Guide
Cisco public

Cisco Wireless Global Use AP Deployment Guide

Cisco Wireless Global Use AP Overview

The Cisco Wireless CW917x series of Access Points is a Unified Hardware with a single product id, that can be deployed with a Cisco Catalyst 9800 Wireless LAN Controller or Meraki Cloud based deployments. The CW917x series Access Points can be deployed anywhere in the world just with the single product id (PID or SKU) and avoids the need to buy a region or country specific access point hardware based on regulatory domain.

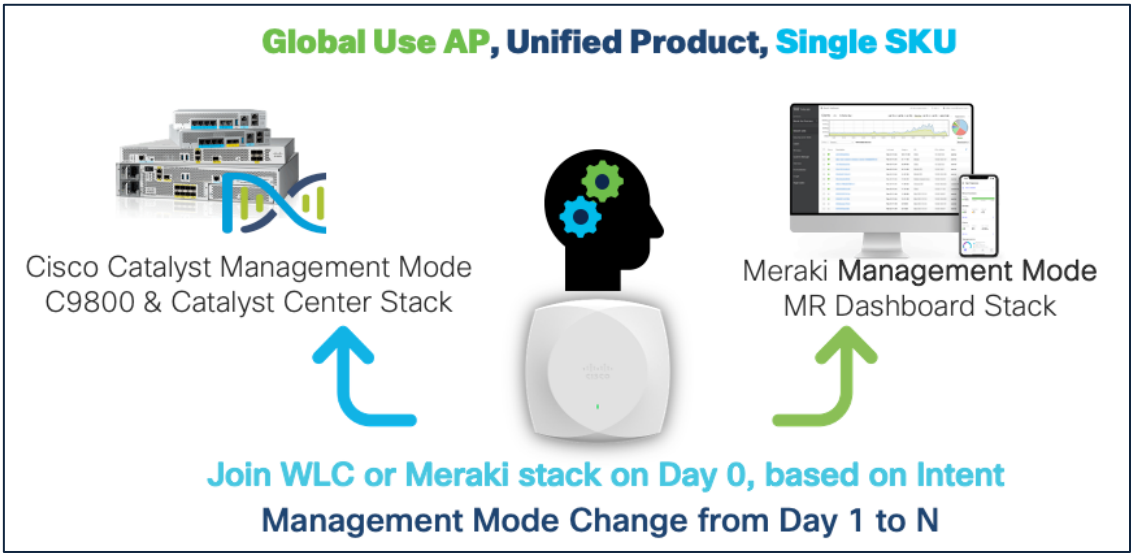


Figure 1. Global Use AP – Management Mode

The Global Use AP simplifies the Cisco Wireless AP portfolio, by

1. Decoupling the AP PID/SKU from which geography (regulatory domain) they can be used.
2. Decoupling AP PID/SKU from the boot mode; i.e WLC or Meraki based.

Examples of PID/SKU (in the past):

C9130AXI-B (where "-B" denotes for US use only)

CW9166I-MR (where -MR denotes it will boot in Meraki mode)Throughout this guide, you will learn how the CW9178I is a wireless powerhouse that can take your network to the next level.

Note: The journey of simplifying by reducing the number of regulatory domains, by combining many countries into -ROW SKU, and a common hardware, where Day 1 to N migration from one management mode to another was made possible with Cisco Wi-Fi 6E Access Points.

Having a Unified Product brings in many benefits:

1. **Simplified ordering** – Customers and Partners do not have to worry about how or where the AP will be deployed.
2. **Simplified deployment** – Planning and installation teams just plug in the Aps, Meraki Dashboard or WLC mode is auto detected. Dashboard can be used as PnP tool by partners.
3. **Simplified lifecycle** – Customers can freely move APs between WLC and Meraki mode. No need to call support. Simplified RMA and factory resets.

Map of a Global Use AP's Journey

A fresh out of box Cisco Wireless CW917x AP, on Day 0, will try to determine if it has to connect to Meraki Dashboard or to a Catalyst 9800 WLC, by checking if it has a cloud connectivity and can reach a Meraki Network or else look for a Wireless LAN Controller in the local network through DHCP, DNS and L2 broadcast discovery mechanisms.

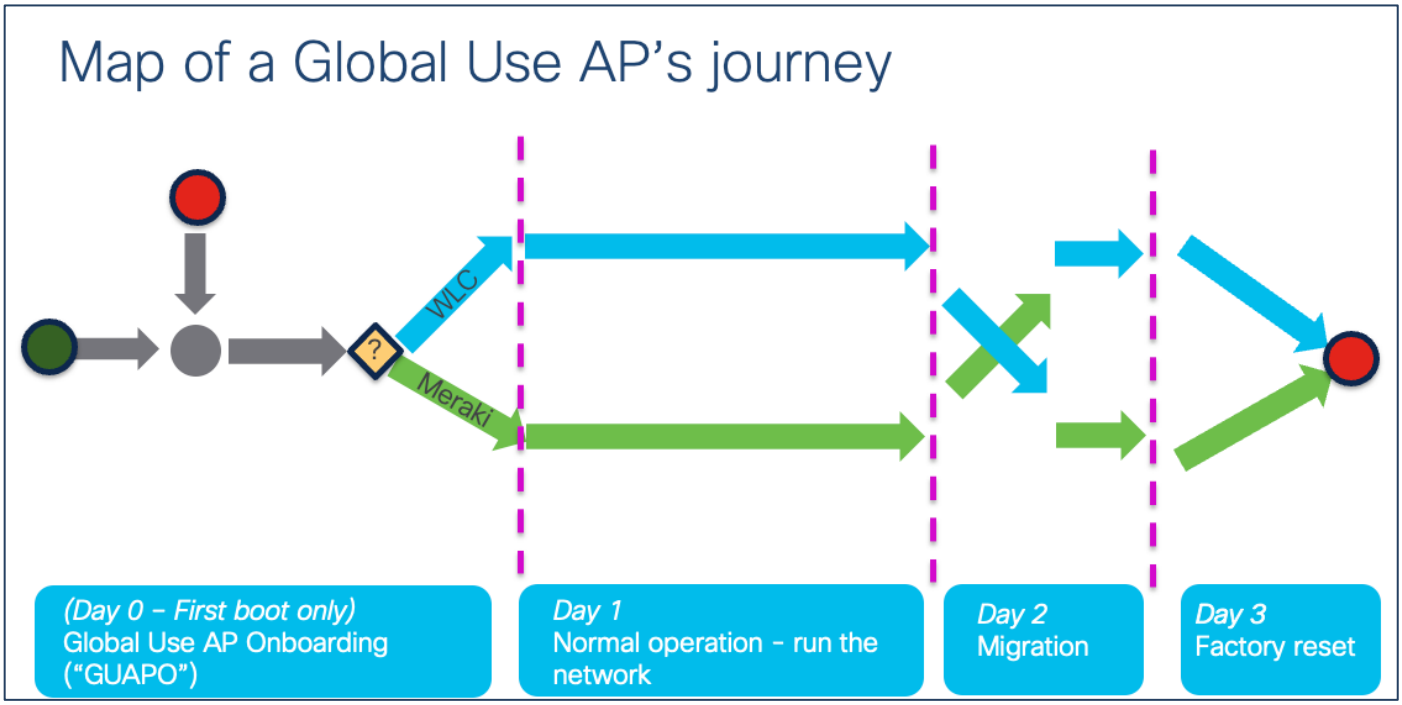


Figure 2. Global Use AP – Journey

Once the AP, based on initial discovery, determines the Management Mode, boots the corresponding firmware image and connects to Meraki Dashboard or a Catalyst 9800 controller and performs operations in that mode. The AP can be migrated from one management mode to another, easily, through a very simple workflow from a Catalyst 9800 WLC or Meraki Dashboard. The AP can be factory reset, back to Out of box, i.e Day 0 mode, at any time.

Note: When the Global Use AP connects to a Catalyst 9800 WLC, it has to determine the country in which it has to operate to adhere to local RF regulations. The Global Use AP can find the country it has to operate, in multiple ways.

1. The Cisco Wireless CW917x series Aps have a built in GPS/GNSS module, that can help to determine the geo location.
2. For APs, deep inside a floor, where it cannot have a clear skyview, it can learn it's country from a neighboring AP, which could be i) a legacy AP that is already connected to the same WLC or ii) another CW917x AP, which had obtained its location through GPS/GNSS, called the Anchor AP, by listening to the NDP messages that is transmitted over Air. This is called Proximity based discovery.
3. For Air gapped customers, where method 1 or 2, does not work, the CW917x Aps can be forced to obtain their country through a manual way of Regulatory Activation File, obtained from Meraki Dashboard and imported into Catalyst 9800 WLC.

All the methods are explained in detail in subsequent section of this document.

Customer Scenario 1 – Meraki Customer

Here is an illustration of a customer, Mr. Miles, who is a Meraki Customer on how he onboards the CW917x series Global Use Aps.

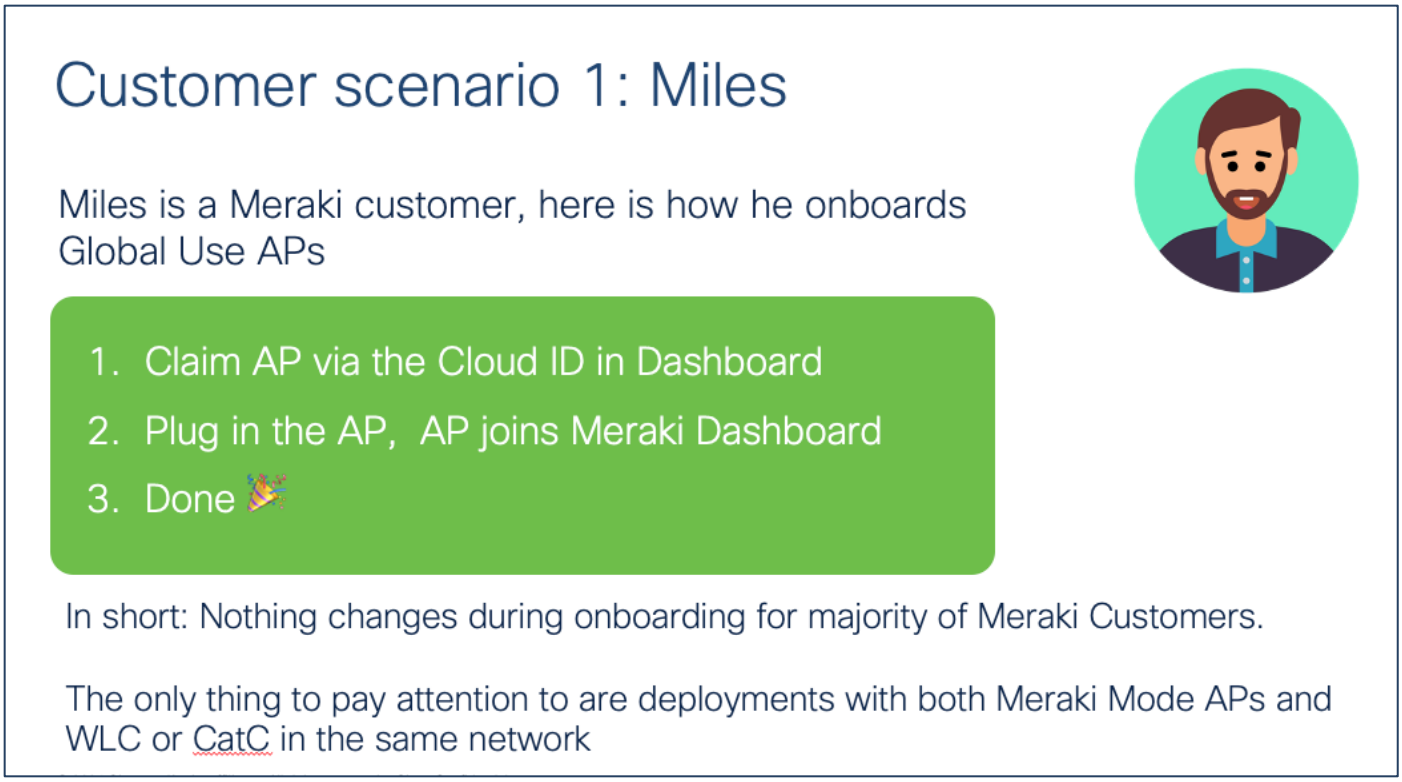


Figure 3. Global Use AP – Onboarding in a Cisco Meraki Deployment

The experience will be exactly same like today.

Customer Scenario 2 – Catalyst WLC Customer

Here is an illustration of a customer, Ms. Catarina, who is a Catalyst WLC Customer on how she onboards the CW917x series Global Use Aps.

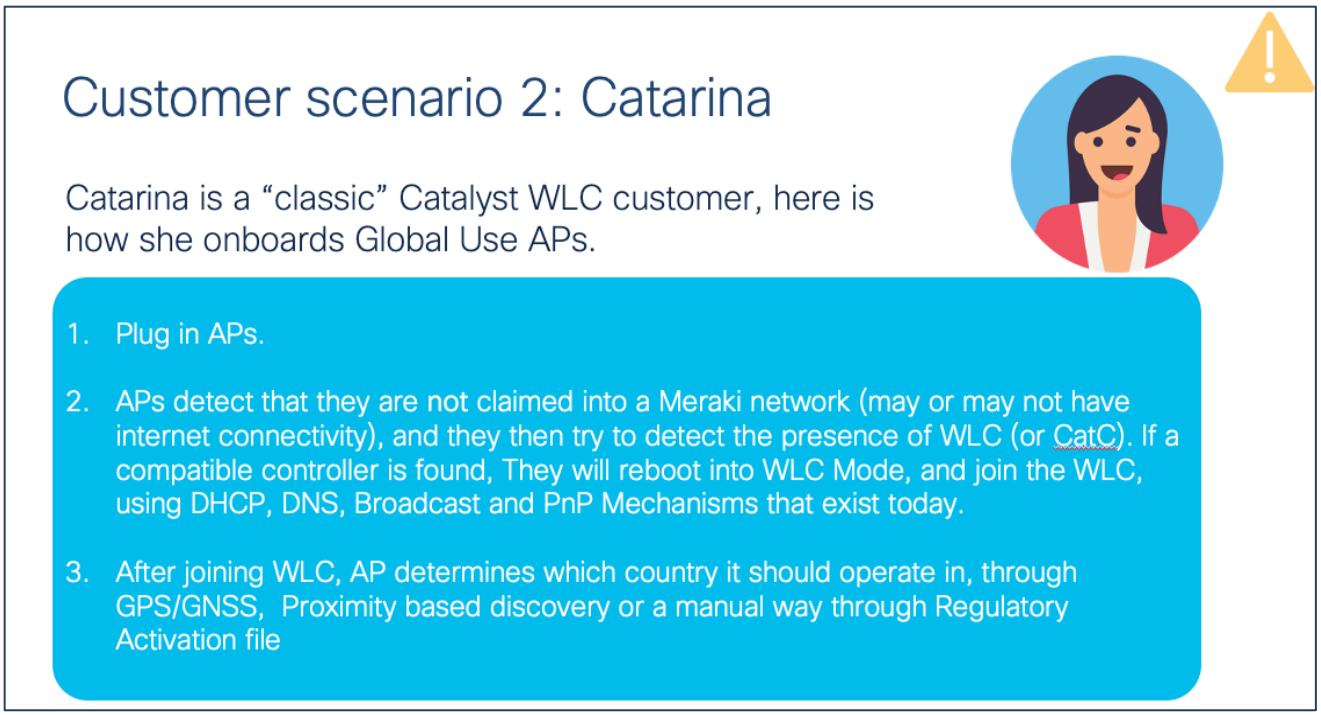


Figure 4. **Global Use AP – Onboarding in a Cisco Catalyst Deployment**

The experience will be mostly same, with a few additional configuration that may be needed, depending on the deployment.

Cloud ID

Starting with CW917x series of APs, the “Meraki Serial Number” has been renamed to “Cloud ID”. This change will reflect on the AP label, AP packaging, QR Code etc. The “Cloud ID” is used in the Meraki device claim workflow. In short, there is no functional change to how this is used in Meraki Dashboard.

Figure 5. **CW917x Product label with Cloud ID**

Day 0 Workflow: Technical Details and Configuration

This section walks through the workflow on how to onboard the CW917x Wi-Fi 7 Access Point to Meraki Dashboard and Catalyst 9800 Wireless LAN Controller.

Intent: Onboard to Meraki Dashboard

If the intent is to onboard CW917x series APs to Meraki dashboard, please make sure

1) There is an internet connectivity from the CW917x AP to reach the Meraki cloud.
2) Devices are claimed in the Meraki Dashboard, either with Order number, Cloud ID or MAC Address.
3) There is no Catalyst 9800 Wireless LAN Controller running IOS-XE version 17.15.2 or later that is present in the same VLAN as the CW917x AP.
4) There are no DHCP, DNS (including wildcard entry), or PnP configurations that can lead the CW917x AP to a Catalyst 9800 Wireless LAN Controller.

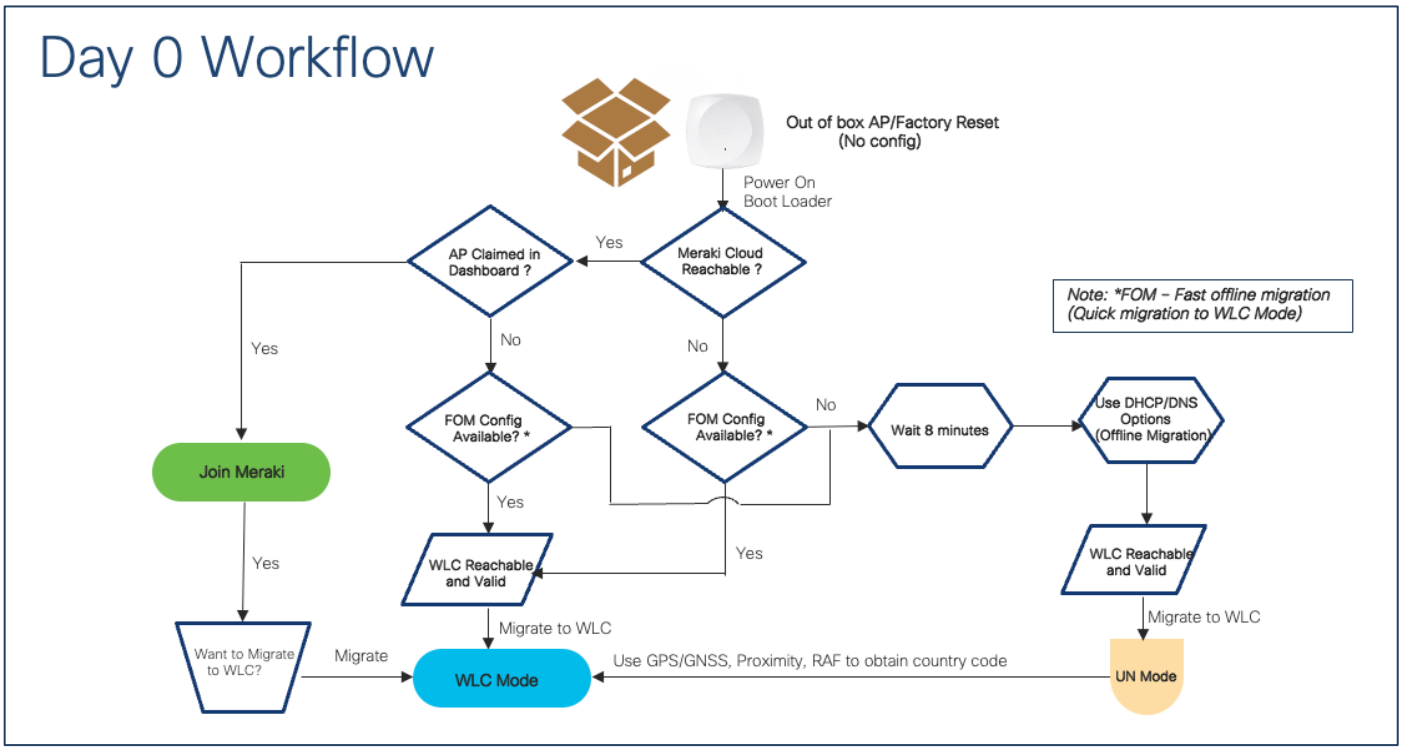
Power on the CW917x series Aps through PoE or Power Injector. The Aps once boots up, will reach the Meraki Cloud and present itself in the Dashboard.

Intent: Onboard to Catalyst Wireless LAN Controller

If the intent is to onboard CW917x series APs to Catalyst 9800 Wireless LAN Controller, there are couple of options:

Option 1: Where there is internet connectivity from the CW917x series APs and customer having a Meraki Dashboard account. Make the APs join the Meraki Dashboard and migrate the APs to WLC.

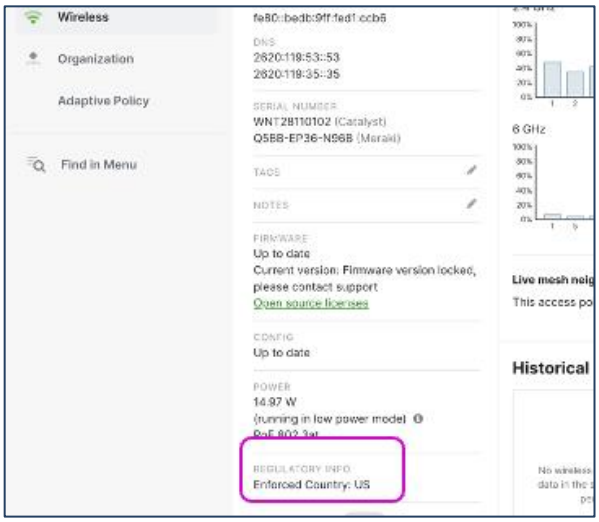
Option 2: Where there is no internet connectivity from the CW917x series APs. Employ discovery mechanisms like DHCP, DNS, Local status page (LSP), Broadcast (IPv4), Multicast (IPv6) or PnP to reach the Catalyst 9800 WLC.



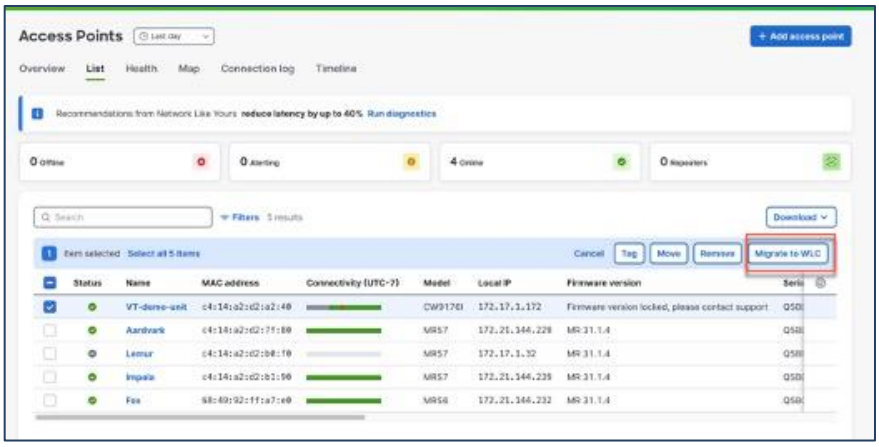
The following sections walk through the details of different options.

Option 1: Migrate through Meraki Dashboard

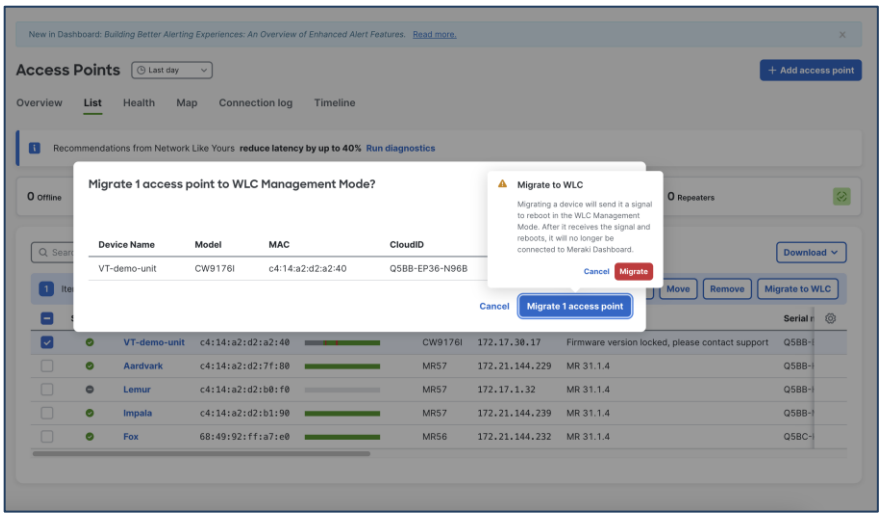
1. Add and claim the devices in a network in the Meraki Dashboard starting from Rel 31.1.5.1, either with Order number, Cloud ID or MAC Address.
2. Power on the CW917x series APs through PoE or Power Injector. Please allow few minutes for the AP to boot up and reach Meraki Cloud and present itself in the Dashboard.
3. Meraki dashboard determines where the APs are located and sets country code accordingly.



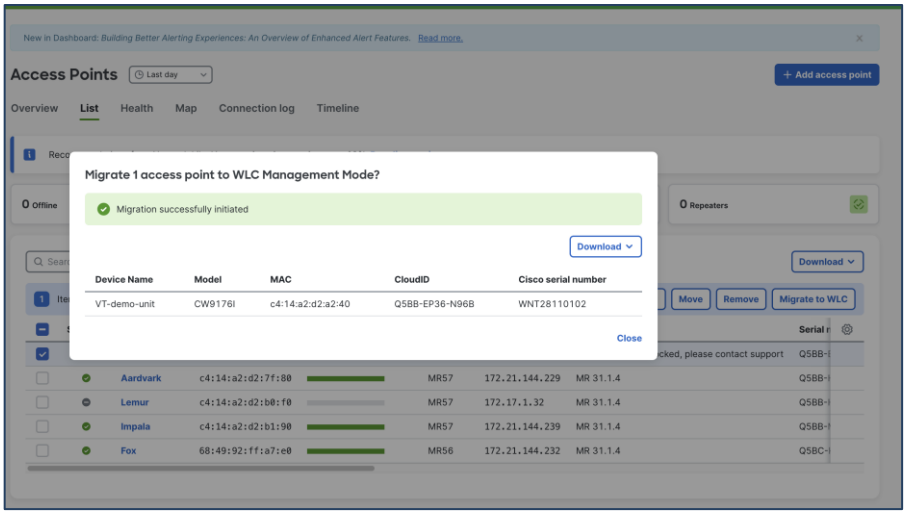
4. Make sure Mesh is disabled on Network-wide → Configure → General → Device Configuration → Mesh. **Note**: Disabling Mesh is a requirement to migrate APs and it's enabled by default in all new networks.
5. Make sure the configuration is up to date in the APs list before performing the migration in the next step. Reference: https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Monitoring_Configuration_Updates_on_Cisco_Meraki_Devices#MR_Series_Access_Points
6. Select the APs that you want to migrate and click on "Migrate to WLC".



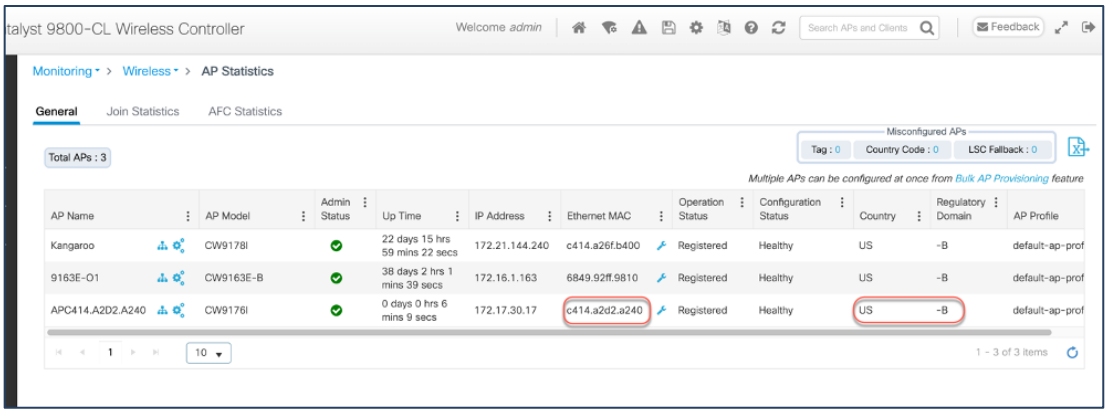
7. Confirm the migration.



8. Once done, the Meraki dashboard will send an instruction to the Access Point to reboot in WLC Management Mode.



9. When the AP reboots and boots up with WLC management mode firmware image, it will do a CAPWAP discovery of the controller through the traditional mechanism of DHCP(IPv4/IPv6), DNS(IPv4/IPv6), Broadcast (IPv4), Multicast (IPv6) and join the WLC.



10. The country code is carried forward during migration. (*No need of any additional steps or configuration needed to configure the country.*)

Option 2: Migrate without Dashboard.

This is the scenario, when there is no internet connection and the intent is to make the CW917x APs join the Catalyst 9800 WLC. This method is termed as “Offline Migration” or “Fast Offline Migration”,

Offline Migration uses traditional DHCP/DNS options, and require zero change on the existing network.

> **Note:** For Offline Migration, the AP needs to wait for 8 minutes before it starts the migration to WLC mode.

Fast Offline Migration uses new DHCP/DNS options and will bypass the 8 minute wait timer.

Note: Without Fast Offline Migration, the CW917x AP will keep looking for cloud for 8 minutes. At the end of 8th minute, it will check and confirm the WLC presence with the IP address it obtained through DHCP and DNS through CAPWAP Discovery/Response, before it migrates to the WLC Management mode. The 8 minute window is only for the very first time (in Day 0 mode), when the AP is trying to discover a cloud or WLC. Any subsequent reboot of the AP, say for example an image upgrade scenario, does not involve a wait time. The users can opt to use Fast Offline Migration techniques, where the period of 8 minute is not acceptable for Day 0 discovery of WLC>

Note: The pre-requisite is to have a Catalyst 9800 WLC with IOS-XE version 17.15.2 software for CW9178I, CW9176I & D1 Access Points and the WLC should be network reachable from APs subnet.

The order of priority for migration is as follows:

- Fast Offline Migration
  - DHCPv4
  - DHCPv6
  - DNSv4
  - DNSv6
- Local Status Page
  - The AP can be manually migrated through the web interface a.k.a Local Status Page of the AP within the 8 minutes, when Fast Offline migration Options are not present.
- Offline Migration
  - DHCPv4
  - DHCPv6
  - DNSv4
  - DNSv6
  - Broadcast/Multicast Discovery

Fast Offline Migration

1) DHCPv4

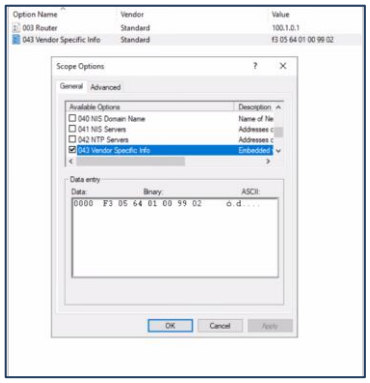
   The option 43 string for DHCPv4 Fast offline migration is as follows:

   - F3 <size> <IP array> Mode=<1|2>, where Mode = 1 → Meraki and 2 → Catalyst
   - Example String:

    - f305ac10011802 (“normal” option 43 “f104ac100118” becomes “f305ac10011802”)
        - Change type from f1 to f3
        - Change length from 04 to 05
        - Add the suboption at the end; 01 for Meraki, 02 for Catalyst
- IOS/IOS-XE configuration example for WLC discovery using DHCPv4:

```
ip dhcp pool vlan192
  network 192.168.200.0 255.255.255.0
  default-router 192.168.200.1
  option 43 hex 0bf305.ac10.0118.02
```

- Windows server configuration screenshot:



Note: At least one IP in the IP array must be either ICMP or CAPWAP reachable. The AP will check for ping the WLC. If there is a response, the AP will migrate to WLC Management mode, else it will try a CAPWAP discovery.

2) DHCPv6

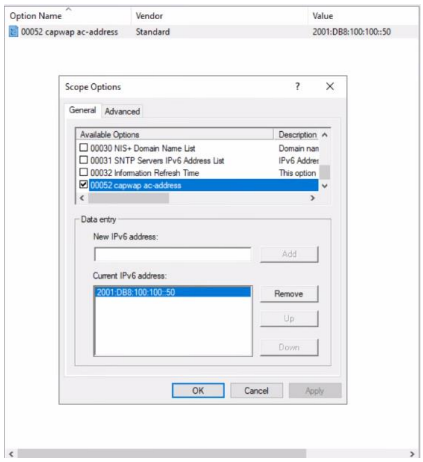
The fast offline migration for DHCPv6 is Option 52 + Option 17

- Option 52 (standard): IPv6 array
- Add Option 17
    - Enterprise ID = 29671; SubCode =1; Size =1; Mode = <1|2>, where Mode = 1 → Meraki and Mode = 2 → Catalyst vendor-specific 29671
- IOS/IOS-XE configuration example for WLC discovery using DHCPv6:

```
ipv6 dhcp pool vlan20
          address prefix 2001:DB8:20:20::/64
          capwap-ac address 2001:DB8:20:20::50
          vendor-specific 29671
          suboption 1 hex 02
```

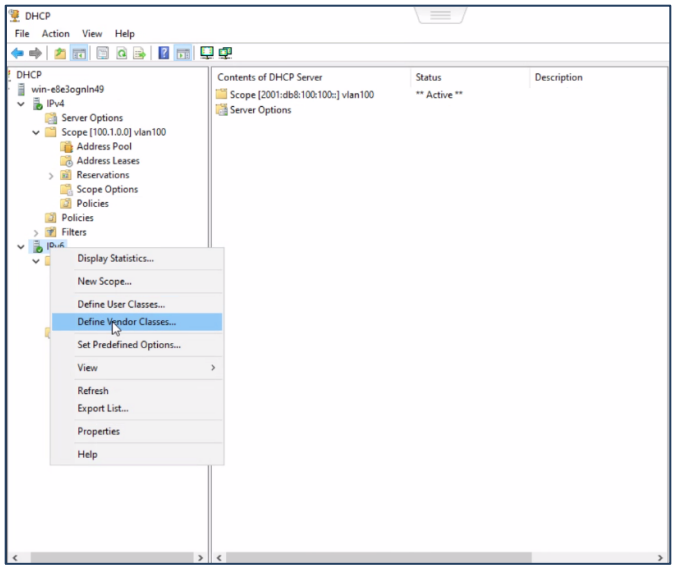
- Windows server configuration steps:

  Option 52:

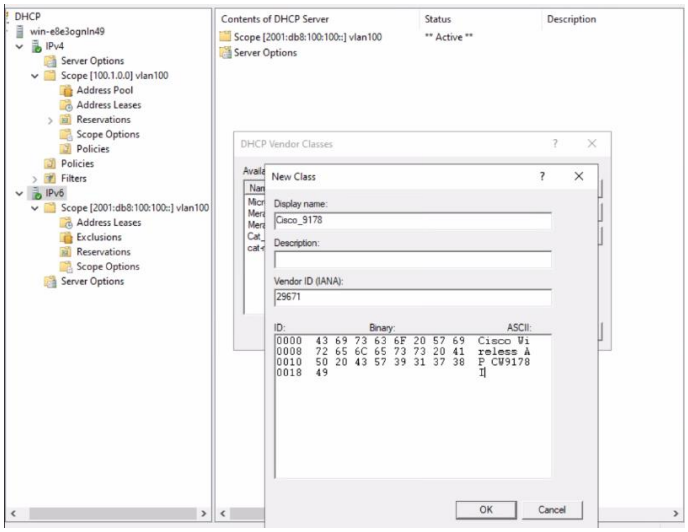


Option 17:

Step 1: Define Vendor Class.



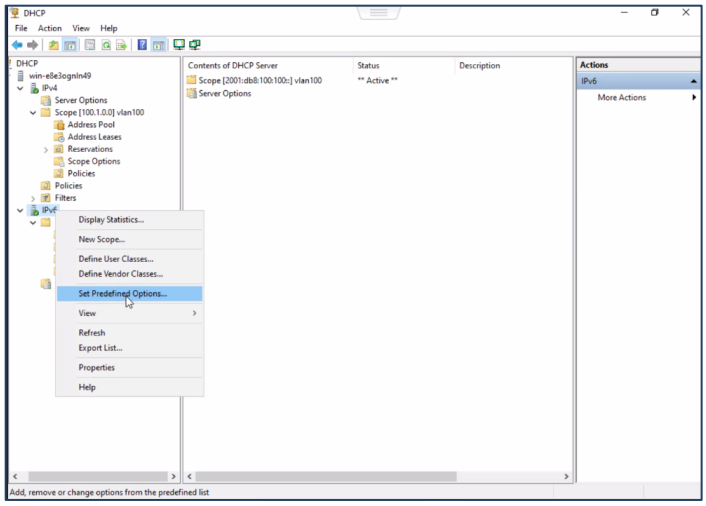
Step 2: Assign a name. Enter the value 29671 for Vendor ID. Enter the ASCII value “Cisco Wireless AP CW9178I” in the text box for CW9178I platform.



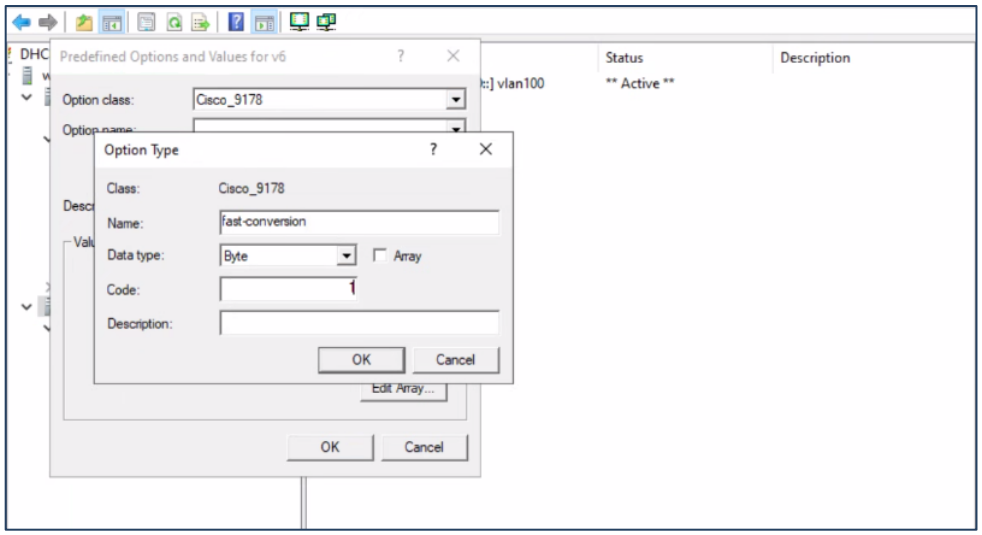
Note: For CW9176I, please use the ASCII string “Cisco Wireless AP CW9176I”.

For CW9176D1, please use the ASCII string “Cisco Wireless AP CW9176D1”

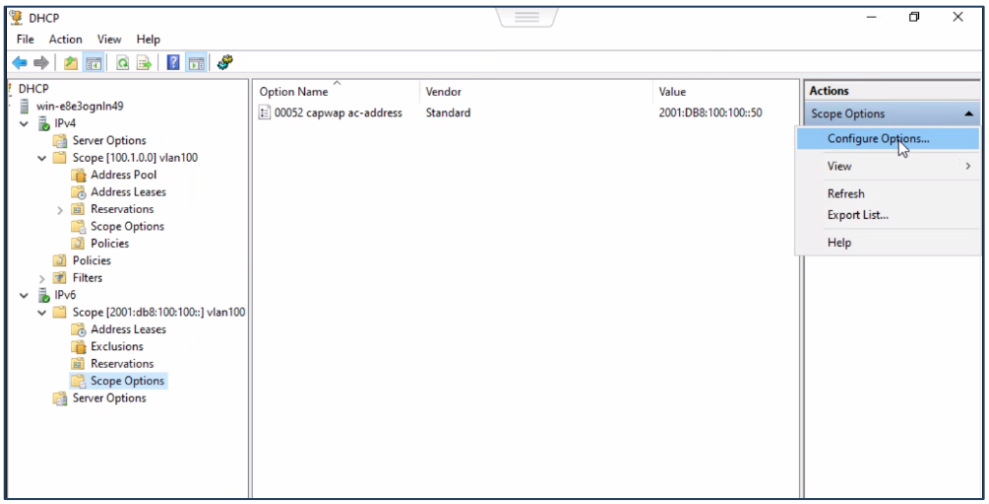
Step 3: Step predefined options.



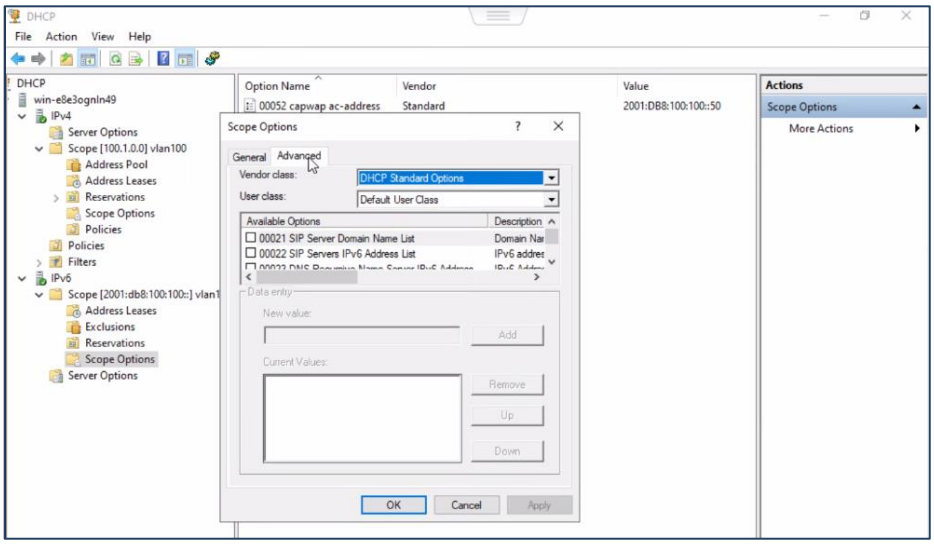
Step 4: Enter the value “1” in the Code field.

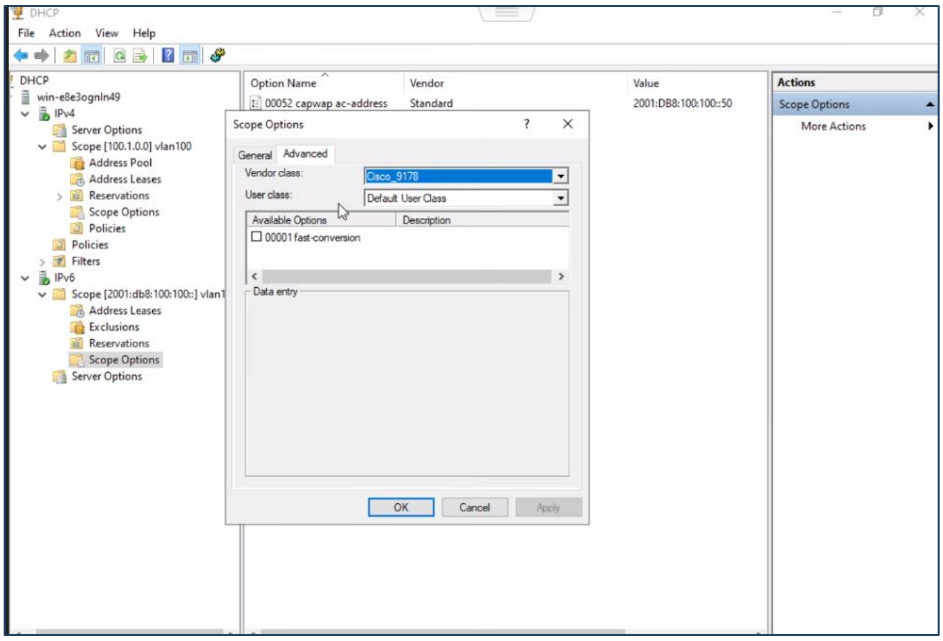


Step 5: Under the scope options, select Configure options.

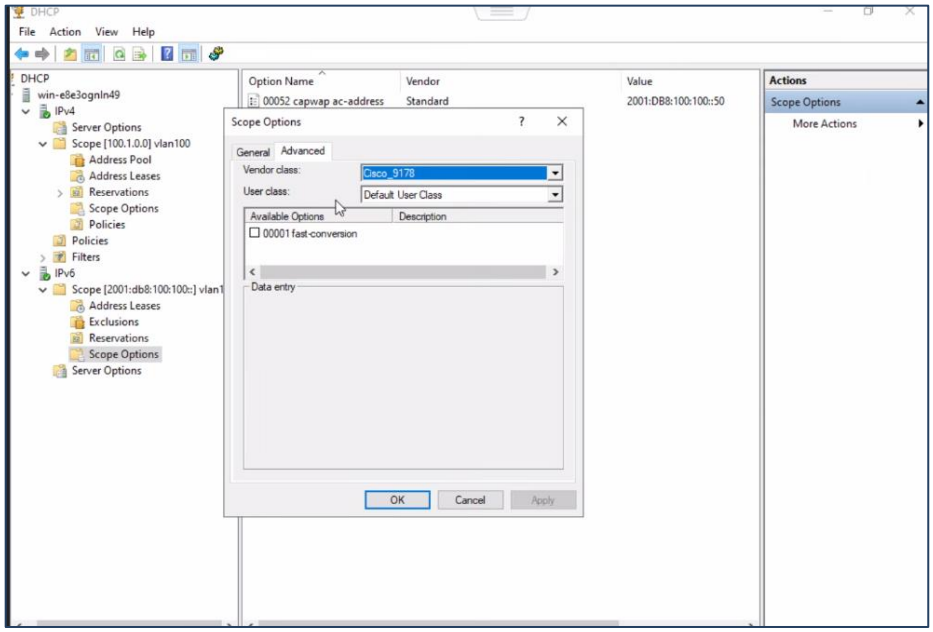


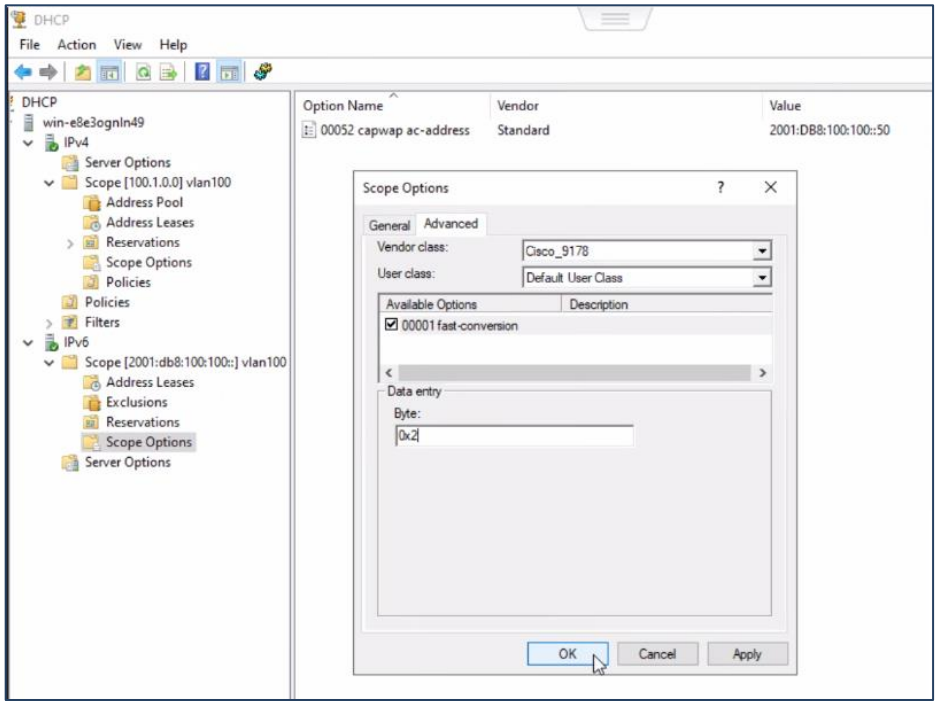
Step 6: Under the advanced tab, select the Vendor Class, created in Step 2.

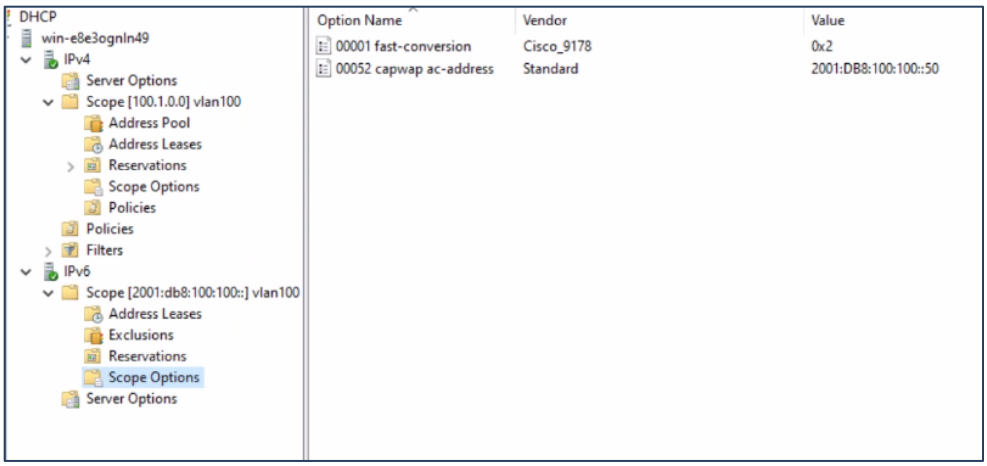




Step 7: Select the available options, and enter the value 0x2







Note: At least one IP in the IP array must be either ICMP or CAPWAP reachable. The AP will check to ping the WLC. If there is a response, the AP will migrate to WLC Management mode, else it will try a CAPWAP discovery.

Note: When both IPv4 and IPv6 (stateful) are present in dual stack, configure migration options in v4.

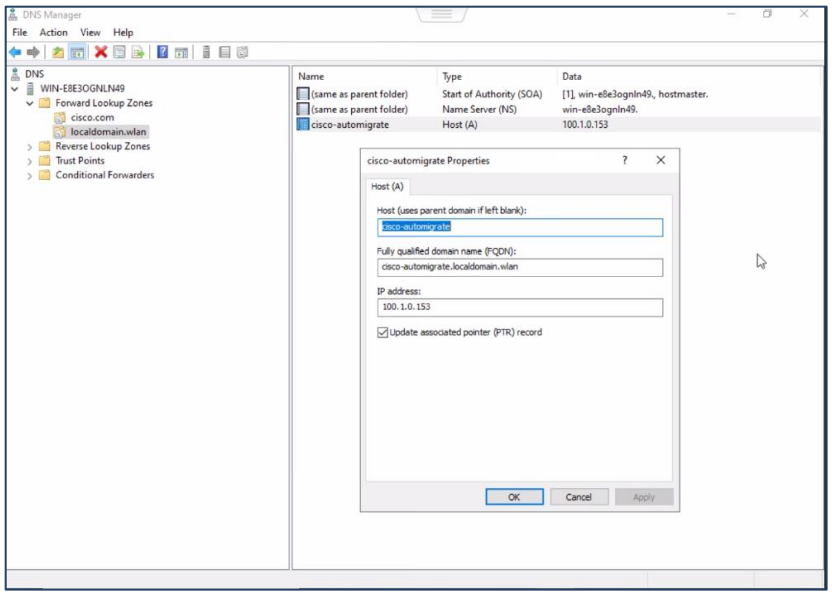
Note: When only IPv6 (stateful) is present, then only Fast Offline migration is supported (Option 17+52)

3) DNSv4/v6

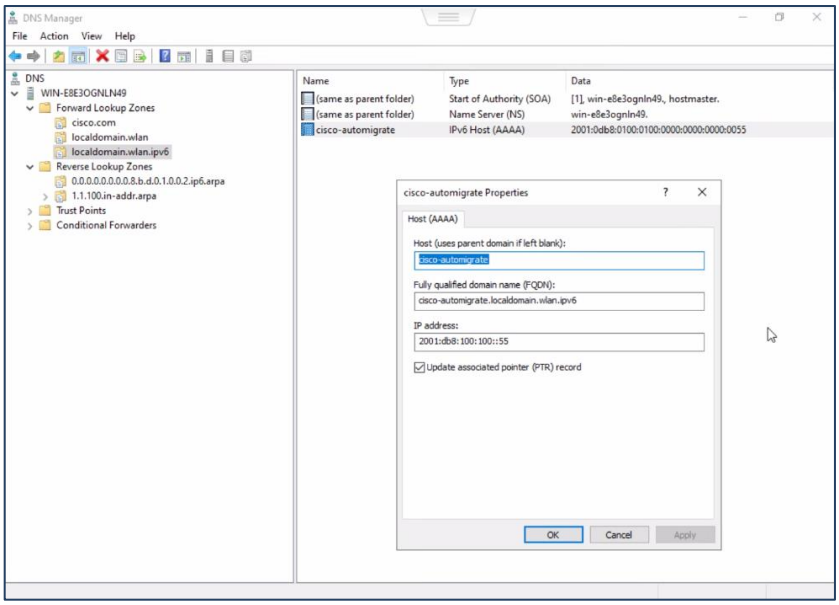
The fast offline migration string for DNS for both v4 and v6 :

- Add the DNS entry (A record) **cisco-automigrate.<domain>** in the DNS server.
- The AP checks for the presence of DNS entry (AAAA record): **cisco-automigrate.<domain>**
  If the dns entry resolves, THEN, ping IP returned from DNS.
  If ping success, then immediately migrate AP to WLC mode
  If ping fails, try CAPWAP discovery
- Windows server screenshots:

  IPv4



IPv6



Local Status Page

The CW917x series APs have a local status page that can be accessed to migrate the AP to WLC Management mode, when in Day 0 mode, during the 8 minute discovery period. Please refer to the document https://documentation.meraki.com/General_Administration/Tools_and_Troubleshooting/Using_the_Cisco_Meraki_Device_Local_Status_Page on how to access the Local Status Page.

From the Local Status Page, click on Migrate to WLC Management mode. This will trigger a reload of the AP, boot with WLC Management Mode firmware and proceed to discover WLCs.

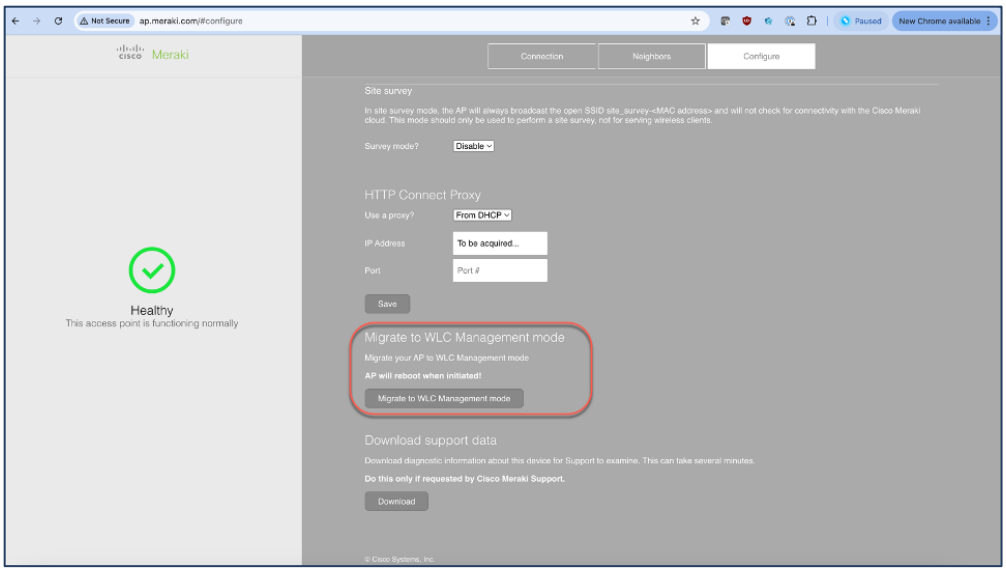


Figure 6. AP Migration to WLC Management Mode using Local Status Page in Cisco Meraki

Offline Migration

Once the 8 minute discovery window (to reach Meraki Cloud, Fast-Offline Migration and migration through Local status page) is over, the AP will resort to traditional discovery mechanisms of DHCP, DNS and Broadcast/Multicast.

The existing configuration used for CAPWAP discovery mechanisms in the Wireless LAN Controller deployments are very much applicable.

Note: The DHCPv4 option 43 with type f2 used for EWC deployments can be used. However, the recommendation is to use standard option 43 values.

Example:

```
option 43 hex f205.c0a8.0a05.01
```

Onboarding through PnP Server

Deployments that employ PnP (Plug-N-Play) server to stage parameters to an access point, is supported as well, with CW917x Access Points in the Day 0 workflow. Onboarding through PnP Server is supported only in Offline Migration and is not supported in the Fast Offline Migration method.

Example configuration of DHCP scope with Option 43 for PnP.

```
ip dhcp pool vlan192
  network 192.168.200.0 255.255.255.0
  default-router 192.168.200.1
  option 43 ascii 5A1D;B2;K4;|192.168.200.5;J8
```

Preventing False Migration

There are few steps put in place to prevent accidental migration.

1. At least one IP in the IP Address array returned by DHCP option or the IP address of the resolved DNS entry should be CAPWAP reachable, which will trigger the bootloader to boot up the WLC Management

mode firmware image for AP join. The CAPWAP response includes the WLC version image, which will be compared by the CW917x AP, to be a valid image, where it can join the WLC. This is done to prevent accidental migration, because of a response from a WLC, that's not intended.

2. If the DNS entry **cisco-do-not-automigrate.<domain>** resolves to an IP address, then AP won't migrate to WLC mode.

   Note: The above method is valid only if DNS method is configured. It's not valid when other methods like DHCP and L2 discovery is present.

3. End user control through CLI. The end user can configure the CLI to prevent WLC to respond to Day 0 CAPWAP discovery requests by the CW917x APs. This way the end user can fine tune its config based on its own deployment specificities.

   Configuration is done in AP Join Profile.

   To "not respond" to CAPWAP Discovery:

```
C9800-L(config)#ap profile onboarding-prof
C9800-L(config-ap-profile)#no capwap-discovery onboarding
C9800-L(config-ap-profile)#exit
C9800-L(config)#
```

   To "respond" to CAPWAP Discovery:

```
C9800-L(config)#ap profile onboarding-prof
C9800-L(config-ap-profile)#capwap-discovery ?
  onboarding  Configure CAPWAP onboarding related parameters
  private     Include private IP in CAPWAP Discovery Response
  public      Include public IP in CAPWAP Discovery Response

C9800-L(config-ap-profile)#capwap-discovery onboarding ?
  all      Configure automatic CAPWAP onboarding from Meraki based on both
           unicast and broadcast discovery request
  unicast  Configure automatic CAPWAP onboarding from Meraki based on unicast
           discovery request only
```

   By default WLC will accept only unicast request for onboarding.

   Note: If the CW917x APs have to be in the same subnet as the WLC and use Broadcast (IPv4) or Multicast (IPv6) for discovery, then capwap-discovery onboarding should be set to "all". Otherwise the WLC will not respond to Broadcast/Multicast discovery requests.

Troubleshooting Day 0 Onboarding

When the CW917x series AP is in Day 0 mode, the console will print the output shown below as a result to any input followed by a character return.

```
<Meraki>

Global Use AP ships with Meraki OS as the primary image and with default no
country domain configured. Depending on the DHCP/DNS configurations and Cloud
connectivity AP will either stay in Meraki or Catalyst mode to reach WLCs. To
get more details on the procedure please look at online documentation.

We have currently detected the Access Point is in Day 0 mode. i.e doesn't have
a persona yet. AP will proceed for offline migration shortly. Offline
migration procedure will check if a Catalyst WLC is present in the network and
automatically migrate to Catalyst if a valid one is detected (>= IOS XE 17.15)

Offline migration can take up to 15 minutes to take a decision. To get logs
and details on the current state of offline migration procedure, please type
'offline-migration-info' command after <Meraki> console prompt.

If the intent for the Access Point is to be connected via Meraki mode, resolve
the Cloud connectivity and follow the Dashboard procedure to claim the device
on the network.

<Meraki>
```

Figure 7. Day 0 information on CW917x Console

Type the command “offline-migration-info” on the <Meraki> prompt to get the details on the Day 0 onboarding process.

```
| [2024-10-04 17:40:28.755] [offline-migration] no migration & not claimed => restart detection
| [2024-10-04 17:40:33.770] [init] start offline migration detection
| [2024-10-04 17:41:33.957] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2024-10-04 17:41:38.973] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2024-10-04 17:41:38.973] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2024-10-04 17:41:38.973] [fast-offline-migration][v4] missing DNS config (server and/or domain)
| [2024-10-04 17:41:38.973] [fast-offline-migration][v6] missing DNS config (server and/or domain)
| [2024-10-04 17:41:38.973] [fast-offline-migration] waiting for 7min before taking any migration decision
| [2024-10-04 17:42:39.165] [fast-offline-migration] waiting for 6min before taking any migration decision
| [2024-10-04 17:43:39.362] [fast-offline-migration] waiting for 5min before taking any migration decision
| [2024-10-04 17:44:39.550] [fast-offline-migration] waiting for 4min before taking any migration decision
| [2024-10-04 17:45:39.736] [fast-offline-migration] waiting for 3min before taking any migration decision
| [2024-10-04 17:46:39.927] [fast-offline-migration] waiting for 2min before taking any migration decision
| [2024-10-04 17:47:40.122] [fast-offline-migration] waiting for 0min before taking any migration decision
| [2024-10-04 17:48:40.315] [offline-migration] forcing DHCP renew
| [2024-10-04 17:48:40.315] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2024-10-04 17:48:45.331] [offline-migration] migration decision
| [2024-10-04 17:48:45.331] [offline-migration][v4] no WLC IP in DHCP option 43
| [2024-10-04 17:48:45.331] [offline-migration][v4] missing DNS config (server and/or domain)
| [2024-10-04 17:48:45.331] [offline-migration][v6] no WLC IP in DHCP option 52
| [2024-10-04 17:48:45.331] [offline-migration][v6] missing DNS config (server and/or domain)
| [2024-10-04 17:48:50.352] [offline-migration][v4][capwap-12] 0 WLC(s) detected (unsupported)
| [2024-10-04 17:48:55.374] [offline-migration][v6][capwap-12] 0 WLC(s) detected (unsupported)
| [2024-10-04 17:48:55.374] [offline-migration] no migration & not claimed => restart detection
| [2024-10-04 17:49:00.389] [init] start offline migration detection
| [2024-10-04 17:50:00.606] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2024-10-04 17:50:05.622] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2024-10-04 17:50:05.622] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2024-10-04 17:50:05.622] [fast-offline-migration][v4] missing DNS config (server and/or domain)
| [2024-10-04 17:50:05.623] [fast-offline-migration][v6] missing DNS config (server and/or domain)
| [2024-10-04 17:50:05.623] [fast-offline-migration] waiting for 7min before taking any migration decision
<Meraki> offline-migration-info
```

Figure 8. Cisco Meraki CLI - Output of <offline-migration-info> command

The “offline-migration-info” command is only available whilst the AP is in Day 0 mode.

Country Code and Regulatory Domain

The Wi-Fi 7 access points need a country code for them to operate in the country they are deployed, and to meet the local regulatory compliance.

For APs operating in Meraki mode, the regulatory enforcement is done based on the Geo-IP location and network-wide setting.

Previously, for APs operating in WLC Mode, the regulatory enforcement was through individual SKU per country or territory. With CW917x series APs having a single SKU or PID, they can be deployed anywhere in the world, as the regulatory enforcement is not done in the hardware. These APs can determine their Country Code in one of the following ways:

1. **GPS/GNSS** – Obtain the geolocation through the integrated GPS/GNSS Antenna.
2. The CW917x series AP have a built in GPS/GNSS. They can obtain the geolocation coordinates, as long as they can get a clear sky view typically placed near a window to obtain the satellite signal. WLC maps the geolocation coordinates to the country. Till the time, the AP obtains the country code, it will have -UN as the regulatory domain.
3. **Note**: The CW917x series APs has an external GPS/GNSS antenna port. If the AP is not very close to a window, then an external GPS/GNSS antenna can be plugged into the AP to obtain the geolocation coordinates. The external antenna has a cable length of 10m (32.80 ft), so the AP can be placed upto 10m from the window or wall of the external Antenna.
4. Part number of the GNSS External Antenna: CW-ANT-GPS1-M-00

```
C9800-L#show ap summary
Number of APs: 1

CC = Country Code
RD = Regulatory Domain

AP Name Slots AP Model  Ethernet MAC   Radio MAC      CC   RD   IP Address
State         Location
-------------------------------------------------------------------------------
----------------------
AP-B2E0   4   CW9178I   c414.a26f.b2e0 c414.a26f.b2f0 --   -UN  20.20.20.52
Registered default location

C9800-L#
```

Once the WLC determines the country code, the AP will undergo a reload and join back with the country code.

```
*Oct 21 22:05:04.146: %APMGR_TRACE_MESSAGE-5-AP_COUNTRY_CODE: Chassis 1 R0/0:
wncd: AP Name Wi-Fi7-AP-B2E0 Mac: c414.a26f.b2f0 Model CW9178I Type
REVERSE_GEOCODING : SUCCESS: Resolve Country Code: [US]

*Oct 21 22:05:31.027: %CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN: Chassis 1
R0/0: wncd: AP Event: AP Name: Wi-Fi7-AP-B2E0 Mac: c414.a26f.b2f0 Session-IP:
20.20.20.52[5272] 20.20.20.11[5246] Disjoined Max Retransmission to AP

C9800-L#show ap name Wi-Fi7-AP-B2E0 config general | inc Country
Country Code                                    : US
Regulatory Domain Allowed by Country            : 802.11bg:-A 802.11a:-AB 802.11
6GHz:-B
AP Country Code                                 : US  - United States
Country Code Resolution Method                  : GPS

C9800-L#show ap summary
```

```
Number of APs: 1


CC = Country Code
RD = Regulatory Domain


AP Name Slots AP Model  Ethernet MAC   Radio MAC      CC   RD   IP Address    State
Location
-----------------------------------------------------------------------------------------------
------
AP-B2E0   4   CW9178I   c414.a26f.b2e0 c414.a26f.b2f0 US   -B  20.20.20.52
Registered default location


C9800-L#
```

Not all the APs need to obtain the GPS/GNSS signal. A few APs on a floor can obtain the GPS/GNSS singnal and serve as Anchor APs. Then, the remaining APs that are located deep within the building can get their country code through Proximity-based discovery. This is covered in the next step.

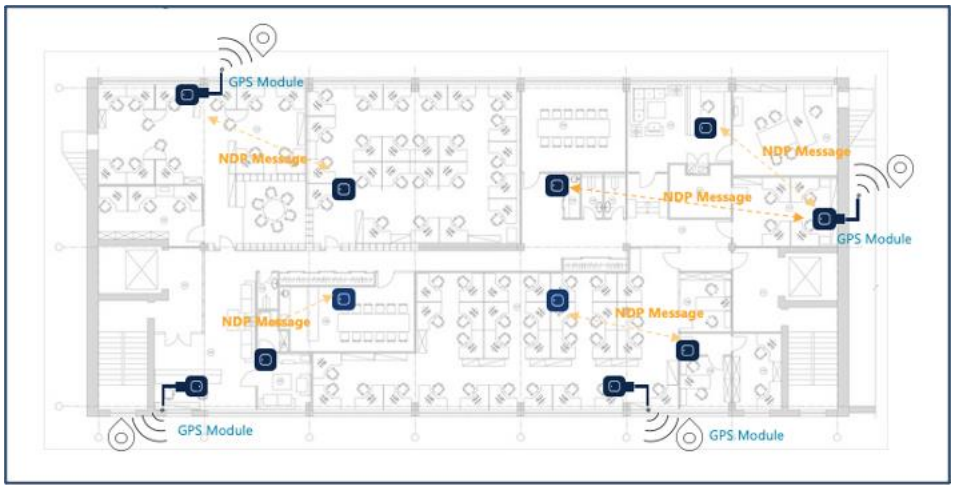


Figure 9. Gelocation through Integrated GPS/GNSS Antennas

Note: In some deployment scenarios, where there are no clear sky view, thick windows, close neighbor buildings, the AP could take a long time or never obtain a GPS/GNSS signal. In such scenarios, the other methods like Proximity, Migration or Regulatory Activation File could be used to obtain the country code and regulatory information for WLC Management mode. For Greenfield deployments, it's recommended to use GPS/GNSS. If there are issues in obtaining the GPS/GNSS signal, as mentioned above, it's recommended to use Migration through Meraki Dashboard.

Proximity based discovery – Learn from the nearby APs connected to the same WLC through RF NDP messages.

For brownfield deployments, where there is difficulty in obtaining the GPS/GNSS signal since there are pre-existing legacy APs on the floor, it's recommended to use proximity-based discovery.

The requirements for proximity-based discovery are to have:

1. Legacy APs in the RF neighborhood, joined to the same WLC and present in the same Site Tag as the Wi-Fi 7 APs, and

2. 2.4 GHz network enabled.

   The Wi-Fi 7 APs listen to the RF NDP messages on the 2.4 GHz channels and learn the country code.

   Note: Proximity based discovery will NOT work, if 2.4 GHz network is disabled. It's mandatory to turn it on.

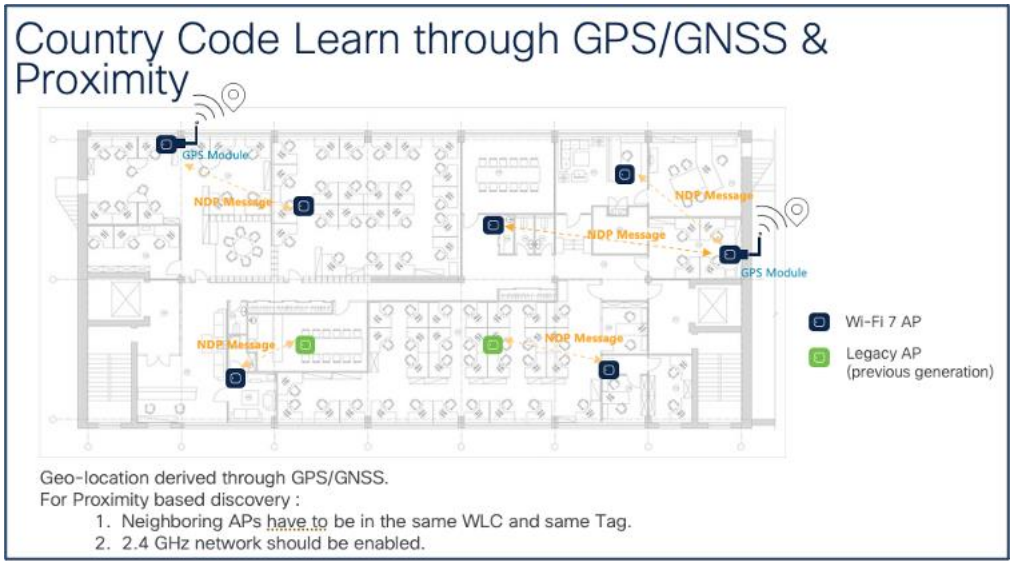


Figure 10. Obtaining Country Code through Proximity-based Discovery

In the above scenario, there are a few APs, where they are able to obtain the GPS/GNSS signal and get the country code. There are also legacy APs present in the floor. The Wi-Fi 7 APs in the RF vicinity can learn their country code from the Wi-Fi 7 APs with GPS Module or from the legacy APs.

<u>AP state before obtaining the country code:</u>

```
C9800-L#show ap summary
Number of APs: 2

CC = Country Code
RD = Regulatory Domain

AP Name  Slots AP Model  Ethernet MAC  Radio MAC       CC   RD   IP Address
State        Location
-------------------------------------------------------------------------------
--------------------------
AP-B2E0    4     CW9178I c414.a26f.b2e0 c414.a26f.b2f0 --   -UN  20.20.20.52
Registered   default location
AP-E040    3     CW9176I 8c88.814f.e040 ecf4.0caf.6a60 US   -B   20.20.20.51
Registered   default location

C9800-L#
```

In the example above, the AP named AP-E040 has it's country code and regulatory domain and the AP named AP-B2E0 is in the nearby proximity, which will learn it's country code from AP-E040. This process takes just few minutes.

The APs undergo a reload, when they learn their country code from the neighboring APs.

```
*Oct 21 21:49:57.664: %APMGR_TRACE_MESSAGE-5-AP_COUNTRY_CODE: Chassis 1 R0/0:
wncd: AP Name Wi-Fi7-AP-B2E0 Mac: c414.a26f.b2f0 Model CW9178I Type PROXIMITY :
SUCCESS: Resolve Country Code: [US ]


*Oct 21 21:49:57.665: %APMGR_TRACE_MESSAGE-6-WLC_APMGR_INFO: Chassis 1 R0/0:
wncd: Info : - c414.a26f.b2f0 Setting country code  to Access Point, Access Point
will reboot and join back to WLC
```

<u>AP state after obtaining the country code:</u>

```
C9800-L#show ap summary
Number of APs: 2


CC = Country Code
RD = Regulatory Domain


AP Name  Slots AP Model  Ethernet MAC  Radio MAC       CC   RD   IP Address
State        Location
-------------------------------------------------------------------------------
--------------------------
AP-B2E0    4     CW9178I c414.a26f.b2e0 c414.a26f.b2f0 US  -B  20.20.20.52
Registered   default location
AP-E040    3     CW9176I 8c88.814f.e040 ecf4.0caf.6a60 US  -B  20.20.20.51
Registered   default location


C9800-L#show ap name Wi-Fi7-AP-B2E0 config general | inc Country
Country Code                                    : US
Regulatory Domain Allowed by Country            : 802.11bg:-A 802.11a:-AB
802.11 6GHz:-B
AP Country Code                                 : US  - United States
Country Code Resolution Method                  : Proximity
C9800-L#
```

5. **Through Migration** – APs migrated from Meraki Dashboard will retain the country code they were operating in.

   For Greenfield customers, where 1) there are no legacy AP deployments, 2) deployment restrictions that makes it difficult to obtain GPS/GNSS signal and 3) easy workflow of migrating the APs to WLC mode for Day 0 and obtain country information, it's recommended to use the Migration method. Meraki dashboard determines where the APs are located, and sets the country code accordingly.

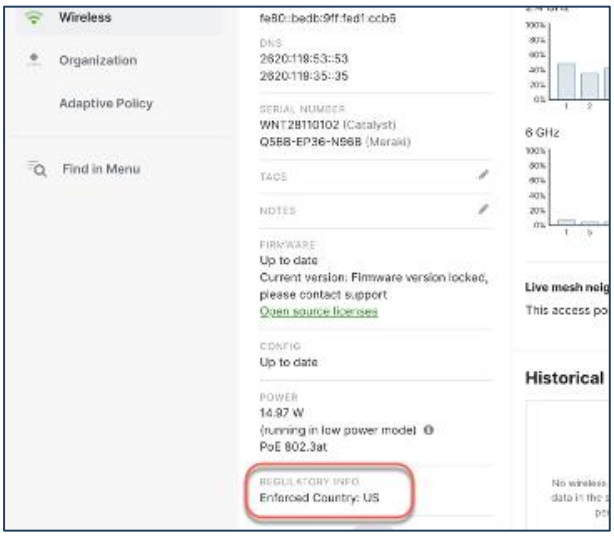


Figure 11. CW917x APs: Geolocation through Migration using Cisco Meraki Dashboard

The workflow steps were explained in the earlier section of Day 0 Workflow → Intent: Onboard to Catalyst Wireless LAN Controller → Option 1.

APs migrated through Migration method, will have the Country Code Resolution Method set as Installed via Meraki Dashboard.

```
C9800-L#show ap name Wi-Fi7-AP-B2E0 config general | inc Country
Country Code                                    : US
Regulatory Domain Allowed by Country            : 802.11bg:-A  802.11a:-AB 802.11
6GHz:-B
AP Country Code                                 : US  - United States
Country Code Resolution Method                  : Installed via Meraki Dashboard
C9800-L#
```

6. **Regulatory Activation File** – Download a Regulatory Activation File (RAF) from Meraki Dashboard, that can be installed on WLC.

   For Air gapped deployments, where there is no way to obtain GPS/GNSS signal, no legacy APs present in the network and where the APs cannot reach the cloud due to policy restrictions by the organization, the country code can be obtained in a manual way through Regulatory Activation File from the Meraki Dashboard.

   The workflow for Regulatory Activation File is as follows

   1. Claim order or Cloud ID in the Meraki Dashboard
   2. Assign AP to a network. AP does "**not**" have to connect to dashboard.
   3. Generate Regulatory Activation File (RAF)
   4. Copy RAF to WLC and install it.

   Note: The entire process can be automated via API and scripting.

   The file contains information for all networks that the current user has write permission to.

The RAF can be generated from Network Wide → Configure → General → Regulatory Info in the Meraki Dashboard. This will generate a “json” file.

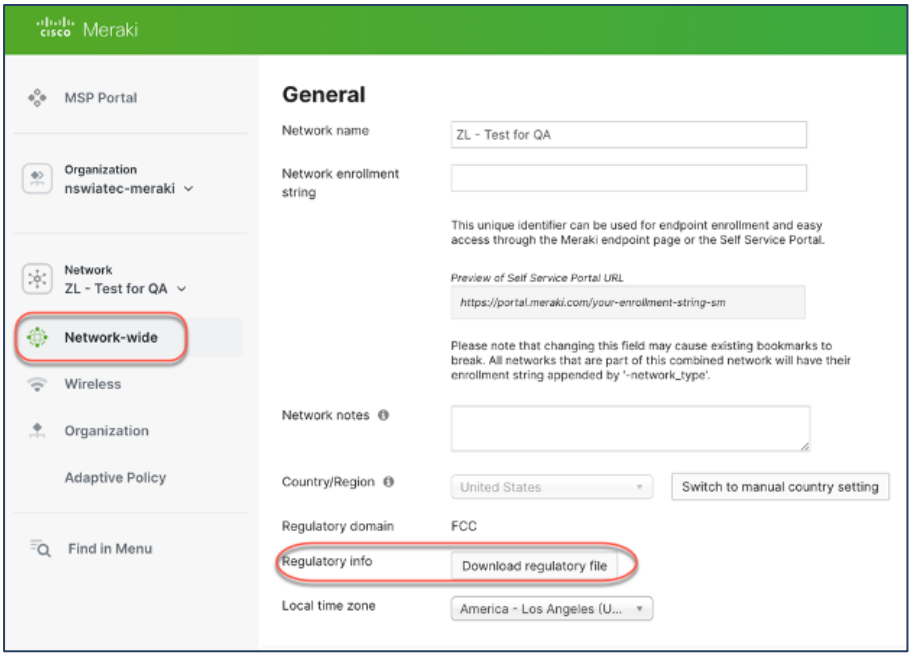
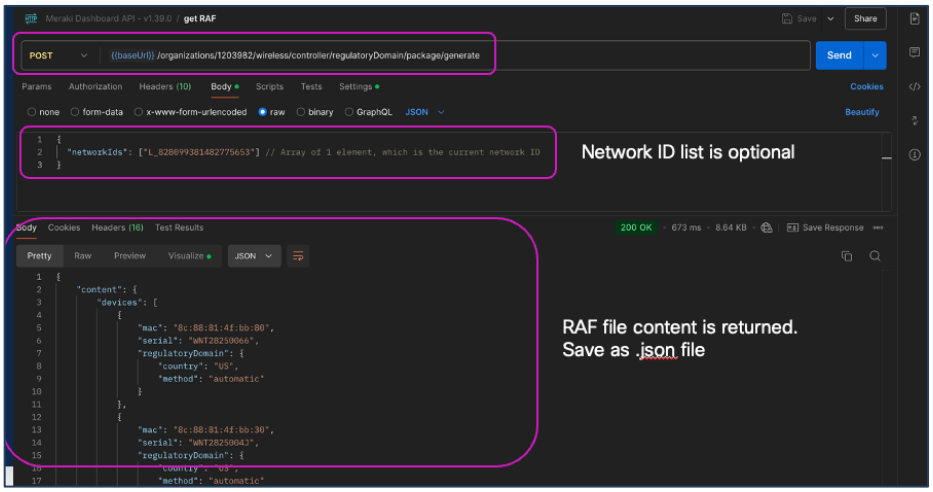
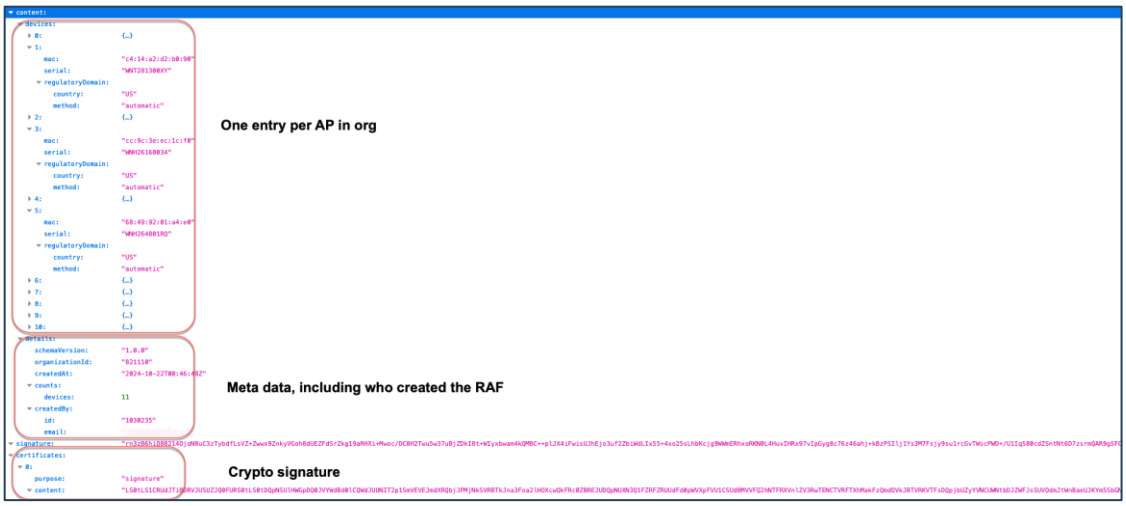


Figure 12. **Generate Regulatory Activation File (RAF) using Cisco Meraki**

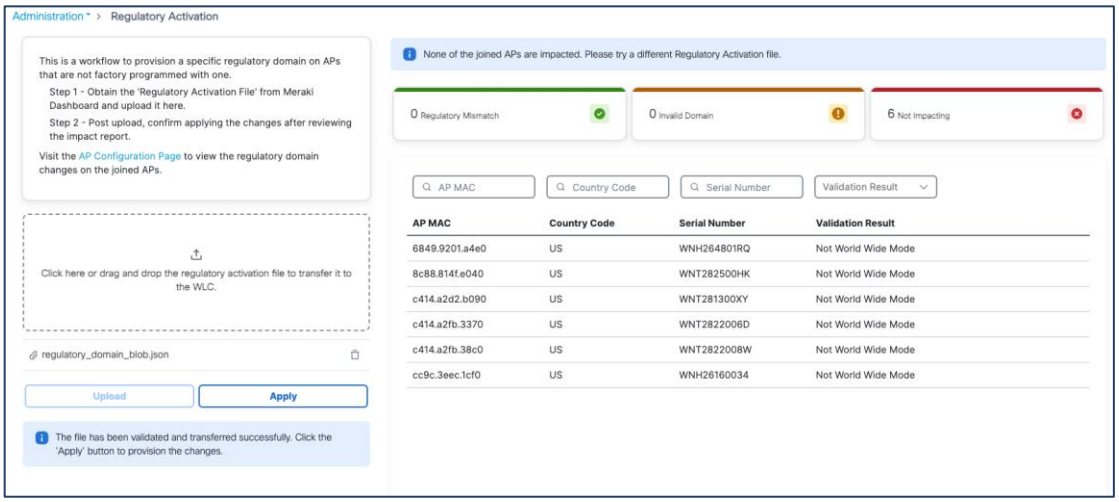
RAF Generation via API:

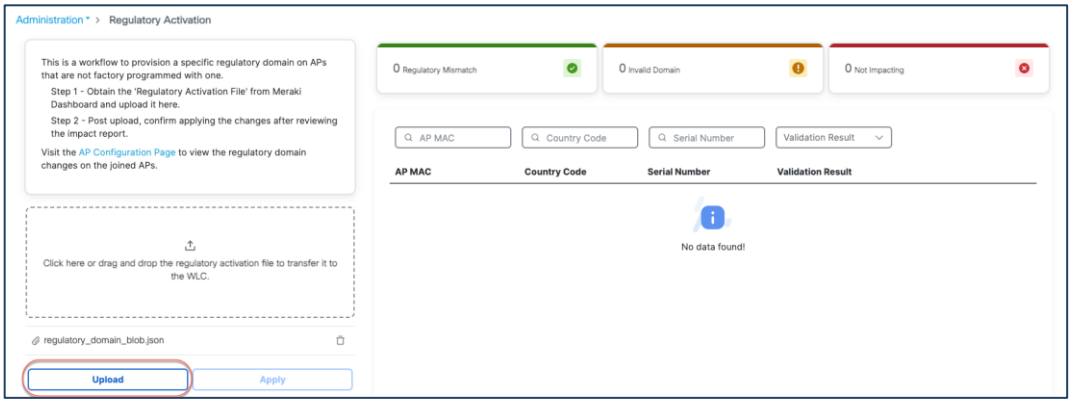


Example of RAF content:



Upload the RAF “json” file in the WLC from Adminstration → Regulatory Activation





Once uploaded, hit the Apply button. This will apply the country code to the applicable APs that have joined and any new APs that will join the WLC. The APs that have joined the controller and in world wide mode, will undergo a reload.

CLI command to show AP regulatory activation details:

```
C9800-L#show ap regulatory activation ?
```

```
  all  Show AP regulatory activation details for all APs
  mac  Show AP country mapping details of particular AP
all

C9800-L#show ap regulatory activation all
Regulatory Activation file Meta-data
------------------------------------
Date Created     : 2024-10-22T00:40:06Z
Created By       : xxx@email.org
Device count     : 11
Organization Id  : 821110

AP MAC              Serial Number      Country code
-----------------------------------------------------
6849.9201.a4e0       WNH264801RQ          US
6849.927a.4490       KWC271505U1
8c88.814f.e040       WNT282500HK          US
c414.a2d2.b090       WNT281300XY          US
c414.a2fb.04c0       WNT2820002R
c414.a2fb.3370       WNT2822006D          US
c414.a2fb.38c0       WNT2822008W          US
cc9c.3ee7.82b0       WNH260700TW
cc9c.3ee8.75c0       WNH261600HD
cc9c.3eec.1cf0       WNH26160034          US

AP MAC              Serial Number      Country code
-----------------------------------------------------
e0cb.bc97.0f87
```

CLI command to apply and clear the AP regulatory activation:

```
C9800-L#ap regulatory activation ?
  apply  Apply regulatory domain configuration
  clear  Clear AP mac to country mapping records
  file   Regulatory domain configuration file
```

Factory Reset

The AP can be factory reset to Out-of-Box, Day 0 Mode using 1) the reset button on the AP 2) through AP CLI.

Factory Reset via reset button on AP

To factory reset, perform the following steps

1. Unplug AP

2. Hold reset PIN
3. Power on AP
4. Hold until LED changes according to the table below.

Reset Option	Reset pin hold time	LED Status
1. Mode indication	~ 5 sec	• Blink green = Meraki Mode • Blink blue = Catalyst Mode
2. Config reset	> 10 sec	Solid white
3. Full reset (maintains management mode)	> 20 seconds	Orange
4. FIPS reset (Catalyst mode only)	> 30 seconds	Solid red
5. Factory reset (back to global use AP onboarding)	> 60 seconds	Solid pink
6. Abort reset	> 90 seconds	NA

Console now outputs the options, and counts.

```
Reset button is pressed. Mode = Catalyst
Keep the button pressed for > 10 seconds for config reset
Keep the button pressed for > 20 seconds for full reset
Keep the button pressed for > 30 seconds for FIPS reset
Keep the button pressed for > 60 seconds for deep (factory) reset

Waiting for the button to be released:    7 seconds
```

This is a unified behavior across Catalyst and Meraki Mode. No change for customers used to Catalyst APs, but different for Meraki.

Factory Reset through AP CLI

CLI to erase config, country and factory-reset

```
AP-B2E0#capwap ap erase
  all            Erase all AP config except country code
  country        Reset country code on AP.
  factory-reset  Factory reset the AP.
  static-ip      Erase static IP/DNS config
  static-ipv6    Erase static IPv6/DNS config
AP-B2E0#
```

The factory-reset option fully wipes and brings the AP to Out-of-Box, Day 0 Mode.

The country erase option clears the country config alone and can be used if the AP's location changes to a different country or re-evaluate its country.

Important Links

1. CW9178I Hardware Installation Guide
2. CW9176I Hardware Installation Guide
3. CW9176D1 Hardware Installation Guide
4. CW9178I AP Deployment Guide
5. CW9176 AP Deployment Guide