You make **possible**

Wireless Network Automation with Cisco DNA Center

Paul Lysander - Technical Marketing Engineer
Peng Xu - Technical Marketing Engineer

BRKEWN-2026

Barcelona | January 27-31, 2020

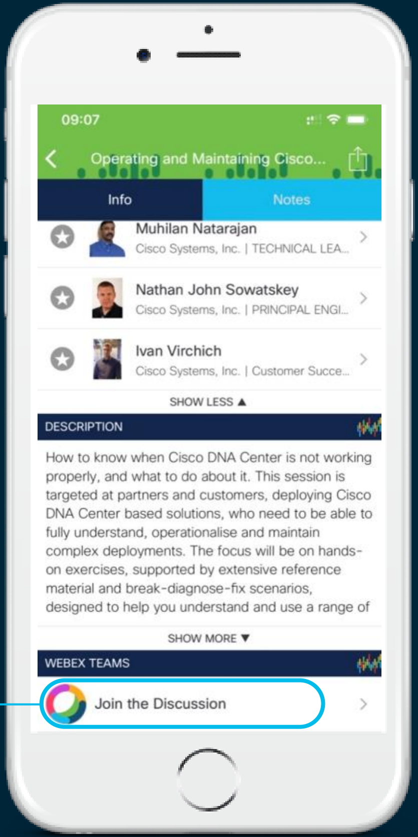
Cisco Webex Teams

Questions?

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

How

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



09:07

Operating and Maintaining Cisco...

Info | Notes

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

SHOW LESS ▲

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

SHOW MORE ▼

WEBEX TEAMS

Join the Discussion

cisco Live!

Introducing Cisco DNA Center

Cisco DNA Center

Intent-based Automation & Assurance Platform

Intent based Platform

- Single pane of glass for all devices
- End-to-end health info in real time
- Granular visibility
- Simplified workflows

Automation for Provisioning

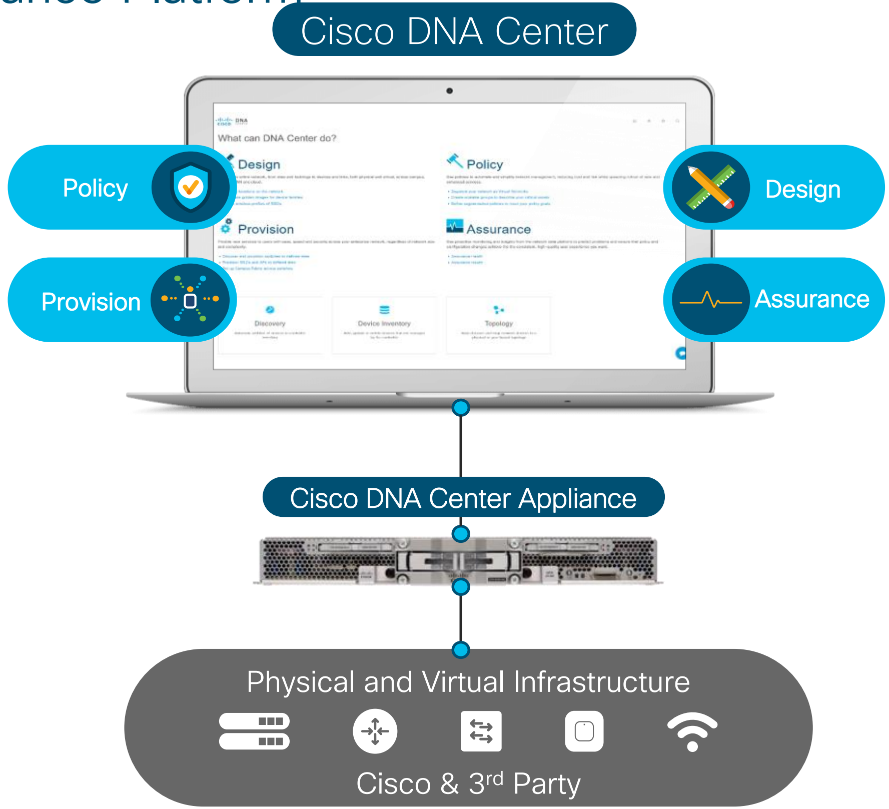
- Zero-touch deployment
- Device Lifecycle Management
- Policy enforcement

Analytics for Assurance

- Verify intent of network settings
- Proactively resolve issues
- Reduce time spent troubleshooting

Platform for Extensibility

- Integrate APIs with 3rd party solutions
- Integrate and customize ServiceNow
- Evolve operational tools and processes



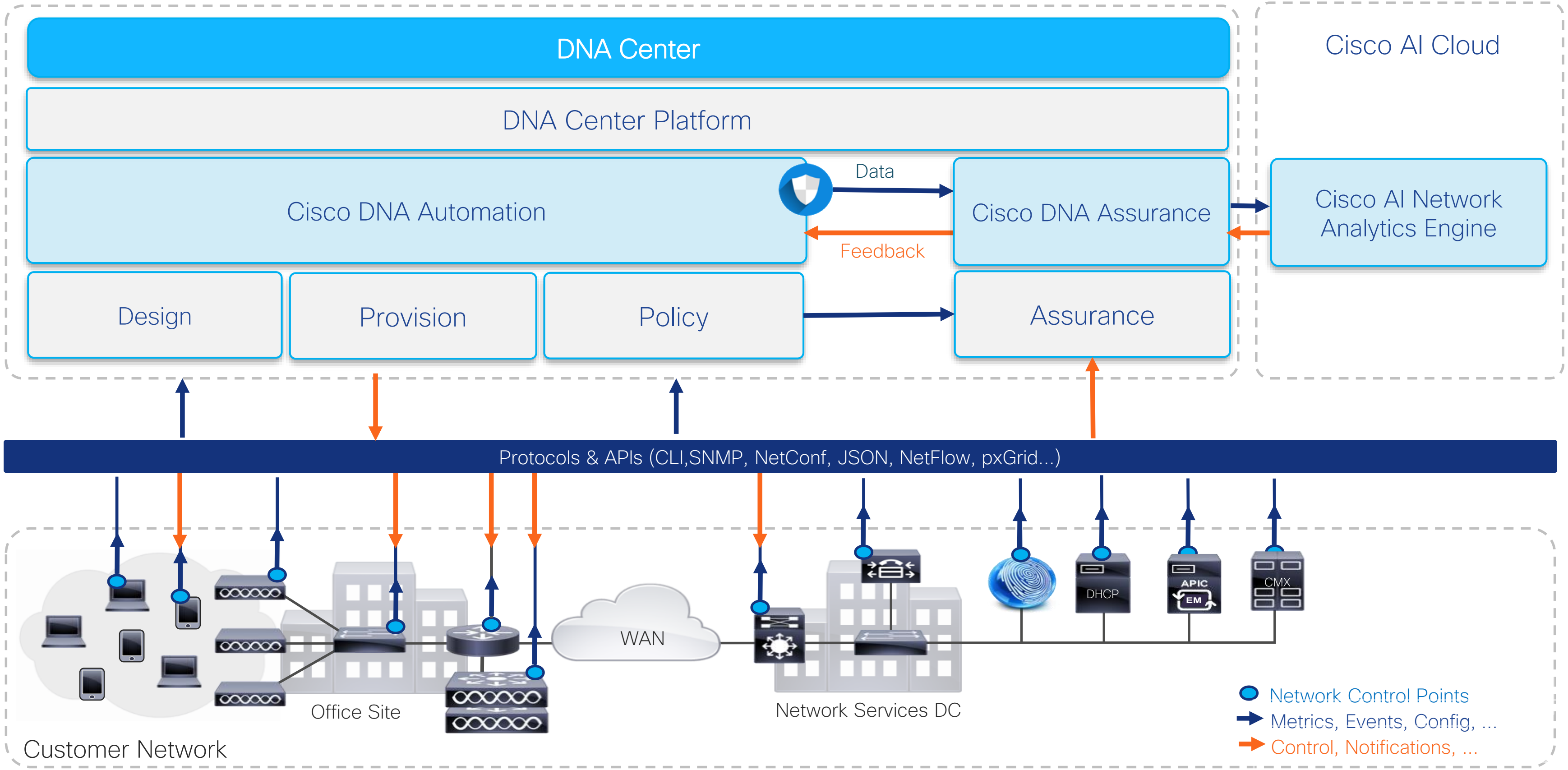
Cisco DNA Automation

Existing Approach	Cisco DNA Approach
Multiple Apps for Management across Domains	Integrated Workflows across Domains
Device Centric Configurations	Intent driving service provisioning & Policy Abstraction
Multiple tools for Automation and Assurance	One Box Solution with closed loop Automation
Software Update is Manual and Reactive	Proactive and Consistent Software update and Patching
IT process tools working in Silos	Out of the box Integration with IT Process tools

The Network that Scales for the Digital Business

DNA Center Overview ..1

Architecture & Components



● Network Control Points
→ Metrics, Events, Config, ...
→ Control, Notifications, ...

DNA Center Overview ..2
Architecture & Components

DNA Center

Cisco DNA Automation

Cisco DNA Assurance

Cisco AI Cloud

Cisco AI Network Analytics Engine

Design

- Create the structure and framework of the network
- The Network settings to discover your network infrastructure
- Create device specific profiles that can be applied throughout the network
- Adding new devices into the network - Zero touch deployment

Provision

- Prepare and configure devices
- Add devices to sites / site locations
- Assigning devices to the inventory
- Deploying the required settings and policies
- Creating fabric domains, and adding devices to the fabric

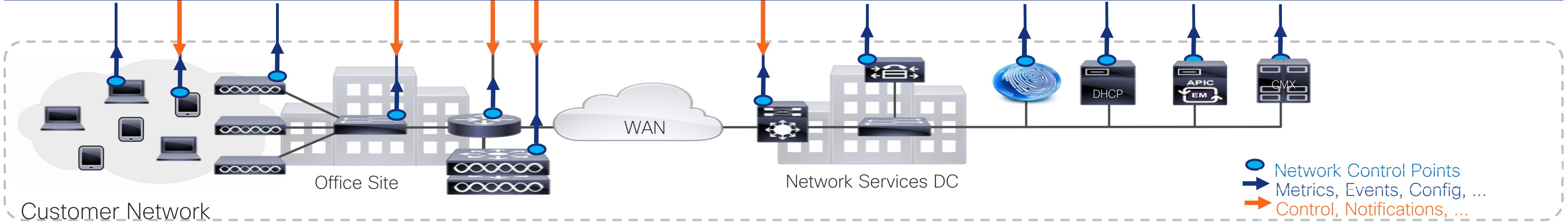
Policy

- Create policies that reflect organization's business intent
- The policy is translated into network or device specific configurations
- Policies vary based on device types, makes, models, operating systems, roles, and resource constraints

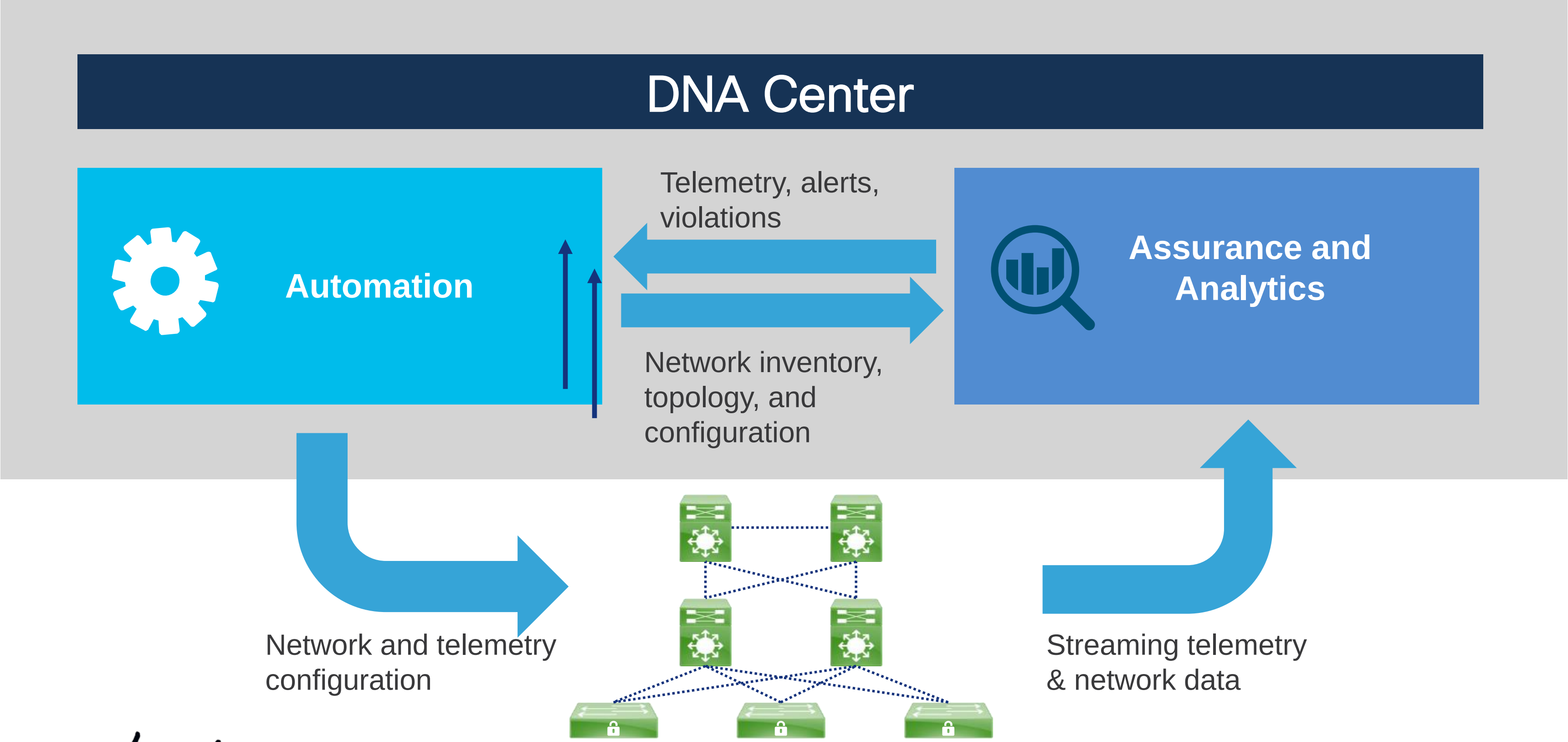
Assurance & Analytics

- Provide proactive and predictive actionable insights
- Performance and health of the network infrastructure, applications, and end-user clients.

Protocols & APIs (CLI,SNMP, NetConf, JSON, NetFlow, pxGrid...)



DNA Center Overview
Power of Automation & Analytics



DNA Center

Automation

Telemetry, alerts, violations

Network inventory, topology, and configuration

Assurance and Analytics

Network and telemetry configuration

Streaming telemetry & network data

Agenda

- Introduction to Cisco DNA Center and C9800 Wireless Controller
- Wireless Automation Workflow with C9800 Wireless Controller
  - Planning-Map Innovation (Planned AP/Ekahau Integration)
  - Network Settings
  - Design Workflow
  - Provision Workflow (N+1 HA Provision)
- Day N Changes
- Deployment Models
  - Embedded Wireless Controller (EWC) on Catalyst Access Points
- Software Image Management (SWIM)
  - Rolling AP Upgrades
- Key Takeaways

Cisco DNA Center - Automation Principles

Lifecycle Management

IT Process Automation

POLICY

Policy Based Automation

Introduction to Cisco Catalyst 9800 Series Controller

Catalyst 9800 Series Wireless Controllers

DNA Center

Translate business intent into network policy and capture actionable insights with DNA Center

Catalyst 9800-80

Catalyst 9800-40

Catalyst 9800-L

Catalyst 9800 for Cloud

Catalyst 9800 embedded wireless

for Cat 9k Switch

Aironet and Catalyst Access Points

Works with Cisco Aironet 802.11ac Wave 1 and Wave 2 and 802.11ax C9100 Access Points

Cisco's Next Gen Wireless Stack is Ready for Scale Deployments

- Enabling next-generation mobility powered for Wi-Fi 6

Cisco Catalyst 9800
Wireless Controllers

Cisco Catalyst 9100
Access Points

Managed by

Cisco DNA Center

Translate business intent into network policy and capture actionable insights

Digitized by

DNA SPACES

Cisco DNA Spaces

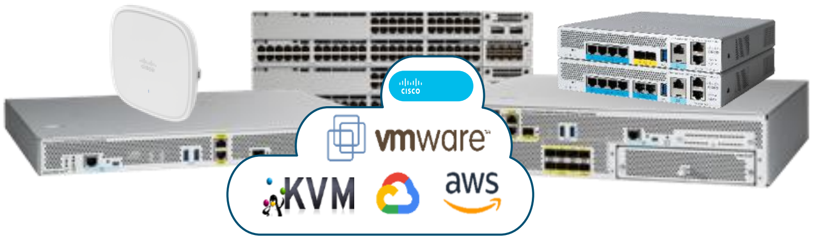
Digitize people, spaces and things

Resilient

Secure

Intelligent

Catalyst 9800 - Fastest Ramping Wireless Controller



7000+ units sold

2,000+ unique customers

cisco Live!

Catalyst Wireless Stack Innovations

Catalyst 9800 Launched

WLC SMU
AP SP and AP DP
Programmability
Encrypted Traffic Analytics
Software Define Access
iPSK, Rogue, wIPS

Catalyst 9100 Launched

11ax features like
OFDMA, MUMIMO,
BSS Coloring, TWT,
Spectrum Intelligence
Device Eco System

Cisco DNA-C Assurance

AI/ML Base Analytics
App Visibility and Experience
Intelligent Capture
Network Sensor
Apple, Samsung Analytics

Cisco DNA Spaces

Partner App integration
Room Finder
Location Analytics
Guest portal management

Innovations on Wireless Stack

ISSU
IoT Gateway
Open Roaming
BLE Management
11ax Analytics

Deploy It the Way You Want It

Catalyst 9800-SW*
200 APs, 4K Clients

Catalyst 9800-CL⁺
1000 APs, 10K Clients

Catalyst 9800-CL
3000 APs, 32K Clients

Catalyst 9800-CL
6000 APs, 64K Clients^

250 APs | 1000 APs | 2000 APs | 3000 APs | 6000 APs

Catalyst 9800-L
250 APs, 5K Clients, 5 Gbps

Catalyst 9800-40
2000 APs, 32K Clients, 40 Gbps

Catalyst 9800-80
6000 APs, 64K Clients, 80 Gbps

On-premise Appliance | Pubic or Private Cloud | On a Switch

**SD-Access only*
⁺C9800-CL for Public Cloud with FlexConnect;

Next-generation Cisco Catalyst wireless access

Ecosystem partnerships with Apple, Samsung, Intel, and Microsoft

Cisco Catalyst 9800 Series Wireless Controllers

Powered by Cisco IOS® XE
Open and programmable

Cisco Catalyst 9100 Access Points

Powered by Wi-Fi 6 technology
Superior RF experience

Resilient

- Zero downtime with Software updates and upgrades
  - WLC SMU
  - AP Service and Device Pack
  - Intelligent Rolling AP Upgrade
- Deterministic capacity at scale
- Superior battery life for IoT and mobile devices

Leadership in Wireless networking

Secure

- Detect encrypted threats with Encrypted Traffic Analytics (ETA)
- RF Snapshots, WPA3, Trustworthy systems
- Automated macro and micro segmentation with SD-Access

Extending Cisco's intent-based network

Intelligent

- Enhanced analytics with Cisco DNA
- Programmable network processor and IOx infra support
- Multi-lingual AP to enable enterprise IoT
- Deploy in infrastructure of choice and cloud of choice

Innovation Beyond the Standard

Benefits of New Configuration Model

Reusability
Config modularized as objects

Simplicity
No inheritance or containers

Easy Provisioning
With AP attribute Tagging

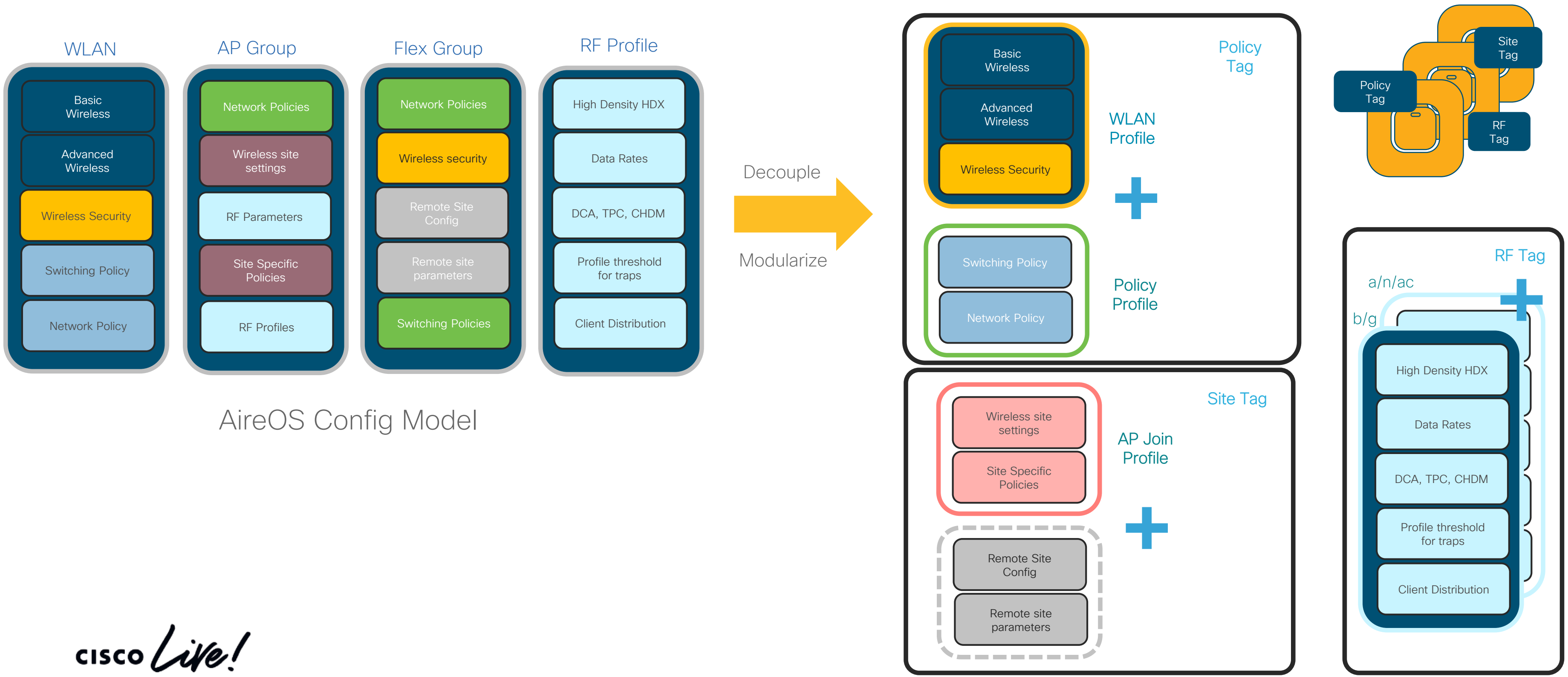
Rule-based Tagging
For easy Day 1 configuration

Change Management
Site based filtering

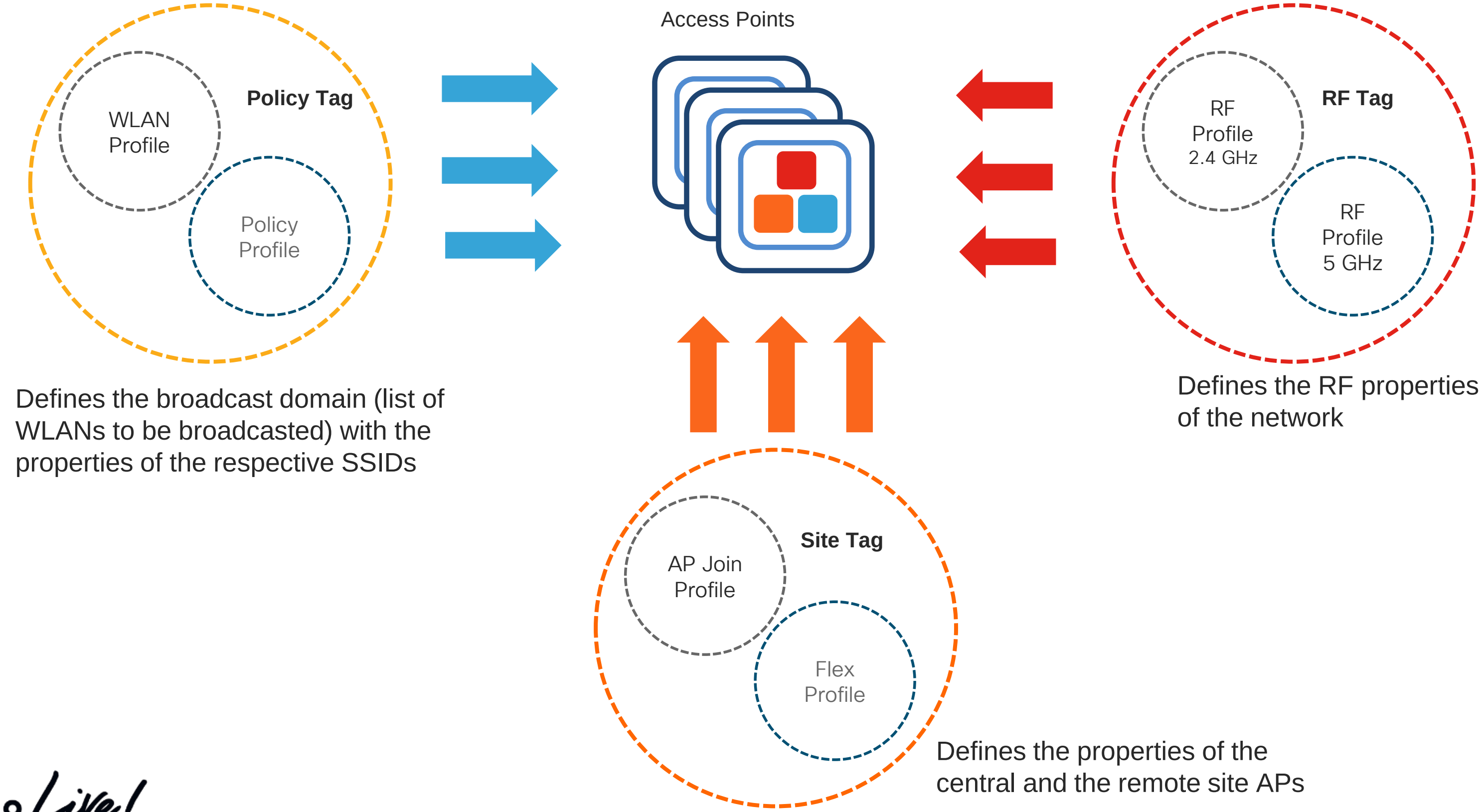
AireOS vs. Catalyst 9800 Config Model

Going towards a more Modularized and Reusable model with Logical decoupling of configuration entities

Granular & simplified
What Policies on which Sites
with what RF characteristics



Cisco Catalyst 9800 Config Model



Defines the broadcast domain (list of WLANs to be broadcasted) with the properties of the respective SSIDs

Defines the RF properties of the network

Defines the properties of the central and the remote site APs

C9800 Wireless LAN Controller Support in Cisco DNA Center

- Same Day-0 Design and Provision Workflows as AireOS WLC.
- Provisioning is done via the combination of NETCONF and CLI.
- Plug-and-Play support for C9800 is on roadmap.

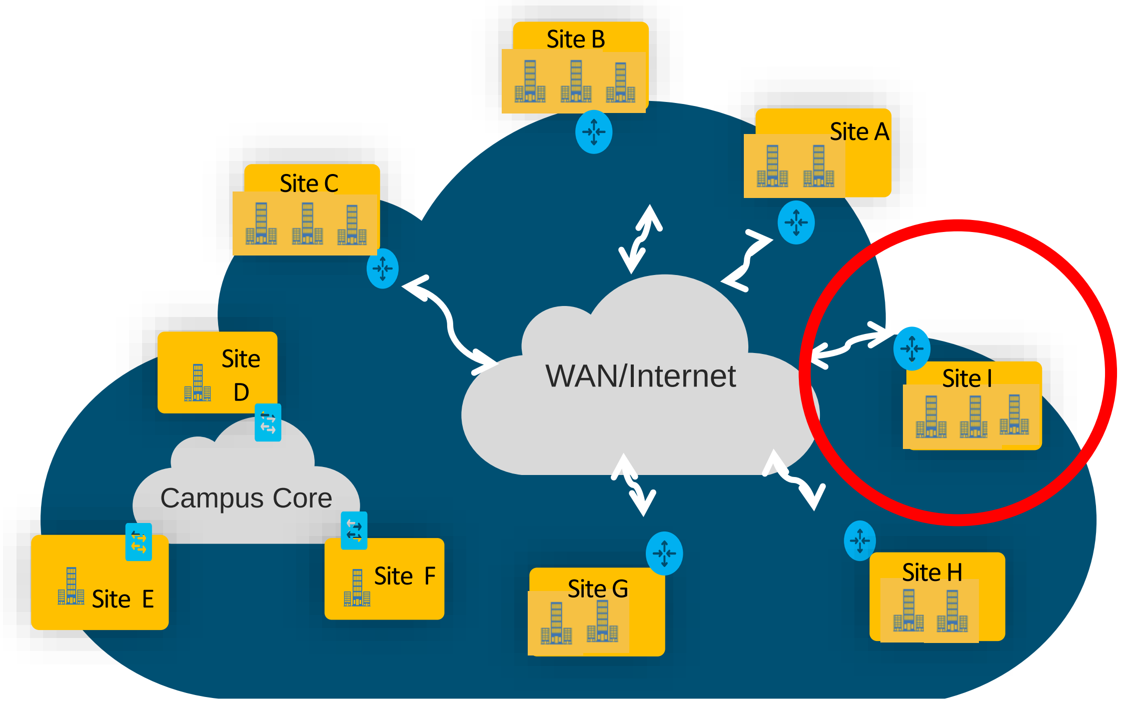
Wireless Automation Workflow with C9800 Wireless Controller

Scenario

A large enterprise is refreshing their wireless infrastructure to C9800 across multiple sites/buildings.

Business Intent

Deploy Enterprise & Guest SSIDs with customized RF profiles across sites.



Typical Customer Network

Wireless Automation - Overview

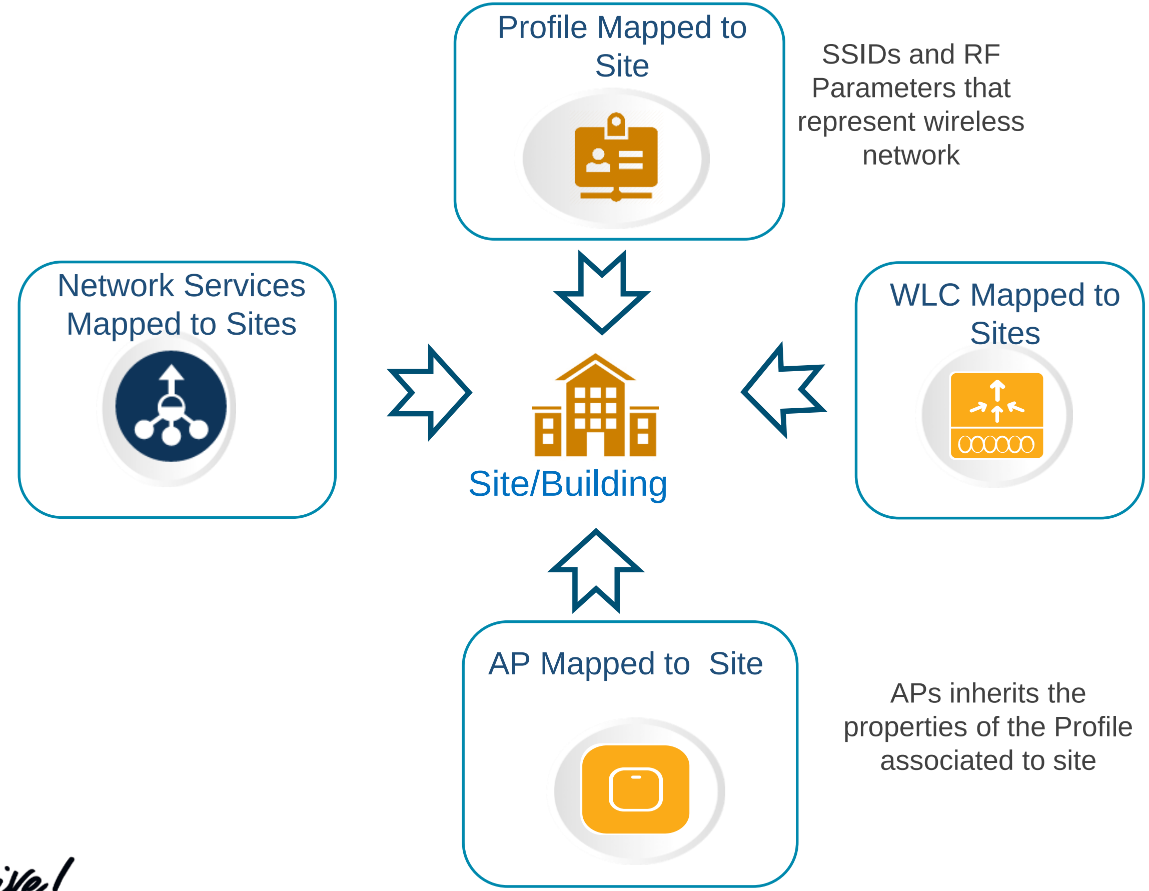
Plan

Design Network Services

Design Network Profile

Provision

Wireless Deployment Workflow



Profile Mapped to Site

SSIDs and RF Parameters that represent wireless network

Network Services Mapped to Sites

Common settings for Sites

Site/Building

WLC Mapped to Sites

Map sites that WLC will manage

AP Mapped to Site

APs inherits the properties of the Profile associated to site

Plan

Site Hierarchy & Maps

Plan

Design Network Services

Design Network Profile

Provision

Scenario - Plan

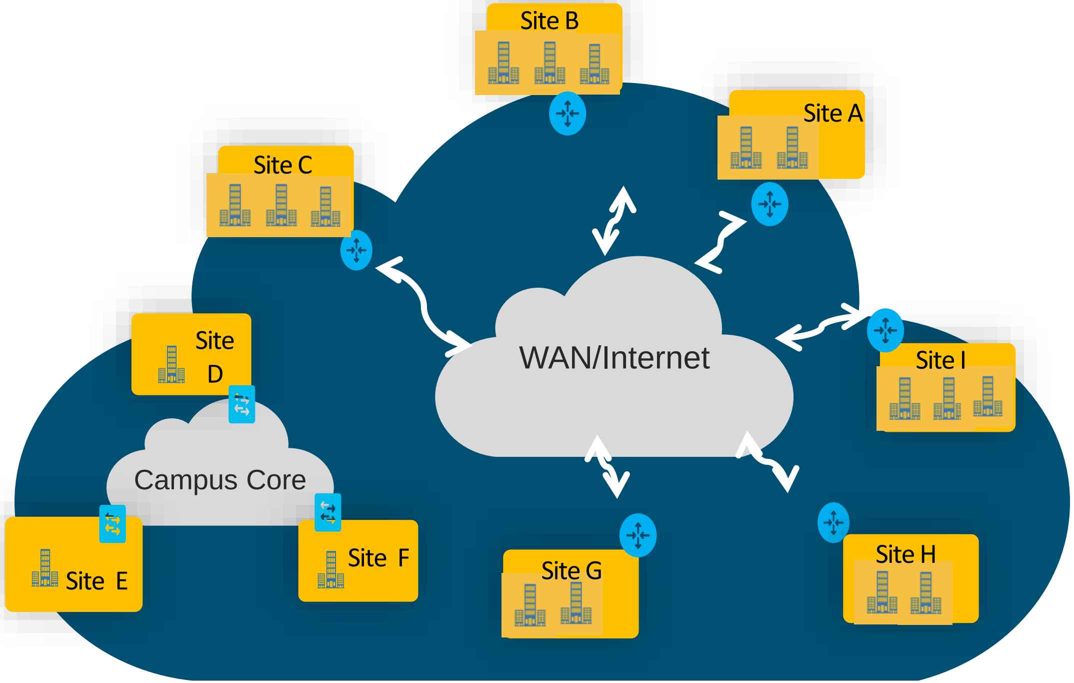
Plan deployment across all sites with common set of network components (i.e. DNS, DHCP, NTP)

Cisco Prime Infrastructure

Cisco CMX

Sites, buildings, floors

WLCs
APs
Switches
Routers



Typical Customer Network

Plan

Step -1 Create Site Hierarchy along with Buildings and Floors

Step -2 Import Floor Maps

Step -3 Manage Floor Map Properties

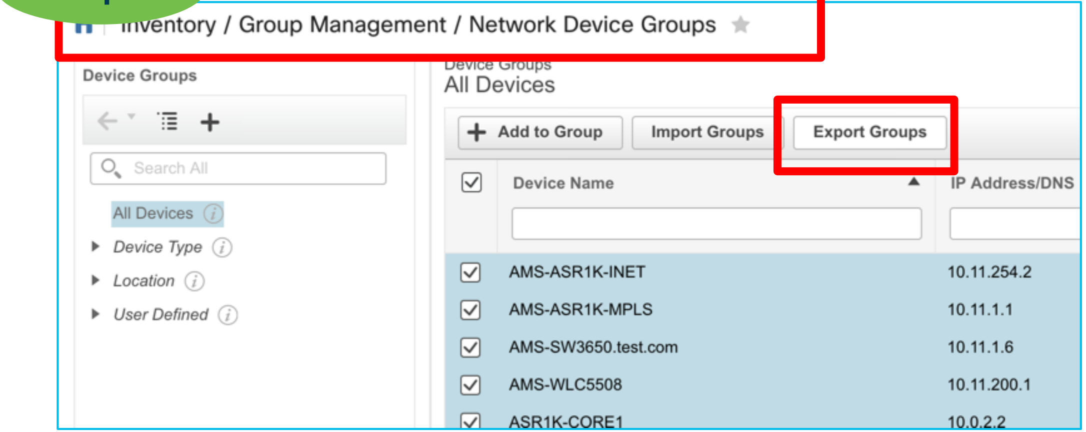
or

Step -4 Export the Site Hierarchy and Maps from PI and import into Cisco DNAC (PI Customers)

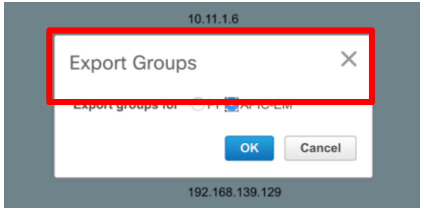
Export Sites and Maps from Prime Infrastructure

Export Sites

Step 1



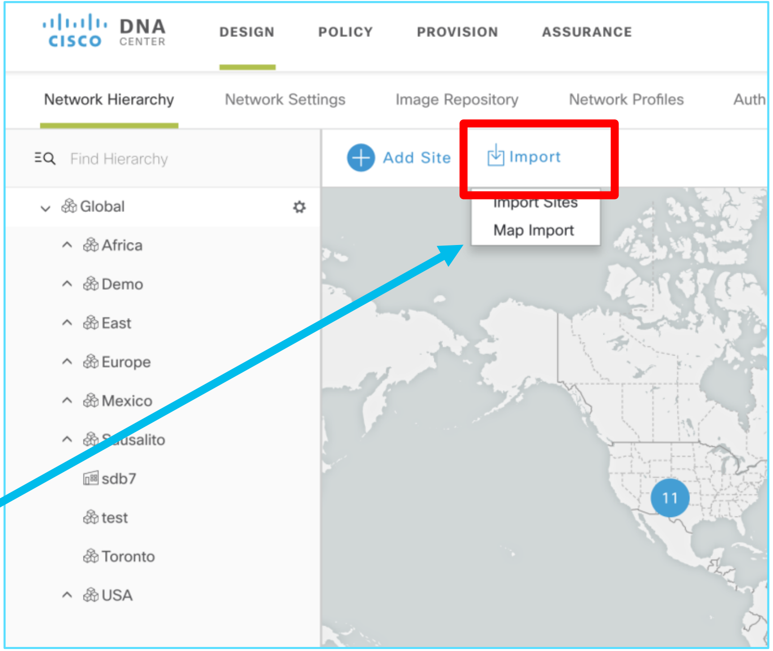
☑	Device Name	IP Address/DNS
☑	AMS-ASR1K-INET	10.11.254.2
☑	AMS-ASR1K-MPLS	10.11.1.1
☑	AMS-SW3650.test.com	10.11.1.6
☑	AMS-WLC5508	10.11.200.1
☑	ASR1K-CORE1	10.0.2.2



Export groups for ○ PI ● APIC-EM

Site.CSV

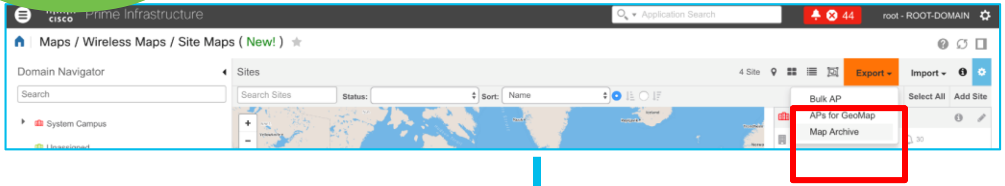
Step 2

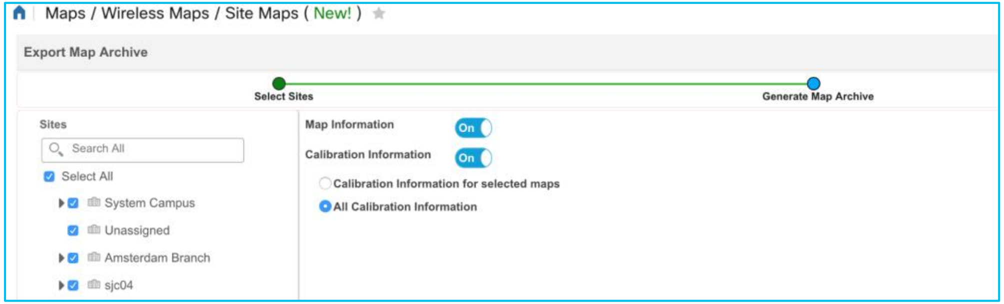


Export Sites and Maps from Prime Infrastructure

Export Maps

Step 1





- ☑ Select All
  - ☑ System Campus
  - ☑ Unassigned
  - ☑ Amsterdam Branch
  - ☑ sjc04

Map Information: On

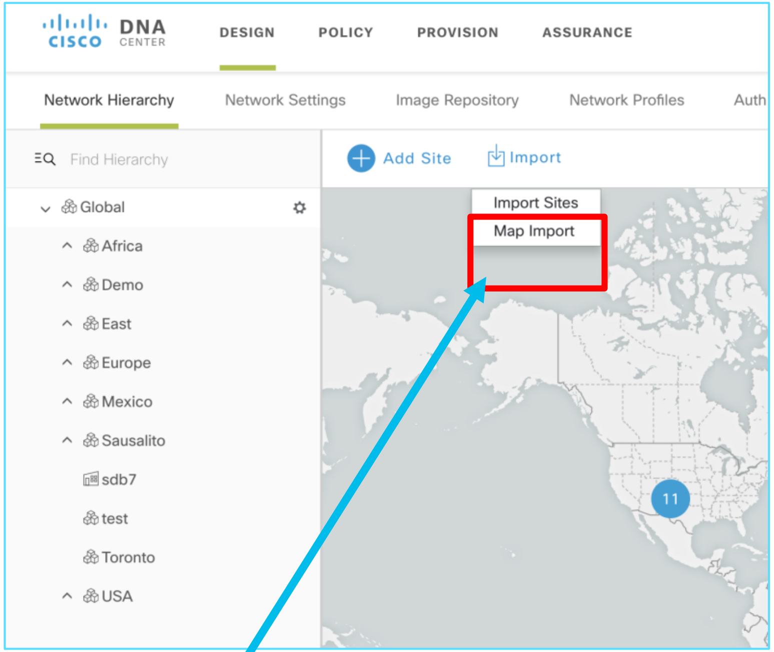
Calibration Information: On

○ Calibration Information for selected maps

● All Calibration Information

Maps.tar.gz

Step 2



cisco Live!

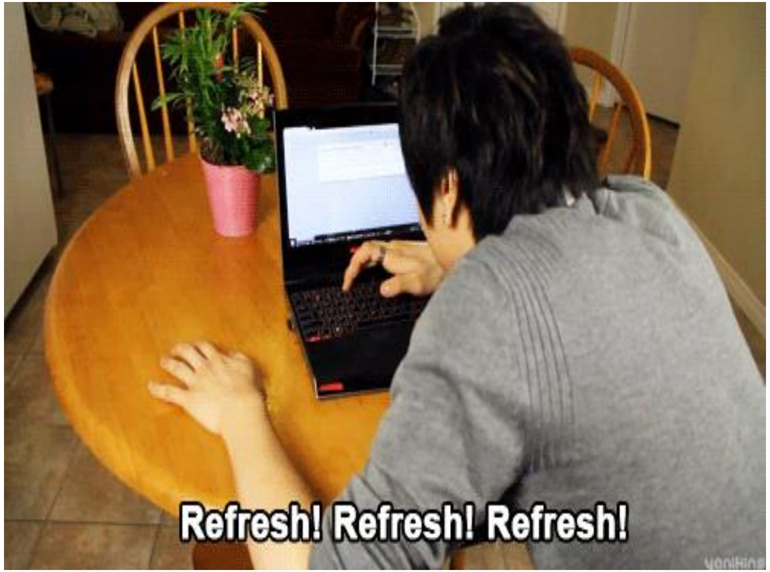
Position APs on Map – Traditional Way

Critical Part of AP Onboarding Lifecyle

1. RF Planning - Real AP or Predictive Site Survey to plan AP positions via RF survey tools
2. Give a copy of floor plan with AP positions to installers for installing APs
3. Installers connect the cables and power on APs.
4. APs join WLC and are discovered by NMS tools.
5. On NMS tools, network admin drags and drops APs to positions on map based on the same floor plan in step 2.

Position APs on Map – Traditional Way

Critical Part of AP Onboarding Lifecyle



Challenges with Traditional Way

- Waiting... Waiting.... Waiting...
- Why position APs manually twice?

  Once in RF tools, Once in NMS map.

Position APs on Map – New Way

How to resolve challenges from traditional way?

Traditional Way

1. RF Planning - Real AP or Predictive Site Survey to plan AP positions via RF survey tools
2. Give a copy of floor plan with AP positions to installers for installing APs
3. Installers connect the cables and power on APs.
4. APs join WLC and are discovered by NMS tools
5. On NMS tools, network admin drags and drops APs to positions on map based on the same floor plan in step 2.

New Way

1. RF Planning - Real AP or Predictive Site Survey to plan AP positions via RF survey tools
2. On Cisco DNA Center, plan AP positions natively or import AP position from Ekahau survey tool
3. Give a copy of floor plan with AP positions to installers for installing APs
4. Installers connect the cables and power on APs.
5. Cisco DNA Center claims APs to desired site/controller via PnP and they are shown on map automatically in planned positions.

Position APs on Map – New Way

Critical Part of AP Onboarding Lifecyle

Position APs on Map – New Way

Planned APs on Map – Under the Hood

Cisco DNA Center 1.3.1

- Users defined planned APs with name, model, antenna and positions on map.
- When real APs are added into inventory either via discovery or PnP claim, Cisco DNA Center will match them against planned APs based on AP name, model and antenna.
  - When all matched, APs are put to planned AP positions automatically. The heatmap are displayed accordingly.
  - Otherwise, planned APs stay. Users can manually assign real APs to planned APs if required.

Position APs on Map – New Way

Planned APs on Map – Under the Hood

Cisco DNA Center 1.3.1

There are two options to define planned APs:

1. Create natively on Cisco DNA Center

   In 1.3.1 release, it only support creating planned APs with name, model, antennas and position. It is NOT predictive RF planning with heatmap.

2. Import from Ekahau project

- Ekahau 10.0.2 or later.
- Only Ekahau project created in planning mode, not site survey mode.
- Support Ekahau project file size to 500 Mb.
- Support importing APs, maps and obstacles

Position APs on Map – New Way

Planned APs on Map – Under the Hood

Cisco DNA Center 1.3.1

To import Ekahau project successfully, follow the rules below:

- Define Network Hierarchy in Cisco DNA Center first.
- Match building and floor names in Cisco DNA Center what are defined in Ekahau.
- Import insertion point in "**Network Hierarchy**" of Cisco DNA Center needs to be one level higher than top level of hierarchy in Ekahau.
  - If building and floors are defined in Ekahau, import at "**Area**" level of Cisco DNA Center.
  - If only floors are defined in Ekahau, import at "**Building**" level of Cisco DNA Center.

Demo - Network Hierarchy and Map with Ekahau Integration

Design Network Services

Plan

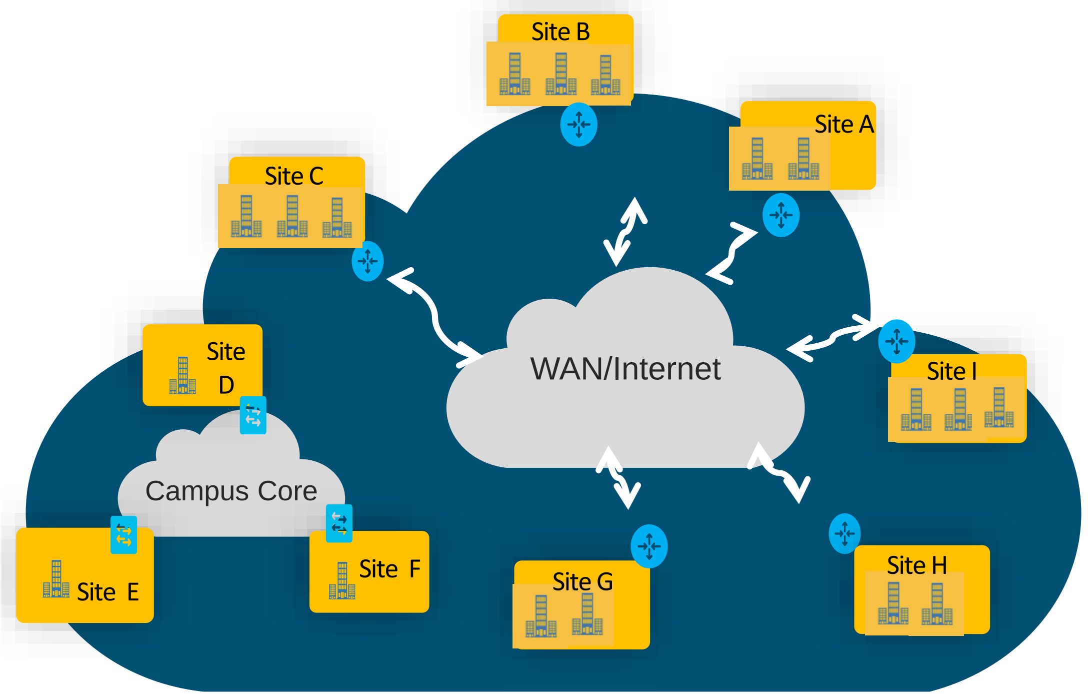
Design Network Services

Design Network Profile

Provision

Scenario - Planning

Plan deployment across all sites with common set of network components (i.e. AAA, DNS, DHCP, NTP, syslog)



Typical Customer Network

Network Services and Credentials

Network Services

- AAA (Network and Client)
- DNS, DHCP
- NTP

Monitoring Services

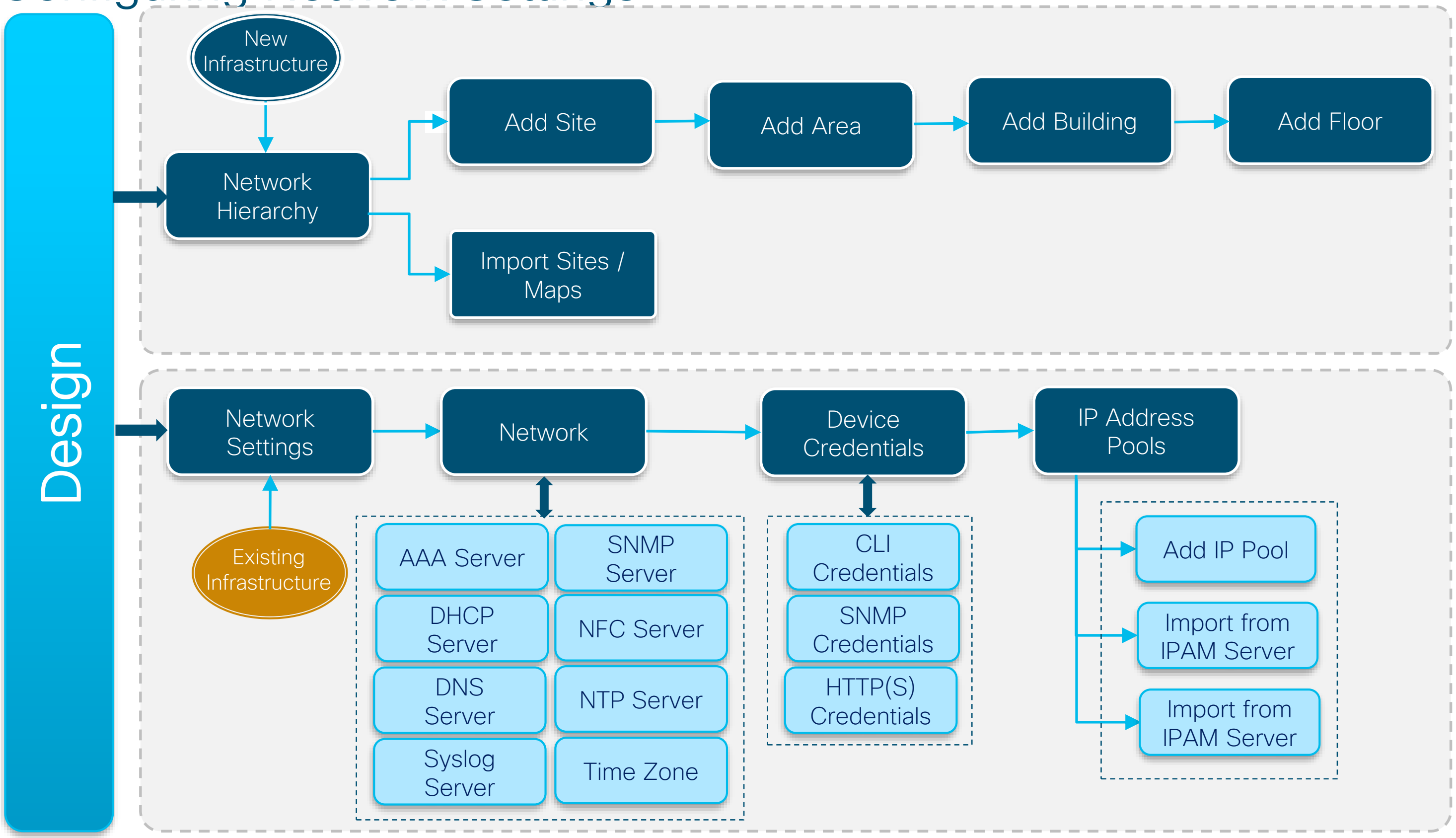
- Syslog
- Traps
- Netflow and Application Visibility

Credentials

- CLI
- SNMP
- HTTP

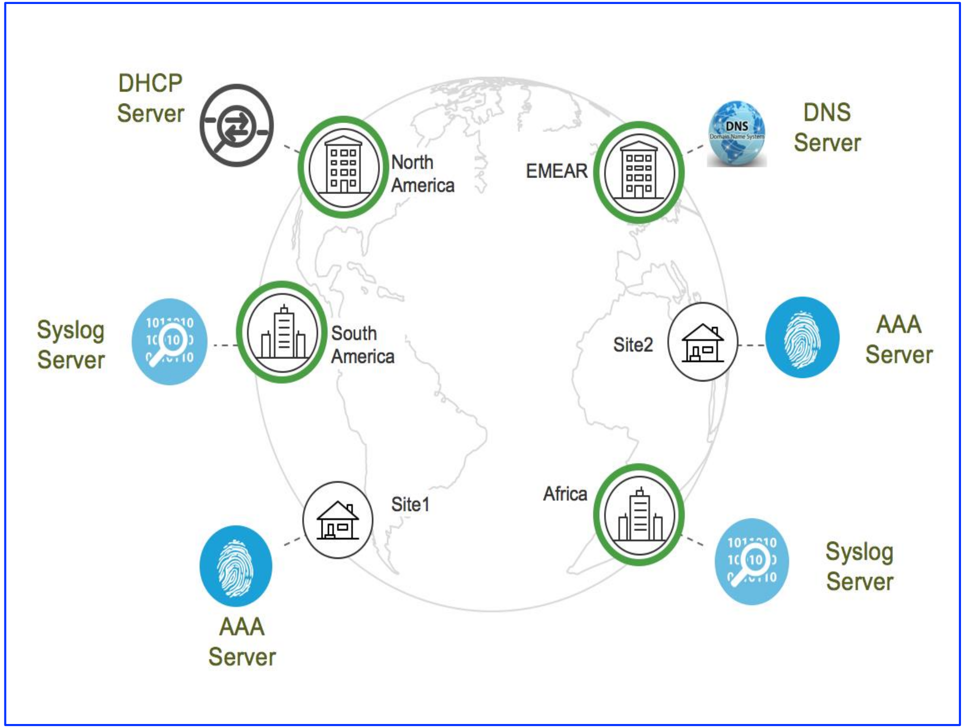
Design Network

Configuring Network Settings



Challenges with Network Services & Credentials

- Vary by :
  - Location
  - Differences in Network Design
- Information often stored in Files - Error Prone
- Day 2 Updates become a challenge



AAA/ISE Integration

AAA Server - ISE Integration

Objectives and Key Points

- Single pane of management for all AAA/policy administration between network devices and ISE
- Automate RADIUS/TACACS configuration for network devices.
- Support only one ISE cluster.
- Enable secure services between Cisco DNAC and ISE:
  - pxGrid Service to pull the info out of ISE (Uni-Directional)

    Obtain TrustSec metadata such as SGT, IP-SGT mappings & TrustSec policy.
  - ERS (External RESTful Services) APIs - Bi-Directional Communication
    - Fetch deployment model from ISE, such as PAN and PSN info
    - Add devices to ISE as network devices
    - Create SGT, IP-SGT mappings & TrustSec policy on ISE

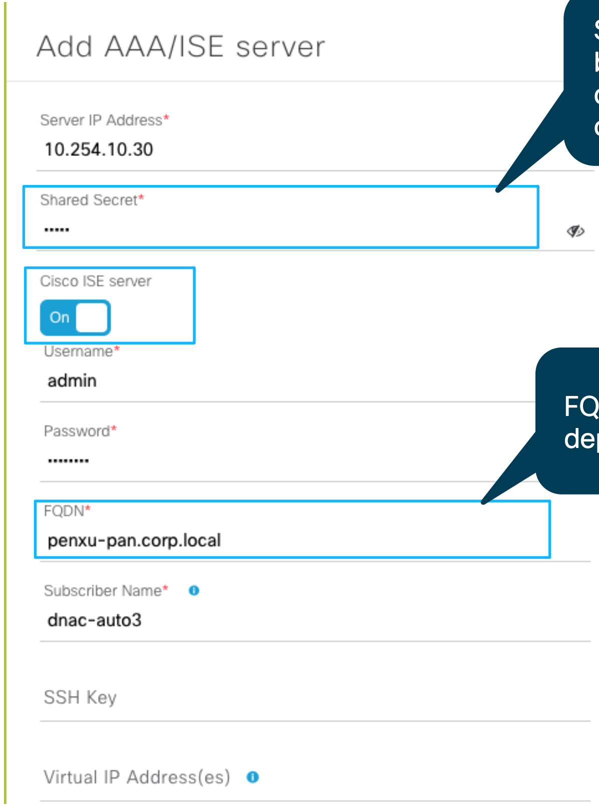
AAA Server - ISE Integration

Pre-Requisites

- The minimum supported ISE version is 2.3
- pxGrid service and SSH should be enabled on ISE.
- ISE super admin credential is used for trust establishment for SSH/ERS API communication.
- ISE CLI and UI user accounts must use the same username and password
- ISE admin certificate must contain ISE IP or FQDN in either CN or SAN.
- DNA-C system certificate must contain DNAC IP or FQDN in either subject name or SAN.
- pxGrid node should be reachable on eth0 IP of ISE from DNA-C.

AAA Server - ISE Integration

Add ISE in DNA-C



Add AAA/ISE server

Server IP Address*
10.254.10.30

Shared Secret*
•••••

Cisco ISE server
On

Username*
admin

Password*
••••••••

FQDN*
penxu-pan.corp.local

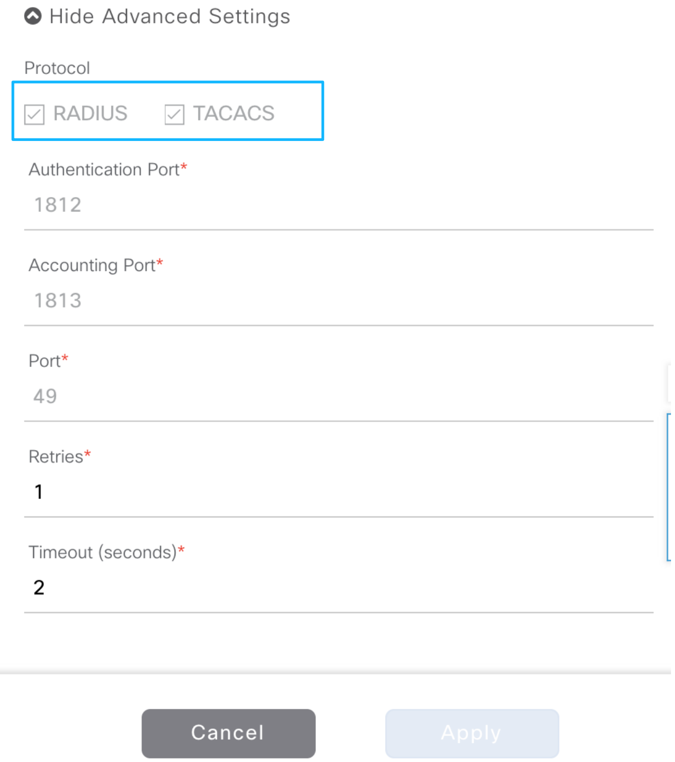
Subscriber Name*
dnac-auto3

SSH Key

Virtual IP Address(es)

Shared secret between ISE and devices for TACACS or Radius

FQDN from ISE deployment



Hide Advanced Settings

Protocol
☑ RADIUS ☑ TACACS

Authentication Port*
1812

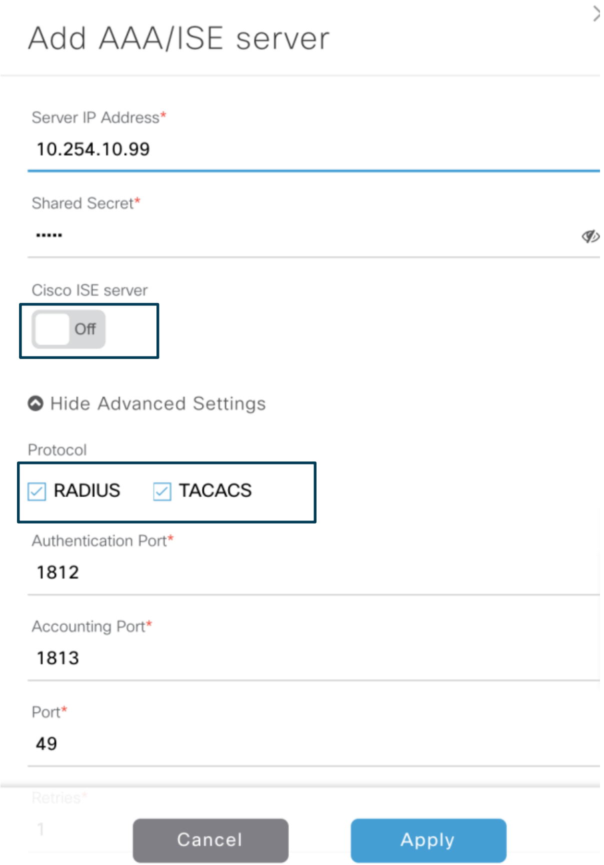
Accounting Port*
1813

Port*
49

Retries*
1

Timeout (seconds)*
2

AAA Server - (Non-ISE) Integration



Add AAA/ISE server

Server IP Address*
10.254.10.99

Shared Secret*
•••••

Cisco ISE server
Off

Hide Advanced Settings

Protocol
☑ RADIUS ☑ TACACS

Authentication Port*
1812

Accounting Port*
1813

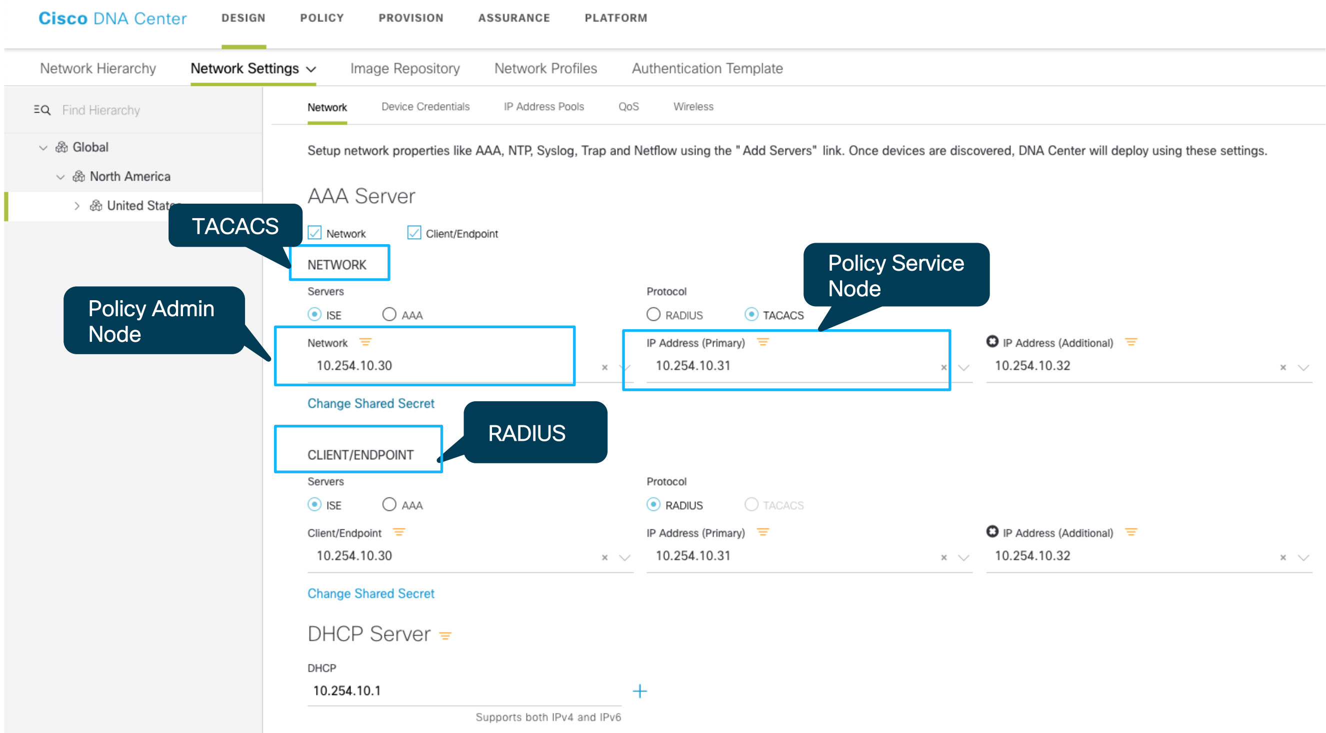
Port*
49

Retries*
1

Key Points:

- Non-ISE server definition:
  - ISE running 2.2 or below
  - ACS or any third-party AAA Server
- Only automate RADIUS/TACACS configuration for network devices
- Require to add network devices to AAA clients manually.
- Can have multiples non-ISE AAA servers

Network Settings



Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Network Hierarchy | Network Settings | Image Repository | Network Profiles | Authentication Template

Find Hierarchy

- Global
  - North America
    - United States

Network | Device Credentials | IP Address Pools | QoS | Wireless

Setup network properties like AAA, NTP, Syslog, Trap and Netflow using the " Add Servers" link. Once devices are discovered, DNA Center will deploy using these settings.

AAA Server

☑ Network ☑ Client/Endpoint

NETWORK

Servers: ● ISE ○ AAA

Protocol: ○ RADIUS ● TACACS

Network: 10.254.10.30

IP Address (Primary): 10.254.10.31

IP Address (Additional): 10.254.10.32

Change Shared Secret

CLIENT/ENDPOINT

Servers: ● ISE ○ AAA

Protocol: ● RADIUS ○ TACACS

Client/Endpoint: 10.254.10.30

IP Address (Primary): 10.254.10.31

IP Address (Additional): 10.254.10.32

Change Shared Secret

DHCP Server

DHCP: 10.254.10.1

Supports both IPv4 and IPv6

TACACS

Policy Admin Node

Policy Service Node

RADIUS

AAA Settings

Demo - Network Settings

What did we do so far?

Planned the Sites & Hierarchy

Extracted Common/Standard across Wired and Wireless to be self managed

Design Network Profile for Wireless

Plan

Design Network Services

Design Network Profile

Provision

Traditionally ..

WLC

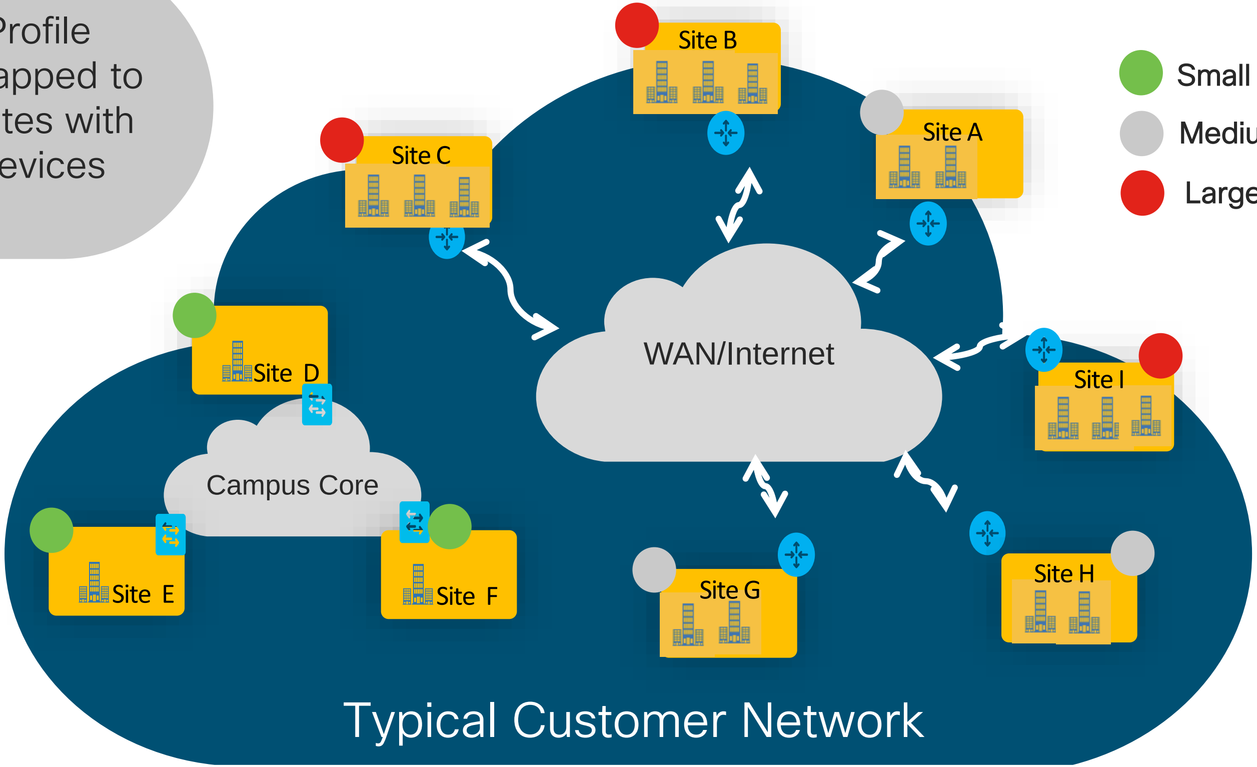
- HA Configuration
- Interfaces Configuration for Enterprise and Guest
- Radius & AAA Servers
- SSID - Authentication, QoS
- Advanced : Local Profiling, Client DHCP, Local/Flex Connect
- Manage AP Groups- RF Profiles (DCA Settings, RRM),WLAN Interface
- Associate AP to AP Groups

Problem with this approach

- Need to manually manage the mapping of AP to AP Groups
- Need to manually map SSID's to AP Groups
- Increased Complexity and Error prone
- Similar issue for AP Configuration
- No Repeatability for Future growth

Network Deployment using Profiles

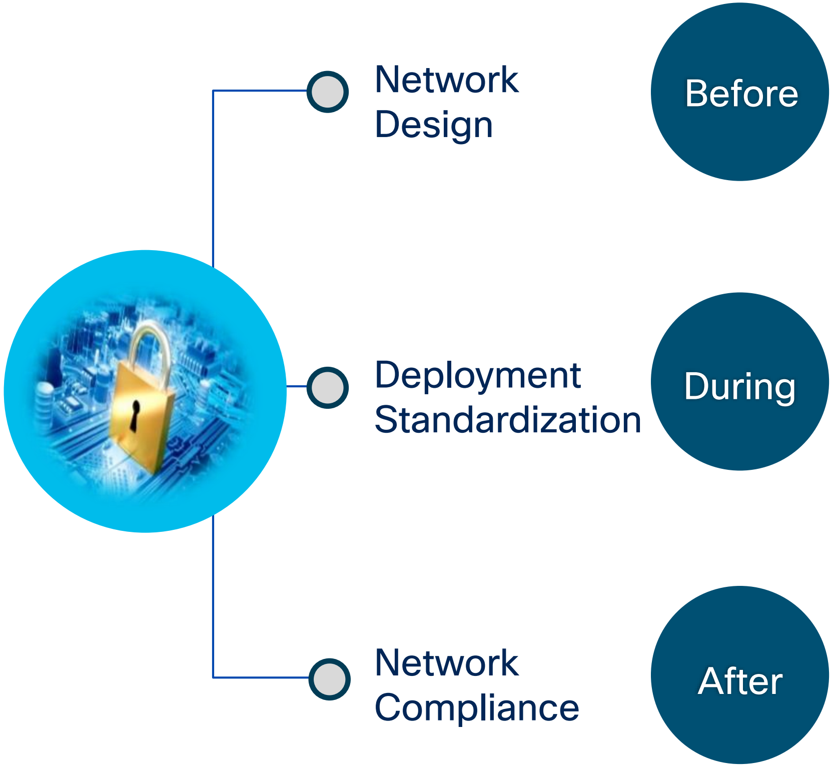
A Single Profile can be mapped to multiple sites with multiple devices



🟢	Small Sites - Small Profile
⚪	Medium Sites - Medium Profile
🔴	Large Sites - Large Profile

Network Deployment using Profile

Profile Based Deployment



Network Design

Before

- Plan for the network deployment
- Feature and Capabilities to be enabled based on requirements
- Topology for network deployment

Deployment Standardization

During

- PnP Based Day 0 Deployment
- Version management of Profile for Day 2 Change Management

Network Compliance

After

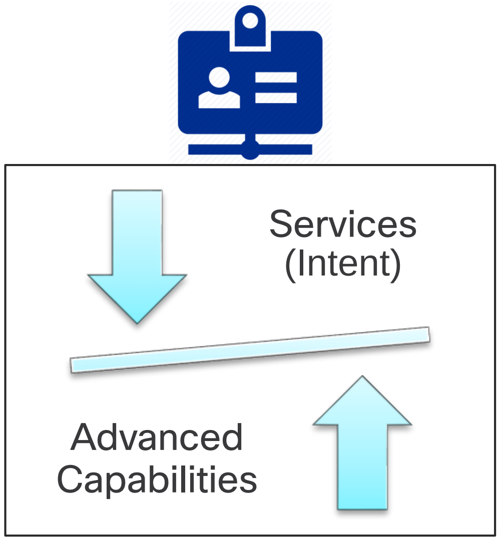
- Configuration Compliance Validation against Profile
- Remediation of Configuration to Golden Configuration

Simplified Network Deployment

Configuration Consistency

Integrated IT Process Flows

Contents of a Wireless Profile



Services

- SSID
- Guest Network
- RF Profiles
- Deployment mode

70%-80% of the WLC Config or more

Named Capabilities

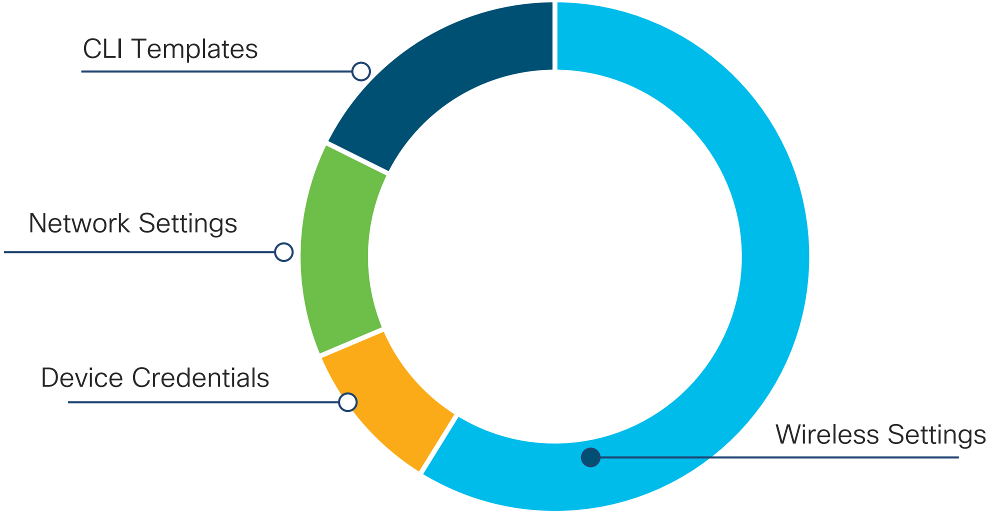
- Clean Air
- 11k
- 11v

CLI Templates

- Customized Features
- Cisco Best Practice Out of the box

20%-30% of the WLC Config or less

Wireless Network Profile - Composition View



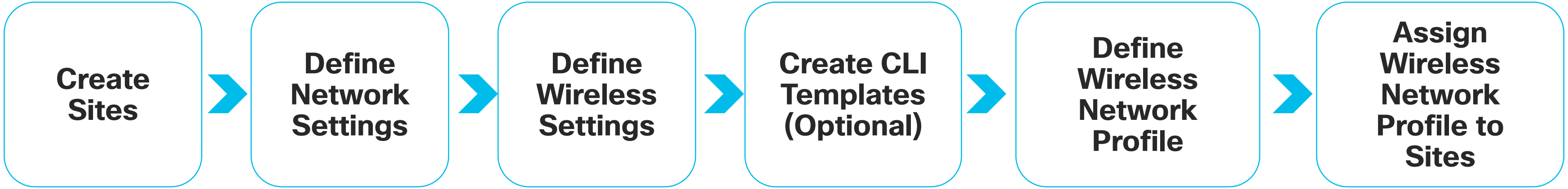
System Generated Configuration by Cisco DNA Center UI Orchestration

- Network Settings
- Device Credentials
- Wireless Settings

User Defined Configuration

- CLI Templates

Wireless Profile - Design Workflow



Create Sites

Define Network Settings

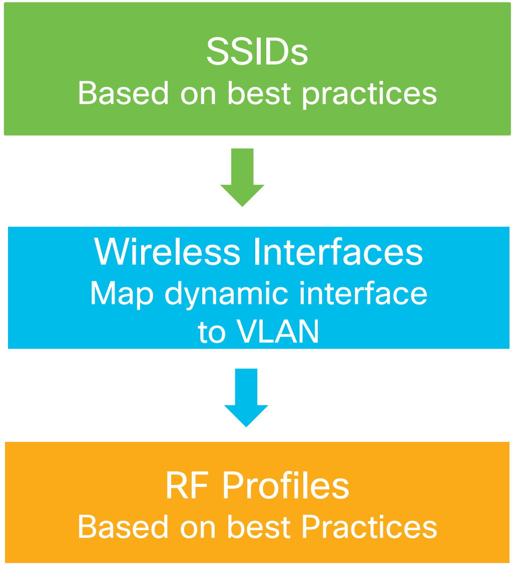
Define Wireless Settings

Create CLI Templates (Optional)

Define Wireless Network Profile

Assign Wireless Network Profile to Sites

Design- Wireless Settings

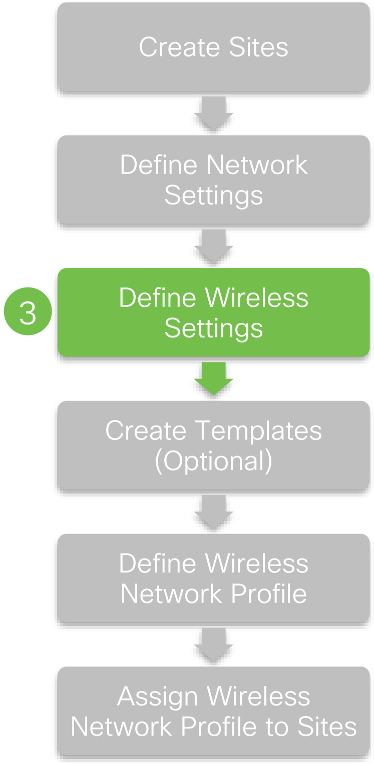


SSIDs
Based on best practices

Wireless Interfaces
Map dynamic interface to VLAN

RF Profiles
Based on best Practices

Design- Define Wireless Settings



Create Sites

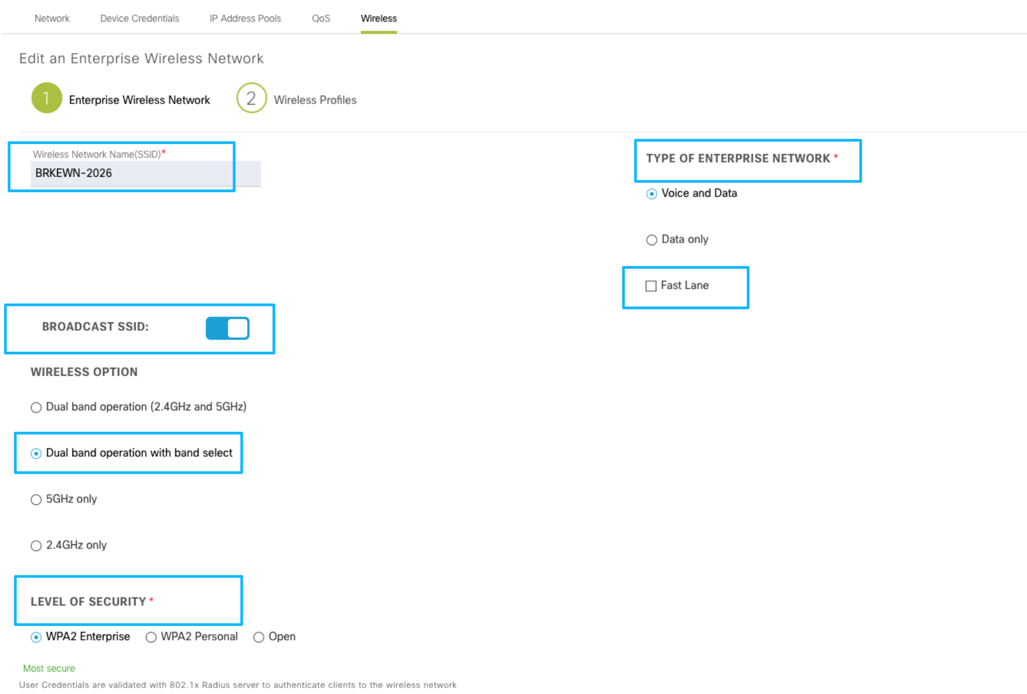
Define Network Settings

3 Define Wireless Settings

Create Templates (Optional)

Define Wireless Network Profile

Assign Wireless Network Profile to Sites



Edit an Enterprise Wireless Network

1 Enterprise Wireless Network 2 Wireless Profiles

Wireless Network Name(SSID)*: BRKEWN-2026

TYPE OF ENTERPRISE NETWORK *

● Voice and Data

○ Data only

□ Fast Lane

BROADCAST SSID: on

WIRELESS OPTION

○ Dual band operation (2.4GHz and 5GHz)

● Dual band operation with band select

○ 5GHz only

○ 2.4GHz only

LEVEL OF SECURITY *

● WPA2 Enterprise ○ WPA2 Personal ○ Open

Most secure

User Credentials are validated with 802.1x Radius server to authenticate clients to the wireless network

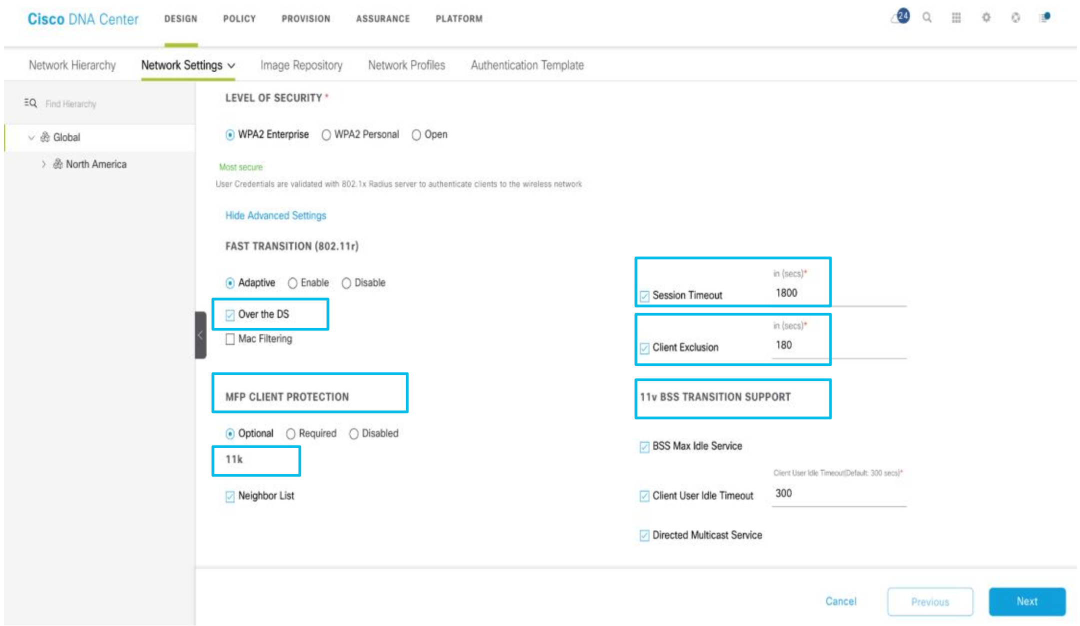
Create Enterprise Wireless SSID

Design- Wireless Settings

Advanced Parameters in SSID

Supported in Cisco DNAC 1.3

- 802.11r - Over the DS
- Session Timeout
- Client Exclusion
- MFP Client Protection
- 802.11k
- 802.11v



LEVEL OF SECURITY *

● WPA2 Enterprise ○ WPA2 Personal ○ Open

Most secure

User Credentials are validated with 802.1x Radius server to authenticate clients to the wireless network

Hide Advanced Settings

FAST TRANSITION (802.11r)

● Adaptive ○ Enable ○ Disable

☑ Over the DS

□ Mac Filtering

MFP CLIENT PROTECTION

● Optional ○ Required ○ Disabled

11k

☑ Neighbor List

☑ Session Timeout — in (secs)*: 1800

☑ Client Exclusion — in (secs)*: 180

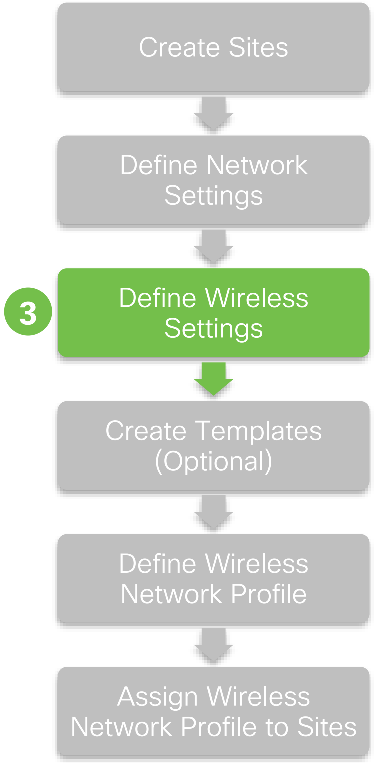
11v BSS TRANSITION SUPPORT

☑ BSS Max Idle Service

☑ Client User Idle Timeout — Client User Idle Timeout(Default: 300 secs)*: 300

☑ Directed Multicast Service

Design - Define Wireless Settings



Create Sites

Define Network Settings

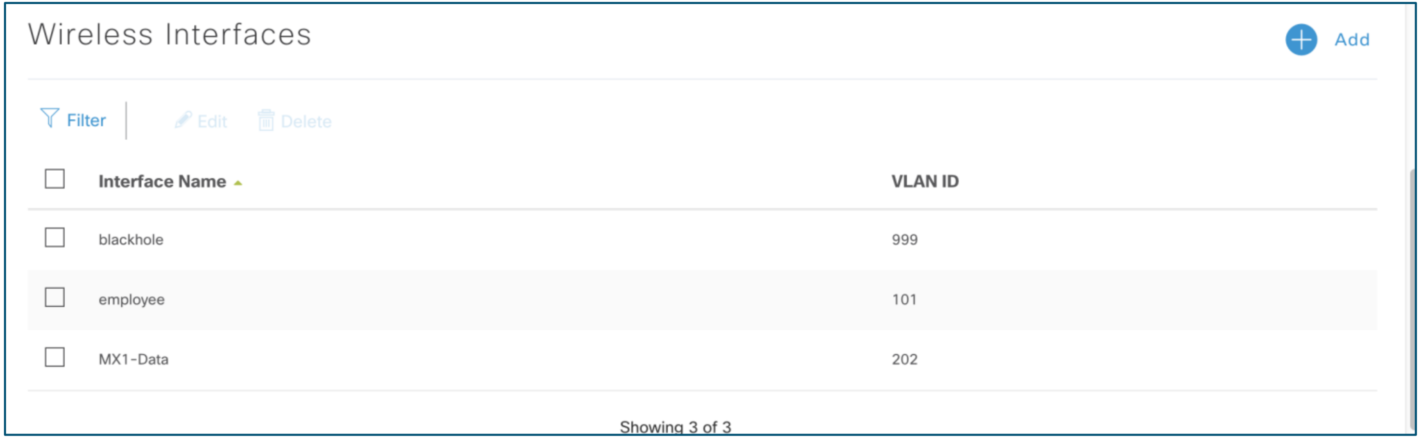
3 Define Wireless Settings

Create Templates (Optional)

Define Wireless Network Profile

Assign Wireless Network Profile to Sites

Create Wireless Interfaces

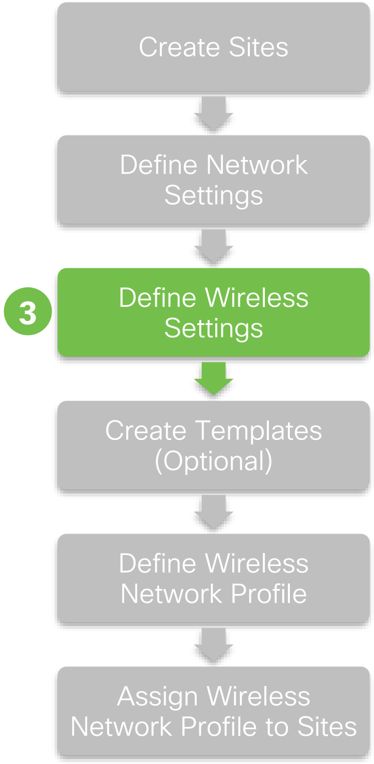


Wireless Interfaces

□	Interface Name ▲	VLAN ID
□	blackhole	999
□	employee	101
□	MX1-Data	202

Showing 3 of 3

Design - Define Wireless Settings



Create Sites

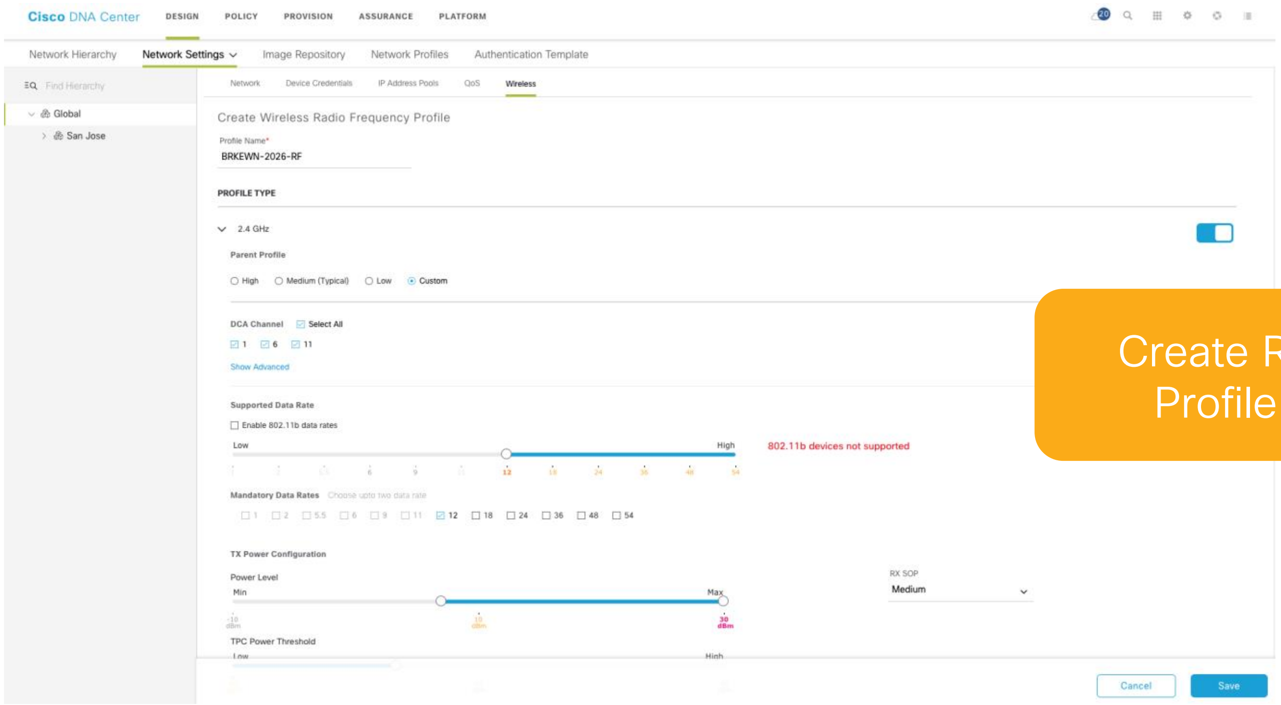
Define Network Settings

3 Define Wireless Settings

Create Templates (Optional)

Define Wireless Network Profile

Assign Wireless Network Profile to Sites



Create Wireless Radio Frequency Profile

Profile Name*: BRKEWN-2026-RF

PROFILE TYPE

2.4 GHz

Parent Profile

○ High ○ Medium (Typical) ○ Low ● Custom

DCA Channel ☑ Select All

☑ 1 ☑ 6 ☑ 11

Show Advanced

Supported Data Rate

□ Enable 802.11b data rates

Low — High: 12 – 54

802.11b devices not supported

Mandatory Data Rates Choose upto two data rate

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

TX Power Configuration

Power Level

Min — Max: 10 dBm – 30 dBm

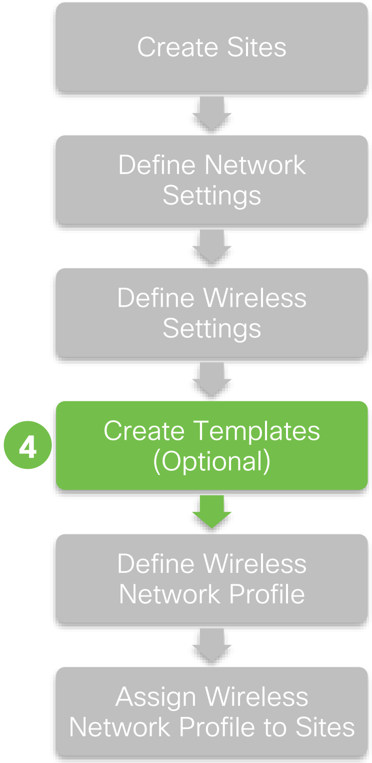
RX SOP: Medium

TPC Power Threshold

Low — High

Create RF Profile

Design - Create Templates



Create Sites

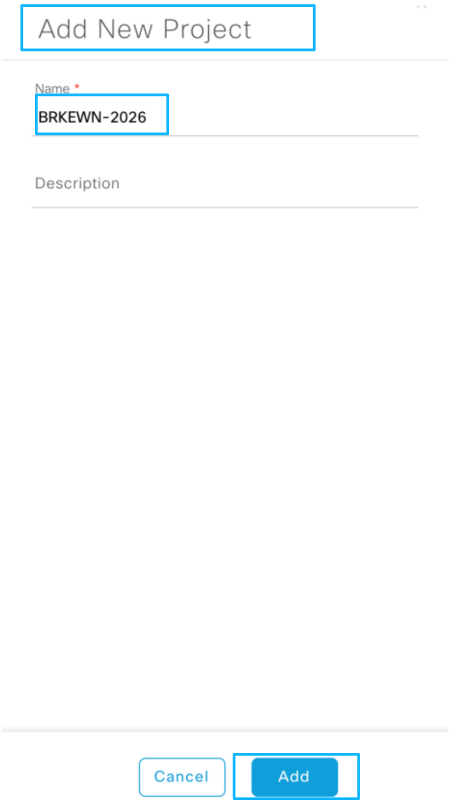
Define Network Settings

Define Wireless Settings

4 Create Templates (Optional)

Define Wireless Network Profile

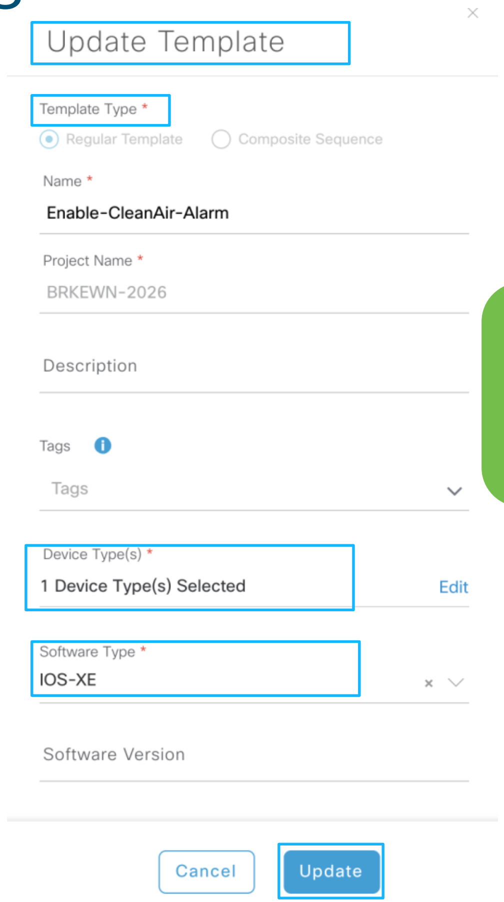
Assign Wireless Network Profile to Sites



Add New Project

Name * BRKEWN-2026

Description



Update Template

Template Type *

● Regular Template ○ Composite Sequence

Name * Enable-CleanAir-Alarm

Project Name * BRKEWN-2026

Description

Tags

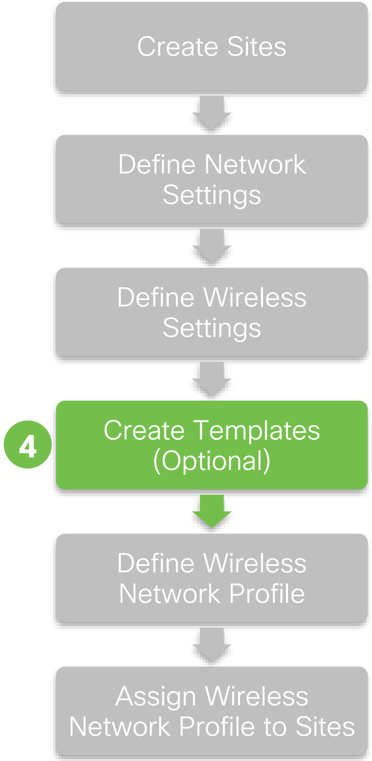
Device Type(s) * 1 Device Type(s) Selected

Software Type * IOS-XE

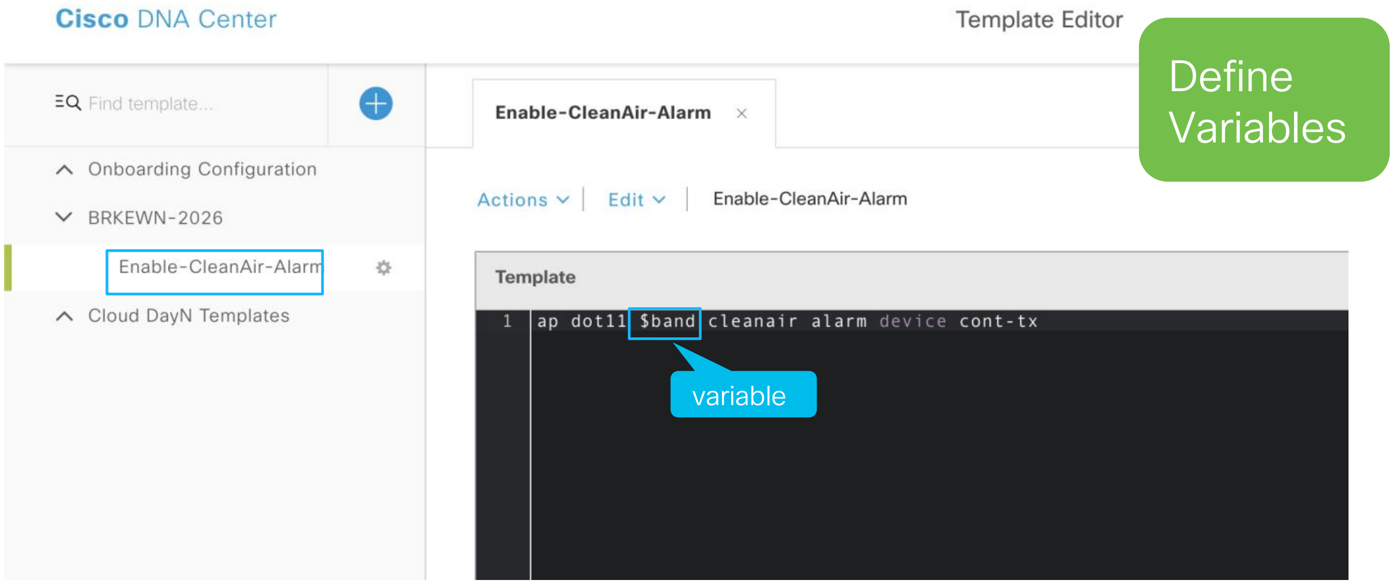
Software Version

Create Project and Template in “Template Editor”

Design - Create Templates


Create Sites
Define Network Settings
Define Wireless Settings
4
Create Templates (Optional)
Define Wireless Network Profile
Assign Wireless Network Profile to Sites

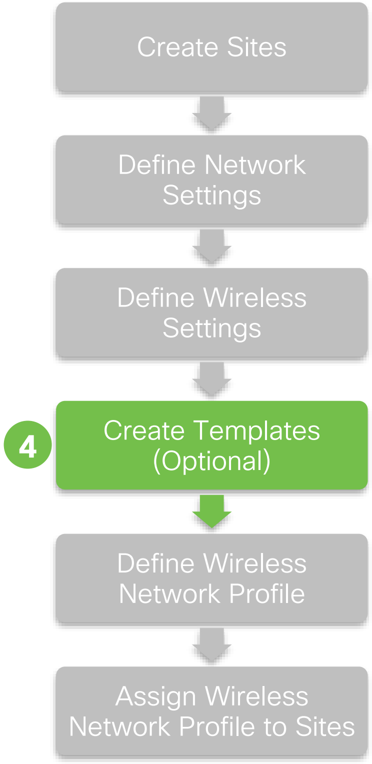
- Cool programming-like template view for copy/paste and editing.
- Template engine is based on Apache Velocity engine.
- Use “$” sign to define variable.



```
ap dot11 $band cleanair alarm device cont-tx
```

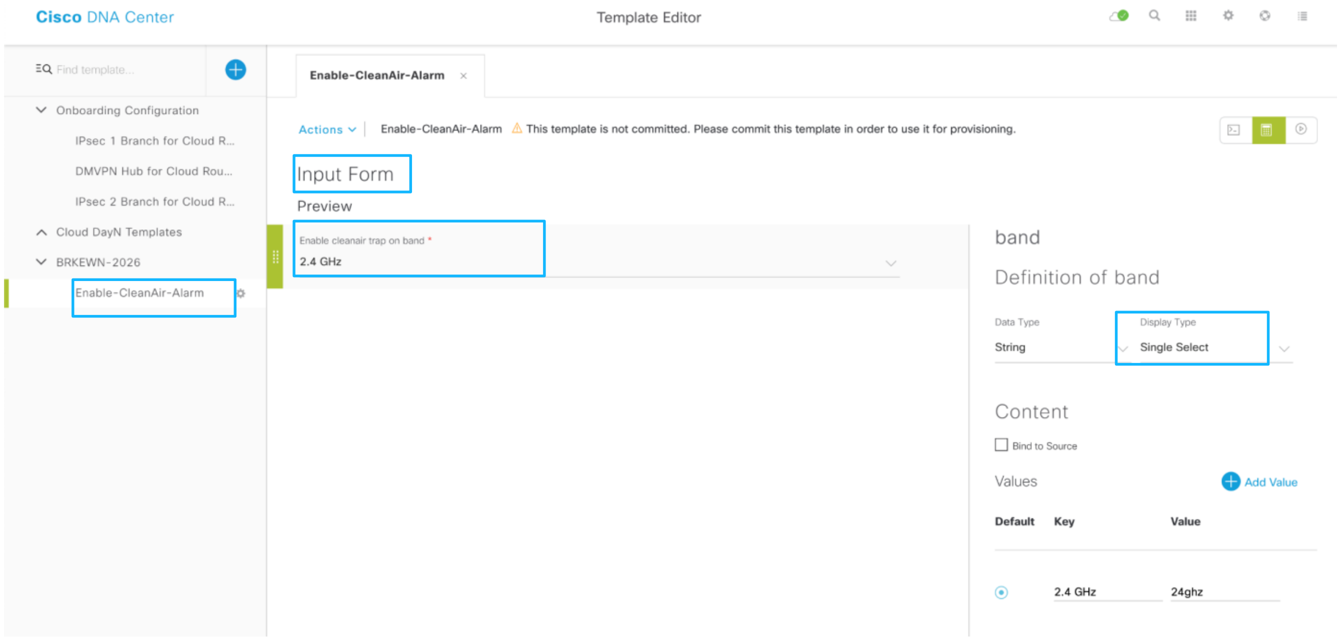
Design - Create Templates

Form View



Create Sites
Define Network Settings
Define Wireless Settings
4
Create Templates (Optional)
Define Wireless Network Profile
Assign Wireless Network Profile to Sites

- Define detailed info of variable in “Input Form” view.
- Default value of variable will auto populate for user during provisioning.



Cisco DNA Center Template Editor

Find template...

- Onboarding Configuration
  - IPsec 1 Branch for Cloud R...
  - DMVPN Hub for Cloud Rou...
  - IPsec 2 Branch for Cloud R...
- Cloud DayN Templates
- BRKEWN-2026
  - Enable-CleanAir-Alarm

Enable-CleanAir-Alarm ×

Actions | Enable-CleanAir-Alarm ⚠ This template is not committed. Please commit this template in order to use it for provisioning.

Input Form

Preview

Enable cleanair trap on band *

2.4 GHz

band

Definition of band

Data Type: String

Display Type: Single Select

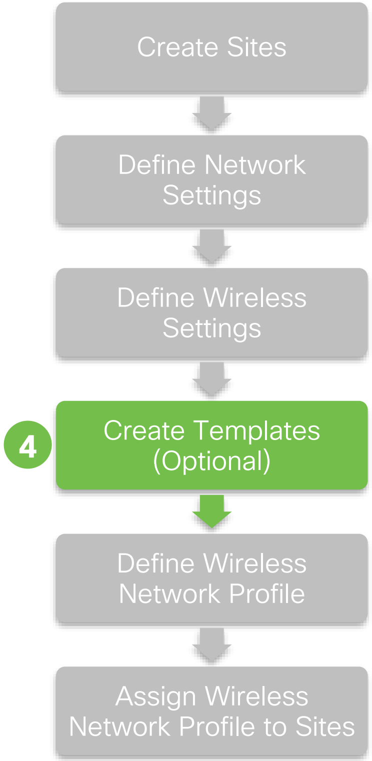
Content

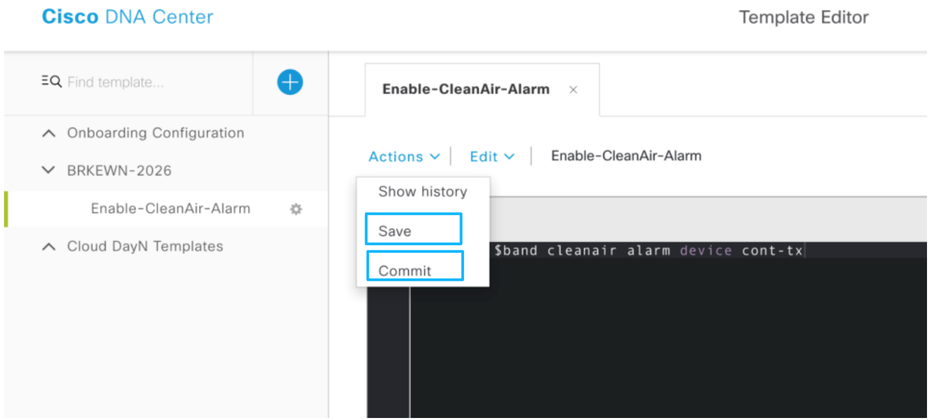
□ Bind to Source

Values ⊕ Add Value

Default	Key	Value
●	2.4 GHz	24ghz

Design - Create Templates


Create Sites
Define Network Settings
Define Wireless Settings
4
Create Templates (Optional)
Define Wireless Network Profile
Assign Wireless Network Profile to Sites

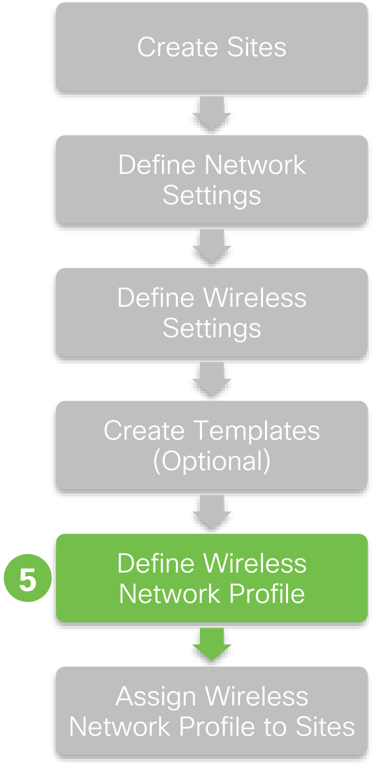


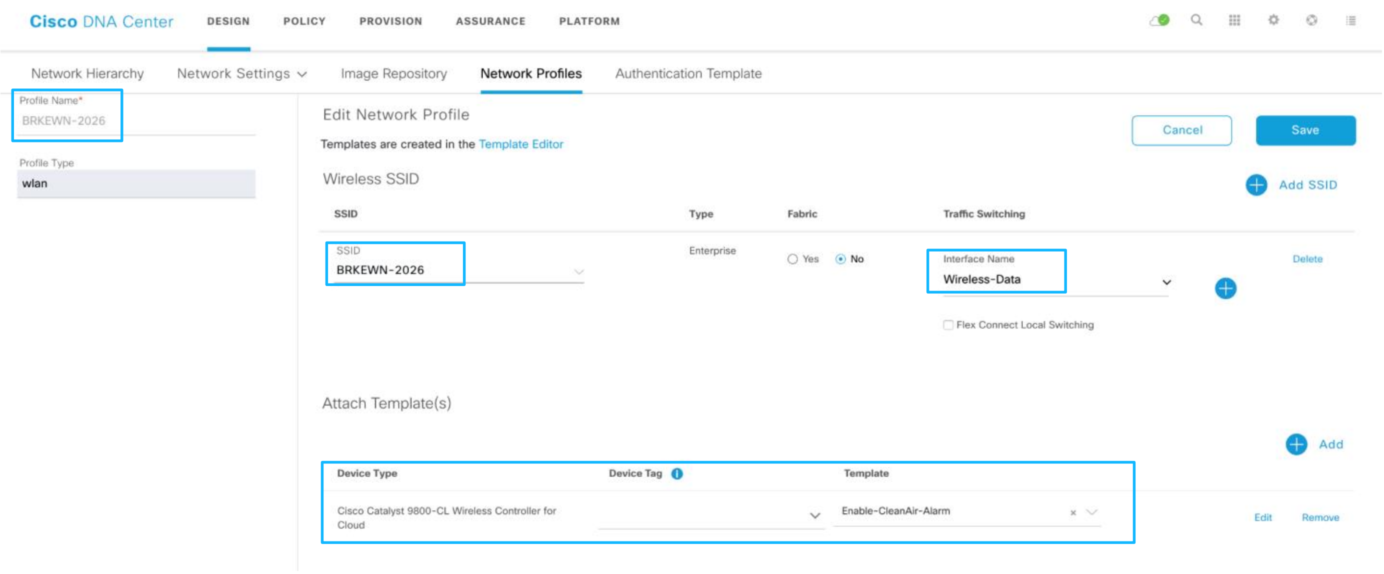
```
$band cleanair alarm device cont-tx
```

Save & Commit

- Save
  - Writable version of template on Cisco DNA Center
  - Can not be used for provisioning
- Commit
  - Once committed, it becomes read-only
  - Can commit multiple times to create multiple versions of template
  - Only latest commit version can be used for provisioning

Design - Define Wireless Network Profile


Create Sites
Define Network Settings
Define Wireless Settings
Create Templates (Optional)
5
Define Wireless Network Profile
Assign Wireless Network Profile to Sites



Profile Name* BRKEWN-2026

Profile Type wlan

Edit Network Profile

Templates are created in the Template Editor

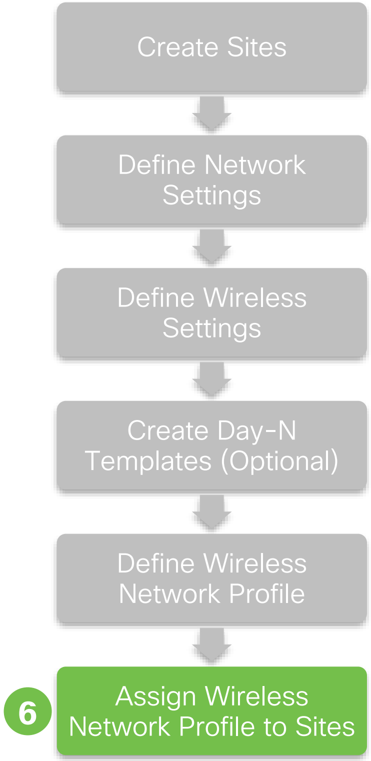
Wireless SSID

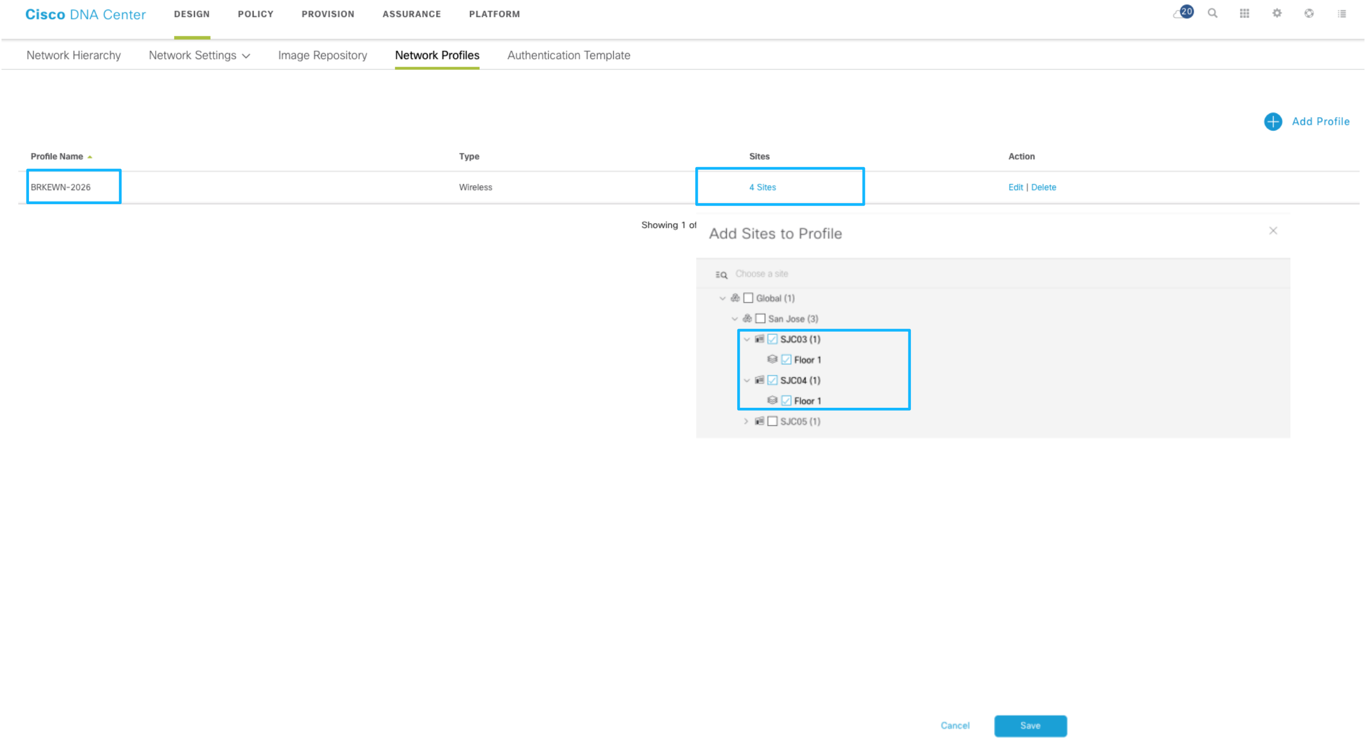
SSID	Type	Fabric	Traffic Switching
SSID BRKEWN-2026	Enterprise	○ Yes ● No	Interface Name Wireless-Data □ Flex Connect Local Switching

Attach Template(s)

Device Type	Device Tag	Template
Cisco Catalyst 9800-CL Wireless Controller for Cloud		Enable-CleanAir-Alarm

Design - Assign Wireless Network Profile to Sites


Create Sites
Define Network Settings
Define Wireless Settings
Create Day-N Templates (Optional)
Define Wireless Network Profile
6
Assign Wireless Network Profile to Sites



Profile Name	Type	Sites	Action
BRKEWN-2026	Wireless	4 Sites	Edit | Delete

Showing 1 of

Add Sites to Profile

Choose a site

- ☐ Global (1)
  - ☐ San Jose (3)
    - ☑ SJC03 (1)
      - ☑ Floor 1
    - ☑ SJC04 (1)
      - ☑ Floor 1
    - ☐ SJC05 (1)

Demo – Design

1. Create Wireless Profile with Enterprise SSID
2. Assign Wireless Profile to Site

What did we do so far?

Planned the Sites & Hierarchy

Extracted Common/Standard across Wired and Wireless to be self managed

Captured the business intent within a Network Profile

Provision

Plan

Design Network Services

Design Network Profile

Provision

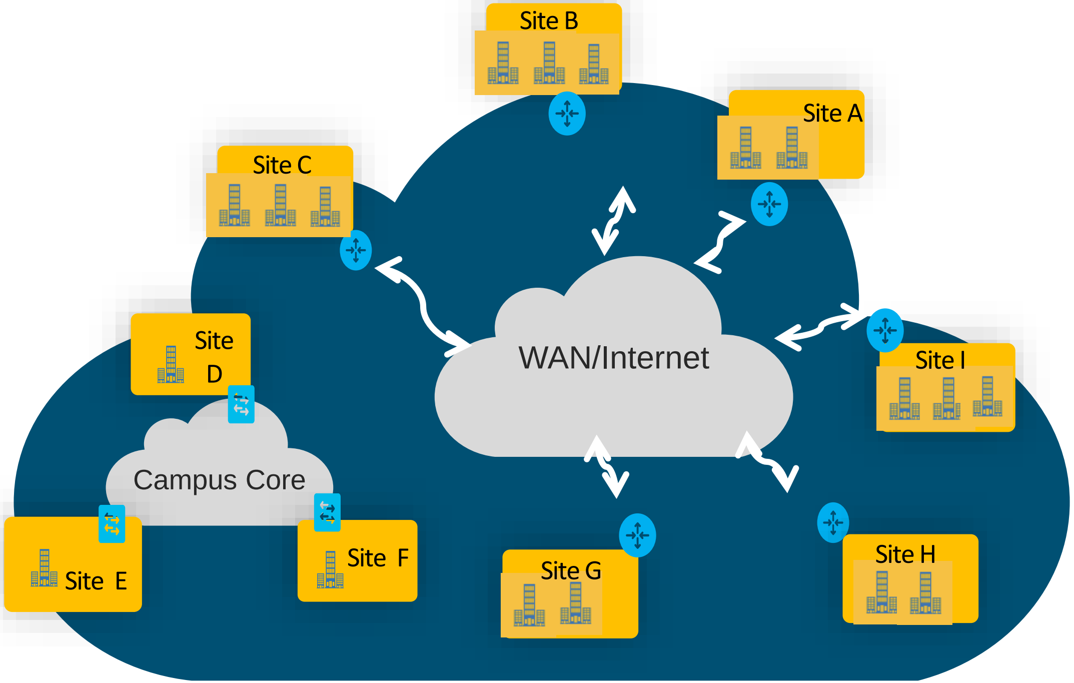
Scenario - Provision

Provision WLCs and APs

Cisco DNA Center

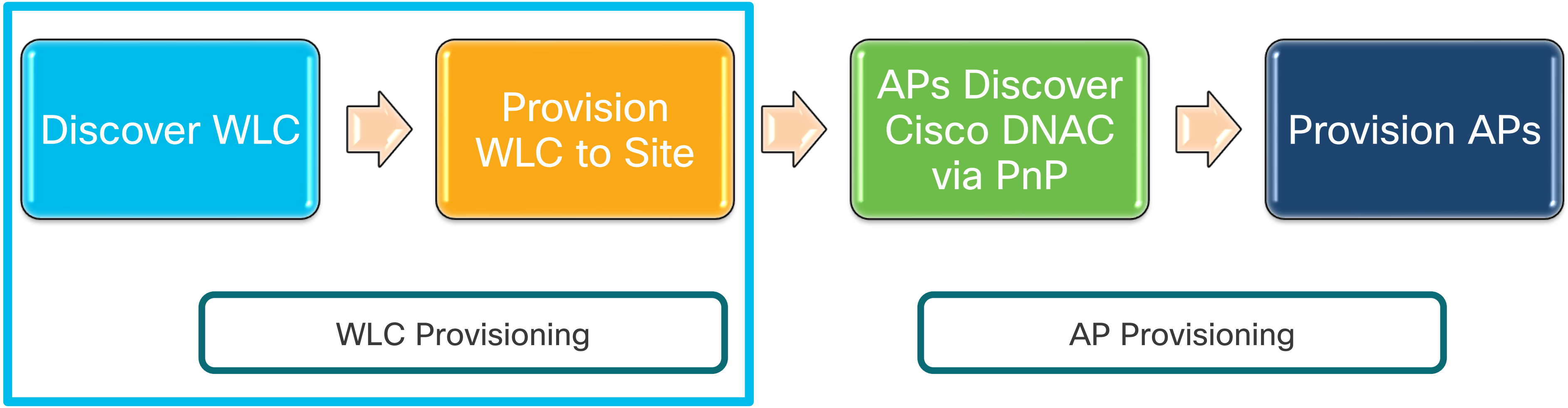
Wireless LAN controller

Access Points



Typical Customer Network

Provision Workflows



Discover WLC

Provision WLC to Site

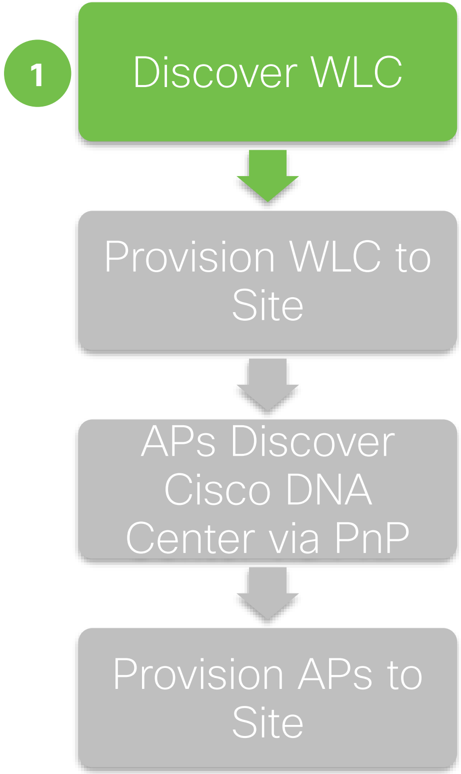
APs Discover Cisco DNAC via PnP

Provision APs

WLC Provisioning

AP Provisioning

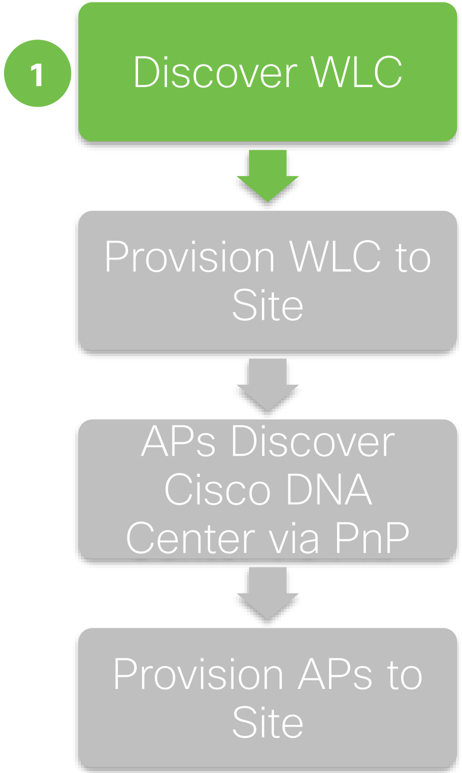
Provision – Discover WLC



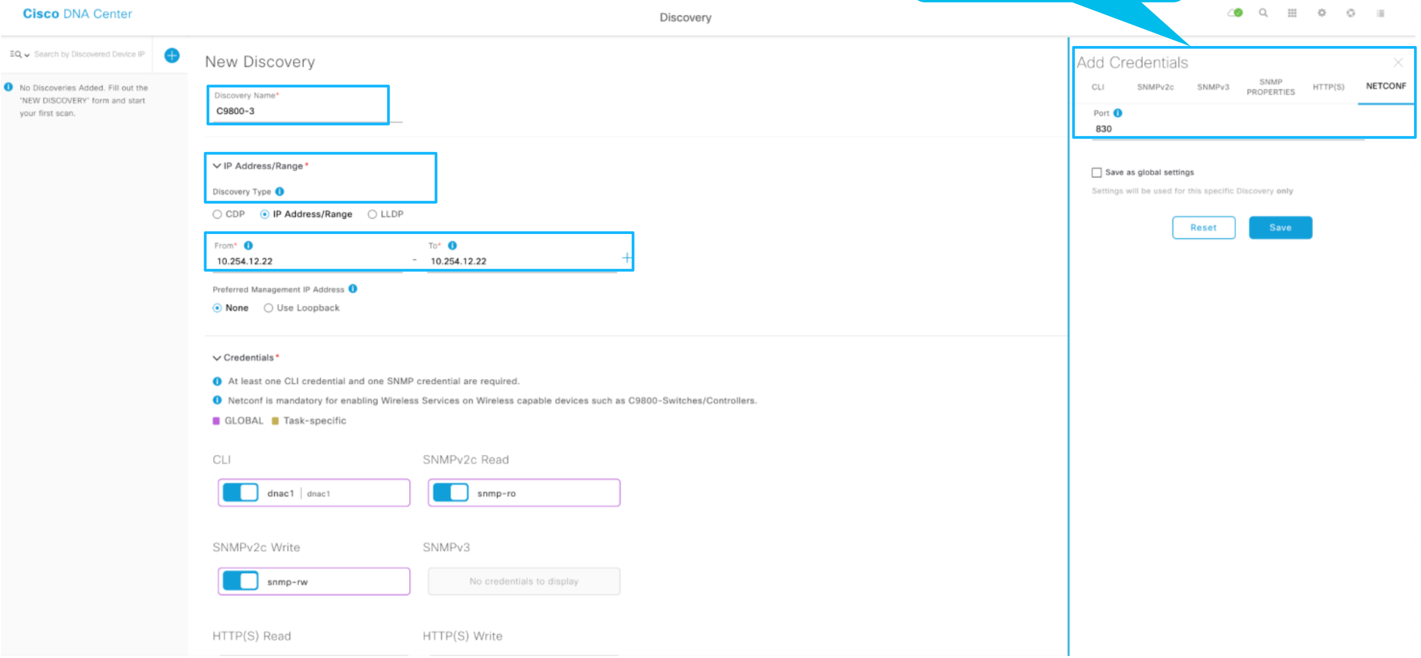
For C9800 Wireless Controller, minimum configuration required for successful discovery and management on Cisco DNA Center are as below:

- SSH and NETCONF are enabled
- CLI Login Credentials
- Wireless Management Interface

Provision - Discover WLC



Ensure NETCONF is enabled



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

New Discovery

Discovery Name*
C9800-3

IP Address/Range*

Discovery Type ⓘ
○ CDP ● IP Address/Range ○ LLDP

From* ⓘ 10.254.12.22 - To* ⓘ 10.254.12.22

Preferred Management IP Address ⓘ
● None ○ Use Loopback

Credentials*

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

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

🟪 GLOBAL 🟨 Task-specific

CLI: dnac1 | dnac1

SNMPv2c Read: snmp-ro

SNMPv2c Write: snmp-rw

SNMPv3: No credentials to display

HTTP(S) Read

HTTP(S) Write

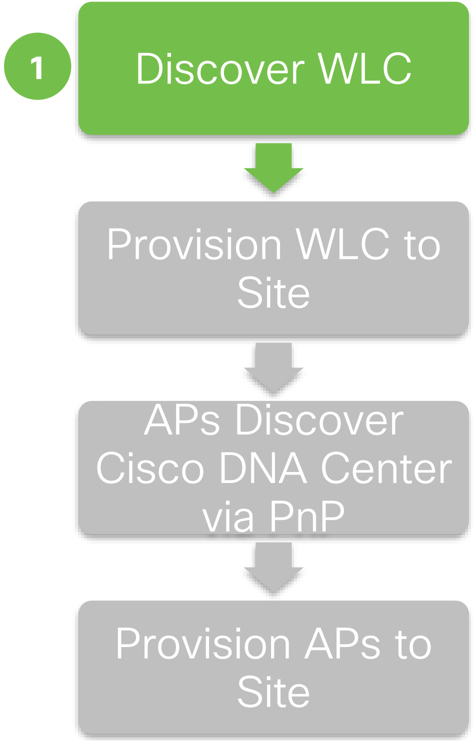
Add Credentials

Port ⓘ
830

□ Save as global settings

Settings will be used for this specific Discovery only

Provision - Discover WLC



1 Discover WLC

Provision WLC to Site

APs Discover Cisco DNA Center via PnP

Provision APs to Site

The following configuration is added to Cat9800 after discovery:

- Install multiple certificates:
    - Cisco DNA Center device certificate issuing ca, sd-network-infra-iwan
    - Enroll device certificate of Cat9800 to sdn-network-infra-iwan for assurance
    - Cisco DNA Center server certificate and its issuing ca certificate
    - Cisco smart licensing agent root CA
    - Generate self-signed certificate named “ewlc-tp1” for AP joining
- SSH/HTTP source interface from management SVI/IP
- Enable network assurance telemetry

Provision - N+1 HA WLCs

Supported HA Deployment Models:

- 1:1 HA from 1.1 release.
- N+1 from 1.3 release.

Challenges in N+1 HA Deployment Models :

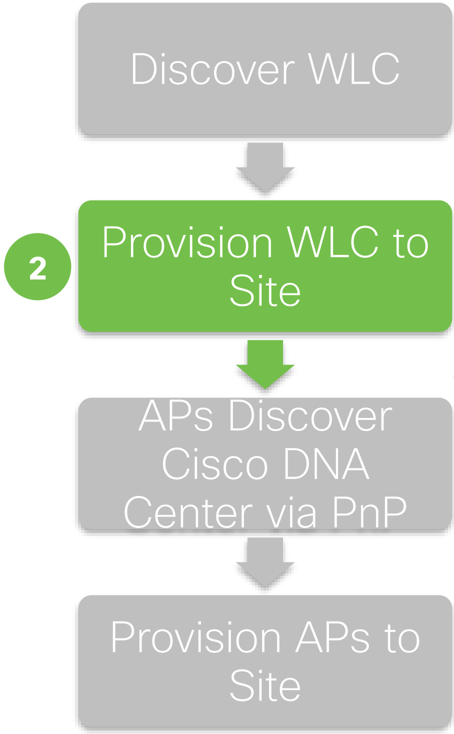
- Ensure primary and secondary WLCs' configuration in sync.
- Ensure APs are provisioned with correct primary and secondary WLCs.

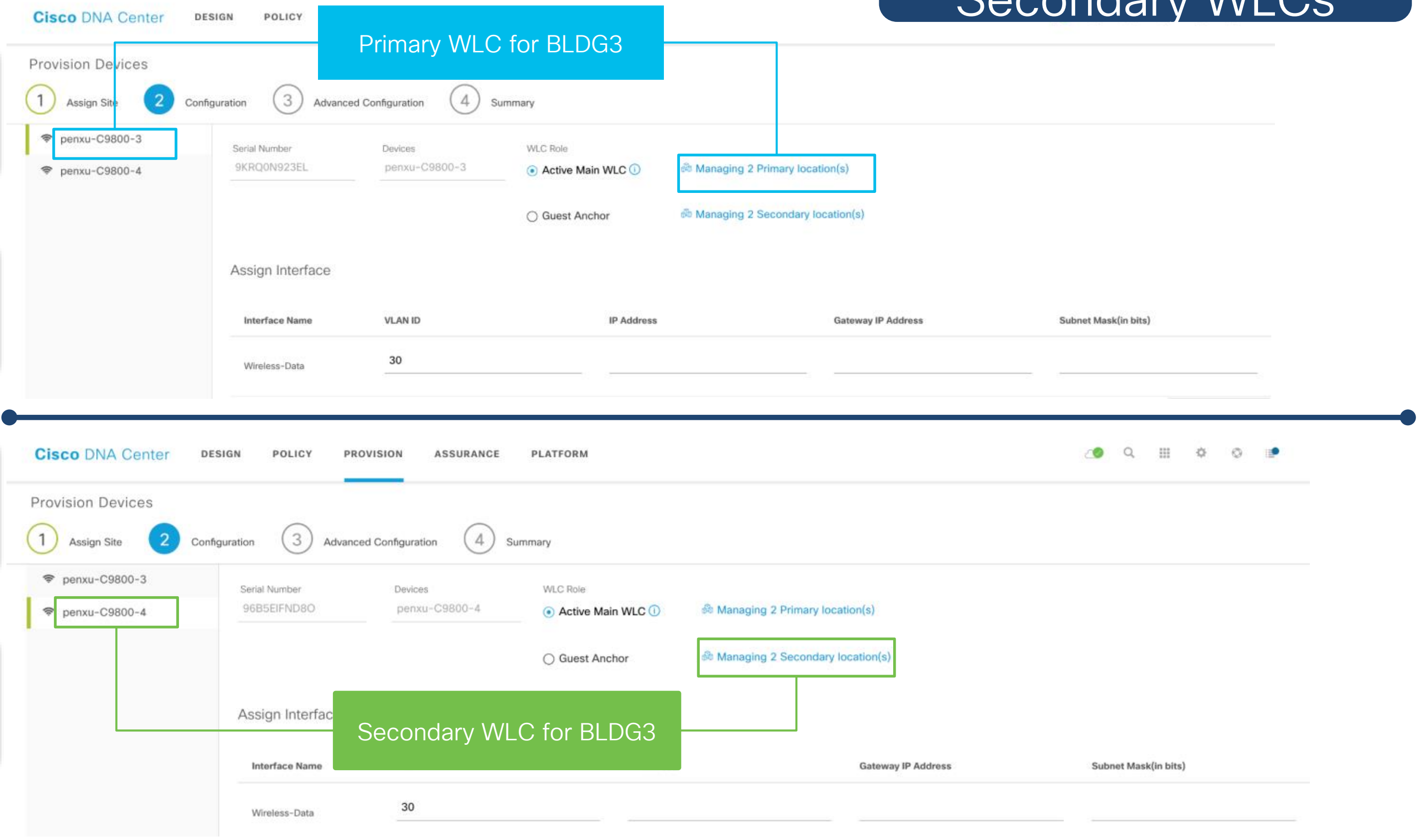
Provision - N+1 HA WLCs

- The same wireless profile is applied to both primary and secondary WLCs.
- “Secondary Managed AP Locations” concept is introduced during WLC provision in 1.3.
- WLC that assigned to be sites with “Secondary Managed AP Locations” acts as secondary WLC for all APs on that site.
- Can not provision secondary WLC to a site if there is no primary WLC assigned to it.
- Claiming APs to a site will provision APs with primary and secondary WLC automatically.

Provision - Provision WLC to Site

Define Primary and Secondary WLCs





Cisco DNA Center DESIGN POLICY

Provision Devices

1 Assign Site 2 Configuration 3 Advanced Configuration 4 Summary

- penxu-C9800-3
- penxu-C9800-4

Serial Number: 9KRQON923EL

Devices: penxu-C9800-3

WLC Role: ● Active Main WLC ⓘ ○ Guest Anchor

Managing 2 Primary location(s)

Managing 2 Secondary location(s)

Assign Interface

Interface Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
Wireless-Data	30			

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Provision Devices

1 Assign Site 2 Configuration 3 Advanced Configuration 4 Summary

- penxu-C9800-3
- penxu-C9800-4

Serial Number: 96B5EIFND8O

Devices: penxu-C9800-4

WLC Role: ● Active Main WLC ⓘ ○ Guest Anchor

Managing 2 Primary location(s)

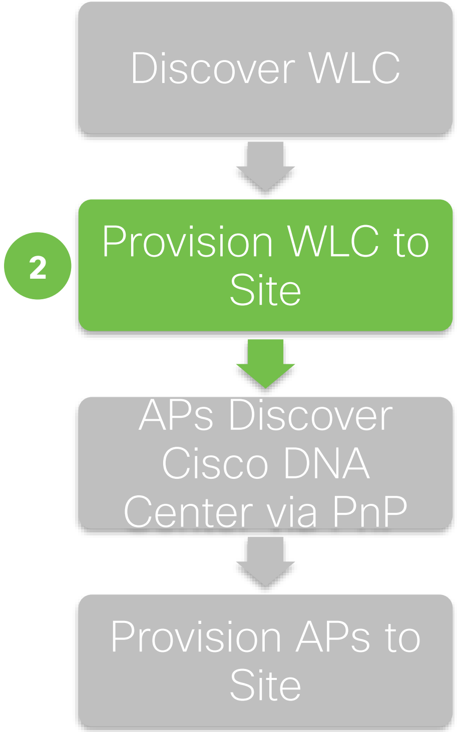
Managing 2 Secondary location(s)

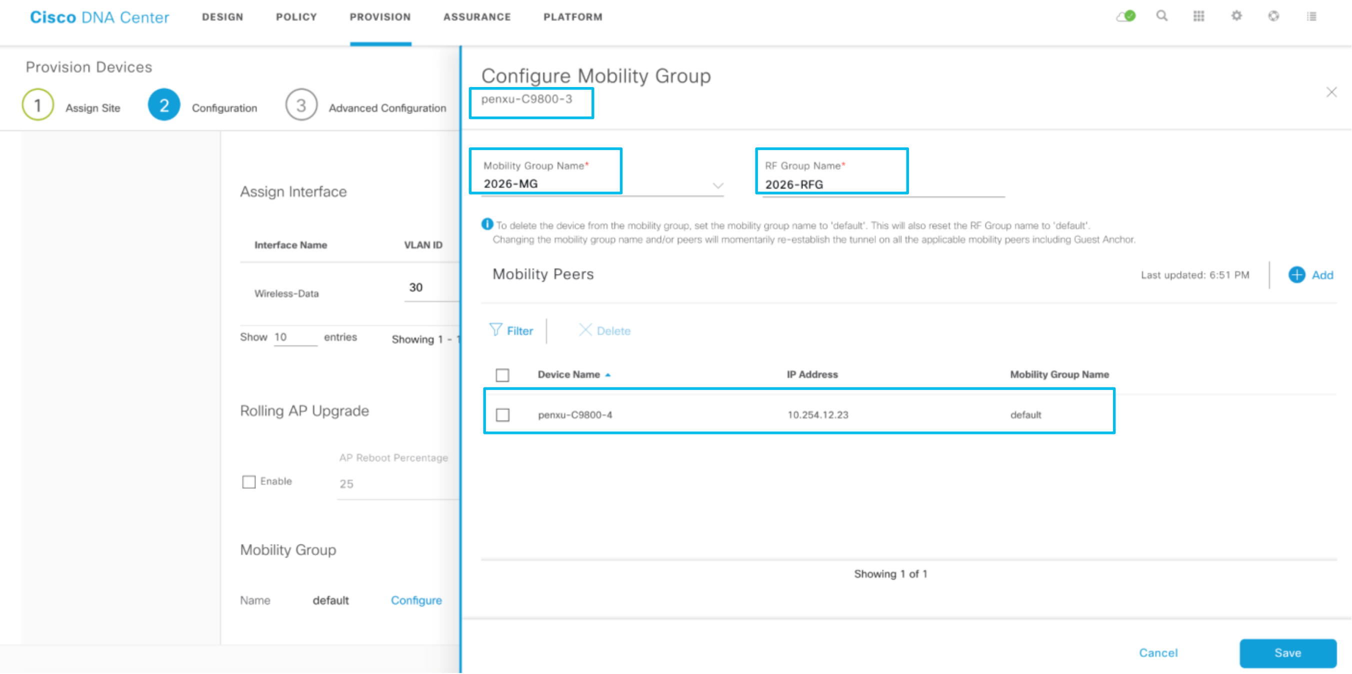
Assign Interface

Interface Name		Gateway IP Address	Subnet Mask(in bits)
Wireless-Data	30		

Provision - Provision WLC to Site

Define Mobility, RF Groups





Provision Devices

1 Assign Site 2 Configuration 3 Advanced Configuration

Assign Interface

Interface Name	VLAN ID
Wireless-Data	30

Show 10 entries Showing 1 - 1

Rolling AP Upgrade

□ Enable AP Reboot Percentage 25

Mobility Group

Name default Configure

Configure Mobility Group

penxu-C9800-3

Mobility Group Name* 2026-MG

RF Group Name* 2026-RFG

To delete the device from the mobility group, set the mobility group name to 'default'. This will also reset the RF Group name to 'default'. Changing the mobility group name and/or peers will momentarily re-establish the tunnel on all the applicable mobility peers including Guest Anchor.

Mobility Peers Last updated: 6:51 PM Add

Filter Delete

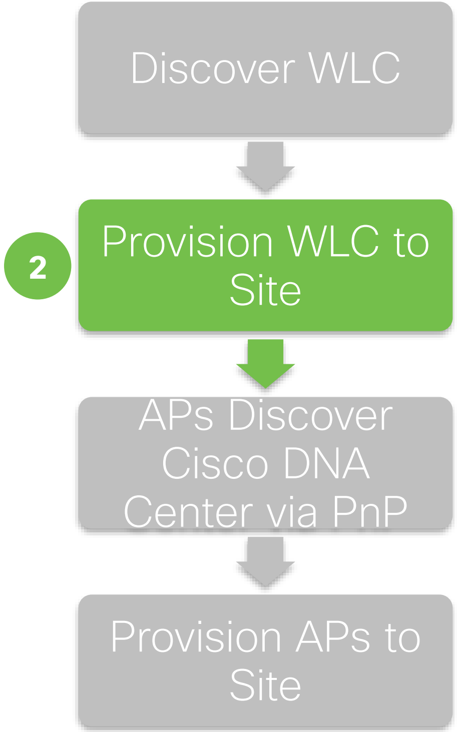
□	Device Name	IP Address	Mobility Group Name
□	penxu-C9800-4	10.254.12.23	default

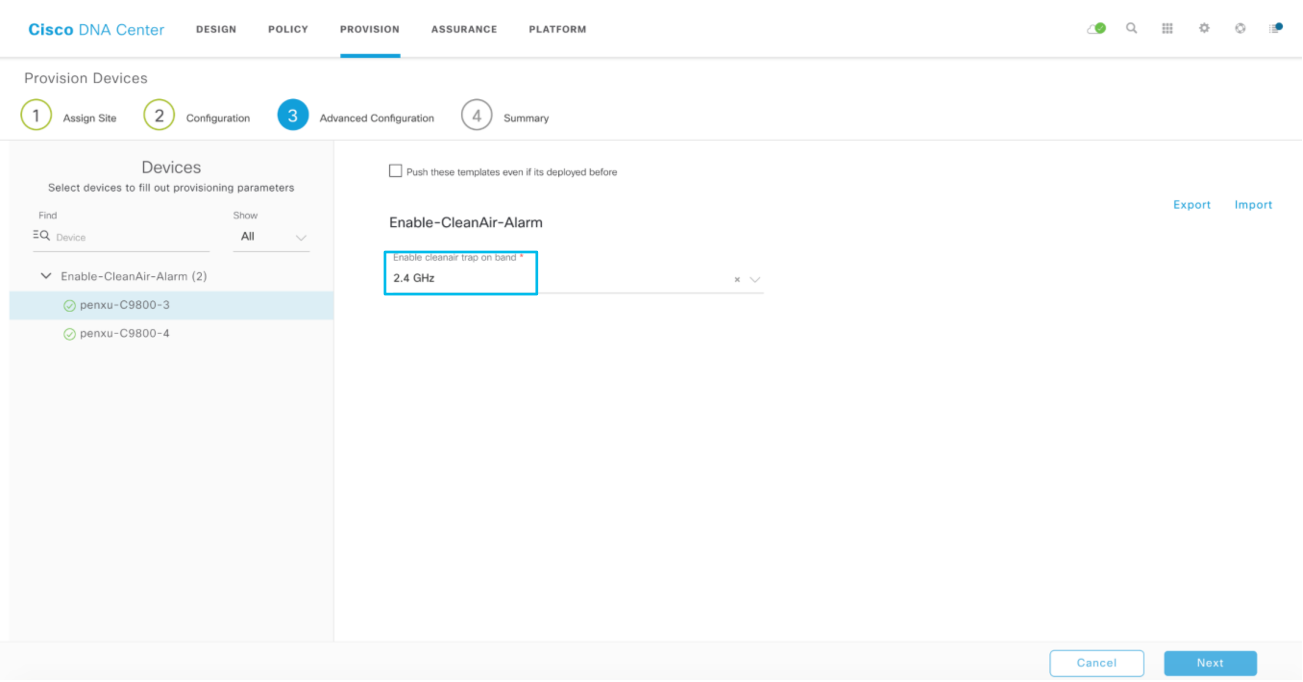
Showing 1 of 1

Cancel Save

Note that you only need to define mobility and RF groups, and mobility peers on primary WLC. Cisco DNA Center will configure mobility peering automatically between mobility peers. Also set the same mobility and RF groups between them.

Provision - Provision WLC to Site





Provision Devices

1 Assign Site 2 Configuration 3 Advanced Configuration 4 Summary

Devices

Select devices to fill out provisioning parameters

Find: Device Show: All

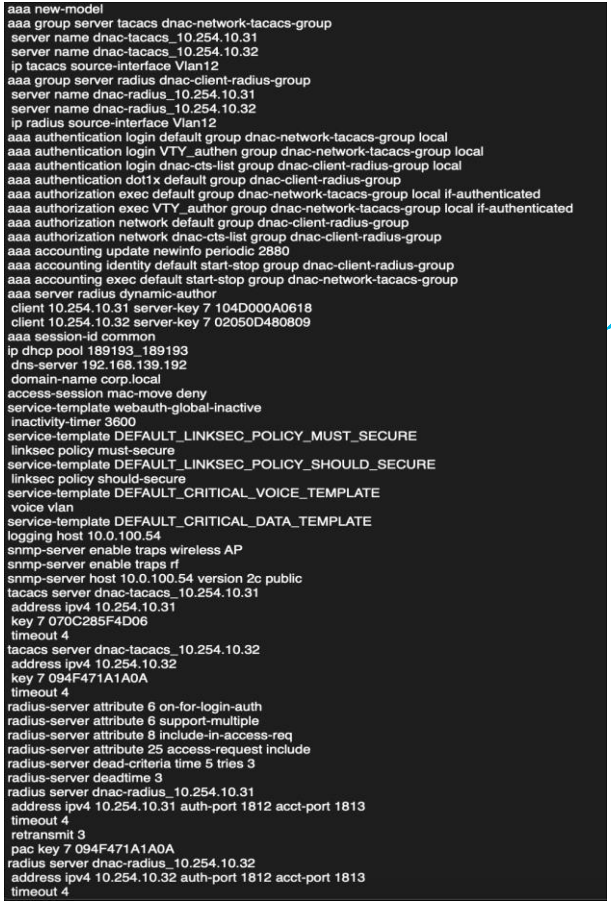
Enable-CleanAir-Alarm (2)
- penxu-C9800-3
- penxu-C9800-4

□ Push these templates even if its deployed before

Enable-CleanAir-Alarm

Enable cleanair trap on band *: 2.4 GHz

Provision - Provision WLC to Site

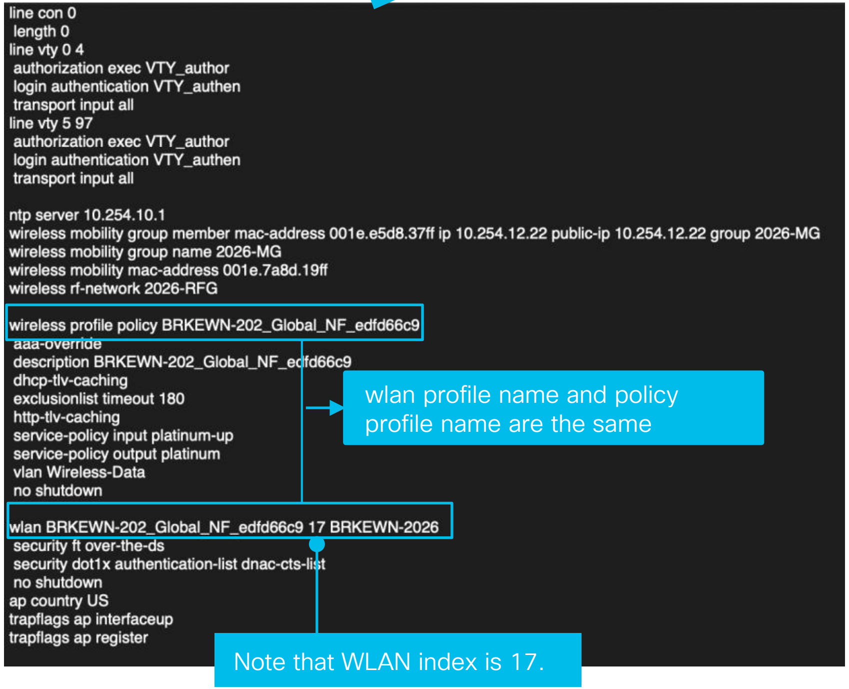


```
aaa new-model
aaa group server tacacs dnac-network-tacacs-group
 server name dnac-tacacs_10.254.10.31
 server name dnac-tacacs_10.254.10.32
 ip tacacs source-interface Vlan12
aaa group server radius dnac-client-radius-group
 server name dnac-radius_10.254.10.31
 server name dnac-radius_10.254.10.32
 ip radius source-interface Vlan12
aaa authentication login default group dnac-network-tacacs-group local
aaa authentication login VTY_authen group dnac-network-tacacs-group local
aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authentication dot1x default group dnac-client-radius-group
aaa authorization exec default group dnac-network-tacacs-group local if-authenticated
aaa authorization exec VTY_author group dnac-network-tacacs-group local if-authenticated
aaa authorization network default group dnac-client-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa accounting update newinfo periodic 2880
aaa accounting identity default start-stop group dnac-client-radius-group
aaa accounting exec default start-stop group dnac-network-tacacs-group
aaa server radius dynamic-author
 client 10.254.10.31 server-key 7 104D000A0618
 client 10.254.10.32 server-key 7 02050D480809
aaa session-id common
ip dhcp pool 189193_189193
 dns-server 192.168.139.192
 domain-name corp.local
access-session mac-move deny
service-template webauth-global-inactive
 inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
 linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
 linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
logging host 10.0.100.54
snmp-server enable traps wireless AP
snmp-server enable traps rf
snmp-server host 10.0.100.54 version 2c public
tacacs server dnac-tacacs_10.254.10.31
 address ipv4 10.254.10.31
 key 7 070C285F4D06
 timeout 4
tacacs server dnac-tacacs_10.254.10.32
 address ipv4 10.254.10.32
 key 7 094F471A1A0A
 timeout 4
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
radius server dnac-radius_10.254.10.31
 address ipv4 10.254.10.31 auth-port 1812 acct-port 1813
 timeout 4
 retransmit 3
 pac key 7 094F471A1A0A
radius server dnac-radius_10.254.10.32
 address ipv4 10.254.10.32 auth-port 1812 acct-port 1813
 timeout 4
```

- Network Settings: TACACS, Radius, SNMP, Syslog, DHCP, DNS, NTP and etc.

On C9800 Wireless Controller

- Country Code
- WLAN and Policy Profiles
- Mobility and RF Groups



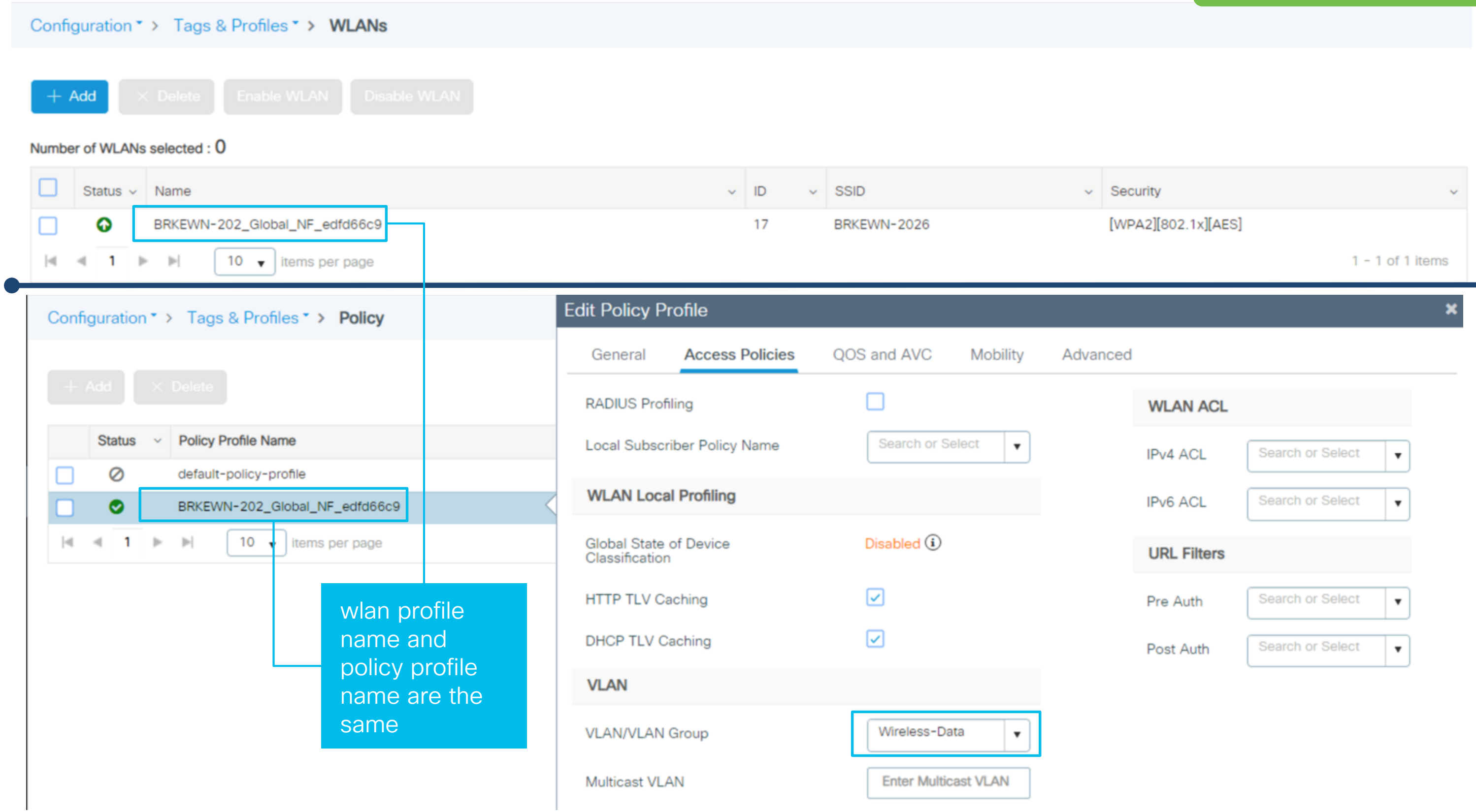
```
line con 0
 length 0
line vty 0 4
 authorization exec VTY_author
 login authentication VTY_authen
 transport input all
line vty 5 97
 authorization exec VTY_author
 login authentication VTY_authen
 transport input all

ntp server 10.254.10.1
wireless mobility group member mac-address 001e.e5d8.37ff ip 10.254.12.22 public-ip 10.254.12.22 group 2026-MG
wireless mobility group name 2026-MG
wireless mobility mac-address 001e.7a8d.19ff
wireless rf-network 2026-RFG

wireless profile policy BRKEWN-202_Global_NF_edfd66c9
 aaa-override
 description BRKEWN-202_Global_NF_edfd66c9
 dhcp-tlv-caching
 exclusionlist timeout 180
 http-tlv-caching
 service-policy input platinum-up
 service-policy output platinum
 vlan Wireless-Data
 no shutdown

wlan BRKEWN-202_Global_NF_edfd66c9 17 BRKEWN-2026
 security ft over-the-ds
 security dot1x authentication-list dnac-cts-list
 no shutdown
ap country US
trapflags ap interfaceup
trapflags ap register
```

wlan profile name and policy profile name are the same

Note that WLAN index is 17.

Provision - Provision WLC to Site

On C9800 Wireless Controller



Configuration ▾ > Tags & Profiles ▾ > **WLANs**

Number of WLANs selected : 0

☐	Status	Name	ID	SSID	Security
☐	⬆	BRKEWN-202_Global_NF_edfd66c9	17	BRKEWN-2026	[WPA2][802.1x][AES]

1 | 10 items per page | 1 - 1 of 1 items

Configuration ▾ > Tags & Profiles ▾ > **Policy**

☐	Status	Policy Profile Name
☐	⊘	default-policy-profile
☐	✓	BRKEWN-202_Global_NF_edfd66c9

1 | 10 items per page

Edit Policy Profile

RADIUS Profiling ☐

Local Subscriber Policy Name: Search or Select

WLAN Local Profiling

Global State of Device Classification: Disabled ⓘ

HTTP TLV Caching ☑

DHCP TLV Caching ☑

VLAN

VLAN/VLAN Group: Wireless-Data

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

URL Filters

Pre Auth: Search or Select

Post Auth: Search or Select

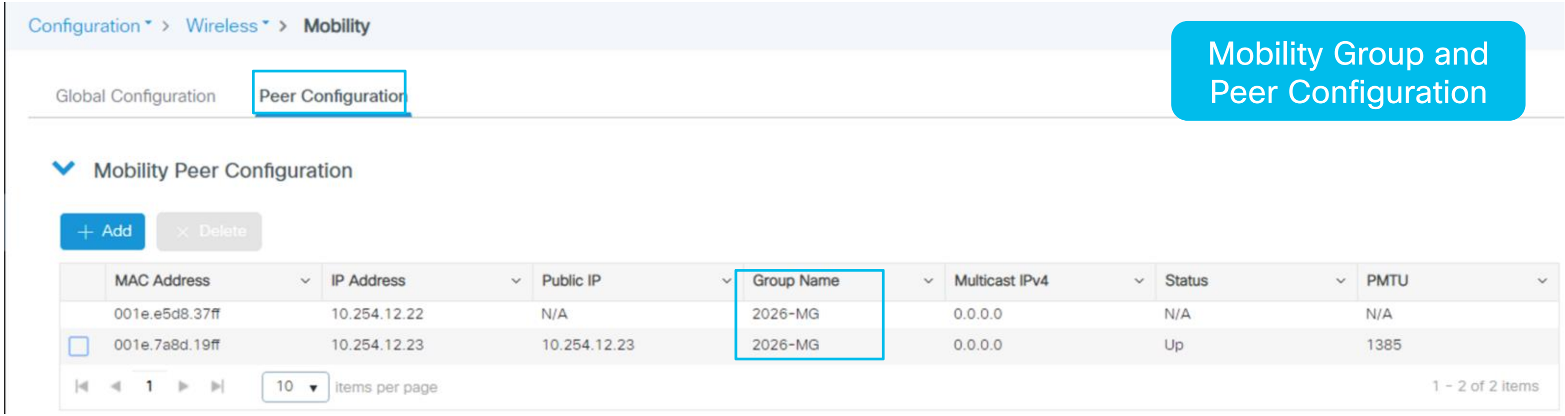
WLAN Profile

Policy Profile

wlan profile name and policy profile name are the same

Provision - Provision WLC to Site

On C9800 Wireless Controller



Configuration > Wireless > Mobility

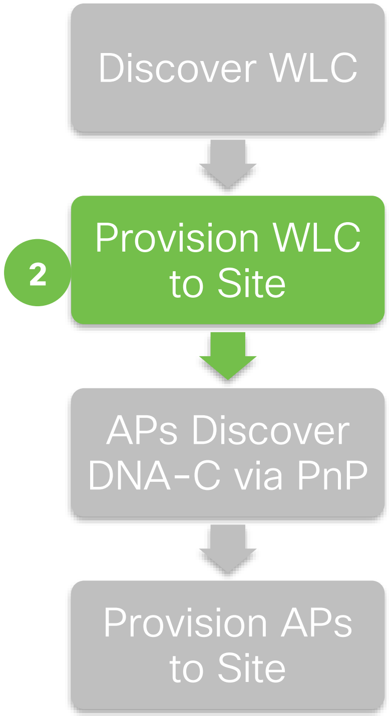
Global Configuration | Peer Configuration

Mobility Peer Configuration

	MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Status	PMTU
	001e.e5d8.37ff	10.254.12.22	N/A	2026-MG	0.0.0.0	N/A	N/A
□	001e.7a8d.19ff	10.254.12.23	10.254.12.23	2026-MG	0.0.0.0	Up	1385

Mobility Group and Peer Configuration

Provision - Provision WLC to Site

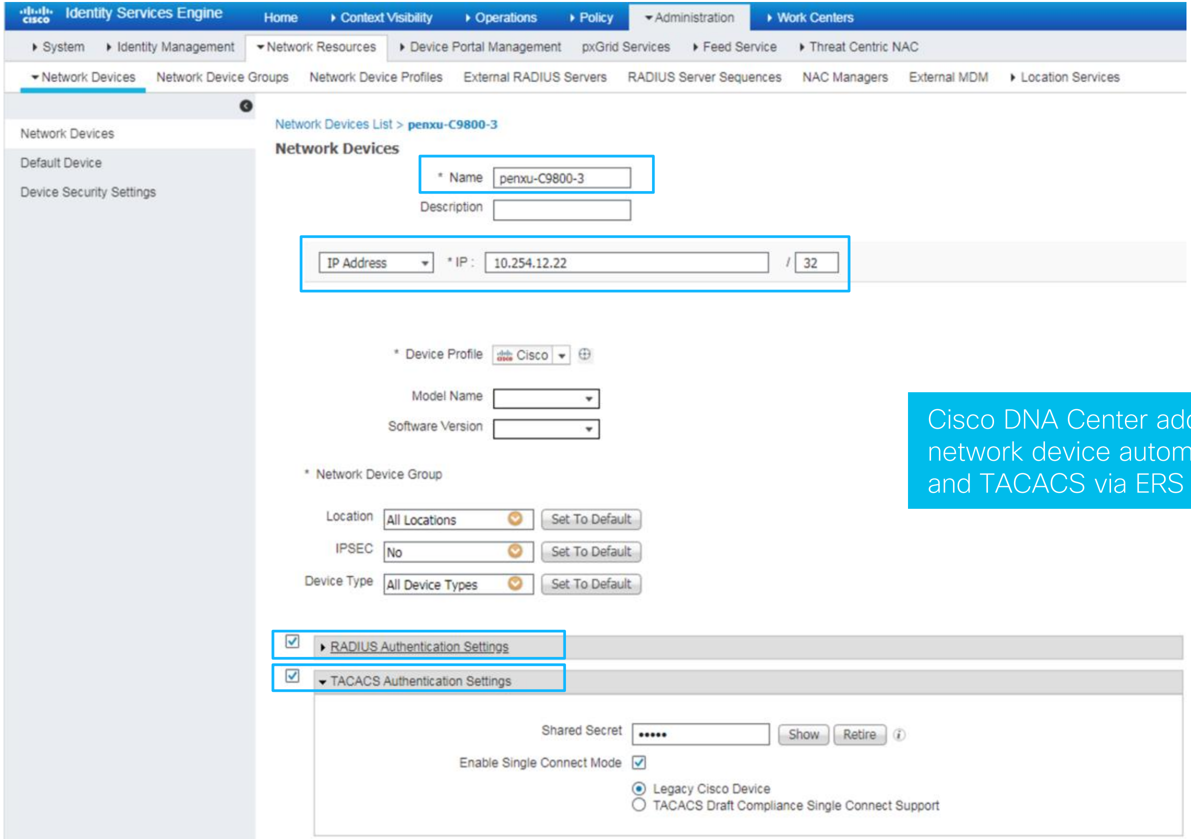


Discover WLC

2 Provision WLC to Site

APs Discover DNA-C via PnP

Provision APs to Site



Network Devices List > **penxu-C9800-3**

Network Devices

* Name: penxu-C9800-3

Description:

IP Address * IP : 10.254.12.22 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret: ••••• Show Retire

Enable Single Connect Mode ☑

● Legacy Cisco Device

○ TACACS Draft Compliance Single Connect Support

On ISE

Cisco DNA Center add WLC into ISE as network device automatically for Radius and TACACS via ERS API.

Demo- WLC Provisioning

What did we do so far?

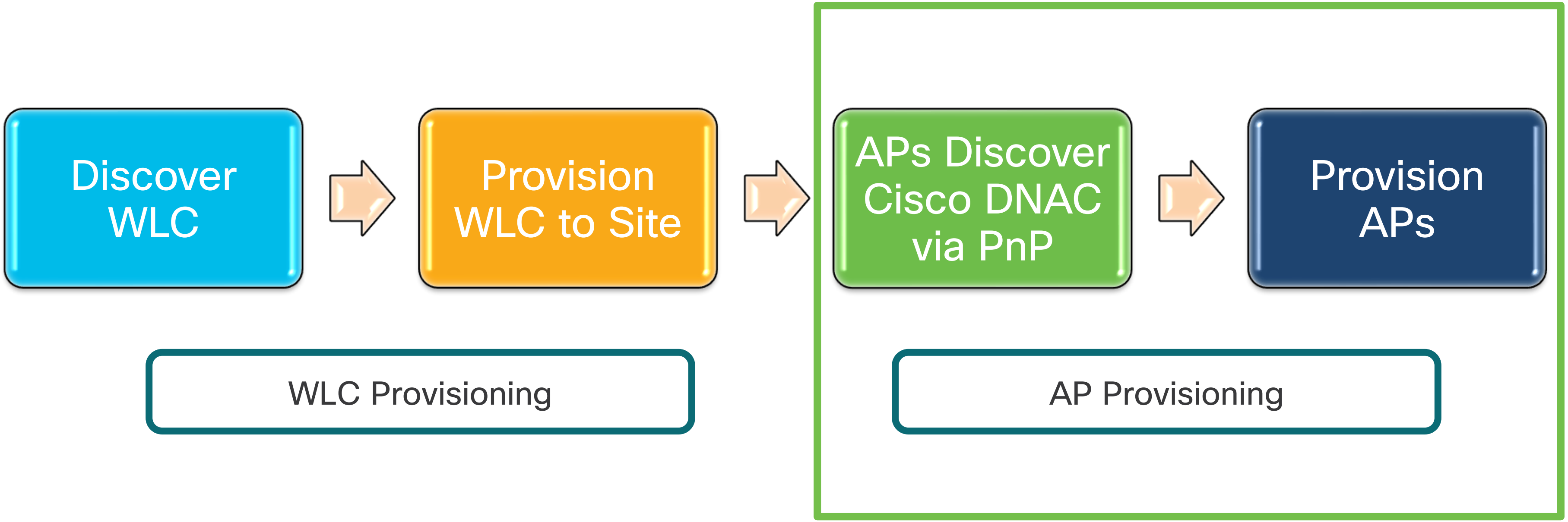
Planned the Sites & Hierarchy

Extracted Common/Standard across Wired and Wireless to be self managed

Captured the business intent within a Network Profile

Converting Business Intent to Network Policy – WLC Provisioning

Provision Workflows


Discover WLC

Provision WLC to Site

APs Discover Cisco DNAC via PnP

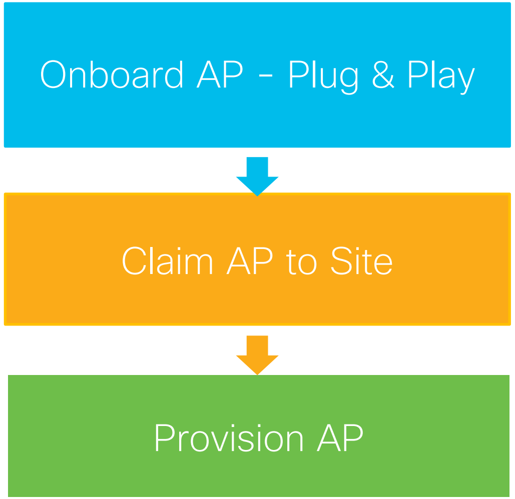
Provision APs

WLC Provisioning

AP Provisioning

Provision Workflow - AP

Option 1- Unclaimed Workflow

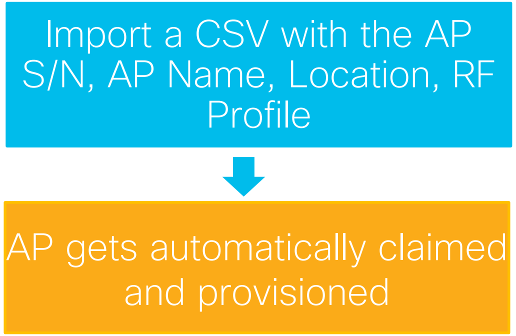

Onboard AP - Plug & Play

Claim AP to Site

Provision AP

More Control on AP Provisioning

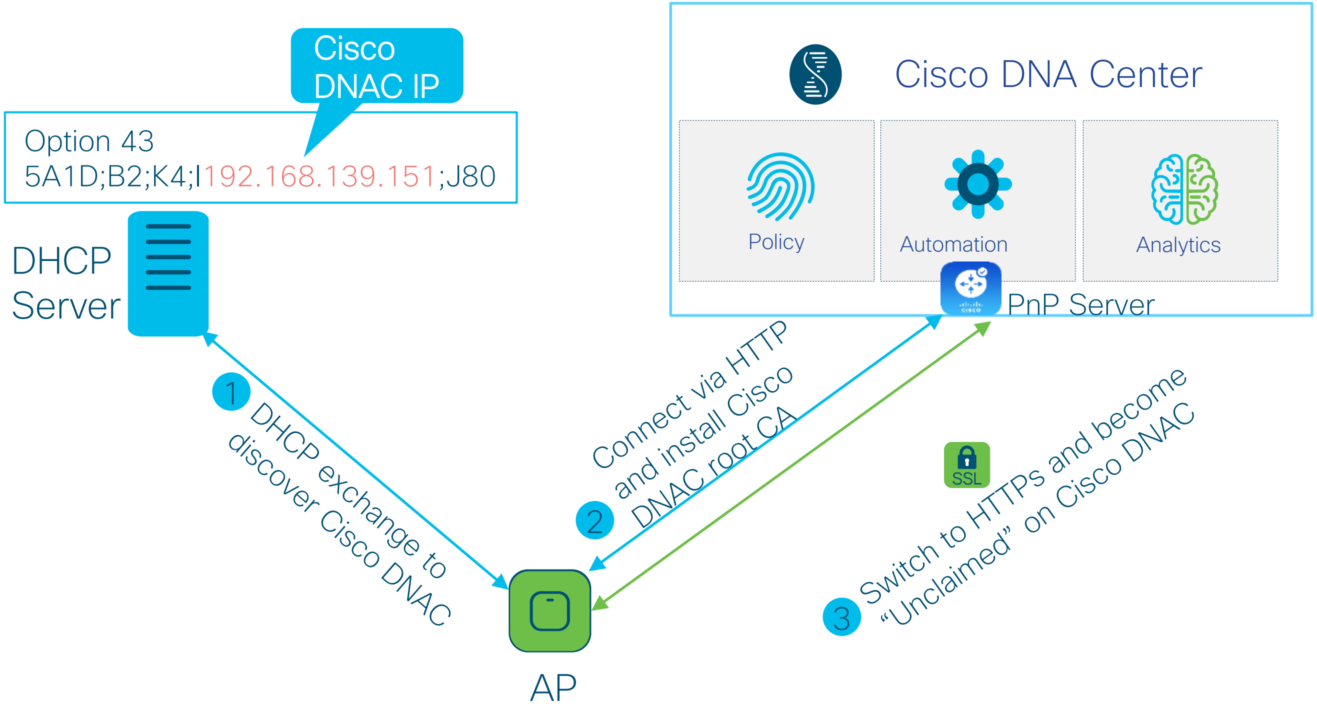
Option - 2


Import a CSV with the AP S/N, AP Name, Location, RF Profile

AP gets automatically claimed and provisioned

Pre-Provisioning/Planned

Provision Workflow – AP PnP Discovery



Cisco DNAC IP

Option 43
5A1D;B2;K4;I192.168.139.151;J80

DHCP Server
Cisco DNA Center
Policy
Automation
Analytics
PnP Server
1 DHCP exchange to discover Cisco DNAC
2 Connect via HTTP and install Cisco DNAC root CA
3 Switch to HTTPs and become "Unclaimed" on Cisco DNAC
SSL
AP

PnP Server Discovery Options

Automated

1 DHCP with option 43

PnP string: 5A1D;B2;K4;I172.19.45.222;J80 added to DHCP Server

2 DNS lookup

pnpserver.localdomain resolves to DNA Center IP Address

3 Cloud re-direction https://devicehelper.cisco.com/device-helper

Cisco hosted cloud, re-directs to on-prem DNA Center IP Address

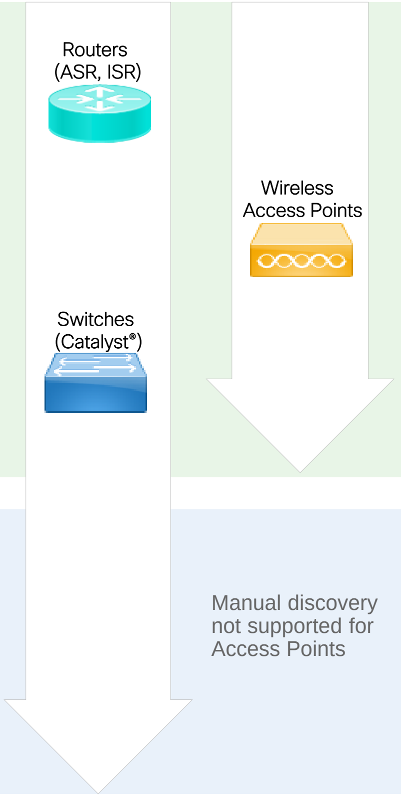
Manual

4 USB-based bootstrapping*

router-confg/router.cfg/ciscortr.cfg

5 Manual - using the Cisco® Installer App**

iPhone, iPad, Android

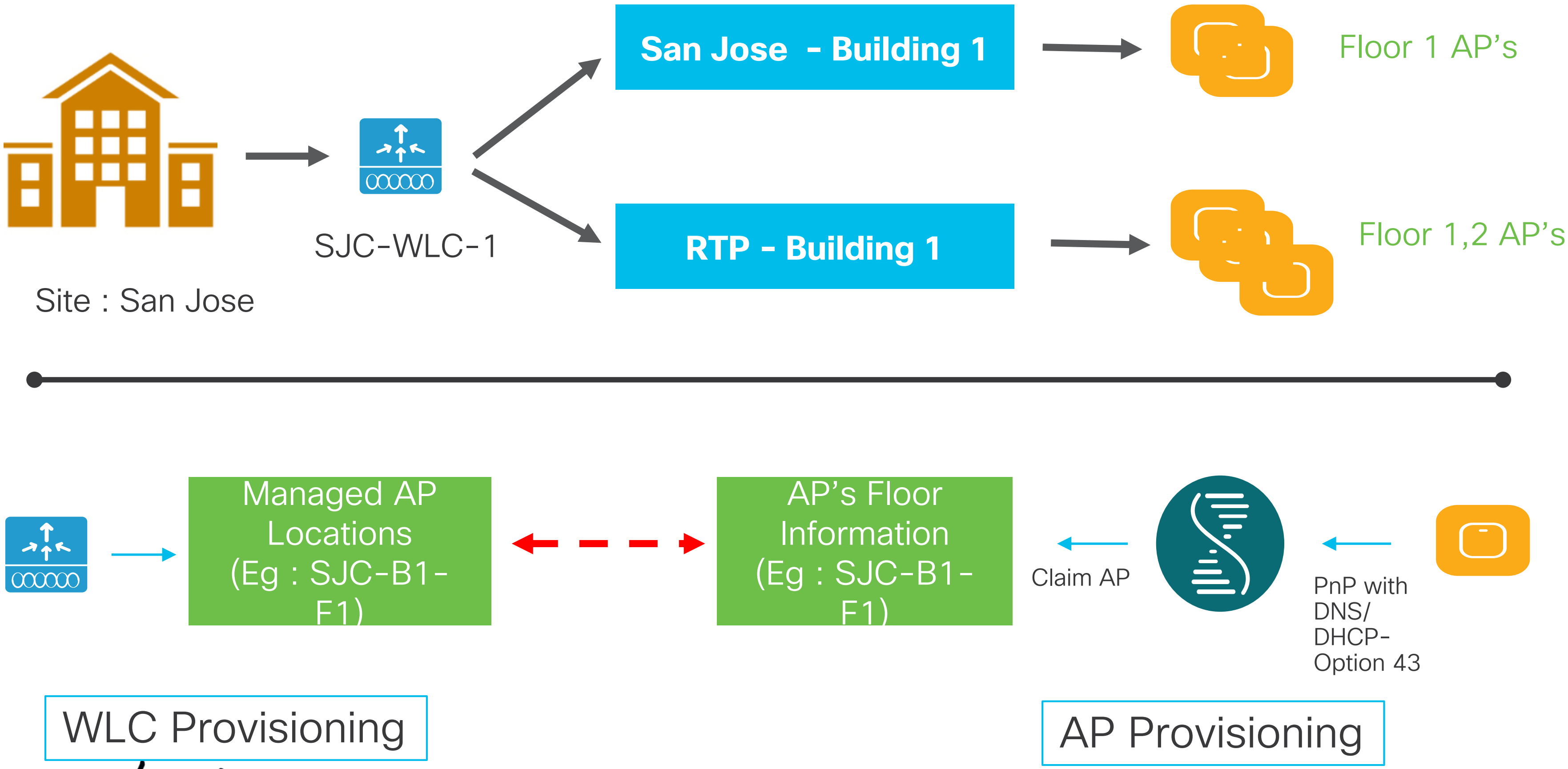


Manual discovery not supported for Access Points

*Supported on Cat 9K only for switches

* *DNA Center Support in Roadmap

How did the APs find their WLC?



Site : San Jose

SJC-WLC-1

San Jose - Building 1

RTP - Building 1

Floor 1 AP's

Floor 1,2 AP's

Managed AP Locations (Eg : SJC-B1-F1)

AP's Floor Information (Eg : SJC-B1-F1)

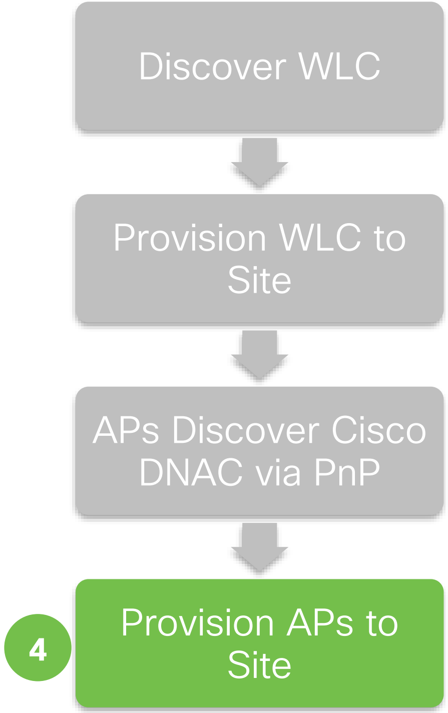
Claim AP

PnP with DNS/ DHCP-Option 43

WLC Provisioning

AP Provisioning

Provision- Provision APs to Site



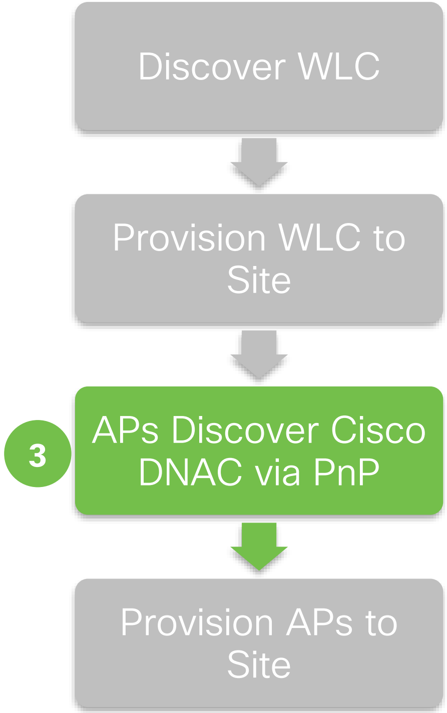
Option –1

What will be provisioned?

- On APs (via PnP):
  - AP Hostname
  - Primary and Secondary WLCs' Hostnames
  - Primary and Secondary WLCs' IPs
  - Policy, Site and RF Tags if WLC is C9800s
- On C9800 WLC (via NETCONF and CLI):
  - Create RF Profile if applicable
  - Create Wireless Flex Profile if applicable
  - Create Policy, Site and RF tags
  - Assign AP mode with corresponding policy, site and RF tags

Provision- Provision APs to Site

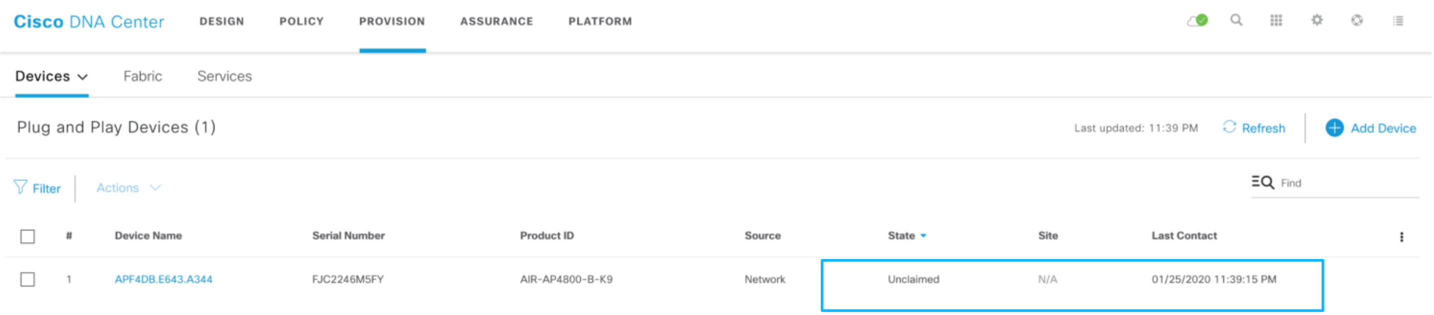
Option -1


Discover WLC

Provision WLC to Site

3 APs Discover Cisco DNAC via PnP

Provision APs to Site

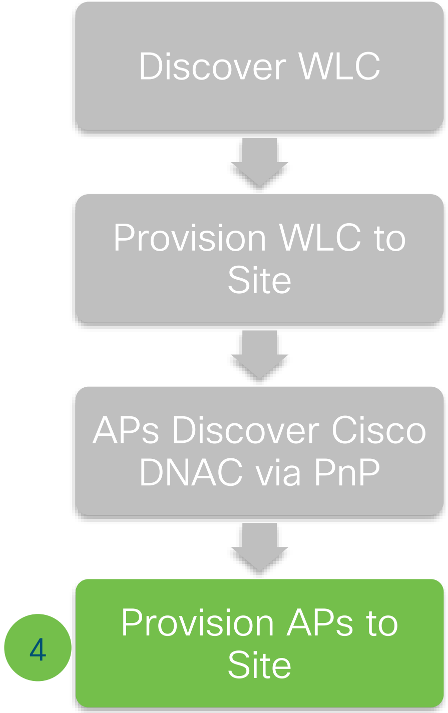


Plug and Play Devices (1)

Last updated: 11:39 PM

☐	#	Device Name	Serial Number	Product ID	Source	State	Site	Last Contact
☐	1	APF4DB.E643.A344	FJC2246M5FY	AIR-AP4800-B-K9	Network	Unclaimed	N/A	01/25/2020 11:39:15 PM

Provision- Provision APs to Site

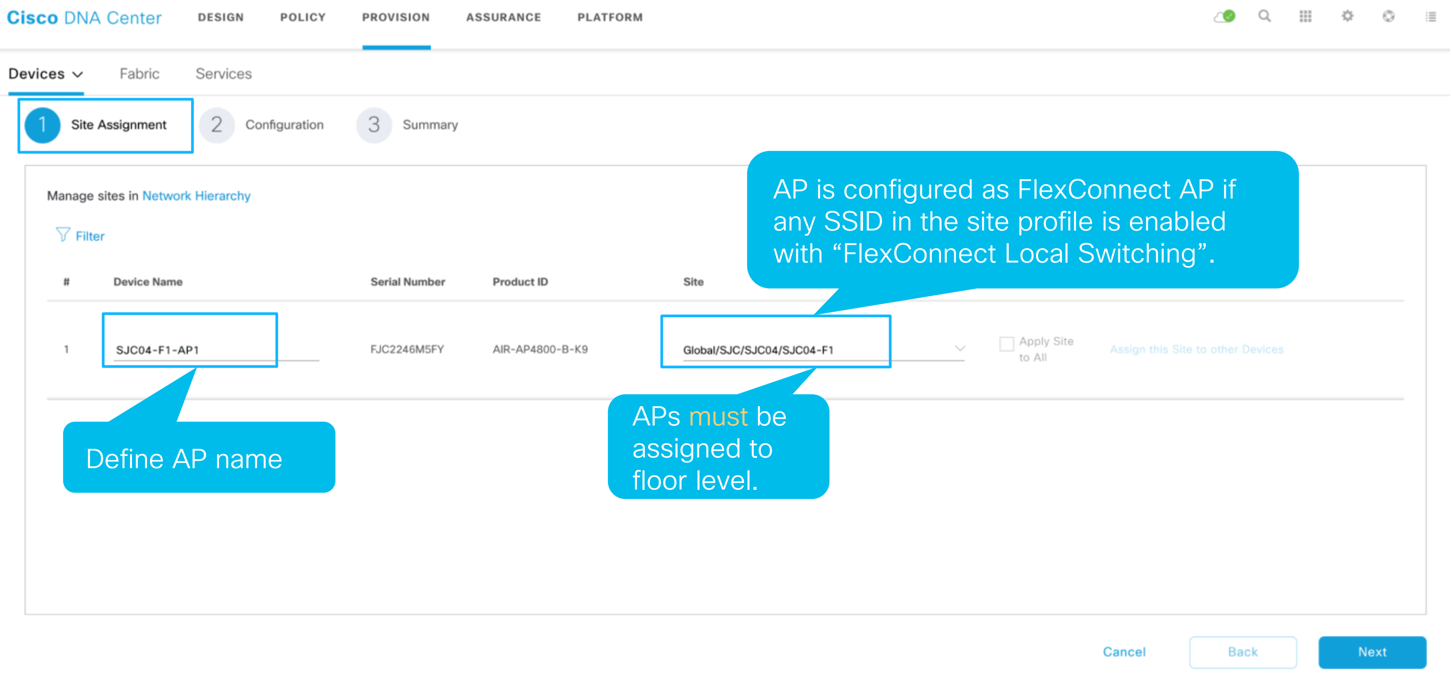

Discover WLC

Provision WLC to Site

APs Discover Cisco DNAC via PnP

4 Provision APs to Site

Option -1



Manage sites in Network Hierarchy

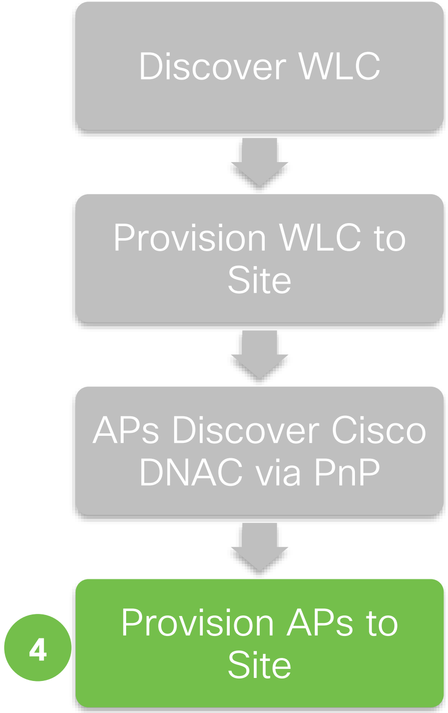
#	Device Name	Serial Number	Product ID	Site		
1	SJC04-F1-AP1	FJC2246M5FY	AIR-AP4800-B-K9	Global/SJC/SJC04/SJC04-F1	□ Apply Site to All	Assign this Site to other Devices

AP is configured as FlexConnect AP if any SSID in the site profile is enabled with “FlexConnect Local Switching”.

Define AP name

APs must be assigned to floor level.

Provision- Provision APs to Site



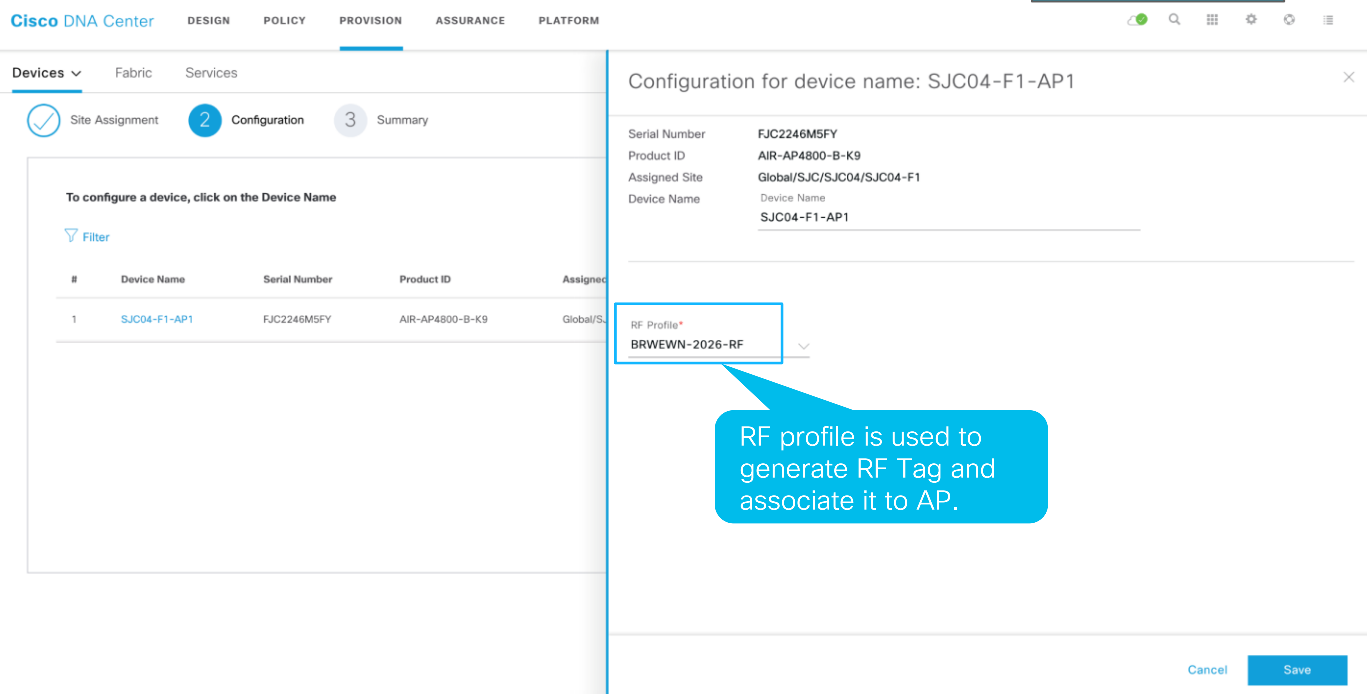
Discover WLC

Provision WLC to Site

APs Discover Cisco DNAC via PnP

4 Provision APs to Site

Option -1



To configure a device, click on the Device Name

#	Device Name	Serial Number	Product ID	Assigned
1	SJC04-F1-AP1	FJC2246M5FY	AIR-AP4800-B-K9	Global/S…

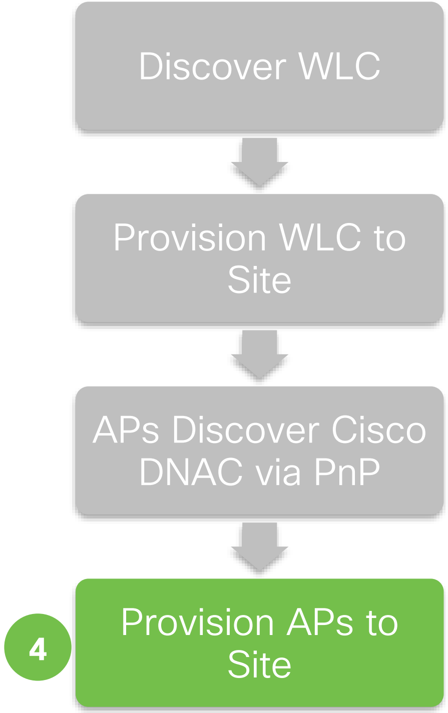
Configuration for device name: SJC04-F1-AP1

Serial Number	FJC2246M5FY
Product ID	AIR-AP4800-B-K9
Assigned Site	Global/SJC/SJC04/SJC04-F1
Device Name	Device Name SJC04-F1-AP1

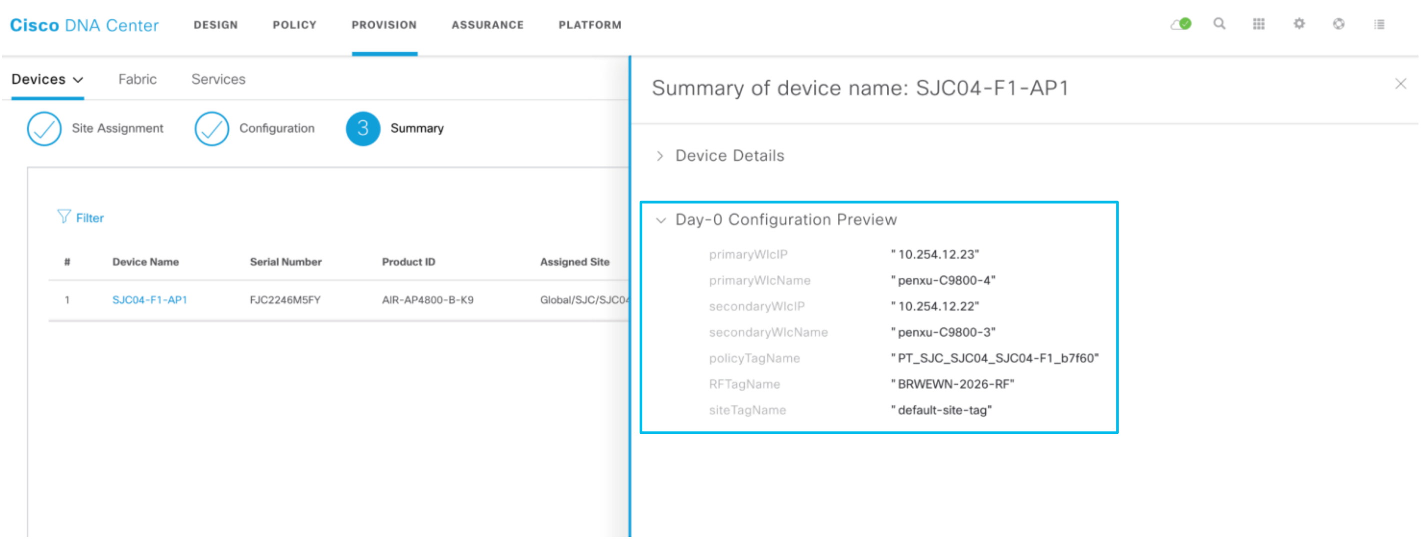
RF Profile*: BRWEWN-2026-RF

RF profile is used to generate RF Tag and associate it to AP.

Provision- Provision APs to Site



Option -1



#	Device Name	Serial Number	Product ID	Assigned Site
1	SJC04-F1-AP1	FJC2246M5FY	AIR-AP4800-B-K9	Global/SJC/SJC04

Summary of device name: SJC04-F1-AP1

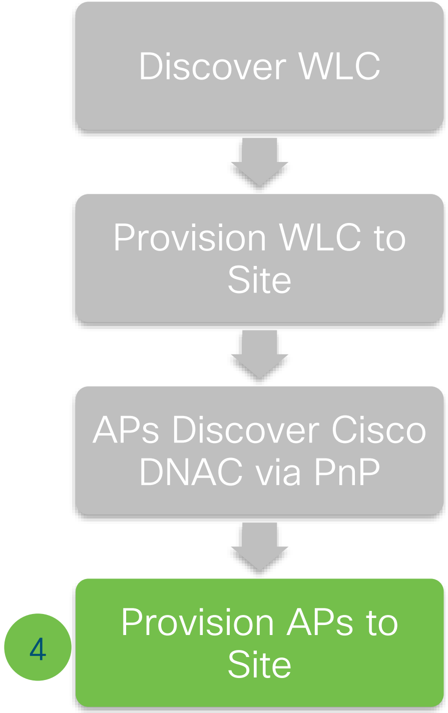
Device Details

Day-0 Configuration Preview

primaryWlcIP	" 10.254.12.23"
primaryWlcName	" penxu-C9800-4"
secondaryWlcIP	" 10.254.12.22"
secondaryWlcName	" penxu-C9800-3"
policyTagName	" PT_SJC_SJC04_SJC04-F1_b7f60"
RFTagName	" BRWEWN-2026-RF"
siteTagName	" default-site-tag"

Provision- Provision APs to Site

Sample AP Console Log



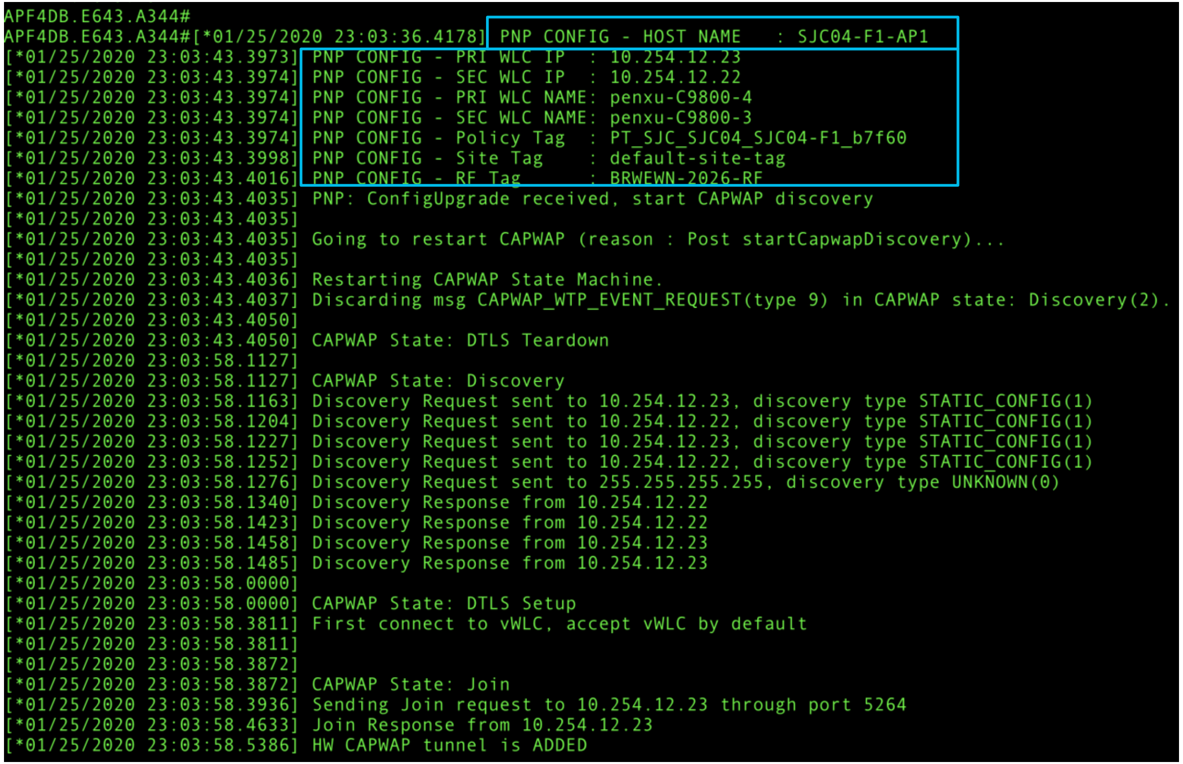
Discover WLC

Provision WLC to Site

APs Discover Cisco DNAC via PnP

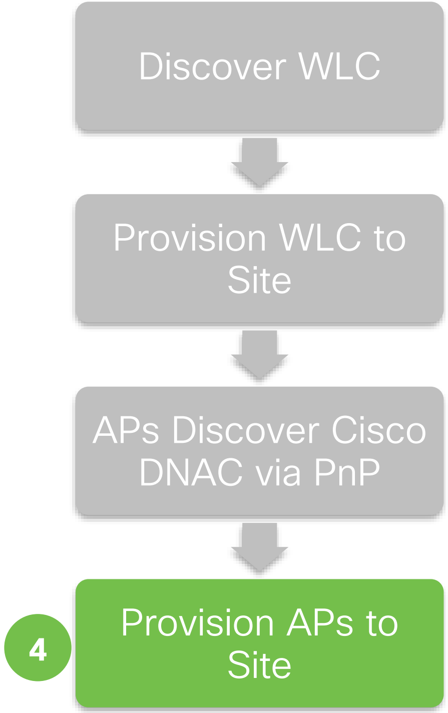
4

Provision APs to Site



```
APF4DB.E643.A344#
APF4DB.E643.A344#[*01/25/2020 23:03:36.4178] PNP CONFIG - HOST NAME    : SJC04-F1-AP1
[*01/25/2020 23:03:43.3973] PNP CONFIG - PRI WLC IP   : 10.254.12.23
[*01/25/2020 23:03:43.3974] PNP CONFIG - SEC WLC IP   : 10.254.12.22
[*01/25/2020 23:03:43.3974] PNP CONFIG - PRI WLC NAME: penxu-C9800-4
[*01/25/2020 23:03:43.3974] PNP CONFIG - SEC WLC NAME: penxu-C9800-3
[*01/25/2020 23:03:43.3974] PNP CONFIG - Policy Tag   : PT_SJC_SJC04_SJC04-F1_b7f60
[*01/25/2020 23:03:43.3998] PNP CONFIG - Site Tag     : default-site-tag
[*01/25/2020 23:03:43.4016] PNP CONFIG - RF Tag       : BRWEWN-2026-RF
[*01/25/2020 23:03:43.4035] PNP: ConfigUpgrade received, start CAPWAP discovery
[*01/25/2020 23:03:43.4035]
[*01/25/2020 23:03:43.4035] Going to restart CAPWAP (reason : Post startCapwapDiscovery)...
[*01/25/2020 23:03:43.4035]
[*01/25/2020 23:03:43.4036] Restarting CAPWAP State Machine.
[*01/25/2020 23:03:43.4037] Discarding msg CAPWAP_WTP_EVENT_REQUEST(type 9) in CAPWAP state: Discovery(2).
[*01/25/2020 23:03:43.4050]
[*01/25/2020 23:03:43.4050] CAPWAP State: DTLS Teardown
[*01/25/2020 23:03:58.1127]
[*01/25/2020 23:03:58.1127] CAPWAP State: Discovery
[*01/25/2020 23:03:58.1163] Discovery Request sent to 10.254.12.23, discovery type STATIC_CONFIG(1)
[*01/25/2020 23:03:58.1204] Discovery Request sent to 10.254.12.22, discovery type STATIC_CONFIG(1)
[*01/25/2020 23:03:58.1227] Discovery Request sent to 10.254.12.23, discovery type STATIC_CONFIG(1)
[*01/25/2020 23:03:58.1252] Discovery Request sent to 10.254.12.22, discovery type STATIC_CONFIG(1)
[*01/25/2020 23:03:58.1276] Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)
[*01/25/2020 23:03:58.1340] Discovery Response from 10.254.12.22
[*01/25/2020 23:03:58.1423] Discovery Response from 10.254.12.22
[*01/25/2020 23:03:58.1458] Discovery Response from 10.254.12.23
[*01/25/2020 23:03:58.1485] Discovery Response from 10.254.12.23
[*01/25/2020 23:03:58.0000]
[*01/25/2020 23:03:58.0000] CAPWAP State: DTLS Setup
[*01/25/2020 23:03:58.3811] First connect to vWLC, accept vWLC by default
[*01/25/2020 23:03:58.3811]
[*01/25/2020 23:03:58.3872]
[*01/25/2020 23:03:58.3872] CAPWAP State: Join
[*01/25/2020 23:03:58.3936] Sending Join request to 10.254.12.23 through port 5264
[*01/25/2020 23:03:58.4633] Join Response from 10.254.12.23
[*01/25/2020 23:03:58.5386] HW CAPWAP tunnel is ADDED
```

Provision- Provision APs to Site



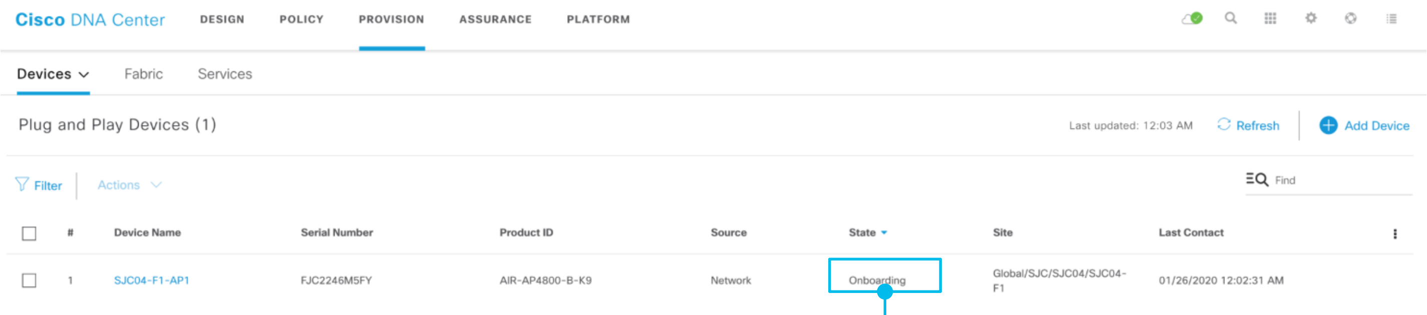
Discover WLC

Provision WLC to Site

APs Discover Cisco DNAC via PnP

4 Provision APs to Site

Option - 1



Plug and Play Devices (1)

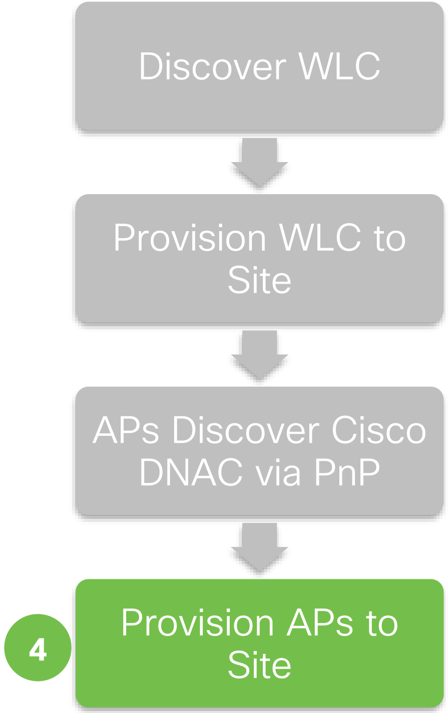
Last updated: 12:03 AM

□	#	Device Name	Serial Number	Product ID	Source	State	Site	Last Contact
□	1	SJC04-F1-AP1	FJC2246M5FY	AIR-AP4800-B-K9	Network	Onboarding	Global/SJC/SJC04/SJC04-F1	01/26/2020 12:02:31 AM

Note that AP will stay in “Onboarding” state until AP joins desired WLC. Once AP joins desired WLC, WLC will send AP join trap to Cisco DNA Center, which in turn triggers resync with WLC and adds AP to inventory. Finally, AP PnP status will become “Provisioned” as PnP completes.

Provision- Provision APs to Site

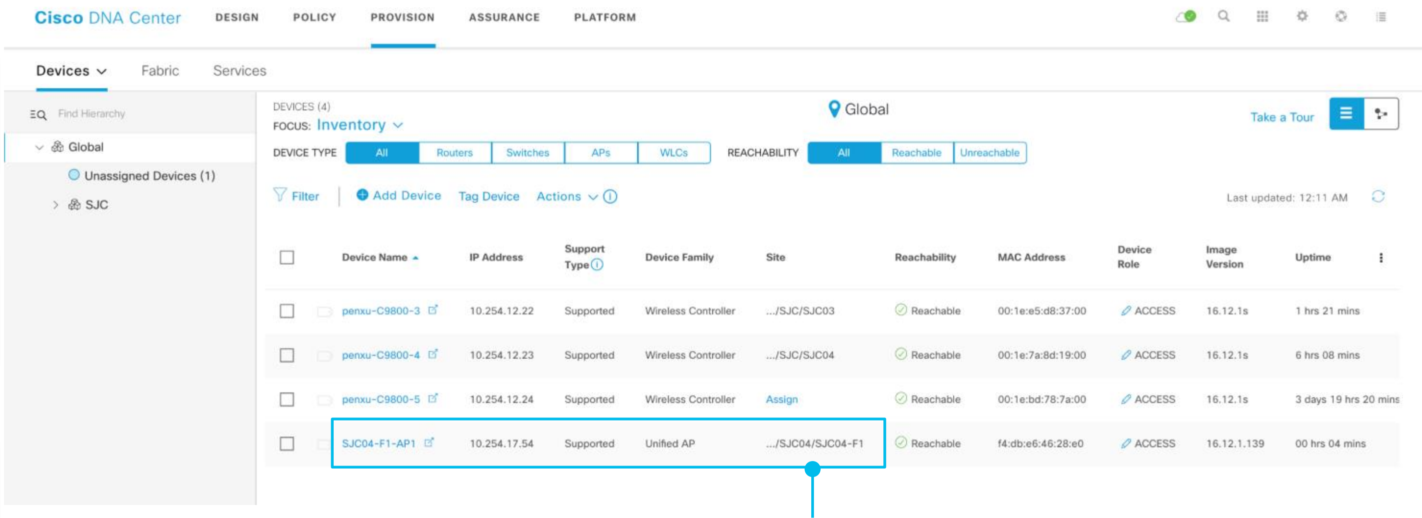
Option -1


Discover WLC

Provision WLC to Site

APs Discover Cisco DNAC via PnP

4 Provision APs to Site



DEVICES (4)

FOCUS: Inventory

Global

Last updated: 12:11 AM

□	Device Name	IP Address	Support Type	Device Family	Site	Reachability	MAC Address	Device Role	Image Version	Uptime
□	penxu-C9800-3	10.254.12.22	Supported	Wireless Controller	.../SJC/SJC03	Reachable	00:1e:e5:d8:37:00	ACCESS	16.12.1s	1 hrs 21 mins
□	penxu-C9800-4	10.254.12.23	Supported	Wireless Controller	.../SJC/SJC04	Reachable	00:1e:7a:8d:19:00	ACCESS	16.12.1s	6 hrs 08 mins
□	penxu-C9800-5	10.254.12.24	Supported	Wireless Controller	Assign	Reachable	00:1e:bd:78:7a:00	ACCESS	16.12.1s	3 days 19 hrs 20 mins
□	SJC04-F1-AP1	10.254.17.54	Supported	Unified AP	.../SJC04/SJC04-F1	Reachable	f4:db:e6:46:28:e0	ACCESS	16.12.1.139	00 hrs 04 mins

AP is added to inventory and assigned to the desired floor.

Provision- Provision APs to Site

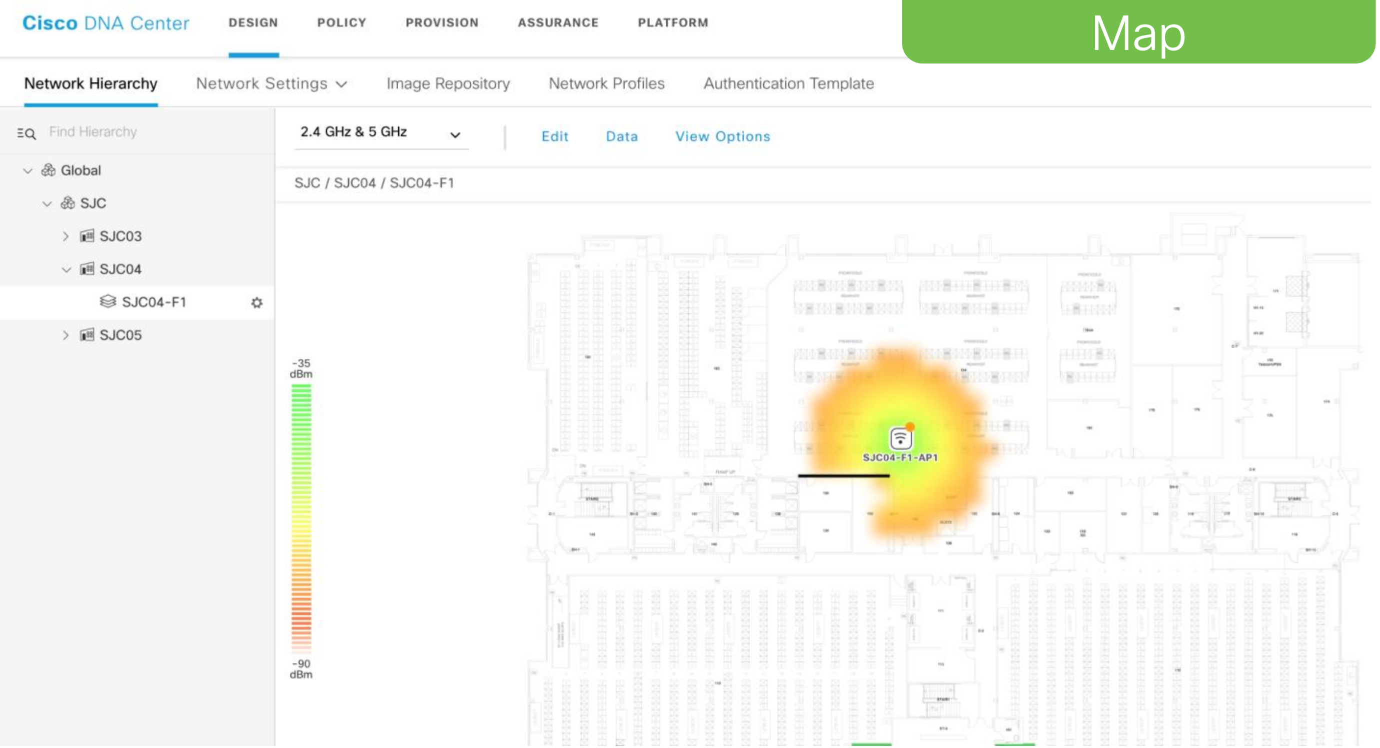
Cisco DNA Center Map

Discover WLC

Provision WLC to Site

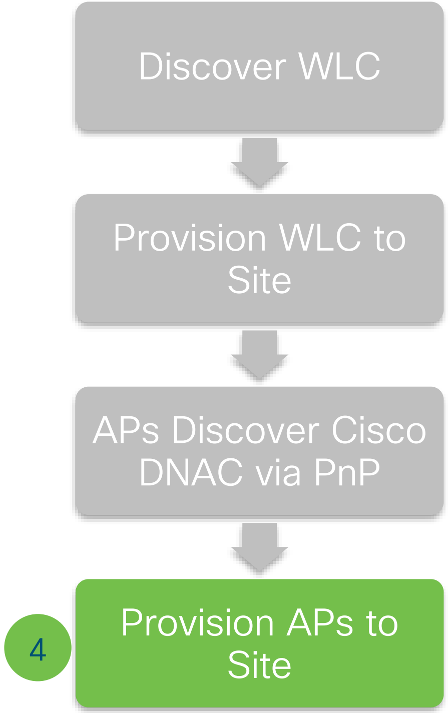
APs Discover Cisco DNAC via PnP

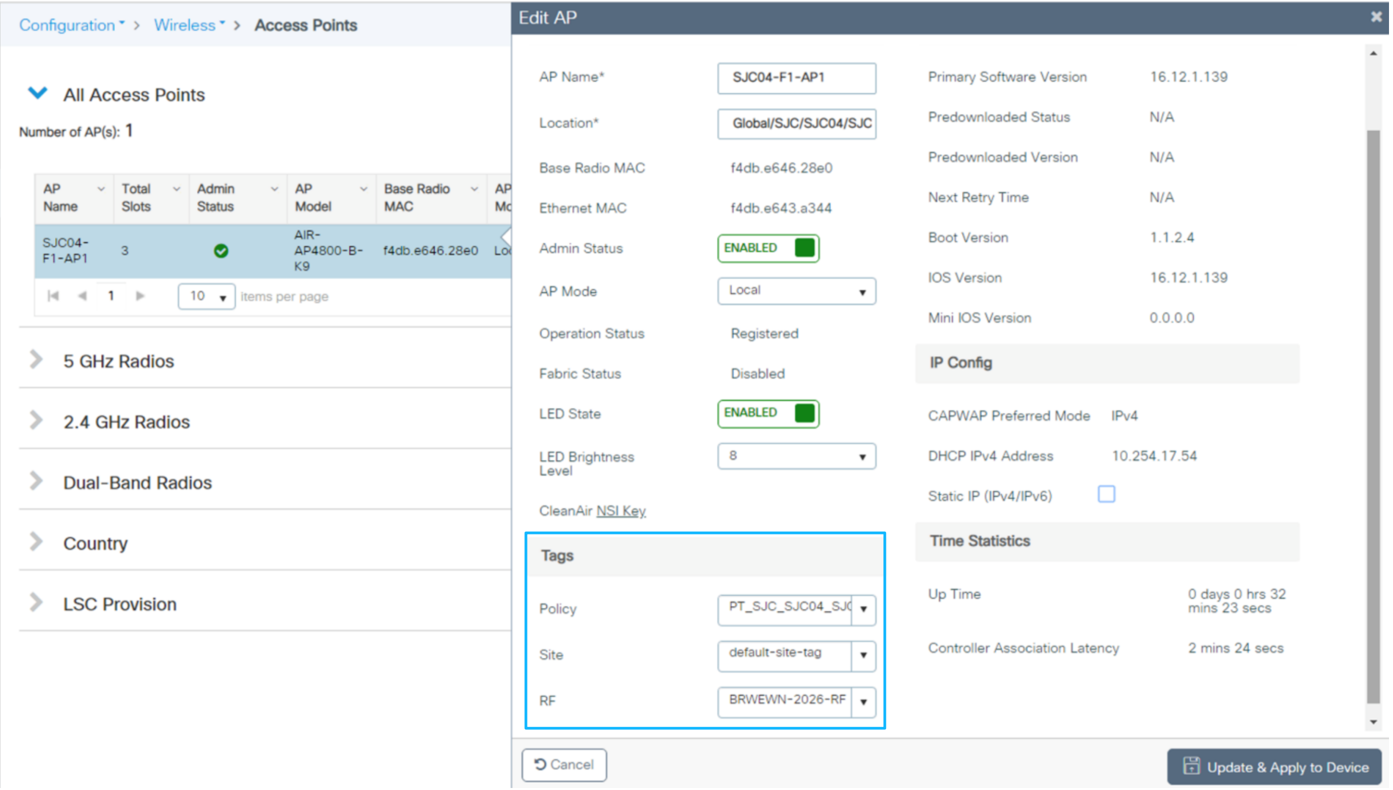
4 Provision APs to Site



Provision- Provision APs to Site

On C9800 Wireless Controller





All Access Points

Number of AP(s): 1

AP Name	Total Slots	Admin Status	AP Model	Base Radio MAC	AP Mo
SJC04-F1-AP1	3	✓	AIR-AP4800-B-K9	f4db.e646.28e0	Lo

1 · 10 items per page

Edit AP

AP Name*	SJC04-F1-AP1	Primary Software Version	16.12.1.139
Location*	Global/SJC/SJC04/SJC	Predownloaded Status	N/A
Base Radio MAC	f4db.e646.28e0	Predownloaded Version	N/A
Ethernet MAC	f4db.e643.a344	Next Retry Time	N/A
Admin Status	ENABLED	Boot Version	1.1.2.4
AP Mode	Local	IOS Version	16.12.1.139
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled		
LED State	ENABLED		
LED Brightness Level	8		
CleanAir NSI Key			

IP Config

CAPWAP Preferred Mode: IPv4

DHCP IPv4 Address: 10.254.17.54

Static IP (IPv4/IPv6) □

Tags

Policy: PT_SJC_SJC04_SJC

Site: default-site-tag

RF: BRWEWN-2026-RF

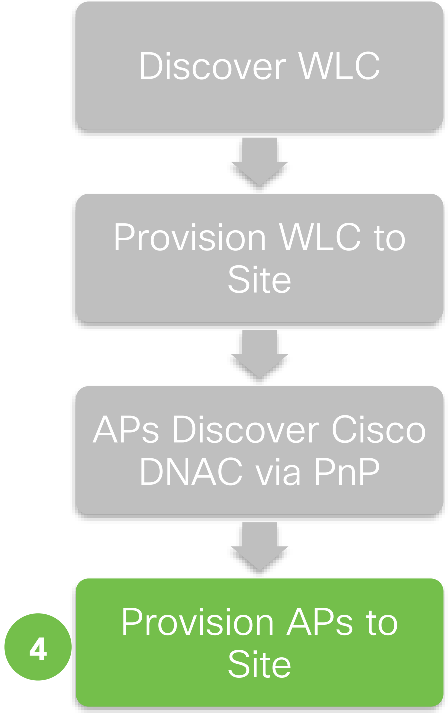
Time Statistics

Up Time: 0 days 0 hrs 32 mins 23 secs

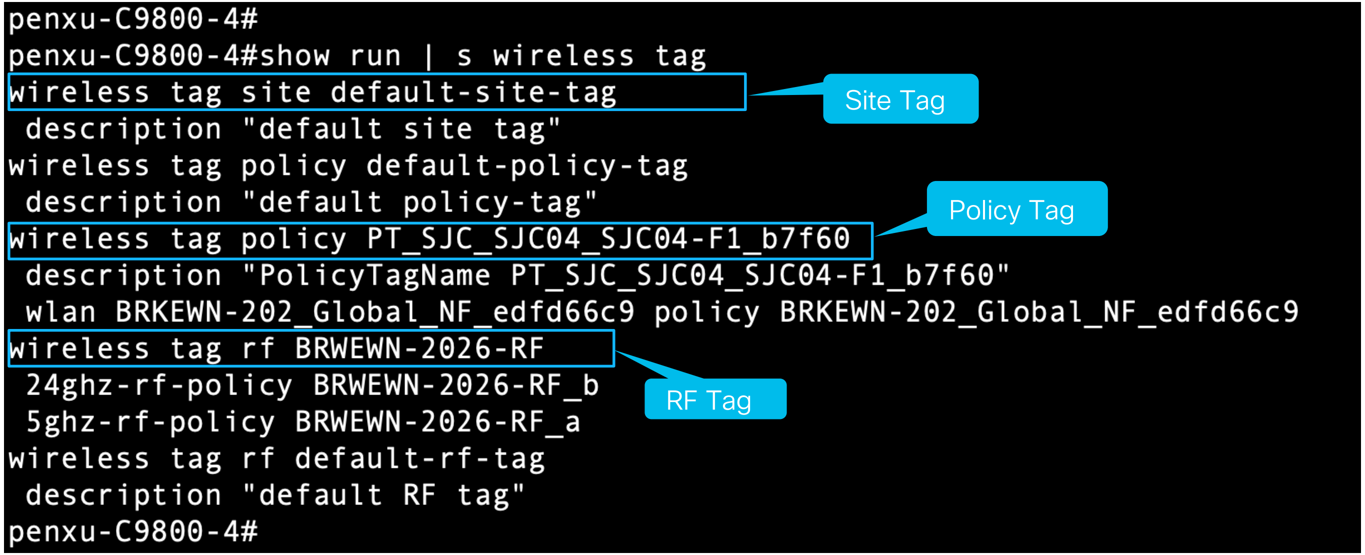
Controller Association Latency: 2 mins 24 secs

cisco Live!

Provision- Provision APs to Site



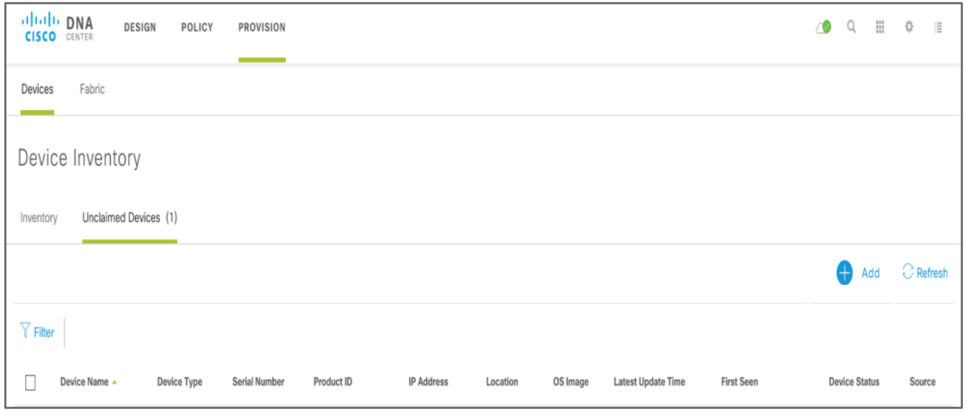
ON C9800 Wireless Controller

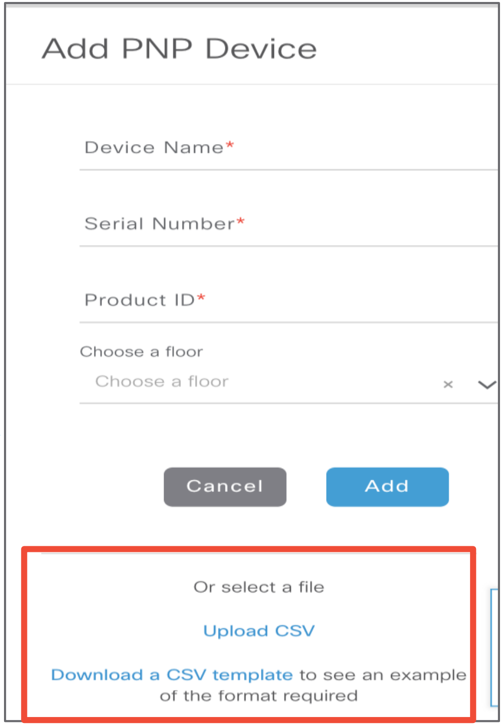


```
penxu-C9800-4#
penxu-C9800-4#show run | s wireless tag
wireless tag site default-site-tag
 description "default site tag"
wireless tag policy default-policy-tag
 description "default policy-tag"
wireless tag policy PT_SJC_SJC04_SJC04-F1_b7f60
 description "PolicyTagName PT_SJC_SJC04_SJC04-F1_b7f60"
 wlan BRKEWN-202_Global_NF_edfd66c9 policy BRKEWN-202_Global_NF_edfd66c9
wireless tag rf BRWEWN-2026-RF
 24ghz-rf-policy BRWEWN-2026-RF_b
 5ghz-rf-policy BRWEWN-2026-RF_a
wireless tag rf default-rf-tag
 description "default RF tag"
penxu-C9800-4#
```

Option - 2 : Bulk AP Deployment

1 Import APs





Add PNP Device

Device Name*

Serial Number*

Product ID*

Choose a floor

Choose a floor

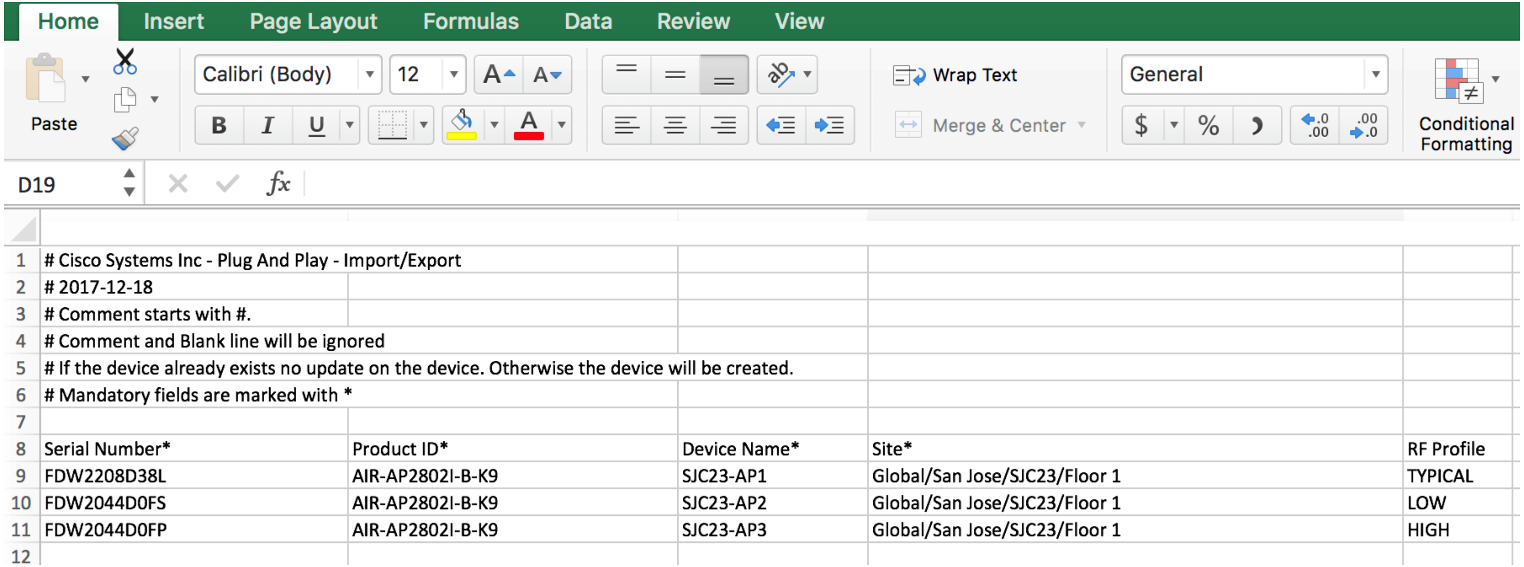
Or select a file

Upload CSV

Download a CSV template to see an example of the format required

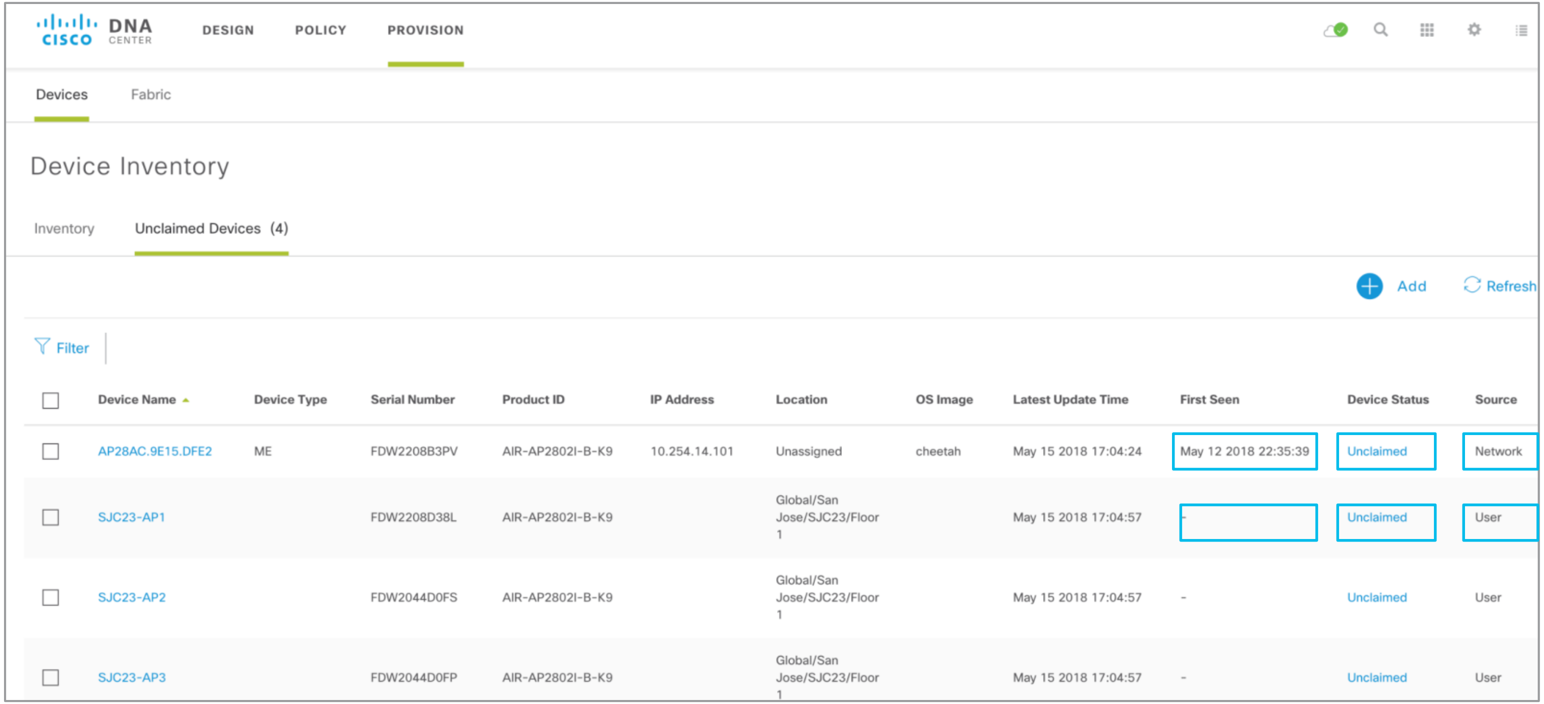
Option – 2 : Bulk AP Deployment

2 Prepare AP Bulk Import CSV and Upload



# Cisco Systems Inc - Plug And Play - Import/Export				
# 2017-12-18				
# Comment starts with #.				
# Comment and Blank line will be ignored				
# If the device already exists no update on the device. Otherwise the device will be created.				
# Mandatory fields are marked with *				
Serial Number*	Product ID*	Device Name*	Site*	RF Profile
FDW2208D38L	AIR-AP2802I-B-K9	SJC23-AP1	Global/San Jose/SJC23/Floor 1	TYPICAL
FDW2044D0FS	AIR-AP2802I-B-K9	SJC23-AP2	Global/San Jose/SJC23/Floor 1	LOW
FDW2044D0FP	AIR-AP2802I-B-K9	SJC23-AP3	Global/San Jose/SJC23/Floor 1	HIGH

Option – 2 : Bulk AP Deployment



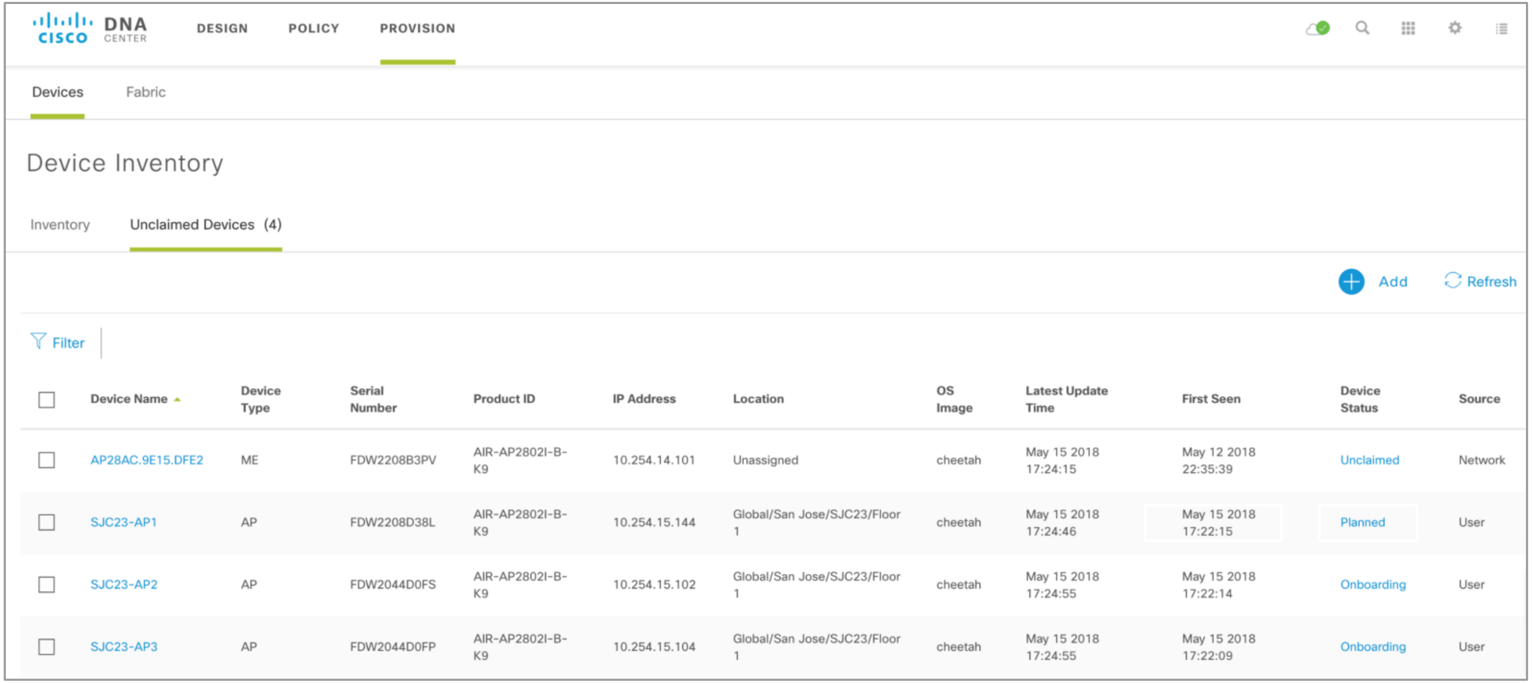
Device Inventory

□	Device Name	Device Type	Serial Number	Product ID	IP Address	Location	OS Image	Latest Update Time	First Seen	Device Status	Source
□	AP28AC.9E15.DFE2	ME	FDW2208B3PV	AIR-AP2802I-B-K9	10.254.14.101	Unassigned	cheetah	May 15 2018 17:04:24	May 12 2018 22:35:39	Unclaimed	Network
□	SJC23-AP1		FDW2208D38L	AIR-AP2802I-B-K9		Global/San Jose/SJC23/Floor 1		May 15 2018 17:04:57	-	Unclaimed	User
□	SJC23-AP2		FDW2044D0FS	AIR-AP2802I-B-K9		Global/San Jose/SJC23/Floor 1		May 15 2018 17:04:57	-	Unclaimed	User
□	SJC23-AP3		FDW2044D0FP	AIR-AP2802I-B-K9		Global/San Jose/SJC23/Floor 1		May 15 2018 17:04:57	-	Unclaimed	User

Status: Import APs vs. Actively Connected APs

Option – 2 : Bulk AP Deployment

3 Auto Claim APs when they contact Cisco DNA Center via PnP



Device Inventory

Inventory | Unclaimed Devices (4)

□	Device Name	Device Type	Serial Number	Product ID	IP Address	Location	OS Image	Latest Update Time	First Seen	Device Status	Source
□	AP28AC.9E15.DFE2	ME	FDW2208B3PV	AIR-AP2802I-B-K9	10.254.14.101	Unassigned	cheetah	May 15 2018 17:24:15	May 12 2018 22:35:39	Unclaimed	Network
□	SJC23-AP1	AP	FDW2208D38L	AIR-AP2802I-B-K9	10.254.15.144	Global/San Jose/SJC23/Floor 1	cheetah	May 15 2018 17:24:46	May 15 2018 17:22:15	Planned	User
□	SJC23-AP2	AP	FDW2044D0FS	AIR-AP2802I-B-K9	10.254.15.102	Global/San Jose/SJC23/Floor 1	cheetah	May 15 2018 17:24:55	May 15 2018 17:22:14	Onboarding	User
□	SJC23-AP3	AP	FDW2044D0FP	AIR-AP2802I-B-K9	10.254.15.104	Global/San Jose/SJC23/Floor 1	cheetah	May 15 2018 17:24:55	May 15 2018 17:22:09	Onboarding	User

Demo - AP Provisioning

What did we do so far?

Planned the Sites & Hierarchy

Extracted Common/Standard across Wired and Wireless to be self managed

Captured the business intent within a Network Profile

Converting Business Intent to Network Policy - WLC Provisioning

Converting Business Intent to Network Policy - AP Provisioning

Summary

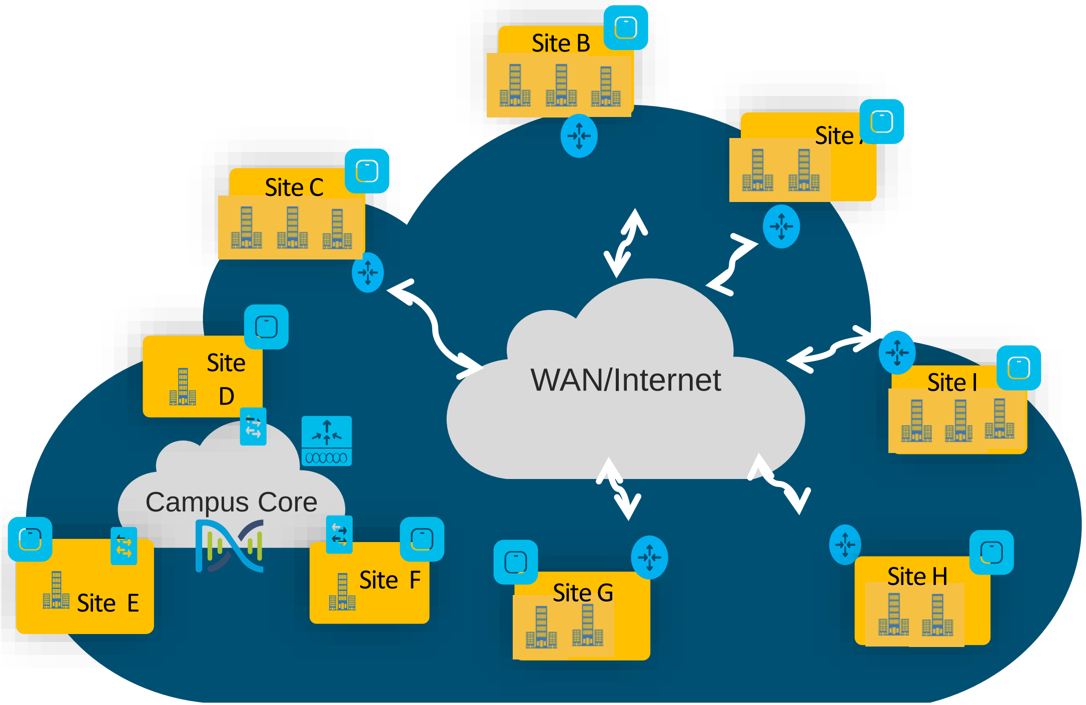
- Network Profiles are mapped to Sites and Site becomes the glue for Automation
- Configuration Standardization & Compliance using Network Profiles
- Automated Policy, Site and RF tags creation for AP Onboarding.
- APs are placed to planned position automatically. No more waiting!

Day 2 Changes

Configuration Changes

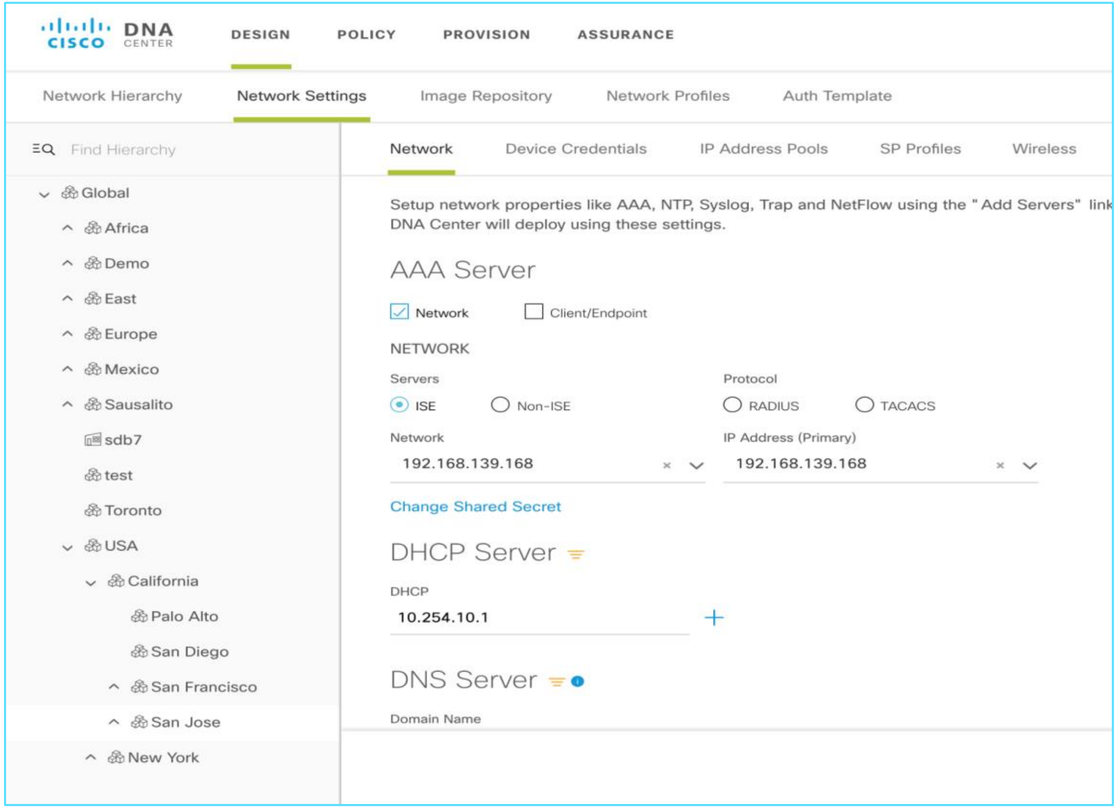
Scenario – Day N Configuration Changes

Provision wireless LAN controllers and access points across sites



Typical Customer Network

Changes with Network Settings & Credentials



Setup network properties like AAA, NTP, Syslog, Trap and NetFlow using the " Add Servers" link
DNA Center will deploy using these settings.

AAA Server

☑ Network □ Client/Endpoint

NETWORK

Servers: ● ISE ○ Non-ISE

Protocol: ○ RADIUS ○ TACACS

Network: 192.168.139.168

IP Address (Primary): 192.168.139.168

Change Shared Secret

DHCP Server

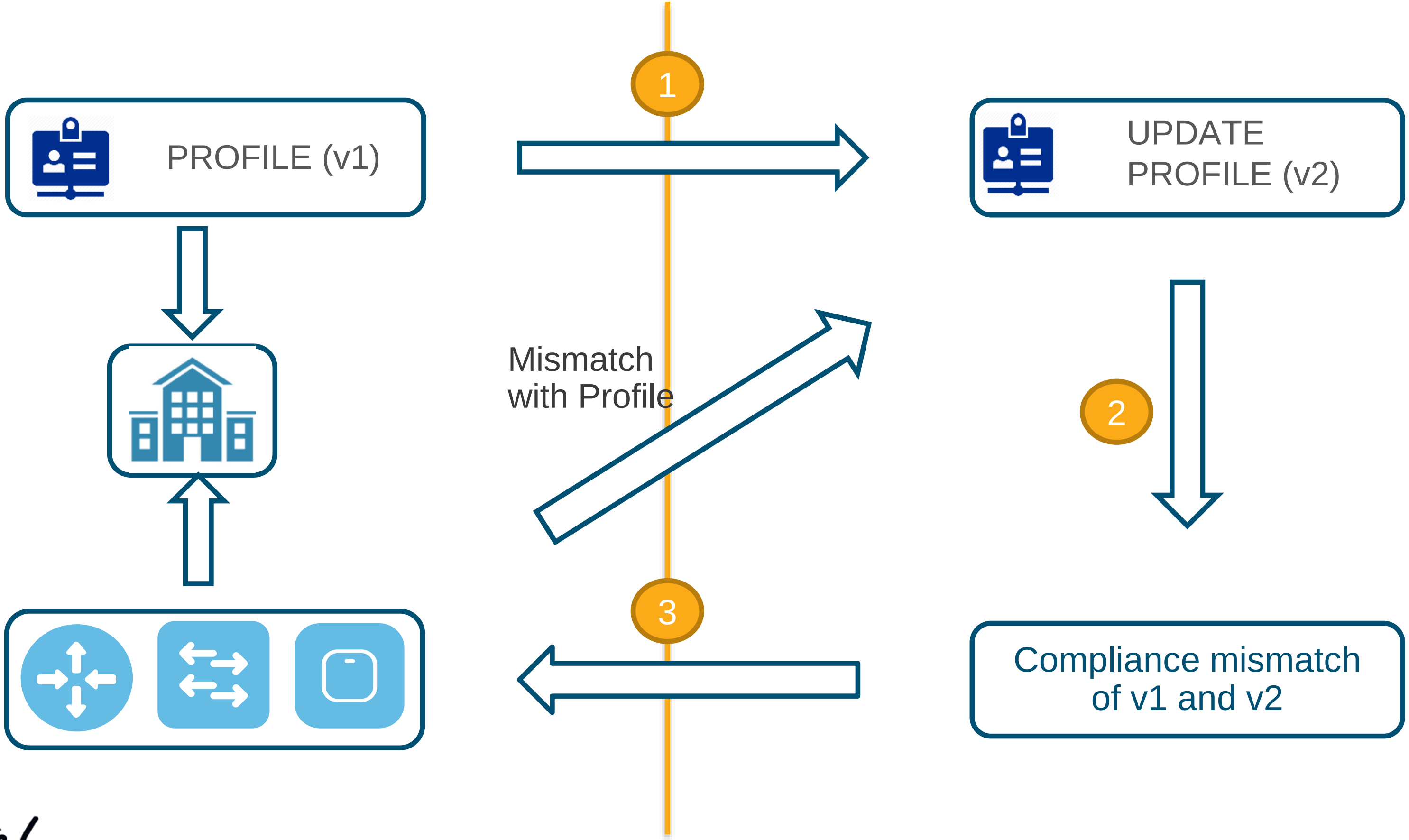
DHCP: 10.254.10.1

DNS Server

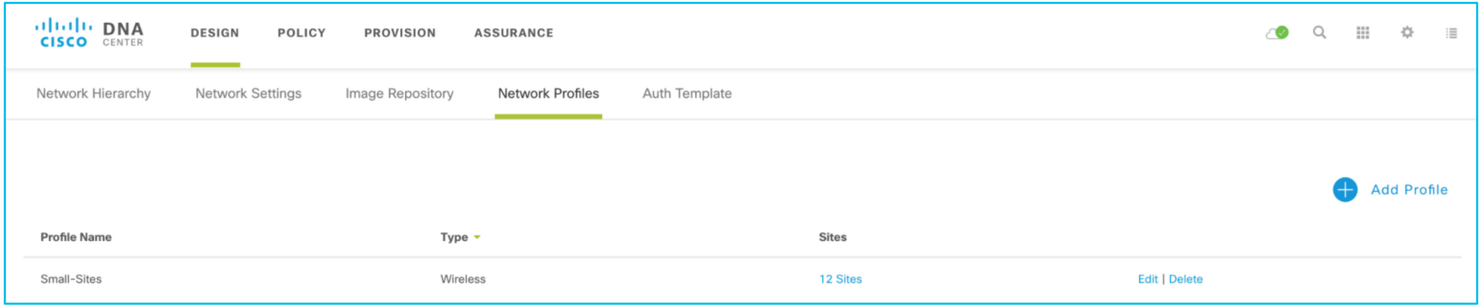
Domain Name

- Single place to change the credentials and Network settings for the sites
- During the device provision, these changes will be configured

Network Profile Lifecycle

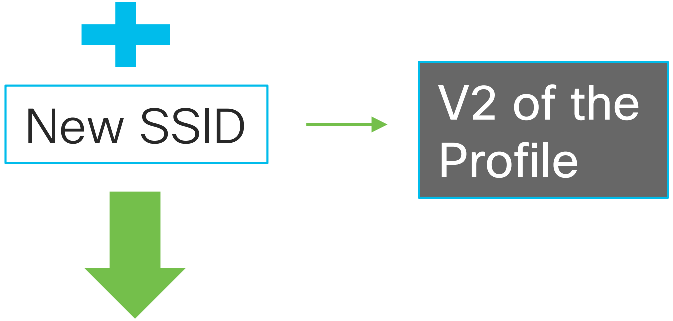


Wireless Profile – Day 2 Changes



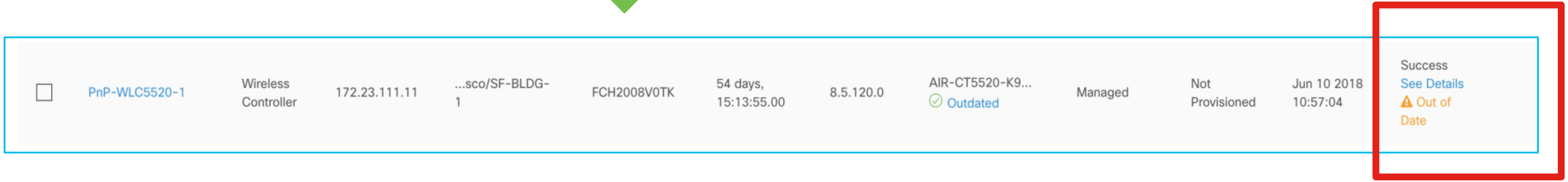
Profile Name	Type	Sites	
Small-Sites	Wireless	12 Sites	Edit | Delete

V1 of the Profile



New SSID

V2 of the Profile



□	PnP-WLC5520-1	Wireless Controller	172.23.111.11	...sco/SF-BLDG-1	FCH2008V0TK	54 days, 15:13:55.00	8.5.120.0	AIR-CT5520-K9... ✓ Outdated	Managed	Not Provisioned	Jun 10 2018 10:57:04	Success See Details ⚠ Out of Date

IRCM for Guest Anchoring

User Case:

Inter-Release Controller Mobility (IRCM) is critical for mobility roaming and guest anchoring. With introduction of C9800 IOS-XE WLC, Cisco DNA Center can simplify both green-field deployment and integration with AireOS WLC, starting guest anchoring support from 1.3 release.

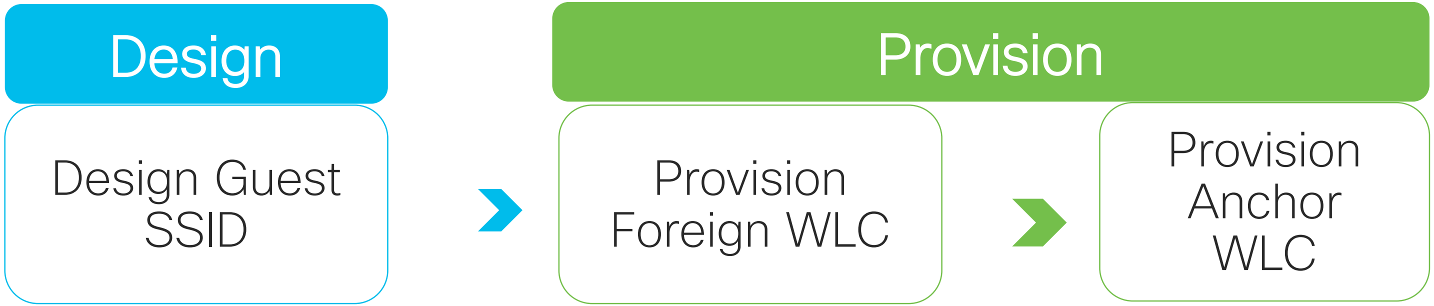
Foreign	Anchor	Cisco DNA Center Support
C9800 IOS-XE WLC	C9800 IOS-XE WLC	Yes from 1.3
C9800 IOS-XE WLC	AireOS WLC	Yes from 1.3
AireOS WLC	AireOS WLC	Yes from 1.2
AireOS WLC	C9800 IOS-XE WLC	No

Note that it requires AireOS WLC release 8.8.111.0 or above.

IRCM for Guest Anchoring Key Points

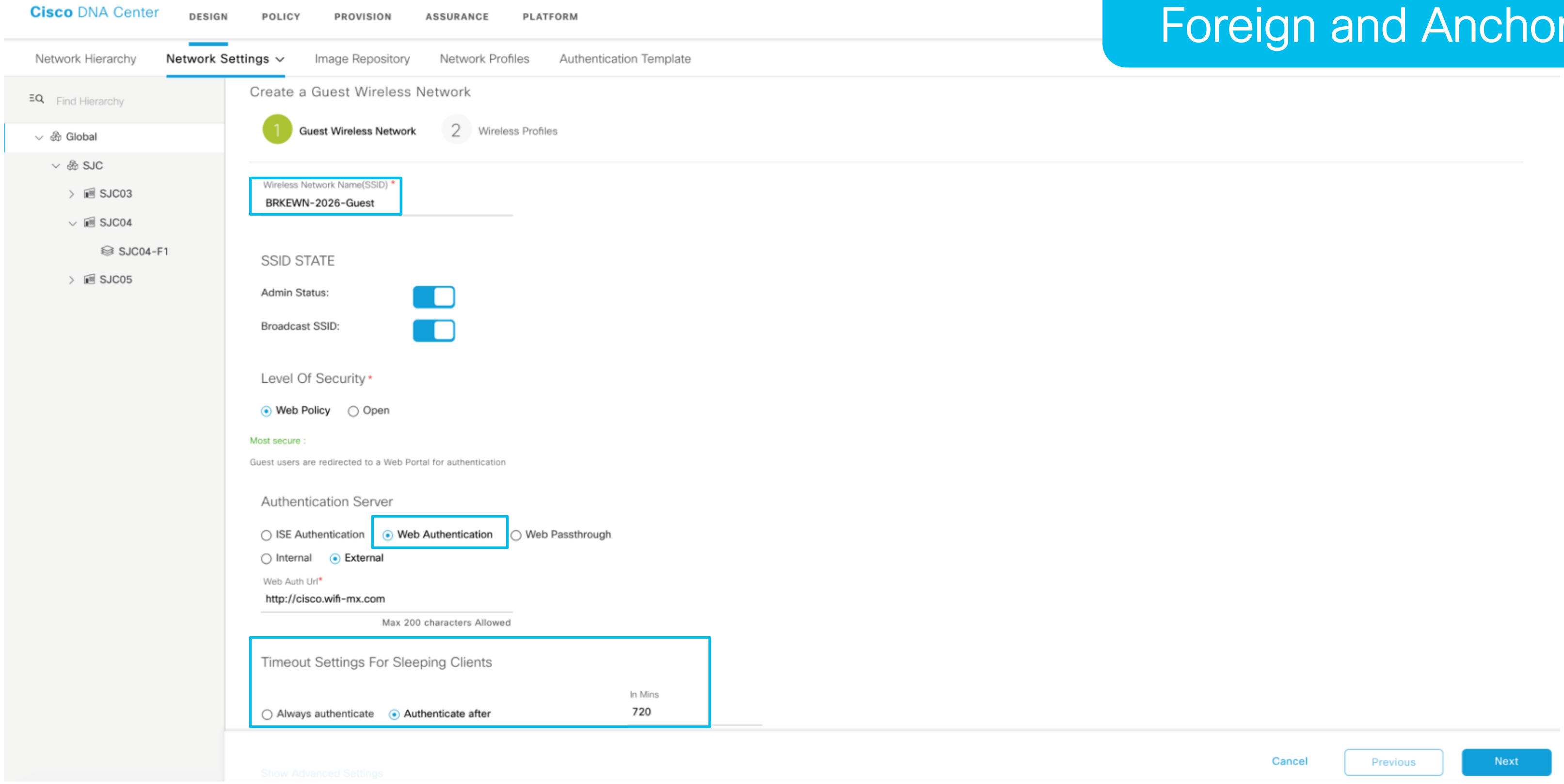
- Only one wireless profile required for both Foreign and Anchor WLCs
- In wireless profile, there is at least one SSID required to be specified as guest anchoring
- For Foreign WLC, Cisco DNA Center provision all SSIDs in the profile
- For Anchor WLC, Cisco DNA Center will deploy only guest anchor SSID in profile based on matching ”Manage AP Location” for Foreign and Anchor WLCs

IRCM for Guest Anchoring Workflow



Day 2 Example- IRCM Guest Anchoring
Design Guest SSID

C9800s as both Foreign and Anchor



Create a Guest Wireless Network

Wireless Network Name(SSID) *: BRKEWN-2026-Guest

SSID STATE

Admin Status: On

Broadcast SSID: On

Level Of Security *

● Web Policy ○ Open

Most secure :

Guest users are redirected to a Web Portal for authentication

Authentication Server

○ ISE Authentication ● Web Authentication ○ Web Passthrough

○ Internal ● External

Web Auth Url*: http://cisco.wifi-mx.com

Max 200 characters Allowed

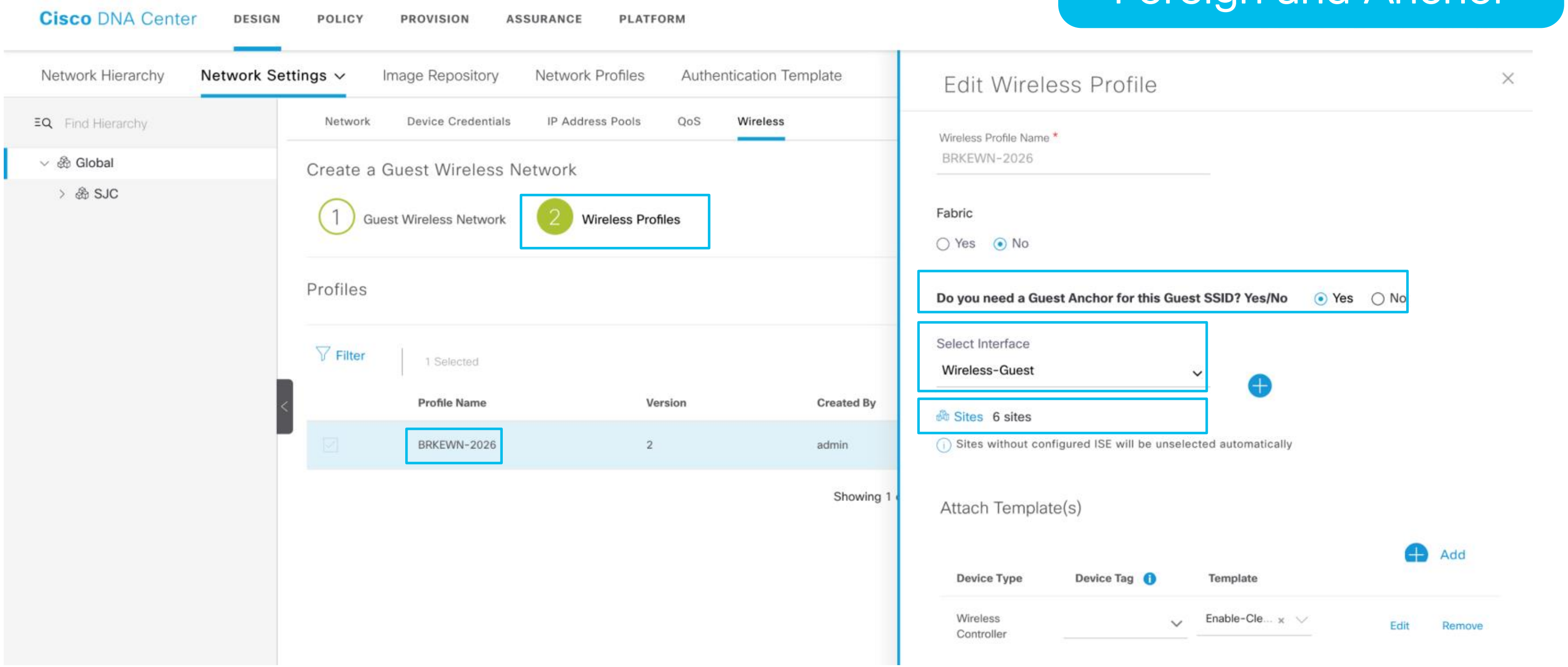
Timeout Settings For Sleeping Clients

○ Always authenticate ● Authenticate after

In Mins: 720

Day 2 Example – IRCM Guest Anchoring Design Guest SSID

C9800s as both Foreign and Anchor



Cisco DNA Center — DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

Network Hierarchy | **Network Settings** | Image Repository | Network Profiles | Authentication Template

Find Hierarchy

- Global
  - SJC

Network | Device Credentials | IP Address Pools | QoS | **Wireless**

Create a Guest Wireless Network

1 Guest Wireless Network — 2 **Wireless Profiles**

Profiles

Filter — 1 Selected

	Profile Name	Version	Created By
☑	BRKEWN-2026	2	admin

Showing 1

Edit Wireless Profile

Wireless Profile Name * BRKEWN-2026

Fabric ○ Yes ● No

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

Select Interface: Wireless-Guest

Sites 6 sites

Sites without configured ISE will be unselected automatically

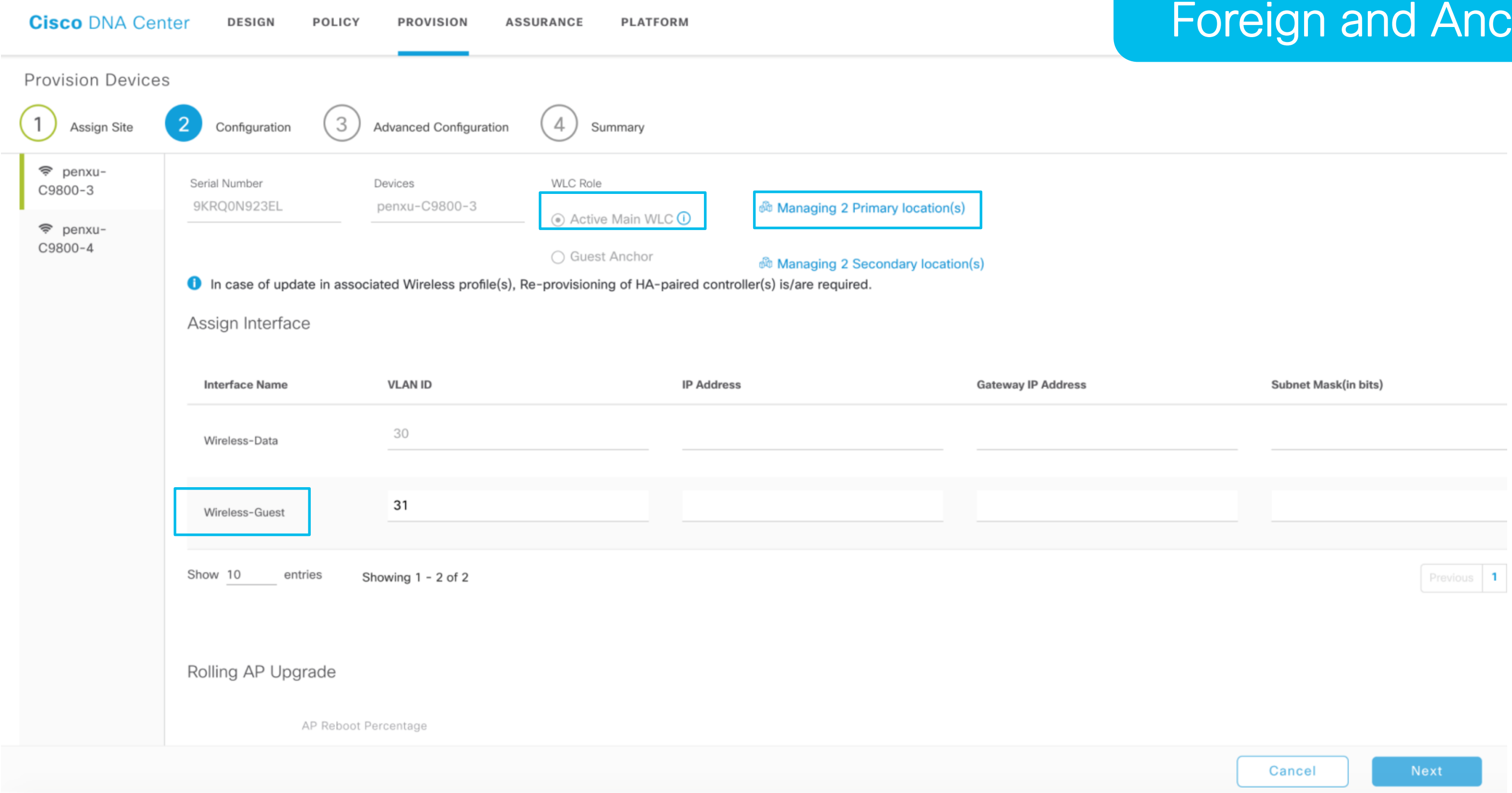
Attach Template(s)

Add

Device Type	Device Tag	Template		
Wireless Controller		Enable-Cle...	Edit	Remove

Day 2 Example – IRCM Guest Anchoring Provision Foreign WLC(s)

C9800s as both Foreign and Anchor



Provision Devices

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

Serial Number	Devices	WLC Role
9KRQ0N923EL	penxu-C9800-3	● Active Main WLC ⓘ ○ Guest Anchor

Managing 2 Primary location(s)

Managing 2 Secondary location(s)

ⓘ In case of update in associated Wireless profile(s), Re-provisioning of HA-paired controller(s) is/are required.

Assign Interface

Interface Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
Wireless-Data	30			
Wireless-Guest	31			

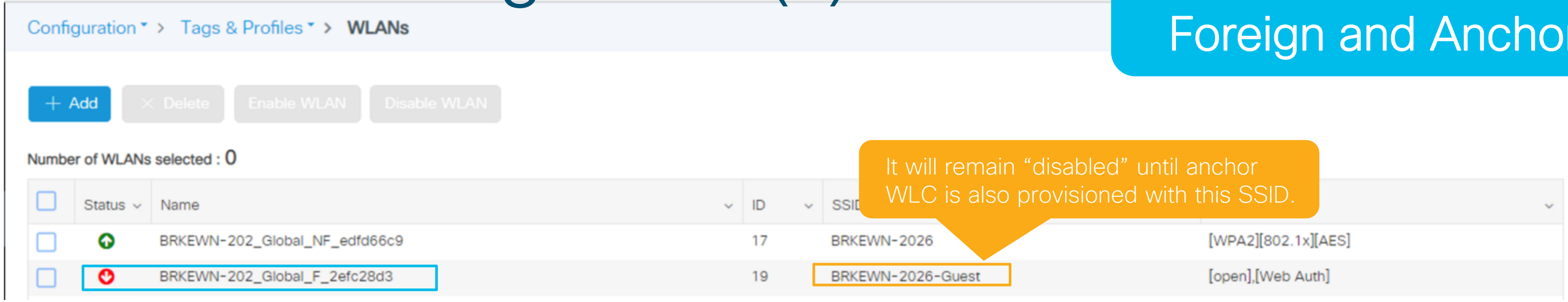
Show 10 entries   Showing 1 - 2 of 2

Rolling AP Upgrade

AP Reboot Percentage

Day 2 Example - IRCM Guest Anchoring Provision Foreign WLC(s)

C9800s as both Foreign and Anchor



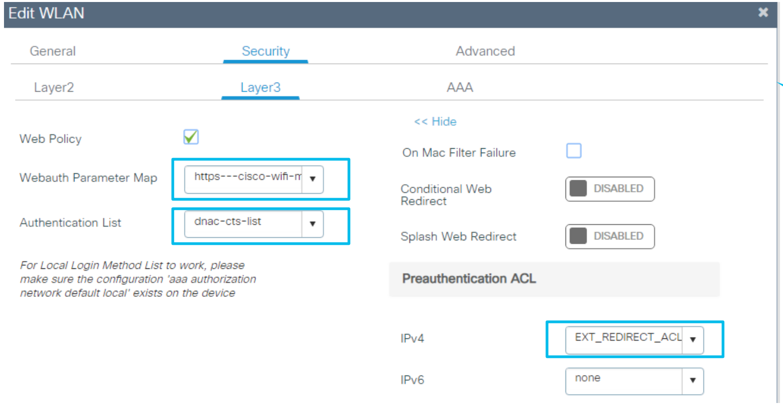
Configuration ˅ > Tags & Profiles ˅ > **WLANs**

+ Add | × Delete | Enable WLAN | Disable WLAN

Number of WLANs selected : 0

□	Status ˅	Name ˅	ID ˅	SSID	˅
□	⬆	BRKEWN-202_Global_NF_edfd66c9	17	BRKEWN-2026	[WPA2][802.1x][AES]
□	⬇	BRKEWN-202_Global_F_2efc28d3	19	BRKEWN-2026-Guest	[open],[Web Auth]

It will remain "disabled" until anchor WLC is also provisioned with this SSID.



Edit WLAN ×

General | Security | Advanced

Layer2 | Layer3 | AAA

Web Policy ☑

Webauth Parameter Map: https---cisco-wifi-m ▾

Authentication List: dnac-cts-list ▾

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

<< Hide

On Mac Filter Failure □

Conditional Web Redirect: DISABLED

Splash Web Redirect: DISABLED

Preauthentication ACL

IPv4: EXT_REDIRECT_ACL ▾

IPv6: none ▾

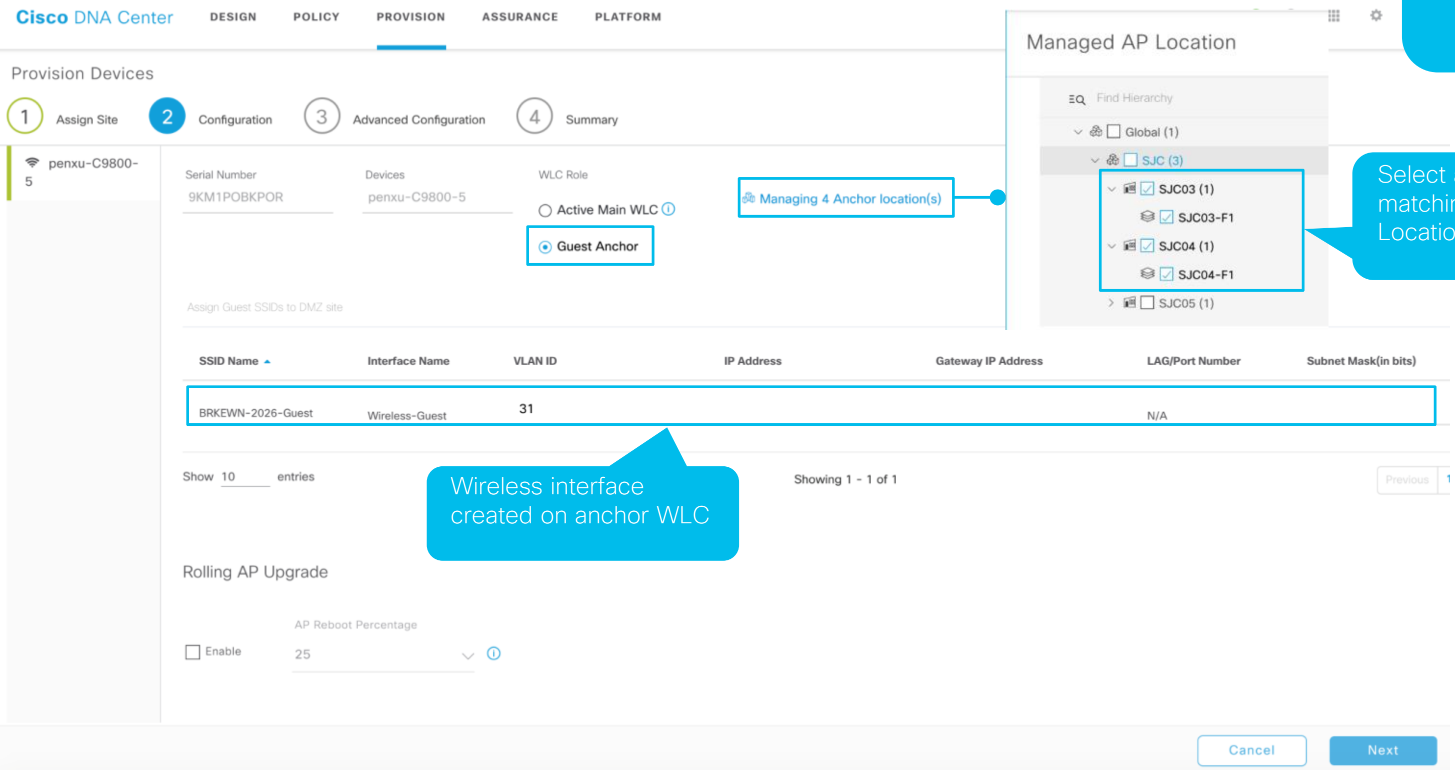
What else in WLAN?

- Webauth Parameter Map
- Authentication List
- Preauthentication ACL

cisco Live!

Day 2 Example - IRCM Guest Anchoring Provision Anchor WLC(s)

C9800s as both Foreign and Anchor



Provision Devices

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

penxu-C9800-5

Serial Number: 9KM1POBKPOR

Devices: penxu-C9800-5

WLC Role:
○ Active Main WLC ⓘ
● Guest Anchor

Managing 4 Anchor location(s)

Managed AP Location

Find Hierarchy
- □ Global (1)
  - □ SJC (3)
    - ☑ SJC03 (1)
      - ☑ SJC03-F1
    - ☑ SJC04 (1)
      - ☑ SJC04-F1
    - □ SJC05 (1)

Assign Guest SSIDs to DMZ site

SSID Name ▲	Interface Name	VLAN ID	IP Address	Gateway IP Address	LAG/Port Number	Subnet Mask(in bits)
BRKEWN-2026-Guest	Wireless-Guest	31			N/A	

Show 10 entries

Showing 1 - 1 of 1

Rolling AP Upgrade

□ Enable

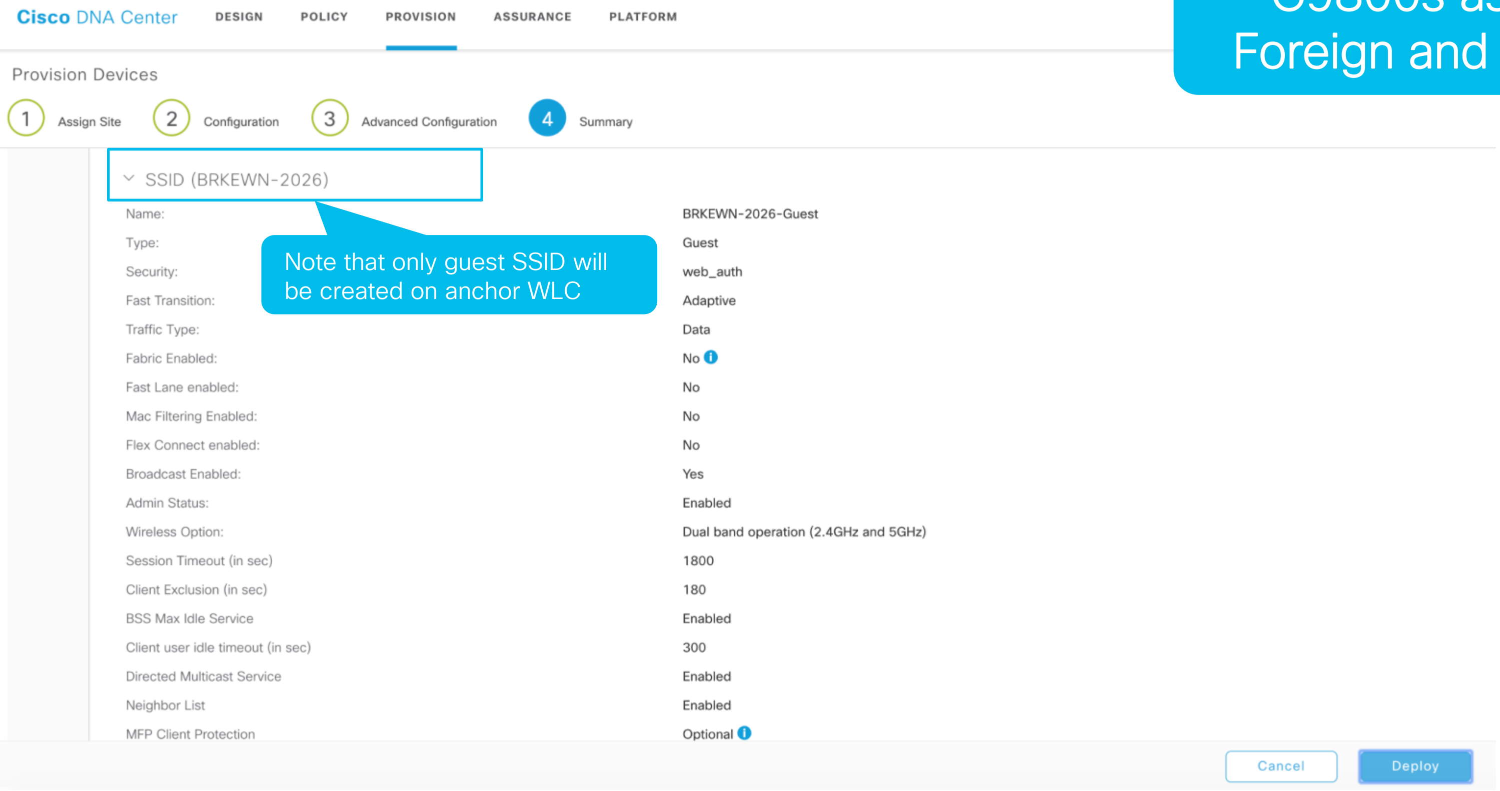
AP Reboot Percentage: 25 ⓘ

Select at least one matching "Manage AP Location" as foreign WLC

Wireless interface created on anchor WLC

Day 2 Example- IRCM Guest Anchoring Provision Anchor WLC(s)

C9800s as both Foreign and Anchor



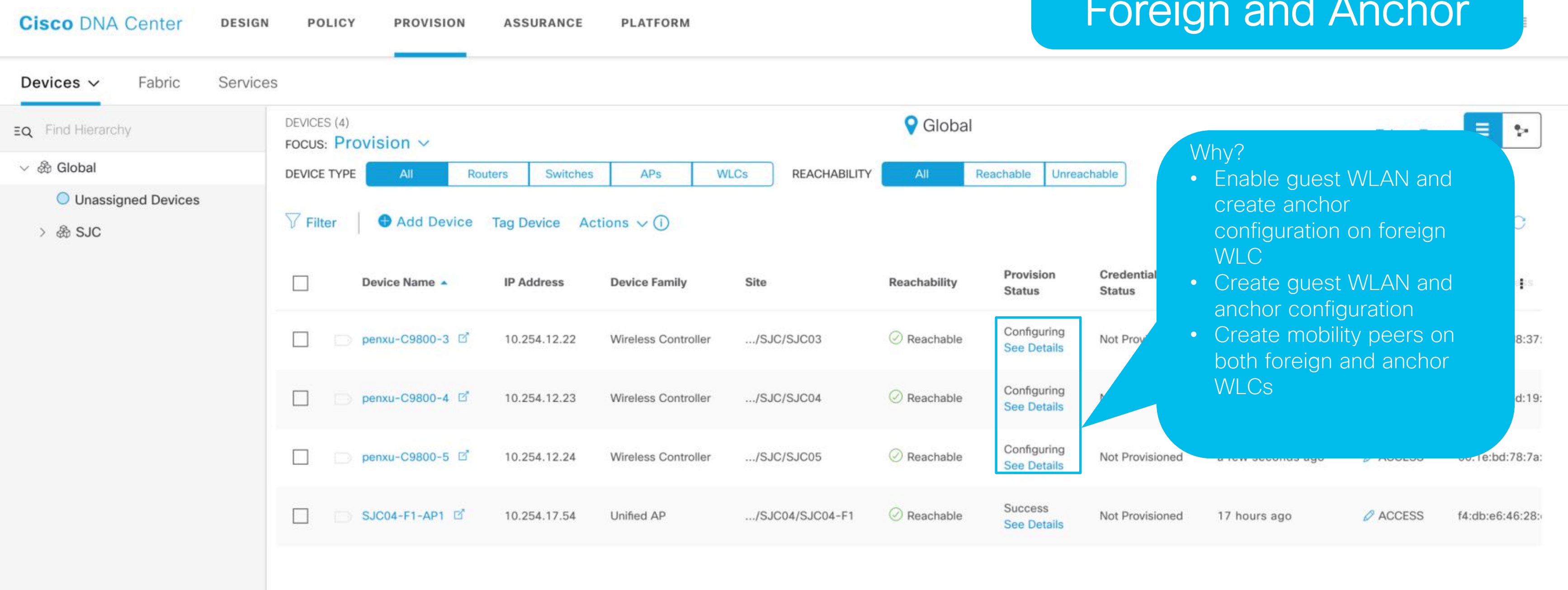
SSID (BRKEWN-2026)

Name:	BRKEWN-2026-Guest
Type:	Guest
Security:	web_auth
Fast Transition:	Adaptive
Traffic Type:	Data
Fabric Enabled:	No ⓘ
Fast Lane enabled:	No
Mac Filtering Enabled:	No
Flex Connect enabled:	No
Broadcast Enabled:	Yes
Admin Status:	Enabled
Wireless Option:	Dual band operation (2.4GHz and 5GHz)
Session Timeout (in sec)	1800
Client Exclusion (in sec)	180
BSS Max Idle Service	Enabled
Client user idle timeout (in sec)	300
Directed Multicast Service	Enabled
Neighbor List	Enabled
MFP Client Protection	Optional ⓘ

Note that only guest SSID will be created on anchor WLC

Day 2 Example - IRCM Guest Anchoring Provision Anchor WLC(s)

C9800s as both Foreign and Anchor



DEVICES (4)

FOCUS: Provision

Global

DEVICE TYPE: All | Routers | Switches | APs | WLCs

REACHABILITY: All | Reachable | Unreachable

□	Device Name	IP Address	Device Family	Site	Reachability	Provision Status	Credential Status			
□	penxu-C9800-3	10.254.12.22	Wireless Controller	.../SJC/SJC03	Reachable	Configuring See Details	Not Prov			8:37:
□	penxu-C9800-4	10.254.12.23	Wireless Controller	.../SJC/SJC04	Reachable	Configuring See Details	N			d:19:
□	penxu-C9800-5	10.254.12.24	Wireless Controller	.../SJC/SJC05	Reachable	Configuring See Details	Not Provisioned	a few seconds ago	ACCESS	00:1e:bd:78:7a:
□	SJC04-F1-AP1	10.254.17.54	Unified AP	.../SJC04/SJC04-F1	Reachable	Success See Details	Not Provisioned	17 hours ago	ACCESS	f4:db:e6:46:28:

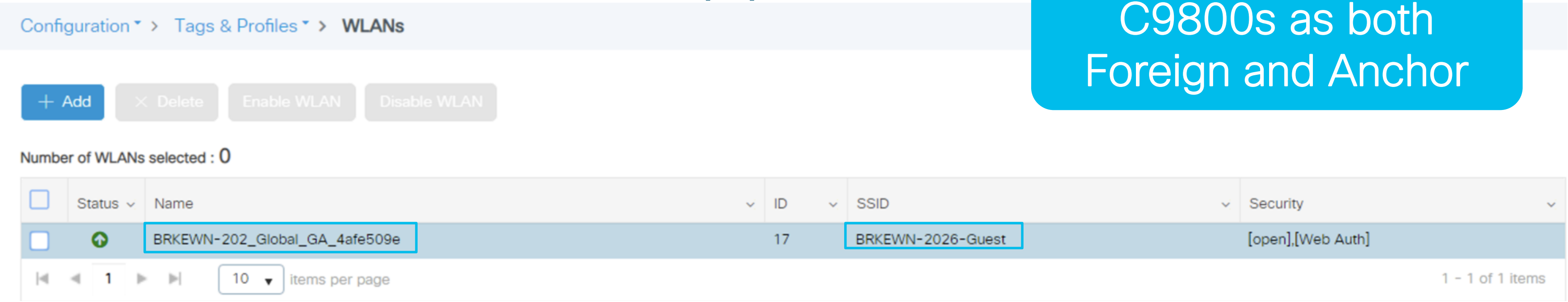
Why?

- Enable guest WLAN and create anchor configuration on foreign WLC
- Create guest WLAN and anchor configuration
- Create mobility peers on both foreign and anchor WLCs

cisco Live!

Day 2 Example- IRCM Guest Anchoring Provision Anchor WLC(s)

C9800s as both Foreign and Anchor

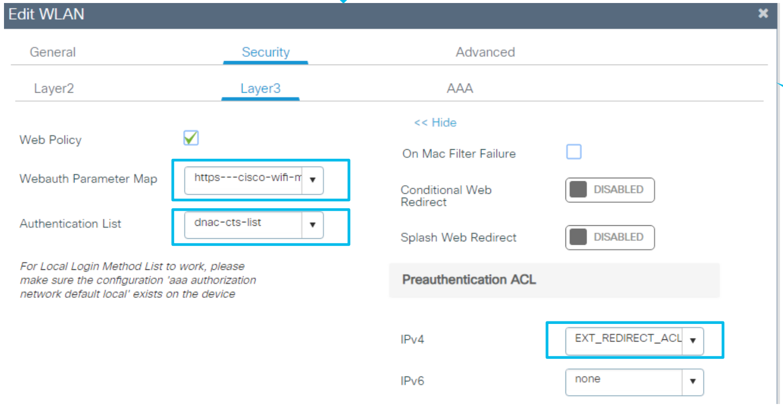


Number of WLANs selected : 0

□	Status	Name	ID	SSID	Security
□	●	BRKEWN-202_Global_GA_4afe509e	17	BRKEWN-2026-Guest	[open],[Web Auth]

1 | 10 items per page | 1 - 1 of 1 items

On Anchor



Web Policy ☑

Webauth Parameter Map: https---cisco-wifi-m

Authentication List: dnac-cts-list

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

On Mac Filter Failure □

Conditional Web Redirect: DISABLED

Splash Web Redirect: DISABLED

Preauthentication ACL

IPv4: EXT_REDIRECT_ACL

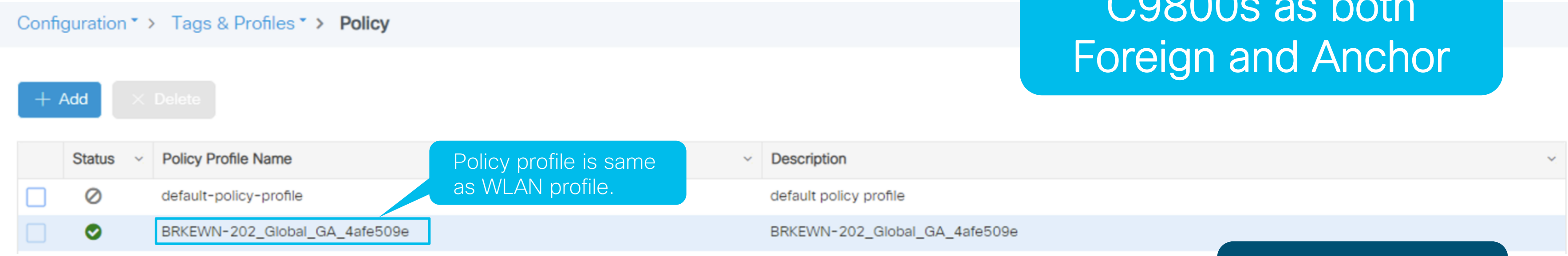
IPv6: none

What else in WLAN?

- Webauth Parameter Map
- Authentication List
- Preauthentication ACL

Day 2 Example - IRCM Guest Anchoring Provision Anchor WLC(s)

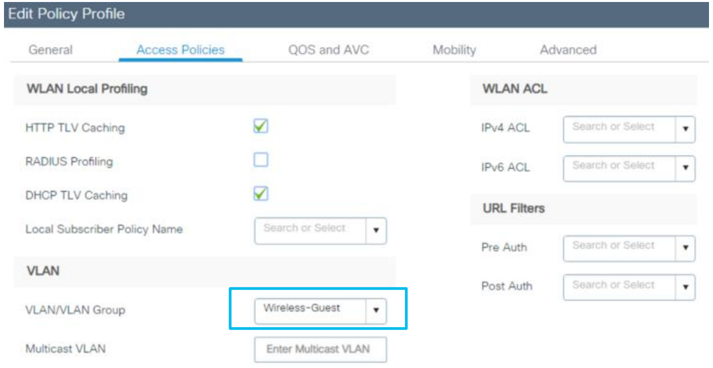
C9800s as both Foreign and Anchor



	Status	Policy Profile Name	Description
□	⊘	default-policy-profile	default policy profile
□	✓	BRKEWN-202_Global_GA_4afe509e	BRKEWN-202_Global_GA_4afe509e

Policy profile is same as WLAN profile.

On Anchor



WLAN Local Profiling

HTTP TLV Caching ☑

RADIUS Profiling □

DHCP TLV Caching ☑

Local Subscriber Policy Name: Search or Select ▾

VLAN

VLAN/VLAN Group: Wireless-Guest ▾

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

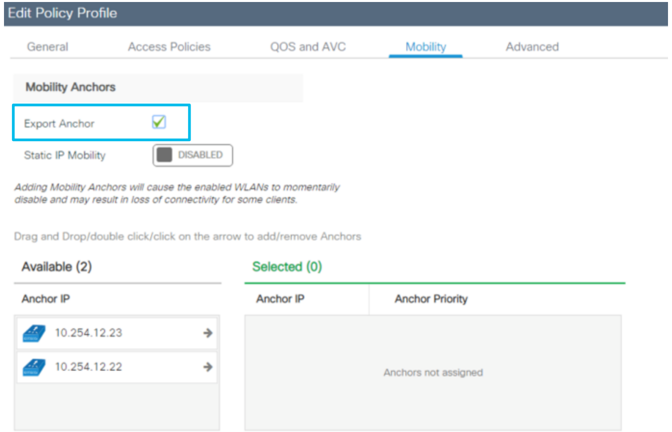
IPv4 ACL: Search or Select ▾

IPv6 ACL: Search or Select ▾

URL Filters

Pre Auth: Search or Select ▾

Post Auth: Search or Select ▾



Mobility Anchors

Export Anchor ☑

Static IP Mobility: DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)

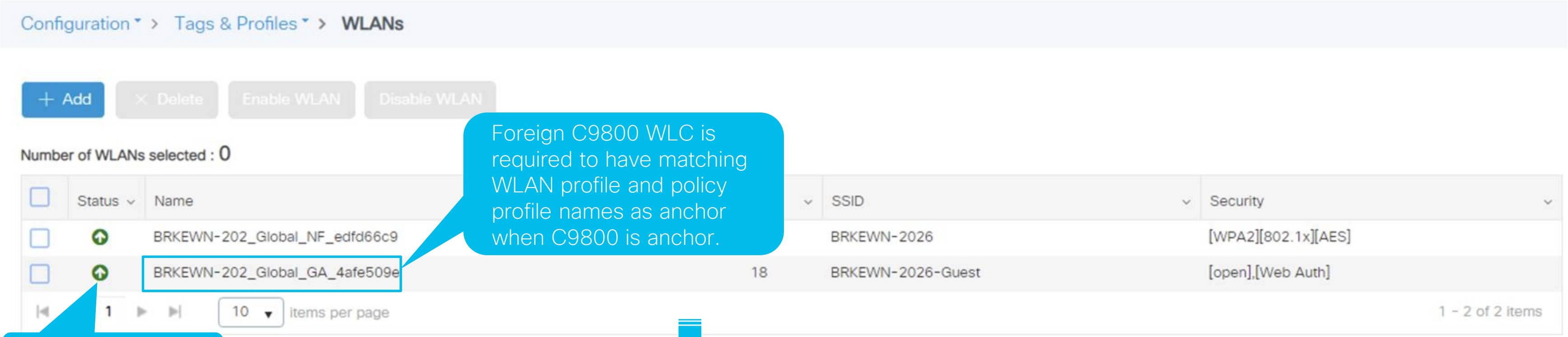
Anchor IP
10.254.12.23 →
10.254.12.22 →

Selected (0)

Anchor IP	Anchor Priority
Anchors not assigned	

Day 2 Example - IRCM Guest Anchoring Provision Anchor WLC(s)

C9800s as both Foreign and Anchor



Configuration ˅ > Tags & Profiles ˅ > **WLANs**

Number of WLANs selected : 0

□	Status	Name		SSID	Security
□	●	BRKEWN-202_Global_NF_edfd66c9		BRKEWN-2026	[WPA2][802.1x][AES]
□	●	BRKEWN-202_Global_GA_4afe509e	18	BRKEWN-2026-Guest	[open],[Web Auth]

1 · 10 items per page · 1 - 2 of 2 items

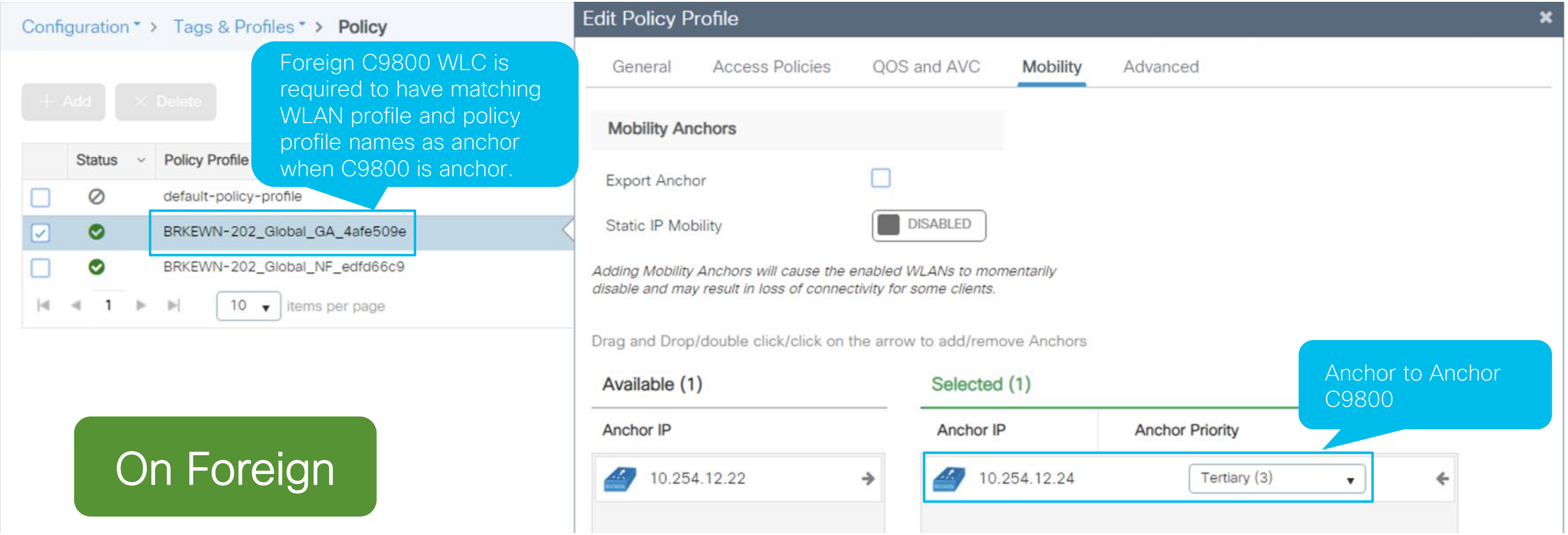
Foreign C9800 WLC is required to have matching WLAN profile and policy profile names as anchor when C9800 is anchor.

it is enabled now.

On Foreign

Day 2 Example - IRCM Guest Anchoring Provision Anchor WLC(s)

C9800s as both Foreign and Anchor



Configuration ˅ > Tags & Profiles ˅ > Policy

	Status	Policy Profile
□	⊘	default-policy-profile
☑	✓	BRKEWN-202_Global_GA_4afe509e
□	✓	BRKEWN-202_Global_NF_edfd66c9

1 · 10 items per page

Foreign C9800 WLC is required to have matching WLAN profile and policy profile names as anchor when C9800 is anchor.

Edit Policy Profile

General · Access Policies · QOS and AVC · **Mobility** · Advanced

Mobility Anchors

Export Anchor □

Static IP Mobility: DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)

Anchor IP
10.254.12.22 →

Selected (1)

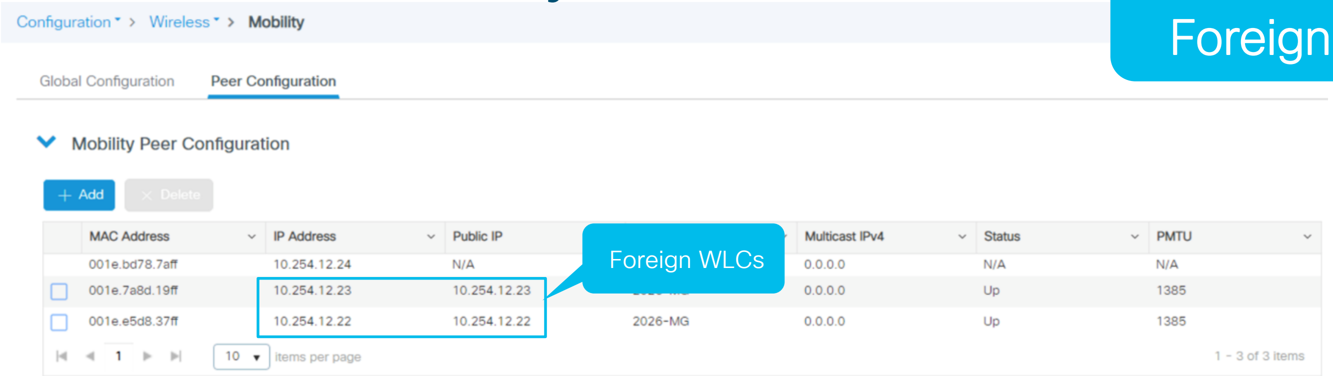
Anchor IP	Anchor Priority
10.254.12.24	Tertiary (3)

Anchor to Anchor C9800

On Foreign

Day 2 Example – IRCM Guest Anchoring Provision Mobility Peers

C9800s as both Foreign and Anchor



Configuration ˅ > Wireless ˅ > **Mobility**

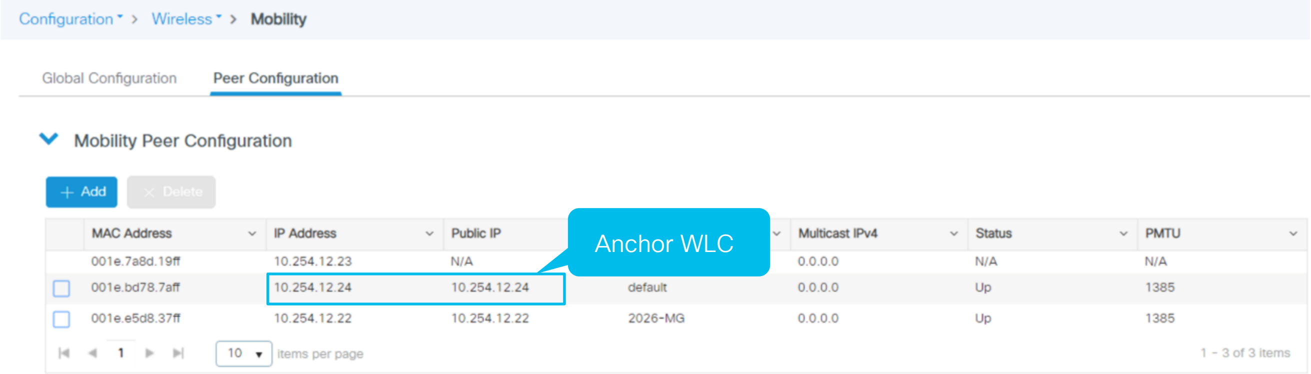
Global Configuration | **Peer Configuration**

Mobility Peer Configuration

	MAC Address	IP Address	Public IP		Multicast IPv4	Status	PMTU
	001e.bd78.7aff	10.254.12.24	N/A		0.0.0.0	N/A	N/A
□	001e.7a8d.19ff	10.254.12.23	10.254.12.23	[illegible]	0.0.0.0	Up	1385
□	001e.e5d8.37ff	10.254.12.22	10.254.12.22	2026-MG	0.0.0.0	Up	1385

Foreign WLCs

On Anchor



Configuration ˅ > Wireless ˅ > **Mobility**

Global Configuration | **Peer Configuration**

Mobility Peer Configuration

	MAC Address	IP Address	Public IP		Multicast IPv4	Status	PMTU
	001e.7a8d.19ff	10.254.12.23	N/A		0.0.0.0	N/A	N/A
□	001e.bd78.7aff	10.254.12.24	10.254.12.24	default	0.0.0.0	Up	1385
□	001e.e5d8.37ff	10.254.12.22	10.254.12.22	2026-MG	0.0.0.0	Up	1385

Anchor WLC

On Foreign

Demo- Day 2

Implement Foreign and Anchor Guest Solution

Deployment Models

Same Workflows for Different Wireless Branch Deployments

Centralized

Ease of Deployment and management

Flex Connect

Eliminate the need for a Controller at every Site

EWC/ME

Controller Functionality Embedded in the Access Point

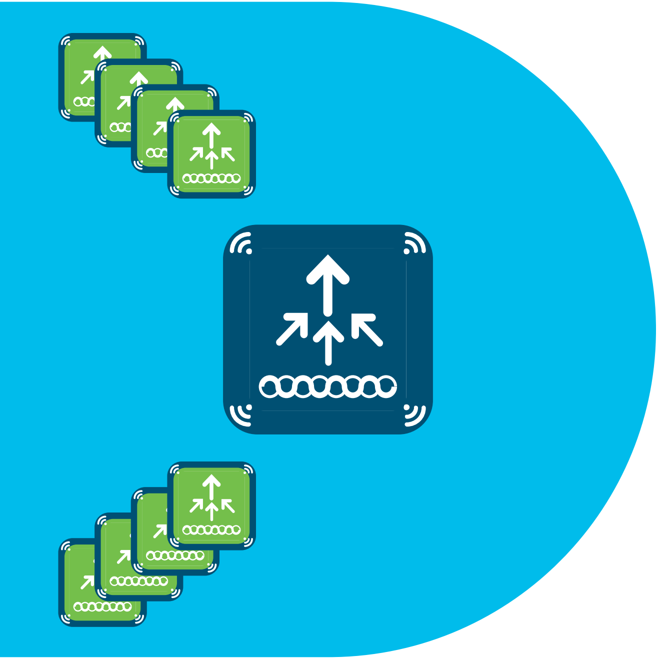
Catalyst 9800

Next Gen Wireless Stack

Embedded Wireless Controller on Catalyst Access Points

EWC on Cisco Catalyst Access Points

Ready for enterprise deployments



Runs 9800 Series Cisco IOS® XE wireless controller on Cisco Catalyst access points	Modern OS, scalable, open and programmable, supports telemetry
Supports advanced enterprise feature set	HA, SMU, adaptive wireless IPS (aWIPS), Cisco Umbrella™, NetFlow, ICAP
Flexible management options	Use mobile app, WebUI, and Cisco DNA Center to deploy, manage, and monitor
Investment protection	Migrate access points to controller for more than 100 access points

EWC on Cisco Catalyst 9100 Access Points

Ideal for single or multisite small to medium-sized enterprise deployments

Mission critical

Best in class

Best suited for high-density enterprise branch deployments

C9115AX-EWC

- 50 APs, 1000 clients
- 4x4 + 4x4
- MU-MIMO, OFDMA
- Spectrum Intelligence
- Bluetooth 5
- 1x 2.5 Multigigabit
- USB
- Integrated or external antenna

C9117AX-EWC

- 50 APs, 1000 clients
- 8x8 + 4x4
- MU-MIMO, OFDMA (only DL)
- Spectrum Intelligence
- Bluetooth 5
- 1x 5 Multigigabit
- USB
- Integrated antenna only

✓ Powered by Cisco RF ASIC

C9120AX-EWC

- 100 APs, 2000 clients
- 4x4 + 4x4
- MU-MIMO, OFDMA
- Cisco RF ASIC
- Dual 5 GHz, HDX
- RF signature capture
- 1x 2.5 Multigigabit
- Integrated or external antenna

✓ Powered by Cisco RF ASIC

C9130AX-EWC

- 100 APs, 2000 clients
- 8x8 + 4x4 or 4x4 + 4x4 + 4x4
- Tri-radio (dual 5 GHz + 2.4 GHz), HDX
- Cisco RF ASIC
- RF signature capture
- Decrypted data packet ICAP
- 1x 5 Multigigabit
- 8-port smart antennas

Software feature parity across APs

Supports up to 100 APs, 2000 clients

Supports Wave 2 APs as client serving

Cisco DNA Assurance with ICAP

EWC Automation Key Points

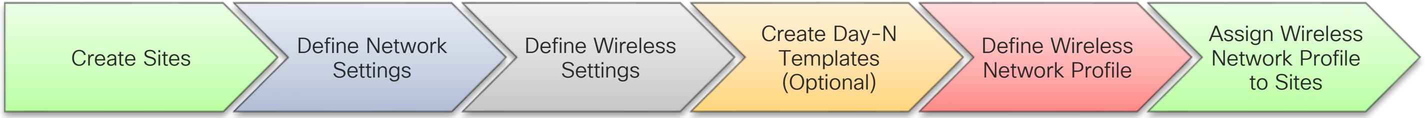
Supported

- EWC Release 16.12.2 and above
- Cisco DNA Center Release 1.3.3
- Profile-based Design and Provision
- For PnP, support only EWC APs running on the same AP base image
- Only Day-N CLI Templates

Not Supported

- EWC Day-0 templates via PnP
- EWC Image upgrade via PnP

EWC Design Workflow


Create Sites
Define Network Settings
Define Wireless Settings
Create Day-N Templates (Optional)
Define Wireless Network Profile
Assign Wireless Network Profile to Sites

EWC design workflow is exactly same as wireless controller.

EWC Onboarding Workflow

Step 0 Plan for PnP Discovery

- DHCP Option 43 or DNS for EWC to discover Cisco DNA Center
- Switch port connecting to EWC should be trunk with management VLAN of EWC as native VLAN
- Only master EWC AP will call home to Cisco DNA Center in case of multiple EWCs

Step 1 Onboard

- Part 1- PnP Claim
  - Device Credentials of Profile
  - Management IP and Default GW
  - Hostname
- Part 2- Add to Inventory
  - Network Settings of Profile
  - Enable wireless assurance
  - Remove day-0 default EWC config (e.g. day-0 banner, webui login, CiscoAirProvision SSID)
  - SSIDs of Profile

Step 2 Complete Profile Provisioning

- Provision Day-N CLI Template(s) (Optional)

Step 3 Provision EWC APs

On EWC:

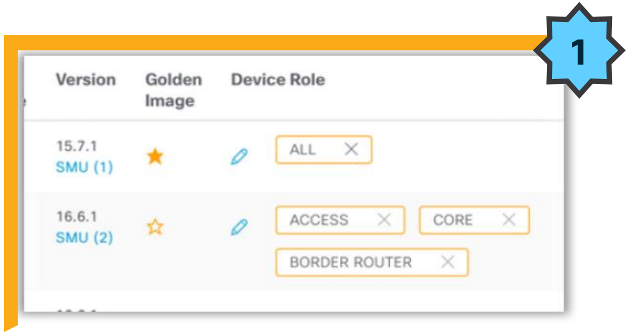
- Create native VLAN and WLAN to VLAN mappings in default flex profile
- Create policy and RF tags
- Assign policy and RF tags to APs

On Cisco DNA Center:

- Place EWC APs on map

Software Image Upgrade (SWIM)

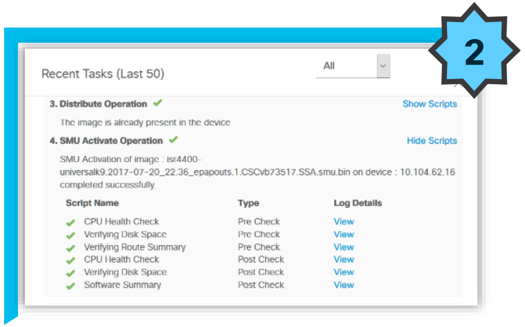
Core Principles of Software Upgrade with DNA Center



Version	Golden Image	Device Role
15.7.1 SMU (1)	★	ALL
16.6.1 SMU (2)	☆	ACCESS CORE BORDER ROUTER

Intent based Network Upgrades

Standardization of Software by Network device role, device type and location



Recent Tasks (Last 50)

3. Distribute Operation ✓

The image is already present in the device

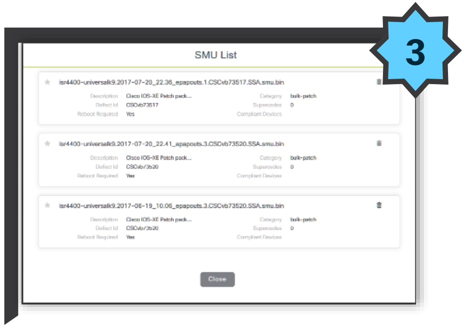
4. SMU Activate Operation ✓

SMU Activation of image : isr4400-universalk9.2017-07-20_22.36_epapouts.1.CSCvb73517.SSA.smu.bin on device : 10.104.62.16 completed successfully

Script Name	Type	Log Details
✓ CPU Health Check	Pre Check	View
✓ Verifying Disk Space	Pre Check	View
✓ Verifying Route Summary	Pre Check	View
✓ CPU Health Check	Post Check	View
✓ Verifying Disk Space	Post Check	View
✓ Software Summary	Post Check	View

Seamless Upgrades

Pre/Post check validations with rollback provide confidence for upgrades



SMU List

isr4400-universalk9.2017-07-20_22.36_epapouts.1.CSCvb73517.SSA.smu.bin

Description	Cisco IOS-XE Patch pack...	Category	bulk-patch
Defect Id	CSCvb73517	Supercedes	0
Reboot Required	Yes	Compliant Devices	

isr4400-universalk9.2017-07-20_22.41_epapouts.3.CSCvb73520.SSA.smu.bin

Description	Cisco IOS-XE Patch pack...	Category	bulk-patch
Defect Id	CSCvb73520	Supercedes	0
Reboot Required	Yes	Compliant Devices	

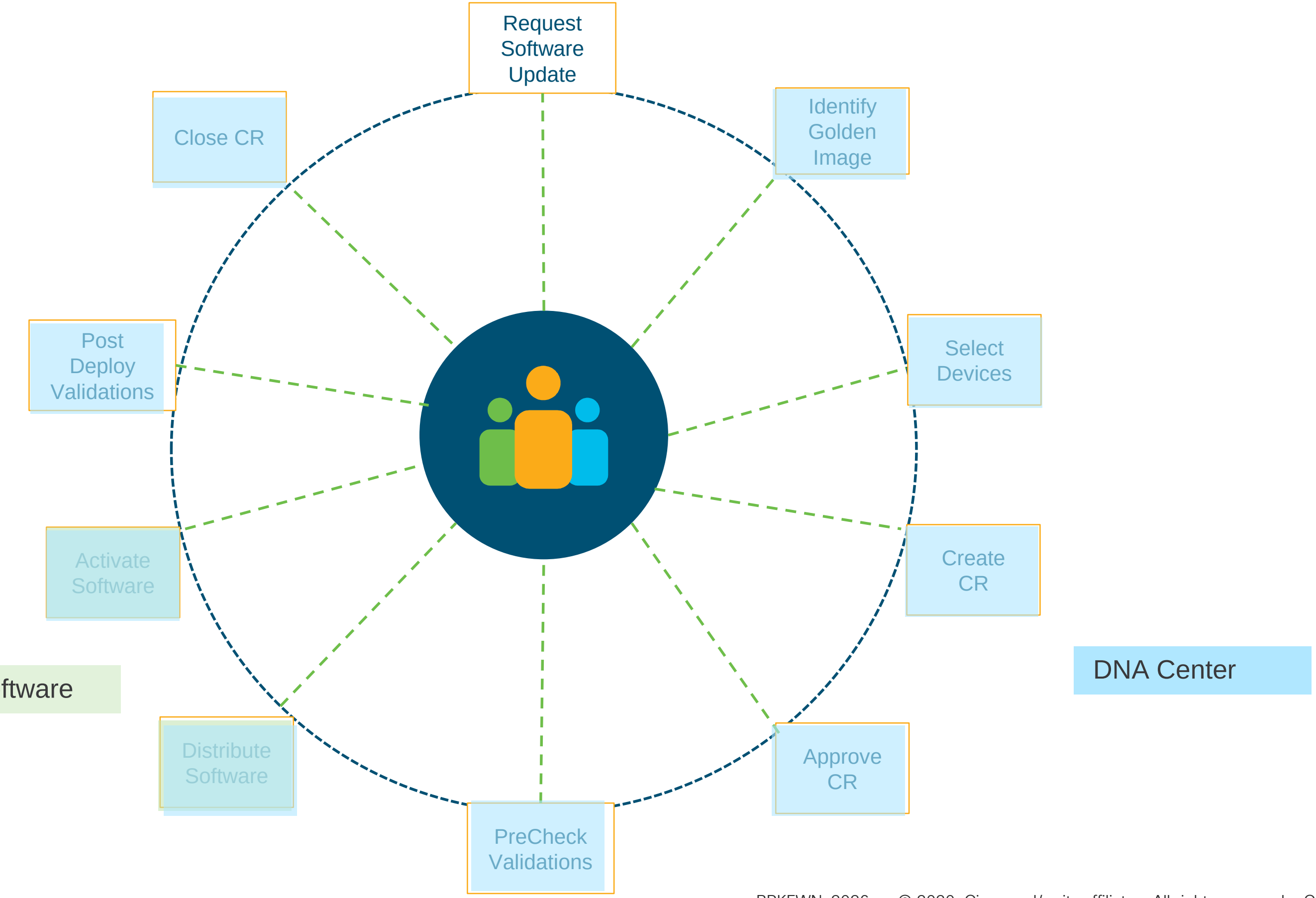
isr4400-universalk9.2017-06-19_10.06_epapouts.3.CSCvb73520.SSA.smu.bin

Description	Cisco IOS-XE Patch pack...	Category	bulk-patch
Defect Id	CSCvb73520	Supercedes	0
Reboot Required	Yes	Compliant Devices	

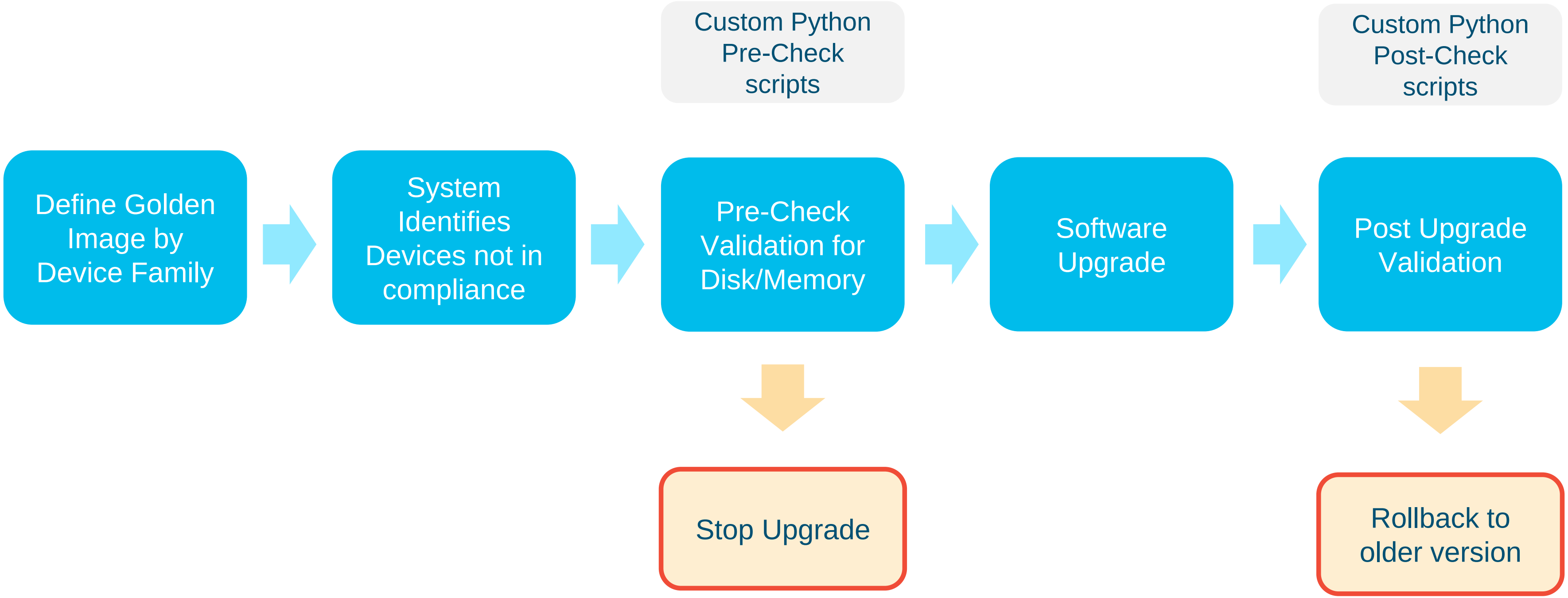
Reduce Downtime with Patching

Upgrade only what is needed with minimal to zero downtime

Software Upgrade Process



DNA Center - Software Update Workflow



Custom Python Pre-Check scripts

Custom Python Post-Check scripts

Define Golden Image by Device Family

System Identifies Devices not in compliance

Pre-Check Validation for Disk/Memory

Software Upgrade

Post Upgrade Validation

Stop Upgrade

Rollback to older version

Defining Golden Image

Device Family

- Golden image per device family
- Device family includes router, switches and wireless (WLC)

Device Role

- Devices in the same family classified by role
- Ex: CAT3850 as a access switch vs distribution switch

Site Override

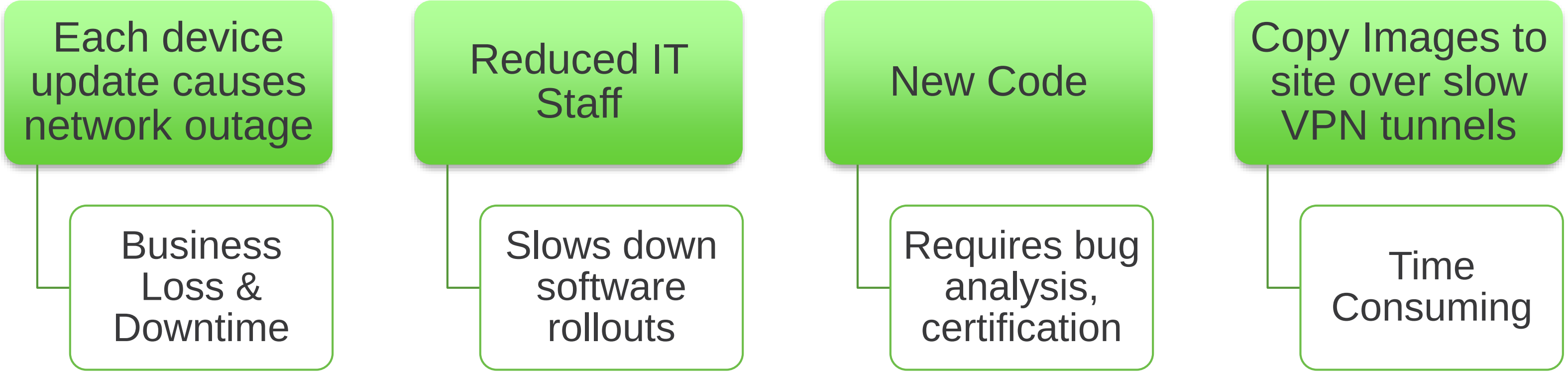
- Golden Images can be overridden at a site level
- Ex: Amer uses v16.1 vs APJC uses v3.8

SMU (Software Maintenance Upgrade)

What is SMU ?

- Point Fixes for the IOS-XE images (16.x onwards)
- Provides the ability to just update what is needed

Why SMU ?



Each device update causes network outage

Business Loss & Downtime

Reduced IT Staff

Slows down software rollouts

New Code

Requires bug analysis, certification

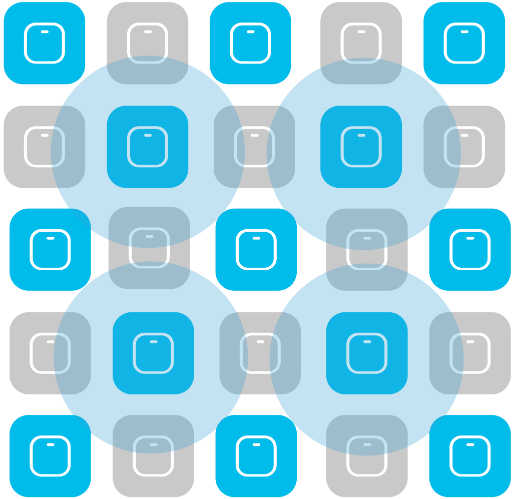
Copy Images to site over slow VPN tunnels

Time Consuming

Rolling AP Upgrade

Use Case: Upgrading AP's in a Staggered way to achieve Zero Down Time of the Network.

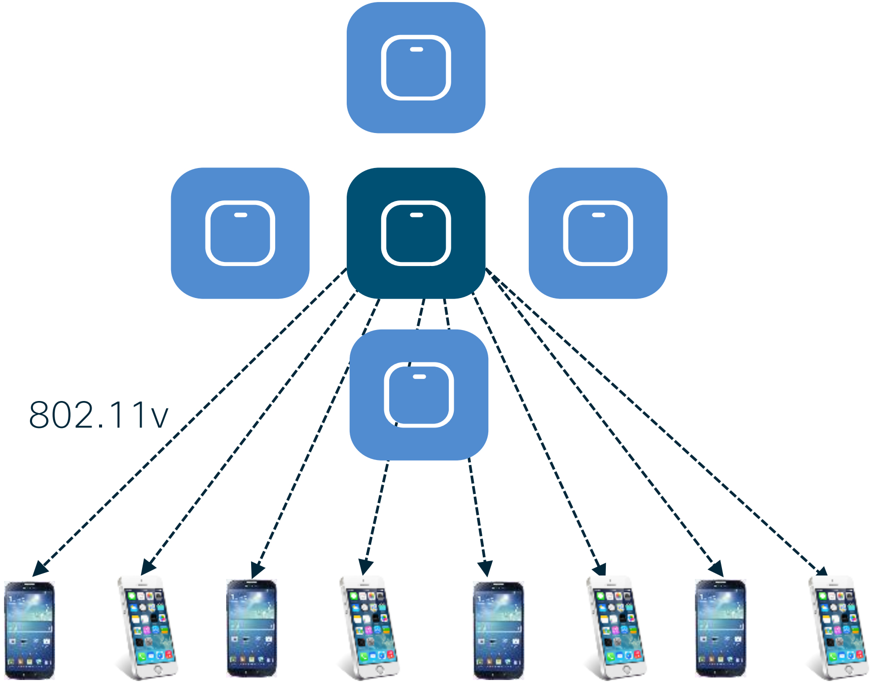
Rolling AP Upgrade – RRM Based Candidate AP Selection



User selects % of APs to upgrade in one go [5, 15, 25]
For 25%, Neighbors marked = 6 [Expected number of iterations ~ 5]
For 15%, Neighbors marked = 12 [Expected number of iterations ~ 12]
For 5%, Neighbors marked = 24 [Expected number of iterations ~ 22]

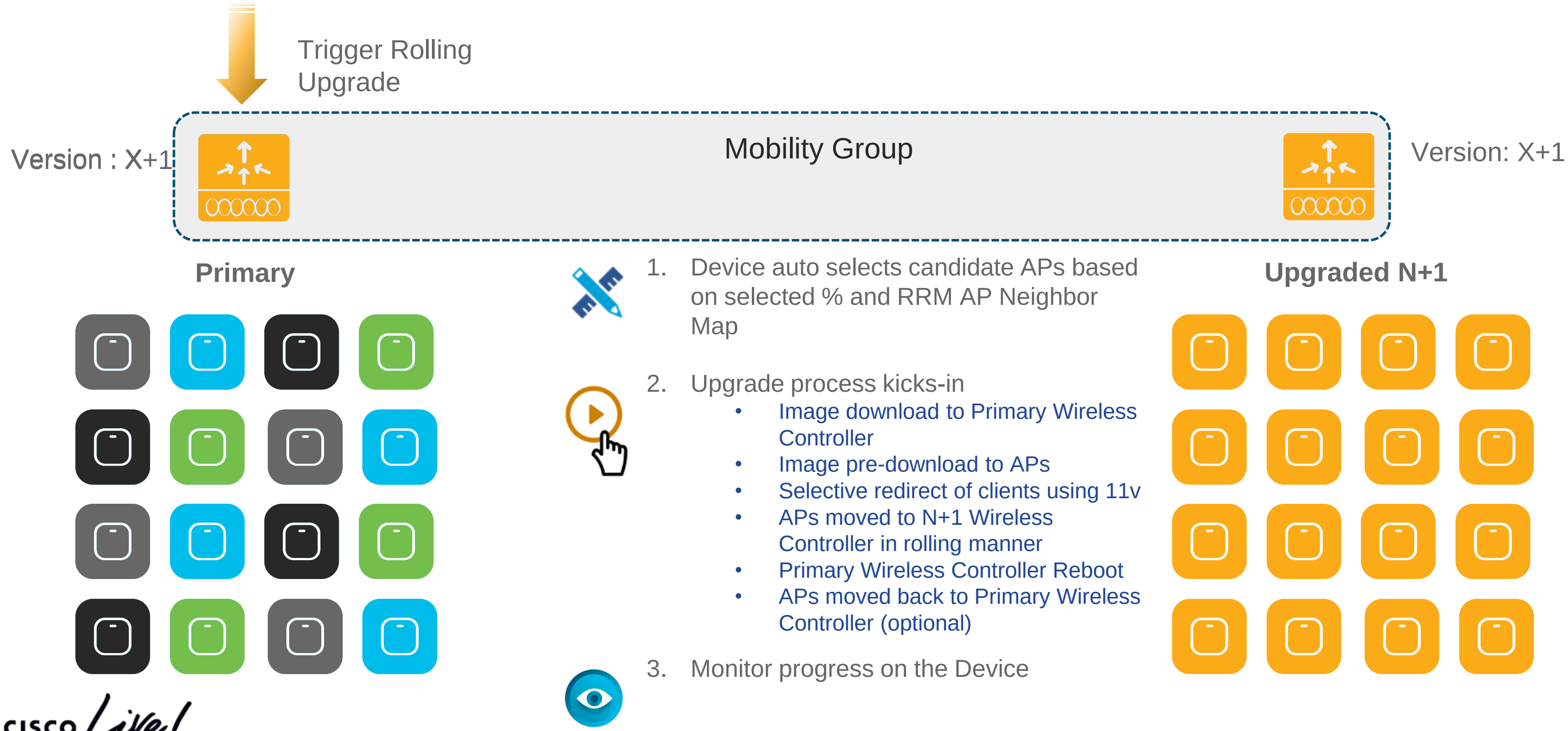
Rolling AP Upgrade - Client Steering

- Clients steered from candidate APs to non-candidate APs
- 802.11v BSS Transition Request
- Dissociation imminent
- If clients do not honor this, they will be de-authenticated before AP reload



N+1 Rolling AP Upgrade

- Wireless Controller image upgrade using N+1 staging Controller



Trigger Rolling Upgrade

Version : X+1

Mobility Group

Version: X+1

Primary

Upgraded N+1

1. Device auto selects candidate APs based on selected % and RRM AP Neighbor Map

2. Upgrade process kicks-in
   - Image download to Primary Wireless Controller
   - Image pre-download to APs
   - Selective redirect of clients using 11v
   - APs moved to N+1 Wireless Controller in rolling manner
   - Primary Wireless Controller Reboot
   - APs moved back to Primary Wireless Controller (optional)

3. Monitor progress on the Device

Rolling AP Upgrade Workflow prerequisites

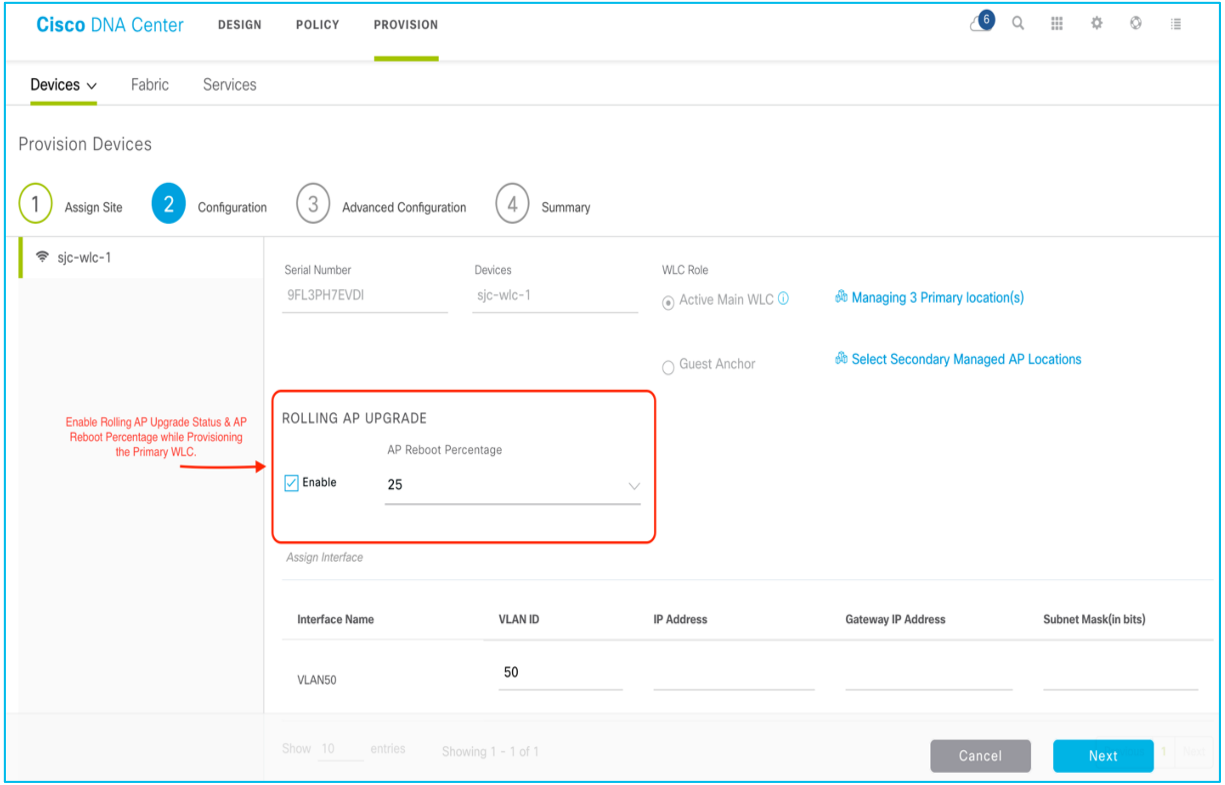
- **Making N+1 WLC is Ready** : The N+1 WLC should be running the same configuration as the Primary WLC in terms of the WLANs and policies. For this reason, the config design of primary WLC should be replicated on the N+1 WLC as a first step.

- **Mobility Tunnel :** The Primary WLC and N+1 WLC should be part of same Mobility Group and the Mobility Tunnel should be UP between the two before initiating the Rolling AP upgrade process

- N+1 WLC should be running on Golden image before starting the Rolling AP upgrade.

- The Rolling AP Upgrade workflow is Only Supported with Catalyst 9800 Wireless Controller

Rolling AP Upgrade Workflow



Provision Devices

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

sjc-wlc-1

Serial Number: 9FL3PH7EVDI

Devices: sjc-wlc-1

WLC Role: ● Active Main WLC ○ Guest Anchor

Managing 3 Primary location(s)

Select Secondary Managed AP Locations

ROLLING AP UPGRADE

☑ Enable

AP Reboot Percentage: 25

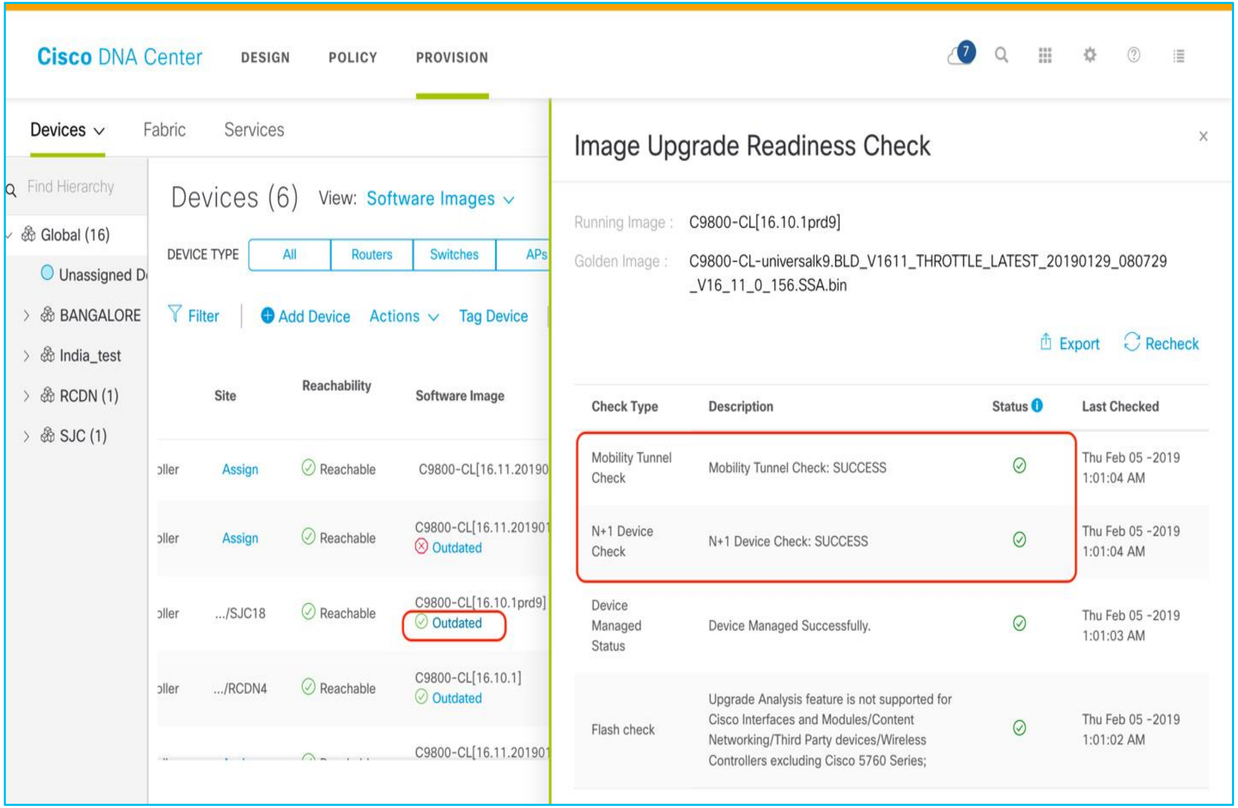
Enable Rolling AP Upgrade Status & AP Reboot Percentage while Provisioning the Primary WLC.

Assign Interface

Interface Name	VLAN ID	IP Address	Gateway IP Address	Subnet Mask(in bits)
VLAN50	50			

The Rolling AP Upgrades should be enabled while provisioning of the primary WLC and Need to Provide the percentage for AP reboot.

Rolling AP Upgrade Workflow



	Site	Reachability	Software Image
oller	Assign	Reachable	C9800-CL[16.11.20190
oller	Assign	Reachable	C9800-CL[16.11.201901 Outdated
oller	.../SJC18	Reachable	C9800-CL[16.10.1prd9] Outdated
oller	.../RCDN4	Reachable	C9800-CL[16.10.1] Outdated
			C9800-CL[16.11.201901

Image Upgrade Readiness Check

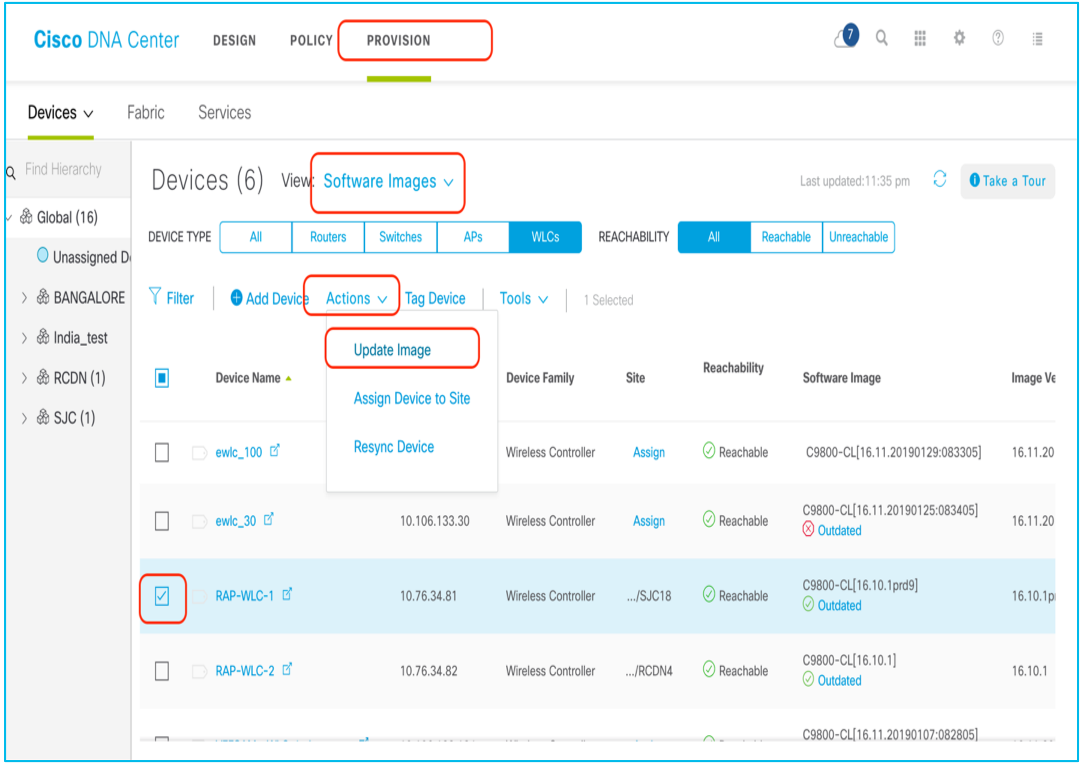
Running Image : C9800-CL[16.10.1prd9]

Golden Image : C9800-CL-universalk9.BLD_V1611_THROTTLE_LATEST_20190129_080729_V16_11_0_156.SSA.bin

Check Type	Description	Status	Last Checked
Mobility Tunnel Check	Mobility Tunnel Check: SUCCESS	✓	Thu Feb 05 -2019 1:01:04 AM
N+1 Device Check	N+1 Device Check: SUCCESS	✓	Thu Feb 05 -2019 1:01:04 AM
Device Managed Status	Device Managed Successfully.	✓	Thu Feb 05 -2019 1:01:03 AM
Flash check	Upgrade Analysis feature is not supported for Cisco Interfaces and Modules/Content Networking/Third Party devices/Wireless Controllers excluding Cisco 5760 Series;	✓	Thu Feb 05 -2019 1:01:02 AM

Check the Image upgrade readiness check to confirm if WLC is meeting Prerequisites.

Rolling AP Upgrade Workflow



Devices (6) View: Software Images

Last updated:11:35 pm

DEVICE TYPE: All | Routers | Switches | APs | **WLCs**

REACHABILITY: **All** | Reachable | Unreachable

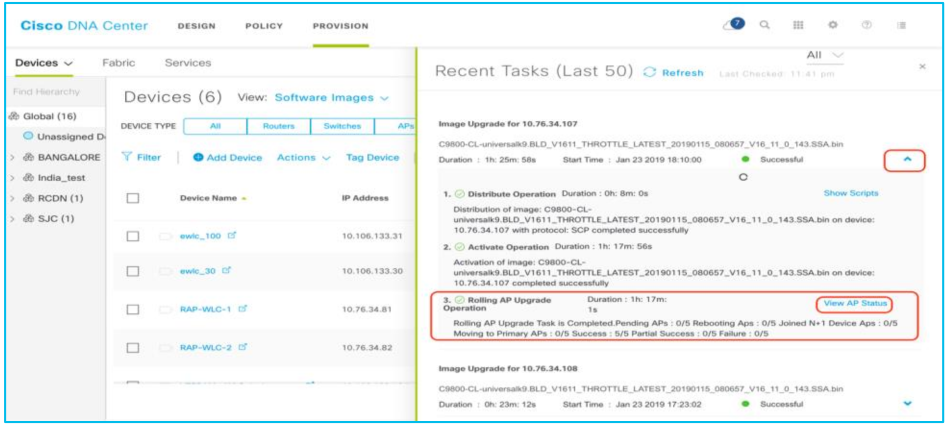
1 Selected

	Device Name ▲		Device Family	Site	Reachability	Software Image	Image Ve
□	ewlc_100		Wireless Controller	Assign	Reachable	C9800-CL[16.11.20190129:083305]	16.11.20
□	ewlc_30	10.106.133.30	Wireless Controller	Assign	Reachable	C9800-CL[16.11.20190125:083405] Outdated	16.11.20
☑	RAP-WLC-1	10.76.34.81	Wireless Controller	.../SJC18	Reachable	C9800-CL[16.10.1prd9] Outdated	16.10.1p
□	RAP-WLC-2	10.76.34.82	Wireless Controller	.../RCDN4	Reachable	C9800-CL[16.10.1] Outdated	16.10.1
						C9800-CL[16.11.20190107:082805]	

Select the Primary WLC to update Image

Rolling AP Upgrade Workflow

- Once the upgrade process started, Rolling AP Upgrade will get triggered and AP’s will be upgraded In a staggered way based on the AP reboot percentage provided.



Device Name	IP Address
ewlc_100	10.106.133.31
ewlc_30	10.106.133.30
RAP-WLC-1	10.76.34.81
RAP-WLC-2	10.76.34.82

Recent Tasks (Last 50)

Image Upgrade for 10.76.34.107

C9800-CL-universalk9.BLD_V1611_THROTTLE_LATEST_20190115_080657_V16_11_0_143.SSA.bin

Duration : 1h: 25m: 58s Start Time : Jan 23 2019 18:10:00 ● Successful

1. **Distribute Operation** Duration : 0h: 8m: 0s

   Distribution of image: C9800-CL-universalk9.BLD_V1611_THROTTLE_LATEST_20190115_080657_V16_11_0_143.SSA.bin on device: 10.76.34.107 with protocol: SCP completed successfully

2. **Activate Operation** Duration : 1h: 17m: 56s

   Activation of image: C9800-CL-universalk9.BLD_V1611_THROTTLE_LATEST_20190115_080657_V16_11_0_143.SSA.bin on device: 10.76.34.107 completed successfully

3. **Rolling AP Upgrade Operation** Duration : 1h: 17m: 1s

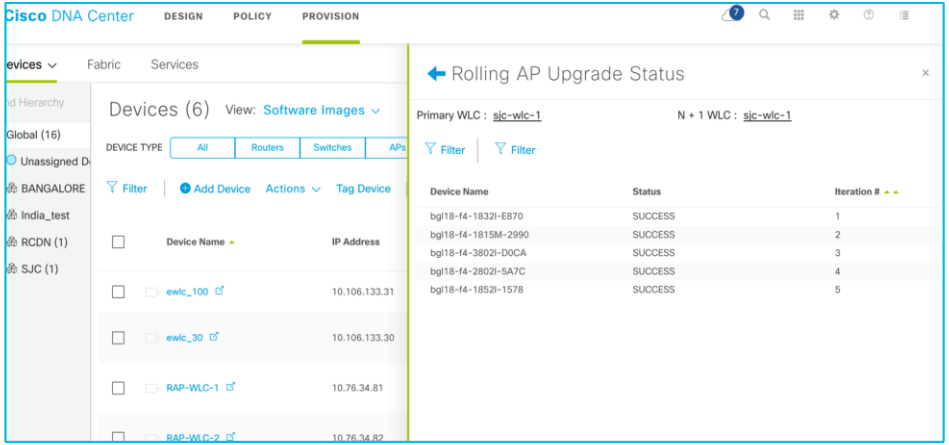
   Rolling AP Upgrade Task is Completed.Pending APs : 0/5 Rebooting Aps : 0/5 Joined N+1 Device Aps : 0/5 Moving to Primary APs : 0/5 Success : 5/5 Partial Success : 0/5 Failure : 0/5

Image Upgrade for 10.76.34.108

C9800-CL-universalk9.BLD_V1611_THROTTLE_LATEST_20190115_080657_V16_11_0_143.SSA.bin

Duration : 0h: 23m: 12s Start Time : Jan 23 2019 17:23:02 ● Successful

- The Detailed View provides the AP’s which got upgraded for each iteration



Device Name	IP Address
ewlc_100	10.106.133.31
ewlc_30	10.106.133.30
RAP-WLC-1	10.76.34.81
RAP-WLC-2	10.76.34.82

Rolling AP Upgrade Status

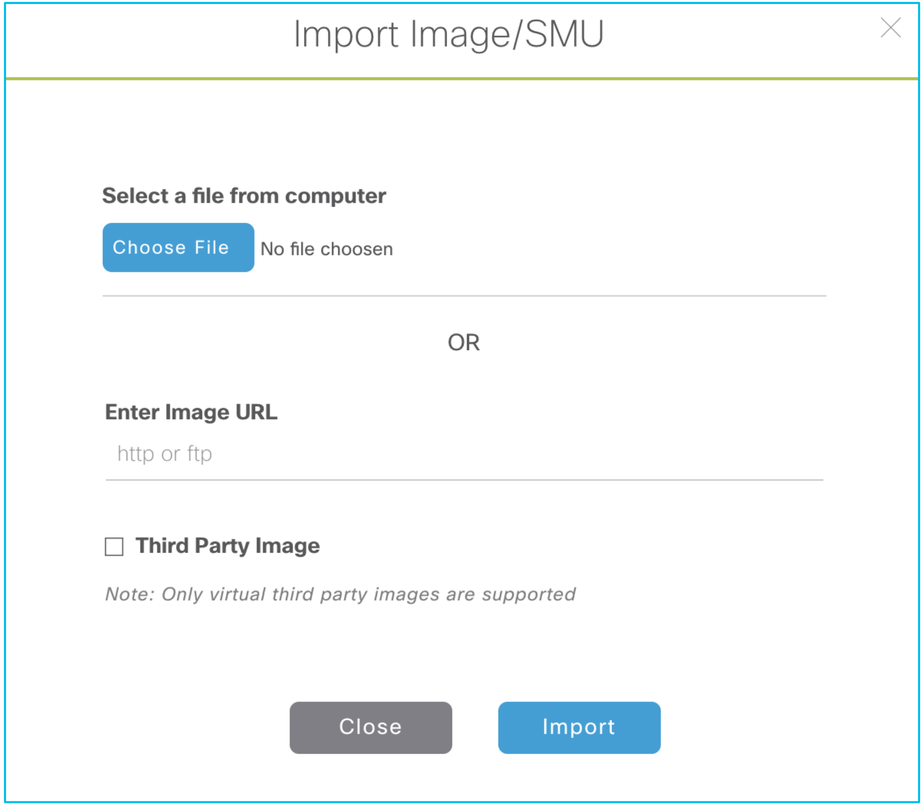
Primary WLC : sjc-wlc-1 N + 1 WLC : sjc-wlc-1

Device Name	Status	Iteration #
bgl18-f4-1832I-E870	SUCCESS	1
bgl18-f4-1815M-2990	SUCCESS	2
bgl18-f4-3802I-D0CA	SUCCESS	3
bgl18-f4-2802I-5A7C	SUCCESS	4
bgl18-f4-1852I-1578	SUCCESS	5

Demo - SWIM

Manage Software Images

- Import Images/SMU from :
  - URL(http/ftp)
  - Local PC
  - cisco.com



Import Image/SMU

Select a file from computer

No file choosen

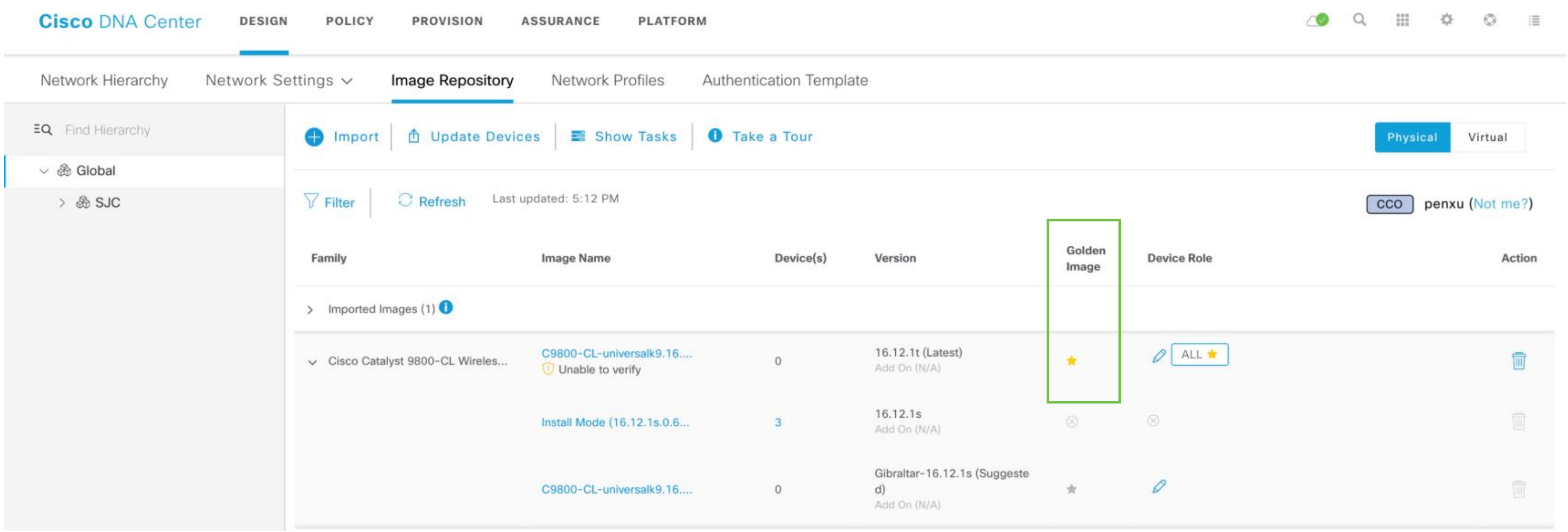
OR

Enter Image URL

□ Third Party Image

Note: Only virtual third party images are supported

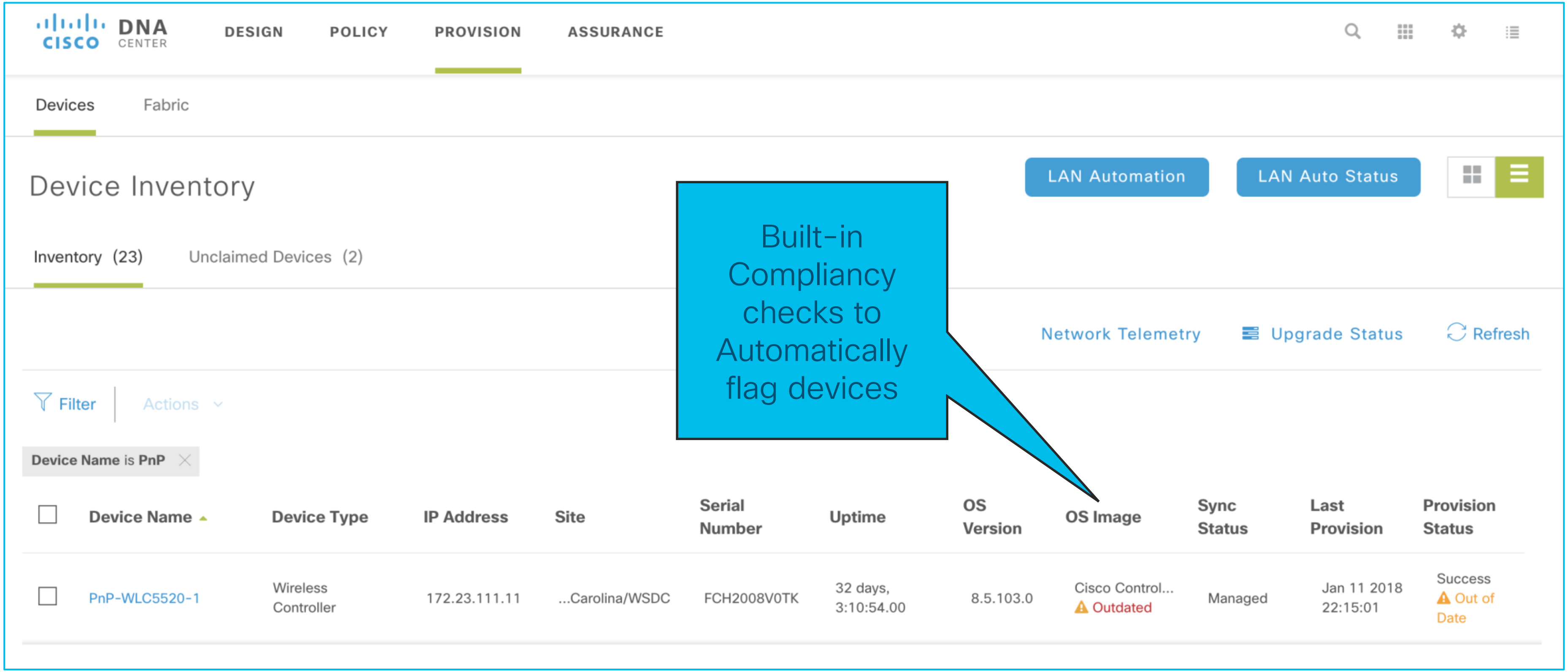
Image Standardization – “Golden Images”



Last updated: 5:12 PM

Family	Image Name	Device(s)	Version	Golden Image	Device Role	Action
Imported Images (1)						
Cisco Catalyst 9800-CL Wireles...	C9800-CL-universalk9.16.... Unable to verify	0	16.12.1t (Latest) Add On (N/A)	★	ALL ★	
	Install Mode (16.12.1s.0.6...	3	16.12.1s Add On (N/A)	⊗	⊗	
	C9800-CL-universalk9.16....	0	Gibraltar-16.12.1s (Suggested) Add On (N/A)	★		

Devices not Compliant with Golden Image



Device Inventory

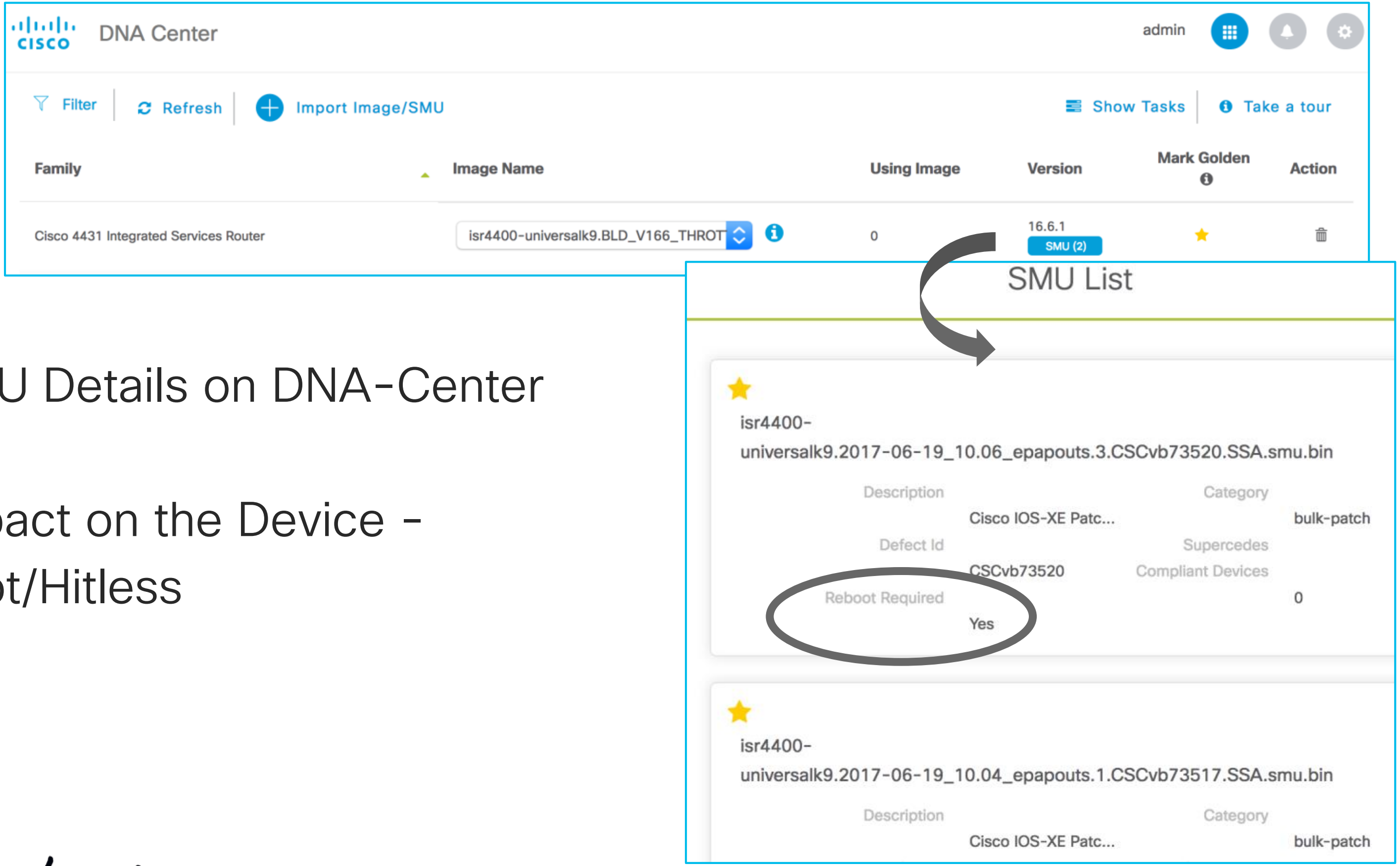
Inventory (23) Unclaimed Devices (2)

Device Name is PnP

□	Device Name	Device Type	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
□	PnP-WLC5520-1	Wireless Controller	172.23.111.11	...Carolina/WSDC	FCH2008V0TK	32 days, 3:10:54.00	8.5.103.0	Cisco Control... ⚠ Outdated	Managed	Jan 11 2018 22:15:01	Success ⚠ Out of Date

Built-in Compliancy checks to Automatically flag devices

SMU (Software Maintenance Upgrade)



Family	Image Name	Using Image	Version	Mark Golden	Action
Cisco 4431 Integrated Services Router	isr4400-universalk9.BLD_V166_THROT	0	16.6.1 SMU (2)	★	🗑

SMU List

★ isr4400-universalk9.2017-06-19_10.06_epapouts.3.CSCvb73520.SSA.smu.bin

Description: Cisco IOS-XE Patc...
Category: bulk-patch
Defect Id: CSCvb73520
Supercedes
Compliant Devices: 0
Reboot Required: Yes

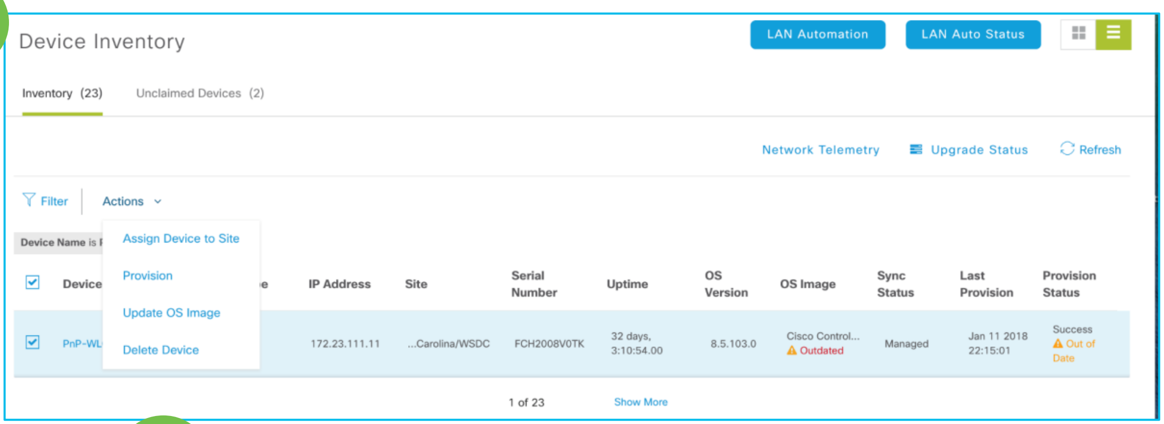
★ isr4400-universalk9.2017-06-19_10.04_epapouts.1.CSCvb73517.SSA.smu.bin

Description: Cisco IOS-XE Patc...
Category: bulk-patch

- SMU Details on DNA-Center
- Impact on the Device - Reboot/Hitless

SWIM/SMU Workflow Experience with DNA Center

1



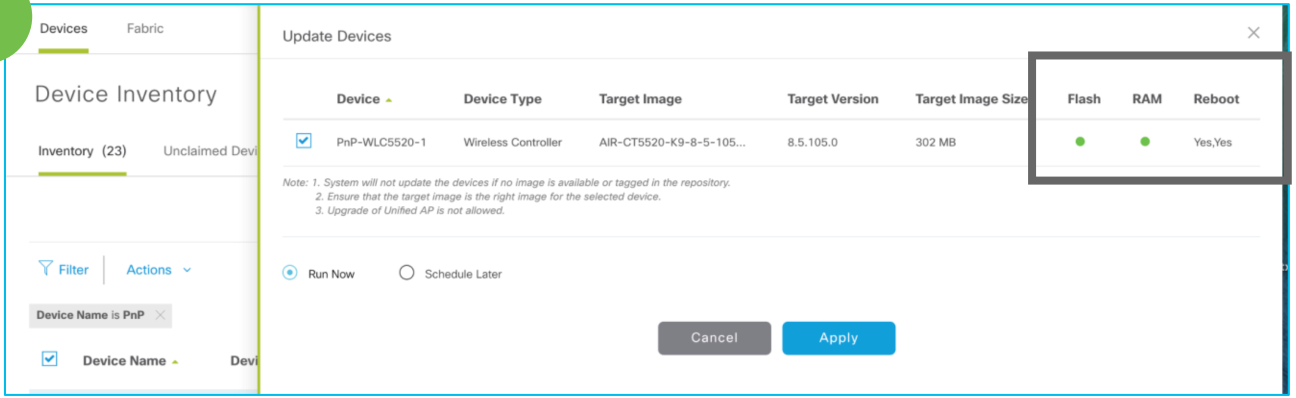
☑	Device	e	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
☑	PnP-WL		172.23.111.11	...Carolina/WSDC	FCH2008V0TK	32 days, 3:10:54.00	8.5.103.0	Cisco Control... ⚠ Outdated	Managed	Jan 11 2018 22:15:01	Success ⚠ Out of Date

1 Select device/(s) to update Image/SMU

2

- Automatic Pre-Checks done for RAM & Flash
- Abort if Pre-Check Fails

2

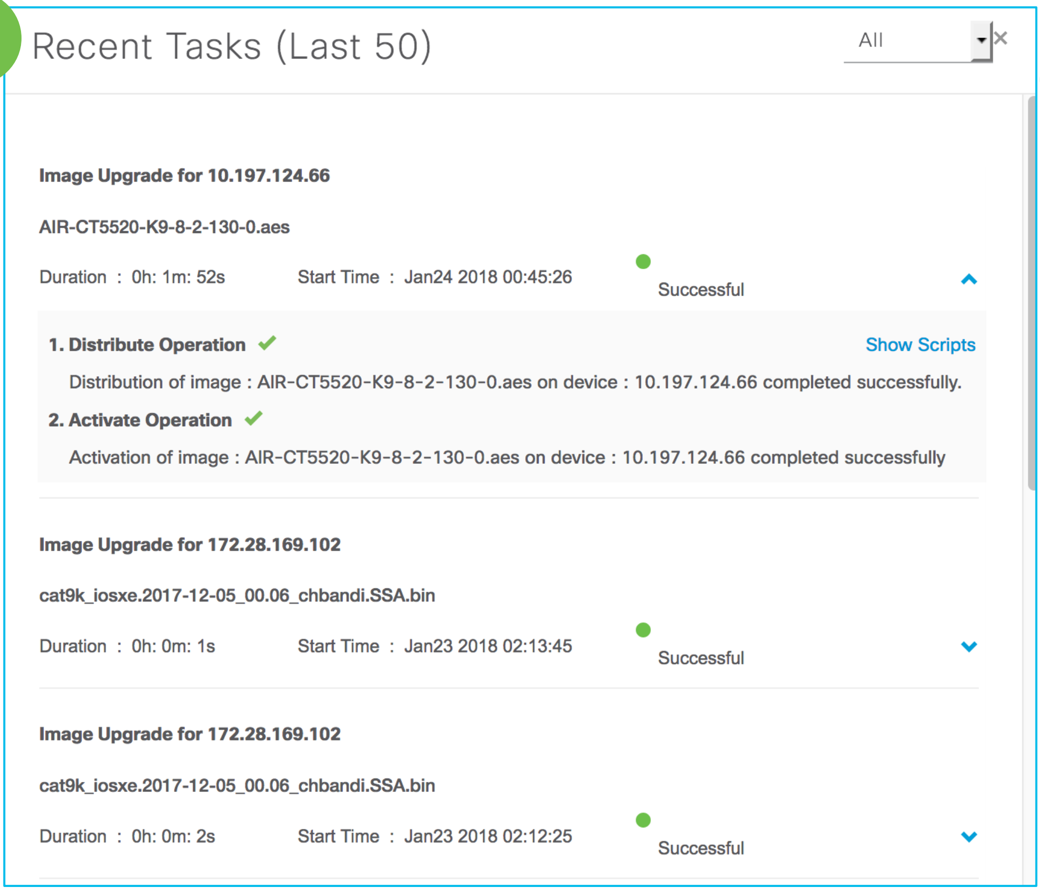


	Device	Device Type	Target Image	Target Version	Target Image Size	Flash	RAM	Reboot
☑	PnP-WLC5520-1	Wireless Controller	AIR-CT5520-K9-8-5-105...	8.5.105.0	302 MB	●	●	Yes,Yes

Note: 1. System will not update the devices if no image is available or tagged in the repository.
2. Ensure that the target image is the right image for the selected device.
3. Upgrade of Unified AP is not allowed.

◉ Run Now ○ Schedule Later

SWIM/SMU Workflow Experience with DNA Center



3

Recent Tasks (Last 50)

Image Upgrade for 10.197.124.66

AIR-CT5520-K9-8-2-130-0.aes

Duration : 0h: 1m: 52s Start Time : Jan24 2018 00:45:26 ● Successful

1. Distribute Operation ✓

Distribution of image : AIR-CT5520-K9-8-2-130-0.aes on device : 10.197.124.66 completed successfully.

2. Activate Operation ✓

Activation of image : AIR-CT5520-K9-8-2-130-0.aes on device : 10.197.124.66 completed successfully

Image Upgrade for 172.28.169.102

cat9k_iosxe.2017-12-05_00.06_chbandi.SSA.bin

Duration : 0h: 0m: 1s Start Time : Jan23 2018 02:13:45 ● Successful

Image Upgrade for 172.28.169.102

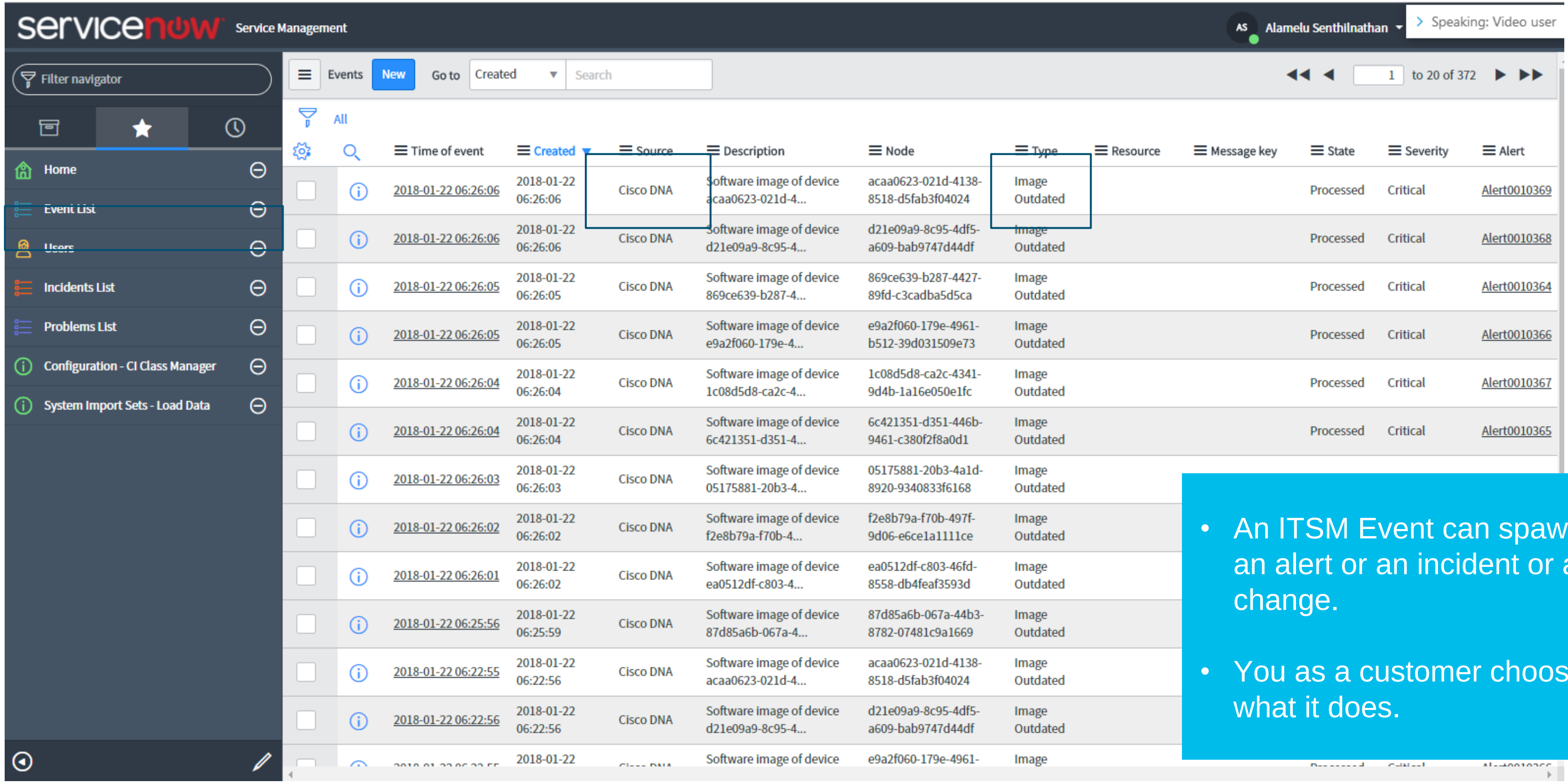
cat9k_iosxe.2017-12-05_00.06_chbandi.SSA.bin

Duration : 0h: 0m: 2s Start Time : Jan23 2018 02:12:25 ● Successful

3

- Detailed status information regarding the Upgrade Process
- SMU Activation Pre and Post Checks with detailed log information – CPU, Disk Space, Route Summary
- In case of failure during Image upgrade or Pre & Post checks, provide reason for failure and automatically Rollback

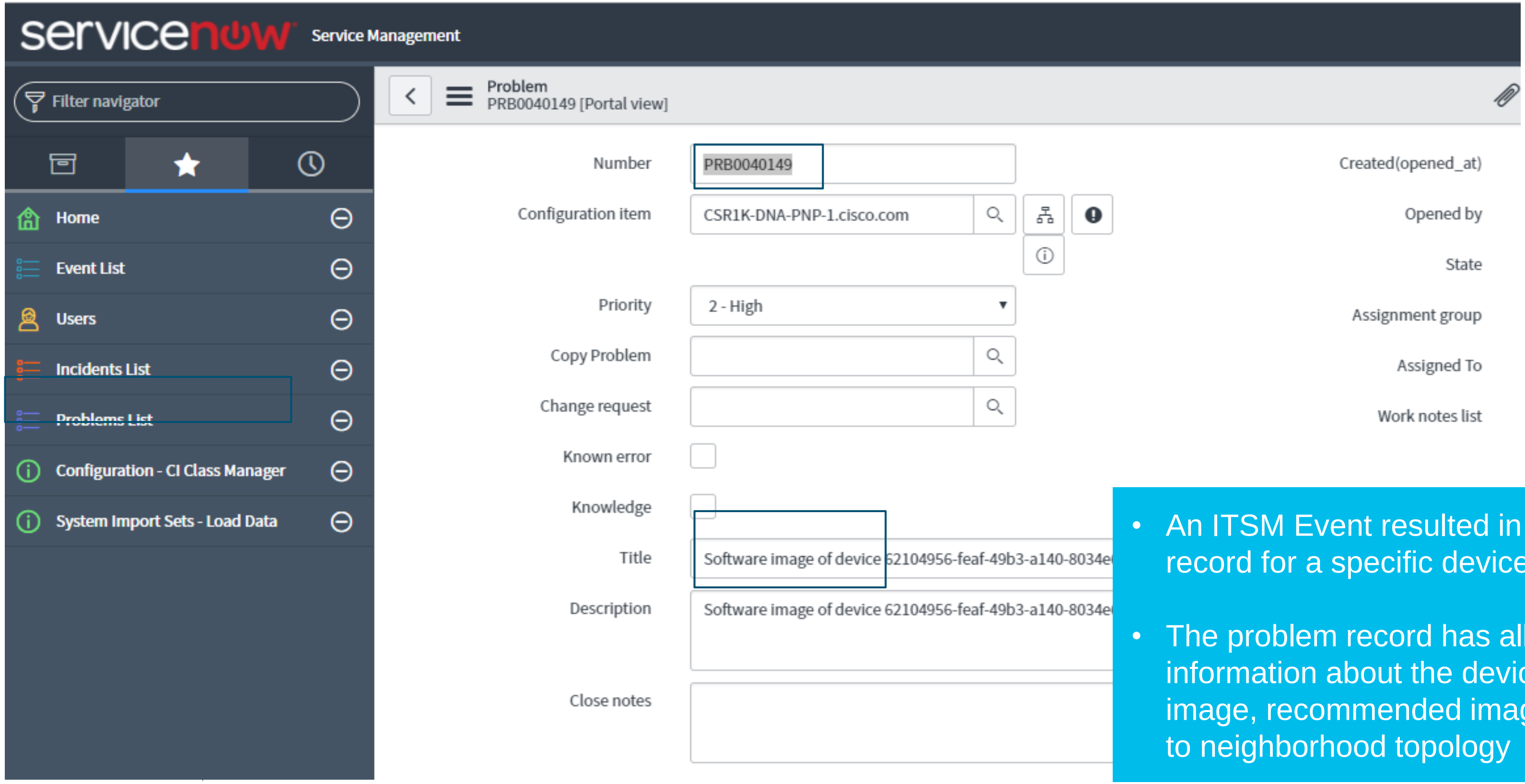
DNA Automation / Assurance driven events or issues translate into ITSM events



	Time of event	Created	Source	Description	Node	Type	Resource	Message key	State	Severity	Alert
☐	2018-01-22 06:26:06	2018-01-22 06:26:06	Cisco DNA	Software image of device acaa0623-021d-4...	acaa0623-021d-4138-8518-d5fab3f04024	Image Outdated			Processed	Critical	Alert0010369
☐	2018-01-22 06:26:06	2018-01-22 06:26:06	Cisco DNA	Software image of device d21e09a9-8c95-4...	d21e09a9-8c95-4df5-a609-bab9747d44df	Image Outdated			Processed	Critical	Alert0010368
☐	2018-01-22 06:26:05	2018-01-22 06:26:05	Cisco DNA	Software image of device 869ce639-b287-4...	869ce639-b287-4427-89fd-c3cadba5d5ca	Image Outdated			Processed	Critical	Alert0010364
☐	2018-01-22 06:26:05	2018-01-22 06:26:05	Cisco DNA	Software image of device e9a2f060-179e-4...	e9a2f060-179e-4961-b512-39d031509e73	Image Outdated			Processed	Critical	Alert0010366
☐	2018-01-22 06:26:04	2018-01-22 06:26:04	Cisco DNA	Software image of device 1c08d5d8-ca2c-4...	1c08d5d8-ca2c-4341-9d4b-1a16e050e1fc	Image Outdated			Processed	Critical	Alert0010367
☐	2018-01-22 06:26:04	2018-01-22 06:26:04	Cisco DNA	Software image of device 6c421351-d351-4...	6c421351-d351-446b-9461-c380f2f8a0d1	Image Outdated			Processed	Critical	Alert0010365
☐	2018-01-22 06:26:03	2018-01-22 06:26:03	Cisco DNA	Software image of device 05175881-20b3-4...	05175881-20b3-4a1d-8920-9340833f6168	Image Outdated					
☐	2018-01-22 06:26:02	2018-01-22 06:26:02	Cisco DNA	Software image of device f2e8b79a-f70b-4...	f2e8b79a-f70b-497f-9d06-e6ce1a1111ce	Image Outdated					
☐	2018-01-22 06:26:01	2018-01-22 06:26:02	Cisco DNA	Software image of device ea0512df-c803-4...	ea0512df-c803-46fd-8558-db4feaf3593d	Image Outdated					
☐	2018-01-22 06:25:56	2018-01-22 06:25:59	Cisco DNA	Software image of device 87d85a6b-067a-4...	87d85a6b-067a-44b3-8782-07481c9a1669	Image Outdated					
☐	2018-01-22 06:22:55	2018-01-22 06:22:56	Cisco DNA	Software image of device acaa0623-021d-4...	acaa0623-021d-4138-8518-d5fab3f04024	Image Outdated					
☐	2018-01-22 06:22:56	2018-01-22 06:22:56	Cisco DNA	Software image of device d21e09a9-8c95-4...	d21e09a9-8c95-4df5-a609-bab9747d44df	Image Outdated					
☐	2018-01-22 06:22:55	2018-01-22	Cisco DNA	Software image of device	e9a2f060-179e-4961-	Image			Processed	Critical	[illegible]

- An ITSM Event can spawn off an alert or an incident or a change.
- You as a customer choose what it does.

ITSM Event spawns off a problem depending on impact and user defined criteria



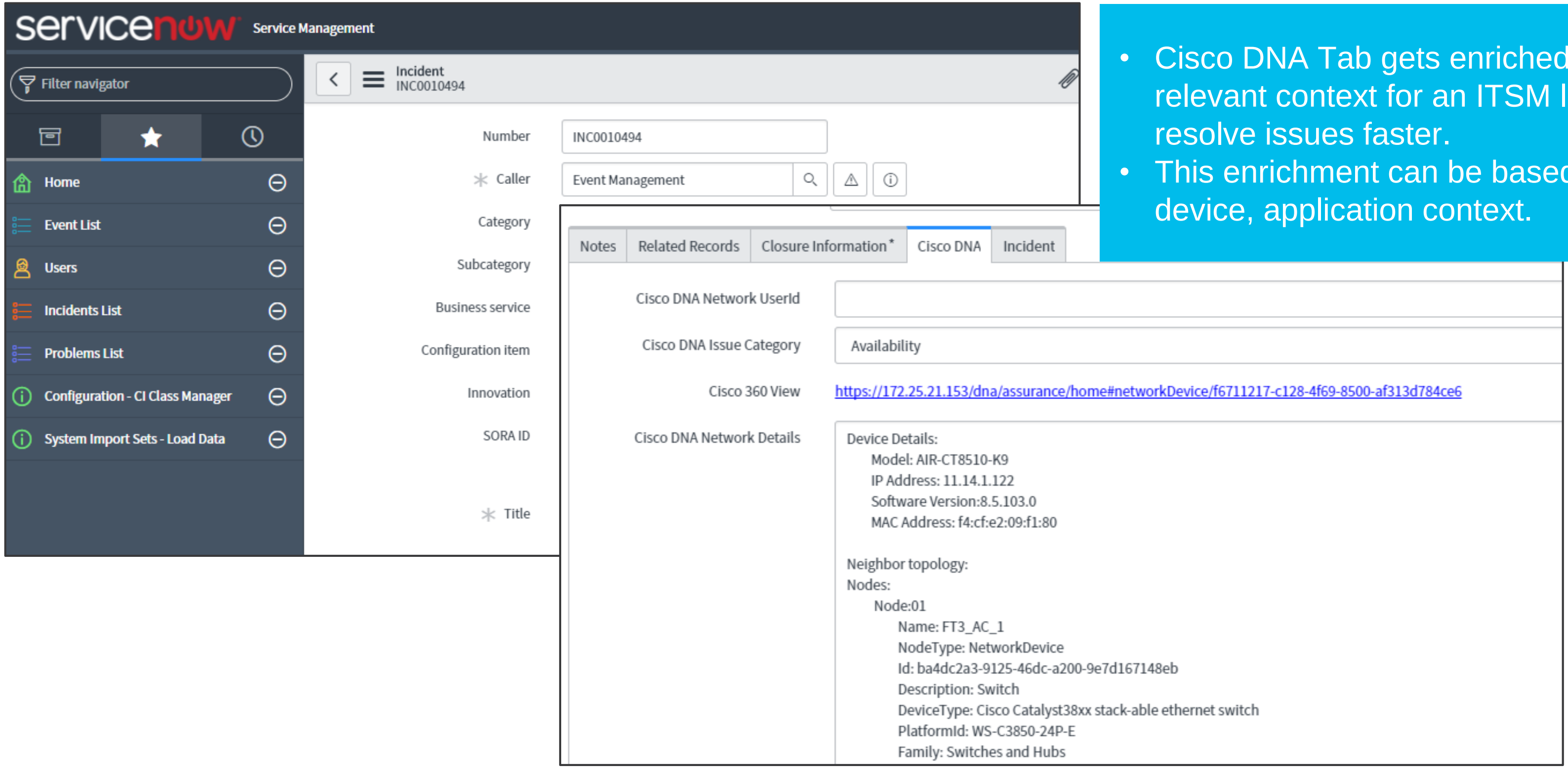
Problem
PRB0040149 [Portal view]

Number	PRB0040149
Configuration item	CSR1K-DNA-PNP-1.cisco.com
Priority	2 - High
Copy Problem	
Change request	
Known error	□
Knowledge	□
Title	Software image of device 62104956-feaf-49b3-a140-8034e
Description	Software image of device 62104956-feaf-49b3-a140-8034e
Close notes	

Created(opened_at)
Opened by
State
Assignment group
Assigned To
Work notes list

- An ITSM Event resulted in a problem record for a specific device.
- The problem record has all the information about the device – current image, recommended image, impact to neighborhood topology

ITSM Incident or Change Request gets updated with relevant analysis from DNA-C



Incident
INC0010494

Number	INC0010494
* Caller	Event Management
Category	
Subcategory	
Business service	
Configuration item	
Innovation	
SORA ID	
* Title	

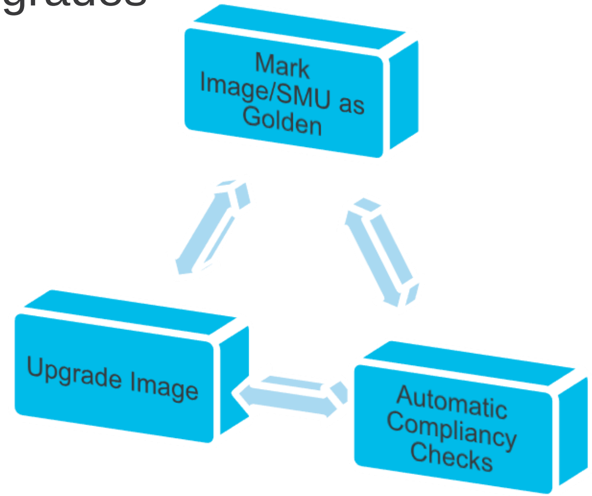
Cisco DNA Network UserId	
Cisco DNA Issue Category	Availability
Cisco 360 View	https://172.25.21.153/dna/assurance/home#networkDevice/f6711217-c128-4f69-8500-af313d784ce6
Cisco DNA Network Details	see below

```
Device Details:
    Model: AIR-CT8510-K9
    IP Address: 11.14.1.122
    Software Version:8.5.103.0
    MAC Address: f4:cf:e2:09:f1:80

Neighbor topology:
Nodes:
    Node:01
        Name: FT3_AC_1
        NodeType: NetworkDevice
        Id: ba4dc2a3-9125-46dc-a200-9e7d167148eb
        Description: Switch
        DeviceType: Cisco Catalyst38xx stack-able ethernet switch
        PlatformId: WS-C3850-24P-E
        Family: Switches and Hubs
```

- Cisco DNA Tab gets enriched with the relevant context for an ITSM leader to resolve issues faster.
- This enrichment can be based on user, device, application context.

Summary

- Software Images are mapped to Sites
- Extremely simplified upgrade process
- Upgrade with Confidence - Integrate with **YOUR** Pre-Check/Post-Check scripts
- Closed Loop Automation for Software Images Upgrades



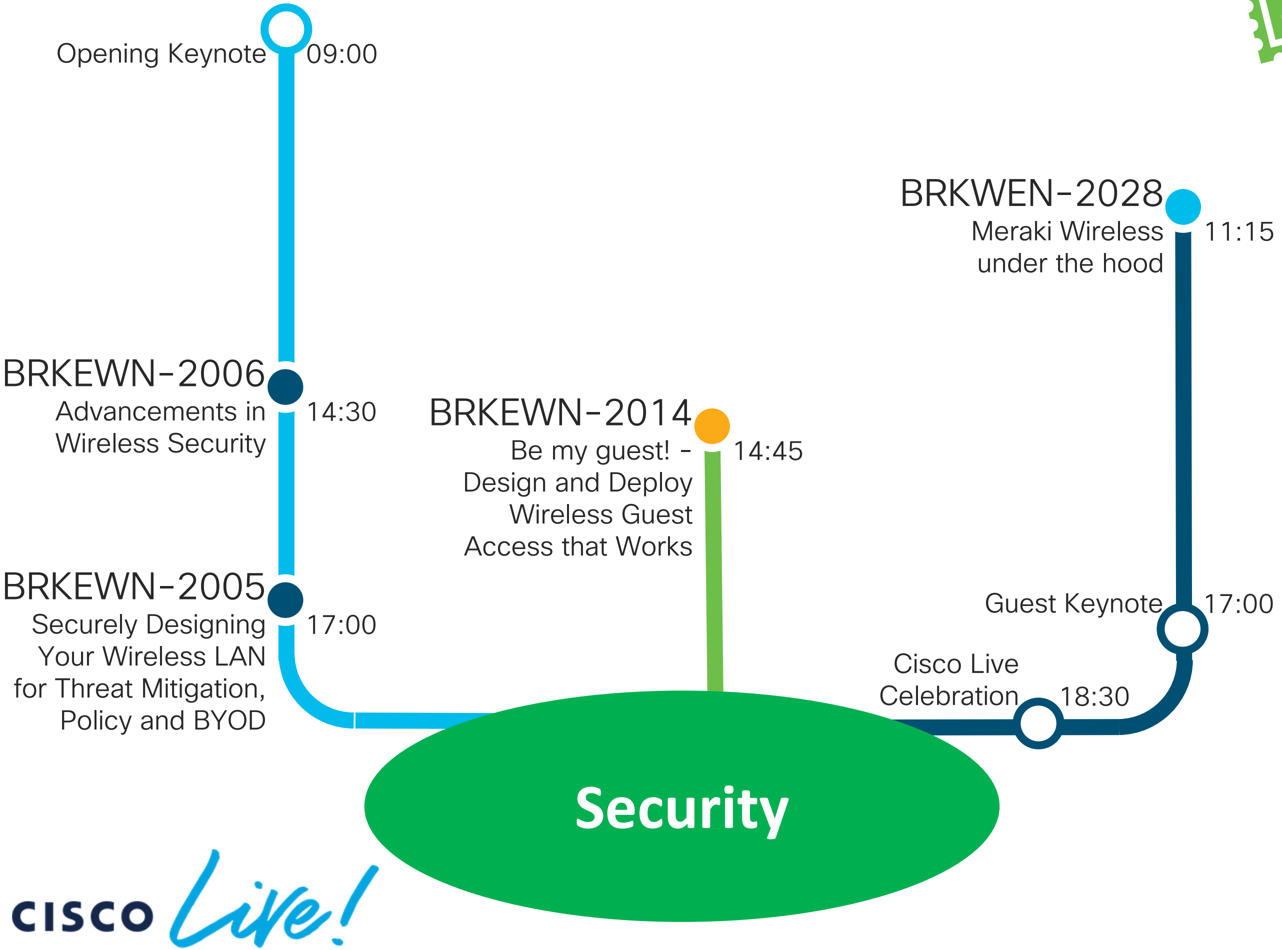
Key Takeaways

Key Takeaways

- Intent Based Workflows that are WLC Architecture Agnostic (Flex vs ME vs EWC vs C9800 vs AireOS)
- “Network Profiles” help deliver Business Intent - Day 0 to Day N
- AP Plug and Play and Ekahau integration provide easy AP onboarding experience and reduce Opex.

MOB

Mobility Track



Opening Keynote 09:00

BRKEWN-2006
Advancements in Wireless Security 14:30

BRKEWN-2005
Securely Designing Your Wireless LAN for Threat Mitigation, Policy and BYOD 17:00

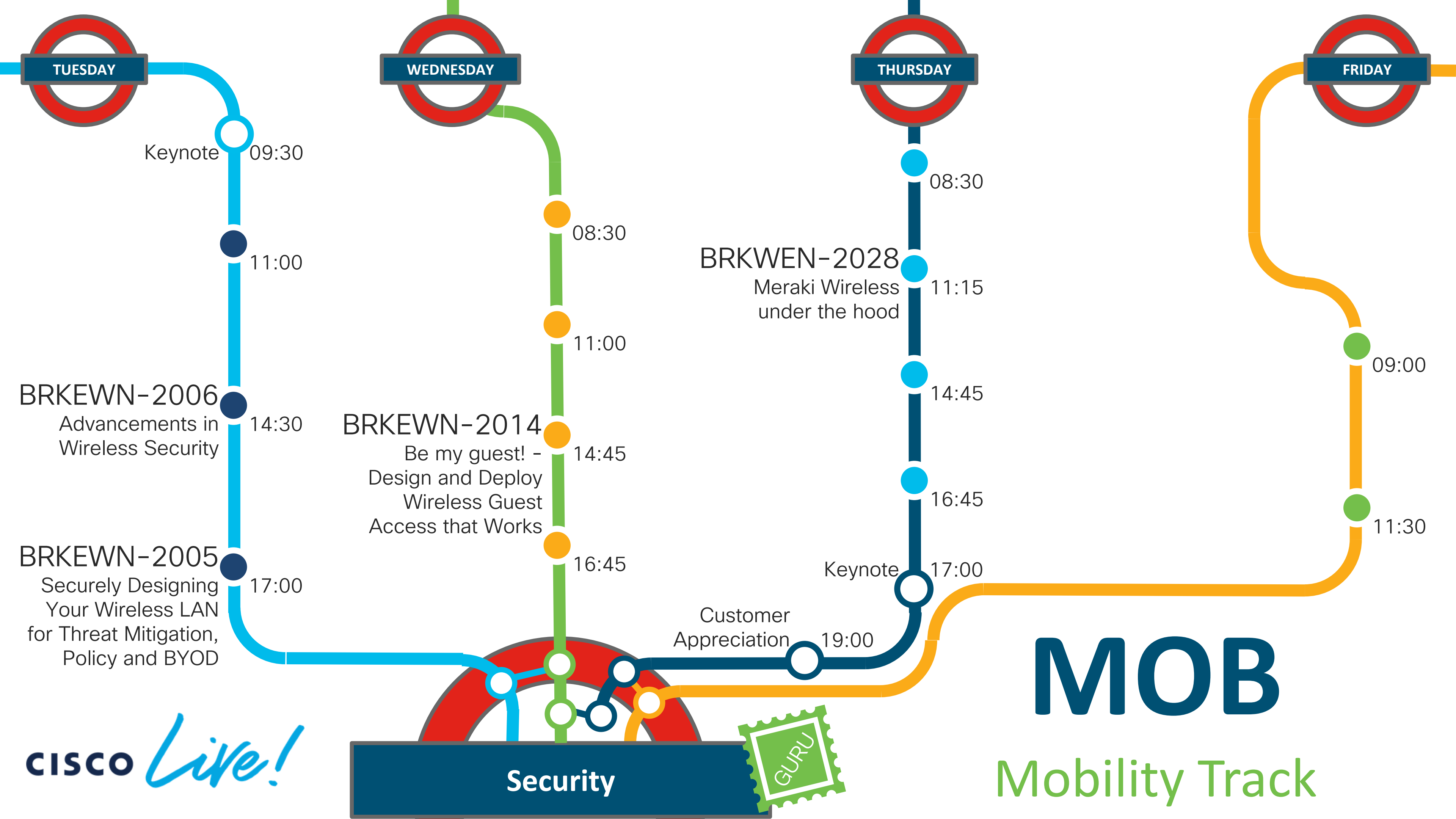
BRKEWN-2014
Be my guest! - Design and Deploy Wireless Guest Access that Works 14:45

BRKWEN-2028
Meraki Wireless under the hood 11:15

Guest Keynote 17:00

Cisco Live Celebration 18:30

Security



TUESDAY

Keynote 09:30

11:00

BRKEWN-2006
Advancements in Wireless Security 14:30

BRKEWN-2005
Securely Designing Your Wireless LAN for Threat Mitigation, Policy and BYOD 17:00

WEDNESDAY

08:30

11:00

BRKEWN-2014
Be my guest! - Design and Deploy Wireless Guest Access that Works 14:45

16:45

THURSDAY

08:30

BRKWEN-2028
Meraki Wireless under the hood 11:15

14:45

16:45

Keynote 17:00

Customer Appreciation 19:00

FRIDAY

09:00

11:30

Security

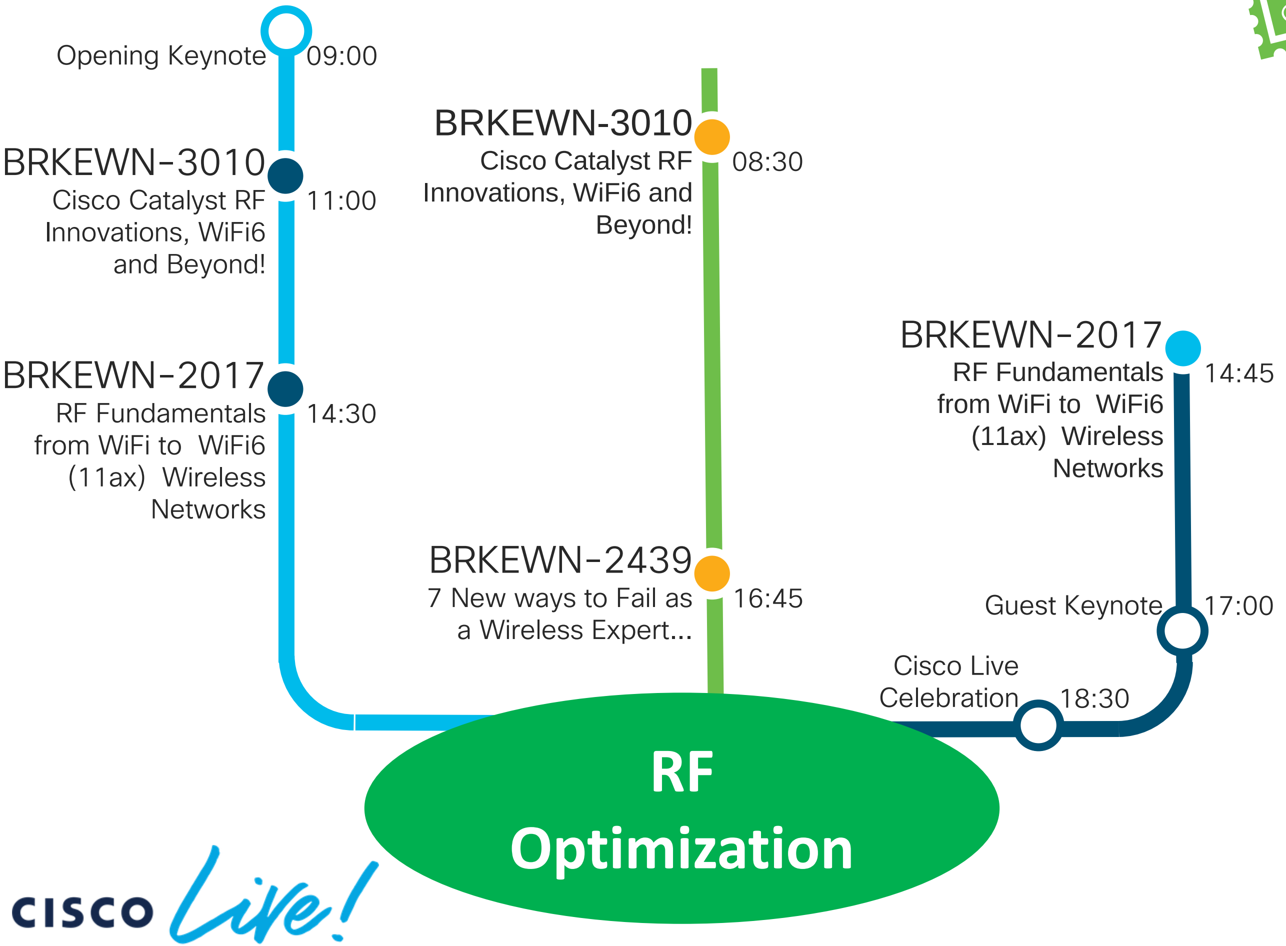
MOB

Mobility Track

GURU

MOB

Mobility Track



Opening Keynote 09:00

BRKEWN-3010 Cisco Catalyst RF Innovations, WiFi6 and Beyond! 11:00

BRKEWN-2017 RF Fundamentals from WiFi to WiFi6 (11ax) Wireless Networks 14:30

BRKEWN-3010 Cisco Catalyst RF Innovations, WiFi6 and Beyond! 08:30

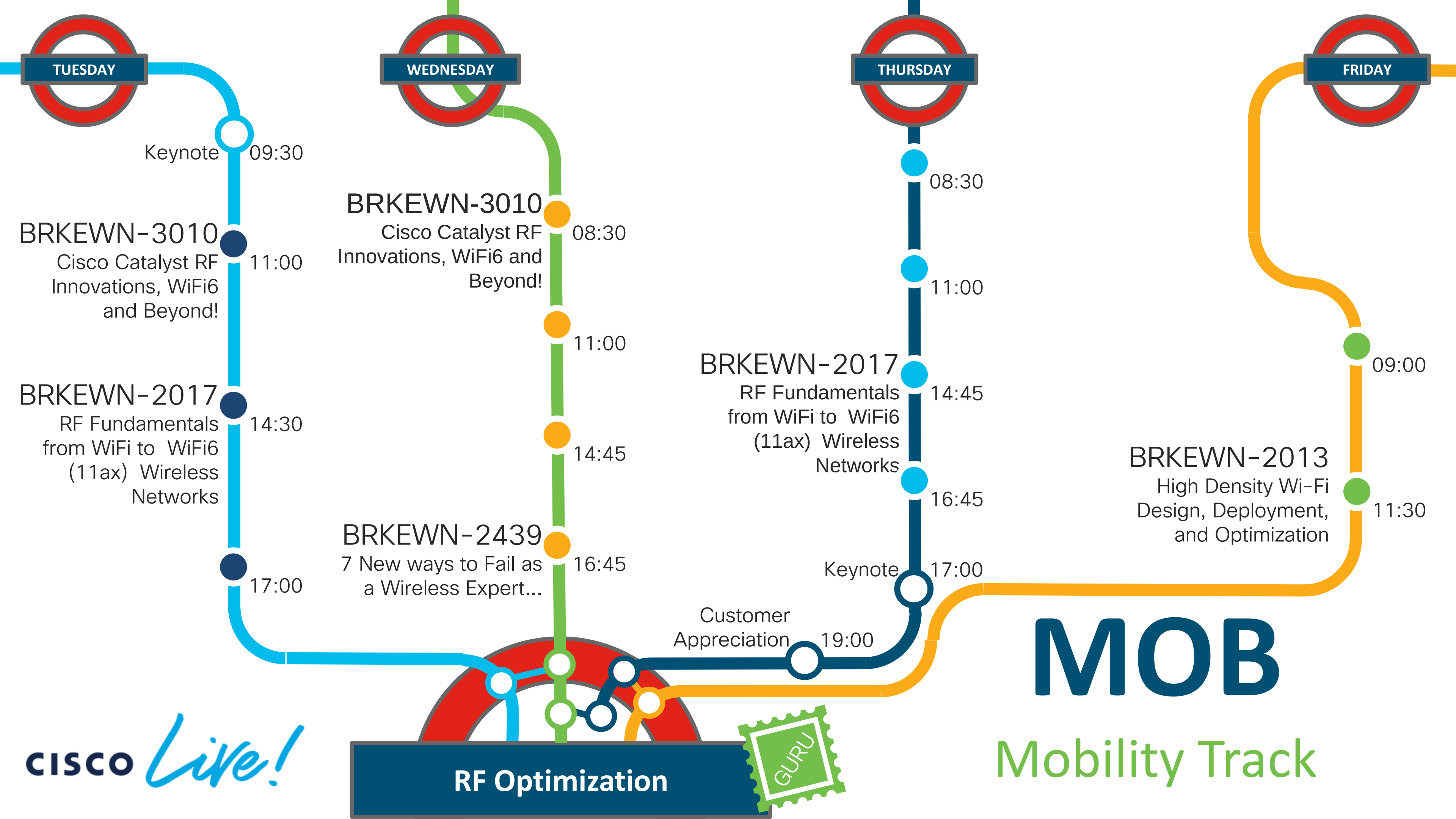
BRKEWN-2439 7 New ways to Fail as a Wireless Expert... 16:45

BRKEWN-2017 RF Fundamentals from WiFi to WiFi6 (11ax) Wireless Networks 14:45

Guest Keynote 17:00

Cisco Live Celebration 18:30

RF Optimization



TUESDAY

Keynote 09:30

BRKEWN-3010 Cisco Catalyst RF Innovations, WiFi6 and Beyond! 11:00

BRKEWN-2017 RF Fundamentals from WiFi to WiFi6 (11ax) Wireless Networks 14:30

17:00

WEDNESDAY

BRKEWN-3010 Cisco Catalyst RF Innovations, WiFi6 and Beyond! 08:30

11:00

14:45

BRKEWN-2439 7 New ways to Fail as a Wireless Expert... 16:45

THURSDAY

08:30

11:00

BRKEWN-2017 RF Fundamentals from WiFi to WiFi6 (11ax) Wireless Networks 14:45

16:45

Keynote 17:00

Customer Appreciation 19:00

FRIDAY

09:00

BRKEWN-2013 High Density Wi-Fi Design, Deployment, and Optimization 11:30

RF Optimization

GURU

MOB

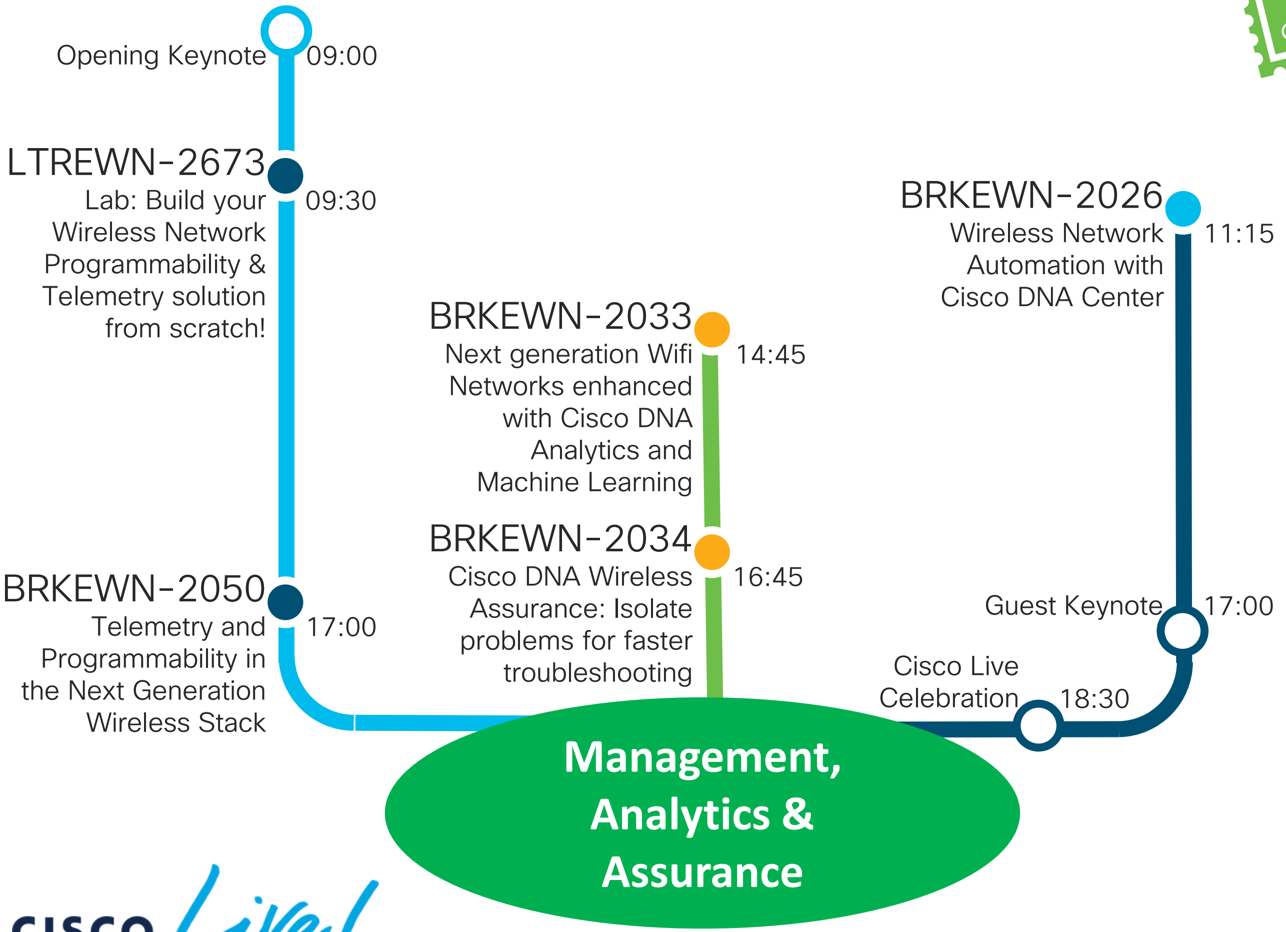
Mobility Track

cisco Live!

GURU

MOB

Mobility Track



Opening Keynote 09:00

LTREWN-2673
Lab: Build your Wireless Network Programmability & Telemetry solution from scratch!
09:30

BRKEWN-2050
Telemetry and Programmability in the Next Generation Wireless Stack
17:00

BRKEWN-2033
Next generation Wifi Networks enhanced with Cisco DNA Analytics and Machine Learning
14:45

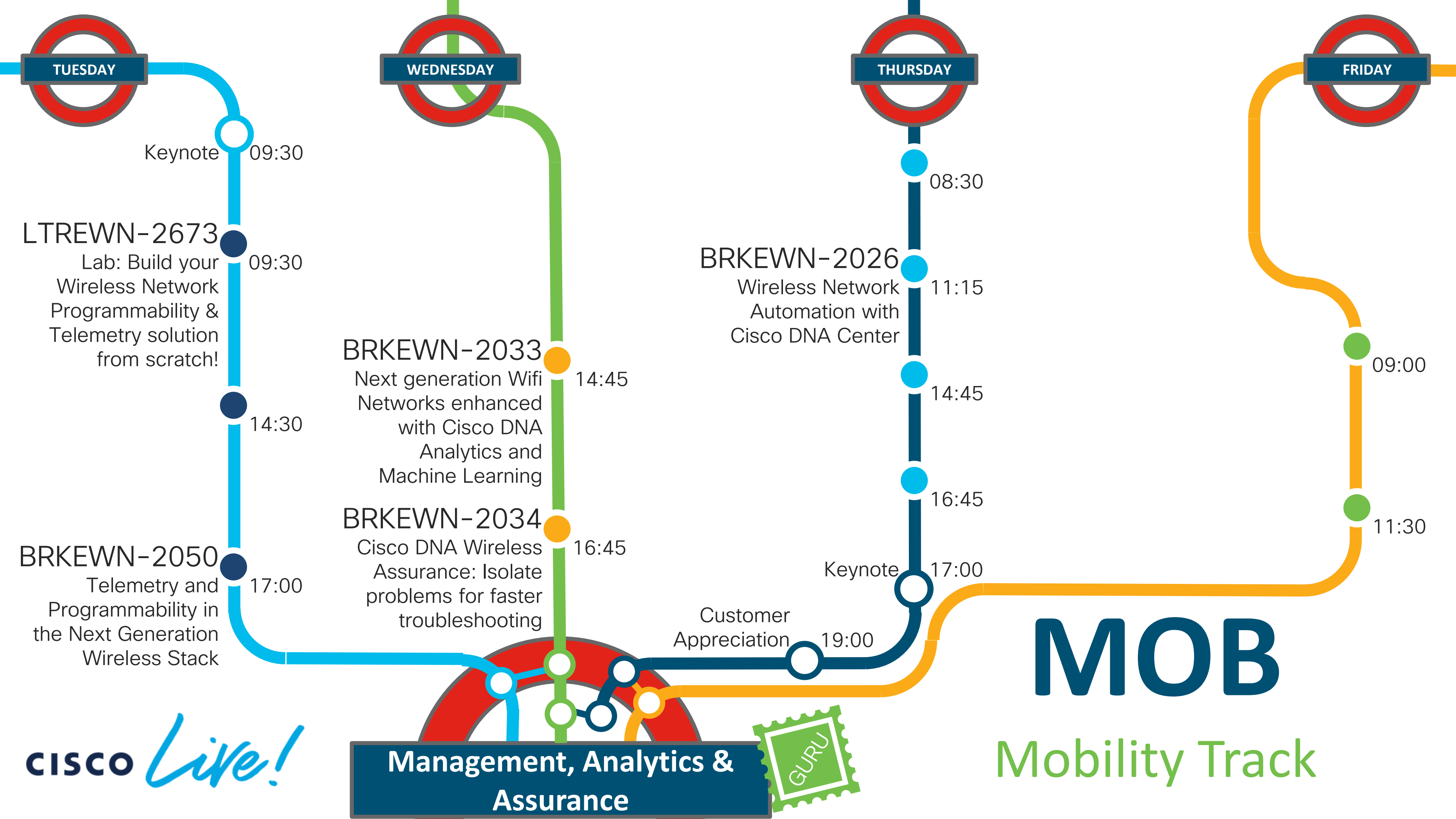
BRKEWN-2034
Cisco DNA Wireless Assurance: Isolate problems for faster troubleshooting
16:45

BRKEWN-2026
Wireless Network Automation with Cisco DNA Center
11:15

Guest Keynote 17:00

Cisco Live Celebration 18:30

Management, Analytics & Assurance



TUESDAY

Keynote 09:30

LTREWN-2673 09:30
Lab: Build your Wireless Network Programmability & Telemetry solution from scratch!

14:30

BRKEWN-2050 17:00
Telemetry and Programmability in the Next Generation Wireless Stack

WEDNESDAY

BRKEWN-2033 14:45
Next generation Wifi Networks enhanced with Cisco DNA Analytics and Machine Learning

BRKEWN-2034 16:45
Cisco DNA Wireless Assurance: Isolate problems for faster troubleshooting

THURSDAY

08:30

BRKEWN-2026 11:15
Wireless Network Automation with Cisco DNA Center

14:45

16:45

Keynote 17:00

Customer Appreciation 19:00

FRIDAY

09:00

11:30

Management, Analytics & Assurance

GURU

MOB

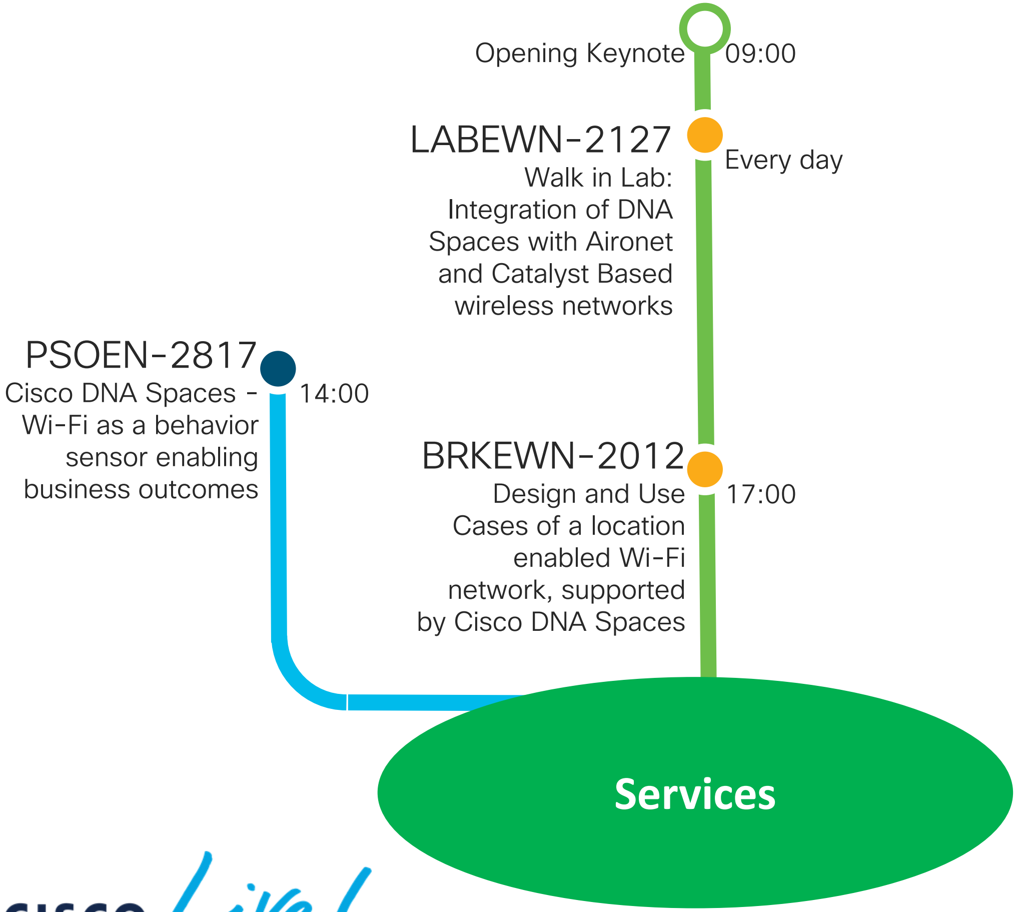
Mobility Track

cisco Live!

GURU

MOB

Mobility Track



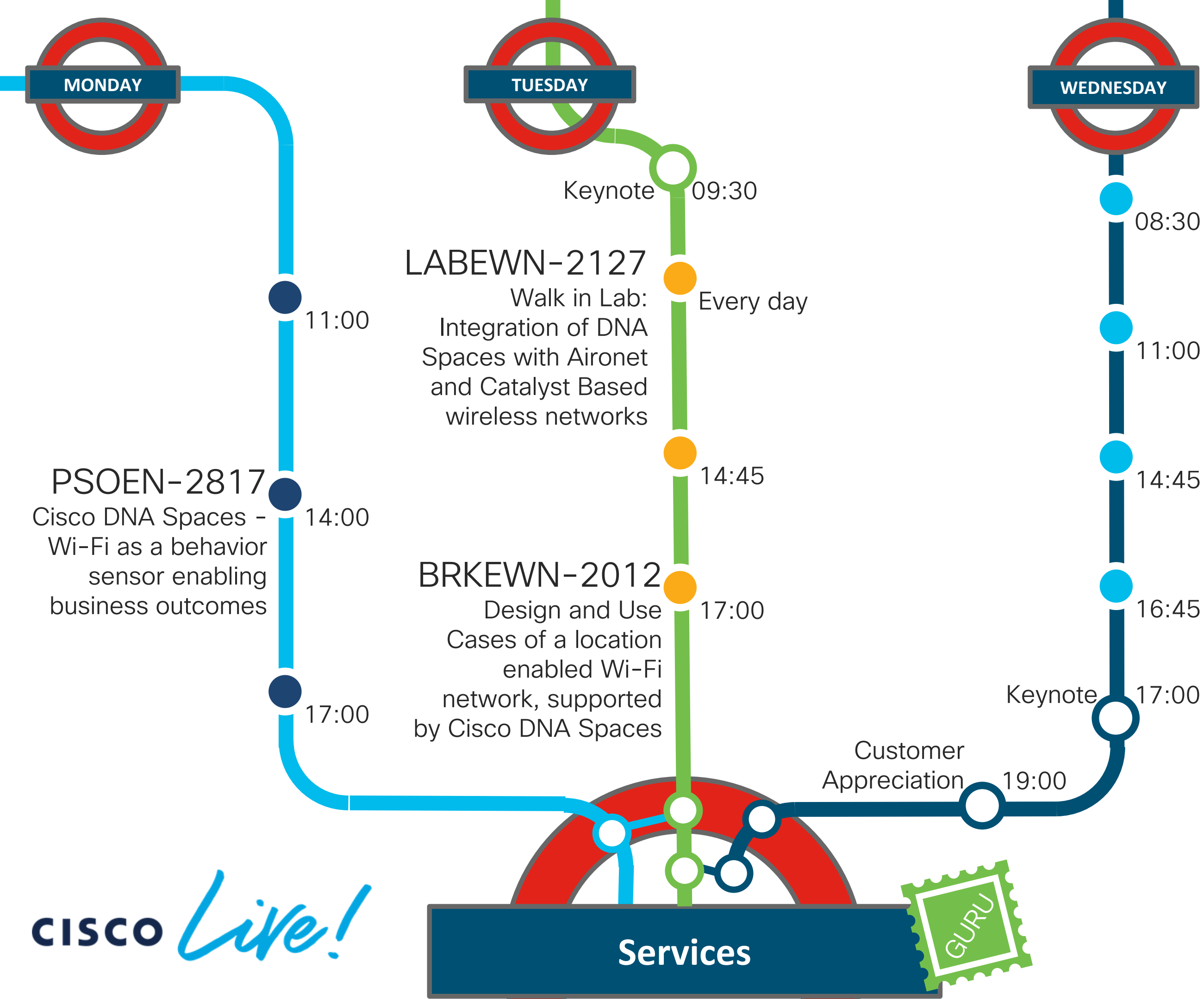
Opening Keynote 09:00

LABEWN-2127 Every day
Walk in Lab:
Integration of DNA
Spaces with Aironet
and Catalyst Based
wireless networks

PSOEN-2817 14:00
Cisco DNA Spaces -
Wi-Fi as a behavior
sensor enabling
business outcomes

BRKEWN-2012 17:00
Design and Use
Cases of a location
enabled Wi-Fi
network, supported
by Cisco DNA Spaces

Services



MONDAY

11:00

PSOEN-2817
Cisco DNA Spaces - Wi-Fi as a behavior sensor enabling business outcomes
14:00

17:00

TUESDAY

Keynote 09:30

LABEWN-2127
Walk in Lab: Integration of DNA Spaces with Aironet and Catalyst Based wireless networks
Every day

14:45

BRKEWN-2012
Design and Use Cases of a location enabled Wi-Fi network, supported by Cisco DNA Spaces
17:00

WEDNESDAY

08:30

11:00

14:45

16:45

Keynote 17:00

Customer Appreciation 19:00

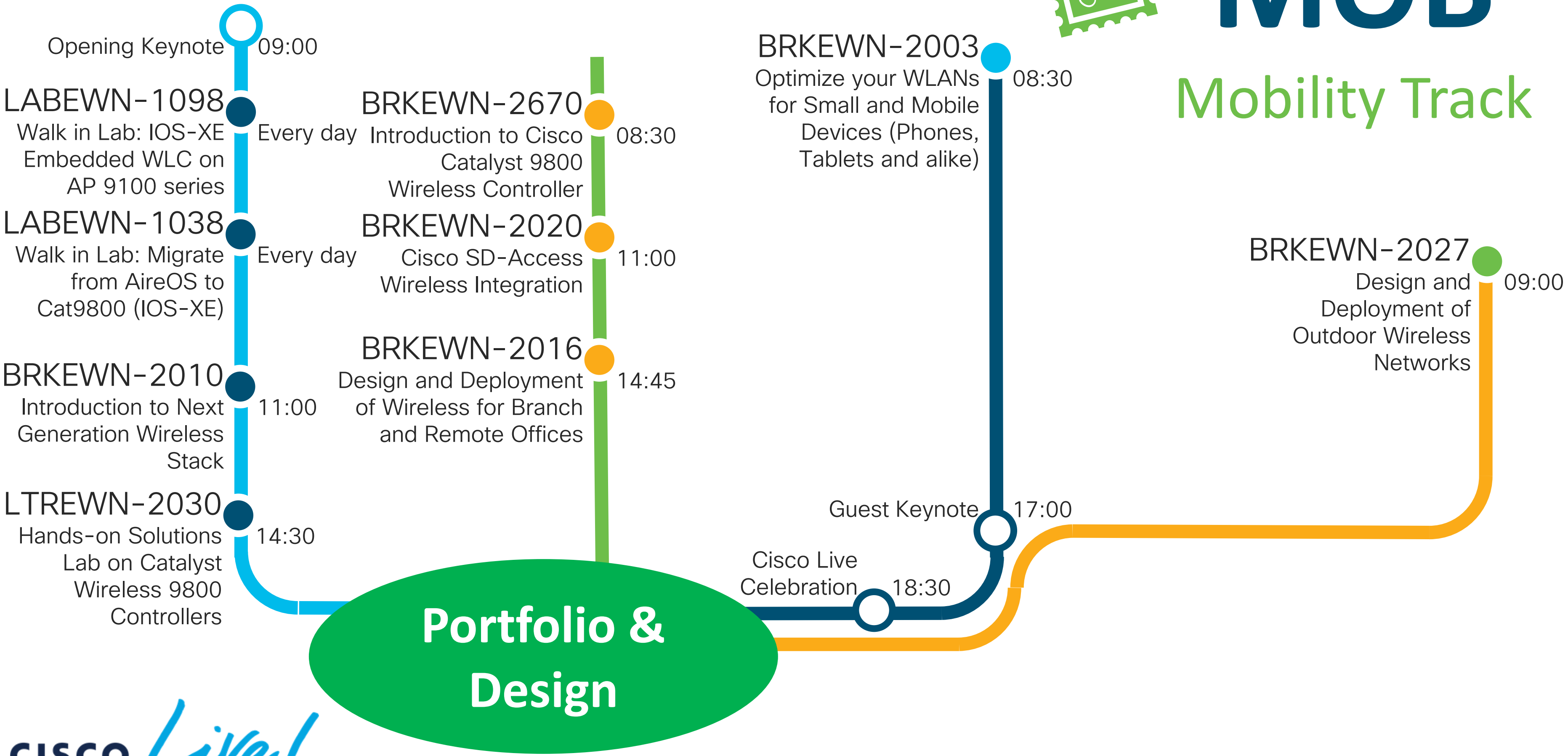
Services

MOB

Mobility Track

MOB

Mobility Track



Opening Keynote 09:00

LABEWN-1098 Every day
Walk in Lab: IOS-XE Embedded WLC on AP 9100 series

LABEWN-1038 Every day
Walk in Lab: Migrate from AireOS to Cat9800 (IOS-XE)

BRKEWN-2010 11:00
Introduction to Next Generation Wireless Stack

LTREWN-2030 14:30
Hands-on Solutions Lab on Catalyst Wireless 9800 Controllers

BRKEWN-2670 08:30
Introduction to Cisco Catalyst 9800 Wireless Controller

BRKEWN-2020 11:00
Cisco SD-Access Wireless Integration

BRKEWN-2016 14:45
Design and Deployment of Wireless for Branch and Remote Offices

BRKEWN-2003 08:30
Optimize your WLANs for Small and Mobile Devices (Phones, Tablets and alike)

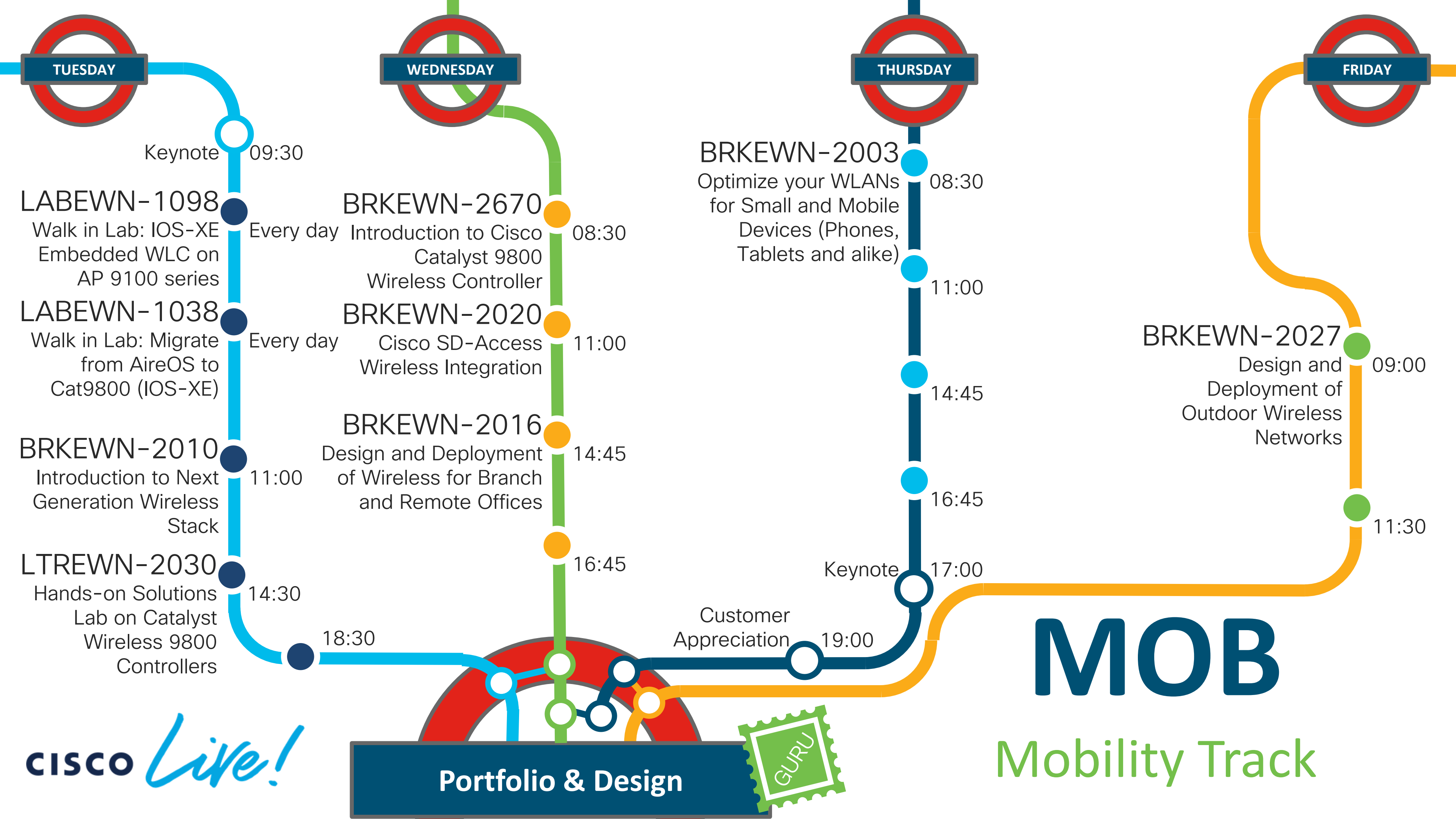
Guest Keynote 17:00

Cisco Live Celebration 18:30

BRKEWN-2027 09:00
Design and Deployment of Outdoor Wireless Networks

MOB

Mobility Track



TUESDAY

Keynote 09:30

LABEWN-1098 Walk in Lab: IOS-XE Embedded WLC on AP 9100 series — Every day

LABEWN-1038 Walk in Lab: Migrate from AireOS to Cat9800 (IOS-XE) — Every day

BRKEWN-2010 Introduction to Next Generation Wireless Stack — 11:00

LTREWN-2030 Hands-on Solutions Lab on Catalyst Wireless 9800 Controllers — 14:30

18:30

WEDNESDAY

BRKEWN-2670 Introduction to Cisco Catalyst 9800 Wireless Controller — 08:30

BRKEWN-2020 Cisco SD-Access Wireless Integration — 11:00

BRKEWN-2016 Design and Deployment of Wireless for Branch and Remote Offices — 14:45

16:45

THURSDAY

BRKEWN-2003 Optimize your WLANs for Small and Mobile Devices (Phones, Tablets and alike) — 08:30

11:00

14:45

16:45

Keynote 17:00

Customer Appreciation 19:00

FRIDAY

BRKEWN-2027 Design and Deployment of Outdoor Wireless Networks — 09:00

11:30

Portfolio & Design

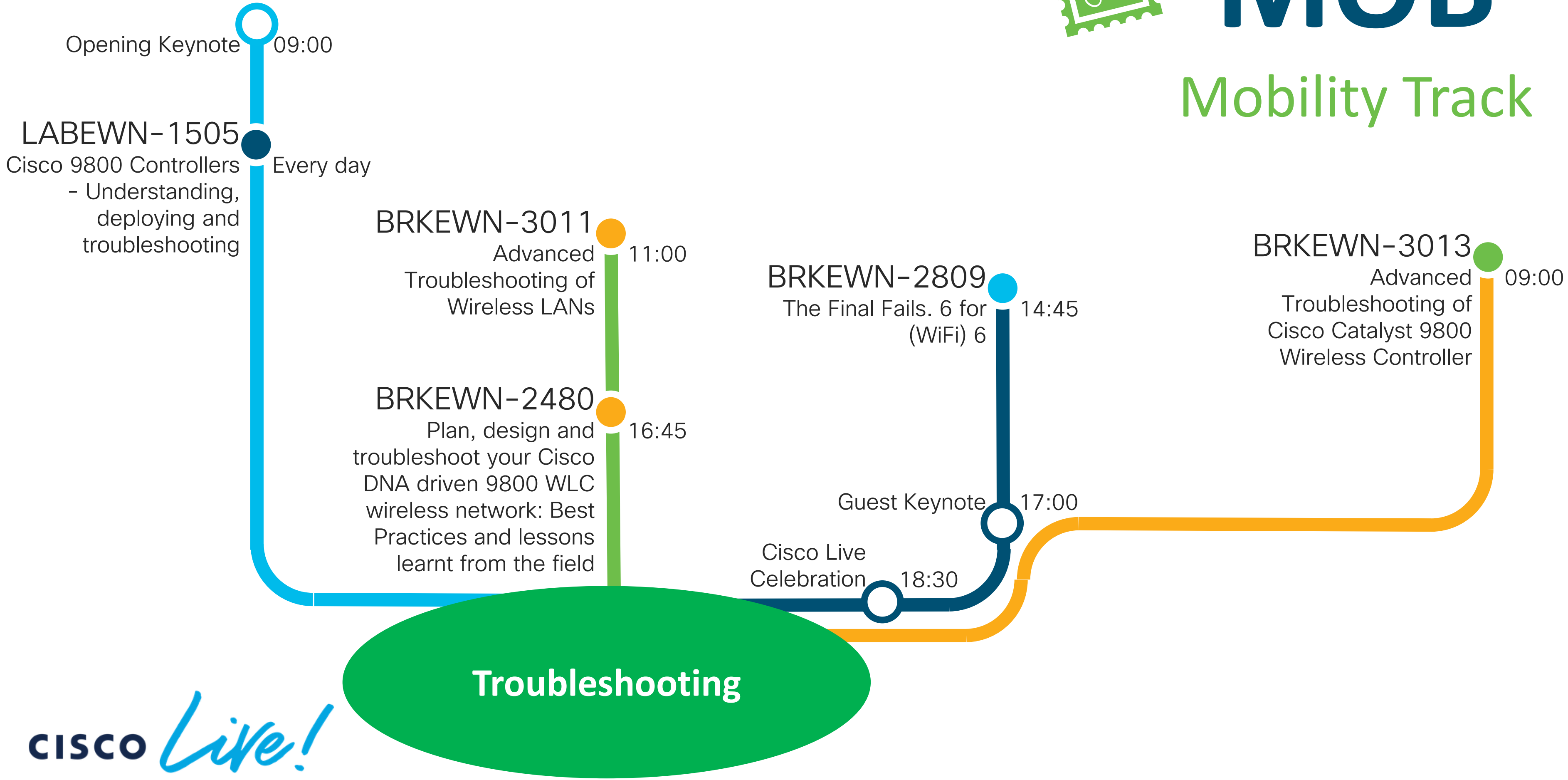
GURU

cisco Live!

GURU

MOB

Mobility Track



Opening Keynote 09:00

LABEWN-1505
Cisco 9800 Controllers - Understanding, deploying and troubleshooting
Every day

BRKEWN-3011
Advanced Troubleshooting of Wireless LANs
11:00

BRKEWN-2480
Plan, design and troubleshoot your Cisco DNA driven 9800 WLC wireless network: Best Practices and lessons learnt from the field
16:45

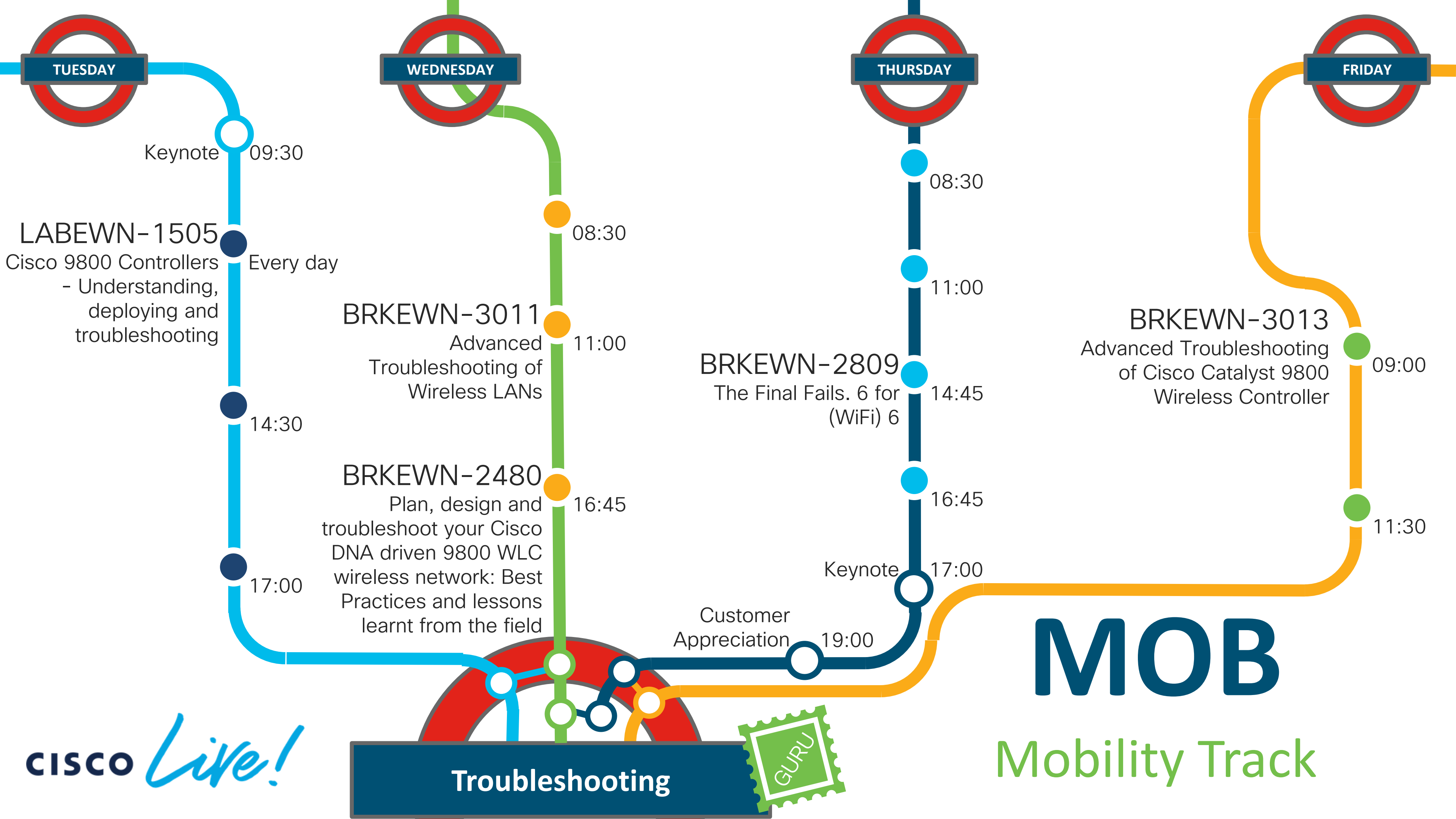
BRKEWN-2809
The Final Fails. 6 for (WiFi) 6
14:45

Guest Keynote 17:00

Cisco Live Celebration 18:30

BRKEWN-3013
Advanced Troubleshooting of Cisco Catalyst 9800 Wireless Controller
09:00

Troubleshooting



TUESDAY

Keynote 09:30

LABEWN-1505
Cisco 9800 Controllers - Understanding, deploying and troubleshooting
Every day

14:30

17:00

WEDNESDAY

08:30

BRKEWN-3011
Advanced Troubleshooting of Wireless LANs
11:00

BRKEWN-2480
Plan, design and troubleshoot your Cisco DNA driven 9800 WLC wireless network: Best Practices and lessons learnt from the field
16:45

THURSDAY

08:30

11:00

BRKEWN-2809
The Final Fails. 6 for (WiFi) 6
14:45

16:45

Keynote 17:00

Customer Appreciation 19:00

FRIDAY

BRKEWN-3013
Advanced Troubleshooting of Cisco Catalyst 9800 Wireless Controller
09:00

11:30

Troubleshooting

MOB

Mobility Track

cisco Live!

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco campus
- Walk-in labs
- Meet the engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**