Configure Mesh on Catalyst 9800 Wireless LAN Controllers

Contents

Introduction

This document describes a basic configuration example on how to join a mesh Access Point (AP) to the Catalyst 9800 Wireless LAN Controller (WLC)

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Catalyst Wireless 9800 configuration model
- Configuration of LAPs
- Control And Provision of Wireless Access Points (CAPWAP)
- Configuration of an external DHCP server
- Configuration of Cisco switches

Components Used

This example uses lightweight access point (1572AP and 1542) which can either be configured as a Root AP (RAP) or Mesh AP (MAP) to join to Catalyst 9800 WLC. Procedure is identical for 1542 or 1562 access points. The RAP is connected to theCatalyst 9800 WLC through a Cisco Catalyst switch.

The information in this document is based on these software and hardware versions:

- C9800-CL v16.12.1
- Cisco Layer 2 Switch
- Cisco Aironet 1572 Series Lightweight Outdoor Access Points for the Bridge section

- Cisco Aironet 1542 for the Flex+Bridge section

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Case study 1: Bridge Mode

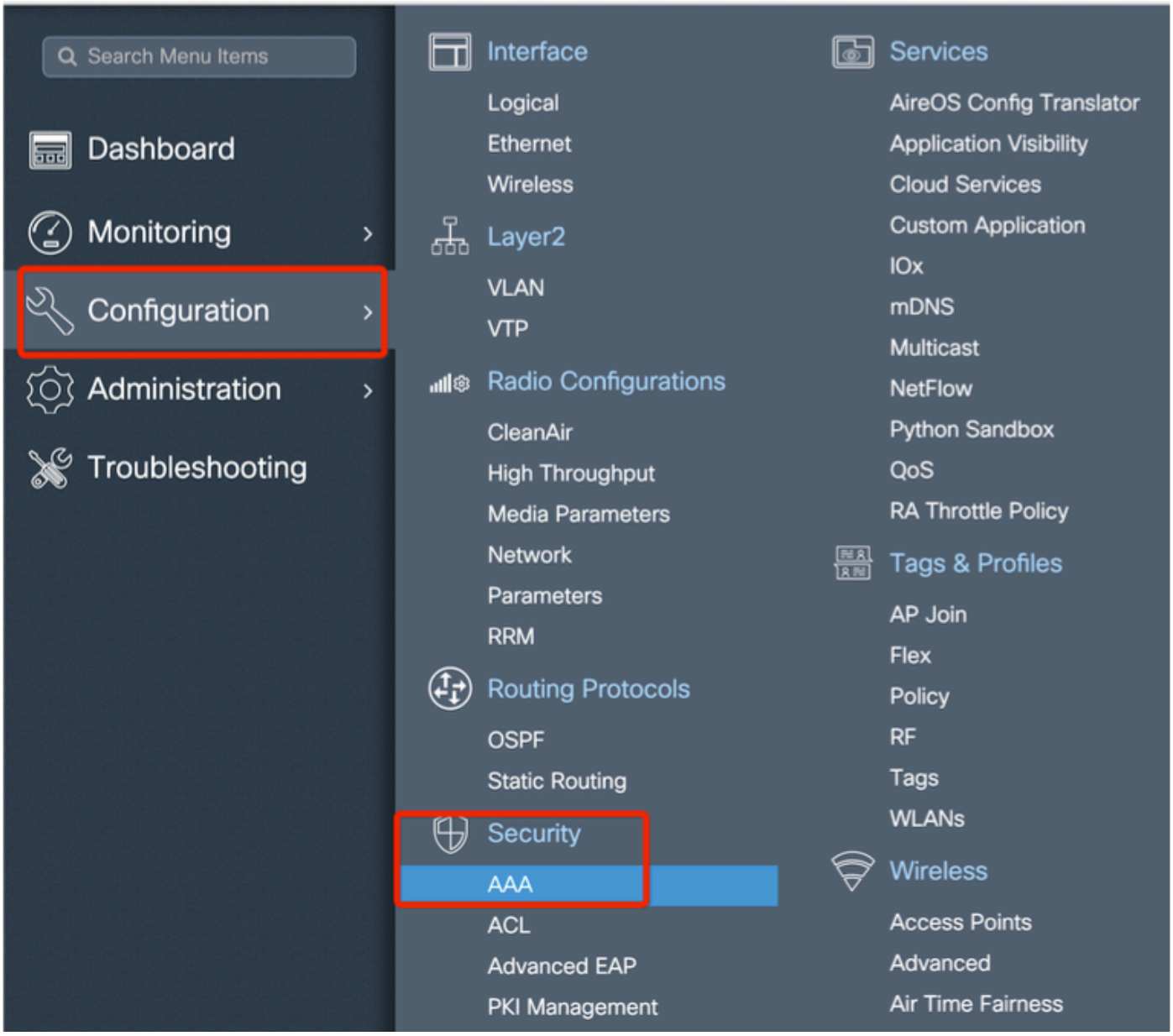
Configurations

A mesh AP needs to be authenticated for it to join the 9800 controller. This case study considers that you join the AP in local mode first to the WLC and then convert it to Bridge (a.k.a) mesh mode.

To avoid assignment of AP join profiles, use this example but configure the default aaa authorization credential-download method so that any mesh AP is allowed to join the controller.

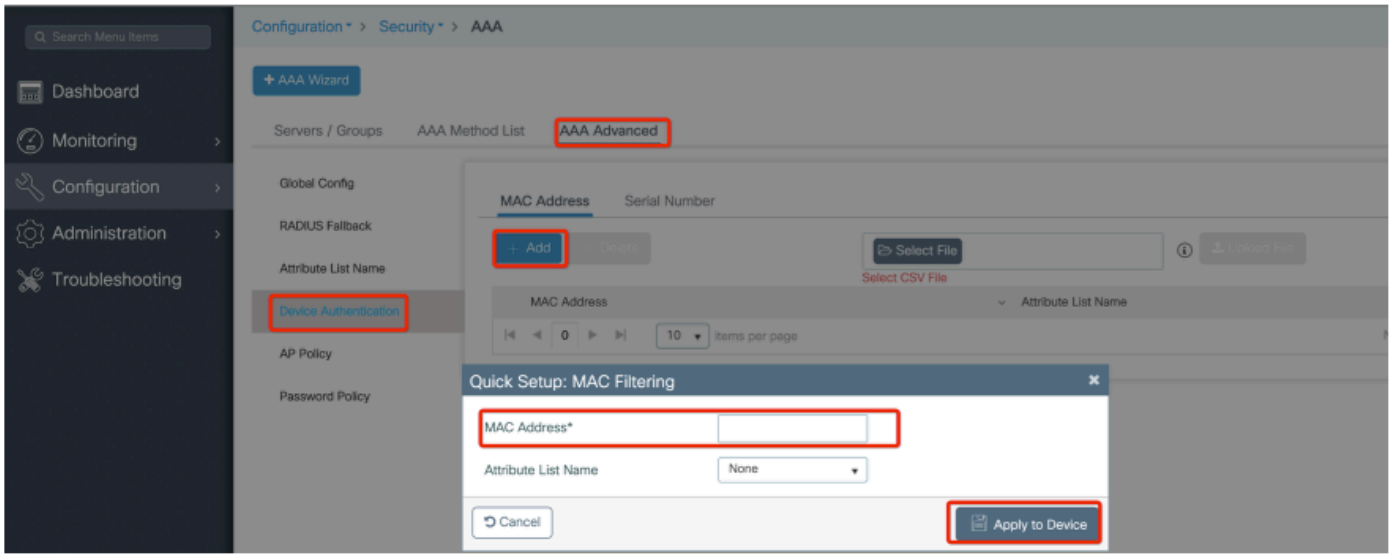
Step1: Configure RAP/MAP mac addresses under Device Authentication.

Go to **Configuration > AAA > AAA Advanced > Device Authentication** .



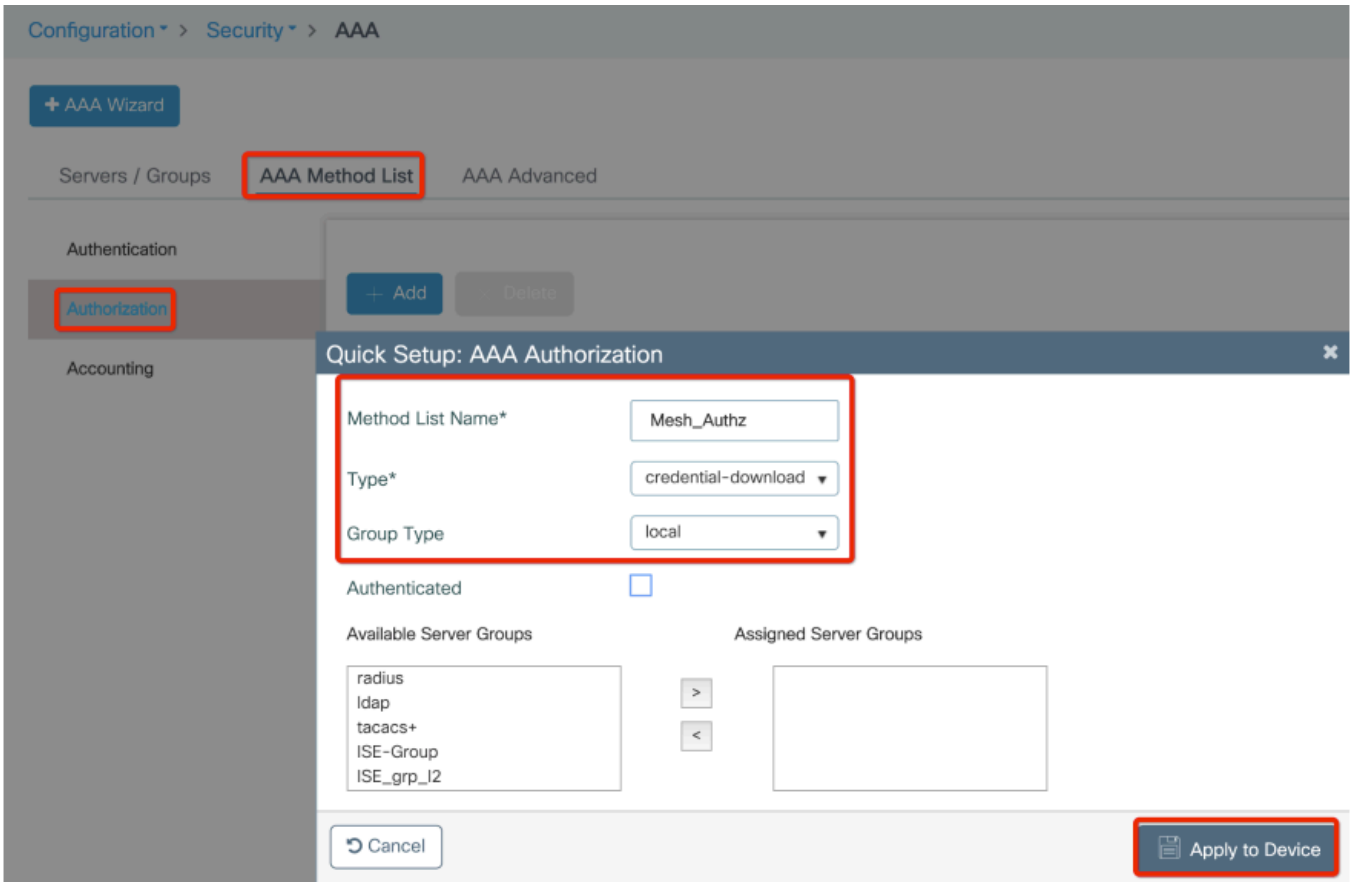
Add the Base Ethernet MAC Address of the mesh access points, add it without any special characters, without '.' or ':'

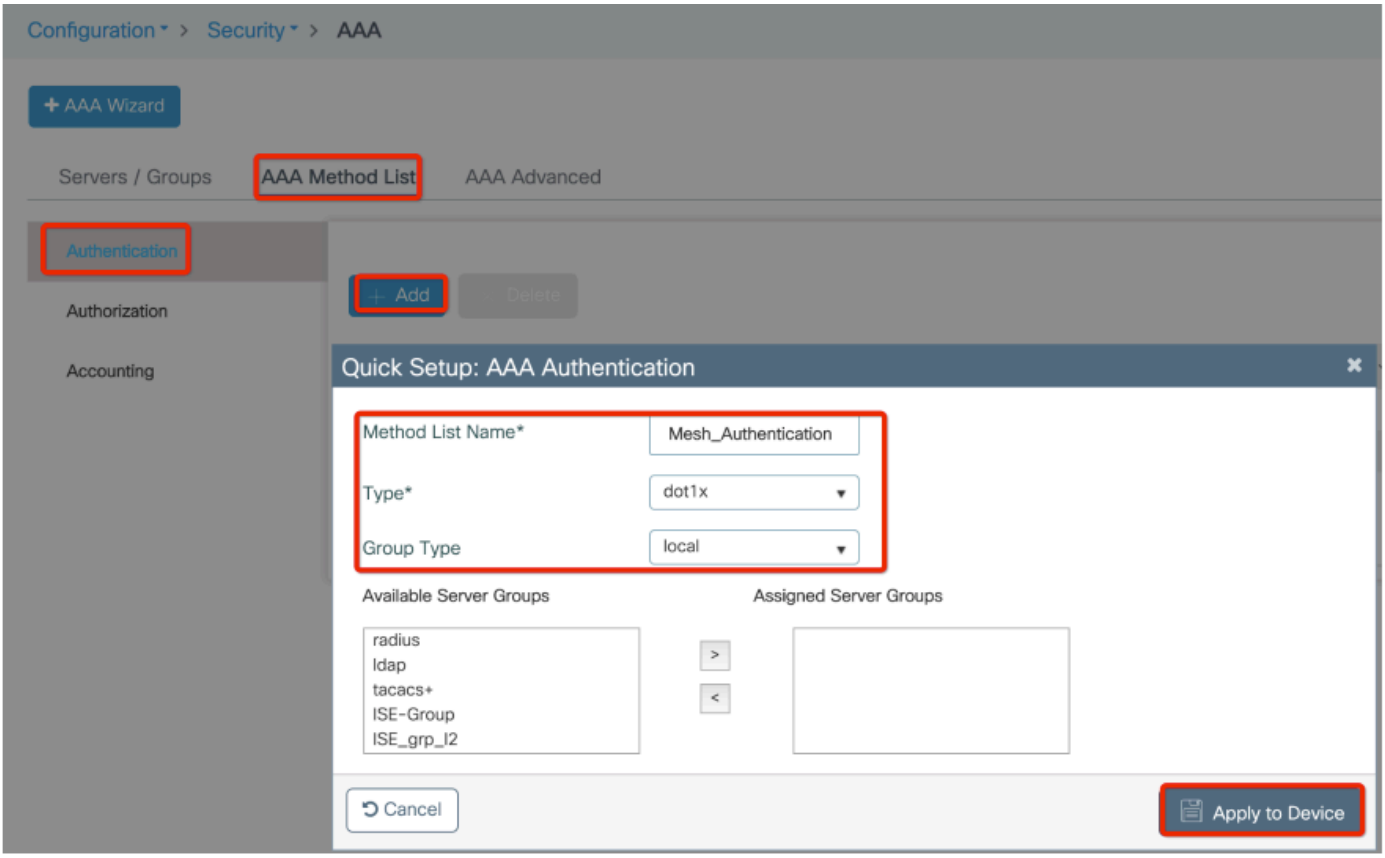
Important: As of 17.3.1 release, if any mac address delimiters like '.', ':' or '-' are added, the AP is not able to join. There are currently 2 enhancements opened for this: Cisco bug ID CSCvv43870 and Cisco bug ID CSCvr07920. In the future, 9800 accepts all mac address formats.



Step 2: Configure the authentication and authorization method list.

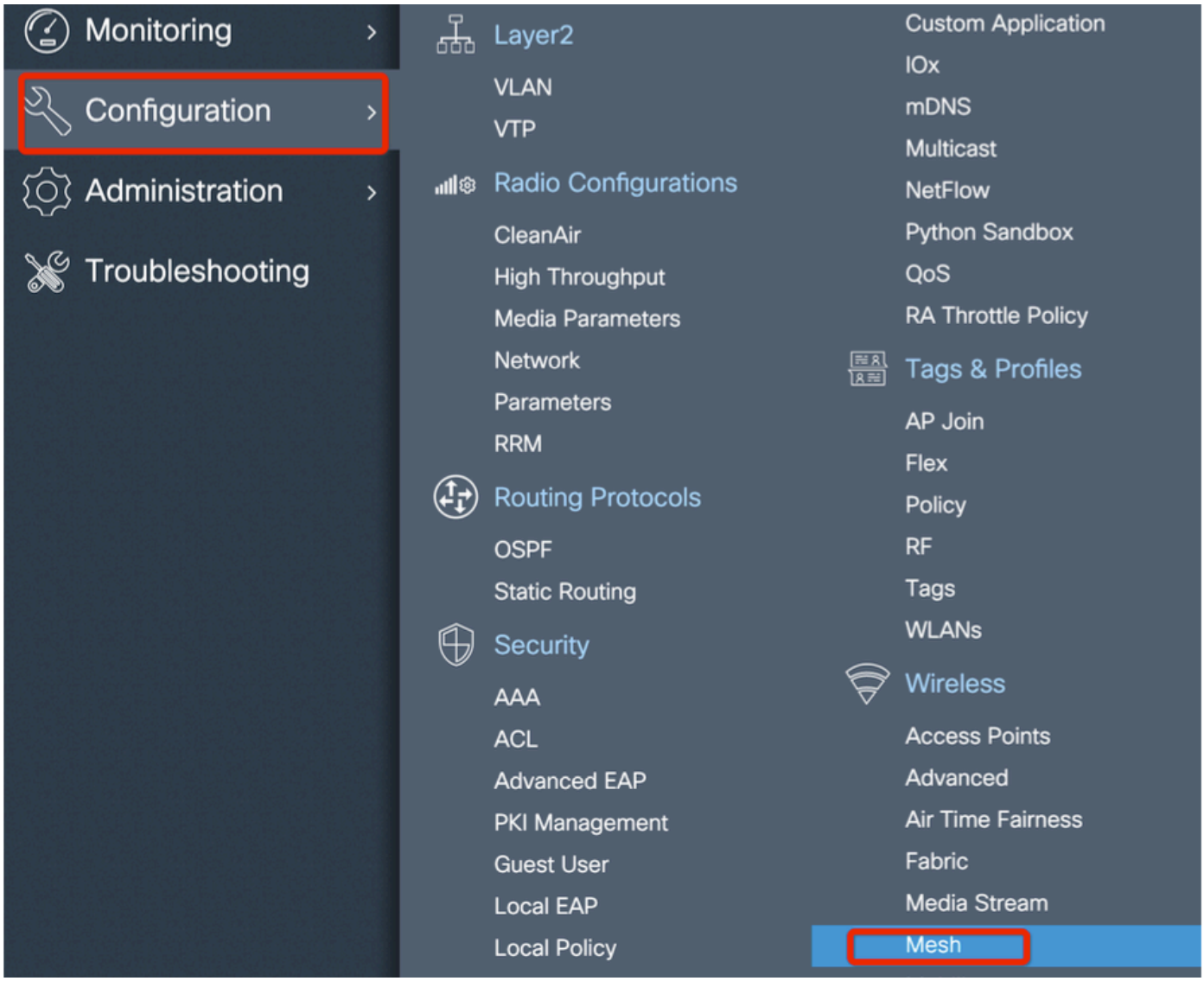
Go to **Configuration > Security > AAA > AAA Method list > Authentication** and create the authentication method list and authorization method list.



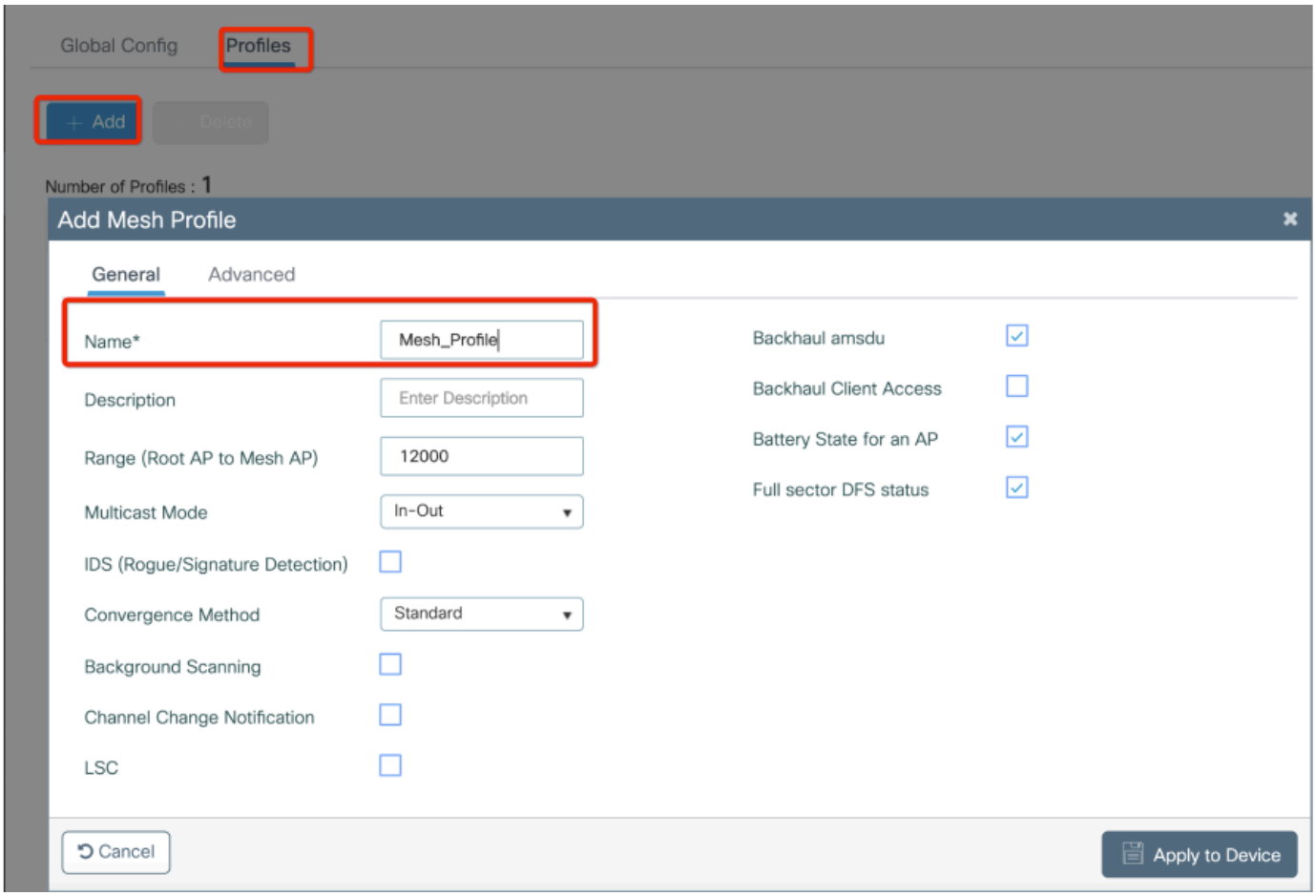


Step 3: Configure the global mesh parameters.

Go to **Configuration> Mesh> Global** parameters. Initially, we can keep these values to default.

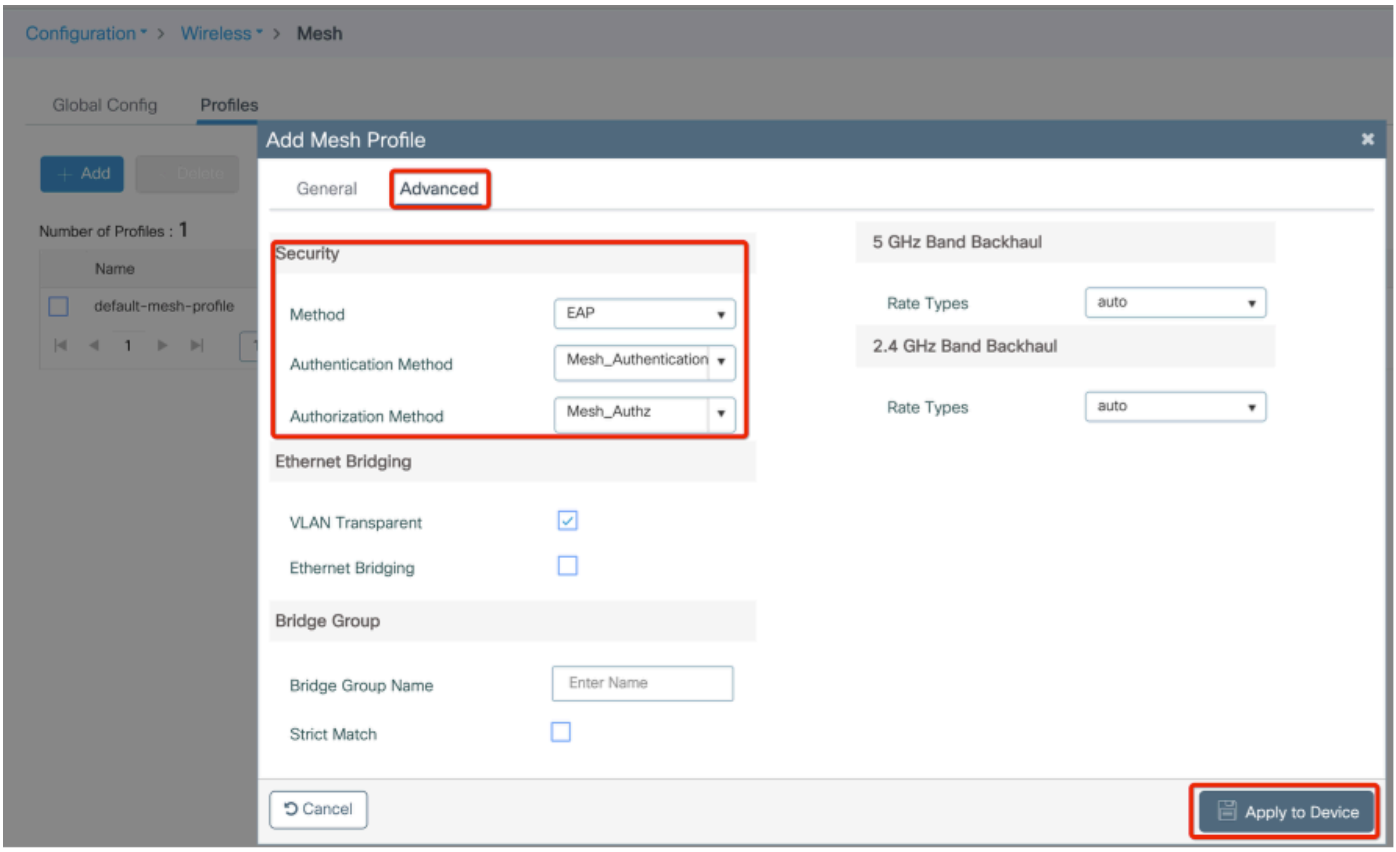


Step 4: Create a new Mesh Profile under **Configuration > Mesh > Profile > +Add**

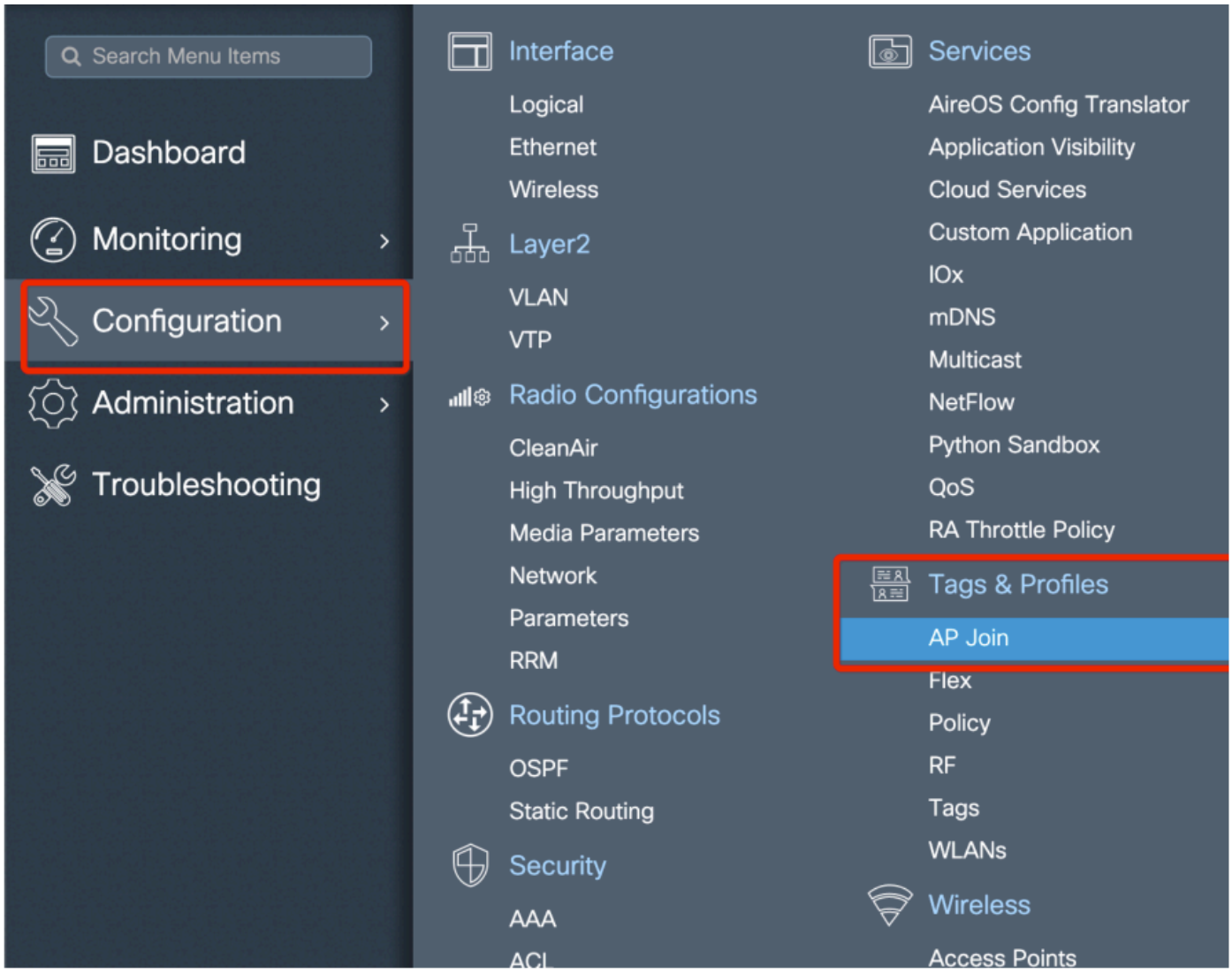


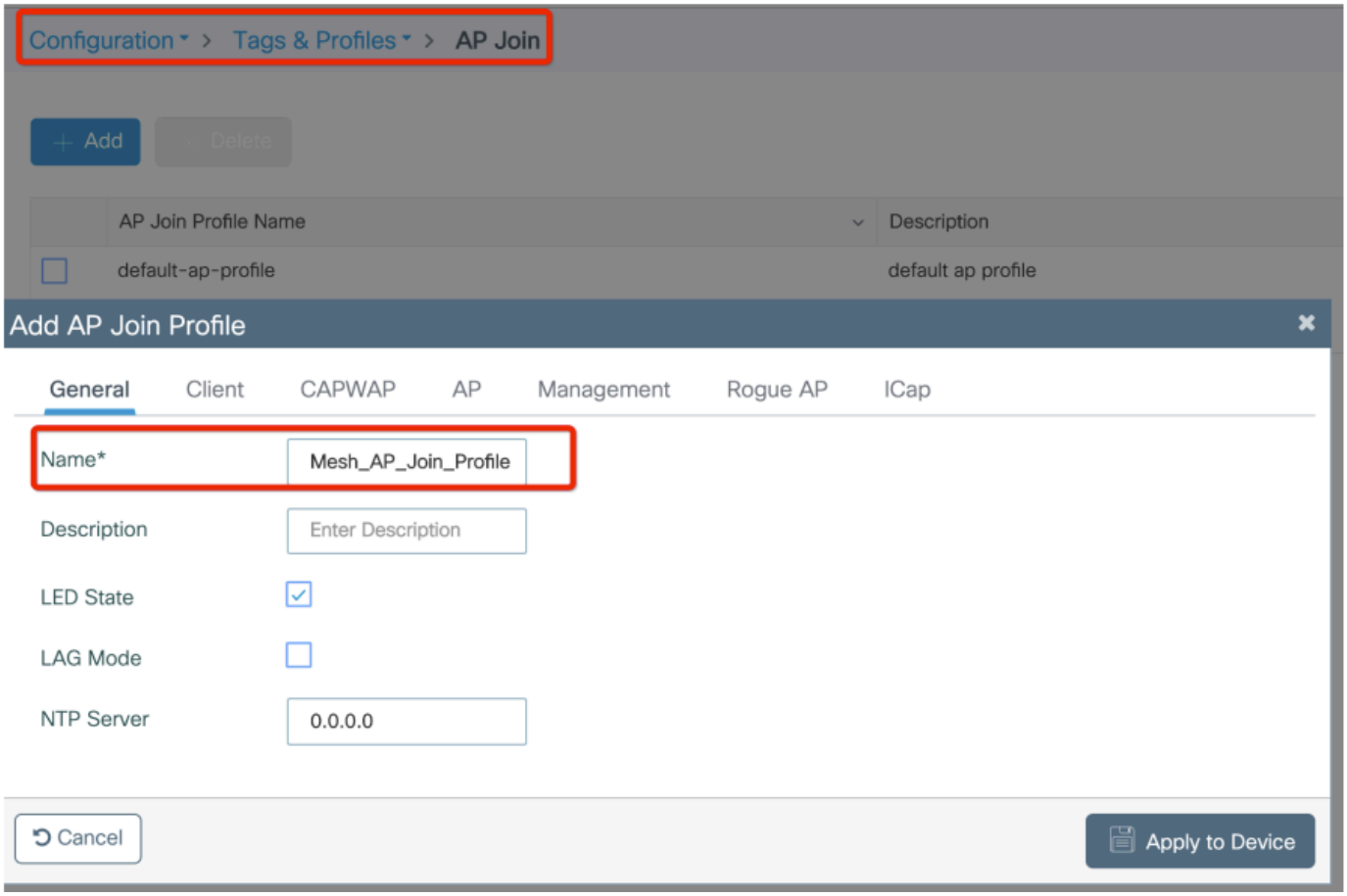
Click the created mesh profile to edit the General and Advanced settings for the mesh profile.

In the diagram as shown we need to map the authentication and authorization profile created before to Mesh profie

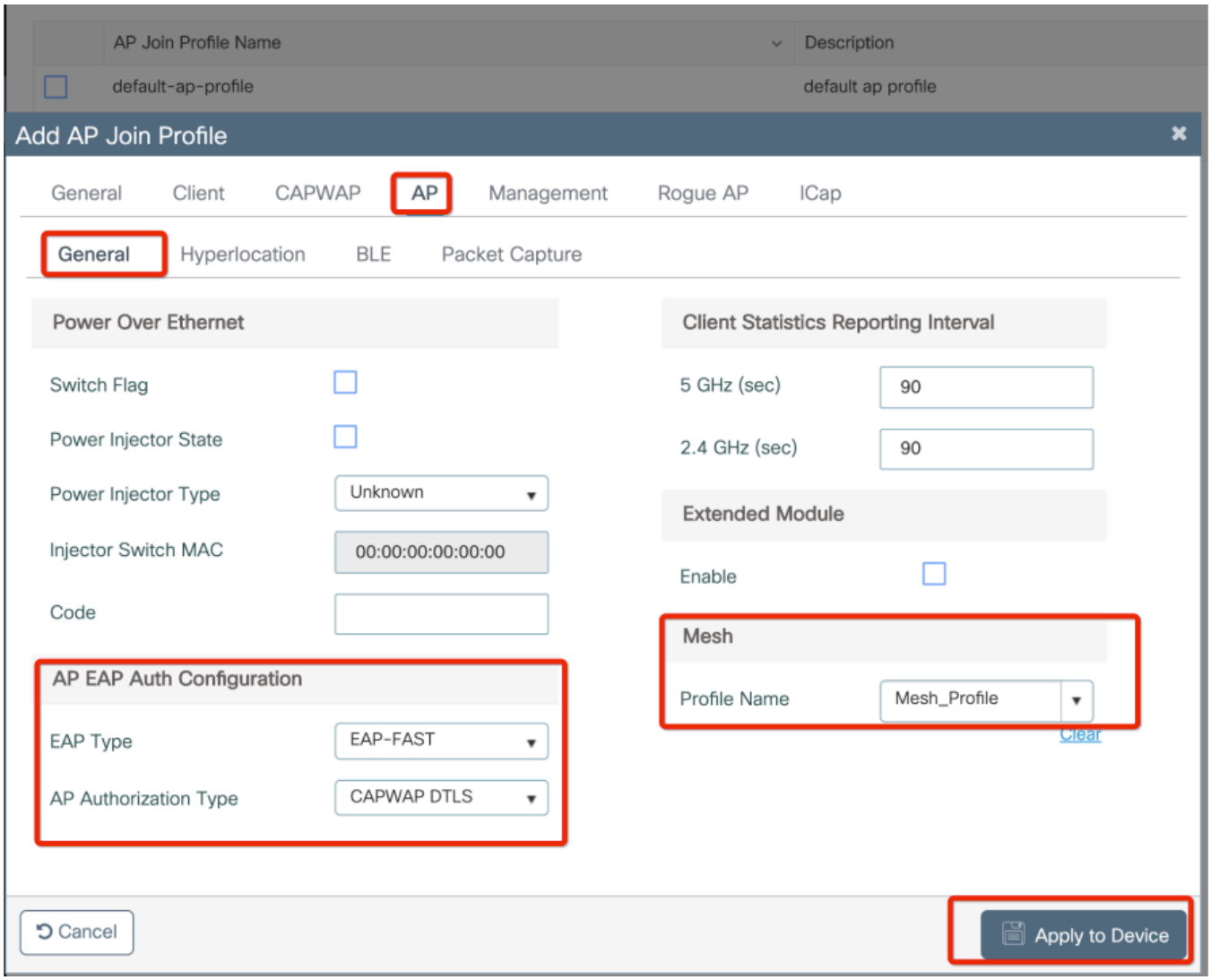


Step 5: Create a new AP join Profile. Go to **Configure > Tags and Profiles: AP Join.**

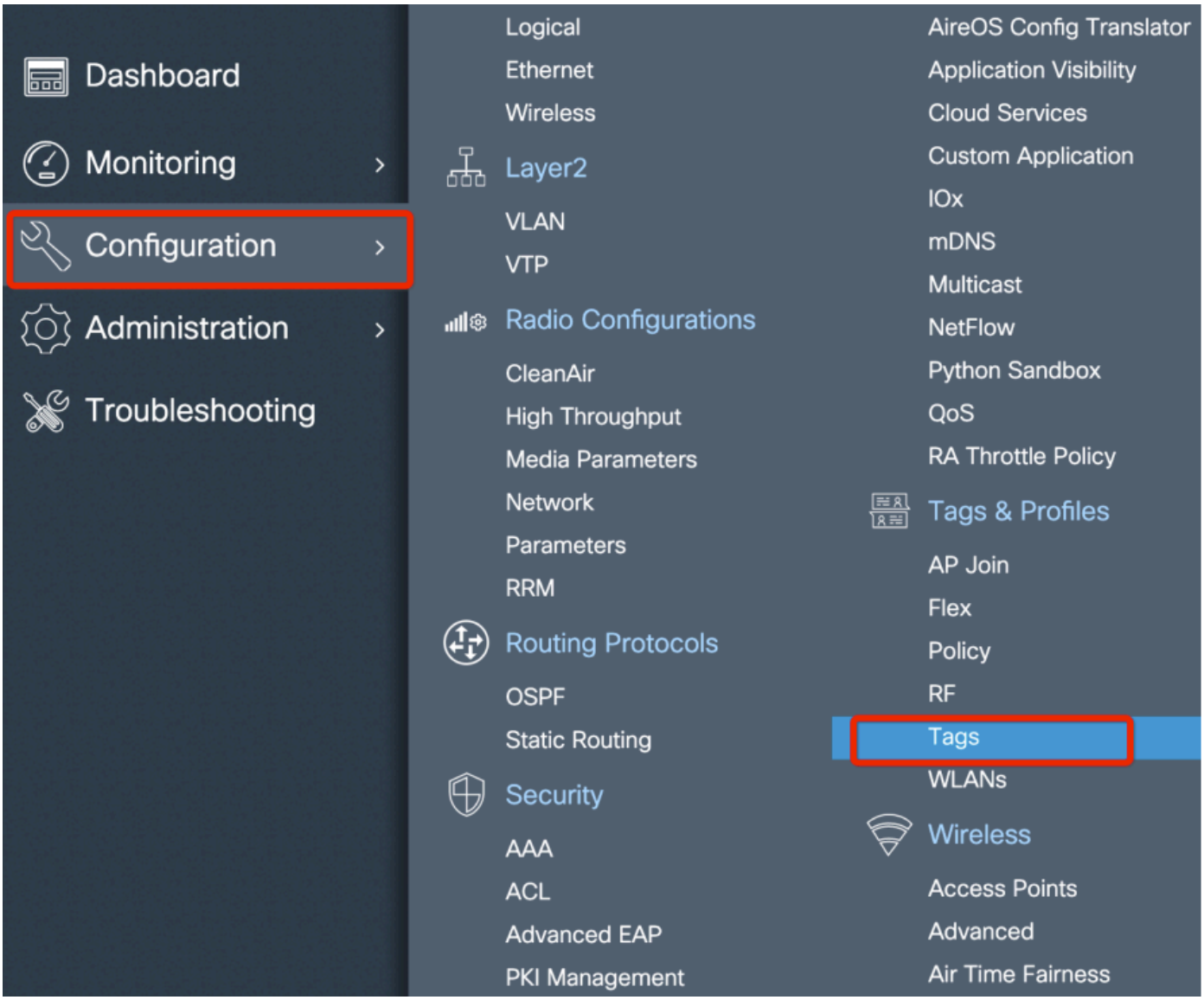

Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Interface
Logical
Ethernet
Wireless
Layer2
VLAN
VTP
Radio Configurations
CleanAir
High Throughput
Media Parameters
Network
Parameters
RRM
Routing Protocols
OSPF
Static Routing
Security
AAA
ACL
Services
AireOS Config Translator
Application Visibility
Cloud Services
Custom Application
IOx
mDNS
Multicast
NetFlow
Python Sandbox
QoS
RA Throttle Policy
Tags & Profiles
AP Join
Flex
Policy
RF
Tags
WLANs
Wireless
Access Points



Apply the previously configured Mesh Profile and configure the AP EAP auth:

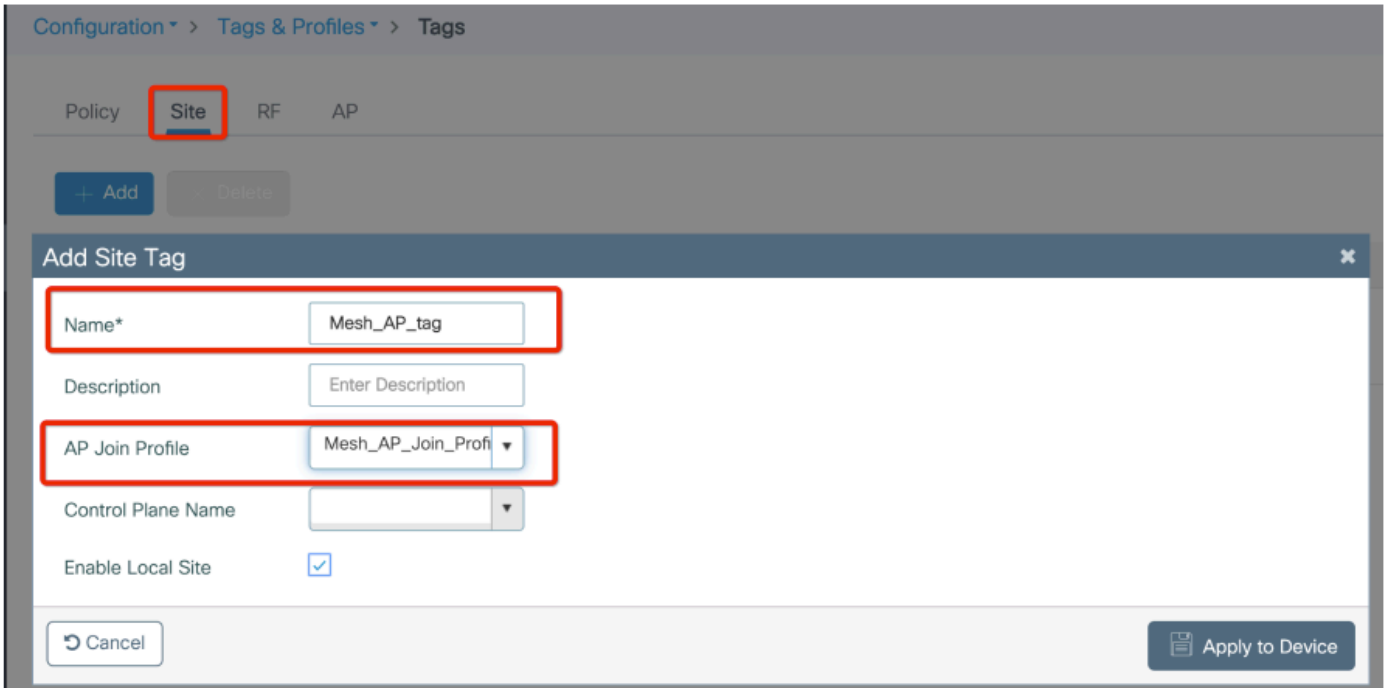


Step 6: Create a mesh location Tag as shown.

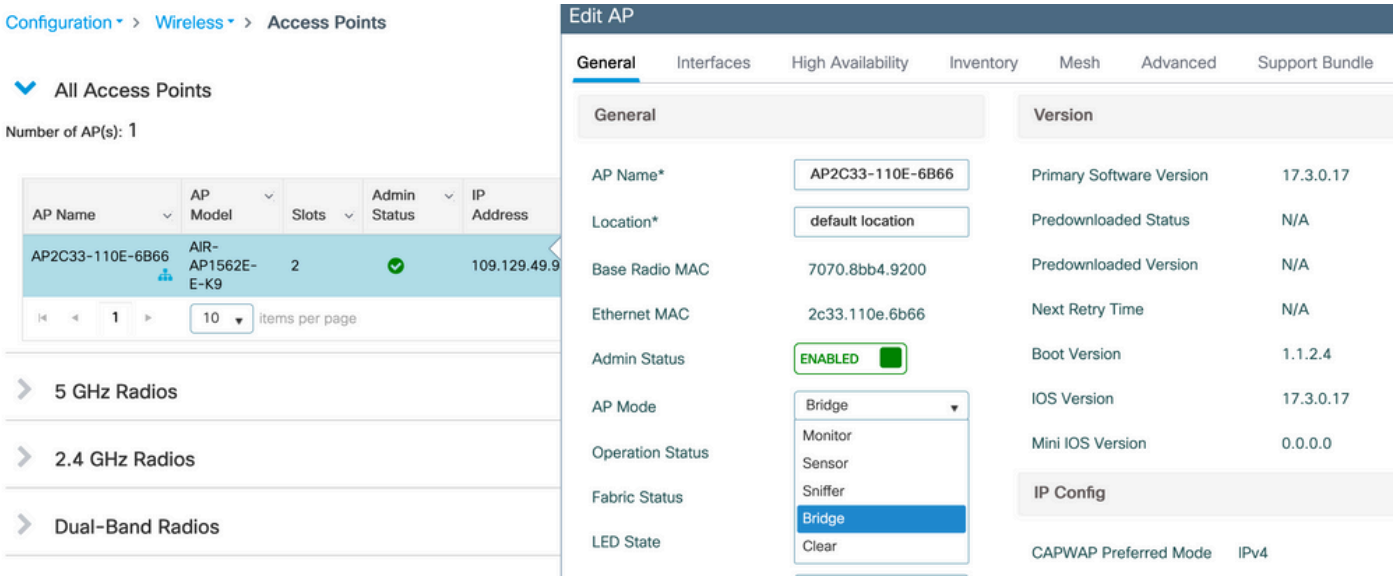


Configure Click the Mesh location TAG created in Step 6 to configure it.

Got to Site tab and apply the previously configured Mesh AP join Profile to it:



Step 7. Convert the AP to Bridge mode.



via CLI you can this commad on the AP :

```
capwap ap mode bridge
```

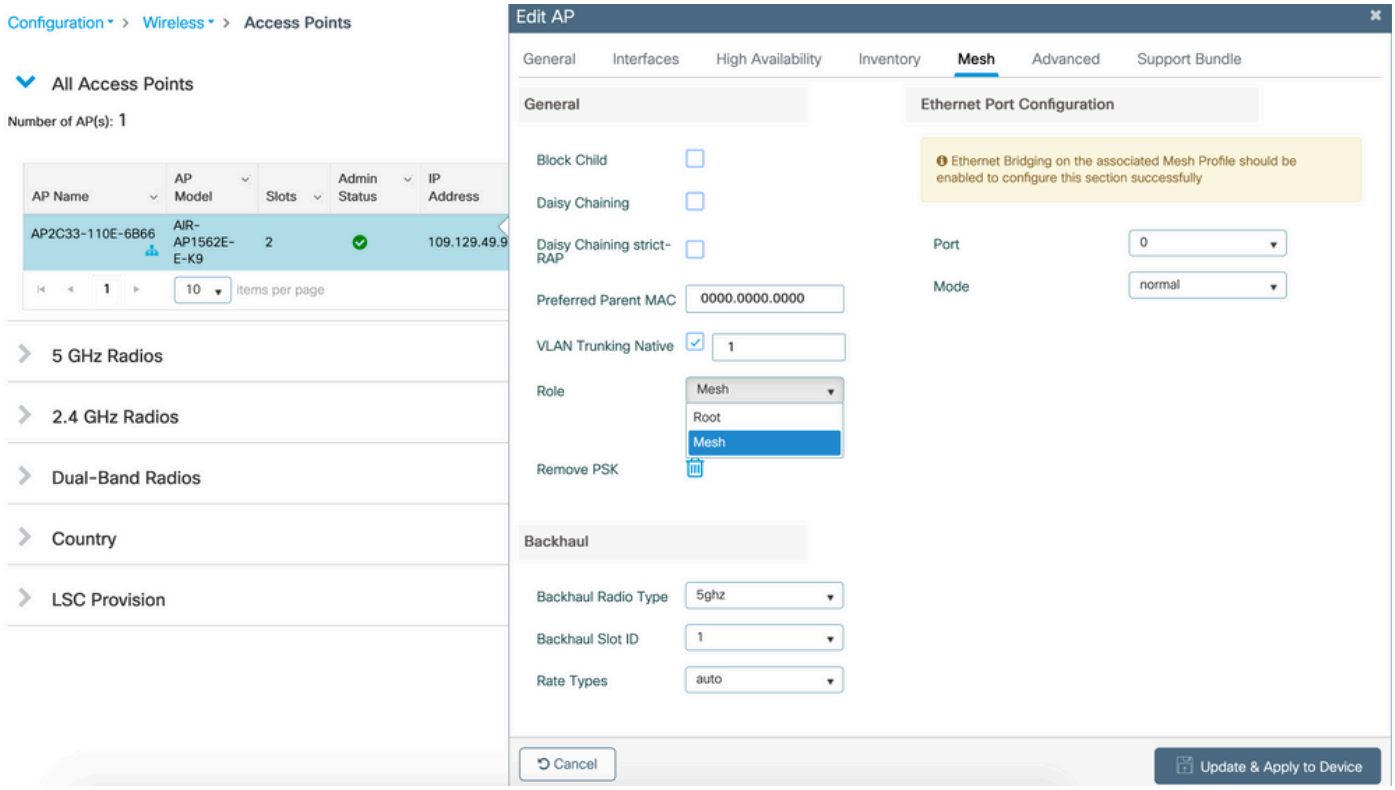
The AP reboots and join back as Bridge mode.

Step 8. You can now define the role of the AP : either root AP or mesh AP.

The root AP is the one with a wired connection to the WLC while the mesh AP joins the WLC via its radio which tries to connect to a root AP.

A mesh AP can join the WLC via its wired interface once it has failed to find a root AP via its radio, for provision purposes.

Do no forget to specify the trunk native vlan in the AP settings in case it is different from the default VLAN 1

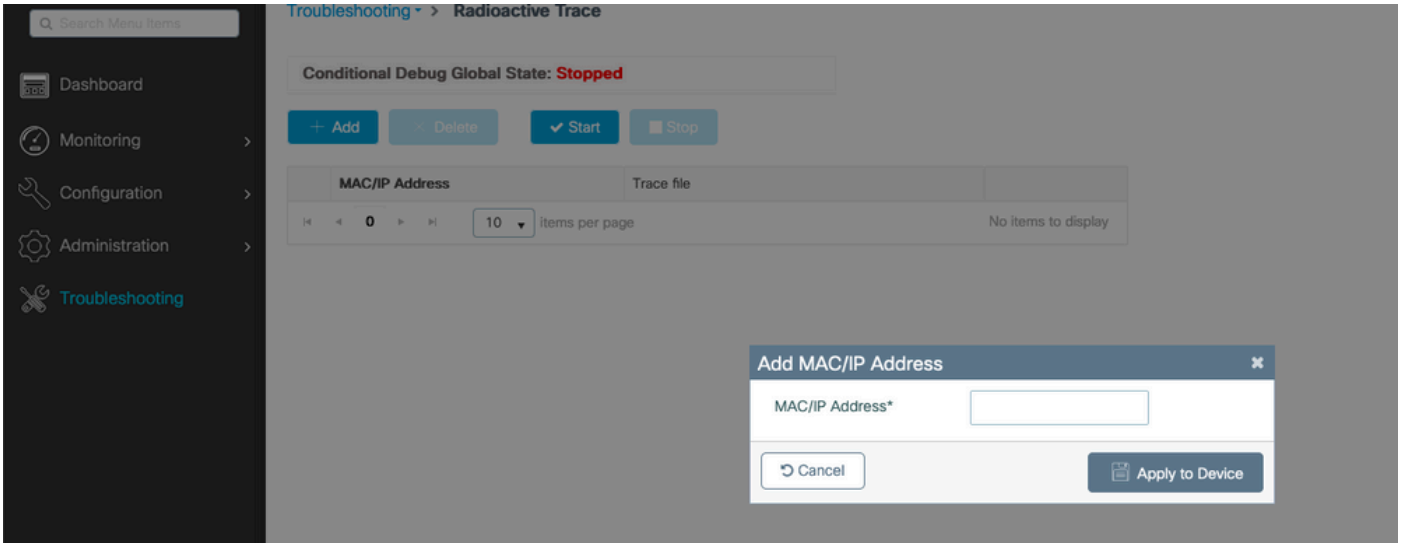


Verify

```
aaa new-model
aaa local authentication default authorization default
!
!
aaa authentication dot1x default local
aaa authentication dot1x Mesh_Authentication local
aaa authorization network default local
aaa authorization credential-download default local
aaa authorization credential-download Mesh_Authz local
username 111122223333 mac
wireless profile mesh Mesh_Profile
 method authentication Mesh_Authentication
 method authorization Mesh_Authz
wireless profile mesh default-mesh-profile
 description "default mesh profile"
wireless tag site Mesh_AP_Tag
 ap-profile Mesh_AP_Join_Profile
ap profile Mesh_AP_Join_Profile
 hyperlocation ble-beacon 0
 hyperlocation ble-beacon 1
 hyperlocation ble-beacon 2
 hyperlocation ble-beacon 3
 hyperlocation ble-beacon 4
 mesh-profile Mesh_Profile
```

Troubleshoot

In **Troubleshoot** > **Radioactive Trace** web UI page, Click **add** and enter the AP mac address.



Click **Start** and wait for the AP to try to join the controller again.

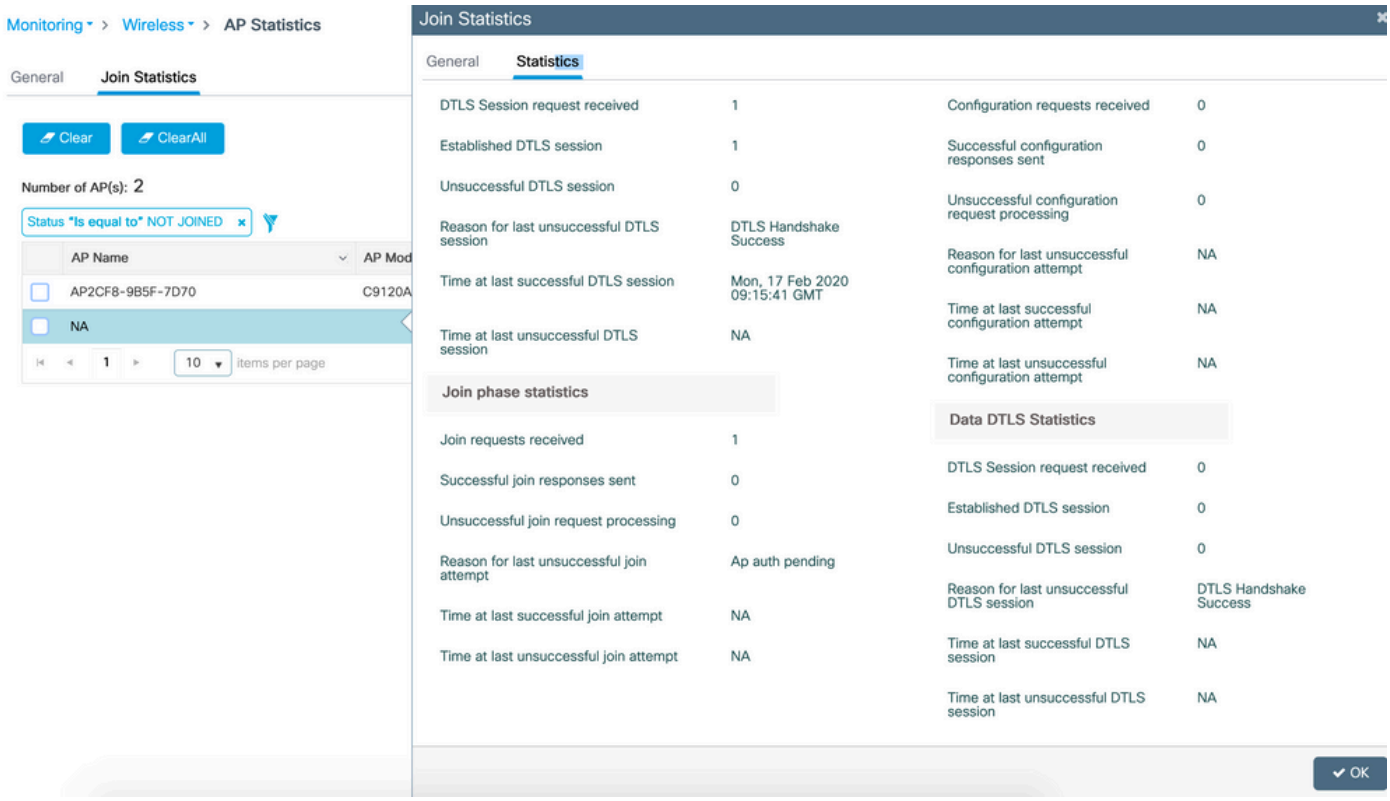
Once done, click **Generate** and chose a time period to collect the logs (last 10 or 30 minutes for example).

Click on the Trace file name to download it from your browser.

Here is an example of AP not joined because of the wrong aaa authorization method name was defined :

```
019/11/28 13:08:38.269 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [23388]: (info): DTLS record type: 23, appli
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (info): 00a3.8e95.6c40 Ap auth p
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): Failed to initialize auth
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): 00a3.8e95.6c40 Auth reque
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get wtp r
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get ap ta
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (ERR): Session-IP: 192.168.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (info): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.289 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [23038]: (debug): instance :0 port:38932MAC
```

The same can be seen more easily in the web UI dashboard when click on APs not joined. "Ap auth pending" is the hint which points towards the authentication of the AP itself:

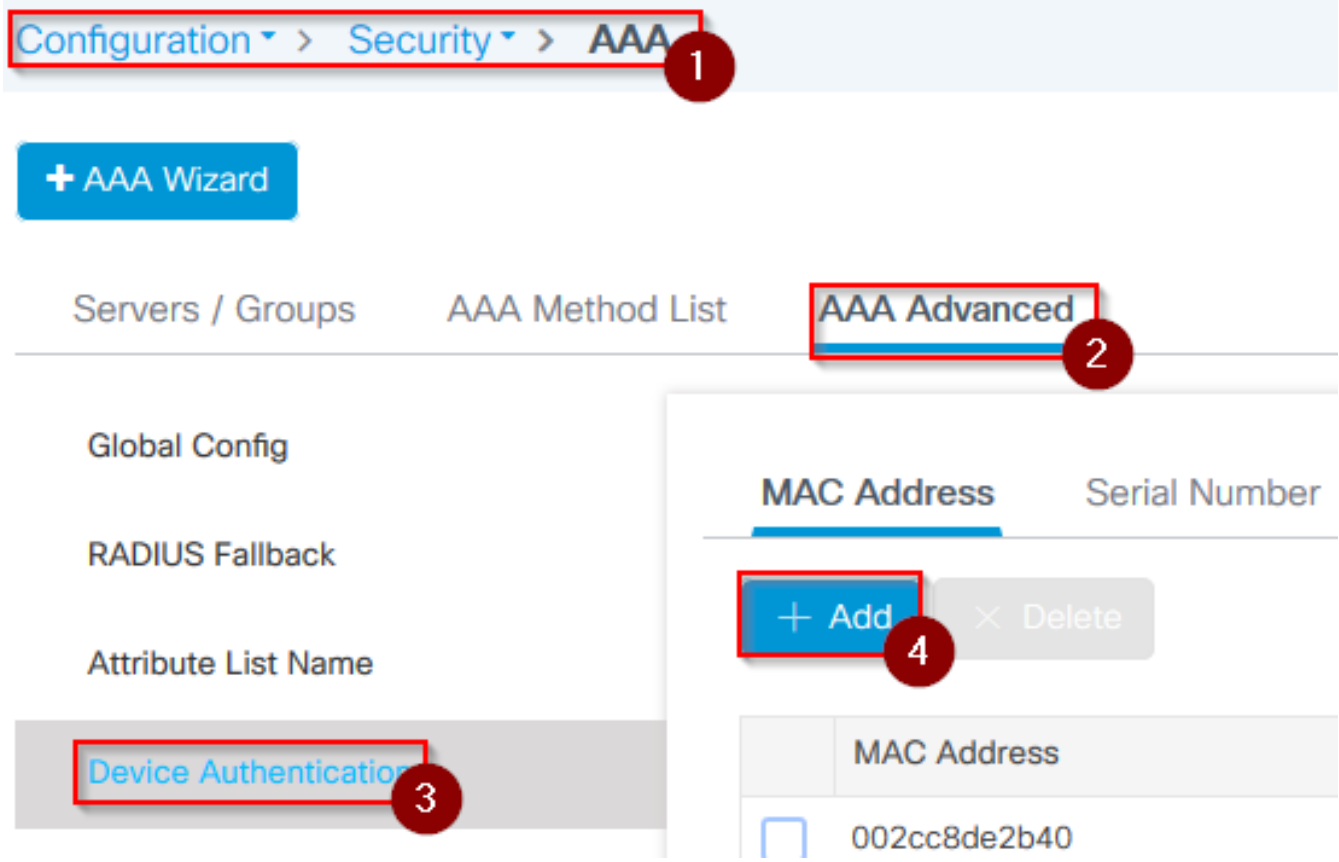


Case study 2 : Flex + Bridge

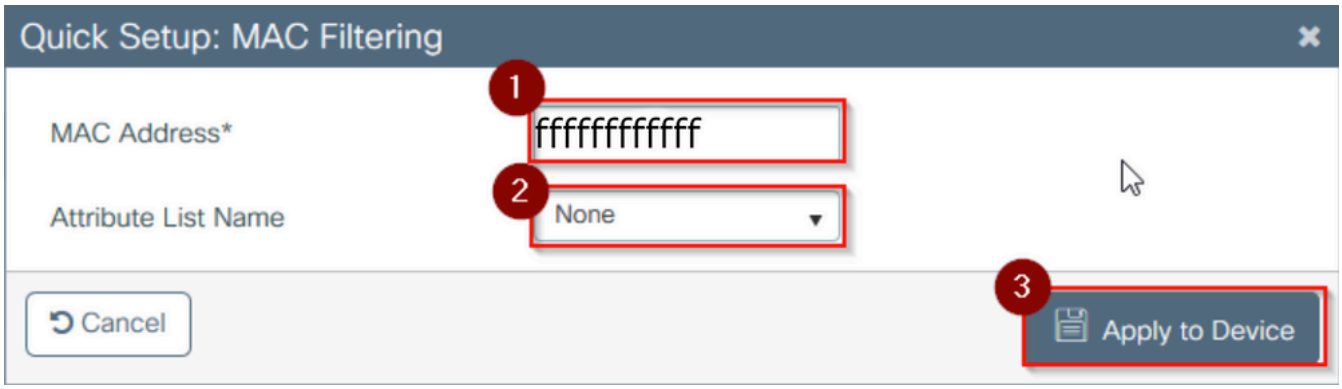
This section highlights the join process of a 1542 AP in Flex+bridge mode with EAP authentication done locally on the WLC.

Configure

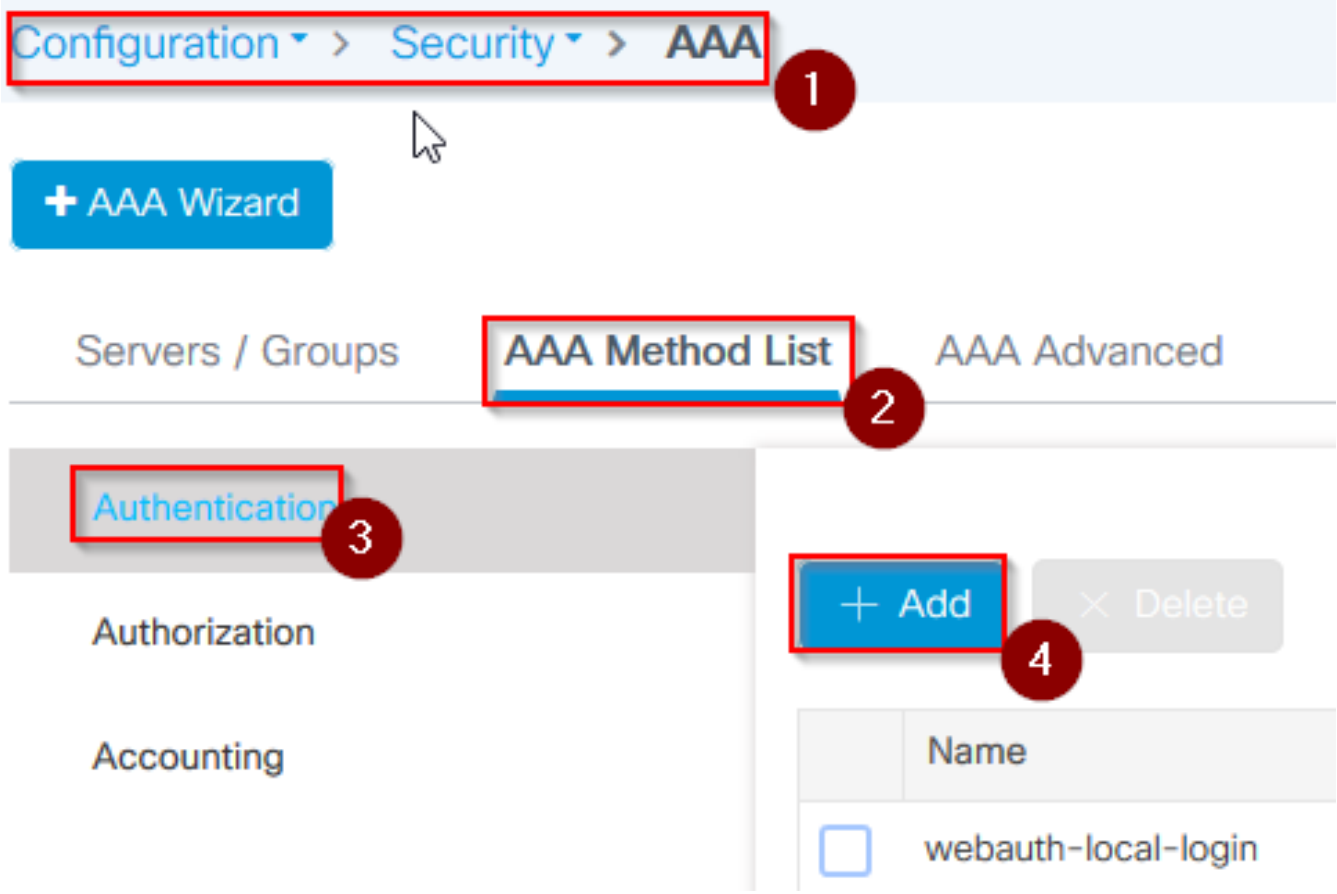
- Step 1. Navigate to **Configuration** > **Security** > **AAA** > **AAA Advanced** > **Device Authentication**



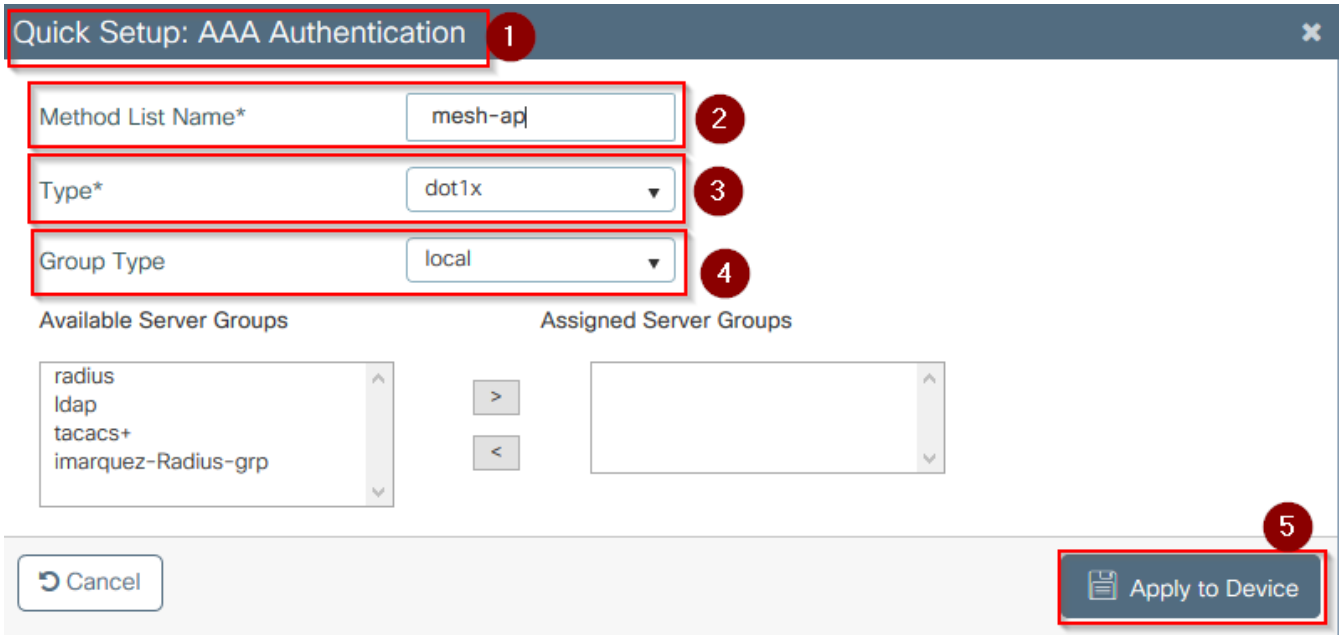
- Step 2. Select **Device Authentication** and select **Add**
- Step 3. Type in the Base Ethernet MAC address of the AP to join to the WLC, leave the **Attribute List Name** blank, and select **Apply to Device**



- Step 4. Navigate to **Configuration** > **Security** > **AAA** > **AAA Method List** > **Authentication**
- Step 5. Select **Add**, the **AAA Authentication** pop-up appears

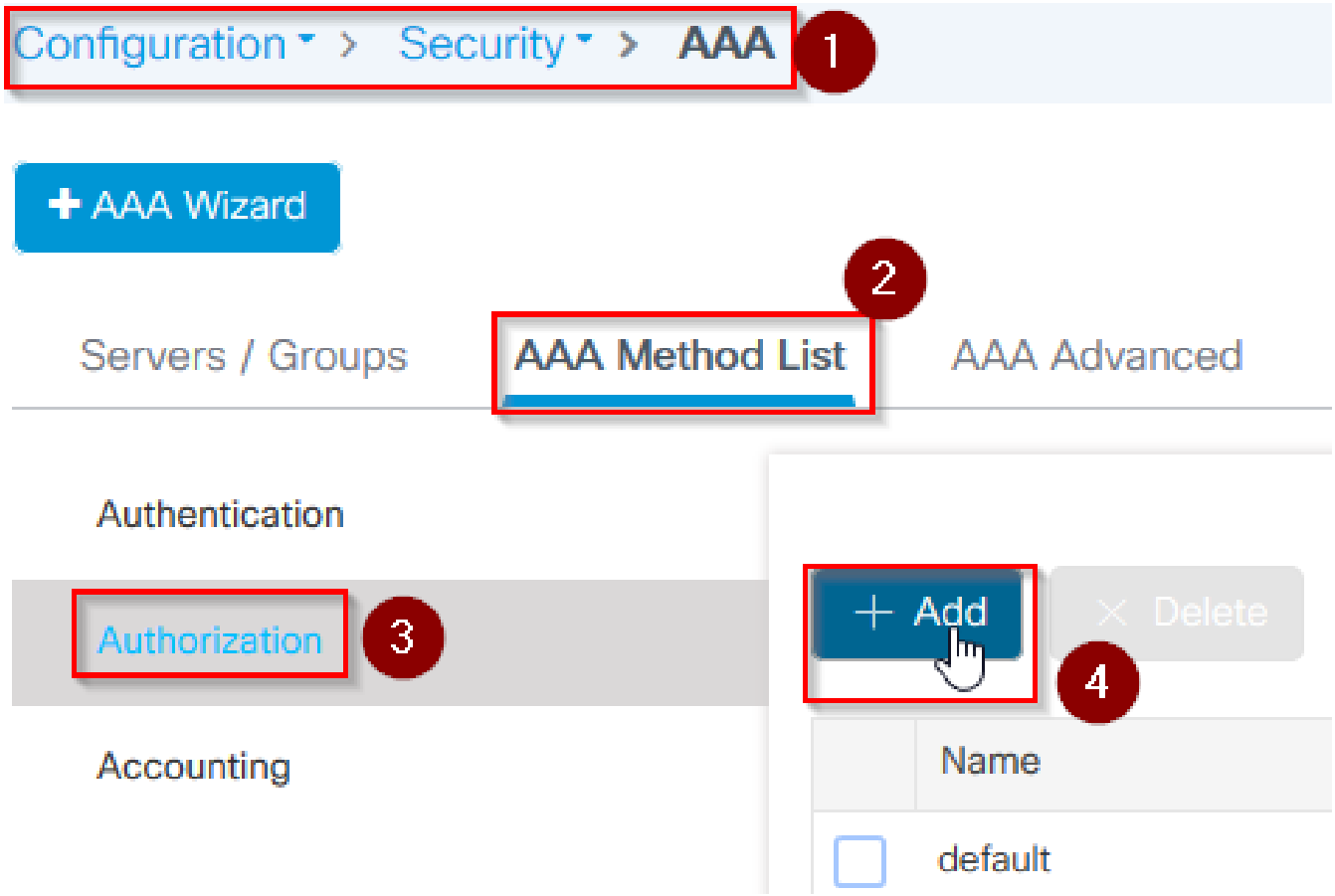


- Step 6. Type in a name in the **Method List Name**, select **802.1x** from the **Type*** drop-down and **local** for the **Group Type**, finally select **Apply to Device**

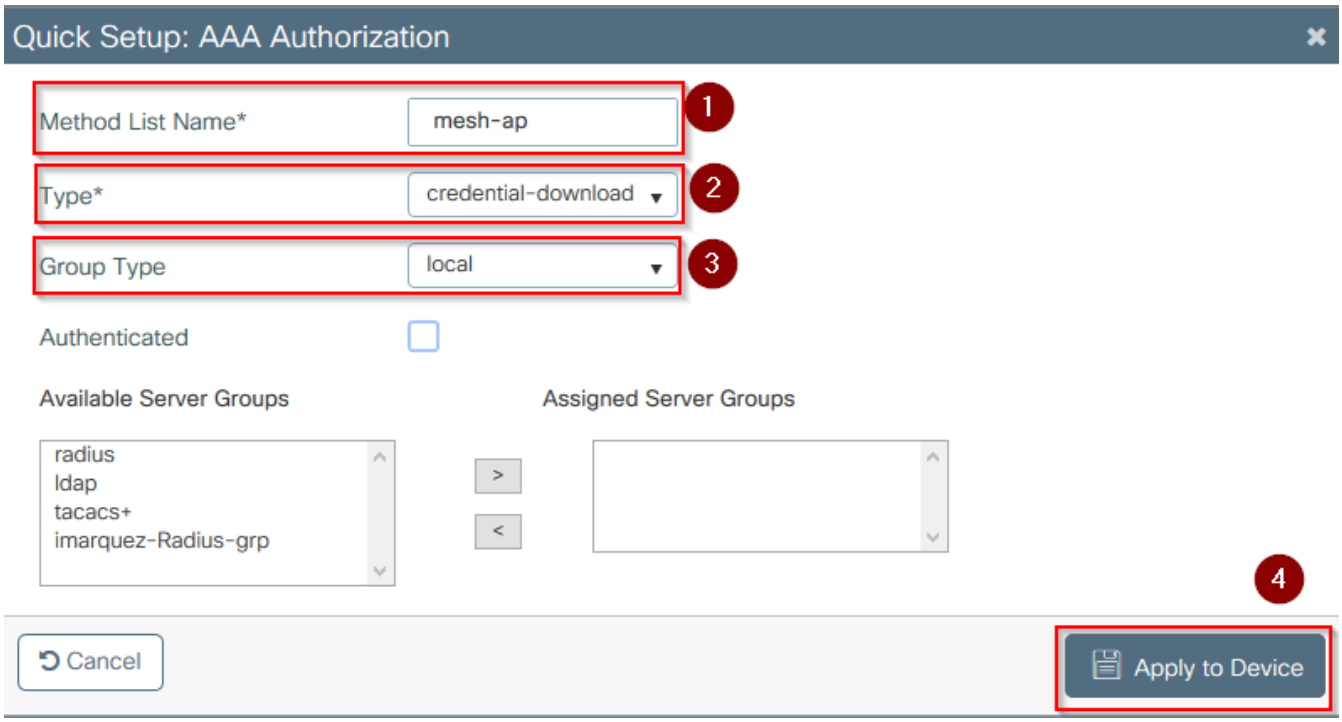


- Step 6b. In case your APs join direclty as Bridge mode and were not assigned a site and policy tag before, repeat step 6 but for the default method.
- Configure a dot1x aaa authetnication method which points to local (CLI aaa authentication dot1x default local)

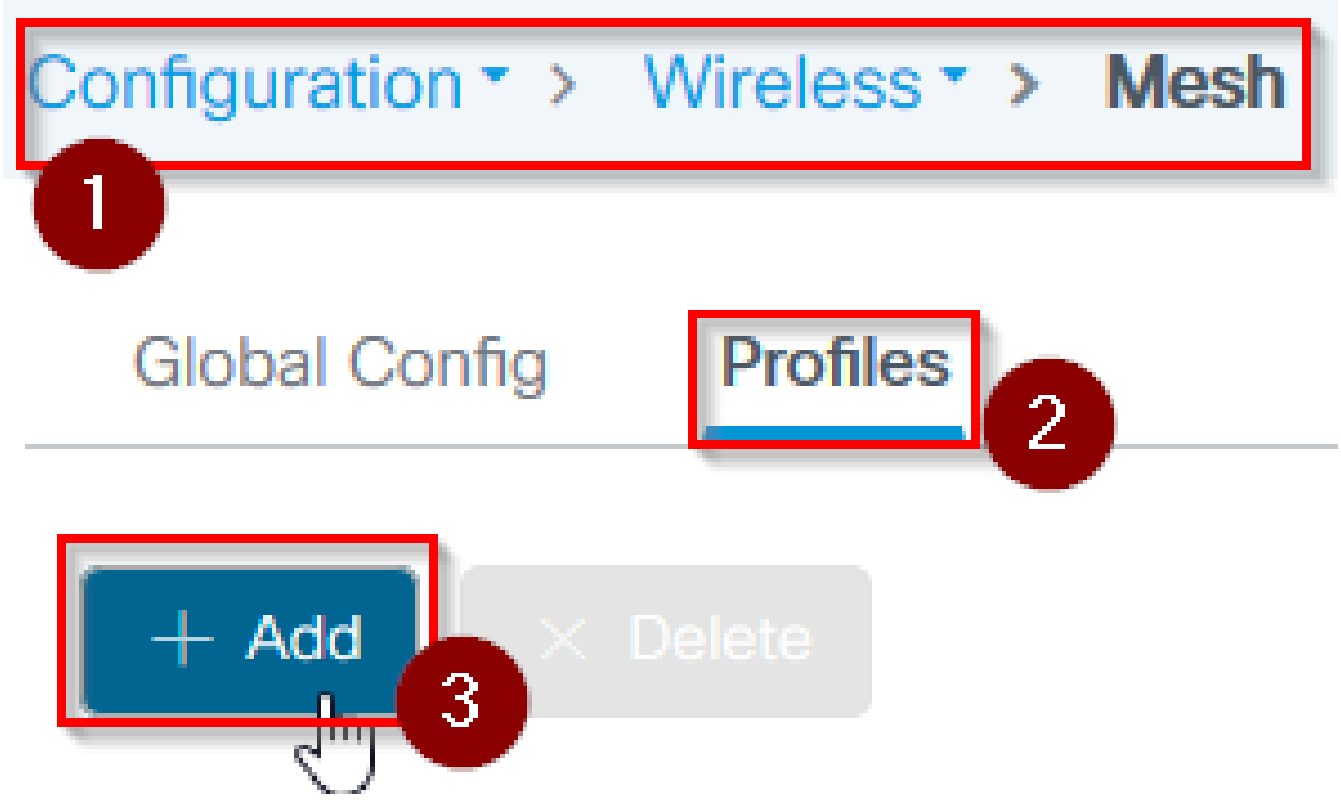
- Step 7. Navigate to **Configuration** > **Security** > **AAA** > **AAA Method List** > **Authorization**
- Step 8. Select **Add**, the **AAA Authorization** pop-up appears



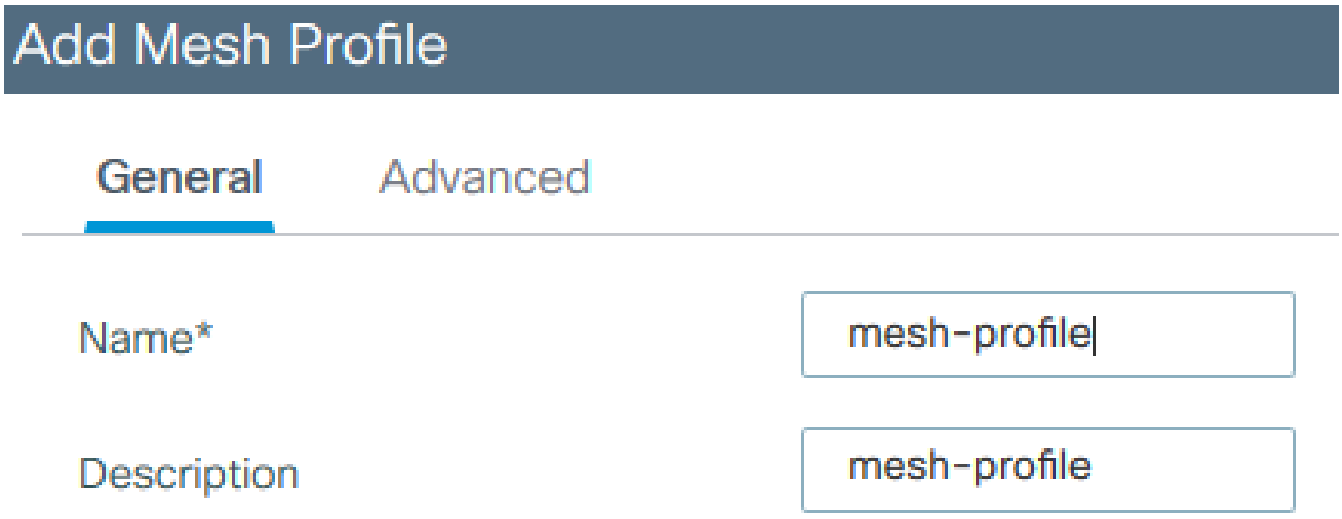
- Step 9. Type in a name in the **Method List Name**, select **credeential download** from the **Type*** drop-down and **local** for the **Group Type**, finally select **Apply to Device**



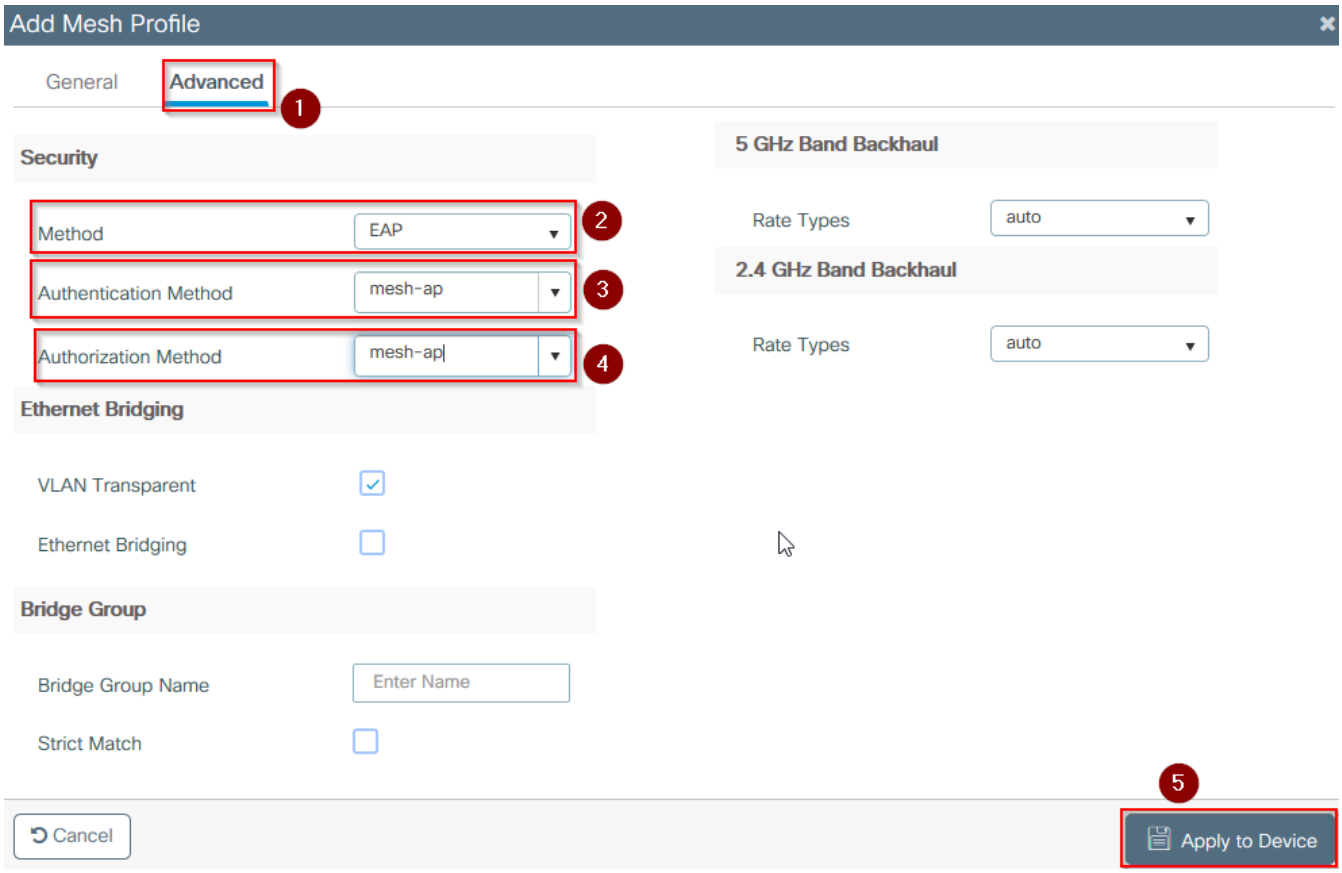
- Step 9b. In case your AP join directly in Bridge mode (that is, it does not join in local mode first), repeat step 9 for the default credential-download method (CLI aaa authorization credential-download default local)
- Step 10. Navigate to **Configuration** > **Wireless** > **Mesh** > **Profiles**
- Step 11. Select **Add**, the **Add Mesh Profile** pop-up appears



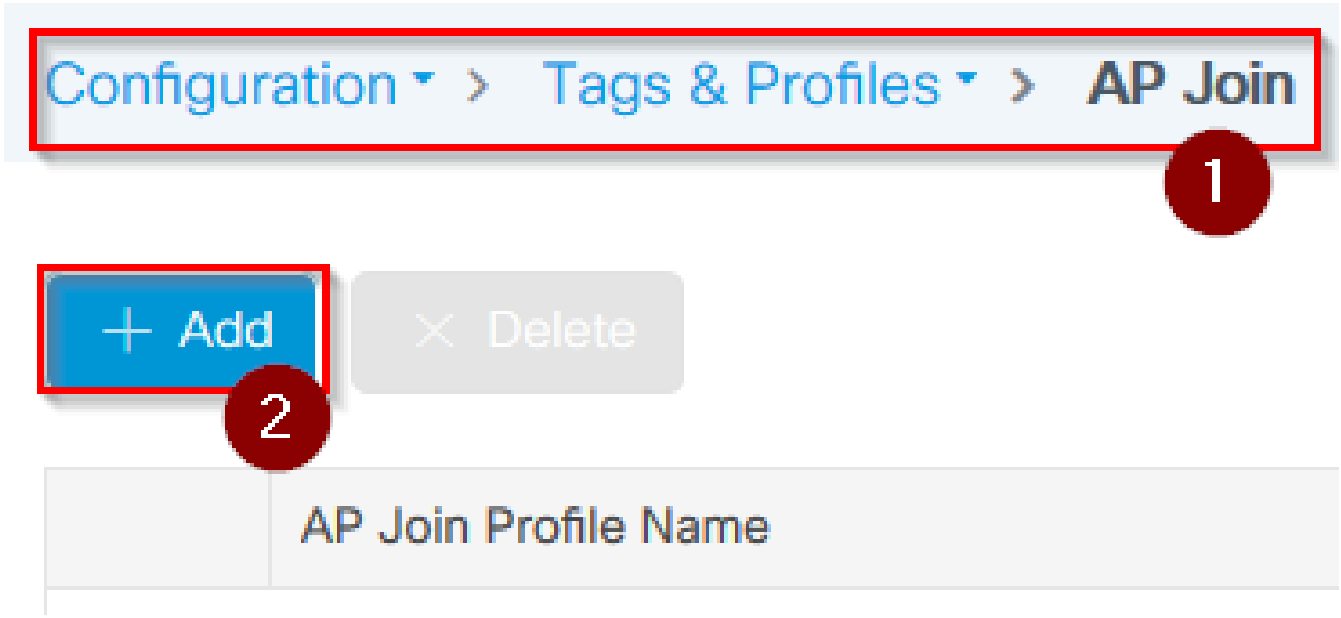
- Step 12. In the **General** tab set a name and description for the Mesh profile

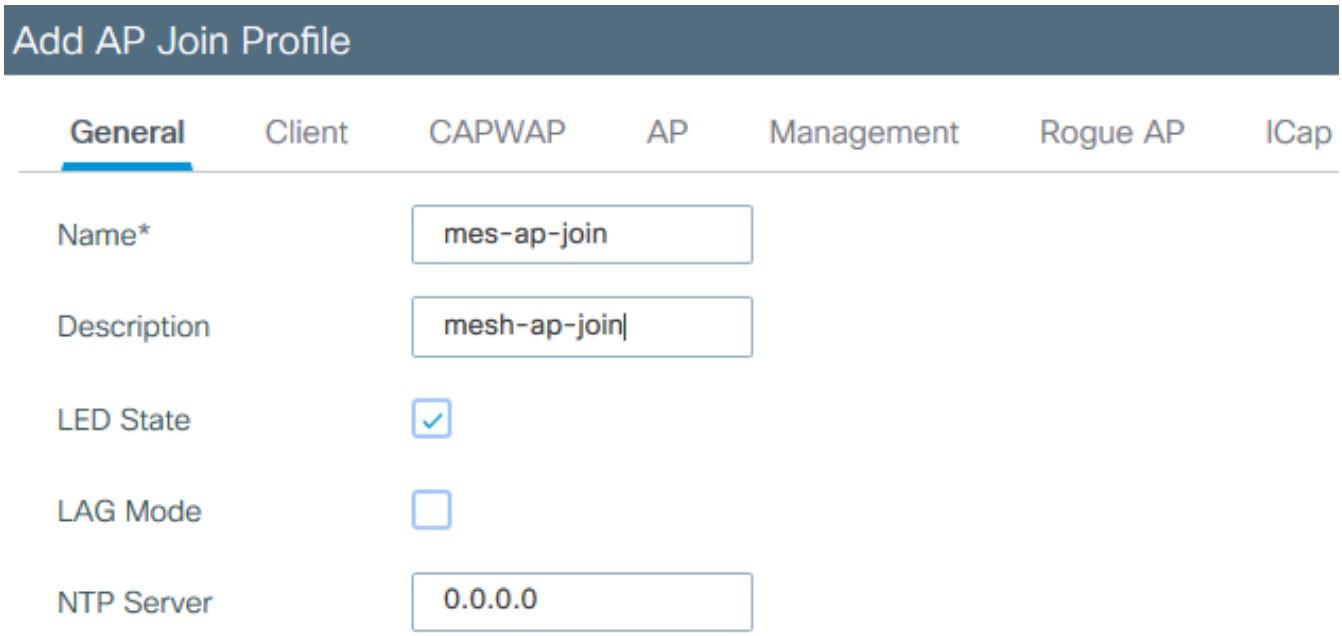


- Step 13. Under the **Advanced** tab select **EAP** for the **Method** field
- Step 14. Select he **Authorization** and **Authentication** profile defined in steps 6 and 9, and select **Apply to Device**

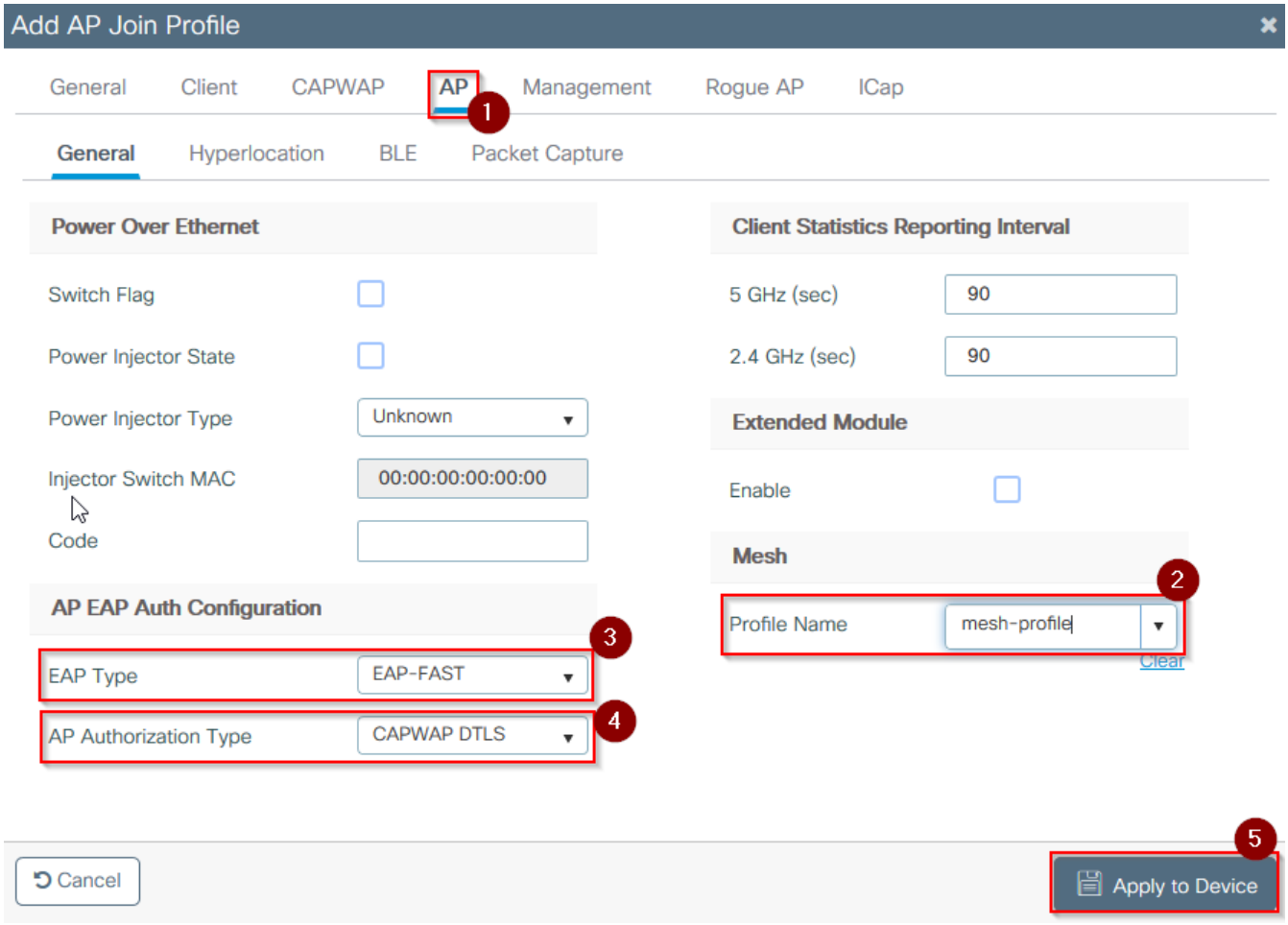


- Step 15. Navigate to **Configuration** > **Tag & Profiles** > **AP Join** > **Profile**
- Step 16. Select **Add**, the **AP Join Profile** pop-up appears, set a name and description for the AP Join profile

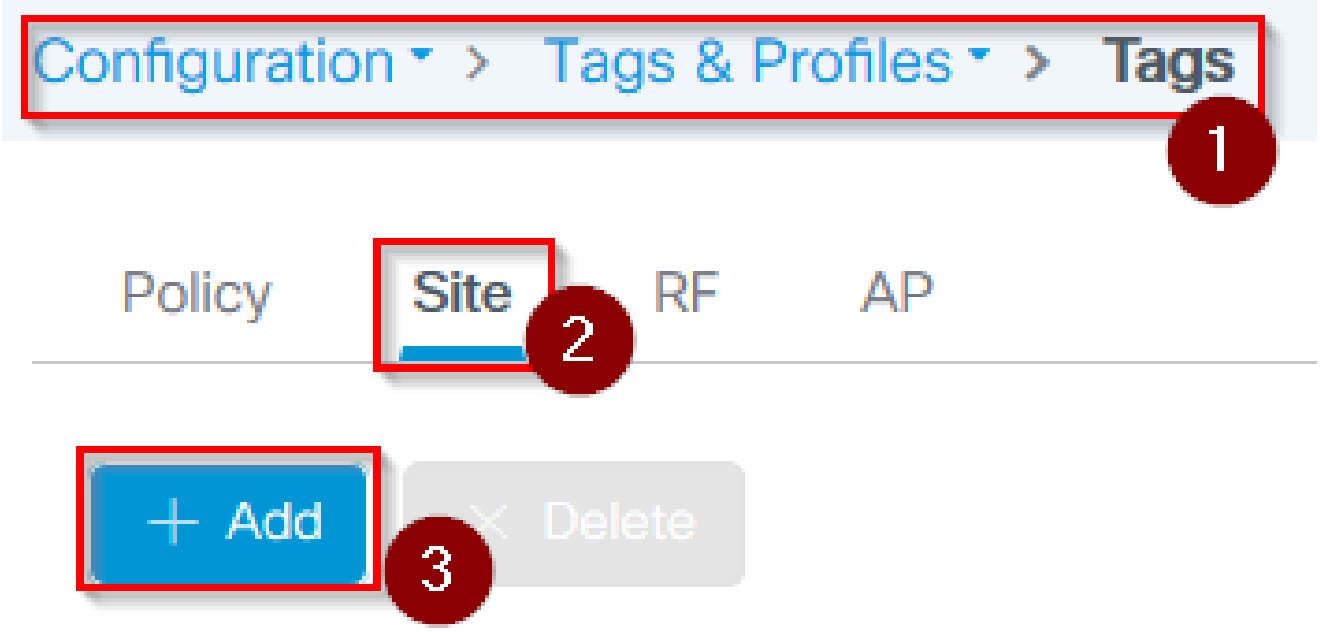




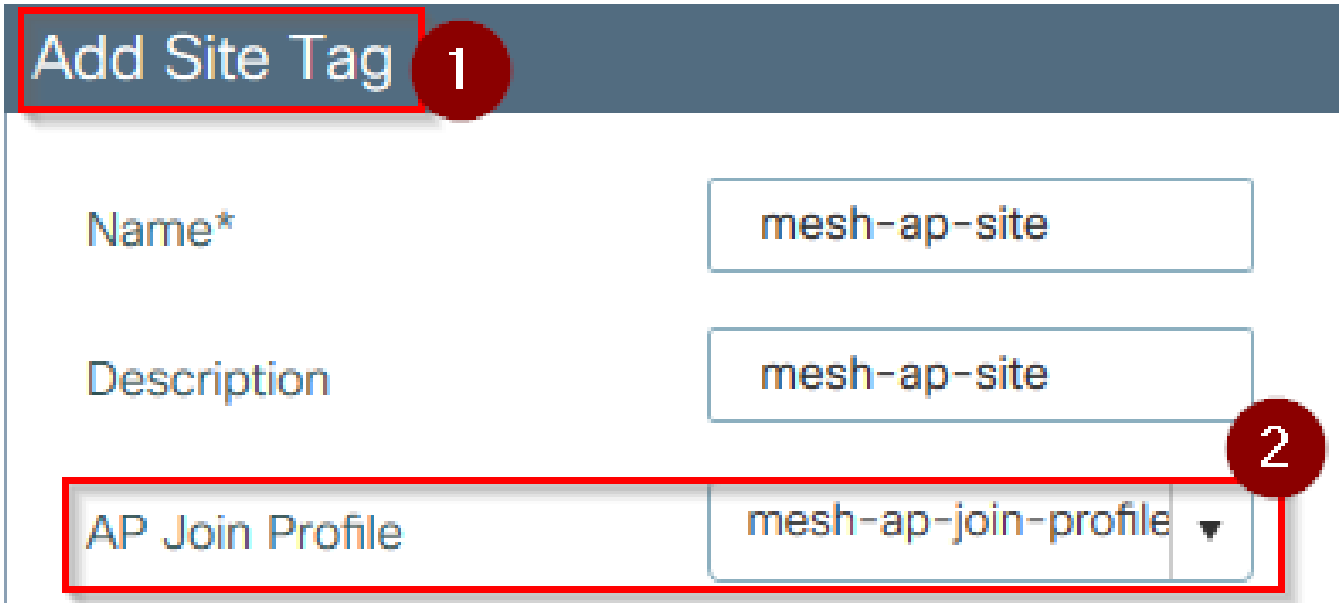
- Step 17. Navigate to the **AP** tab and select the **Mesh Profile** created in step 12 from the **Mesh Profile Name** dropdown
- Step 18. Ensure **EAP-FAST** and **CAPWAP DTLS** are set for the **EAP Type** and **AP Authorization Type** fields respectively
- Steo 19. Select **Apply to Device**



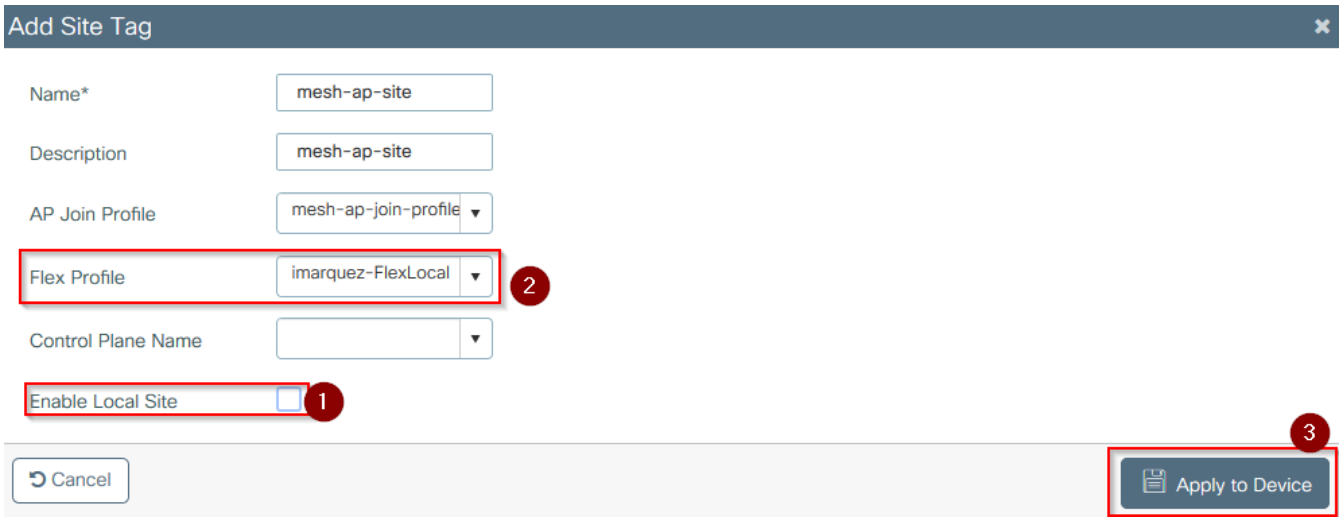
- Step 20. Navigate to **Configuration** > **Tag & Profiles** > **Tags** > **Site**
- Step 21. Select **Add**, the Site Tag pop up appears



- Step 22. Type in a name and description for the Site Tag



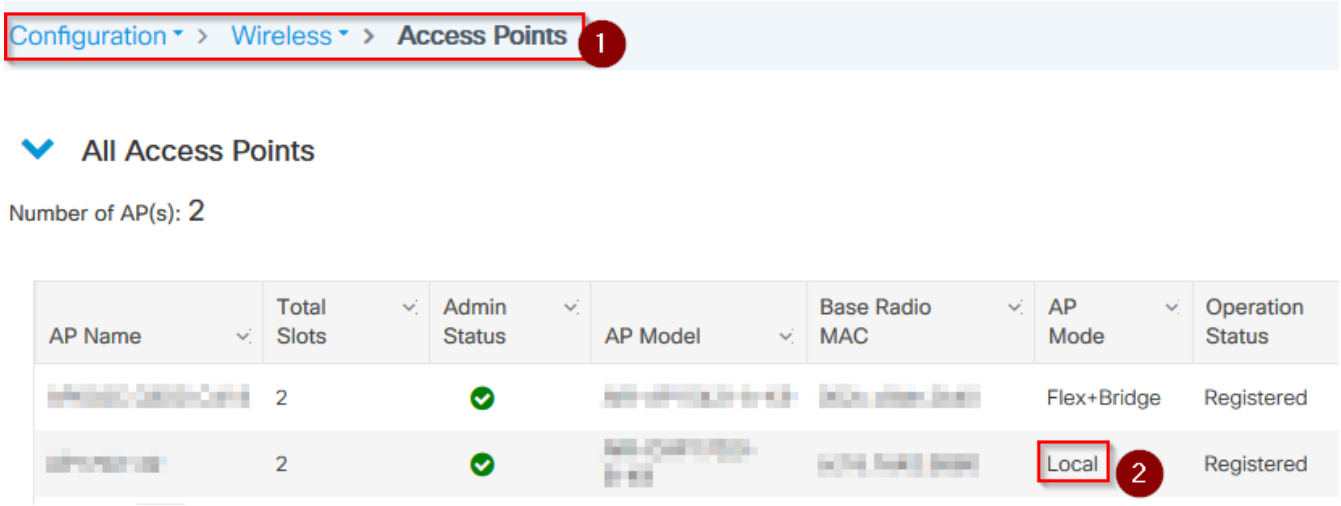
- Step 23. Select the **AP Join Profile** created in step 16 from the **AP Join Profile** dropdown
- Step 24. At the bottom of the Site Tag popup uncheck the **Enable Local Site** checkbox to enable the **Flex Profile** dropdown.
- Step 35. From the **Flex Profile** dropdown select the **Flex Profile** you want to use for the AP



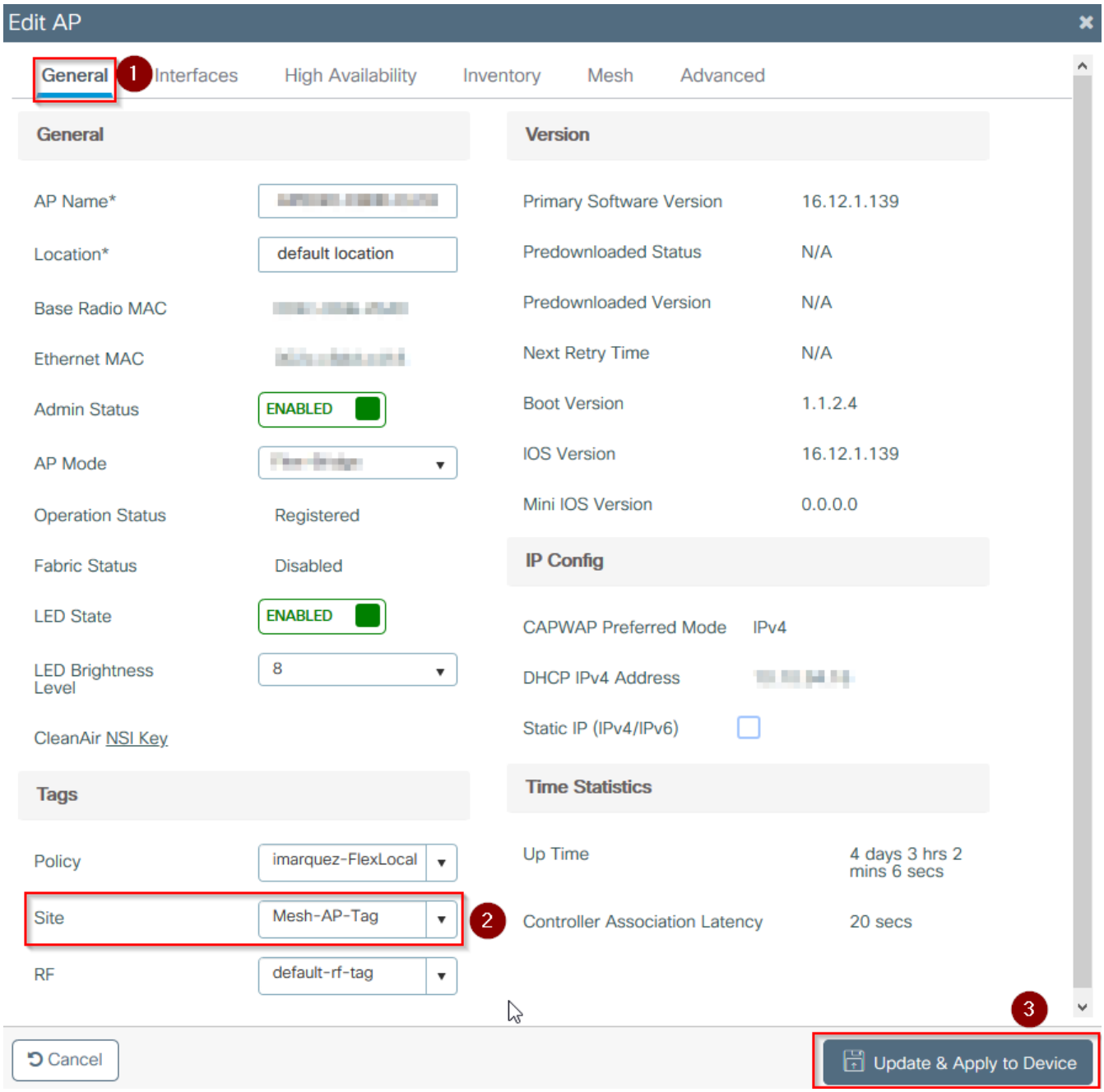
- Step 36. Connect the AP to the network and ensure the AP is in local mode.
- Step 37. To ensure the AP is in local mode issue the command **capwap ap mode local.**

  The AP must have a way to find the controller, either L2 broadcast, DHCP Option 43, DNS resolution or manual setup.

- Step 38. The AP joins the WLC, ensure it is listed under the AP list, navigate to **Configuration** > **Wireless** > **Access Points** > **All Access Points**



- Step 39. Select the AP, the **AP** popup appears.
- Step 40. Select the **Site Tag** created in Step 22 under **General** > **Tags** > **Site** tab within the AP popup, select **Update and Apply to Device**



- Step 41. The AP reboots and must join back the WLC in Flex + Bridge mode

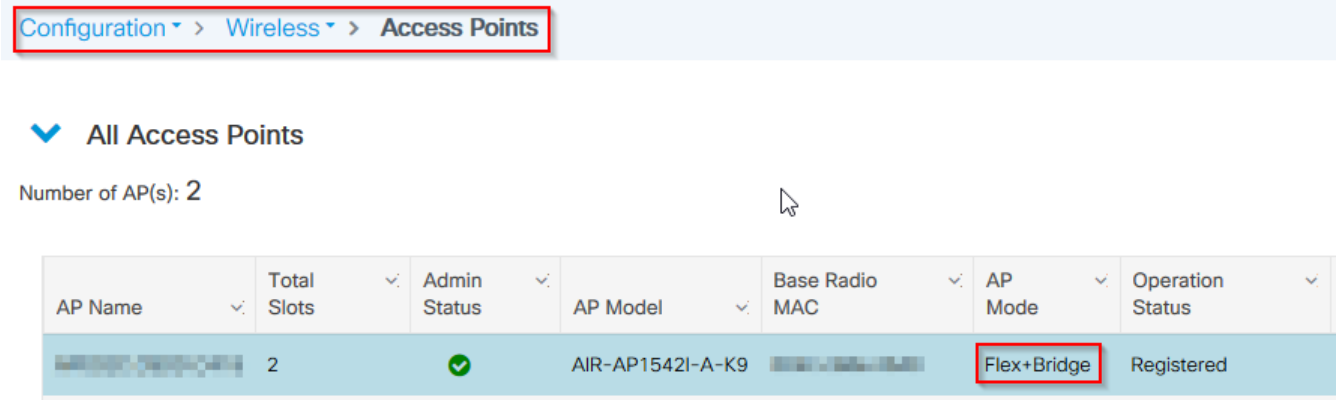
Notice that this method joins the AP first in local mode (where it does not do dot1x authentication) to apply the site tag with the mesh profile and then switch the AP to bridge mode.

To join an AP that is stuck in Bridge (or Flex+Bridge) mode, configure default methods (**aaa authentication dot1x default local** and **aaa authorization cred default local**).

The AP is then able to authenticate and you can assign the tags afterwards.

Verify

Ensure the AP mode is shown as Flex + Bridge as shown in this image.



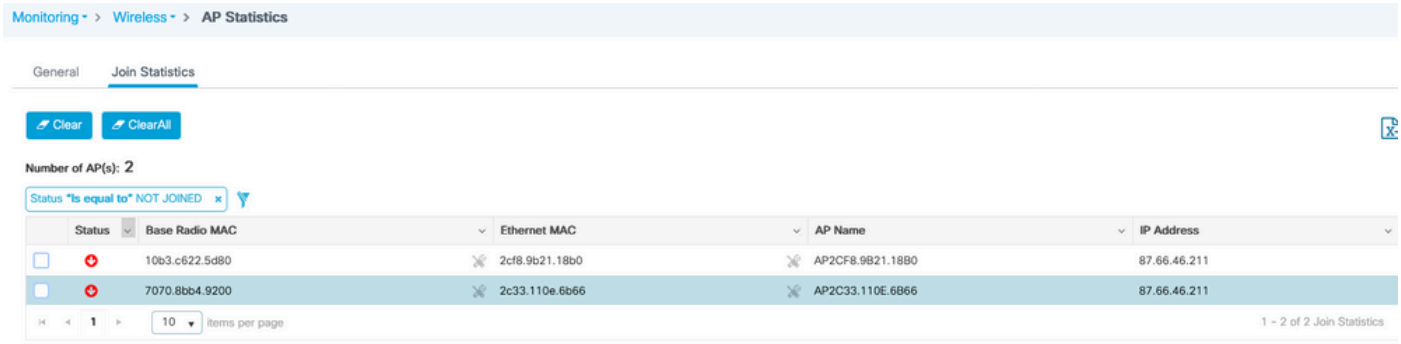
Run these commands from WLC 9800 CLI and look for the **AP Mode** attribute. It must be listed as **Flex+Bridge**

```
aaa authorization credential-download mesh-ap local
aaa authentication dot1x mesh-ap local
wireless profile mesh default-mesh-profile
 description "default mesh profile"
wireless tag site meshsite
 ap-profile meshapjoin
 no local-site
ap profile meshapjoin
 hyperlocation ble-beacon 0
 hyperlocation ble-beacon 1
 hyperlocation ble-beacon 2
 hyperlocation ble-beacon 3
 hyperlocation ble-beacon 4
 mesh-profile mesh-profile
```

Troubleshoot

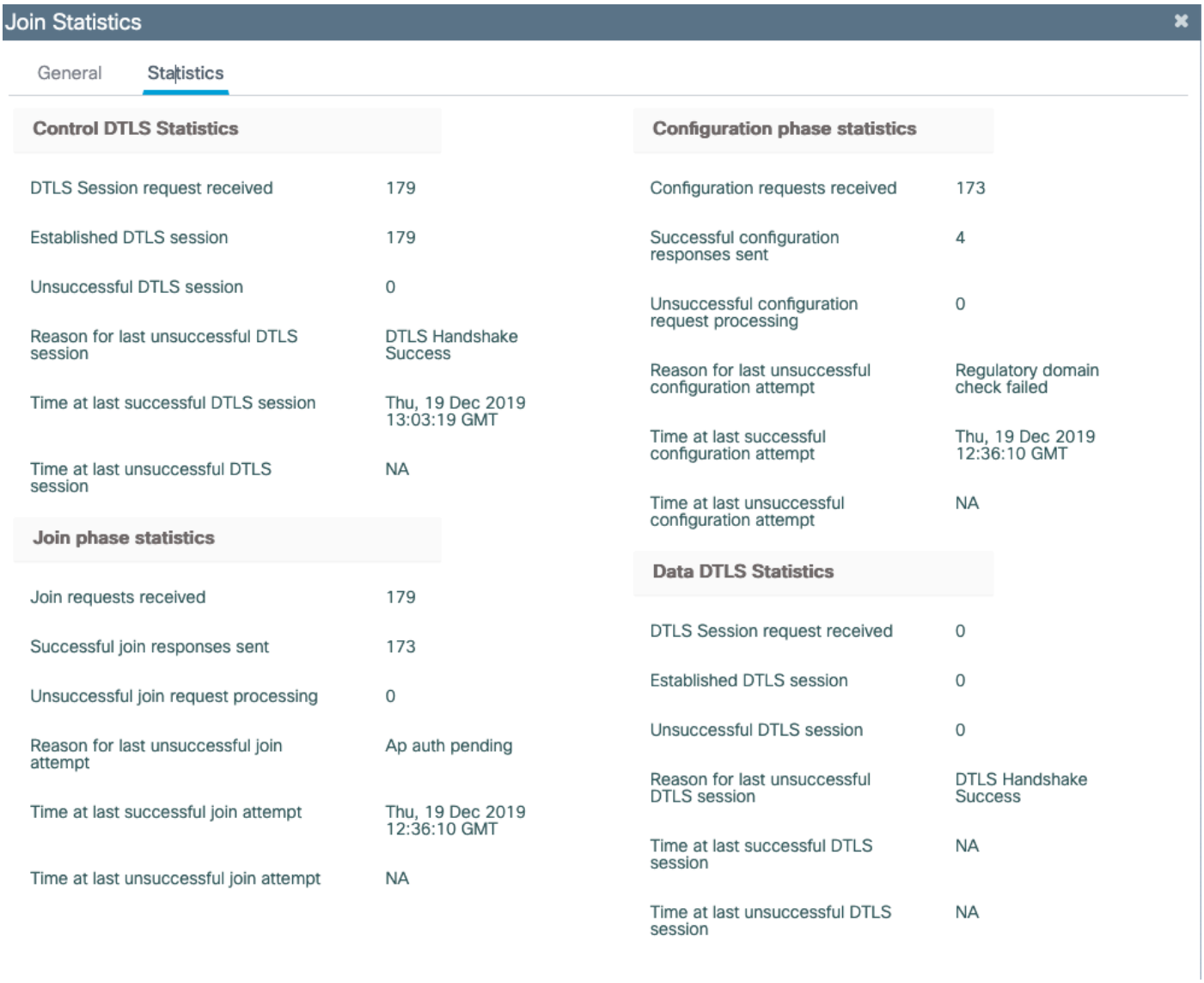
Make sure th ecommands **aaa authentication dot1x default local** and **aaa authorization cred default local** are present. They are needed if your AP was not pre-joined in Local mode.

The main 9800 dashboard has a widget which displays APs not able to join. Click it to get a list of APs that fail to join :



Click on the specific AP to see the reason why it is not joined. In this case, we see an authentication issue (AP auth pending) because the site tag was not assigned to the AP.

Therefore the 9800 did not pick the named authentication/authorization method to authenticate the AP :



For more advanced troubleshooting, go to the **Troubleshooting** > **Radioactive Trace** page on web UI.

If you enter the AP mac address, you can immediately generate a file to get the always-on logs (at notice level) of the AP that tries to join.

Click **Start** to enable advanced debugging for that mac address. The next time that the logs are generated, generate the logs, debug-level logs for the AP joinare shown.