

在Catalyst 9800 WLC上使用驗證設定FlexConnect

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

簡介

本檔案介紹如何在Catalyst 9800無線LAN控制器上使用中央或本機驗證設定FlexConnect。

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
- FlexConnect
- 802.1x

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- C9800-CL、Cisco IOS-XE® 17.3.4

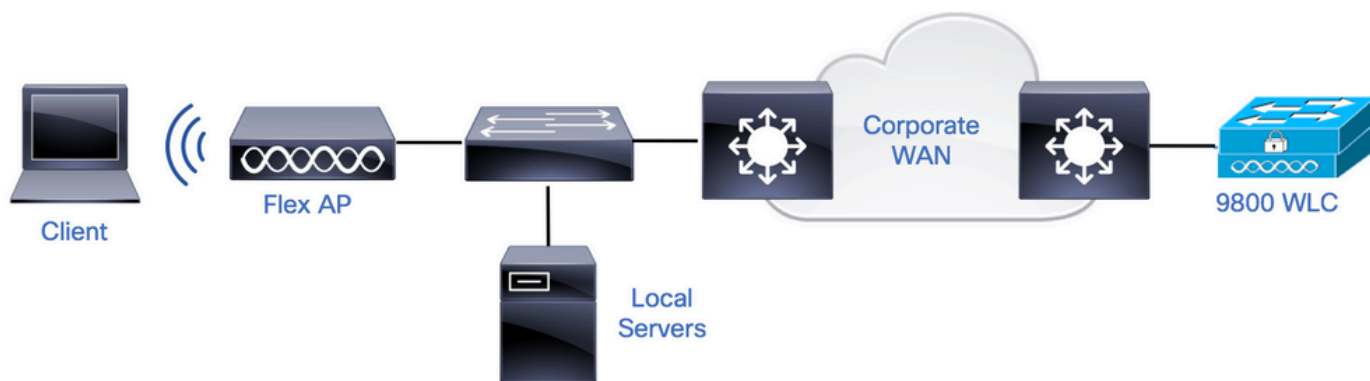
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

FlexConnect是用於遠端辦公室部署的無線解決方案。它允許您通過廣域網(WAN)鏈路從公司辦公室配置遠端位置的接入點(AP)，而無需在每個位置部署控制器。FlexConnect AP可以在本地交換客戶端資料流量，並在與控制器的連線斷開時執行本地客戶端身份驗證。在連線模式下，FlexConnect AP還可以執行本地身份驗證。

設定

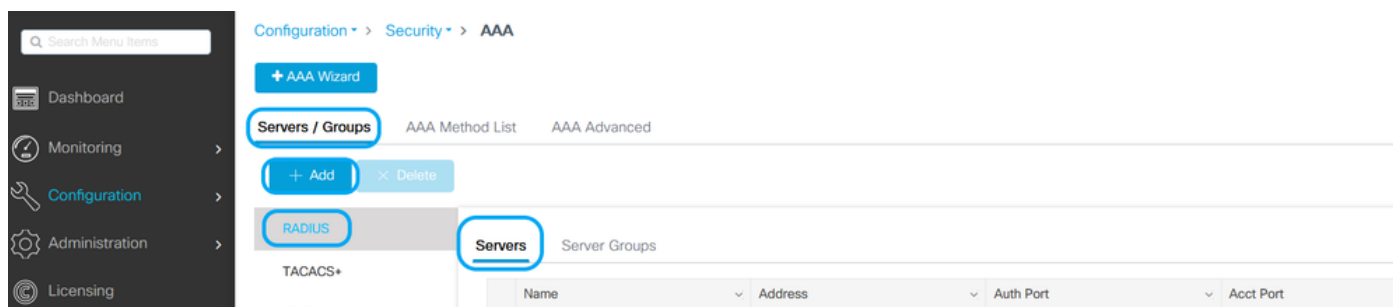
網路圖表



組態

9800 WLC上的AAA組態


步驟 1.宣告RADIUS伺服器。在**GUI**中：導覽至Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Address，然後輸入RADIUS伺服器資訊。



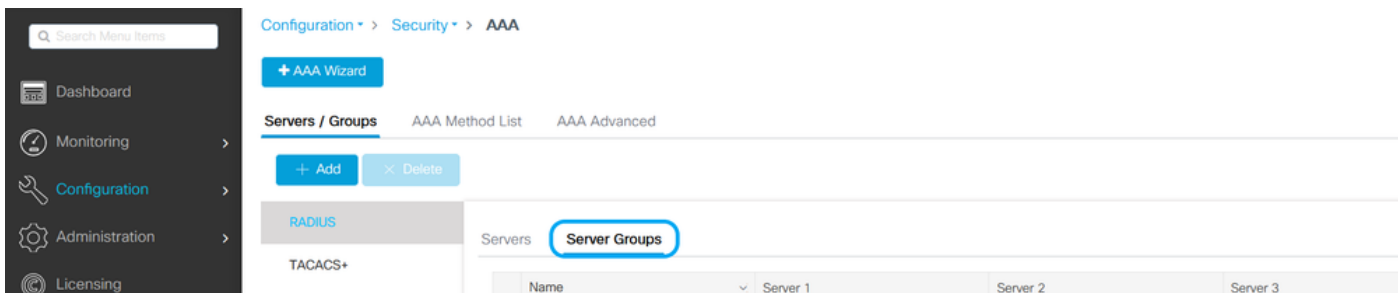
如果您計畫將來使用任何需要CoA的安全型別，請確保支援CoA。

Edit AAA Radius Server ✕

| | |
|--------------------------|---|
| Name* | <input type="text" value="AmmlSE"/> |
| Server Address* | <input type="text" value="10.48.76.30"/> |
| PAC Key | <input type="checkbox"/> |
| Key Type | <input type="text" value="Hidden"/> |
| Key* ⓘ | <input type="password" value="●●●●●●●●●●●●●●●●"/> |
| Confirm Key* | <input type="password" value="●●●●●●●●●●●●●●●●"/> |
| Auth Port | <input type="text" value="1812"/> |
| Acct Port | <input type="text" value="1813"/> |
| Server Timeout (seconds) | <input type="text" value="5"/> |
| Retry Count | <input type="text" value="3"/> |
| Support for CoA | <input checked="" type="checkbox"/> ENABLED |

 **注意：**注意：Flex connect本地身份驗證部署不支援Radius CoA。 .

步驟 2.將RADIUS伺服器新增到RADIUS組。 **在GUI中：** 導航到Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.



The screenshot shows the configuration interface for AAA. The breadcrumb path is Configuration > Security > AAA. Under AAA, there are tabs for Servers / Groups, AAA Method List, and AAA Advanced. The Servers / Groups tab is active, showing a list of server groups. A 'RADIUS' group is selected, and the 'Server Groups' sub-tab is active. Below this, there are buttons for '+ Add' and '× Delete'. A table lists servers: Server 1, Server 2, and Server 3. The 'Server Groups' button is circled in red.

Edit AAA Radius Server Group ✕

| | |
|--------------------------|--------|
| Name* | AmmlSE |
| Group Type | RADIUS |
| MAC-Delimiter | none |
| MAC-Filtering | none |
| Dead-Time (mins) | 2 |
| Source Interface VLAN ID | 76 |

Available Servers

> < >> <<

Assigned Servers

AmmlSE

^ v ^ v ^ v

↶ Cancel 📄 Update & Apply to Device

步驟 3. 建立身份驗證方法清單。在GUI上：導航到 Configuration > Security > AAA > AAA Method List > Authentication > + Add

🔍 Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

+ Add × Delete

| Name | Type |
|------|------|
|------|------|

Quick Setup: AAA Authentication



Method List Name*

Type* ⓘ

Group Type ⓘ

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AmmISE

Cancel

在 CLI 上：

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

WLAN配置

步驟 1. 在GUI上：導覽至Configuration > Wireless > WLANs，然後按一下+Add以建立一個新的WLAN，然後輸入WLAN資訊。然後點選應用到裝置。

The screenshot displays the WLAN configuration interface. At the top, the breadcrumb navigation shows 'Configuration > Tags & Profiles > WLANs'. Below this, there are four buttons: '+ Add' (highlighted with a red circle), 'Delete', 'Enable WLAN', and 'Disable WLAN'. Below the buttons, it indicates 'Number of WLANs selected : 0'. A table with columns for 'Status', 'Name', 'ID', and 'SSID' is visible. Below the table, the 'Add WLAN' dialog box is open, showing the 'General' tab. The dialog has three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab contains the following fields:

- Profile Name*: 802.1x-WLAN
- Radio Policy: All (dropdown menu)
- SSID*: 802.1x
- Broadcast SSID: ENABLED (checkbox)
- WLAN ID*: 1
- Status: ENABLED (checkbox)

At the bottom of the dialog, there are two buttons: 'Cancel' and 'Apply to Device'.

步驟 2. 在GUI上：導覽至Security索引標籤，配置第2層/第3層安全模式（只要加密方法還在使用），並在使用802.1x的情況下配置身份驗證清單。然後按一下Update & Apply to Device。

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

Layer 2 Security Mode

MAC Filtering

Protected Management Frame

PMF

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

PSK

CCKM

FT + 802.1x

FT + PSK

FT + PSK + CCKM

Lobby Admin Access

Fast Transition

Over the DS

Reassociation Timeout

MPSK Configuration

MPSK

Cancel

Update & Apply to Device

原則設定檔組態

步驟 1. 在GUI中：導航至Configuration > Tags & Profiles > Policy，然後點選+Add以建立策略配置檔案。



Search Menu Items



Dashboard

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Status

Policy Profile Name

步驟 2. 新增名稱，並取消選中 Central Switching 框。透過此設定，控制器會處理使用者端驗證，而 FlexConnect 存取點會在本地交換使用者端封包。

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General


Access Policies

QOS and AVC

Mobility

Advanced

Name* Description Status **ENABLED** Passive Client DISABLEDEncrypted Traffic Analytics DISABLED**CTS Policy**Inline Tagging SGACL Enforcement Default SGT **WLAN Switching Policy**Central Switching DISABLEDCentral Authentication **ENABLED** Central DHCP **ENABLED** Central Association DISABLEDFlex NAT/PAT DISABLED

 註：如果禁用了中心交換，則關聯和交換必須始終成對。使用Flexconnect AP時，必須在所有策略配置檔案上禁用中心關聯。

步驟 3. 在**GUI**上：導覽至Access Policies頁籤，分配無線客戶端在預設情況下連線到此**WLAN**時可以分配到的**VLAN**。您可以從下拉選單中選擇一個VLAN名稱，或者作為最佳實踐，手動鍵入VLAN ID。

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local ProfilingGlobal State of Device
Classification

Disabled ⓘ

Local Subscriber Policy Name

 ▼**VLAN**

VLAN/VLAN Group

 ▼

Multicast VLAN

WLAN ACL

IPv4 ACL

 ▼

IPv6 ACL

 ▼**URL Filters**

Pre Auth

 ▼

Post Auth

 ▼

步驟 4.在GUI上：導覽至Advanced 索引標籤，以設定WLAN逾時、DHCP、WLAN Flex Policy和AAA策略，以防它們正在使用。然後點選Update & Apply to Device。

Edit Policy Profile
✕

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

[General](#)
[Access Policies](#)
[QOS and AVC](#)
[Mobility](#)
Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

AAA Policy

Allow AAA Override

NAC State

Policy Name ✕ ▼

Accounting List ▼ ⓘ

Fabric Profile ▼

mDNS Service Policy ▼ [Clear](#)

Hotspot Server ▼

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map ▼ [Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL ▼

Air Time Fairness Policies

2.4 GHz Policy ▼

5 GHz Policy ▼

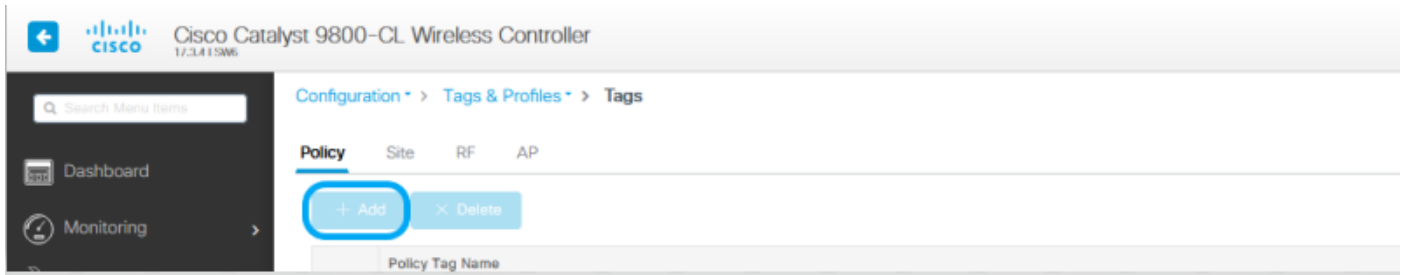
EoGRE Tunnel Profiles

↶ Cancel

📄 Update & Apply to Device

原則標籤組態

步驟 1. 在 **GUI** 中：導航至配置 > 標籤和配置檔案 > 標籤 > 策略 > + 新增。



步驟 2. 分配名稱，並對映之前建立的策略配置檔案和WLAN配置檔案。

Edit Policy Tag



⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Policy

Description

Enter Description

WLAN-POLICY Maps: 1

+ Add

× Delete

| WLAN Profile | Policy Profile |
|--------------|----------------|
| 802.1x-WLAN | VLANX |

10 items per page 1 - 1 of 1 items

Map WLAN and Policy

WLAN Profile*

802.1x-WLAN

Policy Profile*

VLANX



RLAN-POLICY Maps: 0

Cancel

Update & Apply to Device

步驟1.在GUI中：導覽至Configuration > Tags & Profiles > Flex，然後按一下+Add以建立一個新的標籤。

Configuration > Tags & Profiles > Flex

+ Add × Delete

| | Flex Profile Name |
|--------------------------|-------------------|
| <input type="checkbox"/> | Sa_Flex |

Edit Flex Profile

General Local Authentication Policy ACL VLAN Umbrella

Name* Flex-Pro Fallback Radio Shut

Description Enter Description Flex Resilient

Native VLAN ID 71 ARP Caching

HTTP Proxy Port 0 Efficient Image Upgrade

HTTP-Proxy IP Address 0.0.0.0 OfficeExtend AP


CTS Policy

Inline Tagging Join Minimum Latency

SGACL Enforcement IP Overlap

CTS Profile Name default-sxp-profile ✕ ▼ mDNS Flex Profile Search or Select ▼

Cancel Update & Apply to Device

 註：本地VLAN ID是指可分配此Flex配置檔案的AP使用的VLAN，並且該VLAN必須與AP所連線的交換機埠上的本地VLAN ID配置相同。

步驟 2.在VLAN 索引標籤下，新增需要的VLAN、透過Policy Profile預設分配給WLAN的VLAN，或RADIUS伺服器推送的VLAN。然後點選Update & Apply to Device。

Edit Flex Profile

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add - Delete

| VLAN Name | ID | ACL Name |
|---------------------|----|----------|
| No items to display | | |

10 items per page


VLAN Name* VLAN76


VLAN Id* 76

ACL Name Select ACL

Save Cancel

Cancel Update & Apply to Device

 注意：對於Policy Profile，當您選擇分配給SSID的預設VLAN時。如果在此步驟中使用VLAN名稱，請確保在Flex Profile組態中使用相同的VLAN名稱，否則使用者端無法連線到WLAN。

 註：要為flexConnect配置ACL並覆蓋AAA，請僅在「策略ACL」上配置它，如果將ACL分配給特定VLAN，請在新增VLAN時新增ACL，然後在「策略ACL」上新增ACL。

站點標籤配置

步驟 1.在GUI中：導航至Configuration > Tags & Profiles > Tags > Site，然後點選+Add以建立新的站點標籤。取消選中Enable Local Site框以允許AP在本地交換客戶端資料流量，然後新增之前建立的Flex配置檔案。

Search Menu Items

Dashboard

Monitoring

Configuration > Tags & Profiles > Tags

Policy **Site** RF AP

+ Add - Delete

Edit Site Tag

Name* Flex_Site


Description Flex_Site

AP Join Profile default-ap-profile

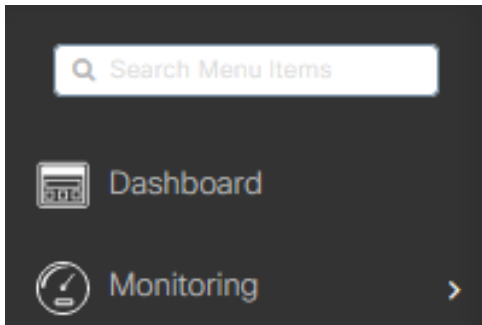
Flex Profile Flex-Pro

Fabric Control Plane Name

Enable Local Site

 注意：禁用「啟用本地站點」後，分配此站點標籤的AP可配置為FlexConnect模式。

步驟 2. 在**GUI**中：導航至Configuration > Wireless > Access Points > AP name，將Site Tag和Policy Tag新增到關聯的**AP**。這可能會導致AP重新啟動其CAPWAP通道並加入回9800 WLC。



Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

General

| | |
|----------------------|---|
| AP Name* | <input type="text" value="talomar1"/> |
| Location* | <input type="text" value="default location"/> |
| Base Radio MAC | b4de.31d7.b920 |
| Ethernet MAC | 005d.7319.bb2a |
| Admin Status | ENABLED <input checked="" type="checkbox"/> |
| AP Mode | <input style="border: 2px solid blue; border-radius: 10px;" type="text" value="Local"/> |
| Operation Status | Registered |
| Fabric Status | Disabled |
| LED State | ENABLED <input checked="" type="checkbox"/> |
| LED Brightness Level | <input type="text" value="8"/> |

Version

| | |
|--------------------------|------------|
| Primary Software Version | 17.3.4.154 |
| Predownloaded Status | N/A |
| Predownloaded Version | N/A |
| Next Retry Time | N/A |
| Boot Version | 1.1.2.4 |
| IOS Version | 17.3.4.154 |
| Mini IOS Version | 0.0.0.0 |

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

| | |
|------------------------|---|
| Policy | <input type="text" value="Policy"/> |
| Site | <input style="border: 2px solid blue; border-radius: 10px;" type="text" value="Flex_Site"/> |
| RF | <input type="text" value="default-rf-tag"/> |
| Write Tag Config to AP | <input type="checkbox"/> |

IP Config

| | |
|-----------------------|--------------------------|
| CAPWAP Preferred Mode | IPv4 |
| DHCP IPv4 Address | 10.48.70.77 |
| Static IP (IPv4/IPv6) | <input type="checkbox"/> |

Time Statistics

| | |
|--------------------------------|-----------------------------|
| Up Time | 0 days 0 hrs 3 mins 28 secs |
| Controller Association Latency | 2 mins 40 secs |

AP連線回後，請注意AP現在處於FlexConnect模式。

All Access Points

Number of AP(s): 1

| AP Name | AP Model | Slots | Admin Status | IP Address | Base Radio MAC | AP Mode | Operation Status | Configuration Status | Policy Tag | Site Tag | RF Tag | Tag Source | Location | Country |
|----------|---------------|-------|--------------------------------------|-------------|----------------|---------|------------------|----------------------|------------|-----------|----------------|------------|------------------|---------|
| talaman1 | AIR-CT5502-K9 | 2 | ● | 10.48.70.77 | b4de.31d7.8920 | Flex | Registered | Healthy | Policy | Flex_Site | default-rt-tag | Static | default location | BE |

使用外部RADIUS伺服器的本機驗證

步驟 1. 將AP作為網路裝置新增到RADIUS伺服器。如需範例，請參閱[如何使用身分識別服務引擎\(ISE\)作為RADIUS伺服器](#)

步驟 2. 建立WLAN。

此組態可以與先前設定的組態相同。

Add WLAN ✕

General

Security

Advanced

Profile Name*

SSID*

WLAN ID*

Status ENABLED

Radio Policy

Broadcast SSID ENABLED

↶ Cancel

📄 Apply to Device

步驟 3. 原則設定檔組態。

您可以建立新配置或使用之前配置的。這一次，取消選中Central Switching、Central Authentication、Central DHCP和Central Association Enable框。

Add Policy Profile



⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

Description

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching DISABLED

Central Authentication DISABLED

Central DHCP DISABLED

Central Association DISABLED

Flex NAT/PAT DISABLED

↶ Cancel

📄 Apply to Device

步驟 4. 原則標籤組態。

將已配置的WLAN與已建立的Policy Profile相關聯。

步驟 5. Flex配置檔案配置。

建立Flex配置檔案，導航到Local Authentication頁籤，配置Radius Server Group，然後選中RADIUS框。

Radius Server Group: AmmISE LEAP

Local Accounting Radius Server Group: Select Accounting S... PEAP

Local Client Roaming: TLS

EAP Fast Profile: Select Profile RADIUS

Users

Select CSV File

| Username | |
|---------------------|--|
| No items to display | |

步驟 6. 站點標籤配置。
配置在步驟5中配置的Flex Profile，並取消選中Enable Local Site框。

Add Site Tag ✕

| | |
|---------------------------|---|
| Name* | <input type="text" value="Local Auth"/> |
| Description | <input type="text" value="Enter Description"/> |
| AP Join Profile | <input type="text" value="default-ap-profile"/> ▼ |
| Flex Profile | <input type="text" value="Local"/> ▼ |
| Fabric Control Plane Name | <input type="text"/> ▼ |
| Enable Local Site | <input type="checkbox"/> |

驗證

在GUI上：導覽至Monitoring > Wireless > Clients，確認Policy Manager State和FlexConnect引數。

集中身份驗證：

[General](#)[QoS Statistics](#)[ATF Statistics](#)[Mobility History](#)[Call Statistics](#)[Client Properties](#)[AP Properties](#)[Security Information](#)[Client Statistics](#)[QoS Properties](#)

| | |
|---------------------------------|-------------------------|
| MAC Address | 484b.aa52.5937 |
| IPv4 Address | 172.16.76.41 |
| User Name | address1 |
| Policy Profile | VLAN2669 |
| Flex Profile | RemoteSite1 |
| Wireless LAN Id | 1 |
| Wireless LAN Name | eWLC_do1x |
| BSSID | 38ed.18c6.902f |
| Uptime(sec) | 9 seconds |
| CCX version | No CCX support |
| Power Save mode | OFF |
| Supported Rates | 9.0,18.0,36.0,48.0,54.0 |
| Policy Manager State | Run |
| Last Policy Manager State | IP Learn Complete |
| Encrypted Traffic Analytics | No |
| Multicast VLAN | 0 |
| Access VLAN | 2669 |
| Anchor VLAN | 0 |
| Server IP | 10.88.173.94 |
| DNS Snooped IPv4 Addresses | None |
| DNS Snooped IPv6 Addresses | None |
| IPv6 DNS Capable | No |
| FlexConnect Data Switching | Local |
| FlexConnect DHCP Status | Local |
| FlexConnect Authentication | Central |
| FlexConnect Central Association | Yes |

本地身份驗證：

| General | QOS Statistics | ATF Statistics | Mobility History | Call Statistics |
|---------------------------------|----------------|--------------------------|-------------------|-----------------|
| Client Properties | AP Properties | Security Information | Client Statistics | QOS Properties |
| MAC Address | | 484b.aa52.5937 | | |
| IPv4 Address | | 172.16.76.41 | | |
| IPv6 Address | | fe80::80c6e782:7c78:68f9 | | |
| User Name | | address1 | | |
| Policy Profile | | VLAN2669 | | |
| Flex Profile | | RemoteSite1 | | |
| Wireless LAN Id | | 1 | | |
| Wireless LAN Name | | eWLC_do1x | | |
| BSSID | | 38ed.18c6.932f | | |
| Uptime(sec) | | 11 seconds | | |
| CCX version | | No CCX support | | |
| Power Save mode | | OFF | | |
| Policy Manager State | | Run | | |
| Last Policy Manager State | | IP Learn Complete | | |
| Encrypted Traffic Analytics | | No | | |
| Multicast VLAN | | 0 | | |
| Access VLAN | | 2669 | | |
| Anchor VLAN | | 0 | | |
| DNS Snooped IPv4 Addresses | | None | | |
| DNS Snooped IPv6 Addresses | | None | | |
| 11v DMS Capable | | No | | |
| FlexConnect Data Switching | | Local | | |
| FlexConnect DHCP Status | | Local | | |
| FlexConnect Authentication | | Local | | |
| FlexConnect Central Association | | No | | |

您可以使用這些命令驗證當前配置：

在 CLI 上：

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```


疑難排解

WLC 9800提供永遠線上的追蹤功能。這可確保所有與客戶端連線相關的錯誤、警告和通知級別消息均持續記錄，並且您可以在發生事故或故障情況後檢視其日誌。



注意：根據生成的日誌量，您可以將時間從幾小時縮短到幾天。

若要檢視9800 WLC在預設情況下蒐集的追蹤，可以透過SSH/Telnet連線到9800 WLC並執行以下步驟（確保將作業階段記錄到文字檔中）。

步驟 1.檢查控制器當前時間，這樣您就可以跟蹤問題發生時之前的日誌。

在 CLI 上：

```
# show clock
```

步驟 2.根據系統配置的指示，從控制器緩衝區或外部系統日誌中收集系統日誌。這樣可以快速檢視系統運行狀況和錯誤（如果有）。

在 CLI 上：

```
# show logging
```

步驟 3.驗證是否已啟用任何調試條件。

在 CLI 上：

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop


IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address                               Port
-----|-----
```



註：如果找到任何列出的條件，則表示遇到啟用條件（mac地址、ip地址等）的所有進程的跟

 蹤將記錄到調試級別。如此可能會增加記錄量。因此，建議您在未主動偵錯時清除所有條件。

步驟 4. 如果您假設在步驟3中未將所測試的mac地址列為條件，請收集特定mac地址的always-on通知級別跟蹤。

在 CLI 上：

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-
```

您可顯示作業階段中的內容，或可將檔案複製到外部 TFTP 伺服器。

在 CLI 上：

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

條件式偵錯和無線電主動追蹤

如果永遠線上(always-on)跟蹤未為您提供足夠的資訊來確定所調查問題的觸發因素，則可以啟用條件調試並捕獲無線活動(RA)跟蹤，該跟蹤可以為與指定條件（本例中為客戶端mac地址）互動的所有進程提供調試級別跟蹤。要啟用條件調試，請完成以下步驟。

步驟 5. 確保未啟用調試條件。

在 CLI 上：


```
# clear platform condition all
```

步驟 6. 為要監控的無線客戶端mac地址啟用調試條件。

此命令開始監控提供的mac地址達30分鐘（1800秒）。您可選擇將此時間增加至 2085978494 秒。

在 CLI 上：

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

 附註：若要同時監控多個用戶端，請針對每個 MAC 位址執行 `debug wireless mac <aaaa.bbbb.cccc>` 指令。

 注意：您看不到終端會話上客戶端活動的輸出，因為所有內容都在內部緩衝，供以後檢視。

步驟 7. 重現您要監控的問題或行為。

步驟 8. 如果在預設或配置的監控器時間開啟之前重現問題，則停止調試。

在 CLI 上：

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

當監控時間結束或偵錯無線停止後，9800 WLC 會產生本機檔案，名稱如下：

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步驟 9. 收集 MAC 位址活動的檔案。 您可將 `ra_trace.log` 複製到外部伺服器，或將輸出內容直接顯示於螢幕上。

檢查 RA 追蹤檔案的名稱

在 CLI 上：

```
# dir bootflash: | inc ra_trace
```

將檔案複製到外部伺服器：

在 CLI 上：

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

顯示內容：


在 CLI 上：

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步驟 10. 如果根本原因仍不明顯，請收集內部日誌，這些日誌是調試級別日誌的更詳細檢視。您無需再次調試客戶端，因為您詳細檢視了已收集並內部儲存的調試日誌。

在 CLI 上：

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file r
```

 注意：此命令輸出返回所有進程的所有日誌記錄級別的跟蹤，而且非常大。請聯絡 Cisco TAC 協助剖析此類追蹤。

您可將 ra-internal-FILENAME.txt 複製到外部伺服器，或將輸出內容直接顯示於螢幕上。

將檔案複製到外部伺服器：

在 CLI 上：

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

顯示內容：

在 CLI 上：

```
# more bootflash:ra-internal-<FILENAME>.txt
```

步驟 11. 移除偵錯條件。

在 CLI 上：

```
# clear platform condition all
```

 注意：請確保在故障排除會話後始終刪除調試條件。

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）。