# cisco.



# SD-Access Wireless Design and Deployment Guide Cisco DNA Center 1.3.3

Software-Defined Access	2
SD-Access Wireless	3
SD-Access Wireless architecture	4
Setting up SD-Access Wireless with Cisco DNA Center	13
SD-Access Design	
SD-Access policy	
SD-Access overlay provisioning	40
SD-Access Wireless – A Look Under the Hood	78
Designing the wireless integration in SD-Access	
SD-Access Wireless guest access design	91
Multicast in SD-Access Wireless	93
High availability in SD-Access Wireless	95
Appendix: SD-Access Wireless features deep dive	

Revised: January 27, 2021

# **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

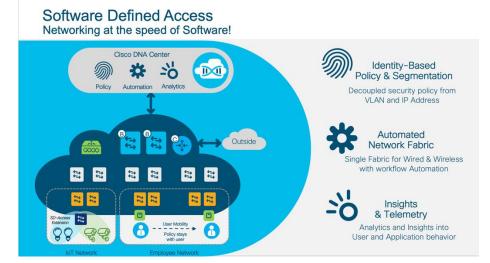
Cisco® Software-Defined Access (SD-Access) is a critical building block of Cisco DNA and brings the principles and advantages of Cisco DNA to Cisco customers.

# **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



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)

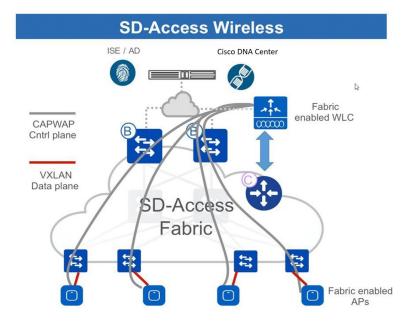
Let's first examine the SD-Access Wireless option, since it brings the full advantages of fabric for wireless users and things. We'll begin by introducing the architecture and main components and then describe how to set up an SD-Access Wireless network using Cisco DNA Center.

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

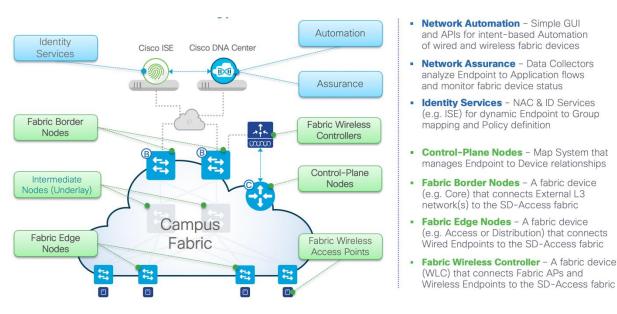


In SD-Access Wireless, the control plane is centralized. This means that, as with Cisco Unified Wireless Network, a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel is maintained between APs and WLC. The main difference is that in SD-Access Wireless, the data plane is distributed using 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



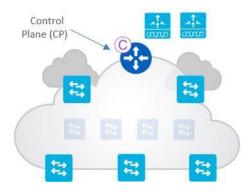
- Control plane (CP) nodes: Host database that manages endpoint ID to device relationships.
- Fabric border (FB) nodes: A fabric device (such as a core or distribution switch) that connects external Layer 3 network(s) to the SD-Access fabric.
- Fabric edge (FE) nodes: A fabric device (such as an access 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



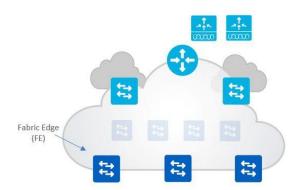
The CP is the host database, tracking endpoint ID (EID) to edge node bindings, along with other attributes. It does the following:

- 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



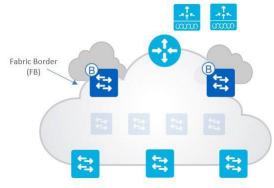
The fabric edge does the following:

- 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



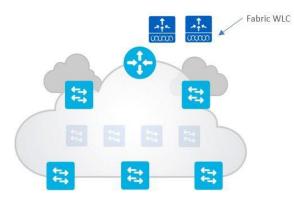
- There are two types of fabric border nodes: border and default border nodes. Both types provide the fundamental routing entry and exit point for all data traffic going into or out of the fabric overlay, as well as for VN and/or group-based policy enforcement (for traffic outside the fabric).
- A fabric 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

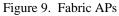
• The fabric-enabled WLC can only manage a single fabric site.

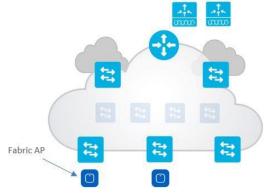


**Note** The WLC and APs need to be within 20 ms of latency. Usually, this means being on the same physical site.

### **Fabric APs**

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





- A fabric AP is a local mode AP and needs to be directly connected to the fabric edge switch or to a classis/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.



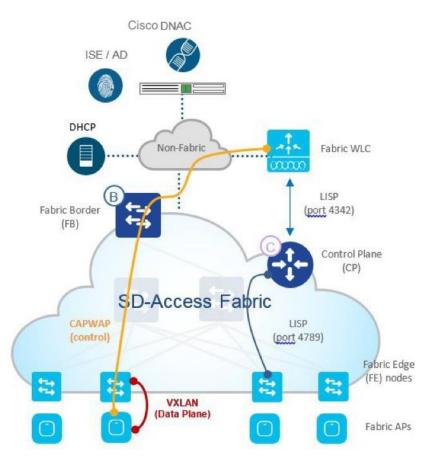
Note For feature support on APs, refer to the WLC release notes.

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 4789.

### **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, and 3800 Series
802.11 Wave 1 Access Points: Cisco Aironet 1700, 2700, and 3700 Series
802.11 Wave 2 outdoor Access Points: Cisco Aironet 1540, 1560
802.11 Wave 2 Access Points: Cisco Aironet 4800 Access Point

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

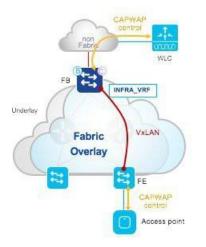
WLCs must be deployed as follows:

- 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.

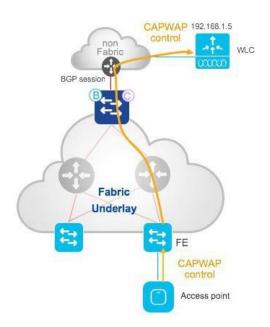
Note: Ensure that the WLC is physically located on-site and does not sit across the WAN. Fabric APs must be in Local mode and need less than 20 ms latency between AP and WLC

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.

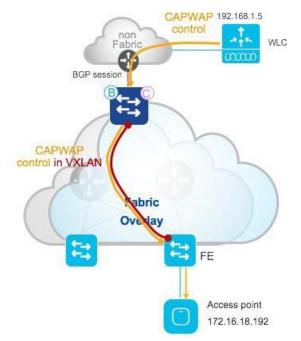
Figure 13. South-north CAPWAP traffic from AP to WLC



- 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)

### 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 9300-245-A Switch
Select a Software Type IOS XE Software IOS XE Winkless Controller Software IOS XE Winkless Controller Software Pickage NDAR2 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 16.12.2t, IOS XE 16.12.1s, IOS XE 16.11.1c

IOS XE 17.1.1s

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.

b Technology		
License Informatio	n:	
	Technology-package	
Туре	Next reboot	
Permanent	network-advantage	
Subscription	dna-advantage	
	License Information	

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.

Devices V Fabric Services Fabric-Enabled Sites	All Fabrics > colarado COIrado	9300-BR.sand.com (9.201.201.13) 健 ⊘Reschable Uptime: 1 minutes
EQ, Find Hierarchy	⊘ Fabric Infrastructure	😼 Run Commands 🛛 🖻 View 360 🔹 Last updated: 1:15 PM 📿 Refres
v 🕲 colrado	<ul> <li>2 device(s) in this site are not com;</li> </ul>	Details Fabric Port Channel Configuration Interfaces
↑ 读 colarado	cleie sau 9300-BR.sand.com	Remove From Fabrio   Fabric <ul> <li>Edge Node</li> <li>Border Node</li> <li>Centrigure</li> <li>Centrol Plane</li> </ul> Capability <ul> <li>Embedded Wireless</li> <li>Configure</li> <li>Configure</li> </ul> <ul> <li>Embedded Wireless</li> <li>Configure</li> </ul>
	Click on the device to open the details tab	Reboot Cancel Add

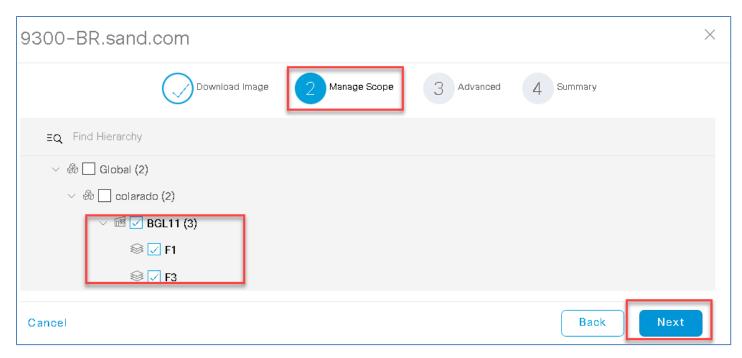
Step 4 Once the embedded wireless capability is added, the next process involves importing the 9800-SW image on the device using the SWIM module on the Cisco DNA center. Click Ok to go through the SWIM process.

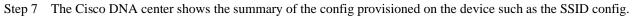
9300-BR.sand.com (9.201.201.13)		
😰 🥝 Reachable - Uptime: 35 minutes		
🔤 Run Comman	ds 🛛 🖻 View 360 🔹 Last updated: 2:34 PM	💭 Refre
Details Fabric Port Channel Configuration Interfaces	Stack	
Remove         Fabric		
Rendezvous Point	Disabled ①	
		Cancel Add

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

9300-BR.sand.com				>
Download Image	2 Manage Scope	3 Advanced	4 Summary	
Select an image from computer Choose File C9800-SW-los2.01.SPA.bin OR				
Enter image URL   Activate image after import  Import				
Cancel			Back	t
9300-BR.sand.com				
Download Image	2 Manage Scope	3 Advanced	4 Summary	
Image imported successfully			,	
C9800 Image activated successfully			v	
Cancel			Back	Next

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				×
	Download Image	Manage Scope	Advanced	4 Summary	_
SYSTEM DETAILS					
Device Name:		9300-BR.sand.com			
Platform Id:		C9300-48UXM, C9300-24U	Х		
Device IP:		9.201.201.13			
Device Location:		BGL11			
SSID(S)					
Name:		sand-site2-1x (sand-denv	er-profile)		
Туре:		Enterprise			
Security:		wpa2_enterprise			
Admin status:		Enabled			
Broadcast: _		Enabled			
Cancel				Back	Save

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

Modify Fabric Domain	
When  Now Later	Cancel

### 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:

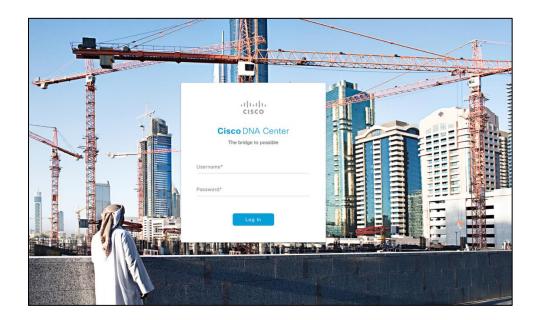
Power consumed by backpla	ne : O Watts		
Mod Ports Card Type		Model	Serial No.
1         12         Sup 8-E         10GE         Si           2         12         10GE         SFP+         3         48         100/1000/2500/5	FP+), 1000BaseX (SFP)	WS-X45-SUP8-E WS-X4712-SFP+E	CAT1947L0LU CAT1849L2F2
	Hw Fw		
+			
1 a89d.21d7.70c0 to a89d 2 74a0.2fa2.eec8 to 74a0 3 78ba.f9a0.9270 to 78ba	.21d7.70cb 1.3 15.1(1r .2fa2.eed3 2.0		
1 a89d.21d7.70c0 to a89d 2 74a0.2fa2.eec8 to 74a0 3 78ba.f9a0.9270 to 78ba Mod Submodule	.21d7.70cb 1.3 15.1(1r .2fa2.eed3 2.0 .f9a0.929f 1.0 0.0 Model	)SG17 03.11.00.E Serial No. Hw St	Ok Ok Ok
1 a89d.21d7.70c0 to a89d 2 74a0.2fa2.eec8 to 74a0 3 78ba.f9a0.9270 to 78ba Mod Submodule	.21d7.70cb 1.3 15.1(1r .2fa2.eed3 2.0 .f9a0.929f 1.0 0.0 Model	)SG17 03.11.00.E Serial No. Hw St	Ok Ok Ok
1 a89d.21d7.70c0 to a89d 2 74a0.2fa2.eec8 to 74a0 3 78ba.f9a0.9270 to 78ba Mod Submodule 	.21d7.70cb 1.3 15.1(1r .2fa2.eed3 2.0 .f9a0.929f 1.0 0.0 Model ++ WS-UA-SUP8E	SG17 03.11.00.E Serial No. Hw St CAT1948LG9Z 1.1 Ok	Ok Ok Ok
1 a89d.21d7.70c0 to a89d 2 74a0.2fa2.eec8 to 74a0 3 78ba.f9a0.9270 to 78ba Mod Submodule	.21d7.70cb 1.3 15.1(1r .2fa2.eed3 2.0 .f9a0.929f 1.0 0.0 Model ++ WS-UA-SUP8E	SG17 03.11.00.E Serial No. Hw St CAT1948LG9Z 1.1 Ok	Ok Ok Ok

# **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.

Cisco DNA Center DESIGN	POLICY PROVISION	ASSURANCE PLATFORM			_❷ Q Ⅲ ✿ ◎ Ⅲ
Welcome, admin				Get Started	Take a Tour 🕞 Learn More
		In a few simple steps, discover your device Get S		ay!	
Assurance Summary					
Health 1 Healthy as of Jan 28, 2020 11:35 AM			Critical Issues Last 24 Hours		
% Network Devices	% Wireless Clients	Wired Clients	P1		O P2
		View Details			View Details
Network Snapshot					
		Network Devices As of Jan 28, 2020 11:46 AM		Application Policies As of Jan 28, 2020 11:46 AM	
		$\frown$	Unclaimed: 0	$\bigcirc$	Successful Deploys: 0

# 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.

	٢	Q		¢	Ø		
Ge	SYSTEM				earn N	lore	
	System Se Audit Log		5				
	음 admin						
	Sign Out						

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:

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM			∠● ♀ Ⅲ ♀ ◎ Ⅲ
System 360 Software Updates	Settings Data Platform Users Backup & Restor	re		
ΞQ. Search	Authentication and Policy Servers			
Account Lockout	Use this page to specify the servers that authenticate Cisco DNA	Center users. ISE servers can also supply policy and user informa	ation.	
Anonymize Data Authentication and Policy Servers			Last updated: 1	:53 PM 😳 Refresh 🖞 Export 😝 Add
Certificate				
Cisco Credentials				
CMX Servers	IP Address	Protocol	Туре	Status
Debugging Logs		No matching records found		
Device Controllability				
Device EULA Acceptance				
Email Configuration				
Events and Subscription				
High Availability				
Integration Settings				
Integrity Verification				
IP Address Manager				

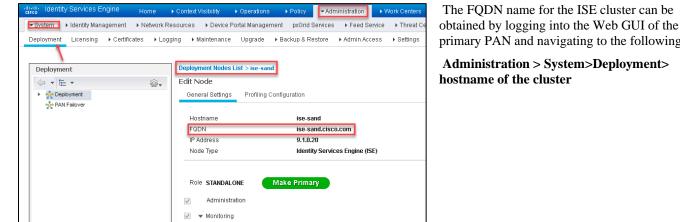
Fill in the ISE information (remember to toggle the "Cisco ISE server" switch):

Add AAA/ISE server	×
Server IP Address* 10.195.180.131	
Shared Secret*	ø
Cisco ISE server Con 0 Usemame*	
admin Password*	ø
FGDN* prabhjit-ise.cisco.com Subsciber Name*	
dnac-133	
55H Key	
Virtual IP Address(es)	
View Advanced Settings	
Cancel Apply	

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).



primary PAN and navigating to the following link. Administration > System>Deployment>

Go to ISE and approve the Cisco DNAC's pxgrid

connection by approving the subscriber name – dnac-133 by going to **Administration > pxGrid Services**.

Identity Services Engine Home + C     System + Identity Management + Network Resources		Administration   Work Center Work Center Head Service   Threat				1 License Warning A Q O O O
All Clients Web Clients Capabilities Live Log	Settings Certificates Permissions					Click here to do wireless setup and visibility setup Do not show this again.
🖌 Enable 🖉 Disable 😨 Approve 🖯 Group 👎 Dec	line 😧 Delete 👻 🍪 Refresh 🛛 Total Pending Appro	val(1) •				1 selected item 1 - 8 of 8 Show 25 🕶 per page Page 1 🗘
Client Name Client Descr	iption Capabilities	Status	Client Group(s)	Auth Method	Log	
ise-admin-prabhjit-ise	Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View	
<ul> <li>ise-pubsub-prabhjit-ise</li> </ul>	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.

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM			∠● ♀ Ⅲ ♀ ◎	=
System 360 Software Updates	Settings Data Platform Users Backup & Resto	re			
EQ. Search	Authentication and Policy Servers				
Account Lockout Anonymize Data	Use this page to specify the servers that authenticate Cisco DNA	Center users. ISE servers can also supply policy and user informa			
Authentication and Policy Servers			Last u	pdated: 4:37 PM 📿 Refresh 🖄 Export 🕀 /	Add
Certificate					
Cisco Credentials	IP Address	Protocol	Туре	Status	
CMX Servers	IP AUGUSS	Protocol	туре	Status	
Debugging Logs	0 10.195.180.131	RADIUS	ISE	ACTIVE	
Device Controllability					
Device EULA Acceptance					
Email Configuration					
Events and Subscription					

# **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.

e proceed monitoring and insights from the network, device dict problem stater and ensure that policy and configurati iness intent and the user experience you want. Assurance Health Assurance Issues		ate end-to-end solutions and add support for grations	TOOLS Discovery Topology Command Runner License Manager
ols			Template Editor Security Advisories Network Telemetry Data and Reports
Discovery Automate addition of devices to controller inventory	Topology Visualize how devices are interconnected and how they communicate	Command Runner Allows you to run diagnostic CLIs against one or more devices	License Manager Visualize and manage license usage
Template Editor	Security Advisories	Network Telemetry	Data and Reports Access Data Sets, Schedule Data Extracts for Download multiple formats like POP sectors, 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.

Cisco DNA Center	Discovery	2● Q Ⅲ ◆ ○ Ⅲ
Discovery Dashboard		
Add Discovery View All Discoveries 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 O O 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.

Cisco DNA Center		Discovery	∠⊗ ⊂ ⊞ ⇔ ⊙ ≣
EQ - Search by Discovered Device IP	New Discovery		♦ Back to Dashboard
No Discoveries Added. Fill out the 'NEW DISCOVERY' form and start your first scan.	Discovery Name* WLC		
	✓ IP Address/Range*  Discovery Type   CDP ⊙ IP Address/Range ○ LLDP		
	From*  From*	To* 0 192.168.1.10 +	
	<ul> <li>Credentials*</li> <li>At least one CLI credential and one SNMF</li> <li>Netconf is mandatory for enabling Wirelet</li> <li>GLOBAL Tak-specific</li> </ul>	🕀 Add Credentials	
	CLI No credentials to display	SNMPv2c Read No credentials to display	
	SNMPv2c Write	SNMPv3	
	No credentials to display	No credentials to display	
	onfig changes will be made on network devices is associated to a site. Learn More   Disable	during	Reset Discover

**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:

Cisco DNA Center	Discovery	< <! <! <! <! <! <! <! <! <! <! <! <!</th
Claco DNA Center	Discovery New Discovery Discovery Name* WC > P Address/Range* Discovery Type 0 (DP) Pitferred Management IP Address 0 Nome (Use Loopback) - To* 0 192.158.1.10 - 192.158.1.10 - 4 Preferred Management IP Address 0 Nome (Use Loopback) - Credentials* A Liess one CU credential and one SMMP credential are required. B Kitcori is mandatory for enabling Wireless Services on Wireless capable devices such as C9800-Switches/Controllers. B GLOBAL Task-specific CLI SNMPV2c Read	Add Credentials (Li SMP/2 SMP) SMP PROPERTIES HTTP(3) NETCONF Mama/Description* admin- Password* 
	No credentials to display         No credentials to display	

Add Credentials × cli <b>SNMPv2c</b> SNMPv3 SNMP HTTP(S) NETCONF	Add Credentials × cLi <b>SNMPv2c</b> SNMPv3 SNMP HTTP(S) NETCONF
Read     Write       Name/Description*       pbagga       Read Community*	Read       Write         Name/Description*       pbagga         Write Community*           Image: Save as global settings         Settings will be used for this task and saved for later
Save as global settings Settings will be used for this specific Discovery only Reset Save	Reset Save

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.

Cisco DNA Center		Discovery	∠● Q Ⅲ ♦ ◎ Ⅲ
EQ - Search by Discovered Device IP	New Discovery		Add Credentials
No Discoveries Added. Fill out the 'NEW DISCOVERY' form and start your first scan.	Discovery Name* WLC		CLI SNMPV2C SNMPV3 SNMP HTTP(S) NETCONF
	GLOBAL Task-specific	ss Services on Wireless capable devices such as C9800-Switches/Controllers.	830
	CLI admin   admin-witc	SNMPv2c Read	Reset
	SNMPv2c Write	SNMPv3 No credentials to display	
	HTTP(S) Read No credentials to display	HTTP(S) Write No credentials to display	
	NETCONF	]	

**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.

✓ Advanced Protocol Order ●	
SSH     \$       Image: Telest     \$	
nfig changes will be made on network devices during s associated to a site. Learn More   Disable	Reset Discover

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

Cisco DNA Center				Discovery					<b>_</b> 9	୦	¢	0 1	۰
i Discovered devices will be added to	Inventory automatic	ally after successful completion of each di	iscovery. View Inven	itory									×
O WLC   1 Reachable Devices Range 192.168.1.10-192.168.1.10			DEVICE STATUS	~			<b>∀</b> Filter				1	History	/~
							IP Address	Device Name	Status ICMP		CLI NE	TCONF	1
		1 Devices	)	<ul> <li>Success(1)</li> <li>Unreachable(</li> <li>Discarded(0)</li> </ul>	0)		192.168.1.10	WLC-3504					
	Discovery D	etails											
	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	Show 25		Showing 1 to 1 of	Pag	je 1 4	of 1	
	IP Filter List	None			Preferred Management IP Address	None		Ø success	UNREACHABLE		NOT TRIED		
	CLI Credentials	admin			SNMPv2c READ	pbagga							
	SNMPv2c WRITE	pbagga			SNMPv3	None							
	HTTP(S) READ	None			HTTP(S) WRITE	None							
	NETCONF	None											

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.

2 - Search by Discovered Device IP	Devices (	Ocompleted	5 Reachable Devices	00h:00m:07s				+	Back to	Dashb	bard	O Take a	Tou
Devices   5 Reachable Devices Range 3.3.3.1-3.3.3.100				DEVICE STATUS	v	√ Filter						Histor	ry 、
WLC   1 Reachable Devices						IP Address	Device Name	Status		SNMP	CLI	NETCONF	
Range 192.168.1.10-192.168.1.10		1				3.3.3.9	FE1-9300- 03.cisco.com						
		(	5	<ul> <li>Success(5)</li> <li>Unreachable(0)</li> </ul>		3.3.3.13	FE2-9300- 04.cisco.com						
			Devices	Discarded(0)		3.3.3.21	CONTROL- PLANE.cisco.co m					•	
						3,3,3.5	INT- BOR.cisco.com					•	
	Discovery I	Details				3.3.3.1	pb-fusion- router					•	
	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	Show 25		Showing 1	to 5 of 5	P	ige 1	¢ of 1	
	IP Filter List	None		Preferred Management IP Address	None		Ø success		HABLE (		NO TR	IED	
	CLI Credentials	lab		SNMPv2c READ	pbagga								
	SNMPv2c WRITE	pbagga		SNMPv3	None								
	HTTP(S) READ	None		HTTP(S) WRITE	None								

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.

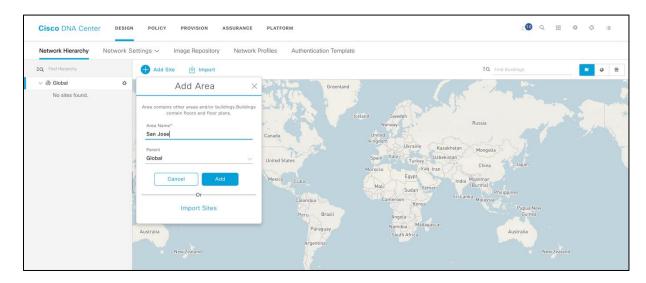
Devices V Fabric Se	rvices									
C Find Hierarchy	DEVICES (6) FOCUS: Inventory ~				<b>Q</b> Glob	bal				Take a Tour 📃 🔋
& Global		witches APs	s WLCs	REACHABILITY	All	Reachable Unre	achable			
	√ Filter	e Actions v (	D						L	ast updated: 4:23 PM 🛛 🗧
	Device Name	IP Address	Support Type ①	Device Family	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 Seri
	E1-9300-03.cisco.com	3.3.3.9	Supported	Switches and Hubs	Assign	Reachable	Managed	4 hours ago	FCW2248AHLW	Cisco Catalyst 9300 Seri
	E2-9300-04.cisco.com	3.3.3.13	Supported	Switches and Hubs	Assign	Reachable	Managed	an hour ago	FCW2248DHHS	Cisco Catalyst 9300 Seri
	INT-BOR.cisco.com	3.3.3.5	Supported	Switches and Hubs	Assign	Reachable	Managed	4 hours ago	FCW1934C1D8	Cisco Catalyst 3850 Seri
	D pb-fusion-router	3.3.3.1	Supported	Switches and Hubs	Assign	Reachable	Managed	3 hours ago	FDO1735Q0FR	Cisco Catalyst 3650 Seri
	🔲 🕞 WLC-3504 🖻	192.168.1.10	Supported	Wireless Controller	Assign	Reachable	Managed	4 hours ago	FCW2221M0JT	Cisco 3500 Series Wirele

# **SD-Access Design**

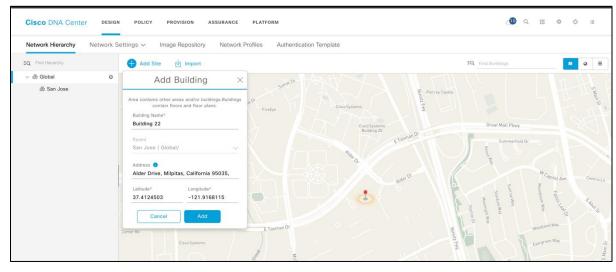
# Get started using Cisco DNA Center Design

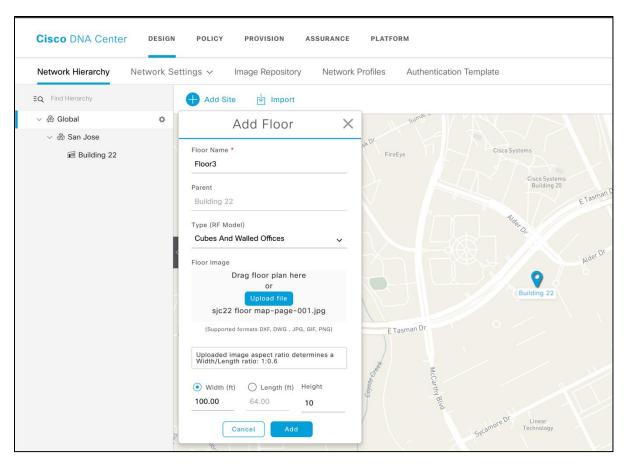
Cisco DNA Center provides a robust Design application to allow customers of every size and scale to easily define their physical sites and common resources. This is implemented using a hierarchical format for intuitive use, while removing the need to redefine the same resource in multiple places when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

### Procedure



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





Network Hierarchy Network S	ettings v Image Repository Network Profiles Authentication Template	
Q Find Hierarchy	5 GHz v Edit Data View Options	EQ Find
v 💩 Global 🔅	San Jose / Building 22 / Floor3	Updated 30 seconds ago 📀
> j≊ Building 22		

## **Network settings**

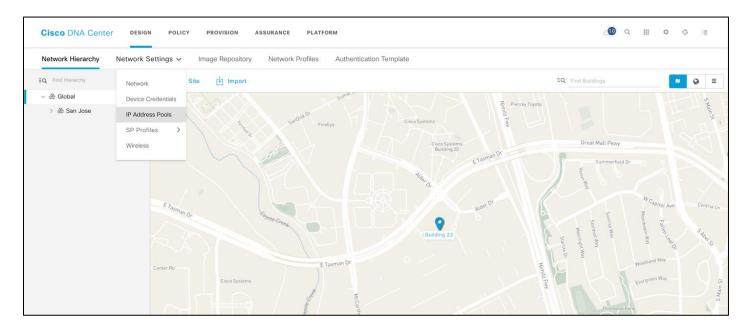
Cisco DNA Center allows you to save common resources and settings with Design's Network Settings application. This allows information pertaining to the enterprise to be stored so it can be reused throughout the Cisco DNA Center. DHCP, DNS servers, and device credentials should already be defined here.

### **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	
IP Address Space	Options
IPv4 O IPv6	
Tunnel Type is supported for IPv4 pools only. If IPv6 is se have to be IPv6 format.	fected, all the below fields will
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 ×	00 \
DNS Server(x)	
171.70.168.183 ×	B ^
EQ: Search or Add Value	+

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

letwork Hierarchy Netwo	ork Settings ~ Image Repository Netwo	rk Profiles Authentication Te	mplate		
Find Hierarchy	Network Device Credentials IP Ad	dress Pools QoS Wireless			
🗞 Global					
> 🛞 San Jose	IP Address Pools (4)				Last updated: 4:42 PM 🛛 📿 Refresh
	$\nabla$ Filter • Add Actions $\vee$ :	SUBNET TYPE All IPv4	IPv6		
	Name 🔺	Туре	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

### **Creating wireless SSIDs**

#### Procedure

**Step 1** Under Network Settings, click the Wireless tab.

EQ. Find Hierarchy Ne	etwork	Site 🕁 Import		
v 🏶 Global De	evice Credentials	/	rporation	Cisco Systems Building 24
> 💩 San Jose	Address Pools			McCaathy Building 24
SF	Profiles >	TechnologyDr	SanDisk	Cisco Systems Building 23
W	ireless	Telic		sumacor
		1 Color	a sandiak Dr	Surv A

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.

Enterprise Wireless Network         2         Wireless Profiles			
Wireless Network Name(SSD)* pbagga-internal	Type Of Enterprise Network *		
Fast Lane	O Data only		
SSID STATE			
Admin Status:			
Broadcast SSID:			
Wireless Option			
<ul> <li>Dual band operation (2.4GHz and 5GHz)</li> </ul>			
Dual band operation with band select			
⊖ 5GHz only			
○ 2.4GHz only			
Level Of Security*			
○ WPA2 Enterprise			
re secure			
assword (Pre-Shared Key PSK with WPA2 encryption ) is needed to access the wireless network			
ss Phrase*			
Ø			

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.

Cisco DNA Center DESIG	N POLICY PROVISION ASSURANCE PLATFORM		⊿@ ♀ ⅲ ጶ ♀ ≡
Network Hierarchy Network S	Settings - Image Repository Network Profiles Authentication Template	Sites	×
EQ. Find Hierarchy	Network Device Credentials IP Address Pools QoS Wireless		
<ul><li>     般 Global</li></ul>	Create an Enterprise Wireless Network	EQ. Choose a site	
> ঐ San Jose	Enterprise Wireless Network     Wireless Profiles	<ul> <li>✓ ⓓ Global (1)     <li>✓ ⓓ Z San Jose (1)     <li>✓  Z Building 22 (1)</li> </li></li></ul>	
	Wireless Profile Name * employee	😂 🗸 Floor3	
	Fabric		
	• Yes ○ No		
	😤 <u>Sites</u> 3 sites		
	Attach Template(s)		
	Device Type Device Tag 🌒		
		-	
		Back OK	

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

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM		∠10	: ◇ ◇ ::
Network Hierarchy Network Se	ettings - Image Repository Network Profiles Authentication Template			
EQ. Find Hierarchy	Network Device Credentials IP Address Pools QoS Wireless			
<ul><li> 公  合 Global</li></ul>				
> 🖓 San Jose	Enterprise Wireless			🕂 Add
	√ Filter 🖉 Edit 📋 Delete			
	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.

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM	∠10 ⊂
Network Hierarchy Network Se	ttings v Image Repository Network Profiles Authentication Template	
EQ Find Hierarchy	Network Device Credentials IP Address Pools QoS Wireless	
V & Global	Create a Guest Wireless Network	
> 🛞 San Jose	Guest Wireless Network 2 Wireless Profiles 3 Portal Customization	
	Witniess Network Name(SSID) * Guest-WiFi	
	SSID STATE	
	Admin Status: Broadcast SSID:	
	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 ? Where will your guests redirect after successful authentication ? Self Registered  Viriginal URL V	
	Show Advanced Settings	
	Ca	ncel Previous Next

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

twork Hierarchy Network	Settings - Image Repository Network Pr	ofiles Authentication Templa	te	Edit Wireless Profile
	Network Device Crodentals IP Address	Pools Qo5 Wireless		Whereas Profile Name *
() Giobal	Create a Guest Wireless Network			employee
> 🗇 San Jose	Guest Wireless Network	less Profiles 3 Portal Custe	mization	Fabric Yes 🔿 No
	Profiles			R Sites 3 sites.
	Filter 1 Selected	Version	Created By	Attach Template(s)
	employee	1	admin	Add Device Type Device Template Tag 0
			Showing 1 of 1	No data to display
				~

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

Basifinal     Page Content     Page Content     Color     Color     Fort     ThrEFACE   Losida Sans   HADER:   2   2   Manual   TITLE TEXT:   14   15   Baisl   Boor Text:   12   Normal     Ponder     Page Content     Login Page   Description Success   Success Page     Page Content			Port	al Builder	
> Page Content     Color     Color     Font     TYPEFACE   Lucida Sans   4   Mormal   *   TTLE TEX:   14   Boild   Boild   BOOY TEXT:     Page Lontent     Page Lontent     Pige Lontent <th>GuesPortal</th> <th></th> <th>Registration Page V</th> <th></th> <th></th>	GuesPortal		Registration Page V		
Font       TypeFACE       Luceta Sans       HEADER:       24 ~ Normal       24 ~ Normal       TITLE TEXT:       114 ~ Bold       120 yr Text:		0	Registration Page	HIGH-TECH	
TYPEACE Lucida Sans   HEADER: 24  Increase Account Crease Account		0			
Lucida Sans          HEADER:          24 ^ Normal          TITLE TEXT:          14 ^ Bold          Boory Text:	/				
24 v Normal v       TTLE TEXT:       14 v Bold v       Body Text:		-			
TITLE TEXT:				Provide us with some information so we can create	5 32
BODY TEXT:				FIRST NAME	
FORM LABEL: Register Cancel					

**Step 8** Click Finish to complete the Guest SSID design phase

Network Device Credentials IP Address Pools QoS Wireless			
Create a Guest Wireless Network			
Guest Wireless Network     O     Wireless Profiles     O     Portal	I Customization		
Portals			🕂 Add
Portal Name	Туре	Action	
GuesPortal	Self registered	Edit   Delete	
	Showing 1 of 1		
		Cancel Previous	Finish

**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.

CISCO CENTER DESI	GN POLICY PROVISION					≡ ¢	1
EQ. Find Hierarchy	A						
<ul> <li>Global</li> </ul>							
↑ Milpitas	Wireless Rad	io Frequency	Profile			e	Ad
San Jose							
SantaClara	∀ Filter						
	Profile Name 🔺	Туре	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	Vie	w
	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	Vie	ew

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

PROPILE NAME* demo	
PROFILE TYPE	
^ 2.4 GHz	0
Parent Profile	
🕘 High 🔿 Medium (Typical) 🖓 Low 🔿 Custom	
A 5 GHz	0
Parent Profile	
○ High ○ Medium (Typical) ○ Low ⓒ Custom	
	Cancel

🔾 High 🔹 Medium (Typical) 🔹 Lo	w 💿 Custom								
Channel Width Best ~									
20 MHz									
AO MH2		UNII-2 52-144			E	UNI-:	3 149-165		
		52 2 56	€ 60	64		1 149	153 157	161	
BO-MH2		100 104	108	112		165	202 202	1000	
160 MHz		116 2 120	124	128					
" exist		2 132 🛛 136	2 140	144					
Best									
Data Rate		~							
i û	13	2:4	, 36	48	54				
TX Power Configuration									
Power Level									
and the second se	0							RX SOP	
io Bin	10 dBm				30 dBm			Auto	~
								High	
	0							Medium	
Power Threshold					-50 ((Brit)				
Power Threshold	-65							Low	

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.

# **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 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.

roup-Based Access Control	<ul> <li>IP Based Access</li> </ul>	s Control 🔨	<ul> <li>Applic</li> </ul>	cation $\checkmark$	Traffic Co	opy ∽ Virtu	al Netwo	rk					
Q Find Virtual Network	Create or M	lodify Virtua	I Network by	selecting A	vailable Sca	lable Groups.						Reset	Save
New Virtual Network	Virtual Network	: Name*											
DEFAULT_VN (18)	loT							vManage VPN		$\sim$	Guest Virtual	Network 🜖	
INFRA_VN (0)	Available Sc	alable Group	IS					Groups in the	e Virtual Netv	vork			
	∃Q, Find Scal	able Group			Show	Unselected	~	EQ Find Scal	able Group				
	AU	BY	со	DE	DS	ЕМ		PO	PC <sup>©</sup>	UN <sup>O</sup>			
	Auditors	BYOD	Contract ors	Develop ers	Develop ment_S	Employe es		Point_of _Sale_S	PCI_Ser vers	Unknow n			
	EX	GU	IN	NS	PS	PU							
	Extranet	Guests	Intranet	Network _Servic	Producti on_Serv	Producti on_User							
	QS	тѕ	TS										
	Quaranti ned_Sy	Test_Se rvers	TrustSe c_Devic										

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.

Cisco DNA Cente	r DESIGN	POLICY P
Group-Based Acces	s Control 🗸	IP Based Acc
Scalable Groups	•	Create of
Access Contracts		Virtual Netv
Policies		loT
IoT (3)		
		Available
		EQ Find S

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.

Cisco	DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM		۵۵	Q Ⅲ ¢ © ∷				
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									
Group-E	3ased Access Control ∽	IP Based Access Control V Application V Traffic Copy V	rtual Network						
Access	Contracts (8)		Last upo	lated: 5:03 PM C Refresh	Create Access Contra				
<i>∀</i> Filter	Actions \vee Deploy								
	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 Acces	s Contract					×
Name* demo_access		Description	ł.			
CONTRACT CONTE	NT (1)	Transport Protocol	Source / Destination	Port	Logging	Action
			Destination	80	Logging	+×
Default Action Permit	<u> </u>	gging				
					Cancel	Save

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

Cisco DNA Center Design Pol	ICY PROVISION ASSURANCE PLATFORM		<b>_10</b>	०, Ⅲ ० ० ≡
Migration is complete. Cisco DNA Center w the administration mode in GBAC Configura	vill be the policy administration point, and screens of Scalable Groups, Access Contract ations	s and Policies in Cisco ISE will be read-only. You	can review the policy migra	tion log, and/or change $~~ imes~$
Group-Based Access Control V IP B	ased Access Control V Application V Traffic Copy Virtua	al Network		
Access Contracts (9)		Last updated	5:07 PM C Refresh	Create Access Contract
$\nabla$ Filter Actions $\vee$ Deploy				
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

	DNA Center DE	SIGN POLIC	Y PROVISION ASS	SURANCE PLATFORM					
	Aigration is complete. Cisco he administration mode in C		be the policy administration p ns	point, and screens of Scalab	ele Groups, Access Contr	acts and Policies in Ci	sco ISE		
Group-	Based Access Contro	ol ∽ IP Bas	ed Access Control $\sim$	Application $\sim$ T	raffic Copy 🗸 Vi	rtual Network			
Access	s Contracts (9)								
7 Filter	er Actions V Deplo	oy 1 Selected							
	Name 🔺		Description				Rule		
	AllowDHCPDNS		Sample contract to allow DHC				2		
	AllowWeb		Sample contract to allow acces	ess to Web			2		
	demo_access						1		
		POLICY	PROVISION ASSURANCE	PLATFORM			1		
	demo_access	N POLICY	PROVISION ASSURANCE	PLATFORM			1	20	◙ <
Sisco [	DNA Center Design	A Center will be the	PROVISION ASSURANCE		ccess Contracts and Policie	is în Cisco ISE will be rea			~~ ### #P \22
Sisco [	DNA Center DESIGN gration is complete. Cisco DN	IA Center will be the C Configurations	policy administration point, and			is în Cîsco ISE will be rea			~~ ### #P \22
Cisco [ Mig the Group-B	DNA Center DESIGN gration is complete. Cisco DN. administration mode in GBAC	IA Center will be the C Configurations	policy administration point, and	screens of Scalable Groups, A				n review the policy r	migration log, and/or change
Cisco [ Mig the Group-B	DNA Center DESIGN gration is complete. Cisco DNA administration mode in GBAC Based Access Control ~ Contracts (9)	IA Center will be the C Configurations	policy administration point, and	screens of Scalable Groups, A			d-only. You ca	n review the policy r	migration log, and/or change
Sisco [ Mig the	DNA Center DESIGN gration is complete. Cisco DNA administration mode in GBAC Based Access Control ~ Contracts (9)	IA Center will be the C Configurations	policy administration point, and	screens of Scalable Groups, A			d-only. You ca	n review the policy r	migration log, and/or change
Cisco □	DNA Center DESIGN gration is complete. Cisco DNJ e administration mode in GBAC Based Access Control V Contracts (9) Actions V Deploy	IA Center will be the C Configurations IP Based Ac	policy administration point, and	l screens of Scalable Groups, A cation ∨ Traffic Cop			d-only. You ca	n review the policy r	migration log, and/or change
Cisco [ Mig the Group-B Cccess f Filter	DNA Center DESIGN gration is complete. Cisco DN. e administration mode in GBAC Based Access Control ~ Contracts (9) Actions ~ Deploy Name -	A Center will be the C Configurations IP Based Ac Desi Sam	policy administration point, and ccess Control ~ Applie	l screens of Scalable Groups, A cation ∨ Traffic Cop		Rules Count	d-only. You ca	Deployed	migration log, and/or change

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.** 

Cisco DNA Cente	er design	POLICY	PROVISION	ASSURANCE	PLATFO	RM
	plete. Cisco DNA C n mode in GBAC C		he policy adminis	tration point, and s	screens of So	calable Grou
Group-Based Acces	ss Control 🗸	IP Based	Access Contro	ol 🗸 Applic	ation 🗸	Traffic
, Scalable Groups	(9)					
Policies						

**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.

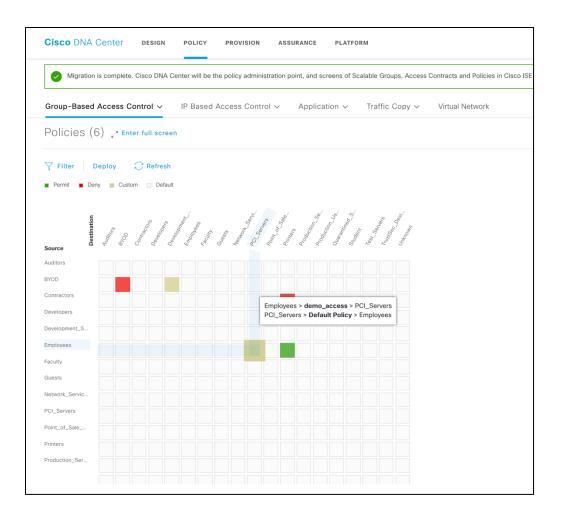
Cisco DNA Center design policy provision assurance platfor	Create Policy ×
S Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Sca	Employees   POL_Servers    Default Policy Status
Group-Based Access Control V IP Based Access Control V Application V	Enabled
Policies (5) 💒 Enter full screen	Contract: Change Contract
🍸 Filter Deploy 📿 Refresh	
Permit Deny Custom Default	
ини и и и и и и и и и и и и и и и и и и	
Addters BYOO Connectors	
Developers	
Development_S	
Employees	
Guests	
Network_Servic	
PCL_Servers Pcint_of_Sele	
Printers	
Production_Ser	
	Cancel Save

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.

	ange Contract		×
V	Filter		
	Name	Description •	Policies Referencing
۲	demo_access		0
0	Deny IP	Deny IP SGACL	3
0	Deny_IP_Log	Deny IP with logging	0
0	dfsfsd	dfsndfsdef	0
0	Permit IP	Permit IP SOACL	1
0	Permit_IP_Log	Permit IP with logging	0
0	AllowWeb	Sample contract to allow access to Web	1
0	AllowDHCPDNS	Sample contract to allow DHCP and DNS	0
0	DesyRemotoServices	Sample contract to block Remote Access and tellest services	0
Show	r 10 entries	Showing 1 - 9 of 9	Previous 1 Next
			Cancel Change

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

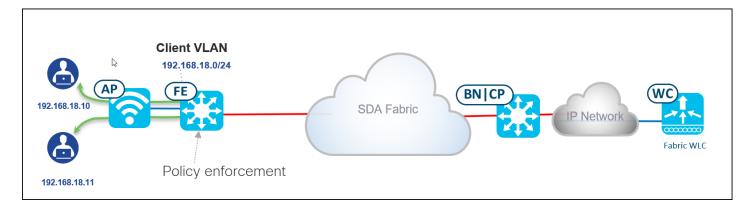
Verify from the Policies Matrix page that the Scalable Group Access List policy got created.



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 V Fabric Servic	25									
o, Find Hierarchy	DEVICES (6) FOCUS: Inventory ~			<b>Q</b> Gl	obal				Take a Tour 📃	*
- 🛞 Global	DEVICE TYPE All Routers Sw	vitches APs WLCs	REACHABILITY AIL	Reachable U	Unreachable					
<ul> <li>Unassigned Devices (1)</li> <li></li></ul>	Filter Add Device Tag Device Actions V 1 Selected		Selected						Last updated: 5:11 PM	0
	Device Name -	Inventory > IF Software Image >	Device Family Site	8	Reachability	MAC Address	Device Role	Image Version	Uptime	1 \$
	CONTROL-PLANE.cisco.com	3 Provision > 3 Device Replacement>	Assign Device to Site	22/Floor3	Reachable	d4:ad:71:30:a7:00	Ø DISTRIBUTION	16.11.1c	14 days 20 hrs 18 mins	N
	FE1-9300-03.cisco.com 0	3. Others >	Provision Device	22/Floor3	Reachable	00:29:c2:be:0e:00	Ø ACCESS	16.11.1c	18 days 16 hrs 13 mins	N
	FE2-9300-04.cisco.com D	3.3.3.13 Supported	LAN Automation Status	22/Floor3	Reachable	00:29:c2:27:51:00	Ø ACCESS	16.11.1c	18 days 16 hrs 08 mins	N
	<	3.3.3.5 Supported	Learn Device Config	22/Floor3	Reachable	38:ed:18:67:a6:00	OISTRIBUTION	16.11.1c	43 days 20 hrs 48 mins	N
	pb-fusion-router D	3.3.3.1 Supported	Configure WLC HA	22/Floor3	Reachable	c0:67:af:ed:af:80	ACCESS	16.11.20190312:035643	107 days 20 hrs 06 mins	N
	[7] WLC-3504 [3]	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
EQ Find Hierarchy
✓ ♣ Global (1)
◇ 総 San Jose (1)
✓ i 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)			$\times$
♣ ⊘ Reachab				
		<b>⊳</b>	Run Commands 🛛 🖻 View 360 🔹 Last updated: 5:13 PM 📿 Refresh	
Details Interfaces	Wireless Info Mobility			
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 IN	MAGES			
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.

evices - Fabric Serv	vices								- 1
Find Hierarchy	DEVICES (6) FOCUS: Inventory ~			Global				Take a Tour 📃	24
🗞 Global	DEVICE TYPE All Routers	Switches APs WLCs	REACHABILITY	Reachable Unreachable					
<ul> <li>Unassigned Devices</li> <li>San Jose</li> </ul>	∀ Filter     Add Device     Tag Devi	ice Actions V ()	Selected					Last updated: 5:13 PM	0
	Device Name	Inventory > Software Image >	Device Family Site	Reachability	MAC Address	Device Role	Image Version	Uptime	rš.
	CONTROL-PLANE.cisco.com 0	3. Provision > 3. Device Replacement>	Assign Device to Site	22/Floor3 🔗 Reachable	d4:ad:71:30:a7:00	ODISTRIBUTION	16.11.1c	14 days 20 hrs 18 mins	
	FE1-9300-03.cisco.com 6	3 Others >	Provision Device	22/Floor3 ② Reachable	00:29:c2:be:0e:00	Ø ACCESS	16.11.1c	18 days 16 hrs 13 mins	v
	FE2-9300-04.cisco.com C	3.3.3.13 Supported	LAN Automation Status	22/Floor3 🕗 Reachable	00:29:c2:27:51:00	Ø ACCESS	16.11.1c	18 days 16 hrs 08 mins	ν.
	<	3.3.3.5 Supported	Learn Device Config Configure WLC HA	22/Floor3 🕗 Reachable	38:ed:18:67:a6:00		16.11.1c	43 days 20 hrs 48 mins	v
		3.3.3.1 Supported		22/Floor3 Reachable	c0:67:af:ed:af:80	Ø ACCESS	16.11.20190312:035643	107 days 20 hrs 06 mins	- N

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

Cisco DNA Center Design PC	LICY PROVISION ASSURANCE PLATFORM	
Provision Devices		
	3 Advanced Configuration (4) Summary	
Serial Number FCW2221M0JT	Devices WLC-3504	බ්ඩු Global/San Jose/Building 22/Floor3 $ imes$

**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.

Cisco DNA Center DE	ESIGN POLICY PRO	VISION ASSURANCE	PLATFORM	
Provision Devices				
1 Assign Site 2 Cont	figuration 3 Advance	d Configuration (4) s	ummary	
♥ WLC-3504	Serial Number	Devices	WLC Role	
	FCW2221M0JT	WLC-3504	Active Main WLC	Managing 1 Primary location(s)
			⊖ Guest Anchor	Relect Secondary Managed AP Locations
	Mobility Group			
	Name RF C	onfigure Reset		

**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.

Provision	Devices	
1) Assi	n Site 2 Configuration 3 Advanced Configuration 4	nmary
WLC-	✓ Device Details	
3504	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
	<ul> <li>Network Setting</li> </ul>	
	AAA Client Server:	AAA clarity indpoint settings are configured based in the settings added for each Managed AP location.
		WARRENE: Do not use "admin" as the username for your device CLI credentias, if you are using IDE 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
	<ul> <li>SSID (employee)</li> </ul>	
	Name	pbsqqa-internal
	Type:	Enterprise
	Security:	wpa2_personal
	Fast Transition:	Adaptive
	Traffic Type:	Voice + Data
	Fabric Enabled:	No O
	Fast Lane enabled:	No
	Mac Filtering Enabled:	No
	Flex Connect enabled:	No
	Broadcast Enabled:	Yes
	Admin Otobury	Exclusion

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.

1 Assign Site (	2 Configuration	3 Advanced Configuration	4 Summary	Optional
⊻ Ma	naged 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)
⊻ Ro	ling AP Upgrade			
Rolling	AP Upgrade			Disabled
AP Reb	oot 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.

ululu cisco	Saye Configuration Ping Logout <u>R</u> ef MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT COMMANDS HELP <u>F</u> EEDBACK <u>A H</u>
Security	RADIUS Authentication Servers Apply New
AAA     General     FADIUS     Authentication     Accounting     Fallback     DNS     Downloaded AVP     TACACS+     LDAP	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
Local Net Users MAC Filtering	User Management Proxy Index Server Address(Ipv4/Ipv6) Port IPSec Admin Status
<ul> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul>	✓ ✓ □ <u>1</u> * 10.195.180.131 1812 Disabled Enabled
Local EAP	
Advanced EAP	
Priority Order	
Certificate	
Access Control Lists	
Wireless Protection Policies	
Web Auth	
TrustSec	
Local Policies	
Umbrella	
Advanced	

cisco	MONITOR V	<u>V</u> LANs	CONTROLLER WIF	RELESS <u>s</u> ec	URITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		Sa <u>v</u> e Configuration	<u>P</u> ing Lo	gout   <u>R</u> efresh n <u>H</u> ome
WLANs	WLANs											Entrie	es 1 - 2 of 2
▼ WLANs WLANs	Current Filter:	Non	e [Change]	Filter] [Clear Fi	lter]				Create New	Go			
Advanced	WLAN ID	Туре	Profile Name	2		WLAN SSID			Admin Status	Security Policies			
	<u>17</u>	WLAN	Internal03_F_	2866e		Internal03			Disabled	[WPA2][Auth(802.1X)]			
	18	WLAN	Guest03_F_45	50ae		Guest03			Disabled	MAC Filtering			

## Screenshot for Cisco Catalyst 9800 WLC:

Cisco Cata	yst 9800-CL Wireless Controller	Welcome sand		¢ 🗄	• •	0	Q	Search	n APs and I
Q Search Menu Items	Configuration > Tags & Profiles > WLANS								
📻 Dashboard	+ Add × Delete Enable WLAN Disable WLAN								
Monitoring >	Number of WLANs selected : $0$								
🔍 Configuration 🕠	🗋 Status Վ Name 🗸 ID	V SSID						~	Security
~	sand-cyclo_Global_F_88f47f3f 17	sand-cyclops-o	pen						[open]
(⊙) Administration →	A\$\$oc1at#_Global_F_3883b8c1 18	A\$\$oc1at#							[open]
💥 Troubleshooting	I → I I → I I0 v items per page								

## 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.

#### 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.

Devices ✓ <b>Fabric</b> S	Services		
Devices V Fabric 3	services		
	obrigg of	ad Tranait/Da	ar Notworko
		nd Transit/Pee	
shoose a rablic of fransit/reer N	etwork below to mana	ge, or add a new item by clicking #	add Pablic of Transit/Peer Network.
Fabrics 🔒			
Fabrics 🛈			
Fabrics 0			
Fabrics 🕚			
Fabrics ① Default LAN Fabric	c	∎ San Jose	
Default LAN Fabric		San Jose	
	Device		

#### 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.

Cisco DNA Center	ESIGN	POLICY PROVISION ASSURANCE PLATFORM	∠● ♀ Ⅲ ♦ ♀ Ⅲ
Devices ~ Fabric Se	ervices		
Fabric-Enabled Sites	•	All Fabrics > Floor3 San Jose	Eq. Find by device IP, type, role, family & MAC 👔 🗈
EQ. Find Hierarchy		⊘ Fabric Infrastructure ⊘ Host Onboarding	Show Task Status
V 🖉 San Jose		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.	Х
<ul> <li>→ 品 San Jose</li> <li>→ 品 Building 22</li> </ul>			Collapse All Custom View Mar 12, 2020 5:33 PM
€ <b>9</b> Floor3	٥	pb-fusion-router	
		NT-BOR.cisco.com	କ୍ କ୍ ତ
			Cancel Save

WLC-3504 (192.168.1.10)	s 7 minutes	×	WLC-3504 (192.168.1.10)	×
Details Fabric Port Channel Interfaces Wire	Run Commands C View 360 Last updated: 5:34 PM	⊖ Refresh	Run Commands         (f' Vew 360         Last updated: 5:34 PM           Details         Fabric         Port Channel         Interfaces         Workless Info         Mobility	📿 Refresh
Remove From Fabric Fabric To Writem			Remove From Fabric Fabric www.	
		Cancel And		Cancel Add

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

**		Modify Fabric Domain	×
pb-Halton-roder Pt-Halton-roder Pt-Halton-roder Pt-Halton-roder COVITR. E Lancacom COVITR. E Lancacom COVITR. E Lancacom FEI-9A.cisco.com FEI-9A.cisco.com	9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9	When • Now O Later Cancel Apply	

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

Cisco DNA Center DESIGN	POLICY PROVISION ASSURANCE PLATFORM	∠ <b>0</b> Q Ⅲ Φ © Ⅲ
Devices V Fabric Services		
Fabric-Enabled Sites	All Fabrics > Food3 San Jose	EQ. Find by device IP, type, role, family & MAC 👔 😫
EQ. Find Hierarchy	Fabric Infrastructure     O Host Onboarding	Show Task Status
✓ 🖉 San Jose	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.	×
マ 後 San Jose マ 後 Building 22		Collapse All Custom View Mar 12, 2020 5:33 PM
S Floor3 o	pb-fusion-router	
	CONTR.E.cisco.com	ଞ୍ ସ (୦)
		Cancel Save

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.

Cisco DNA Center	ESIGN	POLICY PROVISION ASSURANCE PLATFORM
Devices ~ Fabric S	ervices	
Fabric-Enabled Sites	<b>e</b>	All Fabrics > Floor3 San Jose
EQ Find Hierarchy		⊘ Fabric Infrastructure ⊘ Host Onboarding
<ul> <li>✓ ③ San Jose</li> <li>✓ 灸 San Jose</li> <li>✓ 灸 Building 22</li> </ul>		> Authentication Template
Set Floor3	٥	> Virtual Networks
		> Wireless SSID's
		> Port Assignment

**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.

Cisco DNA Center	DESIGN	POLICY PROVISION ASS	SURANCE	PLATFORM						0	Q		o c	
Devices ~ Fabric	Services		Edit V	/irtual Networl	k: INFRA	A_VN								
Fabric-Enabled Sites	•	All Fabrics > Floor3 San Jose												
EQ, Find Hierarchy		Ø Fabric Infrastructure	Advar	nced View						C C	Reset	🖞 Exp	port	<b>A</b>
✓ Ø San Jose ✓ Ø San Jose		> Authentication Temp		Delete							Ξ	Q Find		
				IP Address Pool		Pool Type	Authenticatio	n Policy	Layer-2 Extension		Layer-2	Flooding		
Floor3	¢	<ul> <li>Virtual Networks</li> <li>Select a Virtual Network (</li> </ul>		SJC-AP		AP	SJC-AP		Enabled		Disabled	1		
		Critical Pool: Not Select						Showing 1 of 1						
		> Wireless SSID's												
		> Port Assignment												
											Cancel		Sa	ve

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.

Cisco DNA Center	DESIGN	POLICY PROVISION ASSURANCE PLATFORM		∠● Q. Ⅲ & ◎ Ⅲ
Devices V Fabric	Services			
Fabric-Enabled Sites	•	All Fabrics > Floor3 San Jose		
EQ. Find Hierarchy		⊘ Fabric Infrastructure ⊘ Host Onboarding		Show Task Status
<ul> <li>         、</li></ul>		<ul> <li>Authentication Template</li> <li>Select Authentication Template ①</li> </ul>		
SFloor3	٥	Settings will be applied to all Fabric Edge host ports, unless over	erridden by a static port assignment.	
		Open Authentication ()	Edit	
		Closed Authentication ()	Edit	
		O Low Impact ()	Edit	
		No Authentication ()		
			Set a	is 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".

Selected Interfaces (1) Gigabl/Ethernet1/0/4	
Connected Device Type Access Point(AP)	∞ ^
Eq. Search Dropdown	
User Devices (ip-phone,computer,laptop)	
Access Point(AP)	
Server	
Description	

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. <u>ISE Profiling Design Guide</u>

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
T
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:

dialle Identity Services Engine	Home Context V	isibility 🔹 Op	erations - Policy - Ad	ministration        Work Centers						
Policy Sets Profiling Posture Cli	ient Provisioning 🔹 🕨 P	olicy Elements					Click here to	do wireless setup and visibili	ity setup Do not show	this again. ×
(+)						Result	5			
Status Rule Name	Cond	itions				Profile:	s S	Security Groups	Hits	Actions
Search										
Similar Wired MAB	2	Normalised Ra	adius:RadiusFlowType EQUALS	WiredMAB		×Per	mitAccess +	Auto create security group Select from list	• + 2	¢
May 03, 2020 12:37:21.973 PM	0	9	0 ap1234	78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Prot	filing	Ap_template_retu	m_1
	0	0	0 ap1234 ap1234	78:72:5D:ED:CC:1A 78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800	Default >> Dot1X Default >> Dot1X	Default >> Cisco_AP_Prot Default >> Cisco_AP_Prot		Ap_template_retu Ap_template_retu	
May 03, 2020 12:37:21.973 PM May 03, 2020 12:37:21.957 PM May 03, 2020 12:37:21.908 PM		-						filing		
May 03, 2020 12:37:21.957 PM	_	0	ap1234	78:72:5D:ED:CC:1A 78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800	Default >> Dot1X	Default >> Cisco_AP_Prof	filing filing		m_1
May 03, 2020 12:37:21.967 PM May 03, 2020 12:37:21.908 PM		0	ap1234 ap1234	78:72:5D:ED:CC:1A 78:72:5D:ED:CC:1A cC:1A 78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800	Default >> Dot1X Default >> Dot1X	Default >> Cisco_AP_Prot	filing filing filing	Ap_template_retu	m_1 m_1
May 03, 2020 12:37:21.967 PM May 03, 2020 12:37:21.908 PM May 03, 2020 12:35:28.569 PM May 03, 2020 12:35:00.498 PM			ap1234 ap1234 78:72:5D:ED	78:72:5D:ED:CC:1A 78:72:5D:ED:CC:1A cC:1A 78:72:5D:ED:CC:1A	Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800	Default >> Dot1X Default >> Dot1X Default >> MAB	Default >> Cisco_AP_Prot Default >> Cisco_AP_Prot Default >> Cisco_AP_Prot	filing filing filing	Ap_template_retu Ap_template_retu	m_1 m_1
May 03, 2020 12:37:21.957 PM May 03, 2020 12:37:21.908 PM May 03, 2020 12:35:28.569 PM May 03, 2020 12:35:00.496 PM May 03, 2020 12:35:00.496 PM		0 0 0	ap1234 ap1234 78:72:5D:ED	78:72:50:ED:CC:1A 78:72:50:ED:CC:1A CC:1A 78:72:50:ED:CC:1A CC:1A 78:72:50:ED:CC:1A 78:72:50:ED:CC:1A	Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800	Default >> Dot1X Default >> Dot1X Default >> MAB	Default >> Cisco_AP_Prot Default >> Cisco_AP_Prot Default >> Cisco_AP_Prot	filing filing filing	Ap_template_retu Ap_template_retu	m_1 m_1 m_1
May 03, 2020 12:37:21.957 PM May 03, 2020 12:37:21.908 PM May 03, 2020 12:35:28.569 PM			ap1234 ap1234 78:72:5D:ED 78:72:5D:ED	78:72:50:ED:CC:1A 78:72:50:ED:CC:1A CC:1A 78:72:50:ED:CC:1A CC:1A 78:72:50:ED:CC:1A 78:72:50:ED:CC:1A	Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800 Cisco-AP-Aironet-4800	Default >> Dot1X Default >> Dot1X Default >> MAB Default >> MAB	Default >> Cisco_AP_Prot Default >> Cisco_AP_Prot Default >> Cisco_AP_Prot Default >> Cisco_AP_Prot	filing filing filing	Ap_template_retu Ap_template_retu Ap_template_retu	m_1 m_1 m_1

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:

_											
cisc	liger linder	ntity Serv	vices Engine Home 🔸 🤇	Context Visi	bility	▼Policy	Administration	<ul> <li>Work Centers</li> </ul>			
Po	olicy Set	ts Profil	ling Posture Client Provisionir	ig ⊧Poli	icy Elements				Click here to do wireless setup and visibility setup Do not sh	ow this :	again. ×
									Results		
	+	Status	Rule Name	Conditio	ons				Profiles Security Groups	lits	Actions
C	Search										
		0	Cisco_AP_Profiling	Ê; I	EndPoints-LogicalProfile E	QUALS Cis	co AP		(*Ap_template_return_1) + Select from list +	87	ф

## Profiling information on ISE:

oning information on	1821					
dentity Services Engine	Home   Contex	t Visibility 🔹 🕨 Operatio	ns <b>&gt;</b> Policy <b>&gt;</b> .	Administration	✓Work Centers	
Network Access	▶ TrustSec → BYC	DD Profiler Pos	ture 🔹 🕨 Device Admini	stration 🕨 Passi	velD	
verview Ext Id Sources Network D	evices Endpoint Clas	sification Node Config	Feeds 🔸 Manual Sca	ns 🔸 Policy Elem	ents Profiling Policies P	olicy Sets 🔸 Troubleshoot Repo
ENDPOINTS <sup>®</sup>		e o El		GORIES	<b>P</b> 0	NETWORK DEVICES
Type Profile			OUI OS Types Identity			Location Type Device Nam
mise: [80%]_	_ workstatic	ons: [50%]	apple, inc.: [50%]_	0	_ cisco, inc: [50%]	lceartions" [100%]
Selected C + Ø	Change Authorization	<ul> <li>Clear Threats &amp; Vuller</li> <li>IP Address</li> </ul>	Inerabilities Export	- Import - Hostname	MDM Actions + Release	Rejected Revoke Certificate
× MAC Address	Anomalous Beha	IP Address	Username	Hostname	Location	Endpoint Profile
	Allollialous belle			Tiostianie		
78:72:5D:ED:CC:1A		9.11.50.202	ap	-	Location + All Lo.	Cisco-AP-Aironet-4800
uldentity Services Engine     Home       Network Access     Quest Access     TrustSec       enview     Extld Sources     Network Devices     Endpd       ndpoints     - 78:72:5D:ED:CC:1A     Ø Ø Ø	Context Visibility      F Operatio     BYOD      Profiler      Post	ns	PassiveID	м <i>5</i> 0.		

Current IP Address: 9.11.30.202 Location: Location + All Locations Applications Attributes Authentication Threats Vulnerabilities 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 Cisco AP Software, ap3g3-k9w8 Version: 16.12.2.132 Technical Support: http://www.cisco.com/techsup 14-2015 by Cisco Systems, Inc. cdpCacheVersion Cisco AP Software, ap3g3-k9w8 Version: 16.12.2.132 Technical Support: http://www.cisco.com/lechsup 86-2019 by Cisco Systems, Inc. Compiled Sun Dec 15 03:23:03 PST 2019 by vipendya lidpSystemDescription

Authorization profile for Access point

uthorization Profiles > Ap_							
uthorization Profile							
* Name	Ap_template_	_return_1			:		
Description							
* Access Type	ACCESS_ACCE	PT	*				
Network Device Profile	🎎 Cisco 👻	$\oplus$					
Service Template							
Track Movement							
Passive Identity Tracking							
assive identity fracking	(i)						
▼ Common Tasks							
I MACSec Policy							
NEAT							
		ApAuta	zTemplate				
NEAT Interface Template		ApAut	zTemplate				
☑ Interface Template	Local Web Auth)		zTemplate				
	Local Web Auth)		zTemplate				
☑ Interface Template	Local Web Auth)		z Template				
☑ Interface Template	Local Web Auth)		zTemplate				
☑ Interface Template			zTemplate				
Interface Template Web Authentication ( Advanced Attribute	es Settings		2Template				
✓ Interface Template Web Authentication (I	es Settings	)	2Template				
Interface Template     Web Authentication (     Advanced Attribute	es Settings	)	:Template				
Interface Template     Web Authentication (     Advanced Attribute	es Settings	)	zTemplate				
Interface Template Web Authentication (I Advanced Attribute Select an item Attributes Details	es Settings	)	:Template				
Interface Template Web Authentication ( Advanced Attribute Select an item	es Settings	)					
Interface Template  Web Authentication ( Advanced Attribute  Select an item  Attributes Details  Access Type = ACCESS_	es Settings	)					
Interface Template  Web Authentication ( Advanced Attribute  Select an item  Attributes Details  Access Type = ACCESS_	es Settings	)			ISE	<u>COA a</u>	nd su
Interface Template Web Authentication (I Advanced Attribute Select an item Select an item Attributes Details Access Type = ACCESS_clsco-av-pair = interface-I ay 03, 2020 12:37:21.973 PM	ACCEPT template-name=	)		ap1234	1	/8:72:5D:ED:C	C:1A
Interface Template Web Authentication (I Advanced Attribute Select an item Select an item Attributes Details Access Type = ACCESS_clsco-av-pair = interface-I ay 03, 2020 12:37:21.973 PM ay 03, 2020 12:37:21.977 PM	ACCEPT template-name=	) = [	nplate	ap1234	1	78:72:5D:ED:C 78:72:5D:ED:C	C:1A C:1A
Interface Template Web Authentication (I Advanced Attribute Select an item Select an item Attributes Details Access Type = ACCESS_clsco-av-pair = interface-I ay 03, 2020 12:37:21:973 PM ay 03, 2020 12:37:21:977 PM ay 03, 2020 12:37:21:978 PM ay 03, 2020 12:37:21:908 PM	ACCEPT template-name=	= [	nplate	ap1234 ap1234	1	78:72:5D:ED:C 78:72:5D:ED:C 78:72:5D:ED:C	C:1A C:1A C:1A
Interface Template Web Authentication (I Advanced Attribute Select an item Select an item Attributes Details Access Type = ACCESS_clsco-av-pair = interface-I ay 03, 2020 12:37:21.973 PM ay 03, 2020 12:37:21.977 PM	ACCEPT template-name=	=	nplate	ap1234	1 1 1 C:1A 1	78:72:5D:ED:C 78:72:5D:ED:C	C:1A C:1A C:1A C:1A

#### ISE COA and subsequent re-authentication:

May 03, 2020 12:37:21.973 PM	0		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		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 12:37:21.908 PM	<b>~</b>	Q		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		0		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		0		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	<b>~</b>	0			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM	<b>~</b>	Q		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		0			78:72:5D:ED:00:1A				
May 03, 2020 12:34:19.052 PM		Q		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.

Cisco DNA Center	Template Ed
EQ. Find template	9800-eap ×
∧ Onboarding Configuration	
✓ 9800-template	Actions v   Edit v   9800-eap
9800-eap 💠	Template
<ul> <li>switch-preauthacl</li> <li>Cloud DayN Templates</li> </ul>	<pre>1 ap profile default-ap-profile 2 description "default ap profile" 3 dot1x eap-type eap-peap</pre>
	4 dotlx username <b>ap1234</b> password 0 <b>ap1234</b>

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	9	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	<ul> <li>Image: A set of the set of the</li></ul>	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 12:37:21.908 PM		9		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	<u>~</u>	9		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	<b>~</b>	0		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	<b>~</b>	9			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.444 PM	<ul> <li>Image: A set of the set of the</li></ul>	Q		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	<b>~</b>	0			78:72:5D:ED:CC:1A				
May 03, 2020 12:34:19.052 PM	×	0		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

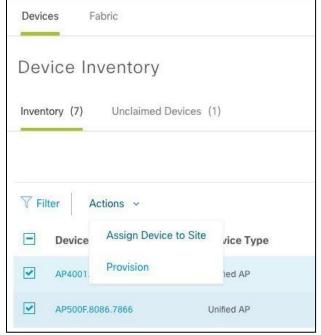
**Step 1** Go back to Provision > Devices > Inventory to see the APs joining the fabric-enabled wireless controller.

sco	DNA Center				Design Policy	Provis
Devic	es Fabric					
Dev	vice Inventory					
Inve	ntory (5) Unassigned [	Devices				
-						
71	t Devices 🗸					
		Device Type	IP Address	Site	Serial Number	
71	Filter	Device Type Unified AP	IP Address 9.6.51.53	Site SJC-14	Serial Number KWC193904BH	
7;	Filter Device Name					
	Filter Device Name AP1850-Edge1	Unified AP	9.6.51.53	SJC-14	KWC193904BH	
	Device Name AP1850-Edge1 AP3800-Edge1	Unified AP Unified	9.6.51.53 9.6.51.54	SJC-14 SJC-14	KWC193904BH FCW2034NWUX	

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.

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.

CISCO CENTER	DESIGN POLICY	PROVISION ASSURANCE	Q III 💠 🗉
Devices Fabric			
Assign Device	to Site		
			Close
Serial Number FDW2130B3L2	Devices AP4001.7A70.6004	Choose a facor	
FDW2130B3KR	AP500F.8086.7866	…Diegem/Floor-1/Diegem …Icor-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.

Devices F	abric	
Device Ir	iventory	
Inventory (7)	Unclaimed Devices (	1)
∑ Filter	Actions ~	
<ul><li>✓ Filter</li><li>✓ Device</li></ul>	Actions ~ Assign Device to Site	/ice Type
		vice Type

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.

Devices Fabric			
Provision De	evices		
1 Assign Site	2 Configuration	3 Summary	
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

#### Click Run Now in the window that pops up.

Devices Fabric			
Provision Devices	Summary		
AP4001.7A70.6004	<ul> <li>Device Details</li> </ul>		
AP500F.8086.7866	Device Name: Serial Number: Mac Address Device Location: RF Profile: Radio Type: Channel Widht: 2.4GHz/5GHz Data Rates	AP4001.7A70.6004 FDW213083L2 70:70.8b.20:29:00 Floor-1 TYPICAL 2.4GHz/5GHz 20 MHz 9.12.18.24.36,48.54/6.9,12,18.24.36,48,54	
			Cancel Deploy
Provision Device		×	
💿 Run Now	O Schedule Later		
j	Cancel	Арріу	

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



**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).

،،ا،،،ا،، cısco	<u>M</u> ONITOR	<u>w</u> lans <u>(</u>	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK		Save Configuration	<u>P</u> ing		<u>R</u> efrest
WLANs	WLANs											E	ntries 1 -	5 of 5
WLANs WLANs	Current Filter	None	[Chan	<u>ge Filter] [Clea</u>	r Filter]			Create Ne	W Y	Go				
<ul> <li>Advanced</li> </ul>														
AP Groups	WLAN ID	Туре	Profile Na	ne		WLAN SSID		Admin	Status Secu	rity Policies				
	<u>1</u>	WLAN	ssid-1			ssid-1		Disable	ed [WPA	2][Auth(802.	1X)]			
	<u>17</u>	WLAN	Guest-WiFi	Global_F_c4d	14f67	Guest-WiFi		Disable	ed MAC	Filtering				
	<u>18</u>	WLAN	pbagga-int_	Global_F_16a	cea8c	pbagga-internal		Disable	ed [WPA	2][Auth(PSK)	)]			
	23	WLAN	pbagga-em	p_Global_F_31	ddd44d	pbagga-employee-c	pen	Disable	ed None			-		
	24	WLAN	pbagga123	4_Global_F_c8	cc58b2	pbagga1234		Disable	ed [WPA	2][Auth(PSK)	)]			
	<u>24</u>	WLAN	pbagga123	4_Global_F_c8	cc58b2	pbagga1234		Disable	⊧d [WPA	2][Auth(PSK	1			

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

ahaha										Save Configuration Pi	ng	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK			<mark>n</mark> <u>H</u> ome
WLANs	AP Group	)\$								Entries 1 - 2 o	of 2	Add Group
VLANs WLANs	AP Group !	Name		A	P Group Desc	ription						
<ul> <li>Advanced</li> <li>AP Groups</li> </ul>	Floor3 TVPI default-grou		<u>4</u>									

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:

Cisco Cata	alyst 9800-CL Wireless Controller		Welcome sand	<b>6</b> E 4
Q Search Menu Items	Configuration * > Wireless * > Access Points	Edit AP		
🔜 Dashboard	All Access Points	Location*	Global/colarado/den	Predowr
	Number of AP(s): 1	Base Radio MAC	7872.5dee.53c0	Predowr
Monitoring >		Ethernet MAC	7872.5ded.cc1a	Next Ret
🔾 Configuration 🕠	AP          Admin          IP          Base Radio          AP            AP Name          Model         Stots          Status         Address         MAC         Mode	Admin Status		Boot Ver
🕥 Administration 🕠	sand-4800- AIR-AP4800- site2 👬 A-K9 3 🥑 9.11.50.202 7872.5dee.53c0 Local	AP Mode	Local v	IOS Vers
💥 Troubleshooting	H 4 1 > 10 v items per page	Operation Status	Registered	Mini IOS
Ψ.V		Fabric Status	Enabled	IP Conf
	> 5 GHz Radios	LED State	ENABLED	CAPWA
	> 2.4 GHz Radios	LED Brightness Level	8 🗸	DHCP IP
	Dual-Band Radios	CleanAir <u>NSI Key</u>		Static IP
		RLOC IP	9.201.201.14	Time St
	> Country	Control Plane Name	default-control- plane	Up Time
	LSC Provision	Tags		Controlle
		Policy	PT_denve_BGL11_F	
		Site	default-site-tag 🔻	
		RF	TYPICAL	

# Details of Policy Tag:

Q Search Menu Items	Configuration > Tags & Profiles > Tags	Edit Policy Tag
Dashboard	Policy Site RF AP	A Changes may result in loss of connectivity for some clients that are associated to APs with the
Monitoring >	+ Add X Delete	Name* PT_denve_BGL11_F
🔾 Configuration 🔹 🔸	Policy Tag Name	Description PolicyTagName PT_(
🏹 Administration 🕠	default-policy-tag	WLAN-POLICY Maps: 3
	PT_denve_BGL11_F1_45efe	
₩ Troubleshooting	I → I I → I IO v items per page	+ Add × Delete
		WLAN 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
		H ◀ 1 ► H 10 v items per page

<b>Q</b> Search Menu Items	Co	onfiguration • > Tags & Profiles • > Tags	E	dit RF Tag	
				Name*	TYPICAL
🔜 Dashboard	-	Policy Site RF AP		Description	Enter Description
Monitoring :				5 GHz Band RF Profile	Typical_Client_Densi
🔧 Configuration 🛛 🤅	>	RF Tag Name		2.4 GHz Band RF Profile	Typical_Client_Densi
() Administration	>	TYPICAL			
-		default-rf-tag			
X Troubleshooting		I I I I I I I I I I I I I I I I I I I			

## Details of the Site tag:

Q Search Menu Items	Configuration > Tags & Profiles > Tags	Edit Site Tag
	Policy Site RF AP	Name* default-site-tag
Monitoring >	+ Add × Delete	AP Join Profile default-ap-profile v
🔾 Configuration 🕠	Site Tag Name	Control Plane Name
Administration	default-site-tag	Enable Local Site
💥 Troubleshooting		

# **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 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.

Cisco DNA Center design policy provision assura	4C	Cisco DNA Center	DESIGN	POLICY	PROVISION	ASSURANCE	PLATFORM
Devices V Fabric Services		Devices 🗸 🛛 Fabric	Services				
SD-Access Fabrics and Transit/Per Choose a Fabric or Transit/Peer Network below to manage, or add a new item by clicking		Fabric-Enabled Sites	•	All Fabr Calif(	es > california Drnia		
		EQ Find Hierarchy					
Fabrics 🕕		✓ Ø california ✓ B Sanjose				<b>A</b> D	
Default LAN Fabric california		へ (武) B 11	۵		sand-cp.sand.com	B11 B sandsand.	
0 Site , 0 Fabric Device 0 Control Plane , 0 Border LAN LAN							

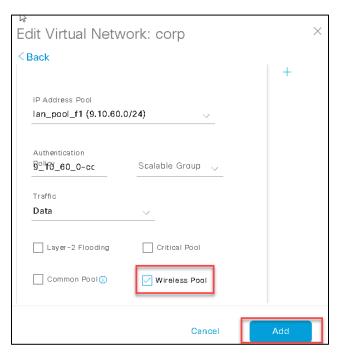
**Step 2** With Cisco DNAC 1.3.3 if a new VN is created, it needs to be manually added to a fabric. For migration to 1.3.3 all the VN's that existed on the previous version would be available on the host onboarding page. If the VN' are not available on the host onboarding page, click on the "Gear" icon 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.

Cisco DNA Center	DESIGN	POLICY	PROVISION	ASSURANCE			<b>2</b> 24
Devices 🗸 🛛 Fabric	Services				Add	Virtual Network	
Fabric-Enabled Sites	•	All Fabrics COlrad	> colarado O		Selected	virtual network(s) will be used	in the Fabric.
EQ Find Hierarchy		⊘ Fa	bric Infrastructi	ure 🤗 Host On			
v 🖉 colrado						Virtual Network 🔺	
∧ 🖑 colarado	\$	> Au	uthentication -	Femplate		VIRtual Network	
Add VN	To Site 🕕 🛩		'N's to a fabirc sit			CAMPUS	
			rtual Network Select a Virtual Net	S work to associate one c		DEFAULT_VN	
Configu	re Multicast 🛈		Critical Pool: Not :			guest	
Delete	Site						
			INFRA_VN				
All Fabrics > colarado COITADO							
⊘ Fabric Infrastru	cture	) Host O	nboarding			Show 1	Fask Status
✓ Virtual Netwo	rks						
Select a Virtual I	letwork to ass	ociate one	or more IP Pool(	s) with the selected	VN.		
Critical Pool: N	ot Selected				[	+ Add Virtual Ne	twork
INFRA_VN			corp				

**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 V	Edit Virtual Network: corp $ imes$										
Advan	ced View	G Reset	ort Add								
Actions	~		ΞQ Find								
	IP Address Pool ▲	Authentication Policy	Traffic Type	Layer-2 Flooding							
		No data to display	ł								



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).

	eless SSID's 🎝	ł						
	Enable Wireless	s Multicast					Reset	Save
							ΞQ Find	
-	SSID Name	Туре	Security	Traffic Type	Address Pool	Scalable Group		
	sand-site1- 1x	Enterprise	WPA2 Enterprise	Voice + Data	Choose Pool 9_10_60_0-corp 🛛 🗸 🗸	Assign SGT		<u> </u>

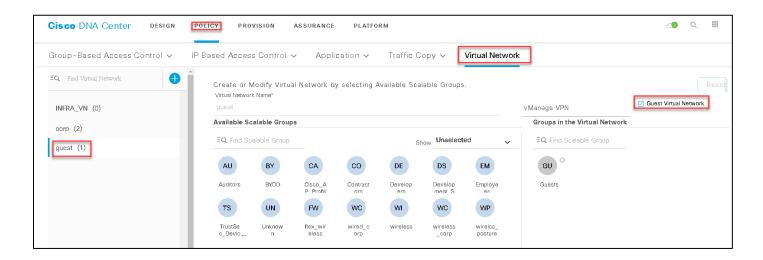
## **Onboarding guest clients**

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.



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.

RAII Fabrics > B11 California				
⊘ Fabric Infrastructure	⊘ Host Onboarding			Show Task S
> Authentication Templa	ate			
✓ Virtual Networks				
Select a Virtual Network to a	associate one or more IP Pool(s) with the s	elected VN.		
Critical Pool: Not Selected	ł			+ Add Virtual Network
DEFAULT_VN	INFRA_VN	corp	guest	$\mathbf{\mathbf{v}}$
		COLD	80001	

Edit V	Edit Virtual Network: guest							
Basic	View	G Reset	1 Export	🕂 Add				
Actions	$\sim$	Ξ	Q Find					
	IP Address Pool 🔺	Authentication Policy	Traffic Type	Scalable Group				
	guest_poo 1	9_10guest	Data	-				
		Showing 1 of 1						
	Basic	Basic View Actions ∨ IP Address Pool ▲	Basic View     ♀ Reset       Actions ∨     ≡       IP     Address       Address     Authentication Policy       Pool ▲     9_10guest	Basic View     ♀ Reset     ① Export       Actions     ✓     ΞQ Find       □     IP Address Pool ▲     Authentication Policy     Traffic Type       □     guest_poo 1     9_10guest     Data				

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.

→ Wir	eless SSID'	s						
	Enable Wirele	ss Multicast					Reset	Save
	SSID Name	Туре	Security	Traffic Type	Address Pool	Scalable Group		
	sand-guest- 1	Guest	Web Auth	Data	Choose Pool	Assign SGT		<u>~</u>
	sand-site1-	Enterprise	WPA2 Enterprise	Voice + Data	9_10_61_0-guest	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.

		Enable Guest	×
All Failings > colarado COITADO	sand-csr-2.sand.com (9.1.0.249) ⊛ ⊘ Reachable Uptime: 30 days 5 hours 42 minutes	Select the role(s) you intent to assign	
⊘ Fabric Infrastructure	Reachable Uptime: 30 days 5 hours 42 minutes	Select the role(s) you interit to assign	
2 device(s) in this site are not comp	Run Commands D' View 36 Details Fabric Port Channel Configuration Interfaces		
	Remove From Fabric	Set as default border	
	Fabric	Routing Protocol BGP V	
Click on the node	E Edge Node	● ASPLAIN ○ ASDOT ○ ASDOT+	
<	B Border Node	Routing AS number/process 65003	
sand-csr-Z.sand.com	G Guest Border / Control Plane		
		Select one quest virtual network	
		Cancel	Enable

**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."

Cisco Cata	Catalyst 9800-CL Wireless Controller							<b>V</b> o	ß	•	9 0	0	Search APs and C
Q Search Menu Items	Configura	ation • > T	ags & Profiles • > WLANs										
Dashboard	+ Add	X De											
Monitoring >	Number o	of WLANs :	selected : O										
Configuration >		Status v	Name	Ŷ	ID v	SSID	~	Securi	ty				
~		0	sand-guest_Sanjos_F_927bb184		17	sand-guest-1		[open]	MAC F	iltering			
() Administration >		0	sand-site1_Sanjos_F_6e15a102		18	sand-site1-1x		[WPA2	][802.	1x][AES]			
	I4 4	1 × ×	10 🔻 items per page										

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

	Catalyst	9800-CL Wireless Contro	ller							Welc	ome sa	and	<b>* b</b>	8	•	9 0
Q Search Menu Items	Ma	onitoring >> Wireless >> Clier	its													
Dashboard Clients Steeping Clients Excluded Clients																
Monitoring	Monitoring > X Delete															
🔧 Configuration		Fotal Client(s) in the Network: 2														
O Administration	>	Number of Client(s) selected: 0 Client MAC Address		IPv4 Address	AP Name	~	SSID	~	WLAN ID V	State	Ŷ	Protoco	ol v	Use	r Nam	e v
💥 Troubleshooting		1c36.bb00.1704	ж	9.10.60.204	sand-3800-site1	-	sand-site1-1x	-	18	Run		11ac		sand		1
		1c36.bbee.09b4	×	9.10.61.200	sand-3800-site1		sand-guest-1		20	Run		11ac				
		14 4 <b>1</b> > 10 v iten	ns per page	9												

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

Monitoring >> Wireless >> Clients				Client			
				360 View General QOS Statisti	cs ATF Statistics Mobility		
Clients Sleeping Clients Excluded Clients				Client Properties AP Properties	Security Information Client St		
				VLAN	uerauit		
× Delete				Multicast VLAN	0		
Total Client(s) in the Network: 2			Server IP	9.1.0.20			
Number of Client(s) selected: 0		11v DMS Capable	No				
Number of Client(s) selected: O				QoS Map Capable	No		
Client MAC Address v IPv4 Address	ldress v IPv6 Address	AP Name v	SSID	FlexConnect Data Switching	N/A		
1c36.bb00.1704 👷 9.10.60.	204 fe80::6d87:cd22:da30:4472	sand-3800-site1	sand-site 🕅	FlexConnect Authentication	N/A		
1c36.bbee.09b4 🕺 9.10.61.	200 N/A	sand-3800-site1	sand-guest	FlexConnect Central Association	N/A		
H 1 F 10 V items per page				Control plane name	default-control-plane		
terris per page				antenna O	9 s ago36 dBm		
				antenna 1	9 s ago36 dBm		
Click on the client				EoGRE	No/Simple client		
mac to open the details				Туре	55 17		
details				Data	11		
				Fabric			
				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 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:

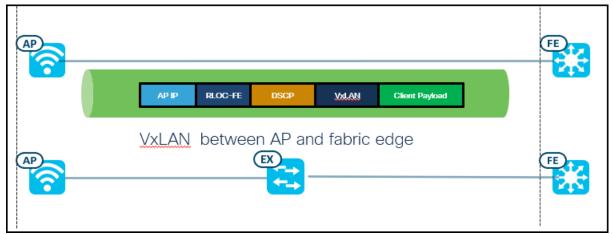
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise Mobility 8-1 Deployment Guide/ch5 QoS.html#73518

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
      RLOC IP (Source) AP IP (Destination) VRF ID Source Port Destination Port
Name
     _____
                   _____ ____
____
      9.254.254.71
Ac1
                   9.40.50.166
                                   0
                                         N/A
                                                   4789
      9.254.254.71
                   9.40.50.160
                                   0
Ac0
                                         N/A
                                                   4789
Name IfId
                 Uptime
0x0000004F 1 days, 13:12:22
Ac1
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:

սիսիս			_	_	_		Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER	W <u>I</u> RELESS	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	6 HE <u>L</u> P	<u>F</u> EEDBACK	User:nortel(ReadWrite) 🔒 Home
Wireless	QoS Map Config						Apply
Access Points     All APs     Radios	Qos Map Disable 👻						
802.11a/n/ac/ax 802.11b/g/n/ax	Up Stream			Dow	n Stream	ı	
Dual-Band Radios Dual-5G Radios Global Configuration	Trust DSCP UpStream  O UP to DSCP Map		DSCP to User Pric		0 🗸		
Advanced	Apply		DSCP St		0 -		
Mesh			DSCP Er		0		
AP Group NTP			Modify				
▶ ATF			DSCP to	JP Map List			
RF Profiles							
FlexConnect Groups FlexConnect ACLs			UP	Start DSCP	End DSCP		
FlexConnect VLAN			0	0	7		
Templates			1	8	15		
Network Lists			2	16	23		
Netflow							
QoS     Profiles     Roles     Qos Map			·				

Navigate to **wireless→Oos→OoSMap** 

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

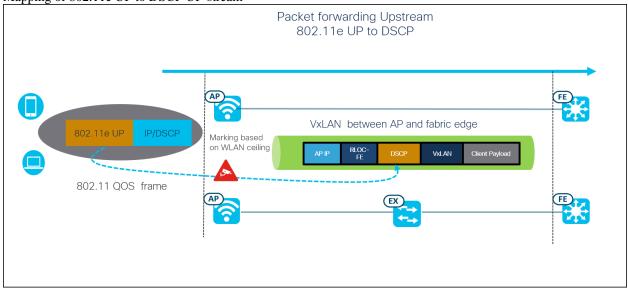
Cisco Catal	yst 9800–CL Wireless Controller	Welcome sand 🛛 🎓 😨 🖺 🌞 🙆 🚱 Srich APs and 🎤 🕪
Q Search Menu Items	Configuration > Tags & Profiles > AP Join	Edit AP Join Profile *
📷 Dashboard	+ Add X Delete	General Client CAPWAP AP Management Security QoS
	AP Join Profile Name t	id
Monitoring >	default-ap-profile of	Trust DSCP Upstream
Configuration	default-ap-profile-fabric	DSCP to UP Range
O Administration	I4 4 1 ► ► 10 v items per page	+ Add × Delete
C Licensing Troubleshooting		User         V         LOW er         V         Upper         ×           Priority         Upstream         Range         Range         Range
		DSCP to UP Exception
		+ Add X Delete
		DSCP v User Priority v
		Device

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.

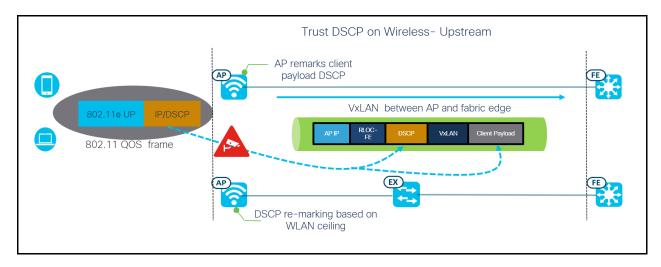
The WLAN ceiling still applies even when the trust DSCP upstream option is enabled on the WLC. For example, if the WLAN metal policy is mapped to Gold and the incoming 802.11 frame from a wireless client carries a DSCP of 46 (Expedited Forwarding). The access point would re-write the DSCP on the original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

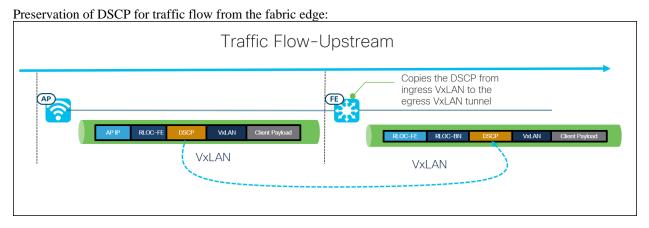
Mapping of 802.11e UP to DSCP UP-stream



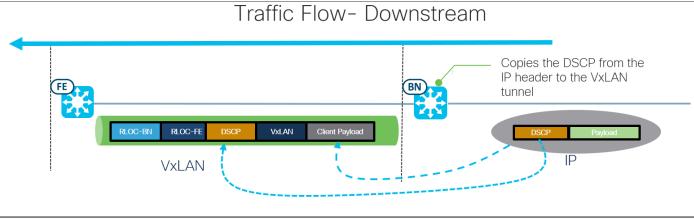
Derivation of DSCP when trust DSCP upstream in enabled on the Wireless LAN Controller:



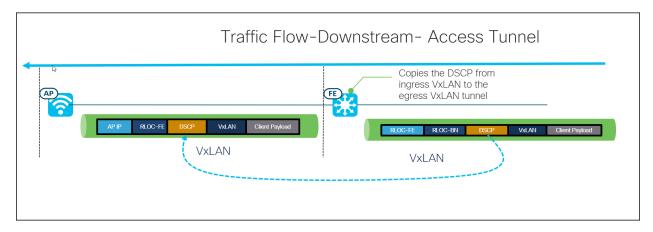
The fabric edge will terminate the VxLAN tunnel from the access point and will determine the destination where the data frame needs to be forwarded. Based on the destination the fabric edge will copy the DSCP from the incoming VxLAN to the egress VxLAN tunnel. Thus the priority is preserved as the data 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.



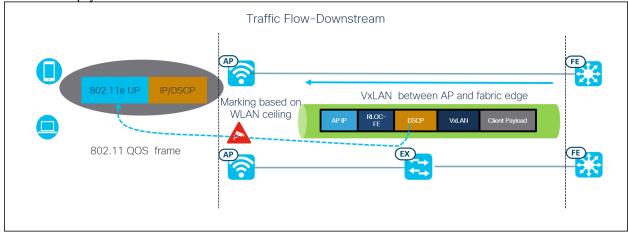
In the downstream direction for traffic originating from outside the fabric, the DSCP from the incoming IP packet is copied onto the VxLAN header at the border node.



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.



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.



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.

≡ Cisco DNA		Design · Network Settings	
Network Device IP A	ddress Pools SP Profiles Wireless Telemetry		
Q Find Hierarchy	Edit an Enterprise Wireless Network		
∨ & Global	Enterprise Wireless Network     (2)     Wireless Pr	rofiles	
> 🗞 US			
	Wireless Network Name(SSID) sand-mg-1x		Type Of Enterprise Network*
	sana-mg- ix		<ul> <li>Voice and Data</li> </ul>
		Configure the	O Data only
	Wireless Option	metal policies on	
	<ul> <li>Dual band operation (2.4GHz and 5GHz)</li> </ul>	the SSID	SSID STATE
	O Dual band operation with band select		Admin Status:
	⊖ 5GHz only		Broadcast \$\$ID:
	O 2.4GHz only		
<			Configure AAA
	Level Of Security *		🗌 Fast Lane
	● Enterprise	n	Mac Filtering
	WPA2 WPA3		
	Most secure		
	User Credentials are validated with 802.1x Radius server to authenticate o WPA3 feature is supported for Wireless Controller version 8.10 & above,		
$\checkmark$			

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

- ahaha -					Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONT	ROLLER W <u>I</u> RE	LESS <u>S</u> ECURITY	M <u>A</u> NAGEMENT	User:admin(ReadWrite) 🔒 Home
WLANs	WLANs > Edit 'sand-m	g-1x_Global_	F_af24c947'		< Back Apply
<ul> <li>WLANS WLANS</li> <li>Advanced</li> </ul>	General Security Quality of Service (QoS) Application Visibility AVC Profile Flex AVC Profile Netflow Monitor	QoS Policy Platinum (vo		anced	E
	Fastlane	Disable 👻	cts (kbps) <sup><u>16</u></sup>		
		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 Ban	dwidth Contra	cts (kbps) 🌆		
	4	DownStream	UpStream		
					, i i i i i i i i i i i i i i i i i i i

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

Cisco Catalys	st 9800-CL Wi	reless Controller		Welcome sand 🛛 🗌 🕯 🥓 🕩
Q Search Menu Items	Configuration • >	Tags & Profiles • > Policy		Edit Policy Profile
📷 Dashboard	+ Add X	General Access Policies QOS and AVC Mobility		
	Status v	Policy Profile Name	Description	Auto QoS None v
G Monitoring >		default-policy-profile	default policy	QoS SSID Policy
Configuration		test-ssid_Global_F_c1c339ec	test-ssid_Glo	Egress platinum 🗙 🔻
Administration	•	sand-mg-1x_Global_F_af24c947	sand-mg-1x	
(O) Administration		sand-mg-op_Global_F_1c12055f	sand-mg-op_	Ingress platinum-up 🗙 🔻
© Licensing	⊣	⊨ 10 🔻 items per page		QoS Client Policy
X Troubleshooting				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.

😑 Cisco DNA Ce		Policy - Application								
Application Policies s in	sand-fabric									
✓ Filter     Actions ∨ xd       Policy Name ∽       ● sand-fabric       ○ sand-non-fabric	2 Total devices	O Failed devices	2 Successful devices	O Aborted devices	O New devices					
	Filter Device Name Site	Status	Status Detalls	Device Ty	: zpe Network Role					
		/US/sanjose/B1 Success 《	Protocol/Application	on based policy is Cisco Ca	atalyst 9800-CL s Controller for 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: <u>https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b\_cg85/quality\_of\_service.html</u>

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.

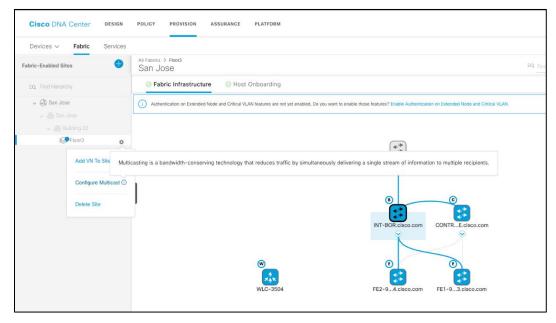


Note Multicast over wireless needs to be considered with some caution.

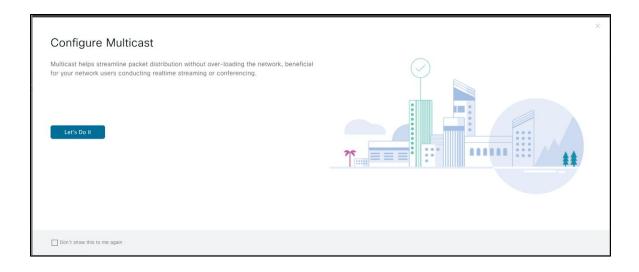
Once multicast IP traffic gets to the AP, these packets are transmitted over the air as broadcast Layer 2 frames; this basically means traffic gets transmitted at the highest mandatory data rate (to be able to reach all connected clients) and the transmission frames are not acknowledged, so a collision 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.



Step2 In the Enable Multicast workflow, click on "Let's do it" to Configure Multicast.



Step3 Select Native or Headend Multicast and click on Next.

Cisco DNA Center design policy provision assurance platform	۵	Q	 ٥	0	
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 multical in your network? O taxim multicast @ Index-end registration					
() Bait				Next	

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

Cisco DNA	Cent	OF DESIGN POLICY PROVISION ASSURANCE PLATFORM		20	Q	 ¢	0	
	Virtu	ual Networks						
	Select	your virtual networks to use in your multicast setup for Floor3						
		alacitad	EQ F	nd				
		Name x						
		Campus						
		DEFAULT_VN						
		Guest						
		ToT						
		Showing 4 of 4						
Exit		Re	view	E	Back	•	Next	

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.

Cisco DNA Center design policy provision assurance platform		٧	Q	 ¢	0	
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*						
≅Q.  Search Dropdown						
Campus-Multicast-SJC (1.1.1.0)						
Guest-Multicast-SJC (2.2.2.0)						
Exit All changes saved	Review	E	Back			

Step6 Select SSM or ASM

Cisco DNA	Center design policy provision assurance platform	٢	Q	 ¢	0	
S	Select SSM or ASM					
v	he Source Specific Multicast (SSM) feature is an extension of IP multicast where traffic is forwarded to receivers from only those multicast sources to hich the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are reated.					
	tulticast can be used to streamline packet distribution without over-loading the network with the same packets. It is especially beneficial if your network sers conduct realtime streaming or conferencing. Choose the method first.					
0	SSM					
(	Maa C					
Exit	Review		Back		Next	

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

<b>Cisco</b> DNA Center design pol	ICY PROVISION ASSURANCE PLATFOR	м	2	Q	 ¢	0	:
SSM	iding 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	+					
		1					
Exit All changes saved		R	eview	Back		Next	

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

Cisco DNA Center design policy provision assurance platform	<b>∠9</b> Q Ⅲ	¢ ⊙ ≡
Summary Review your multicast settings and make any changes. Delete Multicast Config		
<ul> <li>Enabling Multicast Edit</li> <li>Implementation Head-end replication</li> </ul>		
V Virtual Networks Edit Selected VNs Campus Guest		
<ul> <li>Multicast Pool mapping Edit</li> <li>Campus - Campus-Multicast-SJC (1.1.1.0)</li> <li>Guest Guest-Multicast-SJC (2.2.0)</li> </ul>		
<ul> <li>Select SSM or ASM Edit</li> <li>Multicast Type SSM</li> </ul>		
<ul> <li>✓ SSM Edit</li> <li>Cempus 232.0.0.0 0.255.255.255</li> <li>Gwest 232.0.0.0 0.255.255.255</li> </ul>		
Exit All changes saved		Finish

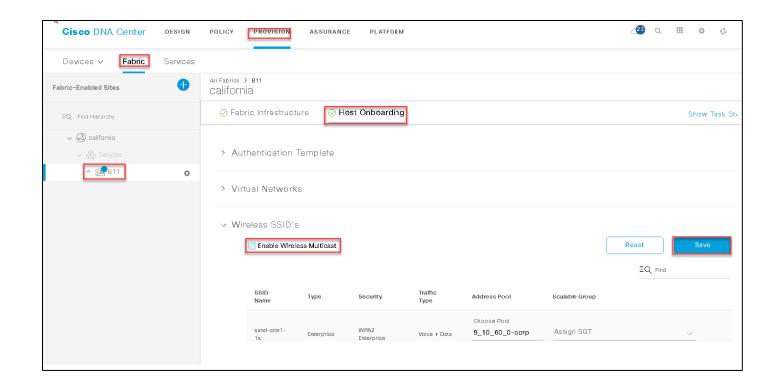
This will complete the Multicast Configuration workflow.

CISCO DNA Center design policy provision assurance platform	
Done! Multicast is initiated successfully!	
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



# **SD-Access Wireless – A Look Under the Hood**

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

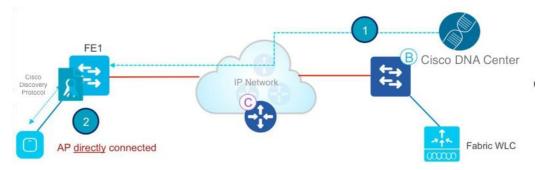


In Cisco DNA Center, first provision and then add the WLC to the fabric domain.

- 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			
Diegen	1>			
Select Devic	ces Host Or	boarding		
Select	t Authenticatio	on template		
O Close	d Authentication	O Easy Connect	<ol> <li>No Authentication</li> </ol>	O Open Authentication

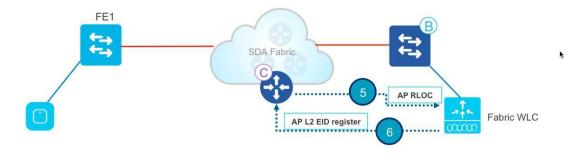
If any other authentication template is selected, the admin user will have to statically map the APs' switch ports to the right IP pool. The AP's are also supported on closed authentication port, the workflow and the steps are defined in the AP onboarding section.

#### 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.

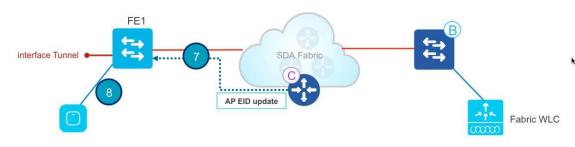


Figure 19. Creating a VXLAN tunnel for the AP

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).

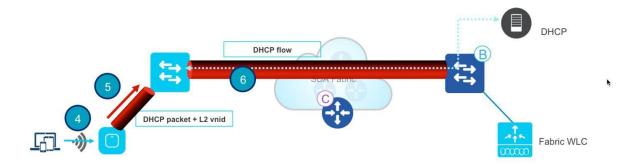
## **Client onboarding flow**

Figure 20. Authentication and policy retrieval



- 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.

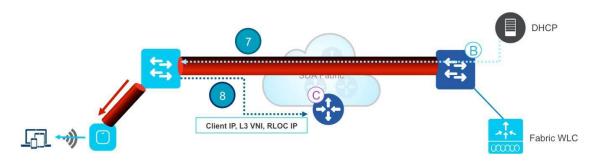
Figure 21. DHCP flow



- 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.

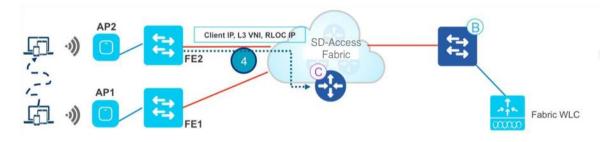
## **Client roaming flow**

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**

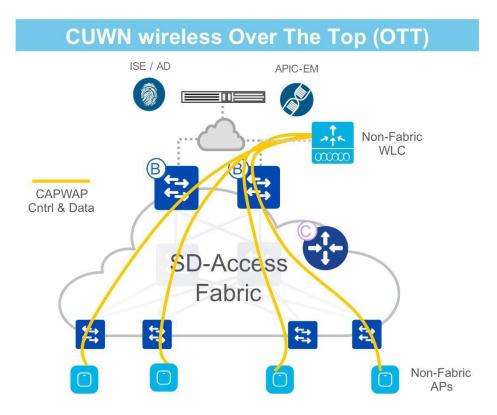
As mentioned earlier, there are two possible designs for deploying wireless with an SD-Access fabric:

- 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



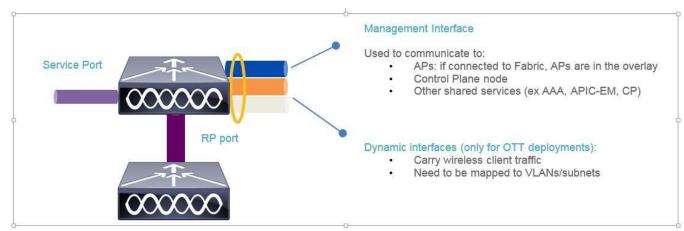
- A traditional Cisco Unified Wireless Network architecture with CAPWAP is used for the control plane and data plane, terminating at the WLC (for Centralized mode).
- The SD-Access fabric is just a transport in the wired infrastructure between the APs and the WLC.
- This is a possible migration step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



- 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:

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.

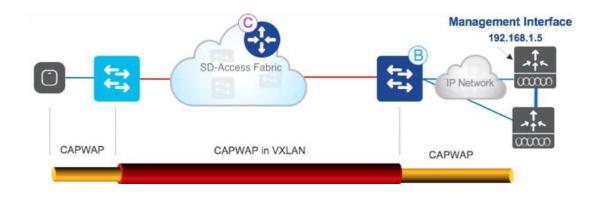
#### Access points

```
Figure 28. AP VLANs
```

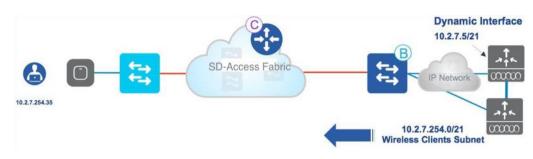


Access points are simply wired hosts to the fabric infrastructure, and hence are connected to the overlay space on fabric edge switches and assigned a specific pool in the EID space. One of the advantages of fabric is that all the APs can be assigned to one big subnet that is the same across the campus,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



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.

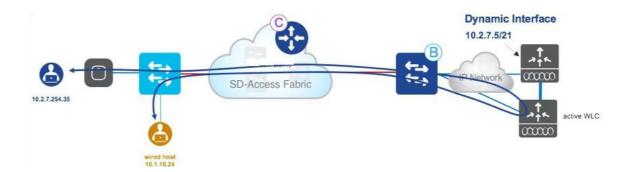
### **Client traffic flow**

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.



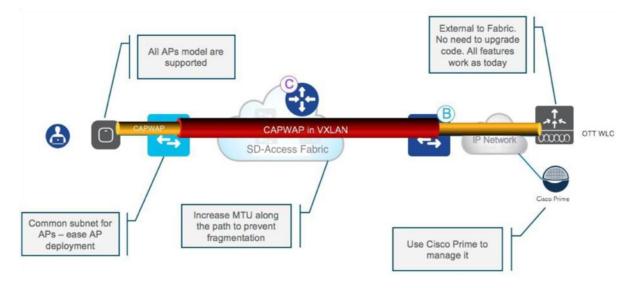
The wireless traffic will go all the way to the WLC, and will be bridged at the WLC dynamic interface VLAN and routed back to the fabric client through the border. For wireless, this is the same thing that happens today with a normal wired network; for the fabric, it is a fabric host communicating to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

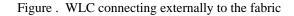


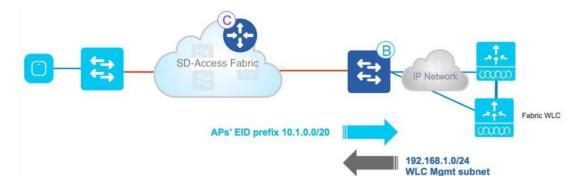
## **SD-Access Wireless network design**

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.





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

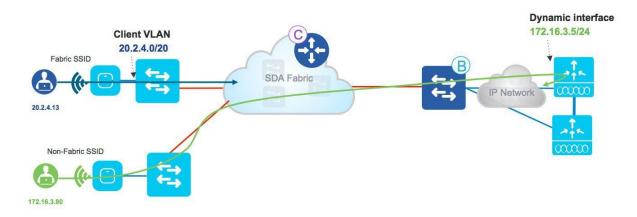


Figure 37. Wireless LAN in SD-Access Wireless

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.



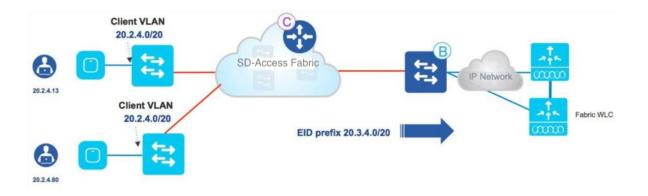
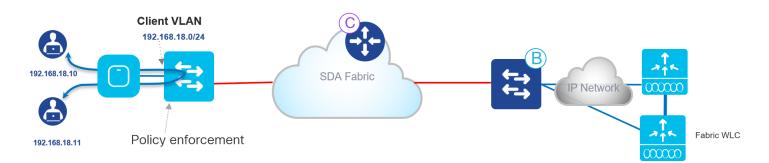


Figure 39. Client traffic flow in SD-Access Wireless on the same SSID/VLAN



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.

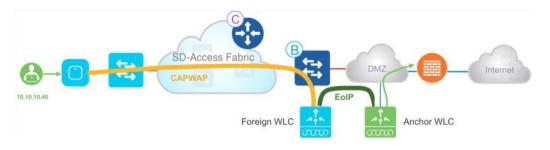
# **SD-Access Wireless guest access design**

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**

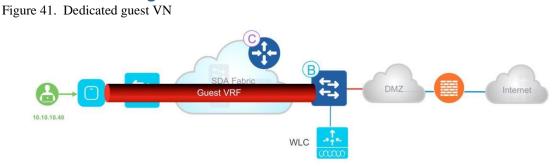
Figure 40. OTT solution using a guest anchor controller



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**



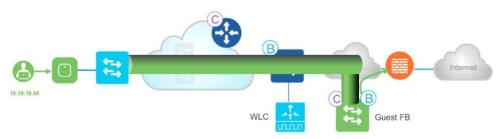
In this design, the guest network is just another VN in the SD-Access Fabric, so end-to-end fabric segmentation (using a VNI, and SGTs for different guest roles if needed) is used to separate the guest data plane from the other enterprise traffic. It's configured through Cisco DNA Center by creating 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**

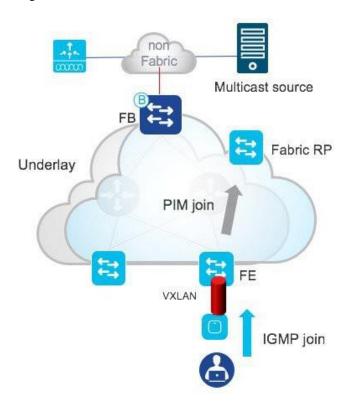
Here are some important things to know about multicast in SD-Access Wireless:

- 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:

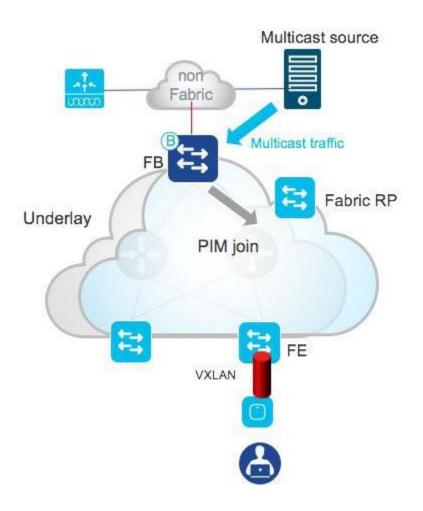
- The multicast client (receiver) is in the overlay. The multicast source can be outside the fabric or in the overlay as well (in Figure 43, the source is shown outside the fabric).
- PIM sparse mode (PIM-SM) or PIM source-specific multicast (PIM-SSM) needs to be running in the overlay (and so needs 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



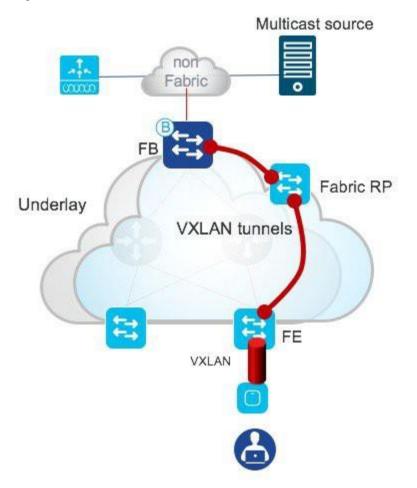
- Being outside of the fabric, in this example the multicast source will send the multicast traffic on the interfaces toward the fabric border which is the designated router for that segment.
- The FB receives the traffic and does a PIM join toward the RP (assuming PIM-SM is used).
- The RP now has the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

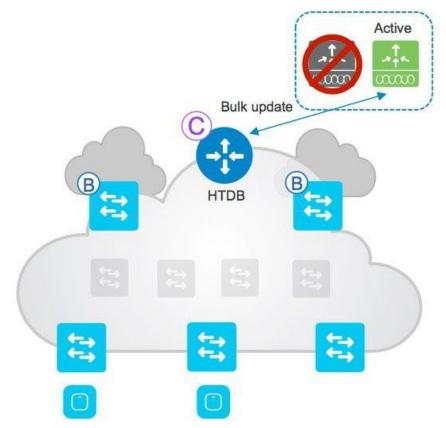
Both the WLC and the CP support high availability.

# **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

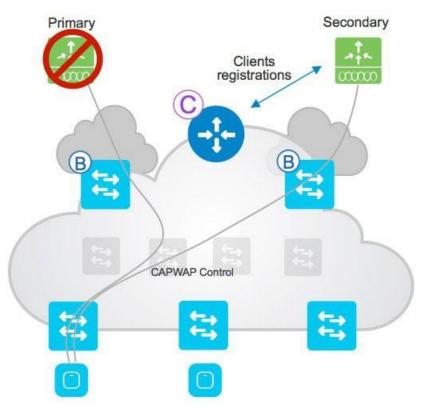


- The WLC SSO pair is seen as one node by the fabric.
- Only the active WLC interacts with the CP node.
- The fabric configuration and CP state are synced between the active and standby WLCs.
- Upon failure, a new active WLC will bulk update fabric clients to the Host Tracking database node (LISP refresh).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

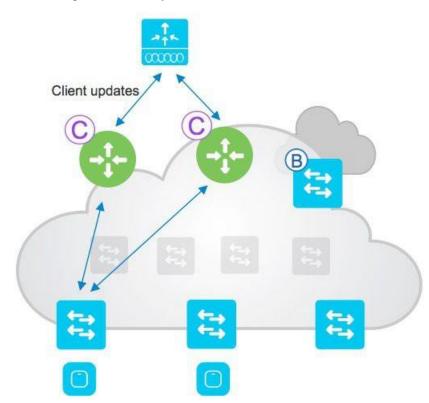
- The AP is configured with primary and secondary.
- The AP and associated clients register with the primary.
- Upon primary failure, the AP disconnects and joins the secondary.
- Clients are also disconnected and join the secondary.
- The secondary performs new client registration in the Host Tracking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

cisco	MONTTOR	<u>w</u> i ANa		WIRFIESS	grainny	MANAGEMENT
Controller	Fabric G	ontrol Pl	ane Configur	ation		
General Trons Inventory Interfaces	Fabric	Enable	a 🗨			
Interface Groups	Enterpris	se.				
Multicast Network Routes		ry IP Addre		16.252	- N	16
<ul> <li>Fabric Configuration</li> <li>Control Plane</li> <li>Interface</li> </ul>	Conne	ection 31211	s			G
i emplates	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	dary 19 Ad		10.252	R	
Redundancy	Prc S	hared Key				
Mobility Management	\$30 m	etteri Stana	•			

reference screenshot from Catalyst 9800 WLC:

Cisco Cisco	Cata	lyst 9800-CL Wireless Controller		Welcome sand
Q Search Menu Items	1	Configuration > Wireless > Fabric		Edit Control Plane
				Control Plane Name* default-control-plan
📰 Dashboard		General Control Plane Profiles		Control Plane Description
Monitoring	>			+ Add X Delete
🔧 Configuration	>	Control Plane Name	Control I	
(0) Administration	>	default-control-plane	<	9.254.254.65
∽ Troubleshooting		I4 ◀ 1 ► ► 10 v items per page		9.254.254.69 H

# **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.

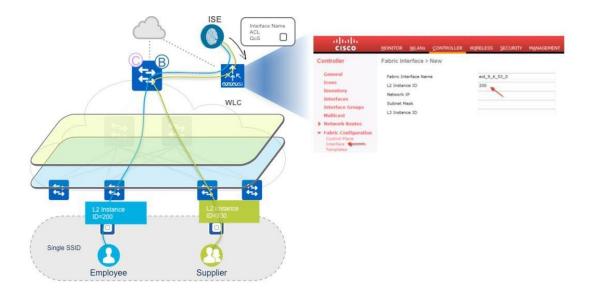
#### Fabric Interface Name override

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



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.

<ul> <li>Advanced Attributes Setting</li> </ul>	S	
Airespace:Airespace-Interface-Nai	· ◯ = 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.



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

cisco	MONITOR M	LANS		WIRELESS	SECURITY	MANAGEMENT
Controller	Fabric ACL	Temp	ate > Edit			
General	Fabric ACL Te Name	emplate	ACL Template			
Inventory	Status		Modified			
Interfaces Interface Groups Multicast	ACL		•]	Add		
Network Routes						
Fabric Configuration     Control Plane     Interface     Templates	Fabric ACL					
	ca-redirect-ac					
	cwa-redirect-a	icl				
Redundancy	test					
Mobility Management Ports						

WLANS WLANS	General	VLANS	AP5	802.11u	Location	Ports/Module	
Advanced AP Groups							Appl
	AP Group Nar	ne	de	fault-group			
	AP Group Des	scription					
	NAS-ID	NAS-ID Enable Client Traffic QinQ					
	Enable Client						
	Enable DHCP	v4 QinQ 🖁					
	QinQ Service	Vlan Id 10	0				

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

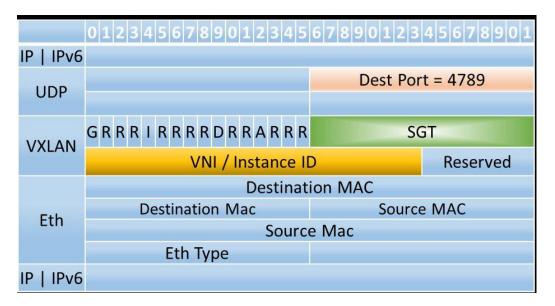
For QoS profile name override:

- 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.

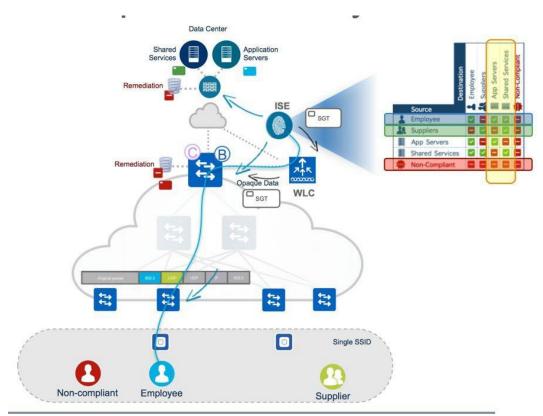
For applying the SGACL on the access switch for wireless clients (enforcement for the traffic destined to a wireless client on the

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.

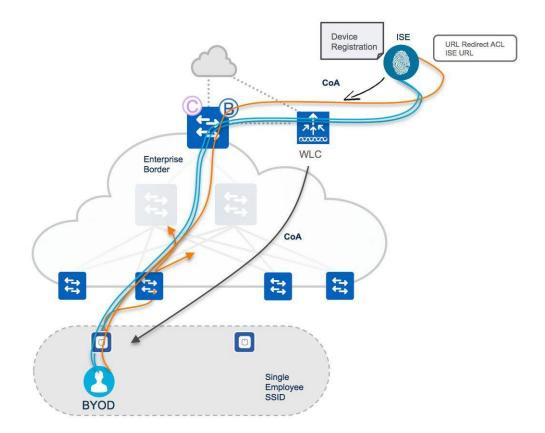
#### Figure 51. SGT for group-based policy



# **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.

# uļuļu cisco.

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.