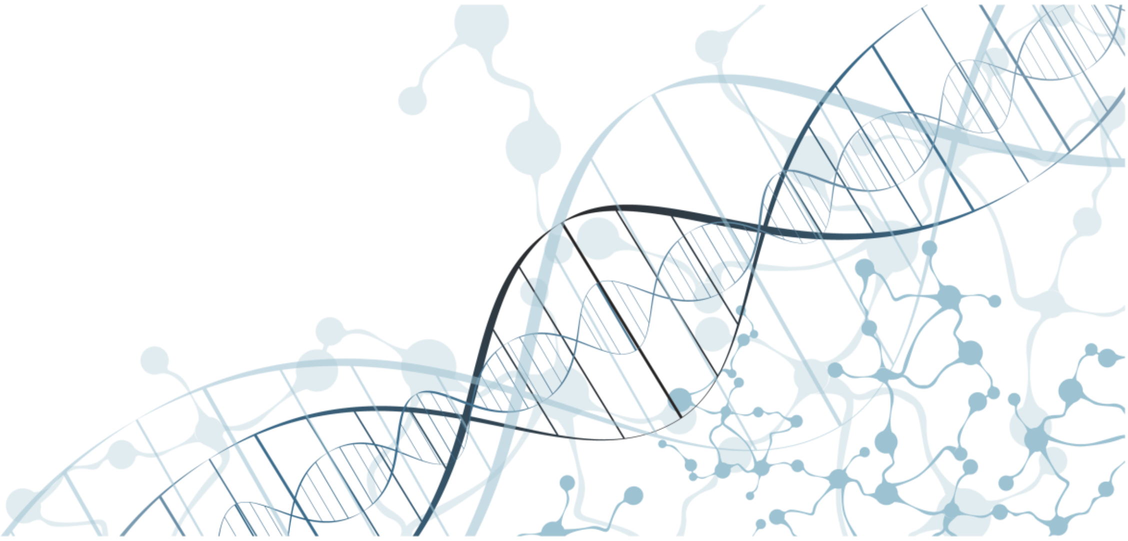


Cisco Catalyst 9800 Wireless on Catalyst 9k switch for SD-Access

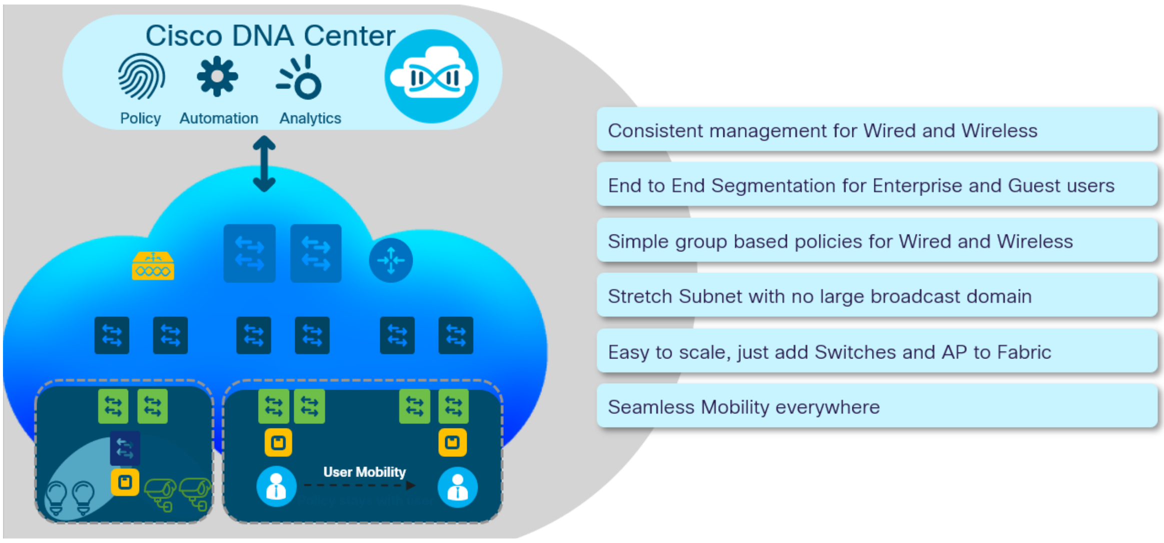
May 2019

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Table of Contents

Cisco SD Access

Cisco Software Defined Access (SD-Access) is the next generation Enterprise Networking access solution, designed to offer integrated security, segmentation, and elastic service roll-outs via a Fabric based infrastructure and an outstanding GUI experience for automated network provisioning via the new 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 resolutions and reduces security breach impacts. This results in a significant CapEx and OpEx savings for the business. The benefits of SDA are summarized in the picture below:


Cisco DNA Center
Policy
Automation
Analytics
User Mobility
Consistent management for Wired and Wireless
End to End Segmentation for Enterprise and Guest users
Simple group based policies for Wired and Wireless
Stretch Subnet with no large broadcast domain
Easy to scale, just add Switches and AP to Fabric
Seamless Mobility everywhere

Note: In this document the focus is on the wireless integration in SD-Access; 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 https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html and SD-Access Design Guide (CVD) https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Sol1dot2-2018DEC.pdf.

Cisco SD-Access Wireless

Cisco SD-Access Wireless is defined as the integration of wireless access in the SD-Access fabric in order to gain all the advantages of Fabric and Cisco DNA-Center automation.

Note: For detailed information on available wireless integration with SD-Access, please refer SD-Access Design and Deployment Guide:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_SD_Access_Wireless_Deployment_Guide.html#concept_7677C58D9651467BA3A12C5CF3E03CCB

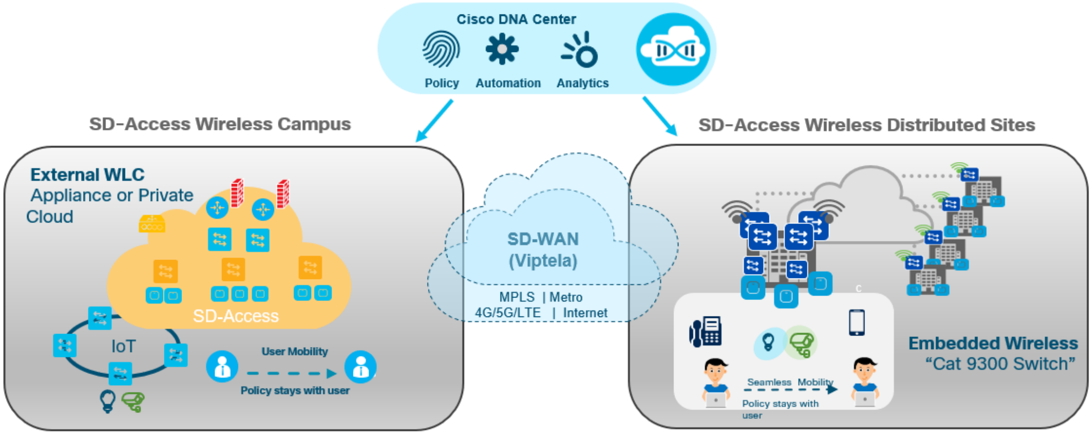
Introducing Cisco SD-Access on Cisco Catalyst 9800

Built from the ground-up for the Intent-based networking and Cisco DNA, Cisco Catalyst 9800 Series Wireless Controllers bring together the magic of Cisco IOS XE and Cisco RF excellence, to create the best-in-class wireless experience for your evolving and growing organization. The Cisco Catalyst 9800 Series Wireless Controllers are built on an open programmable architecture with built-in security, streaming telemetry and rich analytics.

SD-Access Multi-Site Wireless Solution with Catalyst 9800 Series Wireless Controllers

Catalyst 9800 for SD-Access is supported with existing 802.11ac wave 1 APs (1700,2700,3700), 802.11ac wave 2 APs (1800,2800,3800,4800) along with outdoor wave 2 APs (1540,1560). The controller is available in multiple form factors suited for diverse network needs.

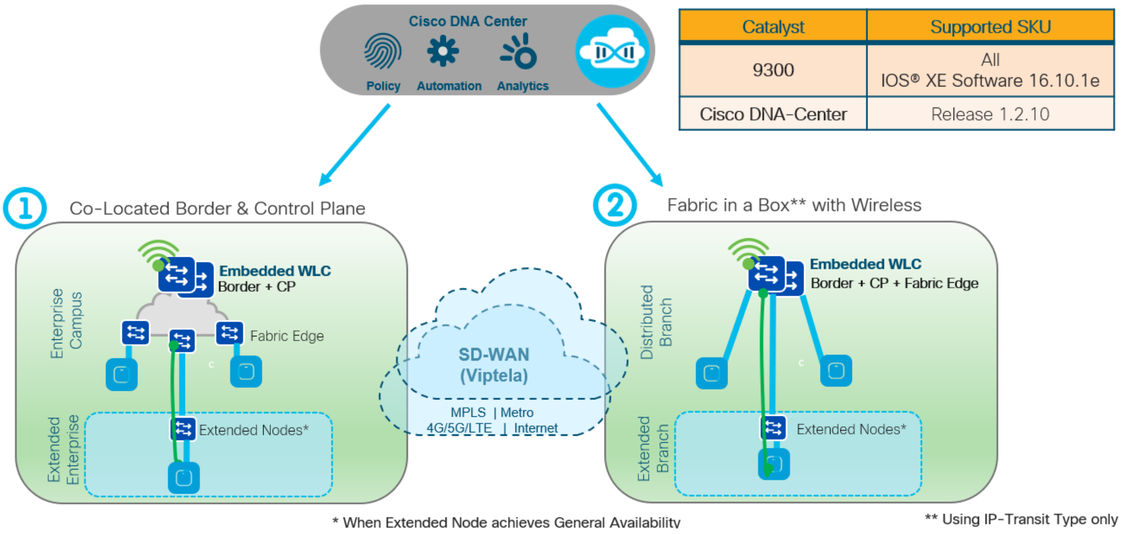
- Cisco Catalyst 9800-80 is our leading modular wireless controller, which supports up to 6000 access points and 64,000 clients.
- Cisco Catalyst 9800-40 is ideal for mid-sized organizations and campus deployments as it supports up to 2000 access points and 32,000 clients.
- Cisco® Catalyst® 9800-CL is the next generation of enterprise class virtual wireless controller built for high availability and security. It comes with multiple scale options to meet the needs of branch and campus network deployments.
- Cisco Catalyst 9800 embedded wireless is a software package that enables wireless on the Catalyst 9000 switching platforms. Supported on Catalyst 9300 switches (in Cisco DNA-Center 1.2.10) offers support of up to 200 Access Points and 4000 wireless clients.



Embedded Wireless (Catalyst 9800) on Catalyst 9k Platform

The Cisco Catalyst 9800 Wireless Controller Software package can be installed on Cisco Catalyst 9300 series switches to enable wireless controller functionality for distributed branches and small campuses. C9800 Wireless Controller Software Package will enable Wireless Functionality only for SD-Access deployments with two supported topologies:

- C9800 Wireless Software Package can be enabled on C9300 series switches functioning as Co-Located Border and Control Plane. Once installed Wireless Controller running on Catalyst 9300 can support up-to 200 APs and 4000 Clients.
- C9800 Wireless Software Package can be enabled on C9300 series switches functioning as Fabric in a Box (Control Plane, Border and Fabric Edge on a single node). This model offers support for 100 APs with 2000 clients.



Catalyst	Supported SKU
9300	All IOS® XE Software 16.10.1e
Cisco DNA-Center	Release 1.2.10

* When Extended Node achieves General Availability

** Using IP-Transit Type only

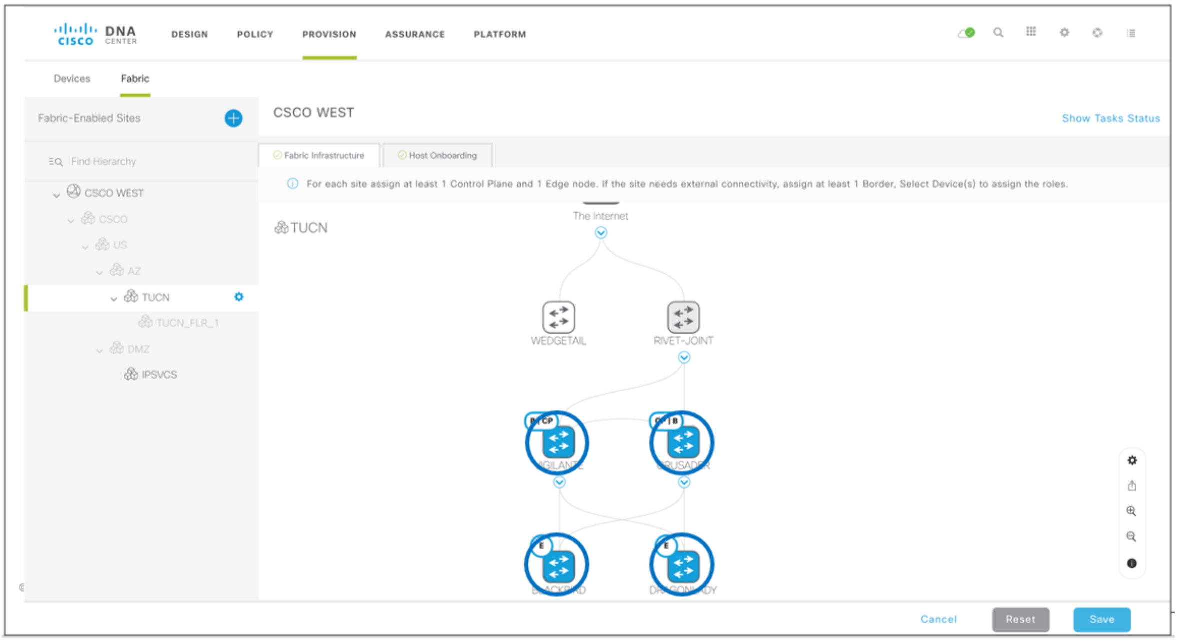
Key items to consider:

- Embedded 9800 runs only over a SD-Access infrastructure
- Orchestration of Embedded Wireless Controller functionality is supported only via Cisco DNA Center
- Guest Access is only supported via
  a. Separate Guest Border/CP
  b. Guest as a VRF on Enterprise Border/CP
- Check the latest Cisco SD-Access compatibility matrix for various solution components https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html

Workflows for Embedded Cisco Catalyst 9800 on Cisco Catalyst 9300 Switches

<u>It is assumed that SD-Access wired infrastructure is configured and operational at this point.</u>

The following section will walk you through introducing and integrating embedded wireless functionality on a Catalyst 9300 switch in fabric.



For each site assign at least 1 Control Plane and 1 Edge node. If the site needs external connectivity, assign at least 1 Border, Select Device(s) to assign the roles.

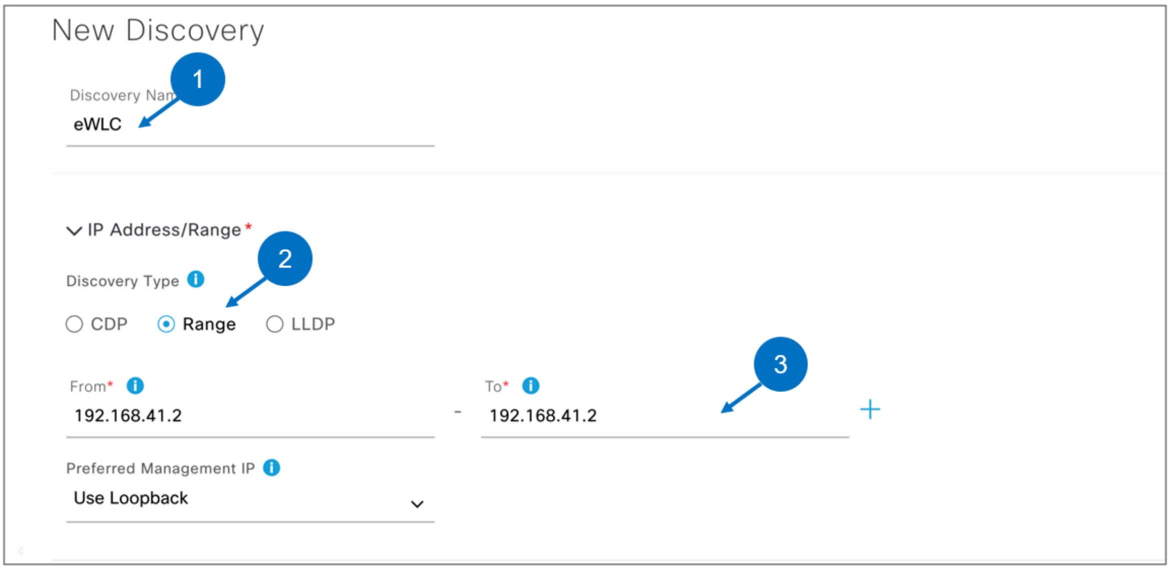
Prerequisites

Make sure that you meet these requirements before you attempt this configuration:

- Cisco Catalyst 9300 boots in "INSTALL" mode by default, from factory. The boot-up mode on the Cisco Catalyst 9300 switch should be "INSTALL" mode, and not BUNDLE mode.
- SSH should be enabled on the Catalyst 9300 switch.
- NETCONF should be enabled in the discovery via Cisco DNA Center.
- NETCONF is used to deploy the Wireless configurations.

Cisco DNA Center Discovery Settings

1. Discover Cat9300 switch:



New Discovery

Discovery Name: eWLC

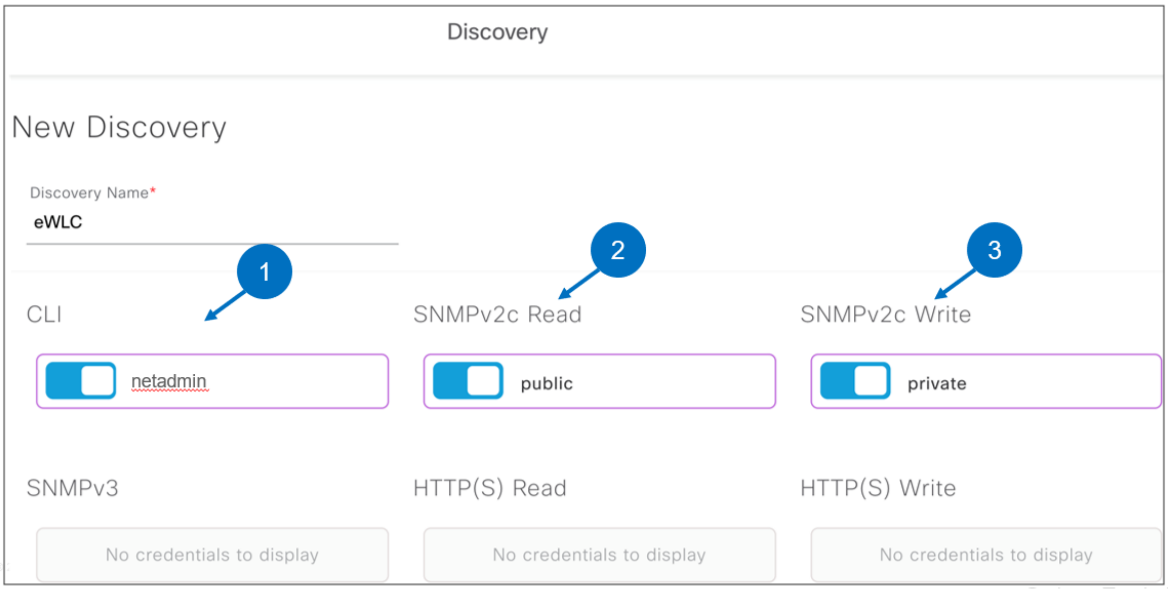
IP Address/Range*

Discovery Type: ○ CDP ● Range ○ LLDP

From*: 192.168.41.2 - To*: 192.168.41.2

Preferred Management IP: Use Loopback

2. Configure device credentials:



Discovery

New Discovery

Discovery Name*: eWLC

CLI: netadmin

SNMPv2c Read: public

SNMPv2c Write: private

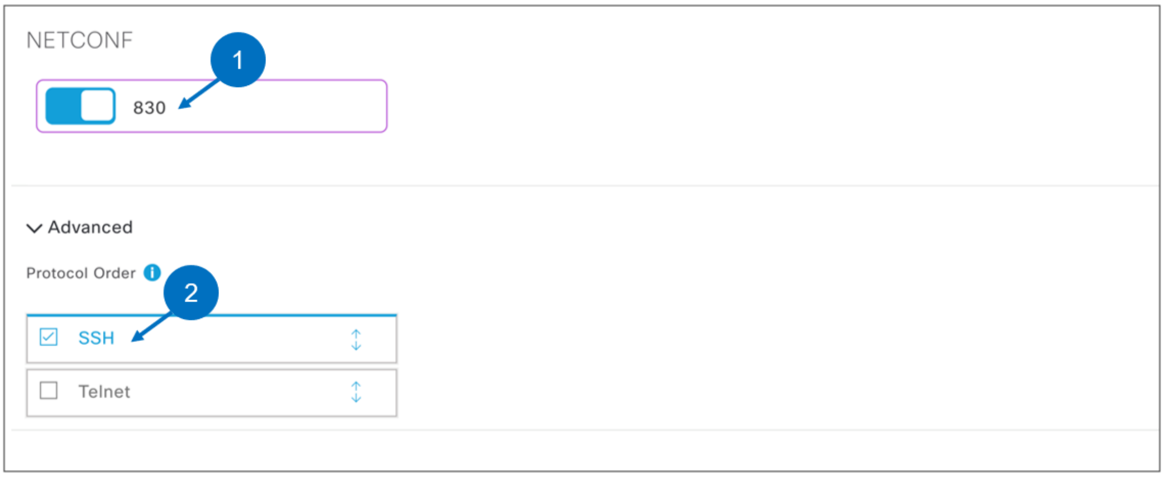
SNMPv3: No credentials to display

HTTP(S) Read: No credentials to display

HTTP(S) Write: No credentials to display

3. Enable NETCONF and SSH for the device discovery: You do not need to enable NETCONF on the target switches to be discovered, Cisco DNA Center will automatically

enable that during discovery.



NETCONF

830

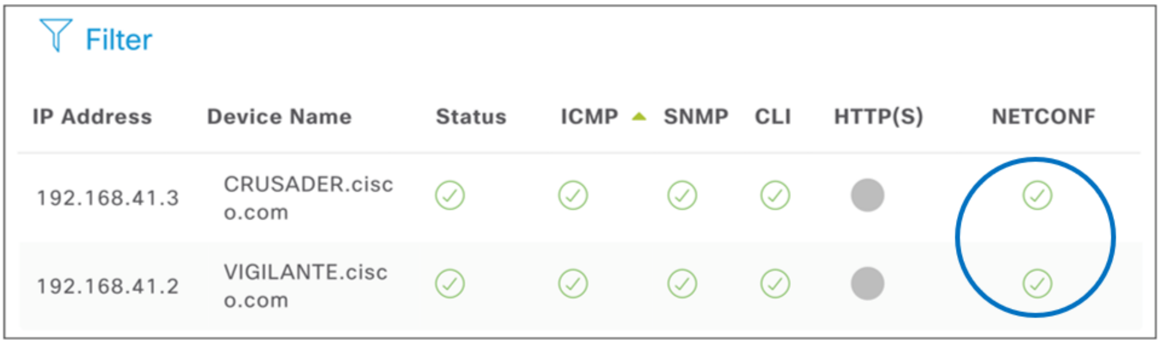
Advanced

Protocol Order

☑ SSH

□ Telnet

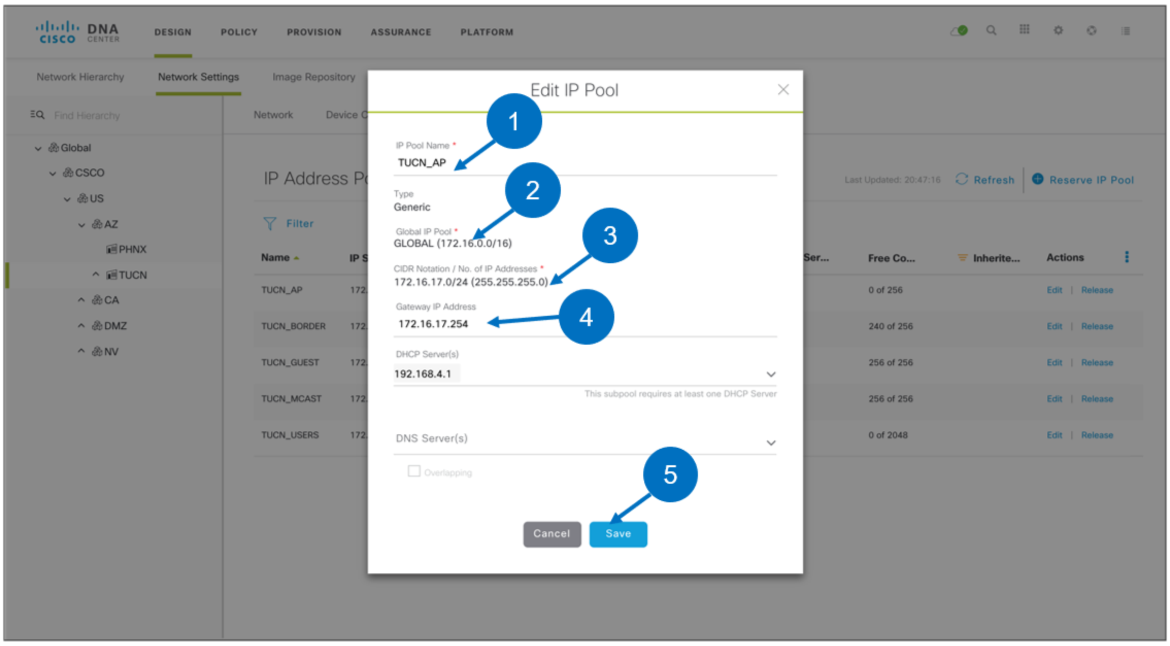
4. Check Cisco DNA Center discovery result to see Cat9300 discovered: The “NETCONF” discovery is essential to be successful for enabling embedded 9800 on the Catalyst 9300 switch.



IP Address	Device Name	Status	ICMP	SNMP	CLI	HTTP(S)	NETCONF
192.168.41.3	CRUSADER.cisco.com	✓	✓	✓	✓	●	✓
192.168.41.2	VIGILANTE.cisco.com	✓	✓	✓	✓	●	✓

Cisco DNA-Center**Design**

1. Click on *Design* tab. Go to *Network Settings* and click on *IP Address Pools.* Create an IP Pool for access points in the network as shown below.



Name	IP S	Ser...	Free Co...	Inherite...	Actions
TUCN_AP	172.		0 of 256		Edit | Release
TUCN_BORDER	172.		240 of 256		Edit | Release
TUCN_GUEST	172.		256 of 256		Edit | Release
TUCN_MCAST	172.		256 of 256		Edit | Release
TUCN_USERS	172.		0 of 2048		Edit | Release

Edit IP Pool

IP Pool Name *
TUCN_AP

Type
Generic

Global IP Pool *
GLOBAL (172.16.0.0/16)

CIDR Notation / No. of IP Addresses *
172.16.17.0/24 (255.255.255.0)

Gateway IP Address
172.16.17.254

DHCP Server(s)
192.168.4.1

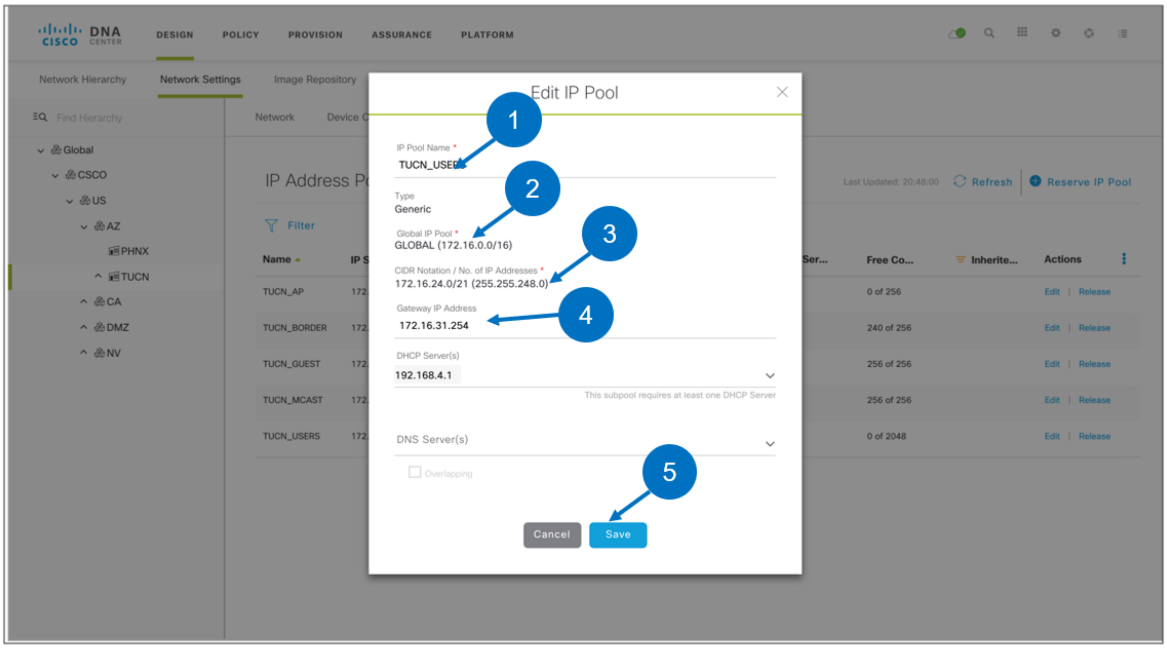
This subpool requires at least one DHCP Server

DNS Server(s)

□ Overlapping

Cancel Save

Similarly, create another IP Pool for wireless users as shown below



Name	IP S	Ser...	Free Co...	Inherite...	Actions
TUCN_AP	172.		0 of 256		Edit | Release
TUCN_BORDER	172.		240 of 256		Edit | Release
TUCN_GUEST	172.		256 of 256		Edit | Release
TUCN_MCAST	172.		256 of 256		Edit | Release
TUCN_USERS	172.		0 of 2048		Edit | Release

Edit IP Pool

IP Pool Name *
TUCN_USERS

Type
Generic

Global IP Pool *
GLOBAL (172.16.0.0/16)

CIDR Notation / No. of IP Addresses *
172.16.24.0/21 (255.255.248.0)

Gateway IP Address
172.16.31.254

DHCP Server(s)
192.168.4.1
This subpool requires at least one DHCP Server

DNS Server(s)

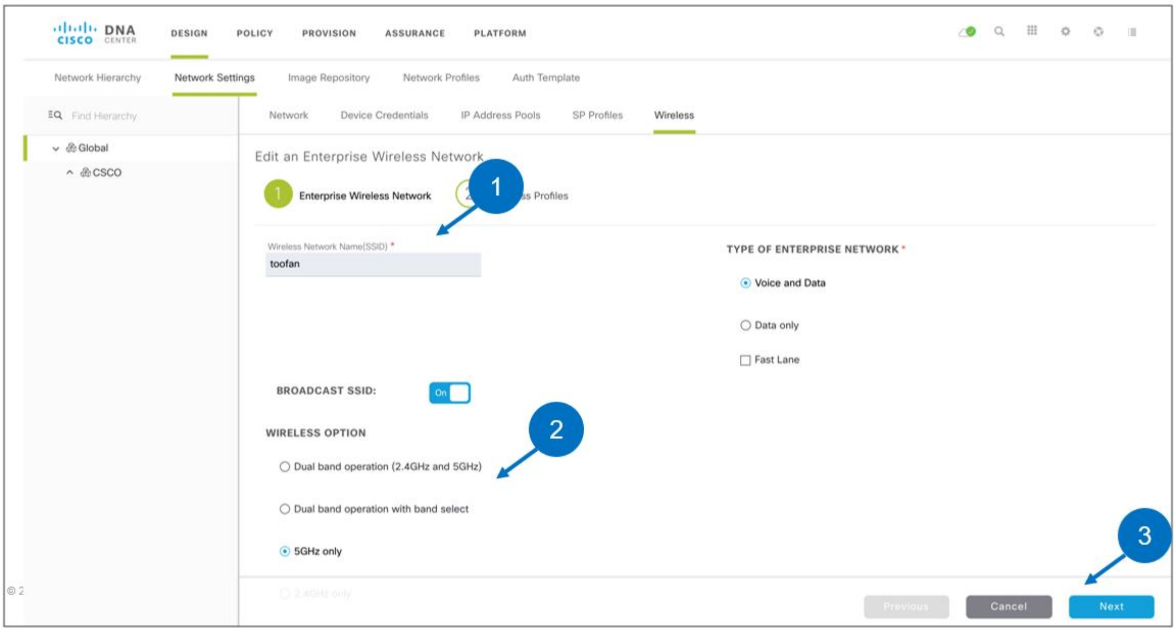
□ Overlapping

Cancel Save

2. Click on *Wireless* tab to create a Wireless Guest SSID.

Under Enterprise Wireless click on the ADD icon. Creation of a SSID is a two-step process. Under Wireless click on the ADD icon.

Create a SSID, configure it for a security and select an authentication server as shown below.



Edit an Enterprise Wireless Network

1 Enterprise Wireless Network 2 ...ss Profiles

Wireless Network Name(SSID) *
toofan

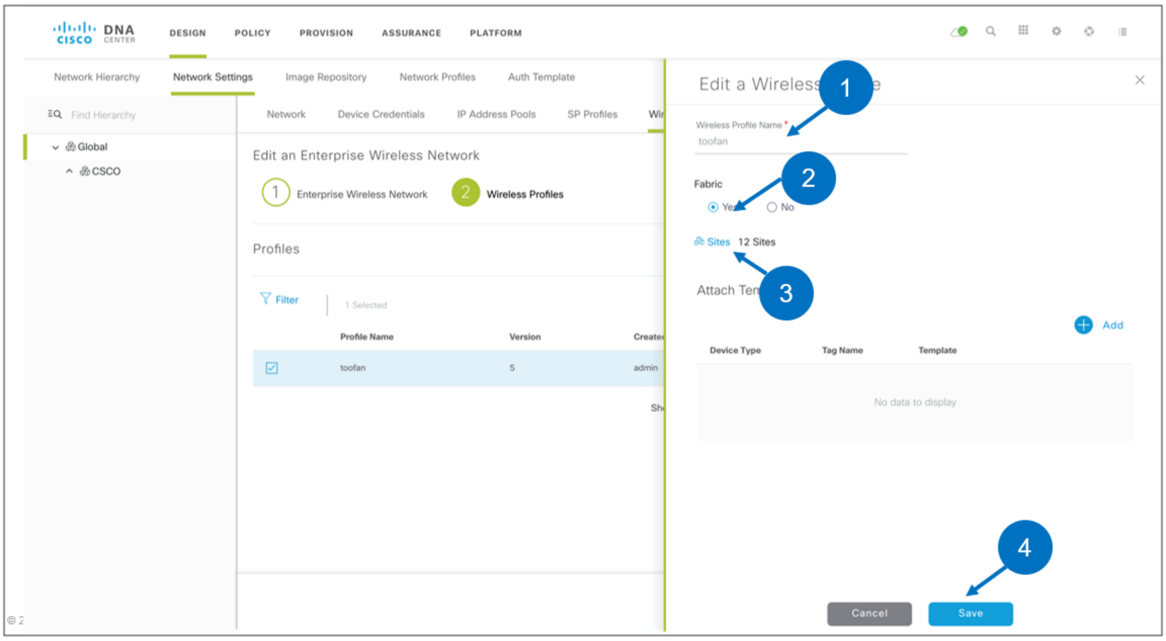
TYPE OF ENTERPRISE NETWORK *
● Voice and Data
○ Data only
□ Fast Lane

BROADCAST SSID: On

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

Previous Cancel Next

c. Click on *Next* and associate the SSID to a site/sites where it is to available.



Profile Name	Version	Created
toofan	5	admin

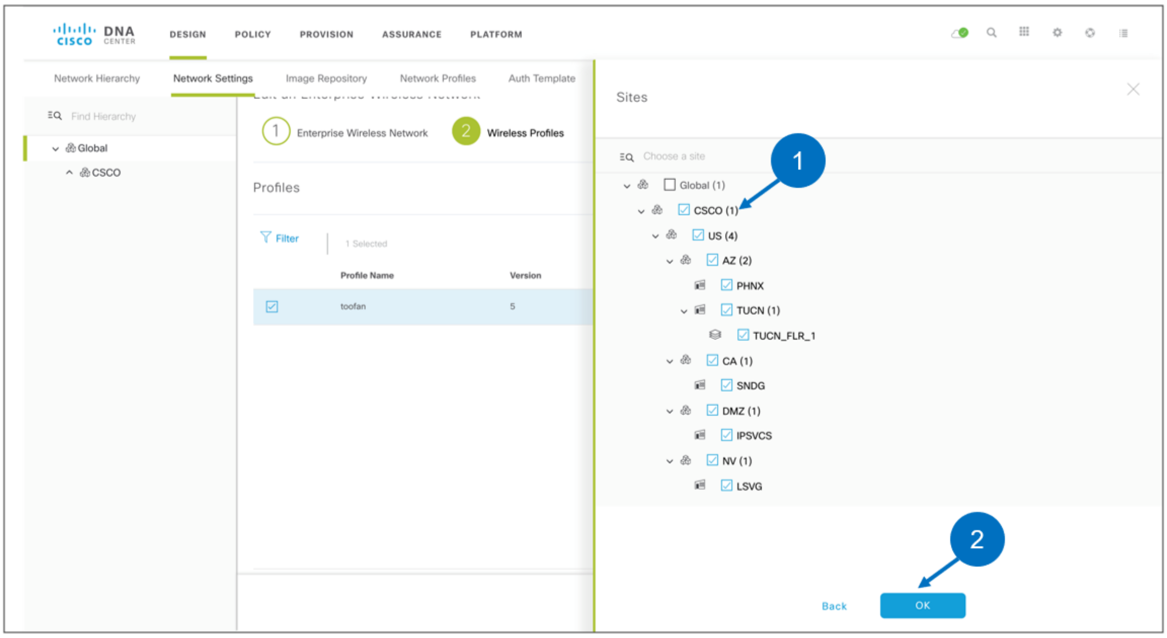
Wireless Profile Name* toofan

Fabric ● Yes ○ No

Sites 12 Sites

Attach Template

We have the option to add multiple sites here.



- □ Global (1)
  - ☑ CSCO (1)
    - ☑ US (4)
      - ☑ AZ (2)
        - ☑ PHNX
        - ☑ TUCN (1)
          - ☑ TUCN_FLR_1
      - ☑ CA (1)
        - ☑ SNDG
      - ☑ DMZ (1)
        - ☑ IPSVCS
      - ☑ NV (1)
        - ☑ LSVG

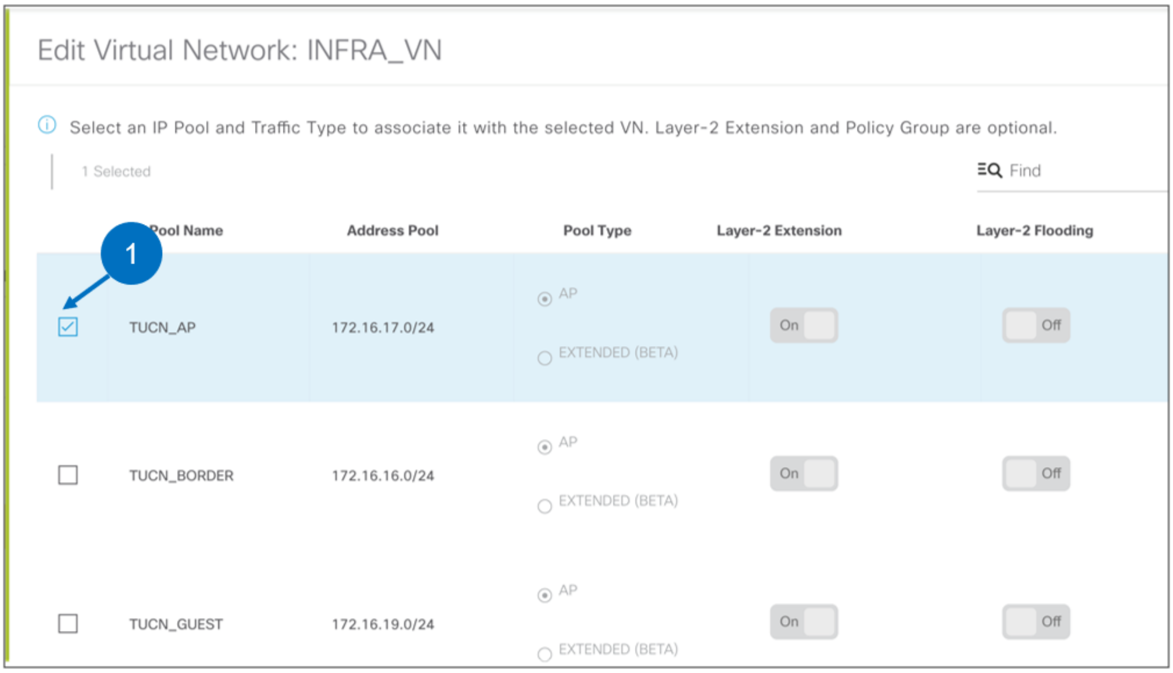
Cisco DNA-Center POLICY

Policy constructs should already been defined as part of creating a wired fabric infrastructure.

Cisco DNA-Center PROVISION

Under Provision, click on *Fabric*. Select your Fabric Domain. Click on the Fabric Domain and go to your Fabric Enabled Site. Click on the tab Host *Onboarding*.

1. Associate AP Pool to INFRA_VN



Edit Virtual Network: INFRA_VN

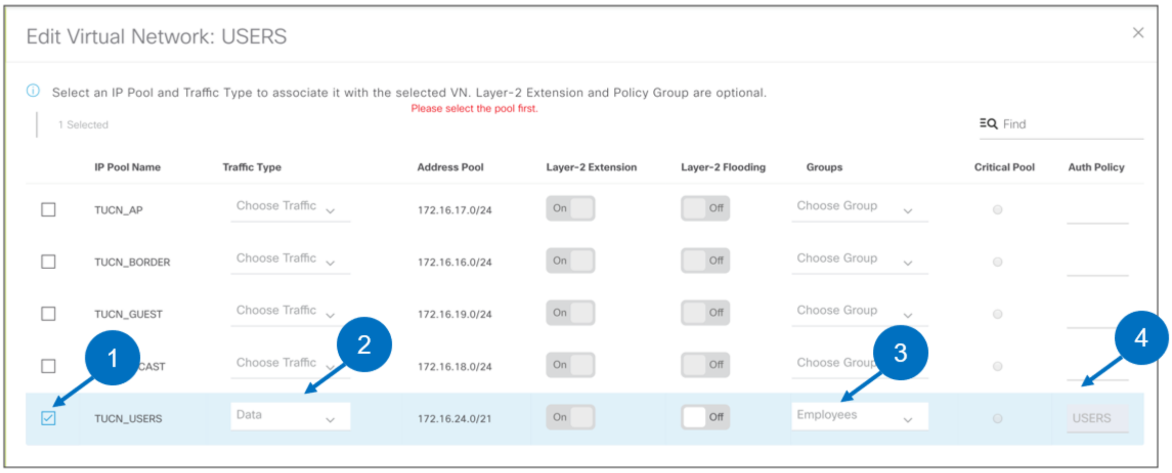
Select an IP Pool and Traffic Type to associate it with the selected VN. Layer-2 Extension and Policy Group are optional.

1 Selected

Find

	Pool Name	Address Pool	Pool Type	Layer-2 Extension	Layer-2 Flooding
☑	TUCN_AP	172.16.17.0/24	● AP ○ EXTENDED (BETA)	On	Off
□	TUCN_BORDER	172.16.16.0/24	● AP ○ EXTENDED (BETA)	On	Off
□	TUCN_GUEST	172.16.19.0/24	● AP ○ EXTENDED (BETA)	On	Off

2. Associate USER Pool to USERS_VN



Edit Virtual Network: USERS

Select an IP Pool and Traffic Type to associate it with the selected VN. Layer-2 Extension and Policy Group are optional.

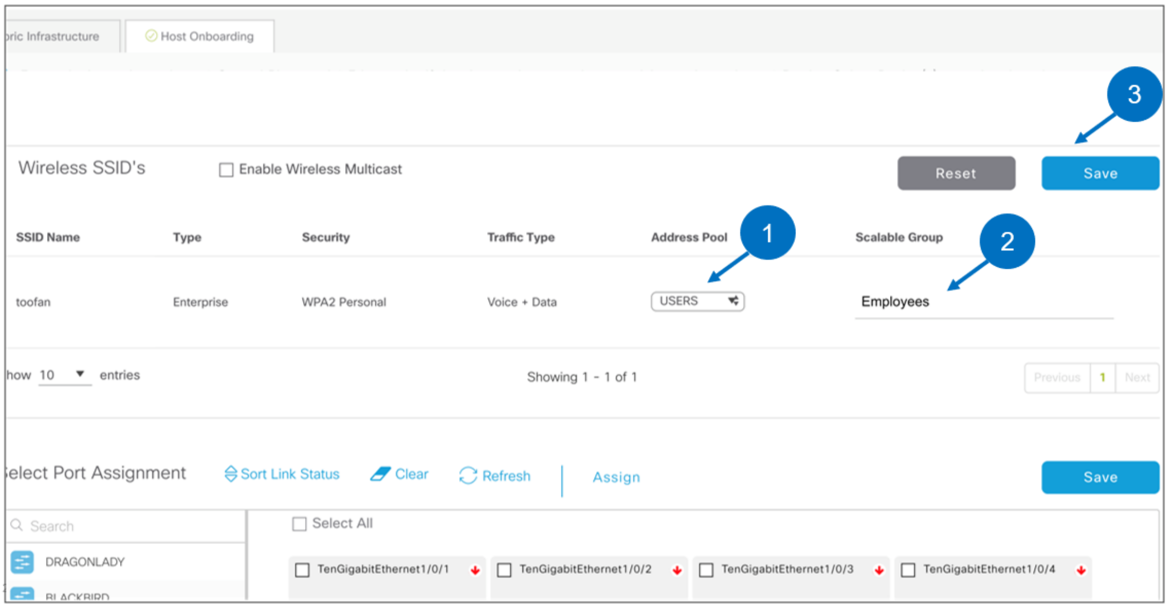
Please select the pool first.

1 Selected

Find

	IP Pool Name	Traffic Type	Address Pool	Layer-2 Extension	Layer-2 Flooding	Groups	Critical Pool	Auth Policy
□	TUCN_AP	Choose Traffic	172.16.17.0/24	On	Off	Choose Group	○	
□	TUCN_BORDER	Choose Traffic	172.16.16.0/24	On	Off	Choose Group	○	
□	TUCN_GUEST	Choose Traffic	172.16.19.0/24	On	Off	Choose Group	○	
□	CAST	Choose Traffic	172.16.18.0/24	On	Off	Choose Group	○	
☑	TUCN_USERS	Data	172.16.24.0/21	On	Off	Employees	○	USERS

3. Associate IP Pool/SGT to Wireless SSID



SSID Name	Type	Security	Traffic Type	Address Pool	Scalable Group
toofan	Enterprise	WPA2 Personal	Voice + Data	USERS	Employees

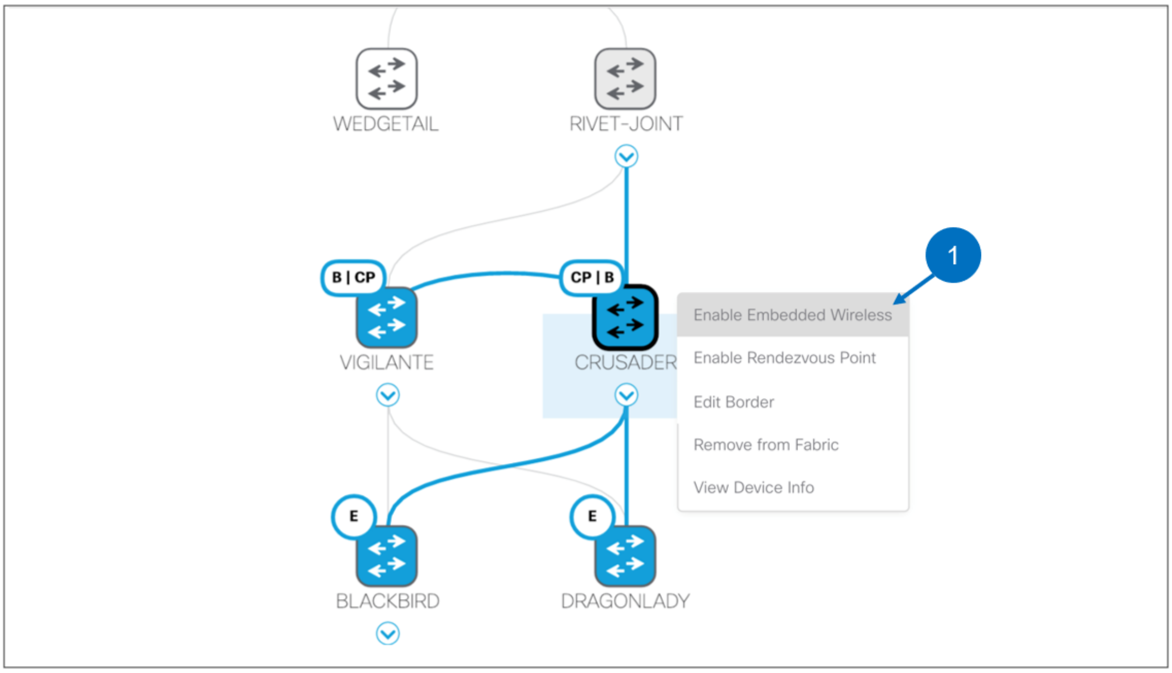
Show 10 entries — Showing 1 - 1 of 1 — Previous 1 Next

Provisioning Catalyst 9800 embedded Wireless LAN Controller

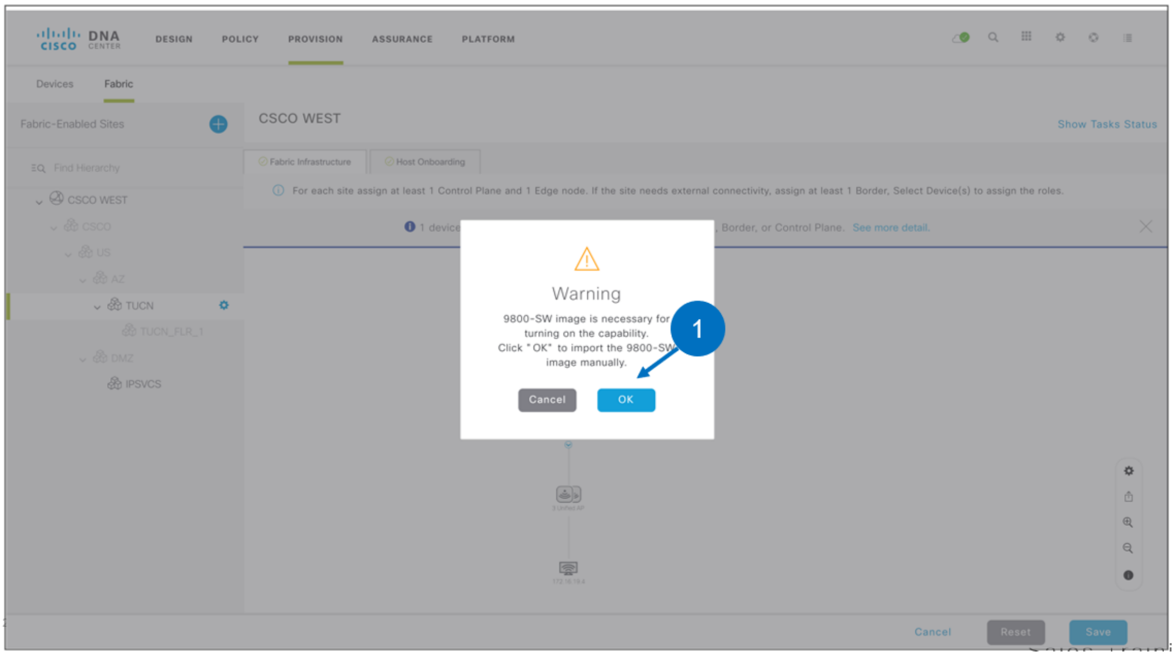
4. Still under the fabric site click on *Fabric Infrastructure*.

a. Click on the Catalyst 9k switch and select *Enable Embedded Wireless*

Note: At this point Fabric is configured across the network devices at a site. Wireless Lan Controller is added to Fabric and the icon shows up in blue as shown below.



b. The user will automatically be prompted to load a wireless bundle on the Catalyst 9k switch.



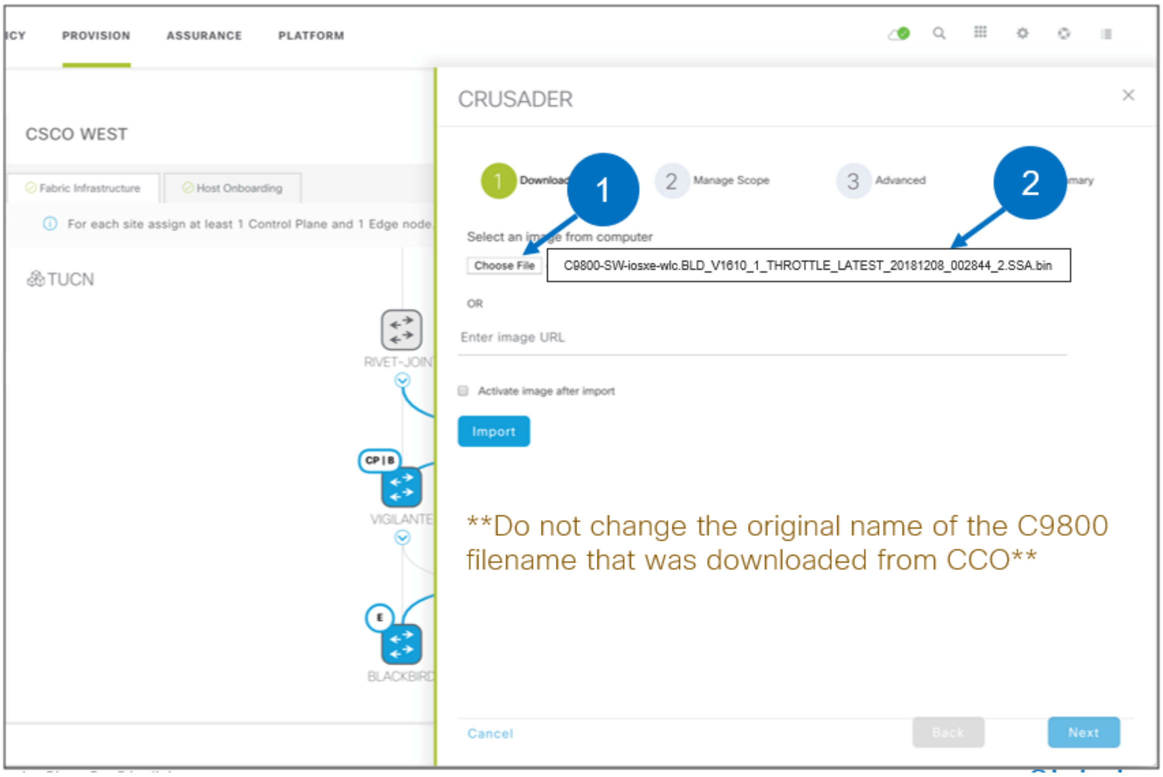
For each site assign at least 1 Control Plane and 1 Edge node. If the site needs external connectivity, assign at least 1 Border, Select Device(s) to assign the roles.

1 device ... Border, or Control Plane. See more detail.

Warning

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

c. Download the Catalyst 9800 wireless image for Catalyst 9k switch from cisco.com and upload it as shown below.



For each site assign at least 1 Control Plane and 1 Edge node.

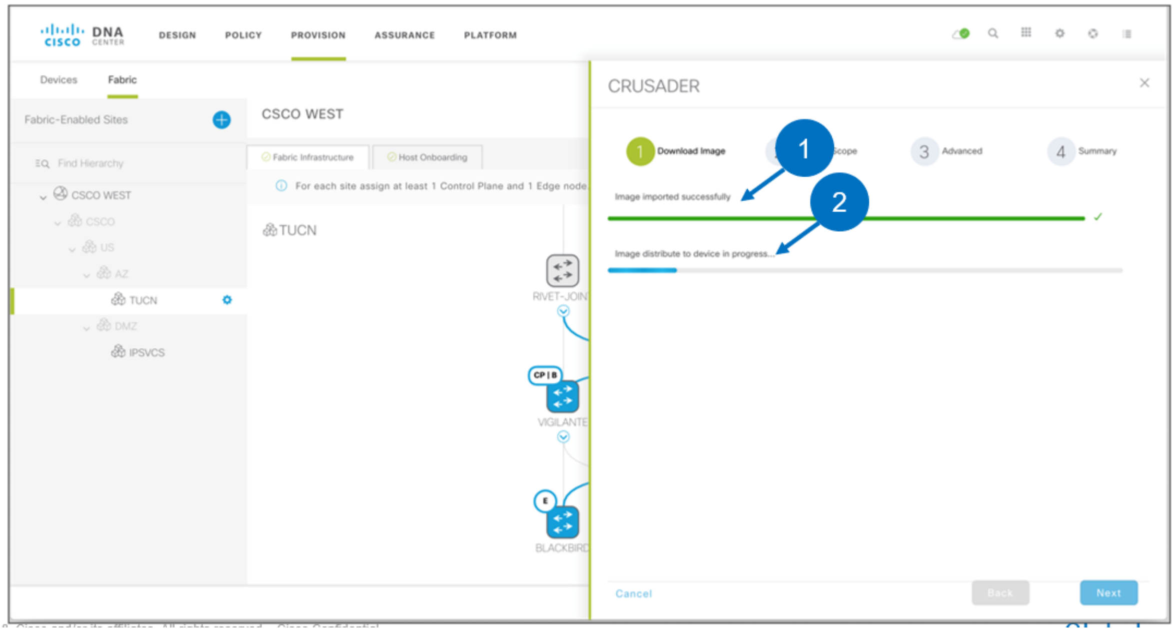
Select an image from computer

C9800-SW-iosxe-wlc.BLD_V1610_1_THROTTLE_LATEST_20181208_002844_2.SSA.bin

☐ Activate image after import

Do not change the original name of the C9800 filename that was downloaded from CCO

d. Import Cisco Catalyst 9800 software

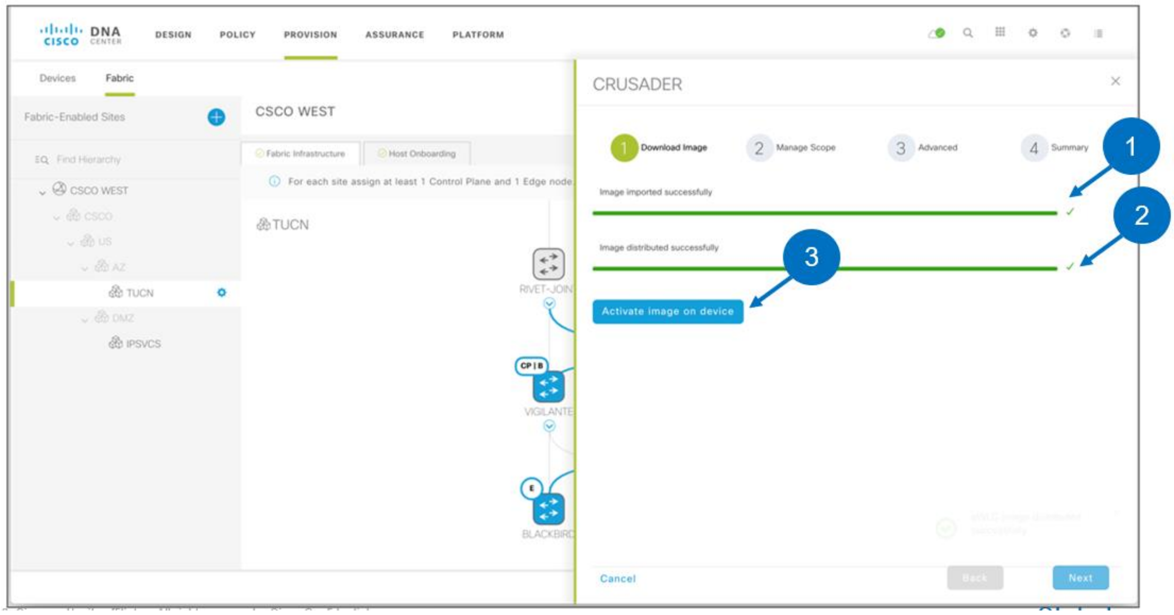


For each site assign at least 1 Control Plane and 1 Edge node

Image imported successfully

Image distribute to device in progress...

e. At this point image is copied to Fabric Border/Control Plane node. Click on *Activate Image on device*

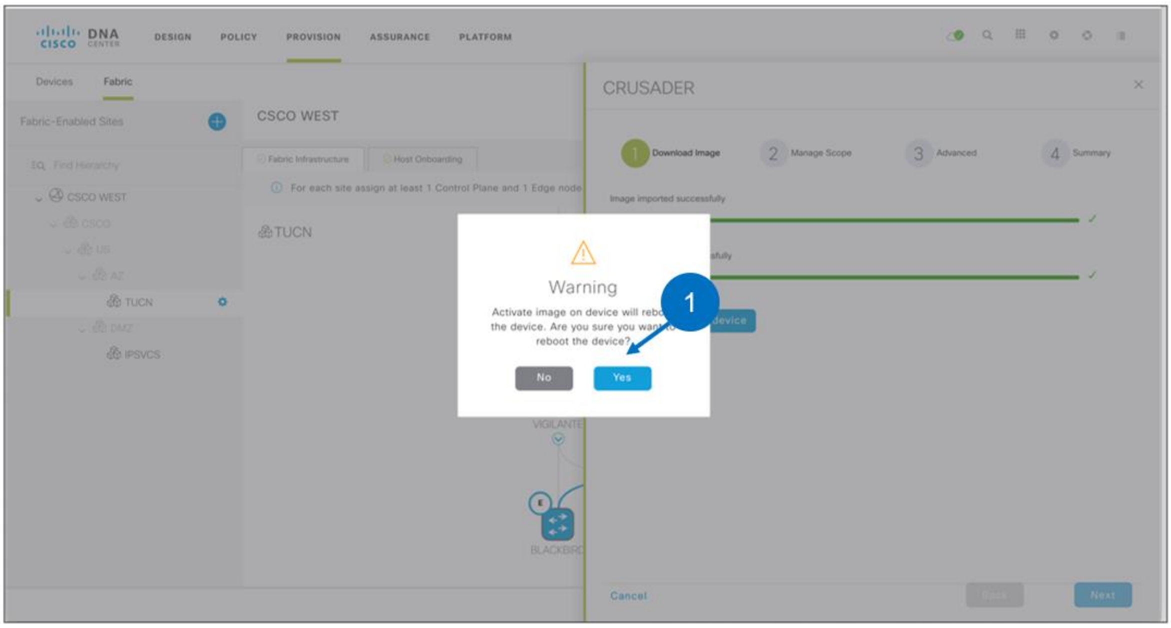


For each site assign at least 1 Control Plane and 1 Edge node

Image imported successfully

Image distributed successfully

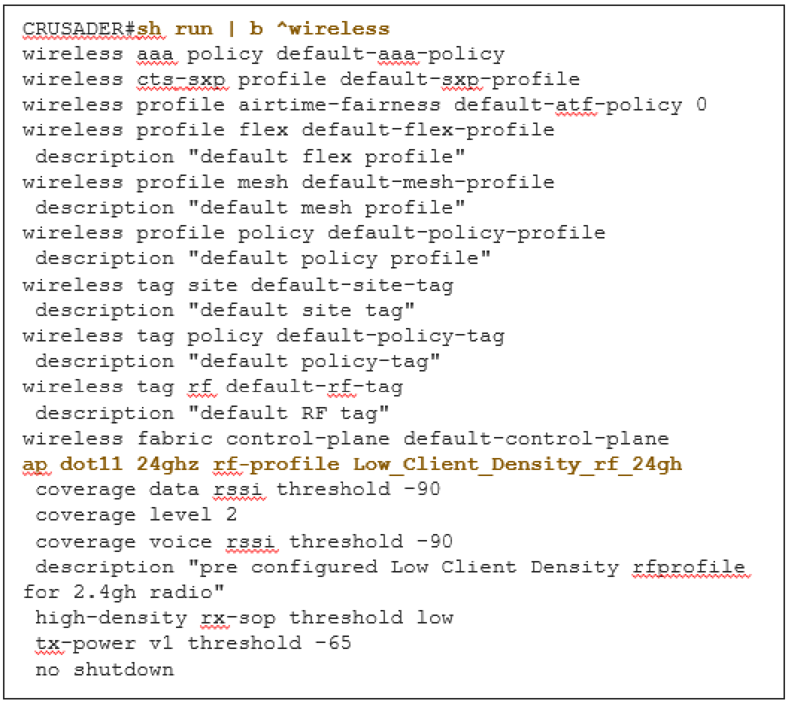
f. The user will be prompted to activate the image which will cause the device to reload



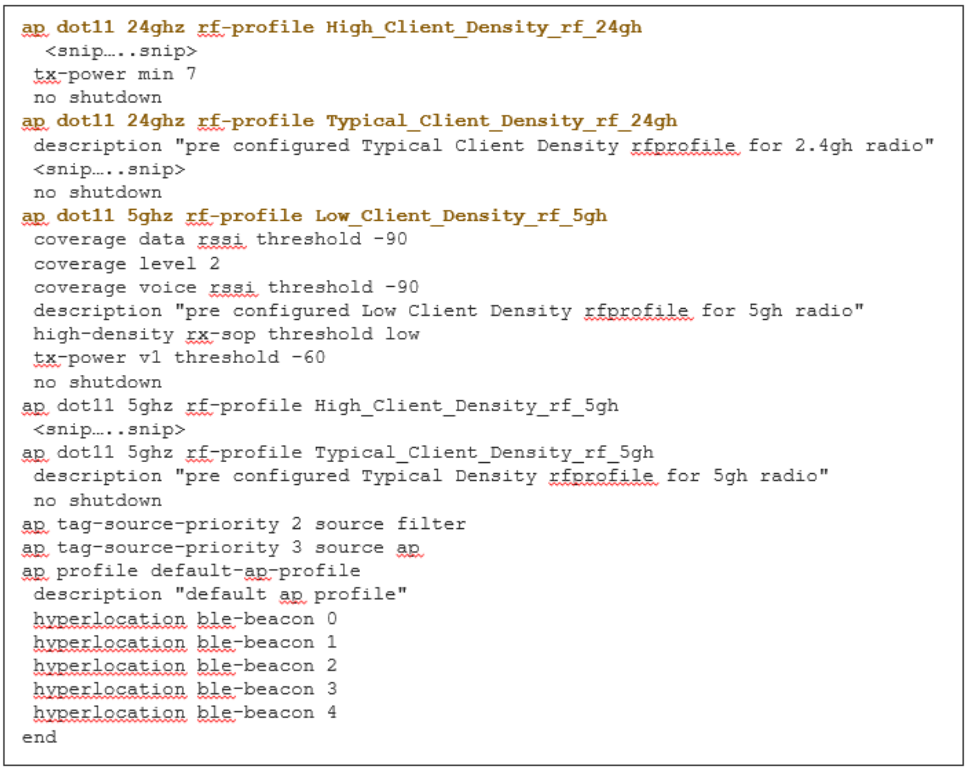
At this point the switch will reboot.

```
.Dec 13 15:04:02.575: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started install add
flash:C9800-SW-iosxe-wlc.BLD_V1610_1_THROTTLE_LATEST_20181208_002844_2.SSA.bin

.Dec 13 15:04:54.311: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds
CRUSADER#
Chassis 1 reloading, reason - Reload command
```

The user will see the following wireless configuration on the Catalyst 9k (Border/Control Plane):



```
CRUSADER#sh run | b ^wireless
wireless aaa policy default-aaa-policy
wireless cts-sxp profile default-sxp-profile
wireless profile airtime-fairness default-atf-policy 0
wireless profile flex default-flex-profile
 description "default flex profile"
wireless profile mesh default-mesh-profile
 description "default mesh profile"
wireless profile policy default-policy-profile
 description "default policy profile"
wireless tag site default-site-tag
 description "default site tag"
wireless tag policy default-policy-tag
 description "default policy-tag"
wireless tag rf default-rf-tag
 description "default RF tag"
wireless fabric control-plane default-control-plane
ap dot11 24ghz rf-profile Low_Client_Density_rf_24gh
 coverage data rssi threshold -90
 coverage level 2
 coverage voice rssi threshold -90
 description "pre configured Low Client Density rfprofile
for 2.4gh radio"
 high-density rx-sop threshold low
 tx-power v1 threshold -65
 no shutdown
```



```
ap dot11 24ghz rf-profile High_Client_Density_rf_24gh
  <snip…..snip>
 tx-power min 7
 no shutdown
ap dot11 24ghz rf-profile Typical_Client_Density_rf_24gh
 description "pre configured Typical Client Density rfprofile for 2.4gh radio"
 <snip…..snip>
 no shutdown
ap dot11 5ghz rf-profile Low_Client_Density_rf_5gh
 coverage data rssi threshold -90
 coverage level 2
 coverage voice rssi threshold -90
 description "pre configured Low Client Density rfprofile for 5gh radio"
 high-density rx-sop threshold low
 tx-power v1 threshold -60
 no shutdown
ap dot11 5ghz rf-profile High_Client_Density_rf_5gh
 <snip…..snip>
ap dot11 5ghz rf-profile Typical_Client_Density_rf_5gh
 description "pre configured Typical Density rfprofile for 5gh radio"
 no shutdown
ap tag-source-priority 2 source filter
ap tag-source-priority 3 source ap
ap profile default-ap-profile
 description "default ap profile"
 hyperlocation ble-beacon 0
 hyperlocation ble-beacon 1
 hyperlocation ble-beacon 2
 hyperlocation ble-beacon 3
 hyperlocation ble-beacon 4
end
```

g. Embedded wireless should be successfully activated at this time

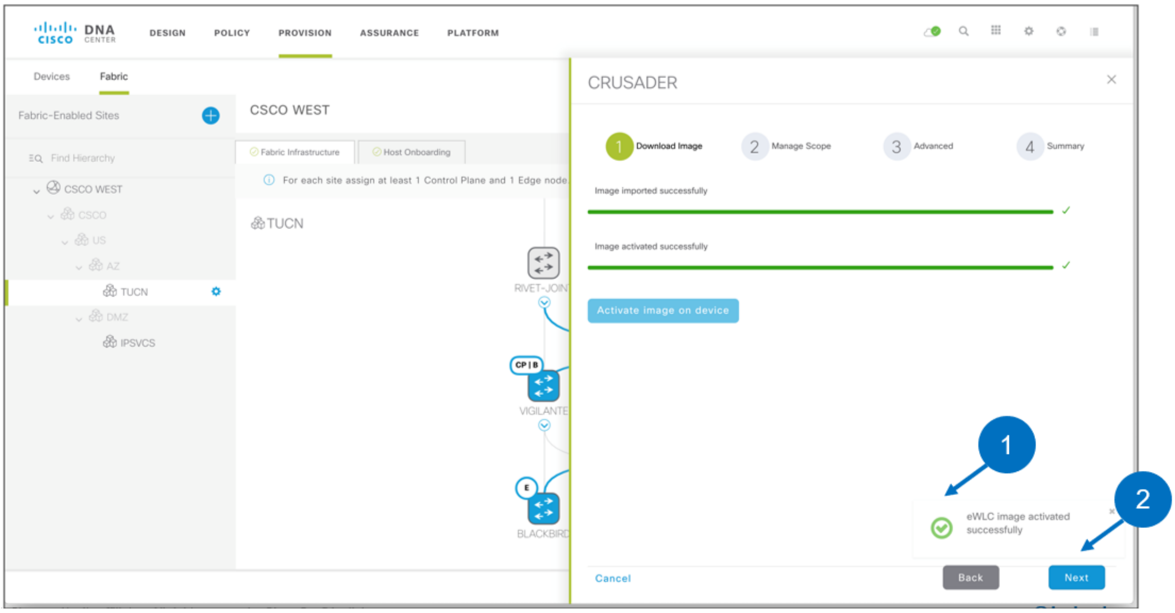


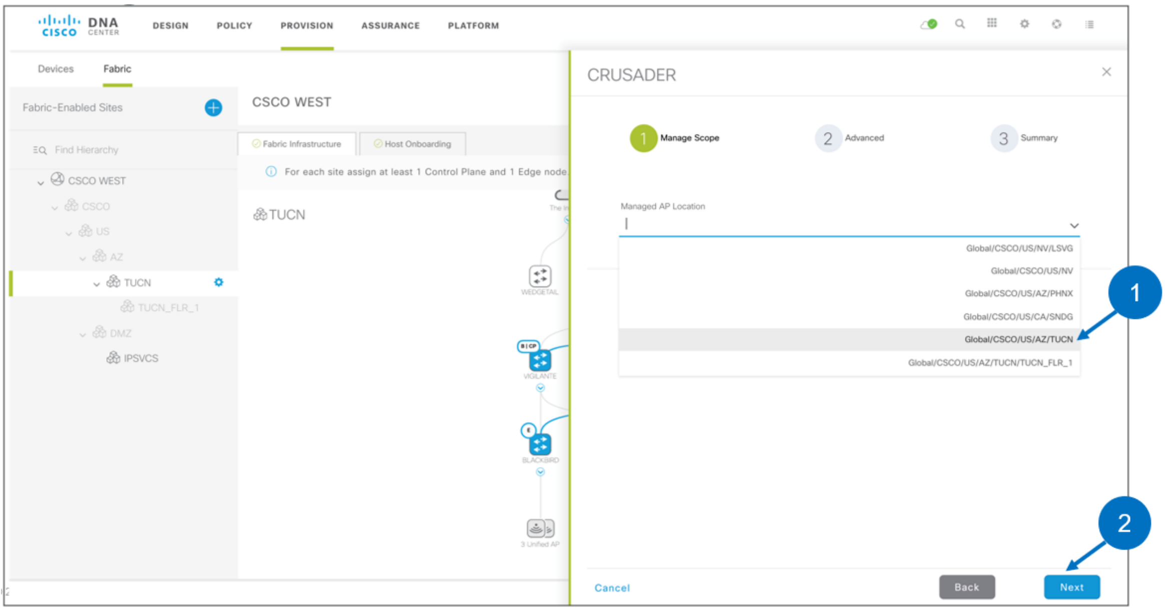
Image imported successfully ✓

Image activated successfully ✓

eWLC image activated successfully

Click *Next*.

h. Next, select all the sites which will have Access Points registered to this wireless controller.

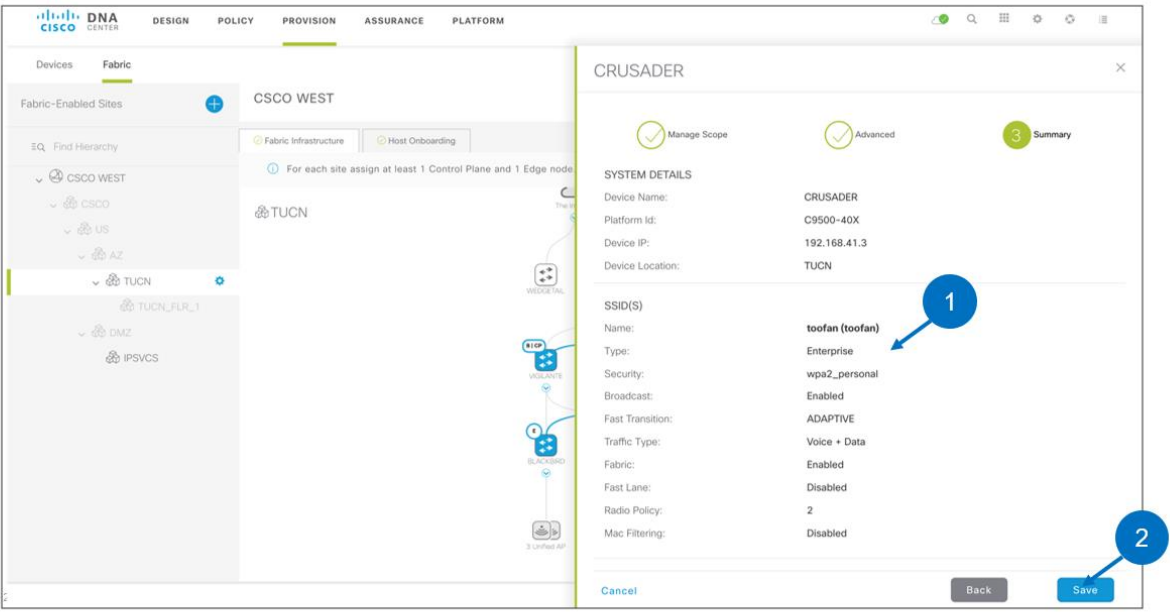


Managed AP Location

Global/CSCO/US/NV/LSVG
Global/CSCO/US/NV
Global/CSCO/US/AZ/PHNX
Global/CSCO/US/CA/SNDG
Global/CSCO/US/AZ/TUCN
Global/CSCO/US/AZ/TUCN/TUCN_FLR_1

Click *Next*

i. Provision the embedded wireless controller with SSIDs and site configuration



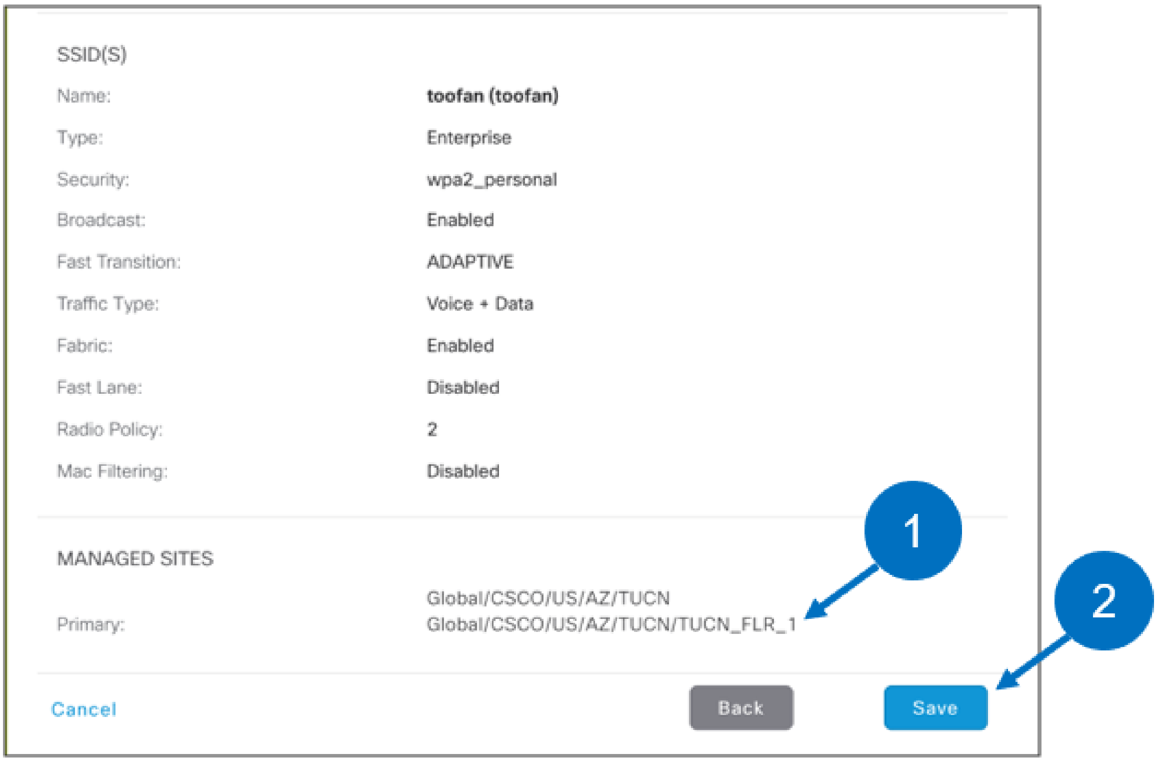
CRUSADER

SYSTEM DETAILS

Device Name:	CRUSADER
Platform Id:	C9500-40X
Device IP:	192.168.41.3
Device Location:	TUCN

SSID(S)

Name:	toofan (toofan)
Type:	Enterprise
Security:	wpa2_personal
Broadcast:	Enabled
Fast Transition:	ADAPTIVE
Traffic Type:	Voice + Data
Fabric:	Enabled
Fast Lane:	Disabled
Radio Policy:	2
Mac Filtering:	Disabled



SSID(S)

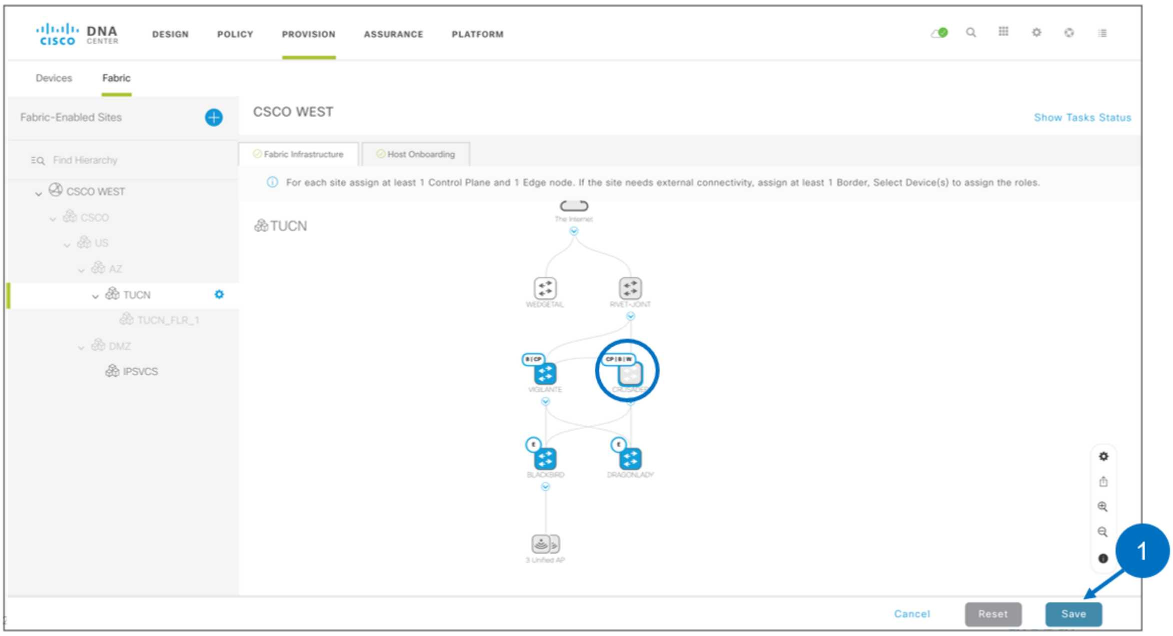
Name:	toofan (toofan)
Type:	Enterprise
Security:	wpa2_personal
Broadcast:	Enabled
Fast Transition:	ADAPTIVE
Traffic Type:	Voice + Data
Fabric:	Enabled
Fast Lane:	Disabled
Radio Policy:	2
Mac Filtering:	Disabled

MANAGED SITES

Primary:	Global/CSCO/US/AZ/TUCN Global/CSCO/US/AZ/TUCN/TUCN_FLR_1

Click *Save*

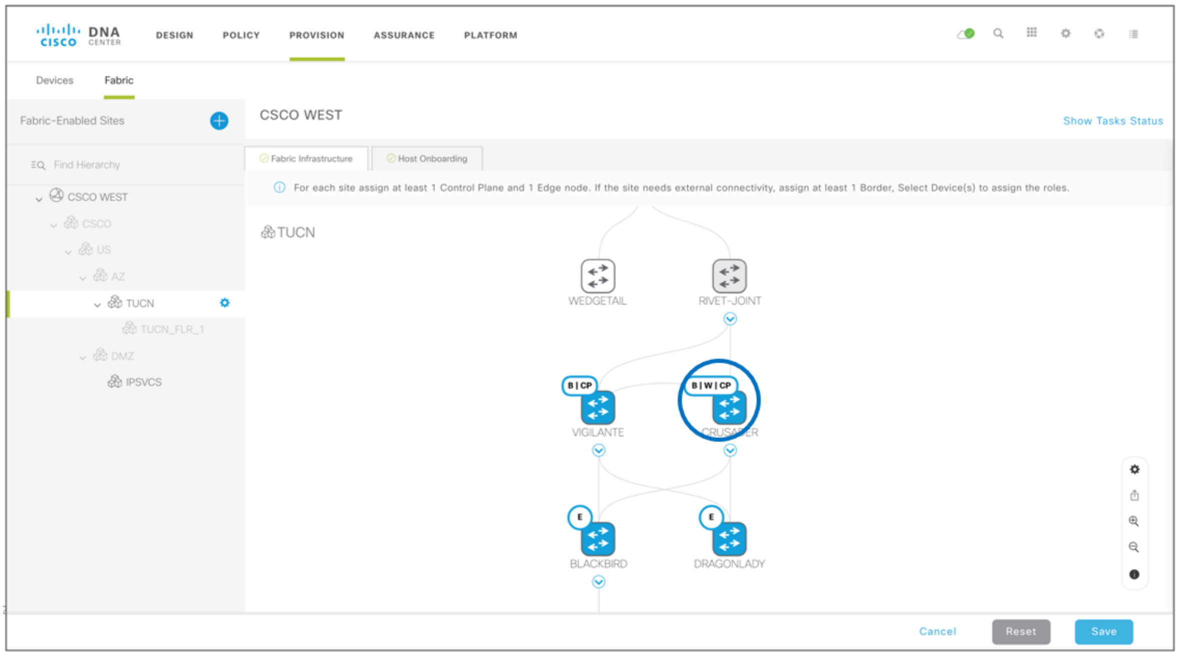
j. At this point, the user will be prompted to the main fabric site page.



For each site assign at least 1 Control Plane and 1 Edge node. If the site needs external connectivity, assign at least 1 Border, Select Device(s) to assign the roles.

Click *Save*

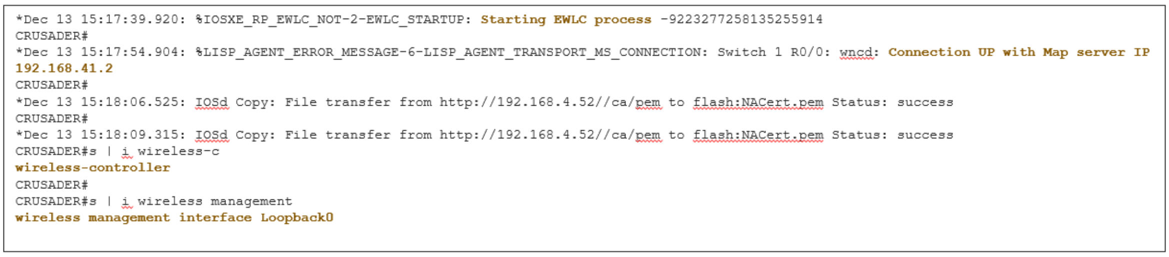
k. This completes provisioning of embedded (Catalyst 9800) wireless controller on Catalyst 9300 to fabric



For each site assign at least 1 Control Plane and 1 Edge node. If the site needs external connectivity, assign at least 1 Border, Select Device(s) to assign the roles.

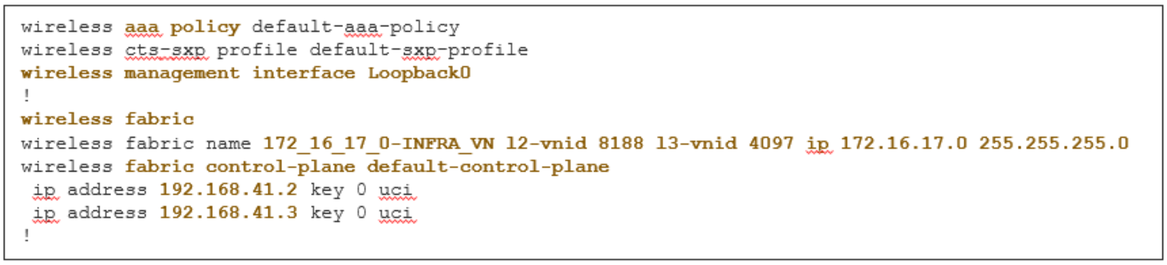
Wireless CLI configurations (pushed on the device):

- On enabling embedded wireless controller on the Catalyst 9k, the user will see the following syslogs on console on the switch



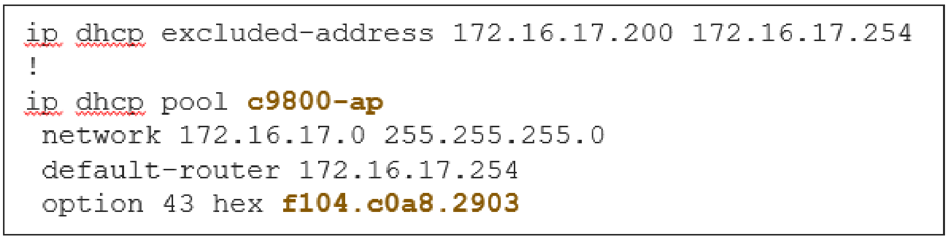
```
*Dec 13 15:17:39.920: %IOSXE_RP_EWLC_NOT-2-EWLC_STARTUP: Starting EWLC process -9223277258135255914
CRUSADER#
*Dec 13 15:17:54.904: %LISP_AGENT_ERROR_MESSAGE-6-LISP_AGENT_TRANSPORT_MS_CONNECTION: Switch 1 R0/0: wncd: Connection UP with Map server IP
192.168.41.2
CRUSADER#
*Dec 13 15:18:06.525: IOSd Copy: File transfer from http://192.168.4.52//ca/pem to flash:NACert.pem Status: success
CRUSADER#
*Dec 13 15:18:09.315: IOSd Copy: File transfer from http://192.168.4.52//ca/pem to flash:NACert.pem Status: success
CRUSADER#s | i wireless-c
wireless-controller
CRUSADER#
CRUSADER#s | i wireless management
wireless management interface Loopback0
```

- Below is the wireless fabric configuration that gets applied on the Catalyst 9k switch:

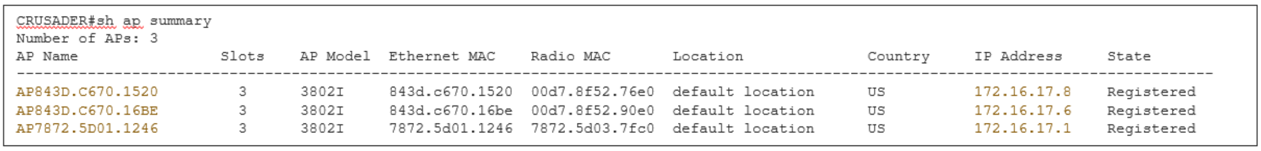


```
wireless aaa policy default-aaa-policy
wireless cts-sxp profile default-sxp-profile
wireless management interface Loopback0
!
wireless fabric
wireless fabric name 172_16_17_0-INFRA_VN l2-vnid 8188 l3-vnid 4097 ip 172.16.17.0 255.255.255.0
wireless fabric control-plane default-control-plane
 ip address 192.168.41.2 key 0 uci
 ip address 192.168.41.3 key 0 uci
!
```

- Access Points will register to the wireless controller via one of the usual means (option 43, DNS or IP helper-address):



```
ip dhcp excluded-address 172.16.17.200 172.16.17.254
!
ip dhcp pool c9800-ap
 network 172.16.17.0 255.255.255.0
 default-router 172.16.17.254
 option 43 hex f104.c0a8.2903
```

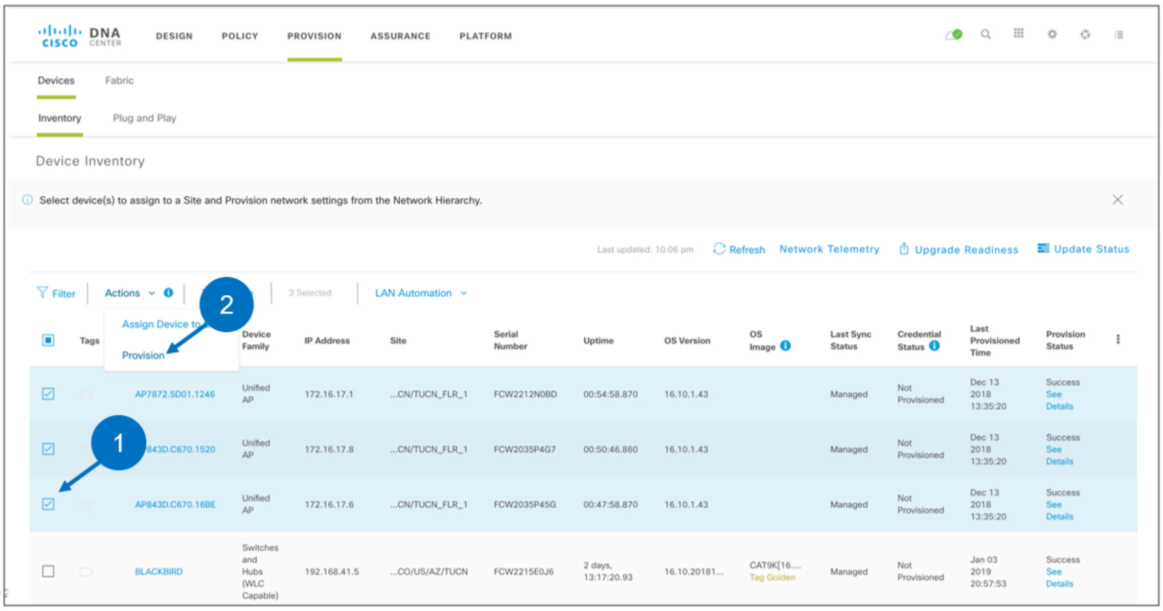


```
CRUSADER#sh ap summary
Number of APs: 3
AP Name                Slots    AP Model  Ethernet MAC    Radio MAC       Location              Country     IP Address     State
---------------------------------------------------------------------------------------------------------------------------------------
AP843D.C670.1520         3      3802I     843d.c670.1520  00d7.8f52.76e0  default location      US          172.16.17.8    Registered
AP843D.C670.16BE         3      3802I     843d.c670.16be  00d7.8f52.90e0  default location      US          172.16.17.6    Registered
AP7872.5D01.1246         3      3802I     7872.5d01.1246  7872.5d03.7fc0  default location      US          172.16.17.1    Registered
```

Provisioning Access Points

Now that the AP obtained an IP address and learnt the WLC's Management IP, the AP will join the WLC. This is under the assumption that there is IP connectivity between AP and WLC (this is outside the scope of this document and really depends on where the WLC is connected, usually outside of Fabric). Once the APs are registered to WLC, they will appear in the Inventory page on Cisco DNA-Center.

5. Go to *PROVISION>Devices* > *Inventory* to see the APs joining the fabric enabled embedded wireless controller (on Catalyst 9k).



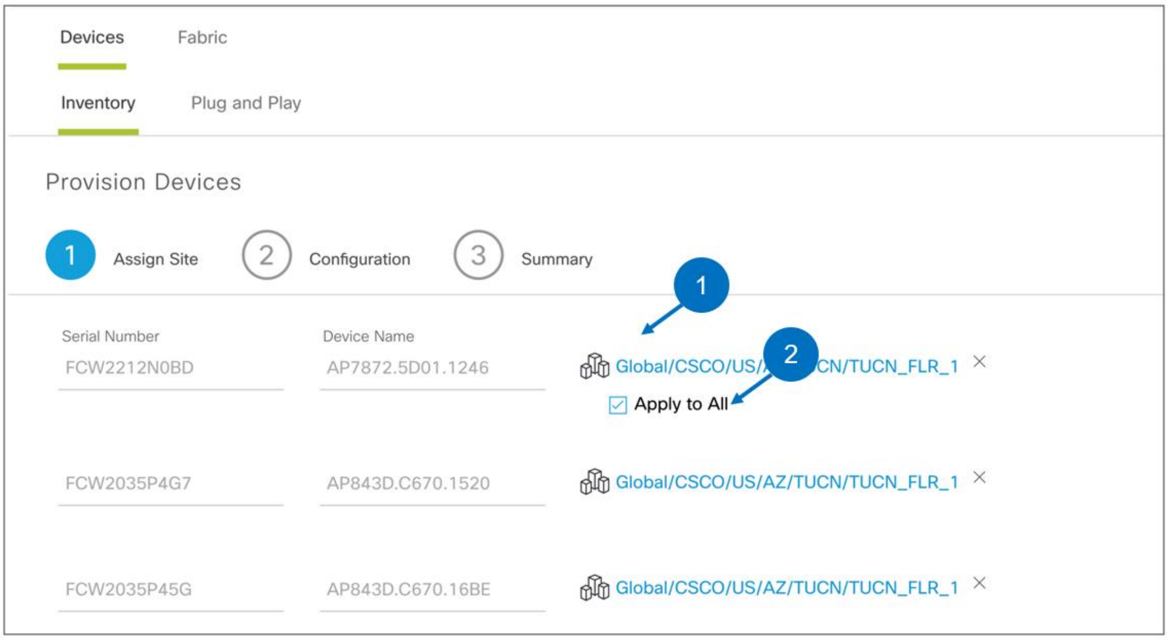
Device Inventory

ⓘ Select device(s) to assign to a Site and Provision network settings from the Network Hierarchy.

Last updated: 10:06 pm Refresh Network Telemetry Upgrade Readiness Update Status

■	Tags	Device Name	Device Family	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Last Sync Status	Credential Status	Last Provisioned Time	Provision Status
☑		AP7872.5D01.1246	Unified AP	172.16.17.1	...CN/TUCN_FLR_1	FCW2212N0BD	00:54:58.870	16.10.1.43		Managed	Not Provisioned	Dec 13 2018 13:35:20	Success See Details
☑		843D.C670.1520	Unified AP	172.16.17.8	...CN/TUCN_FLR_1	FCW2035P4G7	00:50:46.860	16.10.1.43		Managed	Not Provisioned	Dec 13 2018 13:35:20	Success See Details
☑		AP843D.C670.16BE	Unified AP	172.16.17.6	...CN/TUCN_FLR_1	FCW2035P45G	00:47:58.870	16.10.1.43		Managed	Not Provisioned	Dec 13 2018 13:35:20	Success See Details
☐		BLACKBIRD	Switches and Hubs (WLC Capable)	192.168.41.5	...CO/US/AZ/TUCN	FCW2215E0J6	2 days, 13:17:20.93	16.10.20181...	CAT9K[16.... Tag Golden	Managed	Not Provisioned	Jan 03 2019 20:57:53	Success See Details

6. Begin by assigning the Access Points to the site where they are installed

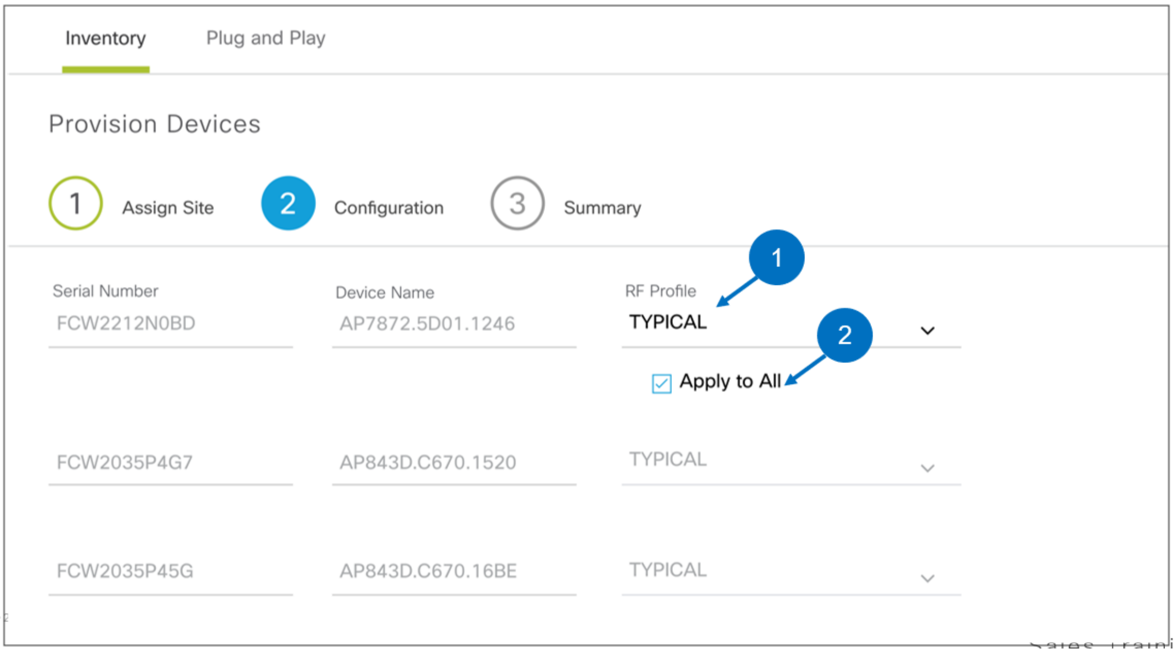


Provision Devices

① Assign Site ② Configuration ③ Summary

Serial Number	Device Name	
FCW2212N0BD	AP7872.5D01.1246	Global/CSCO/US/ CN/TUCN_FLR_1 × ☑ Apply to All
FCW2035P4G7	AP843D.C670.1520	Global/CSCO/US/AZ/TUCN/TUCN_FLR_1 ×
FCW2035P45G	AP843D.C670.16BE	Global/CSCO/US/AZ/TUCN/TUCN_FLR_1 ×

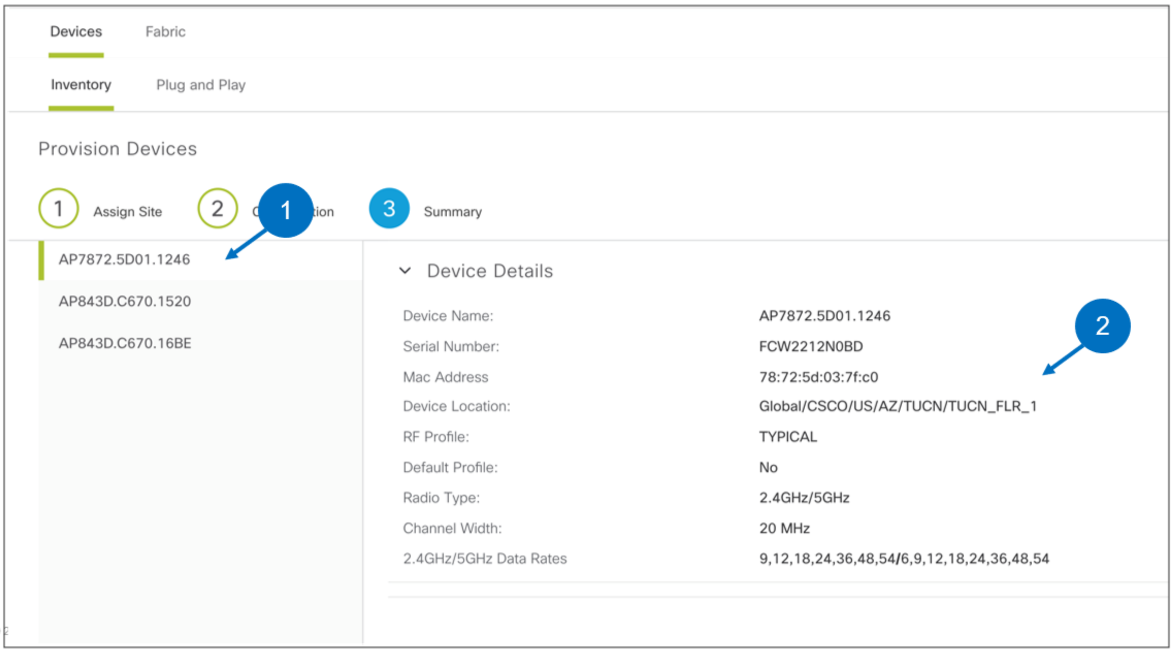
7. Choose a RF profile for the AP from High, Typical and Low or a customized one (if previously defined).



Provision Devices

Serial Number	Device Name	RF Profile
FCW2212N0BD	AP7872.5D01.1246	TYPICAL ☑ Apply to All
FCW2035P4G7	AP843D.C670.1520	TYPICAL
FCW2035P45G	AP843D.C670.16BE	TYPICAL

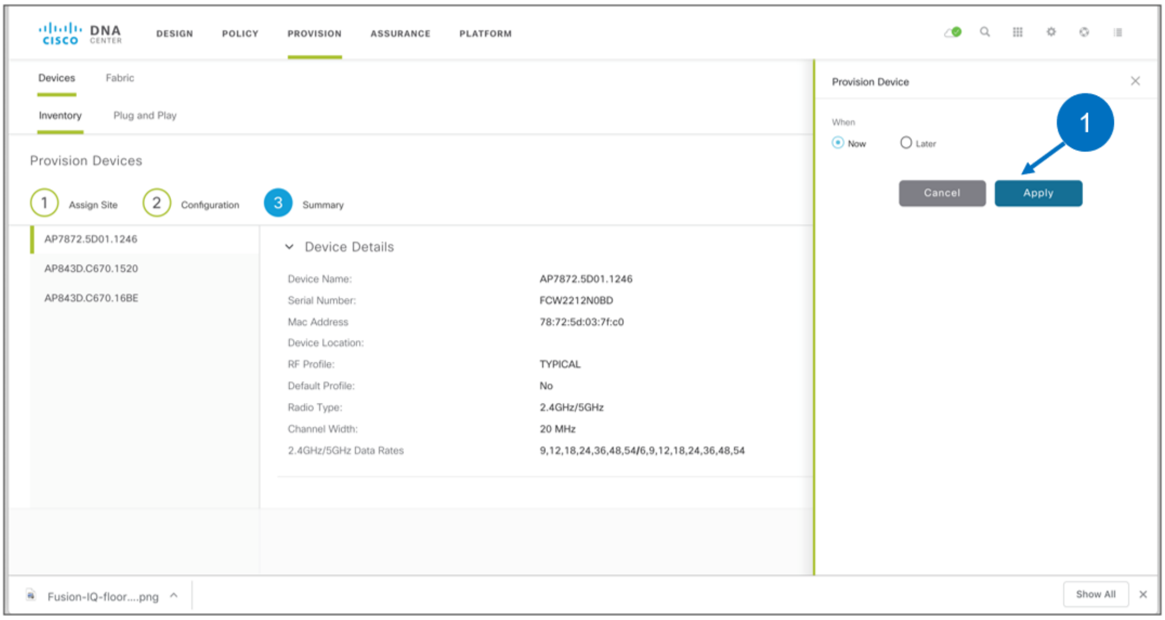
8. Click *Deploy* and as a part of AP provisioning, configuration will be pushed to AP as shown below.



Provision Devices

Device Details

Device Name:	AP7872.5D01.1246
Serial Number:	FCW2212N0BD
Mac Address	78:72:5d:03:7f:c0
Device Location:	Global/CSCO/US/AZ/TUCN/TUCN_FLR_1
RF Profile:	TYPICAL
Default Profile:	No
Radio Type:	2.4GHz/5GHz
Channel Width:	20 MHz
2.4GHz/5GHz Data Rates	9,12,18,24,36,48,54/6,9,12,18,24,36,48,54

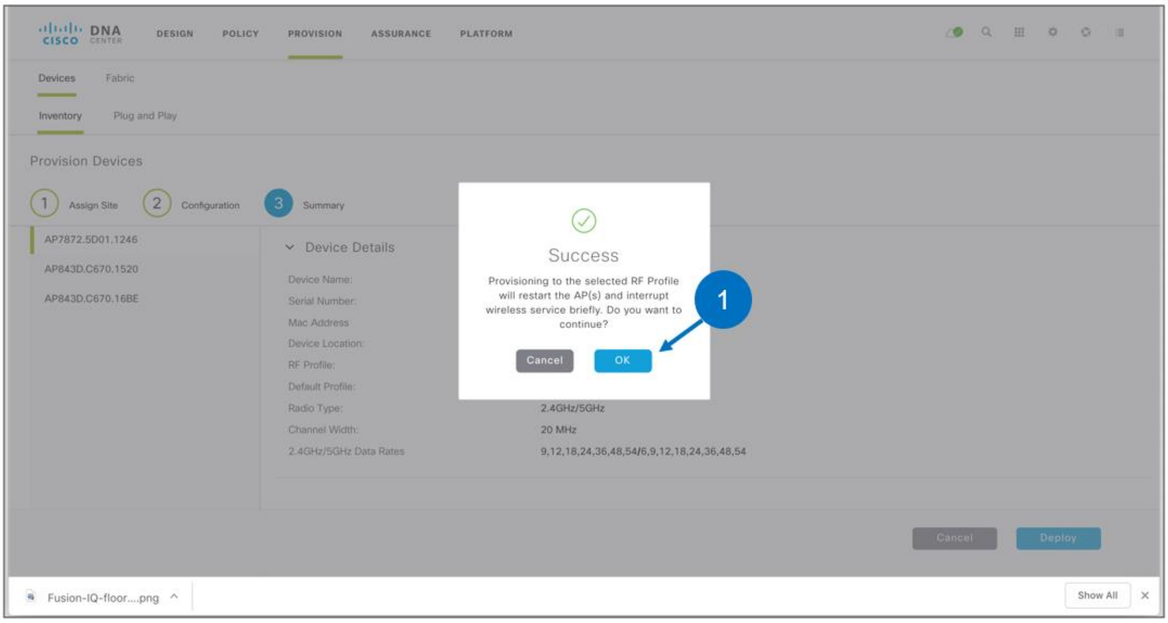


AP7872.5D01.1246
AP843D.C670.1520
AP843D.C670.16BE

Device Details

Device Name:	AP7872.5D01.1246
Serial Number:	FCW2212N0BD
Mac Address	78:72:5d:03:7f:c0
Device Location:	
RF Profile:	TYPICAL
Default Profile:	No
Radio Type:	2.4GHz/5GHz
Channel Width:	20 MHz
2.4GHz/5GHz Data Rates	9,12,18,24,36,48,54/6,9,12,18,24,36,48,54

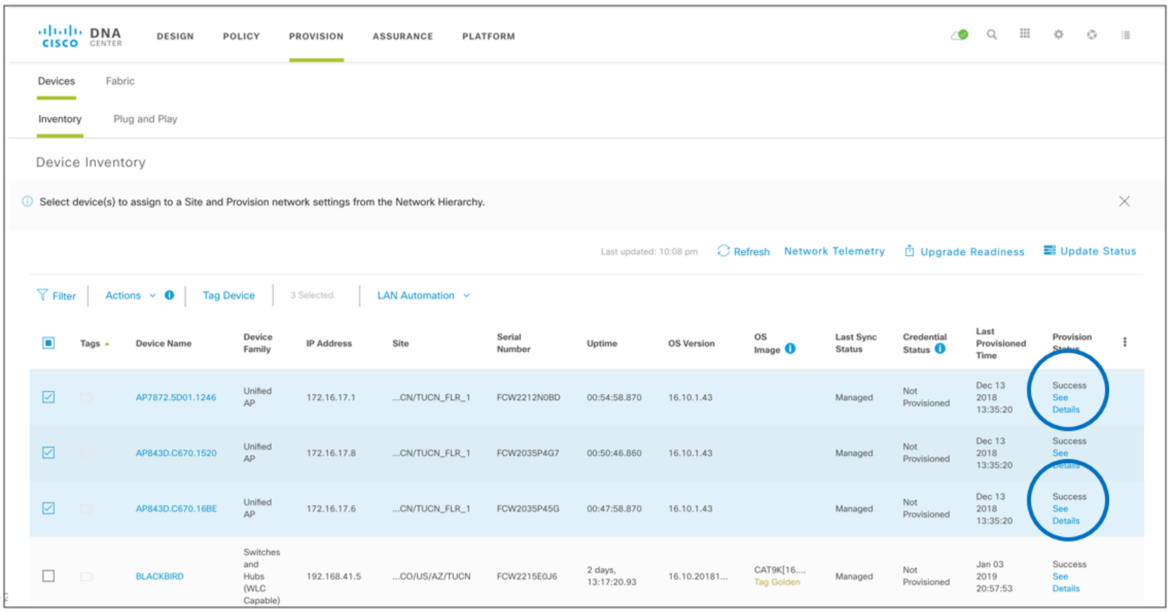
9. AP will reboot and rejoin the wireless controller.



Success

Provisioning to the selected RF Profile will restart the AP(s) and interrupt wireless service briefly. Do you want to continue?

10. The user will now see APs provision as success.



Device Inventory

Select device(s) to assign to a Site and Provision network settings from the Network Hierarchy.

Last updated: 10:08 pm

	Tags	Device Name	Device Family	IP Address	Site	Serial Number	Uptime	OS Version	OS Image	Last Sync Status	Credential Status	Last Provisioned Time	Provision Status
☑		AP7872.5D01.1246	Unified AP	172.16.17.1	...CN/TUCN_FLR_1	FCW2212N0BD	00:54:58.870	16.10.1.43		Managed	Not Provisioned	Dec 13 2018 13:35:20	Success See Details
☑		AP843D.C670.1520	Unified AP	172.16.17.8	...CN/TUCN_FLR_1	FCW2035P4G7	00:50:46.860	16.10.1.43		Managed	Not Provisioned	Dec 13 2018 13:35:20	Success See Details
☑		AP843D.C670.16BE	Unified AP	172.16.17.6	...CN/TUCN_FLR_1	FCW2035P45G	00:47:58.870	16.10.1.43		Managed	Not Provisioned	Dec 13 2018 13:35:20	Success See Details
☐		BLACKBIRD	Switches and Hubs (WLC Capable)	192.168.41.5	...CO/US/AZ/TUCN	FCW2215E0J6	2 days, 13:17:20.93	16.10.20181...	CAT9K[16.... Tag Golden	Managed	Not Provisioned	Jan 03 2019 20:57:53	Success See Details

Registered APs are SD-Access fabric enabled. Catalyst 9k switch will show the following configuration:

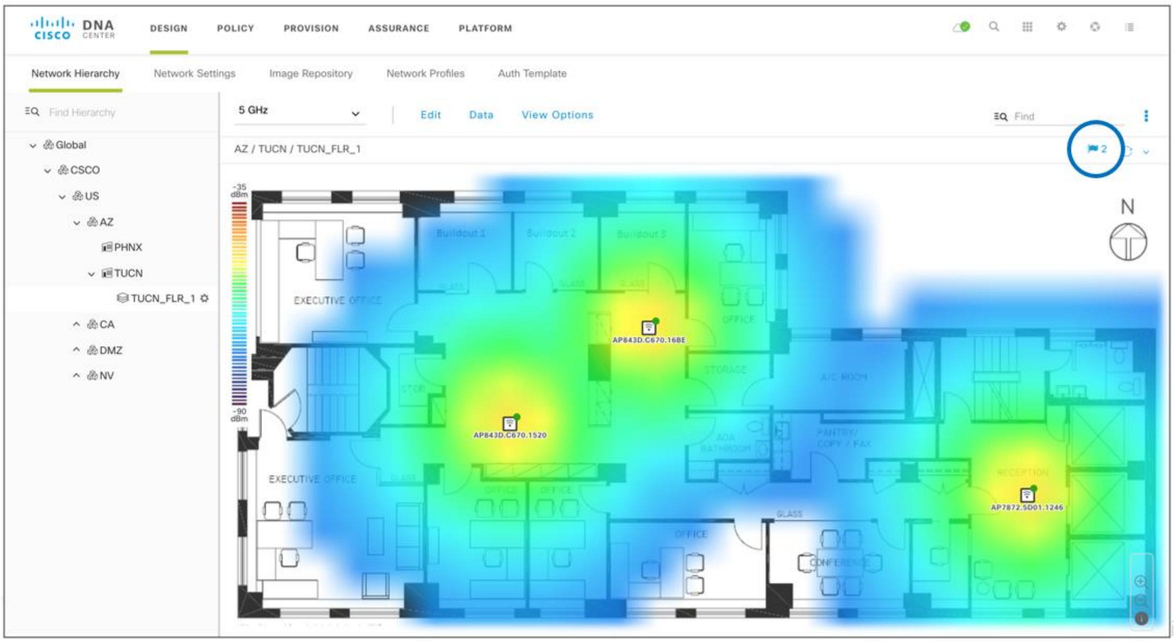
```
ap country US
ap tag-source-priority 2 source filter
ap tag-source-priority 3 source ap
!
ap 7872.5D01.1246
 policy-tag PT_AZ_TUCN_TUCN__7c723
 rf-tag TYPICAL
 site-tag default-site-tag-fabric
ap 843D.C670.1520
 policy-tag PT_AZ_TUCN_TUCN__7c723
 rf-tag TYPICAL
 site-tag default-site-tag-fabric
ap 843D.C670.16BE
 policy-tag PT_AZ_TUCN_TUCN__7c723

CRUSADER#sh fabric ap summary
Number of Fabric AP : 3
AP Name                    Slots   AP Model  Ethernet MAC    Radio MAC       Location          Country    IP Address       State
------------------------------------------------------------------------------------------------------------------------
AP843D.C670.1520        3       3802I     843d.c670.1520  00d7.8f52.76e0  default location  US    172.16.17.8     Registered
AP843D.C670.16BE        3       3802I     843d.c670.16be  00d7.8f52.90e0  default location  US    172.16.17.6     Registered
AP7872.5D01.1246        3       3802I     7872.5d01.1246  7872.5d03.7fc0  default location  US    172.16.17.1     Registered
```

Confirm VXLAN tunnel between the APs and the connected fabric edge:

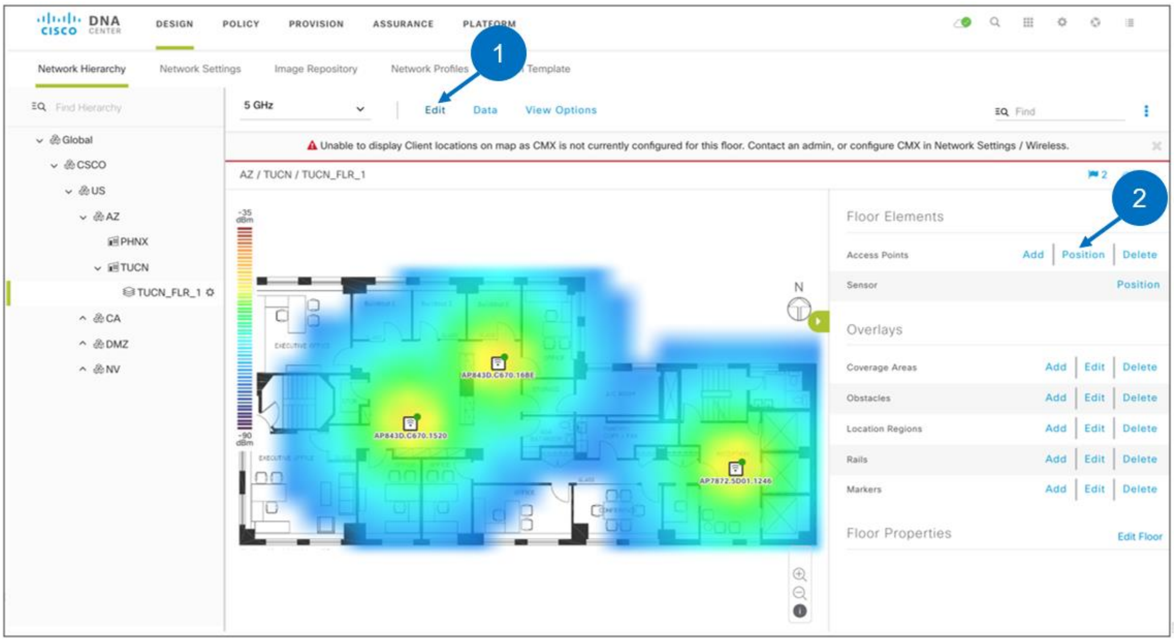
```
BLACKBIRD#sh access-tunnel summary
Access Tunnels General Statistics:
Number of AccessTunnel Data Tunnels       = 3

Name   SrcIP           SrcPort DestIP          DstPort VrfId
------ --------------- ------- --------------- ------- ----
Ac1    192.168.41.5    N/A     172.16.17.6     4789    0
Ac2    192.168.41.5    N/A     172.16.17.8     4789    0
Ac0    192.168.41.5    N/A     172.16.17.1     4789    0

Name   IfId          Uptime
------ ---------- --------------------
Ac1    0x0000003E 0 days, 00:16:07
Ac2    0x0000003F 0 days, 00:15:56
Ac0    0x0000003D 0 days, 00:15:42
```

Placing APs on Map

11. Next, you can place APs on floor maps and get coverage heatmap visualization. Go back to *DESIGN* and select the floor under *Network Hierarchy*.

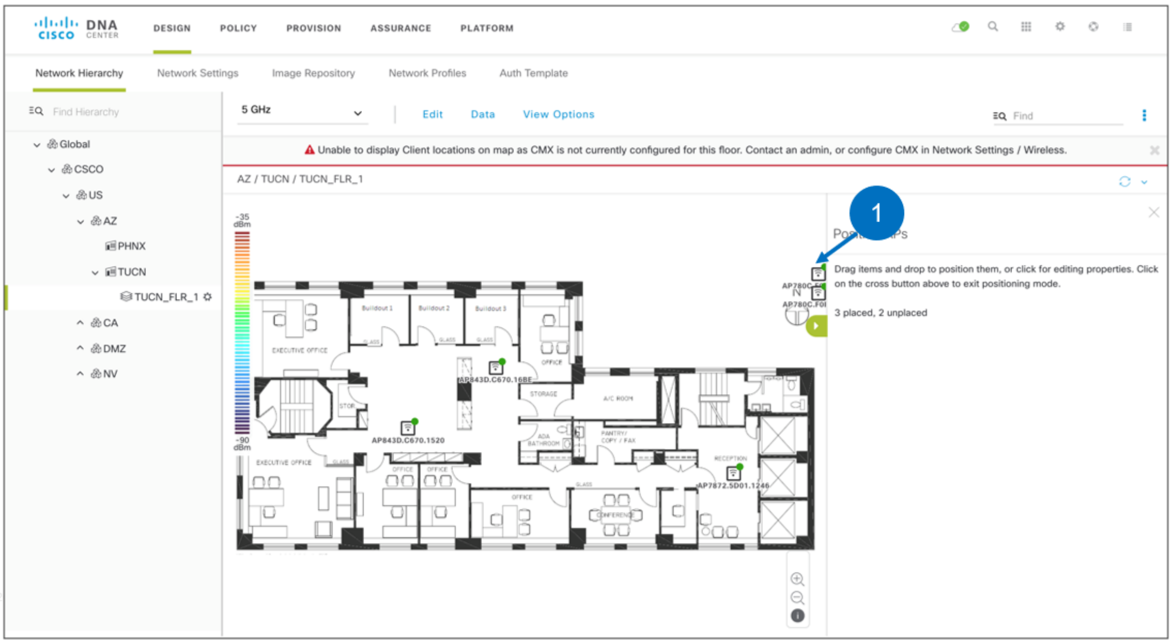


12. Click on *Edit* and the click on *Position*. Example shown below.



Unable to display Client locations on map as CMX is not currently configured for this floor. Contact an admin, or configure CMX in Network Settings / Wireless.

13. The APs will appear in the corner and you can drag and drop them where they are located.

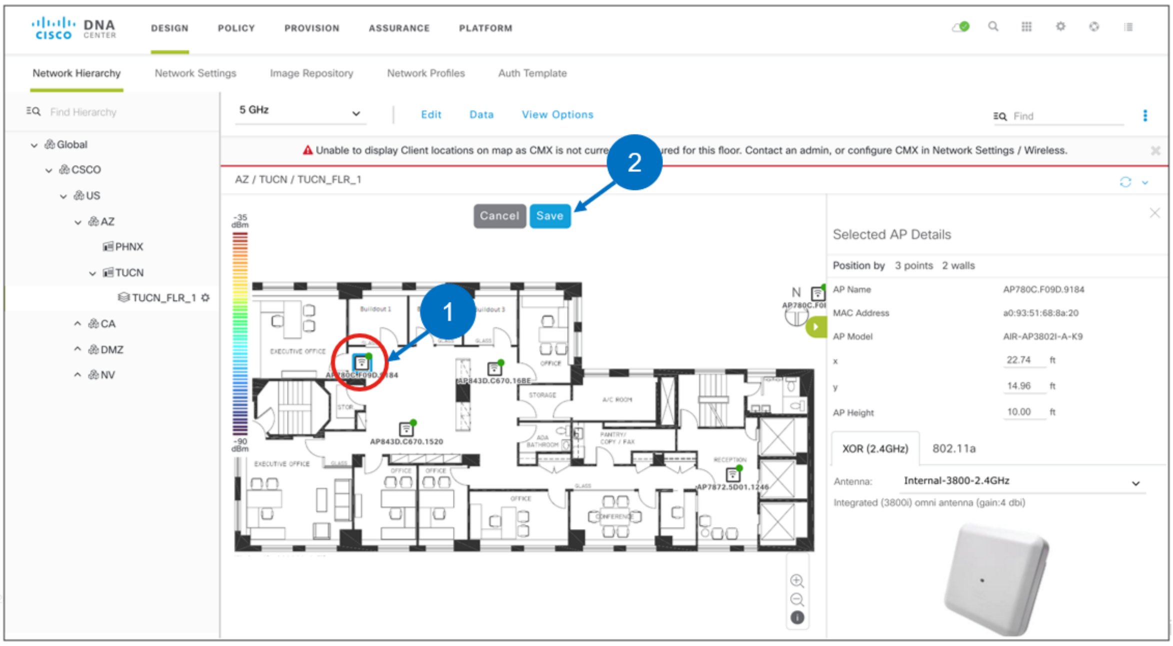


Unable to display Client locations on map as CMX is not currently configured for this floor. Contact an admin, or configure CMX in Network Settings / Wireless.

Drag items and drop to position them, or click for editing properties. Click on the cross button above to exit positioning mode.

3 placed, 2 unplaced

14. Next click *Save*.



Unable to display Client locations on map as CMX is not currently configured for this floor. Contact an admin, or configure CMX in Network Settings / Wireless.

Selected AP Details

Position by 3 points 2 walls

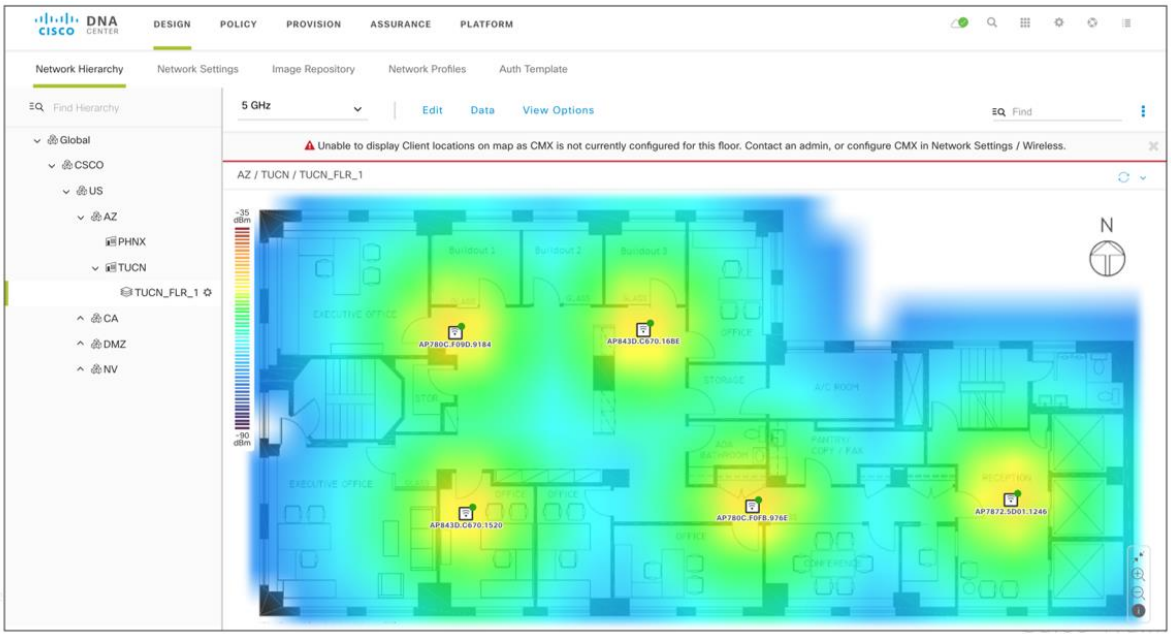
AP Name	AP780C.F09D.9184
MAC Address	a0:93:51:68:8a:20
AP Model	AIR-AP3802I-A-K9
x	22.74 ft
y	14.96 ft
AP Height	10.00 ft

XOR (2.4GHz) 802.11a

Antenna: Internal-3800-2.4GHz

Integrated (3800i) omni antenna (gain:4 dbi)

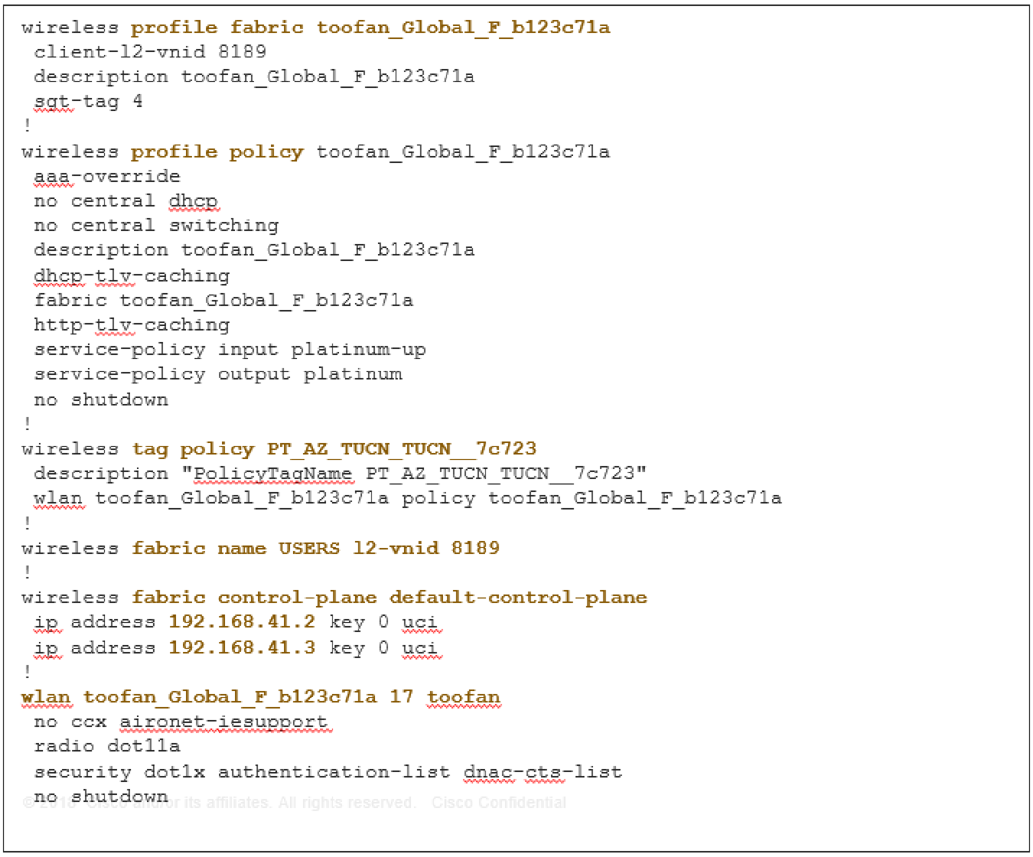
15. Heap maps will be calculated and result displayed as below:



Unable to display Client locations on map as CMX is not currently configured for this floor. Contact an admin, or configure CMX in Network Settings / Wireless.

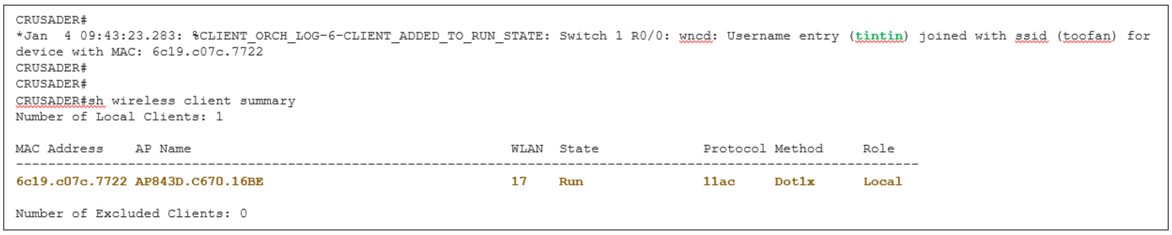
Verifying Wireless Fabric configuration (CLI) on Catalyst 9k switch

1. Below is a sample of enterprise WLAN fabric wireless configuration

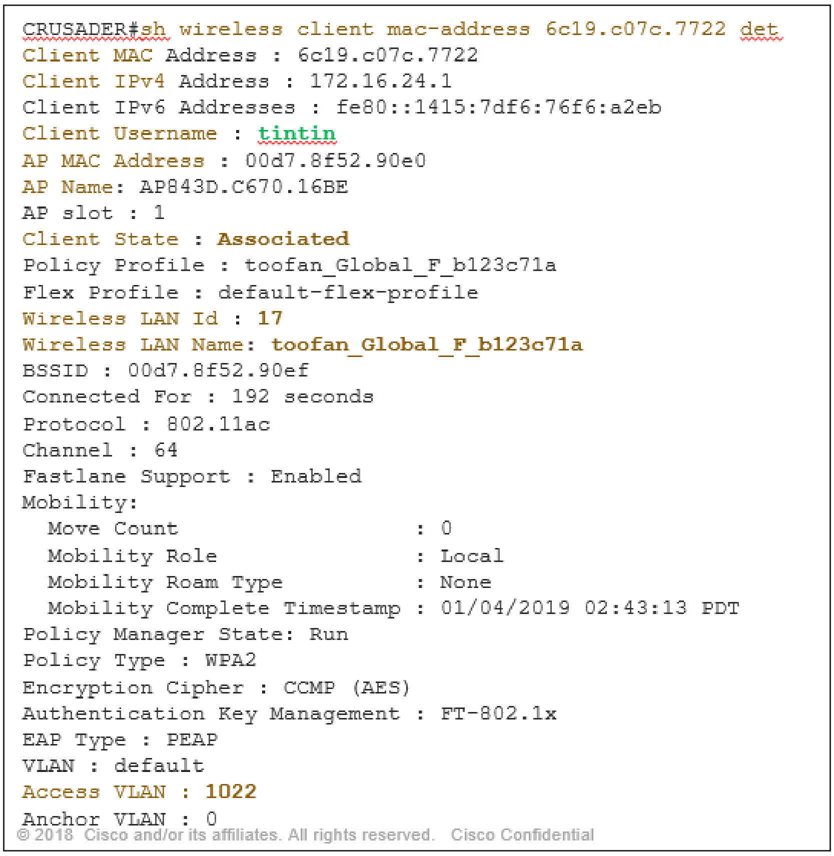


```
wireless profile fabric toofan_Global_F_b123c71a
 client-l2-vnid 8189
 description toofan_Global_F_b123c71a
 sgt-tag 4
!
wireless profile policy toofan_Global_F_b123c71a
 aaa-override
 no central dhcp
 no central switching
 description toofan_Global_F_b123c71a
 dhcp-tlv-caching
 fabric toofan_Global_F_b123c71a
 http-tlv-caching
 service-policy input platinum-up
 service-policy output platinum
 no shutdown
!
wireless tag policy PT_AZ_TUCN_TUCN__7c723
 description "PolicyTagName PT_AZ_TUCN_TUCN__7c723"
 wlan toofan_Global_F_b123c71a policy toofan_Global_F_b123c71a
!
wireless fabric name USERS l2-vnid 8189
!
wireless fabric control-plane default-control-plane
 ip address 192.168.41.2 key 0 uci
 ip address 192.168.41.3 key 0 uci
!
wlan toofan_Global_F_b123c71a 17 toofan
 no ccx aironet-iesupport
 radio dot11a
 security dot1x authentication-list dnac-cts-list
 no shutdown
```

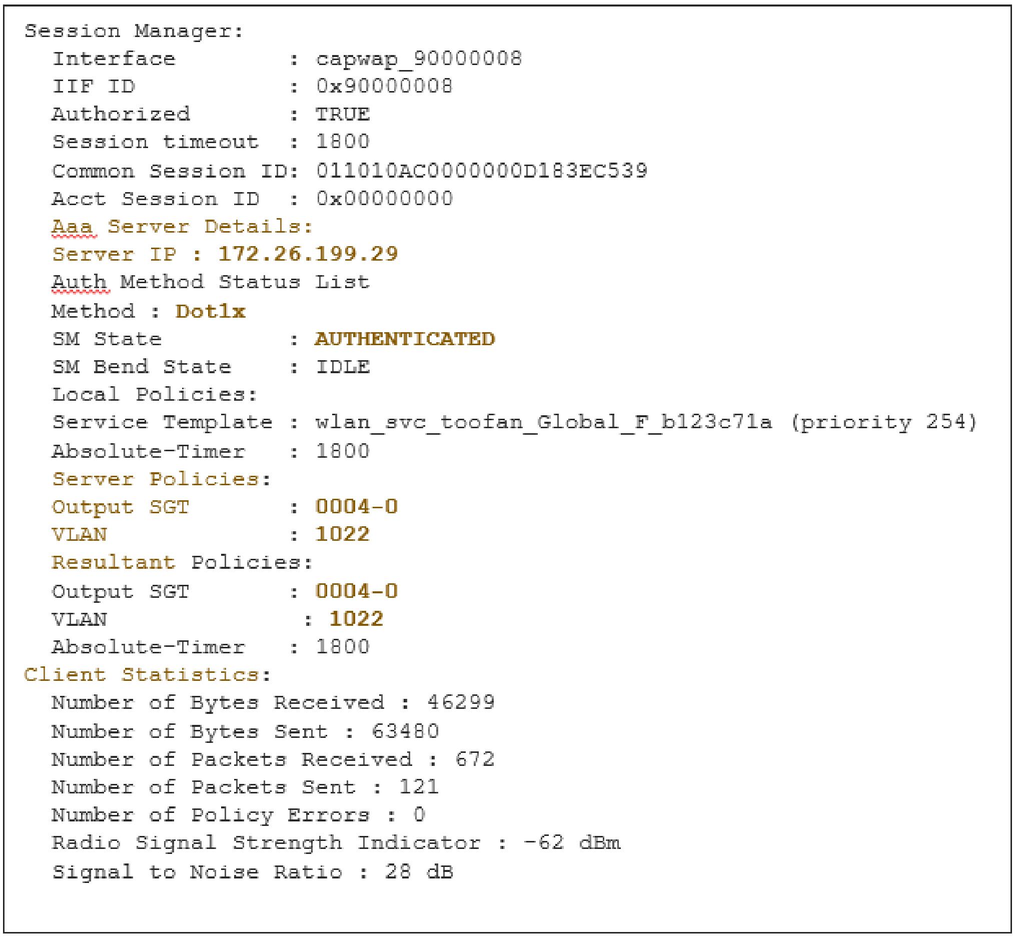
2. Client join details can be monitored from the switch



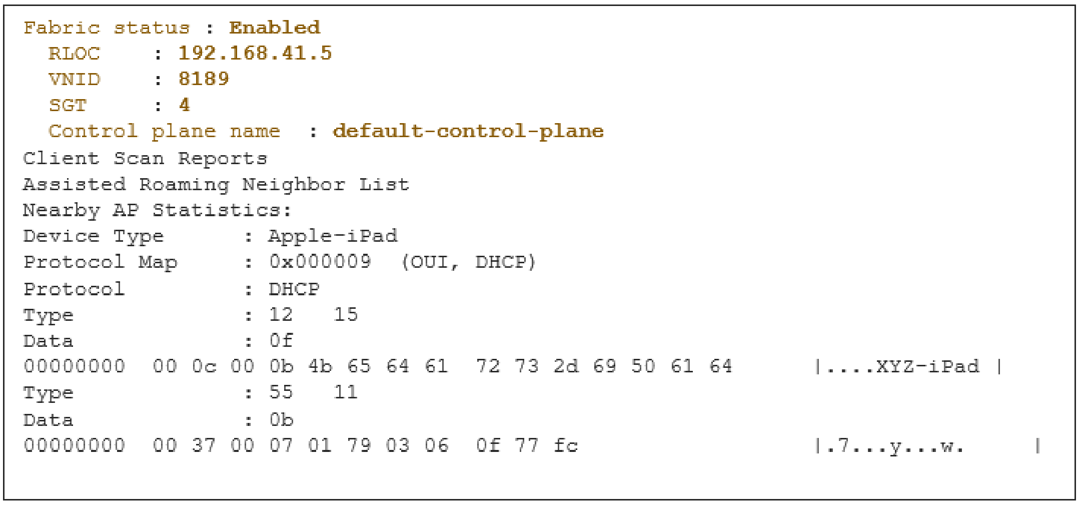
```
CRUSADER#
*Jan  4 09:43:23.283: %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: Switch 1 R0/0: wncd: Username entry (tintin) joined with ssid (toofan) for
device with MAC: 6c19.c07c.7722
CRUSADER#
CRUSADER#
CRUSADER#sh wireless client summary
Number of Local Clients: 1

MAC Address    AP Name                                        WLAN  State              Protocol Method     Role
-------------------------------------------------------------------------------------------------------------------
6c19.c07c.7722 AP843D.C670.16BE                               17    Run                11ac     Dot1x      Local

Number of Excluded Clients: 0
```



```
CRUSADER#sh wireless client mac-address 6c19.c07c.7722 det
Client MAC Address : 6c19.c07c.7722
Client IPv4 Address : 172.16.24.1
Client IPv6 Addresses : fe80::1415:7df6:76f6:a2eb
Client Username : tintin
AP MAC Address : 00d7.8f52.90e0
AP Name: AP843D.C670.16BE
AP slot : 1
Client State : Associated
Policy Profile : toofan_Global_F_b123c71a
Flex Profile : default-flex-profile
Wireless LAN Id : 17
Wireless LAN Name: toofan_Global_F_b123c71a
BSSID : 00d7.8f52.90ef
Connected For : 192 seconds
Protocol : 802.11ac
Channel : 64
Fastlane Support : Enabled
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 01/04/2019 02:43:13 PDT
Policy Manager State: Run
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : FT-802.1x
EAP Type : PEAP
VLAN : default
Access VLAN : 1022
Anchor VLAN : 0
```



```
Session Manager:
  Interface         : capwap_90000008
  IIF ID            : 0x90000008
  Authorized        : TRUE
  Session timeout   : 1800
  Common Session ID: 011010AC0000000D183EC539
  Acct Session ID   : 0x00000000
  Aaa Server Details:
  Server IP : 172.26.199.29
  Auth Method Status List
  Method : Dot1x
  SM State          : AUTHENTICATED
  SM Bend State     : IDLE
  Local Policies:
  Service Template : wlan_svc_toofan_Global_F_b123c71a (priority 254)
  Absolute-Timer    : 1800
  Server Policies:
  Output SGT        : 0004-0
  VLAN              : 1022
  Resultant Policies:
  Output SGT        : 0004-0
  VLAN               : 1022
  Absolute-Timer    : 1800
Client Statistics:
  Number of Bytes Received : 46299
  Number of Bytes Sent : 63480
  Number of Packets Received : 672
  Number of Packets Sent : 121
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -62 dBm
  Signal to Noise Ratio : 28 dB
```



```
Fabric status : Enabled
  RLOC     : 192.168.41.5
  VNID     : 8189
  SGT      : 4
  Control plane name   : default-control-plane
Client Scan Reports
Assisted Roaming Neighbor List
Nearby AP Statistics:
Device Type        : Apple-iPad
Protocol Map       : 0x000009  (OUI, DHCP)
Protocol           : DHCP
Type               : 12   15
Data               : 0f
00000000  00 0c 00 0b 4b 65 64 61  72 73 2d 69 50 61 64      |....XYZ-iPad |
Type               : 55   11
Data               : 0b
00000000  00 37 00 07 01 79 03 06  0f 77 fc                  |.7...y...w.     |
```

3. Monitoring client IP/MAC registration in Control Plane node

```
CRUSADER#sh lisp site instance 4099 | i 172.16.24.1
               00:06:43  yes#   192.168.41.5:24554   4099     172.16.24.1/32

CRUSADER#sh lisp instance 8189 ethernet server
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport


Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   8189     any-mac
               00:07:19  yes#   192.168.41.5:24554   8189     6c19.c07c.7722/48
```