Guide

Cisco public

The bridge to possible

Cisco DNA Center AI-Enhanced RRM

Deployment guide

Contents

Overview of Cisco DNA Center AI-Enhanced RRM

AI-Enhanced RRM is the next evolution of Cisco's award-winning radio resource management (RRM). RRM was originally introduced with Cisco® AireOS and the Cisco Aironet® access points in 2005 and managed the complexities of RF from Wi-Fi 1 through 6 and now Wi-Fi 6E. RRM has fluidly grown to include innovative algorithms such as Flexible Radio Architecture (FRA) and Dynamic Bandwidth Selection (DBS) to the traditional algorithms of Dynamic Channel Assignment (DCA) and Transmit Power Control (TPC).

On a Cisco Catalyst™ 9800 Series Wireless Controller, traditional RRM runs as a service. Cisco RRM manages the RF group (the components making up the RF network) based on dynamic measurements between every access point (AP) and its neighbors. This information is stored in a local database on the RF group leader controller. At runtime, RRM draws on the last 10 minutes of collected data and gently optimizes based on the current network conditions. Cisco RRM has proven to be extremely effective and trustworthy over the years, and when **configured correctly** for the type of RF network coverage desired (capacity vs. coverage) it can adapt to almost any size or deployment density. In Wi-Fi, RF conditions can dynamically change with different network loads, numbers of devices, and numbers of users in the environment. RRM has continued to measure up well to this task, with caveats that do require some learning for the environment being tuned.

Enter Cisco's AI-Enhanced RRM. AI-Enhanced RRM integrates the power of artificial intelligence (AI) and machine learning (ML) into the reliable and trusted Cisco RRM product family algorithms in the cloud. AI-Enhanced RRM is coordinated through Cisco's DNA Center (an on-premises appliance) as a service. Existing Cisco Catalyst 9800 RRM sites can be seamlessly transitioned to an intelligent, centralized service. As with other Cisco DNA Center services, AI-Enhanced RRM brings a host of new features with it. The Cisco DNA Center RRM control center allows administrators to quickly assess the health and performance of the RF coverage, from the enterprise level all the way down to a single site or building level.

Cisco AI-Enhanced RRM is different, as it brings the ability to analyze historical dynamic RF data over time. The ability to evaluate complex RF data often comes down to being able to factor in local knowledge of "normal" against the currently displayed data. "Normal" can and does vary from site to site based on the equipment choices and architectural design vs. the client density.

After an initial learning period, the Cisco AI Analytics Cloud will begin to provide insights into the performance and tuning of the RF network. Insights provide granular guidance on:

- Performance against service-level agreements (SLAs)
- The effectiveness of present settings and configurations
- The quality of the coverage

Together, the AI-Enhanced RRM algorithms, with the power of the Cisco AI Analytics Cloud, and Cisco DNA Center take Wi-Fi RF management to an unprecedented level that correlates 24x7 observations from the network and the client devices themselves and applies 20+ years of Cisco RF excellence to drive exceptional user experiences into the future.

Cisco AI-Enhanced RRM data flows and functional components

Cisco AI-Enhanced RRM operates as a distributed RRM service. RF telemetry is collected from the Cisco Access Points by the Catalyst wireless controller (WLC) and passed through Cisco DNA Center to the Cisco AI Analytics Cloud, where the data is stored. The RRM algorithms run against this telemetry data stored in the cloud. AI analyzes the solutions and passes any configuration change information back to Cisco DNA Center. Cisco DNA Center maintains the control connection with the enrolled Catalyst 9800 and passes any individual AP configuration changes back to the APs. The Cisco AI Analytic Cloud operates just like the WLC RF group leader does on the controller today, but with much more storage, compute power, and intelligent analysis.

Networkwide holistic optimizations are performed by the RRM Resource Analytics Engine, which focuses on dynamically created groups of radios (clusters) to optimize local performance without falling victim to the pitfalls of greedy optimizations that could lead to cascading network changes and potential network disruptions. Algorithms for DCA, TPC, FRA, DBS, and basic service set (BSS) color are some examples of the types of optimizations performed. These algorithms are latency tolerant and lend themselves well to management within the Cisco DNA Center ecosystem.

The RRM Edge Compute Engine focuses on latency-sensitive and client-specific optimizations. Examples of these types of services include optimized roaming, dynamic frequency selection (DFS) optimizations, coverage hole detection and mitigation, event-driven RRM (EDRRM), and dynamic DFS. These functions are maintained on the local WLC, with telemetry data being sent to the AI-Enhanced RRM Analytics Engine. This analysis will provide optimization guidance and insights to the RRM Control Center to help administrators further optimize the configurations and monitor performance.

The Cisco AI Analytics Cloud provides the core support to Cisco DNA Center for AI-Enhanced RRM core services as well as ML features. The architecture supports the methods and framework necessary to create a seamless upgrade path for existing customers to benefit from adaptive RRM optimizations and finally simplify customer configurations using intent-based RRM workflows through both local and cloud-based Catalyst 9800 WLCs.

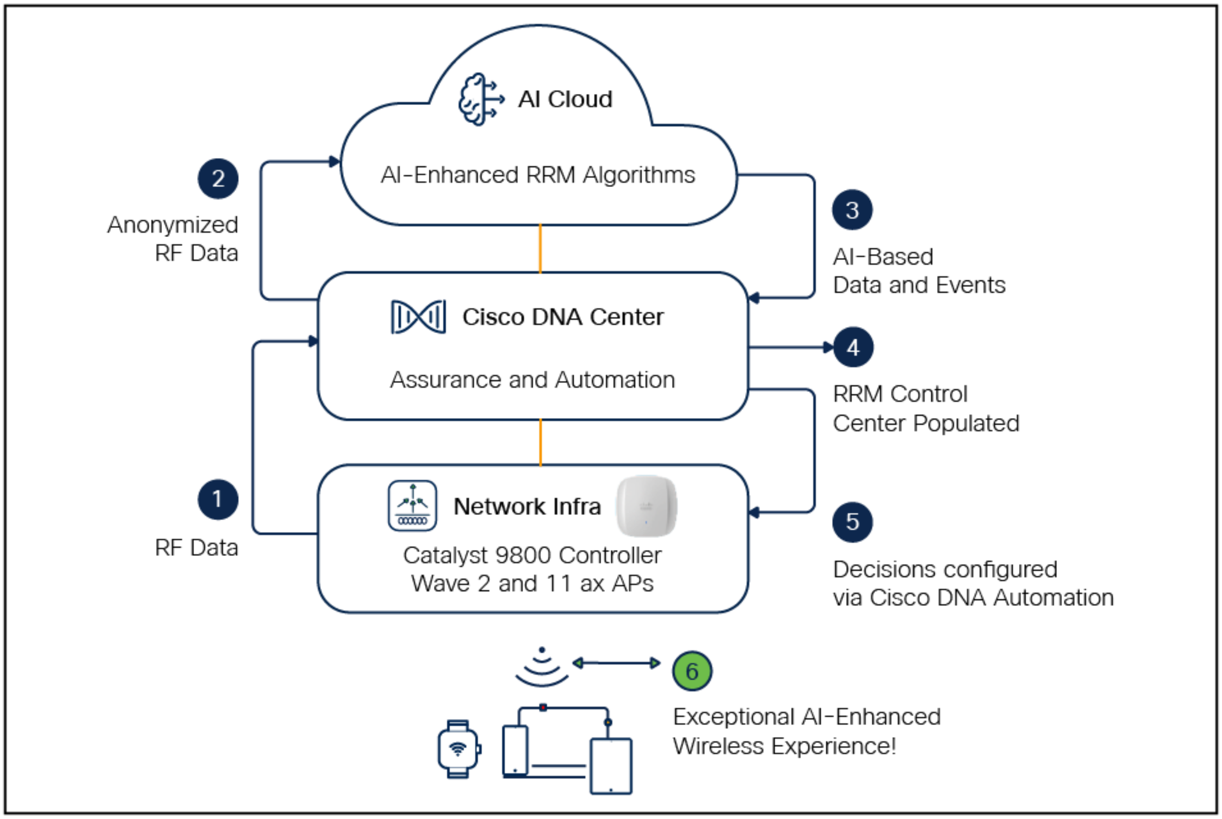


Figure 1.
AI-Enhanced RRM architecture and data flow

Recommended software

- Cisco DNA Center Release 2.3.4
- Cisco WLC and AP Release Cisco IOS® XE 17.9.3

Table 1. Cisco DNA Center and device compatibility matrix

Cisco DNA Center release	WLC release/Cisco IOS XE
2.3.2.x	17.7.1
2.3.3.x	17.8.1
2.3.4.x or later	17.9.3

Table 2. Cisco DNA Center package requirement

Cisco DNA Center package requirements	Minimum supported package version	Recommended package version
AI Network Analytics	2.8.8.306	2.9.21.398
Assurance Base	2.3.2.108	2.3.3.382

Note: This document is based on the recommended Cisco DNA Center Release 2.3.4 and controller/AP release of Cisco IOS XE 17.9.3. Some software features are not supported in earlier software releases.

Supported device software and hardware

Table 3. Cisco Catalyst wireless controllers that support AI-Enhanced RRM

Supported Catalyst wireless controllers	Minimum supported Cisco IOS XE version	Recommended Cisco IOS XE version
Cisco Catalyst 9800-CL Wireless Controller for Cloud	17.7.1	17.9.3
Cisco Catalyst 9800-L Wireless Controller	17.7.1	17.9.3
Cisco Catalyst 9800-40 Wireless Controller	17.7.1	17.9.3
Cisco Catalyst 9800-80 Wireless Controller	17.7.1	17.9.3

Table 4. Cisco APs that support AI-Enhanced RRM

Supported access points	Cisco IOS XE software	
	Minimum version	Recommended version
Aironet 1540 Series	17.7.1	17.9.3
Aironet 1560 Series	17.7.1	17.9.3
Aironet 1815 Series	17.7.1	17.9.3
Aironet 1830 Series	17.7.1	17.9.3
Aironet 1840 Series	17.7.1	17.9.3
Aironet 1850 Series	17.7.1	17.9.3
Aironet 2800 Series	17.7.1	17.9.3
Aironet 3800 Series	17.7.1	17.9.3
Aironet 4800 Series	17.7.1	17.9.3
Catalyst 9105AX Series	17.7.1	17.9.3
Catalyst 9115AX Series	17.7.1	17.9.3

Supported access points	Cisco IOS XE software	
	Minimum version	Recommended version
Catalyst 9120AX Series	17.7.1	17.9.3
Catalyst 9130AX Series	17.7.1	17.9.3
Catalyst 9124AX Series	17.7.1	17.9.3
Catalyst IW6300 Heavy Duty Series	17.7.1	17.9.3
6300 Series Embedded Services	17.7.1	17.9.3
Catalyst 9136 Series	17.7.1	17.9.3
Catalyst 9164 Series	17.9.3	17.9.3
Catalyst 9166 Series	17.9.3	17.9.3
Catalyst 9162 Series	17.9.2	17.9.2

Day-0 configuration: Setting up Cisco DNA Center to use AI-Enhanced RRM

The following subsections provide step-by-step instructions for setting up the day-0 configurations necessary to begin using AI-Enhanced RRM.

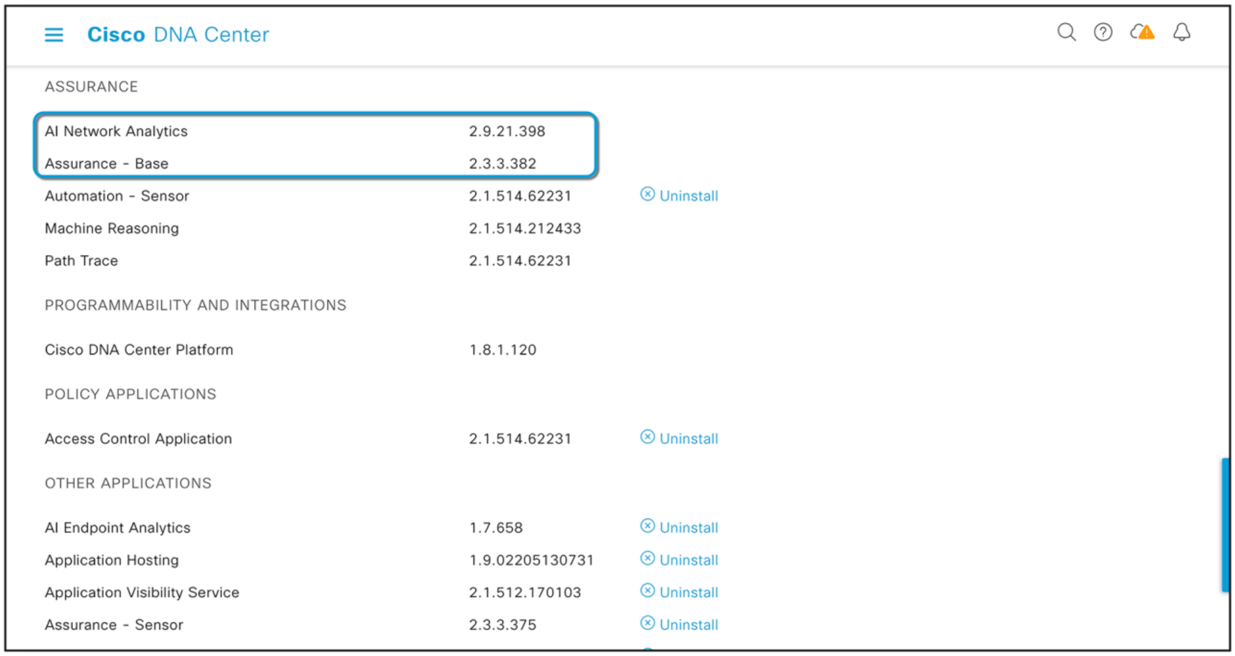
Install the AI Network Analytics package onto Cisco DNA Center

Cisco DNA Center provides the option to download a couple of packages called **AI Network Analytics** and **Assurance – Base**.

To download and install this package, follow the steps below:

- Click the hamburger menu ≡ in the top left corner of the screen. Click System, then Software Updates.
- Click **Installed Apps** on the left side of the screen.
- Scroll down to **Assurance** and you will find the **AI Network Analytics** and **Assurance – Base** packages ready for download and installation (Figure 2).

Note: If you do not see the **AI Network Analytics and Assurance – Base** packages after performing the steps above, please reach out to either a Cisco account sales representative or an account sales engineer for additional support.



ASSURANCE		
AI Network Analytics	2.9.21.398	
Assurance - Base	2.3.3.382	
Automation - Sensor	2.1.514.62231	⊗ Uninstall
Machine Reasoning	2.1.514.212433	
Path Trace	2.1.514.62231	
PROGRAMMABILITY AND INTEGRATIONS		
Cisco DNA Center Platform	1.8.1.120	
POLICY APPLICATIONS		
Access Control Application	2.1.514.62231	⊗ Uninstall
OTHER APPLICATIONS		
AI Endpoint Analytics	1.7.658	⊗ Uninstall
Application Hosting	1.9.02205130731	⊗ Uninstall
Application Visibility Service	2.1.512.170103	⊗ Uninstall
Assurance - Sensor	2.3.3.375	⊗ Uninstall

Figure 2.
Location of the AI Network Analytics package within the Software Updates page

Prepare the Catalyst 9800 wireless controller

Configure NETCONF

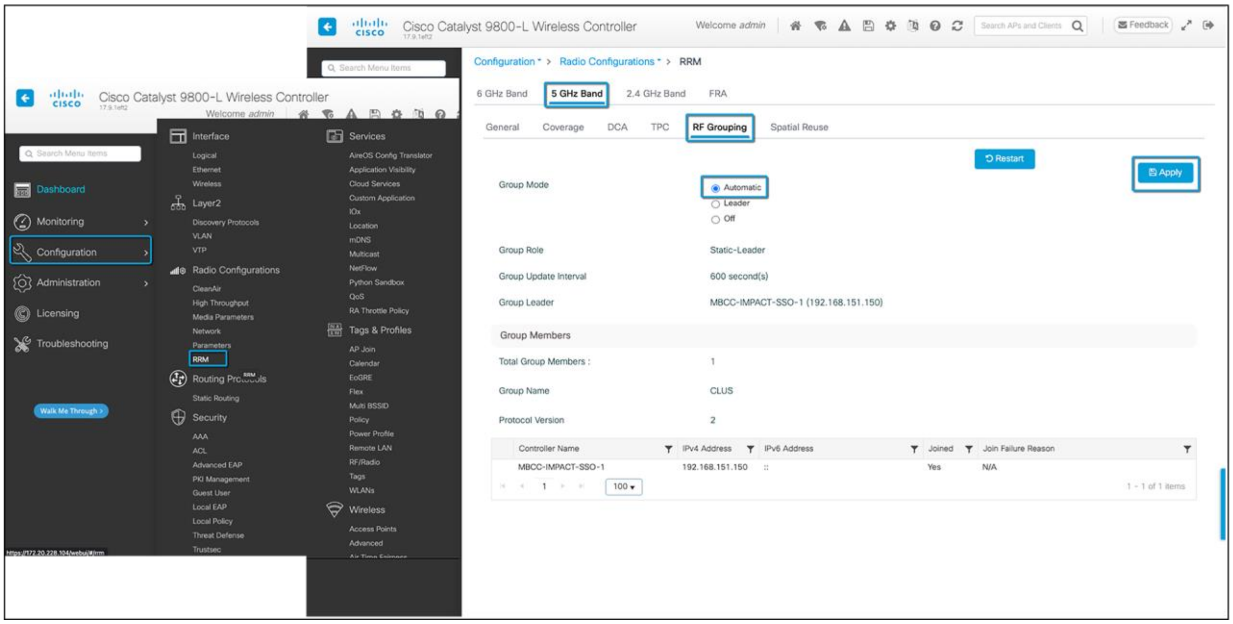
For discovery and inventory, Cisco DNA Center uses NETCONF. Ensure that NETCONF is configured before adding to the Cisco DNA Center inventory.

- The required configuration for NETCONF and AAA authorization: netconf-yang
    - aaa new-model
    - aaa authorization exec default local
- If using an authentication, authorization, and accounting (AAA) server to authenticate the user credentials, make sure the NETCONF user returned from AAA is defined with privilege 15.

Verify RF Grouping

A Catalyst 9800 WLC in RF Grouping mode with static roles (Static Leader and Static Member), along with WLCs in Automatic mode (Auto Leader and Auto Member), should support transformation into remote members of the AI-Enhanced RRM RF group leader.

Note: If the controller is configured as a Static Leader and there are member controllers assigned to it, make sure that the member controllers have the same RRM configuration and RF profile settings before changing the leader configuration to Auto. Once this configuration is set to Auto, all the previous grouped controllers will automatically negotiate a new RF group leader, and the RF group leader will use the new RF group leader controller's RRM configurations.



Group Mode: ● Automatic ○ Leader ○ Off

Group Role: Static-Leader

Group Update Interval: 600 second(s)

Group Leader: MBCC-IMPACT-SSO-1 (192.168.151.150)

Group Members

Total Group Members : 1

Group Name: CLUS

Protocol Version: 2

Controller Name	IPv4 Address	IPv6 Address	Joined	Join Failure Reason
MBCC-IMPACT-SSO-1	192.168.151.150	::	Yes	N/A

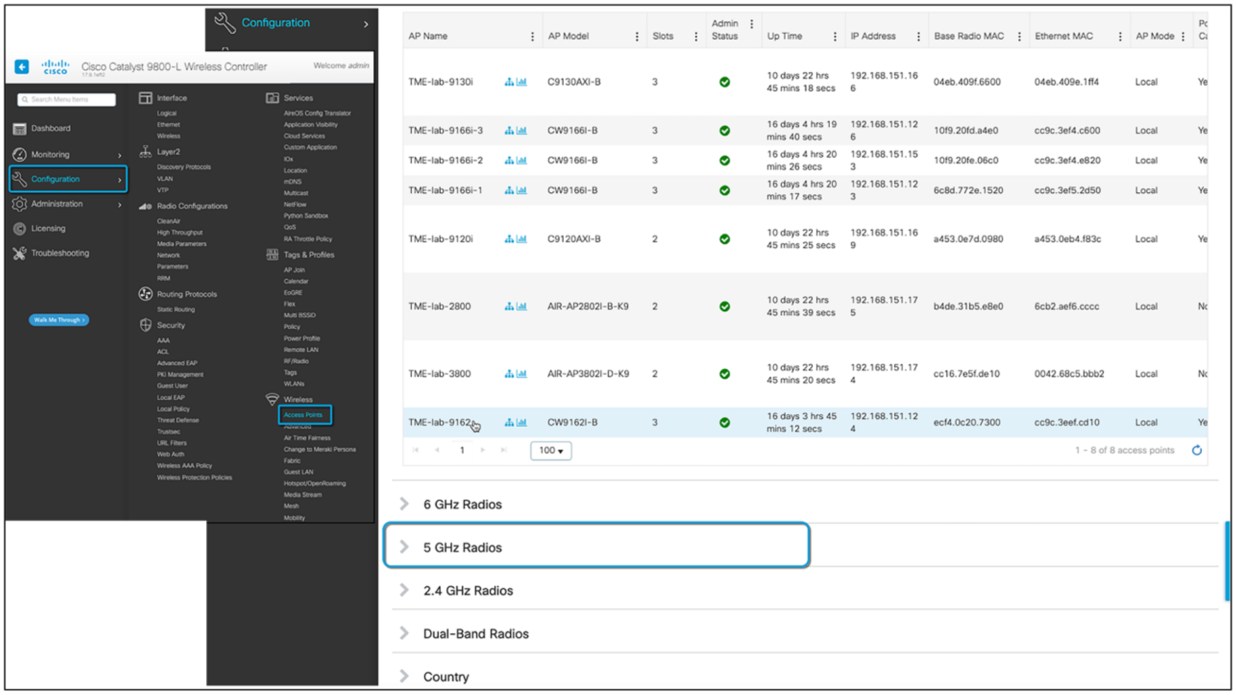
1 - 1 of 1 items

Figure 3.
Changing the RF Grouping mode to Automatic on the Catalyst 9800 wireless controller

Verify Radio settings

In addition to setting RF Grouping to Automatic, ensure that RF Channel Assignment and Tx Power Level Assignment for all radios are operating in Global Assignment mode (Automatic) and are not set to a static value on the AP radio. Although this is encouraged but not mandatory, a subset of the radios can be on a static channel, and power settings and AI-Enhanced RRM will simply work on the other set of radios under automation mode.

To do this, navigate to Configuration > Access Points and expand the 6 GHz, 5 GHz, and 2.4 GHz Radios drop-down. If the Channel and Power Level values contain an asterisk (*), they are operating in Global Assignment mode and will be managed by AI-Enhanced RRM. Manage any radios that do not have an asterisk through the radio configuration dialog and set the channel and power back to Global.



AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Po Ca
TME-lab-9130i	C9130AXI-B	3	✓	10 days 22 hrs 45 mins 18 secs	192.168.151.166	04eb.409f.6600	04eb.409e.1ff4	Local	Ye
TME-lab-9166i-3	CW9166I-B	3	✓	16 days 4 hrs 19 mins 40 secs	192.168.151.126	10f9.20fd.a4e0	cc9c.3ef4.c600	Local	Ye
TME-lab-9166i-2	CW9166I-B	3	✓	16 days 4 hrs 20 mins 26 secs	192.168.151.153	10f9.20fe.06c0	cc9c.3ef4.e820	Local	Ye
TME-lab-9166i-1	CW9166I-B	3	✓	16 days 4 hrs 20 mins 17 secs	192.168.151.123	6c8d.772e.1520	cc9c.3ef5.2d50	Local	Ye
TME-lab-9120i	C9120AXI-B	2	✓	10 days 22 hrs 45 mins 25 secs	192.168.151.169	a453.0e7d.0980	a453.0eb4.f83c	Local	Ye
TME-lab-2800	AIR-AP2802I-B-K9	2	✓	10 days 22 hrs 45 mins 39 secs	192.168.151.175	b4de.31b5.e8e0	6cb2.aef6.cccc	Local	Nc
TME-lab-3800	AIR-AP3802I-D-K9	2	✓	10 days 22 hrs 45 mins 20 secs	192.168.151.174	cc16.7e5f.de10	0042.68c5.bbb2	Local	Nc
TME-lab-9162	CW9162I-B	3	✓	16 days 3 hrs 45 mins 12 secs	192.168.151.124	ecf4.0c20.7300	cc9c.3eef.cd10	Local	Ye

1 100 1 - 8 of 8 access points

6 GHz Radios

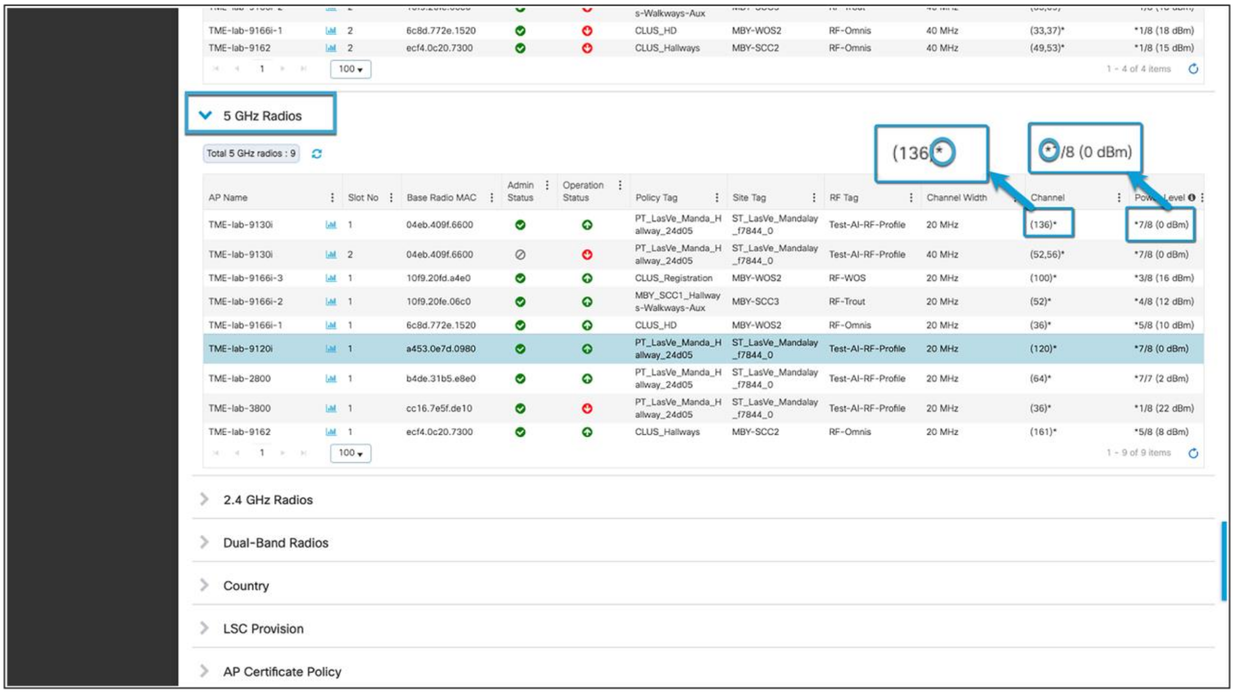
5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

Figure 4.
Location of access point radios on the Catalyst 9800 wireless controller



					s-Walkways-Aux					
TME-lab-9166i-1	2	6c8d.772e.1520	✓	▼	CLUS_HD	MBY-WOS2	RF-Omnis	40 MHz	(33,37)*	*1/8 (18 dBm)
TME-lab-9162	2	ecf4.0c20.7300	✓	▼	CLUS_Hallways	MBY-SCC2	RF-Omnis	40 MHz	(49,53)*	*1/8 (15 dBm)

1 100 1 - 4 of 4 items

5 GHz Radios

Total 5 GHz radios : 9

AP Name	Slot No	Base Radio MAC	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Channel Width	Channel	Power Level
TME-lab-9130i	1	04eb.409f.6600	✓	▲	PT_LasVe_Manda_Hallway_24d05	ST_LasVe_Mandalay_f7844_0	Test-AI-RF-Profile	20 MHz	(136)*	*7/8 (0 dBm)
TME-lab-9130i	2	04eb.409f.6600	⊘	▼	PT_LasVe_Manda_Hallway_24d05	ST_LasVe_Mandalay_f7844_0	Test-AI-RF-Profile	40 MHz	(52,56)*	*7/8 (0 dBm)
TME-lab-9166i-3	1	10f9.20fd.a4e0	✓	▲	CLUS_Registration	MBY-WOS2	RF-WOS	20 MHz	(100)*	*3/8 (16 dBm)
TME-lab-9166i-2	1	10f9.20fe.06c0	✓	▲	MBY_SCC1_Hallways-Walkways-Aux	MBY-SCC3	RF-Trout	20 MHz	(52)*	*4/8 (12 dBm)
TME-lab-9166i-1	1	6c8d.772e.1520	✓	▲	CLUS_HD	MBY-WOS2	RF-Omnis	20 MHz	(36)*	*5/8 (10 dBm)
TME-lab-9120i	1	a453.0e7d.0980	✓	▲	PT_LasVe_Manda_Hallway_24d05	ST_LasVe_Mandalay_f7844_0	Test-AI-RF-Profile	20 MHz	(120)*	*7/8 (0 dBm)
TME-lab-2800	1	b4de.31b5.e8e0	✓	▲	PT_LasVe_Manda_Hallway_24d05	ST_LasVe_Mandalay_f7844_0	Test-AI-RF-Profile	20 MHz	(64)*	*7/7 (2 dBm)
TME-lab-3800	1	cc16.7e5f.de10	✓	▼	PT_LasVe_Manda_Hallway_24d05	ST_LasVe_Mandalay_f7844_0	Test-AI-RF-Profile	20 MHz	(36)*	*1/8 (22 dBm)
TME-lab-9162	1	ecf4.0c20.7300	✓	▲	CLUS_Hallways	MBY-SCC2	RF-Omnis	20 MHz	(161)*	*5/8 (8 dBm)

1 100 1 - 9 of 9 items

2.4 GHz Radios

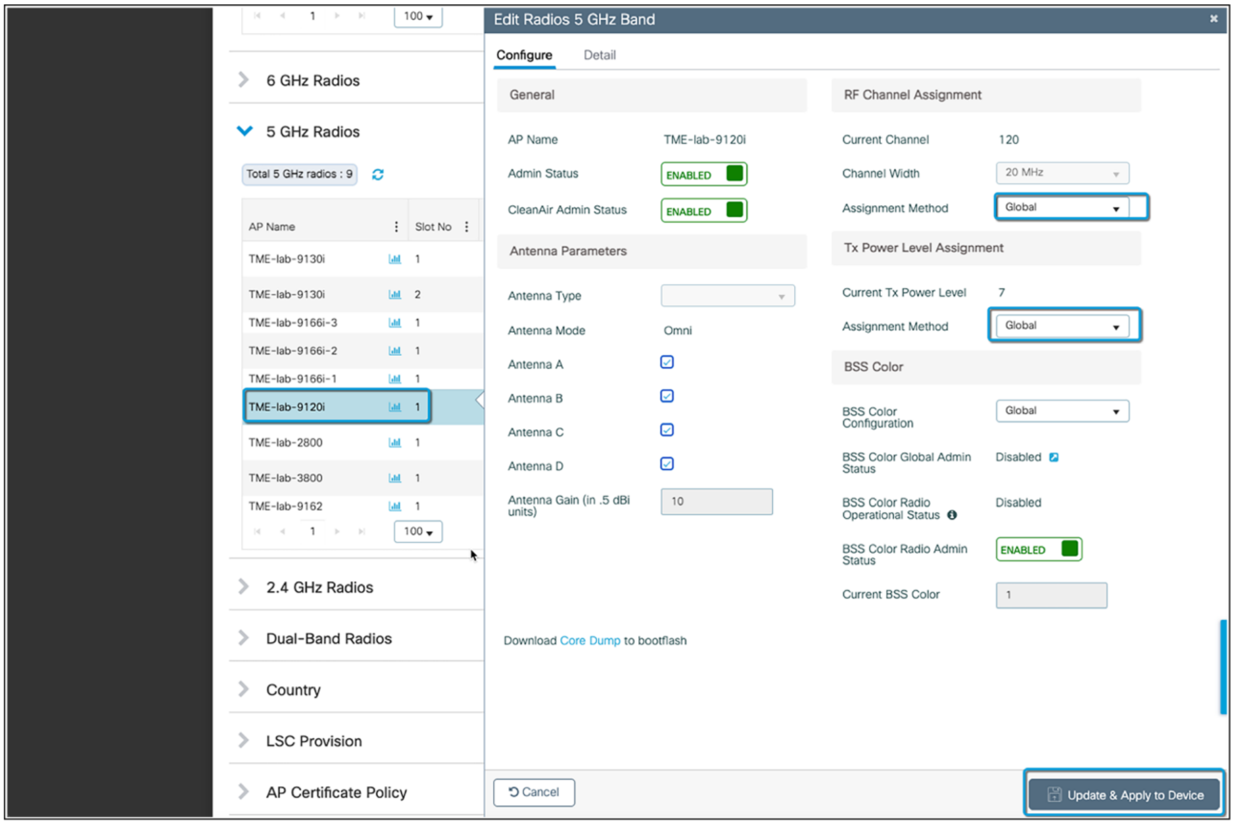
Dual-Band Radios

Country

LSC Provision

AP Certificate Policy

Figure 5.
Verifying the asterisk (*) in the channel and power level assignments in the radios table



AP Name	Slot No
TME-lab-9130i	1
TME-lab-9130i	2
TME-lab-9166i-3	1
TME-lab-9166i-2	1
TME-lab-9166i-1	1
TME-lab-9120i	1
TME-lab-2800	1
TME-lab-3800	1
TME-lab-9162	1

Edit Radios 5 GHz Band

Configure | Detail

General

AP Name: TME-lab-9120i
Admin Status: ENABLED
CleanAir Admin Status: ENABLED

Antenna Parameters

Antenna Type:
Antenna Mode: Omni
Antenna A: ☑
Antenna B: ☑
Antenna C: ☑
Antenna D: ☑
Antenna Gain (in .5 dBi units): 10

RF Channel Assignment

Current Channel: 120
Channel Width: 20 MHz
Assignment Method: Global

Tx Power Level Assignment

Current Tx Power Level: 7
Assignment Method: Global

BSS Color

BSS Color Configuration: Global
BSS Color Global Admin Status: Disabled
BSS Color Radio Operational Status: Disabled
BSS Color Radio Admin Status: ENABLED
Current BSS Color: 1

Download Core Dump to bootflash

Figure 6.
Setting the assignment method for the channel and TX power level to Global for RRM

Note: Combination of Policy/Site/RF Tags used in set of Access Points will be grouped into 1 Network Profile in Cisco DNA Center. Any Policy/Site/RF Tag not assigned to any Access Points will not be learned by DNA Center while doing a Learn Device config workflow. Make sure to add atleast 1 Access Point per unique Policy/Site/RF tag combination on the controller. This will help in any future deployment with these combinations created.

Part 1: Build a site hierarchy

Description: Cisco DNA Center's Design page provides a robust design application to allow customers of every size and scale to easily define their physical sites and common resources.

Section goals: Create and configure network hierarchy sites and settings to define shared services, device credentials, and Simple Network Management Protocol (SNMP) community strings.

Note: If your site hierarchy is already defined or exported from Cisco Prime® Infrastructure, you can skip to Part 2.

Step 1: Navigate to the Network Hierarchy page

Click the hamburger menu ☰ in the top left corner of the screen. Click **Design**, then **Network Hierarchy** (Figure 7).

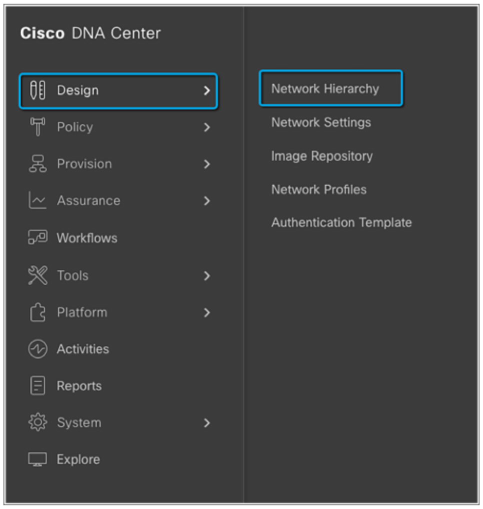


Figure 7.
Displaying the network hierarchy

Step 2: Create sites, buildings, and floors

To allow Cisco DNA Center to group devices based on location, begin by laying out a hierarchy of areas, buildings, and floors as required to accurately represent the location of your network. A site hierarchy lets you enable unique network settings and IP spaces for different groups of devices.

- **Option 1:** To create a site, click the **Add Site** button (Figure 8). A menu will open and provide you an option to create a child area, building, or floor within a desired site.
- **Option 2:** To create a site, click the gear icon (Figure 9) next to the site you would like to create a child site under.
- When creating a floor, click **Upload file** to upload a floor of a building (Figure 10).

  Floor plans must be in DXF, DWG, JPG, GIF, or PNG format.

The behavior of Cisco DNA Center is for settings from the global level to be inherited into subsequent levels in the hierarchy. This enables consistency across large domains while providing administrators the flexibility to adapt and change an individual building or floor.

Notes:

- You can create areas and buildings only within the global site or other areas and can create floors only within buildings.
- When creating a building within the design hierarchy, it is critical that you use a real physical street address for your sites. Cisco DNA Center uses the street address to select the country code for the wireless implementation.

Refer to **Design the Network Hierarchy** in the Cisco DNA Center User Guide for more details on how to create a network hierarchy or migrate your existing network hierarchy from Cisco Prime.

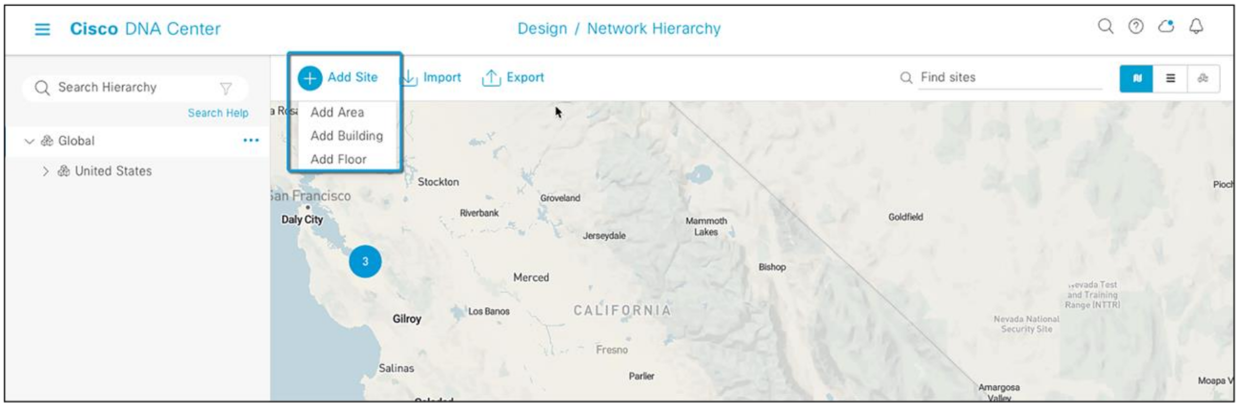


Figure 8.
Clicking Add Site within the Network Hierarchy page

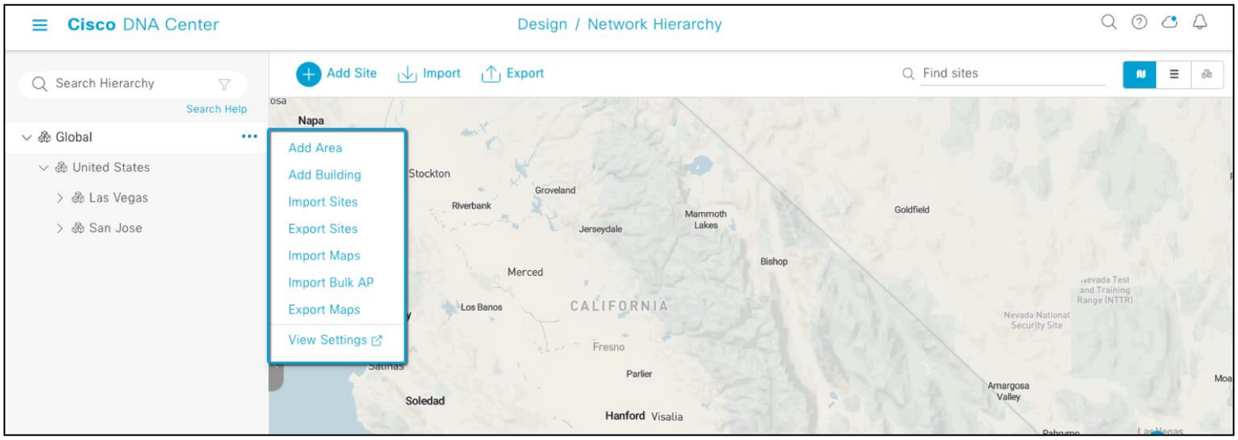
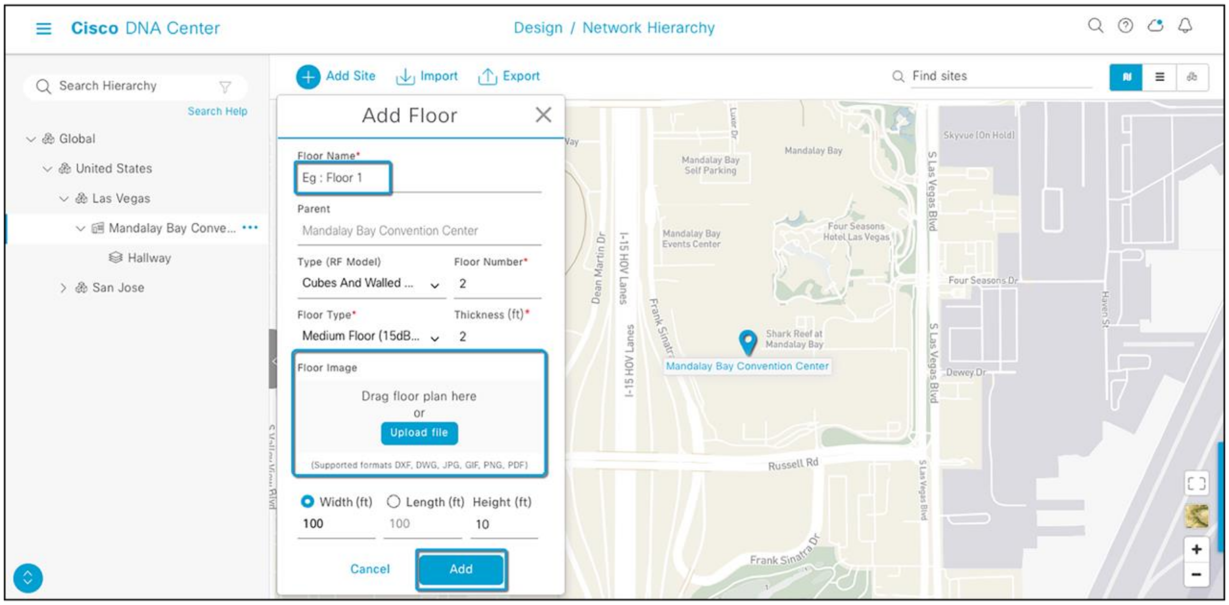


Figure 9.
Clicking the gear icon next to a site within the Network Hierarchy page



Add Floor

Floor Name* Eg : Floor 1

Parent Mandalay Bay Convention Center

Type (RF Model) Cubes And Walled ...

Floor Number* 2

Floor Type* Medium Floor (15dB...

Thickness (ft)* 2

Floor Image

Drag floor plan here
or
Upload file
(Supported formats DXF, DWG, JPG, GIF, PNG, PDF)

● Width (ft) ○ Length (ft) Height (ft)
100 100 10

Cancel Add

Figure 10.
Location of the Upload file button to upload a floor plan during floor creation

Part 2: Discovery and inventory

Cisco DNA Center's **Discovery** application allows a network administrator to add their network device to the platform.

Section goals: Discover WLC and APs and assign them to the site created in the previous section.

If you already have the WLC and APs in inventory, you can skip ahead to the Part 4, Learn an Existing Deployment.

Step 1: Navigate to the Network Settings page

Cisco DNA Center lets you save common resources and settings with the Network Settings application. Information pertaining to the enterprise can be stored and reused across the network.

- To navigate to the Network Settings page, open the hamburger menu ☰ in the top left corner of the screen. Click **Design**, then **Network Settings** (Figure 11).

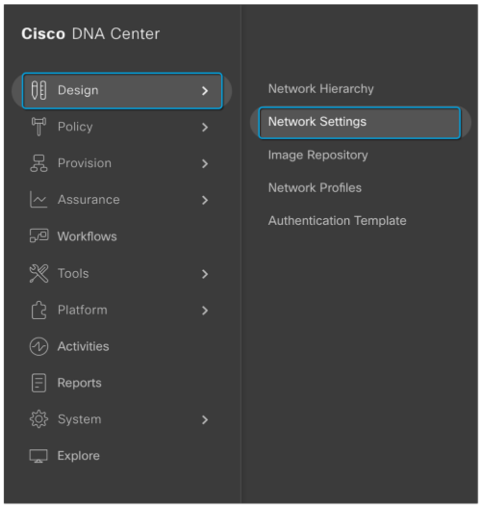
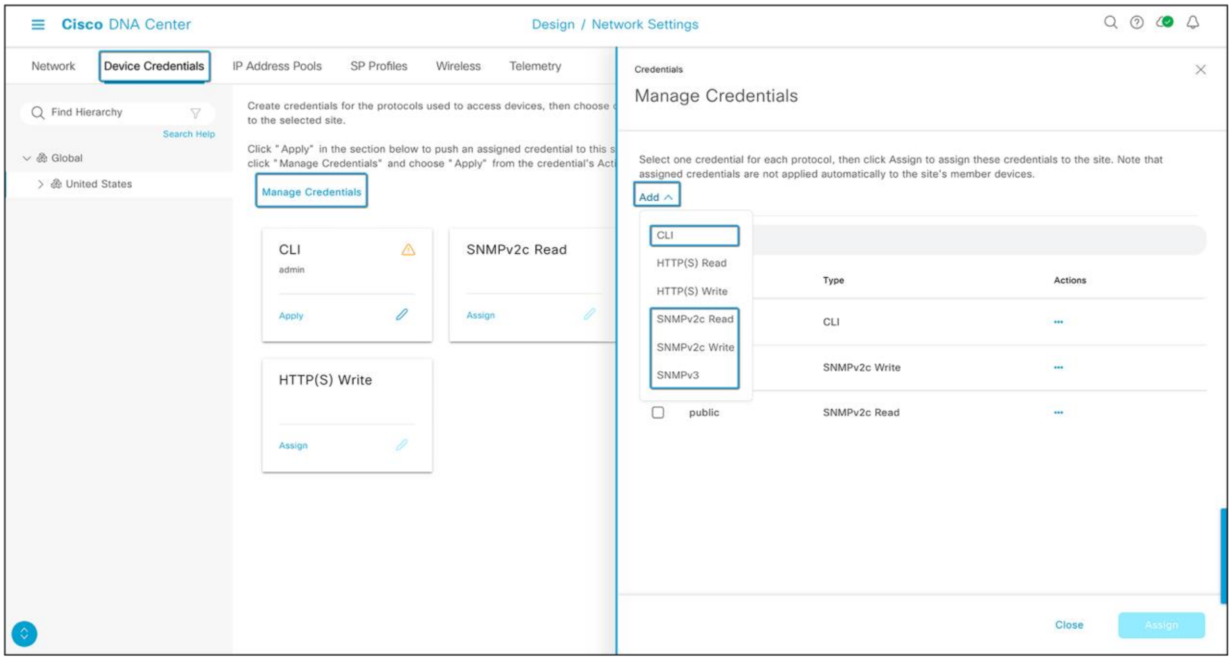


Figure 11.
Location of Network Settings from the hamburger menu

Step 2: Configure network settings and device credentials

This is where you configure all device-related network settings. By default, Cisco DNA Center's IP address is prepopulated in the **Syslog Server** and **SNMP Server** fields. This will enable syslog and SNMP traps to be sent to Cisco DNA Center from network devices when a WLC is added to Cisco DNA Center.

- Click the **Device Credentials** tab to view the existing device command-line interface (CLI) credentials and SNMP community strings (Figure 12).
- Click **Add** to create new credential entries (Figure 13). Cisco DNA Center uses these credentials to discover the network devices.



Create credentials for the protocols used to access devices, then choose to the selected site.

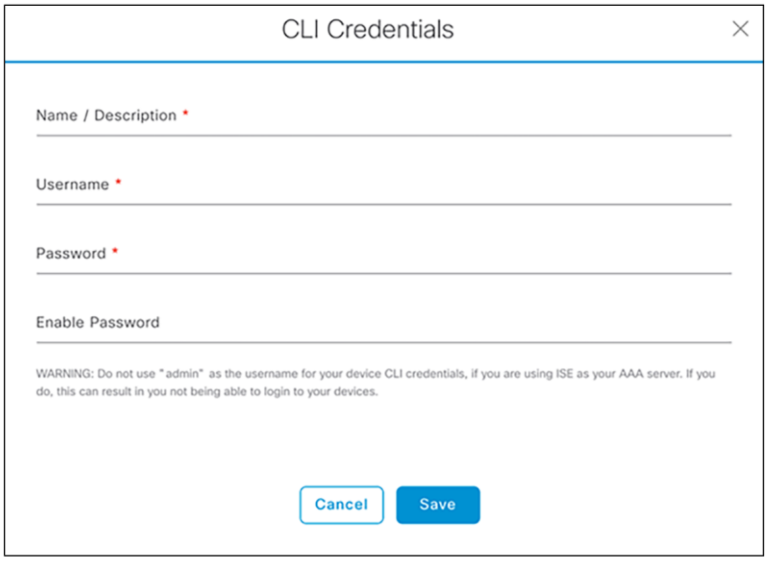
Click "Apply" in the section below to push an assigned credential to this s click "Manage Credentials" and choose "Apply" from the credential's Acti

Manage Credentials

Select one credential for each protocol, then click Assign to assign these credentials to the site. Note that assigned credentials are not applied automatically to the site's member devices.

		Type	Actions
		CLI	•••
		SNMPv2c Write	•••
☐	public	SNMPv2c Read	•••

Figure 12.
Workflow to add device credentials to the network settings



CLI Credentials

Name / Description *

Username *

Password *

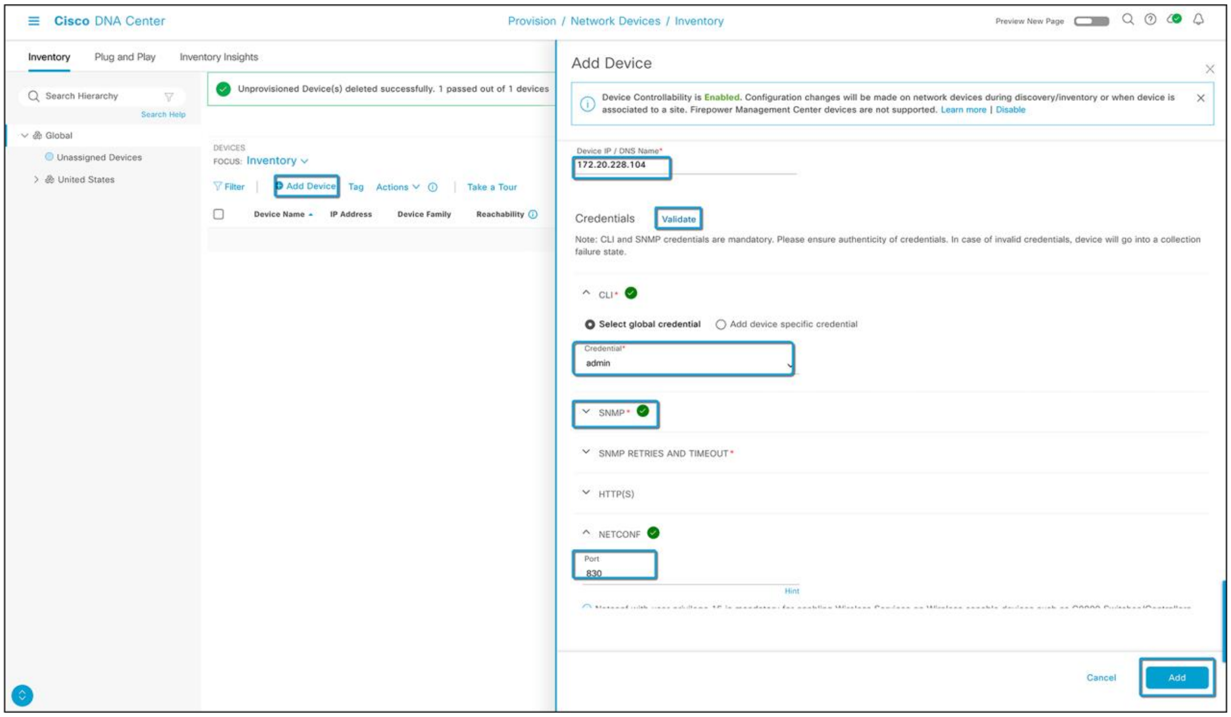
Enable Password

WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.

Figure 13.
CLI Credentials form that appears when you click Add in the previous figure

Step 3: Add device to inventory

- Option 1: Click the hamburger menu (☰) in the top left corner of the screen. Click Inventory, then Add Device.
- Option 2: From the homepage, scroll down to the bottom and click Discovery and then Add Discovery (Figures 15 and 16).



Unprovisioned Device(s) deleted successfully. 1 passed out of 1 devices

Device Controllability is Enabled. Configuration changes will be made on network devices during discovery/inventory or when device is associated to a site. Firepower Management Center devices are not supported. Learn more | Disable

Device IP / DNS Name*: 172.20.228.104

Credentials

Note: CLI and SNMP credentials are mandatory. Please ensure authenticity of credentials. In case of invalid credentials, device will go into a collection failure state.

CLI* ✓

● Select global credential ○ Add device specific credential

Credential*: admin

SNMP* ✓

NETCONF ✓

Port: 830

Figure 14.
Option 1: Add the Catalyst wireless controller details

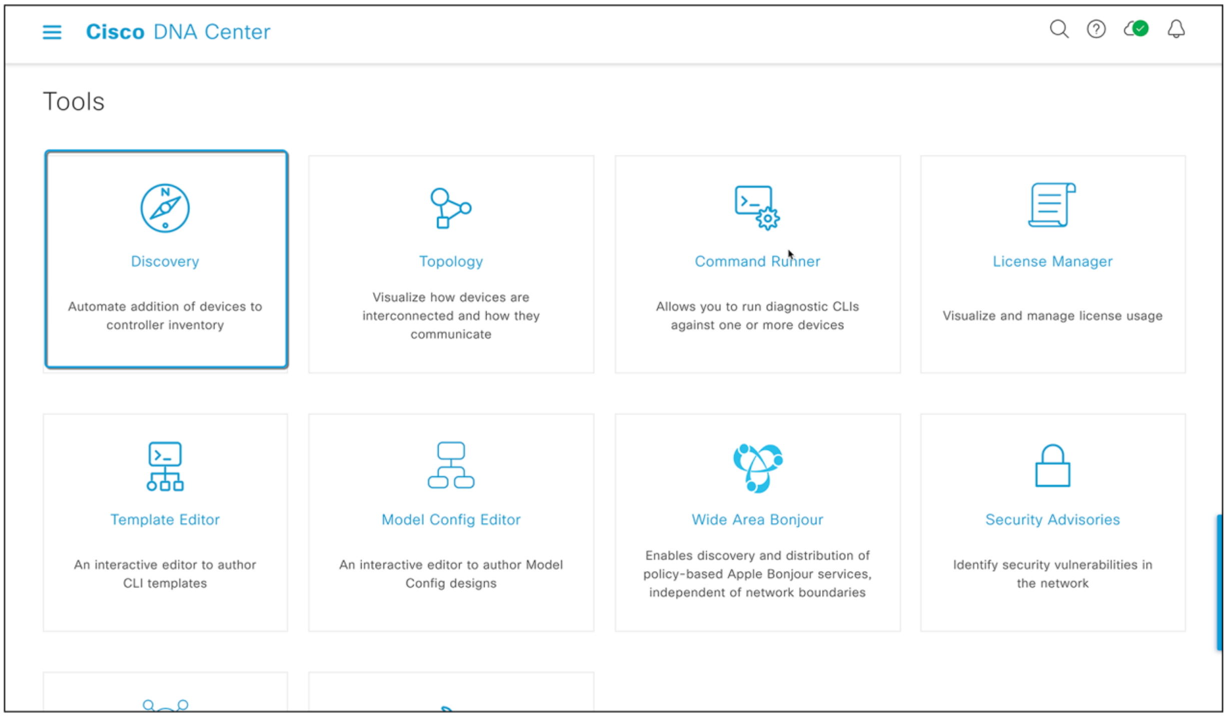
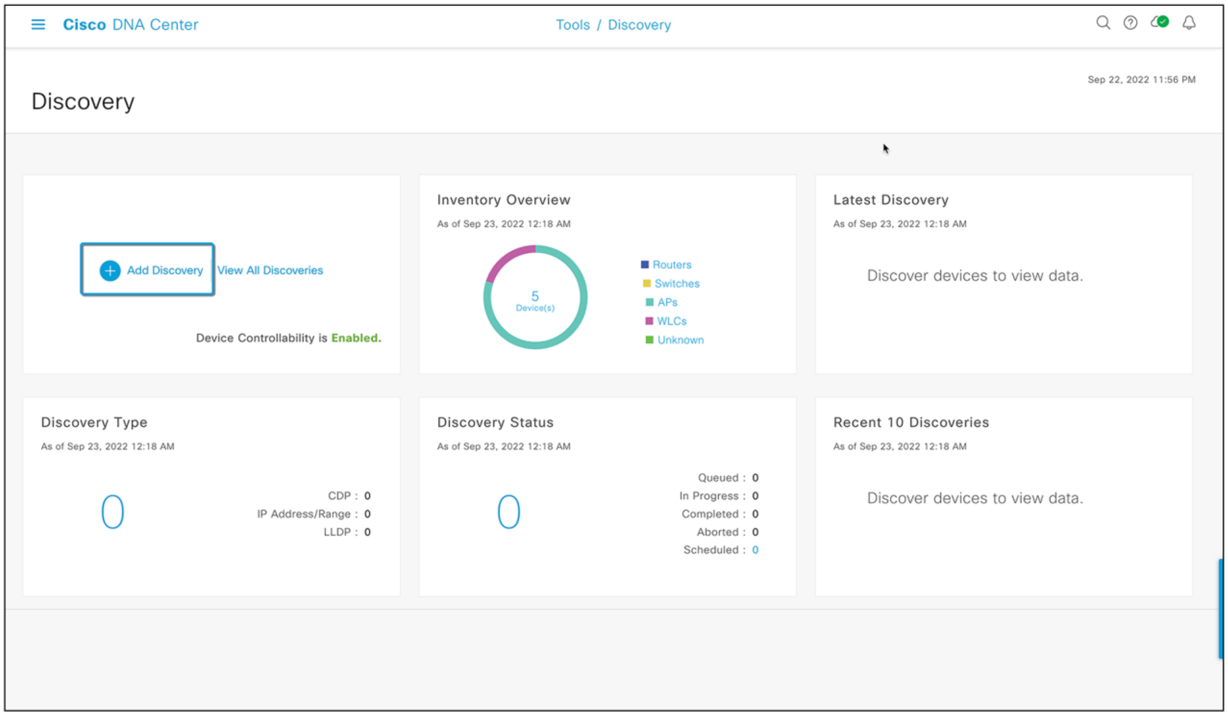

Cisco DNA Center
Tools
Discovery
Automate addition of devices to controller inventory
Topology
Visualize how devices are interconnected and how they communicate
Command Runner
Allows you to run diagnostic CLIs against one or more devices
License Manager
Visualize and manage license usage
Template Editor
An interactive editor to author CLI templates
Model Config Editor
An interactive editor to author Model Config designs
Wide Area Bonjour
Enables discovery and distribution of policy-based Apple Bonjour services, independent of network boundaries
Security Advisories
Identify security vulnerabilities in the network

Figure 15.
Option 2: Location of Discovery button on Cisco DNA Center homepage



Cisco DNA Center   Tools / Discovery

Sep 22, 2022 11:56 PM

Discovery

Add Discovery   View All Discoveries

Device Controllability is Enabled.

Inventory Overview

As of Sep 23, 2022 12:18 AM

5 Device(s)

■ Routers
■ Switches
■ APs
■ WLCs
■ Unknown

Latest Discovery

As of Sep 23, 2022 12:18 AM

Discover devices to view data.

Discovery Type

As of Sep 23, 2022 12:18 AM

0

CDP : 0
IP Address/Range : 0
LLDP : 0

Discovery Status

As of Sep 23, 2022 12:18 AM

0

Queued : 0
In Progress : 0
Completed : 0
Aborted : 0
Scheduled : 0

Recent 10 Discoveries

As of Sep 23, 2022 12:18 AM

Discover devices to view data.

Figure 16.
Option 2: Location of Add Discovery button on Discovery page

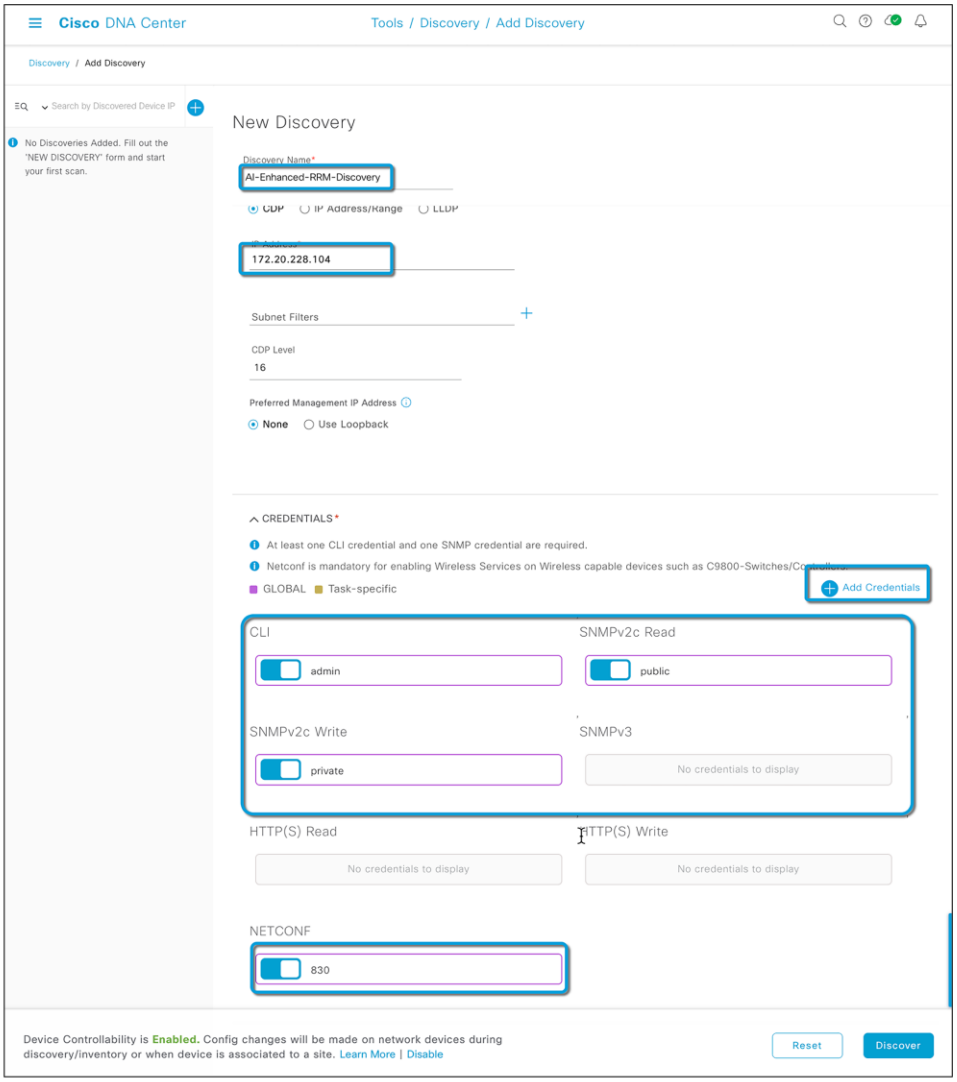
Step 4: Discover controllers and access points in Cisco DNA Center

To discover a WLC in Cisco DNA Center, follow the steps below (Figure 17):

- Enter a discovery name (any unique name for the purpose of classification on the Discovery page).
- Enter either a single IP address or a range of addresses and specify Cisco Discovery Protocol (CDP), IP Address/Range, or Link Layer Discovery Protocol (LLDP).
- Enter the SSH username and password and SNMP read and write credentials (click **Add Credentials** to do so).
- Enter the NETCONF port as 830.
- When the details are filled in, click the **Discover** button.

Notes:

- When you discover a WLC, all the joined APs will also be discovered and placed in Cisco DNA Center's inventory.
- All the CLI credentials defined in the Design section are displayed on the Discovery page.



Cisco DNA Center

Tools / Discovery / Add Discovery

Discovery / Add Discovery

Search by Discovered Device IP

No Discoveries Added. Fill out the 'NEW DISCOVERY' form and start your first scan.

New Discovery

Discovery Name*: AI-Enhanced-RRM-Discovery

● CDP ○ IP Address/Range ○ LLDP

IP Address*: 172.20.228.104

Subnet Filters

CDP Level: 16

Preferred Management IP Address

● None ○ Use Loopback

CREDENTIALS*

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

Netconf is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers.

■ GLOBAL ■ Task-specific

Add Credentials

CLI: admin

SNMPv2c Read: public

SNMPv2c Write: private

SNMPv3: No credentials to display

HTTP(S) Read: No credentials to display

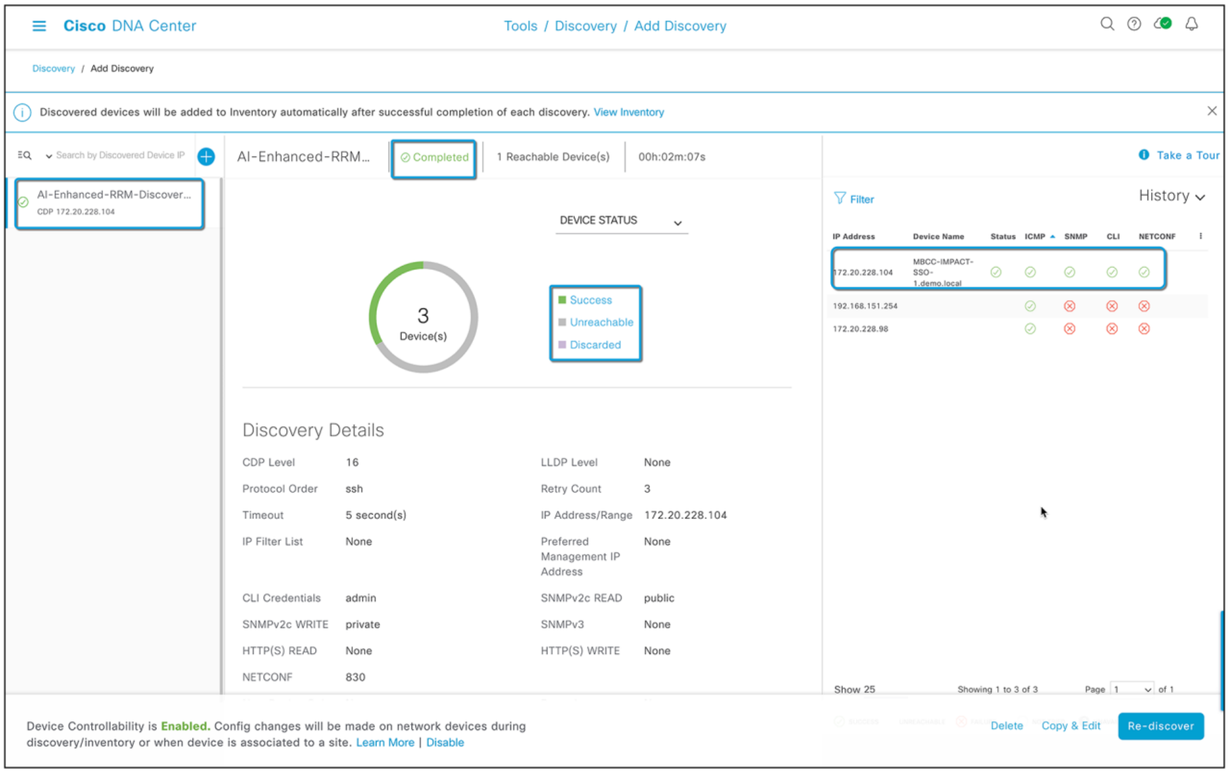
HTTP(S) Write: No credentials to display

NETCONF: 830

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

Figure 17.
Discovery page with credentials filled in and ready for discovery

- After the discovery process completes, ensure that the status of the Internet Control Message Protocol (ICMP), SNMP, NETCONF, and CLI sections is green for every device that has been discovered.



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

IP Address	Device Name	Status	ICMP	SNMP	CLI	NETCONF
172.20.228.104	MBCC-IMPACT-SSO-1.demo.local	✓	✓	✓	✓	✓
192.168.151.254			✓	⊗	⊗	⊗
172.20.228.98			✓	⊗	⊗	⊗

Show 25 Showing 1 to 3 of 3 Page 1 of 1

Discovery Details

CDP Level	16	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Address/Range	172.20.228.104
IP Filter List	None	Preferred Management IP Address	None
CLI Credentials	admin	SNMPv2c READ	public
SNMPv2c WRITE	private	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	830		

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

Figure 18.
Successful discovery of WLC on the Discovery page

Step 5: Navigate to Inventory

After the discovery process is complete, navigate to the Inventory application, where your discovered devices will be located.

- Open the hamburger menu (☰) and click **Provision** and then **Inventory** (Figure 19).

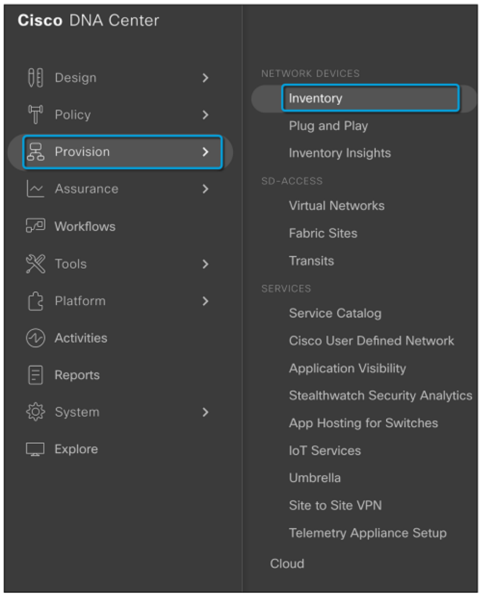
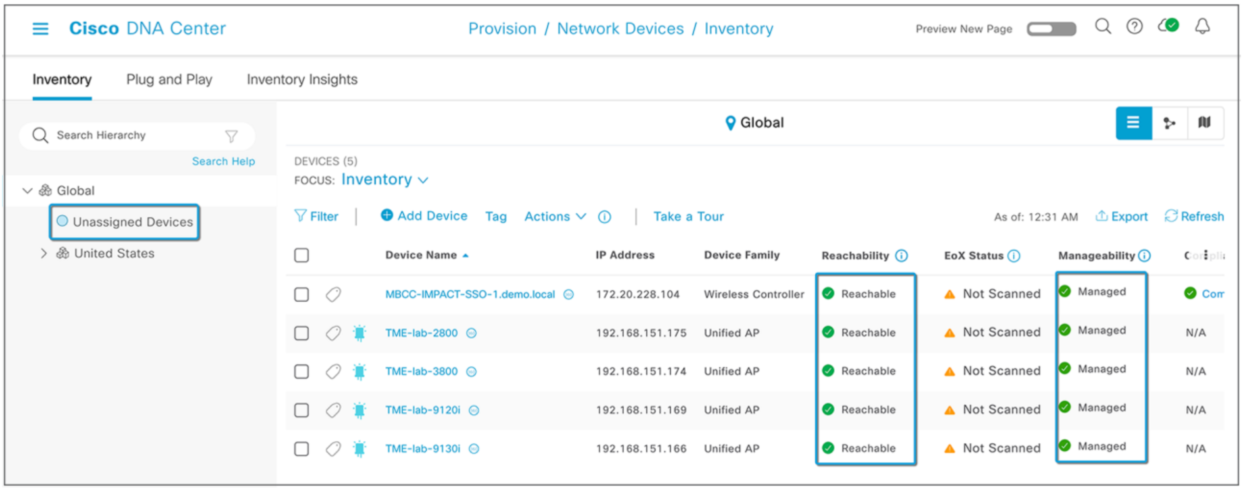


Figure 19.
Location of Inventory within the hamburger menu

- Click **Unassigned Devices** on the left side of the page and ensure that all devices are **Reachable** and that the **Manageability status** is **Managed** (Figure 20).

It is critical that all devices be in the Managed state for Cisco DNA Center Assurance functionality to work. If they are not, check the reachability of your devices.



□	Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	C
□	MBCC-IMPACT-SSO-1.demo.local	172.20.228.104	Wireless Controller	✓ Reachable	⚠ Not Scanned	✓ Managed	✓ Com
□	TME-lab-2800	192.168.151.175	Unified AP	✓ Reachable	⚠ Not Scanned	✓ Managed	N/A
□	TME-lab-3800	192.168.151.174	Unified AP	✓ Reachable	⚠ Not Scanned	✓ Managed	N/A
□	TME-lab-9120i	192.168.151.169	Unified AP	✓ Reachable	⚠ Not Scanned	✓ Managed	N/A
□	TME-lab-9130i	192.168.151.166	Unified AP	✓ Reachable	⚠ Not Scanned	✓ Managed	N/A

Figure 20.
Discovered devices and their Reachability and Manageability status

Refer to Discover Your Network in the Cisco DNA Center User Guide for more details on how to discover and add your Cisco device to the Cisco DNA Center Inventory.

Part 3: Enable Cisco AI-Enhanced RRM

Cisco DNA Center's Cisco AI Analytics page provides an option to enable all AI Analytics features and allows you to select a cloud cluster where the data will be store for AI algorithms to process.

Section goals: Enable AI-Enhanced RRM and choose a cloud cluster where your data will be stored

Step 1: Navigate to the Cisco AI Analytics page

- Click the hamburger menu (☰) in the top left corner of the screen. Click **System**, then Settings.
- Navigate to Cisco AI Analytics on the sidebar as shown.

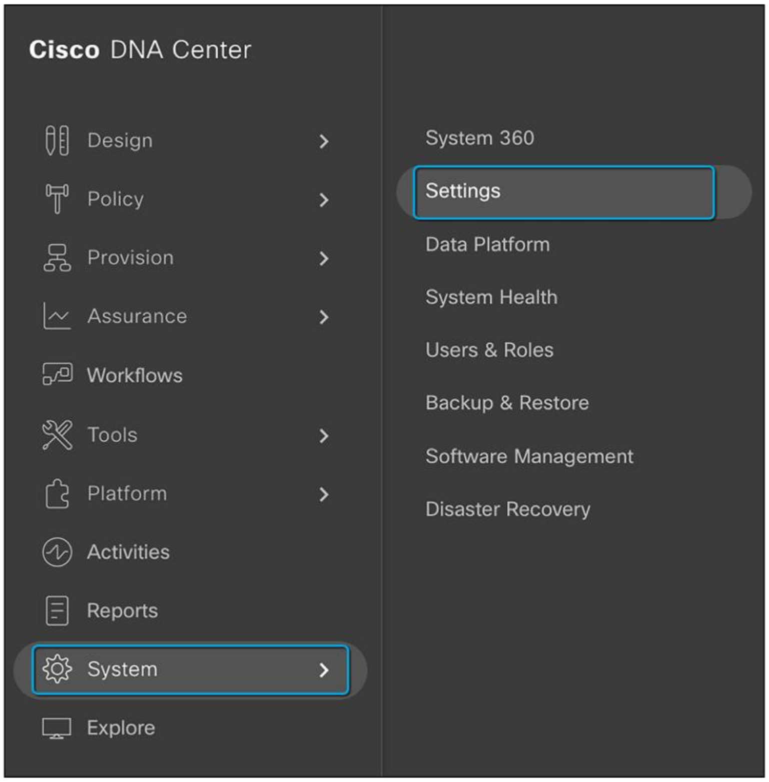
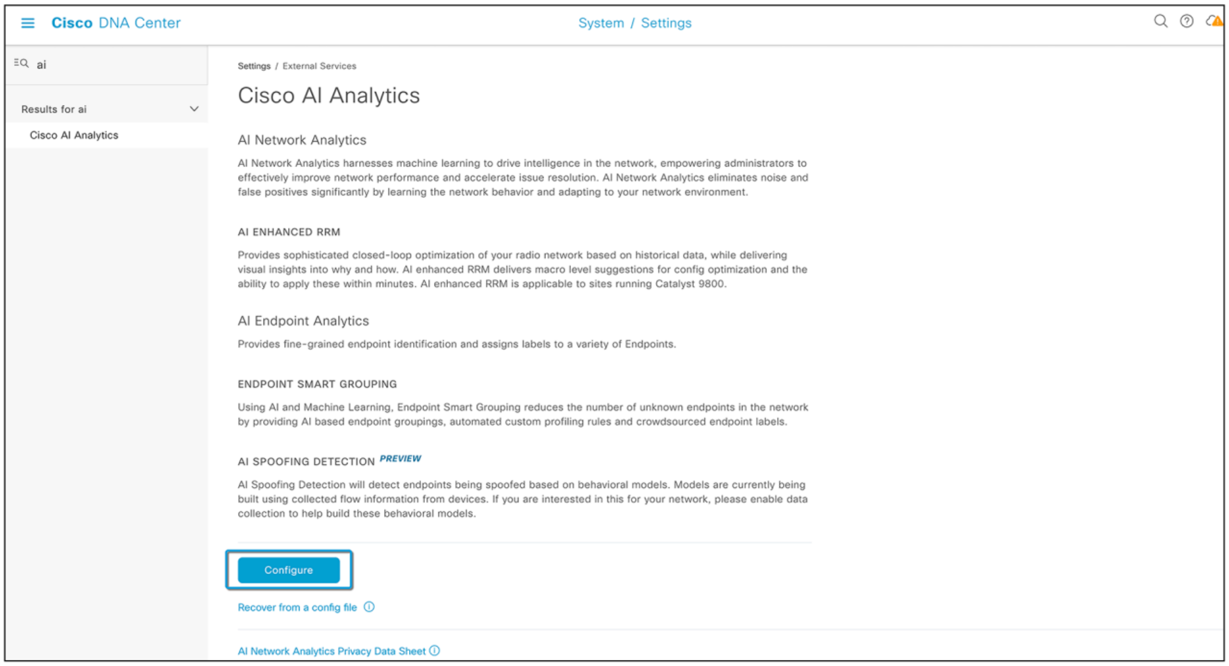


Figure 21.
Settings location



Settings / External Services

Cisco AI Analytics

AI Network Analytics

AI Network Analytics harnesses machine learning to drive intelligence in the network, empowering administrators to effectively improve network performance and accelerate issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning the network behavior and adapting to your network environment.

AI ENHANCED RRM

Provides sophisticated closed-loop optimization of your radio network based on historical data, while delivering visual insights into why and how. AI enhanced RRM delivers macro level suggestions for config optimization and the ability to apply these within minutes. AI enhanced RRM is applicable to sites running Catalyst 9800.

AI Endpoint Analytics

Provides fine-grained endpoint identification and assigns labels to a variety of Endpoints.

ENDPOINT SMART GROUPING

Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI based endpoint groupings, automated custom profiling rules and crowdsourced endpoint labels.

AI SPOOFING DETECTION *PREVIEW*

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices. If you are interested in this for your network, please enable data collection to help build these behavioral models.

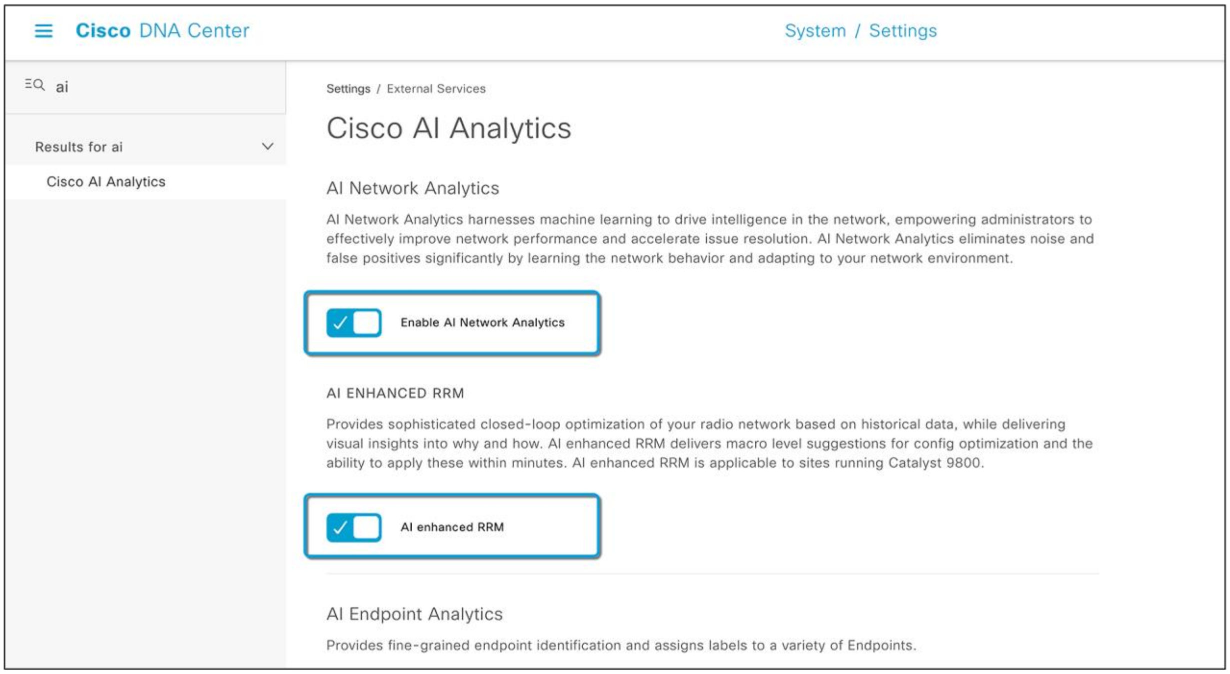
Configure
Recover from a config file
AI Network Analytics Privacy Data Sheet

Figure 22.
Location of the Cisco AI Analytics page on the Cisco DNA Center homepage

Step 2: Enable AI-Enhanced RRM

To allow Cisco DNA Center to turn on AI-Enhanced RRM, you need to:

- Enable AI Network Analytics and AI-Enhanced RRM
- Select the closest or preferred cloud cluster to store your cloud data
- Make sure the cloud connection status is green and click **Enable**



Cisco AI Analytics

AI Network Analytics

AI Network Analytics harnesses machine learning to drive intelligence in the network, empowering administrators to effectively improve network performance and accelerate issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning the network behavior and adapting to your network environment.

✓ Enable AI Network Analytics

AI ENHANCED RRM

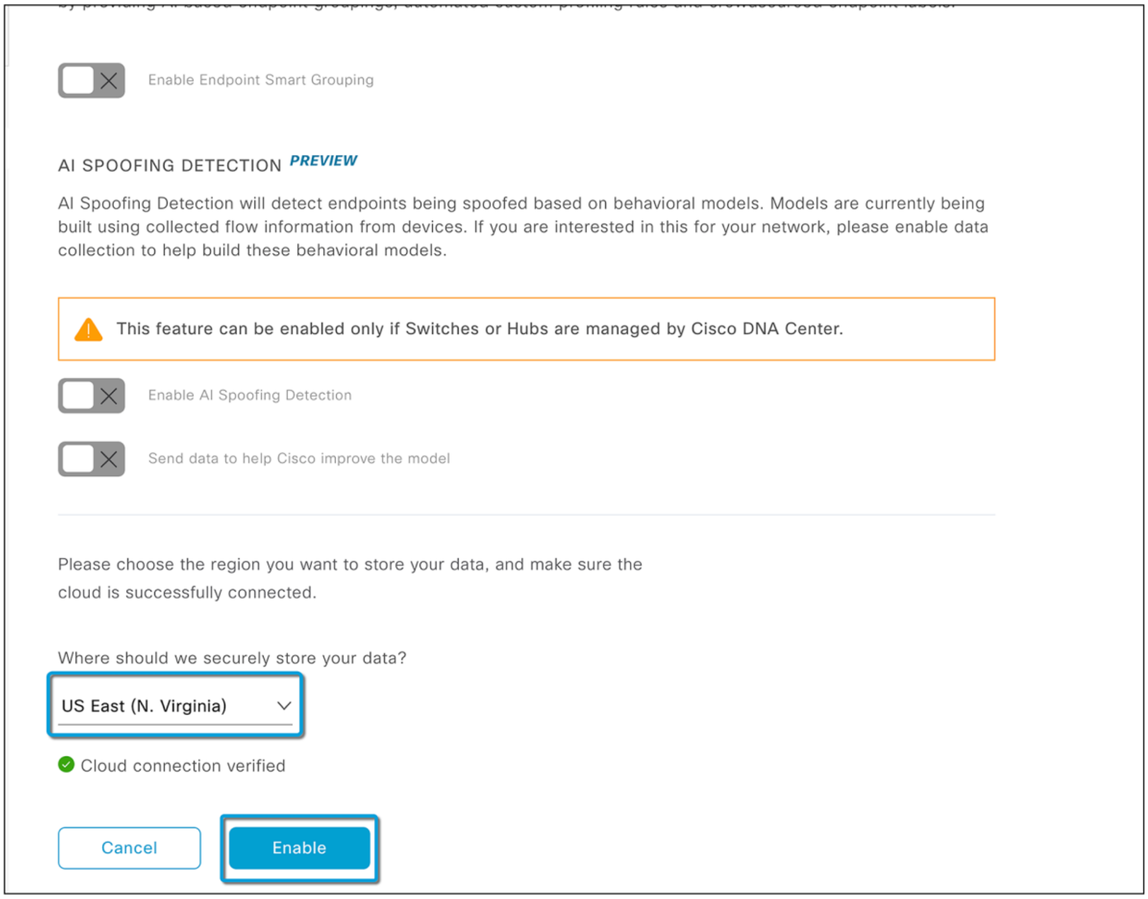
Provides sophisticated closed-loop optimization of your radio network based on historical data, while delivering visual insights into why and how. AI enhanced RRM delivers macro level suggestions for config optimization and the ability to apply these within minutes. AI enhanced RRM is applicable to sites running Catalyst 9800.

✓ AI enhanced RRM

AI Endpoint Analytics

Provides fine-grained endpoint identification and assigns labels to a variety of Endpoints.

Figure 23.
Enabling AI Network Analytics and AI-Enhanced RRM



☒ Enable Endpoint Smart Grouping

AI SPOOFING DETECTION *PREVIEW*

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices. If you are interested in this for your network, please enable data collection to help build these behavioral models.

⚠ This feature can be enabled only if Switches or Hubs are managed by Cisco DNA Center.

☒ Enable AI Spoofing Detection

☒ Send data to help Cisco improve the model

Please choose the region you want to store your data, and make sure the cloud is successfully connected.

Where should we securely store your data?

US East (N. Virginia)

✓ Cloud connection verified

Figure 24.
Selecting the cloud cluster

Part 4: Learn an existing deployment

The focus here is for Cisco DNA Center to learn all wireless configurations from the existing Cisco IOS XE wireless controller. The “Learn Device Configuration” workflow will help you learn the necessary configurations, RF profiles, SSIDs, and other information from the newly added WLC and translate these to the Cisco DNA Center network settings.

Refer to Create Network Profiles for Wireless in the Cisco DNA Center User Guide for a new wireless deployment using Cisco DNA Center.

Before you begin:

- Make sure that you have the Cisco Catalyst 9800 Series Wireless Controller in the inventory. If you do not, discover devices using the Discovery feature, as described in Part 2.
- Ensure that the Catalyst 9800 Series Wireless Controller is reachable and in a Managed state within the Inventory window. For more information, see About Inventory in the Cisco DNA Center User Guide.
- Design your network hierarchy by adding sites, buildings, and floors so that you can later easily identify where to apply design settings or configurations. You can either create a new network hierarchy or, if you have an existing network hierarchy on Cisco Prime Infrastructure, import it into Cisco DNA Center (Part 1).

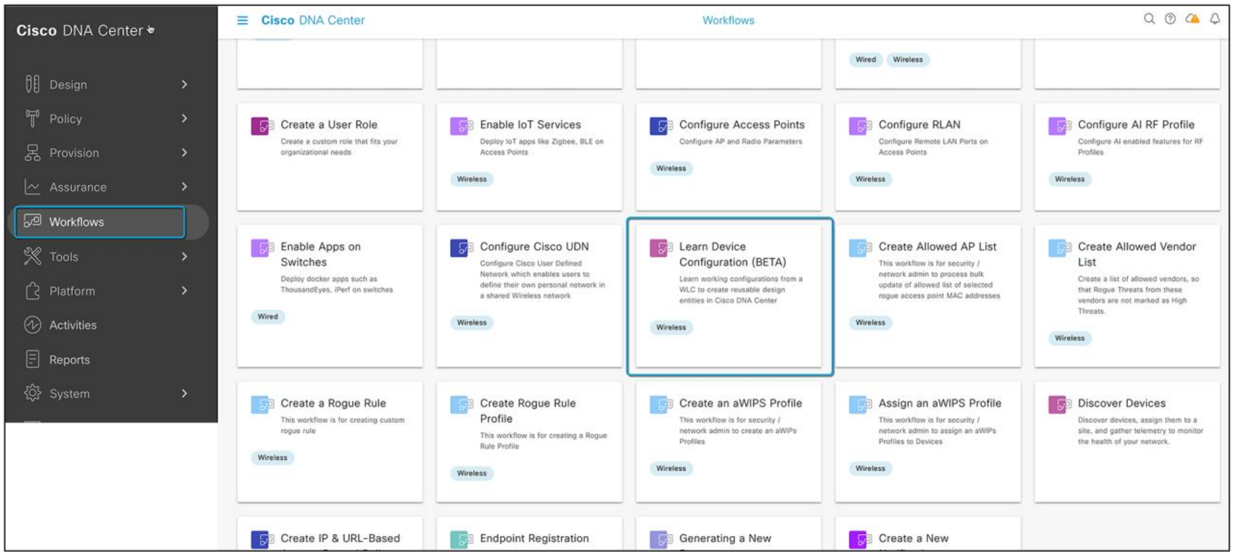
For more information about importing and uploading an existing network hierarchy, see Upload an Existing Site Hierarchy in the Cisco DNA Center User Guide.

For more information about creating a new network hierarchy, see Create a Site in a Network Hierarchy, Add a Building, and Add a Floor to a Building in the Cisco DNA Center User Guide.

Section goals: Create wireless network profiles in Cisco DNA Center using an existing Catalyst 9800 wireless controller.

Step 1: Launch the Learn Device Configuration workflow

From the hamburger menu ☰) in the top left, click Workflows. Then open the Learn Device Configuration workflow.



Create a User Role
Create a custom role that fits your organizational needs

Enable IoT Services
Deploy IoT apps like Zigbee, BLE on Access Points
Wireless

Configure Access Points
Configure AP and Radio Parameters
Wireless

Configure RLAN
Configure Remote LAN Ports on Access Points
Wireless

Configure AI RF Profile
Configure AI enabled features for RF Profiles
Wireless

Enable Apps on Switches
Deploy docker apps such as ThousandEyes, iPerf on switches
Wired

Configure Cisco UDN
Configure Cisco User Defined Network which enables users to define their own personal network in a shared Wireless network
Wireless

Learn Device Configuration (BETA)
Learn working configurations from a WLC to create reusable design entities in Cisco DNA Center
Wireless

Create Allowed AP List
This workflow is for security / network admin to process bulk update of allowed list of selected rogue access point MAC addresses
Wireless

Create Allowed Vendor List
Create a list of allowed vendors, so that Rogue Threats from these vendors are not marked as High Threats.
Wireless

Create a Rogue Rule
This workflow is for creating custom rogue rule
Wireless

Create Rogue Rule Profile
This workflow is for creating a Rogue Rule Profile
Wireless

Create an aWIPS Profile
This workflow is for security / network admin to create an aWIPs Profiles
Wireless

Assign an aWIPS Profile
This workflow is for security / network admin to assign an aWIPs Profiles to Devices
Wireless

Discover Devices
Discover devices, assign them to a site, and gather telemetry to monitor the health of your network.

Create IP & URL-Based

Endpoint Registration

Generating a New

Create a New

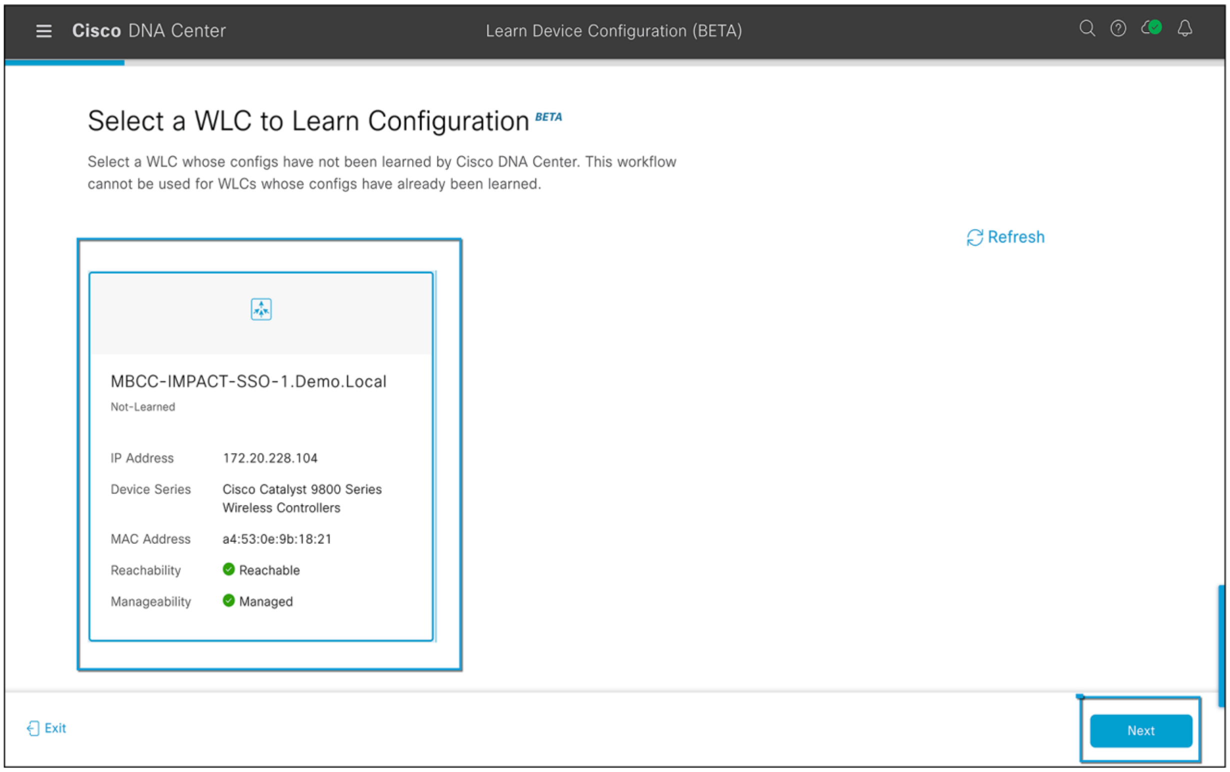
Figure 25.
Learn Device Configuration workflow

Step 2: Select the WLC from which you wish to learn the configuration

In the Select a WLC to Learn Configuration window, click the wireless controller whose configurations have not been learned by Cisco DNA Center and click Next.

Note: Make sure your controller is not provisioned or learned.

Caveat: The only way to use Learn Device Configuration to learn the configuration of a controller that is already provisioned is by deleting the Catalyst 9800 wireless controller from Inventory and adding it back.



Select a WLC to Learn Configuration BETA

Select a WLC whose configs have not been learned by Cisco DNA Center. This workflow cannot be used for WLCs whose configs have already been learned.

MBCC-IMPACT-SSO-1.Demo.Local
Not-Learned

IP Address	172.20.228.104
Device Series	Cisco Catalyst 9800 Series Wireless Controllers
MAC Address	a4:53:0e:9b:18:21
Reachability	✓ Reachable
Manageability	✓ Managed

Figure 26.
Selecting the existing WLC

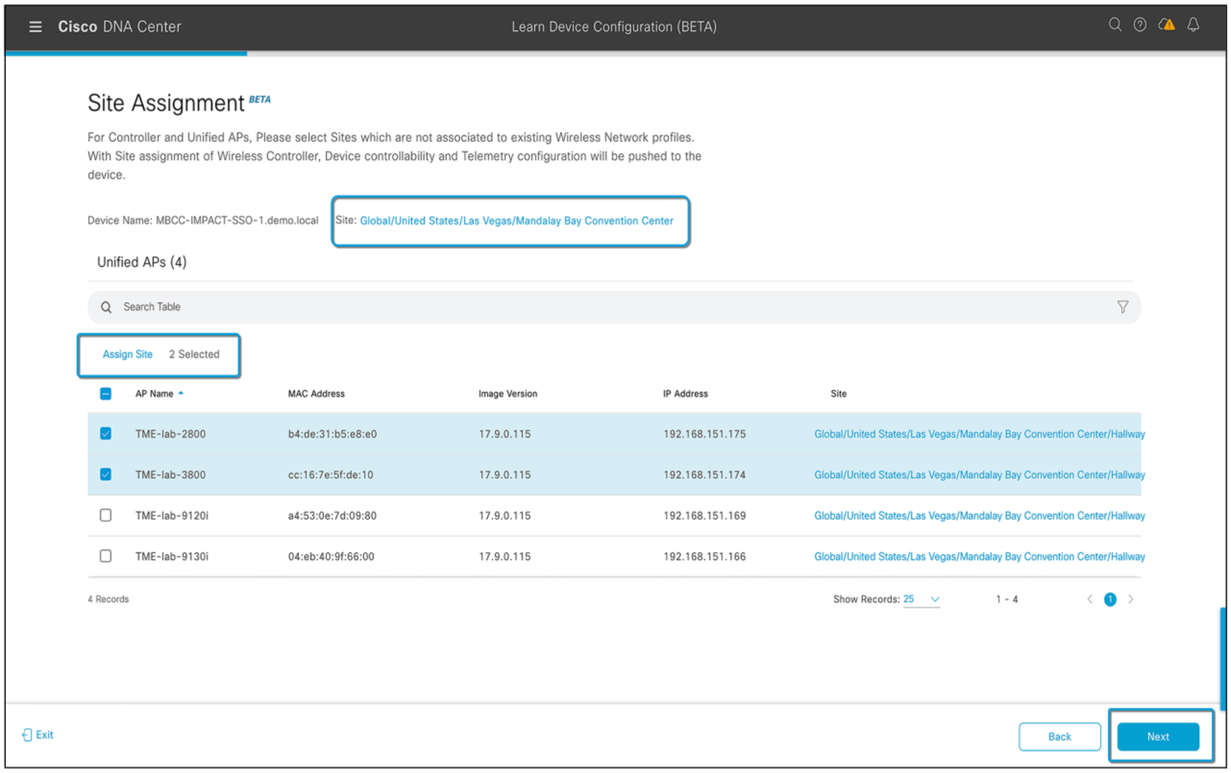
Step 3: Select sites that are NOT associated with the WLC

In the Site Assignment window, select sites that aren't associated with the existing wireless network profiles for wireless controllers and APs. (Figure 27).

Note: While you can learn device configuration without site assignment, we recommend that you assign sites, which is required to manage the same wireless controller from Cisco DNA Center.

- To assign a site to a wireless controller, click **Assign Site** next to the device name.
    - In the Assign Site window, navigate to the building that you want to associate and click **Save**.
- To assign sites to an AP, check the checkbox next to the AP name in the Unified APs table and click **Assign Site**.
    - In the Assign Site window, navigate to the floor and click **Save**.
- Click **Next**.

Note: Only sites that do not have any wireless configurations or profiles associated to them can be overwritten. If there is no fresh site, exit from the current workflow, create a new site, and then restart the workflow.



Site Assignment BETA

For Controller and Unified APs, Please select Sites which are not associated to existing Wireless Network profiles. With Site assignment of Wireless Controller, Device controllability and Telemetry configuration will be pushed to the device.

Device Name: MBCC-IMPACT-SSO-1.demo.local Site: Global/United States/Las Vegas/Mandalay Bay Convention Center

Unified APs (4)

2 Selected

	AP Name	MAC Address	Image Version	IP Address	Site
☑	TME-lab-2800	b4:de:31:b5:e8:e0	17.9.0.115	192.168.151.175	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway
☑	TME-lab-3800	cc:16:7e:5f:de:10	17.9.0.115	192.168.151.174	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway
□	TME-lab-9120i	a4:53:0e:7d:09:80	17.9.0.115	192.168.151.169	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway
□	TME-lab-9130i	04:eb:40:9f:66:00	17.9.0.115	192.168.151.166	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway

4 Records

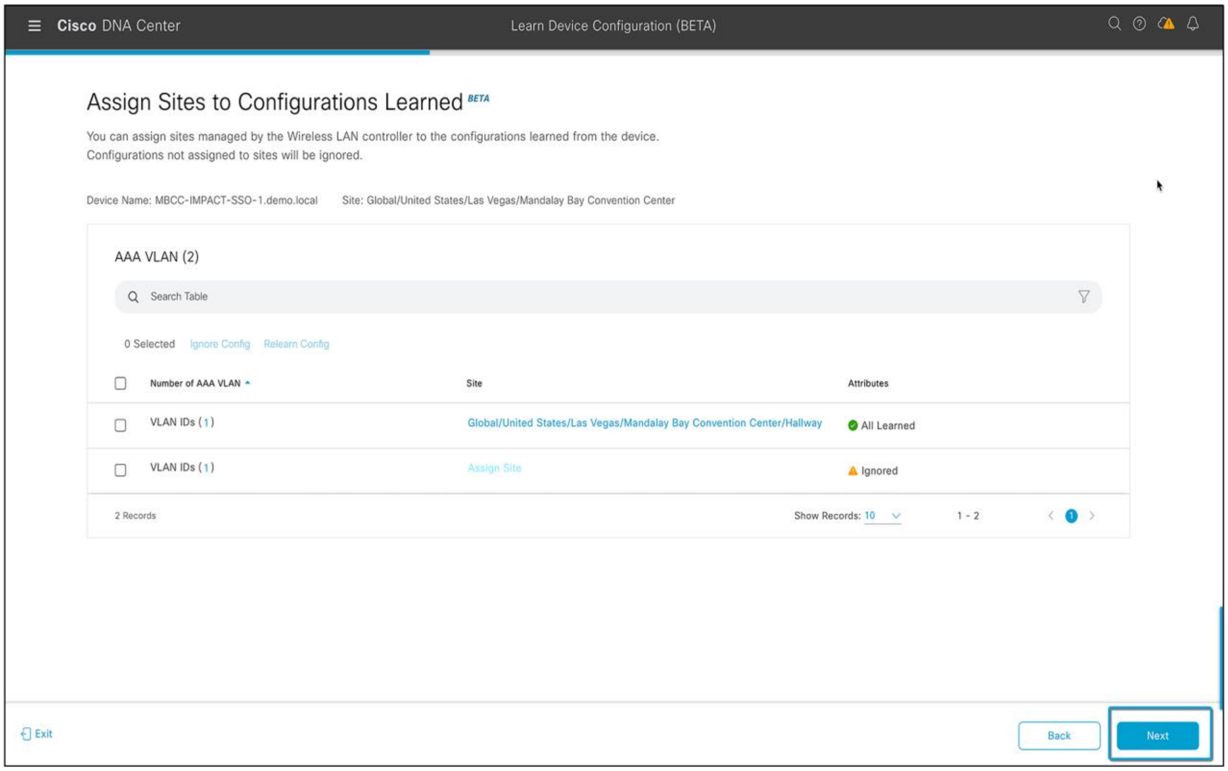
Show Records: 25 1 - 4

Figure 27.
Assigning a site to the WLC and APs

Step 4: Review the learned configurations

In the Assign Sites to Configurations Learned window, you can view the following learned configurations if the configuration is available on the device. The configurations that aren't assigned to sites are ignored.

- Flex override
- AAA server
- VLAN entry
- Mesh configuration
- Enable remote teleworker



Assign Sites to Configurations Learned BETA

You can assign sites managed by the Wireless LAN controller to the configurations learned from the device.
Configurations not assigned to sites will be ignored.

Device Name: MBCC-IMPACT-SSO-1.demo.local Site: Global/United States/Las Vegas/Mandalay Bay Convention Center

AAA VLAN (2)

☐	Number of AAA VLAN	Site	Attributes
☐	VLAN IDs (1)	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway	All Learned
☐	VLAN IDs (1)	Assign Site	Ignored

2 Records Show Records: 10 1 - 2

Figure 28.
AAA VLAN, mesh, and all Flex VLAN configurations that are learned in from an existing configuration

Step 5: Enter the shared secret for all TACACS/AAA servers

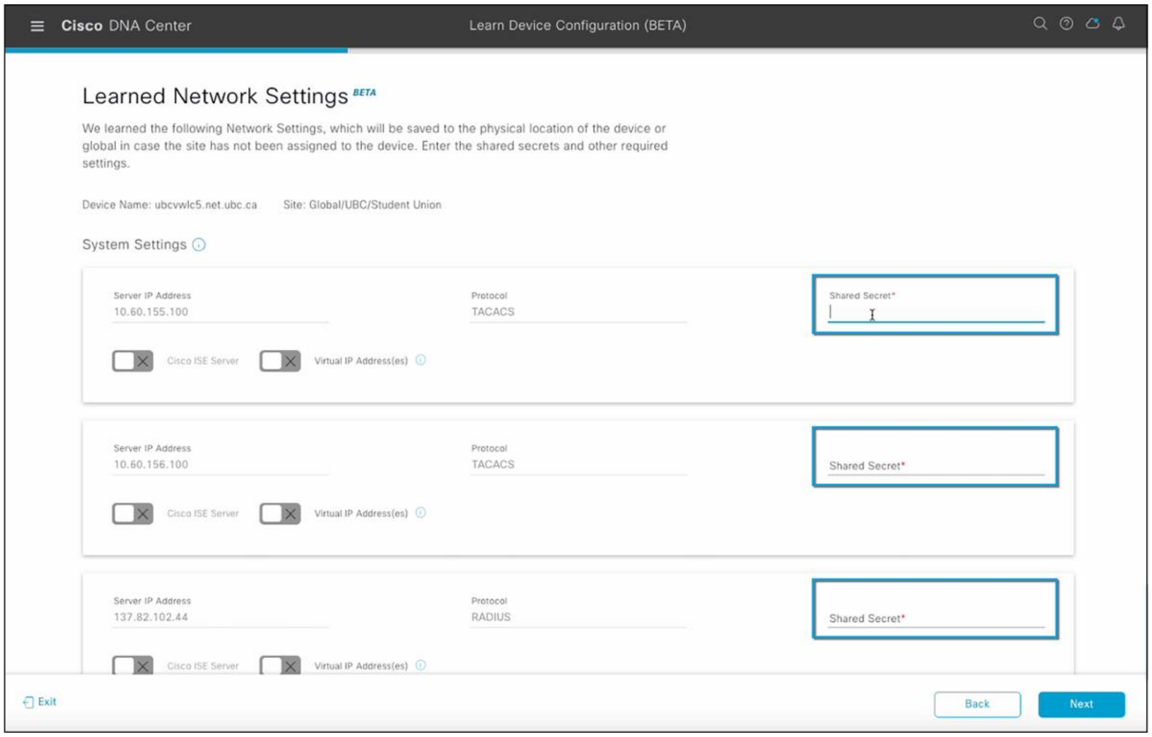
In the Learned Network Settings window, review the following learned network settings. These settings are saved to the physical location of the device. The network servers that are displayed in this window are saved at the site level. This includes Cisco ISE and all other RADIUS servers that are a part of the existing wireless controller.

- Enter the **shared secret** for AAA servers.
- **System Settings**
  - To save an AAA server as a Cisco ISE server, click the **Cisco ISE Server** toggle button and enter the **username, password**, and **FQDN** details.

Note: If the Cisco ISE server is already present on Cisco DNA Center, you cannot save an AAA server as a Cisco ISE server.

After configuring an AAA server as a Cisco ISE server, the certificate from the Cisco ISE server is automatically accepted to establish the trust.

- Click the **Virtual IP Address(es)** toggle button to enter the load balancer IP address.



Cisco DNA Center — Learn Device Configuration (BETA)

Learned Network Settings BETA

We learned the following Network Settings, which will be saved to the physical location of the device or global in case the site has not been assigned to the device. Enter the shared secrets and other required settings.

Device Name: ubcvwlc5.net.ubc.ca Site: Global/UBC/Student Union

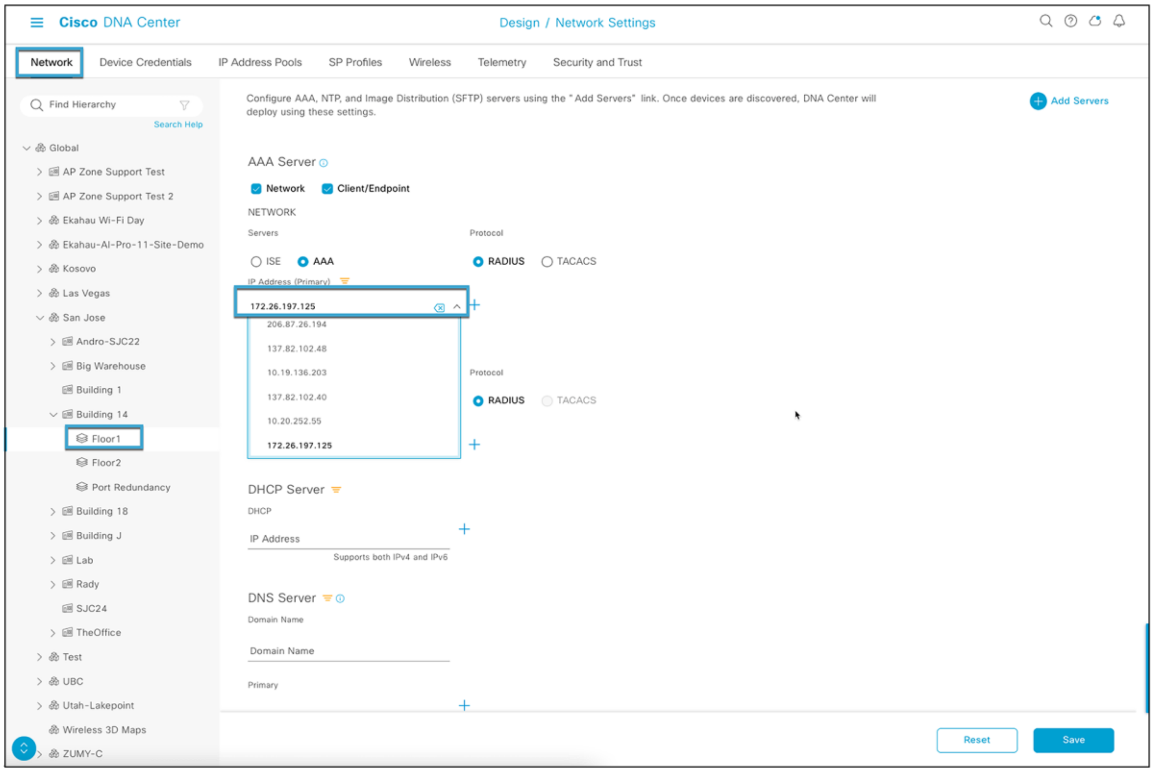
System Settings

Server IP Address: 10.60.155.100 — Protocol: TACACS — Shared Secret*

Server IP Address: 10.60.156.100 — Protocol: TACACS — Shared Secret*

Server IP Address: 137.82.102.44 — Protocol: RADIUS — Shared Secret*

Figure 29.
Entering the shared secret for all AAA servers



Cisco DNA Center — Design / Network Settings

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

AAA Server

☑ Network ☑ Client/Endpoint

NETWORK

Servers: ○ ISE ● AAA — Protocol: ● RADIUS ○ TACACS

IP Address (Primary): 172.26.197.125

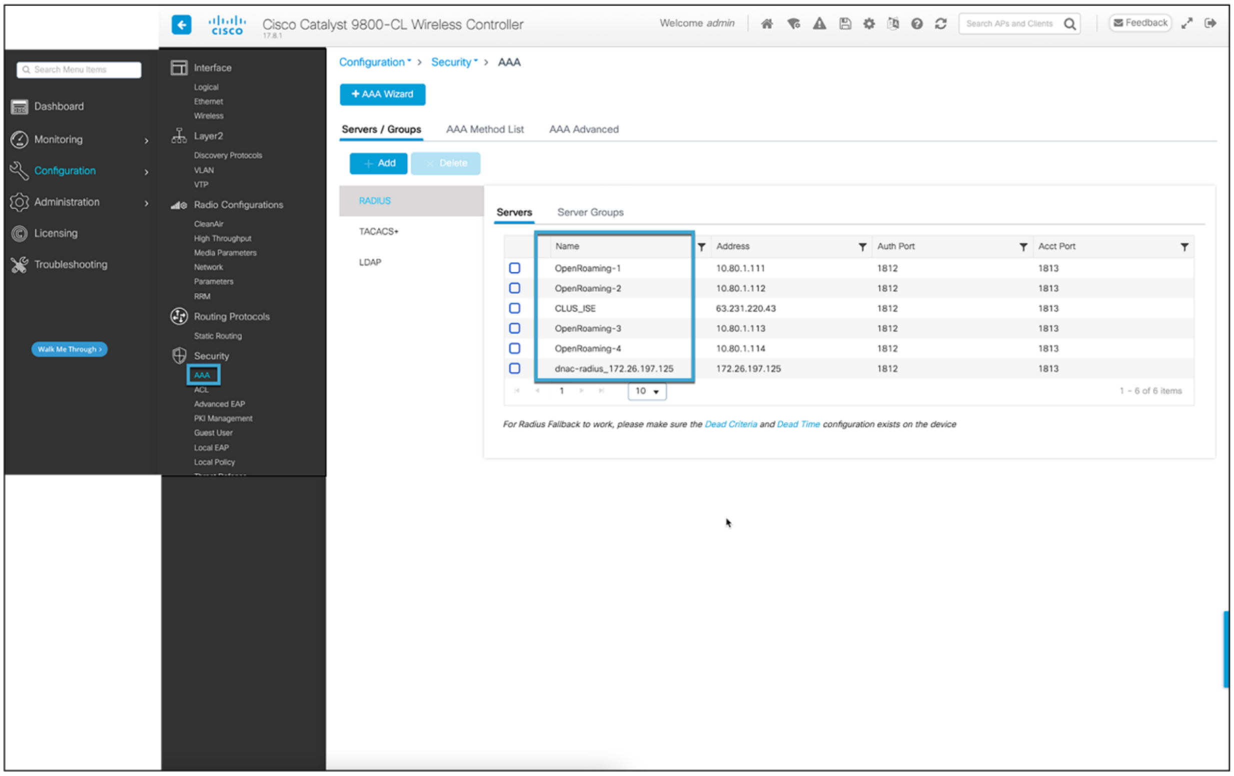
206.87.26.194
137.82.102.48
10.19.136.203
137.82.102.40
10.20.252.55
172.26.197.125

Protocol: ● RADIUS ○ TACACS

DHCP Server
DHCP: IP Address — Supports both IPv4 and IPv6

DNS Server
Domain Name: Domain Name
Primary

Figure 30.
AAA server for a site in Network Settings on Cisco DNA Center (post-learn)



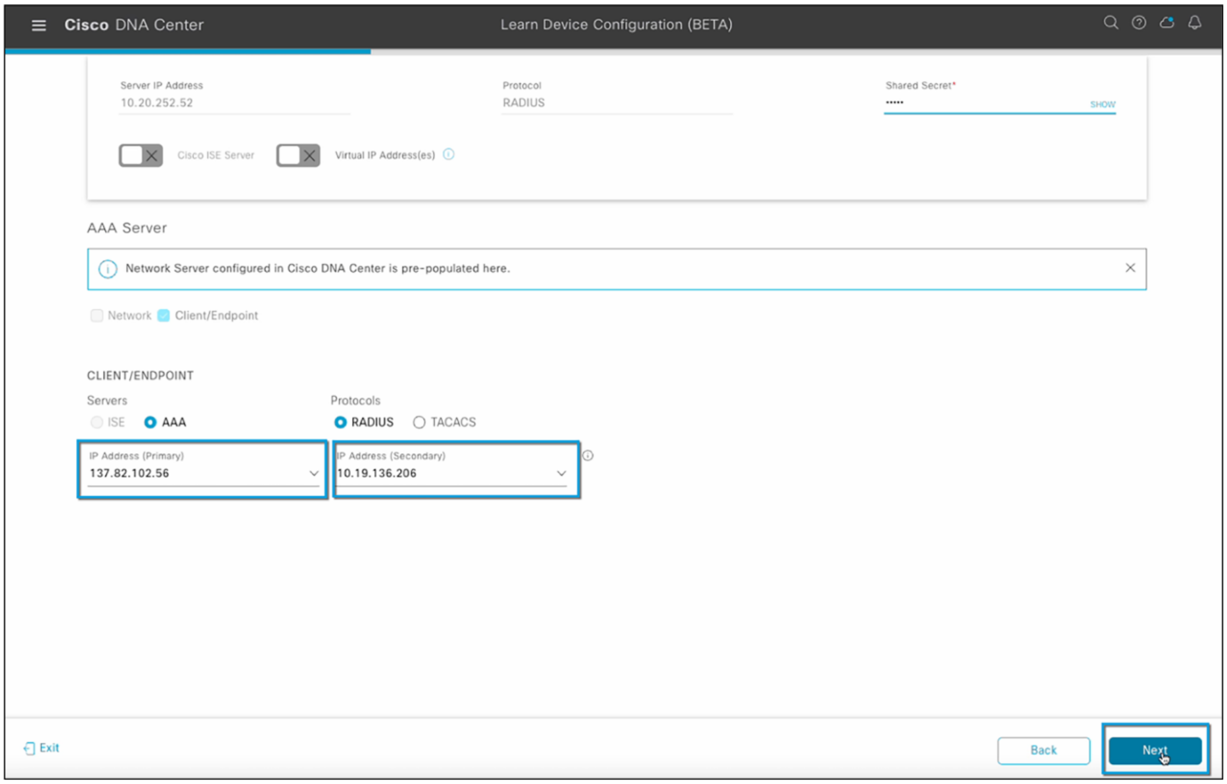
	Name	Address	Auth Port	Acct Port
☐	OpenRoaming-1	10.80.1.111	1812	1813
☐	OpenRoaming-2	10.80.1.112	1812	1813
☐	CLUS_ISE	63.231.220.43	1812	1813
☐	OpenRoaming-3	10.80.1.113	1812	1813
☐	OpenRoaming-4	10.80.1.114	1812	1813
☐	dnac-radius_172.26.197.125	172.26.197.125	1812	1813

For Radius Fallback to work, please make sure the Dead Criteria and Dead Time configuration exists on the device

Figure 31.
List of AAA/RADIUS servers on the Catalyst 9800 wireless controller (pre-learn)

- **AAA Server:** Shows the network servers configured on Cisco DNA Center. These network servers are prepopulated.
    - You can customize the network or client/endpoint for the AAA server. The servers and protocols are chosen by default.
    - From the drop-down list, choose **IP Address (Primary) and IP Address (Secondary)**. These servers are saved at the global level.
        - **DHCP Server:** Shows all the Dynamic Host Configuration Protocol (DHCP) servers available on the device.
        - **NTP Server:** Shows all the Network Time Protocol (NTP) servers available on the device.
    - Click **Next.**

Note: The following caveats apply, as Cisco DNA Center allows only one Cisco ISE and one virtual IP (VIP) server. If you have multiple RADIUS servers added to your Catalyst 9800 wireless controller, you will have to add them as AAA or TACACS servers.



Server IP Address: 10.20.252.52

Protocol: RADIUS

Shared Secret*: ••••• SHOW

☒ Cisco ISE Server ☒ Virtual IP Address(es)

AAA Server

Network Server configured in Cisco DNA Center is pre-populated here.

☐ Network ☑ Client/Endpoint

CLIENT/ENDPOINT

Servers: ○ ISE ● AAA

Protocols: ● RADIUS ○ TACACS

IP Address (Primary): 137.82.102.56

IP Address (Secondary): 10.19.136.206

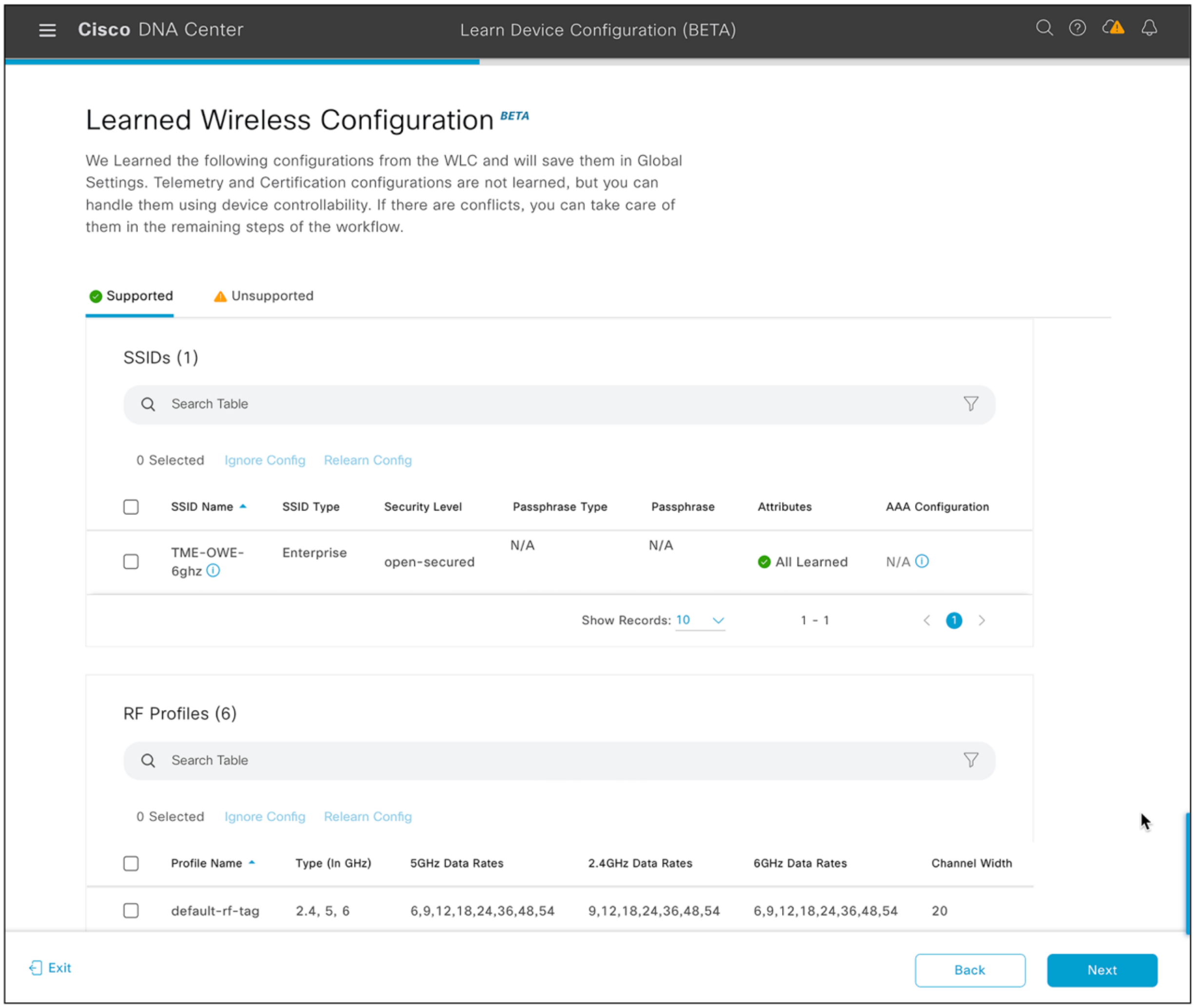
Figure 32.
Selecting primary and secondary AAA and RADIUS servers

Step 6: Verify all learned wireless configurations

In the Learned Wireless Configuration window, review the configurations learned from the wireless controller. The wireless configurations that appear in this window are saved at the global level.

- The Supported tab shows the list of learned configurations, such as SSID, RF profiles, interfaces, interface groups, aWIPS and forensic capture enablement, pre-auth ACLs, and native VLAN.
  - By default, the network access control (NAC) configuration-enabled SSIDs are learned as guest SSIDs. Click the **Edit** icon next to the **SSID Type** in the SSIDs table to change the SSID type from Guest to Enterprise.
  - To ignore the configuration, select the checkbox next to the learned configuration and click **Ignore Config** in the corresponding table.
  - To relearn an ignored SSID, RF profile, interface, or interface group, select it and click **Relearn Config** in the corresponding table.
  - All learned SSIDs without any passphrases are listed in the Supported section of the Learned Wireless Configuration window.

Note: If you have Ignored any Config, make sure add the Ignored config CLI Template to the Wireless Controller in Provisioning Wireless Controller And Access Point section.



Learned Wireless Configuration BETA

We Learned the following configurations from the WLC and will save them in Global Settings. Telemetry and Certification configurations are not learned, but you can handle them using device controllability. If there are conflicts, you can take care of them in the remaining steps of the workflow.

SSIDs (1)

□	SSID Name	SSID Type	Security Level	Passphrase Type	Passphrase	Attributes	AAA Configuration
□	TME-OWE-6ghz	Enterprise	open-secured	N/A	N/A	All Learned	N/A

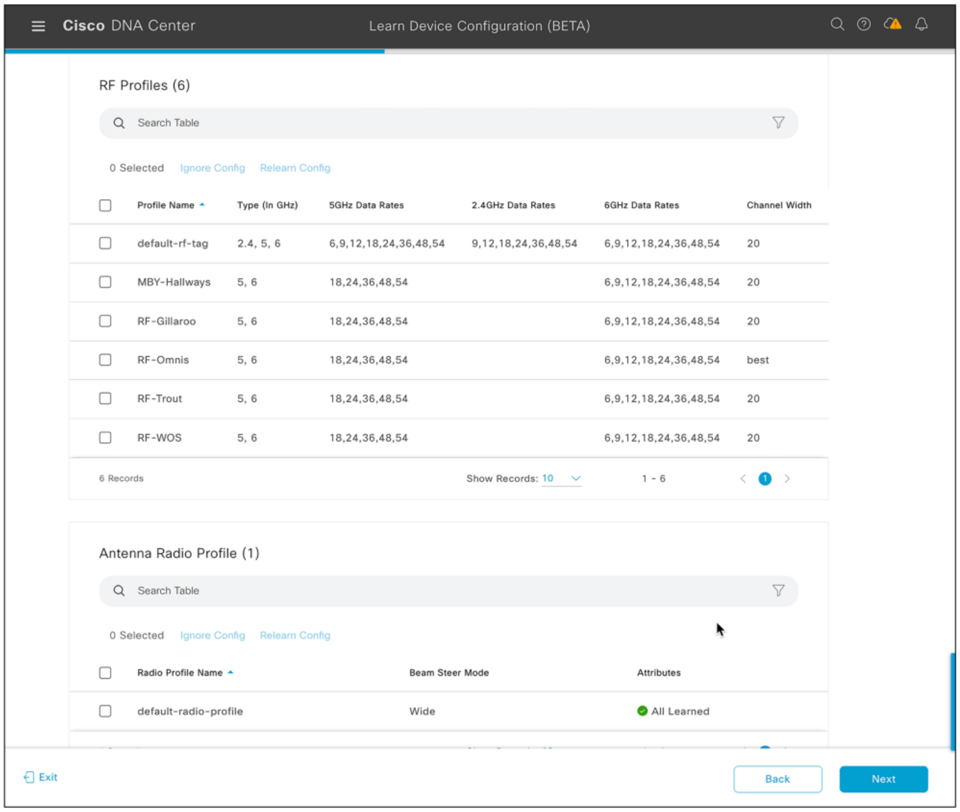
Show Records: 10 1 - 1

RF Profiles (6)

□	Profile Name	Type (In GHz)	5GHz Data Rates	2.4GHz Data Rates	6GHz Data Rates	Channel Width
□	default-rf-tag	2.4, 5, 6	6,9,12,18,24,36,48,54	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20

Figure 33.
Learned wireless configurations

- All Cisco DNA Center-supported RF profiles are listed here, with all bands, supported data rates for each band, and preferred channel width. It also lists all systems and custom-created RF profiles.
- These learned RF profiles can be found in the global site hierarchy, accessed by going to the hamburger menu (☰) and choosing Design > Network Settings > Wireless.
- This list should include all the RF profiles from the Catalyst 9800 wireless controller located in Configuration > Tags & Profiles > RF/Radio > RF, as shown in the figures below.
- A new RF profile will be pushed to the Catalyst 9800 wireless controller in the further steps after the AI RF profile is created.



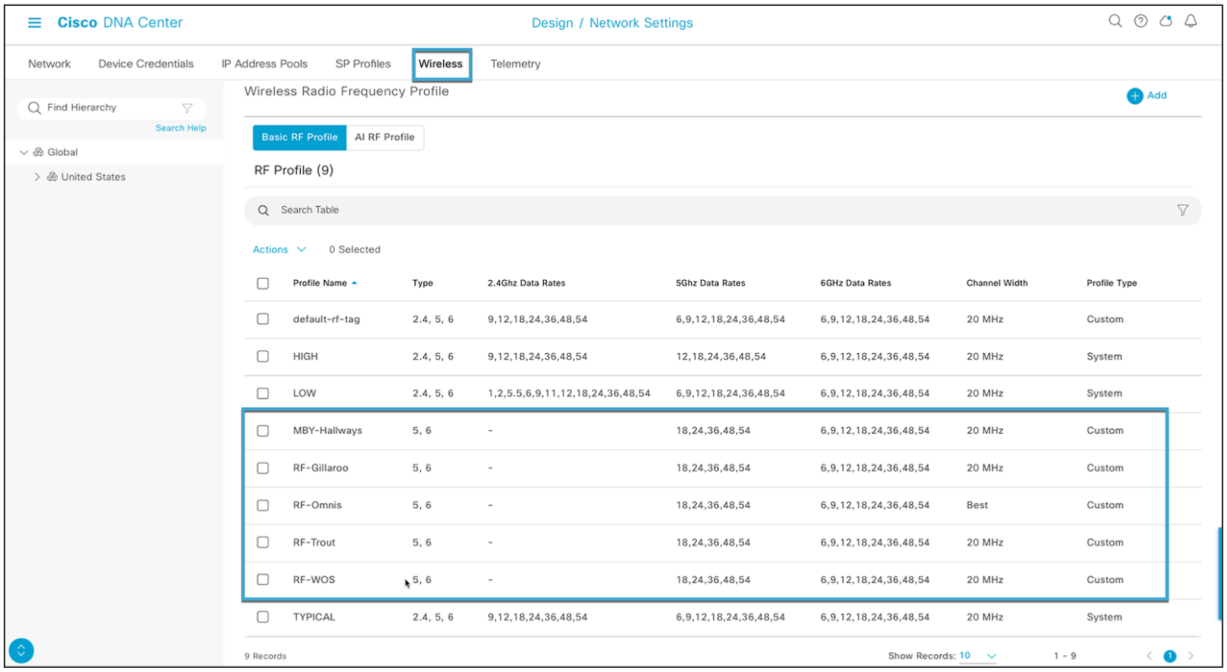
RF Profiles (6)

Profile Name	Type (In GHz)	5GHz Data Rates	2.4GHz Data Rates	6GHz Data Rates	Channel Width
default-rf-tag	2.4, 5, 6	6,9,12,18,24,36,48,54	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20
MBY-Hallways	5, 6	18,24,36,48,54		6,9,12,18,24,36,48,54	20
RF-Gillaroo	5, 6	18,24,36,48,54		6,9,12,18,24,36,48,54	20
RF-Omnis	5, 6	18,24,36,48,54		6,9,12,18,24,36,48,54	best
RF-Trout	5, 6	18,24,36,48,54		6,9,12,18,24,36,48,54	20
RF-WOS	5, 6	18,24,36,48,54		6,9,12,18,24,36,48,54	20

Antenna Radio Profile (1)

Radio Profile Name	Beam Steer Mode	Attributes
default-radio-profile	Wide	✓ All Learned

Figure 34.
Learned wireless configurations (RF profiles)

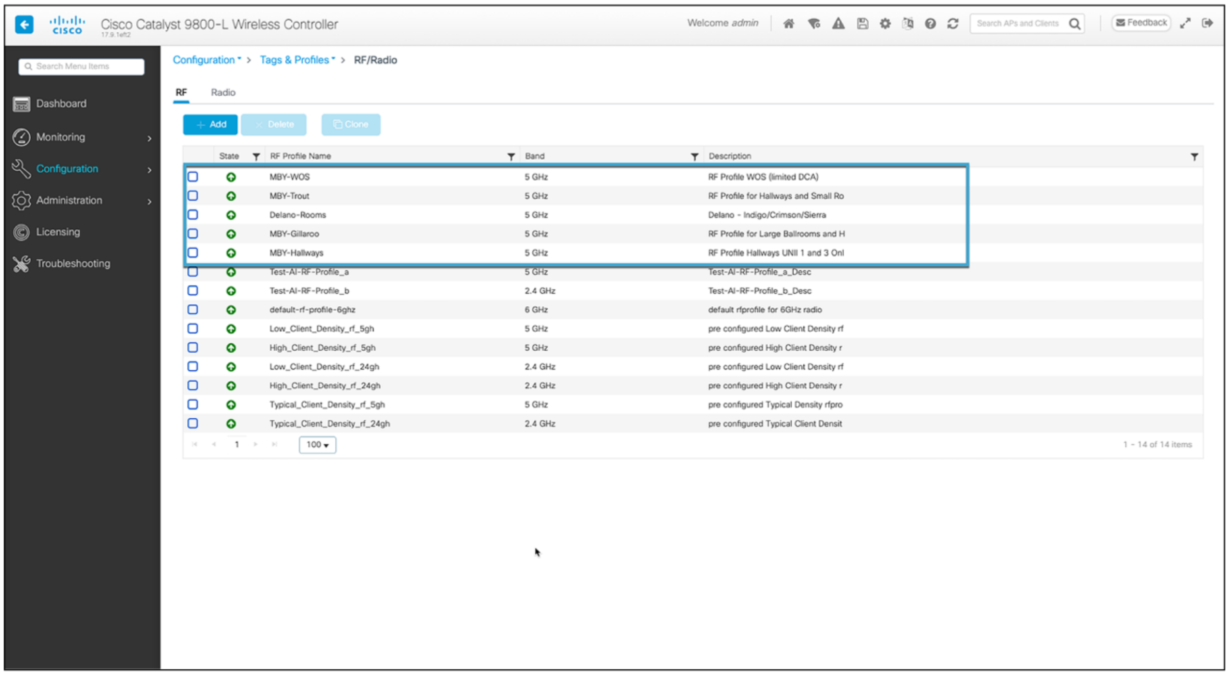


Wireless Radio Frequency Profile

RF Profile (9)

Profile Name	Type	2.4Ghz Data Rates	5Ghz Data Rates	6GHz Data Rates	Channel Width	Profile Type
default-rf-tag	2.4, 5, 6	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
HIGH	2.4, 5, 6	9,12,18,24,36,48,54	12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	System
LOW	2.4, 5, 6	1,2,5.5,6,9,11,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	System
MBY-Hallways	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
RF-Gillaroo	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
RF-Omnis	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	Best	Custom
RF-Trout	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
RF-WOS	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
TYPICAL	2.4, 5, 6	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	System

Figure 35.
RF profiles on Cisco DNA Center in Network Settings > Wireless tab (post-learn)

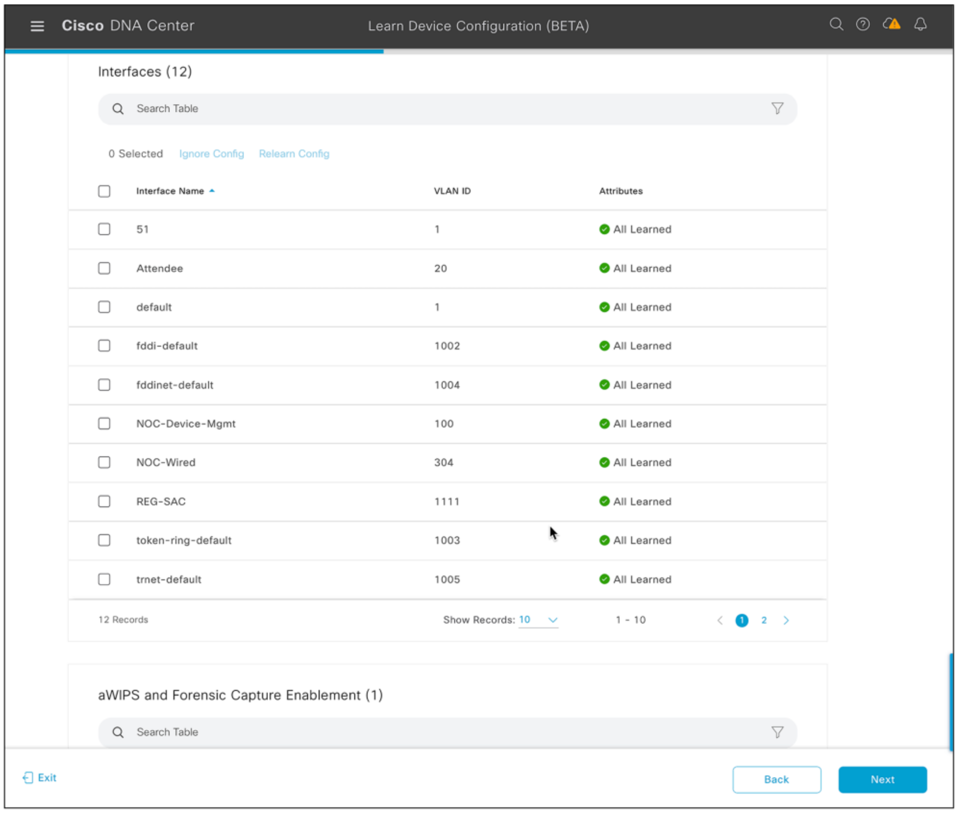


	State	RF Profile Name	Band	Description
☐	⊕	MBY-WOS	5 GHz	RF Profile WOS (limited DCA)
☐	⊕	MBY-Trout	5 GHz	RF Profile for Hallways and Small Ro
☐	⊕	Delano-Rooms	5 GHz	Delano - Indigo/Crimson/Sierra
☐	⊕	MBY-Gillaroo	5 GHz	RF Profile for Large Ballrooms and H
☐	⊕	MBY-Hallways	5 GHz	RF Profile Hallways UNII 1 and 3 Onl
☐	⊕	Test-AI-RF-Profile_a	5 GHz	Test-AI-RF-Profile_a_Desc
☐	⊕	Test-AI-RF-Profile_b	2.4 GHz	Test-AI-RF-Profile_b_Desc
☐	⊕	default-rf-profile-6ghz	6 GHz	default rfprofile for 6GHz radio
☐	⊕	Low_Client_Density_rf_5gh	5 GHz	pre configured Low Client Density rf
☐	⊕	High_Client_Density_rf_5gh	5 GHz	pre configured High Client Density r
☐	⊕	Low_Client_Density_rf_24gh	2.4 GHz	pre configured Low Client Density rf
☐	⊕	High_Client_Density_rf_24gh	2.4 GHz	pre configured High Client Density r
☐	⊕	Typical_Client_Density_rf_5gh	5 GHz	pre configured Typical Density rfpro
☐	⊕	Typical_Client_Density_rf_24gh	2.4 GHz	pre configured Typical Client Densit

1 100 1 - 14 of 14 items

Figure 36.
RF profiles on the Catalyst 9800 wireless controller (pre-learn)

- All wireless and wired interfaces from the Catalyst 9800 wireless controller (Figure 39) are listed here.
- These interfaces will automatically be mapped to any existing SSIDs and Flex groups on the wireless controller.
- Interfaces can also be used for any newly created SSID as well.
    - These wireless interfaces can be found in the global site hierarchy, accessed by going to the hamburger menu (☰) and choosing Design > Network Settings > Wireless (Figure 38).

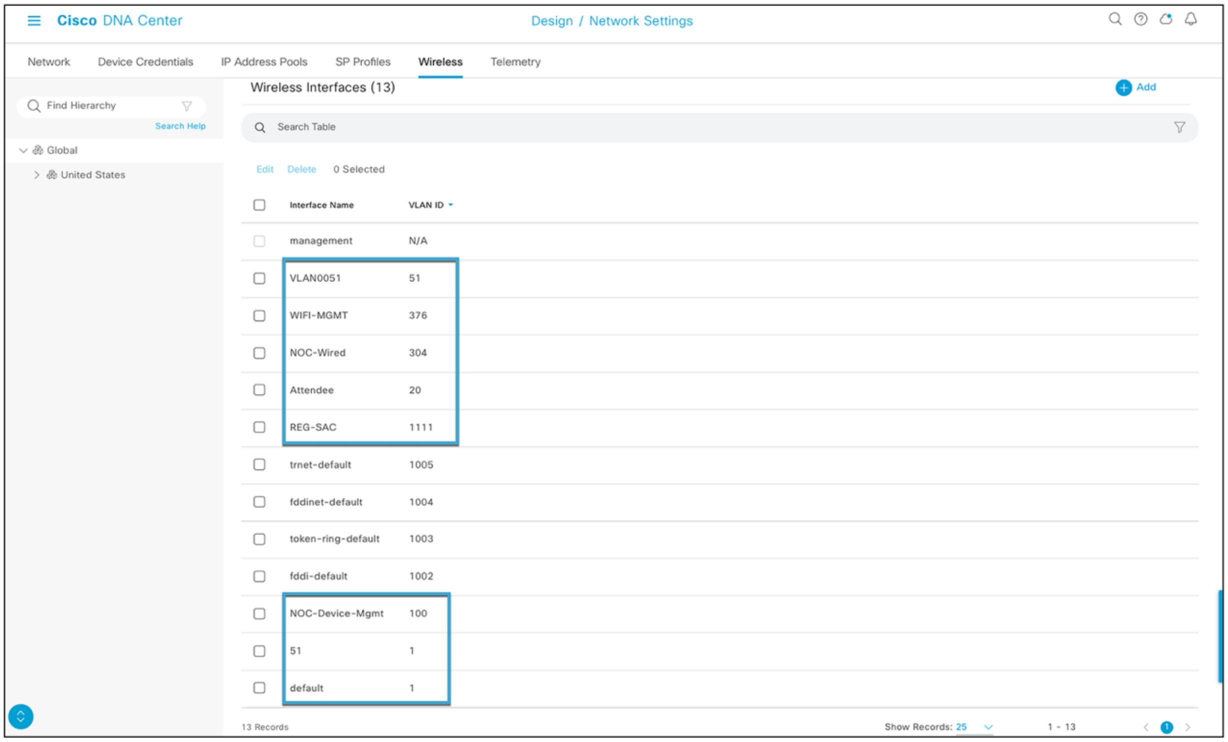


Interfaces (12)

Interface Name	VLAN ID	Attributes
51	1	All Learned
Attendee	20	All Learned
default	1	All Learned
fddi-default	1002	All Learned
fddinet-default	1004	All Learned
NOC-Device-Mgmt	100	All Learned
NOC-Wired	304	All Learned
REG-SAC	1111	All Learned
token-ring-default	1003	All Learned
trnet-default	1005	All Learned

aWIPS and Forensic Capture Enablement (1)

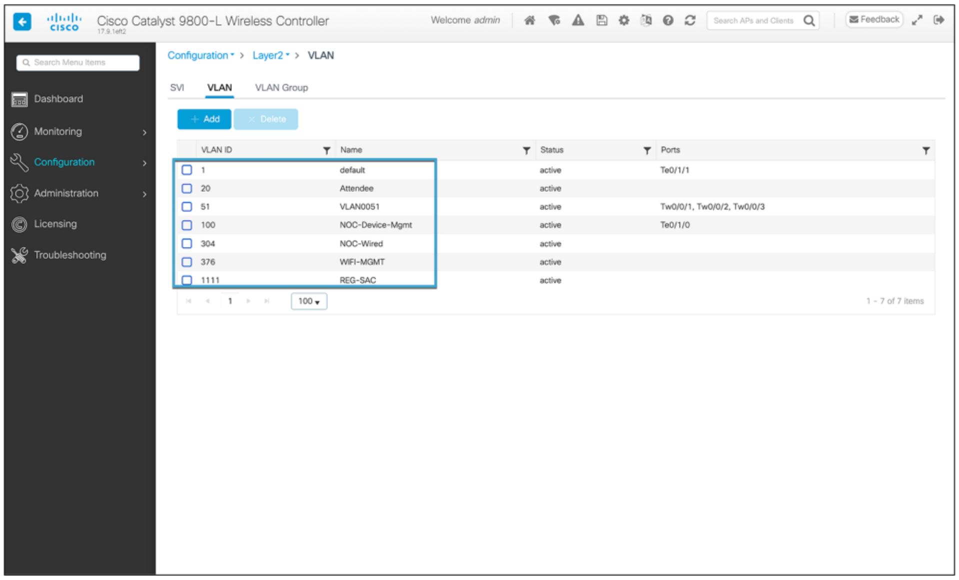
Figure 37.
Learned wireless configurations (interfaces)



Wireless Interfaces (13)

Interface Name	VLAN ID
management	N/A
VLAN0051	51
WIFI-MGMT	376
NOC-Wired	304
Attendee	20
REG-SAC	1111
trnet-default	1005
fddinet-default	1004
token-ring-default	1003
fddi-default	1002
NOC-Device-Mgmt	100
51	1
default	1

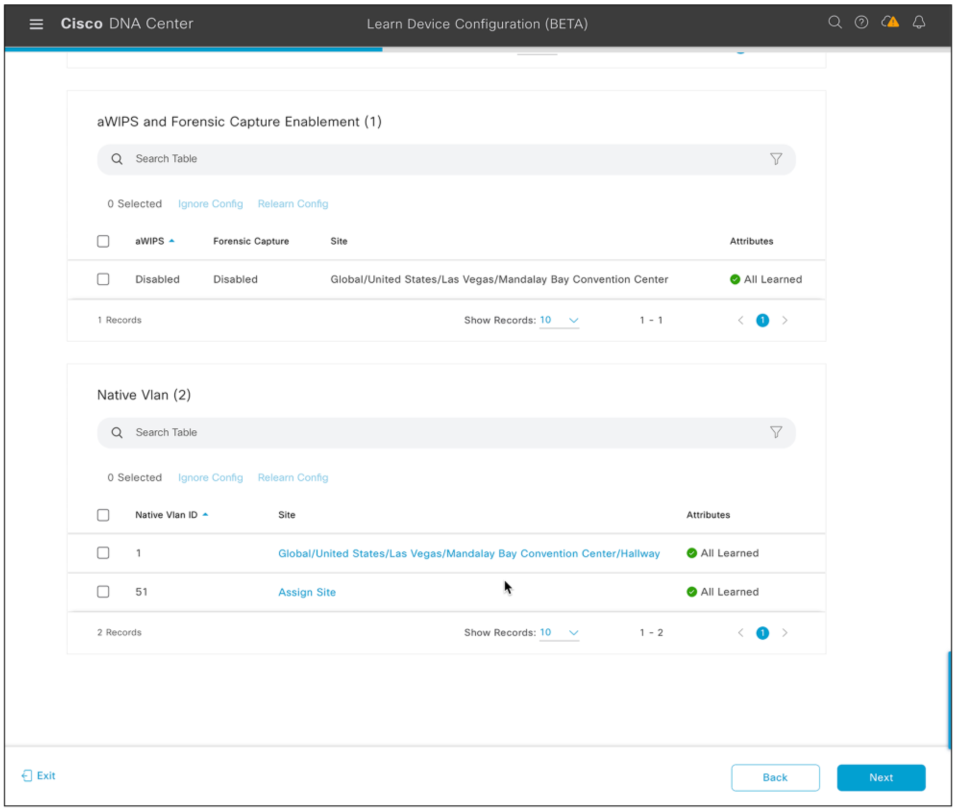
Figure 38.
Wireless interfaces on Cisco DNA Center in Network Settings > Wireless tab (post-learn)



	VLAN ID	Name	Status	Ports
□	1	default	active	Te0/1/1
□	20	Attendee	active	
□	51	VLAN0051	active	Tw0/0/1, Tw0/0/2, Tw0/0/3
□	100	NOC-Device-Mgmt	active	Te0/1/0
□	304	NOC-Wired	active	
□	376	WIFI-MGMT	active	
□	1111	REG-SAC	active	

Figure 39.
Interfaces on the Catalyst 9800 wireless controller (pre-learn)

- Any aWIPS configuration on the Catalyst 9800 wireless controller will be learned here. This configuration can be found in the aWIPS profile on Cisco DNA Center, as shown in Figure 41.



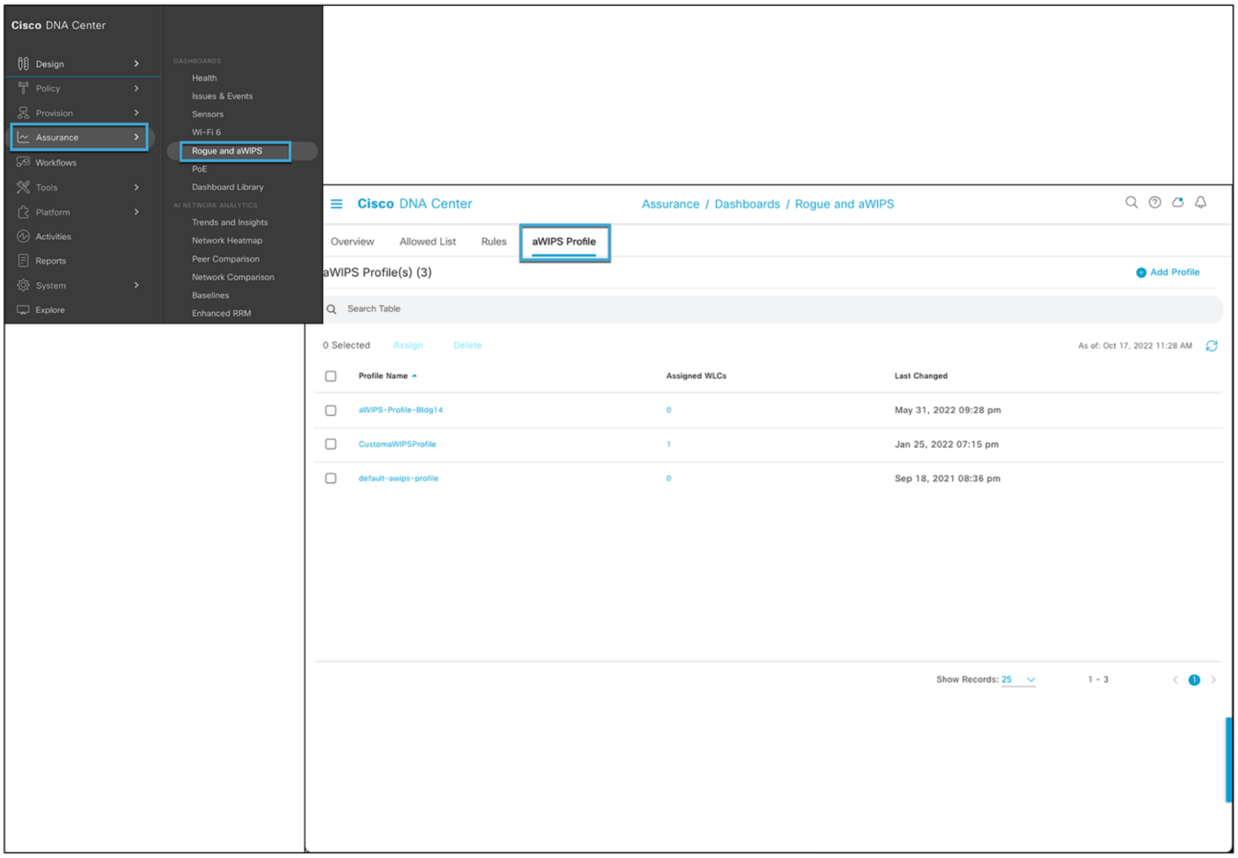
aWIPS and Forensic Capture Enablement (1)

□	aWIPS	Forensic Capture	Site	Attributes
□	Disabled	Disabled	Global/United States/Las Vegas/Mandalay Bay Convention Center	All Learned

Native Vlan (2)

□	Native Vlan ID	Site	Attributes
□	1	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway	All Learned
□	51	Assign Site	All Learned

Figure 40.
Learned wireless configurations (aWIPS)



aWIPS Profile(s) (3)

0 Selected

As of: Oct 17, 2022 11:28 AM

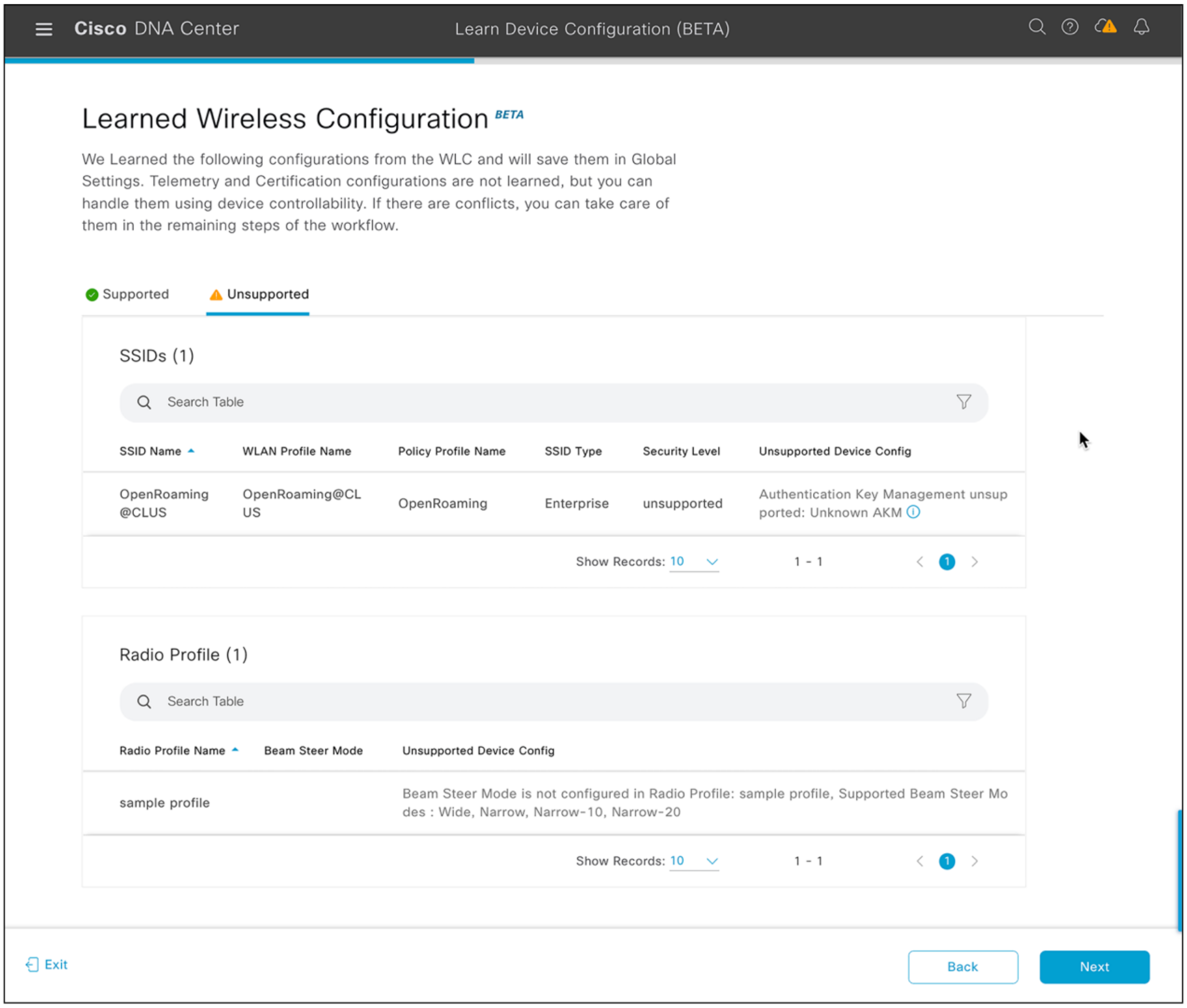
□	Profile Name	Assigned WLCs	Last Changed
□	aWIPS-Profile-Bldg14	0	May 31, 2022 09:28 pm
□	CustomaWIPSProfile	1	Jan 25, 2022 07:15 pm
□	default-awips-profile	0	Sep 18, 2021 08:36 pm

Show Records: 25 1 - 3

Figure 41.
aWIPS profile in Assurance

- The Unsupported tab shows the configurations that are not learned, such as SSIDs, RF profiles, interfaces, pre-auth-ACLs, and interface groups. You can address these unsupported or unknown configurations and use CLI templates.

Note: Any unsupported configuration in the Learn Device Configuration workflow will result in Cisco DNA Center creating a new policy/site tag for the configuration and pushing it to the controller along with the CLI template.



Learned Wireless Configuration BETA

We Learned the following configurations from the WLC and will save them in Global Settings. Telemetry and Certification configurations are not learned, but you can handle them using device controllability. If there are conflicts, you can take care of them in the remaining steps of the workflow.

SSIDs (1)

SSID Name	WLAN Profile Name	Policy Profile Name	SSID Type	Security Level	Unsupported Device Config
OpenRoaming @CLUS	OpenRoaming@CLUS	OpenRoaming	Enterprise	unsupported	Authentication Key Management unsupported: Unknown AKM ⓘ

Radio Profile (1)

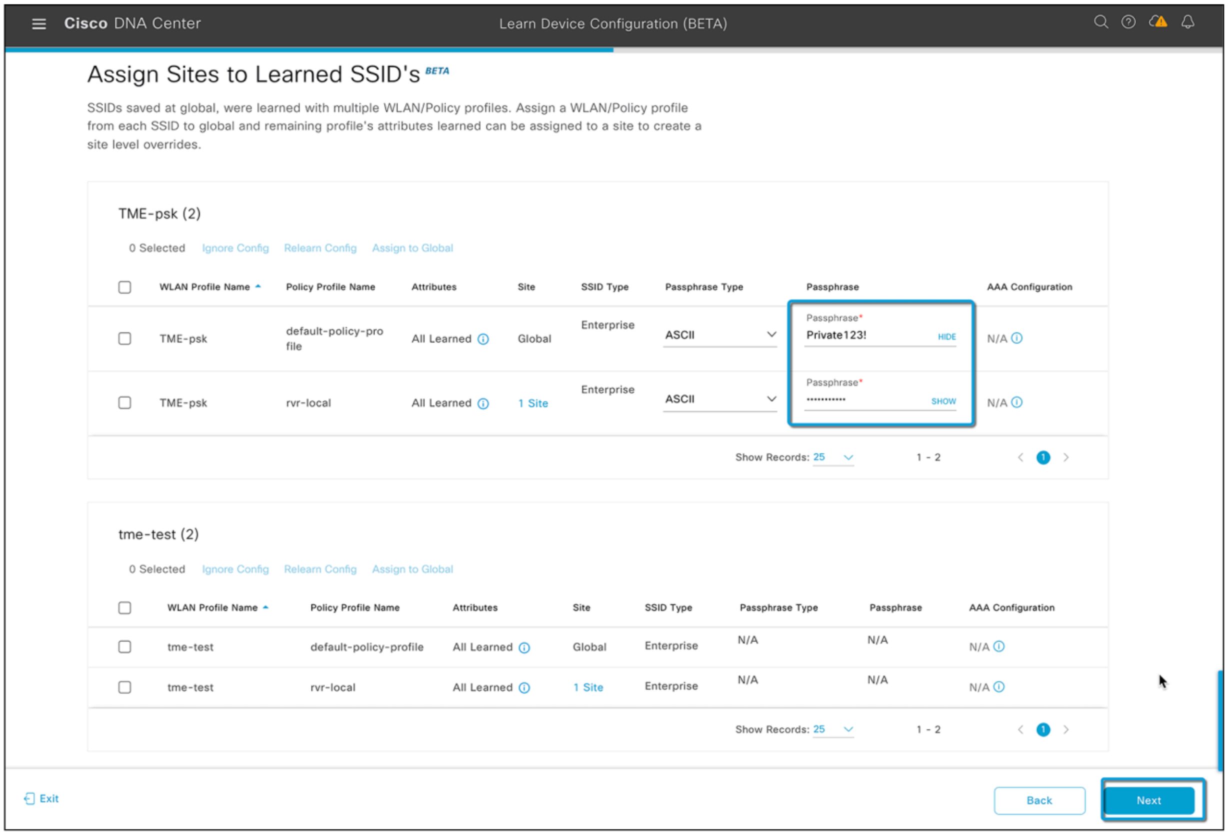
Radio Profile Name	Beam Steer Mode	Unsupported Device Config
sample profile		Beam Steer Mode is not configured in Radio Profile: sample profile, Supported Beam Steer Modes : Wide, Narrow, Narrow-10, Narrow-20

Figure 42.
Unsupported wireless configurations

Step 7: Enter passphrase to all PSK SSIDs

In the Assign Sites to Learned SSIDs window, review and resolve any “multiple WLAN profile” conflicts.

- The SSIDs that are saved at the global level and learned with multiple WLAN profiles are listed. You can assign a WLAN profile from each SSID to the global level and another profile to a particular site to resolve the conflict.
- (Optional) To assign a WLAN profile to a site, click **Assign Site** in the corresponding SSID row.
    - In the Assign Site window, choose a site and click **Save**.



Assign Sites to Learned SSID's BETA

SSIDs saved at global, were learned with multiple WLAN/Policy profiles. Assign a WLAN/Policy profile from each SSID to global and remaining profile's attributes learned can be assigned to a site to create a site level overrides.

TME-psk (2)

0 Selected Ignore Config Relearn Config Assign to Global

□	WLAN Profile Name	Policy Profile Name	Attributes	Site	SSID Type	Passphrase Type	Passphrase	AAA Configuration
□	TME-psk	default-policy-profile	All Learned ⓘ	Global	Enterprise	ASCII	Passphrase* Private123! HIDE	N/A ⓘ
□	TME-psk	rvr-local	All Learned ⓘ	1 Site	Enterprise	ASCII	Passphrase* •••••••••••• SHOW	N/A ⓘ

Show Records: 25 1 - 2

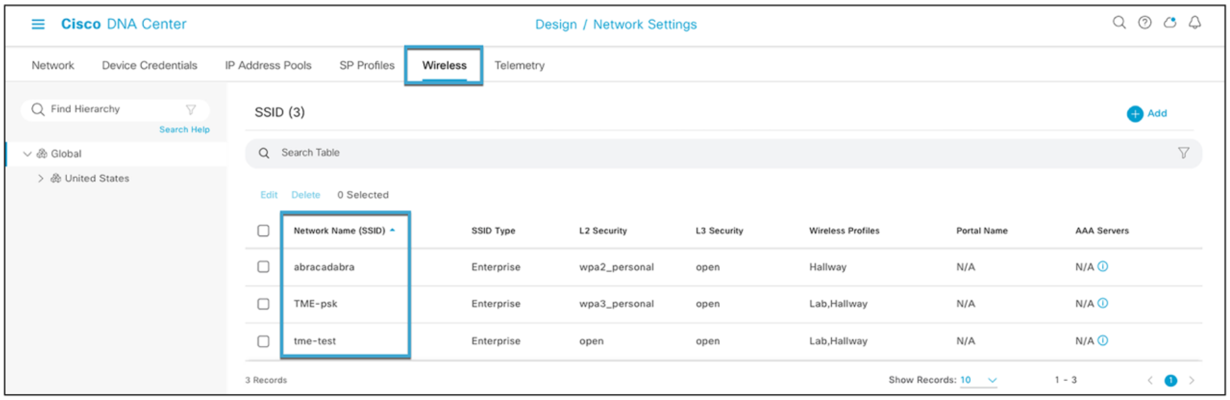
tme-test (2)

0 Selected Ignore Config Relearn Config Assign to Global

□	WLAN Profile Name	Policy Profile Name	Attributes	Site	SSID Type	Passphrase Type	Passphrase	AAA Configuration
□	tme-test	default-policy-profile	All Learned ⓘ	Global	Enterprise	N/A	N/A	N/A ⓘ
□	tme-test	rvr-local	All Learned ⓘ	1 Site	Enterprise	N/A	N/A	N/A ⓘ

Show Records: 25 1 - 2

Figure 43.
Learned SSIDs



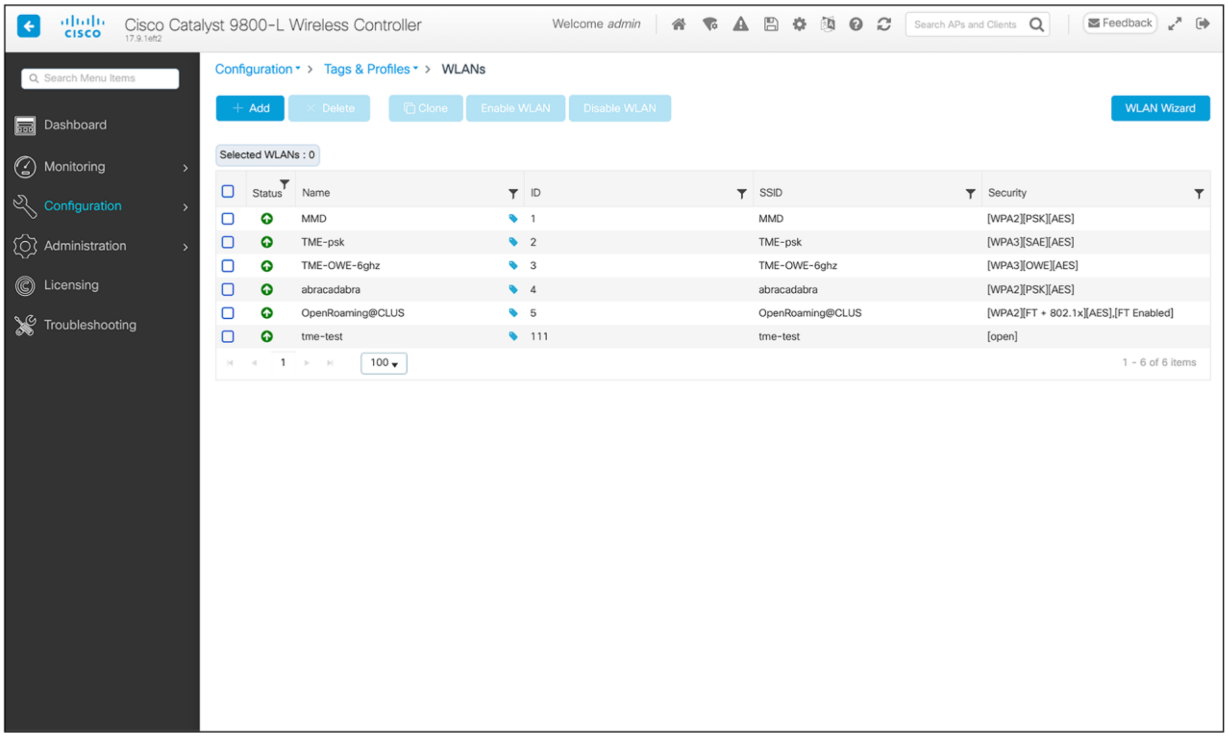
SSID (3)

0 Selected

□	Network Name (SSID)	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
□	abracadabra	Enterprise	wpa2_personal	open	Hallway	N/A	N/A ⓘ
□	TME-psk	Enterprise	wpa3_personal	open	Lab,Hallway	N/A	N/A ⓘ
□	tme-test	Enterprise	open	open	Lab,Hallway	N/A	N/A ⓘ

3 Records Show Records: 10 1 - 3

Figure 44.
Learned SSIDs on Cisco DNA Center in Network Settings > Wireless tab (post-learn)



Selected WLANs : 0

□	Status	Name	ID	SSID	Security
□	●	MMD	1	MMD	[WPA2][PSK][AES]
□	●	TME-psk	2	TME-psk	[WPA3][SAE][AES]
□	●	TME-OWE-6ghz	3	TME-OWE-6ghz	[WPA3][OWE][AES]
□	●	abracadabra	4	abracadabra	[WPA2][PSK][AES]
□	●	OpenRoaming@CLUS	5	OpenRoaming@CLUS	[WPA2][FT + 802.1x][AES],[FT Enabled]
□	●	tme-test	111	tme-test	[open]

1   100   1 - 6 of 6 items

Figure 45.
SSIDs on the Catalyst 9800 wireless controller (pre-learn)

Step 8: Resolve configuration conflicts

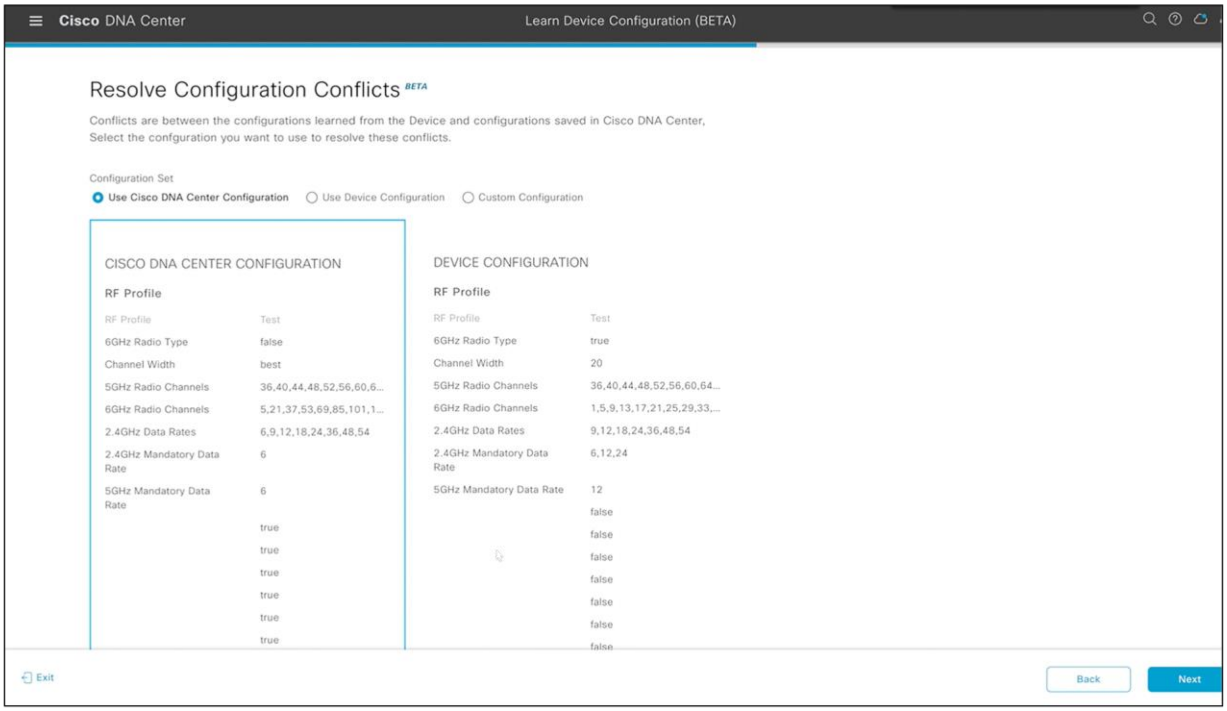
In the Resolve Configuration Conflicts window, review and resolve the available conflicts.

Configurations learned from the device and the configurations saved at the global level are shown.

Choose a configuration set to resolve the conflict:

- Use the Cisco DNA Center configuration to save configurations at the global level.
- Use the device configuration to learn configurations from the device.
- Selecting Use Device Configuration overwrites the configurations saved at the global level.
- Use a custom configuration to customize the configurations by choosing the required wireless interface.

Note: If you have a calibarated RF profile for your wireless network, select device configuration instead of Cisco DNA Center configuration.



Resolve Configuration Conflicts BETA

Conflicts are between the configurations learned from the Device and configurations saved in Cisco DNA Center, Select the confguration you want to use to resolve these conflicts.

Configuration Set

● Use Cisco DNA Center Configuration ○ Use Device Configuration ○ Custom Configuration

CISCO DNA CENTER CONFIGURATION

RF Profile

RF Profile	Test
6GHz Radio Type	false
Channel Width	best
5GHz Radio Channels	36,40,44,48,52,56,60,6...
6GHz Radio Channels	5,21,37,53,69,85,101,1...
2.4GHz Data Rates	6,9,12,18,24,36,48,54
2.4GHz Mandatory Data Rate	6
5GHz Mandatory Data Rate	6
	true
	true
	true
	true
	true
	true

DEVICE CONFIGURATION

RF Profile

RF Profile	Test
6GHz Radio Type	true
Channel Width	20
5GHz Radio Channels	36,40,44,48,52,56,60,64...
6GHz Radio Channels	1,5,9,13,17,21,25,29,33,...
2.4GHz Data Rates	9,12,18,24,36,48,54
2.4GHz Mandatory Data Rate	6,12,24
5GHz Mandatory Data Rate	12
	false
	false
	false
	false
	false
	false
	false

Figure 46.
Resolving configuration conflicts

Step 9: Select model configurations

In the Model Configs Learned window, review the model configurations.

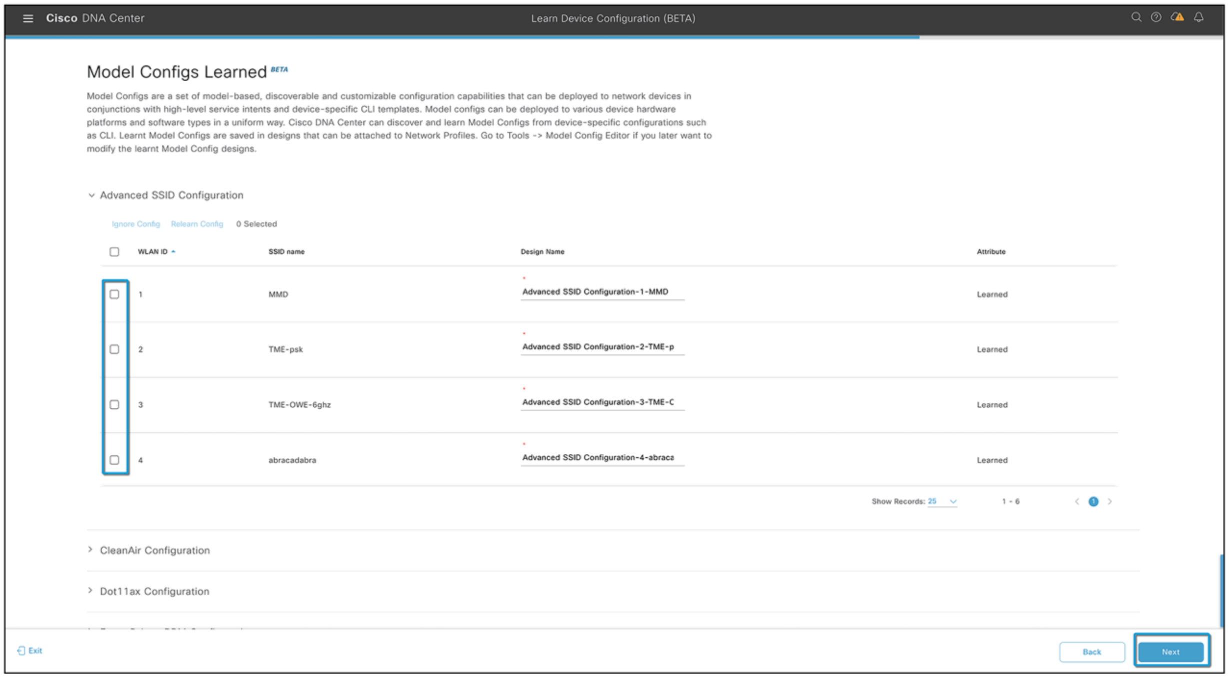
The model configurations are a set of model-based, discoverable, and customizable configuration capabilities that can be deployed on network devices. Model configurations can be deployed on various hardware platforms and software types. Cisco DNA Center discovers and learns model configurations from device-specific configurations such as CLI. The learned model configurations are saved in designs that can be attached to network profiles.

Expand and review the following wireless model configuration design types:

- AAA Radius Attributes Configuration
- Advanced SSID Configuration
- CleanAir Configuration
- Dot11ax Configuration
- Event Driven RRM Configuration
- Global IPv6 Configuration
- Multicast Configuration
- RRM General Configuration

If you want to ignore any configuration from each model configuration design type, select the configuration in the corresponding table and click **Ignore Config**. To relearn the ignored configuration, select the ignored configuration and click **Relearn Config**.

Refer to Design Model Configuration in the Cisco DNA Center User Guide for more information on how to create and edit network-specific model configurations using the Model Config Editor.



Model Configs Learned BETA

Model Configs are a set of model-based, discoverable and customizable configuration capabilities that can be deployed to network devices in conjunctions with high-level service intents and device-specific CLI templates. Model configs can be deployed to various device hardware platforms and software types in a uniform way. Cisco DNA Center can discover and learn Model Configs from device-specific configurations such as CLI. Learnt Model Configs are saved in designs that can be attached to Network Profiles. Go to Tools -> Model Config Editor if you later want to modify the learnt Model Config designs.

Advanced SSID Configuration

Ignore Config Relearn Config 0 Selected

□	WLAN ID	SSID name	Design Name	Attribute
□	1	MMD	Advanced SSID Configuration-1-MMD	Learned
□	2	TME-psk	Advanced SSID Configuration-2-TME-p	Learned
□	3	TME-OWE-6ghz	Advanced SSID Configuration-3-TME-C	Learned
□	4	abracadabra	Advanced SSID Configuration-4-abraca	Learned

Show Records: 25 1 - 6

CleanAir Configuration

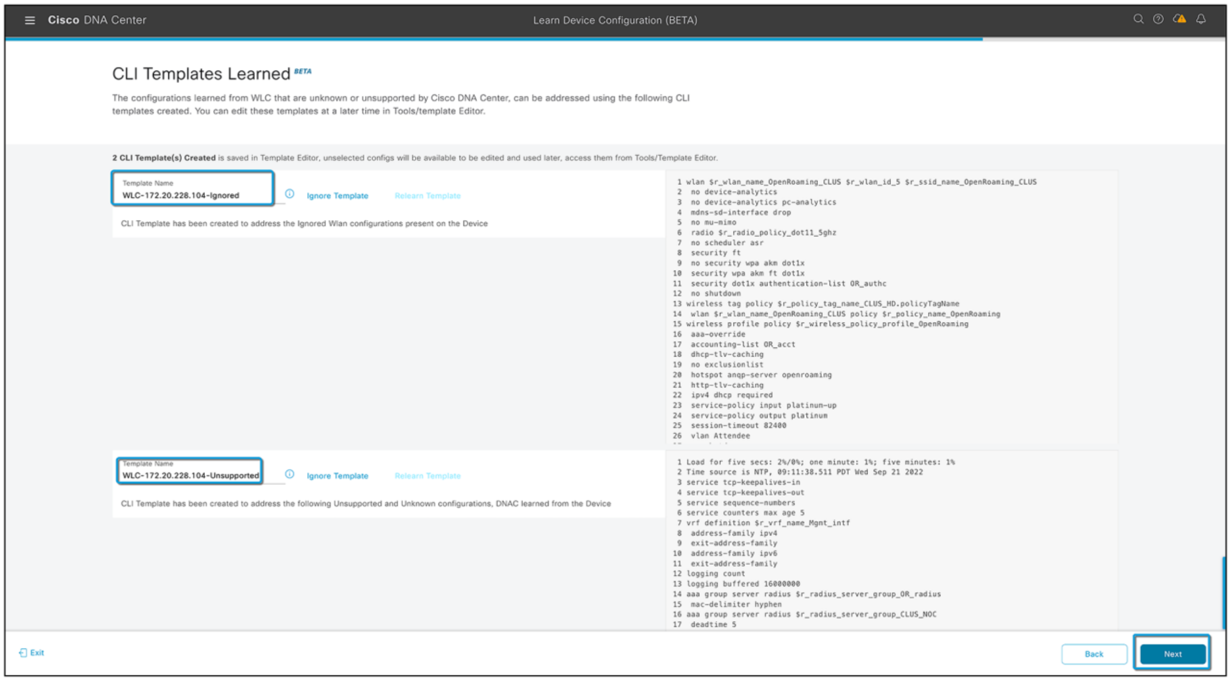
Dot11ax Configuration

Figure 47.
Model configurations learned

Step 10: Add a CLI template to the network profile

In the CLI Templates Learned window, review the CLI templates and use these templates to address the unknown or unsupported configurations.

- All the ignored WLAN configurations are chosen by default. Click **Ignore Template** to restrict the template from addressing the configurations. Click **Relearn Template** to address the configurations.
- All the unknown or unsupported configurations are chosen by default. Click **Ignore Template** to restrict the template from addressing the configurations. Click **Relearn Template** to address the configurations.
- These CLI templates can be edited using the Template Editor, accessed by going to the hamburger menu (☰) and choosing Tools > Template Editor.
- These CLI templates will be saved in Cisco DNA Center for current and future use and will not be deleted.
- This CLI template needs to be attached to the network profile while provisioning the Catalyst 9800 wireless controller.



CLI Templates Learned BETA

The configurations learned from WLC that are unknown or unsupported by Cisco DNA Center, can be addressed using the following CLI templates created. You can edit these templates at a later time in Tools/template Editor.

2 CLI Template(s) Created is saved in Template Editor, unselected configs will be available to be edited and used later, access them from Tools/Template Editor.

Template Name: WLC-172.20.228.104-Ignored

CLI Template has been created to address the Ignored Wlan configurations present on the Device

```
wlan $r_wlan_name_OpenRoaming_CLUS $r_wlan_id_5 $r_ssid_name_OpenRoaming_CLUS
 no device-analytics
 no device-analytics pc-analytics
 mdns-sd-interface drop
 no mu-mimo
 radio $r_radio_policy_dot11_5ghz
 no scheduler asr
 security ft
 no security wpa akm dot1x
 security wpa akm ft dot1x
 security dot1x authentication-list OR_authc
 no shutdown
wireless tag policy $r_policy_tag_name_CLUS_HD.policyTagName
 wlan $r_wlan_name_OpenRoaming_CLUS policy $r_policy_name_OpenRoaming
wireless profile policy $r_wireless_policy_profile_OpenRoaming
 aaa-override
 accounting-list OR_acct
 dhcp-tlv-caching
 no exclusionlist
 hotspot anqp-server openroaming
 http-tlv-caching
 ipv4 dhcp required
 service-policy input platinum-up
 service-policy output platinum
 session-timeout 82400
 vlan Attendee
```

Template Name: WLC-172.20.228.104-Unsupported

CLI Template has been created to address the following Unsupported and Unknown configurations, DNAC learned from the Device

```
Load for five secs: 2%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 09:11:38.511 PDT Wed Sep 21 2022
service tcp-keepalives-in
service tcp-keepalives-out
service sequence-numbers
service counters max age 5
vrf definition $r_vrf_name_Mgmt_intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
logging count
logging buffered 16000000
aaa group server radius $r_radius_server_group_OR_radius
 mac-delimiter hyphen
aaa group server radius $r_radius_server_group_CLUS_NOC
 deadtime 5
```

Figure 48.
CLI template generated for unsupported and ignored configurations

Step 11: Review the network profile configuration

In the Network Profiles window, review the learned network profile configuration. Based on the configurations learned, Cisco DNA Center creates the network profile. You can either use the learned network profile or create a new network profile. The SSIDs are learned and grouped while creating network profile.

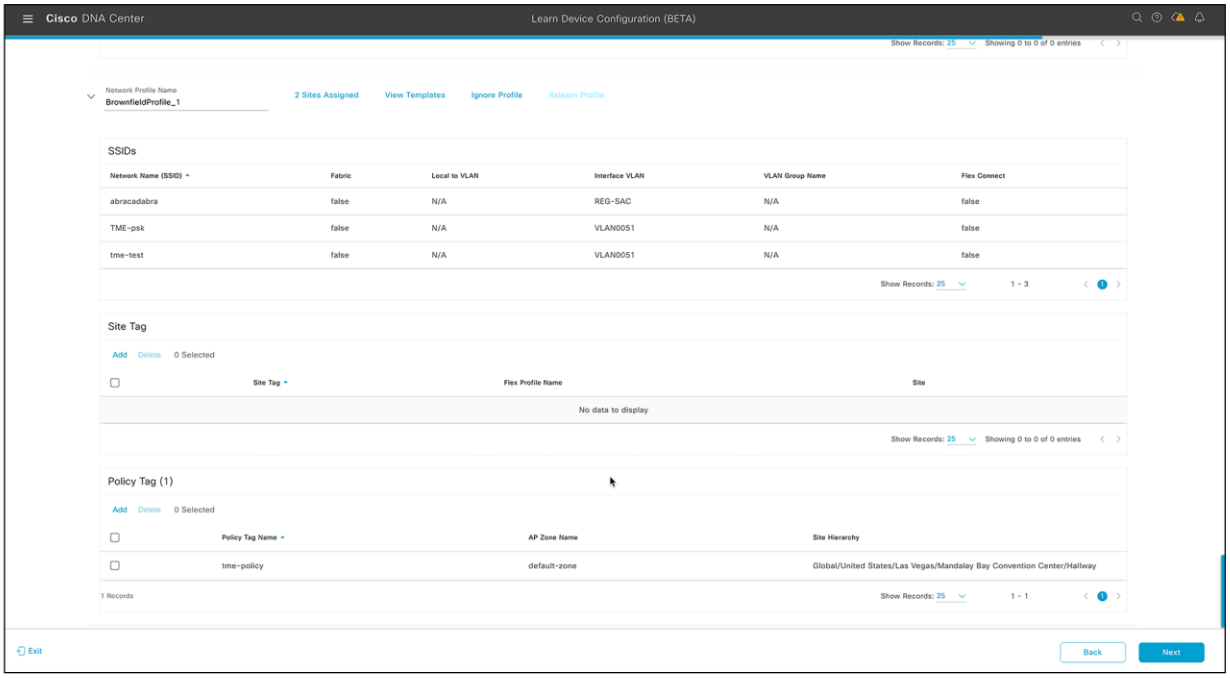
For Cisco AireOS wireless controllers, the Flex group and AP groups are mapped to the network profile. Depending on the AP site assignment, the network profile is assigned to the appropriate site.

For Cisco Catalyst 9800 Series Wireless Controllers, the site tag, policy tag, and site hierarchy mapped to the network profile are displayed.

- Based on the AP site assignment configuration, the network profile is assigned to the appropriate site. Click **Sites Assigned** to view details on the site assigned to the network profile.
- To create a new network profile, click **Create New Profile**.

  The New Profile window appears.

  - In the Network Profile Name field, enter a name for the network profile.
  - From the SSIDs table, select the checkbox next to the network name to select the SSID.
  - Click **Save**.


Cisco DNA Center
Learn Device Configuration (BETA)
Show Records: 25
Showing 0 to 0 of 0 entries

Network Profile Name
BrownfieldProfile_1

SSIDs

Network Name (SSID)	Fabric	Local to VLAN	Interface VLAN	VLAN Group Name	Flex Connect
abracadabra	false	N/A	REG-SAC	N/A	false
TME-psk	false	N/A	VLAN0051	N/A	false
tme-test	false	N/A	VLAN0051	N/A	false

Site Tag

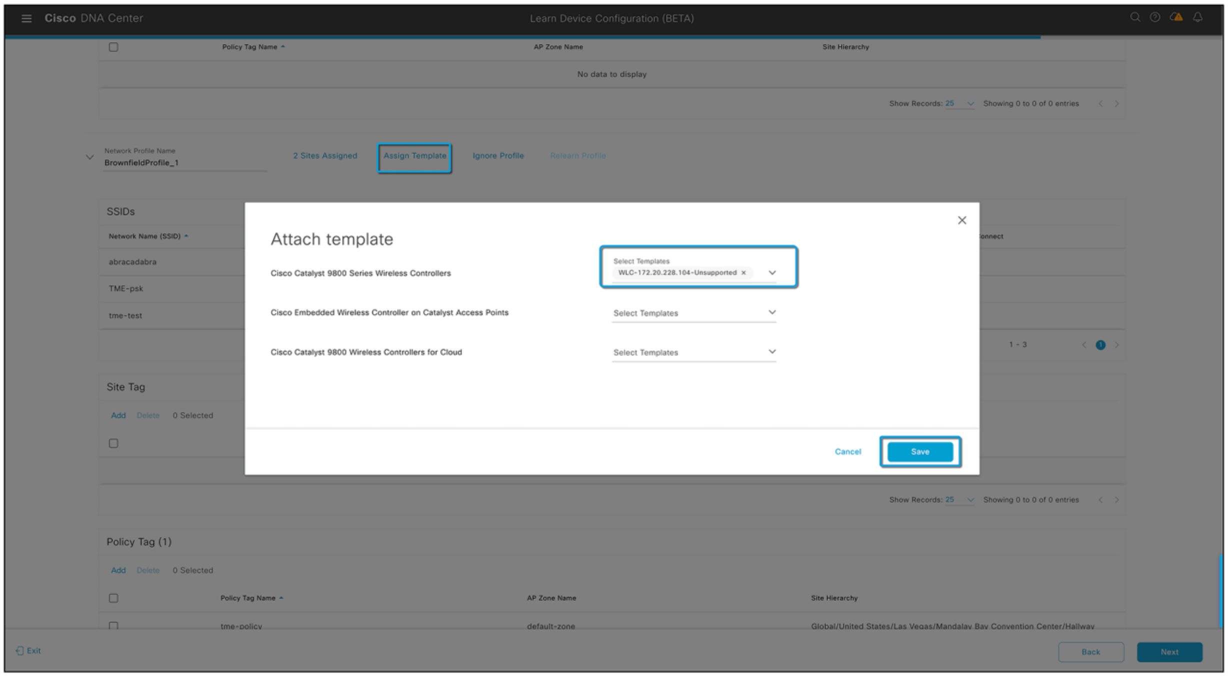
□	Site Tag	Flex Profile Name	Site
	No data to display		

Policy Tag (1)

□	Policy Tag Name	AP Zone Name	Site Hierarchy
□	tme-policy	default-zone	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway

Figure 49.
Network profiles created after learning an existing wireless controller's configuration

- (Optional) Review the template details and edit if you want to make any changes.
  - To assign a site to a network profile, click **Assign Site**. In the Assign Site window, choose a site and click **Save**. Click **Sites Assigned** to view the sites assigned to this profile.
  - To attach a template to a network profile, click **Assign Template**. In the Assign Template window, choose templates from the Select Templates drop-down list for each device in the existing deployment and click **Save**. Click **View Templates** to view the templates assigned to the profile.
  - To ignore a network profile, click **Ignore Profile** and then click **Continue**. If a profile is marked as ignored, all the profile attributes of that profile are removed. This cannot be undone by relearning the profile. To relearn an ignored profile, click **Relearn Profile**.
  - To add a site tag to a network profile, click **Add** in the Site Tag table. In the Add Site Tag window, choose a site tag from the Select Site Tag drop-down list, choose a site from the hierarchy, and click **Save**.



☐	Policy Tag Name	AP Zone Name	Site Hierarchy
		No data to display	

Show Records: 25 Showing 0 to 0 of 0 entries

Network Profile Name: BrownfieldProfile_1

SSIDs

Network Name (SSID)
abracadabra
TME-psk
tme-test

1 - 3

Attach template

Cisco Catalyst 9800 Series Wireless Controllers	Select Templates: WLC-172.20.228.104-Unsupported ×
Cisco Embedded Wireless Controller on Catalyst Access Points	Select Templates
Cisco Catalyst 9800 Wireless Controllers for Cloud	Select Templates

Site Tag

0 Selected

Show Records: 25 Showing 0 to 0 of 0 entries

Policy Tag (1)

0 Selected

☐	Policy Tag Name	AP Zone Name	Site Hierarchy
☐	tme-policy	default-zone	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway

Figure 50.
Adding a CLI template to a network profile

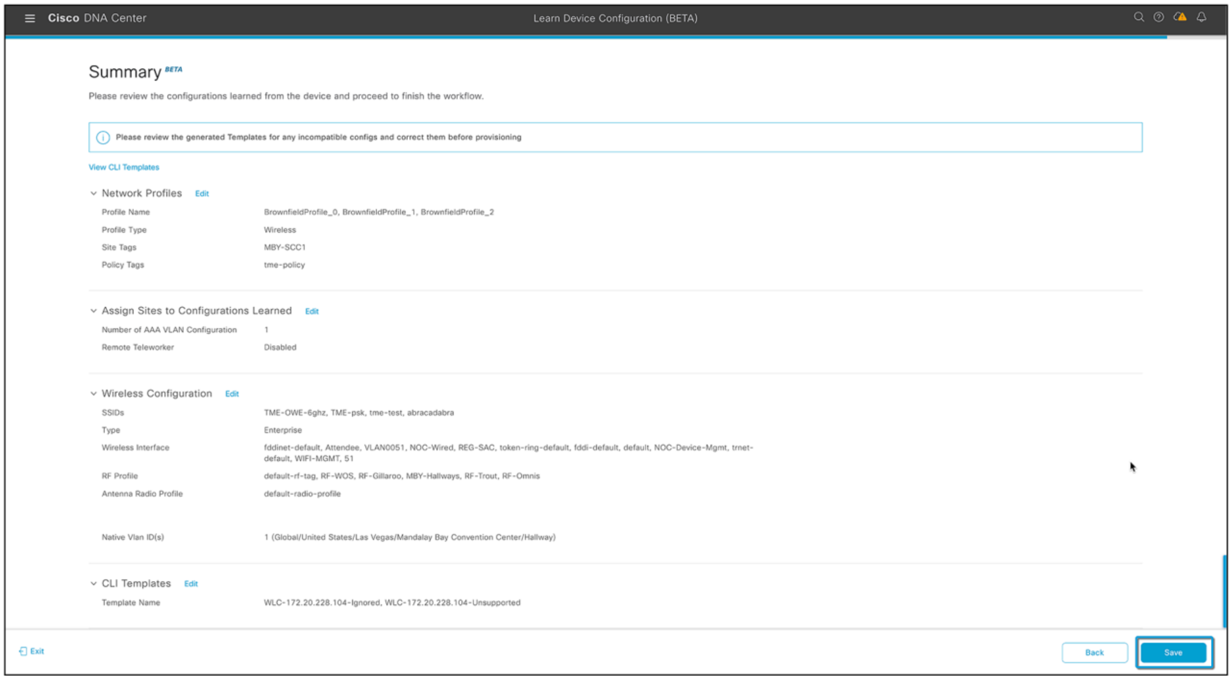
Step 12: Review the configuration summary

In the Summary window, review the following configurations:

- Device Details
- Network Setting
- SSIDs
- Managed Sites
- Rolling AP Upgrade
- Interfaces
- Advanced Configuration

Click **Save**.

The network configurations are created at the global and site levels appropriately.



Summary BETA

Please review the configurations learned from the device and proceed to finish the workflow.

Please review the generated Templates for any incompatible configs and correct them before provisioning

View CLI Templates

Network Profiles Edit

Profile Name	BrownfieldProfile_0, BrownfieldProfile_1, BrownfieldProfile_2
Profile Type	Wireless
Site Tags	MBY-SCC1
Policy Tags	tme-policy

Assign Sites to Configurations Learned Edit

Number of AAA VLAN Configuration	1
Remote Teleworker	Disabled

Wireless Configuration Edit

SSIDs	TME-OWE-6ghz, TME-psk, tme-test, abracadabra
Type	Enterprise
Wireless Interface	fddinet-default, Attendee, VLAN0051, NOC-Wired, REG-SAC, token-ring-default, fddi-default, default, NOC-Device-Mgmt, trnet-default, WIFI-MGMT, 51
RF Profile	default-rf-tag, RF-WOS, RF-Gillaroo, MBY-Hallways, RF-Trout, RF-Omnis
Antenna Radio Profile	default-radio-profile
Native Vlan ID(s)	1 (Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway)

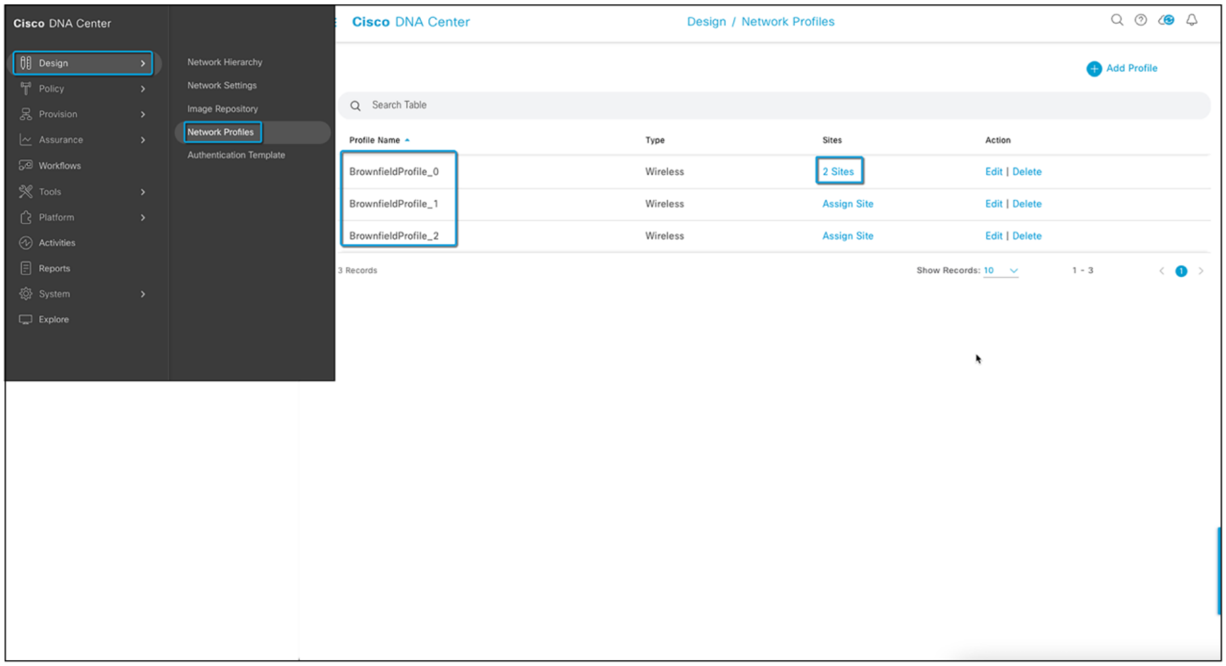
CLI Templates Edit

Template Name	WLC-172.20.228.104-Ignored, WLC-172.20.228.104-Unsupported

Figure 51.
Summary for all learned wireless configurations from an existing wireless controller

Step 13: Review the newly created network profile

- Click the hamburger menu icon (≡) and choose Design > Network Profile.
- The network profiles created from the Learn Device Configuration workflow are listed here.

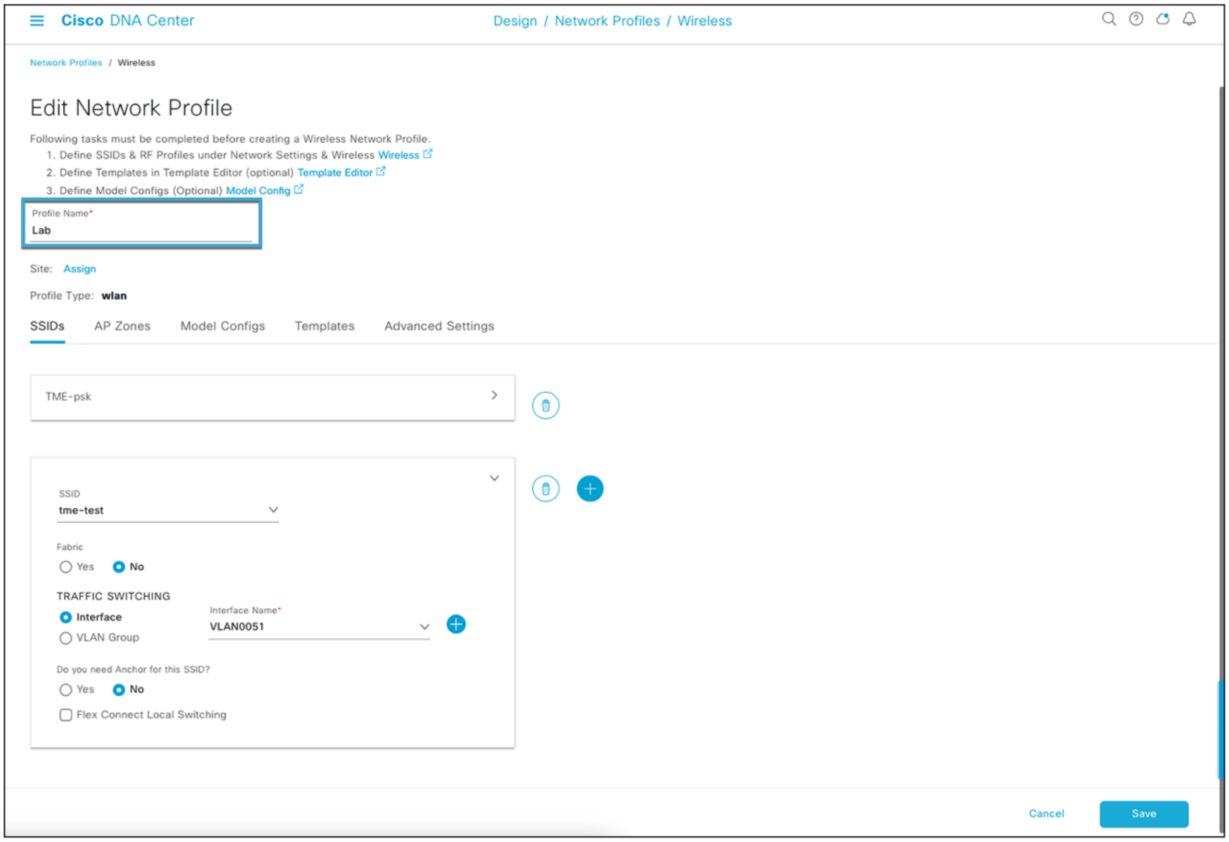


Profile Name	Type	Sites	Action
BrownfieldProfile_0	Wireless	2 Sites	Edit | Delete
BrownfieldProfile_1	Wireless	Assign Site	Edit | Delete
BrownfieldProfile_2	Wireless	Assign Site	Edit | Delete

3 Records Show Records: 10 1 - 3

Figure 52.
Network profiles created from the learned device configuration

- The learned configurations will be pushed to devices when the devices are provisioned.
- A wireless profile (network profile with wireless configurations) must be assigned to a site before the Catalyst 9800 wireless controller is provisioned. This can be done by clicking **Assign** (as shown in the figure below) across your network profile name in the table and selecting all the sites where this network profile needs to be assigned.
- You can click **Edit** in the Action column next to your network profile names. It will allow you to:
  - Change the network profile name if not assigned to any site.



Edit Network Profile

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

1. Define SSIDs & RF Profiles under Network Settings & Wireless Wireless
2. Define Templates in Template Editor (optional) Template Editor
3. Define Model Configs (Optional) Model Config

Profile Name* Lab

Site: Assign

Profile Type: wlan

TME-psk

SSID: tme-test

Fabric: ○ Yes ● No

TRAFFIC SWITCHING: ● Interface ○ VLAN Group

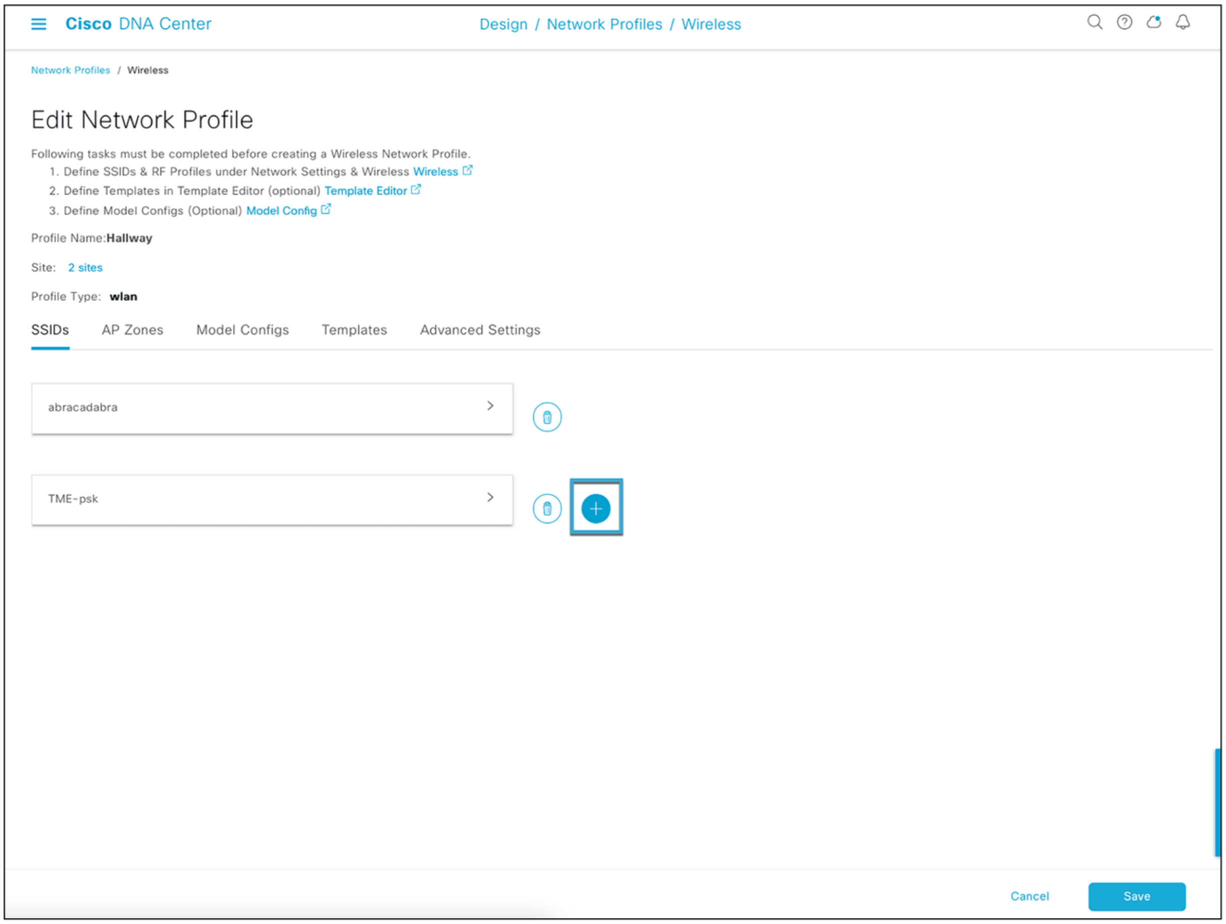
Interface Name*: VLAN0051

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

□ Flex Connect Local Switching

Figure 53.
Changing the network profile name

- Have all supported SSIDs for a particular policy tag. You can add an existing SSID from the Cisco DNA Center Wireless SSID list in Network Settings. You just need to select the “+” button on the SSID tab and add the SSID to the network profile. You also need to select a management interface for the SSID.



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

Edit Network Profile

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

1. Define SSIDs & RF Profiles under Network Settings & Wireless Wireless
2. Define Templates in Template Editor (optional) Template Editor
3. Define Model Configs (Optional) Model Config

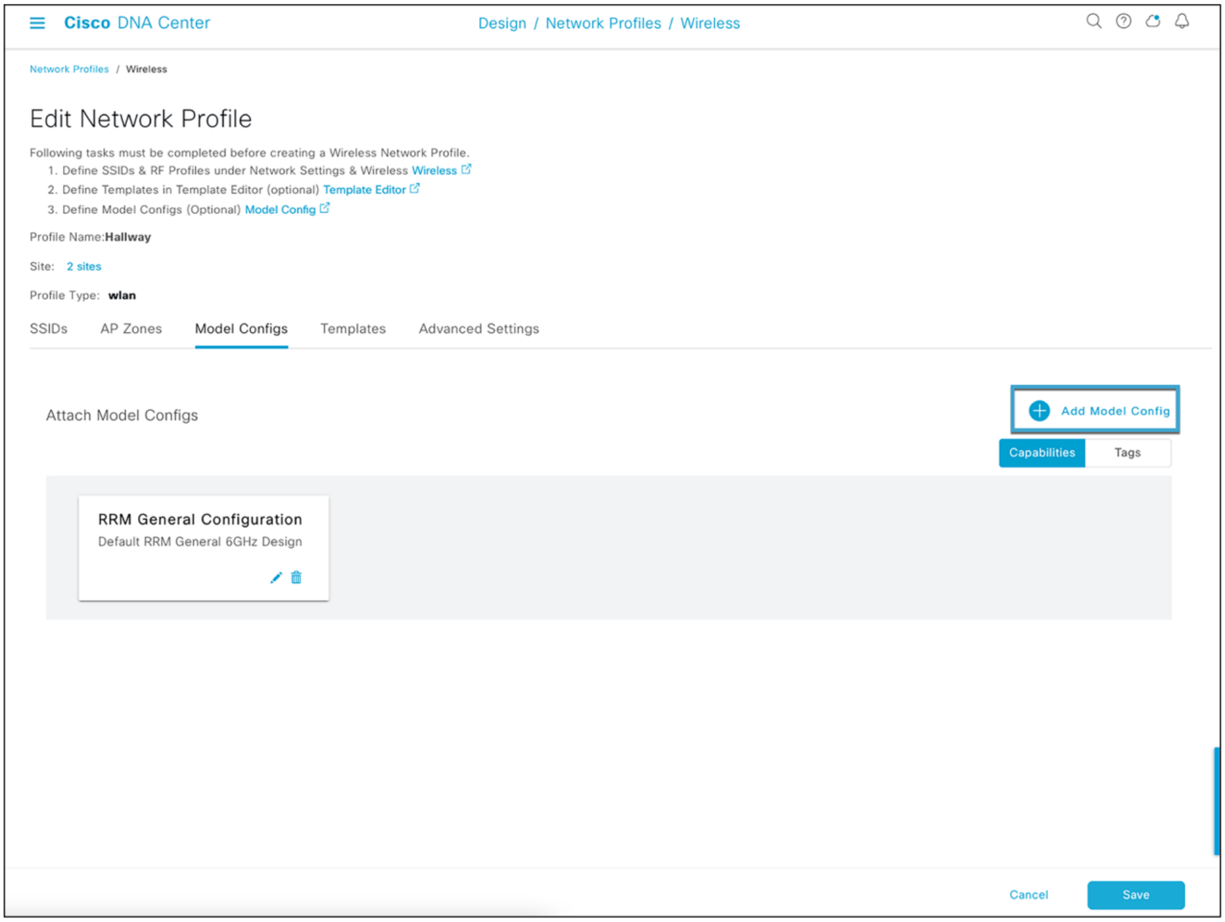
Profile Name:**Hallway**

Site: 2 sites

Profile Type: **wlan**

Figure 54.
Adding SSIDs in the network profile

- You can add any model configurations available for the Catalyst 9800 wireless controller by going to the Model Configs tab. Refer to Design Model Configuration in the Cisco DNA Center User Guide for more information on how to create and edit network-specific model configurations using the Model Config Editor.



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

Edit Network Profile

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

1. Define SSIDs & RF Profiles under Network Settings & Wireless Wireless
2. Define Templates in Template Editor (optional) Template Editor
3. Define Model Configs (Optional) Model Config

Profile Name:**Hallway**

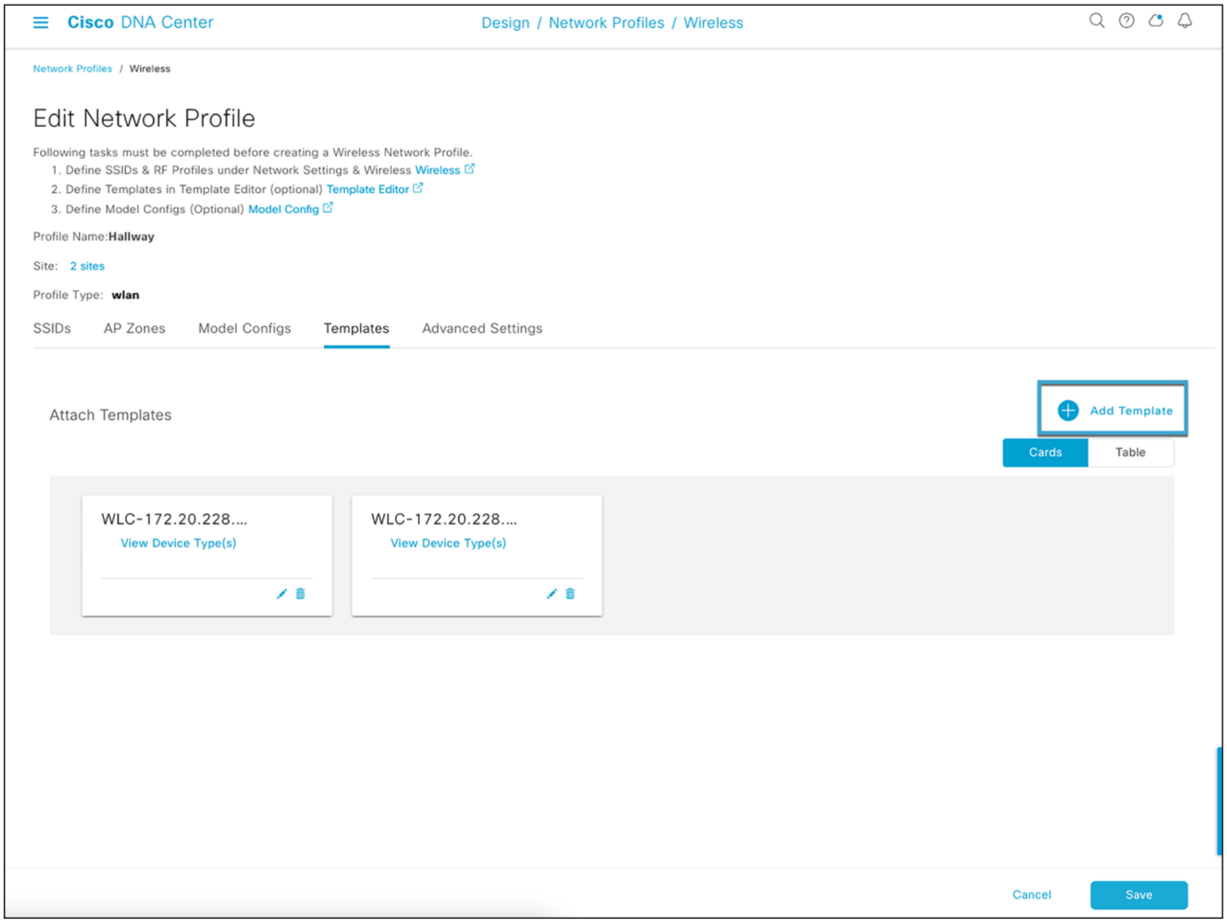
Site: 2 sites

Profile Type: **wlan**

RRM General Configuration
Default RRM General 6GHz Design

Figure 55.
Adding and editing model configurations in the network profile

- You can add CLI templates from a previous Learn Device Configuration attempt or use a CLI template generated from a different device’s Learn Device Configuration learning workflow. This can be done from the Templates tab by selecting the “+” and clicking the CLI template to be added to the network profile.



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

Edit Network Profile

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

1. Define SSIDs & RF Profiles under Network Settings & Wireless Wireless
2. Define Templates in Template Editor (optional) Template Editor
3. Define Model Configs (Optional) Model Config

Profile Name:**Hallway**

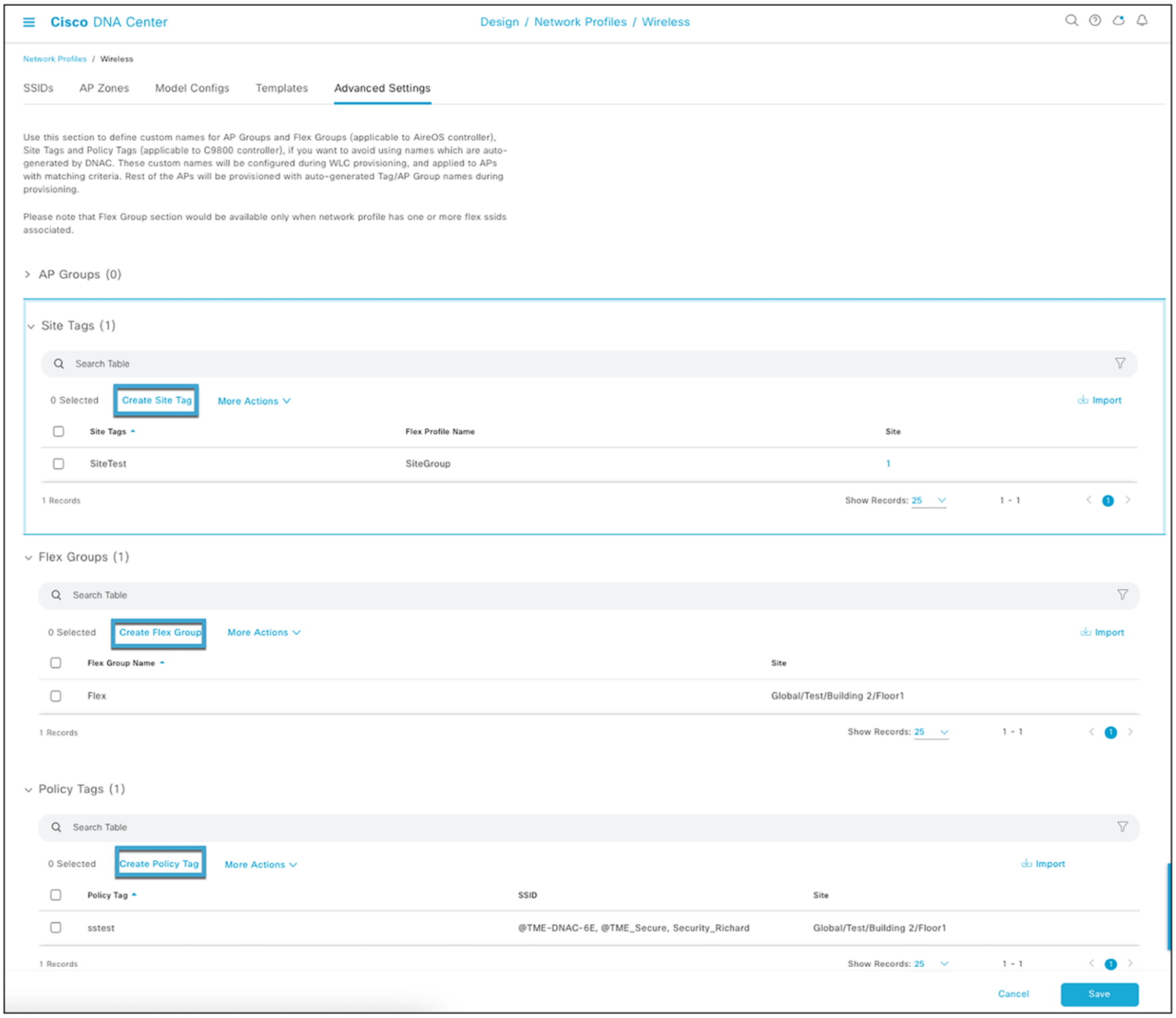
Site: 2 sites

Profile Type: **wlan**

Figure 56.
CLI templates in the network profile

- All site tags, Flex groups, and policy tags associated with this network profile will be listed in Advanced Settings. You can add new tags for a new floor on the same site with existing configurations if necessary.

Note: This space will be blank and will not have any tags if there are unsupported configurations found during the Learn Device Configuration workflow, as Cisco DNA Center-created tags will be used by the controller and no controller tags are learned thoroughly by Cisco DNA Center.



Use this section to define custom names for AP Groups and Flex Groups (applicable to AireOS controller), Site Tags and Policy Tags (applicable to C9800 controller), if you want to avoid using names which are auto-generated by DNAC. These custom names will be configured during WLC provisioning, and applied to APs with matching criteria. Rest of the APs will be provisioned with auto-generated Tag/AP Group names during provisioning.

Please note that Flex Group section would be available only when network profile has one or more flex ssids associated.

> AP Groups (0)

Site Tags (1)

Site Tags	Flex Profile Name	Site
SiteTest	SiteGroup	1

Flex Groups (1)

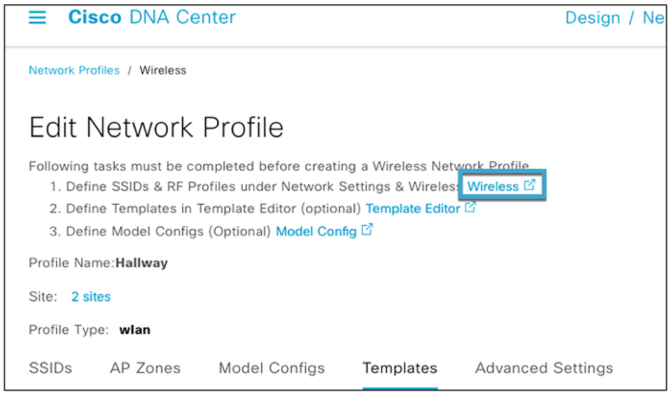
Flex Group Name	Site
Flex	Global/Test/Building 2/Floor1

Policy Tags (1)

Policy Tag	SSID	Site
sstest	@TME-DNAC-6E, @TME_Secure, Security_Richard	Global/Test/Building 2/Floor1

Figure 57.
Tag details in the network profile

- You can click **Wireless** in the steps of the task, as shown below, and all the wireless configurations will be listed there. This page can also be accessed by going to the hamburger menu (☰), choosing Design > Network Settings > Wireless, and selecting Global in the site hierarchy in the sidebar.



Network Profiles / Wireless

Edit Network Profile

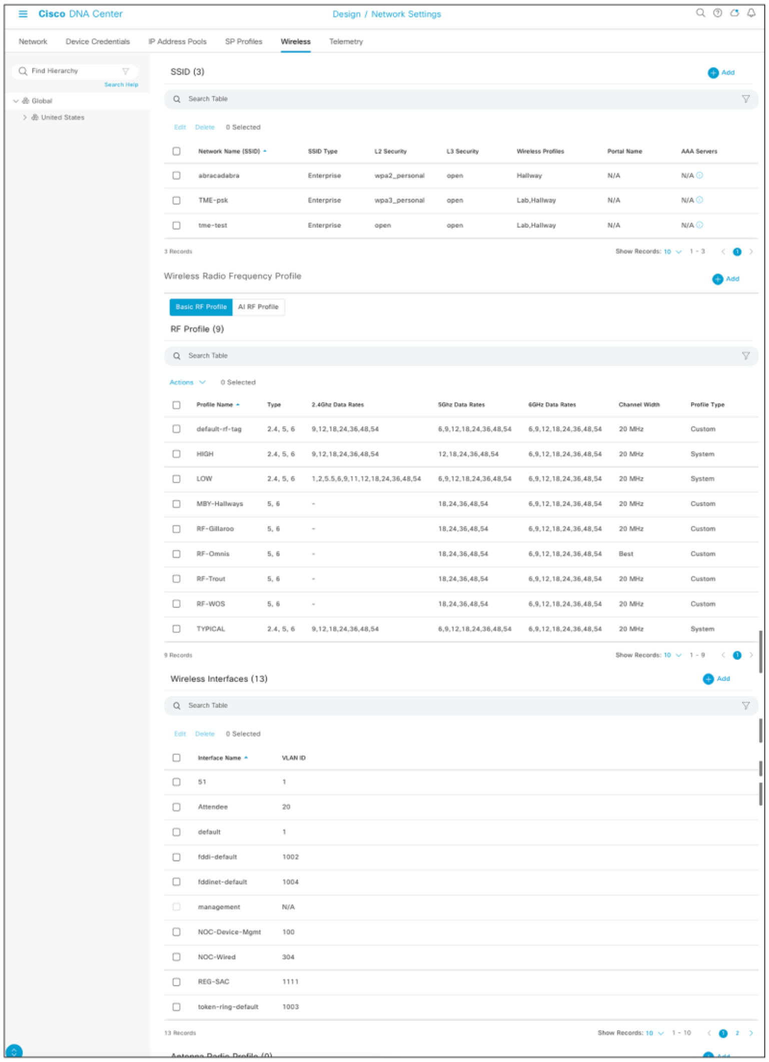
Following tasks must be completed before creating a Wireless Network Profile
1. Define SSIDs & RF Profiles under Network Settings & Wireless Wireless
2. Define Templates in Template Editor (optional) Template Editor
3. Define Model Configs (Optional) Model Config

Profile Name: **Hallway**

Site: 2 sites

Profile Type: **wlan**

Figure 58.
Wireless settings link in the network profile



SSID (3)

0 Selected

	Network Name (SSID)	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
□	abracadabra	Enterprise	wpa2_personal	open	Hallway	N/A	N/A
□	TME-psk	Enterprise	wpa3_personal	open	Lab,Hallway	N/A	N/A
□	tme-test	Enterprise	open	open	Lab,Hallway	N/A	N/A

3 Records Show Records: 10 1 - 3

Wireless Radio Frequency Profile

RF Profile (9)

0 Selected

	Profile Name	Type	2.4Ghz Data Rates	5Ghz Data Rates	6GHz Data Rates	Channel Width	Profile Type
□	default-rf-tag	2.4, 5, 6	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
□	HIGH	2.4, 5, 6	9,12,18,24,36,48,54	12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	System
□	LOW	2.4, 5, 6	1,2,5.5,6,9,11,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	System
□	MBY-Hallways	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
□	RF-Gillaroo	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
□	RF-Omnis	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	Best	Custom
□	RF-Trout	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
□	RF-WOS	5, 6	-	18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	Custom
□	TYPICAL	2.4, 5, 6	9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz	System

9 Records Show Records: 10 1 - 9

Wireless Interfaces (13)

0 Selected

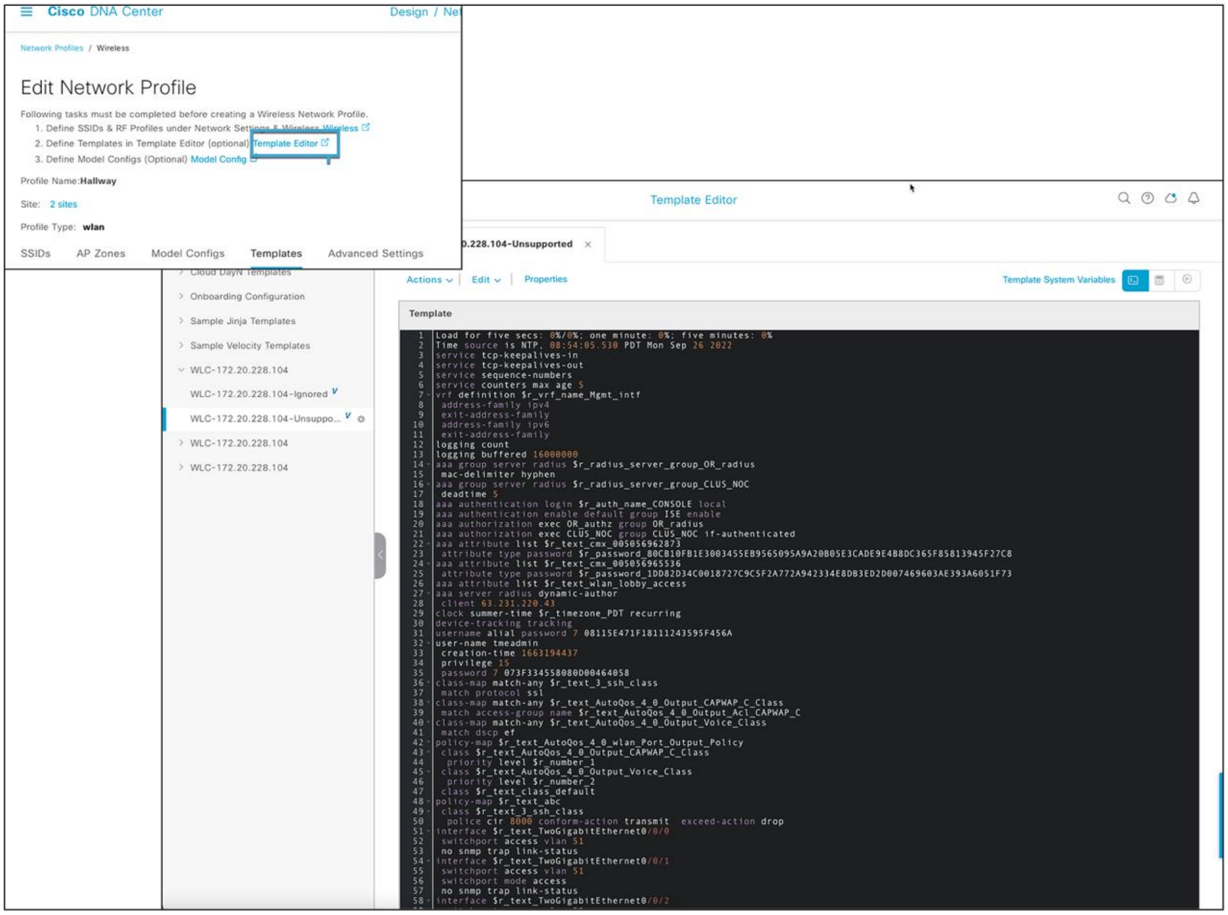
	Interface Name	VLAN ID
□	51	1
□	Attendee	20
□	default	1
□	fddi-default	1002
□	fddinet-default	1004
□	management	N/A
□	NOC-Device-Mgmt	100
□	NOC-Wired	304
□	REG-SAC	1111
□	token-ring-default	1003

13 Records Show Records: 10 1 - 10

Antenna Radio Profile (0)

Figure 59.
Wireless settings on the Network Settings page

Note: You can click Template Editor in the steps of the task as shown below and edit a CLI template, which can be added to the network profile. You can also access the Template Editor by going to the hamburger menu (☰) and choosing Tools > Template Editor). You can also create your own CLI template and add it to the network profile.



Edit Network Profile

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

1. Define SSIDs & RF Profiles under Network Settings & Wireless Wireless
2. Define Templates in Template Editor (optional) Template Editor
3. Define Model Configs (Optional) Model Config

Profile Name:Hallway

Site: 2 sites

Profile Type: wlan

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 08:54:05.530 PDT Mon Sep 26 2022
service tcp-keepalives-in
service tcp-keepalives-out
service sequence-numbers
service counters max age 5
vrf definition $r_vrf_name_Mgmt_intf
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
logging count
logging buffered 16000000
aaa group server radius $r_radius_server_group_OR_radius
 mac-delimiter hyphen
aaa group server radius $r_radius_server_group_CLUS_NOC
 deadtime 5
aaa authentication login $r_auth_name_CONSOLE local
aaa authentication enable default group ISE enable
aaa authorization exec OR_authz group OR_radius
aaa authorization exec CLUS_NOC group CLUS_NOC if-authenticated
aaa attribute list $r_text_cmx_005056962873
 attribute type password $r_password_80CB10FB1E3003455EB9565095A9A20B05E3CADE9E4B8DC365F85813945F27C8
aaa attribute list $r_text_cmx_005056965536
 attribute type password $r_password_1DD82D34C0018727C9C5F2A772A942334E8DB3ED2D007469603AE393A6051F73
aaa attribute list $r_text_wlan_lobby_access
aaa server radius dynamic-author
 client 63.231.220.43
clock summer-time $r_timezone_PDT recurring
device-tracking tracking
username alial password 7 08115E471F18111243595F456A
user-name tmeadmin
 creation-time 1663194437
 privilege 15
 password 7 073F334558080D00464058
class-map match-any $r_text_3_ssh_class
 match protocol ssl
class-map match-any $r_text_AutoQos_4_0_Output_CAPWAP_C_Class
 match access-group name $r_text_AutoQos_4_0_Output_Acl_CAPWAP_C
class-map match-any $r_text_AutoQos_4_0_Output_Voice_Class
 match dscp ef
policy-map $r_text_AutoQos_4_0_wlan_Port_Output_Policy
 class $r_text_AutoQos_4_0_Output_CAPWAP_C_Class
  priority level $r_number_1
 class $r_text_AutoQos_4_0_Output_Voice_Class
  priority level $r_number_2
 class $r_text_class_default
policy-map $r_text_abc
 class $r_text_3_ssh_class
  police cir 8000 conform-action transmit  exceed-action drop
interface $r_text_TwoGigabitEthernet0/0/0
 switchport access vlan 51
 no snmp trap link-status
interface $r_text_TwoGigabitEthernet0/0/1
 switchport access vlan 51
 switchport mode access
 no snmp trap link-status
interface $r_text_TwoGigabitEthernet0/0/2
```

Figure 60.
Template Editor from the network profile

Things to note about the Learn Device Configuration workflow:

- This configuration will overwrite the existing configurations on the controller and will be managed by Cisco DNA Center after provisioning.
- The workflow will create a new policy tag on the controller if any configuration on the existing AP policy tag has any unsupported configuration.
- The CLI template needs to be attached to the network profile to add all the unsupported SSIDs, RF tags, etc. in Step 11 in the Learn Device Configuration workflow in Part 4.
- This workflow will only learn the configurations from policy, site, and RF tags mapped to the access points on the Catalyst 9800 wireless controller. Tags that are not associated with any access point will not be saved to Cisco DNA Center. If any tags/profiles need to be a part of future deployment, make sure to assign atleast 1 Access Point with the tags which can be learned by this workflow.
- Only one Cisco ISE server and virtual IP is supported by Cisco DNA Center. Any other RADIUS server added to the network has to be either an AAA or TACACS server.

Part 5: Create an AI RF profile

To add a site to the AI-Enhanced RRM service to manage the site's and APs' RRM, you must create an AI RF profile. If you have learned the profiles and configurations from the controller already (via the Learn Device Configuration workflow), you can convert an existing RF profile to an AI RF profile. There is also a workflow for creating and assigning an AI RF profile to a site.

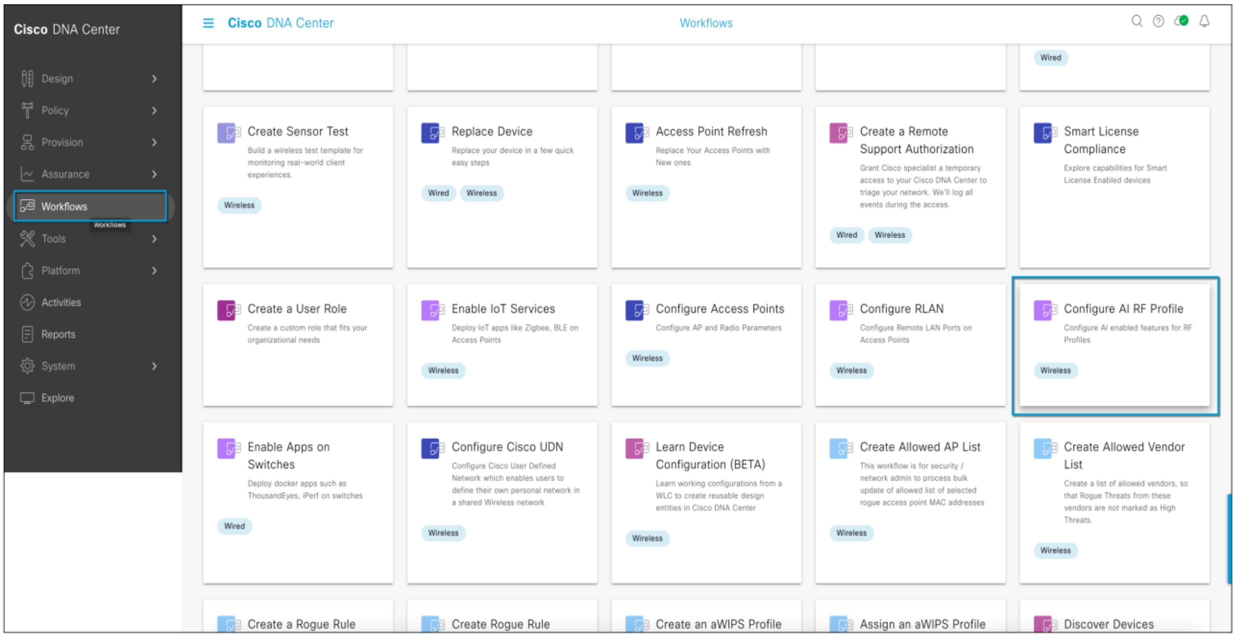
Option 1: Creating AI RF Profile from Network Settings

- Click the hamburger menu icon (☰) and choose **Design > Network Settings > Wireless** Tab > **Global** on Sidebar > Scroll down to **Wireless Radio Frequency Profile**.
- You can check box an existing RF profile > go to Actions and select **Upgrade to AI**.
- To create a brand new AI RF Profile, select +**Add > AI RF Profile** and customize the AI RF profile according to your wireless network requirements.
- Go to **AI RF Profile** tab and you will find your newly created AI RF Profile.
- To assign this AI RF Profile to a site, on your AI RF Profile column click on ... then go to **Assign Locations**
- Select all the building you want to assign this AI RF Profile to and want to use AI-Enhanced RRM then select **Assign**.

Option 2: Creating AI RF Profile using a Workflow

Step 1: Create an AI RF profile

Click the hamburger menu icon (☰) and choose Workflows > Configure AI RF Profile.



Create Sensor Test
Build a wireless test template for monitoring real-world client experiences.

Replace Device
Replace your device in a few quick easy steps

Access Point Refresh
Replace Your Access Points with New ones

Create a Remote Support Authorization
Grant Cisco specialist a temporary access to your Cisco DNA Center to triage your network. We'll log all events during the access.

Smart License Compliance
Explore capabilities for Smart License Enabled devices

Create a User Role
Create a custom role that fits your organizational needs

Enable IoT Services
Deploy IoT apps like Zigbee, BLE on Access Points

Configure Access Points
Configure AP and Radio Parameters

Configure RLAN
Configure Remote LAN Ports on Access Points

Configure AI RF Profile
Configure AI enabled features for RF Profiles

Enable Apps on Switches
Deploy docker apps such as ThousandEyes, iPerf on switches

Configure Cisco UDN
Configure Cisco User Defined Network which enables users to define their own personal network in a shared Wireless network

Learn Device Configuration (BETA)
Learn working configurations from a WLC to create reusable design entities in Cisco DNA Center

Create Allowed AP List
This workflow is for security / network admin to process bulk update of allowed list of selected rogue access point MAC addresses

Create Allowed Vendor List
Create a list of allowed vendors, so that Rogue Threats from these vendors are not marked as High Threats.

Create a Rogue Rule

Create Rogue Rule

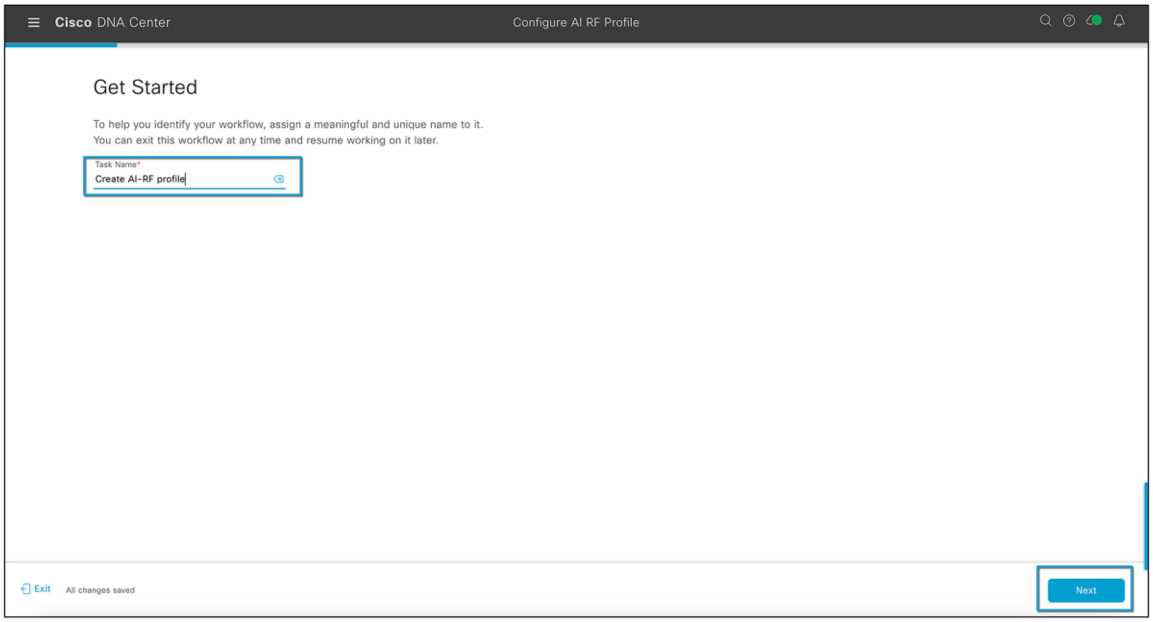
Create an aWIPS Profile

Assign an aWIPS Profile

Discover Devices

Figure 61.
Workflow to create an AI RF profile

Step 2: Assign a name to the task and click Next



Get Started

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

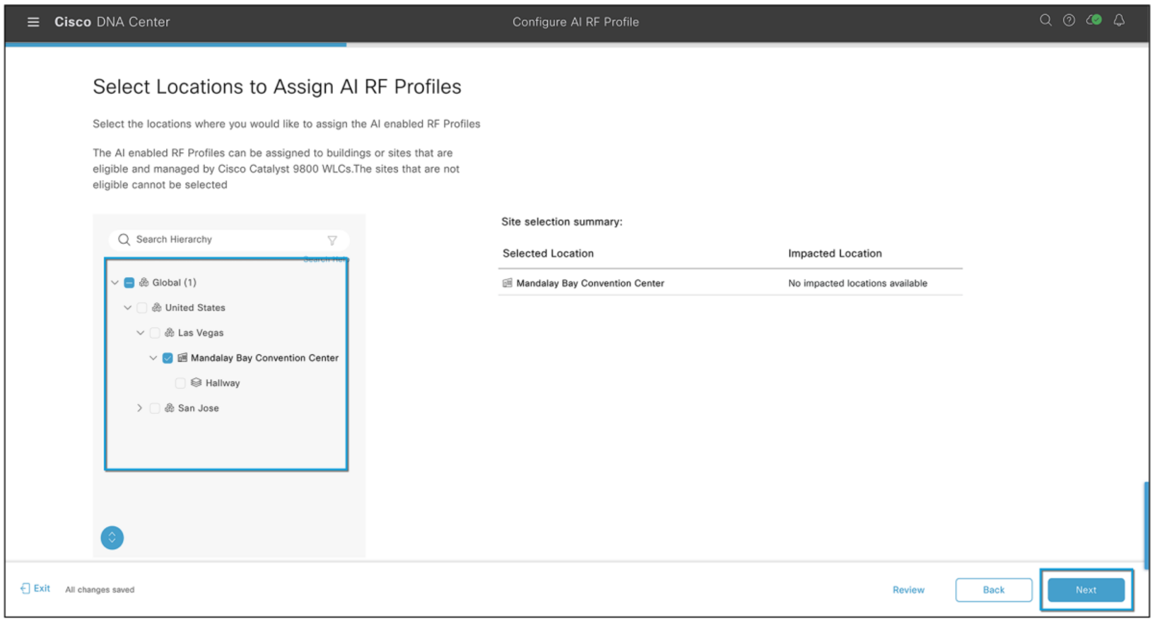
Task Name*: Create AI-RF profile

Figure 62.
Creating a task

Step 3: Select the location to assign the AI RF profile

AI-Enhanced RRM is enabled at the WLC level globally, just as RRM is. All sites having APs associated with the controller but assigned to other buildings will also be managed by AI-Enhanced RRM; this is supported by the workflow. All impacted sites will be listed as Impacted and assigned as well.

Select the site(s) to assign and click **Next**.



Select Locations to Assign AI RF Profiles

Select the locations where you would like to assign the AI enabled RF Profiles

The AI enabled RF Profiles can be assigned to buildings or sites that are eligible and managed by Cisco Catalyst 9800 WLCs.The sites that are not eligible cannot be selected

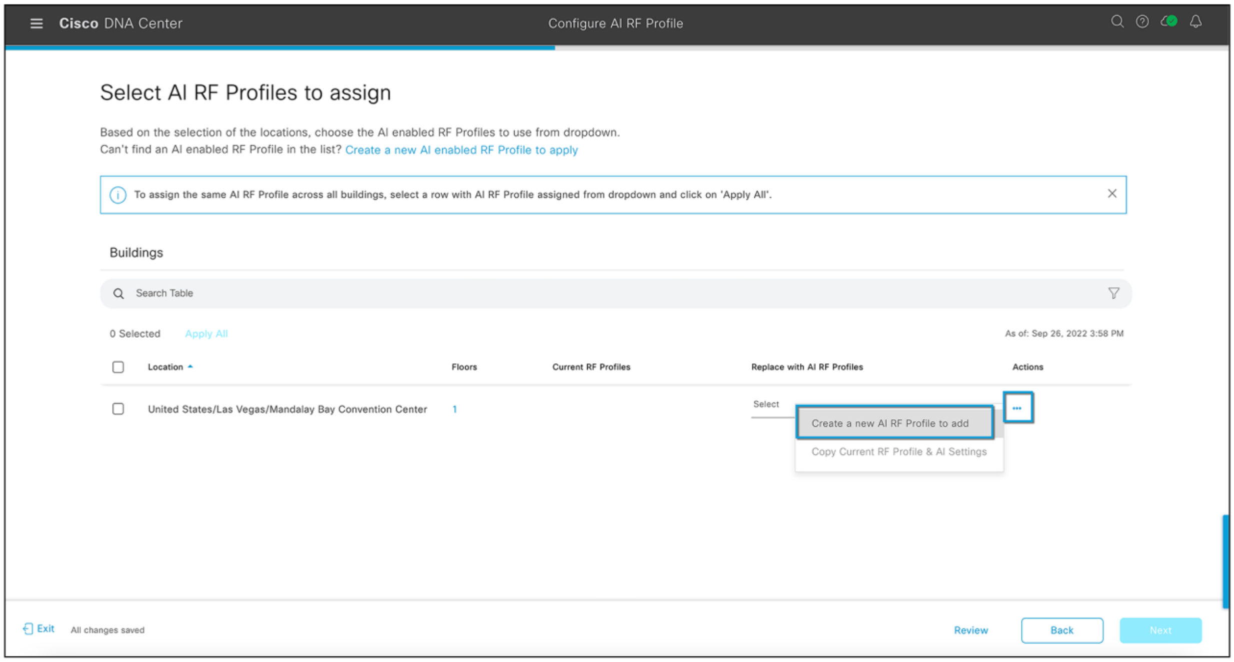
Site selection summary:

Selected Location	Impacted Location
Mandalay Bay Convention Center	No impacted locations available

Figure 63.
Site assignment for the AI RF profile

Step 4: Select the AI RF profile to assign

You can select from a previously configured AI RF profile, or select the Actions menu and choose “Create a new AI RF Profile to add” or “Copy the currently assigned RF Profile and AI Settings.”



Select AI RF Profiles to assign

Based on the selection of the locations, choose the AI enabled RF Profiles to use from dropdown.
Can't find an AI enabled RF Profile in the list? Create a new AI enabled RF Profile to apply

To assign the same AI RF Profile across all buildings, select a row with AI RF Profile assigned from dropdown and click on 'Apply All'.

Buildings

0 Selected Apply All

As of: Sep 26, 2022 3:58 PM

□	Location	Floors	Current RF Profiles	Replace with AI RF Profiles	Actions
□	United States/Las Vegas/Mandalay Bay Convention Center	1		Select	···

All changes saved

Cisco DNA Center
Configure AI RF Profile
Search Table
Create a new AI RF Profile to add
Copy Current RF Profile & AI Settings
Exit
Review
Back
Next

Figure 64.
Selecting the AI RF profile

Step 5: Create a new AI RF profile (6-GHz support starts with Cisco DNA Center Release 2.3.4)

- Enter a name for the AI RF profile.
- Select the bands you want your network to operate on.
- Enter the busy hour of your network and how sensitive your network is to RRM changes.
- Enable all the algorithms you want to use in this AI RF profile.

What is the busy hour? It determines when RRM optimizations will occur, based on how sensitive your network is to changes:

- High sensitivity: RRM optimizations will occur whenever RF improvements are possible.
- Medium sensitivity: RRM optimizations will occur less frequently than for a high sensitivity setting.
- Low sensitivity: RRM optimizations will be deferred until after the configured busy hour.

  Note: Sensitivity outside the configured busy hour is equivalent to high sensitivity.

An AI RF profile contains the same elements as a legacy controller-based RF profile but adds configurations for services and other elements that will be subscribed to.

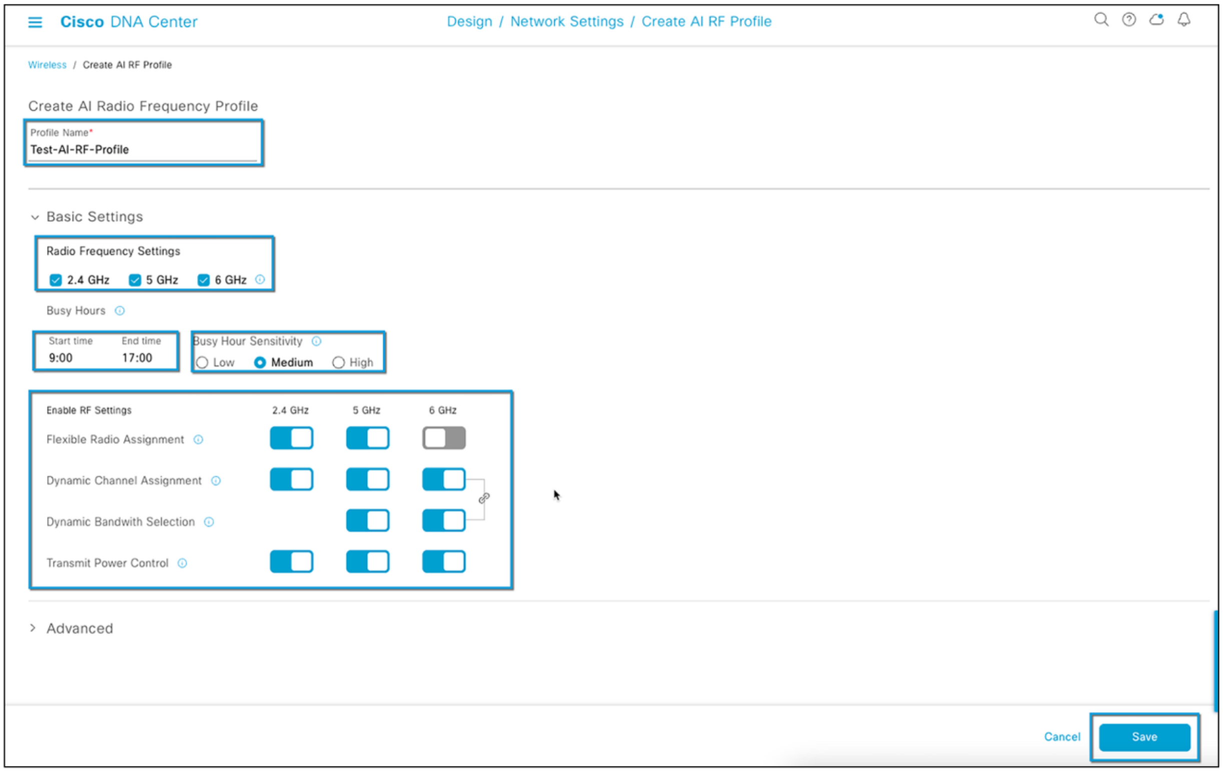
The services include:

- FRA: Flexible Radio Assignment (not supported in 6 GHz as of Cisco DNA Center Release 2.3.4)
- DCA: Dynamic Chanel Assignment
- TPC: Transmit Power Control
- DBS: Dynamic Bandwidth Selection

Note: At least one of the four AI-Enhanced RRM services (FRA, DCA, TPC, and DBS) must be enabled to onboard a site in the AI-Enhanced RRM service.

Any changes or corrections can be made at this time and saved. The profile exists only on Cisco DNA Center at this point. Until the devices are provisioned and have profiles (either classic or AI) selected and pushed, no changes are made to the controllers or the associated APs' operational configurations.

When satisfied, select **Save** to complete the action. Upon saving you will be returned to the AI RF profiles main screen showing the results of the actions.


Cisco DNA Center
Design / Network Settings / Create AI RF Profile
Wireless / Create AI RF Profile

Create AI Radio Frequency Profile

Profile Name*: Test-AI-RF-Profile

Basic Settings

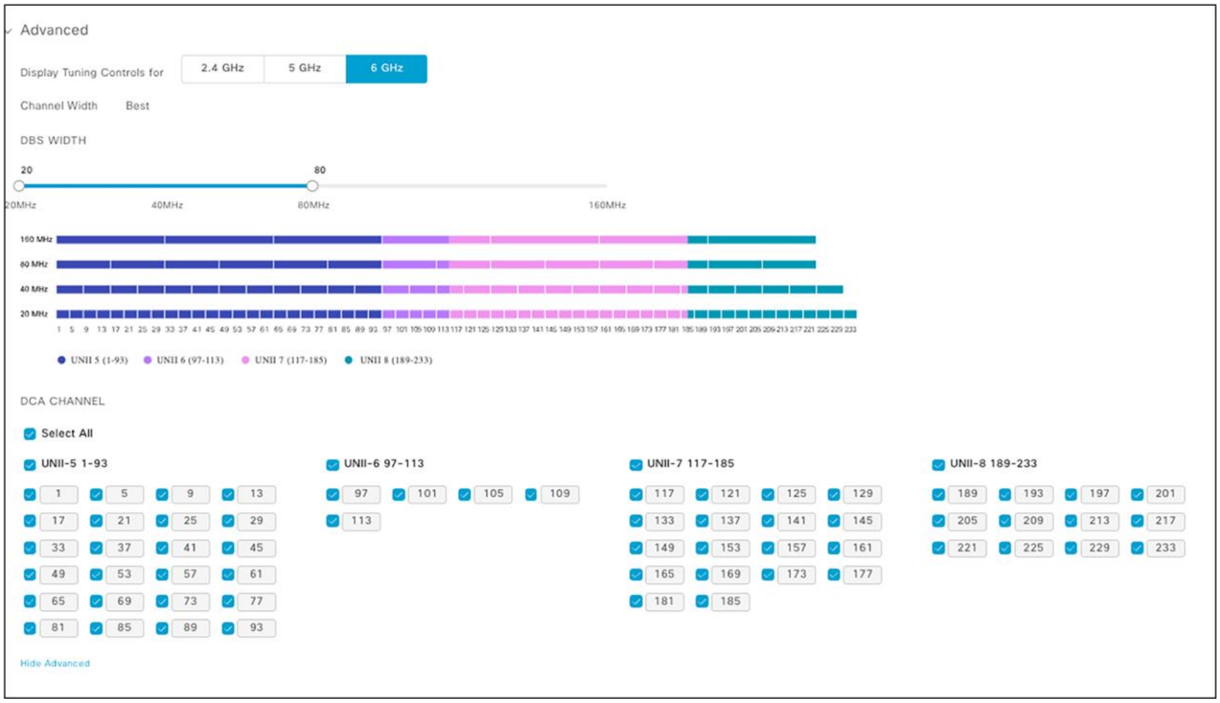
Radio Frequency Settings: ☑ 2.4 GHz ☑ 5 GHz ☑ 6 GHz

Busy Hours: Start time 9:00, End time 17:00

Busy Hour Sensitivity: ○ Low ● Medium ○ High

Enable RF Settings	2.4 GHz	5 GHz	6 GHz
Flexible Radio Assignment	●	●	○
Dynamic Channel Assignment	●	●	●
Dynamic Bandwith Selection		●	●
Transmit Power Control	●	●	●

Figure 65.
Creating an AI RF profile



Advanced

Display Tuning Controls for: 2.4 GHz | 5 GHz | **6 GHz**

Channel Width: Best

DBS WIDTH: 20 – 80

DCA CHANNEL

☑ Select All

☑ UNII-5 1-93

☑ 1 ☑ 5 ☑ 9 ☑ 13
☑ 17 ☑ 21 ☑ 25 ☑ 29
☑ 33 ☑ 37 ☑ 41 ☑ 45
☑ 49 ☑ 53 ☑ 57 ☑ 61
☑ 65 ☑ 69 ☑ 73 ☑ 77
☑ 81 ☑ 85 ☑ 89 ☑ 93

☑ UNII-6 97-113

☑ 97 ☑ 101 ☑ 105 ☑ 109
☑ 113

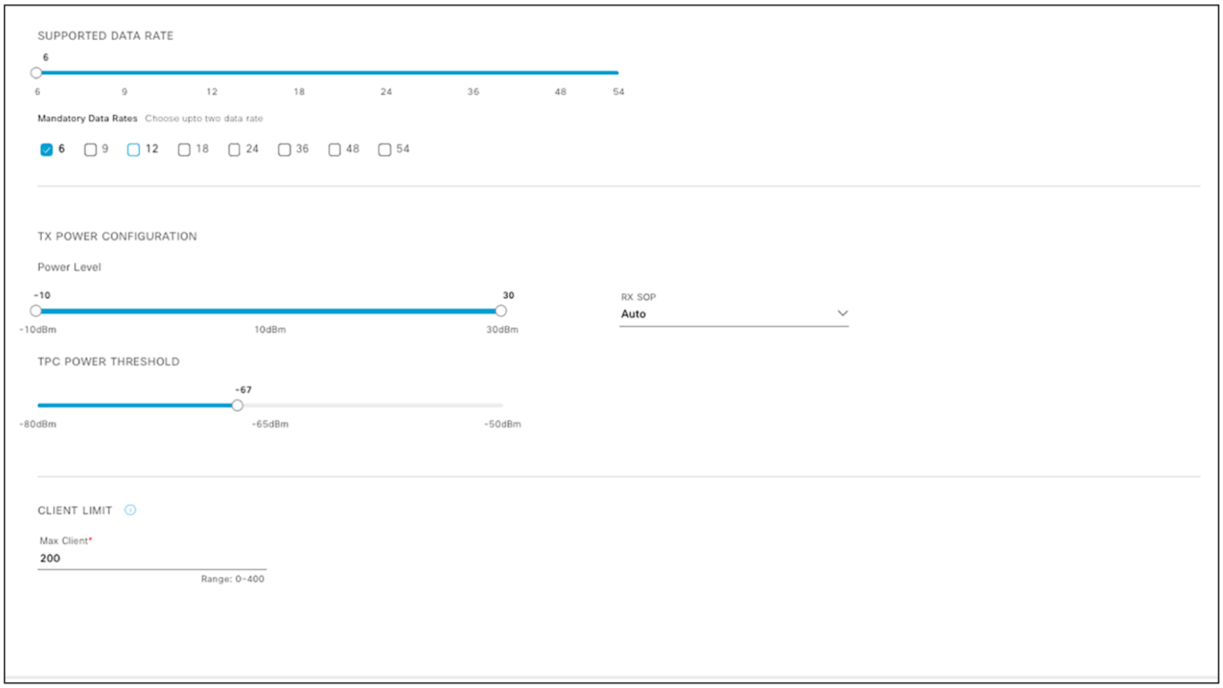
☑ UNII-7 117-185

☑ 117 ☑ 121 ☑ 125 ☑ 129
☑ 133 ☑ 137 ☑ 141 ☑ 145
☑ 149 ☑ 153 ☑ 157 ☑ 161
☑ 165 ☑ 169 ☑ 173 ☑ 177
☑ 181 ☑ 185

☑ UNII-8 189-233

☑ 189 ☑ 193 ☑ 197 ☑ 201
☑ 205 ☑ 209 ☑ 213 ☑ 217
☑ 221 ☑ 225 ☑ 229 ☑ 233

Figure 66.
Advanced AI RF profile configurations for DCA and DBS



SUPPORTED DATA RATE: 6

Mandatory Data Rates Choose upto two data rate

☑ 6 □ 9 □ 12 □ 18 □ 24 □ 36 □ 48 □ 54

TX POWER CONFIGURATION

Power Level: -10 – 30

RX SOP: Auto

TPC POWER THRESHOLD: -67

CLIENT LIMIT

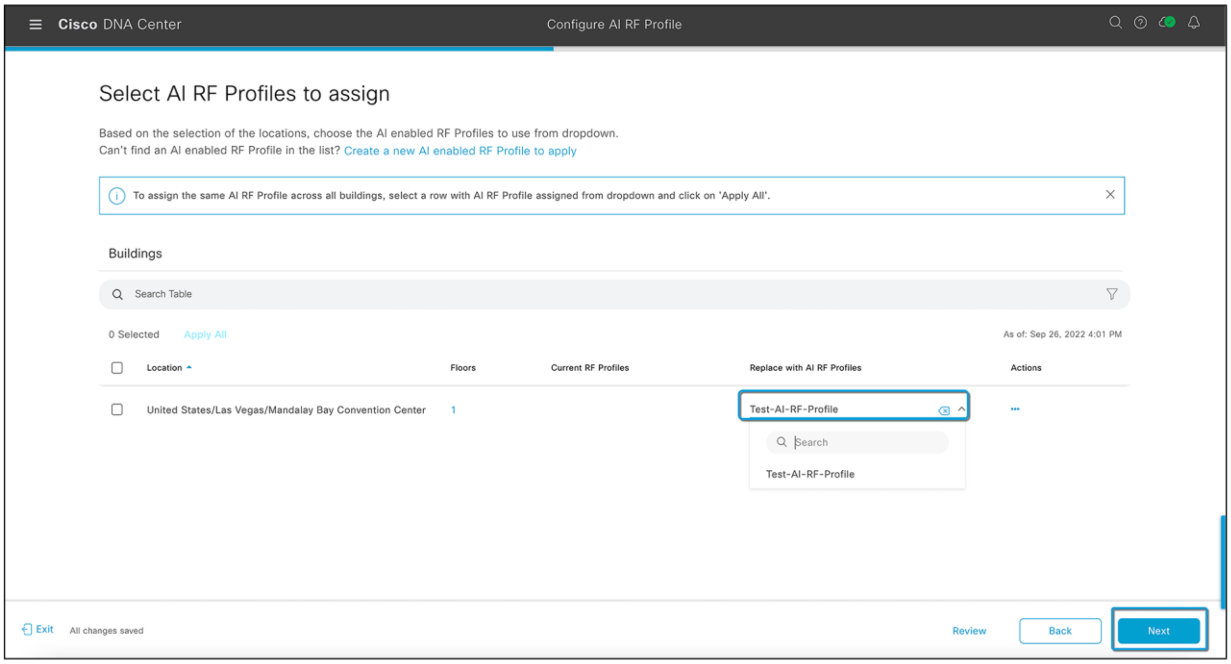
Max Client*: 200

Range: 0-400

Figure 67.
Advanced AI RF profile configurations for TPC and data rate support

Step 6: Assign an AI RF profile to a site

Select an AI RF profile to assign to the site, as shown in Figure 68.



Select AI RF Profiles to assign

Based on the selection of the locations, choose the AI enabled RF Profiles to use from dropdown.
Can't find an AI enabled RF Profile in the list? Create a new AI enabled RF Profile to apply

To assign the same AI RF Profile across all buildings, select a row with AI RF Profile assigned from dropdown and click on 'Apply All'.

Buildings

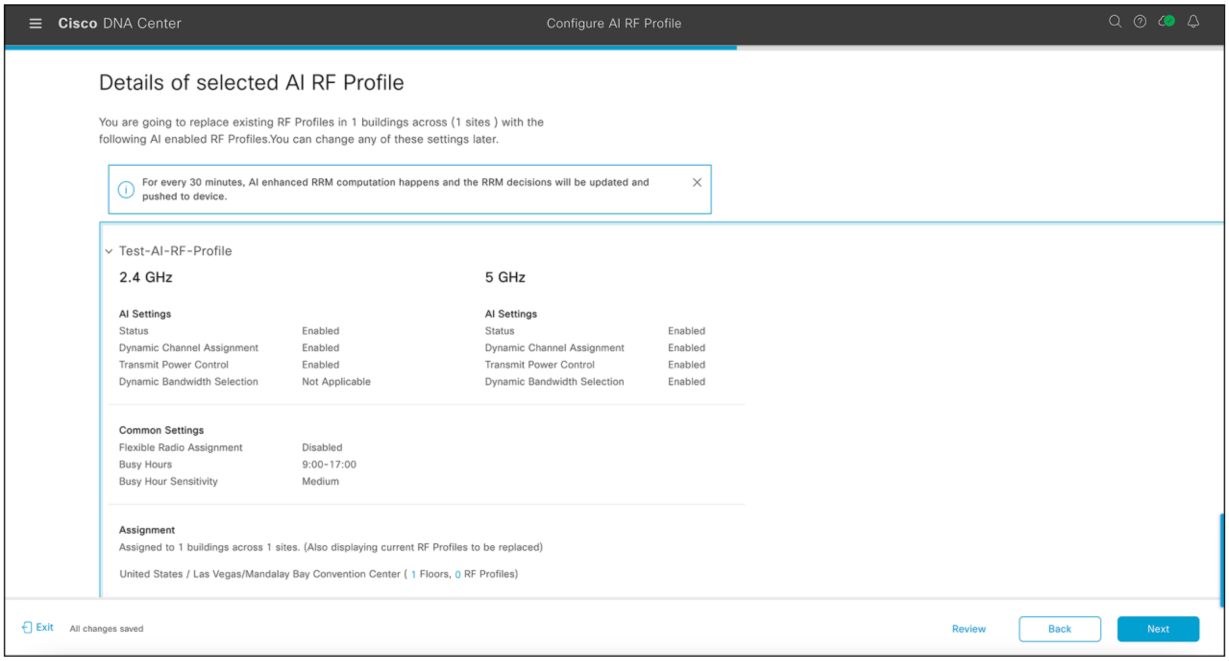
0 Selected Apply All — As of: Sep 26, 2022 4:01 PM

	Location	Floors	Current RF Profiles	Replace with AI RF Profiles	Actions
□	United States/Las Vegas/Mandalay Bay Convention Center	1		Test-AI-RF-Profile	···

Figure 68.
Selecting an AI RF profile

Step 7: Review and verify the summary

On the summary page, all the configurations from the AI RF profile will be listed, along with the site assignments. Click **Next** once you have verified the information.



Details of selected AI RF Profile

You are going to replace existing RF Profiles in 1 buildings across (1 sites) with the following AI enabled RF Profiles.You can change any of these settings later.

For every 30 minutes, AI enhanced RRM computation happens and the RRM decisions will be updated and pushed to device.

Test-AI-RF-Profile

2.4 GHz		5 GHz	
AI Settings		**AI Settings**	
Status	Enabled	Status	Enabled
Dynamic Channel Assignment	Enabled	Dynamic Channel Assignment	Enabled
Transmit Power Control	Enabled	Transmit Power Control	Enabled
Dynamic Bandwidth Selection	Not Applicable	Dynamic Bandwidth Selection	Enabled

Common Settings

Flexible Radio Assignment	Disabled
Busy Hours	9:00-17:00
Busy Hour Sensitivity	Medium

Assignment

Assigned to 1 buildings across 1 sites. (Also displaying current RF Profiles to be replaced)

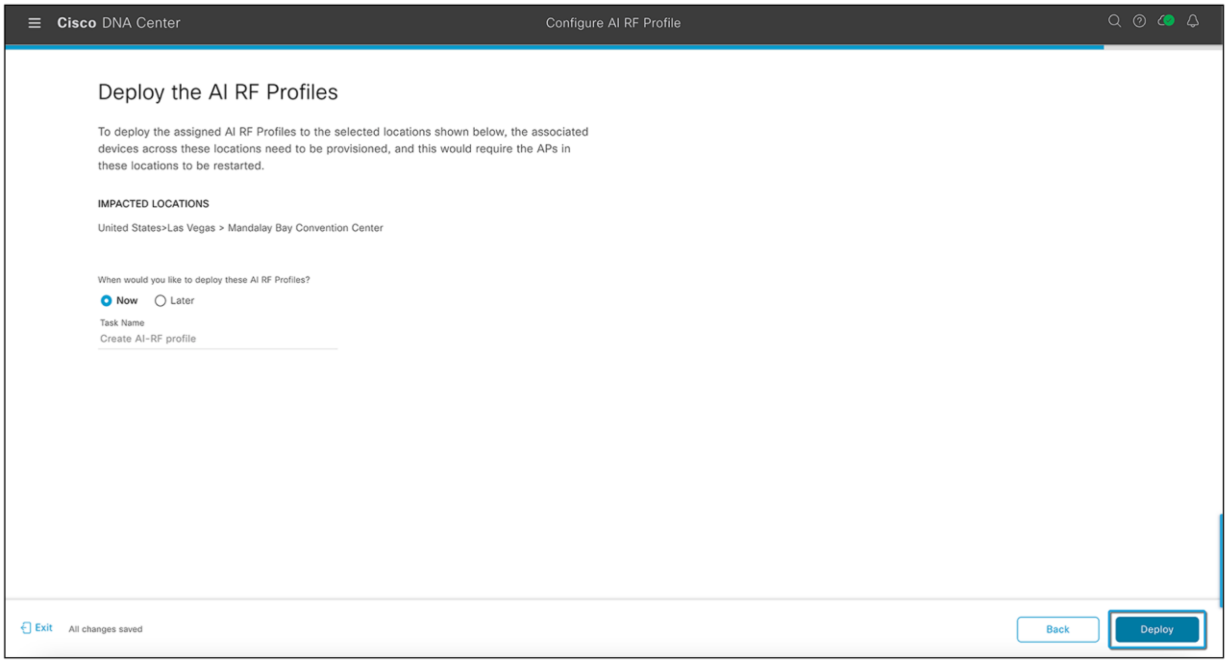
United States / Las Vegas/Mandalay Bay Convention Center (1 Floors, 0 RF Profiles)

Figure 69.
Summary of AI RF profile assignment to a site

Step 8: Choose when to deploy the AI RF profile

AI RF profile deployment can be done now or can be scheduled for a nonoperational hour.

Selecting **Next** will push the AI RF profile to the selected WLC and APs once provisioned. As with legacy RF profiles, changing or applying an RF profile causes a Control and Provisioning of Wireless Access Points (CAPWAP) reset and momentarily disrupts AP connectivity. A warning is displayed, as shown in Figure 71.



Deploy the AI RF Profiles

To deploy the assigned AI RF Profiles to the selected locations shown below, the associated devices across these locations need to be provisioned, and this would require the APs in these locations to be restarted.

IMPACTED LOCATIONS

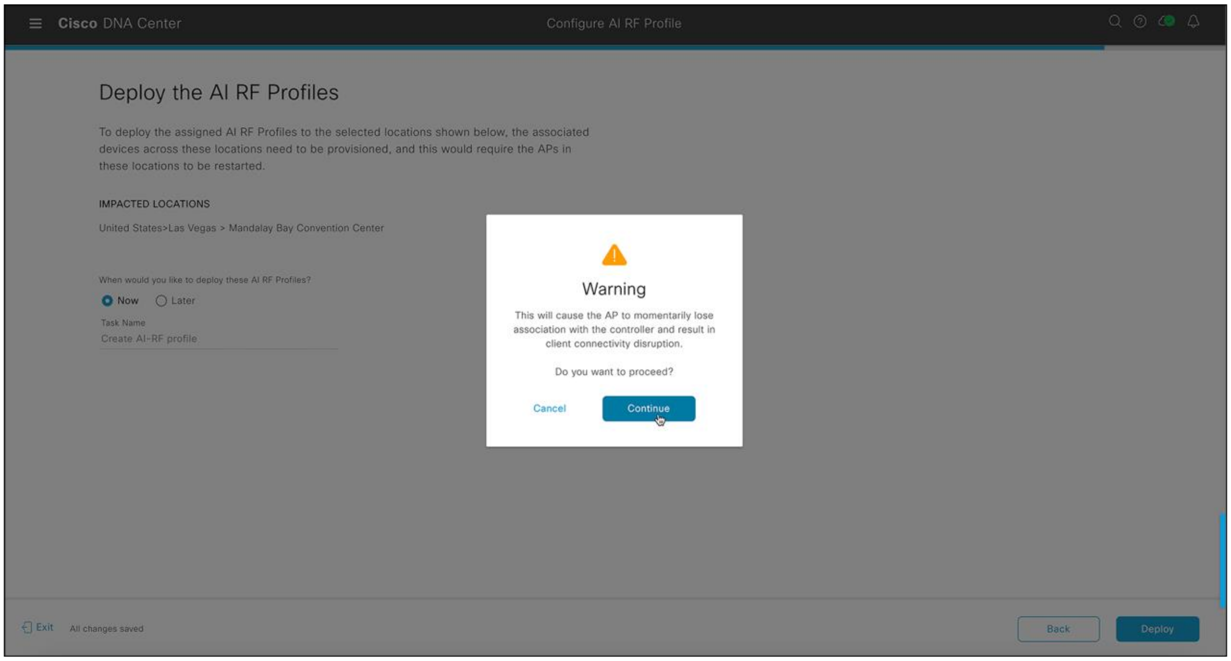
United States>Las Vegas > Mandalay Bay Convention Center

When would you like to deploy these AI RF Profiles?

● Now ○ Later

Task Name: Create AI-RF profile

Figure 70.
Deploying an AI RF profile to a site



Warning

This will cause the AP to momentarily lose association with the controller and result in client connectivity disruption.

Do you want to proceed?

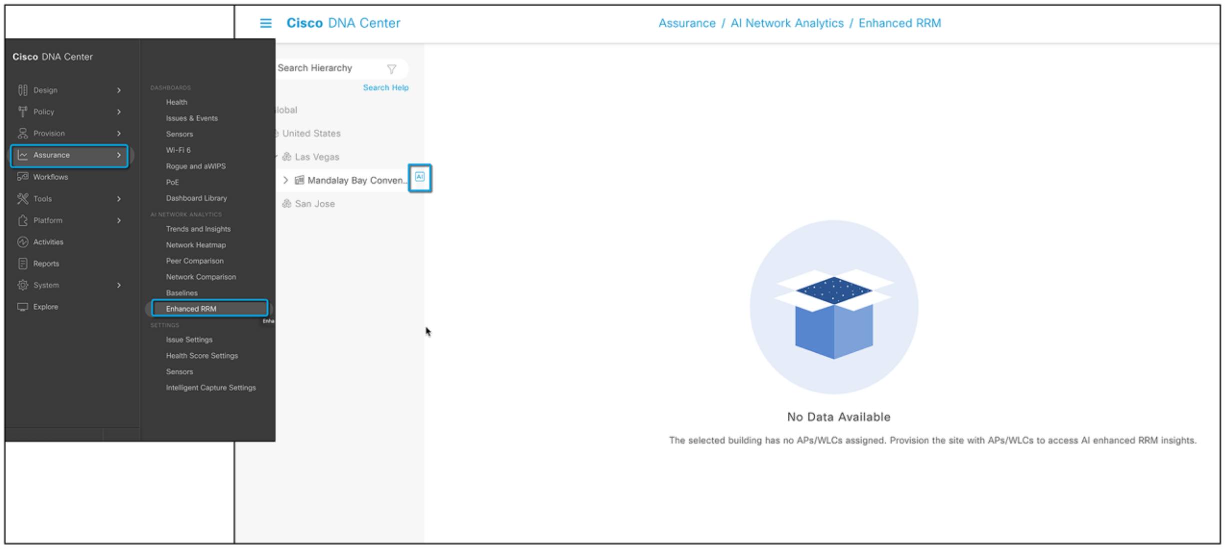
Figure 71.
Warning displayed when deploying an AI RF profile to a site

Step 9: Verify the assignment

Verify that the AI RF profile has been successfully assigned to the site.

- Go to the hamburger menu (☰) and choose Assurance > AI-Enhanced RRM.
- Use the site hierarchy sidebar and navigate to the site where the AI RF profile is deployed.
- An AI logo will be shown and the site name will be highlighted, which confirms that the AI RF profile has been successfully assigned to the site.

The next step is to provision the wireless controller and access points. This will put Cisco DNA Center in control of the controller and APs and allow AI-Enhanced RRM to take control over the controller RRM.



No Data Available

The selected building has no APs/WLCs assigned. Provision the site with APs/WLCs to access AI enhanced RRM insights.

Figure 72.
AI logo on the site with the AI RF profile

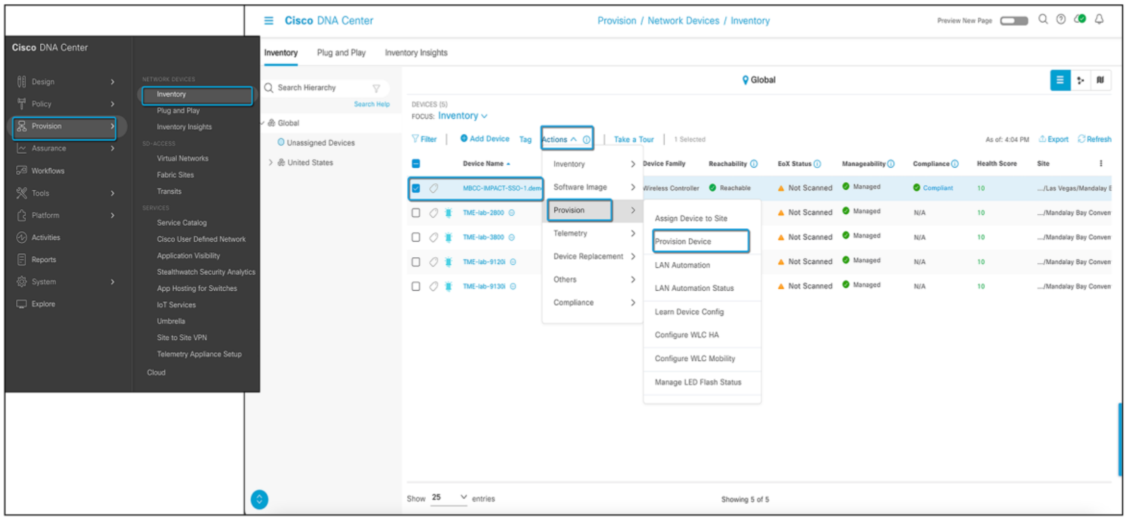
Part 6: Provision the wireless controller and access points

Provisioning devices allows Cisco DNA Center to send manage the device using the configurations in the network profile assigned to the site.

Step 1: Provision the WLC and APs

On Cisco DNA Center, go to the hamburger menu (☰) and choose Provision > Inventory.

- Select the checkbox next to the name of the Catalyst 9800 Series Wireless Controller that you want to provision.
- From the Actions drop-down list, choose Provision > Provision Device.



Device Name	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site
☑ MBCC-IMPACT-SSO-1.dem	Wireless Controller	Reachable	Not Scanned	Managed	Compliant	10	.../Las Vegas/Mandalay E
□ TME-lab-2800			Not Scanned	Managed	N/A	10	.../Mandalay Bay Conven
□ TME-lab-3800			Not Scanned	Managed	N/A	10	.../Mandalay Bay Conven
□ TME-lab-9120i			Not Scanned	Managed	N/A	10	.../Mandalay Bay Conven
□ TME-lab-9130i			Not Scanned	Managed	N/A	10	.../Mandalay Bay Conven

Figure 73.
Provisioning the Catalyst 9800 wireless controller

Step 2: Assign a site

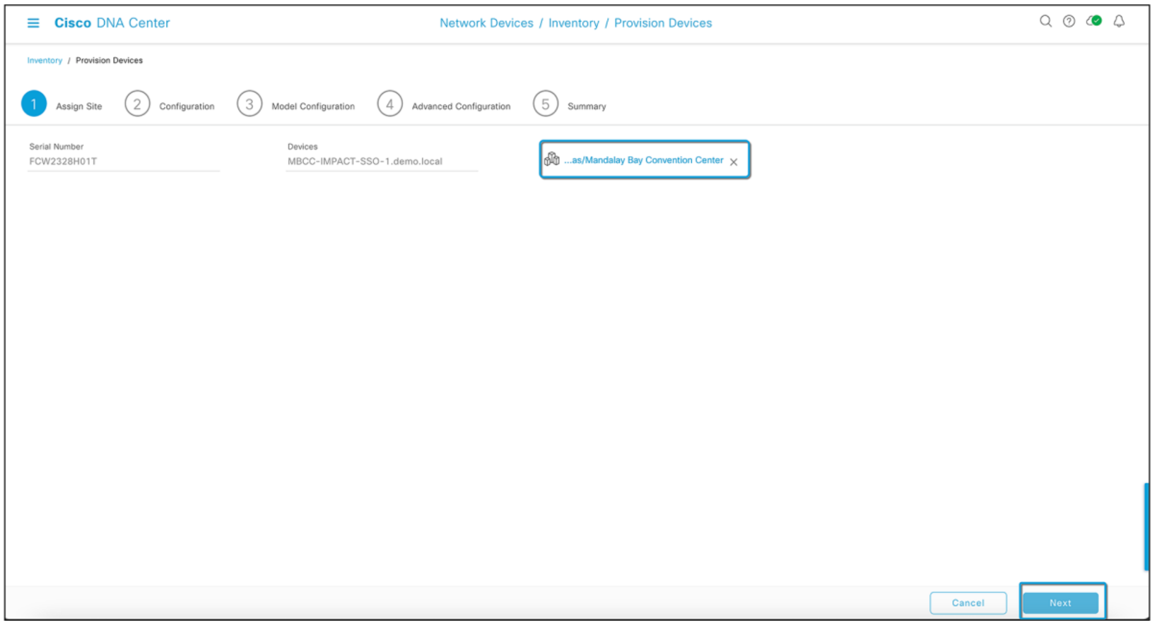
In the Assign Site window, click **Choose a Site** to associate the controller with a site.

In the Choose a Site slide-in window, select the checkbox next to the site name to associate it with the Catalyst 9800 controller and click **Save**.

You can either select a parent site or individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the checkbox to deselect an individual site.

Click **Next**.

The Configuration window appears.



Serial Number: FCW2328H01T

Devices: MBCC-IMPACT-SSO-1.demo.local

...as/Mandalay Bay Convention Center

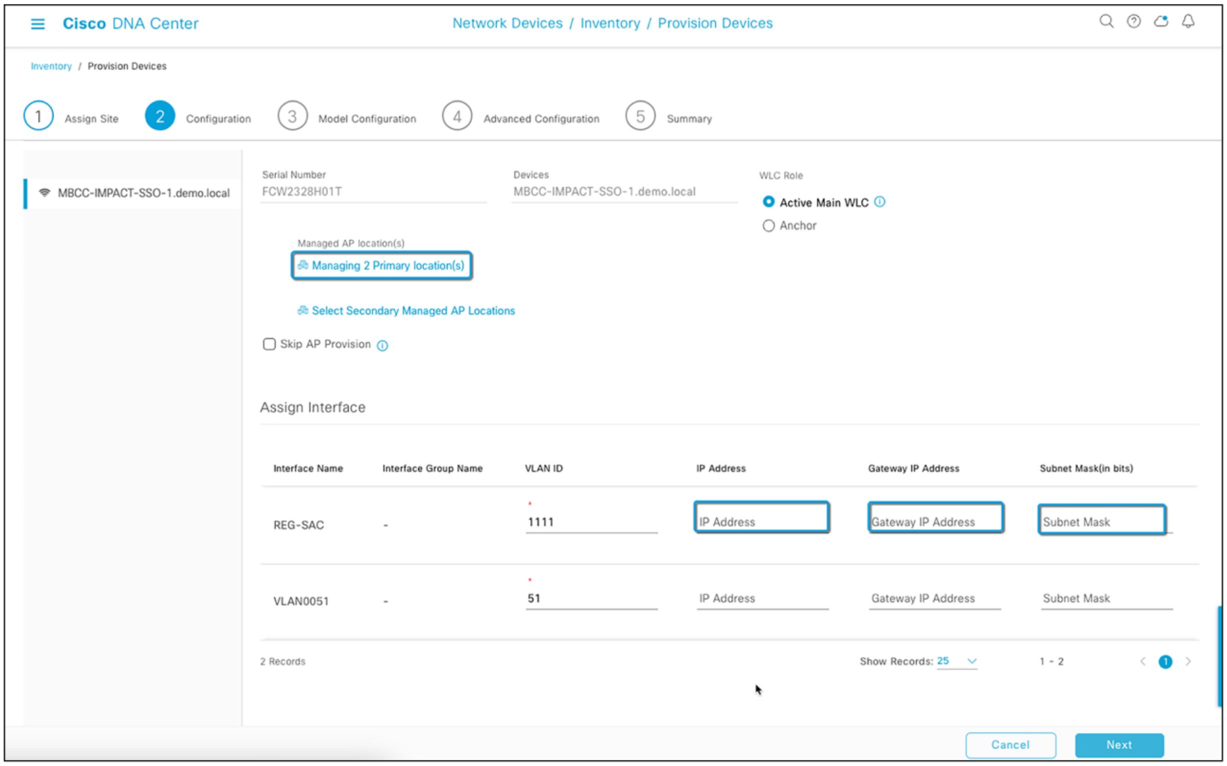
Figure 74.
Assigning a site to the Catalyst 9800 wireless controller

Step 3: Configure the controller configurations

- Select a role for the Catalyst 9800 Series Wireless Controller: **Active Main WLC** or Anchor.
- Click **Select Primary Managed AP Locations** to select the managed AP location for the primary controller (Figure 75).
- Click **Select Secondary Managed AP Locations** to select the managed AP location for the secondary controller.
- You can either select a parent site or the individual sites and click **Save** (Figure 76).
- Click **Next**.

If you select a parent site, all the children under the parent site are also selected. You can uncheck the checkbox to deselect a particular site.

Note: Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that site. One site is managed by only one wireless controller.


Cisco DNA Center
Network Devices / Inventory / Provision Devices
Inventory / Provision Devices
1 Assign Site
2 Configuration
3 Model Configuration
4 Advanced Configuration
5 Summary
MBCC-IMPACT-SSO-1.demo.local

Serial Number: FCW2328H01T

Devices: MBCC-IMPACT-SSO-1.demo.local

WLC Role: ● Active Main WLC ○ Anchor

Managed AP location(s): Managing 2 Primary location(s)

Select Secondary Managed AP Locations

□ Skip AP Provision

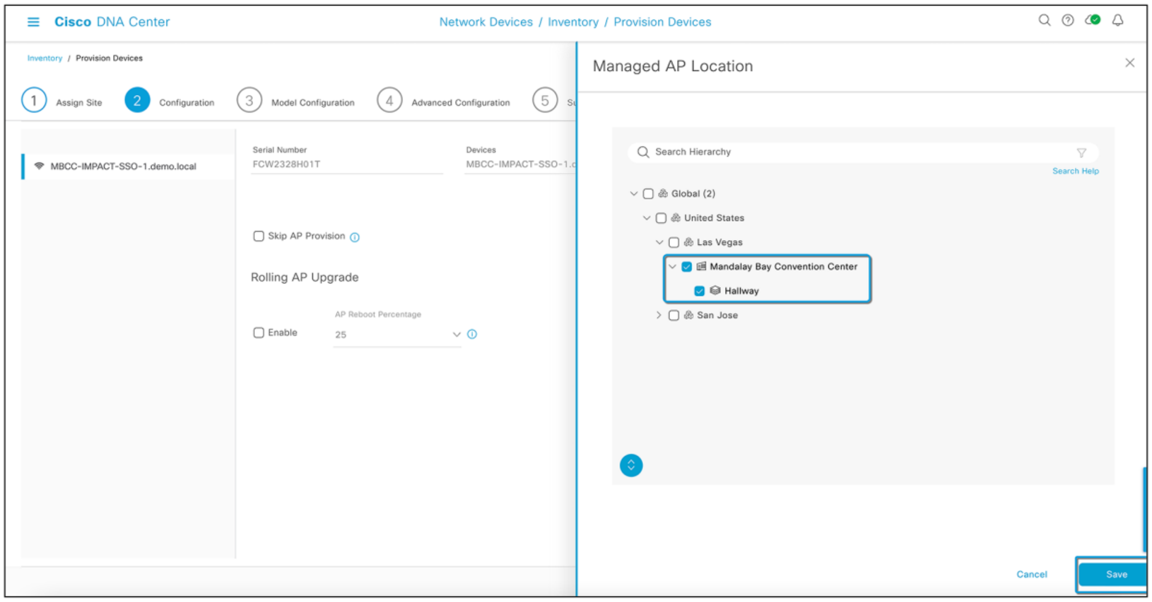
Assign Interface

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
REG-SAC	-	1111	IP Address	Gateway IP Address	Subnet Mask
VLAN0051	-	51	IP Address	Gateway IP Address	Subnet Mask

2 Records

Show Records: 25 1 - 2

Figure 75.
Configuring the AP sites managed by the controller



MBCC-IMPACT-SSO-1.demo.local

Serial Number: FCW2328H01T

Devices: MBCC-IMPACT-SSO-1.c

□ Skip AP Provision

Rolling AP Upgrade

□ Enable

AP Reboot Percentage: 25

Managed AP Location

Search Hierarchy

Search Help

- □ Global (2)
  - □ United States
    - □ Las Vegas
      - ☑ Mandalay Bay Convention Center
        - ☑ Hallway
    - □ San Jose

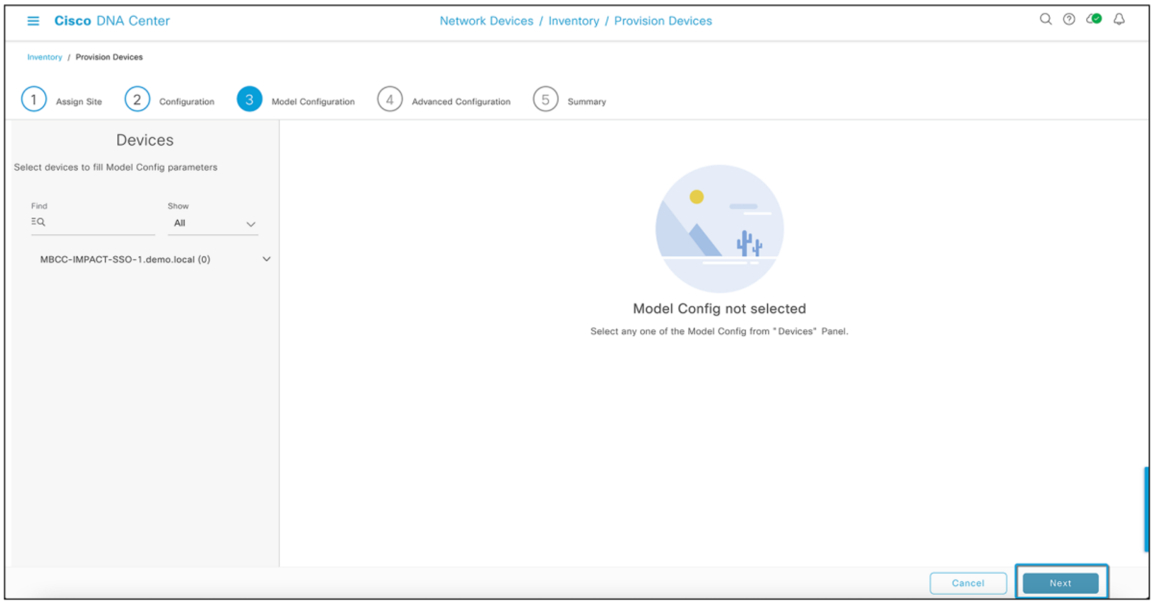
Figure 76.
Selecting the site/area for the managed AP location

Step 4: Assign a model configuration (optional)

In the Devices pane, you can search for a model configuration design by entering its name in the Find field or by expanding the device and selecting a model configuration design.

The selected model configuration design appears in the right pane.

This is an optional step if you want to add a model configuration to your Catalyst 9800 wireless controller on top of the existing configuration. Click **Next** to skip this step. Refer to Design Model Configuration in the Cisco DNA Center User Guide for more information on creating and editing network-specific model configurations using the Model Config Editor. If no model configuration is assigned, simply click **Next** to continue.



Devices

Select devices to fill Model Config parameters

Find

Show: All

MBCC-IMPACT-SSO-1.demo.local (0)

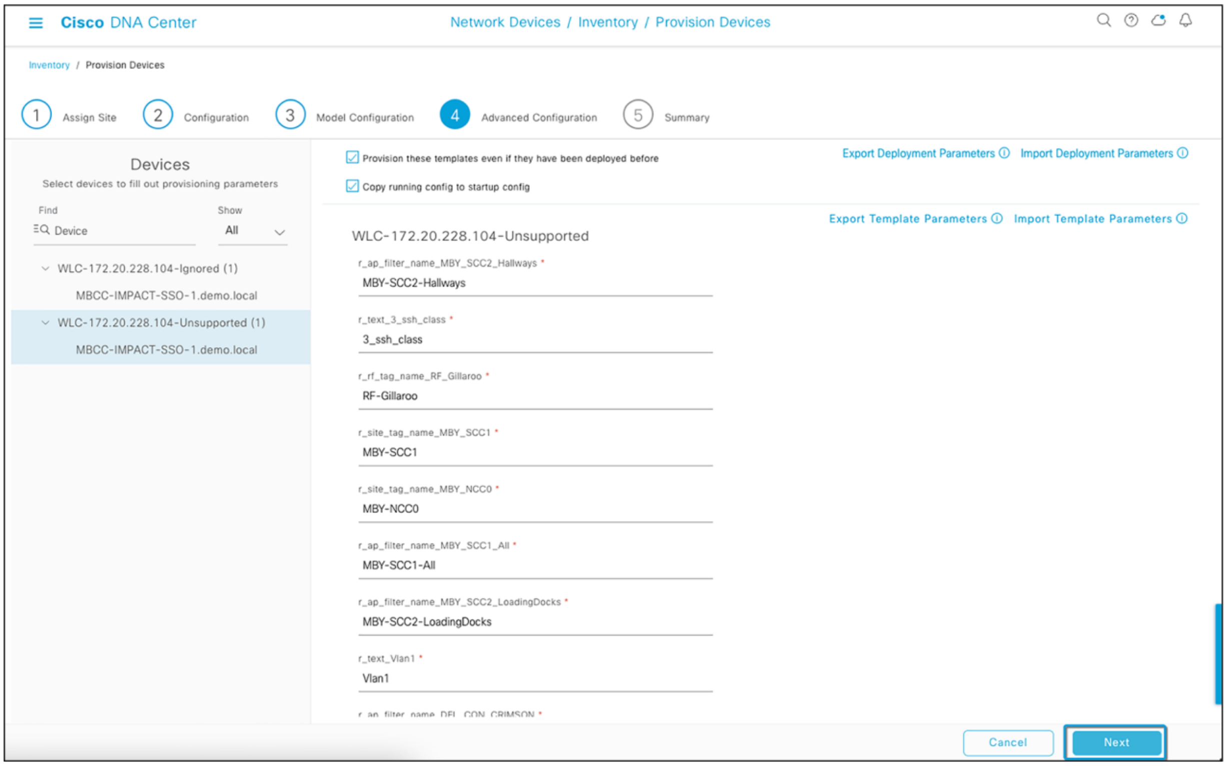
Model Config not selected

Select any one of the Model Config from "Devices" Panel.

Figure 77.
Model configurations for the Catalyst 9800 wireless controller

Step 5: Advanced configuration, select device templates

The **Advanced Configuration** window appears, where you enter values for the predefined template variables. A CLI template will be used to add all the unsupported configuration templates generated from the Learn Device Configuration workflow. You can also use a brand new CLI template if necessary, with more configurations that are not supported by Cisco DNA Center. Search for the device or the template in the **Devices** panel. The selected CLI template will be parsed here and will be verified for all field checks that will be pushed to the new policy/site tag.


Cisco DNA Center
Network Devices / Inventory / Provision Devices
Inventory / Provision Devices
1 Assign Site
2 Configuration
3 Model Configuration
4 Advanced Configuration
5 Summary
Devices
Select devices to fill out provisioning parameters
Find
Device
Show
All
Export Deployment Parameters ⓘ
Import Deployment Parameters ⓘ
Export Template Parameters ⓘ
Import Template Parameters ⓘ
Cancel
Next

WLC-172.20.228.104-Ignored (1)
MBCC-IMPACT-SSO-1.demo.local
WLC-172.20.228.104-Unsupported (1)
MBCC-IMPACT-SSO-1.demo.local

☑ Provision these templates even if they have been deployed before
☑ Copy running config to startup config

WLC-172.20.228.104-Unsupported

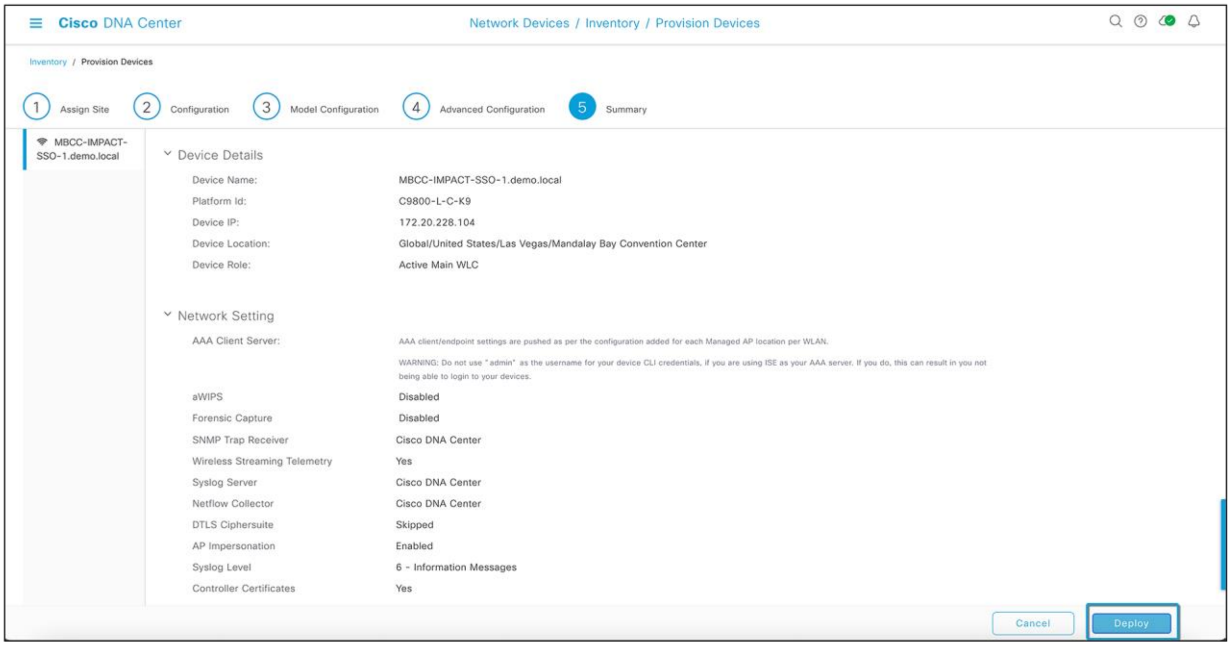
r_ap_filter_name_MBY_SCC2_Hallways *: MBY-SCC2-Hallways
r_text_3_ssh_class *: 3_ssh_class
r_rf_tag_name_RF_Gillaroo *: RF-Gillaroo
r_site_tag_name_MBY_SCC1 *: MBY-SCC1
r_site_tag_name_MBY_NCC0 *: MBY-NCC0
r_ap_filter_name_MBY_SCC1_All *: MBY-SCC1-All
r_ap_filter_name_MBY_SCC2_LoadingDocks *: MBY-SCC2-LoadingDocks
r_text_Vlan1 *: Vlan1
r_ap_filter_name_DFL_CON_CRIMSON *

Figure 78.
Advanced configuration for wireless controller provisioning

Step 6: Review and verify the summary

In the summary window, review the following configurations:

- Device Details
- Network Setting
- SSID
- Managed Sites
- Rolling AP Upgrade
- Model Configs
- Interfaces
- Advanced Configuration



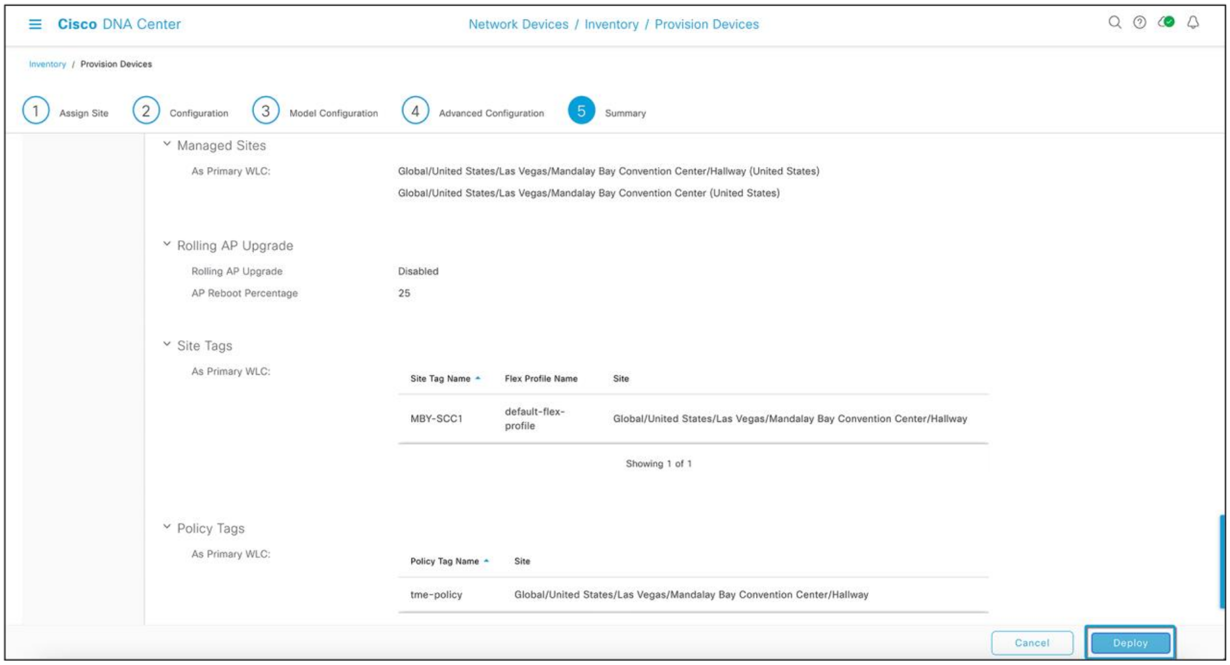
Device Details

Device Name:	MBCC-IMPACT-SSO-1.demo.local
Platform Id:	C9800-L-C-K9
Device IP:	172.20.228.104
Device Location:	Global/United States/Las Vegas/Mandalay Bay Convention Center
Device Role:	Active Main WLC

Network Setting

AAA Client Server:	AAA client/endpoint settings are pushed as per the configuration added for each Managed AP location per WLAN. WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.
aWIPS	Disabled
Forensic Capture	Disabled
SNMP Trap Receiver	Cisco DNA Center
Wireless Streaming Telemetry	Yes
Syslog Server	Cisco DNA Center
Netflow Collector	Cisco DNA Center
DTLS Ciphersuite	Skipped
AP Impersonation	Enabled
Syslog Level	6 - Information Messages
Controller Certificates	Yes

Figure 79.
Wireless controller provisioning summary



Managed Sites

As Primary WLC: Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway (United States)
Global/United States/Las Vegas/Mandalay Bay Convention Center (United States)

Rolling AP Upgrade

Rolling AP Upgrade	Disabled
AP Reboot Percentage	25

Site Tags

As Primary WLC:

Site Tag Name	Flex Profile Name	Site
MBY-SCC1	default-flex-profile	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway

Showing 1 of 1

Policy Tags

As Primary WLC:

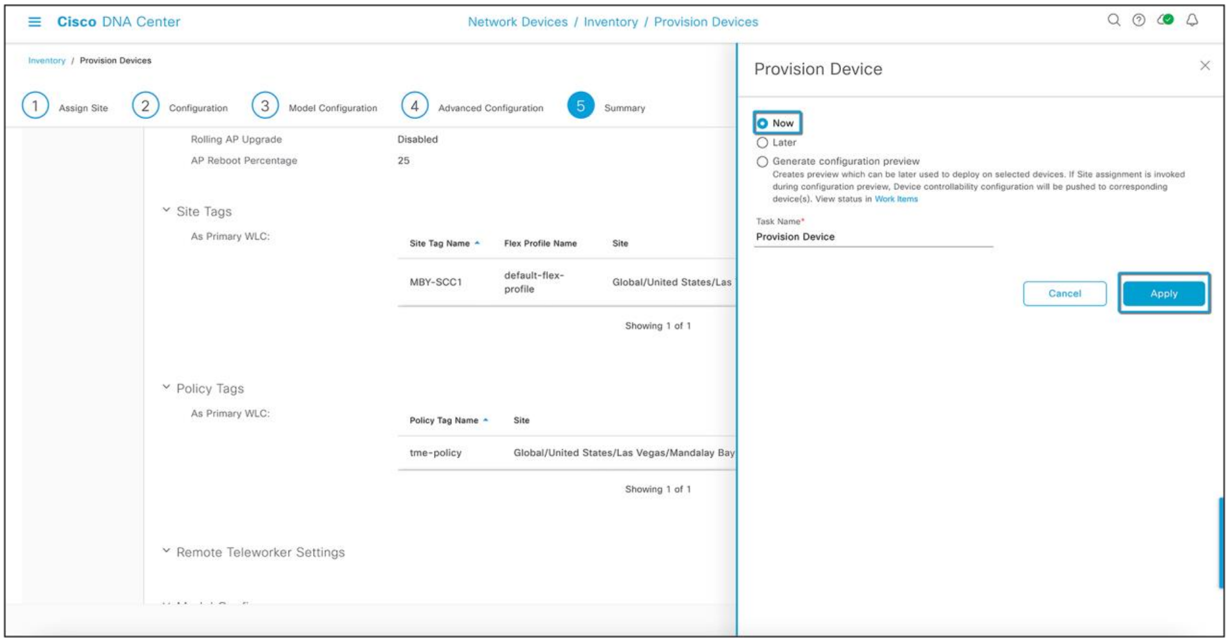
Policy Tag Name	Site
tme-policy	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway

Figure 80.
Wireless controller provisioning summary (cont.)

Step 7: Deploy the configurations

Click **Deploy** to provision the Catalyst 9800 wireless controller.

- To deploy the device immediately, click the **Now** button and then click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** button and define the date and time of the deployment.
- To generate a report on the configurations pushed by Cisco DNA Center to the Catalyst 9800 wireless controller, select Generate Configuration Preview (Figure 70) and click **Apply.**



Rolling AP Upgrade Disabled

AP Reboot Percentage 25

Site Tags

As Primary WLC:

Site Tag Name	Flex Profile Name	Site
MBY-SCC1	default-flex-profile	Global/United States/Las

Showing 1 of 1

Policy Tags

As Primary WLC:

Policy Tag Name	Site
tme-policy	Global/United States/Las Vegas/Mandalay Bay

Showing 1 of 1

Remote Teleworker Settings

Provision Device

● Now

○ Later

○ Generate configuration preview

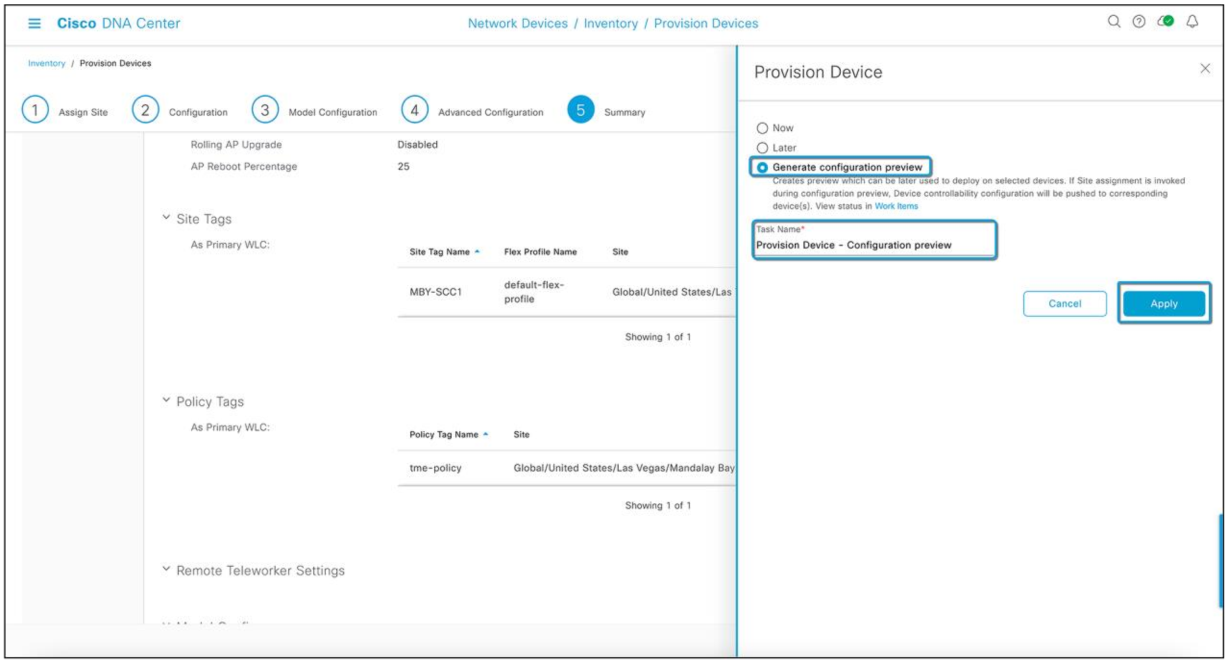
Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s). View status in Work Items

Task Name*

Provision Device

Figure 81.
Provisioning the wireless controller

- In the Task Name field, enter a name for the CLI preview task and click **Apply.**



Cisco DNA Center — Network Devices / Inventory / Provision Devices

Inventory / Provision Devices

1 Assign Site — 2 Configuration — 3 Model Configuration — 4 Advanced Configuration — 5 Summary

Rolling AP Upgrade	Disabled
AP Reboot Percentage	25

Site Tags

As Primary WLC:

Site Tag Name	Flex Profile Name	Site
MBY-SCC1	default-flex-profile	Global/United States/Las

Showing 1 of 1

Policy Tags

As Primary WLC:

Policy Tag Name	Site
tme-policy	Global/United States/Las Vegas/Mandalay Bay

Showing 1 of 1

Remote Teleworker Settings

Provision Device

○ Now

○ Later

● Generate configuration preview

Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s). View status in Work Items

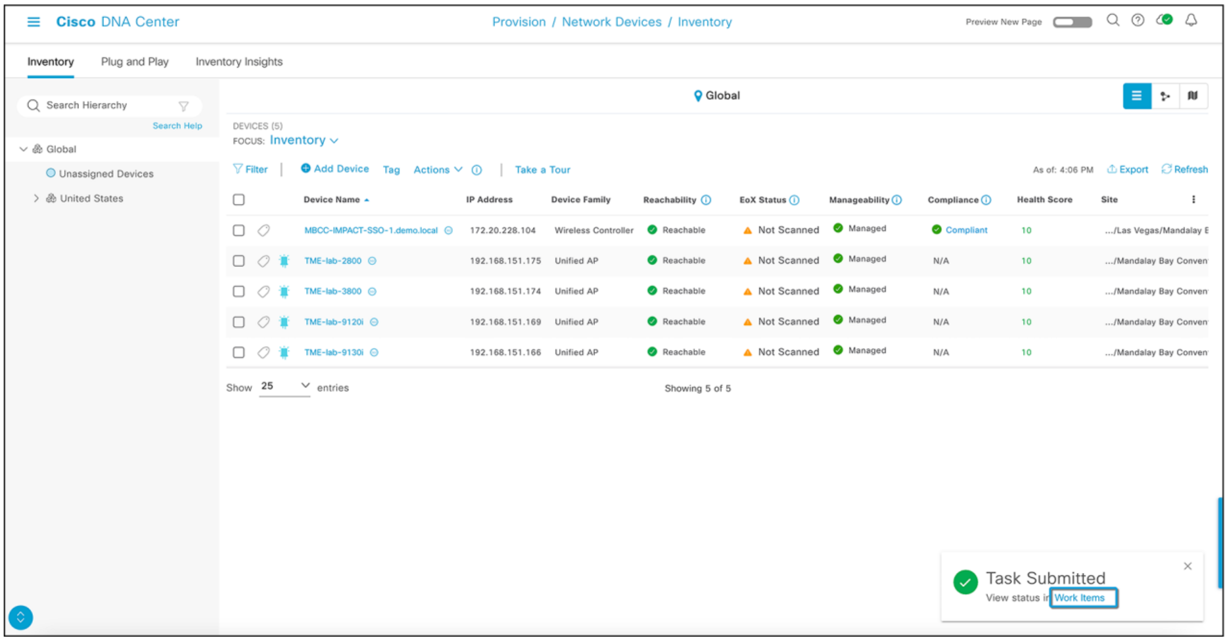
Task Name*: Provision Device - Configuration preview

Figure 82.
Generating a configuration preview

Step 8: Review the work items

In the Task Submitted pop-up, click the **Work Items** link.

Note: If you missed the Task Submitted pop-up, click the hamburger menu icon (☰) and choose Activities > Work Items.



Cisco DNA Center — Provision / Network Devices / Inventory

Global

DEVICES (5)
FOCUS: Inventory

As of: 4:06 PM

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site
MBCC-IMPACT-SSO-1.demo.local	172.20.228.104	Wireless Controller	Reachable	Not Scanned	Managed	Compliant	10	.../Las Vegas/Mandalay E
TME-lab-2800	192.168.151.175	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Mandalay Bay Conven
TME-lab-3800	192.168.151.174	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Mandalay Bay Conven
TME-lab-9120i	192.168.151.169	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Mandalay Bay Conven
TME-lab-9130i	192.168.151.166	Unified AP	Reachable	Not Scanned	Managed	N/A	10	.../Mandalay Bay Conven

Show 25 entries — Showing 5 of 5

Task Submitted
View status in Work Items

Figure 83.
Task Submitted pop-up

Step 9: Review the CLI task

In the Work Items window, click the CLI preview task for which you submitted the configuration preview request.

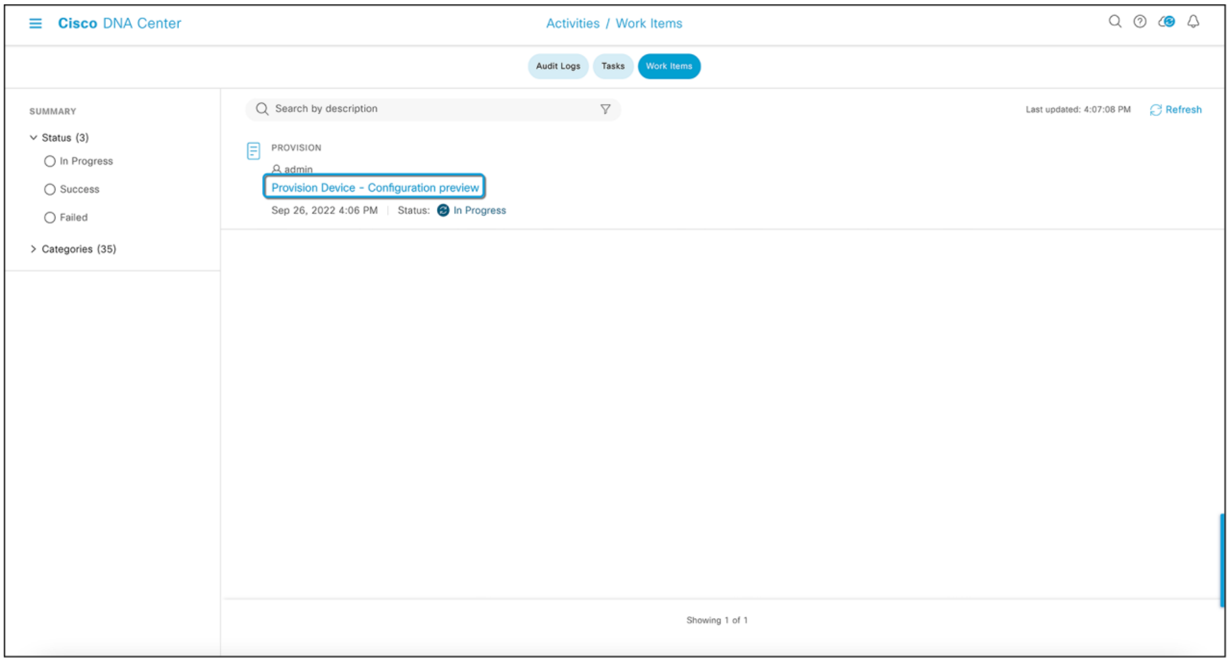
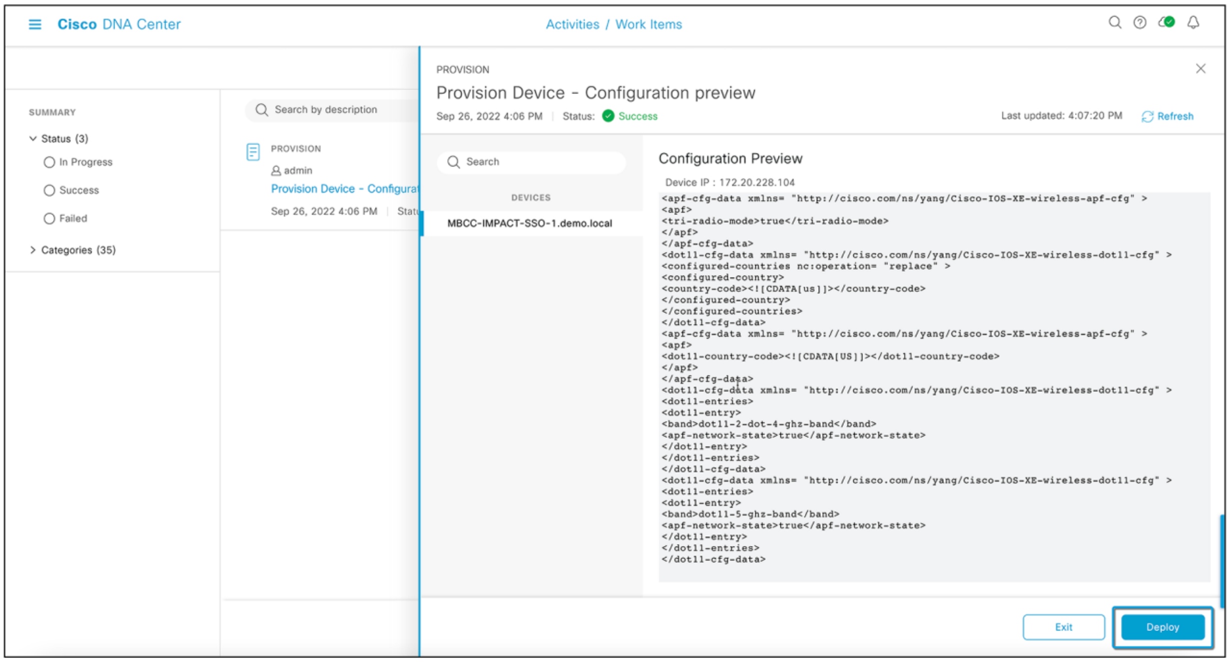


Figure 84.
Work Items list

Step 10: Review the CLI configuration and deploy the template

View the CLI configuration details and click **Deploy**.



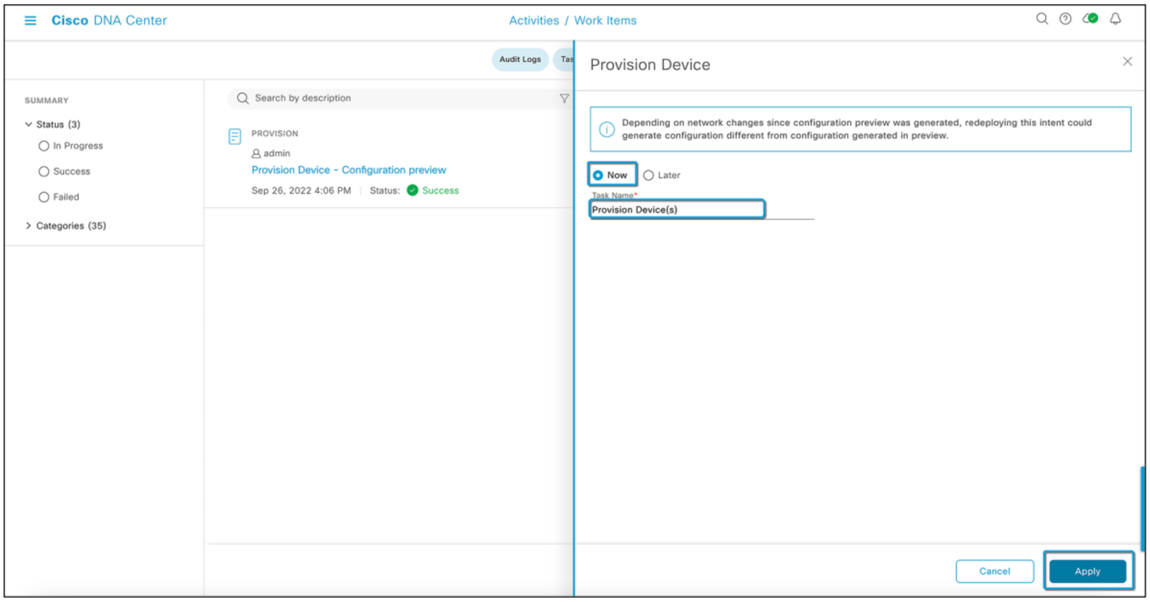
Device IP : 172.20.228.104

```
<apf-cfg-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-apf-cfg" >
<apf>
<tri-radio-mode>true</tri-radio-mode>
</apf>
</apf-cfg-data>
<dot11-cfg-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-dot11-cfg" >
<configured-countries nc:operation= "replace" >
<configured-country>
<country-code><![CDATA[us]]></country-code>
</configured-country>
</configured-countries>
</dot11-cfg-data>
<apf-cfg-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-apf-cfg" >
<apf>
<dot11-country-code><![CDATA[US]]></dot11-country-code>
</apf>
</apf-cfg-data>
<dot11-cfg-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-dot11-cfg" >
<dot11-entries>
<dot11-entry>
<band>dot11-2-dot-4-ghz-band</band>
<apf-network-state>true</apf-network-state>
</dot11-entry>
</dot11-entries>
</dot11-cfg-data>
<dot11-cfg-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-dot11-cfg" >
<dot11-entries>
<dot11-entry>
<band>dot11-5-ghz-band</band>
<apf-network-state>true</apf-network-state>
</dot11-entry>
</dot11-entries>
</dot11-cfg-data>
```

Figure 85.
CLI preview of the Catalyst 9800 configurations

Step 11: Choose when to deploy the device

- To deploy the device immediately, click the **Now** button, and then click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.



PROVISION
admin
Provision Device - Configuration preview
Sep 26, 2022 4:06 PM | Status: ✓ Success

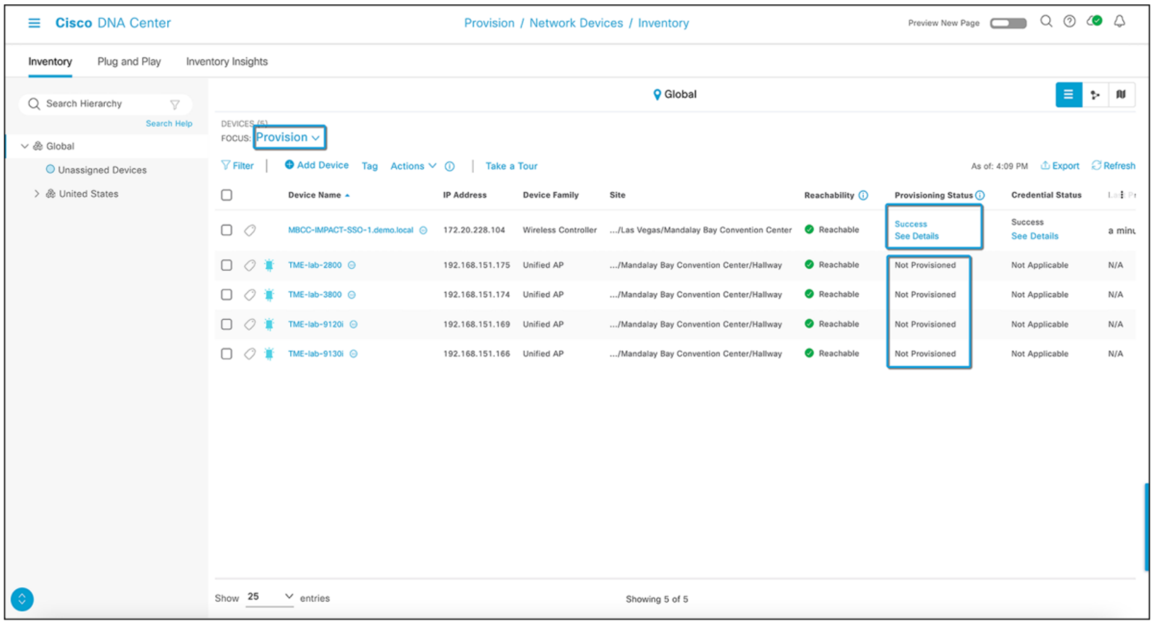
Depending on network changes since configuration preview was generated, redeploying this intent could generate configuration different from configuration generated in preview.

● Now ○ Later

Task Name*: Provision Device(s)

Figure 86.
Provisioning the Catalyst 9800 wireless controller

Change the Focus to Provision in the Inventory window and select the site you wish to see the status for. The Provisioning Status column displays the device's current status. In this example, the Catalyst 9800 wireless controller with AI-Enhanced RRM controller has already been provisioned.



DEVICES (5)
FOCUS: Provision

As of: 4:09 PM

Device Name	IP Address	Device Family	Site	Reachability	Provisioning Status	Credential Status	La Pr
MBCC-IMPACT-SSO-1.demo.local	172.20.228.104	Wireless Controller	.../Las Vegas/Mandalay Bay Convention Center	Reachable	Success See Details	Success See Details	a minu
TME-lab-2800	192.168.151.175	Unified AP	.../Mandalay Bay Convention Center/Hallway	Reachable	Not Provisioned	Not Applicable	N/A
TME-lab-3800	192.168.151.174	Unified AP	.../Mandalay Bay Convention Center/Hallway	Reachable	Not Provisioned	Not Applicable	N/A
TME-lab-9120i	192.168.151.169	Unified AP	.../Mandalay Bay Convention Center/Hallway	Reachable	Not Provisioned	Not Applicable	N/A
TME-lab-9130i	192.168.151.166	Unified AP	.../Mandalay Bay Convention Center/Hallway	Reachable	Not Provisioned	Not Applicable	N/A

Show 25 entries

Showing 5 of 5

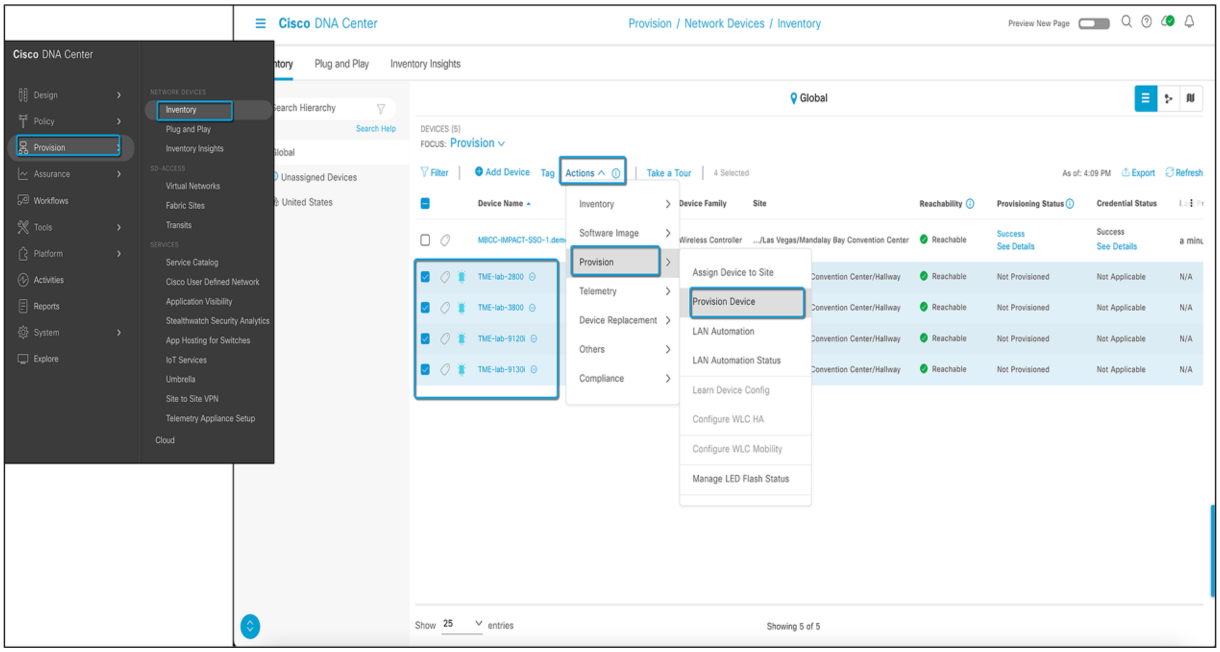
Figure 87.
Catalyst 9800 wireless controller Provisioning status in the Inventory window

Step 12: Provision wireless access points

- Click the hamburger menu icon (☰) and choose Provision > Network Devices > Inventory.
- The Inventory window displays the device information gathered during the discovery process.
- Select the checkbox next to the AP(s) that you want to provision.
- From the Actions drop-down list, choose Provision > Provision Device.

Note: You can either search for a site by entering its name or expand Global to select the site. Devices that are available in the selected site are displayed in the Inventory window.

To filter the devices based on various criteria, such as device family or reachability status, click **Filter**, make your selections, and then click **Apply**.



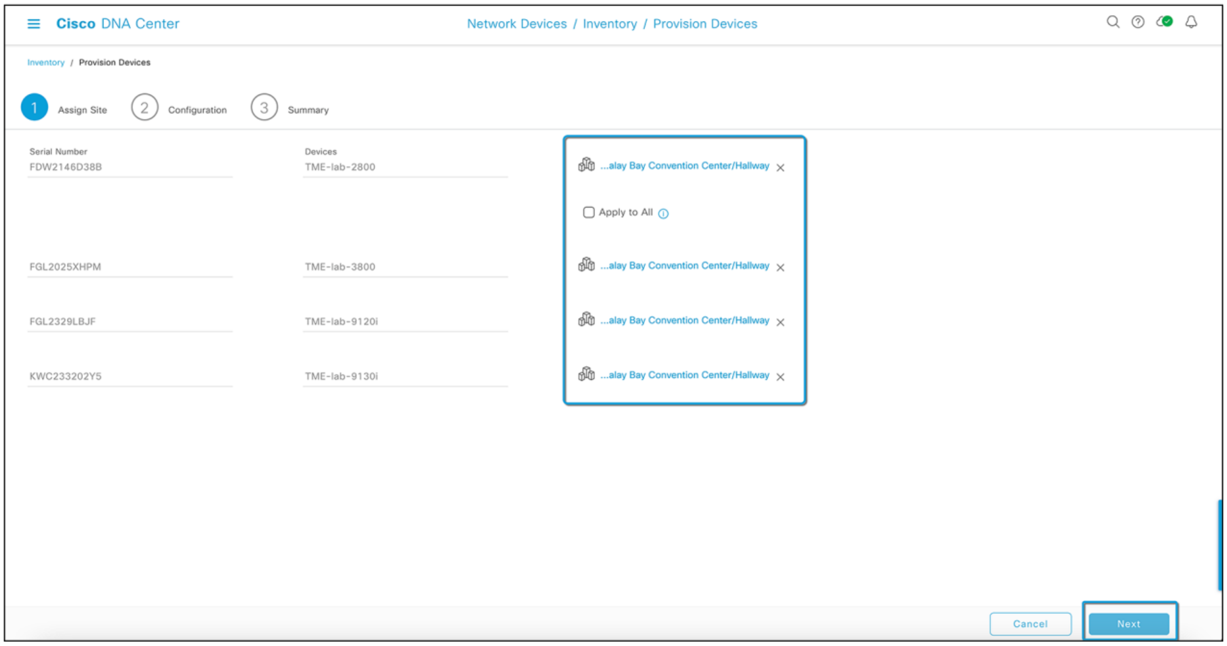
	Device Name	Device Family	Site	Reachability	Provisioning Status	Credential Status	
□	MBCC-IMPACT-SSO-1.dem	Wireless Controller	.../Las Vegas/Mandalay Bay Convention Center	Reachable	Success See Details	Success See Details	a minu
☑	TME-lab-2800		Convention Center/Hallway	Reachable	Not Provisioned	Not Applicable	N/A
☑	TME-lab-3800		Convention Center/Hallway	Reachable	Not Provisioned	Not Applicable	N/A
☑	TME-lab-9120i		Convention Center/Hallway	Reachable	Not Provisioned	Not Applicable	N/A
☑	TME-lab-9130i		Convention Center/Hallway	Reachable	Not Provisioned	Not Applicable	N/A

Figure 88.
Provisioning wireless access points

Step 13: Assign sites

In the Assign Site step, configure the following parameters:

- Click **Choose a floor** and assign an AP to the site.
- In the Choose a Floor slide-in pane, select the floor where the AP resides, and click **Save**.
- Click **Next**.

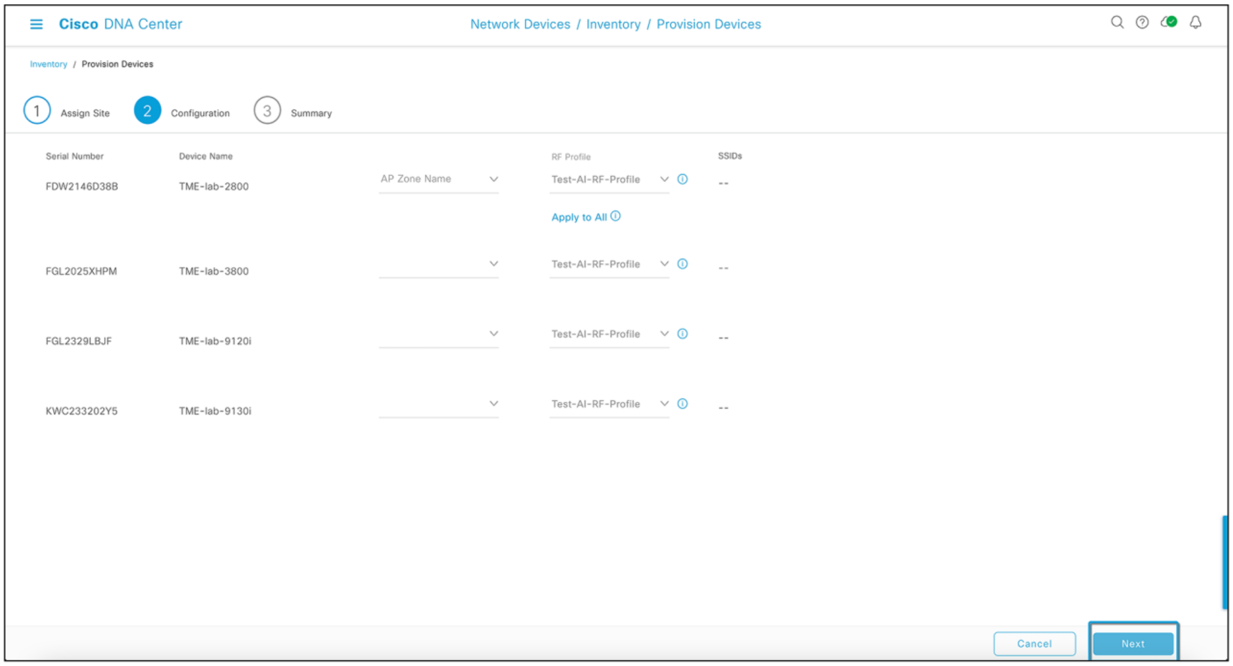

Cisco DNA Center
Network Devices / Inventory / Provision Devices
Inventory / Provision Devices
1 Assign Site
2 Configuration
3 Summary
Cancel
Next

Serial Number	Devices	
FDW2146D38B	TME-lab-2800	...alay Bay Convention Center/Hallway □ Apply to All
FGL2025XHPM	TME-lab-3800	...alay Bay Convention Center/Hallway
FGL2329LBJF	TME-lab-9120i	...alay Bay Convention Center/Hallway
KWC233202Y5	TME-lab-9130i	...alay Bay Convention Center/Hallway

Figure 89.
Assigning floors on sites to wireless access points

Step 14: Configuration

On the Configuration page, RF profile and AP zone names are selected. As we have already assigned an AI RF profile for the site and have no AP zones defined in the network profile, these values are grayed out here. Click **Next**.

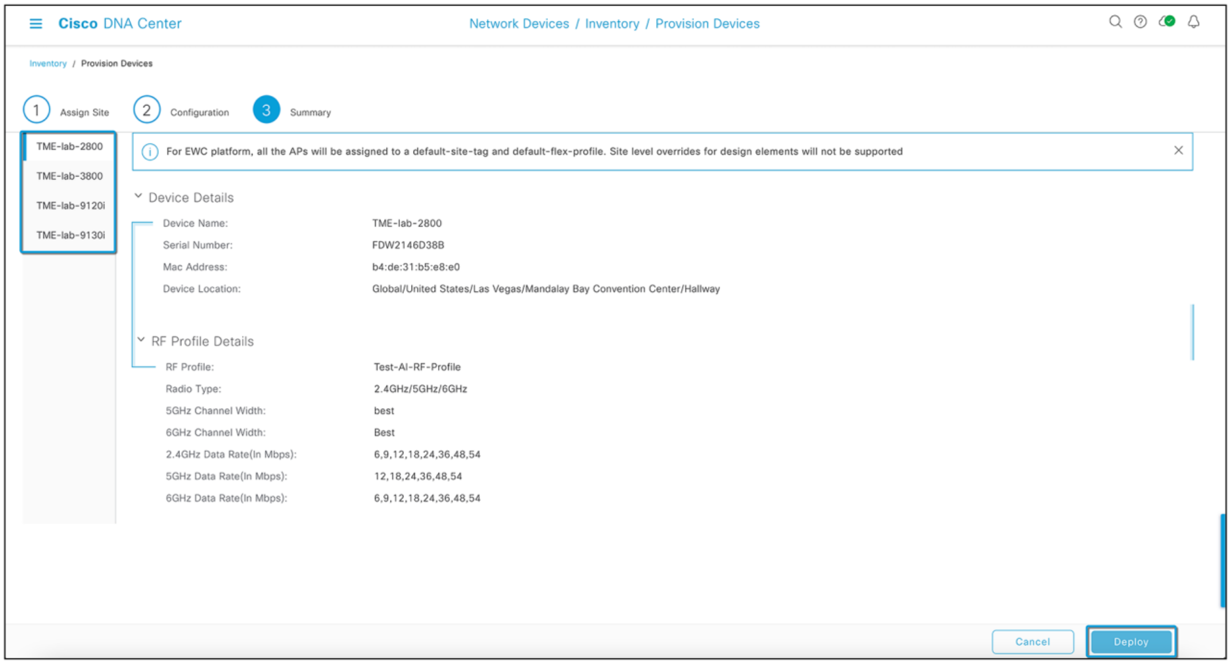

Cisco DNA Center
Network Devices / Inventory / Provision Devices
Inventory / Provision Devices
1 Assign Site
2 Configuration
3 Summary
Cancel
Next

Serial Number	Device Name	AP Zone Name	RF Profile	SSIDs
FDW2146D38B	TME-lab-2800	AP Zone Name	Test-AI-RF-Profile Apply to All	--
FGL2025XHPM	TME-lab-3800		Test-AI-RF-Profile	--
FGL2329LBJF	TME-lab-9120i		Test-AI-RF-Profile	--
KWC233202Y5	TME-lab-9130i		Test-AI-RF-Profile	--

Figure 90.
Wireless access point configurations while provisioning

Step 15: Review and validate the summary

In the Summary step, review the device details and click **Deploy** to provision the AP. The Provision Device slide-in pane appears. It shows the RF profile being assigned to the wireless access points.



For EWC platform, all the APs will be assigned to a default-site-tag and default-flex-profile. Site level overrides for design elements will not be supported

Device Details

Device Name:	TME-lab-2800
Serial Number:	FDW2146D38B
Mac Address:	b4:de:31:b5:e8:e0
Device Location:	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway

RF Profile Details

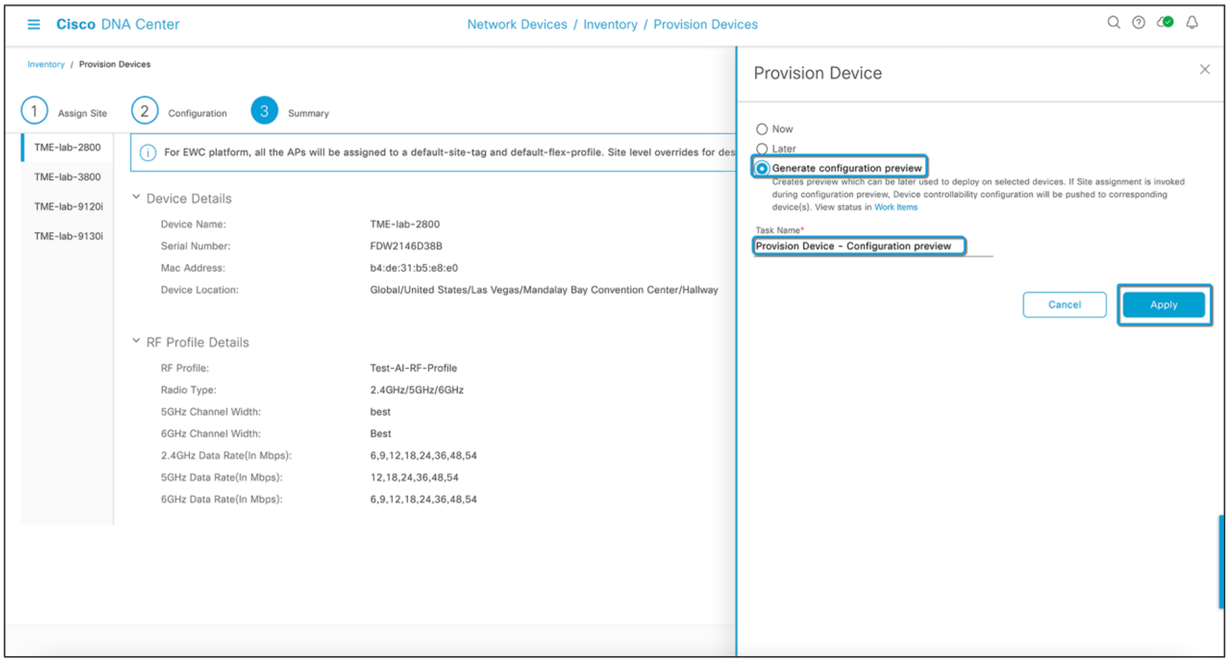
RF Profile:	Test-AI-RF-Profile
Radio Type:	2.4GHz/5GHz/6GHz
5GHz Channel Width:	best
6GHz Channel Width:	Best
2.4GHz Data Rate(In Mbps):	6,9,12,18,24,36,48,54
5GHz Data Rate(In Mbps):	12,18,24,36,48,54
6GHz Data Rate(In Mbps):	6,9,12,18,24,36,48,54

Figure 91.
Wireless access point provisioning summary

Step 16: Choose when to deploy

In the Provision Device slide-in pane, do the following:

- To immediately deploy the device, click the **Now** button, and then click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** button and define the date and time of the deployment.
- To preview the CLI configuration, click the **Generate Configuration Preview** button (Figure 92).



For EWC platform, all the APs will be assigned to a default-site-tag and default-flex-profile. Site level overrides for des

Device Details

Device Name:	TME-lab-2800
Serial Number:	FDW2146D38B
Mac Address:	b4:de:31:b5:e8:e0
Device Location:	Global/United States/Las Vegas/Mandalay Bay Convention Center/Hallway

RF Profile Details

RF Profile:	Test-AI-RF-Profile
Radio Type:	2.4GHz/5GHz/6GHz
5GHz Channel Width:	best
6GHz Channel Width:	Best
2.4GHz Data Rate(In Mbps):	6,9,12,18,24,36,48,54
5GHz Data Rate(In Mbps):	12,18,24,36,48,54
6GHz Data Rate(In Mbps):	6,9,12,18,24,36,48,54

Provision Device

○ Now

○ Later

● Generate configuration preview

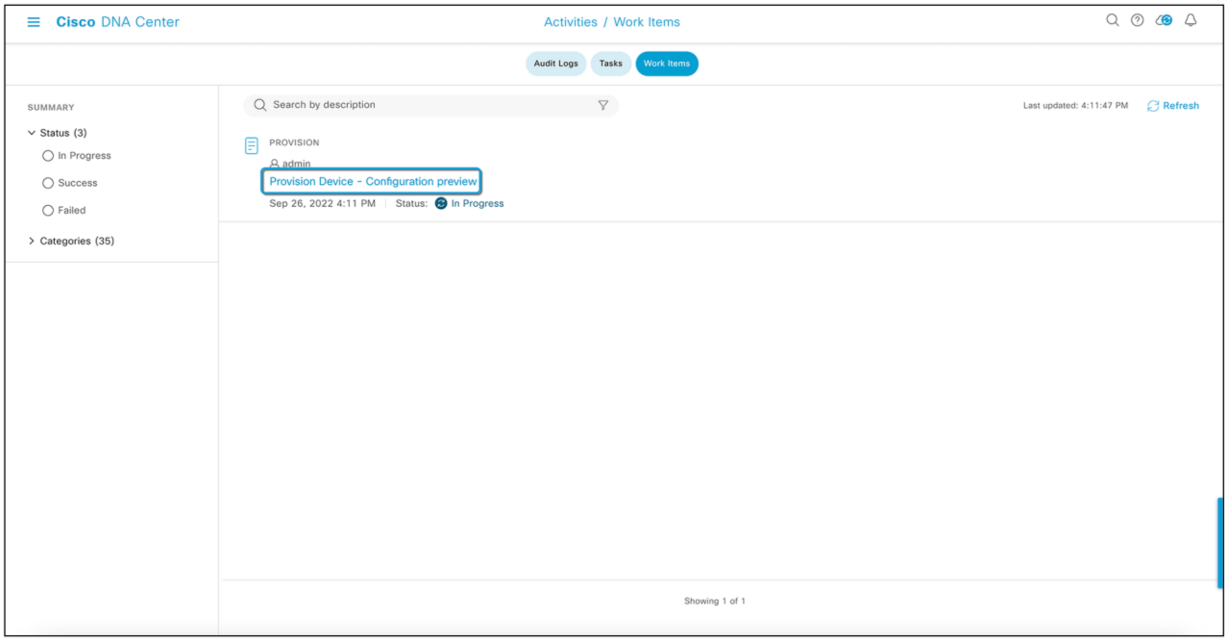
Creates preview which can be later used to deploy on selected devices. If Site assignment is invoked during configuration preview, Device controllability configuration will be pushed to corresponding device(s). View status in Work Items

Task Name*: Provision Device - Configuration preview

Figure 92.
Generating a configuration preview for access point provisioning

Step 17: Monitor the task

In the Task Submitted pop-up, click the hamburger menu icon (☰) and choose Activities > Work Items. In the Work Items window, click the CLI preview task for which you submitted the configuration preview request.



Last updated: 4:11:47 PM

PROVISION

admin

Provision Device - Configuration preview

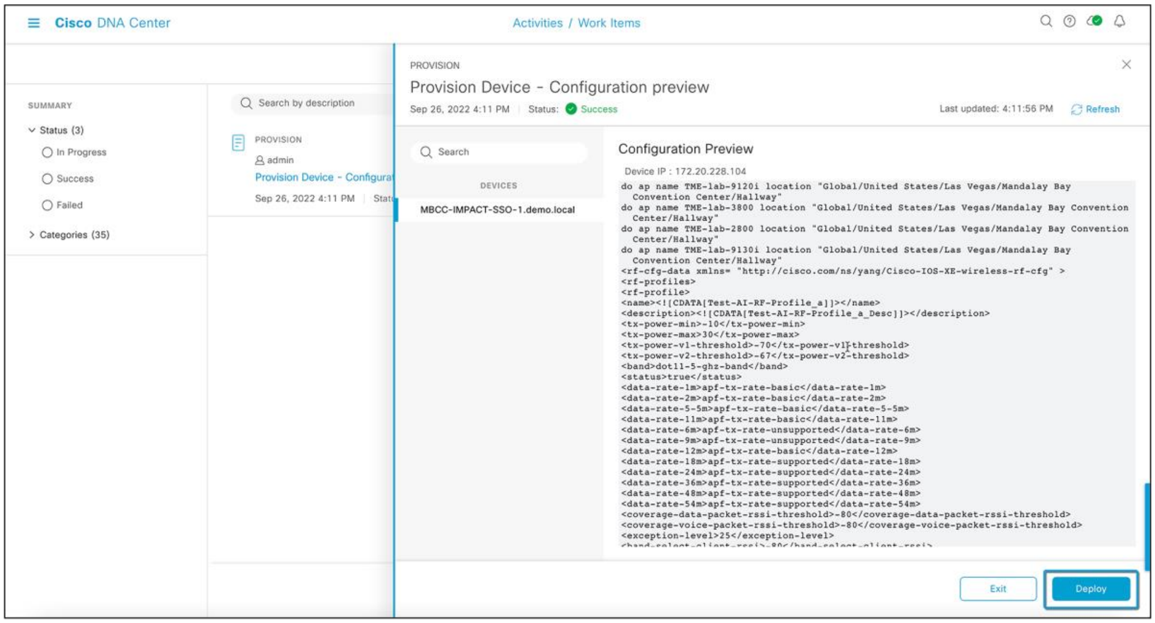
Sep 26, 2022 4:11 PM | Status: In Progress

Showing 1 of 1

Figure 93.
Access point provisioning CLI preview in Work Items

Step 18: Deploy

View the CLI configuration details and click **Deploy**.



Provision Device - Configuration preview

Sep 26, 2022 4:11 PM | Status: Success

Last updated: 4:11:56 PM Refresh

Configuration Preview

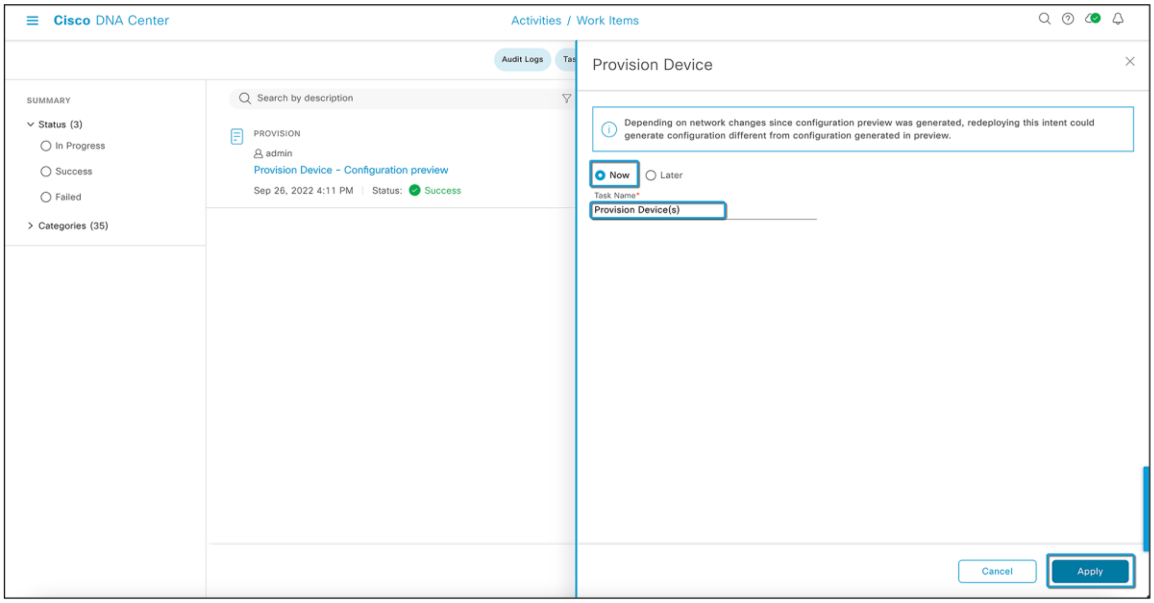
Device IP : 172.20.228.104

```
do ap name TME-lab-9120i location "Global/United States/Las Vegas/Mandalay Bay
  Convention Center/Hallway"
do ap name TME-lab-3800 location "Global/United States/Las Vegas/Mandalay Bay Convention
  Center/Hallway"
do ap name TME-lab-2800 location "Global/United States/Las Vegas/Mandalay Bay Convention
  Center/Hallway"
do ap name TME-lab-9130i location "Global/United States/Las Vegas/Mandalay Bay
  Convention Center/Hallway"
<rf-cfg-data xmlns= "http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-rf-cfg" >
<rf-profiles>
<rf-profile>
<name><![CDATA[Test-AI-RF-Profile_a]]></name>
<description><![CDATA[Test-AI-RF-Profile_a_Desc]]></description>
<tx-power-min>-10</tx-power-min>
<tx-power-max>30</tx-power-max>
<tx-power-v1-threshold>-70</tx-power-v1-threshold>
<tx-power-v2-threshold>-67</tx-power-v2-threshold>
<band>dot11-5-ghz-band</band>
<status>true</status>
<data-rate-1m>apf-tx-rate-basic</data-rate-1m>
<data-rate-2m>apf-tx-rate-basic</data-rate-2m>
<data-rate-5-5m>apf-tx-rate-basic</data-rate-5-5m>
<data-rate-11m>apf-tx-rate-basic</data-rate-11m>
<data-rate-6m>apf-tx-rate-unsupported</data-rate-6m>
<data-rate-9m>apf-tx-rate-unsupported</data-rate-9m>
<data-rate-12m>apf-tx-rate-basic</data-rate-12m>
<data-rate-18m>apf-tx-rate-supported</data-rate-18m>
<data-rate-24m>apf-tx-rate-supported</data-rate-24m>
<data-rate-36m>apf-tx-rate-supported</data-rate-36m>
<data-rate-48m>apf-tx-rate-supported</data-rate-48m>
<data-rate-54m>apf-tx-rate-supported</data-rate-54m>
<coverage-data-packet-rssi-threshold>-80</coverage-data-packet-rssi-threshold>
<coverage-voice-packet-rssi-threshold>-80</coverage-voice-packet-rssi-threshold>
<exception-level>25</exception-level>
<band-select-client-rssi>-80</band-select-client-rssi>
```

Figure 94.
Reviewing the CLI preview of access point provisioning

Step 19: Choose when to deploy

- To immediately deploy the device, click the **Now** button, and then click **Apply**.
- To schedule the device deployment for a later date and time, click the Later button and define the date and time of the deployment.



Provision Device

Depending on network changes since configuration preview was generated, redeploying this intent could generate configuration different from configuration generated in preview.

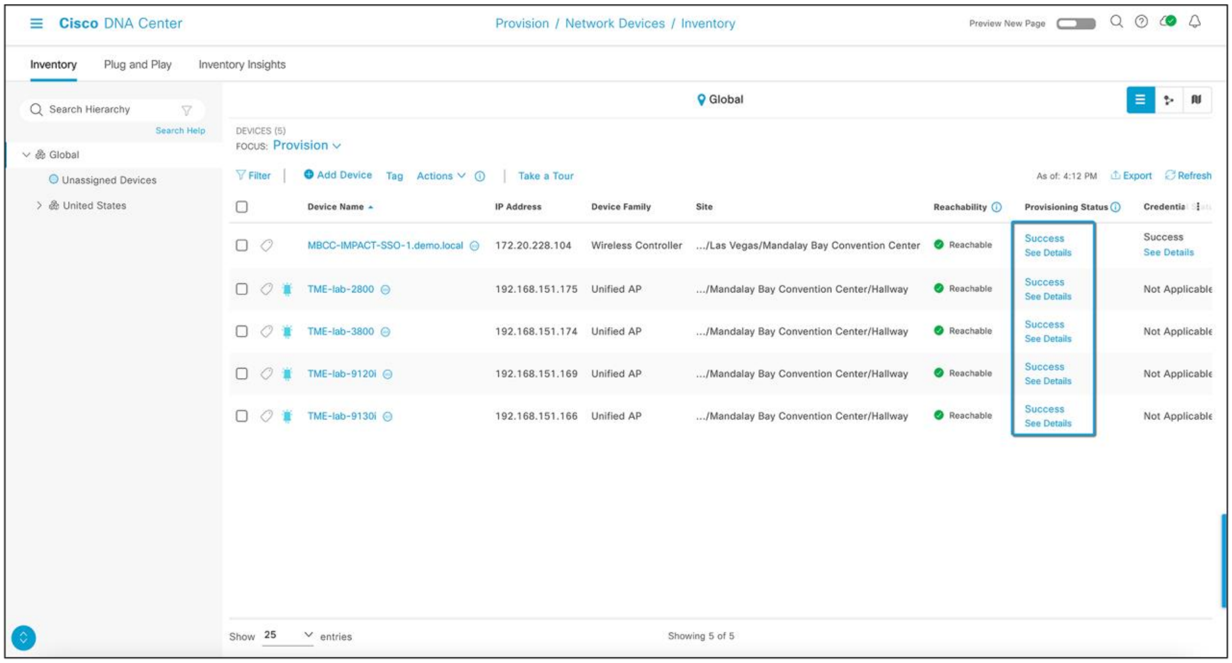
● Now ○ Later

Task Name*: Provision Device(s)

Figure 95.
Provisioning a wireless access point

Step 20: Verify the provisioning status

Change the Focus to Provision in the Inventory window and select the site you wish to see the status for. The Provisioning Status column displays the device's current status. In this example, the Catalyst 9800 wireless controller and wireless access points with AI-Enhanced RRM controller have already been provisioned.



DEVICES (5)
FOCUS: Provision

As of: 4:12 PM

☐	Device Name	IP Address	Device Family	Site	Reachability	Provisioning Status	Credentia
☐	MBCC-IMPACT-SSO-1.demo.local	172.20.228.104	Wireless Controller	.../Las Vegas/Mandalay Bay Convention Center	Reachable	Success See Details	Success See Details
☐	TME-lab-2800	192.168.151.175	Unified AP	.../Mandalay Bay Convention Center/Hallway	Reachable	Success See Details	Not Applicable
☐	TME-lab-3800	192.168.151.174	Unified AP	.../Mandalay Bay Convention Center/Hallway	Reachable	Success See Details	Not Applicable
☐	TME-lab-9120i	192.168.151.169	Unified AP	.../Mandalay Bay Convention Center/Hallway	Reachable	Success See Details	Not Applicable
☐	TME-lab-9130i	192.168.151.166	Unified AP	.../Mandalay Bay Convention Center/Hallway	Reachable	Success See Details	Not Applicable

Show 25 entries

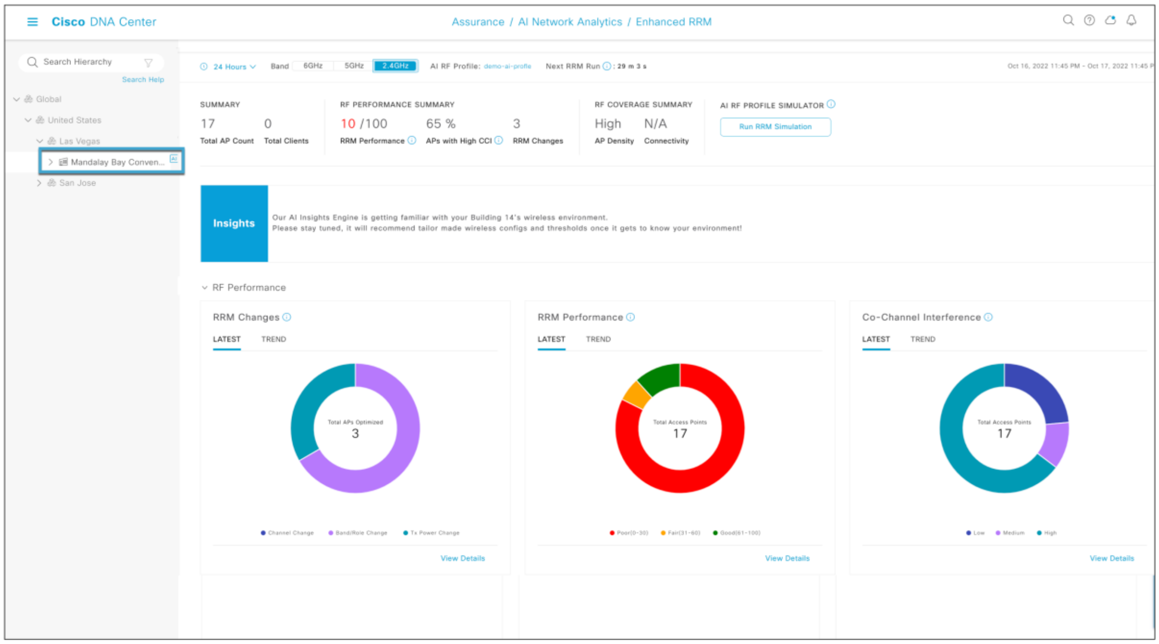
Showing 5 of 5

Figure 96.
Successful access point provisioning

Part 7: Verify the AI-Enhanced RRM deployment

Cisco DNA Center verification

Go to the Enhanced RRM page and select the site with the AI RF profile. The AI-Enhanced RRM controller should be up and should be collecting data from the controller and access points.



24 Hours | Band: 6GHz 5GHz **2.4GHz** | AI RF Profile: demo-ai-profile | Next RRM Run: 29 m 3 s | Oct 16, 2022 11:45 PM - Oct 17, 2022 11:45 P

SUMMARY		RF PERFORMANCE SUMMARY			RF COVERAGE SUMMARY	
17	0	10 /100	65 %	3	High	N/A
Total AP Count	Total Clients	RRM Performance	APs with High CCI	RRM Changes	AP Density	Connectivity

AI RF PROFILE SIMULATOR: Run RRM Simulation

Insights: Our AI Insights Engine is getting familiar with your Building 14's wireless environment.
Please stay tuned, it will recommend tailor made wireless configs and thresholds once it gets to know your environment!

RF Performance

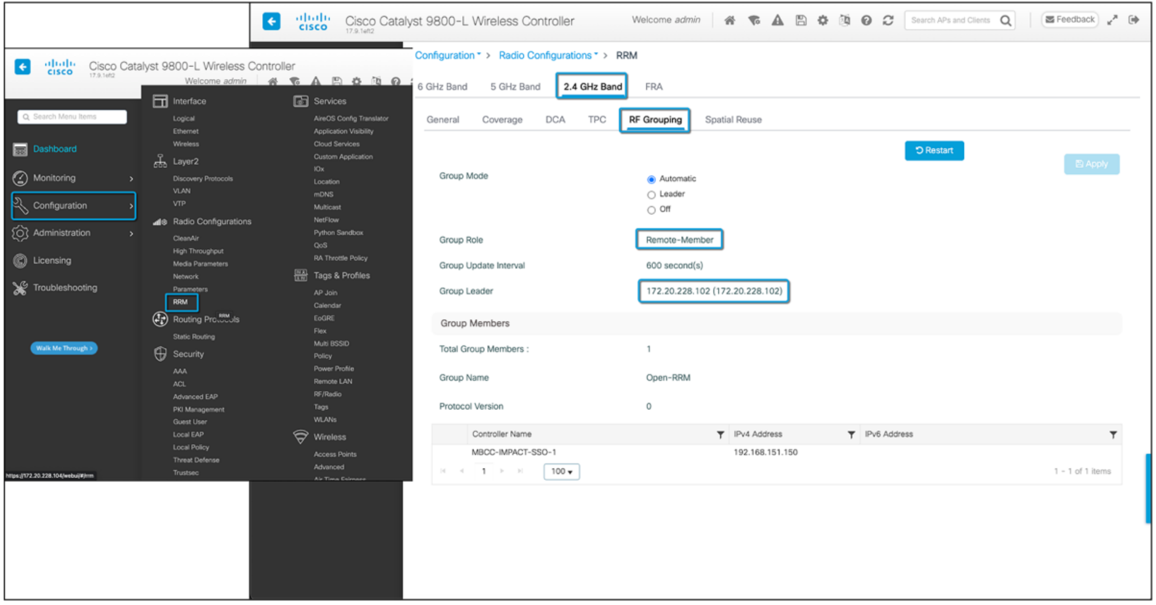
Figure 97.
AI-Enhanced RRM control center

Catalyst 9800 wireless controller verification

Step 1: Verify the RRM group leader

On the Catalyst 9800 controller, go to Configuration > RRM > 6 GHz, 5 GHz, or 2.4 GHz Band > RF Grouping.

- The Group Role should be Remote-Member.
- The Group Leader should be the Cisco DNA Center's IP address.



Configuration > Radio Configurations > RRM

6 GHz Band | 5 GHz Band | **2.4 GHz Band** | FRA

General | Coverage | DCA | TPC | **RF Grouping** | Spatial Reuse

Restart | Apply

Group Mode: ● Automatic ○ Leader ○ Off

Group Role: Remote-Member

Group Update Interval: 600 second(s)

Group Leader: 172.20.228.102 (172.20.228.102)

Group Members

Total Group Members : 1

Group Name: Open-RRM

Protocol Version: 0

Controller Name	IPv4 Address	IPv6 Address
MBCC-IMPACT-SSO-1	192.168.151.150	

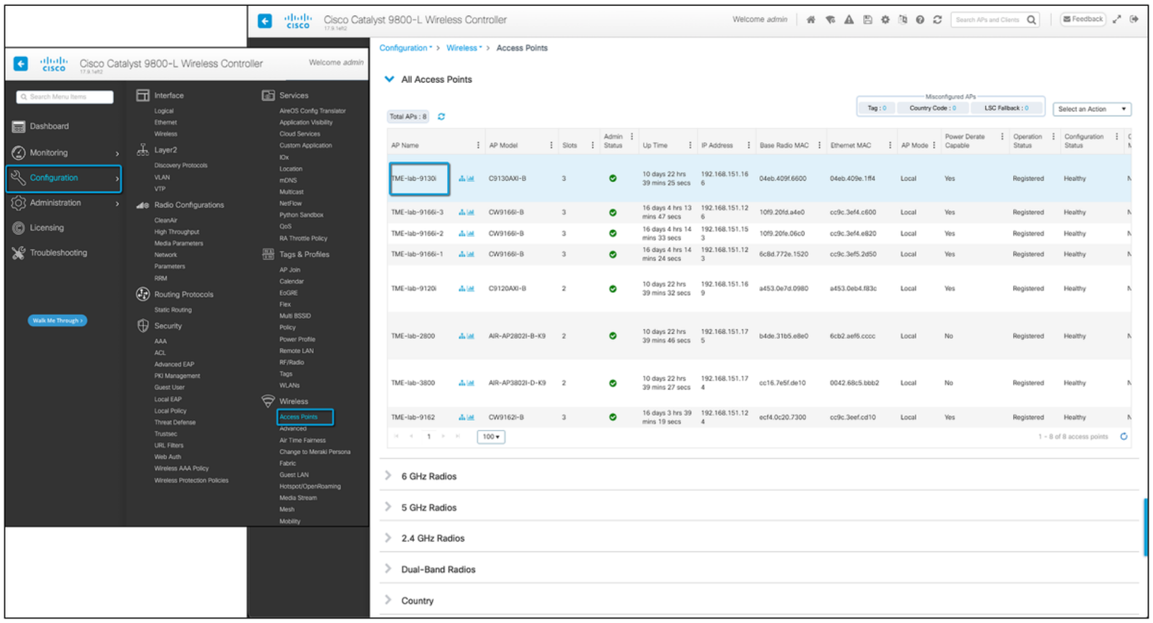
1 | 100 | 1 - 1 of 1 items

Figure 98.
Verifying the RF group leader

Step 2: Verify the AI-RF profile assigned to the access points

Go to Configuration > Access Points > Client on an access point that is part of the AI RF profile.

- The Tags section in the top right should have the AI RF profile in the RF tag.
- Any new policy/site tags created by Cisco DNA Center will be seen here.



Configuration > Wireless > Access Points

All Access Points

Total APs : 8

Misconfigured APs: Tag : 0 | Country Code : 0 | LSC Fallback : 0 | Select an Action

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Configuration Status
TME-lab-9130i	C9130AXI-B	3	✓	10 days 22 hrs 39 mins 25 secs	192.168.151.166	04eb.409f.6600	04eb.409e.1ff4	Local	Yes	Registered	Healthy
TME-lab-9166i-3	CW9166I-B	3	✓	16 days 4 hrs 13 mins 47 secs	192.168.151.126	10f9.20fd.a4e0	cc9c.3ef4.c600	Local	Yes	Registered	Healthy
TME-lab-9166i-2	CW9166I-B	3	✓	16 days 4 hrs 14 mins 33 secs	192.168.151.153	10f9.20fe.06c0	cc9c.3ef4.e820	Local	Yes	Registered	Healthy
TME-lab-9166i-1	CW9166I-B	3	✓	16 days 4 hrs 14 mins 24 secs	192.168.151.123	6c8d.772e.1520	cc9c.3ef5.2d50	Local	Yes	Registered	Healthy
TME-lab-9120i	C9120AXI-B	2	✓	10 days 22 hrs 39 mins 32 secs	192.168.151.169	a453.0e7d.0980	a453.0eb4.f83c	Local	Yes	Registered	Healthy
TME-lab-2800	AIR-AP2802I-B-K9	2	✓	10 days 22 hrs 39 mins 46 secs	192.168.151.175	b4de.31b5.e8e0	6cb2.aef6.cccc	Local	No	Registered	Healthy
TME-lab-3800	AIR-AP3802I-D-K9	2	✓	10 days 22 hrs 39 mins 27 secs	192.168.151.174	cc16.7e5f.de10	0042.68c5.bbb2	Local	No	Registered	Healthy
TME-lab-9162	CW9162I-B	3	✓	16 days 3 hrs 39 mins 19 secs	192.168.151.124	ecf4.0c20.7300	cc9c.3eef.cd10	Local	Yes	Registered	Healthy

1 - 8 of 8 access points

6 GHz Radios

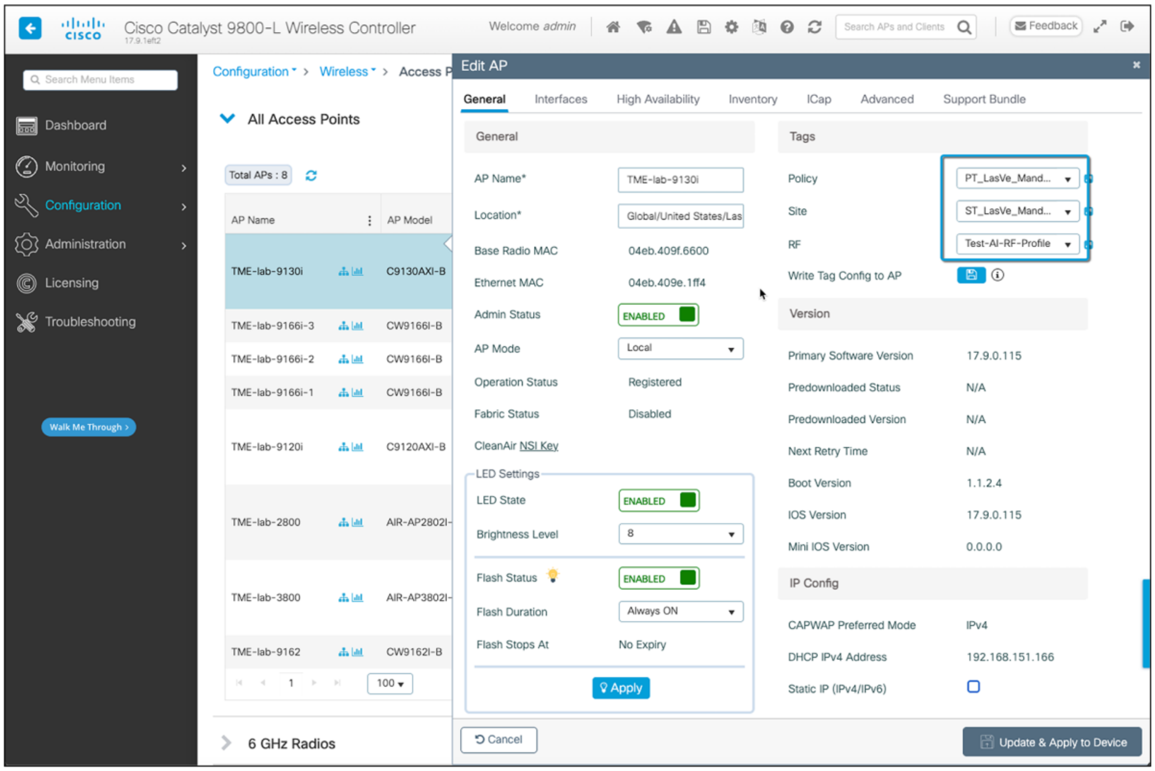
5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

Figure 99.
Navigating to access points



Configuration > Wireless > Access P

All Access Points

Total APs : 8

AP Name	AP Model
TME-lab-9130i	C9130AXI-B
TME-lab-9166i-3	CW9166I-B
TME-lab-9166i-2	CW9166I-B
TME-lab-9166i-1	CW9166I-B
TME-lab-9120i	C9120AXI-B
TME-lab-2800	AIR-AP2802I-
TME-lab-3800	AIR-AP3802I-
TME-lab-9162	CW9162I-B

6 GHz Radios

Edit AP

General

AP Name*	TME-lab-9130i
Location*	Global/United States/Las
Base Radio MAC	04eb.409f.6600
Ethernet MAC	04eb.409e.1ff4
Admin Status	ENABLED
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled
CleanAir NSI Key	

LED Settings

LED State	ENABLED
Brightness Level	8
Flash Status	ENABLED
Flash Duration	Always ON
Flash Stops At	No Expiry

Tags

Policy	PT_LasVe_Mand...
Site	ST_LasVe_Mand...
RF	Test-AI-RF-Profile
Write Tag Config to AP	

Version

Primary Software Version	17.9.0.115
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	17.9.0.115
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv4
DHCP IPv4 Address	192.168.151.166
Static IP (IPv4/IPv6)	□

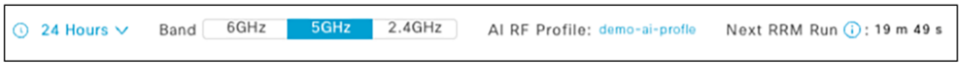
Figure 100.
Cisco DNA Center-created configurations on the Catalyst 9800 wireless controller post-provisioning

Day-1 AI-Enhanced RRM features and use cases

The heart of the AI-Enhanced RRM management is the RRM control center, where information regarding the current (Latest) and Trend information regarding current actions and overall performance can be viewed.

Each element on the dashboard has tool tips that explain what it means or how it's measured.

At the top of the page are the focus selections. This sets the context for the information being displayed on the page. Selections for timespan are 24 hours, 7 days, or 14 days (the current maximum data period). The band selection (2.4, 5, or 6 GHz) and AI RF profile in use are also shown here.



24 Hours

Band: 6GHz | 5GHz | 2.4GHz

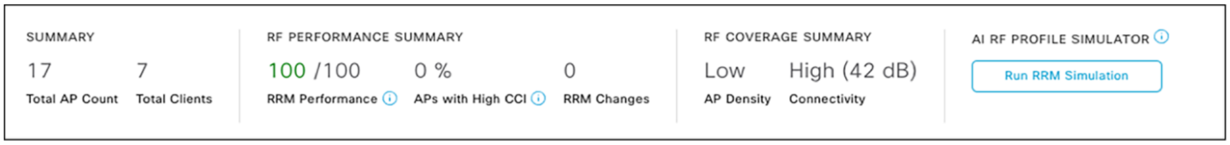
AI RF Profile: demo-ai-profle

Next RRM Run: 19 m 49 s

Figure 101.
Selecting the focus and context of the RRM control center

Hero bar and headlines

Below the focus selections are the headlines regarding the RF coverage and performance, which includes the overall RRM performance score (0 to 100, with 100 being excellent) as well as highlights such as the percentage of APs with high co-channel interference (CCI), and the count of RRM changes being made. The RRM coverage summary looks at the AP density (the number of AP neighbors seen at or above -70 dBm) and connectivity (the average client signal-to-noise ratio [SNR]).



SUMMARY
17 Total AP Count
7 Total Clients

RF PERFORMANCE SUMMARY
100 /100 RRM Performance
0 % APs with High CCI
0 RRM Changes

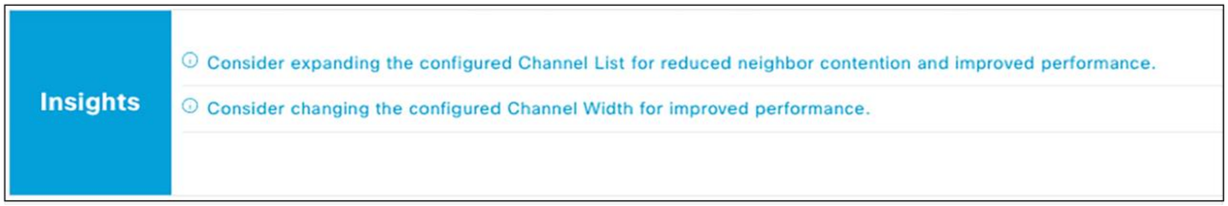
RF COVERAGE SUMMARY
Low AP Density
High (42 dB) Connectivity

AI RF PROFILE SIMULATOR

Figure 102.
The AI-Enhanced RRM "headlines"

Insights

One way that AI-Enhanced RRM truly distinguishes itself from Cisco's already powerful industry-leading RRM is the AI and ML components, along with the ability to store and use historical telemetry data and establish what is "normal" for a given observation over time. RRM on the controller has always been limited to viewing the current conditions, as the data storage requirements were quite high.



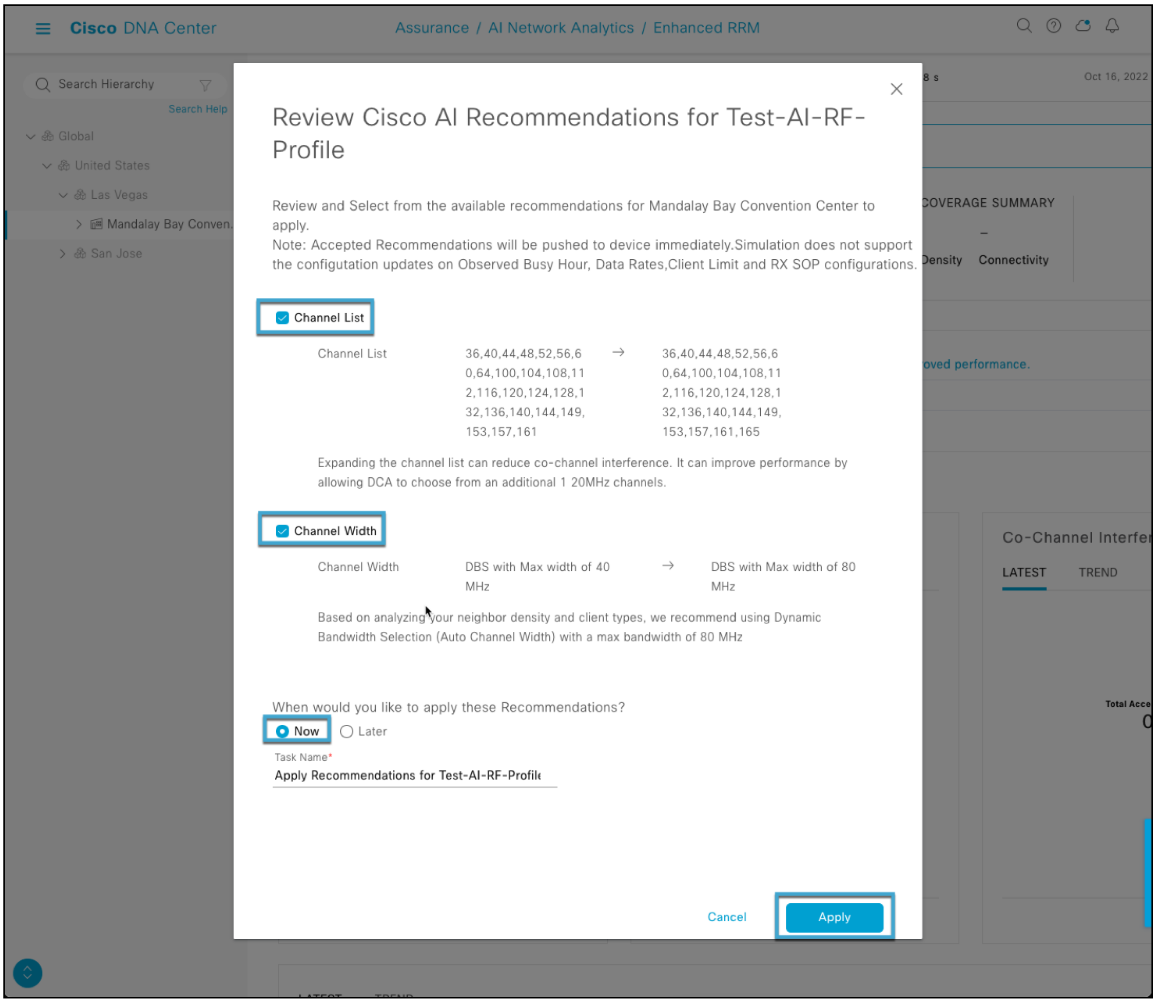
Insights

Consider expanding the configured Channel List for reduced neighbor contention and improved performance.

Consider changing the configured Channel Width for improved performance.

Figure 103.
AI-provided actionable insights into system performance and configuration

Insights displayed here may be blank initially but will populate after an initial week of learning. AI will look at multiple aspects of the configuration and measure against the performance. One example of learned data is the busy hour configuration initially set in the AI RF profile. The initial busy hour was configured when the AI RF profile was created and assigned. Over time, and with clients on the network, AI-Enhanced RRM observes when busy hours (when the network is under load) occur and may suggest an enhancement to the AI RF profile. Selecting the insight test will lead you to where the configuration can be changed. The administrator always has control of when to redeploy or assign the changed profile to the site. AI will provide insights on Tx power, channel bandwidth, DCA settings, AP density, SNR, etc.



Review Cisco AI Recommendations for Test-AI-RF-Profile

Review and Select from the available recommendations for Mandalay Bay Convention Center to apply.
Note: Accepted Recommendations will be pushed to device immediately.Simulation does not support the configutation updates on Observed Busy Hour, Data Rates,Client Limit and RX SOP configurations.

☑ Channel List

Channel List	36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161	→	36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161,165

Expanding the channel list can reduce co-channel interference. It can improve performance by allowing DCA to choose from an additional 1 20MHz channels.

☑ Channel Width

Channel Width	DBS with Max width of 40 MHz	→	DBS with Max width of 80 MHz

Based on analyzing your neighbor density and client types, we recommend using Dynamic Bandwidth Selection (Auto Channel Width) with a max bandwidth of 80 MHz

When would you like to apply these Recommendations?
● Now ○ Later

Task Name*
Apply Recommendations for Test-AI-RF-Profile

Figure 104.
Applying insights to the AI RF profile

Note: For busy hour insight to be generated, there will need to be a difference of at least five clients between the minimum and maximum number of clients – and there must be traffic on the network. Sleeping clients do not count.

In the next section, each of the performance metrics from the headlines is broken out into useful widgets, which let you explore the context of each down to the contributing radios and APs making up each component.

Note: The RF performance matrix will not show radios that are powered down or in power save mode.

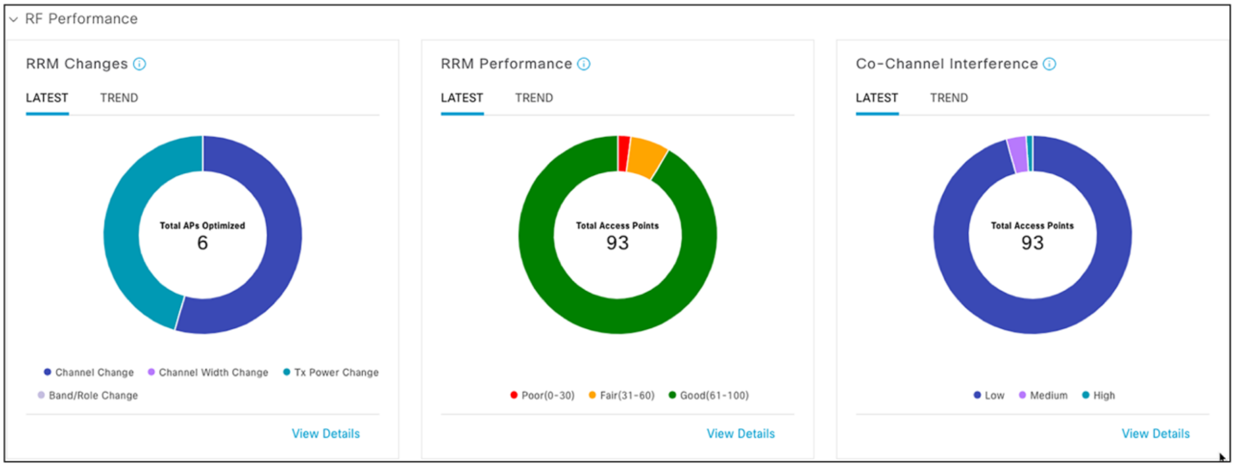


Figure 105.
AI-Enhanced RRM performance widgets

RRM Changes

In AI-Enhanced RRM, the Latest display always shows the current 30-minute AI-Enhanced RRM run period results. On a small network (this one has five APs total), there may not be any changes in the last reporting period so the display will show 0. Trend shows the full span for the currently selected time period (24 hours or 7 or 14 days) and allows the cursor to focus on a specific time in the chart to see how many of each kind of change were made. Selecting **View Details** further expands the selection to include the APs that were affected, and selecting an AP shows the actions that were taken in the RRM change made.

You can export the RRM changes into a CSV file for review.

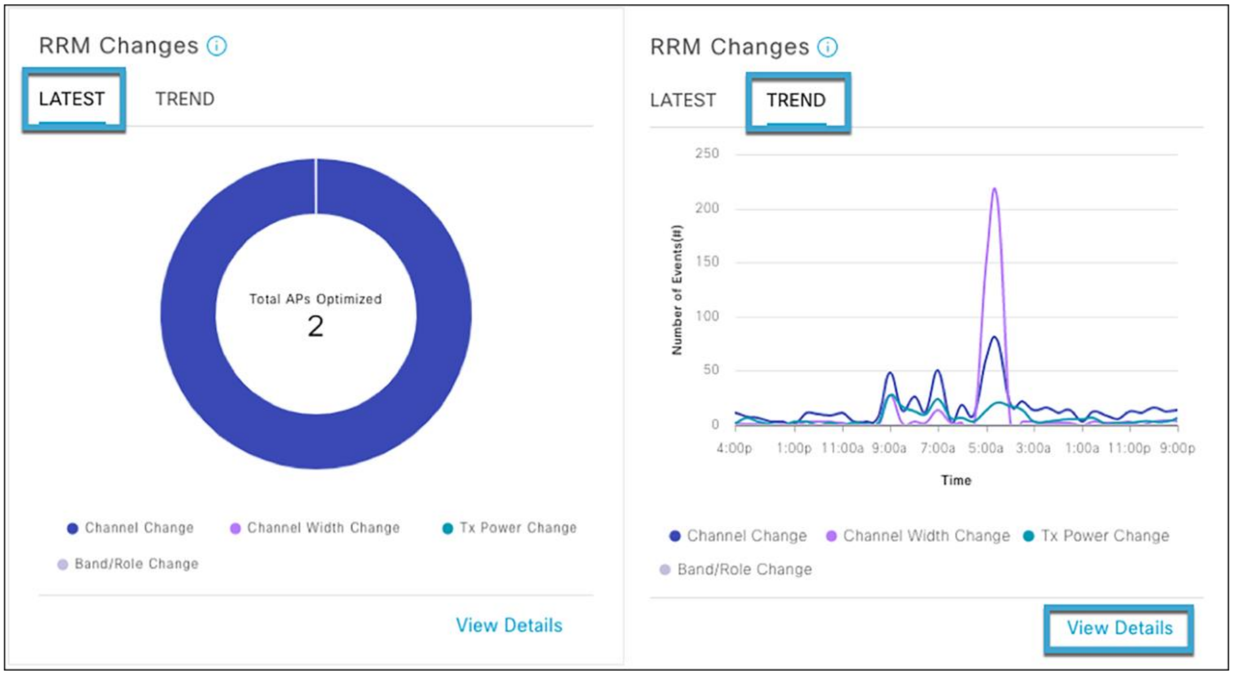
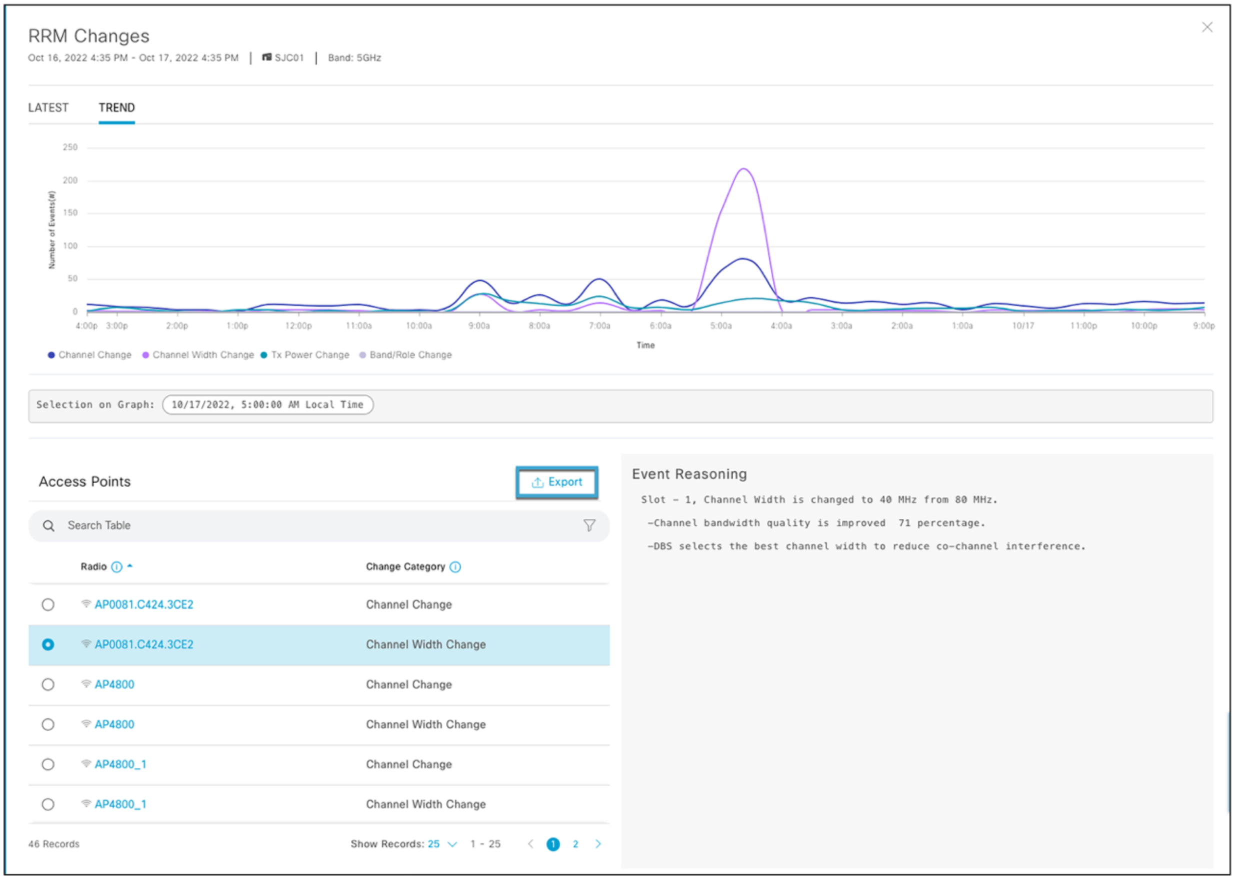


Figure 106.
RRM changes: Trend and detail views provide visibility into AI-Enhanced RRM's actions



RRM Changes

Oct 16, 2022 4:35 PM - Oct 17, 2022 4:35 PM | SJC01 | Band: 5GHz

LATEST TREND

Selection on Graph: 10/17/2022, 5:00:00 AM Local Time

Access Points

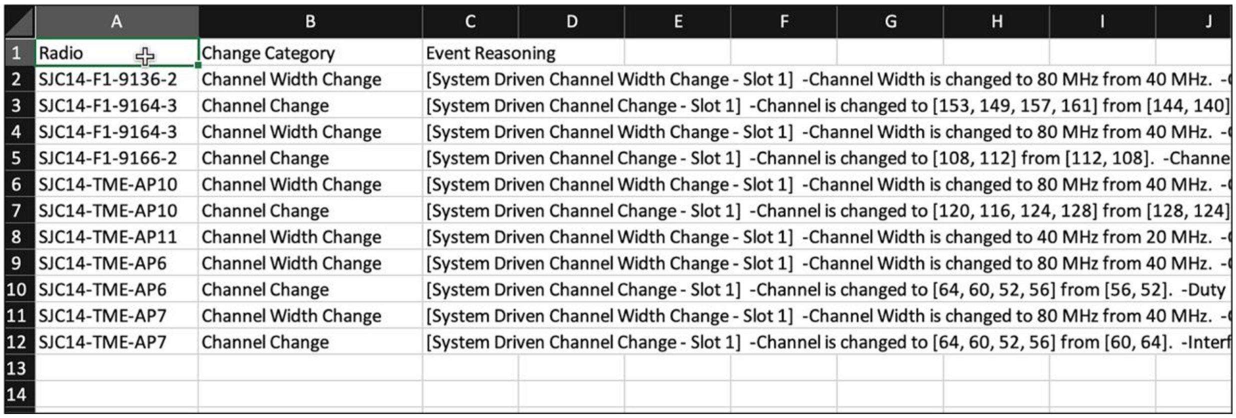
	Radio	Change Category
○	AP0081.C424.3CE2	Channel Change
●	AP0081.C424.3CE2	Channel Width Change
○	AP4800	Channel Change
○	AP4800	Channel Width Change
○	AP4800_1	Channel Change
○	AP4800_1	Channel Width Change

46 Records Show Records: 25 1 - 25 1 2

Event Reasoning

```
Slot - 1, Channel Width is changed to 40 MHz from 80 MHz.
 -Channel bandwidth quality is improved  71 percentage.
 -DBS selects the best channel width to reduce co-channel interference.
```

Figure 107.
Exporting RRM changes to a CSV file



	A	B	C
1	Radio	Change Category	Event Reasoning
2	SJC14-F1-9136-2	Channel Width Change	[System Driven Channel Width Change - Slot 1] -Channel Width is changed to 80 MHz from 40 MHz. -(
3	SJC14-F1-9164-3	Channel Change	[System Driven Channel Change - Slot 1] -Channel is changed to [153, 149, 157, 161] from [144, 140]
4	SJC14-F1-9164-3	Channel Width Change	[System Driven Channel Width Change - Slot 1] -Channel Width is changed to 80 MHz from 40 MHz. -(
5	SJC14-F1-9166-2	Channel Change	[System Driven Channel Change - Slot 1] -Channel is changed to [108, 112] from [112, 108]. -Channe
6	SJC14-TME-AP10	Channel Width Change	[System Driven Channel Width Change - Slot 1] -Channel Width is changed to 80 MHz from 40 MHz. -(
7	SJC14-TME-AP10	Channel Change	[System Driven Channel Change - Slot 1] -Channel is changed to [120, 116, 124, 128] from [128, 124]
8	SJC14-TME-AP11	Channel Width Change	[System Driven Channel Width Change - Slot 1] -Channel Width is changed to 40 MHz from 20 MHz. -(
9	SJC14-TME-AP6	Channel Width Change	[System Driven Channel Width Change - Slot 1] -Channel Width is changed to 80 MHz from 40 MHz. -(
10	SJC14-TME-AP6	Channel Change	[System Driven Channel Change - Slot 1] -Channel is changed to [64, 60, 52, 56] from [56, 52]. -Duty
11	SJC14-TME-AP7	Channel Width Change	[System Driven Channel Width Change - Slot 1] -Channel Width is changed to 80 MHz from 40 MHz. -(
12	SJC14-TME-AP7	Channel Change	[System Driven Channel Change - Slot 1] -Channel is changed to [64, 60, 52, 56] from [60, 64]. -Interf
13			
14			

Figure 108.
RRM changes in a CSV file

RRM Performance

RRM Performance tracks the performance score and how it changes over time. RRM Performance consists of multiple scores measuring co-channel interference, near-channel interference, and duty cycle. The default Latest view shows the results as of the last RRM run (30 minutes). Trend displays a trend line and transitions for all APs contributing to the scores and allows selection of a specific point in time. Selecting **View Details** shows all the APs included in the score at any point in time. Note the Export button, which will send any of the chart's data to a CSV file for download. Selecting any access point cross-links to the Device 360 view to further investigate the AP's history and behavior.

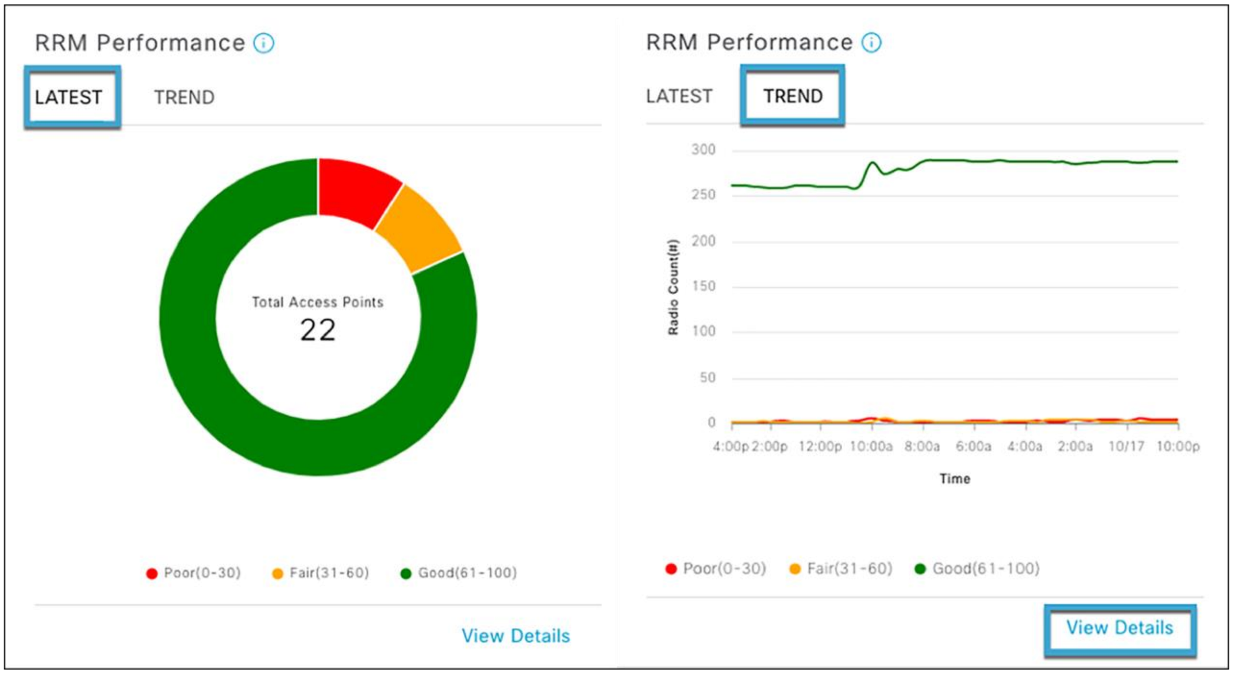
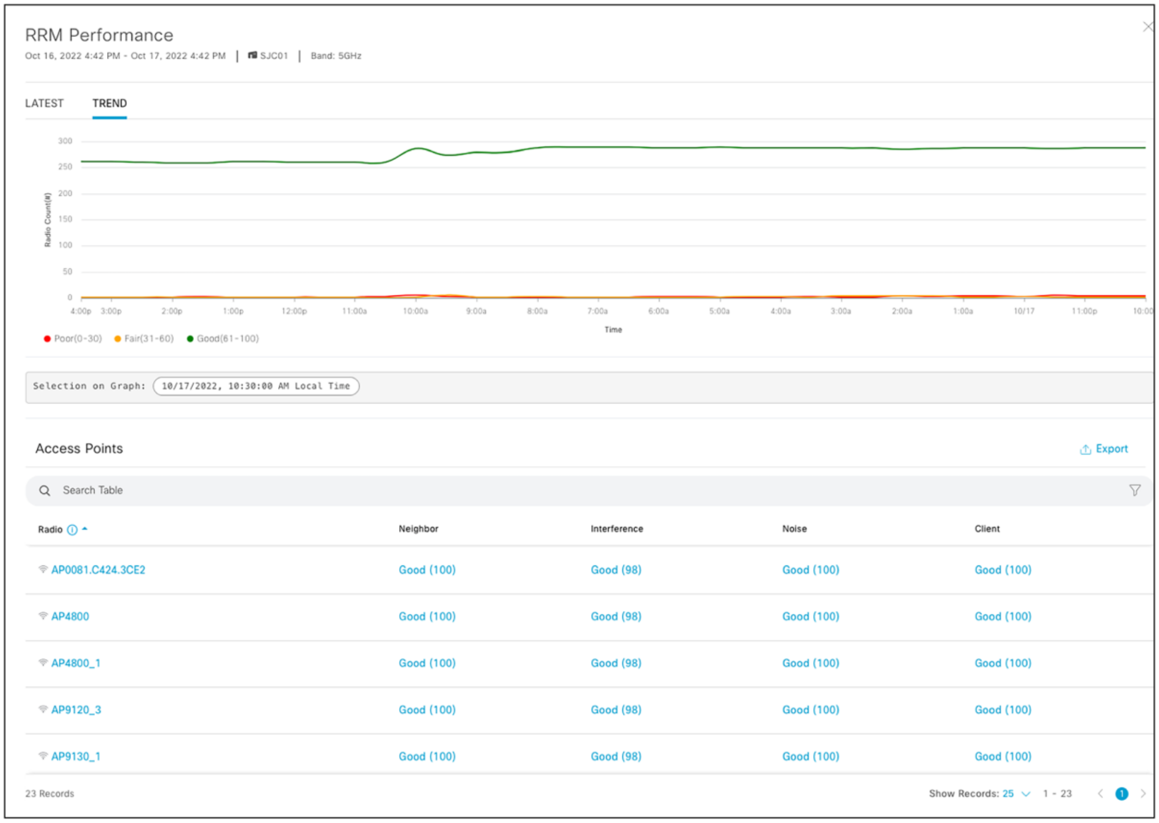


Figure 109.
RRM Performance trend detail views – visualize transitions in AP RF health scores



Selection on Graph: 10/17/2022, 10:30:00 AM Local Time

Access Points

Radio	Neighbor	Interference	Noise	Client
AP0081.C424.3CE2	Good (100)	Good (98)	Good (100)	Good (100)
AP4800	Good (100)	Good (98)	Good (100)	Good (100)
AP4800_1	Good (100)	Good (98)	Good (100)	Good (100)
AP9120_3	Good (100)	Good (98)	Good (100)	Good (100)
AP9130_1	Good (100)	Good (98)	Good (100)	Good (100)

23 Records Show Records: 25 1 - 23

Figure 110.
RRM Performance detail views

The Co-Channel Interference widget follows the same pattern, with Latest showing the data from the last 30-minute interval and Trend detailing the channel currently in use, an impact score (based on the duty cycle and RF distance of co-channel neighbors), the CCI values in dBm, and the channel duty cycle (at that point in time)

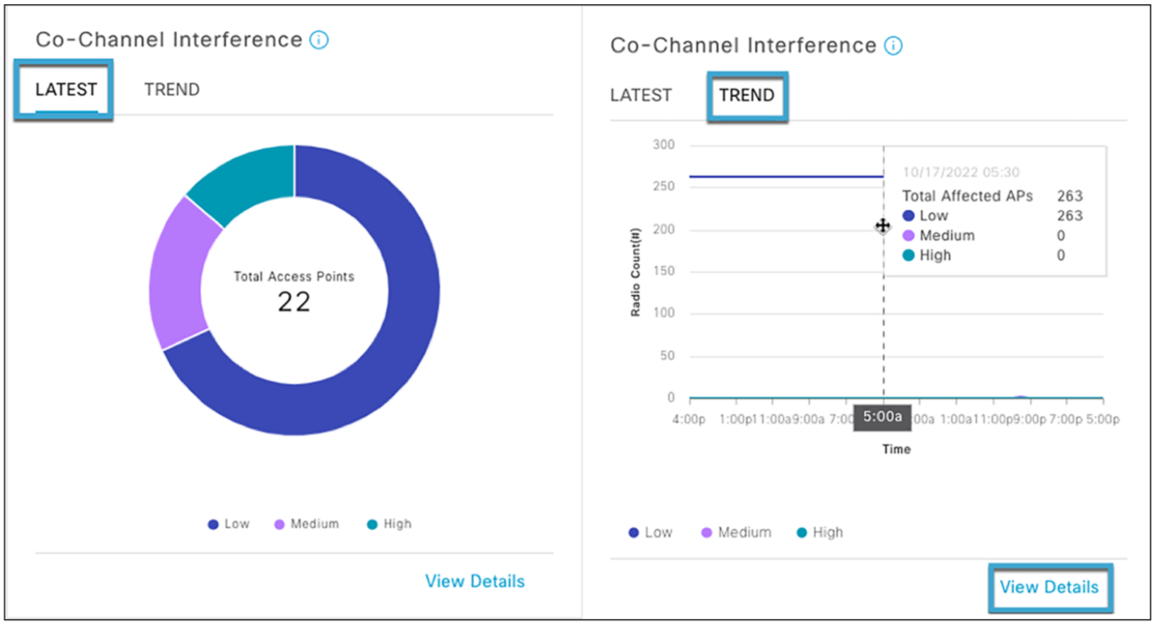
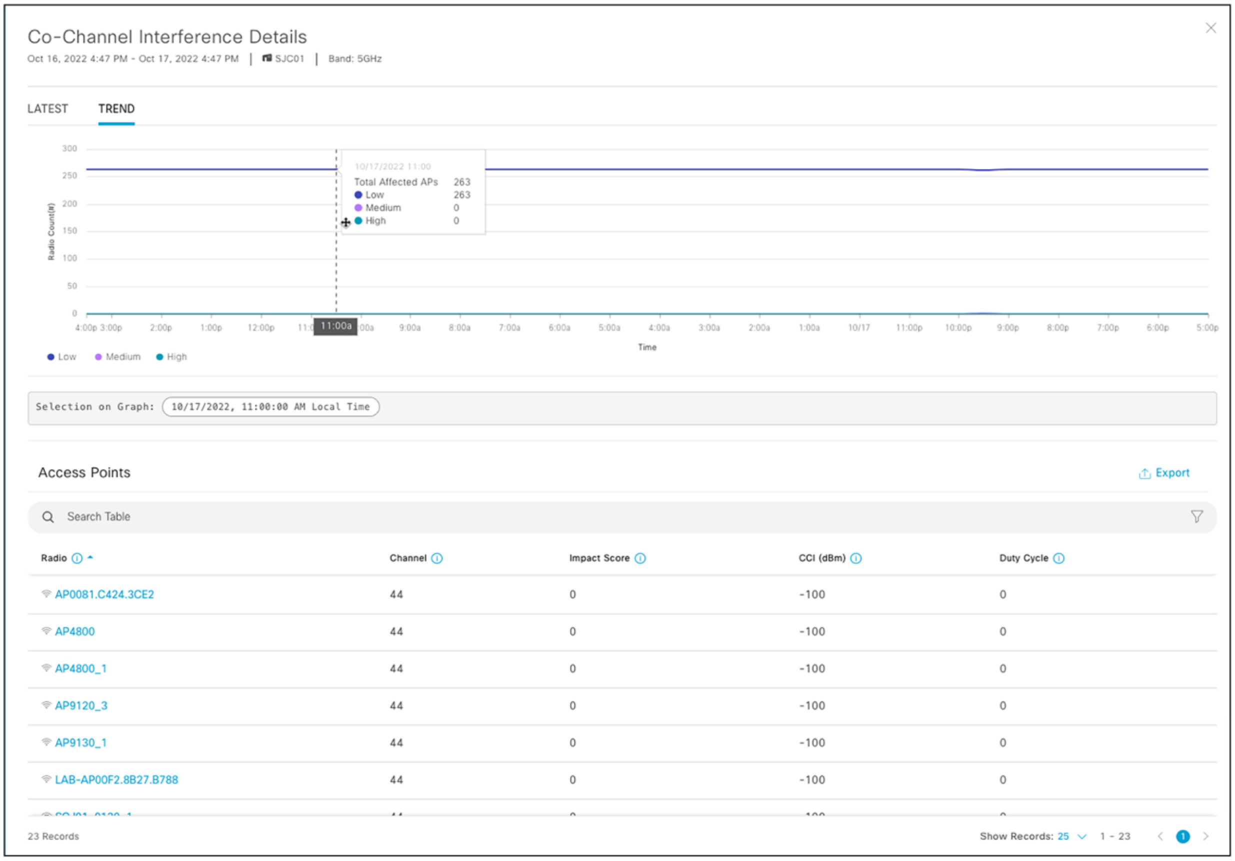


Figure 111.
Co-Channel Interference trend data helps visualize the co-channel interference scores of managed APs



Co-Channel Interference Details

Oct 16, 2022 4:47 PM - Oct 17, 2022 4:47 PM | SJC01 | Band: 5GHz

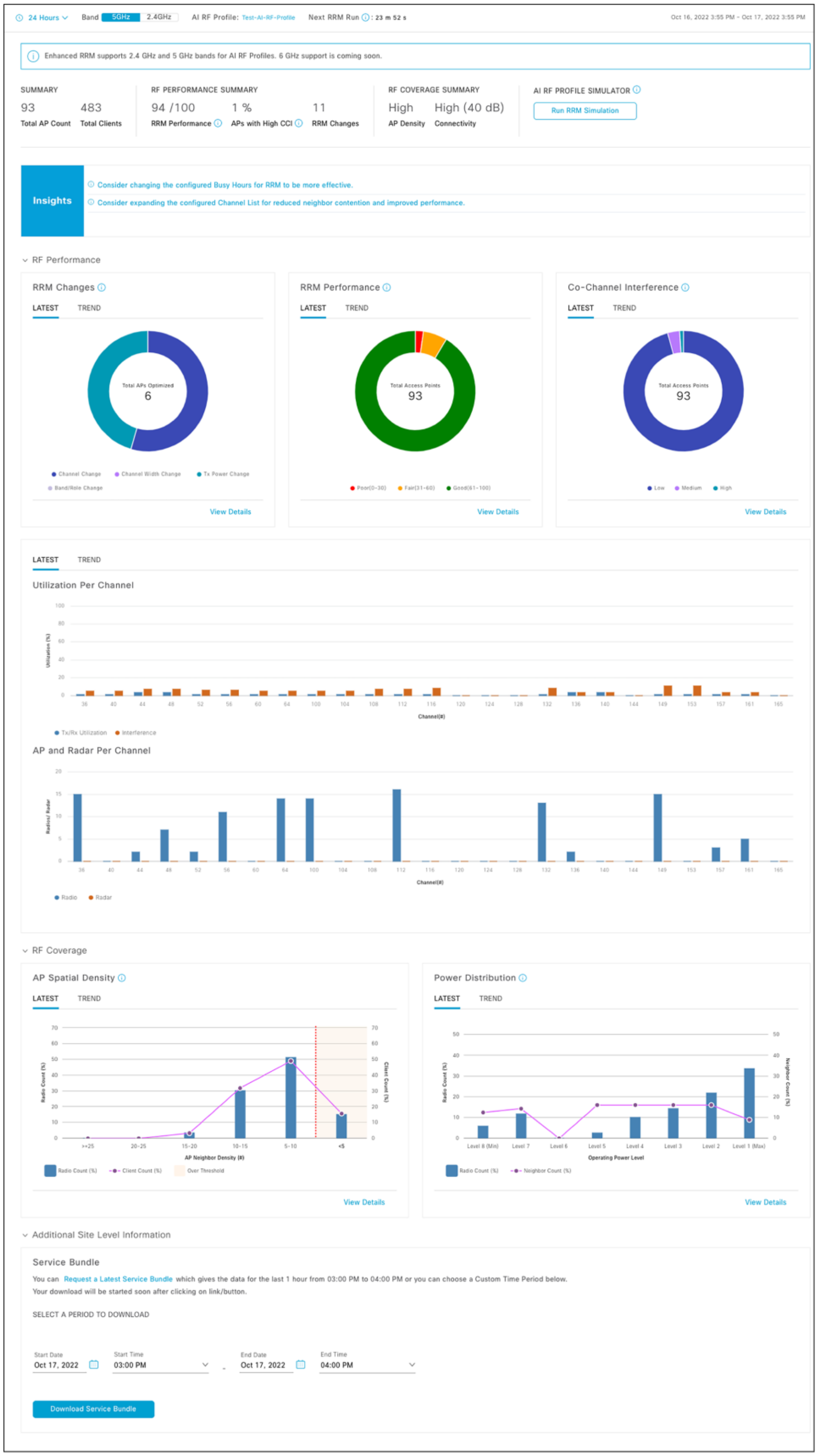
Selection on Graph: 10/17/2022, 11:00:00 AM Local Time

Access Points

Radio	Channel	Impact Score	CCI (dBm)	Duty Cycle
AP0081.C424.3CE2	44	0	-100	0
AP4800	44	0	-100	0
AP4800_1	44	0	-100	0
AP9120_3	44	0	-100	0
AP9130_1	44	0	-100	0
LAB-AP00F2.8B27.B788	44	0	-100	0

23 Records

Figure 112.
Co-channel interference data



AI RF Profile: Test-AI-RF-Profile

Next RRM Run: 23 m 52 s

Enhanced RRM supports 2.4 GHz and 5 GHz bands for AI RF Profiles. 6 GHz support is coming soon.

SUMMARY		RF PERFORMANCE SUMMARY			RF COVERAGE SUMMARY		AI RF PROFILE SIMULATOR
93	483	94 /100	1 %	11	High	High (40 dB)	
Total AP Count	Total Clients	RRM Performance	APs with High CCI	RRM Changes	AP Density	Connectivity	

Consider changing the configured Busy Hours for RRM to be more effective.

Consider expanding the configured Channel List for reduced neighbor contention and improved performance.

Service Bundle

You can Request a Latest Service Bundle which gives the data for the last 1 hour from 03:00 PM to 04:00 PM or you can choose a Custom Time Period below.

Your download will be started soon after clicking on link/button.

SELECT A PERIOD TO DOWNLOAD

Start Date: Oct 17, 2022
Start Time: 03:00 PM
-
End Date: Oct 17, 2022
End Time: 04:00 PM

Figure 113.
AI-Enhanced RRM control center

In the full RRM control center view, AP Spatial Density visualizes the neighboring AP/radio density in the RF neighborhood as the number of neighbors that can be seen at or above -70 dBm.

The Power Distribution chart visualizes power distribution across the networks and provides a corresponding neighbor count to correlate AP density with power assignments. Trend allows visualization of history for up to two weeks. Selecting a time on the trend line opens the detail for that point in time, listing the contributing APs.

Utilization per Channel shows the channel utilization. Trend allows visualization of history for up to two weeks. Selecting a time on the trend line opens the detail for that point in time, listing the contributing APs.

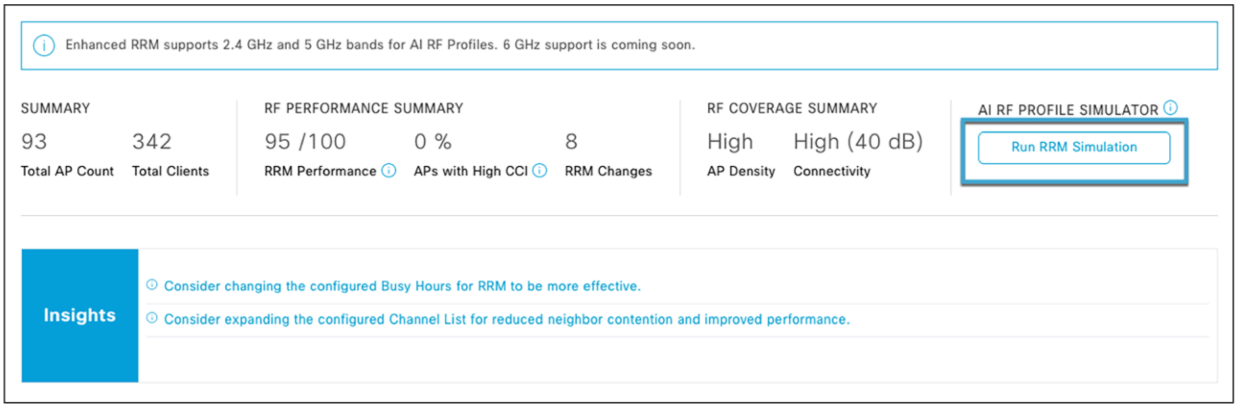
AP and Radar per Channel breaks out the channel assignment spread by AP count. Radar detected is displayed on impacted channels for context.

RRM simulator

The RRM simulator enables the network operator to preview the impact of RRM changes on the live network. When Cisco DNA Center recommends RRM setting changes through its Insights feature, or when the network administrator plans changes to settings such as channel, channel width, and power, the network administrator will be able to:

- Simulate how the RF environment will respond to the changes
- Analyze the impact of potential changes during a particular time interval
- View the proposed changes measured in quantified statistics, including RRM health, co-channel interference and utilization, and RRM changes

Step 1. To use this feature on Cisco DNA Center, go to the AI-Enhanced RRM control center by choosing the hamburger menu and selecting Assurance > Enhanced-RRM. Select the site where you want to try these changes using the RRM simulator. Click **Run RRM Simulation from the hero bar**.



Enhanced RRM supports 2.4 GHz and 5 GHz bands for AI RF Profiles. 6 GHz support is coming soon.

SUMMARY: 93 Total AP Count; 342 Total Clients

RF PERFORMANCE SUMMARY: 95 /100 RRM Performance; 0 % APs with High CCI; 8 RRM Changes

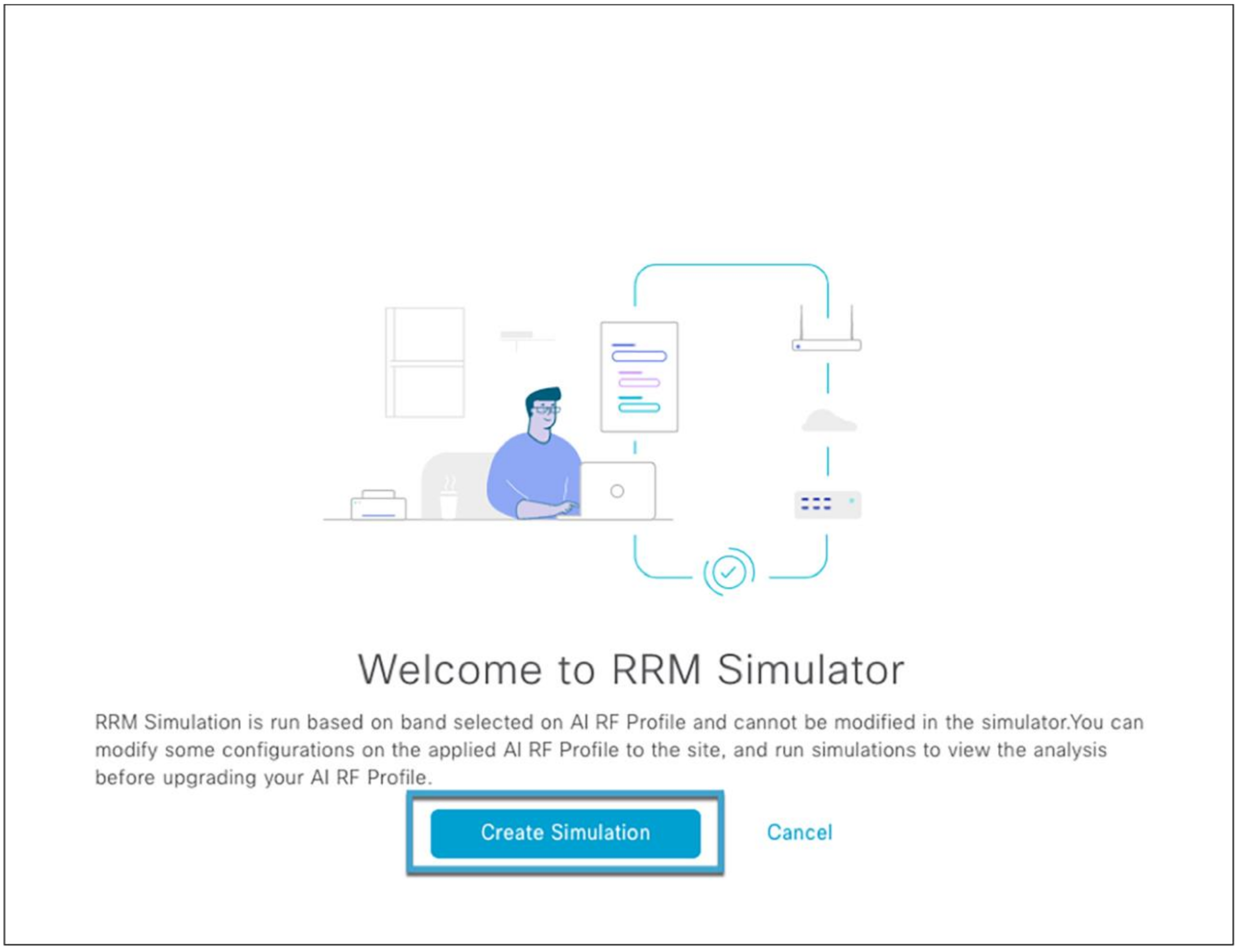
RF COVERAGE SUMMARY: High AP Density; High (40 dB) Connectivity

Consider changing the configured Busy Hours for RRM to be more effective.

Consider expanding the configured Channel List for reduced neighbor contention and improved performance.

Figure 114.
Location of RRM simulator on AI-Enhanced RRM control center

Step 2. Click **Create Simulation** from the Welcome to RRM Simulator page



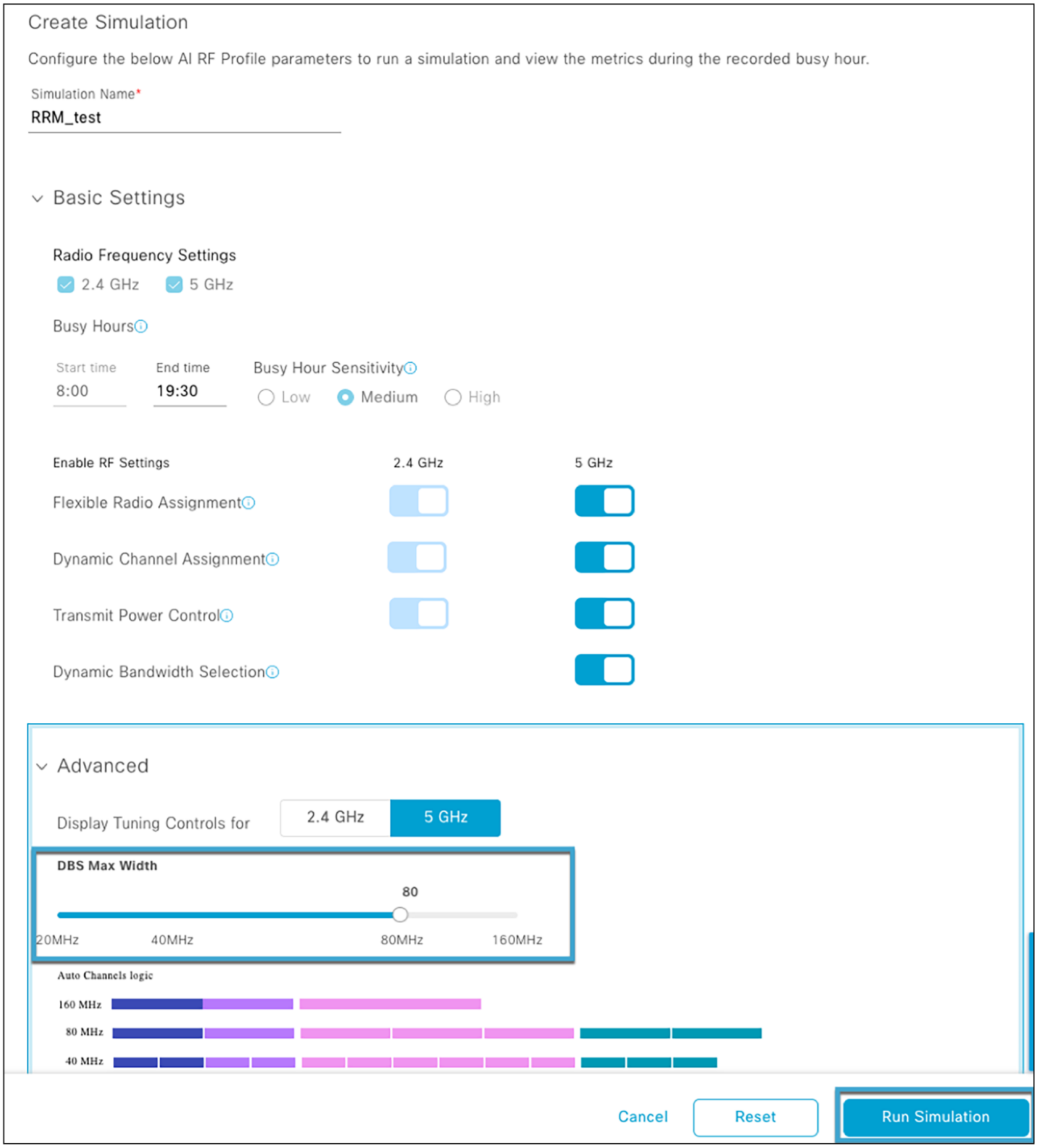
Welcome to RRM Simulator

RRM Simulation is run based on band selected on AI RF Profile and cannot be modified in the simulator.You can modify some configurations on the applied AI RF Profile to the site, and run simulations to view the analysis before upgrading your AI RF Profile.

Figure 115.
Create Simulation button on RRM simulator

Step 3. Make the changes necessary to the simulation profile you need to analyze.

- In this case, we will change the DBS from 40 MHz to 80 MHz.
- Click **Run Simulation** to simulate RF performance data for the newly modified RF settings.



Create Simulation

Configure the below AI RF Profile parameters to run a simulation and view the metrics during the recorded busy hour.

Simulation Name*: RRM_test

Basic Settings

Radio Frequency Settings

☑ 2.4 GHz ☑ 5 GHz

Busy Hours

Start time: 8:00

End time: 19:30

Busy Hour Sensitivity: ○ Low ● Medium ○ High

Enable RF Settings	2.4 GHz	5 GHz
Flexible Radio Assignment	○	●
Dynamic Channel Assignment	○	●
Transmit Power Control	○	●
Dynamic Bandwidth Selection		●

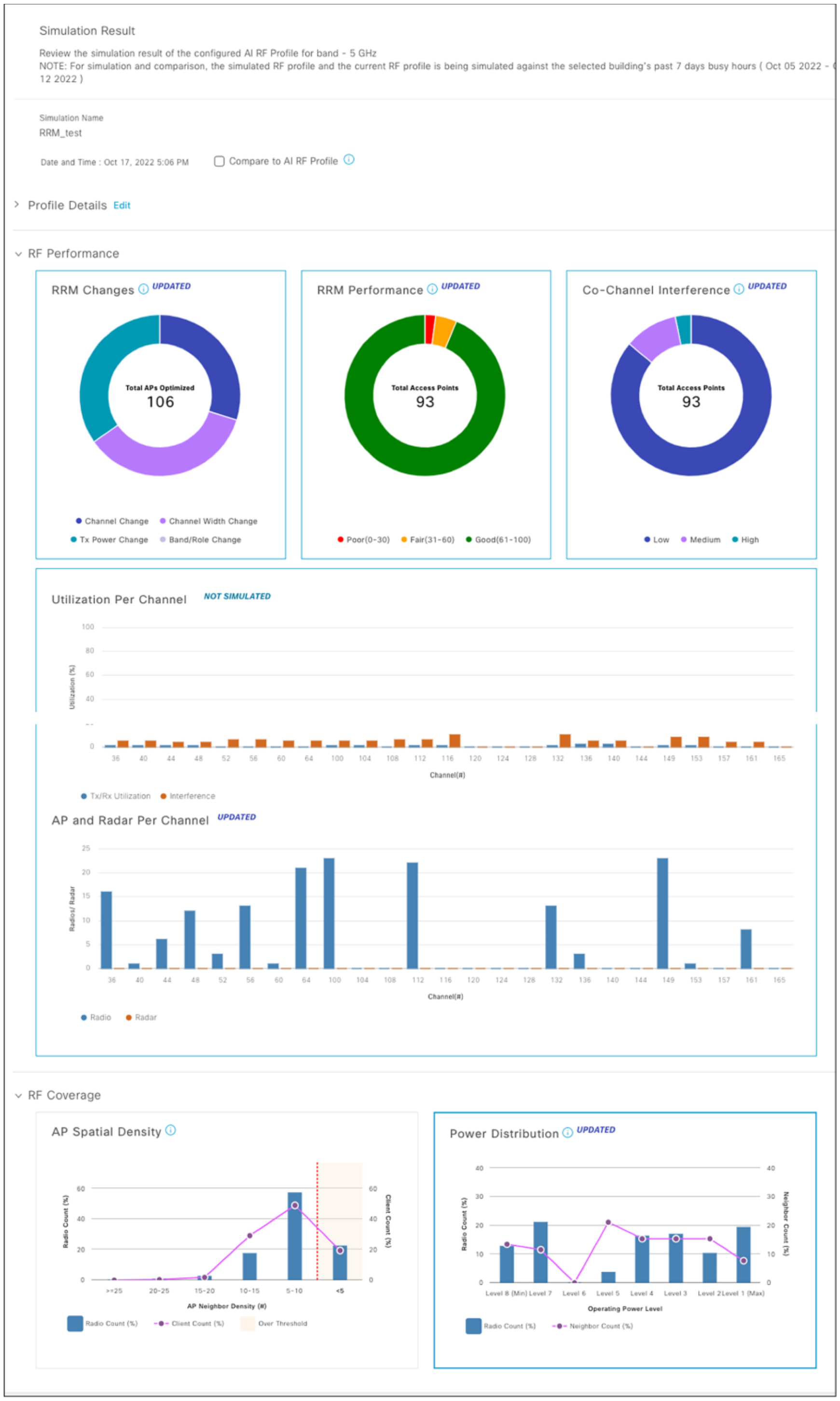
Advanced

Display Tuning Controls for: 2.4 GHz [✓ 5 GHz]

DBS Max Width: 80

Figure 116.
Changing the AI RF profile before running the simulation

Step 4. The simulation result is displayed as shown in the figure below. All the widgets tagged as UPDATED have changed after the RF settings modification. You can compare the simulated RF performance data with your current RF performance data by selecting the **Compare to AI RF Profile** checkbox.



Simulation Result

Review the simulation result of the configured AI RF Profile for band - 5 GHz
NOTE: For simulation and comparison, the simulated RF profile and the current RF profile is being simulated against the selected building's past 7 days busy hours (Oct 05 2022 - (
12 2022)

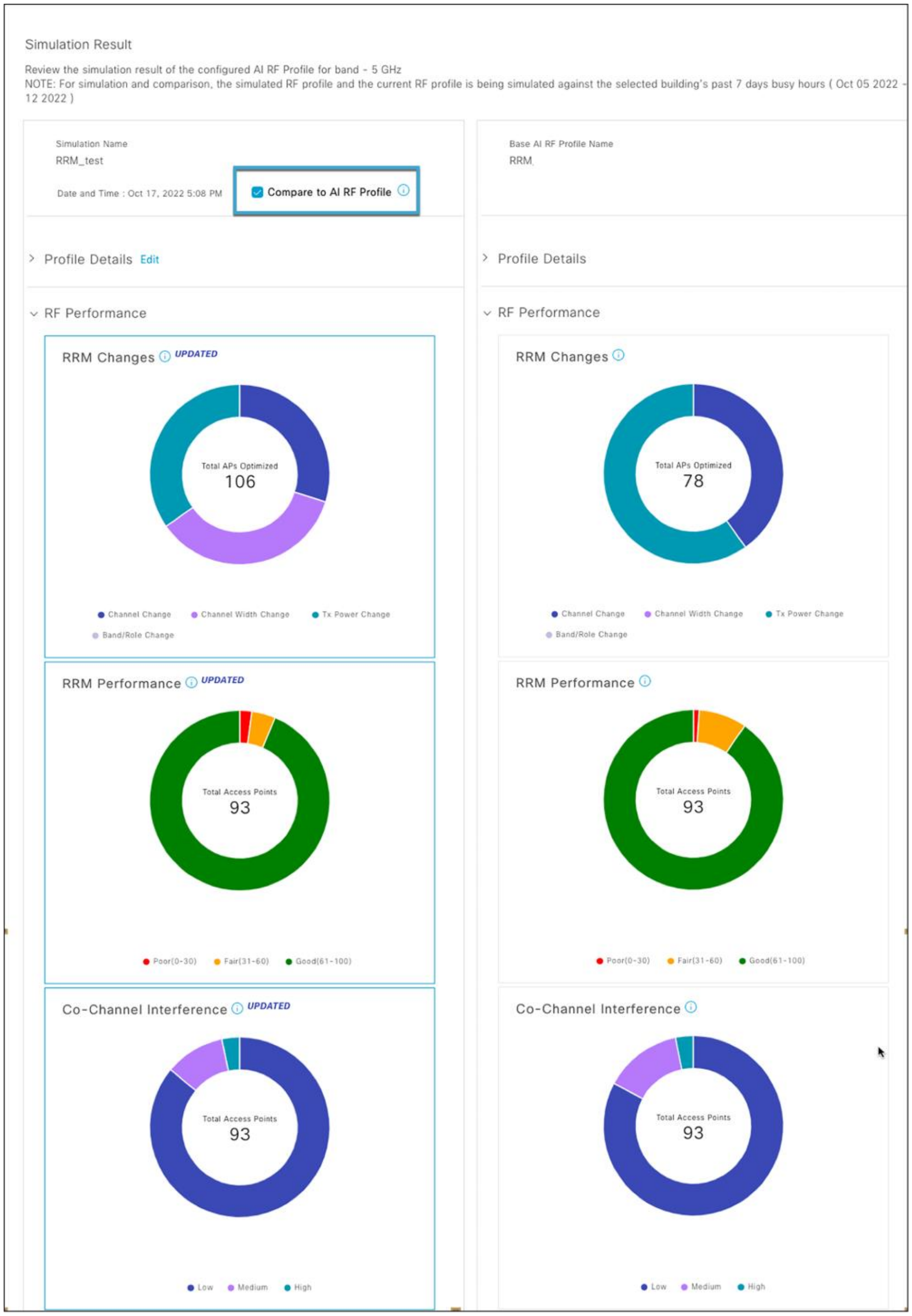
Simulation Name
RRM_test

Date and Time : Oct 17, 2022 5:06 PM

□ Compare to AI RF Profile

Figure 117.
RRM simulator result after making changes to AI RF profile

Step 5. You can compare all the widgets between the simulation and deployed AI RF profile for this site. The comparison is shown below. You can select **Upgrade AI RF Profile** if you wish to add these changes to the current AI RF profile. Select **Cancel** if you do not wish to make the changes.



Simulation Result

Review the simulation result of the configured AI RF Profile for band - 5 GHz
NOTE: For simulation and comparison, the simulated RF profile and the current RF profile is being simulated against the selected building's past 7 days busy hours (Oct 05 2022 - 12 2022)

Simulation Name: RRM_test

Date and Time : Oct 17, 2022 5:08 PM

☑ Compare to AI RF Profile

Base AI RF Profile Name: RRM

Figure 118.
Comparing the simulation result with current RF performance parameters

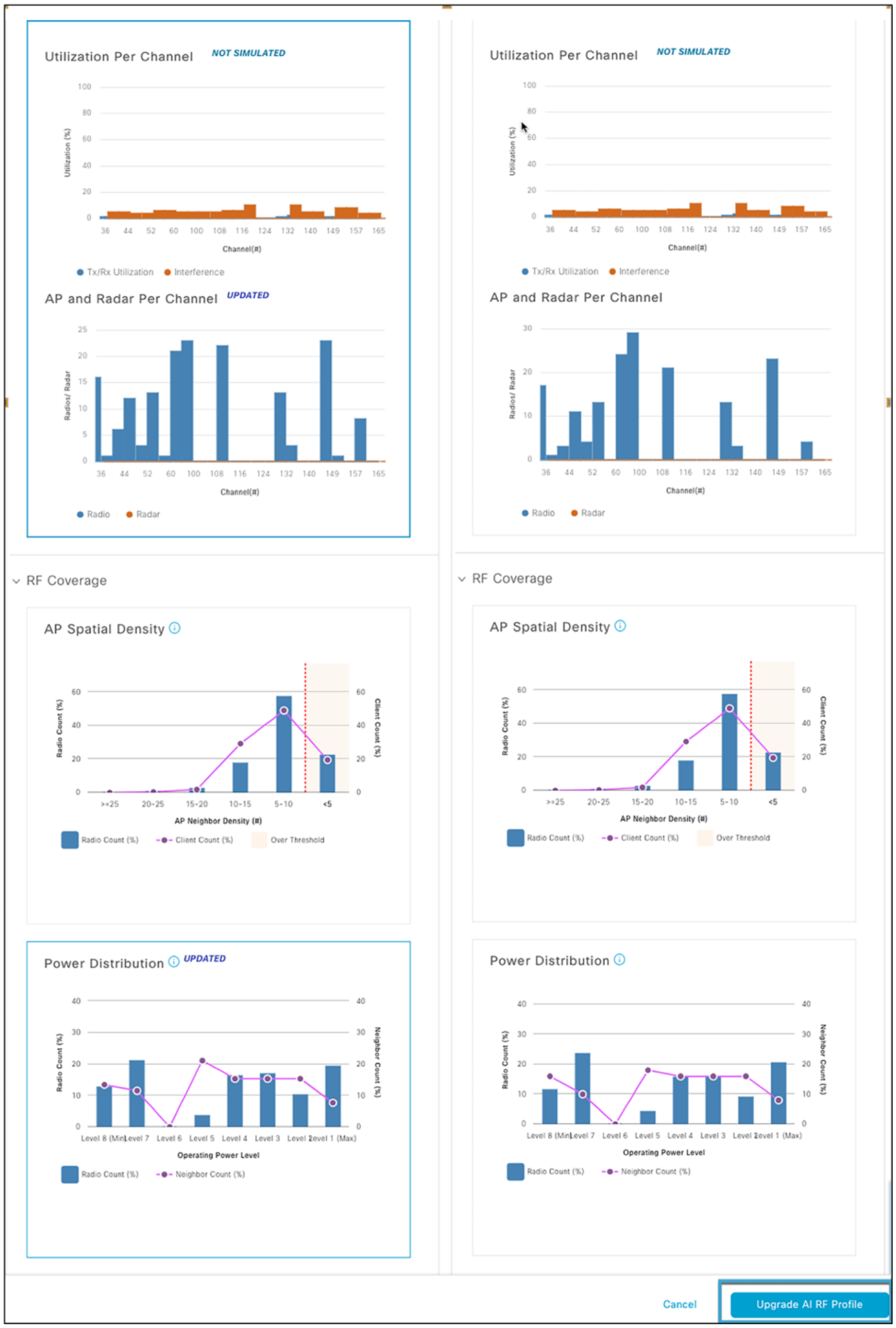


Figure 119.
Comparing the simulation result with current RF performance parameters (cont.)

Useful links

Cisco DNA Center User Guide, Release 2.3.4

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-4/user_guide/b_cisco_dna_center_ug_2_3_4.html

Cisco DNA Center information

- https://www.cisco.com/site/us/en/products/networking/catalyst-center/index.html?dtid=osscdc000283

Cisco Catalyst 9800 Series information

- https://www.cisco.com/c/en/us/products/wireless/catalyst-9800-series-wireless-controllers/index.html

Cisco Catalyst 9100 information

- https://www.cisco.com/c/en/us/products/wireless/catalyst-9100ax-access-points/index.html

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**.

Printed in USA C07-3296242-01 08/23