPE > 2.4 GHz > Supported Data Rates > Enable 802.11b Data Rates	Check box	This check box works with the preceding slider. Checking the box enables the 802.11b data rates 1, 2, 5.5, 6, 9, and 11 Mbps on the slider. For the Typical RF deployment, this check box is unchecked.
PROFILE TYPE > 2.4 GHz > Mandatory Data Rates	Multiple choice radio button	This is used to select the data rates that the wireless client must support to be able to associate with the wireless network in the 2.4-GHz band. Choices are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. For the Typical RF profile, the only data rate that is mandatory is 12 Mbps.

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	This slider determines the minimum and maximum power levels that TPC can configure on 2.4-GHz radios in APs associated with this RF profile. The full range of the slider is from –10 to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based on RSSI from neighboring APs. For the Typical RF profile, the sliders are set so that the full range of power levels (–10 to 30 dBm) is available to TPC. For environments of medium client density, APs may be more closely spaced, and therefore may need to transmit at moderate power levels for complete coverage. This setting allows TPC to adjust the 2.4-GHz radios across the full range of power levels.
PROFILE TYPE > 2.4 GHz > TX Power Configuration > RX SOP	Drop-down menu	The RX-SOP determines the RF signal level at which the 2.4-GHz radio demodulates and decodes a wireless packet. Lower RX-SOP levels increase the sensitivity of the 2.4-GHz radio to wireless clients. Wireless client traffic with lower RSSI values is decoded by the AP. Because lower RSSI is often due to the wireless client being farther from the AP, this has the effect of increasing the cell size (coverage) of the AP. This is beneficial for environments of low client density, where APs may be spaced farther apart. For the Typical RF profile, this is set to Auto.
PROFILE TYPE > 2.4 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and therefore the coverage behavior of the system. The TPC Power Threshold ranges from –80 to –50 dBm. Wireless deployments of medium client density typically have more APs. Decreasing the TPC Power Threshold value can result in lower transmit power levels of the radios of individual APs, decreasing the overall coverage of each AP, but also minimizing cochannel interference (CCI). For the Typical RF profile, this is set to –70 dBm for the 2.4-GHz radio.
PROFILE TYPE > 5 GHz	On/off toggle	Enables or disables the 5-GHz band for the RF profile. Set to On.
PROFILE TYPE > 5 GHz > Parent Profile	Radio button	This is the parent profile from which this RF profile is derived. This field only applies when creating custom RF profiles, because custom RF profiles can be based on a preconfigured RF profile. For the Typical RF profile, this is set to Medium (Typical). Available options: • High: High client density RF profile. • Medium (Typical): Medium client density RF profile. • Low: Low client density RF profile. • Custom: Custom RF profile.

Feature	Type	Description
PROFILE TYPE > 5 GHz > Channel Width	Drop-down menu	Selects the channel width for the 5-GHz band. Choices are 20, 40, 80, and 160 MHz or Best. Best allows DCA to select the optimal channel width for the environment. For the Typical RF profile, channel width is set to 20 MHz.
PROFILE TYPE > 5 GHz > DCA Channel	Multiple choice radio button	Selects the channels in which DCA operates in automatic mode within the 5-GHz band. Choices vary based on regulatory domain: UNII-1 channels 36 – 48, UNII-2 channels 52 – 144, and UNII-3 channels 149 – 165. This field is not visible in the 5-GHz band when editing one of the preconfigured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 5-GHz band.
PROFILE TYPE > 5GHz > Supported Data Rates	Single direction slider with multiple positions	Slider with multiple positions to indicate the range of data rates supported in the 5-GHz band. Rates are as follows from lowest to highest: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. For the Typical RF profile, this is set for all data rates.
PROFILE TYPE > 5 GHz > Mandatory Data Rates	Multiple choice radio button	This is used to select the data rates that the wireless client must support to be able to associate with the wireless network in the 5-GHz band. Choices are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. For the Typical RF profile, the following data rates are mandatory: 6, 12, and 24 Mbps.
PROFILE TYPE > 5 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	This slider determines the minimum and maximum power levels that TPC can configure on 5-GHz radios in APs associated with this RF profile. The full range of the slider is from –10 to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based on RSSI from neighboring APs. For the Typical RF profile, the sliders are set so that the full range of power levels (–10 to 30 dBm) is available to TPC. For environments of medium client density, APs may be more closely spaced, and therefore may need to transmit at moderate power levels for complete coverage. This setting allows TPC to adjust the 5-GHz radios across the full range of power levels.
PROFILE TYPE > 5 GHz > TX Power Configuration > RX SOP	Drop-down menu	The RX-SOP determines the RF signal level at which the 5-GHz radio demodulates and decodes a wireless packet. Lower RX-SOP levels increase the sensitivity of the 5-GHz radio to wireless clients. Wireless client traffic with lower RSSI values is decoded by the AP. Because lower RSSI is often due to the wireless client being farther from the AP, this has the effect of increasing the cell size (coverage) of the AP. This is beneficial for environments of low client density, where APs may be spaced farther apart. For the Typical RF profile, this is set to Auto.

Feature	Type	Description
PROFILE TYPE > 5 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and therefore the coverage behavior of the system. The TPC Power Threshold ranges from –80 to –50 dBm. Wireless deployments of medium client density typically have more APs. Decreasing the TPC Power Threshold value can result in lower transmit power levels of the radios of individual APs, decreasing the overall coverage of each AP, but also minimizing CCI. For the Typical RF profile, this is set to –70 dBm for the 5-GHz radio.

Table 35: Settings for the High Wireless RF Profile

Feature	Type	Description
Profile Name	Text field	HIGH
PROFILE TYPE > 2.4 GHz	On/off toggle	Enables or disables the 2.4-GHz band for the RF profile. Set to On.
PROFILE TYPE > 2.4 GHz > Parent Profile	Radio button	This is the parent profile from which this RF profile is derived. This field only applies when creating custom RF profiles, because custom RF profiles can be based on a preconfigured RF profile. For the High RF profile, this is set to High. Available options: • High: High client density RF profile. • Medium (Typical): Medium client density RF profile. • Low: Low client density RF profile. • Custom: Custom RF profile.
PROFILE TYPE > 2.4 GHz > DCA Channel	Multiple choice radio button	Selects the channels in which DCA operates in automatic mode within the 2.4-GHz band. Choices are channels 1 to 14. The default setting is channels 1, 6, and 11. This field is not visible in the 2.4-GHz band when editing one of the preconfigured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 2.4-GHz band. Note that it is generally not recommended to implement channels other than 1, 6, and 11 in the 2.4-GHz band.

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > Supported Data Rates	Single direction slider with multiple positions	Slider with multiple positions to indicate the range of data rates supported in the 2.4-GHz band. Rates are as follows from lowest to highest: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. For the High RF profile, this is set to rates of 9 Mbps and higher. The High RF profile is designed for wireless environments of high client density. In these environments, having wireless clients connecting to APs at lower speeds decreases the overall throughput of the wireless network. Sufficient AP density should be deployed such that the clients can connect and transmit at higher rates.
PROFILE TYPE > 2.4 GHz > Supported Data Rates > Enable 802.11b Data Rates	Check box	This check box works with the preceding slider. Checking the box enables the 802.11b data rates 1, 2, 5.5, 6, 9, and 11 Mbps on the slider. For the High RF deployment, this check box is unchecked.
PROFILE TYPE > 2.4 GHz > Mandatory Data Rates	Multiple choice radio button	This is used to select the data rates that the wireless client must support to be able to associate with the wireless network in the 2.4-GHz band. Choices are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. For the High RF profile, the only data rate that is mandatory is 12 Mbps.
PROFILE TYPE > 2.4 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	This slider determines the minimum and maximum power levels that TPC can configure on 2.4-GHz radios in APs associated with this RF profile. The full range of the slider is from –10 to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based on RSSI from neighboring APs. For the High RF profile, the sliders are set so that the range of power levels (7 to 30 dBm) is available to TPC. In environments of high client density like lecture halls, when the room is full, the amount of RF energy reaching the floor could be significantly attenuated due to the number of people in the room. TPC incrementally increases the transmit power of the APs within the room to account for the additional attenuation. However, TPC increases power gradually over time. Setting a higher TPC minimum power level ensures there is sufficient RF energy reaching the floor initially (when the lecture begins).
PROFILE TYPE > 2.4 GHz > TX Power Configuration > RX SOP	Drop-down menu	The RX-SOP determines the RF signal level at which the 2.4-GHz radio demodulates and decodes a wireless packet. Higher RX-SOP levels decrease the sensitivity of the 2.4-GHz radio to wireless clients. Wireless client traffic with lower RSSI values is not decoded by the AP. Because lower RSSI is often due to the wireless client being farther from the AP, this has the effect of decreasing the cell size (coverage) of the AP. This is beneficial for environments of high client density, where APs may be more densely deployed. For the High RF profile, this is set to Medium.

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and therefore the coverage behavior of the system. The TPC Power Threshold ranges from –80 to –50 dBm. Wireless deployments of high client density typically have more APs. Decreasing the TPC Power Threshold value can result in lower transmit power levels of the radios of individual APs, decreasing the overall coverage of each AP, but also minimizing CCI. For the High RF profile, this is set to –70 dBm for the 2.4-GHz radio.
PROFILE TYPE > 5 GHz	On/off toggle	Enables or disables the 5-GHz band for the RF profile. Set to On.
PROFILE TYPE > 5 GHz > Parent Profile	Radio button	This is the parent profile from which this RF profile is derived. This field only applies when creating custom RF profiles, because custom RF profiles can be based on a preconfigured RF profile. For the High RF profile, this is set to High. Available options: • High: High client density RF profile. • Medium (Typical): Medium client density RF profile. • Low: Low client density RF profile. • Custom: Custom RF profile.
PROFILE TYPE > 5 GHz > Channel Width	Drop-down menu	Selects the channel width for the 5-GHz band. Choices are 20, 40, 80, and 160 MHz or Best. Best allows DCA to select the optimal channel width for the environment. For the High RF profile, channel width is set to 20 MHz.
PROFILE TYPE > 5 GHz > DCA Channel	Multiple choice radio button	Selects the channels in which DCA operates in automatic mode within the 5-GHz band. Choices vary based on regulatory domain: UNII-1 channels 36 – 48, UNII-2 channels 52 – 144, and UNII-3 channels 149 – 165. This field is not visible in the 5-GHz band when editing one of the preconfigured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 5-GHz band.
PROFILE TYPE > 5GHz > Supported Data Rates	Single direction slider with multiple positions	Slider with multiple positions to indicate the range of data rates supported in the 5-GHz band. Rates are as follows from lowest to highest: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. For the High RF profile, this is set to rates of 12 Mbps and higher.
PROFILE TYPE > 5 GHz > Mandatory Data Rates	Multiple choice radio button	This is used to select the data rates that the wireless client must support to be able to associate with the wireless network in the 5-GHz band. Choices are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. For the High RF profile, the 12 and 24 Mbps data rates are mandatory.

Feature	Type	Description
PROFILE TYPE > 5 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	This slider determines the minimum and maximum power levels that TPC can configure on 5-GHz radios in APs associated with this RF profile. The full range of the slider is from –10 to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based on RSSI from neighboring APs. For the High RF profile, the sliders are set so that the range of power levels (7 to 30 dBm) is available to TPC. In environments of high client density like lecture halls, when the room is full, the amount of RF energy reaching the floor could be significantly attenuated due to the number of people in the room. TPC incrementally increases the transmit power of the APs within the room to account for the additional attenuation. However, TPC increases power gradually over time. Setting a higher TPC minimum power level ensures there is sufficient RF energy reaching the floor initially (when the lecture begins).
PROFILE TYPE > 5 GHz > TX Power Configuration > RX SOP	Drop-down menu	The RX-SOP determines the RF signal level at which the 5-GHz radio demodulates and decodes a wireless packet. Higher RX-SOP levels decrease the sensitivity of the 5-GHz radio to wireless clients. Wireless client traffic with lower RSSI values is not decoded by the AP. Because lower RSSI is often due to the wireless client being farther from the AP, this has the effect of decreasing the cell size (coverage) of the AP. This is beneficial for environments of high client density, where APs may be more densely deployed. For the High RF profile, this is set to Medium.
PROFILE TYPE > 5 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and therefore the coverage behavior of the system. The TPC Power Threshold ranges from –80 to –50 dBm. Wireless deployments of high client density typically have more APs. Decreasing the TPC Power Threshold value can result in lower transmit power levels of the radios of individual APs, decreasing the overall coverage of each AP, but also minimizing CCI. For the High RF profile, this is set to –65 dBm for the 5-GHz radio.

Glossary

AP

access point

Cisco ISE

Cisco Identity Services Engine

Cisco SDA

Cisco Software-Defined Access

CDP

Cisco Discovery Protocol

CWA

Central Web Authentication

DS

distribution system

FT

fast transition

HA

high availability

IBN

intent-based networking

L2

Layer 2

LWA

local web authentication

Microsoft AD

Microsoft active directory

PSK

preshared key

PSN

policy service node

RF

radio frequency

RSSI

received signal strength indication

RX-SOP

receiver start of packet detection threshold

SSID

service set identifier

SSO

stateful switchover

SVI

switched virtual interface

SWIM

software image management

TPC

transmit power control

VLAN

virtual local area network

WLAN

wireless local area network

WNM

wireless network management

WPA

Wi-Fi protected alliance

References

- *Deployment Guide for Cisco Catalyst 9800 Wireless Controller for Cloud on Amazon Web Services*
- *Cisco Aironet Active Sensor Deployment Guide*
- *Cisco Catalyst 9800 Series Configuration Best Practices*

For comments and suggestions about our guides, join the discussion on Cisco Community.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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