



The bridge to possible

# Wireless Network Automation & Assurance with Cisco Catalyst Center

Ramkumar Chellappa, Technical Leader, TME

@ramkchel

BRKEWN-2306

CISCO *Live!*

#CiscoLive

# Cisco Webex App

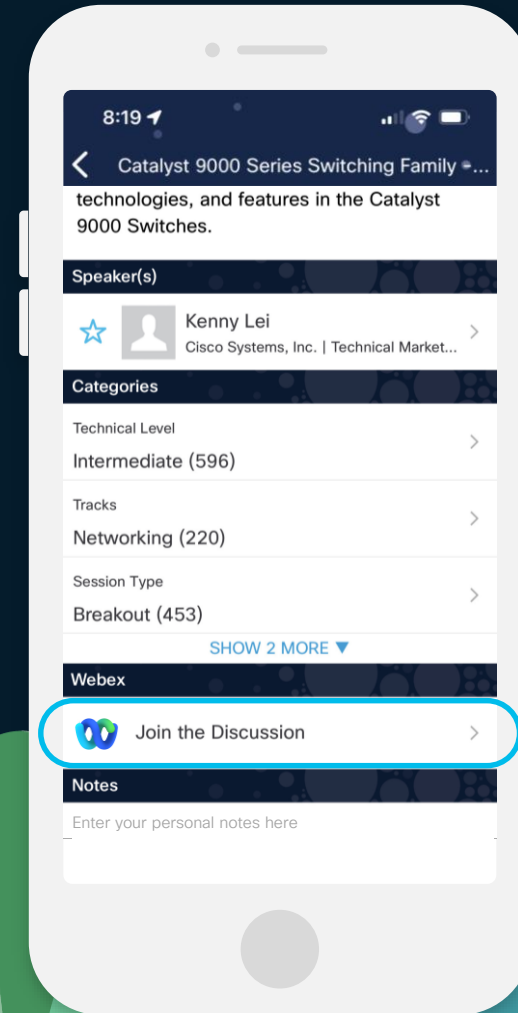
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 7, 2024.



# Ramkumar Chellappa

Technical Lead-TME for Catalyst Center NetOps



## Fields of Expertise

14+ years of Experience. TME for Wireless Automation in Catalyst Center



## Personal Life

Indian, Chennai. Married with 2 Kids



## Hobbies

Playing Cricket, Long Drives

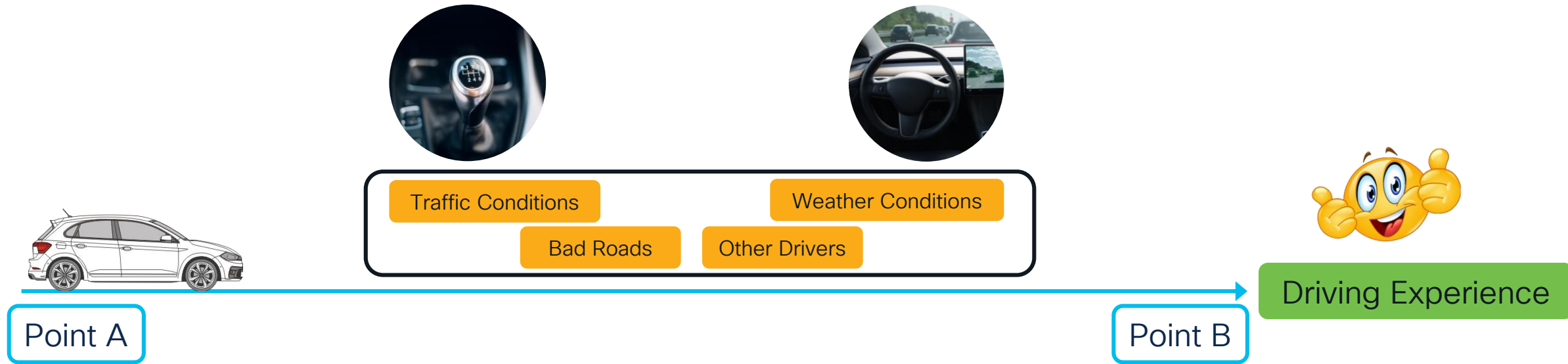
Scan to add me on LinkedIn! →

[www.linkedin.com/in/ramkumarchellappa](https://www.linkedin.com/in/ramkumarchellappa)



**CISCO** *Live!*

# My Road Trip...



## Goals:

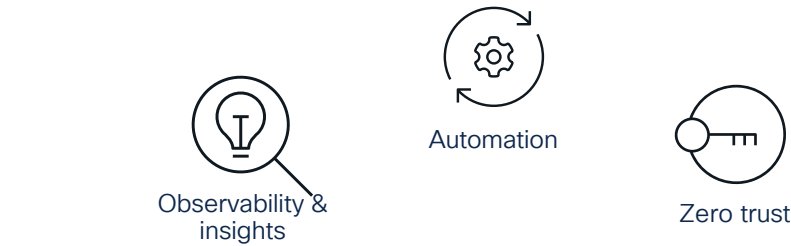
- Safety
- Fun
- Enjoyment

It's about having a fun, safe road trip with **Less driving Effort.**

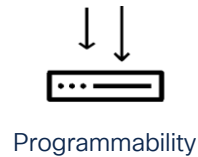


# Simplifying Network Operations

Facilitating the jobs your teams need to do



## Cisco Catalyst Center



Physical and virtual infrastructure



NetOps

**Automation and workflows** simplify building and maintaining large scale networks. AI/MR **streamlines and simplifies complex tasks**



AIOps

AI/ML and predictive insights for **proactive optimization** to ensure consistent performance and reliability and the **optimal user experience**



SecOps

AI/ML and DPI Identify and classify endpoints, enforce security policies and mitigate threats for a **complete workplace zero trust solution**



DevOps

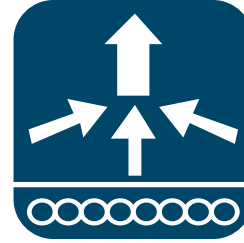
Mature APIs, SDKs, and **closed-loop integrations**, untangle the complexities of interconnecting third party systems



# Agenda

- Onboard Devices to Catalyst Center
- Manage Brownfield wireless network
- Gain visibility from your network
- Completely Automate Wireless Network

# Components



C9800\*  
17.9/17.14



C91xx  
AIR-AP-4800



Cisco Catalyst Center  
2.3.7.5

\*Local Mode / FlexConnect Mode (Central/Local Switching)

# Managed Only vs Managed & Provisioned WLC



- Wireless LAN Controller (WLC) only managed by Catalyst Center, not configured.
- Wireless configuration is done directly on the WLC.

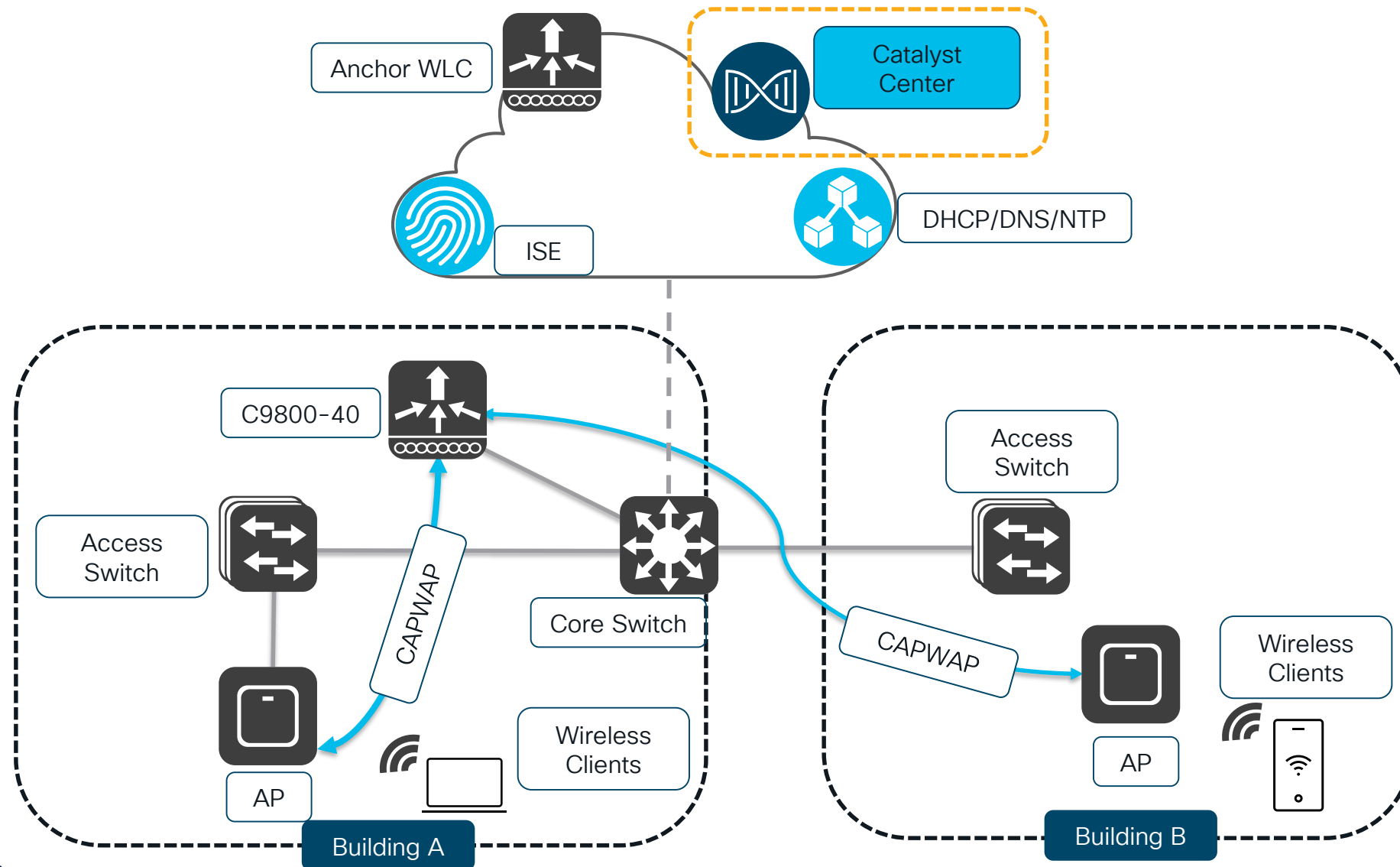


- Wireless LAN Controller (WLC) managed and configured by Catalyst Center

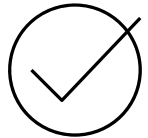
# Onboard Network Devices to Catalyst Center

CISCO *Live!*

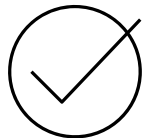
# Typical Customer Network



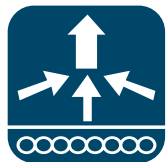
# Prerequisites for Onboarding



CLI Credentials & NETCONF enabled



Catalyst Center Enterprise IP / VIP allowed in SNMP ACL list



UDP: 161  
TCP: 22/830



Catalyst Center Discover Devices admin

## Provide Credentials

Global credentials are provided only for ease of use when entering credentials. At the device level, only the device-specific credentials are saved. The device-to-global-credentials association isn't saved.

Next, confirm the credentials that Catalyst Center uses for the devices it discovers. At least one CLI credential and one SNMP credential are required. You can have a maximum of five global credentials and one task-specific credential for each type. Optionally, you can update SNMP properties and protocols used for CLI.

- SNMPv2c Read (1)
- SNMPv2c Write (0)
- SNMPv3 (0)
- NETCONF (1)**
- Advanced Settings
  - HTTP(S) Read (0)
  - HTTP(S) Write (0)
  - Protocol Order

If your network contains IOS XE-based wireless controllers, please enter the port that should be used for discovery and the enabling of wireless services on these controllers. Select from existing ports or add new ones. You can add either a job specific port or a global port.

We recommend using port number 830. **Do not use standard ports like 22, 80, 8080.**

**EXISTING GLOBAL NETCONF PORT**

- 830
- [+ Add NETCONF Port](#)

Exit Review Back Next

# Device Onboarding Process- Wireless Discovery



```
<..config snip..>
SVI
Credentials
NETCONF
SNMP
```



Network Administrator onboards devices in Catalyst Center

Catalyst Center Reference / Discovery Details

All Discoveries

POD4- Discovery Date - Mar 13, 2024 12:05 PM (6)

Completed Type: Range Retry Count: 3 Protocol Order: Telnet Total Time: 0 minutes 11 seconds [View all data](#)

DEVICE SUMMARY

6	6	0	0
Discovered	Successful	Failed	Discarded

Search Table

IP Address	Device Name	Status	ICMP
192.168.4.1	POD4-Core-ISR	✓	✓
192.168.4.2	POD4-3850-Distribution	✓	✓
192.168.4.3	POD4-C9300-Access2	✓	✓
192.168.4.4	POD4-C9300-Access1.tmelab.com	✓	✓
192.168.4.5	POD4-C9800-40	✓	✓
192.168.4.7	POD4-C9800-CL1	✓	✓

6 Record(s)

Catalyst Center Provision / Inventory

To provision subscriptions on devices that have not been discovered with NETCONF, rediscover the devices with NETCONF, and update the Telemetry Settings

Global ✓ All Routers Switches Wireless Controllers Access Points Sensors

Devices (20) Focus: Inventory

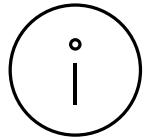
Click here to apply basic or advanced filters or view recently applied filters

0 Selected [Tag](#) [Add Device](#) [Edit Device](#) [Delete Device](#) [Actions](#)

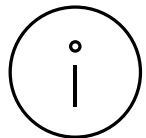
Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability
	POD4-Core-ISR	192.168.4.1	Cisco	✓ Reachable	4 alerts	✓ Managed
	POD4-C9800-CL1.tmelab.com	192.168.4.7	Cisco	✓ Reachable	1 alert	✓ Managed
	POD4-C9800-40.tmelab.com	192.168.4.5	Cisco	✓ Reachable	2 alerts	✓ Managed
	POD4-C9300-Access2	192.168.4.3	Cisco	✓ Reachable	2 alerts	✓ Managed
	POD4-C9300-Access1.tmelab.com	192.168.4.4	Cisco	✓ Reachable	1 alert	✓ Managed
	POD4-AP3	192.168.4.74	NA	✓ Reachable	⚠ Not Scanned	✓ Managed
	POD4-AP2	192.168.4.13	NA	✓ Reachable	⚠ Not Scanned	✓ Managed



# Tips & Tricks



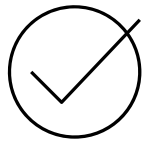
NETCONF not enabled on the devices



AAA method list (default) not configured

The screenshot shows the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'Provision / Inventory'. Below the navigation bar, there are filters for 'Global' and various device types: 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. The main content area displays a table of devices. The table has columns for 'Tags', 'Device Name', 'IP Address', 'Vendor', 'Reachability', 'EoX Status', 'Manageability', and 'Compliance'. One device is listed: 'POD4-C9800-40' with IP '192.168.4.5', Vendor 'Cisco', Reachability 'Reachable', EoX Status 'Not Scanned', and Manageability 'Managed Netconf Authentication Failure'. A yellow box highlights the 'Managed Netconf Authentication Failure' status. Below the table, there is a log entry: '\*Apr 29 10:03:39.020: %DMI-5-AUTHORIZATION\_FAILED: Chassis 1 R0/0: dmiauthd: User 'ciscodna' from 172.100.1.53:56656 was not authorized for netconf over ssh.' The bottom of the page shows '1 Record(s)' and 'Show Records: 25'.

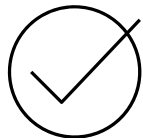
# Tips & Tricks

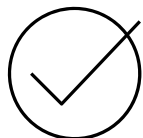


Netconf authentication and authorization uses the default group

```
C9800-Virtual#sh run aaa
!  
aaa authentication login default group  
dnac-network-tacacs-group local  
  
aaa authorization exec default group  
dnac-network-tacacs-group local if-  
authenticated
```

# Tips & Tricks

 Netconf authentication and authorization uses the default group

 AAA method list for programmatic interfaces starting 17.9

```
C9800-Virtual#sh version  
Cisco IOS XE Software, Version 17.09.03
```

```
C9800-Virtual#sh run aaa  
yang-interfaces aaa authentication  
method-list <mymethodlist>  
  
yang-interfaces aaa authorization method-  
list <mymethodlist>
```

# Prime to Catalyst Center Readiness Assessment PDART Tool

Cisco PDART - A Cisco DNA Center Readiness tool for the Cisco Prime Infrastructure

Translations Download Print

Updated: August 8, 2021 Document ID: 217059

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used

#### Tool Requirements

#### How to Execute the Tool

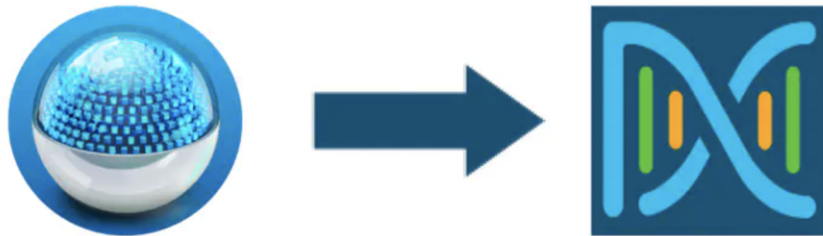
- Option 1: Execute the PDART executable from CLI
- Option 2: Execute the PDART via Updated Bundle File (UBF patch)

#### Sample Report

#### Issues with the tool

## Introduction

The Cisco PDART (Cisco Prime Infrastructure Cisco DNA Center Assessment & Readiness Tool) analyzes a Cisco Prime Infrastructure deployment and assesses whether Cisco DNA Center supports the current deployment.

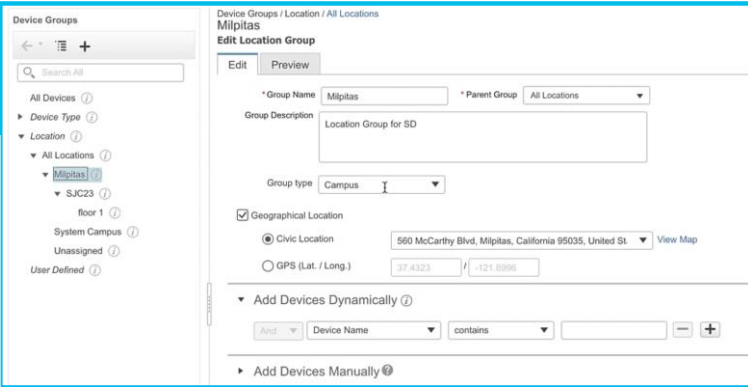


The PDART assesses the Cisco Prime Infrastructure from the following perspectives:

Cisco DNA Center Ready			
Current Cisco Prime Infrastructure Version : 3.9.0			
Recommended Cisco DNA Center Version : 2.1.2.6			
Devices			
518	517	0	1
Total	Supported	Requires SW Upgrade	Unsupported
Use Cases			
48	26	8	13
Used / In Use	Supported	Unsupported	Roadmap
Reports			
0	0	0	0
Used / In Use	Supported	Unsupported	Roadmap
Scale			
Professional Appliance in Use		DN2-HW-APL Recommended Appliance	
Platform			
csg-bgl18-00a-pi01 Hostname		7 Total Checks Run	

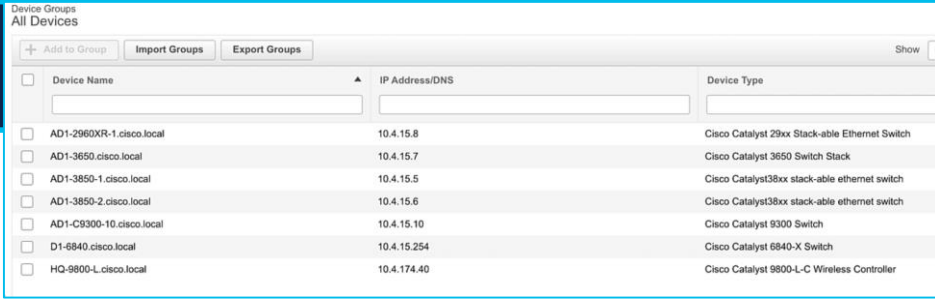
<https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/prime-infrastructure/217059-cisco-pdart-a-cisco-dna-center-readine.html>

# Prime Data Migration Tool



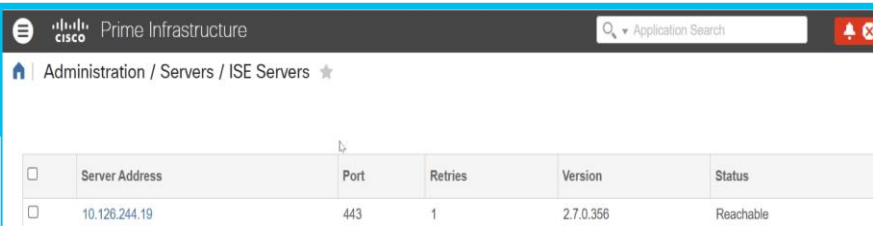
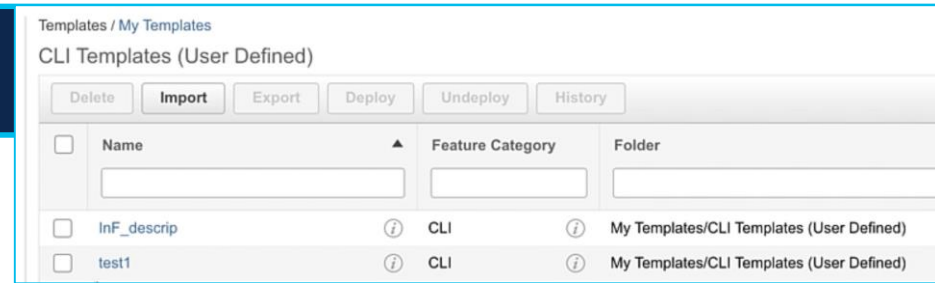
Site Hierarchy

Inventory



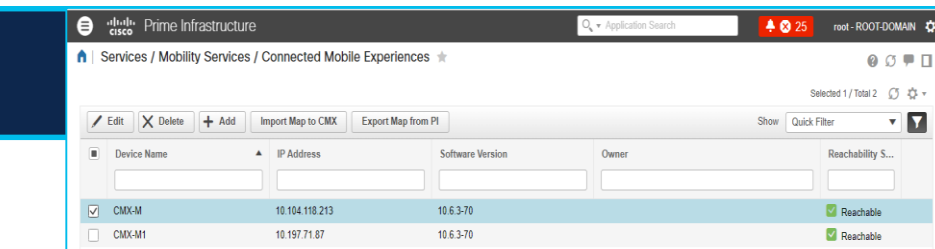
Maps

Templates



ISE

CMX



# Tips & Tricks- Templates Migration

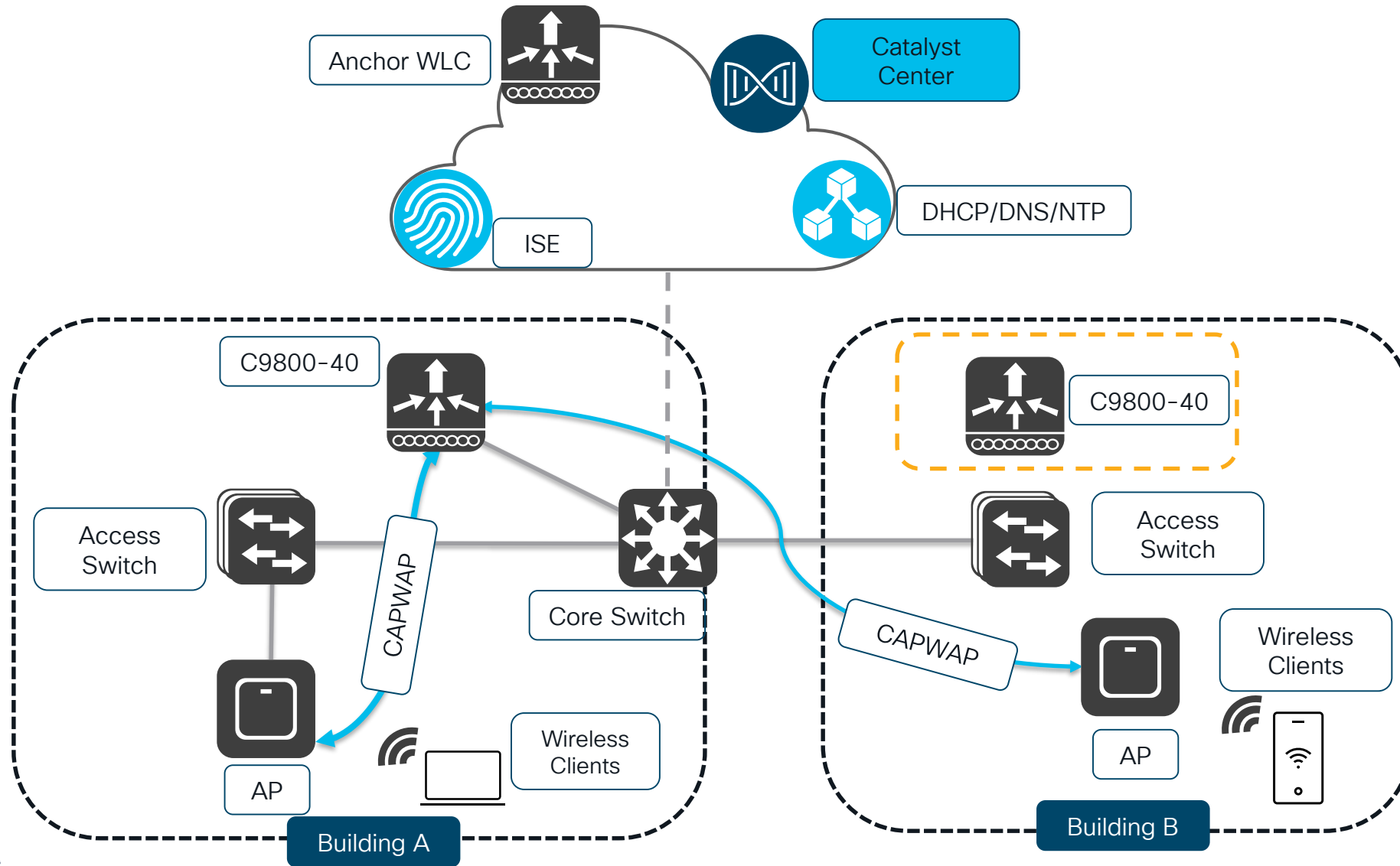
✓ User Defined CLI templates with variables and composite templates

i System Defined Templates- **Not Migrated**

i Migrated Templates moved to Design > CLI Templates > Prime Migrated Templates

The screenshot shows the Cisco Prime Infrastructure interface for migrating CLI templates. At the top, a progress bar indicates five steps: 1. Add Cisco DNA Center Server, 2. Sync Settings, 3. Select Groups, 4. ISE & CMX Server, and 5. Select CLI Templates. The main interface displays the 'CLI Templates' section with a search bar and a list of templates. A 'Save as New Template' dialog box is open, showing the 'Template Basic' section with fields for Name (TemplateCLI1), Device Type (Routers), and Author (root). A 'Save Template' dialog box is also open, showing the 'Folder' dropdown set to 'CLI Templates (User Defined)'. The 'Template Detail' section is visible at the bottom, including 'CLI Content', 'Form View', and 'Add Variable' options.

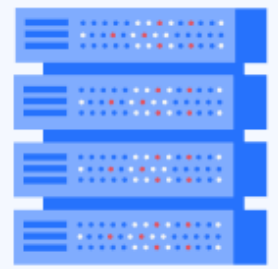
# Device Onboarding Process- WLC PnP



# Device Onboarding Process- PnP

Device validates server's location and establishes a communication with the server

DHCP Server



Catalyst Center  
(PnP Server)



```
<..snip..>
CISCO_PNP.pnpserver
"5A;B2;K4;I10.104.49.27;J80"
<..snip..>
```

IP Address  
10.104.49.27



Day 1

- Remote Installer
- Mount and cable devices
  - Power-on

Network Devices / Plug and Play

WLC (192.168.1.251)  
Serial Number: FCL24140056 Site: Global/Chennai/POD1-Building As of: a minute ago

SUDI Authenticated

Status Device added to Site Global/Chennai/POD1-Building

Details History Configuration TW 0/0/0

History (29) As of: May 7, 2024 2:04 PM

Status	Date Updated	Details	Work Item Details
✓	May 07, 2024 1:46:36 PM	Deleted Device from PnP	NA
✓	May 07, 2024 1:27:00 PM	Task: System Task Completed	Info
✓	May 07, 2024 1:26:39 PM	Executing System Workflow to Initialize Device	NA
✓	May 07, 2024 1:26:39 PM	Executing Task: System Task	NA
✓	May 07, 2024 1:26:24 PM	Device Authenticated Successfully	NA
✓	May 07, 2024 1:26:17 PM	Secured Device	NA
✓	May 07, 2024 1:26:00 PM	Securing Device	NA



> Network Plug and Play Overview

Device Status **All (2)** Unclaimed (2) Error (0) Provisioned (0)

Devices (2) Focus: Default

Auto-refresh: 30 s

Search PnP devices

0 Selected Actions Add Devices

As of: May 26, 2024 7:45 AM Refresh

<input type="checkbox"/>	#	Device Name	Serial Number	Product ID	Last Contact	State	Onboarding Progress	IP Address	MAC Address	Source
<input type="checkbox"/>	1	AP5CE1.7628.EE30	FGL2420LGCG	C9120AXI-D	May 26, 2024 7:45:33 AM	Unclaimed	Device is ready to be claimed.	192.168.10.7	5C:E1:76:28:EE:30	Network
<input type="checkbox"/>	2	WLC	FCL24140056	C9800-L-C-K9	May 26, 2024 7:45:21 AM	Unclaimed	Device is ready to be claimed.	192.168.1.252	-	Network

2 Record(s)

Show Records: 25 1 - 2

> Network Plug and Play Overview

Device Status **All (2)** Unclaimed (1) Error (0) Provisioned (1)

Devices (2) Focus: Default ▾

Auto-refresh: 30 s ▾ ⚙️

🔍 Search PnP devices

0 Selected Actions ▾ + Add Devices

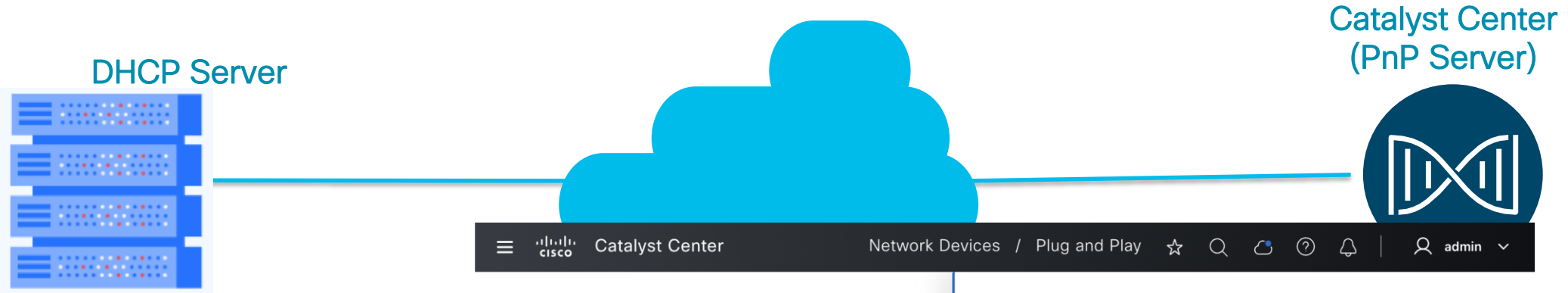
As of: May 27, 2024 4:17 AM 🔄 Refresh

<input type="checkbox"/>	#	Device Name ⓘ	Serial Number	Product ID	Last Contact	State ⓘ	Onboarding Progress ⓘ	IP Address	MAC Address ⓘ	Source ⓘ
<input type="checkbox"/>	1	AP5CE1.7628.EE30	FGL2420LGCG	C9120AXI-D	May 27, 2024 4:16:09 AM	Unclaimed	🔄 Device is ready to be claimed.	192.168.10.7	5C:E1:76:28:EE:30	Network
<input type="checkbox"/>	2	WLC	FCL24140056	C9800-L-C-K9	May 26, 2024 8:07:01 AM	Provisioned	✅ Provisioned	192.168.1.12	-	Network

2 Record(s)

Show Records: 25 ▾ 1 - 2 < 1 >

# Device Onboarding Process- WLC PnP



The screenshot shows the Catalyst Center web interface. The top navigation bar includes the Cisco logo, "Catalyst Center", and "Network Devices / Plug and Play". The main content area is titled "Add a Single Device" and contains the following form fields:

- Serial Number\*: FCL24140056 (Info link)
- Product ID\*: C9800-L-C-K9 (dropdown menu, Info link)
- Device Name: POD1-C9800-LC (text input, Info link)

Below the form, there is a section for SUDI authorization:

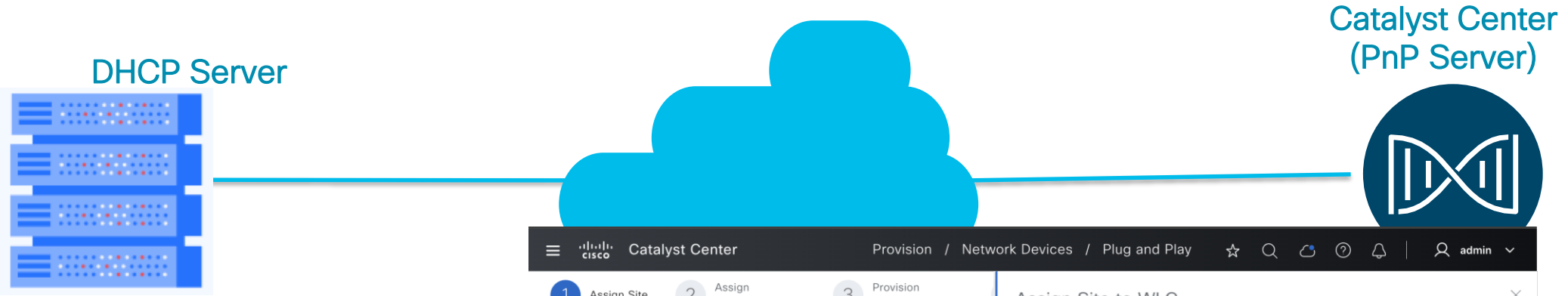
Enables secure unique device identifier (SUDI) authorization on devices that support it. When SUDI Authorization enabled, when a device attempts to connect to a PnP server, the PnP server compares the serial number on the SUDI certificate with the user-provided serial number. When the serial numbers match, the device is verified and connects to the PnP server.

Enable SUDI Authorization

At the bottom of the form, there are three buttons: "Back", "Add + Claim" (highlighted with a yellow box), and "Add Device".

- ✓ Pre-Staged Workflow using Device Sr.Number
- ✓ Site Assignment needed for WLC

# Device Onboarding Process- WLC PnP



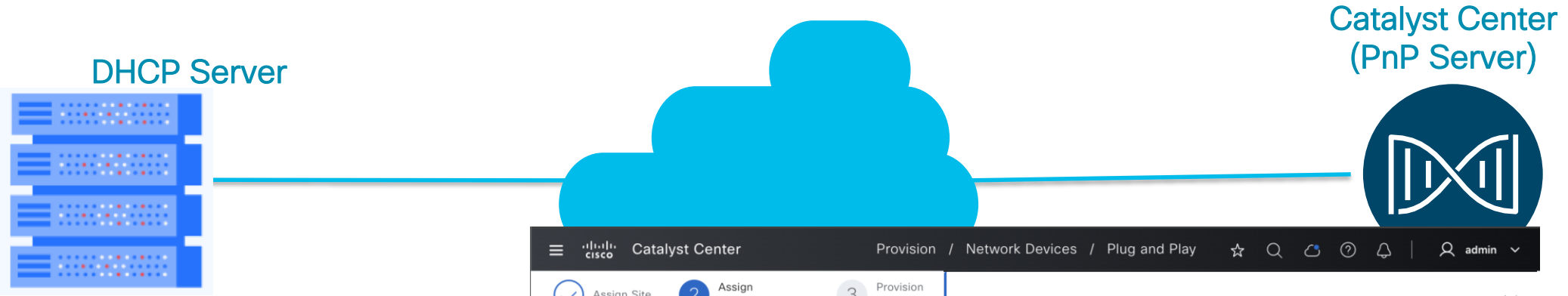
The screenshot shows the Catalyst Center interface during the 'Assign Site to WLC' step. The breadcrumb trail is 'Provision / Network Devices / Plug and Play'. The workflow progress shows three steps: 1. Assign Site (active), 2. Assign Configuration, and 3. Provision Templates. The main content area is titled 'Assign Site' and contains a table with one device entry:

Device Name	Serial Number	Pro
WLC	FCL24140056	C9

Below the table, there is a 'Showing' indicator. To the right, a modal window titled 'Assign Site to WLC' is open, showing a 'Select a site' dropdown menu with a search hierarchy. The hierarchy includes: Global, Andaman, Chennai, Hardy, Neville, POD1-Building, Floor-1, and RTP. At the bottom of the modal are 'Cancel' and 'Assign' buttons.

- ✓ Pre-Staged Workflow using Device Sr.Number
- ✓ Site Assignment needed for WLC

# Device Onboarding Process- WLC PnP



Pre-Staged Workflow using Device Sr.Number



Site Assignment needed for WLC

The screenshot shows the Catalyst Center web interface. The breadcrumb navigation is 'Provision / Network Devices / Plug and Play'. The current step is 'Assign Configuration', which is highlighted with a blue circle and the number '2'. The page title is 'Configuration for device name: POD1-C9800-LC'. A red error message at the top of the configuration pane states: 'There are total of 1 devices missing required configuration. Show details'. Below this is a table with one device entry:

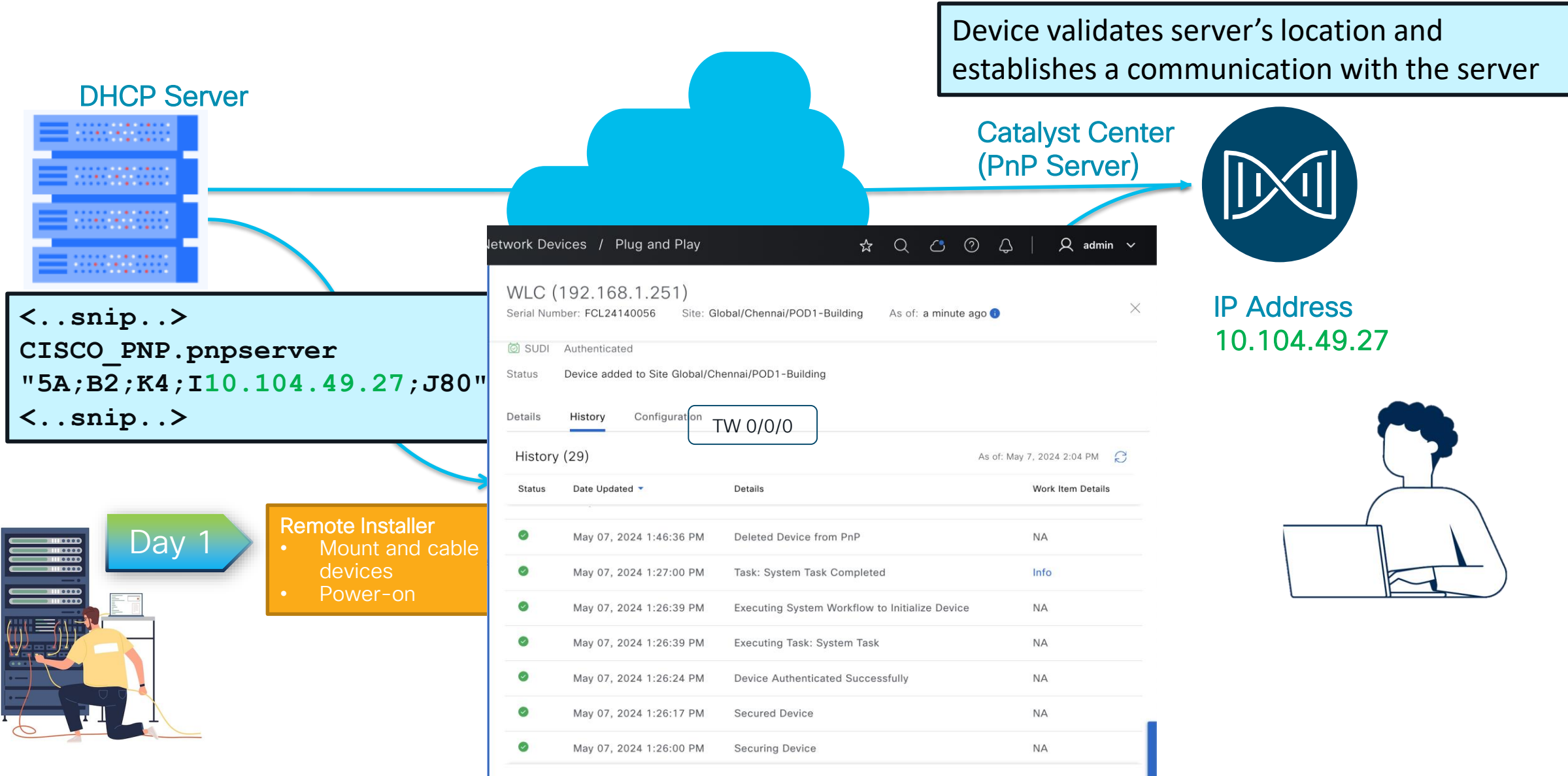
Device Name	Serial Number	Product ID
WLC	FCL24140056	C9800-L-C-K9

The configuration pane on the right shows the following settings for the Catalyst Wireless LAN Controller:

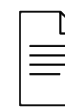
- Wireless Management IP\*: 192.168.1.12 (IPv4)
- Subnet Mask\*: 255.255.255.0 (IPv4)
- Gateway\*: 192.168.1.1 (IPv4)
- IP Interface Name\*: TwoGigabitEthernet0/0/0
- VLAN ID: 1 (Info)

Buttons for 'Cancel' and 'Save' are visible at the bottom right of the configuration pane.

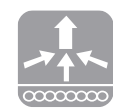
# Device Onboarding Process- PnP



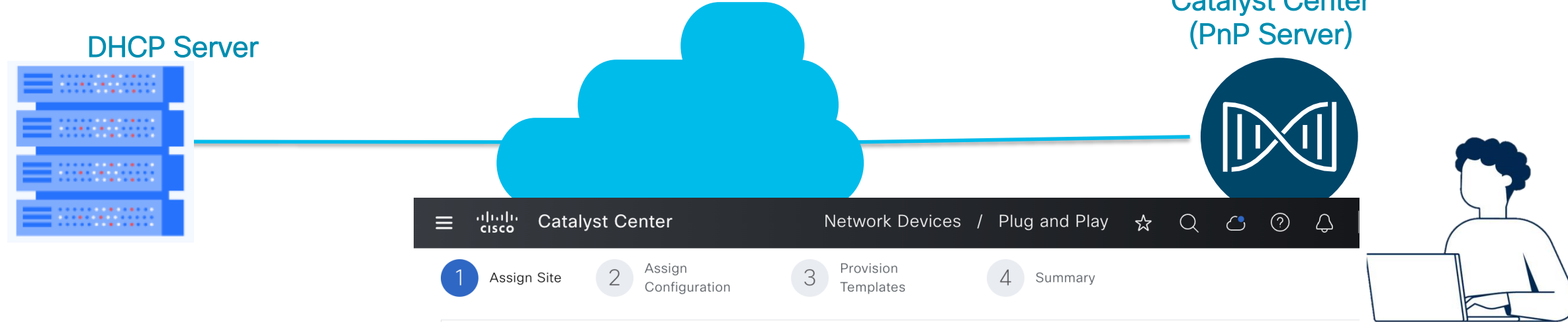
# Device Onboarding Process- AP PnP



For your reference



Managed only



Pre-Staged Workflow using Device Sr.Number



Site Assignment is not mandatory

## Assign Site

⚠ One (1) Warning Alert and One (1) Information Alert on this page. [Expand](#) to see details.

Devices (1)

🔍 Search Table

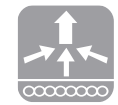
Device Name ⓘ	Serial Number	Product ID	Device Type ⓘ	Site (Recommended) ⓘ
CL-AP-Demo	FGL2323LGC6	C9120AXI-D	AP	<a href="#">Assign</a>

Showing 1 of 1

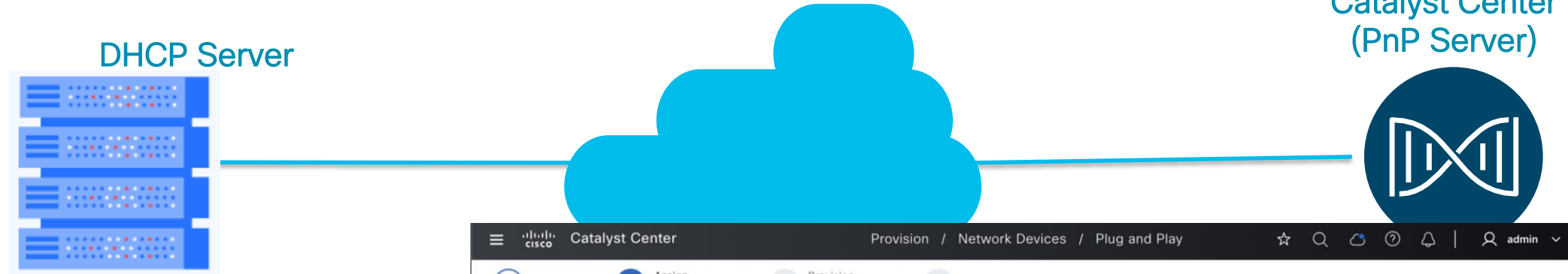
# Device Onboarding Process- AP PnP



For your reference



Managed only



Template Assignment is Mandatory

Catalyst Center Provision / Network Devices / Plug and Play

Assign Site 2 Assign Configuration 3 Provision Templates 4 Summary

### Assign Configuration

There are total of 1 devices missing required configuration. [Show devices.](#)

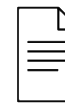
AP Location will **not be configured** as the assigned site during the claim process. To change this setting, go to [System -> Settings -> PnP AP Location](#). After the setting is updated, click [Refresh](#).

Devices (1) [Clear Configuration](#)

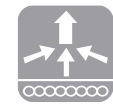
Search Table

Device Name	Serial Number	Product ID	Assigned Site	Configuration	Actions
NA	FGL2323LGC6	C9120AXI-D	-	Template: <a href="#">Assign*</a>	...

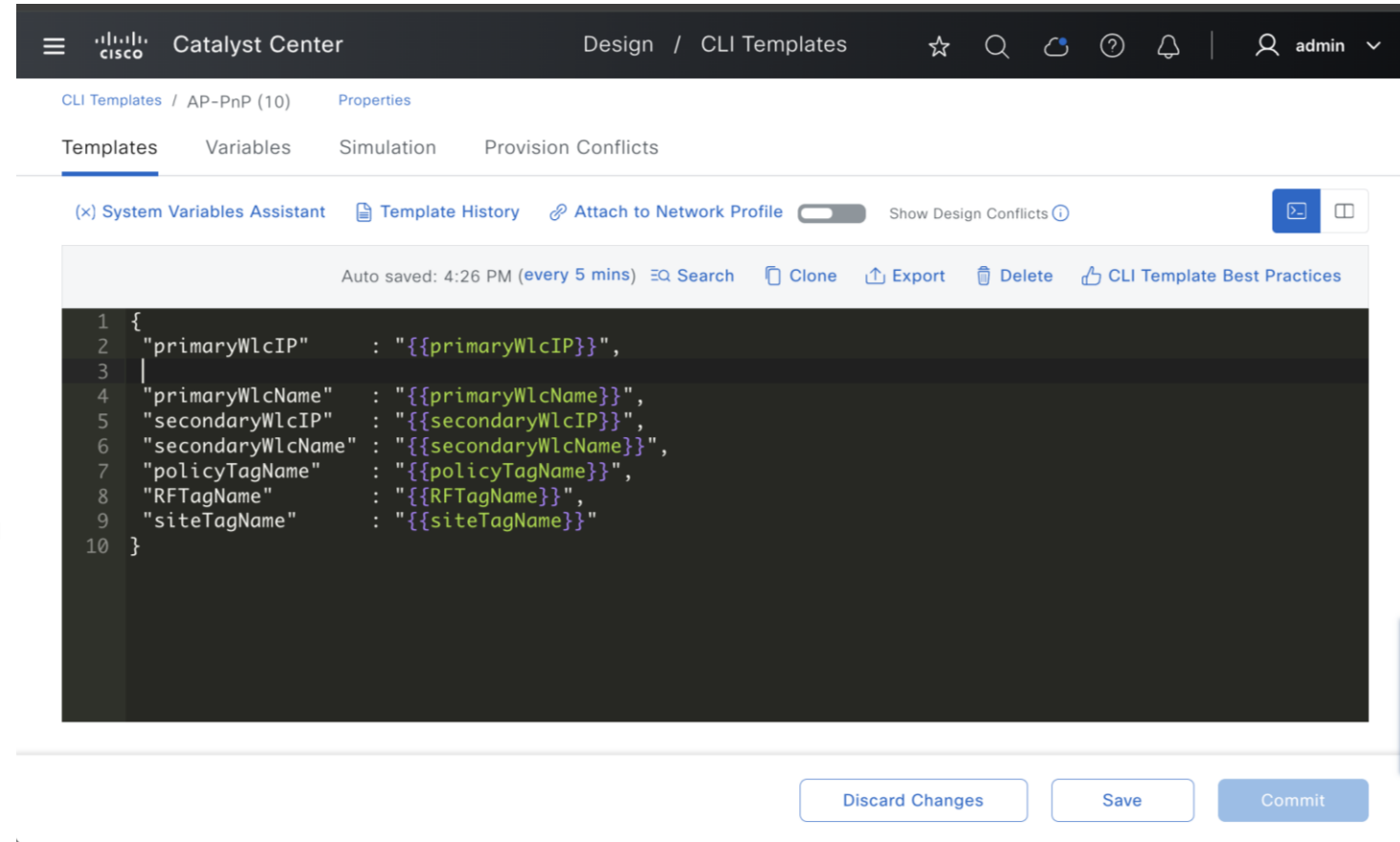
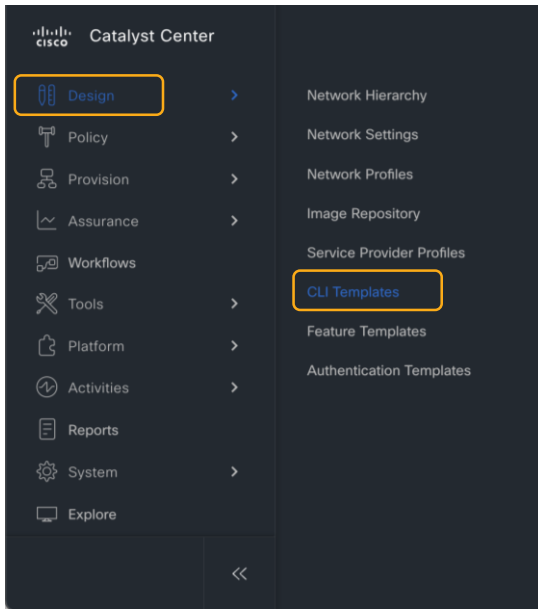
# How to build Templates for AP PnP



For your reference

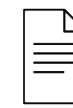


Managed only

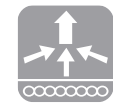


- ✓ Project Name: Onboarding Configuration
- ✓ Language: Jinja / Velocity
- ✓ Device Family: Wireless Lan Controller
- ✓ Software Type: IOS-XE

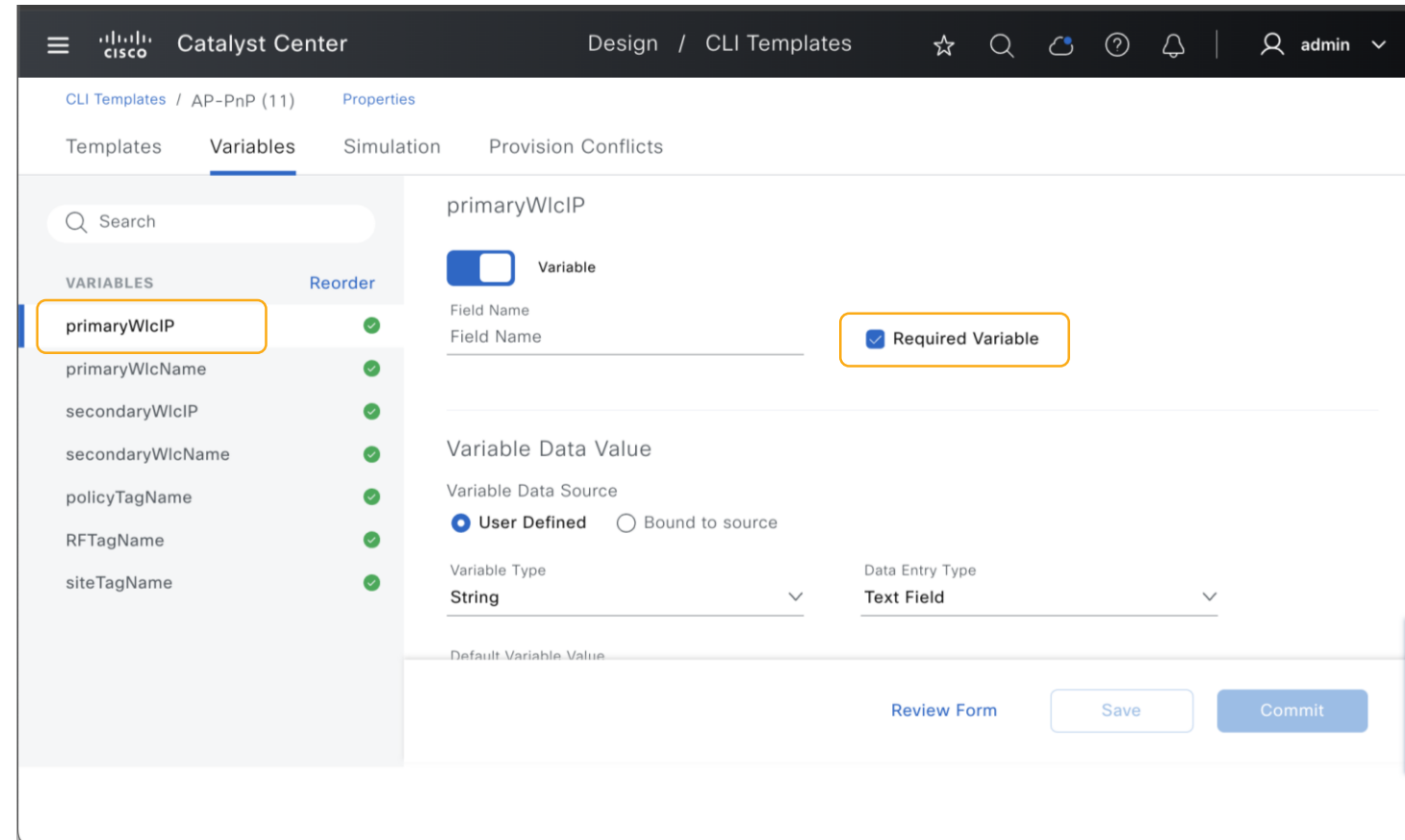
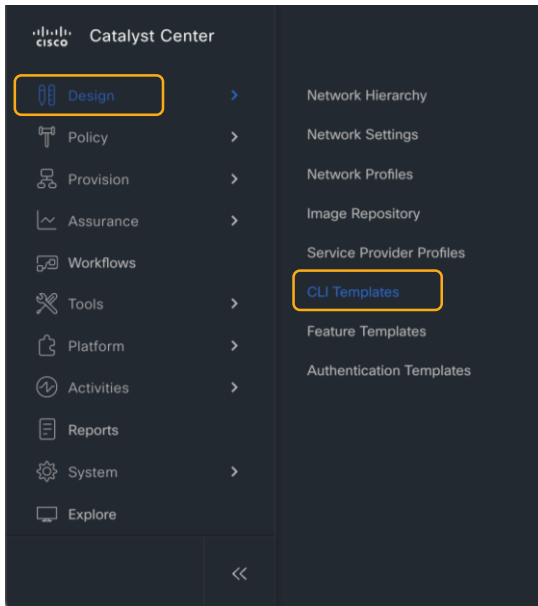
# How to build Templates for AP PnP





For your reference



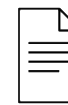
Managed only



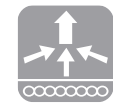
 Required Variable: primaryWLCIP

 Rest other variables is Optional

# Device Onboarding Process- AP PnP



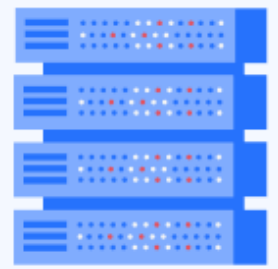
For your reference



Managed only

Device validates server's location and establishes a communication with the server

DHCP Server



Catalyst Center (PnP Server)



```
<..snip..>
CISCO_PNP.pnpserver
"5A;B2;K4;I10.104.49.27;J80
<..snip..>
```

Network Devices / Plug and Play

Device Name: AP5CE1.7628.FE14 (SN: FGL2420LGCF)

SUDI Not Supported

Status Provisioned Device

Details History Configuration

History As of: May 7, 2024 4:17 PM

Status	Time	Details	Info
✓	Apr 16, 2024 5:58:55 PM	Provisioned Device	Info
✓	Apr 16, 2024 5:58:55 PM	Access point joined the controller.	Info
✓	Apr 16, 2024 5:55:01 PM	Claimed Device	Info

IP Address  
10.104.49.27



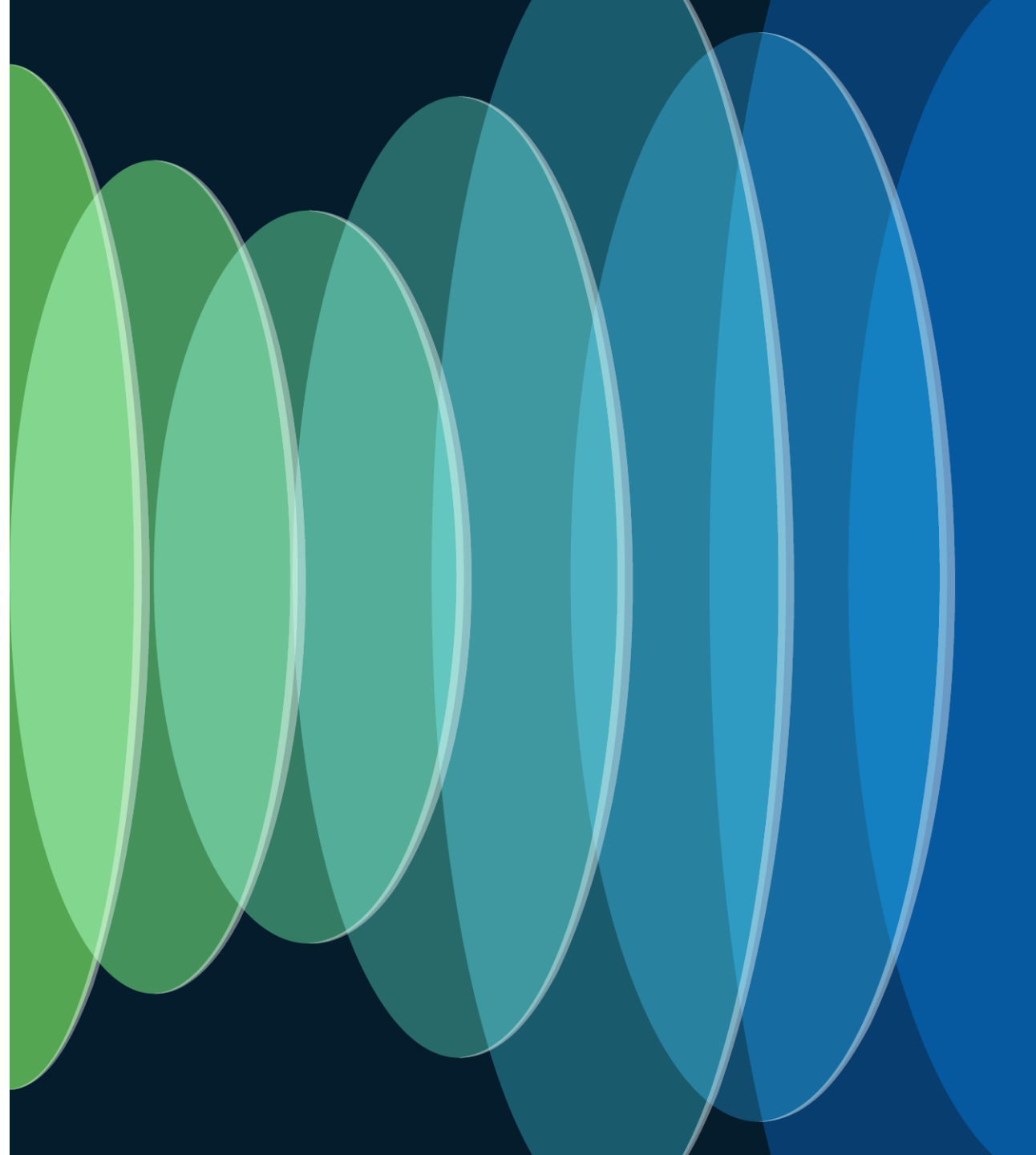
Day 1

- Remote Installer
- Mount and cable devices
  - Power-on

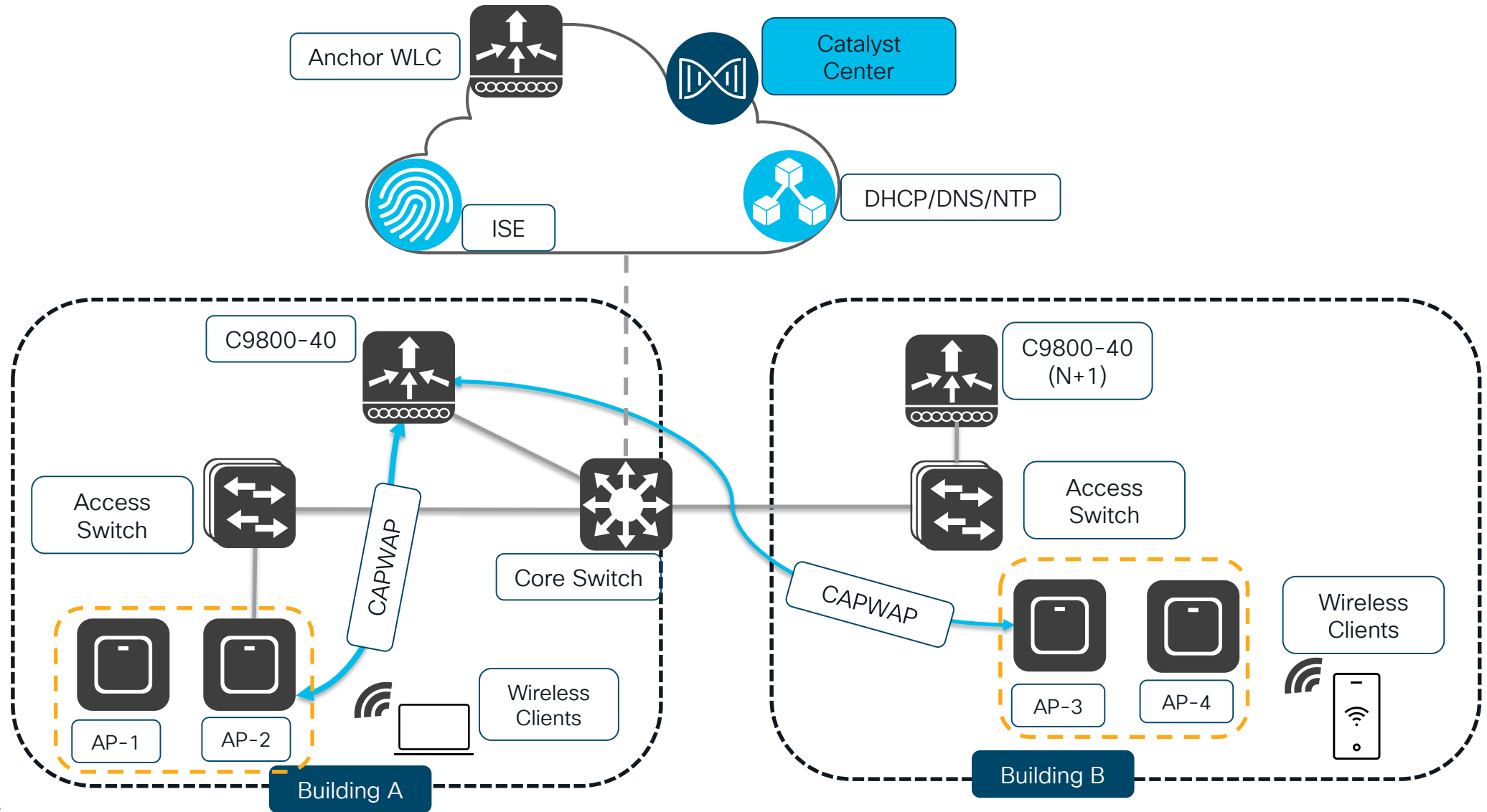


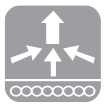
# Manage Brownfield wireless network

CISCO *Live!*

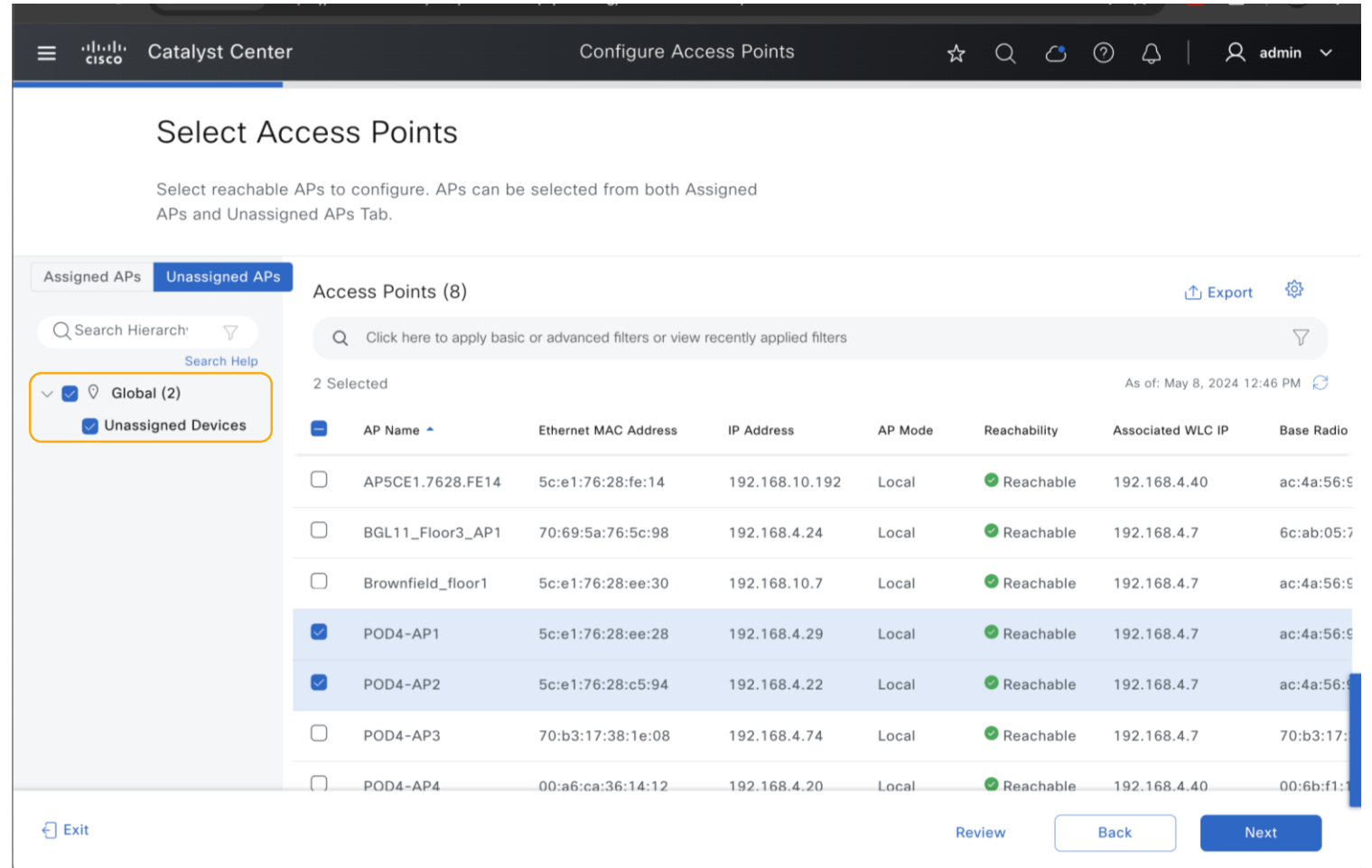
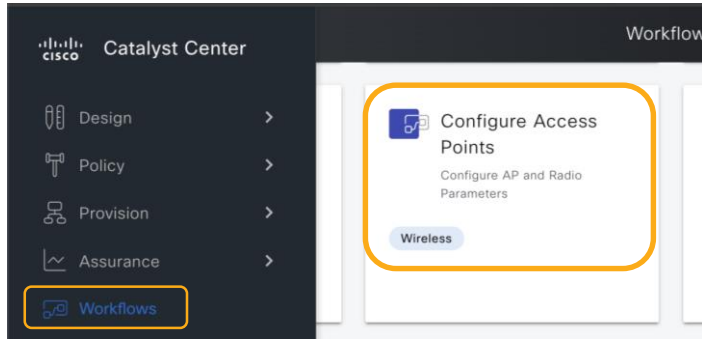


# Configuring High Availability for APs





# Configuring High Availability for APs



Select All Steps

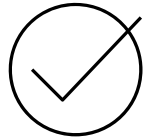
Select the steps you want to configure

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

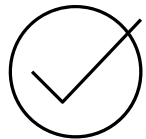
It is NOT MANDATORY for APs to be Assigned to Sites



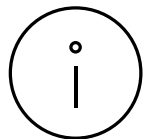
# Configuring High Availability for APs



AP Parameters for WLC High Availability



Configure Managed or Unmanaged WLC as Primary/Secondary/Tertiary WLC for AP



Other AP Parameters include:

- Admin Status
- LED
- Location
- Radio Parameters
  - Admin Status
  - Antenna
  - Channel Power

The screenshot shows the Catalyst Center interface for configuring an Access Point. The 'High Availability' section is highlighted with an orange border. The configuration includes:

- High Availability ⓘ
- Select Primary Controller Name: **POD4-C9800-CL1**
- Select Secondary Controller Name: **C9800-vWLC**
- Select Tertiary Controller Name: **C9800-40**
- Primary Controller IP Address: **192.168.4.7**
- Secondary Controller IP Address: **192.168.4.40**
- Tertiary Controller IP Address: **192.168.4.5**

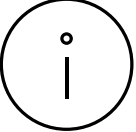
Other visible settings include:


- AP Location ⓘ
- AP Failover Priority
- Use currently assigned site location ⓘ
- Enter Location: \_\_\_\_\_
- CleanAir Pro / CleanAir / Spectrum Intelligence ⓘ
- 2.4 GHz Radio Band (Enable/Disable)
- 5 GHz Radio Band (Enable/Disable)
- 6 GHz Radio Band (Enable/Disable)

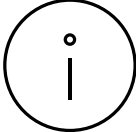
Navigation buttons at the bottom: Exit, Review, Back, Next.

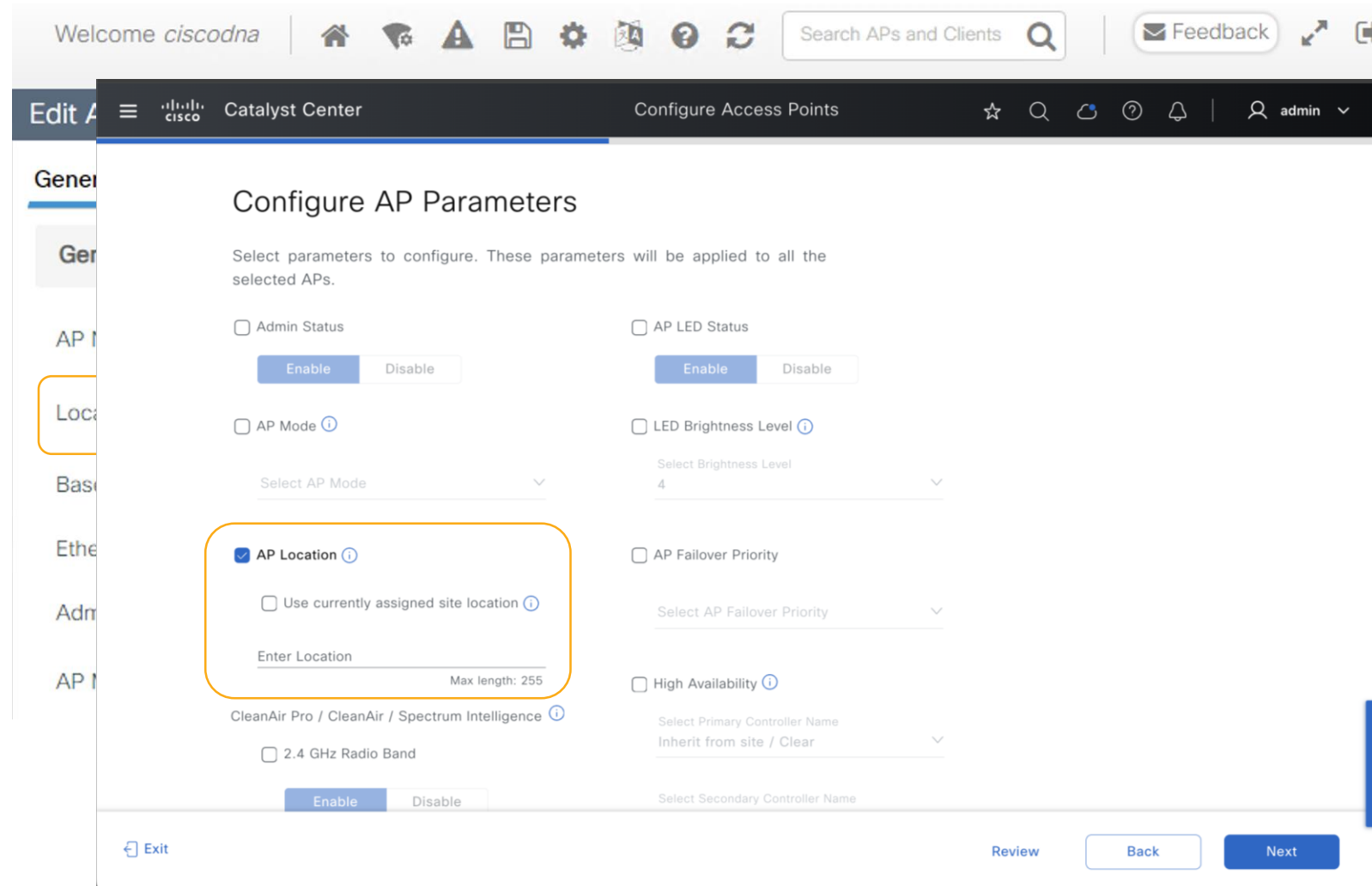


# Tips & Tricks

 AP Provisioning **does not** update the location field

 Location needs to be updated using Config AP Workflow

 Only Applicable for AP Provisioning and not for AP Provisioned via PnP



Welcome *ciscodna* | Search APs and Clients | Feedback

Edit AP | Cisco Catalyst Center | Configure Access Points | admin

### Configure AP Parameters

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

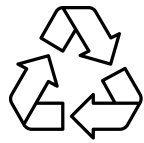
- Admin Status (Enable/Disable)
- AP LED Status (Enable/Disable)
- AP Mode (Select AP Mode)
- LED Brightness Level (Select Brightness Level: 4)
- AP Location
  - Use currently assigned site location
  - Enter Location (Max length: 255)
- AP Failover Priority (Select AP Failover Priority)
- High Availability (Select Primary Controller Name: Inherit from site / Clear)

CleanAir Pro / CleanAir / Spectrum Intelligence (2.4 GHz Radio Band)

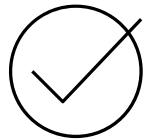
Exit | Review | Back | Next



# Reusable Templates- Configure AP Workflow



Save the workflow as Reusable Template for quicker deployments



Template can be launched from Configure AP Workflow

Catalyst Center Configure Access Points

### How do you want to configure APs?

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

- Configure AP And Radio Parameters  
Choose which steps to configure relevant parameters on the selected APs.
- Schedule Recurring Events...  
You can configure the Admin and LED status of the AP and the Radio Admin status as recurring events.
- Configure AP Parameters Usin...  
You can use existing templates for AP configuration.

Template List (1)

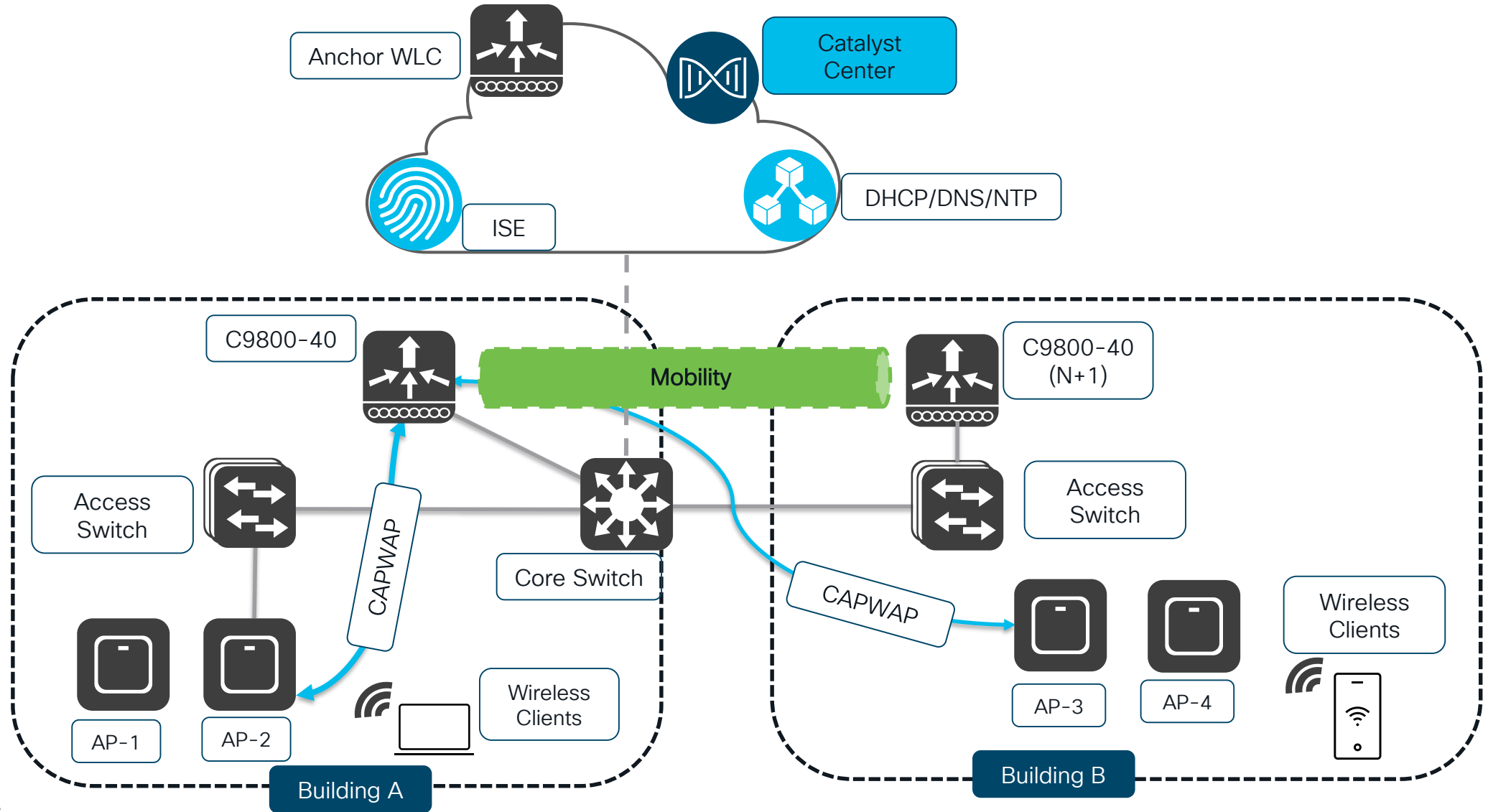
Search Table

1 Selected [Delete](#)

<input checked="" type="checkbox"/>	Template Name	Description
<input checked="" type="checkbox"/>	Template-AP Workflow for N-1	

Exit Review Back Next

# Configuring Mobility for Endpoint



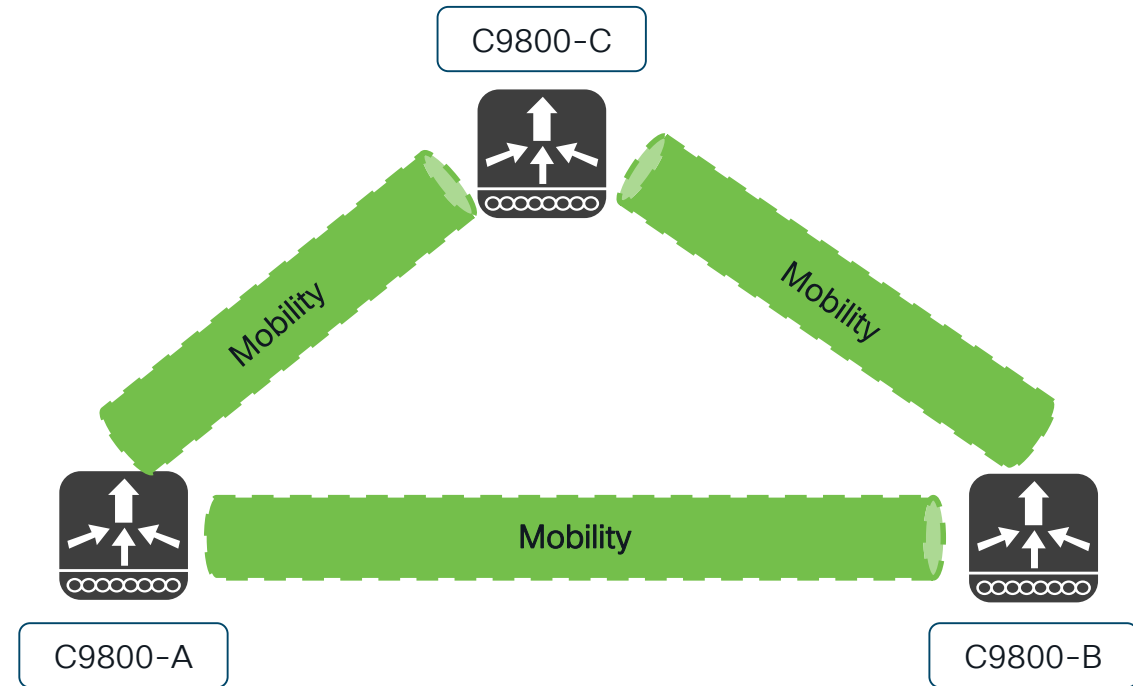
# Mobility Provisioning- How it works??

## Manual Mobility Configuration Steps

- Step 1: Configure C as Peer in A
- Step 2: Configure Mobility Group in C and A as Peer in C
- Step 3: Configure B as Peer in C
- Step 4: Configure C as Peer in B

## Mobility Configuration Steps in CC

- Step 1: Configure Mobility Group in C
- Step 2: Configure C as Peer in A



Global

- All
- Routers
- Switches
- Wireless Controllers
- Access Points
- Sensors

Grid, List, Map, Location icons

Devices (4) Focus: Inventory

Take a tour Export

Click here to apply basic or advanced filters or view recently applied filters

0 Selected Tag Add Device Edit Device Delete Device Actions

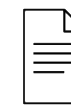
As of: May 27, 2024 6:11 AM

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability	Compliance	Site	Image Version	Last Updated
	WLC	192.168.1.12	Cisco	Reachable	Not Scanned	Managed	Non-Compliant	.../Chennai/POD1-Building	17.9.1	21 hours 52 m Latest Sync Detail
	POD4-C9800-CL1	192.168.4.7	Cisco	Reachable	1 alert	Managed	Non-Compliant	.../Chennai/RITP	17.9.3	1 hour 45 min Latest Sync Detail
	POD4-3504-1	192.168.4.9	Cisco	Reachable	Not Scanned	Managed	Compliant	.../Chennai/Hardy	8.10.171.0	4 hours 29 min Latest Sync Detail
	C9800-vWLC	192.168.4.40	Cisco	Reachable	0 alerts	Managed	Compliant	.../Chennai/Neville	17.14.1	13 minutes ago Latest Sync Detail

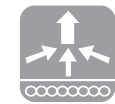
4 Record(s)

Show Records: 25 1 - 4



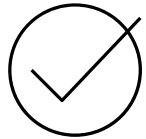


For your reference

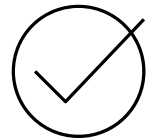


Managed only

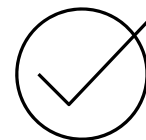
# Mobility



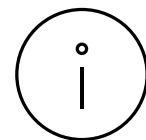
Learns any existing Mobility Peers configured



Ability to add additional Peer which are part of Catalyst Center or Unmanaged



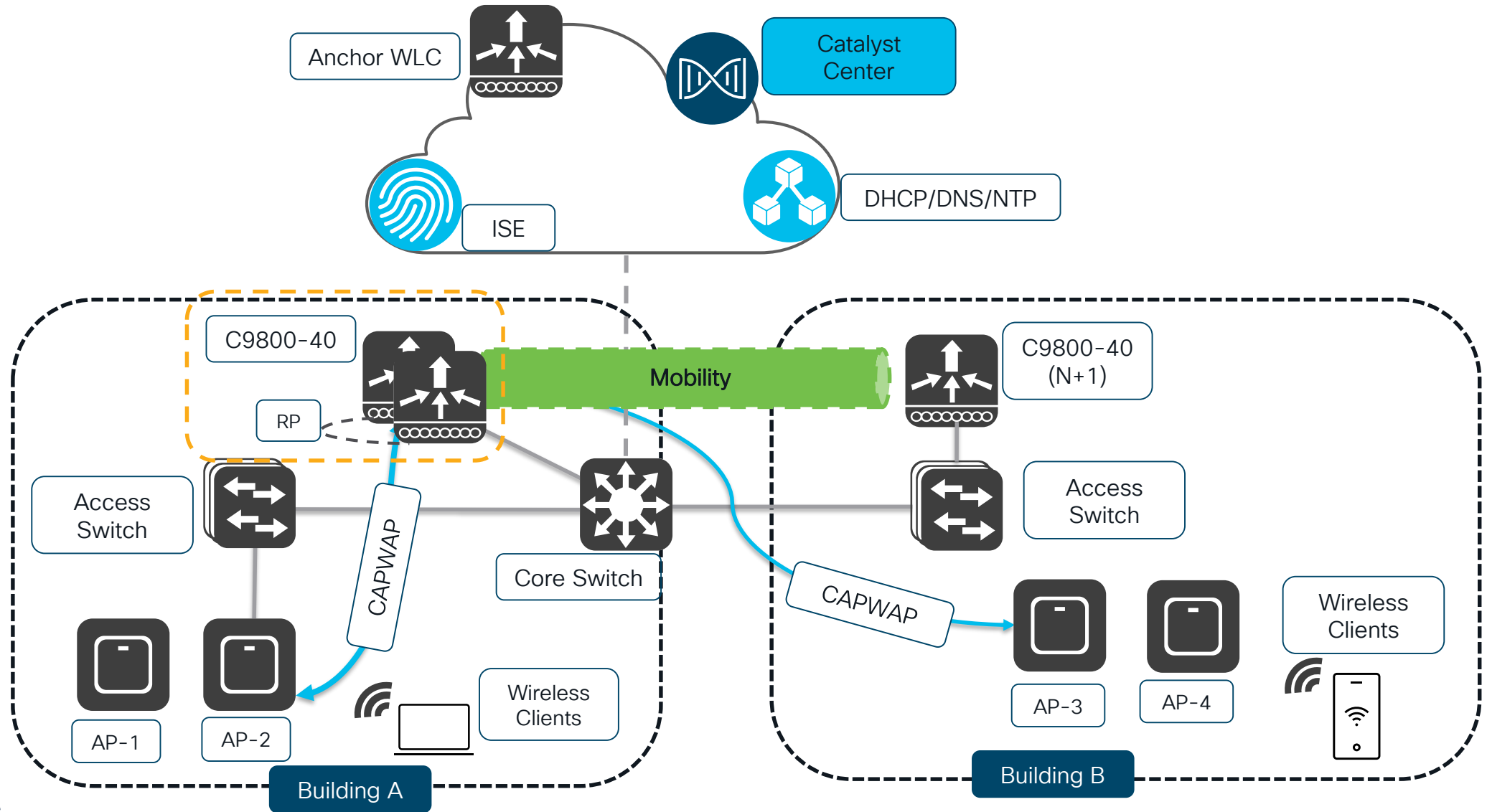
Configure Peers from Actions > Provisioning > Configure WLC Mobility



For Intra controller mobility (Different Subnet) ports 16666 and 16667 is Open

The screenshot displays the Cisco Catalyst Center interface for configuring a mobility peer. The main window is titled 'Add Mobility Peer' and is part of the 'Configure Mobility Group' workflow. A search bar at the top of the device list is highlighted with an orange box, containing the text 'Click here to apply basic or advanced filters or view'. Below the search bar, a table lists four devices: 'WLC', 'POD4-C9800-CL1', 'POD4-3504-1', and 'C9800-vWLC'. The 'C9800-vWLC' device is selected. In the 'Device Details' section, the 'Managed WLC' radio button is selected and highlighted with an orange box. The 'Device Name' is set to 'POD4-3504-1', the 'IP Address' is '192.168.4.9', and the 'MAC Address' is 'dc:f7:19:d3:1e:80'. The 'Mobility Group Name' is 'OOB-Foreign' and the 'Hash' field is empty. At the bottom right, there are 'Cancel' and 'Save' buttons.

# Configuring High Availability-SSO





# Configure HA-SSO

- ✓ Launch Workflow from Actions > Provision > Configure WLC HA
- ✓ Select secondary WLC from drop down
- ✓ Select Primary & Secondary RMI Interface
- ✓ Provide IP address for RMI interfaces

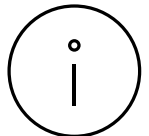
The screenshot shows the Catalyst Center 'High Availability' configuration page. On the left, a table lists four devices: WLC, POD4-C9800-CL1 (selected), C9800-vWLC, and POD4-C9800-CL2. The right panel is titled 'High Availability' and contains a warning alert. Below the alert, the configuration fields are as follows:

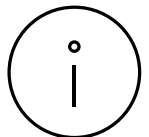
Field	Value
Primary C9800	POD4-C9800-CL1
Select Primary Interface	GigabitEthernet3
Redundancy Management IP*	192.168.4.11
Select Secondary C9800	POD4-C9800-CL2
Select Secondary Interface	GigabitEthernet3
Peer Redundancy Management IP*	192.168.4.12
Device IP	192.168.4.8
Netmask*	/24 (255.255.255.0)

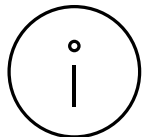
At the bottom right, there are 'Cancel' and 'Configure HA' buttons.

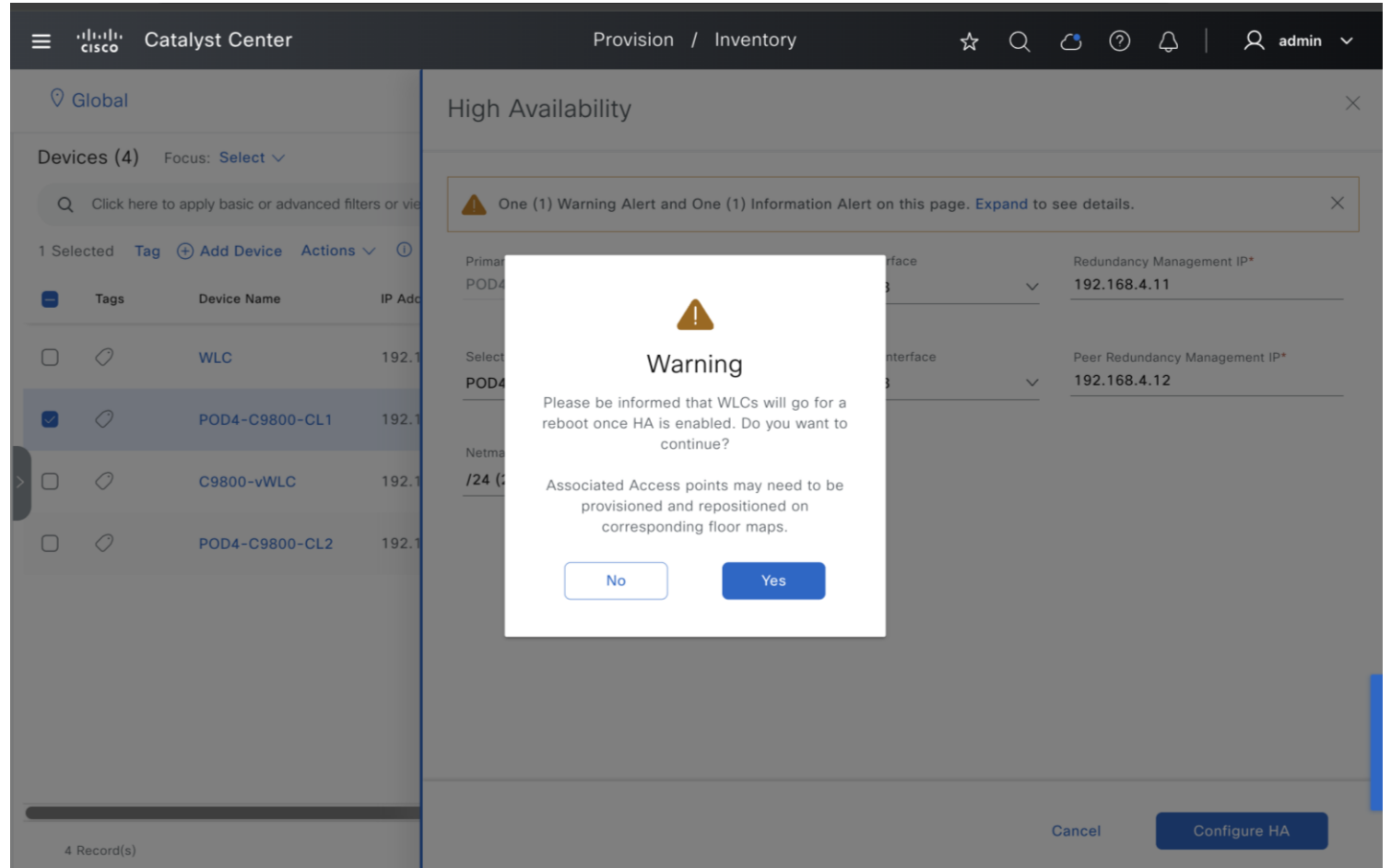


# Tips & Tricks

 Configuring HA will reboot both the WLCs

 Both the WLCs should be running same software version

 If WLC was provisioned from CC, AP may need Re-provisioning



The screenshot shows the Cisco Catalyst Center interface. On the left, a table lists devices: WLC, POD4-C9800-CL1 (selected), C9800-vWLC, and POD4-C9800-CL2. The right pane shows the 'High Availability' configuration page with a warning dialog box. The dialog box contains the following text:

**Warning**

Please be informed that WLCs will go for a reboot once HA is enabled. Do you want to continue?

Associated Access points may need to be provisioned and repositioned on corresponding floor maps.

Buttons: No, Yes

Background text in the dialog: One (1) Warning Alert and One (1) Information Alert on this page. Expand to see details.

Background text in the High Availability page: Redundancy Management IP\* 192.168.4.11, Peer Redundancy Management IP\* 192.168.4.12, Cancel, Configure HA



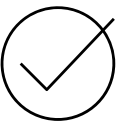
# Break HA



If you "write erase; reload" in HA mode, you will lose G3.



"show romvar" will show "CHASSIS\_HA\_IFNAME = GigabitEthernet3"



"clear chassis redundancy" is your friend

The screenshot shows the Catalyst Center interface for configuring High Availability. On the left, a table lists three devices: WLC, C9800-vWLC, and POD4-C9800-CL1. The 'POD4-C9800-CL1' device is selected, and an 'Actions' menu is open, highlighting the 'Provision' option. On the right, the 'High Availability' configuration page is displayed, showing a 'Redundancy Summary' table with the following details:

Parameter	Value
Primary C9800	POD4-C9800-CL1
Unit MAC	00:0c:29:0c:55:27
Redundancy State	SSO
Mobility MAC	00:1e:bd:13:20:ff
Sync Status	Duplex
Primary Chassis Serial No.	9PVDTNHIB9E
Secondary Chassis Serial No.	9G5P10WK2TM
Active RMI IP	192.168.4.11
Standby RMI IP	192.168.4.12
Gateway Monitoring	Enabled
Recovery mode	Not Applicable

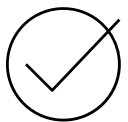
Below the table, a note states: "The High Availability for Wireless controller is either configured outside the Catalyst Center, or it was configured earlier using the Catalyst Center." At the bottom right, there are two buttons: 'Cancel' and 'Disable HA', with the latter highlighted by a dashed orange box.



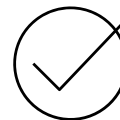
# Tips & Tricks

```
POD4-C9800-CL1#sh ip int br
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1	unassigned	YES	unset	administratively down	down
GigabitEthernet2	unassigned	YES	unset	administratively down	down
<b>GigabitEthernet3</b>	<b>unassigned</b>	<b>YES</b>	<b>unset</b>	<b>up</b>	<b>up</b>
Vlan1	192.168.4.7	YES	NVRAM	administratively down	down



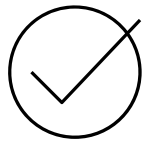
Disable HA will reload standby chassis after clearing HA and Startup config WLC version 17.6 & below



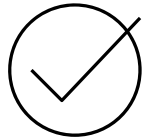
17.7 & above, standby controller boots with active config



# Monitor HA Status of WLC



HA State change events logged as Syslog events



Events can be viewed from Assurance > Issues and Events



Catalyst Center Assurance / Dashboards / Issues and Events

Issues > Events Event Analytics - Preview

Events (44)

Category Type: Devices Endpoints Router: 0 Switch: 1 **Wireless Controller: 43** AP: 0 Third Party Device: 0

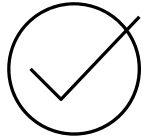
Filter Table

Event Name	Status	Severity	Timestamp	Device Name	Event Type	Device IP
RF:RF_TERMINAL_STATE	●	Notice	May 8, 2024 12:27:45.174 PM	POD4-C9800-CL1	Syslog	192.168.4.7
HA_CONFIG_SYNC:BULK_CFGSYNC_SUCCEED	●	Info	May 8, 2024 12:27:43.125 PM	POD4-C9800-CL1	Syslog	192.168.4.7
STACKMGR:DUAL_ACTIVE_CFG_MSG	●	Alert	May 8, 2024 12:27:29.995 PM	POD4-C9800-CL1	Syslog	192.168.4.7
CAPWAPAC_SMGR_TRACE_MESSAGE:AP_JOIN_DISJOIN	●	Notice	May 8, 2024 12:27:15.362 PM	POD4-C9800-CL1	Syslog	192.168.4.7
CAPWAPAC_SMGR_TRACE_MESSAGE:AP_JOIN_DISJOIN	●	Notice	May 8, 2024 12:27:04.102 PM	POD4-C9800-CL1	Syslog	192.168.4.7
CAPWAPAC_SMGR_TRACE_MESSAGE:AP_JOIN_DISJOIN	●	Notice	May 8, 2024 12:26:46.154 PM	POD4-C9800-CL1	Syslog	192.168.4.7
REDUNDANCY:PEER_MONITOR_EVENT	●	Notice	May 8, 2024 12:26:32.413 PM	POD4-C9800-CL1	Syslog	192.168.4.7
REDUNDANCY:PEER_MONITOR_EVENT	●	Notice	May 8, 2024 12:26:32.411 PM	POD4-C9800-CL1	Syslog	192.168.4.7

43 Record(s) Show Records: 100 1 - 43



# Alerting HA State events



View Details of HA events and connected AP/Endpoint events



Convert these Events into User Defined Issues



The screenshot displays the Cisco Catalyst Center interface. At the top, the navigation bar includes 'Assurance / Dashboards / Issues and Events' and a user profile 'admin'. The main content area is divided into two panels. The left panel, titled 'Events', shows a filter for 'Global' and a time range of '24 Hours'. Below this is a bar chart showing event counts for various categories: Router, Switch, Wireless Controller, AP, Third Party Device, Wired Endpoints, and Wireless Endpoints. The right panel displays the details of a specific event: 'REDUNDANCY:PEER\_MONITOR\_EVENT NOTICE' from May 8, 2024, at 12:26:32.413 PM. The event type is 'Syslog' and the message text is '435: May 8 06:50:00.374: %REDUNDANCY-5-PEER\_MONITOR\_EVENT: Active detected a standby insertion (raw-event=PEER\_REDUNDANCY\_STATE\_CHANGE(5))'. The device name is 'POD4-C9800-CL1' and the device IP is '192.168.4.7'. A 'Create an Issue' button is visible next to the event type. Below the event details, there is a section for 'Connected Device Events' with filters for 'AP' and 'Wireless Endpoints'. A 'Show Events (±15 mins)' button is located at the bottom right of the event details panel.



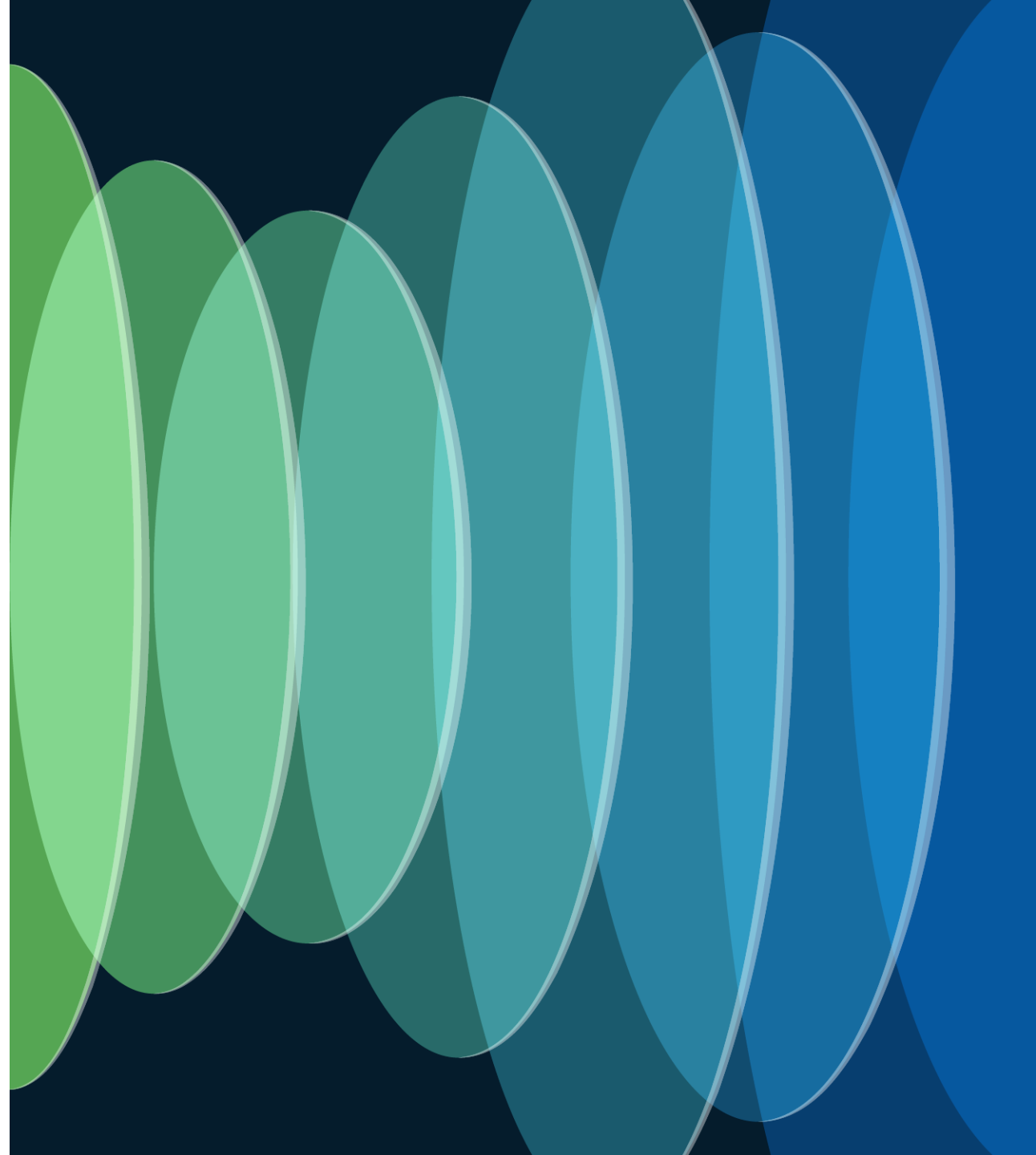
# Alerting HA State events

- ✓ Severity, Facility & Mnemonic auto populated
- ✓ Message Pattern to match Regex string
- ✓ Custom Threshold definition
- ✓ Notification alerts sent to Email, Webhook, Syslog servers

The screenshot shows the 'Create an Issue' configuration page in Cisco Catalyst Center. The page is divided into two main sections: 'Global Profile' and 'User Defined'. The 'User Defined' section is active, showing a 'User Defined Issue' configuration. The 'Message Pattern' field is set to 'Active detected a standby insertion (rav)'. The 'Number of Occurrences & Duration' section shows 'Occurrences' set to 1 and 'Duration' set to 0 min. The 'Enabled' checkbox is checked, and the 'Priority' is set to P1. The 'Notification' checkbox is also checked. A 'Back' button and a 'Save' button are visible at the bottom of the configuration panel.

Learn how to get  
visibility from your  
network

CISCO *Live!*





# Prerequisites for Visibility

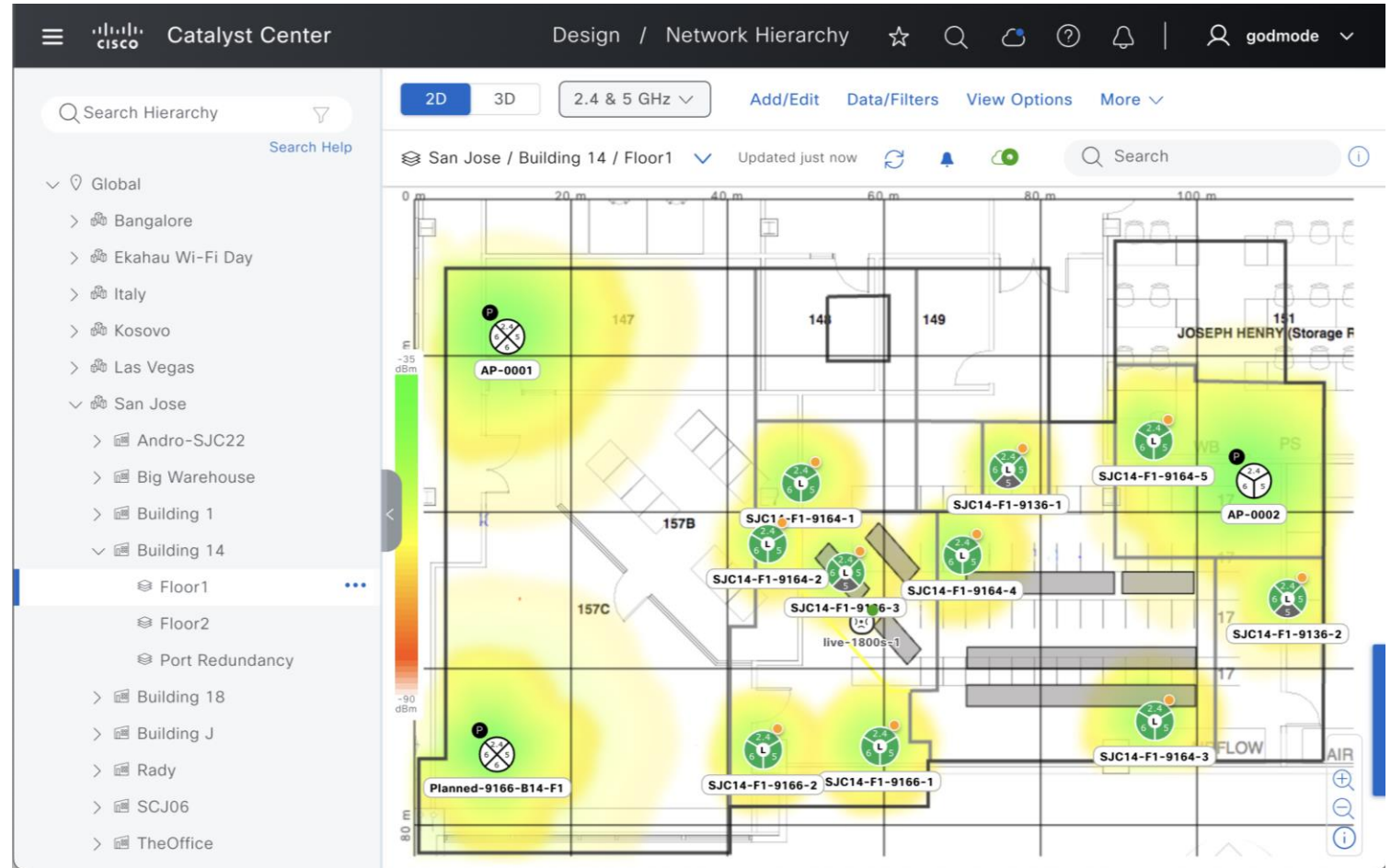
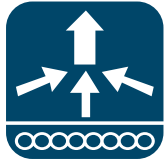
UDP: 162/ 514

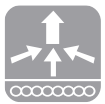
TCP: 80/ 443/ 25103

UDP: 161

TCP: 22/830

TCP: 443/ 32626

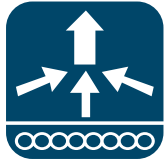




# Prerequisites for Visibility

UDP: 162/ 514

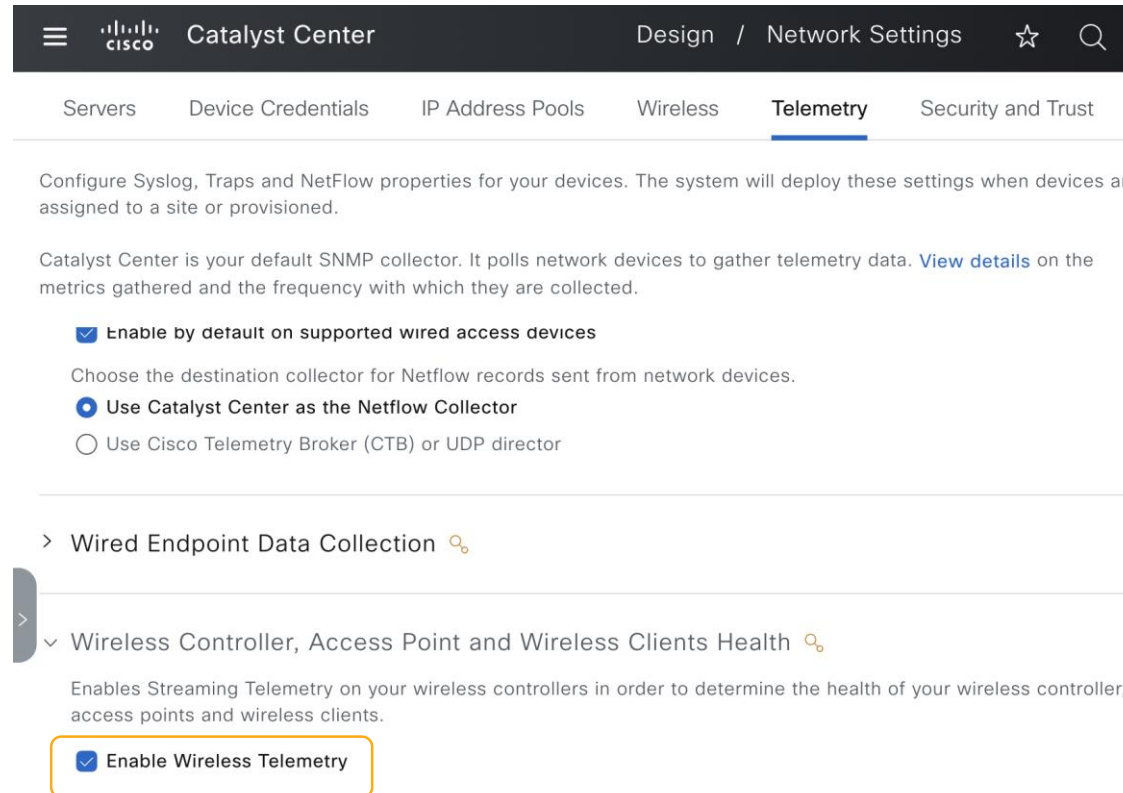
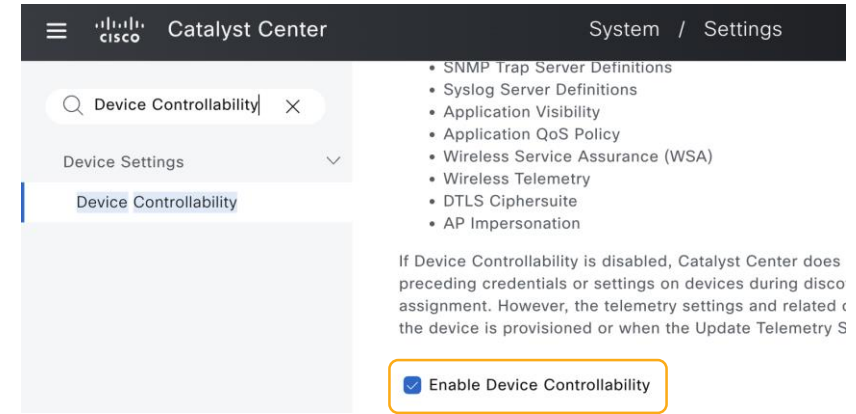
TCP: 80/ 443/ 25103



UDP: 161

TCP: 22/830

TCP: 443/ 32626





# Wireless Assurance- Site Assignment

Assign WLCs to Buildings

Assign APs to Floors

Catalyst Center Provision / Inventory admin

Global

Assign Device to Site

Serial Number: 9PVDTNHIB9E, 9C  
Devices: POD4-C9800-CL1

Global/Chennai/RITP

Tags	Device Name
<input type="checkbox"/>	WLC
<input checked="" type="checkbox"/>	POD4-C9800-CL1
<input type="checkbox"/>	POD4-AP4
<input type="checkbox"/>	POD4-AP6
<input type="checkbox"/>	POD4-AP2
<input type="checkbox"/>	BGL11_Floor3_AP1
<input type="checkbox"/>	POD4-AP1
<input type="checkbox"/>	C9800-vWLC
<input type="checkbox"/>	POD4-AP3
<input type="checkbox"/>	Brownfield_floor1
<input type="checkbox"/>	AP5CE1.7628.FE14

11 Record(s)

Device Controllability is **Enabled**. Learn More | Disable

Cancel Next

Catalyst Center Provision / Inventory admin

Global

Assign Device to Site

Serial Number: FGL2245A8EK  
Devices: POD4-AP3

...bal/Chennai/RITP/Floor 2

Tags	Device Name
<input type="checkbox"/>	WLC
<input type="checkbox"/>	POD4-C9800-CL1
<input type="checkbox"/>	POD4-AP4
<input type="checkbox"/>	POD4-AP6
<input checked="" type="checkbox"/>	POD4-AP2
<input checked="" type="checkbox"/>	BGL11_Floor3_AP1
<input checked="" type="checkbox"/>	POD4-AP1
<input type="checkbox"/>	C9800-vWLC
<input checked="" type="checkbox"/>	POD4-AP3
<input type="checkbox"/>	Brownfield_floor1
<input type="checkbox"/>	AP5CE1.7628.FE14

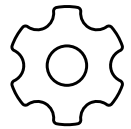
11 Record(s)

Device Controllability is **Enabled**. Learn More | Disable

Cancel Next



# Configuration Preview (Visibility & Control)



For better control, 'Configuration Preview' is enabled by default under **System > Settings > Visibility and Control**



Catalyst Center Provision / Inventory

Global

Devices (11) Focus: Select

Click here to apply basic or advanced filters or view

1 Selected Tag Add Device Actions

Tags	Device Name
<input type="checkbox"/>	WLC
<input checked="" type="checkbox"/>	POD4-C9800-CL1
<input type="checkbox"/>	POD4-AP4
<input type="checkbox"/>	POD4-AP6
<input type="checkbox"/>	POD4-AP2
<input type="checkbox"/>	BGL11_Floor3_AP1
<input type="checkbox"/>	POD4-AP1
<input type="checkbox"/>	C9800-vWLC
<input type="checkbox"/>	POD4-AP3
<input type="checkbox"/>	Brownfield_floor1
<input type="checkbox"/>	AP5CE1.7628.FE14

11 Record(s)

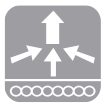
Assign Device to Site

This workflow supports enforcing network administrators and other users to preview configurations before deploying them on the network devices. To configure this setting, go to [System > Settings > Visibility and Control of Configurations](#)

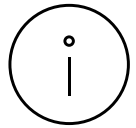
Now  
 Later  
 **Generate configuration preview**  
Creates preview which can be later used to deploy on selected devices. View status in [Tasks](#)

Task Name\*  
 Assign/Unassign 1 Device(s) to/from Site

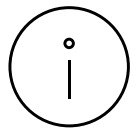
Device Controllability is **Enabled**. [Learn More](#) | [Disable](#) [Cancel](#) [Back](#) [Preview](#)



# Configuration Preview (Visibility & Control)



Starting IOS-XE 17.13 and above, Configurations can be viewed in CLI format



Running config compared with CLI generated

The screenshot displays the Cisco Catalyst Center interface. The top navigation bar shows 'Catalyst Center' and 'Provision / Inventory'. A modal window titled 'Configurations - Side by side view' is open, showing a search bar and a 'Deploy' button. Below this, another modal window titled 'Configuration to be Deployed' is shown, displaying the following information:

Device Name: C9800-vWLC  
 Configuration Source: All

Generated CLI (955 Line(s))

Below is the "CLI preview" of configuration change in the device after applying the YANG configuration payload.

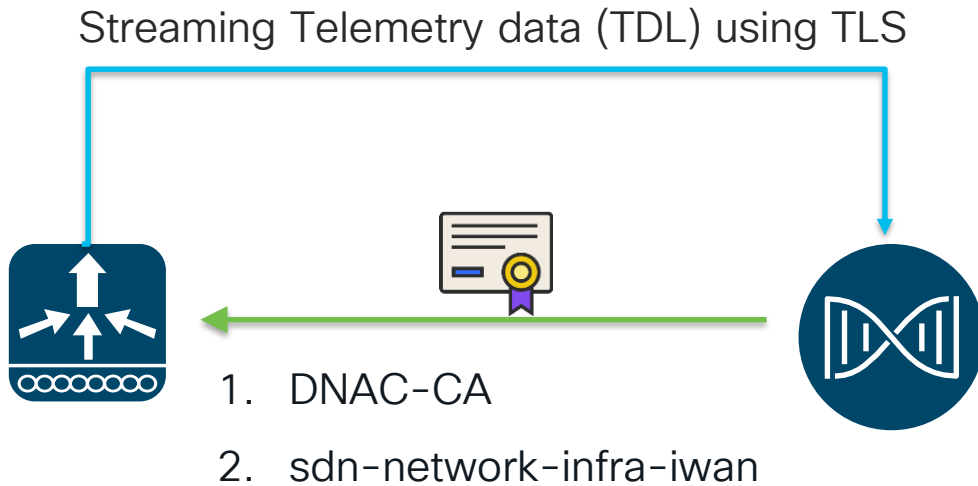
```

1 crypto pki import sdn-network-infra-iwan pkcs12 http://172.100.1.53/api/v1/trust-point/pkcs12/PREVIEW password $pe
2 crypto pki trustpoint sdn-network-infra-iwan
3 auto-enroll 80 regenerate
4 enrollment url http://172.100.1.53:80/ejbca/publicweb/apply/scep/sdncscep-PREVIEW
5 fgdn PREVIEW_FQDN.com
6 hash sha256
7 revocation-check crl
8 source interface Vlan1
9 rsa-keypair sdn-network-infra-iwan
10 subject-name CN=PREVIEW_sdn-network-infra-iwan
11 !
12 device classifier
13
14 network-assurance enable
15 network-assurance icap server port 32626
16 network-assurance url https://172.100.1.53
17 wireless feature-usage enable
18
19 telemetry ietf subscription 750
20 encoding encode-tdl
21 filter tdl-uri /services/serviceName:scep_email_opn/environment sensor
  
```

At the bottom of the modal, there are buttons for 'Generation Status Legend', 'Exit and Preview Later', 'Discard', and 'Deploy'.



# Certificates- Recommendations



## Catalyst Center System Certificate (DNAC-CA)

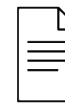
If custom required, replace before adding devices

## Device Certificate (sdn-network-infra-iwan)

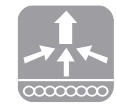
Catalyst Center issuer of Device Certificate

Catalyst Center can be a Sub CA of External CA

Can query external CA with SCEP URL



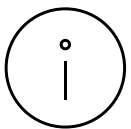
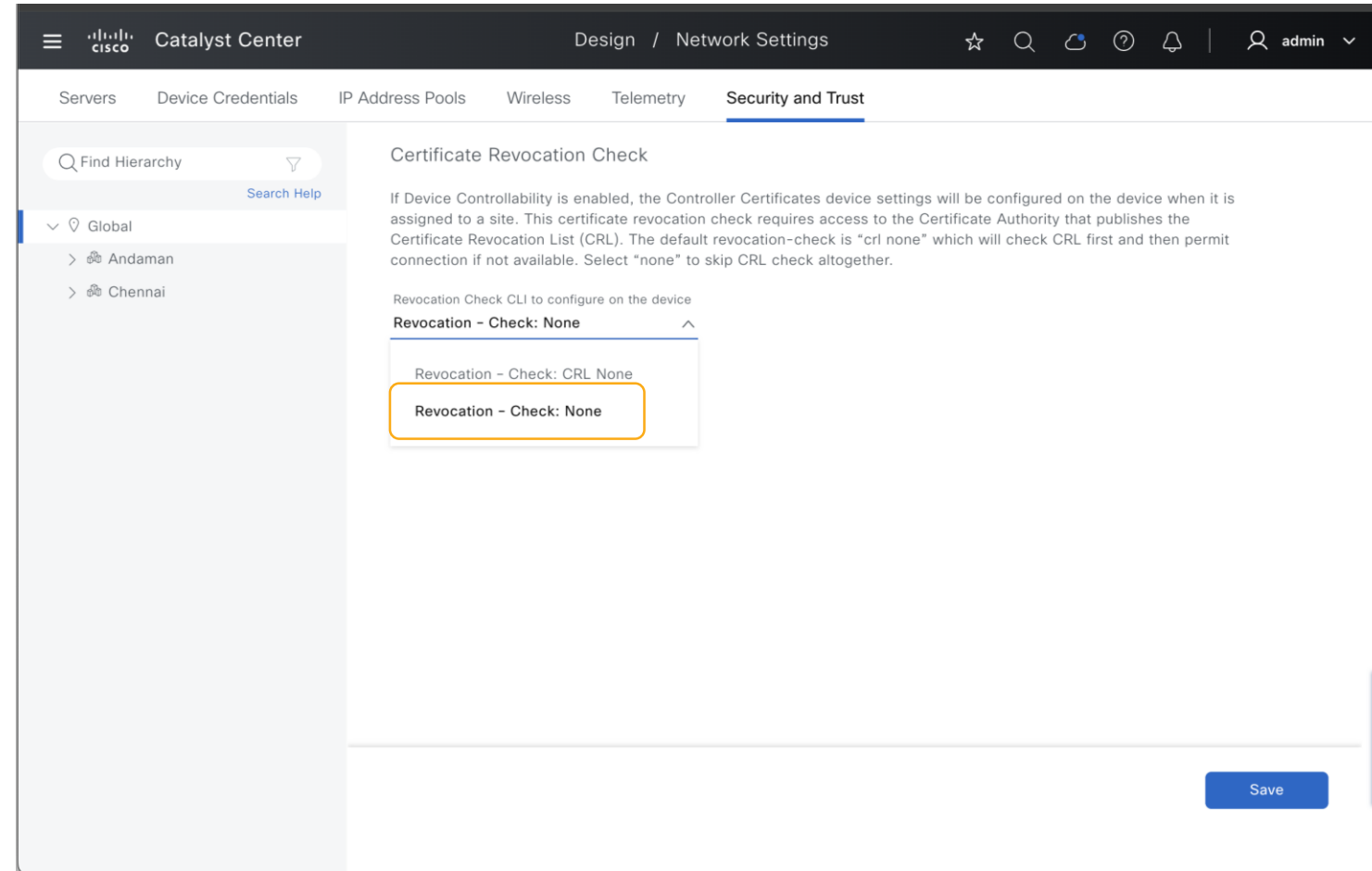
For your reference



Managed only

# Certificates- Tips & Tricks

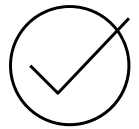
### Streaming Telemetry data (TDL) using TLS



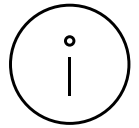
Disable Certificate Revocation Checks



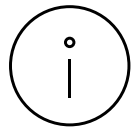
# Application Visibility



Enable Application Telemetry from Provision > Actions > Telemetry > Enable Application Telemetry



WLC need not be provisioned for enabling Application telemetry

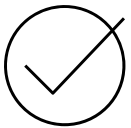


Supported for local, Flex/Fabric SSIDs

The screenshot shows the Cisco Catalyst Center interface. On the left, a table lists devices under the 'Provision' focus. The 'POD4-C9800-CL1' device is selected, and the 'Telemetry' action is chosen from the dropdown menu. The right pane shows the 'Enable Application Telemetry' configuration for this device. It includes a warning about network disruption and a note about disabling and re-enabling the feature. The configuration for 'POD4-C9800-CL1' shows 'Local' selected for the application telemetry source, with 'Flex/Fabric' and 'Include Guest SSIDs' options unselected. The 'Telemetry Source' is set to 'NetFlow'. At the bottom right, there are 'Cancel' and 'Enable' buttons.



# Application Visibility- Tips & Tricks



Enable Application Telemetry temporarily Disables policy profiles

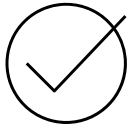
```
C9800-Virtual#wireless profile policy
xxx
shutdown
ipv4 flow monitor avc_ipv4_assurance
input
ipv4 flow monitor
avc_ipv4_assurance_dns input
ipv4 flow monitor
avc_ipv4_assurance_rtp input
...
no shutdown
```



# Application Visibility- Tips & Tricks



Enable Application Telemetry temporarily Disables policy profiles



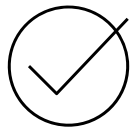
Application Telemetry enables DNS Service monitoring (local mode) 17.10 and above for both IPv4 and IPv6

```
C9800-Virtual#wireless profile policy
xxx
shutdown
ipv4 flow monitor avc_ipv4_assurance
input
ipv4 flow monitor avc_ipv4_assurance_dns
input
ipv4 flow monitor avc_ipv4_assurance_rtp
input
...
no shutdown
```

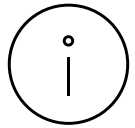


# Intelligent Capture & Anomaly Detection

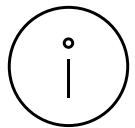
Assurance > Settings > Intelligent Capture Settings



Enable AP Stats and Anomaly Capture for Specific APs or Selected WLC



AP stats limited to 1000 APs



For newly added AP Join Profiles, iCAP needs to be pushed by Disabling & Enabling

Catalyst Center Settings / Intelligent Capture Setting

Onboarding Packet Capture Full Packet Capture OTA Sniffer Capture **Access Point**

Access Point

AP Stats Capture  Anomaly Capture

Specific - select specific APs and enable  Global - select specific WLCs and enable

Search Table

1 Selected Enable Disable

Device Name	Configuration Status	IP Address	Model	OS Version	Overall Health	Location
<input checked="" type="checkbox"/> C9800-vWLC	Not Configured	192.168.4.40	C9800-CL-K9	17.14.1	--	--
<input type="checkbox"/> POD4-C9800-40	Not Configured	192.168.4.5	C9800-40-K9	17.9.3	--	--

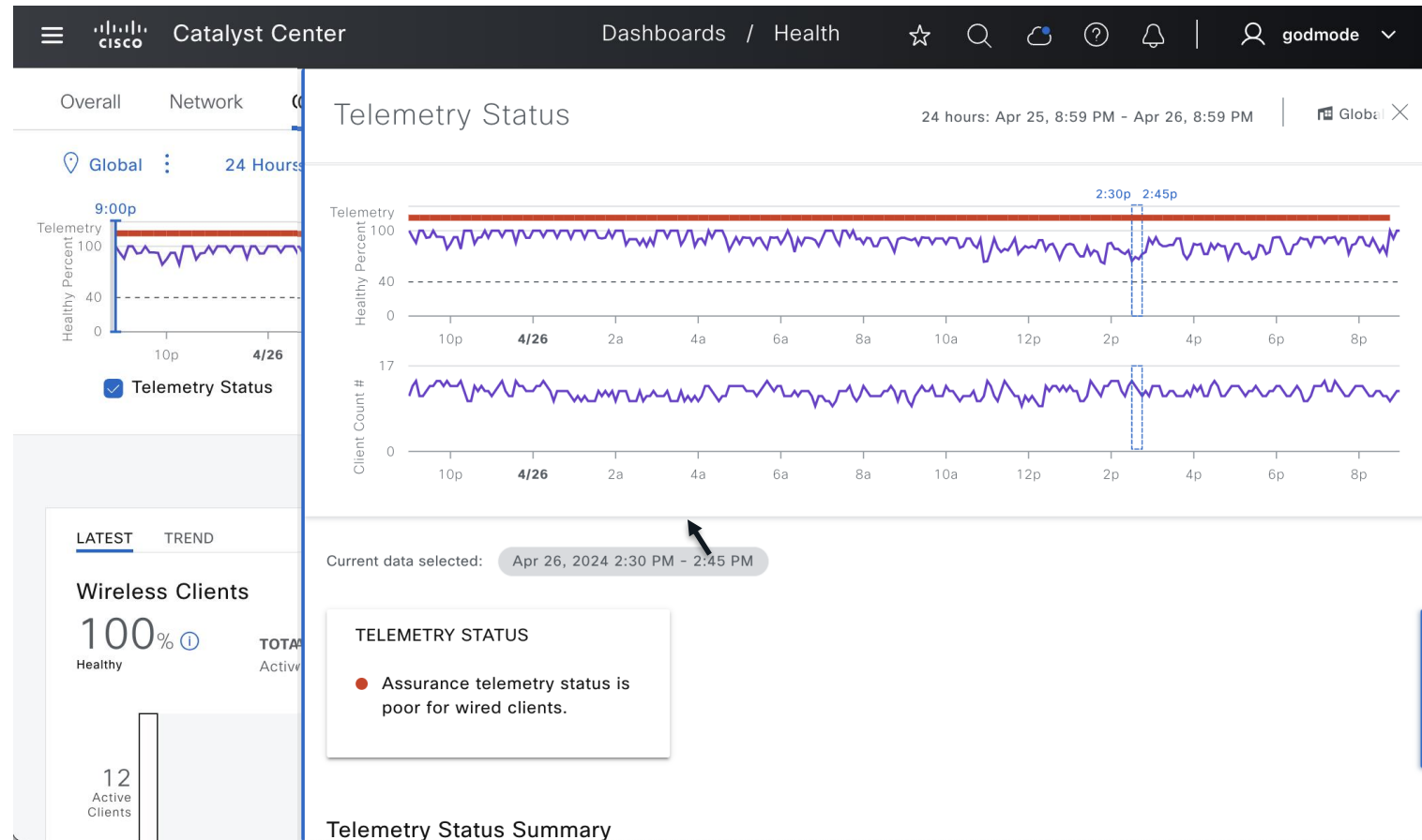
# Visibility into Telemetry Status



Gain Visibility into Telemetry received for Network Devices, Clients and Applications



Insights into summary of Telemetry Status for easier troubleshooting



# Troubleshoot Telemetry

```
POD4-C9800-CL1#sh telemetry connection all
Telemetry connections
```

Index	Peer Address	Port	VRF	Source Address	State	State Description
109	172.100.1.53	25103	0	192.168.4.7	Active	Connection up

```
POD4-C9800-CL1#sh telemetry ietf subscription summary
Subscription Summary
```

```
=====
Maximum supported: 128
```

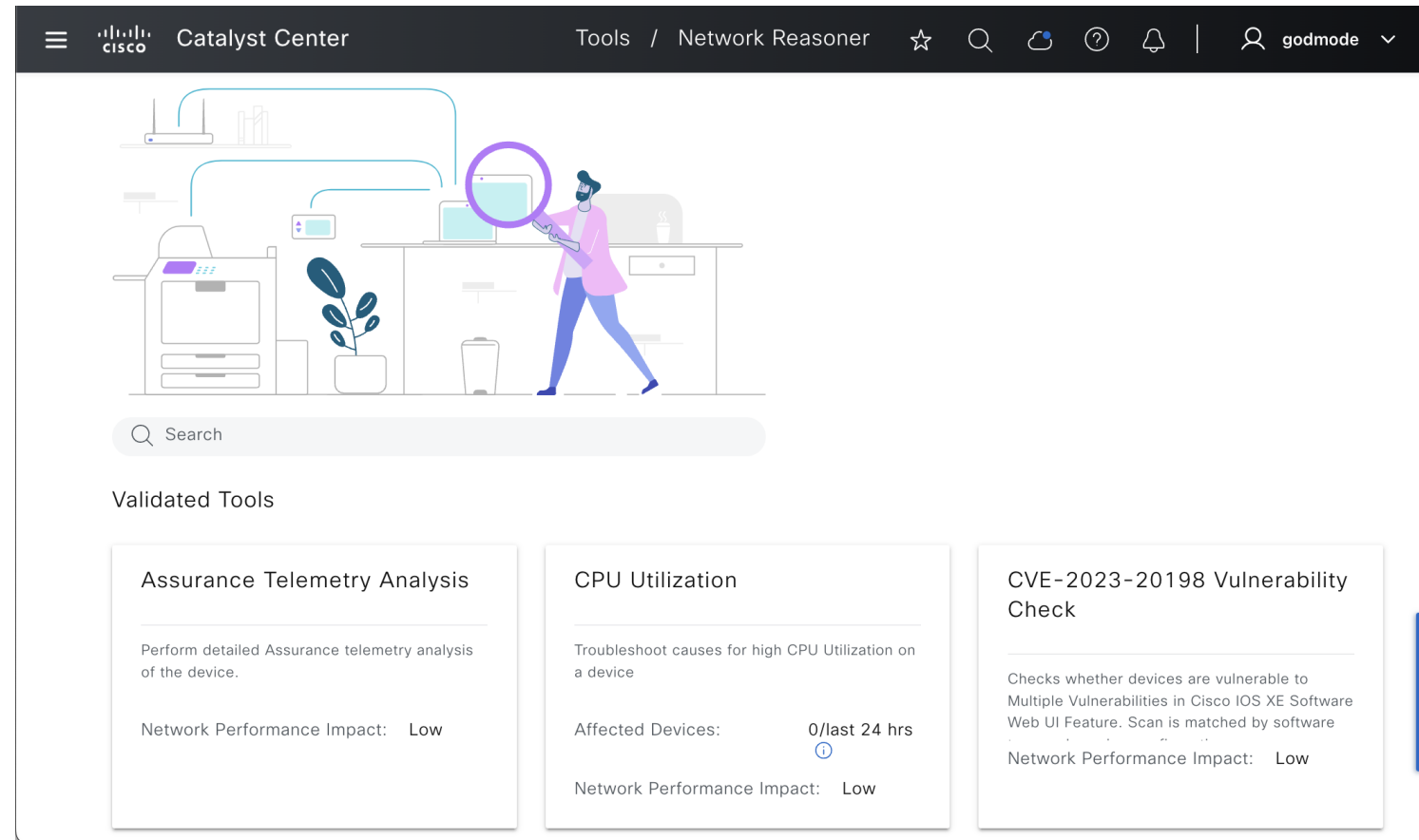
Subscription	Total	Valid	Invalid
All	112	112	0
Dynamic	0	0	0
Configured	112	112	0
Permanent	0	0	0

Active - All good  
Connecting - Cert/FW issue  
N/A - Telemetry config missing

# MRE- Troubleshoot Telemetry



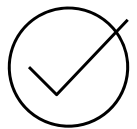
From Tools > Network Reasoner,  
Launch Assurance Telemetry  
Analysis



The screenshot shows the Cisco Catalyst Center Network Reasoner interface. At the top, the navigation bar includes the Cisco logo, 'Catalyst Center', and 'Tools / Network Reasoner'. Below the navigation bar is a large illustration of a person in a pink shirt and blue pants looking at a laptop, with various network devices and a plant in the background. A search bar is located below the illustration. Underneath the search bar, there is a section titled 'Validated Tools' which contains three tool cards:

- Assurance Telemetry Analysis**: Perform detailed Assurance telemetry analysis of the device. Network Performance Impact: Low
- CPU Utilization**: Troubleshoot causes for high CPU Utilization on a device. Affected Devices: 0/last 24 hrs. Network Performance Impact: Low
- CVE-2023-20198 Vulnerability Check**: Checks whether devices are vulnerable to Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature. Scan is matched by software. Network Performance Impact: Low

# MRE- Troubleshoot Telemetry



Select the device and click troubleshoot for MRE to analyze Telemetry data collection



Conclusions provide details on what might cause telemetry issues

The screenshot shows the Cisco Catalyst Center interface for Assurance Telemetry Analysis. The navigation pane on the left includes a search hierarchy with categories like Global, Bangalore, Ekahau Wi-Fi, Italy, Kosovo, Las Vegas, San Jose, and various buildings. The main content area is titled 'Assurance Telemetry Analysis' and shows a 'Root Cause Analysis' section. A 'Reasoning Activity' tab is selected, displaying 'Conclusions (12)'. The conclusions are represented by seven hexagonal tiles, each with a checkmark and a task name: 'Check Device Controllability status on Catalyst Center', 'Check Assurance config auto-correct setting on Catalyst Center', 'Check device manageability', 'Check Device Site', 'Check device active issues', 'Check Context-cache', and 'Check if device is present in database'. A 'Run Again' button is located in the top right corner of the analysis area.

# Telemetry- Force Push



Force push telemetry config from  
Inventory > Actions > Telemetry >  
Update Telemetry Settings

The screenshot shows the Catalyst Center interface with the 'Update Telemetry Settings' dialog open. The dialog is titled 'Update Telemetry Settings' and has a close button (X) in the top right corner. At the top left of the dialog, there is a warning icon and a message: 'This release enables new telemetry subscription is provided in this release for NETCONF and will be applied to the applic...'. Below this, there is a 'Global' section with a location pin icon. The main content area shows a list of devices under the heading 'Devices (1) Focus: Default'. A search bar is present with the text 'Click here to apply basic or advanced filter'. Below the search bar, there are options for '1 Selected', 'Tag', '+ Add Device', and 'Actions'. A table of devices is shown with columns for 'Tags' and 'Device Name'. One device is selected: 'LIVE-C9800-40-SSO.wireless-tme.com' with a 'Watchlist' tag. To the right of the device list, there is a 'Force Configuration Push' checkbox which is currently unchecked. Below this, a list of settings is shown for the selected device. The settings are: Syslog Server (Catalyst Center), Cisco TrustSec (CTS) Credentials (Yes), Streaming Telemetry (Yes), SNMP Trap Receiver (Catalyst Center), DNS Server ((Domain name: wireless-tme.com), 10.10.105.7), DTLS Ciphersuite (Skipped), AP Impersonation (Enabled (Infra MFP)), Syslog Level (6 - Information Messages), and Controller Certificates (Yes (Expires on: Mar 29, 2025)). At the bottom right of the dialog, there are 'Cancel' and 'Next' buttons.

Catalyst Center Provision / Inventory godmode

Update Telemetry Settings

Force Configuration Push

GLOBAL/SAN JOSE/BUILDING 14

LIVE-C9800-40-SSO.wireless-tme.com

The following settings will be deployed during assignment to site.

Syslog Server	Catalyst Center
Cisco TrustSec (CTS) Credentials	Yes
Streaming Telemetry	Yes
SNMP Trap Receiver	Catalyst Center
DNS Server	(Domain name: wireless-tme.com), 10.10.105.7
DTLS Ciphersuite	Skipped
AP Impersonation	Enabled (Infra MFP)
Syslog Level	6 - Information Messages
Controller Certificates	Yes (Expires on: Mar 29, 2025 )

Cancel Next

# Scenario- User Onboarding Issue



Not able to connect to my application



Helpdesk

Authentication Problem?, RF Issue or app problem?

Network is stable. Must be the app.



Network Ops



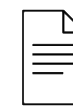
IT Routing Loop

Code is fine. Don't care about anything else

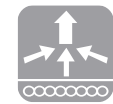


AppDev

Dear User: We do not have enough info/context to troubleshoot further and are thus wait/closing your case.



For your reference



Managed only

# AI-Enhanced RRM

## Instantaneous visibility

**Summary**

SUMMARY	RF PERFORMANCE SUMMARY	RF COVERAGE SUMMARY	AI RF PROFILE SIMULATOR
15 Total AP Count	3 Total Clients	48 / 100 RRM Performance	0% APs with High CCI
	2 RRM Changes	High AP Density	High (41 dB) Connectivity

**Insights**

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

**Actionable insights**

**Performance**

**RRM Changes**

Channel Change	Channel Width Change	Tx Power Change	RF Bandwidth Change
1	0	0	0

**FRA Changes**

2.4 GHz	5 GHz	60GHz
27	0	0

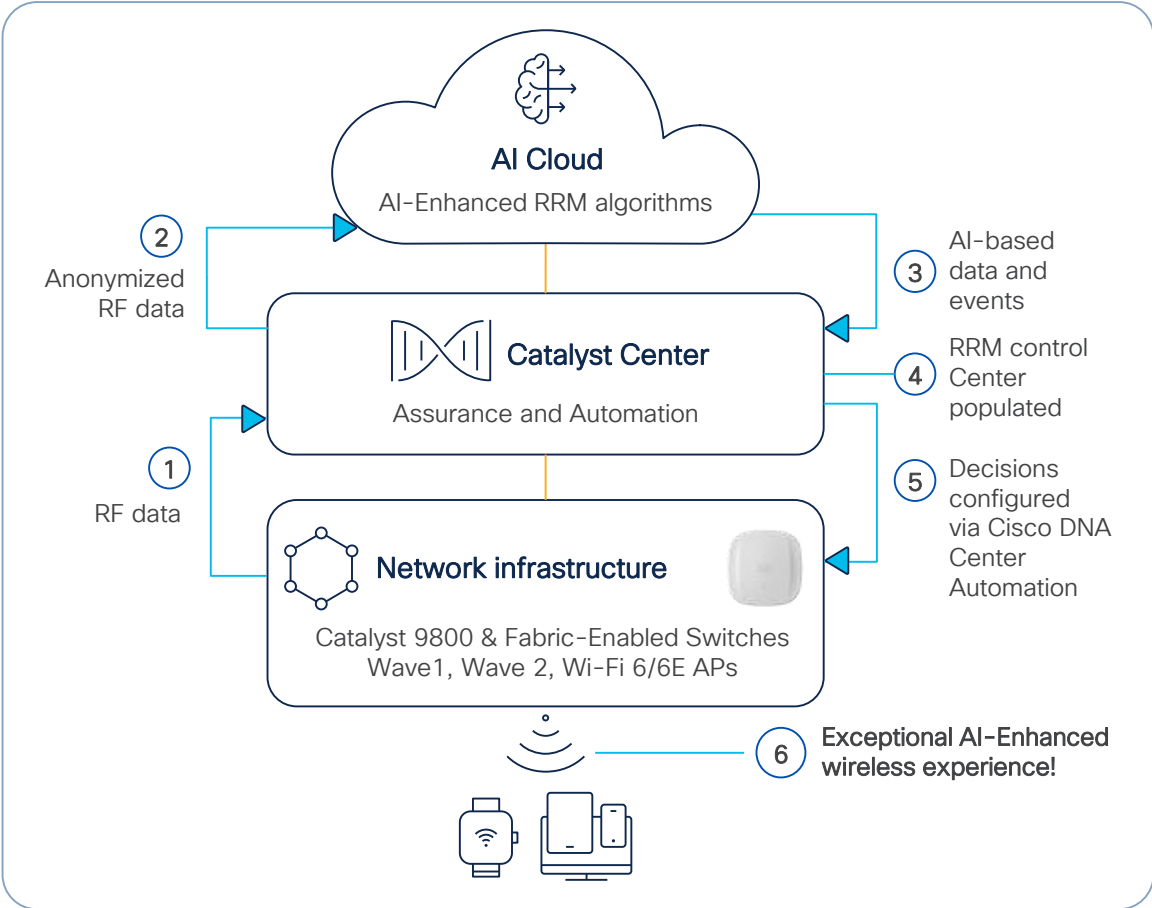
**RRM Performance**

Power(0-30)	Power(31-60)	Power(61-100)
16	0	0

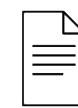
**Co-Channel Interference**

Low	Medium	High
16	0	0

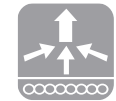
## Proactive optimizations



# Enabling AI-Enhanced RRM-Assurance Only

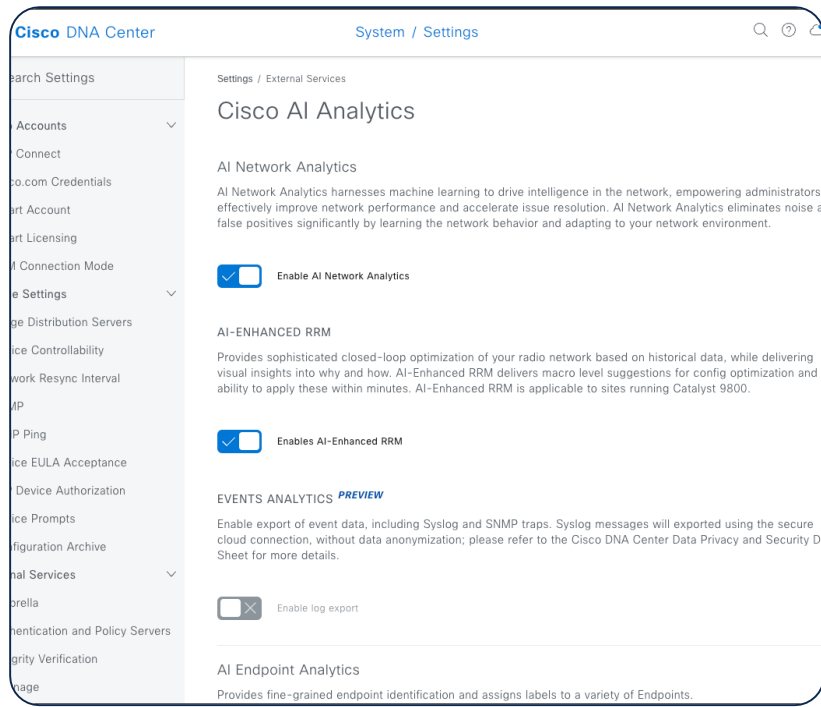


For your reference

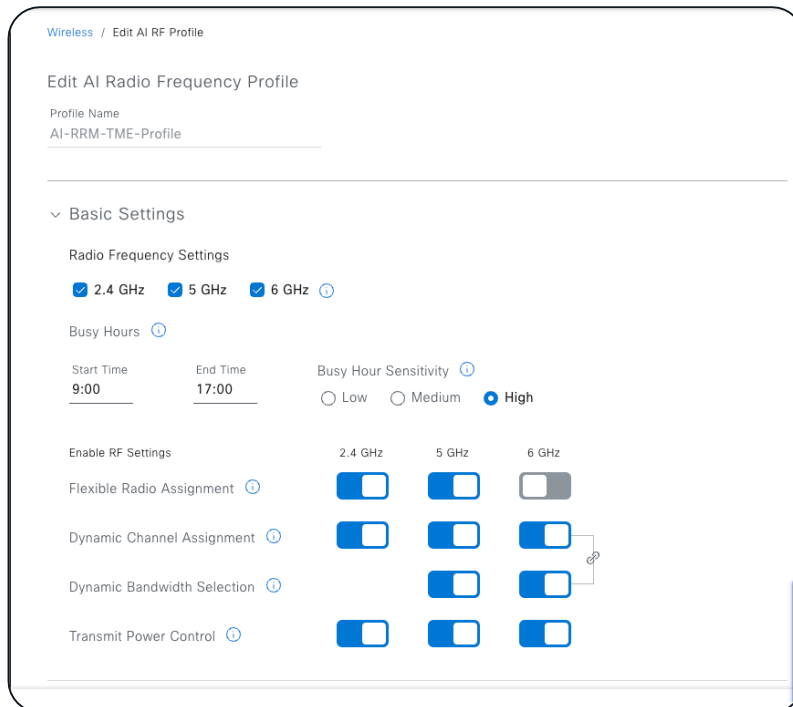


Managed only

1 Give AI-Enhanced RRM Cloud Access in Settings.



2 Create an AI RF Profile.



3 Assign AI RF Profile C9800 WLC.

**Configure AI-Enhanced RRM**

Deploy AI-Enhanced RRM with or without provisioning your wireless controllers and access points

**Wireless**

**Enable Without Device Provisioning**

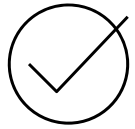
This flow enables AI-Enhanced RRM without provisioning your wireless controllers or access points from Catalyst Center. You may provision using your choice of tool or WLC WebUI or CLI.

If you do not want Catalyst Center to manage the configuration of your devices, choose this option.

# Observe PoE Analytics



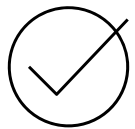
Assurance > PoE Dashboard



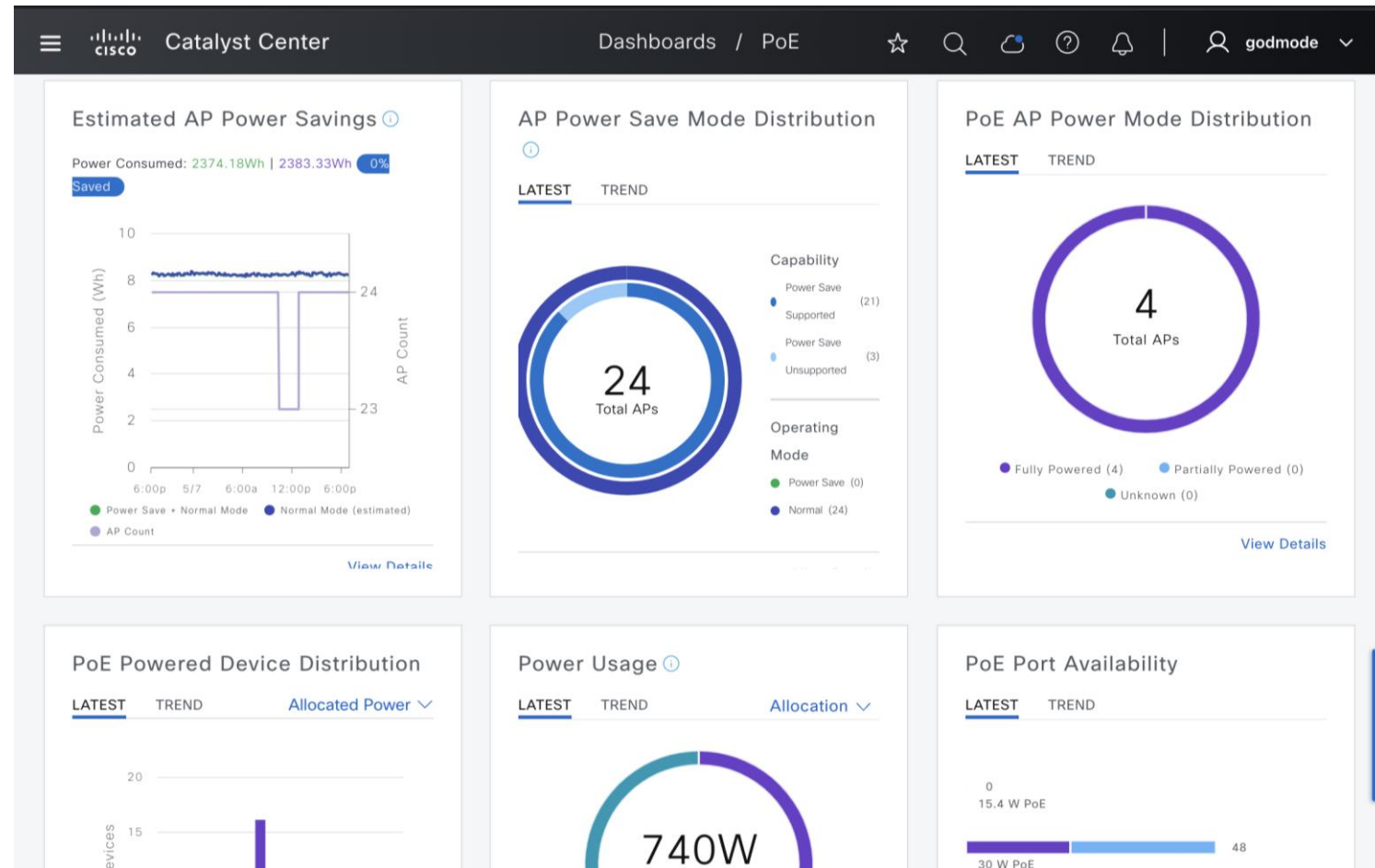
Requires IOS-XE 17.10 and above



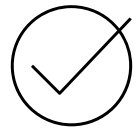
Switches where APs are connected needs to be added to inventory



Switches should be enabled with NETCONF and telemetry



# Observe Wi-Fi6 Dashboard



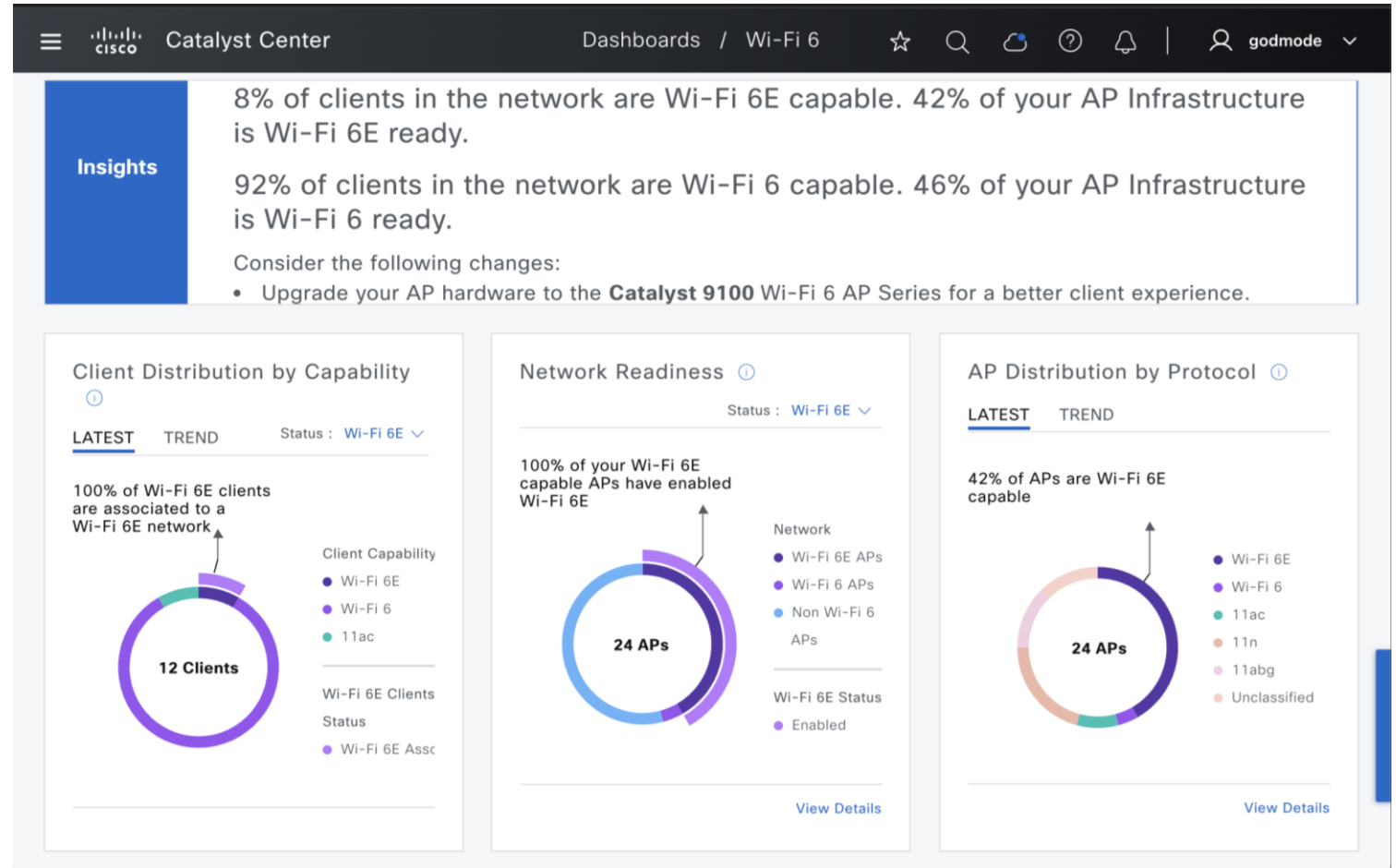
Insights into Wi-Fi 6/6E readiness



Details of Client Distribution by capacity



Network Readiness, Wireless Air Time Efficiency

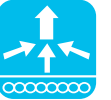


Helps plan upgrade your network to Wi-Fi 6E for Enhanced Security (WPA3), Increased Bandwidth with Lesser interference



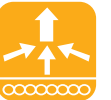
# Refresh AP

The screenshot shows the Cisco Catalyst Center interface. On the left is a navigation sidebar with options: Design, Policy, Provision, Assurance, Workflows (highlighted), Tools, Platform, Activities, Reports, System, and Explore. The main content area is titled 'Workflows' and features a header with a search icon, a refresh icon, a notification bell, and a user profile 'admin'. Below the header, there's a main heading 'Maintain your network efficiently with Workflows.' followed by an illustration of a person at a laptop with a city skyline. A section titled 'Network Devices' contains a grid of workflow cards: 'Replace Device' (with 'Wired' and 'Wireless' tags), 'Access Point Refresh' (with 'Wireless' tag), 'Smart License Compliance', 'Configure REP Ring (Fabric)', 'Configure Access Points', and 'Provision Template'.



## Assurance Usecase

AP will not be provisioned in this scenario and only old configuration will be copied



## Automation Usecase

AP will be provisioned in this scenario



# Refresh APs- Tips & Tricks

- ✓ Old AP needs to be Assigned to Site
- ✓ New AP should not be Assigned to Sites
- ✓ For Pre-staging, Old AP need not be in unreachable state for completing the workflow
- ✓ If new AP is connected to same switch port, workflow will auto detect new AP

Catalyst Center Access Point Refresh ☆ 🔍 🔄 ?

### Assign New APs to Old APs

You have selected 1 Old APs for refresh. Assign New AP for each Old one. If New AP(s) is already connected, it will be detected in Catalyst Center either through WLC inventory or PnP based on the existing configuration. If New AP is not yet connected, provide the Serial Number of those New APs against each Old AP.

You can also download the Old APs list in CSV format, provide the details of the New AP against each Old AP and Upload it.

Would you like to auto detect your APs based on Switch Port **NEW**

ACCESS POINTS (1)

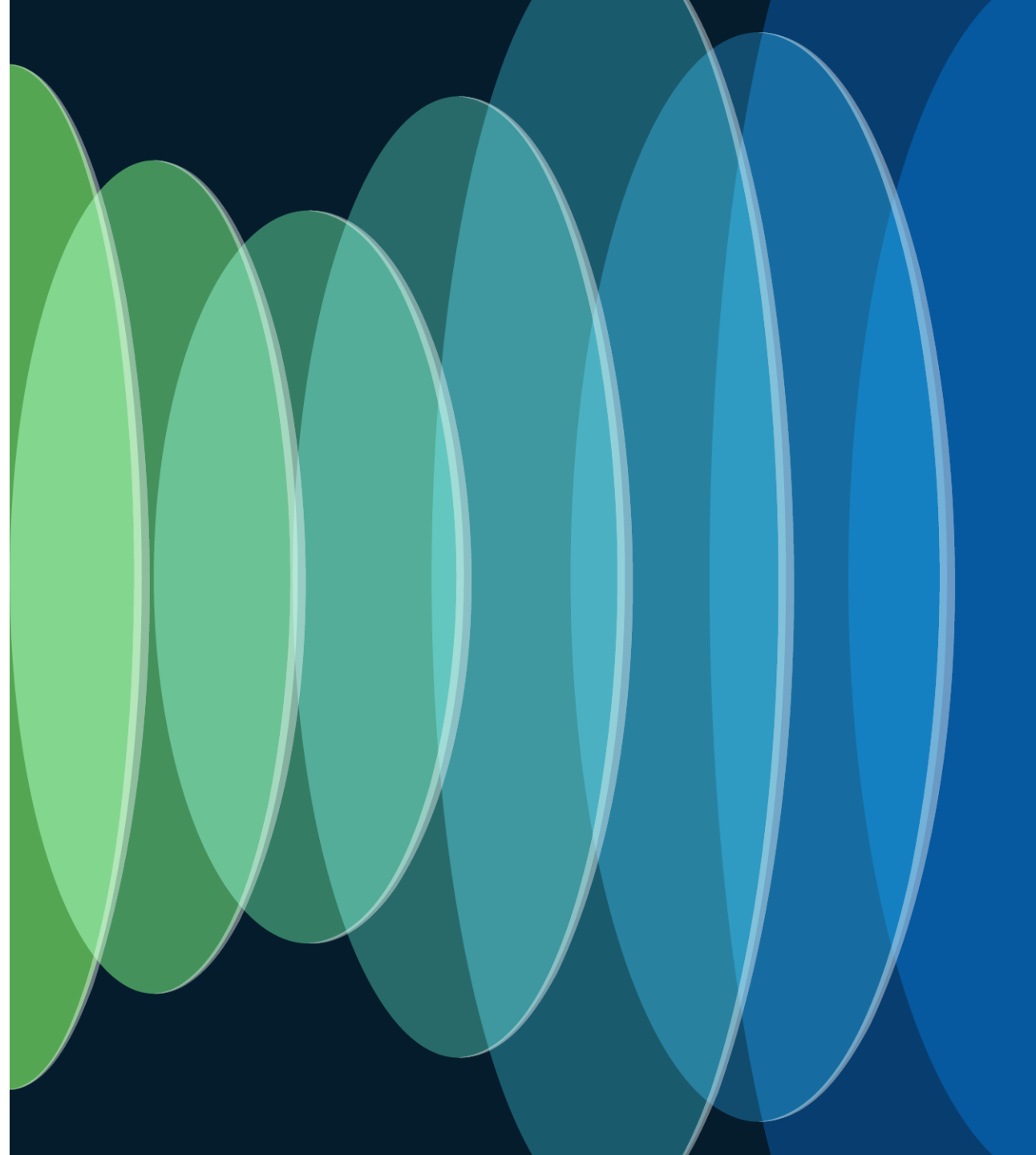
🔍 Search Table

[Upload CSV](#) [Download CSV](#) 1 Selected [Delete](#)

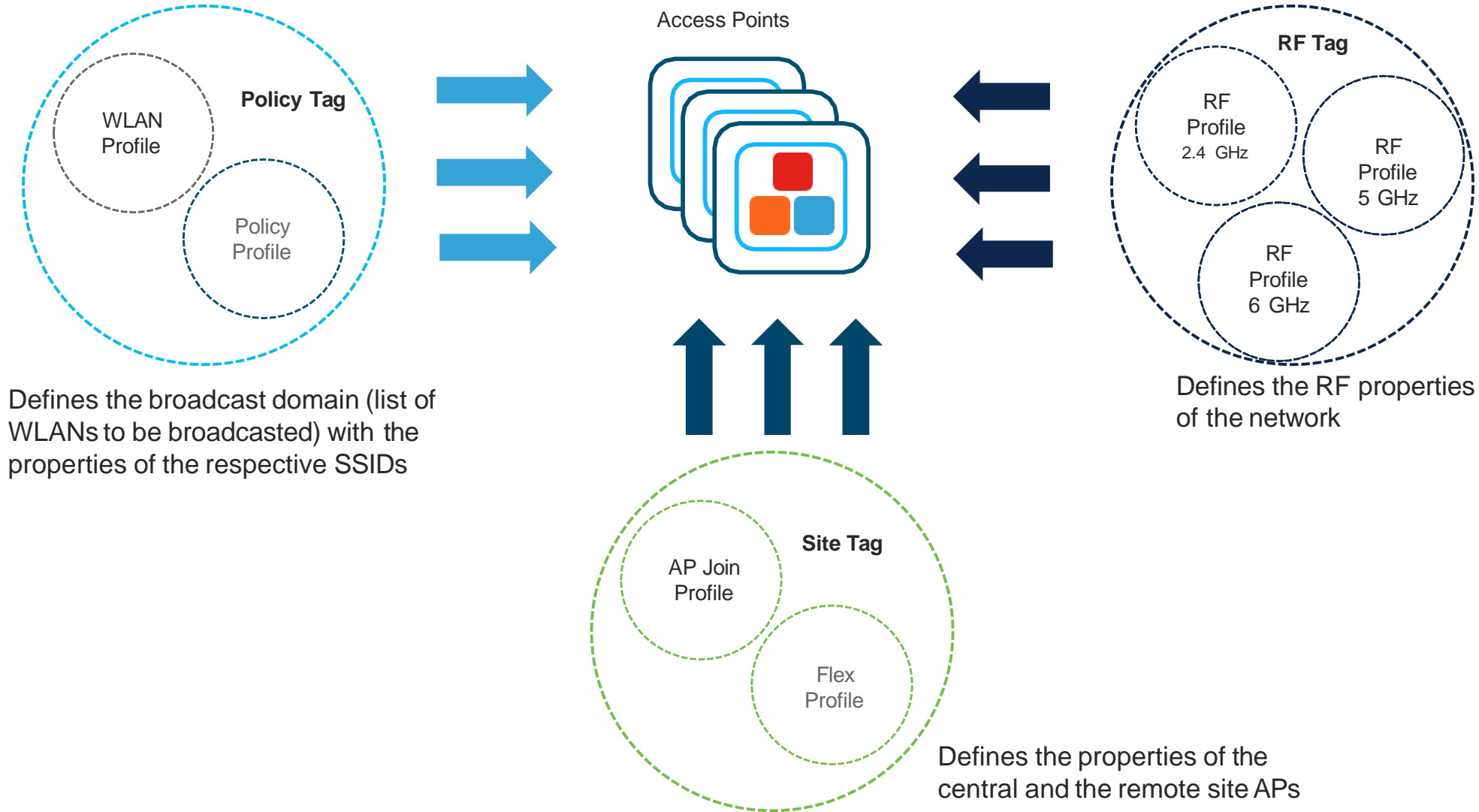
Old Devices			New Devices			
Device Name	Platform	Site	Edit	Device Name*	Platform	Serial Number* ⓘ
<input checked="" type="checkbox"/> POD4-AP3 192.168.4.74 FGL2245A8EK	AIR-AP4800-D-K9 Cisco 4800 Series ...	..India/Bengaluru	<a href="#">✎</a>	POD4-AP3	C9115AXI-D	abc

# Learn how to Completely Automate Wireless Network

CISCO *Live!*



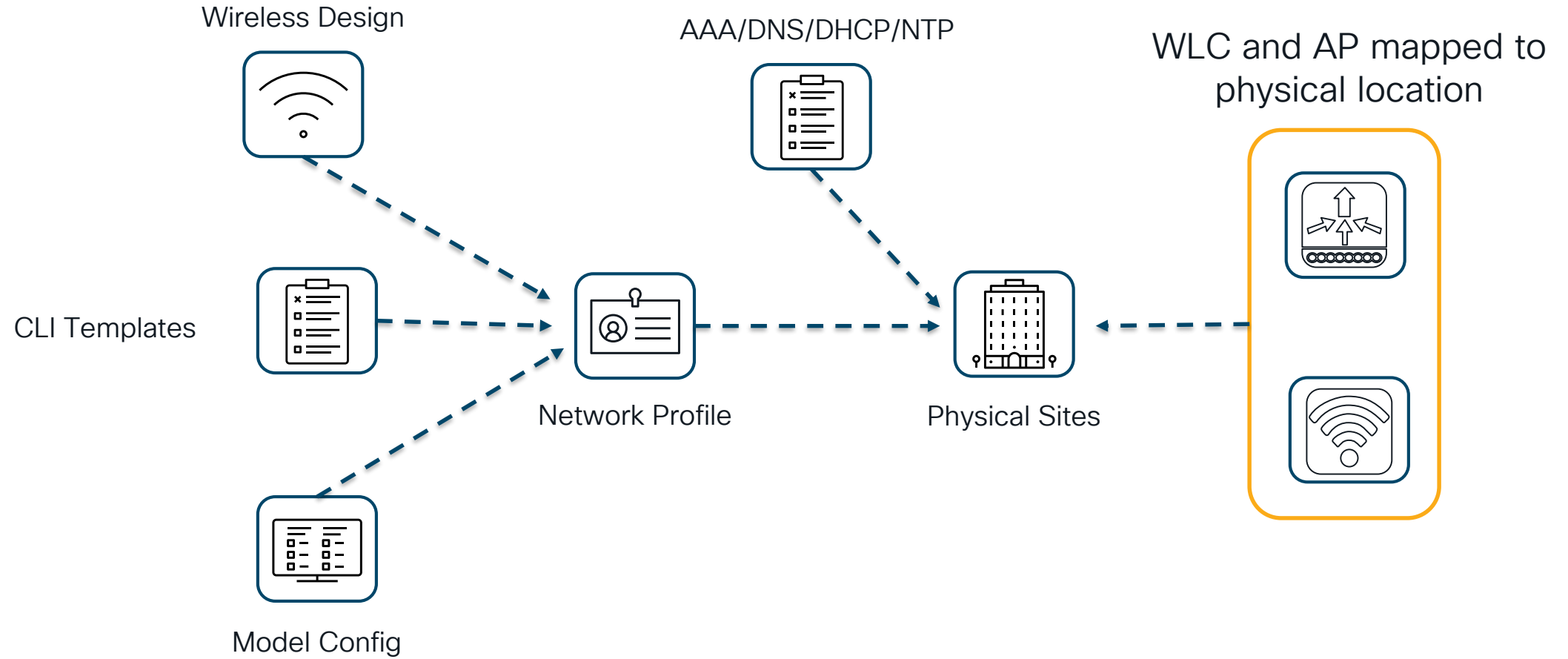
# Cisco C9800 Config Model



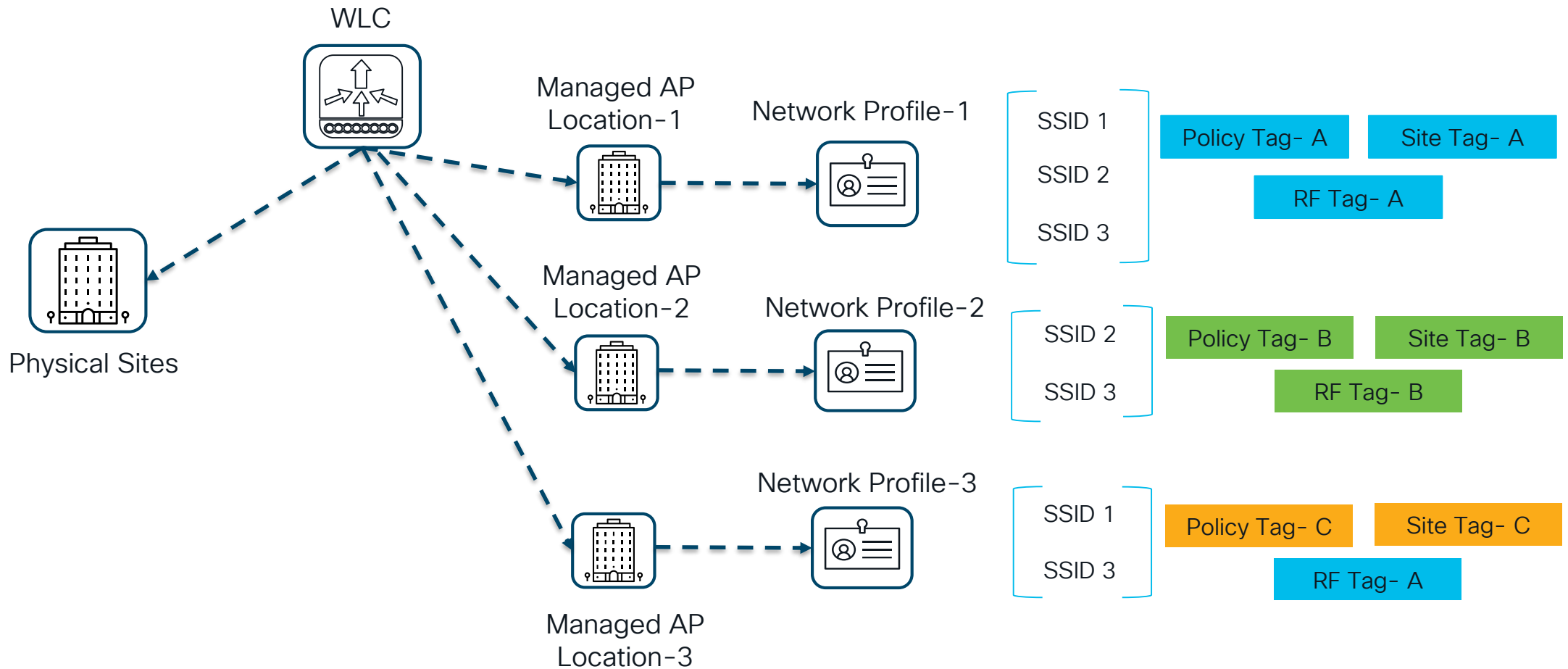
# Catalyst Center Wireless Intent Design



# Catalyst Center Wireless Intent Design

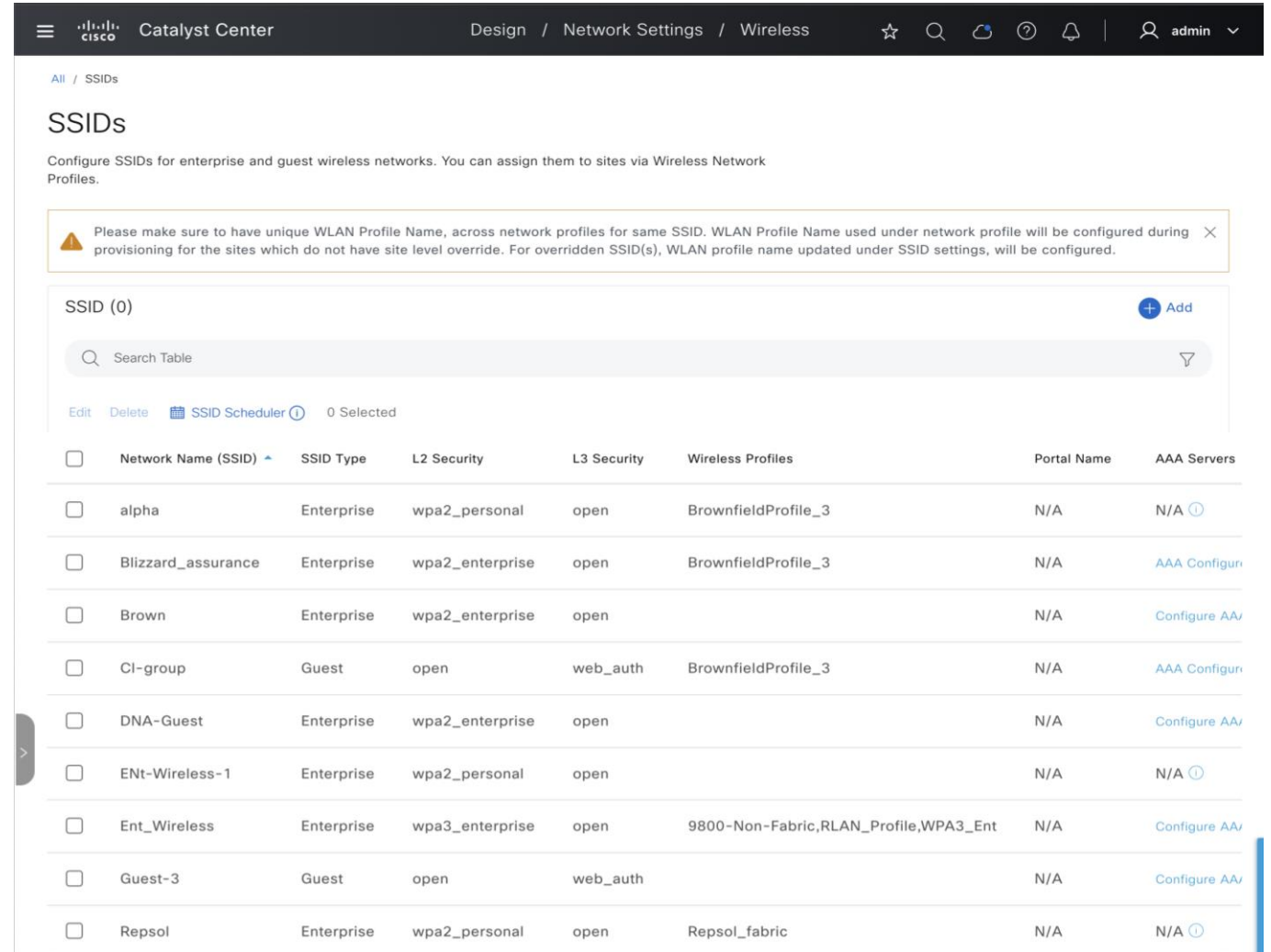


# Managed AP Location & Network Profile



# Wireless Design- Definition Areas


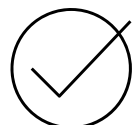
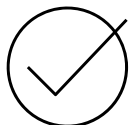
Wireless Settings	Site Element
SSID	Global/Area/Building/Floor
SSID Scheduler	Global
RF	Global
Wireless Interface	Global
Antenna Radio Profile	Global
AP Authorization List	Global
Anchor Group	Global
VLAN Group	Global
Pre-Auth ACL	Global
AP Authentication (PnP)	Global
DNA Spaces/CMX Integration	Global/Area/Building/Floor
Flex Connect VLAN	Global/Area/Building/Floor
AAA Override VLAN	Global/Area/Building/Floor
AP Impersonation	Global/Area/Building/Floor
aWIPS and Forensic Capture	Global/Area/Building/Floor
Configure DTLS Cipher suites	Global/Area/Building/Floor
Remote Teleworker	Area
Mesh Settings	Floor

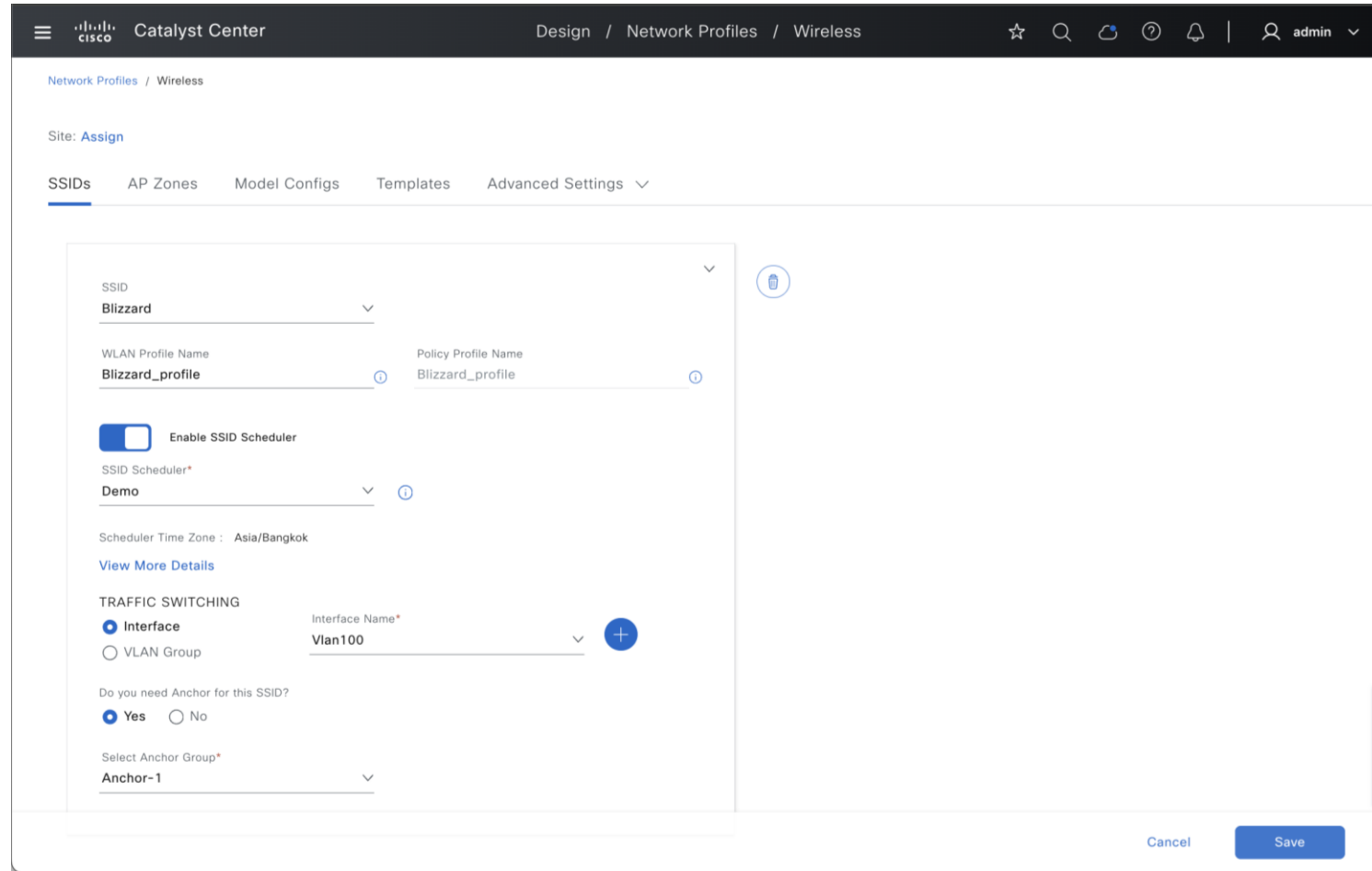


The screenshot shows the Catalyst Center interface for SSID configuration. The breadcrumb trail is Design / Network Settings / Wireless. The page title is SSIDs. A warning message states: "Please make sure to have unique WLAN Profile Name, across network profiles for same SSID. WLAN Profile Name used under network profile will be configured during provisioning for the sites which do not have site level override. For overridden SSID(s), WLAN profile name updated under SSID settings, will be configured." Below the warning is a table of SSIDs with columns for Network Name (SSID), SSID Type, L2 Security, L3 Security, Wireless Profiles, Portal Name, and AAA Servers. The table contains 12 rows of SSID configurations.

Network Name (SSID)	SSID Type	L2 Security	L3 Security	Wireless Profiles	Portal Name	AAA Servers
alpha	Enterprise	wpa2_personal	open	BrownfieldProfile_3	N/A	N/A
Blizzard_assurance	Enterprise	wpa2_enterprise	open	BrownfieldProfile_3	N/A	AAA Configur
Brown	Enterprise	wpa2_enterprise	open		N/A	Configure AA
Cl-group	Guest	open	web_auth	BrownfieldProfile_3	N/A	AAA Configur
DNA-Guest	Enterprise	wpa2_enterprise	open		N/A	Configure AA
ENT-Wireless-1	Enterprise	wpa2_personal	open		N/A	N/A
Ent_Wireless	Enterprise	wpa3_enterprise	open	9800-Non-Fabric,RLAN_Profile,WPA3_Ent	N/A	Configure AA
Guest-3	Guest	open	web_auth		N/A	Configure AA
Repsol	Enterprise	wpa2_personal	open	Repsol_fabric	N/A	N/A

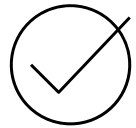
# Network Profile Mappings

-  Design > Network Profile > Wireless
-  Options to enable
  - SSID Scheduler
  - Create additional L2 Interfaces
  - Map Anchor Groups
-  Assign Network Profiles to Sites

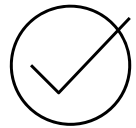


The screenshot shows the Cisco Catalyst Center interface for configuring a Network Profile. The breadcrumb navigation is Design / Network Profiles / Wireless. The page title is Network Profiles / Wireless. The site is set to Assign. The configuration is for the SSID 'Blizzard'. The WLAN Profile Name is 'Blizzard\_profile' and the Policy Profile Name is 'Blizzard\_profile'. The 'Enable SSID Scheduler' checkbox is checked. The SSID Scheduler is set to 'Demo' with a time zone of 'Asia/Bangkok'. Under TRAFFIC SWITCHING, the 'Interface' radio button is selected, and the Interface Name is 'Vlan100'. The question 'Do you need Anchor for this SSID?' is answered 'Yes'. The Select Anchor Group is 'Anchor-1'. There are 'Cancel' and 'Save' buttons at the bottom right.

# Custom Site Tags & Policy Tags



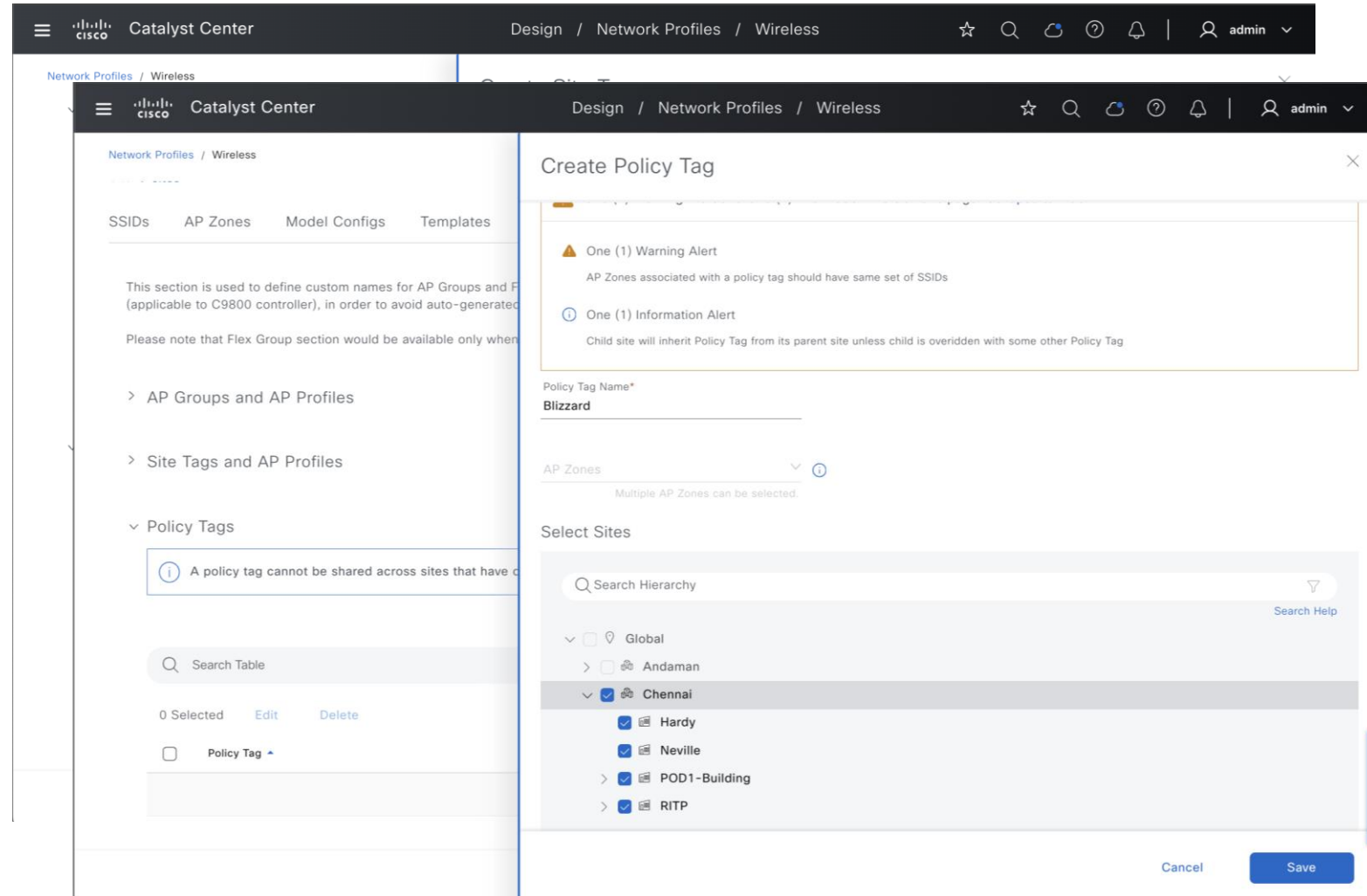
Site & Policy Tags can be re-used across multiple floors in a building



AP Join Profiles mapped to Custom Site Tags



AP Zones mapped to Policy Tags



Catalyst Center Design / Network Profiles / Wireless

Network Profiles / Wireless

SSIDs AP Zones Model Configs Templates

This section is used to define custom names for AP Groups and Profiles (applicable to C9800 controller), in order to avoid auto-generated names.

Please note that Flex Group section would be available only when Flex Group is enabled.

> AP Groups and AP Profiles

> Site Tags and AP Profiles

< Policy Tags

A policy tag cannot be shared across sites that have different AP Zones.

Search Table

0 Selected Edit Delete

Policy Tag

Create Policy Tag

One (1) Warning Alert  
AP Zones associated with a policy tag should have same set of SSIDs

One (1) Information Alert  
Child site will inherit Policy Tag from its parent site unless child is overridden with some other Policy Tag

Policy Tag Name\*  
Blizzard

AP Zones  
Chennai  
Multiple AP Zones can be selected.

Select Sites

Search Hierarchy

Global

Andaman

Chennai

Hardy

Neville

POD1-Building

RITP

Cancel Save

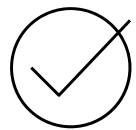
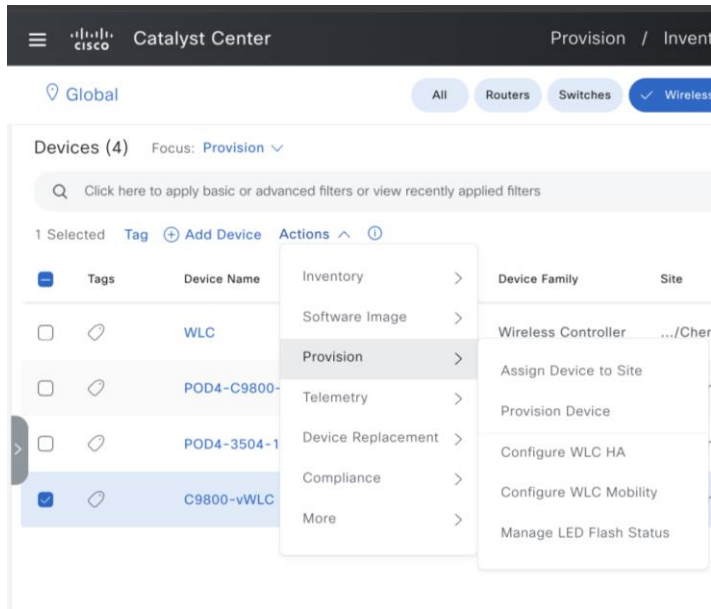


# AP Join Profile

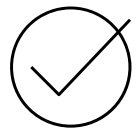
- ✓ Configure AP Credentials
- ✓ aWIPS/Rogue Detection Settings
- ✓ Mesh Bridge Group & Backhaul settings
- ✓ Power Profiles and Calendar Profiles for APs

The screenshot shows the 'Create Access Point Profile' configuration page in Cisco Catalyst Center. The page is for an IOS-XE based profile. The 'AP Profile Name' is 'Chennai-AP'. The 'Description' field is empty. There is a checkbox for 'Remote Teleworker' which is currently unchecked. The 'Power' tab is selected, showing the 'AP Power Profile' section with a dropdown menu set to 'Deny 24 Ghz'. Below that is the 'Calendar Power Profile' section. At the bottom right, there are 'Cancel' and 'Save' buttons.

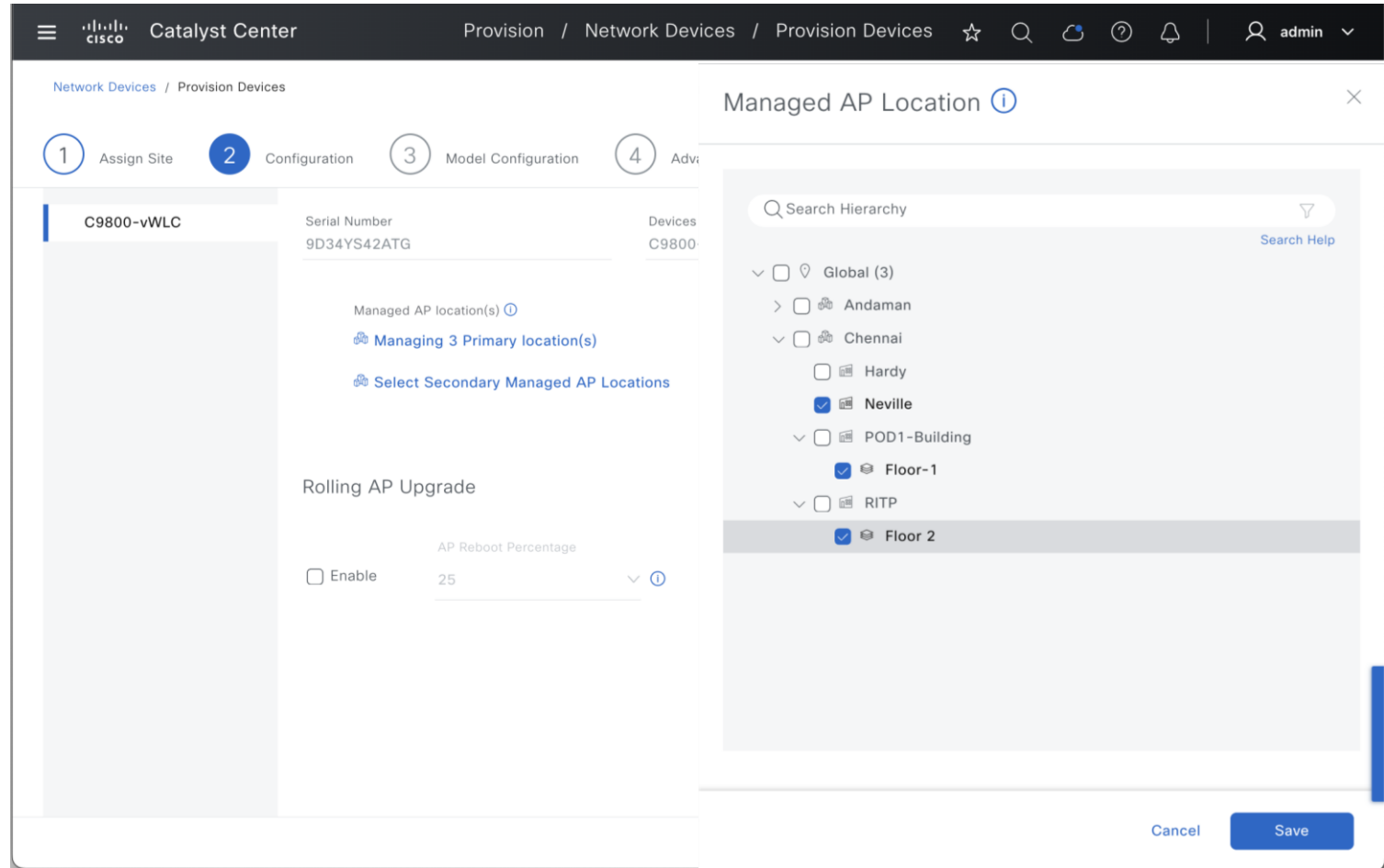
# Provisioning WLC (Primary WLC)



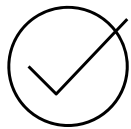
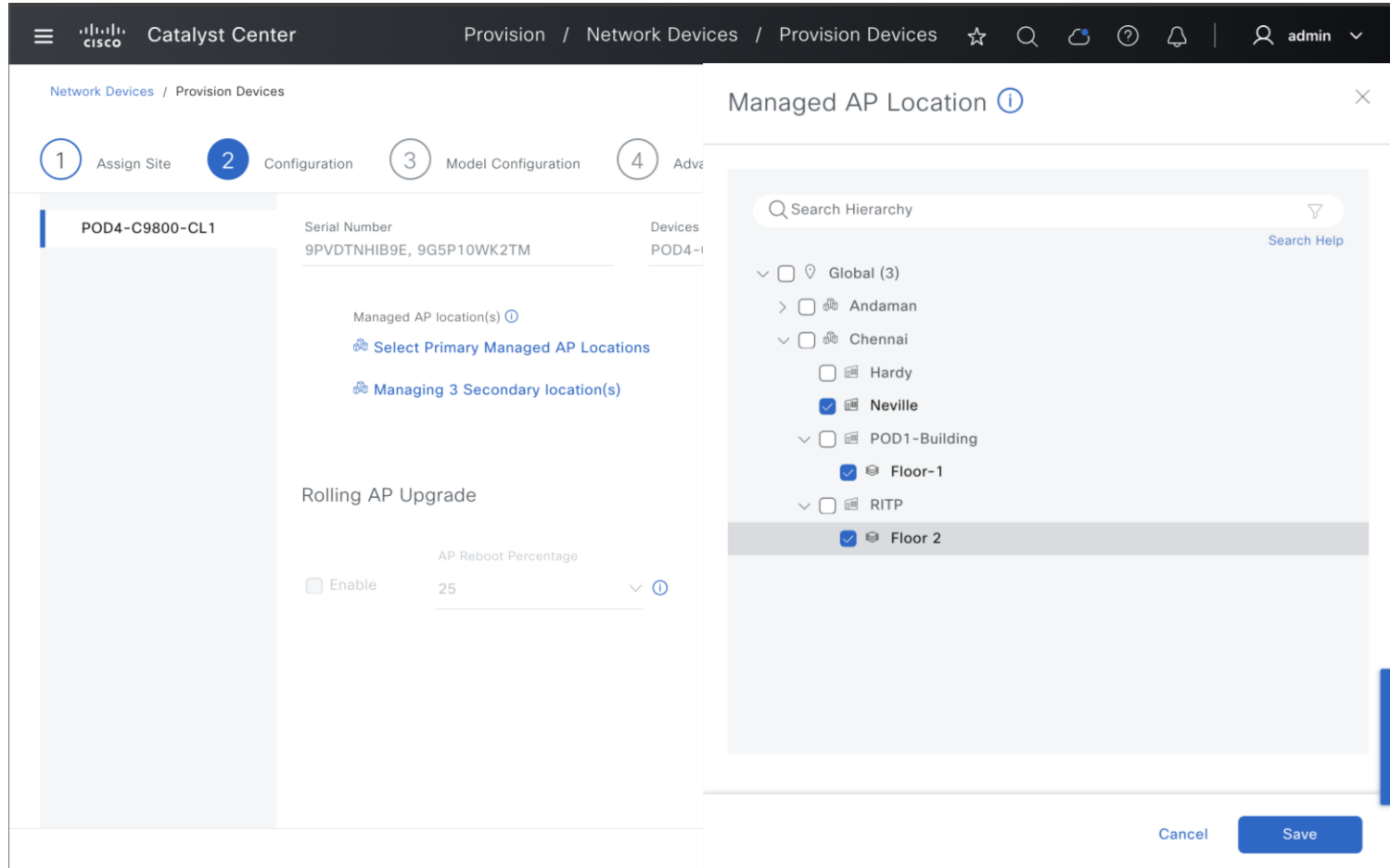
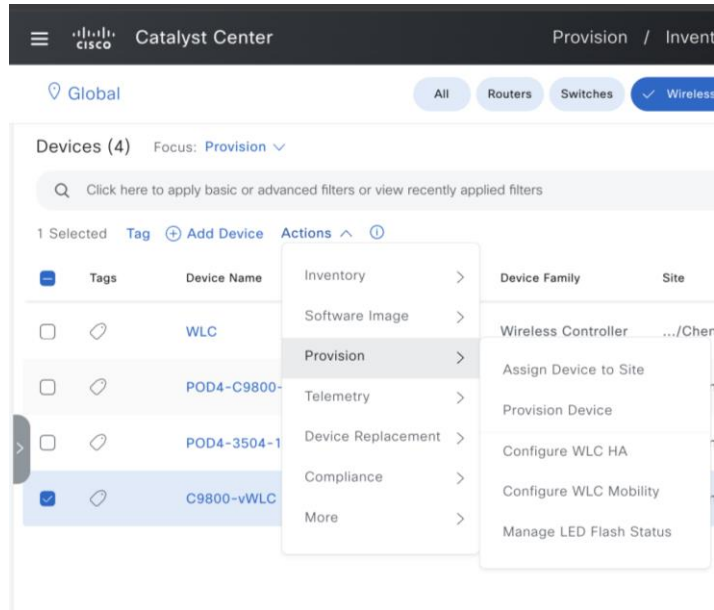
Define WLC Role Active or Anchor



Select Buildings or Floors which are going to be managed by the WLC



# Provisioning WLC (N+1 WLC)

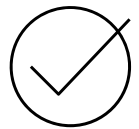
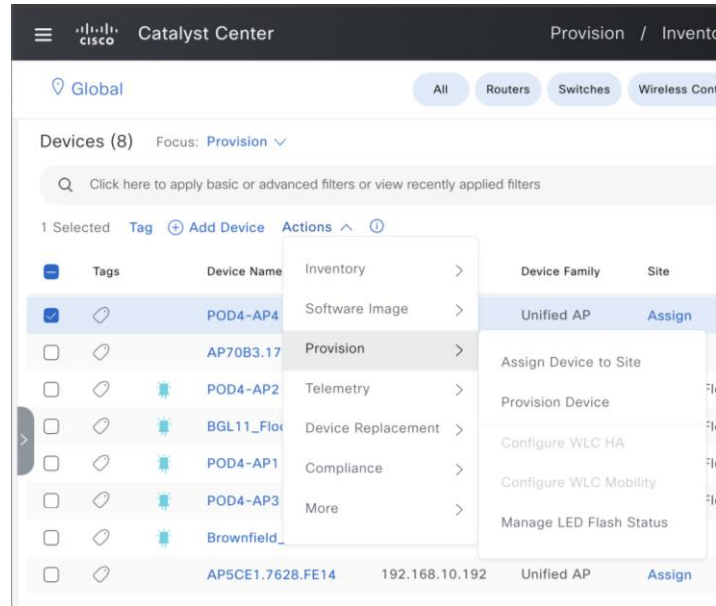


Define WLC Role Active or Anchor

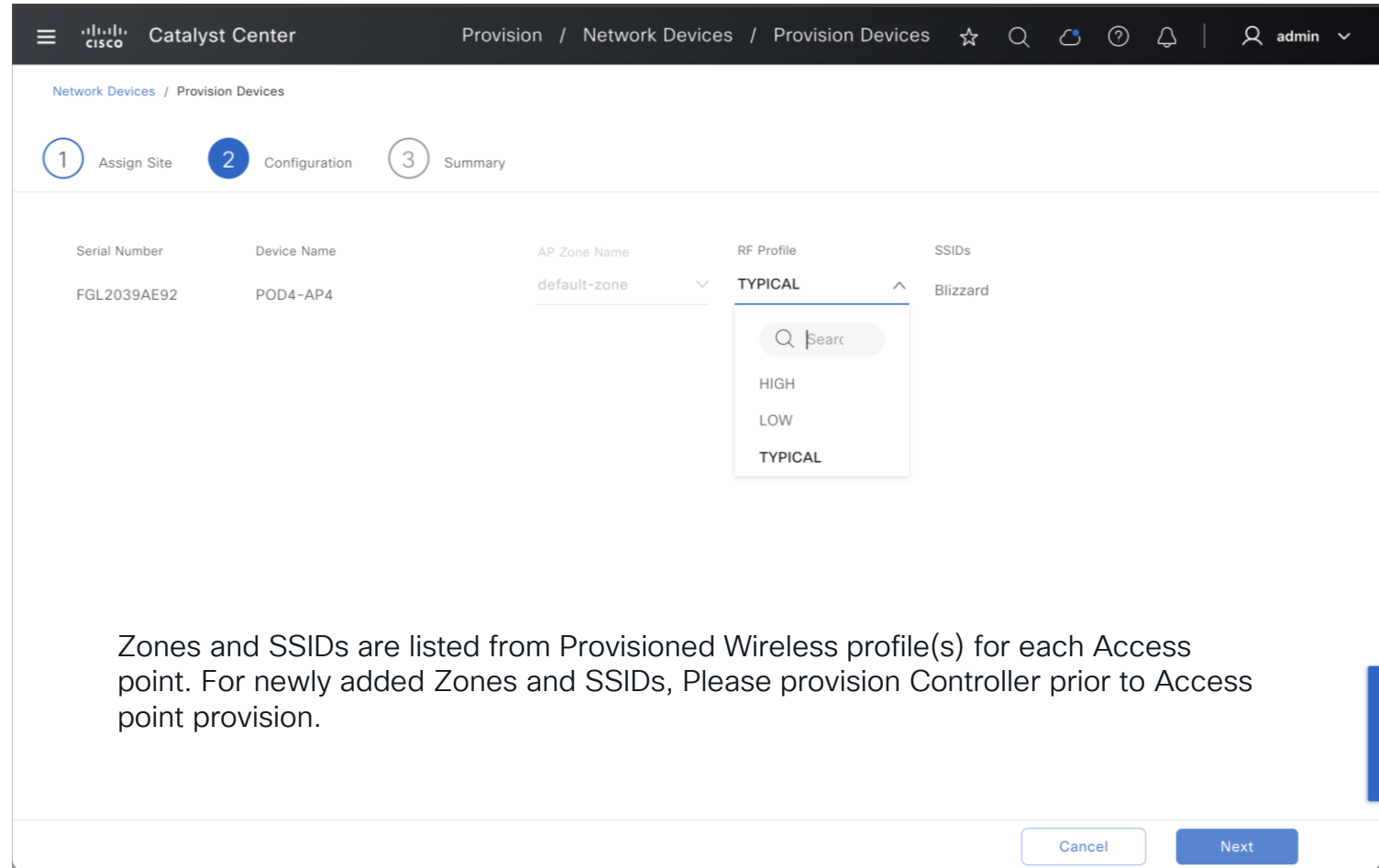


Select Buildings or Floors which are going to be managed by the WLC

# AP Provisioning



Select RF/AI RF Profile to be pushed to APs



Zones and SSIDs are listed from Provisioned Wireless profile(s) for each Access point. For newly added Zones and SSIDs, Please provision Controller prior to Access point provision.

# Cisco Live US Catalyst Center Learning Map

## Sunday—2<sup>nd</sup>

- TECOPS-2001 2PM**  
The Ultimate Guide to Install, Onboard, Operate your Campus Network with Catalyst Center
- LTRSEC-2005 2PM**  
Building Cisco SD-Access with Cisco Catalyst Center and ISE
- LTRENS-2890 9AM**  
Deploying and Operating Cisco SD-Access with Pub-Sub using Cisco Catalyst Center

## Monday—3<sup>rd</sup>

- BRKOPS-2548 8AM**  
Network Troubleshooting Using Cisco Catalyst Center APIs
- BRKEWN-2029 9:30AM**  
7 Ways to Optimize User Experience using Catalyst Center Wireless AIOps and Assurance
- BRKOPS-2416 10:30AM**  
7 Habits for Success with Cisco Catalyst Center
- DEWVKS-1004 11AM**  
Deploy Cisco Catalyst Center with Rest-APIs in Seconds
- IBOOPS-2882 1PM**  
Let's Talk about Catalyst Center Integrations
- BRKOPS-2596 1PM**  
Revolutionize Your Network Management with Cisco Catalyst Center: Physical or Virtual on AWS or VMware ESXi
- BRKOPS-1461 1PM**  
Discovering and Managing Brownfield Deployment with Cisco Catalyst Center
- BRKIOT-2016 2:30PM**  
Automating OT Services with Cisco Catalyst Center Best Practices

## Tuesday—4<sup>th</sup>

- BRKOPS-2208 10:30AM**  
Discovering the Secrets of AI/ML in Cisco Catalyst Center
- DEVNET-1087 12PM**  
Cisco Catalyst Center Platform: APIs, Event Notifications, Integrations, and DevOps Resources
- BRKCOC-2041 1PM**  
Catalyst Center Automation and Use Cases in Cisco IT
- BRKOPS-2402 3PM**  
Automate the Deployment of a Wireless Network with the Help of Cisco Catalyst Center

## Wednesday—5<sup>th</sup>

- BRKOPS-2032 10:30AM**  
3 Catalyst Center and ITSM Workflows: CMDB, Incident Management, and SWIM
- BRKENS-1601 10:30AM**  
Catalyst Center and Meraki Cloud: The Right Choice for your Catalyst 9000 Switch Management!
- BRKGRN-1012 10:30AM**  
Fostering Sustainable Campus Communities: Cisco Catalyst Center and Smart Buildings
- IBOENS-2600 10:30AM**  
Revolutionizing Campus Networks: The Power of Automation with Catalyst Center
- DEWVKS-2041 2PM**  
Cisco Catalyst Center and Targeting Event Notifications via Webex Messaging
- TACENT-2011 2:45PM**  
Unlocking the troubleshooting power of Cisco Catalyst Center
- DEVNET-3000 3PM**  
Chatbot for Catalyst Center—on Open Source AI-based Bot

## Thursday—6<sup>th</sup>

- BRKOPS-2343 8:30AM**  
Decoding Site Reliability Engineering Through Catalyst Center
- SKILLS-1660 9AM**  
Introduction to Catalyst Center
- SKILLS-1661 10AM**  
Introduction to Catalyst Center Platform
- BRKEWN-2306 1PM**  
Wireless Network Automation and Assurance with Cisco Catalyst Center

○ BU-led sessions



# Cisco Live US Campus AIOps Learning Map

## Sunday—2<sup>nd</sup>

### TECEWN-2004 9AM

Wireless Design, AIOps, and Assurance: Optimize Your Wi-Fi Networks with Cisco Catalyst Wireless

### TECAPP-2903 2PM

Supercharge End-to-End visibility with ThousandEyes using APIs and Integrations

## Monday—3<sup>rd</sup>

### BRKENT-2209 11AM

AI/ML for Network Engineers

### BRKXAR-1008 1PM

Modern Network Design Is More Complex Than Ever, Leverage AI as Your Cheat Code to Survival

### CENETI-1001 1PM

Is Your Organization AI-Ready? How To Manage, Secure, and Scale AI-Powered Technologies

### ITLBRK-1113 3:15PM

Strategies for Safer, Faster Deployment of GenAI Apps and Services at Scale

### BRKENT-1105 11AM

An Introduction to GenAI Technologies & Solutions

### DEVNET-1084 11AM

Explore Generative AI Capabilities

### AIHUB-1004 12PM

Redefine your AI/ML networks with Cisco Silicon One

### PSOIND-1013 12PM

The AI Revolution is Helping to Enable and Secure Critical Infrastructure!

## Tuesday—4<sup>th</sup>

### BRKOPS-2208 10:30AM

Discovering the Secrets of AI/ML in Cisco Catalyst Center

### BRKEWN-3007 1PM

Demystifying the Role of Applied AI in Your Cisco Wireless Deployments

### CENCX-1004 2PM

Accelerating AI-Ready Infrastructures and Execution Strategies

### PSOAPP-1020 2:30PM

Harnessing AI and AIOps in Cisco Full-Stack Observability for Unparalleled Insight

### AIHUB-2005 4:30PM

Leverage your enterprise data assets to build AI assistants with Motific

## Wednesday—5<sup>th</sup>

### BRKEWN-2926 10:30AM

Tune Your Cisco Wi-Fi Designs for the Most Demanding Clients and Applications, Boosted with Applied AI

### AIHUB-1009 12:00PM

Cross Architecture Approach to AI

### PSOENT-1013 12:30PM

Power proactive business outcomes with AI Assistant

### IBOIoT-2101 1PM

Revolutionizing Industrial Operations: Unveiling the Power of AI in IIoT with Cisco Solutions and Emerging Industry Trends

### DEVNET-3000 3PM

Chatbot for Catalyst Center—on Open Source AI-based Bot

### CSSOPS-1050 4PM

Powering Automation and Security: Software Defined Access and Catalyst Center's Impact on a Global Energy Giant

## Thursday—6<sup>th</sup>

### BRKETI-2010 9:30AM

Beyond the Noise: Harnessing Generative AI for Telemetry Data

### BRKXAR-3001 10:30AM

End-to-End Visibility and Actionable Insights Using ThousandEyes, DNAC, ISE, and SD-WAN

### BRKNWT-2403 11AM

GenAI-Driven Network Test Automation: A Groundbreaking Strategy for Comprehensive Network Transformation Using Advanced Technologies

### AIHUB-2008 11:15AM

How Cisco uses Generative AI to make TAC Engineers Super-Human



# Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

---



**Earn 100 points** per survey completed and compete on the Cisco Live Challenge leaderboard.

---



Level up and earn **exclusive prizes!**

---



Complete your surveys in the **Cisco Live mobile app.**

# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](http://www.CiscoLive.com/on-demand)

Contact me at: [ramkchel@cisco.com](mailto:ramkchel@cisco.com)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive

# References

Prime to Catalyst Center Gradual Migration

<https://www.youtube.com/watch?v=oCMp-LcdfTI>

Co-Existence Prime & Catalyst Center

<https://www.youtube.com/watch?v=uCdLUBnBy6M>

Prime 3.10 to Catalyst Center Migration

<https://www.youtube.com/watch?v=Yla0YJYknGs>

Prime to Catalyst Center Migration

<https://www.youtube.com/watch?v=L-JaloEyW78>



[Tips and Tricks for Prime Infrastructure to Cisco Catalyst Center Migration](#)

[Best Practice for Prime to Cisco Catalyst Center migration](#)



# Intel Connectivity, Apple, Samsung Analytics

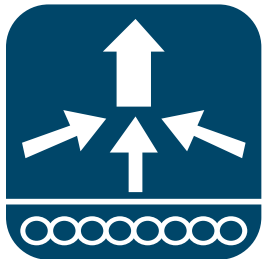
	Driver Version Device Type	Catalyst Center	IOS-XE Release
Intel Connectivity Analytics	Intel 22.50.1 or newer on AX1650/1675 AC8561/9560 AX200/201/210/211/411	2.3.3	17.6.1
Apple Analytics	iOS 11 on iPhone 7 or later	2.2.1	16.12.1s
Samsung Analytics	Android 9 or later on Galaxy S10 or newer	2.2.1	17.1.1



# How to configure Client Analytics?

## Wireless Global

Configure Device Classifier



Configuration > Wireless > Wireless Global

Default Mobility Domain \* default

RF Group Name\* cleu-cn-group

Maximum Login Sessions Per User\* 0

Management Via Wireless

Device Classification

AP LAG Mode

Dot15 Radio

Wireless Password Policy None

Assisted Roaming

Denial Maximum\* 5

Floor Bias(dBm)\* 15

Prediction Minimum\* 3

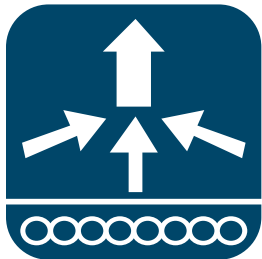
Apply



# How to configure Client Analytics?

## Policy Profile | Access Policies

Configure Device Classifier



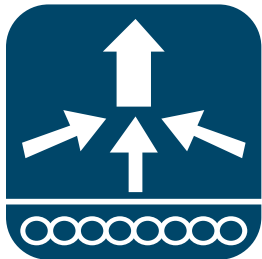
The screenshot shows the 'Edit Policy Profile' configuration page in a web browser. The browser address bar shows 'https://localhost:6445/webui/#/policyProfile'. The page has a dark sidebar with menu items: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Edit Policy Profile' and has a warning banner: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' Below the banner are tabs for 'General', 'Access Policies', 'QOS and AVC', 'Mobility', and 'Advanced'. The 'Access Policies' tab is active. It contains several sections: 'RADIUS Profiling' with a checkbox; 'HTTP TLV Caching' and 'DHCP TLV Caching', both with checked checkboxes and highlighted by an orange box; 'WLAN Local Profiling' with a green 'Enabled' status; 'Global State of Device Classification' with a green 'Enabled' status; 'Local Subscriber Policy Name' with a search/select dropdown; 'VLAN' section with 'VLAN/VLAN Group' set to 'mobile-device-2' and 'Multicast VLAN' with an input field; 'WLAN ACL' section with 'IPv4 ACL' and 'IPv6 ACL' search/select dropdowns; and 'URL Filters' section with 'Pre Auth' and 'Post Auth' search/select dropdowns.



# How to configure Client Analytics?

WLANs | Security | Layer 2

PMF Optional or Required



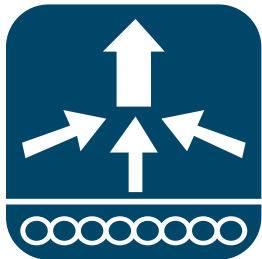
The screenshot shows the 'Edit WLAN' configuration page in the Cisco Catalyst 9800-CL Wireless Controller. The 'Protected Management Frame' section is highlighted with a yellow box. The dropdown menu for PMF is open, showing the following options: Optional (selected), Disabled, Optional (with a warning icon), and Required. Other visible settings include WPA2 Policy, WPA2 Encryption (AES(CCMP128), CCMP256, GCMP128, GCMP256), Over the DS, Reassociation Timeout (20), Auth Key Mgmt (802.1x, PSK, Easy-PSK, CCKM, FT + 802.1x, FT + PSK, 802.1x-SHA256, PSK-SHA256), and MPSK Configuration (Enable MPSK).



# How to configure Client Analytics?

## WLANs | Advanced

Advertise Support



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller web interface. The main page is titled 'Edit WLAN'. On the left, there is a navigation menu with options: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area shows the configuration for a specific WLAN. The 'Device Analytics' section is highlighted with an orange box and contains the following settings:

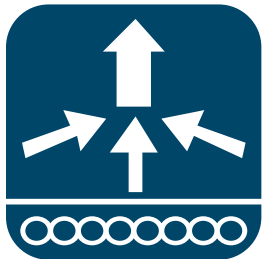
- Advertise Support:
- Advertise PC Analytics Support:
- Share Data with Client:

Other visible settings include '11ax' (checked), 'Downlink OFDMA' (checked), 'Uplink OFDMA' (checked), 'Downlink MU-MIMO' (checked), 'Uplink MU-MIMO' (checked), and 'BSS Target Wake Up Time' (unchecked). At the bottom right, there is a button labeled 'Update & Apply to Device'.



# How to support the Clients? - optional

WLANs | Advanced  
802.11k/v  
and 'Share Data'  
with client



The screenshot shows the 'Edit WLAN' configuration page in the Cisco Catalyst 9800-CL Wireless Controller. The page is titled 'Cisco Catalyst 9800-CL Wireless Controller' and 'Welcome admin'. The configuration page is divided into several sections:

- Per WLAN:** Per WLAN (0), Per AP Per WLAN (0), Per AP Radio Per WLAN (200).
- 11v BSS Transition Support:** BSS Transition (checked), Dual Neighbor List (unchecked), BSS Max Idle Service (checked), BSS Max Idle Protected (unchecked), Directed Multicast Service (checked).
- Assisted Roaming (11k):** Prediction Optimization (unchecked), Neighbor List (checked), Dual Band Neighbor List (unchecked).
- Device Analytics:** Advertise Support (checked), Advertise PC Analytics Support (checked).
- Share Data with Client:** Share Data with Client (checked).
- 11k Beacon Radio Measurement:** Client Scan Report (unchecked).

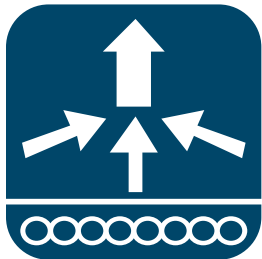
The 'Share Data with Client' checkbox is highlighted with an orange box. The '11v BSS Transition Support' section is also highlighted with an orange box. The 'Assisted Roaming (11k)' section is highlighted with an orange box. The '11k Beacon Radio Measurement' section is highlighted with an orange box.



# How to get the Client view? - optional

## WLANs | Advanced

Receive Radio Measurement



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller web interface. The main content area is titled 'Edit WLAN' and displays configuration options for a specific WLAN. A table lists various settings:

Setting	Value
Per WLAN	0
Per AP Per WLAN	0
Per AP Radio Per WLAN	200
<b>11v BSS Transition Support</b>	
BSS Transition	<input checked="" type="checkbox"/>
Dual Neighbor List	<input type="checkbox"/>
BSS Max Idle Service	<input checked="" type="checkbox"/>
BSS Max Idle Protected	<input type="checkbox"/>
Directed Multicast Service	<input checked="" type="checkbox"/>
<b>Assisted Roaming (11k)</b>	
Prediction Optimization	<input type="checkbox"/>
Neighbor List	<input checked="" type="checkbox"/>
Dual Band Neighbor List	<input type="checkbox"/>
<b>DTIM Period (in beacon intervals)</b>	
5 GHz Band (1-255)	1
2.4 GHz Band (1-255)	1
<b>11k Beacon Radio Measurement Client Scan Report</b>	
On Association	<input checked="" type="checkbox"/>
On Roam	<input checked="" type="checkbox"/>

The '11k Beacon Radio Measurement Client Scan Report' section is highlighted with an orange box. Below the configuration table, there is a note: 'Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only'. At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons.



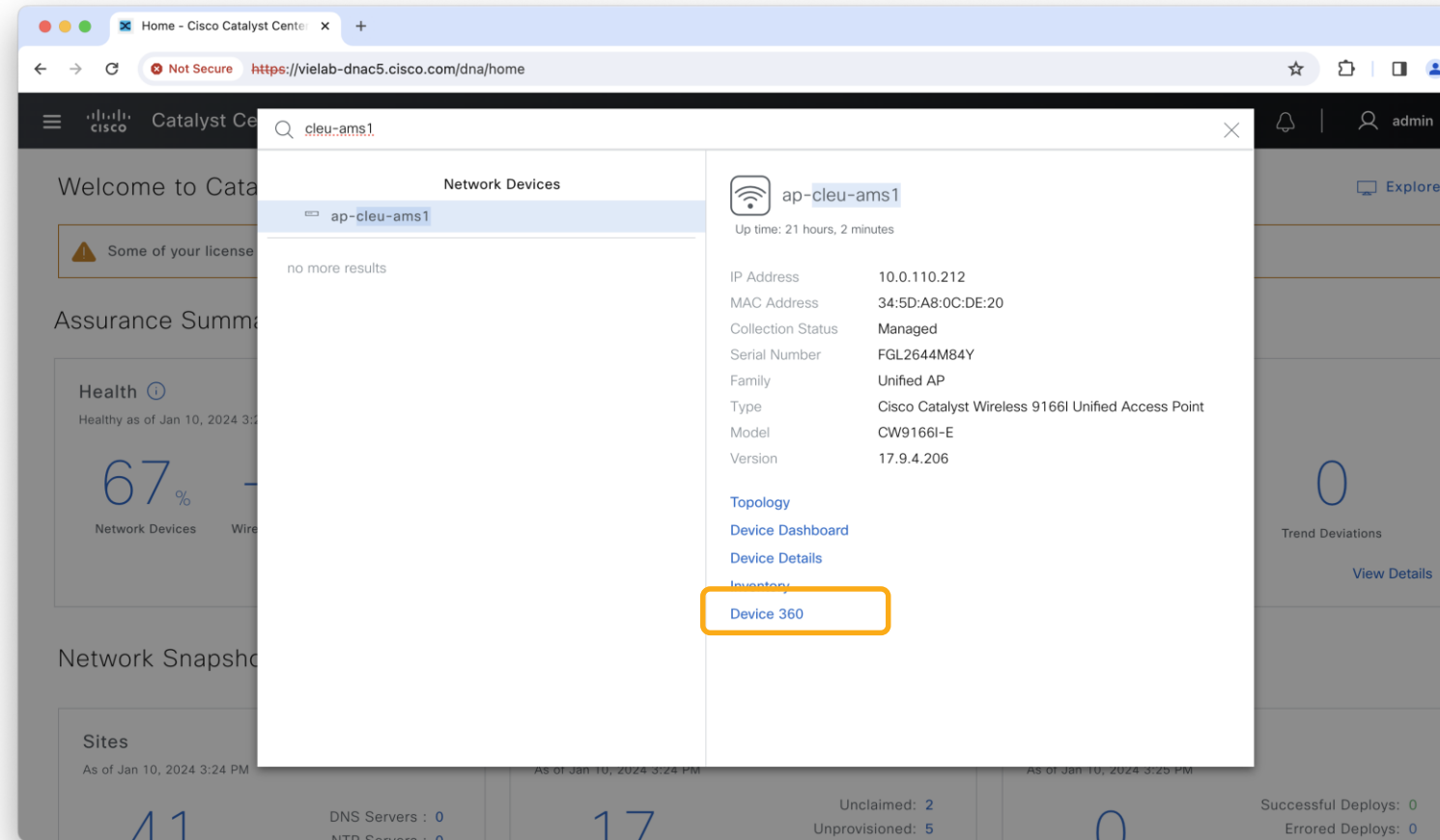
# How to get the Client view? - optional

```
C9800#  
! Required Config  
network-assurance enable  
wlan ciscolive 24 ciscolive  
  shutdown  
mbo  
  no shutdown  
  
! How to request Client report  
wireless client mac-address H.H.H scan-  
report once mode ...  
! Display Result  
show wireless client mac-address H.H.H  
detail | sec Scan
```



# How to enable Spectrum Analysis?

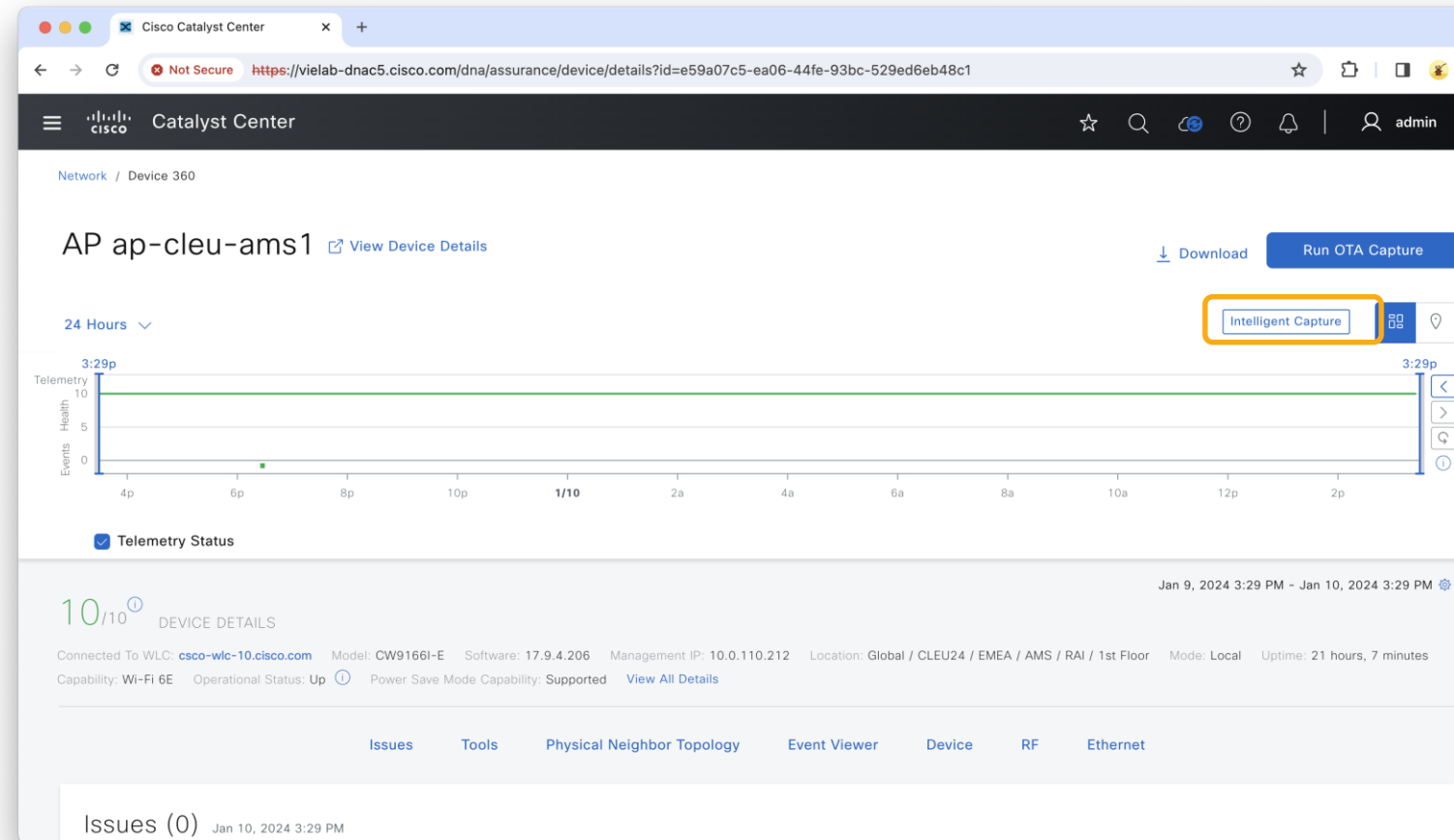
- Go to Accesspoint Device 360 View





# How to enable Spectrum Analysis?

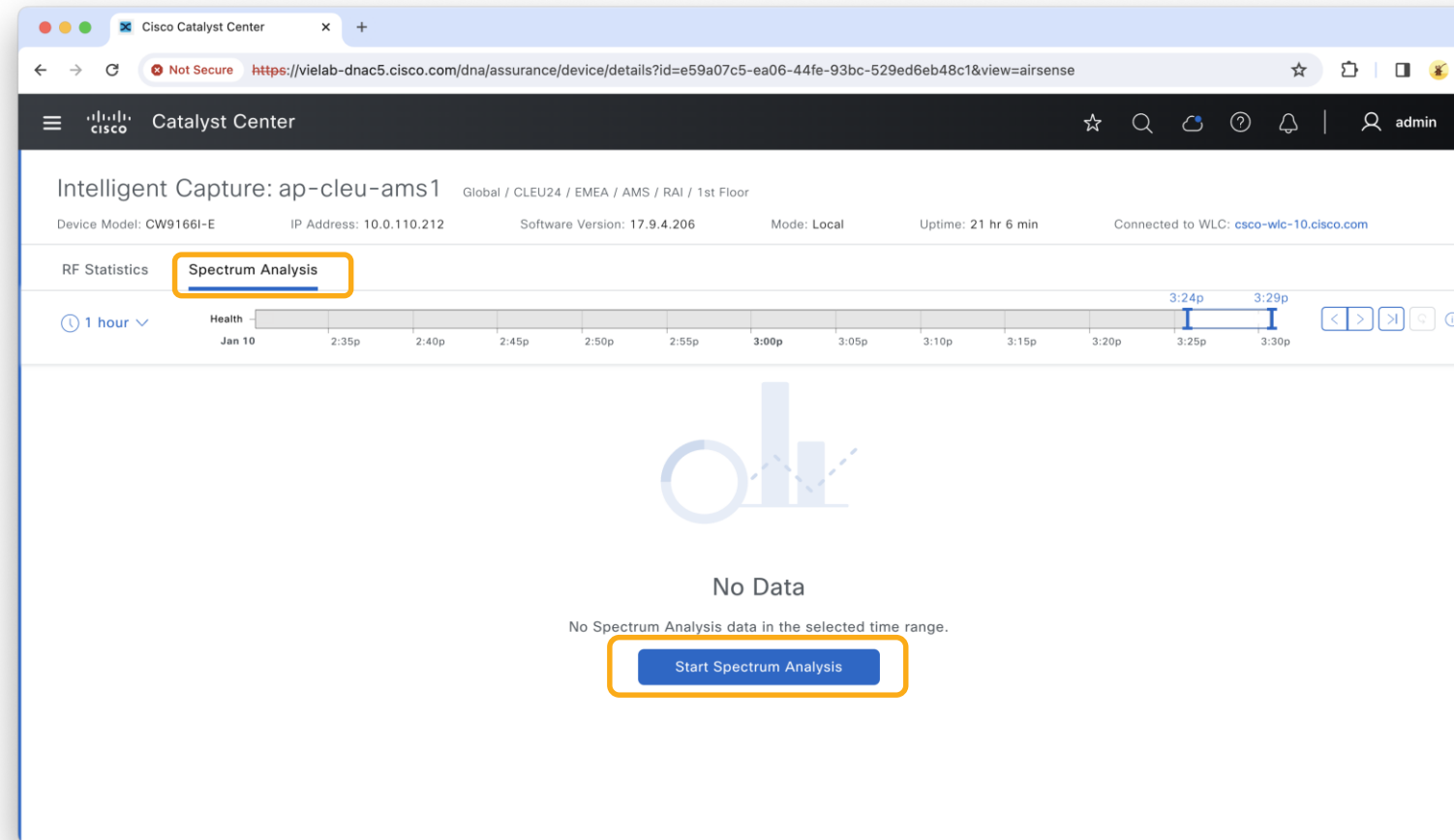
- Go to Accesspoint Device 360 View
- Intelligent Capture





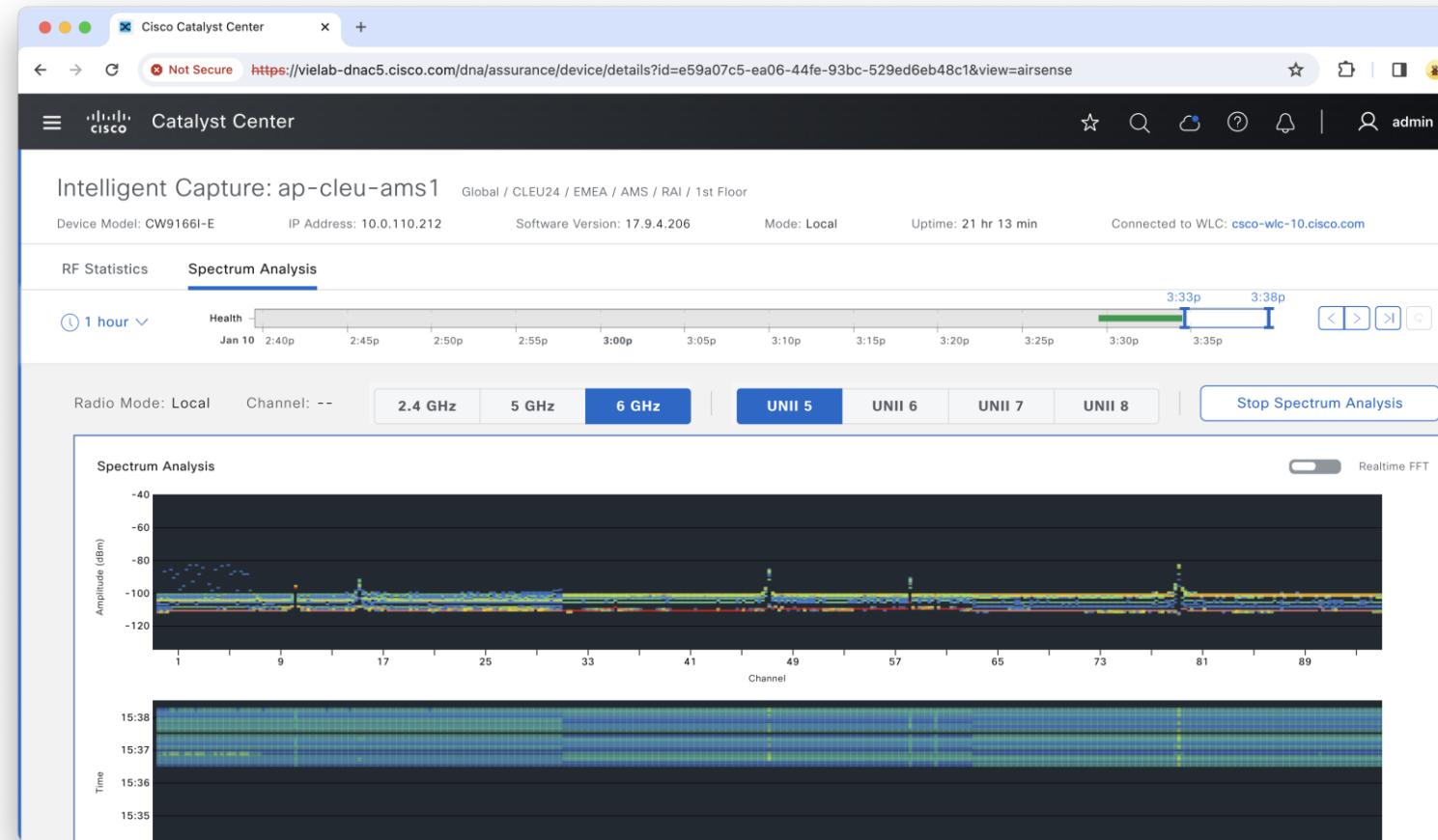
# How to enable Spectrum Analysis?

- Go to Accesspoint Device 360 View
- Intelligent Captures
- Start Spectrum Analysis



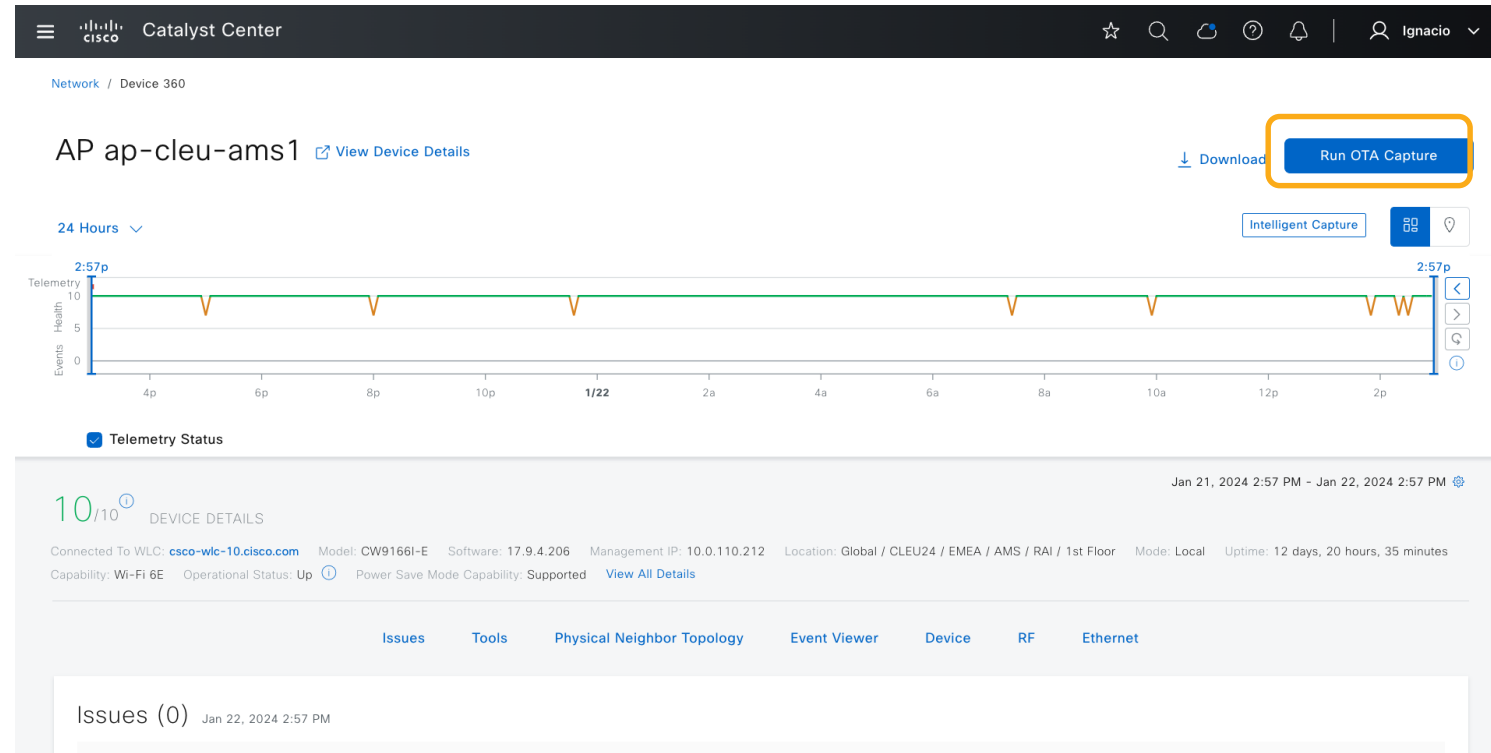
# How to enable Spectrum Analysis?

- Go to Accesspoint Device 360 View
- Intelligent Capture
- Start Spectrum Analysis



# How to run over the air (OTA) capture?

- Go to Accesspoint Device 360 View
- Run OTA Capture
- Select band, radio, channel width and channel

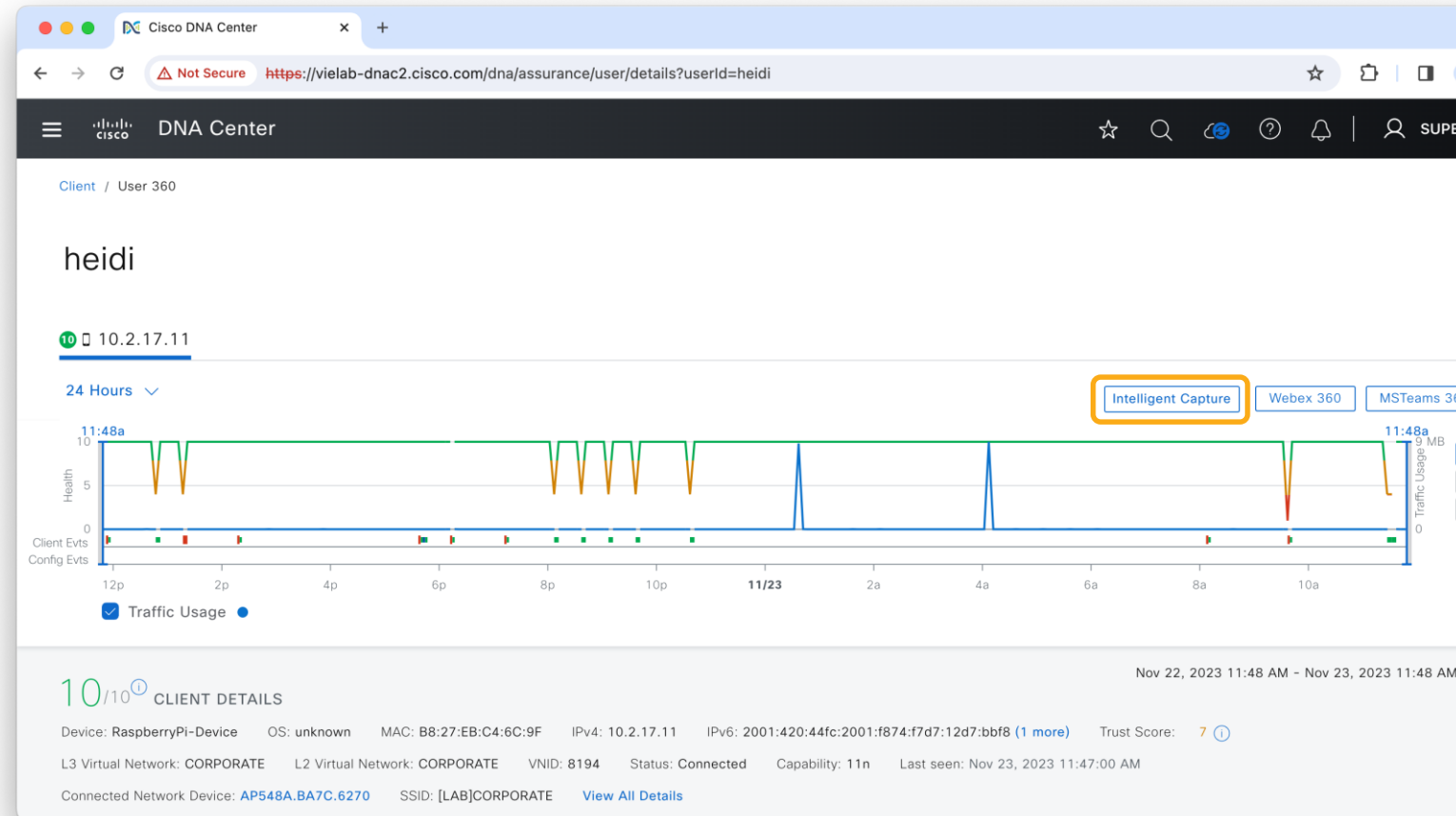


The screenshot displays the Cisco Catalyst Center interface for an Access Point (AP) named 'ap-cleu-ams1'. The interface includes a navigation bar at the top with the Cisco logo and 'Catalyst Center' text. Below the navigation bar, the AP name and a 'View Device Details' link are shown. A 'Download' button is visible next to the AP name. A prominent blue button labeled 'Run OTA Capture' is highlighted with an orange box. Below this, there is a '24 Hours' time range selector and an 'Intelligent Capture' button. A line graph shows 'Telemetry Health' over a 24-hour period, with a green line indicating health status and several orange downward-pointing triangles indicating events. Below the graph, a 'Telemetry Status' section is visible, showing '10/10' device details and various system information such as 'Connected To WLC: cisco-wlc-10.cisco.com', 'Model: CW9166I-E', 'Software: 17.9.4.206', 'Management IP: 10.0.110.212', 'Location: Global / CLEU24 / EMEA / AMS / RAI / 1st Floor', 'Mode: Local', and 'Uptime: 12 days, 20 hours, 35 minutes'. At the bottom, there are tabs for 'Issues', 'Tools', 'Physical Neighbor Topology', 'Event Viewer', 'Device', 'RF', and 'Ethernet'. The 'Issues' tab is currently selected, showing 'Issues (0) Jan 22, 2024 2:57 PM'.



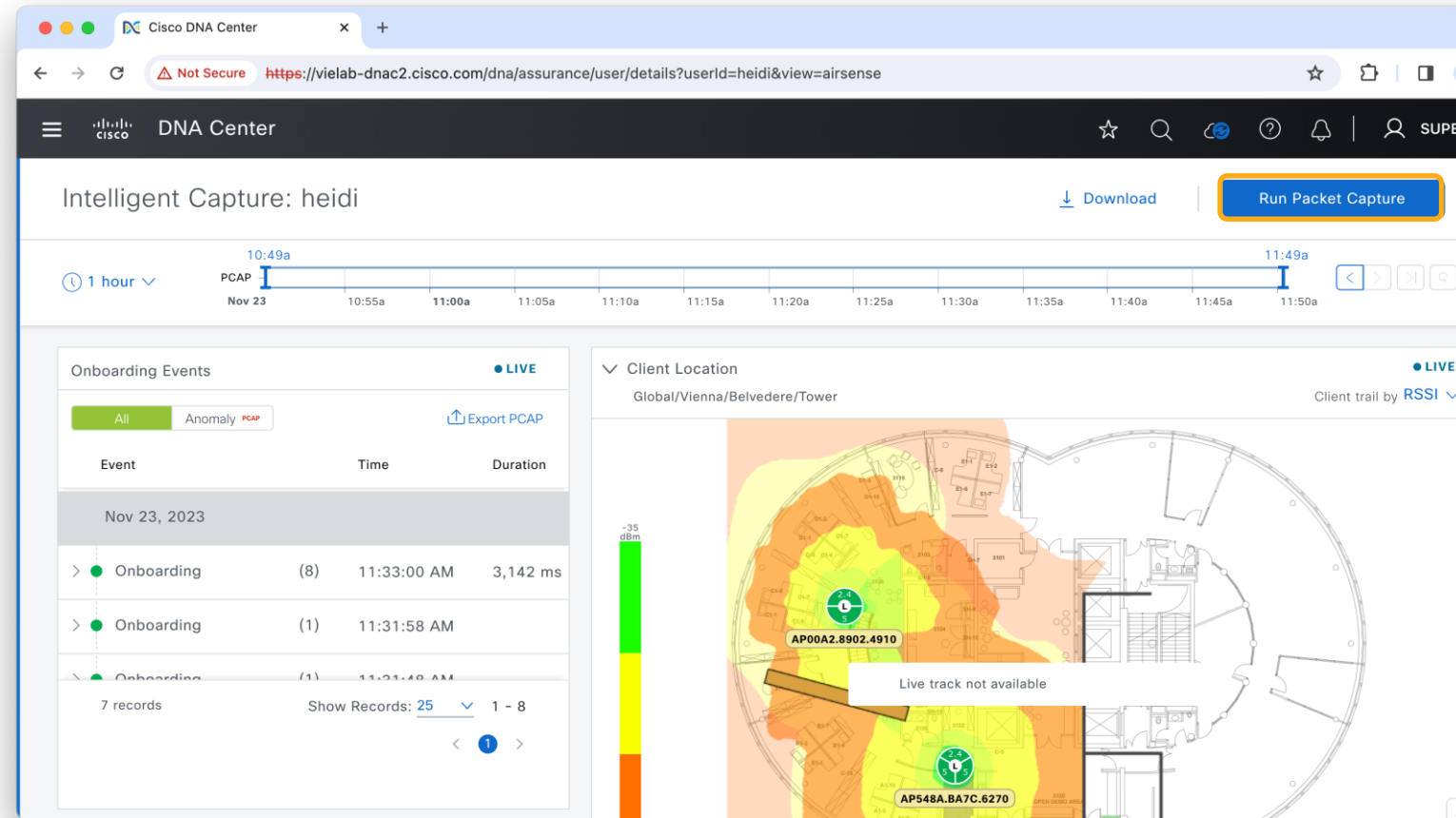
# How to run client Live Packet Capture?

- Go to Client 360 View > Intelligent Capture



# How to run client Live Packet Capture?

- Go to Client 360 View > Intelligent Capture
- Run Packet Capture



The screenshot shows the Cisco DNA Center web interface for Intelligent Capture. The browser address bar displays the URL: <https://vielab-dnac2.cisco.com/dna/assurance/user/details?userId=heidi&view=airsense>. The page title is "Intelligent Capture: heidi". A "Run Packet Capture" button is highlighted in orange. Below the title is a timeline for "PCAP" from 10:49a to 11:49a on Nov 23. The interface is divided into two main sections: "Onboarding Events" and "Client Location".

**Onboarding Events** (LIVE):

Event	Time	Duration
Nov 23, 2023		
> Onboarding (8)	11:33:00 AM	3,142 ms
> Onboarding (1)	11:31:58 AM	
> Onboarding (1)	11:31:49 AM	

7 records | Show Records: 25 | 1 - 8

**Client Location** (LIVE):

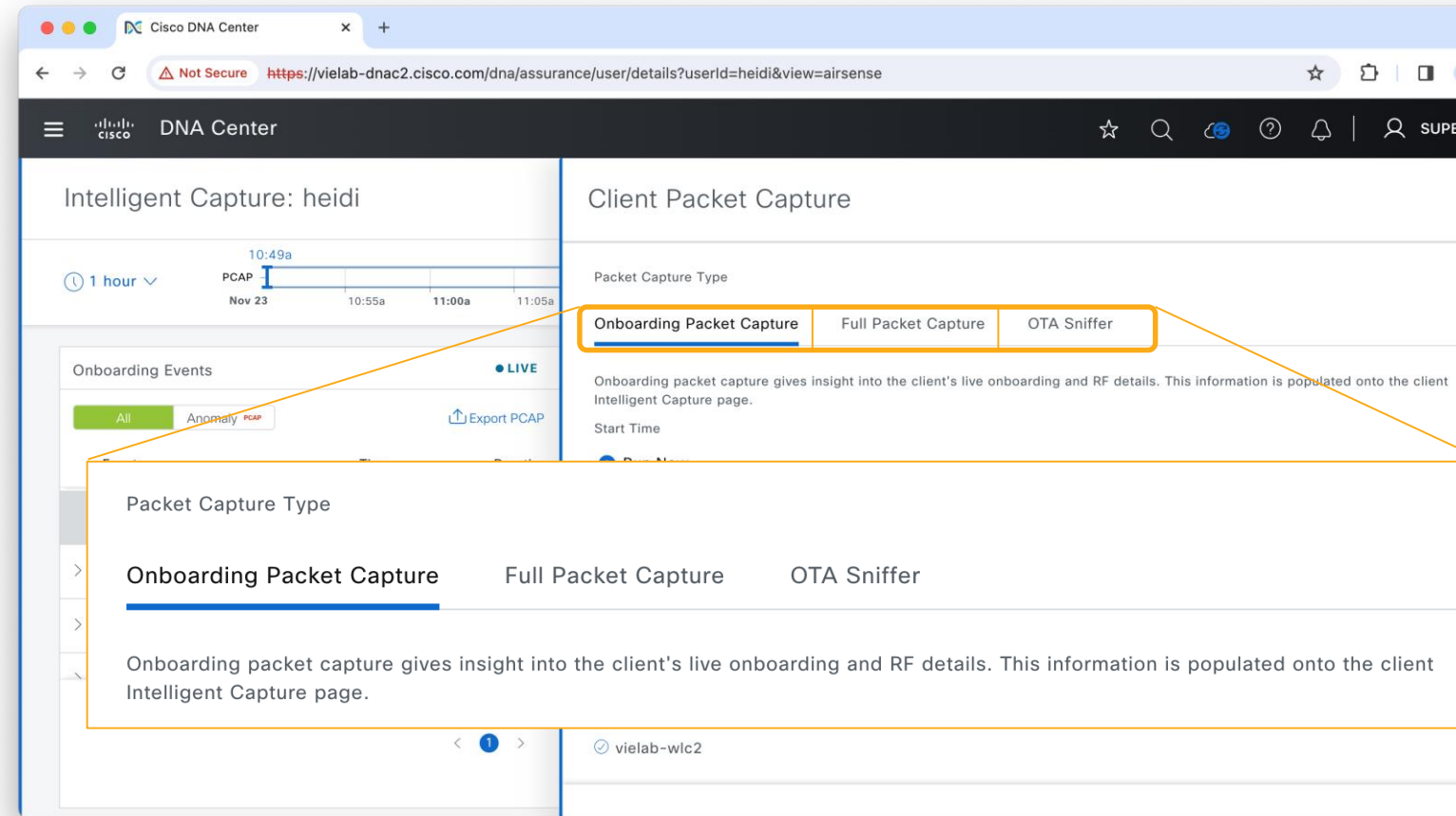
Global/Vienna/Belvedere/Tower | Client trail by RSSI

The client location map shows a floor plan with a heatmap overlay. Two access points are labeled: AP00A2.8902.4910 and AP548A.BA7C.6270. A tooltip over the map indicates "Live track not available".



# How to run client Live Packet Capture?

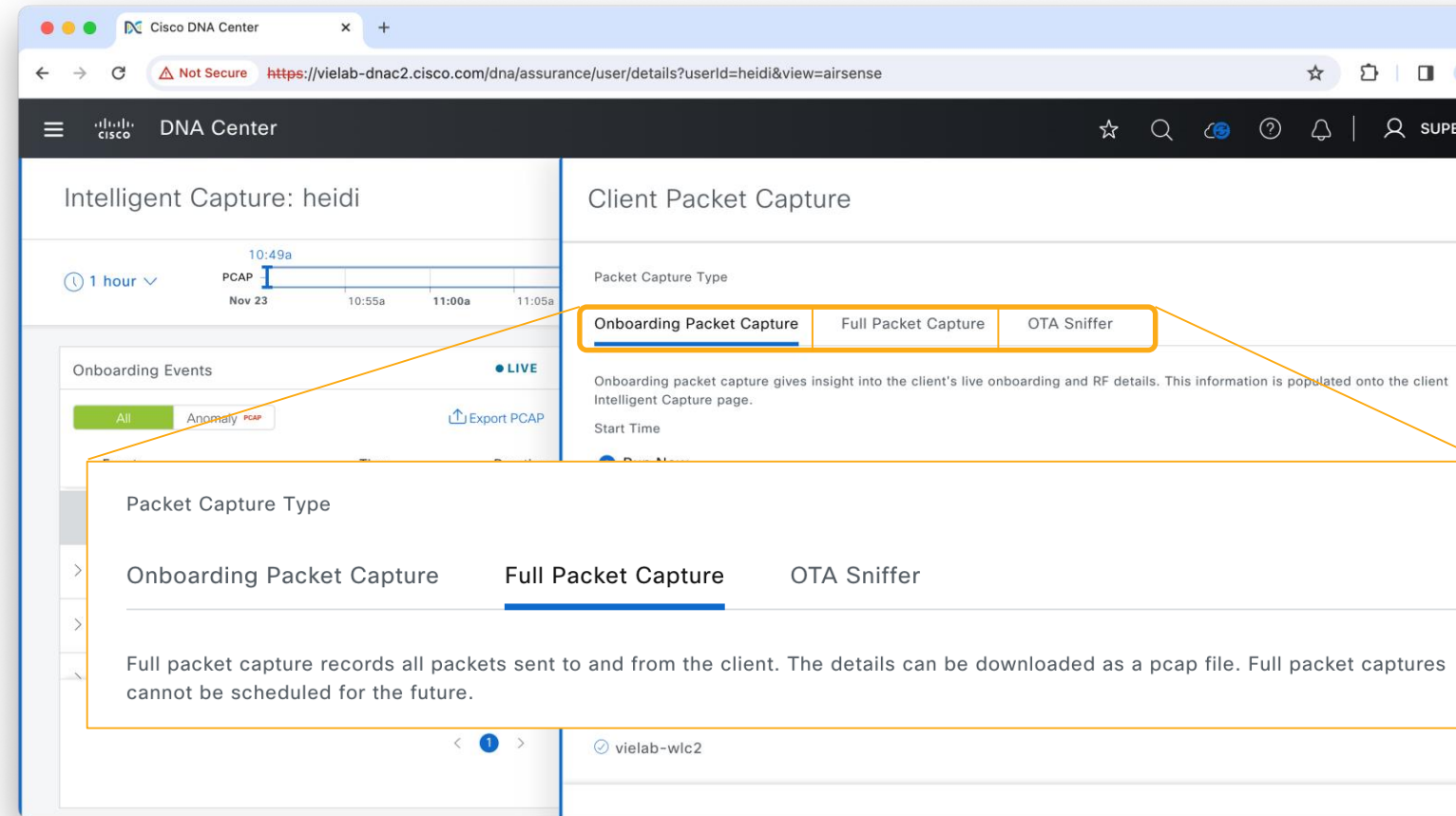
- Go to Client 360 View > Intelligent Capture
- Run Packet Capture
- Select Packet Capture Type





# How to run client Live Packet Capture?

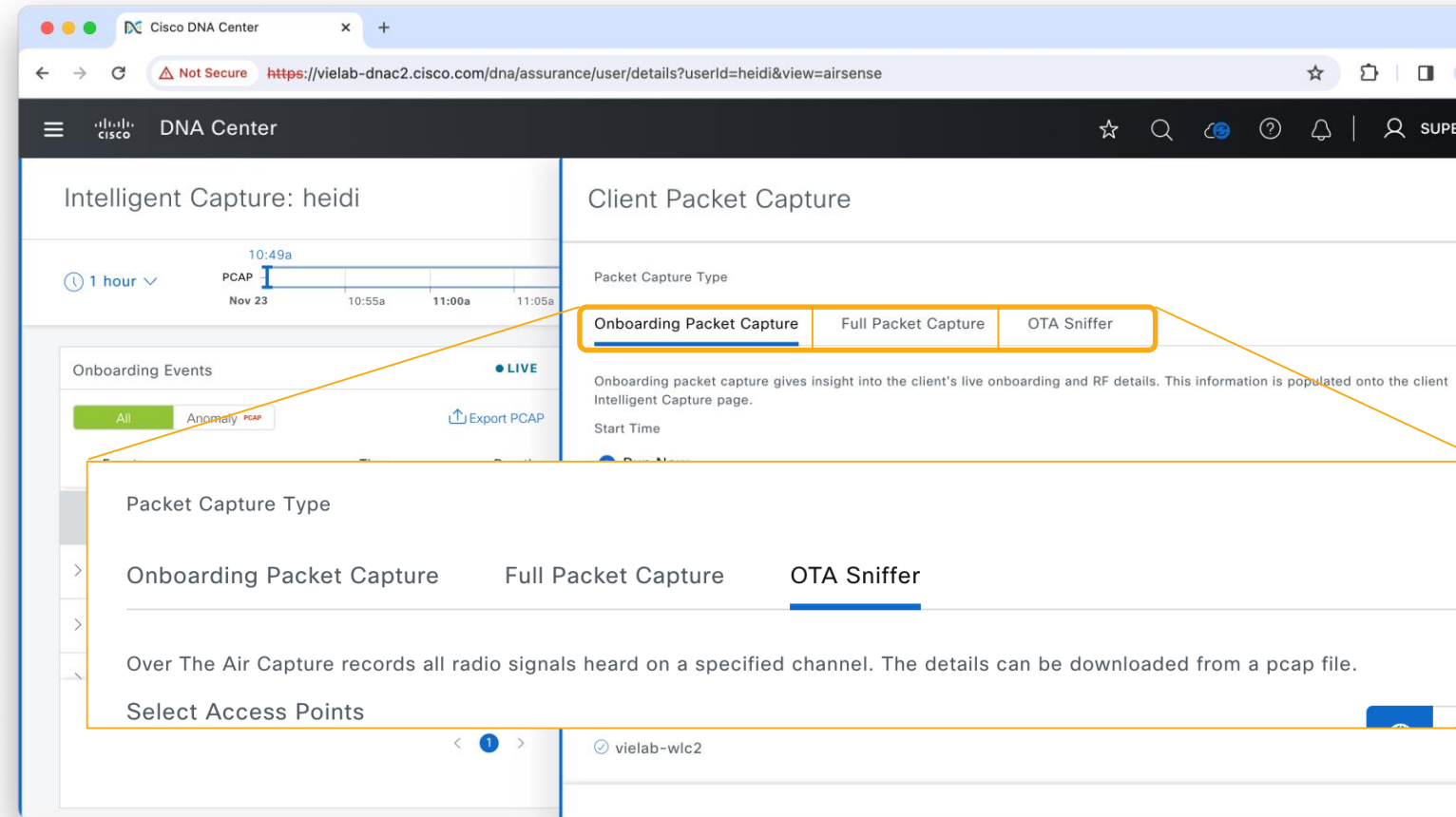
- Go to Client 360 View > Intelligent Capture
- Run Packet Capture
- Select Packet Capture Type





# How to run client Live Packet Capture?

- Go to Client 360 View > Intelligent Capture
- Run Packet Capture
- Select Packet Capture Type





# Packet Capture Types

- Onboarding Packet Capture
  - At AP radio level
  - No client impact
  - Onboarding Packets for a client (EAP, ICMP, DNS,...)

→	91	10.0.120.40	10.0.120.254	ICMP	2023-12-20 1
	92	Cisco_05:74:4f	ca:e2:16:ad:5f:13	802.11	2023-12-20 1
	93	ca:e2:16:ad:5f:13	Cisco_05:74:4f	802.11	2023-12-20 1
	94	10.0.120.40	144.254.71.184	DNS	2023-12-20 1
	95	10.0.120.40	144.254.71.184	DNS	2023-12-20 1
←	96	10.0.120.254	10.0.120.40	ICMP	2023-12-20 1
	97	10.0.120.36	10.0.120.40	ICMP	2023-12-20 1
	98	10.0.120.40	10.0.120.36	ICMP	2023-12-20 1
	99	10.0.120.36	10.0.120.40	ICMP	2023-12-20 1
	100	10.0.120.40	10.0.120.36	ICMP	2023-12-20 1

```
> Frame 96: 1440 bytes on wire (11520 bits), 1440 bytes captured (11520) on interface 0
> Radiotap Header v0, Length 38
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.0.120.254, Dst: 10.0.120.40
> Internet Control Message Protocol
```



# Packet Capture Types

- Onboarding Packet Capture
  - At AP radio level
  - No client impact
  - Onboarding Packets for a client (EAP, ICMP, DNS,...)
- Full Packet Capture
  - At AP radio level
  - No client impact
  - All data packets for a client
  - APs: C9130/C9136/CW9166

7597	74.125.100.234	10.0.120.40	TCP	QoS Data
7598	74.125.100.234	10.0.120.40	TCP	QoS Data
7599	74.125.100.234	10.0.120.40	TCP	QoS Data
7600	74.125.100.234	10.0.120.40	TCP	QoS Data
7601	74.125.100.234	10.0.120.40	TCP	QoS Data
7602	74.125.100.234	10.0.120.40	TCP	QoS Data
7603	ca:e2:16:ad:5f:1...	Cisco_05:74:4f (...)	802.11	802.11 Block Ack
7604	74.125.100.234	10.0.120.40	TLSv1.2	QoS Data
7605	ca:e2:16:ad:5f:1...	Cisco_05:74:4f (...)	802.11	802.11 Block Ack
7606	ca:e2:16:ad:5f:1...	Cisco_05:74:4f (...)	802.11	Request-to-send
7607		ca:e2:16:ad:5f:1...	802.11	Clear-to-send
7608	ca:e2:16:ad:5f:13	Cisco_f3:d7:9f	802.11	QoS Data
7609	Cisco_05:74:4f (...)	ca:e2:16:ad:5f:1...	802.11	802.11 Block Ack
7610	74.125.100.234	10.0.120.40	TCP	QoS Data

```

> Frame 7604: 1362 bytes on wire (10896 bits), 1362 bytes captured (10896 bits)
> Radiotap Header v0, Length 38
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 74.125.100.234, Dst: 10.0.120.40
> Transmission Control Protocol, Src Port: 443, Dst Port: 65159, Seq: 3481122, Ack: 65159
> [14 Reassembled TCP Segments (16406 bytes): #7589(1233), #7590(1238), #7591(1238), #7592(1238), #7593(1238), #7594(1238), #7595(1238), #7596(1238), #7597(1238), #7598(1238), #7599(1238), #7600(1238), #7601(1238), #7602(1238)]
> Transport Layer Security

```



# Packet Capture Types

- OTA Sniffer
  - At AP radio level
  - Turns radio into Sniffer mode, no client serving capability
  - Captures all packets on specific channel
  - Requires 17.11 and 2.3.7

29637	Cisco_2f:dd:e2	Broadcast	802.11	Beacon frame
29638	Cisco_b3:e6:99	PVST+	802.11	Data
29639	Apple_3d:39:07	ca:e2:16:ad:5f:13	802.11	QoS Data
29640	ca:e2:16:ad:5f:1...	Cisco_05:74:40 (...)	802.11	802.11 Block Ack
29641	ca:e2:16:ad:5f:1...	Cisco_05:74:40 (...)	802.11	Request-to-send
29642		ca:e2:16:ad:5f:1...	802.11	Clear-to-send
29643	ca:e2:16:ad:5f:13	Apple_3d:39:07	802.11	QoS Data
29644	Cisco_05:74:40 (...)	ca:e2:16:ad:5f:1...	802.11	802.11 Block Ack
29645	Cisco_30:0c:e2	Cisco_e3:58:66	802.11	Probe Response
29646		Cisco_30:0c:e2 (...)	802.11	Acknowledgement
29647	Cisco_2f:dd:e2	Cisco_e3:58:66	802.11	Probe Response
29648	Cisco_2f:dd:e2	Cisco_e3:58:66	802.11	Probe Response
29649	Cisco_2f:dd:e2	Cisco_e3:58:66	802.11	Probe Response

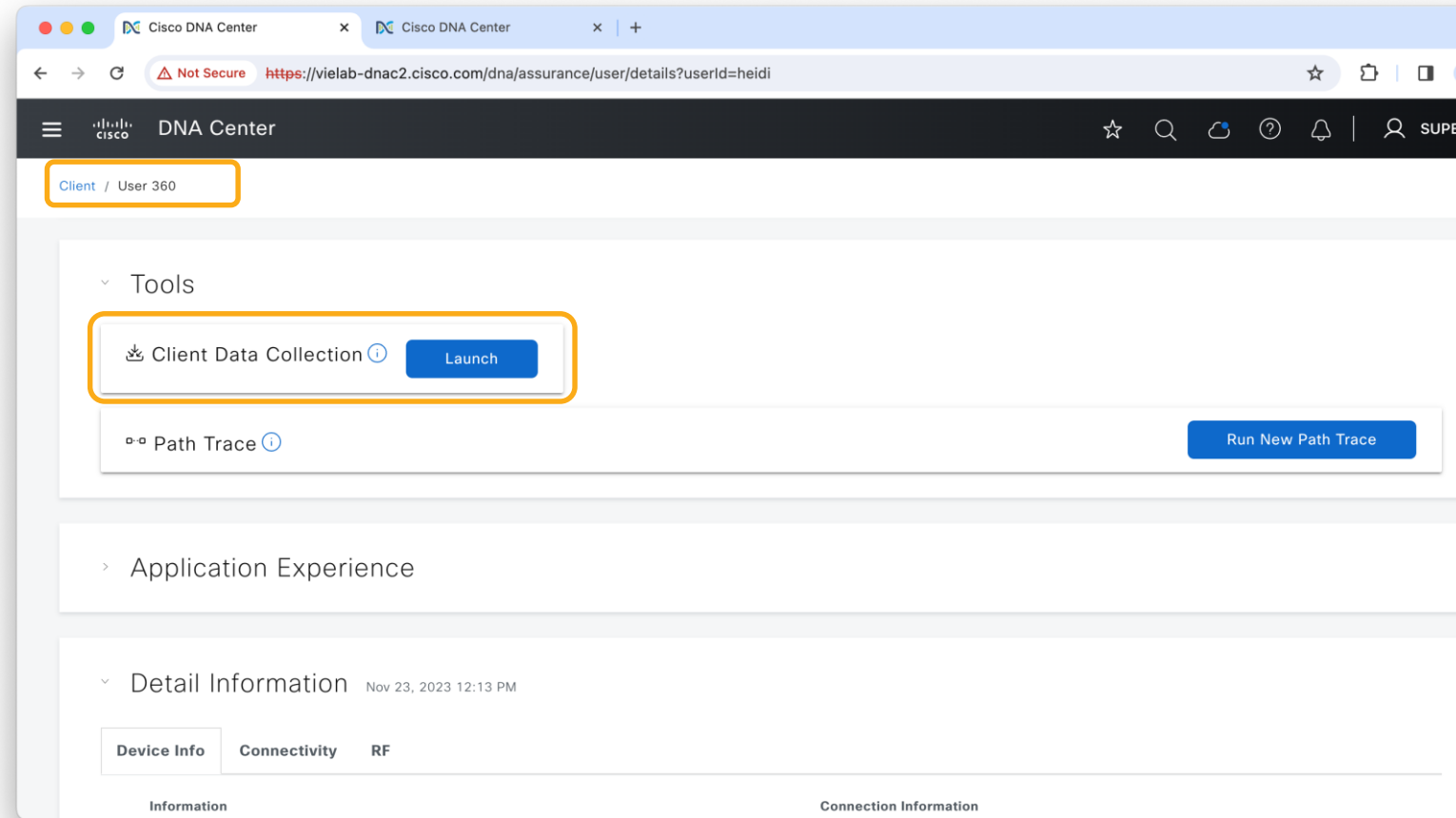
```

> Frame 29643: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .p.....T
> Data (100 bytes)
  
```



# How to collect AP/Client Wireless data?

- Go to Device/Client 360 Tools section





# How to collect AP/Client Wireless data?

- Go to Device/Client 360 Tools section
- Launch the MRE workflow and collect the data

The screenshot shows a web browser window with three tabs labeled 'Cisco DNA Center'. The address bar displays a URL: `https://vielab-dnac2.cisco.com/dna/tools/network-reasoner/generic?id=wirelesstroubleshootclientdatacollectionmultiwic`. The page title is 'DNA Center' and the breadcrumb navigation shows 'Tools / Network Reasoner / Wireless Client Data Collection'. A modal dialog box titled 'Reasoner Inputs' is open, containing the following fields:

- Step 1: Enter client information
- Client MAC address\*  
B8:27:EB:C4:6C:9F
- Troubleshoot Duration (1-30 minutes)\*  
10

At the bottom of the dialog, there are three buttons: 'Cancel', 'Back', and 'Next'.

# How to collect AP/Client Wireless data?

- Go to Device/Client 360 Tools section
- Launch the MRE workflow and collect the data

