

## LTREWN-2511

# Automating Wireless deployments at scale using Catalyst Center (formerly Cisco DNA Center)

Marcin Dorecki – Customer Delivery Architect

Alejandro Ramirez Gomez – Consulting Engineer

## *Introduction*

### Table of Contents

Introduction.....	2
Scenario.....	4
Task 0: VPN to dCloud Network .....	8
Task 1: Manual Site Hierarchy Creation .....	11
Task 2: Ekahau to Catalyst Center Import.....	15
Task 3: Prime Infrastructure to CATALYST CENTER Migration .....	20
Task 4: Hamina Integration with Catalyst Center .....	26
Task 5: Add Wireless LAN Controller to Catalyst Center.....	30
Task 6: Access Point Discovery .....	47
Task 7: Network Settings and Centrally Switched WLANs.....	59
Task 8: Configure Flex Local Switching Architecture .....	89
Task 9: Addressing Specific Custom Requirements.....	99
Task 10: Client Connectivity Testing .....	133
Task 11: Bonus Tasks – Anchoring.....	142
Task 12: Bonus Tasks – Configuring HA-SSO .....	164
Task 13: Bonus Tasks – AP Power Save (Read Only) .....	170
FAQ .....	171
Related Sessions at CiscoLive.....	173

## Learning Objectives

Upon completion of this lab, you will be able to:

- Manage site hierarchy using Catalyst Center and use different methods of migrating existing ones into Catalyst Center.
- Discover and manage wireless devices using Catalyst Center
- Design and configure wireless networks using Catalyst Center
- Utilize available Wireless workflows in Catalyst Center to adjust configuration of WLCs and APs as needed.

## Disclaimer

This training document is to familiarize with wireless network provisioning using Catalyst Center. Although the lab design and configuration examples could be used as a reference, it's not a real design, thus not all recommended features are used, or enabled optimally. For the design related questions please contact your representative at Cisco, or a Cisco partner.

## Scenario

In this lab activity, you will learn how to use **Catalyst Center** as single pane of management for your wireless network based on Catalyst 9800 WLCs.

The goal of this lab is to **explore** and **implement** various **configurations** to achieve a comprehensive wireless network design using Cisco 9800 controllers and Catalyst Center **simulating a real-world network**.

The lab focuses on key features, including Hamina and Prime Infrastructure to CATALYST CENTER migration, importing Ekahau plans, and mainly using Catalyst Center to push the intended wireless configuration to deploy Central Switching and FlexConnect Local Switching WLANs.

In the process, the participants will gain hands-on experience with all the configuration elements such as:

- Wireless-specific settings,
- Network Profiles with AP Zones,
- Model Config Editor,
- CLI Templates,
- AP workflows

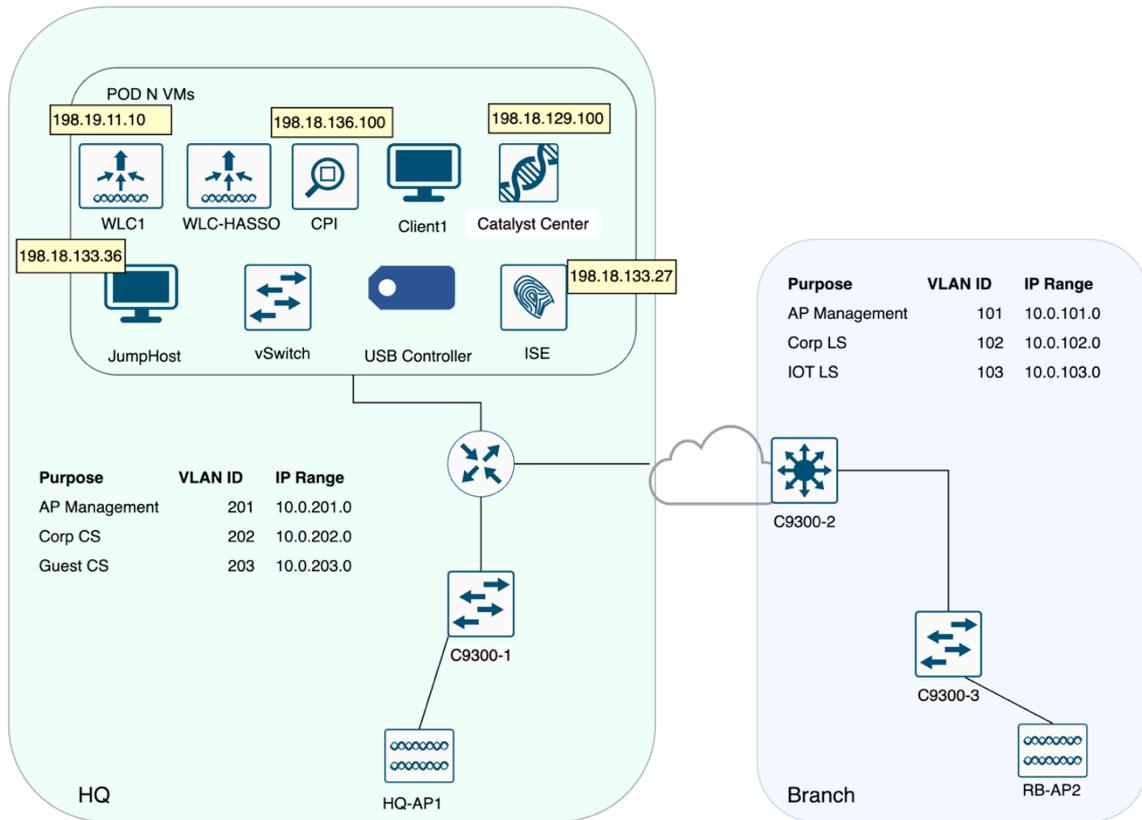
All of these in order to streamline advanced configurations. This approach facilitates the deployment process, ensuring consistency and adherence to best practices across the network.

The scenario in this lab includes a **main site called HQ** and a **branch site called BR**. Different SSID deployment scenarios will be explored, with a focus on both central and FlexConnect Local switching modes. This will enable participants to understand the benefits and considerations associated with automating each mode.

Ultimately, if time allows, participants will be able to get a glimpse of operating a functioning network by executing optional tasks such as Managed and External Anchor Groups and setting up HA SSO.

## Lab Logical Topology

Figure 1 Lab Topology



## Lab Matrix

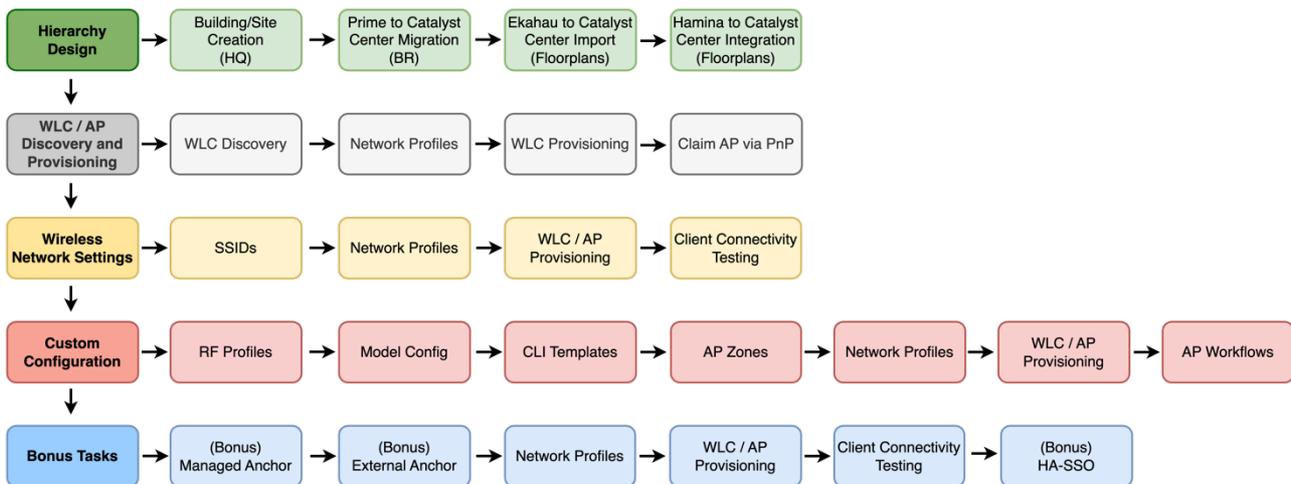
Table 1 Devices and Virtual Machines Addressing and Credentials

Name	IP Address	Username	Password	Preferred Access Method
Jump Host	198.18.133.36	DCLLOUD\admin	C1sco12345	RDP
Catalyst Center (DNAC)	198.18.129.100	admin	C1sco12345	Chrome
Prime Infrastructure	198.18.136.100	root	@Dm!n12345	Chrome
C9800-CL (WLC1)	198.19.11.10	admin	C1sco12345	Chrome / SSH
C9800-CL (WLC-HASSO)	198.19.11.11	admin	C1sco12345	Chrome / SSH
C9800-CL (WLC2-ANCHOR)	198.19.12.10	admin	C1sco12345	Chrome / SSH

C9800-CL (WLC3-EXTANCHOR)	198.19.13.10	admin	C1sco12345	Chrome / SSH
ISE 3.0	198.18.133.27	admin	C1sco12345	Chrome
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP
Client4	198.18.134.4	DCLOUD\admin	C1sco12345	RDP
ISR4331	198.18.133.145	admin	C1sco12345	SSH
9300-1 Switch	198.18.128.22	admin	C1sco12345	SSH
9300-2 Switch	198.18.128.23	admin	C1sco12345	SSH
9300-3 Switch	198.18.128.24	admin	C1sco12345	SSH

## Lab Tasks

Figure 2 Lab Task Details



## Guidelines and Best Practices

Follow these guidelines and best practices when using the environment.

1. **Configure unique SSIDs (using the POD ID).** This will ensure that your clients are attaching to your network.
2. **DO NOT perform a system or application download/update in the Cisco DNA Center software in this demo,** as it may cause performance/functionality issues, which falls outside of dCloud support.

3. Don't set a console password. A console password will prevent hardware automation from accessing the hardware to apply the default configurations and will require physical intervention.
4. DO NOT erase the IOS on the devices. If the hardware boots into ROMMON mode it requires physical intervention and makes the pod unavailable for the next user.
5. If you disconnect the wireless network interface card from a client, you must reboot the USB controller via the dCloud Power Control feature. This is a known bug in the card.

## Specific Requirements

Besides creating CORP, IOT and GUEST Networks, there are extra requirements to accommodate it to a real world scenario. In one of the tasks the lab show cases the different tools in Catalyst Center's toolbox.

**Table 2 Customer Requirements**

No	Description	Tool	Task
1	Allow legacy scanners to work in Warehouse area of HQ. Disable 2.4GHz in the Office space of HQ	RF Profiles	Task 9 Step 1
2	For the site survey purpose, enable Aironet IE for CORP SSID	Model Config	Task 9 Step 2
3	Static RF Leader for both bands	CLI Templates	Task 9 Step 3
4	Increase DCA interval on 2,4GHz and 5GHz bands to 12 hours with anchor time set to 4	CLI Templates	Task 9 Step 3
5	Remove channels 120 124 128 from DCA global channel plan	CLI Templates	Task 9 Step 3
6	Enable SSH on all APs HQ and RB with credentials admin/C1sco12345	AP Profiles	Task 9 Step 4
7	No need for IOT SSID in the OFFICE area at HQ site	AP Zones	Task 9 Step 9
8	Define Primary WLC to all APs Rename APs at RB	AP Workflows	Task 9 Step 13
9	Disable LEDs to APs at HQ	AP Workflows	Task 9 Step 13

We'll come back to these in a later stage, for now, **let's go** to the LAB!

## Task 0: VPN to dCloud Network

In order to access to the lab devices, a VPN tunnel must be established with the dCloud network provider.



Steps 1-2 should be already prepared for the attendees, jump to Step 3 (Working with Jumphost) if your VPN connection is established by now.

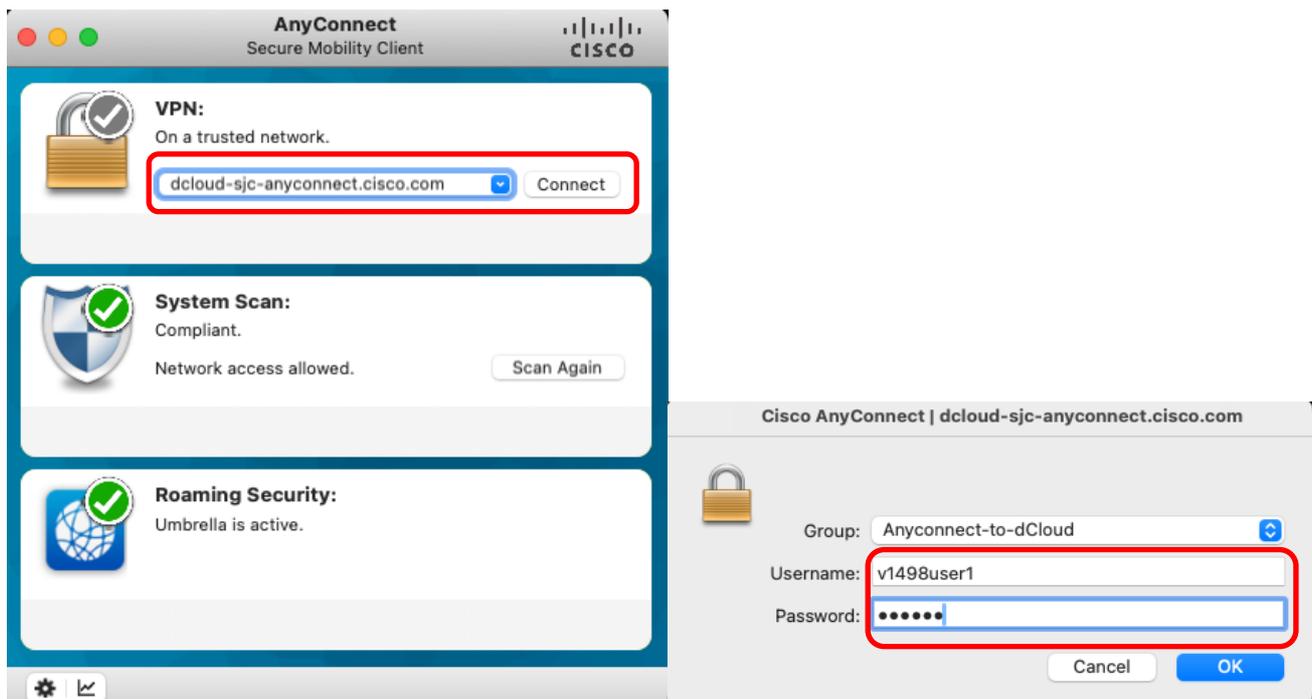
### Step 1: Finding out POD Number and VPN credentials

To determine you POD number and VPN credentials, look at Session Details card provided in front of your workstation.

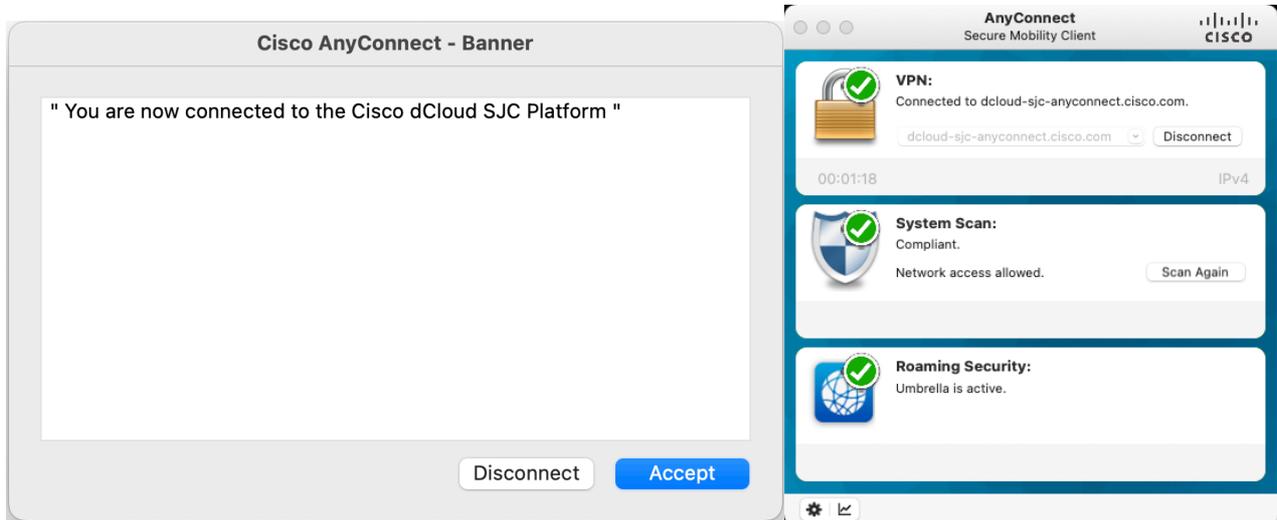
### Step 2: Use AnyConnect Secure Mobile Client

Open Anyconnect VPN client and use the details in previous step to connect:

Figure 3 Connecting to VPN



**Figure 4 VPN Connectivity Successful**



### Step 3: Working from Jump Host

Open your RDP Client and use the JumpHost information to login:

**IP Address:** 198.18.133.36

**username:** DCLOUD\admin

**password:** C1sco12345

**Figure 5 Working from Jump host**

The screenshot shows the 'Add PC' configuration window. At the top, there are tabs for 'General', 'Display', 'Devices & Audio', and 'Folders', with 'General' selected. The 'PC name' field contains the IP address '198.18.133.36'. The 'User account' dropdown is set to 'Ask when required'. Below the tabs, the 'Friendly name' field is set to 'Optional', and the 'Group' dropdown is set to 'Saved PCs'. The 'Gateway' dropdown is set to 'No gateway', and the 'Bypass for local addresses' checkbox is checked. At the bottom, there are three checkboxes: 'Reconnect if the connection is dropped' (checked), 'Connect to an admin session' (unchecked), and 'Swap mouse buttons' (unchecked). At the very bottom of the window are 'Cancel' and 'Add' buttons.

**Add PC**

PC name: 198.18.133.36

User account: Ask when required

General Display Devices & Audio Folders

Friendly name: Optional

Group: Saved PCs

Gateway: No gateway

Bypass for local addresses

Reconnect if the connection is dropped

Connect to an admin session

Swap mouse buttons

Cancel Add

## Task 1: Manual Site Hierarchy Creation

The main objective of this task is to create site hierarchy supporting the company geographical locations.

For the purpose of this lab, we will create one of the company's locations, namely HQ, using Catalyst Center Site Hierarchy workflow. Table below shows the HQ location Hierarchy to be created in Catalyst Center

Table 3 HQ Site Hierarchy

Company Location	Area	Building	Floor
HQ	CLEMEA24	HQ	GF

### Step 1: Defining Site Hierarchy Elements

In order to create site hierarchy supporting all the locations of the Company, **Open a browser** and **navigate** to Catalyst Center GUI and login using provided credentials:

**IP Address:** <https://198.18.129.100/>

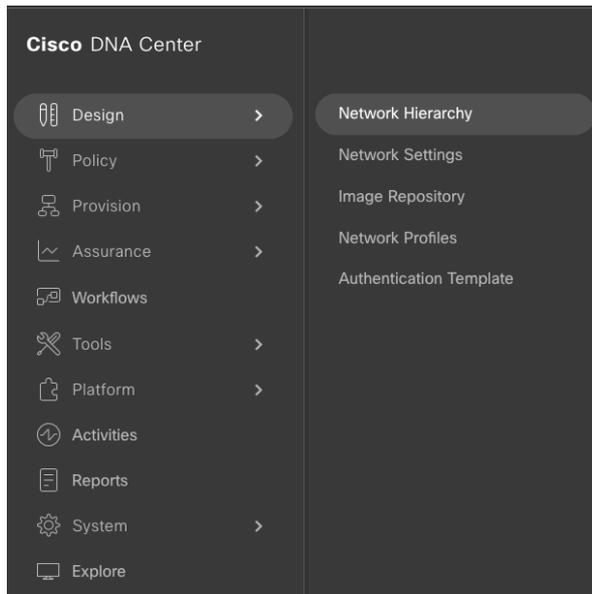
**Credentials:** admin / C1sco12345

Figure 6 Logging in to Catalyst Center

The screenshot shows the Cisco DNA Center login interface. At the top, the Cisco DNA Center logo is displayed with the tagline 'The bridge to possible'. Below the logo, a green success message box contains a checkmark and the text 'Success!'. Underneath, there are two input fields: 'Username\*' with the value 'admin' and 'Password\*' with a masked password represented by ten dots. The login form is styled with a clean, modern look using blue and green accents.

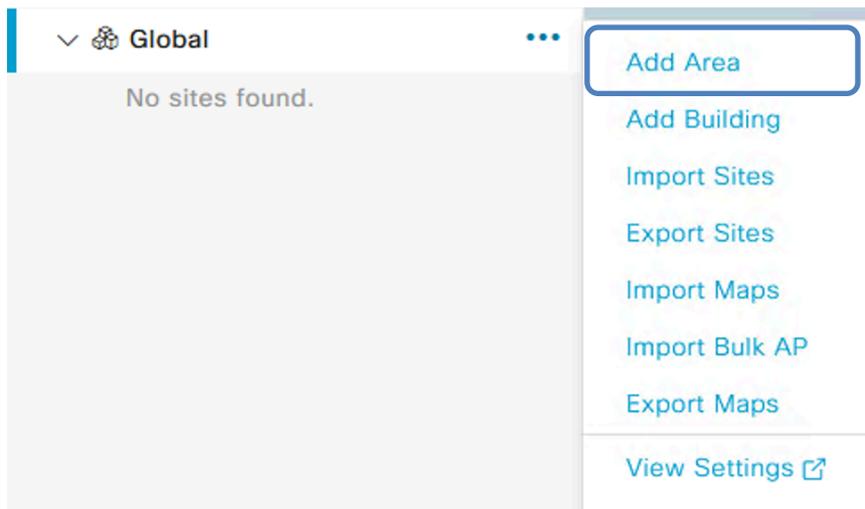
Next, navigate to **Design > Network Hierarchy**

**Figure 7 Network Hierarchy**



Hover over the three dots in front of **Global**

**Figure 8 Site Hierarchy - Area**



click on **Add Area** and specify following details and click **Add**

## Figure 9 Site Hierarchy - Area

### Add Area ×

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

Area Name\*  
**CLEMEA24**

Parent  
**Global** ▼

---

Or

[Import Sites](#)

As a next step, hover over newly created **CLEMEA24** Area and click on **Add Building**

- Building Name: **HQ**
- Latitude: **37.4117**
- Longitude: **-121.9322**

## Figure 10 Site Hierarchy - Building

### Add Building ×

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

Building Name\*  
**HQ**

Parent  
**CLEMEA24 | Global/** ▼

Address ⓘ  
**Artisan Cafe, 350 E Tasman Dr, San Jos**

Latitude\* **37.4117**      Longitude\* **-121.9322**

Once the building is created you will see it in the hierarchy on the left.

Hover over the three dots and click on **Add Floor**, name it as **GF** and use provided file **HQ-GF** to upload as floor plan using the default scale and sizing settings.

**Figure 11 Site Hierarchy - Floor**

The screenshot shows the 'Add Floor' dialog box in a site hierarchy tool. The dialog is titled 'Add Floor' and has a close button (X) in the top right corner. It contains the following fields and options:

- Floor Name\***: GF
- Parent**: HQ
- Type (RF Model)\***: Cubes And Walled Offices (dropdown)
- Floor Number\***: 1
- Floor Type\***: Medium Floor (15dB/ft) (dropdown)
- Thickness (ft)\***: 2
- Floor Image**: HQ-GF.png (upload field with a trash icon)
- Warning**: Uploaded image aspect ratio determines a width/length ratio: 1:0.9
- Dimensions**:
  - Width (ft)\***: 100.00
  - Length (ft)\***: 86.00
  - Height (ft)\***: 10
- Buttons**: Cancel, Add

Having completed the procedure till now, your hierarchy should look as follows:

**Figure 12 Site Hierarchy - Task 1**

The screenshot shows the site hierarchy view. At the top is a search bar labeled 'Find Hierarchy'. Below it is a tree structure with the following levels:

- Global (expanded)
- CLEMEA24 (expanded)
- HQ (expanded)
- GF (newly added floor, highlighted with a blue bar)

## Task 2: Ekahau to Catalyst Center Import

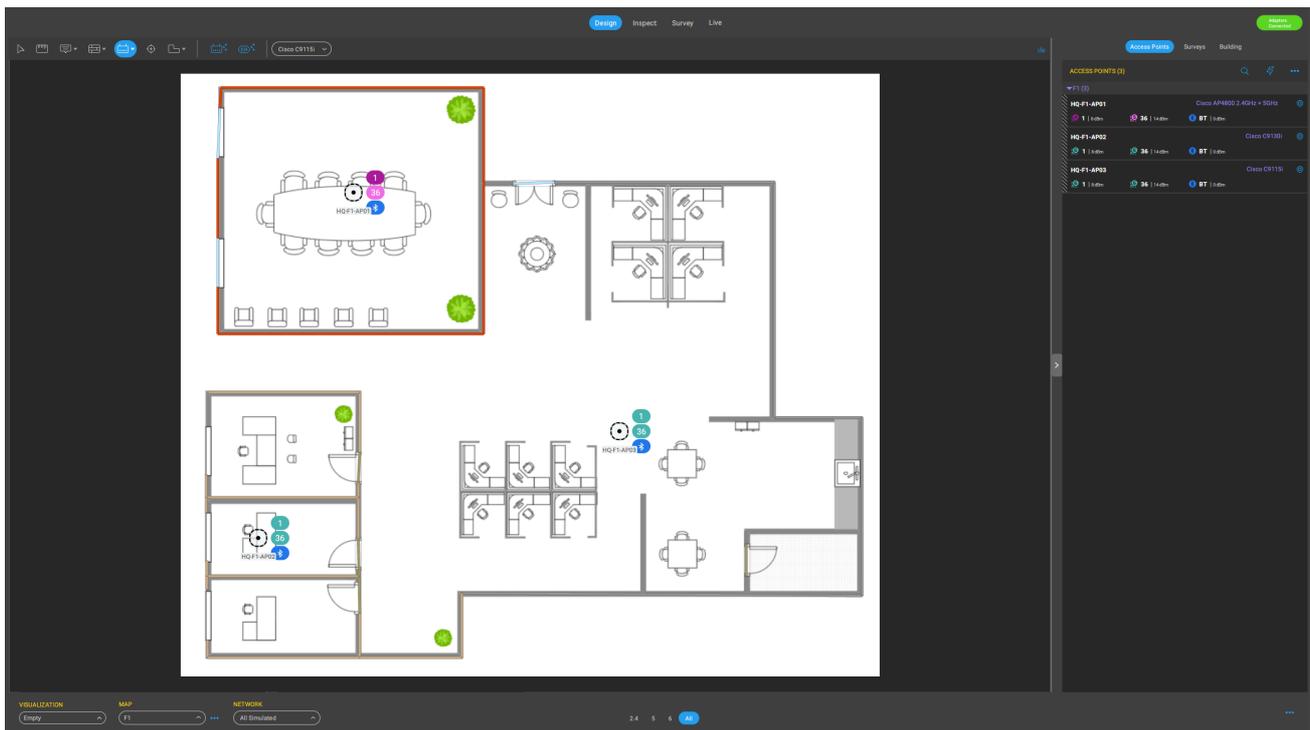
This activity will focus on importing Ekahau file with AP Placement into Catalyst Center hierarchy. This use case focuses on customers performing pre-deployment designs and helps them to import Ekahau files to maintain the AP positions as well as scale and obstacles.

In this task we will import **Floor 1** into **HQ** site hierarchy.

For your reference, an image of the Ekahau project file is provided below.

The Building **HQ** was created in .esx file and a floor named **F1** with three APs and several wall types.

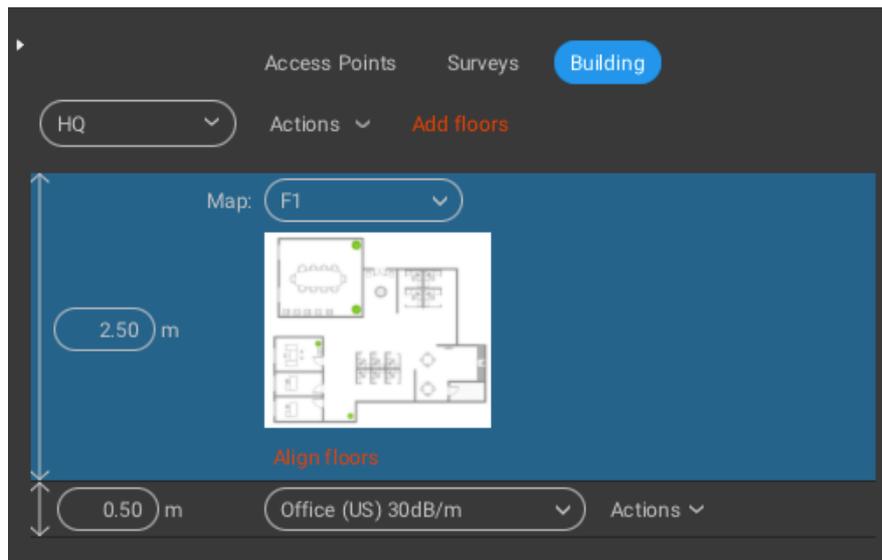
Figure 13 Ekahau Project





In order to import an Ekahau project into Catalyst Center, it requires a building to be created in .esx project matching the name of the one present in Catalyst Center Hierarchy. This is a glance at the building structure that was created in Ekahau file.

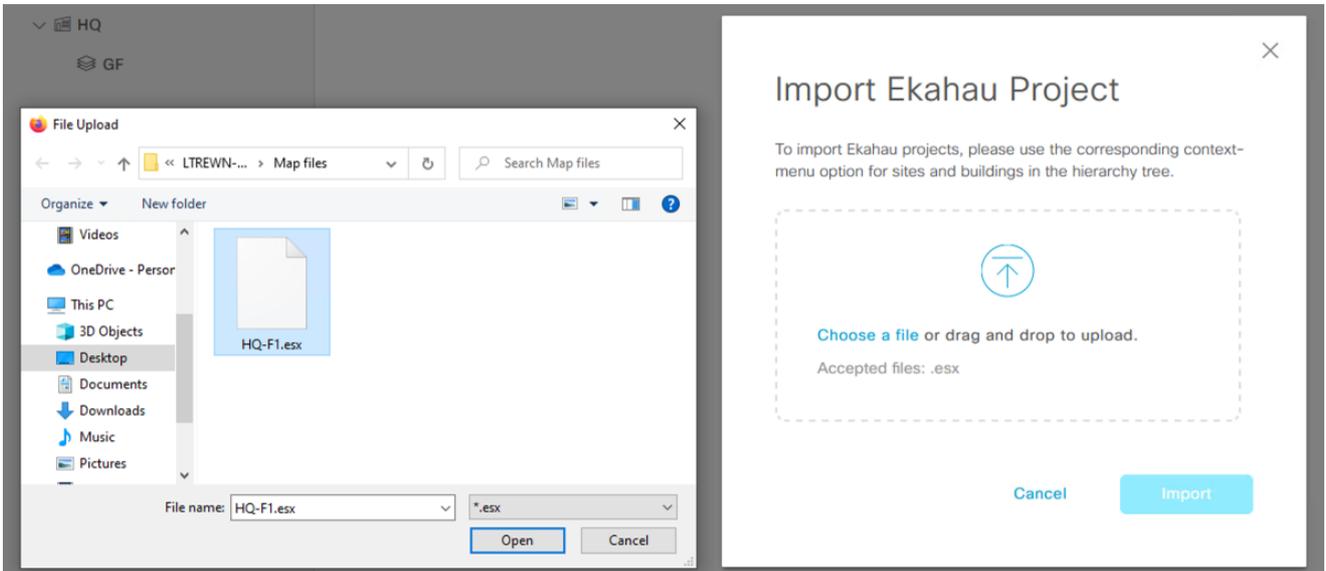
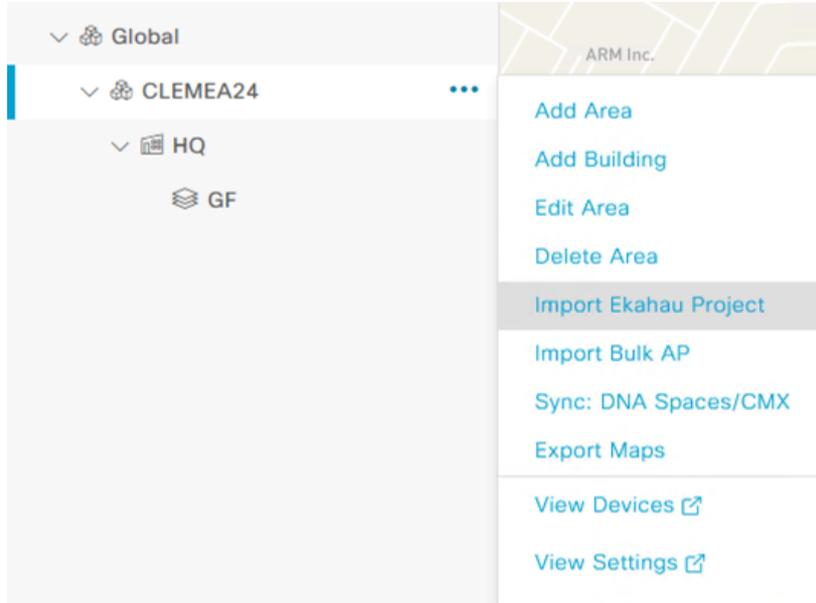
**Figure 14 Ekahau Project - Building**



## Step 1: Importing Ekahau Project into Catalyst Center Hierarchy

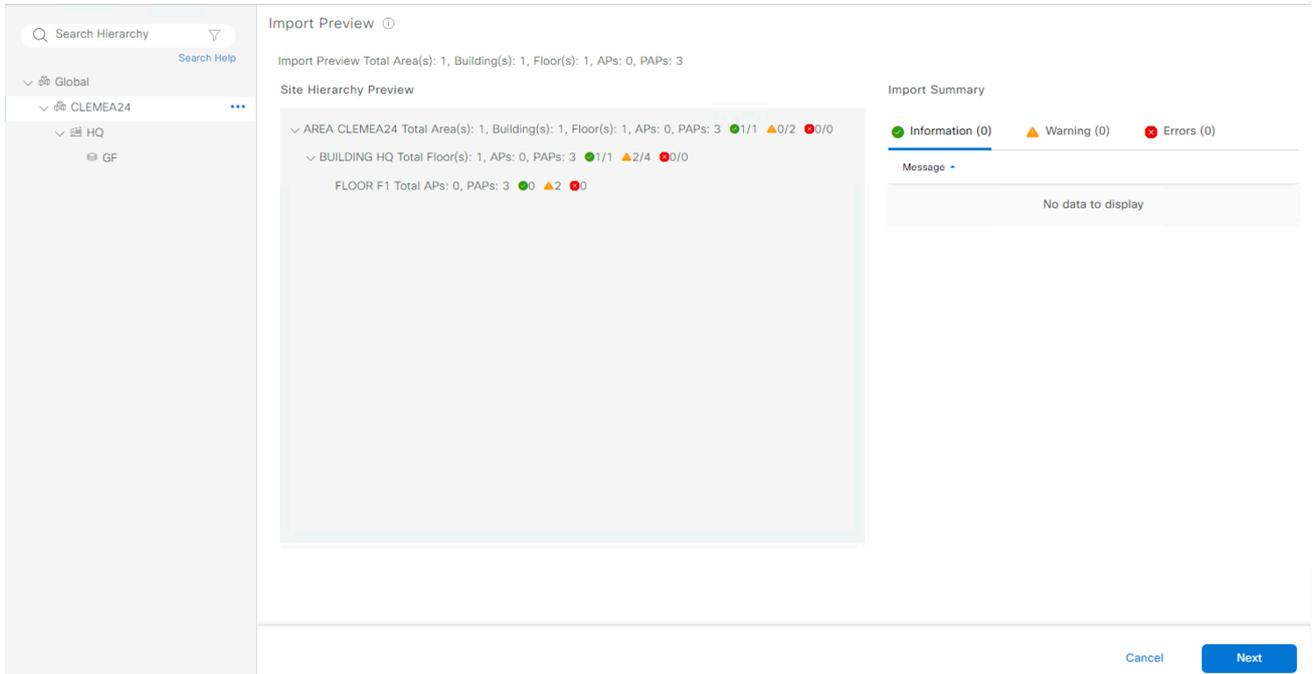
Hover over **CLEMEA24 Area** and click on **Import Ekahau Project** and choose local .esx file named **HQ-F1.esx** from your jumphost local drive, then confirm by clicking on **Import**.

**Figure 15 Import Preview - Ekahau**



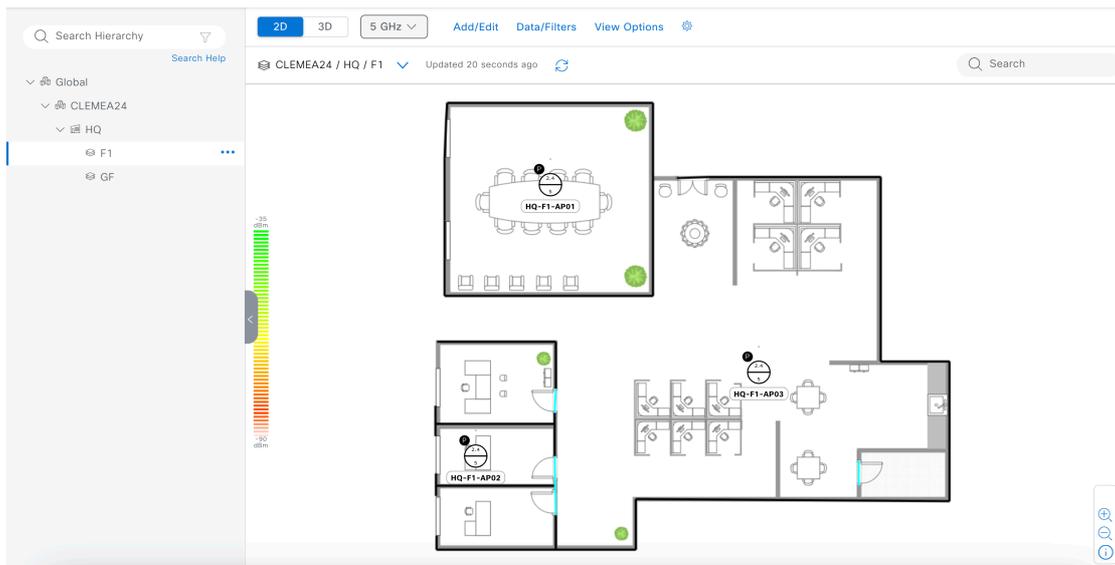
Import Preview screen should summarize all the items that will be imported into site hierarchy as in the screenshot below:

Figure 16 Import Preview - Ekahau



Click on **Next** and proceed to **View Hierarchy** to verify that the floor HQ-F1 was successfully imported into site hierarchy.

Figure 17 Site Hierarchy - Ekahau Project Import



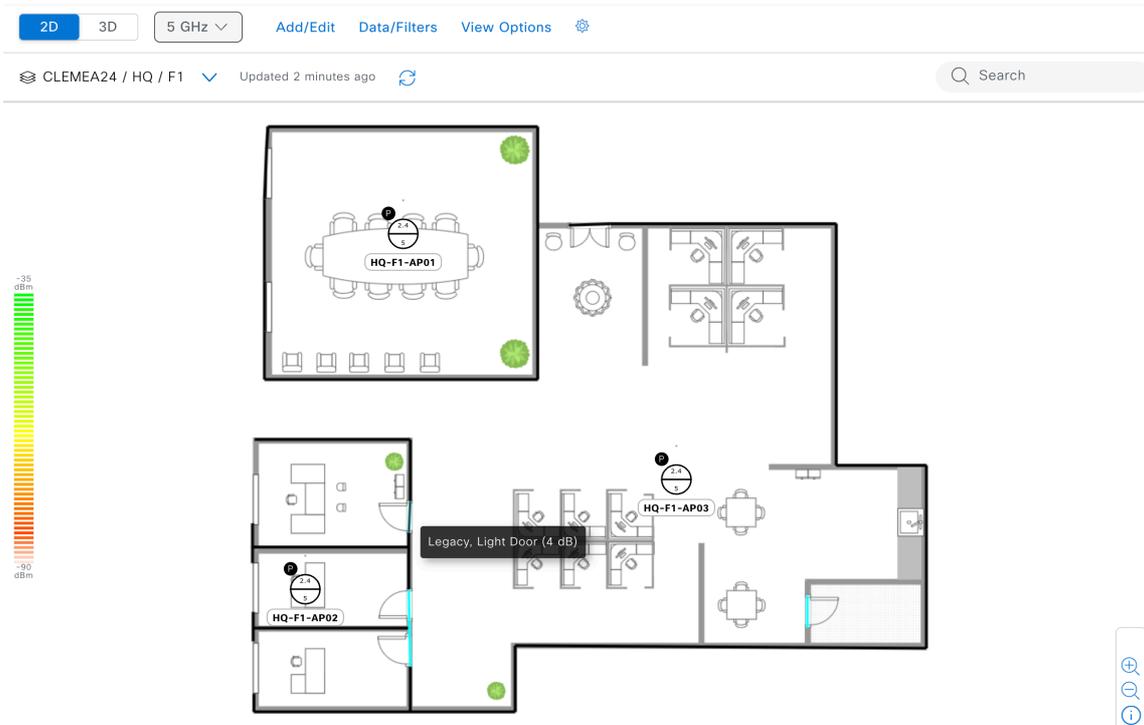


Please note that at this point in time, all the APs have the “P” icon which means they are Planned and not mapped to any physical APs.

## Step 2: Verify Ekahau Project Import Verification

In order to make sure that all the floor characteristics were carried over when importing our Ekahau design, let us review some of the possibilities available in Site Hierarchy. We will hover over one of the doors in light blue that was created in the .esx design:

Figure 18 Network Hierarchy - Wall Attenuation



As we can see the attenuation values associated with each of the walls were carried over when importing the .esx design.



Please refer to the **Cisco Catalyst Center Compatibility Matrix** for the compatible versions of Ekahau and Catalyst Center. This lab is based on the Ekahau AI Pro 11.0.2 and Catalyst Center 2.3.5.5

## Task 3: Prime Infrastructure to CATALYST CENTER Migration

In order to support customers migrating from Prime Infrastructure to Catalyst Center, this task will guide you through the procedure needed to migrate your network hierarchy from Prime Infrastructure to Catalyst Center. This task will focus on Remote branch of the company.

### Step 1: Verify Site Maps in Prime Infrastructure

Site Hierarchy was already pre-created in Prime Infrastructure. In order to take a look at the Site Maps for our Remote Branch location, navigate to the GUI of Prime Infrastructure <https://198.18.136.100>



Google Chrome is the recommended browser for this task

**username:** root

**password:** @Dm!n12345

Ignore any licensing warnings and Go to **Maps > Site Maps (New!)**

This is the view of the RB site that was created beforehand in Prime Infrastructure:

**Figure 19 Prime Infrastructure - Site Maps**

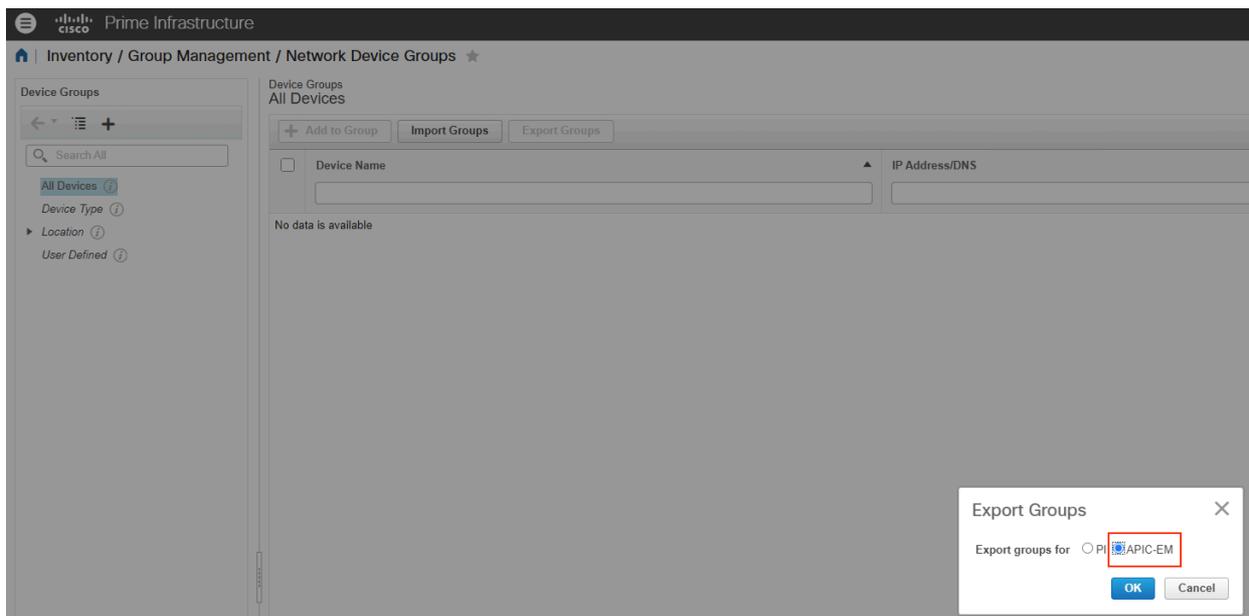


## Step 2: Export Prime Infrastructure Device Groups

We will now export Device Groups from PI so they can be then reused when importing to Catalyst Center.

Navigate to **Inventory > Network Device Groups** and select **Export Groups** and select **APIC-EM**.

**Figure 20 Prime Infrastructure – Device Group Export**



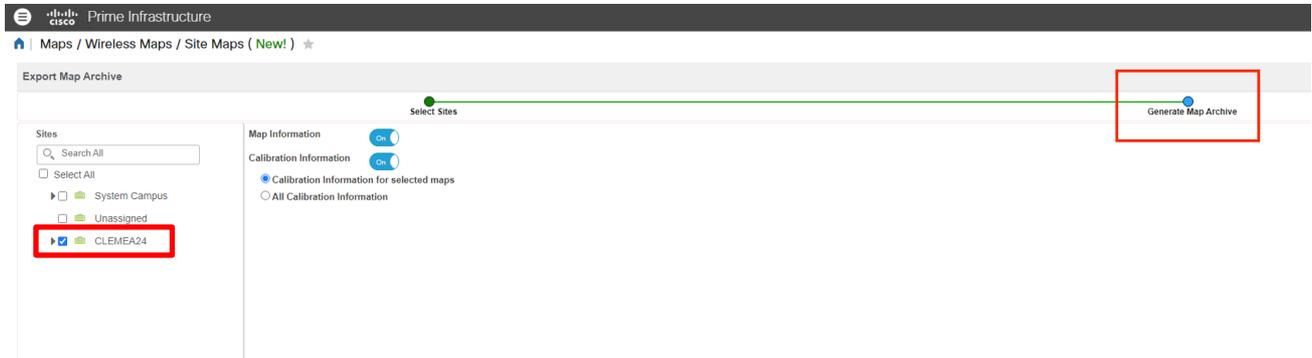
CSV file will be automatically saved to your workstation/jumphost.

## Step 3: Export Prime Infrastructure Site Maps

We will now export Site Maps from PI so they can be then reused when importing to Catalyst Center.

Navigate to **Site Maps (New!) > Export > Map Archive** and select **CLEMEA24** area.

**Figure 21 Prime Infrastructure - Map Archive Export**



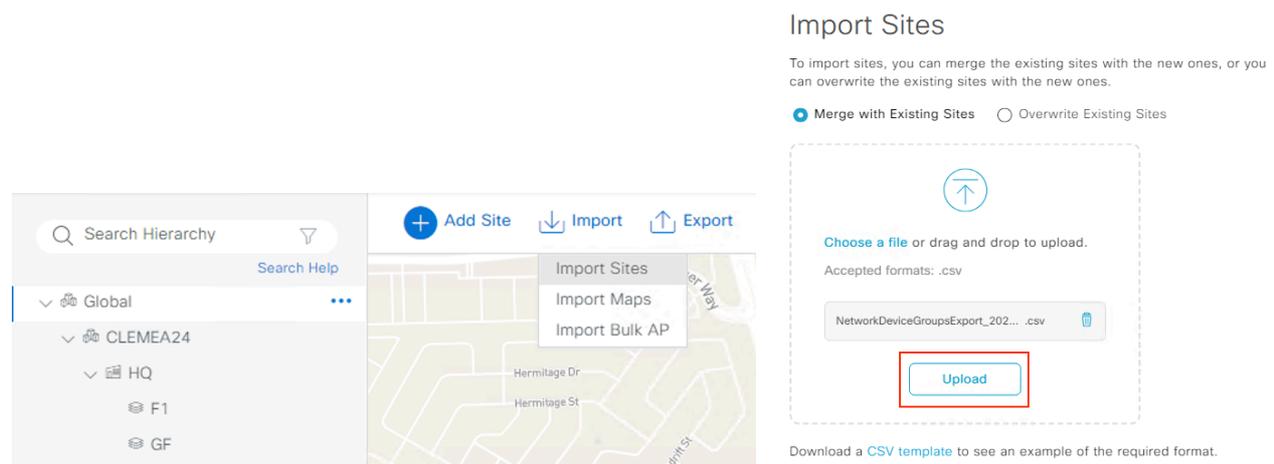
Click on **Generate Map Archive**. Tar.gz file will be automatically saved to your workstation/jumphost.

#### Step 4: Import Prime Infrastructure Device Groups to Catalyst Center

We will now import Device Groups into Catalyst Center.

- Navigate to **Design > Network Hierarchy > Global > Import > Import Sites**
- choose the **Merge with Existing Sites** option.
- Select the **CSV file** that was exported from Prime Infrastructure for **CLEMEA24** area and click **Upload**.

**Figure 22 Catalyst Center - Device Group Import**



Once Uploaded, site hierarchy with newly added locations will appear, click on **Import**.

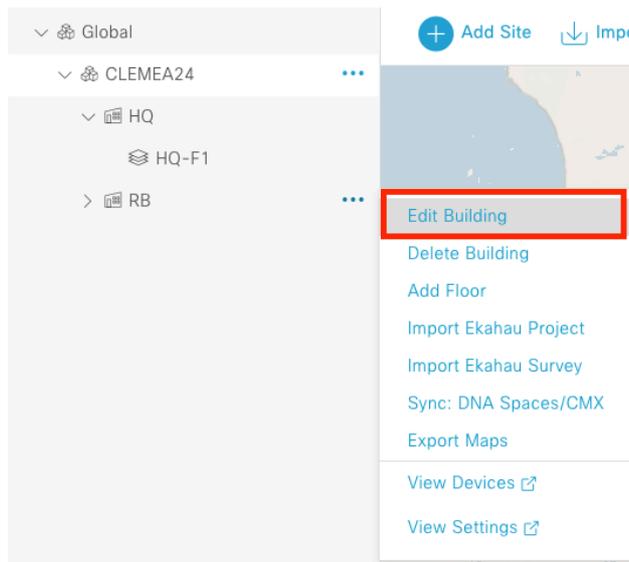
Figure 23 Catalyst Center - Sites Import



Click **OK** when asked “Merge with Existing Sites”

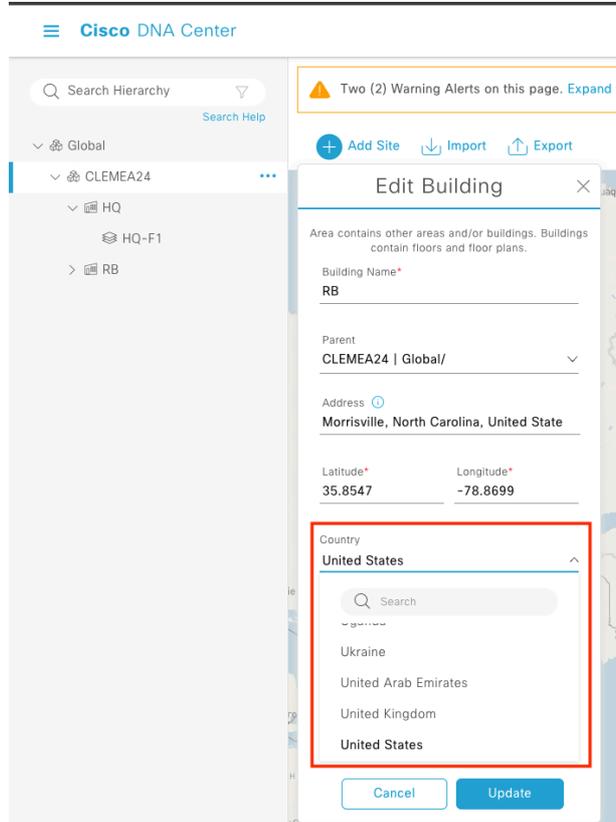
Once imported, we will proceed by setting correct **Country** for the RB location. Select **Edit Building** when hovering over three dots next to **RB** building:

Figure 24 Edit Building - Country



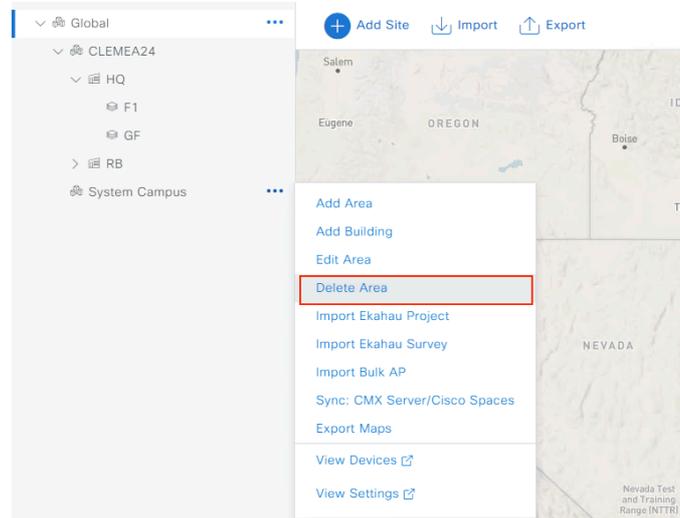
We will set the **Country** to **United States** to comply with the APs available in the lab:

Figure 25 Edit Building - Country



To keep site Catalyst Center hierarchy clean, you can remove the **System Campus** imported from PI by deleting the **System Campus Area**

**Figure 26 Hierarchy - Removing System Campus**



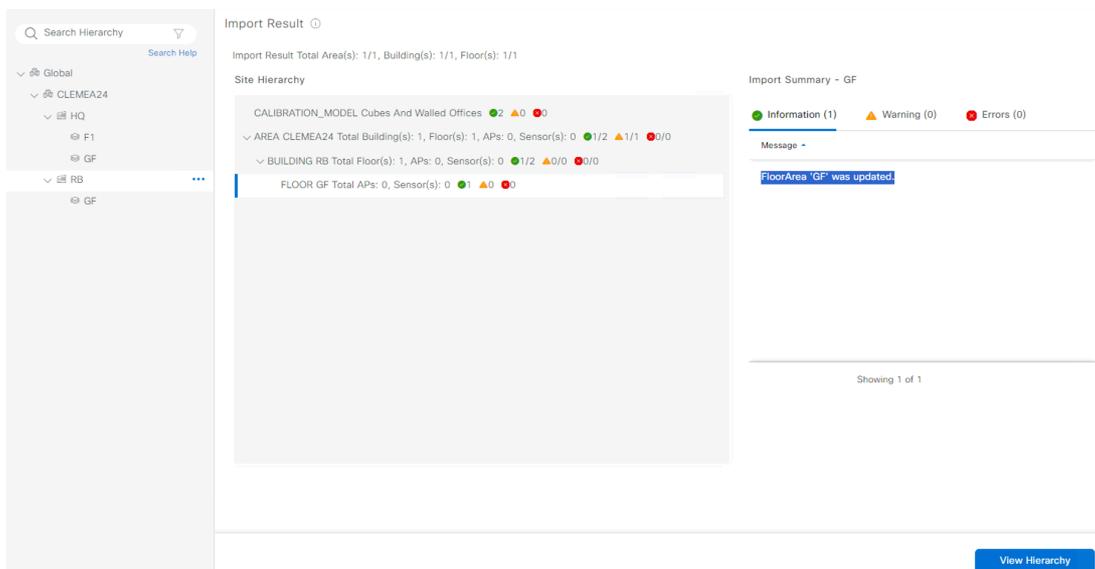
## Step 5: Import Prime Infrastructure Map Archive to Catalyst Center

We will now import Site Maps Archive into Catalyst Center.

- Navigate to **Design > Network Hierarchy > RB > Import > Import Maps**
- select the tar.gz file that was exported from Prime Infrastructure for **RB** site.
- Click **Next** and then Click **View Hierarchy**.

At this point, your hierarchy should look as follows:

**Figure 27 Catalyst Center – Hierarchy Import for RB**



## Task 4: Hamina Integration with Catalyst Center

This task focuses on importing your Hamina design into Catalyst Center.

For customers adopting Hamina Wireless for their RF designs, there is a Beta feature that allows to export Hamina design and import it into Catalyst Center. Before we proceed, list of pre-requisites and requirements is presented:



Building and floor name in Hamina project should match the one in Catalyst Center. If not building or floor is present in Catalyst Center the import will fail.

As this activity requires paid Hamina subscription, the design was created for the participants beforehand and is stored on your Jumphost. Image below presents the view of the design.

Figure 28 Hamina Wireless - Design

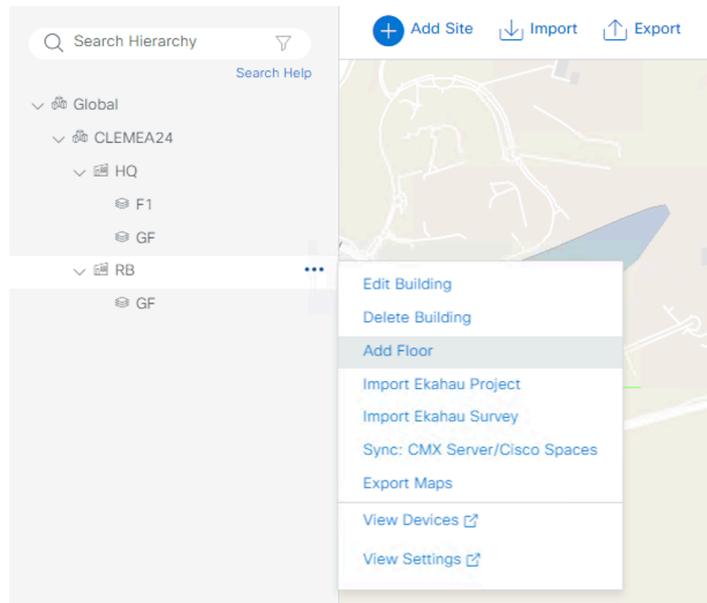


The same design was already exported according to the procedure found in the link <https://docs.hamina.com/planner/import-export/cisco-catalyst-center>

Before we import the file, we need to create the floor matching the floor name from Hamina design.

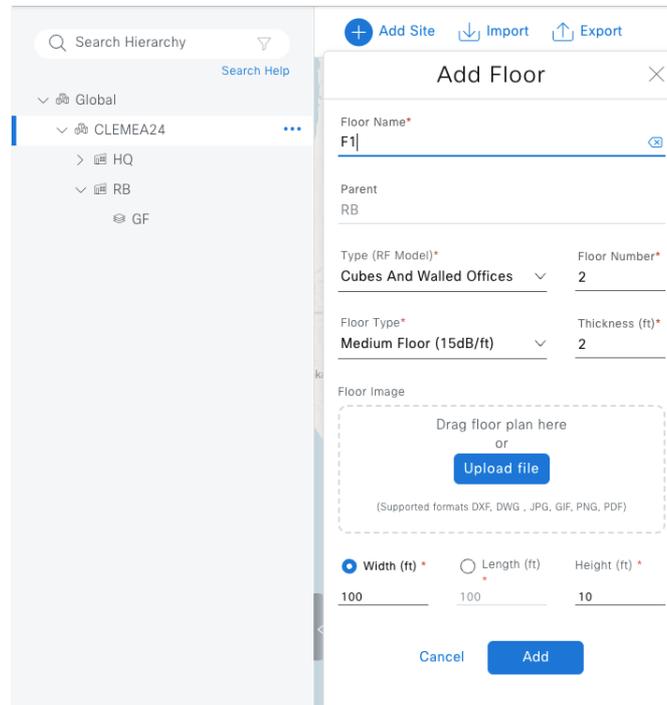
- Navigate to **Design > Network Hierarchy > RB**
- Select **Add Floor** under **RB** building

**Figure 29 RB - Add Floor**



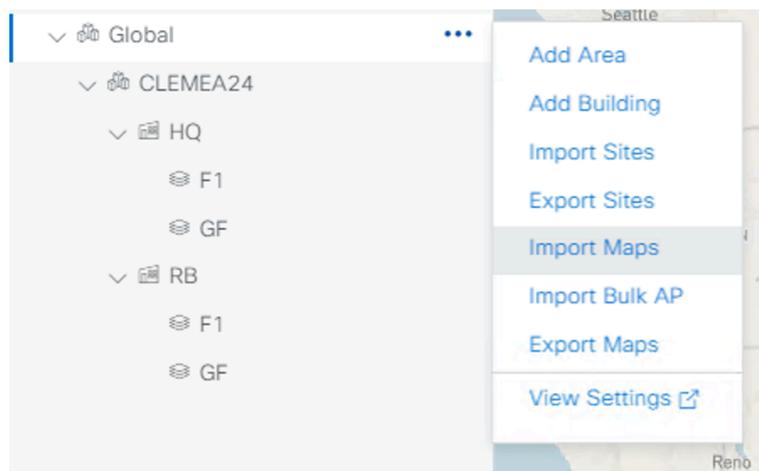
- Name the floor as **F1** and do not upload any floor plan as of now
- Click **Add**

**Figure 30 RB - F1 creation**



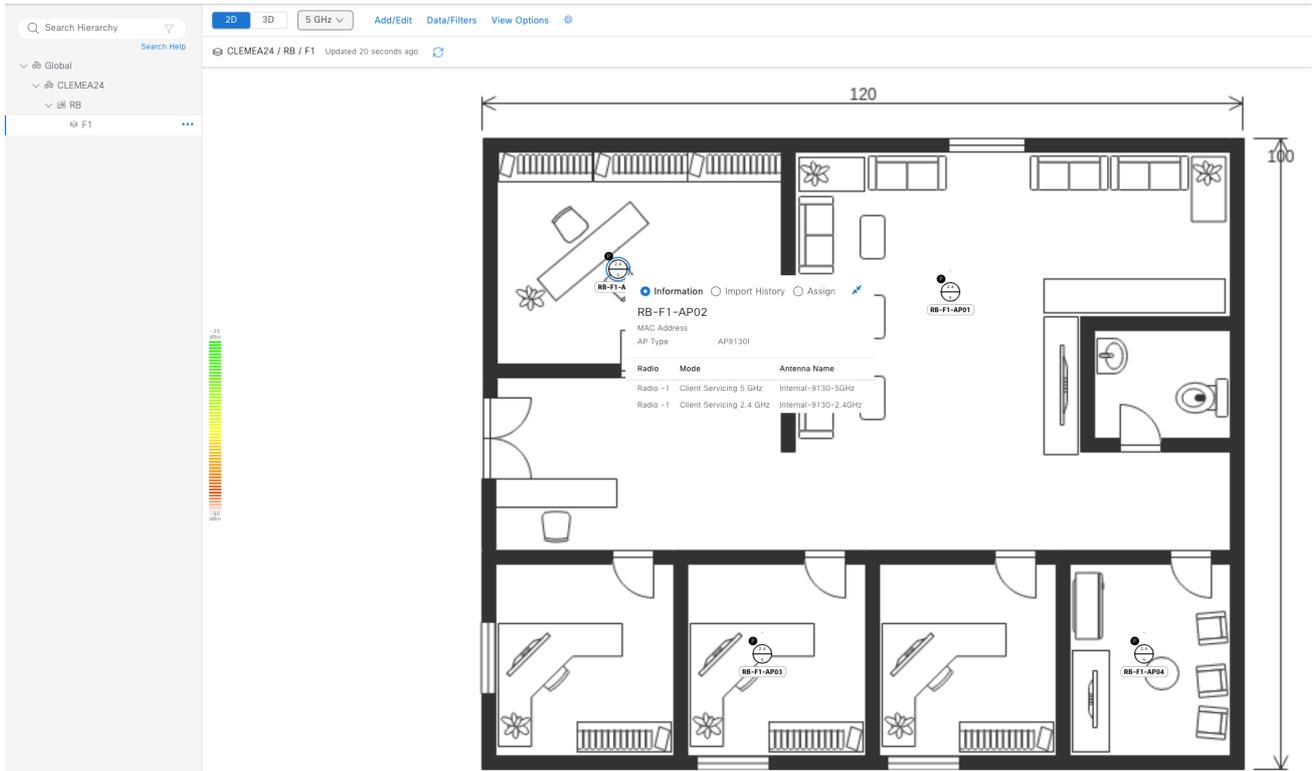
- Hover over three dots next to **Global** and select **Import Maps**

**Figure 31 Hamina - Import Maps**



- Select the file named **“HAMINA-IMPORT.tar.gz”** stored on the Jumphost, click **Import**
- Go through the summary to make sure the floors and APs will be imported successfully.
- A view of the imported floorplan will be as follows:

### Figure 32 Hamina - Floor Imported



Please note as this feature is still in development phase, it is currently missing following functionalities: Obstacles, including walls, are not carried over from Hamina Wireless to Catalyst Center

## Task 5: Add Wireless LAN Controller to Catalyst Center

The main goal of this task is to discover 9800 WLCs using Catalyst Center. WLCs are already deployed in the network, so we will make sure they have all the needed configuration for the discovery.

Once successfully discovered, they will be then assigned and provisioned for the first time to the corresponding locations.

### Step 1: Prepare the WLCs with the required configuration before performing the discovery

Before we will discover the WLCs using Catalyst Center, we will make sure that all the required configuration is present on the WLC. This will include:

- SNMP configuration
- AAA method lists
- NETCONF
- Admin username/password

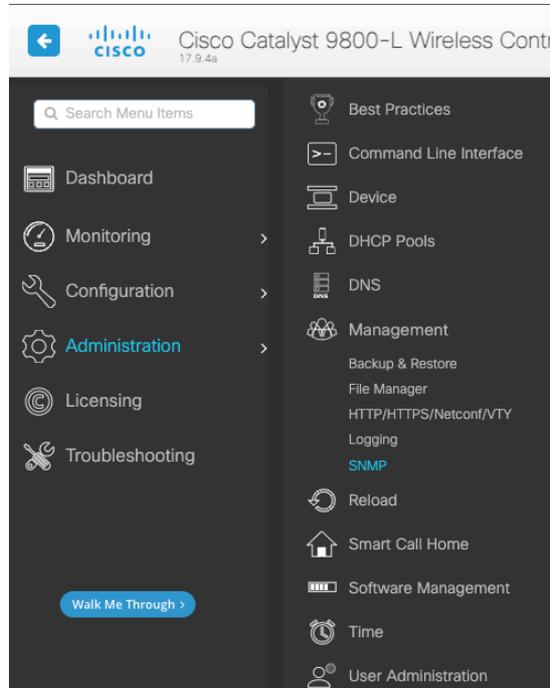
Navigate to the 9800 WLC GUI via <https://198.19.11.10>

**Username:** admin

**Password:** C1sco12345

Then go to **Administration >Management> SNMP**

**Figure 33 9800 WLC GUI - SNMP**



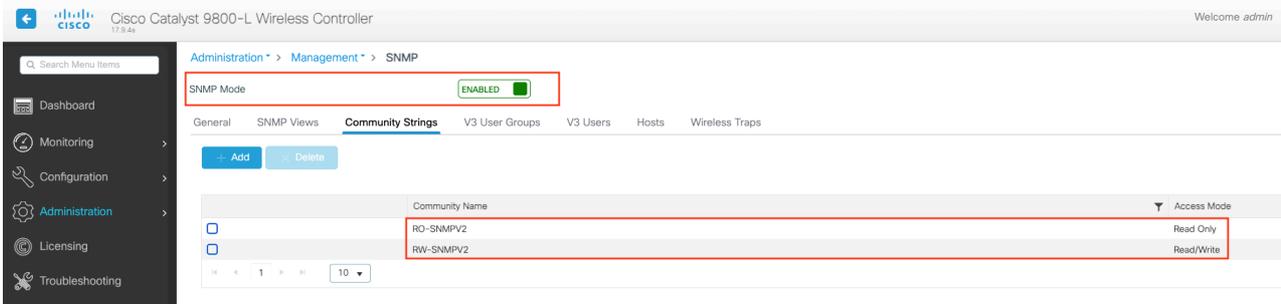
- **Enable** the SNMP Mode,
- then navigate to the **community strings** page and add two SNMPv2 communities:

**Table 4 WLC Discovery - SNMP Communities**

Community Name	Access Mode
<b>RO-SNMPV2</b>	Read Only
<b>RW-SNMPV2</b>	Read/Write

The configuration of SNMPv2 required on the 9800 WLC is summarized in the picture below:

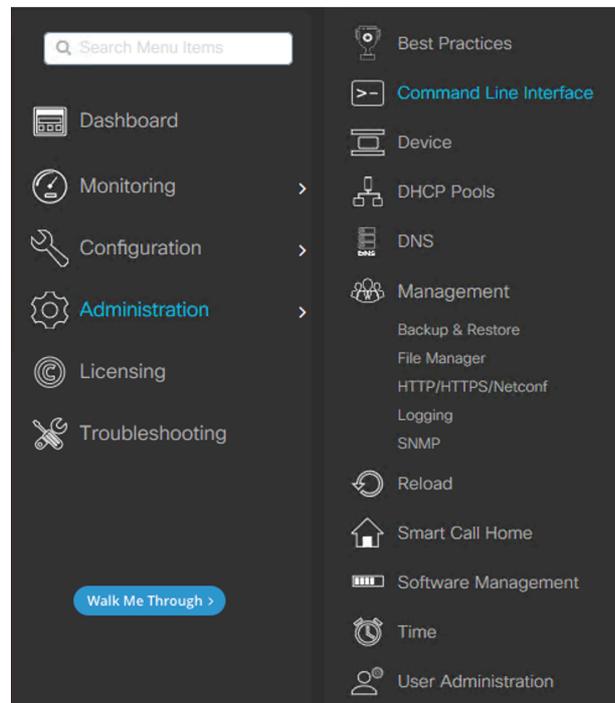
### Figure 34 SNMPv2 Configuration



For Catalyst Center to communicate with WLC 9800, we need to **enable NETCONF** and **enable local authorization** profile on C9800.

The simplest way to achieve this is to navigate from C9800 GUI **Administration > Command Line Interface**

### Figure 35 WLC 9800 - CLI via GUI



This page is just like a CLI (SSH session) from GUI.

Click **“Configure”**, then paste the below commands and execute **“Run Command”**

```
netconf-yang
aaa authorization exec default local
username dnaadmin privilege 15 password 0 C1sco12345
```



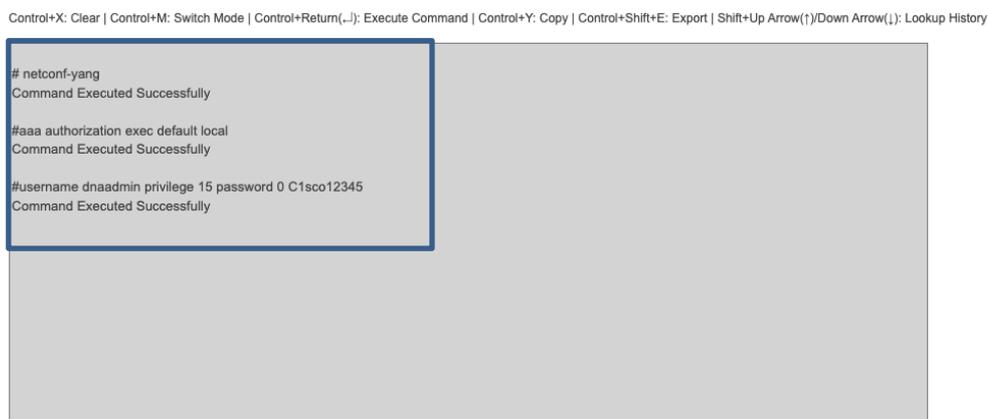
**Note:** This new username is to support Catalyst Center password requirements for HTTPS access.

**Figure 36 9800 WLC - CLI Commands**



Once executed, the output should look as follows:

**Figure 37 9800 WLC - CLI Execution**



WLC 9800 is now prepared for Catalyst Center Discovery.

## Step 2: Add WLC to Catalyst Center Inventory

This step will focus on discovering the WLC using Catalyst Center.

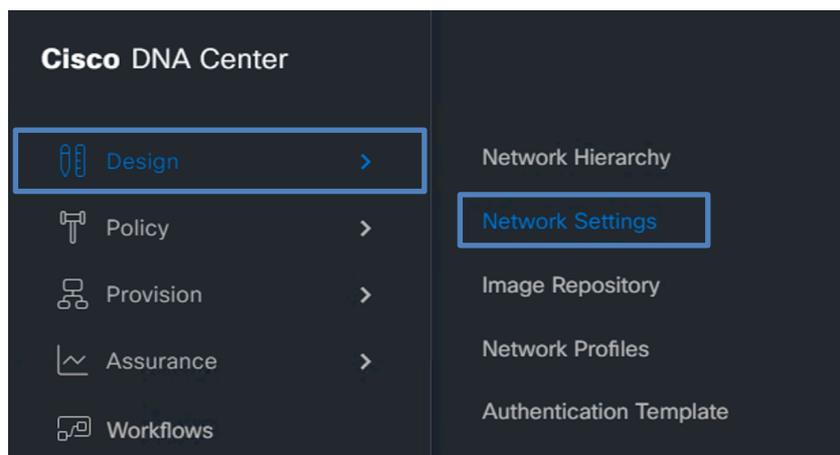
Log into Catalyst Center GUI using <https://198.18.129.100/> using credentials:

**Username:** admin

**Password:** C1sco12345

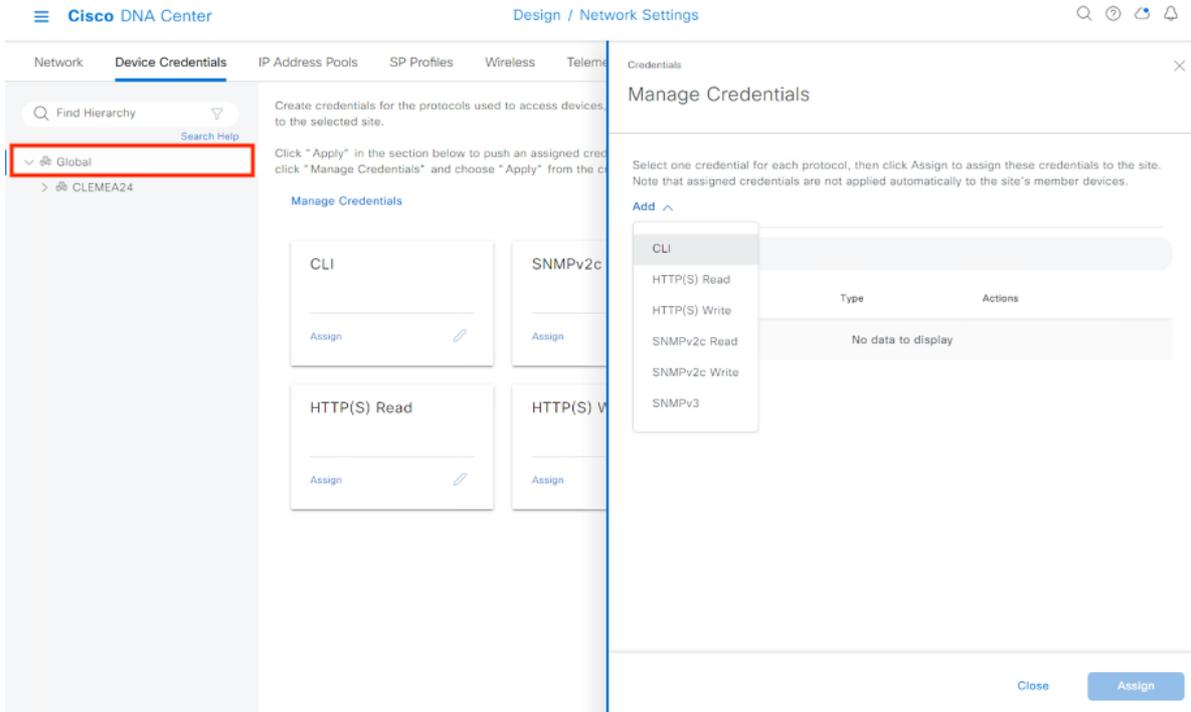
Navigate to the Dashboard top menu and click on **Design > Network Settings**

**Figure 38 Catalyst Center – Design – Network Settings**



- Under **Global** hierarchy, go to **Device Credentials**
- Click **Manage Credentials** then click **Add > CLI**

**Figure 39 Device Credentials**



Populate the information with the information from below table.

**Table 5 WLC Discovery – Details**

CLI Name / description	Username	Password / Enable Password	Assign Credentials to Site Global
CLI dnaadmin	dnaadmin	C1sco12345	[✓]



For 9800 WLCs, CLI, SNMP and Netconf configuration is Mandatory.



HTTPS Read Write credentials are also pre-configured but they are not needed, these credentials are used for App hosting and Meraki dashboard (not used in this lab)

## Figure 40 Catalyst Center – CLI Credentials Example

[Credentials](#) / [Add New Credential](#)

### CLI

Name / Description\*

CLI dnaadmin

Username\*

dnaadmin

[View Username Policy](#)

Password\*

\*\*\*\*\*

[SHOW](#)

[View Password Policy](#)

Enable Password

\*\*\*\*\*

[SHOW](#)

[View Password Policy](#)

Assign credential to site **Global**



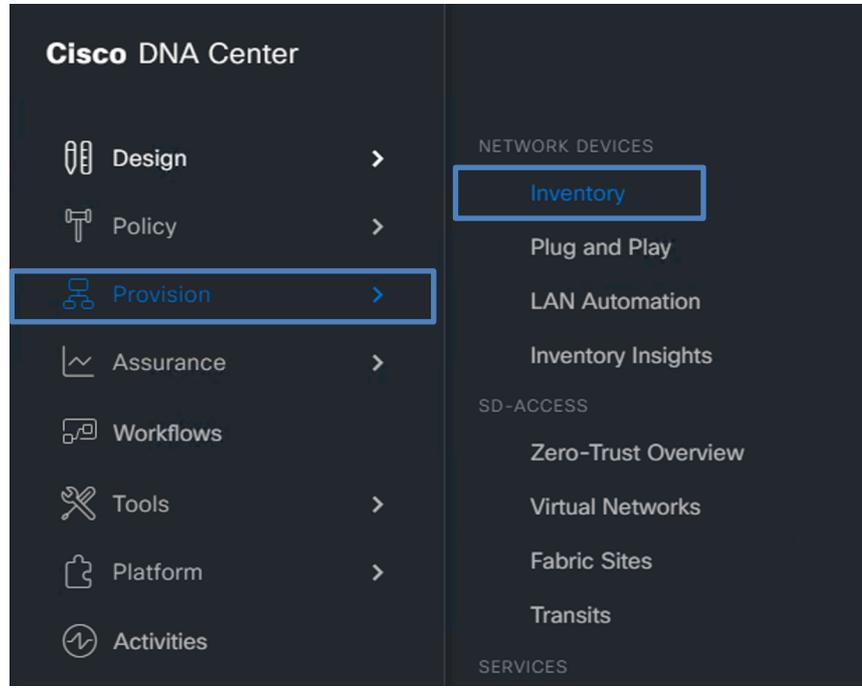
We prefilled SNMP, only insert CLI Credentials 😊

### Table 6 WLC Discovery - SNMP Communities

SNMPv2 Name	Community	Assign Credentials to Site Global
SNMPv2 Read	RO-SNMPV2	[✓]
SNMPv2 Write	RW-SNMPV2	[✓]

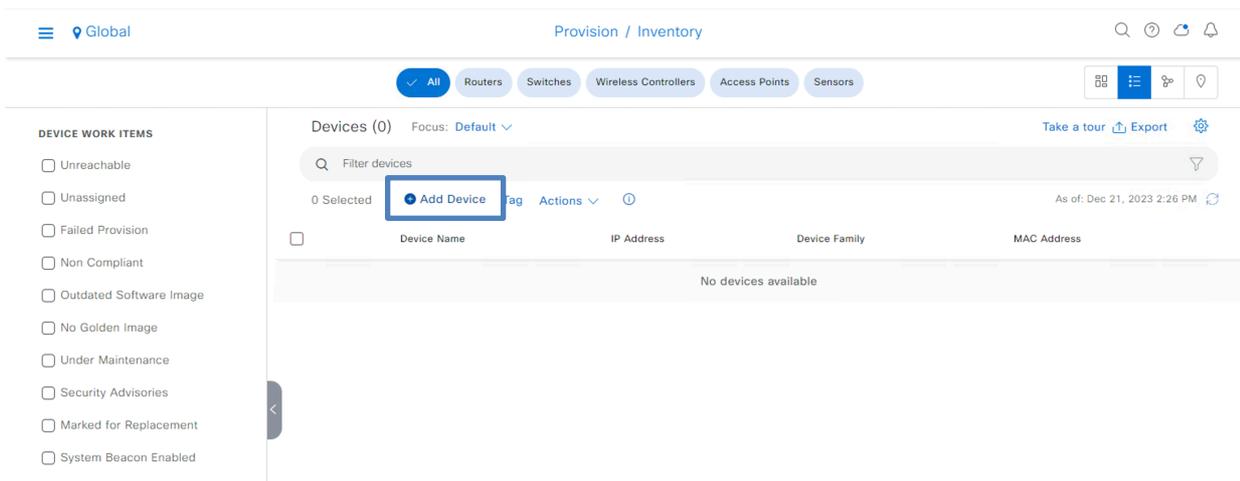
When finished with the network credentials, navigate to the Dashboard top menu and click on **Provision > Inventory**

Figure 41 Catalyst Center - Provision - Inventory



On the Inventory page, click “Add Device”

Figure 42 Catalyst Center - Inventory - Add Device



- Enter the WLC details as configured previously on the WLC 9800.
- WLC IP address: **198.19.11.10**
- Select the **Global credentials** for **CLI**

- Select the **"Write" Global credentials for SNMP**
- Make sure to use NETCONF port **830**

## Figure 43 Provision - Add Device Details

### Add Device

Type \*  
Network Device

Device IP / DNS Name\*  
198.19.11.10

Credentials [Validate](#)

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\*  
CLI dnaadmin

SNMP\*

Select global credential  Add device specific credential

V2C

Credential\*  
SNMPv2 Write | Write

SNMP Retries and Timeout\*

Retries\* 3 Timeout (in Seconds)\* 5

HTTP(S)

NETCONF

Port  
830

Note: NETCONF with user privilege 15 is mandatory for enabling Wireless Services on Wireless capable devices such as Catalyst 9000 series Switches and C9800 Series ~~Controllers~~ Controllers. The NETCONF credentials are required to connect to C9800 Series ~~Controllers~~ NETCONF Controllers as the majority of data collection is done using NETCONF for these Devices.

Protocol

Specify the protocol to use for this device.

SSH2  Telnet

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](#)

[Cancel](#) [Add](#)

Click **“Add”** and the device will get added to the cisco CATALYST CENTER inventory.



It may take couple of minutes for the WLC to appear on this page.

Once the Discovery runs successfully refresh the inventory page and validate that the device is in a **“Managed”** state.

### Figure 44 Inventory - Discovered Devices

The screenshot shows the Cisco Catalyst Center 'Provision / Inventory' page. It features a navigation bar with tabs for 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. The 'Wireless Controllers' tab is selected. Below the navigation bar, there is a search bar and a table of discovered devices. The table has columns for 'Device Name', 'IP Address', 'Device Family', and 'MAC Address'. Two devices are listed: 'AP\_4800-1' (Unified AP) and 'WLC1' (Wireless Controller).

Device Name	IP Address	Device Family	MAC Address
AP_4800-1	10.0.101.11	Unified AP	14-db:e6:21-b9:20
WLC1	198.19.11.10	Wireless Controller	00:1e:bd:4e:d8:ff

WLC 9800 is now added to Cisco Catalyst Center.



The RB AP should be joined to the WLC and should appear in the Catalyst Center Inventory too. Ask your proctor for help if AP is not joined to WLC.

### Step 3: Configure Network Profiles

In order to bond the wireless settings with the hierarchy, we must prepare two **Network Profiles** to support **HQ** and **RB** locations.

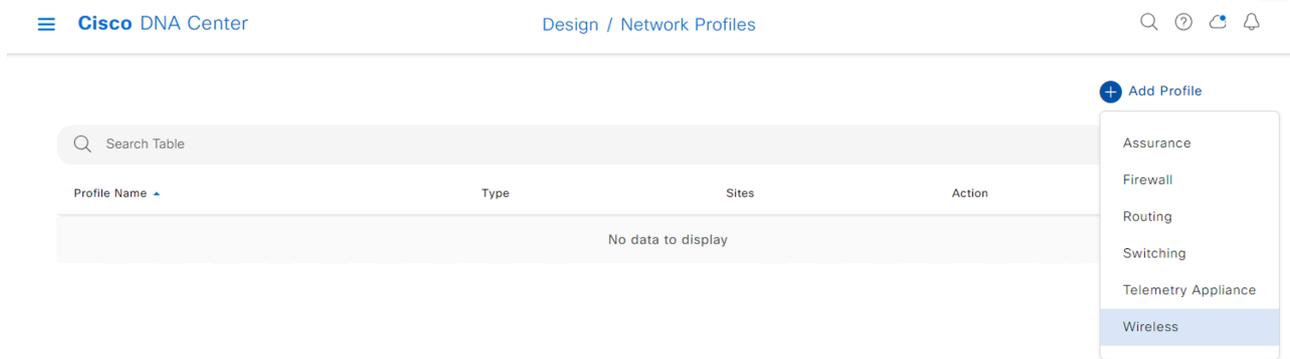
Network Profiles help users to group site-specific settings and map them to the desired locations.



Network Profiles are also a requirement for AP joining via Plug and Play PnP (Task 6)

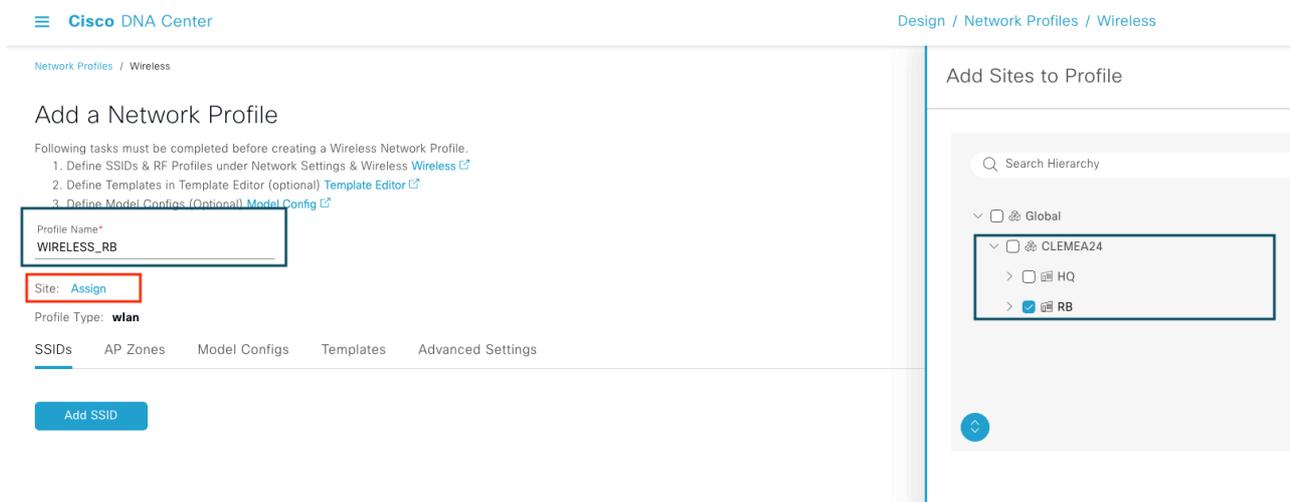
- Go to **Design > Network Profiles**,
- click on **Add Profile > Wireless**

## Figure 45 Network Profiles - WIRELESS\_RB



- Create profile named **WIRELESS\_RB**:
- Click **Assign** and select the RB site from the hierarchy.
- Click on **Save**

## Figure 46 Network Profiles - WIRELESS\_RB



Repeat the procedure for HQ Network Profile using following values the name **WIRELESS\_HQ**:

Table 7 Network Profiles – WIRELESS\_HQ

Parameter	Value
Profile Name	WIRELESS_HQ
Site	Global > CLEMEA24 > HQ

Once created, your Network Profiles should look as follows:

**Figure 47 Network Profiles - Summary**

The screenshot shows the Cisco DNA Center interface for Network Profiles. The breadcrumb path is "Design / Network Profiles". There is a search bar and an "Add Profile" button. The table below lists two network profiles:

Profile Name	Type	Sites	Action
WIRELESS_HQ	Wireless	3	Edit   Delete
WIRELESS_RB	Wireless	3	Edit   Delete

At the bottom of the table, it indicates "2 Records", "Show Records: 10", and "1 - 2".

With this Network Profile configuration is enough for PnP, but we'll come back to this element in a later section of the lab.

#### Step 4: Assign to site and Provision WLC for the first time.

Provisioning is nothing more than pushing configurations to the WLC that were intended.

For now, as there is not any wireless configuration yet, Catalyst Center will push the information needed for **Device Controllability** (enabled by default) which includes the following depending on the process:

- Device Discovery
  - o SNMP Credentials
  - o NETCONF Credentials
  
- Adding Devices to Inventory
  - o Cisco TrustSec (CTS) Credentials (if the Global site is configured with Cisco ISE as AAA).
  
- Assigning Devices to a Site
  - o Controller Certificates
  - o SNMP Trap Server Definitions
  - o Syslog Server Definitions

- NetFlow Server Definitions
- Wireless Service Assurance (WSA)
- IPDT Enablement

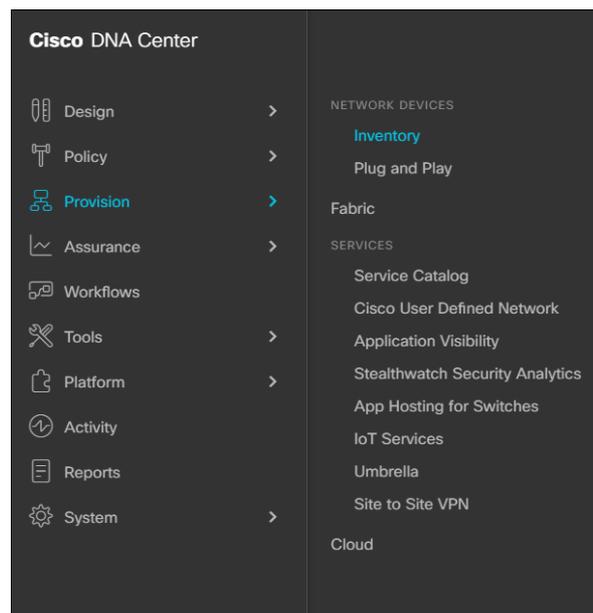


This is an important process in this lab as it is required for other sections in the lab and will be repeated as we progress through the tasks to push intended configuration to WLC and APs.

During the **Provisioning** process the WLC will also be **Assigned to Site**

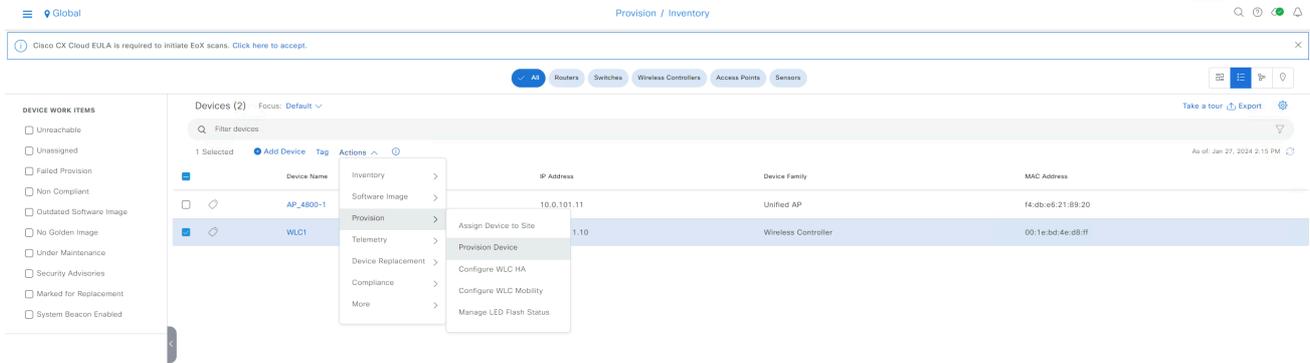
For this, click on the **Provision > Inventory** tab

**Figure 48 Assign to site and Provision**



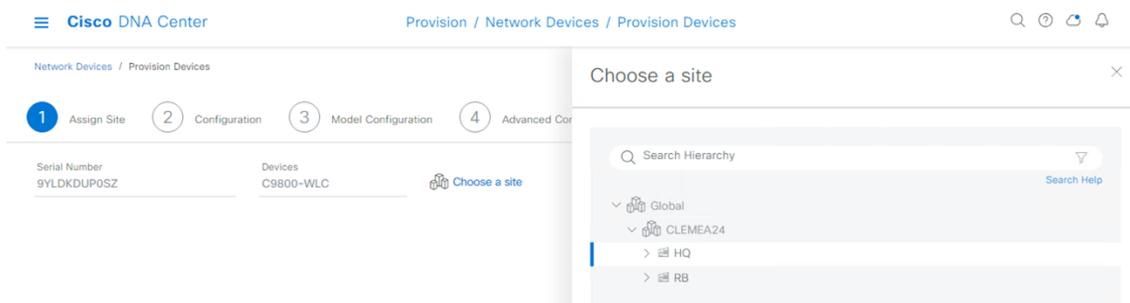
Select the WLC and hover over “**Actions**” field and navigate to “**Provision**” and then to “**Provision Device**”.

**Figure 49 Assign to site and Provision**



Click **“Choose a Site”** and add device to **HQ** Building

**Figure 50 Assign to site and Provision**



Click **Save** and **Next**

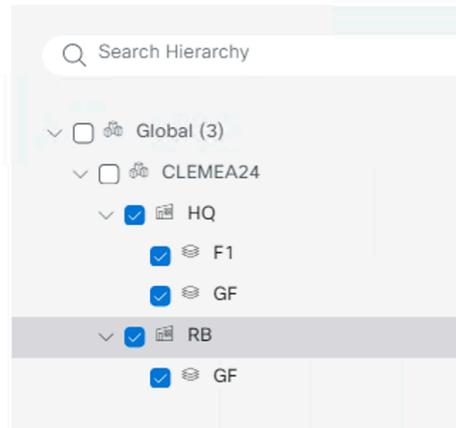


Note: Ignore any warnings about ISE, at the moment we do not intend to push any SSID config.

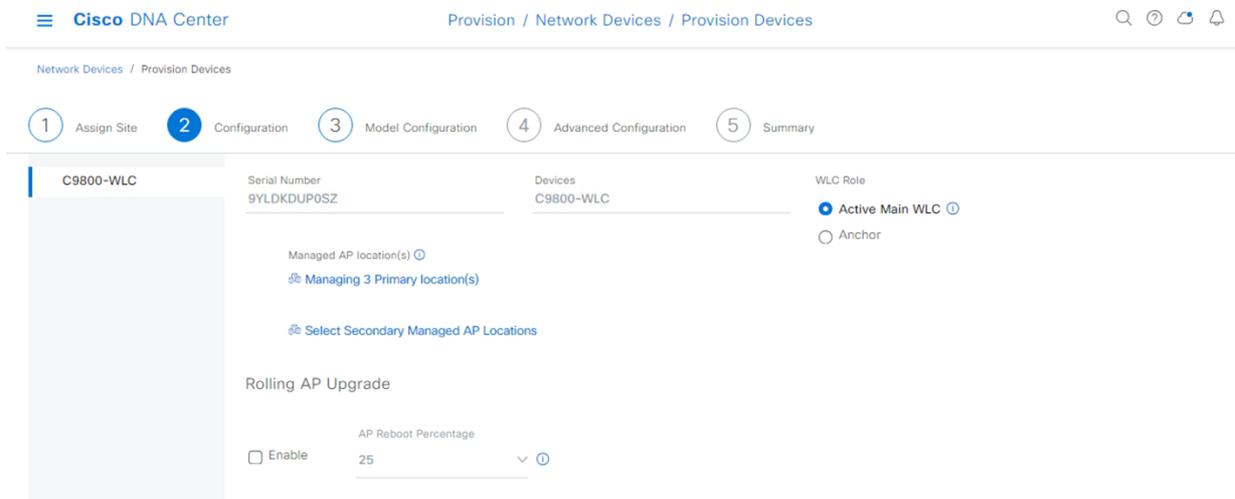
- On the **“Configuration”** step, edit **“Select Primary Managed AP Locations”**,
- click **HQ** and **RB** buildings,
- then click **Save**
- then click **Next**

**Figure 51 Assign to site and Provision**

## Managed AP Location ⓘ



**Figure 52 Assign to site and Provision**



Skip past **“Model Configuration”** and **“Advanced Configuration”** and head into **“Summary”**

**Figure 53 Assign to site and Provision**

**Cisco DNA Center** Provision / Network Devices / Provision Devices

Network Devices / Provision Devices

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

**C9800-WLC**

- Default AP Profile (Default\_AP\_Profile\_Aireos/default-ap-profile) will be applied to all Cisco DNA Center generated AP Groups/Site Tags
- Warning: Cisco DNA Center will clean up unused custom Site Tags/ Policy Tags, which does not have any Cisco DNA Center provisioned Access Points. Any out of band configurations using these tags will be impacted post this provision.

**Device Details**

Device Name:	C9800-WLC
Platform Id:	C9800-CL-K9
Device IP:	198.18.134.100
Device Location:	Global/CLEMEA24/HQ
Device Role:	Active Main WLC
Associated Anchor device(s)	None

**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.
Syslog Server	Cisco DNA Center
Netflow Collector	(Not configured)
Cisco TrustSec (CTS) Credentials	No
Wireless Streaming Telemetry	Yes
SNMP Trap Receiver	Cisco DNA Center
DNS Server	(Not configured)
DTLS Ciphersuite	Skipped

Cancel Deploy

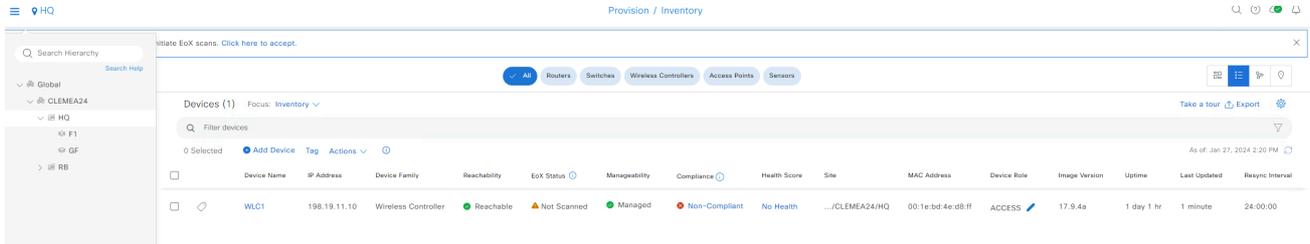


Warning: Cisco DNA Center will clean up unused custom Site Tags and Policy Tags **which do not have any configured Access Points**. Any out of band configurations using these tags will be impacted post this provision.

Click **“Deploy”** and Click **“Apply”** Now

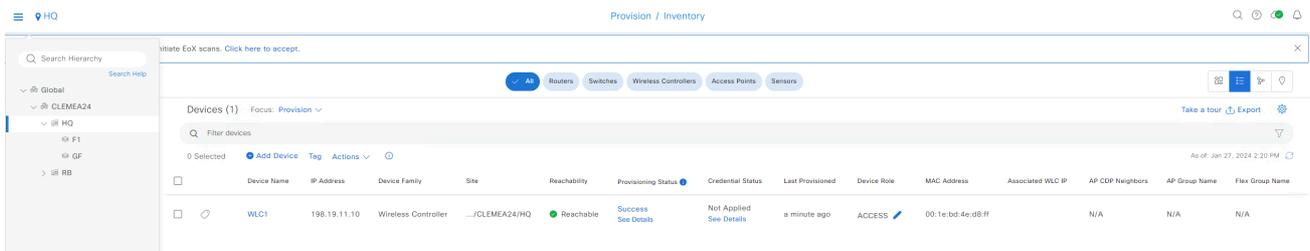
Validate if the provisioning was successful by clicking in **HQ** in the hierarchy and confirming the WLC is placed there.

Figure 54 Assign to site and Provision.



Change the filter to **Provision**, Status must be **"Success"**.

Figure 55 Assign to site and Provision.



The device will now start syncing telemetry data with Catalyst Center, use the Device 360 view to discover all the information gathered.

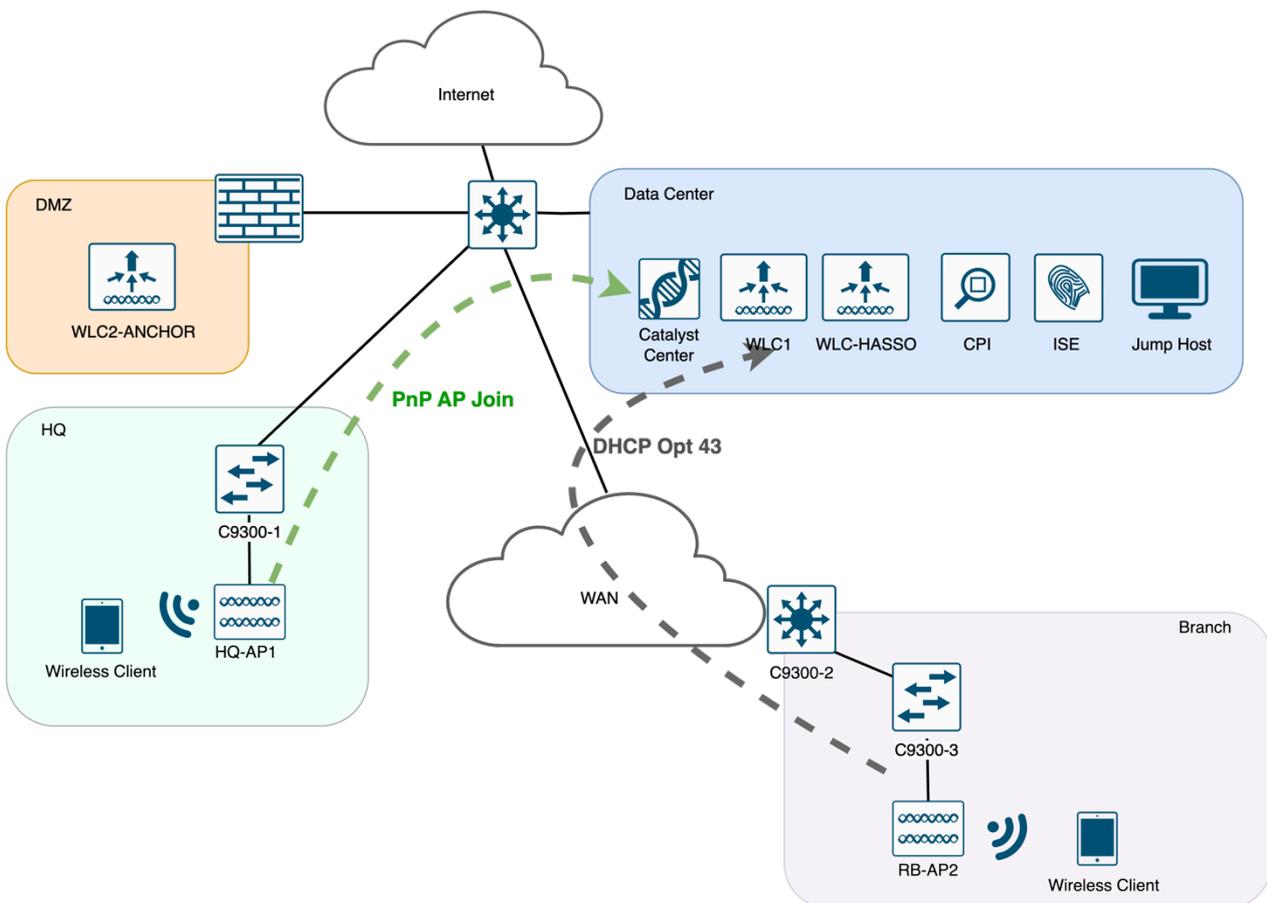
Click the **device name**, then click **"View 360"**.

## Task 6: Access Point Discovery

Having discovered the WLCs in the previous task, we will now progress to the AP discovery to make sure they are ready to be configured and service wireless clients. This task will cover two main AP discovery methods:

- **Remote Branch (RB)**
  - AP joining the WLC using DHCP Option 43 and Catalyst Center discovering the AP as part of WLC inventory sync.
  
- **Head Quarters (HQ)**
  - Claiming the AP via PnP workflow available in Catalyst Center

**Figure 56 AP Discovery Methods**



## AP Joining via DHCP Opt 43

AP located in the Remote Branch will join the WLC using one of the most widely adopted WLC Discovery mechanisms, DHCP Option 43.

Here is the **snippet** of the DHCP Pool configured for the APs on **9300-3**:

```
ip dhcp pool AP_Remote_Pool
 network 10.0.101.0 255.255.255.0
 default-router 10.0.101.1
 dns-server 198.18.128.1
 option 43 hex f104c6128664
 !!! WLC ip is 198.19.11.10 that translates to hex of c6130b0a

ip dhcp excluded-address 10.0.101.1 10.0.101.10
 !!!Excludes 1 to 10 from pool
```

This AP obtains the IP address in the VLAN 101, the port where it connects is trunk needed for FlexConnect scenario.

Here is the **snippet** of the switch **9300-2** at port Gig 1/0/2.

```
Conf t
int gig1/0/2
 Switchport mode trunk
 Switchport trunk native vlan 101
 Switchport trunk allowed vlan add 101, 102, 103
No shut
```

The AP should obtain IP address from the 10.0.101.x network and should join the WLC.

If all goes well, the Remote Branch AP should be now visible in the Inventory as discovered by Catalyst Center via WLC Inventory sync.

Figure 57 AP Joined via DHCP Opt 43

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The top navigation bar includes the Cisco logo, the controller name 'Cisco Catalyst 9800-CL Wireless Controller 17.9.4a', and a 'Welcome admin' message. The main dashboard area is divided into three sections: 'Network' with 6 GHz, 5 GHz, and 2.4 GHz indicators; 'Wireless LANs' with 0 indicators; and 'Access Points' with 1 indicator highlighted in a red box. Below the dashboard, there is a 'Provision / Inventory' section with a table of devices. The table has columns for Device Name, IP Address, Device Family, Reachability, EoX Status, Manageability, Compliance, Health Score, Site, MAC Address, Device Role, Image Version, Uptime, Last Updated, and Resync Interval. Two devices are listed: AP\_4800-1 and WLC1.

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site	MAC Address	Device Role	Image Version	Uptime	Last Updated	Resync Interval
AP_4800-1	10.0.101.11	Unified AP	Reachable	Not Scanned	Managed	N/A	10	Assign	14-8b-e6-21-89-20	ACCESS	17.9.4.27	1 day 1 hr	1 minute	N/A
WLC1	198.19.11.10	Wireless Controller	Reachable	Not Scanned	Managed	Non-Compliant	10	...	...ICLEMEA24/HQ 00:1e:bd:4e:d8:f	ACCESS	17.9.4a	1 day 1 hr	1 minute	24:00:00

## AP Joining via Plug and Play

In order for PNP to work, the following prerequisites are mandatory:

1. Define a Network Profiles.
2. Set the Cisco Smart Account
3. Accept the End User License Agreement (EULA)
4. Set PnP AP Location
5. Ready software images for SWIM



Prerequisite 1 was already addressed in the previous task, and the rest of them we already performed for you.

Feel free to go to **Catalyst Center Menu > System > Settings** and check the configurations that were added for you.

**Figure 58 System Settings – PnP Pre-requisites**

The screenshot shows the Cisco DNA Center interface. At the top left, there is a search bar with 'eula' entered. Below it, a list of search results is shown, with 'Device EULA Acceptance' selected. The main content area is titled 'Device EULA Acceptance' and shows the 'Cisco.com ID' field with a value that has been redacted. Below this, there is a checkbox labeled 'I have read and accept the Device EULA' which is checked. A 'Save' button is located at the bottom of the form.

## Step 1: Preparing DHCP Option 43 for AP PnP using Catalyst Center

For PnP to work we will also use Option 43 but pointing to the Catalyst Center IP address. The DHCP Pool for the HQ AP is already configured on the HQ's ISR.

- Snippet below presents configuration present on the device:

```
ip dhcp pool AP_PNP_Pool
 network 10.0.201.0 255.255.255.0
 default-router 10.0.201.1
 dns-server 198.18.128.1
 option 43 ascii "5A1N;B2;K4;I198.18.129.100;J80"
 !!! Catalyst Center IP is 198.18.129.100

ip dhcp excluded-address 10.0.201.1 10.0.201.10
 !!! Excludes 1 to 10 from pool
```

## Step 2: Testing the AP PnP process

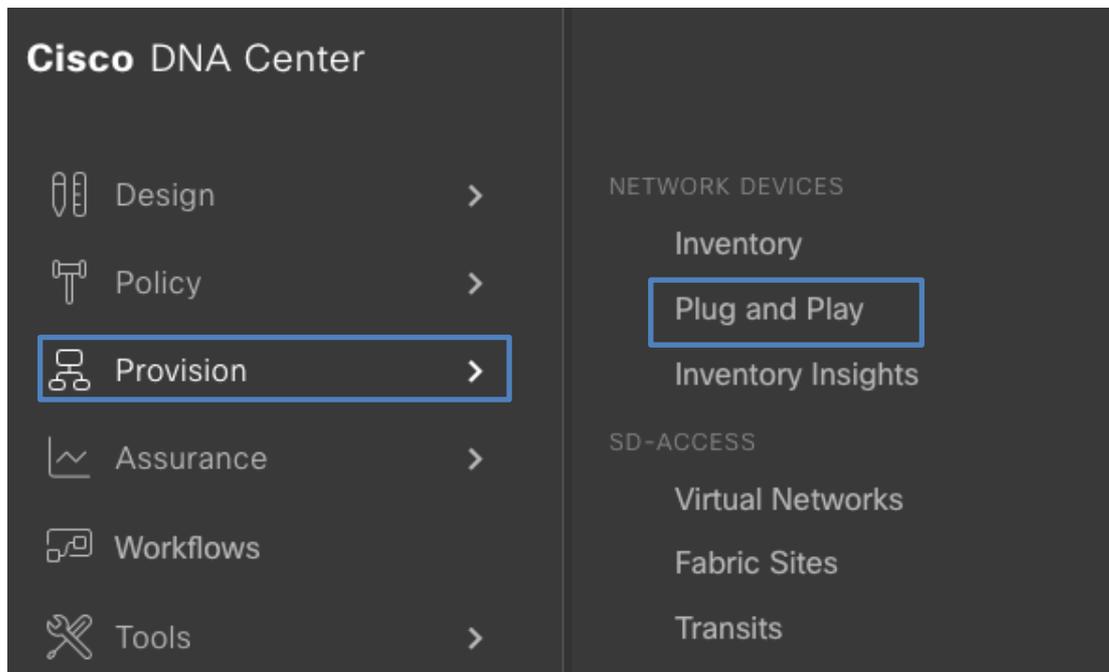
This AP obtains the IP address in the VLAN 201, the port where it connects is "access mode" needed for "local mode AP scenario".

Here is the **snippet** of the switch 9300-1 at port Gig 1/0/2 as access in VLAN 201.

```
Int gig1/0/2
Switchport mode access
Switchport access vlan 201
No shut
```

The HQ AP will be available after some time in the PnP Dashboard accessible via **Provision > Plug and Play**

**Figure 59 Provision - Plug and Play**



The AP will appear in the Unclaimed section.

## Figure 60 Provision - Plug and Play

Device Status: **Unclaimed (1)** Error (0) Provisioned (0) All (1)

Devices (1) Focus: Default Auto-refresh: 30 s

Search Table

0 Selected Actions + Add Devices As of: Dec 21, 2023 4:48 PM Refresh

#	Device Name	Serial Number	Product ID	IP Address	Source	State	Onboarding Progress	Site	Last Contact
1	AP7872.5DFB.8E78	FJC2234M44N	AIR-AP4800-B-K9	10.0.101.11	Network	Unclaimed	40%	NA	Dec 21, 2023 4:47:52 PM

Check the check box next to one or more wireless devices that you want to claim

From the menu bar above the device table, choose **Actions > Claim**.

## Figure 61 Plug and Play AP Claim

Device Status: **Unclaimed (1)** Error (0) Provisioned (0) All (1)

Devices (1) Focus: Default Auto-refresh: 30 s

Search Table

1 Selected Actions + Add Devices As of: Dec 22, 2023 8:12 AM Refresh

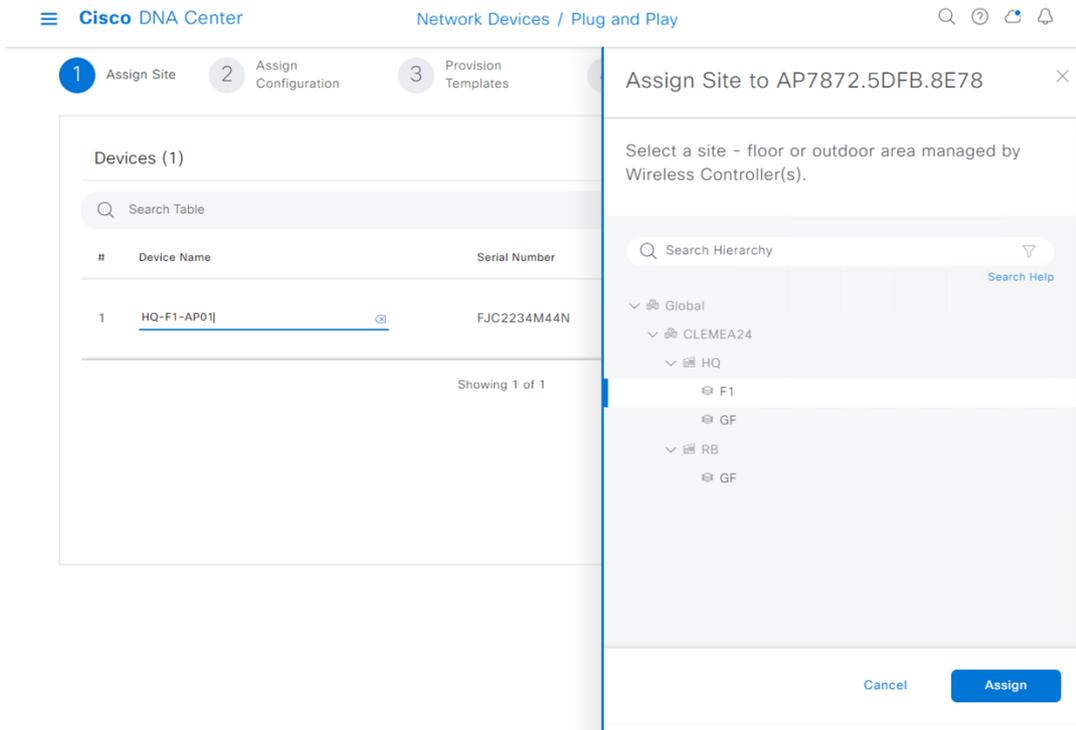
#	Device Name	Serial Number	Product ID	IP Address	Source	State	Onboarding Progress	Site	Last Contact
1	AP7872.5DFB.8E78	FJC2234M44N	AIR-AP4800-B-K9	10.0.101.11	Network	Unclaimed	40%	NA	Dec 22, 2023 8:11:54 AM

- Claim
- Edit
- Reset
- Delete
- Authorize

Change the AP name to **HQ-F1-AP01**

From the Select a Site drop-down list, choose **HQ > F1** then click **Assign**

**Figure 62 Plug and Play AP Claim**



Note: APs must be assigned to a floor with a wireless controller managing the building.

Click **Next**.

The Assign Configuration window opens.

For an AP device, in the Radio Frequency Profile drop-down list, choose **TYPICAL**

### Figure 63 Plug and Play AP Claim

Configuration for device name: HQ-F1-AP01

Serial Number: FJC2234M44N  
 Product ID: AIR-AP4800-B-K9  
 Assigned Site: Global/CLEMEA24/HQ/F1  
 Device Name: HQ-F1-AP01

Radio Frequency Profile\*: TYPICAL

#	Device Name	Serial Number	Product ID	Assigned Site
1	HQ-F1-AP01	FJC2234M44N	AIR-AP4800-B-K9	Global/CLEMEA24/HQ/F1

click **Save**

### Figure 64 Plug and Play AP Claim

AP Location will be **configured** as the assigned site as part of the provision during the claim process. To change this setting, go to [System -> Settings -> PnP AP Location](#).

After the setting is updated, click [Refresh](#)

Devices (1) Clear Configuration

#	Device Name	Serial Number	Product ID	Assigned Site	Configuration	Actions
1	HQ-F1-AP01	FJC2234M44N	AIR-AP4800-B-K9	Global/CLEMEA24/HQ/F1	RF Profile: TYPICAL	...

Cancel Back Next

Click **Next**

## Figure 65 Plug and Play AP Claim

The screenshot shows the Cisco DNA Center Provisioning interface. The breadcrumb navigation is 'Provision / Network Devices / Plug and Play'. The progress bar indicates four steps: 'Assign Site' (checked), 'Assign Configuration' (checked), 'Provision Templates' (active, step 3), and 'Summary' (step 4). A message box states: 'No action required on this step because no devices have been configured with a template. Click Next to proceed.'

The Summary window appears, where you can view details about the devices and configuration.

Click "**Preview Configuration**" to see the Tags to be pushed to WLC and assigned to AP.

## Figure 66 Plug and Play AP Claim

The screenshot shows the Summary window for device name: HQ-F1-AP01. It contains three sections: Day-0 Configuration Preview, Device Details, and Radio Frequency Profile.

Day-0 Configuration Preview	
primaryWlcIP	198.19.11.10
primaryWlcName	WLC1
policyTagName	PT_CLEME_HQ_F1_888ae
RFTagName	TYPICAL
siteTagName	default-site-tag

Device Details	
Device Name	HQ-F1-AP01
Serial Number	FJC25051K3K
Product ID	C9130AXI-B
Device Type	AP
Site	Global/CLEMEA24/HQ/F1

Radio Frequency Profile	
Radio Frequency Profile	TYPICAL

Click **Claim** and **Confirm operation**.



In the background Catalyst Center provisions the WLC with a Policy Tag and a Site Tag, then provisions the AP to the selected floor and assigns the AP the mentioned Tags.

See PnP process by Clicking the AP Name and go to History Tab

**Figure 67 Plug and Play AP Claim**

Device Name: HQ-F1-AP01 (SN: FJC2234M44N) ✕

---

SUDI Not Supported  Refresh

Status Executing User Workflow (00:56)

Details History Configuration

---

History As of: Dec 22, 2023 3:23 PM

Status	Time	Details	Info
	Dec 22, 2023 3:23:36 PM	Executing Task: Site Config Task	<a href="#">Info</a>
	Dec 22, 2023 3:22:34 PM	Executing User Workflow	<a href="#">Info</a>
	Dec 22, 2023 3:21:48 PM	Day 0 Config Generated	<a href="#">Info</a>
	Dec 22, 2023 3:21:33 PM	Day 0 Config Requested	<a href="#">Info</a>
	Dec 22, 2023 3:20:33 PM	Claimed Device	<a href="#">Info</a>
	Dec 22, 2023 9:14:56 AM	Task: System Task Completed	<a href="#">Info</a>
	Dec 22, 2023 9:14:53 AM	Executing Task: System Task	<a href="#">Info</a>
	Dec 22, 2023 9:14:53 AM	Executing System Workflow to Initialize Device	<a href="#">Info</a>

**Figure 68 Plug and Play AP Claim**

Device Status: **Unclaimed (1)** Error (0) Provisioned (0) All (1)

Devices (1) Focus: Default Auto-refresh: 30 s

Search Table

0 Selected Actions Add Devices As of: Dec 22, 2023 3:24 PM Refresh

#	Device Name	Serial Number	Product ID	IP Address	Source	State	Onboarding Progress	Site	Last Contact
1	HQ-F1-AP01	FJC2234M44N	AIR-AP4800-B-K9	10.0.101.11	Network	Onboarding	80%	Global/CLEMEA24/HQ/F1	Dec 22, 2023 3:



This process may take some minutes as AP may reboot in the claiming process.

When finished and successful, verify Config pushed to the WLC:

**Figure 69 Plug and Play AP Claim**

Monitoring > Wireless > AP Statistics

General Join Statistics

Total APs: 1 Misconfigured APs: Tag: 0 Country Code: 0 LSC Fallback: 0

AP Name	AP Model	Admin Status	IP Address	Policy Tag	Site Tag	RF Tag	Location	Country
HQ-F1-AP01	AIR-AP4800-B-K9	✓	10.0.101.11	PT_CLEME_HQ_F1_cb0e2	ST_CLEME_HQ_e673b_0	TYPICAL	Global/CLEMEA...	US



In case of AP showing as Misconfigured on the WLC, resync the WLC from the Catalyst Center. Navigate to **Provision > Inventory**. Select the **WLC1**, then **Actions > Inventory > Resync Device**. This behavior is due to the bug CSCwi21444a.

Snippet from WLC Config looks like:

```
wireless tag site ST_CLEME_HQ_e673b_0
description "Site Tag ST_CLEME_HQ_e673b_0"
```

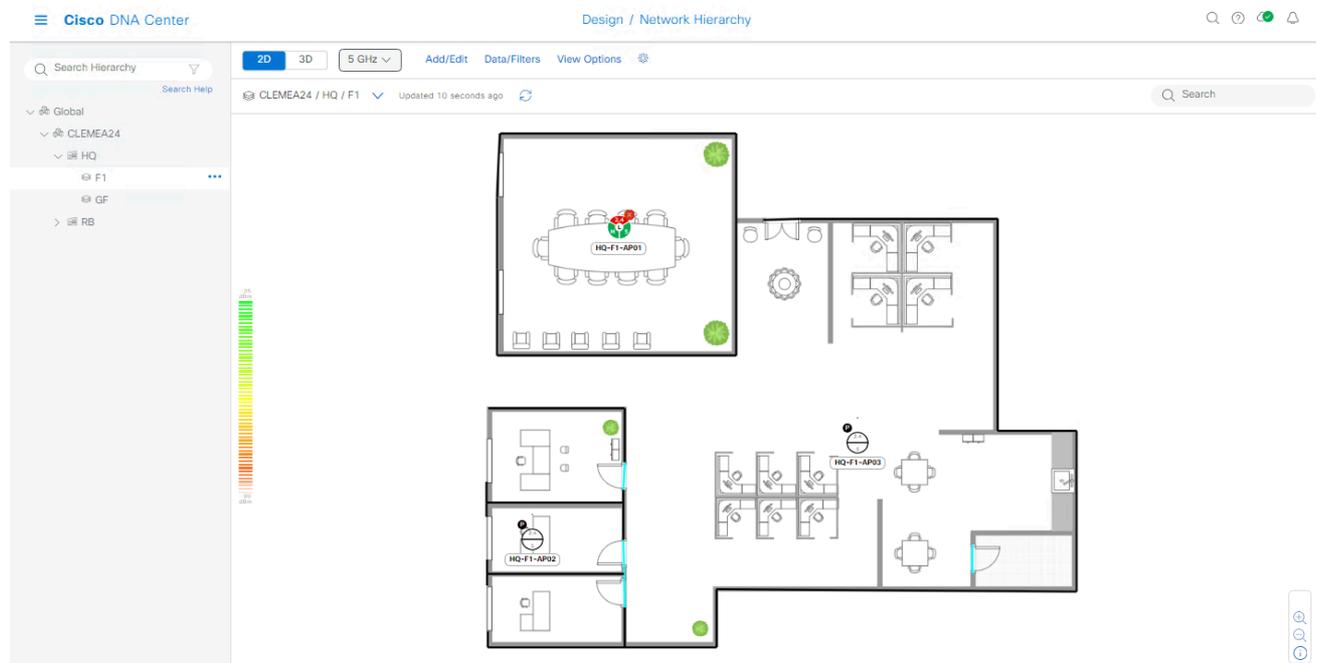
```
wireless tag policy PT_CLEME_HQ_F1_cb0e2
  description "PolicyTagName PT_CLEME_HQ_F1_cb0e2"

wireless tag rf TYPICAL
  24ghz-rf-policy Typical_Client_Density_rf_24gh
  5ghz-rf-policy Typical_Client_Density_rf_5gh

ap 7872.5dfb.8e78
  policy-tag PT_CLEME_HQ_F1_cb0e2
  rf-tag TYPICAL
  site-tag ST_CLEME_HQ_e673b_0
```

As the chosen AP name “HQ-F1-AP01” matched the Planned AP name from the Ekahau file, the AP should be automatically placed in the map and the “Planned” AP icon should disappear, verify by navigating to **Design > Network Hierarchy** and opening the map for **HQ > F1**.

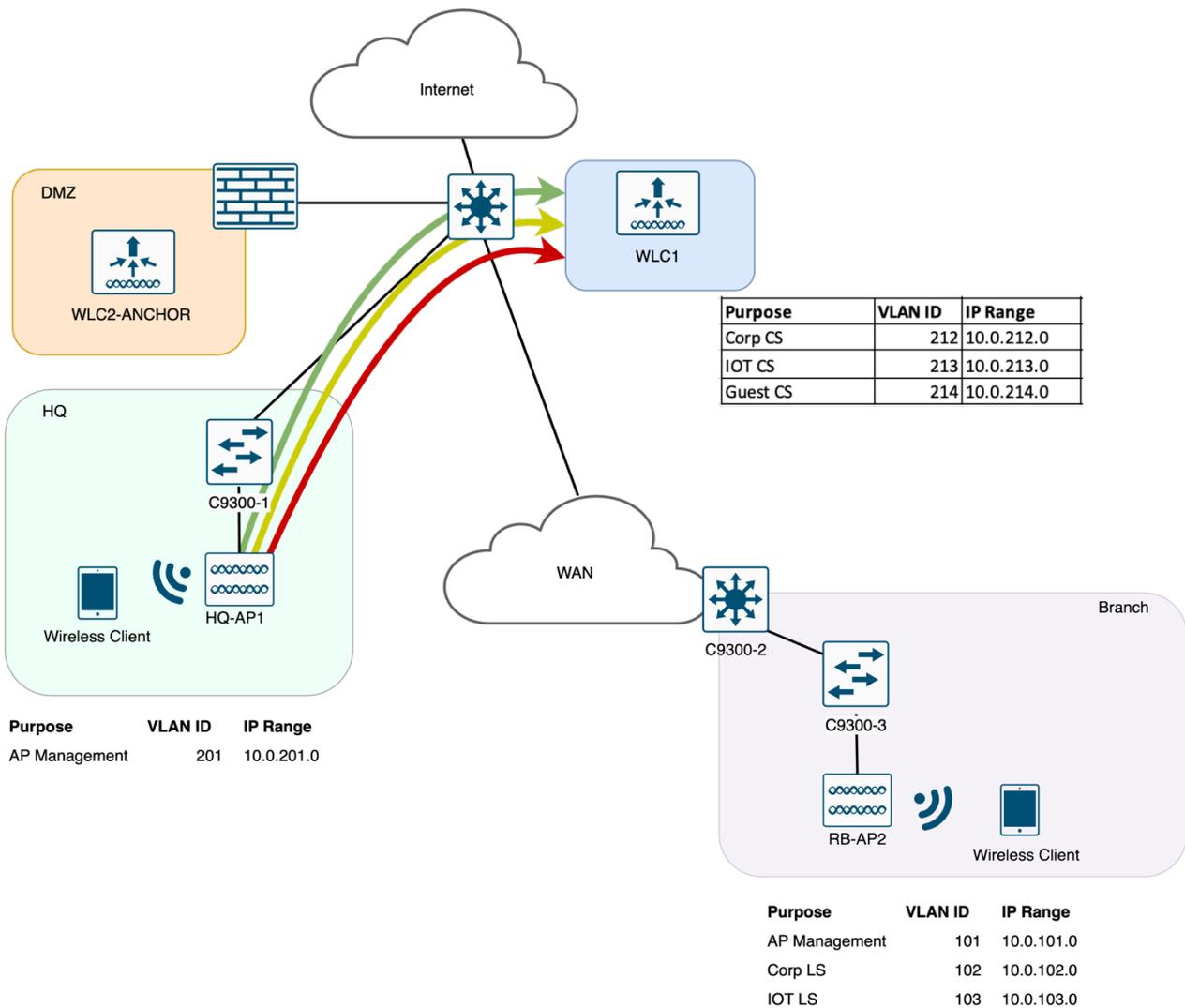
**Figure 70 AP PnP - AP Placement**



## Task 7: Network Settings and Centrally Switched WLANs

In this task we'll create the SSIDs **Corp**, **Guest** and **IOT** with **Central Switching** architecture.

Figure 71 Wireless Architecture



All the site-specific settings including AAA Servers, DHCP, DNS, SSIDs or RF Profile will be created. Those will be later used when provisioning the devices to make sure applicable settings are used for specific sites.

First we go with **Global Network Settings**:

## Step 1: Configure Global Network Settings



Cisco ISE is already deployed and integrated with Catalyst Center

Before we focus on the specific wireless settings, let us configure global network settings including DNS, DHCP and NTP by navigating to **Design > Network Settings**. Before proceeding to define the settings, make sure that it is done under the Global level in the hierarchy:

**Figure 72 Network Settings - Hierarchy**

The screenshot shows the Cisco DNA Center interface for Network Settings. The breadcrumb is 'Design / Network Settings'. The left sidebar shows a hierarchy with 'Global' selected. The main content area shows configuration options for DHCP Server, DNS Server, Time Zone, and Message of the day. The DHCP Server section has an 'Add Servers' (+) button. The DNS Server section also has an 'Add Servers' (+) button. The Message of the day section has a checkbox for 'Do not override the existing MOTD banner on the device' which is checked.

In the top-right corner click on **Add Servers** and select following additional servers and click **OK**

- AAA
- NTP

**Figure 73 Network Settings - Add Servers**

×

## Add Servers

- AAA
- Image Distribution
- NTP
- Stealthwatch Flow Destination

Cancel
OK

Once ready, let us fill the values for the network settings as per the below table:

**Table 8 Network Settings - General**

Parameter		Value
<b>AAA Server</b>	<input checked="" type="checkbox"/> Client/Endpoint	<input checked="" type="checkbox"/> ISE <input checked="" type="checkbox"/> RADIUS
<b>AAA Server</b>	IP Address	198.18.133.27
<b>DHCP Server</b>	N/A	N/A
<b>DNS Server</b>	Domain Name	LTREWN2511.lab
<b>DNS Server</b>	IP Address	198.18.128.1
<b>NTP Server</b>	IP Address	198.18.128.1
<b>Time Zone</b>		America/Los_Angeles
<b>Message of the Day</b>		<input checked="" type="checkbox"/> Do not override the existing MOTD banner on the device

**Figure 74 Network Settings**

AAA Server ⓘ

Network  Client/Endpoint

CLIENT/ENDPOINT

Servers	Protocol
<input checked="" type="radio"/> ISE <input type="radio"/> AAA	<input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS
Client/Endpoint	IP Address (Primary)
198.18.133.27	198.18.133.27

[Change Shared Secret](#)

DHCP Server

DHCP

IP Address +

Supports both IPv4 and IPv6

DNS Server ⓘ

Domain Name

LTREWN2511.lab

Primary +

198.18.128.1

Supports both IPv4 and IPv6

NTP Server

NTP +

198.18.128.1

## Step 2: Configure IOT SSID

We will now continue to define Wireless specific settings.

- Navigate to **Network Settings > Wireless**.
- In the SSID section, in the top-right corner, navigate to **Add > Enterprise**

**Figure 75 Wireless Settings - SSID**

The screenshot shows the Cisco DNA Center interface for configuring SSIDs. The main table is currently empty, with a message 'No data to display'. Below it, the 'Wireless Radio Frequency Profile' section is visible, showing a table of RF profiles. A red box highlights the 'Add' button in the top right corner of the SSID configuration area.

Profile Name	Type	2.4GHz Data Rates	5GHz Data Rates	6GHz Data Rates	Channel Width (2.4/5/6GHz)	Profile Type
HIGH	2, 4, 5, 6	9, 12, 18, 24, 36, 48, 54	12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54	20 MHz / Best / Best	System
LOW	2, 4, 5, 6	1, 2, 5, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54	20 MHz / Best / Best	System
TYPICAL	2, 4, 5, 6	9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54	20 MHz / Best / Best	System

We will start by creating IOT, PSK-based SSID to be used across our sites.

SSID will be named **XX\_CLEMEA24\_IOT** where XX corresponds to the POD number you are assigned to. See example below with pod 01.

## Figure 76 SSID - IOT - Basic Settings

### Basic Settings

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

Sensor ⓘ

Wireless Network Name (SSID)* 01_CLEMEA24_IOT	WLAN Profile Name* 01_CLEMEA24_IOT_profile	Policy Profile Name 01_CLEMEA24_IOT_profile ⓘ
--	---	--

Wireless Option ⓘ

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

Primary Traffic Type  
VoIP (Platinum) ▼ ⓘ

SSID STATE

Admin Status

Broadcast SSID

- Click **Next**
- continue to specify Security Settings for the SSID
  - o Level of Security: **Personal WPA2**
  - o Set the PSK as **C1sco12345**
  - o Leave the rest with default values

## Figure 77 SSIDs - IOT - Security Settings

### Security Settings

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

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

**SSID Name:** 01\_CLEMEA24\_IOT (Enterprise)

Level of Security

Enterprise  Personal  Open Secured  Open

WPA2  WPA3

Most secure  
A password (Pre-Shared Key PSK with WPA2 encryption ) is needed to access the wireless network.  
WPA3 feature is supported for Wireless Controller version 8.10 & above, For Catalyst 9800 Controllers version 16.12 & above.

Passphrase Type

Pass Phrase\*  
C1sco12345 HIDE

[Configure MPSK](#) ⓘ

Authentication, Authorization, and Accounting Configuration

[Configure AAA](#)

AAA Override  Fast Lane ⓘ

Identity PSK ⓘ  Deny RCM Clients ⓘ

Finalize the SSID settings by specifying advanced parameters:

- **Fast Transition:** Enable
- **Session Timeout:** 43200
- Leave the rest with default values.

## Figure 78 SSIDs - IOT - Advanced Settings

### Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: 01\_CLEMEA24\_IOT (Enterprise)

Fast Transition (802.11r)

Adaptive  Enable  Disable  
 Over the DS

MFP Client Protection ⓘ

Optional  Required  Disabled

Protected Management Frame (802.11w)

Optional  Required  Disabled

11k

Neighbor List

Session Timeout ⓘ in (secs)\*  
43200

Client Exclusion ⓘ in (secs)\*  
180

11v BSS Transition Support

BSS Max Idle Service

Client User Idle Timeout ⓘ Client User Idle Timeout(Default: 300 secs)\*  
300

Directed Multicast Service

Radius Client Profiling  ⓘ

NAS-ID ⓘ

NAS-ID Opt 1  +

Configure CCKM  ⓘ

Configure Client Rate Limit ⓘ

Click on **Next** to assign the SSID to the required Network Profiles.

All the SSIDs will be used in both HQ and Remote Branch, so we need to configure both network profiles.

Let's start with **WIRELESS\_HQ** Network Profile.

- Rename the **WLAN Profile Name**: XX\_CLEMEA24\_IOT\_Central
  - a. XX being the POD ID
- Choose **No** in the **Fabric** setting.
- Click "+" sign next to interface name
  - a. **Interface Name**: IOT
  - b. **VLAN ID**: 213

**Figure 79 SSIDs - IOT - Network Profile – HQ (Central Switching)**

SSID Name: 01\_CLEMEA24\_IOT (Enterprise)

The screenshot displays the configuration page for a wireless profile. On the left, a sidebar shows a search bar and a list of profiles: 'WIRELESS\_HQ' (with a green checkmark) and 'WIRELESS\_RB'. The main content area has a top bar with '+ Add Profile', 'Disassociate Profile', and 'Save' buttons. Below this, the configuration fields are as follows:

- Profile Name:** WIRELESS\_HQ
- WLAN Profile Name:** 01\_CLEMEA24\_IOT\_Central
- Policy Profile Name:** 01\_CLEMEA24\_IOT\_Central
- Fabric:**  Yes  No
- Enable SSID Scheduler:**
- Interface Selection:**  Interface  VLAN Group
- Interface Name\*:** IOT
- Do you need Anchor for this SSID?:**  Yes  No
- Flex Connect Local Switching:**

- Then click on **Associate Profile** for the changes to be applied, then click **Next**
- In the Summary page, click **Save**

### Step 3: Provision IOT Configuration to WLC

- Go to **Provision > Inventory**
- Select the WLC and hover over **“Actions”** field and navigate to **“Provision”** and then to **“Provision Device”**
- You’ll notice new Interface there,
  - o **IOT** should be VLAN ID: **213**
- Skip past (hit next) for **“Model Configuration”** and **“Advanced Configuration”** and head into **“Summary”**

- Click **“Deploy”**
- Click **“Apply”** Now

As this is the 2<sup>nd</sup> time the WLC is provisioned we expect to see the following information pushed to the WLC:

- Domain Name: LTREWN2511.lab, name server: 198.18.128.1
- Central WLAN Profiles
- Central Policy Profiles
- VLAN 213 named IOT
- And the following AAA config (if it wasn't already)

```
aaa authentication dot1x default local
aaa authentication login default local
aaa server radius dynamic-author
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server deadtime 3
```

Since the HQ AP was provisioned in the PNP Process it's not needed to reprovision again.

This SSID is now ready to be tested with a wireless client. (Skip this step if you want to test at the end)

#### Step 4: Testing IOT SSID with a Wireless Client

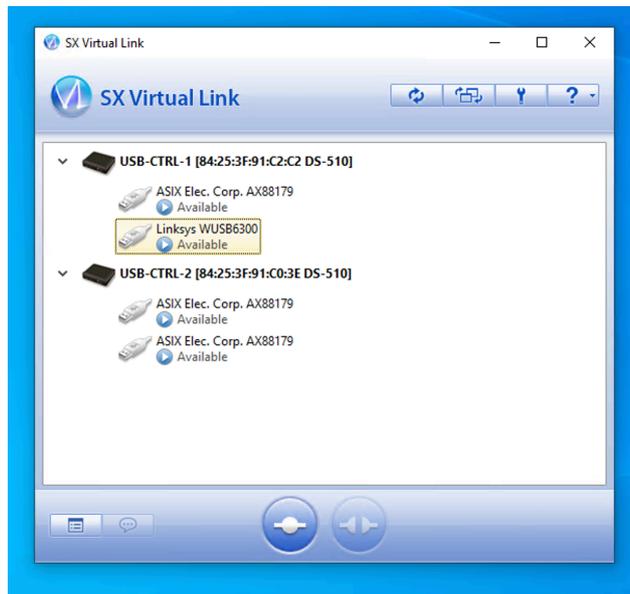
Open an RDP session to one of the Wireless Clients:

**Table 9 Wireless Clients Addressing and Credentials**

Name	IP Address	Username	Password	Preferred Access Method
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP
Client4	198.18.134.4	DCLOUD\admin	C1sco12345	RDP

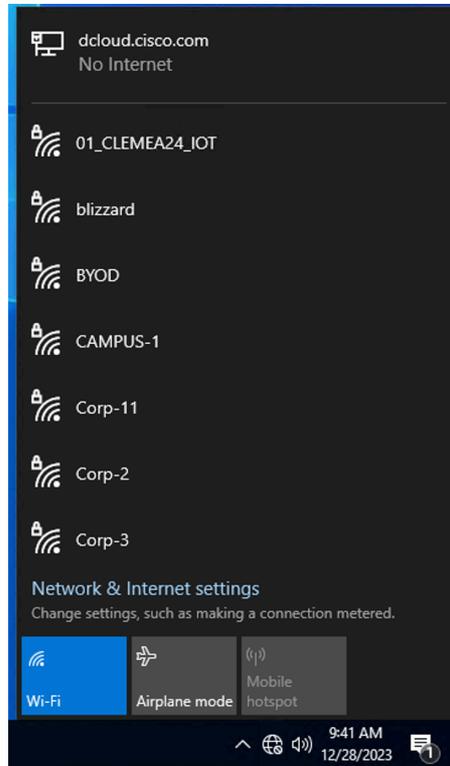
- Open SX Virtual Link app in the Desktop
- Enable the Linksys **WUSB6300** Adapter by clicking on the **“Connect”** button below.

**Figure 80 SX Virtual Link Adapter Configuration**



Then connect to the desired SSID using the default network manager in Windows  
Disable the checkbox **“Connect Automatically”**

Figure 81 Connecting to WLAN



Verify using CMD if the wireless client gets an IP address from the desired VLAN.  
The below example is for IOT at the HQ

### Figure 82 Connecting to WLAN – Verify IP Address

```
Windows IP Configuration

Ethernet adapter Ethernet0 3:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 198.18.134.1
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6cba:984d:9a37:23a9%16
    IPv4 Address. . . . . : 10.0.213.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.213.1

C:\Users\admin.DCLOUD>
```

Also verify on the WLC if the client is in the RUN State  
Go to the WLC UI, **Monitoring > Clients**

### Figure 83 Connecting to WLAN – Verify in WLC

The screenshot shows the Cisco WLC Monitoring > Clients page. The breadcrumb navigation is Monitoring > Wireless > Clients. There are three tabs: Clients (selected), Sleeping Clients, and Excluded Clients. A 'Delete' button and a refresh icon are visible. Below the tabs, it says 'Selected 0 out of 1 Clients'. A table displays the client information:

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name
c441.1e83.4520	10.0.213.11	fe80::6cba:984d:9a37:23a9	HQ-F1-AP02	01_CLEMEA24_IOT	17	WLAN	Run	11ac	

At the bottom of the table, there is a pagination control showing '1' of 10 items and '1 - 1 of 1 clients'.

## Step 5: Configure CORP SSID

We will now continue the same steps for the Corporate, 802.1x SSID.

- Navigate to **Network Settings > Wireless**.
- In the SSID section, in the top-right corner, navigate to **Add > Enterprise**



Use the default settings if not specifically called out in the table

**Table 10 SSIDs – Settings – CORP - HQ**

Parameter	Value
Wireless Network Name	<b>XX_CLEMEA24_CORP</b>
Wireless Option	Multi band operation (2.4GHz, 5GHz and 6GHz)
Type of Enterprise Network	<b>VoIP (Platinum)</b>
Admin Status	<b>Enable</b>
Broadcast SSID	<b>Enable</b>
Level of Security	Enterprise > WPA2
Authentication, Authorization and Accounting Configuration (See figure below)	ISE (198.18.133.27)
AAA Override	<b>Enable</b>
Fast Transition (802.11r)	Adaptive, Over the DS
Session Timeout	Enable, 43200

## Figure 84 SSIDs - CORP – Configure AAA (Central Switching)

✕

Configure AAA Server for 01\_CLEMEA24\_CORP

⚠ Two (2) Warning Alerts on this page. [Collapse](#) to hide.

---

⚠ Two (2) Warning Alerts

Catalyst 9800 Controllers versions less than 17.9 support only upto 8 Accounting Method list configuration. Configuring more than that will result in provisioning failure. To ensure the right configuration is pushed for this SSID, configure one or more AAA/PSN.

Configure Authentication and Authorization Servers

Server  
198.18.133.27

Copy same Servers for Accounting

Configure Accounting Server

Server  
198.18.133.27

Cancel Configure

## Table 11 Network Profile – Settings – CORP HQ

Parameter	Value
Associate SSID to Profile	WIRELESS_HQ
WLAN Profile Name:	XX_CLEMEA24_CORP_Central
Fabric	No
<b>Interface Name: (Create if non existing)</b>	CORP
<b>VLAN ID</b>	212
Anchor	No
FlexConnect Local Switching	No

## Figure 85 SSIDs - CORP – Configure AAA (Central Switching)

Interface Name  
CORP

Only 31 characters are allowed

VLAN ID\*  
212

VLAN ID range is 0-4094

Click on **Associate Profile** for the changes to take effect then **Next**

In the Summary page, click **Save**

## Step 6: Configure GUEST SSID

Let us now finish the SSID configuration with the Guest SSID:

- Navigate to **Network Settings > Wireless**.
- In the SSID section, in the top-right corner, navigate to **Add > Guest**



Please use the default settings if not specifically called out in the table

**Table 12 SSID – Settings – GUEST HQ**

Parameter	Value
Wireless Network Name	<b>XX_CLEMEA24_GUEST</b>
Wireless Option	Multi band operation (2.4GHz, 5GHz and 6GHz)
Type of Enterprise Network	<b>Best Effort (Silver)</b>
Level of Security	Open > Web Policy
Authentication Server ( <i>See screenshot below</i> )	<b>CWA &gt; Hotspot &gt; Original URL</b>
AAA Configuration	ISE (198.18.133.27)
AAA Override	Enable
Mac Filtering	Enable
Session Timeout	Enable, 3600

**Figure 86 SSIDs - GUEST – Configure Security Settings (Central Switching)**

Level of Security

L2 SECURITY

Enterprise
  Personal
  Open Secured
  Open

Least Secure :

Any user can associate to the network.

L3 SECURITY

Web Policy
  Open

Most secure

Guest users are redirected to a Web Portal for authentication

Authentication Server

What kind of portal are you creating today ?
   
 Central Web Authentication
   
 Hotspot
   
 Where will your guests redirect after successful authentication ?
   
 Original URL

Authentication, Authorization, and Accounting Configuration

AAA Configured (1)

AAA Override
  Fast Lane ⓘ

Mac Filtering
  Deny RCM Clients ⓘ

Pre-Auth ACL List Name

**Table 13 Network Profile – Settings – GUEST HQ**

Parameter	Value
Associate SSID to Profile	WIRELESS_HQ
WLAN Profile Name:	XX_CLEMEA24_GUEST_Central
Fabric	No
Interface Name: (Create if non existing)	GUEST
VLAN ID	214
Anchor	No
FlexConnect Local Switching	No

Click on **Associate Profile** for the changes to take effect then **Next**.

Catalyst Center allows the portal creation and customization on this workflow, to start with this process click **Create Portal**:

## Figure 87 SSIDs - GUEST – Configure Hotspot Portal (Central Switching)

### Portal Settings

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

SSID Name: 01\_CLEMEA24\_GUEST (Guest)

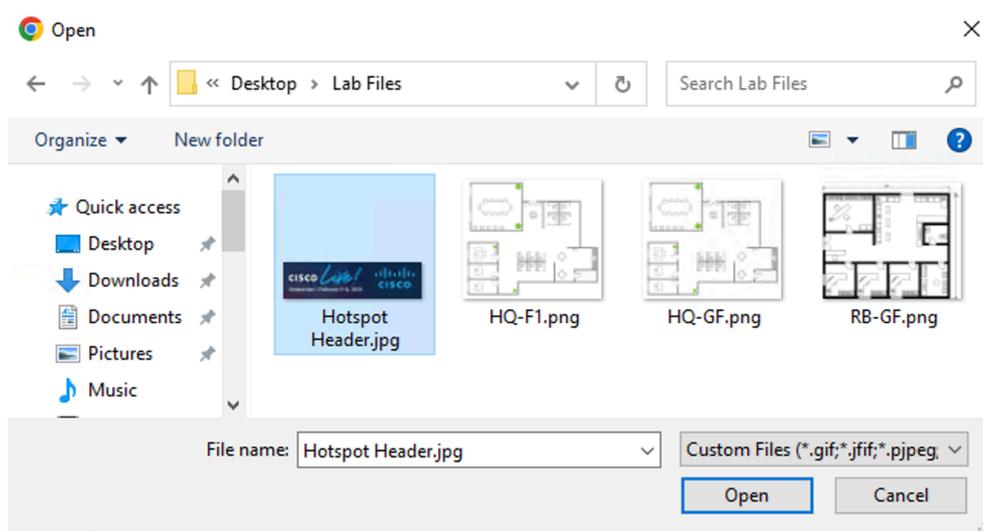
No Hotspot Portal Available

Use the create portal button to create a new portal

Create Portal

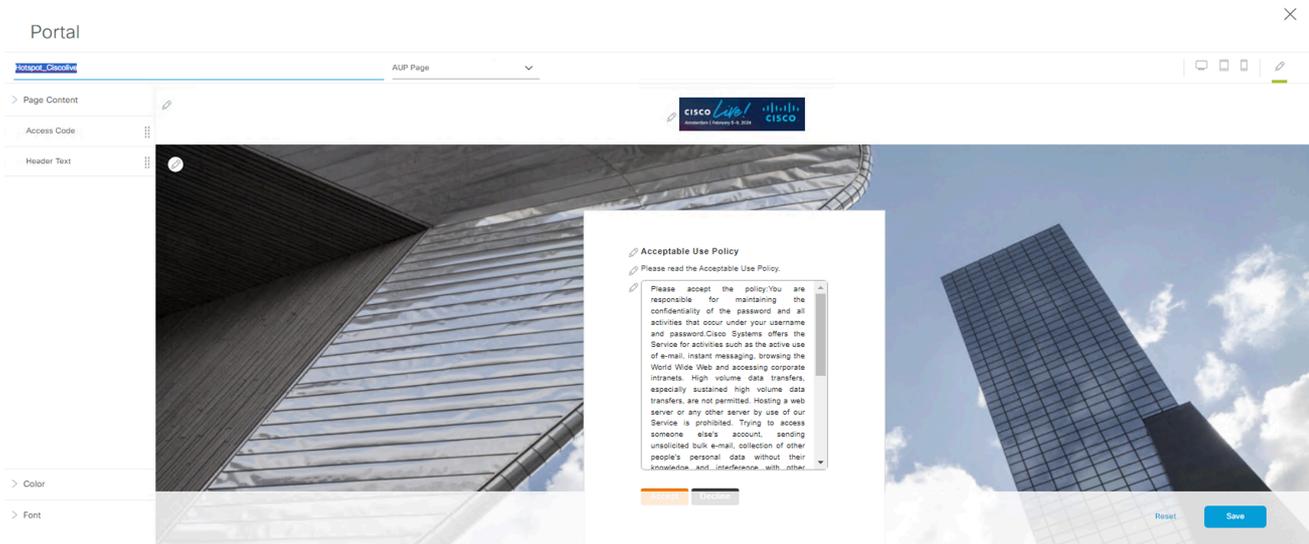
- Name the portal as “**Hotspot\_Ciscolive**”
- Edit the Portal Header, use the file in the Desktop. Click in the **Pencil** next to the header logo, click **Upload** and select the new file.
- Then click **Save**

## Figure 88 SSIDs - GUEST – Configure Hotspot Portal (Central Switching)



When finished it should look like this:

## Figure 89 SSIDs - GUEST – Configure Hotspot Portal (Central Switching)



Advance to the summary page, then click **Save** to finish the process.

Catalyst Center will push the following configuration to ISE automatically:

- The Configured Portal
- Authorization Profile for redirecting to portal
- Two Authorization Policies for this portal in the Default Policy Set

Snippet of pushed config in ISE:

## Figure 90 SSIDs - GUEST –ISE Hotspot Portal

The screenshot shows the Cisco ISE interface for configuring Guest Portals. The breadcrumb trail is "Work Centers · Guest Access". The navigation menu includes Overview, Identities, Identity Groups, Ext Id Sources, Administration, Network Devices, Portals & Components (selected), Manage Accounts, Policy Elements, Policy Sets, and More. The left sidebar shows "Guest Portals" with sub-items: Guest Types, Sponsor Groups, and Sponsor Portals. The main content area is titled "Guest Portals" and contains the instruction: "Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access." Below this are four portal cards:

- Hotspot Guest Portal (default)**: Guests do not require username and password credentials to access the network, but you can optionally require an access code. Status: Authorization setup required (warning icon).
- Hotspot\_Ciscolve**: DNA hotspot Portal. Status: Used in 1 rules in the Authorization policy (success icon).
- Self-Registered Guest Portal (default)**: Guests may create their own accounts and be assigned a username and password, or use their social login to access the network. Status: Used in 1 rules in the Authorization policy (success icon).
- Sponsored Guest Portal (default)**: Sponsors create guest accounts, and guests access the network using their assigned username and password. Status: Authorization setup required (warning icon).

## Figure 91 SSIDs - GUEST –ISE Authz Profiles

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The breadcrumb trail is "Policy · Policy Elements". The navigation menu includes Dictionaries, Conditions, and Results (selected). The left sidebar shows a tree view with categories: Authentication, Authorization (expanded), Profiling, Posture, and Client Provisioning. Under "Authorization", the "Authorization Profiles" section is selected. The main content area is titled "Authorization Profile" and shows the configuration for "Hotspot\_Ciscolve\_Profile":

- Name**: Hotspot\_Ciscolve\_Profile
- Description**: DNA generated Authorization Profile for portal - Hotspot\_Ciscolve
- Access Type**: ACCESS\_ACCEPT
- Network Device Profile**: Cisco
- Service Template**:
- Track Movement**:  ⓘ
- Agentless Posture**:  ⓘ
- Passive Identity Tracking**:  ⓘ

Under the "Common Tasks" section:

- Web Redirection (CWA, MDM, NSP, CPP)** ⓘ
- Hot Spot**:  ACL: DNAC\_ACL\_WEBAUTH\_RED... Value: Hotspot\_Ciscolve
- Static IP/Host name/FQDN
- Suppress Profiler CoA for endpoints in Logical Profile
- Auto Smart Port

**Figure 92 SSIDs - GUEST –ISE Policies**

The screenshot shows the Cisco ISE Policy Sets configuration page for 'Authorization Policy (14)'. It displays a table of policies with columns for Status, Rule Name, Conditions, Results (Profiles, Security Groups), Hits, and Actions.

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Hotspot_Ciscolive_GuestAccessPolicy	AND InternalUser-IdentityGroup EQUALS Endpoint Identity Groups:GuestEndpoints Radius-Called-Station-ID ENDS_WITH :01_CLEMEA24_GUEST	PermitAccess x	Guests	0	⚙️
✓	Hotspot_Ciscolive_RedirectPolicy	AND Wireless_MAB Radius-Called-Station-ID ENDS_WITH :01_CLEMEA24_GUEST	Hotspot_Ciscolive_Pro... x	Select from list	0	⚙️
✓	Wireless Black List Default	AND Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blocked List	Blackhole_Wireless_Ac... x	Select from list	0	⚙️
✓	Profiled Cisco IP Phones	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones x	Select from list	0	⚙️
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones x	Select from list	0	⚙️

Once completed, this is how the Wireless main screen will present:

**Figure 93 SSIDs - Summary**

The screenshot shows the SSID Summary table with columns for Network Name (SSID), WLAN Profile Name, Policy Profile Name, SSID Type, L2 Security, L3 Security, Wireless Profiles, Portal Name, and AAA Servers.

Network Name (SSID)	WLAN Profile Name	Policy Profile Name	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
01_CLEMEA24_CORP	01_CLEM... (1)	01_CLEM... (1)	Enterprise	wpa2_enterprise	open	WIRELESS_HQ	N/A	AAA Configured (1)
01_CLEMEA24_GUEST	01_CLEM... (1)	01_CLEM... (1)	Guest	open	web_auth	WIRELESS_HQ	Hotspot_Ciscolive	AAA Configured (1)
01_CLEMEA24_IOT	01_CLEM... (1)	01_CLEM... (1)	Enterprise	wpa2_personal	open	WIRELESS_HQ	N/A	Configure AAA

## Step 7: Provision CORP and Guest Configuration to WLC

- Go to **Provision > Inventory**
- Select the WLC and hover over **“Actions”** field and navigate to **“Provision”** and then to **“Provision Device”**
- You’ll notice new Interfaces there,
  - o **CORP** should be VLAN ID: **212**
  - o **GUEST** should be VLAN ID: **214**

Figure 94 Provision CORP and GUEST to WLC

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

WLC1.LTREW2511.lab

Serial Number: 9XBUQSVUVUK

Devices: WLC1.LTREW2511.lab

WLC Role:  Active Main WLC  Anchor

Managed AP location(s): [Managing 5 Primary location\(s\)](#)  
[Select Secondary Managed AP Locations](#)

Skip AP Provision

Assign Interface

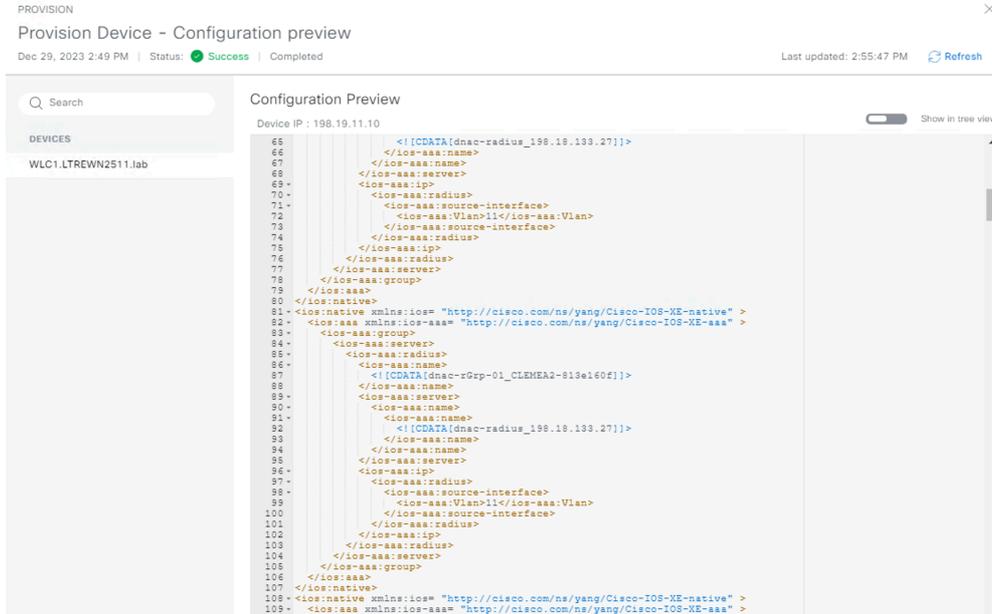
Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
CORP	-	212	IP Address	Gateway IP Address	Subnet Mask
GUEST	-	214	IP Address	Gateway IP Address	Subnet Mask
IOT	-	213	IP Address	Gateway IP Address	Subnet Mask

3 Records Show Records: 25 1 - 3

Skip past (hit next) for “**Model Configuration**” and “**Advanced Configuration**” and head into “**Summary**”

- Click “**Deploy**”
- (OPTIONAL): Click “**Generate Configuration Preview**” then “**Work Items**” to see xml-form config to be pushed to WLC via Netconf.

**Figure 95 Preview Configuration WLC**



- Click **“Apply”** Now

This time we expect Catalyst Center to push the following config:

- AAA Servers and AAA Groups
- AAA Dynamic Authorization for CoA
- Method-lists for CWA and 802.1x
- Webauth Redirect ACL
- CORP and GUEST WLANS
- CORP and GUEST Central switching Policy Profiles

## Step 8: Testing CORP SSID

Open an RDP session to one of the Wireless Clients:

**Table 14 Wireless Clients Addressing and Credentials**

Name	IP Address	Username	Password	Preferred Access Method
------	------------	----------	----------	-------------------------

Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP
Client4	198.18.134.4	DCLOUD\admin	C1sco12345	RDP

- Make sure the SX Virtual Link has the **WUSB6300** connected.
- Connect to CORP SSID using the credentials:

**Username:** testuser

**Password:** C1sco12345

The image displays two sequential screenshots of a Windows network connection dialog box. The left screenshot shows the 'Enter your user name and password' step for the '01\_CLEMEA24\_CORP' network. The right screenshot shows the 'Continue connecting?' confirmation step for the same network. Both screenshots show the network name '01\_CLEMEA24\_CORP' as 'Secured' and the status 'No Internet' for the connection.

**Left Screenshot:**

- Connection: dcloud.cisco.com (No Internet)
- Network: 01\_CLEMEA24\_CORP (Secured)
- Text: Enter your user name and password
- Checkbox:  Use my Windows user account
- Username field: testuser
- Password field: [masked]
- Buttons: OK, Cancel

**Right Screenshot:**

- Connection: dcloud.cisco.com (No Internet)
- Network: 01\_CLEMEA24\_CORP (Secured)
- Text: Continue connecting? If you expect to find 01\_CLEMEA24\_CORP in this location, go ahead and connect. Otherwise, it may be a different network with the same name. Show certificate details
- Buttons: Connect, Cancel

At the bottom of both screenshots, the Windows taskbar shows the following network settings:

- Wi-Fi: On
- Airplane mode: Off
- Mobile hotspot: Off

```
Command Prompt
C:\Users\admin.DCLOUD>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 3:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 198.18.134.1
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6cba:984d:9a37:23a9%16
    IPv4 Address. . . . . : 10.0.212.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.212.1

C:\Users\admin.DCLOUD>ping 10.0.212.1 -t

Pinging 10.0.212.1 with 32 bytes of data:
Reply from 10.0.212.1: bytes=32 time=3ms TTL=255
Reply from 10.0.212.1: bytes=32 time=3ms TTL=255
Reply from 10.0.212.1: bytes=32 time=4ms TTL=255
Reply from 10.0.212.1: bytes=32 time=3ms TTL=255
Reply from 10.0.212.1: bytes=32 time=3ms TTL=255

Ping statistics for 10.0.212.1:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

ISE Radius Live Logs show authentication successful.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...
Dec 29, 2023 03:49:41.9...			0	testuser	C4:41:1E:83:45:20	Belkin-De...	Default >>...	Default >>...	PermitAcc...	10.0.212.11,f...	
Dec 29, 2023 03:49:39.8...				testuser	C4:41:1E:83:45:20	Belkin-De...	Default >>...	Default >>...	PermitAcc...		WLC1.LTREW...

WLC shows client in RUN

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

× Delete 



Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
<input type="checkbox"/>	c441.1e83.4520	10.0.212.11	fe80::6cba:984d:9a37:23a9	AP7872.5DFB.8E78	01_CLEMEA24_CORP	20	WLAN	Run	11ac	testuser	Microsoft-Workstation	Local

1 - 1 of 1 clients 

## Step 9: Testing GUEST SSID

Open an RDP session to one of the Wireless Clients:

**Table 15 Wireless Clients Addressing and Credentials**

Name	IP Address	Username	Password	Preferred Access Method
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP
Client4	198.18.134.4	DCLOUD\admin	C1sco12345	RDP

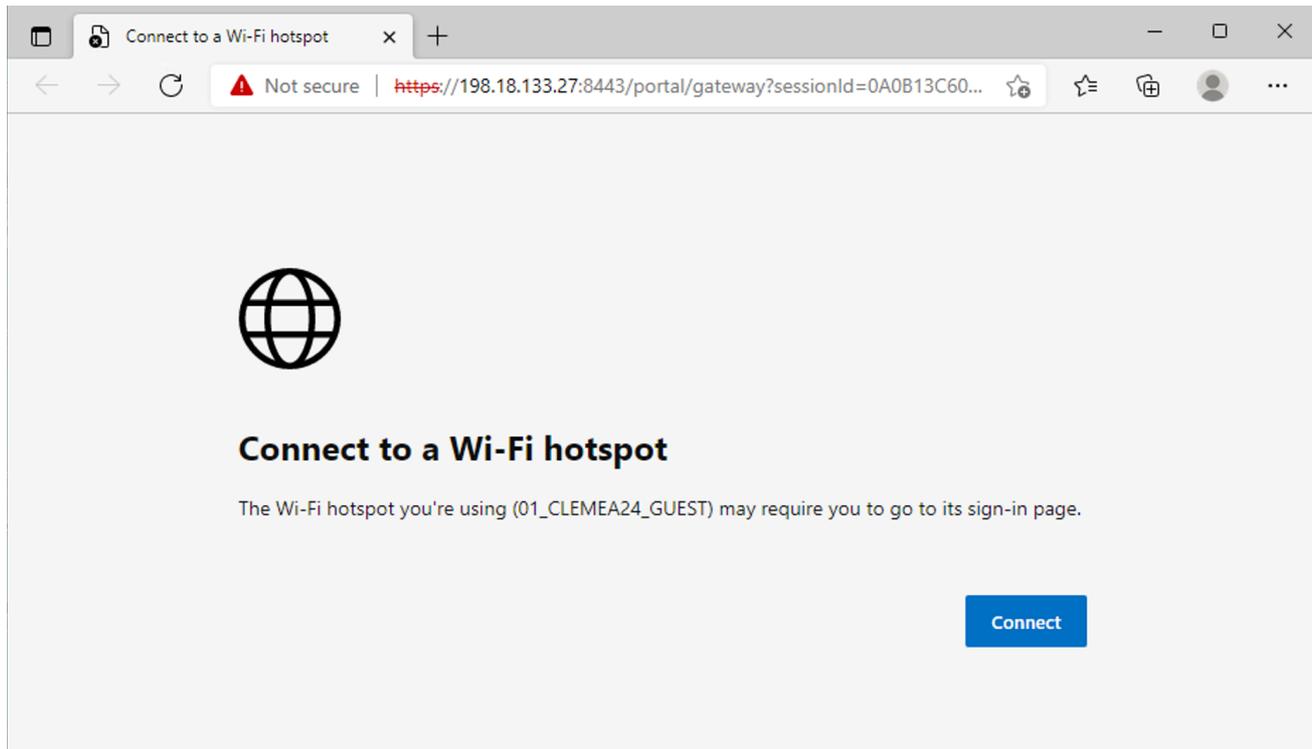
- Make sure the SX Virtual Link has the **WUSB6300** connected.
- Connect to GUEST SSID
- Wait for a redirection



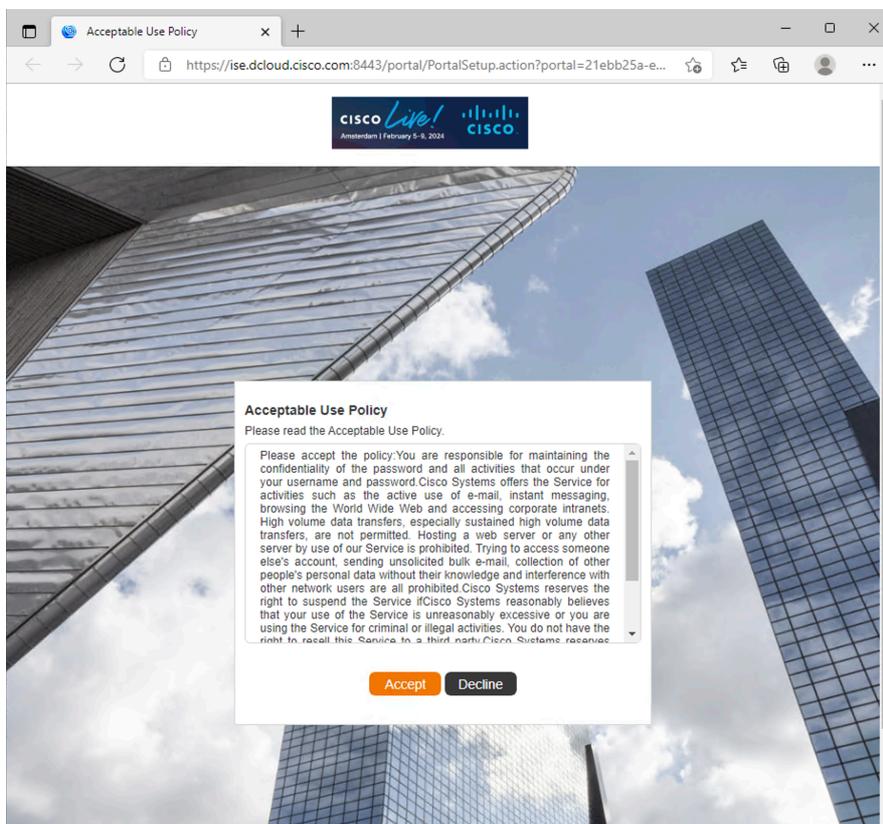
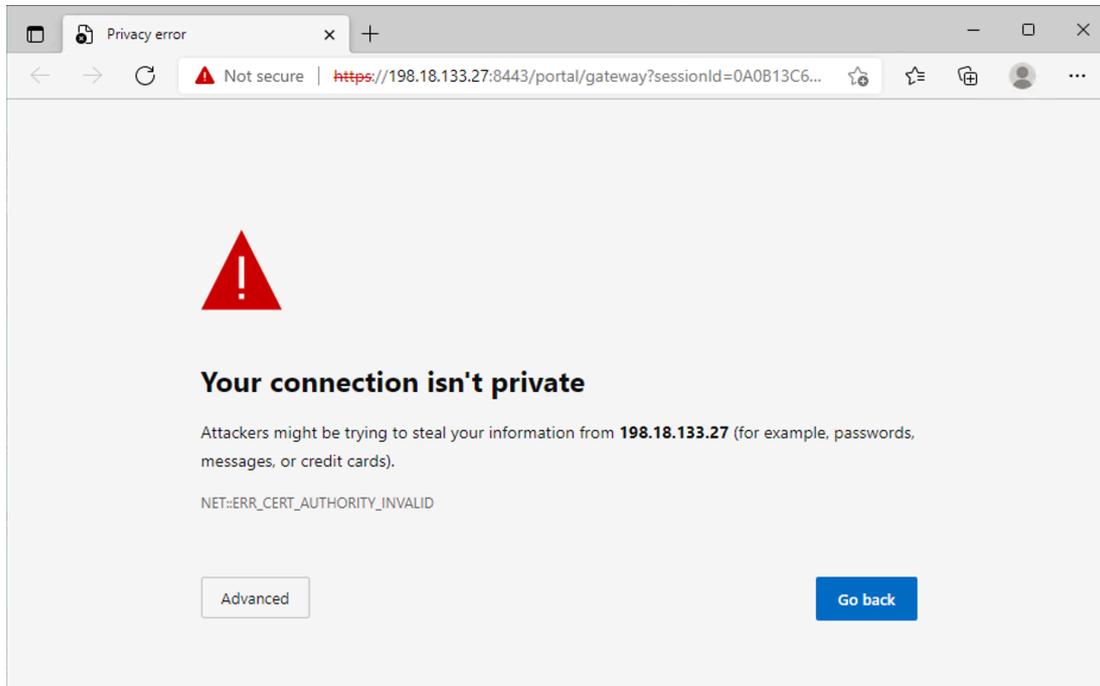
In case you get a page like the one below do the following steps:

1. Click in the page,
2. type "thisisunsafe" (even if it's not showing anywhere)
3. hit ENTER,
4. then reload page

Then you should see the normal warning page. This is expected as ISE does not have a trusted Root CA installed for this purpose.



- Click advanced and proceed to the captive portal



After clicking "Accept" the user is now authenticated.

```
C:\Users\admin.DCLOUD>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 3:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 198.18.134.2
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 13:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e054:d229:13b8:567d%34
    IPv4 Address. . . . . : 10.0.214.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.214.1

C:\Users\admin.DCLOUD>ping 10.0.214.1

Pinging 10.0.214.1 with 32 bytes of data:
Reply from 10.0.214.1: bytes=32 time=4ms TTL=255
Reply from 10.0.214.1: bytes=32 time=4ms TTL=255
Reply from 10.0.214.1: bytes=32 time=4ms TTL=255
```

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
<input type="checkbox"/>	c441.1e83.4520	10.0.214.11	fe80::e054:d229:13b8:567d	AP7872.5DFB.8E78	01_CLEMEA24_GUEST	19	WLAN	Run	11ac	C4-41-1E-83-45-20	Microsoft-Workstation	Local

## Step 10: Disabling HQ AP

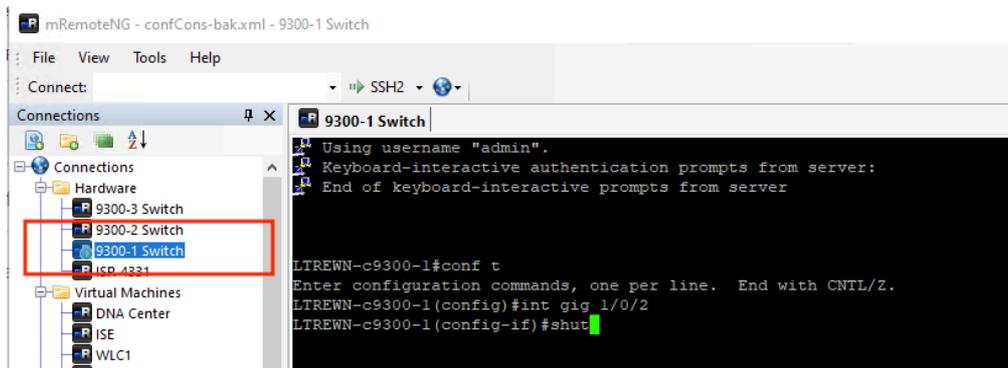
Before we proceed to configure and test the RB site, let us disable the HQ AP not to interfere with our wireless client testing.

Navigate to **mRemoteNG** on your Jumphost and open a session to switch **9300-1**. Shut down port Gig 1/0/2 by issuing following commands:



```
conf t
int gig 1/0/2
shut
```

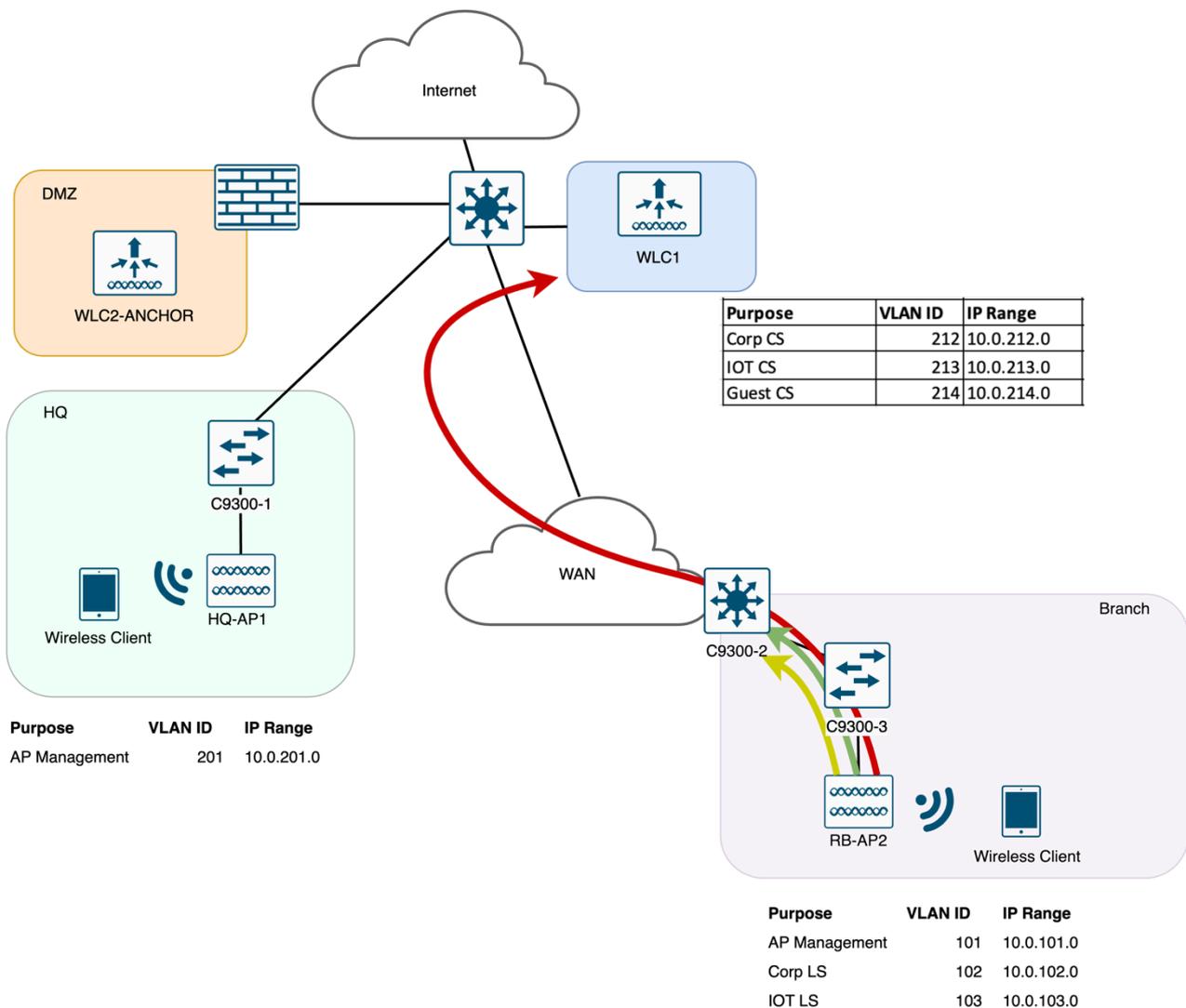
**Figure 96 mRemoteNG - 9300-1**



## Task 8: Configure Flex Local Switching Architecture

In this task we'll create the **FlexConnect** SSIDs. **Corp** and **IOT** will be using **Local switching** however **Guest** is kept centralized.

Figure 97 FlexConnect Wireless Architecture



## Step 1: Configure IOT, CORP and GUEST Network Profiles

As the WLANs were already created, we only need to add the WLANs in the Network Profile with the desired architecture.

We will start with this:

- click on **Design > Network Profile > WIRELESS\_RB > Edit**.
- in the SSIDs tab, click **Add SSID**, one SSID will appear.
- Click the **+** to add all the SSIDs (scroll down to confirm all are there).

Configure the IOT Network Profile as Flexconnect Local Switching like this:

### - Table 16 Network Profile – Settings – IOT RB

Parameter	Value
SSID	XX_CLEMEA24_IOT
WLAN Profile Name:	XX_CLEMEA24_IOT_Flex
Fabric	No
Interface Name:	<b>IOT</b>
Anchor	No
<b>FlexConnect Local Switching</b>	<b>Yes</b>
<b>Local to VLAN</b>	<b>103</b>

**Figure 98 FlexConnect Wireless Architecture**

Network Profiles / Wireless



This configuration is critical for Flex Architecture to work as in this section we configure what it will be mapped to the Policy Profile and Flex Profile.

Configure the CORP Network Profile as Flexconnect Local Switching like this:

- **Table 17 Network Profile – Settings – CORP RB**

Parameter	Value
SSID	XX_CLEMEA24_CORP
WLAN Profile Name:	XX_CLEMEA24_CORP_Flex
Fabric	No
Interface Name:	<b>CORP</b>
Anchor	No
FlexConnect Local Switching	Yes
Local to VLAN	102

Finally, configure the GUEST Network Profile as **Central Switching** like this:

- **Table 18 Network Profile – Settings – GUEST RB**

Parameter	Value
SSID	XX_CLEMEA24_GUEST
WLAN Profile Name:	XX_CLEMEA24_GUEST_Central
Fabric	No
<b>Interface Name: (Create if non existing)</b>	<b>GUEST</b>
Anchor	No
<b>FlexConnect Local Switching</b>	<b>No</b>

- When finished, Click on **Save**

In order to make Site Specific configuration being Local (FlexConnect), we need to click on the RB in the hierarchy.

Edit the Network Settings in order to include the FlexConnect configuration at RB

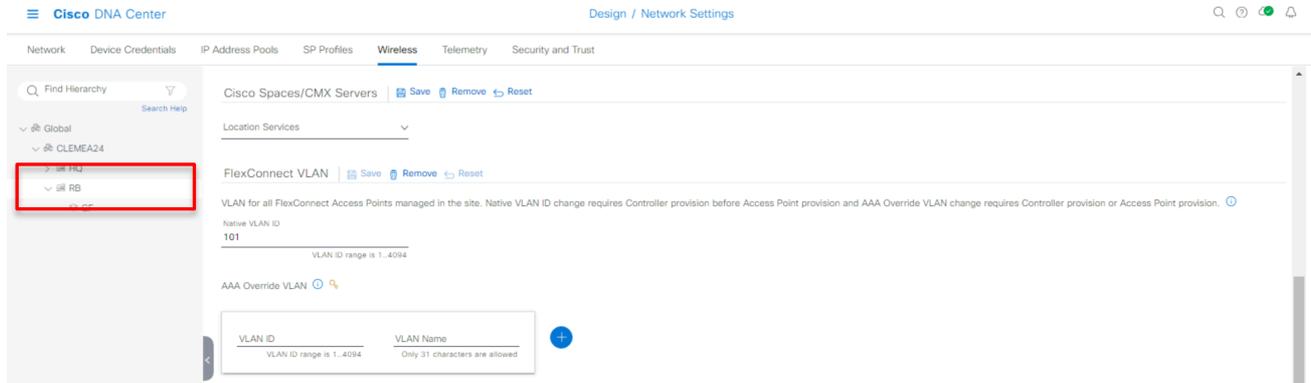
- **Design > Network Settings > Wireless**
- In the hierarchy, **Click** in **RB Building**

Find the **FlexConnect VLAN** parameters

- Add the Native VLAN as 101

When finished it should look like this:

**Figure 99 FlexConnect IOT Parameters at RB site**



The configuration is now done, but we need to push it to the WLC and to AP.

### Step 2: Provision the WLC

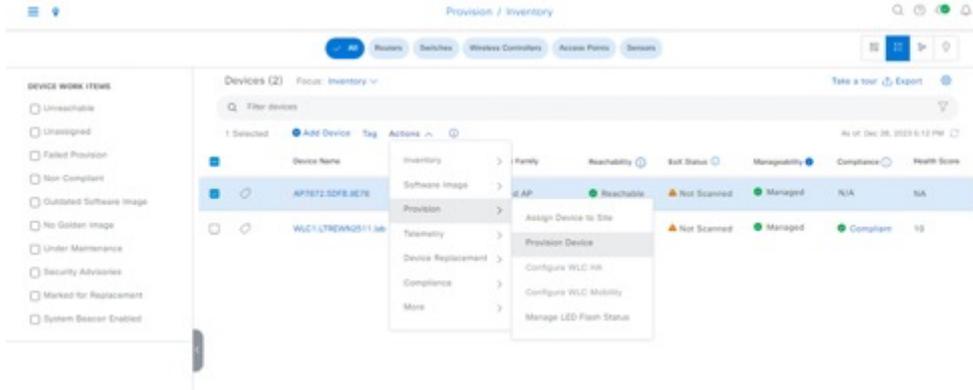
Next step is to Provision WLC

- Go to **Provision > Inventory**
- Select the WLC and hover over “**Actions**” field and navigate to “**Provision**” and then to “**Provision Device**”
- Skip past (hit next) “**Configuration**”, “**Model Configuration**” and “**Advanced Configuration**” and head into “**Summary**”
- Click “**Deploy**”
- Click “**Apply**” Now
- Wait until is finished, then proceed to provision RB AP

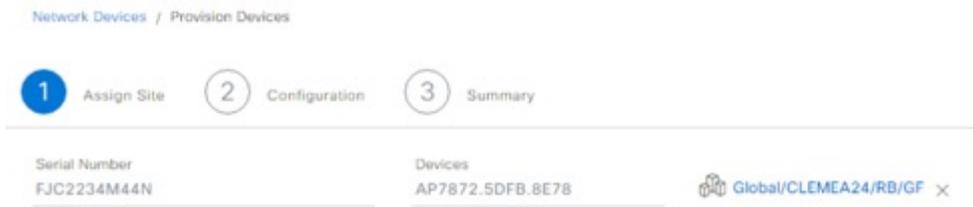
### Step 3: Provision the RB AP

Provision RB AP to get Flex config in WLC and tags on AP

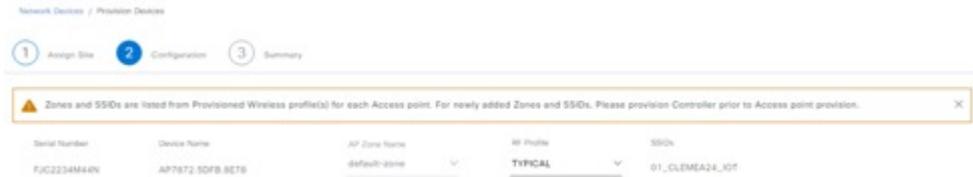
**Figure 100 Provision AP with Flex IOT**



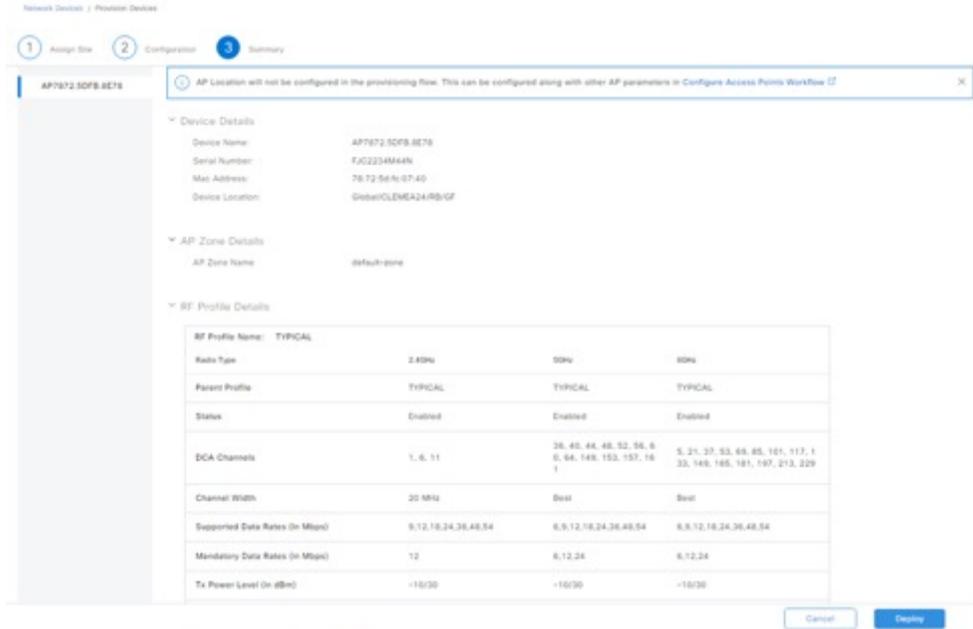
**Figure 101 Provision AP with Flex IOT**



**Figure 102 Provision AP with Flex IOT**



**Figure 103 Provision AP with Flex IOT**



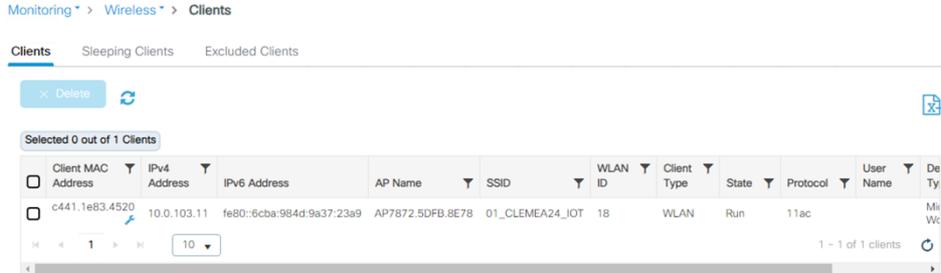
As we provision the WLC and AP, we expect to see the following information pushed:

- Flex WLAN Profiles
- Flex Policy Profiles
- Flex Profile linked to a different Site tag (not local= Remote)
- Native VLAN 101
- CORP VLAN 102 in the Flex Profile
- IOT VLAN 103 in the Flex Profile

#### Step 4: Testing IOT Flex SSID

Client should get an IP address of VLAN 103, range 10.0.103.x

**Figure 104 Testing wireless client to Flex IOT**



**Figure 105 Testing wireless client to Flex IOT**

```
C:\Users\admin.DCLOUD>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 3:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 198.18.134.1
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6cba:984d:9a37:23a9%16
    IPv4 Address. . . . . : 10.0.103.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.103.1

C:\Users\admin.DCLOUD>ping 10.0.103.1 -t

Pinging 10.0.103.1 with 32 bytes of data:
Reply from 10.0.103.1: bytes=32 time=3ms TTL=254
Reply from 10.0.103.1: bytes=32 time=3ms TTL=254
Reply from 10.0.103.1: bytes=32 time=3ms TTL=254
Reply from 10.0.103.1: bytes=32 time=239ms TTL=254
Reply from 10.0.103.1: bytes=32 time=111ms TTL=254
Reply from 10.0.103.1: bytes=32 time=132ms TTL=254
Reply from 10.0.103.1: bytes=32 time=75ms TTL=254
Reply from 10.0.103.1: bytes=32 time=3ms TTL=254
Reply from 10.0.103.1: bytes=32 time=3ms TTL=254
Reply from 10.0.103.1: bytes=32 time=3ms TTL=254
Reply from 10.0.103.1: bytes=32 time=24ms TTL=254
```

### Step 5: Testing CORP Flex SSID

Use the following credentials:

**Username:** testuser

**Password:** C1sco12345

Client should get an IP address of VLAN 102, range 10.0.102.x

### Figure 106 Testing wireless client to Flex CORP

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
c441.1e83.4520	10.0.102.11	fe80::e054:d229:13b8:567d	AP7872.5DFB.8E78	01_CLEMEA24_CORP	21	WLAN	Run	11ac	testuser	Microsoft-Workstation	Local

1 - 1 of 1 clients

### Figure 107 Testing wireless client to Flex CORP

```
C:\Users\admin.DCLOUD>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 3:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 198.18.134.2
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 13:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e054:d229:13b8:567d%34
    IPv4 Address. . . . . : 10.0.102.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.102.1

C:\Users\admin.DCLOUD>

C:\Users\admin.DCLOUD>ping 10.0.102.1

Pinging 10.0.102.1 with 32 bytes of data:
Reply from 10.0.102.1: bytes=32 time=3ms TTL=254
Reply from 10.0.102.1: bytes=32 time=6ms TTL=254
Reply from 10.0.102.1: bytes=32 time=4ms TTL=254
```

## Step 6: Testing GUEST SSID – Remote Branch



Traffic switching and user experience for Guest in RB is same as for the one in HQ. This is SSID with central switching in both scenarios. Feel free to test this use case or skip to the next task.

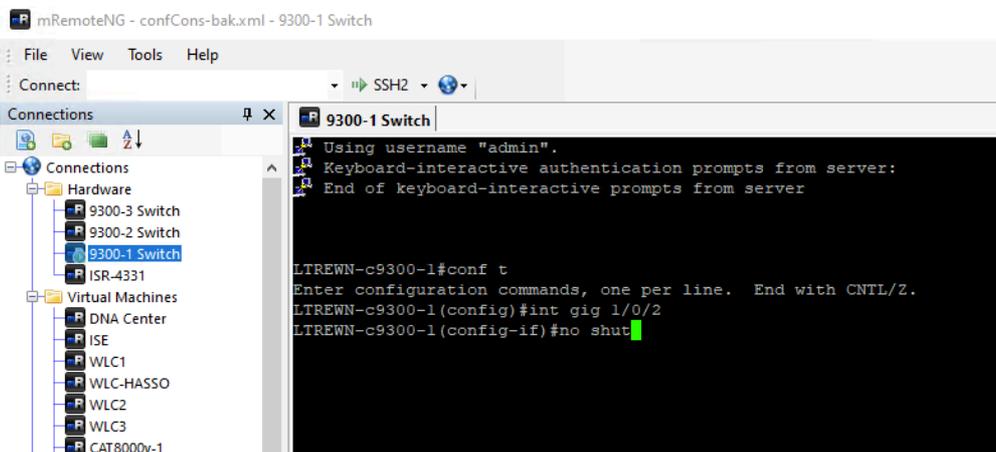
## Step 7: Enabling HQ AP

Before we proceed to configure custom requirements, let us quickly enable the HQ AP that was disabled before.

Navigate to **mRemoteNG** on your Jumphost and open a session to switch **9300-1**. Enable port Gig 1/0/2 by issuing following commands:

```
conf t
int gig 1/0/2
no shut
```

Figure 108 mRemoteNG - 9300-1



## Task 9: Addressing Specific Custom Requirements

In the following task we will

1. **Configure** specific settings using the following tools:
  - **RF Profiles**
  - **Model Config Editor**
  - **Template Hub**
  - **AP Profiles**
2. Bond these elements together using **Network Profiles** depending on the site.
3. Ultimately, **Provision WLC** and **APs** to see the configuration reflected.

### Step 1: Configure Wireless RF Profiles

We will now continue to define RF Profiles to support different requirements depending on the area.

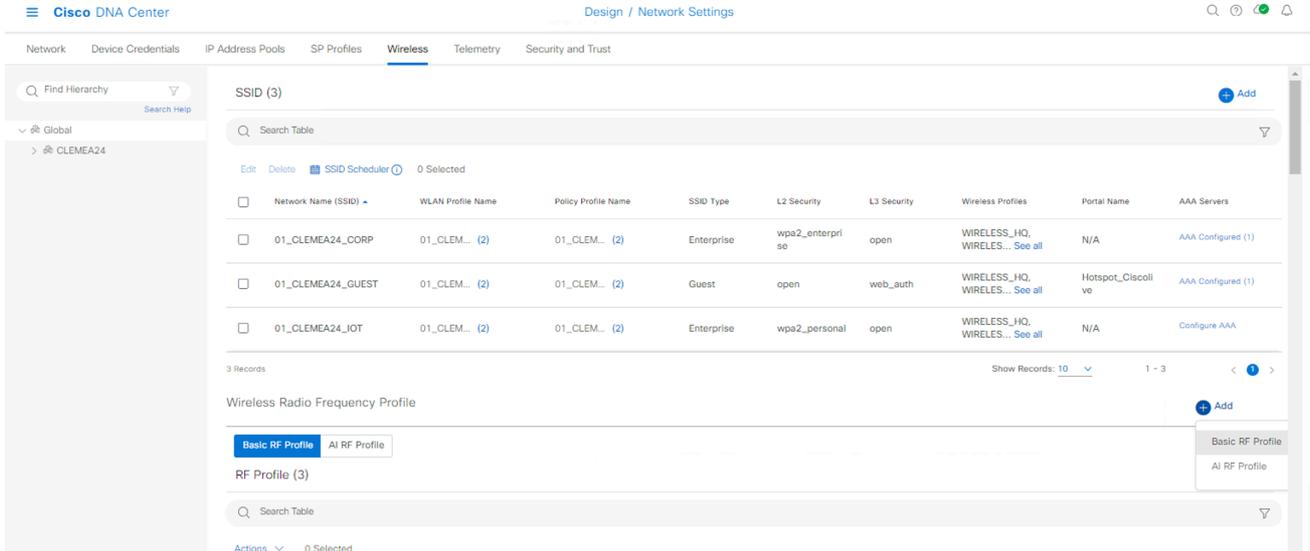
The configuration achieved in this section satisfies the custom requirements outlined at the beginning of the lab. The list below presents the details of the required configurations:

- *“At HQ we have 2 main areas, WAREHOUSE and OFFICE”*
- *“At Office, we only need 5GHz band enabled, with dynamic low power (from -10dBm to 11dBm) and Minimum data rate 12Mbps as Supported but 24Mbps as Mandatory.”*
- *“At Warehouse we must use 2,4GHz as we have old RF Scanners, make sure to use non-overlapping channels, allow Legacy data rates with Minimum Supported Rate 6Mbps and 11Mbps as Mandatory”*
- *“At RB we only have OFFICE area”*

In order to satisfy the RF requirements, we must work with RF Profiles and AP Zones.

- Under **Global**, navigate to **Design > Network Settings > Wireless**, locate the **RF Profile** section
- Click on **Add > Basic RF Profile**:

**Figure 109 Wireless Settings - RF Profile - Add**



We will start by creating the WAREHOUSE RF Profile. Apply the settings for 2.4 GHz band as per the below image and leave the 5 GHz settings to default:

**Table 19 RF Profile – WAREHOUSE Requirements**

Profile Name	WAREHOUSE	
	2.4GHz	5GHz
<b>Parent Profile</b>	Custom	Default
<b>DCA Channels</b>	1,6,11	Default
<b>Enable 802.11b data rates</b>	Enabled	N/A
<b>Supported Data Rates</b>	6 Mbps and above	Default
<b>Mandatory Data Rates</b>	11	Default
<b>Tx Power</b>	10 to 30	Default

**Figure 110 RF Profile - WAREHOUSE**

Edit Wireless Radio Frequency Profile

Profile Name  
WAREHOUSE

---

PROFILE TYPE

2.4 GHz

Parent Profile

High Medium (Typical) Low **Custom**

DCA Channel

Select All

1  6  11

Advanced Options

Select All

Show Advanced

---

Supported Data Rate

Enable 802.11b data rates

1 2 5.5 6 9 11 12 18 24 36 48 54

Mandatory Data Rates Choose upto two data rate

1  2  5.5  6  9  11  12  18  24  36  48  54

---

TX Power Configuration

Power Level

-10dBm 10dBm 30dBm

TPC Power Threshold

-80dBm -70dBm -65dBm -50dBm

RX SOP  
Medium

Leave 5GHz and 6GHz tabs as Default, Click **Save**

We will now continue to create the **OFFICE** RF Profile.

- Add New **Basic RF Profile**
- Disable 2.4 GHz band knob, accept the warning.
- Go to 5GHz tab.
- Apply the 5 GHz parameters as per the screenshot below:

**Table 20 RF Profile – OFFICE Requirements**

Profile Name	OFFICE	
	2.4GHz	5GHz
Parent Profile	Disabled	Click <b>Medium</b> (but it will change to Custom)
Channel Width		20 MHz
DCA Channels		UNII-1 (36, 40, 44, 48)

		UNII-2 (All channels except 120, 124, 128)
<b>Supported Data Rates</b>		12 Mbps and above
<b>Mandatory Data Rates</b>		24 Mbps
<b>Tx Power</b>		-10 to 11



The parent profile is a template for LOW, TYPICAL and HIGH Density, it defines the RXSOP Config among other parameters.

**Figure 111 RF Profile – OFFICE 2.4GHz Band**

### Create Wireless Radio Frequency Profile

Profile Name\*

OFFICE

2.4 GHz

5 GHz

6 GHz

2.4 GHz



## Figure 112 RF Profile – OFFICE 5 GHz Band

[Cisco DNA Center](#) [Design / Network Settings / Edit RF Profile](#)

---

Wireless / Edit RF Profile

2.4 GHz **5 GHz** 6 GHz

5 GHz

Parent Profile

High Medium (Typical) Low **Custom**

Channel Width  
20 MHz

Zero Wait DFS

DCA Channel

Select All

UNII-1 36-48  UNII-2 52-144  UNII-3 149-173

36  40  44  48  52  56  60  64  149  153  157  161

100  104  108  112  165  169  173

116  120  124  128

132  136  140  144

Hide Advanced

Supported Data Rate

6 9 12 18 24 36 48 54

Mandatory Data Rates Choose upto two data rate

6  9  12  18  24  36  48  54

TX Power Configuration

Power Level

-10 11 30dBm

RX SOP  
Auto

Leave the rest of the settings as **Default** and click **Save**.

Once created, the RF Profiles section will look as follows:

## Figure 113 RF Profiles - Summary

RF Profile (5)

Search Table

Actions 0 Selected

Profile Name	Type	2.4Ghz Data Rates	5Ghz Data Rates	6Ghz Data Rates	Channel Width (2.4/5/6GHz)	Profile Type
HIGH	2, 4, 5, 6	9,12,18,24,36,48,54	12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System
LOW	2, 4, 5, 6	1,2,5,5,6,9,11,12,18,24,36,48,54	6,9,12,18,24,36,48,54	6,9,12,18,24,36,48,54	20 MHz / Best / Best	System
OFFICE	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 / 20 MHz / Best	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 / Best / Best	System
WAREHOUSE	2, 4, 5, 6	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 / 20 MHz / Best	Custom

5 Records Show Records: 10 1 - 5

## Step 2: Working with Model Config

Model Config allows to apply settings that are not part of the global Network Settings to support specific use cases.

- “Enable Aironet IE in CORP SSID as it will be used for a site survey with Ekahau”

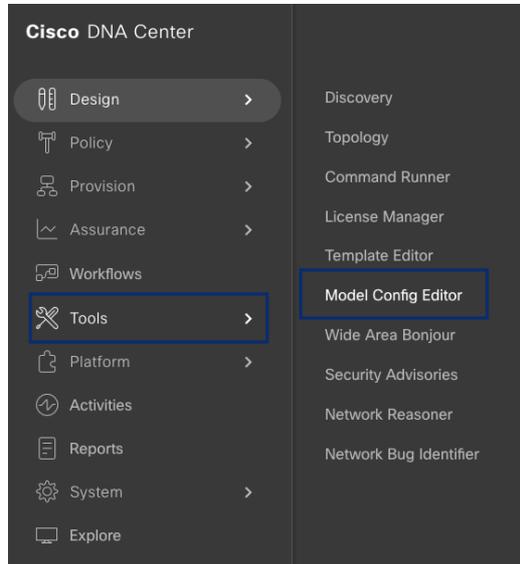


Enabling Aironet IE on the SSID adds AP Hostname to the wireless beacons. This can be used by surveyors to easily position the AP on the maps.

In order to meet the requirement, the tool “Model Config Editor” will be used to apply this setting to the CORP SSID.

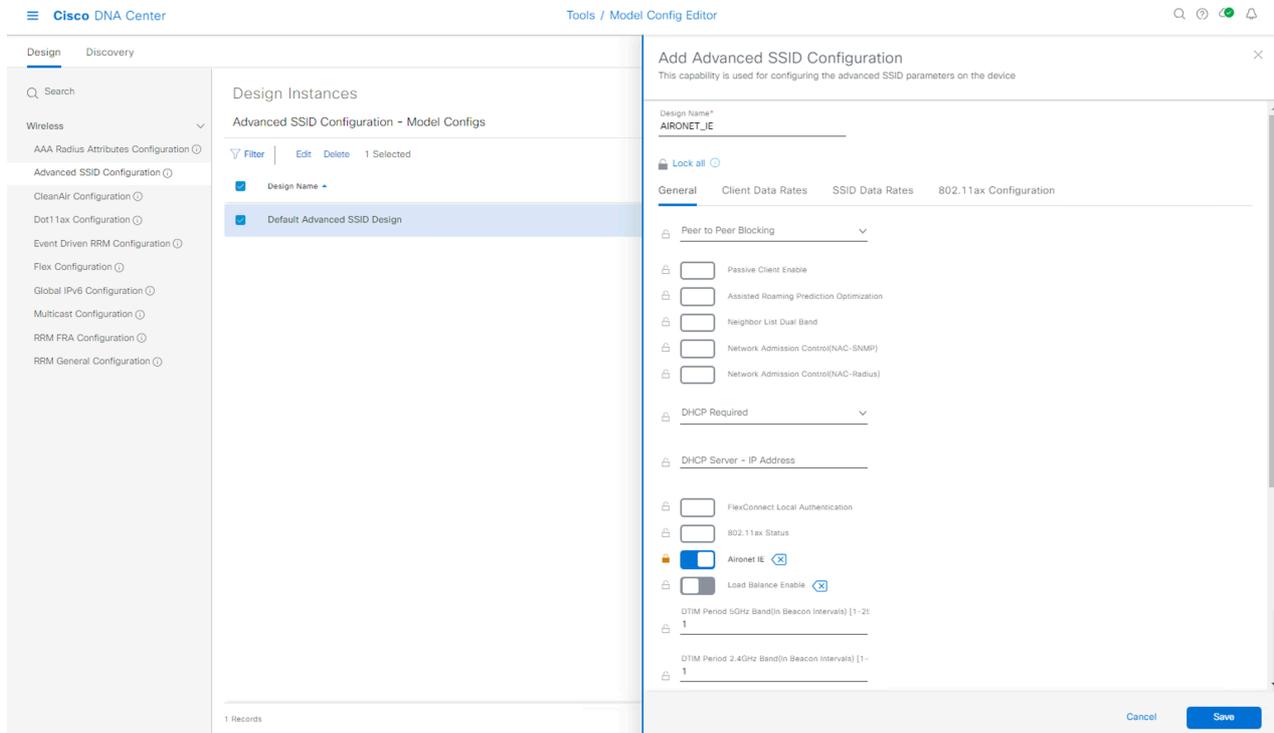
- Navigate to **Tools > Model Config Editor:**

Figure 114 Model Config Editor



- Choose **Advanced SSID Configuration** and click on **Add**.
- Name the Design as **AIRONET\_IE** and populate the config as per the screenshot below
- Click on **Save**

Figure 115 Model Config – Aironet IE



Model Config is saved successfully.

## Step 3: Working with Template Hub

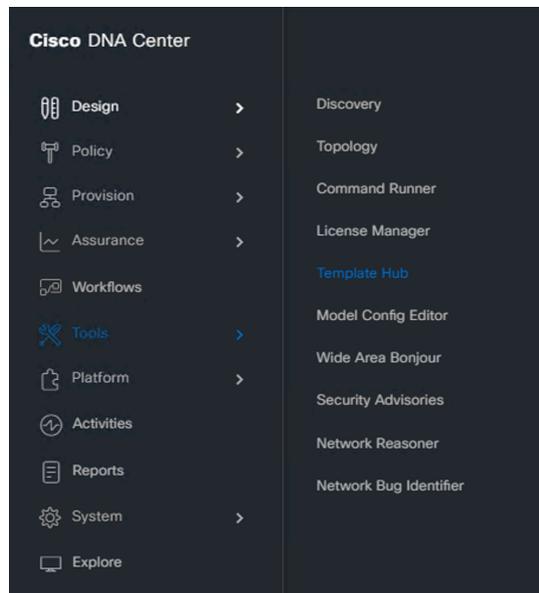
For any configurations that are not part of the Network Settings or Model Config, Template Hub can be utilized to push CLI-based configs to the devices.

In this lab exercise we will use Template Hub to satisfy RF requirements:

- Static RF Leader for both bands
- Increase DCA interval on 2,4GHz and 5GHz bands to 12 hours with anchor time set to 4
- Remove channels 120 124 128 from DCA global channel plan.

Navigate to **Tools > Template Hub**

Figure 116 Tools - Template Hub



Click the “+Add” icon and choose **New Template**. Fill the required information:

Table 21 CLI Templates – Values

Parameter	Value
-----------	-------

<b>Template Name</b>	9800 Global RF Parameters
<b>Project Name</b>	Onboarding Configuration
<b>Template Type</b>	Regular Template
<b>Template Language</b>	JINJA
<b>Software type</b>	IOS-XE
<b>Device Details</b>	<b>Add Device Details</b> Add 9800 WLCs (see <i>screenshot below</i> )

**Figure 117 Template Hub – Add Device Details**

The screenshot shows the 'Add Device Details' page in the Cisco Template Hub. At the top, there is a breadcrumb 'Add New Template / Add Device Details' and a close button. Below this is the title 'Add Device Details'. A dropdown menu for 'Device Family\*' is set to 'Wireless Controller'. A search bar contains the text '9800'. Below the search bar, there are two tabs: 'Device Series' (selected) and 'Device Models'. Under the 'Device Series' tab, there is a 'Device' dropdown menu. Below this, there are two search results, each with a checked checkbox: 'Cisco Catalyst 9800 Series Wireless Controllers' and 'Cisco Catalyst 9800 Wireless Controllers for Cloud'.

Make sure to choose **Cisco Catalyst 9800 Wireless Controllers for Cloud** as Device Type:

**Figure 118 Template Hub – Template Details**

Add New Template
✕

---

**Template Details**  
Define the properties for the template.

Template Name\*  
9800 Global RF Parameters

---

Project Name\*  
Onboarding Configuration

---

Template Type  
 Regular Template    Composite Sequence

Template Language  
 JINJA    VELOCITY

Software Type\*  
IOS-XE

---

**Device Type Details**  
Add the types of devices you want to associate with the template

DEVICE DETAILS\*   [Edit Device Details](#)

Device Family	Wireless Controller
Devices	Cisco Catalyst 9800 Series Wireless Controllers Cisco Catalyst 9800 Wireless Controllers for Cloud

---

> Additional Details

- Click in **Continue** to edit the Template.



Template hub is a powerful tool, you can create templates with variables to be filled with values upon provisioning, for now we will push static values

- Populate the Template with following content:

```
ap dot11 24ghz rrm group-mode leader
ap dot11 5ghz rrm group-mode leader
ap dot11 6ghz rrm group-mode leader

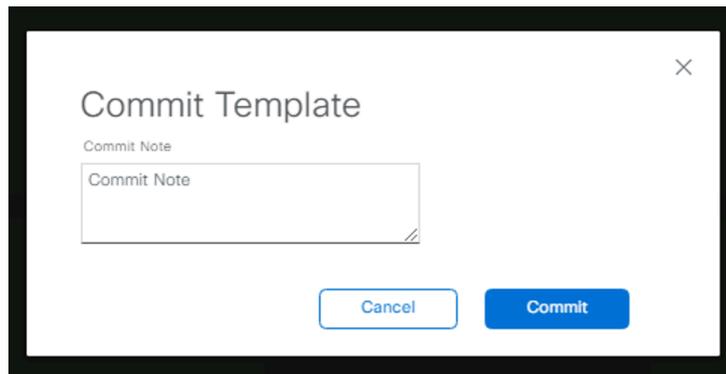
ap dot11 24ghz rrm channel dca interval 12
ap dot11 24ghz rrm channel dca anchor-time 4

ap dot11 5ghz rrm channel dca interval 12
ap dot11 5ghz rrm channel dca anchor-time 4

ap dot11 5 rrm channel dca remove 120
ap dot11 5 rrm channel dca remove 124
ap dot11 5 rrm channel dca remove 128
```

- Click on **Commit** for the CLI Template to be ready to be applied.
- Click **Commit** again on the confirmation page.

**Figure 119 Commit Template**



We could attach this template to the network profile in this section but we will do this later for all the other configured elements.

## Step 4: Configuring AP Profiles

As part of the requirements the customer defined that we must enable SSH access to APs to all APs at HQ and RB, for this we must use AP profiles.

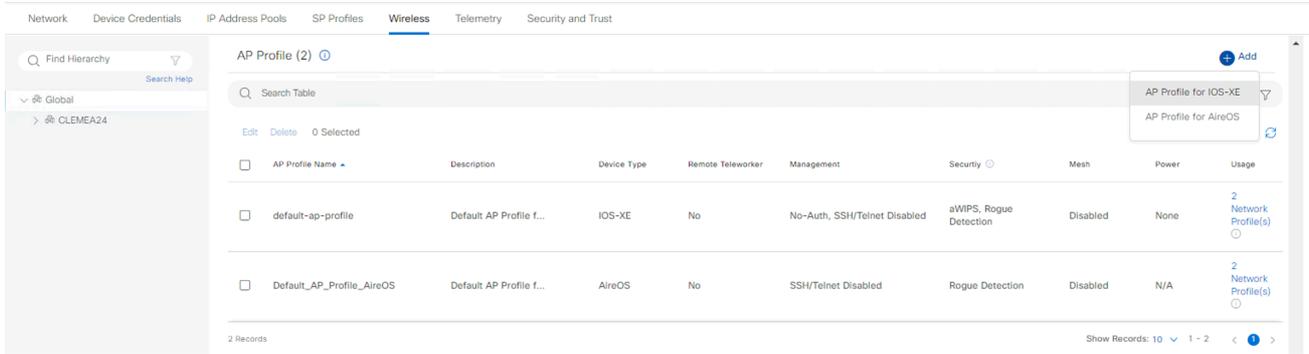


SSH AP Mgmt credentials: **admin / C1sco12345**

For this requirement to be satisfied, as it's needed on All APs in the company, you could edit the default AP profile, but for this lab we will create a new AP Profile:

- Navigate to **Design > Network Settings > Wireless**.
- At **global hierarchy**, scroll down and find **AP Profiles**
- Click **Add > AP Profile for IOS-XE**

**Figure 120 AP Profiles – Add AP Profile**



Use the information below to configure the RB AP Profile:

**Table 22 AP Profile –Requirements**

Parameter	Value
<b>AP Profile Name</b>	APJ_CLEMEA24
<b>Description</b>	SSH ON
<b>Access Point Authentication</b>	NO-AUTH
<b>SSH and Telnet</b>	[✓] SSH [ ] Telnet
<b>Username</b>	admin
<b>Password</b>	C1sco12345
<b>Enable Password</b>	C1sco12345

Figure 121 AP Profiles – Add AP profile

Wireless / Create AP Profile

Access Point Profile is used to manage and provision access points. AP Profiles can be assigned to sites by associating them to Wireless Network Profiles.

AP Profile Name\*

APJ\_CLEMEA24

[Hint](#)

Description

SSH ON

Check this box if this AP Profile is for Remote Teleworker APs or OEAPs.

Remote Teleworker ⓘ

Management Security Mesh Power Additional

Access Points Authentication ⓘ

These settings are applicable during PnP claim and for day-N authentication of AP. Changing these settings will be service impacting for the PnP onboarded APs and will need a factory-reset for those APs.

NO-AUTH

EAP-TLS

Extensible Authentication Protocol - Transport Layer Security (EAP-TLS). TLS uses certificate based authentication.

EAP-PEAP

Protected Extensible Authentication Protocol (EAP-PEAP). Enter the user name and the password and a certificate will be generated and applied during PnP claim process.

EAP-FAST

Flexible Authentication via Secure Tunneling (EAP-FAST). Enter the user name and the password to be applied during PnP claim process.

SSH and Telnet

Enable SSH and Telnet to add credentials for device management. If SSH and Telnet are disabled, credentials can still be added for console access.



SSH



Telnet

Username\*

admin

[View Username Policy](#)

Password\*

.....

[SHOW](#)

Enable Password\*

.....

[SHOW](#)

- Click **Save**

## Step 5: Configuring Network Profiles

So far, we have:

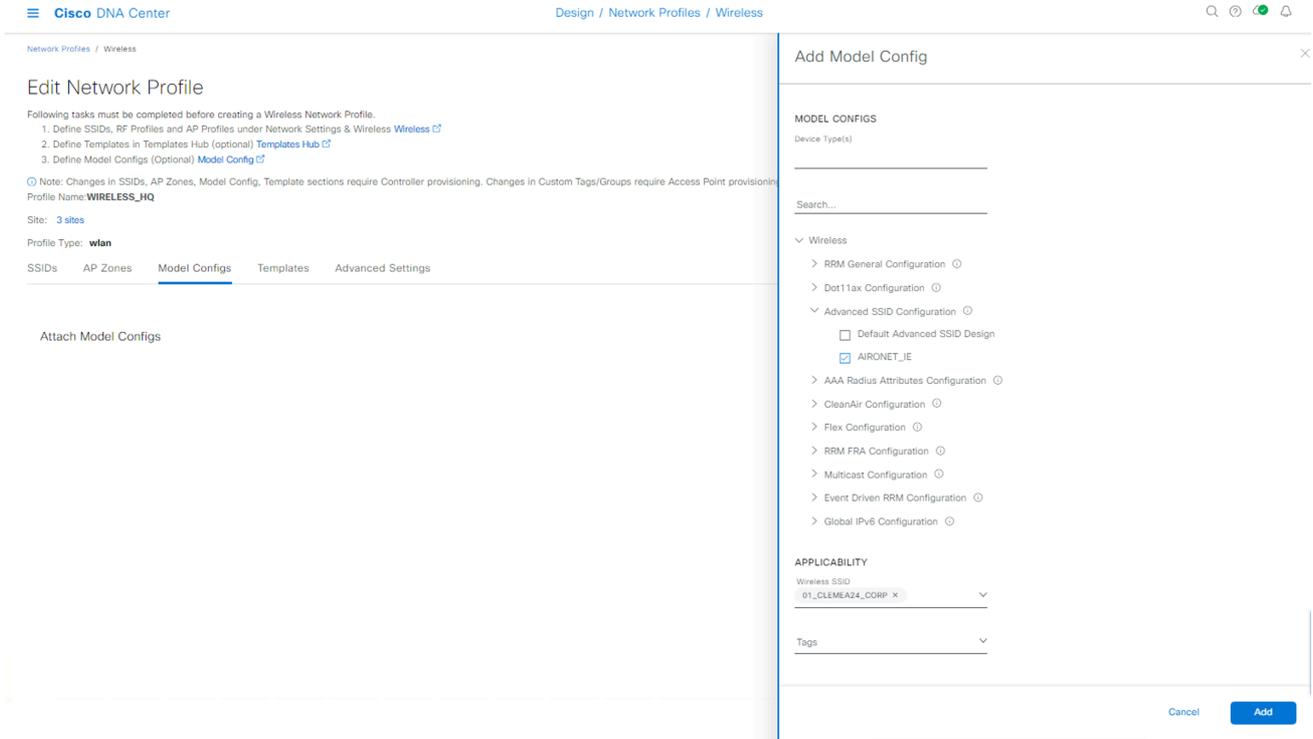
- Created two sites HQ and RB
- Created two Network Profiles to support HQ and Remote Branch settings.
- SSIDs were also associated with the Network Profiles.

Now we will proceed to link all the remaining settings (Model Config, CLI Templates, AP Zones, AP Profiles) to the respective sites also using **Network Profiles**.

## Step 6: Applying Model Config to the Network Profile at HQ

- Navigate to **Design > Network Profiles**.
- Click on **Edit** to modify **WIRELESS\_HQ** Network Profile.
- Navigate to **Model Configs** tab.
- Click on **Add Model Config**
- Expand "**Wireless**" and look for "**Advanced SSID Configuration**".
- Mark **AIRONET\_IE**
- Under **Applicability** select the Wireless SSID **XX\_CLEMEA24\_CORP**
- Click **Add**

Figure 122 Model Config - Add



Once added, Network Profile should have the Model Config applied as per the below image:

**Figure 123 Network Profile - Model Config - Summary**

Network Profiles / Wireless

## Edit Network Profile

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

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

Note: Changes in SSIDs, AP Zones, Model Config, Template sections require Controller provisioning. Changes in Custom Tags/Groups require Access Point provisioning.

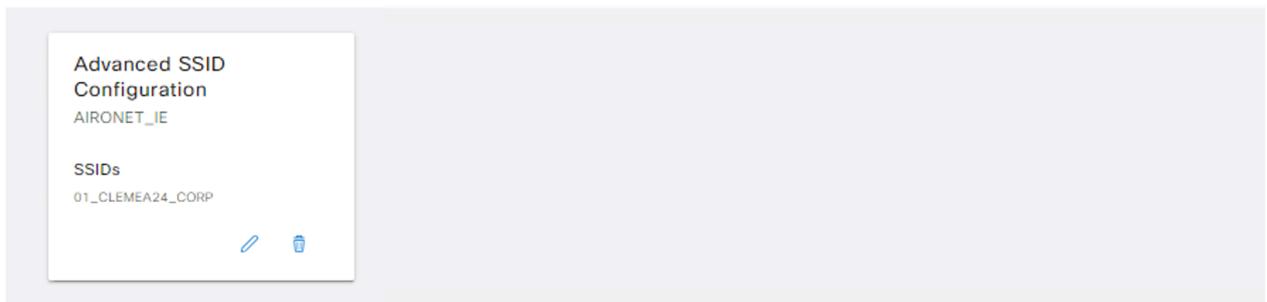
Profile Name: **WIRELESS\_HQ**

Site: [3 sites](#)

Profile Type: **wlan**

SSIDs   AP Zones   **Model Configs**   Templates   Advanced Settings

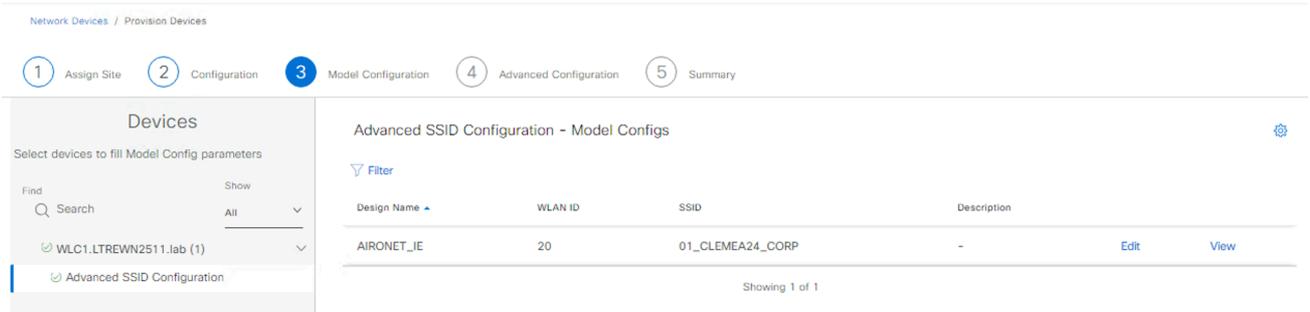
### Attach Model Configs



If you decide to provision the WLC now, you can expect Catalyst Center to push:  
- Aironet IE set to enabled only on the CORP WLAN Profile at HQ.

You'll find something like this in the provisioning process.

**Figure 124 Provisioning - Model Config**



No need to provision AP in this step as the config goes to an existing WLAN.

## Step 7: Applying CLI Template to the Network Profile at HQ

In order to apply the CLI Template to the HQ site,

- Navigate to **Design > Network Profiles**.
- Click on **Edit** to modify **WIRELESS\_HQ** Network Profile.
- Navigate to **Templates** tab.
- Click on **Add Template** and select previously created CLI Template named **9800 Global RF Parameters**
- Click on **Add**.

Figure 125 Network Profile - CLI Template

The screenshot displays the Cisco configuration interface for editing a network profile. The main page is titled 'Edit Network Profile' for the profile 'WIRELESS\_HQ'. It includes a list of tasks to complete before creating a profile and a note about provisioning requirements. The 'Templates' tab is active, showing an 'Attach Templates' section with 'No data Available'. An 'Add Template' modal is open on the right, showing a search for templates under 'Onboarding Configuration' with '9800 Global RF Parameters' selected.

When successfully applied, this is how the summary of Templates for WIRELESS\_HQ Network Profile presents:

## Figure 126 Network Profile - CLI Template

Network Profiles / Wireless

### Edit Network Profile

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

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

Note: Changes in SSIDs, AP Zones, Model Config, Template sections require Controller provisioning. Changes in Custom Tags/Groups require Access Point provisioning.

Profile Name: **WIRELESS\_HQ**

Site: [3 sites](#)

Profile Type: **wlan**

SSIDs   AP Zones   Model Configs   **Templates**   Advanced Settings

---

#### Attach Templates

9800 Global RF Paramet...

[View Device Type\(s\)](#)

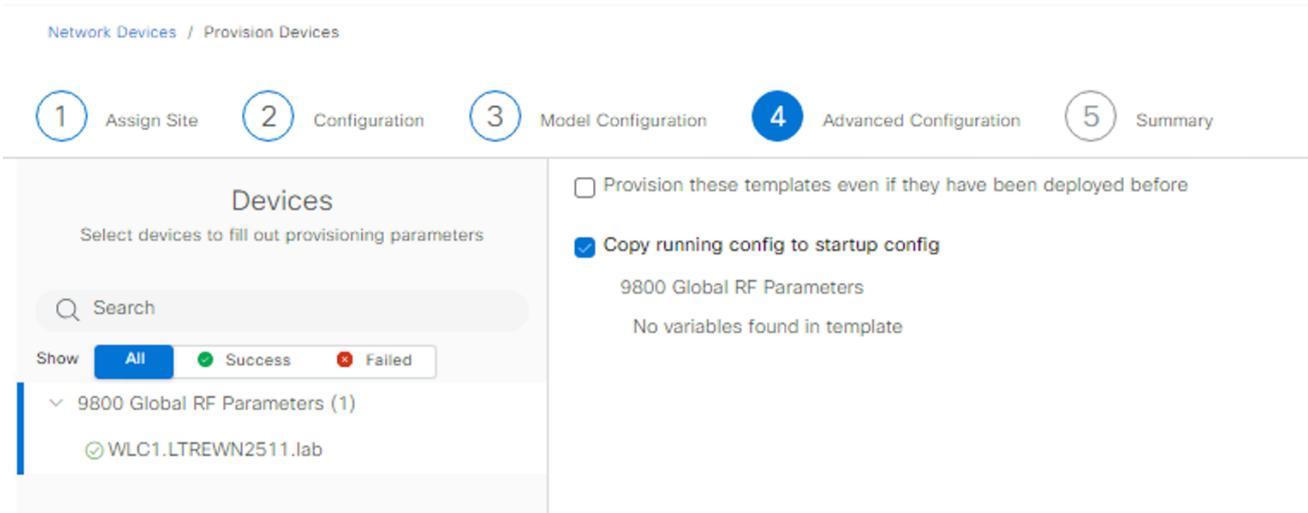
If you decide to provision the WLC now, you can expect Catalyst Center to push:

- Aironet IE set to enabled only on the CORP WLAN Profile at HQ (from previous task)
- The command lines to configure the global RF settings. (this is a global config so it also impacts RB)

No need to provision AP in this step as the config goes to an existing WLAN, and the rest is global.

You'll find something like this in the provisioning process.

**Figure 127 Provisioning – CLI Templates**



## Step 8: Applying the Custom AP Profile to an existing Site Tag

In order to apply the AP Profile to the HQ site,

- Navigate to **Design > Network Profiles**.
- Click on **Edit** to modify **WIRELESS\_HQ** Network Profile.
- Navigate to **Advanced Settings** tab.
- Expand **"Site Tags and AP Profiles"**
- Click **Create Custom Site Tag**

Map the APJ\_CLEMEA24 to the existing Site Tag corresponding to the building at HQ.

- Get the Site Tag name from the WLC using the command below (snippet)

```
WLC1#sh wireless tag site summary
```

```
Number of Site Tags: 3
```

Site Tag Name	Description
default-site-tag	default site tag
ST_CLEME_HQ_e673b_0	Site Tag ST_CLEME_HQ_e673b_0
ST_CLEME_RB_d6d66_0	Site Tag ST_CLEME_RB_d6d66_0

- Copy the **Site Tag** name from WLC and paste it to Catalyst Center **Site Tag Name**

- Map the **APJ\_CLEMEA24 Profile**
- Select **HQ** in the hierarchy.

The screenshot shows the Cisco DNA Center interface for creating a site tag. The main window is titled 'Create Site Tag'. It includes a 'NOTE' about custom site tags for remote teleworker floors. The 'Site Tag Name\*' field is filled with 'ST\_CLEME\_HQ\_e673b\_0'. The 'AP Profile\*' dropdown is set to 'APJ\_CLEMEA24', and the 'Flex Profile Name' is 'default-flex-profile'. Below this is a 'Select Sites' section with a search bar and a tree view showing a hierarchy: Global > CLEMEA24 > HQ (selected) > RB. At the bottom right, there are 'Cancel' and 'Save' buttons, with 'Save' being highlighted in blue.

- Click **Save**

If you decide to provision the WLC now, you can expect Catalyst Center to push:

- Aironet IE set to enabled only on the CORP WLAN Profile at HQ (from previous task)
- The command lines to configure the global RF settings. (this is a global config so it also impacts RB) (from previous task)
- The new AP Join Profile and Map it to the HQ Site Tag

No need to provision AP in this step as the config goes to an existing WLAN, Existing Site Tag and the rest is global.



If you decide to create a new Site Tag name with the new AP Profile you must provision the AP to see the changes reflected

## Step 9: Configuring AP Zones at HQ

AP Zones help us to create grouping of APs to assign different sets of SSIDs or RF characteristics to them.

In this task we will create two AP Zones inside HQ site.

- OFFICE will have CORP and GUEST SSIDs applied
- WAREHOUSE one will have all three SSIDs applied.

In order to create the AP Zones for the HQ site,

- navigate to **Design > Network Profiles**.
- Click on **Edit** to edit **WIRELESS\_HQ** Network Profile
- navigate to **AP Zones** tab.
- Define two AP Zones with following values:

**Table 23 AP Zones – HQ Requirements**

AP Zone Name	OFFICE	WAREHOUSE
<b>RF Profile</b>	OFFICE	WAREHOUSE
<b>SSID</b>	XX_CLEMEA24_CORP XX_CLEMEA24_GUEST	XX_CLEMEA24_CORP XX_CLEMEA24_GUEST XX_CLEMEA24_IOT

**Figure 128 Network Profiles - AP Zones**

Profile Name: WIRELESS\_HQ

Site: 3 sites

Profile Type: wlan

SSIDs AP Zones Model Configs Templates Advanced Settings

AP Zone will allow you to apply different SSID and RF Profile for set of APs on the same site. Device Tags can be used to Identify APs where you want to apply AP Zone. These configurations will be applied to APs only during AP provisioning.

If AP Zone is not assigned to any AP, then during AP provisioning, all SSIDs assigned to the network profile will be applied to AP and you will need to manually select RF Profile. AP zones will not be applicable to AP in Plug and Play flow.

 AP Zone configuration change requires Controller provision before Access Point provision. ✕

AP Zone Name\*  
OFFICE

Device Tags

Device Tags ▼

RF Profile\*  
OFFICE ▼

SSID\*

01\_CLEMEA24\_CORP (Non Flex) ✕

01\_CLEMEA24\_GUEST (Non Flex) ▼



AP Zone Name\*  
WAREHOUSE

Device Tags

Device Tags ▼

RF Profile\*  
WAREHOUSE ▼

SSID\*

01\_CLEMEA24\_CORP (Non Flex) ✕

01\_CLEMEA24\_IOT (Non Flex) ✕

01\_CLEMEA24\_GUEST (Non Flex) ▼



Click on **Save** for the changes to be applied.

If you decide to provision the WLC and AP now, you can expect Catalyst Center to push:

- Aironet IE set to enabled only on the CORP WLAN Profile at HQ (from previous task)
- The command lines to configure the global RF settings. (this is a global config so it also impacts RB) (from previous task)
- The new AP Join Profile and Map it to the HQ Site Tag (from previous task)
- Policy tags and RF Tags for each Area

Provisioning the HQ AP is crucial in order to complete the configuration as it tags the access point with the correct Policy Tag and RF Tag (WAREHOUSE OR OFFICE)

**Figure 129 Network Profiles - AP Zones**

The figure consists of two screenshots from the Cisco configuration interface, showing the 'Configuration' step of provisioning a network profile. Both screenshots show a table with columns for Serial Number, Device Name, AP Zone Name, and RF Profile. A dropdown menu is open for the RF Profile column, showing options: 01\_CLEMEA24\_IOT, 01\_CLEMEA24\_GUEST, and 01\_CLEMEA24\_CORP.

**Screenshot 1 (Warehouse):** The AP Zone Name is set to 'WAREHOUSE' and the RF Profile is set to 'WAREHOUSE'. The table row shows Serial Number 'FJC2234M44N' and Device Name 'AP7872.5DFB.8E78'. The RF Profile dropdown shows the value '3'.

**Screenshot 2 (Office):** The AP Zone Name is set to 'OFFICE' and the RF Profile is set to 'OFFICE'. The table row shows Serial Number 'FJC2234M44N' and Device Name 'AP7872.5DFB.8E78'. The RF Profile dropdown shows the value '2'.

Below the screenshots, a callout box with a book icon states: "This step is not needed for the RB site as the AP Zones requirement was for HQ only."

## Step 10: Applying Model Config to the Network Profile at RB

Repeat the process for Network Profile at RB

- Navigate to **Design > Network Profiles**.
- Click on **Edit** to modify **WIRELESS\_RB** Network Profile.
- navigate to **Model Configs** tab.
- Click on **Add Model Config**
- Expand "**Wireless**" and look for "**Advanced SSID Configuration**".
- Mark **AIRONET\_IE**
- Under **Applicability** select the Wireless SSID **XX\_CLEMEA24\_CORP**
- Click **Add**

## Step 11: Applying CLI Template to the Network Profile at RB

This step is not technically needed as it is pushed with the HQ config. You could map it for consistency.

## Step 12: Applying the Custom AP Profile to an existing Site Tag

In order to apply the AP Profile to the RB site,

- Navigate to **Design > Network Profiles**.
- Click on **Edit** to modify **WIRELESS\_HQ** Network Profile.
- navigate to **Advanced Settings** tab.
- Expand "**Site Tags and AP Profiles**"
- Click **Create Custom Site Tag**

Map the APJ\_CLEMEA24 to the existing Site Tag corresponding to the building at HQ.



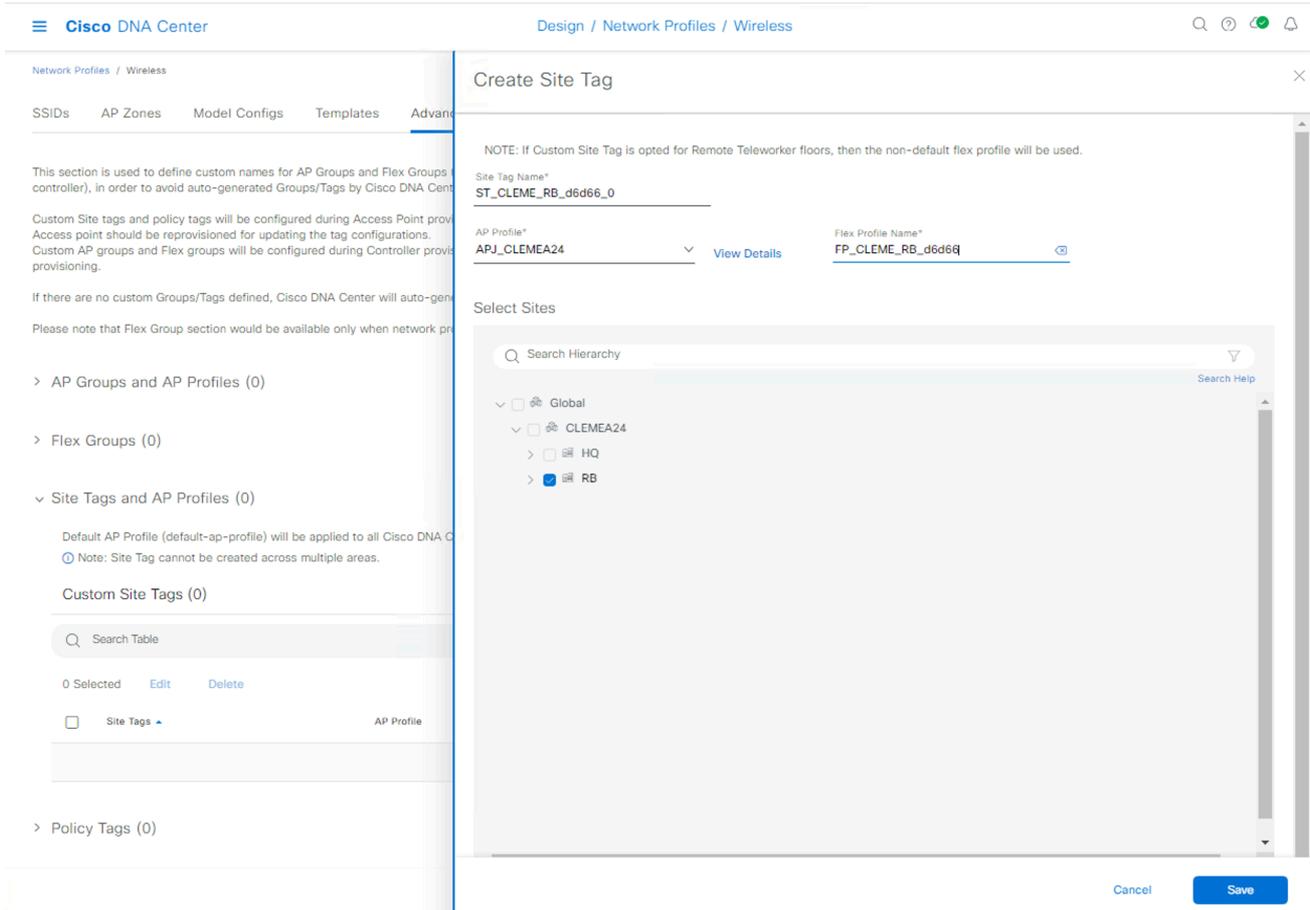
Since this is a Flex site we also need to collect the **Flex Profile Name**.

- **Get the name from WLC using the command below (snippet)**

```
WLC1#sh run | s tag site
wireless tag site default-site-tag
  description "default site tag"
wireless tag site ST_CLEME_HQ_e673b_0
  ap-profile APJ_CLEMEA24
  description "Site Tag ST_CLEME_HQ_e673b_0"
wireless tag site ST_CLEME_RB_d6d66_0
  description "Site Tag ST_CLEME_RB_d6d66_0"
  flex-profile FP_CLEME_RB_d6d66
no local-site
```

- Copy the **Site Tag** and **Flex Profile** Name from WLC and paste it to Catalyst Center
- Map the **APJ Profile**
- Select **RB** in the hierarchy

**Figure 130 Network Profiles – Reusing Existing Site Tag**



**Table 24 Customer Requirements (Status so far)**

No	Description	Task	Status
1	Allow legacy scanners to work in Warehouse area of HQ. Disable 2.4GHz in the Office space of HQ	Task 9 Step 1	Completed
2	For the site survey purpose, enable Aironet IE for CORP SSID	Task 9 Step 2	Completed
3	Static RF Leader for both bands	Task 9 Step 3	Completed
4	Increase DCA interval on 2,4GHz and 5GHz bands to 12 hours with anchor time set to 4	Task 9 Step 3	Completed
5	Remove channels 120 124 128 from DCA global channel plan	Task 9 Step 3	Completed
6	Enable SSH on all APs HQ and RB with credentials admin/C1sco12345	Task 9 Step 4	Completed

7	No need for IOT SSID in the OFFICE area at HQ site	Task 9 Step 9	Completed
8	Define Primary WLC to all APs Rename APs at RB	Task 9 Step 13	
9	Disable LEDs to APs at HQ	Task 9 Step 13	

## Step 13: Working with AP Workflows

In order to satisfy the requirements of defining the Primary WLC Hostname and IP Address, renaming the RB AP and disabling LEDs for HQ APs, AP Workflows will be utilized.

- Go to **Workflows > Configure Access Points** and create new Task named **Primary WLC and Rename RB AP**

### Figure 131 AP Workflows Steps

## 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\*

Primary WLC and Rename RB AP

Proceed by selecting all the options under **Configure AP and Radio Parameters**:

## Figure 132 AP Workflows Steps

### How do you want to configure APs?

Choose how you want to configure the AP and Radio parameters.

#### Configure AP And Radio Parameters

---

Choose which steps to configure relevant parameters on the selected APs.

#### Schedule Recurring Events For AP And Radio Parameters

---

You can configure the Admin and LED status of the AP and the Radio Admin status as recurring events.

Select the steps you want to configure

- Modify AP Name
- Configure AP Parameters
- Configure 5 GHz Radio Parameters
- Configure 2.4 GHz Radio Parameters
- Configure 6 GHz Radio Parameters
- Configure Dual-Band (XOR) Radio Parameters
- Configure Tri-Radio Parameters

Select the RB AP:

## Figure 133 AP Workflows Steps

### Select Access Points

Select reachable APs to configure. APs can be selected from both Assigned APs and Unassigned APs Tab.

AP Name	Ethernet MAC Address	IP Address	AP Mode	Reachability	Associated WLC IP	MAC Address	Site	Device Tags	Image Version	Series
AP7872.SDFB.8E78	78-72:5d:fb:8e:78	10.0.101.12	FlexConnect	Reachable	198.19.11.10	78-72:5d:fc:07:40	.../CLEMEA24/RB/GF	--	17.9.4.27	Cisco 44

We will start by changing the AP Hostname for the RB AP. We will use the **RB-GF-AP01** hostname for this AP.

## Figure 134 AP Workflows Steps – Rename AP

### Modify AP Name

This is an optional step. Use the sample CSV file to enter a new name for each AP, or create a new naming convention. You can also edit individual APs.

Create a Naming Convention  Upload a CSV File

#### Bulk Access Point Naming

To edit the names of the selected APs, change the AP name below to a custom name. Cisco DNA Center will use "###" to allot a logical numerical sequence to the selected APs.

AP Name  
AP-###  [Apply Pattern](#)  
Sample Naming: AP-001

AP Name	New AP Name
AP7872.5DFB.8E78	RB-GF-AP01

Once applied, we will continue to define the WLC Hostname and IP address for the AP. Enable **High Availability** checkbox and specify following information:

- Select Primary Controller Name - **WLC1**
- Primary Controller IP Address – **198.19.11.10**

**Figure 135 AP Workflows Steps – Primary WLC**

### Configure AP Parameters

Select parameters to configure. These parameters will be applied to all the selected APs.

<input type="checkbox"/> Admin Status <input type="button" value="Enable"/> <input type="button" value="Disable"/>	<input type="checkbox"/> AP Failover Priority Select AP Failover Priority <input type="button" value="v"/>
<input type="checkbox"/> AP Mode ⓘ Select AP Mode <input type="button" value="v"/>	<input checked="" type="checkbox"/> High Availability ⓘ Select Primary Controller Name <b>WLC1</b> <input type="button" value="v"/>
<input type="checkbox"/> AP Location ⓘ <input type="checkbox"/> Use currently assigned site location ⓘ Enter Location <input type="text"/> <small>Max length: 255</small>	Select Secondary Controller Name <b>Inherit from site / Clear</b> <input type="button" value="v"/> ⓘ
<input type="checkbox"/> AP LED Status <input type="button" value="Enable"/> <input type="button" value="Disable"/>	Select Tertiary Controller Name <b>Clear</b> <input type="button" value="v"/>
<input type="checkbox"/> LED Brightness Level ⓘ Select Brightness Level <b>4</b> <input type="button" value="v"/>	Primary Controller IP Address <b>198.19.11.10</b>
	Secondary Controller IP Address <input type="text"/>
	Tertiary Controller IP Address <input type="text"/>

Skip the remaining Radio-related pages.

In the Schedule Provision select Now and click Next

Summary Page and optionally Preview the CLI

## Figure 136 AP Workflows Steps – Summary

### Summary

Review your AP configuration. To make any changes, click Edit. To apply the configuration, click Configure.

⚠ Some of the selected configurations could temporarily disrupt the wireless client connectivity.

[Preview the CLI](#)

> Task Name

∨ How do you want to configure APs? [Edit](#)

Non Recurring

∨ Select Access Points [Edit](#)

Total APs selected 1

∨ Modify AP Name [Edit](#)

Total AP names modified 1

∨ Configure AP Parameters [Edit](#)

Primary Controller Name WLC1

Secondary Controller Name/IP Address Inherit from site / Clear

Tertiary Controller Name/IP Address Clear

Primary Controller IP Address 198.19.11.10

## Figure 137 AP Workflows Steps – CLI Preview

### Summary

Review your AP configuration. To make any changes, click Edit. To apply the configuration, click Configure.

⚠ Some of the selected configurations could temporarily disrupt the wireless client connectivity.

[Preview the CLI](#)

> Task Name

∨ How do you want to configure APs?

Non Recurring

∨ Select Access Points

Total APs selected

∨ Modify AP Name

Total AP names modified

∨ Configure AP Parameters

Primary Controller Name

Secondary Controller Name/IP Address Inherit from site / Clear

Tertiary Controller Name/IP Address Clear

Primary Controller IP Address 198.19.11.10

### CLI Preview

Select a controller from the left panel and preview CLI configurations that will be provisioned to the device.

🔍 Search

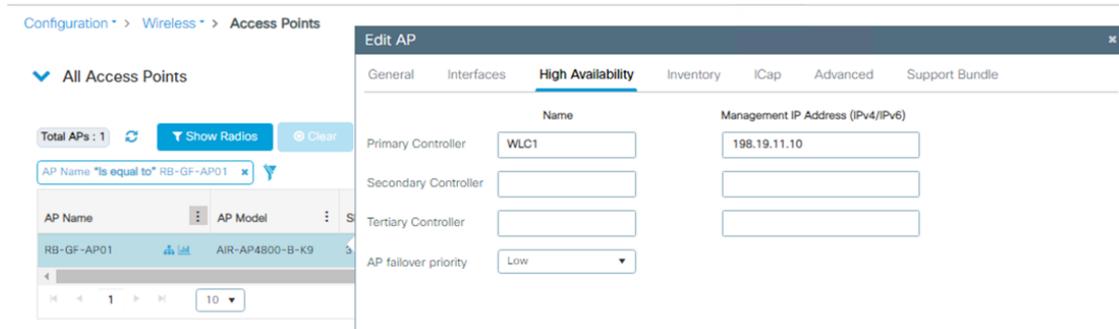
#### CONTROLLERS

198.19.11.10

Controller Name: WLC1.LTREWN2511.lab

```
do ap name AP7872.50F8.8E78 name RB-GF-AP01
do ap name RB-GF-AP01 controller primary "WLC1" 198.19.11.10
do ap name RB-GF-AP01 no controller secondary temName 0.0.0.0
do ap name RB-GF-AP01 no controller tertiary temName 0.0.0.0
```

Figure 138 AP Workflows Steps – Verify



Repeat the process to Disable LEDs to APs at HQ. Let us create the **Disable LED** AP Workflow first.

Figure 139 AP Workflows Steps – Disable LED

## 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\*  
Disable LED

We will limit this task to **Configure AP Parameters** only.

## Figure 140 AP Workflows Steps – Disable LED

### How do you want to configure APs?

Choose how you want to configure the AP and Radio parameters.

#### Configure AP And Radio Parameters

Choose which steps to configure relevant parameters on the selected APs.

#### Schedule Recurring Events For AP And Radio...

You can configure the Admin and LED status of the AP and the Radio Admin status as recurring events.

Select the steps you want to configure

- Modify AP Name
- Configure AP Parameters
- Configure 5 GHz Radio Parameters
- Configure 2.4 GHz Radio Parameters
- Configure 6 GHz Radio Parameters
- Configure Dual-Band (XOR) Radio Parameters
- Configure Tri-Radio Parameters

Select the **HQ-F1-AP01** AP and click **Next**:

### Figure 141 AP Workflows - AP Selection

Select Access Points

Select reachable APs to configure. APs can be selected from both Assigned APs and Unassigned APs Tab.

Assigned APs | Unassigned APs

Search Hierarchy

- Global (3)
- CLEMEA24
  - HQ
    - F1**
    - GF
  - RB

Access Points (1)

Filter devices

1 Selected

AP Name	Ethernet MAC Address	IP Address	AP Mode	Reachability	Associated WLC IP	MAC Address	Site	Device Tags	Image Version	Series
HQ-F1-AP01	04:5f:b9:ca:05:24	10.0.201.97	Local	Reachable	198.19.11.10	68:7d:b4:90:a3:60	./CLEMEA24/HQ/F1	--	17.9.4.27	Cisco Catalyst 9130AXI Series Unified Access Points

Check the **AP LED Status** box and set the value to **Disabled**.

### Figure 142 AP Workflows Steps – Disable LED

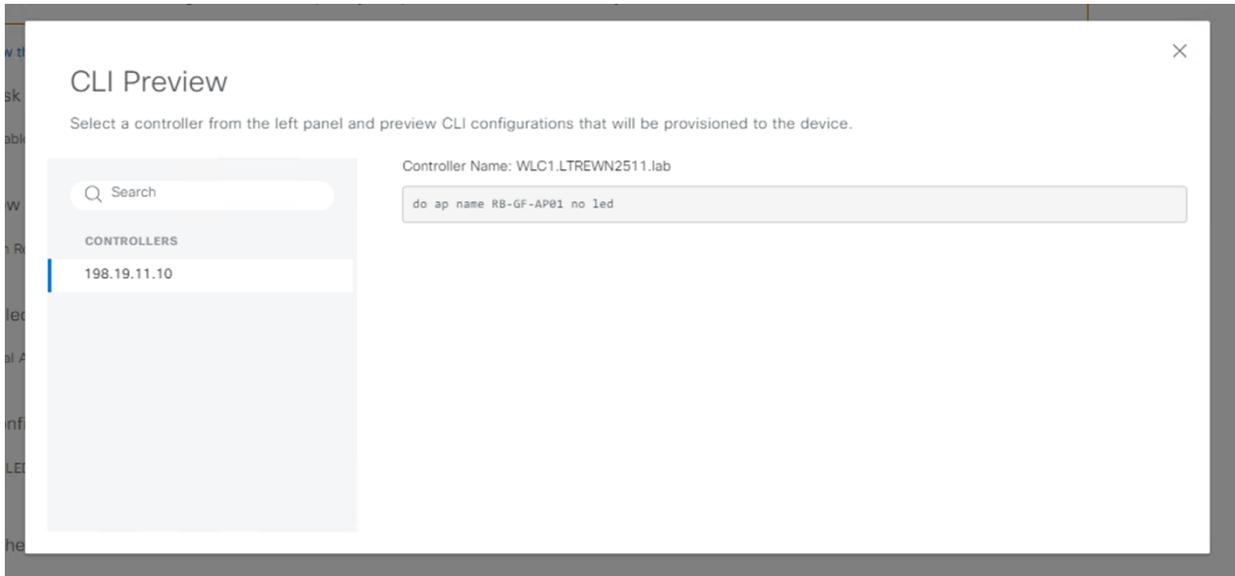
#### Configure AP Parameters

Select parameters to configure. These parameters will be applied to all the selected APs.

<input type="checkbox"/> Admin Status	<input type="checkbox"/> AP Failover Priority
<input type="button" value="Enable"/> <input type="button" value="Disable"/>	Select AP Failover Priority <input type="text"/>
<input type="checkbox"/> AP Mode ⓘ	<input type="checkbox"/> High Availability ⓘ
Select AP Mode <input type="text"/>	Select Primary Controller Name <input type="text"/>
<input type="checkbox"/> AP Location ⓘ	Inherit from site / Clear
<input type="checkbox"/> Use currently assigned site location ⓘ	Select Secondary Controller Name <input type="text"/>
Enter Location <input type="text"/>	Inherit from site / Clear
Max length: 255	Select Tertiary Controller Name <input type="text"/>
<input checked="" type="checkbox"/> AP LED Status	Clear
<input type="button" value="Enable"/> <input checked="" type="button" value="Disable"/>	Primary Controller IP Address <input type="text"/>
<input type="checkbox"/> LED Brightness Level ⓘ	Secondary Controller IP Address <input type="text"/>
Select Brightness Level <input type="text"/>	Tertiary Controller IP Address <input type="text"/>
4	

CLI preview should look something this:

**Figure 143 AP Workflows Steps – CLI Preview**



## Task 10: Client Connectivity Testing

Having configured all the devices deployed both in HQ and in Remote Branch, we will now focus on making sure that our wireless clients can connect to the SSIDs that we have created.

Additionally, we will be checking on their successful authentication results, IP Subnet assignments as well as proper resource reachability.

Additionally, we will be utilizing Catalyst Center Assurance to monitor client connection state and spot any potential issues.

- Open an RDP session to one of the Wireless Clients:

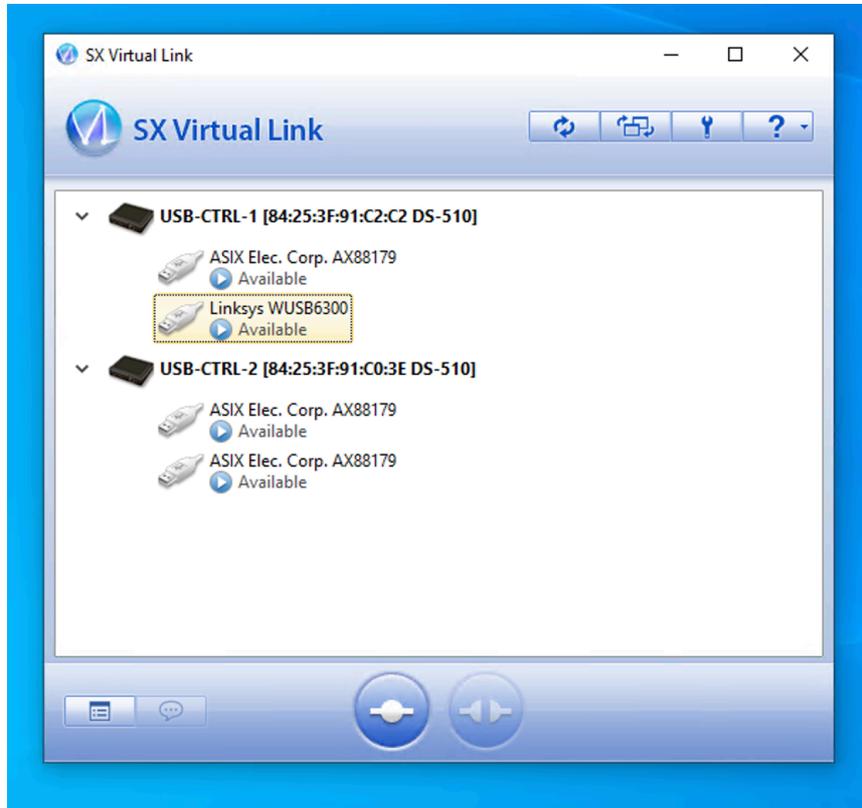
**Table 25 Wireless Clients Addressing and Credentials**

Name	IP Address	Username	Password	Preferred Access Method
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP
Client4	198.18.134.4	DCLOUD\admin	C1sco12345	RDP

### Step 1: Configure the wireless adapter

Open SX Virtual Link, Enable the Linksys WUSB6300 Adapter by clicking on the **“Connect”** button below

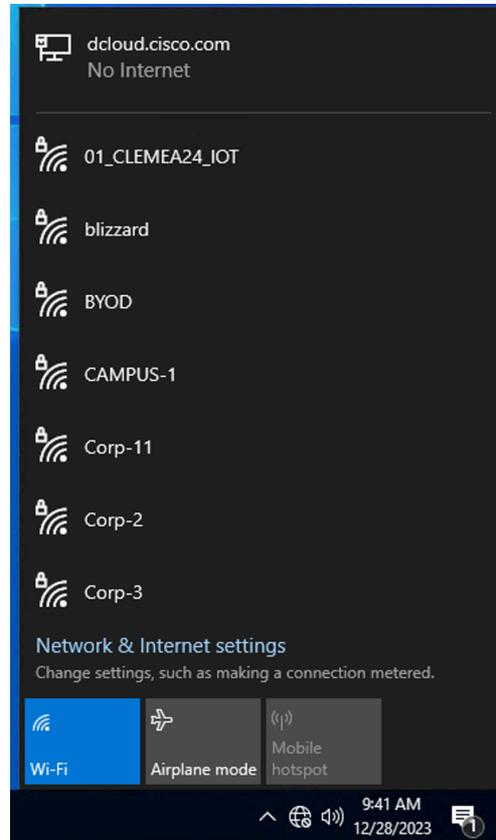
**Figure 144 Configure SX Virtual Adapter**



Then connect to the desired SSID using the default network manager in Windows

## Step 2: Test IOT SSID

**Figure 145 Client Connectivity Testing**



Verify using CMD if the wireless client gets an IP address from the desired VLAN.  
The below example is for IOT at the HQ

Figure 146 Client Connectivity Testing – Verify IP with ipconfig

```
Windows IP Configuration

Ethernet adapter Ethernet0 3:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 198.18.134.1
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6cba:984d:9a37:23a9%16
    IPv4 Address. . . . . : 10.0.213.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.213.1

C:\Users\admin.DCLOUD>
```

Also verify on the WLC if the client is in RUN State  
Go to the WLC UI, **Monitoring > Clients**

Figure 147 Client Connectivity Testing – Verify in WLC

The screenshot shows the Cisco WLC Monitoring > Clients page. The breadcrumb navigation is 'Monitoring > Wireless > Clients'. There are three tabs: 'Clients', 'Sleeping Clients', and 'Excluded Clients'. The 'Clients' tab is active. Below the tabs, there are 'Delete' and 'Refresh' buttons. A message says 'Selected 0 out of 1 Clients'. Below that is a table with the following data:

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name
c441.1e83.4520	10.0.213.11	fe80::6cba:984d:9a37:23a9	HQ-F1-AP02	01_CLEMEA24_IOT	17	WLAN	Run	11ac	

At the bottom of the table, there is a pagination control showing '1' of '10' items and '1 - 1 of 1 clients'.

### Step 3: Test CORP SSID

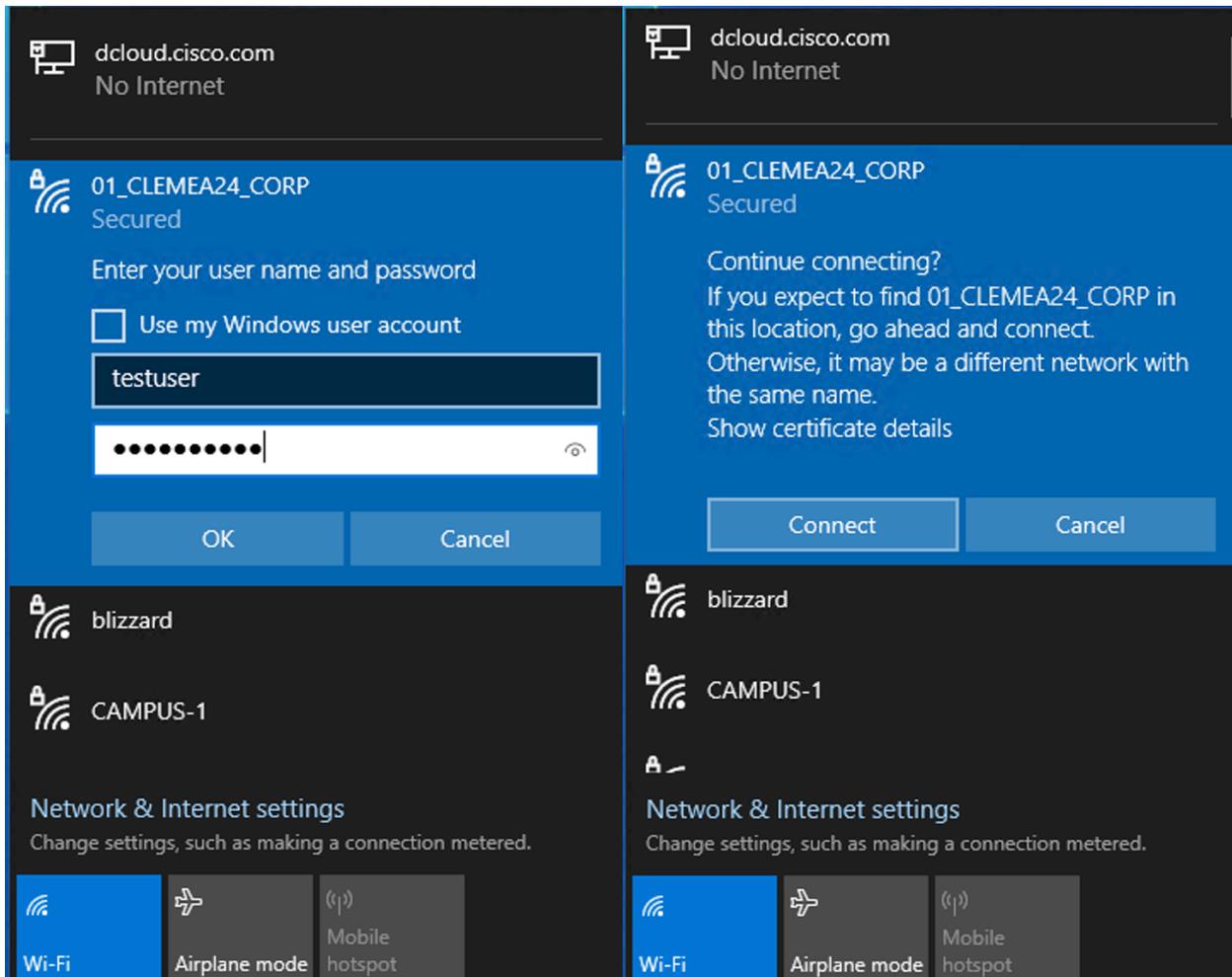
- RDP to a wireless client

- Make sure the SX Virtual Link has the **WUSB6300** connected.
- Connect to CORP SSID using the credentials:

**Username:** testuser

**Password:** C1sco12345

**Figure 148 Client Connectivity Testing – CORP SSID**



## Step 4: Test GUEST SSID

- RDP to a wireless client
- Make sure the SX Virtual Link has the **WUSB6300** connected.
- Connect to GUEST SSID
- Wait for a redirection

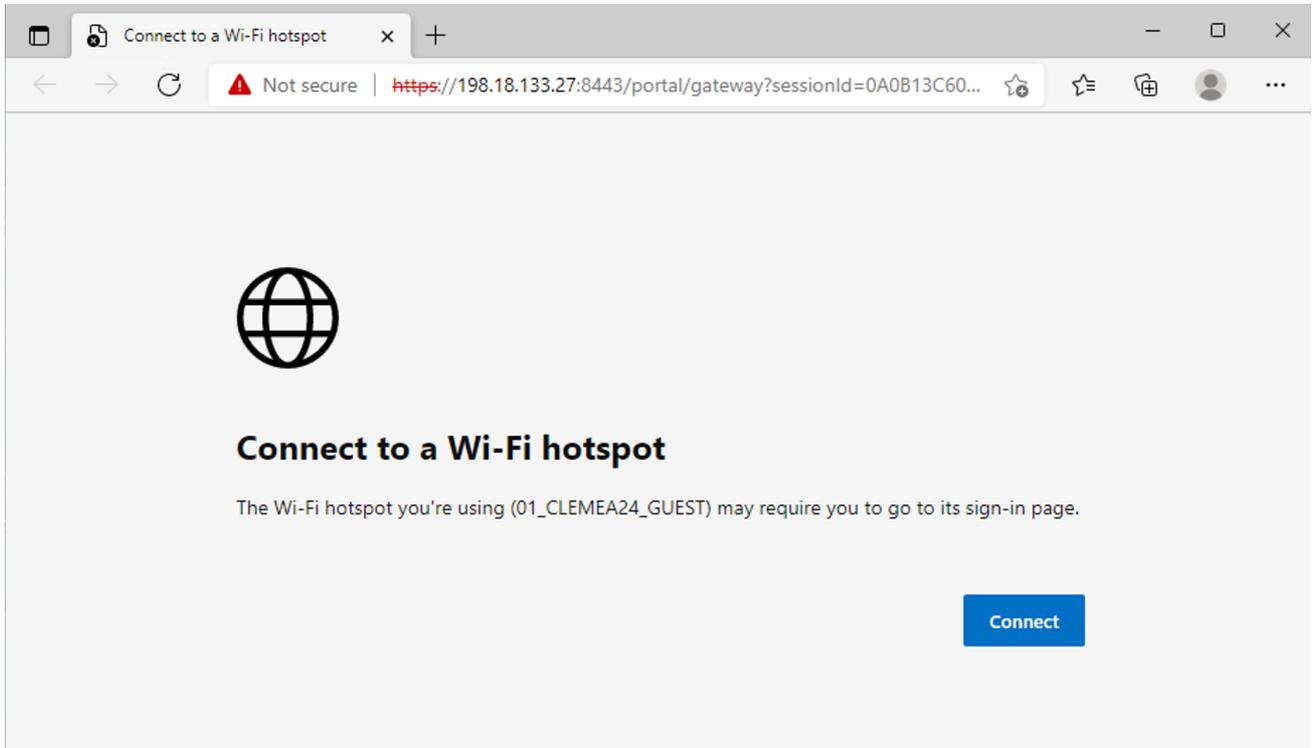


In case you get a page like the one below do the following steps:

1. Click in the page,
2. type "thisisunsafe" (even if it's not showing anywhere)
3. hit ENTER,
4. then reload page

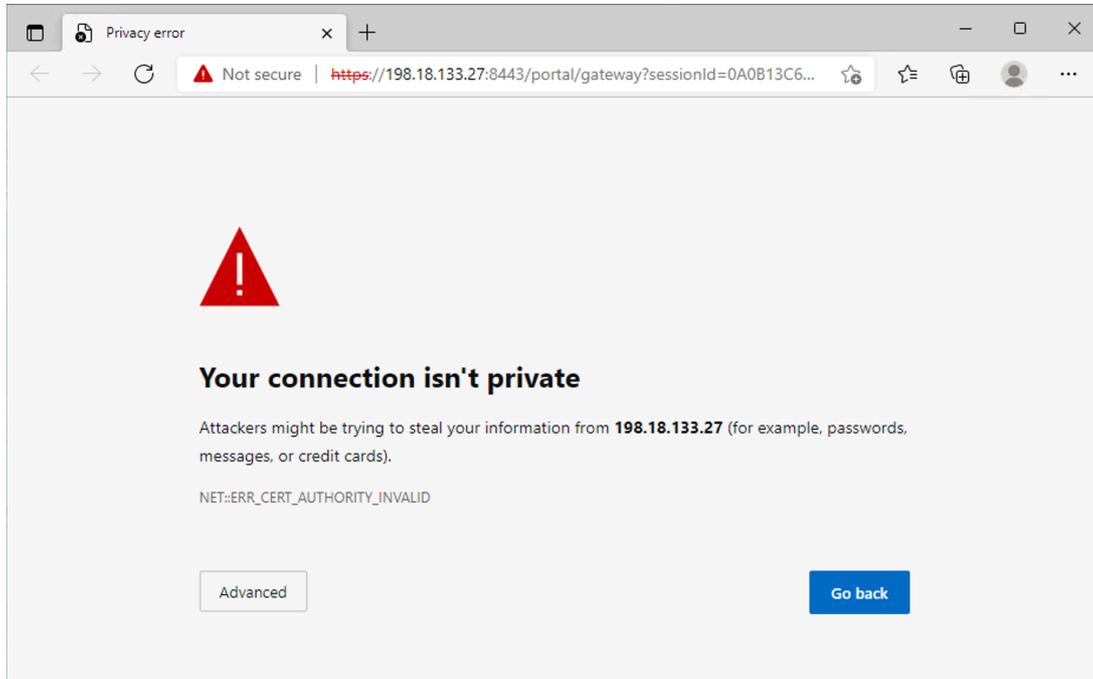
Then you should see the normal warning page. This is expected as ISE does not have a trusted Root CA installed for this purpose.

**Figure 149 Client Connectivity Testing – Browser Warning**



- Click advanced and proceed to the captive portal

- **Figure 150 Client Connectivity Testing – Browser Warning**





## Task 11: Bonus Tasks – Anchoring

With Catalyst Center's Anchor Groups feature, you can create with up to three Cisco Wireless Controllers per anchor group and set the priority for each of the anchors.

Priority order of the anchors determines the traffic sharing across the anchors:

- **Equal sharing:** When the priority order of all the anchors is the same (for example, 1, 1, and 1).
- **Partial sharing:** When the priority order of more than one anchor is the same (for example, 1, 1, and 2).
- **Sequential sharing:** When the priority order of the anchors is sequential (for example, 1, 2, and 3).



In order to use anchoring you must add at least one anchor to an anchor group.

You can add the following devices as anchors:

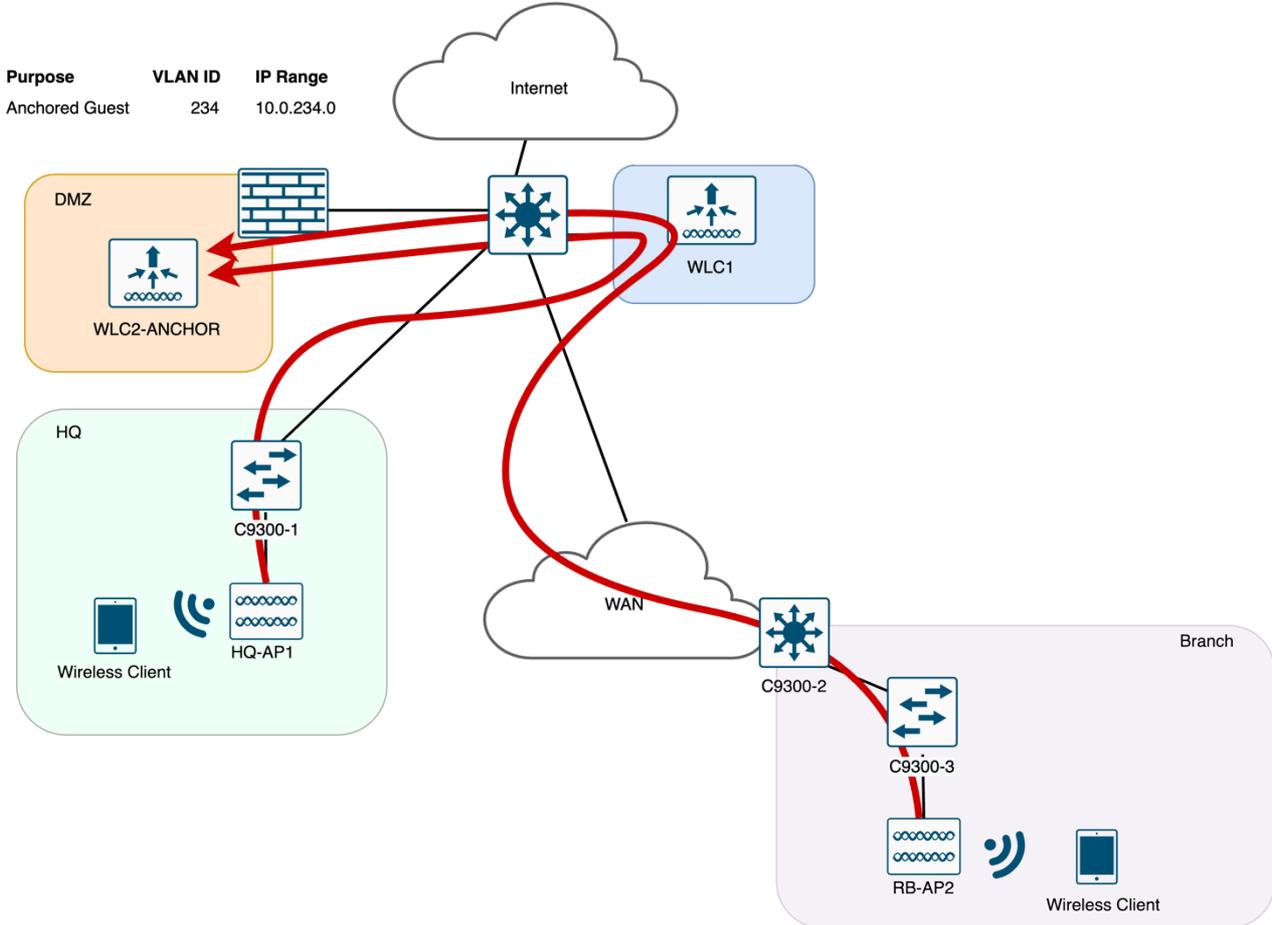
- Cisco Wireless Controllers that are managed by Cisco DNA Center.
- Cisco Wireless Controllers that are not managed by Cisco DNA Center (external wireless controllers).

### Anchoring SSID to a Managed Anchor WLC

In this section participants will learn how to anchor the GUEST SSID to an Anchor WLC located in a DMZ that is Managed by Catalyst Center.

This is a common architecture that increases security by segmenting the GUEST traffic encapsulating it to the DMZ behind a Firewall like the figure below:

**Figure 152 Topology – Anchoring GUEST with Managed WLC**



## Step 1: Add Anchor WLC to Inventory

The first thing is to Discover the Anchor WLC, referred to as **WLC2-ANCHOR**

Navigate to the Dashboard top menu and click on **Provision > Inventory**

On the Inventory page, click **“Add Device”**

- WLC IP address is **198.19.12.10**
- Select the **“Write” Global credentials** for CLI, SNMP
- Make sure to use NETCONF port **830**

**Figure 153 Add Device Details – WLC2-Anchor**

Add Device ×

---

Type \*  
Network Device ▼  
[Hint](#)

Device IP / DNS Name\*  
198.19.12.10

---

Credentials [Validate](#)

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\*  
CLI dnaadmin ▼

---

▼ SNMP\*

Select global credential  Add device specific credential

V2C ▼

Credential\*  
SNMPv2 Write | Write ▼

---

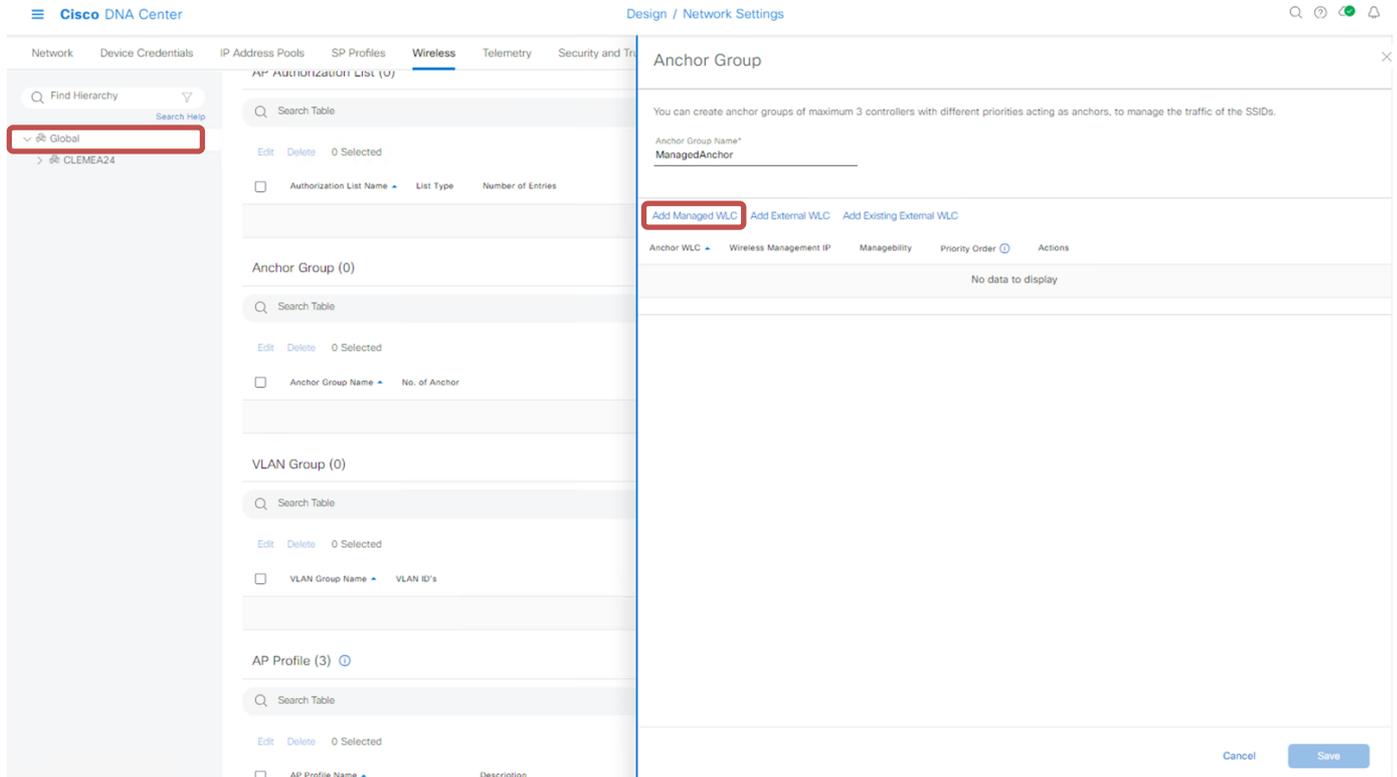
> SNMP Retries and Timeout\*

---

## Step 2: Configure Anchor Group

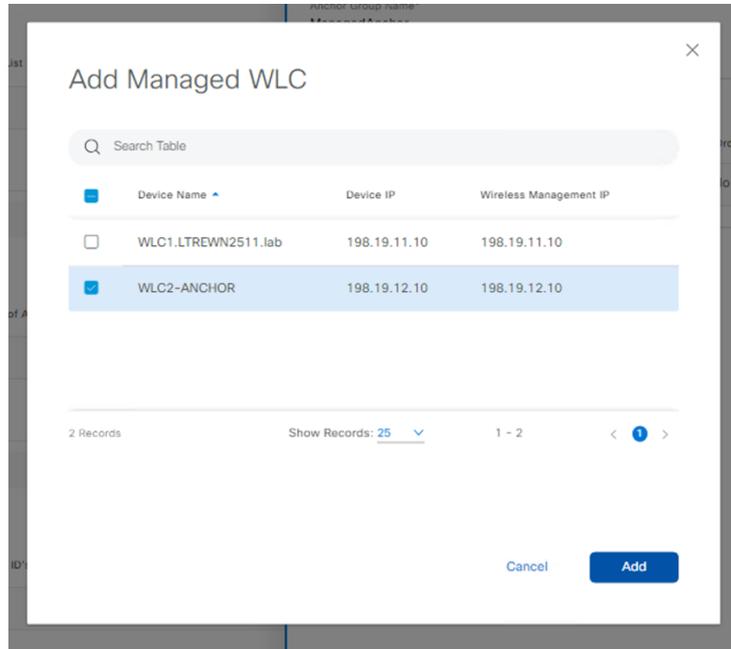
- Navigate to **Design > Network Settings**
- Click in the **Global** part of the Hierarchy.
- Under **Wireless > Anchor Group** click **Add**

**Figure 154 Anchor Group – Managed Anchor**

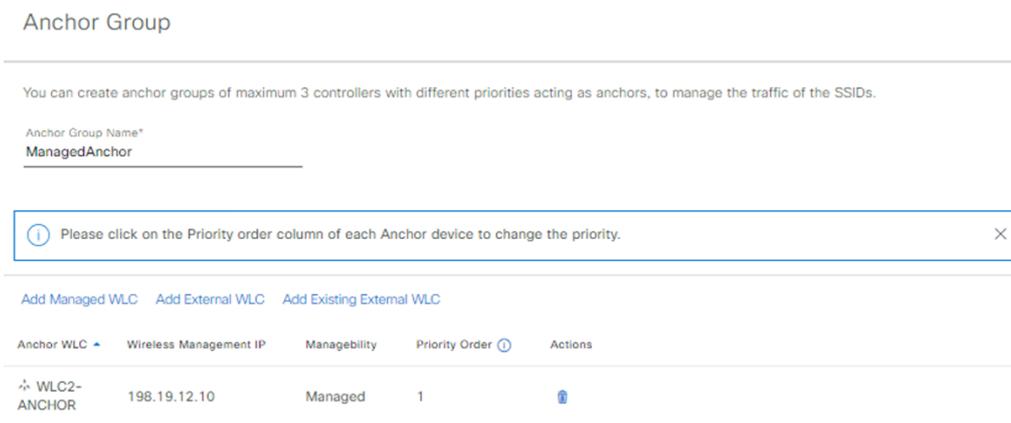


- Name the Anchor Group: **ManagedAnchor**
- Click **Add Managed WLC**
- Select **WLC2-ANCHOR** from the list and click **Add**
- Then **Save**

- **Figure 155 Anchor Group – Managed Anchor**



**Figure 156 Anchor Group – Managed Anchor**



### Step 3: Edit Network Profiles

Next step is to edit Network Profiles to reconfigure the GUEST SSID as Anchored

- Go to **Design > Network Profiles**, click on **WIRELESS\_HQ** to edit the profile.
- In the SSIDs tab, find the **XX\_CLEMEA24\_GUEST** SSID and edit it with the following parameters:

**Table 26 Network Profile – Settings – Anchored GUEST HQ**

Parameter	Value
Network Profile	WIRELESS_HQ
WLAN Profile Name:	XX_CLEMEA24_GUEST_Central
Fabric	No
Interface Name:	GUEST
<b>Anchor</b>	<b>Yes</b>
<b>Select Anchor Group</b>	<b>ManagedAnchor</b>

It should look like this:

**Figure 157 Network Profile WIRELESS\_HQ –Anchoring GUEST SSID**

Network Profiles / Wireless

## Edit Network Profile

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

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

Note: Changes in SSIDs, AP Zones, Model Config, Template sections require Controller provisioning. Changes in Custom Tags/Groups require Access Point provisioning.

Profile Name: **WIRELESS\_HQ**

Site: 3 sites

Profile Type: wlan

SSIDs | AP Zones | Model Configs | Templates | Advanced Settings

SSID  
01\_CLEMEA24\_GUEST

WLAN Profile Name  
01\_CLEMEA24\_GUEST\_Central

Policy Profile Name  
01\_CLEMEA24\_GUEST\_Central

Fabric  
 Yes  No

Enable SSID Scheduler

TRAFFIC SWITCHING  
 Interface  VLAN Group

Interface Name\*  
GUEST

Do you need Anchor for this SSID?  
 Yes  No

Select Anchor Group\*  
ManagedAnchor

- Save the configuration.
- Repeat the process for **WIRELESS\_RB** Network Profile
- **Table 27 Network Profile – Settings – Anchored GUEST RB**

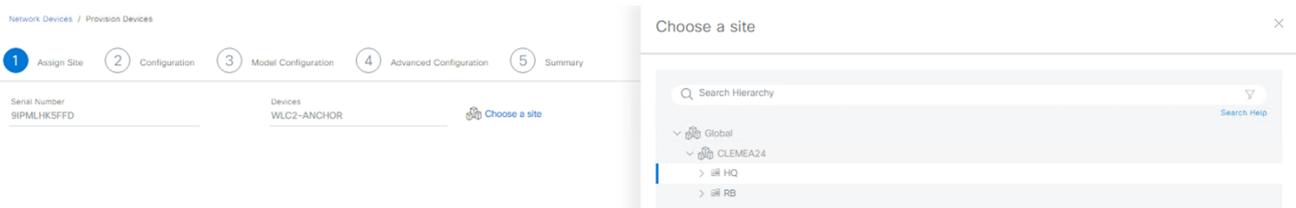
Parameter	Value
Associate SSID to Profile	WIRELESS_RB
WLAN Profile Name:	XX_CLEMEA24_GUEST_Central
Fabric	No
Interface Name:	GUEST
<b>Anchor</b>	<b>Yes</b>
<b>Select Anchor Group</b>	<b>ManagedAnchor</b>

## Step 4: Provision WLC2-ANCHOR

Next, Provision the WLC2-ANCHOR

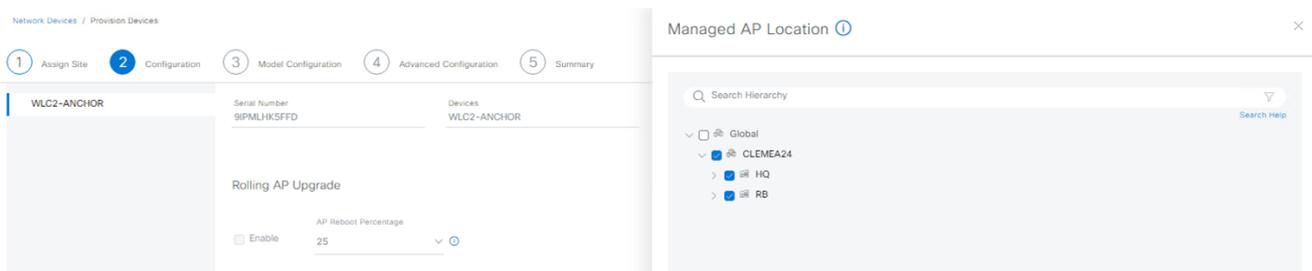
- Go to **Provision > Inventory**
  - Select the WLC and hover over “**Actions**” field and navigate to “**Provision**” and then to “**Provision Device**”
1. Select **HQ Site**, click **Next**

Figure 158 Provision WLC2-ANCHOR



2. In the second step,
  - o on **WLC Role** select **Anchor**
  - o select the **HQ** and **RB** Buildings:

Figure 159 Provision WLC2-ANCHOR



Only buildings can be associated in this step.

- o Reconfigure **VLAN ID to 234** (anchored VLAN in DMZ with subnet 10.0.234.0/24)

**Figure 160 Provision WLC2-ANCHOR**

Network Devices / Provision Devices

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

**WLC2-ANCHOR**

Serial Number: 9PMLHK5FFD | Devices: WLC2-ANCHOR | WLC Role:  Anchor | Managed AP location(s): Managing 5 Anchor location(s)

Assign Guest SSIDs to DMZ site

Interface Name	Interface Group Name	VLAN ID	IP Address	Gateway IP Address	LAG/Port Number	Subnet Mask(in bits)
GUEST	-	234	IP Address	Gateway IP Address	N/A	Subnet Mask

1 Records | Show Records: 25 | 1 - 1

Rolling AP Upgrade

Enable | AP Reboot Percentage: 25

- Skip past (hit next), “**Model Configuration**” and “**Advanced Configuration**” and head into “**Summary**”
- Click “**Deploy**”
- Click “**Apply**” Now



Provisioning WLC2-ANCHOR also triggers a Provisioning on WLC1 to automate the Anchoring of the desired SSID.

When finished, expect the normal Device Controllability configuration to be pushed to WLC2-ANCHOR such as: AAA ISE config, Method lists, SNMP traps, etc, and also the specific config for anchoring

**Pushed config to WLC2-ANCHOR:**

- Mobility
- WLAN Profile and Policy Profile (with Anchor config)
- Redirect ACL
- VLAN 234

**Pushed config to ISE:**

- Added WLC2-Anchor as Network Device

## Pushed config to WLC1:

- Mobility
- Modified Policy Profile of GUEST SSID with Anchor WLC IP

Feel free to verify this configuration on the different network devices.

## Step 5: Testing Anchored GUEST SSID

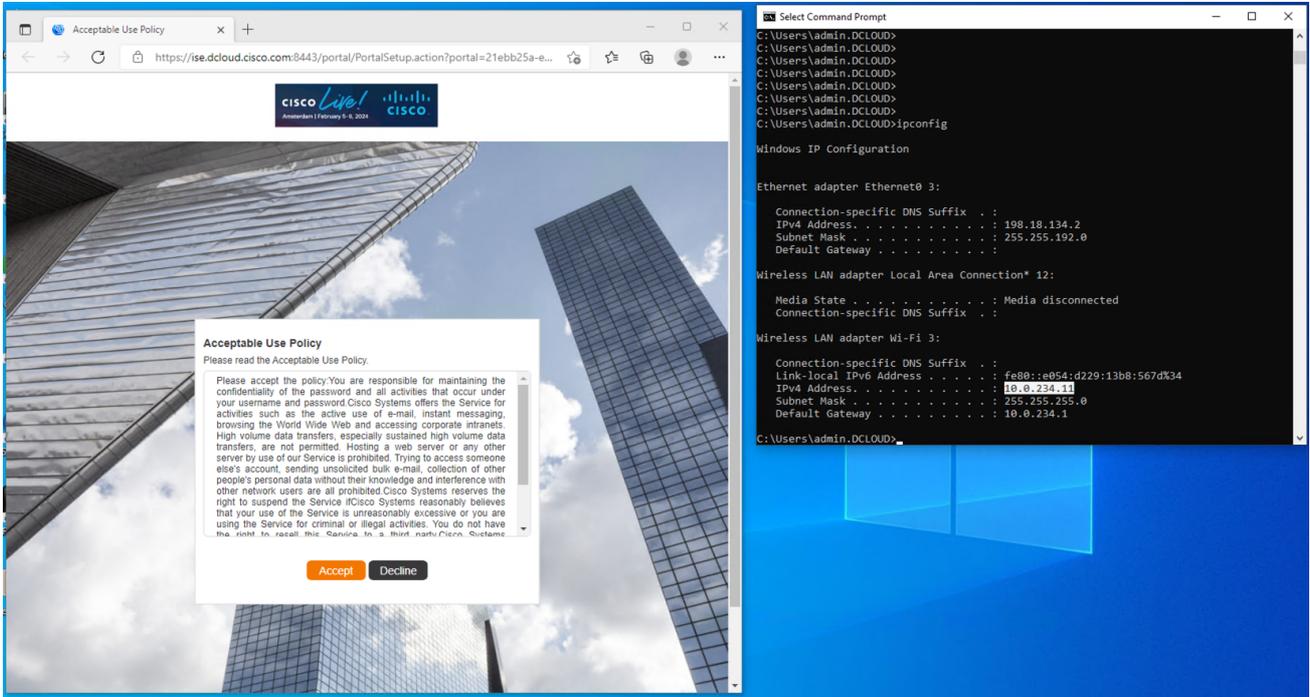
Open an RDP session to one of the Wireless Clients:

**Table 28 Wireless Clients Addressing and Credentials**

Name	IP Address	Username	Password	Preferred Access Method
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP
Client4	198.18.134.4	DCLOUD\admin	C1sco12345	RDP

- Make sure the SX Virtual Link has the **WUSB6300** connected.
- Connect to GUEST SSID
- Wait for a redirection

**Figure 161 Testing Anchored GUEST**



- Verify on both WLCs and ISE

**Figure 162 Verify Client Status on WLC2-ANCHOR**

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
c441.1e83.4520	10.0.234.11	fe80::e054:d229:13b8:567d	198.19.11.10	01_CLEMEA24_GUEST	17	WLAN	Run	N/A	C4-41-1E-83-45-20	Microsoft-Workstation	Export Anchor

1 - 1 of 1 clients

**Figure 163 Verify Client Status on WLC1**

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
c441.1e83.4520	10.0.234.11	fe80::e054:d229:13b8:567d	RB-GF-AP01	01_CLEMEA24_GUEST	19	WLAN	Run	11ac	C4-41-1E-83-45-20	Microsoft-Workstation	Export Foreign

1 - 1 of 1 clients

**Figure 164 Verify Client Status on ISE**

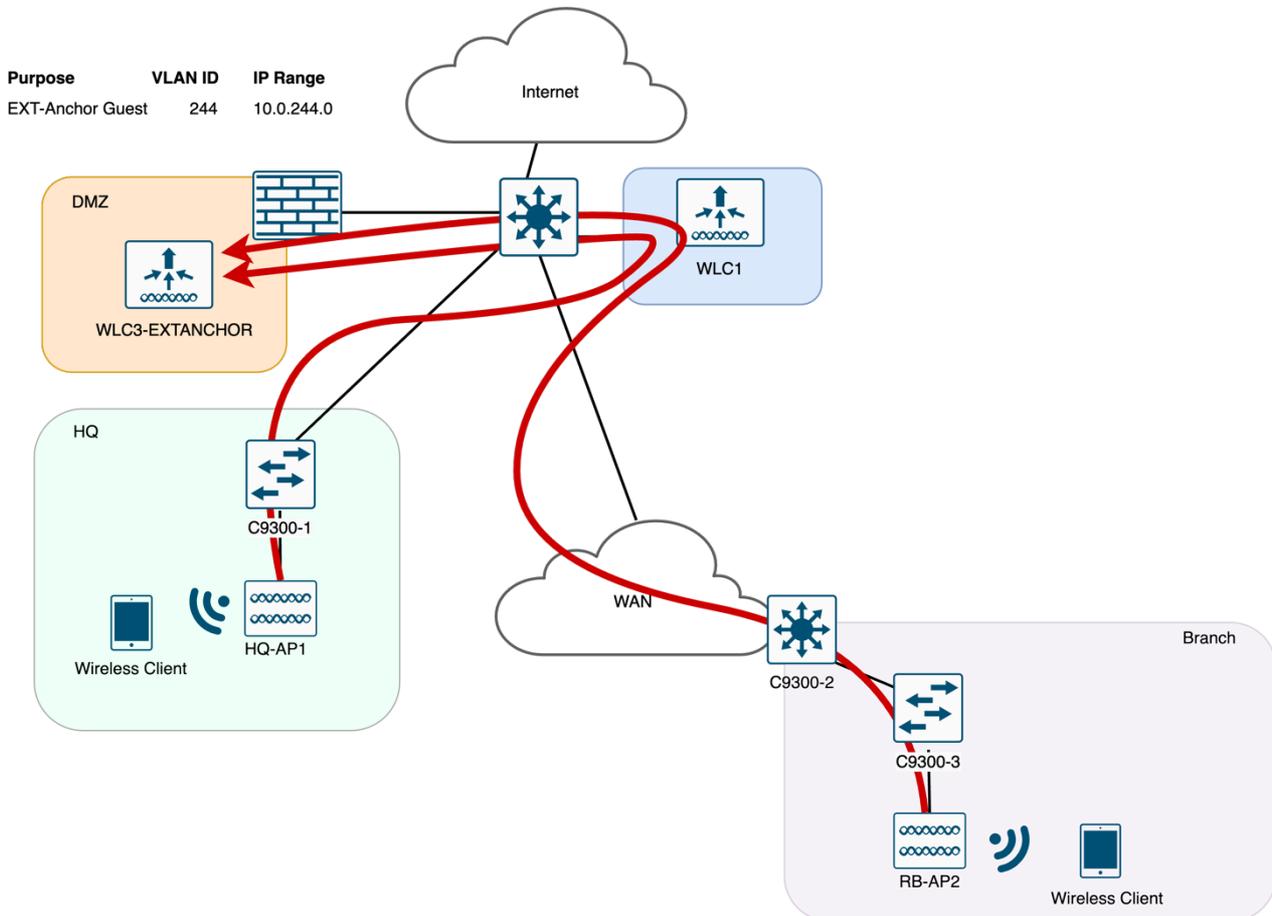
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port
Jan 04, 2024 04:50:02.6...	<span style="color: blue;">●</span>		9	C4:41:1E:83:45...	C4:41:1E:83:45:20	Windows1...	Default >>...	Default >>...	PermitAcc...	10.0.234.11.f...		
Jan 04, 2024 04:39:25.9...	<span style="color: green;">■</span>			C4:41:1E:83:45...	C4:41:1E:83:45:20	Windows	Default >> Hotspot_Ciscollive_GuestAccessPolicy				WLC1.LTREW...	

## Anchoring SSID to an External Anchor WLC

In this section participants will learn how to anchor the GUEST SSID to an External WLC located in a DMZ that is Not Managed by Catalyst Center.

Catalyst Center offers flexibility to use this configuration in scenarios where the Anchor WLC cannot be managed by Catalyst Center, reasons may be due to compatibility or WLC being managed by a 3<sup>rd</sup> party, etc.

**Figure 165 Topology – Anchoring GUEST with EXTERNAL WLC**



Similarly to the previous task, we start by adding the **WLC3-EXTANCHOR** to the Anchor Group Configuration.

### Step 1: Configure Anchor Group

- Navigate to **Design > Network Settings**
- Click in the **Global** part of the Hierarchy.
- Under **Wireless > Anchor Group** click **Add**
- Name the Anchor Group: **ExternalAnchor**

**Figure 166 Anchor Group – External Anchor**

### Anchor Group ✕

You can create anchor groups of maximum 3 controllers with different priorities acting as anchors, to manage the traffic of the SSIDs.

Anchor Group Name\*  
ExternalAnchor

---

[Add Managed WLC](#) [Add External WLC](#) [Add Existing External WLC](#)

Anchor WLC ▲	Wireless Management IP	Manageability	Priority Order ⓘ	Actions
No data to display				

## Step 2: Add External WLC

- Click **Add External WLC**

**Figure 167 Anchor Group – Add External Anchor**

### Add External WLC ✕

Device Name*	Device Series* ▼
Peer IP Address*	NAT IP Address
MAC Address*	Mobility Group Name*
Hash	
<small>For C9800-CL model only</small>	

Note: To ensure a successful mobility tunnel between Cisco DNA Center managed controller and the external controller, you will be required to make some manual configurations on the external controller. Instructions will be provided during the configuration of the Mobility Group of the managed WLC.

[Cancel](#) [Add](#)



This part of the lab assumes that the WLC3-EXTANCHOR is already configured with the GUEST settings matching the ones in WLC1 for all pods, hence only covers the Catalyst Center steps to automate the configuration to WLC1.

- In order to fill in the required information you must login to the WLC3-EXTANCHOR via SSH and collect the missing parameters:

Parameter	Value
Device Name	WLC3-EXTANCHOR
Device Series	Cisco Catalyst 9800 Series
Peer IP Address	198.19.13.10
NAT IP Address	198.19.13.10
<b>MAC Address</b>	<b>!! To be collected via CLI</b>
Mobility Group Name	default
<b>Hash</b>	<b>!! To be collected via CLI</b>

- To collect the MAC Address of EXTANCHOR, run the following command:

```
WLC3-EXTANCHOR#sh wireless mobility summary
!(Snip)
Mobility MAC Address: 001e.7abb.29ff
!
```



Enter the MAC Address in xx:xx:xx:xx:xx:xx format in Catalyst Center

- Take the Certificate Hash from the CLI with this command and paste it in Catalyst Center

```
WLC3-EXTANCHOR#sh wireless management trustpoint
Trustpoint Name : WLC3_WLC_TP
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 4664e770fc6f921d7124f05251a1345da5f2e5fb
Private key Info : Available
FIPS suitability : Not Applicable
```

When finished it should look like the figure below, then click **Add**

**Figure 168 Anchor Group – Add External Anchor**

### Add External WLC

Device Name  
**WLC3-EXTANCHOR**

Peer IP Address\*  
**198.19.13.10**

MAC Address\*  
**00:1e:7a:bb:29:ff**

Hash  
**4664e770fc6f921d7124f05251a1345d**  
For C9800-CL model only

Device Series\*  
**Cisco Catalyst 9800 Series**

NAT IP Address  
**198.19.13.10**

Mobility Group Name\*  
**default**

Note: To ensure a successful mobility tunnel between Cisco DNA Center managed controller and the external controller, you will be required to make some manual configurations on the external controller. Instructions will be provided during the configuration of the Mobility Group of the managed WLC.

Cancel Add

**Figure 169 Anchor Group – External Anchor Summary**

## Anchor Group

You can create anchor groups of maximum 3 controllers with different priorities acting as anchors, to manage the traffic of the SSIDs.

Anchor Group Name  
**ExternalAnchor**

Please click on the Priority order column of each Anchor device to change the priority.

[Add Managed WLC](#)   [Add External WLC](#)   [Add Existing External WLC](#)

Anchor WLC	Wireless Management IP	Manageability	Priority Order	Actions
<b>WLC3-EXTANCHOR</b>	198.19.13.10	External	1	

### Step 3: Edit Network Profiles

Next step is to edit Network Profiles to reconfigure the GUEST SSID as Anchored

- Go to **Design > Network Profiles**, click on **WIRELESS\_HQ** to edit the profile.
- In the SSIDs tab, find the **XX\_CLEMEA24\_GUEST** SSID and edit it with the following parameters:

**Table 29 Network Profile – Settings – Anchored GUEST HQ**

Parameter	Value
Network Profile	WIRELESS_HQ
WLAN Profile Name:	XX_CLEMEA24_GUEST_Central
Fabric	No
Interface Name:	GUEST
<b>Anchor</b>	<b>Yes</b>
<b>Select Anchor Group</b>	<b>ExternalAnchor</b>

It should look like this:

**Figure 170 Network Profile WIRELESS\_HQ –Anchoring GUEST SSID**

Network Profiles / Wireless

### Edit Network Profile

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

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

Note: Changes in SSIDs, AP Zones, Model Config, Template sections require Controller provisioning. Changes in Custom Tags/Groups require Access Point provisioning.

Profile Name: **WIRELESS\_HQ**

Site: **3 sites**

Profile Type: **wlan**

SSIDs | AP Zones | Model Configs | Templates | Advanced Settings

SSID  
01\_CLEMEA24\_GUEST

WLAN Profile Name  
01\_CLEMEA24\_GUEST\_Central

Policy Profile Name  
01\_CLEMEA24\_GUEST\_Central

Fabric  
 Yes  No

Enable SSID Scheduler

TRAFFIC SWITCHING  
 Interface  VLAN Group

Interface Name\*  
GUEST

Do you need Anchor for this SSID?  
 Yes  No

Select Anchor Group\*  
ExternalAnchor

- Save the configuration.
- Repeat the process for **WIRELESS\_RB** Network Profile
- **Table 30 Network Profile – Settings – Anchored GUEST RB**

Parameter	Value
Network Profile	WIRELESS_RB
WLAN Profile Name:	XX_CLEMEA24_GUEST_Central
Fabric	No
Interface Name:	GUEST
<b>Anchor</b>	<b>Yes</b>
<b>Select Anchor Group</b>	<b>ExternalAnchor</b>

#### Step 4: Provision WLC1

Next step is to Provision WLC1

- Go to **Provision > Inventory**

- Select the WLC and hover over “**Actions**” field and navigate to “**Provision**” and then to “**Provision Device**”
- Skip past (hit next) “**Configuration**”, “**Model Configuration**” and “**Advanced Configuration**” and head into “**Summary**”
- Click “**Deploy**”
- Click “**Apply**” Now

After provisioning the WLC1 expect to see the following pushed configuration:

- Mobility to WLC3-EXTANCHOR
- Reconfigured the GUEST Policy Profile with the Anchor Configuration pointing to WLC3-ANCHOR IP address.

Feel free to verify this configuration on the WLC.

## Step 5: Adding Mobility Configurations to WLC3-EXTANCHOR

Before we proceed to test the SSID, we still need to configure one more thing.

As Catalyst Center automated the Mobility configuration to WLC1, the config on the Anchor side is missing and must be configured manually.

- Navigate to **mRemoteNG** on your Jumphost and open a session to the WLC1 using, run the following commands and get the MAC Address and Hash:

```
WLC1#sh wireless mobility summary
!(Snip)
Mobility MAC Address: 001e.bd4e.d8ff          !! This is an Example
!
!
!
WLC1#sh wireless management trustpoint
Trustpoint Name : WLC3_WLC_TP
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : c2e32379055271f998728317ce91d8476e5ffe16    !! This is an Example
Private key Info : Available
```

FIPS suitability : Not Applicable

- Then, SSH to the WLC3-EXTANCHOR via mRemoteNG and in configuration mode, paste the following command:



Replace the MAC Address and Certificate Hash with the ones collected from WLC1

```
wireless mobility group member mac-address [WLC1-MAC ADDRESS] ip 198.19.11.10 public-ip 198.19.11.10 group default ssc-hash [WLC1-CERTIFICATE HASH]
```

Example:

```
WLC3-EXTANCHOR#config terminal
WLC3-EXTANCHOR(config)#
WLC3-EXTANCHOR(config)#wireless mobility group member mac-address 001e.bd4e.d8ff
ip 198.19.11.10 public-ip 198.19.11.10 group default ssc-hash
c2e32379055271f998728317ce91d8476e5ffe16
```

- Verify mobility tunnel with the command:

```
WLC3-EXTANCHOR#sh wireless mobility summary
```



Mobility Status should UP be before proceeding to test, it may take 2-3 mins,

## Step 6: Testing Anchored GUEST SSID

Open an RDP session to one of the Wireless Clients:

**Table 31 Wireless Clients Addressing and Credentials**

Name	IP Address	Username	Password	Preferred Access Method
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP

Client4	198.18.134.4	DCLLOUD\admin	C1sco12345	RDP
---------	--------------	---------------	------------	-----

- Make sure the SX Virtual Link has the **WUSB6300** connected.
- Connect to GUEST SSID
- Wait for a redirection.

The wireless client should take an IP address of the 10.0.244.0/24 range.

**Figure 171 Testing Anchored GUEST**

The figure consists of two side-by-side screenshots. The left screenshot shows a web browser window with an 'Acceptable Use Policy' dialog box overlaid on a background image of modern skyscrapers. The dialog box contains text about policy acceptance and 'Accept' and 'Decline' buttons. The right screenshot shows a terminal window with the following output:

```

Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix . . . : 
Link-local IPv6 Address . . . . . : fe80::1030:672d:7b9e:3048%31
IPv4 Address. . . . . : 10.0.244.11
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.244.1

C:\Users\admin.DCLOUD>ping 10.0.244.1

Pinging 10.0.244.1 with 32 bytes of data:
Reply from 10.0.244.1: bytes=32 time=4ms TTL=255
Reply from 10.0.244.1: bytes=32 time=4ms TTL=255
Reply from 10.0.244.1: bytes=32 time=4ms TTL=255

Ping statistics for 10.0.244.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms
Control-C
^C
C:\Users\admin.DCLOUD>
  
```

**Figure 172 Verify Client Status on WLC3-EXTANCHOR**

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
<input type="checkbox"/>	c441.1e83.4520	10.0.244.11	fe80::1030:672d:7b9e:3048	198.19.11.10	01_CLEMEA24_GUEST	17	WLAN	Run	N/A	C4-41-1E-83-45-20	Microsoft-Workstation	Export Anchor

1 - 1 of 1 clients

**Figure 173 Verify Client Status on WLC1**

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role
<input type="checkbox"/>	c441.1e83.4520	10.0.244.11	fe80::1030:672d:7b9e:3048	RB-GF-AP01	01_CLEMEA24_GUEST	19	WLAN	Run	11ac	C4-41-1E-83-45-20	Microsoft-Workstation	Export Foreign

1 - 1 of 1 clients

**Figure 174 Verify Client Status on ISE**

Jan 04, 2024 06:08:33.3...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	C4:41:1E:83:45...	C4:41:1E:83:45:20	Windows1...	Default >>...	Default >>...	PermitAcc...	10.0.244.11,f...
Jan 04, 2024 06:08:30.3...	<input checked="" type="checkbox"/>	<input type="checkbox"/>		C4:41:1E:83:45...	C4:41:1E:83:45:20	Windows1...	Default >>...	Default >>...	PermitAcc...	WLC1.LTREW...
Jan 04, 2024 06:06:55.6...	<input checked="" type="checkbox"/>	<input type="checkbox"/>		C4:41:1E:83:45...	C4:41:1E:83:45:20	Windows	Default >> Hotspot_Ciscolive_GuestAccessPolicy			WLC1.LTREW...

## Task 12: Bonus Tasks – Configuring HA-SSO

Cisco Wireless Controller High Availability (HA) can be configured through Cisco DNA Center. Currently, both the formation and breaking of wireless controller HA is supported.



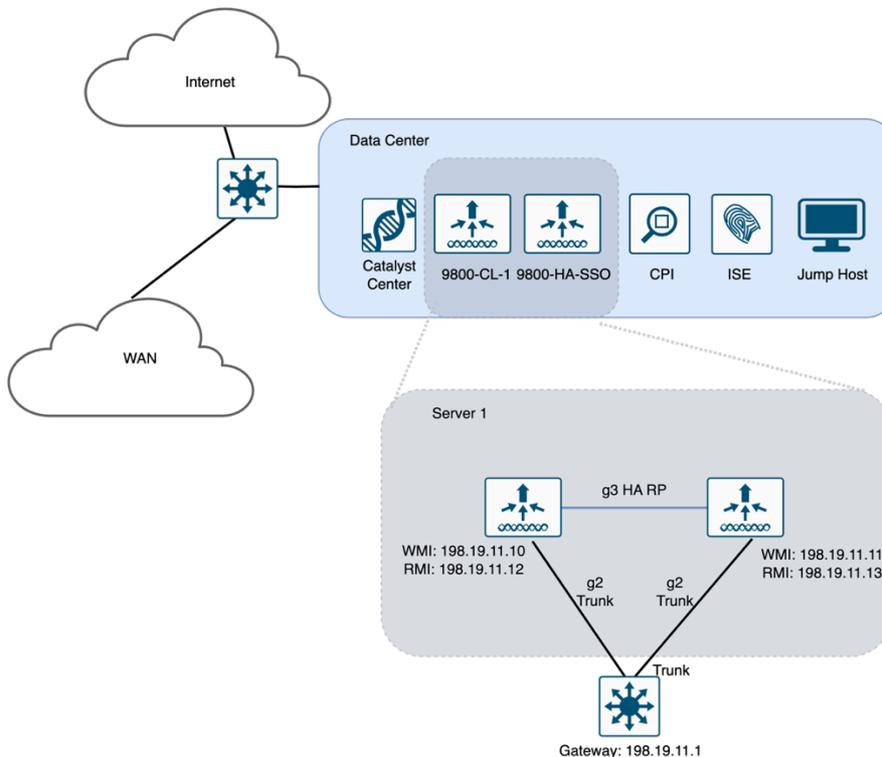
Switchover options are not supported.



Please bear in mind that the recovery of WLC1 or WLC2 may not be possible or be very slow if this task is not executed properly, we recommend leaving this task to the end.

As this lab is hosted on a virtual environment, we aim to pair the WLC1 and WLC2 **referred to as WLC-HASSO** using the Gig3 interface both hosted in the same server.

**Figure 175 WLC HA SSO Virtual Setup**



The pre-requisites for Configuring Cisco 9800 Wireless Controller High Availability via Catalyst Center are:

1. WLC1 and WLC2 must be Discovered and in the Managed state.
2. WLC1 and WLC2 must be deployed with the same hardware specs (CPU, MEM, Disk) and booted in INSTALL mode.
3. The service ports and the management ports of wireless controller 1 and wireless controller 2 must be configured.
4. The redundancy ports of WLC1 and WLC2 must be physically connected.
5. The management address of WLC1 and WLC2 must be in the same subnet.
6. The redundancy management address of WLC1 and WLC2 must also be in the same subnet.
7. Boot variables must be manually configured on the wireless controller as follows:

```
config t
boot system bootflash:packages.conf
config-register 0x2102
```

```
#show boot

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

In this section of the lab, we have pre-configured all the prerequisites except number 1, so let us begin:

## Step 1: Add WLC-HASSO to Inventory

The first thing is to Discover the WLC-HASSO

Navigate to the Dashboard top menu and click on **Provision > Inventory**

On the Inventory page, click **"Add Device"**

- WLC IP address is **198.19.11.11**
- Select the **"Write" Global credentials** for CLI, SNMP
- Make sure to use NETCONF port **830**

**Figure 176 Add Device – WLC-HASSO**

Provision / Inventory

Devices (2) Focus: Provision

Device Name	IP Address	Device Family
RB-GF-AP01	10.0.101.12	Unified AP
WLC1.LTREW2511.lab	198.19.11.10	Wireless Contr

**Add Device**

Type \*  
Network Device

Device IP / DNS Name\*  
198.19.11.11

Credentials [Validate](#)

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\*  
CLI dnaadmin

SNMP\*

Select global credential  Add device specific credential

V2C  
SNMPv2 Write | Write

SNMP Retries and Timeout\*

HTTP(S)

Select global credential  Add device specific credential

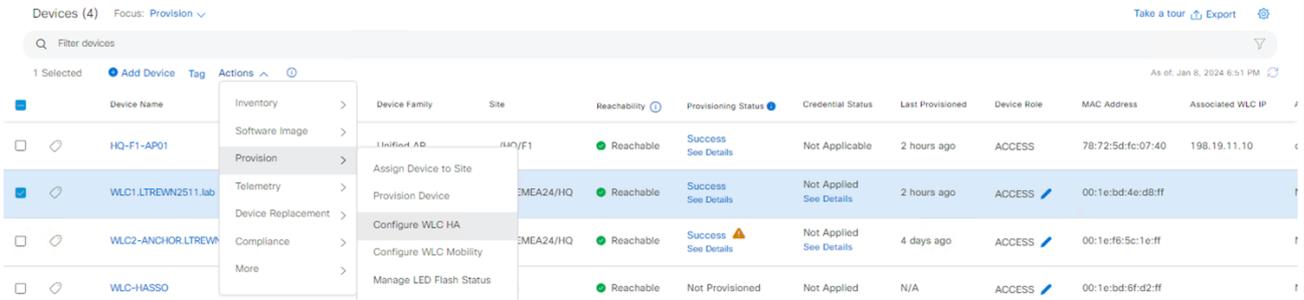
Device Controllability is Enabled. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. [Learn More](#)

Cancel **Add**

## Step 2: Configure WLC-HASSO

- From the **Actions** drop-down list, choose **Provision > Configure WLC HA**.
- The High Availability slide-in pane is displayed.

**Figure 177 Provision – Configure WLC HA**



- From the Select Secondary WLC drop-down list, choose the secondary controller **WLC-HASSO**.

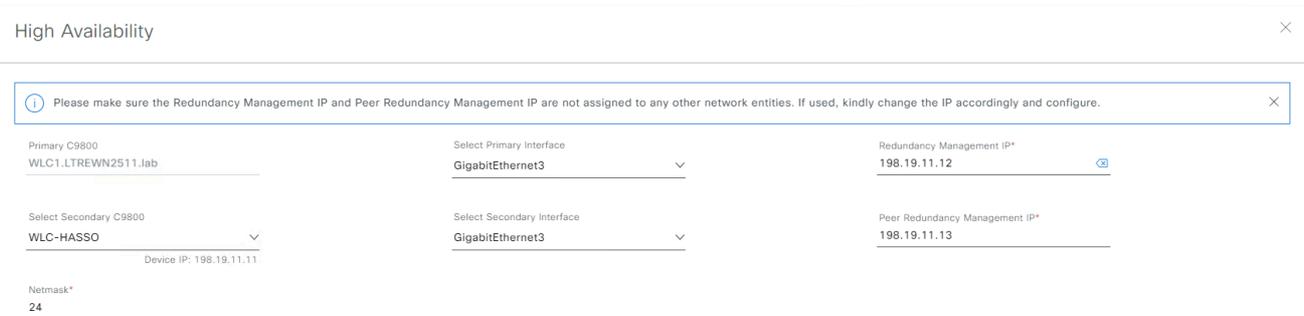


When you choose the secondary controller, based on the wireless management interface IP subnet of the primary controller, the redundancy management IP is auto populated.



Make sure the Interfaces are mapped to the **Gigabit Ethernet 3**

**Figure 178 Provision – WLC-HASSO**



- Populate the IP addresses with the following parameters:

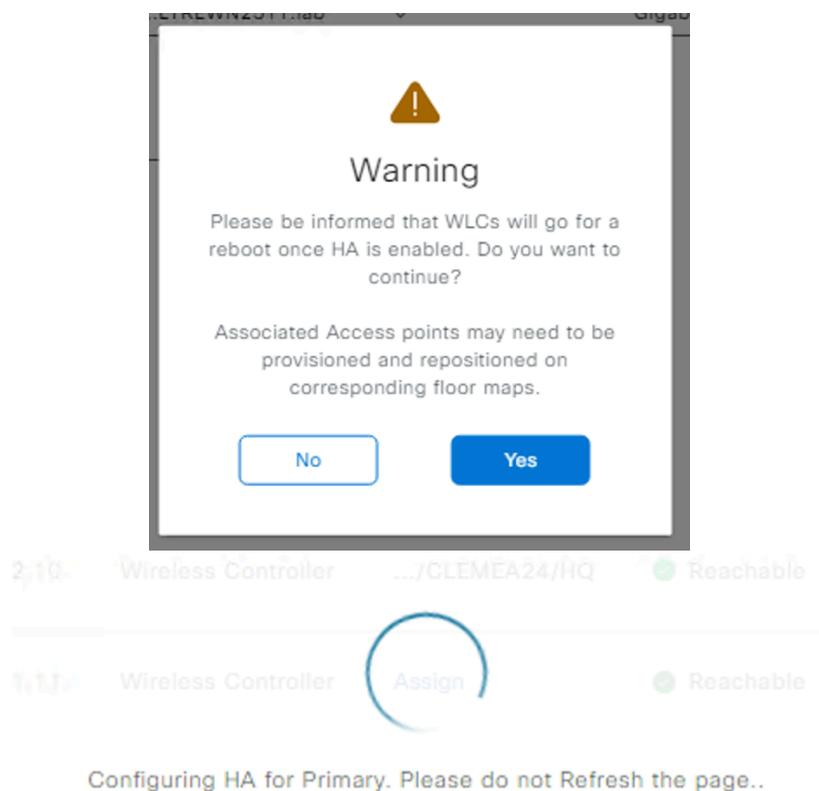
**Table 32 Provision – Configure WLC HA**

C9800	Interface	Redundancy Management Interface
<b>WLC1-LTREW2511.lab</b>	GigabitEthernet3	198.19.11.12
<b>WLC-HASSO</b>	GigabitEthernet3	198.19.11.13

When finished the configuration should look like this:

- Click **Configure HA**
- In the warning, Click **Yes** to confirm.

**Figure 179 Provision – WLC-HASSO**



The HA configuration is initiated in the background using the CLI commands, here is an overview of the process:

1. First, the primary wireless controller is configured.
2. On success, the secondary wireless controller is configured.
3. After the configuration is complete, both wireless controllers reboot.



This process may take up to 3 minutes to complete.

### Step 3: Verify WLC-HASSO Status

- To verify the HA configuration, on the **Devices > Inventory** window,
- Click on **WLC1 > View Device Details**
- Click the **Wireless Info** tab.
- The Redundancy Summary displays the **Sync Status as In Progress**.
- When Cisco DNA Center finds that HA pairing succeeded, the **Sync Status changes to Complete**.

**Figure 180 Provision – WLC-HASSO - Success**

All Devices / WLC1.LTREW2511.lab

WLC1.LTREW2511.lab [Run Commands](#) [Learn WLC Config](#) [View 360](#)

Reachable | Managed | IP Address: 198.19.11.10 | Device Model: Cisco Catalyst 9800-CL Wireless Controller for Cloud | Device Role: ACCESS | Uptime: 4 mins | Site: Global/CLEMEA24/HQ

**DETAILS**

- Interfaces >
- Hardware & Software
- User Defined Fields
- Config Drift
- REP Rings
- Wireless Info**
- Mobility

**SECURITY**

- Advisories

**COMPLIANCE**

- Summary

**MANAGED SITES**

Primary Managed Locations **2 Sites Managed** Secondary Managed Locations None

Wireless Summary	Redundancy Summary	Health Parameters	Additional Details
Primary WLC:	WLC1.LTREW2511.lab		
Secondary WLC:	WLC-HASSO		
Unit MAC:	00:0c:29:f1:a8:62		
Redundancy State:	SSO		
Mobility MAC:	00:1e:bd:4e:d8:ff		
Sync Status:	Complete		
Active RMI IP:	198.19.11.12		
Standby RMI IP:	198.19.11.13		
Gateway Monitoring:	Enabled		
Recovery mode:	Not Applicable		

## Task 13: Bonus Tasks – AP Power Save (Read Only)

As part of the sustainability efforts, this lab includes this section to focus on Power Profiles to the APs to define how they should operate in case of insufficient power provided or to define operation principles outside of business hours.

This is a read only section as we reference to existing documentation.

### Feature Support

- AP Power Save feature is supported as a standalone feature in IOSXE 9800 code since 17.8.x
- This feature is available and supported with Catalyst Center from 2.3.7 and C9800 version 17.10.x
- This functionality can be leveraged only with the following Access Points models:
  - o Cisco Catalyst 9115 Series Access Points
  - o Cisco Catalyst 9117 Series Access Points
  - o Cisco Catalyst 9120 Series Access Points
  - o Cisco Catalyst 9130 Series Access Points
  - o Cisco Catalyst 9136 Series Access Points

### Catalyst 9800 Configuration Guide:

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b\\_wl\\_17\\_8\\_cg/m\\_access\\_point\\_power\\_control.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b_wl_17_8_cg/m_access_point_power_control.html)

### Catalyst Center 2.3.7 Management Guide:

[https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/user\\_guide/b\\_cisco\\_dna\\_center\\_ug\\_2\\_3\\_7/m\\_configure-network-settings.html#create-an-ap-power-profile](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-7/user_guide/b_cisco_dna_center_ug_2_3_7/m_configure-network-settings.html#create-an-ap-power-profile)

## FAQ

This section explains the impact on the network depending on the configuration change upon provisioning. In other words, it answers the questions that frequently comes up before provisioning.

*¿What is the impact on Wireless clients, APs and WLC?*

*¿Shall I provision WLC or both AP and WLC?*

The following scenarios explain the impact on an existing wireless environment, assuming that the WLC and APs have been provisioned, and you want to make a new change:

### Scenario 1. Change something in one of the existing SSID.

Let's suppose you want to change the PSK, for this you need to change the config in CATALYST CENTER Network Settings, then provision the WLC so the change is reflected in the WLC.

This impacts all current clients on the SSID on all the sites that you have mapped this SSID to via Network Profiles.

### Scenario 2. Add a new SSID to APs

In CATALYST CENTER, you need to create a new SSID, add it in the Network Profile corresponding to the site, then provision WLC, should not need to provision APs.

Catalyst Center should reuse the same Policy Tag and simply adds this new SSID to the same Policy Tag hence AP should not bounce CAPWAP tunnel.

This should not impact wireless clients on other SSIDs.

### Scenario 3. Changing the AP Location to a new site

This scenario refers to moving AP in the hierarchy in Catalyst Center to another building, e.g from Bldg1 to Bldg2 where a different Network Profile is configured.

For this you need to provision the AP in the new building. Should not need to provision WLC.

This will have an impact on wireless clients associated to all the SSIDs on that AP, because Catalyst Center will change the site tag, and this bounces CAPWAP tunnel.

#### Scenario 4. Changing something in an existing RF Profile (RF Tag in the AP)

If you change something on the existing RF Config in Catalyst Center and then you should just provision WLC, no need to reprovision AP as RF Config (RF Tag in the AP) is the same.

Be careful as new configuration will be updated on ALL the APs with this RF Tag associated.

APs should not reset CAPWAP as is the same RF Tag, but depending on the change it may impact wireless clients regardless of the SSID.

E.g, removing channel 36 from 5GHz profile will have an impact on all APs with this channel as they need to choose a new one (assuming they are dynamically assigned via DCA), hence there is a radio reset thus impacting all wireless clients

#### Scenario 5. Changing RF profile to a new one

Create new RF profile in Catalyst Center, Provision WLC, here you should not have any impact, then provision AP or APs.

This impacts all wireless clients on the selected APs as the AP will reset CAPWAP for the new RF Tag.

#### Scenario 6. Reprovision of the AP without changes in the configuration (same tags)

This should not have any impact on the wireless clients

#### Scenario 7. Change in the FlexConnect Profile

Let's suppose you want to add/remove one additional VLAN to the Flex Profile so it can be used by AAA override.

Add the config in Catalyst Center Wireless Setting on the Flex Site you desire the config to be added, then provision the WLC, no need to provision the APs as they already have the corresponding Site Tag (with the Flex Profile linked to it)

Provisioning the WLC should not have any impact on the wireless clients.

## Related Sessions at CiscoLive

You can search CiscoLive Amsterdam content catalog with specific keyword and recommend sessions that are relevant to your lab.

[Content Catalog Link](#)

Session ID	TITLE	SPEAKERS	SESSION TYPE
<b>BRKEWN-2029</b>	Cisco DNA Center AIOps for Catalyst Wi-Fi 6/6E	Karthik Iyer	Breakout
<b>BRKEWN-2043</b>	Saving Energy and Money with Your Cisco Wireless Network	Simone Arena	Breakout
<b>BRKEWN-2339</b>	Catalyst 9800 Configuration Best Practices	Justin Loo	Breakout
<b>BRKEWN-2667</b>	Catalyst Wireless Supercharged by Cisco DNA Center: The Ultimate Guide to Bring Your Wireless Operation to the Next Level	Ignacio Lopez	Breakout
<b>BRKEWN-2926</b>	Tune your Cisco Wi-Fi designs for the most demanding clients and applications, boosted with applied AI	Jerome Henry	Breakout
<b>BRKEWN-3004</b>	Understanding Wireless Security and the Implications for Secure Wireless Network Design	Mark Krischer	Breakout
<b>BRKEWN-3413</b>	Advanced RF Tuning for Wi-Fi6E with Catalyst Wireless: Become an Expert, while getting a little help from AI	Jim Florwick	Breakout
<b>BRKEWN-3628</b>	Troubleshoot Catalyst 9800 Wireless Controllers	Nicolas Darchis	Breakout
<b>LABEWN-2738</b>	Securing Catalyst 9800 WLC Using Cisco ISE and TACACS+	Guilian Deflandre and Rasheed Hamdan	Walk-in Lab
<b>LABEWN-1330</b>	Powerful APs and Sustainability, how to?	Rasheed Hamdan	Walk-in Lab