

Configure Mesh on Catalyst 9800 Wireless LAN Controllers

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Case study 1: Bridge Mode](#)

[Configurations](#)

[Verify](#)

[Troubleshoot](#)

[Case study 2 : Flex + Bridge](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

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 the Catalyst 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

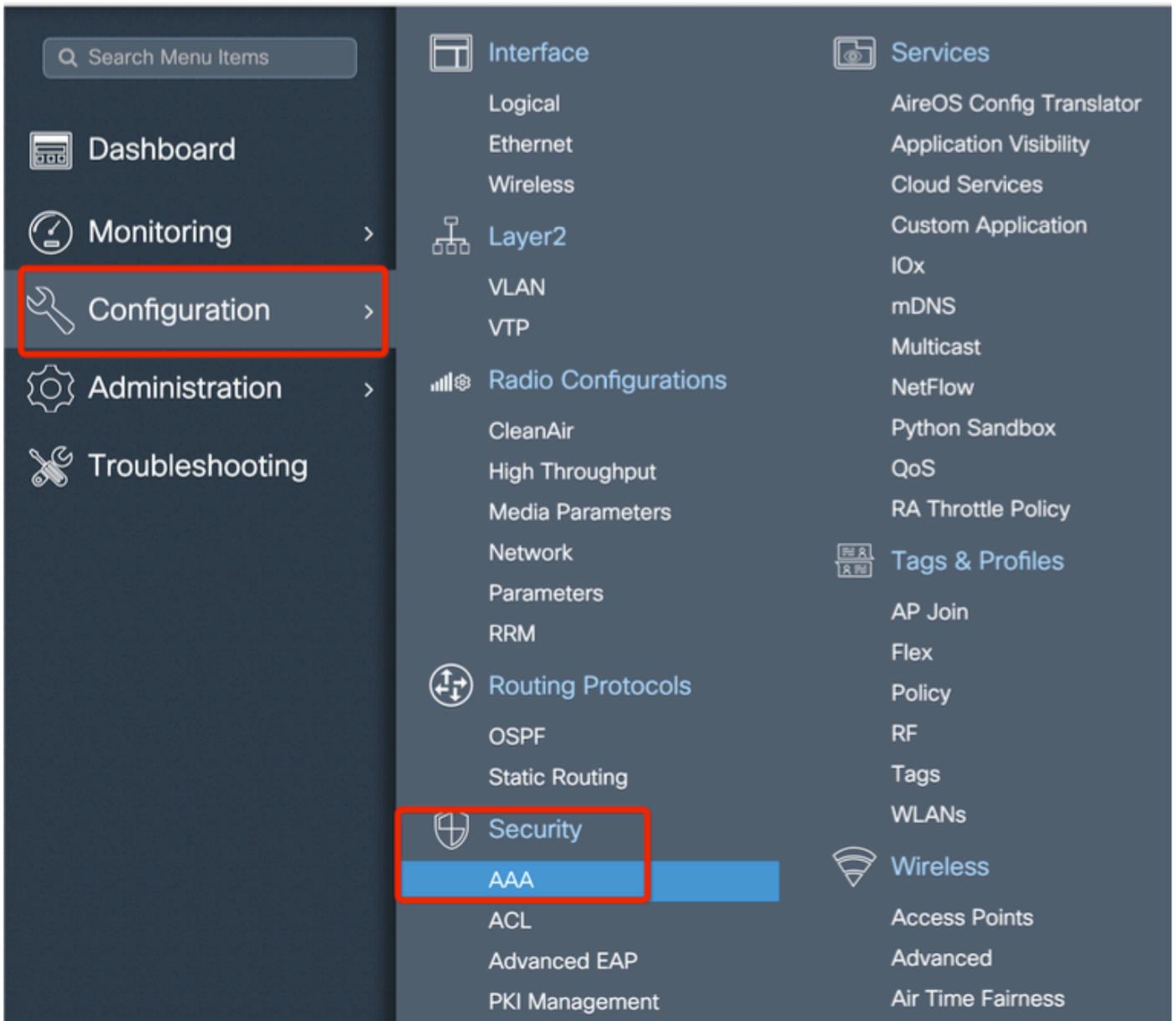
Configurations

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.

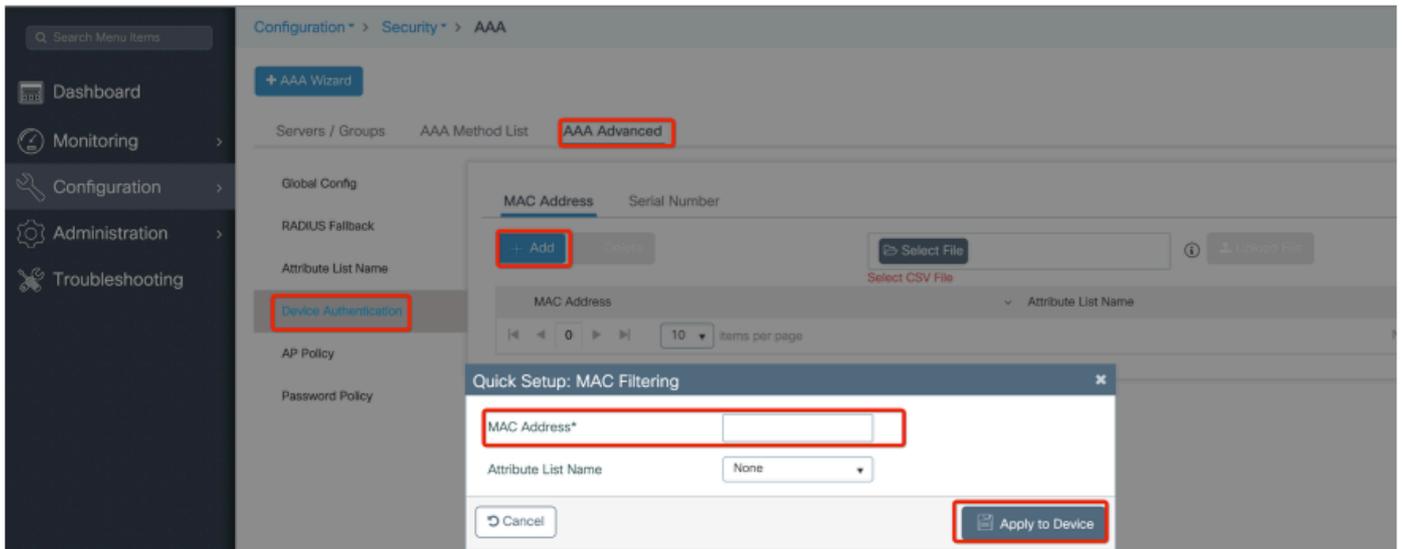
Step1: Configure RAP/MAP mac addresses under Device Authentication.

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



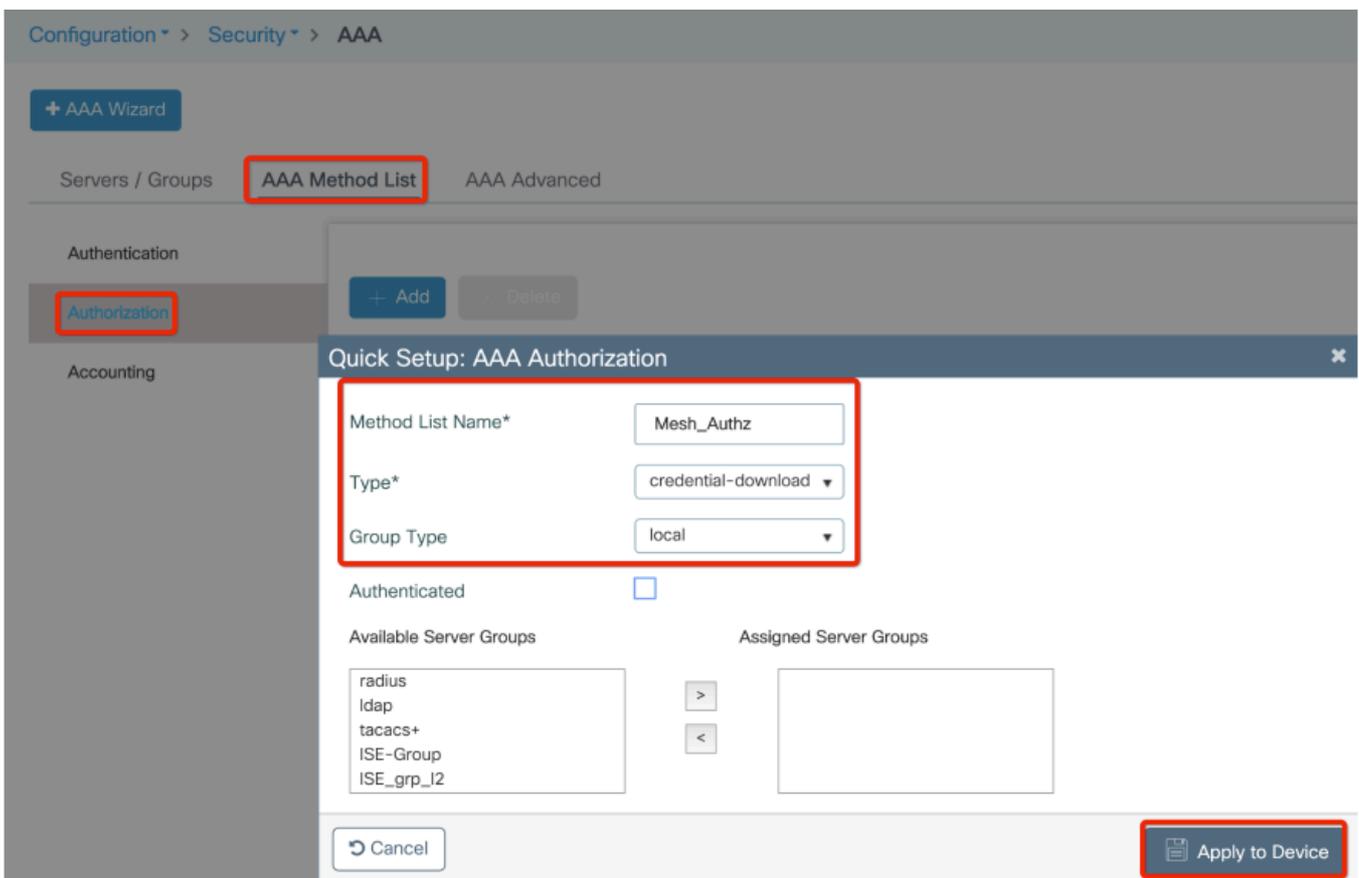
Add the Base Ethernet MAC Address of the mesh access points, add it without any special characters, without '.' or ':'

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.



Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization

Accounting

+ Add Delete

Quick Setup: AAA Authentication

Method List Name* Mesh_Authentication

Type* dot1x

Group Type local

Available Server Groups Assigned Server Groups

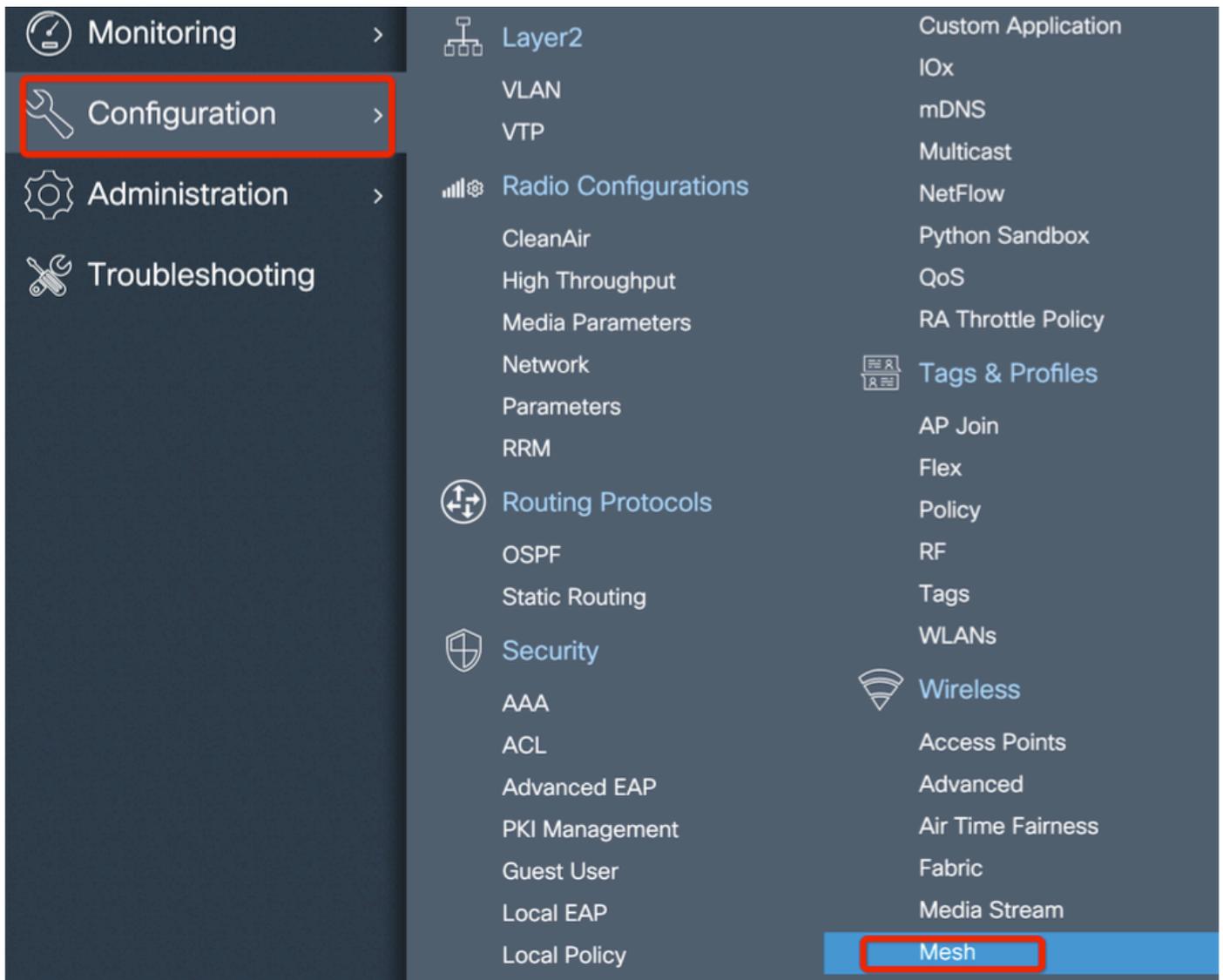
radius
ldap
tacacs+
ISE-Group
ISE_grp_I2

>
<

Cancel Apply to Device

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**

Global Config **Profiles**

+ Add Delete

Number of Profiles : 1

Add Mesh Profile

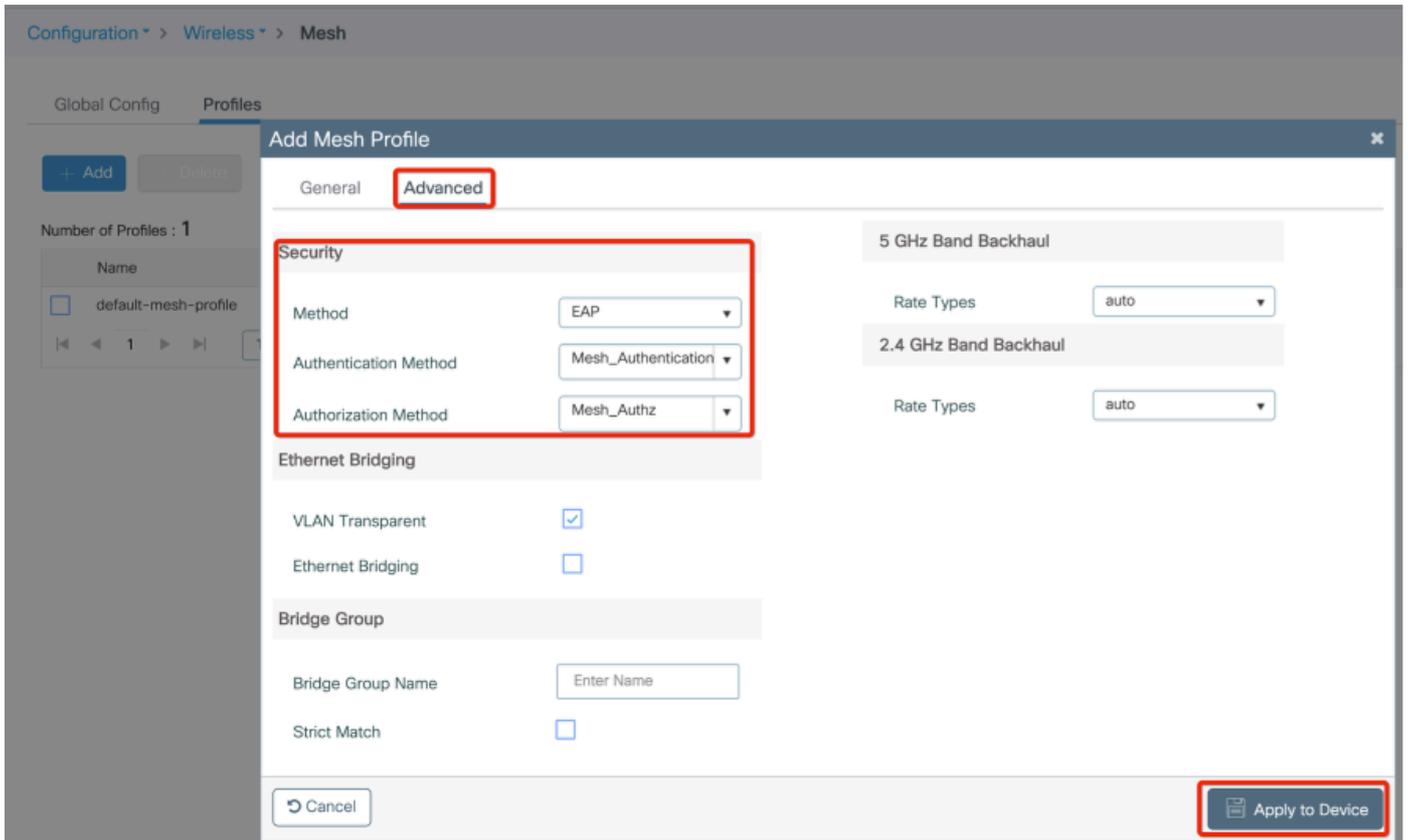
General Advanced

Name*	Mesh_Profile	Backhaul amsdu	<input checked="" type="checkbox"/>
Description	Enter Description	Backhaul Client Access	<input type="checkbox"/>
Range (Root AP to Mesh AP)	12000	Battery State for an AP	<input checked="" type="checkbox"/>
Multicast Mode	In-Out	Full sector DFS status	<input checked="" type="checkbox"/>
IDS (Rogue/Signature Detection)	<input type="checkbox"/>		
Convergence Method	Standard		
Background Scanning	<input type="checkbox"/>		
Channel Change Notification	<input type="checkbox"/>		
LSC	<input type="checkbox"/>		

Cancel Apply to Device

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 profile



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

Configuration > Tags & Profiles > AP Join

+ Add - Delete

AP Join Profile Name	Description
<input type="checkbox"/> default-ap-profile	default ap profile

Add AP Join Profile

General Client CAPWAP AP Management Rogue AP ICap

Name* Mesh_AP_Join_Profile

Description Enter Description

LED State

LAG Mode

NTP Server 0.0.0.0

Cancel Apply to Device

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

AP Join Profile Name	Description
<input type="checkbox"/> default-ap-profile	default ap profile

Add AP Join Profile

General Client CAPWAP **AP** Management Rogue AP ICap

General Hyperlocation BLE Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Code

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

Extended Module

Enable

AP EAP Auth Configuration

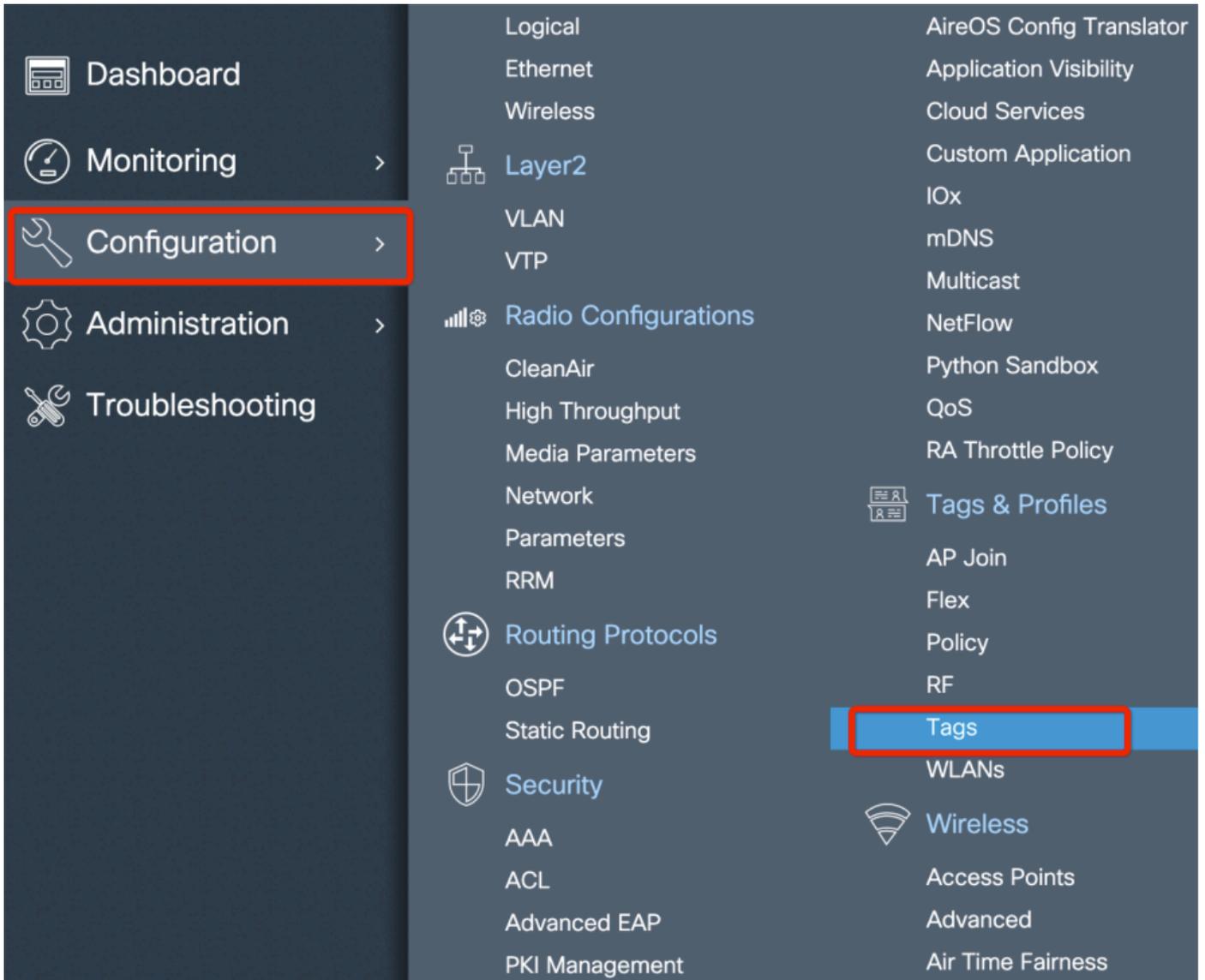
EAP Type

AP Authorization Type

Mesh

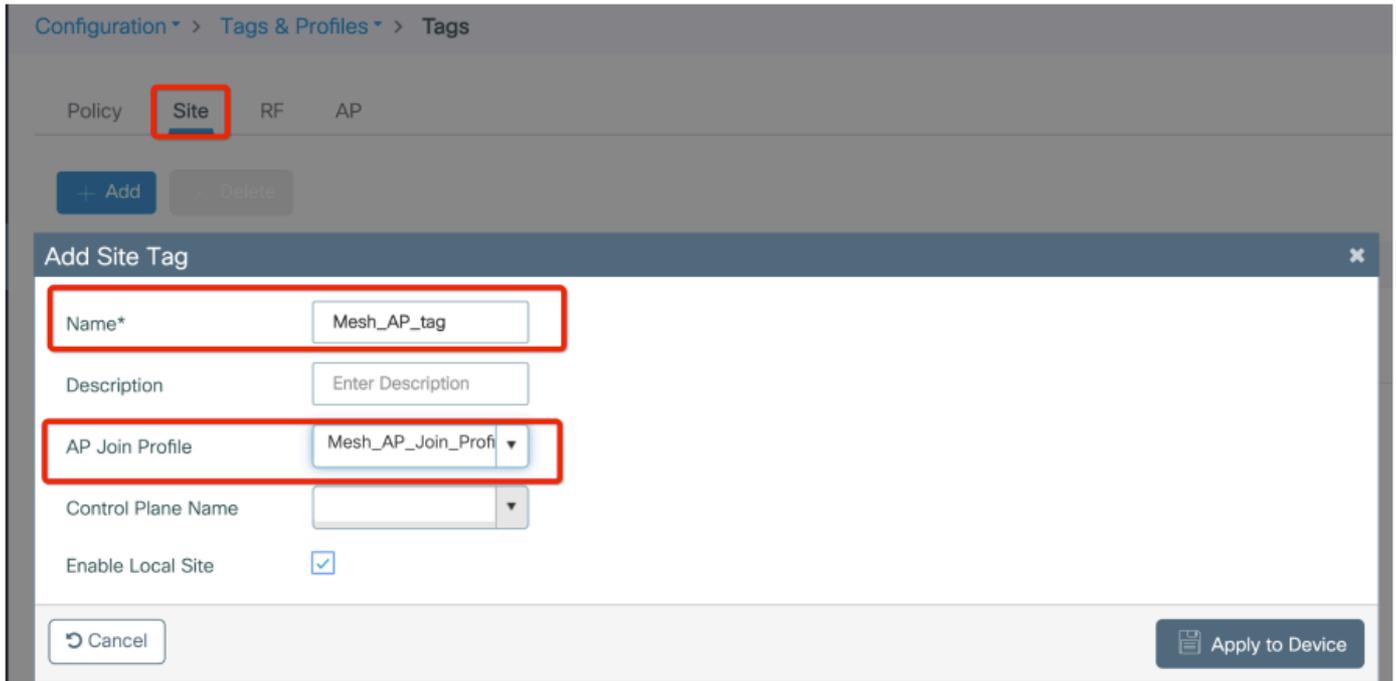
Profile Name [Clear](#)

Step 6: Create a mesh location Tag as shown.

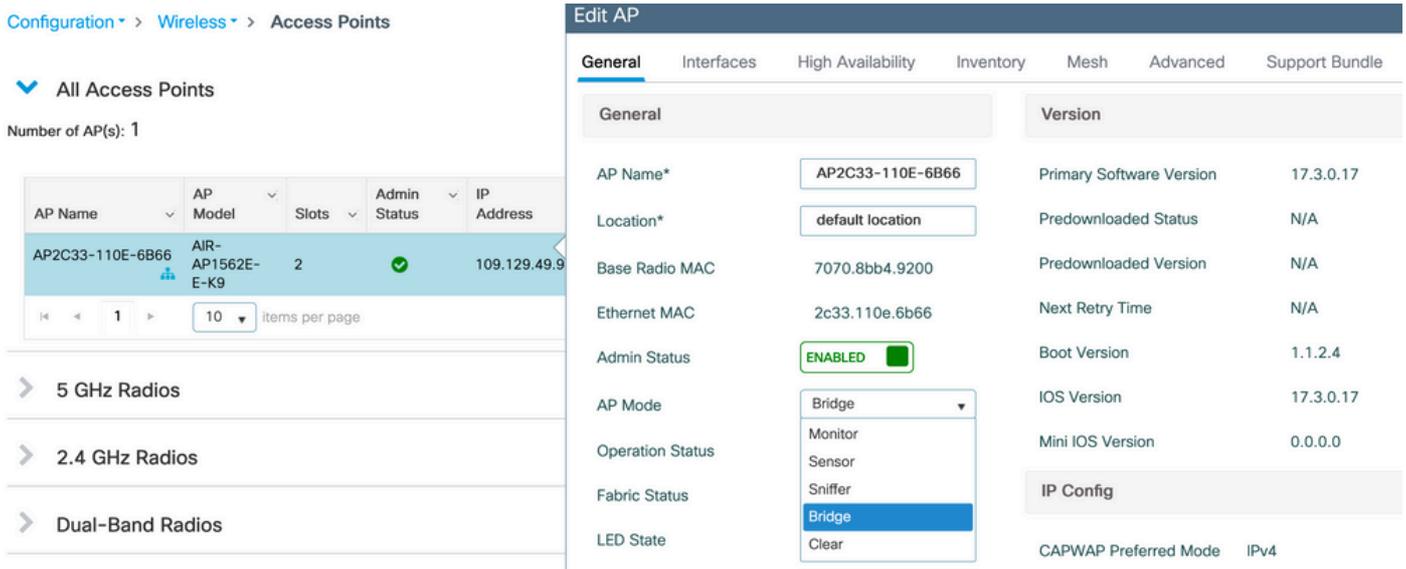


Configure Click the Mesh location TAG created in Step 6 to configure it.

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 not forget to specify the trunk native vlan in the AP settings in case it is different from the default VLAN 1

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address
AP2C33-110E-6B66	AIR-AP1562E-E-K9	2	✓	109.129.49.9

10 items per page

- 5 GHz Radios
- 2.4 GHz Radios
- Dual-Band Radios
- Country
- LSC Provision

Edit AP

General Interfaces High Availability Inventory **Mesh** Advanced Support Bundle

General

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

VLAN Trunking Native

Role

Remove PSK

Backhaul

Backhaul Radio Type

Backhaul Slot ID

Rate Types

Ethernet Port Configuration

ⓘ Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully

Port

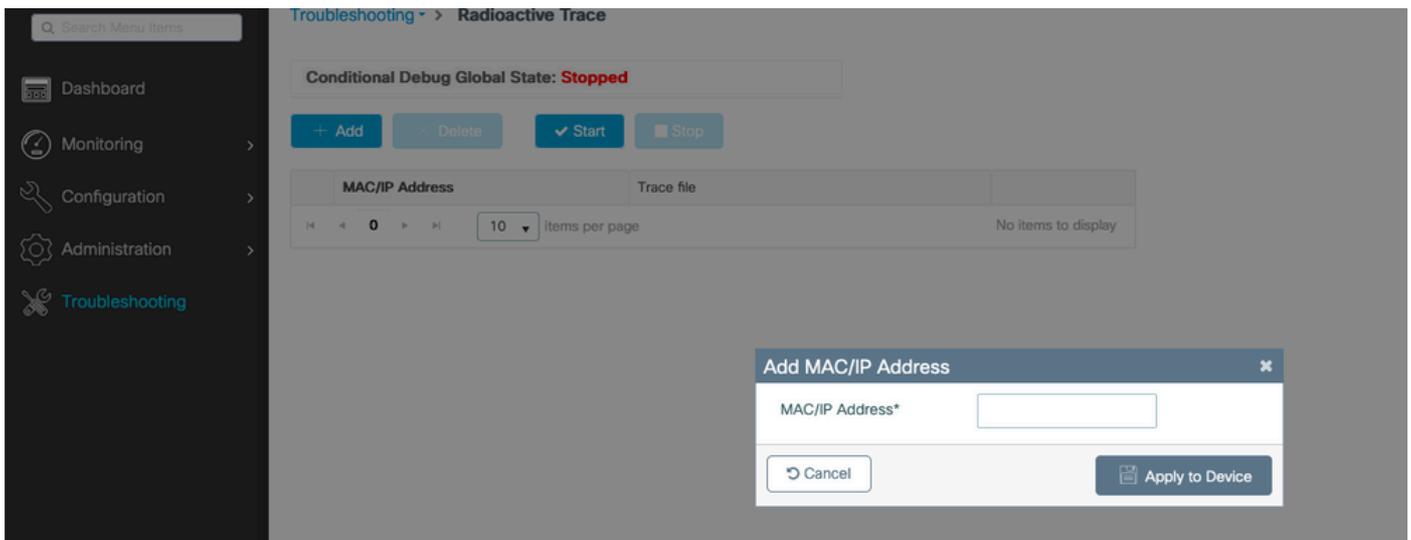
Mode

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 11112223333 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 :

```
2019/11/28 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 requ
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:

Monitoring > Wireless > AP Statistics

General **Join Statistics**

Clear ClearAll

Number of AP(s): 2

Status "Is equal to" NOT JOINED x

AP Name	AP Mod
<input type="checkbox"/> AP2CF8-9B5F-7D70	C9120A
<input checked="" type="checkbox"/> NA	

10 items per page

Join Statistics

General **Statistics**

DTLS Session request received	1	Configuration requests received	0
Established DTLS session	1	Successful configuration responses sent	0
Unsuccessful DTLS session	0	Unsuccessful configuration request processing	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success	Reason for last unsuccessful configuration attempt	NA
Time at last successful DTLS session	Mon, 17 Feb 2020 09:15:41 GMT	Time at last successful configuration attempt	NA
Time at last unsuccessful DTLS session	NA	Time at last unsuccessful configuration attempt	NA

Join phase statistics

Join requests received	1
Successful join responses sent	0
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	Ap auth pending
Time at last successful join attempt	NA
Time at last unsuccessful join attempt	NA

Data DTLS Statistics

DTLS Session request received	0
Established DTLS session	0
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	NA
Time at last unsuccessful DTLS session	NA

OK

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**

Configuration > Security > AAA

1

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

2

Global Config

RADIUS Fallback

Attribute List Name

Device Authentication

3

MAC Address

Serial Number

+ Add

4

× Delete

MAC Address

002cc8de2b40

- 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**

Quick Setup: MAC Filtering

MAC Address*

ffffffffffff

1

Attribute List Name

None

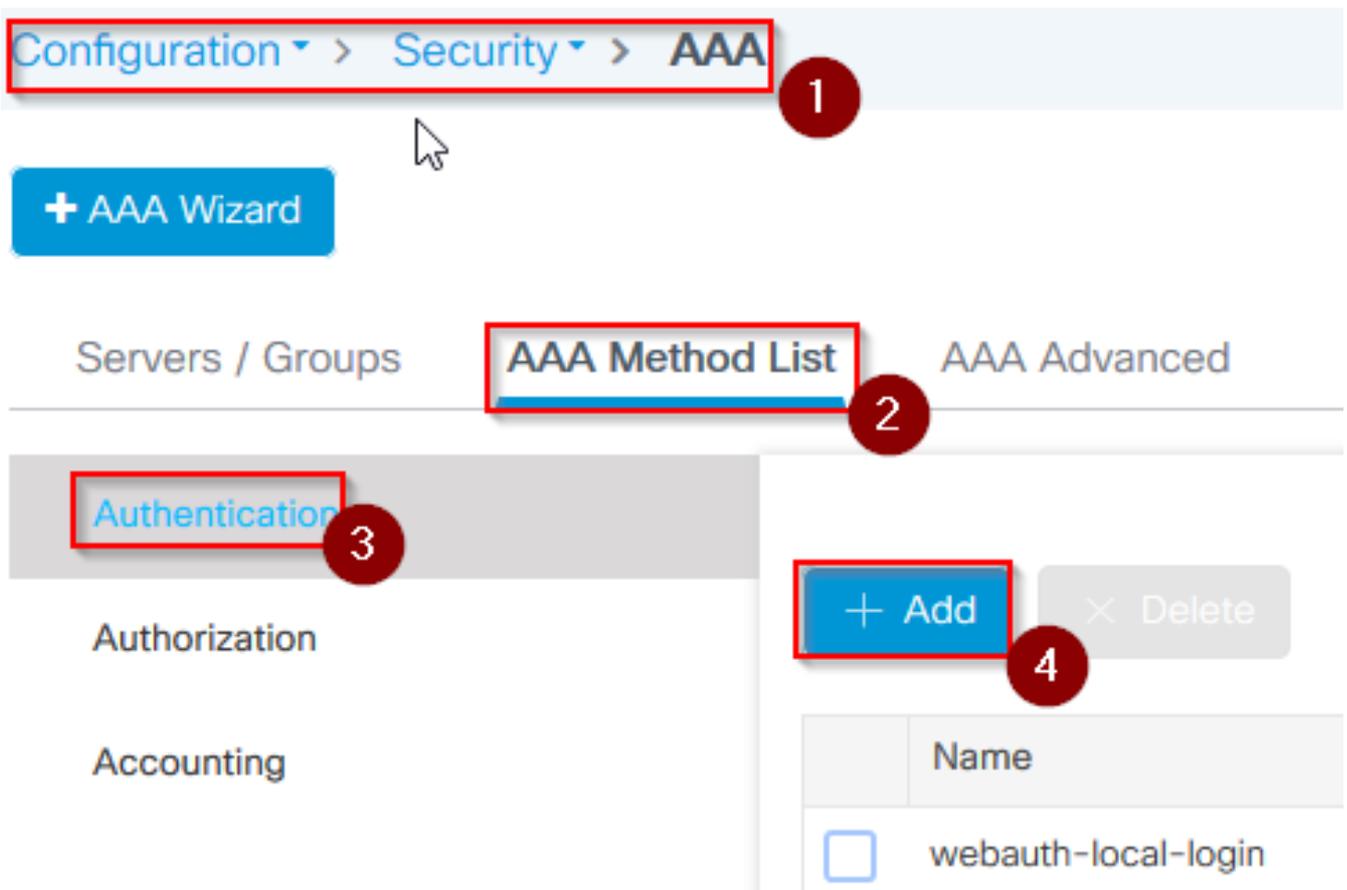
2

Cancel

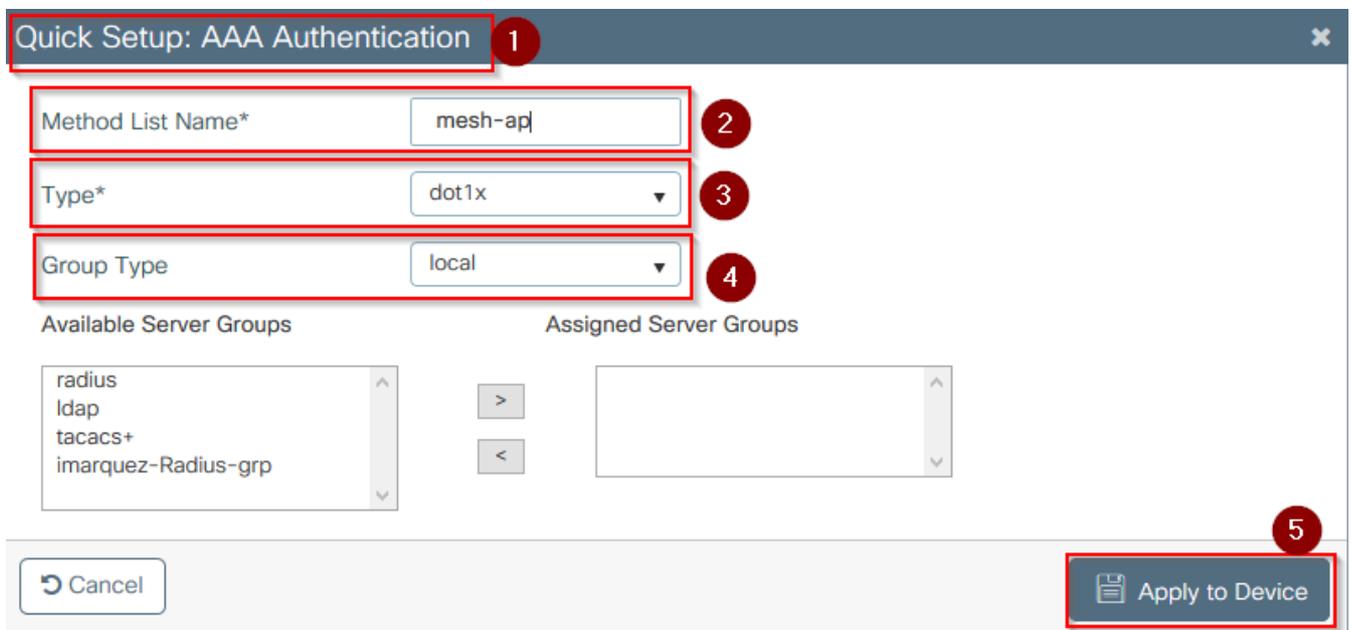
3

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 directly 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 authentication 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

Configuration > Security > AAA 1

+ AAA Wizard

Servers / Groups

AAA Method List 2

AAA Advanced

Authentication

Authorization 3

Accounting

+ Add 4

× Delete

Name
<input type="checkbox"/> default

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

Quick Setup: AAA Authorization

Method List Name* mesh-ap 1

Type* credential-download 2

Group Type local 3

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+
- imarquez-Radius-grp

Assigned Server Groups

-

Cancel

Apply to Device 4

- 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

Configuration ▾ > Wireless ▾ > Mesh

1

Global Config

Profiles

2

+ Add

× Delete

3

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

Add Mesh Profile

General

Advanced

Name*

mesh-profile|

Description

mesh-profile

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

Add Mesh Profile ✕

General **Advanced** 1

Security

Method 2 EAP

Authentication Method 3 mesh-ap

Authorization Method 4 mesh-ap|

Ethernet Bridging

VLAN Transparent

Ethernet Bridging

Bridge Group

Bridge Group Name

Strict Match

5 GHz Band Backhaul

Rate Types 5 auto

2.4 GHz Band Backhaul

Rate Types 5 auto

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5 5

5 5 5 5

Add AP Join Profile

General	Client	CAPWAP	AP	Management	Rogue AP	ICap
Name*	<input type="text" value="mes-ap-join"/>					
Description	<input type="text" value="mesh-ap-join"/>					
LED State	<input checked="" type="checkbox"/>					
LAG Mode	<input type="checkbox"/>					
NTP Server	<input type="text" value="0.0.0.0"/>					

- 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**

Add AP Join Profile

General Client CAPWAP **AP** Management Rogue AP ICap

General Hyperlocation BLE Packet Capture

Power Over Ethernet		Client Statistics Reporting Interval
Switch Flag	<input type="checkbox"/>	5 GHz (sec) <input type="text" value="90"/>
Power Injector State	<input type="checkbox"/>	2.4 GHz (sec) <input type="text" value="90"/>
Power Injector Type	<input type="text" value="Unknown"/>	Extended Module
Injector Switch MAC	<input type="text" value="00:00:00:00:00:00"/>	Enable <input type="checkbox"/>
Injector Switch Code	<input type="text"/>	Mesh
AP EAP Auth Configuration		Profile Name <input type="text" value="mesh-profile"/>
EAP Type	<input type="text" value="EAP-FAST"/>	<input type="text" value="mesh-profile"/>
AP Authorization Type	<input type="text" value="CAPWAP DTLS"/>	<input type="text" value="mesh-profile"/>

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

Configuration ▾ > Tags & Profiles ▾ > Tags

1

Policy

Site

2

RF

AP

+ Add

3

× Delete

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

Add Site Tag

1

Name*

mesh-ap-site

Description

mesh-ap-site

AP Join Profile

mesh-ap-join-profile ▾

2

- 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

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile 2

Control Plane Name

Enable Local Site 1

Apply to Device 3

- 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**

Configuration > Wireless > Access Points 1

▼ **All Access Points**

Number of AP(s): 2

AP Name	Total Slots	Admin Status	AP Model	Base Radio MAC	AP Mode	Operation Status
[blurred]	2	✔	[blurred]	[blurred]	Flex+Bridge	Registered
[blurred]	2	✔	[blurred]	[blurred]	Local	Registered

- 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**

Edit AP ✕

General
1
Interfaces
High Availability
Inventory
Mesh
Advanced

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status Registered

Fabric Status Disabled

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Tags

Policy

Site

RF

Version

Primary Software Version 16.12.1.139

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 1.1.2.4

IOS Version 16.12.1.139

Mini IOS Version 0.0.0.0

IP Config

CAPWAP Preferred Mode IPv4

DHCP IPv4 Address

Static IP (IPv4/IPv6)

Time Statistics

Up Time 4 days 3 hrs 2 mins 6 secs

Controller Association Latency 20 secs

Cancel
Update & 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.

▼ All Access Points

Number of AP(s): 2

AP Name	Total Slots	Admin Status	AP Model	Base Radio MAC	AP Mode	Operation Status
[REDACTED]	2	✓	AIR-AP1542I-A-K9	[REDACTED]	Flex+Bridge	Registered

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 the commands **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 :

Monitoring > Wireless > AP Statistics

General | **Join Statistics**

Clear Clear All

Number of AP(s): 2

Status "Is equal to" NOT JOINED

Status	Base Radio MAC	Ethernet MAC	AP Name	IP Address
✗	10b3.c622.5d80	2cf8.9b21.18b0	AP2CF8.9B21.18B0	87.66.46.211
✗	7070.8bb4.9200	2c33.110e.6b66	AP2C33.110E.6B66	87.66.46.211

1 - 2 of 2 Join Statistics

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 :

Join Statistics

General **Statistics**

Control DTLS Statistics

DTLS Session request received	179
Established DTLS session	179
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	Thu, 19 Dec 2019 13:03:19 GMT
Time at last unsuccessful DTLS session	NA

Join phase statistics

Join requests received	179
Successful join responses sent	173
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	Ap auth pending
Time at last successful join attempt	Thu, 19 Dec 2019 12:36:10 GMT
Time at last unsuccessful join attempt	NA

Configuration phase statistics

Configuration requests received	173
Successful configuration responses sent	4
Unsuccessful configuration request processing	0
Reason for last unsuccessful configuration attempt	Regulatory domain check failed
Time at last successful configuration attempt	Thu, 19 Dec 2019 12:36:10 GMT
Time at last unsuccessful configuration attempt	NA

Data DTLS Statistics

DTLS Session request received	0
Established DTLS session	0
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	NA
Time at last unsuccessful DTLS session	NA

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 join are shown.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller web UI. The breadcrumb navigation is **Troubleshooting > Radioactive Trace**. Below the breadcrumb, there is a link to **Back to Troubleshooting Menu**. A status bar indicates **Conditional Debug Global State: Stopped**. Below this, there are four buttons: **+ Add**, **× Delete**, **✓ Start**, and **■ Stop**. A table lists the trace entries:

MAC/IP Address	Trace file	
<input type="checkbox"/> 2c33.110e.6b66	debugTrace_2c33.110e.6b66.txt	Generate

At the bottom of the table, there is a pagination control showing **1** of **10** items per page, and **1 - 1 of 1 items**.