SD-Access Wireless Design and Deployment Guide
Cisco DNA Center 2.1.1

Revised: Jan 13th, 2022

Executive summary

Digitization is transforming business in every industry, requiring every company to be an IT company. Studies show that companies that master digital not only drive more revenue, but are 29 percent more profitable on average (Source: Leading Digital). This transformation is critical and urgent, as 40 percent of incumbents are at risk of being displaced (Source: Digital Vortex).

The Cisco Digital Network Architecture (Cisco DNA Center) is an open, software-driven architecture built on a set of design principles to provide:

- **Insights and actions** to drive faster business innovation
- **Automaton and assurance** to lower costs and complexity while meeting business and user expectations
- **Security and compliance** to reduce risk as the organization continues to expand and grow

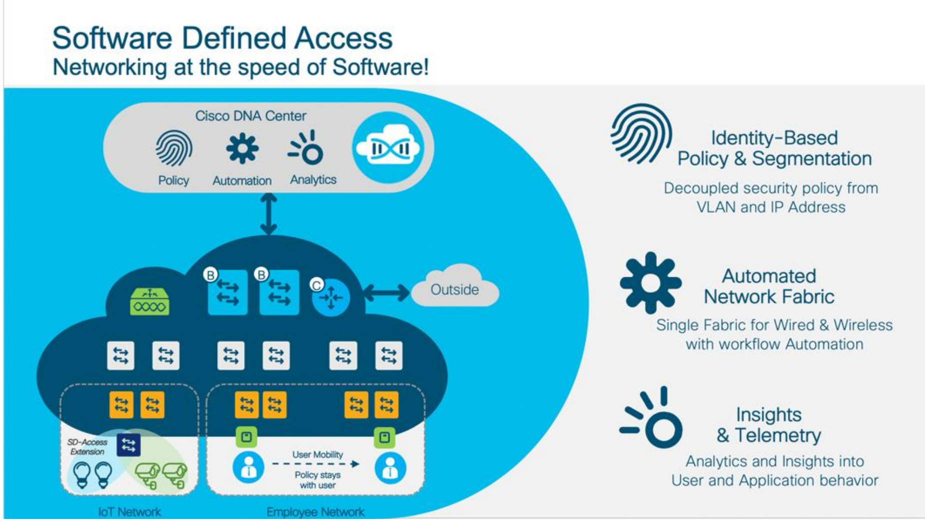
Cisco® Software-Defined Access (SD-Access) is a critical building block of Cisco DNA and brings the principles and advantages of Cisco DNA to Cisco customers.

Software-Defined Access

SD-Access is Cisco's next-generation enterprise networking access solution, designed to offer integrated security, segmentation, and elastic service rollouts via a fabric-based infrastructure. It features an outstanding GUI experience for automated network provisioning via the Cisco DNA Center application. By automating day-to-day tasks such as configuration, provisioning, and troubleshooting, SD-Access reduces the time it takes to adapt the network, improves issue resolution, and reduces the impact of security breaches. These benefits result in significant CapEx and OpEx savings for the business.

Figure 1 summarizes the benefits of SD-Access.

Figure 1. Benefits of SD-Access


Software Defined Access
Networking at the speed of Software!
Cisco DNA Center
Policy
Automation
Analytics
B
B
C
Outside
SD-Access Extension
User Mobility
Policy stays with user
IoT Network
Employee Network
Identity-Based Policy & Segmentation
Decoupled security policy from VLAN and IP Address
Automated Network Fabric
Single Fabric for Wired & Wireless with workflow Automation
Insights & Telemetry
Analytics and Insights into User and Application behavior

In this document the focus is on the wireless integration in SD-Access, and it is assumed that the reader is familiar with the concept of SD-Access fabric and the main components of this network architecture.

For additional information on SD-Access capabilities, please refer to the SD-Access site at https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html and the SD-Access Design Guide (Cisco Validated Design).

SD-Access Wireless

SD-Access Wireless integrates wireless access into the SD-Access architecture to gain all the advantages of fabric and Cisco DNA Center automation.

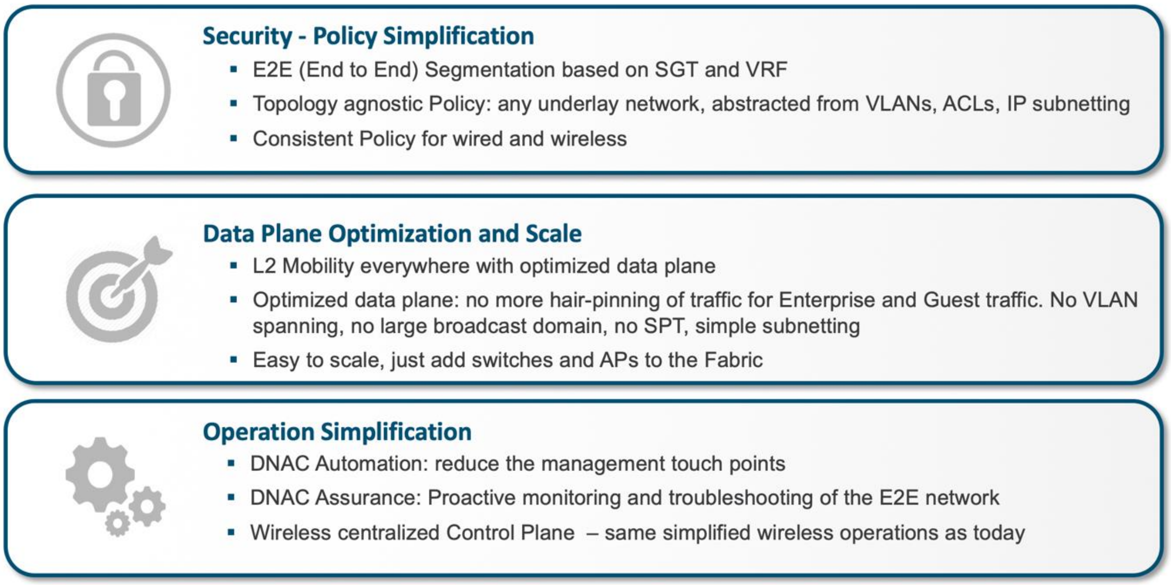
Some of the benefits of SD-Access Wireless are:

- **Centralized wireless control plane**: The innovative RF features found in Cisco Unified Wireless Network deployments are also leveraged in SD-Access Wireless. Wireless operations are the same as with Cisco Unified Wireless Network in terms of radio resource management (RRM), client onboarding, client mobility, and so on, which simplifies IT adoption.
- **Optimized distributed data plane**: The data plane is distributed at the edge switches for optimal performance and scalability without the hassles usually associated with distributing traffic (spanning VLANs, subnetting, large broadcast domains, etc.)
- **Seamless Layer 2 roaming everywhere**: The SD-Access fabric allows clients to roam seamlessly across the campus while retaining the same IP address.
- **Simplified guest and mobility tunneling**: An anchor wireless controller (WLC) is no longer needed; guest traffic can go directly to the network edge (DMZ) without hopping through a foreign controller.
- **Policy simplification**: SD-Access breaks the dependencies between policy and network constructs (IP address and VLANs), simplifying the way we can define and implement policies for both wired and wireless clients.
- **Segmentation made easy**: Segmentation is carried end to end in the fabric and is hierarchical, based on virtual network identifiers (VNIs) and scalable group tags (SGTs). The same segmentation policy is applied to both wired and wireless users.

All these advantages are present while still maintaining:

- **Best-in-class wireless** with future-ready WiFi 6 Access Points (APs), 802.11 Wave 1, 802.11ac Wave 2 AP, Cisco 3504, 5520, 8540, C9800-40, C9800-80, C9800-CL and the EWC(9800 software running on a Catalyst 9300/9400/9500).
- **Investment protection** by supporting existing AireOS WLCs; SD-Access Wireless is optimized for 802.11ac Wave 2 APs but also supports Wave 1 APs.

Figure 2. Benefits of SD-Access Wireless



Security - Policy Simplification

- E2E (End to End) Segmentation based on SGT and VRF
- Topology agnostic Policy: any underlay network, abstracted from VLANs, ACLs, IP subnetting
- Consistent Policy for wired and wireless

Data Plane Optimization and Scale

- L2 Mobility everywhere with optimized data plane
- Optimized data plane: no more hair-pinning of traffic for Enterprise and Guest traffic. No VLAN spanning, no large broadcast domain, no SPT, simple subnetting
- Easy to scale, just add switches and APs to the Fabric

Operation Simplification

- DNAC Automation: reduce the management touch points
- DNAC Assurance: Proactive monitoring and troubleshooting of the E2E network
- Wireless centralized Control Plane – same simplified wireless operations as today

Wireless integration in SD-Access

Customers with a wired network based on SD-Access fabric have two options for integrating wireless access:

- SD-Access Wireless Architecture
- Cisco Unified Wireless Network Wireless Over the Top (OTT)

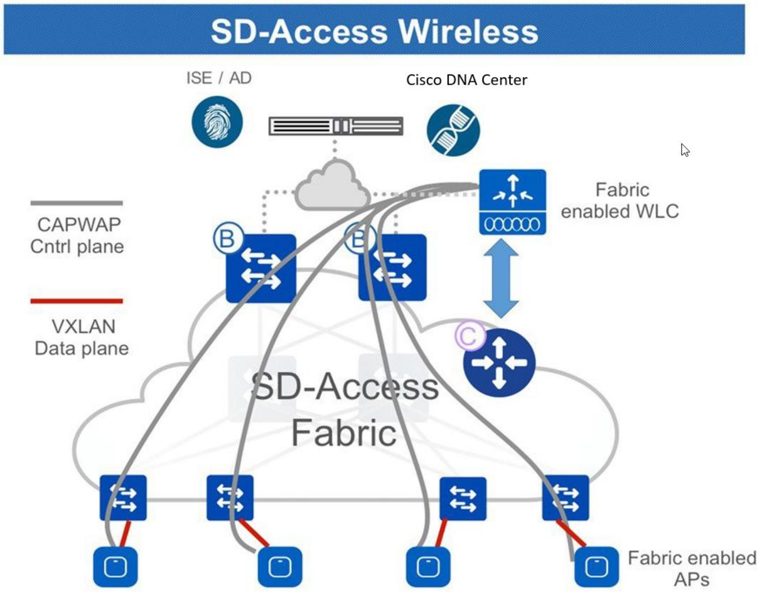
Let's first examine the SD-Access Wireless option, since it brings the full advantages of fabric for wireless users and things. We'll begin by introducing the architecture and main components and then describe how to set up an SD-Access Wireless network using Cisco DNA Center.

OTT basically involves running traditional wireless on top of a fabric wired network. This option will be covered later in the document, together with the design considerations.

SD-Access Wireless architecture

Figure 3 shows the overall SD-Access Wireless architecture.

Figure 3. SD-Access Wireless architecture

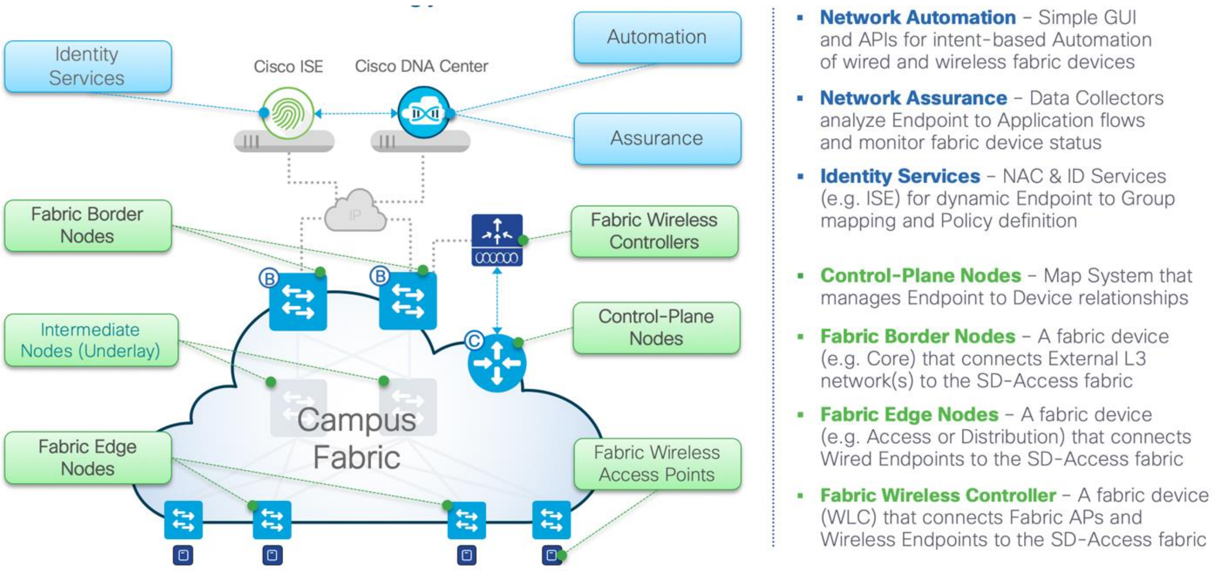


In SD-Access Wireless, the control plane is centralized. This means that, as with Cisco Unified Wireless Network, a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel is maintained between APs and WLC. The main difference is that in SD-Access Wireless, the data plane is distributed using a Virtual Extensible LAN (VXLAN) directly from the fabric-enabled APs. The WLC and APs are integrated into the fabric, and the APs connect to the fabric overlay (endpoint ID space) network as "special" clients.

Components of the SD-Access Wireless architecture

Figure 4 shows the main components of the SD-Access Wireless architecture. A description of these components follows.

Figure 4. SD-Access Wireless architecture components



- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

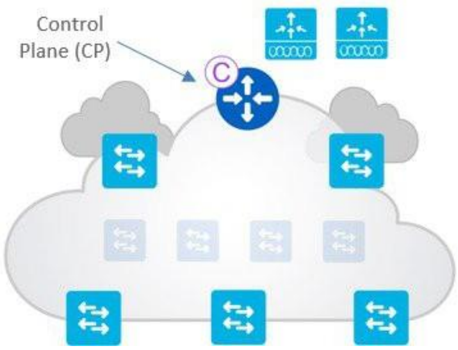
- **Control plane (CP) nodes:** Host database that manages endpoint ID to device relationships.
- **Fabric border (FB) nodes:** A fabric device (such as a core or distribution switch) that connects external Layer 3 network(s) to the SD-Access fabric.
- **Fabric edge (FE) nodes:** A fabric device (such as an access switch) that connects wired endpoints to the SD-Access fabric.
- **Fabric WLC:** Wireless controller that is fabric enabled.
- **Fabric APs:** Access points that are fabric enabled.
- **Cisco DNA Center:** Single pane of glass for enterprise network automation and assurance. Cisco DNA Center brings together the enterprise software-defined networking (SDN) controller and the policy engine (Cisco Identity Services Engine [ISE]).
- **Policy engine:** An external ID service (such as ISE) that provides dynamic user or device to group mapping and policy definition.
- **Assurance engine:** A data collector (NDP) running on Cisco DNAC analyzes user or device to app flows and monitors fabric status.

The following sections describe the roles and functions of the main components of the SD-Access Wireless architecture.

Control plane node

The fabric control-plane node is based on a LISP map server/resolver and runs the Fabric Endpoint ID Database to provide overlay reachability information.

Figure 5. Control plane node



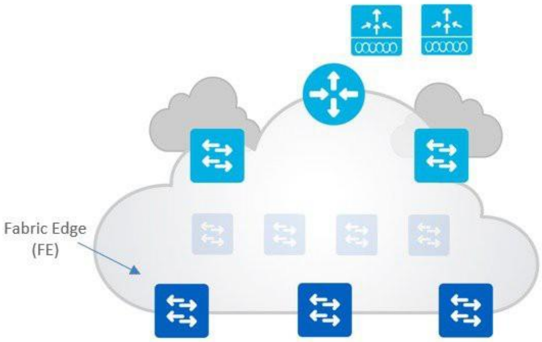
The CP is the host database, tracking endpoint ID (EID) to edge node bindings, along with other attributes. It does the following:

- Supports multiple types of EID lookup keys (IPv4/32, IPv6/128, or MAC addresses).
- Receives prefix registrations from edge nodes and fabric WLCs for wired local endpoints and wireless clients, respectively.
- Resolves lookup requests from remote edge nodes to locate endpoints.
- Updates fabric edge nodes and border nodes with wireless client mobility and routing locator (RLOC) information.

Fabric edge node

The fabric edge provides connectivity for users and devices connected to the fabric.

Figure 6. Fabric edge node



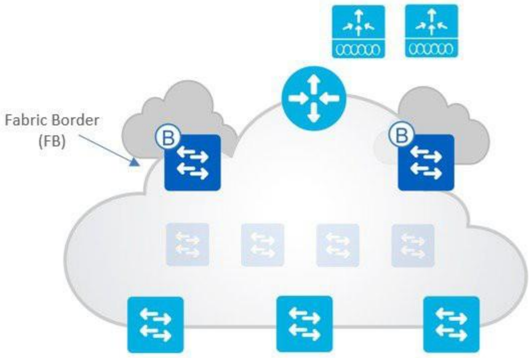
The fabric edge does the following:

- Is responsible for identifying and authenticating wired endpoints
- Registers wireless IPv4/IPv6 endpoint ID information with the control-plane node(s)
- Provides an anycast Layer 3 gateway for connected endpoints
- Provides virtual network (VN) services for wireless clients
- Onboards APs into the fabric and forms VXLAN tunnels with APs
- Provides guest functionality for wireless hosts interacting with the guest border and guest control-plane node

Fabric border node

All traffic entering or leaving the fabric goes through the fabric border.

Figure 7. Fabric border node



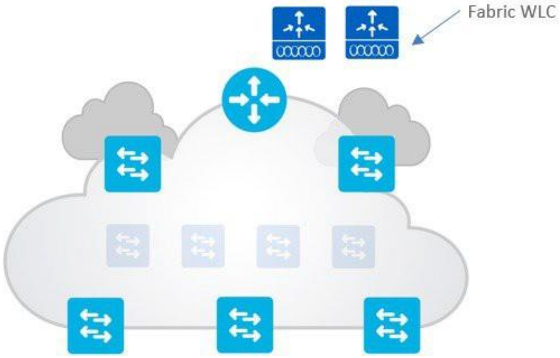
- There are two types of fabric border nodes: border and default border nodes. Both types provide the fundamental routing entry and exit point for all data traffic going into or out of the fabric overlay, as well as for VN and/or group-based policy enforcement (for traffic outside the fabric).
- A fabric border is used to add “known” IP/mask routes to the map system. A known route is any IP/mask that you want to advertise to your fabric edge nodes (remote WLC, shared services, data center, branch, private cloud, and so on)
- A default border is used for any “unknown” routes (such as the Internet or public cloud), as a gateway of last resort.
- A border is where fabric and non-fabric domains exchange endpoint reachability and policy information.
- Borders are responsible for translation of context (virtual route forwarding [VRF] and SGT) from one domain to another.

Fabric-enabled WLC

• **The fabric-enabled WLC integrates with the LISP control plane.**

The control plane is centralized at the WLC for wireless functions.

Figure 8. Fabric-enabled WLC



- The WLC is still responsible for AP image/configuration, RRM, client session management and roaming, and all the other wireless control plane functions.
- For fabric integration:
  - For wireless, the client **MAC address is used as the EID.**
  - Interacts with the Host Tracking database on the control-plane node for **client MAC address registration** with SGT and VNI.
  - The VN information is mapped to a VLAN on the fabric edges.
  - The WLC is responsible for updating the Host Tracking database with **roaming** information for wireless clients

.

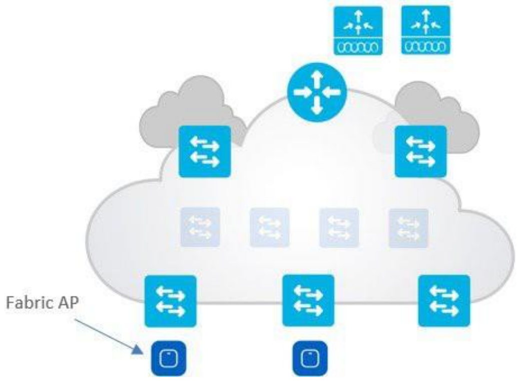
- **The fabric-enabled WLC** can only manage a single fabric site.

Note The WLC and APs need to be within 20 ms of latency. Usually, this means being on the same physical site.

Fabric APs

Fabric APs extend the SD-Access data plane to the wireless edge.

Figure 9. Fabric APs



- A fabric AP is a local mode AP and needs to be **directly connected** to the fabric edge switch or to a classic/policy extended node.
- The CAPWAP control plane goes to the WLC using fabric as the transport.
- Fabric is enabled per service set identifier (SSID):
  - For a fabric-enabled SSID, the AP converts 802.11 traffic to 802.3 and encapsulates it into VXLAN, encoding the VNI and SGT information of the client.
  - The AP forwards client traffic based on the forwarding table as programmed by the WLC. The VXLAN tunnel destination is always the Fabric Edge where the access tunnel is terminated. In case of an extended node the access tunnel is terminated on the Fabric Edge where the extended nodes are connected.
  - SGT- and VRF-based policies for wireless users on fabric SSIDs are applied at the fabric edge, the same as they are for wired.
- For fabric-enabled SSIDs, the user data plane is distributed at the APs, using VXLAN as encapsulation.
- The AP applies all wireless-specific features, such as SSID policies, Application Visibility and Control (AVC), quality of service (QoS), etc.

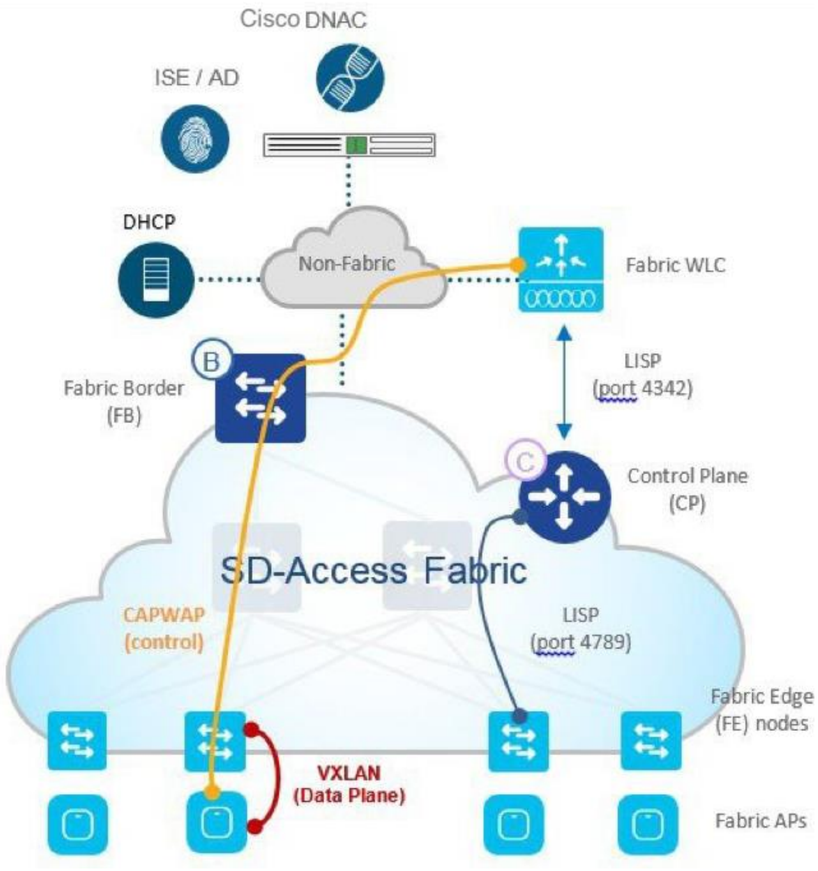
Note For feature support on APs, refer to the WLC release notes.

APs can optionally be connected to one of the supported fabric extended nodes. Refer to the ordering guide for supported switch models (https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-c07-739242.html).

SD-Access Wireless protocols and communication interfaces

Figure 10 illustrates the protocols and interfaces used in SD-Access Wireless.

Figure 10. Communication between the different components



- Between the WLC and APs: Communication between the control plane WLC and AP is via CAPWAP, similar to existing modes.
- Between the APs and switch: Data traffic is switched from the AP to the edge switch using VXLAN tunnel encapsulation, with UDP port is 4789 as per standard.
- Between the WLC and control-plane node: The WLC communicates with the control plane running on TCP port 4342 on the controller.
- Between Cisco DNA Center and the WLC: For Aire-OS platforms, Cisco DNA Center uses the command-line interface (CLI) through SSH/Telnet to configure the WLC.
- On the Catalyst 9800 Platforms, the Cisco DNA Center uses the netconf-yang model to push/provision configuration on the device. Enabling netconf-yang is covered in the subsequent sections. The netconf uses TCP port 830.
- On EWC (9800 software on Catalyst 9300/9400 and 9500), the control plane resides on the Catalyst switch. There exists a LISP agent on the 9800 software responsible to talk to the control plane.
- Between the switch and control plane node: The fabric-enabled switches communicate with the control-plane node on TCP port 4342.

SD-Access Wireless platform support

The SD-Access Wireless architecture is supported on the following WLCs and APs:
Cisco 3504, 5520, and 8540 Series Wireless Controllers
Cisco Catalyst 9800 Series Wireless Controllers (9800-40, 9800-80, 9800-L, 9800-CL)

Cisco Catalyst 9800 Embedded Wireless on C9300, C9400, C9500 Series Switch
WiFi 6 Access Points: Cisco Catalyst 9115AX and Cisco Catalyst 9117AX
WiFi 6 Access Points: Cisco Catalyst 9120AX Series
WiFi 6 Access Points: Cisco Catalyst 9130AX Series
802.11 Wave 2 Access Points: Cisco Aironet 1800, 2800,3800, and 4800 Series
802.11 Wave 2 outdoor Access Points: Cisco Aironet 1540, 1560
802.11 Wave 2 Access Points: Cisco Catalyst IW6300 Heavy Duty Series Access Points
802.11 Wave 2 Access Points: Cisco 6300 Series Embedded Services Access Points

Please refer to the SD-Access Compatibility Matrix for the latest supported device and software information:
https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html

SD-Access Wireless network deployment

This section gives some important considerations for deploying WLC and APs in an SD-Access Wireless network. please refer to the picture below:

Access points must be deployed as follows:

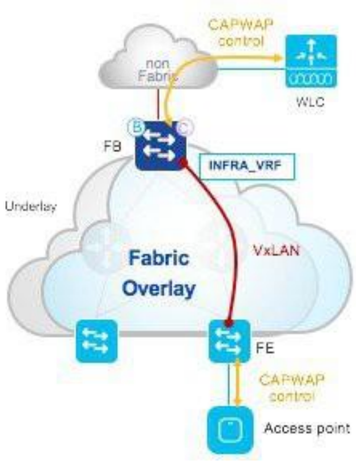
- Be directly connected to the fabric edge (or to an extended node switch)
- Be part of the fabric overlay
- Belong to the INFRA_VN, which is mapped to the global routing table
- Join the WLC in Local mode

WLCs must be deployed as follows:

- Be connected outside the fabric (optionally directly to border)
- Reside in the global routing table
- No need for inter-VRF leaking for an AP to join the WLC
- Communicate to only one control-plane node (two for redundancy); hence one WLC can belong to only one fabric domain (FD)

Note To make the fabric control plane protocol more resilient, it’s important that a **specific route to the WLC be present in each fabric node’s global routing table**. The route to the WLC’s IP address be should be either redistributed into the underlay Interior Gateway Protocol (IGP) at the border or configured statically at each node. The WLC is considered as an RLOC within the SD-Access, so as part of LISP RLOC reachability check a specific route to the WLC is needed on the underlay. In other words, the WLC should not be reachable through the default route.

Figure 12. Deployment of AP and WLC



AP-to-WLC communication

From a network deployment perspective, the access points are connected in the overlay network while the WLC resides outside the SD-Access fabric in the traditional IP network.

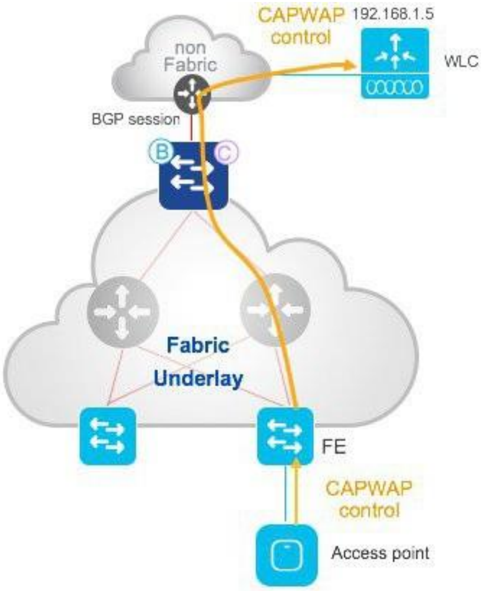
Note: Ensure that the WLC is physically located on-site and does not sit across the WAN. Fabric APs must be in Local mode and need less than 20 ms latency between AP and WLC

The WLC subnet will be advertised into the underlay so that fabric nodes in the network (fabric edge and control plane) can do native routing to reach the WLC. The AP subnets in the overlay will be advertised to the external network so the WLC can reach the APs via the overlay.

Let’s look a bit deeper into how the CAPWAP traffic flows between APs and WLC for fabric-enabled SSIDs. This is the control plane traffic only for an AP join operation and all the other control plane traffic. (Client data plane traffic does not go to the WLC, as it is distributed from APs to the switch using VXLAN.)

CAPWAP traffic in the south-north direction, from APs to WLC, is illustrated in Figure 13.

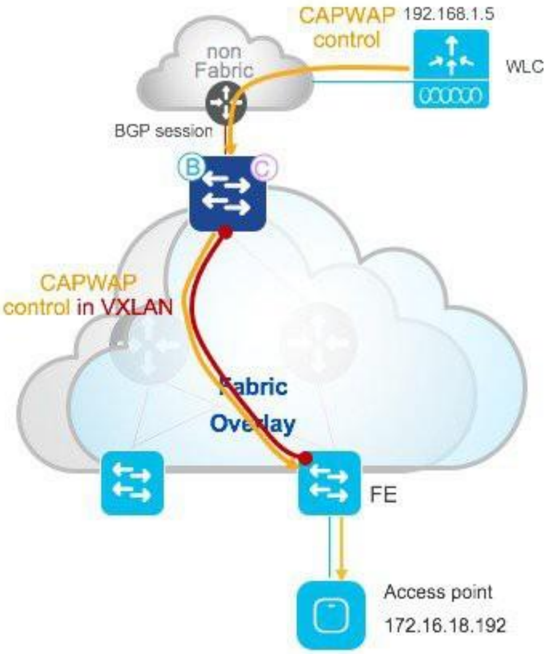
Figure 13. South-north CAPWAP traffic from AP to WLC



- The border (internal or external) redistributes the WLC route in the underlay (using the IGP of choice).
- The FE learns the route in the global routing table.
- When the FE receives a CAPWAP packet from the AP, the FE finds a match in the RIB and the packet is forwarded with no VXLAN encapsulation.
- The AP-to-WLC CAPWAP traffic travels in the underlay.

CAPWAP traffic in the north-south direction, from WLC to APs, is illustrated in Figure 14.

Figure 14. North-south CAPWAP traffic from WLC to AP



- The AP subnet is registered in the control plane, as it is part of the overlay.
- The border exports the AP's local EID space from the control plane to the global routing table and also import the AP routes into the LISP map-cache entry.
- The border advertises the local AP EID space to the external domain.
- When the border receives a CAPWAP packet from the WLC, the LISP lookup happens and traffic is sent to the FE with VXLAN encapsulation.
- The WLC-to-AP CAPWAP traffic travels in the overlay.

Note: We have described the CAPWAP traffic path from AP to WLC. The same path applies to other types of traffic originated from the AP and sent to destinations known in the global routing table, such as DHCP, DNS, etc

Setting up SD-Access Wireless with Cisco DNA Center

This section provides a step-by-step guide to setting up wireless capabilities in SD-Access through Cisco DNA Center. Cisco DNA Center is the single pane of glass that provides automation, policy, and assurance for the SD-Access solution.

One of the prerequisites in setting up the SD-Access wireless is to have the Cisco DNA Center installed. The Wireless LAN Controller (WLC) should be installed with the image supported by the Cisco DNA Center.

The workflow and screenshots in the further sections are taken from Cisco DNA Center 1.3.3.

The Identity Service Engine (ISE) needs to be installed and ready with the following personas at a minimum: The Primary PAN/PSN/MNT. Refer to the ISE deployment guide mentioned below to suite a distributed model that supports the scale required. The Identity Service Engine (ISE) has to have the following service running: PxGRID and ERS API.

For more information on the compatible software recommendation for SDA, please refer to the compatibility matrix guide posted below.

SD-Access Compatibility Guide

For Cisco DNA Center install and upgrade process, please follow the instructions on the given link:

Cisco DNA Center Install Guide.

To install and set up the Cisco Wireless LAN Controller (WLC) and to get the initial configuration completed. Please refer the instructions below for the Aire-OS /Catalyst 9800 platforms

Cisco Aire-OS 8540 deployment guide:

Cisco Aire-OS 5520 deployment guide:

Cisco Catalyst 9800 deployment guide:

Installation guide for Identify Service Engine (ISE)

RMA Process for Fabric wireless

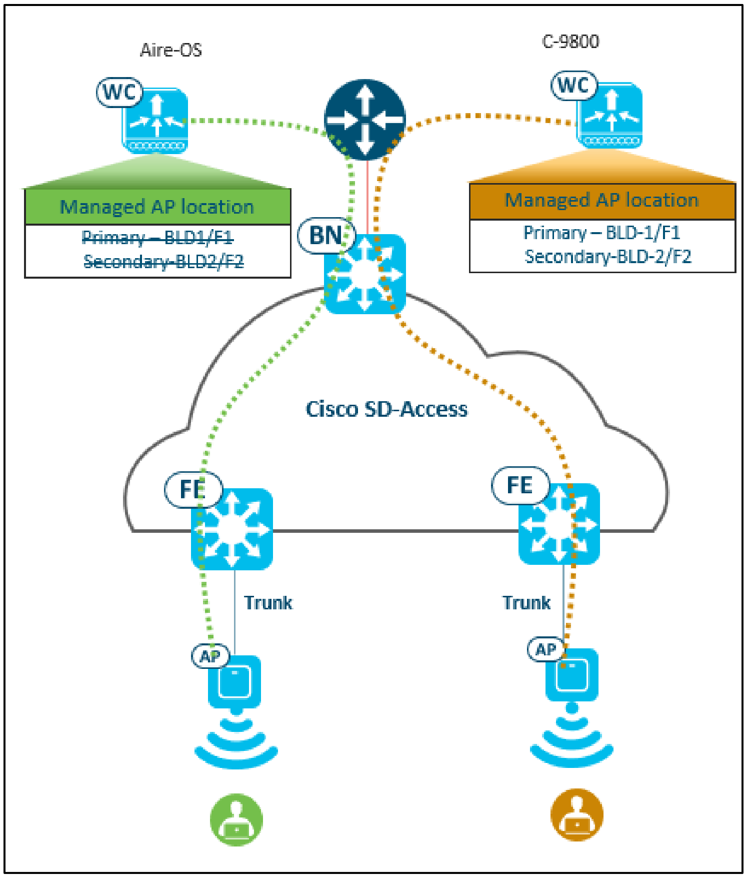
The Return Material Authorization (RMA) workflow in Cisco DNA Center provides users the ease of automation to replace failed devices quickly, thus improving productivity and reducing operational expense. RMA provides a common workflow to replace routers, switches, and access points.

Currently, the RMA workflow on the Cisco DNA center can be utilized only for fabric Access-Point. The RMA workflow for a fabric Wireless Lan Controller and EWC-9k is not supported with Cisco DNA Center 2.2.x.x. To replace a fabric Wireless Lan Controller, kindly raise a TAC case to have an expert drive the RMA process.

For more information on the RMA workflow, please refer to the configuration guide of the Cisco DNA Center.

RMA workflow configuration on the Cisco DNA Center.

Migration: AireOS to C-9800



With the introduction of the Catalyst 9800 Wireless LAN Controller, existing customers who have deployed fabric with the AireOS based controller would require a migration path towards the C-9800 based controller. In this section, we will detail the steps that can aid the customer in migrating their fabric-enabled wireless from AireOS to C9800.

An SD-Access fabric site can support multiple Wireless LAN Controllers within a single fabric site. An exception to this when using EWC-9k. A fabric site can only support a maximum of two embedded wireless LAN controllers within a fabric site. The migration outlined in this section can't be used to migrate from an AireOS to an EWC-9k controller. The first step in the emigration path is to onboard the catalyst C-9800 Wireless LAN Controller on the Cisco DNA Center inventory app. The details of how to discover the device and add them to the inventory are mentioned in the following section:

Discovery of Devices on the Cisco DNA Center

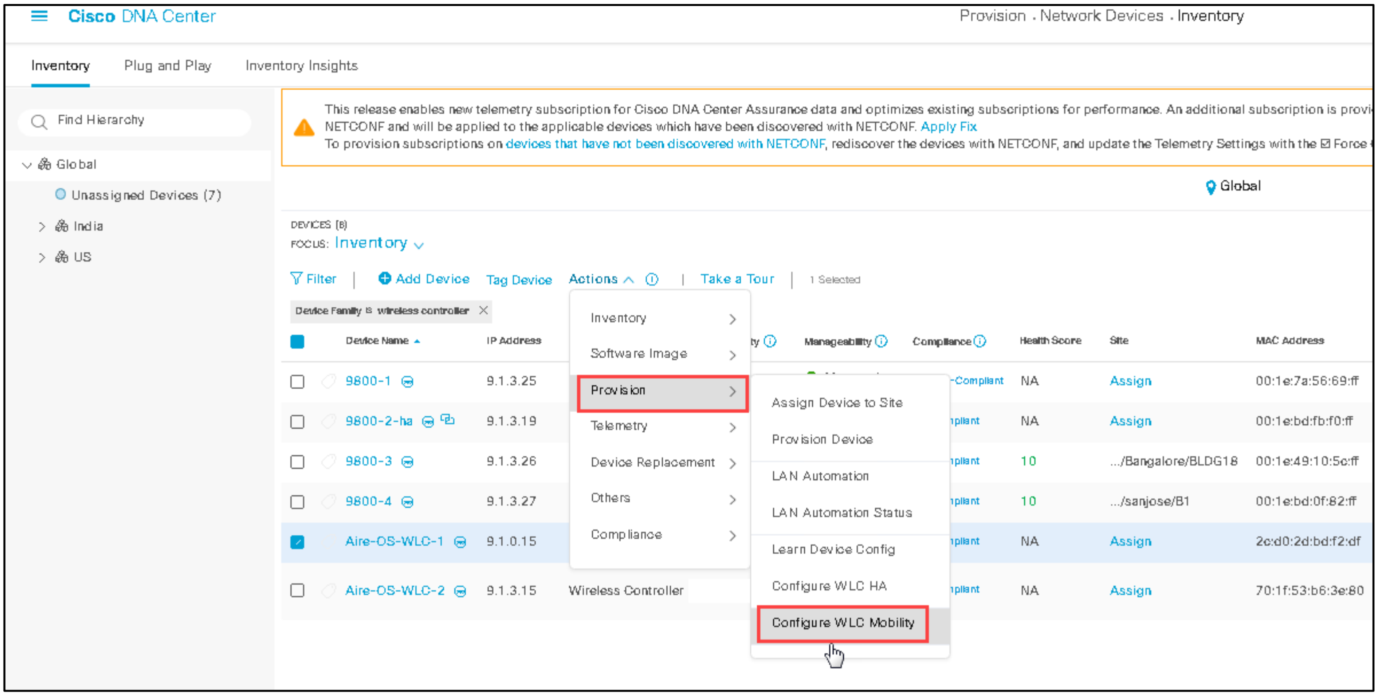
Once the device is discovered and added to the inventory, the device needs to be provisioned. To provision the wireless LAN controller, we would have to take a phased approach. A managed site could either be a building or a floor within the site hierarchy needs to be unmanaged from the current Aire-OS controller and be managed by the C-9800 controller. Once the device is provisioned, the site is migrated and managed by the C-9800 controller. The C-9800 controller can now be added to the fabric as a fabric-enabled Wireless LAN Controller.

Note N+1 HA is not supported with Aire-OS and C-9800 acting as primary and secondary to each other. Due to the config model differences between the Aire-OS based controller and the C-9800, the Cisco DNA center will not provision these controllers to act in N+1 HA mode. The N+1 HA mode in wireless allows controllers to act a primary and secondary for sites, acting as a backup to each other

A site once migrated to the C-9800 controller will have the AP dissociate from the current Aire-OS based controller. The AP will now associate with the C-9800 controller, this can result in a downtime for the AP to download the new image and relevant config from the C-9800 controller. Please ensure that the migration is planned with a proper maintenance window accommodating this downtime.

Seamless roaming is supported for the same SSID across these controllers. A wireless endpoint associated with an AP on an Aire-OS based controller can seamlessly roam to an AP associated with the C-9800 based controller. For seamless roaming to happen the controllers needs to be configured with the respective mobility configuration.

For Cisco DNAC- 2.1.2.x version and below, the mobility configuration is automated by the Cisco DNA Center. For releases 2.2.x.x and above the mobility configuration needs to be provisioned using the workflow provided on the inventory app.

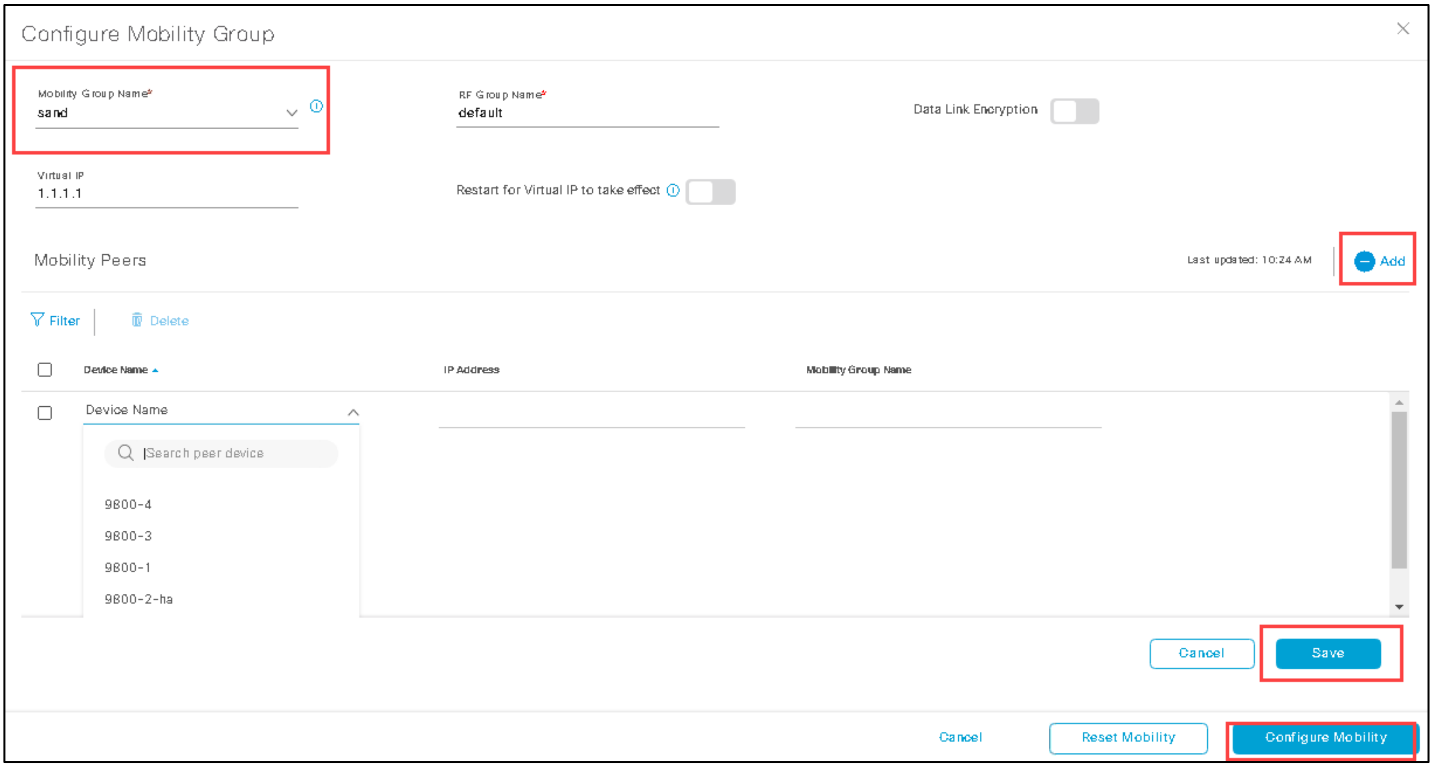


This release enables new telemetry subscription for Cisco DNA Center Assurance data and optimizes existing subscriptions for performance. An additional subscription is provi
NETCONF and will be applied to the applicable devices which have been discovered with NETCONF. Apply Fix
To provision subscriptions on devices that have not been discovered with NETCONF, rediscover the devices with NETCONF, and update the Telemetry Settings with the ☑ Force

Global

DEVICES (8)
FOCUS: Inventory

☐	Device Name	IP Address		Manageability	Compliance	Health Score	Site	MAC Address
☐	9800-1	9.1.3.25			-Compliant	NA	Assign	00:1e:7a:56:69:ff
☐	9800-2-ha	9.1.3.19			pliant	NA	Assign	00:1e:bd:fb:f0:ff
☐	9800-3	9.1.3.26			pliant	10	.../Bangalore/BLDG18	00:1e:49:10:5c:ff
☐	9800-4	9.1.3.27			pliant	10	.../sanjose/B1	00:1e:bd:0f:82:ff
☑	Aire-OS-WLC-1	9.1.0.15			pliant	NA	Assign	2c:d0:2d:bd:f2:df
☐	Aire-OS-WLC-2	9.1.3.15	Wireless Controller		pliant	NA	Assign	70:1f:53:b6:3e:80



Mobility Group Name* sand

RF Group Name* default

Data Link Encryption

Virtual IP 1.1.1.1

Restart for Virtual IP to take effect

☐	Device Name	IP Address	Mobility Group Name
☐	Device Name		

Search peer device

9800-4
9800-3
9800-1
9800-2-ha

Note

Cisco DNA Center expects the mobility name to be user-defined and not to use the default mobility group name for security reasons.

AP fallback a common feature used in wireless to allow an AP to do fallback from the primary controller to the secondary controller is not supported in this scenario. For redundancy aspects, a customer could deploy the Aire-os or the C-9800 WLC in HA-SSO mode.

9800 Embedded Wireless LAN Controller(EWC)

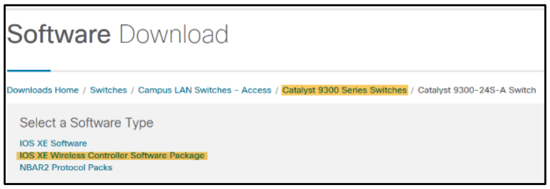
One of the pre-requisites to install the Embedded Wireless Controller on a Catalyst 9k switch is to have netconf enabled. The Cisco DNA Center takes care of the enabling netconf on the device. The netconf is one of the methods the Cisco DNA Center uses to provision configuration to the devices.

The below section highlights the steps required to enable netconf manually on the Catalyst 9k switch if not done through the Cisco DNA Center. For the Cisco DNA center to provision netconf to the device ensure netconf is selected as one of the credentials during the discovery process. The Catalyst Switch should be running in install mode for the wireless package to be installed. The version of the wireless package should be the same as that of the Cisco IOS-XE version running on the switching platform.

If the Catalyst 9k switch is running on 16.11.1c, the 9800-SW package should be of the same version -16.11.1. For the wireless package to install properly you need to have the DNA-advantage license active on the switch. You can check this through show version command. If not, you can activate the evaluation through the normal license commands.

The software for the wireless package on the Catalyst 9k family is located on Cisco.com under the switching product family.

The images are also posted as special releases, to obtain the images under the special release browse through the SDA compatibility matrix.

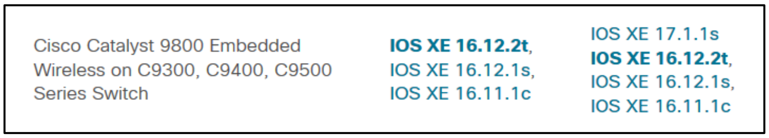


Software Download

Downloads Home / Switches / Campus LAN Switches - Access / Catalyst 9300 Series Switches / Catalyst 9300-24S-A Switch

Select a Software Type

IOS XE Software
IOS XE Wireless Controller Software Package
NBAR2 Protocol Packs



Cisco Catalyst 9800 Embedded Wireless on C9300, C9400, C9500 Series Switch	**IOS XE 16.12.2t**, IOS XE 16.12.1s, IOS XE 16.11.1c	IOS XE 17.1.1s **IOS XE 16.12.2t**, IOS XE 16.12.1s, IOS XE 16.11.1c

The EWC is currently supported only with SD-Access deployments. The Cisco DNA Center is used to provision and install the wireless package on the Catalyst 9k switch.

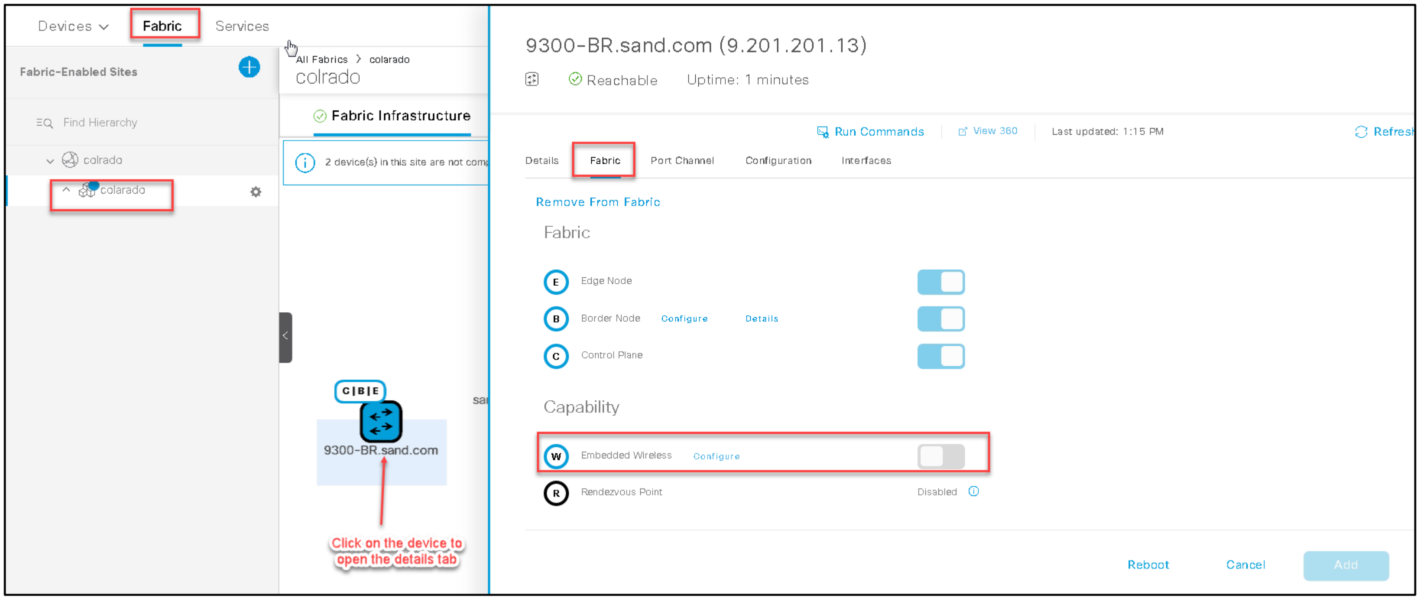
Step 1 check the DNA-advantage license is enabled.

```
Switch#show version | b Technology

Technology Package License Information:

 -----------------------------------------------------------------------------

Technology-package                                   Technology-package

Current                        Type                      Next reboot

------------------------------------------------------------------------------

network-advantage             Permanent           network-advantage

dna-advantage                 Subscription        dna-advantage
```

Step 2 Enable netconf on the Catalyst Switch manually:

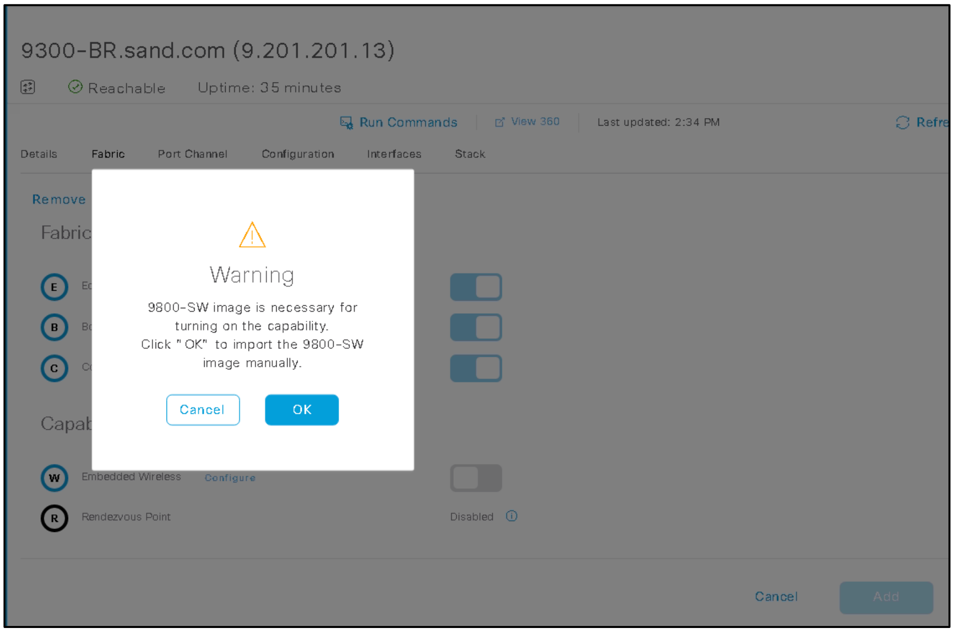
```
Switch(config-t)# netconf-yang -> Enable NETCONF/YANG globally. It may take up to 90 seconds to initialize
Switch(config-t)# aaa new-model
Switch(config-t)# authorization exec default local -> Required for NETCONF-SSH connectivity and edit-config
operations

Switch#show  netconf-yang status
netconf-yang: enabled -> netconf status
netconf-yang ssh port: 830-> Port on which Cisco DNA center to the device
netconf-yang candidate-datastore: disabled
```

Step 3 Once the device is discovered and added to a Fabric, the 9800-SW needs to be enabled on the Catalyst 9k switch. To enable the wireless controller functionality click on the device to open the device details page. In the details page an administrator can see the capabilities supported on the device. One of the capabilities supported is the “Embedded wireless”. Move the slide bar to enable the option.



Click on the device to open the details tab

Step 4 Once the embedded wireless capability is added, the next process involves importing the 9800-SW image on the device using the SWIM module on the Cisco DNA center. Click Ok to go through the SWIM process.



9300-BR.sand.com (9.201.201.13)

Reachable Uptime: 35 minutes

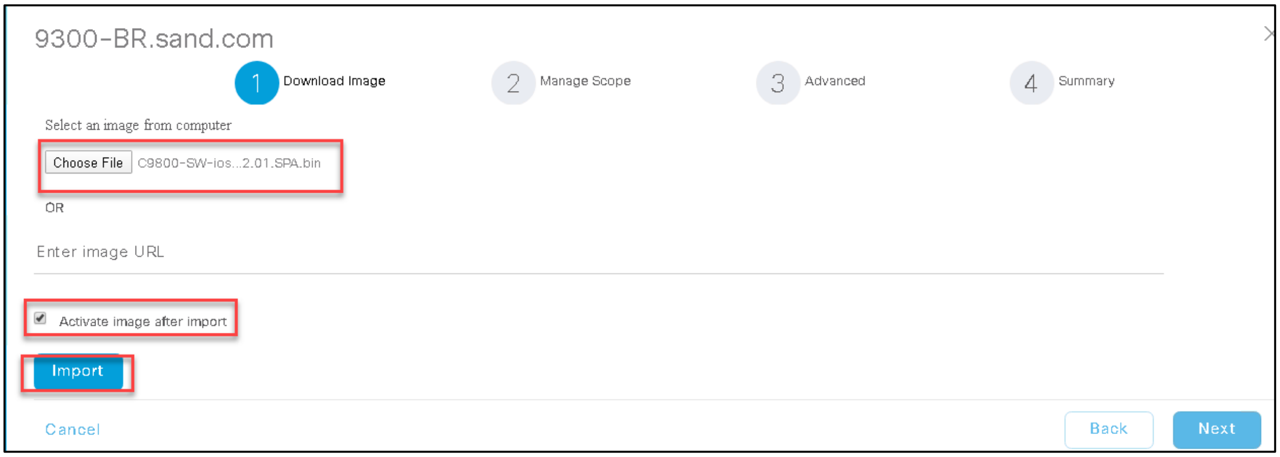
Last updated: 2:34 PM

Warning

9800-SW image is necessary for turning on the capability. Click " OK" to import the 9800-SW image manually.

Disabled

Step 5 Specify the location of the image. Enable the activate option and click on "Import"



9300-BR.sand.com

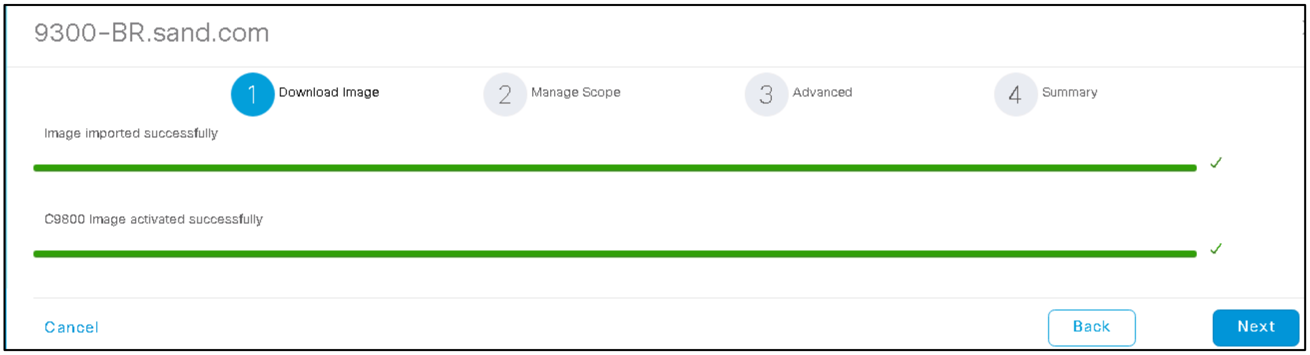
Select an image from computer

C9800-SW-ios...2.01.SPA.bin

OR

Enter image URL

☑ Activate image after import

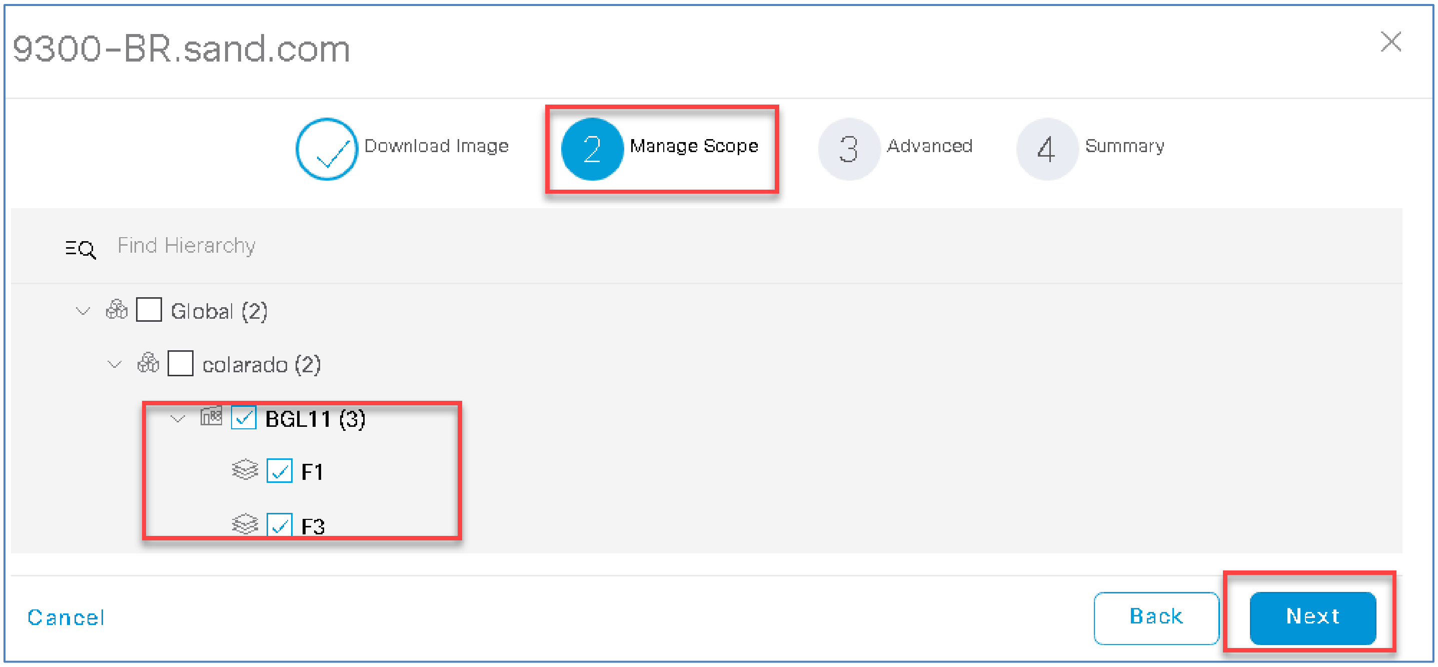


9300-BR.sand.com

Image imported successfully ✓

C9800 Image activated successfully ✓

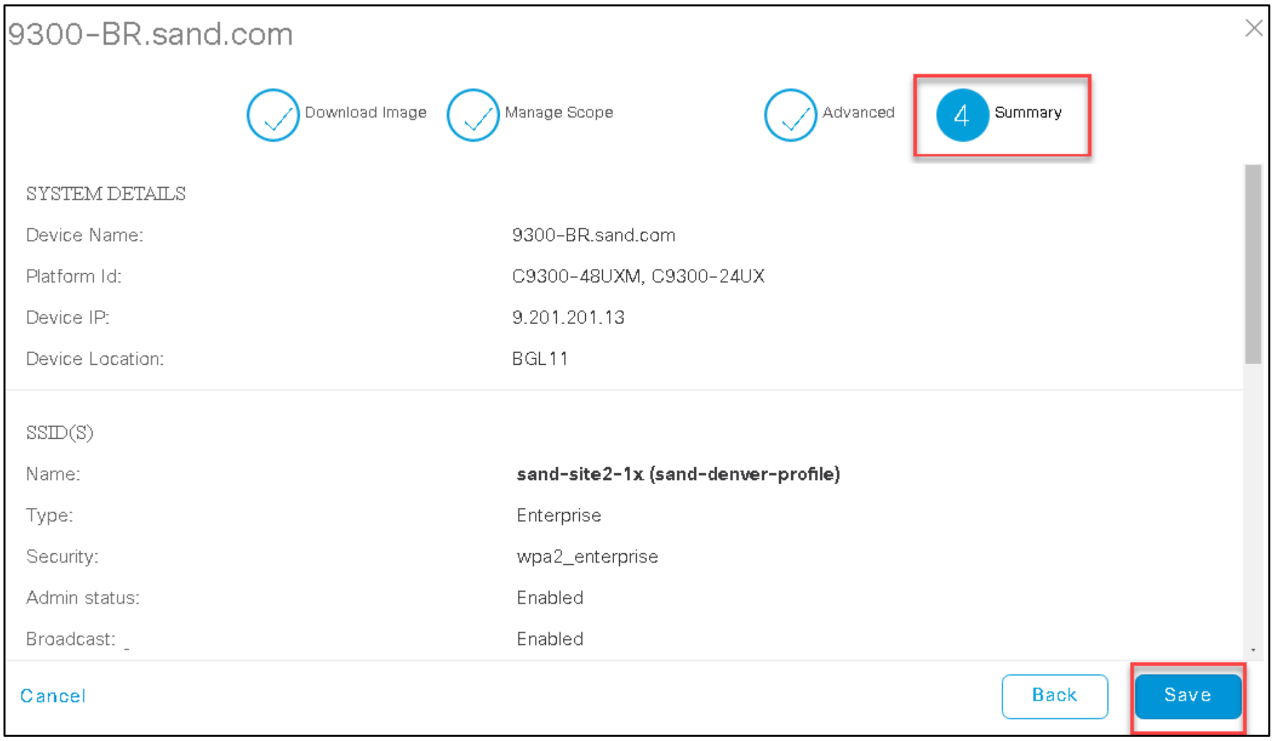
Step 6 Once the image is imported and activated on the device, select the sites that are managed by the device.



9300-BR.sand.com

- □ Global (2)
  - □ colarado (2)
    - ☑ BGL11 (3)
      - ☑ F1
      - ☑ F3

Step 7 The Cisco DNA center shows the summary of the config provisioned on the device such as the SSID config.



9300-BR.sand.com

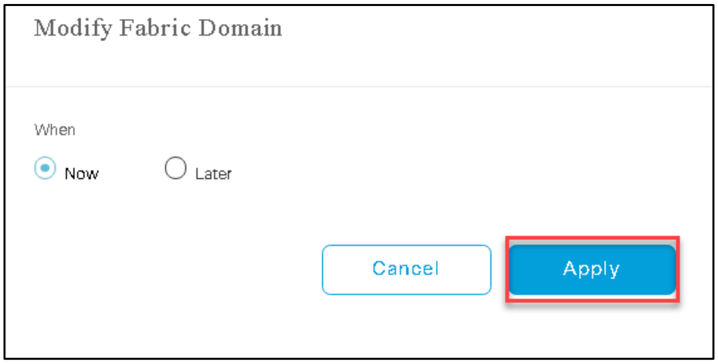
SYSTEM DETAILS

Device Name:	9300-BR.sand.com
Platform Id:	C9300-48UXM, C9300-24UX
Device IP:	9.201.201.13
Device Location:	BGL11

SSID(S)

Name:	**sand-site2-1x (sand-denver-profile)**
Type:	Enterprise
Security:	wpa2_enterprise
Admin status:	Enabled
Broadcast:	Enabled

Step 8 After the embedded wireless is added, save the fabric configuration:



Modify Fabric Domain

When

● Now ○ Later

Fabric Enabled AP and Catalyst 4500E as Fabric Edge

Special consideration should be taken if the SD-Access fabric consists of a catalyst 4500E as a Fabric Edge (FE) and the AP's are directly connected. With Fabric Enabled Wireless (FEW) the Cisco Access-point creates a VxLAN tunnel to the respective Fabric Edge. To have the Catalyst 4500E to support the VxLAN tunnel, the switch needs to be booted in install mode. The daughter card on the switch is responsible for the de-encapsulation of the VxLAN header coming from the access-tunnel.

For the recommended release, Supervisor modules, and the line cards that are supported with the Catalyst 4500E, please refer to the SDA compatibility guide.

The other important consideration is that the ports on the Supervisor module must be used for connecting upstream to the rest of

the fabric, while the Access Points (AP) can be connected directly to the supported line cards.

To verify if the daughter card is enabled on the platform, please use the show module CLI:

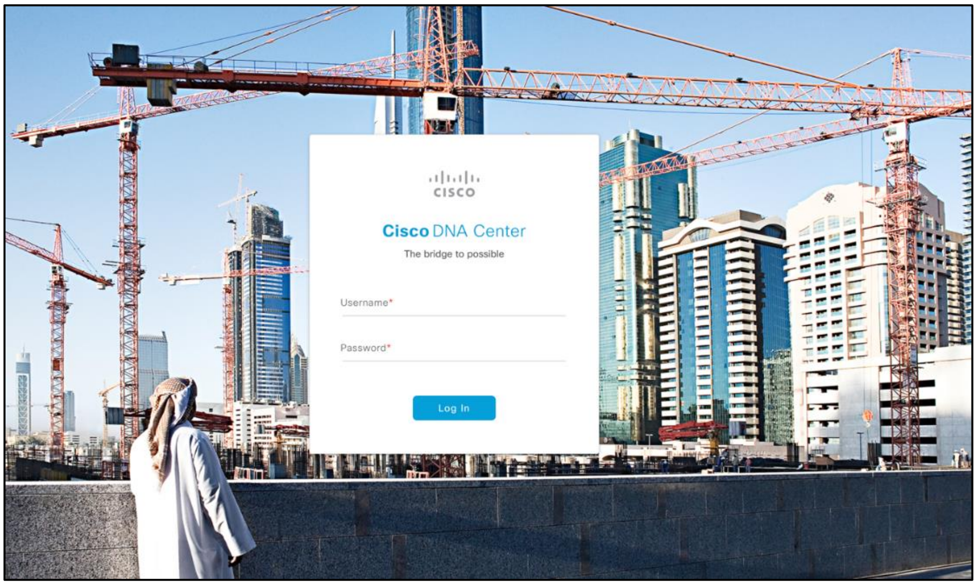
```
4503-02#show module
Chassis Type : WS-C4503-E

Power consumed by backplane : 0 Watts

Mod Ports Card Type                              Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 1    12  Sup 8-E 10GE (SFP+), 1000BaseX (SFP)   WS-X45-SUP8-E      CAT1947L0LU
 2    12  10GE SFP+                              WS-X4712-SFP+E     CAT1849L2F2
 3    48  100/1000/2500/5000/10GBaseT UPOE E Ser WS-X4748-12X48U+E  CAT1925L9E3

 M MAC addresses                    Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 1 a89d.21d7.70c0 to a89d.21d7.70cb 1.3 15.1(1r)SG17 03.11.00.E       Ok
 2 74a0.2fa2.eec8 to 74a0.2fa2.eed3 2.0                               Ok
 3 78ba.f9a0.9270 to 78ba.f9a0.929f 1.0 0.0                           Ok

Mod  Submodule               Model             Serial No.   Hw   Status
----+-----------------------+-----------------+------------+----+---------
 1   Daughter Card           WS-UA-SUP8E       CAT1948LG9Z  1.1  Ok

Mod LinecardMode
----+---------------------------------------------------------------------
3     1

4503-02#
```

SD-Access WLC underlay discovery

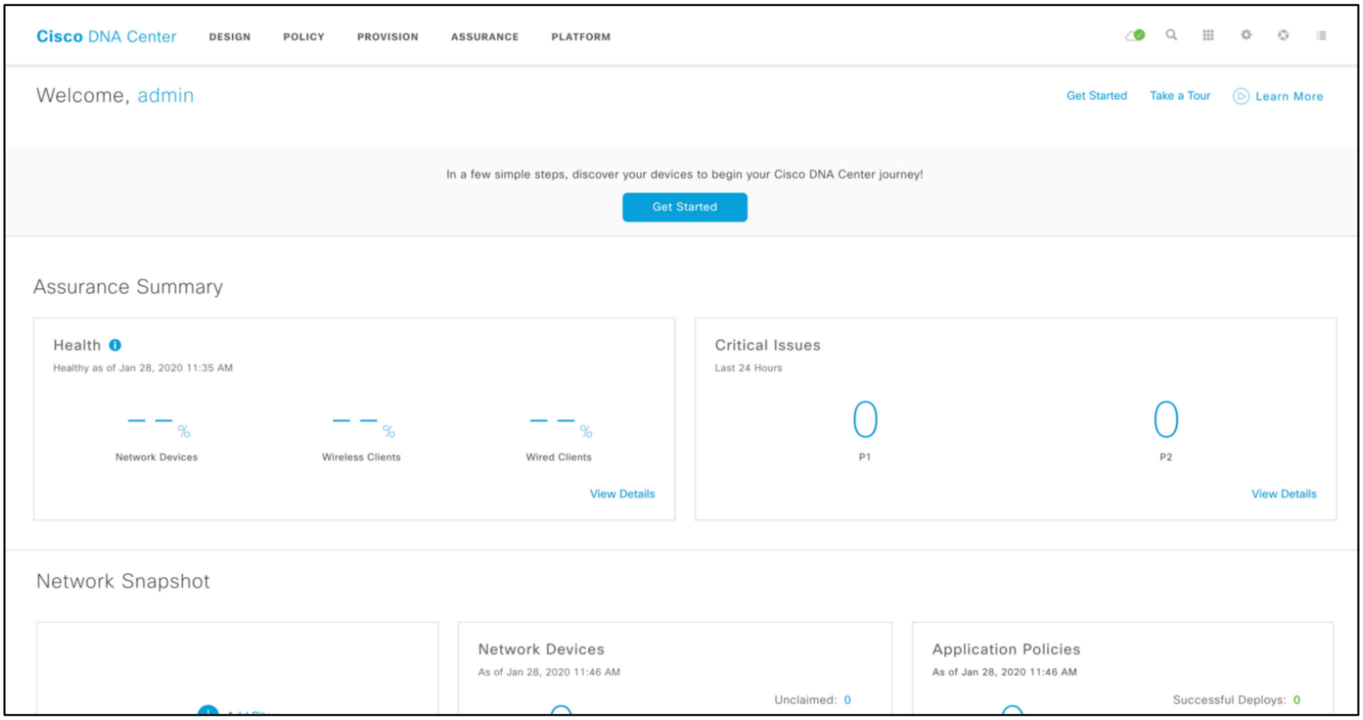
Please upgrade your browser to the latest version before logging in to Cisco DNA Center.

Procedure

Step 1 Log in to Cisco DNA Center using the management IP address and credentials assigned when it was installed.



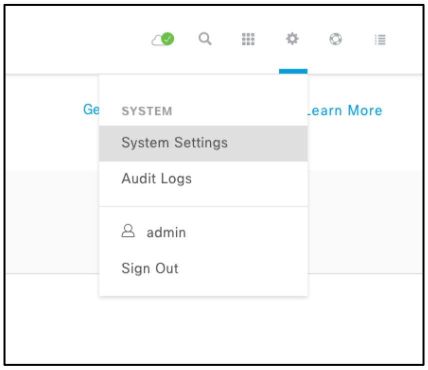
Step 2 Once logged in, you will see the Cisco DNA Center landing page.



In a few simple steps, discover your devices to begin your Cisco DNA Center journey!

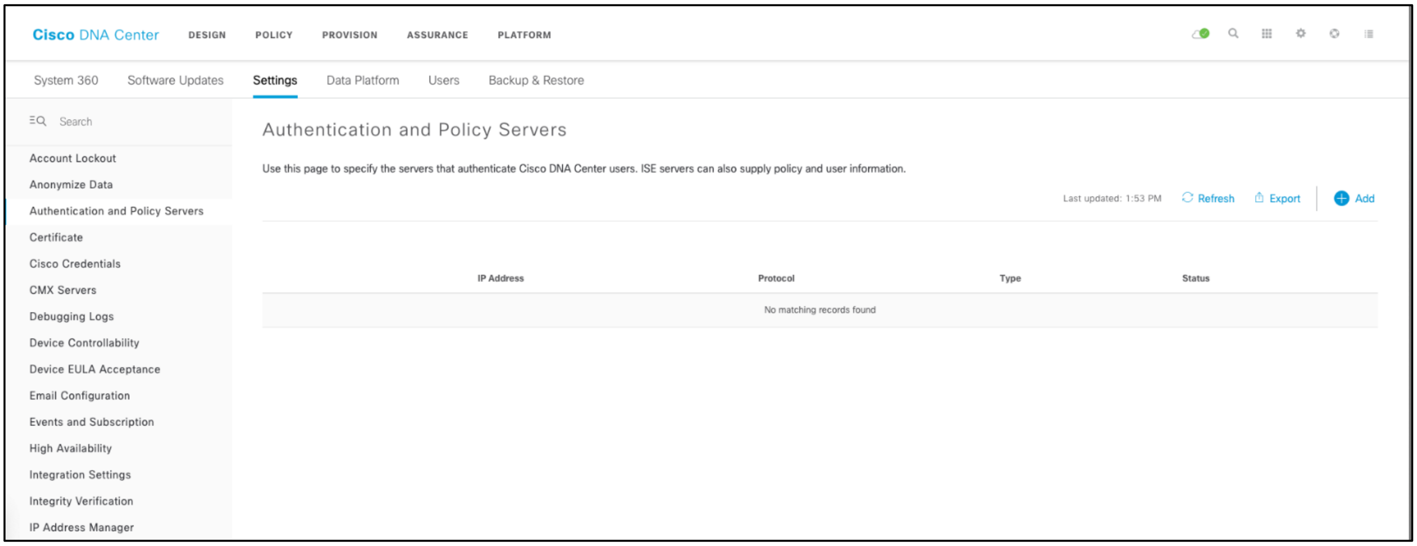
Adding ISE to Cisco DNA Center

Cisco DNA Center must be able to communicate securely with ISE to be able to download SGTs and create new policies. The ISE server and Cisco DNA Center exchange information through pxGrid and REST API services.



Adding ISE to Cisco DNA Center is a very simple operation: in Cisco DNA Center, go to System Settings by clicking the “gear” symbol on the right top corner of the homepage:

On the System Settings page, click Authentication and Policy Servers and click Add to add a new server:



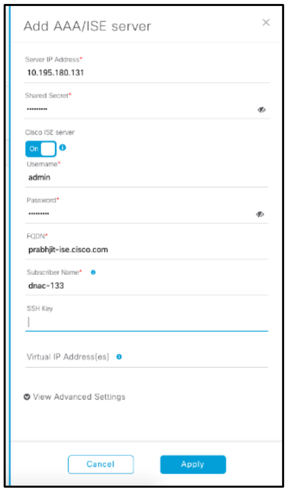
Authentication and Policy Servers

Use this page to specify the servers that authenticate Cisco DNA Center users. ISE servers can also supply policy and user information.

Last updated: 1:53 PM

IP Address	Protocol	Type	Status
No matching records found			

Fill in the ISE information (remember to toggle the “Cisco ISE server” switch):


Add AAA/ISE server

Server IP Address*
10.195.180.131

Shared Secret*
•••••••••

Cisco ISE server
On

Username*
admin

Password*
•••••••••

FQDN*
prabhjit-ise.cisco.com

Subscriber Name*
dnac-133

SSH Key

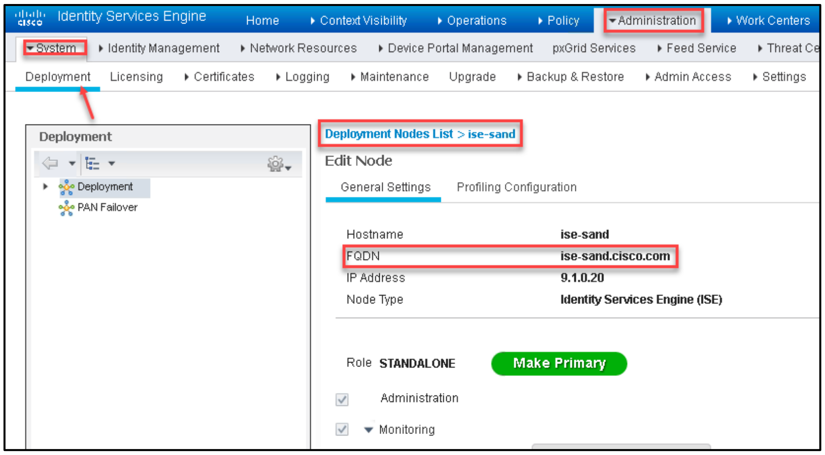
Virtual IP Address(es)

.

The shared secret defines the passphrase used on the network devices (switches and WLC) and the same is configured on the ISE when creating a Network Access Device(NAD). The Cisco DNA center automates the radius server configuration on the network devices and the NAD configuration on the ISE server. The username and password are the administrator credentials for the ISE cluster. Enter the FQDN for ISE (hostname plus domain name).

Note: Ensure the administrator credentials are the same for web GUI and SSH access.

As of today, Cisco DNA Center will not verify the FQDN with DNS, but the name has to match the real name of the ISE server. Don’t forget to add a subscriber name; this is important to establish the pxGrid credentials (this name doesn’t have to match any existing user name on ISE).



Hostname ise-sand
FQDN ise-sand.cisco.com
IP Address 9.1.0.20
Node Type Identity Services Engine (ISE)

Role STANDALONE

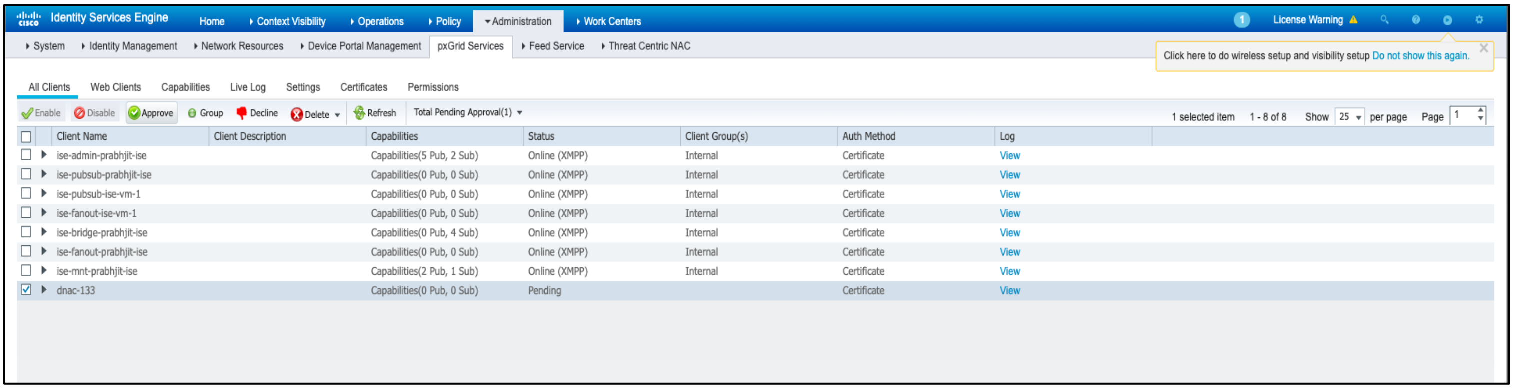
☑ Administration

☑ Monitoring

The FQDN name for the ISE cluster can be obtained by logging into the Web GUI of the primary PAN and navigating to the following link.

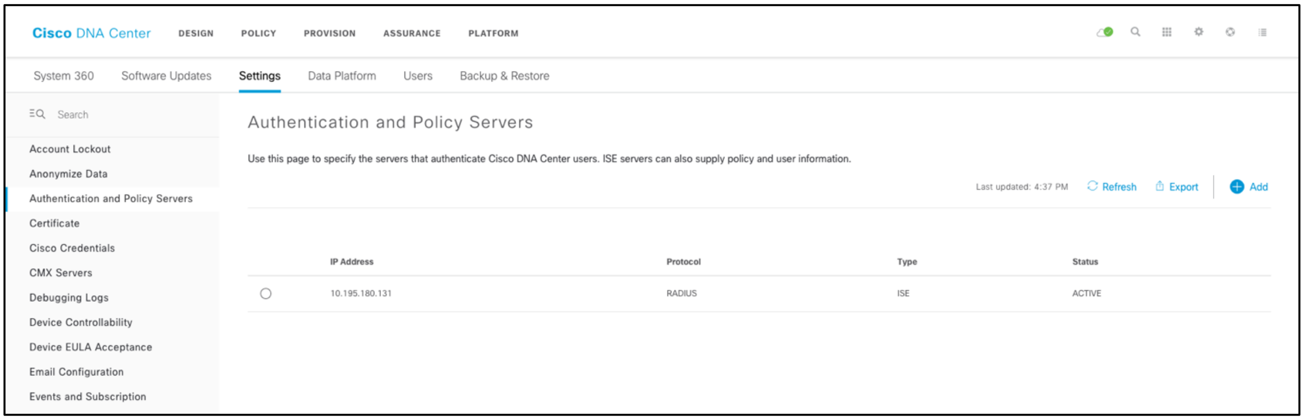
Administration > System>Deployment> hostname of the cluster

Go to ISE and approve the Cisco DNAC’s pxgrid connection by approving the subscriber name – dnac-133 by going to **Administration > pxGrid Services**.



☐	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
☐	ise-admin-prabhjit-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-pubsub-prabhjit-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-pubsub-ise-vm-1		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-fanout-ise-vm-1		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-bridge-prabhjit-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-fanout-prabhjit-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
☐	ise-mnt-prabhjit-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
☑	dnac-133		Capabilities(0 Pub, 0 Sub)	Pending		Certificate	View

Check the status of ISE on Cisco DNAC.



Authentication and Policy Servers

Use this page to specify the servers that authenticate Cisco DNA Center users. ISE servers can also supply policy and user information.

Last updated: 4:37 PM

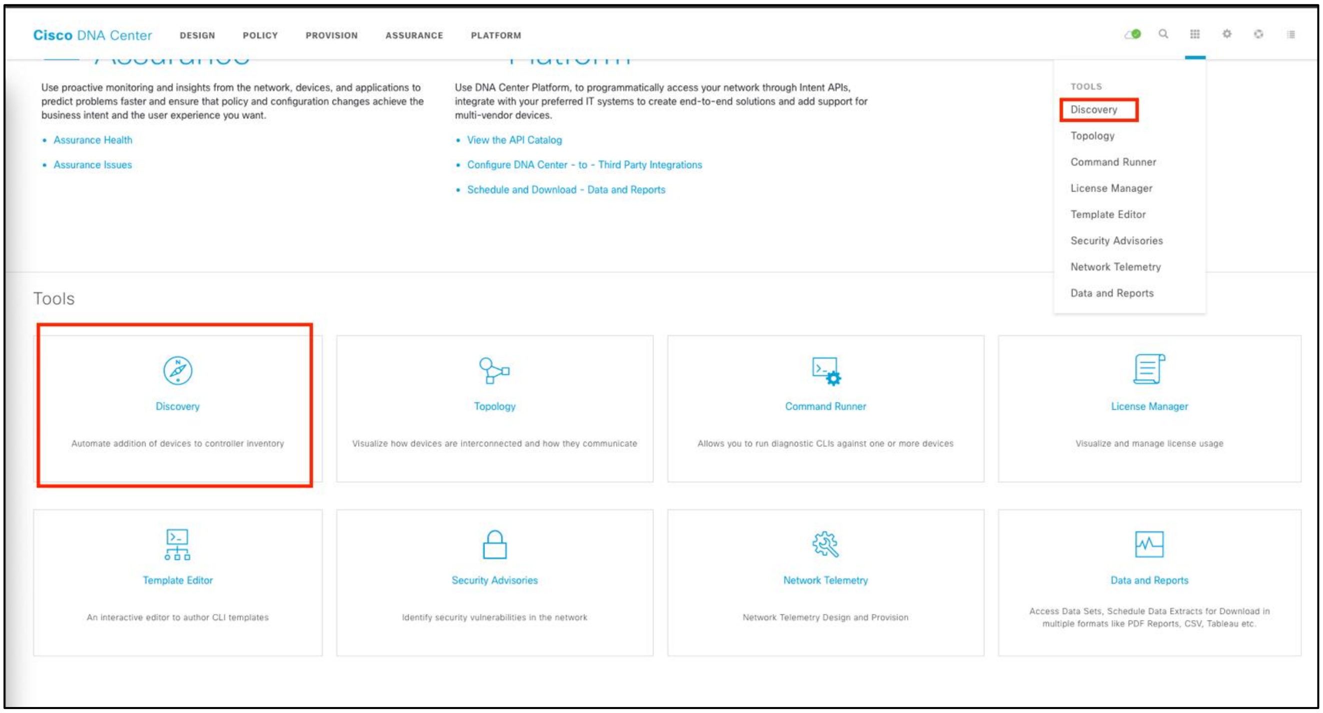
	IP Address	Protocol	Type	Status
○	10.195.180.131	RADIUS	ISE	ACTIVE

SD-Access WLC discovery

In Cisco DNA Center, the Discovery tool is used to find existing underlay devices using Cisco Discovery Protocol or IP address ranges. The assumption here is that the wired network has already been discovered.

Procedure

Step 1 In the homepage of Cisco DNAC, scroll down to **Tools** > **Discovery** or on top right > Discovery to discover your devices and begin the Cisco DNA Center journey.



Use proactive monitoring and insights from the network, devices, and applications to predict problems faster and ensure that policy and configuration changes achieve the business intent and the user experience you want.

Use DNA Center Platform, to programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.

Automate addition of devices to controller inventory

Visualize how devices are interconnected and how they communicate

Allows you to run diagnostic CLIs against one or more devices

Visualize and manage license usage

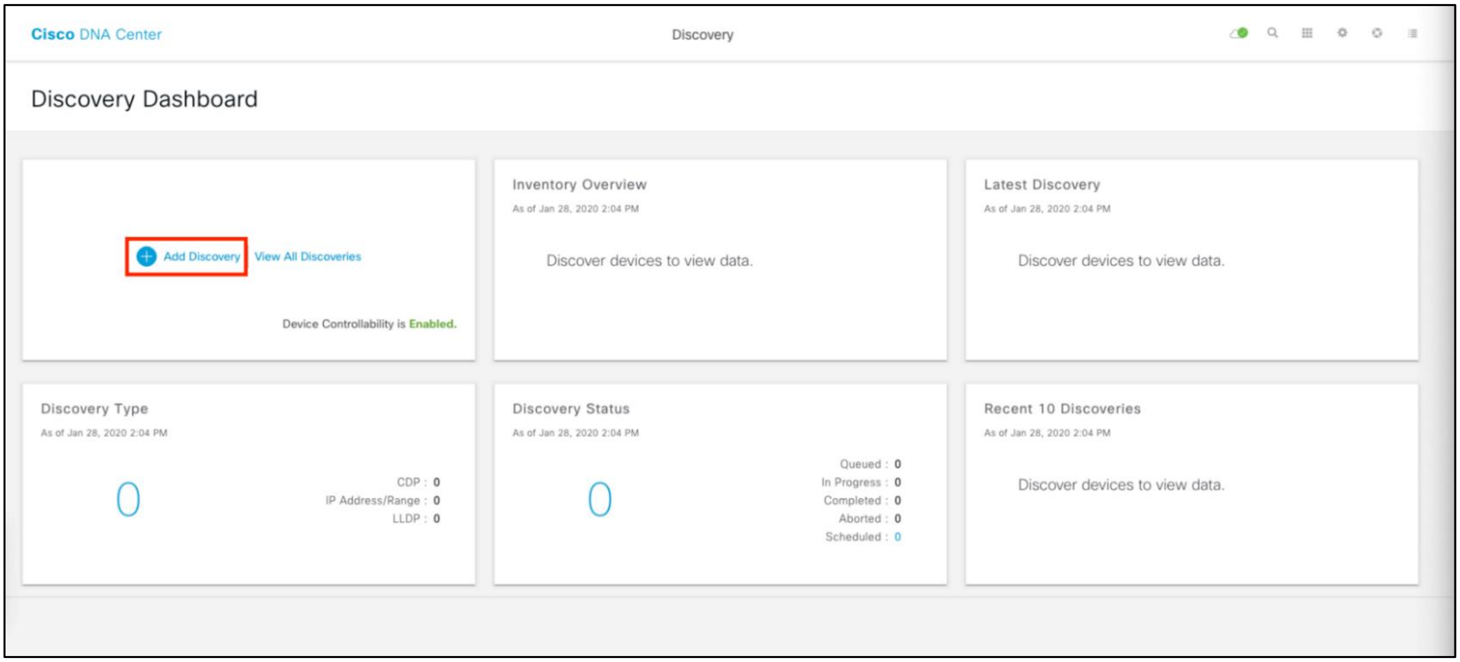
An interactive editor to author CLI templates

Identify security vulnerabilities in the network

Network Telemetry Design and Provision

Access Data Sets, Schedule Data Extracts for Download in multiple formats like PDF Reports, CSV, Tableau etc.

This will take us to the Discovery dashboard where an overview of discovered devices can be seen. Click on “Add Discovery” to start a new discovery.



Device Controllability is Enabled.

Inventory Overview
As of Jan 28, 2020 2:04 PM
Discover devices to view data.

Latest Discovery
As of Jan 28, 2020 2:04 PM
Discover devices to view data.

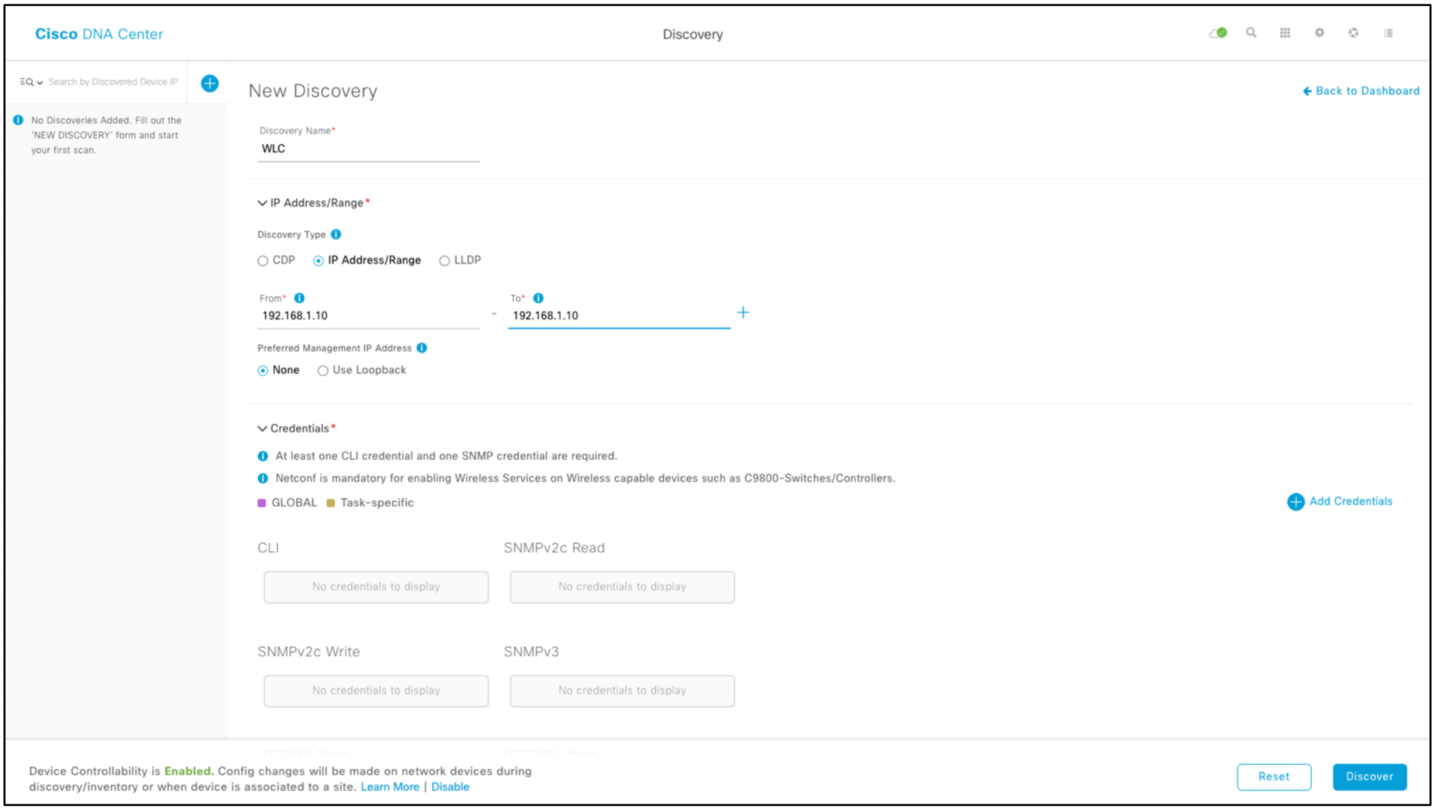
Discovery Type
As of Jan 28, 2020 2:04 PM
CDP : 0
IP Address/Range : 0
LLDP : 0

Discovery Status
As of Jan 28, 2020 2:04 PM
Queued : 0
In Progress : 0
Completed : 0
Aborted : 0
Scheduled : 0

Recent 10 Discoveries
As of Jan 28, 2020 2:04 PM
Discover devices to view data.

Step 2 Enter a Discovery Name, select Range for discovery type, enter the management IP address of your network WLC as the start and end of the range. Ensure that the Wireless management interface option is selected. In case of Aire-OS this would be management interface and in case of 9800 the wireless management interface. Please specific the exact IP and don't specify the range as this would cause DNAC to discover the RMI interface if the WLC is in HA mode.

Ensure the device controllability is enabled on Cisco DNA Center for assurance to work as there is no way to enable if the WLC is discovered in disabled mode.



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

New Discovery

Discovery Name*: WLC

IP Address/Range*

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

From*: 192.168.1.10 - To*: 192.168.1.10

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: No credentials to display

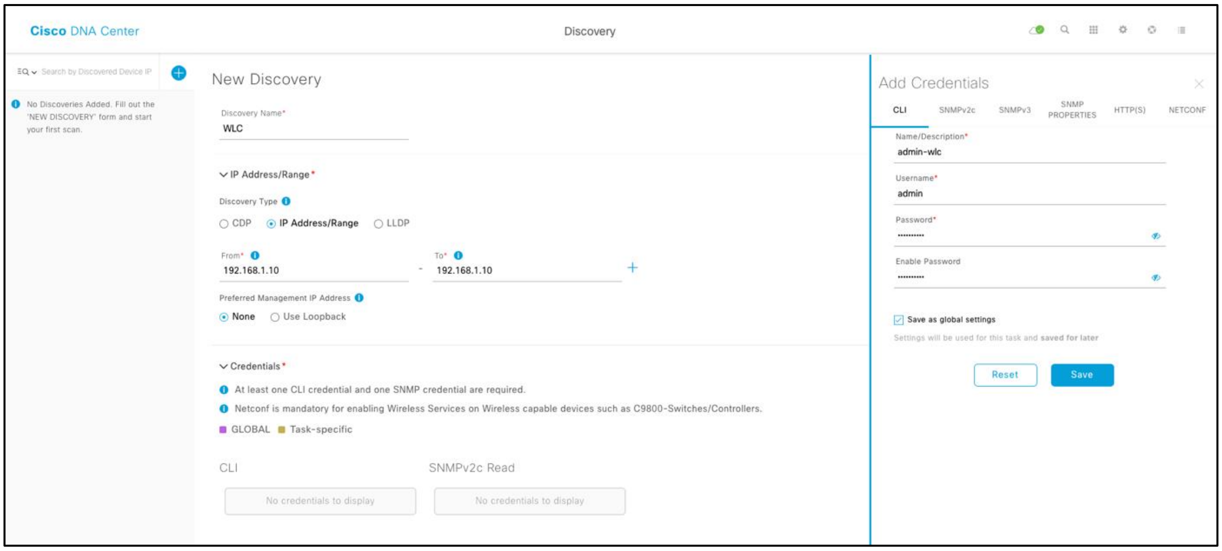
SNMPv2c Read: No credentials to display

SNMPv2c Write: No credentials to display

SNMPv3: No credentials to display

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

Step 3 Click on "Add Credentials" to add credentials to access WLC. Fill in the device Simple Network Management Protocol (SNMP) credentials (read and write) as shown below:



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

New Discovery

Discovery Name*: WLC

IP Address/Range*

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

From*: 192.168.1.10 - To*: 192.168.1.10

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: No credentials to display

SNMPv2c Read: No credentials to display

Add Credentials

Name/Description*: admin-wlc

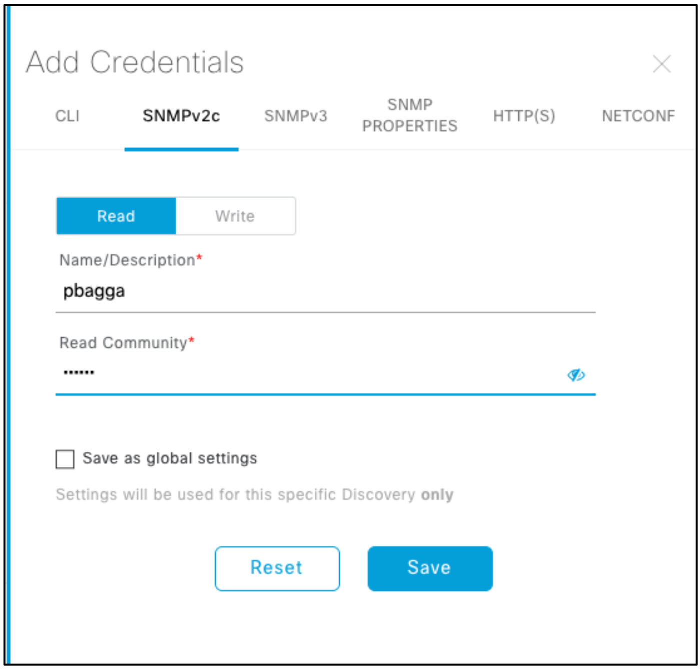
Username*: admin

Password*: ••••••••••

Enable Password: ••••••••••

☑ Save as global settings

Settings will be used for this task and **saved for later**

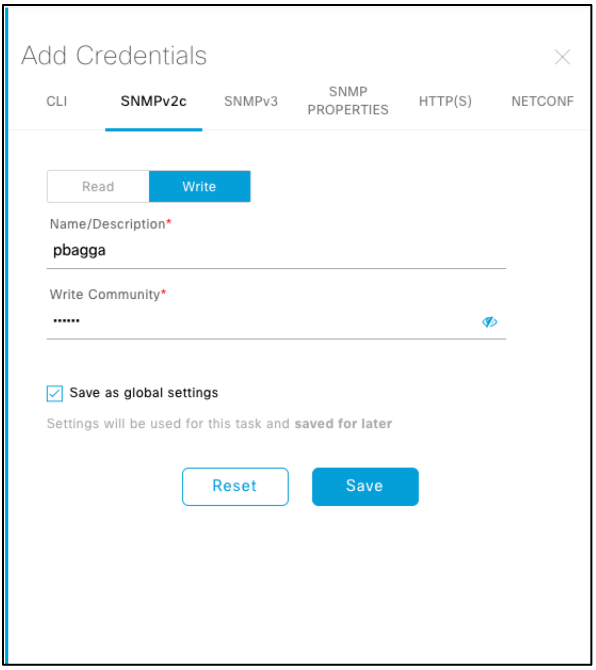


Name/Description* pbagga

Read Community* ••••••

□ Save as global settings

Settings will be used for this specific Discovery **only**



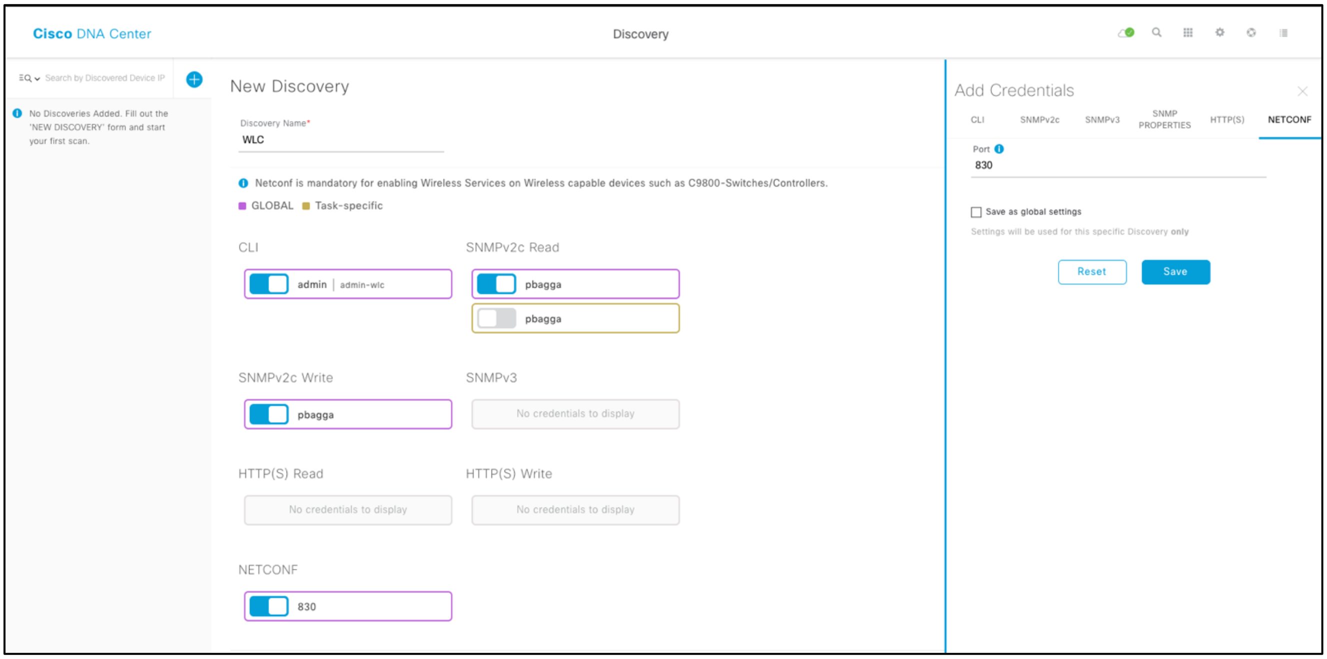
Name/Description* pbagga

Write Community* ••••••

☑ Save as global settings

Settings will be used for this task and **saved for later**

Enabling all the given options for the credentials during the discovery will initiate the Cisco DNA Center to configure them on the discovered WLC. The Cisco DNA Center will log in to the device through Telnet/SSH and enable SNMP and netconf on the device. The SNMP read/write is used for Assurance, while the netconf being one of the methods to provision configuration on the Wireless LAN Controller (WLC). Please refer to the Wireless LAN controller configuration guide on how to enable SSH on the platform.



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

Discovery Name* WLC

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

■ GLOBAL ■ Task-specific

CLI: admin | admin-wlc

SNMPv2c Read: pbagga; pbagga

SNMPv2c Write: pbagga

SNMPv3: No credentials to display

HTTP(S) Read: No credentials to display

HTTP(S) Write: No credentials to display

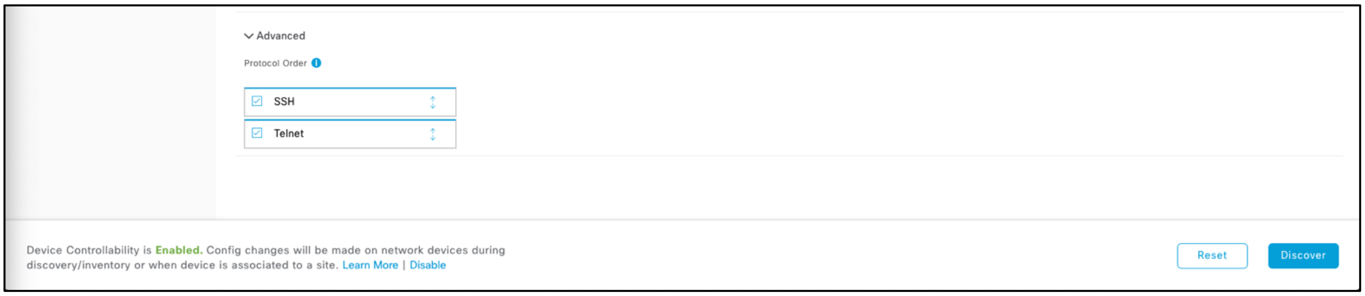
NETCONF: 830

Port 830

□ Save as global settings

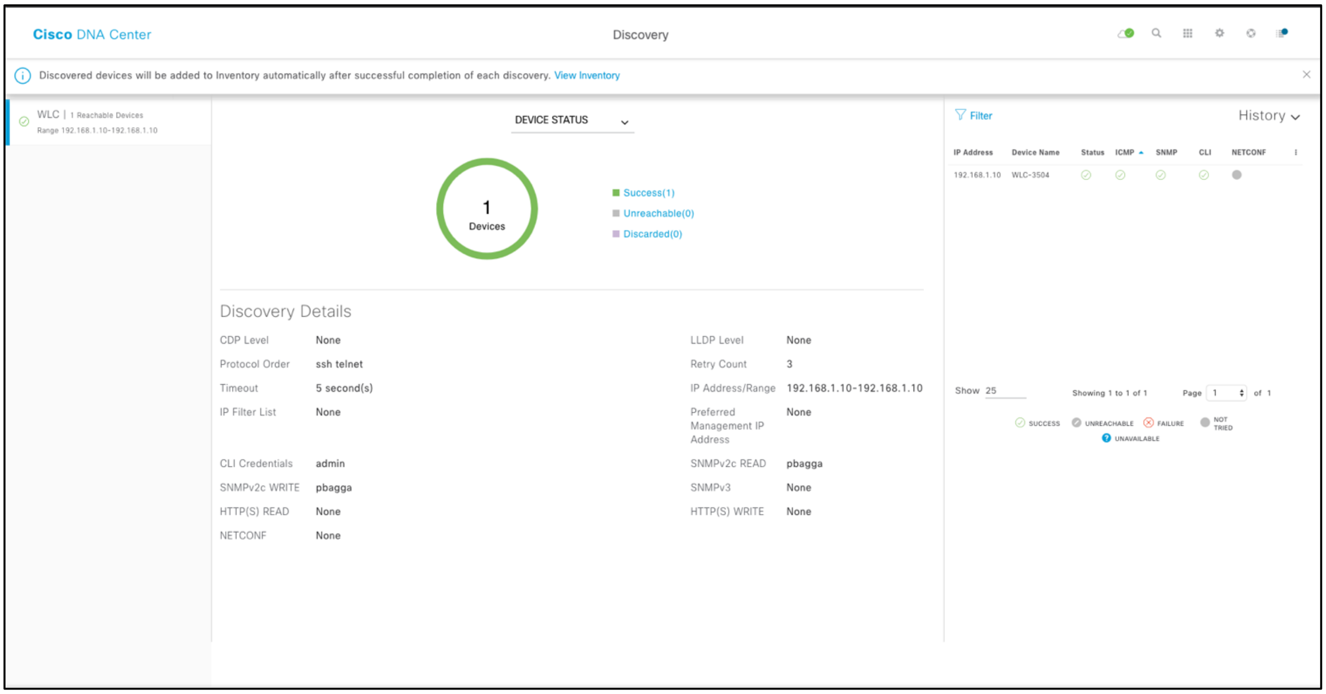
Settings will be used for this specific Discovery **only**

Step 4 Collapse the Credentials section and expand the Advanced section. Select Telnet and/or SSH by clicking on it. SSH is enabled by default on the AIRE-OS based Wireless LAN Controller (WLC). To enable SSH on the Catalyst 9800 WirelessLAN Controller(WLC), refer to the configuration guide.



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

Click Discover in the lower right corner. Once the discovery starts, the page will present the discovery settings and details.



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

Discovery Details

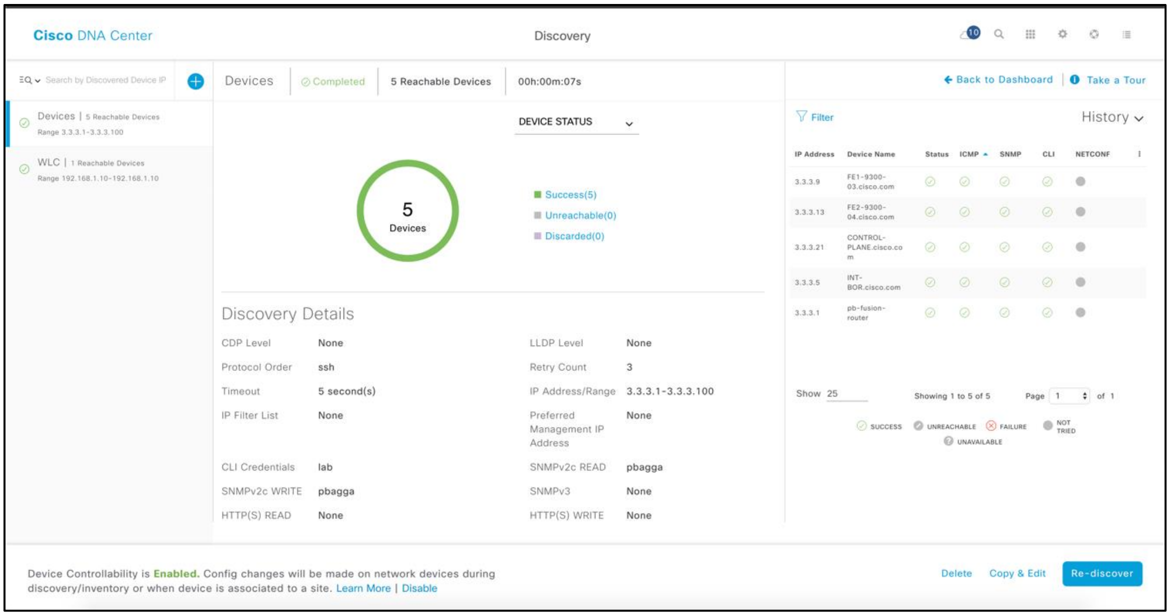
CDP Level	None	LLDP Level	None
Protocol Order	ssh telnet	Retry Count	3
Timeout	5 second(s)	IP Address/Range	192.168.1.10-192.168.1.10
IP Filter List	None	Preferred Management IP Address	None
CLI Credentials	admin	SNMPv2c READ	pbagga
SNMPv2c WRITE	pbagga	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	None		

IP Address	Device Name	Status	ICMP	SNMP	CLI	NETCONF
192.168.1.10	WLC-3504	✓	✓	✓	✓	●

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

Similarly, discover other devices in your network that you would like to make part of the fabric. Names of wired devices will begin appearing on the right of the screen as they are discovered.

Again, the assumption here is that the other fabric wired devices (border and edge nodes) have been discovered already. Cisco Discovery Protocol discovery is recommended for switches.



Discovery Details

CDP Level	None	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Address/Range	3.3.3.1-3.3.3.100
IP Filter List	None	Preferred Management IP Address	None
CLI Credentials	lab	SNMPv2c READ	pbagga
SNMPv2c WRITE	pbagga	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None

IP Address	Device Name	Status	ICMP	SNMP	CLI	NETCONF
3.3.3.9	FE1-9300-03.cisco.com	✓	✓	✓	✓	●
3.3.3.13	FE2-9300-04.cisco.com	✓	✓	✓	✓	●
3.3.3.21	CONTROL-PLANE.cisco.com	✓	✓	✓	✓	●
3.3.3.5	INT-BOR.cisco.com	✓	✓	✓	✓	●
3.3.3.1	pb-fusion-router	✓	✓	✓	✓	●

Show 25 Showing 1 to 5 of 5 Page 1 of 1

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

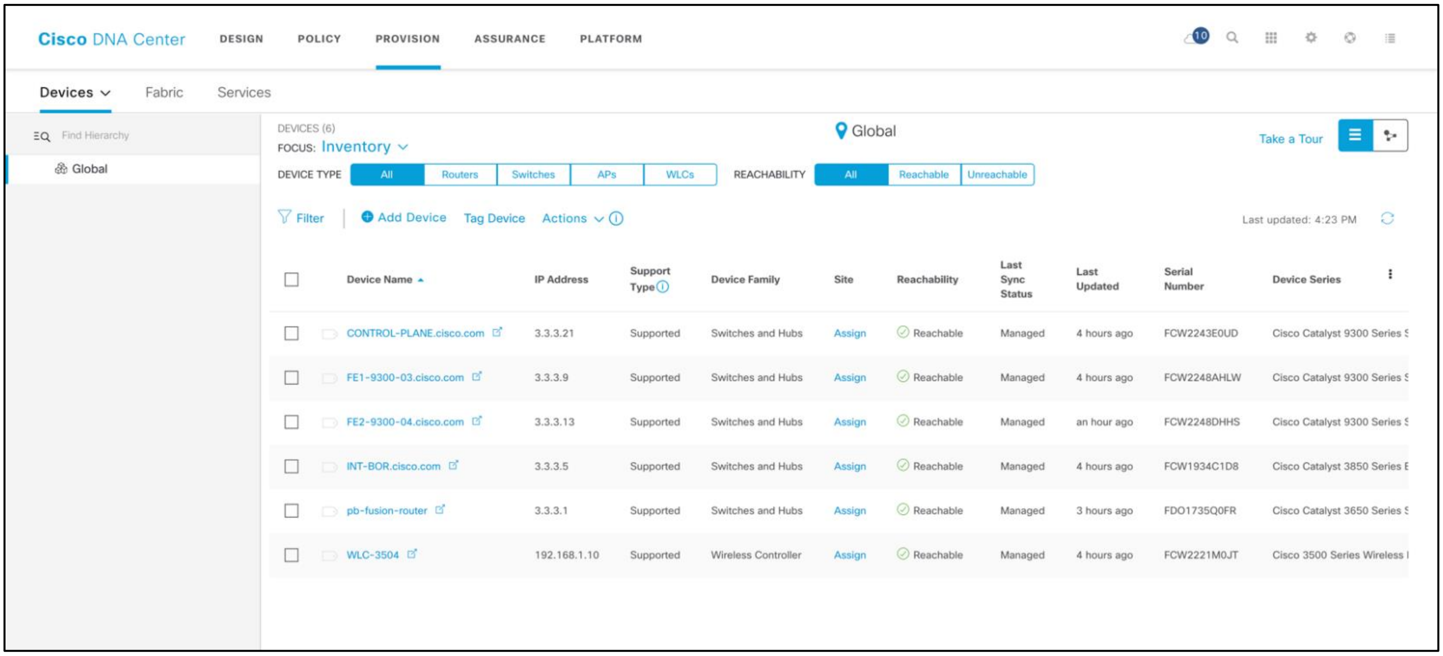
Once the device discovery is complete, all of the discovered devices are populated into the device inventory of the Cisco DNA Center.

Inventory app

Procedure

Once the devices are discovered, click on Provision > Inventory up top to open the Device Inventory app to view the discovered devices. In the Provision > Inventory page, all the devices should have a "Reachability Status" of "Reachable," and the "Last Inventory Collection Status" should be "Managed."

If you have jumped over the discovery steps above, make sure the devices are listed as managed. If they are not, you need to correct this before proceeding.



Last updated: 4:23 PM

	Device Name	IP Address	Support Type	Device Family	Site	Reachability	Last Sync Status	Last Updated	Serial Number	Device Series
□	CONTROL-PLANE.cisco.com	3.3.3.21	Supported	Switches and Hubs	Assign	✓ Reachable	Managed	4 hours ago	FCW2243E0UD	Cisco Catalyst 9300 Series S
□	FE1-9300-03.cisco.com	3.3.3.9	Supported	Switches and Hubs	Assign	✓ Reachable	Managed	4 hours ago	FCW2248AHLW	Cisco Catalyst 9300 Series S
□	FE2-9300-04.cisco.com	3.3.3.13	Supported	Switches and Hubs	Assign	✓ Reachable	Managed	an hour ago	FCW2248DHHS	Cisco Catalyst 9300 Series S
□	INT-BOR.cisco.com	3.3.3.5	Supported	Switches and Hubs	Assign	✓ Reachable	Managed	4 hours ago	FCW1934C1D8	Cisco Catalyst 3850 Series E
□	pb-fusion-router	3.3.3.1	Supported	Switches and Hubs	Assign	✓ Reachable	Managed	3 hours ago	FDO1735Q0FR	Cisco Catalyst 3650 Series S
□	WLC-3504	192.168.1.10	Supported	Wireless Controller	Assign	✓ Reachable	Managed	4 hours ago	FCW2221M0JT	Cisco 3500 Series Wireless I

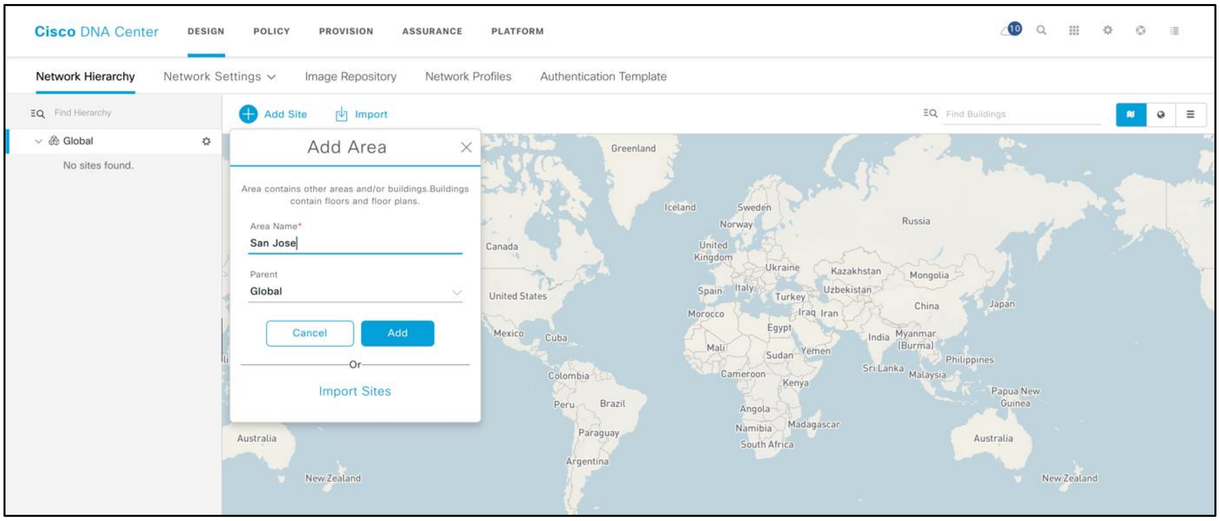
SD-Access Design

Get started using Cisco DNA Center Design

Cisco DNA Center provides a robust Design application to allow customers of every size and scale to easily define their physical sites and common resources. This is implemented using a hierarchical format for intuitive use, while removing the need to redefine the same resource in multiple places when provisioning devices.

Procedure

Step 1 Create the sites and site hierarchy of your network, using the Design page similar to the example below.

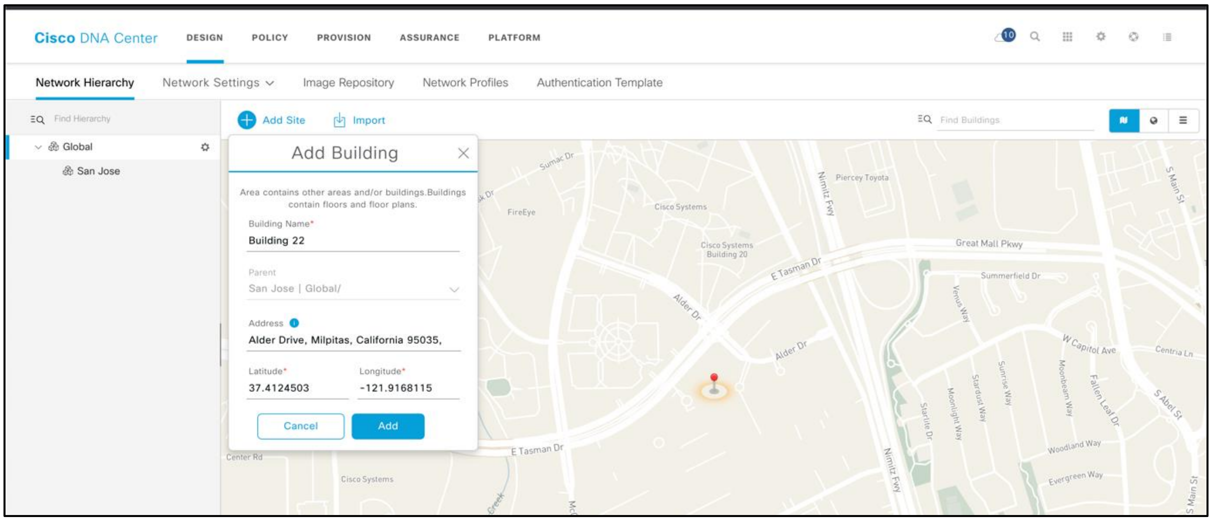


Add Area

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

Area Name* San Jose

Parent Global



Add Building

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

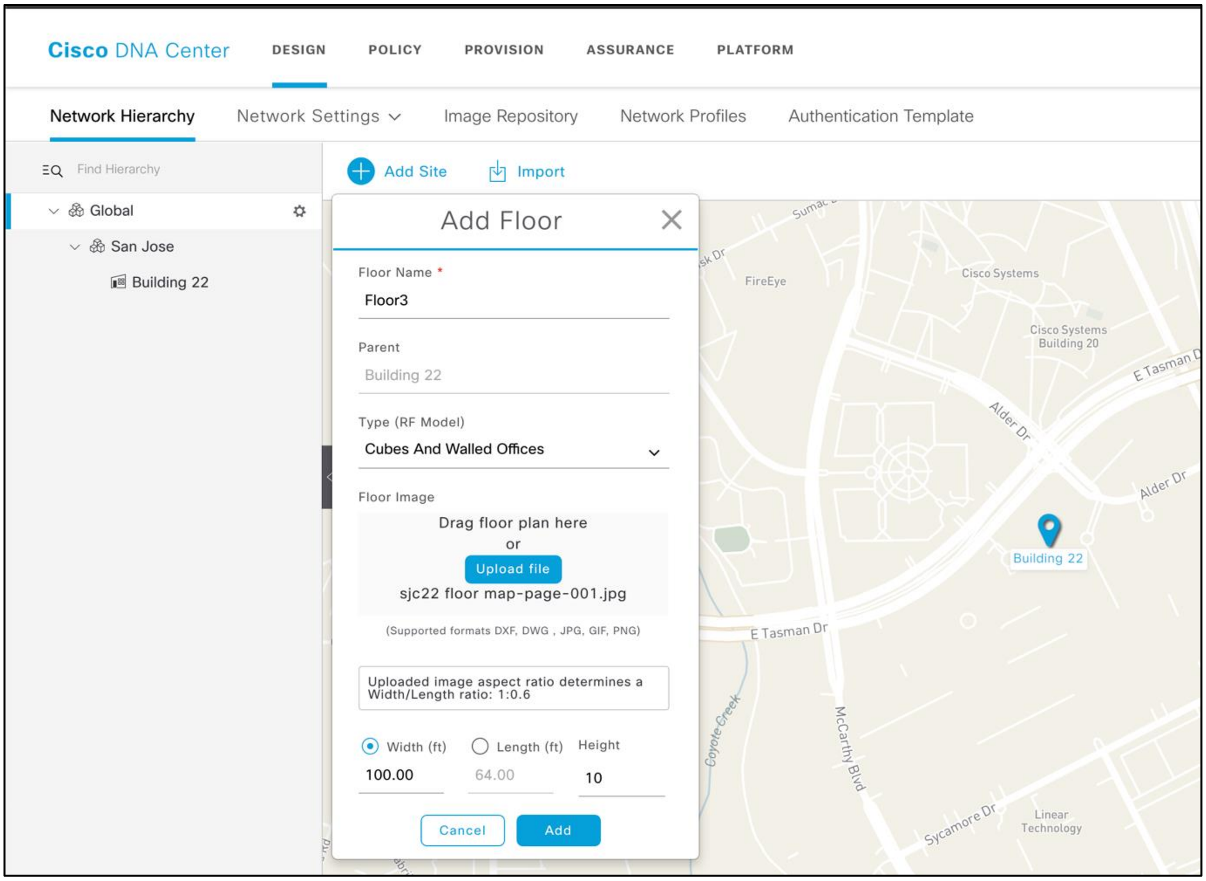
Building Name* Building 22

Parent San Jose | Global/

Address Alder Drive, Milpitas, California 95035,

Latitude* 37.4124503

Longitude* -121.9168115



Add Floor

Floor Name *
Floor3

Parent
Building 22

Type (RF Model)
Cubes And Walled Offices

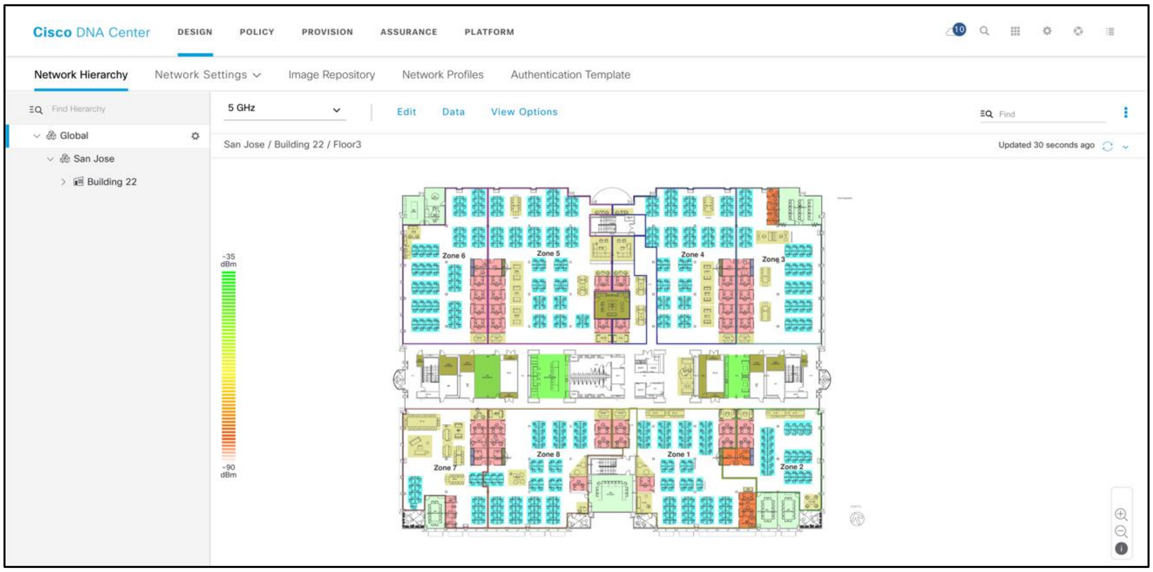
Floor Image
Drag floor plan here
or
Upload file
sjc22 floor map-page-001.jpg

(Supported formats DXF, DWG , JPG, GIF, PNG)

Uploaded image aspect ratio determines a Width/Length ratio: 1:0.6

● Width (ft) 100.00 ○ Length (ft) 64.00 Height 10

Cancel Add



San Jose / Building 22 / Floor3

Updated 30 seconds ago

e

Network settings

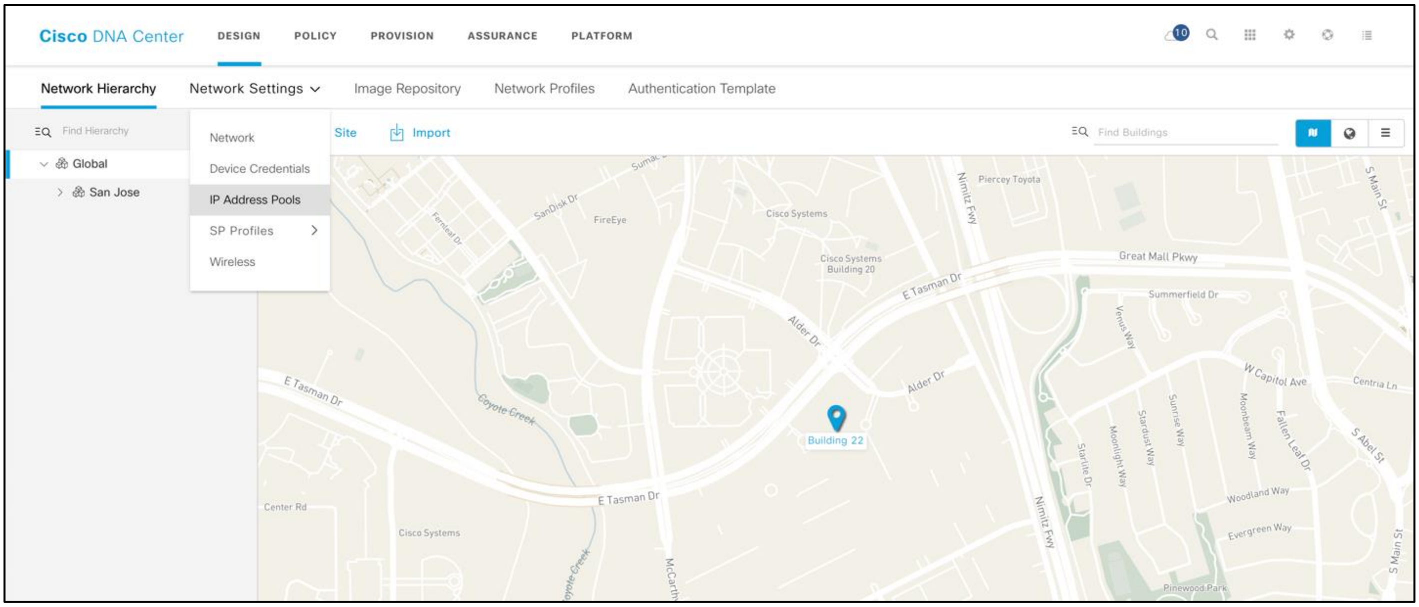
Cisco DNA Center allows you to save common resources and settings with Design's Network Settings application. This allows information pertaining to the enterprise to be stored so it can be reused throughout the Cisco DNA Center. DHCP, DNS servers, and device credentials should already be defined here.

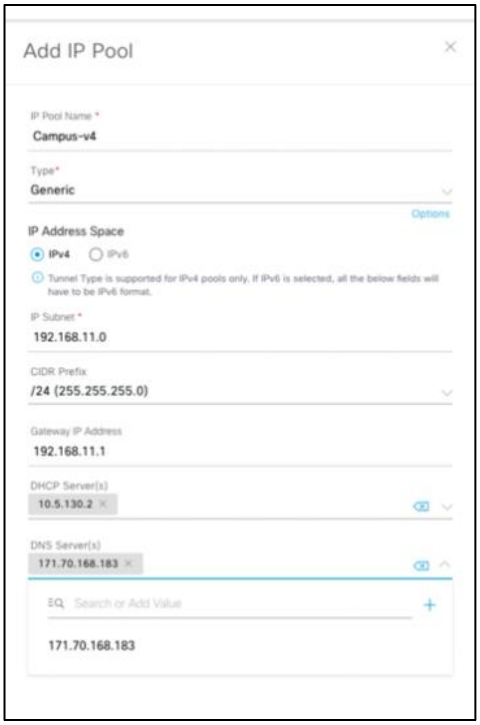
Creating IP pools

Please configure IP pools manually for both your APs and client subnets, as per the network addressing scheme on your DHCP server. Additionally, ensure that you have DHCP option 43 defined in your DHCP server for the AP IP pool to allow AP registration with the WLC. Cisco DNA Center does not provide automation for this step, as this guide doesn't leverage the IP address manager (Infoblox) integration.

Procedure:

Using the menu, navigate to Design > Network Settings, then select IP Address Pools. Click Add to open a dialog box for creating new IP pools.




Add IP Pool

IP Pool Name *
Campus-v4

Type*
Generic

Options

IP Address Space
● IPv4 ○ IPv6

Tunnel Type is supported for IPv4 pools only. If IPv6 is selected, all the below fields will have to be IPv6 format.

IP Subnet *
192.168.11.0

CIDR Prefix
/24 (255.255.255.0)

Gateway IP Address
192.168.11.1

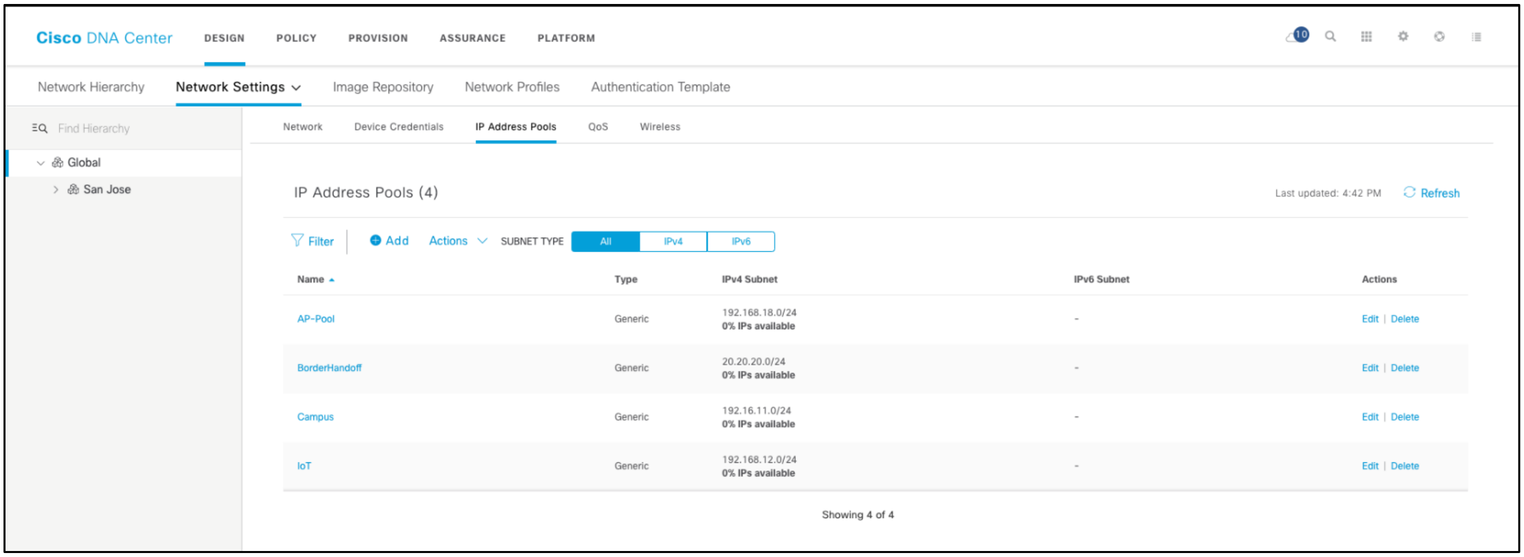
DHCP Server(s)
10.5.130.2

DNS Server(s)
171.70.168.183

Search or Add Value

171.70.168.183

When completed, the Cisco DNA Center IP Address Pools tab for clients and APs should look very similar to the following page.



IP Address Pools (4)

Last updated: 4:42 PM

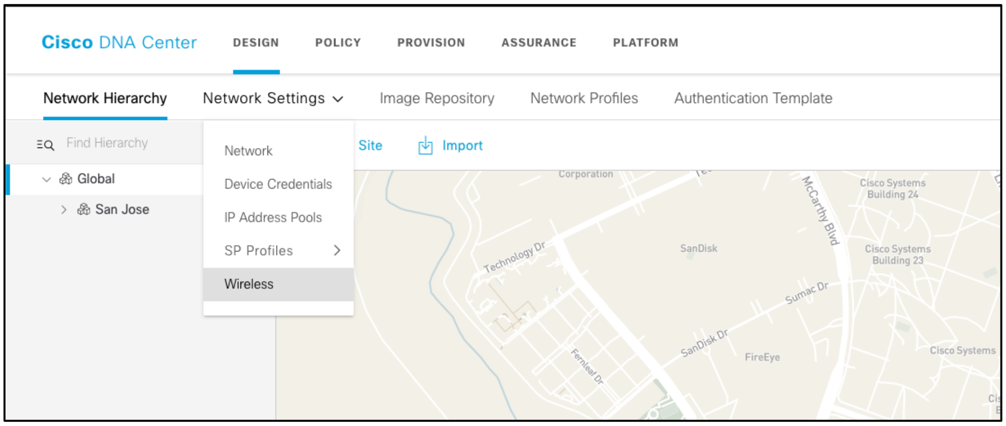
Name	Type	IPv4 Subnet	IPv6 Subnet	Actions
AP-Pool	Generic	192.168.18.0/24 0% IPs available	-	Edit | Delete
BorderHandoff	Generic	20.20.20.0/24 0% IPs available	-	Edit | Delete
Campus	Generic	192.16.11.0/24 0% IPs available	-	Edit | Delete
IoT	Generic	192.168.12.0/24 0% IPs available	-	Edit | Delete

Showing 4 of 4

Creating wireless SSIDs

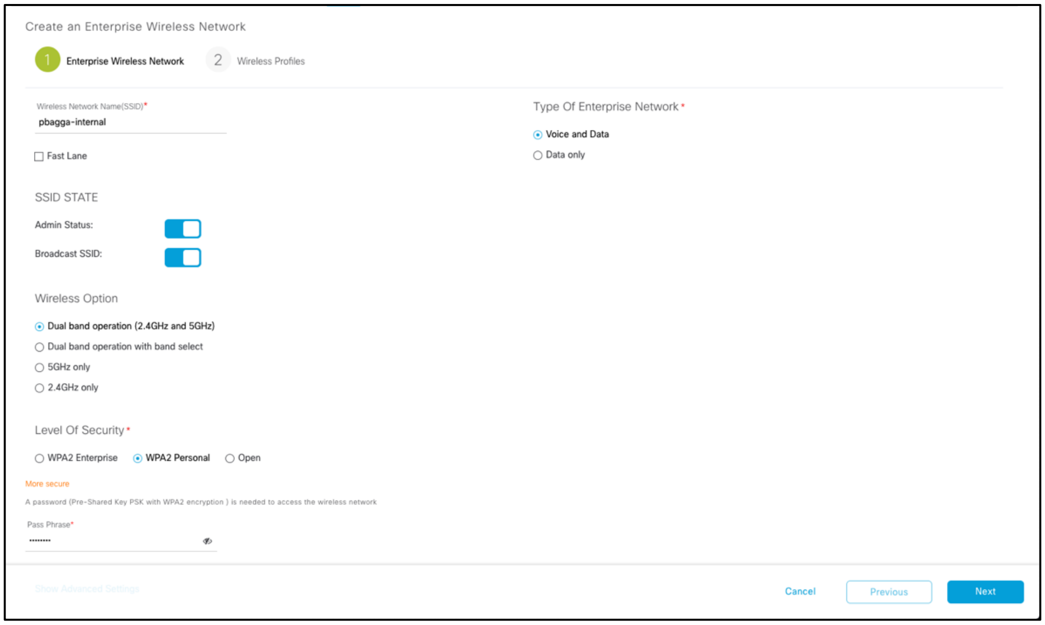
Procedure

Step 1 Under Network Settings, click the Wireless tab.



Creating an SSID is a two-step process. First, create a wireless network by choosing the type of network and assigning a security type; second, create or assign a wireless profile. If you create a new profile, add sites where you want this SSID to be broadcasted. See the steps below to follow the workflow.

Step 2 Click Add in the Enterprise Wireless SSID ("Internal03" in this example) and choose WPA2 Personal and a secure passphrase as the Level of Security. Fast Transition (802.11r) can be configured in the SSID creation phase.



Create an Enterprise Wireless Network

1 Enterprise Wireless Network   2 Wireless Profiles

Wireless Network Name(SSID)*: pbagga-internal

□ Fast Lane

Type Of Enterprise Network*

● Voice and Data
○ Data only

SSID STATE

Admin Status: On
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

More secure

A password (Pre-Shared Key PSK with WPA2 encryption) is needed to access the wireless network

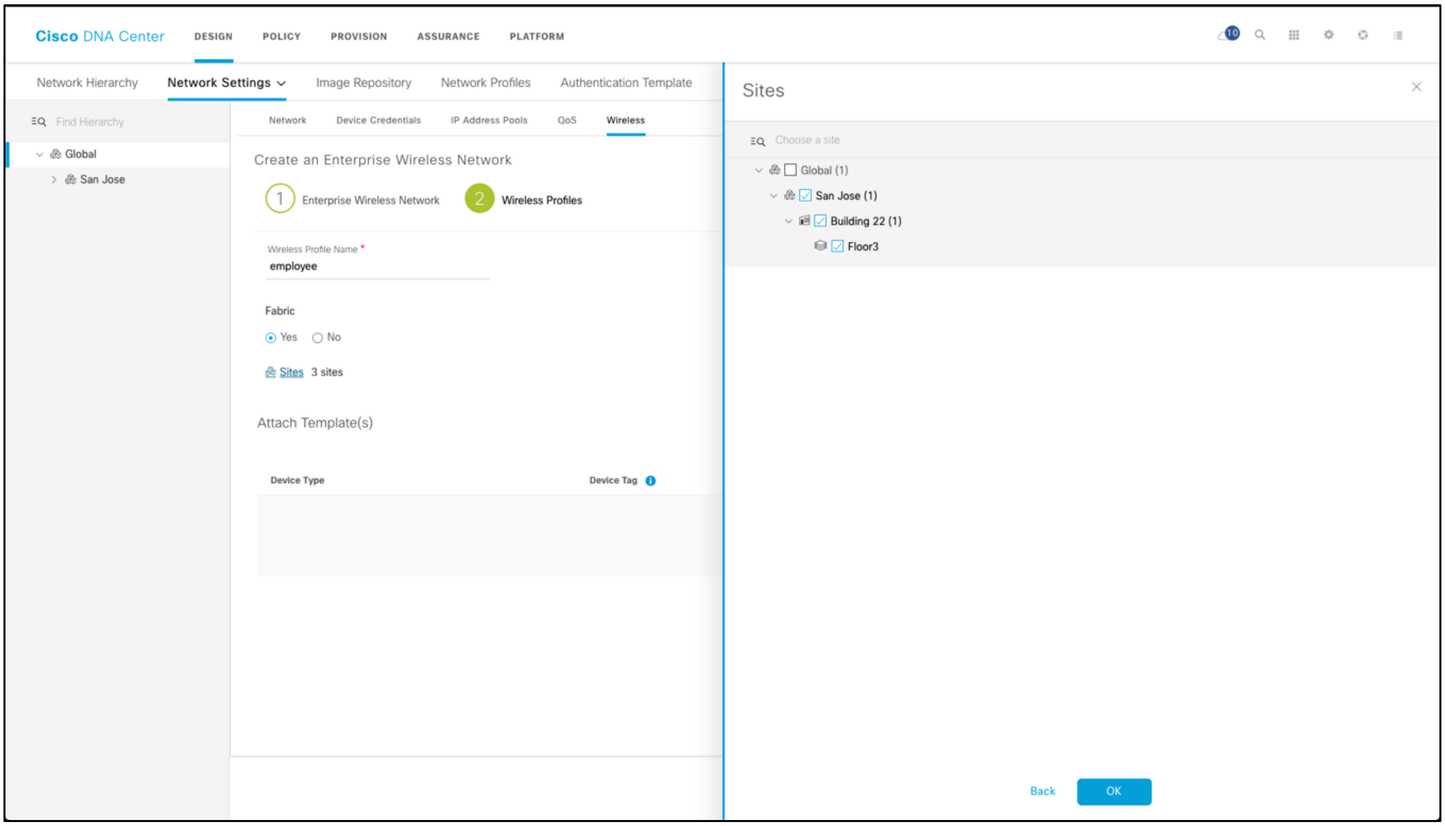
Pass Phrase*: ••••••••

Show Advanced Settings

In all the examples in this guide, names for SSIDs, profiles, pools, etc. are just for reference. You can specify your own names.

Step 3 Click Next. If not configured already, Cisco DNA Center will prompt you to create a Wireless Profile to associate with the SSID. Name of Wireless Profile in this case is "employee". If already present, you can select one of the existing profiles. The network profile defines the type of SSID, fabric or non-fabric, and the sites where it will be broadcasted. Click Finish to create the Wireless Profile.

Under Wireless Profile it can be determined if the Profile is for an SD-Access Fabric or not and add locations where the SSIDs in this profile will be broadcasted. In the example shown below, SSID pbagga-internal is mapped to site Sanjose, and the children sites (Floor-1) will inherit the settings. Just type the first letters of the site to see it appear.



Create an Enterprise Wireless Network

1 Enterprise Wireless Network   2 Wireless Profiles

Wireless Profile Name*: employee

Fabric

● Yes ○ No

Sites 3 sites

Attach Template(s)

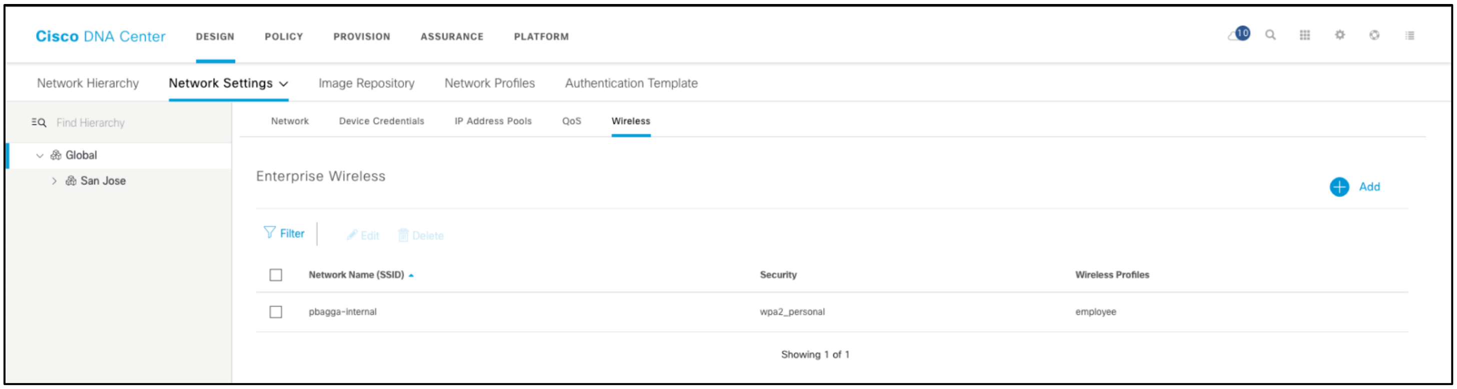
Device Type	Device Tag

Sites

Choose a site

- □ Global (1)
  - ☑ San Jose (1)
    - ☑ Building 22 (1)
      - ☑ Floor3

Step 4 Once the profile is configured, you can click Save and return to the main SSID page.

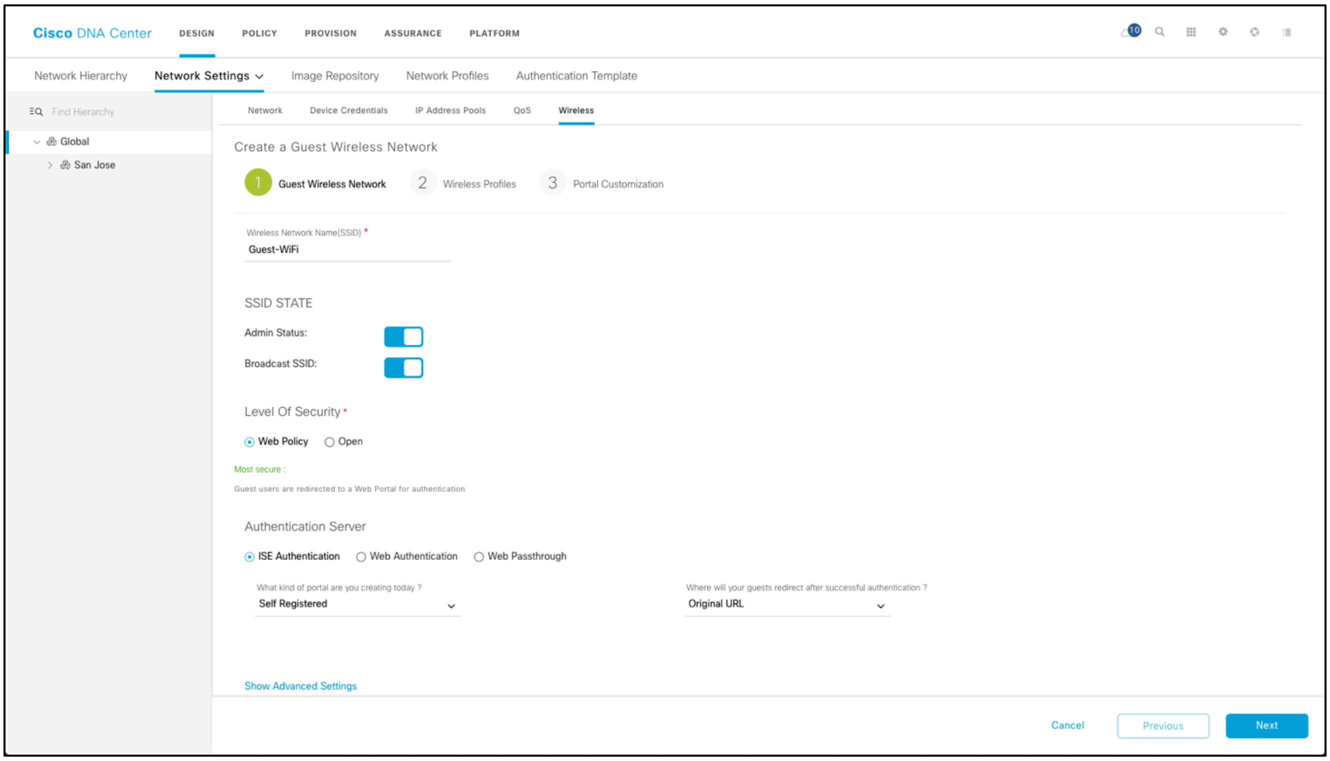


Enterprise Wireless

Network Name (SSID)	Security	Wireless Profiles
pbagga-internal	wpa2_personal	employee

Showing 1 of 1

Step 5 You can now create a guest SSID. Under Guest Wireless, click the Add icon to add a guest SSID.



Create a Guest Wireless Network

Wireless Network Name(SSID) *: Guest-WiFi

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

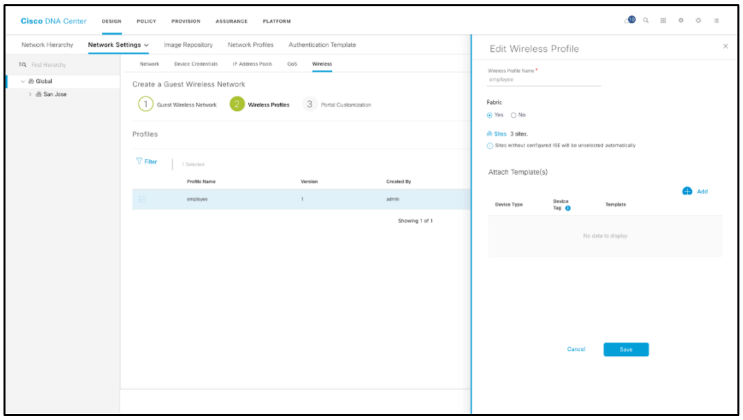
Authentication Server

● ISE Authentication ○ Web Authentication ○ Web Passthrough

What kind of portal are you creating today ?: Self Registered

Where will your guests redirect after successful authentication ?: Original URL

Step 6 Add the SSID to a network profile as you have done for the non–guest SSID.



Create a Guest Wireless Network

Profiles

Profile Name	Version	Created By
employee	1	admin

Showing 1 of 1

Edit Wireless Profile

Wireless Profile Name *: employee

Fabric: ● Yes ○ No

Sites 3 sites.

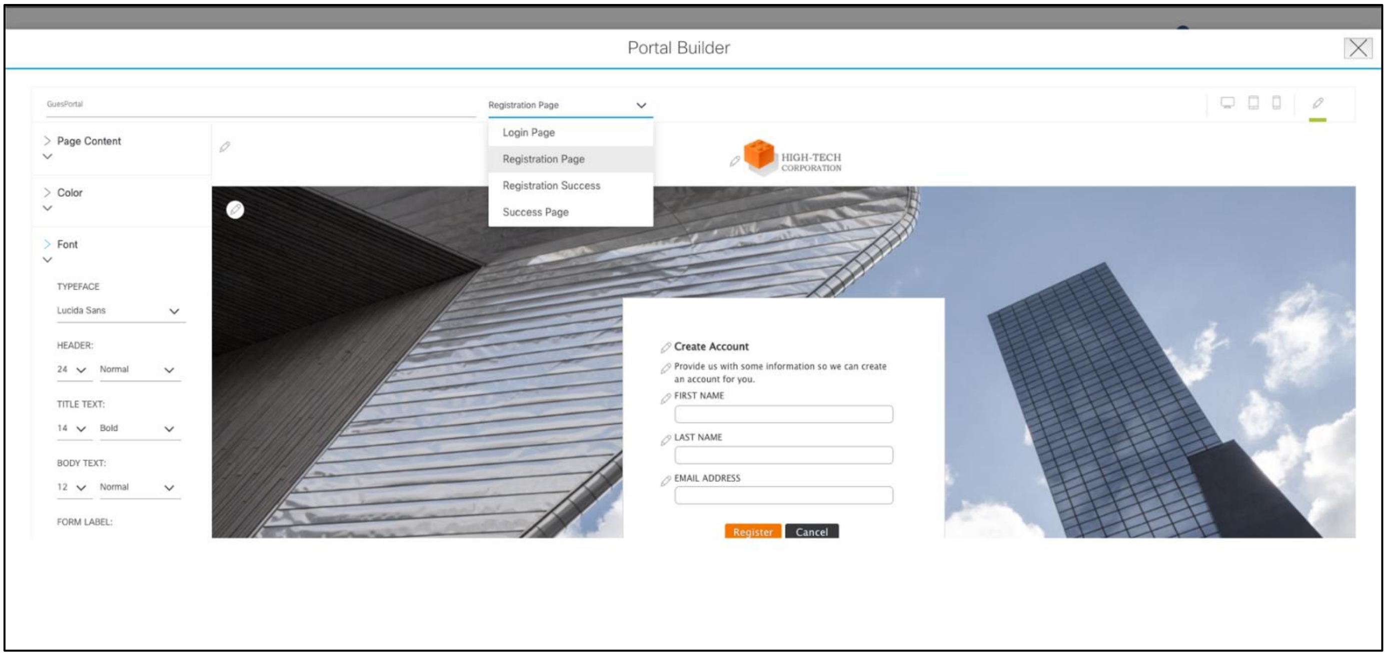
Sites without configured ISE will be unselected automatically

Attach Template(s)

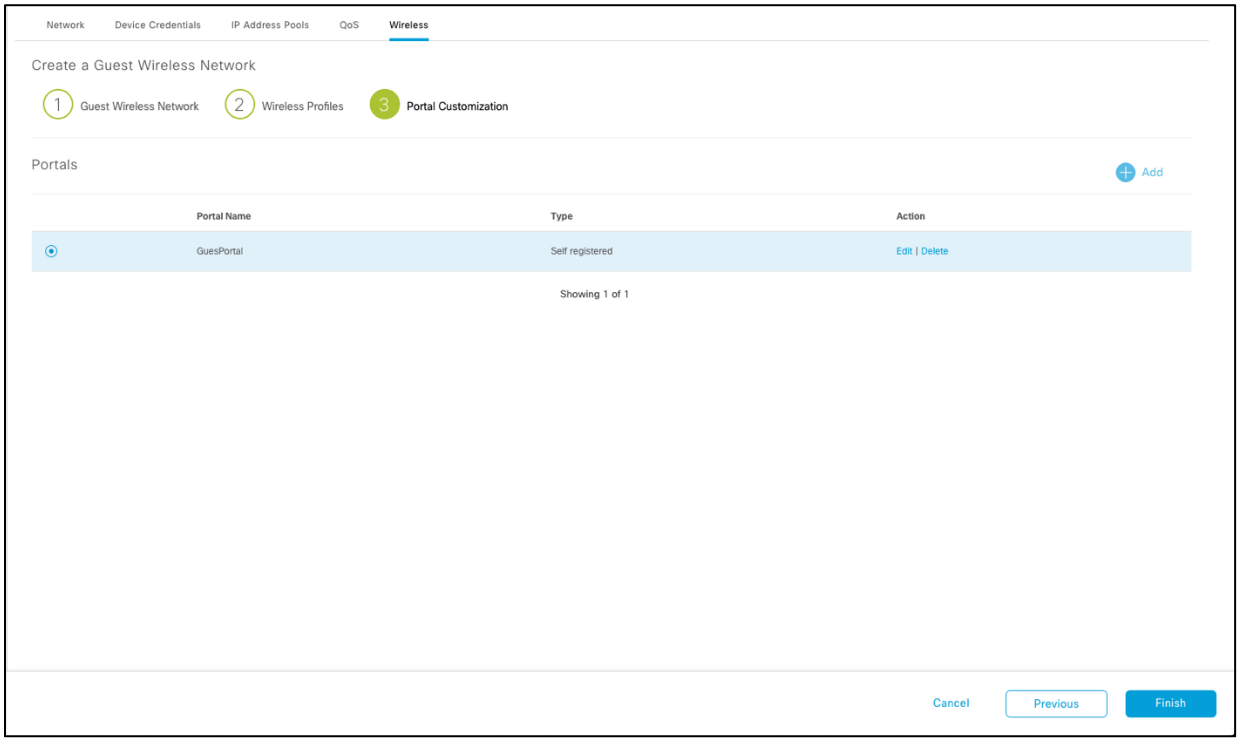
Device Type	Device Tag	Template

No data to display

Step 7 Cisco DNA Center offers back-end integration with ISE for portal and profile configuration. The screenshot below shows theavailable options for portal customization. Central Web Auth (CWA) with ISE is supported.

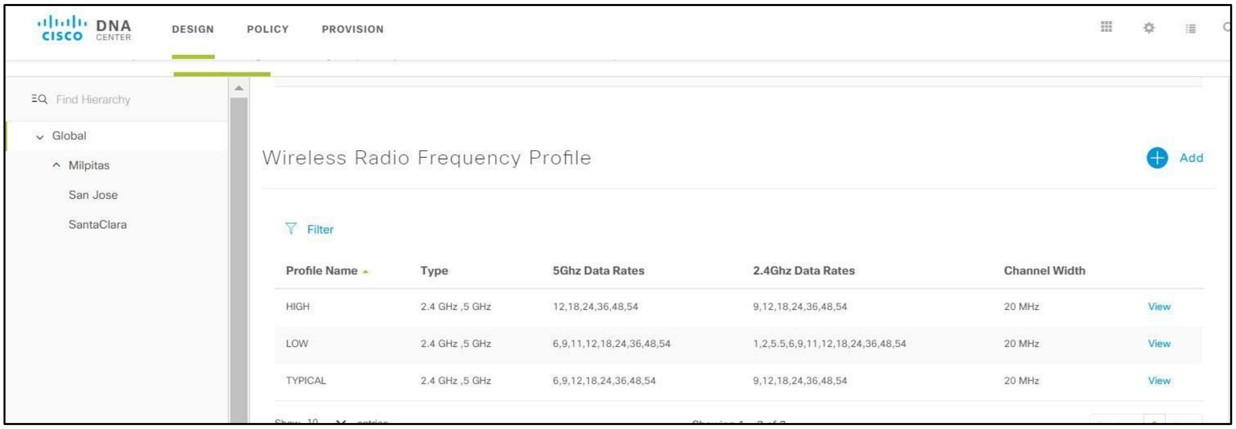


Step 8 Click Finish to complete the Guest SSID design phase



	Portal Name	Type	Action
●	GuesPortal	Self registered	Edit | Delete

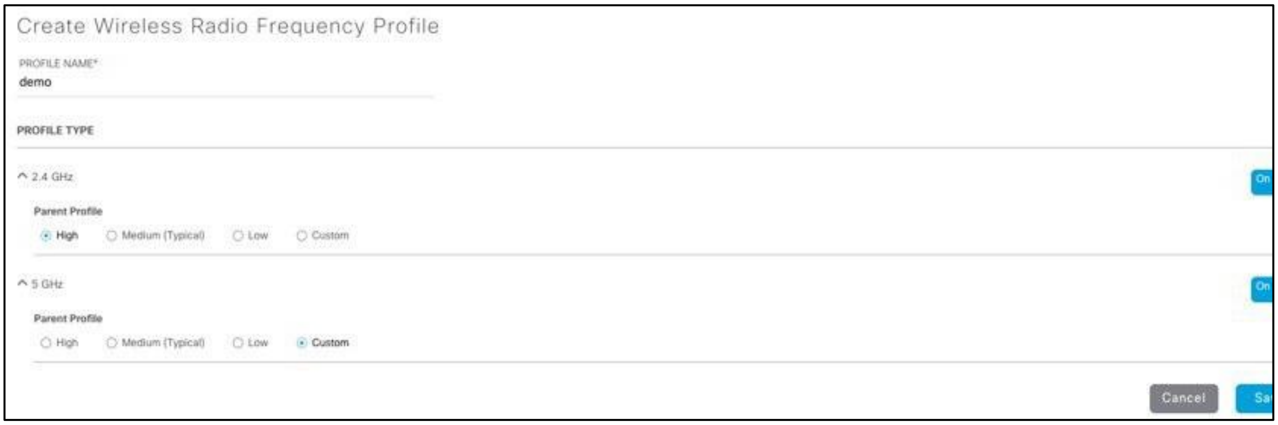
Step 9 Optionally, you can configure a customized RF profile. The profile in the design phase is then applied in the provisioning phase (described later in this guide). Scroll down the wireless page to view the available wireless radio frequency profiles.



Wireless Radio Frequency Profile

Profile Name	Type	5Ghz Data Rates	2.4Ghz Data Rates	Channel Width	
HIGH	2.4 GHz ,5 GHz	12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz	View
LOW	2.4 GHz ,5 GHz	6,9,11,12,18,24,36,48,54	1,2,5.5,6,9,11,12,18,24,36,48,54	20 MHz	View
TYPICAL	2.4 GHz ,5 GHz	6,9,12,18,24,36,48,54	9,12,18,24,36,48,54	20 MHz	View

To create a new profile, click Add. The following page is displayed.



Create Wireless Radio Frequency Profile

PROFILE NAME*: demo

PROFILE TYPE

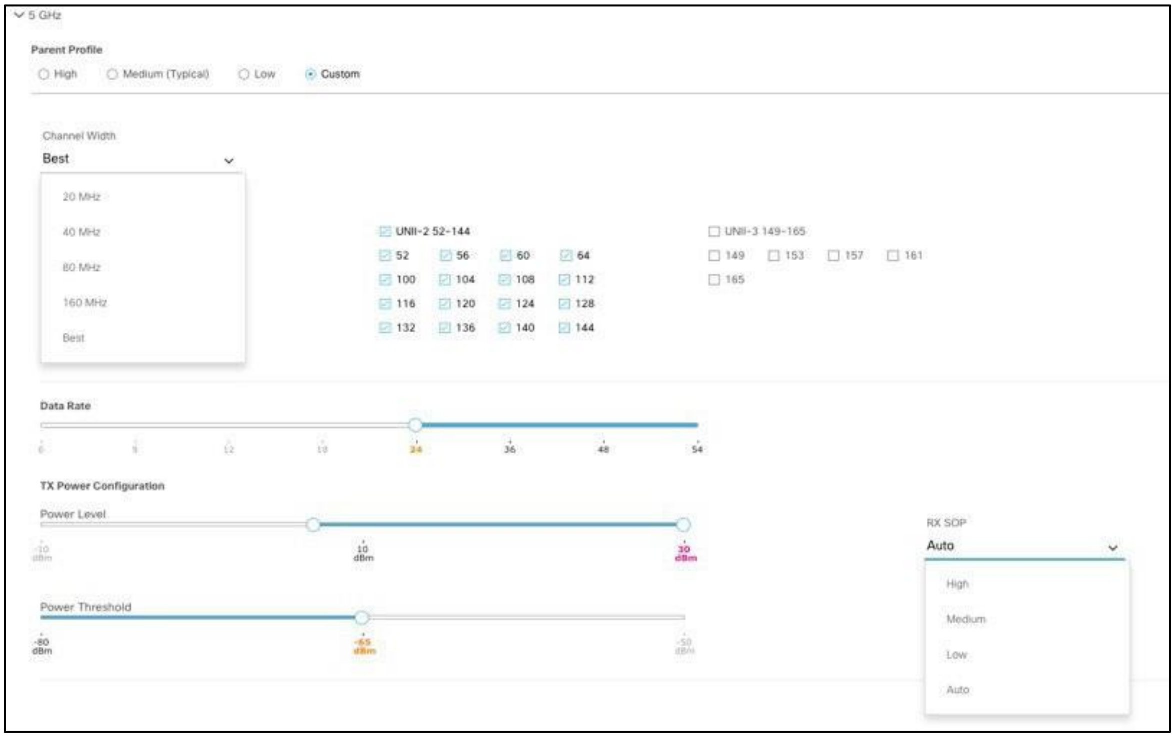
2.4 GHz — On

Parent Profile: ● High ○ Medium (Typical) ○ Low ○ Custom

5 GHz — On

Parent Profile: ○ High ○ Medium (Typical) ○ Low ● Custom

Choose customization parameters (dynamic bandwidth selection, DCA channel flexibility, and HD RF settings) for the parent profile on the 2.4- or 5-GHz band.



5 GHz

Parent Profile: ○ High ○ Medium (Typical) ○ Low ● Custom

Channel Width: Best

☑ UNII-2 52-144

☑ 52 ☑ 56 ☑ 60 ☑ 64
☑ 100 ☑ 104 ☑ 108 ☑ 112
☑ 116 ☑ 120 ☑ 124 ☑ 128
☑ 132 ☑ 136 ☑ 140 ☑ 144

□ UNII-3 149-165

□ 149 □ 153 □ 157 □ 161
□ 165

Data Rate: 24

TX Power Configuration

Power Level: 10 dBm – 30 dBm

Power Threshold: -65 dBm

RX SOP: Auto

AAA server per SSID

In this section, we will discuss the AAA server per SSID feature introduced as part of the Cisco DNAC-2.2.1.0 release. Prior to Cisco DNAC-2.2.1.0 release the AAA sever used by an SSID was defined in the design network settings. The number of the AAA server that can be defined in the network settings was limited to just two. There was no way to specify a unique set of AAA servers that can be mapped to an SSID, as the AAA servers defined under the design settings page were common to the wired and wireless infrastructure. The AAA server per SSID allows an administrator to map up to six AAA servers per SSID. An upgrade from a pre-Cisco DNAC 2.2.1.0 to 2.2.1.0 or above will have the AAA server auto-populated and migrated from the network settings to the per SSID AAA server settings.

The AAA server defined for an SSID can be a mix of an ISE PSN and regular AAA servers. The feature provides the flexibility to define a different group of AAA servers for an enterprise SSID and a different set of servers for the Guest SSID. It is a common practice to isolate AAA servers for trusted and untrusted users. Administrators can also override the AAA servers defined for an SSID at the floor/building or a location within the site hierarchy. When doing an override, the Cisco DNAC will provision multiple SSID with the same name but a different profile name based on the layer where the override was done. The feature is supported on the Aire-OS-based controllers and the Catalyst 9800 Wireless LAN Controllers. The support for this feature on the EWC-9k platforms is only supported from the Cisco DNAC-2.2.2.0 release onwards.

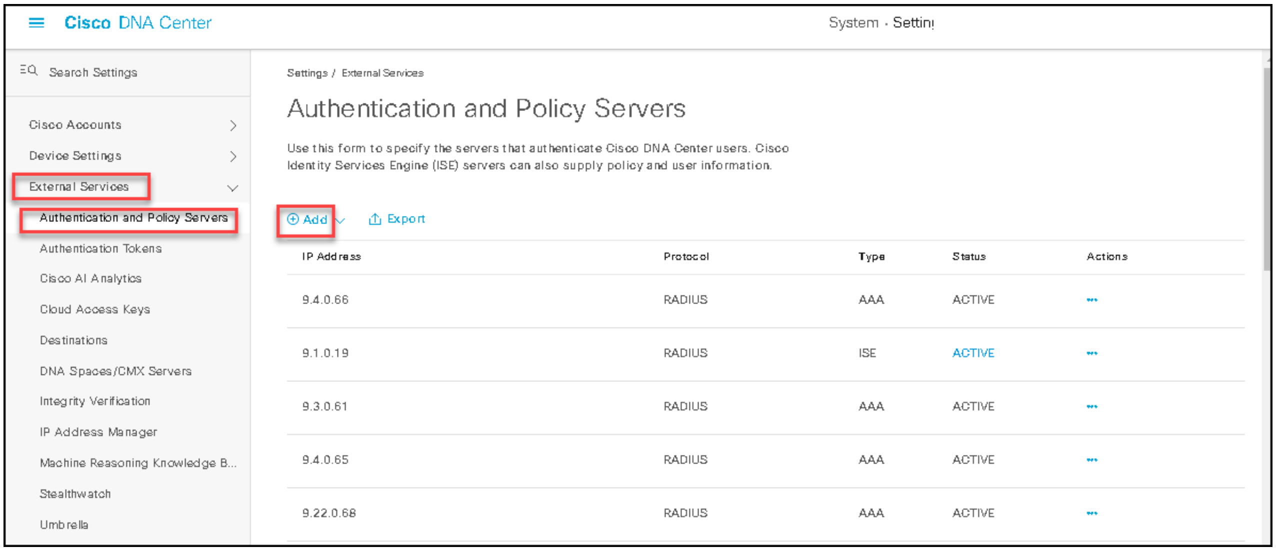
If using Aire-OS based controllers, the maximum number of global AAA servers that can be supported on the platform is limited to 32. The sum of all the different AAA servers configured under the SSID should be within the limit of 32. If the AAA servers exceed the value of 32, a provisioning failure would occur.

The AAA server per SSID workflow on an SSID would be activated only if the security configuration on the SSID requires authentication and authorization. Any changes made to the AAA server on an SSID would require the WLC to be re-provisioned for the new settings to take effect.

The following defines the steps to enable the AAA server per SSID feature.

Step1: Integrate/add the ISE PAN/AAA servers to the Cisco DNAC**.**

Navigate to **System->Settings->External services ->Athentication and policy servers.**

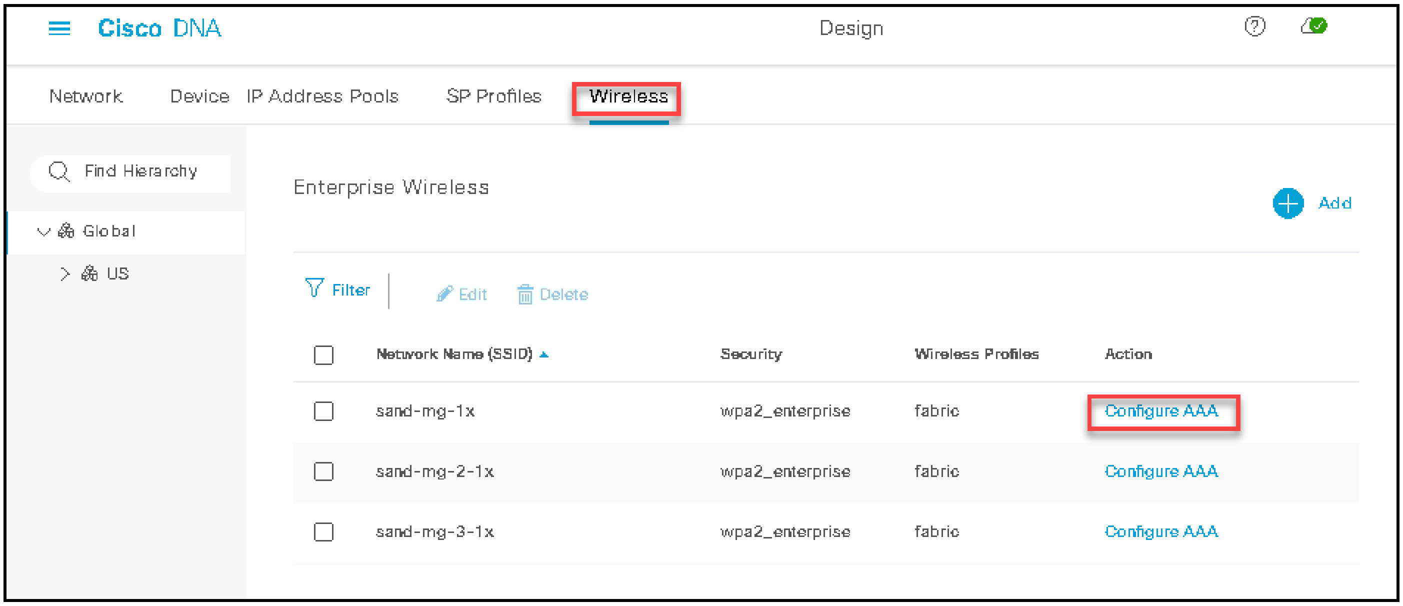


Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

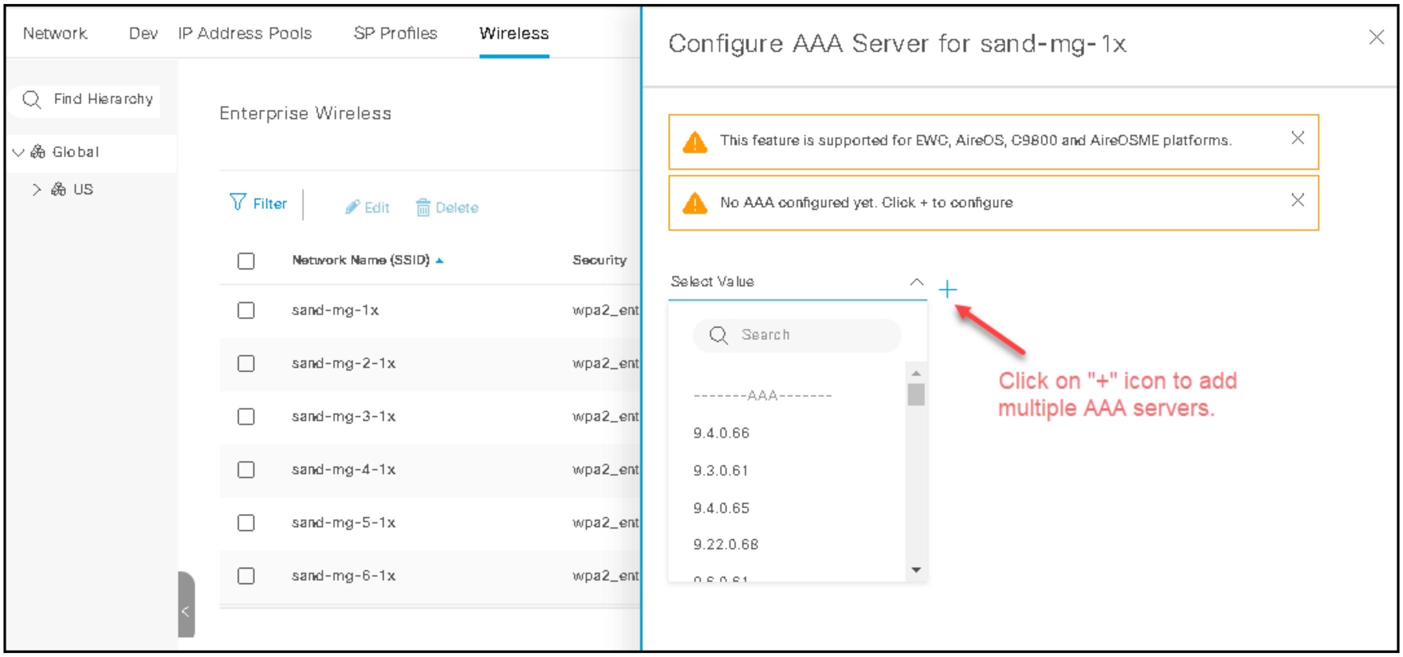
IP Address	Protocol	Type	Status	Actions
9.4.0.66	RADIUS	AAA	ACTIVE	•••
9.1.0.19	RADIUS	ISE	ACTIVE	•••
9.3.0.61	RADIUS	AAA	ACTIVE	•••
9.4.0.65	RADIUS	AAA	ACTIVE	•••
9.22.0.68	RADIUS	AAA	ACTIVE	•••

Step2: The next step is to create an SSID, and map the AAA servers on the SSID. The AAA server mapping can be done while creating the SSID. Any modification to the AAA server can be done post SSID creation by navigating to the **Design->Network Settings.**



Enterprise Wireless

□	Network Name (SSID) ▲	Security	Wireless Profiles	Action
□	sand-mg-1x	wpa2_enterprise	fabric	Configure AAA
□	sand-mg-2-1x	wpa2_enterprise	fabric	Configure AAA
□	sand-mg-3-1x	wpa2_enterprise	fabric	Configure AAA



Enterprise Wireless

□	Network Name (SSID) ▲	Security
□	sand-mg-1x	wpa2_ent
□	sand-mg-2-1x	wpa2_ent
□	sand-mg-3-1x	wpa2_ent
□	sand-mg-4-1x	wpa2_ent
□	sand-mg-5-1x	wpa2_ent
□	sand-mg-6-1x	wpa2_ent

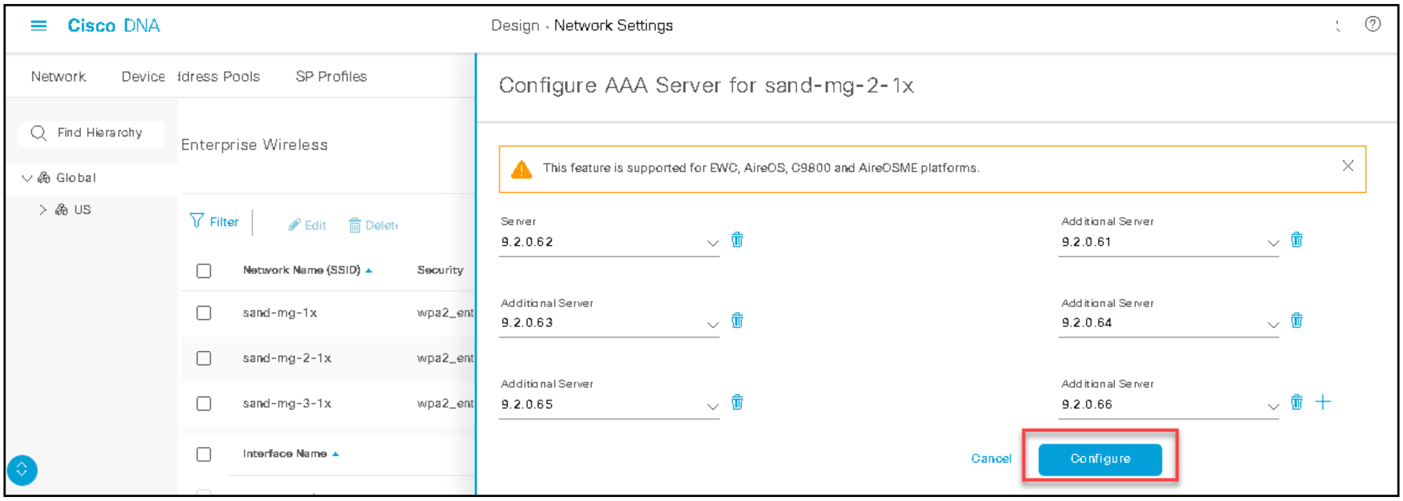
Configure AAA Server for sand-mg-1x

This feature is supported for EWC, AireOS, C9800 and AireOSME platforms.

No AAA configured yet. Click + to configure

-------AAA-------
9.4.0.66
9.3.0.61
9.4.0.65
9.22.0.68

Click on "+" icon to add multiple AAA servers.



Enterprise Wireless

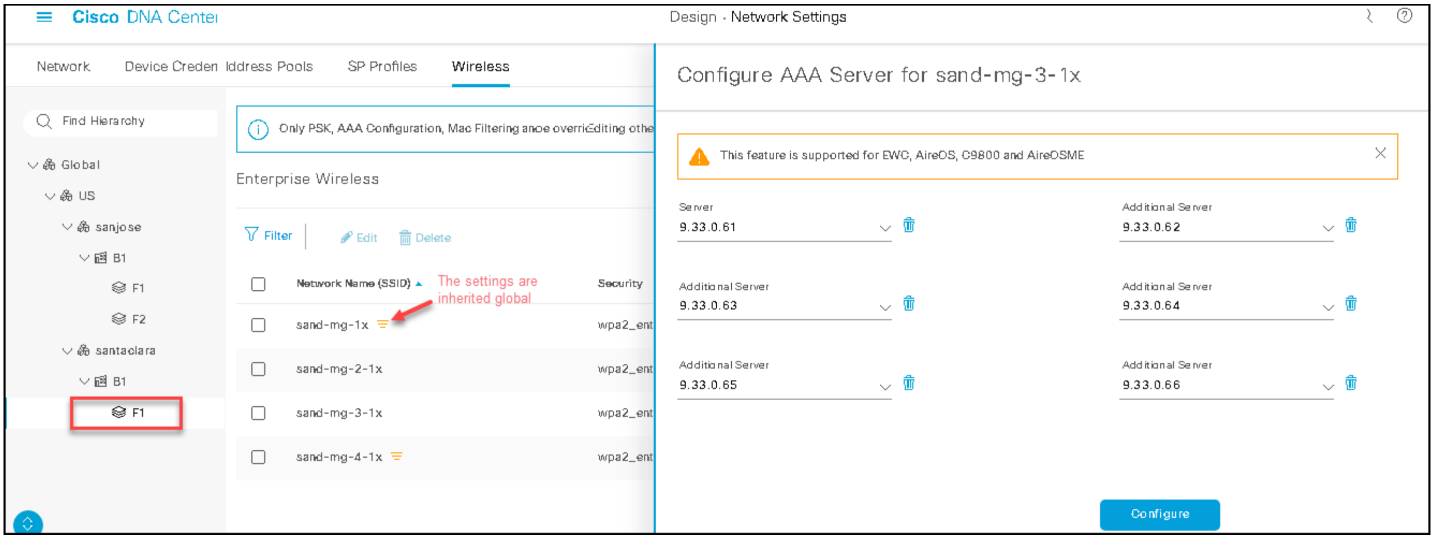
□	Network Name (SSID) ▲	Security
□	sand-mg-1x	wpa2_ent
□	sand-mg-2-1x	wpa2_ent
□	sand-mg-3-1x	wpa2_ent
□	Interface Name ▲	

Configure AAA Server for sand-mg-2-1x

This feature is supported for EWC, AireOS, C9800 and AireOSME platforms.

Server: 9.2.0.62
Additional Server: 9.2.0.61
Additional Server: 9.2.0.63
Additional Server: 9.2.0.64
Additional Server: 9.2.0.65
Additional Server: 9.2.0.66

Step4: This is an optional step. To override the AAA server per site. Navigate to the respective site and modify the AAA server. The icon ≡ shows the SSID inherits the settings such as a AAA server from the global configuration and the absence of it signifies the configuration is overridden at the site level.



Only PSK, AAA Configuration, Mac Filtering ance overriEditing othe

Enterprise Wireless

☐	Network Name (SSID) ▲	Security
☐	sand-mg-1x ≡	wpa2_ent
☐	sand-mg-2-1x	wpa2_ent
☐	sand-mg-3-1x	wpa2_ent
☐	sand-mg-4-1x ≡	wpa2_ent

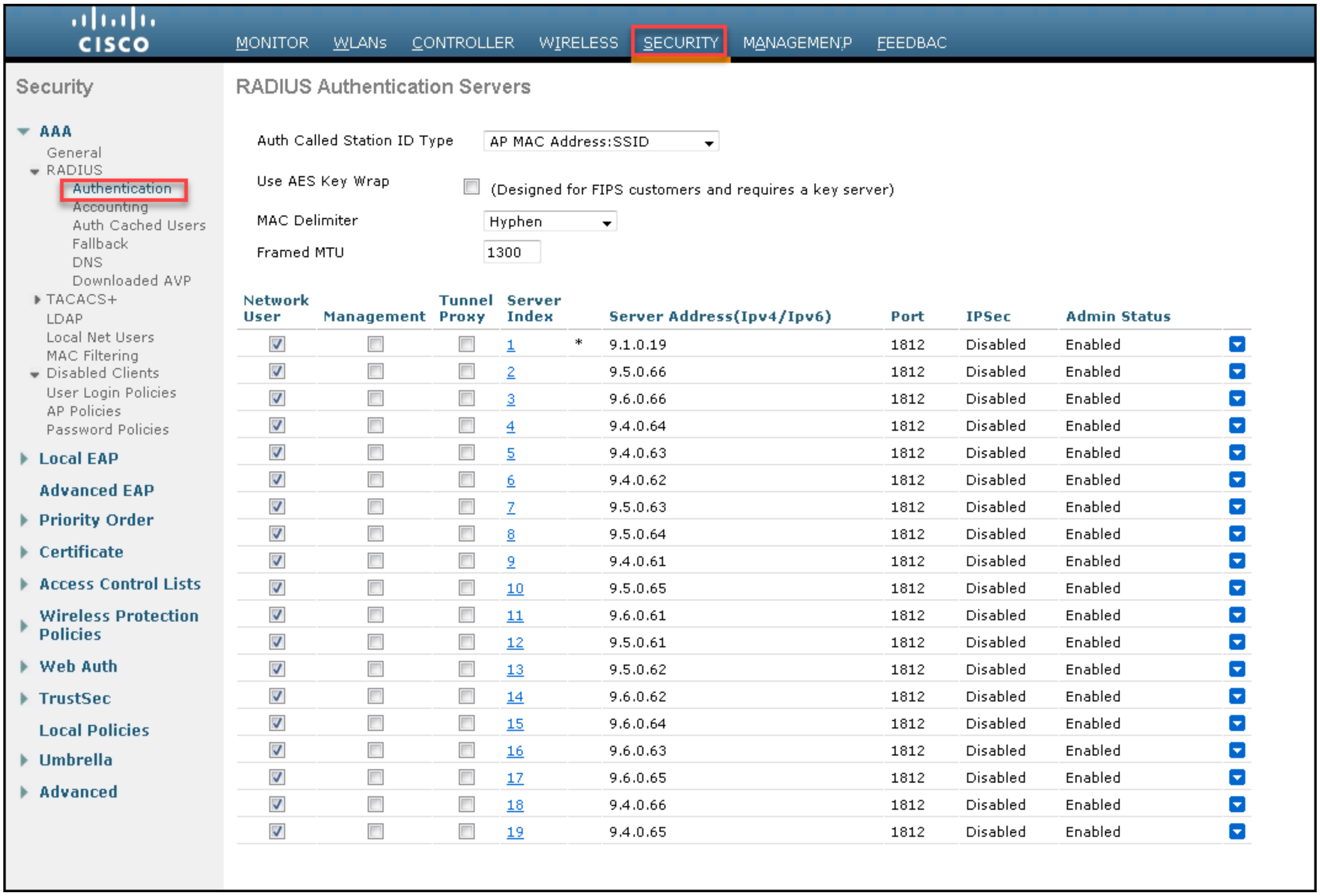
Configure AAA Server for sand-mg-3-1x

This feature is supported for EWC, AireOS, C9800 and AireOSME

Server: 9.33.0.61
Additional Server: 9.33.0.62
Additional Server: 9.33.0.63
Additional Server: 9.33.0.64
Additional Server: 9.33.0.65
Additional Server: 9.33.0.66

Step4: Provision the WLC to have the SSID and AAA server configs to be pushed on the WLC. To provision, the WLC navigate to **Provision->Inventory**. Select the WLC and on the action tab select provision.

Once the WLC is provisioned successfully. For an Aire-OS based controller, the AAA servers are configured globally and mapped to the SSID. For the Catalyst 9800 based Controllers, the Cisco DNAC uses the following sequence to map the AAA server per SSID. AAA Servers are created first and the servers get mapped to a server group. The server groups now get mapped into a method list and the method list is mapped to the SSID. For Accounting, the method list is mapped to the respective policy profile used by the SSID.



RADIUS Authentication Servers

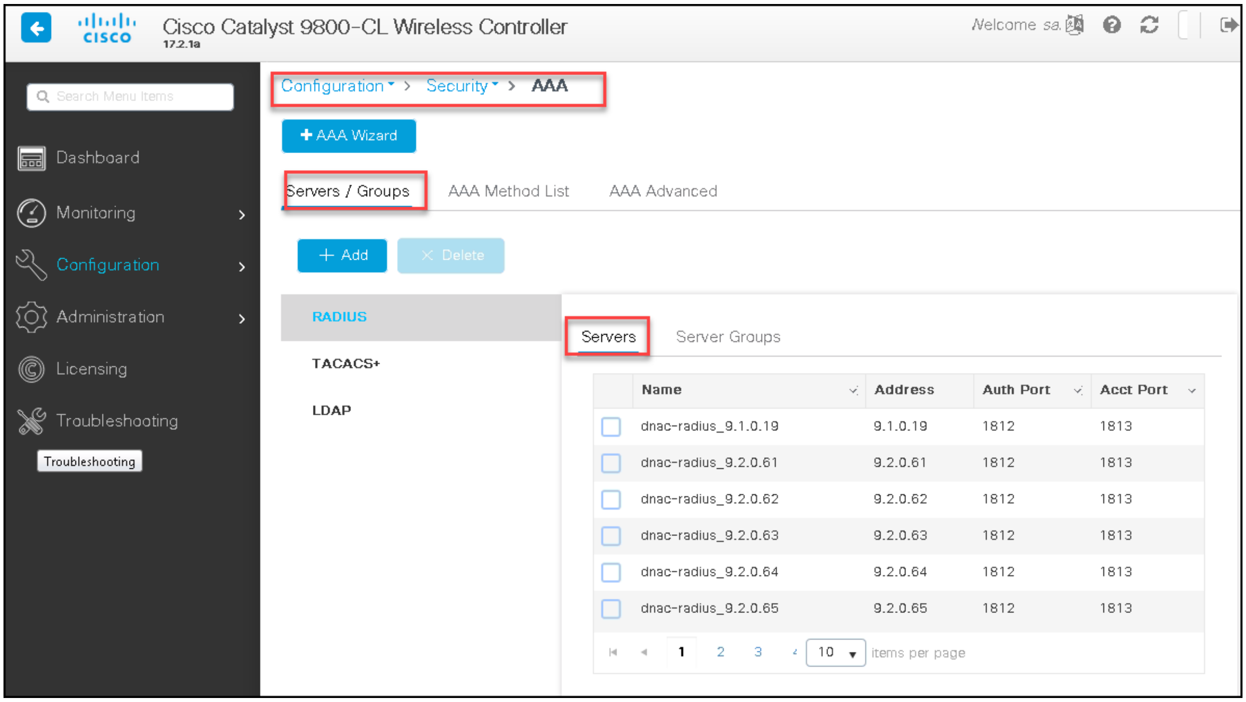
Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap □ (Designed for FIPS customers and requires a key server)

MAC Delimiter: Hyphen

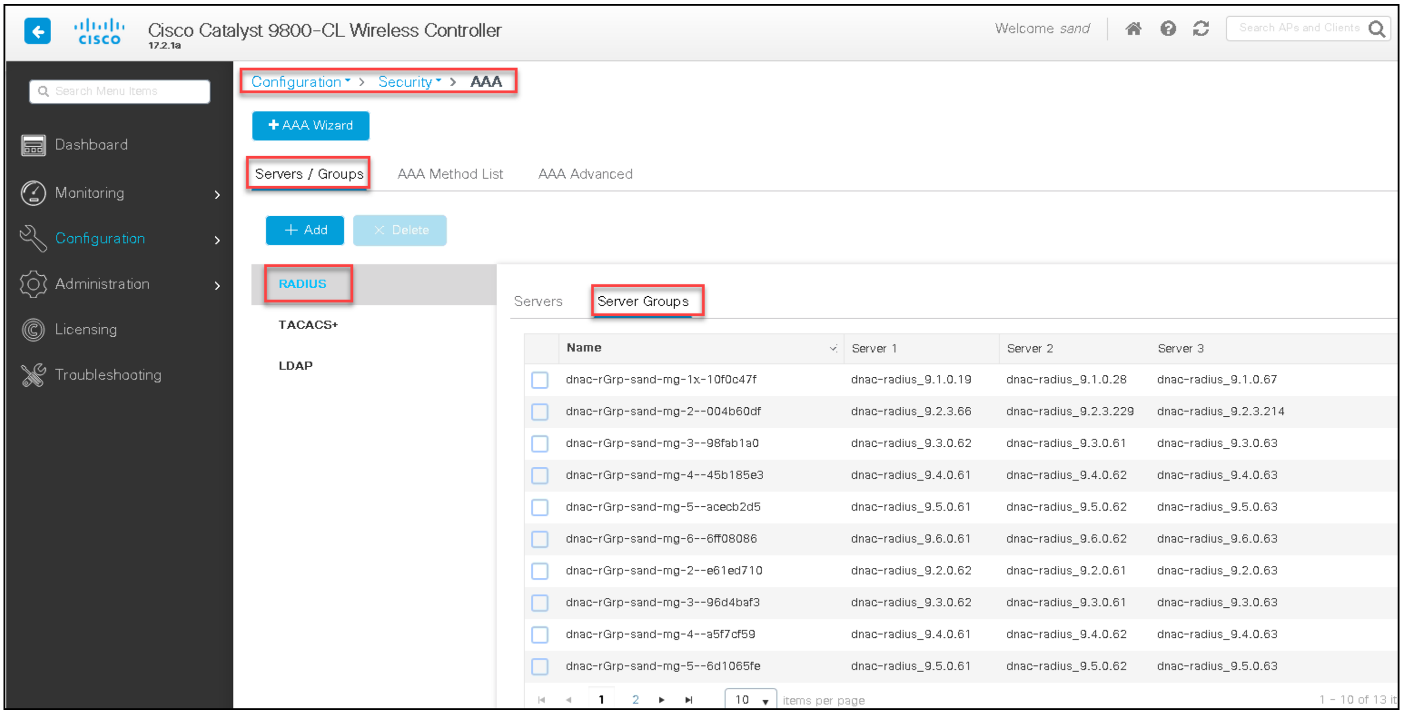
Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index		Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	□	□	1	*	9.1.0.19	1812	Disabled	Enabled
☑	□	□	2		9.5.0.66	1812	Disabled	Enabled
☑	□	□	3		9.6.0.66	1812	Disabled	Enabled
☑	□	□	4		9.4.0.64	1812	Disabled	Enabled
☑	□	□	5		9.4.0.63	1812	Disabled	Enabled
☑	□	□	6		9.4.0.62	1812	Disabled	Enabled
☑	□	□	7		9.5.0.63	1812	Disabled	Enabled
☑	□	□	8		9.5.0.64	1812	Disabled	Enabled
☑	□	□	9		9.4.0.61	1812	Disabled	Enabled
☑	□	□	10		9.5.0.65	1812	Disabled	Enabled
☑	□	□	11		9.6.0.61	1812	Disabled	Enabled
☑	□	□	12		9.5.0.61	1812	Disabled	Enabled
☑	□	□	13		9.5.0.62	1812	Disabled	Enabled
☑	□	□	14		9.6.0.62	1812	Disabled	Enabled
☑	□	□	15		9.6.0.64	1812	Disabled	Enabled
☑	□	□	16		9.6.0.63	1812	Disabled	Enabled
☑	□	□	17		9.6.0.65	1812	Disabled	Enabled
☑	□	□	18		9.4.0.66	1812	Disabled	Enabled
☑	□	□	19		9.4.0.65	1812	Disabled	Enabled



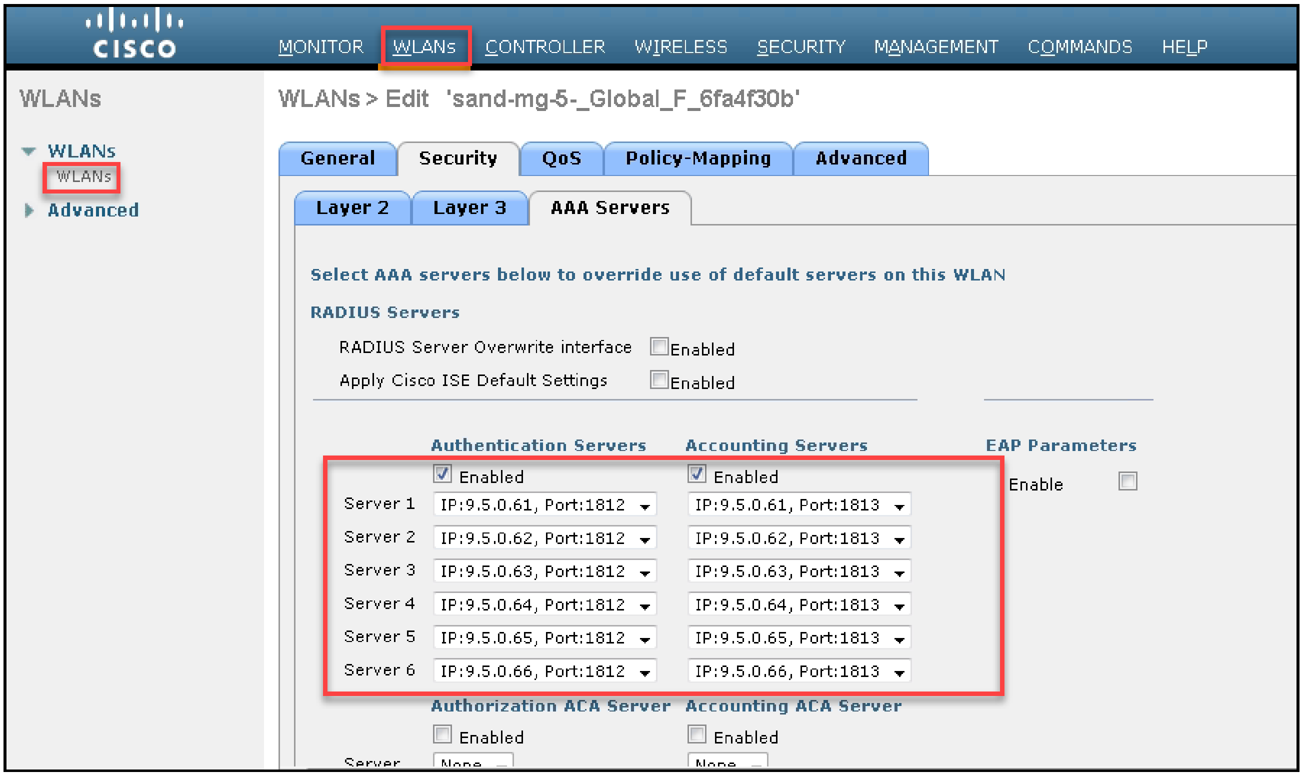
	Name	Address	Auth Port	Acct Port
□	dnac-radius_9.1.0.19	9.1.0.19	1812	1813
□	dnac-radius_9.2.0.61	9.2.0.61	1812	1813
□	dnac-radius_9.2.0.62	9.2.0.62	1812	1813
□	dnac-radius_9.2.0.63	9.2.0.63	1812	1813
□	dnac-radius_9.2.0.64	9.2.0.64	1812	1813
□	dnac-radius_9.2.0.65	9.2.0.65	1812	1813

1 2 3 | 10 items per page



	Name	Server 1	Server 2	Server 3
□	dnac-rGrp-sand-mg-1x-10f0c47f	dnac-radius_9.1.0.19	dnac-radius_9.1.0.28	dnac-radius_9.1.0.67
□	dnac-rGrp-sand-mg-2--004b60df	dnac-radius_9.2.3.66	dnac-radius_9.2.3.229	dnac-radius_9.2.3.214
□	dnac-rGrp-sand-mg-3--98fab1a0	dnac-radius_9.3.0.62	dnac-radius_9.3.0.61	dnac-radius_9.3.0.63
□	dnac-rGrp-sand-mg-4--45b185e3	dnac-radius_9.4.0.61	dnac-radius_9.4.0.62	dnac-radius_9.4.0.63
□	dnac-rGrp-sand-mg-5--acecb2d5	dnac-radius_9.5.0.61	dnac-radius_9.5.0.62	dnac-radius_9.5.0.63
□	dnac-rGrp-sand-mg-6--6ff08086	dnac-radius_9.6.0.61	dnac-radius_9.6.0.62	dnac-radius_9.6.0.63
□	dnac-rGrp-sand-mg-2--e61ed710	dnac-radius_9.2.0.62	dnac-radius_9.2.0.61	dnac-radius_9.2.0.63
□	dnac-rGrp-sand-mg-3--96d4baf3	dnac-radius_9.3.0.62	dnac-radius_9.3.0.61	dnac-radius_9.3.0.63
□	dnac-rGrp-sand-mg-4--a5f7cf59	dnac-radius_9.4.0.61	dnac-radius_9.4.0.62	dnac-radius_9.4.0.63
□	dnac-rGrp-sand-mg-5--6d1065fe	dnac-radius_9.5.0.61	dnac-radius_9.5.0.62	dnac-radius_9.5.0.63

1 2 ▸ ▸| 10 items per page 1 – 10 of 13 it



WLANs > Edit 'sand-mg-5-_Global_F_6fa4f30b'

Select AAA servers below to override use of default servers on this WLAN

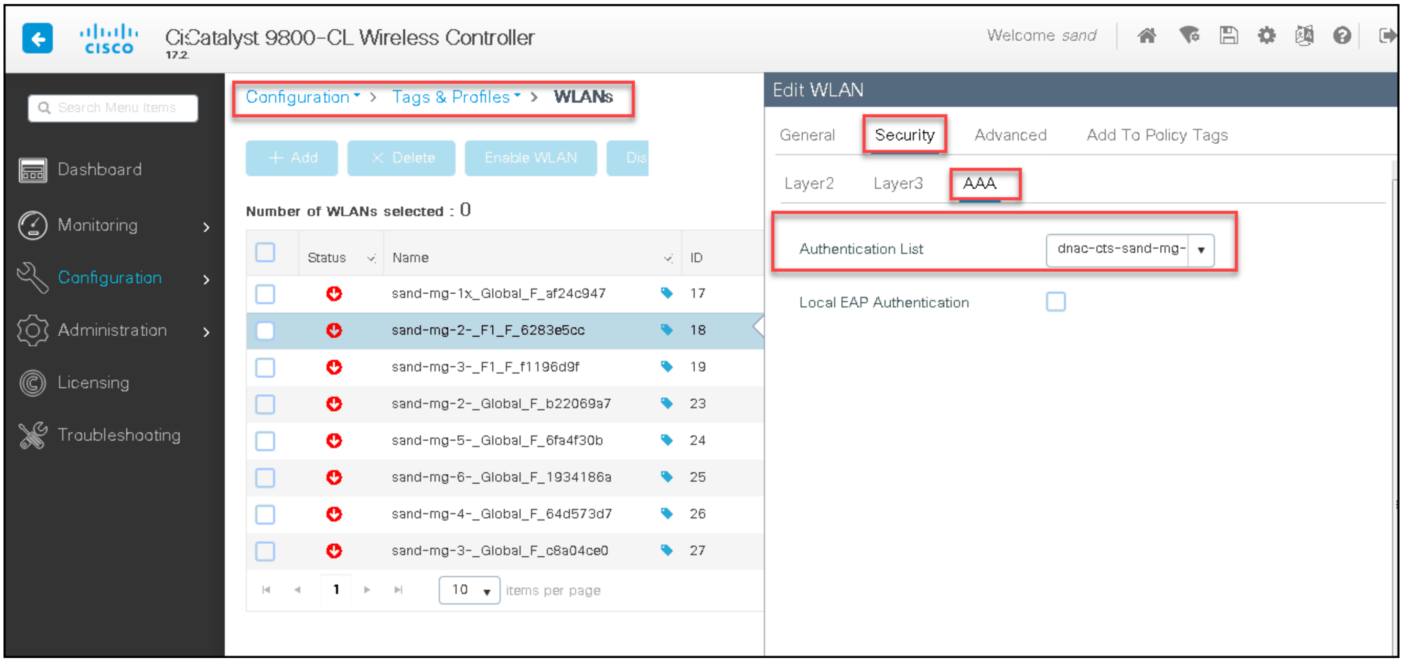
RADIUS Servers

RADIUS Server Overwrite interface □ Enabled

Apply Cisco ISE Default Settings □ Enabled

	Authentication Servers	Accounting Servers	EAP Parameters	
	☑ Enabled	☑ Enabled	Enable	□
Server 1	IP:9.5.0.61, Port:1812	IP:9.5.0.61, Port:1813		
Server 2	IP:9.5.0.62, Port:1812	IP:9.5.0.62, Port:1813		
Server 3	IP:9.5.0.63, Port:1812	IP:9.5.0.63, Port:1813		
Server 4	IP:9.5.0.64, Port:1812	IP:9.5.0.64, Port:1813		
Server 5	IP:9.5.0.65, Port:1812	IP:9.5.0.65, Port:1813		
Server 6	IP:9.5.0.66, Port:1812	IP:9.5.0.66, Port:1813		

	Authorization ACA Server	Accounting ACA Server
	□ Enabled	□ Enabled
Server	None	None



Number of WLANs selected : 0

Status	Name	ID
●	sand-mg-1x_Global_F_af24c947	17
●	sand-mg-2-_F1_F_6283e5cc	18
●	sand-mg-3-_F1_F_f1196d9f	19
●	sand-mg-2-_Global_F_b22069a7	23
●	sand-mg-5-_Global_F_6fa4f30b	24
●	sand-mg-6-_Global_F_1934186a	25
●	sand-mg-4-_Global_F_64d573d7	26
●	sand-mg-3-_Global_F_c8a04ce0	27

1 · 10 items per page

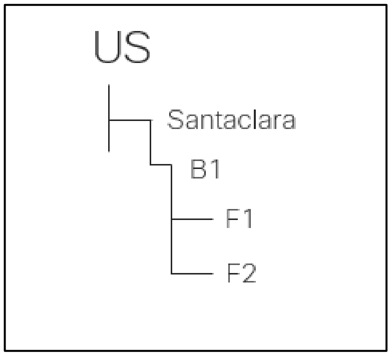
Authentication List: dnac-cts-sand-mg-

Local EAP Authentication □

AAA Sever Override

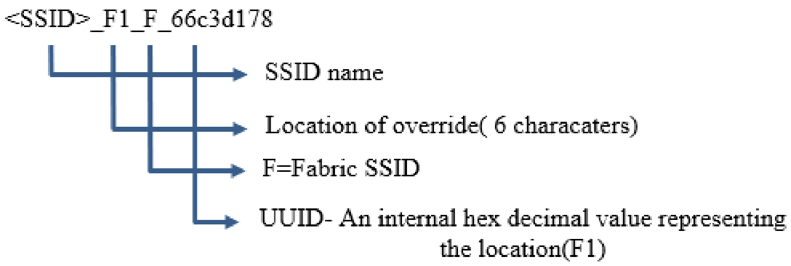
As outlined in step4 the AAA server per SSID feature, the AAA servers are inherited from the global settings. The administrator has an option to override the AAA server on a per-site/location/building or a per-floor basis. In the case where an override for the AAA server is done, the Cisco DNAC provisions multiple SSID with the same name but a different profile name. Each of these SSID would have a unique set of AAA servers based on the override.

Let us take an example to understand the provisioning logic on the Cisco DNAC when an override is done on a per floor basis. The logic is similar even if the override is done on a per-site/location or per building.



In this case, we have a fabric site at the site hierarchy level "Santa Clara" and are overriding the AAA server on floor-1 and floor-2 under the building "B1. The Cisco DNAC will now provision the two SSID with the same name but mapped to two different profile names. The way to differentiate between the SSID would be based on a unique identified WLAN profile name. Cisco DNAC will also provision the respective policy profile and create a policy tag and have that attached to the AP when an AP is assigned for that respective location.

The WLAN profile created by the Cisco DNAC follows the logic as defined below. The following nomenclature is used by the Cisco DNAC to derive the WLAN profile name. <SSID>_F1_F_66c3d178 and <SSID>_F2_F_3f83cc83.



<SSID>_F1_F_66c3d178
SSID name
Location of override(6 characaters)
F=Fabric SSID
UUID- An internal hex decimal value representing the location(F1)

```
show wlan summary

Number of WLANs: 2

ID   Profile Name                     SSID                            Status   Security
-------------------------------------------------------------------------------------------------------
17   fabricssid_F1_F_66c3d178         fabricssid                        UP   [WPA2][802.1x][AES]
18   fabricssid_F2_F_3f83cc83         fabricssid                        UP   [WPA2][802.1x][AES]
```

SD-Access policy

In SD-Access, the network policy is a group-based policy based on Cisco TrustSec®. Virtual networks (VNs) (the equivalent of VRFs) and scalable group tags (SGTS) are used to provide a hierarchical network policy and segmentation: at a macro level, you can use VNs to completely separate groups of users, from a control plane and data plane perspective. This is stateful segmentation, as you would usually go through a firewall to allow inter-VRF traffic. Within the VN, SGTs allow customers to implement micro-segmentation and define a stateless policy between users based on secure group access control lists (SGACLs). The beauty of SD-Access is that this applies to both wired and wireless users.

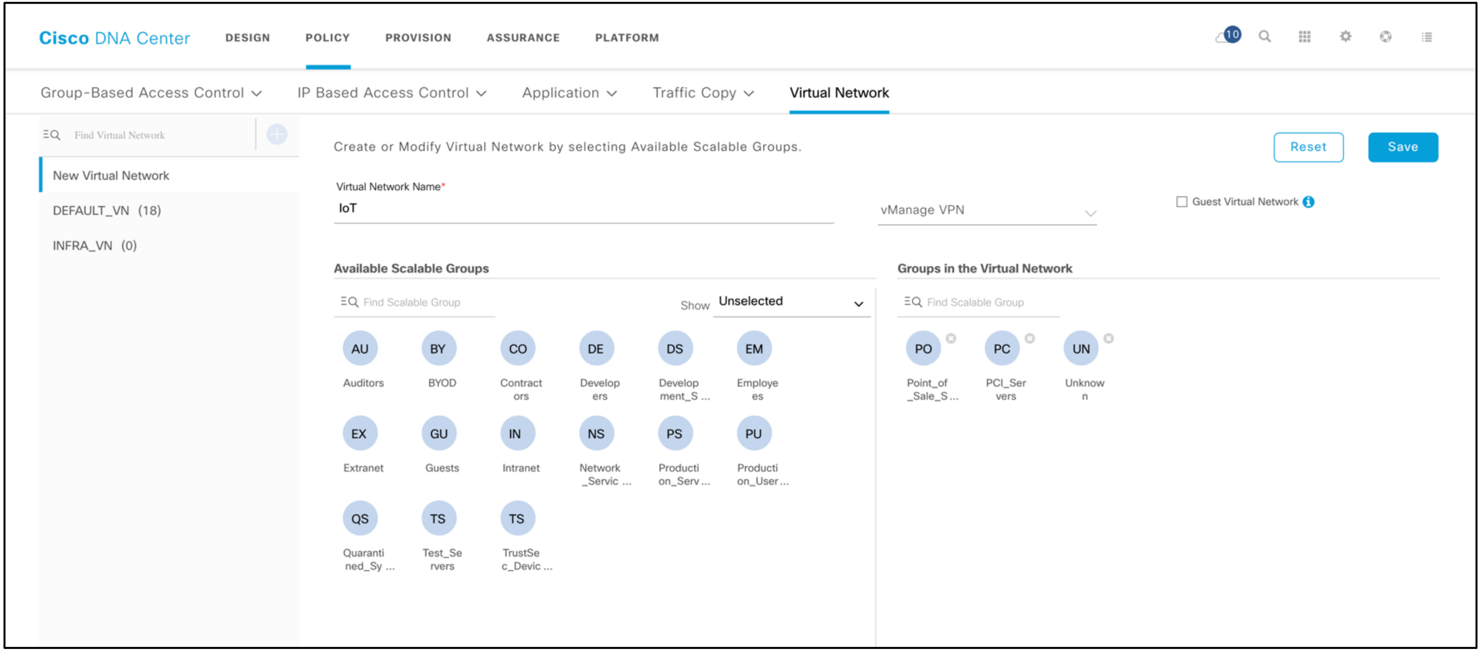
In the subsequent section, we would create a policy between two groups in the fabric and assign a contract. A contract “demo_access” is created to allow HTTP access between the two user groups “employees” and “pci_servers”.

To assign an SGT to a user, refer to the Identity service Engine(ISE) guide for segmentation.

ISE Segmentation Guide.

Procedure

Step 1 In Policy > Virtual Network page, create a new VN by clicking the “+” icon. Choose a name and assign scalable groups to the VN. This is an optional step.



Create or Modify Virtual Network by selecting Available Scalable Groups.

Virtual Network Name* IoT

vManage VPN

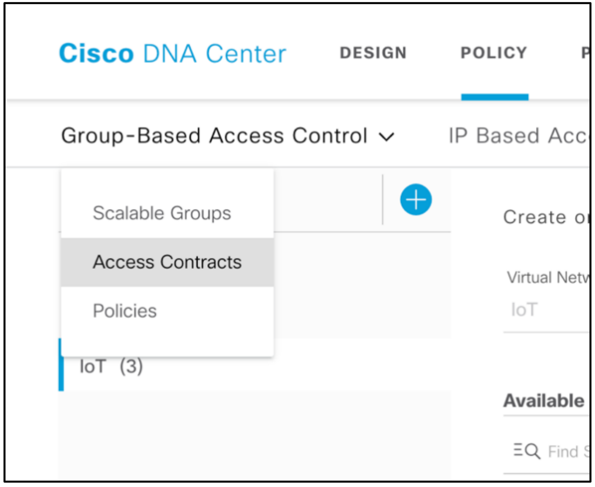
□ Guest Virtual Network

The reason you might want to add groups (SGTs) to a VN at this point will become clear in the onboarding section: if you want to statically assign an SGT to an SSID or a port, you can do it through a pool association, and when selecting the SGT you can choose from the ones you have included in the VN at this point.

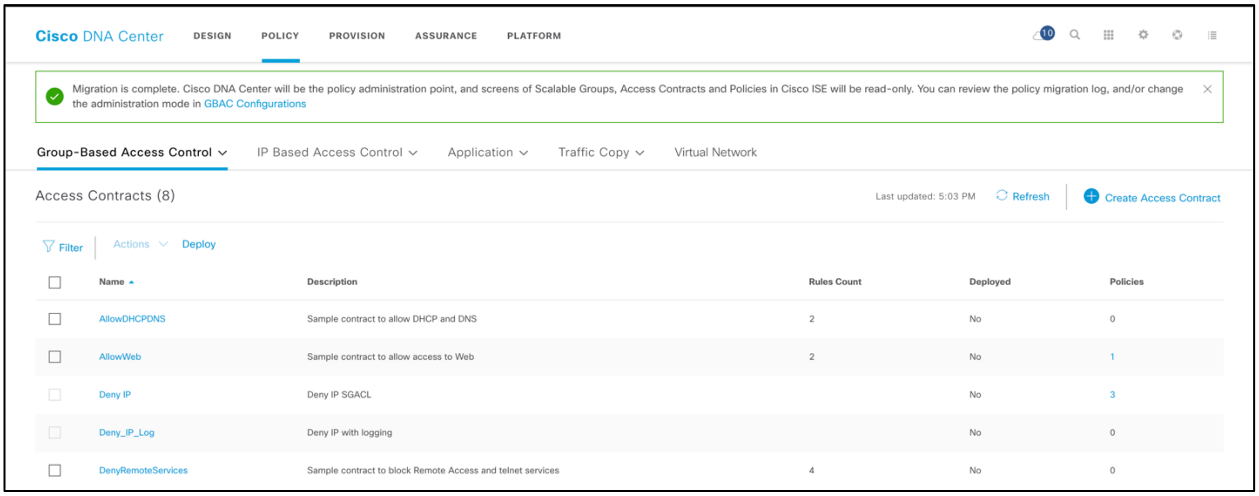
Step 2 Click Save to create the VN.

Upon successful creation, you will see a message pop up in the lower right corner of the screen.

Step 3 Next, click Policy > Group-Based Access Control > Access Contracts to add a Contract. A contract is where you define what traffic is permitted between scalable groups.



Click the Add Contract icon on the top right corner of the window to open up the contract editor as shown below. In this example, we have created "demo_access" with Permit action for a specific port/protocol, in this case HTTPs. Note the implicit Deny action; you can change it to default Permit. Click Save to create the contract.

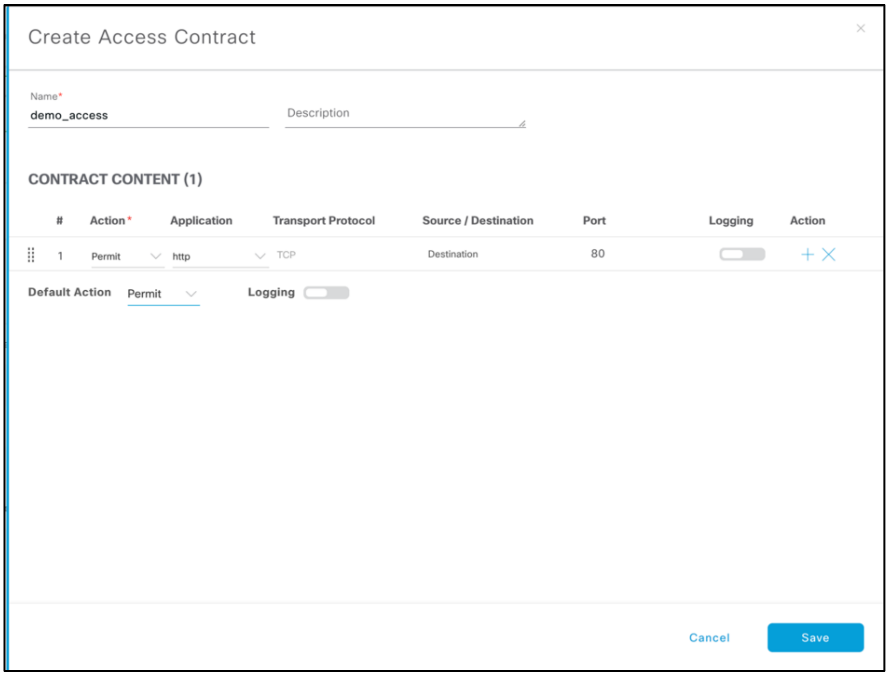


Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations

Access Contracts (8)

Last updated: 5:03 PM

□	Name	Description	Rules Count	Deployed	Policies
□	AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	No	0
□	AllowWeb	Sample contract to allow access to Web	2	No	1
□	Deny IP	Deny IP SGACL		No	3
□	Deny_IP_Log	Deny IP with logging		No	0
□	DenyRemoteServices	Sample contract to block Remote Access and telnet services	4	No	0



Create Access Contract

Name* demo_access

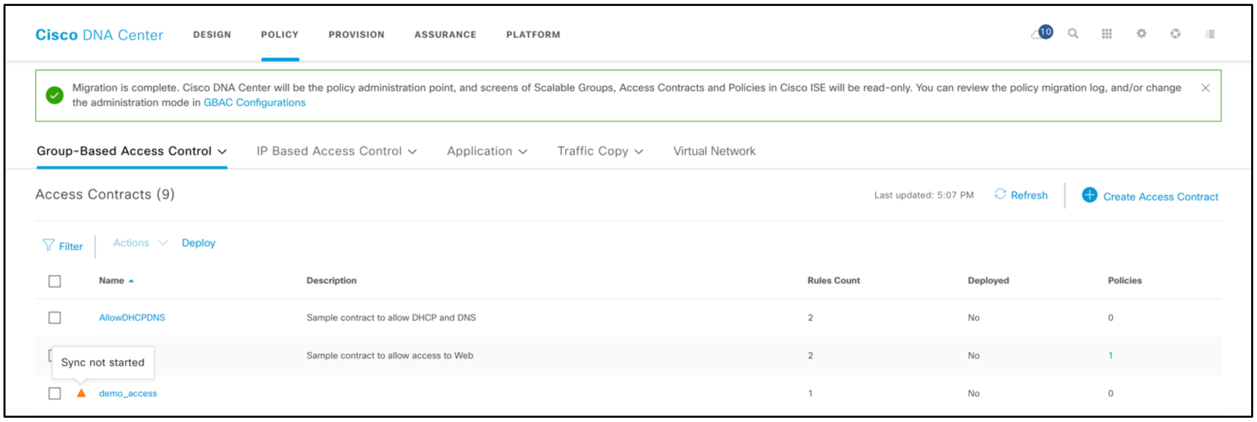
Description

CONTRACT CONTENT (1)

#	Action*	Application	Transport Protocol	Source / Destination	Port	Logging	Action
1	Permit	http	TCP	Destination	80		+ ×

Default Action Permit Logging

A new contract is created but it is not yet deployed. To deploy it, click on the new contract checkbox and click on Deploy.

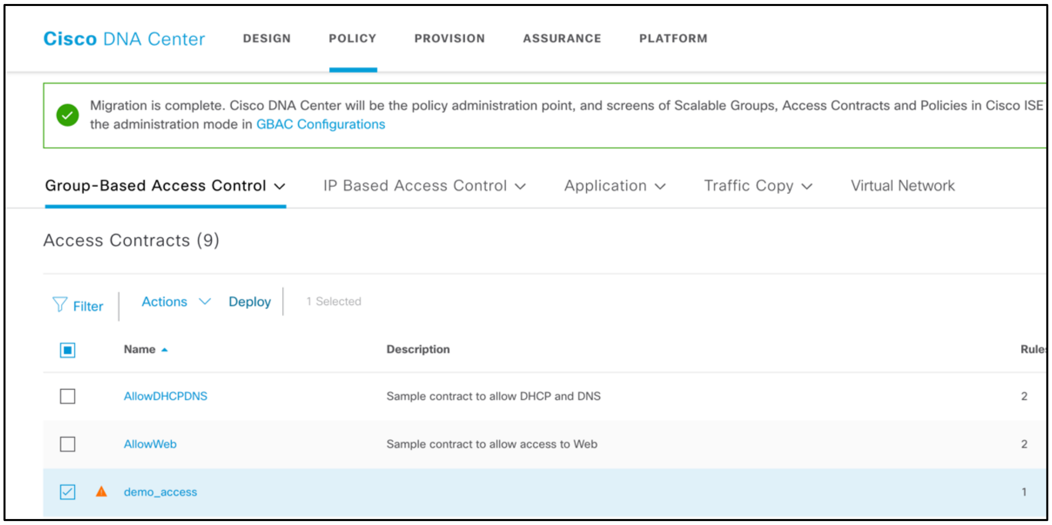


Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations

Access Contracts (9)

Last updated: 5:07 PM

☐	Name ▲	Description	Rules Count	Deployed	Policies
☐	AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	No	0
☐	Sync not started	Sample contract to allow access to Web	2	No	1
☐	▲ demo_access		1	No	0

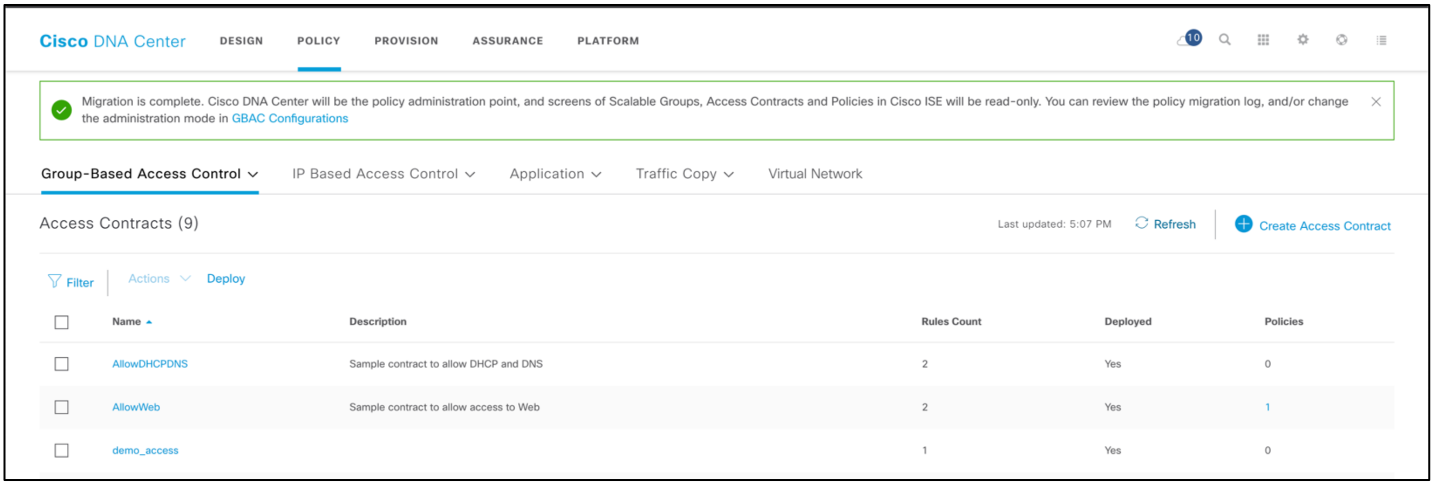


Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE
the administration mode in GBAC Configurations

Access Contracts (9)

1 Selected

■	Name ▲	Description	Rule
☐	AllowDHCPDNS	Sample contract to allow DHCP and DNS	2
☐	AllowWeb	Sample contract to allow access to Web	2
☑	▲ demo_access		1



Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations

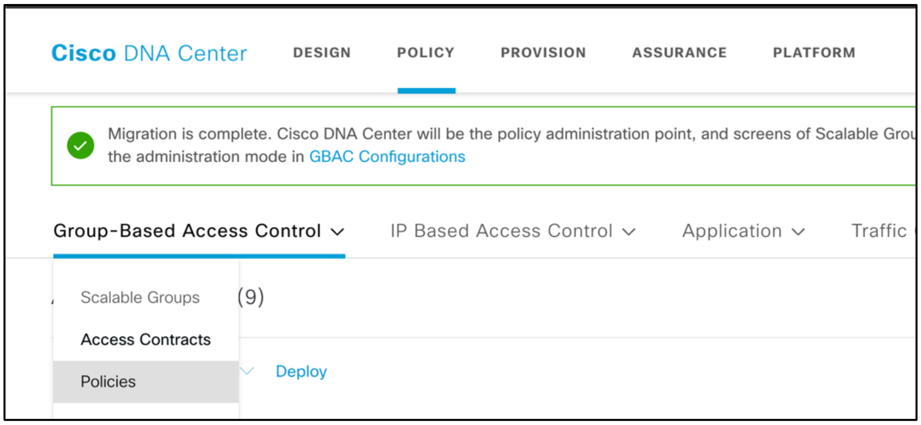
Access Contracts (9)

Last updated: 5:07 PM

□	Name ▲	Description	Rules Count	Deployed	Policies
□	AllowDHCPDNS	Sample contract to allow DHCP and DNS	2	Yes	0
□	AllowWeb	Sample contract to allow access to Web	2	Yes	1
□	demo_access		1	Yes	0

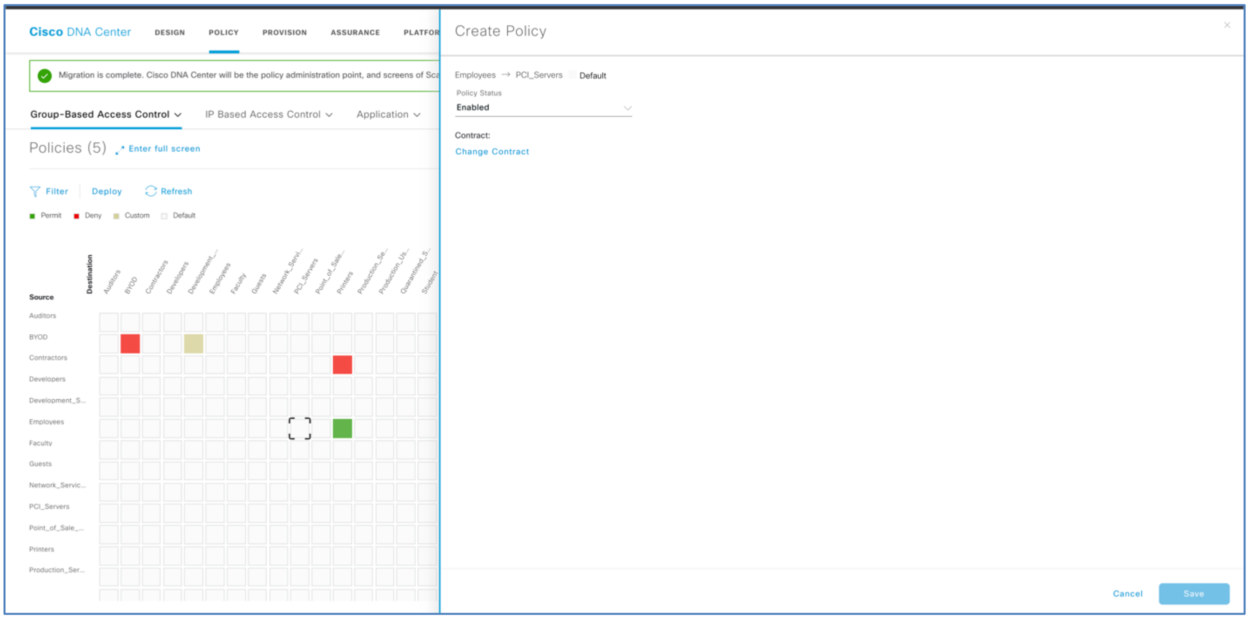
The screenshot is for reference only. You can name the contract as per your choice and assign any permission to it.

Step 4 Lastly, create a group-based access policy using the contract (created in step 3) to tie scalable groups together. Go to **Policy** > **Group-Based Access Control** > **Policies.**



Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Grou
the administration mode in GBAC Configurations

Step 5 In the Policy you will notice a Matrix with Source and Destination Scalable Groups. Click on any of the combinations of Scalable groups, for example: Employees > PCI_Servers.



Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Sca

Policies (5)

🟩 Permit 🟥 Deny ▨ Custom □ Default

Source \ Destination	Auditors	BYOD	Contractors	Developers	Development_...	Employees	Faculty	Guests	Network_Servi...	PCI_Servers	Point_of_Sale...	Printers	Production_Se...	Production_Us...	Quarantined_S...	Student
Auditors																
BYOD		🟥			▨											
Contractors												🟥				
Developers																
Development_S...																
Employees												🟩				
Faculty																
Guests																
Network_Servic...																
PCI_Servers																
Point_of_Sale_...																
Printers																
Production_Ser...																

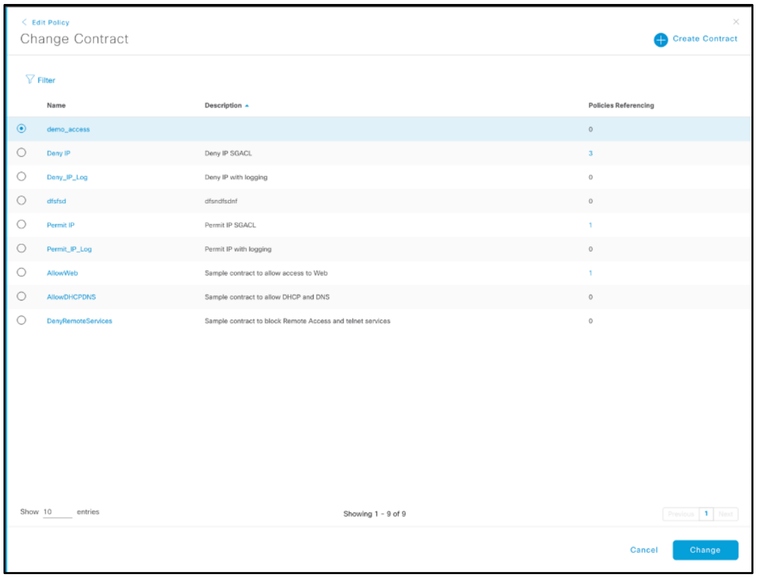
Create Policy

Employees → PCI_Servers Default

Policy Status: Enabled

Contract:

Click on Change Contract from the right-hand side pane and select the “demo_access” contract that we created in the last step. This is Policy between Employee and PCI_Servers.



< Edit Policy

Change Contract

⊕ Create Contract

Filter

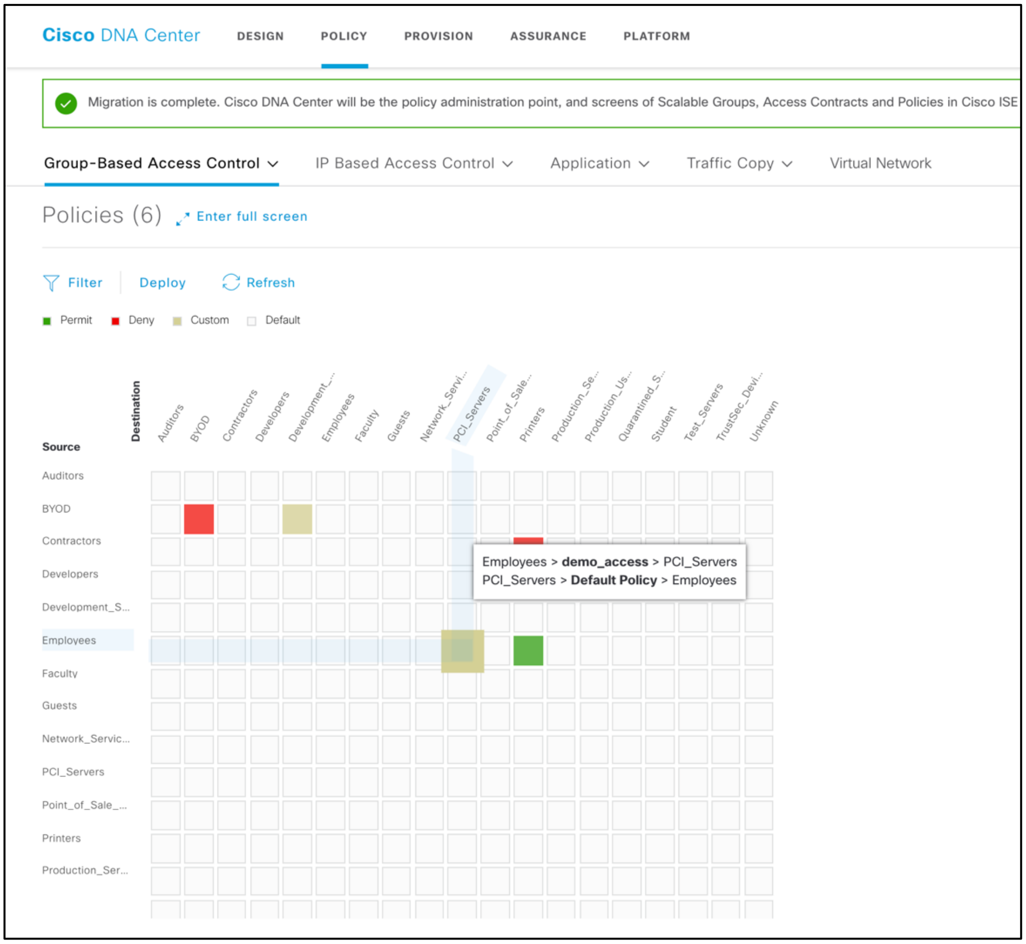
	Name	Description ▲	Policies Referencing
●	demo_access		0
○	Deny IP	Deny IP SGACL	3
○	Deny_IP_Log	Deny IP with logging	0
○	dfsfsd	dfsndfsdnf	0
○	Permit IP	Permit IP SGACL	1
○	Permit_IP_Log	Permit IP with logging	0
○	AllowWeb	Sample contract to allow access to Web	1
○	AllowDHCPDNS	Sample contract to allow DHCP and DNS	0
○	DenyRemoteServices	Sample contract to block Remote Access and telnet services	0

Show 10 entries

Showing 1 - 9 of 9

Click on Change and Save to see that this policy gets applied.

Verify from the Policies Matrix page that the Scalable Group Access List policy got created.



Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE

Policies (6)

🟩 Permit 🟥 Deny ▨ Custom □ Default

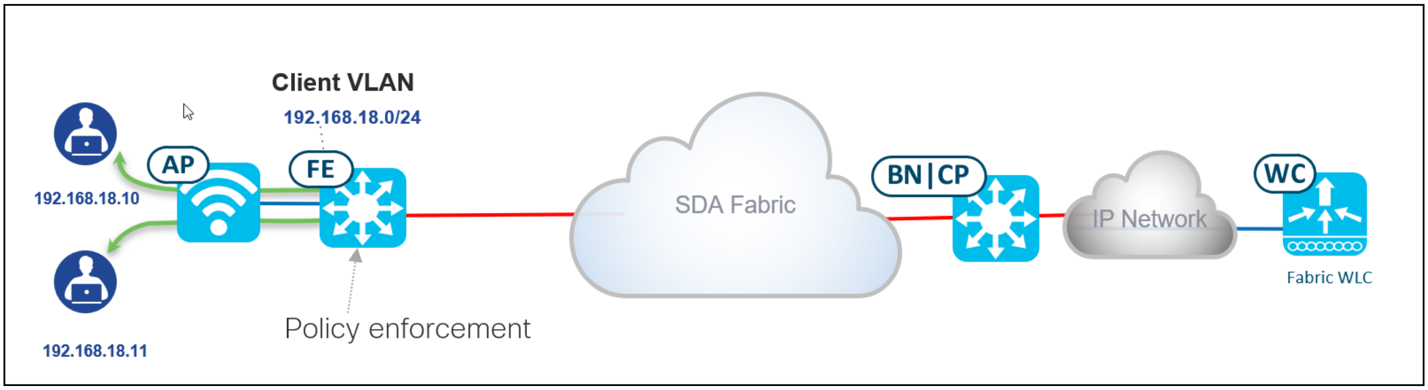
Source \ Destination	Auditors	BYOD	Contractors	Developers	Development_...	Employees	Faculty	Guests	Network_Servi...	PCI_Servers	Point_of_Sale...	Printers	Production_Se...	Production_Us...	Quarantined_S...	Student	Test_Servers	TrustSec_Devi...	Unknown
Auditors																			
BYOD		🟥			▨														
Contractors												🟥							
Developers																			
Development_S...																			
Employees										▨		🟩							
Faculty																			
Guests																			
Network_Servic...																			
PCI_Servers																			
Point_of_Sale_...																			
Printers																			
Production_Ser...																			

Employees > **demo_access** > PCI_Servers
PCI_Servers > **Default Policy** > Employees

The above screenshot is for illustration purposes only. Create a policy depending on your selection of scalable groups.

Peer to Peer Blocking

One of the most common features used in the wireless network is peer to peer blocking. Peer to peer blocking is used in scenarios where an Administrator would want to restrict users in the same SSID to talk to each other. The most common use-case for guest traffic is where untrusted users are not allowed to communicate with each other for security reasons. To achieve peer to peer blocking in SD-Access fabric we would need to create a policy that defines the same SGT as the source and destination and deny IP communication between them. Native peer to peer blocking is NOT supported on the SDA-wireless. An administrator would have to use the Cisco Trustsec policy to achieve the desired output.



Traffic flow between clients connected to the same AP/SSID and on the same VLAN will always get switched at the Fabric edge, the AP encapsulates the traffic in a VxLAN tunnel to the fabric edge and the fabric edge does the switching of the traffic back to the same AP. By having the fabric edge to do the switching, the policy enforcement for peer to peer blocking can be achieved by having an SGACL that denies IP communication between the SGT's. The fabric edge downloads the SGACL from the Identity Service Engine (ISE) and can do the enforcement.

SD-Access overlay provisioning

The Provision section is where you push the network configurations to the devices.

Device (WLC) provisioning

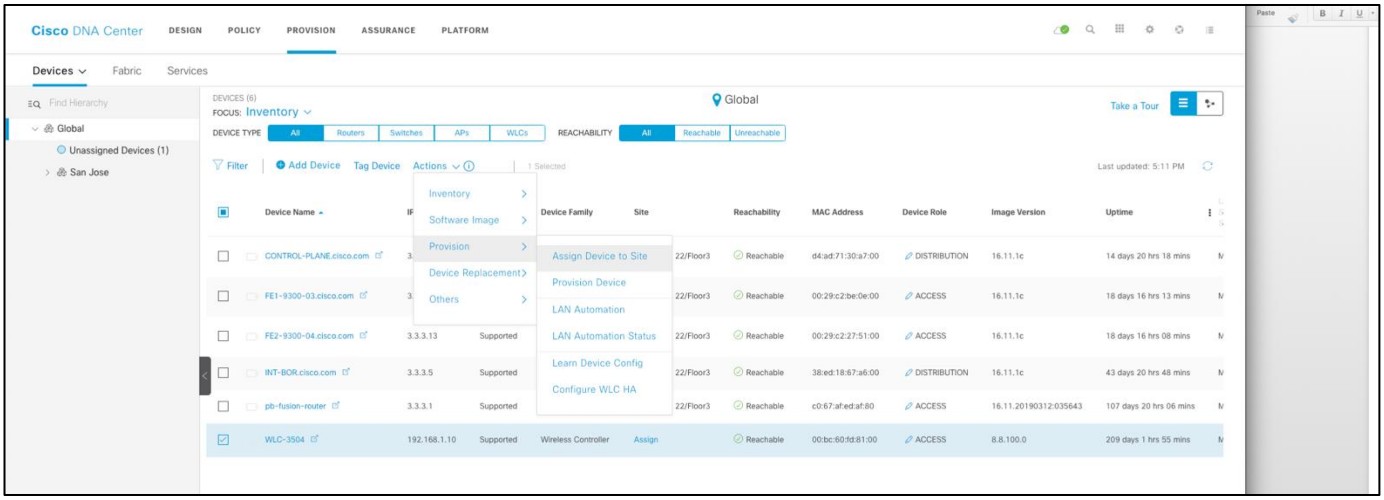
Procedure

Step 1 From the top menu, select the Provision tab.

Begin the provisioning process by selecting the WLC and associating it to the sites previously created during the design phase.

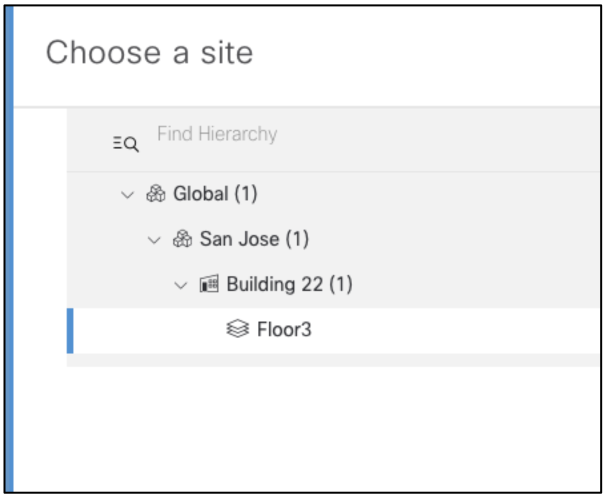
Step 2 Select the WLC using a single click. Once it is selected, pull down the Actions menu and choose Assign Device to Site, and then assign it to the location where the WLC is physically located. This step is important to assign the WLC to a regulatory domain corresponding to the site where it is physically located. The site needs to be a building or a floor – in other words, a site with coordinates.

Note The above screenshot is for illustration purposes only. Please select your network WLC.



DEVICES (6)
FOCUS: Inventory
DEVICE TYPE: All | Routers | Switches | APs | WLCs
REACHABILITY: All | Reachable | Unreachable
Last updated: 5:11 PM

	Device Name	IP		Device Family	Site	Reachability	MAC Address	Device Role	Image Version	Uptime
□	CONTROL-PLANE.cisco.com	3.			22/Floor3	Reachable	d4:ad:71:30:a7:00	DISTRIBUTION	16.11.1c	14 days 20 hrs 18 mins
□	FE1-9300-03.cisco.com	3.			22/Floor3	Reachable	00:29:c2:be:0e:00	ACCESS	16.11.1c	18 days 16 hrs 13 mins
□	FE2-9300-04.cisco.com	3.3.3.13	Supported		22/Floor3	Reachable	00:29:c2:27:51:00	ACCESS	16.11.1c	18 days 16 hrs 08 mins
□	INT-BOR.cisco.com	3.3.3.5	Supported		22/Floor3	Reachable	38:ed:18:67:a6:00	DISTRIBUTION	16.11.1c	43 days 20 hrs 48 mins
□	pb-fusion-router	3.3.3.1	Supported		22/Floor3	Reachable	c0:67:af:ed:af:80	ACCESS	16.11.20190312:035643	107 days 20 hrs 06 mins
☑	WLC-3504	192.168.1.10	Supported	Wireless Controller	Assign	Reachable	00:bc:60:fd:81:00	ACCESS	8.8.100.0	209 days 1 hrs 55 mins

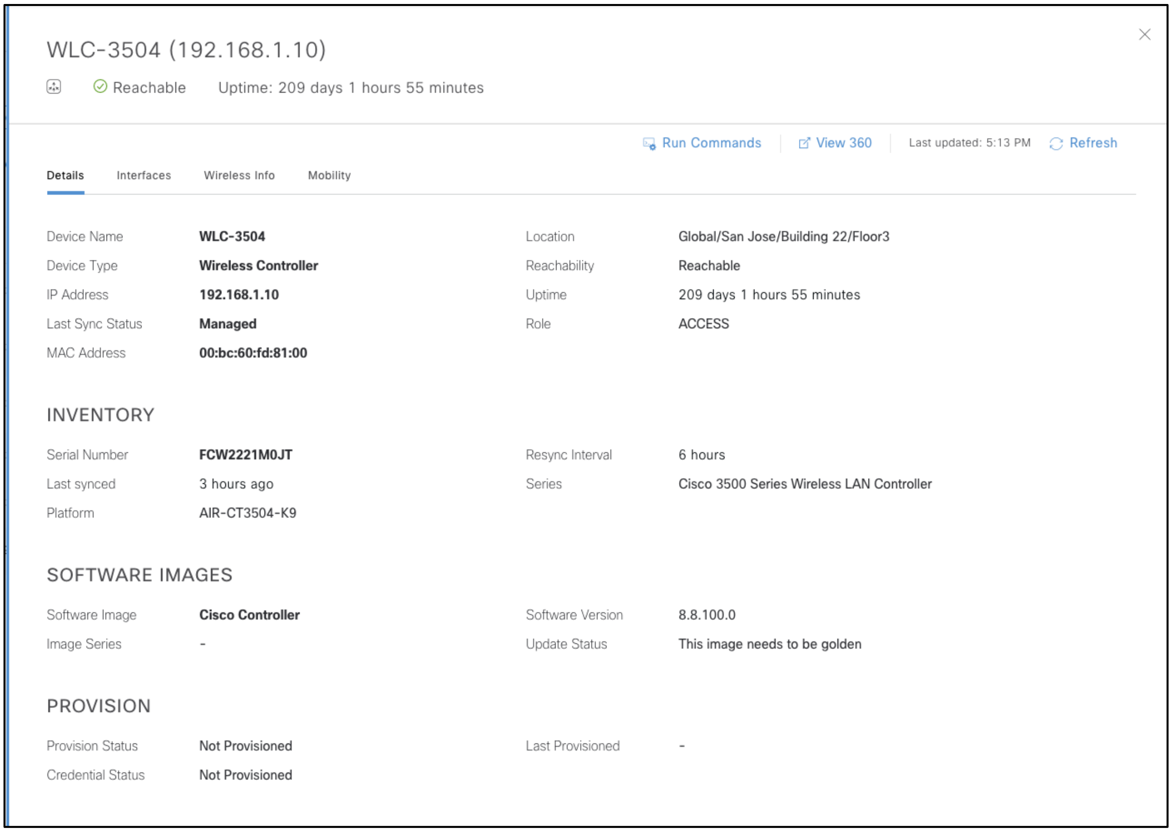


Choose a site

Find Hierarchy

- Global (1)
  - San Jose (1)
    - Building 22 (1)
      - Floor3

If you want to configure stateful switchover high availability (SSO HA), you need to add the second WLC to the same site at this point. Then, from the same Device Inventory page, click the WLC you want to configure as primary and go to the High Availability tab. Here enter the Management and Redundancy Management information for both the primary and secondary controllers and then click OK. The controllers will reboot, and after some time you will see only one WLC in the inventory. From now on, you can continue to provision as if it was a single WLC.



WLC-3504 (192.168.1.10)

Reachable   Uptime: 209 days 1 hours 55 minutes

Last updated: 5:13 PM

Device Name	WLC-3504	Location	Global/San Jose/Building 22/Floor3
Device Type	Wireless Controller	Reachability	Reachable
IP Address	192.168.1.10	Uptime	209 days 1 hours 55 minutes
Last Sync Status	Managed	Role	ACCESS
MAC Address	00:bc:60:fd:81:00		

INVENTORY

Serial Number	FCW2221M0JT	Resync Interval	6 hours
Last synced	3 hours ago	Series	Cisco 3500 Series Wireless LAN Controller
Platform	AIR-CT3504-K9		

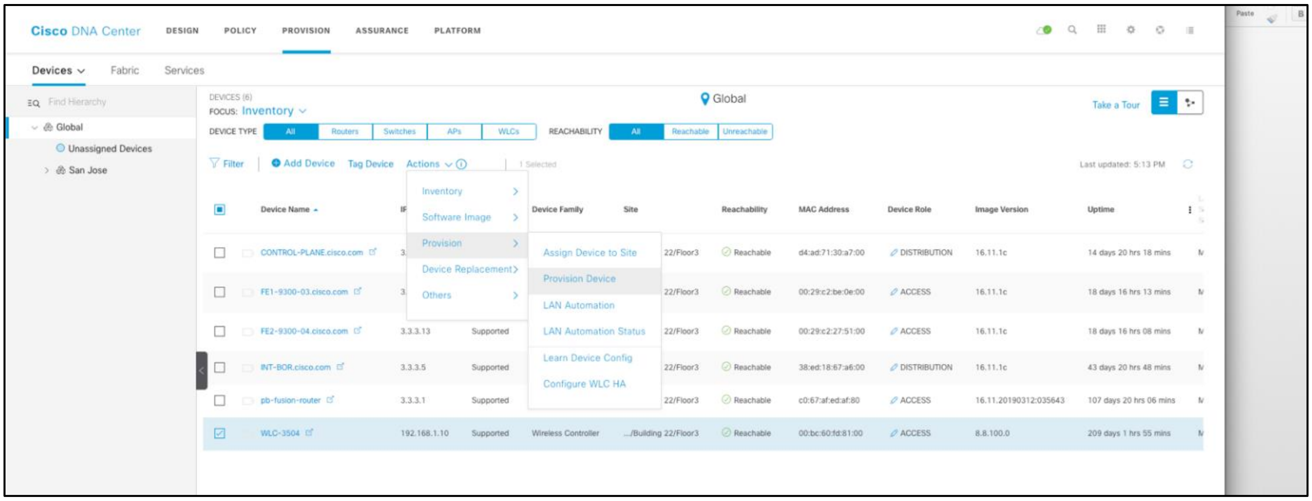
SOFTWARE IMAGES

Software Image	Cisco Controller	Software Version	8.8.100.0
Image Series	-	Update Status	This image needs to be golden

PROVISION

Provision Status	Not Provisioned	Last Provisioned	-
Credential Status	Not Provisioned		

Step 3 Once the WLC is added to the site, select it and click Provision.



DEVICES (6)

FOCUS: Inventory

Global

DEVICE TYPE: All

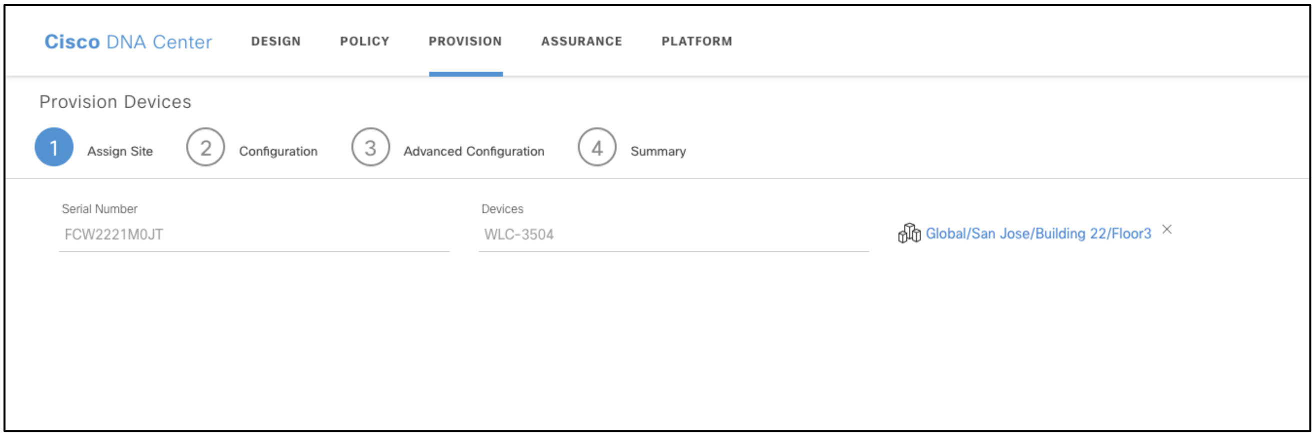
REACHABILITY: All

1 Selected

Last updated: 5:13 PM

	Device Name	IP		Device Family	Site	Reachability	MAC Address	Device Role	Image Version	Uptime
☐	CONTROL-PLANE.cisco.com	3.			22/Floor3	Reachable	d4:ad:71:30:a7:00	DISTRIBUTION	16.11.1c	14 days 20 hrs 18 mins
☐	FE1-9300-03.cisco.com	3.			22/Floor3	Reachable	00:29:c2:be:0e:00	ACCESS	16.11.1c	18 days 16 hrs 13 mins
☐	FE2-9300-04.cisco.com	3.3.3.13	Supported		22/Floor3	Reachable	00:29:c2:27:51:00	ACCESS	16.11.1c	18 days 16 hrs 08 mins
☐	INT-BOR.cisco.com	3.3.3.5	Supported		22/Floor3	Reachable	38:ed:18:67:a6:00	DISTRIBUTION	16.11.1c	43 days 20 hrs 48 mins
☐	pb-fusion-router	3.3.3.1	Supported		22/Floor3	Reachable	c0:67:af:ed:af:80	ACCESS	16.11.20190312:035643	107 days 20 hrs 06 mins
☑	WLC-3504	192.168.1.10	Supported	Wireless Controller	.../Building 22/Floor3	Reachable	00:bc:60:fd:81:00	ACCESS	8.8.100.0	209 days 1 hrs 55 mins

Step 4 Select the location where the WLC is placed, the Settings defined in the network profiles such as the Syslog/SNMP and NTP are pushed to the WLC

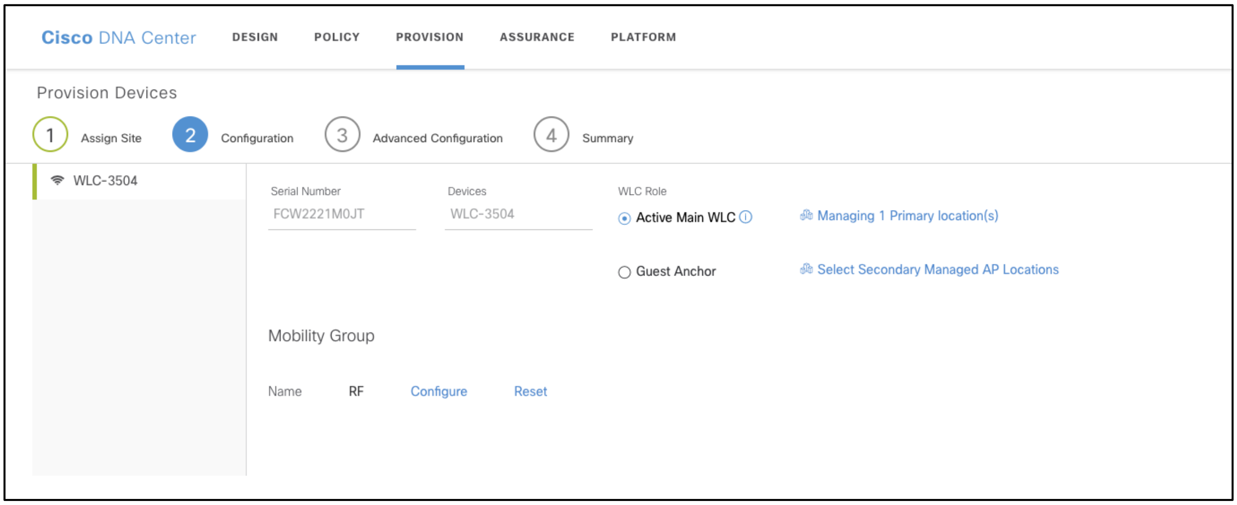


Serial Number: FCW2221M0JT

Devices: WLC-3504

Global/San Jose/Building 22/Floor3 ×

Step 5 Select the AP locations managed by this WLC. It is important to select the floors where you will have APs deployed, if any. Click Next.



Serial Number: FCW2221M0JT

Devices: WLC-3504

WLC Role

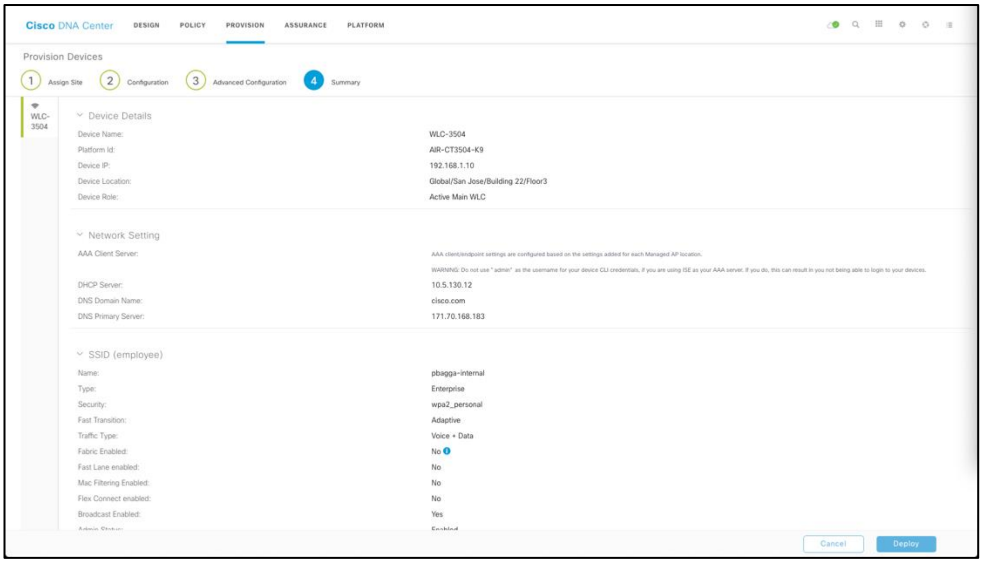
● Active Main WLC ⓘ — Managing 1 Primary location(s)

○ Guest Anchor — Select Secondary Managed AP Locations

Mobility Group

Name RF

Step 6 Review the configuration – system details, global settings for authentication, authorization, and accounting (AAA), DHCP, DNS servers, SSID, and managed sites that will be pushed as part of WLC provisioning from Cisco DNA Center. Click Deploy.



Device Details

Device Name: WLC-3504

Platform Id: AIR-CT3504-K9

Device IP: 192.168.1.10

Device Location: Global/San Jose/Building 22/Floor3

Device Role: Active Main WLC

Network Setting

AAA Client Server: AAA client/endpoint settings are configured based on the settings added for each Managed AP location.

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

DHCP Server: 10.5.130.12

DNS Domain Name: cisco.com

DNS Primary Server: 171.70.168.183

SSID (employee)

Name: pbagga-internal

Type: Enterprise

Security: wpa2_personal

Fast Transition: Adaptive

Traffic Type: Voice + Data

Fabric Enabled: No ⓘ

Fast Lane enabled: No

Mac Filtering Enabled: No

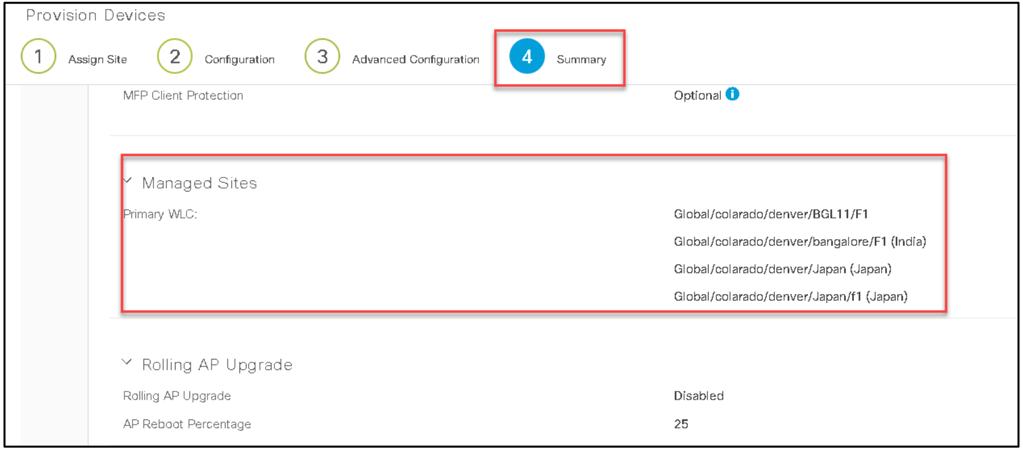
Flex Connect enabled: No

Broadcast Enabled: Yes

Admin Status: Enabled

Note: The Country code of the WLC is chosen based on the region where the Access point is mapped. If the WLC is managing the Access Point mapped to a region for example: India and the US. Then the country code pushed by the DNAC is "US, IN". The

country code is mapped to a Building and the floors beneath it inherit it from the building.
Refer to the screenshot below to understand the country codes pushed to the WLC by the Cisco DNA Center.



Provision Devices

MFP Client Protection	Optional

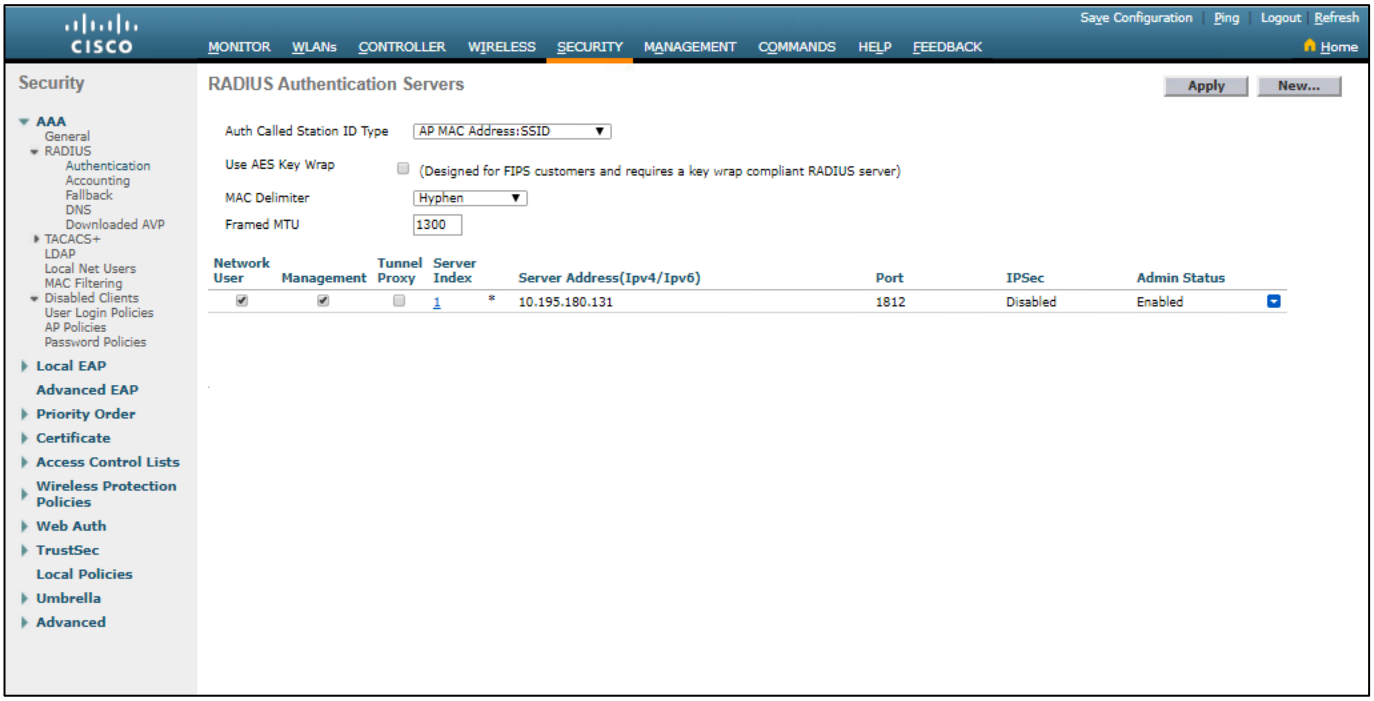
Managed Sites

Primary WLC:	Global/colarado/denver/BGL11/F1
	Global/colarado/denver/bangalore/F1 (India)
	Global/colarado/denver/Japan (Japan)
	Global/colarado/denver/Japan/f1 (Japan)

Rolling AP Upgrade

Rolling AP Upgrade	Disabled
AP Reboot Percentage	25

Step 7 The configuration pushed through Cisco DNA Center can be viewed on the WLC, such as the RADIUS server for authentication and accounting. Also, two WLANs are created with WLAN ID >17 and status disabled, one for each site the WLAN is associated with. The WLANs will be disabled until you configure Host Onboarding and assign a pool to the SSID.



RADIUS Authentication Servers

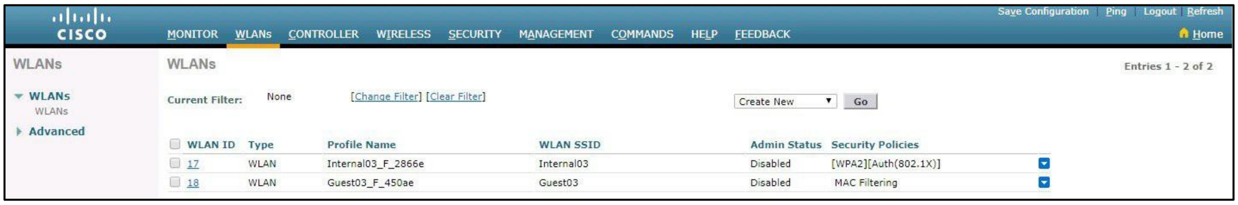
Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap: □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index		Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
☑	☑	□	1	*	10.195.180.131	1812	Disabled	Enabled



Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
Create New
Go

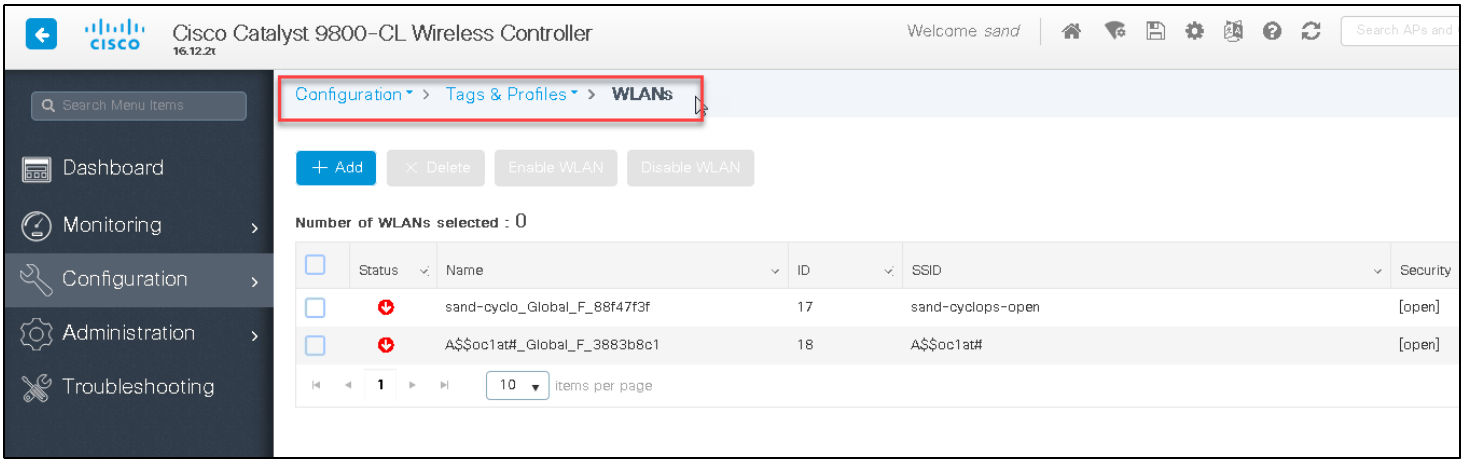
WLANs

Entries 1 - 2 of 2

Current Filter: None [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 17	WLAN	Internal03_F_2866e	Internal03	Disabled	[WPA2][Auth(802.1X)]
□ 18	WLAN	Guest03_F_450ae	Guest03	Disabled	MAC Filtering

Screenshot for Cisco Catalyst 9800 WLC:



Number of WLANs selected : 0

Status	Name	ID	SSID	Security
●	sand-cyclo_Global_F_88f47f3f	17	sand-cyclops-open	[open]
●	A$$oc1at#_Global_F_3883b8c1	18	A$$oc1at#	[open]

Note:

The above screenshots are for illustration purposes only. You will see your network-related configuration (IP address and names) on the WLC.

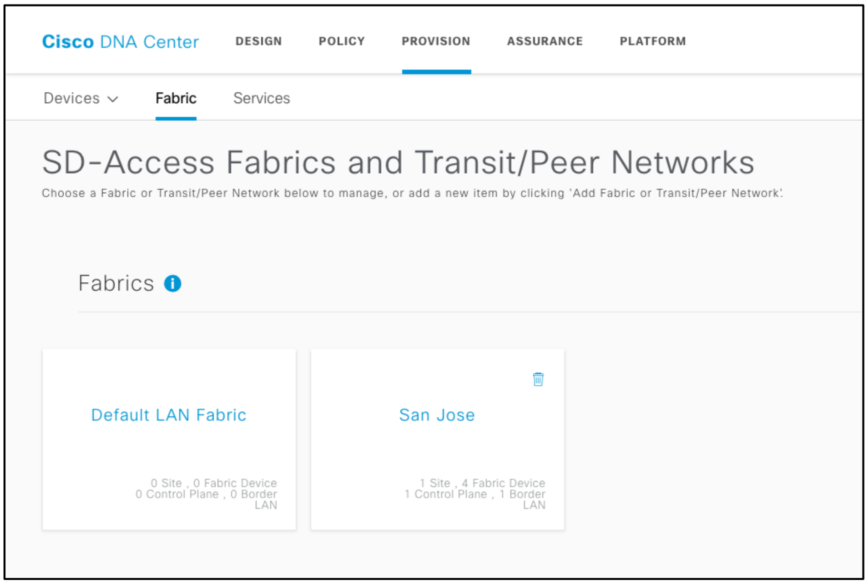
Now that Cisco DNA Center is aware of where devices reside within the sites, you can begin the fabric provisioning.

Creating fabric

Procedure

Step 1 Select Fabric from the menu. You will be taken to a new page for creating and managing the SD-Access fabric.

Step 2 You can create a new fabric or click Default LAN Fabric. In the example below, we have created a new fabric called San Jose.



SD-Access Fabrics and Transit/Peer Networks

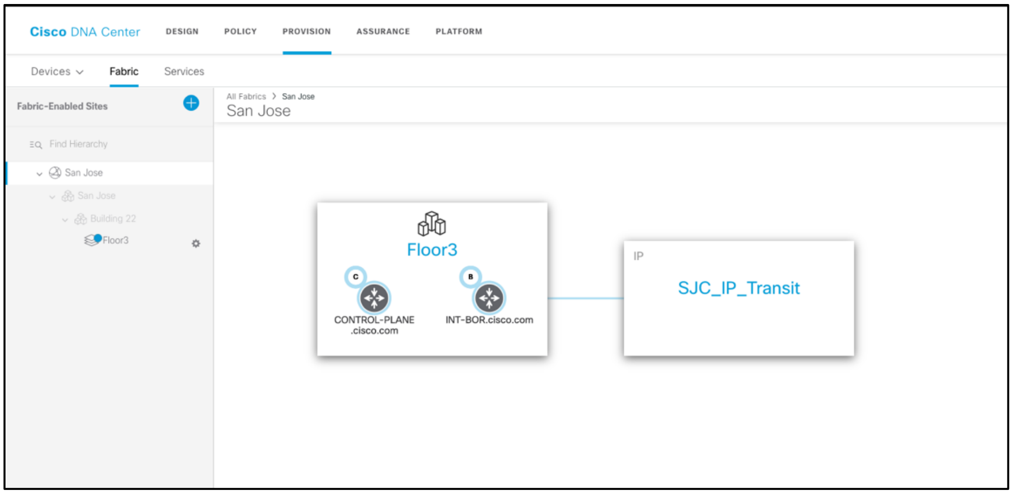
Choose a Fabric or Transit/Peer Network below to manage, or add a new item by clicking 'Add Fabric or Transit/Peer Network'.

Fabrics

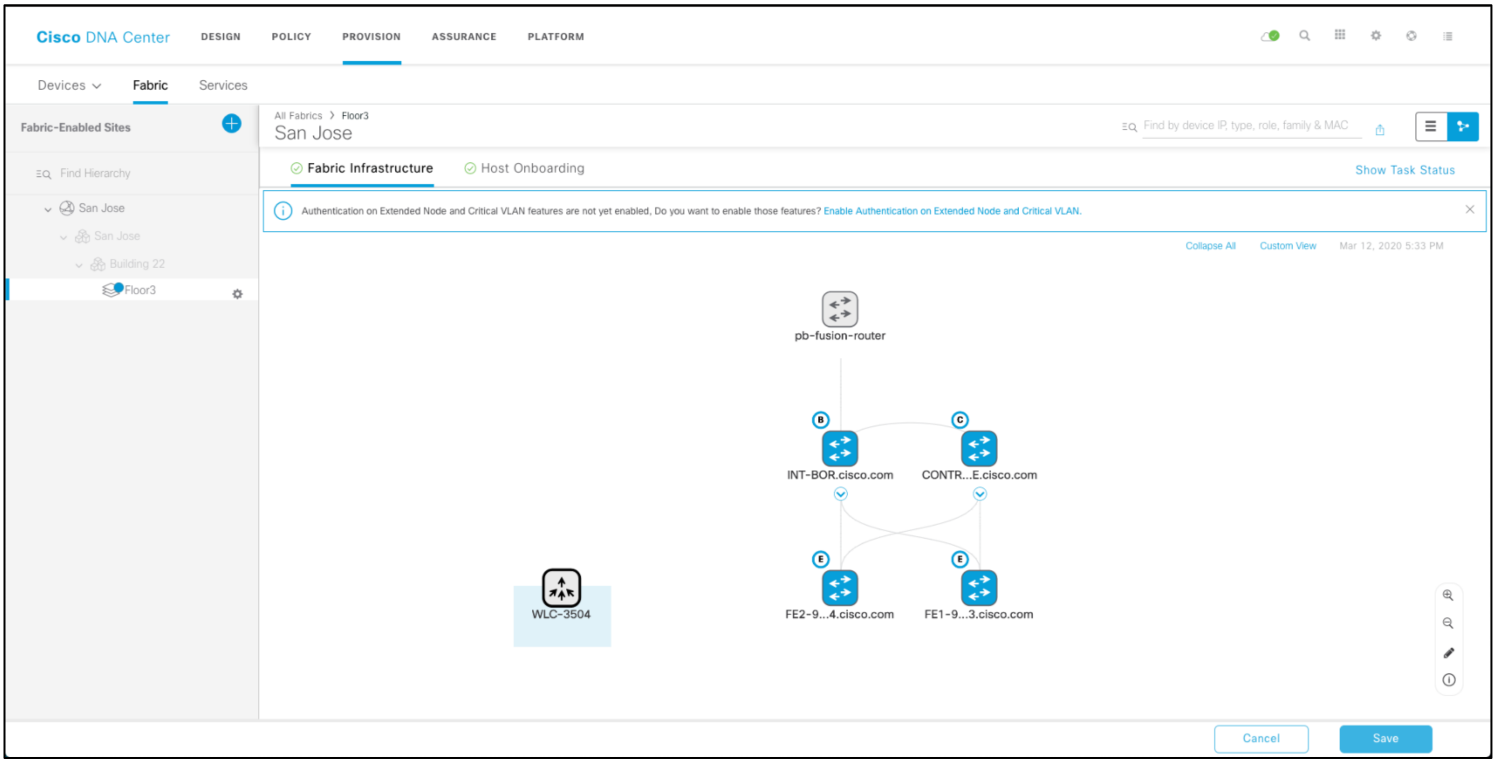
Default LAN Fabric
0 Site , 0 Fabric Device
0 Control Plane , 0 Border
LAN

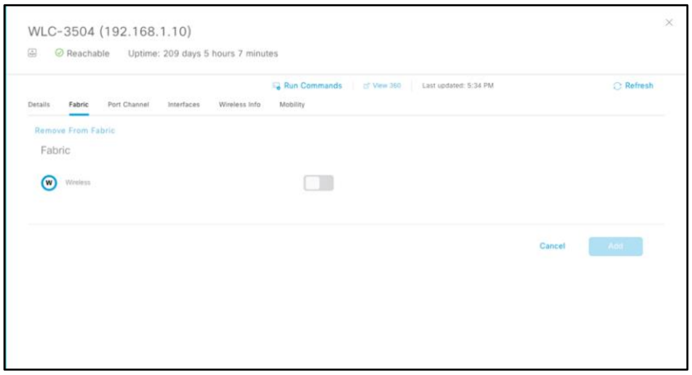
San Jose
1 Site , 4 Fabric Device
1 Control Plane , 1 Border
LAN

In San Jose Fabric, click on "Floor 3"

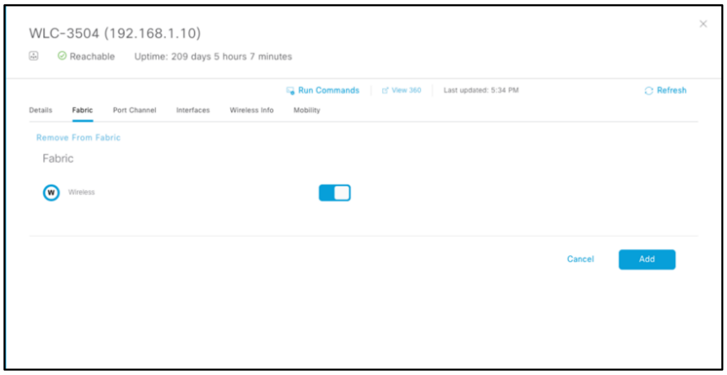


Step 3 Click Select Devices and add nodes to the fabric. To add a device to the fabric, just click the WLC-3504 and select the Wireless radio button to add the WLC to Fabric. Click Add.


Authentication on Extended Node and Critical VLAN features are not yet enabled, Do you want to enable those features? Enable Authentication on Extended Node and Critical VLAN.

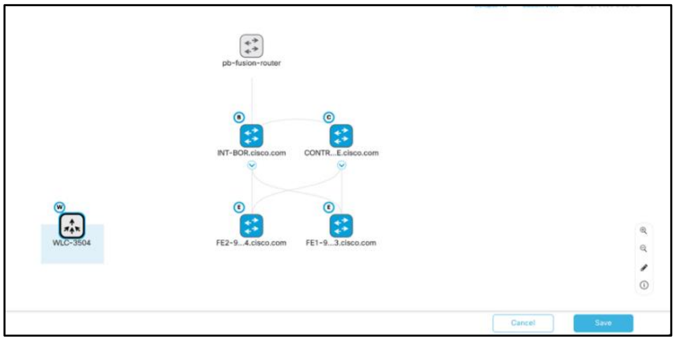

WLC-3504 (192.168.1.10)

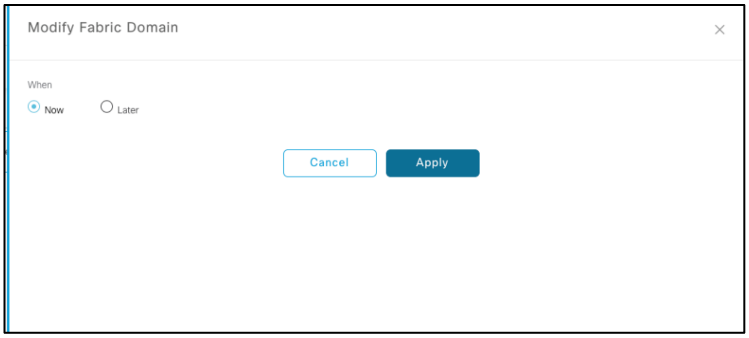
Reachable Uptime: 209 days 5 hours 7 minutes


WLC-3504 (192.168.1.10)

Reachable Uptime: 209 days 5 hours 7 minutes

Click Save and Apply to push the configurations to WLC and make it part of the Fabric.

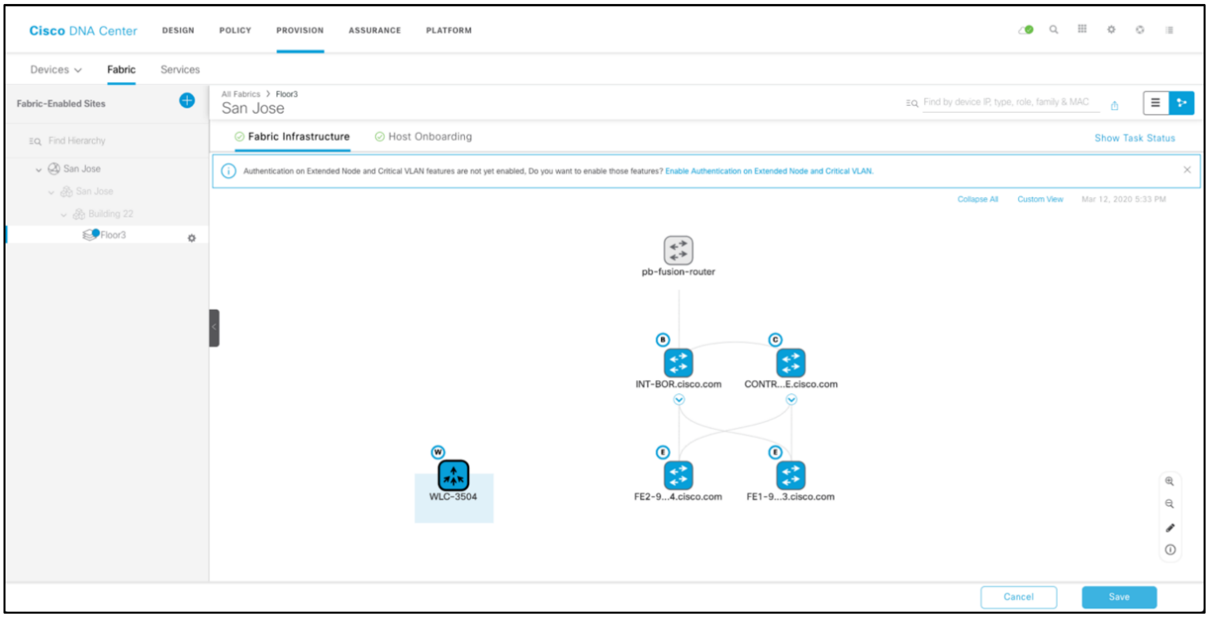



Modify Fabric Domain

When

● Now ○ Later

Step 4 The devices should change color from grey to blue once they are added to the fabric, as shown in the example below.



Authentication on Extended Node and Critical VLAN features are not yet enabled, Do you want to enable those features? Enable Authentication on Extended Node and Critical VLAN.

Note The above screenshot is for illustration purposes only. You may have multiple nodes as part of the fabric.

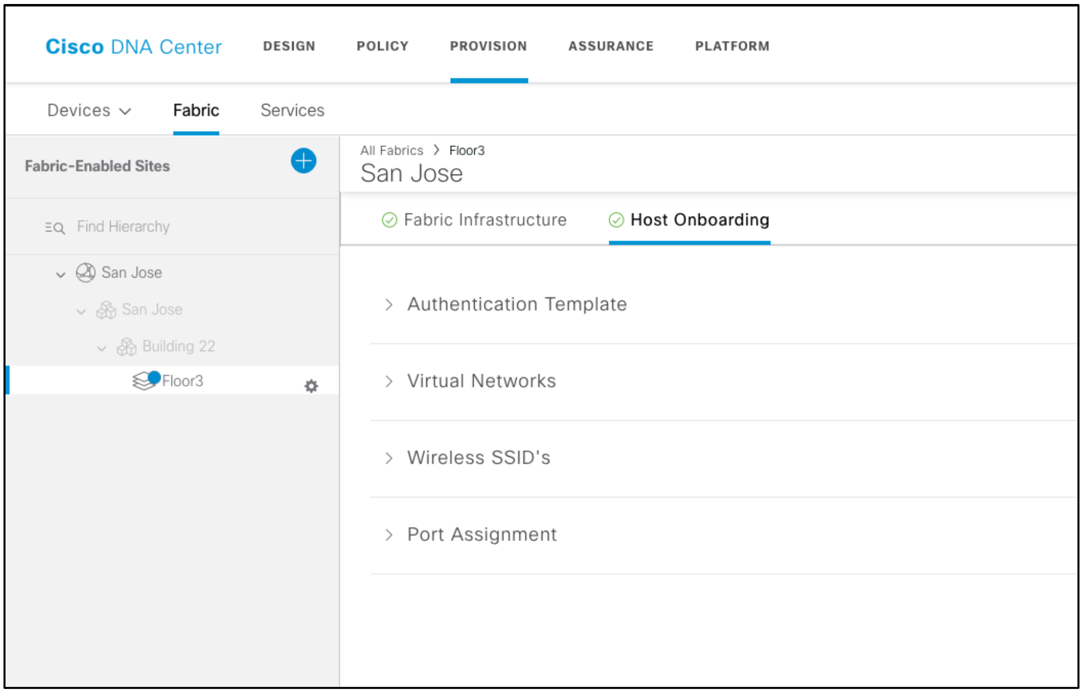
AP and host onboarding

In this guide, it is assumed that the fabric wired network has been provisioned already, so after adding the WLC it’s time to onboard APs and wireless clients. For this, IP address pools need to be added to enable APs and wireless hosts to communicate within the fabric. When an IP pool is configured in SD-Access, Cisco DNA Center immediately connects to each edge node to create the appropriate switch virtual interface (SVI) to allow the hosts to communicate.

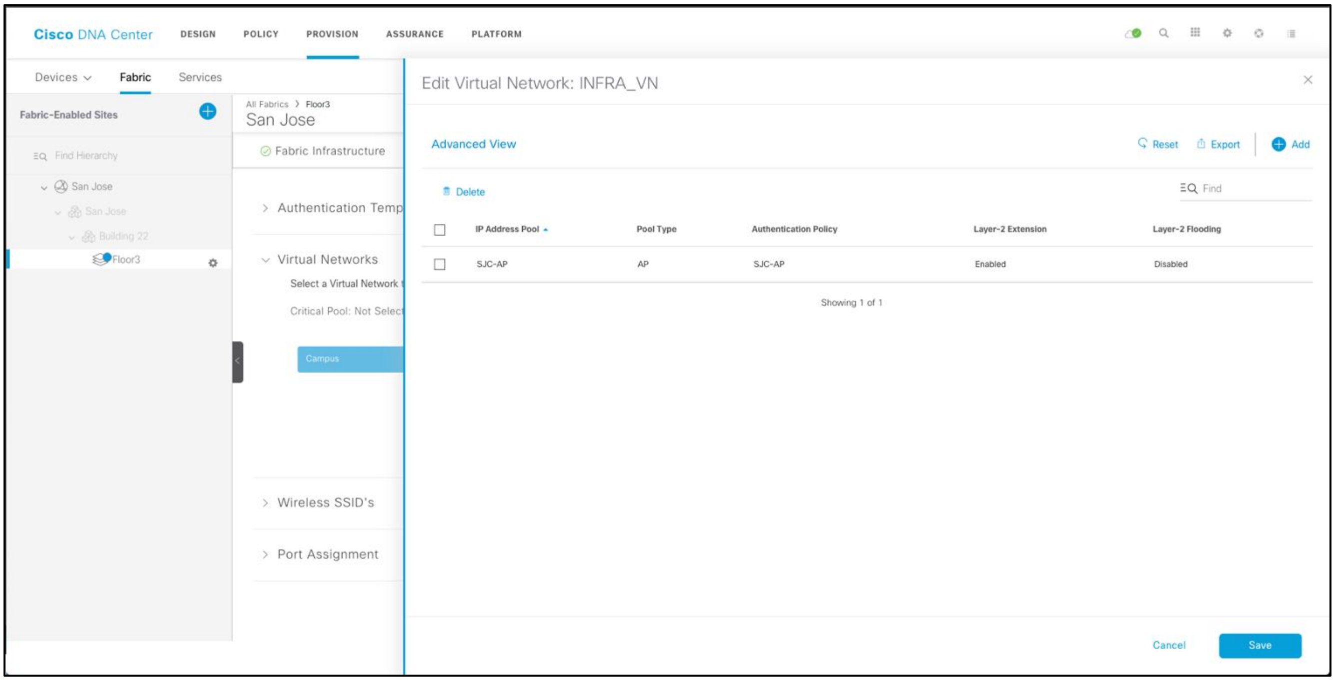
In addition, an anycast gateway is applied to all edge nodes. This is an essential element of SD-Access, as it allows hosts to easily roam to any edge node with no additional provisioning.

Procedure

Step 1 Click Host Onboarding at the top of this screen to start enabling the IP pools for APs and client devices.



Step 2 In Virtual Networks, click INFRA VN, and a window will open with configured address pools. Select the address pool for APs. Notice how AP provisioning and Layer 2 extension are already turned on for this VN, as both are needed to onboard APs. Click Save.



Edit Virtual Network: INFRA_VN

□	IP Address Pool	Pool Type	Authentication Policy	Layer-2 Extension	Layer-2 Flooding
□	SJC-AP	AP	SJC-AP	Enabled	Disabled

Showing 1 of 1

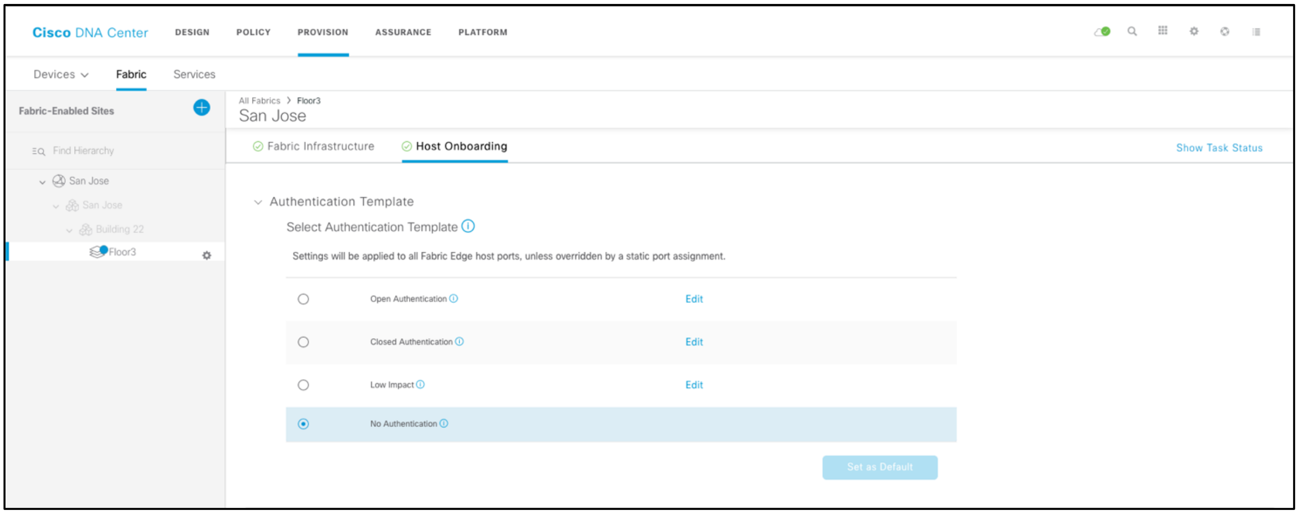
The Layer 2 Extension setting enables Layer 2 LISP and associates a Layer 2 VNID to this pool so that the Ethernet frame can be carried end to end on the fabric. This is what allows a simulated Layer 2 stretched subnet service.

Selecting AP Provision Pool will automatically push a configuration macro to all the edge node switches, so that when the AP is directly connected, the switch will recognize that it's an AP through Cisco Discovery Protocol and the macro will be applied to the port automatically, assigning the physical port to the right VLAN associated with the pool.

The **CDP macro** on the FEs for AP onboarding is pushed **only if** the **No Authentication** template is selected for the port.

With Cisco DNA Center 1.2.x macros were used to identify the device connected to a Fabric Edge (FE) as an AP. Once the macro detects the device to be a Cisco Access point, the relevant configuration is provisioned on that port.

With Cisco DNA Center 1.3.x, Autoconf is used to identify the device as a Cisco Access Point, so the port is provisioned with the right configurations. The example below shows the port configured as “No Authentication” mode. The Access point can be connected to a closed authentication port. The details on how to onboard an Access point on closed auth mode is discussed further in the following section. The Autoconf uses the Device Classifier to identify the end devices that are connected to a port.



Authentication Template

Select Authentication Template

Settings will be applied to all Fabric Edge host ports, unless overridden by a static port assignment.

○ Open Authentication Edit

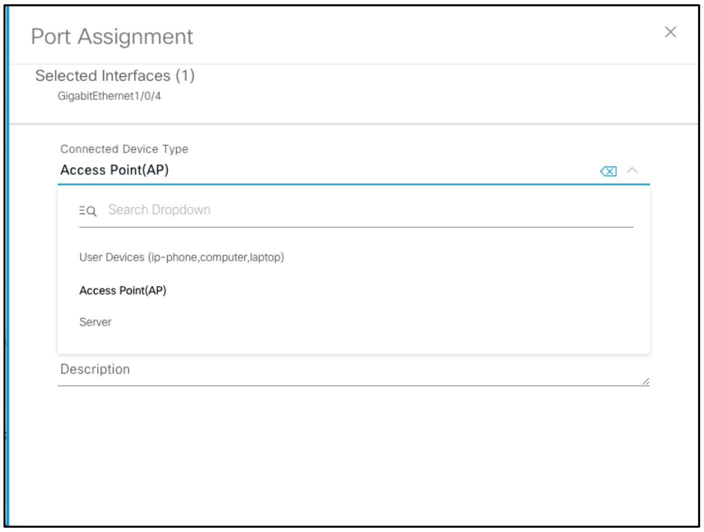
○ Closed Authentication Edit

○ Low Impact Edit

● No Authentication

Set as Default

In the Port Assignment section select on the ports that are connected to AP, and select the “Connected Device Type” as Access Point (AP). This step is required if using Cisco DNA Center 1.2.x and, if the Authentication template for the fabric is something other than “No Authentication”.



Port Assignment

Selected Interfaces (1)
GigabitEthernet1/0/4

Connected Device Type: Access Point(AP)

At this point, the AP will be assigned to the right VLAN/subnet, will obtain an IP address from the specified pool, and will discover the WLC through one of the standard mechanisms (Plug and Play, DHCP option 43, DNS, etc.). The AP then joins the WLC.

AP onboarding with Closed Authentication

In this section, it is assumed that the users have an understanding of closed authentication mode. The SD-Access fabric on DNAC 1.3.3 supports closed authentication mode with dot1x as the first priority followed by Machine Authentication Bypass(MAB). The Access point out of the box doesn’t have the dot1x supplicant enabled and is not provisioned with the credential to authenticate with the Fabric Edge. One of the main features that are used to onboard an AP with closed auth, is the use of profiling feature on Identity Service Engine(ISE).

The profiling feature enables ISE to identify the identity of the endpoints and once profiled assign the appropriate authorization profiles.

More details on the Profiling, refer to the guide on the community page.
ISE Profiling Design Guide
The Cisco DNA center automates the profiling configuration on the Fabric devices, an example of the profiling configuration pushed to the fabric devices are as follows:

```
device-sensor filter-list cdp list iseCDP
 tlv name device-name
 tlv name capabilities-type
 tlv name version-type
 tlv name platform-type
!
device-sensor filter-list dhcp list iseDHCP
 option name host-name
 option name parameter-request-list
 option name class-identifier
!
device-sensor filter-list lldp list iseLLDP
 tlv name system-name
 tlv name system-description
 tlv name system-capabilities
device-sensor filter-spec dhcp include list iseDHCP
device-sensor filter-spec lldp include list iseLLDP
device-sensor filter-spec cdp include list iseCDP
device-sensor notify all-changes
```

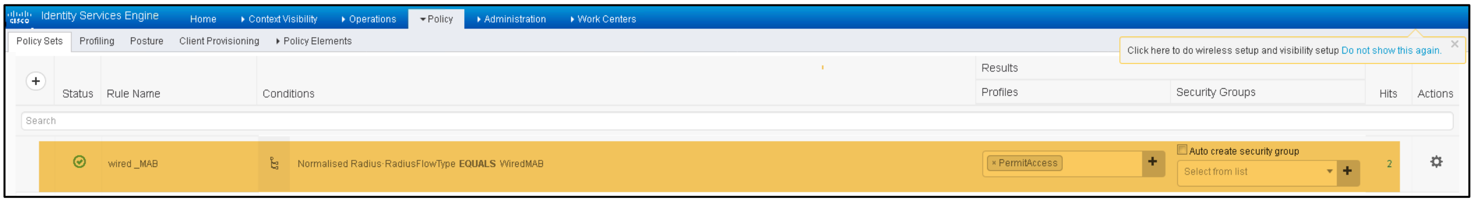
The Cisco DNA center automates a template on the Fabric Edge, this template needs to be returned as an attribute once the Access Point has been profiled on the Identity service Engine.
A sample of the template pushed to the fabric device are as follows:

```
template ApAutzTemplate
 switchport access vlan 2045
 switchport mode access
 access-session interface-template sticky timer 10
!
```

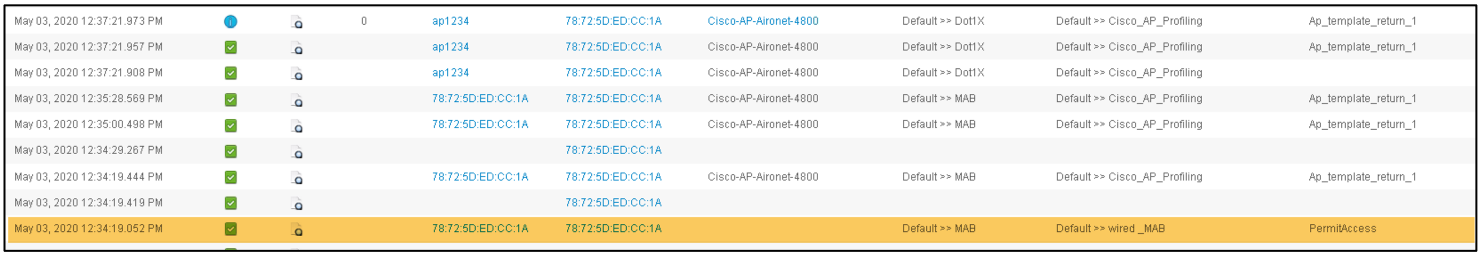
Let's discuss on the AP onboarding flow for closed auth

Step 1: AP connects to a port on the Fabric Edge configured for Closed authentication, the AP fails to respond to dot1x messages and the fabric edge does a fallback to MAB.

Initial authentication of Access Point using MAB:



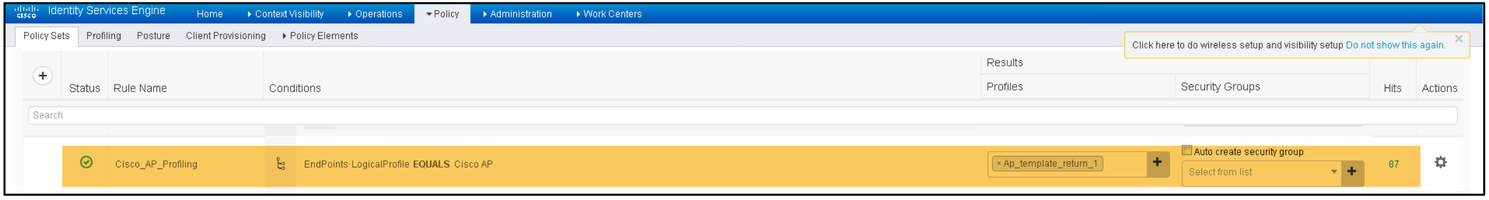
Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	wired _MAB	Normalised Radius·RadiusFlowType **EQUALS** WiredMAB	× PermitAccess	☐ Auto create security group Select from list	2	⚙



May 03, 2020 12:37:21.973 PM	●		0	ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.957 PM	✓			ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.908 PM	✓			ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	
May 03, 2020 12:35:28.569 PM	✓			78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM	✓			78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM	✓				78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM	✓			78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM	✓				78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM	✓			78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A		Default >> MAB	Default >> wired _MAB	PermitAccess

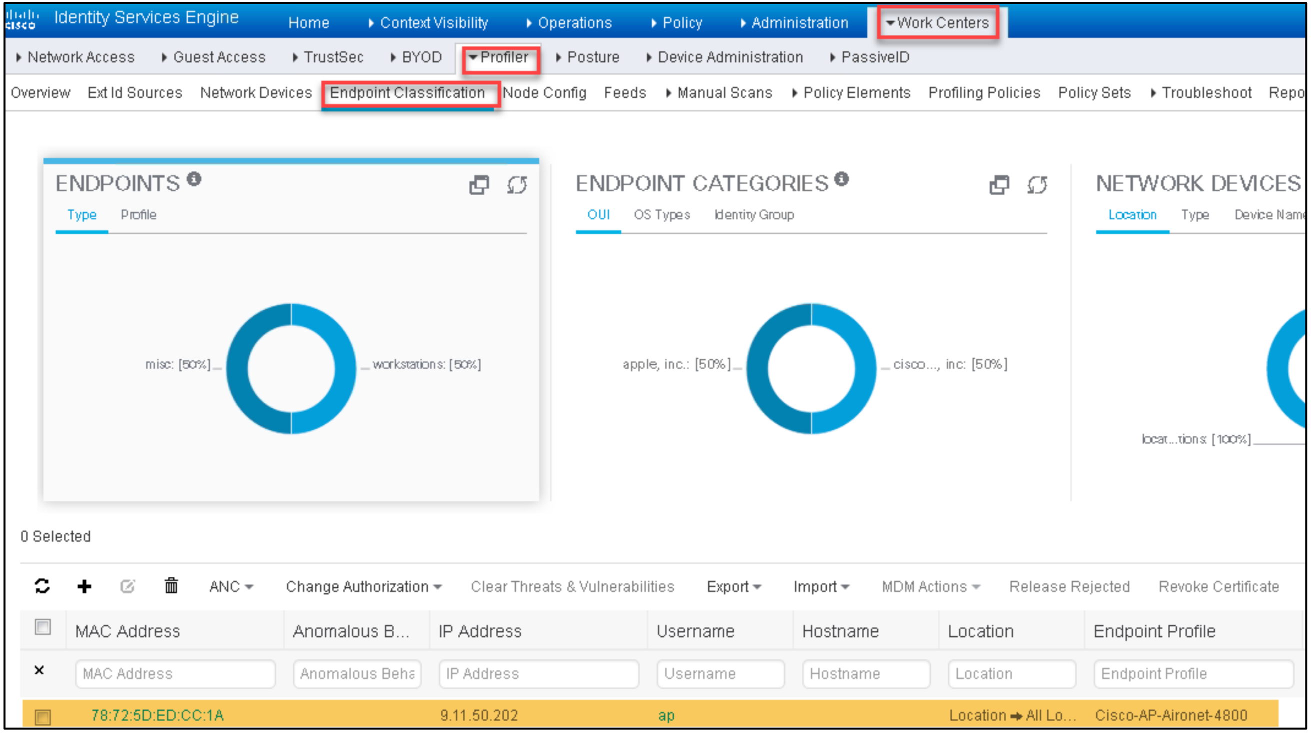
Step 2: Once the port is authorized using MAB. The identity service engine will now profile the endpoint and categorize it as an Access point.
The ISE will initiate a COA to the Fabric edge. The Fabric edge will restart the authentication process.
These steps are highlighted in the ISE policy logs below. The fabric edge will send the profiling information using Radius accounting packets to the Identity Service Engine.

Policy Set on ISE:



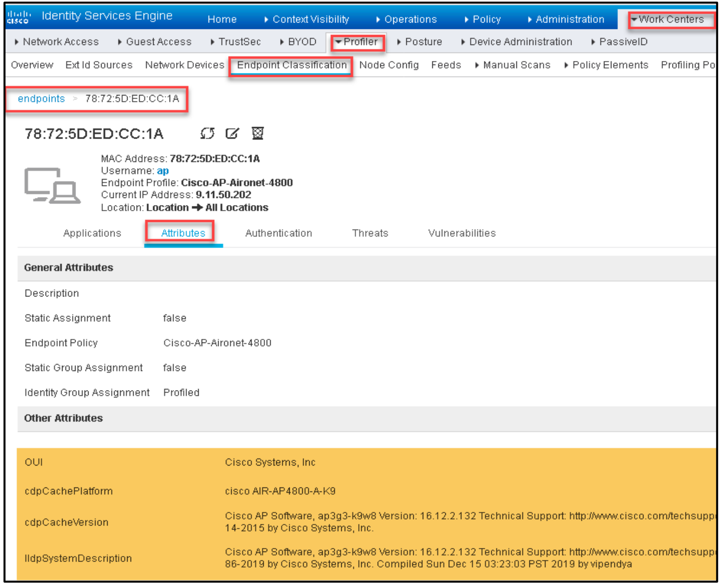
Status	Rule Name	Conditions	Results Profiles	 Security Groups	Hits	Actions
✓	Cisco_AP_Profiling	EndPoints·LogicalProfile **EQUALS** Cisco AP	Ap_template_return_1	Select from list	87	⚙

Profiling information on ISE:



MAC Address	Anomalous B...	IP Address	Username	Hostname	Location	Endpoint Profile
78:72:5D:ED:CC:1A		9.11.50.202	ap		Location ➔ All Lo...	Cisco-AP-Aironet-4800

Profiling data send to the Identity Service Engine(ISE) by the Fabric Edge:



78:72:5D:ED:CC:1A

MAC Address: **78:72:5D:ED:CC:1A**
Username: ap
Endpoint Profile: **Cisco-AP-Aironet-4800**
Current IP Address: **9.11.50.202**
Location: **Location ➔ All Locations**

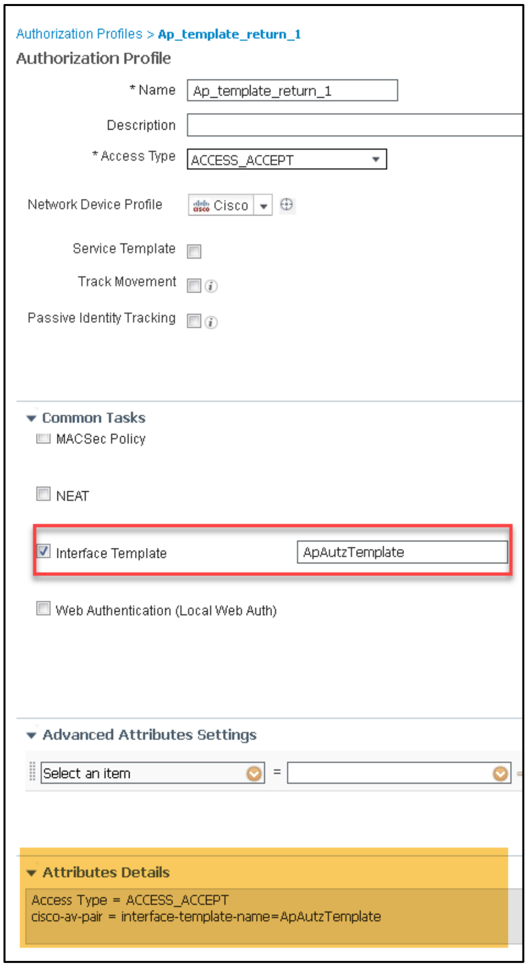
General Attributes

Description	
Static Assignment	false
Endpoint Policy	Cisco-AP-Aironet-4800
Static Group Assignment	false
Identity Group Assignment	Profiled

Other Attributes

OUI	Cisco Systems, Inc
cdpCachePlatform	cisco AIR-AP4800-A-K9
cdpCacheVersion	Cisco AP Software, ap3g3-k9w8 Version: 16.12.2.132 Technical Support: http://www.cisco.com/techsupp 14-2015 by Cisco Systems, Inc.
lldpSystemDescription	Cisco AP Software, ap3g3-k9w8 Version: 16.12.2.132 Technical Support: http://www.cisco.com/techsupp 86-2019 by Cisco Systems, Inc. Compiled Sun Dec 15 03:23:03 PST 2019 by vipendya

Authorization profile for Access point



Authorization Profiles > **Ap_template_return_1**

Authorization Profile

* Name: Ap_template_return_1

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ MACSec Policy

□ NEAT

☑ Interface Template: ApAutzTemplate

□ Web Authentication (Local Web Auth)

Advanced Attributes Settings

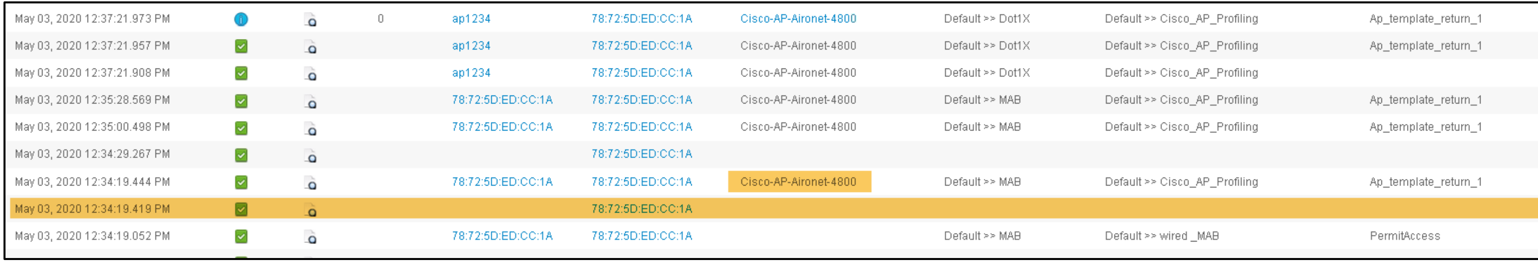
Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=ApAutzTemplate

:

ISE COA and subsequent re-authentication:



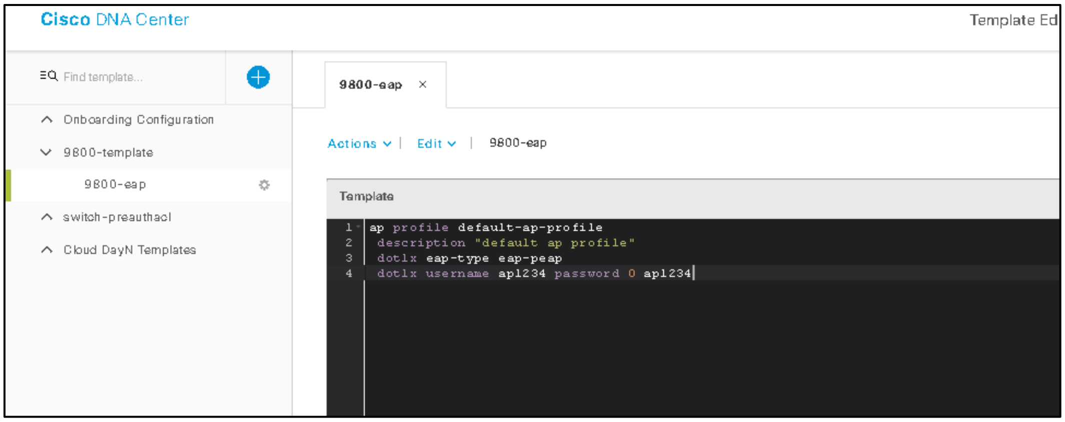
May 03, 2020 12:37:21.973 PM	ⓘ		0	ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.957 PM	✓			ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.908 PM	✓			ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	
May 03, 2020 12:35:28.569 PM	✓			78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM	✓			78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM	✓				78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM	✓			78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM	✓				78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM	✓			78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A		Default >> MAB	Default >> wired _MAB	PermitAccess

Step 3: Once the AP re-authenticates using MAB. The AP will join the Cisco Wireless LAN Controller(WLC) using option 43. The WLC will have the relevant configuration to enable the dot1x supplicant on the Access point. For more information on how to enable dot1x configuration on the Access point, refer to the following URL. The configuration on WLC can be enabled by logging into the WLC or by using templates on Cisco DNA Center.

Enabling Dot1x on AIRE-OS based Wireless LAN Controllers:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_802_1x_eap_supplicant_on_cos_ap.html

Enabling Dot1x on Catalyst 9800 Wireless LAN Controllers:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-1x-support.html

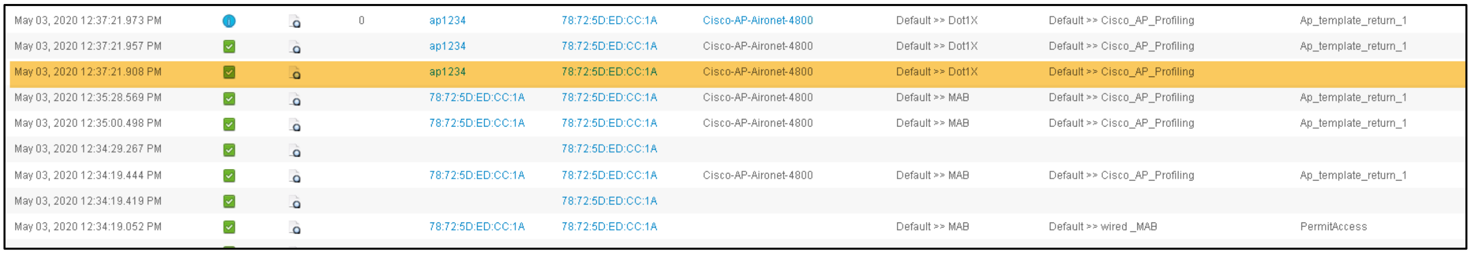
Given below is a screenshot of a sample template for the Catalyst 9800 Wireless LAN Controller, the template shown is for illustration purpose.
Please re-write and modify the template as per the requirements.



```
ap profile default-ap-profile
 description "default ap profile"
 dot1x eap-type eap-peap
 dot1x username ap1234 password 0 ap1234
```

Step 4: The Access point resets and enables the dot1x supplicant and authenticates with the ISE. The ISE as part of the authorization returns the template “ApAutzTemplate” for the fabric edge to assign the right template to the port.

AP resets once dot1x supplicant is enabled and Authenticates with ISE:



May 03, 2020 12:37:21.973 PM	ⓘ	🔍	0	ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.957 PM	✓	🔍		ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:37:21.908 PM	✓	🔍		ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Profiling	
May 03, 2020 12:35:28.569 PM	✓	🔍		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:35:00.498 PM	✓	🔍		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:29.267 PM	✓	🔍			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM	✓	🔍		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> MAB	Default >> Cisco_AP_Profiling	Ap_template_return_1
May 03, 2020 12:34:19.419 PM	✓	🔍			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM	✓	🔍		78:72:5D:ED:CC:1A	78:72:5D:ED:CC:1A		Default >> MAB	Default >> wired _MAB	PermitAccess

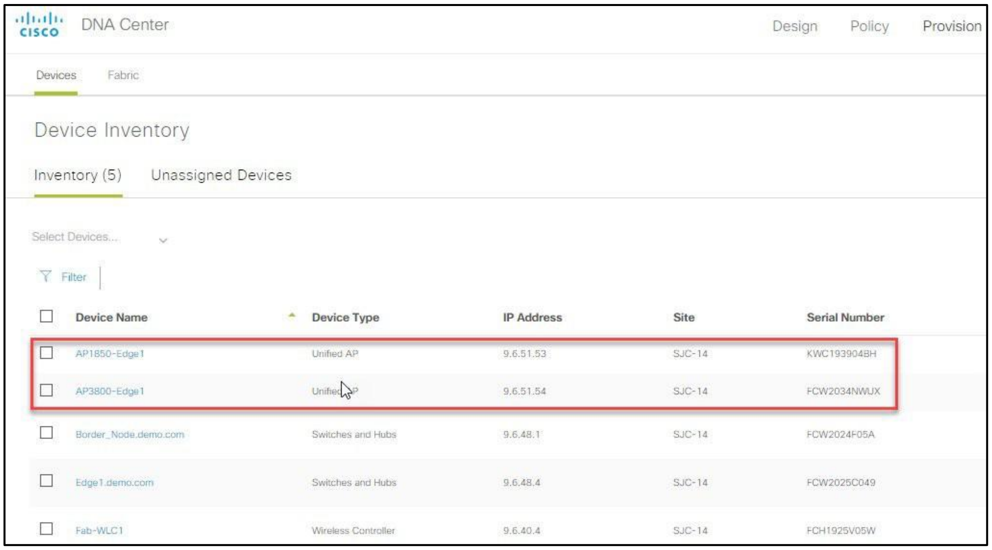
Note: For profiling to happen with much-needed accuracy the profiler feed should be updated to the latest on the Identity service Engine.
A credential needs to be configured on the Identity Service Engine (ISE) to be used by Access Point in the case of EAP-FAST or PEAP.
For EAP-TLS a certificate needs to be pushed to the AP, refer the URL’s in Step 3 on how to push a certificate to the Access Point.

Provisioning the APs

Now that the AP has obtained an IP address and learned the WLC’s management IP address, the AP will join the WLC. Of course, this is assuming that there is IP connectivity between the AP and WLC (this is outside the scope of this document and really depends on where the WLC is connected, usually outside of the fabric). Once the APs are registered to the WLC, they will appear on the Inventory page on Cisco DNA Center.

Procedure

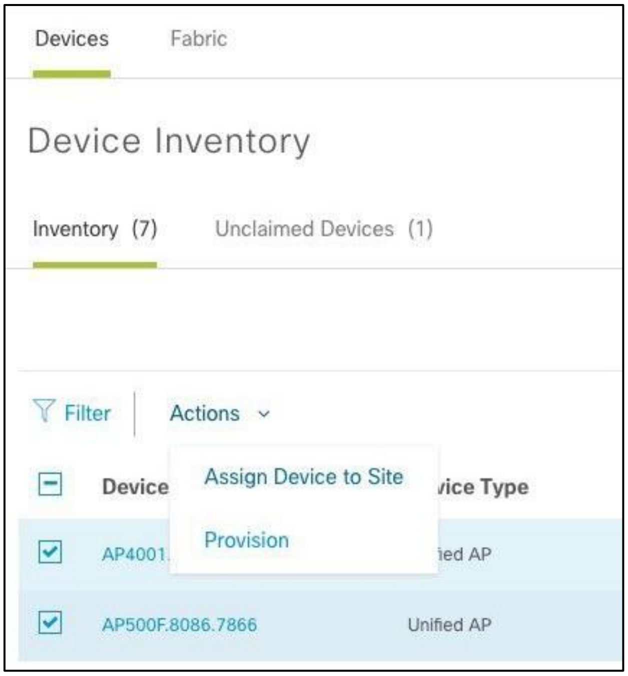
Step 1 Go back to Provision > Devices > Inventory to see the APs joining the fabric-enabled wireless controller.



☐	Device Name	Device Type	IP Address	Site	Serial Number
☐	AP1850-Edge1	Unified AP	9.6.51.53	SJC-14	KWC193904BH
☐	AP3800-Edge1	Unified AP	9.6.51.54	SJC-14	FCW2034NWUX
☐	Border_Node.demo.com	Switches and Hubs	9.6.48.1	SJC-14	FCW2024F05A
☐	Edge1.demo.com	Switches and Hubs	9.6.48.4	SJC-14	FCW2025C049
☐	Fab-WLC1	Wireless Controller	9.6.40.4	SJC-14	FCH1925V05W

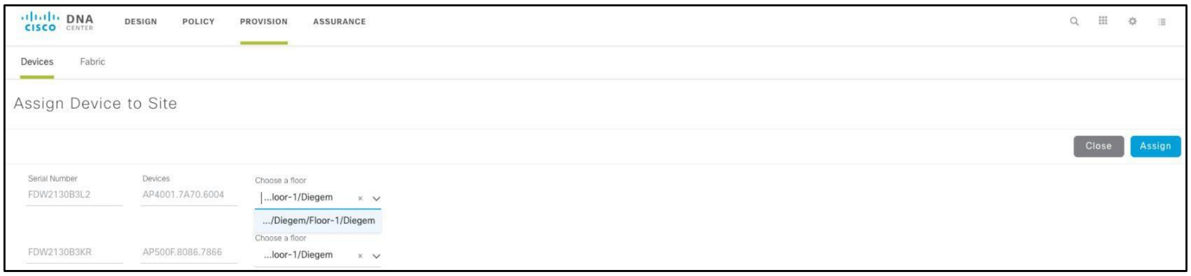
The above screenshot is for illustration purposes only. You may have different 802.11ac Wave 2 access point models in your setup.

Step 2 Select one or more APs from the Device list and choose Assign Device to Site as shown in the example below.



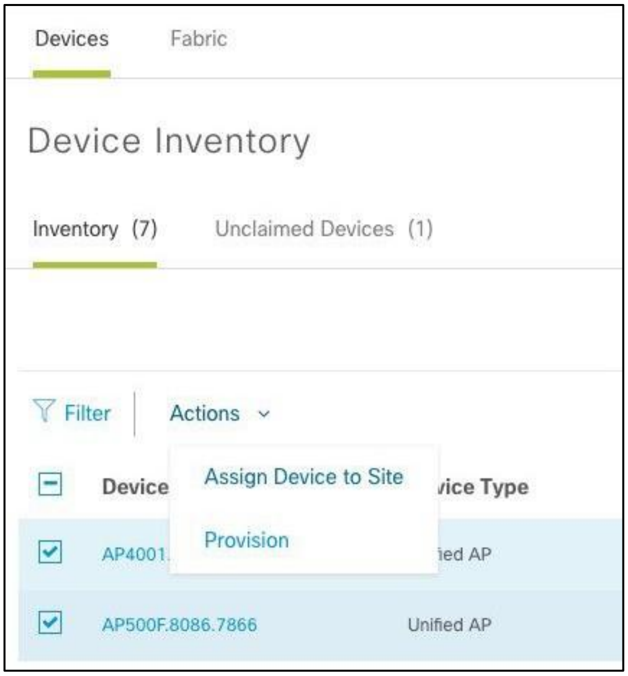
☑	AP4001.	ied AP
☑	AP500F.8086.7866	Unified AP

Choose a floor where the APs will be placed and click Assign. Make sure that the WLC that the APs are registered to has been provisioned to manage that floor. If the floor was added later, you can go back and provision the WLC again to add the specific floor.



Serial Number	Devices	Choose a floor
FDW2130B3L2	AP4001.7A70.6004	...loor-1/Diegem .../Diegem/Floor-1/Diegem
FDW2130B3KR	AP500F.8086.7866	...loor-1/Diegem

Step 3 Next, select one or more APs from the Device list and provision them as shown in the example below. This time, select Provision from the Actions menu.

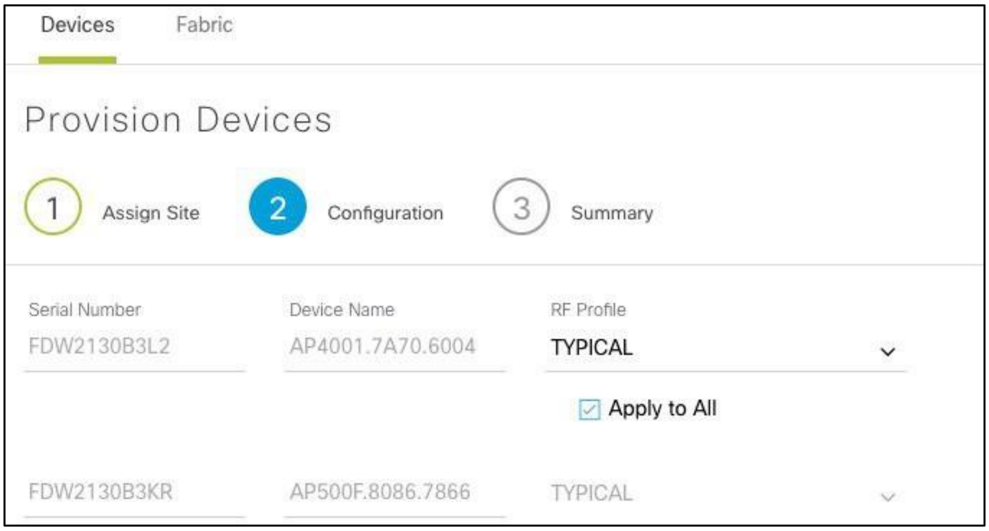


Device	ice Type
☑ AP4001.	ied AP
☑ AP500F.8086.7866	Unified AP

Choose a floor or just click Next if already selected.

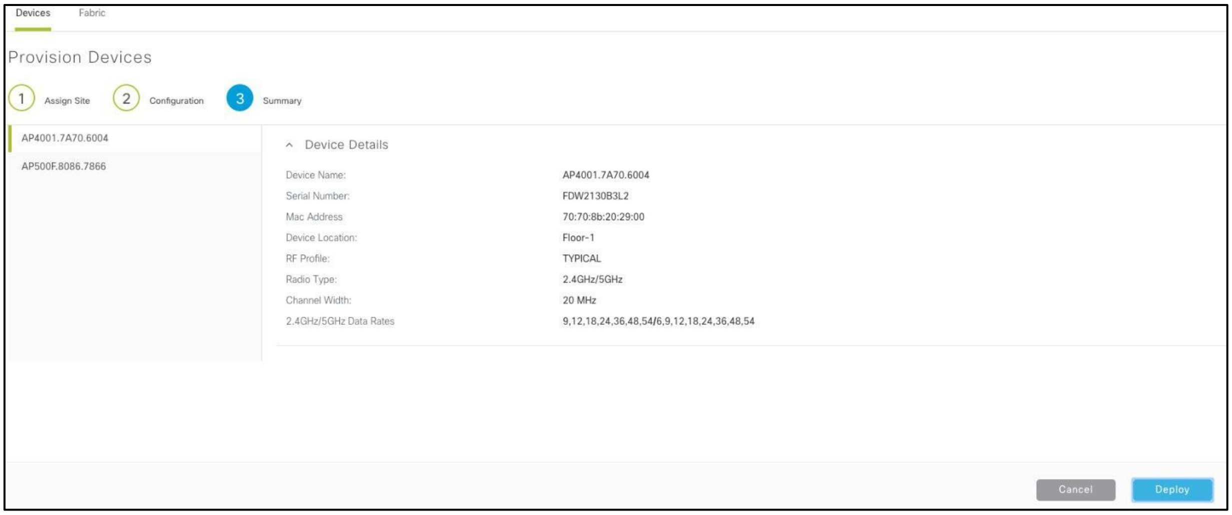
Note You can select Apply to All for the site to be mapped to all devices.

Step 4 For the RF profile for the AP, choose from High, Typical, or Low or a customized one defined previously. In the example below, we have selected Typical and clicked Next.



Serial Number	Device Name	RF Profile
FDW2130B3L2	AP4001.7A70.6004	TYPICAL ☑ Apply to All
FDW2130B3KR	AP500F.8086.7866	TYPICAL

Step 5 Click Deploy, and as a part of AP provisioning, the configuration will be pushed to the AP, as shown below. The AP will reboot and rejoin the WLC

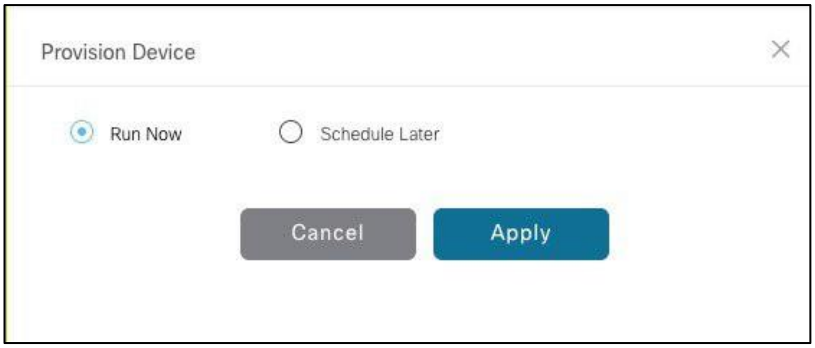


Provision Devices

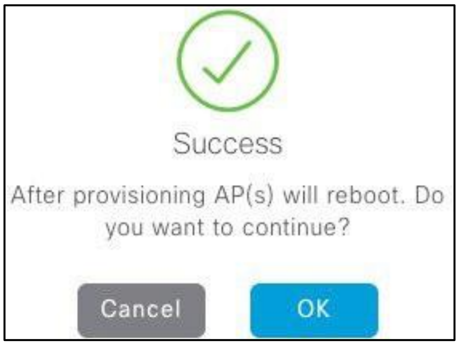
Device Details

Device Name:	AP4001.7A70.6004
Serial Number:	FDW2130B3L2
Mac Address	70:70:8b:20:29:00
Device Location:	Floor-1
RF Profile:	TYPICAL
Radio Type:	2.4GHz/5GHz
Channel Width:	20 MHz
2.4GHz/5GHz Data Rates	9,12,18,24,36,48,54/6,9,12,18,24,36,48,54

Click Run Now in the window that pops up.

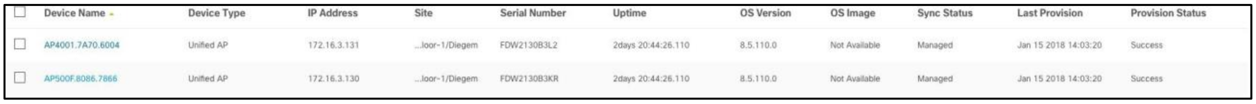

Provision Device

A message appears warning you that the APs will reboot. Click OK.


Success

After provisioning AP(s) will reboot. Do you want to continue?

Step 6 You will now see the Provision Status for the AP listed as "Success."

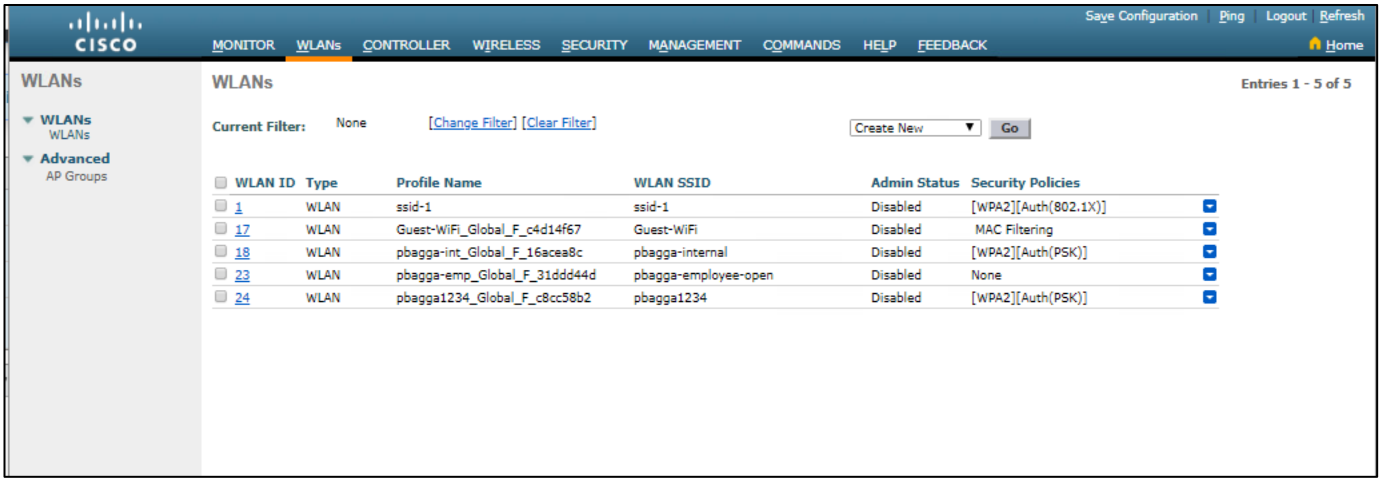


□	Device Name	Device Type	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
□	AP4001.7A70.6004	Unified AP	172.16.3.131	...loor-1/Diegem	FDW2130B3L2	2days 20:44:26.110	8.5.110.0	Not Available	Managed	Jan 15 2018 14:03:20	Success
□	AP500F.8086.7866	Unified AP	172.16.3.130	...loor-1/Diegem	FDW2130B3KR	2days 20:44:26.110	8.5.110.0	Not Available	Managed	Jan 15 2018 14:03:20	Success

Note: The above screenshot is for illustration purposes only. The AP deployment details may be different in your setup.

Step 7 As part of AP provisioning, some configuration is pushed on the WLC.

An AP group will be created with the name of the site it was mapped to (step 3 above).



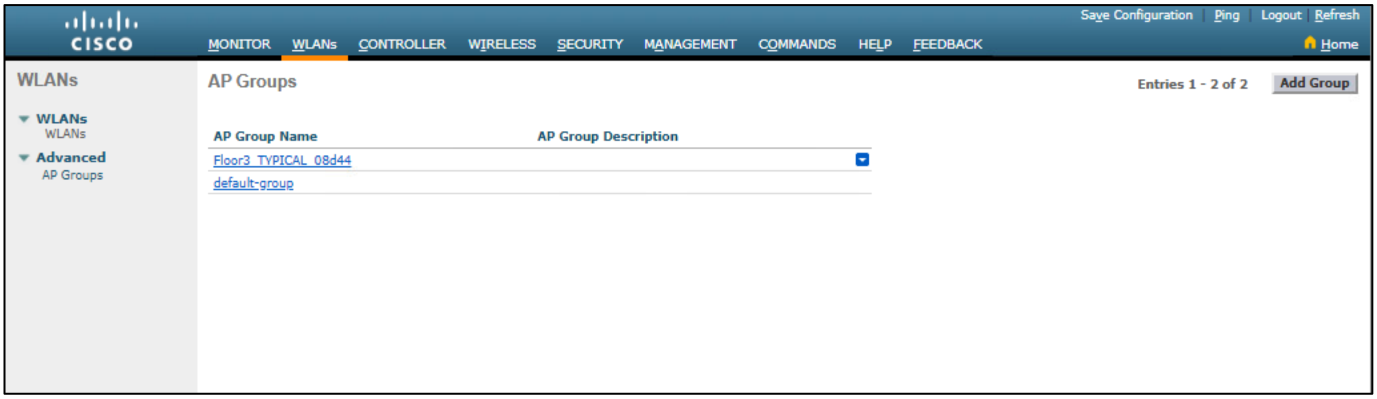
WLANs

Entries 1 - 5 of 5

Current Filter: None [Change Filter] [Clear Filter]

□	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□	1	WLAN	ssid-1	ssid-1	Disabled	[WPA2][Auth(802.1X)]
□	17	WLAN	Guest-WiFi_Global_F_c4d14f67	Guest-WiFi	Disabled	MAC Filtering
□	18	WLAN	pbagga-int_Global_F_16acea8c	pbagga-internal	Disabled	[WPA2][Auth(PSK)]
□	23	WLAN	pbagga-emp_Global_F_31ddd44d	pbagga-employee-open	Disabled	None
□	24	WLAN	pbagga1234_Global_F_c8cc58b2	pbagga1234	Disabled	[WPA2][Auth(PSK)]

APs and WLANs will be part of that AP group, as shown in the example below.



AP Groups

Entries 1 - 2 of 2

AP Group Name	AP Group Description
Floor3_TYPICAL_08d44	
default-group	

In case of Catalyst 9800 WLC, three tags are assigned to an Access Point:

Site Tag: A site tag contains the Ap join profile characteristics such as CAPWAP timers, AP username, and password.

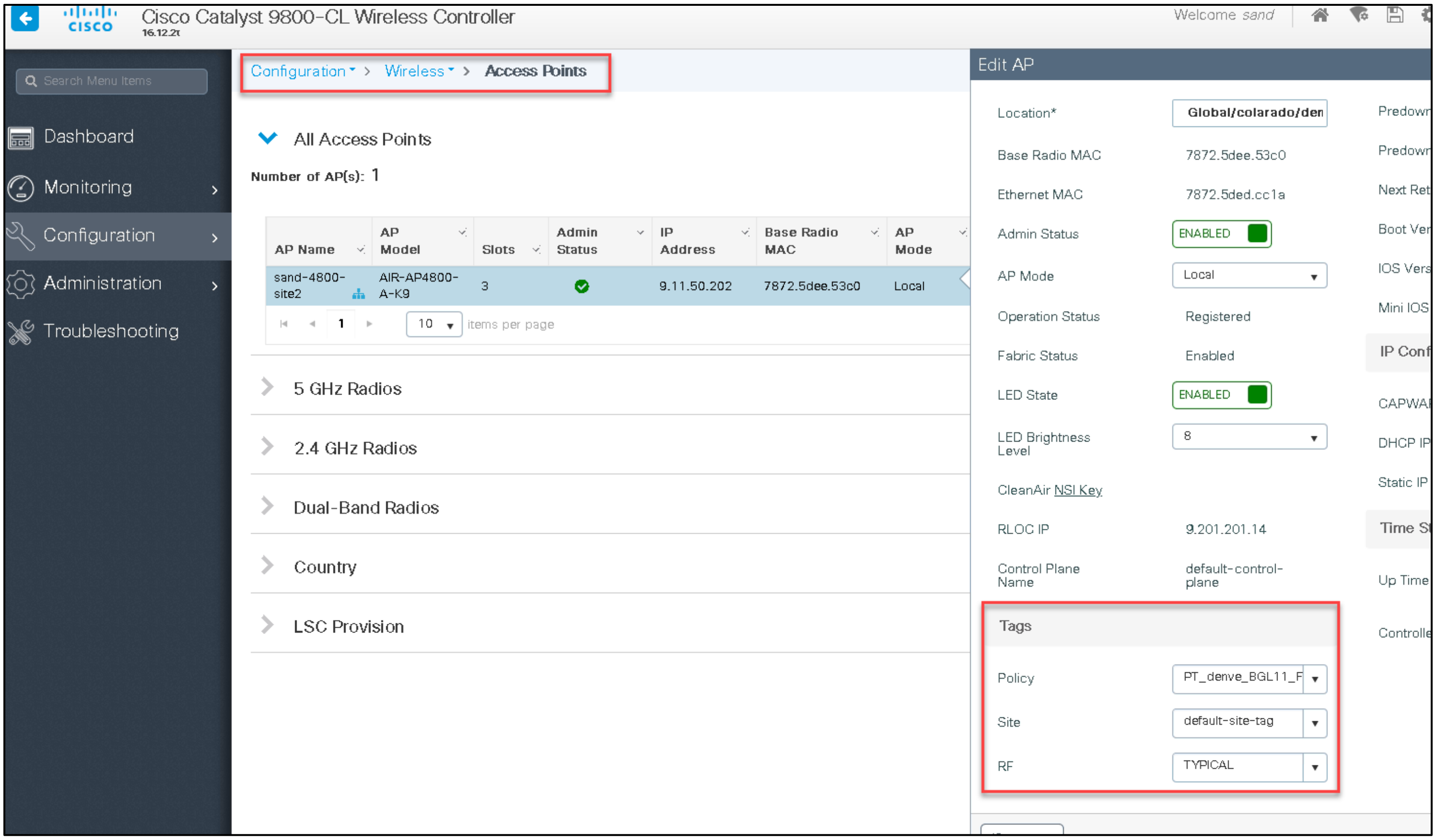
RF Tag: The RF tag contains the RF profile characteristics assigned.

Policy Tag: The Policy tag contains the WLAN and policy profile mapping.

For more information on the usage of tags, refer the URL below to understand the config model on Catalyst 9800:

Understand Catalyst 9800 Wireless Controller Configuration Model:

Tags Assigned to the Access Point:



Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode
sand-4800-site2	AIR-AP4800-A-K9	3	✓	9.11.50.202	7872.5dee.53c0	Local

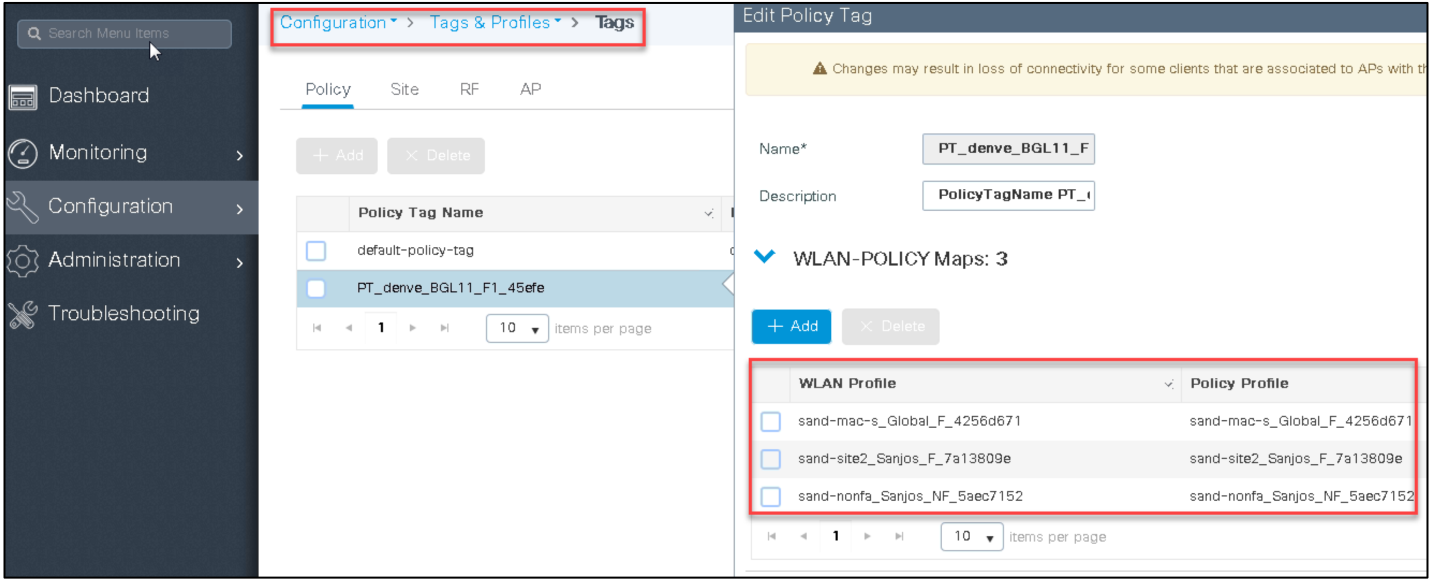
1 | 10 items per page

Location*	Global/colarado/den
Base Radio MAC	7872.5dee.53c0
Ethernet MAC	7872.5ded.cc1a
Admin Status	ENABLED
AP Mode	Local
Operation Status	Registered
Fabric Status	Enabled
LED State	ENABLED
LED Brightness Level	8
CleanAir NSI Key	
RLOC IP	9.201.201.14
Control Plane Name	default-control-plane

Tags

Policy	PT_denve_BGL11_F
Site	default-site-tag
RF	TYPICAL

Details of Policy Tag:



Policy Tag Name
default-policy-tag
PT_denve_BGL11_F1_45efe

1 | 10 items per page

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with th

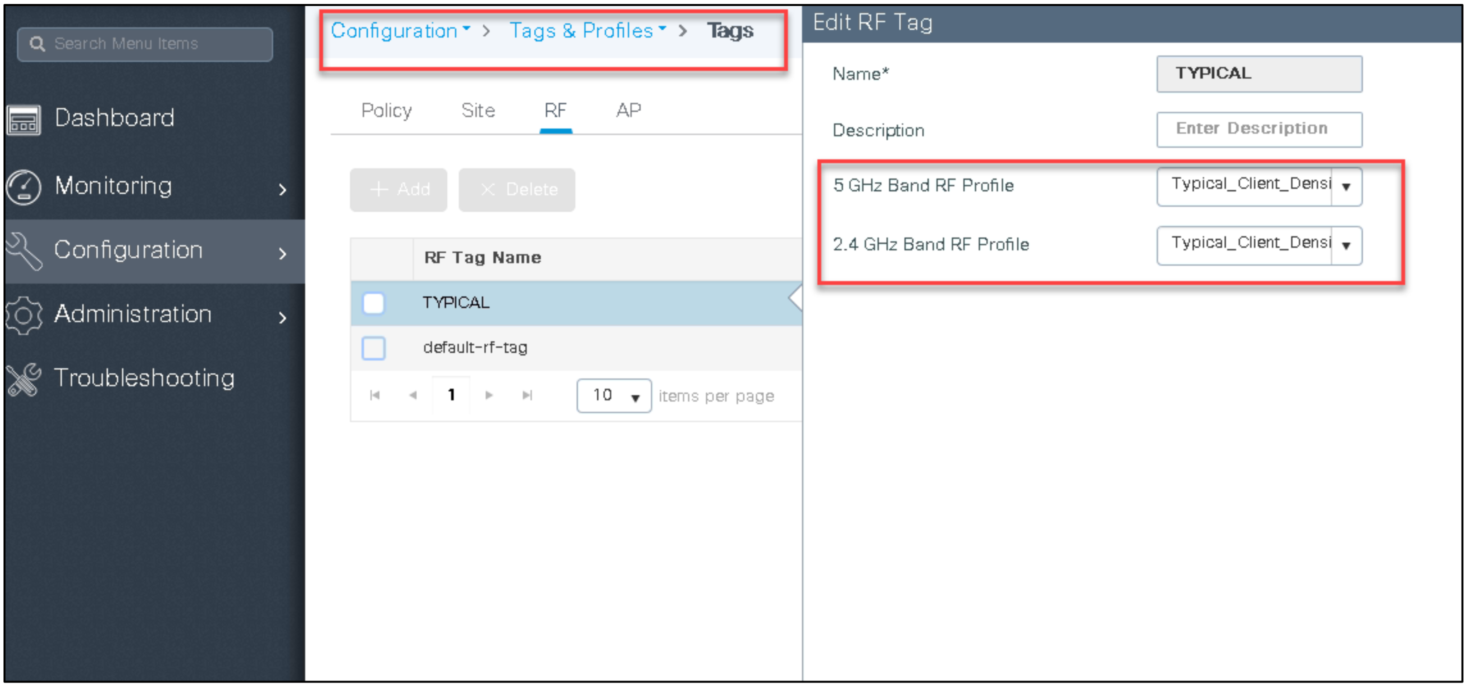
Name*	PT_denve_BGL11_F
Description	PolicyTagName PT_(

WLAN-POLICY Maps: 3

WLAN Profile	Policy Profile
sand-mac-s_Global_F_4256d671	sand-mac-s_Global_F_4256d671
sand-site2_Sanjos_F_7a13809e	sand-site2_Sanjos_F_7a13809e
sand-nonfa_Sanjos_NF_5aec7152	sand-nonfa_Sanjos_NF_5aec7152

1 | 10 items per page

Details of RF tag:

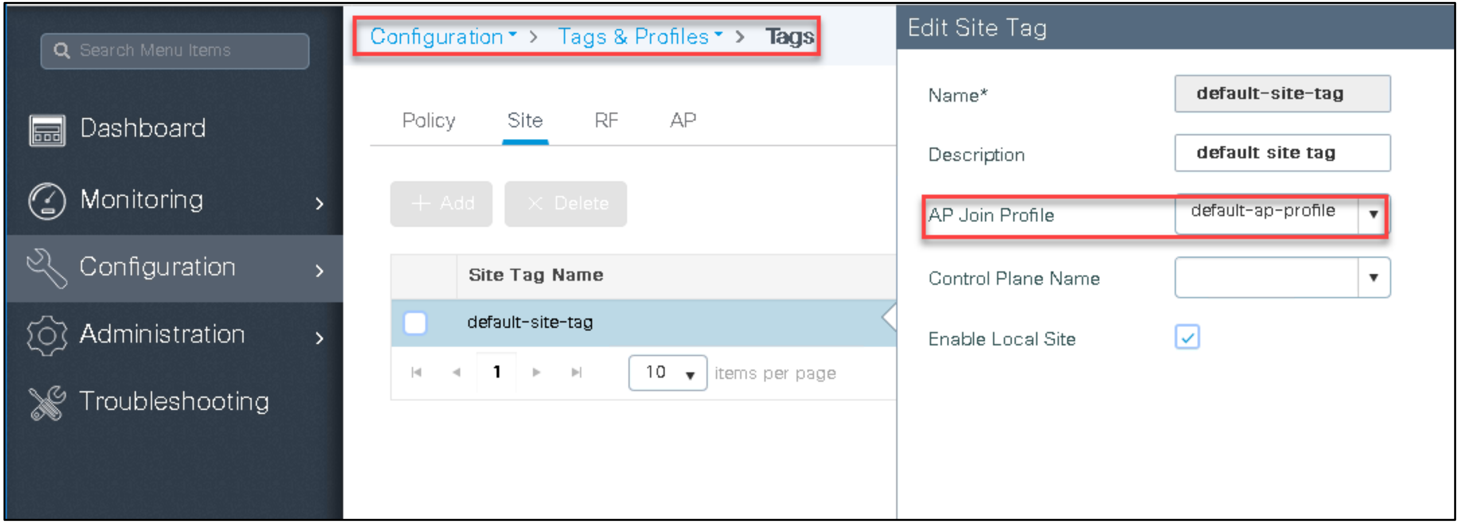


	RF Tag Name
□	TYPICAL
□	default-rf-tag

Edit RF Tag

Name*	TYPICAL
Description	Enter Description
5 GHz Band RF Profile	Typical_Client_Densi
2.4 GHz Band RF Profile	Typical_Client_Densi

Details of the Site tag:



	Site Tag Name
□	default-site-tag

Edit Site Tag

Name*	default-site-tag
Description	default site tag
AP Join Profile	default-ap-profile
Control Plane Name	
Enable Local Site	☑

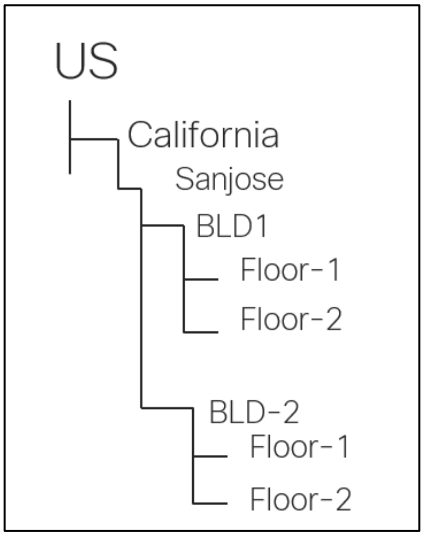
Site tag Provisioning on C9800.

Auto-generated Site tag:

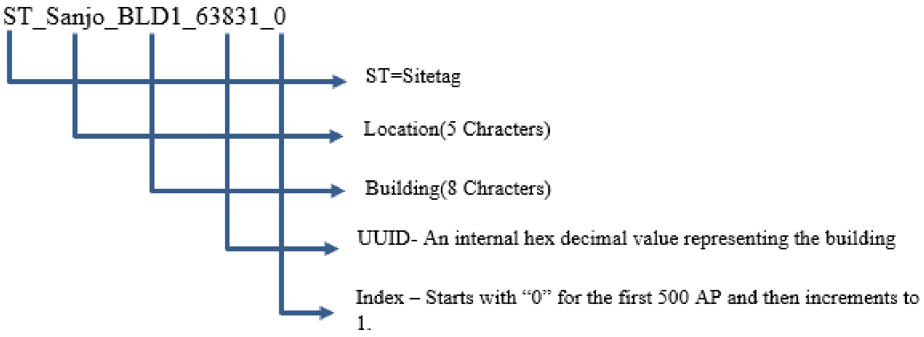
The Cisco DNAC has introduced the use of a custom site tag starting from 2.1.1.x release. The site tag is a way of grouping Access points on the Cisco Catalyst 9800 WLC. A site tag represents a roaming domain in wireless. Creating multiple site tags helps the WLC to load balance access points to internal processes within the system. Having a custom site tag helps an administrator to have more granular control on how the AP's are grouped when provisioned by the Cisco DNAC. In this section, we will discuss how the DNAC provisions a site tag and how to create a custom site tag and have that provisioned on the Cisco WLC. The auto-generated site tag by the Cisco DNAC is created at a building level and all the floors under the building inherit the same site tag. The Access points are provisioned to the multiple floors of the same building will inherit the same site tag.

The Cisco DNAC uses the following format internally to generate the respective site tag:-
ST_<location>_<building_name>_<building_UUID>_<index>

Let's take an example to understand the auto-generated site tag created, a sample network hierarchy shown below is used to understand how the Cisco DNAC derives the site tag.



Assuming the fabric site is created at the root level which in this case is the global location “US” and an Access point provisioned to the location “Building-1/Floor-1” or “building-1/Floor-2” will inherit the following site tag.


ST_Sanjo_BLD1_63831_0
ST=Sitetag
Location(5 Chracters)
Building(8 Chracters)
UUID- An internal hex decimal value representing the building
Index – Starts with “0” for the first 500 AP and then increments to 1.

If the Access point is provisioned to “Building-2/floor-1 or floor-2”. The following site tag would be auto-generated by the Cisco DNAC.

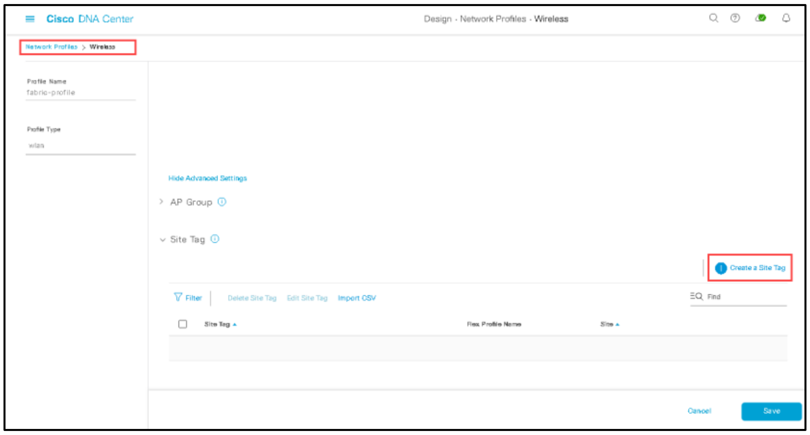
ST_Sanjo_BLD2_45121_0

A single tag can accommodate about 500 AP, if the number of AP’s exceeds the 500 AP limit then the index is incremented and a new site tag is created.

Custom Site tag:

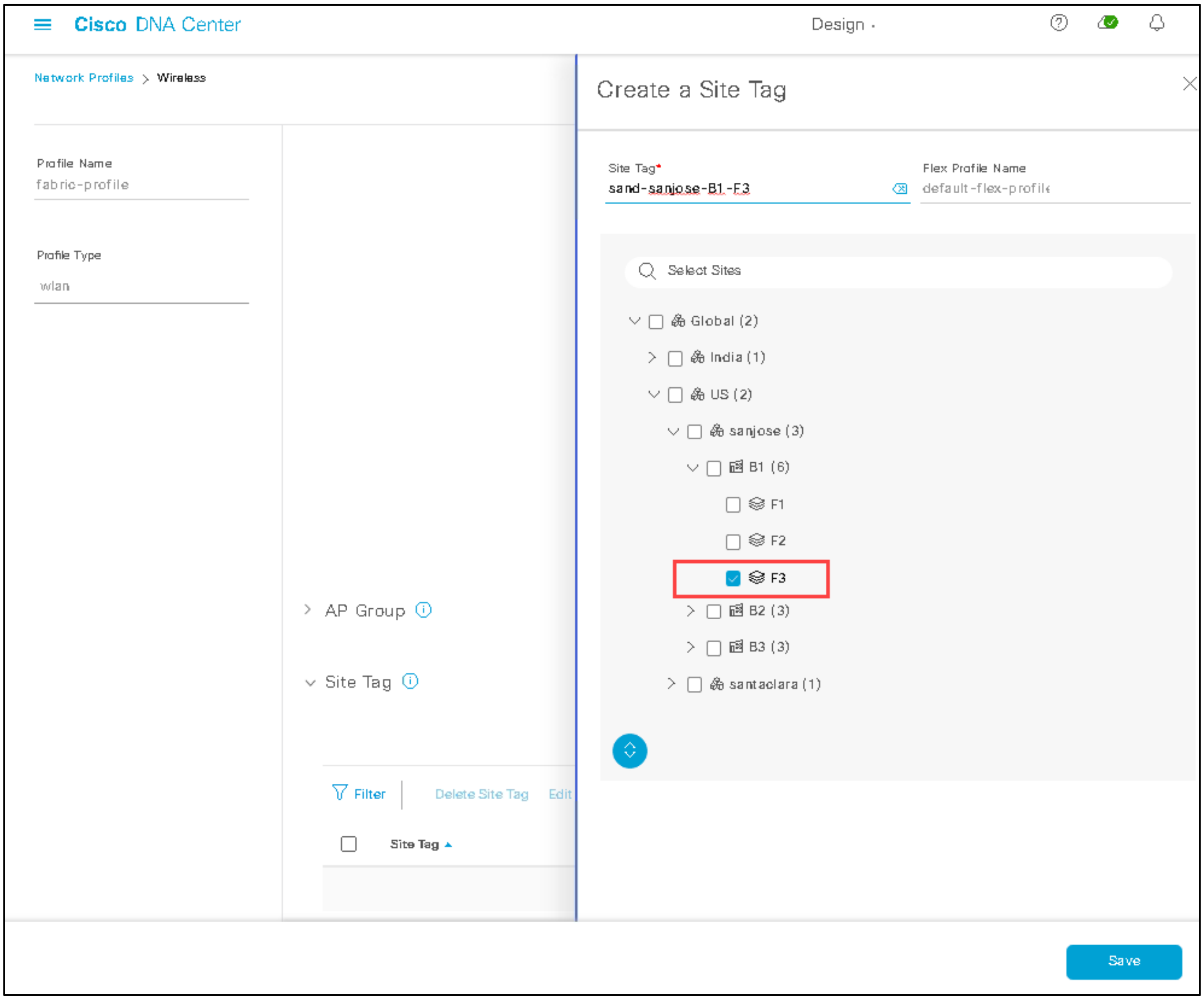
A custom site tag allows an administrator to group access points on a per floor or a building level and create a roaming domain. The auto-generated site tag by Cisco DNAC is created at a building level while a custom site allows the tag to be mapped over to a building or on a per floor level.

The custom site tag association with the floor/building is done on the wireless profile. If a custom site tag is mapped to a floor, all the Access points on that floor would be assigned the respective site tag, while the other floors in the building would be mapped to the auto-generated site tag created by the Cisco DNAC.



Profile Name
fabric-profile

Profile Type
wlan



Profile Name: fabric-profile

Profile Type: wlan

Site Tag*: sand-sanjose-B1-F3

Flex Profile Name: default-flex-profile

☑ F3

To verify the site tag on the Catalyst 9800 WLC, login to the CLI of the WLC and issue the following CLI:

```
9800-1#sh wireless tag site summary

Number of Site Tags: 6

Site Tag Name                     Description
------------------------------------------------------------------------
default-site-tag                  default site tag  ← Default site tag on the system
sand-sanjose-B1-F3                Site Tag sand-sanjose-B1-F3 ← Custom site tag
ST_sanjo_B1_a42cc_0               Site Tag ST_sanjo_B1_a42cc_0 ← auto-generated site tag-cisco DNAC
ST_sanjo_B2_1fe90_0               Site Tag ST_sanjo_B2_1fe90_0
ST_sanjo_B3_61190_0               Site Tag ST_sanjo_B3_61190_0
```

```
9800-1#sh ap tag summary
Number of APs: 6
```

```
AP Name                 AP Mac           Site Tag Name                      Policy Tag Name                   RF
Tag Name                       Misconfigured    Tag Source
-----------------------------------------------------------------------------------------------------------------
------------------------------------------------------------
sand-3800-fe2-gi-1-0-2  00f6.636f.9282   sand-sanjose-B1-F3                 PT_sanjo_B1_F3_8cd9e
TYPICAL                           No               Static
sand-3800-fe2-gi-1-0-7  cc16.7e98.79a6   ST_sanjo_B1_a42cc_0                PT_sanjo_B1_F3_8cd9e
TYPICAL                           No               Static
sand-4800-wol           7872.5ded.caa6   ST_sanjo_B2_1fe90_0                PT_sanjo_B2_F2_2be9a
TYPICAL                           No               Static
sand-4800-9300ER-tw-1-  7872.5ded.cc1a   sand-sanjose-B1-F3                 PT_sanjo_B1_F2_3d612
TYPICAL                           No               Static
sand-3800-fe-1          00f6.6373.879a   ST_sanjo_B2_1fe90_0                PT_sanjo_B2_F3_cb741
TYPICAL                           No               Static
sand-3800-wol-nei       00f6.6373.87c2   ST_sanjo_B3_61190_0                PT_sanjo_B3_F3_a0127
TYPICAL                           No               Static
```

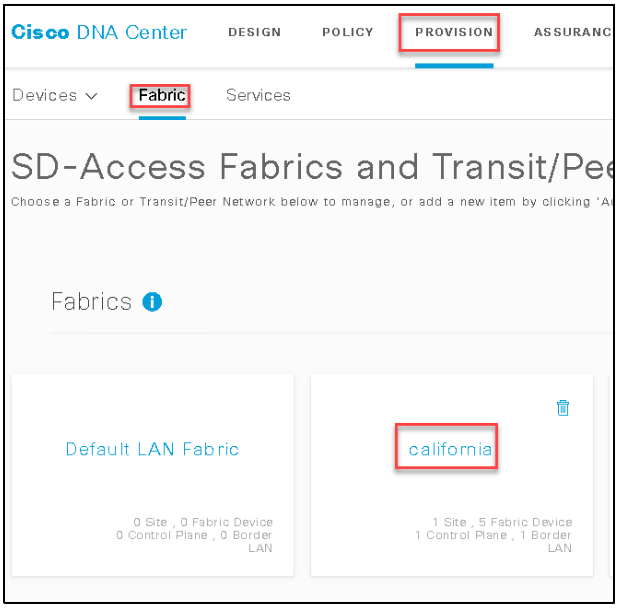
Onboarding clients

Now we need to assign IP pools to wireless clients and SSIDs to enable clients to join the wireless network.

Procedure

Step From the Cisco DNA Center home page. Navigate to **Provision > Fabric.**

In this example, we are editing the fabric by the name “California”. It is assumed that the fabric has a control plane and border already configuration. the Section will focus on how to add a Wireless Lan controller to the fabric and enable host onboarding for a wireless client.

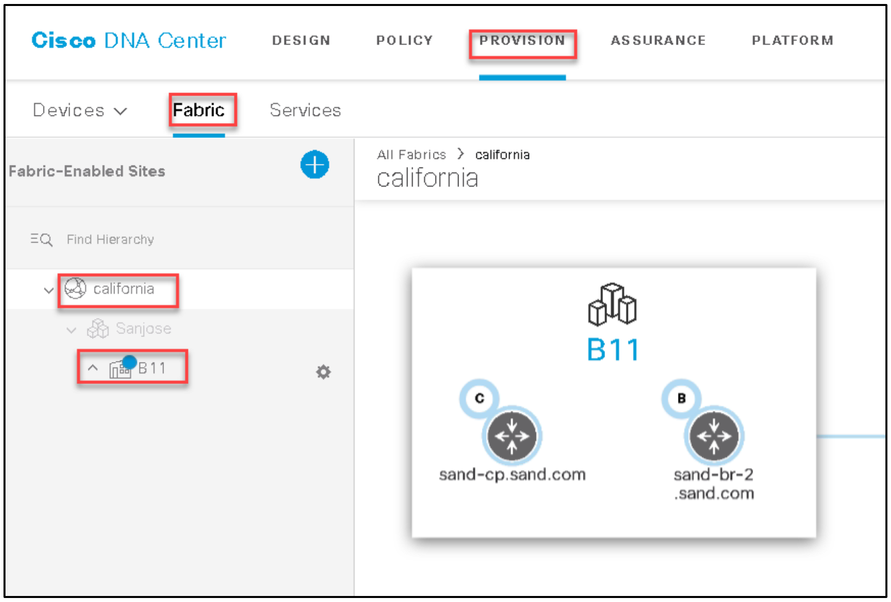


SD-Access Fabrics and Transit/Pee

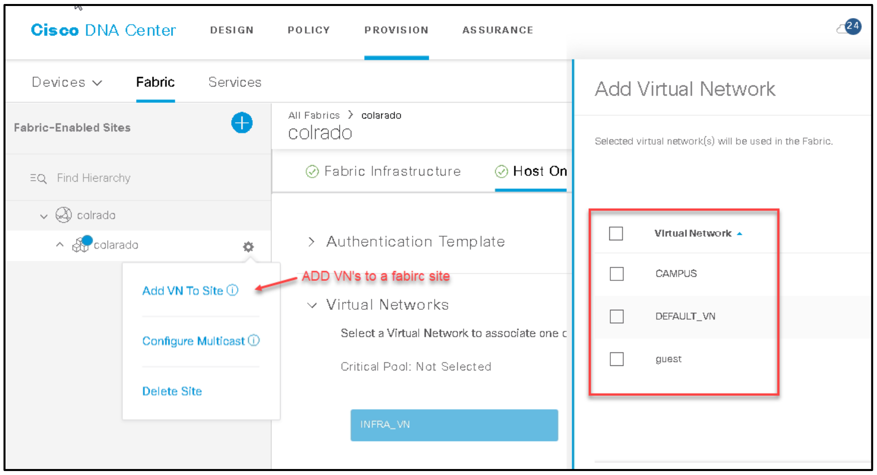
Choose a Fabric or Transit/Peer Network below to manage, or add a new item by clicking 'A

Default LAN Fabric: 0 Site , 0 Fabric Device 0 Control Plane , 0 Border LAN

california: 1 Site , 5 Fabric Device 1 Control Plane , 1 Border LAN

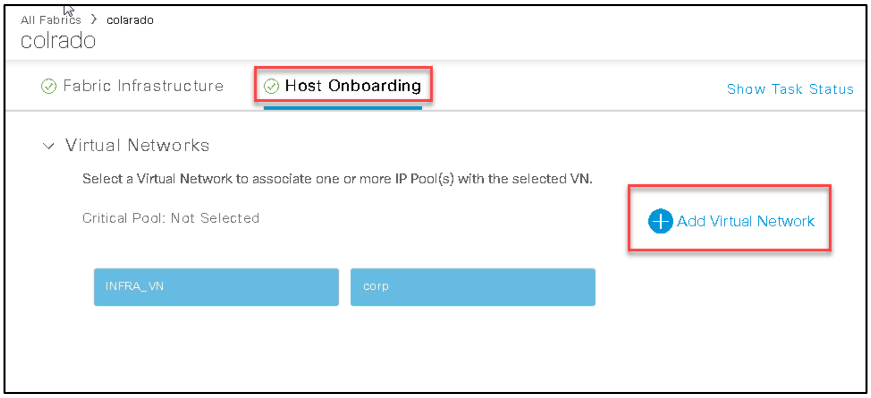


Step 2 With Cisco DNAC 1.3.3 if a new VN is created, it needs to be manually added to a fabric. For migration to 1.3.3 all the VN's that existed on the previous version would be available on the host onboarding page. If the VN' are not available on the host onboarding page, click on the "Gear" icon next to the site to add a VN in the Fabric. Alternatively, add a VN from the host onboarding page. Ensure that the new VN that is added has a handoff configured from the Fabric border.



Select a Virtual Network to associate one c

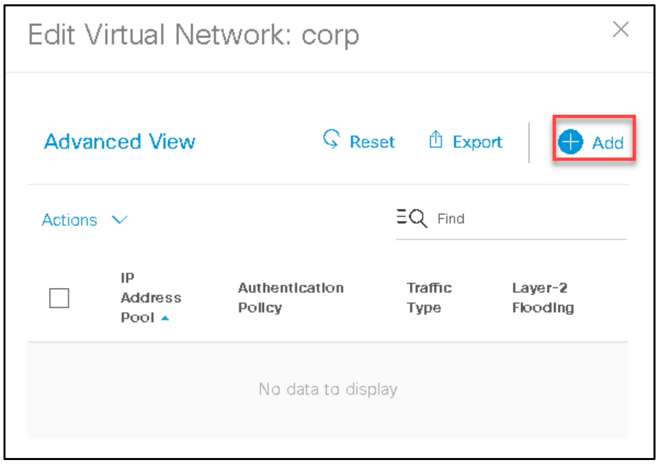
Selected virtual network(s) will be used in the Fabric.

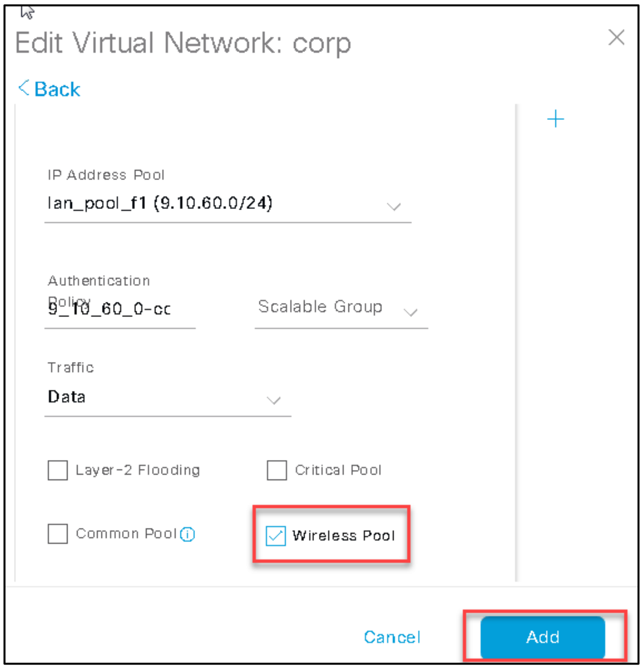


Select a Virtual Network to associate one or more IP Pool(s) with the selected VN.

Step 3 Once the Virtual Networks are added to a site. An IP pool needs to be associated with the VN to be used by the clients in the fabric. Click on the VN (corp in the example below) and, from the available address pools, select the address pool for wireless clients.

IMPORTANT: Enable the option wireless pool if the wireless clients need to use the pool.





Edit Virtual Network: corp

< Back

IP Address Pool
lan_pool_f1 (9.10.60.0/24)

Authentication Policy
9_10_60_0-cc

Scalable Group

Traffic
Data

□ Layer-2 Flooding □ Critical Pool

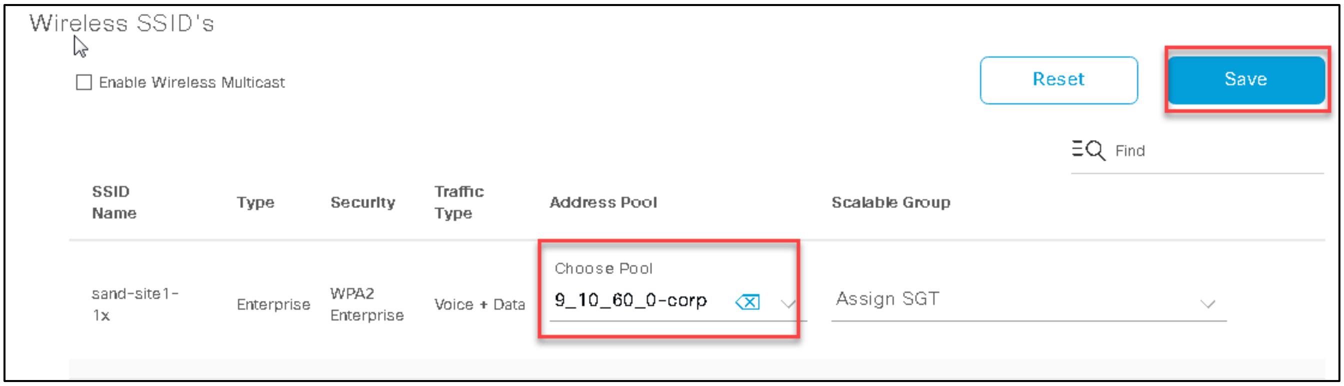
□ Common Pool ☑ Wireless Pool

Click add to associate the pool to a VN. The traffic type option (Data or Data + Voice) is relevant only for wired clients. The correspondent settings for wireless clients are done at the SSID level.

By default starting from Cisco DNA Center 1.3 an administrator would need to enable the "Wireless pool" option to push the pool to a Wireless LAN Controller(WLC).
This was done to optimize the layer 2 VNID provisioned on the Cisco WLC. A pool that doesn't have a wireless pool option enabled will not be provisioned on the WLC with the respective layer 2 VNID.

Note: If using VNID override as part of client authorization, please ensure that the override pool has the "Wireless pool" option enabled.

Step 4 Associate the SSID with the pool that you configured earlier (optionally you can also associate an SGT to be assigned to all clients joining this SSID).



Wireless SSID's

□ Enable Wireless Multicast

SSID Name	Type	Security	Traffic Type	Address Pool	Scalable Group
sand-site1-1x	Enterprise	WPA2 Enterprise	Voice + Data	Choose Pool 9_10_60_0-corp	Assign SGT

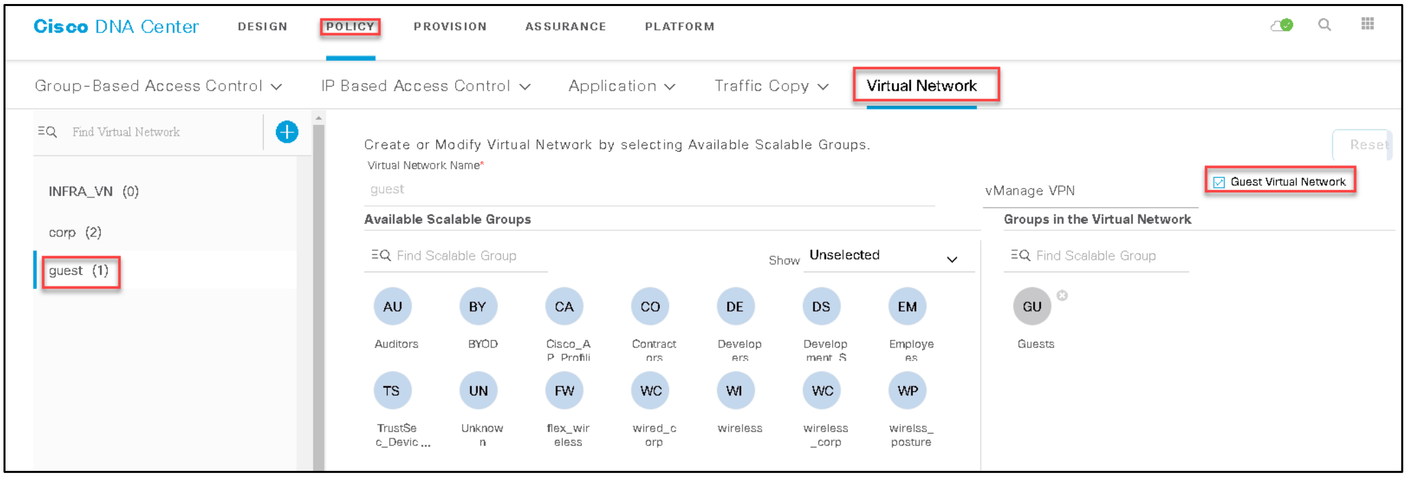
Onboarding guest clients

For the guest SSID, you have two implementation choices (the different available designs are presented in more details later, in the Guest Design section):

1. Use the same enterprise guest CP node for guest traffic: The guest SSID is associated with a dedicated guest VN in the fabric and uses fabric segmentation (VNI, SGT) to isolate guest traffic.
2. Dedicated a guest control plane and border for guest traffic.

In both cases, before configuring the SSID, you need to mark the VN as being guest enabled. This tells Cisco DNA Center that this is a "special" VN that needs to be configured accordingly.

Go to **Policy** > **Virtual Networks** and create a new VN. Check the Guest Virtual Network checkbox as shown below, and add the scalable groups that belong to this virtual network.

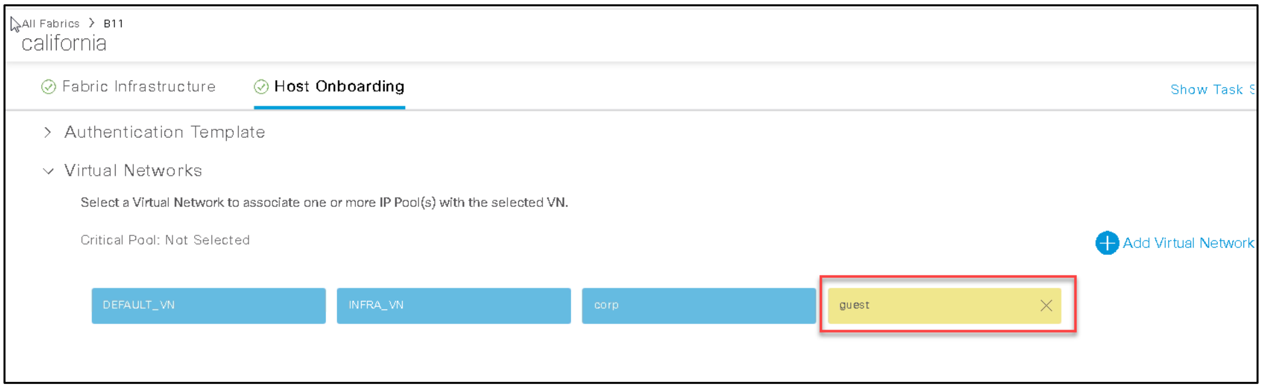


Virtual Network Name* guest

☑ Guest Virtual Network

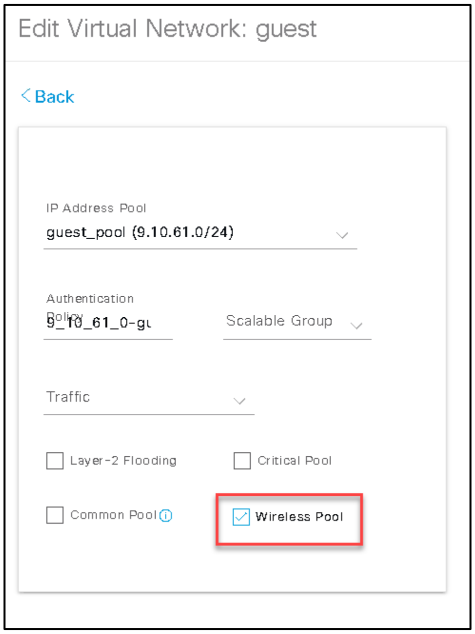
Refer step no:2 in the client onboarding section to add the VN to a site.

Now you can configure the SSID in the onboarding session. For the common control-plane node, the procedure is the same as for any other SSID configuration: simply click on the VN you are using for guest clients, and from the available address pools, select the address pool for wireless clients. Click Update. See the example below.



Select a Virtual Network to associate one or more IP Pool(s) with the selected VN.

Critical Pool: Not Selected



IP Address Pool: guest_pool (9.10.61.0/24)

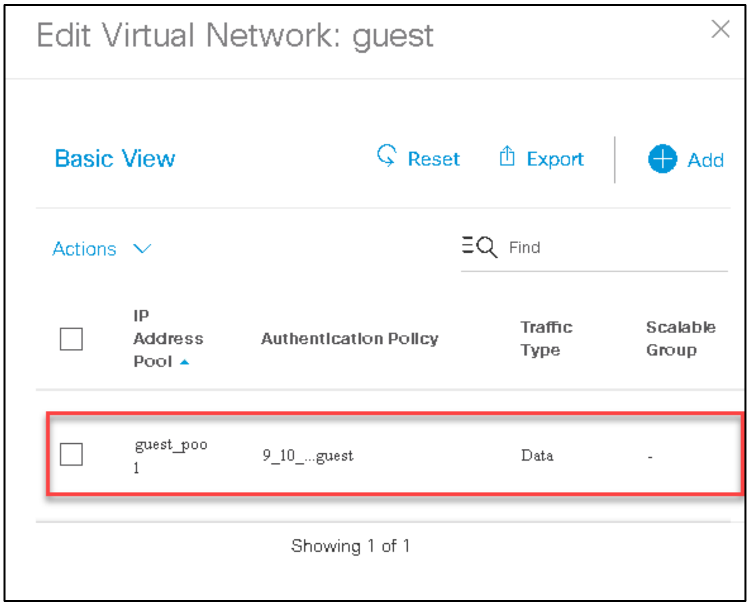
Authentication Policy: 9_10_61_0-gu

Scalable Group

Traffic

☐ Layer-2 Flooding ☐ Critical Pool

☐ Common Pool ☑ Wireless Pool

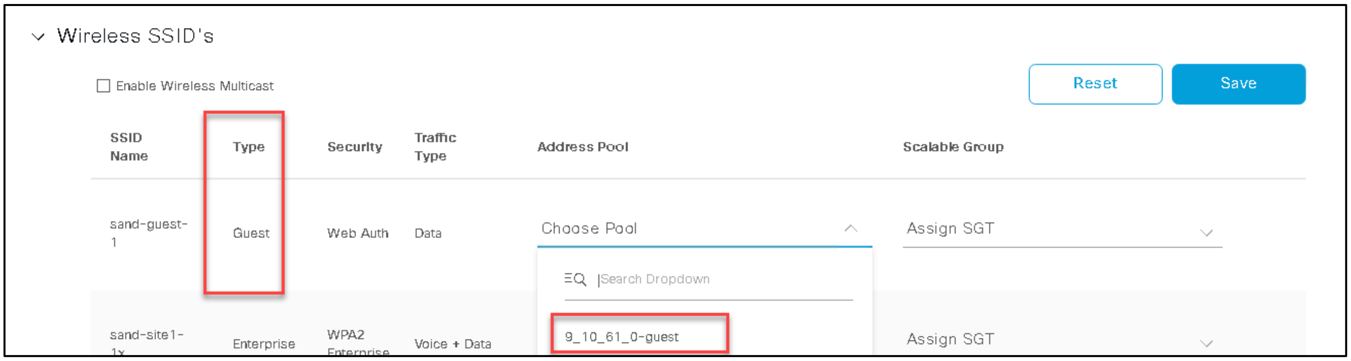


	IP Address Pool	Authentication Policy	Traffic Type	Scalable Group
☐	guest_pool	9_10_...guest	Data	-

Showing 1 of 1

From DNAC 1.3, we must click on the “Wireless Pool” checkbox to be able to associate this IP Pool to Wireless SSID in Wireless SSID’s subsection.

Then associate the guest SSID with the pool and click Save, as you did in step 4 for the regular enterprise SSID.



Wireless SSID's

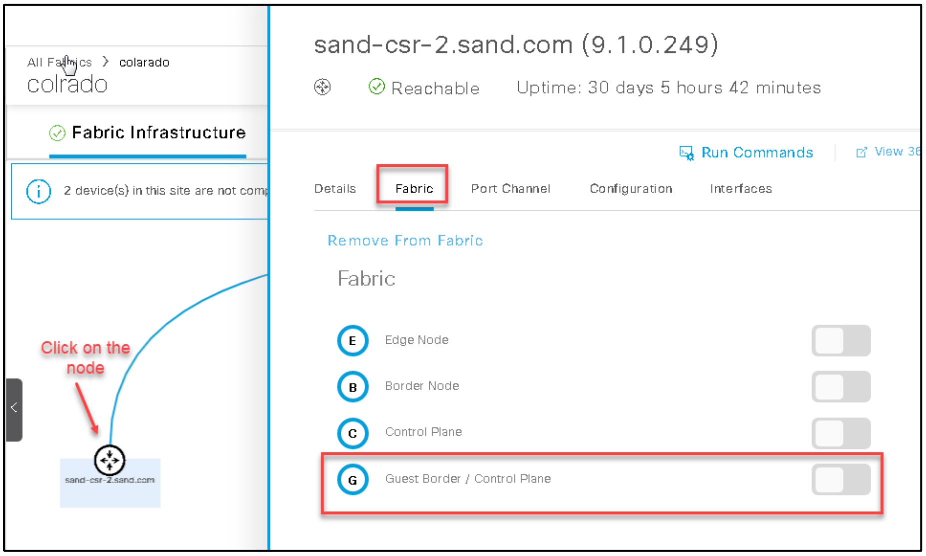
☐ Enable Wireless Multicast

SSID Name	Type	Security	Traffic Type	Address Pool	Scalable Group
sand-guest-1	Guest	Web Auth	Data	Choose Pool Search Dropdown 9_10_61_0-guest	Assign SGT
sand-site1-1x	Enterprise	WPA2 Enterprise	Voice + Data		Assign SGT

If you are using a dedicated border and control plane for guest traffic, you need to add the guest control-plane and border to the fabric: click the device icon to open the device details page.

The window shown below will pop up, and you can select both Border and Control Plane functionality. Also, the VN you marked as being guest enabled will show up here. Internally, Cisco DNA Center will take care of the fabric configuration to associate the guest SSID with the pool and map that pool to the guest control-plane and border.

An important point note is that it is recommended to keep the Guest Border and Control plane co-located on the same device. The handoff from the Guest Border is a manual process, the administrator can configure a protocol of choice to do the handover to the external domain.



All Fabrics > colarado

colrado

Fabric Infrastructure

2 device(s) in this site are not comp

Click on the node

sand-csr-2.sand.com

sand-csr-2.sand.com (9.1.0.249)

Reachable   Uptime: 30 days 5 hours 42 minutes

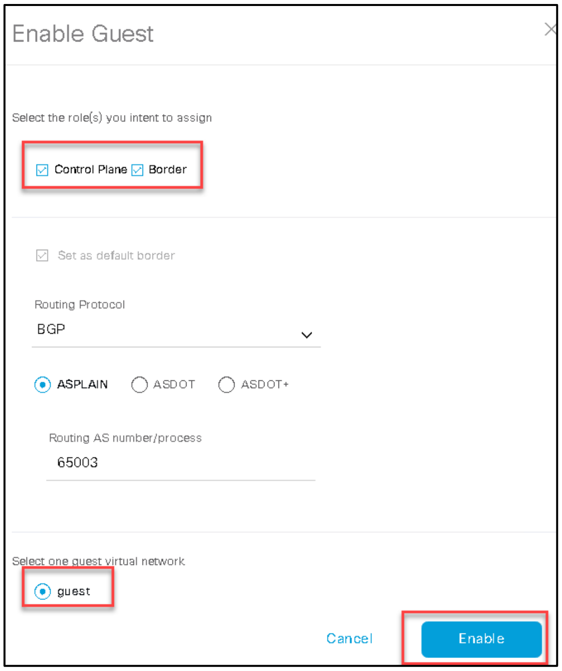
Fabric

E Edge Node

B Border Node

C Control Plane

G Guest Border / Control Plane



Enable Guest

Select the role(s) you intent to assign

☑ Control Plane ☑ Border

☑ Set as default border

Routing Protocol

BGP

● ASPLAIN ○ ASDOT ○ ASDOT+

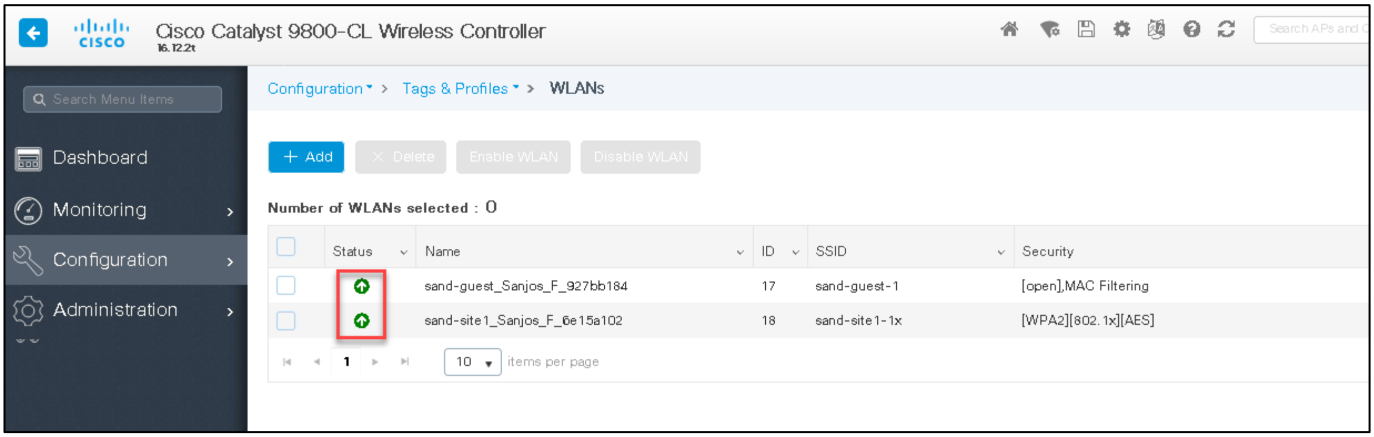
Routing AS number/process

65003

Select one guest virtual network

● guest

Step 5 Once you have associated the SSID with a pool in step 4, on the WLC, you will see that the Admin Status of the SSIDs is now "Enabled."



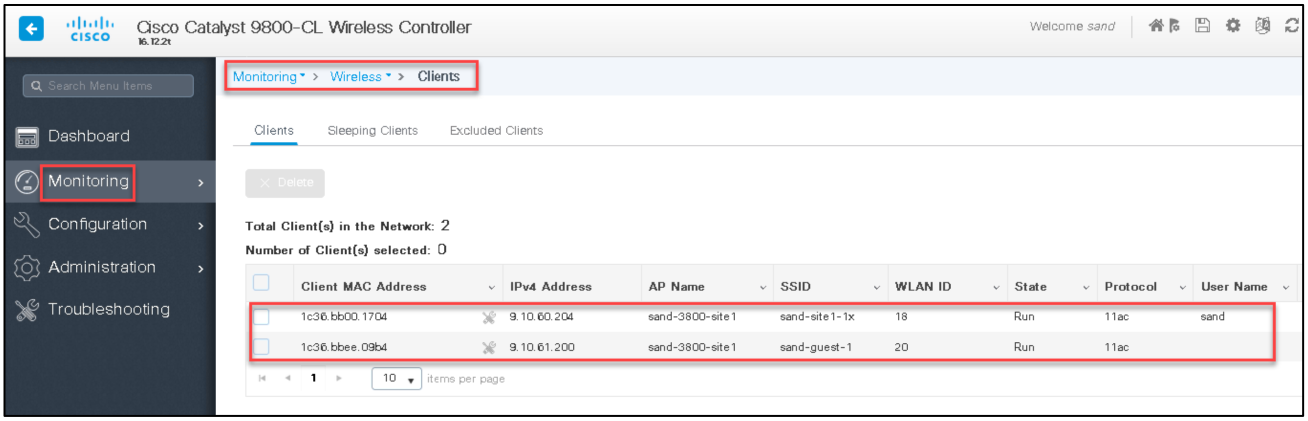
Number of WLANs selected : 0

□	Status	Name	ID	SSID	Security
□	●	sand-guest_Sanjos_F_927bb184	17	sand-guest-1	[open],MAC Filtering
□	●	sand-site1_Sanjos_F_6e15a102	18	sand-site1-1x	[WPA2][802.1x][AES]

Note The above screenshot from the WLC is for illustration purposes only. The WLAN name and security may be different in your setup.

Step 6 Clients can now be connected to the fabric-enabled wireless SSID. You can go to your WLC and view the connected client details.

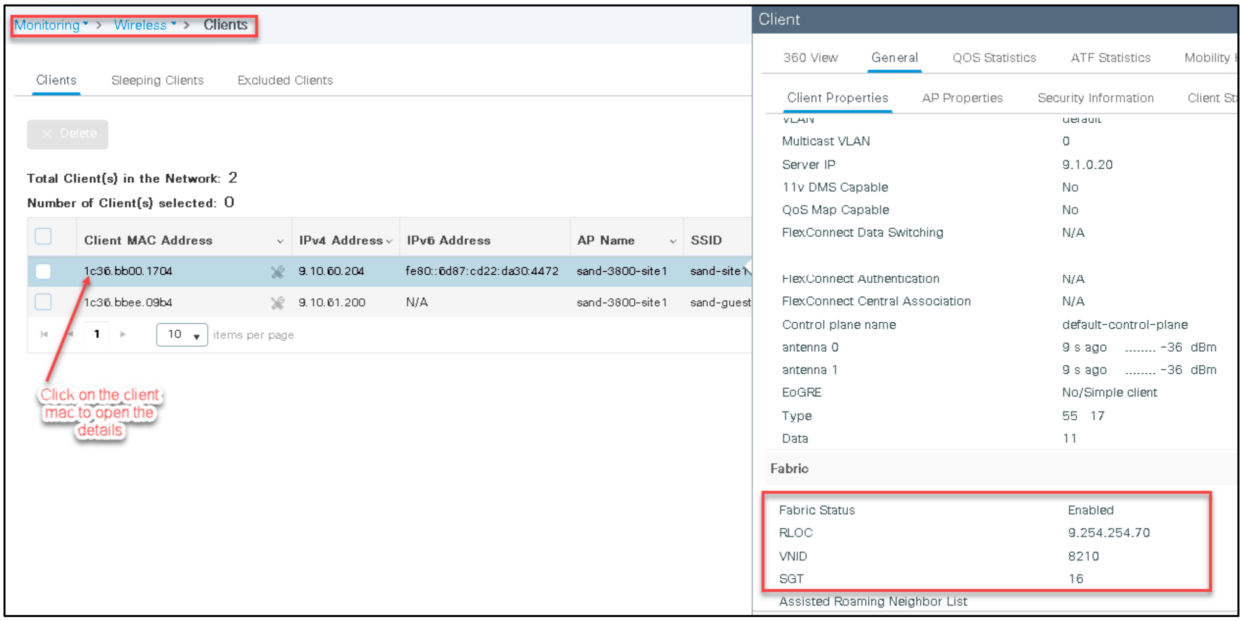
Navigate to Monitoring->Wireless->Clients



Total Client(s) in the Network: 2
Number of Client(s) selected: 0

Client MAC Address	IPv4 Address	AP Name	SSID	WLAN ID	State	Protocol	User Name
1c36.bb00.1704	9.10.60.204	sand-3800-site1	sand-site1-1x	18	Run	11ac	sand
1c36.bbee.09b4	9.10.61.200	sand-3800-site1	sand-guest-1	20	Run	11ac	

You can see the client fabric status and the SGT tag pushed to the WLC from ISE based on the authorization rule.



Total Client(s) in the Network: 2
Number of Client(s) selected: 0

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID
1c36.bb00.1704	9.10.60.204	fe80::6d87:cd22:da30:4472	sand-3800-site1	sand-site1
1c36.bbee.09b4	9.10.61.200	N/A	sand-3800-site1	sand-guest

VLAN	default
Multicast VLAN	0
Server IP	9.1.0.20
11v DMS Capable	No
QoS Map Capable	No
FlexConnect Data Switching	N/A
FlexConnect Authentication	N/A
FlexConnect Central Association	N/A
Control plane name	default-control-plane
antenna 0	9 s ago .... -36 dBm
antenna 1	9 s ago .... -36 dBm
EoGRE	No/Simple client
Type	55 17
Data	11
Fabric Status	Enabled
RLOC	9.254.254.70
VNID	8210
SGT	16
Assisted Roaming Neighbor List	

QoS on SDA Wireless

Quality of Service (QoS) provides the ability to prioritize the traffic by giving preferential treatment to specific traffic over the other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput.

In this section, we will focus on how traffic is prioritized and maintained when the traffic is originated and destined to a wireless client/endpoint. There are four metal policies or access categories that are defined by the standard IEEE 802.11e specifications. These policies define the priority and queues associated with the wireless medium(radio). The parameters for the metal policies can't be modified by an Administrator as these are defined in the 802.11e specifications. These metal policies define their usage and are available on the Aire-OS and Catalyst 9800 Wireless LAN controller. The QoS in a wireless network is to give preferential treatment to access the wireless medium and also translate that priority over the wired medium both in the upstream(wireless client to wired network) and downstream (wired network to wireless client) direction. The wireless medium is half-duplex unlike wired so to ensure that high-priority applications always get an opportunity to transmit and access the medium, there are certain parameters such as contention window, back off timer, and transmission opportunity which control how packets in each of the queue access the physical media. The access point maintains separate queues and transmission timers for each of the metal queue. If there is a data stream that is traversing downstream direction(wired to wireless) the access point maps the incoming frame from the wired network to one of the metal queues based on the incoming DSCP, and thus giving priority in transmission in the downstream direction. Similarly, if there is a data frame in the upstream direction wireless client would categorize the frame and follow the timers associated with the respective metal queue. Once the data frame is received at the access point, the access point needs to translate the priority to the wired medium by mapping the priority of the incoming frame onto the DSCP of the outgoing packet to the wired medium. For more information in understanding how each of the metal policies access the medium and the respective timers, please refer to the following documentation:

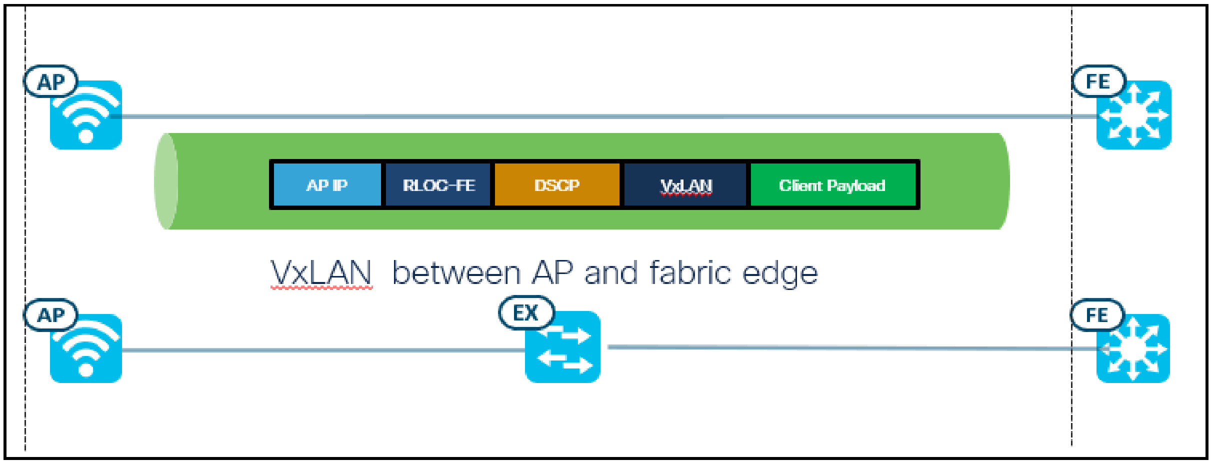
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/ch5_QoS.html#73518

The four metal policies/ access categories on the system are as follows:

- Platinum—Used for VoIP clients.
- Gold—Used for video clients.
- Silver— Used for traffic that can be considered best-effort.
- Bronze—Used for Non-real time traffic

Fabric AP Access Tunnel

The access point in a fabric mode has a VxLAN tunnel(Access-Tunnel) build to the fabric edge where the AP is attached. In cases where the AP is attached to an Extended Node(EN) or a Policy Extended Node(PEN). The access-tunnels are build between the Access Point (AP) and the respective fabric edge where the extended node is uplinked to. The VxLAN tunnel between an AP and a fabric edge is to preserve the segmentation till the access point. The access point is responsible to insert the SGT tag in the VxLAN tunnel to the fabric edge.



The following output is taken from a fabric edge which has two fabric AP attached to it and has two VxLAN/access tunnels. The below output is for illustration purposes while the actual output may vary based on the number of AP's attached to the Fabric edge directly or indirectly through an extended node/policy extended node.

```
show access-tunnel summary

Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 2


Name    RLOC IP(Source)  AP IP(Destination)  VRF ID  Source Port  Destination Port
------  ---------------  ------------------  ------  -----------  ----------------
Ac1     9.254.254.71     9.40.50.166         0       N/A          4789
Ac0     9.254.254.71     9.40.50.160         0       N/A          4789


Name   IfId            Uptime
------ ---------- --------------------
Ac1    0x0000004F 1 days, 13:12:22
Ac0    0x0000004E 0 days, 19:30:51
```

QoS profile on SSID

WLAN data in an SDA fabric Network is tunneled in VxLAN (IP UDP packets).To maintain the QoS classification that has been applied to a WLAN frame, the fabric AP uses a process of mapping classifications to and from 802.11e UP/DSCP. For example, when WMM classified traffic is sent by a WLAN client, it has an 802.11e UP classification in the 802.11 header and a DSCP carried in the IP header. The AP needs to translate this classification i.e 802.11e UP or DSCP into a DSCP value for the VxLAN encapsulated packet carrying the frame. This is done to ensure that the packet is treated with the appropriate priority while traversing across the SDA fabric.

An application running on a wireless endpoint can insert the right QoS in the data frame by tagging the data frame with an

802.11e UP and by inserting the right DSCP value in the IP header. The Cisco AP can inspect the 802.11e UP/DSCP in an 802.11 data frame from a wireless endpoint and derive the respective DSCP value which would be inserted into the DSCP field of the outer IP header in the tunneled VxLAN packet.

The derivation of the DSCP to be inserted in the IP header of the VxLAN is based on the Cisco AVVID table and metal policies which define the mapping of the respective 802.11e UP /DSCP to the equivalent DSCP.

An SSID has a Qos profile attached to it. The QoS profile is associated with one of the metal classes defined on the system which is defined as follows based on the priority.

- Platinum – Voice
- Gold - Video
- Silver – Best Effort
- Bronze - Background

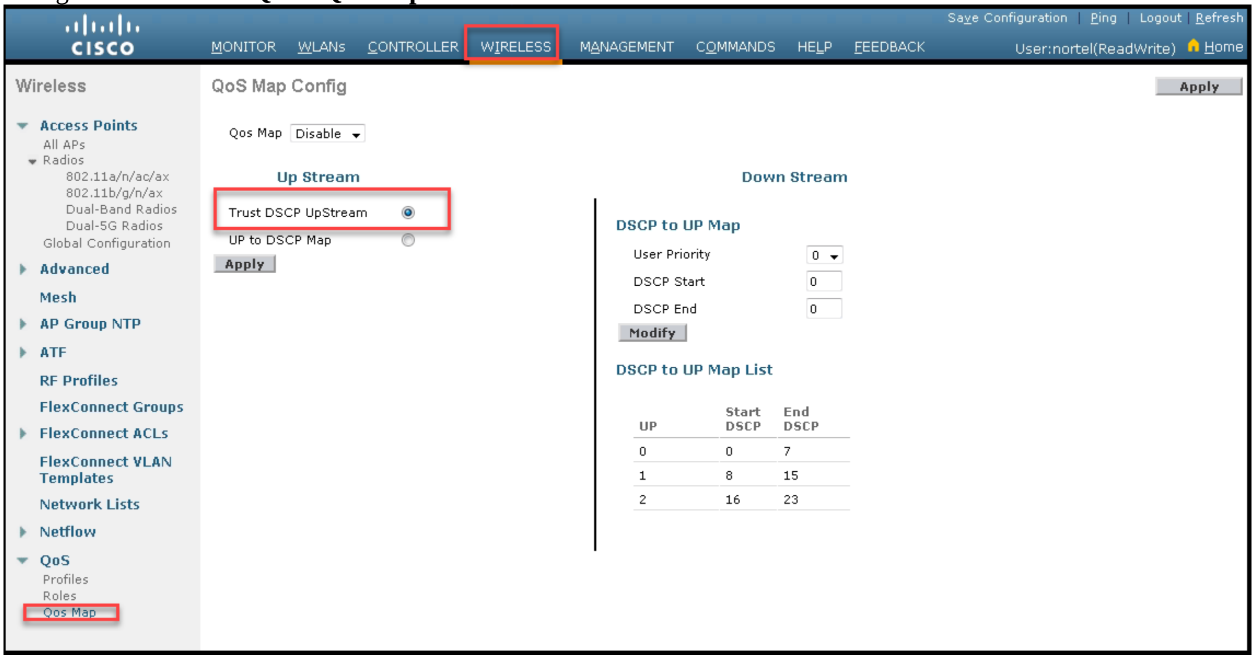
The role of assigning a metal policy to an SSID is to set the ceiling for the data frame that can be allowed on that SSID. If the profile is set to Silver – best effort then any traffic tagged with a voice priority is degraded and re-written to best effort on the AP and transmitted. If the profile is set to platinum then traffic tagged with voice/video/best-effort and background are allowed by the system.

Currently, there is an interop issue between different vendors in the wireless world as different vendors follow different paradigm structure to map the 802.11e UP and the respective DSCP. This creates an issue as the infrastructure may not be able to categorize the traffic correctly. ***To circumvent this issue the Cisco recommends as a best practice to trust the DSCP in the upstream direction (wireless to wired medium).***

Note: Starting with Cisco IOS-XE-17.4, trust DSCP upstream is enabled by default. Release prior to 17.4, trust DSCP needs to manually enabled on the WLC. Refer to the respective controller configuration guide to manually set the option.

The trust DSCP upstream config option on an Aire-OS-based WLC:

Navigate to **wireless→Qos→QoSMap**



QoS Map Config

Qos Map: Disable

Up Stream

Trust DSCP UpStream ●
UP to DSCP Map ○

Apply

Down Stream

DSCP to UP Map

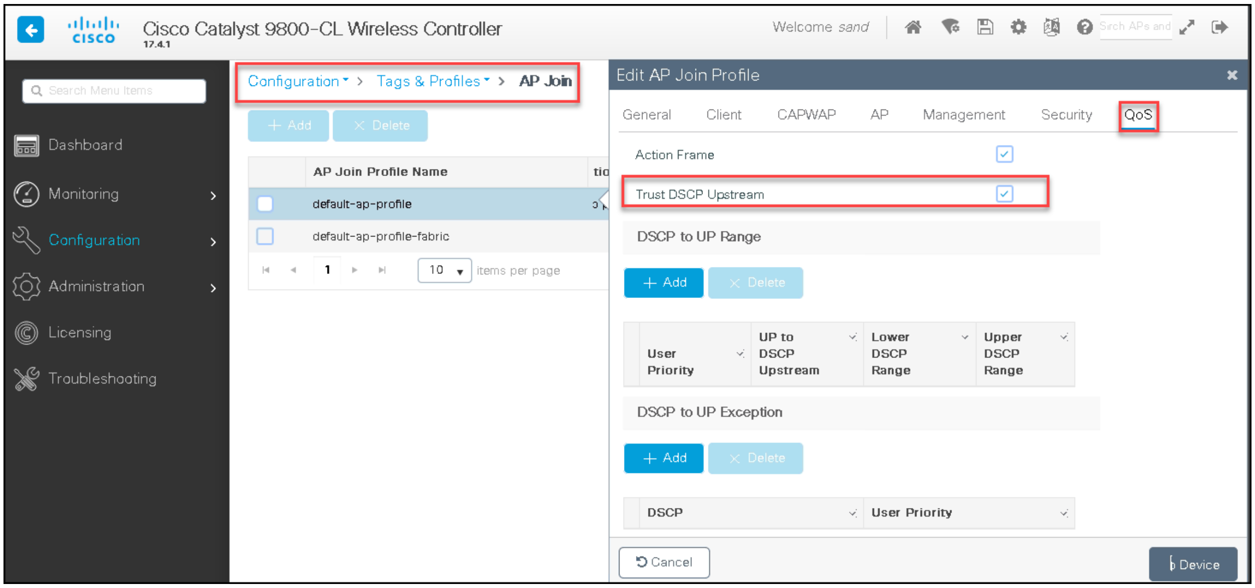
User Priority: 0
DSCP Start: 0
DSCP End: 0

Modify

DSCP to UP Map List

UP	Start DSCP	End DSCP
0	0	7
1	8	15
2	16	23

Trust DSCP upstream config for the Catalyst 9800 IOS-XE based WLC is configured under the respective AP join profile:



Action Frame ☑

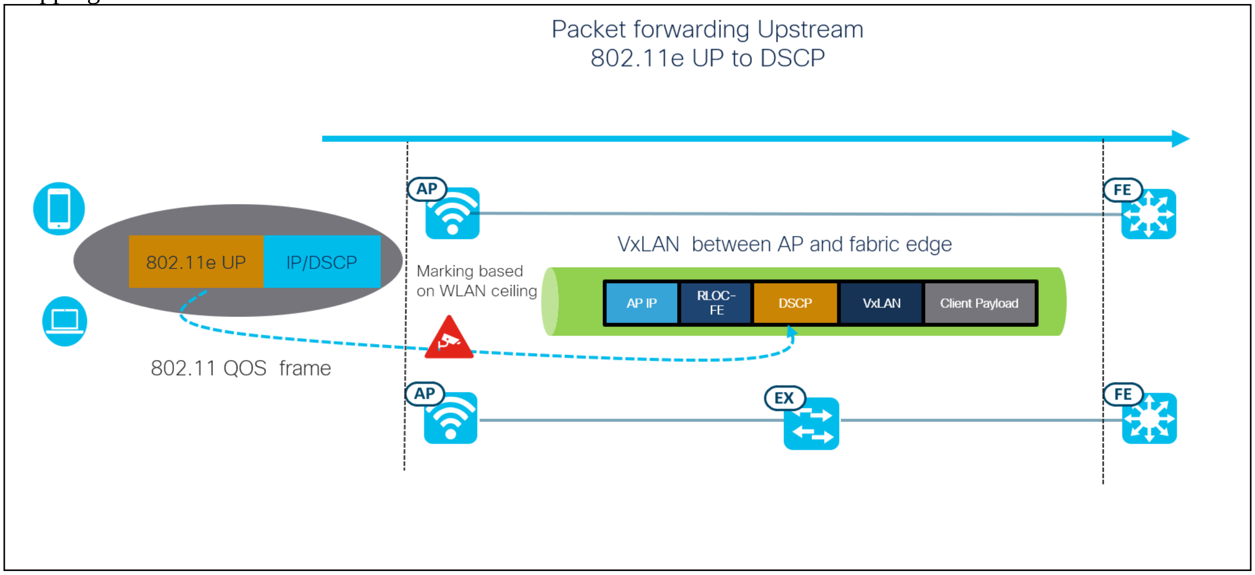
Trust DSCP Upstream ☑

In the case of the trust DSCP the access point extracts the DSCP from the incoming 802.11 client payload and copies it to the VxLAN outer IP header.

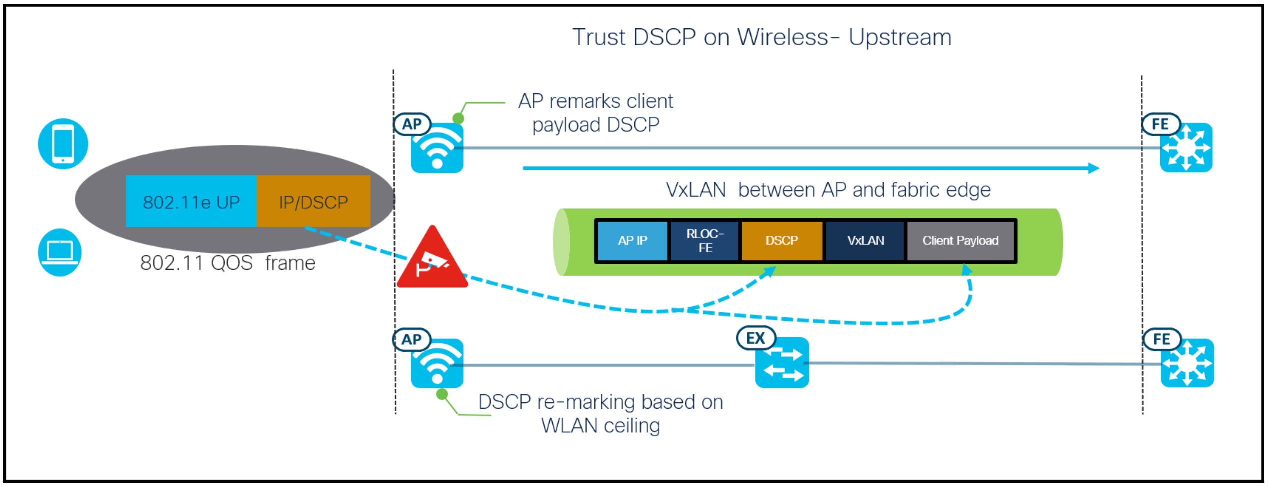
The WLAN ceiling still applies even when the trust DSCP upstream option is enabled on the WLC. For example, if the WLAN metal policy is mapped to Gold and the incoming 802.11 frame from a wireless client carries a DSCP of 46 (Expedited Forwarding). The access point would re-write the DSCP on the original client payload to AF41 and the VxLAN IP header carries the DSCP of AF41.

The following figures show the mapping of how the 802.11e UP /DSCP is carried upstream from a wireless client and how the priority is maintained and preserved in the SDA fabric.

Mapping of 802.11e UP to DSCP UP-stream

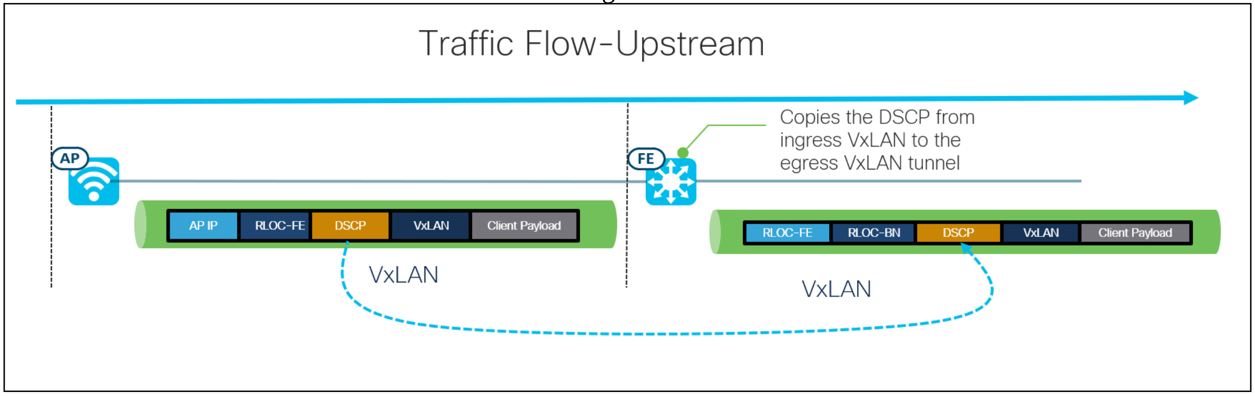


Derivation of DSCP when trust DSCP upstream in enabled on the Wireless LAN Controller:

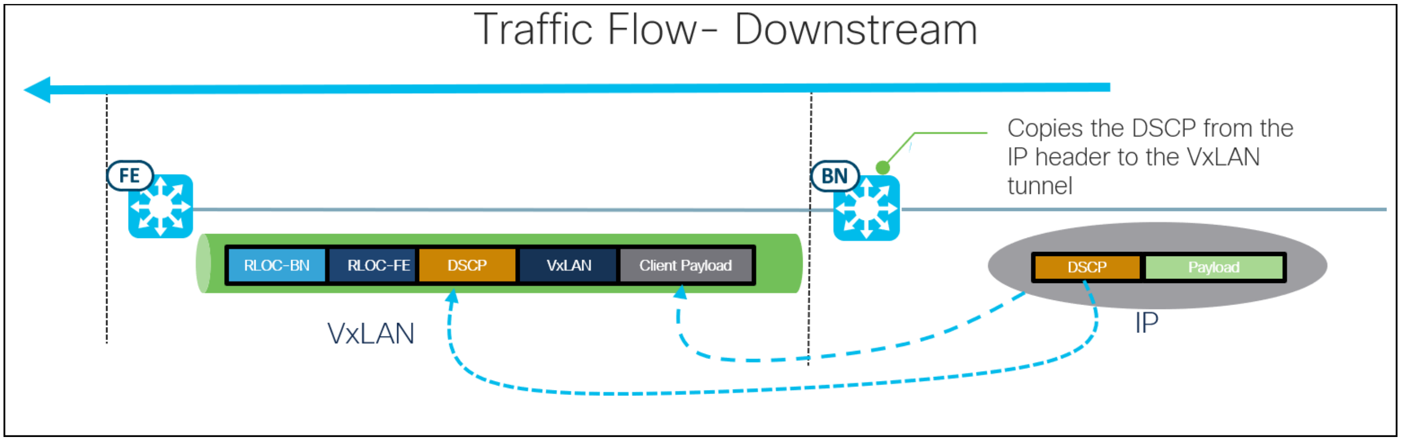

Trust DSCP on Wireless- Upstream
AP remarks client payload DSCP
AP
FE
VxLAN between AP and fabric edge
802.11e UP
IP/DSCP
802.11 QOS frame
AP IP
RLOC-FE
DSCP
VxLAN
Client Payload
AP
EX
FE
DSCP re-marking based on WLAN ceiling

The fabric edge will terminate the VxLAN tunnel from the access point and will determine the destination where the data frame needs to be forwarded. Based on the destination the fabric edge will copy the DSCP from the incoming VxLAN to the egress VxLAN tunnel. Thus the priority is preserved as the data frame propagates within the fabric. If the traffic is destined northbound, the termination of the VxLAN happens on the border node and the client payload is transmitted preserving the DSCP in the packet.

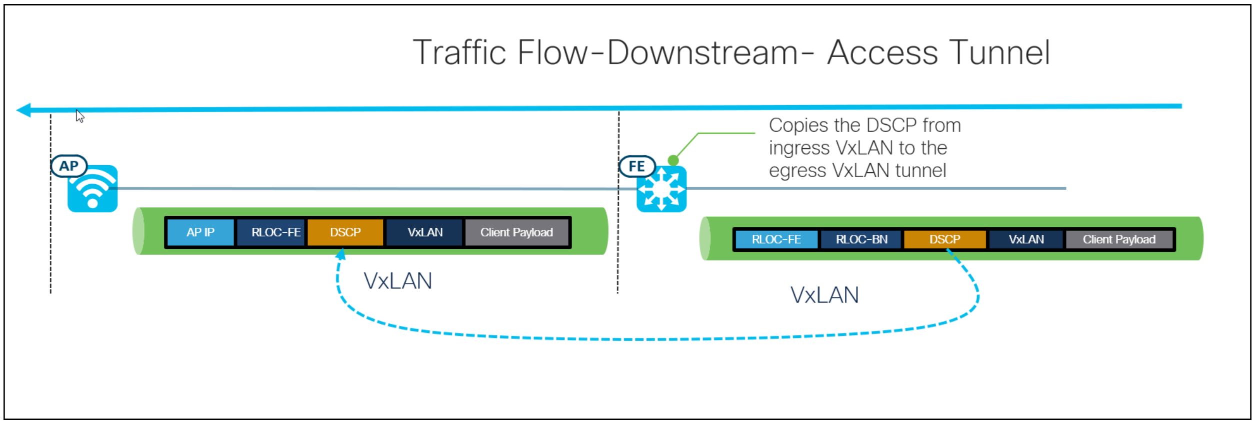
Preservation of DSCP for traffic flow from the fabric edge:



In the downstream direction for traffic originating from outside the fabric, the DSCP from the incoming IP packet is copied onto the VxLAN header at the border node.

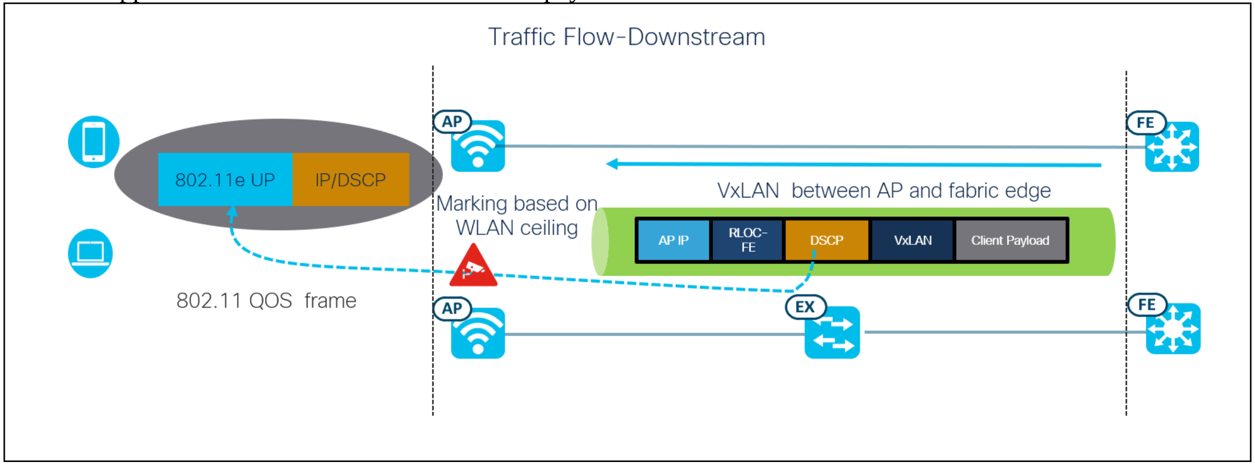


The VxLAN data frame is terminated at the fabric edge and will copy the DSCP from the incoming frame onto the access tunnel to the fabric AP.



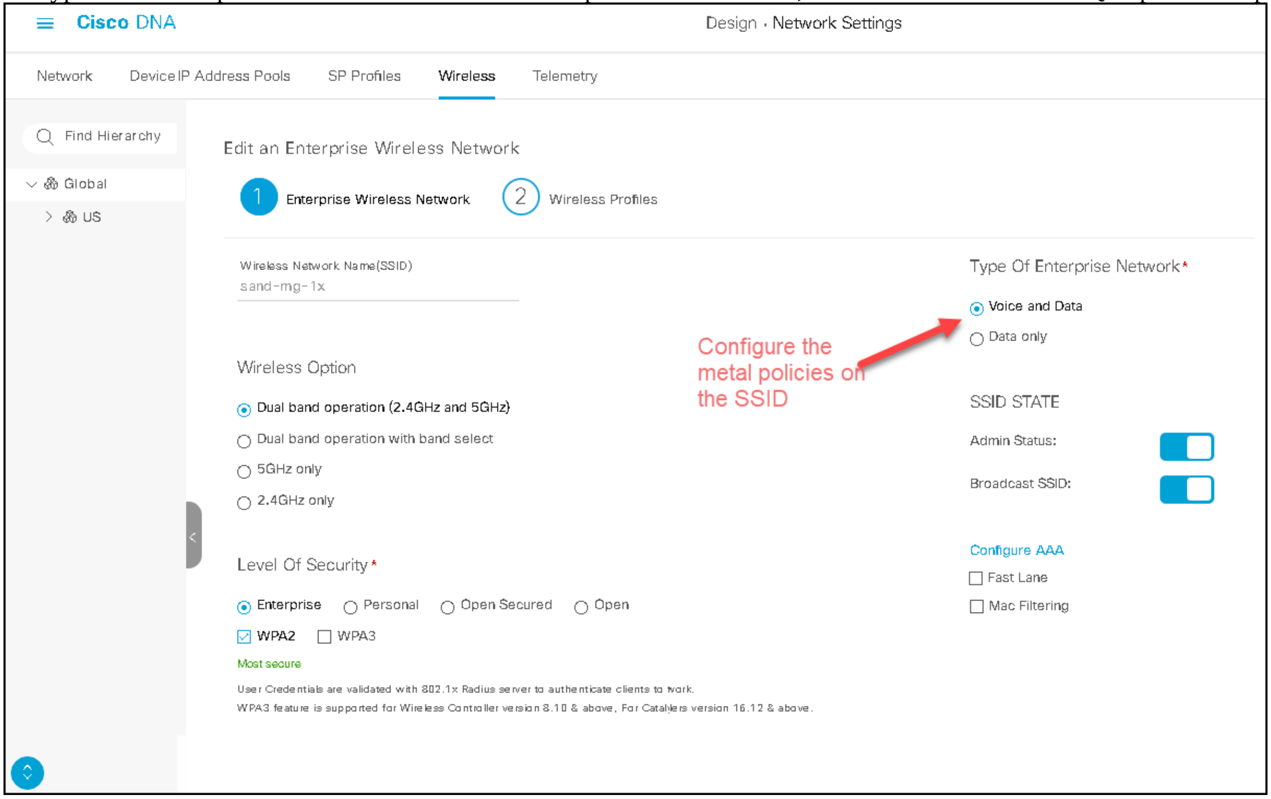
Traffic Flow-Downstream- Access Tunnel

The access point will terminate the VxLAN tunnel and derive the equivalent 802.11e UP to be forwarded to the wireless client. The access point will cap the DSCP of the client payload and the 802.11e UP based on the WLAN QoS profile mapping. For example, if the incoming DSCP in the VxLAN is set to EF and the WLAN QoS profile is marked for Gold, then the 802.11eUP will be capped at five and the DSCP of the client payload will be re-written to AF41.



Traffic Flow-Downstream

The Cisco DNAC automates the QOS metal policies for the SSID. During the SSID creation, an administrator needs to specify the type of the enterprise network. If the SISD is set up for voice and data, the DNAC automates the QoS profile for platinum.



Edit an Enterprise Wireless Network

1 Enterprise Wireless Network   2 Wireless Profiles

Wireless Network Name(SSID)
sand-mg-1x

Type Of Enterprise Network*

● Voice and Data
○ Data only

Configure the metal policies on the SSID

Wireless Option

● Dual band operation (2.4GHz and 5GHz)
○ Dual band operation with band select
○ 5GHz only
○ 2.4GHz only

SSID STATE

Admin Status: on

Broadcast SSID: on

Configure AAA

□ Fast Lane
□ Mac Filtering

Level Of Security*

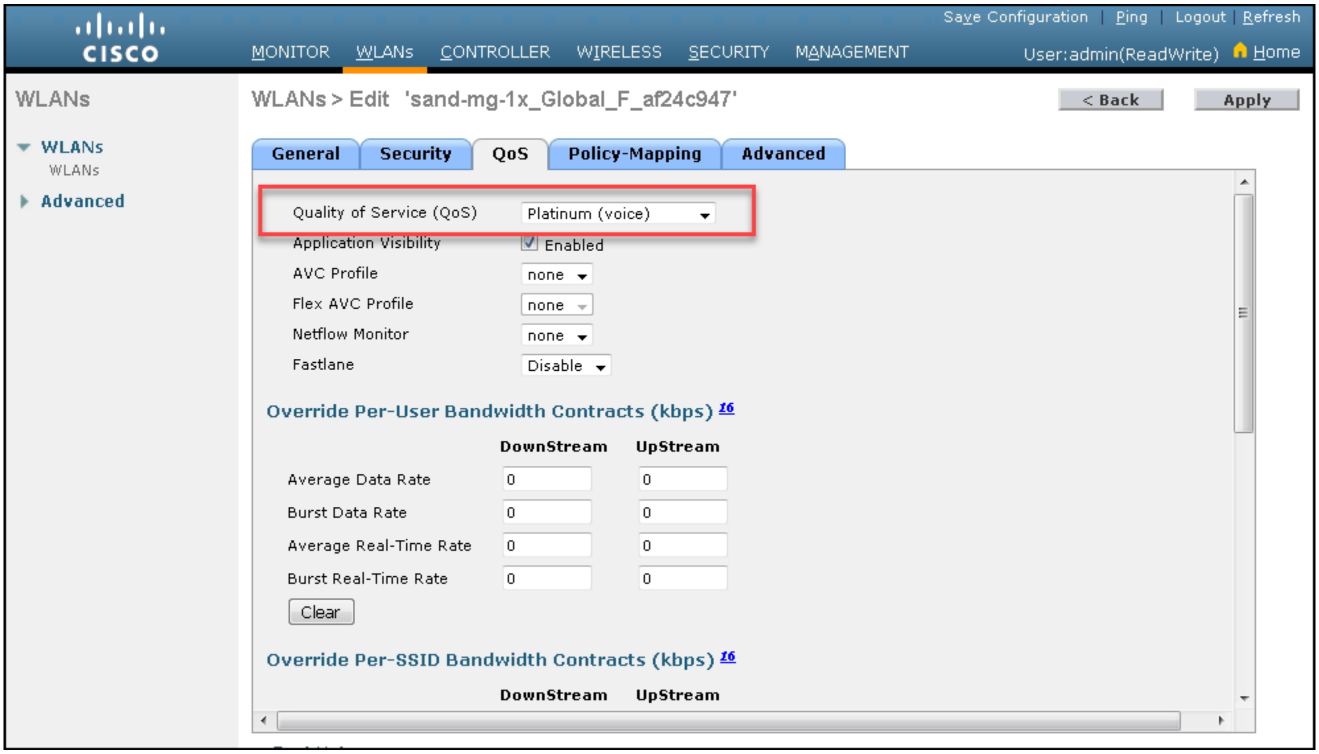
● Enterprise ○ Personal ○ Open Secured ○ Open

☑ WPA2 □ WPA3

Most secure

User Credentials are validated with 802.1x Radius server to authenticate clients to work.
WPA3 feature is supported for Wireless Controller version 8.10 & above, For Catalysts version 16.12 & above.

The QoS profile provisioned by the Cisco DNAC on an Aire-OS based WLC:



WLANs > Edit 'sand-mg-1x_Global_F_af24c947'

Quality of Service (QoS): Platinum (voice)
Application Visibility: ☑ Enabled
AVC Profile: none
Flex AVC Profile: none
Netflow Monitor: none
Fastlane: Disable

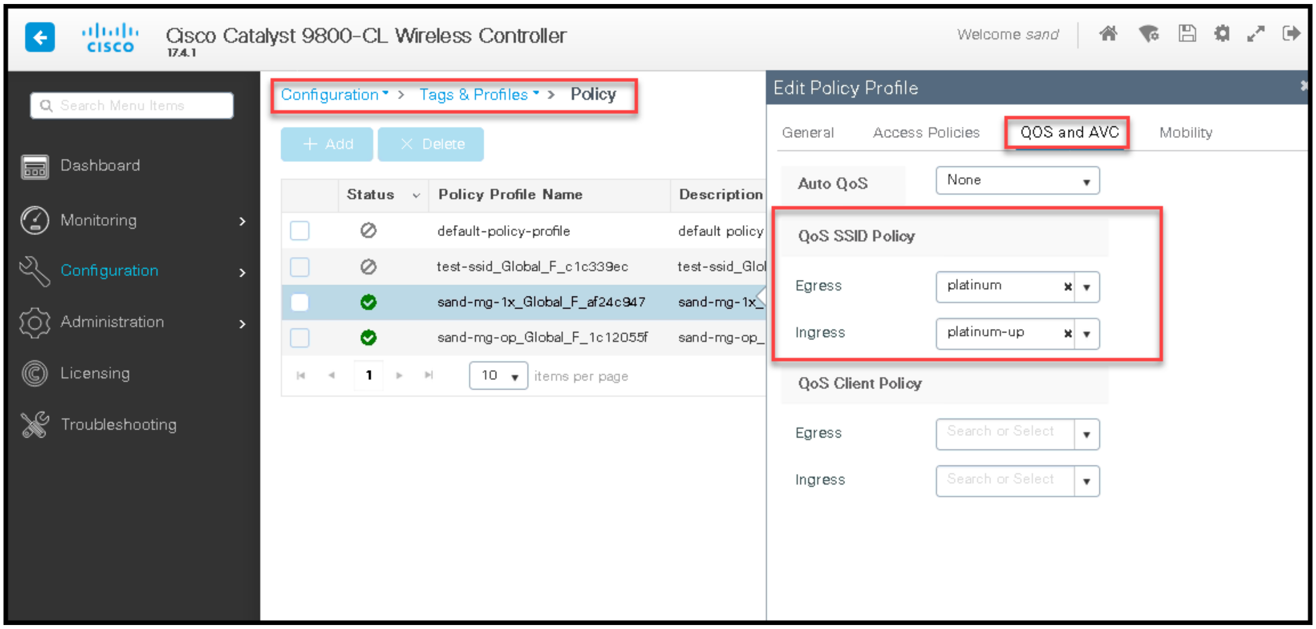
Override Per-User Bandwidth Contracts (kbps) 16

	DownStream	UpStream
Average Data Rate	0	0
Burst Data Rate	0	0
Average Real-Time Rate	0	0
Burst Real-Time Rate	0	0

Override Per-SSID Bandwidth Contracts (kbps) 16

DownStream UpStream

The QoS profile for the Catalyst 9800 based WLC is provisioned on the policy profile mapped to the SSID:



Cisco Catalyst 9800-CL Wireless Controller 17.4.1

Configuration > Tags & Profiles > Policy

	Status	Policy Profile Name	Description
□	⊘	default-policy-profile	default policy
□	⊘	test-ssid_Global_F_c1c339ec	test-ssid_Glol
□	✓	sand-mg-1x_Global_F_af24c947	sand-mg-1x_
□	✓	sand-mg-op_Global_F_1c12055f	sand-mg-op_

1 | 10 items per page

Edit Policy Profile

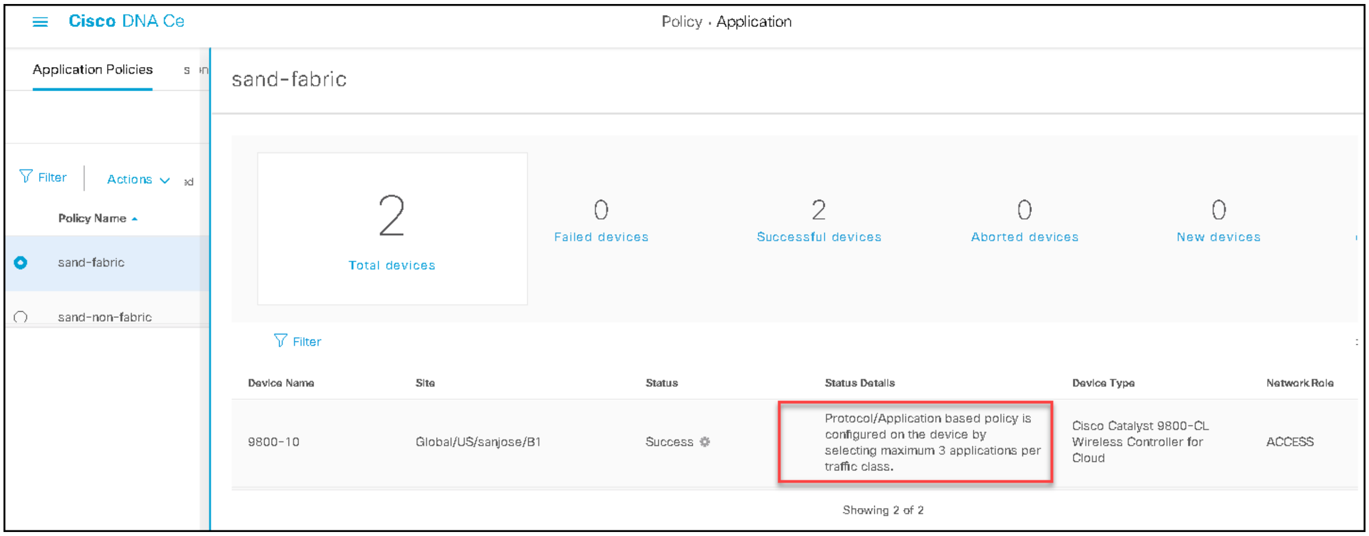
Auto QoS: None

QoS SSID Policy
Egress: platinum
Ingress: platinum-up

QoS Client Policy
Egress: Search or Select
Ingress: Search or Select

AVC on SDA Wireless

The Cisco DNAC can be used to provision application policies and these policies are supported on Aire-OS and Catalyst 9800 based WLC. In the case of Catalyst 9800 based WLC, the cisco DNAC doesn’t support metal policies and application policy at the same time as both of them get configured as an SSID policy. The Catalyst 9800 wireless controller when working in fabric mode can only support up to three applications per traffic class. There are about eleven traffic classes, which make a total of 33 applications that be recognized by the system when working in fabric mode.



Device Name	Site	Status	Status Details	Device Type	Network Role
9800-10	Global/US/sanjose/B1	Success	Protocol/Application based policy is configured on the device by selecting maximum 3 applications per traffic class.	Cisco Catalyst 9800-CL Wireless Controller for Cloud	ACCESS

Showing 2 of 2

Please refer to the guide below in enabling Application policies on the Cisco DNAC.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-1-0/user_guide/b_cisco_dna_center_ug_1_3_1_0/b_cisco_dna_center_ug_1_3_1_0_chapter_01011.html#id_51875

References:
Understanding Wireless QoS:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide/ch5_QoS.html#73518

Cisco AVVID mapping table:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/quality_of_service.html

Catalyst 9800 QOS Configuration guide:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-11/config-guide/b_wl_16_11_cg/quality-of-service.html#id_136353

Note: Application Assurance is not supported on wireless when operating in fabric mode(Cisco DNAC 2.1.2.x.)

Configuring multicast

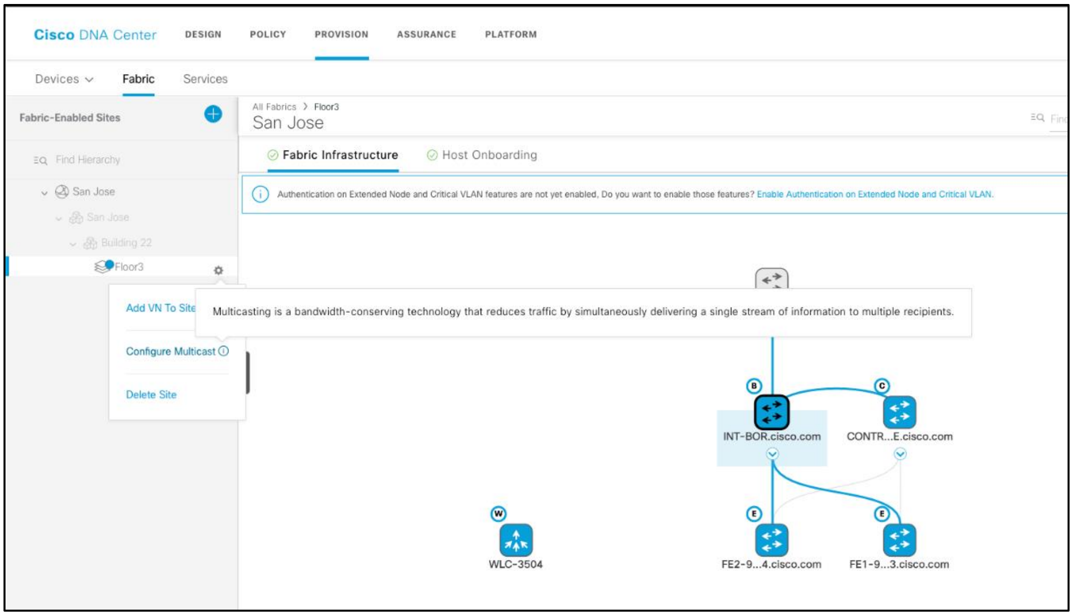
To enable multicast for wireless, you first need to configure multicast in the wired network. Cisco DNA Center makes it very easy to configure both, as outlined in the steps below.

Note Multicast over wireless needs to be considered with some caution.

Once multicast IP traffic gets to the AP, these packets are transmitted over the air as broadcast Layer 2 frames; this basically means traffic gets transmitted at the highest mandatory data rate (to be able to reach all connected clients) and the transmission frames are not acknowledged, so a collision in the air will result in the loss of the frame. This has implications for the achievable throughput of multicast traffic over the air. To improve the performance and reliability of multicast traffic over Wi-Fi, Cisco has developed the VideoStream feature, which converts multicast frames into unicast frames at the AP, solving the problems mentioned above. The support for VideoStream (also known as the multicast-to-unicast feature) is supported by using templates starting from Cisco DNA Center 1.3.

Procedure

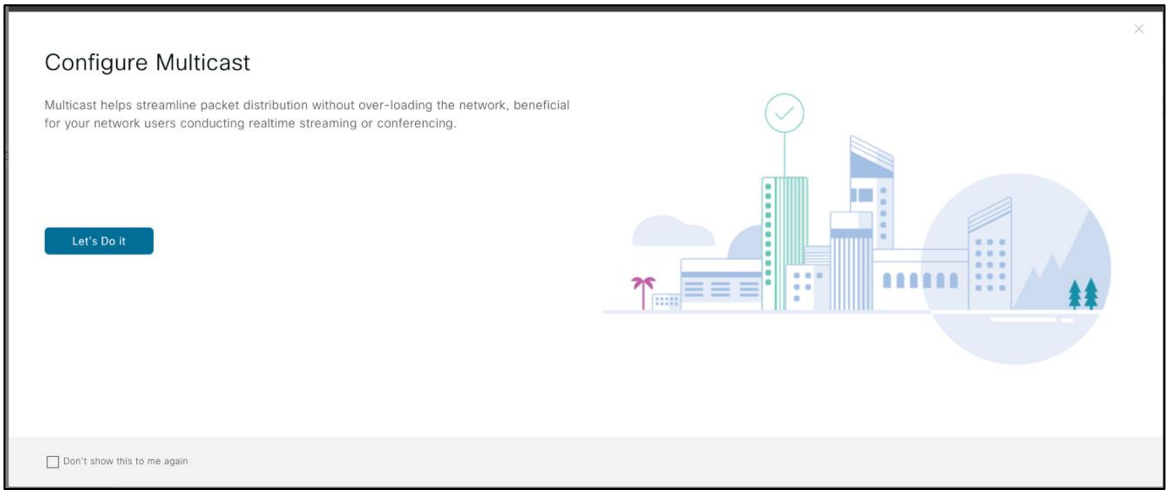
Step1 Click on the site gear menu in the Fabric > San Jose > Floor 3 and click on “Configure Multicast”. By clicking on this, you will be taken a walkthrough of steps to enable Multicast in your fabric.



Authentication on Extended Node and Critical VLAN features are not yet enabled. Do you want to enable those features? Enable Authentication on Extended Node and Critical VLAN.

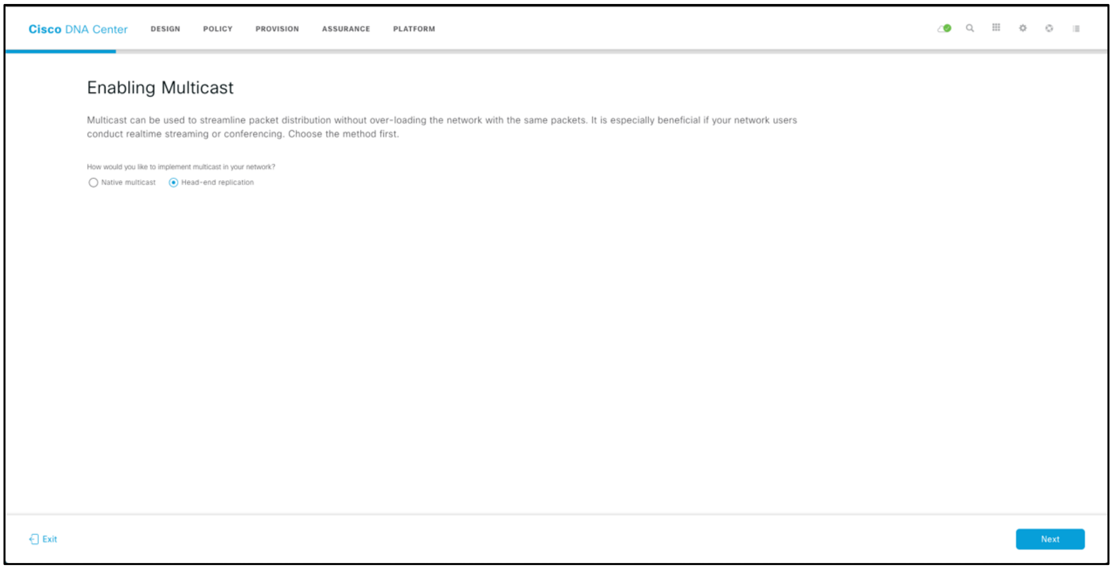
Multicasting is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to multiple recipients.

Step2 In the Enable Multicast workflow, click on “Let’s do it” to Configure Multicast.


Configure Multicast

Multicast helps streamline packet distribution without over-loading the network, beneficial for your network users conducting realtime streaming or conferencing.

Step3 Select Native or Headend Multicast and click on Next.



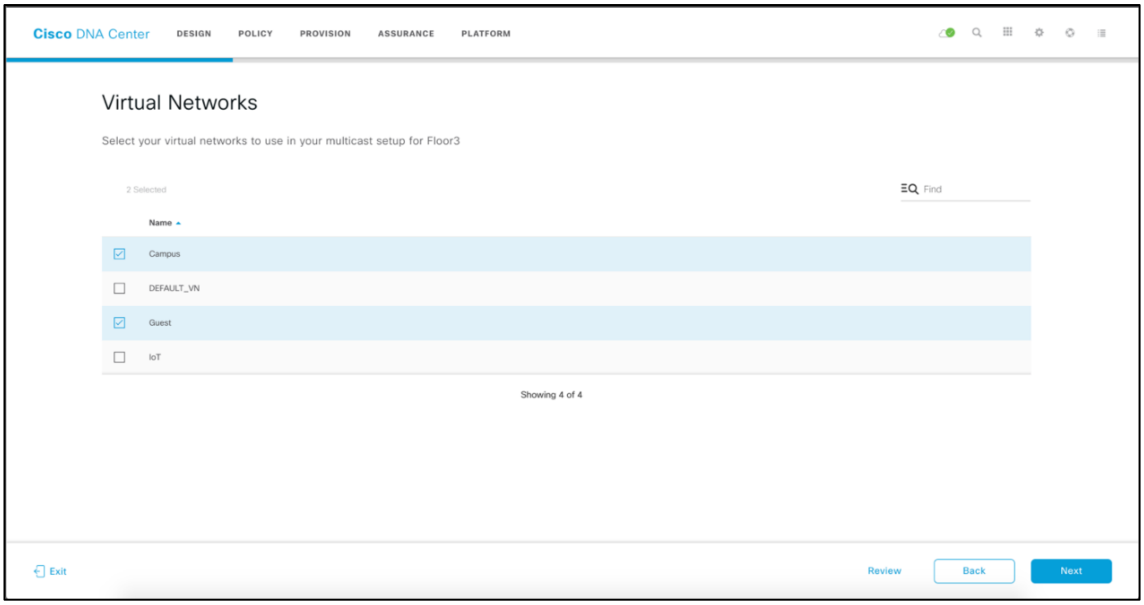
Enabling Multicast

Multicast can be used to streamline packet distribution without over-loading the network with the same packets. It is especially beneficial if your network users conduct realtime streaming or conferencing. Choose the method first.

How would you like to implement multicast in your network?

○ Native multicast ● Head-end replication

Step4 Select your virtual networks to use in your multicast setup for Floor3 and click on Next.



Virtual Networks

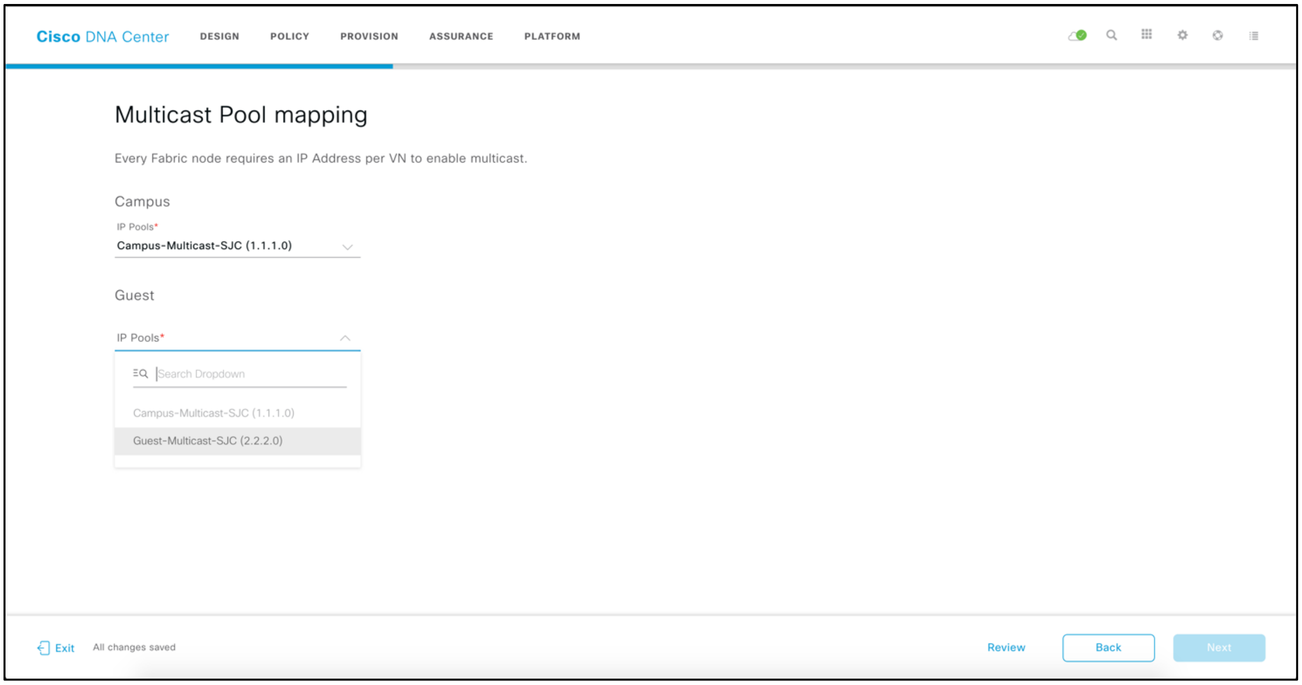
Select your virtual networks to use in your multicast setup for Floor3

2 Selected

	Name ▲
☑	Campus
□	DEFAULT_VN
☑	Guest
□	IoT

Showing 4 of 4

Step5 In the Multicast Pool mapping page, select the IP Pools that will be used to send multicast traffic. Every Fabric node requires an IP Address per VN to enable multicast. Click “Next” to go to the next section



Multicast Pool mapping

Every Fabric node requires an IP Address per VN to enable multicast.

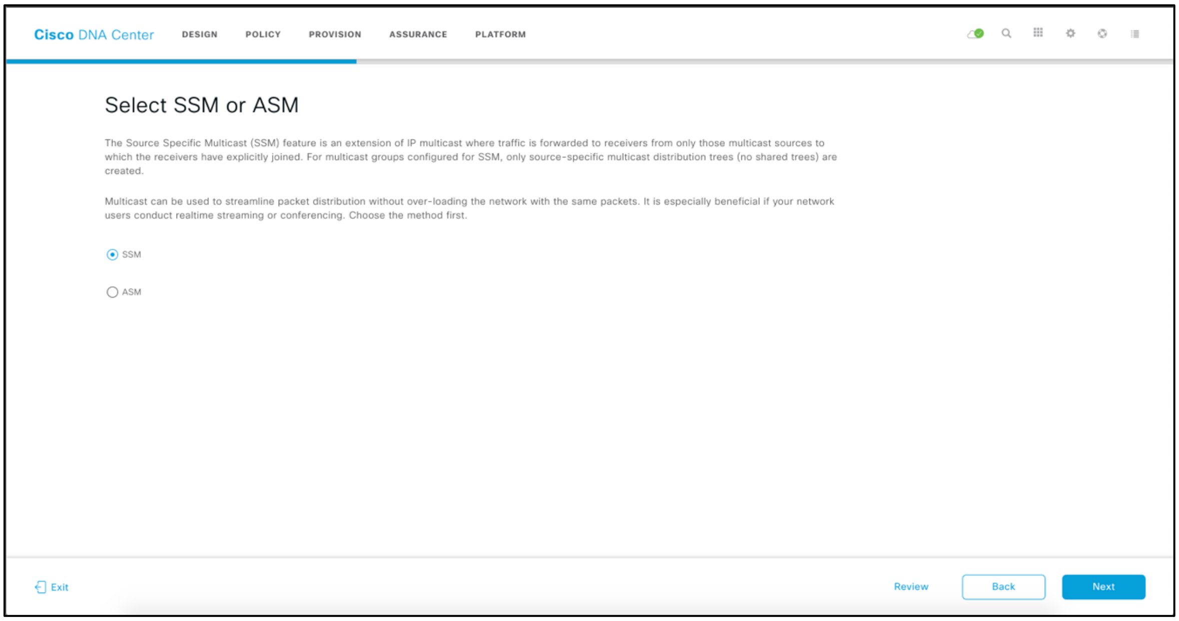
Campus

IP Pools*: Campus-Multicast-SJC (1.1.1.0)

Guest

IP Pools*

Step6 Select SSM or ASM



Select SSM or ASM

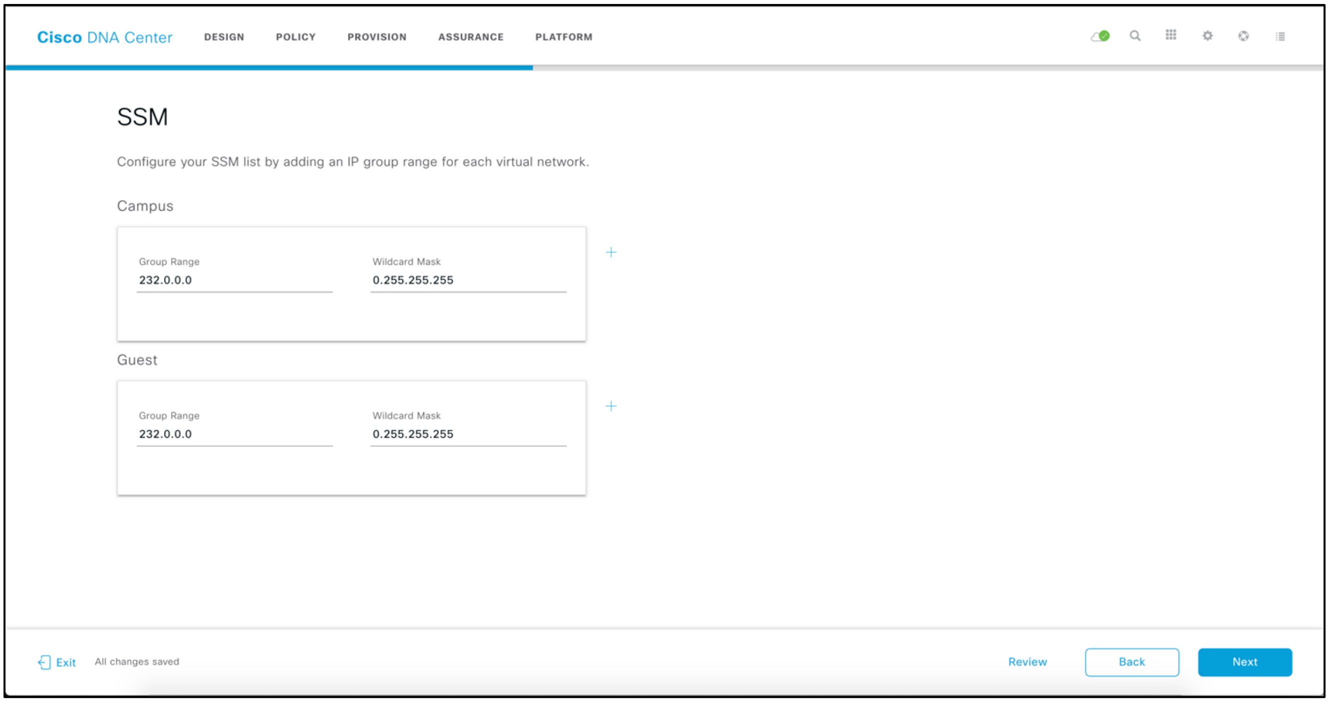
The Source Specific Multicast (SSM) feature is an extension of IP multicast where traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.

Multicast can be used to streamline packet distribution without over-loading the network with the same packets. It is especially beneficial if your network users conduct realtime streaming or conferencing. Choose the method first.

● SSM

○ ASM

Step7 Select the multicast IP range for SSM. Configure your SSM list by adding an IP group range for each virtual network.



SSM

Configure your SSM list by adding an IP group range for each virtual network.

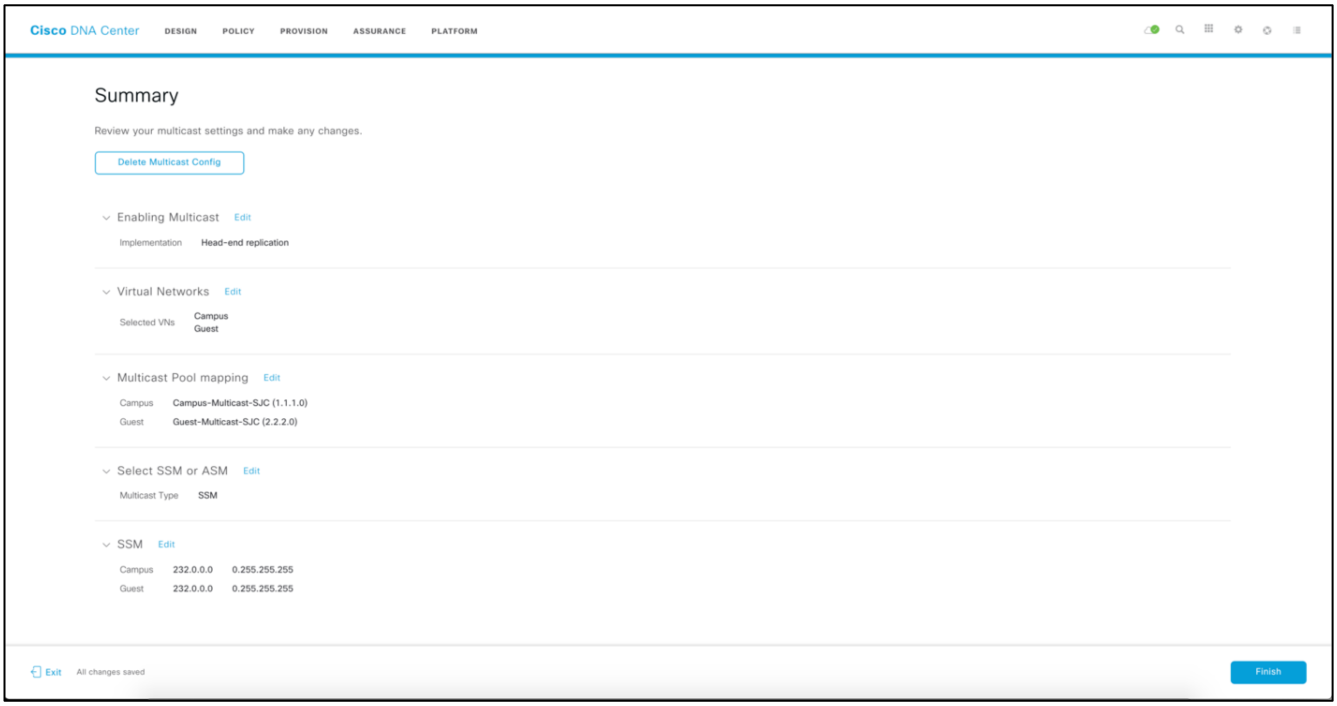
Campus

Group Range: 232.0.0.0
Wildcard Mask: 0.255.255.255

Guest

Group Range: 232.0.0.0
Wildcard Mask: 0.255.255.255

Step8 Review all the multicast configs and click on "Finish" to deploy Multicast.



Summary

Review your multicast settings and make any changes.

Enabling Multicast

Implementation: Head-end replication

Virtual Networks

Selected VNs: Campus, Guest

Multicast Pool mapping

Campus	Campus-Multicast-SJC (1.1.1.0)
Guest	Guest-Multicast-SJC (2.2.2.0)

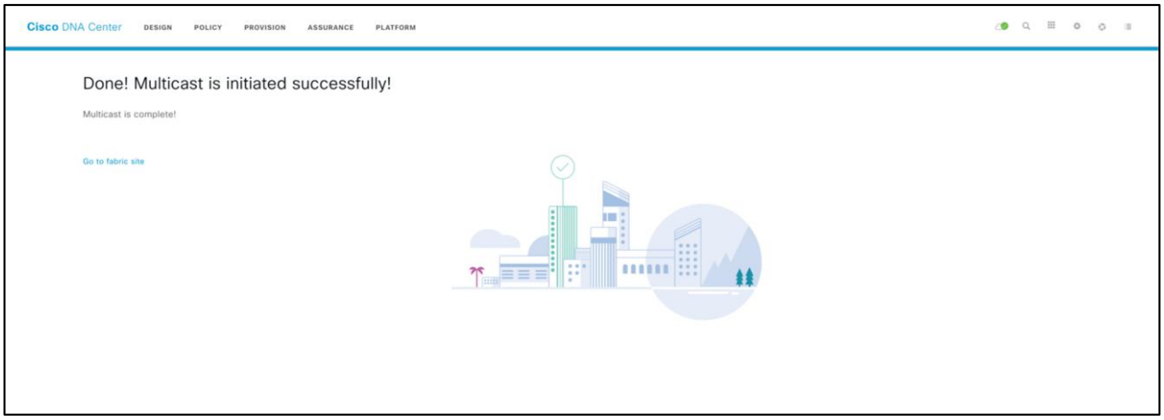
Select SSM or ASM

Multicast Type: SSM

SSM

Campus	232.0.0.0	0.255.255.255
Guest	232.0.0.0	0.255.255.255

This will complete the Multicast Configuration workflow.



Done! Multicast is initiated successfully!

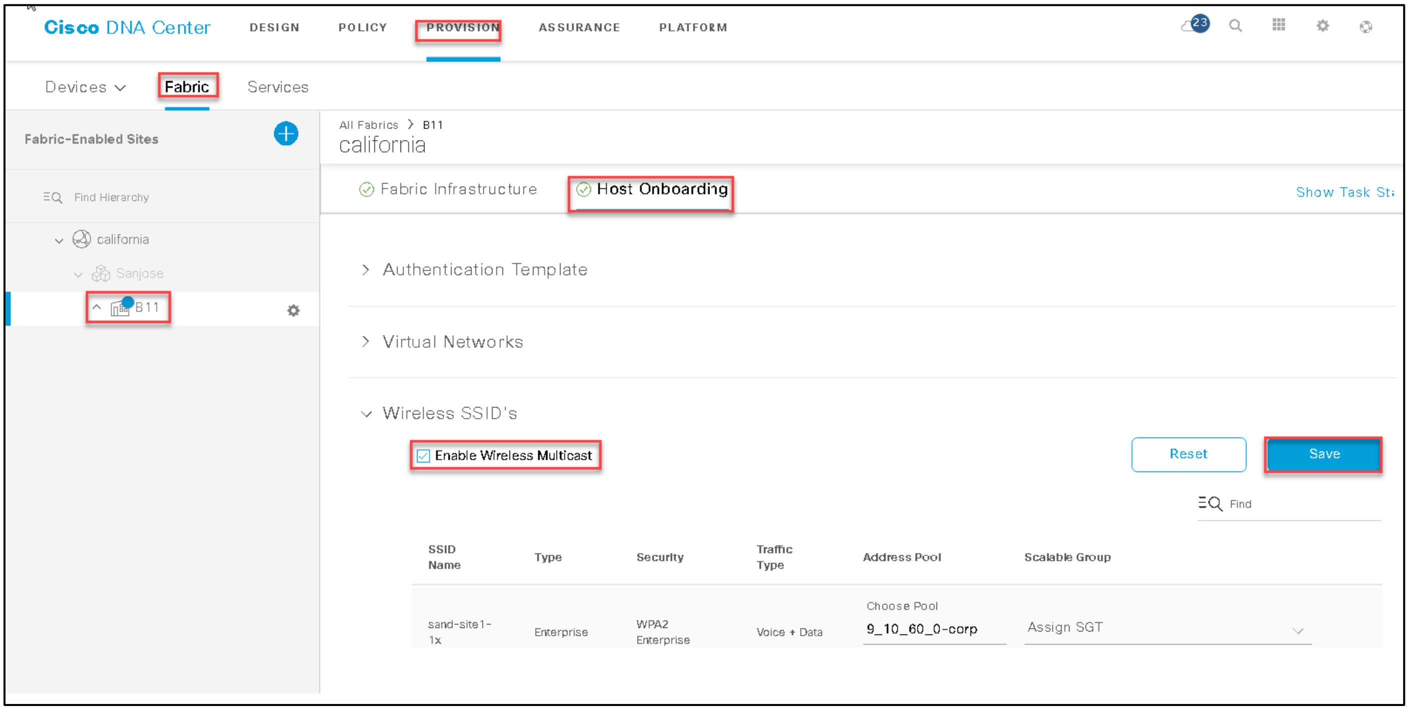
Multicast is complete!

Go to fabric site

Step9 After deploying multicast on the wired fabric infrastructure. The multicast needs to be enabled on the SD-Access wireless infrastructure. The option to enable multicast on wireless is located on the SSID configuration on the host onboarding page**.**

Navigate from Cisco DNA Center Homepage **:**

Provision->Fabric ->Fabric site->Host onboarding->Wireless SSID's



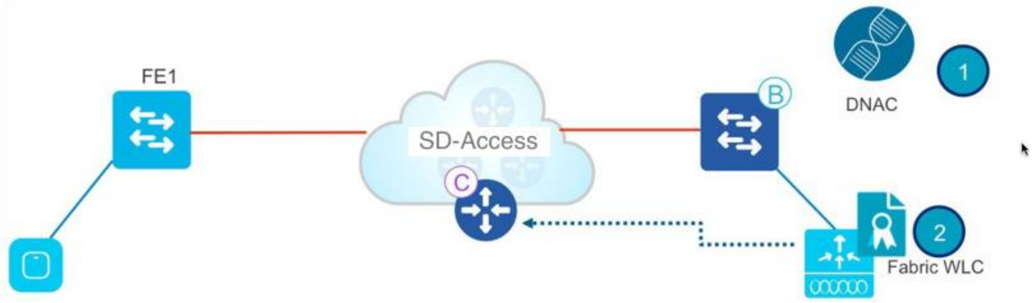
☑ Enable Wireless Multicast

SSID Name	Type	Security	Traffic Type	Address Pool	Scalable Group
sand-site1-1x	Enterprise	WPA2 Enterprise	Voice + Data	Choose Pool 9_10_60_0-corp	Assign SGT

This section describes and explains the basic operations of SD-Access Wireless to give you a clear understanding of what happens "behind the scenes" of the Cisco DNA Center. This flow assumes that you are done with the Design phase and just focuses on the implementation and provisioning phase.

Adding a WLC to the fabric

Figure 15. Adding a WLC to the fabric



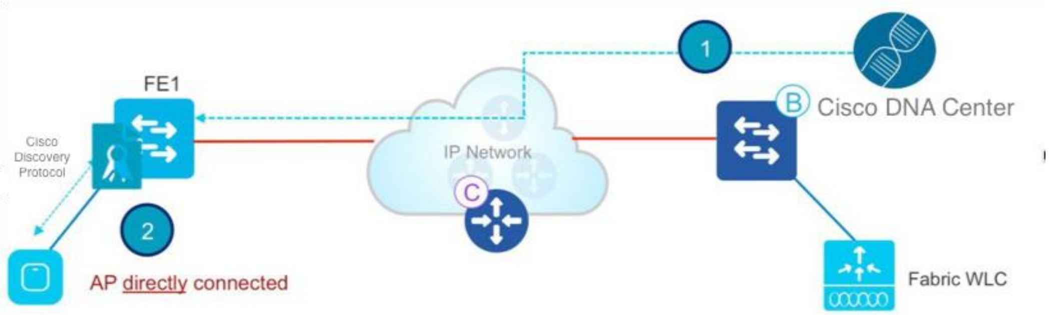
In Cisco DNA Center, first provision and then add the WLC to the fabric domain.

1. Fabric configuration is pushed to the WLC. The WLC becomes fabric aware. Most importantly, the WLC is configured with credentials to established a secure connection to the fabric control plane.

2. The WLC is ready to participate in SD-Access Wireless.

AP join flow

Figure 16. Connecting and discovering the AP

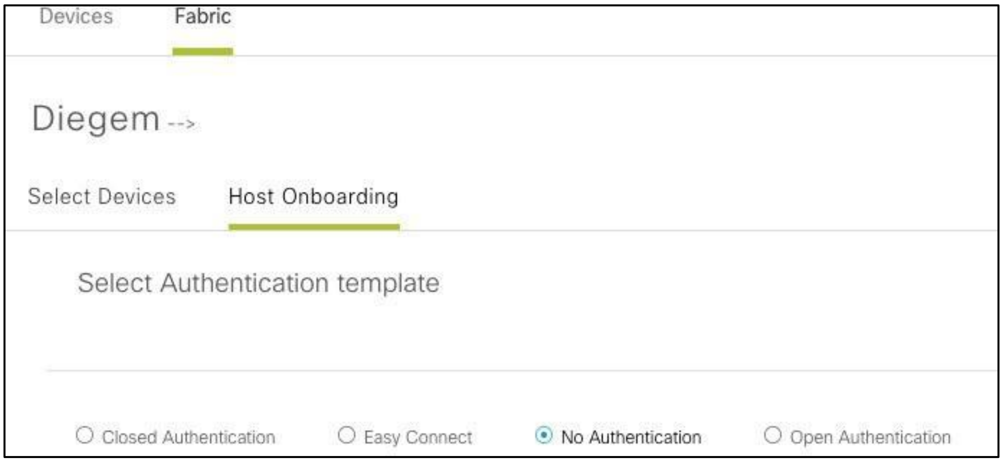


1. An admin user configures a pool in Cisco DNA Center to be dedicated to APs in the INFRA_VN (this means checking the AP Provisioning box in the pool definition). Cisco DNA Center pre provisions the AP VLAN and related template on the fabric edges. Cisco DNA Center 1.3 and above uses Autoconf while release 1.2 uses macro.
2. The AP is plugged in and powers up. The device classifier on FE discovers it's an AP through Cisco Discovery Protocol and applies the template configuration to assign the switch port to the right VLAN.

3. The AP gets an IP address through DHCP. It is a "special" wired host to the fabric.

NOTE: As of Cisco DNA Center, 1.3 Autoconf is used to identify the device as an Access point. Autoconf only works if the port is set as "No Authentication" mode. A switch port template is selected during host onboarding configuration. This is shown in the screenshot below.

If any other authentication template is selected, the admin user will have to statically map the APs' switch ports to the right IP pool. The AP's are also supported on closed authentication port, the workflow and the steps are defined in the AP onboarding section.



Devices Fabric

Diegem -->

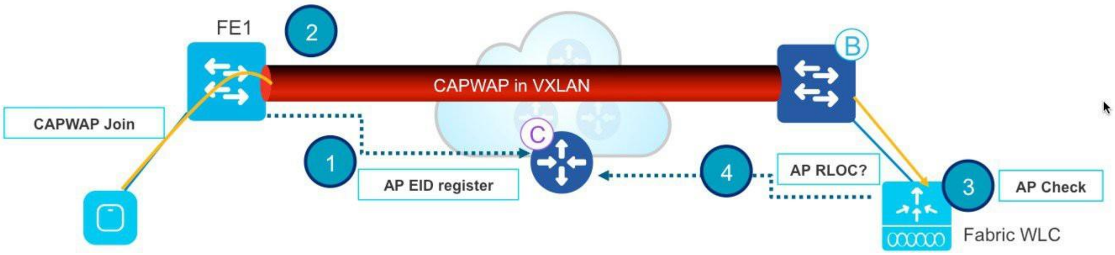
Select Devices Host Onboarding

Select Authentication template

○ Closed Authentication ○ Easy Connect ● No Authentication ○ Open Authentication

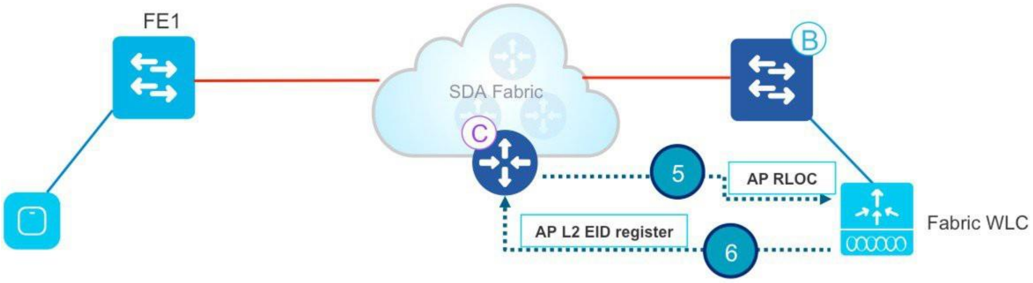
If any other authentication template is selected, the admin user will have to statically map the APs' switch ports to the right IP pool. The AP's are also supported on closed authentication port, the workflow and the steps are defined in the AP onboarding section.

Figure 17. AP onboarding



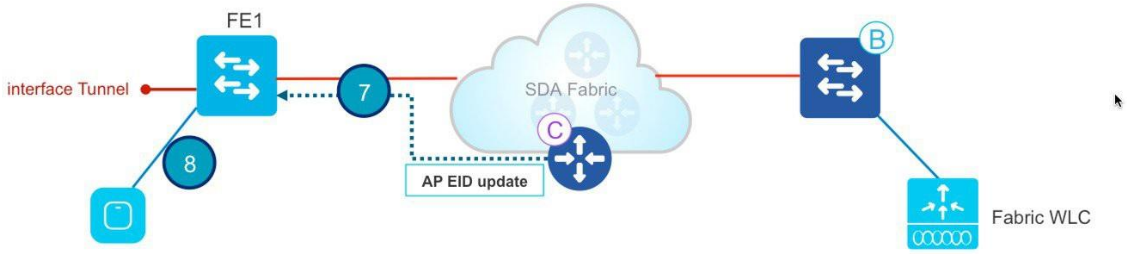
1. The fabric edge registers the AP's IP address in the control-plane node. The AP location is now known in the fabric.
2. The AP learns about the WLC using traditional methods (DHCP option 43, DNS, Plug and Play) and joins the WLC. The fabric AP joins as a Local mode AP.
3. The WLC checks whether the AP is fabric capable (that is, a Wave 2 or Wave 1 AP).
4. If the AP model is supported, the WLC queries the CP to learn whether the AP is connected to the fabric.

Figure 18. Exchanging RLOC and EID information



5. The CP replies to the WLC with the RLOC information. This means the AP is attached to the fabric and will be shown as fabric enabled in the WLC AP details.
6. The WLC does a Layer 2 LISP registration for the AP in the Host Tracking database (this registers the AP as a "special" secure client). This is used to pass important metadata information from the WLC to the FE.

Figure 19. Creating a VXLAN tunnel for the AP

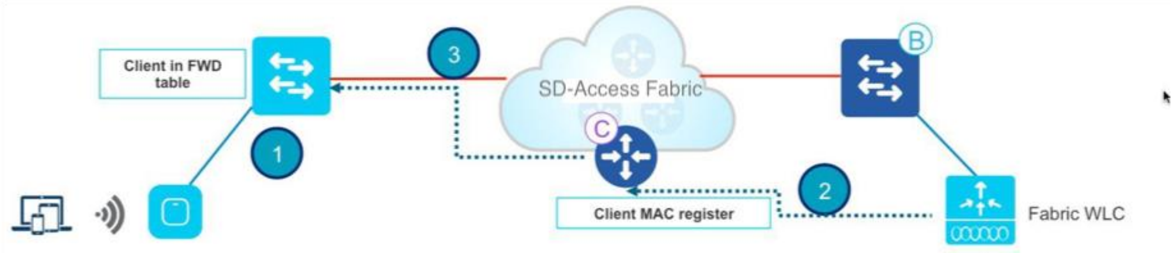


7. In response to this proxy registration by the WLC, the CP notifies the fabric edge and passes the metadata received from the WLC (a flag that says it's an AP and provides the AP's IP address).

8. The fabric edge processes the information, learns that this client is an AP, and creates a VXLAN tunnel interface to the specified IP address (optimization: the switch side is ready for clients to join).

Client onboarding flow

Figure 20. Authentication and policy retrieval

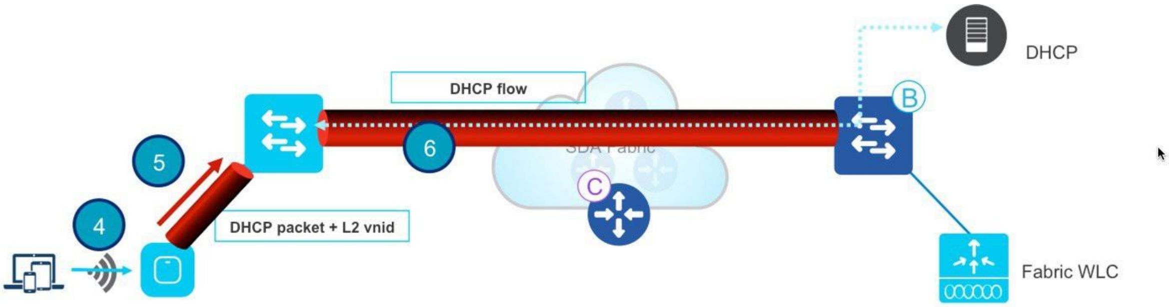


1. The client authenticates to a fabric-enabled WLAN. The WLC gets the client SGT from ISE (assuming the WLAN is configured for 802.1X authentication) and updates the AP with the client Layer 2 VNID and SGT. The WLC knows the RLOC of the AP from its own internal record (saved during the AP join process).

2. The WLC proxy registers the client's Layer 2 information in the CP; this is a LISP modified message to pass additional information, such as the client SGT.

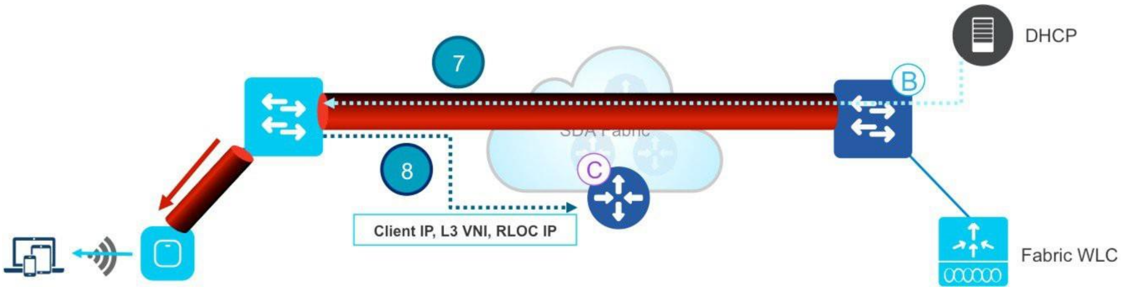
3. The CP notifies the FE, which adds the client's MAC address to the Layer 2 forwarding table and fetches the policy from ISE based on the SGT.

Figure 21. DHCP flow



4. The client initiates a DHCP request.
5. The AP encapsulates it in VXLAN with Layer 2 VNI information.
6. The fabric edge maps the Layer 2 VNID to the VLAN and VLAN interface and forwards DHCP in the overlay using anycast IP as the DHCP relay (the same as for a wired fabric client).

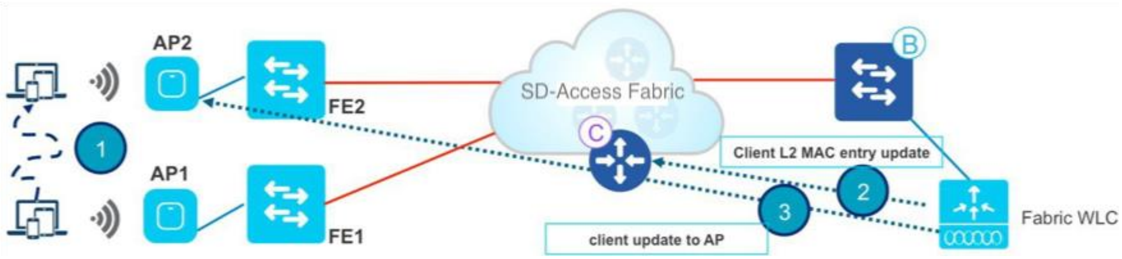
Figure 22. Completing the onboarding process



7. The client receives an IP address from DHCP.
8. DHCP snooping (and/or ARP for static) triggers the fabric edge to register the client to the Host Tracking database. This completes the client onboarding process.

Client roaming flow

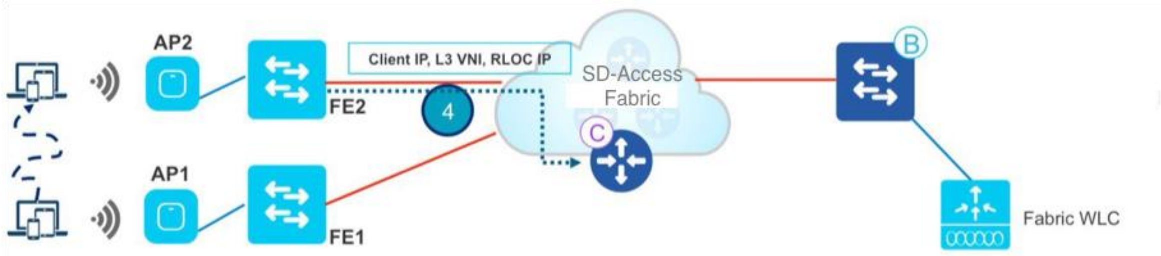
Figure 23. Updating the client information



1. The client roams to AP2 on FE2 (Interswitch roaming). AP2 notifies the WLC.
2. The WLC updates the forwarding table on the AP with the client information (SGT, RLOC IP address).

3. The WLC updates the Layer 2 MAC entry in the CP with the new RLOC for FE2.

Figure 24. Control plane notifications



4. The CP then notifies:
    - Fabric edge FE2 (the "roam-to" switch) to add the client MAC to the forwarding table pointing to the VXLAN tunnel
    - Fabric edge FE1 (the "roam-from" switch) to do cleanup for the wireless client
    - The fabric border to update the internal RLOC for this client

5. The FE will update the Layer 3 entry (IP address) in the CP upon receiving traffic.

    Roam is Layer 2, as FE2 has the same VLAN interface (anycast gateway).

Designing the wireless integration in SD-Access

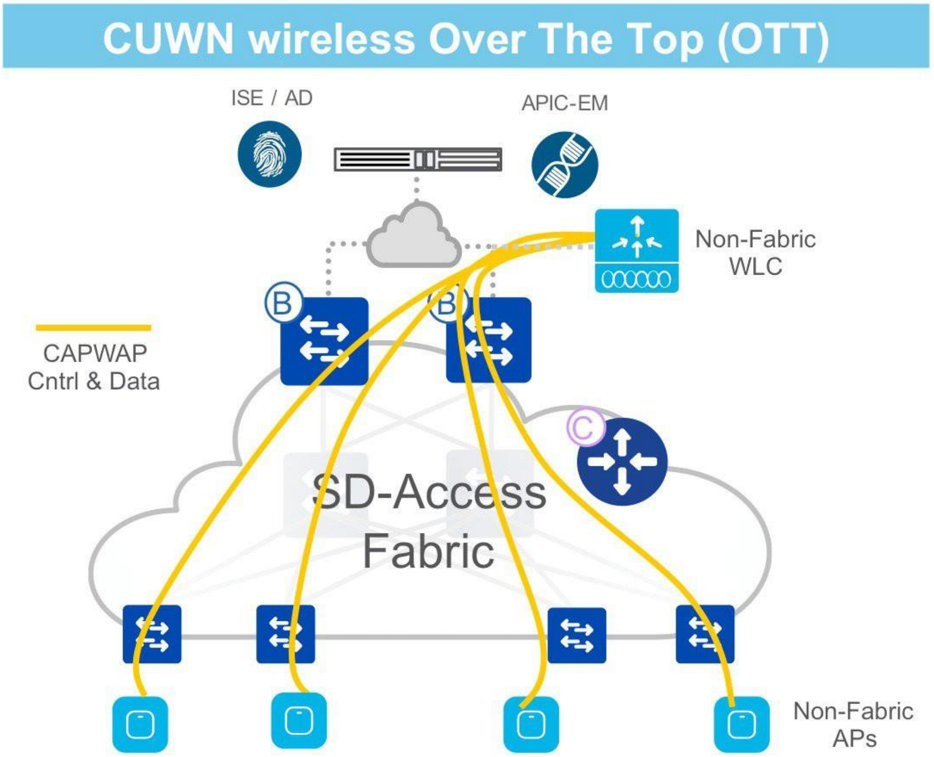
As mentioned earlier, there are two possible designs for deploying wireless with an SD-Access fabric:

- Cisco Unified Wireless Network wireless OTT: The SD-Access fabric is just an IP transport network, and wireless is a pure overlay.
- SD-Access Wireless: Wireless is integrated into SD-Access and can leverage all the advantages of the fabric.

Cisco Unified Wireless Network wireless OTT

In this case traditional wireless is carried on top of the SD-Access fabric. This mode is important as a migration step for customers that decide to implement SD-Access first on the wired network and then plan the wireless integration.

Figure 25. Cisco Unified Wireless Network wireless OTT



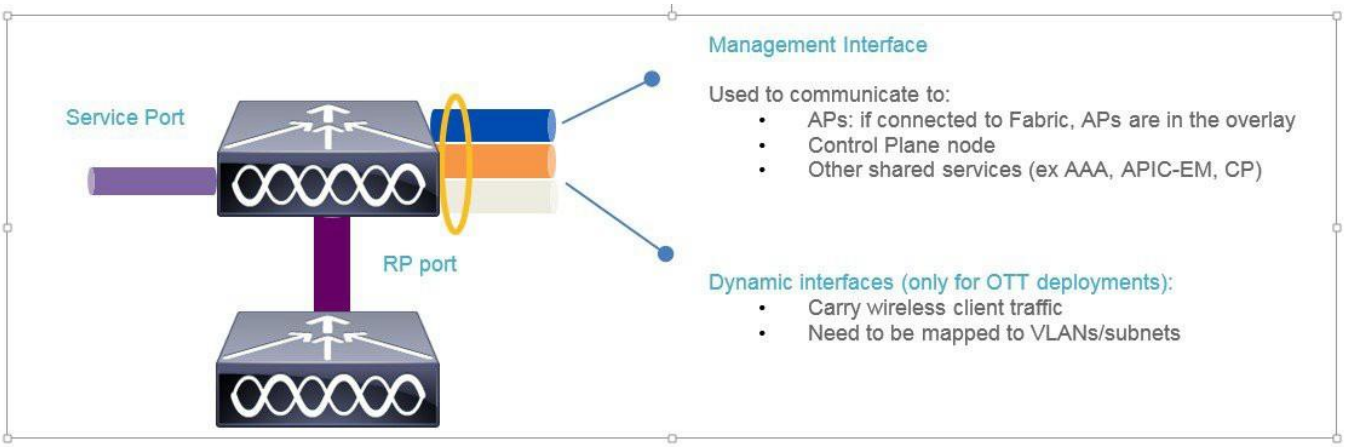
- A traditional Cisco Unified Wireless Network architecture with CAPWAP is used for the control plane and data plane, terminating at the WLC (for Centralized mode).
- The SD-Access fabric is just a transport in the wired infrastructure between the APs and the WLC.
- This is a possible migration step to full SD-Access adoption.

Before considering the different design considerations for the two deployment types. let’s clarify what interfaces of the WLC are used and how they are used in the different deployments.

WLC interfaces

For both SD-Access integration modes, let's consider the WLC interfaces as they apply to SD-Access Wireless and OTT.

Figure 26. WLC interface



Management Interface

Used to communicate to:

- APs: if connected to Fabric, APs are in the overlay
- Control Plane node
- Other shared services (ex AAA, APIC-EM, CP)

Dynamic interfaces (only for OTT deployments):

- Carry wireless client traffic
- Need to be mapped to VLANs/subnets

- WLC is connected in the underlay network (global routing table) outside the fabric network.

- The AP’s, when connected to a fabric network, are assumed to be in the overlay. In other words, the ports of a fabric edge are all fabric enabled. It is not supported to have some ports connected in the overlay and other ports connected in the underlay.
- The management interface is used, as usual, for the WLC-to-APs CAPWAP control channel and to talk to shared services such as AAA, Cisco DNA Center, etc.
- When deployed using SD-Access Wireless, the management interface is also used to integrate with the control-plane node.
- The redundancy port (RP) is used for high availability (HA) communication between an active and standby HA pair to provide seamless and stateful switchover in the event of a box or network failure.
- The dynamic interfaces are used only if wireless is deployed over the top, meaning that the fabric infrastructure is just a transport for the CAPWAP control and data channels to be transported back to the WLC for centralized processing.
- The service port is used for out-of-band management, as usual.

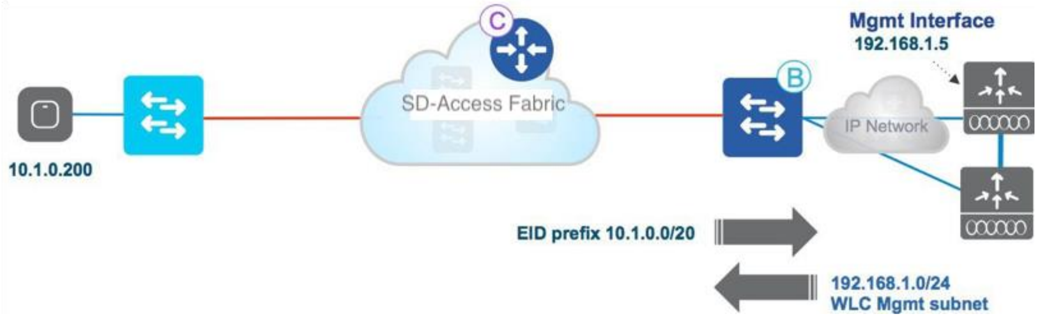
Cisco Unified Wireless Network wireless OTT network design

First of all, what is Cisco Unified Wireless Network wireless OTT? In this mode, traditional CAPWAP tunnels between the APs and WLC run as overlays to the fabric network. In other words, the fabric is a transport for CAPWAP. Why would you deploy Cisco Unified Wireless Network wireless OTT? There are two primary reasons:

1. The OTT solution can be a migration step: Customers want or need to first migrate the wired infrastructure to the SD-Access fabric and keep the wireless network “as is,” meaning not touching the way their wireless works today. This could be the result of different IT operations teams managing the wired and wireless infrastructure, a different buying cycle that determines an upgrade to the wired network first, or simply that the IT team wants to first get familiar with fabric on the wired side before they integrate the wireless part.
2. Another reason for deploying wireless OTT could be that customer doesn’t want or cannot migrate to fabric for wireless. This might be because they have a majority of older APs (802.11n or older) that are not supported with SD-Access, or the customer might require a certification of the new WLC software required to run SD-Access Wireless (8.5 and above), or the customer may simply want to leave the wireless “as is” and not touch it.

Let's consider some of the most important design considerations for each component.

Figure 27. WLC connection

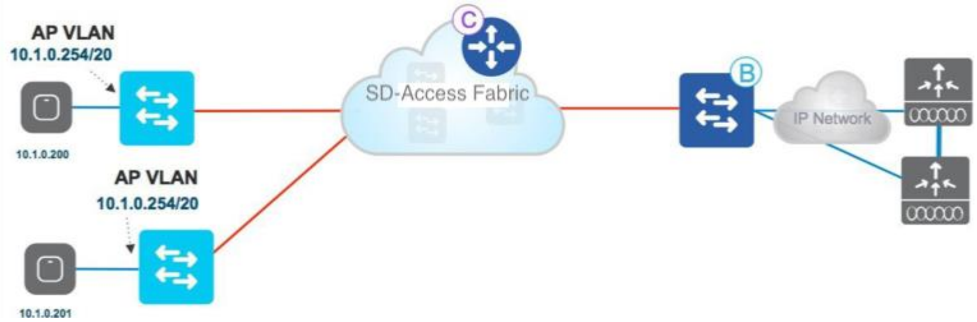


The recommendation is to connect the WLC (or WLCs for redundancy) outside the fabric, as shown in Figure 27. The WLC can also be connected to the border node of the Cisco SD-Access solution, the configuration for the same has to be done manually on the border node. Usually the WLC is connected in a centralized place in the network (data center or shared services), so, realistically, the WLC is not connected to a fabric edge node, which is usually an access switch.

Since the WLC sits outside the fabric, the border node is responsible for providing reachability between the management interface subnet (192.168.1.0/24 in this example) and the APs’ IP pool (10.1.0.0/16 in this example), so that the CAPWAP tunnel can form and the AP can register to the WLC. In Cisco DNA Center 1.3, the APs reside in INFRA_VRF, which is mapped to the global routing table, so route leaking is not needed.

Access points

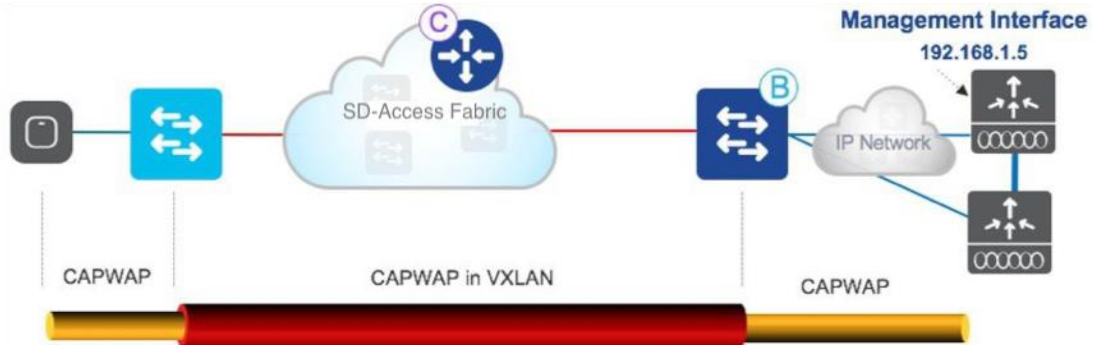
Figure 28. AP VLANs



Access points are simply wired hosts to the fabric infrastructure, and hence are connected to the overlay space on fabric edge switches and assigned a specific pool in the EID space. One of the advantages of fabric is that all the APs can be assigned to one big subnet that is the same across the campus, simplifying subnet design and hence the onboarding operations.

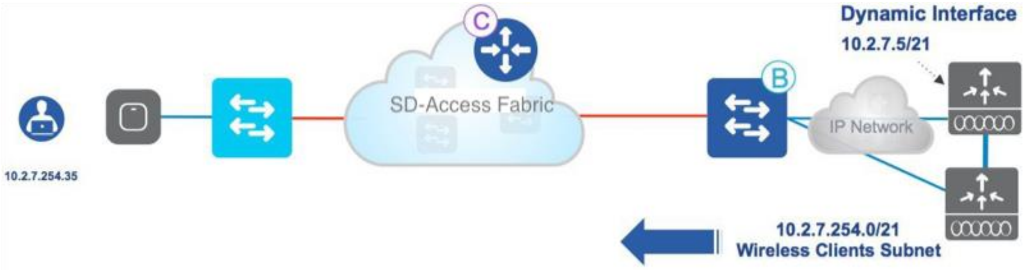
Since APs are like wired clients, they get registered in the fabric control plane node by the fabric edge switch they are connected to; hence their location will be made known in fabric and the APs will be reachable. At this point, the CAPWAP tunnel is formed from the AP to the WLC over the fabric, as shown in Figure 29.

Figure 29. CAPWAP tunnel from AP to WLC



Wireless LANs

Figure 30. Wireless LAN connections



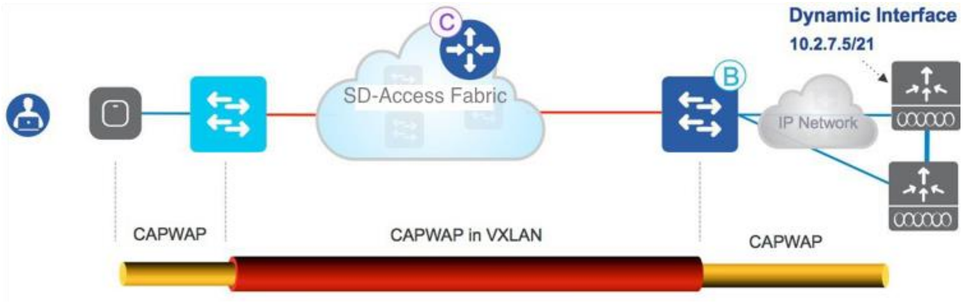
As mentioned, wireless works “as is,” meaning that wireless SSIDs on the WLC are mapped to a VLAN/subnet at the WLC in the form of dynamic interfaces, and wireless traffic enters the wired network at the WLC and is routed from there.

The border node advertises the wireless client subnets to the fabric so that connectivity can be established between a fabric host and a wireless client.

Client traffic flow

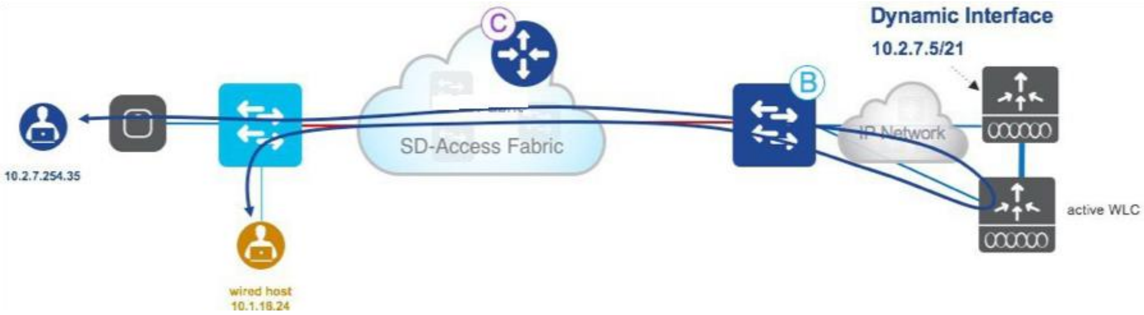
As a wireless client sends some traffic, the CAPWAP tunnel is built from the AP to the WLC. From the AP, the CAPWAP traffic hits the fabric edge switch, gets encapsulated in the VXLAN, and is forwarded to the border. The outer VXLAN header is removed and the underlying CAPWAP packet is forwarded to the WLC.

Figure 31. Client traffic flow via CAPWAP tunnel



As with the Cisco Unified Wireless Network, clients are authenticated and onboarded by the WLC, and the wireless client traffic is external to the fabric. Figure 32 shows the traffic flow for a communication between a wireless client and a local fabric wired host.

Figure 32. Traffic flow between a wireless client and a local fabric wired host



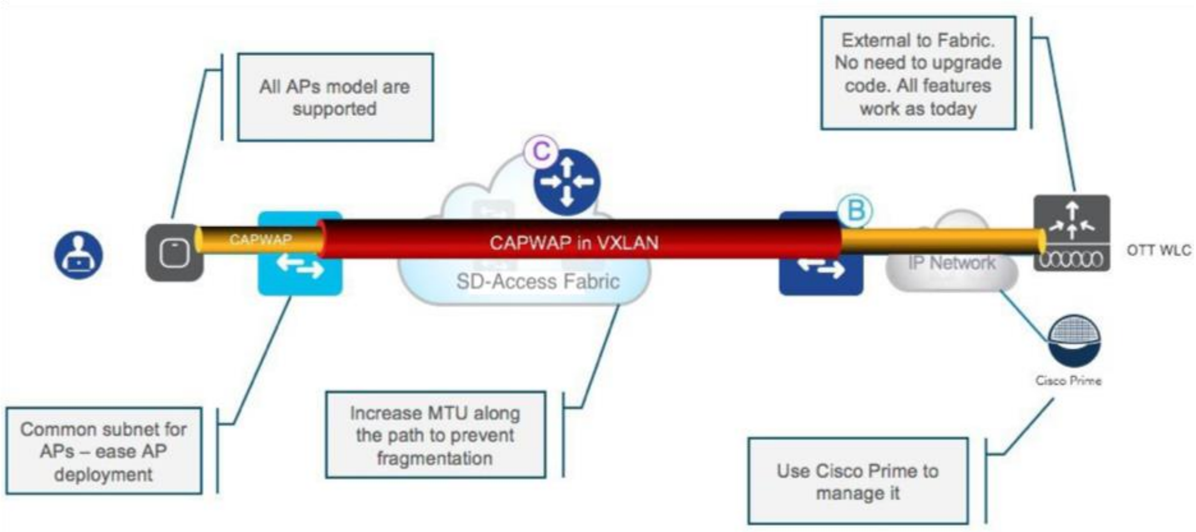
The wireless traffic will go all the way to the WLC, and will be bridged at the WLC dynamic interface VLAN and routed back to the fabric client through the border. For wireless, this is the same thing that happens today with a normal wired network; for the fabric, it is a fabric host communicating to a known destination external to the fabric.

Wireless as an overlay (OTT) – design considerations

Let's recap some of the important design considerations for OTT mode:

- All APs and WLC models are supported. Since wireless is not integrated into the fabric, there are no requirements regarding the hardware and software models.
- The WLC is connected external to the fabric and can be on any code version.
- We recommend increasing the maximum transmission unit (MTU) along the path to prevent fragmentation of packets due to double (CAPWAP in VXLAN) encapsulation. This is done automatically if all the switches in the path are Cisco and support jumbo frames.
- At FCS, the only mode supported as OTT is Centralized.
- At FCS, use Cisco Prime to manage OTT wireless networks.

Figure 33. Design considerations for OTT mode:


All APs model are supported
External to Fabric. No need to upgrade code. All features work as today
C
B
CAPWAP
CAPWAP in VXLAN
SD-Access Fabric
IP Network
OTT WLC
Cisco Prime
Common subnet for APs – ease AP deployment
Increase MTU along the path to prevent fragmentation
Use Cisco Prime to manage it

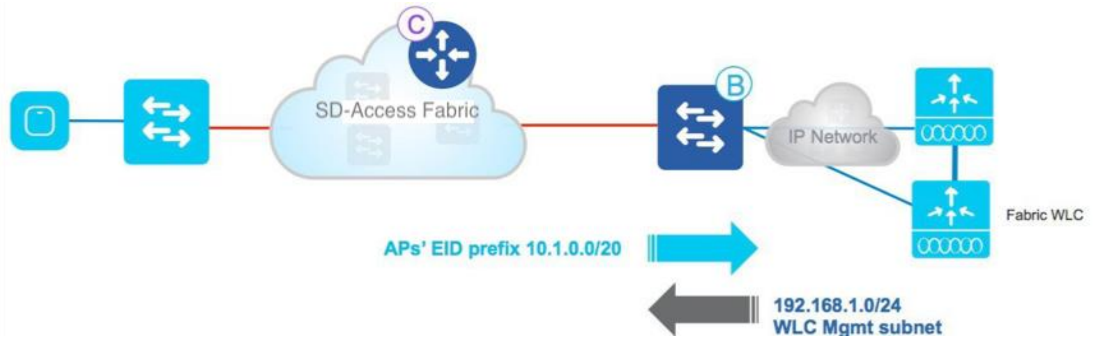
SD-Access Wireless network design

To gain all the advantages of SD-Access fabric, you should choose the integrated design and hence the SD-Access Wireless solution. From an architecture perspective, the integration brings three main advantages:

- Simplified management and control plane: Cisco DNA Center provides the necessary automation to bring up the fabric and configure the wireless integration in a few clicks. The centralized wireless control plane (based on CAPWAP) provides the same functionalities as today's Cisco Unified Wireless Network controller.
- Optimized data plane: The data plane is distributed without the usual caveats that this usually brings; thanks to the fabric, there is no VLAN spanning multiple access switches, and subnetting is simplified.
- Integrated policy and segmentation from end to end: Policy is not an afterthought; it is integrated from the ground up in the architecture. The VXLAN header carries both the VRF (VNID) and SGT information, providing end-to-end hierarchical segmentation.

Let's briefly analyze the design aspects of the wireless integrated solution.

Figure . WLC connecting externally to the fabric



The recommendation is to connect the WLC (or WLCs for redundancy) externally to the fabric, as shown in Figure 35.

Usually the WLC is connected in a centralized place in the network (data center or shared services), so it's realistic that the WLC is not connected to a fabric edge node, which is usually an access switch.

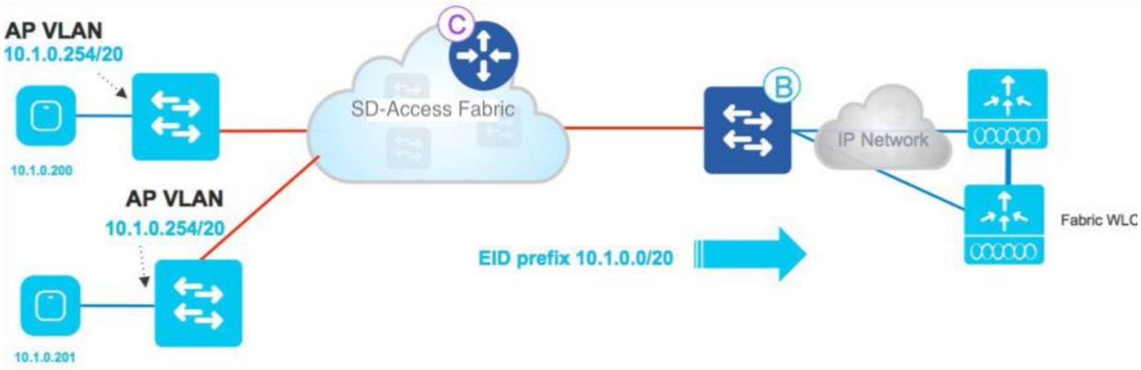
Since the WLC sits outside the fabric, the border node is responsible for providing reachability between the management interface subnet (192.168.1.0/24 in this example) and the APs' IP pool (10.1.0.0/16 in this example) so that the CAPWAP tunnel can form and the AP can register to the WLC. The APs reside in INFRA_VRF, which is mapped to the global routing table, so route leaking is not needed.

Also, the WLC needs to be collocated with the access points. The requirement is the same as for Local mode APs in Cisco

Unified Wireless Network: The maximum latency between APs and WLC needs to be less than 20 ms, which usually means that the WLC cannot be sitting across a WAN from the APs.

Access points

Figure 36. Access points in SD-Access Wireless

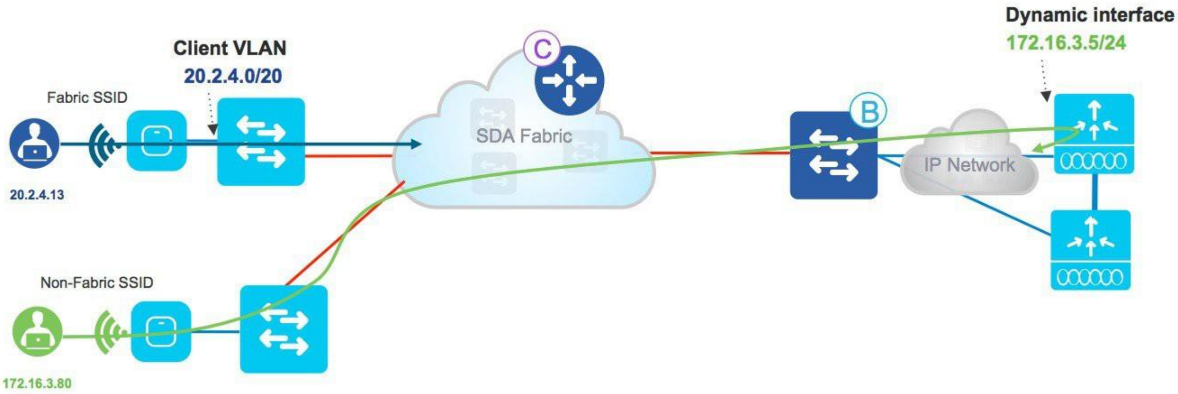


In SD-Access Wireless, APs need to be connected directly to the fabric edge nodes. Access points are “special” wired hosts to the fabric infrastructure and hence are connected to the overlay space on fabric edge switches and assigned a specific pool in the EID space. One of the advantages of fabric is that all the APs can be assigned to one big subnet that is the same across the campus, simplifying subnet design and hence the onboarding operations.

Since APs are like wired clients, they get registered in the fabric control plane node by the fabric edge switch they are connected to, and hence their location will be made known in the fabric and the APs will be reachable. The AP will form a CAPWAP tunnel to the WLC for control-plane functionalities in the same way that has been described for OTT design.

Wireless LANs

Figure 37. Wireless LAN in SD-Access Wireless



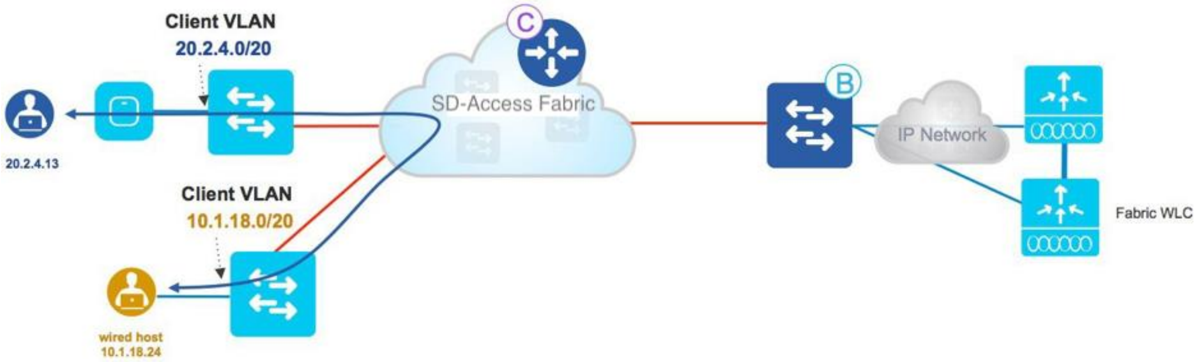
Fabric capability is enabled on a per-WLAN basis. For WLANs that are fabric enabled, the client traffic is distributed and will not go to the centralized controller but will be encapsulated in VXLAN at the AP and sent to the first-hop switch.

Centralized CAPWAP WLANs can coexist with fabric-enabled WLANs on the same or different APs using a common fabric-enabled WLC. This is called “mixed mode,” and with Cisco DNA Center 1.1 it is supported for WLC deployments with no preexisting fabric or Cisco Unified Wireless Network wireless configuration, so it is for new deployments only.

Client flow

For fabric-enabled SSIDs, the wireless client traffic is distributed at the switch, so there is no hairpinning to the centralized controller. The communication to wired clients is directly through the fabric and hence is optimized.

Figure 38. Client flow in SD-Access Wireless



Client subnets are distributed at the fabric edge switches, and there is no need to define dynamic interfaces and client subnets at the WLC. Instead, client subnets are defined and mapped to the VLAN with an anycast gateway at all fabric edge switches. This means that no matter where the wireless client connects, it will be able to talk to the same gateway for its subnet, which means that the client will be able to retain its original IP address everywhere; in other words, all wireless roams in the fabric are Layer 2 roams.

Figure 39. Client subnets in SD-Access Wireless

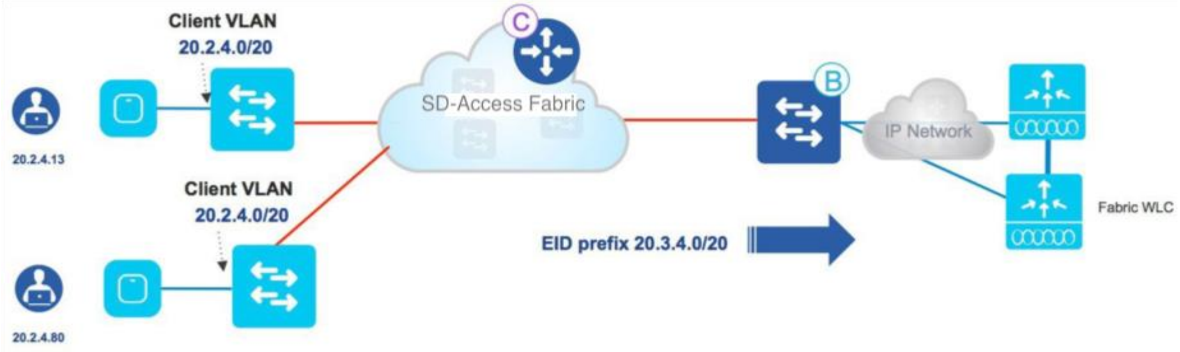
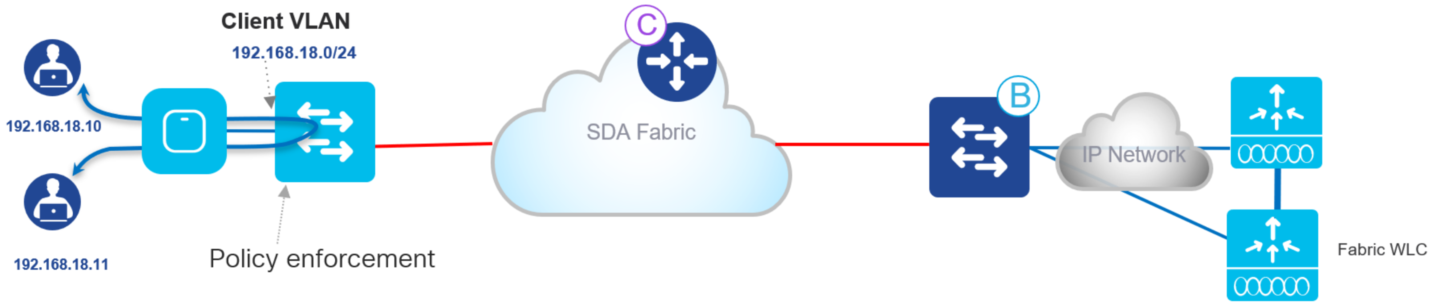


Figure 39. Client traffic flow in SD-Access Wireless on the same SSID/VLAN



Client subnets are distributed at the fabric edge switches, and there is no need to define dynamic interfaces and client subnets at the WLC. Instead, client subnets are defined and mapped to the VLAN with an anycast gateway at all fabric edge switches. This means that no matter where the wireless client connects, it will be able to talk to the same gateway for its subnet, which means that the client will be able to retain its original IP address everywhere; in other words, all wireless roams in the fabric are Layer 2 roams.

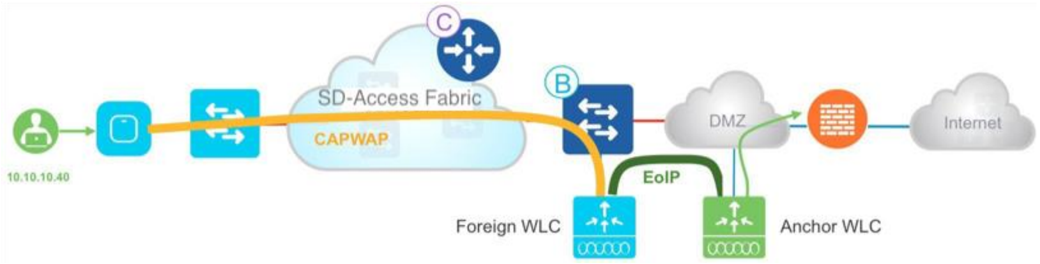
SD-Access Wireless guest access design

When considering guest design, the integration with fabric offers three different solutions:

- The OTT solution leveraging a guest anchor controller
- A dedicated guest virtual network
- A dedicated guest fabric domain

OTT solution leveraging Cisco Unified Wireless Network guest anchor

Figure 40. OTT solution using a guest anchor controller



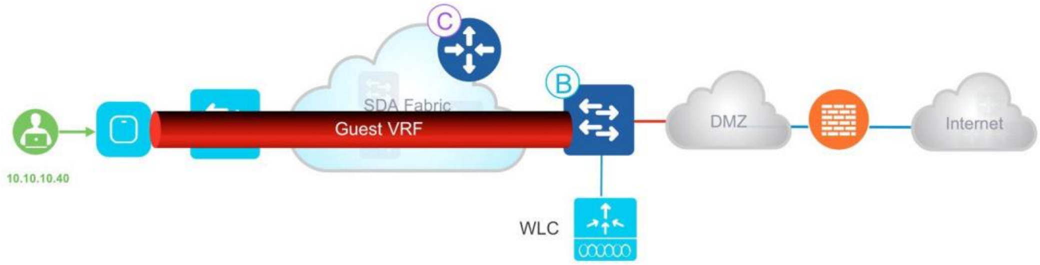
You can continue to leverage your investment in guest anchor controllers by deploying the guest wireless network as OTT. The WLAN for guests will be configured to be anchored at a guest anchor controller in the DMZ, and the traffic will be an overlay to the fabric. This well-proven Cisco Unified Wireless Network solution protects the customer investment and is particularly suited for brownfield deployments. Of course, this solution has the limitations partially inherited from the Cisco Unified Wireless Network solution:

- It is limited to 71 guest tunnels.

- There is a separate solution for wired guests, managed differently from the anchor WLC.

Dedicated VN for guest

Figure 41. Dedicated guest VN



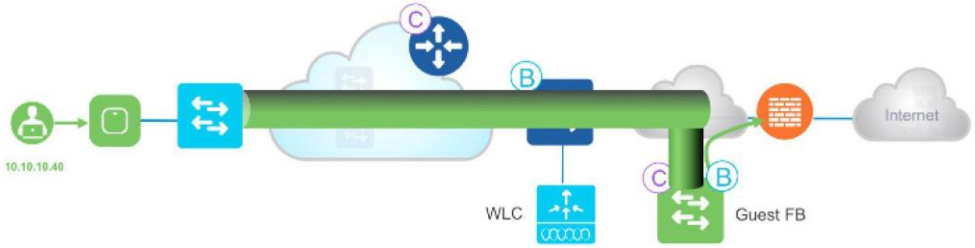
In this design, the guest network is just another VN in the SD-Access Fabric, so end-to-end fabric segmentation (using a VNI, and SGTs for different guest roles if needed) is used to separate the guest data plane from the other enterprise traffic. It’s configured through Cisco DNA Center by creating a guest VN, defining the IP pools, and associating the SSID to one or more pools for guests. One of the main advantages of this approach over the previous solution is that it is a consistent solution and policy for wired and wireless guest users.

Guest as a separate fabric domain

If you require complete isolation for the guest network, not only for the data plane traffic but also in terms of the control plane, you can configure a dedicated guest control plane and border (so essentially a dedicated fabric domain) in Cisco DNA Center to manage guest users.

In this solution the traffic is still encapsulated at the AP in the VXLAN to the fabric edge switch, but then the FE is configured to use a different border node. This border node can reside in your DMZ, providing complete traffic isolation, similar to the guest anchor solution. The guest users will be registered in a dedicated CP (that may be colocated with the border or not), and the users will get an IP address in the DMZ.

Figure 42. Guest control plane and border



Similar to the previous VN solution, this design provides policy consistency for wired and wireless guests. The choice of a guest control plane and border will depend on the scalability of the solution.

The handoff from the guest border is a manual process, the administrator can choose the appropriate protocol including static routes to do the handover to the external node in the DMZ.

Multicast in SD-Access Wireless

Here are some important things to know about multicast in SD-Access Wireless:

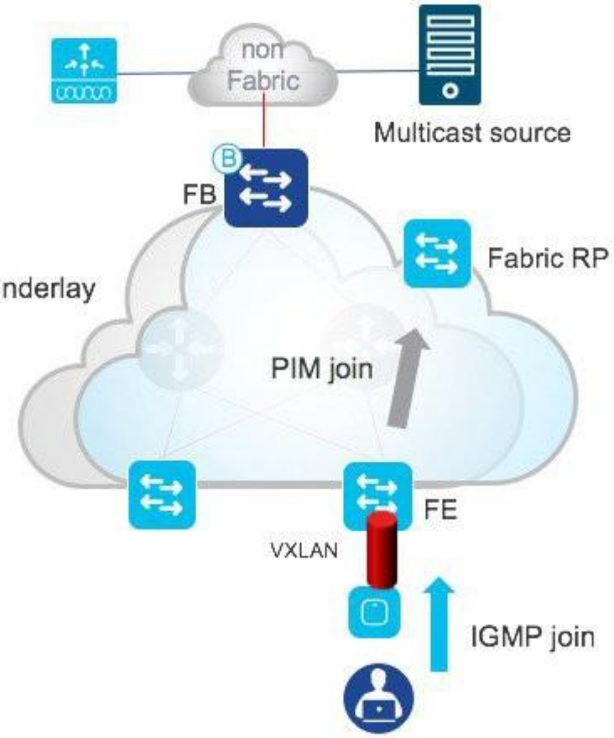
- Multicast traffic is transported in the overlay, in the EID space, for both wired and wireless clients.
- To enable multicast for wireless, Global Multicast mode and Internet Group Management Protocol (IGMP) snooping need to be enabled globally on the WLC.
- With Cisco DNA Center 1.3, multicast traffic forwarding in a fabric uses two methods: the head-end replication and native forwarding. These methods differ from each other on how the multicast traffic is forwarded in the underlay. For head-end replication the underlay network doesn't need to have multicast-enabled. This method is not optimal, as multicast traffic coming into the fabric is replicated in multiple unicast VXLAN tunnels, one for each fabric edge node that has some multicast receiver attached. In the case of native multicast the underlay needs to have multicast-enabled. This method is an efficient, as multicast traffic of the overlay is forwarded in an underlay multicast. The replication of packets is done by the network based on where the interested receivers are.

Let's now examine how multicast works:

- The multicast client (receiver) is in the overlay. The multicast source can be outside the fabric or in the overlay as well (in Figure 43, the source is shown outside the fabric).
- PIM sparse mode (PIM-SM) or PIM source-specific multicast (PIM-SSM) needs to be running in the overlay (and so needs to be enabled per VRF).
- The client sends an IGMP join for a specific multicast group.
- The AP encapsulates it in the VXLAN and sends it to the upstream switch.
- The fabric edge node receives it and does a PIM join towards the fabric rendezvous point (RP) (assuming PIM-SM is used).
- The RP needs to be present in the overlay as part of the endpoint IP space.

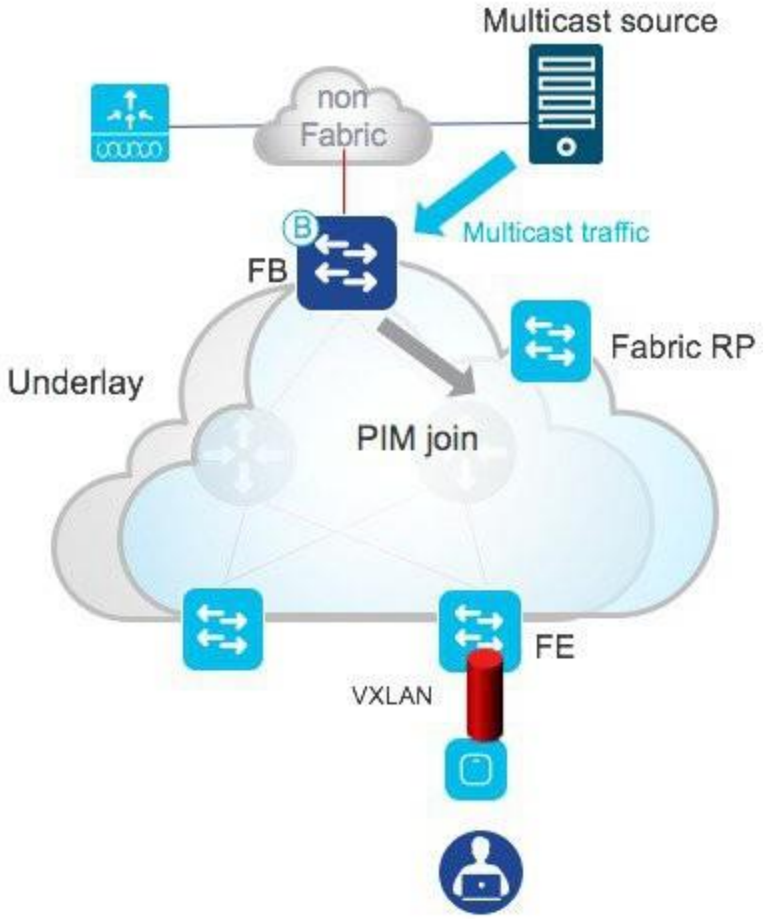
- Figure 43 illustrates the above steps.

Figure 43. Multicast in SD-Access Wireless



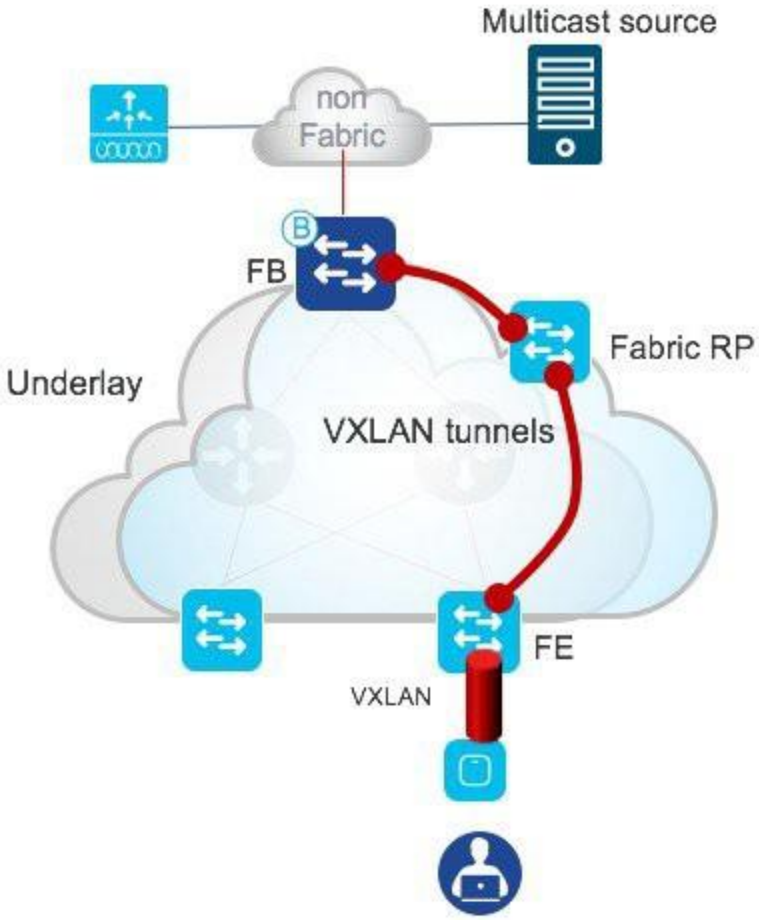
- Being outside of the fabric, in this example the multicast source will send the multicast traffic on the interfaces toward the fabric border which is the designated router for that segment.
- The FB receives the traffic and does a PIM join toward the RP (assuming PIM-SM is used).
- The RP now has the source and receiver information for that multicast group.

Figure 44. Multicast in SD-Access Wireless
(North to South)



- The RP now has the source and receiver information for a particular multicast group.
- The FB will send the multicast source traffic over a VXLAN tunnel to the RP, and the RP will forward that traffic to the FE over another VXLAN tunnel.
- The FE receives the VXLAN packets, decapsulates them, applies policy, and then forwards them again to the AP over a VXLAN tunnel.
- The AP removes the VXLAN header and sends the original IP multicast packet into the air.

Figure 45. Multicast in SD-Access Wireless



- Once the first multicast packet is delivered to the FE, the shortest path failover (SPT) happens and the traffic is forwarded between the FB and the FE directly.
- The FE knows that the FB owns the multicast source, based on the first multicast packet received, and sends a PIM join directly to the FB for that multicast group.
- FB now knows which FEs have clients that requested the specific multicast group.
- It performs headend replication or native multicast, and VXLAN encapsulates the multicast traffic and forwards it to the interested FEs.
- The multicast traffic is sent in the overlay.
- FE receives the VXLAN packets, decapsulates them, applies policy, and then forwards them again to the AP.
- The AP removes the VXLAN header and sends the original IP multicast packet into the air.

High availability in SD-Access Wireless

The most critical components of the SD-Access Wireless solution are the WLC and the control plane node. Compared to wired fabric clients, the control plane plays an even more important role for wireless, as it is critical in client roaming because it is responsible for keeping the updated client location information.

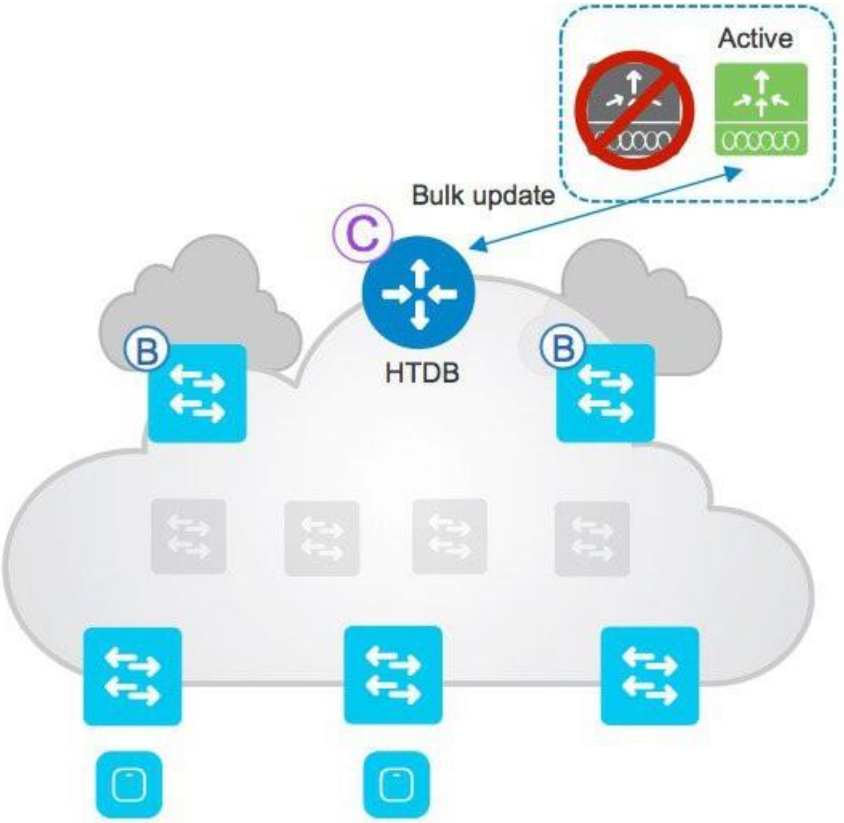
Both the WLC and the CP support high availability.

Controller redundancy

Controller high availability is supporting using both N+1 and SSO for the fabric-aware controller.

Stateful redundancy with SSO

Figure 46. Stateful switchover

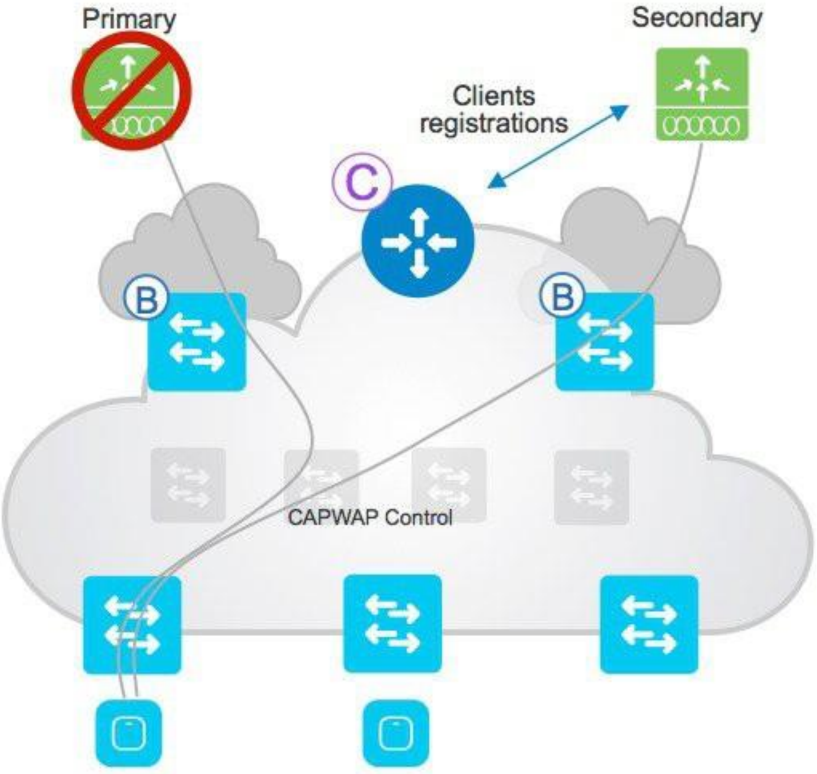


- The WLC SSO pair is seen as one node by the fabric.
- Only the active WLC interacts with the CP node.
- The fabric configuration and CP state are synced between the active and standby WLCs.
- Upon failure, a new active WLC will bulk update fabric clients to the Host Tracking database node (LISP refresh).
- APs and clients stay connected.

As discussed in the design section, at FCS the WLC is connected outside the fabric, so the usual consideration for connecting an SSO pair will apply: the bandwidth and latency requirements between the two controllers are the same as in the Cisco Unified Wireless Network architecture.

Stateless redundancy with N+1

Figure 47. N+1 redundancy



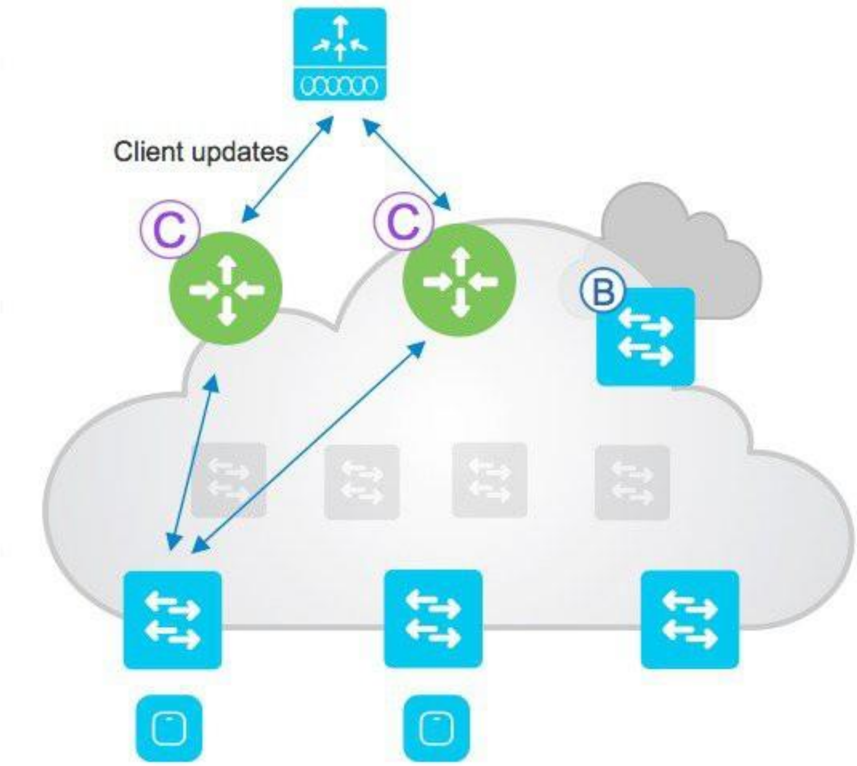
N+1 redundancy is supported if you don’t need stateful HA. N+1 redundancy is not automated till Cisco DNA Center 1.3; support for this functionality is on the Cisco DNA Center roadmap. Here are the important considerations:

- The AP is configured with primary and secondary.
- The AP and associated clients register with the primary.
- Upon primary failure, the AP disconnects and joins the secondary.
- Clients are also disconnected and join the secondary.
- The secondary performs new client registration in the Host Tracking database.

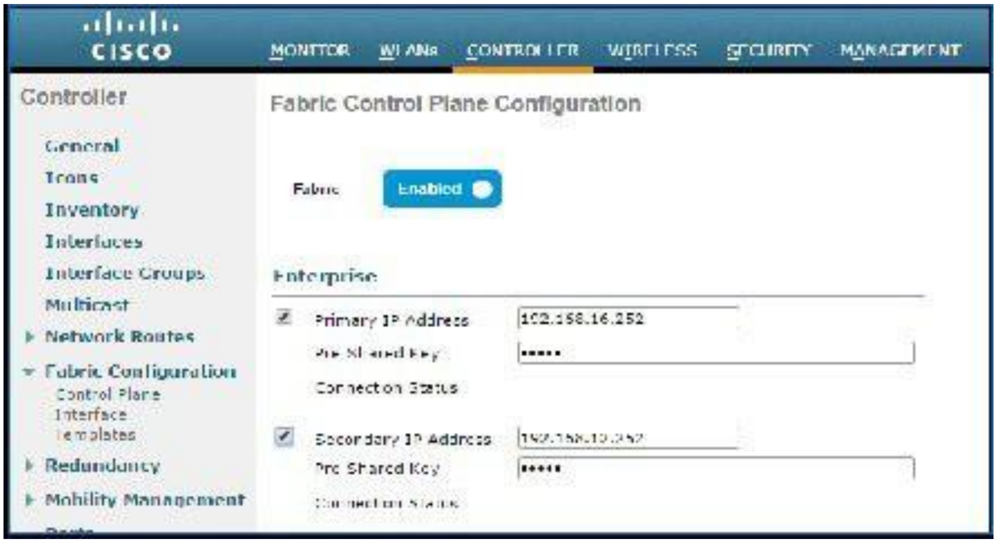
Note N+1 redundancy is not automated till Cisco DNA Center 1.3. Support for this functionality is on the Cisco DNA Center roadmap.

Control plane redundancy

Figure 48. Control plane redundancy



- Redundancy for the control plane node is supported in an active/active configuration. The WLC (and the fabric edges) are configured with two CP nodes and sync information to both
- If one CP node fails, all client information is available at the other CP node. Here is the configuration on the WLC for reference screenshot from Aire-OS:



Fabric Control Plane Configuration

Fabric: Enabled

Enterprise

☑ Primary IP Address: 192.168.16.252

Pre Shared Key: •••••

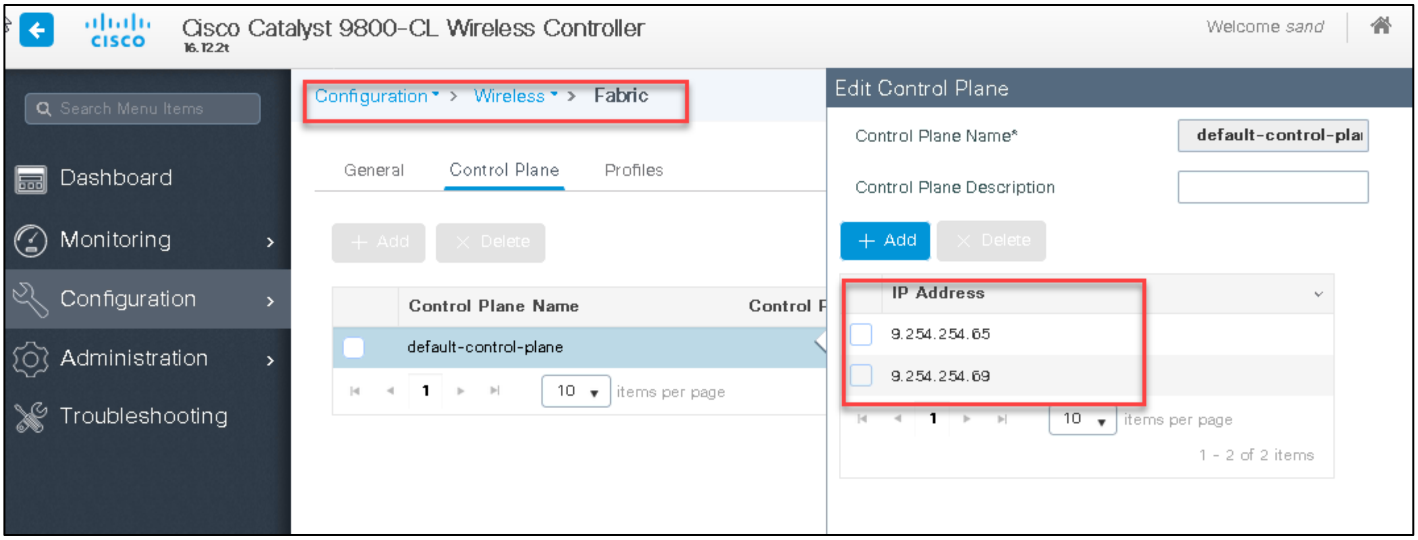
Connection Status

☑ Secondary IP Address: 192.168.10.252

Pre Shared Key: •••••

Connection Status

reference screenshot from Catalyst 9800 WLC:



Control Plane Name* default-control-pla

Control Plane Description

Control Plane Name
default-control-plane

IP Address
9.254.254.65
9.254.254.69

Appendix: SD-Access Wireless features deep dive

The following table captures some of the key features supported on the SD-Access Wireless architecture.

Table 1: Key features supported in the SD-Access Wireless architecture

Open/static Wired Equivalent Privacy (WEP)	Supported
Wireless Protected Access with preshared keys (WPA-PSK)	Supported
802.1X (WPA/WPA2)	Supported
MAC filtering	Supported
Local Extensible Authentication Protocol (EAP)	Supported
AAA override	Supported
Internal/external web authentication	Supported
Pre-authentication access control list (ACL)	Supported
IPv4 ACL for clients	Supported (SGTs are preferred and recommended)
Application Visibility and Control (AVC)	Supported*
Local profiling	Supported
RADIUS profiling	Supported
QoS profiles	Supported
Per-user bandwidth contracts	Supported
Wireless intrusion prevention system (wIPS)	Supported
Cisco Connected Mobile Experiences (CMX) integration	Supported
NetFlow export	Supported
HA SSO	Supported

*Wave 2 APs only

Let's examine some of the features to understand how they work in a fabric network.

AAA override

ISE can override the parameters Fabric Interface Name, ACL, QoS, and SGT on an SD-Access Wireless SSID.

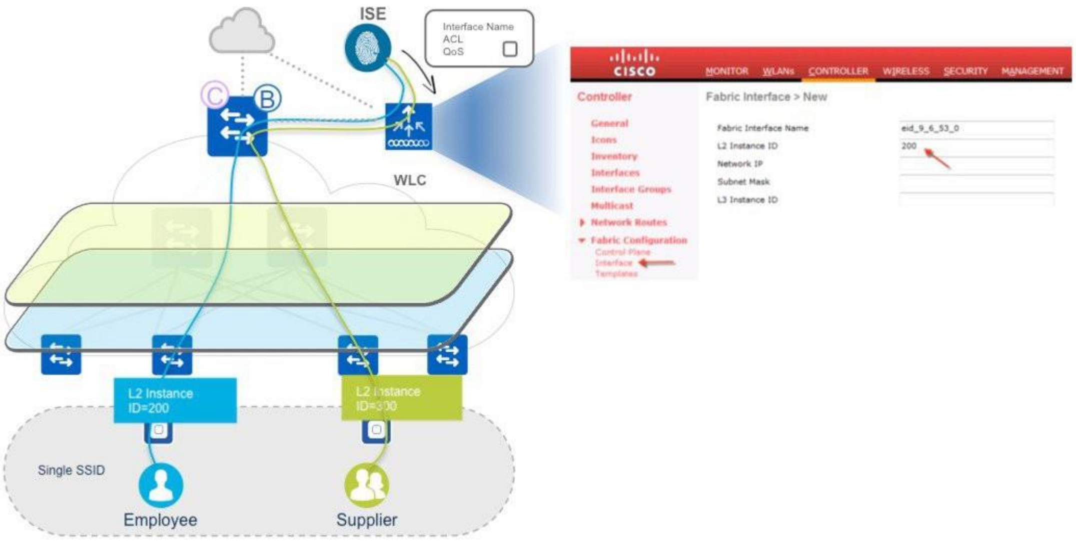
Fabric Interface Name override

What if you want to have the same SSID mapped to different pools/subnets based on client authentication and role? In Cisco Unified Wireless Network we use VLAN override for this, passing the VLAN ID (name or number) from the AAA server back to the WLC.

In fabric, the VLAN has only a local switch, and what the IP pool is mapped to is a Layer 2 VNID. This is the network identifier that is associated with a subnet/pool and, for wireless, with an SSID. The Layer 2 VNID is transported from the AP to the switch in the VXLAN header. The Layer 2 VNID is ultimately mapped to a VLAN locally at the fabric edge switch and to an SVI (anycast gateway) and hence to a Layer 3 VNID (VRF).

In SD-Access Wireless, we need to pass the Layer 2 VNID to differentiate different pools. Since ISE or other AAA doesn't use VNIDs directly, we use the Cisco Audio-Video Protocol (AVP) Aire-Interface-Name or Interface-Name to return a specific name at the time of client authentication. The client Layer 2 authentication always happens at the controller, so it's the WLC that talks to ISE, gets that interface name value, and maps it to a Layer 2 VNID.

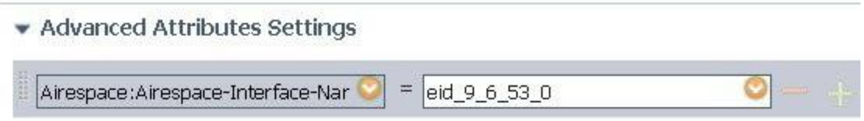
Figure 49. AAA override



Fabric Interface > New

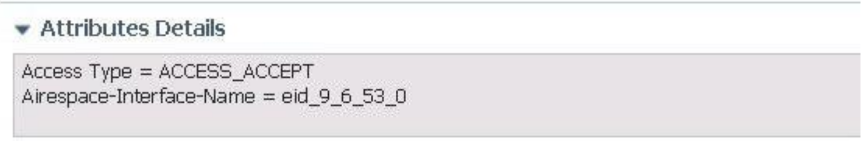
Fabric Interface Name eid_9_6_53_0
L2 Instance ID 200
Network IP
Subnet Mask
L3 Instance ID

In ISE the user needs to configure the specific group authorization profile to return the specific interface name, as you can see in the screenshot below, so when the user authenticates, ISE will return the specific attribute in the RADIUS ACCEPT_ACCEPT message.



Advanced Attributes Settings

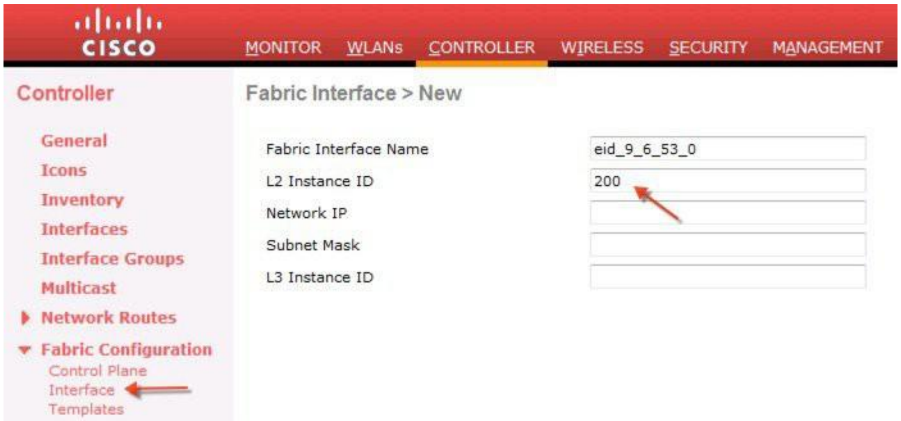
Airespace:Airespace-Interface-Nar = eid_9_6_53_0



Attributes Details

Access Type = ACCESS_ACCEPT
Airespace-Interface-Name = eid_9_6_53_0

The fabric interface name is then mapped to the Layer 2 instance ID, using the mapping shown below. Important: All this mapping and configuration happens automatically when you configure Cisco DNA Center.



Fabric Interface > New

Fabric Interface Name	eid_9_6_53_0
L2 Instance ID	200
Network IP	
Subnet Mask	
L3 Instance ID	

The Layer 2 instance ID is sent to the AP to embed it into the VXLAN header.

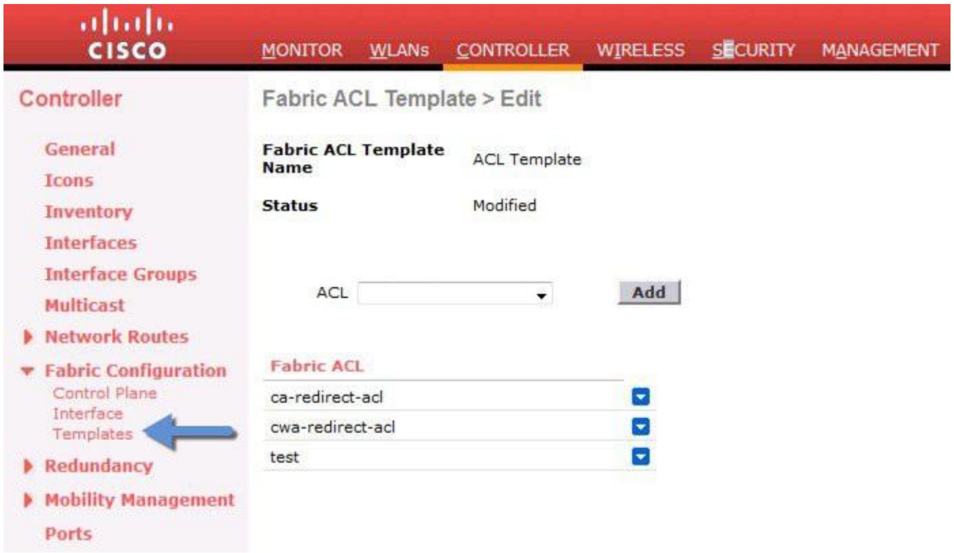
ACL and QoS profile AAA override

The fabric ACL on the WLC will be applied on the AP. The main difference between the local WLC ACL and the fabric ACL lies in the fact that fabric ACLs do not have a direction associated with them. On the fabric SSID, a flex ACL will be configured on the SSID. The same ACL will be applied on both ingress and egress.

For AAA override of ACL:

- The override ACL name must be a fabric ACL (flex ACL) on the AP.

ACL templates can be used to push ACLs to APs

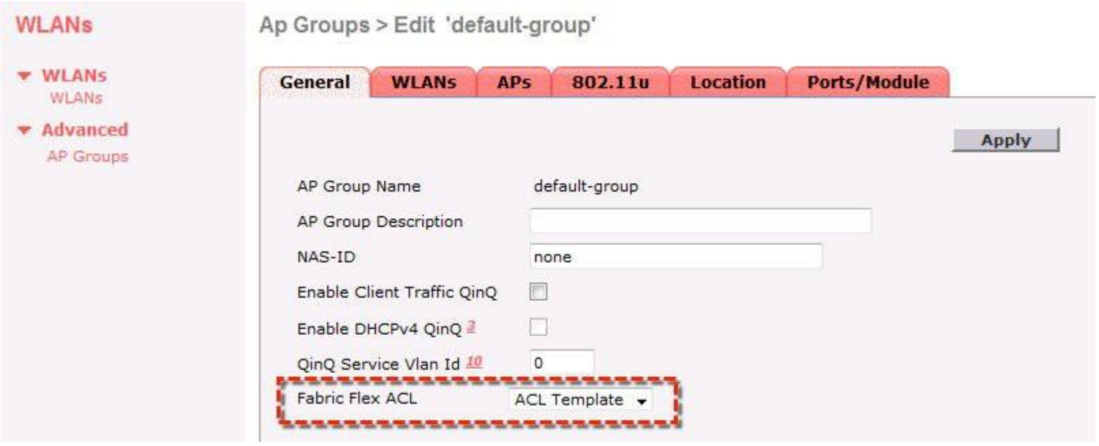


Fabric ACL Template > Edit

Fabric ACL Template Name	ACL Template
Status	Modified

ACL

Fabric ACL
ca-redirect-acl
cwa-redirect-acl
test



Ap Groups > Edit 'default-group'

AP Group Name	default-group
AP Group Description	
NAS-ID	none
Enable Client Traffic QinQ	□
Enable DHCPv4 QinQ [2]	□
QinQ Service Vlan Id [10]	0
Fabric Flex ACL	ACL Template ▾

Note Although IP ACLs are supported, the recommended way to apply a security policy in SD-Access is with SGTs

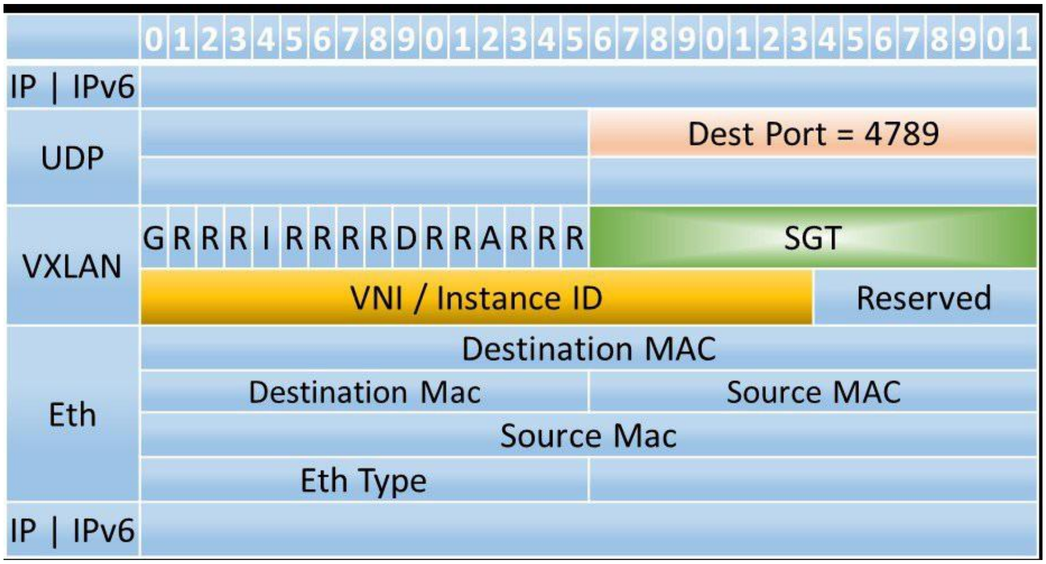
For QoS profile name override:

- The QoS profile name is pushed from ISE.
- Upstream and downstream QoS is applied at the AP.
- VXLAN tunnel QoS is picked from the inner header.

Group-based policies with SGTs

The WLC sends an SGT to the AP to use for the wireless client when the client joins. The AP puts this SGT in the VXLAN header when it forwards data packets from the wireless client to the access switch over the VXLAN tunnel. This SGT is carried from end to end through the fabric.

Figure 50. VXLAN header includes SGT and VNI



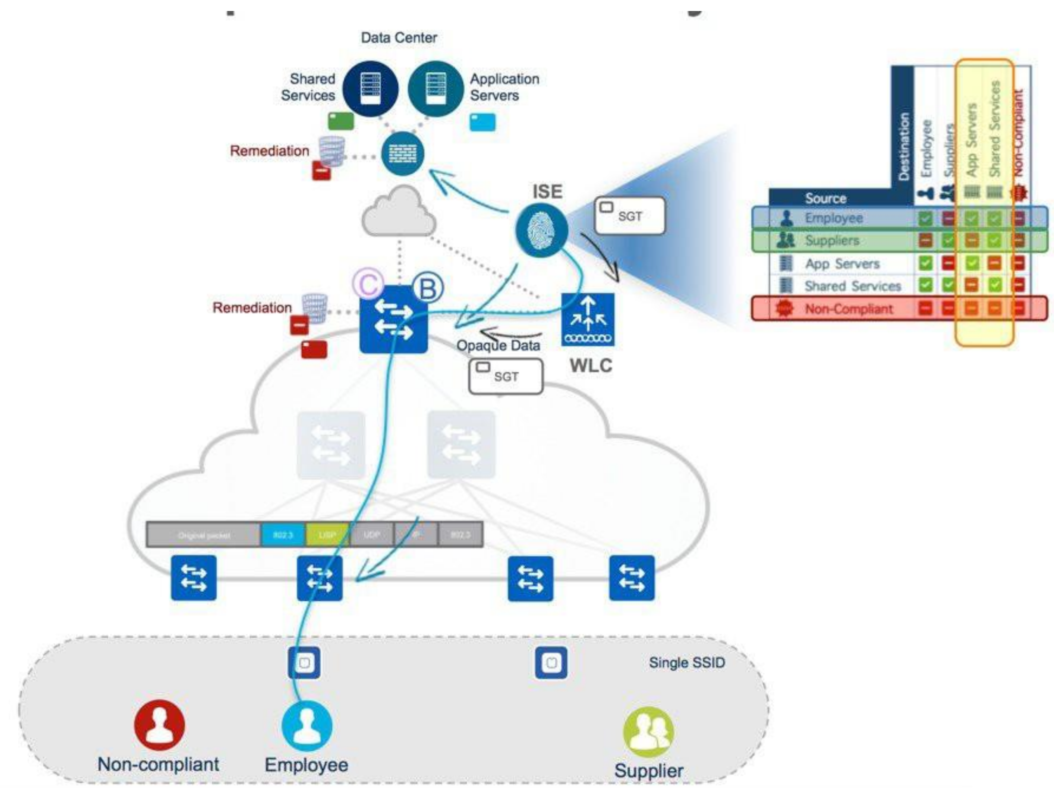
At the egress access switch, the SGT/DGT pair determines the SGACL to be applied. The SGT comes from the packet, and the DGT is derived based on the destination host IP binding.

For applying the SGACL on the access switch for wireless clients (enforcement for the traffic destined to a wireless client on the access switch, or the VXLAN tunnel source), the tag (SGT/DGT) need to be learned on the switch.

The following steps describe the flow for group-based policies:

- Client Layer 2 authentication happens at the WLC.
- The WLC sends an SGT to the AP at the client join.
- The WLC updates the CP with the SGT at client registration.
- The CP updates the FE with the SGT in opaque data. Based on the received SGT, the switch downloads the policy from ISE.
- The AP puts this SGT in the VXLAN header.
- The SGT is carried end to end through the fabric in the LISP header.
- At the egress switch, the SGT/DGT pair determines the SGACL based on the SGT in the packet header.

Figure 51. SGT for group-based policy

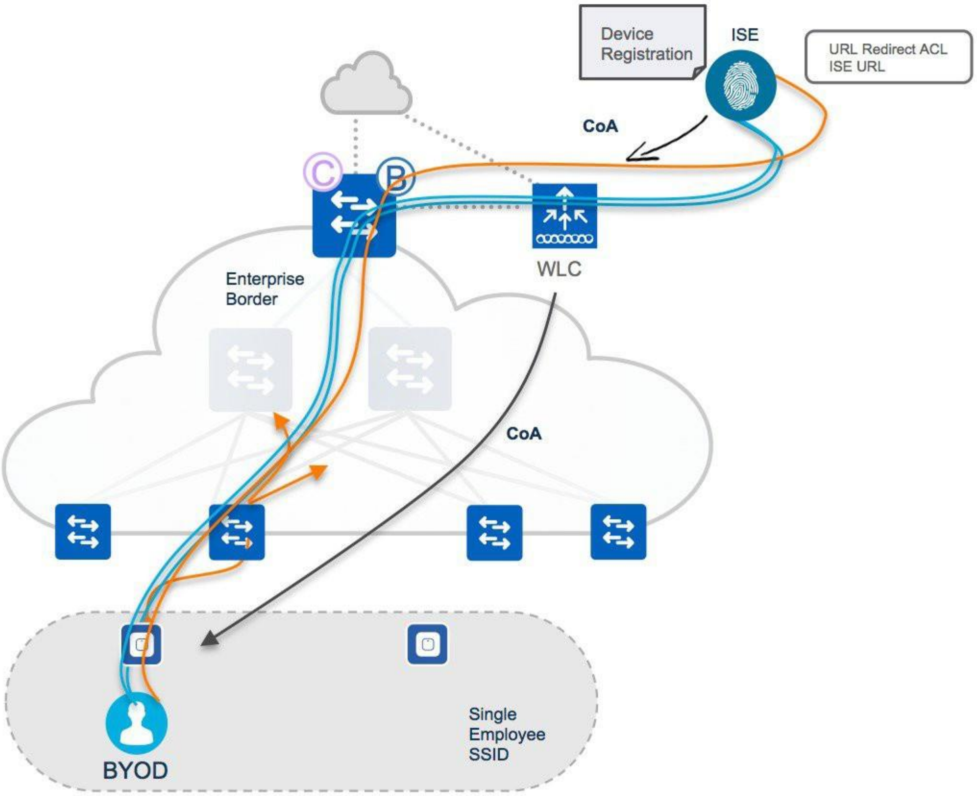


Source \ Destination	Employee	Suppliers	App Servers	Shared Services	Non-Compliant
Employee	✓	−	✓	✓	−
Suppliers	−	✓	−	✓	−
App Servers	✓	−	✓	−	−
Shared Services	✓	✓	−	✓	−
Non-Compliant	−	−	−	−	−

CWA and ISE for BYOD

This section describes the basic flow for central web authentication (CWA). This is the only type of web authentication supported though Cisco DNA Center automation.

Figure 52. CWA with ISE



1. Layer 2 authentication happens at the ISE server. MAC filtering needs to be configured on the WLC.
2. During the client authentication phase, a URL redirect ACL (flex ACL type) and a redirect URL are pushed to the AP.
3. Client traffic is redirected to the ISE portal for device registration and native supplicant provisioning on a VXLAN tunnel.
4. Once complete, ISE sends a change of authorization (CoA) to the WLC, and the WLC pushes the CoA to the AP.
5. The client then reauthenticates using EAP-TLS. Since the device is now known to the ISE server, the authentication goes through, and any further data traffic is switched from the AP to VXLAN onto the fabric edge.

The flow is as follows:

1. Layer 2 authentication happens at the WLC, and the client moves into the WEBAUTH_REQD state.
2. HTTP redirect happens at the WLC.
3. Web authentication can be internal (a webpage hosted on the WLC) or external (a webpage hosted on an external server).
4. Traffic matches the pre-authentication ACL for external local web authentication and is switched out on the VXLAN tunnel. If internal WebAuth, the traffic is sent to the WLC through CAPWAP.
5. Once Layer 3 authentication is complete, the client moves to the RUN state and the pre-authentication ACL is removed.
6. Guest data traffic is switched from the FE to the guest border node in the DMZ. If internal WebAuth, the traffic is sent to the WLC through CAPWAP.

Note All configurations need to be done directly on the WLC user interface.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.