



The bridge to possible

Guide
Cisco public

Catalyst 9800 Non-Fabric Deployment using Cisco DNA Center

Solutions Adoption Prescriptive Reference-Design Guide

January 2021

Contents

Introduction	3
Define the wireless network	4
Design the wireless network	6
Deploy the wireless network	37
Operate the wireless network	79
Appendix A-New in this guide	91
Appendix B-Hardware and software used for validation	92
Appendix C-Glossary	92
Appendix D-Settings within each of the pre-configured RF profiles	93
About this guide	104

Introduction

About the Solution

This guide focuses on how to deploy a wireless local area network (WLAN) within a campus network, using Catalyst 9800 Series WLAN controllers (WLCs) with access points (APs) in centralized (local mode) operation, using Cisco DNA Center.

About This Guide

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

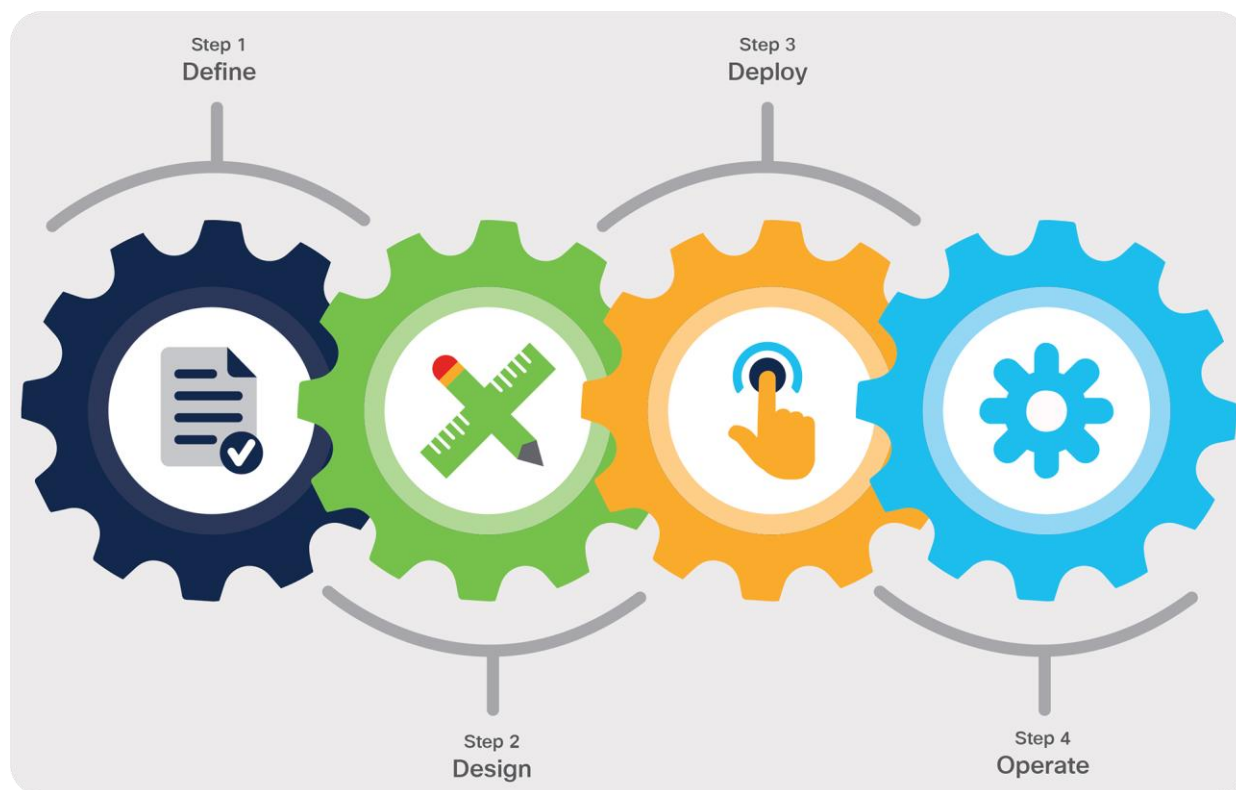


Figure 1.
Implementation flow

This document contains four major sections:

- The Define the wireless network section presents a high-level overview of the campus WLAN which will be designed and deployed through Cisco DNA Center. It consists of an enterprise high availability (HA) stateful switch-over (SSO) WLC pair, with APs operating in centralized (local) mode, along with a traditional guest anchor controller.

-
- The Design the wireless network section discusses the integration of Cisco DNA Center with Cisco Identity Services Engine (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.
 - The Deploy the wireless network section discusses discovery of the WLCs; managing the software images running on the WLCs; configuring HA SSO redundancy on the WLCs; provisioning the enterprise and guest WLCs within Cisco DNA Center; joining APs to the enterprise WLC HA SSO pair; provisioning the APs within Cisco DNA Center; and positioning the APs on the floor maps within Cisco DNA Center.
 - The Operate the wireless network section briefly discusses how Cisco DNA Assurance can be used to monitor and troubleshoot the WLAN deployment.

Define the wireless network

Audience

The audience for this document includes network design engineers and network operations personnel who wish to implement a Cisco WLAN within their campus networks using Cisco DNA Center.

Purpose of this document

This guide focuses on how to deploy a WLAN within a campus network using Cisco DNA Center. Within this design, a pair of Cisco Catalyst 9800-40 wireless LAN controllers (WLCs) in an HA SSO configuration functions as the enterprise WLC for access points (APs) located on multiple floors, within multiple buildings of the campus. All APs operate in centralized (local) mode for this design and deployment guide. Wireless guest access is provided through a separate Cisco Catalyst 9800-CL Cloud controller functioning as traditional guest WLC, anchored to the enterprise (foreign) WLC. The design and deployment of the WLAN is fully automated, utilizing intent-based networking (IBN) through Cisco DNA Center.

Solution overview

The following figure shows the high-level design for this deployment guide.

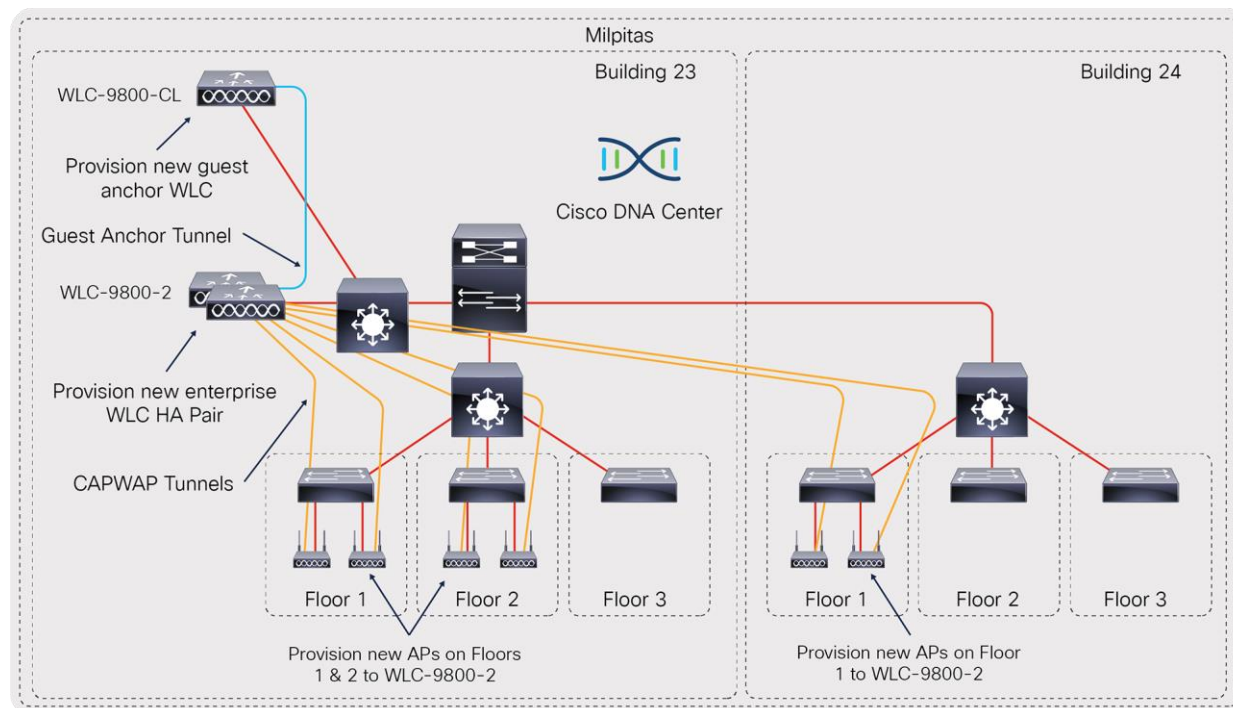


Figure 2.
High-level design

The specifics of the use case covered within this design and deployment guide are as follows:

- Site hierarchy consisting of a single area (**Milpitas**) with multiple buildings (**Buildings 23 & 24**), each with multiple floors (**Floors 1 - 3**).
- Non-Cisco SDA (non-fabric) centralized (local-mode) wireless deployment, in which all wireless traffic is backhauled to the WLC.
- Single enterprise and guest SSIDs.
- Single pair of Catalyst 9800-40 enterprise WLCs in an HA SSO configuration.
- Guest wireless access through a dedicated Catalyst 9800-CL guest WLC, auto-anchored to the enterprise HA SSO WLC pair

Technical Note: The connectivity of the guest anchor controller is shown as being on the same switch as the enterprise WLC in the figure above. This is done simply to demonstrate the ability of Cisco DNA Center to provision both the enterprise and guest WLCs in a foreign / anchor controller relationship and does not represent best practices for deployment of a guest anchor controller. In production environments, the guest anchor controller is typically connected to a DMZ segment off of a firewall, to isolate 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 WLC and the guest anchor WLC.

Cisco DNA Center is designed for intent-based networking (IBN). It provides a level of abstraction from the device-level user interface - regardless of whether the device is a Catalyst 9800 Series or Cisco AireOS WLC. The advantage of this abstraction is that a single user interface within Cisco DNA Center can be used to

configure either Cisco Catalyst 9800 Series WLCs, or AireOS WLCs, without having to learn the specific syntax of commands on either platform.

Technical Note: The Cisco DNA Center web-based GUI does not provide access to all features which can be configured by the device-level user interface of either Cisco Catalyst 9800 Series or Cisco AireOS WLCs. The specific WLC features that can be configured via Cisco DNA Center are discussed within this document.

WLCs must be assigned to sites during the Cisco DNA Center provisioning process. For this deployment guide a Catalyst 9800-40 WLC HA SSO pair (**WLC-9800-2**) will be assigned to **Building 23** within the **Milpitas** area. There can be only one primary enterprise (non-guest) WLC for APs on a floor at a given time. This means that only one enterprise WLC can be provisioned per floor within Cisco DNA Center. For this deployment guide APs on **Floor 1** and **Floor 2** within **Building 23**, and APs on **Floor 1** within **Building 24**, will be provisioned to **WLC-9800-2** through Cisco DNA Center.

Design the wireless network

The processes for designing the wireless network are as follows:

- Integrate Cisco Identity Services Engine (ISE) with Cisco DNA Center
- Configure the site hierarchy within Cisco DNA Center and import floor maps
- Configure network services necessary for network operation
- Configure wireless settings for the WLAN deployment

Process: Integrate Cisco Identity Services Engine (ISE) with Cisco DNA Center

Integration of Cisco ISE and Cisco DNA Center enables sharing of information between the two platforms, including device and group information. Specific to this design and deployment guide, integration of Cisco DNA Center with Cisco ISE allows you to create a guest portal within Cisco ISE through a workflow within Cisco DNA Center. The guest portal is created when the guest wireless network is defined within a wireless profile in Cisco DNA Center. This is discussed within the Configure Wireless Settings for the WLAN Deployment process within this section of the guide.

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

- Configure Cisco ISE as an authentication and policy server to Cisco DNA Center
- Permit pxGrid connectivity from Cisco DNA Center into Cisco ISE

Procedure 1: Configure Cisco ISE as an authentication and policy server

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

For example: <https://<Cisco DNA Center IPaddr or FQDN>>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

2. In the top right corner of any screen within Cisco DNA Center click on the gear icon. From the drop-down menu select **System Settings**.

This will take you to the **System 360** tab within the **System Settings** screen. An example is shown in the following figure.

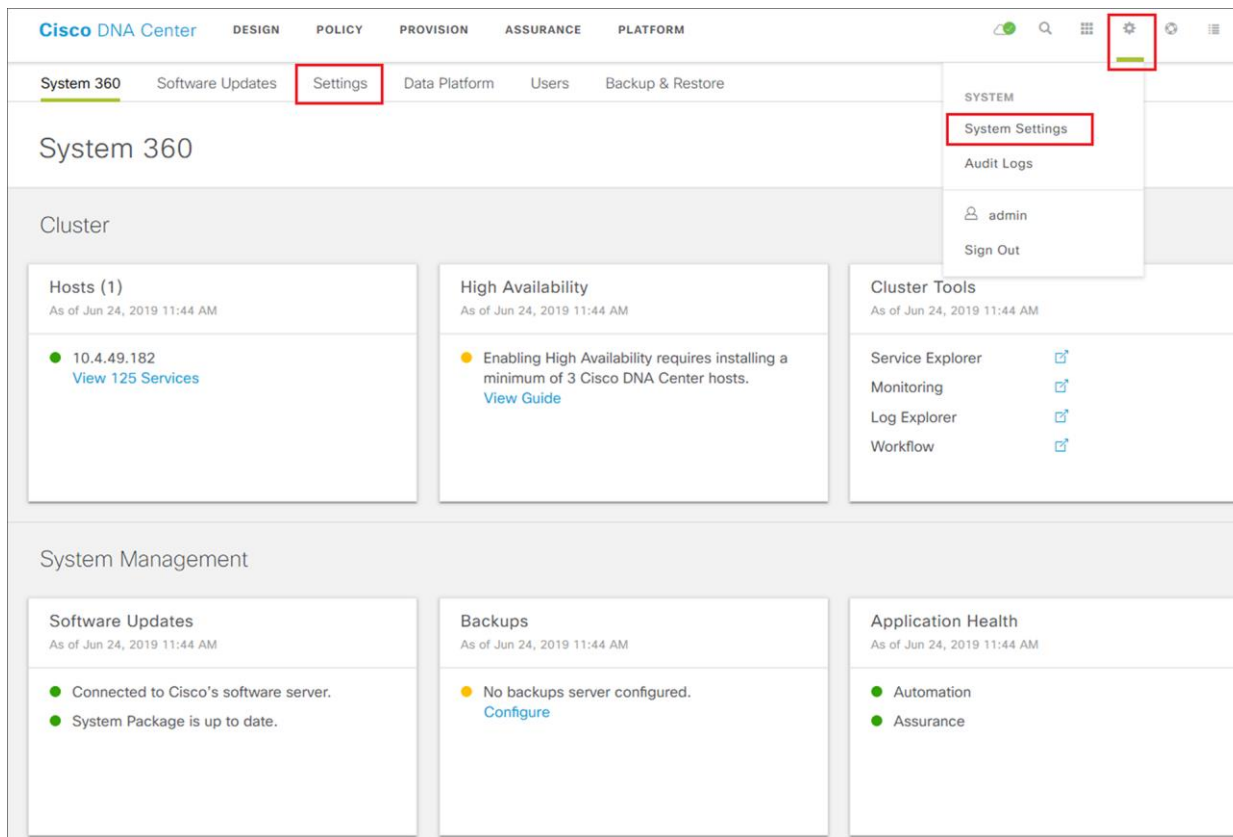


Figure 3.
System Settings screen - System 360 tab

3. Click on the **Settings** tab.
4. In the navigation panel on the left side of the screen, select **Authentication and Policy Servers**.

This will bring up the **Authentication and Policy Servers** dashboard.

5. Click the **Add** button to add an ISE server
6. Fill in the information within the **Add AAA/ISE server** panel which appears.

The following table discusses the fields within the **Add AAA/ISE server** panel.

Table 1. Add AAA/ISE server panel fields

Field	Settings	Description
Server IP Address	Text Field	The IP address of the AAA/ISE server
Shared Secret	Text Field	This is the shared secret used by network devices for communicating with the AAA/ISE server. This is also referred to the PAC key within IOS XE device configuration.
Cisco ISE Server	Toggle Switch	Enabled when the AAA server is a Cisco ISE server. Note that although there can be multiple AAA servers, there can only be one ISE server (high-availability standalone ISE deployment or distributed ISE deployment) defined to Cisco DNA Center.

Field	Settings	Description
Username	Text Field	This is the username of the default super admin account that you created during the Cisco ISE installation.
Password	Text Field	This is the password of the default super admin account that you created during the Cisco ISE installation.
FQDN	Text Field	This is the fully-qualified domain name of the Cisco ISE server.
Subscriber Name	Text Field	This is client name which the Cisco DNA Center server will be known by to the pxGrid service within Cisco ISE.
SSH Key	Check Box	Optional SSH key for authentication between Cisco DNA Center and Cisco ISE.
Virtual IP Address	Text Field	One or more Policy Services Nodes (PSN) may be behind a single load balancer. In those cases, 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) used. The choices are as follows: <ul style="list-style-type: none"> • RADIUS - This is the default setting, using 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.
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.

Table 2. Add AAA/ISE server panel settings

Field	Value
Server IP Address	10.4.48.18
Shared Secret	****
Cisco ISE Server	On
Username	admin
Password	****
FQDN	ISE23.cisco.local
Subscriber Name	dnacmgmt
SSH Key	None (empty)

Field	Value
Virtual IP Address	None (empty)
Advanced Settings > Protocol	RADIUS
Advanced Settings > Authentication Port	1812
Advanced Settings > Accounting Port	1813
Advanced Settings > Port	Not applicable - TACACS not selected
Retries	3
Timeout (seconds)	4

7. Click the **Apply** button to create the Cisco ISE server within Cisco DNA Center.

This will take you back to the **Authentication and Policy Servers** dashboard. The new Cisco ISE server should appear with a **Status** of **Active**. You can edit the server if you need to change or correct any settings by selecting it and clicking on **Edit**. An example is shown in the following figure.

The screenshot displays the Cisco DNA Center interface. The top navigation bar includes 'Cisco DNA Center' and tabs for 'DESIGN', 'POLICY', 'PROVISION', 'ASSURANCE', and 'PLATFORM'. Below this, a secondary navigation bar shows 'System 360', 'Software Updates', 'Settings' (selected), 'Data Platform', 'Users', and 'Backup & Restore'. The left sidebar contains a search bar and a list of settings categories, with 'Authentication and Policy Servers' selected. The main content area is titled 'Authentication and Policy Servers' and includes a sub-header 'Use this page to specify the servers that authenticate Cisco DNA Center users. ISE servers can also supply policy and user information.' Below this is a table with columns 'IP Address', 'Protocol', and 'Type'. A single entry is shown: IP Address '10.4.48.18', Protocol 'RADIUS', and Type 'ISE'. To the right of the table are 'Edit' and 'Delete' buttons. An 'Edit AAA/ISE server' modal is open on the right, showing fields for 'Server IP Address*' (10.4.48.18), 'Shared Secret*' (masked), 'Cisco ISE server' (checked), 'Username*' (admin), 'Password*' (masked), 'FQDN*' (ISE23.cisco.local), 'Subscriber Name*' (dnacmgmt), 'SSH Key', and 'Virtual IP Address(es)'. At the bottom of the modal, there are checkboxes for 'RADIUS' (checked) and 'TACACS', and buttons for 'Cancel' and 'Apply'.

Figure 4.
Editing an existing ISE server

Procedure 2: Permit pxGrid connectivity from Cisco DNA Center into Cisco ISE

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

For example: <https://<CiscoISEIPAddrorFQDN>/admin>.

2. Navigate to **Administration > PxGrid Services > All Clients**.

This will take you to a screen similar to the following.

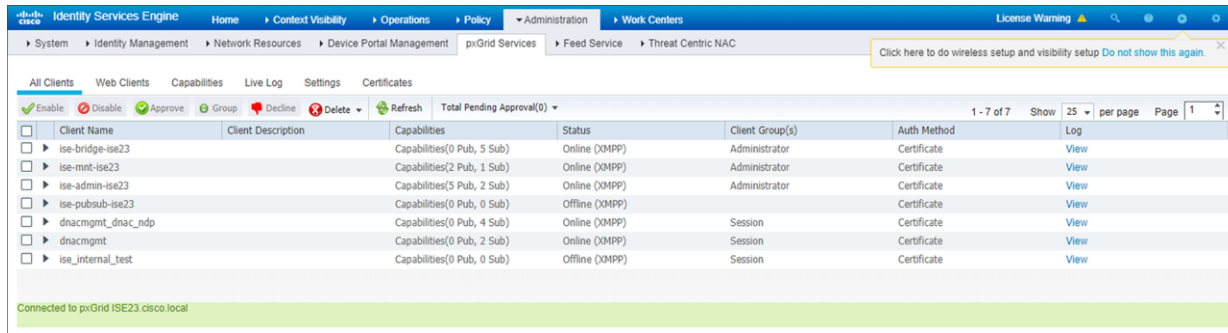


Figure 5.
ISE PxGrid Services screen

3. Locate and select the **Client Name** in the list based upon the subscriber name you configured when adding the Cisco ISE server to Cisco DNA Center in the previous procedure.

For this design and deployment guide the **Client Name** is **dnacmgmt**.

4. Click the **✓ Approve** button to activate the new client.

The status of the client should transition to **Online (XMPP)**.

Technical Note: Alternatively, you could change the PxGrid settings to automatically approve new certificate-based accounts through the **Settings** tab shown in the figure above.

5. Click on the **>** next to the client name (**dnacmgmt**) to display the client capabilities.

An example is shown in the figure below.

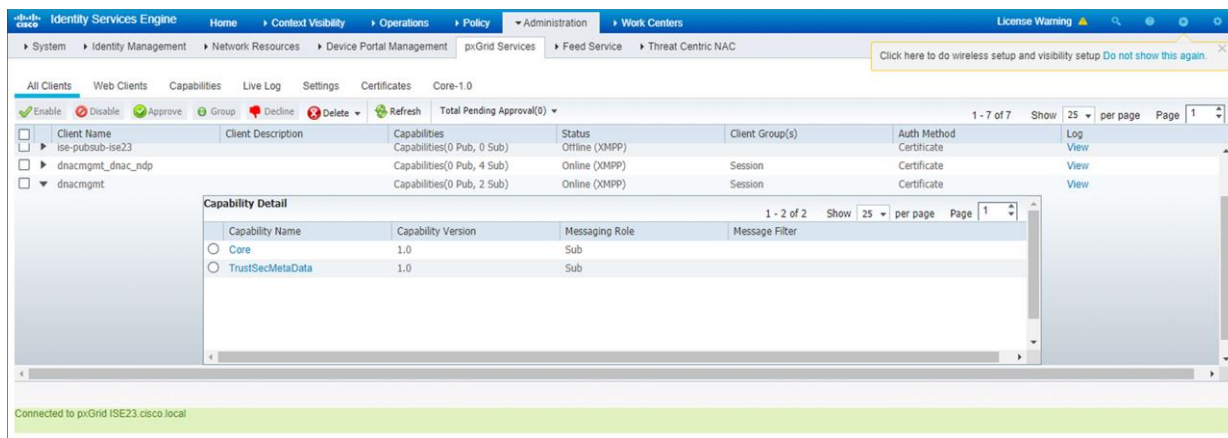


Figure 6.
PxGrid client capabilities

Cisco ISE should now be integrated with Cisco DNA Center through PxGrid.

Process: Configure the site hierarchy within Cisco DNA Center and import floor maps

Configuring the site hierarchy involves defining the network sites for the deployment, and their hierarchical relationships. Network sites consist of areas, buildings, and floors. Their hierarchical relationship is important because child sites automatically inherit certain attributes from parent sites. However, these attributes may be overridden within the child site.

The following table summarizes the site hierarchy for this design and deployment guide. A single area (**Milpitas**) with multiple buildings (**Buildings 23 & 24**), each with multiple floors (**Floors 1 - 3**) is provisioned.

Table 3. Design & deployment guide site hierarchy

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, 95
Floor 1	Floor	Building 23	Dimensions: 200 ft. x 274 ft. x 10 ft. APs on this floor will be provisioned onto the Catalyst 9800 WLC HA pair within the use case.
Floor 2	Floor	Building 23	Dimensions: 200 ft. x 274 ft. x 10 ft. APs on this floor will be provisioned onto the Catalyst 9800 WLC HA pair within the use case.
Floor 3	Floor	Building 23	Dimensions: 200 ft. x 274 ft. x 10 ft. No APs on the floor this deployment guide.
Floor 1	Floor	Building 24	Dimensions: 200 ft. x 250 ft. x 10 ft. APs on this floor will be provisioned onto the Catalyst 9800 WLC HA pair within the use case.
Floor 2	Floor	Building 24	Dimensions: 200 ft. x 250 ft. x 10 ft. No APs on the floor this deployment guide.
Floor 3	Floor	Building 24	Dimensions: 200 ft. x 250 ft. x 10 ft. No APs on the floor this deployment guide.

The following are the procedures for configuring the site hierarchy for this design and deployment guide:

- Create an area.
- Create buildings within the area.
- Create floors within each building and import floor maps

Procedure 1: Create an area

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

For example: <https://<Cisco DNA Center IPAddr or FQDN>>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

2. From the main Cisco DNA Center dashboard, navigate to **Design > Network Hierarchy**.

This will take you to the **Network Hierarchy** dashboard. An example is shown in the following figure.

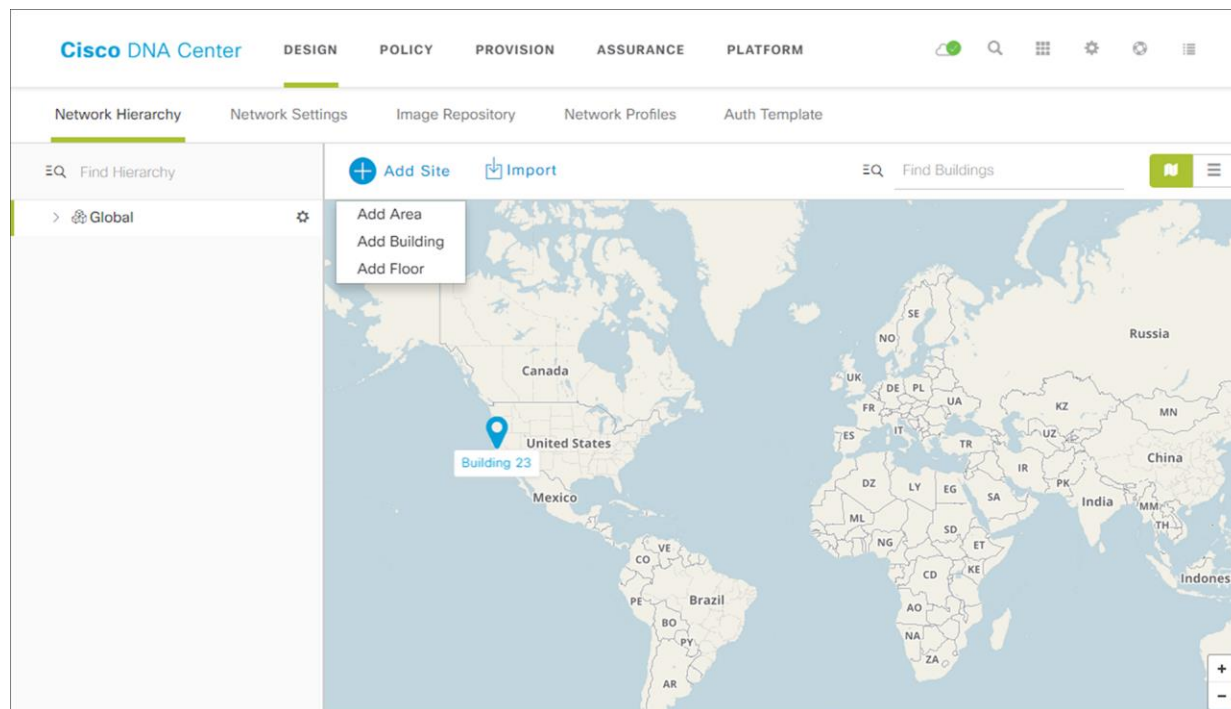


Figure 7.
Network Hierarchy dashboard

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

3. Click the **Add Site** button. From the drop-down menu select **Add Area**, as shown in the figure above.

The **Add Area** pop-up window will appear. An example is shown in the following figure.

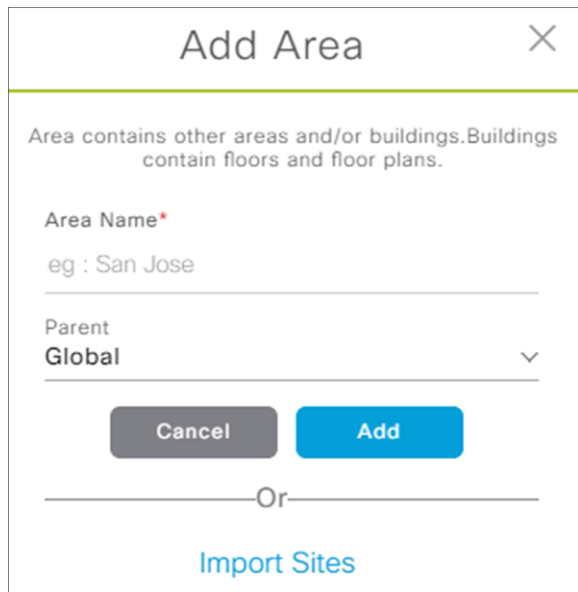
The image shows a pop-up window titled "Add Area" with a close button (X) in the top right corner. Below the title bar, there is a descriptive text: "Area contains other areas and/or buildings. Buildings contain floors and floor plans." This is followed by a text input field labeled "Area Name*" with a red asterisk indicating it is required. Below the input field is a hint text "eg : San Jose". Underneath is a dropdown menu labeled "Parent" with "Global" selected and a downward arrow. At the bottom of the form are two buttons: "Cancel" (grey) and "Add" (blue). Below these buttons is a horizontal line with the word "Or" in the center, and below that is a blue link labeled "Import Sites".

Figure 8.
Add Area pop-up window

4. In the **Add Area** pop-up window, type in the name of the area in the text field under **Area Name**.

For this deployment guide a single area named **Milpitas** is configured.

5. Leave the Parent set at the default of **Global**.
6. Click the **Add** button to add the area.
7. In the navigation panel on the left side of the **Network Hierarchy** dashboard, click the > next to **Global** to expand the hierarchy.

The new area, **Milpitas**, should now appear.

Procedure 2: Create buildings within the area

1. From the **Network Hierarchy** dashboard click the **Add Site** button again.
2. From the drop-down menu select **Add Building**.

The **Add Building** pop-up window will appear. An example is shown in the following figure.

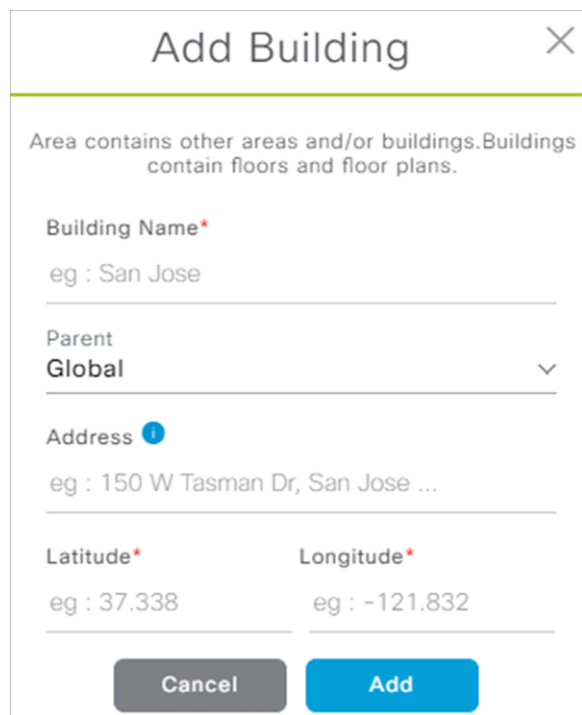


Figure 9.
Add Building pop-up window

3. In the **Add Building** pop-up window, type in the name of the building in the text field under **Building Name**.

For this deployment guide the first building is named **Building 23**.

4. Change the Parent to **Milpitas | Global/**.
5. Start typing in the address of the building in the text field under **Address**, then select it from the drop-down menu which automatically appears. Alternatively, you can type in the GPS coordinates of the building in the text fields under **Latitude** and **Longitude**.

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

6. Click the **Add** button to add the building.
7. In the navigation panel on the left side of the **Network Hierarchy** dashboard, click the > next to **Milpitas** to expand the hierarchy.

Building 23 should now appear.

8. Repeat **Steps 1 - 7** to add the second building, **Building 24**, to the **Milpitas** area.

Procedure 3: Create floors within the buildings

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

1. From the **Network Hierarchy** dashboard click the **Add Site** button again. From the drop-down menu select **Add Floor**.

The **Add Floor** pop-up window will appear. An example is shown in the following figure.

The screenshot shows the 'Add Floor' pop-up window. It has a title bar with the text 'Add Floor' and a close button (X). The form inside includes the following fields and options:

- Floor Name***: A text input field containing 'Floor 1'.
- Site**: A dropdown menu showing 'Milpitas | Global/'.
- Building***: A dropdown menu showing 'Building 23 | Global/Milpitas/'.
- Type (RF Model)**: A dropdown menu showing 'Indoor High Ceiling'.
- Floor Image**: A section with a drag-and-drop area containing the text 'Drag floor plan here or Upload file'. Below this, it says '(Supported formats DXF, DWG, JPG, GIF, PNG)'.
- Dimensions**: Three radio buttons for 'Width (ft)', 'Length (ft)', and 'Height (ft)'. The 'Width (ft)' radio button is selected. Below these are input fields with the values '274', '200', and '10' respectively.
- Buttons**: 'Cancel' and 'Add' buttons at the bottom.

Figure 10.
Add Floor pop-up window

2. In the **Add Floor** pop-up window, type in the name of the first floor (**Floor 1**) in the text field below **Floor Name**.
3. Change the **Site** to **Milpitas | Global/**.
4. Change the **Building** to **Building 23 | Global/Milpitas/**

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 which you have exported from Cisco Prime Infrastructure, you should make sure the site hierarchy you have configured in Cisco DNA Center is the same as what you have configured in Cisco Prime Infrastructure. For this deployment guide the floor plan archive was exported from Cisco Prime Infrastructure version 3.5.

5. Drag and drop a floor plan file for **Floor 1** from your desktop to the pop-up window. Alternatively, you can click the **Upload** file button, navigate to the floor plan file and upload it.
6. Click the **Width (ft)** radio button and type in the width of the floor in feet.
7. Click the **Length (ft)** radio button and type in the length of the floor in feet.
8. Click the **Height (ft)** radio button and type in the ceiling height in feet.

This is necessary to scale the floor plan correctly for the positioning of APs and for wireless coverage (heatmaps). For this deployment guide the dimensions of all of the floors in **Building 23** are **200 ft. x 275 ft. x 10 ft.**

9. Click the **Add** button to add the floor.
10. In the navigation panel on the left side of the **Network Hierarchy** dashboard, click the > next to **Building 23** to expand the hierarchy.

Floor 1 should now appear.

11. Repeats **Steps 1 - 10** to add **Floors 2 & 3** to **Building 23**.
12. Repeats Steps 1 - 11 to add **Floors 1 - 3** to **Building 24**.

Process: Configure network services necessary for network operation

In this process, you will configure AAA, DHCP, DNS, syslog, and SNMP services that align to the site hierarchy in Cisco DNA Center. If the services use the same servers across the entire site hierarchy, you can configure them globally. The inheritance properties of the site hierarchy make global settings available to all sites. Differences for individual sites can then be applied on a site-by-site basis. This design and deployment guide shows the network services created globally.

1. Within Cisco DNA Center, navigate to **Design > Network Settings > Network**.

This will take you to the screen where you can add or configure various network services. An example is shown in the following figure.

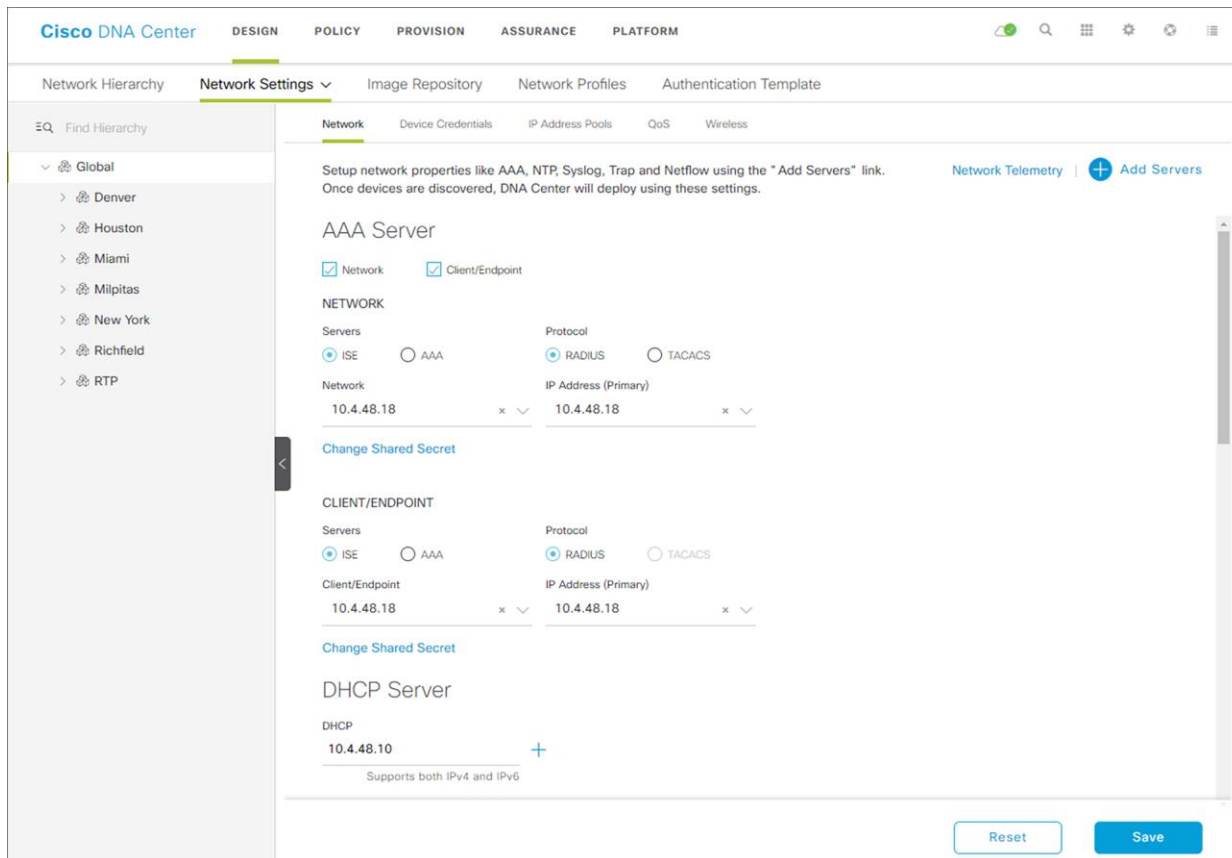


Figure 11.
Adding network services

2. Select **Global** in the navigation panel on the left side of the screen.
3. Click on the + **Add Servers** button.
4. From the **Add Servers** popup screen check the boxes next to **AAA** and **NTP**, and click the **OK** button.

This will close the **Add Servers** popup and add entries for a AAA server and an NTP server to the screen. This design and deployment guide does not require the deployment of NetFlow collectors. Therefore, **NetFlow Collectors** is not checked in the **Add Servers** popup screen.

5. Locate the **AAA Servers** section and fill in the necessary information.

This design and deployment guide uses Cisco ISE as the AAA server, using the RADIUS protocol, for both network devices and for wireless clients. For this guide, the following information was entered for the **AAA Servers** section.

Table 4. AAA server fields

Field	Value
Network	Checked
Client/Endpoint	Checked

Field	Value
Network > Servers	ISE
Network > Protocol	RADIUS
Network > Network	10.4.48.18
Network > IP Address (Primary)	10.4.48.18
Network > Shared Secret	*****
Client/Endpoint > Servers	ISE
Client/Endpoint > Protocol	RADIUS
Client/Endpoint > Network	10.4.48.18
Client/Endpoint > IP Address (Primary)	10.4.48.18
Client/Endpoint > Shared Secret	*****

6. Locate the **DHCP Server** section and fill in the necessary information.

This design and deployment guide uses a single Microsoft Active Directory (AD) server functioning as both the DNS and DHCP servers for the network. The following information was entered for the DHCP Server section.

Table 5. DHCP server fields

Field	Value
DHCP	10.4.48.10

7. Locate the **DNS Server** section and fill out the necessary information.

Since the network for this design and deployment guide was a lab network, a single DNS domain, **cisco.local**, was configured. The following information was entered for the DHCP Server section.

Table 6. DNS server fields

Field	Value
Domain Name	cisco.local
Primary	10.4.48.10

8. Locate the **Syslog Servers** section and fill out the necessary information.

Table 7. Syslog server fields

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

This design and deployment guide uses Cisco DNA Center as the syslog server. This setting is necessary for syslog information to be sent to Cisco DNA Center for Cisco DNA Analytics although Cisco DNA Analytics is not covered within this design and deployment guide.

9. Locate the **SNMP Servers** section and fill out the necessary information.

Table 8. SNMP server fields

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

This design and deployment guide uses Cisco DNA Center as the SNMP server. This setting necessary for SNMP trap information to be sent to Cisco DNA Center for Cisco DNA Analytics – although Cisco DNA Analytics is not covered within this design and deployment guide.

10. Locate the **NTP Servers** section and fill out the necessary information.

Table 9. NTP server fields

Field	Value
IP Address	10.4.48.17

This design and deployment guide uses a single internal NTP server, since this is a lab network. 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.

11. Locate the **Time Zone** section and from the drop-down menu select the correct time zone.

Table 10. Time zone configuration

Field	Value
Time Zone	US/Pacific (PDT)

This design and deployment guide uses a single time zone, since this is a lab network. For production networks, each site within the site hierarchy would reflect the actual time zone of the location.

12. Locate the **Message of the Day** section and check the box next to **Do not overwrite the existing motd banner on the device**.

The message of the day (motd) setting controls the message displayed when logging into the network device. This setting is not relevant to this design and deployment guide. Therefore, the existing motd banner is not modified by Cisco DNA Center for this guide.

13. When you have filled in all of the sections, click the **Save** button to save the changes to the network services.

Process: Configure wireless settings for the WLAN deployment

Configuring wireless settings involves creating the following within Cisco DNA Center:

- Wireless interfaces - These are the Ethernet interfaces (VLANs) for terminating wireless traffic.
- Enterprise wireless networks - These are the non-guest WLANs / SSIDs for the deployment.
- Guest wireless networks - These are the guest WLANs / SSIDs for the deployment.
- Wireless radio frequency (RF) profiles - These are the RF profiles for the deployment.
- Wireless sensor settings - Wireless sensors provide the ability to run diagnostic tests on the WLAN as well as perform packet captures. Wireless sensors are not discussed within this design and deployment guide.
- CMX servers - Integration with CMX servers allows the location of wireless clients to be displayed on floor maps. Integration with CMX servers is not discussed within this design and deployment guide.
- Native VLAN - The native VLAN configuration is specific to FlexConnect AP deployments. Since the wireless network discussed within this deployment guide assumes APs in centralized (local-mode) operation, no discussion of FlexConnect is included.

Each of these is discussed in a separate procedure below.

Procedure 1: Configuring wireless interfaces

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

Table 11. Wireless interfaces

Name	VLAN	Usage
employee	160	Employee voice & data VLAN
guest-dmz	168	Guest data VLAN

The following are the steps for configuring wireless interfaces within Cisco DNA Center.

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

For example: <https://<Cisco DNA Center IPaddr or FQDN>>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

2. From the main Cisco DNA Center dashboard navigate to **Design > Network Settings > Wireless**.

This will take you to the **Wireless Network Settings** dashboard. An example is shown in the following figure.

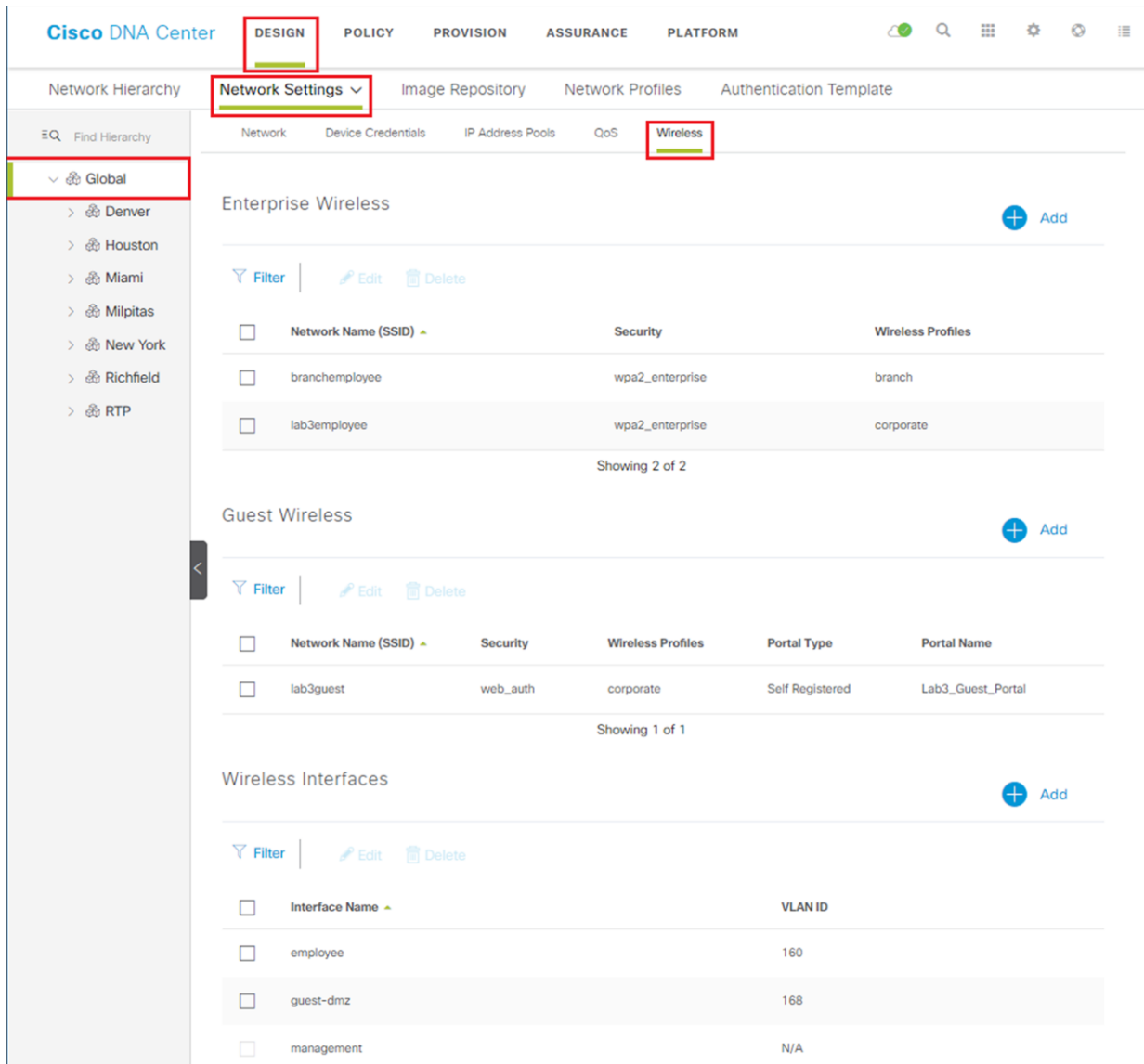


Figure 12.
Wireless network settings dashboard

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. Wireless interfaces must be defined at the **Global** level of the site hierarchy.

3. Click the **Add** button to the right of **Wireless Interfaces**.

This will bring up the **New Wireless Interface** side panel. An example is shown in the following figure.

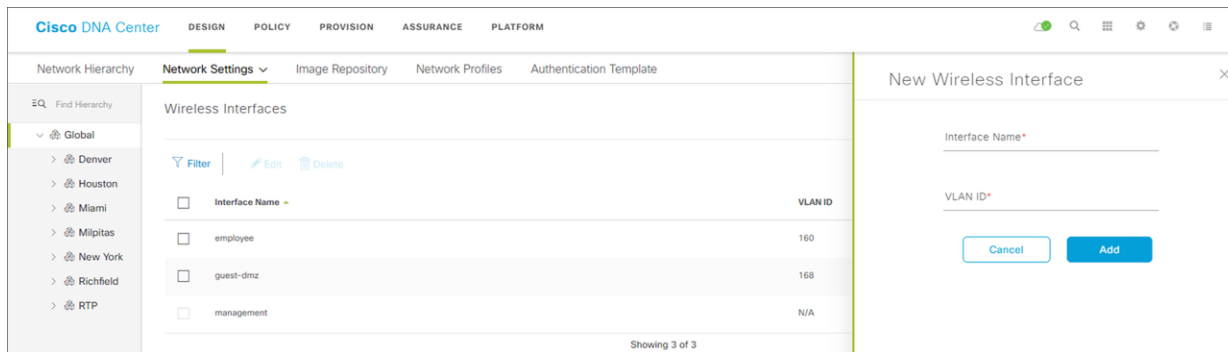


Figure 13.
New Wireless Interface side panel

4. Fill in the **Interface Name** and **VLAN ID** for the wireless interface corresponding to the enterprise VLAN (**employee**) and click the **Add** button.
5. Repeat the same 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 above.

Procedure 2: Configure enterprise wireless networks (SSIDs)

Enterprise wireless networks are the non-guest WLANs / SSIDs which will be available for broadcast across the deployment. They must be defined at the Global level of the site hierarchy. Once defined, enterprise 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 enterprise WLAN / SSID named **lab3employee** is provisioned. The following are the steps for configuring the enterprise wireless network within Cisco DNA Center.

1. From the **Wireless Network Settings** dashboard, click the **Add** button to the right of **Enterprise Wireless**.

This will bring up a screen displaying the first step in the **Create an Enterprise Wireless Network** workflow. An example is shown in the following figure.

Figure 14.
Create an Enterprise Wireless Network workflow step 1 create the SSID

The following table lists and explains the features which can be configured for enterprise wireless networks 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.
BROADCAST SSID:	On/Off Toggle	Determines whether the SSID will be broadcast in wireless beacons and probe responses.

Feature	Type	Description
WIRELESS OPTION	Radio Button	<p>Determines in which RF bands the SSID will be broadcast. The choices are as follows:</p> <ul style="list-style-type: none"> • Dual band operation (2.4GHz and 5GHz) • Dual band 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
LEVEL OF SECURITY	Radio Button	<p>Determines the Layer 2 (L2) security settings for the WLAN. The choices are as follows:</p> <ul style="list-style-type: none"> • WPA2 Enterprise This is WPA2 security with 802.1X authentication key management. • WPA2 Personal This is WPA2 security with a pre-shared key (PSK) • Open This is an open SSID, with no authentication
TYPE OF ENTERPRISE NETWORK	Radio Button	<p>For Catalyst 9800 Series WLCs, 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 WLC in centralized (local mode) designs.</p> <p>For AireOS WLCs, this setting applies a QoS profile to the WLAN / SSID. Application Visibility is enabled on the WLAN / SSID, but no AVC profile is applied.</p> <p>The radio button choices are as follows:</p> <ul style="list-style-type: none"> • Voice and Data - This corresponds to the Cisco AireOS Platinum (voice) QoS profile. With this QoS profile the maximum DSCP marking within the CAPWAP header is Voice (EF). • Data Only - This corresponds to the Cisco AireOS Silver (best effort) QoS profile. With this QoS profile, the maximum DSCP marking with the CAPWAP header is Best Effort (default).
Fastlane	Check Box	<p>This box can only be checked when the Type of Enterprise Network has been selected as Voice and Data.</p> <p>For Catalyst 9800 Series WLCs, 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. Note however, that no precious metals QoS SSID policy is applied to the WLAN / SSID when the Fastlane check box is selected.</p> <p>For AireOS WLCs, 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. The Fastlane EDCA profile is selected for both the 5 GHz and 2.4 GHz bands.</p>

Feature	Type	Description
Advanced Settings - FAST TRANSITION (802.11r)	Radio Button & Check Box	<p>Additional L2 security settings for the WLAN which controls 802.11r Fast Transition (FT). The radio button choices are as follows:</p> <ul style="list-style-type: none"> • Adaptive - This setting allows devices which 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 <p>Over the DS - Checkbox which 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 WLC. The default setting is enabled.</p>
Advanced Settings - Mac Filtering	Check Box	This is an additional L2 security settings that applies MAC address filtering for the WLAN.
Advanced Settings - Session timeout	Check Box & 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 & 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).
Advanced Settings - MFP CLIENT PROTECTION	Radio Button	<p>Additional security setting which controls the use of 802.11w Protected Management Frames for the WLAN. The radio button choices are as follows:</p> <ul style="list-style-type: none"> • Optional - This setting allows wireless stations which support 802.11w Protected Management Frames to use them, as well other wireless stations which do not support PMFs to co-exist 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) which the client is associated.
Advanced Settings 11v BSS TRANSITION SUPPORT	Multiple Check Boxes & Integer Field	<p>Additional settings for support of 802.11v Wireless Network Management (WNM) for the WLAN. The settings are as follows:</p> <ul style="list-style-type: none"> • BSS Max Idle Service - Checkbox which enables the maximum idle service for the WLAN. Allows APs to send the timeout value to the wireless client within association and re-association response frames. The default setting is enabled. • Client User Idle Timeout - Checkbox with bounded integer field which specifies maximum amount of time an AP will keep 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 - Checkbox which allows the client to request from the AP that multicast streams to be sent as unicast streams to the client. By default, this setting is enabled.

2. Fill in the necessary information and click the **Next** button at the bottom of the screen.

The following are the settings for the enterprise wireless network configured for this deployment guide.

Table 13. Enterprise wireless network settings

Feature	Settings
Wireless Network Name(SSID)	lab3employee
Broadcast SSID	On
Wireless Option	Dual-band operation (2.4 GHz and 5 GHz)
Level of Security	WPA2
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, 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

This should take you to the next screen in the workflow; where you can attach the enterprise wireless network to an existing wireless profile or create a new wireless profile and attach the Enterprise wireless network to it. An example of the screen is shown in the figure below.

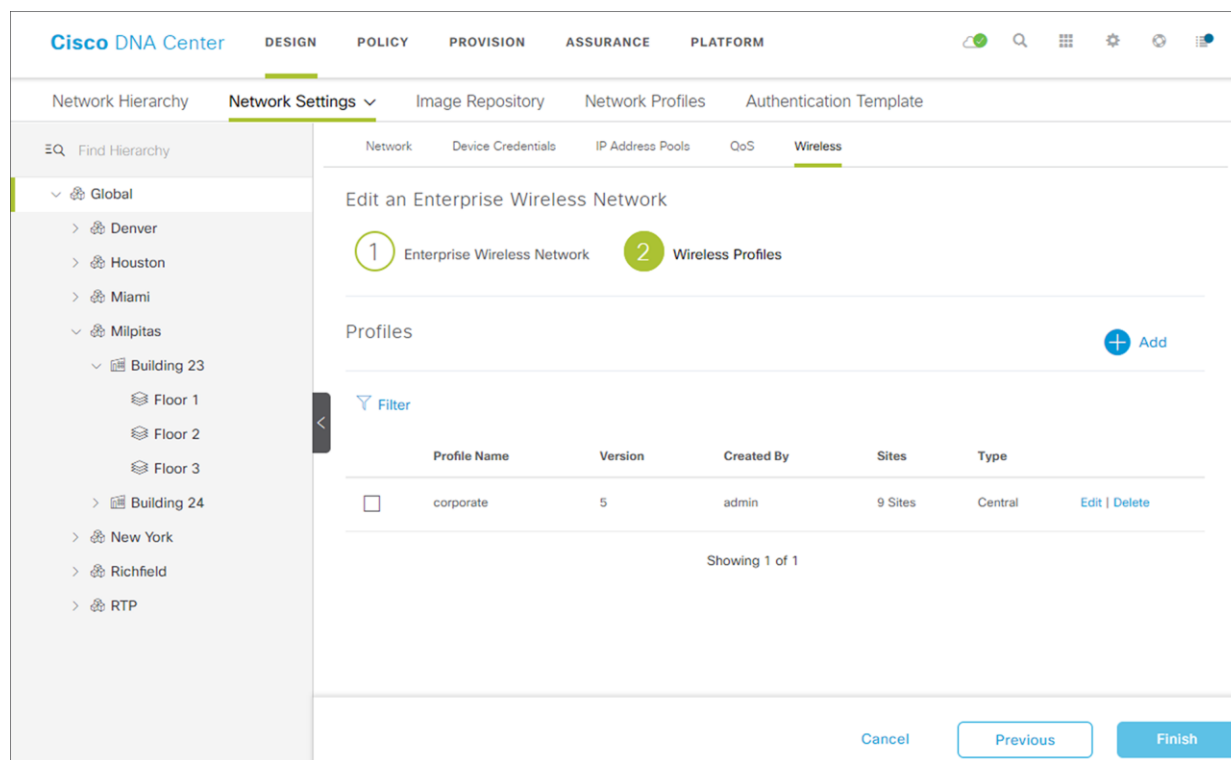


Figure 15.
Create an Enterprise Wireless Network workflow – step 2 wireless profiles

3. Click the **+ Add** button to add a new wireless profile.

This will bring up the **Create a Wireless Profile** side panel, as shown in the figure below.

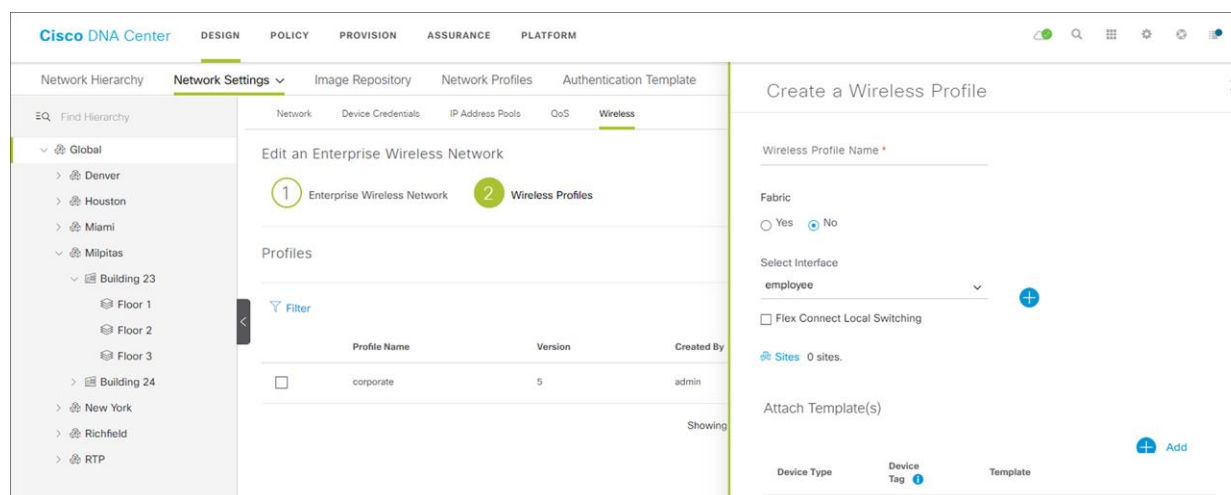


Figure 16.
Create a Wireless Profile side panel

4. Type in the name of the new wireless profile in the text field under **Wireless Profile Name**.

For this deployment guide, a wireless profile named **corporate** was created.

5. Under **Fabric**, select **No** from the radio button options.

This deployment guide only discusses non-SDA wireless deployments using Cisco DNA Center. Selecting No will automatically cause the **Select Interface** field to appear.

6. From the drop-down menu under **Select Interface** select **employee**.

This will terminate the **lab3Employee** SSID onto the **employee** VLAN (**VLAN 160**) created in the previous procedure.

7. Leave the box next to **Flex Connect Local Switching** unchecked.

This design guide only discusses centralized (local mode) WLAN deployments.

8. Click the **Sites** button to bring up another panel displaying the site hierarchy.
9. Under **Global** click the > to display up the **Milpitas** area.
10. Select the **Milpitas** area. This should automatically check the child site locations - **Building 23, Floors 1 - 3** and **Building 24, Floors 1 - 3**, as shown in the figure above.
11. Click **OK** to close the site hierarchy side panel.

CLI-based templates can be added to the enterprise wireless network configuration by clicking the **+ Add** button under **Attach Template(s)**. These templates must already be defined within the **Template Editor** dashboard of Cisco DNA Center. This design & deployment guide will not discuss the addition of templates, since it does require knowledge of the CLI syntax of the specific WLC platform to implement. However, wireless features not supported by the web-based graphical user interface of Cisco DNA Center may be added through templates.

12. Click the **Add** button at the bottom of the **Create a Wireless Profile** side panel to create the new **corporate** wireless profile.

This assigns the wireless profile named **corporate** to the **Milpitas** area. Since the wireless profile contains the **lab3employee** SSID, this also ensures that when WLCs and APs are assigned to the **Milpitas** area, the APs will broadcast the **lab3employee** SSID.

13. Click the **Finish** button to add the **lab3employee** enterprise wireless network.

When you are completed, the new enterprise wireless network should appear in the **Wireless Network Settings** dashboard, as shown in the figure above.

Procedure 3: Configure guest wireless networks (SSIDs)

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 **lab3guest** is provisioned. The following are the steps for configuring guest wireless networks within Cisco DNA Center.

1. From the **Wireless Network Settings** dashboard, click the **Add** button to the right of **Guest Wireless**.

This will bring up the **Create a Guest Wireless Network** screen. An example is shown in the following figure.

The screenshot displays the Cisco DNA Center interface for creating a guest wireless network. The top navigation bar includes tabs for DESIGN, POLICY, PROVISION, ASSURANCE, and PLATFORM. The left sidebar shows a network hierarchy starting with 'Global'. The main content area is titled 'Create a Guest Wireless Network' and features three numbered steps: 1. Guest Wireless Network, 2. Wireless Profiles, and 3. Portal Customization. The first step is currently active. The form contains several sections: 'Wireless Network Name (SSID)' with a text input field; 'BROADCAST SSID' with a toggle switch; 'LEVEL OF SECURITY' with radio buttons for 'Web Auth' (selected) and 'Open'; 'AUTHENTICATION SERVER' with radio buttons for 'ISE Authentication' (selected) and 'External Authentication'; and 'Where will your guests redirect after successful authentication?' with a dropdown menu set to 'Original URL'. There are also sections for 'MFP CLIENT PROTECTION' (with 'Optional' selected) and '11v BSS TRANSITION SUPPORT' (with 'BSS Max Idle Service', 'Client User Idle Timeout' set to 300, and 'Directed Multicast Service' selected). At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Figure 17.
Create a Guest Wireless Network – step 1 Guest Wireless Network

The following table lists and explains the features which can be configured for guest wireless networks 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.
Broadcast SSID	On/Off Toggle	Determines whether the SSID will be broadcast in wireless beacons and probe responses. The default setting is on.
LEVEL OF SECURITY	Radio Button	Determines the Layer 2 (L2) security settings for the WLAN. The choices are as follows: <ul style="list-style-type: none"> • 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.
AUTHENTICATION SERVER	Radio Button	This selection is only available if Web Auth is selected within LEVEL OF SECURITY. Determines the web portal / authentication server for Web Auth. <ul style="list-style-type: none"> • ISE 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 authentication server. This is the default setting. • External Authentication - This setting configures Local Web Authentication (LWA), to an external server.
AUTHENTICATION SERVER > ISE Authentication > What kind of portal are you creating today?	Drop-down Menu	This selection is only available if ISE Authentication is selected. Determines the type of guest portal which will be created within the Cisco ISE server. The choices are as follows: <ul style="list-style-type: none"> • 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.
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 choices are as follows: <ul style="list-style-type: none"> • Success Page - A dedicated page you create which indicates authentication was successful. From there, the guest would need to re-type in the original URL he/she was attempting to reach. • Original URL - Once authentication is successful, the guest is automatically redirected to the original URL he/she was 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.
Advanced Settings - Session timeout	Check Box & 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).

Feature	Type	Description
Advanced Settings - Client Exclusion	Check Box & 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).
Advanced Settings - MFP CLIENT PROTECTION	Radio Button	Additional security setting which controls the use of 802.11w Protected Management Frames for the WLAN. The radio button choices are as follows: <ul style="list-style-type: none"> • Optional - This setting allows wireless stations which support 802.11w Protected Management Frames to use them, as well other wireless stations which do not support PMFs to co-exist 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) which the client is associated.
Advanced Settings - 11v BSS TRANSITION SUPPORT	Multiple Check Boxes & Integer Field	Additional settings for support of 802.11v Wireless Network Management (WNM) for the WLAN. The settings are as follows: <ul style="list-style-type: none"> • BSS Max Idle Service - Checkbox which enables the maximum idle service for the WLAN. Allows APs to send the timeout value to the wireless client within association and re-association response frames. The default setting is enabled. • Client User Idle Timeout - Checkbox with bounded integer field which specifies maximum amount of time an AP will keep 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 - Checkbox which allows the client to request from the AP that multicast streams to be sent as unicast streams to the client. By default, this setting is enabled.

2. Fill in the necessary information and click the **Next** button at the bottom of the screen.

The following are the settings for the guest wireless network configured for this deployment guide.

Table 15. Guest wireless network settings

Feature	Settings
Wireless Network Name(SSID)	lab3guest
Broadcast SSID	On
LEVEL OF SECURITY	Web Auth
AUTHENTICATION SERVER	ISE Authentication
AUTHENTICATION SERVER > ISE Authentication > What kind of portal are you creating today?	Self Registered

Feature	Settings
AUTHENTICATION SERVER > ISE Authentication > Where will your guests redirect after successful authentication?	Original URL
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

This should take you to the next screen in the workflow, where you can attach the guest wireless network to the existing **corporate** wireless profile. An example of the screen is shown in the figure below.

The screenshot shows the Cisco DNA Center interface for editing a guest wireless network. The top navigation bar includes tabs for DESIGN, POLICY, PROVISION, ASSURANCE, and PLATFORM. The left sidebar shows a network hierarchy under 'Global', including locations like Denver, Houston, Miami, Milpitas, and various buildings and floors. The main content area is titled 'Edit a Guest Wireless Network' and features a three-step progress bar: 1. Guest Wireless Network, 2. Wireless Profiles (active), and 3. Portal Customization. Below the progress bar, the 'Profiles' section shows a table with one selected profile named 'corporate'. The table columns are Profile Name, Version, Created By, Sites, and Type. The 'corporate' profile has version 5, was created by 'admin', is associated with 9 sites, and has a 'Central' type. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Figure 18.
Create a Guest Wireless Network – step 2 Wireless Profiles

3. Select the **corporate** wireless profile.

The **Edit a Wireless Profile** side panel will appear, allowing you to edit the profile to add the guest wireless network. An example is shown in the following figure.

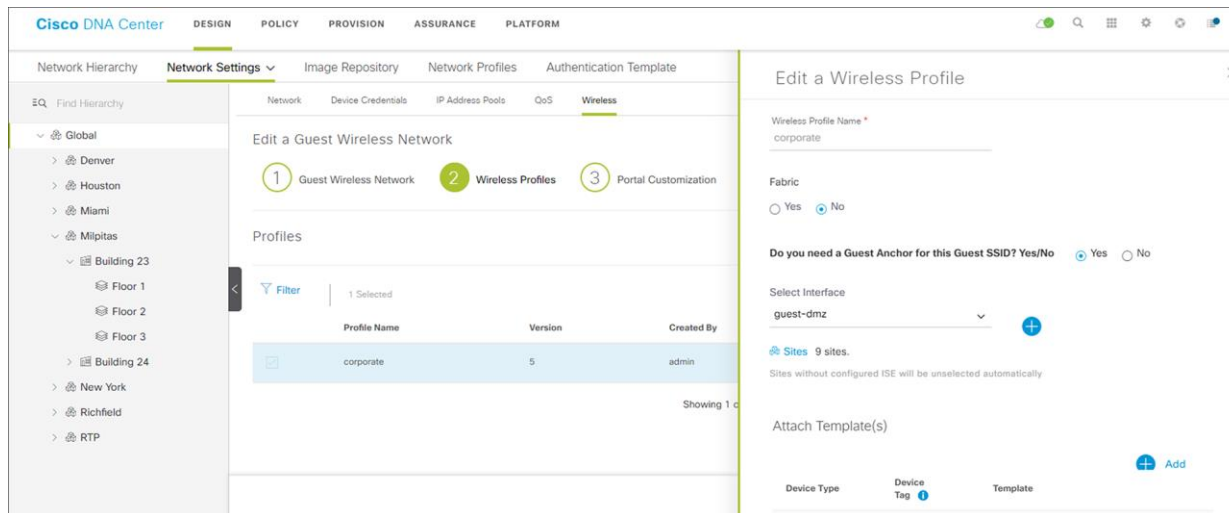


Figure 19.
Edit a Wireless Profile side panel

4. Under **Fabric**, select **No** from the radio button options.

This deployment guide only discusses non-SDA wireless deployments using Cisco DNA Center. Selecting **No** will automatically cause additional fields to appear.

5. Select the **Yes** radio button next to **Do you need a Guest Anchor for this Guest SSID?**

This will configure a traditional auto-anchor relationship between the enterprise (foreign) WLC and the guest (anchor) WLC. Typically, the guest (anchor) WLC is located within an Internet Edge DMZ segment of the campus network.

6. From the drop-down menu under the **Select Interface** field, select **guest-dmz**.

This will terminate guest traffic on the **guest-dmz** VLAN (**VLAN 168**) of the guest (anchor) WLC.

1. Click the **Sites** button to bring up another panel displaying the site hierarchy.
2. Under **Global** click the **>** to display up the **Milpitas** area.
3. Select the **Milpitas** area. This should automatically check the child site locations - **Building 23, Floors 1 - 3** and **Building 24, Floors 1 - 3**, as shown in the figure above.
4. Click **OK** to close the site hierarchy side panel.

CLI-based templates can be added to the enterprise wireless network configuration by clicking the **+ Add** button under **Attach Template(s)**. These templates must already be defined within the **Template Editor** dashboard of Cisco DNA Center. This deployment guide will not discuss the addition of templates, since it does require knowledge of the CLI syntax of the specific WLC platform to implement. However, wireless features not supported by the web-based graphical user interface of Cisco DNA Center may be added through templates.

5. Click the **Save** button at the bottom of the **Edit a Wireless Profile** side panel to save the edits to the **corporate** wireless profile.

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

- 6. Click the **Save** button to add the **lab3guest** guest wireless network to the **corporate** wireless profile.
- 7. Click **Next** to move to the next step in the workflow, the **Portal Customization** screen.

An example is shown in the following figure.

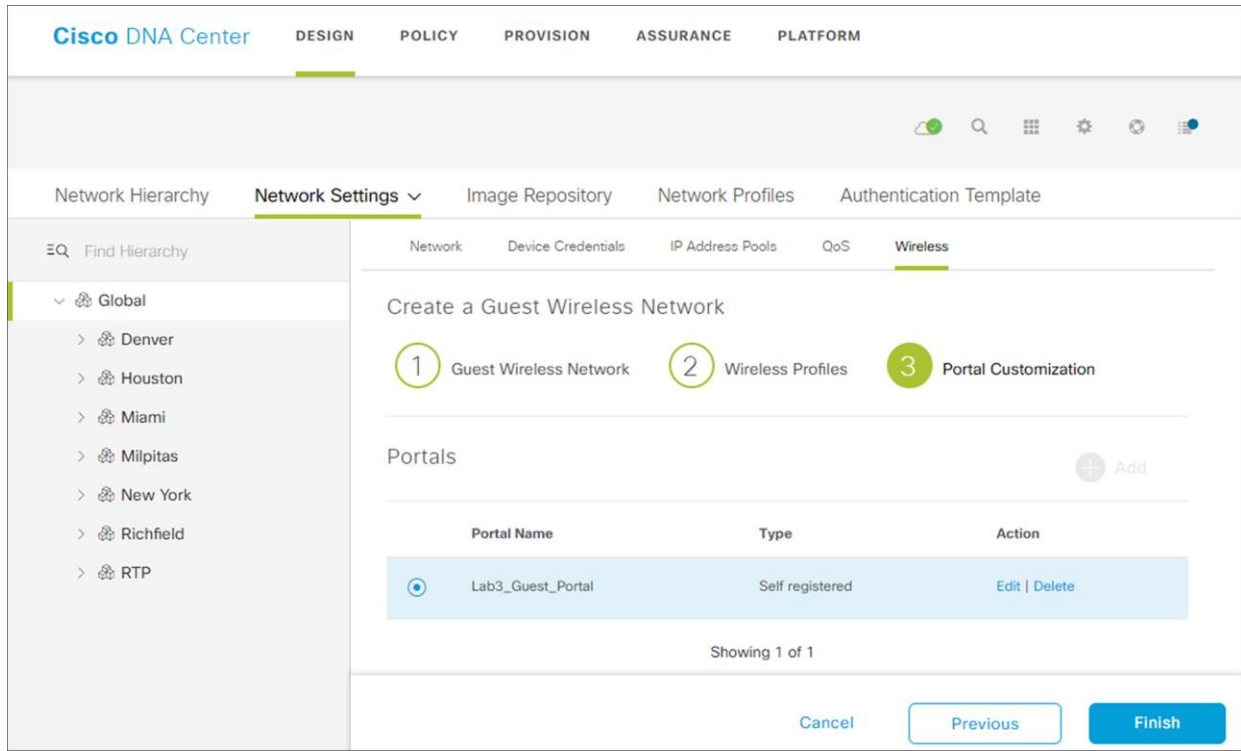


Figure 20.
Create a Guest Wireless Network - step 3 Portal Customization

- 8. To add a new guest portal within Cisco ISE, click the **+ Add** button.

This will bring the **Portal Builder** screen. An example is shown in the following figure.

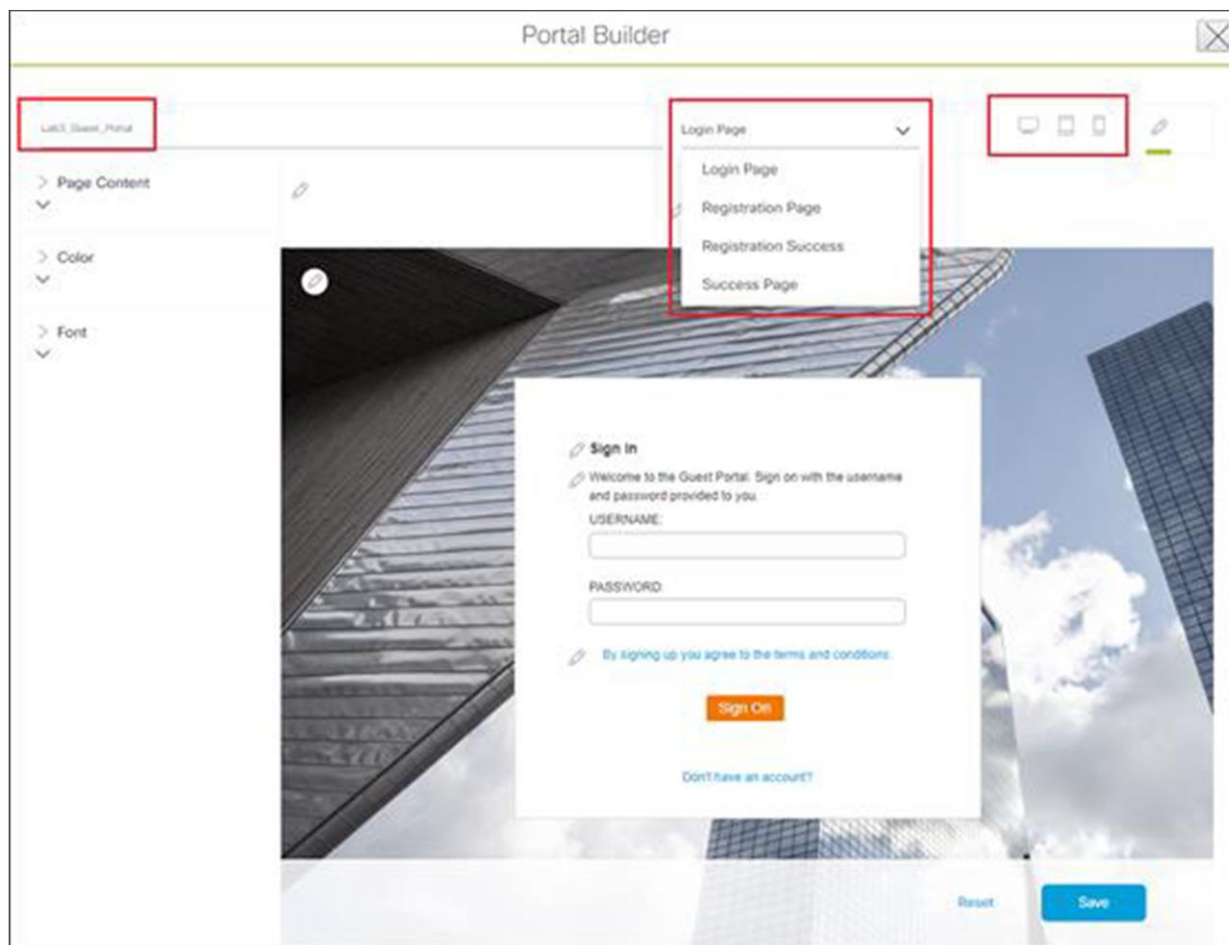


Figure 21.
Portal Builder Screen

9. The minimum you must do is to 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 PC / laptop.

10. When you are done customizing the portal click the **Save** button to create the new guest portal on the Cisco ISE server and return to the guest wireless network workflow.

The new guest portal should now appear.

11. Click the **Finish** button to complete the addition of the guest wireless network and return you to the **Wireless Network Settings** dashboard.

When you are completed, the guest wireless SSID (**lab3guest**) should appear in the **Wireless Network Settings** dashboard.

Procedure 4: 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 pre-configured RF profiles within Cisco DNA Center. These RF profiles are also pre-configured within Cisco Catalyst 9800 Series and Cisco AireOS WLCs.
- Create custom RF profiles in which you can fine tune various RF aspects of your wireless deployment.
- Select either a pre-configured or custom RF profile as the default RF profile that is assigned to APs within Cisco DNA Center.

When provisioning APs within Cisco DNA Center, the default RF profile configured within the **Wireless Settings** dashboard will be applied. However, this setting can also be overridden per AP.

The three pre-configured RF profiles are as follows:

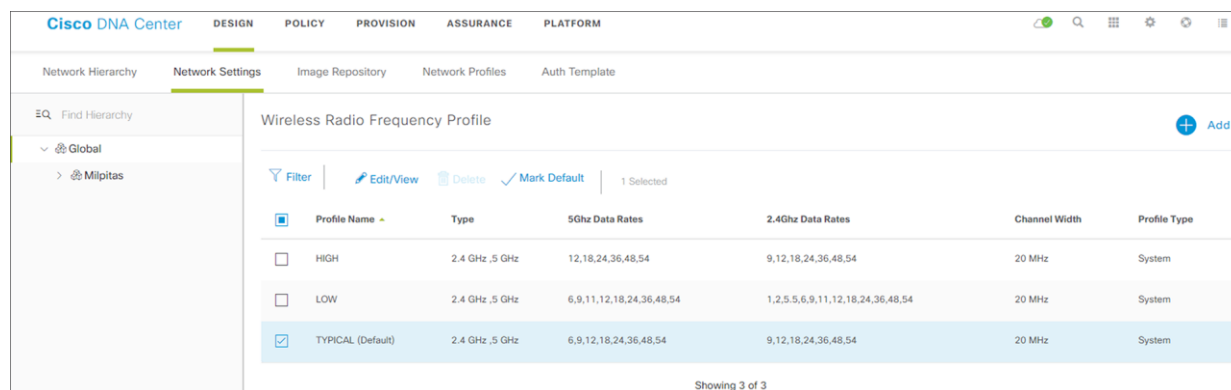
- **LOW** - This profile tunes the RF attributes in both bands (2.4 GHz and 5 GHz) for low client density deployments.
- **TYPICAL** - This profile tunes the RF attributes in both bands (2.4 GHz and 5 GHz) for medium client density deployments.
- **HIGH** - This profile tunes the RF attributes in in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

Appendix D explains the specific settings within each of the three pre-configured RF profiles within Cisco DNA Center.

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

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

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 box next to the name of one of the available profiles and click on the **✓Mark Default** button.



Profile Name	Type	5Ghz Data Rates	2.4Ghz Data Rates	Channel Width	Profile Type
<input type="checkbox"/> HIGH	2.4 GHz, 5 GHz	12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz	System
<input type="checkbox"/> LOW	2.4 GHz, 5 GHz	6,9,11,12,18,24,36,48,54	1,2,5,6,9,11,12,18,24,36,48,54	20 MHz	System
<input checked="" type="checkbox"/> 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

Figure 22.
Wireless Radio Frequency Profile section

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

You are now ready to move on to the next step of the design and deployment guide using Cisco DNA Center to deploy the wireless networks defined within this 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 Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**) and a Catalyst 9800-CL guest WLC (**WLC-9800-CL**).

The processes for deploying the wireless network are as follows:

- Discover and manage the Catalyst 9800 Series WLCs
- Manage software images for the Catalyst 9800 Series WLCs
- Use software image management (SWIM) to update the Catalyst 9800 Series WLC software
- Configure high availability (HA) stateful switch-over (SSO) on the Catalyst 9800-40 enterprise WLCs
- Provision the Catalyst 9800-40 enterprise WLC HA SSO pair
- Provision the Catalyst 9800-CL guest anchor WLC
- Join new APs to the enterprise WLC HA SSO pair
- Provision the new APs
- Position the new APs on the floor map

Process: Discover and manage the Catalyst 9800 Series WLCs

This deployment guide uses IP address ranges for discovery of both of the Catalyst 9800-40 WLCs deployed as enterprise WLCs and the Catalyst 9800-CL WLC deployed as the guest WLC. This requires enabling IP connectivity to the devices, before initiating the discovery. When using IP address ranges, you can reduce the range to just the WLCs to speed the discovery.

Technical 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 process:

- The two Catalyst 9800-40 WLCs (**WLC-9800-1** and **WLC-9800-2**) are connected to the network as standalone WLCs. Configuration of the two Catalyst 9800-40 WLCs into an HA SSO pair will be done within Cisco DNA Center in an upcoming process.
- NETCONF is enabled on all of the Catalyst 9800 Series WLCs (**WLC-9800-1**, **WLC-9800-2**, and **WLC-9800-CL**).
- All Catalyst 9800 Series WLCs are already on the network with wireless management IP addresses configured for reachability.

- SSH access is already enabled on all of the Catalyst 9800 Series WLCs, with a userid and password configured within the local user database.
- All Catalyst 9800 Series WLCs already have hostnames configured (**WLC-9800-1**, **WLC-9800-2**, and **WLC-9800-CL**). This will allow the devices to be identified by their hostnames within Cisco DNA Center inventory after discovery.

The following table shows the hostnames, platform models, and IP addresses of the WLCs for this design and deployment guide.

Table 16. Hostnames, platform models, and IP addresses of WLCs

Hostname	Platform Model	IP Address
WLC-9800-1	Cisco Catalyst 9800-40 WLC	10.4.174.32
WLC-9800-2	Cisco Catalyst 9800-40 WLC	10.4.174.34
WLC-9800-CL	Cisco Catalyst 9800-CL WLC	10.4.174.36

The following are the procedures for this process:

- Discover the two Catalyst 9800-40 WLCs which will serve as the enterprise HA SSO pair for the WLAN deployment.
- Discover the Catalyst 9800-CL WLC which will serve as the guest anchor WLC for the WLAN deployment.

Procedure 1: Discover the two Catalyst 9800-40 WLCs which will serve as the enterprise HA SSO pair for the WLAN deployment

The following are the steps for discovery of the Catalyst 9800-40 WLCs (**WLC-9800-1** and **WLC-9800-2**).

2. Navigate to the main Cisco DNA Center dashboard.
3. At the bottom of the page, within the **Tools** section, click on **Discovery**.

This will take you to the **Discovery Dashboard**. An example is shown in the following figure.

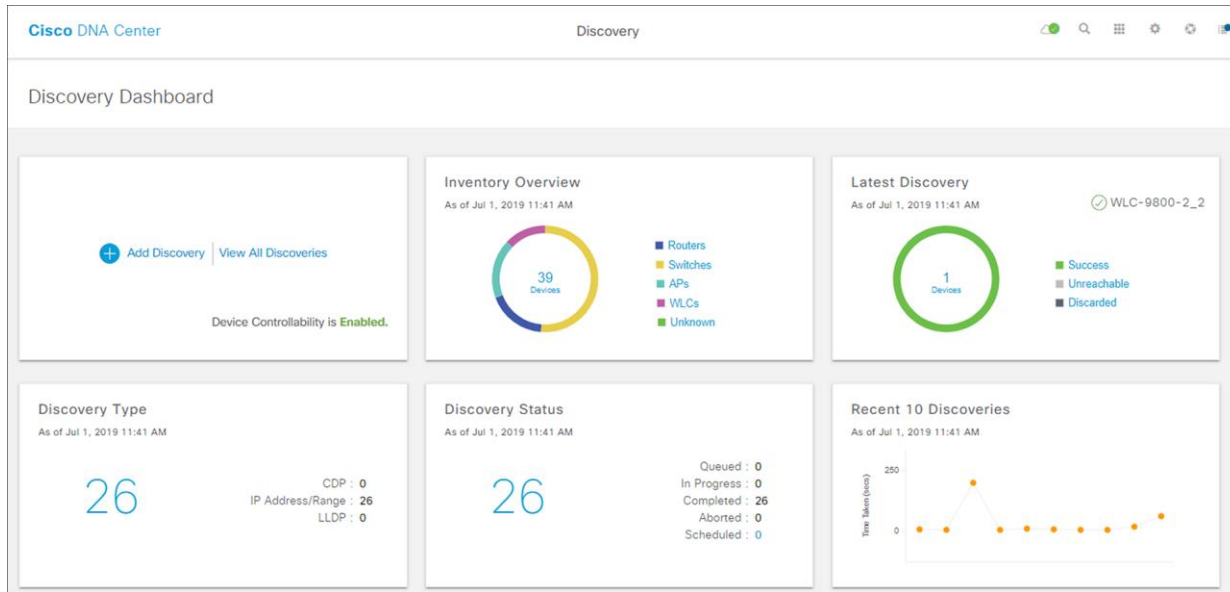


Figure 23.
Discovery Dashboard

4. Click on the **+ Add Discovery** widget to create a new discovery.

This will take you to the **New Discovery** dashboard. An example is shown in the following figure.

The screenshot shows the 'New Discovery' configuration page in Cisco DNA Center. The 'Discovery Name' is 'Catalyst_9800_WLCs'. Under 'IP Address/Range', the 'Discovery Type' is 'Range', with 'From' IP '10.4.174.32' and 'To' IP '10.4.174.34'. 'Preferred Management IP' is set to 'None'. In the 'Credentials' section, 'CLI' has 'CiscoDNA' and 'netadmin' credentials. 'SNMPv2c Read' is set to 'Read', 'SNMPv2c Write' is set to 'Write', and 'SNMPv3' shows 'No credentials to display'. A 'Start' button is visible at the bottom right.

Figure 24.
New Discovery

5. In the **IP Address/Range** section, under **Discovery Type**, select the **Range** radio button.
6. Type in the beginning IP address in the text field under **From**, and the ending IP address in the text field under **To**.

In the figure above the range configured is **10.1.174.32 - 10.1.174.34**, which is sufficient to discover the two Catalyst 9800-40 WLCs (**WLC-9800-1** and **WLC-9800-2**).

7. For **Preferred Management IP**, if a device has a loopback interface used for management, select the **Use Loopback** radio button. Otherwise leave the radio button at **None**.

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

8. Make sure the **CLI**, **SNMP**, and **NETCONF** credential ON/OFF toggle switches are set to **On**.

All Catalyst 9800 Series WLCs require NETCONF for discovery and provisioning. The userid/password used for NETCONF access to the WLCs is the same as the SSH password.

9. In the **Advanced** section, under **Protocol Order**, check the box next to **SSH**.

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

10. Click **Start** to begin the discovery.

The discovery details are displayed while the discovery runs. When the discovery has completed, it should appear as shown in the following figure.

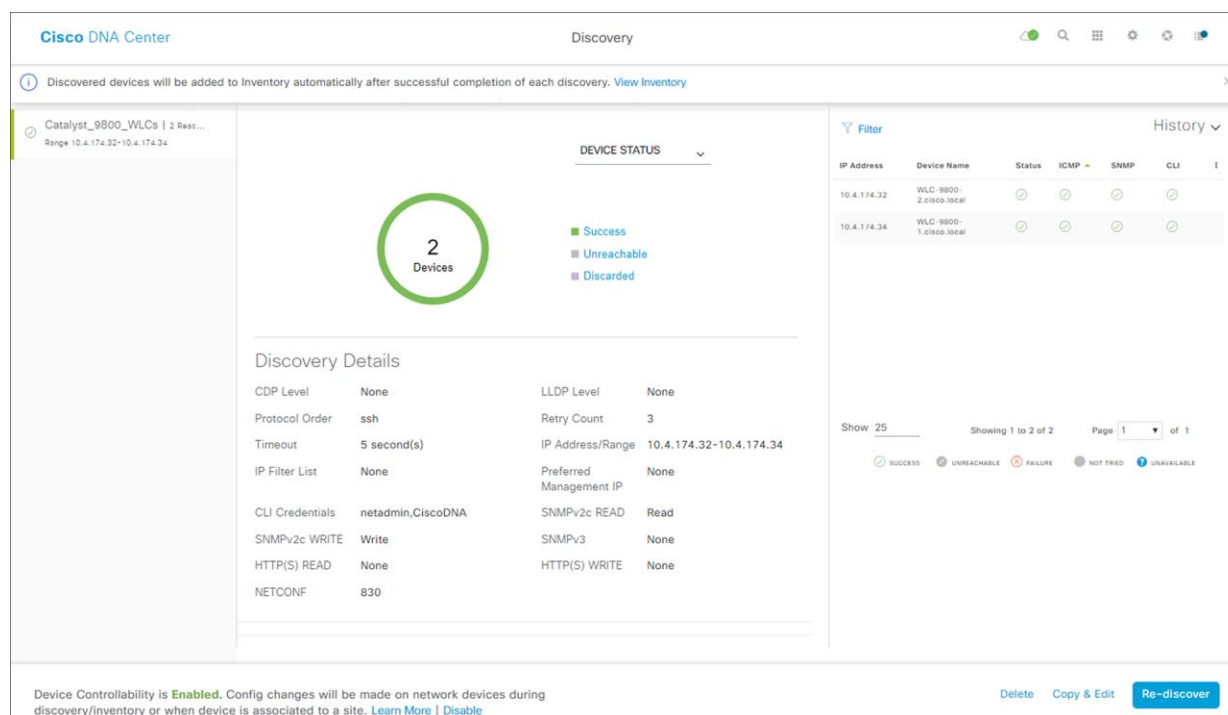


Figure 25.
Completed Discovery

11. After the discovery process successfully finishes, navigate to the main Cisco DNA Center dashboard.
12. Navigate to **Provision** to display the inventory.

This will display the list of devices known to Cisco DNA Center. Included within the list will be the two Catalyst 9800-40 WLCs (**WLC-9800-1** and **WLC-9800-2**) just discovered. The Catalyst 9800-40 WLCs should show a **Last Sync Status of Managed**. An example of the inventory is shown in the figure below.

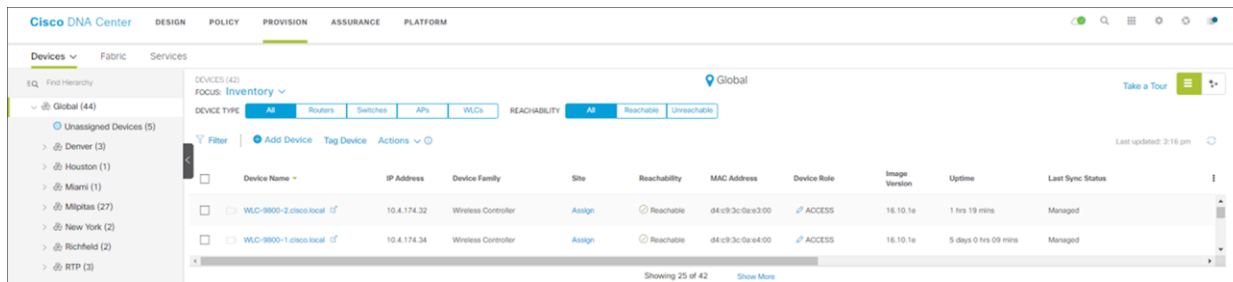


Figure 26.
Cisco DNA Center inventory

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

Procedure 2: Discover the Catalyst 9800-CL WLC which will serve as the guest anchor WLC for the WLAN deployment

- Repeat the previous procedure to discover the Catalyst 9800-CL guest WLC (**WLC-9800-CL**).

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

Technical Note: Optionally, you can discover all the WLCs in a single discovery which includes the IP address range of both the Catalyst 9800-40 enterprise WLCs (**WLC-9800-1** and **WLC-9800-2**) as well as the Catalyst 9800-CL guest WLC (**WLC-9800-CL**).

Process: Manage software images for the Catalyst 9800 Series WLCs

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

Table 17. Software images for the Catalyst 9800 Series WLCs

Platform	Software Version	Software Image
Cisco Catalyst 9800-40 WLC	IOS XE Release 16.10.1e	C9800-40-universalk9_wlc.16.10.01e.SPA.bin
Cisco Catalyst 9800-CL WLC	IOS XE Release 16.10.1e	C9800-CL-universalk9.16.10.01e.SPA.bin

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

The following are the procedures for this process:

- Upload the software image for the Catalyst 9800-40 WLCs.
- Upload the software image for the Catalyst 9800-CL WLC.

Procedure 1: Upload the software image for the Catalyst 9800-40 WLCs

The following steps discuss the image upload to Cisco DNA Center for the Catalyst 9800-40 WLCs (**WLC-9800-1** and **WLC-9800-2**).

1. Navigate to the main Cisco DNA Center dashboard.
2. Click on **Design**, and then click on **Image Repository**.

This will take you to the main image repository screen. An example is shown in the following figure.

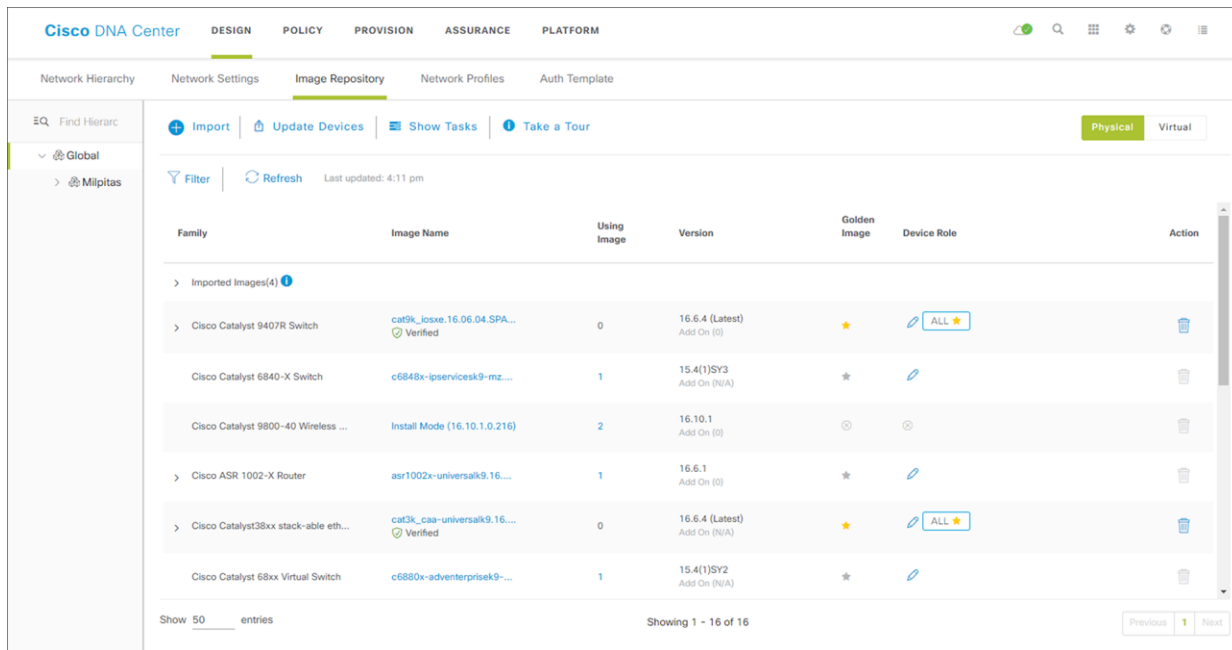


Figure 27.
Image Repository Screen

3. To import a new image, click the **Import** button.

This will bring up the **Import Image/Add-On** pop-up screen. An example is shown in the figure below.

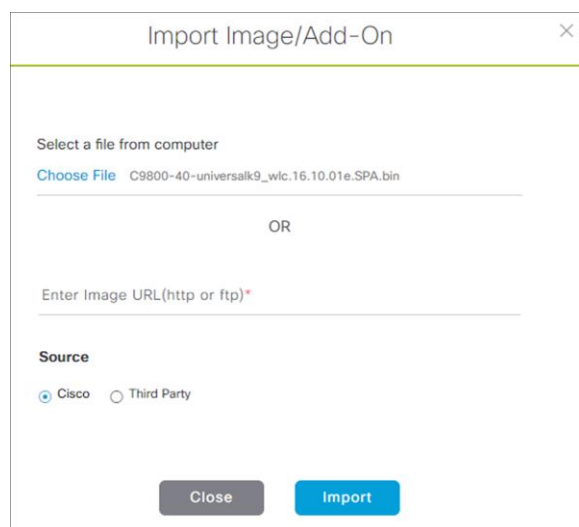


Figure 28.
Import Image/Add-On screen

4. Click on **Choose File**, navigate to the Catalyst 9800-40 software image on your PC / laptop, and select the image (**C9800-40-universalk9_wlc.16.10.01e.SPA.bin**).
5. Under **Source**, select the **Cisco** radio button, since this is a Cisco software image.
6. Click the **Import** button to import the image to the Cisco DNA Center image repository.

A status bar will appear which tracks the progress of the upload. Once the upload is completed, you will be taken back to the main image repository screen.

7. You can verify the import is in the image repository and ready to deploy by clicking **Show Tasks** to bring up the **Recent Tasks (Last 50)** side panel.

It may take a few minutes until the new image transitions from being listed in yellow - meaning the task is still running, to green with a check mark next to it - meaning the task completed successfully.

8. Close the **Recent Tasks (Last 50)** side panel by clicking on the X in the upper right corner of the panel.
9. From the **Image Repository** screen, click on the > next to Imported Images to expand the list of imported images.
10. Click on **Assign** next to the image file you just uploaded.

This will bring up the Assign Device Family side panel. An example is shown in the figure below.

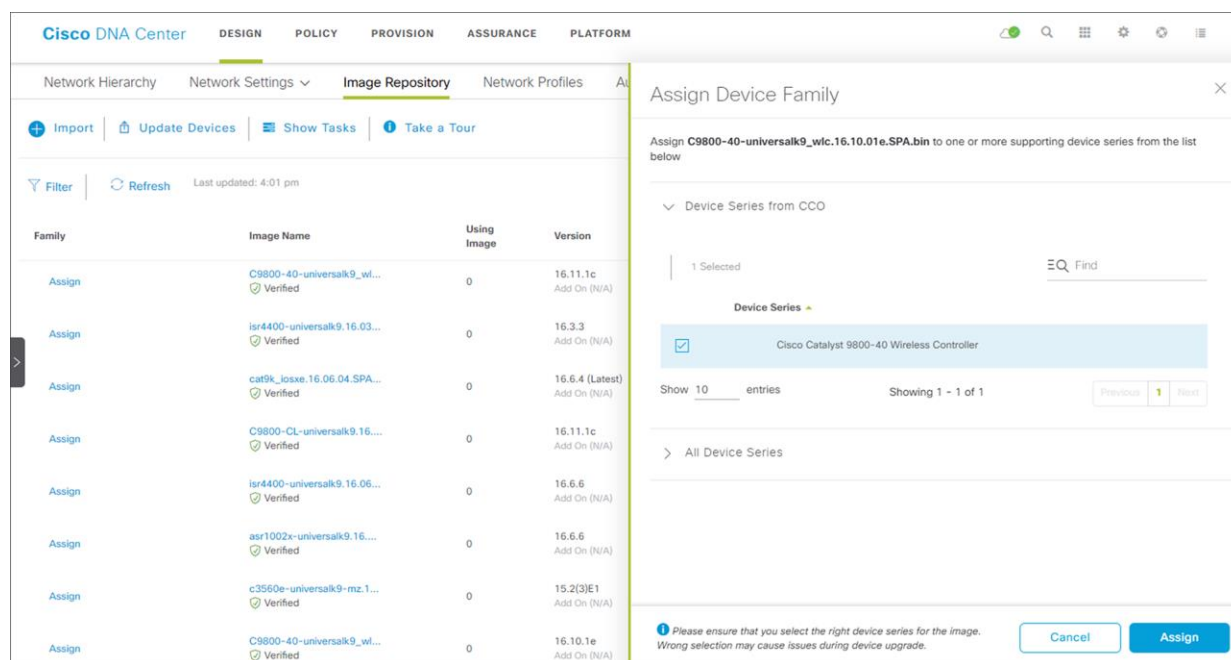


Figure 29.
Assign Device Family side panel

11. Check the box next to **Cisco Catalyst 9800-40 Wireless Controller** and click **Assign** to assign this image to its device family.
12. Locate the Catalyst 9800-40 wireless controllers under the **Family** column in the list of devices within the main image repository screen and click the > to expand the list of available images for the device.

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

13. Click the star for **Golden Image** to mark the image as the preferred one for the Catalyst 9800-40 WLC platform.

Procedure 2: Upload the software image for the Catalyst 9800-CL WLC

1. Repeat **Steps 1 - 13** of the previous procedure for the Catalyst 9800-CL guest WLC (**WLC-9800-CL**).

For the Catalyst 9800-CL guest WLC, the upload image name is for this deployment guide is **C9800-CL-universalk9.16.10.01e.SPA.bin**.

Process: Use software image management (SWIM) to update the Catalyst 9800 Series WLC software

This process is used for the following:

- To distribute (download) the software image from the Cisco DNA Center image repository to the WLCs.
- To upgrade the software images running on the WLCs.

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

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

The following are the procedures for this process:

- Upgrade the software images for the Catalyst 9800-40 WLCs.
- Upgrade the software image for the Catalyst 9800-CL WLC.

Procedure 1: Upgrade the software images for the Catalyst 9800-40 WLCs

The following are the steps for upgrading the software images of the Catalyst 9800-40 WLCs (**WLC-9800-1** and **WLC-9800-2**).

1. From the main Cisco DNA Center dashboard navigate to **Provision**

This will take you to the main provisioning screen that displays the devices within the inventory.

2. From the drop-down menu adjacent to **Focus:** select **Software Images**.

This will change the screen to display the software image running on each device within inventory. An example is shown in the following figure.

Cisco DNA Center

DESIGNPOLICYPROVISIONASSURANCEPLATFORM

DevisesFabricServices

DEVICES (42)

FOCUS: Software Images

Take a Tour

DEVICE TYPEAllRoutersSwitchesAPsWLCsREACHABILITYAllReachableUnreachable

FilterAdd DeviceTag DeviceActions

Last updated: 4:07 pm

	Device Name	IP Address	Device Family	Site	Reachability	Software Image	Image Version	Update Status	Provision Status
<input type="checkbox"/>	<div>WLC-9800-2.cisco.local</div>	10.4.174.32	Wireless Controller	Assign	<div>Reachable</div>	<div>C9800-40-universalk9_wl</div> <div>Outdated</div>	16.10.1	Distribution Pending	Not Provisioned
<input type="checkbox"/>	<div>WLC-9800-1.cisco.local</div>	10.4.174.34	Wireless Controller	Assign	<div>Reachable</div>	<div>C9800-40-universalk9_wl</div> <div>Outdated</div>	16.10.1	Distribution Pending	Not Provisioned

Figure 30.
Inventory focus within Provisioning

3. From the list of devices, locate one of the Catalyst 9800-40 WLCs (**WLC-9800-1** or **WLC-9800-2**)
4. Under the **Software Image** column of the Catalyst 9800-40 WLC click on the **Outdated** icon.

This will bring up the **Image Upgrade Readiness Check** panel. An example is shown in the figure below.

The screenshot displays the Cisco DNA Center interface. On the left, the 'Device Inventory' pane shows a list of devices. On the right, the 'Image Upgrade Readiness Check' panel is open, showing the results of a readiness assessment for a specific device.

Image Upgrade Readiness Check Panel Details:

- Running Image:** C9800[16.10.1.0.216]
- Golden Image:** C9800-40-universalk9_wlc.16.10.01e.SPA.bin
- Buttons:** Export, Recheck

Check Type	Description	Status	Last Checked (UTC)
NTP Clock check	No diff in time between Device and DNAC cluster!	Success (Green)	Fri Mar 22 2019 11:57:40 AM
File Transfer Check	HTTPS/SCP is reachable :10.4.48.183	Success (Green)	Fri Mar 22 2019 11:57:40 AM
Config register check	Could not validate the Config Register Actual : 0x2102	Warning (Yellow)	Fri Mar 22 2019 11:57:39 AM
Crypto RSA check	Crypto RSA Key configured on the device	Success (Green)	Fri Mar 22 2019 11:57:39 AM
Crypto TLS check	TLS 1.2 Configured on device	Success (Green)	Fri Mar 22 2019 11:57:38 AM
IP Domain name check	Domain name is configured with cisco.local	Success (Green)	Fri Mar 22 2019 11:57:38 AM
Startup config check	Startup configuration exist for this device	Success (Green)	Fri Mar 22 2019 11:57:38 AM
Device Managed Status	Device Managed Successfully.	Success (Green)	Fri Mar 22 2019 11:57:37 AM
Flash check	Flash check: SUCCESS	Success (Green)	Fri Mar 22 2019 11:57:37 AM

At the bottom of the table, it says 'Showing 1 - 9 of 9'.

Figure 31.
Image Upgrade Readiness Check panel

You must ensure that the **Status** column of all the checks shows either a green icon indicating success, or a yellow icon indicating a warning. If any of the checks shows a red icon indicating failure, the image on the platform cannot be upgraded.

5. If necessary, correct any issues on the WLC which resulted in a red icon indicating failure. Click the **Recheck** button in the upper right corner to re-run the readiness assessment.

Technical Note: Configuring a time zone within IOS XE devices via the “clock timezone...” IOS CLI command may cause a warning to appear within the **Image Upgrade Readiness Check** panel, indicating 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 within inventory, and clicking on the **Recheck** button to run the readiness assessment again. This will cause the time format of the device be displayed in UTC time, rather than the local time zone.

6. When you have corrected all checks which indicate a failure, close the **Image Upgrade Readiness Check** panel by clicking on the **X** in the upper right corner of the panel.
7. Repeat **Steps 2 - 6** for the other Catalyst 9800-40 WLC.
8. Select the check boxes next to both of the Catalyst 9800-40 WLCs (**WLC-9800-1** and **WLC-9800-2**).
9. Under the **Actions** drop-down menu, select **Software Image > Update Image**.

The **Update Image** side panel will appear. An example is shown in the following figure.

Update Image

1 device(s)

1 Distribute 2 Activate 3 Confirm

When

☐ Now ☒ Later

Task Name *

Create Distribute Task

7 / 5 / 2019

3 : 44 : PM

Time Zone

☒ Site Settings

Note: The task will run based on site time zone. Un-check to select a specific time zone from the list below.

Currently using site time zone.

Cancel Next

Figure 32.

Update Image side panel – Step 1 Distribute

The **Update Image** side panel will take you through a three-step workflow.

Step 1 - Distribute. In this step of the workflow you can choose when you want to distribute the image from the Cisco DNA Center server to the WLCs you have selected. You can choose to distribute the new image now or schedule the distribution for a future date and time.

10. Click the **Now** radio button or leave the **Later** radio button selected and adjust the data and time for the image distribution.

For this deployment guide the **Now** radio button was selected.

11. Click the **Next** button to continue to the next step in the workflow.

Step 2 - Activate. In this step of the workflow you can choose when you want to activate the image that was distributed in the previous step to the devices you have selected. An example is shown in the following figure.

Figure 33.
Update Image side panel – Step 2 Activate

If the software has not been distributed (downloaded from the Cisco DNA Center repository to the WLCs) you cannot choose the **Now** button. However, you can schedule the software to be activated immediately after the software distribution completes, 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.

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

12. Check the box next to **Schedule Activation after Distribution is Completed**. Alternatively, leave the **Later** radio button selected and adjust the data and time for the image distribution.

Checking the **Schedule Activation after Distribution is Completed** box will activate the image immediately after it is distributed. Essentially this combines the download and activation of the image into a single scheduled process, rather than scheduling download and activation separately. For this design and deployment guide, the **Schedule Activation after Distribution is Completed** box was selected.

13. Click the **Next** button to continue to the next step in the workflow.

Step 3 - Confirm. In this step of the workflow you confirm the distribution and activation times you have configured. An example is shown in the following figure.

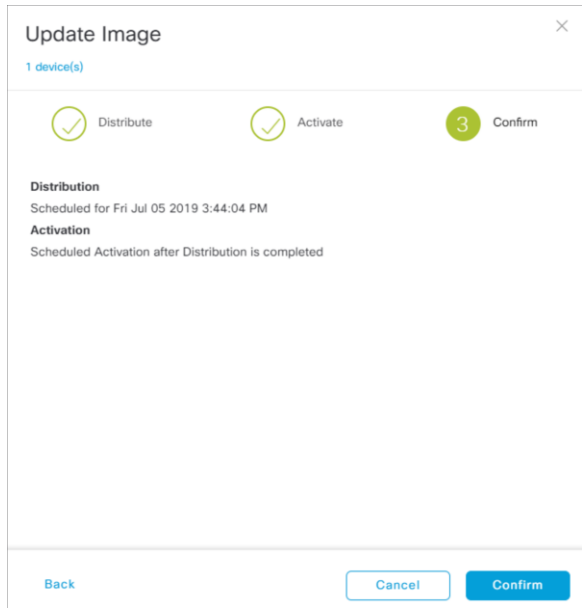


Figure 34.
Update Image side panel - Step 3 Confirm

14. Click the **Confirm** button to confirm the image update.

This will take you back to the **Provisioning** screen. If you have scheduled the distribution and activation for a future date and/or time you can view the upcoming scheduled task.

15. Click on the **Notifications** icon in the upper right corner of any Cisco DNA Center screen.

This will bring up the **Scheduled Tasks** side panel. An example is shown in the following figure.

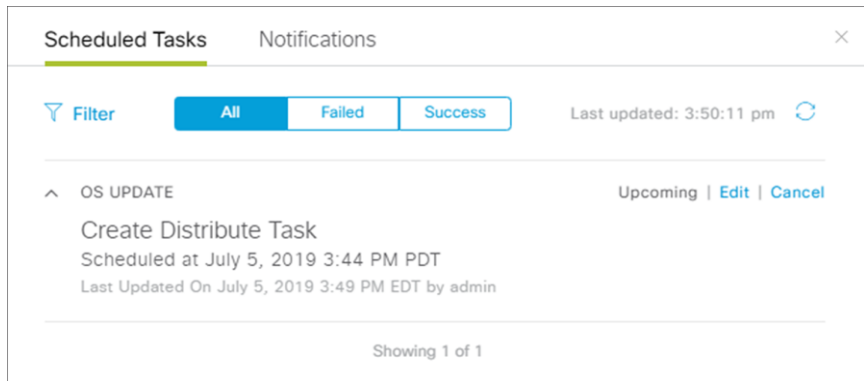


Figure 35.
Scheduled Tasks side panel

You can view, edit the date & time of the task, or cancel the task from this panel. When the task begins, an icon will appear next to it indicating that the update is in progress. You can expand on the task to see the specifics regarding the distribution and activation of the image, as shown in the following figure.

Scheduled Tasks Notifications

Filter All Failed Success Last updated: 5:23:40 pm

OS UPDATE ⚠ In Progress

Create Distribute Task
Started at March 22, 2019 2:00 PM PDT
Last Updated On March 22, 2019 5:00 PM EDT by admin

Image Upgrade for 10.4.174.34

C9800-40-universalk9_wlc.16.10.01e.SPA.bin
Duration : 0h: 23m: 44s Start Time : Mar22 2019 17:00:00 ● In Progress

1. ✔ **Distribute Operation** Duration : 0h: 6m: 0s
Distribution of image: C9800-40-universalk9_wlc.16.10.01e.SPA.bin on device: 10.4.174.34 with protocol: SCP completed successfully

2. **Activate Operation** Duration :
Started activate of image: C9800-40-universalk9_wlc.16.10.01e.SPA.bin on device: 10.4.174.34

Image Upgrade for 10.4.174.32

C9800-40-universalk9_wlc.16.10.01e.SPA.bin
Duration : 0h: 20m: 11s Start Time : Mar22 2019 17:00:00 ● Successful

1. ✔ **Distribute Operation** Duration : 0h: 5m: 43s
Distribution of image: C9800-40-universalk9_wlc.16.10.01e.SPA.bin on device: 10.4.174.32 with protocol: SCP completed successfully

2. ✔ **Activate Operation** Duration : 0h: 14m: 24s
Activation of image: C9800-40-universalk9_wlc.16.10.01e.SPA.bin on device: 10.4.174.32 completed successfully

Showing 1 of 1

Figure 36.
OS update in progress

When the task completes successfully, an icon will appear next to it indicating that the update was a success. Again, you can expand on the task to see the specifics regarding the distribution and activation of the image.

16. Close the **Scheduled Tasks** side panel to go back to the inventory list within the main provisioning screen.

The images for the Catalyst 9800-40 WLCs (**WLC-9800-1 & WLC-9800-2**) should now be displayed as being updated to the OS version which you selected.

Procedure 2: Upgrade the software images for the Catalyst 9800-CL WLC

1. Repeat the previous procedure for the Catalyst 9800-CL guest WLC (**WLC-9800-CL**).

Process: Configure high availability (HA) stateful switch-over (SSO) on the Catalyst 9800-40 enterprise WLCs

Catalyst 9800 Series WLCs support the ability to be configured in an active/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 OS version, and configure them into an HA SSO pair.

The following steps will discuss configuring the Catalyst 9800-40 WLCs (**WLC-9800-1** and **WLC-9800-2**) as an HA SSO pair.

2. From the main Cisco DNA Center dashboard navigate to **Provision**.

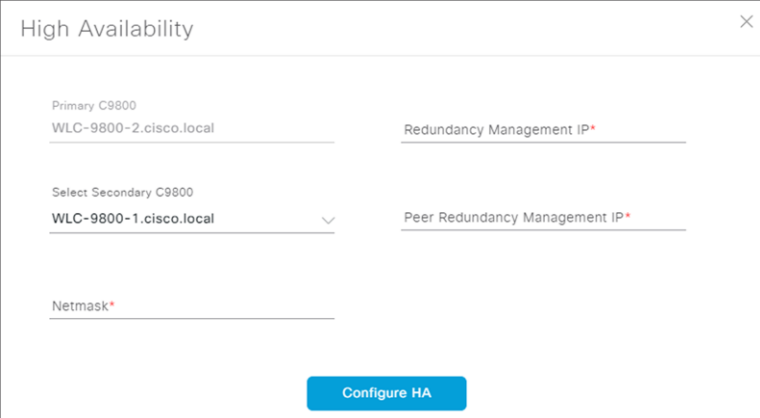
This will take you to the main provisioning screen that displays the devices within the inventory. By default, the **Focus**: will be set for **Inventory**.

3. Locate and check the box next to the Catalyst 9800-40 WLC which will be the primary of the HA SSO WLC pair.

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

4. From the drop-down menu under Actions, select **Provision > Configure WLC HA**.

This will bring up the High Availability side panel. An example is shown in the figure below.



The screenshot shows a 'High Availability' configuration window. It contains the following fields and controls:

- Primary C9800:** A text field containing 'WLC-9800-2.cisco.local'.
- Redundancy Management IP*:** An empty text field.
- Select Secondary C9800:** A dropdown menu with 'WLC-9800-1.cisco.local' selected.
- Peer Redundancy Management IP*:** An empty text field.
- Netmask*:** An empty text field.
- Configure HA:** A blue button at the bottom right.

Figure 37.
High Availability side panel

5. Fill in the necessary information and click the **Configure HA** button.

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

Table 18. High availability settings

Field	Value
Primary C9800	WLC-9800-2.cisco.local
Redundancy Management IP	203.0.113.1
Select Secondary C9800	WLC-9800-2.cisco.local
Peer Redundancy Management IP	203.0.113.2
Netmask	24

For Catalyst 9800 Series WLCs, the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses which need to be configured within Cisco DNA Center are actually the redundancy port and peer redundancy port IP addresses. These are referred to as the **Local IP** and **Remote IP** addresses within the Web UI of the Catalyst 9800 Series WLCs. The IP subnet for the redundancy port must be a separate IP subnet from any other interface on the Catalyst 9800 Series WLC. Also, the primary and standby Catalyst 9800 Series WLCs must be using the same IP subnet for the redundancy port - meaning the redundancy port connection must be a Layer 2 connection.

A pop-up window will inform you that the WLCs will be rebooted once they are placed high availability mode.

6. Click **OK** to accept and put the two Catalyst 9800-40 WLCs in HA SSO mode.

It will take several minutes for the WLCs to reboot and come up in HA SSO mode. All configuration from the primary Catalyst 9800-40 WLC - including the IP address of the management interface - will be copied to the secondary Catalyst 9800-40 WLC. Cisco DNA Center will no longer show two WLCs in inventory. Instead, only a single WLC HA SSO pair with two serial numbers will appear in inventory.

For this deployment guide, WLC HA SSO pair is **WLC-9800-2**.

7. If you select the WLC (WLC-9800-2), and from the drop-down menu under Actions, select **Provision > Configure WLC HA** you can now see additional information regarding the Catalyst 9800-40 WLC HA SSO pair.

An example is shown in the following figure.

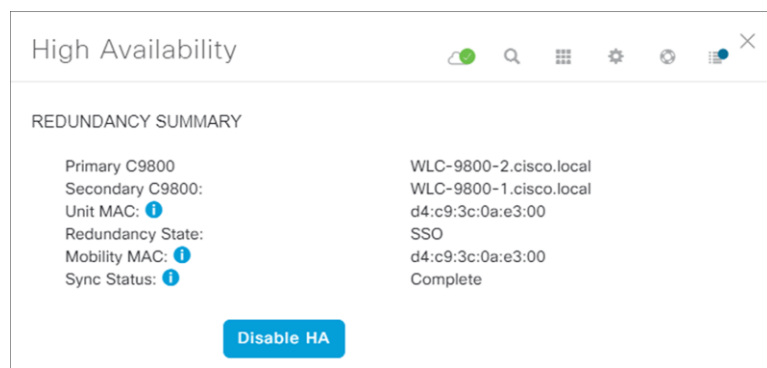


Figure 38.
Wireless HA SSO pair

Process: Provision the Catalyst 9800-40 enterprise WLC HA SSO pair

The following steps provision the **corporate** wireless profile defined in the Define the wireless network section of this document to the Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**).

1. From the main Cisco DNA Center dashboard navigate to **Provision**.

This will take you to the main provisioning screen that displays the devices within the inventory. By default, the **Focus:** will be set for **Inventory**.

2. Locate and check the box next to **WLC-9800-2**.
3. From the drop-down menu under Actions, select **Provision > Provision Device**.

This will take you through a four-step workflow for provisioning the enterprise WLC HA SSO pair (**WLC-9800-2**), starting with **Step 1 - Assign Site**.

4. Click on the **Choose a Site** button in the middle of the screen.

A side panel will appear, showing the site hierarchy configured for Cisco DNA Center. For this deployment guide, the enterprise WLC HA SSO pair (**WLC-9800-2**) is assigned to the building level.

5. Expand the site hierarchy under **Milpitas** and select **Building 23**.

An example is shown in the following figure.

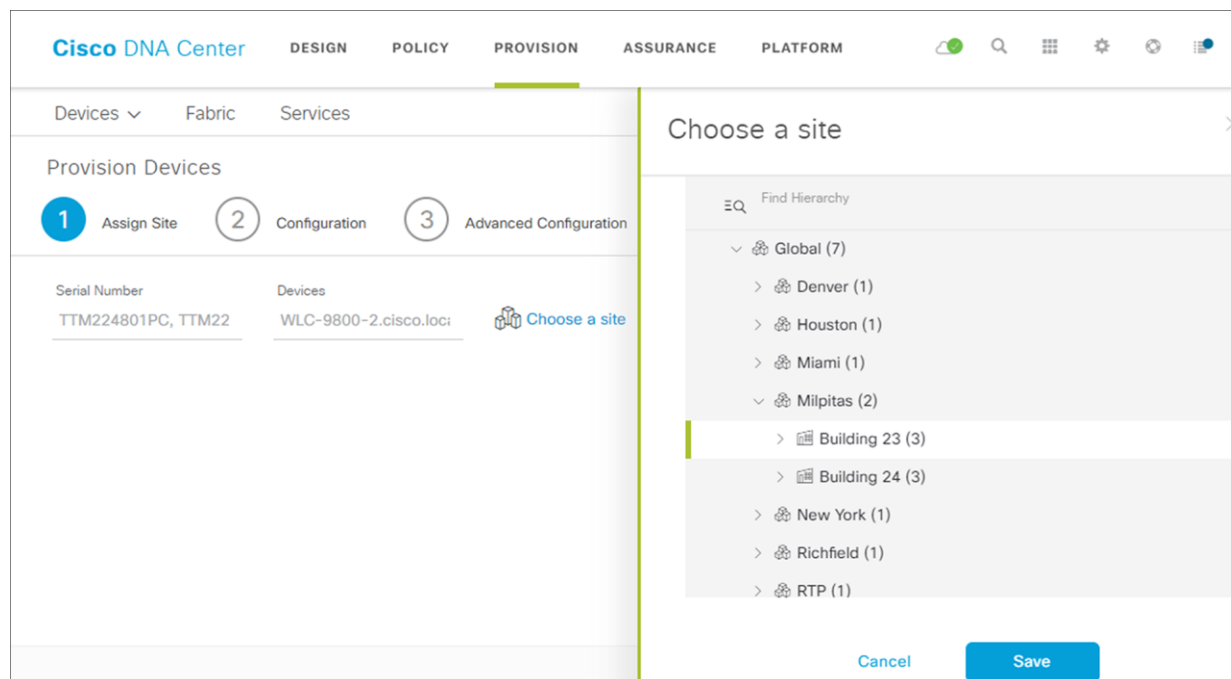


Figure 39.
Enterprise WLC provisioning Step 1 - Assign Site

Technical Note: The enterprise WLC HA SSO pair (**WLC-9800-2**) must be assigned to a building or floor within the Cisco DNA Center site hierarchy. It cannot be assigned to an area (i.e. **Milpitas**) or to the global level of the site hierarchy. Even though **WLC-9800-2** is assigned to a building (**Building 23** in this deployment guide), APs located on floors within other buildings are supported by the WLC.

6. Click the **Save** button to assign **WLC-9800-2** to **Building 23**.
7. Click **Next** to move to the **Step 2** in the device provisioning workflow - **Configuration**.
8. Within the **Configuration** screen, select the **WLC Role** to be **Active Main WLC**.
9. Click on **Select Primary Managed AP locations**.

The **Managed AP Location** side panel will appear, showing the site hierarchy for Cisco DNA Center. An example is shown in the following figure.

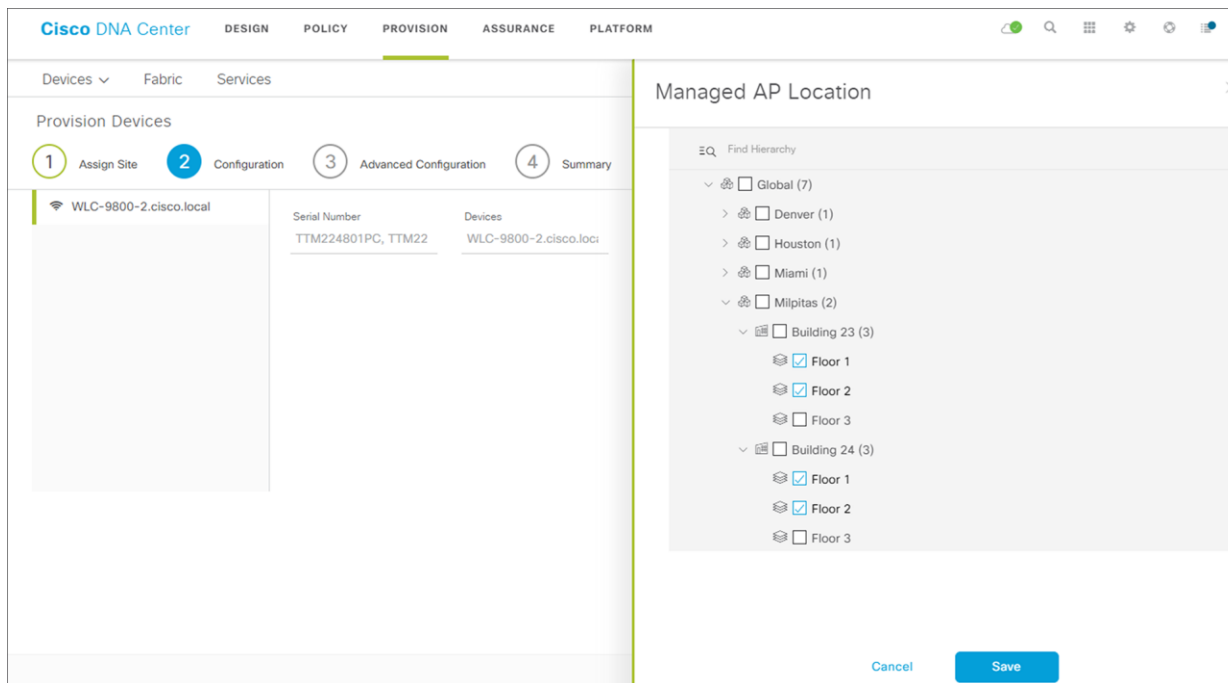


Figure 40.
Enterprise WLC Provisioning Step 2 Configuration

Cisco DNA Center 1.3 supports the ability to configure N+1 redundancy for APs as well as 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 this wireless controller will serve as the primary WLC within the AP high availability configuration. Secondary managed AP locations are sites where this wireless controller will serve as the secondary WLC within the AP high availability configuration. Should the primary WLC or WLC HA SSO pair fail, APs will re-establish CAPWAP connections to this WLC.

For the use case within this deployment guide the Catalyst 9800-40 WLC HA SSO pair (**WLC-9800-2**) will be the primary WLC managing APs within **Floors 1 & 2** on **Buildings 23 & 24**. No secondary managed AP locations will be configured, since the WLC HA SSO pair already provides redundancy in a campus network where all of the APs are operating in a centralized (local) mode deployment.

10. Expand the site hierarchy, select **Floors 1 & 2** under **Building 23** and **Floors 1 & 2** under **Building 24**, and click the **Save** button.

This will close the **Managed AP Location** side panel. Because you have selected this WLC to be an **Active Main WLC**, additional fields will appear within the screen. Since 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**, these will automatically appear. Likewise, since 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 168**, these will also automatically appear.

11. Fill in 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 19. Enterprise WLC settings

Field	Value
SSID Name	lab3employee
Interface Name	employee
VLAN ID	160
IP Address	10.4.160.32
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	168
IP Address	10.4.168.32
Gateway IP Address	10.4.168.1
LAG/Port Number	1
Subnet Mask(in bits)	24

An example is shown in the following figure.

Cisco DNA Center DESIGN POLICY **PROVISION** ASSURANCE PLATFORM

Devices ▾ Fabric Services

Provision Devices

1 Assign Site 2 **Configuration** 3 Advanced Configuration 4 Summary

WLC-9800-2.cisco.local

Serial Number: TTM224801PC, TTM22

Devices: WLC-9800-2.cisco.local

WLC Role:

- ☒ Active Main WLC ⓘ Managing 4 Primary location(s)
- ☐ Guest Anchor Select Secondary Managed AP Locations

Assign Interface

Interface Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
employee	160	10.4.160.32	10.4.160.1	24
guest-dmz	168	10.4.168.32	10.4.168.1	24

Show 10 entries Showing 1 - 2 of 2

Previous 1 Next

Cancel Next

Figure 41.
Enterprise WLC settings

Technical Note: Note that the **guest-dmz** interface is also defined on the enterprise foreign WLC. When the anchor tunnel is up between the enterprise foreign WLC and the guest anchor WLC, guest wireless traffic is automatically terminated on the **guest-dmz** interface of the guest anchor WLC. However, if the anchor tunnel is down, guest wireless traffic is terminated on the **guest-dmz** interface of the enterprise foreign WLC. It is a best practice to specify an isolated Layer 2 VLAN for the **guest-dmz** interface on the enterprise foreign WLC with no DHCP server for supplying 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.

12. Click **Next** to move to **Step 3** in the device provisioning workflow – **Advanced Configuration**.

If you have configured a template within the **Template Editor** 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 WLC HA SSO pair (**WLC-9800-2**).

13. Click **Next** to move to the **Step 4** in the device provisioning workflow – **Summary**.

This screen provides a summary of the configuration which will be provisioned to the Catalyst 9800-40 WLC HA SSO pair (**WLC-9800-2**). An example is shown in the following figure.

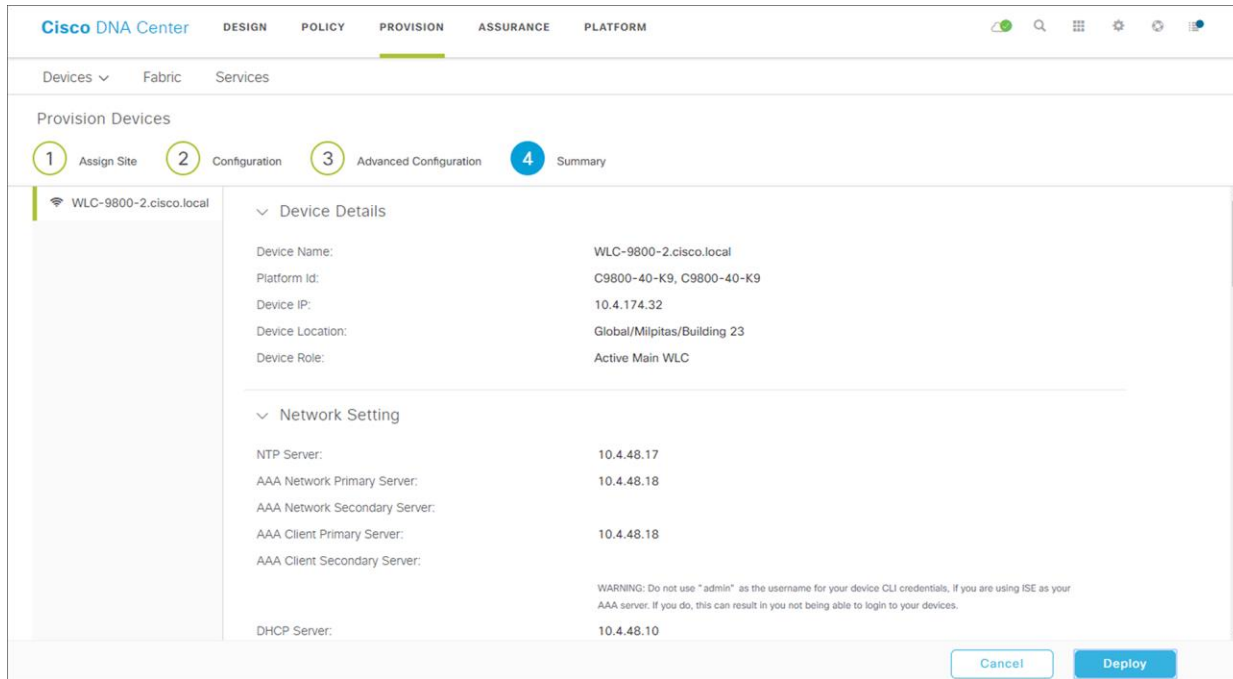


Figure 42.
Device Provisioning – Step 4 Summary

You can expand each section to see the details of the configuration. The configuration is based on the **corporate** wireless profile, created during the Design the wireless network section of this deployment guide.

14. Click **Deploy** to deploy the configuration to the Catalyst 9800-40 WLC HA SSO pair (**WLC-9800-2**).

A side panel will appear, asking if you wish to deploy the configuration now, or schedule it for later.

Technical Note: It is generally a best-practice to make configuration changes and provision new devices onto your network only during scheduled network operations change windows.

15. Select the **Now** radio button and click **Apply** to apply the configuration.

You will be taken back to the inventory screen within **Provisioning**. The provisioning status of the device will temporarily show "Provisioning". It should transition to "Success" after a few minutes. You can click on the **See Details** button directly below the provisioning status of the device, and drill down into the details of what was provisioned for more information.

Cisco DNA Center will dynamically create two new WLAN Profiles within the Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**). Each WLAN profile has a dynamically generated name, based on the SSID name specified within the **corporate** wireless profile, 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 **WLC-9800-2** for this deployment guide.

Table 20. WLAN Profiles dynamically generated by Cisco DNA Center

WLAN Profile Name	SSID	WLAN ID
lab3guest_Global_GA_cb10b955	lab3guest	17
lab3employ_Global_NF_e15bc00b	lab3employee	18

An example of the WLAN configuration, as seen from the web-based GUI of **WLC-9800-2** is shown in the figure below.

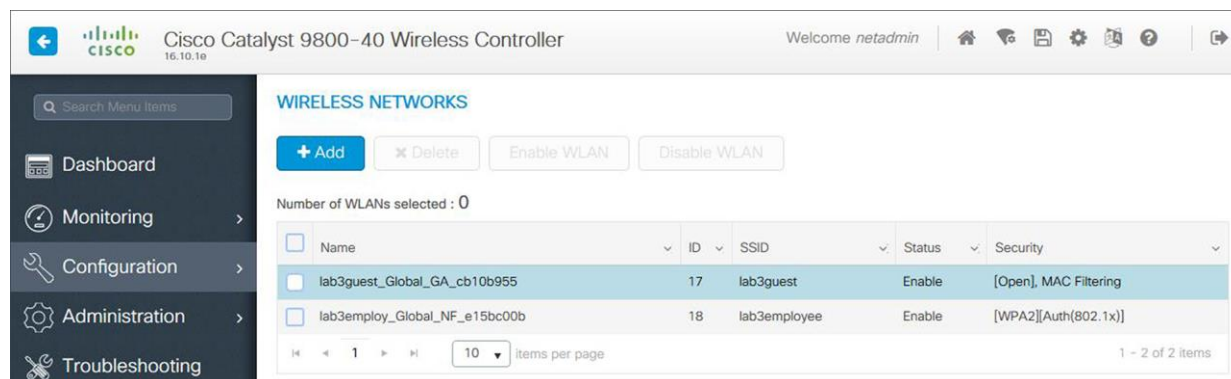


Figure 43.
WLANs / SSIDs dynamically created by Cisco DNA Center

Note that the WLAN IDs corresponding to the two SSIDs - **lab3guest** and **lab3employee** - are 17 and 18, respectively. APs joined to Cisco Catalyst 9800 Series WLCs will broadcast SSIDs of WLANs which have IDs from 1 - 16, when the APs are assigned the Policy Tag named default-policy-tag. In order to avoid creating WLAN IDs which are broadcast with the 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 the **WLC-9800-2**. The names of the new Policy Profiles match the names of the WLAN Profiles created. An example of the configuration, as seen from the web-based GUI of **WLC-9800-2** is shown in the figure below.

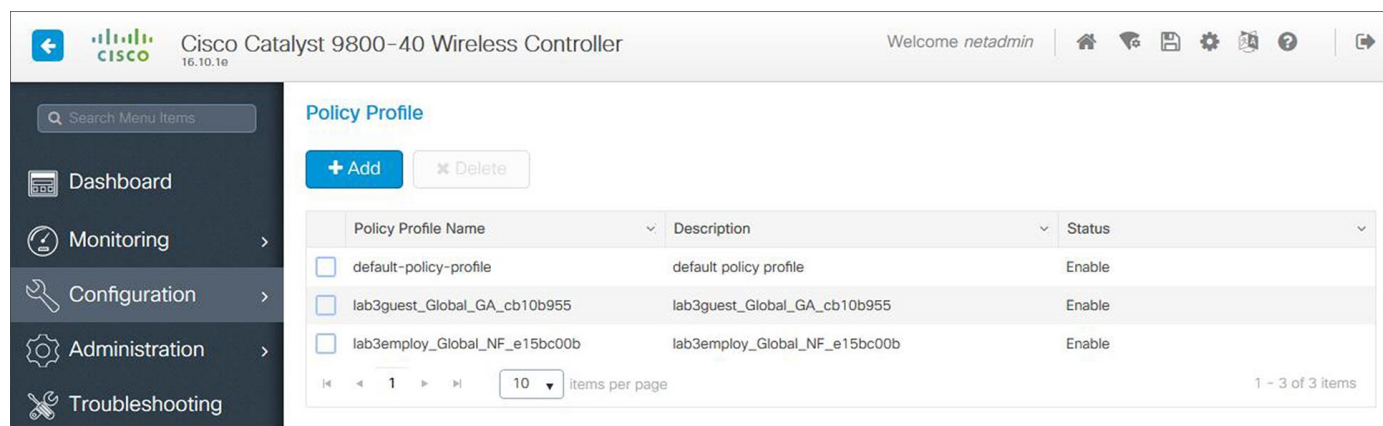


Figure 44.
Example of Catalyst 9800 Policy Profiles created by Cisco DNA Center

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. This will be discussed below, when the APs are provisioned with Cisco DNA Center.

Process: Provision the Catalyst 9800-CL guest anchor WLC

The following steps provision the **corporate** wireless profile created within the Design the wireless network section of this document to the Catalyst 9800-CL guest anchor WLC (**WLC-9800-CL**).

1. From the main Cisco DNA Center dashboard navigate to **Provision**.

This will take you to the main provisioning screen that displays the devices within the inventory. By default, the **Focus:** will be set for **Inventory**.

2. Locate and check the box next to **WLC-9800-CL**.
3. From the drop-down menu under Actions, select **Provision > Provision Device**.

This will take you through a four-step workflow for provisioning the guest anchor WLC (**WLC-9800-CL**), starting with **Step 1 - Assign Site**.

4. Click on the **Choose a Site** button in the middle of the screen.

A side panel will appear, showing the site hierarchy configured for Cisco DNA Center. For this deployment guide, the guest anchor WLC (**WLC-9800-CL**) is assigned to the building level.

5. Expand the site hierarchy under **Milpitas** and select **Building 23**.

An example is shown in the following figure.

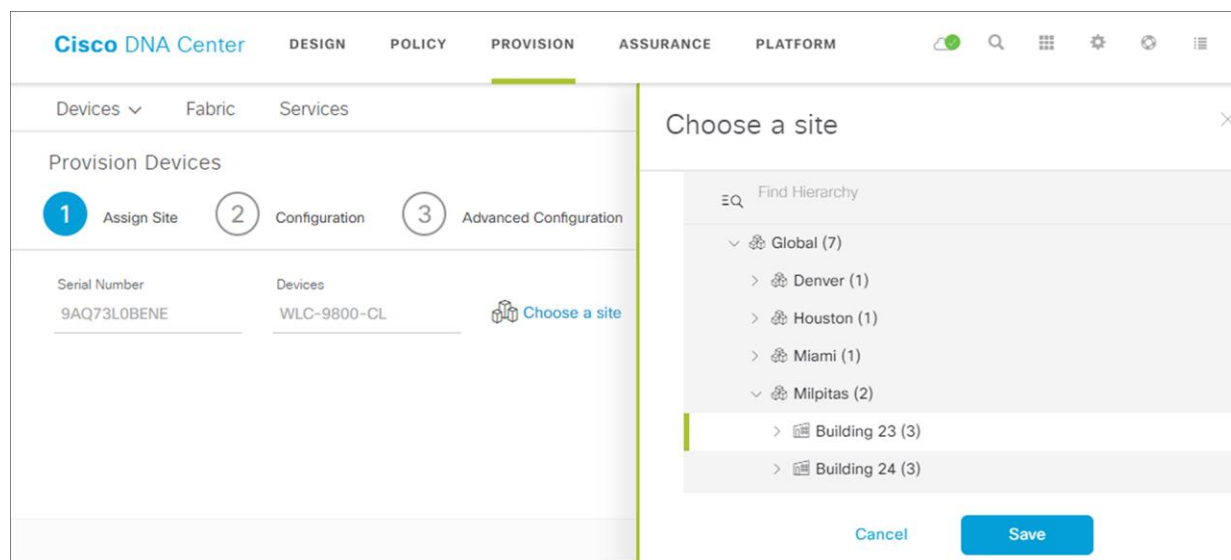


Figure 45.
Guest WLC Provisioning Step 1 - Assign Site

Technical Note: The guest anchor WLC (**WLC-9800-CL**) must be assigned to a building or floor within the Cisco DNA Center site hierarchy. It cannot be assigned to an area (i.e. **Milpitas**) or to the global level of the site hierarchy. Even though **WLC-9800-CL** is assigned to a building (**Building 23** in this deployment guide), APs located on floors in other buildings are supported by the WLC.

6. Click **Save** to assign **WLC-9800-2** to **Building 23**.
7. Click **Next** to move to **Step 2** in the device provisioning workflow - **Configuration**.
8. Within the **Configuration** screen, select the **WLC Role** to be **Guest Anchor**.
9. Click on **Select Anchor Managed AP locations**.

The **Managed AP Location** side panel will appear, showing the site hierarchy for Cisco DNA Center. An example is shown in the following figure.

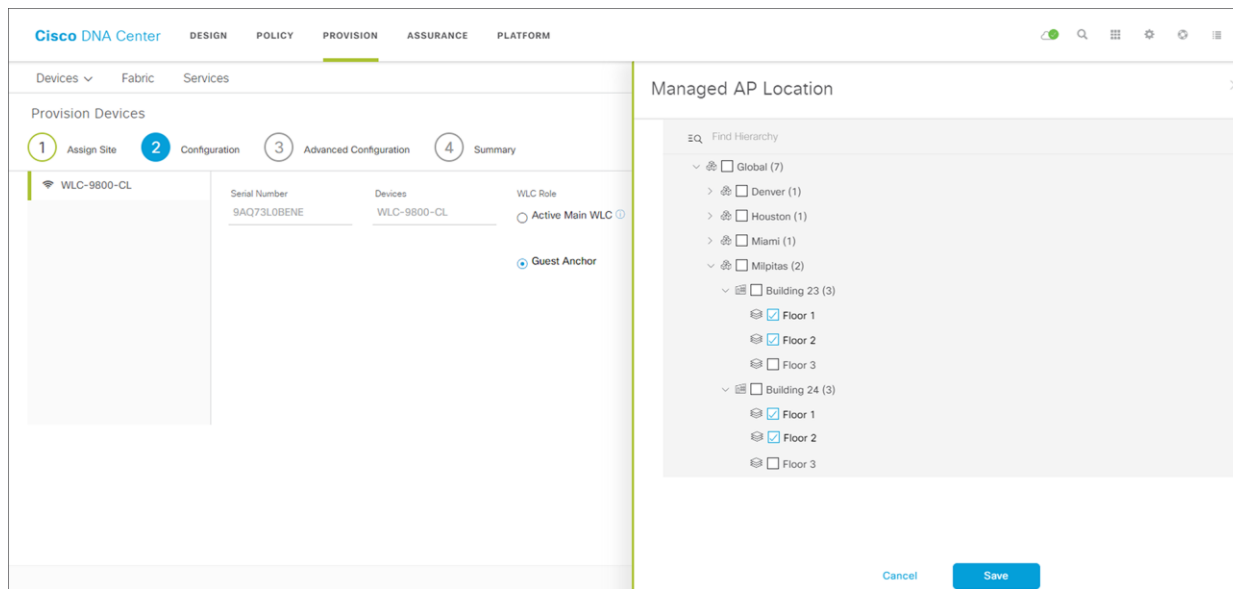


Figure 46.
Guest WLC Provisioning - Step 2 Configuration

For the use case of this deployment guide the guest anchor WLC (**WLC-9800-CL**) will manage APs on **Floors 1 & 2**, in **Buildings 23 & 24**.

10. Expand the site hierarchy, select the desired sites within the site hierarchy, and click the **Save** button.

This will close the **Managed AP Location** side panel. Because you have selected this WLC to be a **Guest Anchor WLC**, additional fields will appear within the screen. Specifically, since 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**, these will automatically appear. However, you must fill in the **IP address**, **Gateway IP address**, **LAG/Port Number** and **Subnet Mask (in bits)** fields.

11. Fill in 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 21. Guest WLC settings

Field	Value
SSID Name	lab3guest
Interface Name	Guest-dmz
VLAN ID	168
IP Address	10.4.168.36
Gateway IP Address	10.4.168.1
LAG/Port Number	1
Subnet Mask(in bits)	24

An example is shown in the following figure.

The screenshot shows the Cisco DNA Center Provisioning interface. The top navigation bar includes tabs for DESIGN, POLICY, PROVISION (active), ASSURANCE, and PLATFORM. Below the navigation bar, there are sections for Devices, Fabric, and Services. The main content area is titled 'Provision Devices' and shows a workflow with four steps: 1. Assign Site, 2. Configuration (active), 3. Advanced Configuration, and 4. Summary. The configuration step is divided into two main sections: 'WLC-9800-CL' and 'Assign Guest SSIDs to DMZ site'. The 'WLC-9800-CL' section shows the Serial Number '9AQ73L0BENE' and the WLC Role 'Guest Anchor' (selected). The 'Assign Guest SSIDs to DMZ site' section shows a table with the following data:

SSID Name	Interface Name	VLAN ID	IP Address	Gateway IP Address	LAG/Port Number	Subnet Mask(in bits)
lab3guest	guest-dmz	168	10.4.168.36	10.4.168.1	N/A	24

At the bottom of the interface, there are 'Cancel' and 'Next' buttons.

Figure 47.
Guest WLC settings

- Click **Next** to move to **Step 3** in the device provisioning workflow - **Advanced Configuration**.

If you have configured a template within the **Template Editor** 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-CL guest anchor WLC (**WLC-9800-CL**).

- Click **Next** to move to **Step 4** in the device provisioning workflow - Summary.

This screen provides a summary of the configuration which will be provisioned to **WLC-9800-CL**. An example is shown in the following figure.

The screenshot shows the Cisco DNA Center interface with the **PROVISION** tab selected. The navigation bar includes **DESIGN**, **POLICY**, **PROVISION**, **ASSURANCE**, and **PLATFORM**. Below the navigation bar, there are tabs for **Devices**, **Fabric**, and **Services**. The main content area is titled **Provision Devices** and shows a progress bar with four steps: **1 Assign Site**, **2 Configuration**, **3 Advanced Configuration**, and **4 Summary**. The **Summary** step is currently active. On the left, a list of devices includes **WLC-9800-CL**. The main panel displays the configuration details for this device, organized into two sections: **Device Details** and **Network Setting**.

Device Details	
Device Name:	WLC-9800-CL
Platform Id:	C9800-CL-K9
Device IP:	10.4.174.36
Device Location:	Global/Milpitas/Building 23
Device Role:	Anchor WLC

Network Setting	
NTP Server:	10.4.48.17
AAA Network Primary Server:	10.4.48.18
AAA Network Secondary Server:	
AAA Client Primary Server:	10.4.48.18
AAA Client Secondary Server:	

At the bottom right of the configuration panel, there are two buttons: **Cancel** and **Deploy**.

Figure 48.
Device Provisioning – Step 4 Summary

You can expand each section to see the details of the configuration. The configuration is based on the **corporate** wireless profile, created during the **Design the wireless network** section of this deployment guide.

14. Click **Deploy** to deploy the configuration to **WLC-9800-CL**.

A side panel will appear, asking if you wish to deploy the configuration now, or schedule it for later.

Technical Note: It is generally a best-practice to make configuration changes and provision new devices onto your network only during scheduled network operations change windows.

15. Select the **Now** radio button and click **Apply** to apply the configuration.

You will be taken back to the inventory screen within **Provisioning**. The provisioning status of the device will temporarily show "Provisioning". It should transition to "Success" after a few minutes. You can click on the **See Details** button directly below the provisioning status of the device, and drill down into the details of what was provisioned for more information.

Cisco DNA Center will dynamically create a new WLAN Profile within the Catalyst 9800-CL guest anchor WLC (**WLC-9800-CL**). The following table shows the name of the WLAN Profile and respective SSID generated by Cisco DNA Center during the provisioning of **WLC-9800-CL** for this deployment guide.

Table 22. WLAN Profiles generated by Cisco DNA Center for the guest anchor WLC

WLAN Profile Name	SSID	WLAN ID
lab3guest_Global_GA_cb10b955	lab3guest	17

The WLAN profile has the same dynamically generated name as the guest profile generated when provisioning the enterprise WLC HA SSO pair (**WLC-9800-2**) in the previous procedure. The name is based on the SSID specified within the **corporate** wireless profile, 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 **WLC-9800-CL** is shown in the figure below.

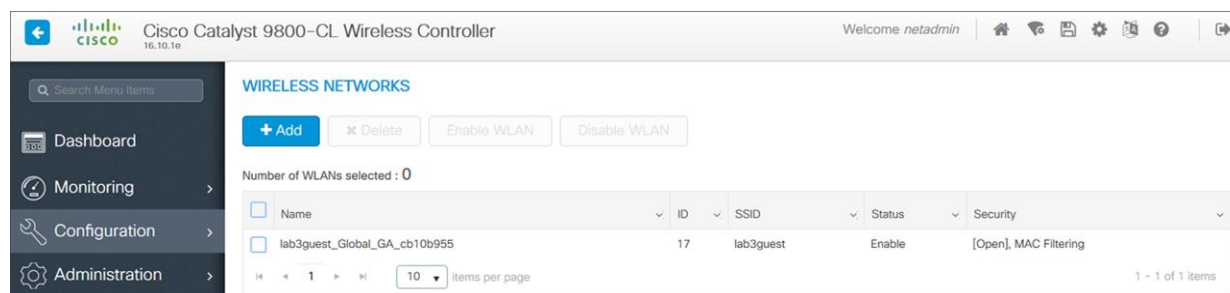


Figure 49.
WLAN / SSID created by Cisco DNA Center for the guest anchor WLC

Note that the WLAN ID corresponding to the **lab3guest** SSID 17. APs joined to Cisco Catalyst 9800 Series WLCs will broadcast SSIDs of WLANs which have IDs from 1 - 16, when the APs are assigned the Policy Tag named **default-policy-tag**. In order to avoid creating WLAN IDs which are broadcast with the **default-policy-tag**, Cisco DNA Center creates WLANs / SSIDs beginning with WLAN ID 17 and higher.

During provisioning, Cisco DNA Center also creates a new Policy Profile within the **WLC-9800-CL**. The name of the new Policy Profile matches the name of the WLAN Profiles created. An example of the configuration, as seen from the web-based GUI of **WLC-9800-CL** is shown in the figure below.



Figure 50.
Example of Catalyst 9800-CL Policy Profile created by Cisco DNA Center

Cisco DNA Center will also provision the mobility tunnel between the enterprise WLC HA SSO pair (**WLC-9800-2**) which functions as the foreign controller, and the guest WLC (**WLC-9800-CL**) which functions as the anchor controller. This is shown in the following two figures below.

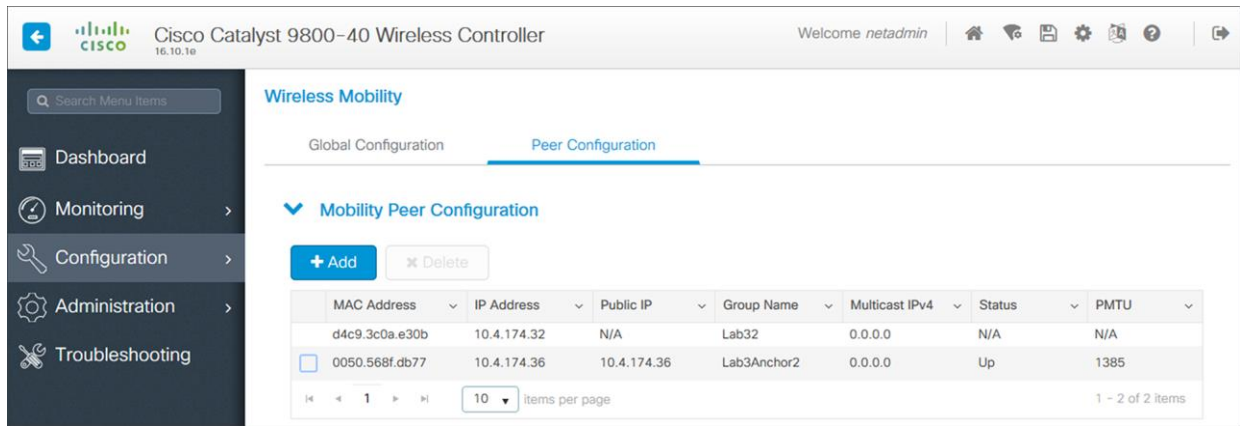


Figure 51.
Mobility tunnel on the foreign controller (WLC-9800-2)

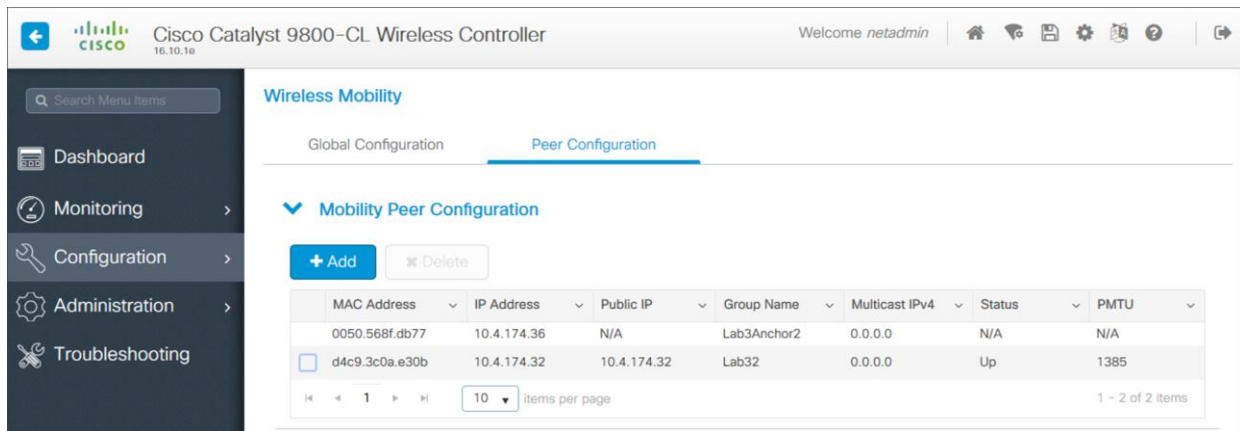


Figure 52.
Mobility tunnel on the anchor controller (WLC-9800-CL)

Clicking on the **lab3guest_Global_GA_cb10b955** Policy Profile within the foreign controller (**WLC-9800-2**), and navigating to the **Mobility Tab**, displays the mapping of the anchor controller (IP address **10.4.174.36**) to the Policy Profile. Again, this is automatically configured by Cisco DNA Center during provisioning. An example is shown in the figure below.

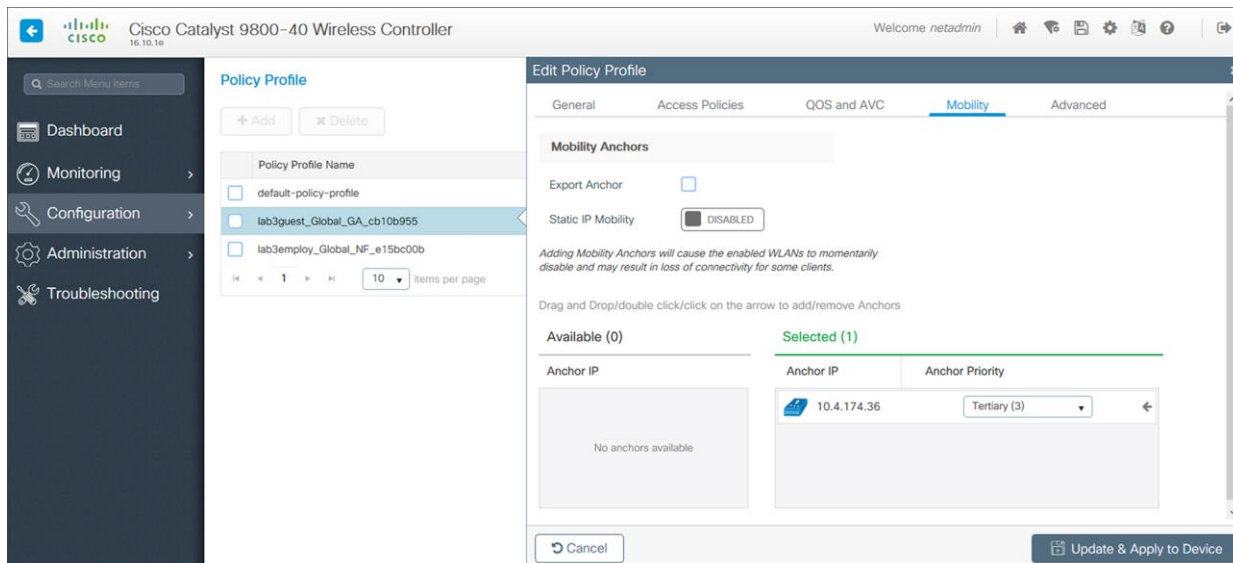


Figure 53.
Foreign controller (WLC-9800-2) guest policy profile with mobility settings

Clicking on the **lab3guest_Global_GA_cb10b955** policy profile within the anchor controller (**WLC-9800-CL**), and navigating to the **Mobility Tab**, displays the export of the anchor controller within the policy profile (similar to the configuration of the anchor and foreign controllers within Cisco AireOS WLCs). Again, this is automatically configured by Cisco DNA Center during provisioning. An example is shown in the figure below.

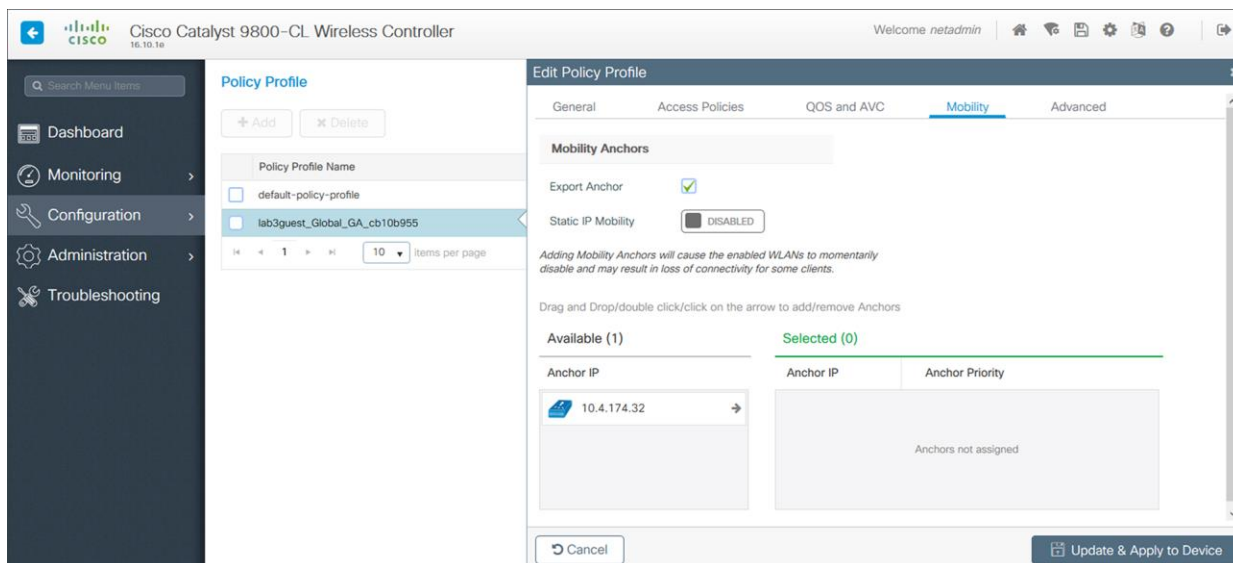


Figure 54.
Anchor controller (WLC-9800-CL) policy profile with mobility settings

Process: Join new APs to the enterprise WLC HA SSO pair (WLC-9800-2)

The use case of this deployment guide assumes new APs which will use IP DHCP Discovery to discover the Catalyst 9800-40 WLC HA SSO pair (**WLC-9800-2**). The new APs are assumed to have never been primed. A Cisco AP has been primed when it has previously joined (established a CAPWAP tunnel) to a WLC and cached the IP address of the WLC in NVRAM; or when primary, secondary, or tertiary WLC management IP addresses have been configured within the AP. In such scenarios, the AP will give preference to the primary, secondary, or tertiary WLC configuration over IP DHCP Discovery.

With IP DHCP Discovery, DHCP servers use Option 43 to provide one or more WLC management IP addresses to the APs. Once an AP learns the management IP address of the Catalyst 9800-40 WLC HA SSO pair (**WLC-9800-2**), it will send a CAPWAP join request message to the WLC. When joined, the WLC manages the APs configuration, firmware, control transactions, and data transactions.

The following are the steps for discovering and joining APs to the enterprise WLC HA SSO pair (**WLC-9800-2**).

1. Configure the necessary VLANs on the Layer 2 access switches that support Cisco APs which will join the Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**).

This deployment guide assumes APs connected to Layer 2 access switches, and a dedicated VLAN on the switches for APs – 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, although it does result in additional VLANs deployed on the switches. An example of the configuration on a Layer 2 access switch is as follows:

```
vlan 102
name AP_management
```

2. Configure the switch ports to which the APs will be connected to be part of the VLAN configured above. Make sure the switch ports are not shutdown.

An example of an interface configuration is as follows:

```
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) associated with the VLAN on which the AP is connected to, 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.**

3. Configure the necessary DHCP relay commands on the upstream Layer 3 devices that support APs which will join the Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**).

An example of the configuration on a Layer 3 switch using a VLAN switched virtual interface (SVI) is as follows:

```
interface Vlan102
ip address 10.4.2.1 255.255.255.0
ip helper-address 10.4.48.10
```

4. Configure the DHCP scopes within the IP DHCP server to return the management IP address of the Catalyst 9800-40 enterprise WLC 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 WLC HA SSO pair (**WLC-9800-2**) configured within DHCP Option 43 is **10.4.74.32**. Configuration of the DHCP scopes within the Microsoft AD server is outside the scope of this document.

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 WLC HA SSO pair (**WLC-9800-2**). The new APs should appear in the Cisco DNA Center inventory, although you may need to wait until the inventory resync interval for **WLC-9800-2** passes. Alternatively, you can manually resync the inventory for the WLC using the following steps.

6. From the main Cisco DNA Center dashboard, navigate to **Provision**.

This will take you to the main provisioning screen that displays the devices within the inventory. By default, the **Focus:** will be set for **Inventory**.

7. Locate and check the box next to **WLC-9800-2**.
8. From the drop-down menu under **Actions**, select **Inventory > Resync Device**.

A pop-up warning will ask you to confirm the resync.

9. Select **OK** to confirm the resync and close the warning.

Process: Provision the new APs

Once the APs have been joined to the Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**), they need to be provisioned. Provisioning with Cisco DNA Center is necessary for APs to receive their correct configuration to advertise the **lab3employee** and **lab3guest** SSIDs. The following table lists the APs which were provisioned for this deployment guide, along with their locations.

Table 23. APs and their locations provisioned within Cisco DNA Center

AP Name	AP Model	Location
AP00F6.6313.B796	AIR-AP2802I-B-K9	Building 23, Floor 1
AP3800_8C14	AIR-AP3802I-B-K9	Building 23, Floor 1
AP0042.68A7.6454	AIR-AP3802I-B-K9	Building 23, Floor 1
APf07f.06d7.0398	AIR-CAP2702I-A-K9	Building 23, Floor 2
AP80e0.1dfd.5b64	AIR-CAP3702I-A-K9	Building 23, Floor 2
AP0462.7366.10f0	AIR-CAP3702I-A-K9	Building 23, Floor 2
AP2800_6C56	AIR-AP2802I-B-K9	Building 24, Floor 1

Technical 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 WLC 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 in provisioning APs within Cisco DNA Center.

1. From the main Cisco DNA Center dashboard navigate to **Provision**.

This will take you to the main provisioning screen that displays the devices within the inventory. By default, the **Focus:** will be set for **Inventory**.

2. Locate and check the boxes next to each of the APs to be provisioned.

For this design and deployment guide, the APs are listed in the table above.

3. From the drop-down menu under Actions, select **Provision > Provision Device**.

This will take you through a four-step workflow for provisioning the APs, starting with **Step 1 - Assign Site**.

4. For each of the APs listed, click on the **Choose a Site** button.

A side panel will appear, showing the site hierarchy configured for Cisco DNA Center.

Expand the site hierarchy under **Milpitas**, then select the building (**Building 23** or **Building 24**) and the floor (**Floor 1** or Floor 2) for each AP.

The building and floor location of each AP is shown in the table above. An example is shown in the following figure.

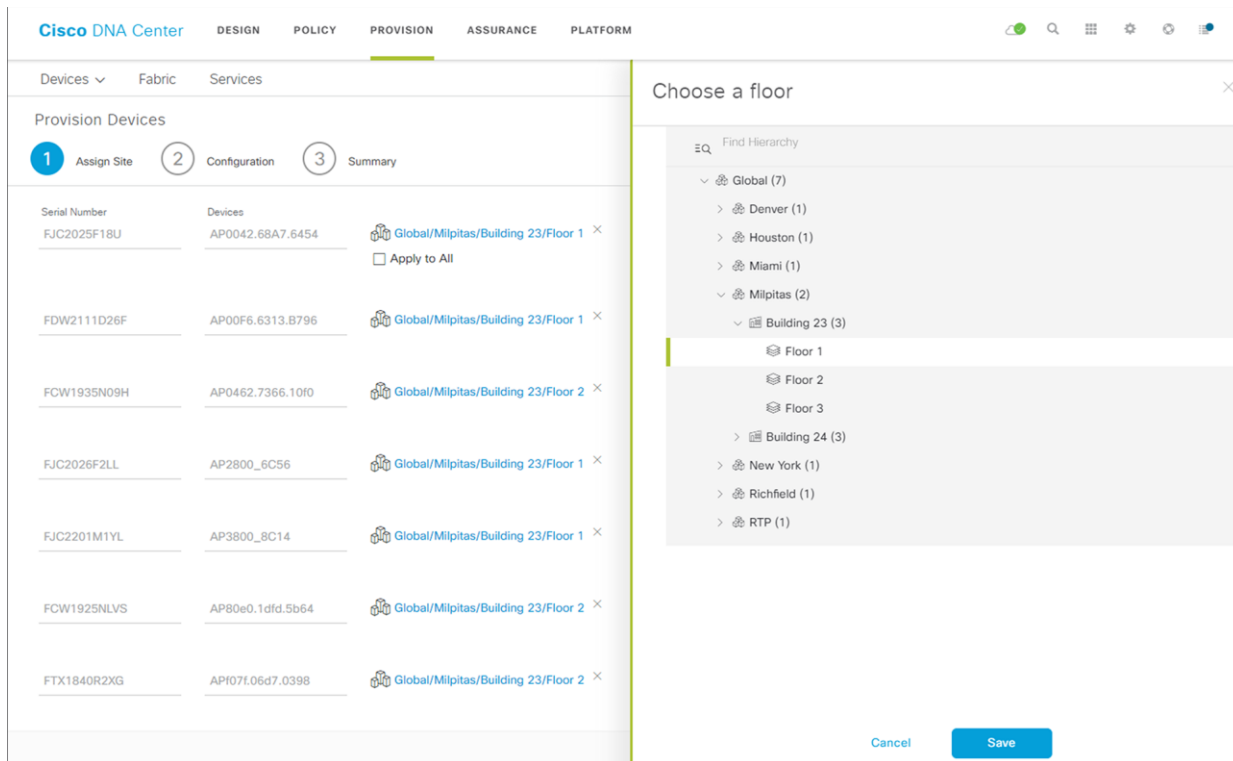


Figure 55.
AP Provisioning Step 1 - Assign Site

5. Click the **Save** button to save the site assignments for the APs.
6. Click the **Next** button to advance to the **Step 2** in the provisioning workflow - **Configuration**.
7. From the drop-down menu under **RF Profile**, select the RF profile to assign to each of the APs.

For this deployment guide the **TYPICAL** RF profile was selected. This RF profile was also selected as the default RF profile within the design section of this deployment guide. An example is shown in the following figure.

The screenshot displays the Cisco DNA Center interface for provisioning devices. The top navigation bar includes tabs for DESIGN, POLICY, PROVISION (active), ASSURANCE, and PLATFORM. Below the navigation bar, there are tabs for Devices, Fabric, and Services. The main section is titled 'Provision Devices' and shows a progress indicator with three steps: 1. Assign Site, 2. Configuration (current step), and 3. Summary. The table below lists the devices being provisioned, with columns for Serial Number, Device Name, and RF Profile. All devices have the 'TYPICAL' RF profile assigned. A checkbox for 'Apply to All' is present. At the bottom right, there are 'Cancel' and 'Next' buttons.

Serial Number	Device Name	RF Profile
FJC2025F18U	AP0042.68A7.6454	TYPICAL
FDW2111D26F	AP00F6.6313.B796	TYPICAL
FCW1935N09H	AP0462.7366.10f0	TYPICAL
FJC2026F2LL	AP2800_6C56	TYPICAL
FJC2201M1YL	AP3800_8C14	TYPICAL
FCW1925NLVS	AP80e0.1dfd.5b64	TYPICAL
FTX1840R2XG	APf07f.06d7.0398	TYPICAL

Figure 56.
AP Provisioning Step 2 - Configuration

8. Click the **Next** button to advance to the **Step 3** in the provisioning workflow - **Summary**.

The **Summary** screen will provide a summary of the configuration which will be provisioned to each the APs. An example is shown in the following figure.

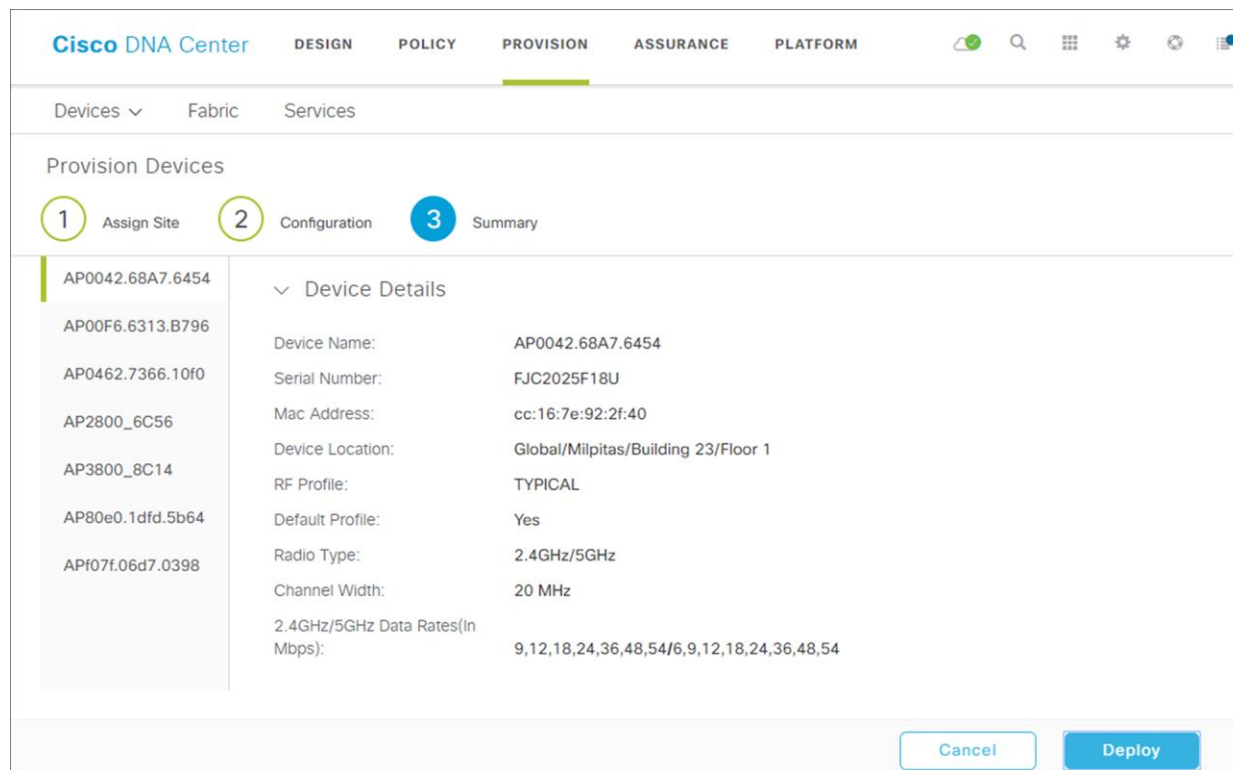


Figure 57.
AP provisioning Step 3 Summary

9. Click the **Deploy** button to provision the APs.

A side panel will appear, asking if you wish to deploy the configuration now, or schedule it for later.

Technical Note: It is generally a best-practice to make configuration changes and provision new devices onto your network only during scheduled network operations change windows.

10. Select the **Now** radio button and click **Apply** to apply the configuration.

A **Success** pop-up screen should appear, with additional text indicating that after provisioning the APs will reboot.

11. Click **OK** to confirm.

This will return you to the list of inventory within the main **Provisioning** screen. The provisioning status of the APs will temporarily show "Provisioning". They should transition to "Success" after a few minutes. You can click on the **See Details** button directly below the provisioning status of each AP, and drill down into the details of what was provisioned for more information.

Cisco DNA Center will create a new Policy Tag within the Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**) for each floor which contains APs that are provisioned. An example is shown in the figure below.

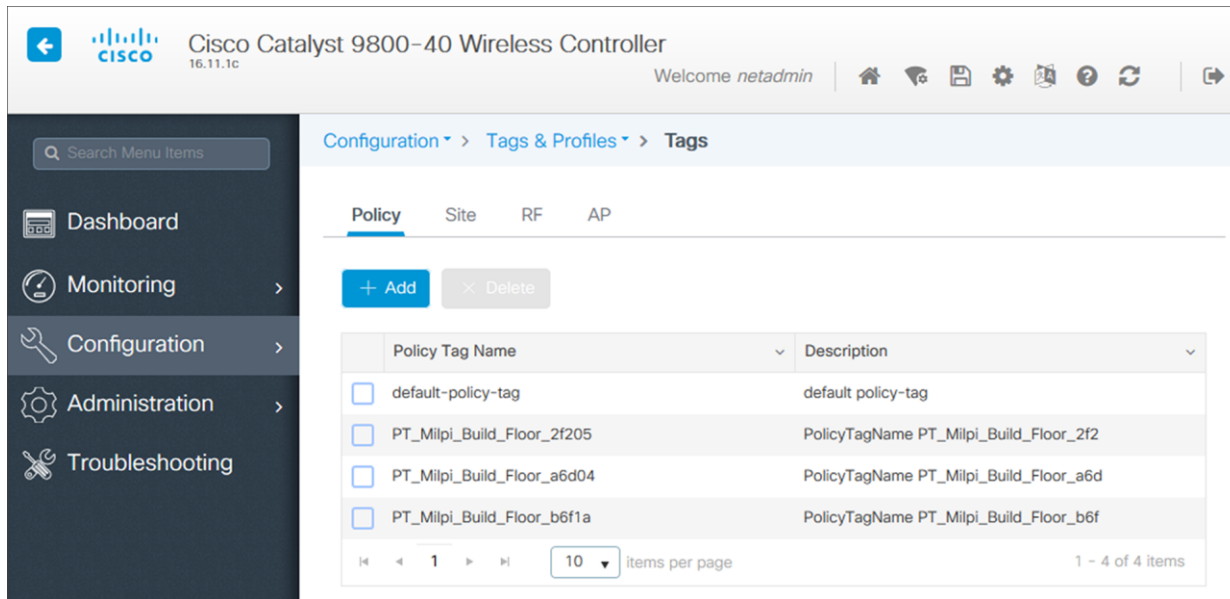


Figure 58.
Policy Tags created by Cisco DNA Center within the Catalyst 9800-40 enterprise WLC

In the figure above, three new Policy Tags have been created, corresponding to the APs provisioned on **Floors 1 & 2 of Building 23**, and **Floor 1 of Building 24**. Each policy tag is unique to a site - meaning a specific floor within a building. Because no APs have been provisioned to **Floor 2 of Building 24**, no new Policy Tag has been created for this floor, yet. 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 which are added to the new Policy Tag by Cisco DNA Center. An example is shown in the figure below.

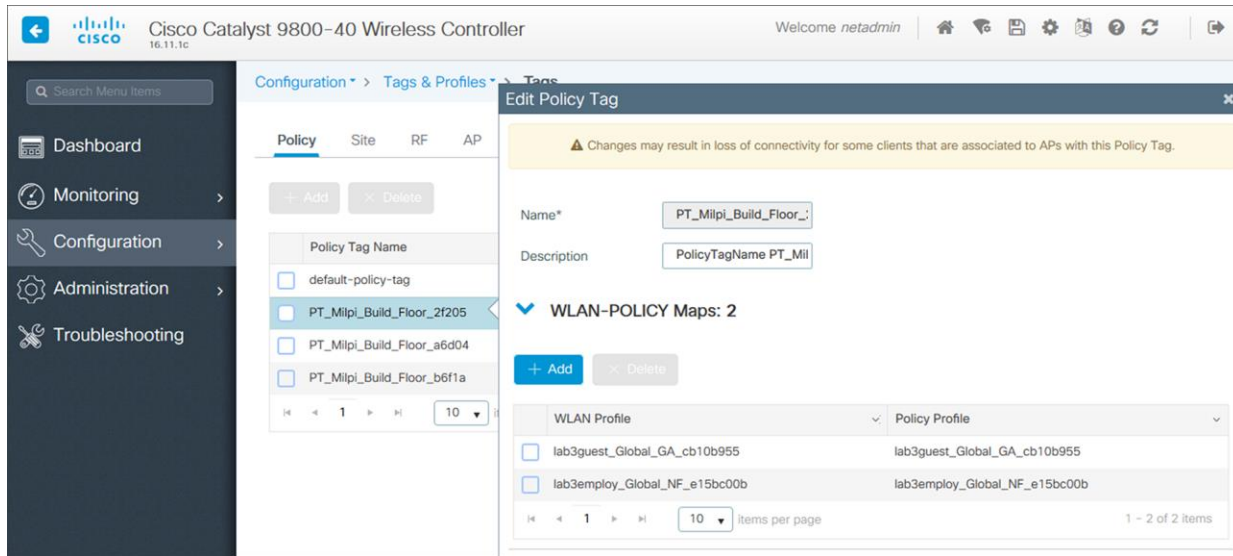


Figure 59.
Policy Tag details

As can be seen, the WLAN Profiles and the Policy Profiles created during the provisioning of the Catalyst 9800-40 enterprise WLC HA SSO pair have been added to each of the Policy Tags. This is controlled by the **corporate** WLAN profile created within Cisco DNA Center within the **Design** section of this design and deployment guide. The **corporate** WLAN profile specified the **lab3employee** and **lab3guest** SSIDs to be broadcast throughout the **Milpitas** area (**Floors 1 - 3 of Buildings 23 & 24**).

During the AP provisioning process, the TYPICAL RF Profile was selected. Cisco DNA Center creates a new RF Tag named **TYPICAL** within the Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**). An example is shown in the following figure.

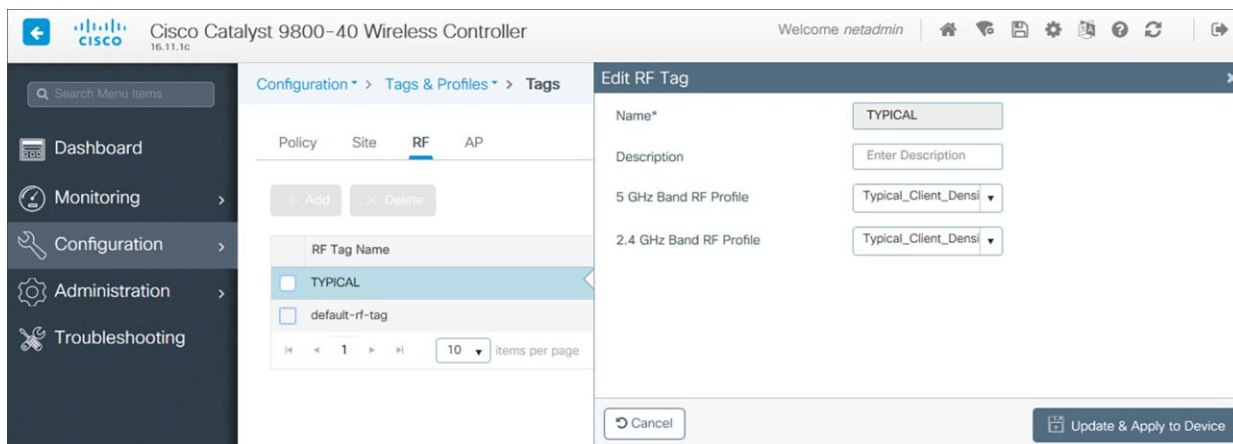


Figure 60.
TYPICAL RF Tag created by Cisco DNA Center

Finally, Cisco DNA Center statically assigns a Policy Tag (specific to each floor), the RF Tag (named **TYPICAL** since this was the only RF Profile specified during AP provisioning), and the default Site Tag (named **default-site-tag**) to each AP, within the Catalyst 9800-40 enterprise WLC HA SSO pair (**WLC-9800-2**). The **default-site-tag** contains the default AP Join Profile named **default-ap-profile**. Cisco DNA Center does not currently generate specific Site Tags or specific AP Join Profiles based upon the configuration within the provisioning of Catalyst 9800 Series WLCs or APs.

An example of the static assignment of the Policy Tag, Site Tag, and RF Tag to each AP is shown in the following figure.

The screenshot shows the Cisco Catalyst 9800-40 Wireless Controller configuration page. The breadcrumb navigation is Configuration > Tags & Profiles > Tags. The 'AP' tab is selected under the 'Tag Source' section. The 'Static' tab is active, showing a table of APs with their assigned tags. The table has columns for AP MAC Address, Policy Tag Name, Site Tag Name, and RF Tag Name. There are 7 items displayed, with 10 items per page.

AP MAC Address	Policy Tag Name	Site Tag Name	RF Tag Name
0042.68a7.6454	PT_Milpi_Build_Floor_2f205	default-site-tag	TYPICAL
00a7.4298.8c14	PT_Milpi_Build_Floor_2f205	default-site-tag	TYPICAL
00f6.6313.b796	PT_Milpi_Build_Floor_2f205	default-site-tag	TYPICAL
0462.7366.10f0	PT_Milpi_Build_Floor_b6f1a	default-site-tag	TYPICAL
80e0.1dfd.5b64	PT_Milpi_Build_Floor_b6f1a	default-site-tag	TYPICAL
cc16.7edb.6c56	PT_Milpi_Build_Floor_a6d04	default-site-tag	TYPICAL
f07f.06d7.0398	PT_Milpi_Build_Floor_b6f1a	default-site-tag	TYPICAL

Figure 61.
Static assignment of tags to APs by Cisco DNA Center

The assignment of the Policy Tag to the AP is what 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.

Process: Position the new APs on the floor map

You will need to position the newly discovered APs within the floor maps for each of the buildings and floors within Cisco DNA Center.

1. From the main Cisco DNA Center dashboard navigate to **Design > Network Hierarchy**.
2. Expand the network hierarchy in the panel on the left side of the screen and select **Milpitas > Building 23 > Floor 1**.

This should display the floor plan for **Floor 1**.

3. Click **Edit** to edit the floor plan.

This will bring up a new side panel, allowing you to edit various aspects of the floor plan. An example is shown in the following figure.

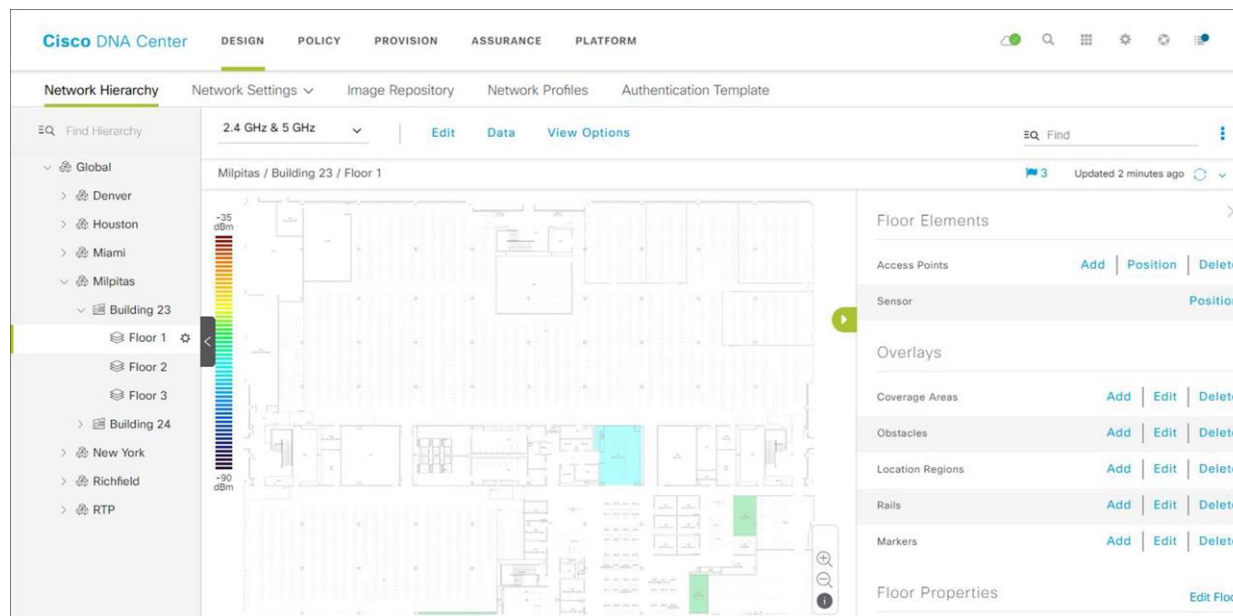


Figure 62.
Edit the floor plan

4. Within the **Floor Elements** section, locate **Access Points**, and click on **Position**.

This will change the floor map to display APs which have not been positioned. The newly discovered APs from the previous process will appear in the upper right corner of the floor map.

5. Click on an AP, drag it to the correct location on the floor map, and release it.

The floor map will again change, showing additional details about the position of the AP on the floor map. An example is shown in the following figure.

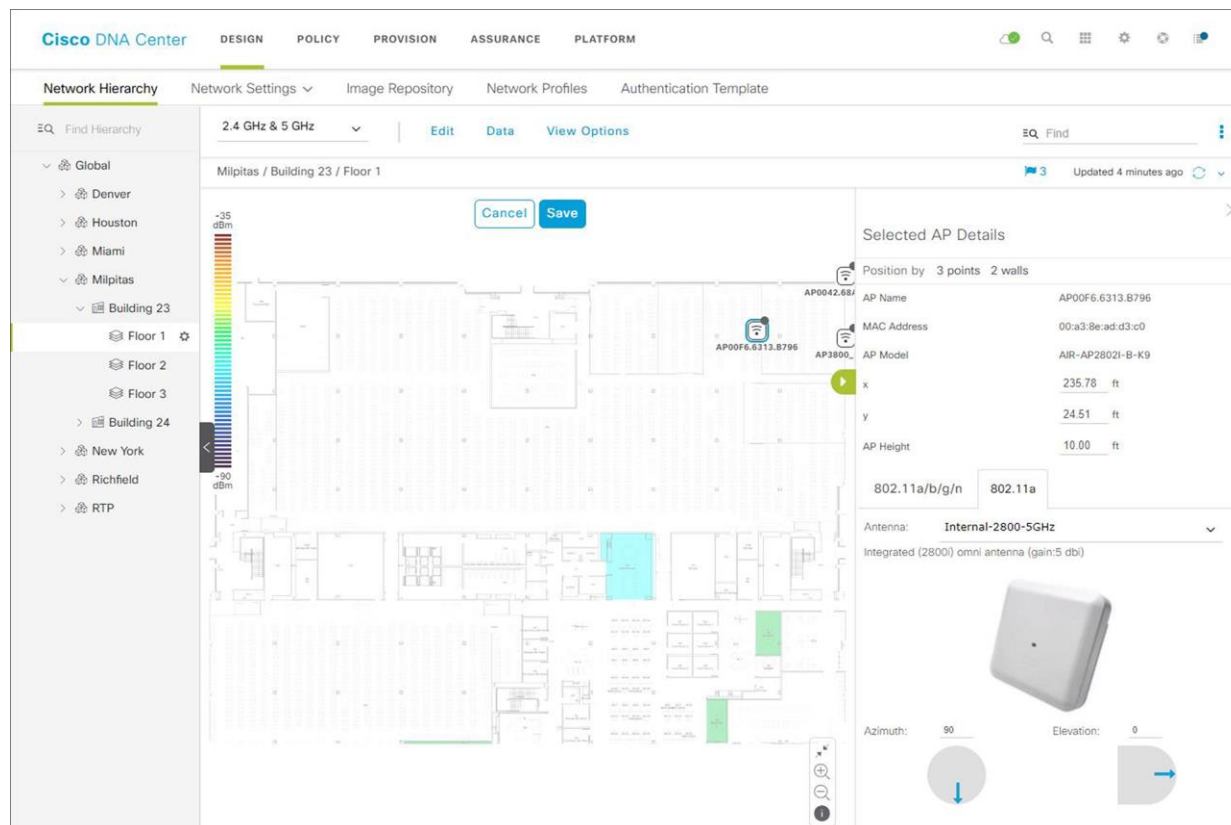


Figure 63.
Place APs on the floor map

You may need to select the antenna for the AP, depending upon the model of AP which you are positioning. This will be indicated by a red error warning appearing above the floor plan when placing the AP.

6. If necessary click on the **802.11a/b/g/n** tab to display the **Antenna**, **Azimuth**, and **Elevation** settings.
7. From the drop-down menu, next to **Antenna**, select the antenna type for the AP being positioned.

For this design and deployment guide, internal antennas were used on all APs.

8. Repeat **Steps 6 - 7** with the **802.11a** tab.

You can fine tune the position and adjust the AP height, once it is placed on the floor map. The AP height will by default be set based upon the height of the floor which you specified when you imported the floor map. You can also adjust the **Azimuth** and **Elevation** settings of the antennas or for APs with integrated antennas, the **Azimuth** and **Elevation** of the AP.

9. Repeat **Steps 1 - 8** for the remaining APs on the floor.
10. Click on **Save** to save the positioning of the APs on the floor map.

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.

11. Optionally click **Edit** again, to edit the floor plan.
12. Within the **Overlays** section you can optionally add **Coverage Areas**, **Obstacles**, **Location Regions**, **Rails** and **Markers** to further tune the floor plan to more accurately reflect the RF characteristics of the actual floor.

An example is shown in the figure below. Note that only the 5 GHz heat maps have been selected for display in the figure.

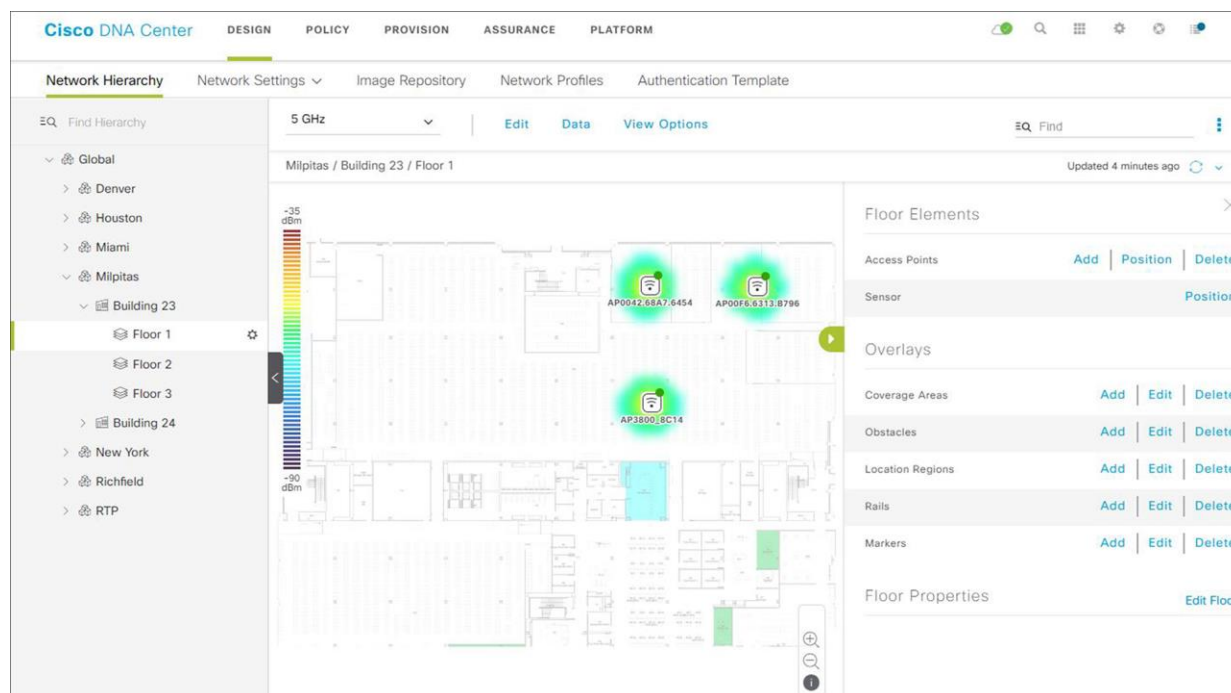


Figure 64.
Editing a floor plan to add overlays

13. Repeat **Steps 1 - 12** for the APs on the other floors.

Operate the wireless network

This section of the design and deployment guide briefly discusses how Cisco DNA Assurance can be used to monitor and troubleshoot the WLAN deployment. Cisco DNA Assurance provides the ability to monitor the health of Cisco WLCs, access points, and wireless clients.

The following processes are discussed:

- Network Assurance for troubleshooting RF issues on APs.
- Client Assurance for monitoring wireless clients.

This section of the deployment guide assumes that Optimal Telemetry is enabled for the WLCs within the Telemetry section of Cisco DNA Center.

Process: Network Assurance for troubleshooting RF issues on APs

The following is an example of the use of Network Assurance to troubleshoot RF issues on APs.

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

For example: <https://<Cisco DNA Center IPaddr or FQDN>>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

2. From the main Cisco DNA Center dashboard navigate to **Assurance**.

This will take you to the **Overall Health** dashboard within Cisco DNA Assurance. An example is shown in the following figure.

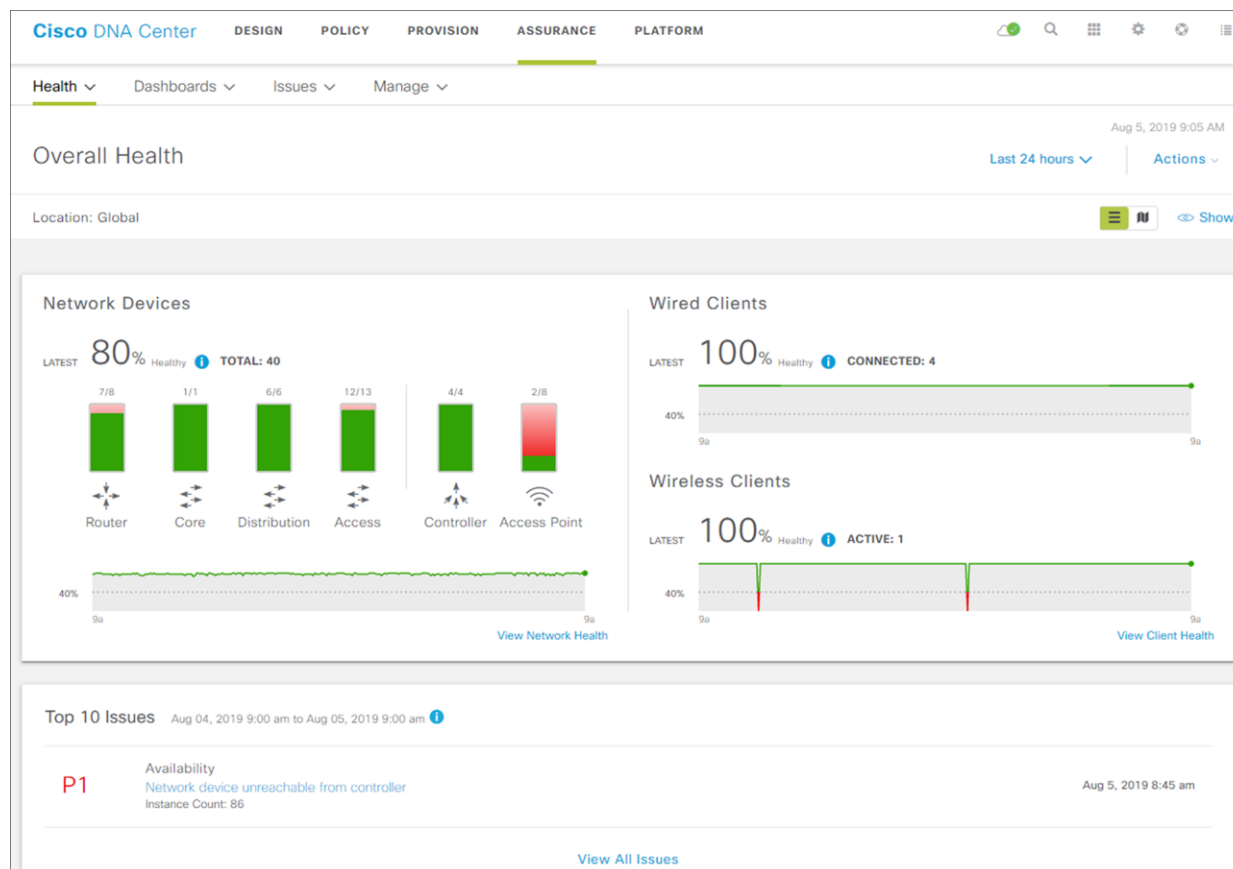


Figure 65.
Cisco DNA Assurance Overall Health dashboard

The **Network Devices** panel within **Overall Health** dashboard can be used to quickly identify the health of WLCs (Controllers) and Access Points. For example, in the figure above it can be seen that there are four WLCs (Controllers), and that the overall health of all four controllers is solid green - indicating good health. It can also be seen that there are eight Access Points (APs) connected to the WLCs. Two APs are showing a health of solid green - indicating good health. The other APs are showing a health of red indicating degraded health.

3. Within the Network Devices panel, click on **View Network Health** to drill down into the **Network Health** dashboard.

An example of the Network Health dashboard is shown in the figure below.

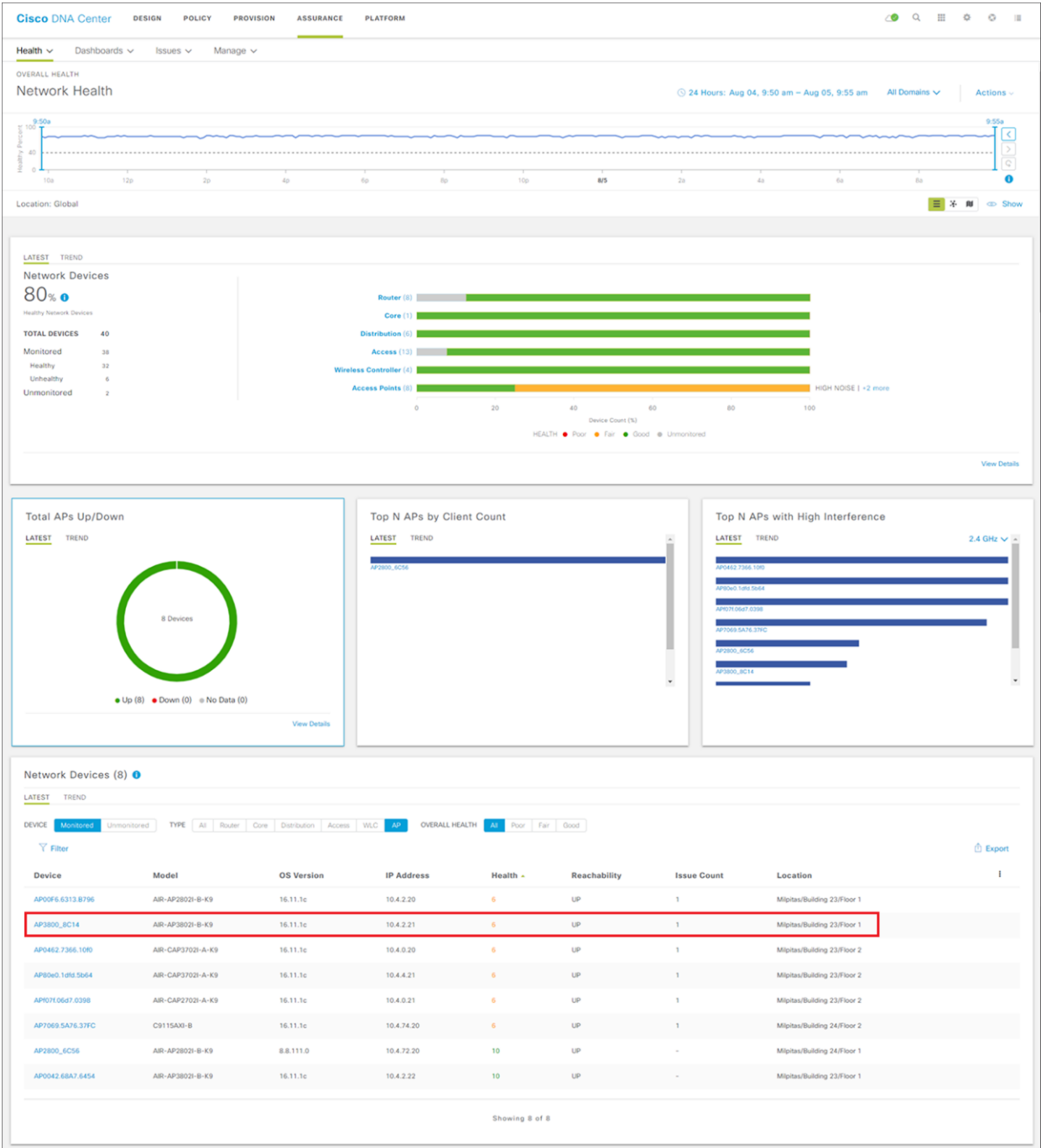


Figure 66.
Network Health dashboard

From the panels within the Network Health dashboard, you can quickly determine that **AP3800_8C14** is one of the APs with a degraded health score (6 of 10).

4. Click on **AP2800_8C14** in the bottom panel of the **Network Health** dashboard.

This will take you to the **Device 360** dashboard for the AP. The top panel of the **Device 360** dashboard presents a timeline of the overall health score of the device. By default, the timeline is over the previous 24 hours.

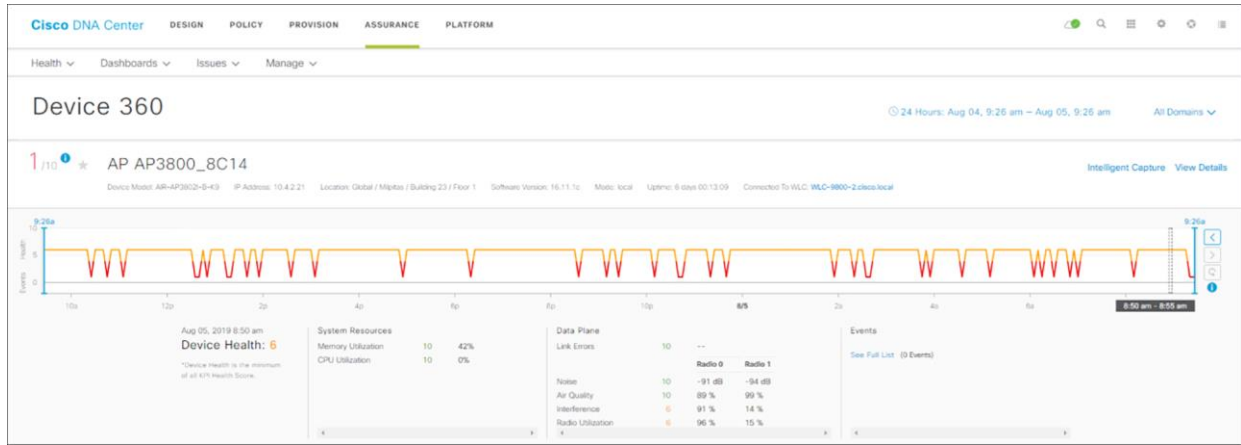


Figure 67.
Device 360 dashboard top panel

5. Hover your cursor over a section of the timeline.

Under the timeline you will see details regarding how the overall score of the AP is determined for that particular time. For example, in the figure above, it can be seen that the overall health score of the device is based on the score for **System Resources** and the score for **Data Plane**. The score for **System Resources** is based on two factors - **Memory Utilization** and **CPU Utilization**. From the figure above, it can be seen that the health score for both of these factors is **10** (highlighted in green), visually indicating a good score. The score for **Data Plane** is based on four factors - **Noise**, **Air Quality**, **Interference**, and **Radio Utilization**. From the figure above, it can be seen that the health scores for **Noise** and **Air Quality** are both **10** (highlighted in green), visually indicating a good score. However, the health scores for **Interference** and **Radio Utilization** are both **6** (highlighted in orange), indicating a fair score. Additionally, the **Interference** (in percentage) and **Radio Utilization** (in percentage) for each of the radios is listed next to the score. This provides valuable insight as to the cause of the degraded health score of the AP, as well as in which band the **Interference** and **Radio Utilization** are occurring.

The overall health score for the device is based on the lowest score of any one of the factors under **System Resources** or **Data Plane**. As can be seen from the figure above, since the both **Interference** and **Radio Utilization** have a score of **6** for the particular time selected in the timeline above - the overall health of the AP is given a score of **6** for that time.

6. At the bottom of the Device 360 dashboard, select the **RF tab** under **Detailed Information**.

This will provide you with graphical timelines of the **Noise**, **Air Quality**, **Interference**, and **Utilization** of each radio over the last 24 hours by default. An example is shown in the following figure.



Figure 68.
Device 360 dashboard - Device Details - RF tab

The graphical timeline can be used to determine if the **Interference** and **Radio Utilization** are transient – meaning that it only occurs during certain times of the day for a limited time – or if they are continuous. As can be seen from the graph above, the Interference and Noise for Radio 0 – which corresponds to the 2.4 GHz band – is more or less continuous.

Technical Note: The Cisco DNA Center Assurance data presented here within this design and deployment guide is from a lab environment with multiple APs. Therefore, the amount of RF interference and noise are expected to be high, particularly within the 2.4 GHz band, since there are only 3 non-overlapping channels in this band.

Process: Client Assurance for monitoring wireless clients

The following is an example of the use of Client Assurance to monitor wireless clients.

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

For example: <https://<Cisco DNA Center IPAddr or FQDN>>. The credentials (userid and password) you enter must have SUPER-ADMIN-ROLE OR NETWORK-ADMIN-ROLE privileges.

2. From the main Cisco DNA Center dashboard navigate to **Assurance**.

This will take you to the **Overall Health** dashboard within Cisco DNA Assurance. An example is shown in the following figure.

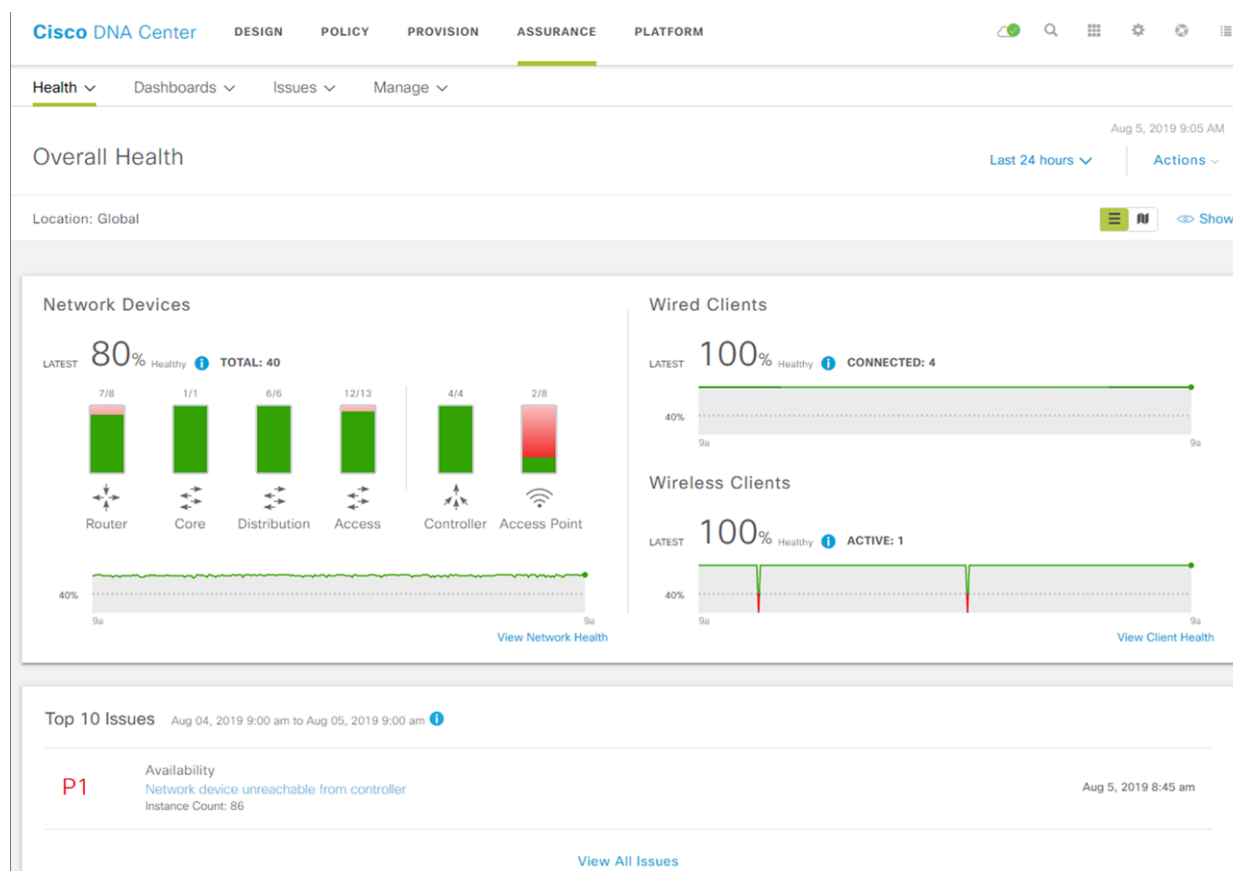


Figure 69.
Cisco DNA Assurance Overall Health dashboard

The **Wireless Clients** panel within the **Overall Health** dashboard provides a historical graph of the overall health of all wireless clients, as well as a count of the current number of active wireless clients.

3. Within the **Wireless Clients** panel, click on **View Client Health** to drill down into the **Client Health** dashboard.

An example of the top two panels within **Client Health** dashboard is shown in the figure below.

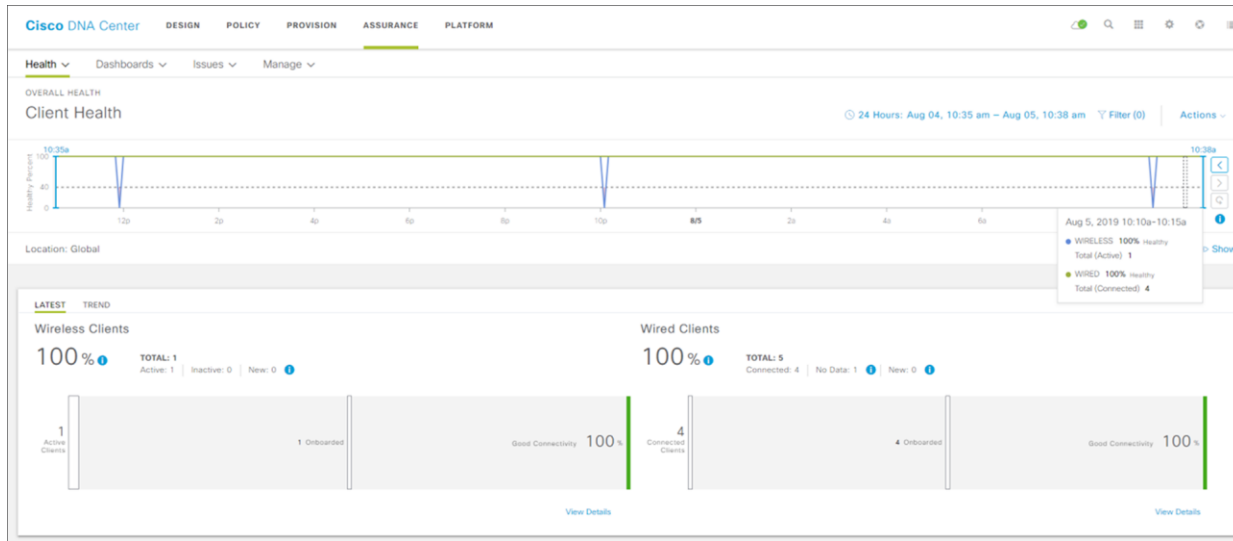


Figure 70.
Client Health dashboard – top two panels

The top panel of the **Client Health** dashboard presents a timeline of the overall health score of the all wireless devices. By default, the timeline is over the previous 24 hours.

4. Hover your cursor over a section of the timeline.

The pop-up menu, shown in the figure above, provides you a quick overview of the number of connected wired and wireless devices for that point in time, as well as the overall percentage of healthy devices.

The second panel separates information between wireless and wired clients. For wireless clients, it provides additional information regarding the number of currently active vs. inactive clients.

5. Scroll down to the next set of panels.

The next set of panels provides even more detailed monitoring information regarding wireless clients on your network. An example is shown in the figure below.

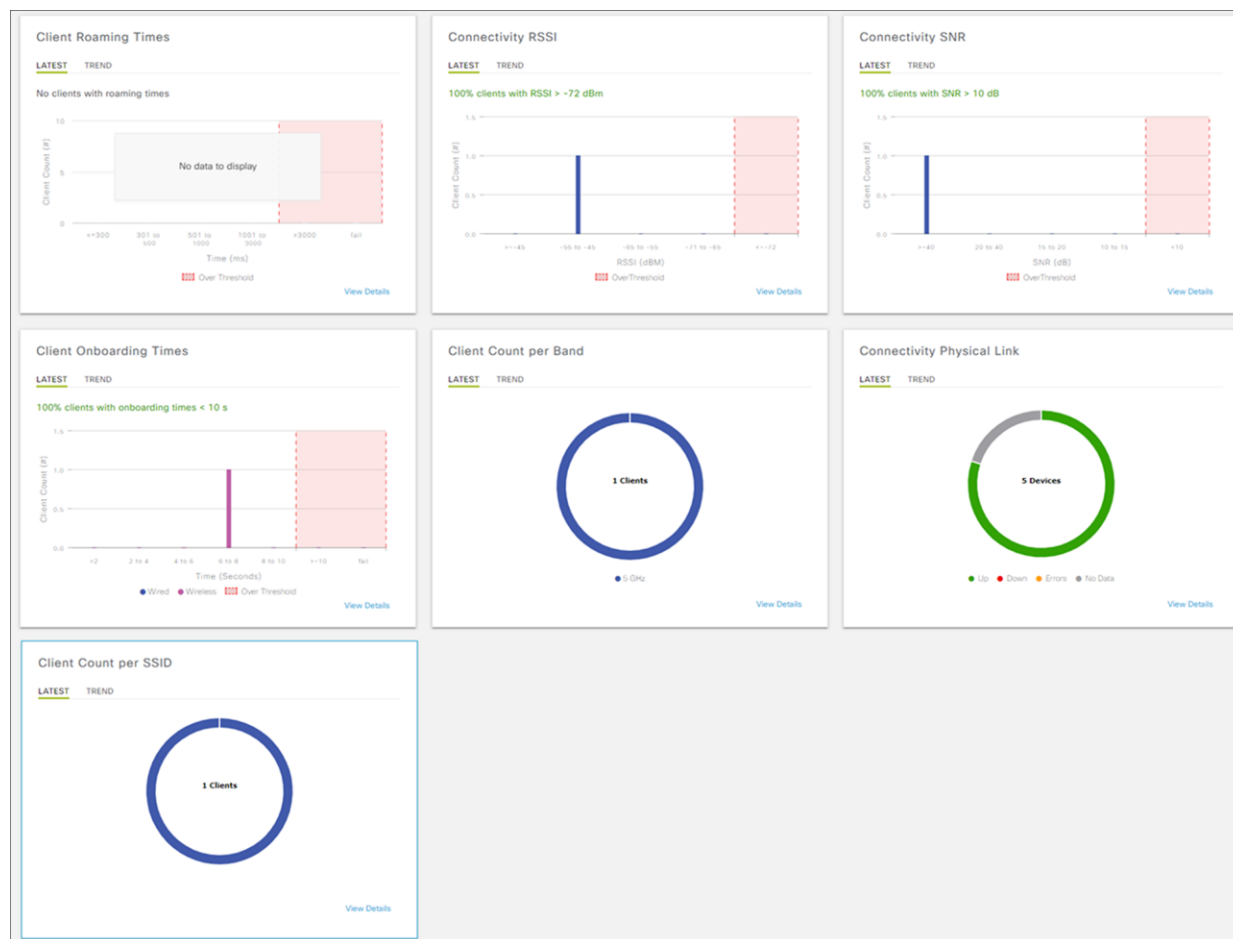


Figure 71.
Client Health dashboard - middle panels

The middle panels of the **Client Health** dashboard provide the following information:

- **Client Roaming Times** – This provides a distribution graph regarding how long wireless clients have been taking to complete roaming from one AP to another AP. There is a pre-configured **Over Threshold** limit of 10 seconds, displayed on the graph, to quickly give you a visual indication of potential roaming time issues.

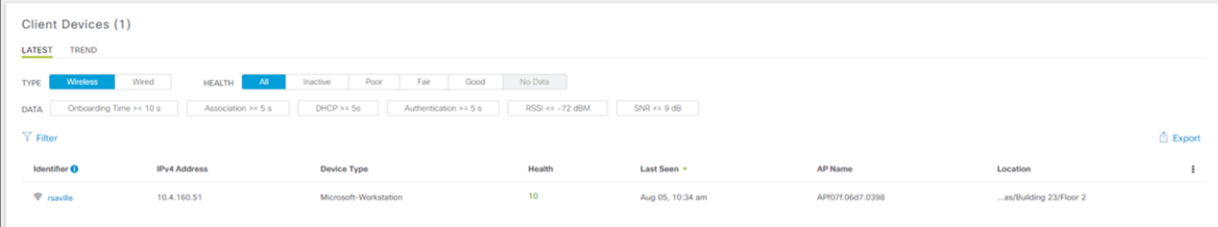
Technical Note: If no roaming has occurred within the network, no data will be displayed. The example shown in the figure above was taken from a lab network in which wireless clients were not roaming.

- **Connectivity RSSI** – This provides a distribution graph of the signal strengths of the wireless clients, as seen from the APs they are connected to. There is a pre-configured **Over Threshold** value of -72 dBm, displayed on the graph. Wireless clients seen with a signal strength less than or equal to -72 dBm will be counted here. This provides you with a quick visual indication of possible RF dead spots or **sticky clients** (**clients that don't roam** to a new AP despite low RSSI values) within your network.
- **Connectivity SNR** – This provides a distribution graph of the signal to noise ratio of the wireless clients, as seen from the APs they are connected to. There is a pre-configured **Over Threshold** value of greater than 10 dB, displayed on the graph. Wireless clients seen with a signal to noise ratio less than 10 dB will be counted here. This provides you with a quick visual indication of possible RF noise issues within your network.
- **Client Onboarding Times** – This provides a distribution graph of the amount of time wireless clients are taking to onboard to the network. Wired and wireless clients are individually color-coded. For wireless clients, onboarding time includes the time taken to associate with the AP, receive an IP address (when using DHCP), and to authenticate to the network. There is a pre-configured **Over Threshold** limit of 10 seconds, displayed on the graph, to quickly give you a visual indication of potential onboarding issues.
- **Client Count per Band** – This provides a quick visual indication of the number of wireless clients per band (2.4 GHz or 5 GHz). Hovering over each of the colors in the circular graph causes a pop-up tag to appear with the band and the number of clients corresponding to that particular color.
- **Connectivity Physical Link** – This provides a quick visual indication of the number wired clients which have physical connectivity currently **Up**, **Down**, **With Errors** (in an error state), or **No Data**. Hovering over each of the colors in the circular graph causes a pop-up tag to appear with the connectivity state and the number of clients corresponding to that particular state.
- **Client Count per SSID** – This provides a quick visual indication of the number of wireless clients per SSID. Hovering over each of the colors in the circular graph causes a pop-up tag to appear with the SSID name, and the number of clients associated to that particular SSID.

For each of the graphs, either the latest sample data or the trend over time can be displayed.

6. Scroll down to the bottom panel.

The last panel provides information regarding individual wired and wireless clients. An example is shown in the following figure.



The screenshot shows a dashboard titled "Client Devices (1)" with tabs for "LATEST" and "TREND". Below the tabs are filters for "TYPE" (Wireless, Wired), "HEALTH" (All, Inactive, Poor, Fair, Good, No Data), and "DATA" (Onboarding Time >= 10 s, Association >= 5 s, DHCP >= 5s, Authentication >= 5 s, RSSI <= -72 dBm, SNR <= 9 dB). There is a "Filter" button and an "Export" button. The main table has columns: Identifier, IP v4 Address, Device Type, Health, Last Seen, AP Name, and Location. One client is listed with Identifier "rsu01e", IP v4 Address "10.4.160.51", Device Type "Microsoft-Workstation", Health "10", Last Seen "Aug 05, 10:34 am", AP Name "AP057H.0567.0398", and Location "...as/Bldg 23/Floor 2".

Identifier	IP v4 Address	Device Type	Health	Last Seen	AP Name	Location
rsu01e	10.4.160.51	Microsoft-Workstation	10	Aug 05, 10:34 am	AP057H.0567.0398	...as/Bldg 23/Floor 2

Figure 72.
Client Health dashboard bottom panel

Information can be displayed based upon the following selections:

- **Type** – Wireless or wired clients.
- **Health** – All clients, only inactive clients, only active clients, clients in poor health, clients in fair health, clients in good health, or clients with no data (this selection is only available for wired clients).
- **Data** – This includes the following selections:
 - **Onboarding Time >= 10 S** – Displays clients which took greater than the default threshold of 10 seconds to onboard to the network. For wireless clients onboarding time consists of the time it took for the wireless client to associate with the AP (**Association Time**), time to get a DHCP address (**DHCP Time**), and the time to authenticate to the network (**Authentication Time**). This narrows the display of device to those which may have onboarding issues.
 - **Association Time >= 5 S** – Displays wired or wireless clients which took greater than 5 seconds from the time the client issued a DHCP Request to when the client received an IP address from the DHCP server. This can be used to narrow the display of clients to only those whose high onboarding time may be the result of delays in getting an IP address. Slow response times from DHCP servers may be an indication of exhaustion of an IP address pool (meaning there are no more addresses within the scope to hand out), an overrun DHCP server, or potentially networking issues between the DHCP server and the client.
 - **Authentication >= 5 S** – Displays wired or wireless clients which took greater than 5 seconds to authenticate to the network. This can be used to narrow the display of clients to only those whose high onboarding time may be the result of delays in authentication. Slow authentication times may be an indication of an overrun AAA server, possible networking issues between the AAA server and the network device (WLC or switch) or client, or even issues between the AAA server and the back-end data store for user credentials – such as a Microsoft AD server or LDAP server.
 - **RSSI <= -72 dBm** – Displays wireless clients which were seen with a received signal strength indication (RSSI) of the pre-configured threshold value of less than or equal to -72 dBm. This can be used to narrow the display of wireless clients to only those who may be having performance problems due to location – meaning possible RF dead spots in the wireless deployment; or potentially to sticky clients who do not roam when their RSSI drop to low values.

Technical Note: Individual RSSI readings from mobile devices can vary considerably based upon multiple factors which include the position of the wireless device with respect to the person holding the device, as well as the number and density of people in the room – since RF energy is absorbed by people. Additionally, RSSI is affected by the position and movement of the device with respect to the access point to which the device is associated, since various surfaces in most wireless environments either reflect or absorb RF energy.

- **SNR <= 9 dBm** – Displays wireless clients which were seen with a signal to noise ratio (SNR) less than or equal to the default threshold of 9 dBm. This can be used to narrow the display of wireless clients to only those who may be having performance problems due to RF noise based on location – meaning possible interfering devices such as microwave ovens in the 2.4 GHz band; or being too far from the nearest AP – possibly indicating a dead spot in the wireless deployment.

In the figure above all wireless clients has been selected.

7. Click on a wireless client to display even more detailed monitoring information regarding wireless clients on your network.

This will take you to the **Client 360** dashboard for the wireless client. An example of the top pane of the **Client 360** dashboard is shown in the figure below.

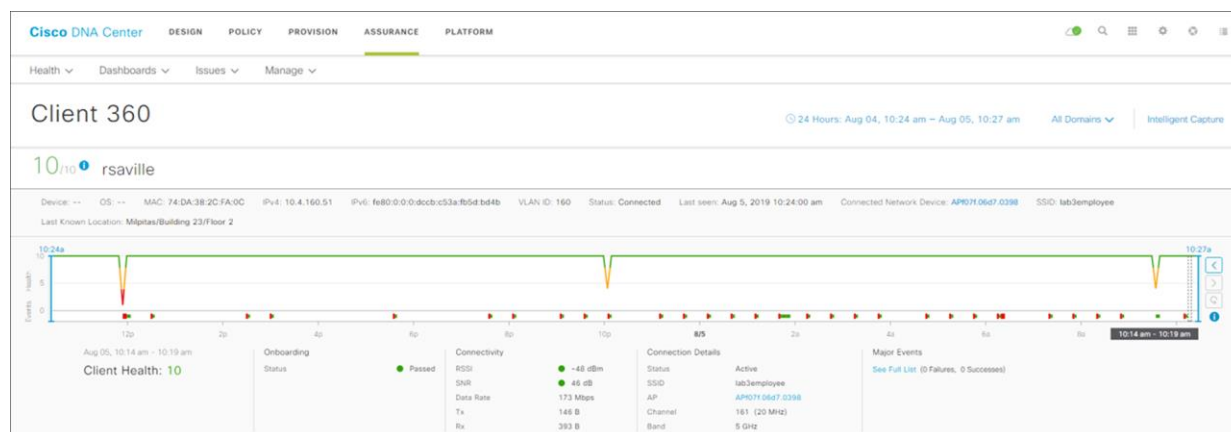


Figure 73.
Client 360 dashboard – top panel

The top panel of the **Client 360** dashboard presents a timeline of the overall health score of the device. By default, the timeline is over the previous 24 hours.

8. Hover your cursor over a section of the timeline.

Under the timeline you will see details regarding how the overall score of the wireless client is determined for that particular time. For example, in the figure above, it can be seen that the overall health score of the client is based on the score for **Onboarding**, and the score for **Connectivity**.

The score for **Onboarding** is based on whether the device successfully onboarded. Onboarding itself consists of associating to an AP, receiving an IP address from a DHCP server (when using DHCP), and authenticating to the network. If any of these steps fails, then onboarding will fail, the **Onboarding Status** will appear as **Failed** with a red circle, and the overall **Client Health** score will be **1** highlighted in red.

The score for **Connectivity** is based on two factors – **RSSI** and **SNR**. From the figure above, it can be seen that the **RSSI** is **-48 dBm** for the particular time selected in the timeline. This corresponds to a good value (since it is above the default threshold of **-72 dBm**) and therefore has a green circle next to it. The **SNR** is **46 dBm** for the particular time selected in the timeline. Again, this corresponds to a good value (since it is above the default threshold of **9 dB**) and therefore has a green circle next to it.

The overall health score for the wireless client is based on the lowest score of any one of the factors under **Onboarding** or **Connectivity**. As can be seen from the figure above, since **Onboarding** has passed (a score of **10**) and both **RSSI** and **SNR** are above their thresholds (again both scores of **10**) for the particular time selected in the timeline above – the overall health of the wireless is given a score of **10** for that time.

9. Scroll down to the **Event Viewer** panel.

An example of the **Event Viewer** panel of the **Client 360** dashboard is shown in the figure below.

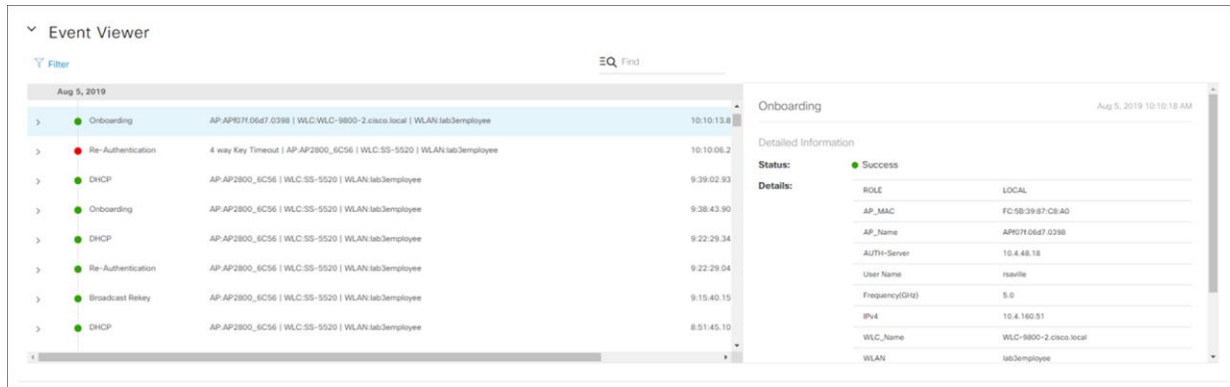


Figure 74.
Client 360 dashboard – Event Viewer panel

The **Event Viewer** panel provides you with a historical timeline of onboarding and connectivity events of the wireless client. It can be useful in troubleshooting previous onboarding issues by identifying what stage in onboarding – association, DHCP, authentication, etc. may have failed.

10. Scroll down to the **Onboarding** panel.

An example of the **Onboarding** panel of the **Client 360** dashboard is shown in the figure below.



Figure 75.
Client 360 Onboarding panel

The **Onboarding** panel provides a quick visual indication of the onboarding status of the wireless client. It provides a diagram which shows the following:

- The color-coded health of the wireless client (a green **10** in the figure above).
- The SSID to which the wireless client is connected (the **lab3employee** SSID in the figure above).
- The AP to which the wireless client is connected, as well as the color-coded health of the AP (an orange **6** in the figure above).
- The WLC to which the AP is associated, as well as the color-coded health of the WLC (a green **10** in the figure above).

11. Scroll down to the **Detail Information** panel and select the RF tab.

An example of the **RF** tab within the **Detail Information** panel of the **Client 360** dashboard is shown in the figure below.



Figure 76.
Client 360 - Detail Information - RF tab

The **Detail Information** panel provides more detailed information regarding the client. It contains the following tabs:

- The **Device Info** tab provides additional information about the client itself, such as the hostname, MAC address, IP address, etc.
- The **Connectivity** tab provides historical graphs of information such as transmit (Tx) and receive (Rx) rates, Tx and Rx errors, etc. This can be used to troubleshoot performance issues with the client due to link errors.
- The **RF tab** is only displayed for wireless clients. The **RF tab** provides historical graphs of the **RSSI** and **SNR** of the wireless client. This can be used to troubleshoot historical problems with the wireless client which may be related to RF issues.

This section of the design and deployment guide has just briefly touched upon the capabilities of Cisco DNA Assurance. Additional design and deployment guides focused specifically on Cisco DNA Assurance will more deeply cover the use cases for wireless Assurance.

Appendix A-New in this guide

This guide is new and is not updated from a previous version.

Appendix B-Hardware and software used for validation

This design & deployment guide was created using the following hardware and software.

Table 24. Hardware and software

Functional area	Product	Software version
Enterprise Wireless LAN Controllers	Cisco Catalyst 9800-40 WLCs	16.10.1e
Guest Wireless LAN Controller	Cisco Catalyst 9800-CL Cloud Controller	16.10.1e
Enterprise SDN Controller	Cisco DNA Center	1.3.0
AAA Server	Cisco Identity Services Engine (ISE)	2.3.0.298

Appendix C-Glossary

AP Access Point

Cisco ISE Cisco Identity Service 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 Pre-shared 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 Switch-over

SVI Switched Virtual Interface

SWIM Software Image Management

TPC Transmit Power Control

VLAN Virtual Local Area Network

WLAN Wireless Local Area Network

WLC Wireless LAN Controller

WNM Wireless Network Management

WPA WiFi Protected Alliance

Appendix D-Settings within each of the pre-configured RF profiles

The following table lists and explains the settings for each of the three default RF profiles within Cisco DNA Center. Note that the settings of the three default RF profiles cannot be changed. To change any setting, you must create a custom profile and assign it as the default RF profile.

Table 25. Settings for the LOW wireless radio frequency 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 for On.
PROFILE TYPE > 2.4 GHz > Parent Profile	Radio Button	<p>This is the parent profile from which this RF profile is derived. This field only makes sense when creating custom RF profiles, since custom RF profiles can be based on one of the three pre-configured RF profiles.</p> <p>The choices are as follows:</p> <ul style="list-style-type: none">• High - This is the high client density RF profile• Medium (Typical) - This is the medium client density RF profile• Low - This is the low client density RF profile• Custom - This is a custom RF profile <p>For the Low RF profile this is set for Low.</p>
PROFILE TYPE > 2.4 GHz > DCA Channel	Multiple choice radio button	<p>Selects the channels which Dynamic Channel Assignment (DCA) will operate in automatic mode within in the 2.4 GHz band. Choices are channels 1 - 14. The default setting is channels 1, 6, and 11.</p> <p>This field is not visible in the 2.4 GHz band when editing one of the pre-configured 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.</p>

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > Supported Data Rates	Single direction slider with multiple positions	<p>Slider with multiple positions indicating 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.</p> <p>For the Low RF profile, this is set for all data rates, allowing maximum device compatibility.</p> <p>The Low RF profile is designed for wireless environments of low client density. In such environments, wireless clients may connect to APs at potentially further distances and lower data rates.</p>
PROFILE TYPE > 2.4 GHz > Supported Data Rates > Enable 802.11b data rates	Check box	<p>This check box works with the slider discussed above. Checking the box enables the 802.11b data rates: 1, 2, 5.5, 6, 9, and 11 Mbps on the slider.</p> <p>For the Low RF profile, this box is checked.</p>
PROFILE TYPE > 2.4 GHz > Mandatory Data Rates	Multiple choice radio button	<p>This is used to select the data rates which the wireless client must support to be able to associate with the wireless network in the 2.4 GHz band. Choices are as follows: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps.</p> <p>For the Low RF profile, the following data rates are mandatory: 1, 2, 5.5, and 11 Mbps.</p>
PROFILE TYPE > 2.4 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	<p>This slider determines the minimum and maximum power levels which 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 dBm to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based upon RSSI from neighboring APs.</p> <p>For the Low RF profile, the sliders are set so that the full range of power levels from a minimum of -10 dBm to a maximum of 30 dBm is available to TPC.</p> <p>For environments of low client density, APs may be further 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.</p>
PROFILE TYPE > 2.4 GHz > TX Power Configuration > RX SOP	Drop-down Menu	<p>The Receiver Start of Packet Detection Threshold (RX-SOP) determines the RF signal level at which the 2.4 GHz radio will demodulate and decode a wireless packet.</p> <p>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 will be decoded by the AP. Since lower RSSI is often due to the wireless client being further 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 further spaced.</p> <p>For the Low RF profile, this is set to Low (-80 dBm).</p>

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	<p>The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and hence the coverage behavior of the system.</p> <p>The TPC Power Threshold ranges from -80 to -50 dBm. For wireless deployments of low client density, typically there are 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.</p> <p>For the Low RF profile, this is set to -65 dBm for the 2.4 GHz radio.</p>
PROFILE TYPE > 5 GHz	On/Off Toggle	Enables or disables the 5 GHz band for the RF profile. Set for On.
PROFILE TYPE > 5 GHz > Parent Profile	Radio Button	<p>This is the parent profile from which this RF profile is derived. This field only makes sense when creating custom RF profiles, since custom RF profiles can be based on one of the three pre-configured RF profiles.</p> <p>The choices are as follows:</p> <ul style="list-style-type: none"> • High - This is the high client density RF profile • Medium (Typical) - This is the medium client density RF profile • Low - This is the low client density RF profile • Custom - This is a custom RF profile <p>For the Low RF profile this is set for Low.</p>
PROFILE TYPE > 5 GHz > Channel Width	Drop-down Menu	<p>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.</p> <p>For the Low RF profile channel width is set for 20 MHz.</p>
PROFILE TYPE > 5 GHz > DCA Channel	Multiple choice radio button	<p>Selects the channels which Dynamic Channel Assignment (DCA) will operate in automatic mode within in the 5 GHz band.</p> <p>Choices vary based on regulatory domain UNII-1 channels 36 48; UNII-2 channels 52 144, and UNII-3 channels 149 165.</p> <p>This field is not visible in the 5 GHz band when editing one of the pre-configured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 5 GHz band.</p>
PROFILE TYPE > 5GHz > Supported Data Rates	Single direction slider with multiple positions	<p>Slider with multiple positions indicating 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.</p> <p>For the Low RF profile, this is set for all data rates.</p> <p>The Low RF profile is designed for wireless environments of low client density. In such environments, wireless clients may connect to APs at potentially further distances and lower data rates.</p>

Feature	Type	Description
PROFILE TYPE > 5 GHz > Mandatory Data Rates	Multiple choice radio button	<p>This is used to select the data rates which the wireless client must support to be able to associate with the wireless network in the 5 GHz band. Choices are as follows: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.</p> <p>For the low RF profile, the following data rates are mandatory: 6, 12, and 24 Mbps.</p>
PROFILE TYPE > 5 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	<p>This slider determines the minimum and maximum power levels which Transmit Power Control (TPC) can configure on 5 GHz radios in APs associated with this RF profile. The full range of the slider is from -10 dBm to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based upon RSSI from neighboring APs.</p> <p>For the low RF profile, the sliders are set so that the full range of power levels from a minimum of -10 dBm to a maximum of 30 dBm is available to TPC.</p> <p>For environments of low client density, APs may be further 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.</p>
PROFILE TYPE > 5 GHz > TX Power Configuration > RX SOP	Drop-down Menu	<p>The Receiver Start of Packet Detection Threshold (RX-SOP) determines the RF signal level at which the 5 GHz radio will demodulate and decode a wireless packet.</p> <p>Lower RX-SOP levels increase the sensitivity of the 5 GHz radio to wireless clients. Wireless client traffic with lower Received Signal Strength Indication (RSSI) values will be decoded by the AP. Since lower RSSI is often due to the wireless client being further 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 further spaced.</p> <p>For the Low RF profile, this is set to Low (-80 dBm).</p>
PROFILE TYPE > 5 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	<p>The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and hence the coverage behavior of the system.</p> <p>The TPC Power Threshold ranges from -80 to -50 dBm. For wireless deployments of low client density, typically there are 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.</p> <p>For the Low RF profile, this is set to -60 dBm for the 5 GHz radio.</p>

Table 26. Settings for the TYPICAL (Default) wireless radio frequency profile

Feature	Type	Description
Profile Name	Text Field	TYPICAL
PROFILE TYPE > 2.4 GHz	On/Off Toggle	Enables or disables the 2.4 GHz band for the RF profile. Set for On.
PROFILE TYPE > 2.4 GHz > Parent Profile	Radio Button	<p>This is the parent profile from which this RF profile is derived. This field only makes sense when creating custom RF profiles, since custom RF profiles can be based on one of the three pre-configured RF profiles.</p> <p>The choices are as follows:</p> <ul style="list-style-type: none"> • High - This is the high client density RF profile • Medium (Typical) - This is the medium client density RF profile • Low - This is the low client density RF profile • Custom - This is a custom RF profile <p>For the Typical RF profile this is set for Medium (Typical).</p>
PROFILE TYPE > 2.4 GHz > DCA Channel	Multiple choice radio button	<p>Selects the channels which Dynamic Channel Assignment (DCA) will operate - in automatic mode within in the 2.4 GHz band. Choices are channels 1 -14. The default setting is channels 1, 6, and 11.</p> <p>This field is not visible in the 2.4 GHz band when editing one of the pre-configured 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.</p>
PROFILE TYPE > 2.4 GHz > Supported Data Rates	Single direction slider with multiple positions	<p>Slider with multiple positions indicating 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.</p> <p>For the Typical RF profile, this is set for rates of 9 Mbps and higher.</p> <p>The Typical RF profile is designed for wireless environments of medium client density. In such environments, having wireless clients connecting to APs at lower speeds will decrease the overall throughput of the wireless network. Sufficient AP density should be deployed such that the clients can connect and transmit at higher rates.</p>
PROFILE TYPE > 2.4 GHz > Supported Data Rates > Enable 802.11b data rates	Check box	<p>This check box works with the slider discussed above. Checking the box enables the 802.11b data rates: 1, 2, 5.5, 6, 9, and 11 Mbps on the slider.</p> <p>For the Typical RF deployment, this box is unchecked.</p>
PROFILE TYPE > 2.4 GHz > Mandatory Data Rates	Multiple choice radio button	<p>This is used to select the data rates which the wireless client must support to be able to associate with the wireless network in the 2.4 GHz band. Choices are as follows: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps.</p> <p>For the Typical RF profile, the only data rate that is mandatory is 12 Mbps.</p>

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	<p>This slider determines the minimum and maximum power levels which 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 dBm to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based upon RSSI from neighboring APs.</p> <p>For the Typical RF profile, the sliders are set so that the full range of power levels from a minimum of -10 dBm to a maximum of 30 dBm is available to TPC.</p> <p>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.</p>
PROFILE TYPE > 2.4 GHz > TX Power Configuration > RX SOP	Drop-down Menu	<p>The Receiver Start of Packet Detection Threshold (RX-SOP) determines the RF signal level at which the 2.4 GHz radio will demodulate and decode a wireless packet.</p> <p>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 will be decoded by the AP. Since lower RSSI is often due to the wireless client being further 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 further spaced.</p> <p>For the Typical RF profile, this is set to Auto.</p>
PROFILE TYPE > 2.4 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	<p>The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and hence the coverage behavior of the system.</p> <p>The TPC Power Threshold ranges from -80 to -50 dBm. For wireless deployments of medium client density, typically there are 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 co-channel interference (CCI).</p> <p>For the Typical RF profile, this is set to -70 dBm for the 2.4 GHz radio.</p>
PROFILE TYPE > 5 GHz	On/Off Toggle	Enables or disables the 5 GHz band for the RF profile. Set for On.
PROFILE TYPE > 5 GHz > Parent Profile	Radio Button	<p>This is the parent profile from which this RF profile is derived. This field only makes sense when creating custom RF profiles, since custom RF profiles can be based on one of the three pre-configured RF profiles.</p> <p>The choices are as follows:</p> <ul style="list-style-type: none"> • High - This is the high client density RF profile • Medium (Typical) - This is the medium client density RF profile • Low - This is the low client density RF profile • Custom - This is a custom RF profile <p>For the Typical RF profile this is set for Medium (Typical).</p>

Feature	Type	Description
PROFILE TYPE > 5 GHz > Channel Width	Drop-down Menu	<p>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.</p> <p>For the Typical RF profile channel width is set for 20 MHz.</p>
PROFILE TYPE > 5 GHz > DCA Channel	Multiple choice radio button	<p>Selects the channels which Dynamic Channel Assignment (DCA) will operate - in automatic mode - within in the 5 GHz band.</p> <p>Choices vary based on regulatory domain - UNII-1 channels 36 - 48; UNII-2 channels 52 - 144, and UNII-3 channels 149 - 165.</p> <p>This field is not visible in the 5 GHz band when editing one of the pre-configured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 5 GHz band.</p>
PROFILE TYPE > 5GHz > Supported Data Rates	Single direction slider with multiple positions	<p>Slider with multiple positions indicating 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.</p> <p>For the Typical RF profile, this is set for all data rates.</p>
PROFILE TYPE > 5 GHz > Mandatory Data Rates	Multiple choice radio button	<p>This is used to select the data rates which the wireless client must support to be able to associate with the wireless network in the 5 GHz band. Choices are as follows: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.</p> <p>For the Typical RF profile, the following data rates are mandatory: 6, 12, and 24 Mbps.</p>
PROFILE TYPE > 5 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	<p>This slider determines the minimum and maximum power levels which Transmit Power Control (TPC) can configure on 5 GHz radios in APs associated with this RF profile. The full range of the slider is from -10 dBm to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based upon RSSI from neighboring APs.</p> <p>For the Typical RF profile, the sliders are set so that the full range of power levels from a minimum of -10 dBm to a maximum of 30 dBm is available to TPC.</p> <p>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.</p>
PROFILE TYPE > 5 GHz > TX Power Configuration > RX SOP	Drop-down Menu	<p>The Receiver Start of Packet Detection Threshold (RX-SOP) determines the RF signal level at which the 5 GHz radio will demodulate and decode a wireless packet.</p> <p>Lower RX-SOP levels increase the sensitivity of the 5 GHz radio to wireless clients. Wireless client traffic with lower Received Signal Strength Indication (RSSI) values will be decoded by the AP. Since lower RSSI is often due to the wireless client being further 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 further spaced.</p> <p>For the Low RF profile, this is set to Low (-80 dBm).</p>

Feature	Type	Description
PROFILE TYPE > 5 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	<p>The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and hence the coverage behavior of the system.</p> <p>The TPC Power Threshold ranges from -80 to -50 dBm. For wireless deployments of medium client density, typically there are 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 co-channel interference (CCI).</p> <p>For the Typical RF profile, this is set to -70 dBm for the 5 GHz radio.</p>

Table 27. Settings for the HIGH wireless radio frequency 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 for On.
PROFILE TYPE > 2.4 GHz > Parent Profile	Radio Button	<p>This is the parent profile from which this RF profile is derived. This field only makes sense when creating custom RF profiles, since custom RF profiles can be based on one of the three pre-configured RF profiles.</p> <p>The choices are as follows:</p> <ul style="list-style-type: none"> • High - This is the high client density RF profile • Medium (Typical) - This is the medium client density RF profile • Low - This is the low client density RF profile • Custom - This is a custom RF profile <p>For the High RF profile this is set for High.</p>
PROFILE TYPE > 2.4 GHz > DCA Channel	Multiple choice radio button	<p>Selects the channels which Dynamic Channel Assignment (DCA) will operate - in automatic mode - within in the 2.4 GHz band. Choices are channels 1 - 14. The default setting is channels 1, 6, and 11.</p> <p>This field is not visible in the 2.4 GHz band when editing one of the pre-configured 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.</p>

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > Supported Data Rates	Single direction slider with multiple positions	<p>Slider with multiple positions indicating 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.</p> <p>For the High RF profile, this is set for rates of 9 Mbps and higher.</p> <p>The High RF profile is designed for wireless environments of high client density. In such environments, having wireless clients connecting to APs at lower speeds will decrease the overall throughput of the wireless network. Sufficient AP density should be deployed such that the clients can connect and transmit at higher rates.</p>
PROFILE TYPE > 2.4 GHz > Supported Data Rates > Enable 802.11b data rates	Check box	<p>This check box works with the slider discussed above. Checking the box enables the 802.11b data rates: 1, 2, 5.5, 6, 9, and 11 Mbps on the slider.</p> <p>For the High RF deployment, this box is unchecked.</p>
PROFILE TYPE > 2.4 GHz > Mandatory Data Rates	Multiple choice radio button	<p>This is used to select the data rates which the wireless client must support to be able to associate with the wireless network in the 2.4 GHz band. Choices are as follows: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps.</p> <p>For the High RF profile, the only data rate that is mandatory is 12 Mbps.</p>
PROFILE TYPE > 2.4 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	<p>This slider determines the minimum and maximum power levels which 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 dBm to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based upon RSSI from neighboring APs.</p> <p>For the High RF profile, the sliders are set so that the range of power levels is from a minimum of 7 dBm to a maximum of 30 dBm is available to TPC.</p> <p>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 will incrementally increase 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).</p>
PROFILE TYPE > 2.4 GHz > TX Power Configuration > RX SOP	Drop-down Menu	<p>The Receiver Start of Packet Detection Threshold (RX-SOP) determines the RF signal level at which the 2.4 GHz radio will demodulate and decode a wireless packet.</p> <p>Higher RX-SOP levels decrease the sensitivity of the 2.4 GHz radio to wireless clients. Wireless client traffic with lower Received Signal Strength Indication (RSSI) values will not be decoded by the AP. Since lower RSSI is often due to the wireless client being further 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.</p> <p>For the High RF profile, this is set to Medium.</p>

Feature	Type	Description
PROFILE TYPE > 2.4 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	<p>The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and hence the coverage behavior of the system.</p> <p>The TPC Power Threshold ranges from -80 to -50 dBm. For wireless deployments of high client density, typically there are 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 co-channel interference (CCI).</p> <p>For the High RF profile, this is set to -70 dBm for the 2.4 GHz radio.</p>
PROFILE TYPE > 5 GHz	On/Off Toggle	Enables or disables the 5 GHz band for the RF profile. Set for On.
PROFILE TYPE > 5 GHz > Parent Profile	Radio Button	<p>This is the parent profile from which this RF profile is derived. This field only makes sense when creating custom RF profiles, since custom RF profiles can be based on one of the three pre-configured RF profiles.</p> <p>The choices are as follows:</p> <ul style="list-style-type: none"> • High - This is the high client density RF profile • Medium (Typical) - This is the medium client density RF profile • Low - This is the low client density RF profile • Custom - This is a custom RF profile <p>For the High RF profile this is set for High.</p>
PROFILE TYPE > 5 GHz > Channel Width	Drop-down Menu	<p>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.</p> <p>For the High RF profile channel width is set for 20 MHz.</p>
PROFILE TYPE > 5 GHz > DCA Channel	Multiple choice radio button	<p>Selects the channels which Dynamic Channel Assignment (DCA) will operate in automatic mode within in the 5 GHz band.</p> <p>Choices vary based on regulatory domain - UNII-1 channels 36 - 48; UNII-2 channels 52 - 144, and UNII-3 channels 149 - 165.</p> <p>This field is not visible in the 5 GHz band when editing one of the pre-configured profiles (LOW, TYPICAL, or HIGH). It is only visible when creating a new RF profile in the 5 GHz band.</p>
PROFILE TYPE > 5GHz > Supported Data Rates	Single direction slider with multiple positions	<p>Slider with multiple positions indicating 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.</p> <p>For the High RF profile, this is set for rates of 12 Mbps and higher.</p>
PROFILE TYPE > 5 GHz > Mandatory Data Rates	Multiple choice radio button	<p>This is used to select the data rates which the wireless client must support to be able to associate with the wireless network in the 5 GHz band. Choices are as follows: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.</p> <p>For the High RF profile, the following data rates are mandatory: 12 and 24 Mbps.</p>

Feature	Type	Description
PROFILE TYPE > 5 GHz > TX Power Configuration > Power Level	Multiple direction slider with multiple settings	<p>This slider determines the minimum and maximum power levels which Transmit Power Control (TPC) can configure on 5 GHz radios in APs associated with this RF profile. The full range of the slider is from -10 dBm to 30 dBm in increments of 1 dBm. TPC automatically adjusts the TX power of each radio based upon RSSI from neighboring APs.</p> <p>For the High RF profile, the sliders are set so that the range of power levels is from a minimum of 7 dBm to a maximum of 30 dBm is available to TPC.</p> <p>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 will incrementally increase 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).</p>
PROFILE TYPE > 5 GHz > TX Power Configuration > RX SOP	Drop-down Menu	<p>The Receiver Start of Packet Detection Threshold (RX-SOP) determines the RF signal level at which the 2.4 GHz radio will demodulate and decode a wireless packet.</p> <p>Higher RX-SOP levels decrease the sensitivity of the 2.4 GHz radio to wireless clients. Wireless client traffic with lower Received Signal Strength Indication (RSSI) values will not be decoded by the AP. Since lower RSSI is often due to the wireless client being further 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.</p> <p>For the High RF profile, this is set to Medium.</p>
PROFILE TYPE > 5 GHz > TX Power Configuration > TPC Power Threshold	Multiple direction slider with multiple settings	<p>The TPC Power Threshold is used to control the desired power levels at the cell boundaries of the APs, and hence the coverage behavior of the system.</p> <p>The TPC Power Threshold ranges from -80 to -50 dBm. For wireless deployments of high client density, typically there are 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 co-channel interference (CCI).</p> <p>For the High RF profile, this is set to -65 dBm for the 5 GHz radio.</p>

About this guide

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2019 Cisco Systems, Inc. All rights reserved.

Feedback & Discussion

For comments and suggestions about our guides, please join the discussion on [Cisco Community](#).

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)