cisco Live!
Amsterdam | February 5-9, 2024

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

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

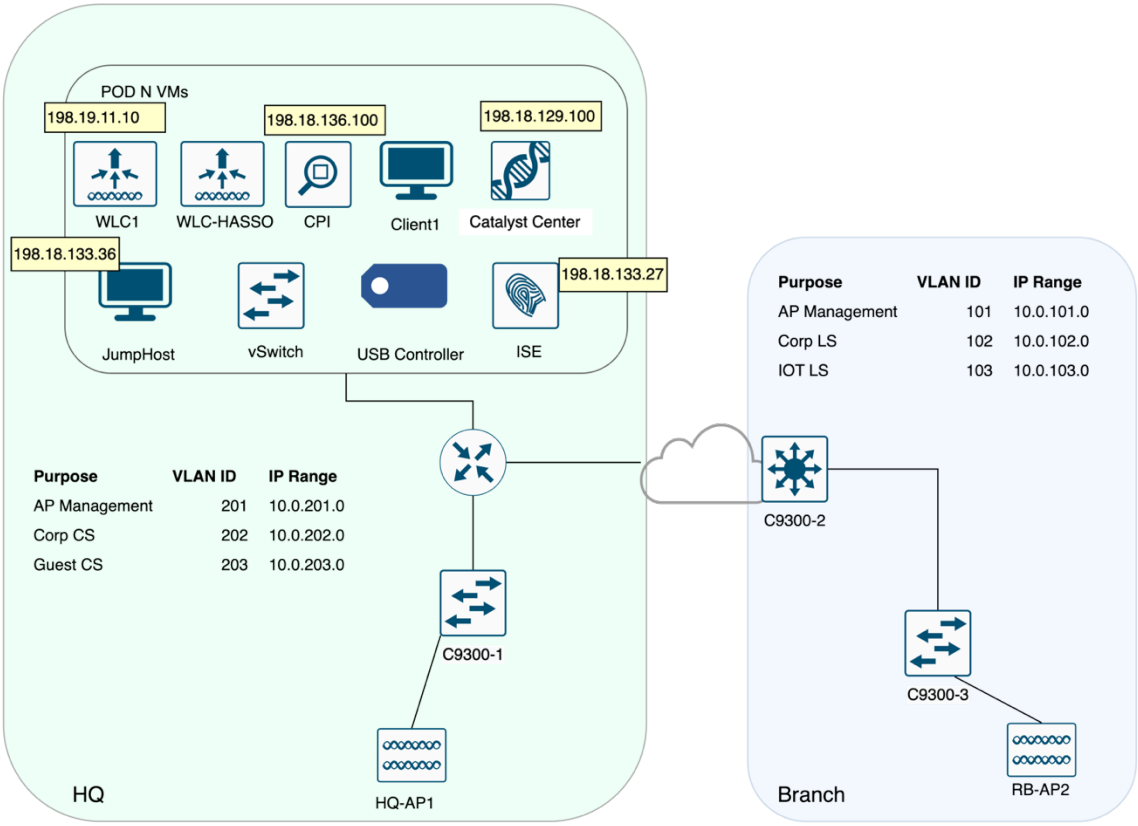
All of these in order to streamline advanced configurations. This approach facilitates the deployment process, ensuring consistency and adherence to best practices across the network.

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

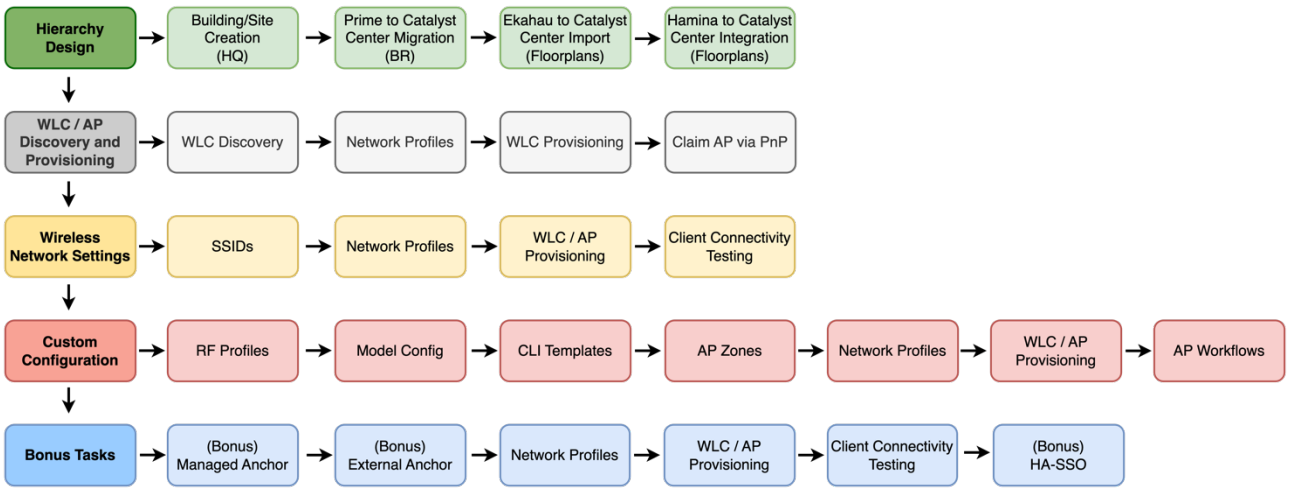
Table 1 Devices and Virtual Machines Addressing and Credentials

Name	IP Address	Username	Password	Preferred Access Method
Jump Host	198.18.133.36	DCLOUD\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 stablished 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

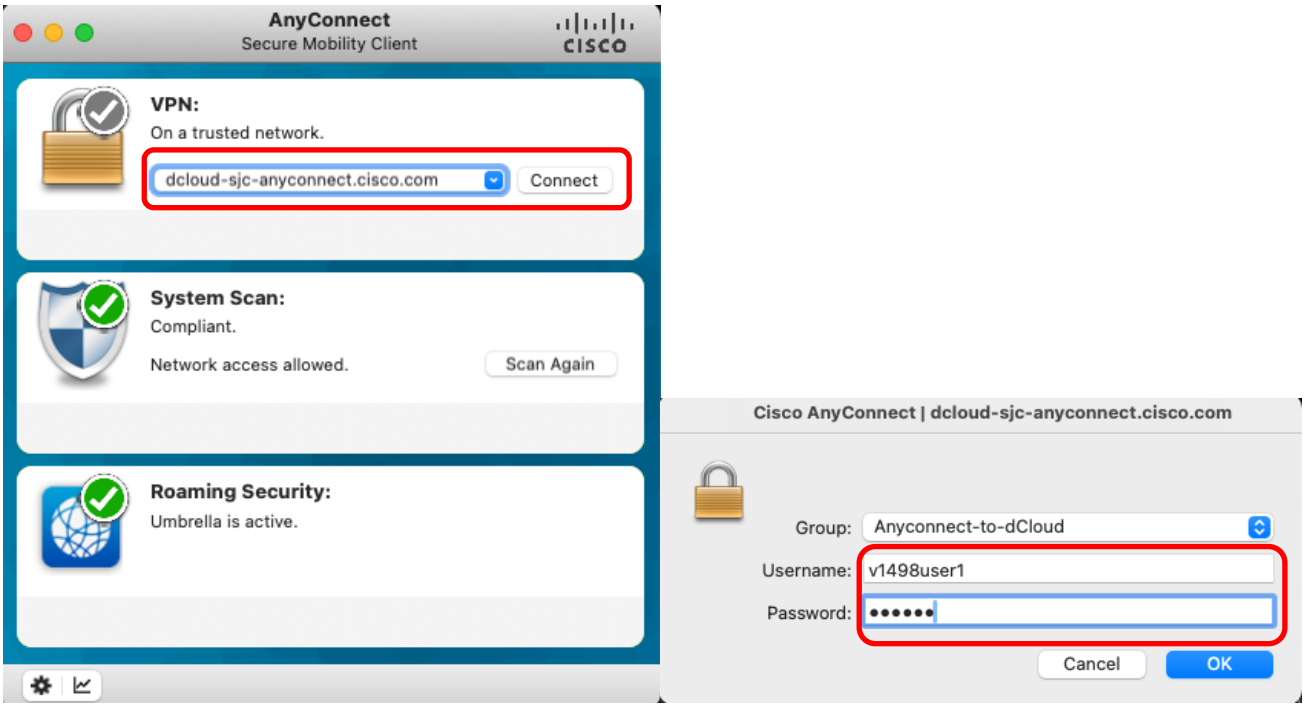
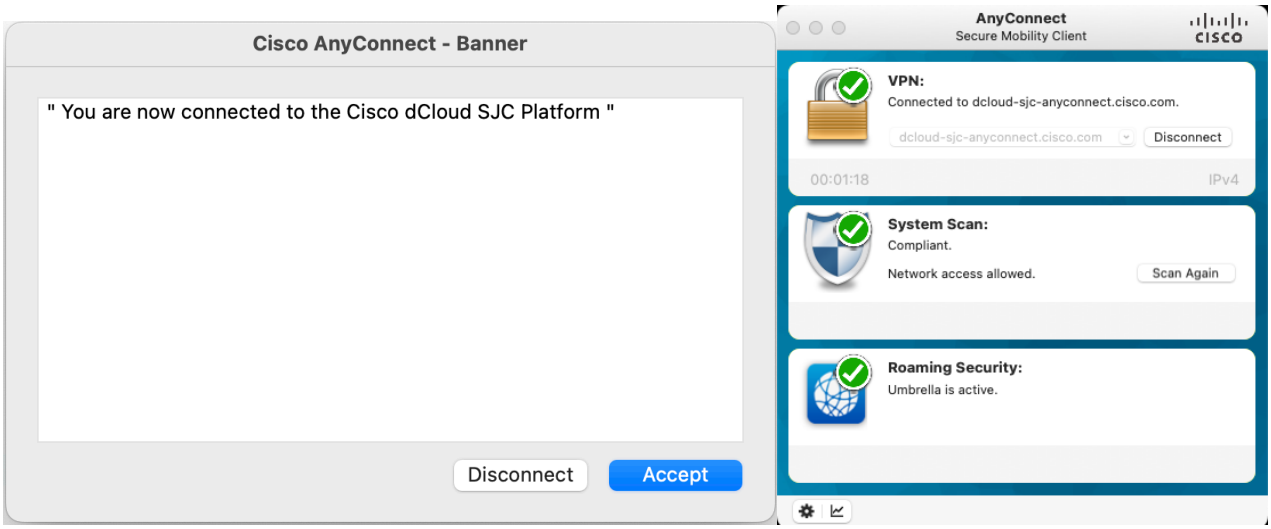


Figure 4 VPN Connectivity Successful



Step 3: Working from Jump Host

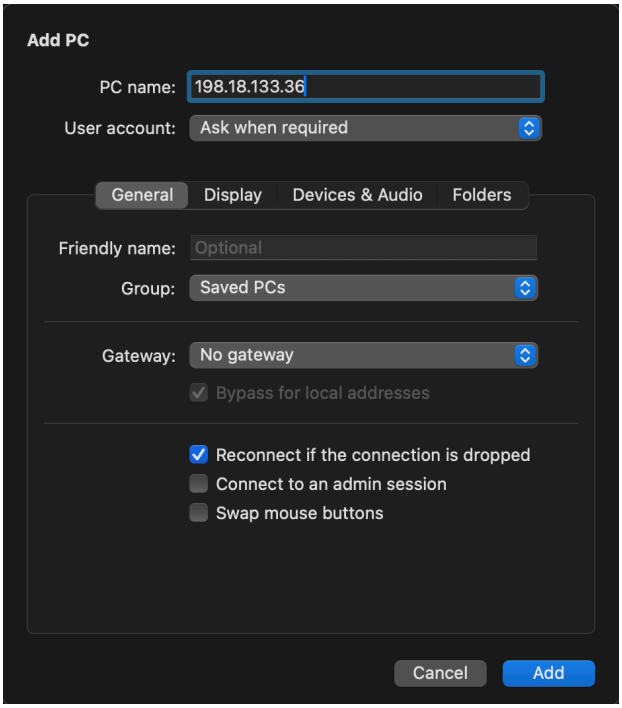
Open your RDP Client and use the JumpHost information to login:

IP Address: 198.18.133.36

username: DCLOUD\admin

password: C1sco12345

Figure 5 Working from Jump host



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

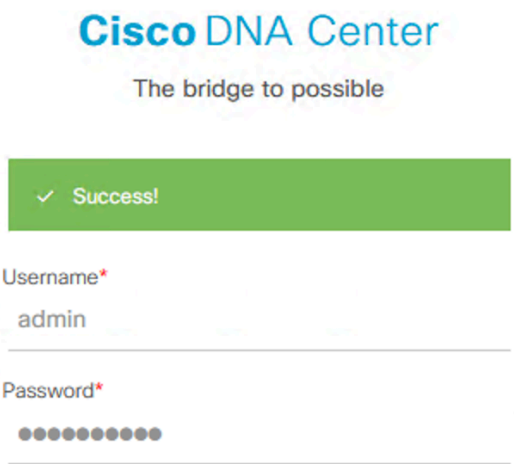
Step 1: Defining Site Hierarchy Elements

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/

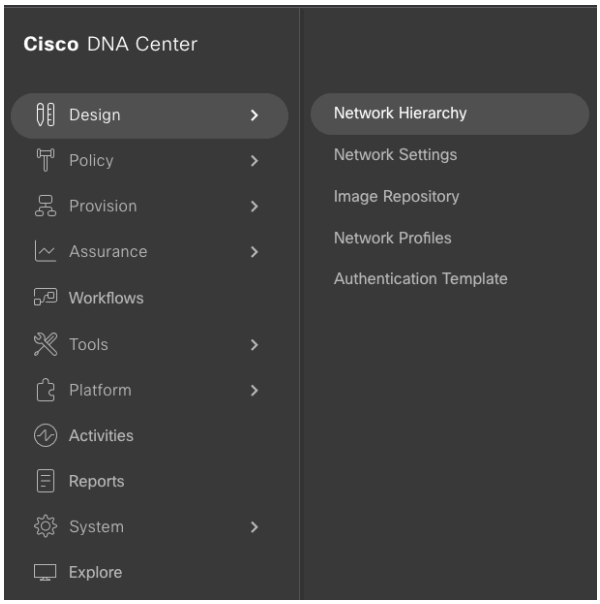
Credentials: admin / C1sco12345

Figure 6 Logging in to Catalyst Center



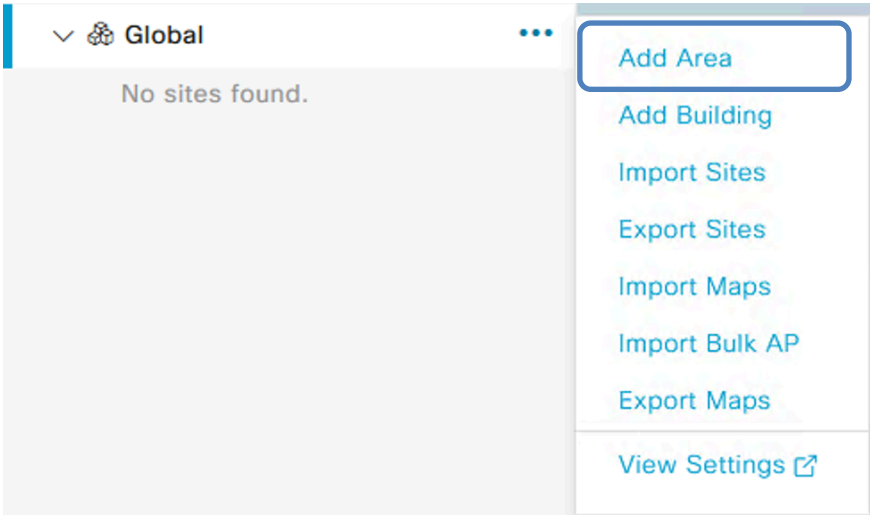
Next, navigate to **Design > Network Hierarchy**

Figure 7 Network Hierarchy



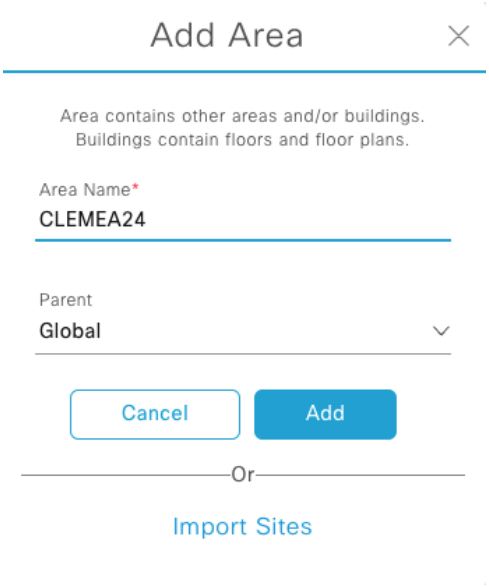
Hover over the three dots in front of **Global**

Figure 8 Site Hierarchy - Area



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

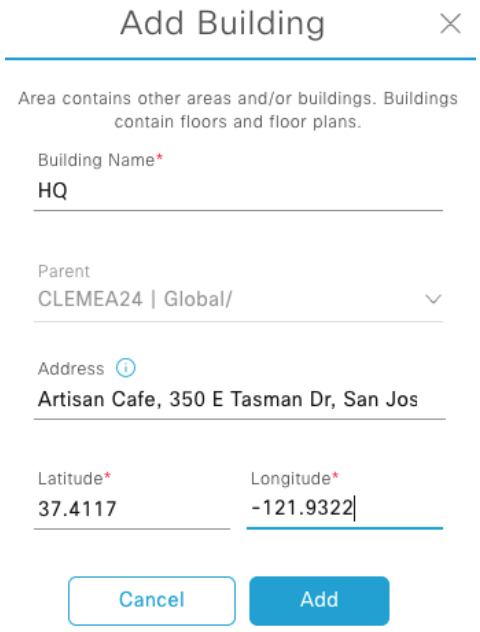
Figure 9 Site Hierarchy - Area



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

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

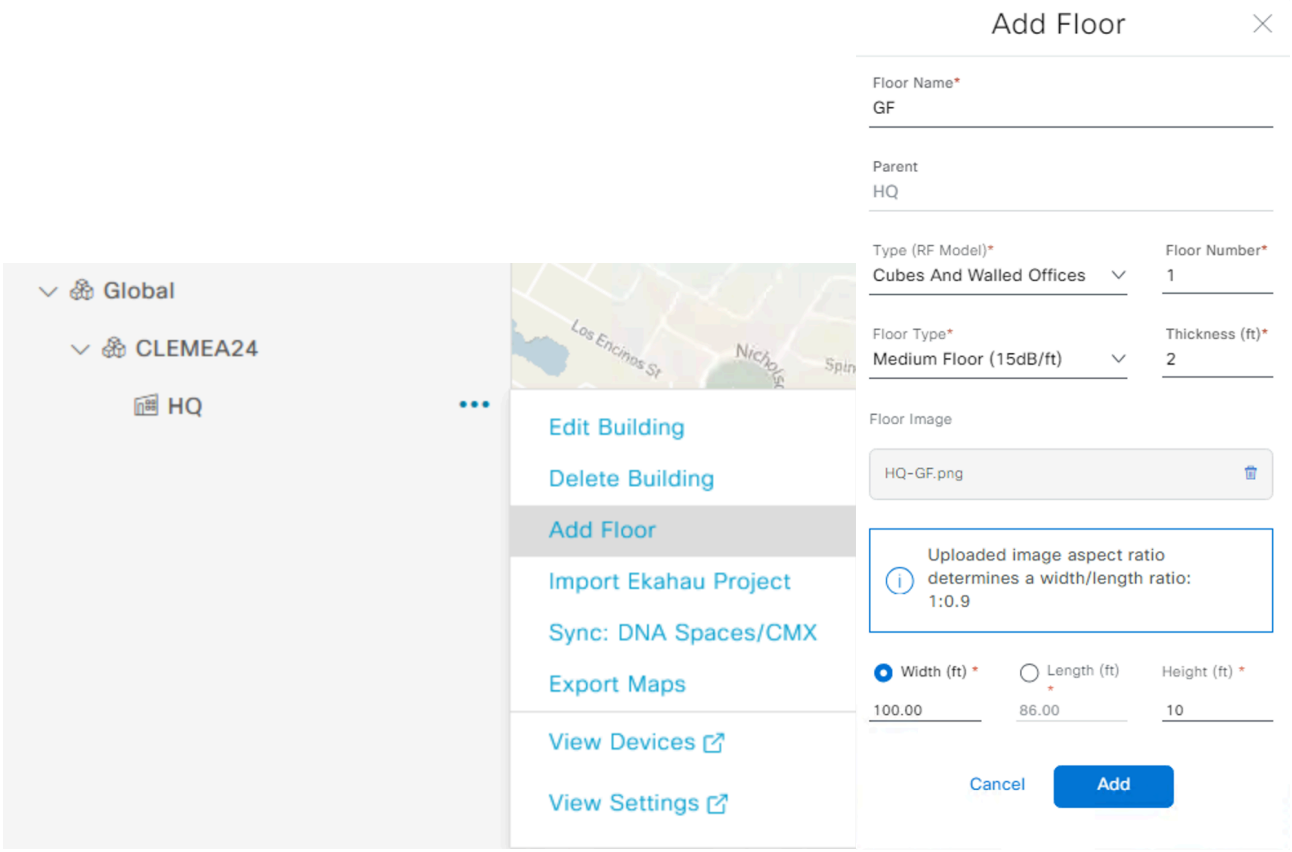
Figure 10 Site Hierarchy - Building



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

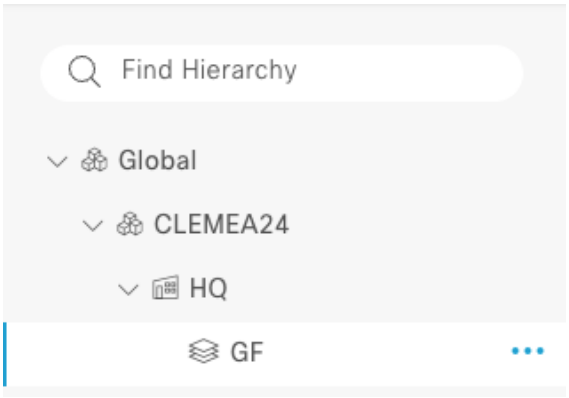
Hover over the three dots and click on **Add Floor,** name it as **GF** and use provided file **HQ-GF** to upload as floor plan using the default scale and sizing settings.

Figure 11 Site Hierarchy - Floor



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

Figure 12 Site Hierarchy - Task 1



Task 2: Ekahau to Catalyst Center Import

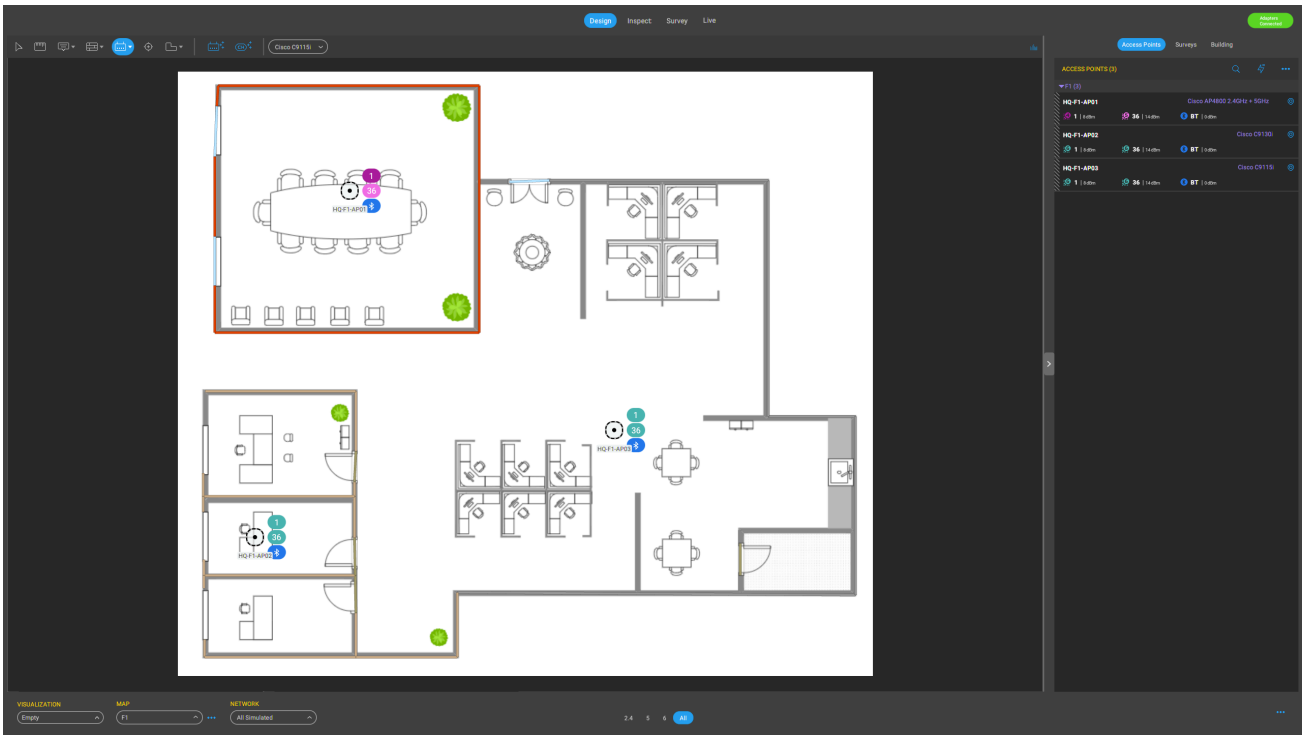
This activity will focus on importing Ekahau file with AP Placement into Catalyst Center hierarchy. This use case focuses on customers performing pre-deployment designs and helps them to import Ekahau files to maintain the AP positions as well as scale and obstacles.

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.

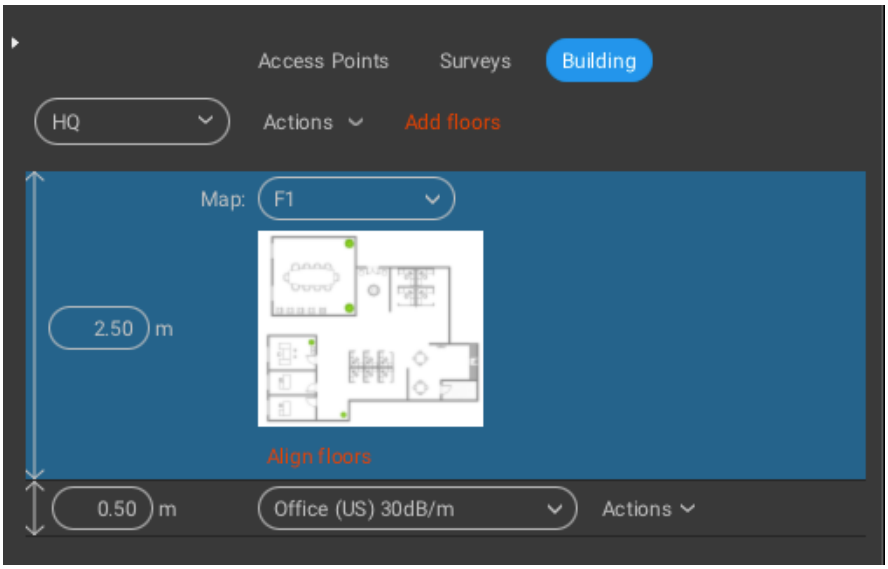
The Building **HQ** was created in .esx file and a floor named **F1** with three APs and several wall types.

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.

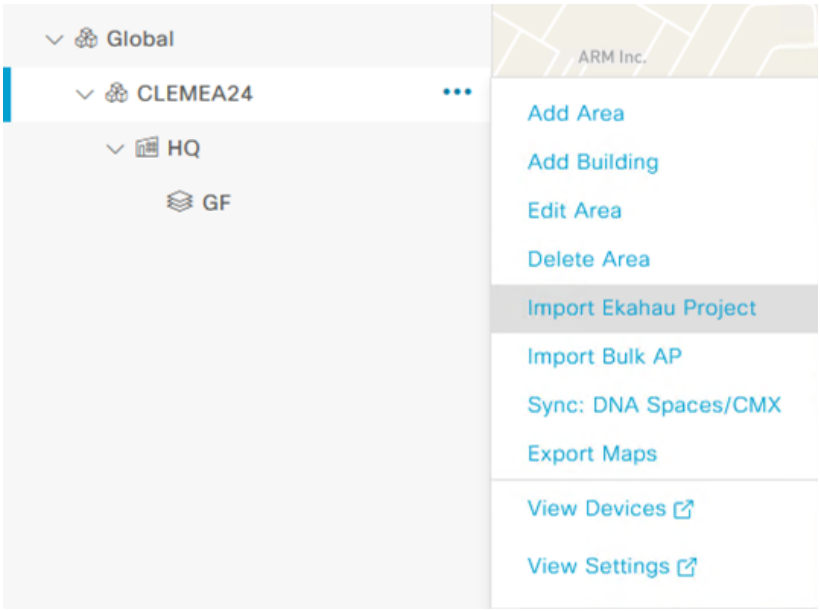
Figure 14 Ekahau Project - Building

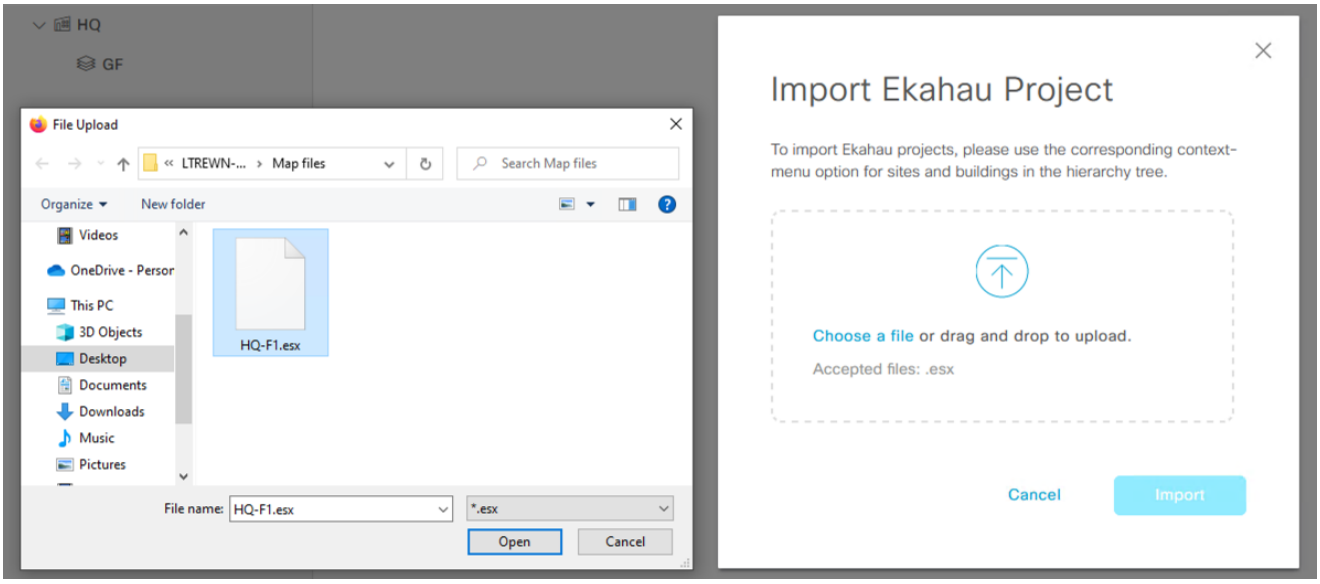


Step 1: Importing Ekahau Project into Catalyst Center Hierarchy

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.**

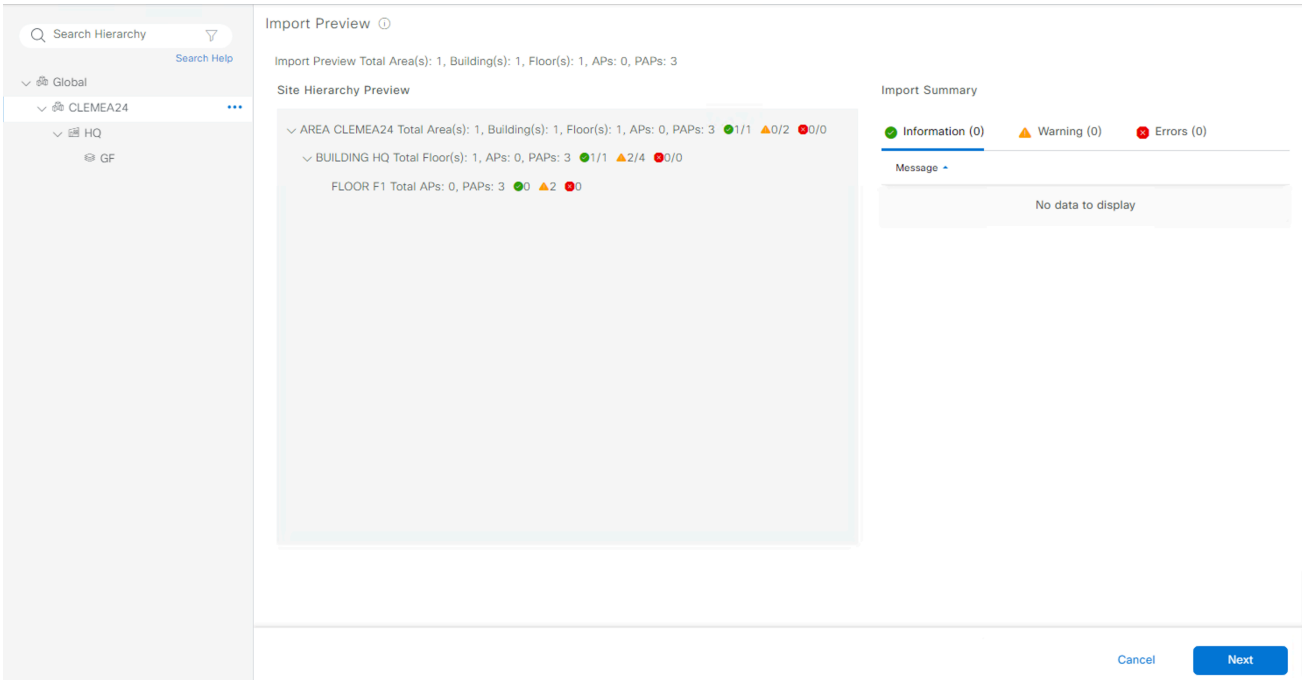
Figure 15 Import Preview - Ekahau





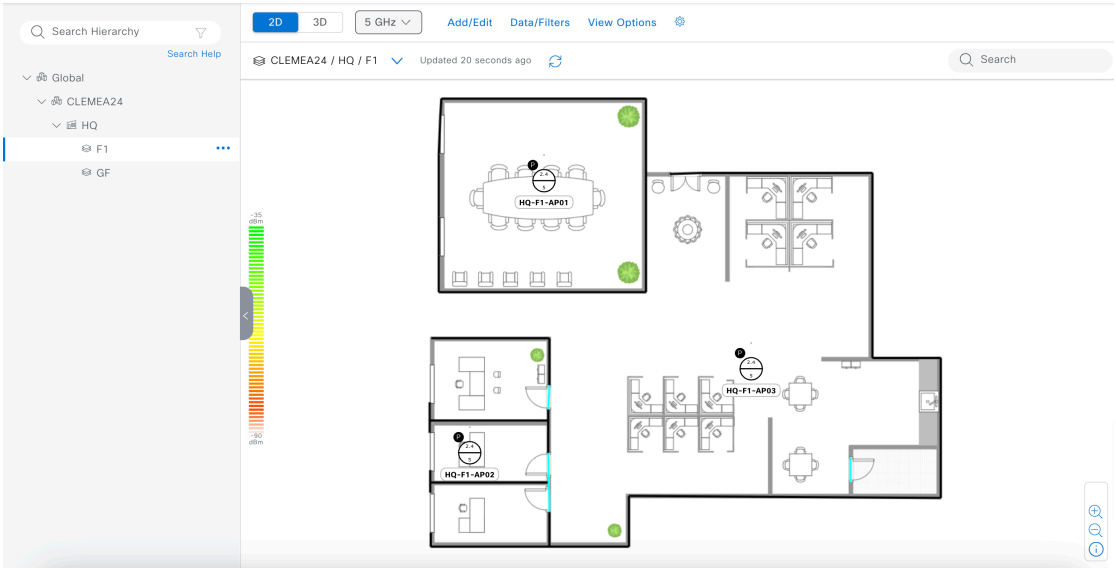
Import Preview screen should summarize all the items that will be imported into site hierarchy as in the screenshot below:

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

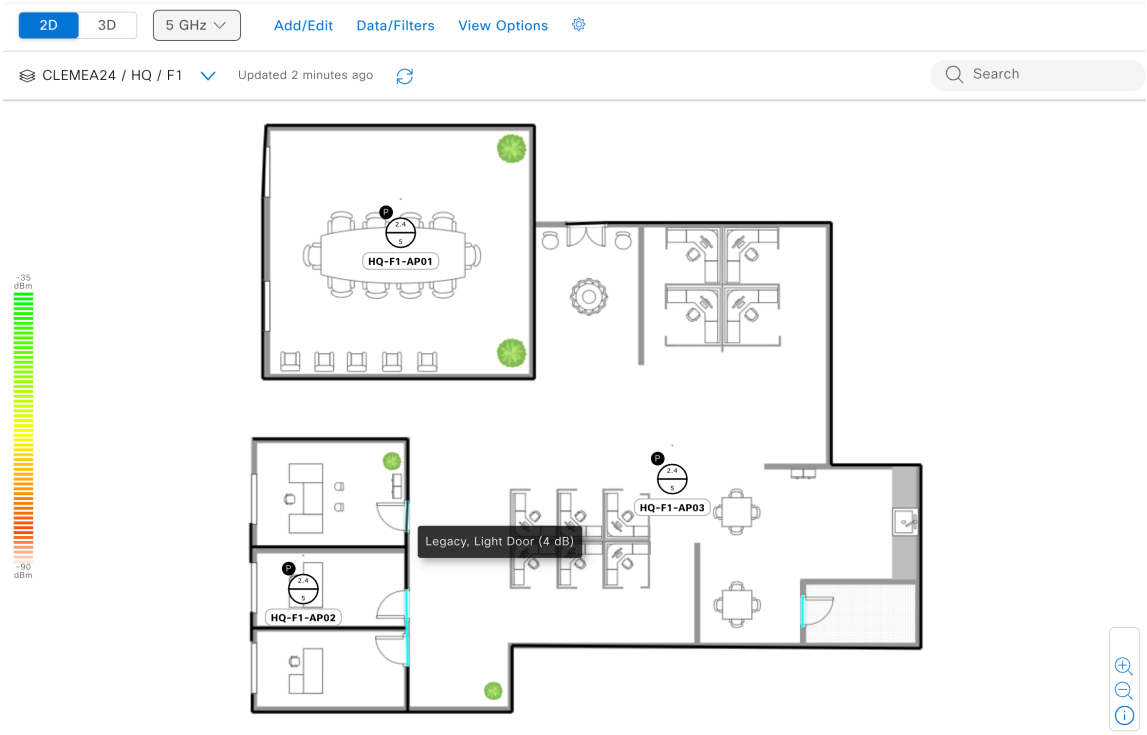


Please note that at this point in time, all the APs have the “P” icon which means they are Planned and not mapped to any physical APs.

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

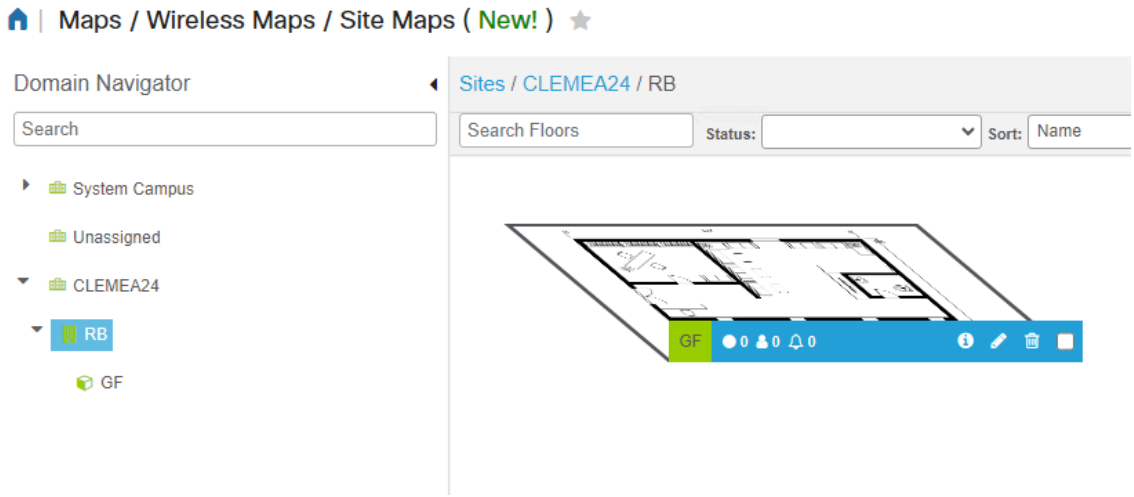
Google Chrome is the recommended browser for this task

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:

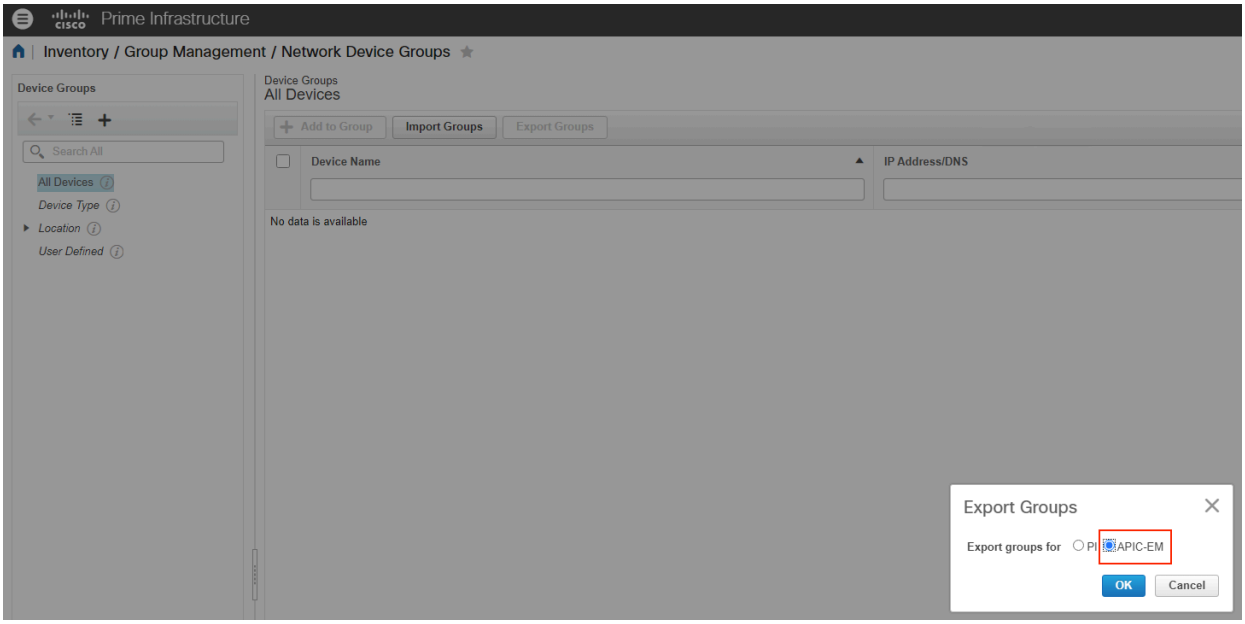
Figure 19 Prime Infrastructure - Site Maps



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

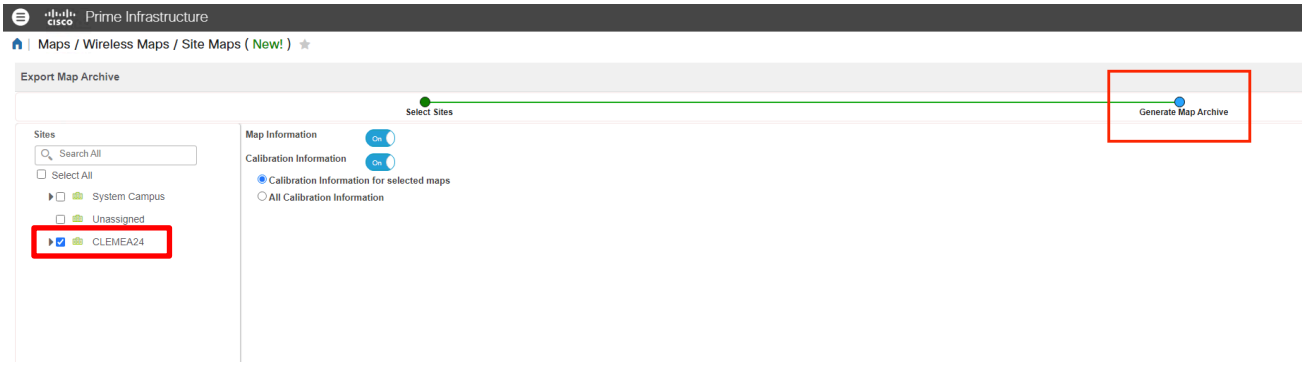


CSV file will be automatically saved to your workstation/jumphost.

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



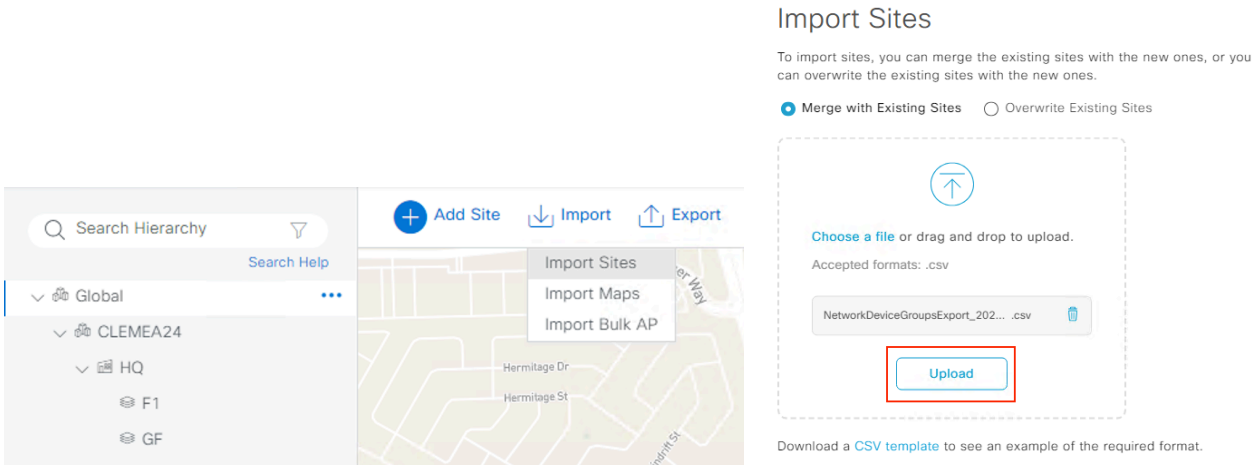
Click on **Generate Map Archive.** Tar.gz file will be automatically saved to your workstation/jumphost.

Step 4: Import Prime Infrastructure Device Groups to Catalyst Center

We will now import Device Groups into Catalyst Center.

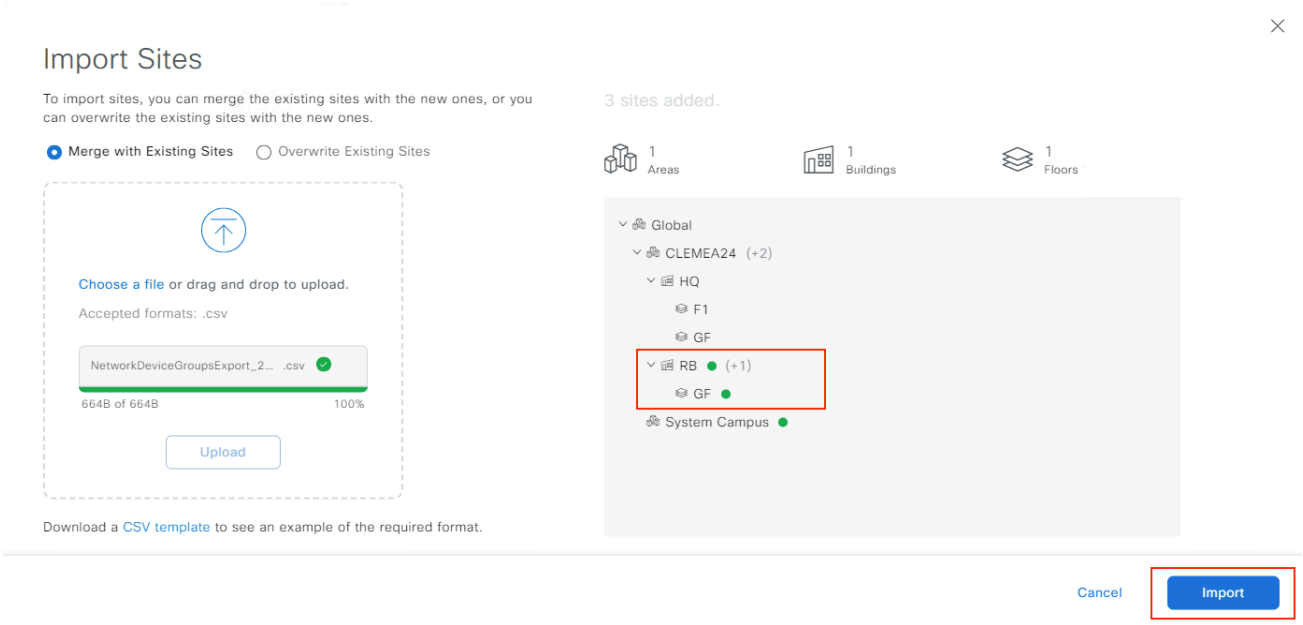
- Navigate to **Design > Network Hierarchy > Global > Import > Import Sites**
- choose the **Merge with Existing Sites** option.
- Select the **CSV file** that was exported from Prime Infrastructure for **CLEMEA24** area and click **Upload**.

Figure 22 Catalyst Center - Device Group Import



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

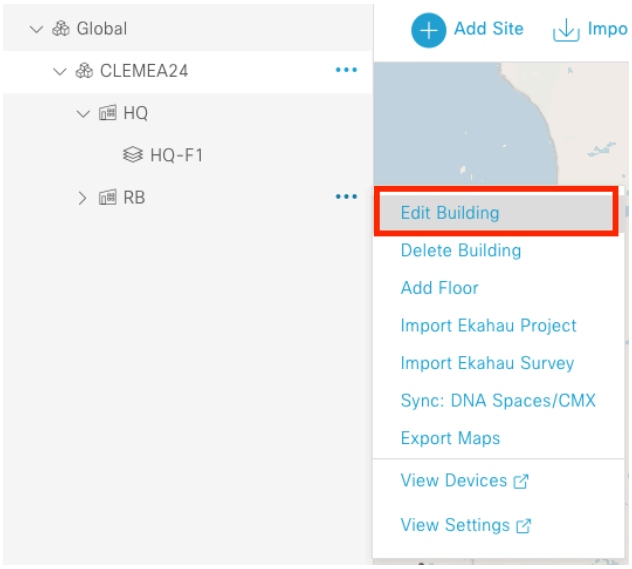
Figure 23 Catalyst Center - Sites Import



Click **OK** when asked "**Merge with Existing Sites**"

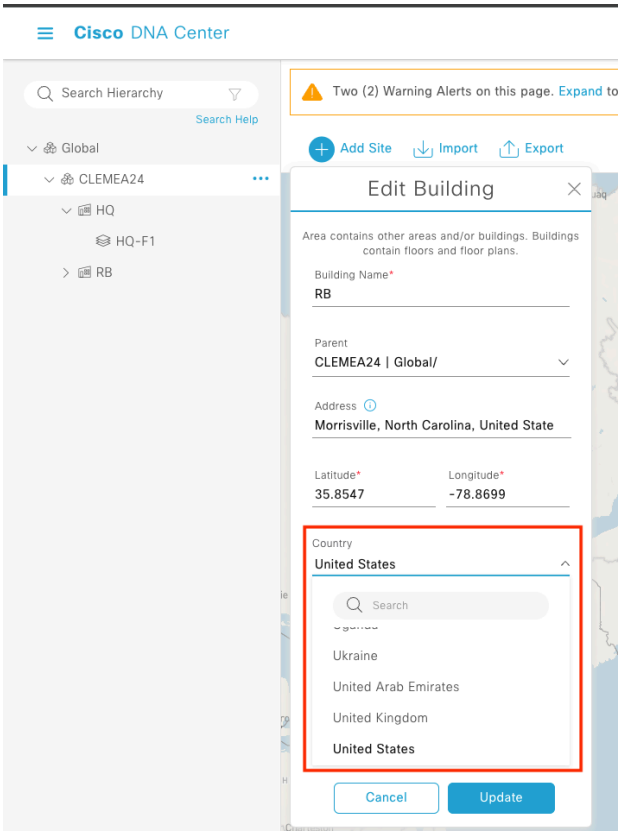
Once imported, we will proceed by setting correct **Country** for the RB location. Select **Edit Building** when hovering over three dots next to **RB** building:

Figure 24 Edit Building - Country



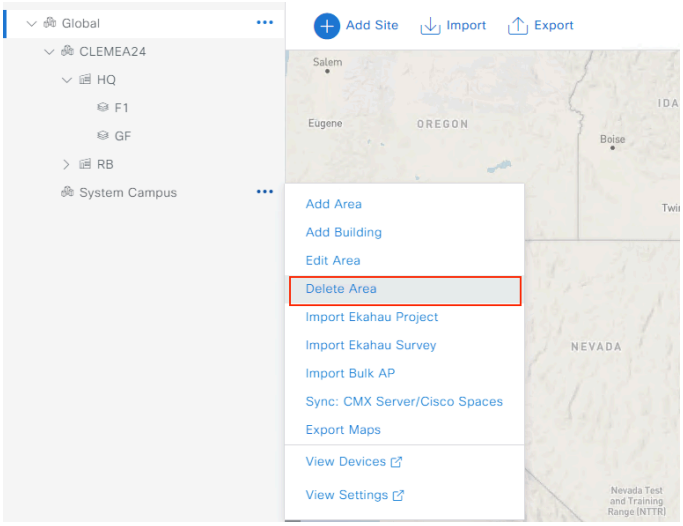
We will set the **Country** to **United States** to comply with the APs available in the lab:

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



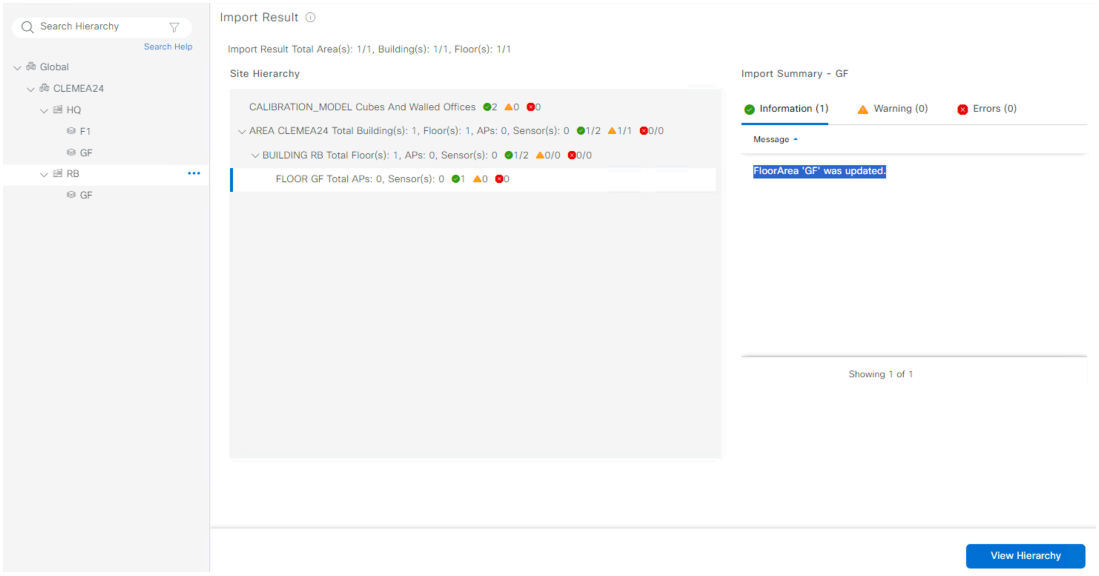
Step 5: Import Prime Infrastructure Map Archive to Catalyst Center

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

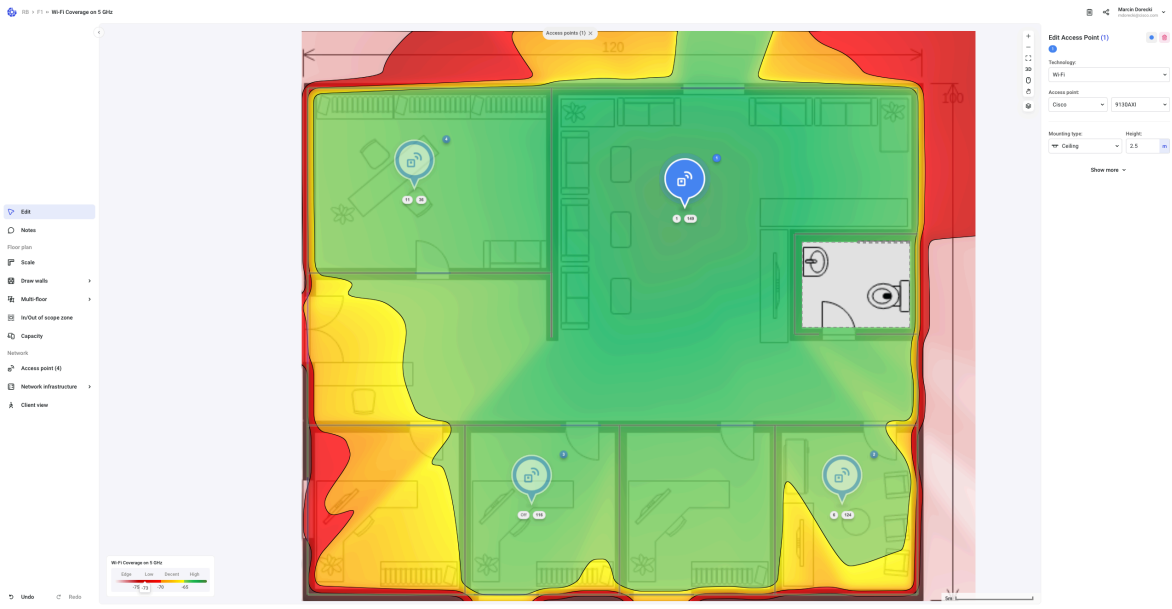
This task focuses on importing your Hamina design into Catalyst Center.

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

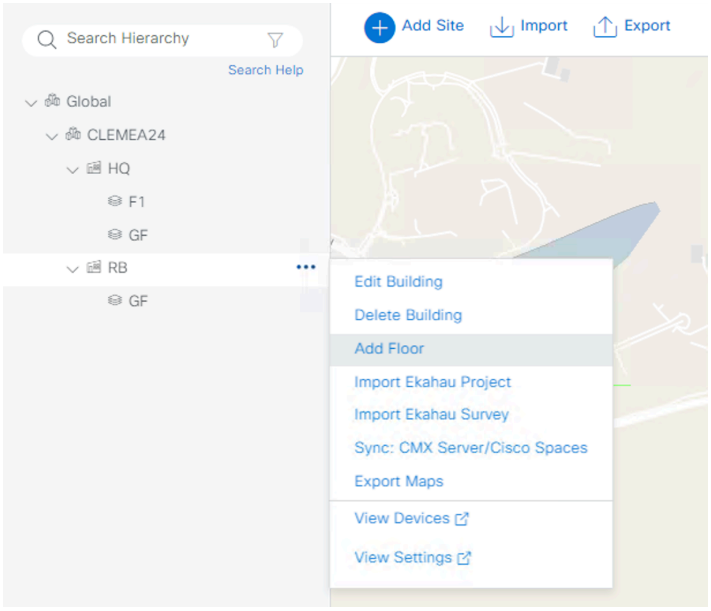


The same design was already exported according to the procedure found in the link https://docs.hamina.com/planner/import-export/cisco-catalyst-center

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

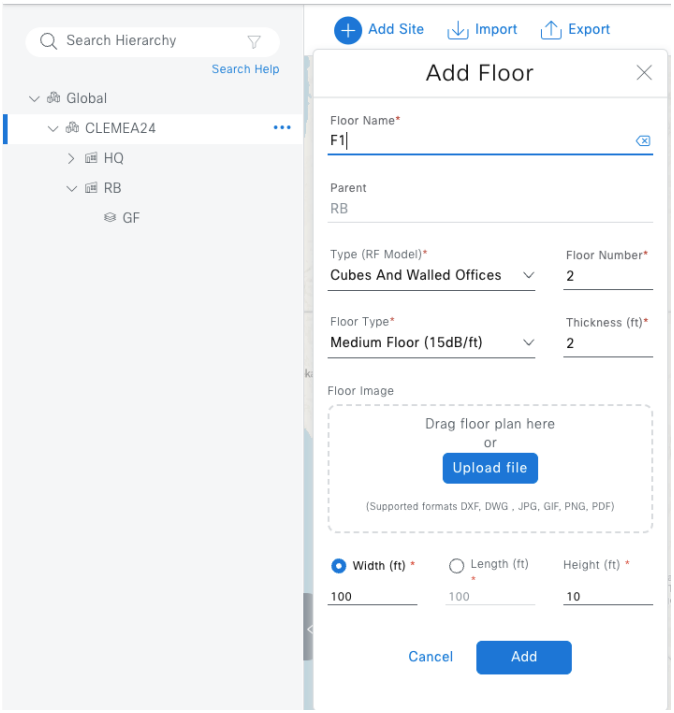
- Navigate to **Design> Network Hierarchy > RB**
- Select **Add Floor** under **RB** building

Figure 29 RB - Add Floor



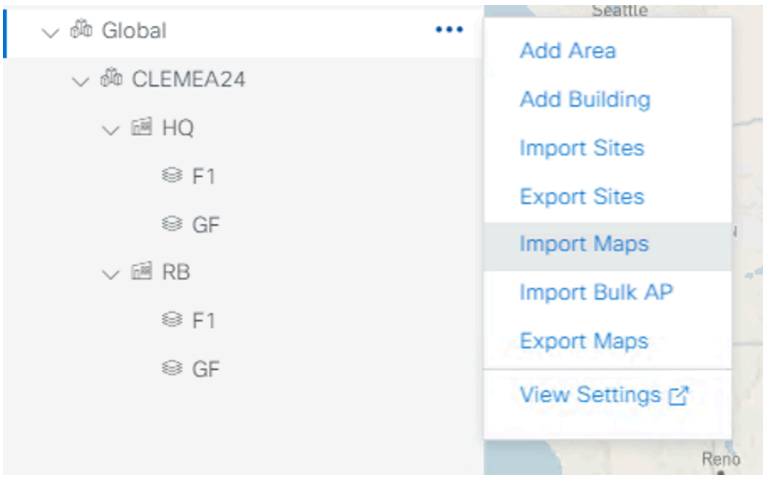
- Name the floor as **F1** and do not upload any floor plan as of now
- Click **Add**

Figure 30 RB - F1 creation



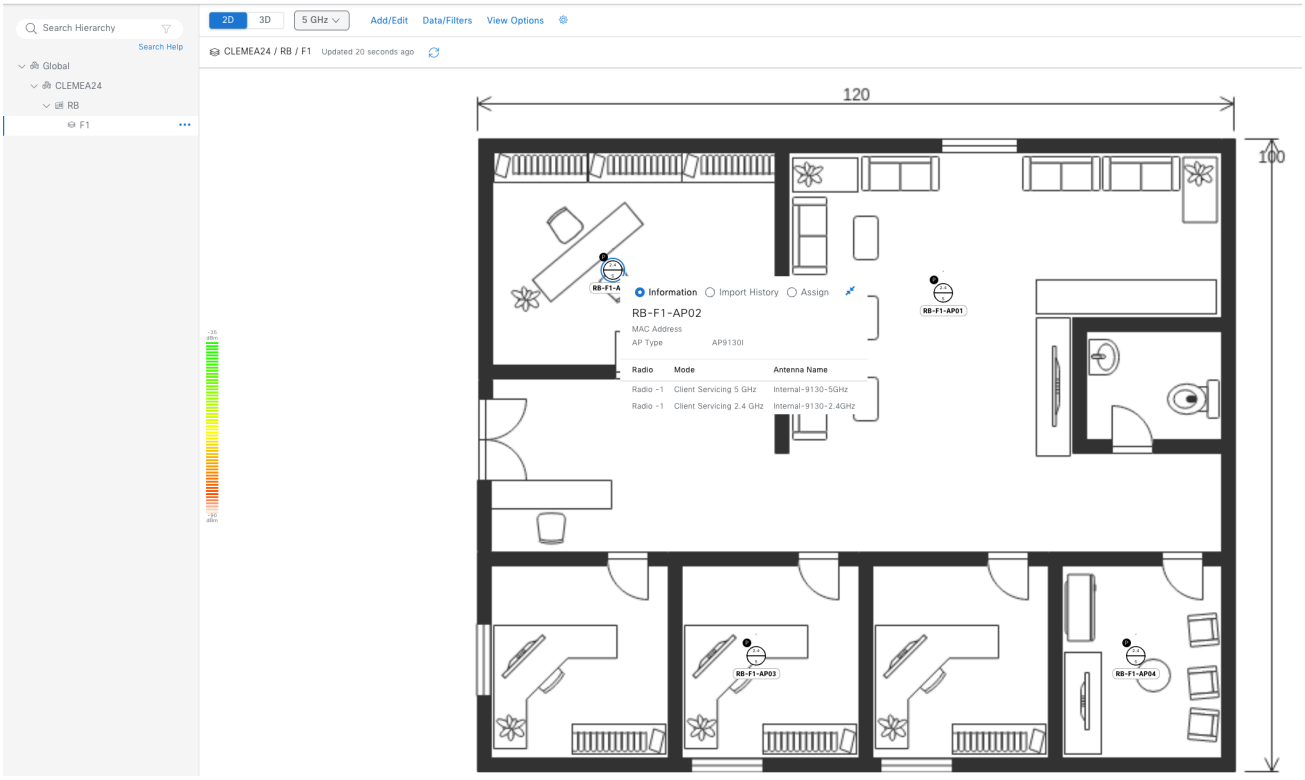
- Hover over three dots next to **Global** and select **Import Maps**

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

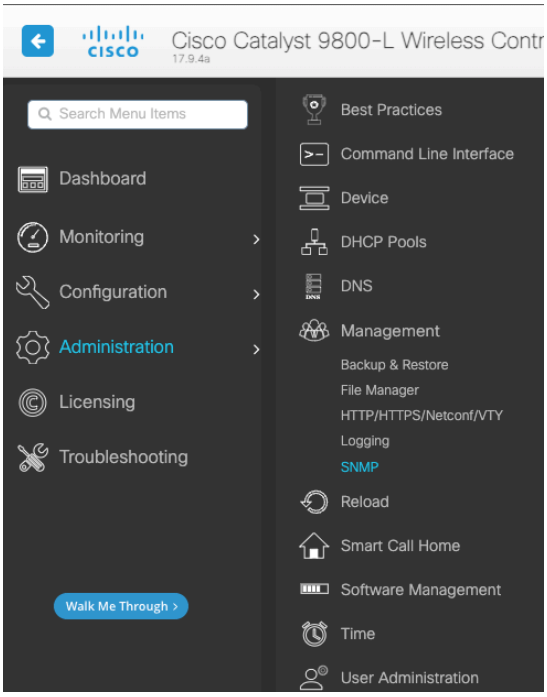
Navigate to the 9800 WLC GUI via https://198.19.11.10

Username: admin

Password: C1sco12345

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

Figure 33 9800 WLC GUI - SNMP



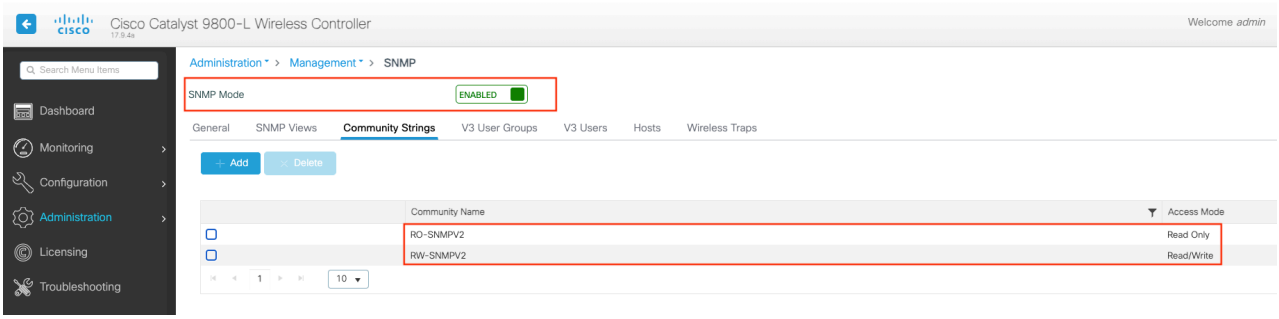
- **Enable** the SNMP Mode,
- then navigate to the **community strings** page and add two SNMPv2 communities:

Table 4 WLC Discovery - SNMP Communities

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

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

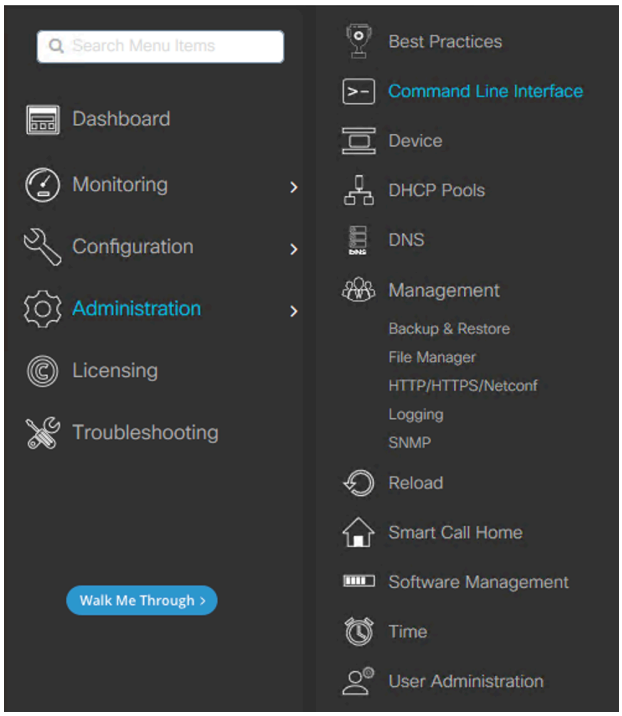
Figure 34 SNMPv2 Configuration



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



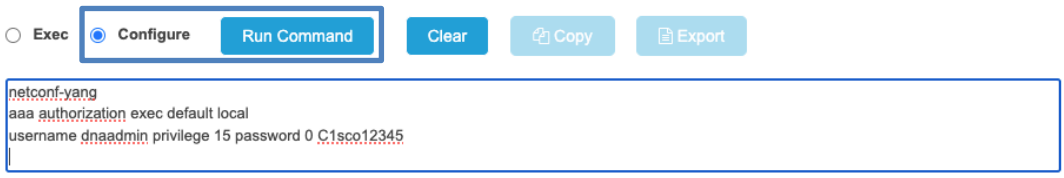
This page is just like a CLI (SSH session) from GUI.

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
```

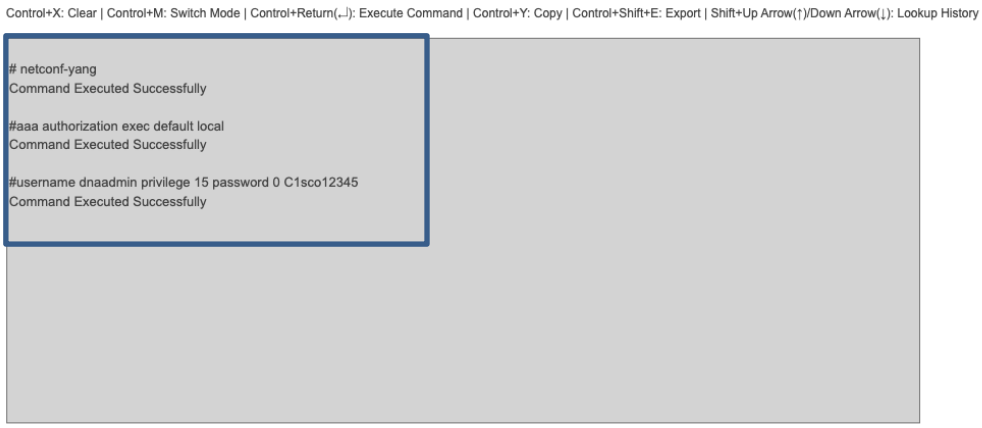
Note: This new username is to support Catalyst Center password requirements for HTTPS access.

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.

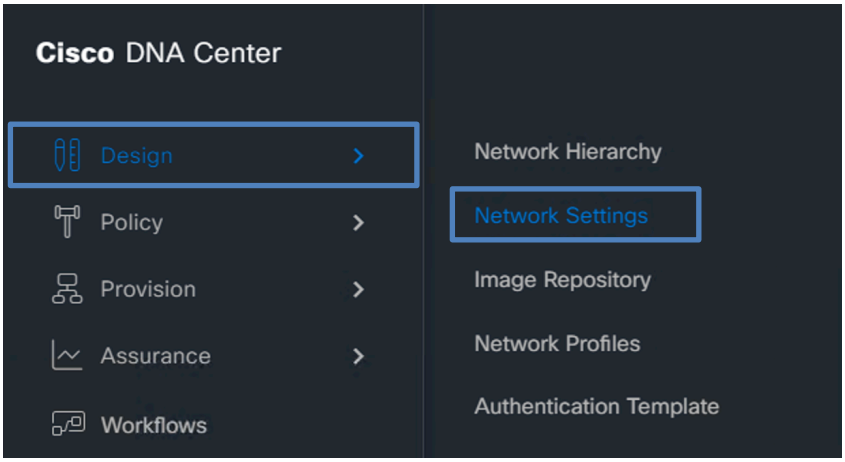
Log into Catalyst Center GUI using https://198.18.129.100/ using credentials:

Username: admin

Password: C1sco12345

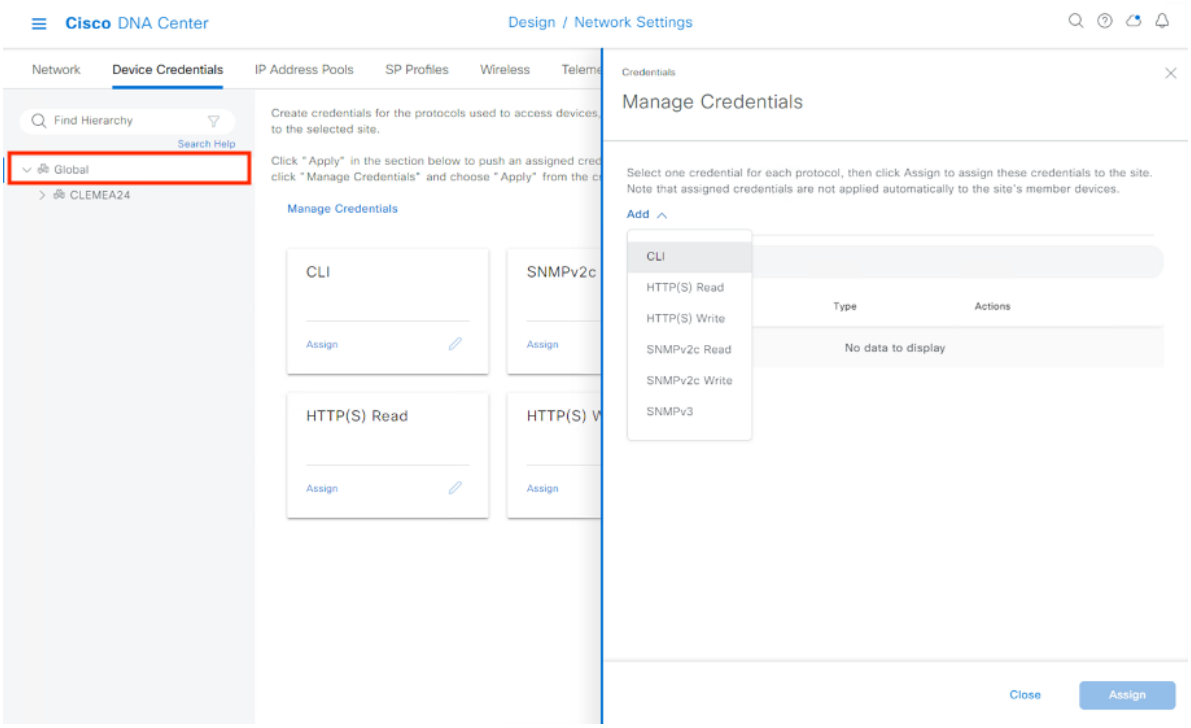
Navigate to the Dashboard top menu and click on **Design > Network Settings**

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.

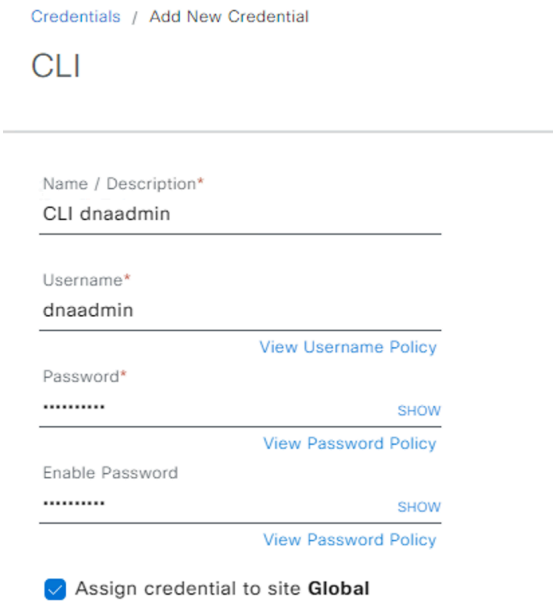
Table 5 WLC Discovery – Details

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



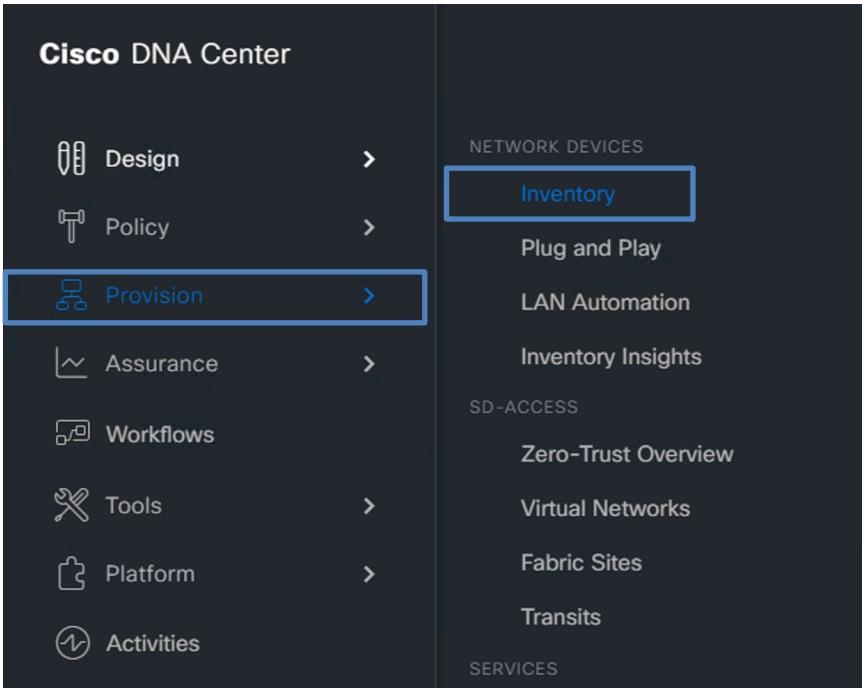
We prefilled SNMP, only insert CLI Credentials ☺

Table 6 WLC Discovery - SNMP Communities

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

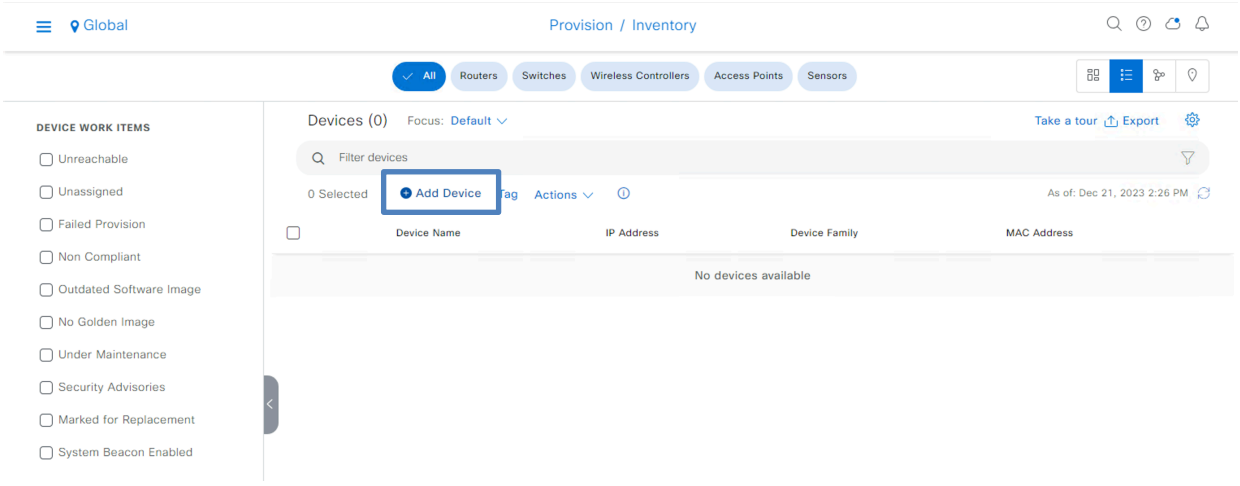
When finished with the network credentials, navigate to the Dashboard top menu and click on **Provision > Inventory**

Figure 41 Catalyst Center - Provision - Inventory



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

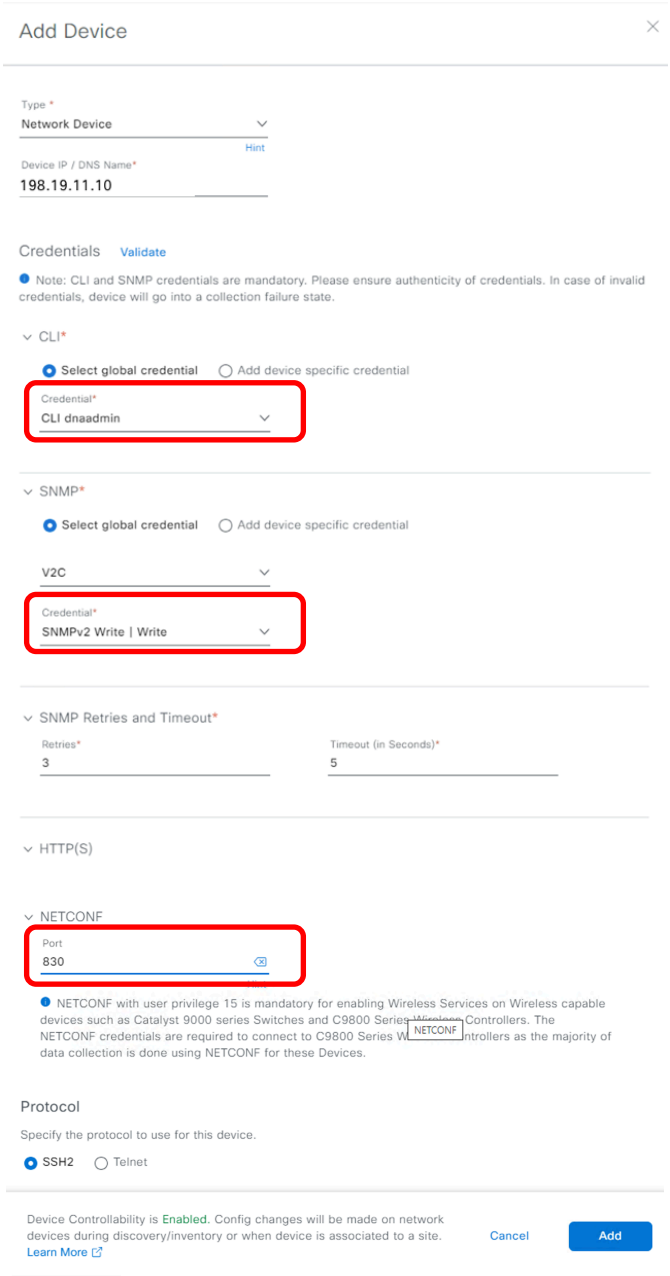
Figure 42 Catalyst Center - Inventory - Add Device



- 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

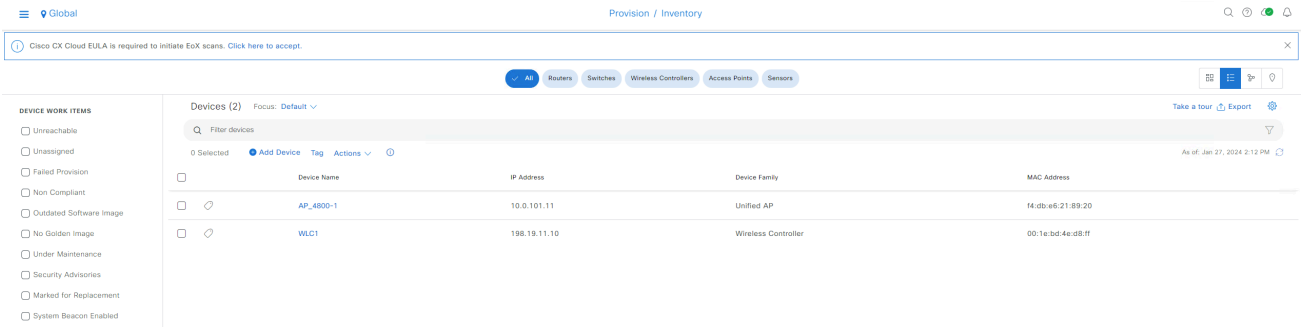


Click “**Add**” and the device will get added to the cisco CATALYST CENTER inventory.

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



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

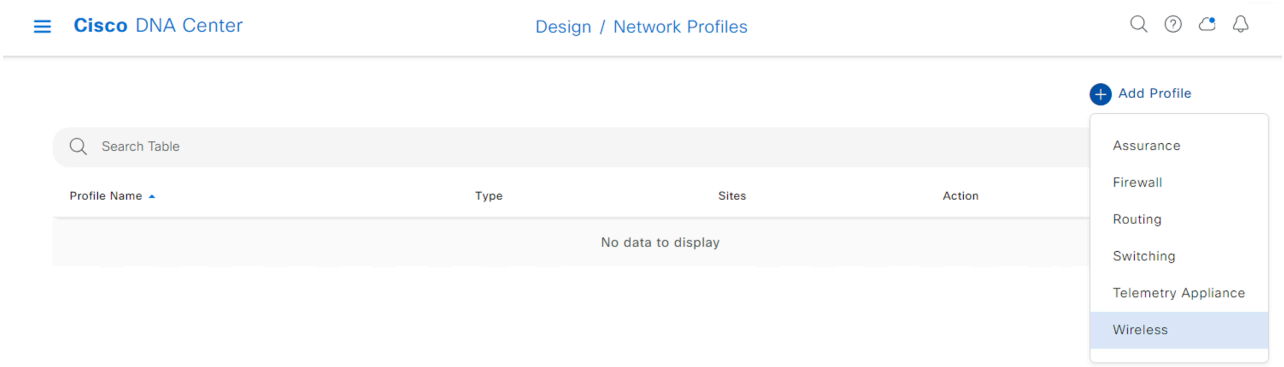
In order to bond the wireless settings with the hierarchy, we must prepare two **Network Profiles** to support **HQ** and **RB** locations.

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)

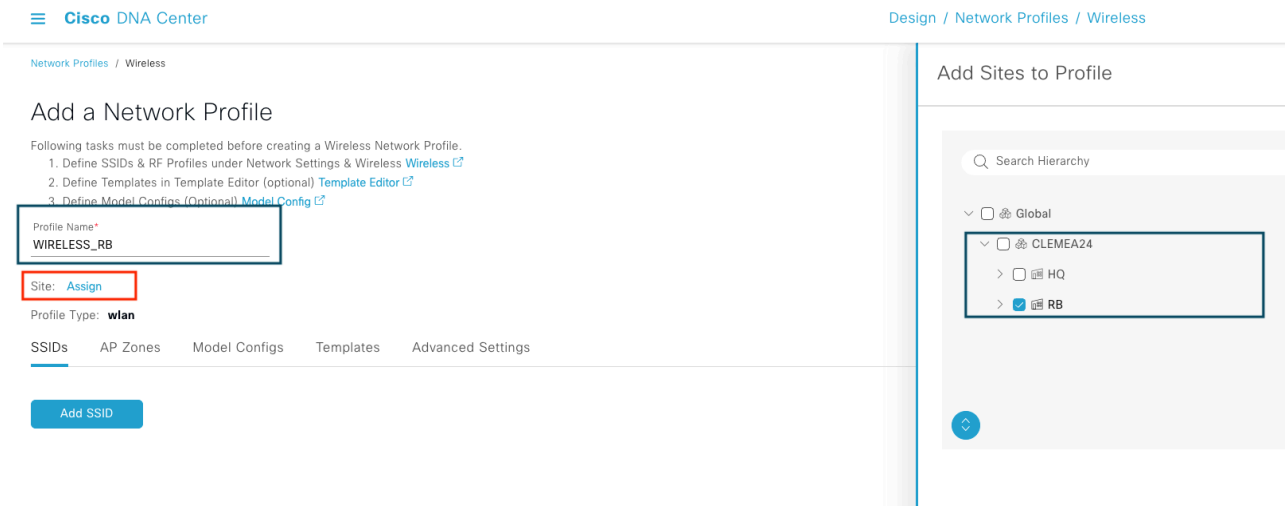
- Go to **Design > Network Profiles**,
- click on **Add Profile > Wireless**

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



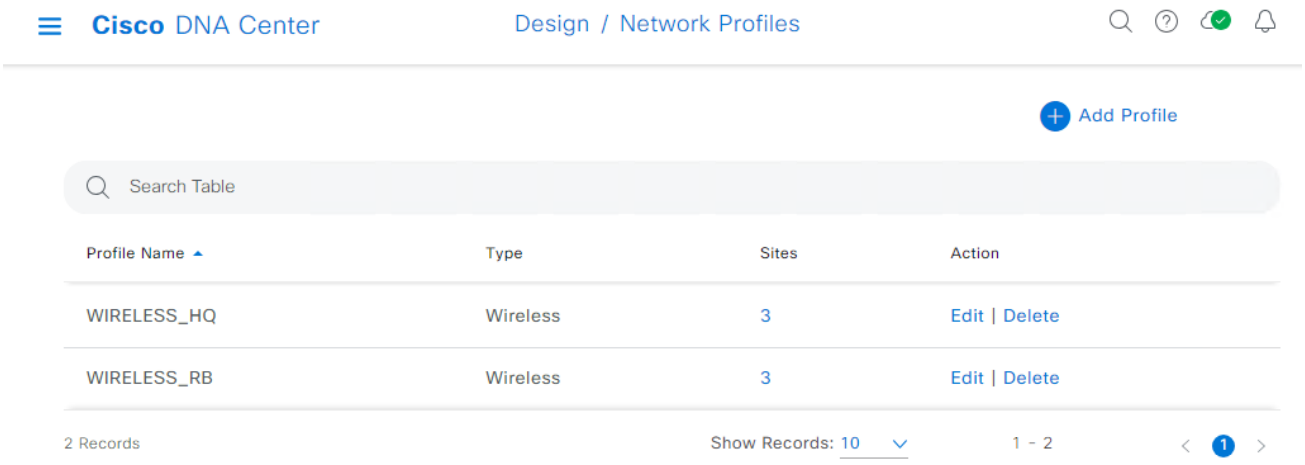
Repeat the procedure for HQ Network Profile using following values the name **WIRELESS_HQ**:

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



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
  - SNMP Credentials
  - NETCONF Credentials

- Adding Devices to Inventory
  - Cisco TrustSec (CTS) Credentials (if the Global site is configured with Cisco ISE as AAA).

- Assigning Devices to a Site
  - Controller Certificates
  - SNMP Trap Server Definitions
  - Syslog Server Definitions

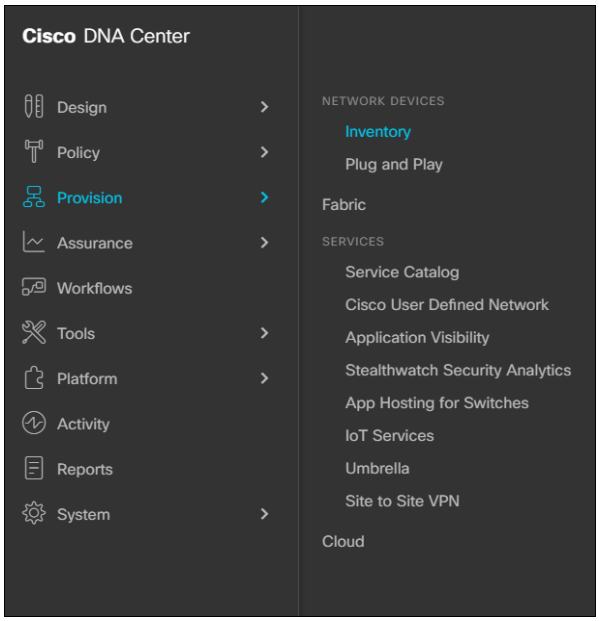
- NetFlow Server Definitions
- Wireless Service Assurance (WSA)
- IPDT Enablement

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**

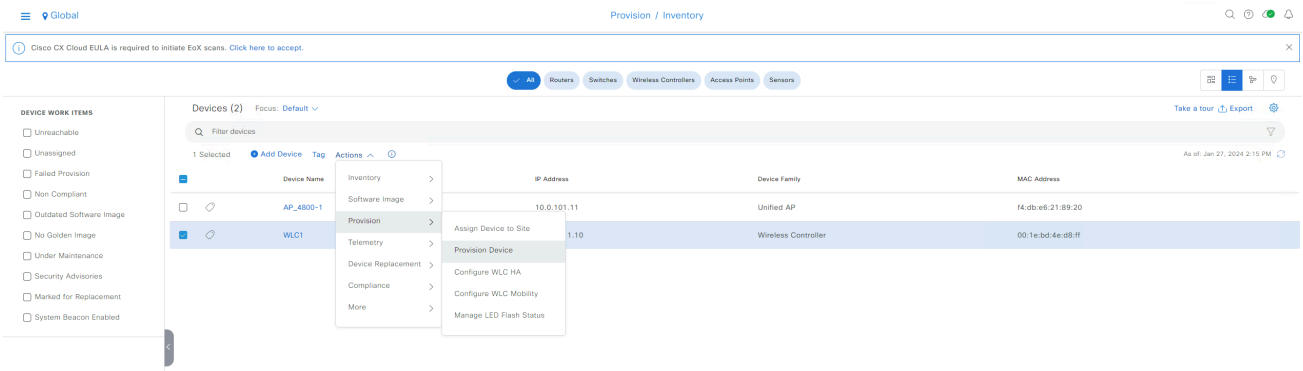
For this, click on the **Provision > Inventory** tab

Figure 48 Assign to site and Provision



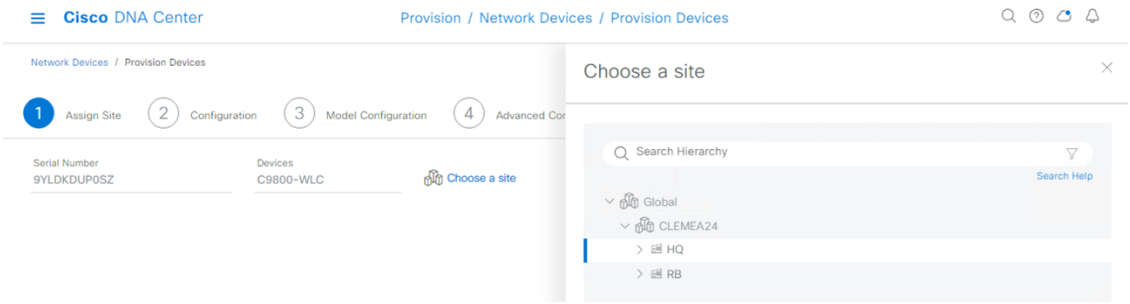
Select the WLC and hover over “**Actions**” field and navigate to “**Provision**” and then to “**Provision Device**”.

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

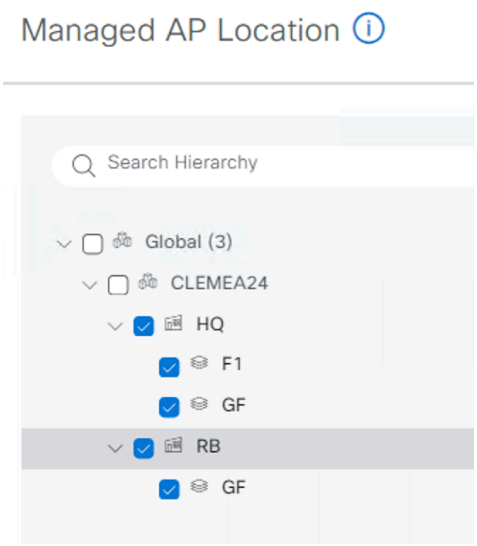
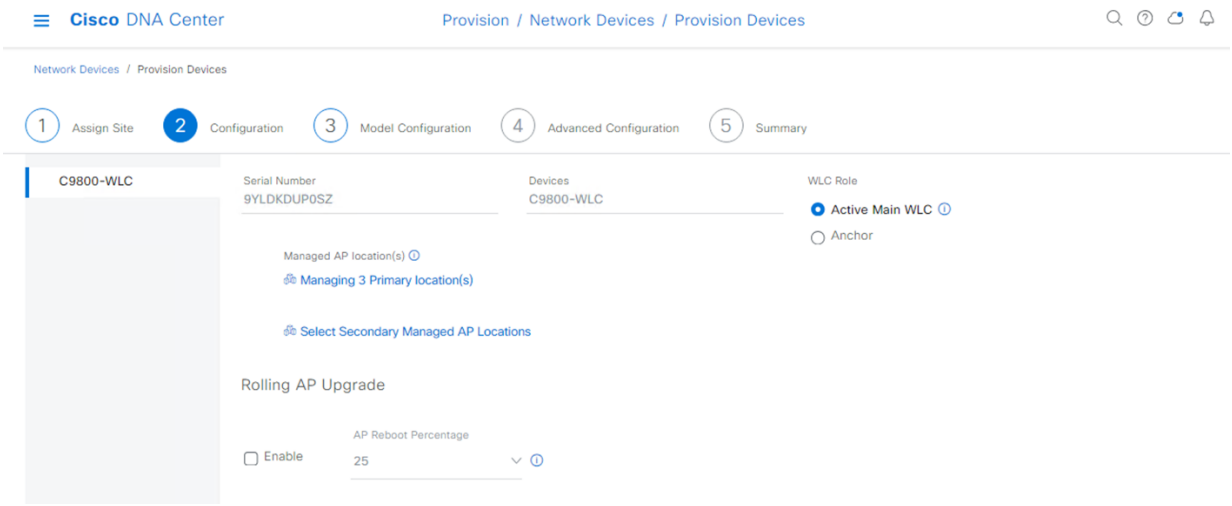
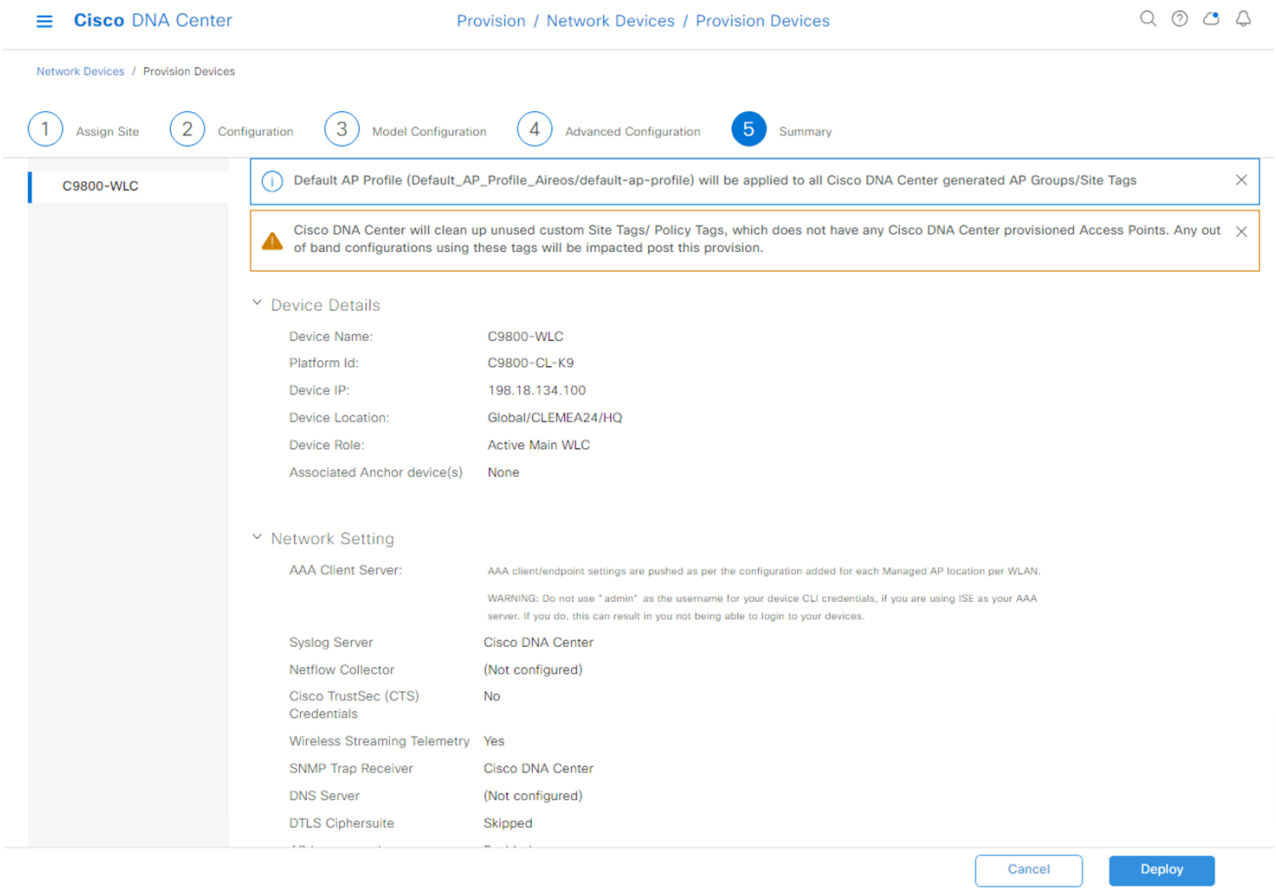


Figure 52 Assign to site and Provision



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

Figure 53 Assign to site and Provision

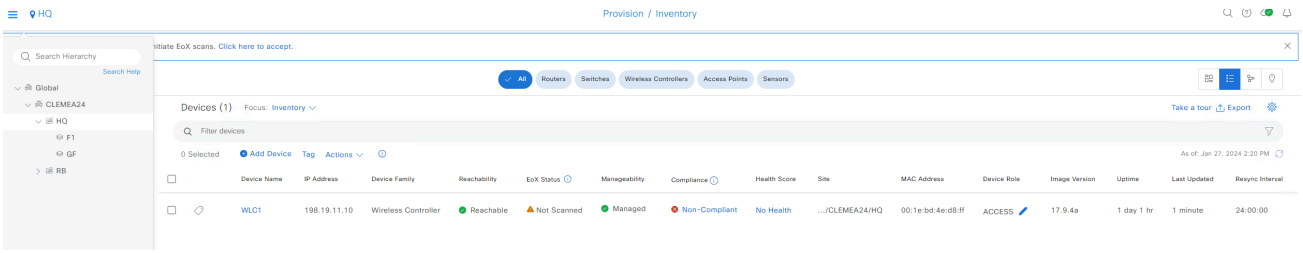


Warning: Cisco DNA Center will clean up unused custom Site Tags and Policy Tags **which do not have any configured Access Points**. Any out of band configurations using these tags will be impacted post this provision.

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

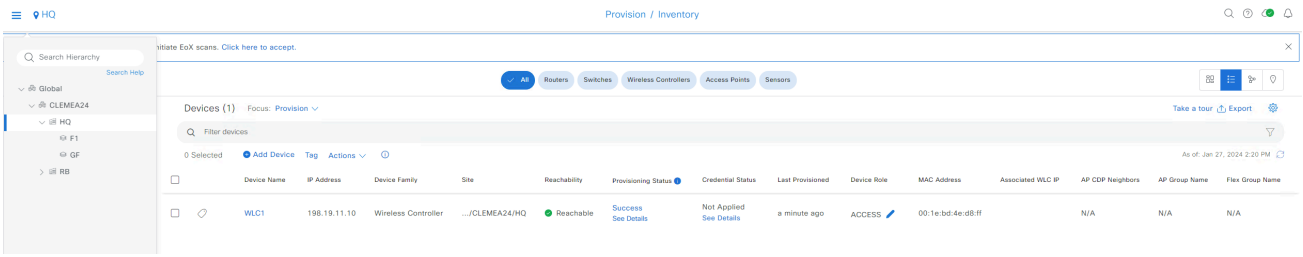
Validate if the provisioning was successful by clicking in **HQ** in the hierarchy and confirming the WLC is placed there.

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**”.

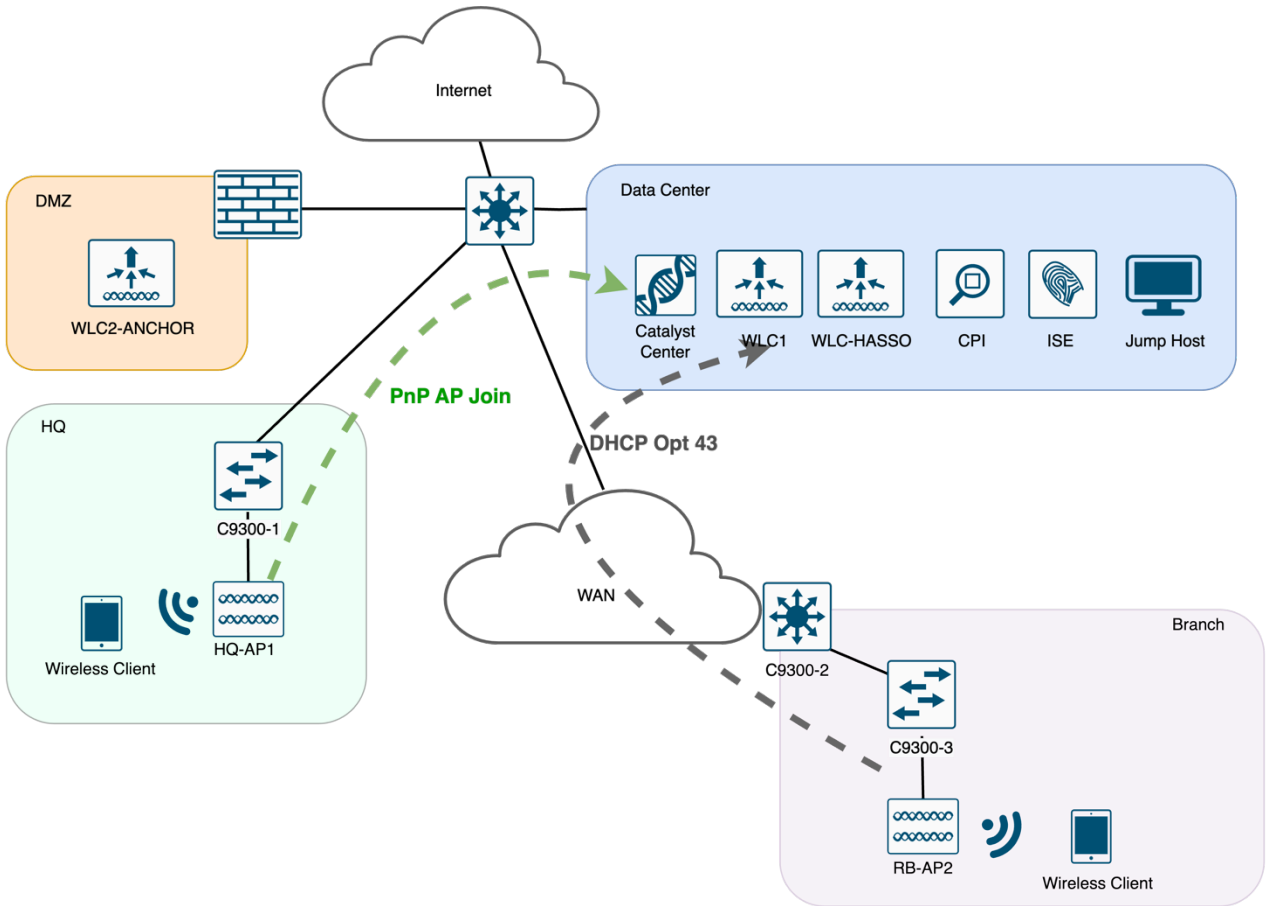
Task 6: Access Point Discovery

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.

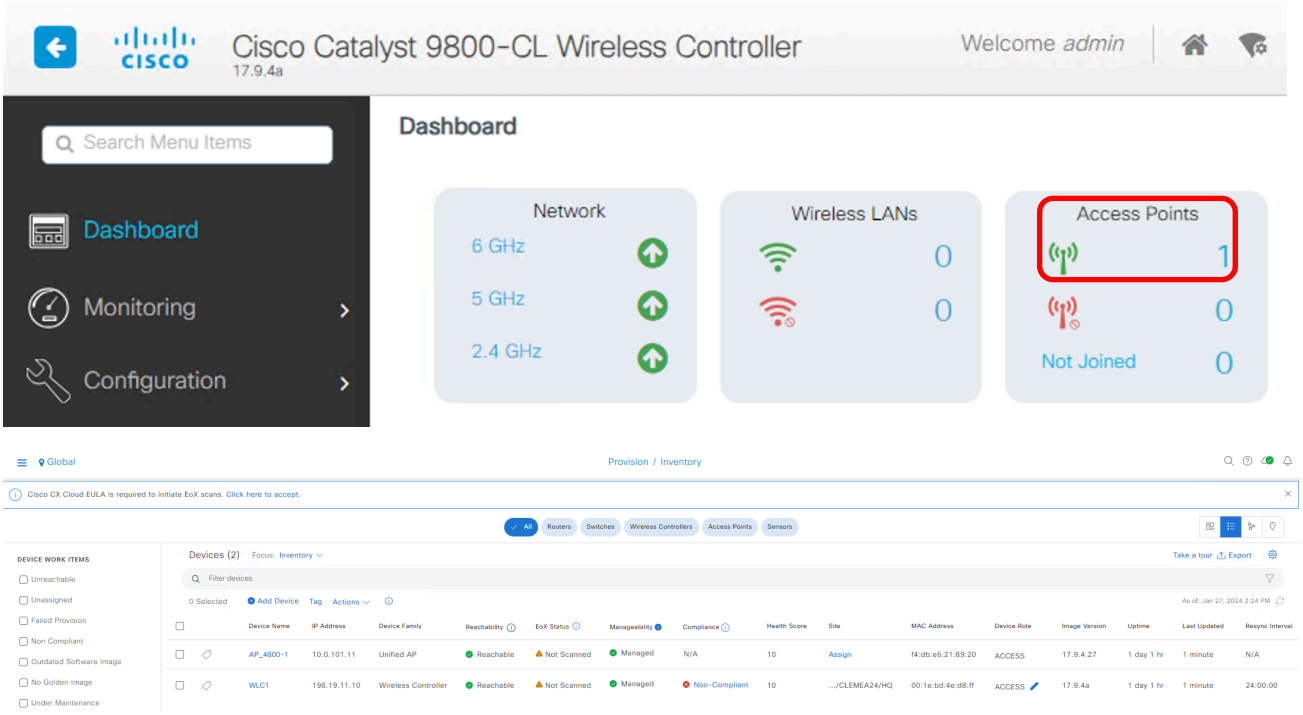
Here is the **snippet** of the switch **9300-2** at port Gig 1/0/2.

```
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



AP Joining via Plug and Play

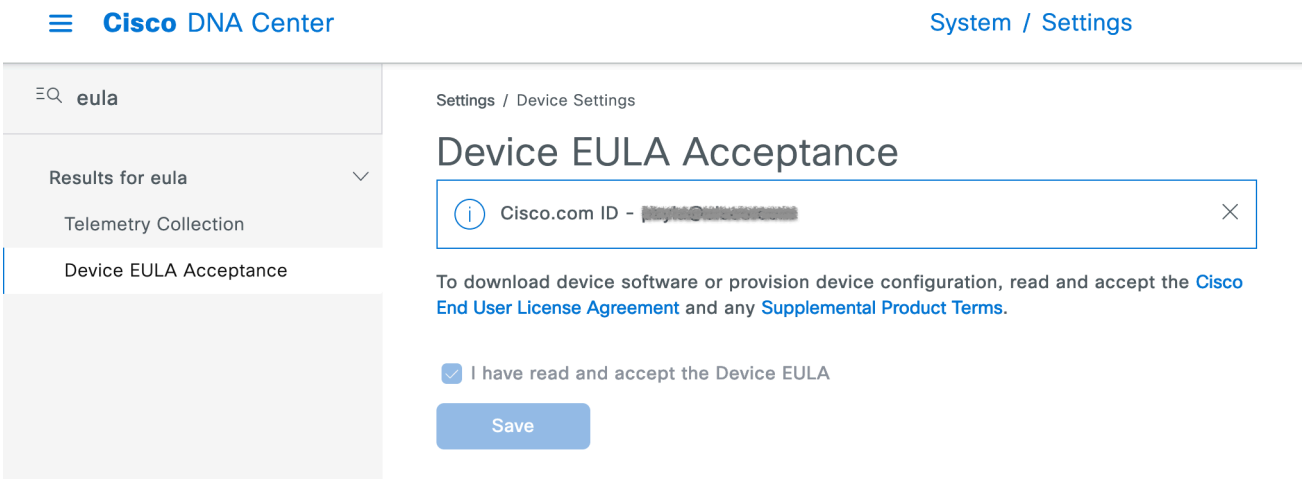
In order for PNP to work, the following prerequisites are mandatory:

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



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

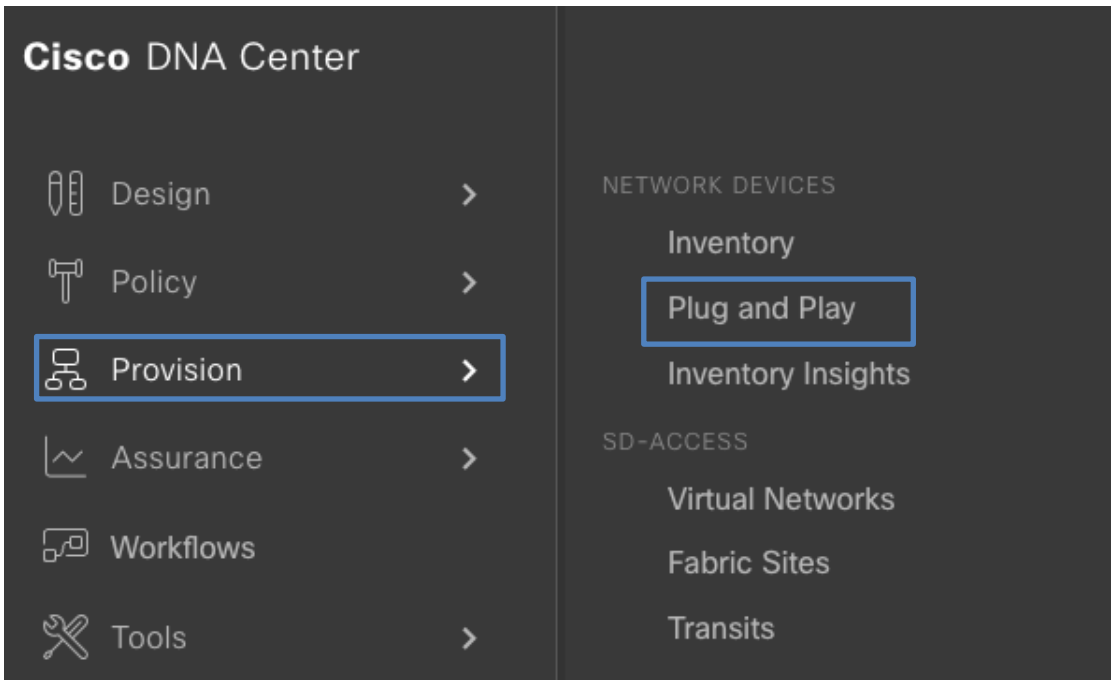
This AP obtains the IP address in the VLAN 201, the port where it connects is "access mode" needed for "local mode AP scenario".

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



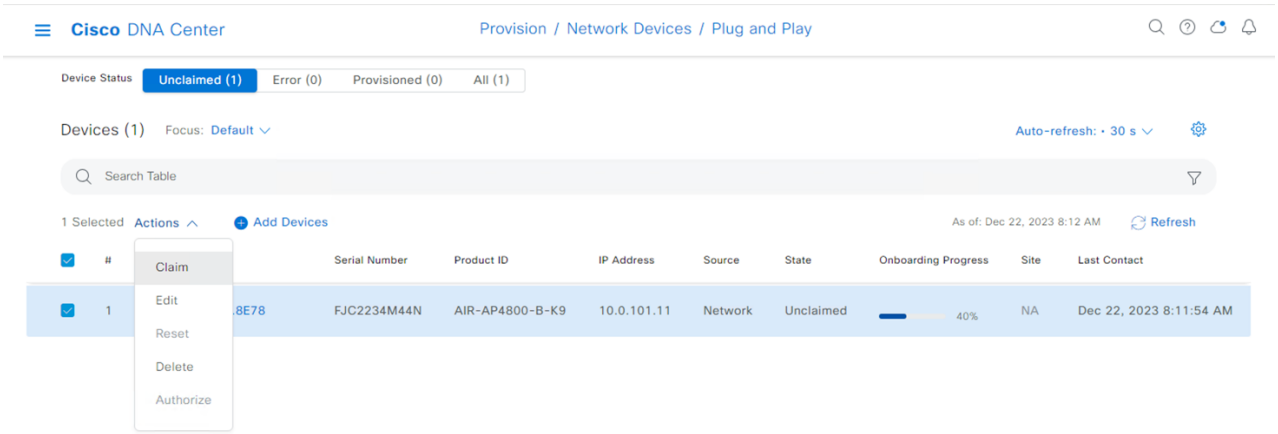
The AP will appear in the Unclaimed section.

Figure 60 Provision - Plug and Play

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**.

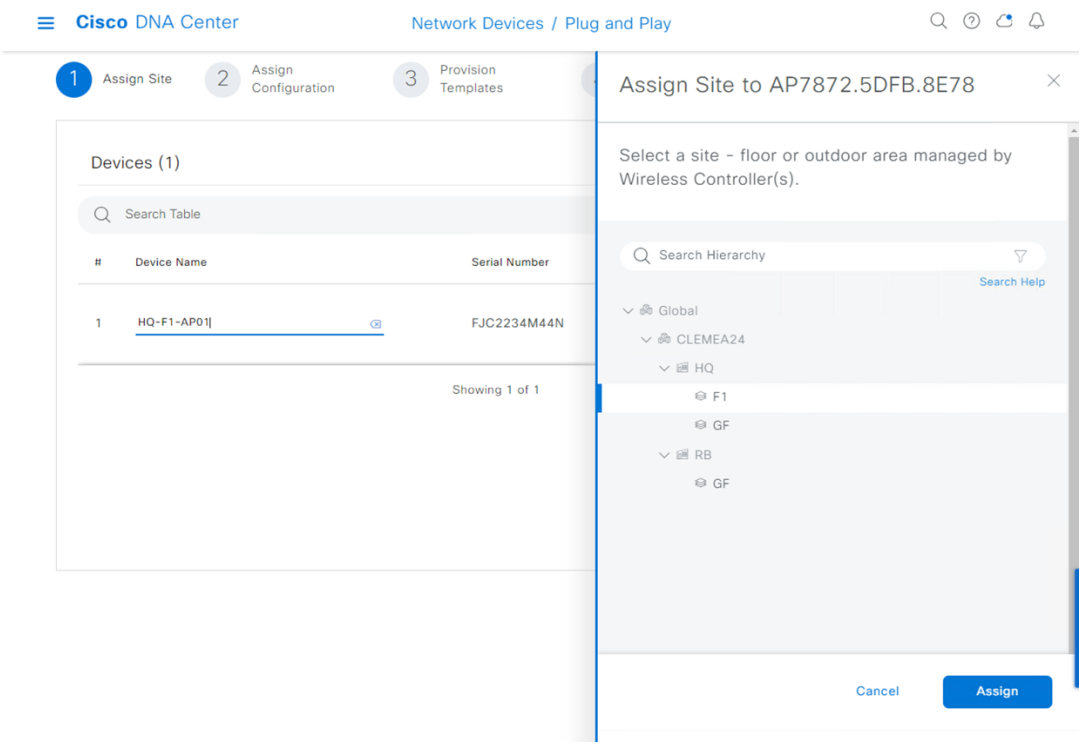
Figure 61 Plug and Play AP Claim



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



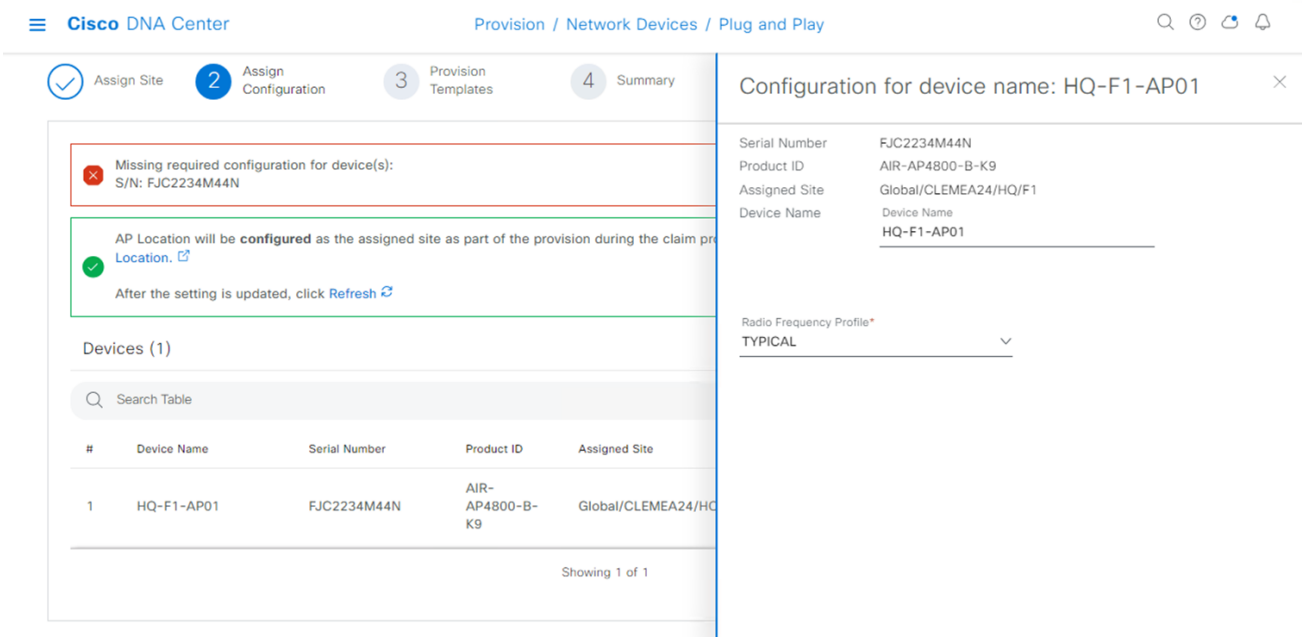
Note: APs must be assigned to a floor with a wireless controller managing the building.

Click **Next**.

The Assign Configuration window opens.

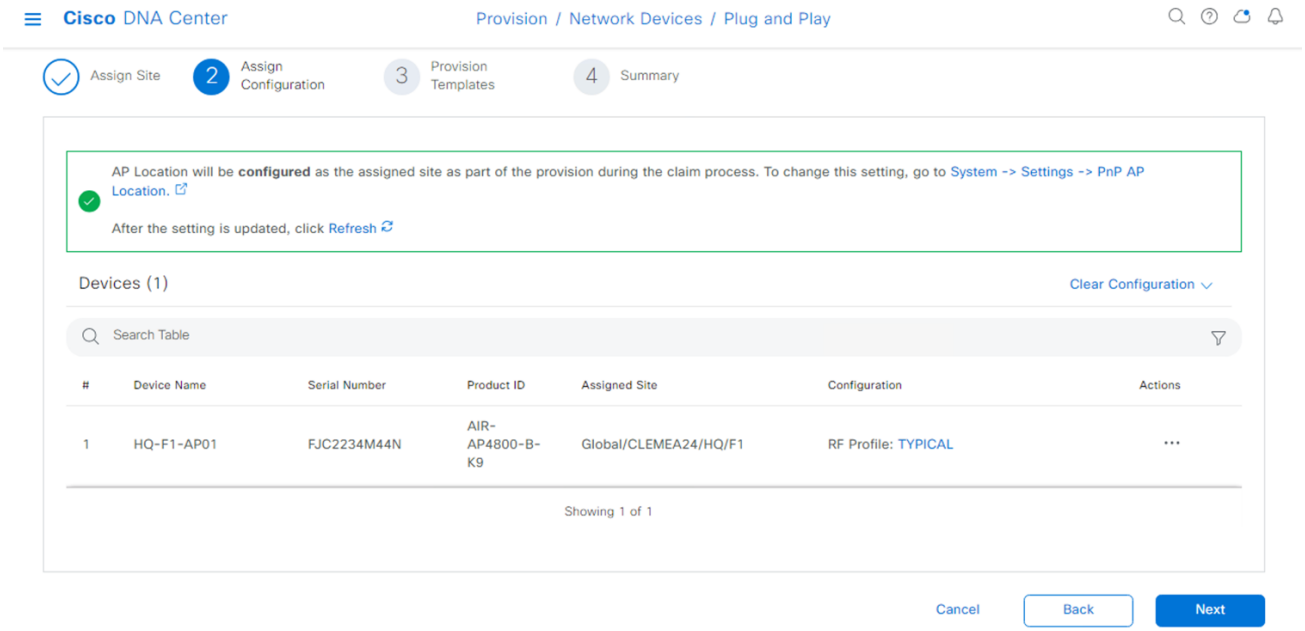
For an AP device, in the Radio Frequency Profile drop-down list, choose **TYPICAL**

Figure 63 Plug and Play AP Claim



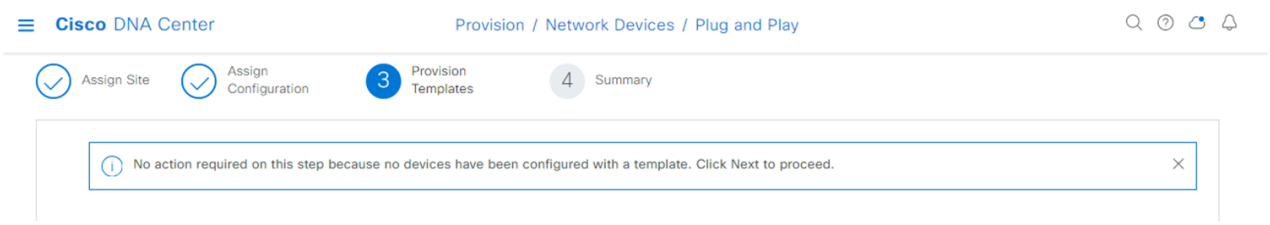
click **Save**

Figure 64 Plug and Play AP Claim



Click **Next**

Figure 65 Plug and Play AP Claim



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

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

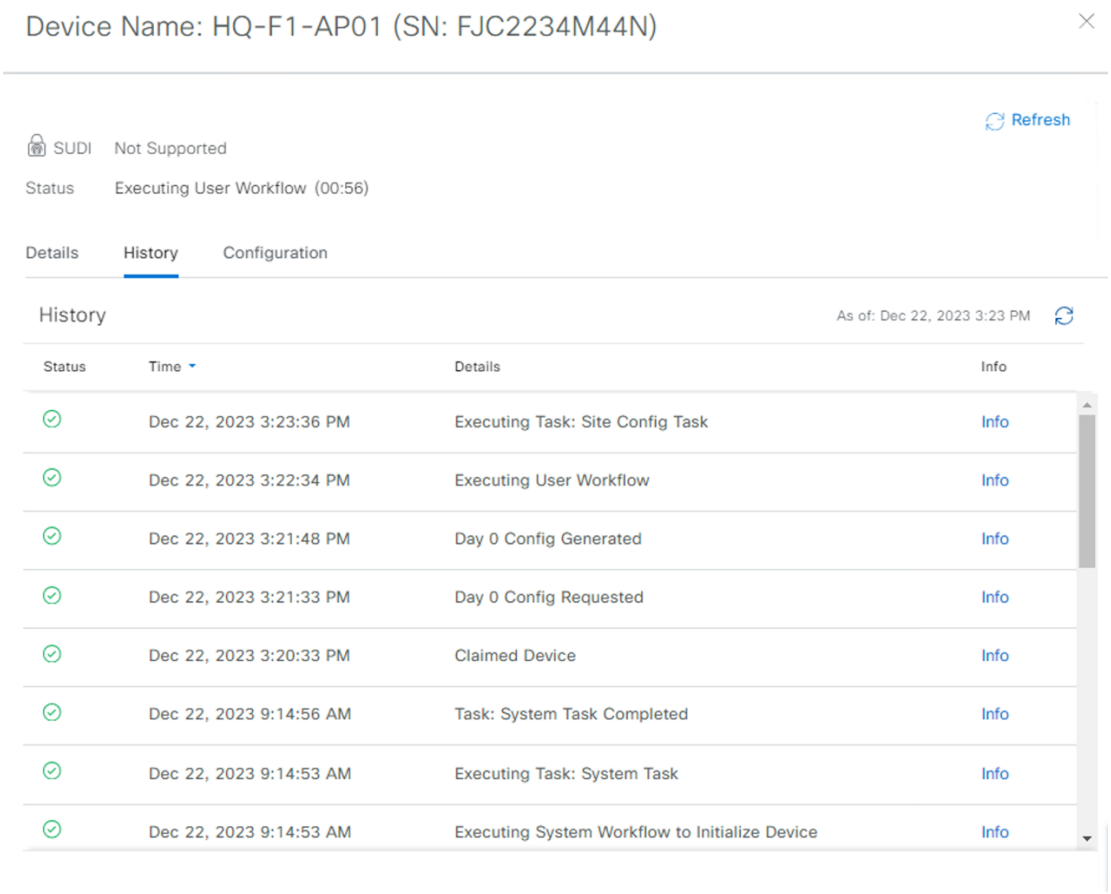
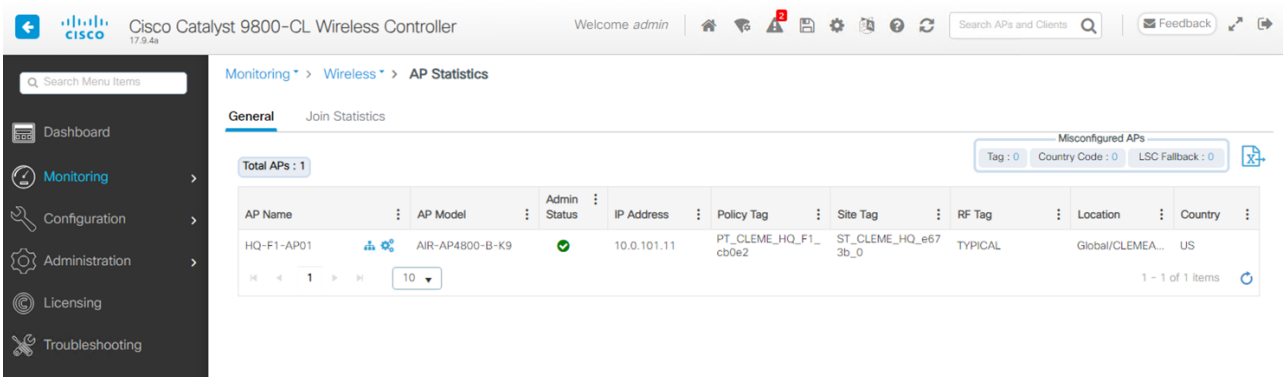


Figure 68 Plug and Play AP Claim

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



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.

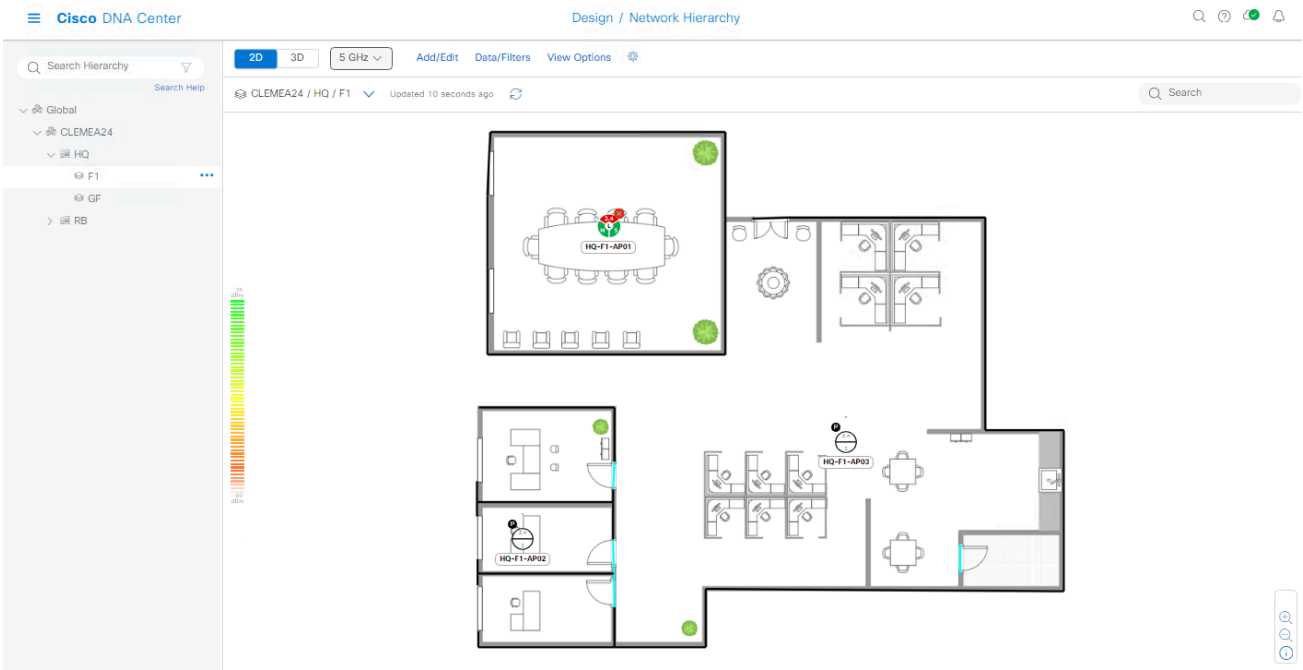
Snippet from WLC Config looks like:

```
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.**

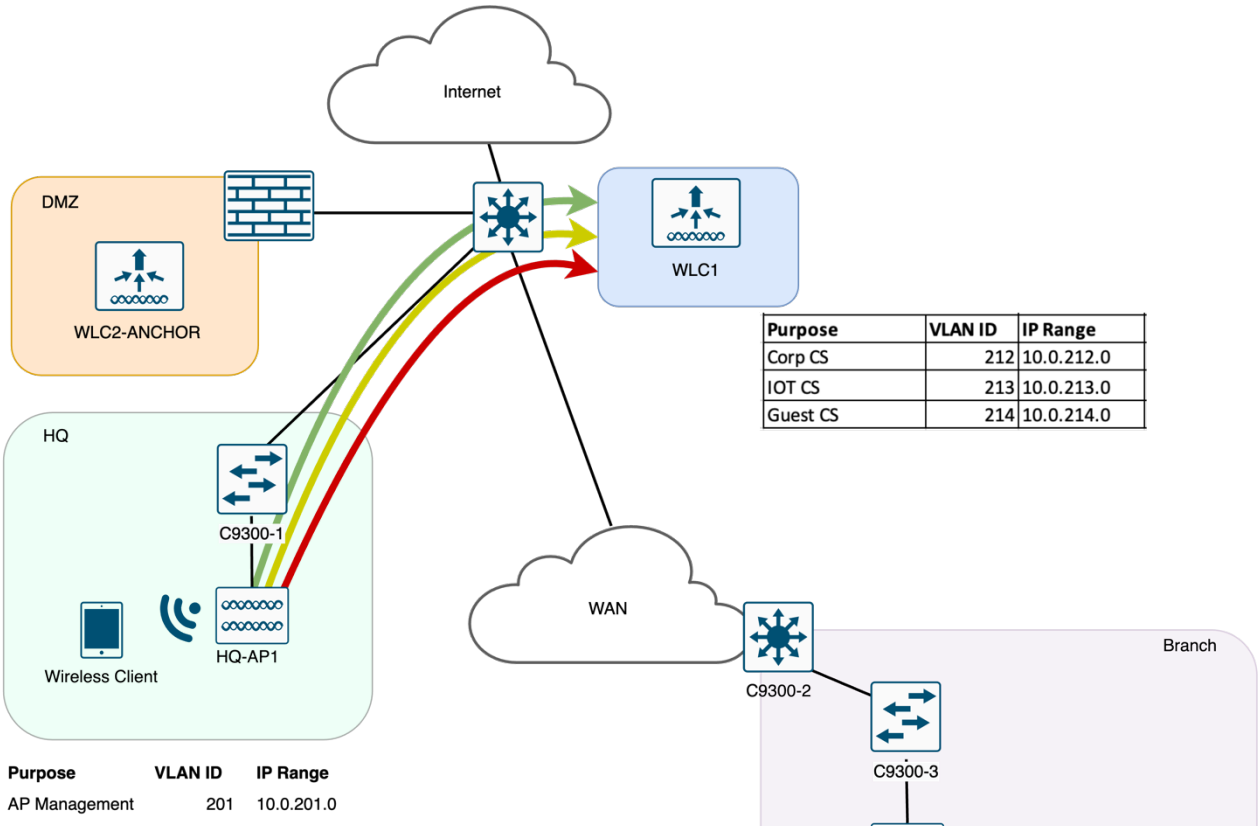
Figure 70 AP PnP - AP Placement



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



Purpose	VLAN ID	IP Range
Corp CS	212	10.0.212.0
IOT CS	213	10.0.213.0
Guest CS	214	10.0.214.0

Purpose	VLAN ID	IP Range
AP Management	201	10.0.201.0

Purpose	VLAN ID	IP Range
AP Management	101	10.0.101.0
Corp LS	102	10.0.102.0
IOT LS	103	10.0.103.0

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.

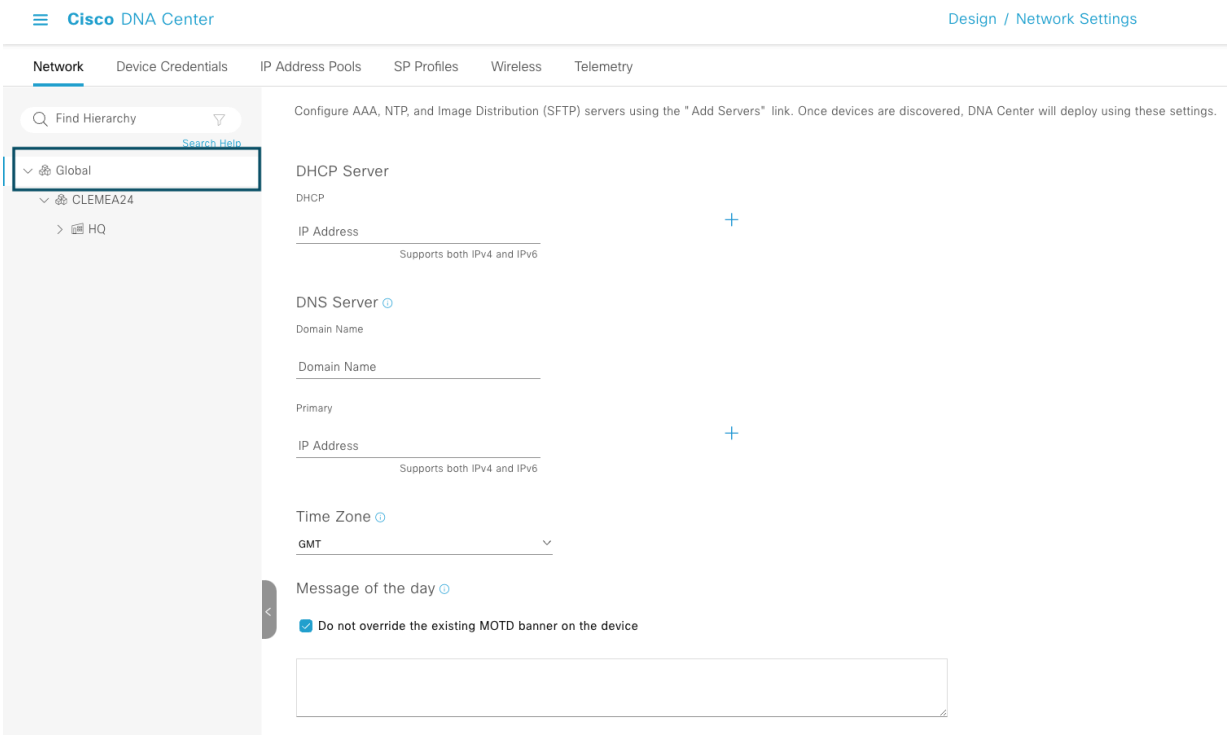
First we go with **Global Network Settings**:

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:

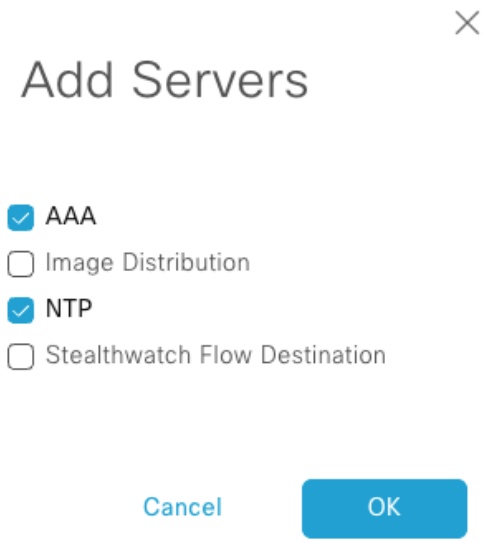
Figure 72 Network Settings - Hierarchy



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

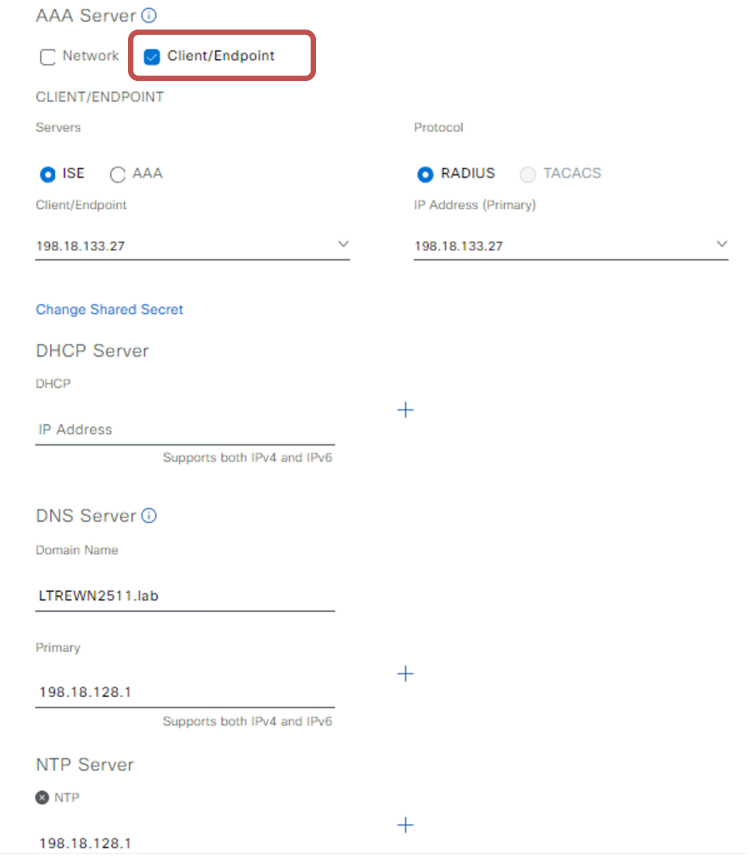


Once ready, let us fill the values for the network settings as per the below table:

Table 8 Network Settings - General

Parameter		Value
AAA Server	[✓] Client/Endpoint	[✓] ISE [✓] RADIUS
AAA Server	IP Address	198.18.133.27
DHCP Server	N/A	N/A
DNS Server	Domain Name	LTREWN2511.lab
DNS Server	IP Address	198.18.128.1
NTP Server	IP Address	198.18.128.1
Time Zone		America/Los_Angeles
Message of the Day		[✓] Do not override the existing MOTD banner on the device

Figure 74 Network Settings

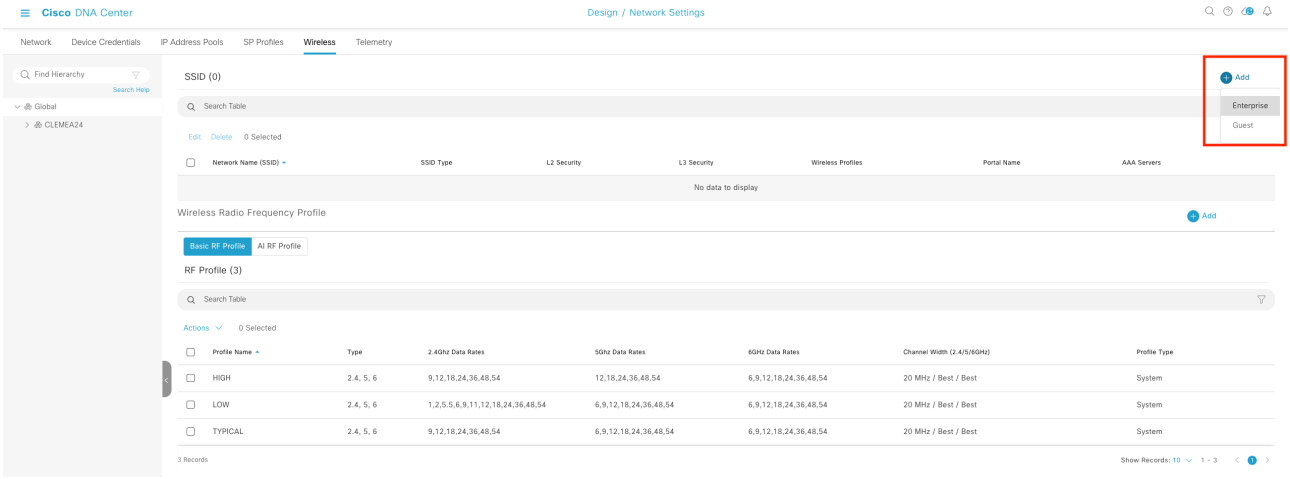


Step 2: Configure IOT SSID

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**

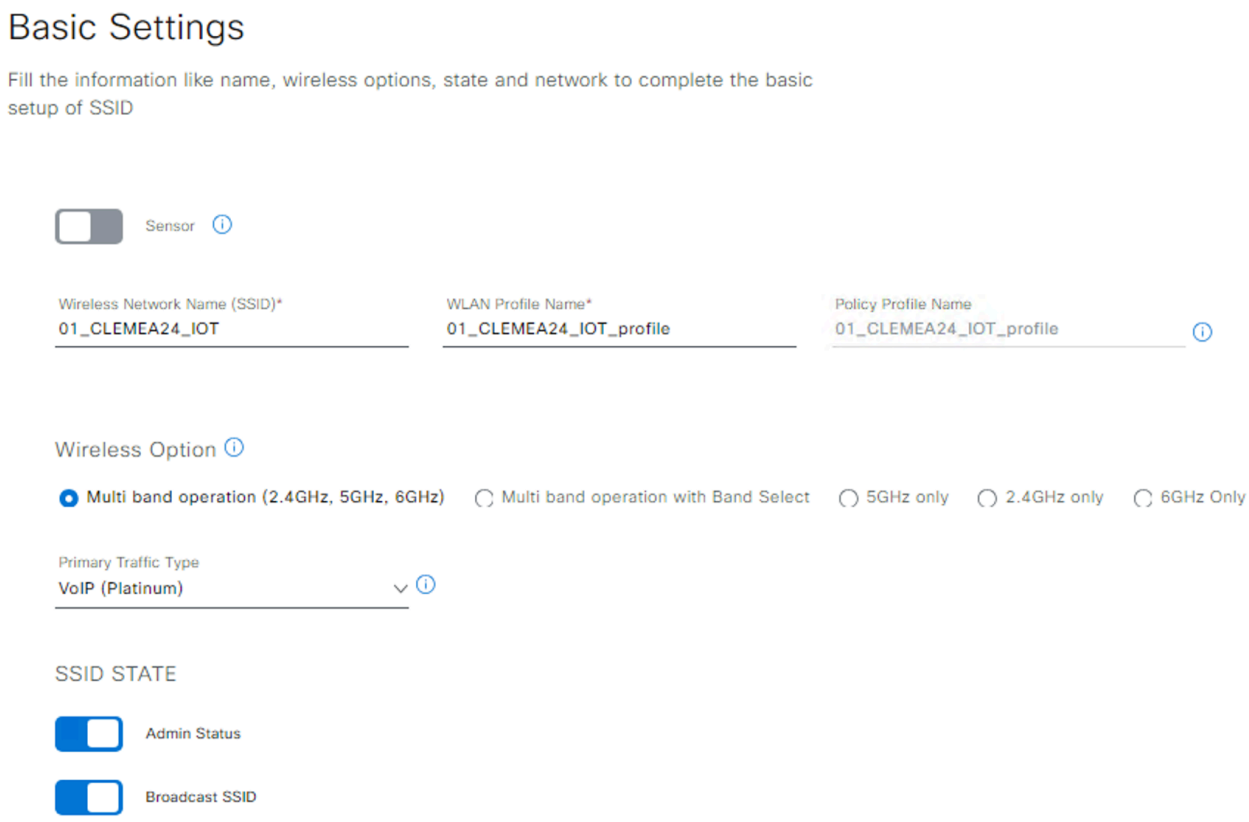
Figure 75 Wireless Settings - SSID



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

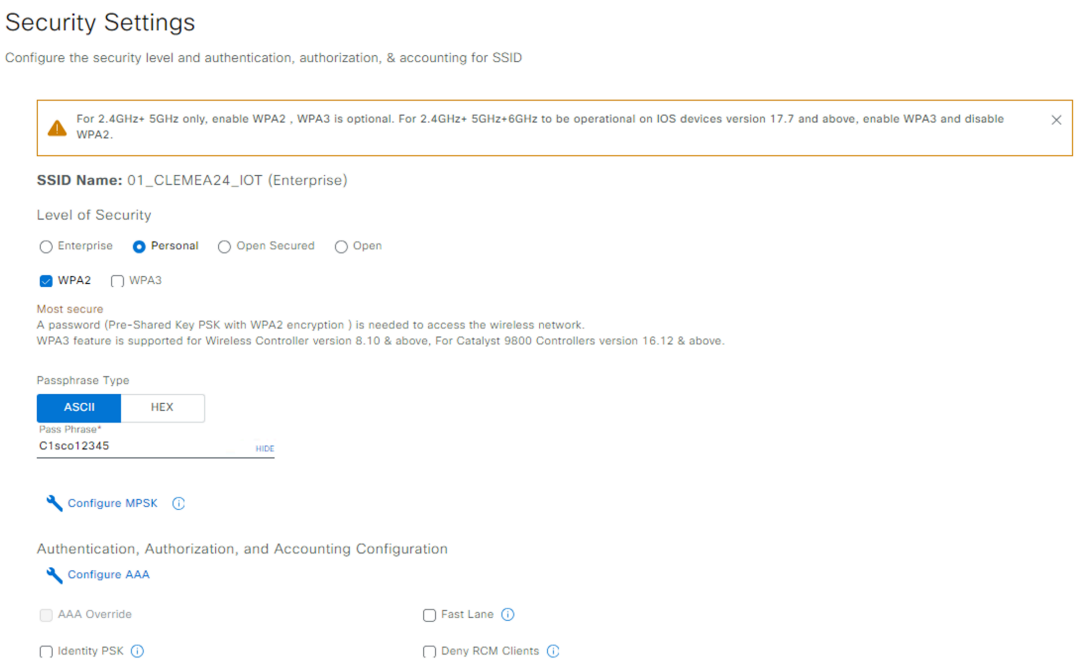
SSID will be named **XX_CLEMEA24_IOT** where XX corresponds to the POD number you are assigned to. See example below with pod 01.

Figure 76 SSID - IOT - Basic Settings



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

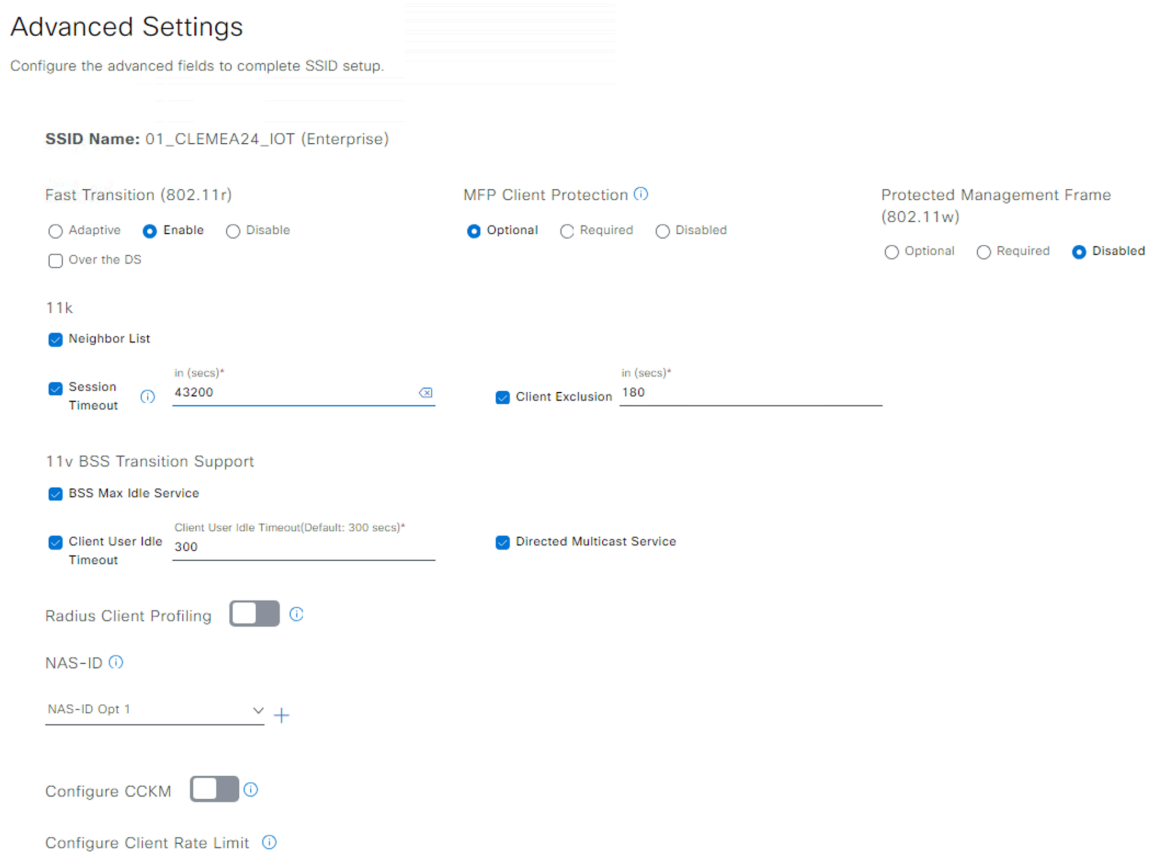
Figure 77 SSIDs - IOT - Security Settings



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

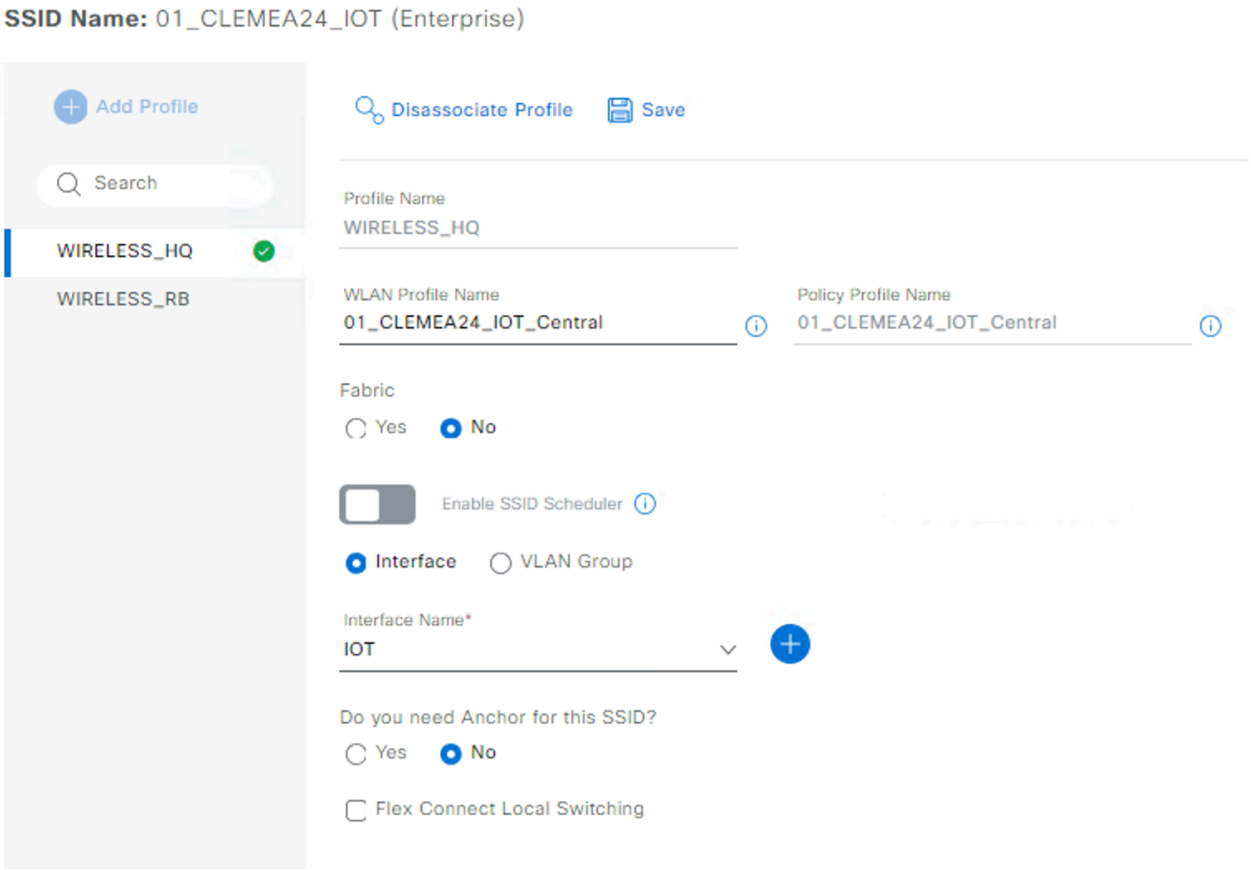


Click on **Next** to assign the SSID to the required Network Profiles.
All the SSIDs will be used in both HQ and Remote Branch, so we need to configure both network profiles.

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)



- 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,
  - **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 2nd 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

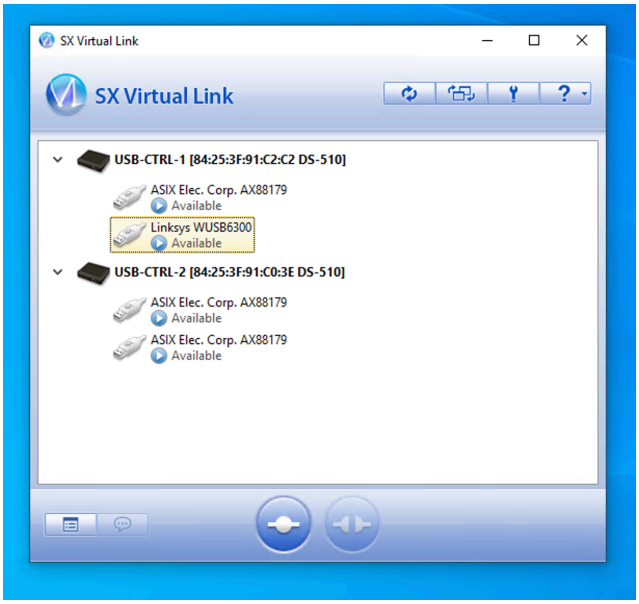
Open an RDP session to one of the Wireless Clients:

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.

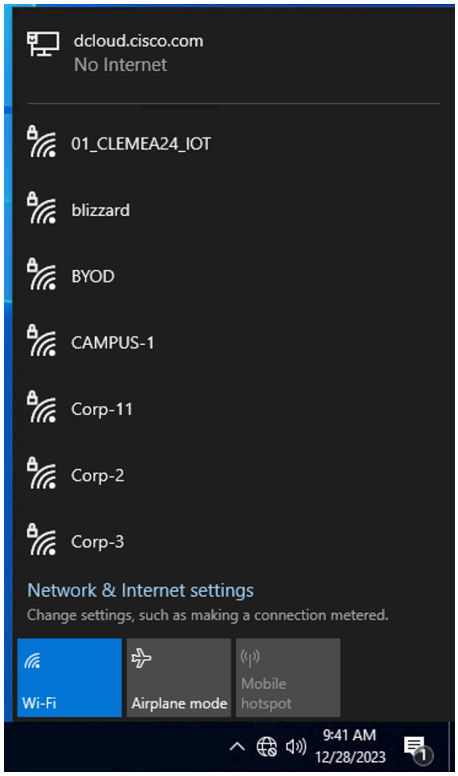
Figure 80 SX Virtual Link Adapter Configuration



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

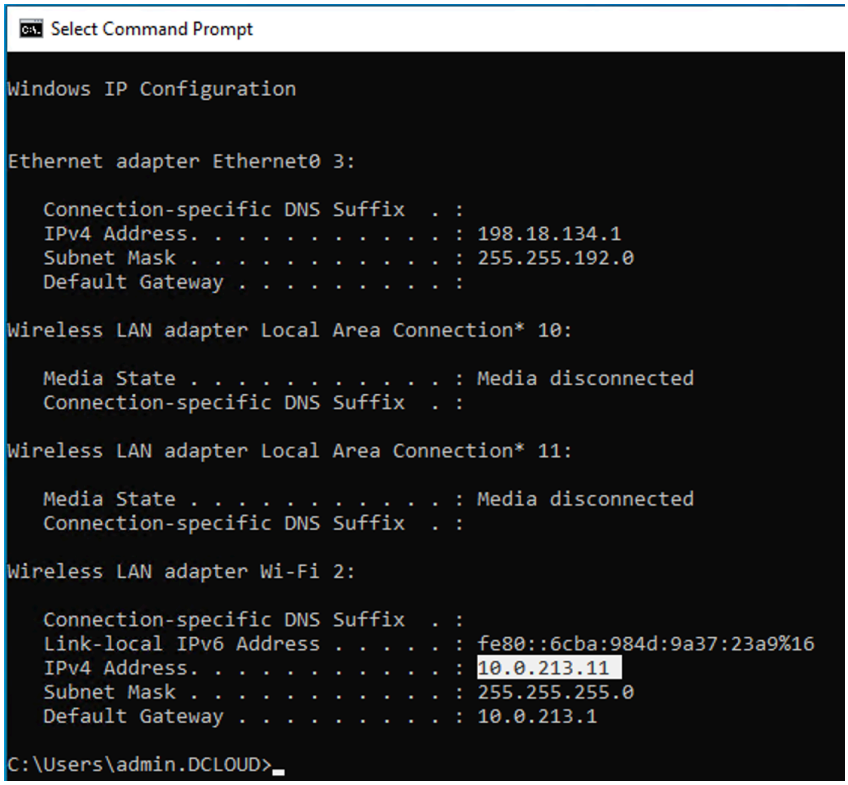
Disable the checkbox "**Connect Automatically**"

Figure 81 Connecting to WLAN



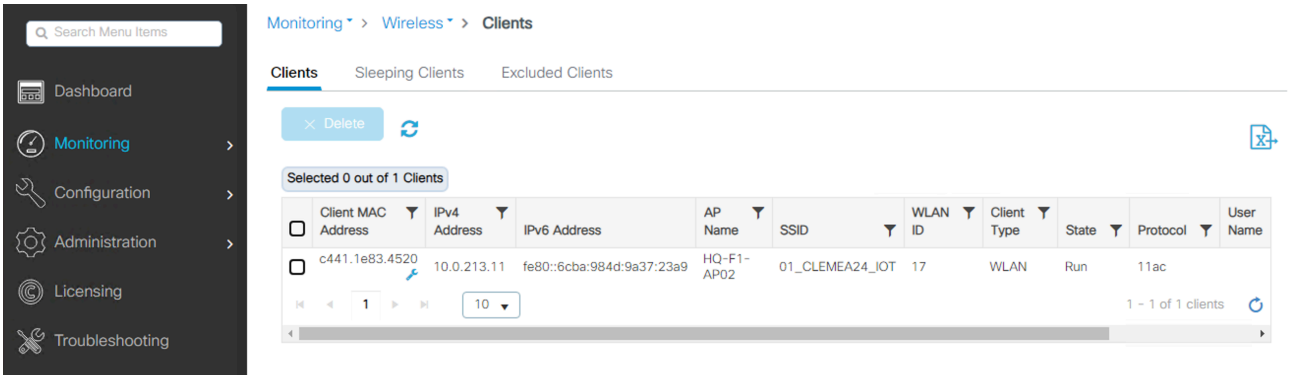
Verify using CMD if the wireless client gets an IP address from the desired VLAN.
The below example is for IOT at the HQ

Figure 82 Connecting to WLAN – Verify IP Address



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



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

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

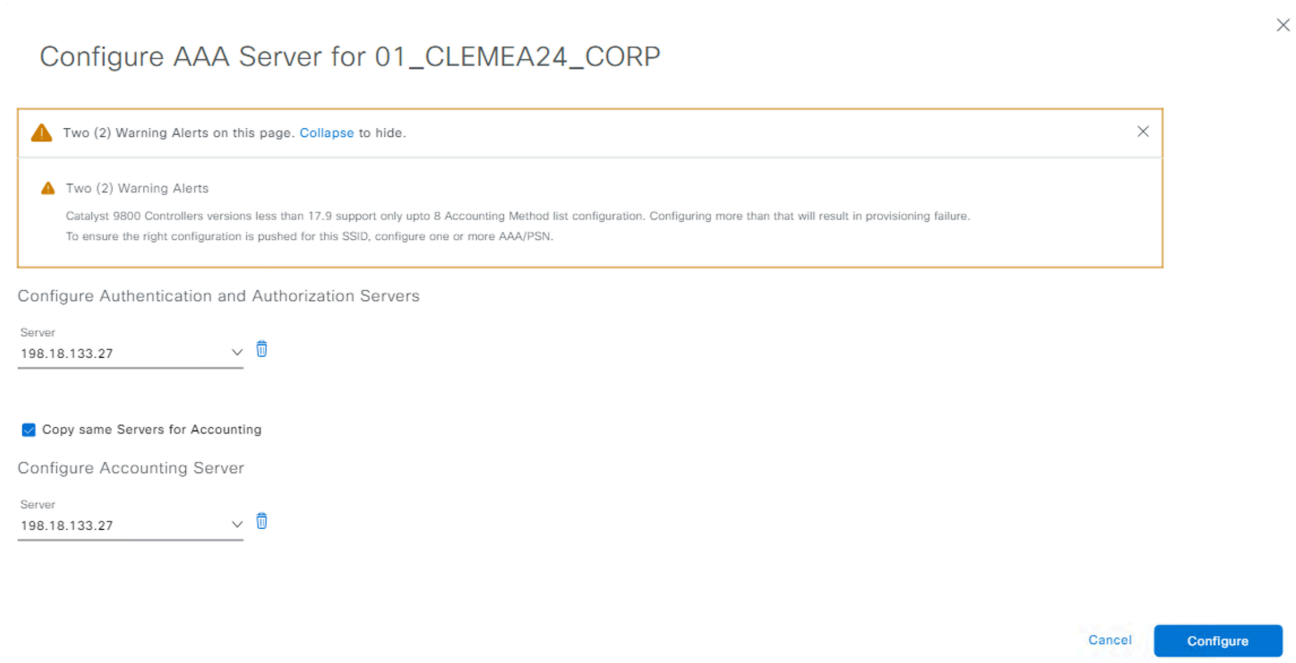
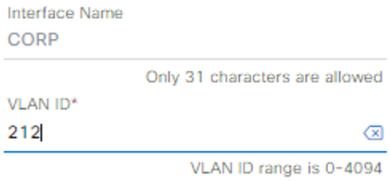


Table 11 Network Profile – Settings – CORP HQ

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

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



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	**XX_CLEMEA24_GUEST**
Wireless Option	Multi band operation (2.4GHz, 5GHz and 6GHz)
Type of Enterprise Network	**Best Effort (Silver)**
Level of Security	Open > Web Policy
Authentication Server (*See screenshot below*)	**CWA** > **Hotspot** > **Original URL**
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)

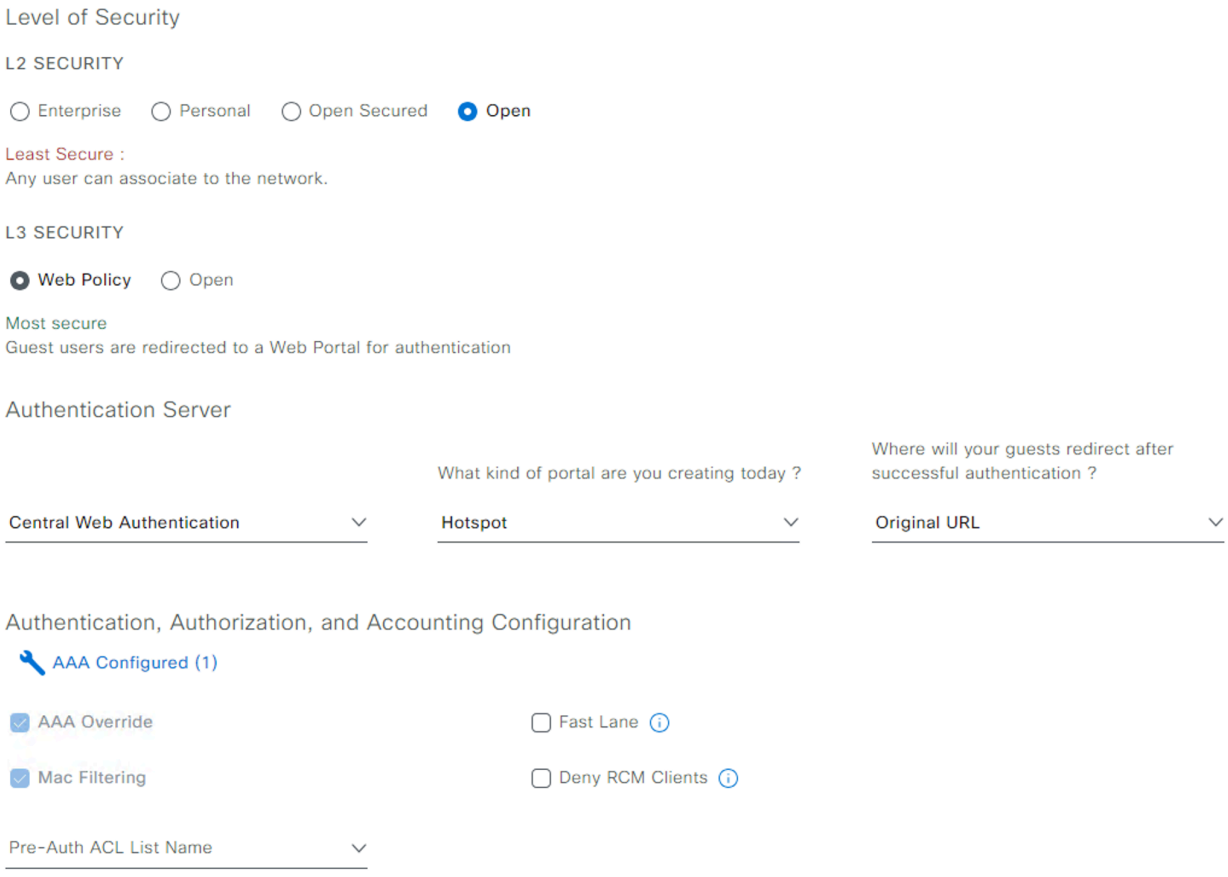


Table 13 Network Profile – Settings – GUEST HQ

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

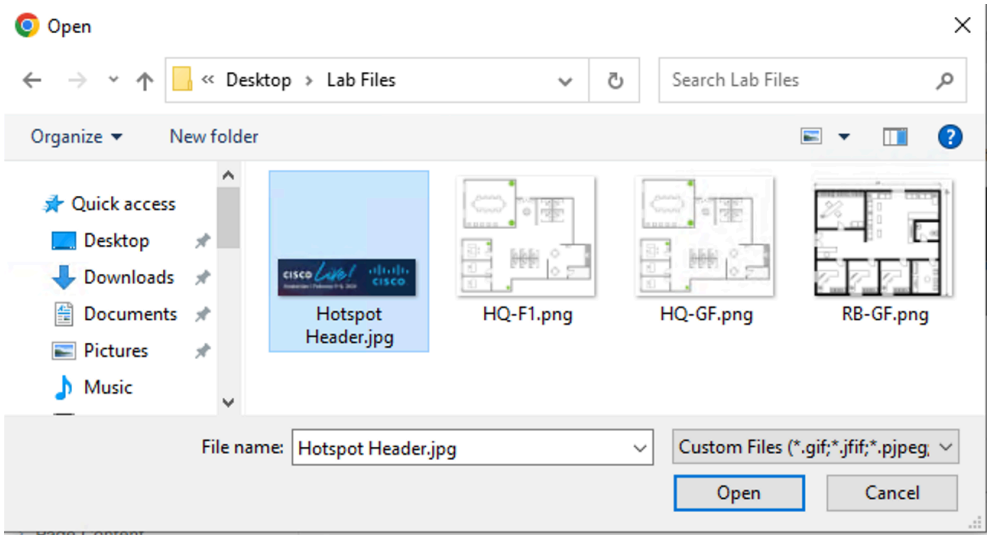
Click on **Associate Profile** for the changes to take effect then **Next.**

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)

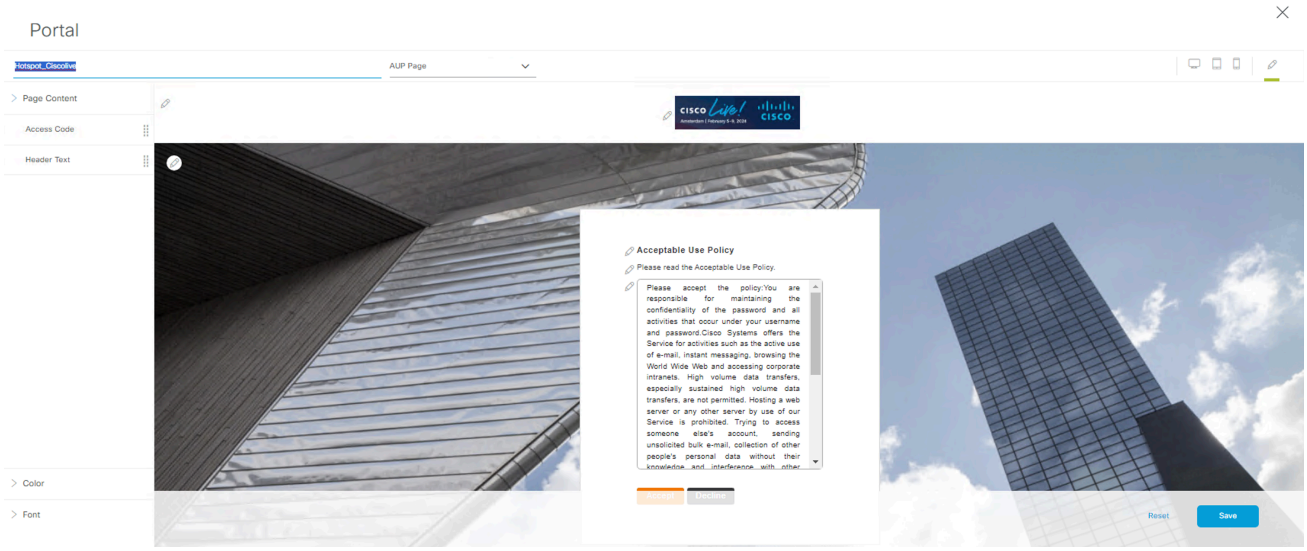
- Name the portal as “**Hotspot_Ciscolive**”
- Edit the Portal Header, use the file in the Desktop. Click in the **Pencil** next to the header logo, click **Upload** and select the new file.
- Then click **Save**

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

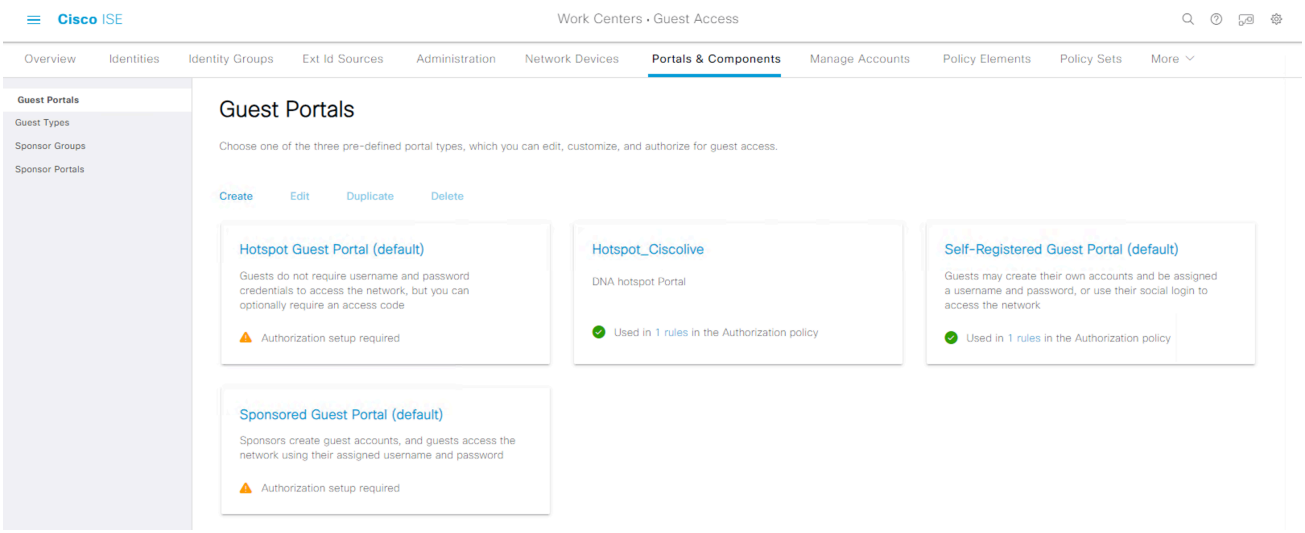


Figure 91 SSIDs - GUEST –ISE Authz Profiles

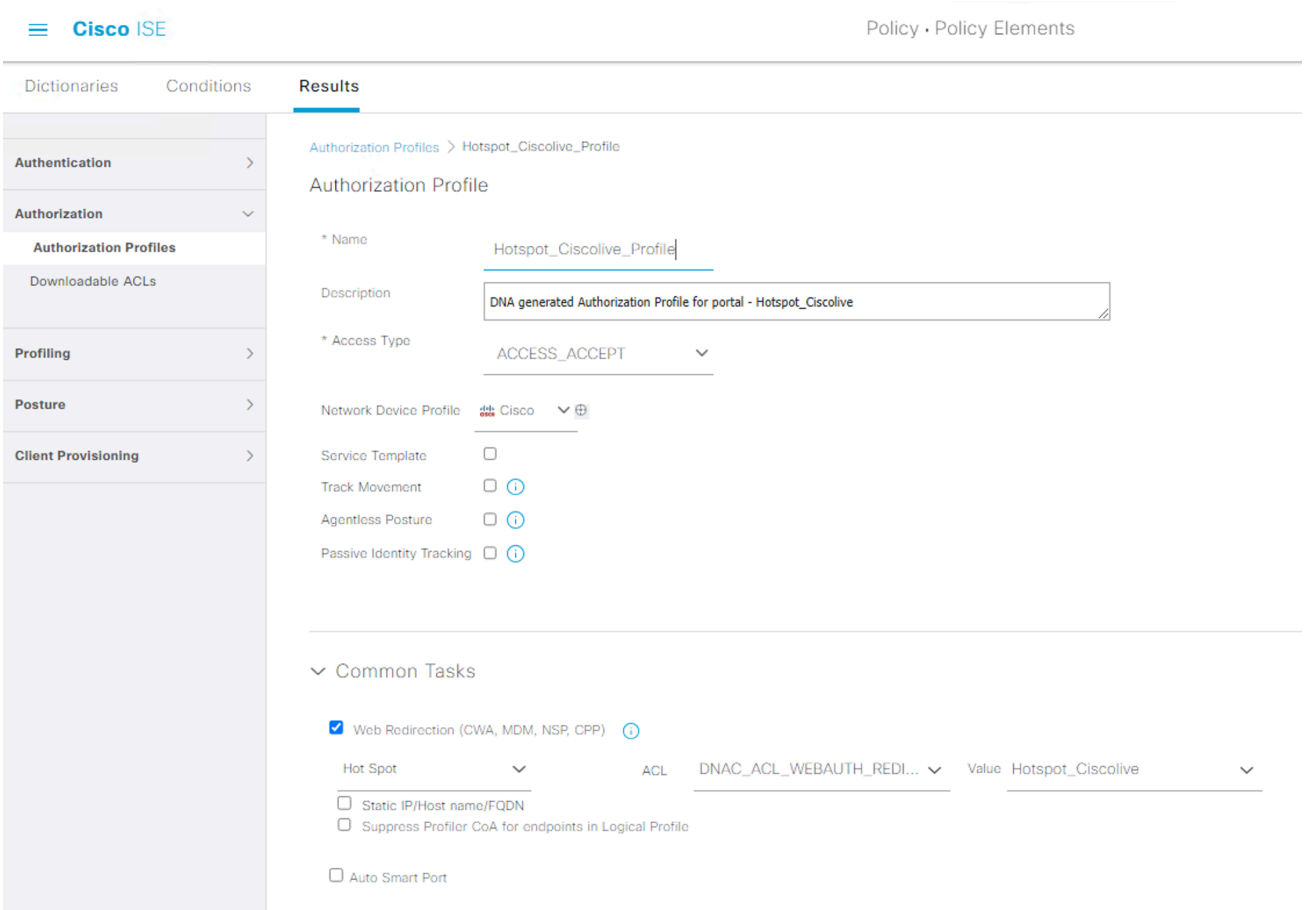
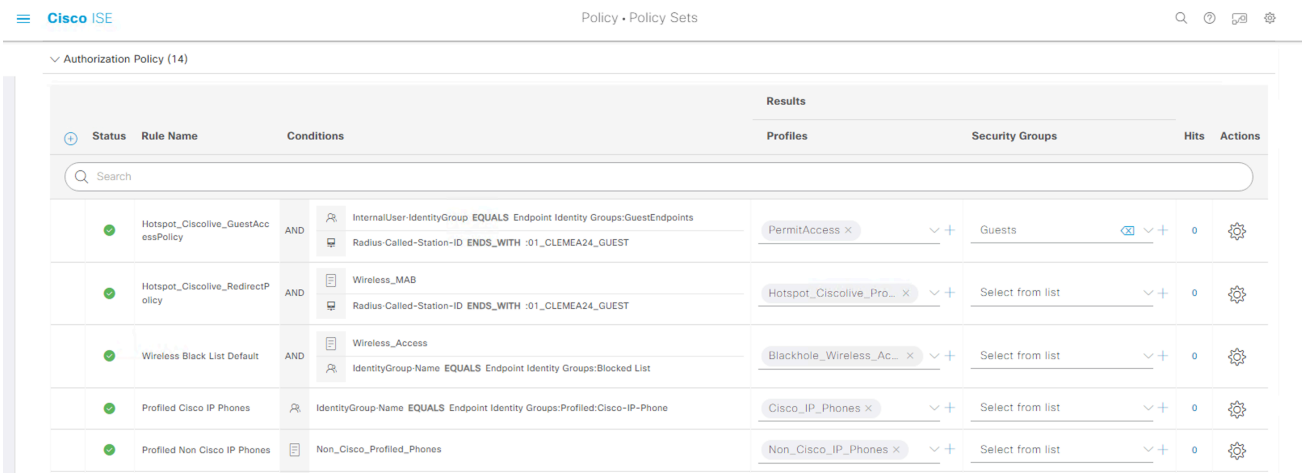
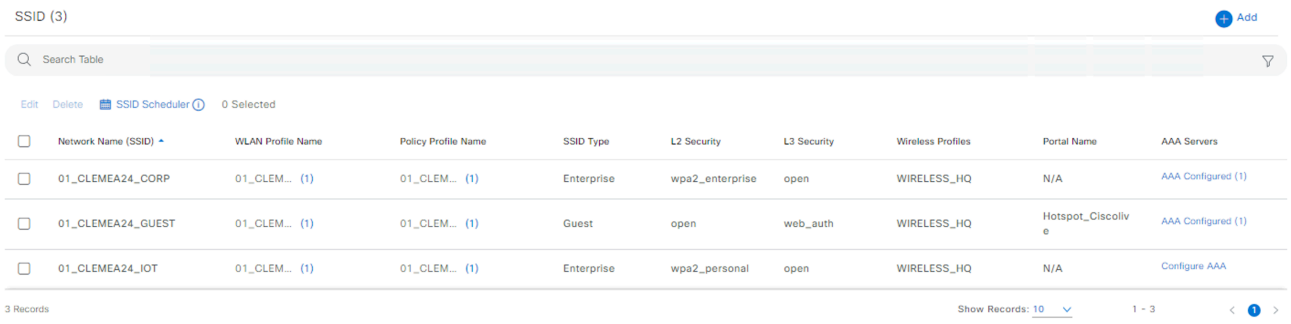


Figure 92 SSIDs - GUEST –ISE Policies



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

Figure 93 SSIDs - Summary

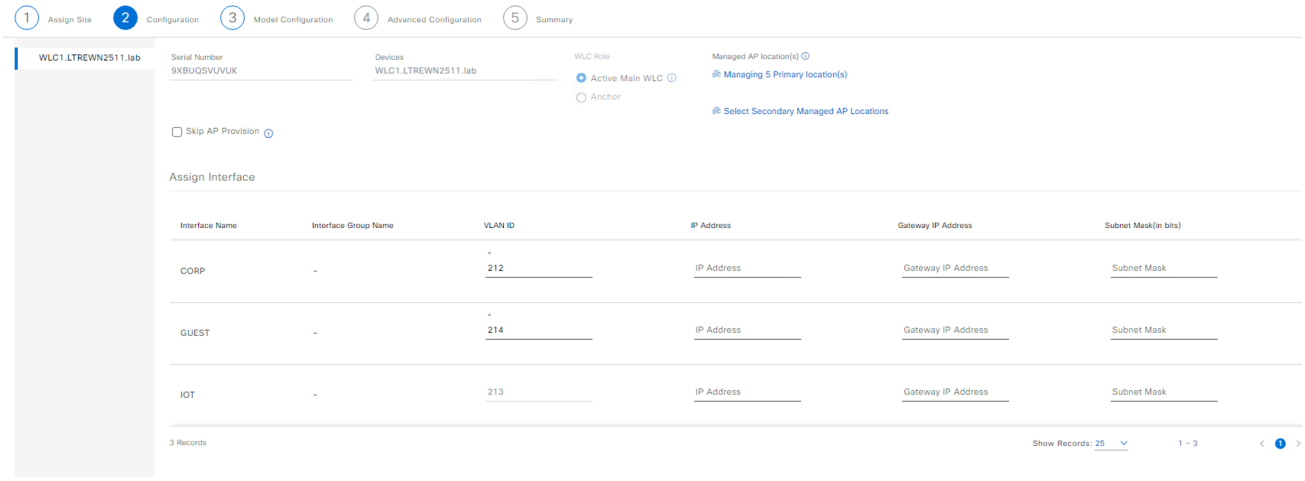


Step 7: Provision CORP and Guest Configuration to WLC

- 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,
  - **CORP** should be VLAN ID: **212**
  - **GUEST** should be VLAN ID: **214**

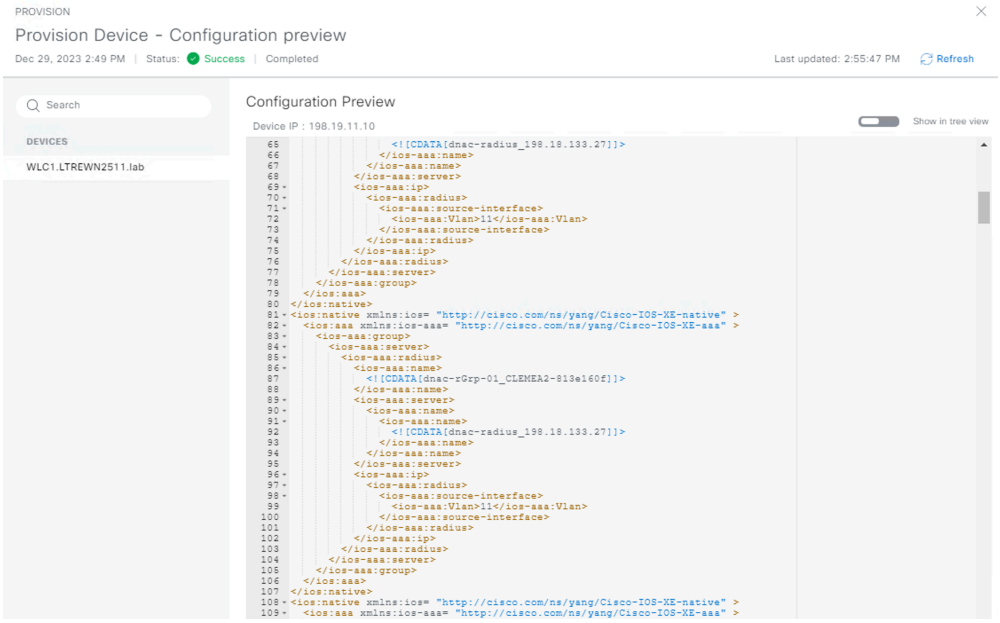
Figure 94 Provision CORP and GUEST to WLC



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

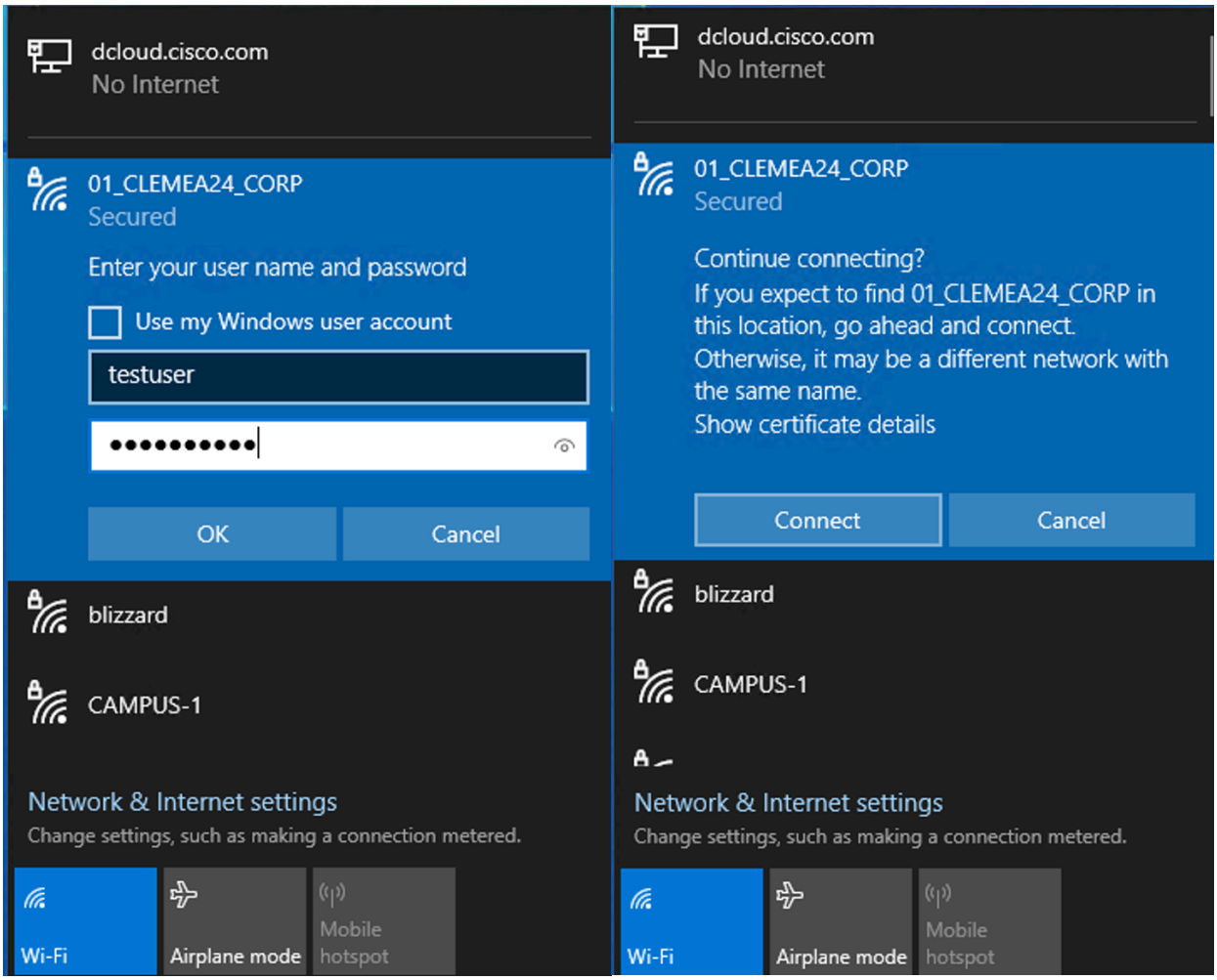
Name	IP Address	Username	Password	Preferred Access Method

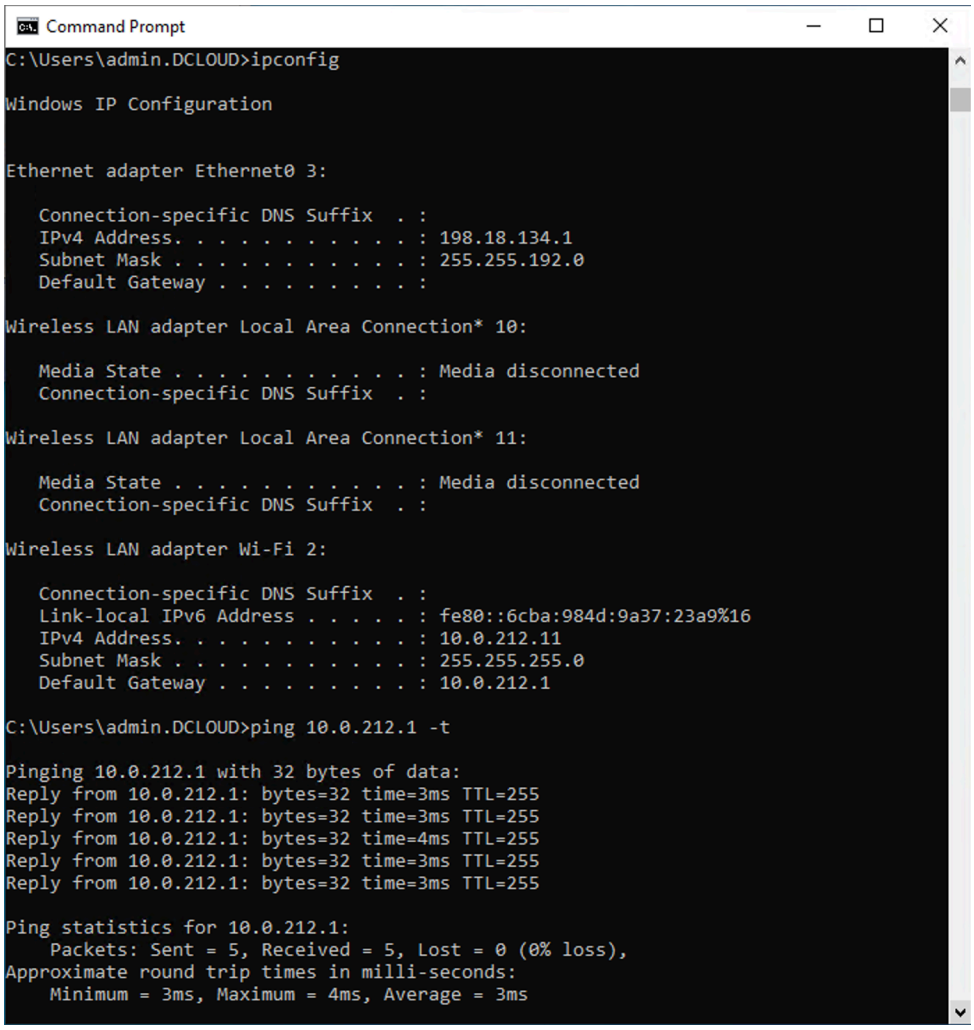
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP
Client4	198.18.134.4	DCLOUD\admin	C1sco12345	RDP

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

Username: testuser

Password: C1sco12345

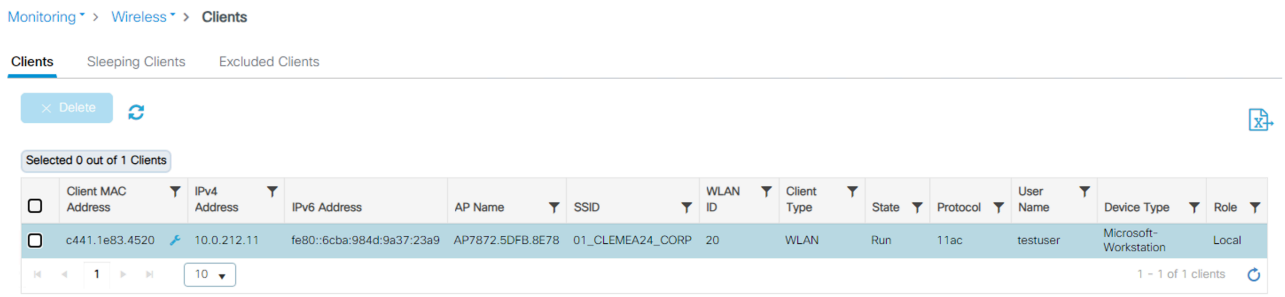




ISE Radius Live Logs show authentication successful.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...
				Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	Network Devic
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



Step 9: Testing GUEST SSID

Open an RDP session to one of the Wireless Clients:

Table 15 Wireless Clients Addressing and Credentials

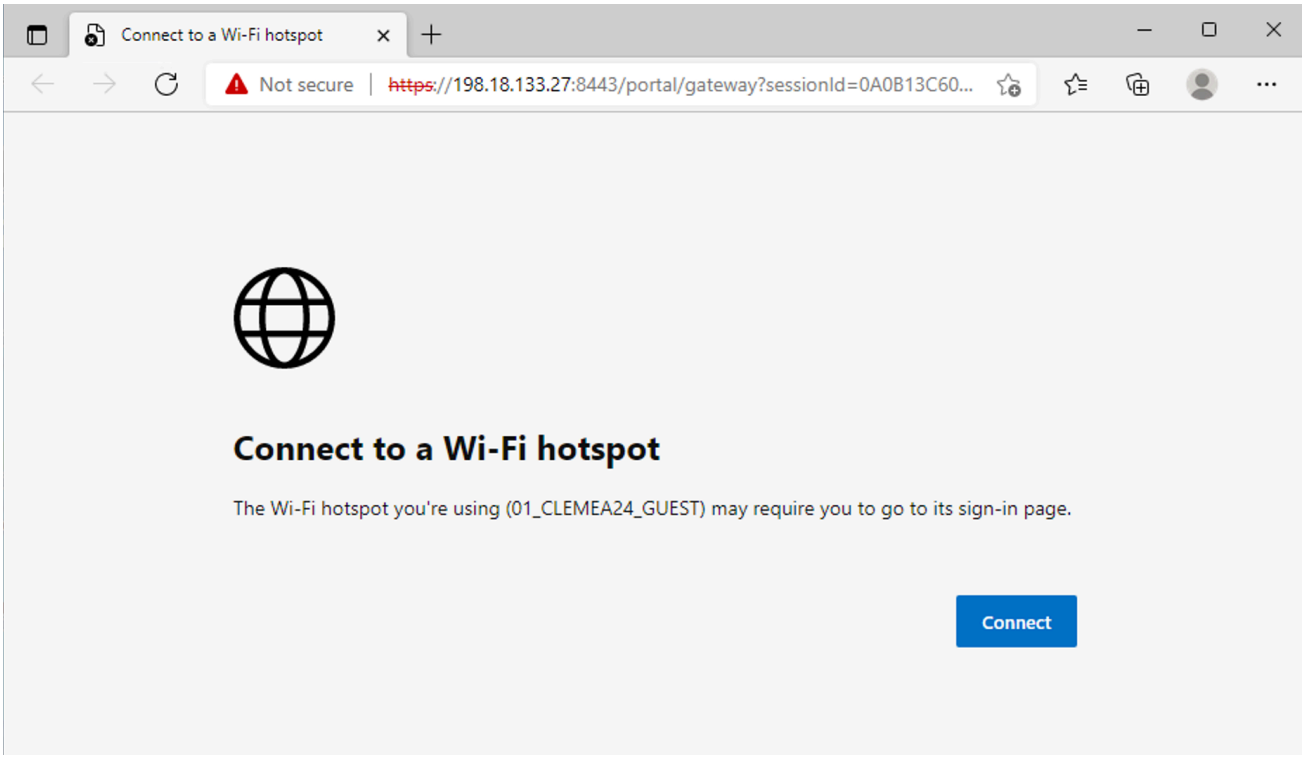
Name	IP Address	Username	Password	Preferred Access Method
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP
Client4	198.18.134.4	DCLOUD\admin	C1sco12345	RDP

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

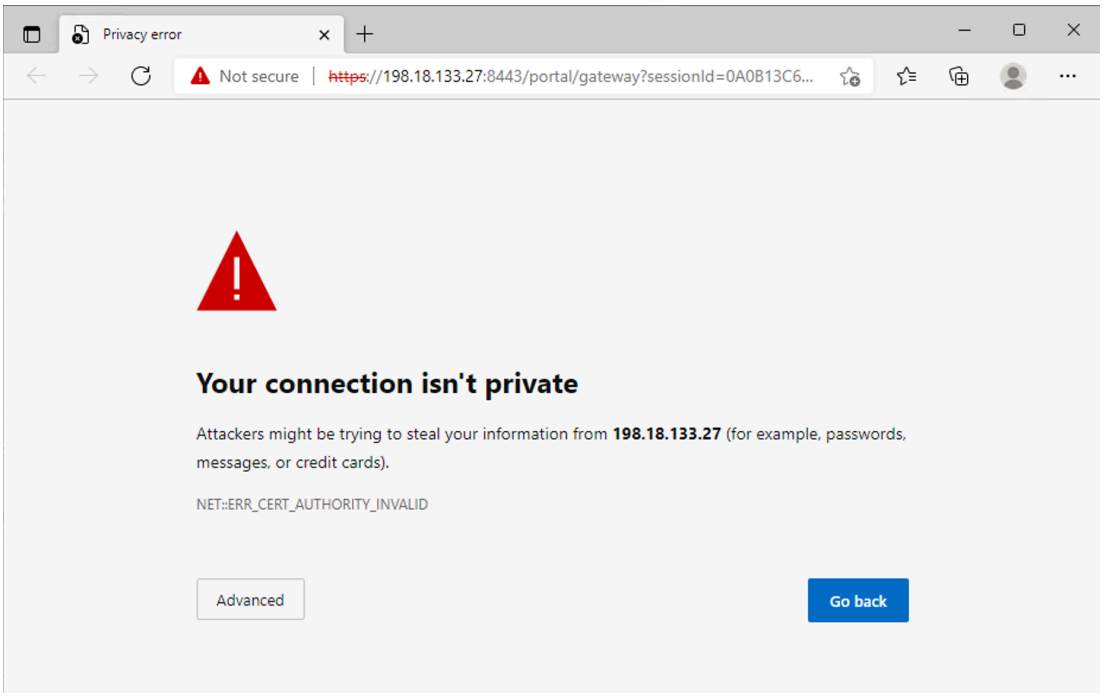
In case you get a page like the one below do the following steps:

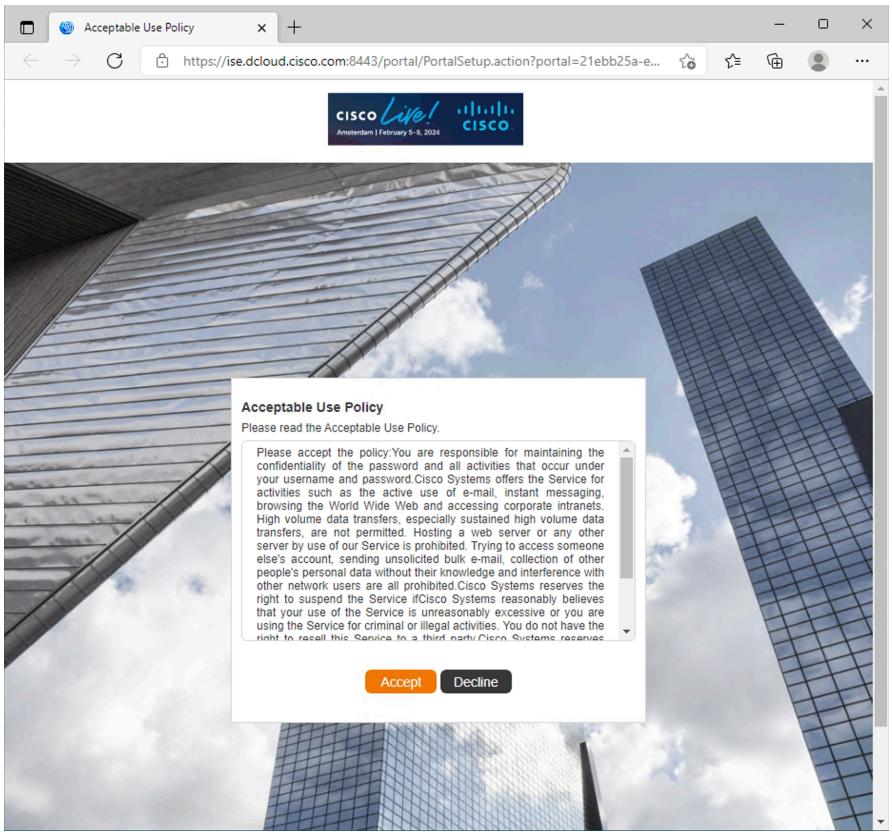
1. Click in the page,
2. type “thisisunsafe” (even if it’s not showing anywhere)
3. hit ENTER,
4. then reload page

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



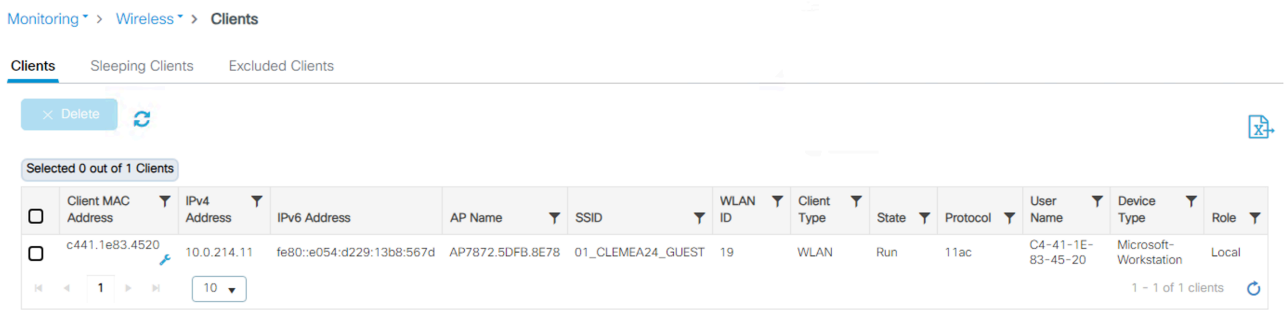
- Click advanced and proceed to the captive portal





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
```



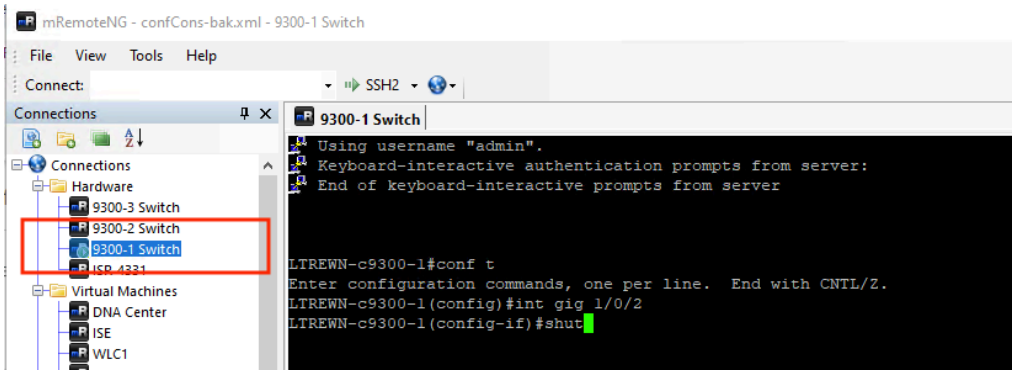
Step 10: Disabling HQ AP

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
```

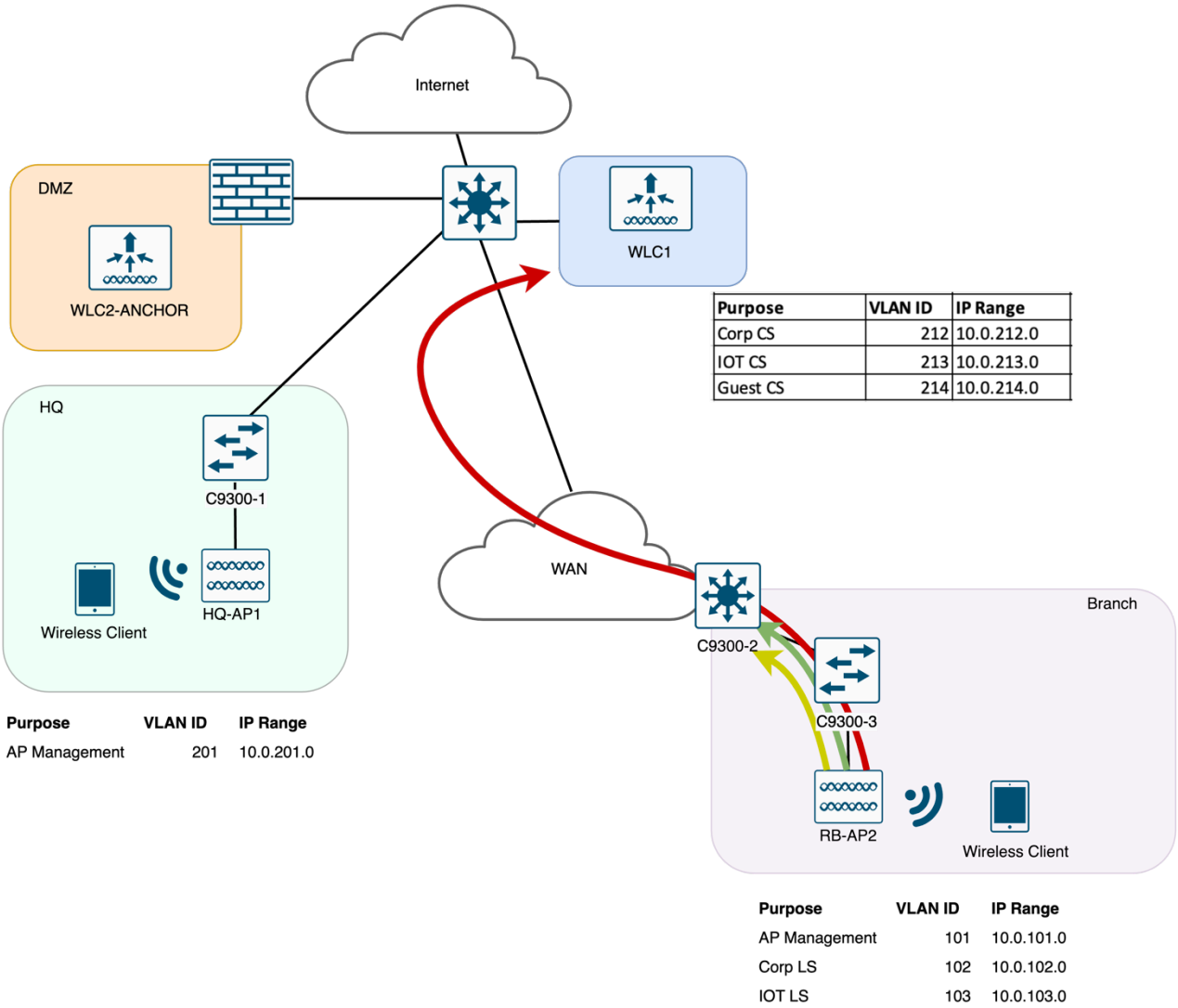
Figure 96 mRemoteNG - 9300-1



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



Purpose	VLAN ID	IP Range
Corp CS	212	10.0.212.0
IOT CS	213	10.0.213.0
Guest CS	214	10.0.214.0

Purpose	VLAN ID	IP Range
AP Management	201	10.0.201.0

Purpose	VLAN ID	IP Range
AP Management	101	10.0.101.0
Corp LS	102	10.0.102.0
IOT LS	103	10.0.103.0

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:

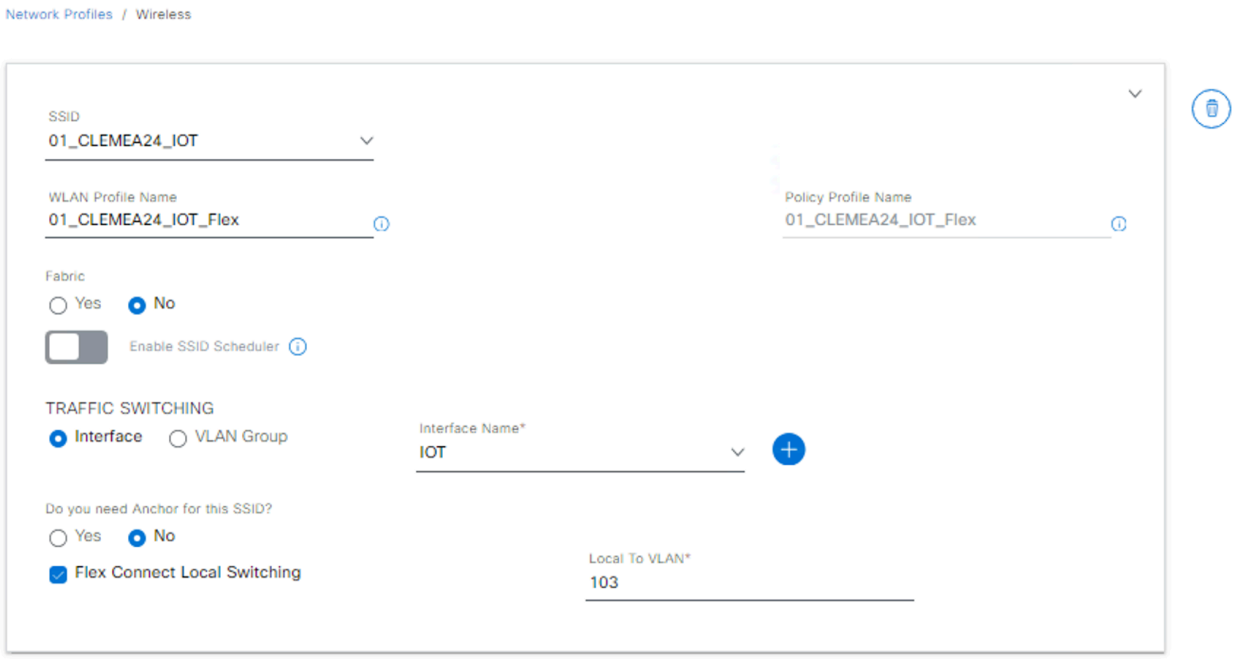
- click on **Design > Network Profile > WIRELESS_RB > Edit.**
- in the SSIDs tab, click **Add SSID,** one SSID will appear.
- Click the **+** to add all the SSIDs (scroll down to confirm all are there).

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:	**IOT**
Anchor	No
FlexConnect Local Switching	**Yes**
Local to VLAN	**103**

Figure 98 FlexConnect Wireless Architecture



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:	**CORP**
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
Interface Name: (Create if non existing)	**GUEST**
Anchor	No
FlexConnect Local Switching	**No**

- 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

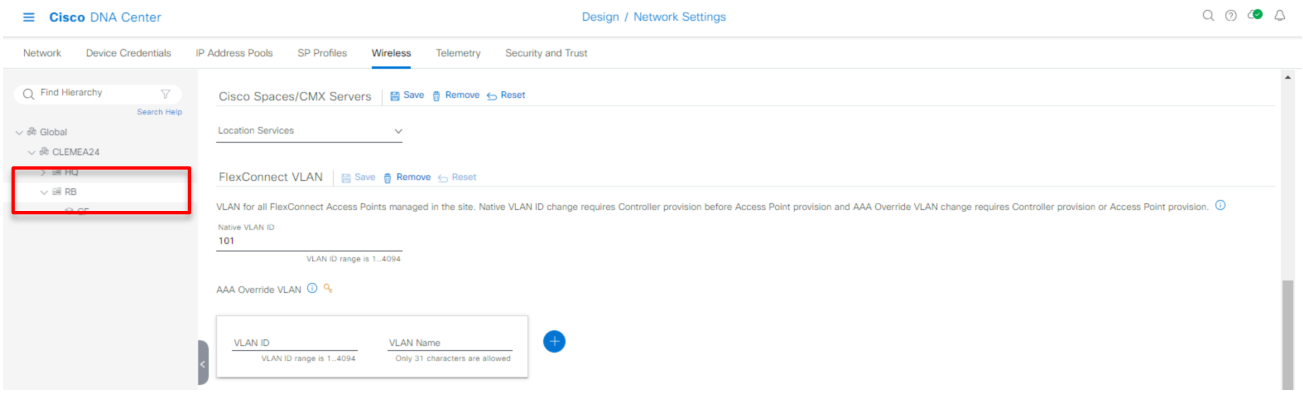
- **Design > Network Settings > Wireless**
- In the hierarchy, **Click** in **RB** Building

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

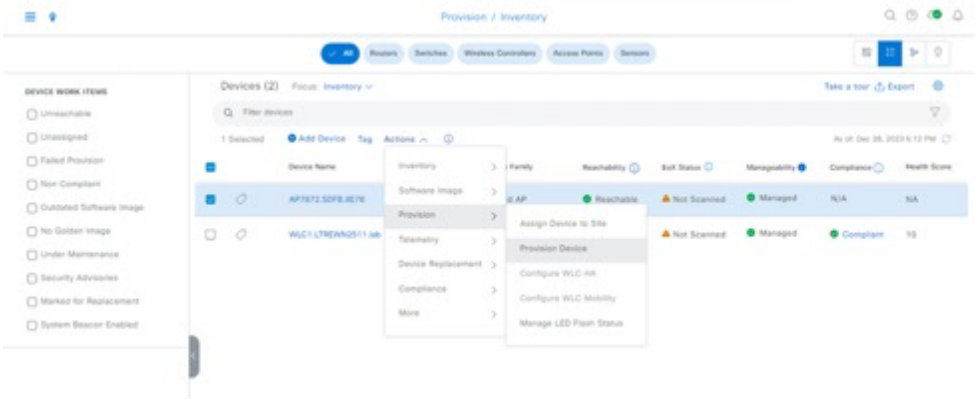


Figure 101 Provision AP with Flex IOT

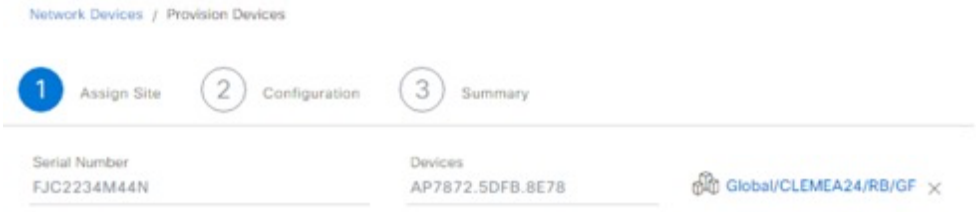
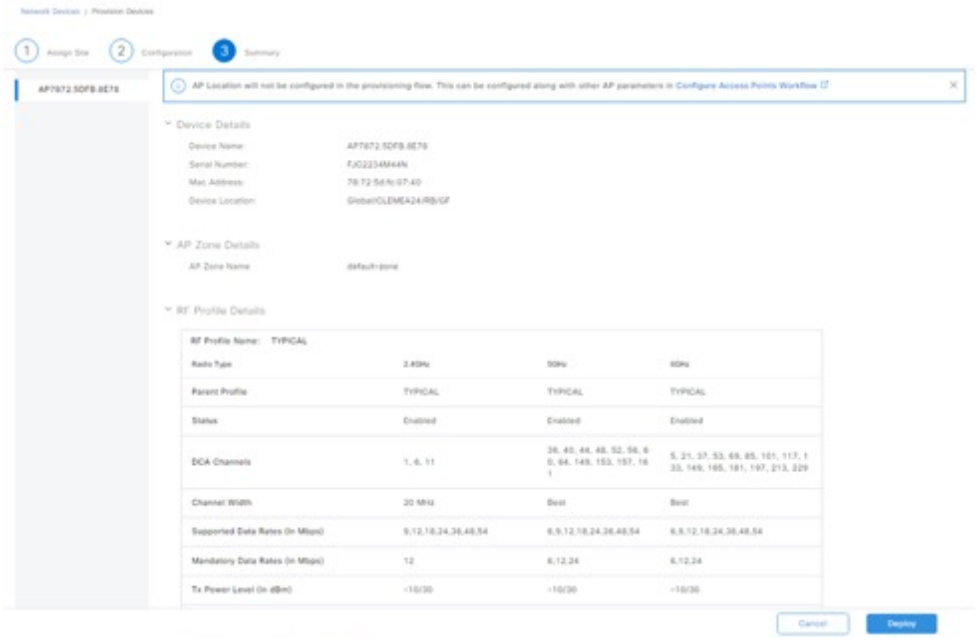


Figure 102 Provision AP with Flex IOT

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 bet an IP address of VLAN 103, range 10.0.103.x

Figure 104 Testing wireless client to Flex IOT

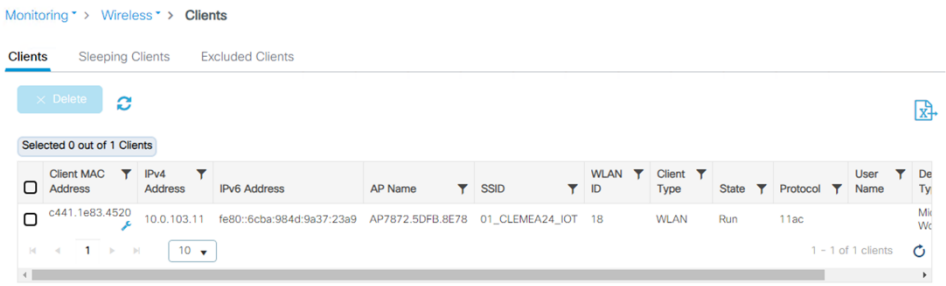
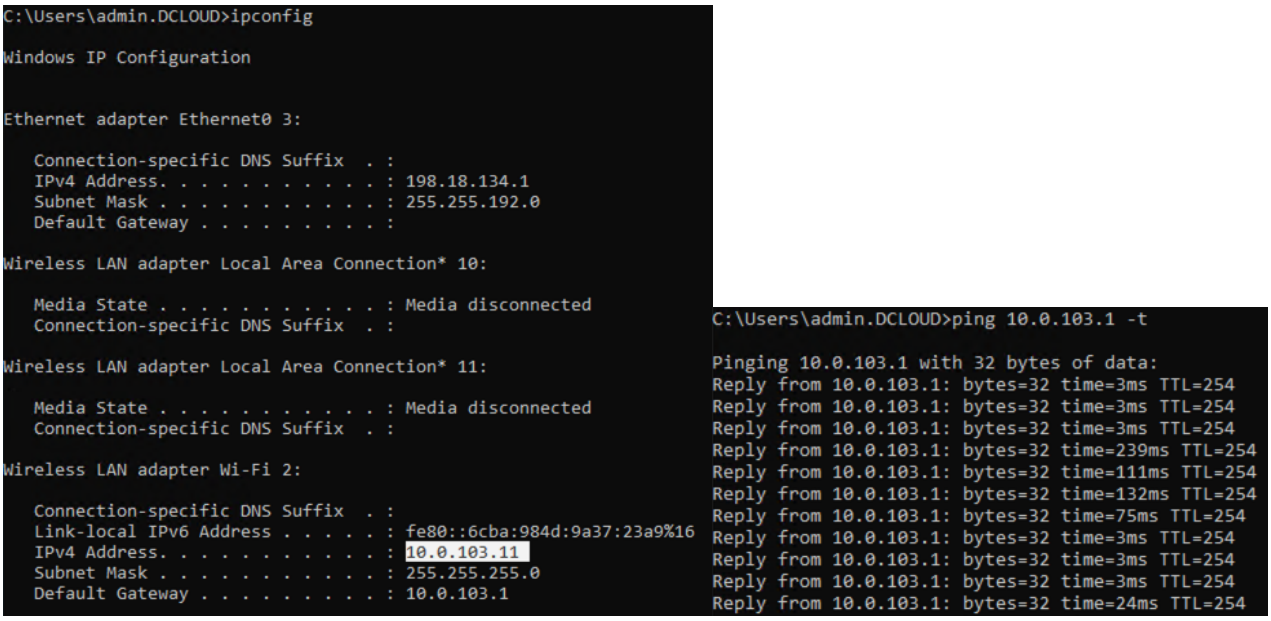


Figure 105 Testing wireless client to Flex IOT



Step 5: Testing CORP Flex SSID

Use the following credentials:

Username: testuser

Password: C1sco12345

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

Figure 106 Testing wireless client to Flex CORP

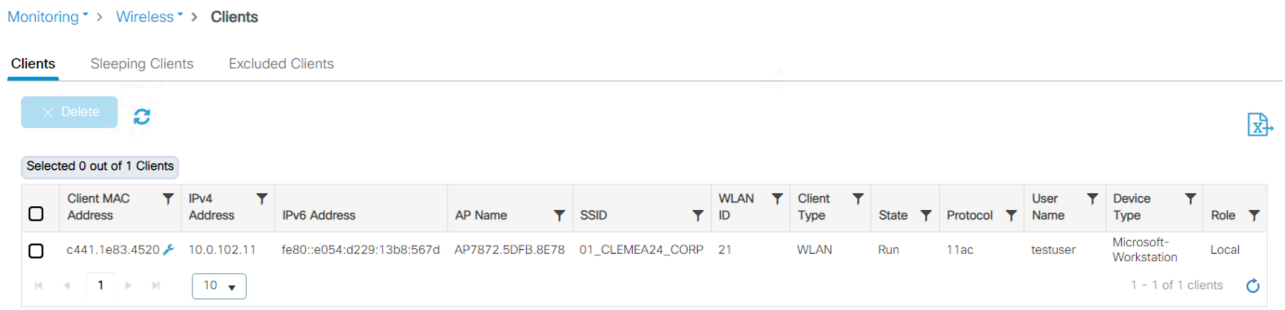


Figure 107 Testing wireless client to Flex CORP

```
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.

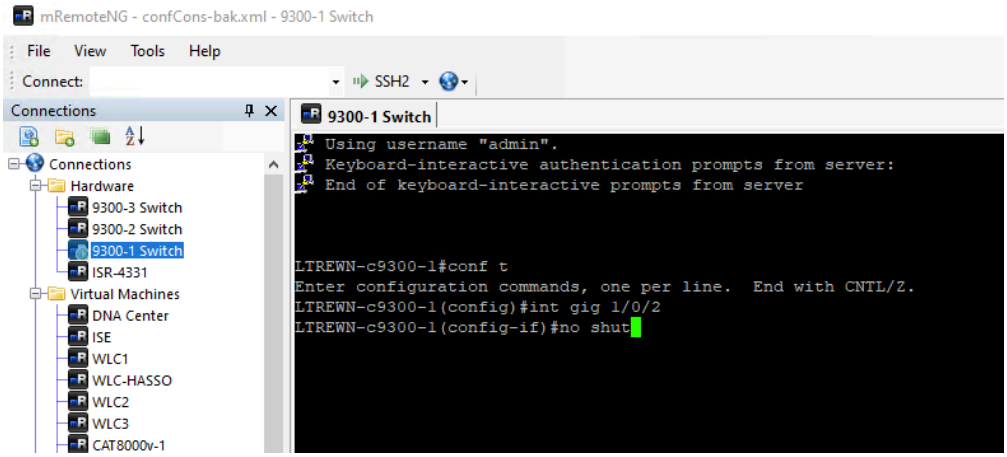
Step 7: Enabling HQ AP

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.

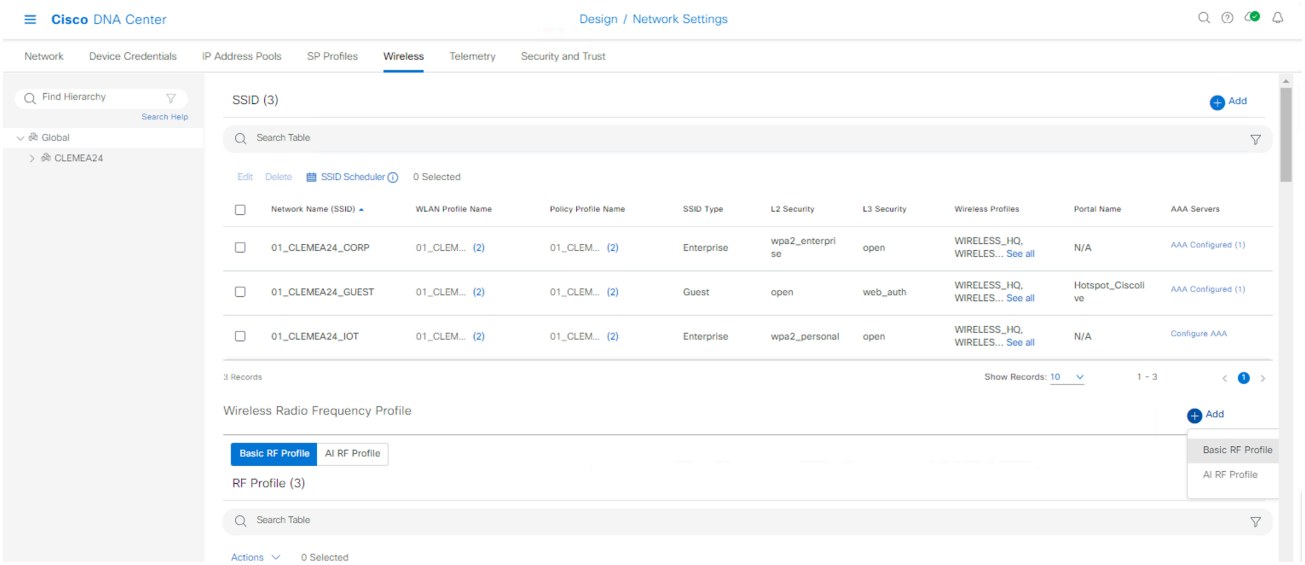
The configuration achieved in this section satisfies the custom requirements outlined at the beginning of the lab. The list below presents the details of the required configurations:

- *"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
Parent Profile	Custom	Default
DCA Channels	1,6,11	Default
Enable 802.11b data rates	Enabled	N/A
Supported Data Rates	6 Mbps and above	Default
Mandatory Data Rates	11	Default
Tx Power	10 to 30	Default

Figure 110 RF Profile - WAREHOUSE

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 **Medium** (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)
Supported Data Rates		12 Mbps and above
Mandatory Data Rates		24 Mbps
Tx Power		-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

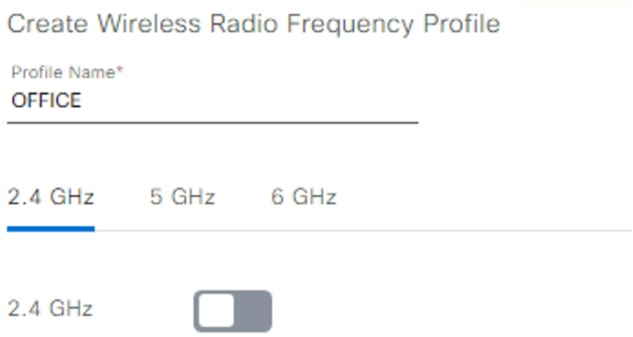
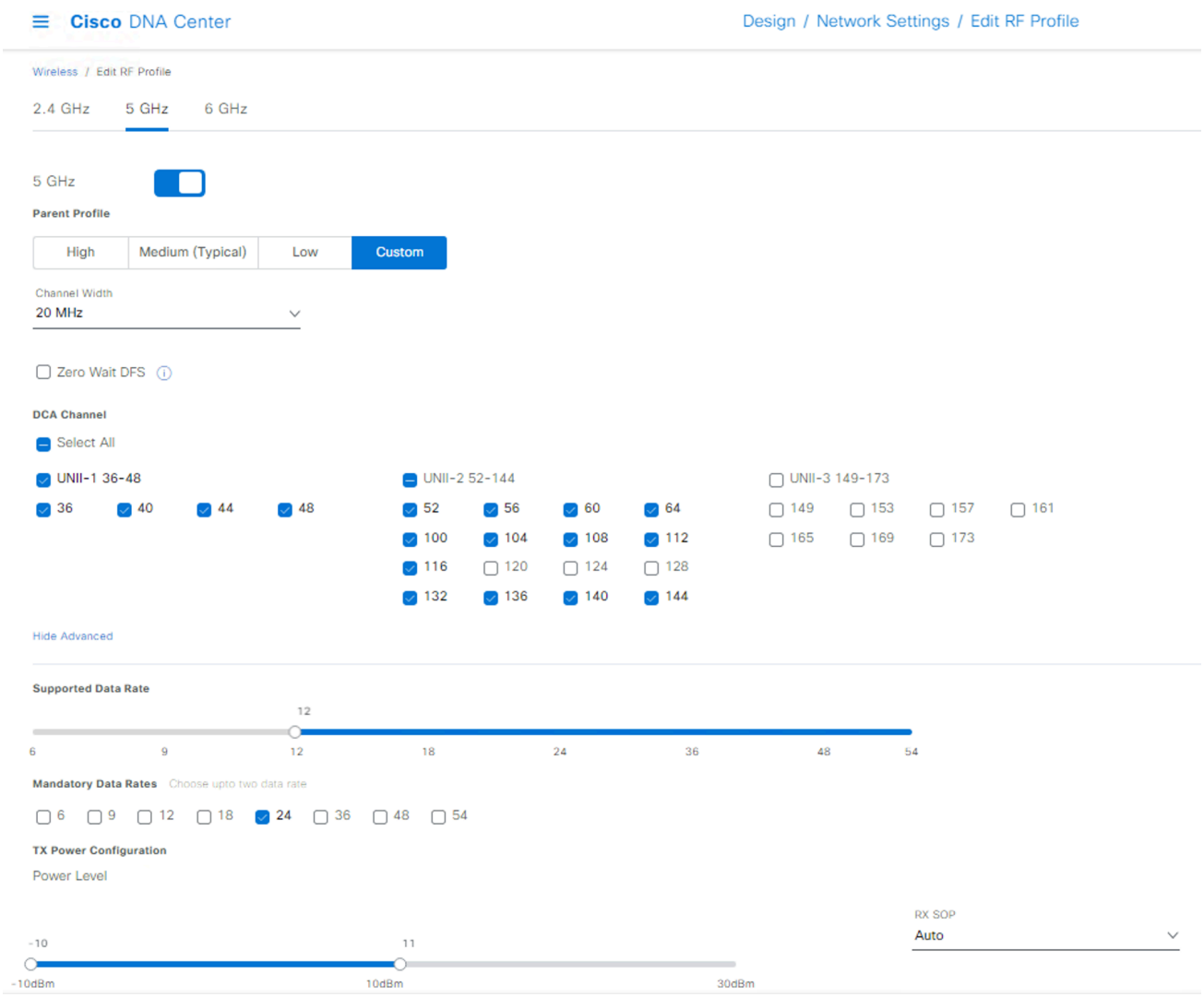


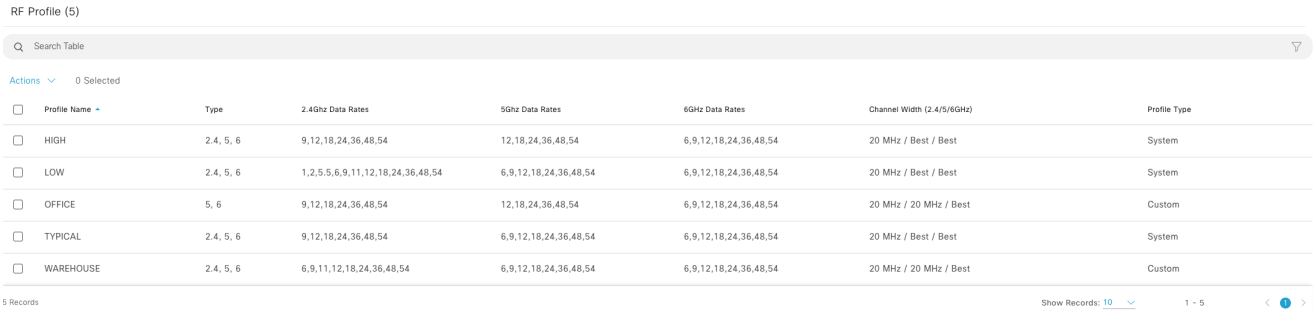
Figure 112 RF Profile – OFFICE 5 GHz Band



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



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.

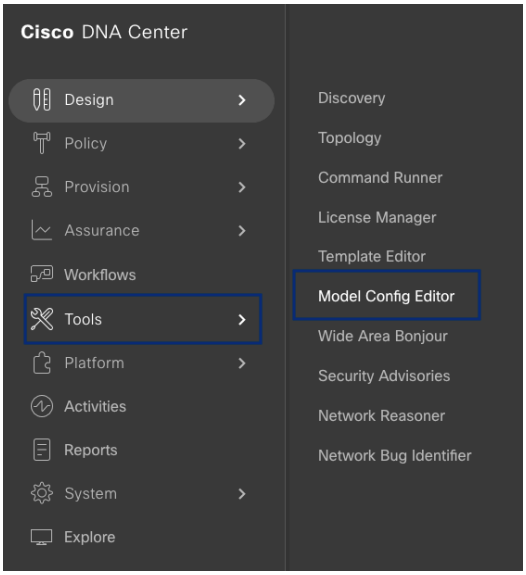
- “Enable Aironet IE in CORP SSID as it will be used for a site survey with Ekahau”

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.

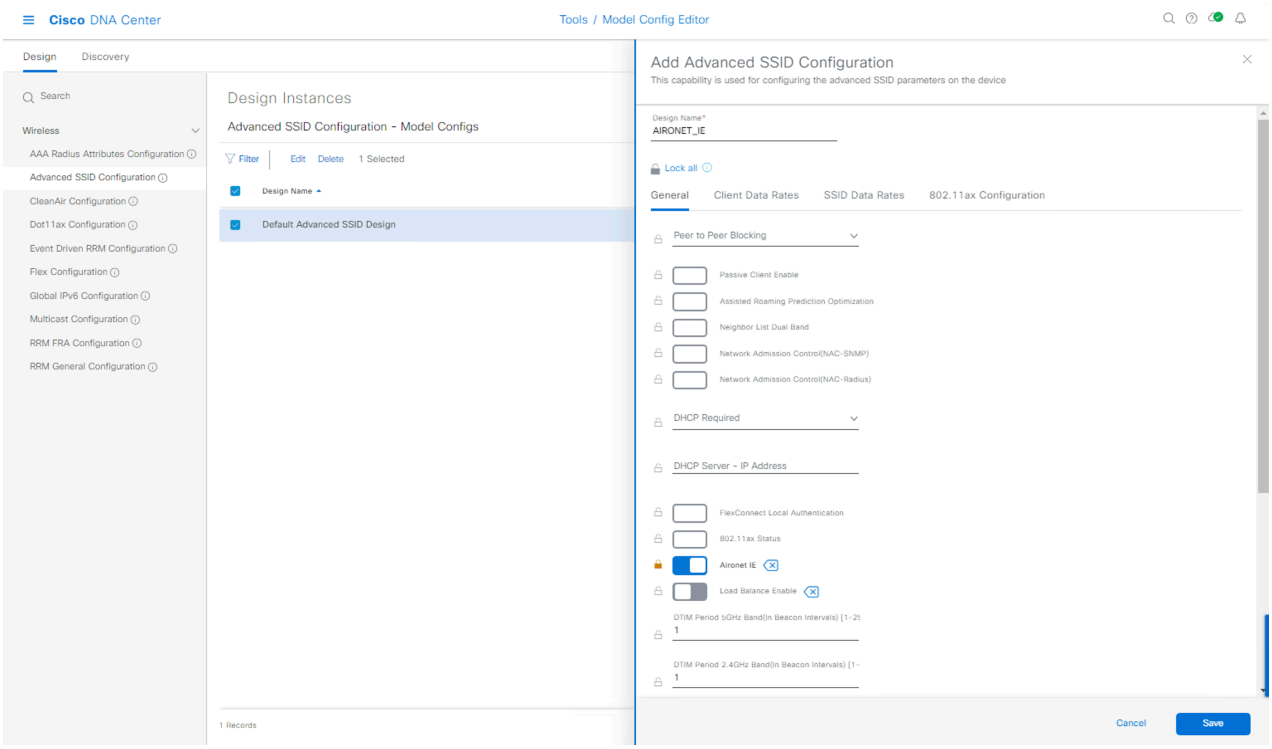
- Navigate to **Tools > Model Config Editor:**

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

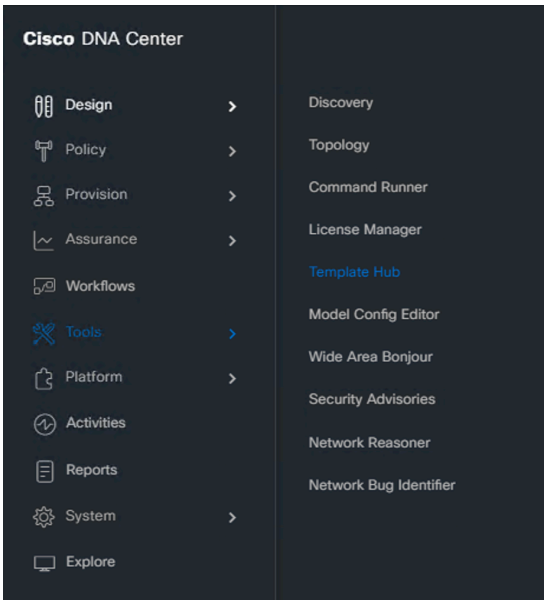
For any configurations that are not part of the Network Settings or Model Config, Template Hub can be utilized to push CLI-based configs to the devices.

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



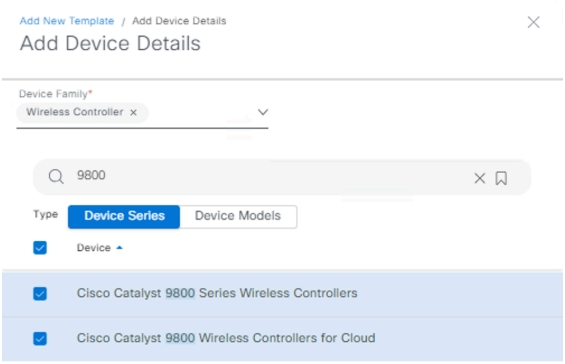
Click the "**+Add"** icon and choose **New Template.** Fill the required information:

Table 21 CLI Templates – Values

Parameter	Value

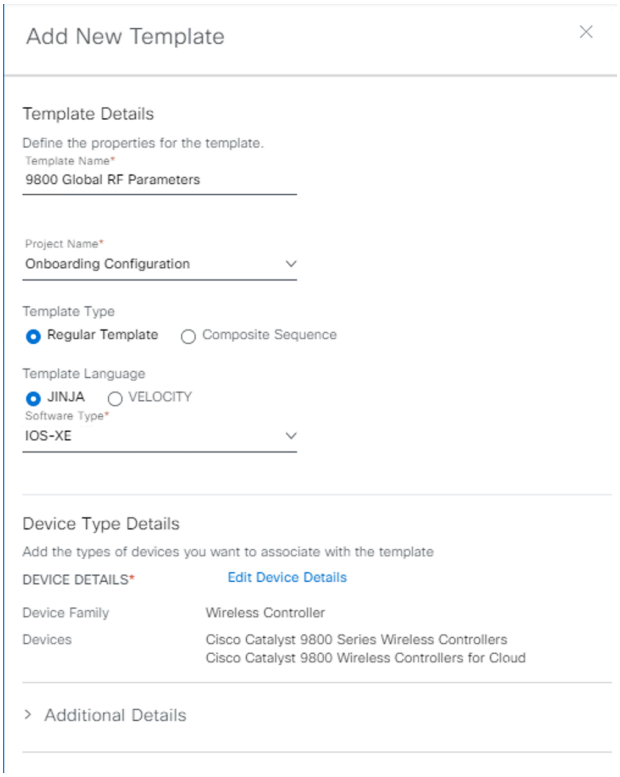
Template Name	9800 Global RF Parameters
Project Name	Onboarding Configuration
Template Type	Regular Template
Template Language	JINJA
Software type	IOS-XE
Device Details	**Add Device Details** Add 9800 WLCs (*see screenshot below*)

Figure 117 Template Hub – Add Device Details



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

Figure 118 Template Hub – Template Details



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

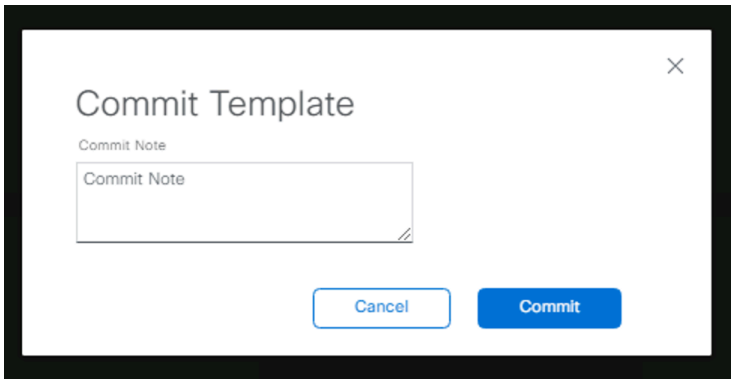
Template hub is a powerful tool, you can create templates with variables to be filled with values upon provisioning, for now we will push static values

- 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

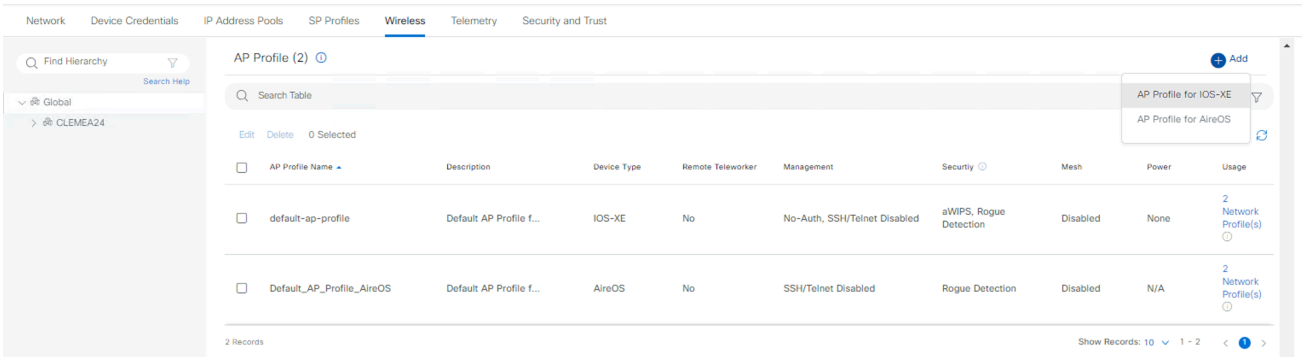
As part of the requirements the customer defined that we must enable SSH access to APs to all APs at HQ and RB, for this we must use AP profiles.

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

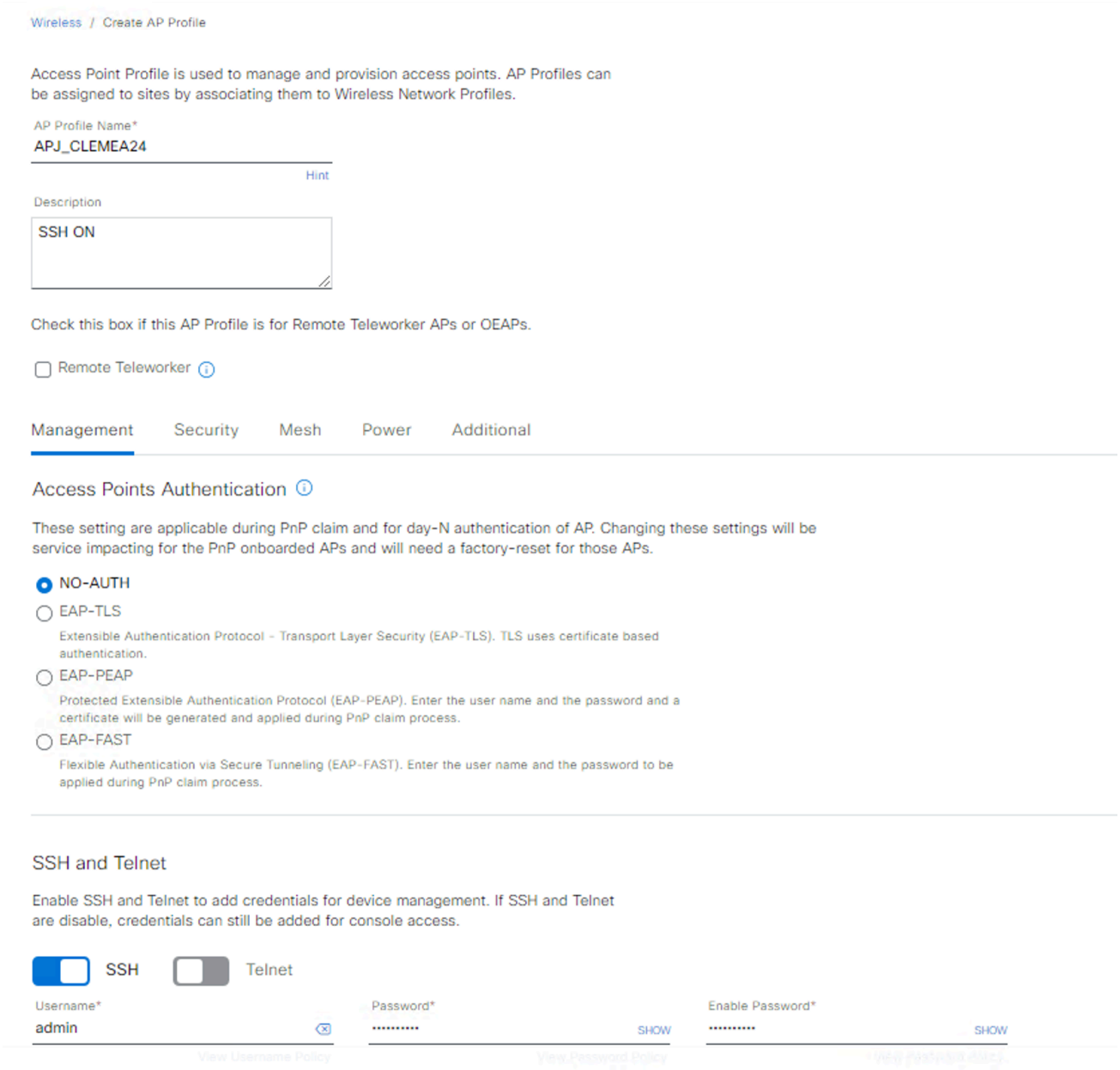


Use the information below to configure the RB AP Profile:

Table 22 AP Profile –Requirements

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

Figure 121 AP Profiles – Add AP profile



- Click **Save**

Step 5: Configuring Network Profiles

So far, we have:

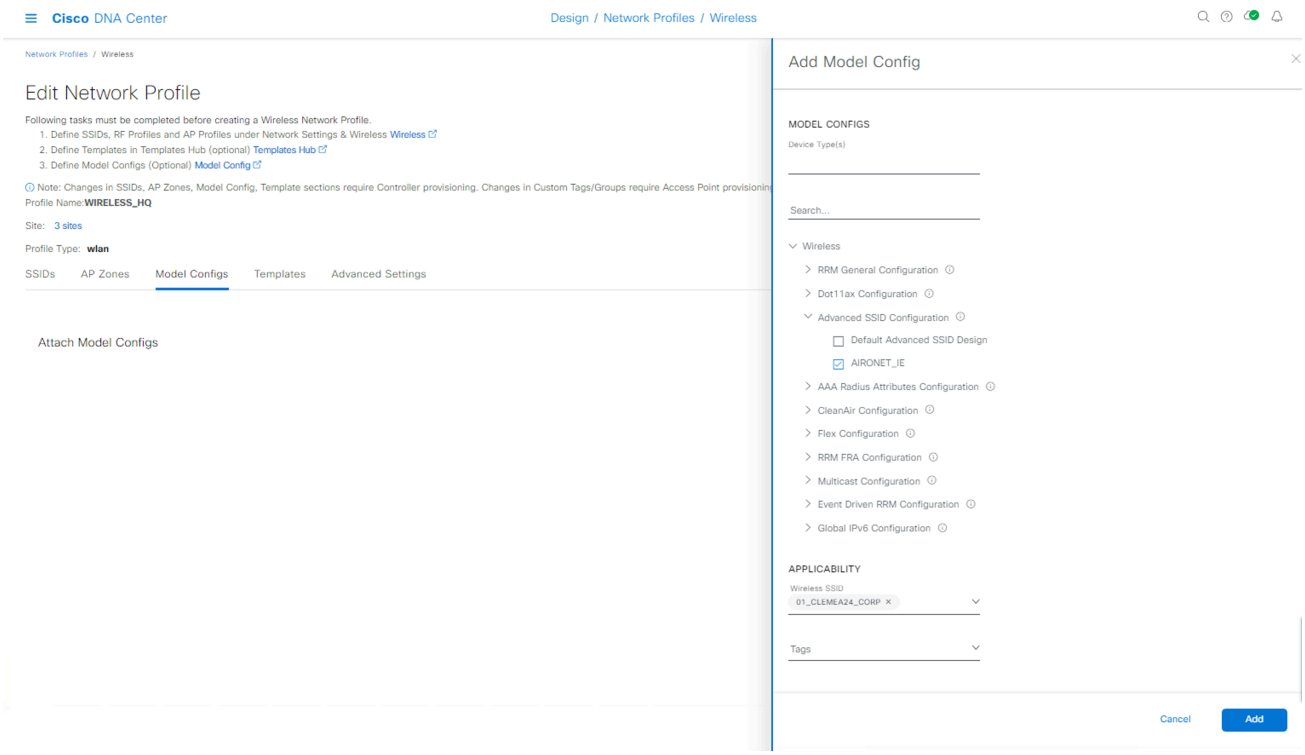
- Created two sites HQ and RB
- Created two Network Profiles to support HQ and Remote Branch settings.
- SSIDs were also associated with the Network Profiles.

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

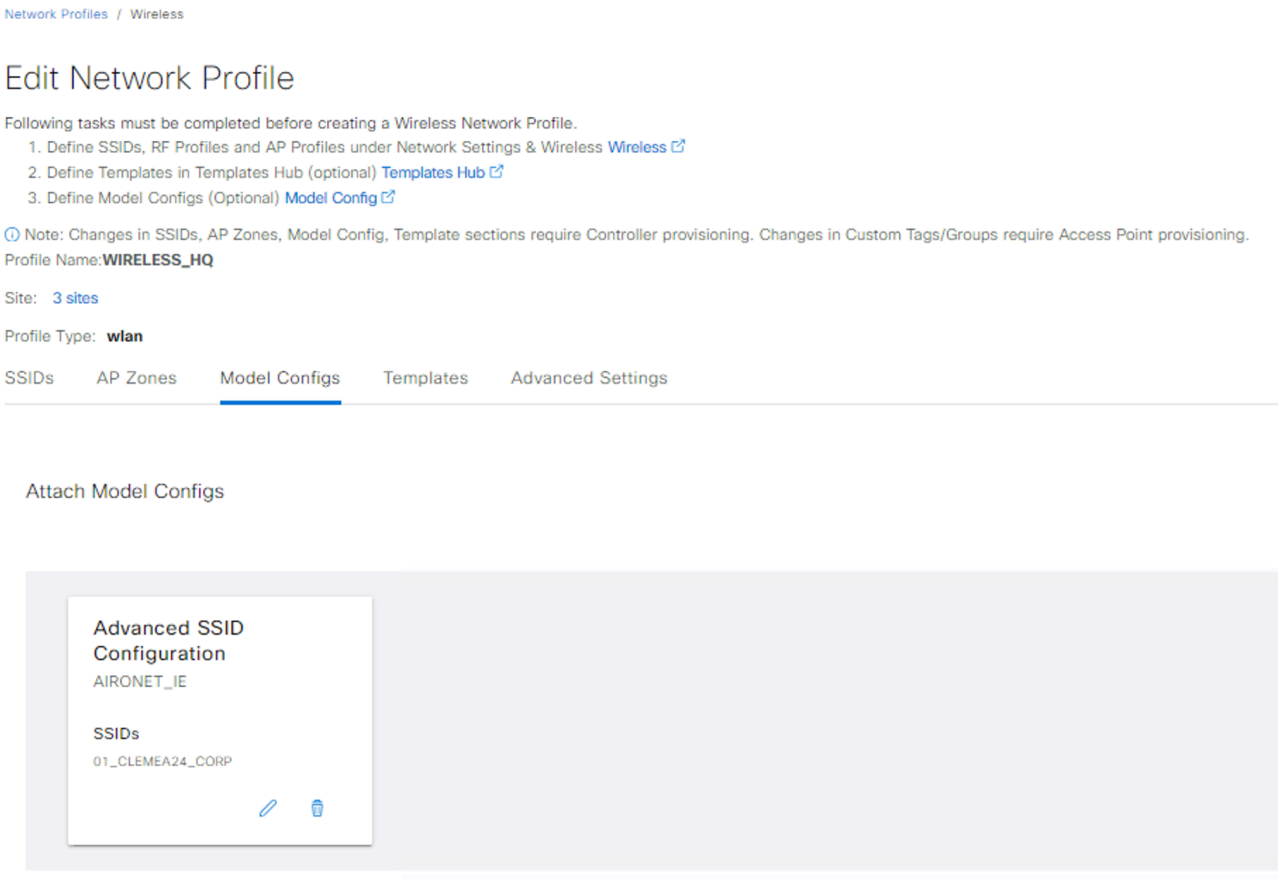
- Navigate to **Design > Network Profiles.**
- Click on **Edit** to modify **WIRELESS_HQ** Network Profile.
- Navigate to **Model Configs** tab.
- Click on **Add Model Config**
- Expand "**Wireless**" and look for "**Advanced SSID Configuration**".
- Mark **AIRONET_IE**
- Under **Applicability** select 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

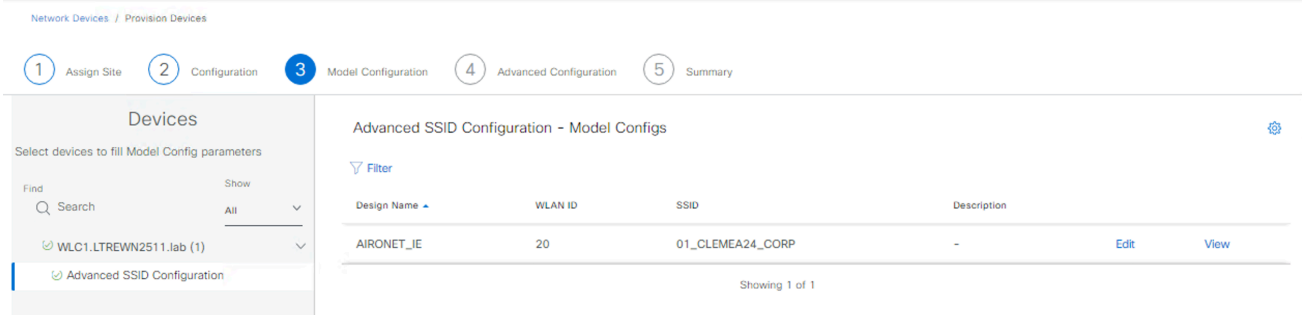


If you decide to provision the WLC now, you can expect Catalyst Center to push:

- 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



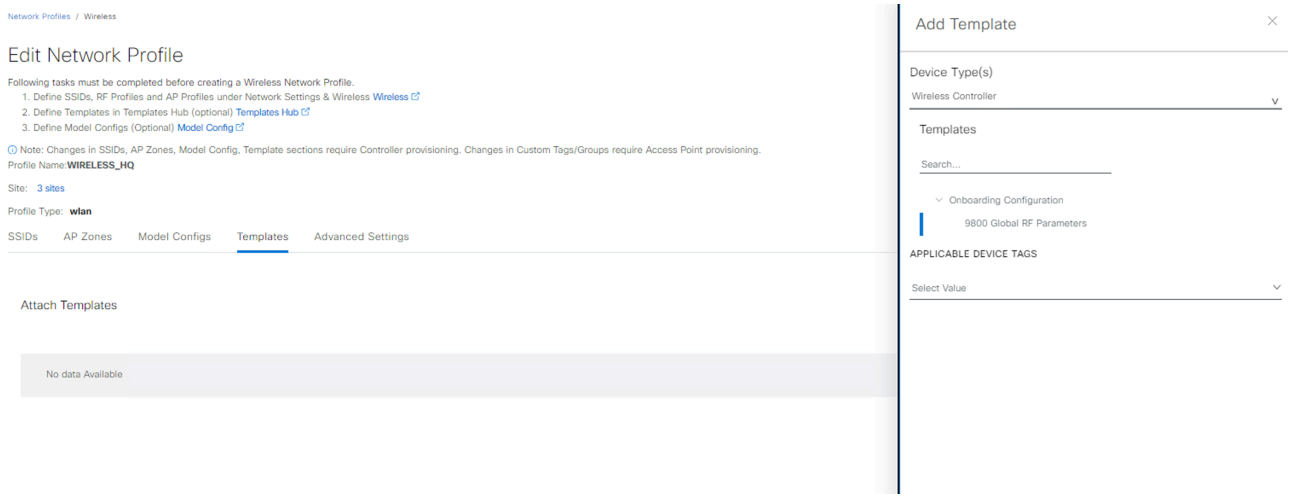
No need to provision AP in this step as the config goes to an existing WLAN.

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

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

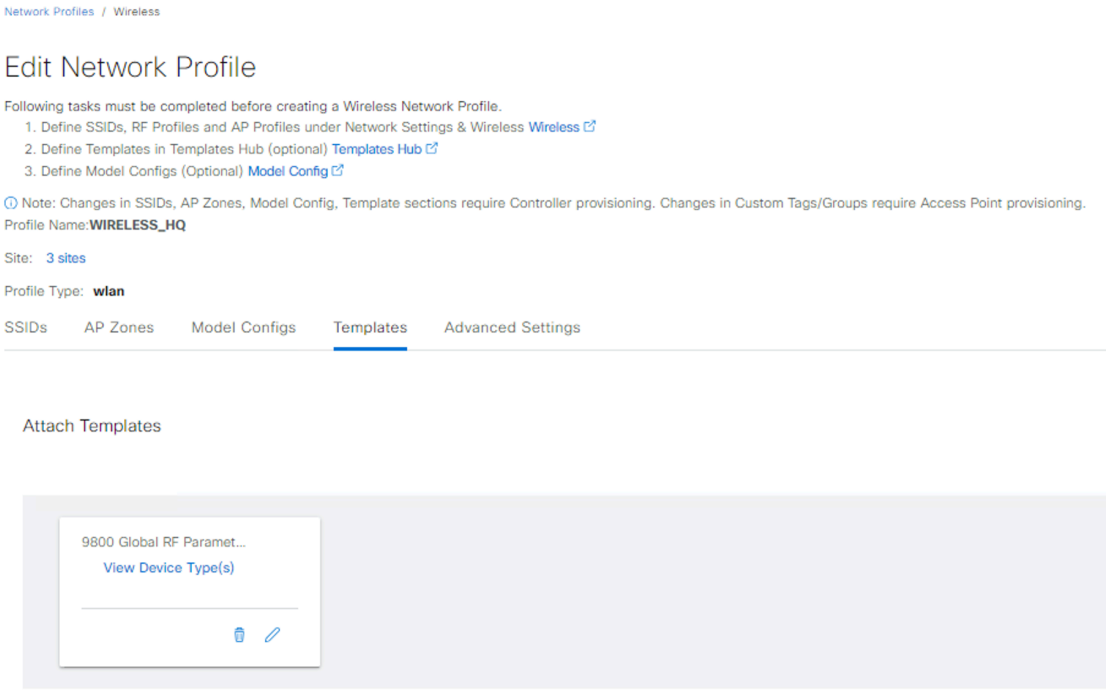
- Navigate to **Design > Network Profiles.**
- Click on **Edit** to modify **WIRELESS_HQ** Network Profile.
- Navigate to **Templates** tab.
- Click on **Add Template** and select previously created CLI Template named **9800 Global RF Parameters**
- Click on **Add**.

Figure 125 Network Profile - CLI Template



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

Figure 126 Network Profile - CLI Template



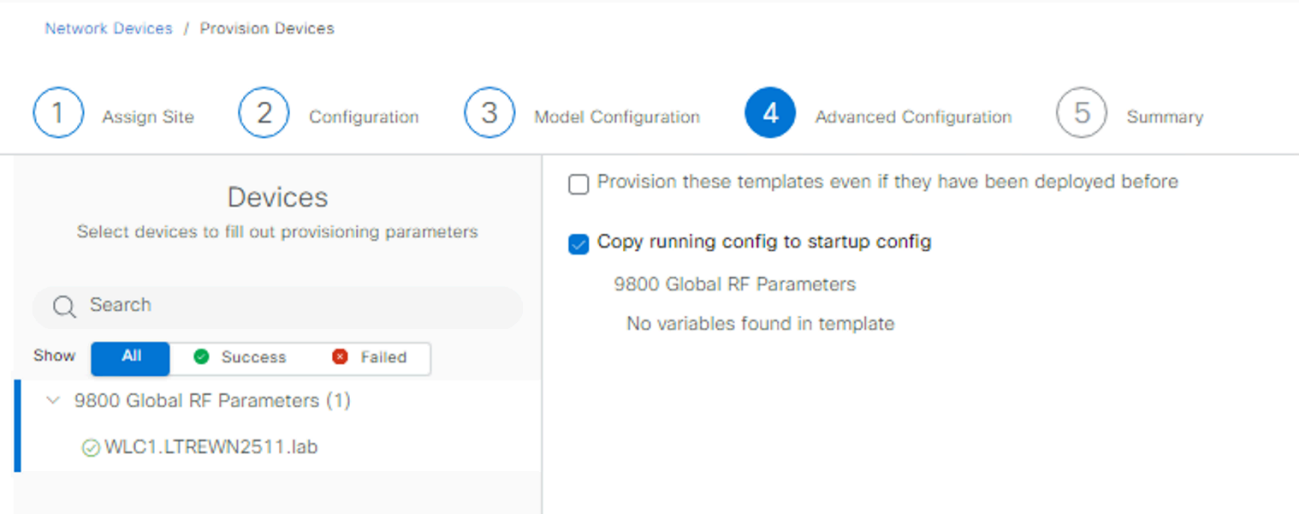
If you decide to provision the WLC now, you can expect Catalyst Center to push:

- 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**

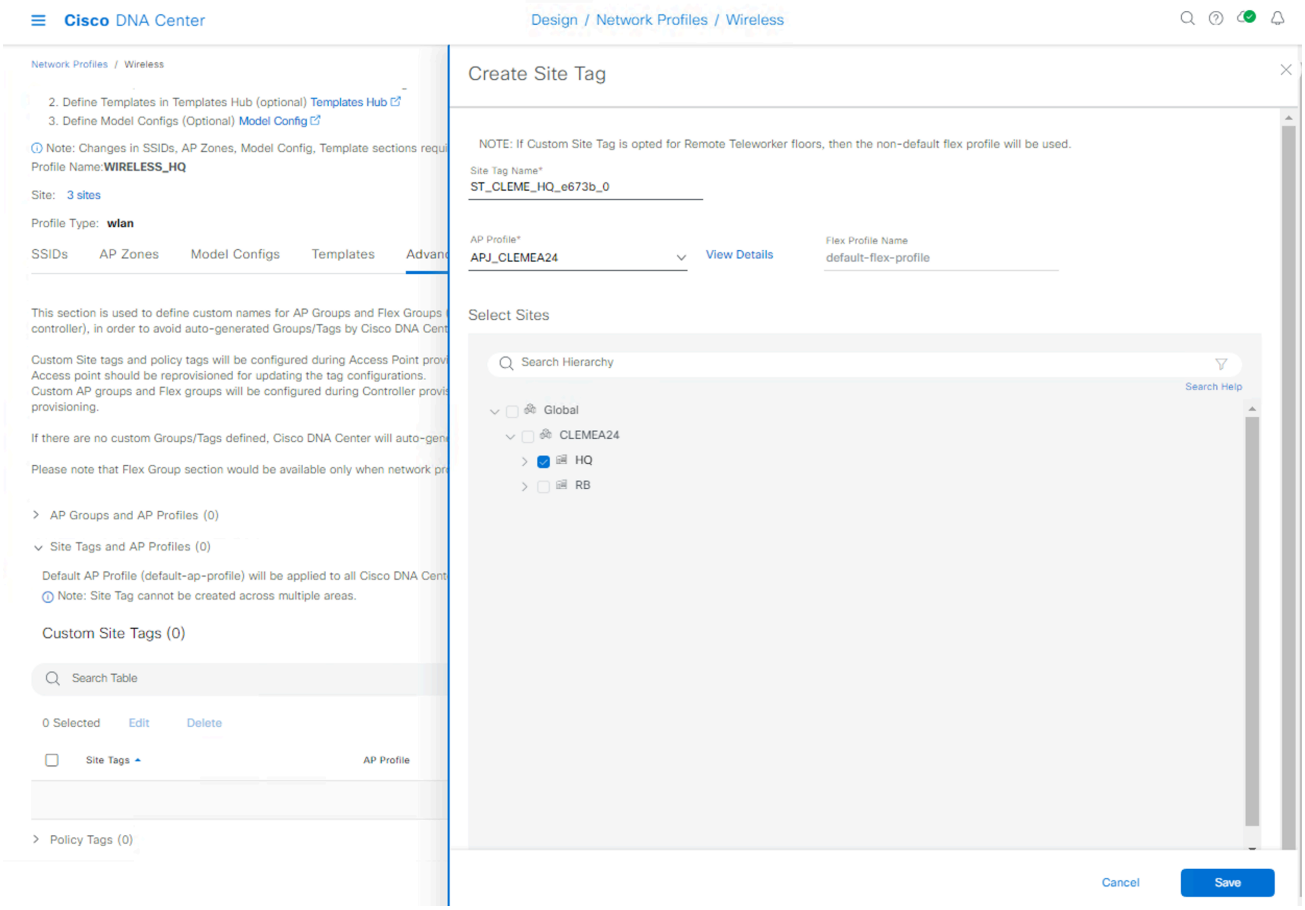
Map the APJ_CLEMEA24 to the existing Site Tag corresponding to the building at HQ.

- 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.



- 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.

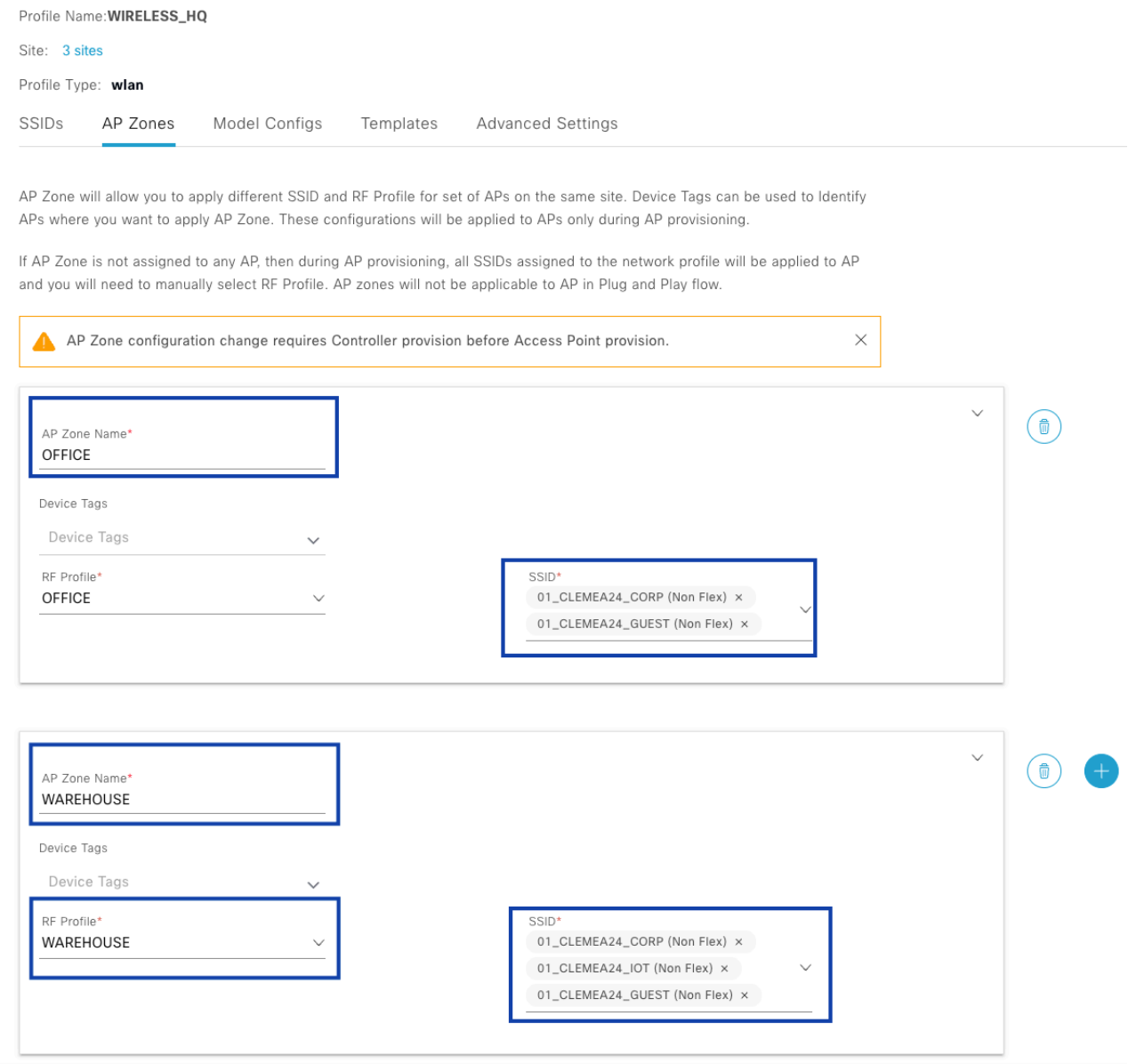
In order to create the AP Zones for the HQ site,

- 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
RF Profile	OFFICE	WAREHOUSE
SSID	XX_CLEMEA24_CORP XX_CLEMEA24_GUEST	XX_CLEMEA24_CORP XX_CLEMEA24_GUEST XX_CLEMEA24_IOT

Figure 128 Network Profiles - AP Zones



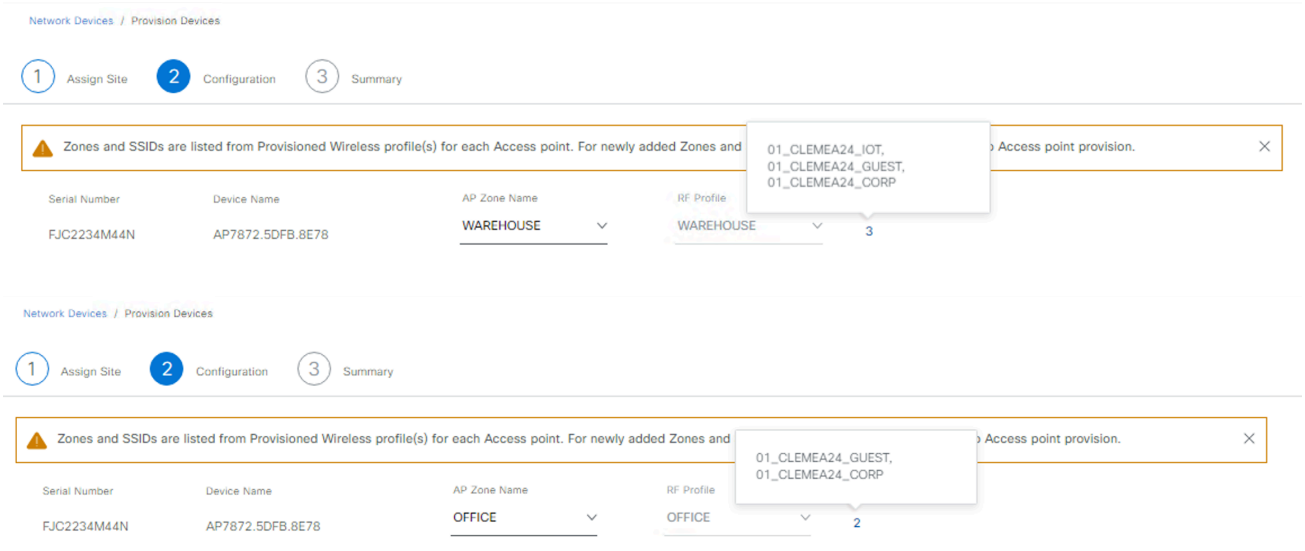
Click on **Save** for the changes to be applied.

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



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

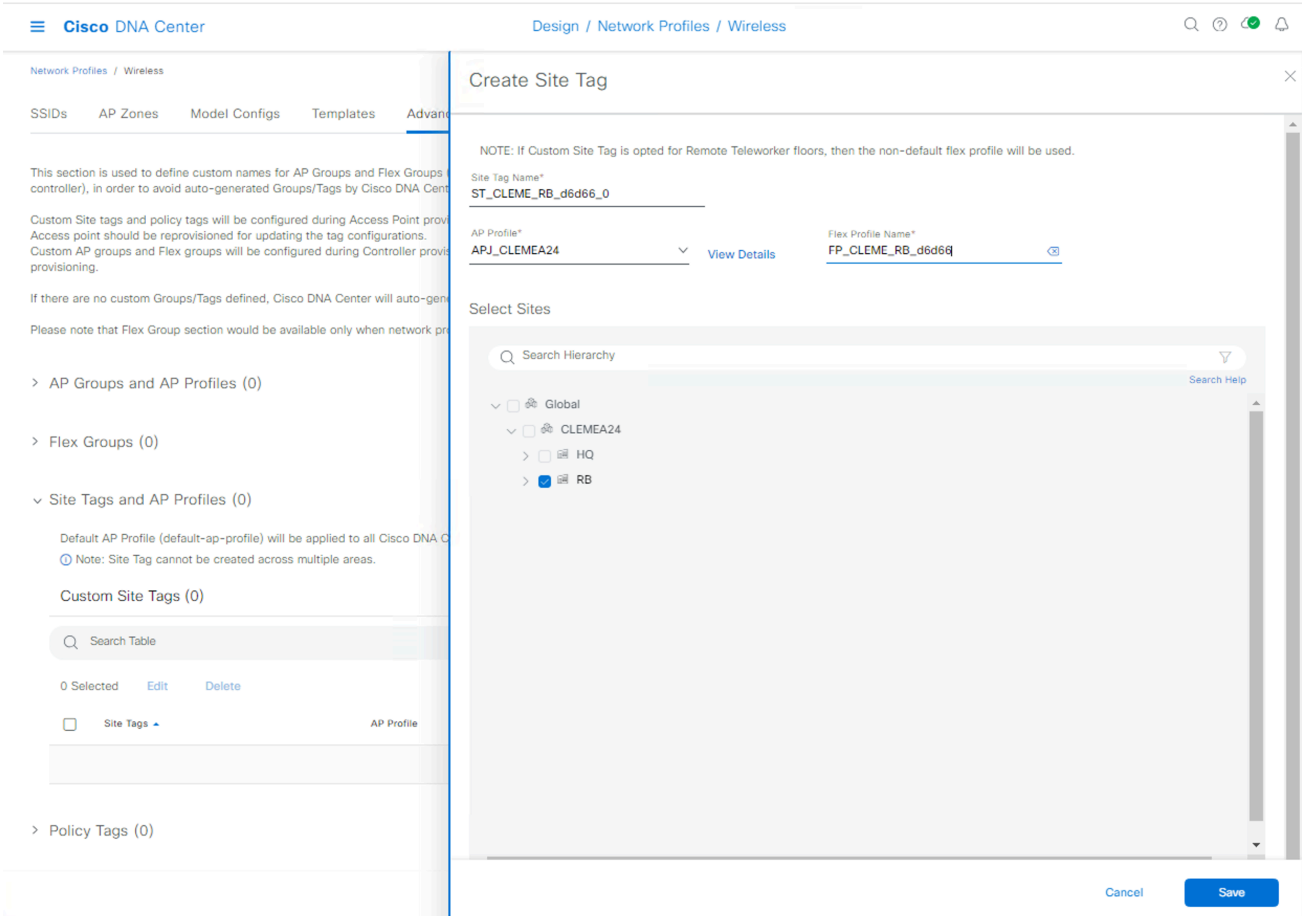


Table 24 Customer Requirements (Status so far)

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

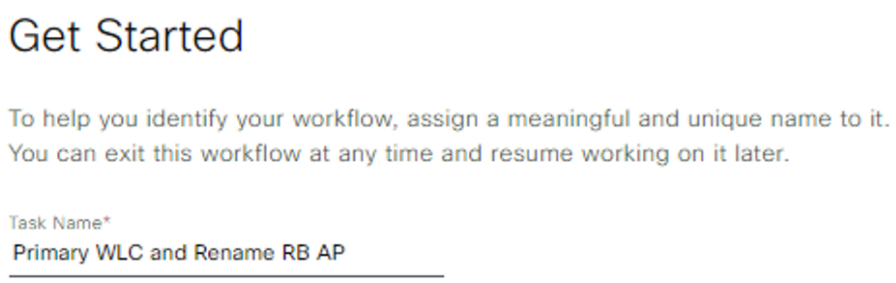
7	No need for IOT SSID in the OFFICE area at HQ site	Task 9 Step 9	Completed
8	Define Primary WLC to all APs Rename APs at RB	Task 9 Step 13	
9	Disable LEDs to APs at HQ	Task 9 Step 13	

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.

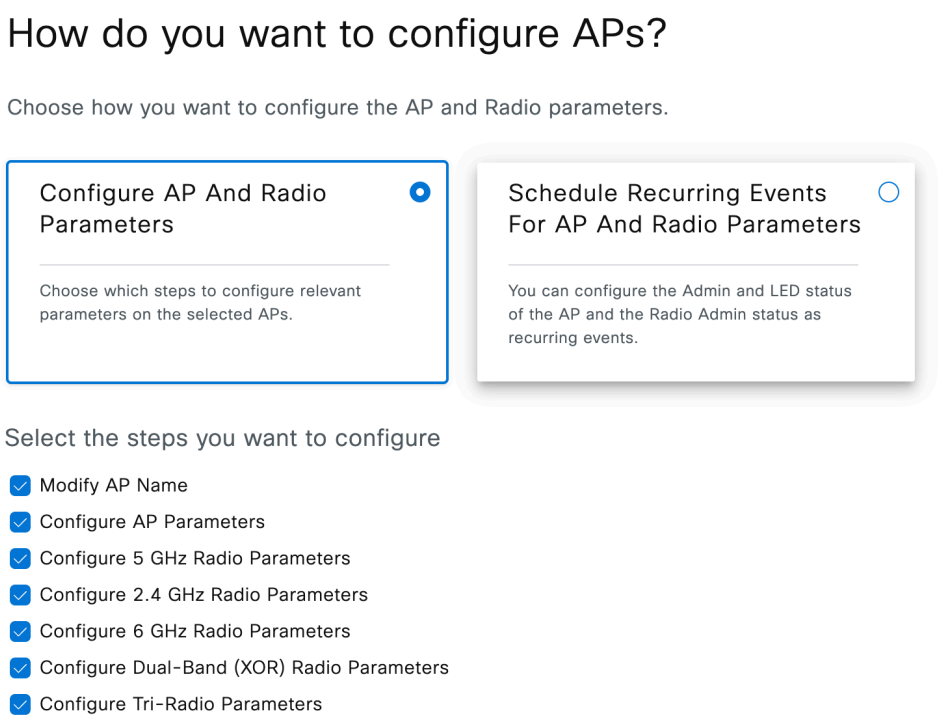
- Go to **Workflows > Configure Access Points** and create new Task named **Primary WLC and Rename RB AP**

Figure 131 AP Workflows Steps



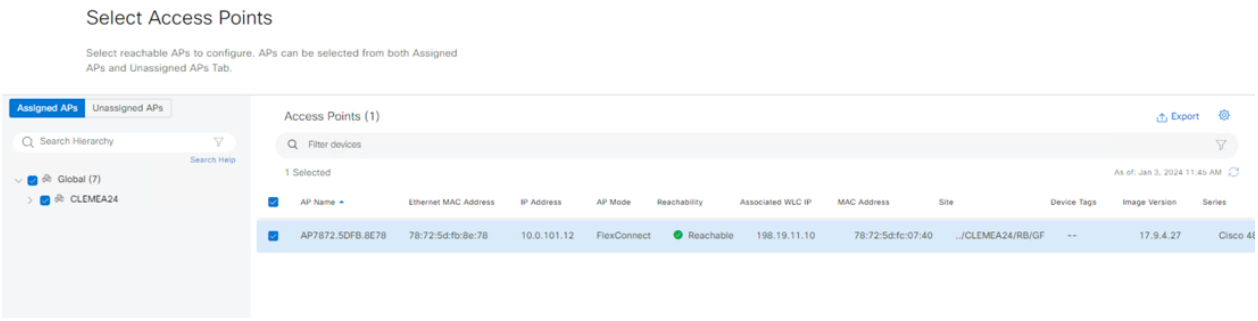
Proceed by selecting all the options under **Configure AP and Radio Parameters**:

Figure 132 AP Workflows Steps



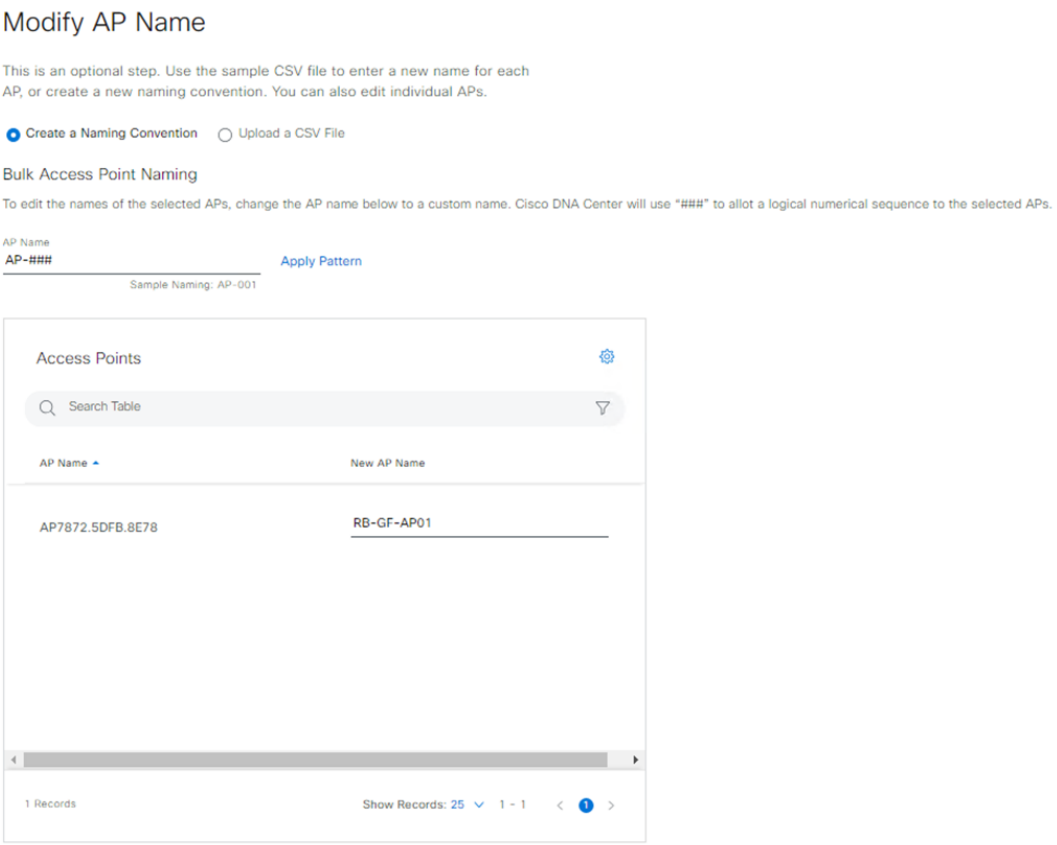
Select the RB AP:

Figure 133 AP Workflows Steps



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

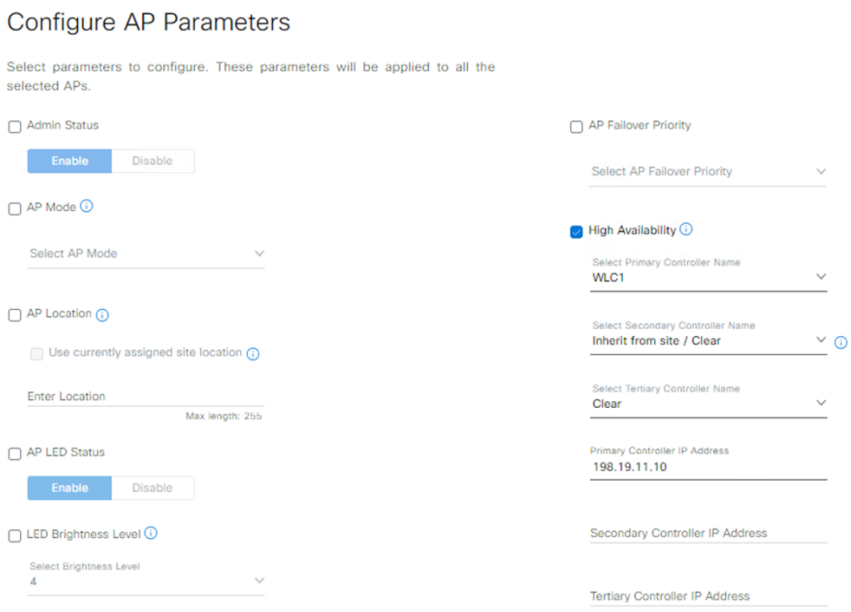
Figure 134 AP Workflows Steps – Rename AP



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



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

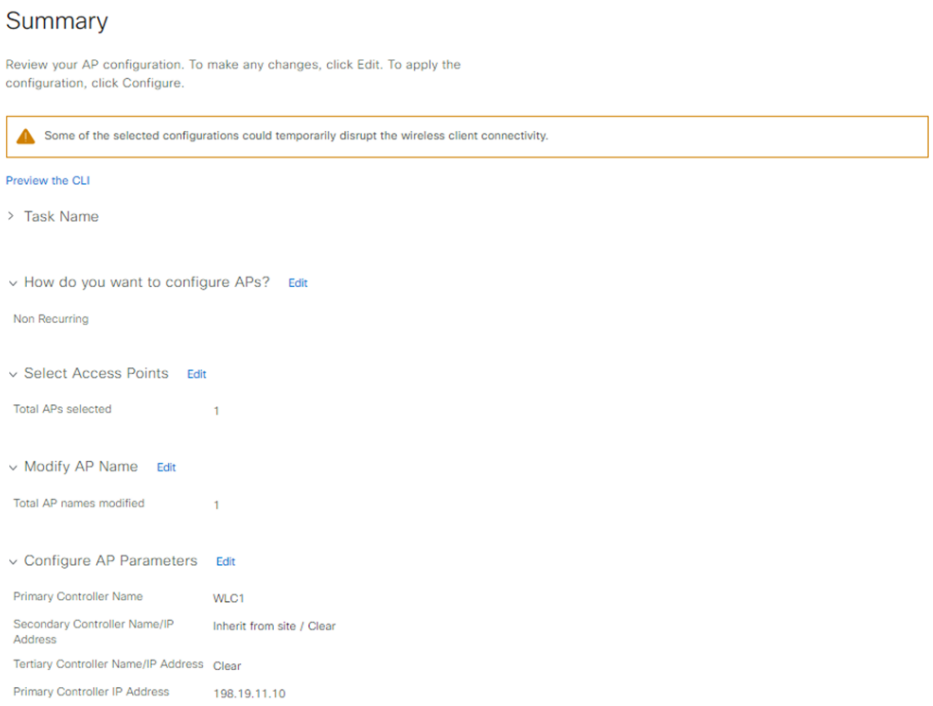


Figure 137 AP Workflows Steps – CLI Preview

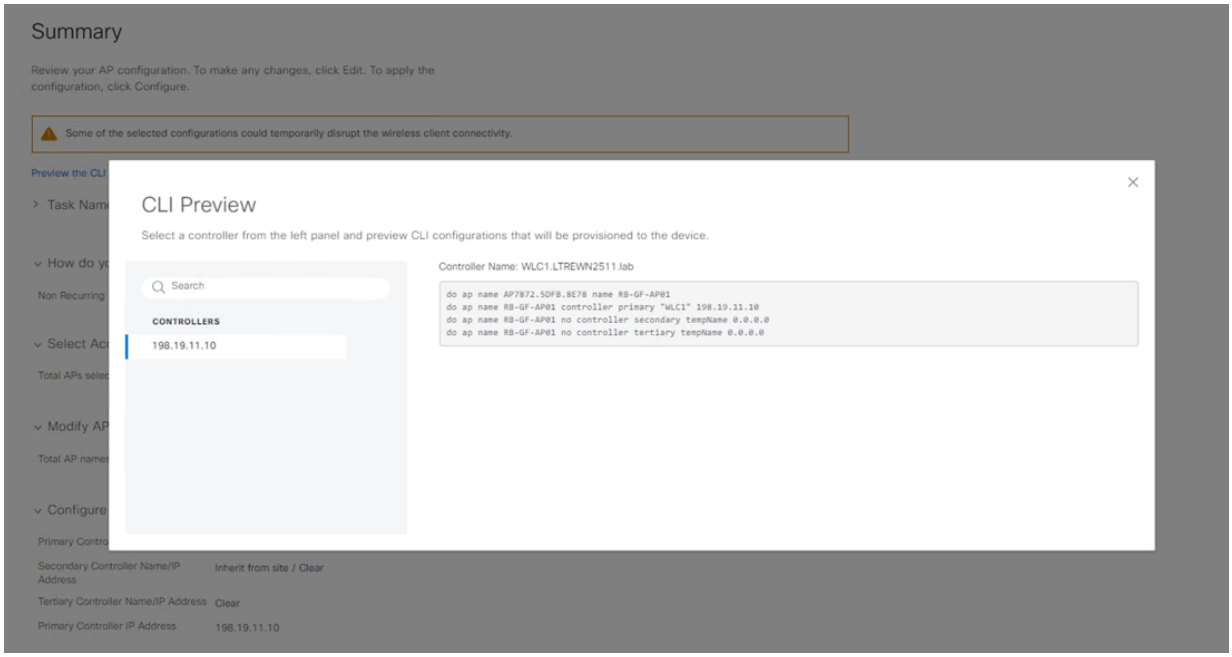
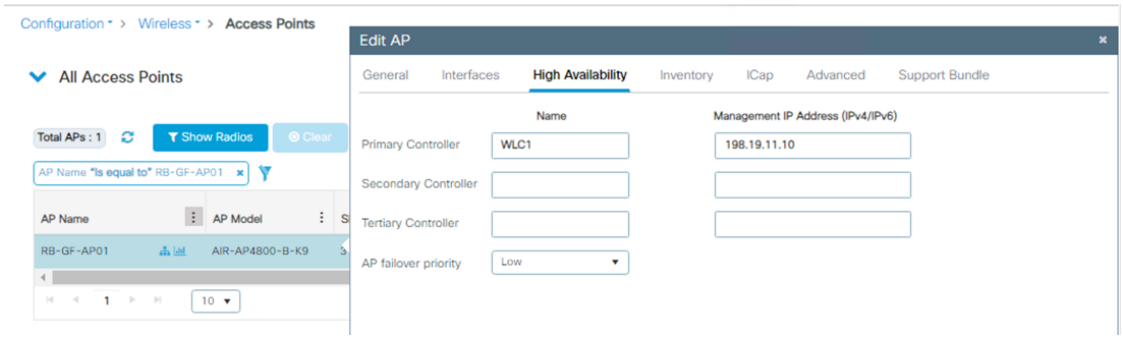
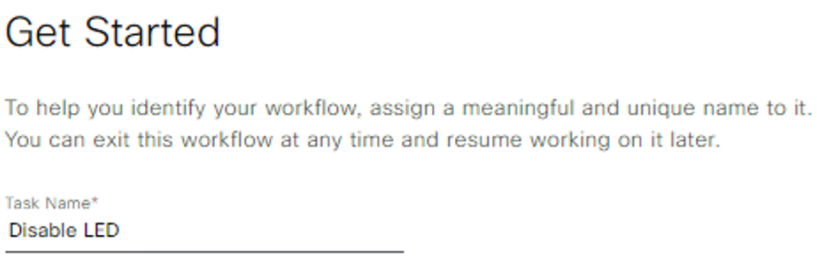


Figure 138 AP Workflows Steps – Verify



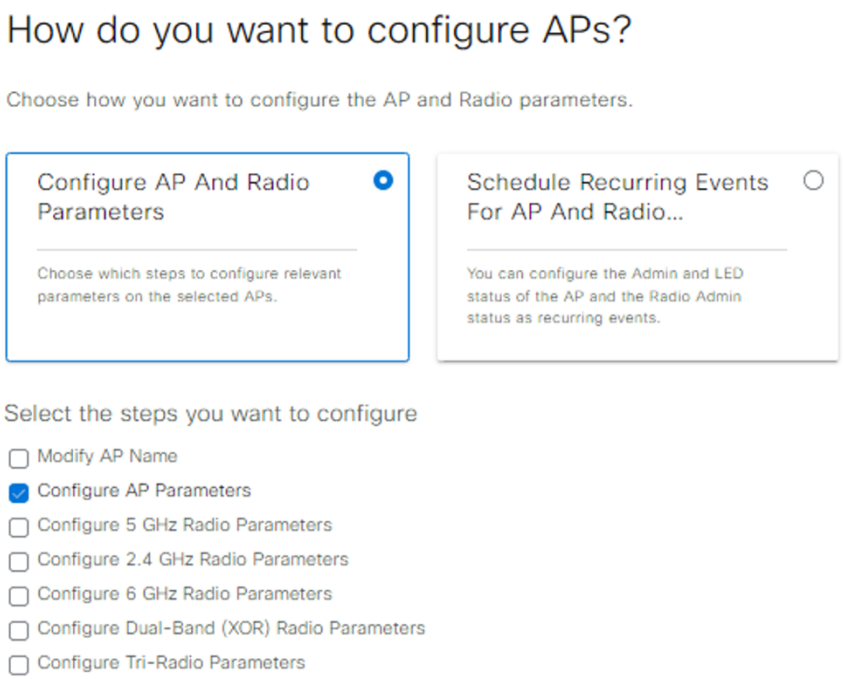
Repeat the process to Disable LEDs to APs at HQ. Let us create the **Disable LED** AP Workflow first.

Figure 139 AP Workflows Steps – Disable LED



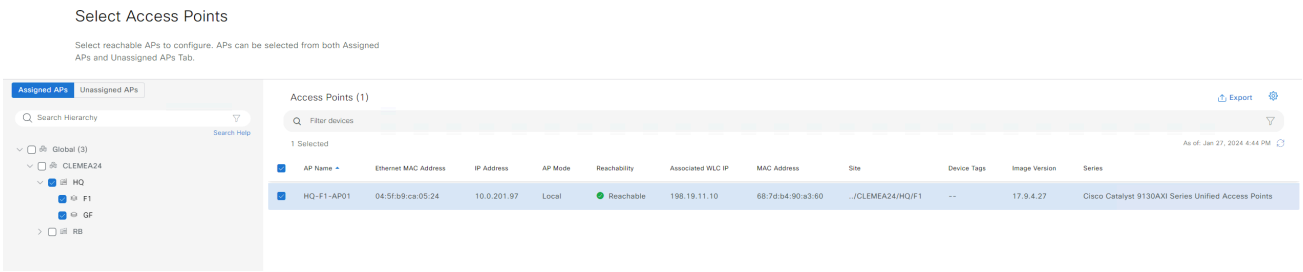
We will limit this task to **Configure AP Parameters** only.

Figure 140 AP Workflows Steps – Disable LED



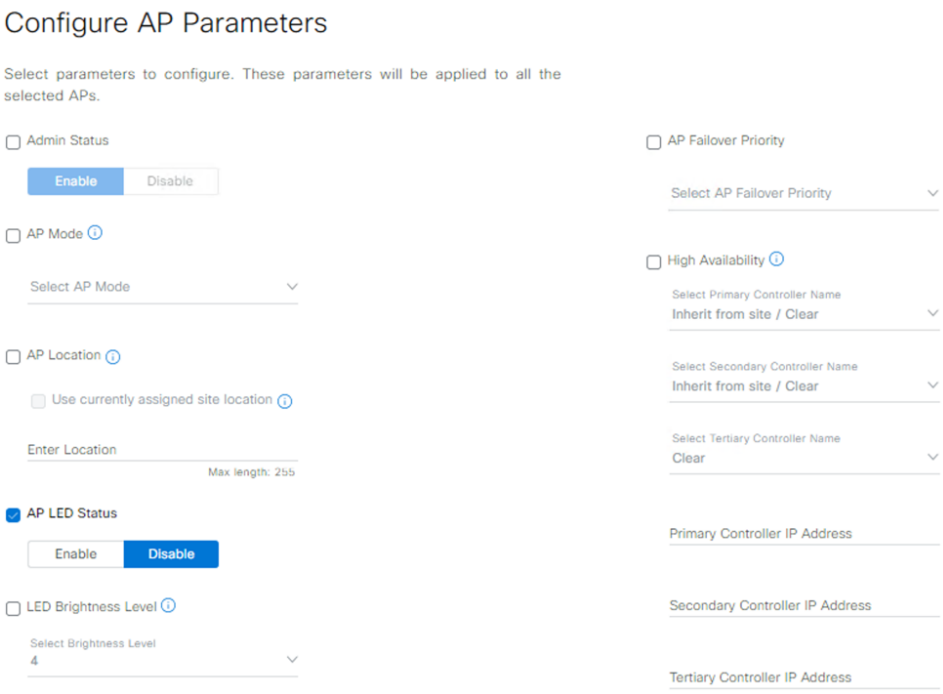
Select the **HQ-F1-AP01** AP and click **Next:**

Figure 141 AP Workflows - AP Selection



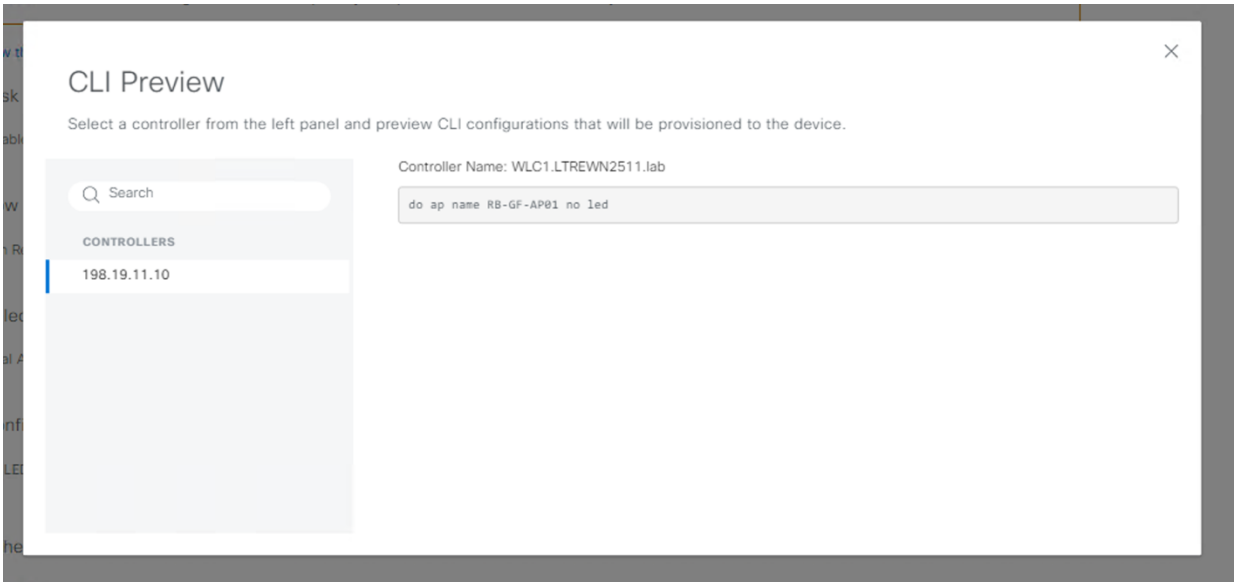
Check the **AP LED Status** box and set the value to **Disabled**.

Figure 142 AP Workflows Steps – Disable LED



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:

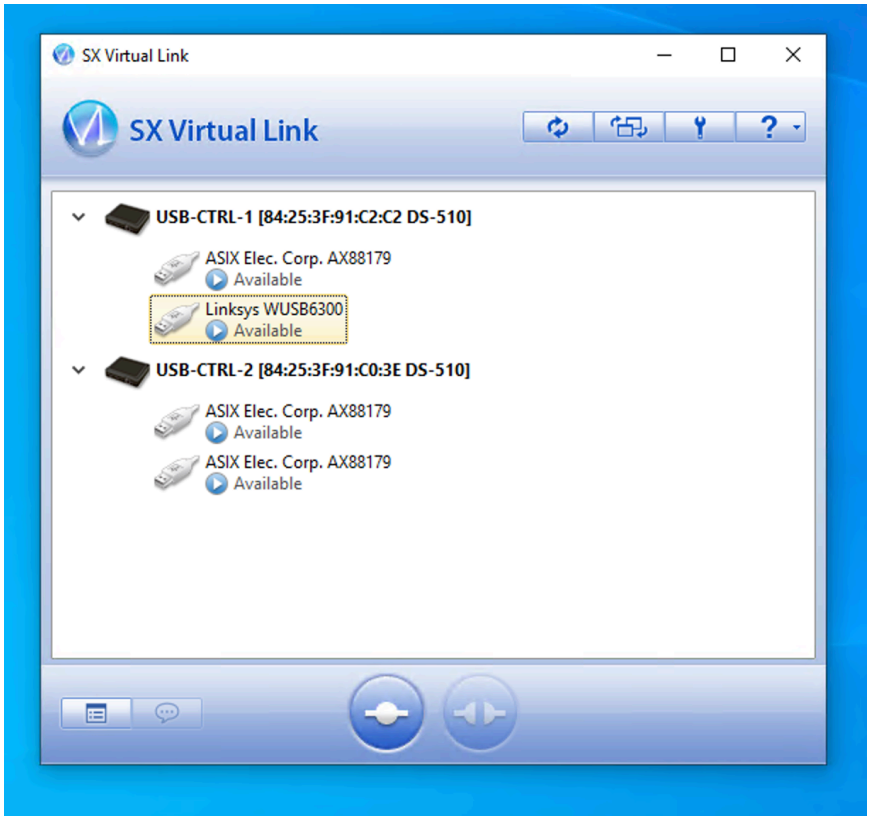
Table 25 Wireless Clients Addressing and Credentials

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

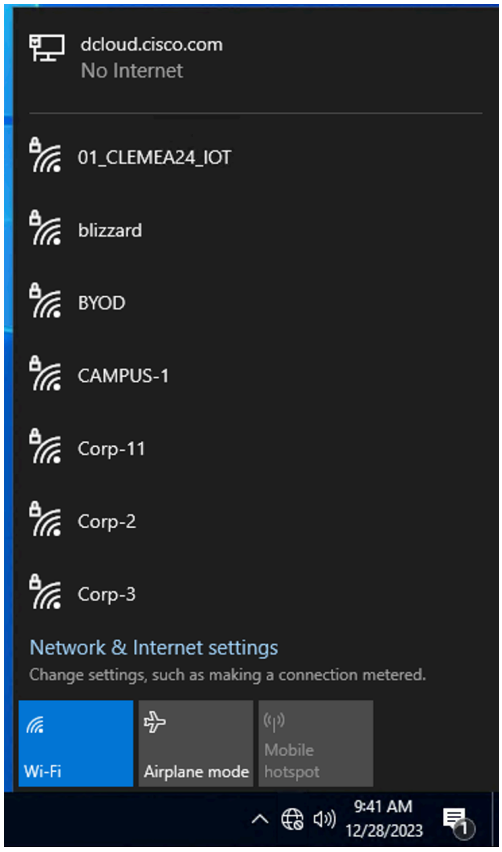
Figure 144 Configure SX Virtual Adapter



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

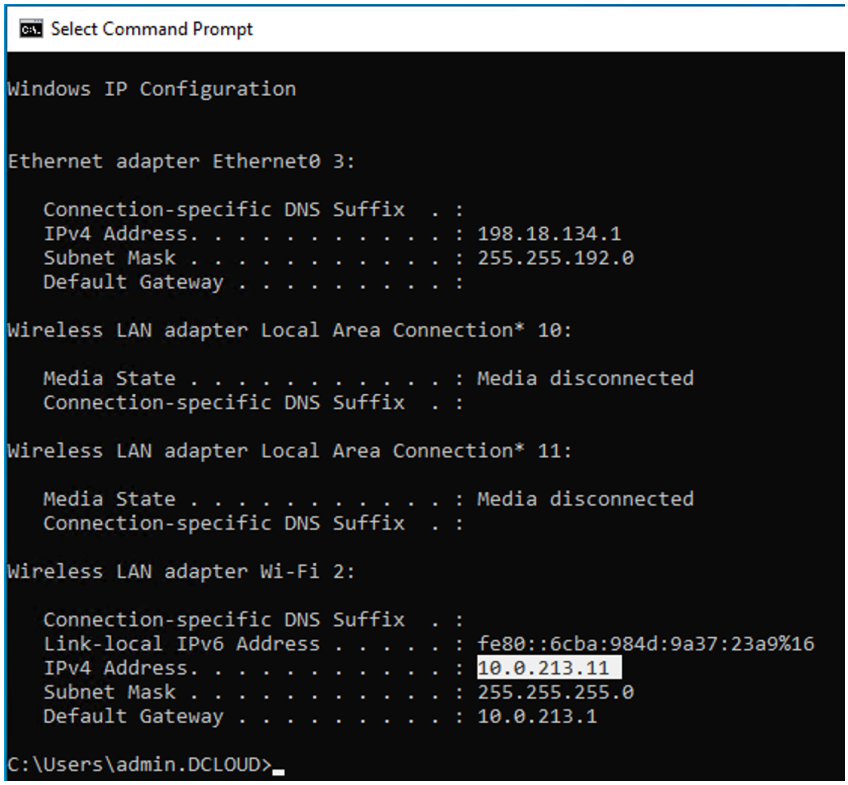
Step 2: Test IOT SSID

Figure 145 Client Connectivity Testing



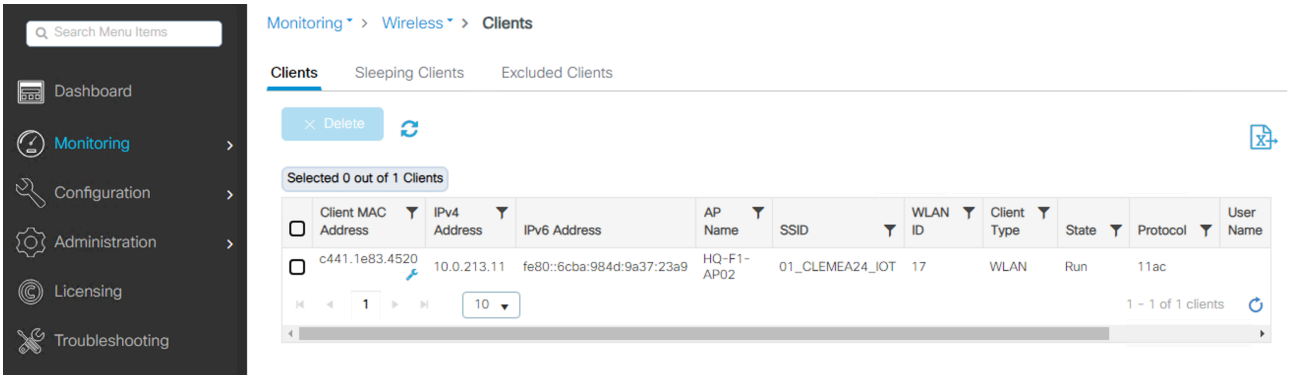
Verify using CMD if the wireless client gets an IP address from the desired VLAN.
The below example is for IOT at the HQ

Figure 146 Client Connectivity Testing – Verify IP with ipconfig



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



Step 3: Test CORP SSID

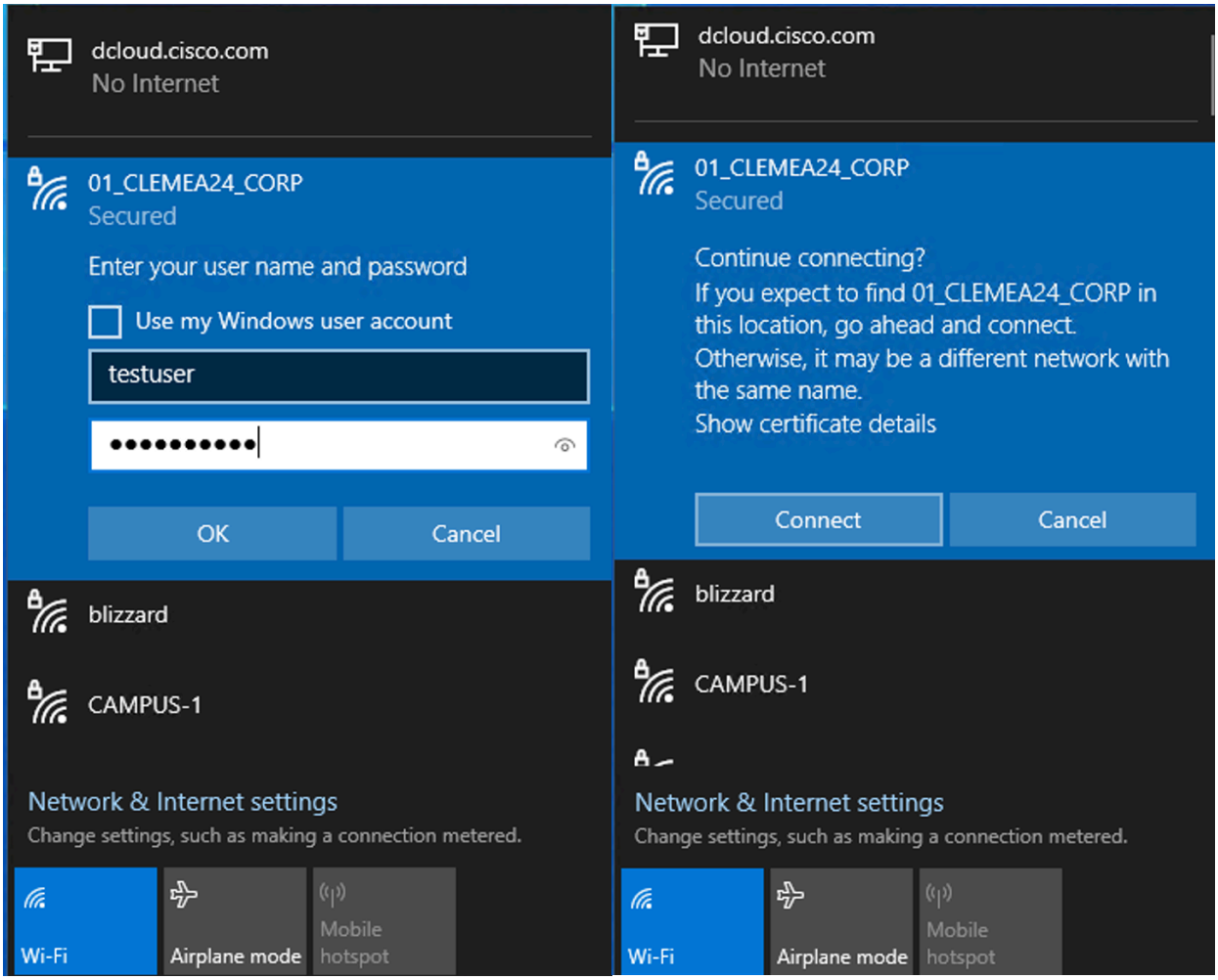
- RDP to a wireless client

- 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

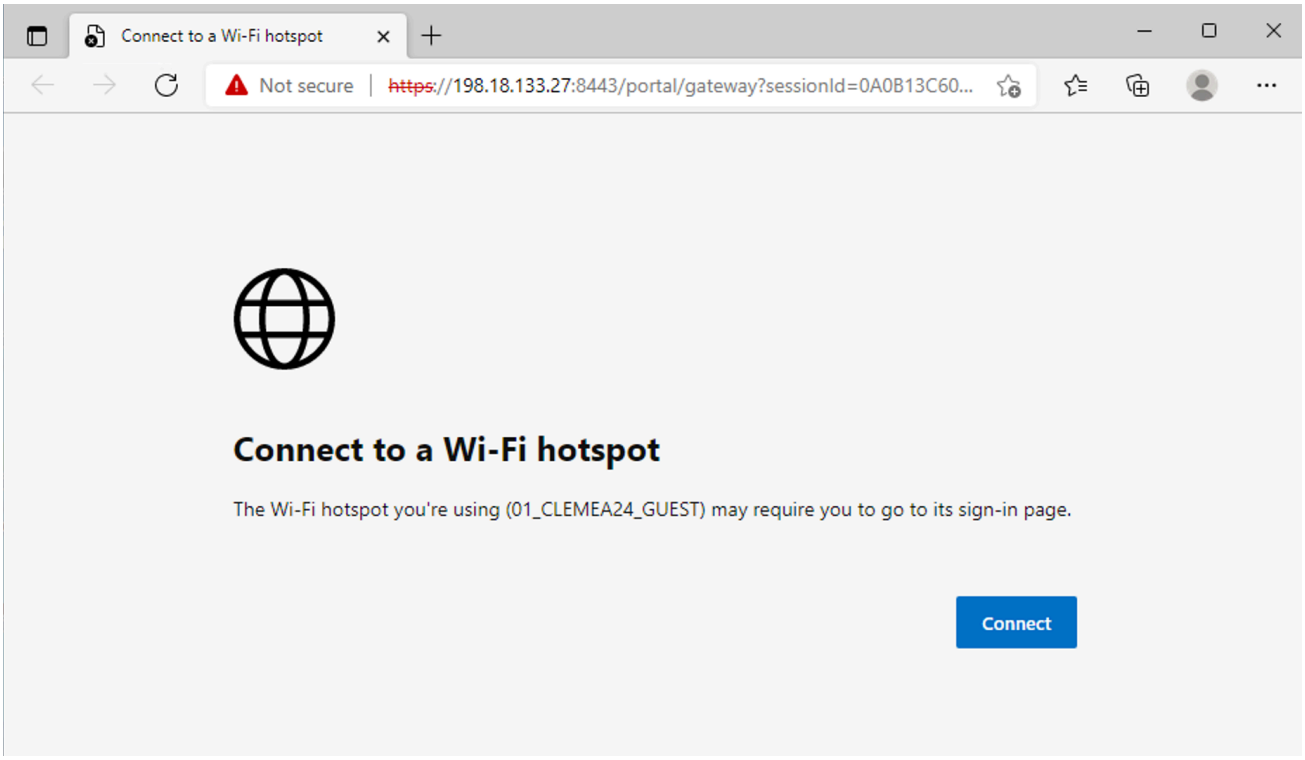
- RDP to a wireless client
- Make sure the SX Virtual Link has the **WUSB6300** connected.
- Connect to GUEST SSID
- Wait for a redirection

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**

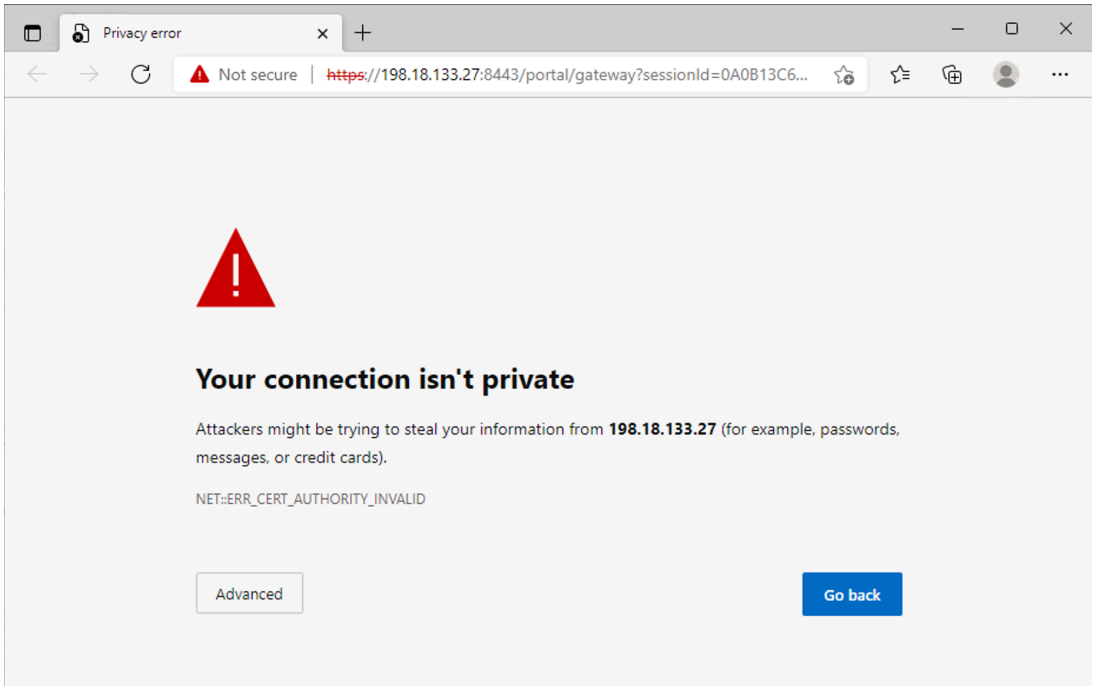
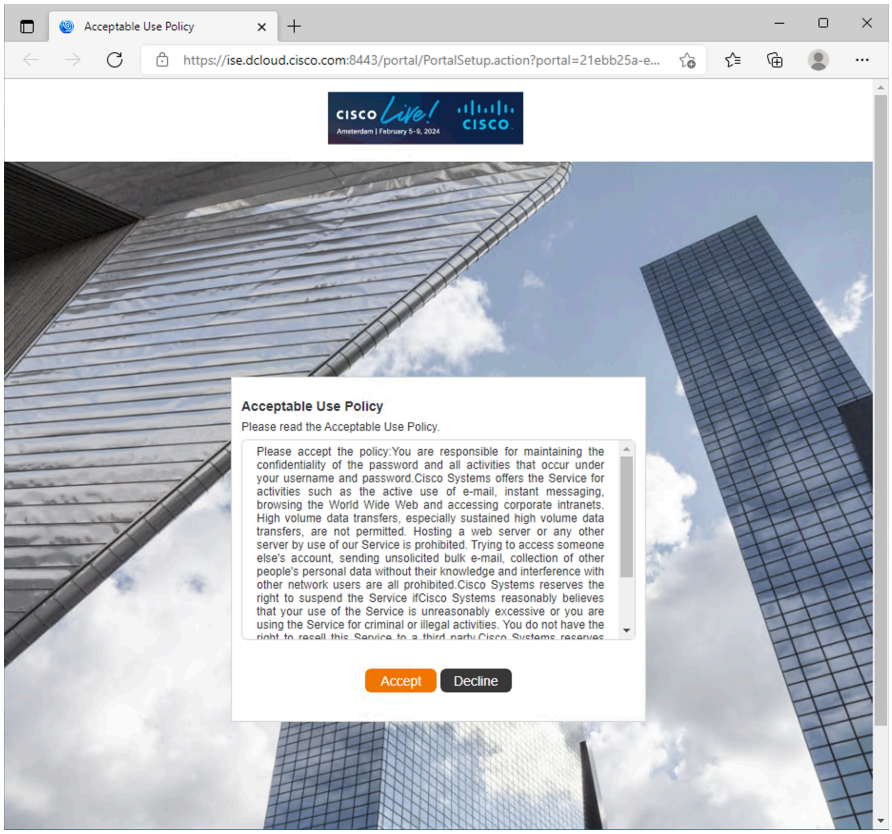


Figure 151 Client Connectivity Testing – Redirect to Captive Portal



After clicking “Accept” the user is now authenticated.

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:

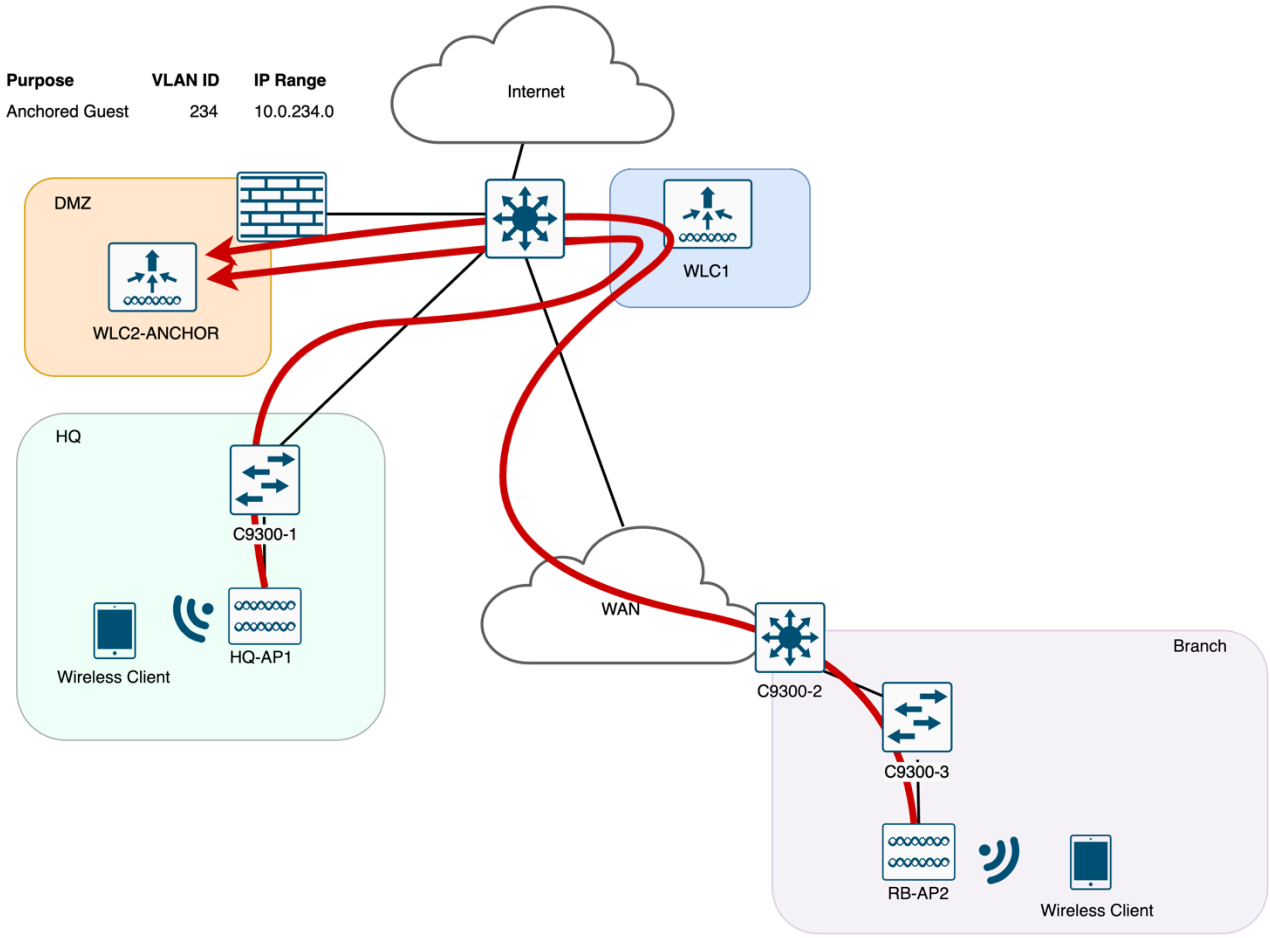
- Cisco Wireless Controllers that are managed by Cisco DNA Center.
- Cisco Wireless Controllers that are not managed by Cisco DNA Center (external wireless controllers).

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

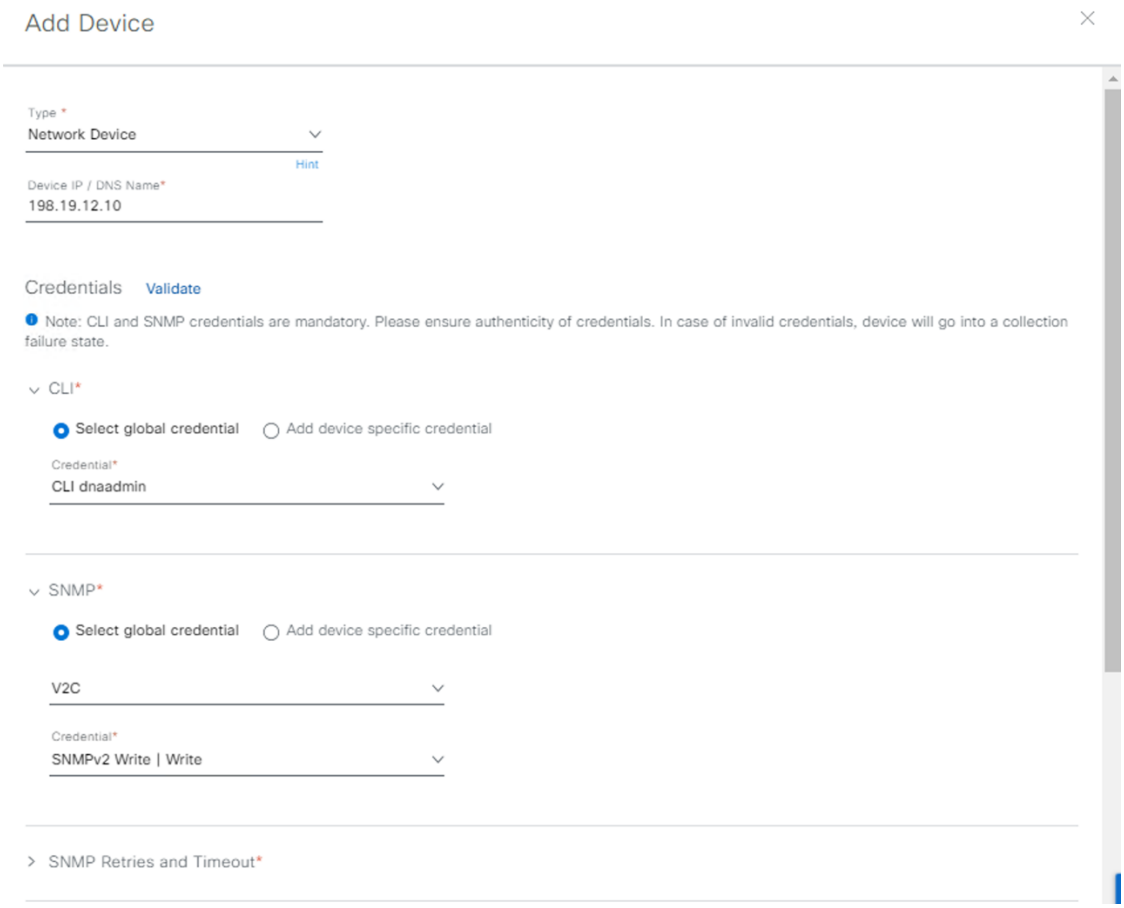
The first thing is to Discover the Anchor WLC, referred to as **WLC2-ANCHOR**

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**

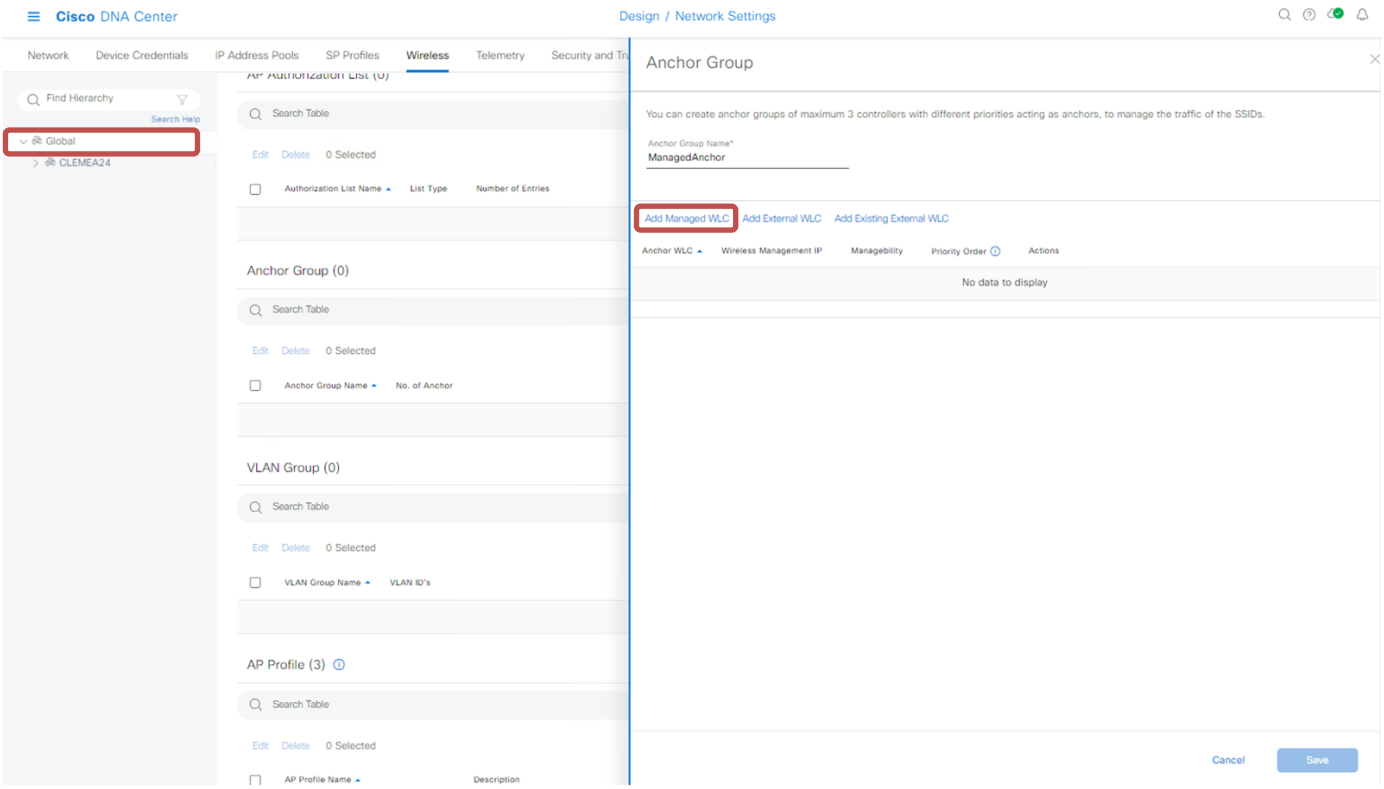
Figure 153 Add Device Details – WLC2-Anchor



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**

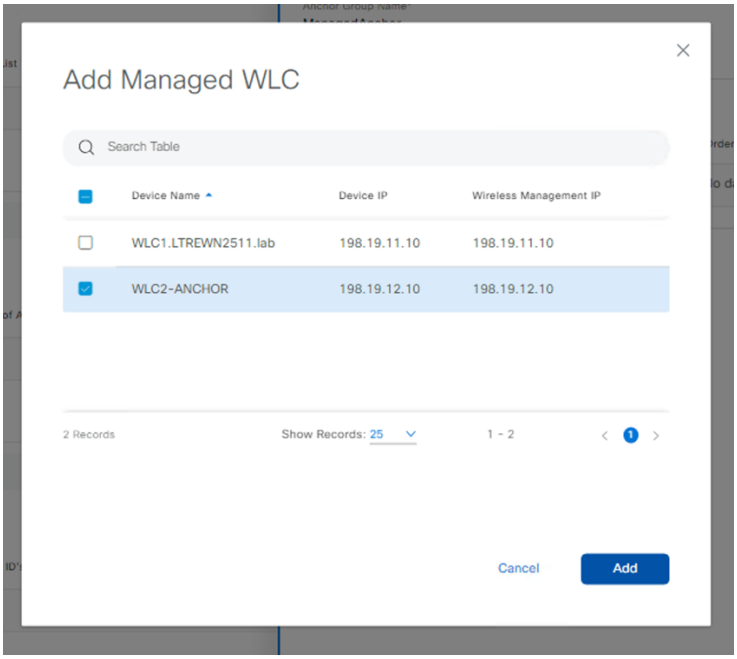
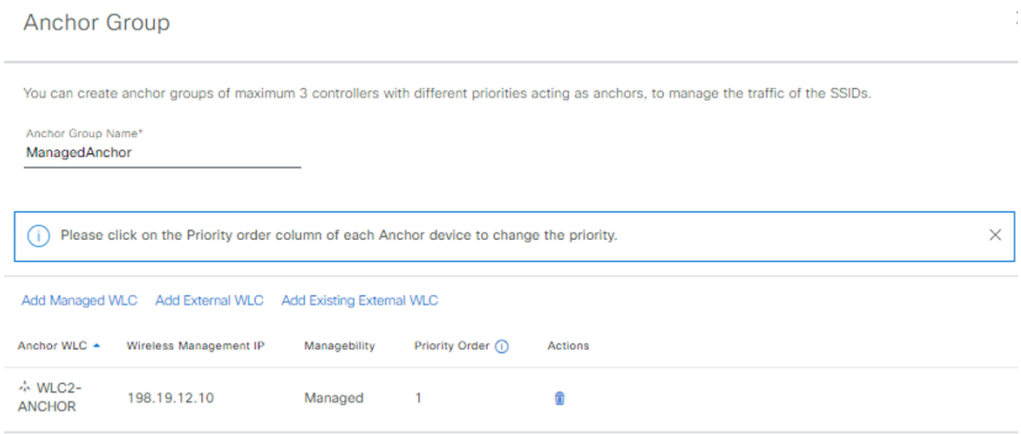


Figure 156 Anchor Group – Managed Anchor



Step 3: Edit Network Profiles

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

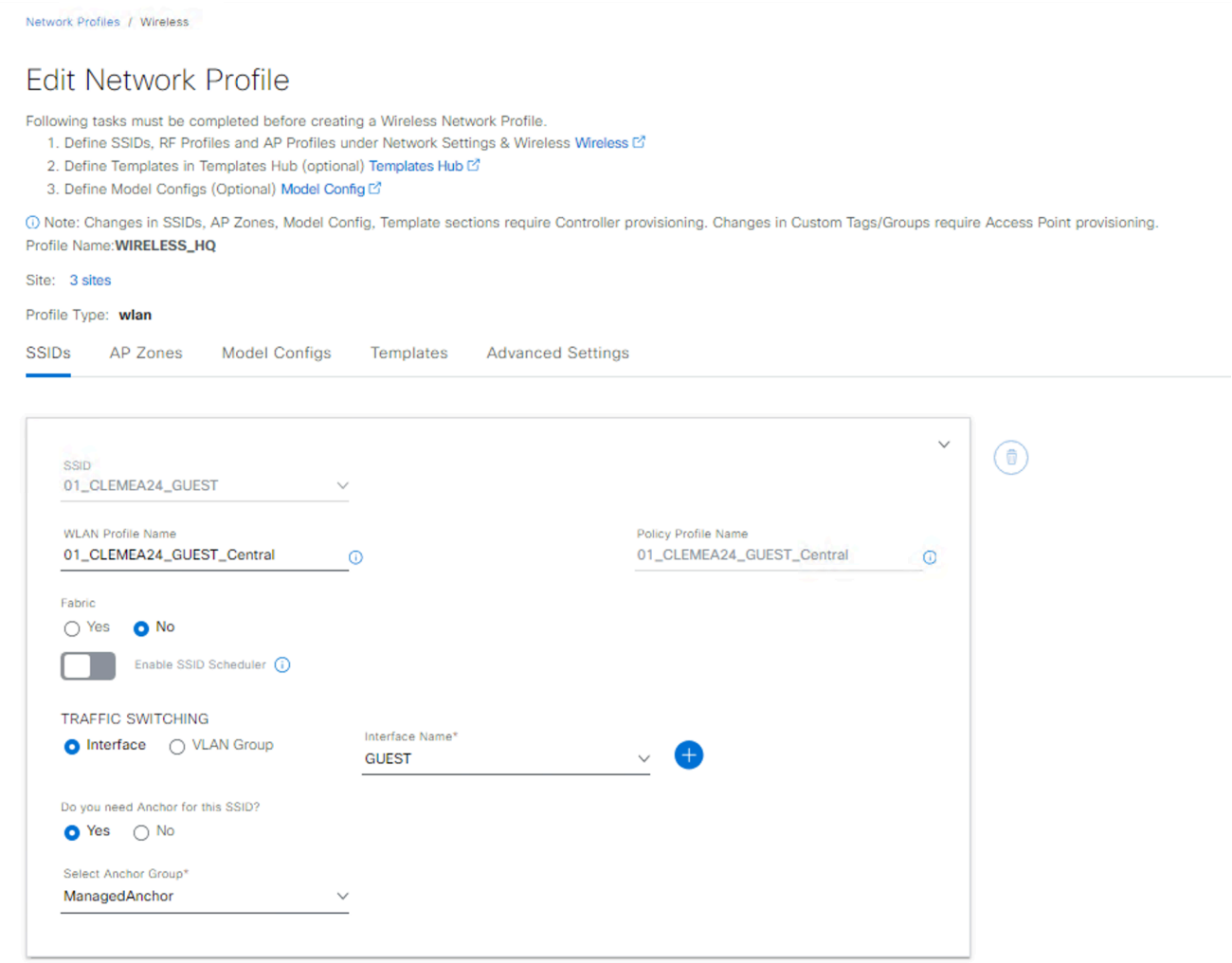
- Go to **Design > Network Profiles**, click on **WIRELESS_HQ** to edit the profile.
- In the SSIDs tab, find the XX_CLEMEA24_GUEST SSID and edit it with the follwing parameters:

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
Anchor	**Yes**
Select Anchor Group	**ManagedAnchor**

It should look like this:

Figure 157 Network Profile WIRELESS_HQ –Anchoring GUEST SSID



- 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
Anchor	**Yes**
Select Anchor Group	**ManagedAnchor**

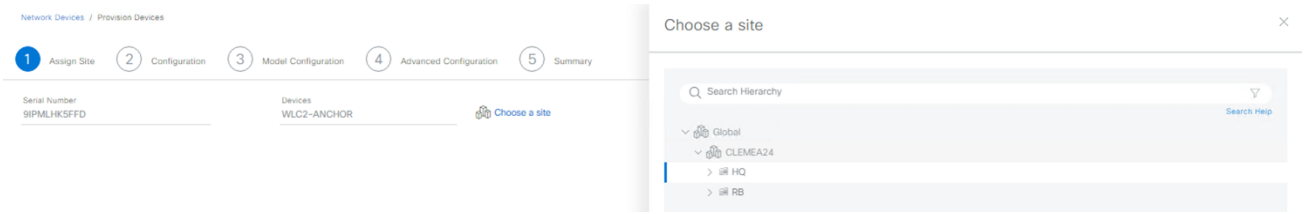
Step 4: Provision WLC2-ANCHOR

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**"

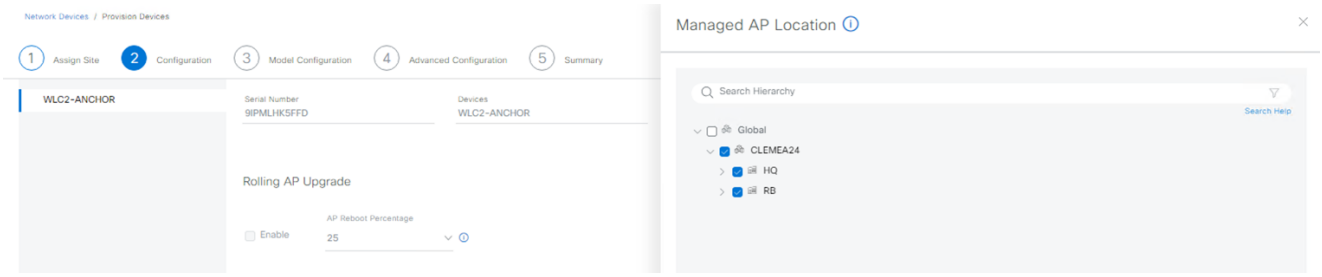
1. Select **HQ** Site, click **Next**

Figure 158 Provision WLC2-ANCHOR



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

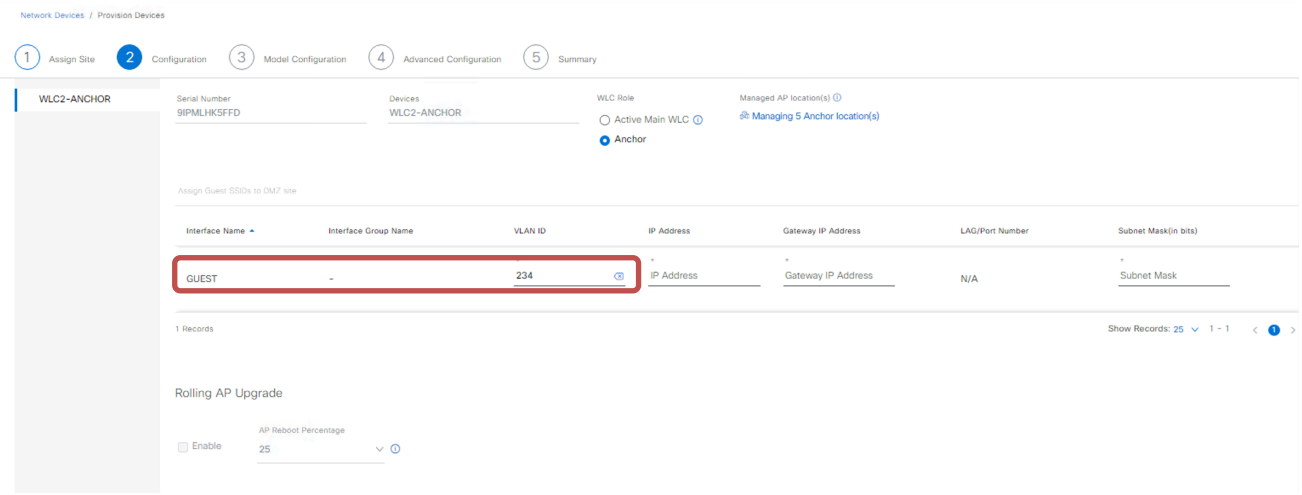
Figure 159 Provision WLC2-ANCHOR



Only buildings can be associated in this step.

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

Figure 160 Provision WLC2-ANCHOR



- 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

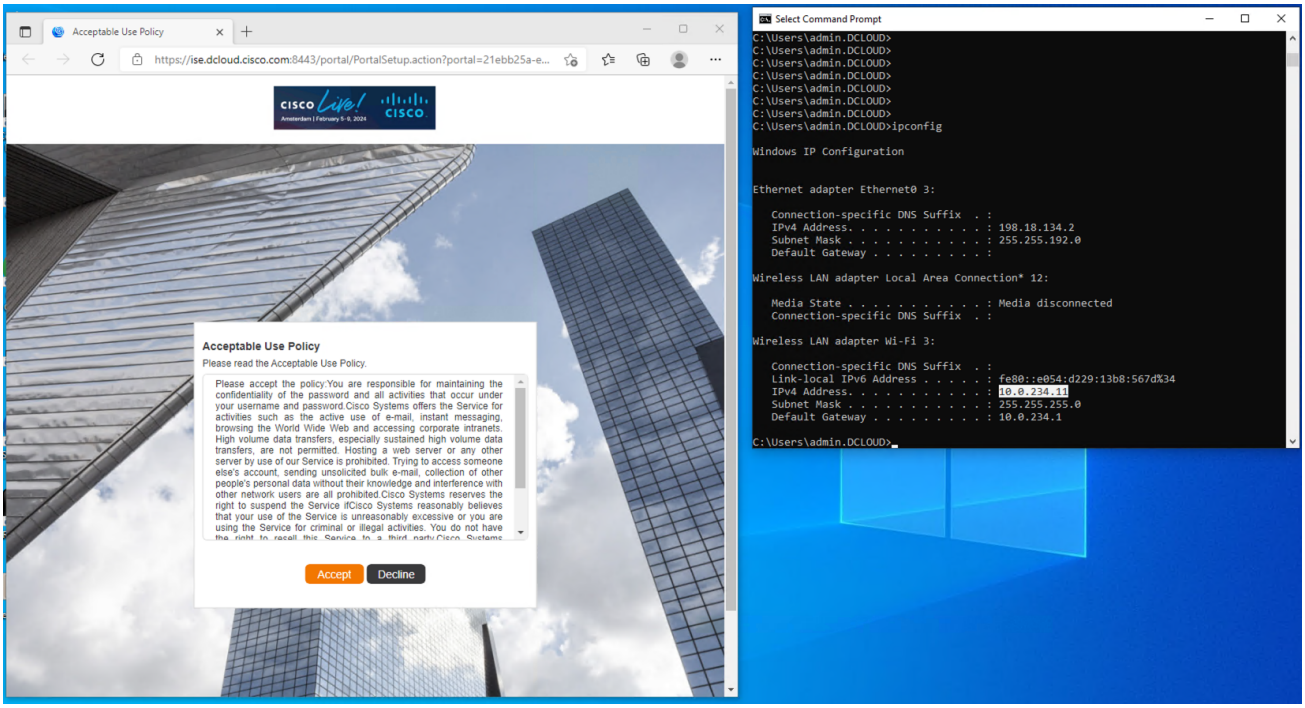
Open an RDP session to one of the Wireless Clients:

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

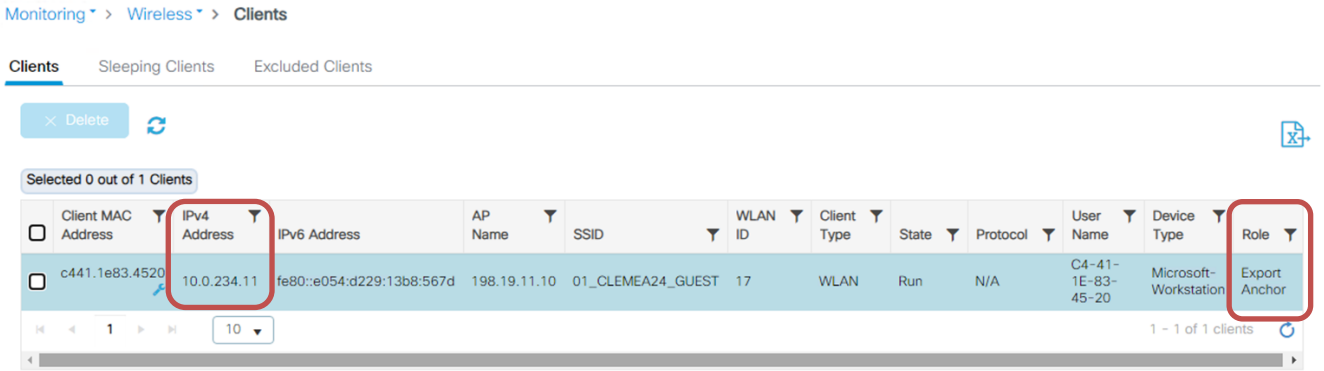


Figure 163 Verify Client Status on WLC1

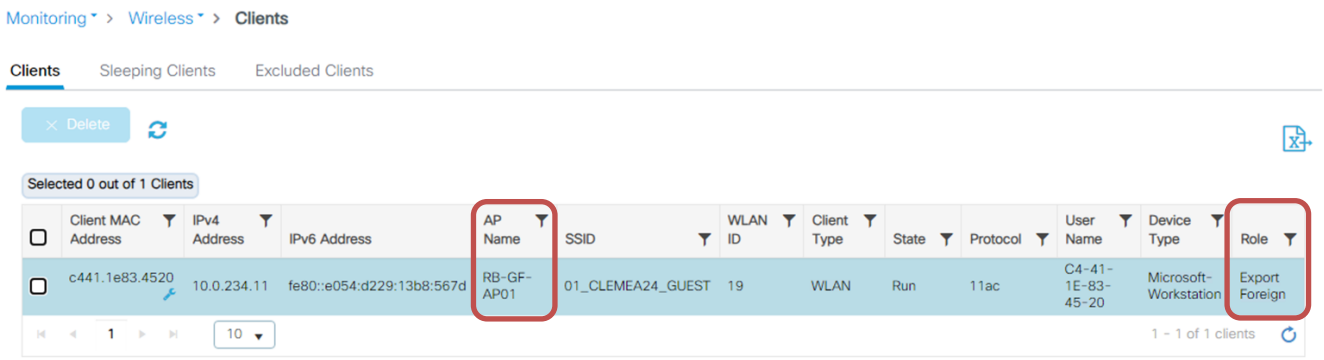
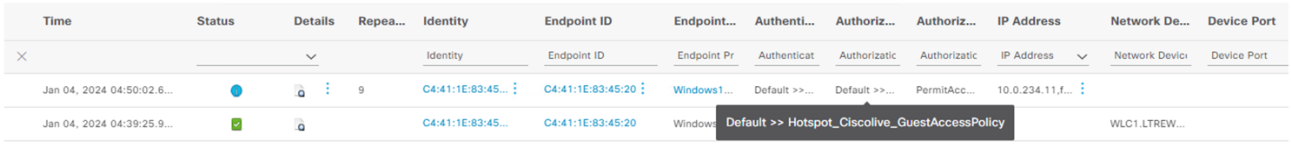


Figure 164 Verify Client Status on ISE

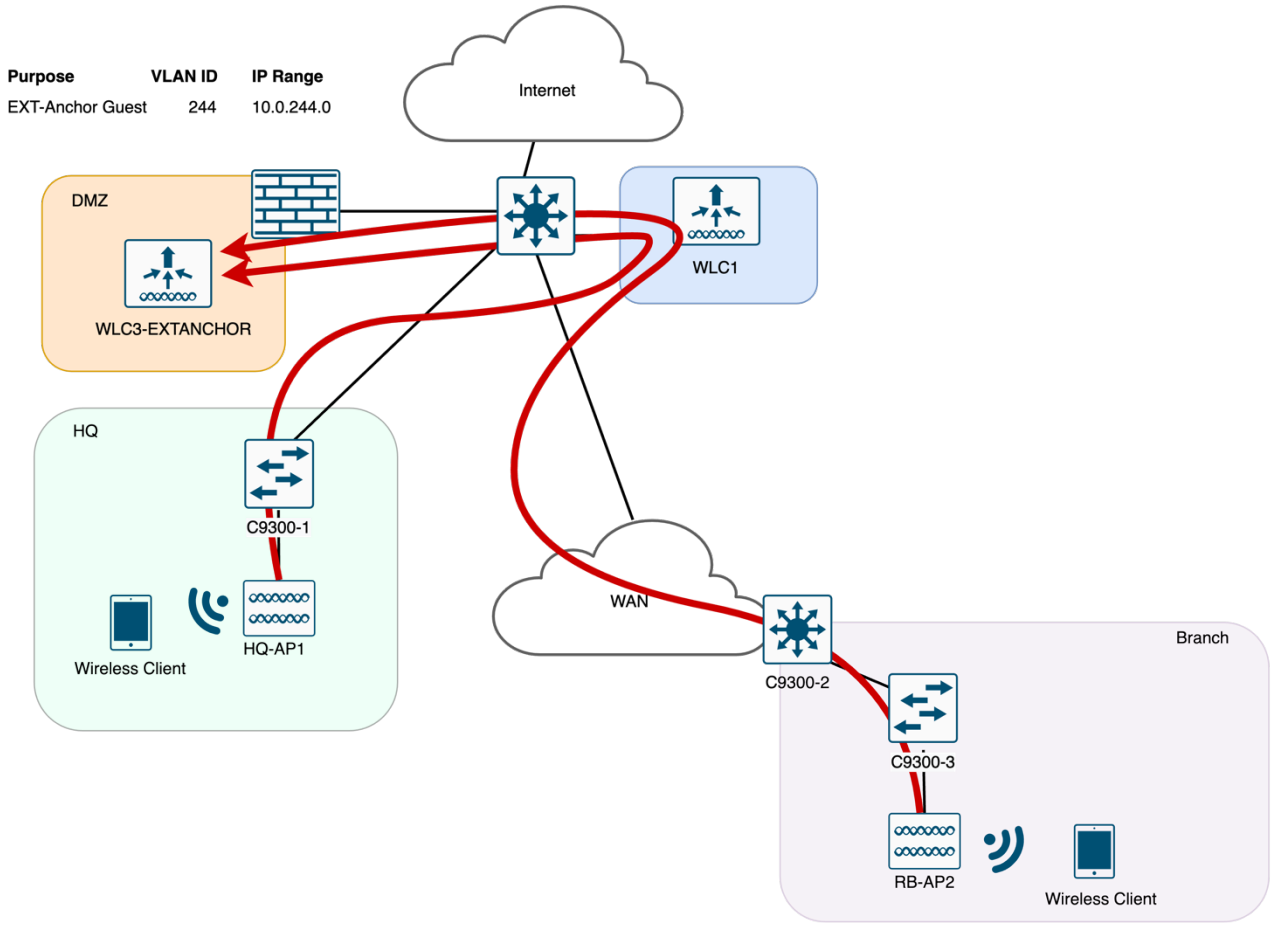


Anchoring SSID to an External Anchor WLC

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 3rd party, etc.

Figure 165 Topology – Anchoring GUEST with EXTERNAL WLC

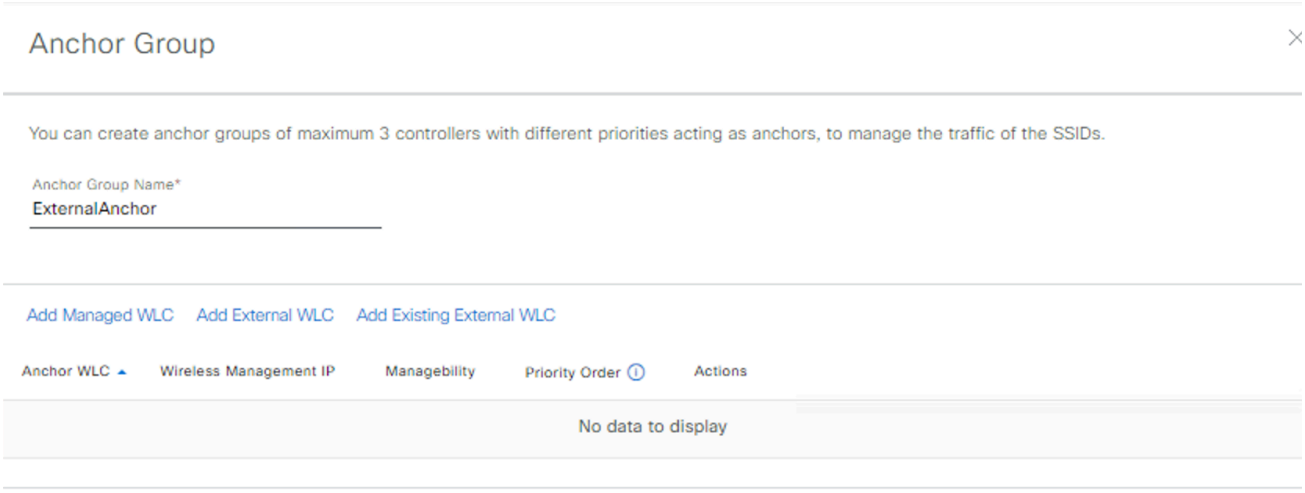


Similarly to the previous task, we start by adding the **WLC3-EXTANCHOR** to the Anchor Group Configuration.

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**

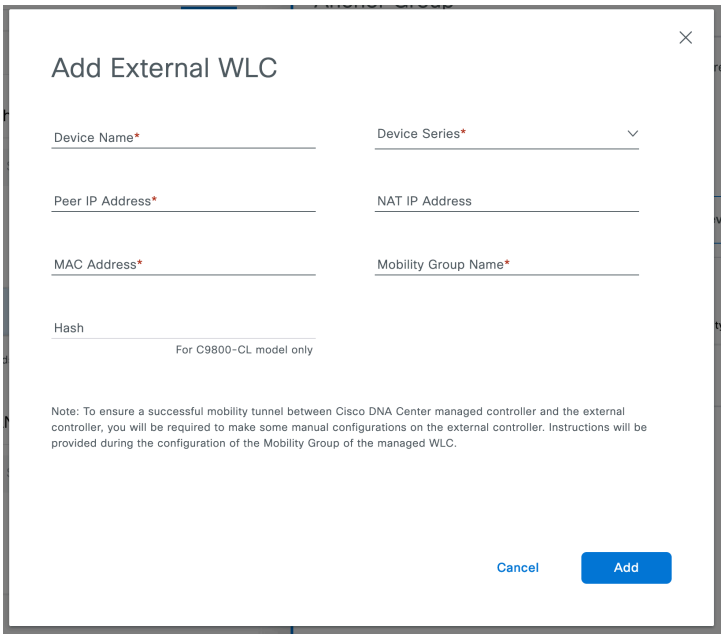
Figure 166 Anchor Group – External Anchor



Step 2: Add External WLC

- Click **Add External WLC**

Figure 167 Anchor Group – Add External Anchor



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
MAC Address	**!! To be collected via CLI**
Mobility Group Name	default
Hash	**!! To be collected via CLI**

- 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

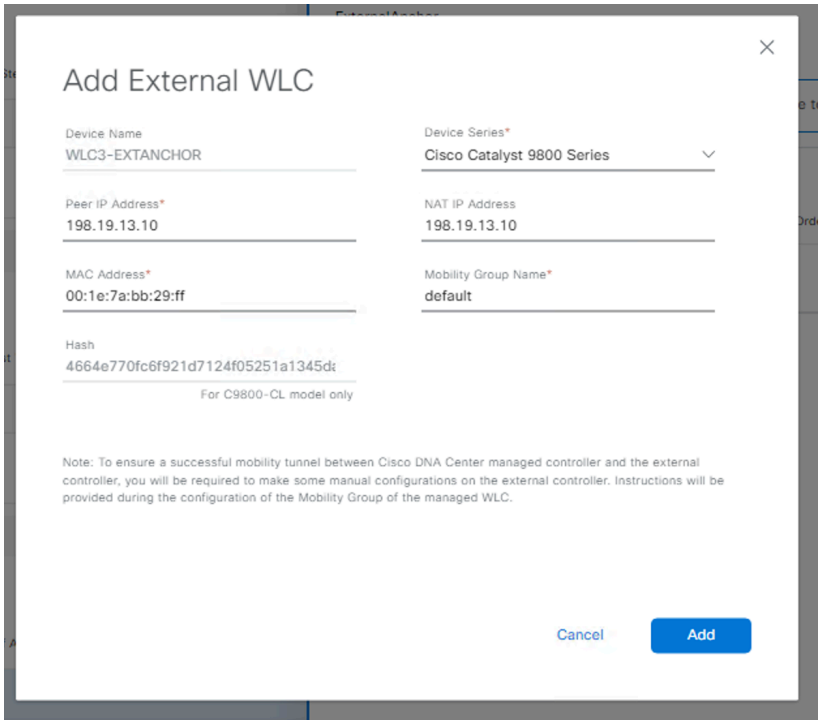
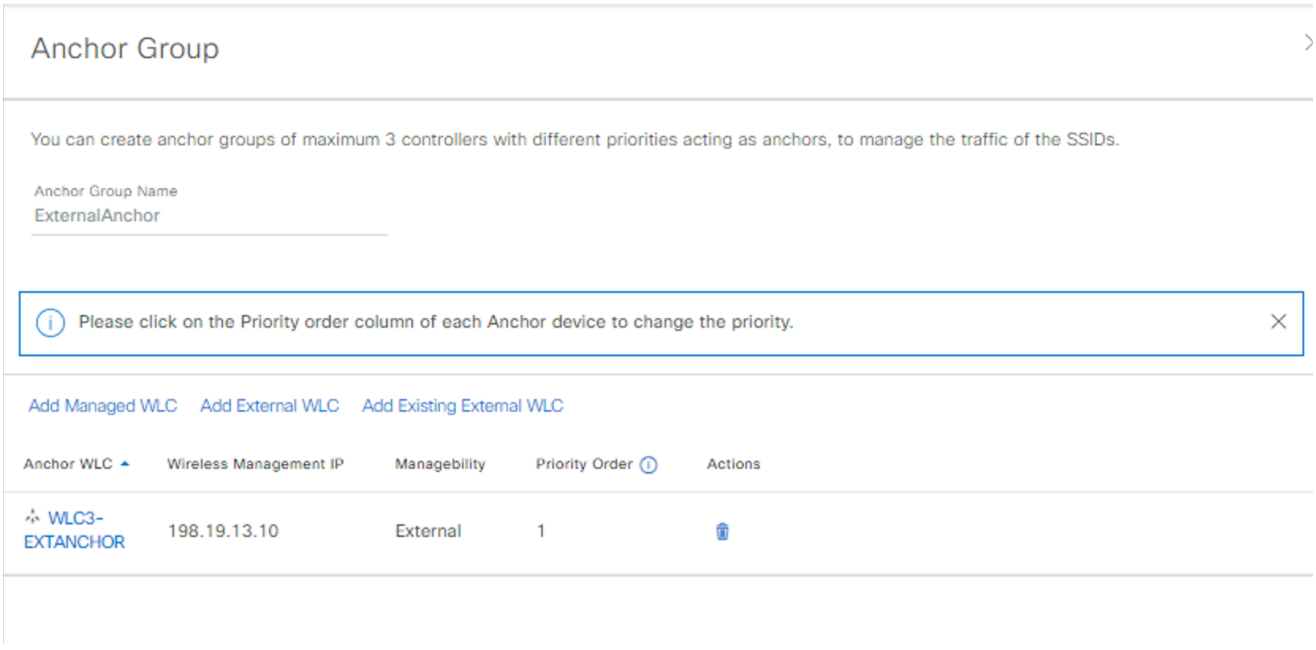


Figure 169 Anchor Group – External Anchor Summary



Step 3: Edit Network Profiles

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

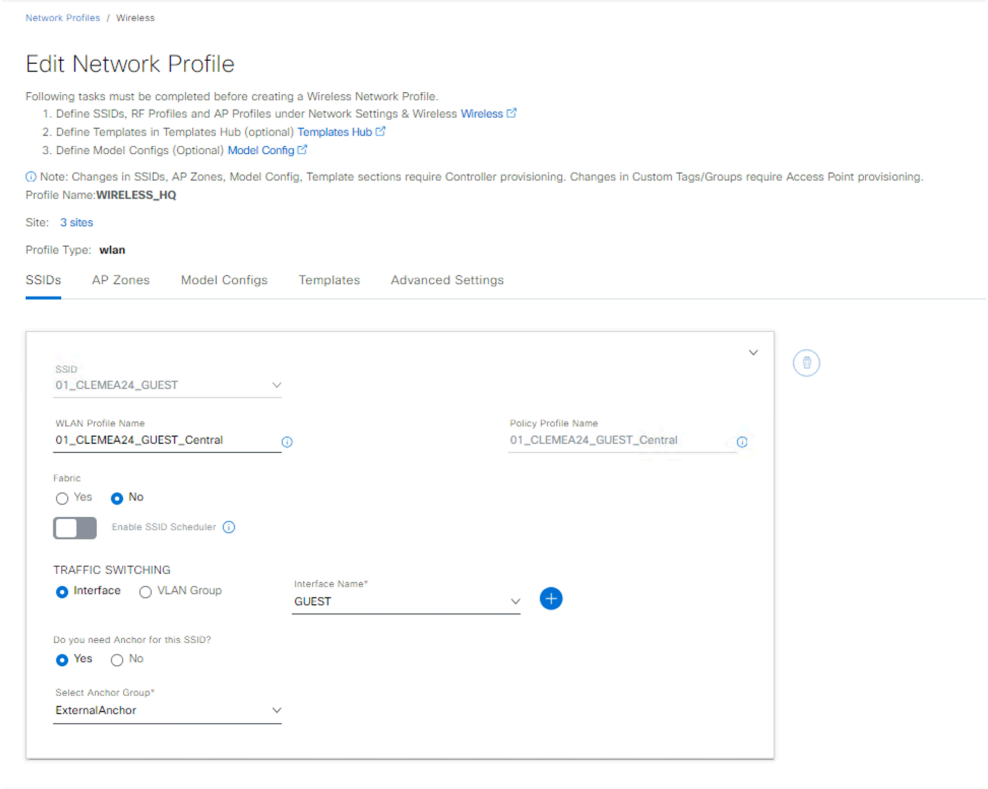
- Go to **Design > Network Profiles**, click on **WIRELESS_HQ** to edit the profile.
- In the SSIDs tab, find the XX_CLEMEA24_GUEST SSID and edit it with the follwing parameters:

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
Anchor	**Yes**
Select Anchor Group	**ExternalAnchor**

It should look like this:

Figure 170 Network Profile WIRELESS_HQ –Anchoring GUEST SSID



- 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
Anchor	**Yes**
Select Anchor Group	**ExternalAnchor**

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

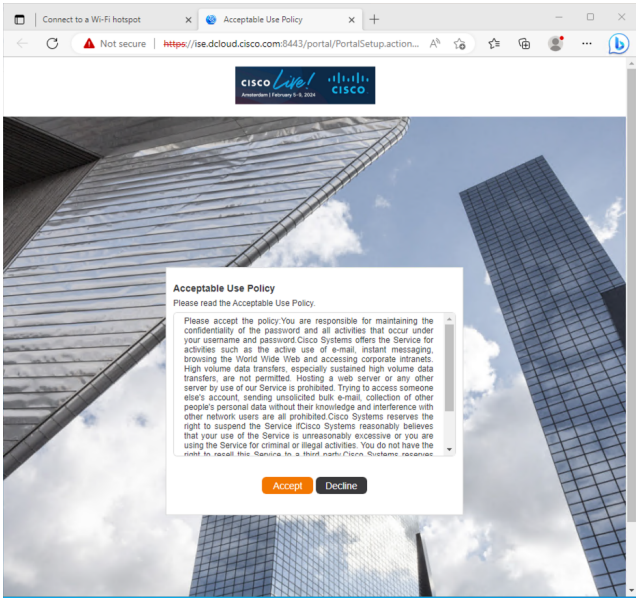
Name	IP Address	Username	Password	Preferred Access Method
Client1	198.18.134.1	DCLOUD\admin	C1sco12345	RDP
Client2	198.18.134.2	DCLOUD\admin	C1sco12345	RDP
Client3	198.18.134.3	DCLOUD\admin	C1sco12345	RDP

Client4	198.18.134.4	DCLOUD\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



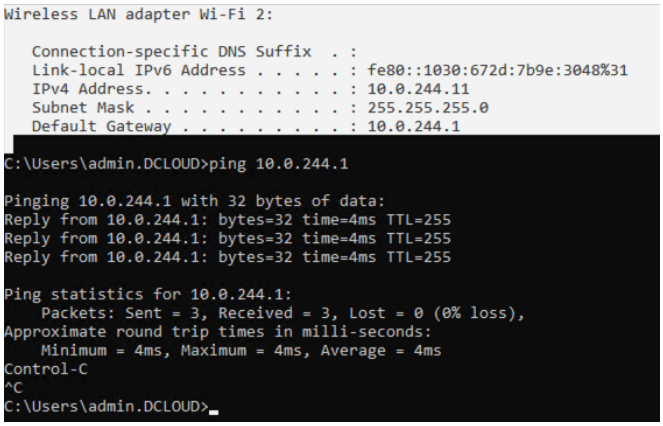


Figure 172 Verify Client Status on WLC3-EXTANCHOR

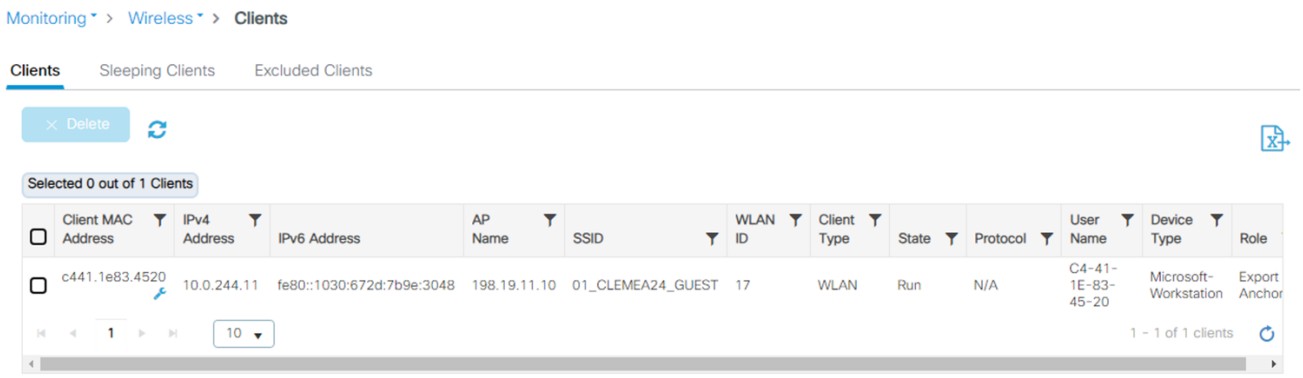


Figure 173 Verify Client Status on WLC1

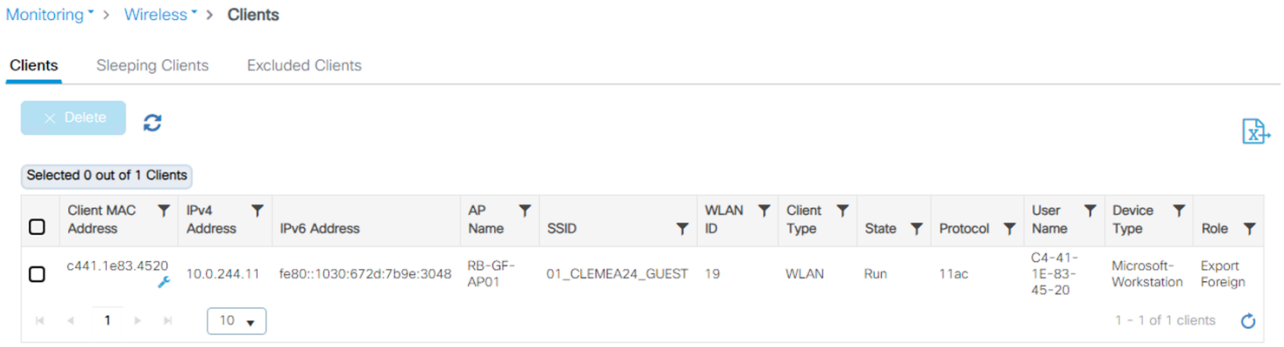
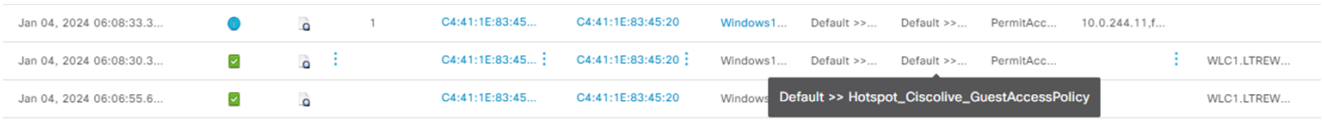


Figure 174 Verify Client Status on ISE



Task 12: Bonus Tasks – Configuring HA-SSO

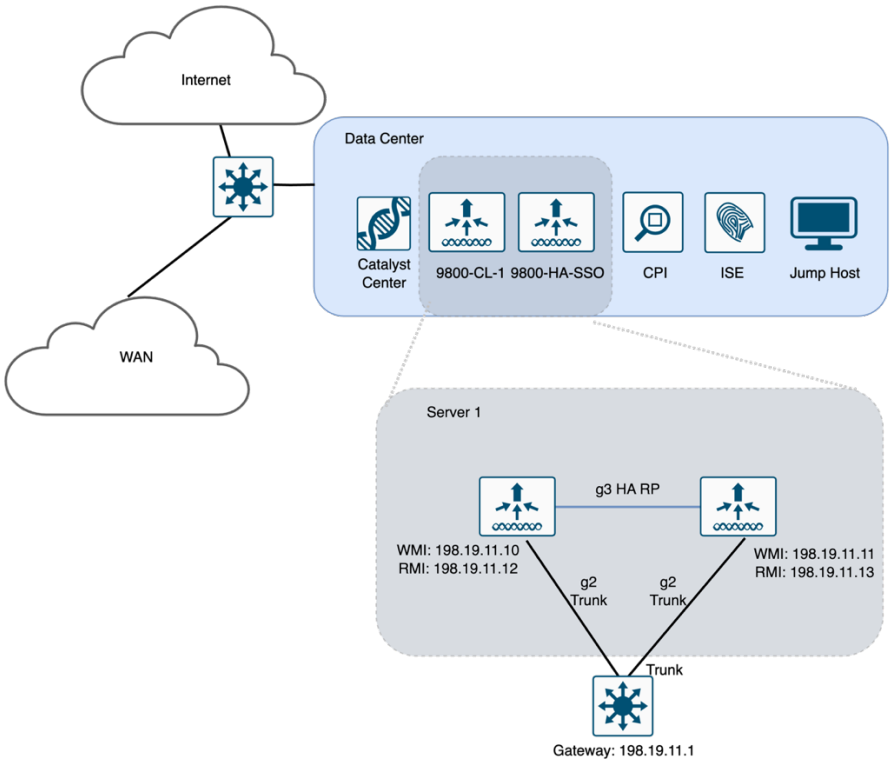
Cisco Wireless Controller High Availability (HA) can be configured through Cisco DNA Center. Currently, both the formation and breaking of wireless controller HA is supported.

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 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 the all the prerequisites except number 1, so let us begin:

Step 1: Add WLC-HASSO to Inventory

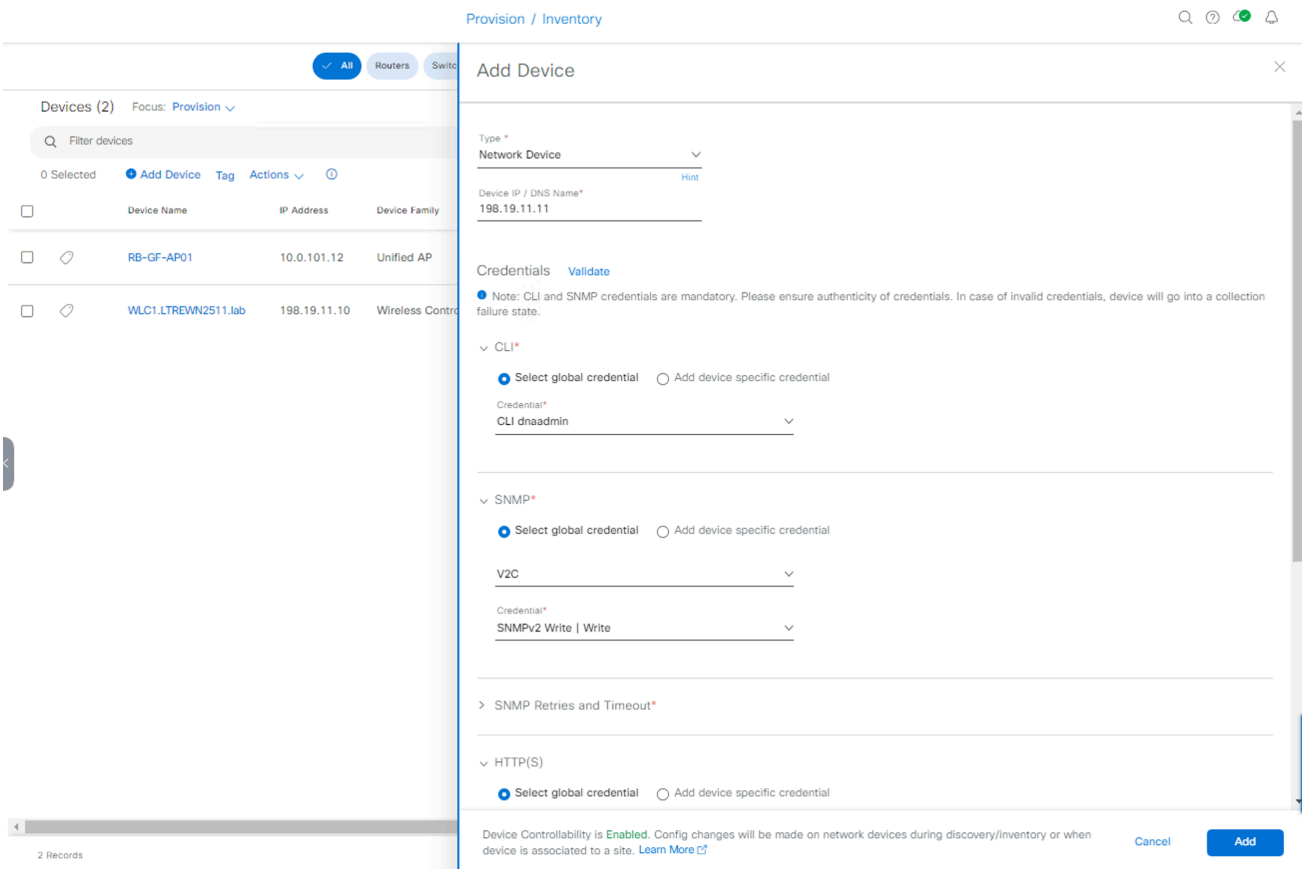
The first thing is to Discover the WLC-HASSO

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**

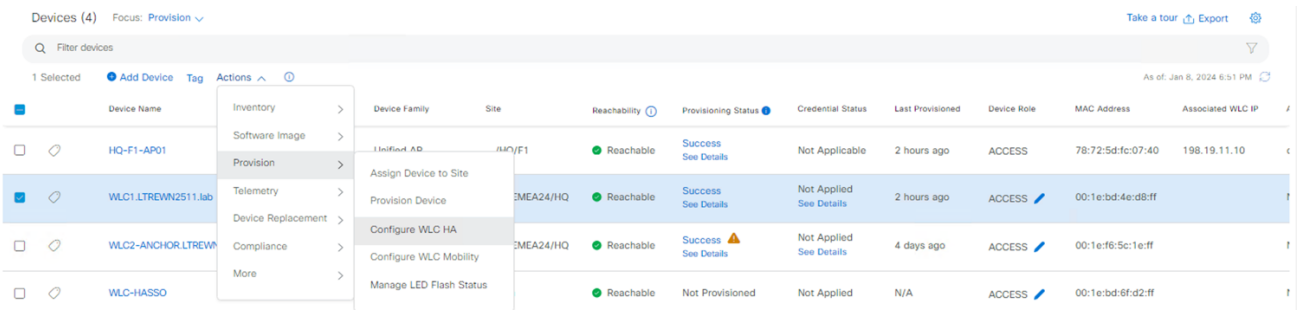
Figure 176 Add Device – WLC-HASSO



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

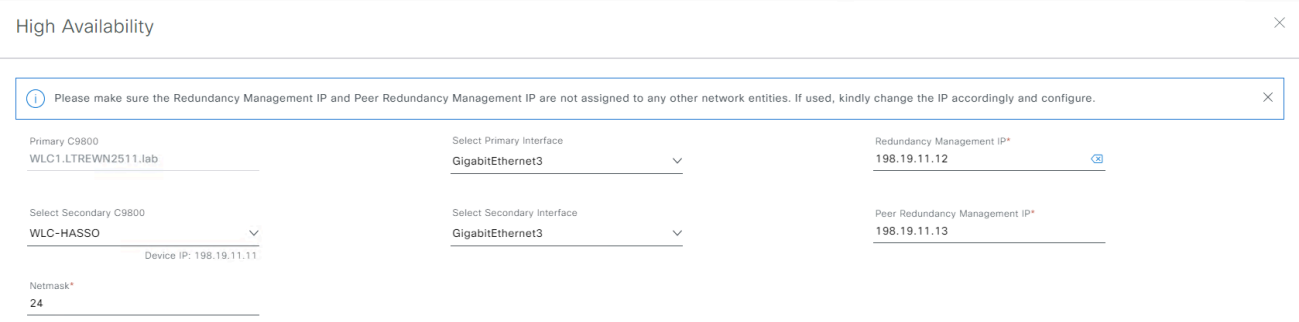


- From the Select Secondary WLC drop-down list, choose the secondary controller **WLC-HASSO**.

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:

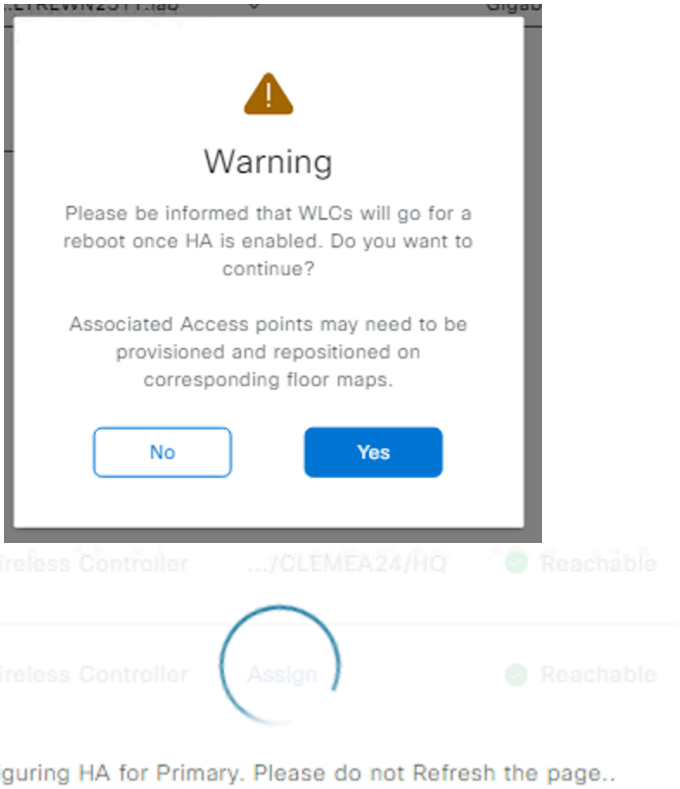
Table 32 Provision – Configure WLC HA

C9800	Interface	Redundancy Management Interface
WLC1-LTREWN2511.lab	GigabitEthernet3	198.19.11.12
WLC-HASSO	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:

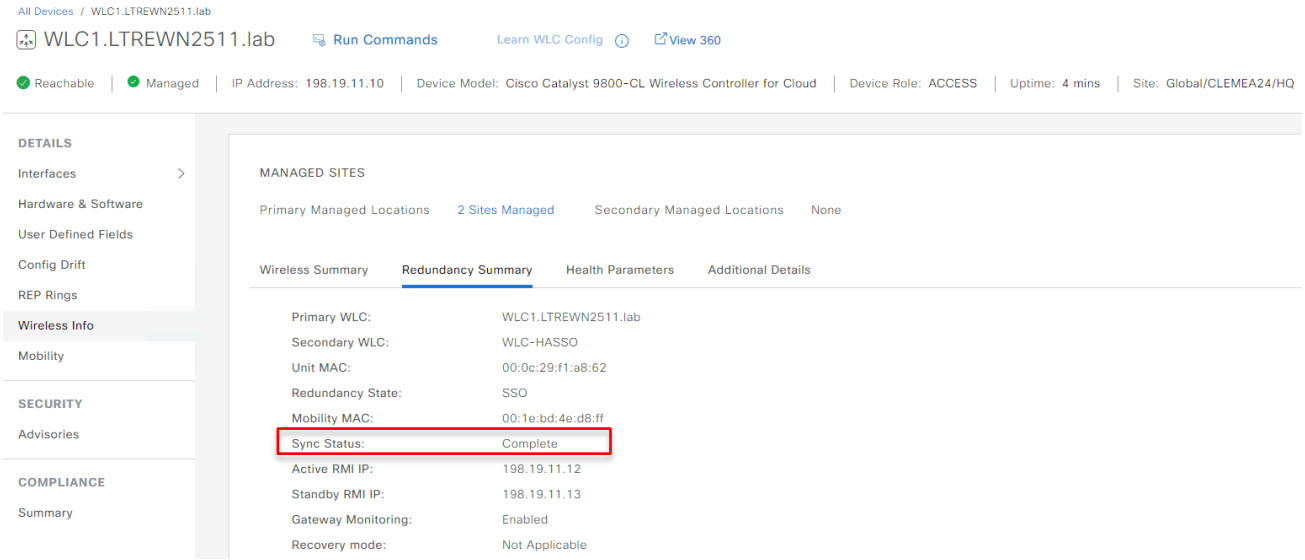
1. First, the primary wireless controller is configured.
2. On success, the secondary wireless controller is configured.
3. After the configuration is complete, both wireless controllers reboot.

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



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:
    - Cisco Catalyst 9115 Series Access Points
    - Cisco Catalyst 9117 Series Access Points
    - Cisco Catalyst 9120 Series Access Points
    - Cisco Catalyst 9130 Series Access Points
    - 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

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

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
BRKEWN-2029	Cisco DNA Center AIOps for Catalyst Wi-Fi 6/6E	Karthik Iyer	Breakout
BRKEWN-2043	Saving Energy and Money with Your Cisco Wireless Network	Simone Arena	Breakout
BRKEWN-2339	Catalyst 9800 Configuration Best Practices	Justin Loo	Breakout
BRKEWN-2667	Catalyst Wireless Supercharged by Cisco DNA Center: The Ultimate Guide to Bring Your Wireless Operation to the Next Level	Ignacio Lopez	Breakout
BRKEWN-2926	Tune your Cisco Wi-Fi designs for the most demanding clients and applications, boosted with applied AI	Jerome Henry	Breakout
BRKEWN-3004	Understanding Wireless Security and the Implications for Secure Wireless Network Design	Mark Krischer	Breakout
BRKEWN-3413	Advanced RF Tuning for Wi-Fi6E with Catalyst Wireless: Become an Expert, while getting a little help from AI	Jim Florwick	Breakout
BRKEWN-3628	Troubleshoot Catalyst 9800 Wireless Controllers	Nicolas Darchis	Breakout
LABEWN-2738	Securing Catalyst 9800 WLC Using Cisco ISE and TACACS+	Guilian Deflandre and Rasheed Hamdan	Walk-in Lab
LABEWN-1330	Powerful APs and Sustainability, how to?	Rasheed Hamdan	Walk-in Lab