Migrating AireOS Wireless Controller to Catalyst 9800 Controller for Cisco DNA Center Intent-Based Deployments, Cisco DNA Center 2.3.5.5

Table of Contents

1. About this documentation

This guide focuses on the steps and recommendations for migrating from an AireOS-based WLAN controller to a Catalyst 9800 WLAN controller. The procedure outlined in this document is applicable only for deployments that utilize the Cisco DNA Center for orchestration and automation. The supported deployment includes fabric-enabled wireless (FEW) for SDA and non-fabric wireless networks, which leverage Cisco Catalyst intent-based network automation.

2. Purpose

To serve as a reference document for migrating to the Catalyst 9800 wireless controller, the following procedures are detailed in this document:

- Cisco DNA Center intent level migrations.
- Onboarding the Catalyst 9800 controller onto Cisco DNA Center.
- Mobility pairing for seamless roaming with Inter-Release Controller Mobility (IRCM).
- Recommendation, explaining two different approaches for moving Access points to the Catalyst 9800 controller.

3. Prerequisites

Before starting the procedures described in this document, ensure the below prerequisites are taken care of.

- Catalyst 9800 wireless controller is brought up and discoverable from the Cisco DNA Center if Day N discovery would be used for onboarding or the C9800 can be added to the Cisco DNA Center inventory using the Day 0 PnP process.
- Ensure that routing is in place between the existing AP subnet and the C9800 management interface subnet.
- If the Guest Anchor was provisioned in a non-fabric deployment using Cisco DNA Center, ensure the Catalyst 9800 controller can reach the Anchor controller.
- Check the compatibility matrix to ensure Catalyst 9800 would be running an Inter-Release Controller Mobility (IRCM) compatible image with the AireOS controller.
- Ensure the APs that will be migrated are compatible with the Catalyst 9800 controller version. Please refer to the link for compatibility check.

- Plan to download the Catalyst 9800 based AP images locally in a TFTP server for the corresponding APs that will be migrated, these images can be pre-downloaded later to the APs using [WLAN poller](#) before migration reducing the downtime significantly.
- Ensure AP fallback is enabled in AireOS controller using CLI "*show network summary*".

4. Introduction

This document serves as a comprehensive guide to the migration procedure, focusing on the intricacies and best practices involved in transitioning from an existing AireOS-based wireless controller to Catalyst 9800 wireless controller for Cisco DNA Center intent-based deployments i.e., Cisco SD-Access fabric wireless and also nonfabric wireless deployment that has leveraged Cisco DNA Center network automation.

Any migration process must address the following essential considerations:

- Initiate the migration by targeting a smaller subset of the network, such as a single floor. If the initial migration proves successful, proceed to migrate additional floors gradually.
- Robust rollback mechanism to revert changes in the event that the migration does not proceed as anticipated. This ensures a safety net and minimizes potential disruptions.
- Recognize that the migration and evaluation phases may extend over days to weeks. Throughout this period, it is crucial to maintain seamless functionality in the wireless network, allowing for coexistence between the old and new components of the network.

The procedure and steps outlined in the document embody the essential considerations mentioned above as integral elements for the migration process.

Below is a sample topology depicting the network at a high level, where we have two floors of Building BGL18 (F1, F2) initially being managed by the AireOS controller and later one of the floor being migrated and being managed by the Catalyst 9800 controller. This results in a coexistence of both AireOS and Catalyst 9800 seamlessly working together, while you can evaluate and progressively migrate the other floors based on the evaluation.

The document is written by validating the scenario outlined with the following versions:
Cisco DNA Center: 2.3.5.5

AireOS: 8.10.183.0
C9800: 17.9.4a

However, the steps outlined in the document should work and are independent of the versions used.
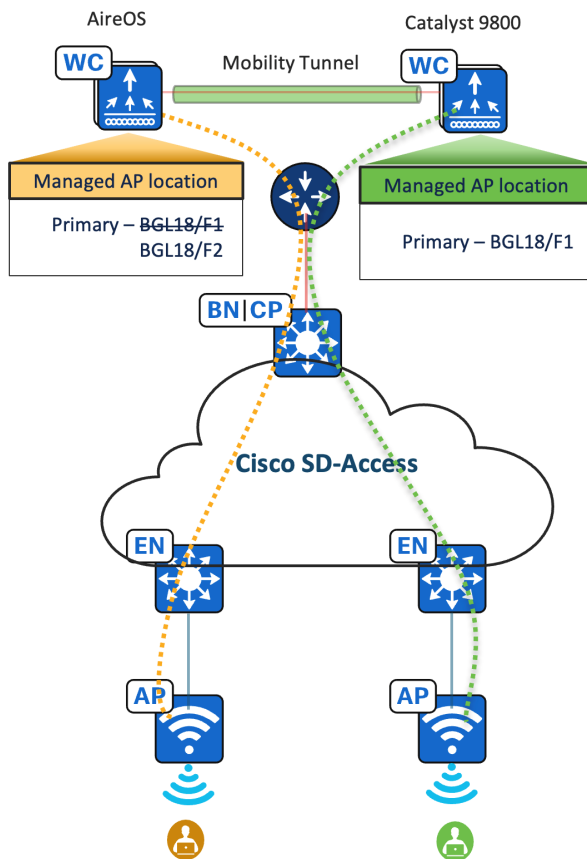

Figure 1 High level Network topology depicting migration scenario of SD-Access network

5. Wireless controller migration

5.1   Migrate the design elements

As we are migrating from AireOS to Catalyst 9800 wireless controller, which is based on two different architectures and with configuration model differences, a few intent-level changes need to be taken care of in Cisco DNA Center.

The design elements that are discussed in the below subsections need to be taken care of for all the Wireless network profiles in Cisco DNA Center, that are attached to the sites managed by the AireOS controller.

5.1.1 Custom AP profile

AP profile on the Cisco DNA Center has general AP settings such as SSH/Telnet, AP authentication, Security, Mesh, and many more. Cisco DNA Center doesn't allow to reuse of the existing custom AP profiles which were created for AireOS-based controllers to the C9800 controllers. As a part of the migration process, we need to replicate the custom AP profiles, if used with existing AireOS controllers, for the Catalyst 9800 controller.

Procedure

1. From the Global Site hierarchy navigate to the wireless page
   Design -> Network Settings -> Wireless

2. In the wireless page scroll down to find the AP Profile option, click Add "AP profile for IOS-XE"
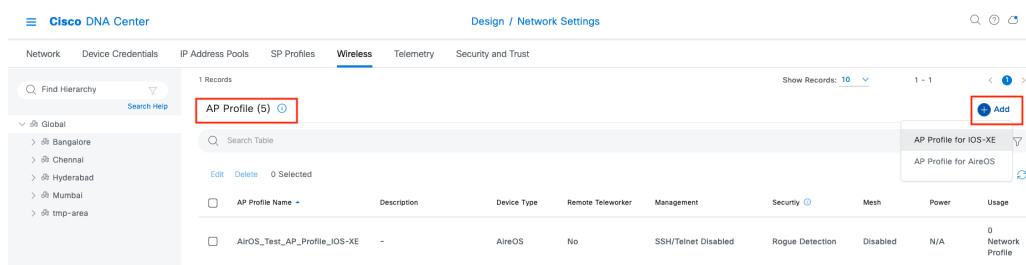

Figure 2 AP profile for Catalyst 9800 controller

3. Configure the required settings to replicate the existing Aire-OS based AP profiles used or you may even add additional features supported for Catalyst 9800 controllers.
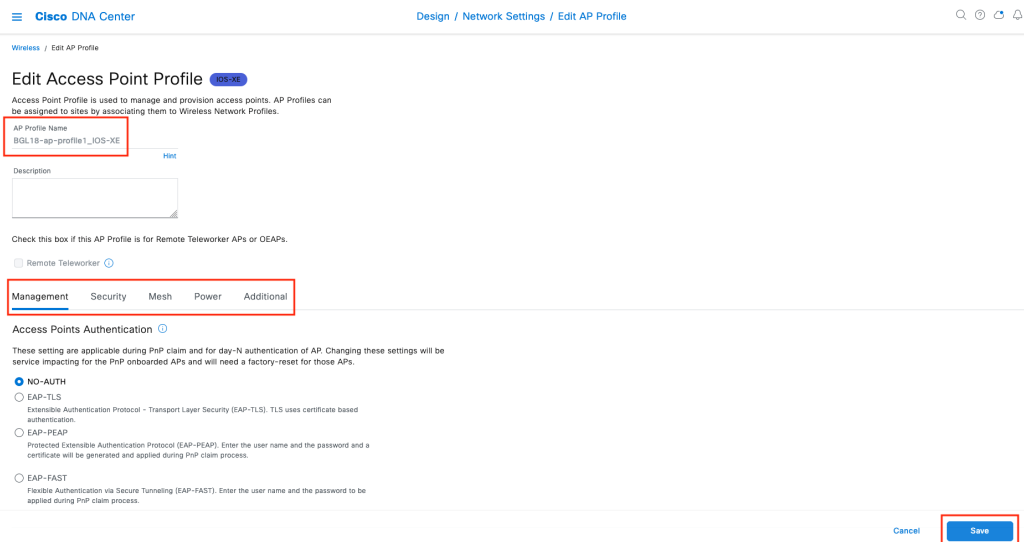
Figure 3 AP profile configuration for Catalyst 9800 controller

Repeat the above steps for the entire set of AP profiles used with AireOS based controller.

5.1.2 AP group, Flex group to site tag and policy tag migration

AP groups – AP groups in general are logical groupings of APs within a geographic area such as a building, floor, or remote branch office that share common configurations. AP groups are useful in a Cisco wireless network deployment because they allow network administrators to assign specific configurations to different groups of APs.

AP Profile – AP profiles consolidate the AP authentication settings, aWIPS, rogue management, and mesh settings in Cisco DNA Center. AP profiles allow you to manage and provision APs. Cisco DNA Center provides a default AP profile for both AireOS and IOS-XE based controller.

AP zone – An AP zone with Cisco DNA Center allows you to associate different SSIDs and RF profiles for a set of APs on the same site. You can create separate AP zones with a subset of SSIDs configured in the network profile.

Site Tag – Custom site tags can be provisioned using Cisco DNA Center, which helps in mapping an Area/Building/Floor to the site tag along with AP Profile.

Policy Tag – Policy Tag with Cisco DNA Center helps in creating a custom policy tag per floor along with an option to map an AP zone to it.

The AP group feature in Cisco DNA Center facilitates grouping a set of access points that share similar characteristics, such as WLANs broadcasted and AP profiles for AireOS controller deployment. These AP groups are then mapped to floors/buildings within the network hierarchy in the wireless network profile in Cisco DNA Center. However, with Catalyst 9800 Wireless controller, there is no AP group concept. Instead, similar functionality is achieved through the use of site tags and policy tags. Therefore, if AP groups were used in Cisco DNA Center for AireOS-based controllers, it's necessary to migrate them to Site tags and policy tags within the Cisco DNA Center wireless network profile.

AP group configurations on Cisco DNA Center have AP zone, AP profile, RF profile, and site mapping as parameters, whereas the Cisco DNA Center Site tag configuration takes care of mapping the AP profile to a set of sites. Policy tag helps to create a custom policy tag per floor along with AP zone mapping if any.

Flex connect group, which helps in grouping a set of flex sites that have to be part of a roaming domain. This option in Cisco DNA Center is applicable only for AireOS-based controllers, but the same functionality is taken care with the Custom site tag option where we can have this custom flex profile created along with site mapping.

Technical Note – *The flex options in Cisco DNA Center will appear only when you have flex SSIDs configured in the network profile.*

Below is a snapshot capturing the custom flex profile option for a Wireless network profile that has flex SSIDs part of it.
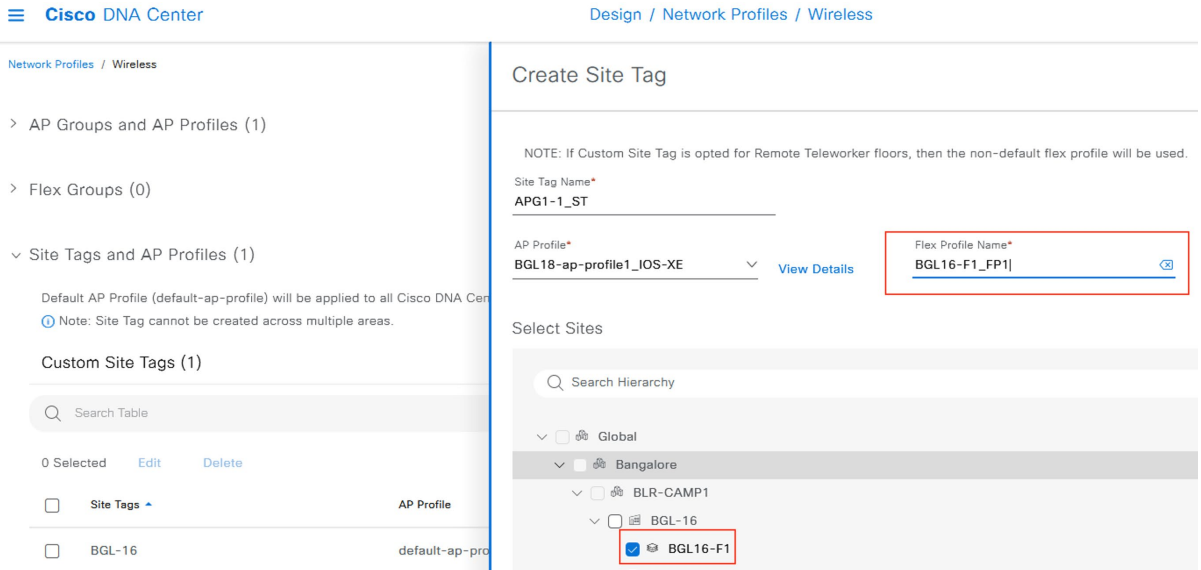
Figure 4 Custom flex profile along with site tag creation

Procedure

Below snapshot in Figure 5 depicts a scenario, wherein we have two AP groups (APG1-1, APG1-2) for same floor BGL18-F1 with different AP profile, AP zone and RF profile combinations. Below procedure explains, how we can migrate this to relevant site tag and policy tag in Cisco DNA Center.

Figure 5 Custom AP groups

1. For site tag creation we need, AP profile, flex profile (if any) and the site mapping. Create site tag say for example APG1-1_ST and map it with an AP profile that we had created for IOS-XE as part of the previous section (5.1.1). We can also create a new AP profile while mapping it to site tag.

   Design -> Network profiles -> Edit Network profile -> Advanced Settings -> Site tag and AP profiles -> Create custom site tag
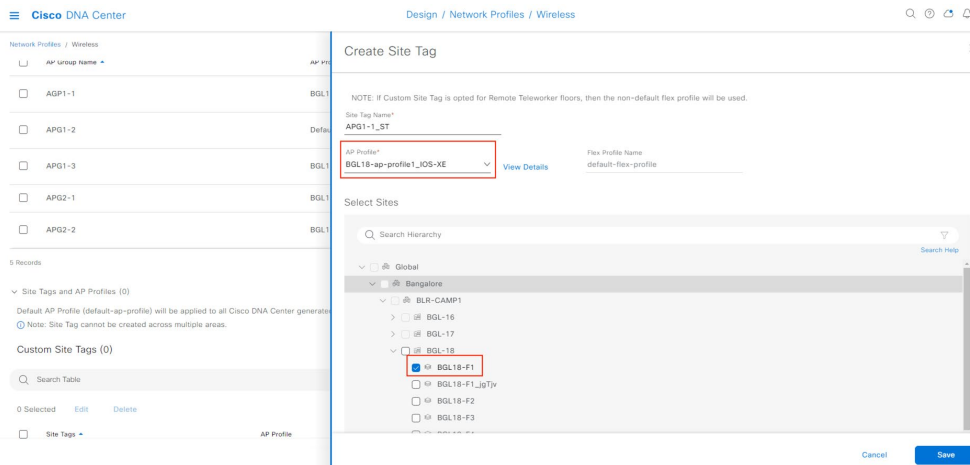
Figure 6 Custom site tag creation

Technical Note –
In the given example, there were two AP groups for the same floor, but we cannot have two site tag constructs for the same site with different AP profiles. We may need to consolidate to a single site.

While creating custom site tags along with flex profile, we may need to ensure the flex settings (like AP Native vlan, and client Vlan mapping) are common across the sites that we are grouping here. If this is not taken care of, will result in a Wireless controller provision error.

2. If the Custom AP groups were used along with AP zones, and if the Network admin wants to avoid Cisco DNA Center auto-generated Policy tags in the Catalyst 9800 controller we may need to create custom policy tags.

   Custom policy tags are per floor and per AP zone. In our example as per figure 5 we had two AP groups (APG1-1, APG1-2) with different AP zones for the same floor. When we create corresponding Policy tags to match it for Catalyst 9800 control, we need to have two Policy tags created.

   Create policy tag1 (APG1-1_PT1), with the respective AP zone and floor mapped to it. Similarly, repeat the process to create policy tag2 (say, APG1-1_PT2) mapped with its AP zone and same floor.

   Design -> Network profiles -> Edit Network profile -> Advanced Settings -> Policy tag -> Create Policy Tag
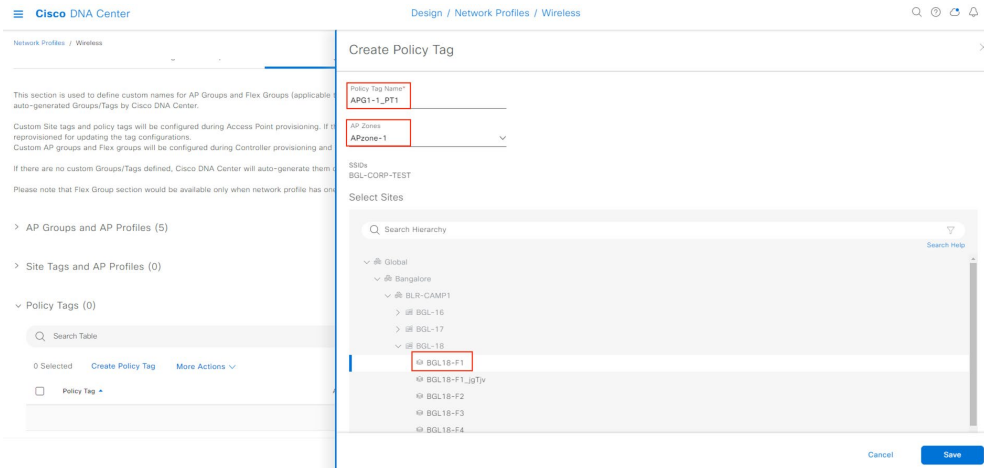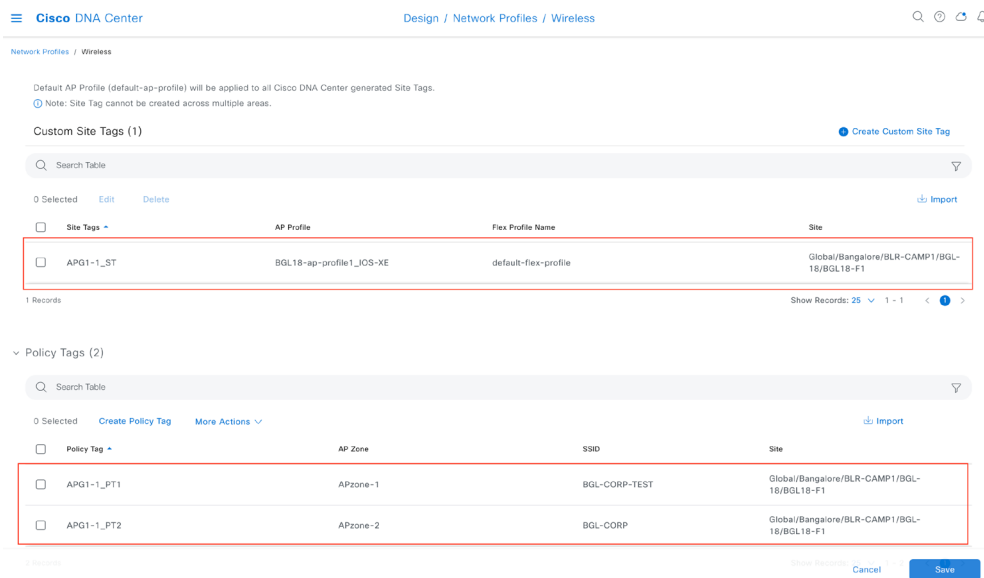
Figure 7 Custom Policy tag creation

Figure 8 Custom site tag and Policy tag view

5.1.3 Model config

Cisco DNA Center supports various wireless model config types, if a model config design was attached to the wireless network profile that was used with AireOS based controller, we may need to ensure this model config design is considered for Catalyst 9800 controller too.

5.1.4 Cli Template

Cisco DNA Center offers an interactive template hub that allows users to author CLI templates. These templates can be designed easily with predefined configurations using parameterized elements or variables. Once created, these templates can be used to deploy devices in one or more sites throughout the network.

Due to the configuration model differences between the AireOS controller and Catalyst 9800 wireless controllers, any CLI templates used for the existing AireOS controller will need to be converted for use with the Catalyst 9800 controller. This involves creating corresponding CLI templates specifically for the Catalyst controller.

After creating the CLI templates for the Catalyst 9800 controller, it is important to ensure that these templates are attached to the corresponding wireless network profile. This ensures that the correct configuration is applied to the wireless network when provisioning the Catalyst 9800 controller.

Technical Note –

[WLC config converter](#) *can be used to convert the specific set of configuration that is being provisioned through cli template for AireOS controller to Catalyst 9800 relevant configurations and then templatizing it in Cisco DNA Center .*

5.2 Onboard Catalyst 9800 controller to Cisco DNA Center

Onboard Catalyst 9800 controller to Cisco DNA Center, one may choose to onboard the controller to Cisco DNA Center using Day 0 PnP onboarding or as a Day N onboarding process with the Cisco DNA Center Discovery feature.

1. If Day 0 PnP onboarding was used, as a part of the claim process assign the Wireless controller to the same physical site as AireOS controller, also you will be able to configure the Wireless management IP, Subnet mask, Gateway, IP interface name, and optionally, VLAN ID.

   If day N Discovery was used to onboard the Catalyst 9800 controller, assign the Wireless controller to the same physical site as AireOS controller.

Technical Note – *The same physical site is being used to reuse the site-level network settings in Cisco DNA Center for the Catalyst 9800 controller.*

2. Ensure the telemetry configuration push is successful at this stage, and the telemetry connection to Cisco DNA Center is in an "UP" state.

Figure 9 Telemetry connection status

Technical Note – *If you have a pair of Catalyst 9800 to be onboarded as a single HA SSO pair, you can onboard both the controllers individually to Cisco DNA Center and then form an HA pair with the help of Cisco DNA Center. Here is a* config guide *on how to do it.*

3. Provision the Catalyst 9800 controller in Cisco DNA Center, as a part of the provisioning workflow the controller needs to be the primary controller managing a wireless site. To achieve this, we create a temporary site and attach it to a Wireless Network profile that is attached to the sites managed by AireOS controller. Ensure this temporary site is not managed by the AireOS controller before provisioning the Catalyst 9800 controller.
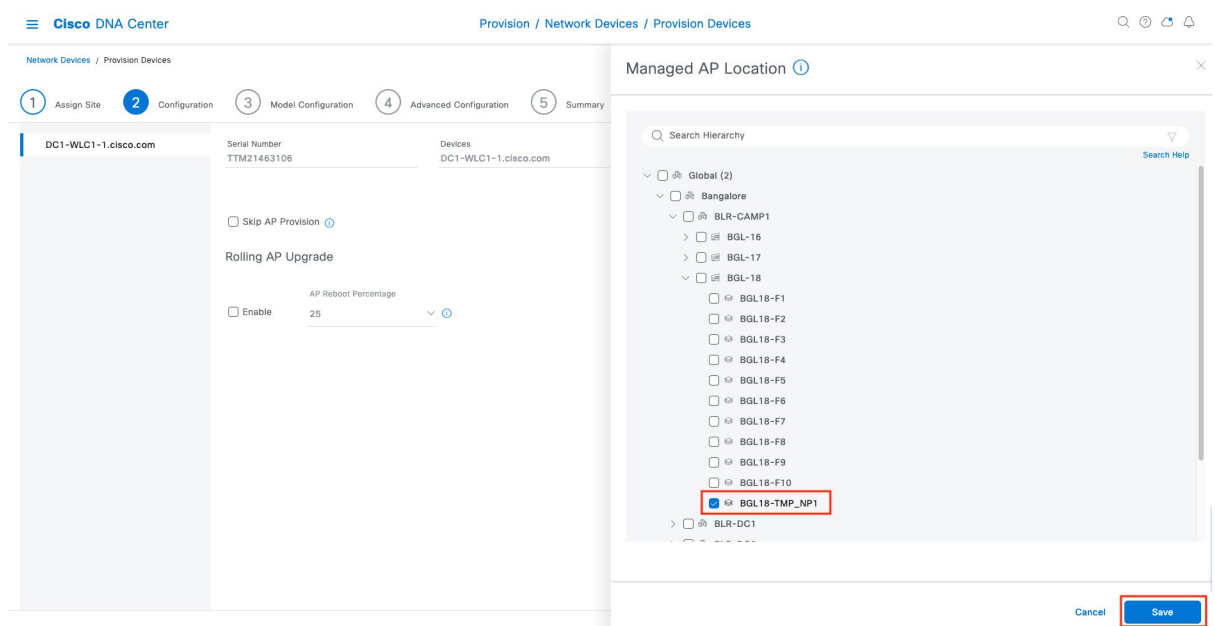
Figure 10 Provision Catalyst 9800 controller with temp site

If the APs are onboarded using local/AAA authorization ensure AP auth list is checked while provisioning the Catalyst 9800 Controller. We can reuse the existing Auth list that was created for AireOS based controller.
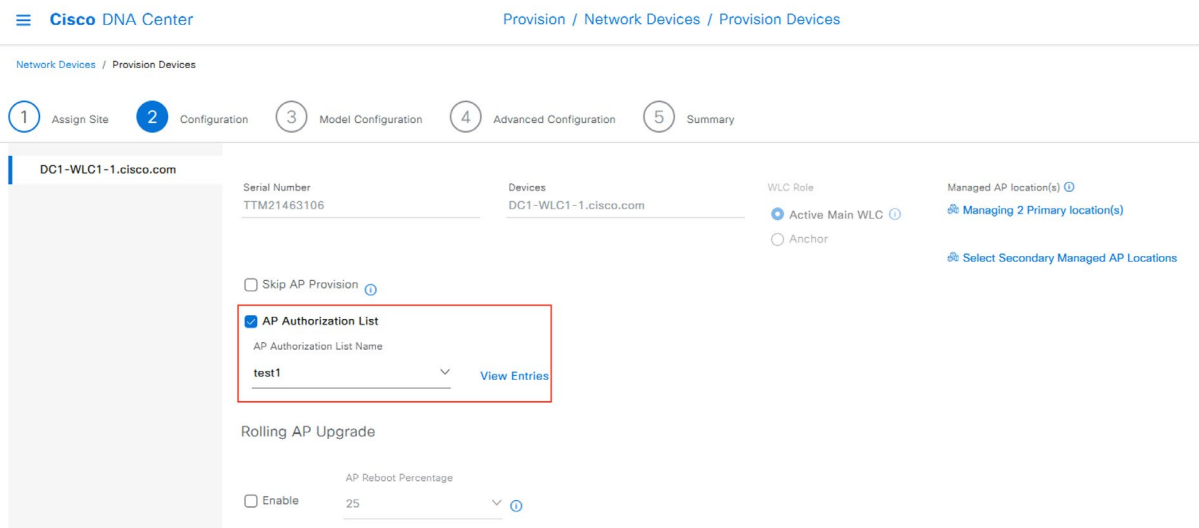
Figure 11 AP Authorization list provision

For nonfabric WLANs, the provisioning flow would also include the interface config associated with the WLAN.
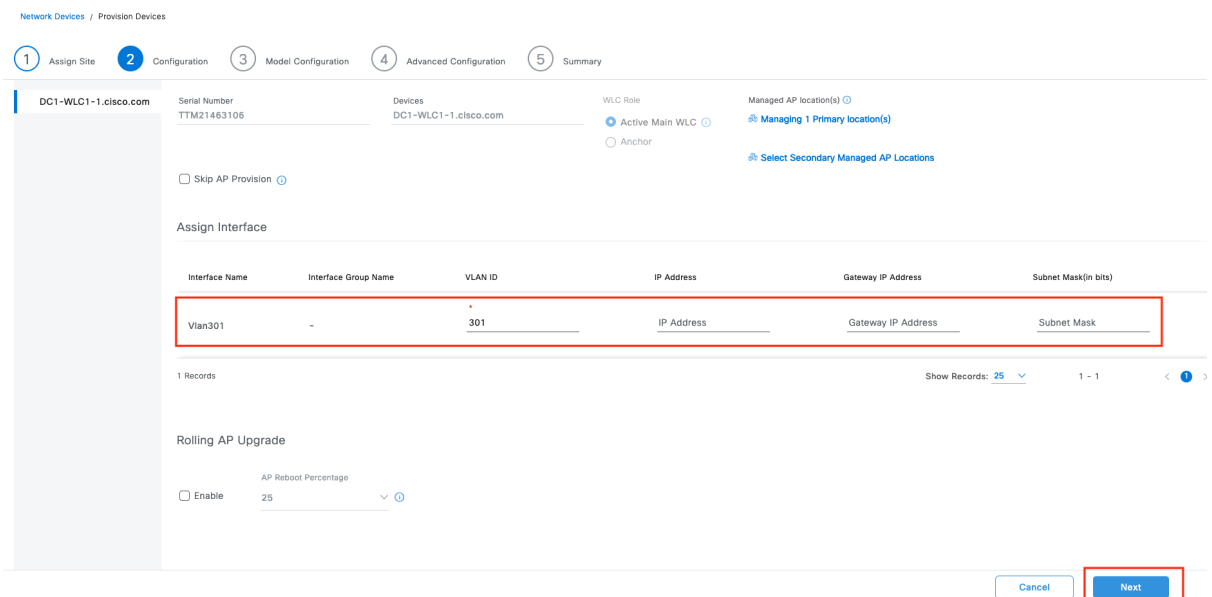
Figure 12 Provision Catalyst 9800 controller non Fabric flow

14

4. Once the provision of the Catalyst 9800 controller is successful, add the wireless controller to the Fabric. At this point, you will have both the AireOS and Catalyst 9800 controller part of the same Fabric site.
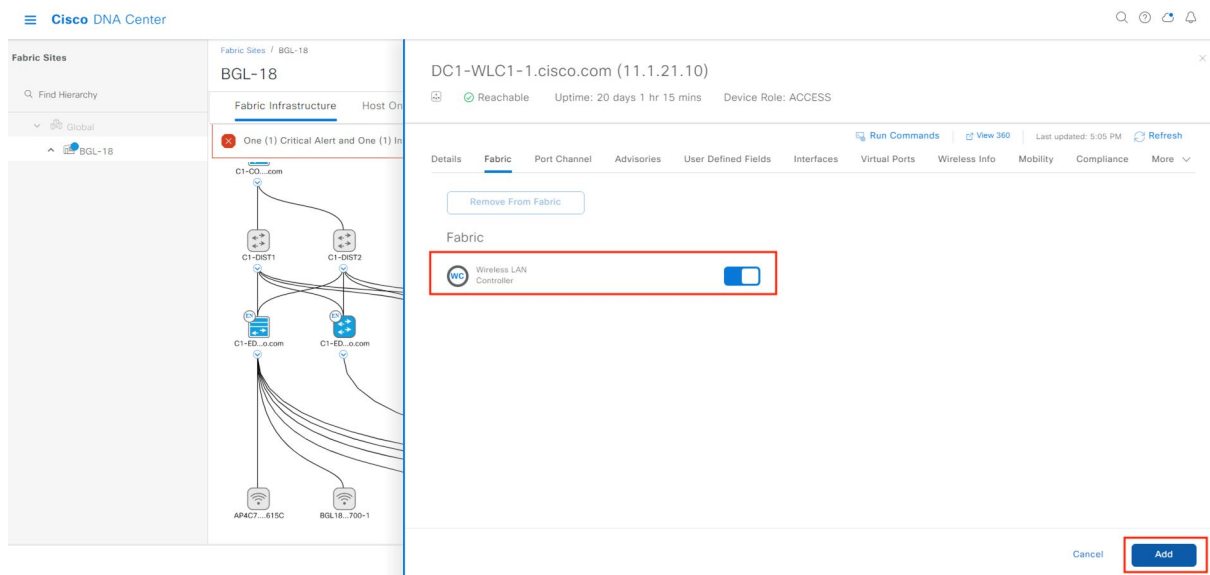
Figure 13 Add Catalyst 9800 controller to Fabric

5.3 Setup mobility tunnel between AireOS and Catalyst 9800 controller

When designing a migration between an AireOS deployment and the Catalyst 9800 wireless controller, it is common to adopt a phased approach. In this strategy, the access points are planned to be migrated in batches to the new Catalyst 9800 controller.

Cisco supports Inter-Release Controller Roaming (IRCM) between the Catalyst 9800 and AireOS wireless controllers. This feature is crucial in ensuring seamless mobility during brownfield and migration scenarios. It allows clients to roam smoothly between the two controllers without any interruption or loss of connectivity.

Cisco DNA Center supports the provisioning of mobility tunnel between the AireOS and Catalyst 9800 controllers.

1. Select the *AireOS controller-> Provision -> Configure WLC Mobility*
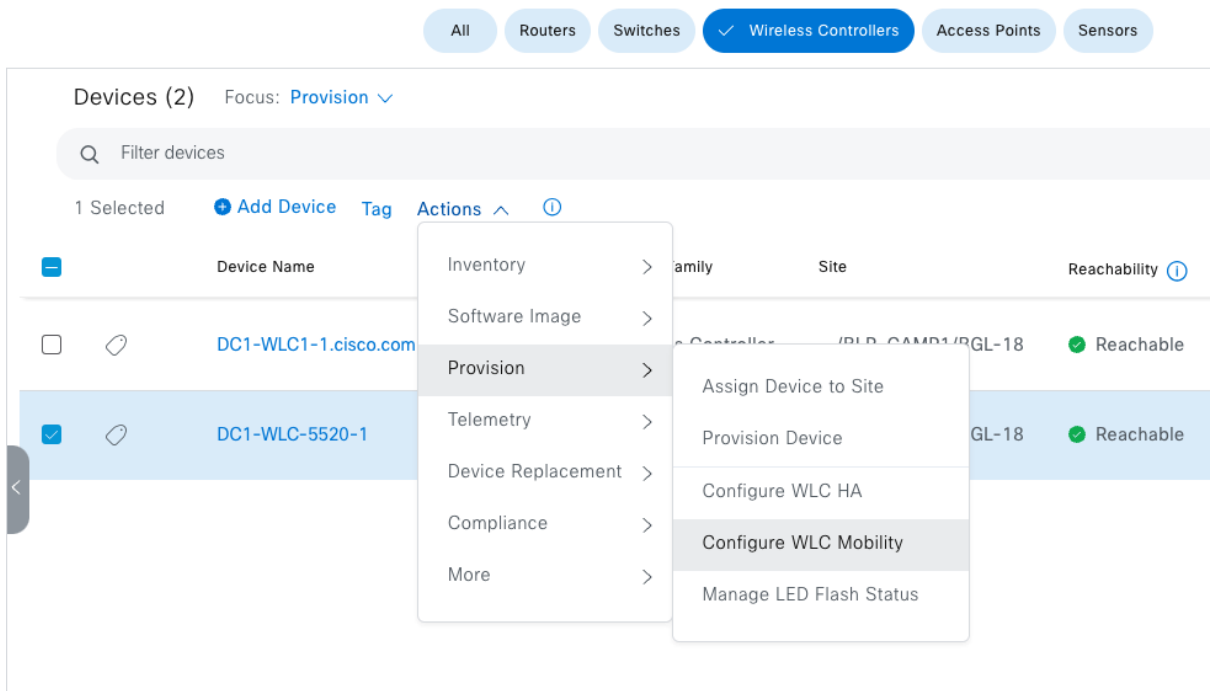
Figure 14 Mobility provision with AireOS

2. Provide a custom mobility group name, and RF group name and configure mobility to deploy the configuration to the AireOS wireless controller.
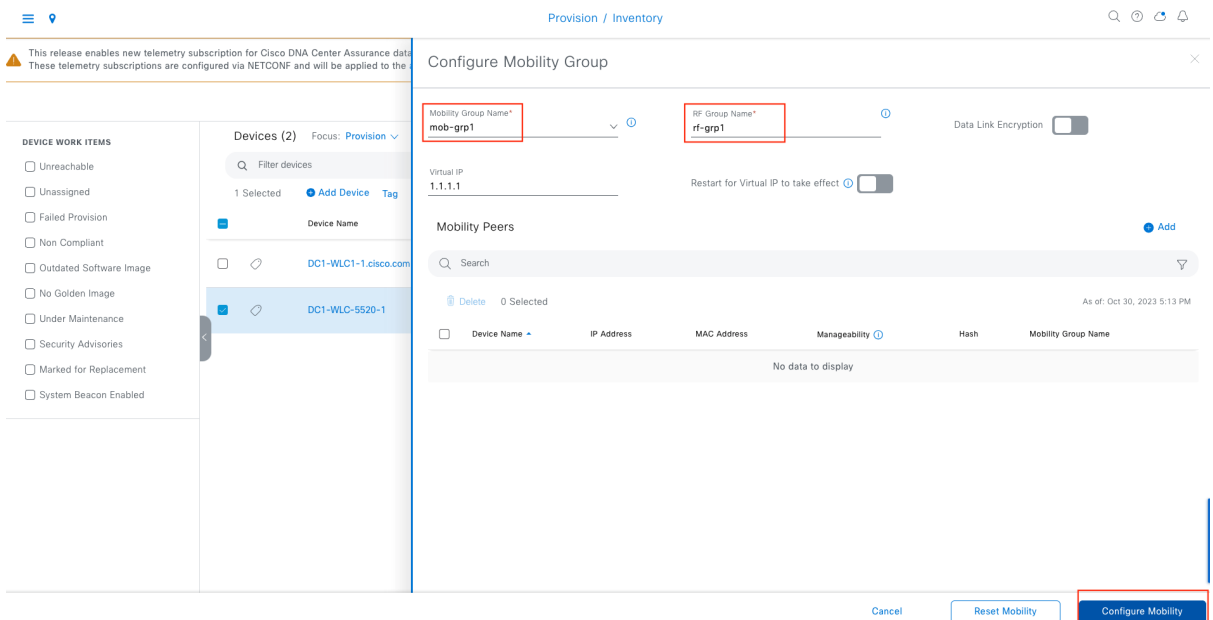
Figure 15 Mobility configuration with AireOS controller

3. Launch the mobility workflow group for Catalyst 9800 WLC, existing mobility group names are listed in the drop-down box. Select the mobility

16

group name configured with the AireOS controller, mob-grp1 in our example. RF group name will be auto-populated.
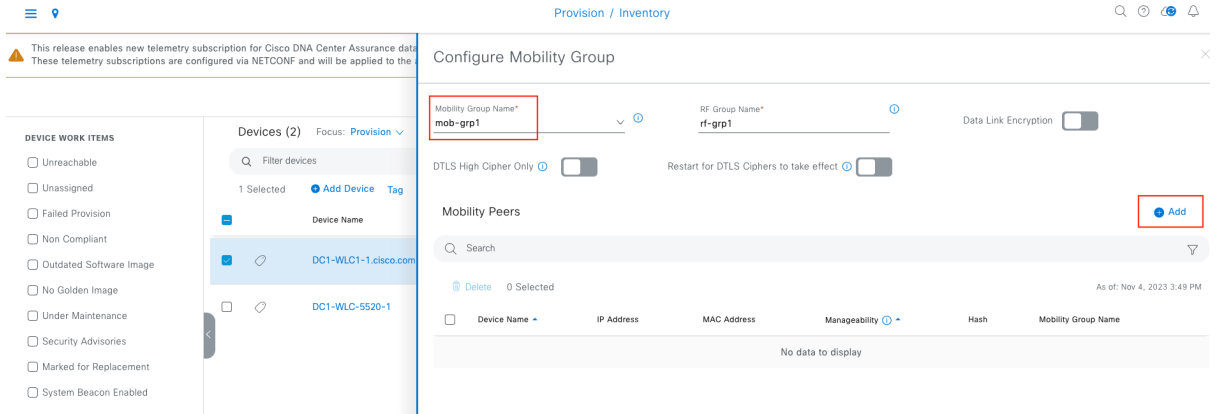
Figure 16 Mobility provision with Catalyst 9800 controller

Add the AireOS wireless controller as the peer controller depicted in *Figure 17* and save the configuration, followed by deploying the changes.
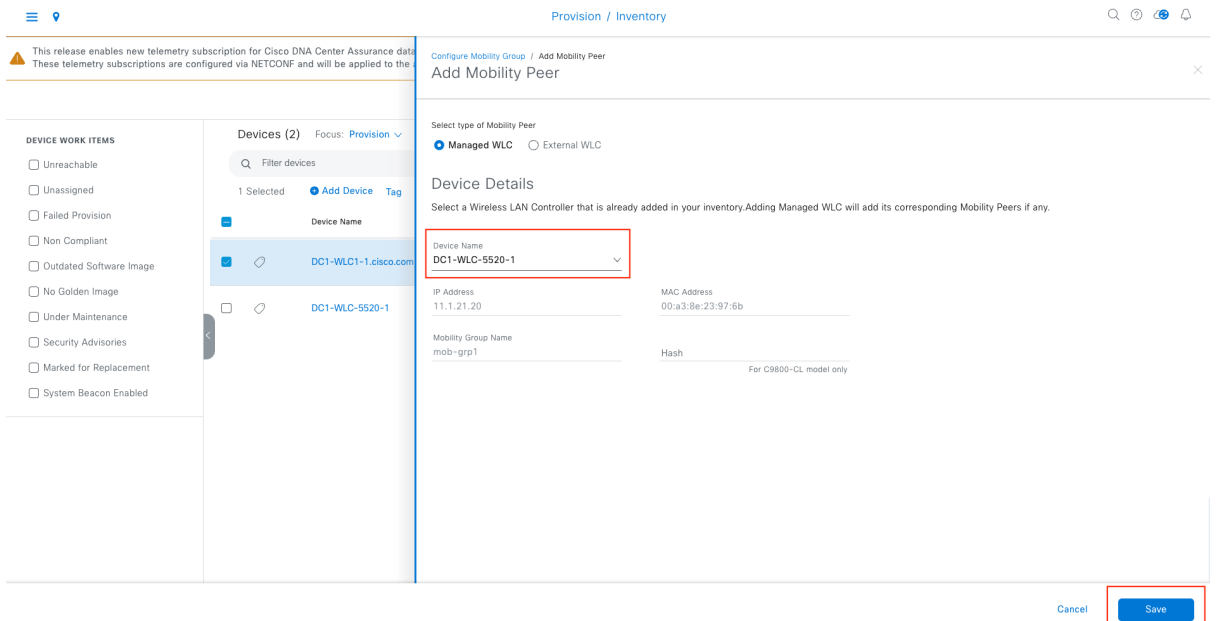
Figure 17 Mobility peer addition for Catalyst 9800 controller
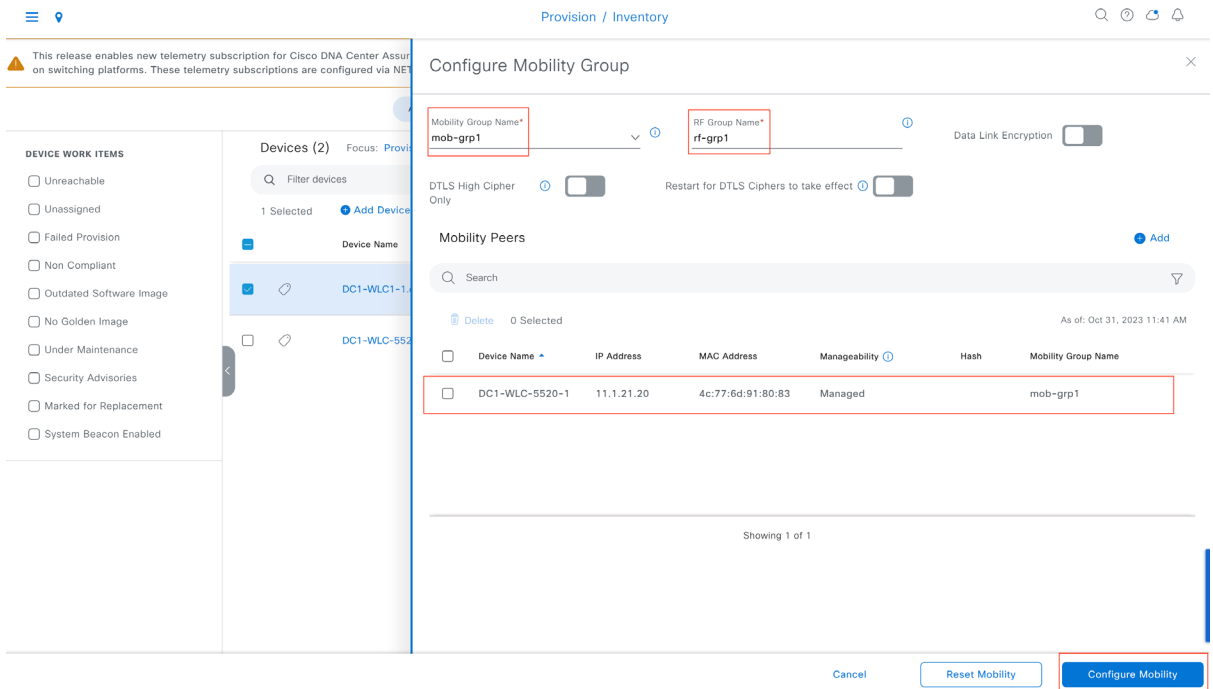
Figure 18 Mobility provision summary

The mobility tunnel provisioned by Cisco DNA Center has been successfully configured on the wireless controllers, as confirmed through the command runner output in *Figure 19*.
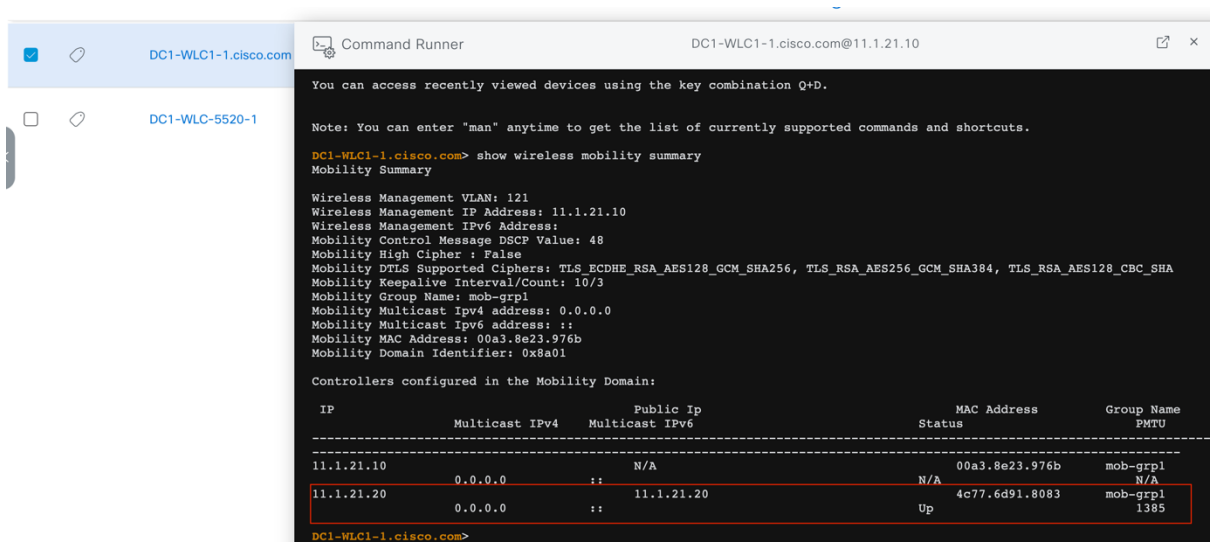
Figure 19 Mobility tunnel status, provisioned through Cisco DNA Center

5.4 AP movement

When migrating an access point from an AireOS-based wireless controller to a Cisco IOS XE-based controller, you have the flexibility to choose between two suggested approaches based on the network requirements.
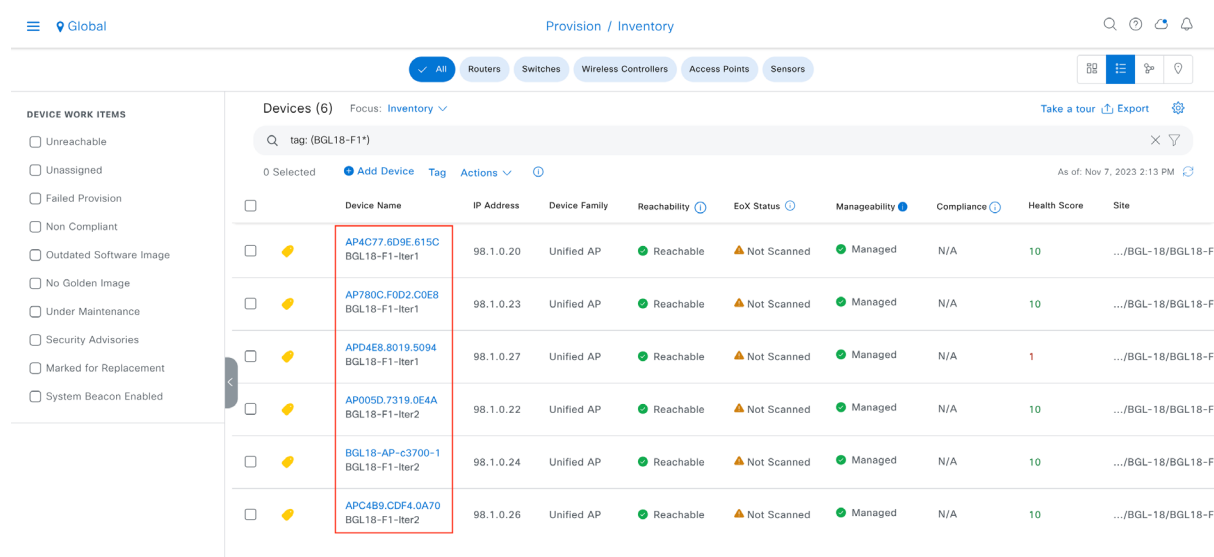
5.4.1 Iterative AP migration within a floor (least disruption)

As the wireless controllers are based on two different operating systems, achieving a hitless migration of access points is not possible. However, we have devised an approach to minimize disruption as much as possible.

Let's consider an example of a meeting room in an enterprise network that is served by two access points. In this scenario, the network administrator can choose to migrate one access point to the Catalyst 9800 wireless controller. Once successfully onboarded and serving clients, the other access points can be gradually moved from AireOS to the Catalyst 9800 controller.

This example can be extrapolated to an entire floor, where the network administrator can choose to move the access points in multiple iterations within that floor. This ensures network availability at any given point during the migration process.

1. Pick a floor that needs to be migrated and decide on the number of iterations and respective Access points part of each iteration. Tag the APs in Cisco DNA Center accordingly for easy filtering during migration.

Figure 20 Access points tagged with device tags identifying the iteration

2. Create a temporary floor (ex. *BGL18-F1_jgTjv* in Figure 21) in the same network hierarchy as the floor which you are trying to migrate.

Technical Note – *The interim purpose of this logical temp floor in this step is to mimic the actual floor, hence in case of any floor level overrides with Design -> Network Settings -> Wireless for the actual floor needs to be replicated for the temp floor too.*
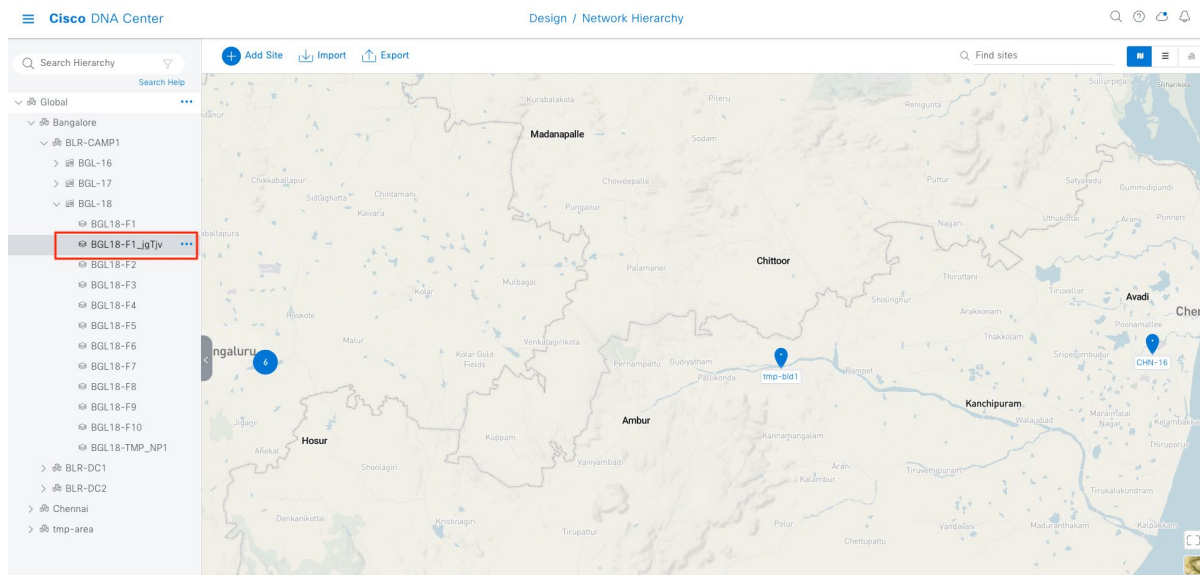

Figure 21 Temporary floor mirroring the actual floor that is being migrated

Check if this temp floor is mapped to the same wireless network profile that has the actual floor mapping, if not map this temp floor to the corresponding wireless network profile.
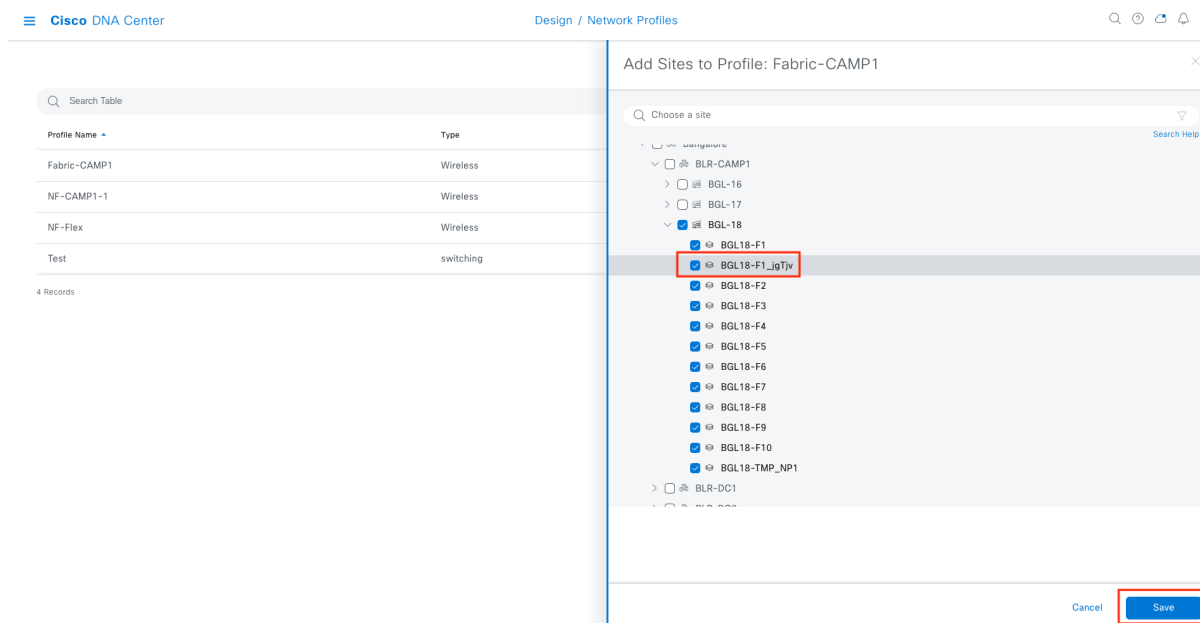

Figure 22 Temporary floor attached to the Wireless network profile

Ensure this temp floor is not managed by the AireOS controller in Cisco DNA Center. This can happen if the entire building was already primarily managed by the AireOS controller. If so, uncheck this temp floor from the primary managed locations of the AireOS controller and provision the AireOS controller for this change to take effect.

Technical Note – *Ensure this location is not secondary managed by an AireOS N+1 controller, as we don't support a location that is being primarily managed by Catalyst 9800 controller to be secondary managed by an AireOS controller.*
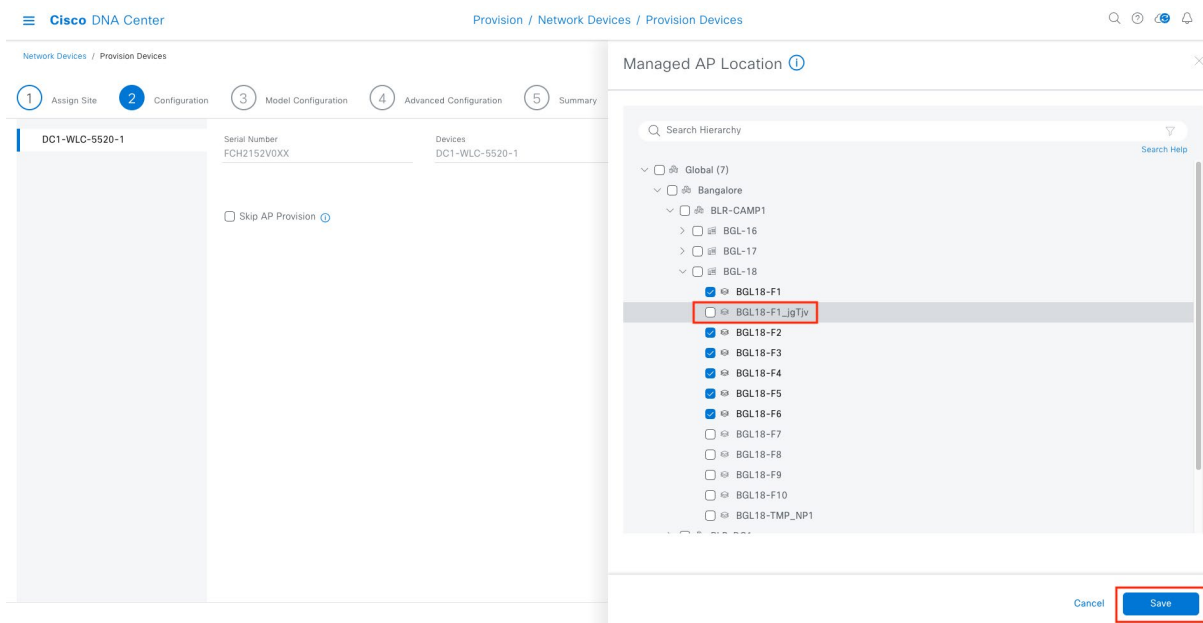

Figure 23 Temporary floor not being managed by AireOS controller

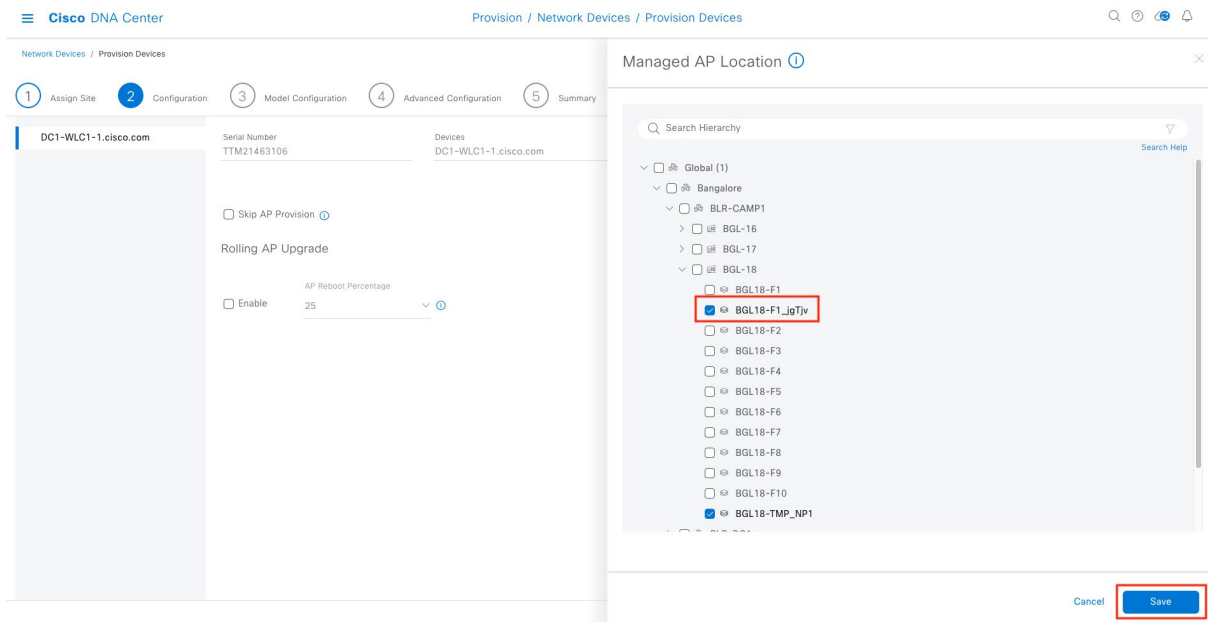3. Provision the Catalyst 9800 controller to primary manage this new temp floor.

Figure 24 Temporary floor being managed by Catalyst 9800 controller

Technical Note – *Make a note of the AP to RF profile and Ap Zone (if any) attached to each AP, as this information is lost once the APs are moved to the Catalyst 9800 controller.*

4. As you know, the first time the AP joins a controller based on a different OS, it will have to download the image and reload. This can be accelerated if we pre-download the Catalyst 9800 based image to the AP while it is associated with AireOS controller. We recommend doing this to make it as least disruptive as possible. There is a tool named WLAN poller hosted in Cisco Devnet, which can be used to pre-download the image to a set of APs using SSH protocol. Below are the recommended steps which can be followed.

   a) Once the WLAN poller tool is downloaded, there are few files that needs to be edited to match our requirement. Let's start with editing the config.ini file. The below snapshot highlight captures the changes that has been done to the existing config.ini file. Either, we are commenting or uncommenting the default values and also updating the uncommented lines with respective required values.

```
[General]
# Label
label = test

; active value should be based on 1 == AiroS WLC, 2 == eWLC and False for failure.

;wlc_type: 1

; config global mode for WLC and AP connection: "ssh" or "telnet"
mode: ssh
ap_mode: ssh

; set global WLC credentials
;wlc_user: wow123
;wlc_pasw: Pass_123
;wlc_enable: Pass_123

; set global AP credentials
ap_user: admin
ap_pasw: Pass_123
ap_enable: Pass_123

; syslog address
syslog_server: self
; log file mode: one file per "day" (default) or one file per timestamp "time":
;log_fo_file_mode: time

; set transfer mode (tftp or ftp, default is tftp)
;transfer_mode = tftp

; tftp
tftp_addr: 19.1.1.200
tftp_addr_v6: self
tftp_path:

; ftp
;ftp_addr: self
ftp_path:
ftp_user: <ftp_user>
ftp_pasw: <ftp_pasw>

; FEATURES
; enable data-poller
poller_enable: True
; radio event collection
event_enable: False
; dfs trace
dfstrace_enable: False

; ap file system checks (WARNING: recover will force IOS image download and AP reload)
ap_fs_check: False
ap_fs_recover: False

; IOS AP certificate check
ap_cert_check: False

; WLC config backup and ap crash file collection (default is disabled)
;wlc_config_backup: True
;collect_ap_crash: True
;collect_supp_bundle: True

; data poller command lists
cmdlist_wlc = cmdlist_wlc.txt
cmdlist_ewlc = cmdlist_ewlc.txt
cmdlist_ios = cmdlist_ios.txt
cmdlist_cos = cmdlist_cos.txt
cmdlist_cos_qca = cmdlist_cos_qca.txt
cmdlist_cos_bcm = cmdlist_cos_bcm.txt

# working directories
poller_root = ./data/
#syslog_root = ./syslog/
#tftp_root = ./tftpboot/
archive = ./archive/
;logs = ./logs/
```

Annotations:
- *Commented out, as not performing any operation in WLC* → ;wlc_type: 1 and WLC credentials
- *AP SSH login credentials needs to be added* → set global AP credentials
- *TFTP server that would be used for image copy from AP* → tftp section
- *commented out, as FTP is not used* → ;ftp_addr: self

Figure 25 WLAN Poller config.ini file changes part1

```
ap_fs_recover: False

; IOS AP certificate check
ap_cert_check: False

; WLC config backup and ap crash file collection (default is disabled)
;wlc_config_backup: True
;collect_ap_crash: True
;collect_supp_bundle: True

; data poller command lists
cmdlist_wlc = cmdlist_wlc.txt
cmdlist_ewlc = cmdlist_ewlc.txt
cmdlist_ios = cmdlist_ios.txt
cmdlist_cos = cmdlist_cos.txt
cmdlist_cos_qca = cmdlist_cos_qca.txt
cmdlist_cos_bcm = cmdlist_cos_bcm.txt

# working directories
poller_root = ./data/
#syslog_root = ./syslog/
#tftp_root = ./tftpboot/
archive = ./archive/
;logs = ./logs/

; AP name filter
;ap_name_filter =

; location filter
;loc_filter: False          ◄─────────────────  Commented out Location filter, as we are using AP
;loc_list: location1,location2                      list updated in CSV file

; concurrent connections (default: 30)
;concurrent_conn: 10

; timeout when waiting for AP commands to execute
ap_timeout=120
# use UTC timestamps
# utctime = True
# per-file timestamp
#  False (default): one file per device per day, in time based directory structure
#  True           : one timestamped file per run, in root data directory
# file_timestamp = True

; WLC sections must be named as [WLC-<wlcname>]
;[WLC-1]
;active: False          ◄─────────────────  Commented out WLC details section
;ipaddr: 11.1.21.20
;mode: ssh

;[WLC-2]
;active: False
;ipaddr: <wlc-ip-addr>
;mode: ssh

[AP-CSV]
aplist: aplist.csv          ◄─────────────────  aplist.csv file part of theWLAN poller bundle is updated with AP IPs

;[AP-List]
;<ap-name>: <ap-ipaddr>

;rq
[DataExport]
;textfile_out = True
;dx_enable = True
;dx_srv_addr = localhost
;dx_srv_port = 5672
;dx_srv_user = guest
;dx_srv_pasw = guest

[FTS]
username:
password:
path:
```

Figure 26 WLAN Poller config.ini file changes part2

b) Next step is to edit the cmdlist_* (except cmdlist_wlc and cmdlist_ewlc) files that are actually used for executing the commands at the Access points. Delete the existing set of commands or comment it out with # and add the below command.

archive download-sw /no-reload tftp://19.1.1.200/<apimage>

Please replace the tftp server IP with your tftp server, and the ap image depends on the actual AP which is in your network. You can get this mapping with *"show ap bundle all"* in AireOS controller.

Below would be an actual command for C9120 Access point.
archive download-sw /no-reload tftp://19.1.1.200/ap1g7

   c) As a final step, run the wlanpoller.exe that is part of the bundle. The
      executable shows the progress in the console, and logs are captured in data
      and logs folder.

5. Export the map of the particular floor at *Design-> Network Hierarchy -> Floor
   -> Export Maps*

Technical Note – *While we move the Access Points to a temp floor, exporting and
preserving it ensure we don't lose the AP positioning. This exported file can be imported
again to the same floor, once the APs are back to the actual floor later.*
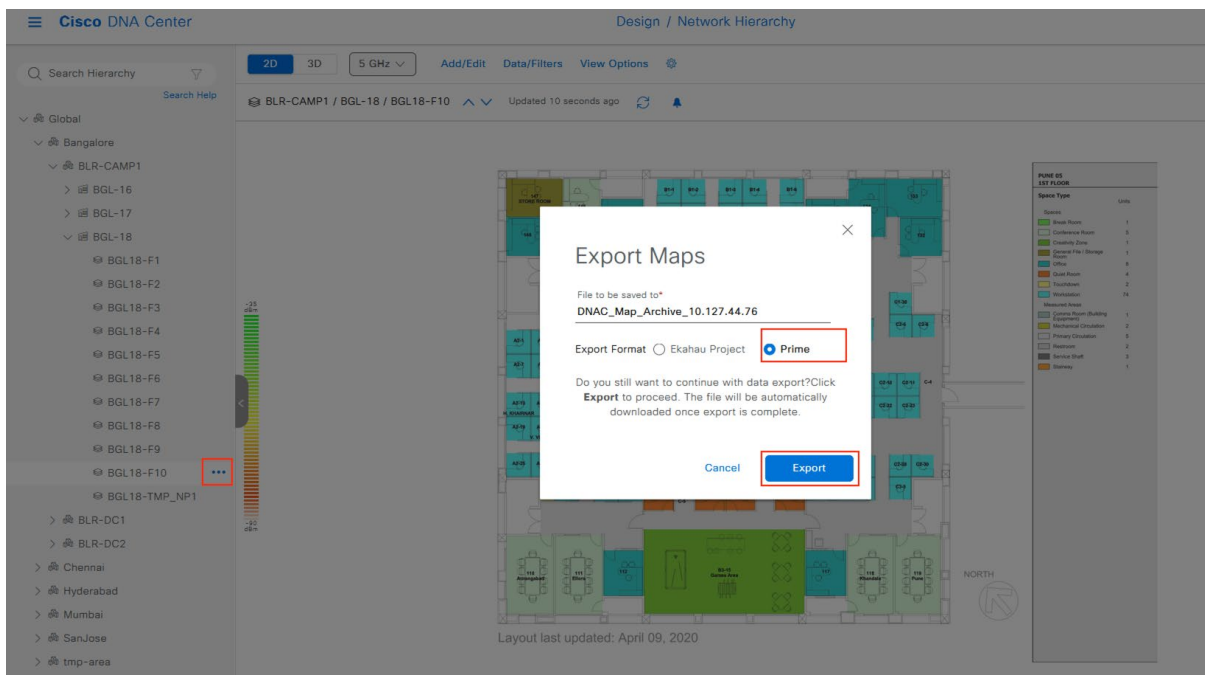
Figure 27 Floor map exported in prime format

6. Config AP workflow in Cisco DNA Center is used to configure the Catalyst
   9800 controller as the primary WLC. Pick the APs marked for iteration 1 in
   the floor that we are migrating and provision the same using config ap
   workflow.
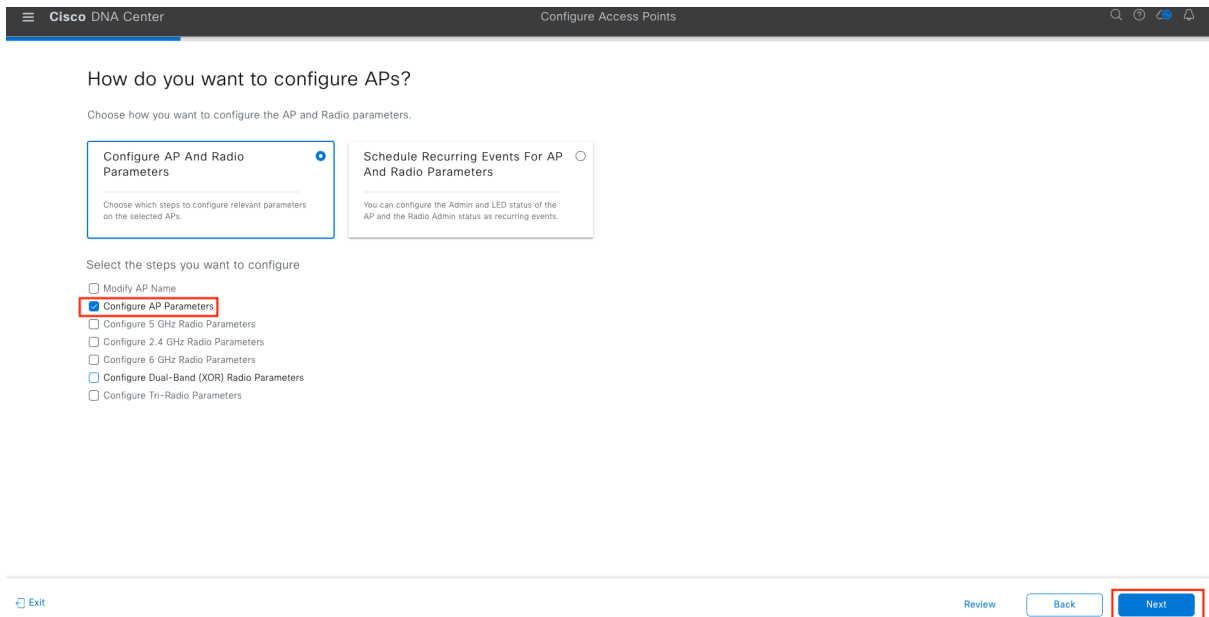
Figure 28 Configure Access point workflow
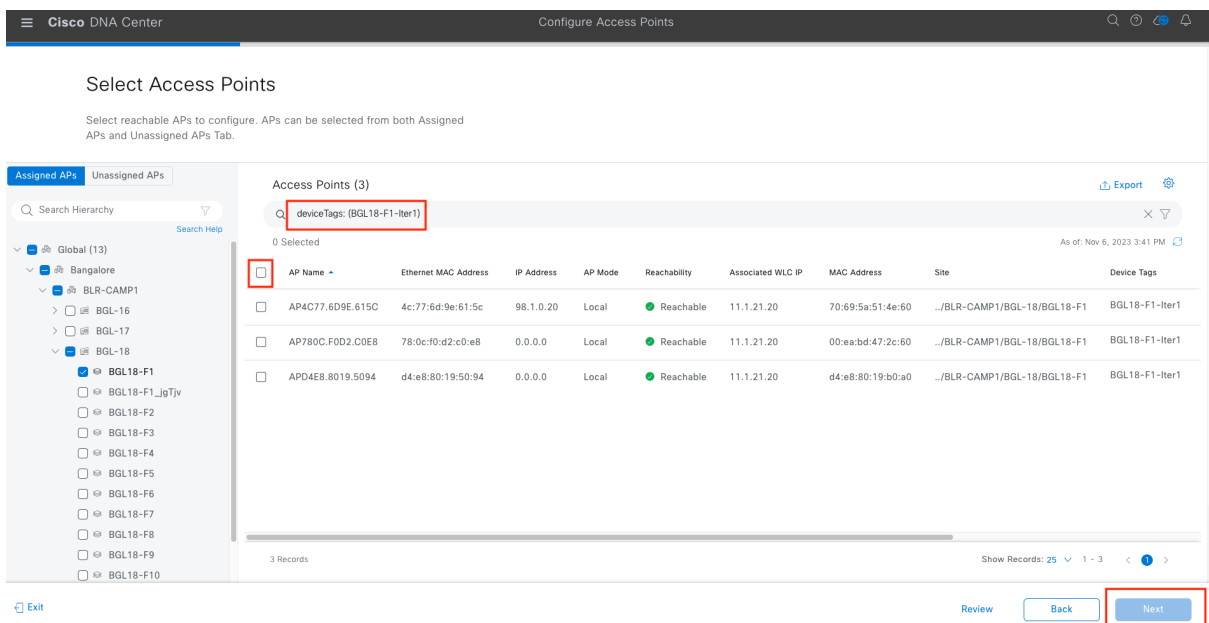
Figure 29 Access points filtered with device tag part of the first iteration
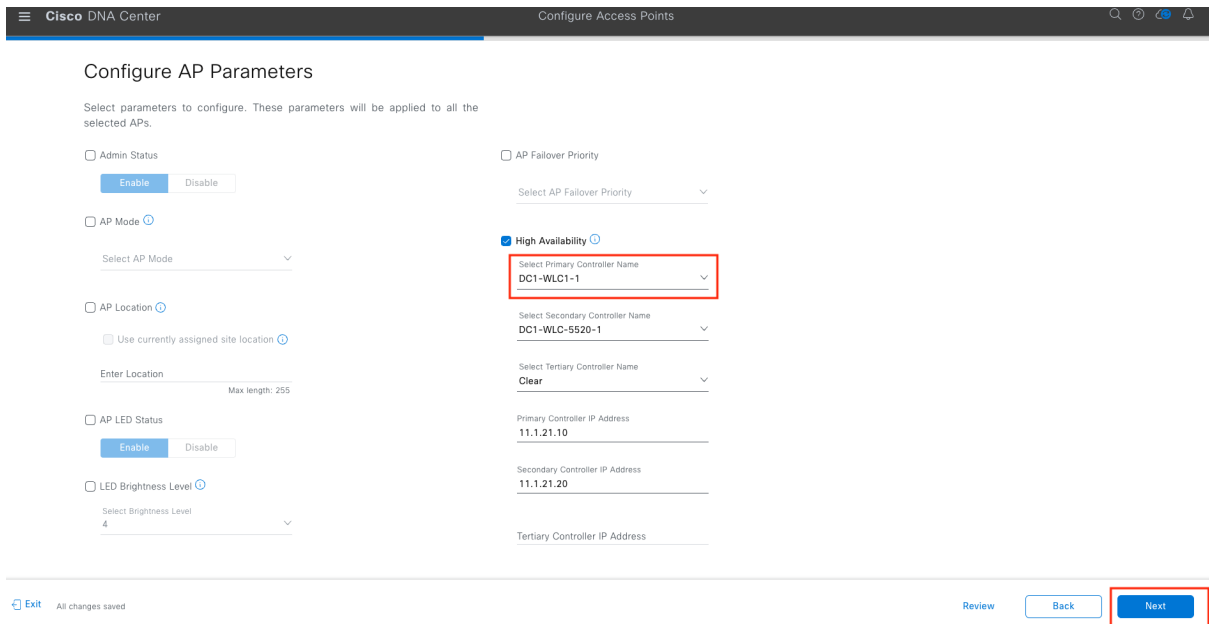
Figure 30 Catalyst 9800 controller being configured as Primary controller

7. Once all the APs part of the first iteration have joined the Catalyst 9800 controller, provision this set of APs to the temp floor managed by the Catalyst 9800 controller.

Technical Note – *We can provision a maximum of 300 APs one time, if the number for the iteration exceeds we may need to split the provision accordingly.*

Figure 31 APs part of the first iteration joined Catalyst 9800 controller
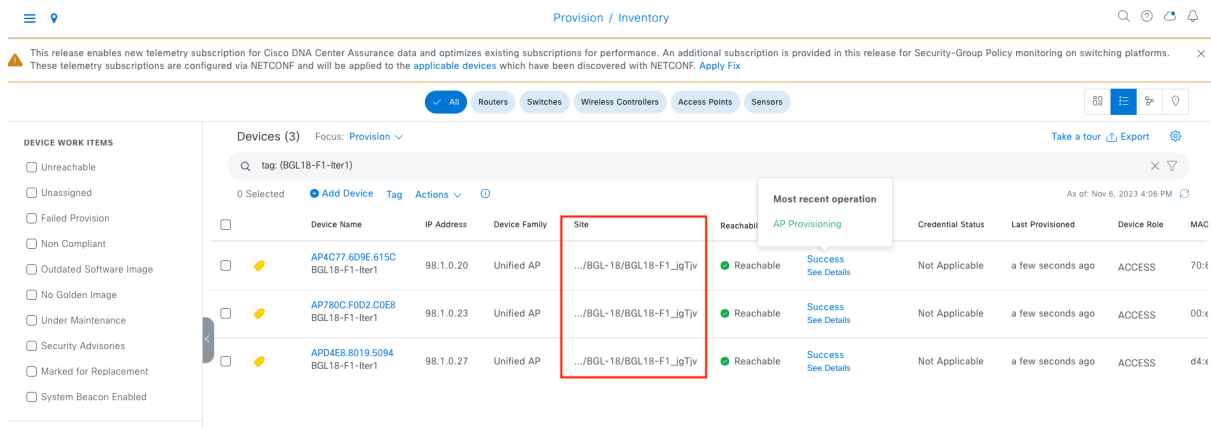
Figure 32 APs part of first iteration provisioned successfully to temp floor

8. Repeat the steps 4-8 detailed above for the remaining iterations, and once all the APs part of that floor is moved temp floor. Provision the AireOS controller to not manage this actual floor, also ensure this actual floor is not secondary managed by an AireOS N+1 controller if any.
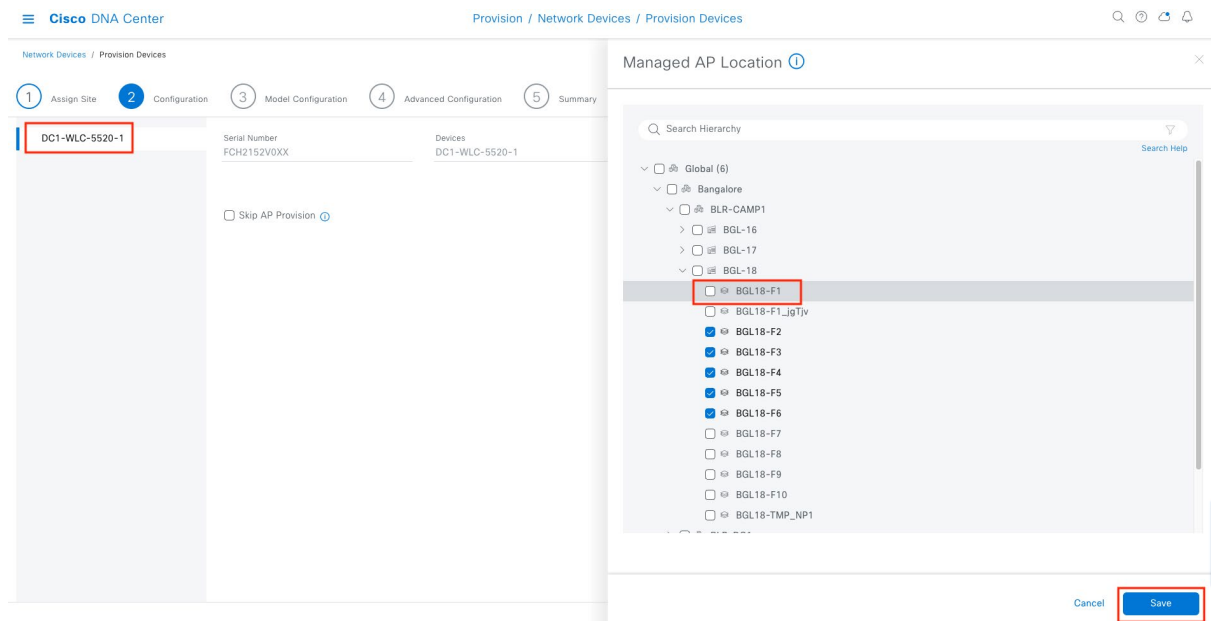

Figure 33 AireOS controller not managing the actual floor
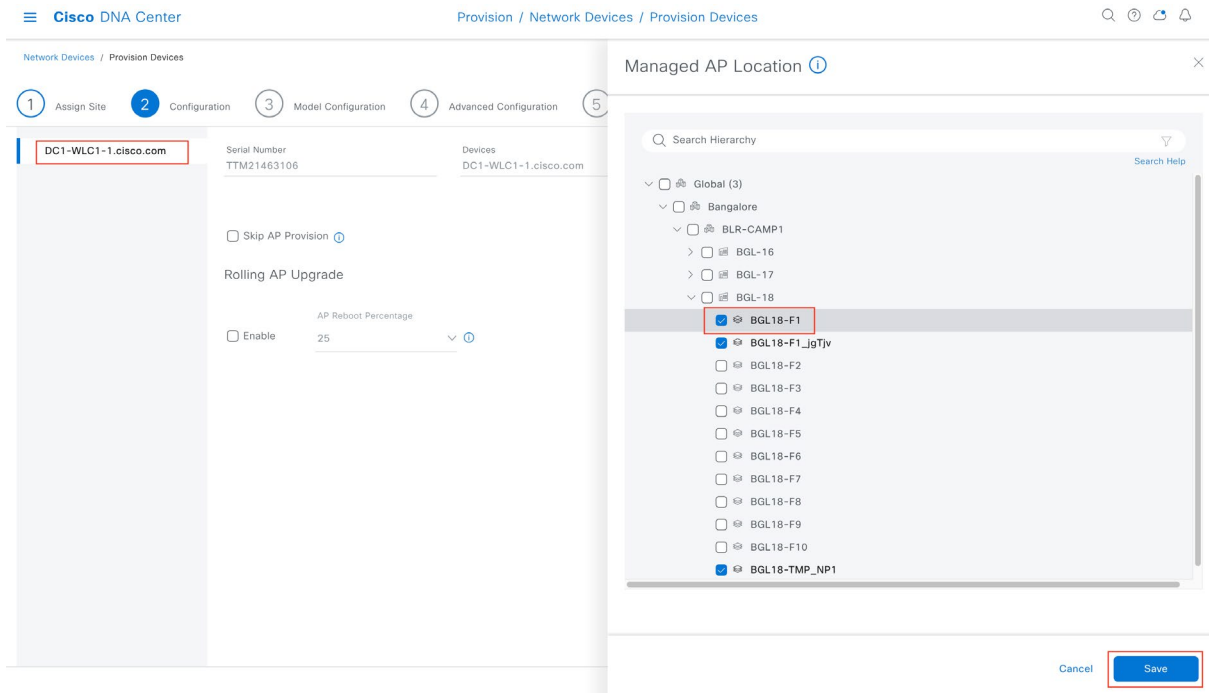
9. Provision the actual floor to be managed by Catalyst 9800 controller.

Figure 34 Actual floor being managed by Catalyst 9800 controller

10. Provision the Access points to the actual floor in the same iterative way.

Technical Note – *we do this because the temp floor was always meant to be a temporary positioning as we cannot have a single floor being managed by two wireless controllers in Cisco DNA Center . Also, there could be maps with AP positioning, custom site tags, and policy tags associated with the actual floor. Hence, we recommend always moving back to the actual floor where the AP was attached before migration*.

Figure 35 APs part of the floor BGL18-F1 is successfully migrated to Catalyst 9800 controller

11. Actual floor is migrated and managed by Catalyst 9800 controller, now we can import the map that was exported in step 5, that way we retain the AP positioning post migrating the floor.

Technical Note – *Import is always at the global level, but as the imported file has details of only one floor that we exported, Cisco DNA Center ensures other floors AP positioning is untouched.*
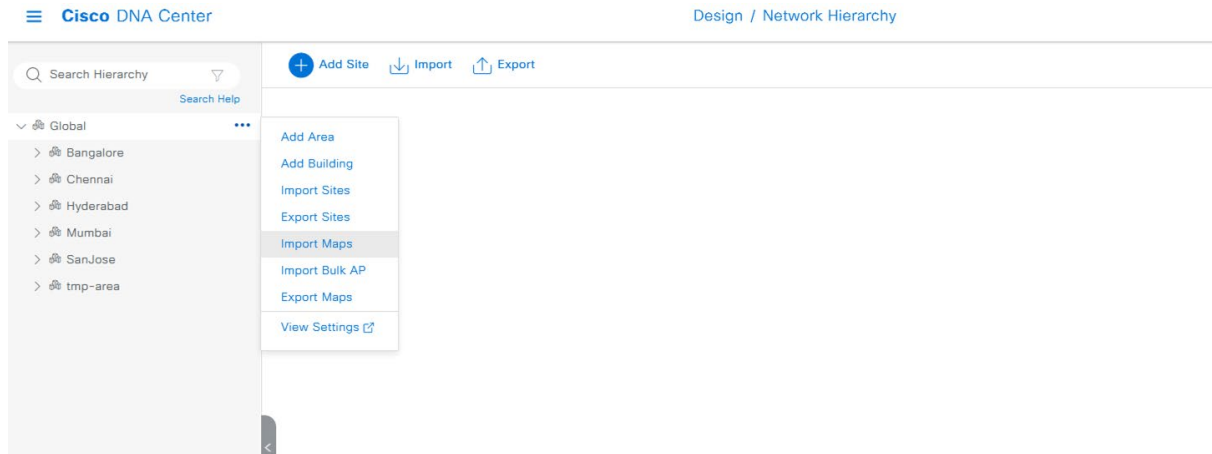

Figure 36 Map being imported back at Global level

12. Remove the temp floor from the site hierarchy, as all the APs have been moved back to the actual floor which is now being managed by the Catalyst 9800 controller.

13. As config Access point workflow was used to override the primary WLC of the APs, we may need to revert back by using the workflow again to let it use site inherited parameters.

Figure 37 Config AP workflow to revert the WLC HA parameters

14. Repeat the steps 1-13 for other floors one by one. For the last floor that's being migrated while provisioning the AireOS controller to not manage that particular floor, you may need have some dummy floor managed by the AireOS controller as at least one floor has to be managed for the provisioning to succeed.

5.4.2 Floor-wise migration of APs to a new controller

You may decide to take a hit to migrate the entire set of Access points in a floor to the Catalyst 9800 controller without bothering about the disruption and hassles of steps described in the previous section. Below are the steps recommended if you wish to follow this approach.

1. The first step is to pick the floor that you want to migrate to Catalyst 9800 controller.

2. As you know, the first time the AP joins a controller based on a different OS, it will have to download the image and go for a reload. This can be accelerated if we pre-download the IOS-XE-based image to the AP while it

is associated with the AireOS controller. We recommend doing this to make it as least disruptive as possible. There is a tool named [WLAN poller](#) provided by Cisco, which can be used to pre-download the image to a set of APs using SSH protocol. Please check Section 5.4.1 -> Step 4 of this document for more details on this.

3. Now, the APs are ready to be moved to the Catalyst 9800 controller. We can use the Cisco DNA Center config AP workflow to configure the Access points with the Catalyst 9800 controller as the primary controller.
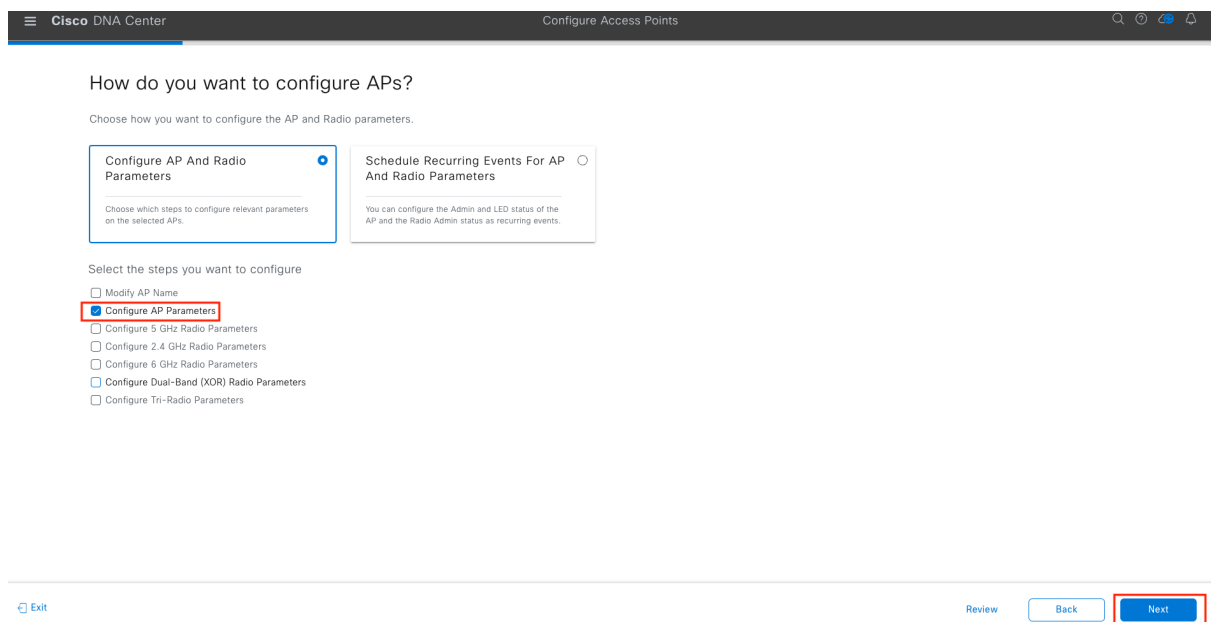
Figure 38 Configure Access point workflow
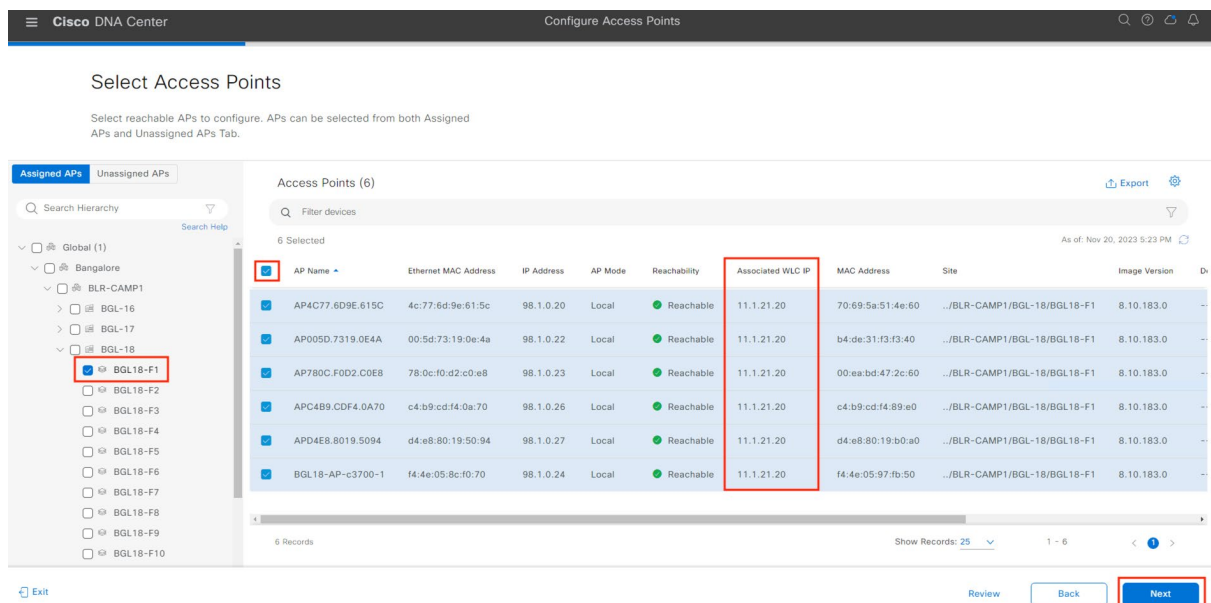
Figure 39 APs part of the floor BGL18-F1 is selected
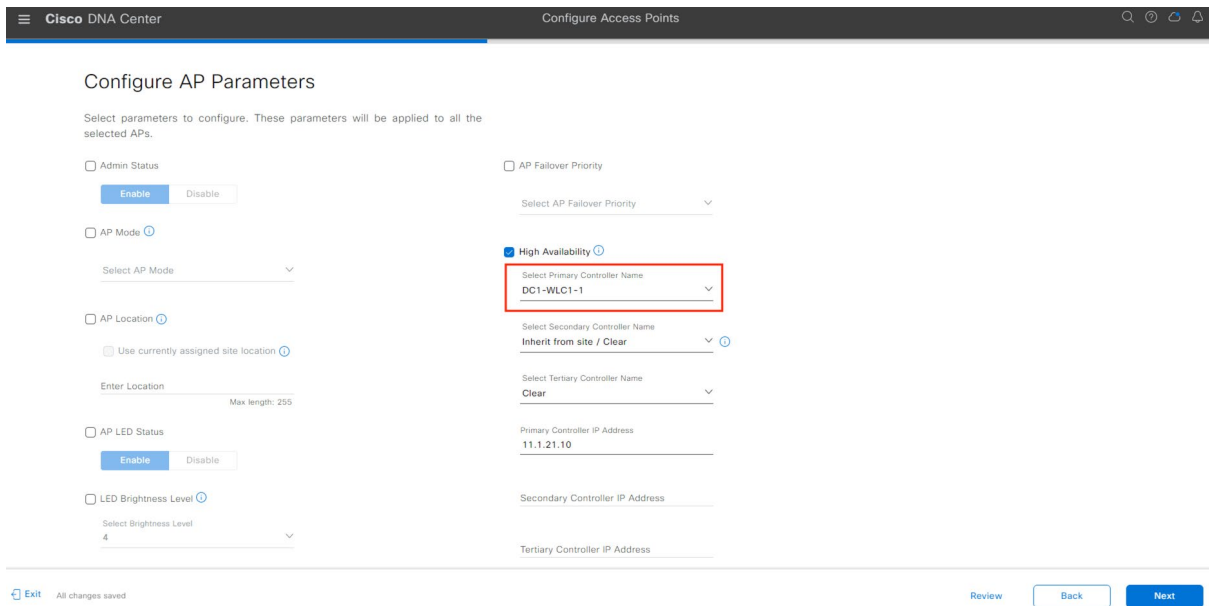
Figure 40 Catalyst 9800 controller is configured as Primary controller

Ensure the Access points are successfully joined to the Catalyst 9800 controller.
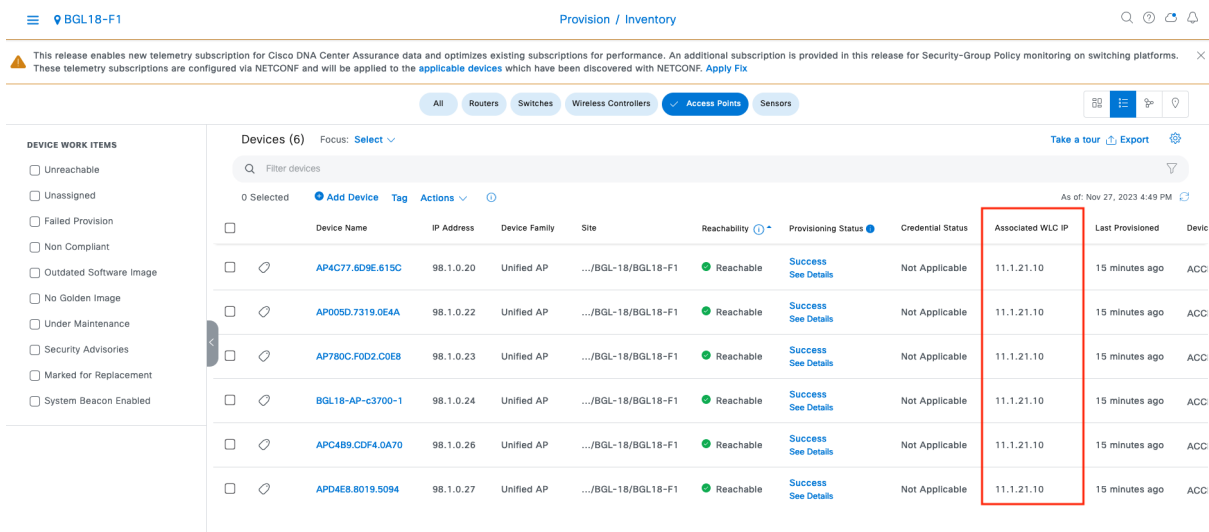
Figure 41 APs successfully Associated to the Catalyst 9800 controller

4. Provision the AireOS-based controller to not manage the chosen floor for migration. Additionally, ensure that this location is not secondary managed by any N+1 AireOS controller, if applicable.
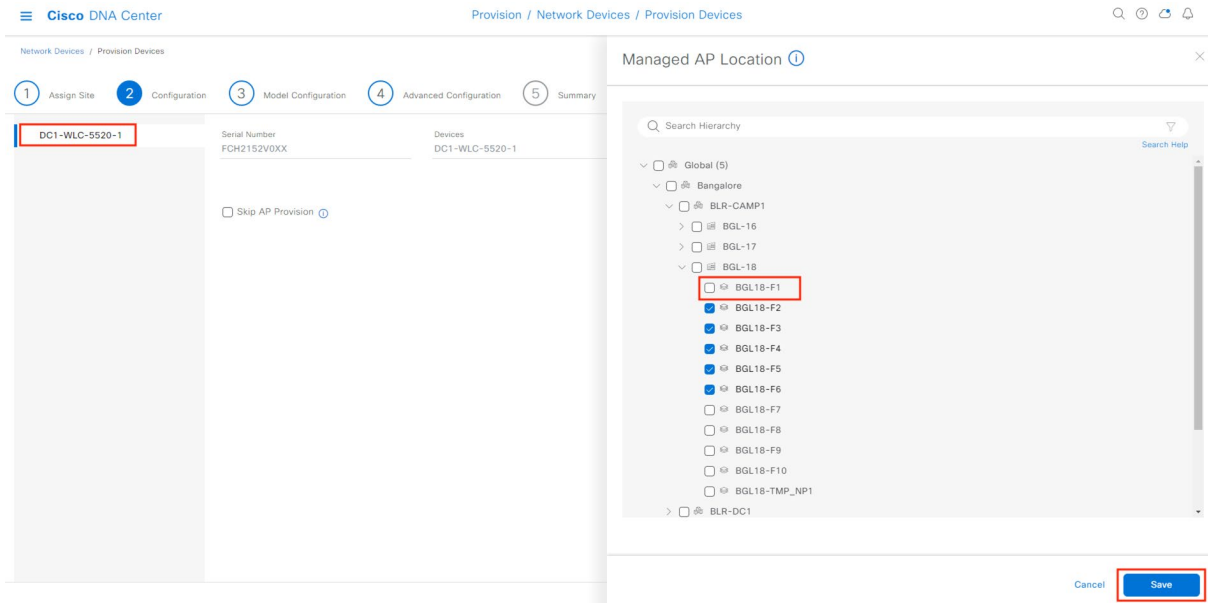
Figure 42 Floor BGL18-F1 is not being managed by AireOS controller through provision

5. Provision the Catalyst 9800 controller to manage this floor.
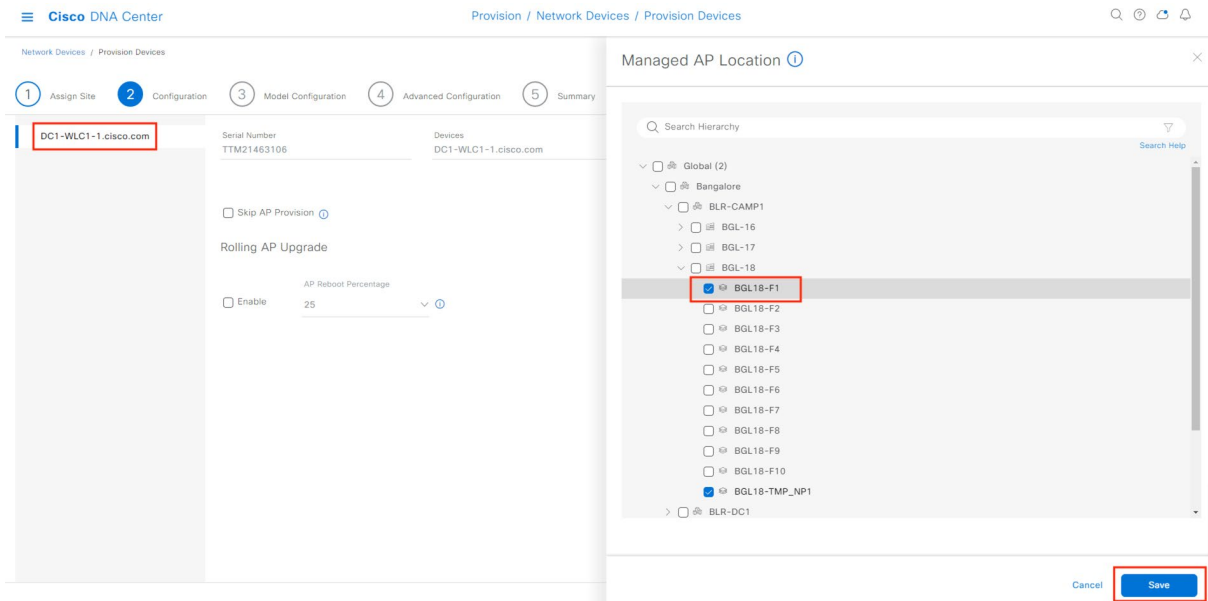
Figure 43 Floor BGL18-F1 is being managed by Catalyst 9800 controller

6. Provision the Access points part of this floor to get it configured as part of a location managed by Catalyst 9800 controller.

Technical Note – *The RF profile and AP zone related information don't persist as we have moved this location to be managed by a new Catalyst 9800 controller. Please reuse the AP to RF and Zone mappings which were recommended to be captured earlier.*

① Assign Site   ② Configuration   ③ Summary

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

Serial Number	Device Name	AP Zone Name	RF Profile	SSIDs
FOC21461RR4	AP4C77.6D9E.615C	APzone-1	HIGH	BGL-CORP-TEST
		Apply to All ⓘ	Apply to All ⓘ	
FGL2148A2N6	AP005D.7319.0E4A	APzone-2	LOW	BGL-CORP
FGL2232ABMG	AP780C.F0D2.C0E8	default-zone	TYPICAL	3
FTX1842R3HU	BGL18-AP-c3700-1	APzone-1	HIGH	BGL-CORP-TEST
KWC2108050F	APC4B9.CDF4.0A70	APzone-2	LOW	BGL-CORP
0	APD4E8.8019.5094	default-zone	TYPICAL	3

Cancel   Next

Figure 44 AP provision after the location is now being managed by Catalyst 9800 controller

⚠ This release enables new telemetry subscription for Cisco DNA Center Assurance data and optimizes existing subscriptions for performance. An additional subscription is provided in this release for Security-Group Policy monitoring on switching platforms. ✕
These telemetry subscriptions are configured via NETCONF and will be applied to the applicable devices which have been discovered with NETCONF. Apply Fix

All   Routers   Switches   Wireless Controllers   ✓ Access Points   Sensors

DEVICE WORK ITEMS

Devices (6)   Focus: Select ⌄   Take a tour ⬆ Export ⚙

☐ Unreachable
☐ Unassigned
☐ Failed Provision
☐ Non Compliant
☐ Outdated Software Image
☐ No Golden Image
☐ Under Maintenance
☐ Security Advisories
☐ Marked for Replacement
☐ System Beacon Enabled

🔍 Filter devices

0 Selected   ➕ Add Device   Tag   Actions ⌄   ⓘ   As of: Nov 27, 2023 4:36 PM ⟳

Most recent operation
AP Provisioning

		Device Name	IP Address	Device Family	Site	Reachabil		Credential Status	Associated WLC IP	Last Provisioned	Devic
☐	⊘	AP4C77.6D9E.615C	98.1.0.20	Unified AP	.../BGL-18/BGL18-F1	● Reachable	Success See Details	Not Applicable	11.1.21.10	2 minutes ago	ACCI
☐	⊘	AP005D.7319.0E4A	98.1.0.22	Unified AP	.../BGL-18/BGL18-F1	● Reachable	Success See Details	Not Applicable	11.1.21.10	2 minutes ago	ACCI
☐	⊘	AP780C.F0D2.C0E8	98.1.0.23	Unified AP	.../BGL-18/BGL18-F1	● Reachable	Success See Details	Not Applicable	11.1.21.10	2 minutes ago	ACCI
☐	⊘	BGL18-AP-c3700-1	98.1.0.24	Unified AP	.../BGL-18/BGL18-F1	● Reachable	Success See Details	Not Applicable	11.1.21.10	2 minutes ago	ACCI
☐	⊘	APC4B9.CDF4.0A70	98.1.0.26	Unified AP	.../BGL-18/BGL18-F1	● Reachable	Success See Details	Not Applicable	11.1.21.10	2 minutes ago	ACCI
☐	⊘	APD4E8.8019.5094	98.1.0.27	Unified AP	.../BGL-18/BGL18-F1	● Reachable	Success See Details	Not Applicable	11.1.21.10	2 minutes ago	ACCI

Figure 45 APs successfully provisioned

```
Welcome to Cisco DNA Center command runner.

You can access this window from anywhere using the key combination Q+T.
You can access recently viewed devices using the key combination Q+D.

Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.

DC1-WLC1-1.cisco.com> show ap tag sum
Number of APs: 6

AP Name                 AP Mac          Site Tag Name   Policy Tag Name               RF Tag Name   Misconfigured  Tag Source
-----------------------------------------------------------------------------------------------------------------------------
AP780C.F0D2.C0E8        780c.f0d2.c0e8  APG1-1_ST       PT_BLR-C_BGL-1_BGL18-F1_35585 TYPICAL       No             Static
AP4C77.6D9E.615C        4c77.6d9e.615c  APG1-1_ST       APG1-1_PT1                    HIGH          No             Static
AP005D.7319.0E4A        005d.7319.0e4a  APG1-1_ST       APG1-1_PT2                    LOW           No             Static
APC4B9.CDF4.0A70        c4b9.cdf4.0a70  APG1-1_ST       APG1-1_PT2                    LOW           No             Static
APD4E8.8019.5094        d4e8.8019.5094  APG1-1_ST       PT_BLR-C_BGL-1_BGL18-F1_35585 TYPICAL       No             Static
BGL18-AP-c3700-1        f44e.058c.f070  APG1-1_ST       APG1-1_PT1                    HIGH          No             Static

DC1-WLC1-1.cisco.com>
```

Figure 46 Controller output capturing the custom site tag/policy tag provisioned

7. As config Access point workflow was used to override the primary WLC of the APs, we may need to revert back by using the workflow again to let it use site inherited parameters.

Figure 47 Config AP workflow to revert the WLC HA parameters

8. Repeat the above steps for other floors sequentially. For the last floor that's being migrated while provisioning the AireOS controller to not manage that floor, you may need have some dummy floor managed by the AireOS controller as at least one floor has to be managed for the provisioning to succeed.

6. Technical References

- [AireOS to Catalyst 9800 migration device side best practices](#)
- [Inter Release Controller Mobility release support matrix](#)
- [Configuration model for Cisco Catalyst 9800 wireless controller](#)
- [AP image download – WLAN poller tool](#)
- [WLC config converter tool for AireOS to Catalyst 9800 cli](#)