

Configure Mesh APs for Local Data Bridging in Flex and Bridge Mode

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Add Access Point to Controller Local Database](#)

[AAA Method List for Authentication](#)

[AAA Method List for Authorization](#)

[Mesh Profile](#)

[AP Join Profile](#)

[Flex Profile](#)

[Policy Profile](#)

[WLAN Tag](#)

[Policy Tag](#)

[Site Tag](#)

[Configuration of Access Points](#)

[Switch Port Configuration](#)

[Verify](#)

Introduction

This document describes the configuration of MAPs in Flex and Bridge mode for local client data bridging, bypassing the RAP.

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 Cisco switches

Components Used

This example utilizes lightweight access points (9124AP models), which can be configured as either a Root

Access Point (RAP) or a Mesh Access Point (MAP) to seamlessly integrate with the Catalyst 9800 Wireless LAN Controller (WLC).

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

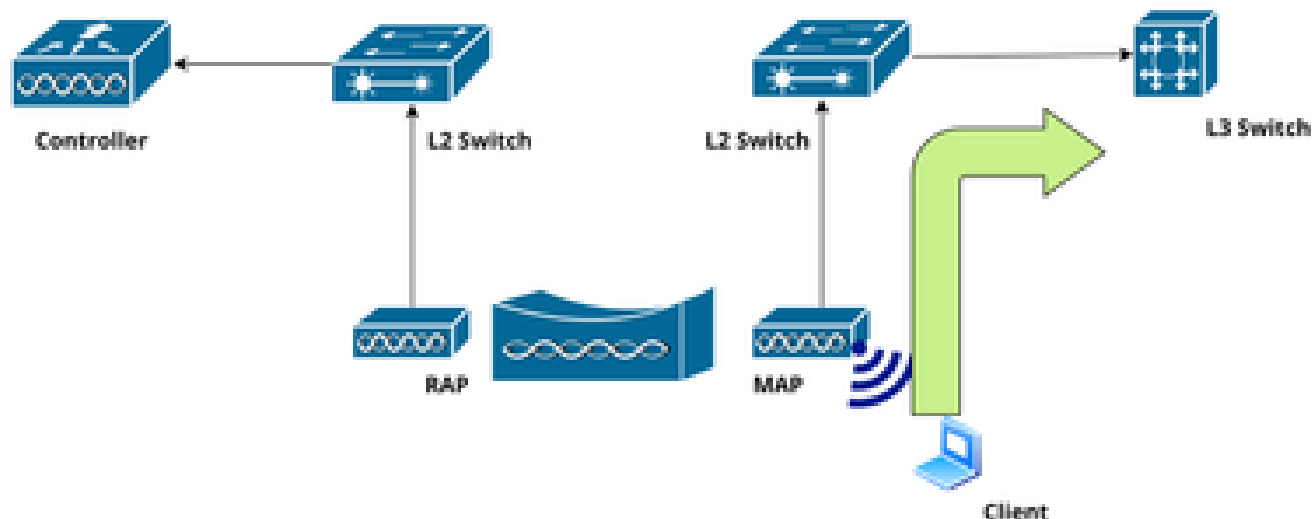
- C9800-L v17.12.5
- Cisco Catalyst 3850 Switch
- Cisco Catalyst 9124AX Series Access Point

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

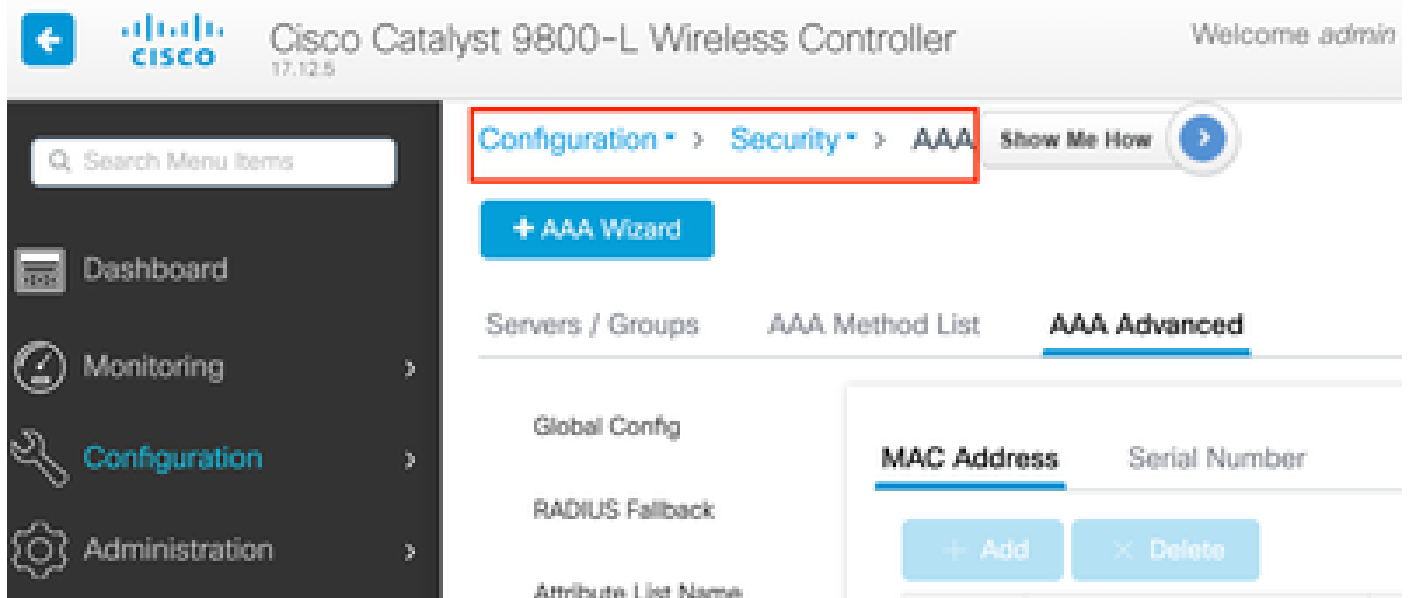
This section outlines configuration of Mesh Access Points (MAPs) operating in Mesh + Bridge mode, allowing local client data to be bridged directly to the uplink switch, bypassing the Root Access Point (RAP).

Network Diagram

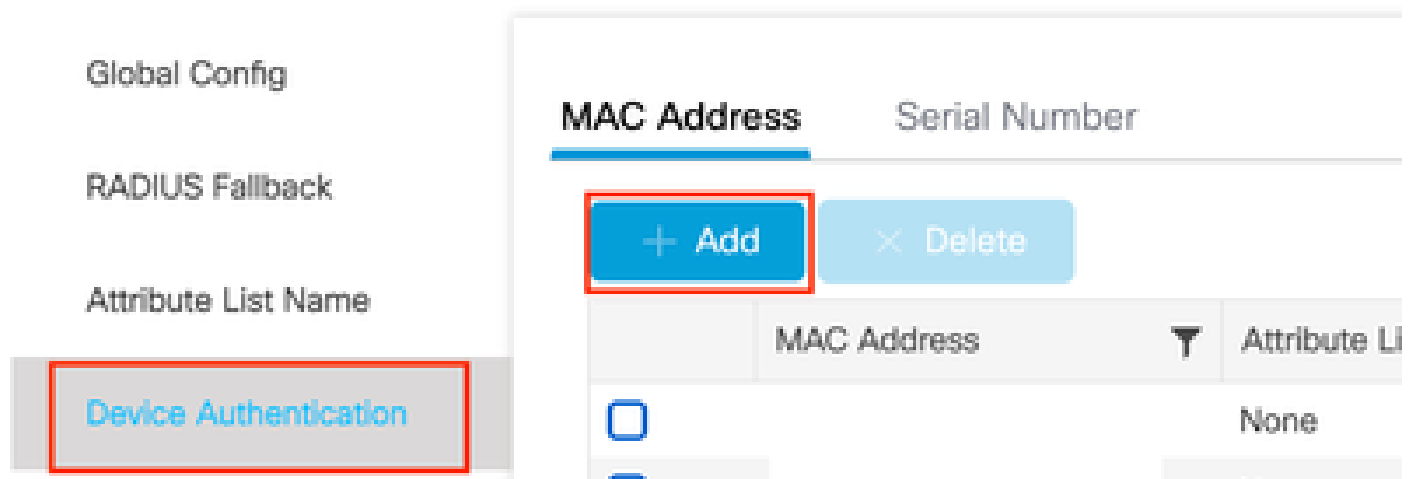


Add Access Point to Controller Local Database

Step 1: Navigate to **Configuration > Security > AAA > AAA Advanced**.



Step 2. Select **Device Authentication** and select **Add**.



Step 3. Type in the **Base Ethernet MAC address** of the AP to join the WLC. Leave the **Attribute List Name** blank, and select **Apply to Device**.

MAC Address*

3a5f1c8e729b

Attribute List Name

None

Description

WLAN Profile Name

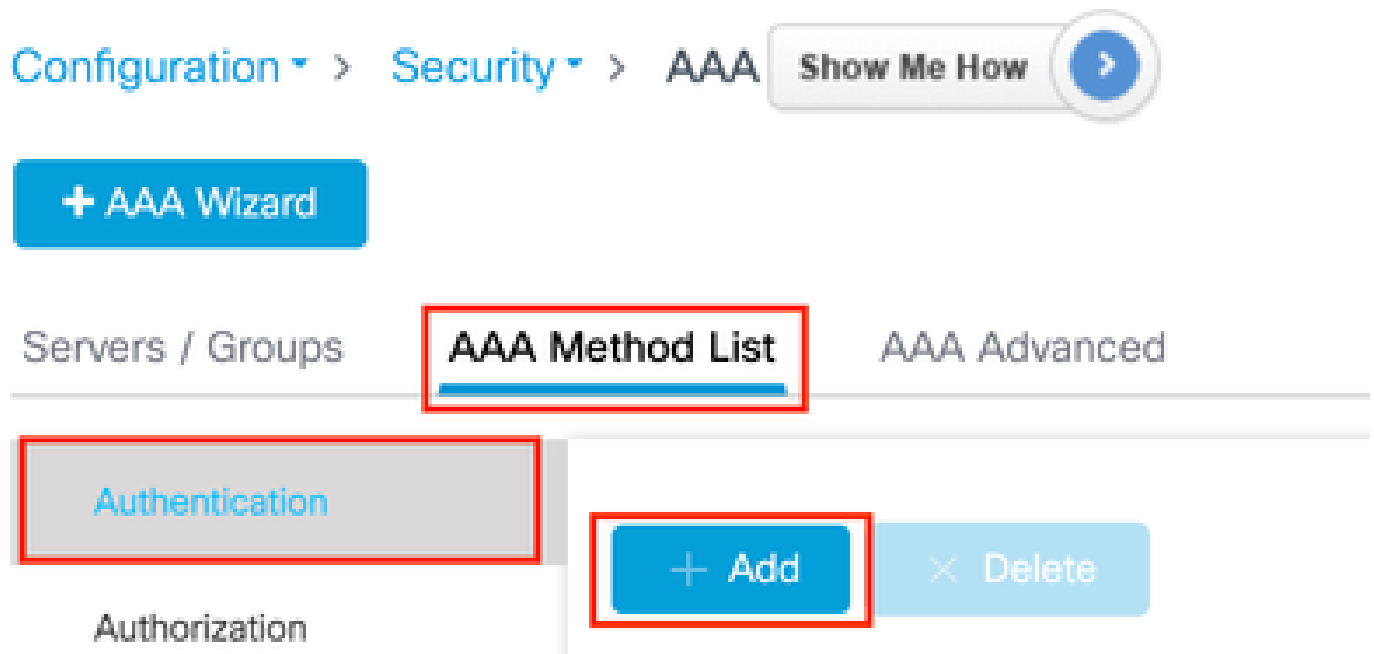
Select a value

Cancel

Apply to Device

AAA Method List for Authentication

Step 1: Navigate to **Configuration > Security > AAA > AAA Method List > Authentication** and select **Add**.



Step 2: Define Method List Name. Select **dot1x** from the **Type*** drop-down and **local** for the **Group Type**. Select **Apply to Device** to save the configuration.

Method List Name*	MESH		
Type*	dot1x		
Group Type	local		
Available Server Groups	Assigned Server Groups		
radius ldap tacacs+ HTTSGROUP ISE_DD_Group ISE_HA Test	> < > <		+ - + -

Cancel

Update & Apply to Device

AAA Method List for Authorization

Step 1: Navigate to **Configuration > Security > AAA > AAA Method List > Authorization** and select **Add**.

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

	Name	Type
	default	exec

Step 2: Define **Method List Name**, select **credential download** from the **Type*** dropdown and **local** for the **Group Type**. Click **Apply to Device**.

Method List Name* MESH-Authorization

Type* credential-downlo... ⓘ

Group Type local ⓘ

Authenticated ☐

Available Server Groups

radius
ldap
tacacs+
HTTSGROUP
ISE_DD_Group
ISE_HA
Trust



Assigned Server Groups



 Cancel

 Update & Apply to Device

Mesh Profile

Step 1: Navigate to **Configuration > Wireless > Mesh > Profiles** and select **Add**.

Configuration ▾ > Wireless ▾ > Mesh

Global Config Profiles

+ Add

× Delete

Step 2: Under the **General** tab, define a name and description (optional) for the **Mesh profile**.

General Advanced

Name*

MESH-Profile

Description

Enter Description

Range (Root AP to Mesh AP)

12000

Multicast Mode

In-Out ▼

IDS (Rogue/Signature Detection)

☐

Step 3: In the **Advanced** tab, set the **Method** field to **EAP**, then select the previously created **Authorization** and **Authentication** profiles from the dropdown menus. Finally, enable the **Ethernet Bridging** checkbox and select Update and apply.

General

Advanced

Security

Method

EAP

Authentication Method

MESH

Authorization Method

MESH-Authorizati...

Ethernet Bridging

VLAN Transparent

☐

Ethernet Bridging

☒

AP Join Profile

Step 1: Navigate to **Configuration** > **Tag & Profiles** > **AP Join** > **Profile**, click **Add**.

Configuration ▾ > **Tags & Profiles** ▾ > **AP Join**

+ Add

× Delete

Clone

AP Join Profile Name

Step 2: Define profile **name** and description (optional).

General	Client	CAPWAP	AP	Management	S
Name*	Mesh-AP-Join				
Description	Enter Description				
Country Code	IN  				
Time Zone	☒ Not Configured ☐ Use-Controller ☐ Delta from WLC				

Step 3: Navigate to the **AP** tab, select the **Mesh Profile** from the **Mesh Profile Name** dropdown, set **EAP-FAST** for the **EAP Type** and **CAPWAP DTLS** for the **AP Authorization Type**, and click **Apply to Device**.

Edit AP Join Profile

General

Client

CAPWAP

AP

Management

Security

ICap

QoS

Geolocation

General

Power Management

Hyperlocation

AP Statistics

Power Over Ethernet

Switch Flag

☐

Power Injector State

☐

Power Injector Type

Unknown

Injector Switch MAC

0000.0000.0000

AP EAP Auth Configuration

EAP Type

EAP-FAST

AP Authorization Type

CAPWAP DTLS

Client Statistics Reporting Interval

5 GHz (sec)

90

2.4 GHz (sec)

90

Extended Module

Enable

☐

Mesh

Profile Name

MESH-Profile

Cancel

Update & Apply to Device

Flex Profile

Step 1: **Configuration** > **Tags & Profiles** > **Flex**, then click **Add**.

Configuration ▾ > Tags & Profiles ▾ > Flex

+ Add

× Delete

Clone

Step 2: Define a **name** for Flex profile.

General	Local Authentication	Policy ACL	VLAN	DNS Layer Security
Name*	Mesh-Flex		Fallback Radio Shut	
Description	Enter Description		Flex Resilient	

Step 3: Navigate to the **vlan** tab and Configure the **VLAN Name** and **VLAN ID** for Local Bridging of Wireless Client Traffic, click **Save**.

General	Local Authentication	Policy ACL	VLAN	DNS Layer Security								
+ Add × Delete <table border="1"> <thead> <tr> <th>VLAN Name</th> <th>ID</th> <th>Ingress ACL</th> <th>Egress ACL</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>10</td> <td></td> <td></td> </tr> </tbody> </table> No items to display					VLAN Name	ID	Ingress ACL	Egress ACL	0	10		
VLAN Name	ID	Ingress ACL	Egress ACL									
0	10											
VLAN Name* Bridge-VLAN VLAN ID* 100 ACL Unidirectional ☒ Bidirectional ☐ Ingress ACL Select ACL Egress ACL Select ACL ✓ Save ↺ Cancel												
↺ Cancel ↻ Update & Apply to Device												

Policy Profile

Step 1: Navigate to **Configuration > Tags & Profiles > Policy** and click **Add**.

Configuration ▾ > Tags & Profiles ▾ > Policy

+ Add

× Delete

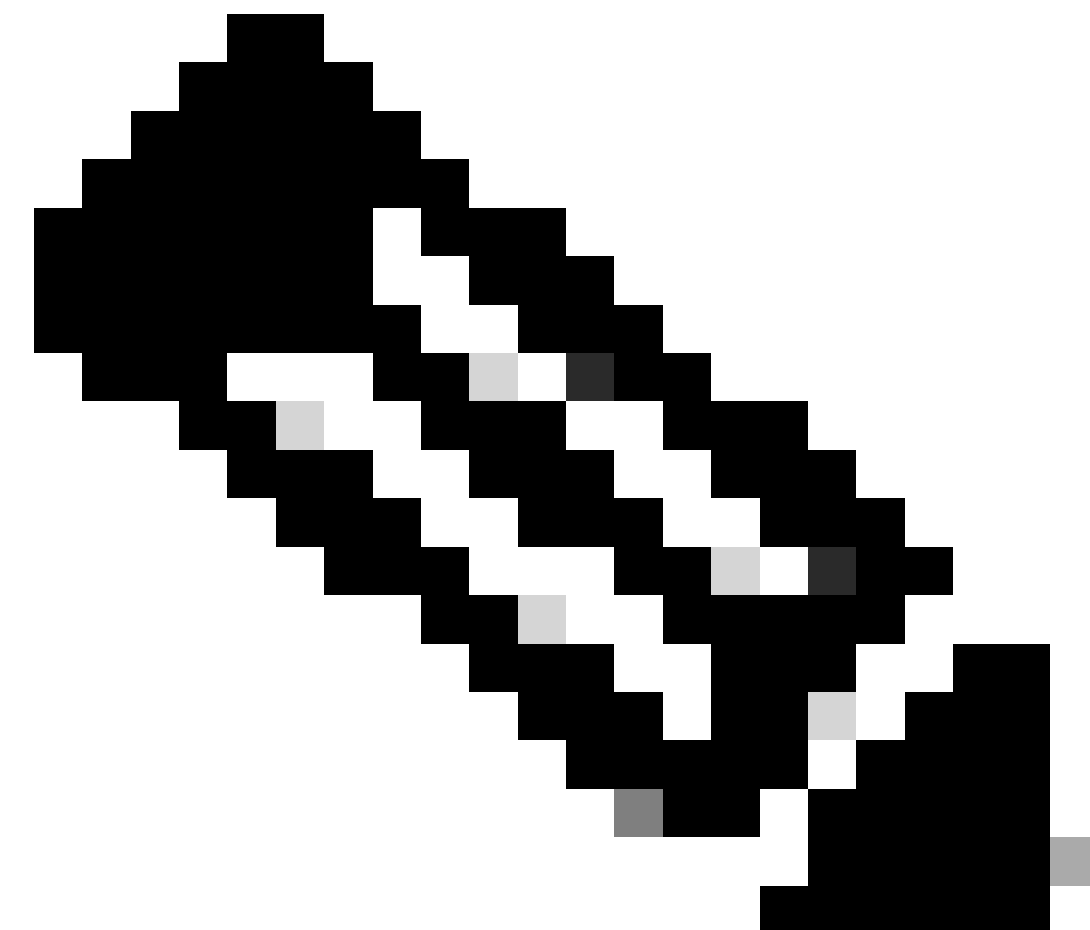
Clone

Admin
Status ▾

Associated
Policy Tags ⓘ ▾

Policy Profile Name

Step 2: Under the **General** tab, define the profile **name**, set **Status** to **Enabled**, and **Disable Central Switching**.



Note: To enable local bridging of client traffic, **Central Switching** must be disabled. Based on the SSID configuration, other options can be enabled or disabled as needed.

General

Access Policies

QoS and AWC

Mobility

Advanced

Name*

Bridge-Policy

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED

Flex NAT/PAT

DISABLED

Cancel

Update & Apply to Device

Step 3: Configure the **VLANID** specified under the VLAN tab of the AP Flex Profile, and click **Update & Apply**.

General	Access Policies	QoS and AVC	Mobility	Advanced
RADIUS Profiling ☐ HTTP TLV Caching ☐ DHCP TLV Caching ☐		WLAN ACL IPv4 ACL Search or Select IPv6 ACL Search or Select		
WLAN Local Profiling Global State of Device Classification Enabled Local Subscriber Policy Name Search or Select		URL Filters Pre Auth Search or Select Post Auth Search or Select		
VLAN VLAN/VLAN Group 100 Multicast VLAN Enter Multicast VLAN				

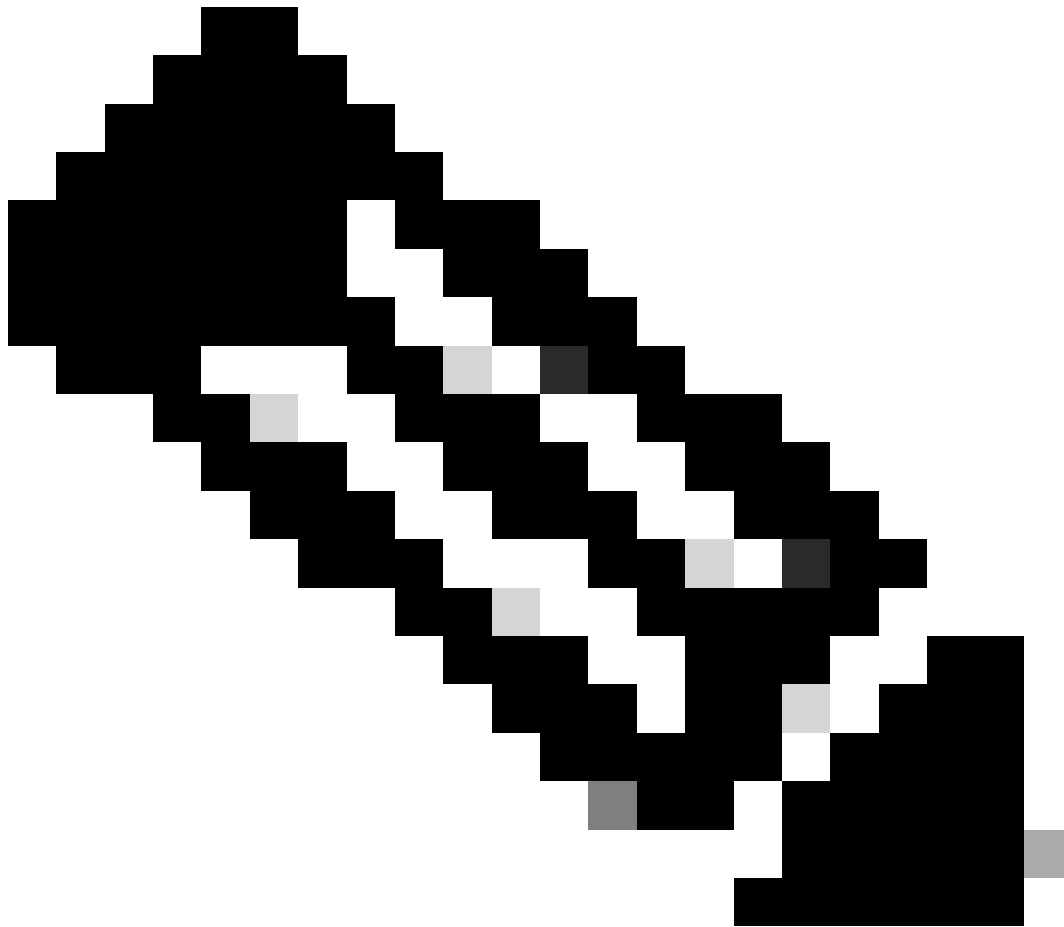
Cancel
 Update & Apply to Device

WLAN Tag

Step 1: Navigate to **Configuration > Tags & Profiles > WLANs** and select **Add**.

Step 2: Under the **General** Tab, Configure the **Profile name**, **SSID** and set the status to **enabled**.

Step 3: Select the Security Tab, Enable **WAP+WPA2** and configure a **Pre-shared key**.



Note: SSID configuration depends entirely on your requirements. For this example, a PSK-based SSID is configured.

General

Security

Advanced

Add To Policy Tags

Profile Name*

Bridge

R

SSID*

Bridge-SSID

WLAN ID*

6

6

St

Status

ENABLED



Broadcast SSID

ENABLED



5

St

Edit WLAN

General
Security
Advanced
Add To Policy Tags

Layer2
Layer3
AAA

☒ WPA + WPA2
☐ WPA2 + WPA3
☐ WPA3
☐ Static WEP
☐ None

MAC Filtering
☐

Lobby Admin Access
☐

WPA Parameters

WPA Policy
☐
WPA2 Policy
☒
OSN Policy
☐

GTK Randomize
☐

Fast Transition

Status
Disabled

Over the DS
☐

Reassociation Timeout *
20

WPA2 Encryption

AES(CCMP128)
☒
CCMP256
☐
GCMP128
☐
GCMP256
☐

Protected Management Frame

PMF
Disabled

Auth Key Mgmt

802.1X
☐
PSK
☒
Easy-PSK
☐
OAKM
☐
FT + 802.1X
☐
FT + PSK
☐
802.1X-SHA256
☐
PSK-SHA256
☐

PSK Format
ASCII

PSK Type
AES

Pre-Shared Key*

Cancel
Update & Apply to Device

Policy Tag

Step 1: Navigate to **Configuration > Tags & Profiles > Tags > Policy** Tab, click **Add**.

Step 2: Create a Policy Tag by defining a **name** and associating the **WLAN** and **Policy Profile**.

Add Policy Tag

Name*

Mesh-Policy-Tag

Description

Enter Description

WLAN-POLICY Maps: 0

+ Add

× Delete

WLAN Profile

Policy Profile

10

No items to display

Map WLAN and Policy

WLAN Profile*

Bridge

Policy Profile*

Bridge-Policy

×

✓

> WLAN-POLICY Maps: 0

Cancel

Apply to Device

Site Tag

Step 1: Navigate to **Configuration > Tags & Profiles > Tags > Site** and click **Add**.

Configuration > Tags & Profiles > Tags

Policy **Site** RF AP

+ Add

× Delete

Clone

Step 2: Configure the Tag **Name**, disable the **Enable Local Site** option, and associate both the **AP Join Profile** and the **Flex Profile**.

Edit Site Tag

Name*

Mesh-Site-Tag

Description

Enter Description

AP Join Profile

Mesh-AP-Join

Flex Profile

Mesh-Flex

Fabric Control Plane Name

Enable Local Site

☐

Load* ⓘ

0

Cancel

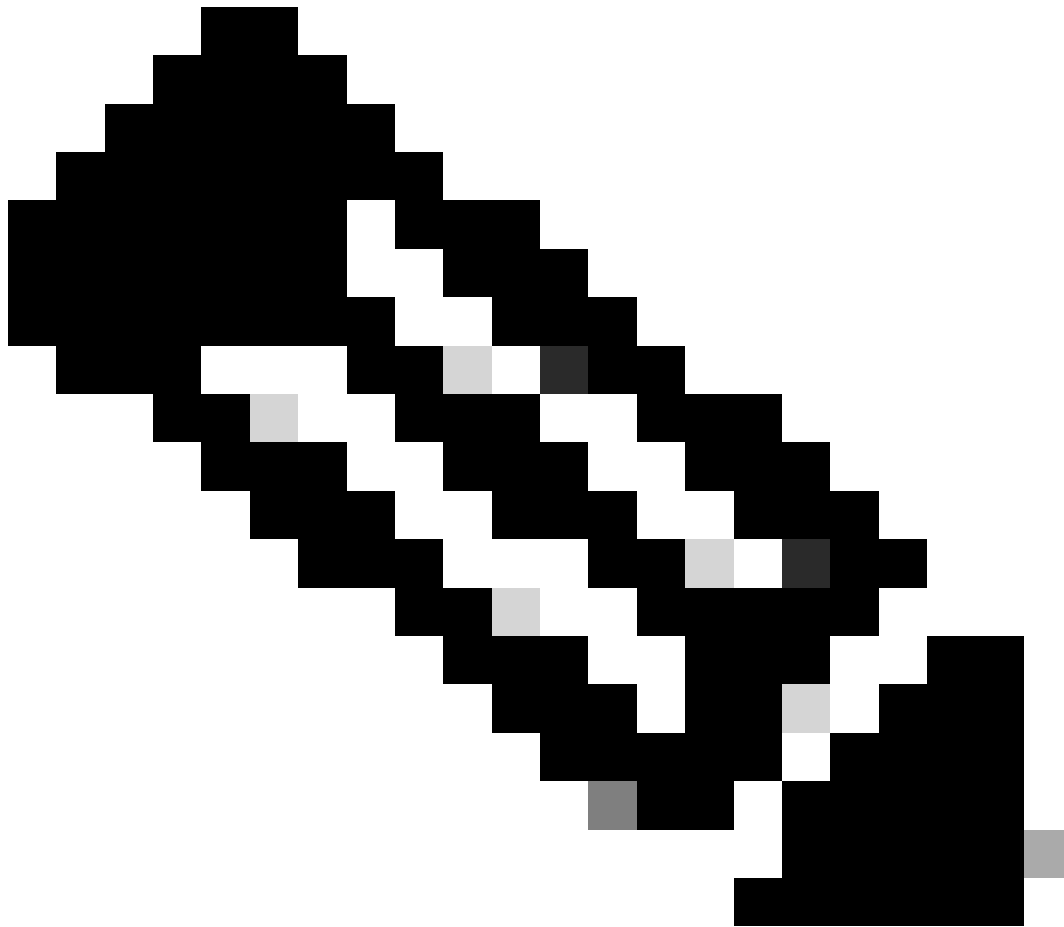
Update & Apply to Device

Configuration of Access Points

This case study assumes the Access Point (AP) is first joined to the Wireless LAN Controller (WLC) in Local Mode and then transitioned to Flex+Bridge mode.

Step 1: Navigate to **Configuration > Wireless > Access Points** and Select the **AP**.

Step 2: Assign the **Site Tag** and **Policy Tag** to the Access Points (APs).



Note: The Access Point (AP) reboots, establish connection with the controller in Flex+Bridge mode, and the Mesh tab is available.

General		Tags	
AP Name*	AP34B8.8314.A204	 Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.	
Location*	default location		
Base Radio MAC	34b8.83fd.05a0		
Ethernet MAC	34b8.8314.a204	Policy	Mesh-Policy-Tag 
Admin Status	ENABLED 	Site	Mesh-Site-Tag 

Step 3: Under the **Mesh** Tab, Select the Role to **Root**

Edit AP

General
Interfaces
High Availability
Inventory
Geolocation
Mesh
Advanced
Support Bundle

General

Ethernet Port Configuration

Block Child
☐

Daisy Chaining
☐

Daisy Chaining strict-RAP
☐

Preferred Parent MAC

Role

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

Port

Mode

VLAN ID*

Step 4: Repeat Steps 1 and 2 for the Access Point (AP) designated to function as a Mesh AP to bring it online in Flex+Bridge mode. Navigate to the **Mesh** tab and configure the role as **Mesh**.

Step 5: The Mesh Access Point is connected to the switch on Port 0, configured in **Trunk Mode**, with the APs VLAN set as **Native VLAN**. Ensure the **allowed VLANs** include the client VLAN specified in the Flex profile.

Step 6: Click **Update and Apply**.

General
Interfaces
High Availability
Inventory
Geolocation
Mesh
Advanced
Support Bundle

General

Ethernet Port Configuration

Block Child
☐

Daisy Chaining
☐

Daisy Chaining strict-RAP
☐

Preferred Parent MAC

Role

Remove PSK

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

Port

Mode

Native VLAN ID*

Allowed VLAN IDs

Switch Port Configuration

```
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 100
switchport mode trunk
end
```

Verify

Mesh AP association to Root AP:

```
#show wireless mesh ap summary
AP Name AP Model BVI MAC BGN AP Role
-----
AP34B8.8314.A204 C9124AXI-ROW 34b8.8314.a204 Default Root AP
APC828.E536.D47C C9124AXI-ROW c828.e536.d47c Default Mesh AP
Number of Flex+Bridge APs : 2
Number of Flex+Bridge RAPs : 1
Number of Flex+Bridge MAPs : 1
```

```
#show wireless mesh ap tree
=====
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=====
[Sector 1]
-----
AP34B8.8314.A204 [0, 0, Default, (36,40), 0000.0000.0000, 5%, 0]
|-APC828.E536.D47C [1, 68, Default, (36,40), 0000.0000.0000, 6%, 0]

Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1
```

Client association on the Mesh AP:

```
#show flexconnect client
Flexconnect Clients:
mac radio vap aid state encr aaa-vlan aaa-acl aaa-ipv6-acl assoc auth switching key-method roam key-pro
52:95:C7:EE:B7:E5 0 0 1 FWD AES_CCM128 none none none Local Central Local Other regular No Yes No 0

#show controllers dot11Radio 0 client
mac radio vap aid state encr Maxrate Assoc Cap is_wgb_wired wgb_mac_addr
52:95:C7:EE:B7:E5 0 0 1 FWD AES_CCM128 MCS92SS HE HE false 00:00:00:00:00:00

#show flexconnect client aaa-override
Flexconnect Clients:
mac vlan qos acl ipv6-acl vlan-name avgdtids avgrtdtids bstdtids bstrtdtids avgdtus avgrtdtus bstdtus bstrt
52:95:C7:EE:B7:E5 none none none none Bridge-VLAN 0 0 0 0 0 0 0 0
```

Traffic from the Mesh Access Point (MAP) is directly bridged to the uplink switch, bypassing the Root Access Point (RAP):

<#root>

DHCP:

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2883] [ 62081:607119] [APC828.E536.D47C]
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2884] chatter: dhcp_req_local_sw_nonat: 1
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2885] [ 62081:607245] [APC828.E536.D47C]
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2885] chatter: dhcp_reply_nonat: 17485791
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2943] [ 62081:613080] [APC828.E536.D47C]
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2943] [ 62081:613123] [APC828.E536.D47C]
```

ARP:

```
May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0572] [ 62464:537183] [APC828.E536.D47C]
May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0572] [ 62464:537219] [APC828.E536.D47C]
May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0573] chatter: ethertype_cl1: 1748579504
May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0628] [ 62464:542842] [APC828.E536.D47C]
May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0629] chatter: fromdevs_arp_resp: arp rep
May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0629] [ 62464:542971] [APC828.E536.D47C]
May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0630] [ 62464:543018] [APC828.E536.D47C]
May 30 04:31:45 APC828.E536.D47C kernel: [*05/30/2025 04:31:45.4301] [ 62465:910100] [APC828.E536.D47C]
```

ICMP:

```
May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3059] [ 62489:785903] [APC828.E536.D47C]
May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3059] [ 62489:785938] [APC828.E536.D47C]
May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3104] [ 62489:790444] [APC828.E536.D47C]
May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3105] [ 62489:790534] [APC828.E536.D47C]
May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3105] [ 62489:790583] [APC828.E536.D47C]
```