

在Catalyst 9800無線LAN控制器上設定網狀網路

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[案例研究1: 網橋模式](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[案例研究2: Flex + 網橋](#)

[設定](#)

[驗證](#)

[疑難排解](#)

簡介

本文說明如何將網狀存取點(AP)連線到Catalyst 9800無線LAN控制器(WLC)的基本組態範例

必要條件

需求

思科建議您瞭解以下主題：

- Catalyst無線9800組態型號
- LAP配置
- 控制和提供無線接入點(CAPWAP)
- 配置外部DHCP伺服器
- 思科交換機的配置

採用元件

此範例使用輕型存取點 (1572AP和1542)，其可設定為根AP(RAP)或網狀AP(MAP)以加入Catalyst 9800 WLC。1542或1562接入點的過程相同。RAP通過Cisco Catalyst交換機連線到Catalyst 9800 WLC。

本文中的資訊係根據以下軟體和硬體版本：

- C9800-CL v16.12.1
- 思科第2層交換器
- 適用於網橋的Cisco Aironet 1572系列輕量型室外接入點部分

- 適用於Flex+Bridge部分的Cisco Aironet 1542

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

案例研究1：網橋模式

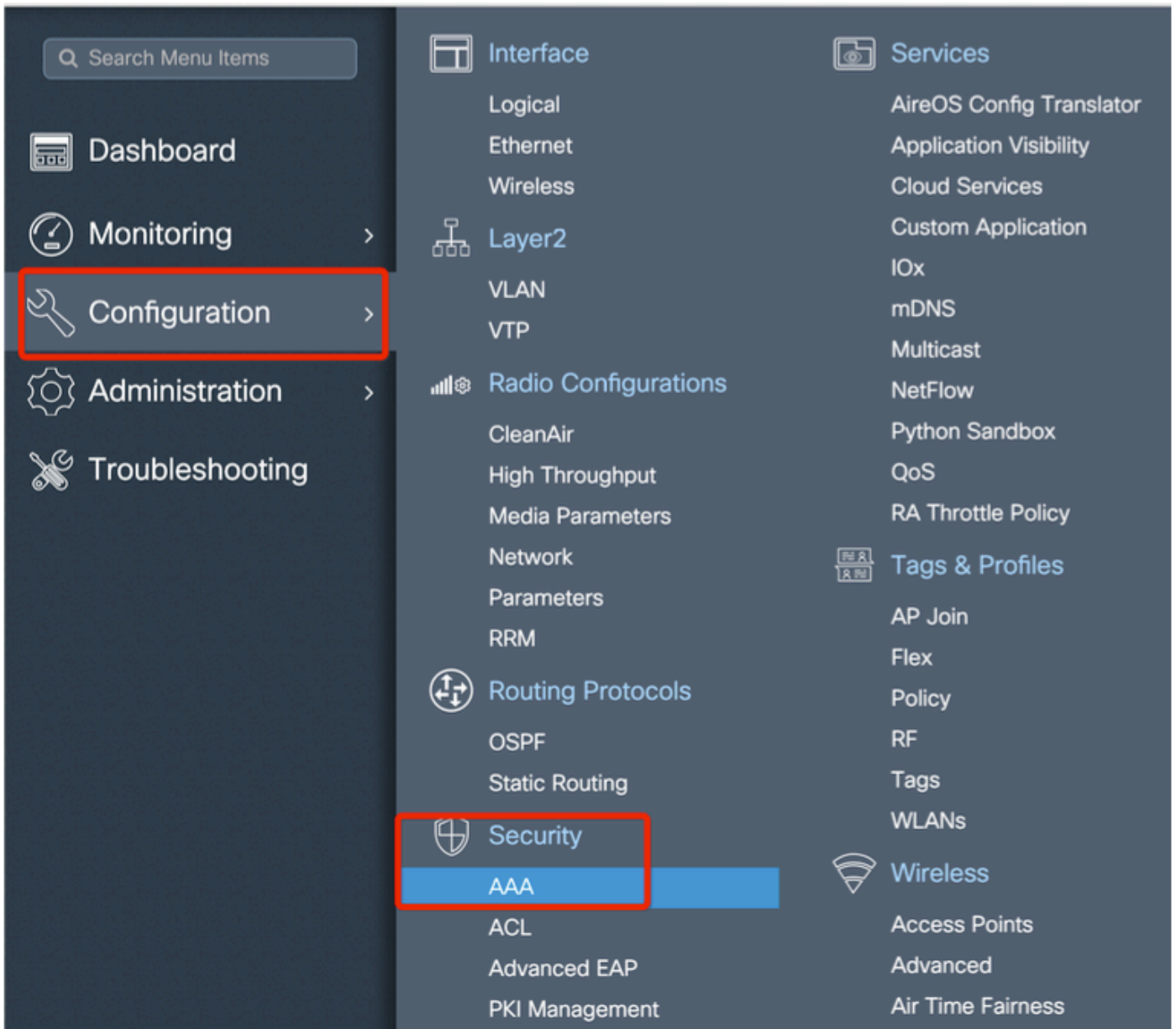
組態

網狀存取點需要透過驗證才能加入9800控制器。本案例研究認為您先以本機模式加入AP到WLC，然後將其轉換為橋接器(a.k.a)網狀模式。


要避免分配AP加入配置檔案，請使用此示例，但配置預設aaa authorization credential-download方法，以便允許任何網狀AP加入控制器。

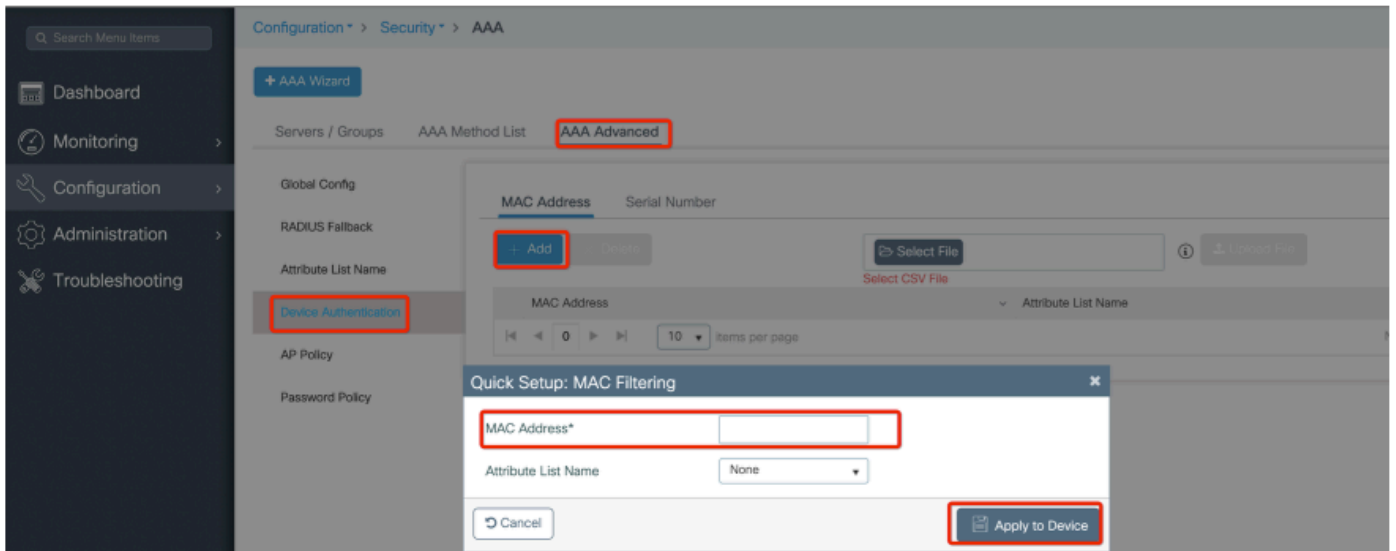
第1步：在Device Authentication下配置RAP/MAP mac地址。

轉至Configuration > AAA > AAA Advanced > Device Authentication。



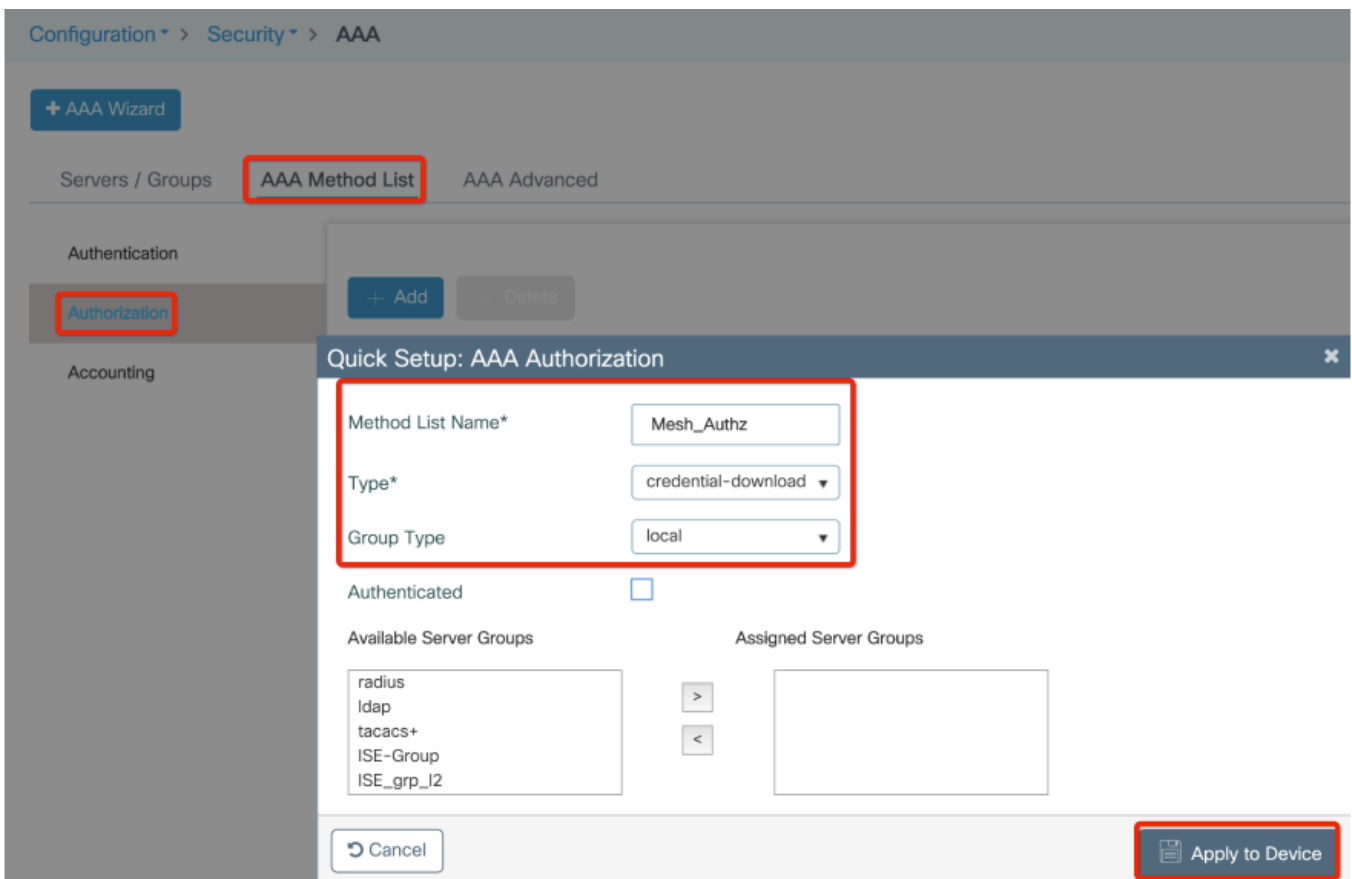
新增網狀無線接入點的基本乙太網MAC地址，新增時不帶任何特殊字元，不帶「。」或「：」

 **重要：**自17.3.1版本起，i如果新增任何mac地址分隔符，如「。」、「：」或「 — 」，則AP無法加入。目前為此版本開啟了兩個增強功能：[思科錯誤ID CSCvv43870](#)和思科錯誤ID [CSCvr07920](#)。將來，9800會接受所有mac地址格式。



第2步：配置身份驗證和授權方法清單。

轉至 Configuration > Security > AAA > AAA Method list > Authentication，然後建立身份驗證方法清單和授權方法清單。



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

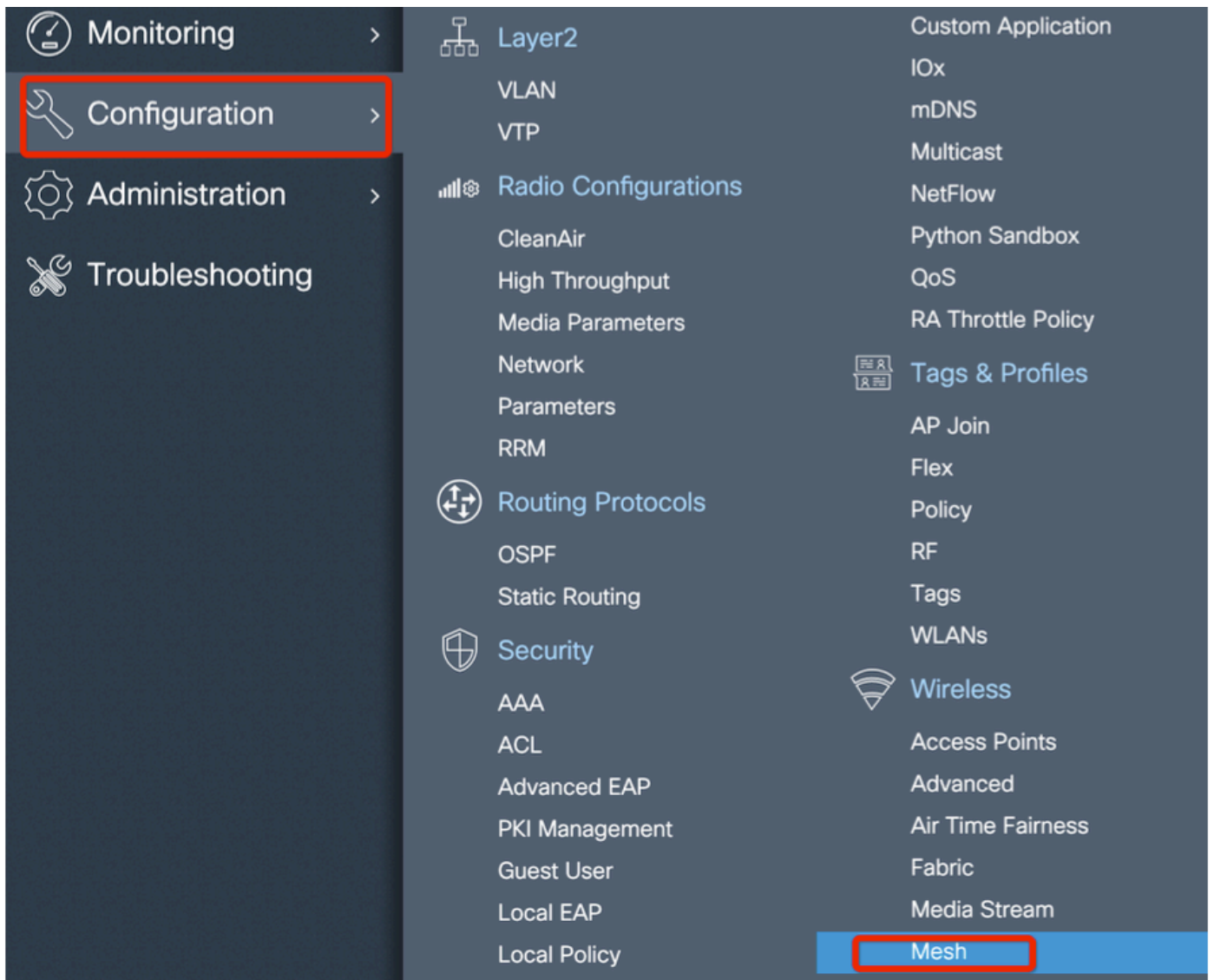
radius
ldap
tacacs+
ISE-Group
ISE_grp_I2

>
<

Cancel Apply to Device

第3步：配置全域性網格引數。

轉至Configuration > Mesh > Global parameters。最初，我們可以將這些值保留為預設值。



第4步：在配置(Configuration)>網格(Mesh)>輪廓(Profile)> +新增(Add)下建立新的網格輪廓

Global Config **Profiles**

+ Add Delete

Number of Profiles : 1

Add 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)

Convergence Method Standard

Background Scanning

Channel Change Notification

LSC

Backhaul amsdu

Backhaul Client Access

Battery State for an AP

Full sector DFS status

Cancel Apply to Device

按一下建立的網格剖面，編輯網格剖面的常規和高級設定。

如圖所示，我們需要將之前建立的身份驗證和授權配置檔案對映到Mesh配置檔案

Configuration > Wireless > Mesh

Global Config **Profiles**

+ Add Delete

Number of Profiles : 1

Name default-mesh-profile

Add Mesh Profile

General **Advanced**

Security

Method EAP

Authentication Method Mesh_Authentication

Authorization Method Mesh_Authz

Ethernet Bridging

VLAN Transparent

Ethernet Bridging

Bridge Group

Bridge Group Name Enter Name

Strict Match

5 GHz Band Backhaul

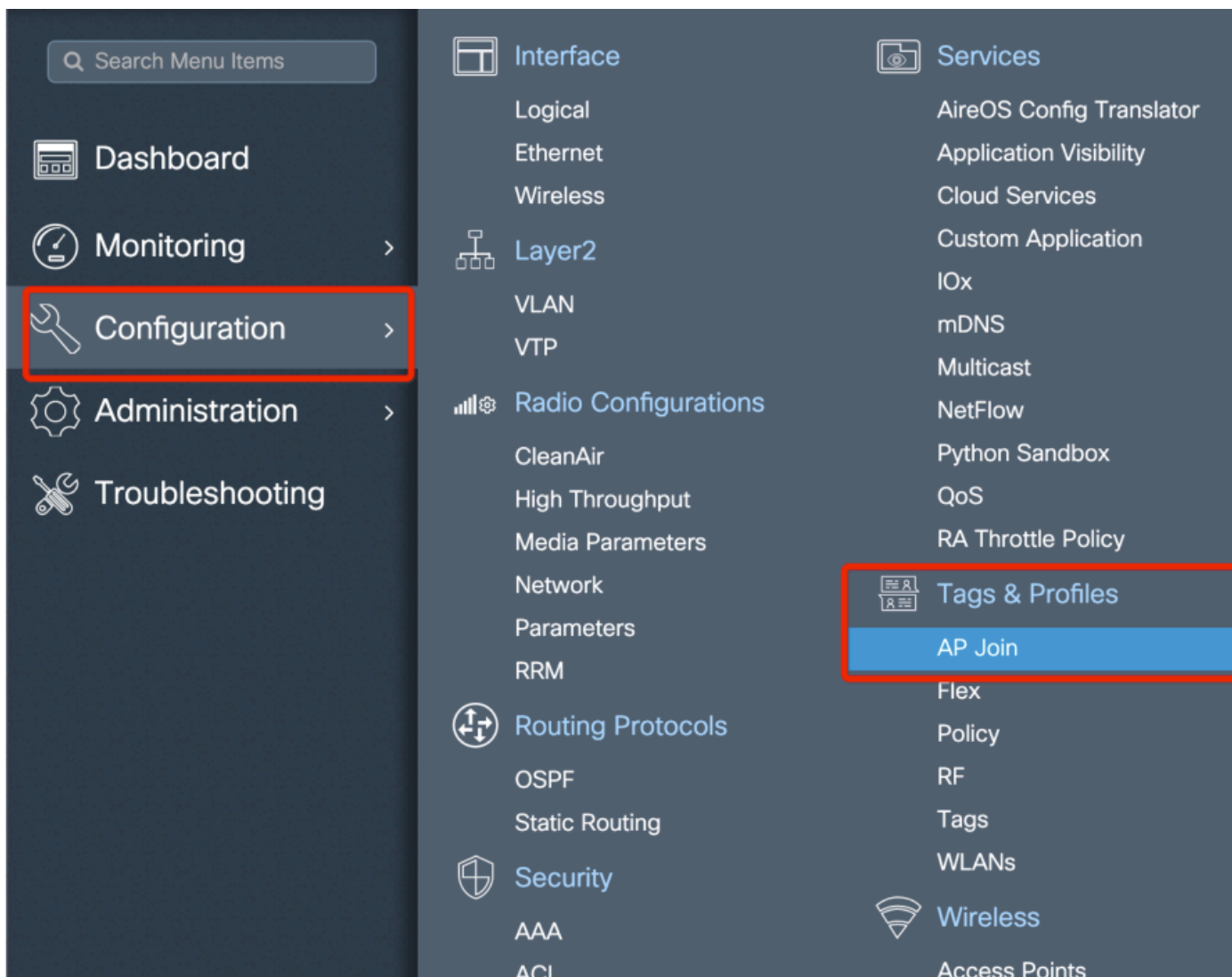
Rate Types auto

2.4 GHz Band Backhaul

Rate Types auto

Cancel Apply to Device

第5步：創建新的AP加入配置檔案。轉至Configure > Tags and Profiles: AP Join。



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

應用先前配置的網狀配置檔案並配置AP EAP身份驗證：

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

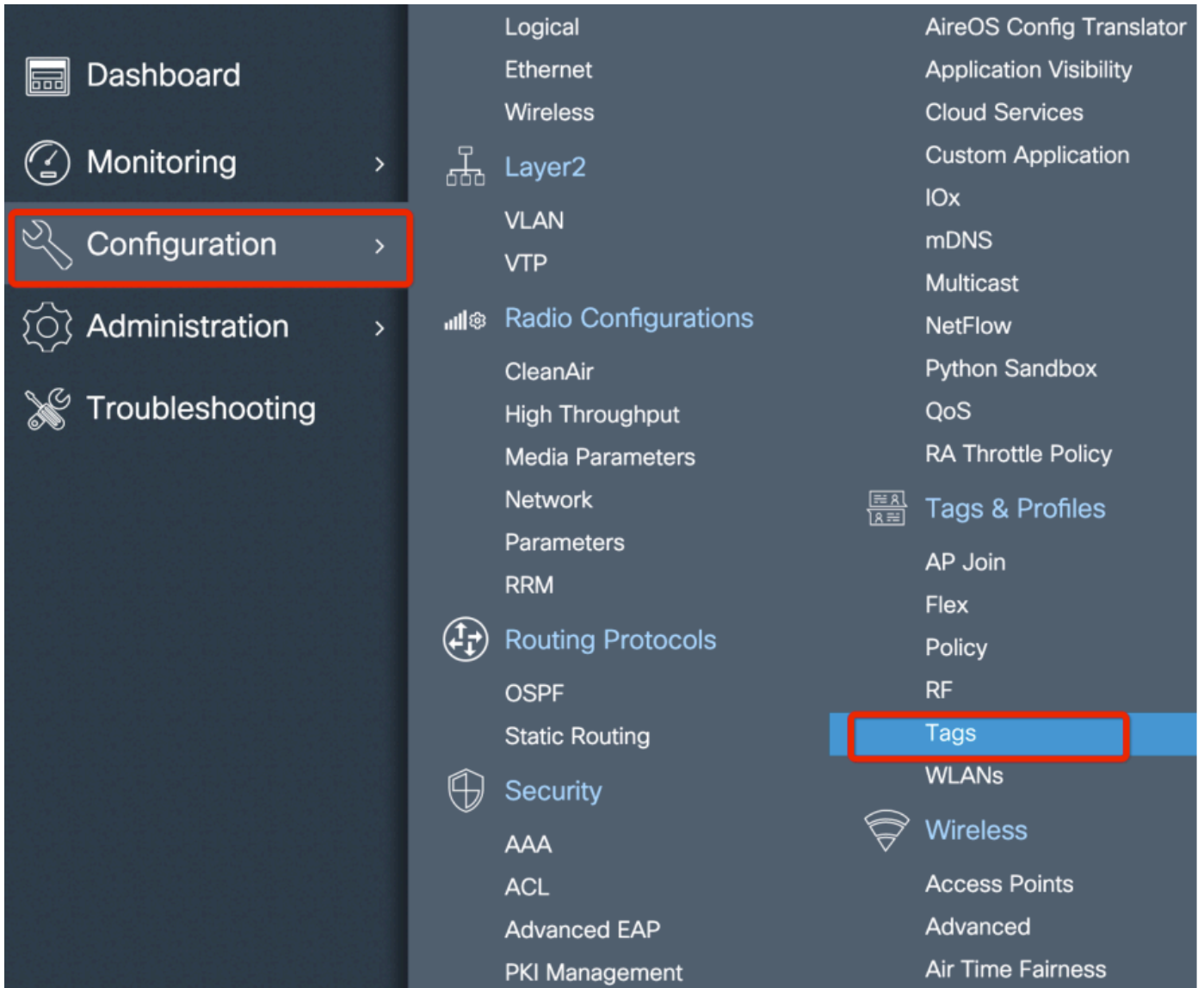
EAP Type

AP Authorization Type

Mesh

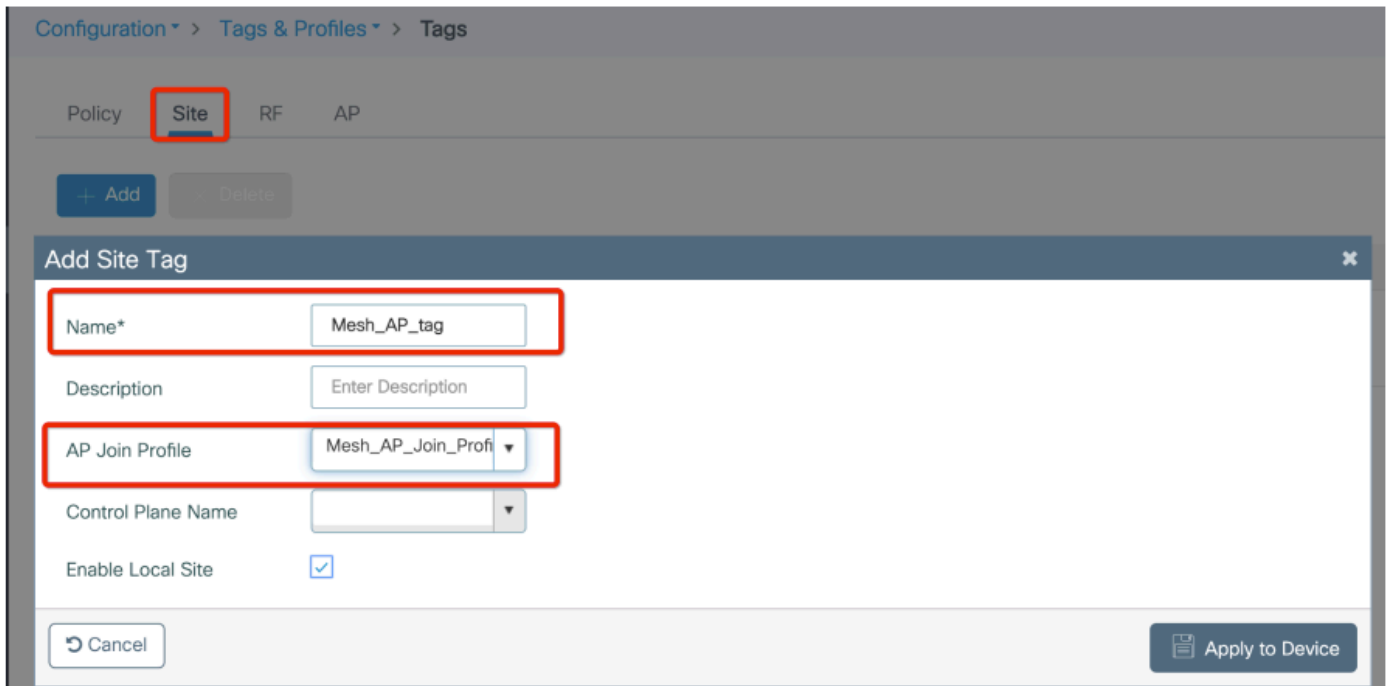
Profile Name [Clear](#)

第6步：建立網格位置標籤，如下所示。



配置按一下在步驟6中建立的Mesh位置TAG對其進行配置。

轉至「站點」頁籤並將先前配置的「網狀AP連線配置檔案」應用到該頁籤：



步驟 7. 將AP轉換為網橋模式。

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

Edit AP

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

General		Version	
AP Name*	AP2C33-110E-6B66	Primary Software Version	17.3.0.17
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	7070.8bb4.9200	Predownloaded Version	N/A
Ethernet MAC	2c33.110e.6b66	Next Retry Time	N/A
Admin Status	ENABLED	Boot Version	1.1.2.4
AP Mode	Bridge	IOS Version	17.3.0.17
Operation Status	Monitor	Mini IOS Version	0.0.0.0
Fabric Status	Sniffer	IP Config	
LED State	Bridge	CAPWAP Preferred Mode	IPv4
	Clear		

您可透過CLI在AP上發出此命令：

```
capwap ap mode bridge
```

AP重新啟動後以橋接模式重新加入。

步驟 8. 現在，您可以定義AP的角色：根AP或網格AP。

當網狀AP透過其嘗試連線到根AP的無線電加入WLC時，根AP是具有有線連線到WLC的AP。

網狀無線接入點在無法通過其無線電找到根AP以進行調配時，可以通過其有線介面加入WLC。

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

> 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

Mesh
 Root
Mesh

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

↶ Cancel
Update & Apply to Device

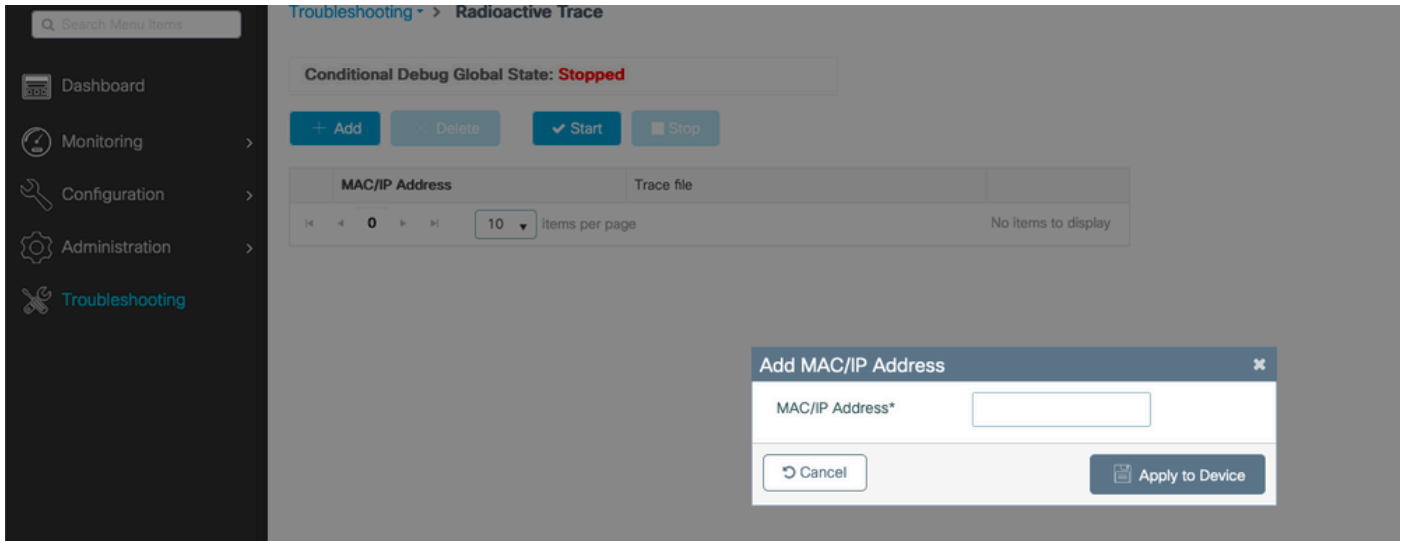
驗證

```

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
    
```

疑難排解

在Troubleshooting > Radiative Trace Web UI頁面中，按一下add並輸入AP MAC地址。



按一下「Start」，然後等待AP再次嘗試加入控制器。

完成後，按一下Generate並選擇收集日誌的時間段（例如，過去10或30分鐘）。

按一下跟蹤檔名從瀏覽器下載。

以下範例顯示由於定義了錯誤的aaa授權方法名稱而未加入AP：

```
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
```

按一下未加入的AP時，在Web UI控制面板中更容易看到相同的內容。「Ap auth pending」是提示，指向AP本身的身份驗證：

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

案例研究2:Flex +網橋

本部分重點介紹1542 AP在Flex+網橋模式下與EAP身份驗證在WLC本地進行的加入過程。

設定

- 步驟 1.導覽至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

- 步驟 2.選擇Device Authentication，然後選擇Add
- 步驟 3.鍵入要加入WLC的AP的基本乙太網MAC地址，將Attribute List Name留空，然後選擇Apply to Device

Quick Setup: MAC Filtering

MAC Address*

ffffffffffff

1

Attribute List Name

None

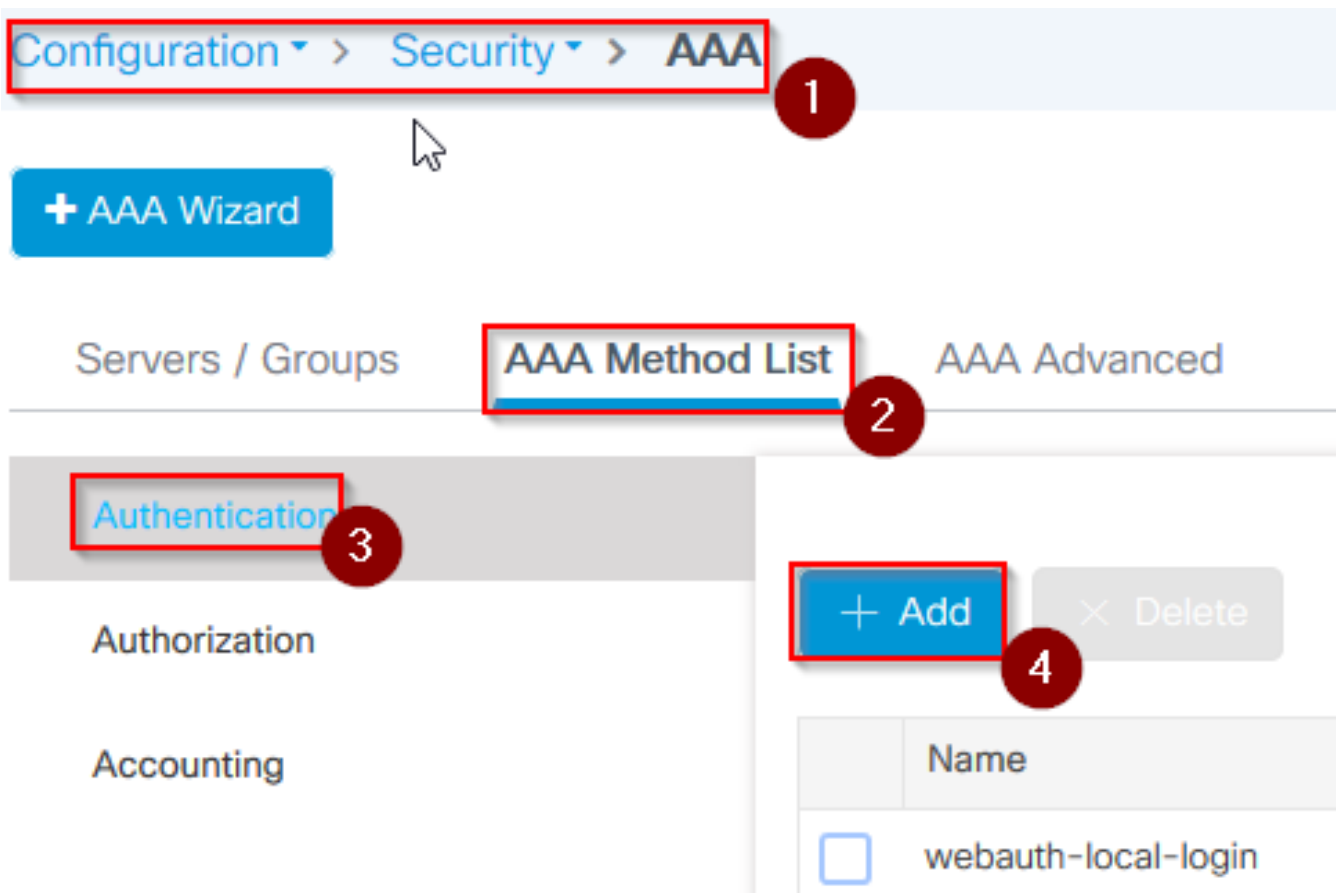
2

Cancel

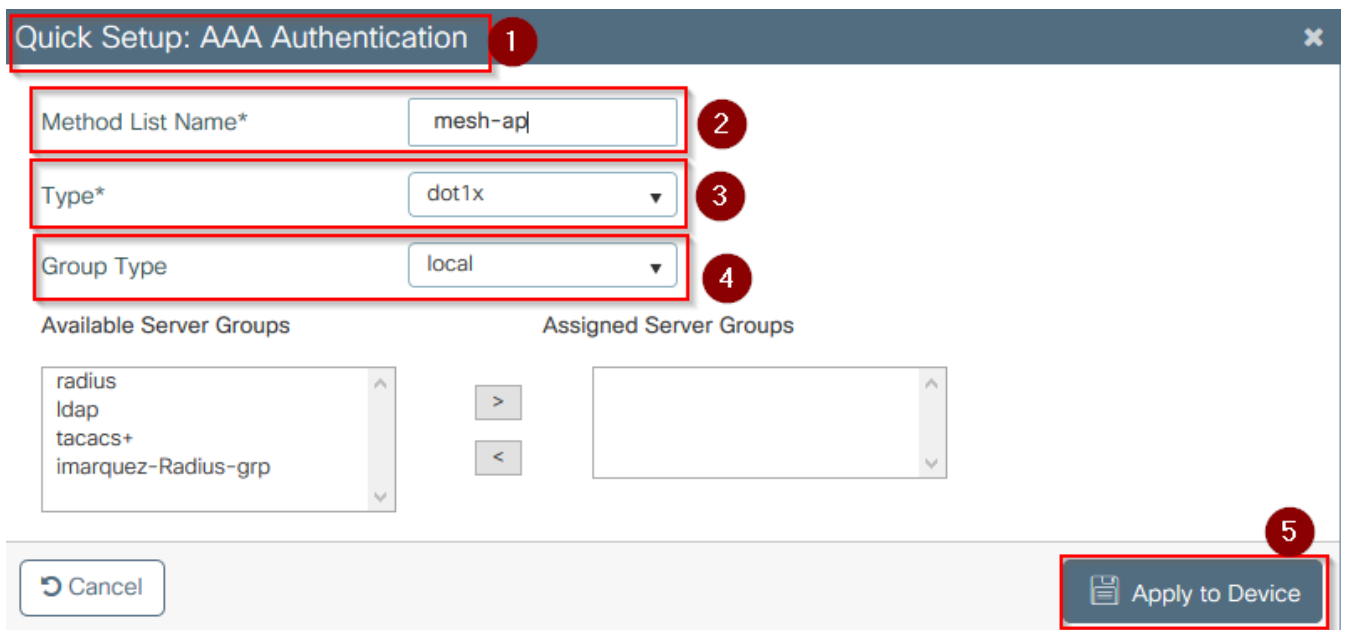
Apply to Device

3

- 步驟 4.導覽至Configuration > Security > AAA > AAA Method List> 驗證
- 步驟 5.選擇Add，系統將顯示AAA Authentication彈出視窗



- 步驟 6.在Method List Name中鍵入名稱，從Type*下拉選單中選擇802.1x，並為Group Type選擇local，最後選擇Apply to Device



- 第6b步：如果您的AP直接以網橋模式加入，並且之前未分配站點和策略標籤，請重複步驟 6，但使用預設方法。
- 配置指向本地的dot1x aaa身份驗證方法(CLI aaa authentication dot1x default local)
- 步驟 7.導覽至Configuration > Security > AAA > AAA Method List> Authorization
- 步驟 8.選擇Add，系統將顯示AAA Authorization彈出視窗

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

- 步驟 9.在Method List Name中鍵入名稱，從Type*下拉選單中選擇credential download，然後為Group Type選擇local，最後選擇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

- 第9b步：如果您的AP直接以網橋模式加入（即它不會首先以本地模式加入），請對預設憑證下載方法(CLI aaa authorization credenticate-download default local)重複步驟9
- 步驟 10.導覽至Configuration > Wireless > Mesh > Profiles
- 步驟 11.選擇Add，此時會顯示Add Mesh Profile彈出視窗

Configuration ▾ > Wireless ▾ > Mesh

1

Global Config

Profiles

2

+ Add

× Delete

3

- 步驟 12.在「General」頁籤中，為「網格」輪廓設定名稱和說明

Add Mesh Profile

General

Advanced

Name*

mesh-profile|

Description

mesh-profile

- 步驟 13.在Advanced頁籤下，為Method欄位選擇EAP
- 步驟 14.選擇步驟6和9中定義的Authorization和Authentication配置檔案，然後選擇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 auto

2.4 GHz Band Backhaul

Rate Types auto

5

Cancel Apply to Device

- 步驟 15.導覽至Configuration > Tag & Profiles > AP Join > Profile
- 步驟 16.選擇Add，出現AP Join Profile彈出視窗，為AP Join配置檔案設定名稱和說明

Configuration ▾ > Tags & Profiles ▾ > AP Join

1

+ Add

× Delete

2

	AP Join Profile Name

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"/>					

- 步驟 17. 導航到AP頁籤，從Mesh Profile Name下拉選單中選擇步驟12中建立的Mesh Profile
- 步驟 18. 確保分別為EAP Type和AP Authorization Type欄位設定EAP-FAST和CAPWAP DTLS
- 步驟 19. 選擇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"/>
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="Clear"/>
AP Authorization Type	<input type="text" value="CAPWAP DTLS"/>	

- 步驟 20. 導覽至Configuration > Tag & Profiles > Tags > Site
- 步驟 21. 選擇「Add」，系統將顯示「站點標籤」彈出視窗

Configuration ▾ > Tags & Profiles ▾ > Tags

1

Policy

Site

2

RF

AP

+ Add

3

× Delete

- 步驟 22. 輸入站點標籤的名稱和說明

Add Site Tag

1

Name*

mesh-ap-site

Description

mesh-ap-site

AP Join Profile

mesh-ap-join-profile ▾

2

- 步驟 23. 從AP Join Profile下拉選單中選擇在步驟16中建立的AP加入配置檔案
- 步驟 24. 在Site Tag彈出視窗的底部，取消選中Enable Local Site覈取方塊以啟用Flex Profile下拉選單。
- 步驟 35. 從Flex Profile下拉選單中，選擇要用於AP的Flex Profile

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile 2

Control Plane Name

Enable Local Site 1

3

- 步驟 36.將AP連線到網路並確保該AP處於本地模式。
- 步驟 37.要確保AP處於本地模式，請發出命令capwap ap ap mode local。

AP必須找到控制器，可以是L2廣播、DHCP選項43、DNS解析或手動設定。

- 步驟 38.AP加入WLC，確保它列在AP清單下，導航至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
	2	✔			Flex+Bridge	Registered
	2	✔			Local	Registered

- 步驟 39.選擇AP，出現AP彈出視窗。
- 步驟 40.在AP彈出視窗的General > Tags > Site頁籤下，選擇Update and Apply to Device下的Site Tag，在步驟22中建立

Edit AP

General **1** Interfaces High Availability Inventory Mesh Advanced

General

AP Name* [text input]

Location* [text input: default location]

Base Radio MAC [text input]

Ethernet MAC [text input]

Admin Status **ENABLED**

AP Mode [dropdown: Flex-Bridge]

Operation Status Registered

Fabric Status Disabled

LED State **ENABLED**

LED Brightness Level [dropdown: 8]

CleanAir NSI Key

Tags

Policy [dropdown: imarquez-FlexLocal]

Site [dropdown: Mesh-AP-Tag] **2**

RF [dropdown: default-rf-tag]

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 [text input]

Static IP (IPv4/IPv6)

Time Statistics

Up Time 4 days 3 hrs 2 mins 6 secs

Controller Association Latency 20 secs

3

Cancel Update & Apply to Device

- 步驟 41.AP重新啟動，必須以Flex +網橋模式連線回WLC

請注意，此方法首先在本地模式（不執行dot1x身份驗證）下加入AP，以應用帶有網格剖面的站點標籤，然後將AP切換到網橋模式。

要加入停滯在Bridge（或Flex+Bridge）模式中的AP，請配置預設方法(aaa authentication dot1x default local和aaa authorization cred default local)。

然後AP能夠進行身份驗證，您之後可以分配標籤。

驗證

確保AP模式顯示為Flex +網橋，如下圖所示。

Configuration > Wireless > Access Points

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

從WLC 9800 CLI運行這些命令，並尋找「AP Mode」屬性。必須列為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
```

疑難排解

確儲存在aaa authentication dot1x default local和aaa authorization cred default local命令。如果您的AP未預先加入本地模式，則需要這些引數。

主9800儀表板有一個顯示無法加入的AP的小部件。按一下它可獲取無法加入的AP清單：

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

按一下特定AP以檢視其未加入的原因。在這種情況下，我們看到身份驗證問題（AP身份驗證掛起），因為站點標籤未分配給AP。

因此，9800沒有選取命名驗證/授權方法來驗證AP：

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

如需更多高級疑難排解，請前往Web UI上的疑難排解 > 放射追蹤頁面。

如果您輸入AP MAC地址，則可以立即生成檔案來獲取嘗試加入的AP的永遠線上（通知級別）日誌。

按一下Start以啟用該MAC地址的高級調試。下次生成日誌時，將顯示AP連線的生成日誌和調試級別日誌。



Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting**

Troubleshooting > Radioactive Trace

[← Back to Troubleshooting Menu](#)

Conditional Debug Global State: **Stopped**

[+ Add](#) [x Delete](#) [✓ Start](#) [■ Stop](#)

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

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。