Catalyst 9800無線控制器上具有802.1x AAA覆寫的FlexConnect WLAN

目錄

簡介

本文說明如何使用FlexConnect模式存取點(AP)設定彈性無線LAN控制器(9800 WLC)，以及使用虛擬區域網路(VLAN)驗證、授權及計量(AAA)覆寫進行本地交換的802.1x無線區域網路(WLAN)。

必要條件

需求

思科建議您瞭解以下主題：

- 9800 WLC組態模式
- FlexConnect

採用元件

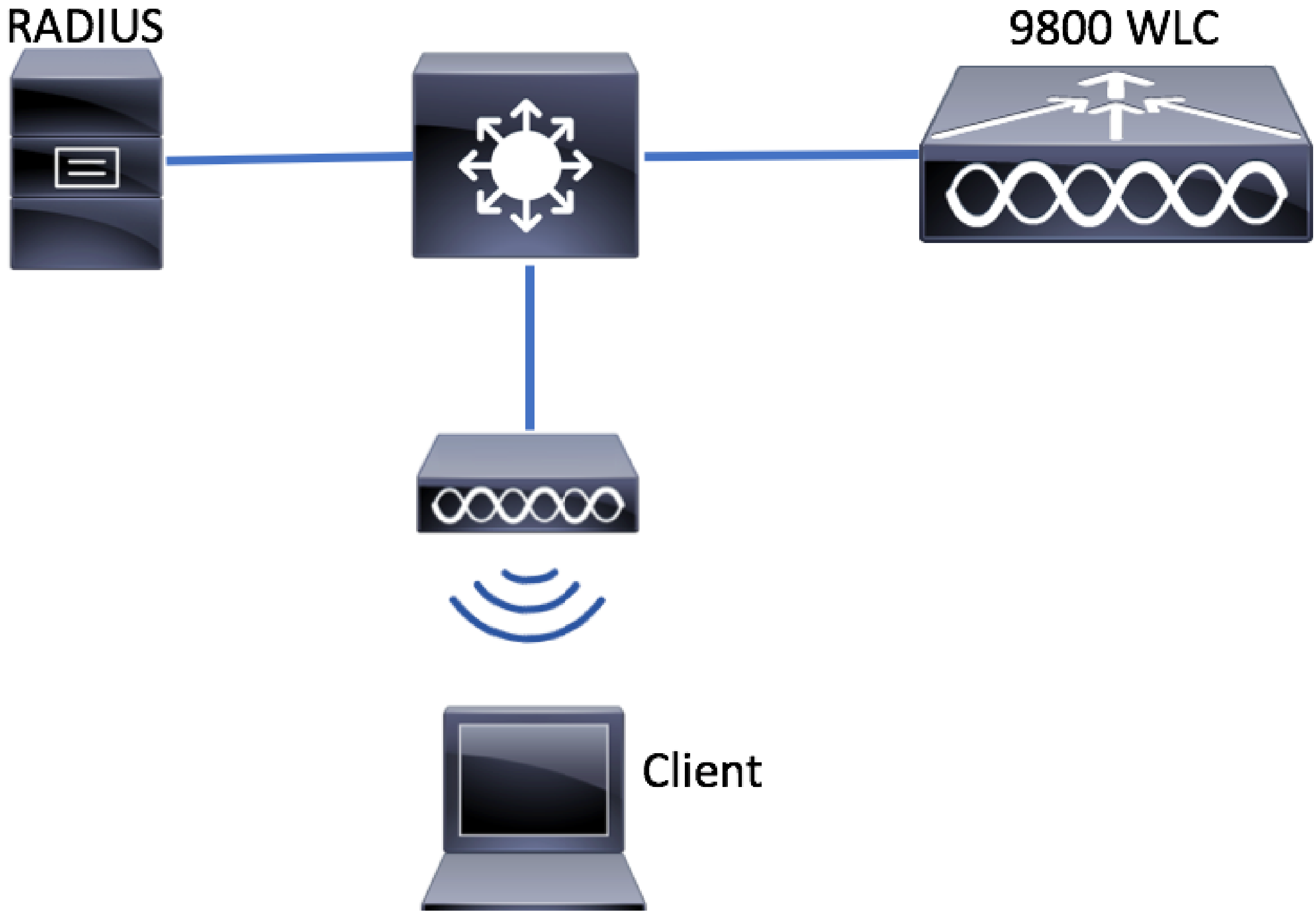
本文中的資訊係根據以下軟體和硬體版本：

- 9800 WLC v16.10

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

網路圖表



組態

9800 WLC 的 AAA 組態

您可以遵循此連結中的說明：

9800 WLC 的 AAA 組態

WLAN配置

您可以遵循此連結中的說明：

WLAN配置

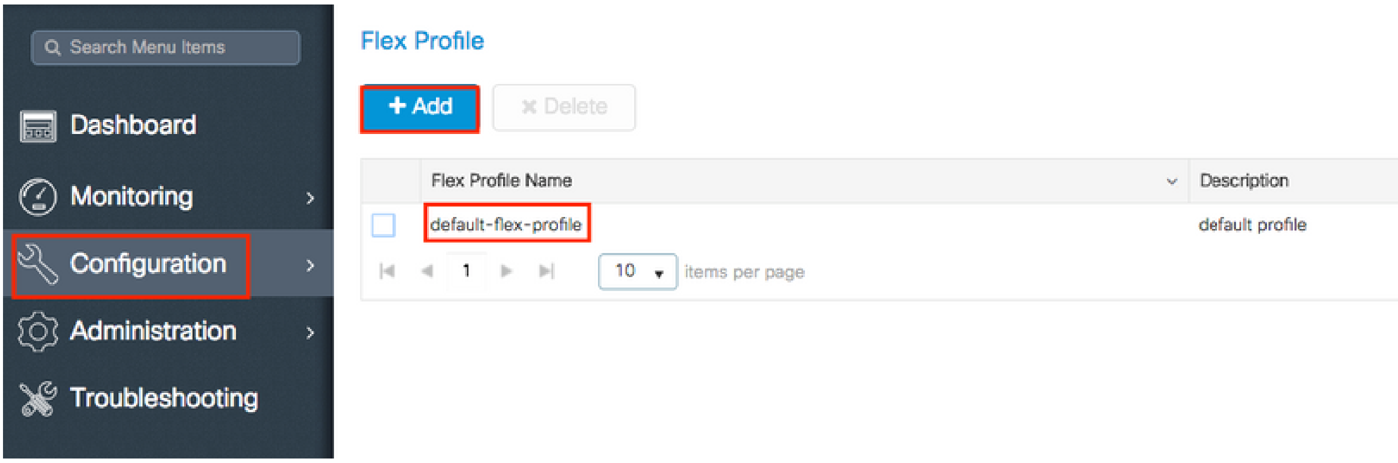
將AP設定為FlexConnect模式

與AireOS配置不同，在9800 WLC上，無法直接從AP配置AP本地或flexconnect模式。按照以下步驟在FlexConnect模式下配置AP。

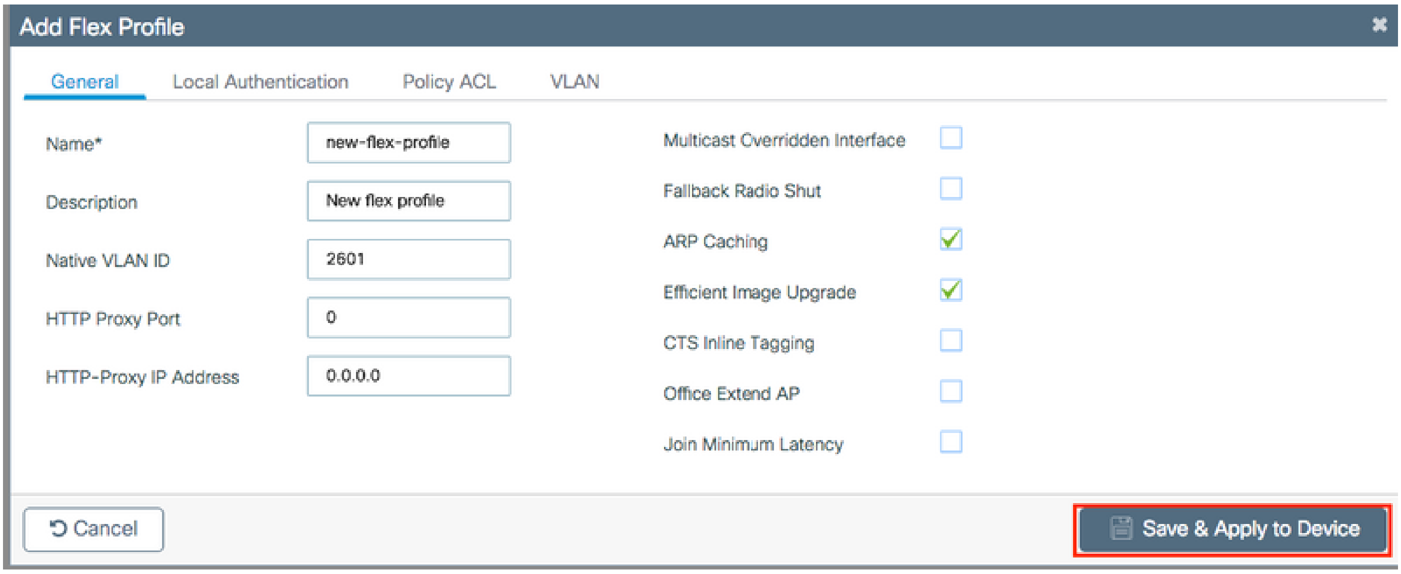
GUI

步驟1.配置Flex配置檔案。

導航至 **配置>標籤與配置檔案>Flex** 並修改**default-flex-profile** 或按一下**+Add**以建立一個新配置檔案。



Flex Profile Name	Description
default-flex-profile	default profile



Name* new-flex-profile

Description New flex profile

Native VLAN ID 2601

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

Multicast Overridden Interface □

Fallback Radio Shut □

ARP Caching ☑

Efficient Image Upgrade ☑

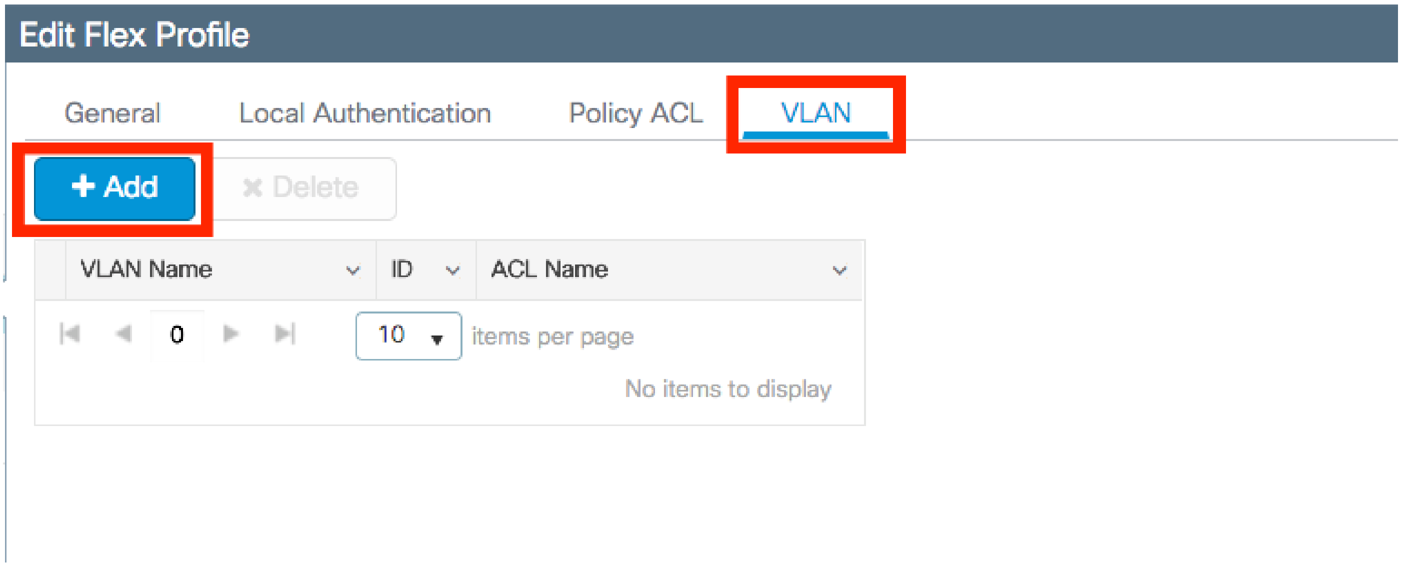
CTS Inline Tagging □

Office Extend AP □

Join Minimum Latency □

步驟2.新增所需的VLAN（預設WLAN的VLAN或從ISE推送的VLAN）。

註：在**策略配置檔案配置一節的步驟3中，選擇分配給SSID的預設VLAN。**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。

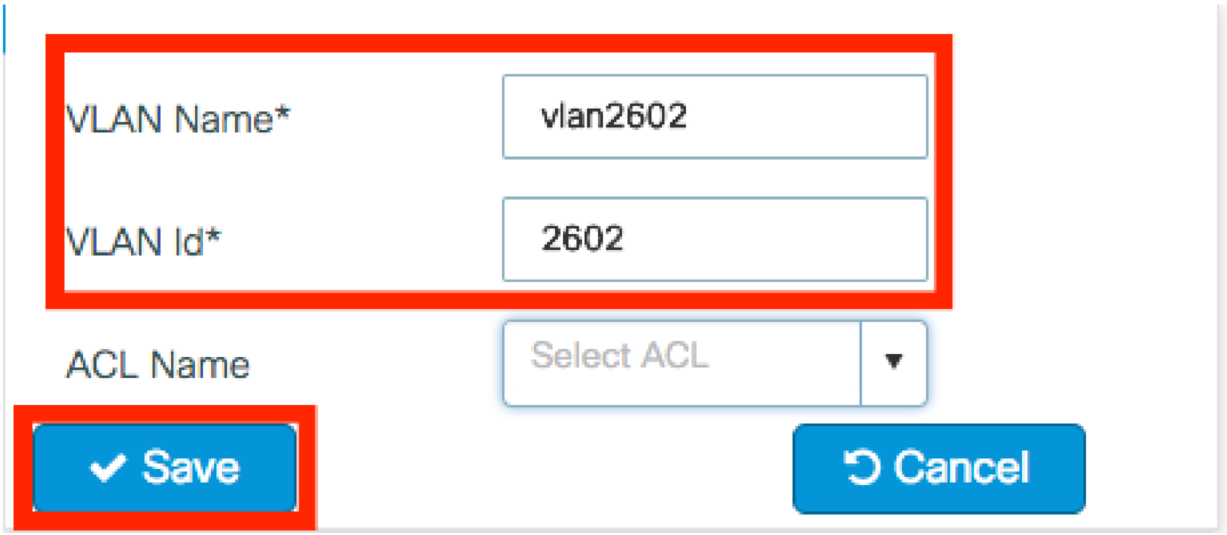


Edit Flex Profile

VLAN Name	ID	ACL Name

No items to display

您可以選擇性為每個VLAN新增特定ACL。

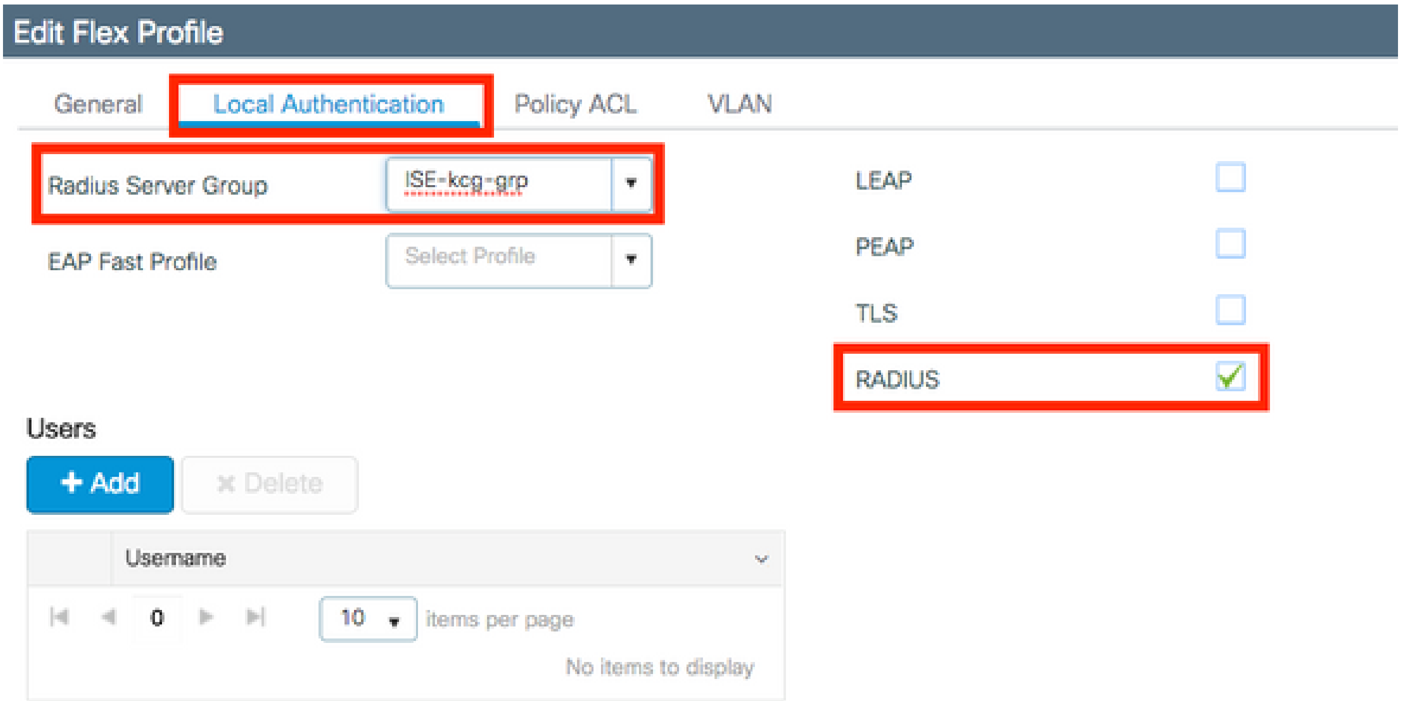


VLAN Name*: vlan2602

VLAN Id*: 2602

ACL Name: Select ACL

或者，分配一個Radius伺服器組以允許FlexConnect AP執行本地身份驗證。



Edit Flex Profile

Radius Server Group: ISE-kcg-grp

EAP Fast Profile: Select Profile

LEAP □

PEAP □

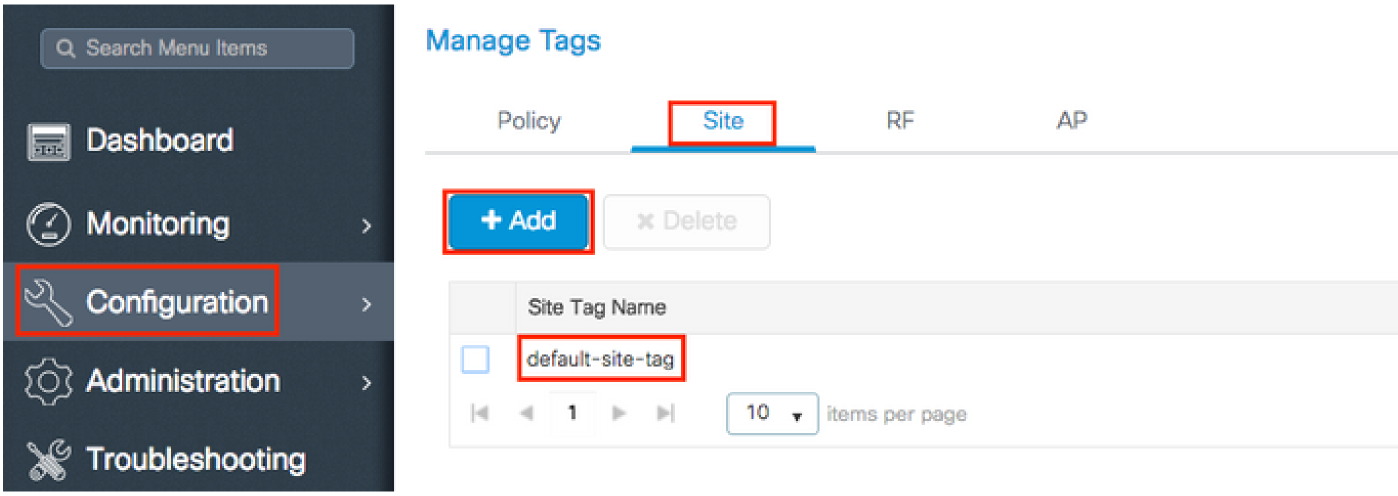
TLS □

RADIUS ☑

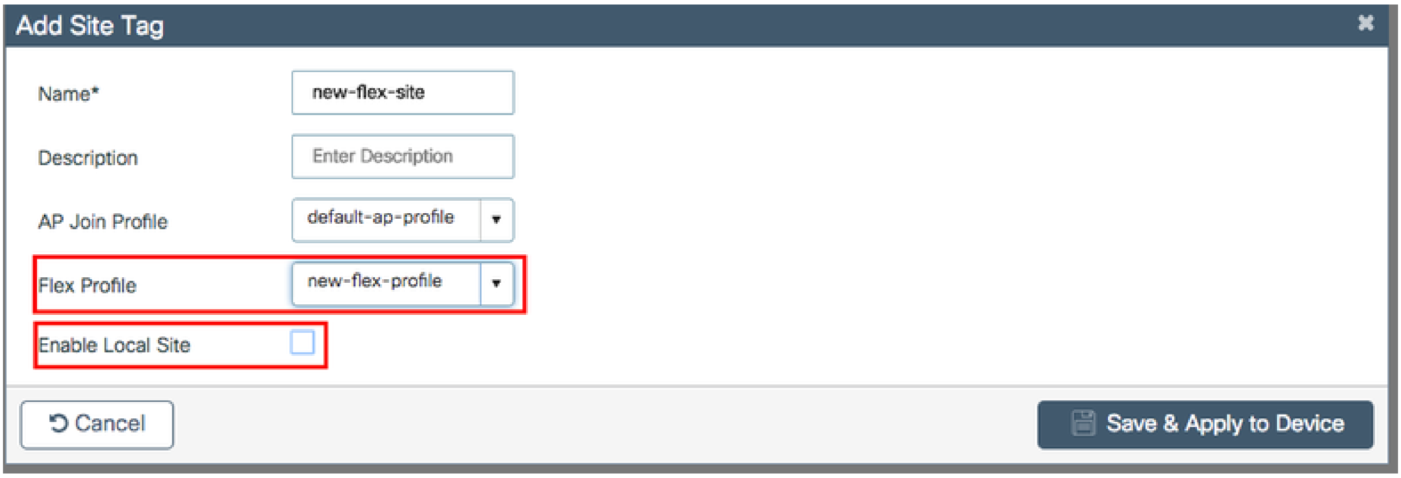
Users

步驟3.配置站點標籤。

導航到**Configuration > Tags & Profiles > Tags > Site**。修改**default-site-tag**（預設情況下分配給所有AP的標籤）或建立一個新標籤(按一下**+Add**建立一個新標籤)。



確保禁用**啟用本地站點**選項，否則**Flex配置檔案**選項不可用。



Add Site Tag

Name*: new-flex-site

Description: Enter Description

AP Join Profile: default-ap-profile

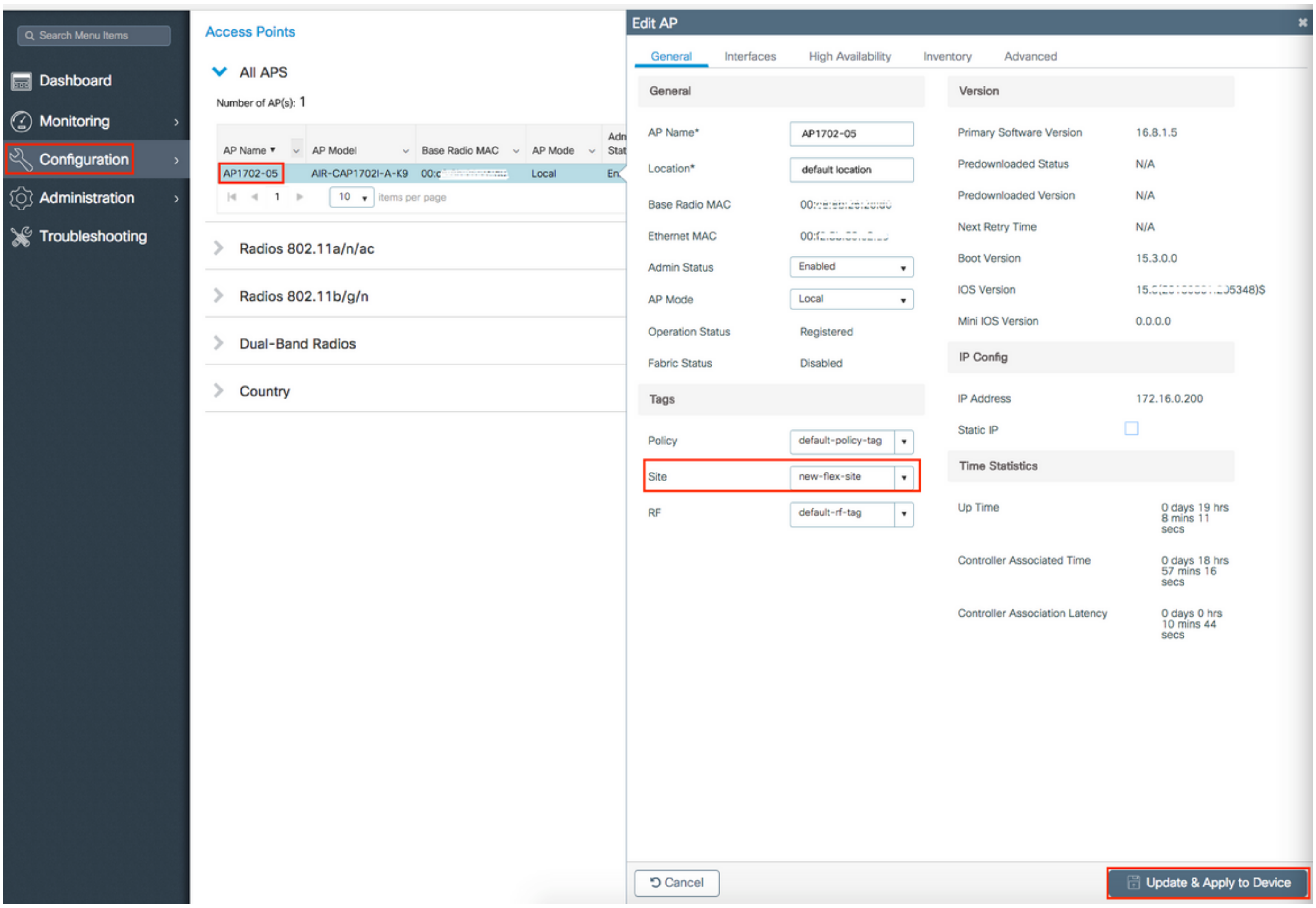
Flex Profile: new-flex-profile

Enable Local Site □

附註：任何獲取啟用了**啟用本地站點**的站點標籤的AP都配置為本地模式。同樣，任何獲取禁用了**啟用本地站點**的站點標籤的AP都配置為flexconnect模式。

步驟4.將AP與9800 WLC關聯並分配在步驟2中配置的站點標籤。

導航到**Configuration > Wireless > Access Points > AP name**並設定Site標籤。然後點選**Update & Apply to Device**以設定更改。



Number of AP(s): 1

AP Name	AP Model	Base Radio MAC	AP Mode	Admin Status
AP1702-05	AIR-CAP1702I-A-K9	00:c[redacted]	Local	En

General

AP Name* AP1702-05
Location* default location
Base Radio MAC 00:[redacted]
Ethernet MAC 00:[redacted]
Admin Status Enabled
AP Mode Local
Operation Status Registered
Fabric Status Disabled

Tags

Policy default-policy-tag
Site new-flex-site
RF default-rf-tag

Version

Primary Software Version 16.8.1.5
Predownloaded Status N/A
Predownloaded Version N/A
Next Retry Time N/A
Boot Version 15.3.0.0
IOS Version 15.[redacted]5348)$
Mini IOS Version 0.0.0.0

IP Config

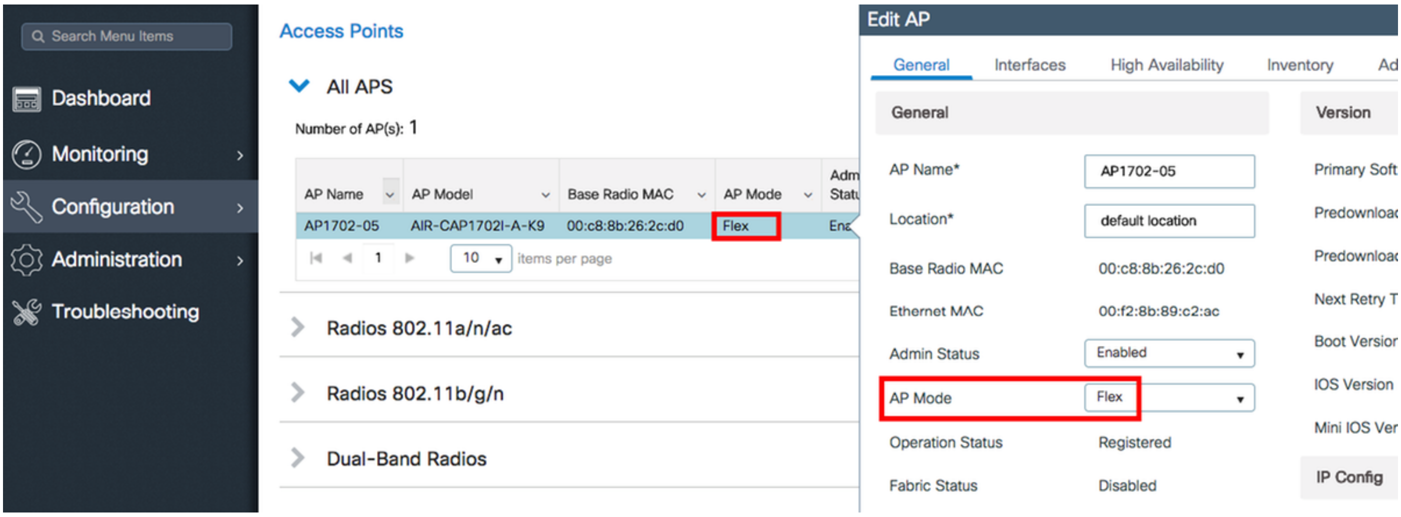
IP Address 172.16.0.200
Static IP □

Time Statistics

Up Time 0 days 19 hrs 8 mins 11 secs
Controller Associated Time 0 days 18 hrs 57 mins 16 secs
Controller Association Latency 0 days 0 hrs 10 mins 44 secs

注意:請注意，變更AP上的標籤後，AP會失去與9800 WLC的關聯，並在約1分鐘內重新加入。

步驟5.當AP連線回後，請注意AP模式為Flex



Number of AP(s): 1

AP Name	AP Model	Base Radio MAC	AP Mode	Adm Statu
AP1702-05	AIR-CAP1702I-A-K9	00:c8:8b:26:2c:d0	Flex	Ena

General

AP Name* AP1702-05

Location* default location

Base Radio MAC 00:c8:8b:26:2c:d0

Ethernet MAC 00:f2:8b:89:c2:ac

Admin Status Enabled

AP Mode Flex

Operation Status Registered

Fabric Status Disabled

CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                                               : FlexConnect
```

交換器組態

配置AP所連線的交換機介面。

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

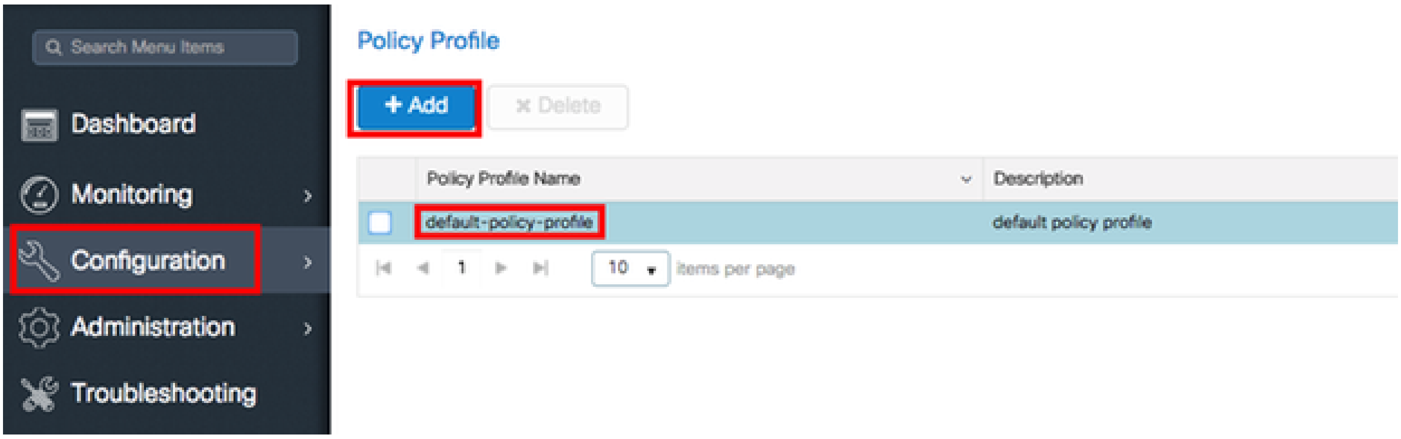
原則設定檔組態

在策略配置檔案中，您可以決定向哪個VLAN分配客戶端，以及其他設定（如訪問控制清單[ACL]、服務品質[QoS]、移動錨點、計時器等）。

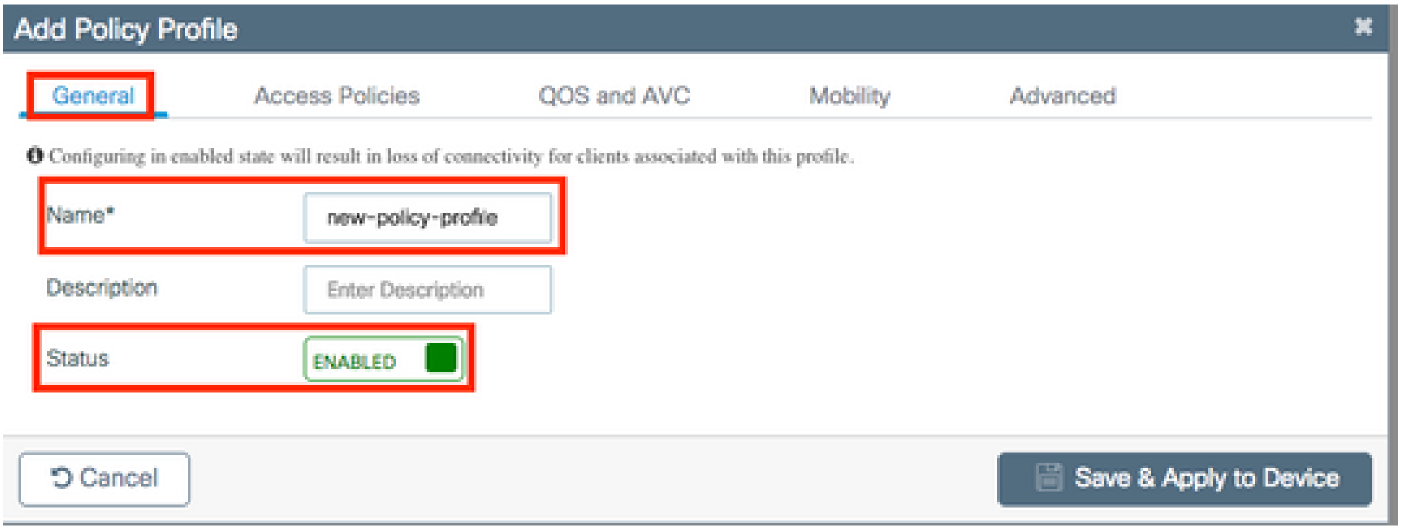
GUI

步驟1.配置要分配給WLAN的策略配置檔案。

導航到**Configuration > Tags & Profiles > Policy**，然後建立新配置檔案或修改**default-policy-profile**。



步驟2.在**General**選項**卡中，為**Policy Profile指定一個名稱，並將其狀態更改為**ENABLED。**



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

Name* new-policy-profile

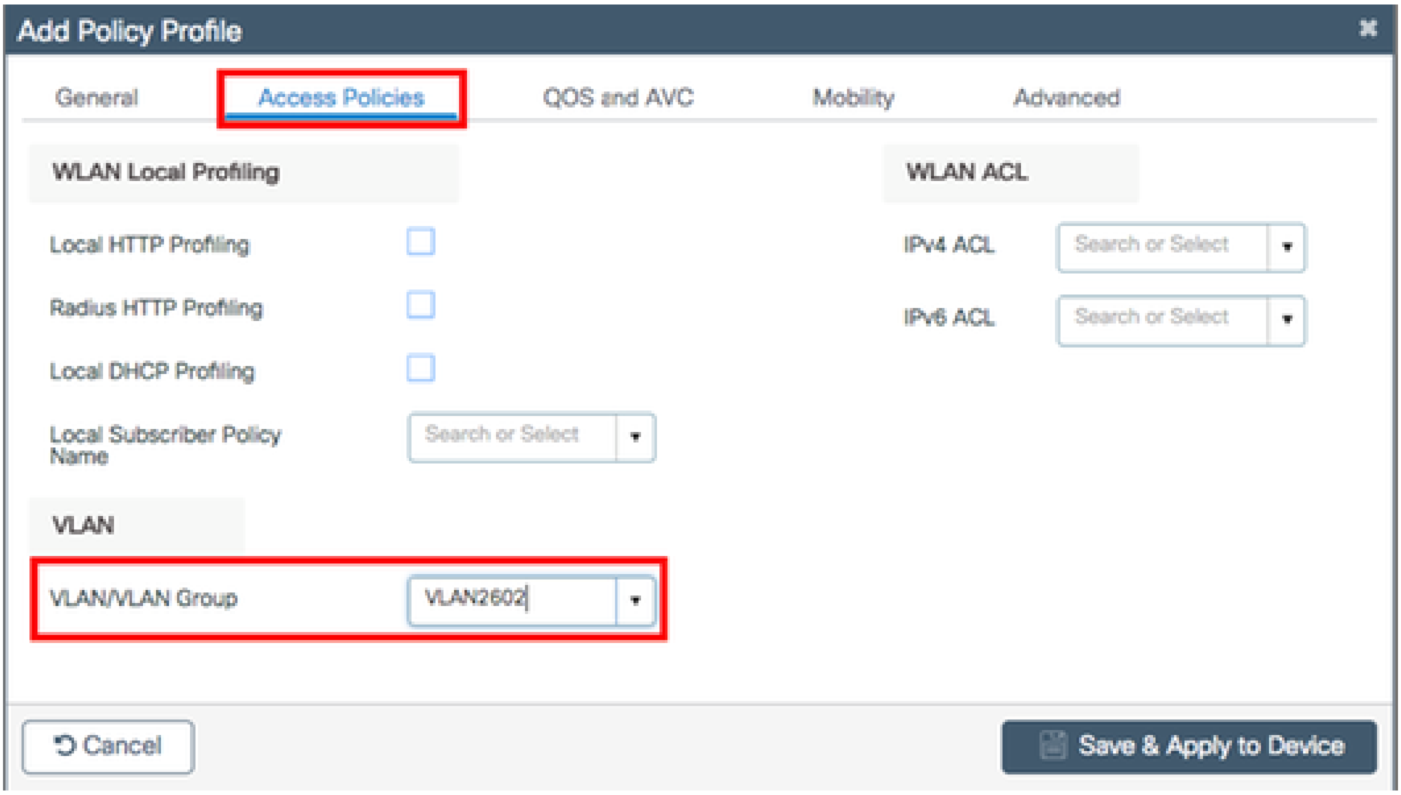
Description Enter Description

Status ENABLED

步驟3.在**Access Policies**索引標籤中，指定無線客戶端在預設情況下連線到此WLAN時分配到的VLAN。

您可以從下拉選單中選擇一個VLAN名稱，也可以手動鍵入VLAN ID。

註:如果從下拉選單中選擇vlan名稱，請確保它與在**將AP設定為FlexConnect模式一節的步驟2中使用的vlan名稱相匹配。**



WLAN Local Profiling

Local HTTP Profiling □

Radius HTTP Profiling □

Local DHCP Profiling □

Local Subscriber Policy Name: Search or Select

VLAN

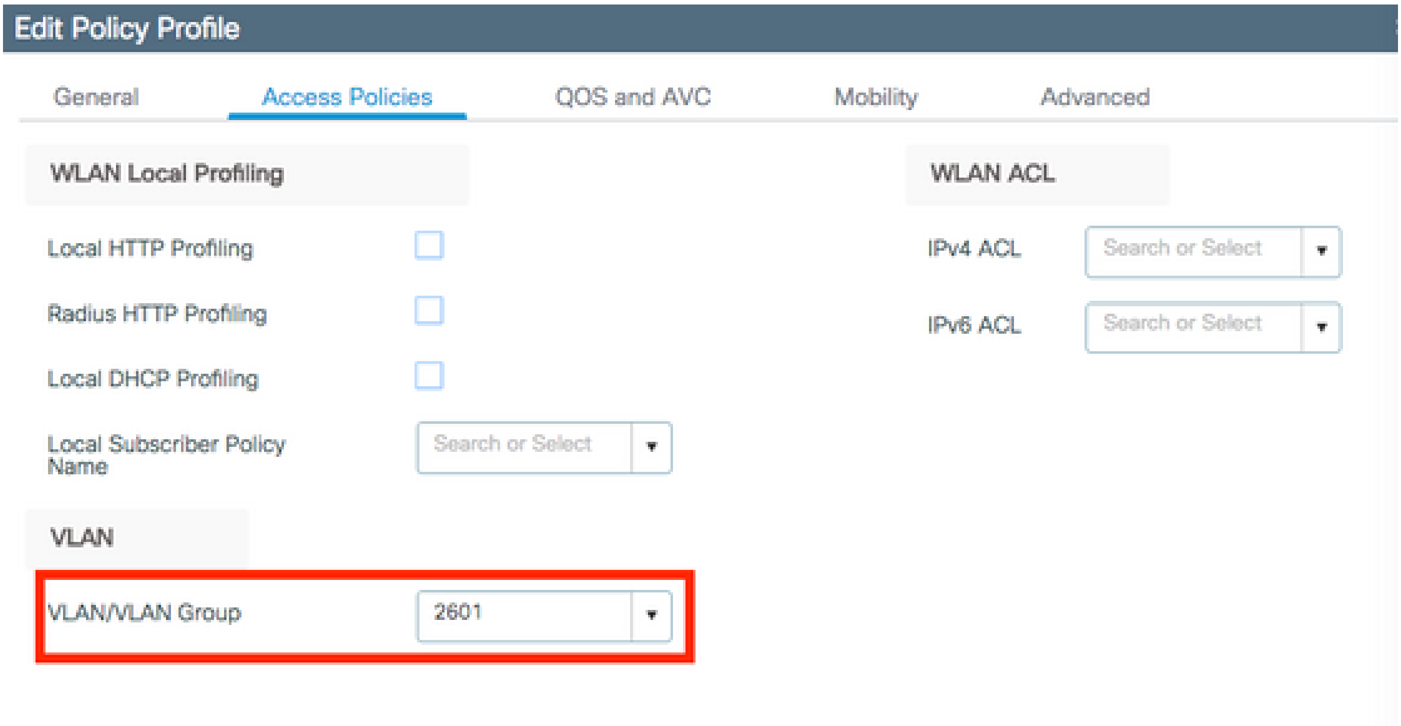
VLAN/VLAN Group: VLAN2602

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

或



WLAN Local Profiling

Local HTTP Profiling □

Radius HTTP Profiling □

Local DHCP Profiling □

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: 2601

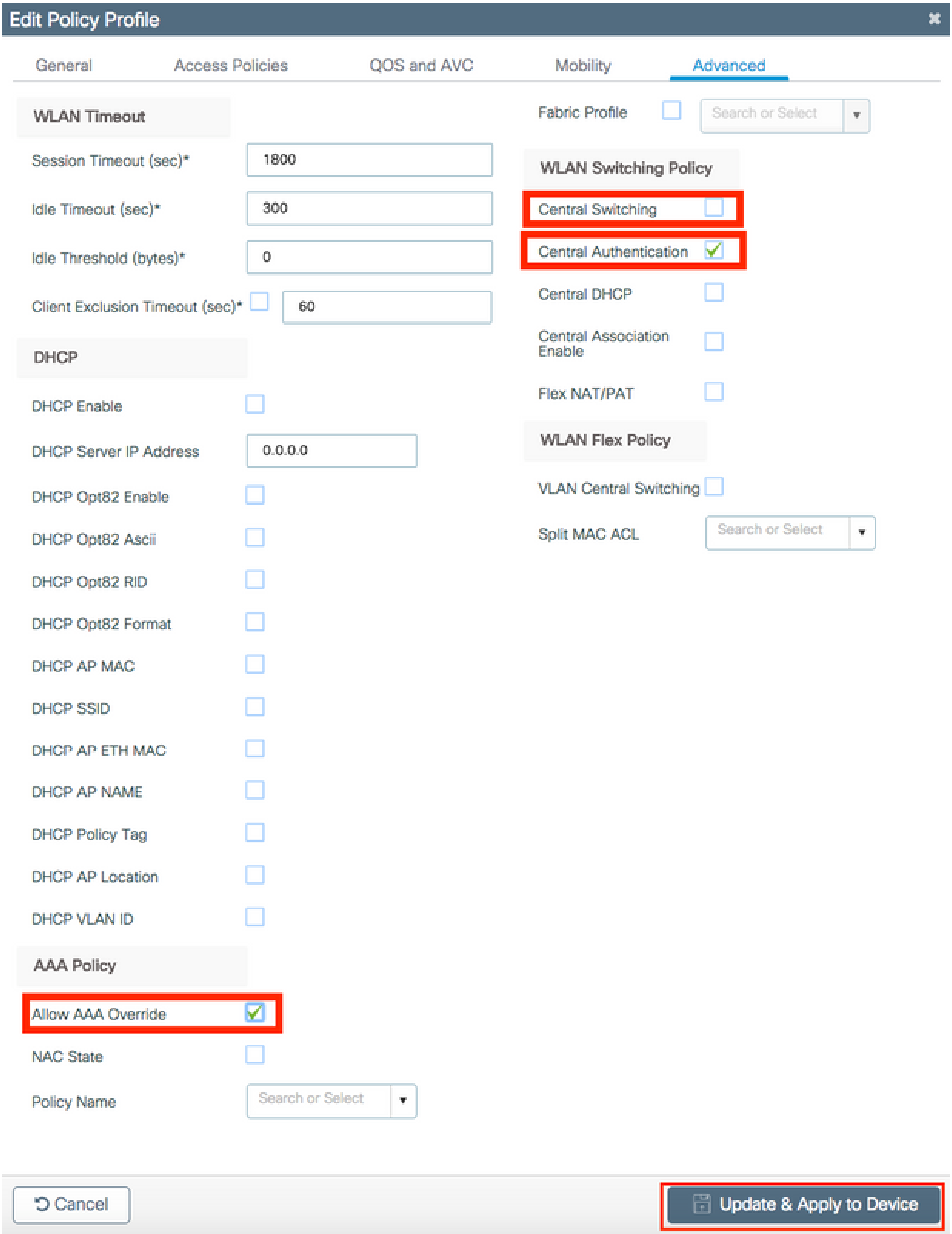
WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

步驟4.導覽至**Advanced** 索引標籤，並啟用**Central Authentication Enable**和**Allow AAA** Overrideoptions。**必須禁**用集中交換。

如果希望9800 WLC集中執行驗證程式，必須啟用集中驗證。如果您希望FlexConnect AP對無線客戶端進行身份驗證，請將其禁用。



WLAN Timeout

Session Timeout (sec)* 1800

Idle Timeout (sec)* 300

Idle Threshold (bytes)* 0

Client Exclusion Timeout (sec)* □ 60

DHCP

DHCP Enable □

DHCP Server IP Address 0.0.0.0

DHCP Opt82 Enable □

DHCP Opt82 Ascii □

DHCP Opt82 RID □

DHCP Opt82 Format □

DHCP AP MAC □

DHCP SSID □

DHCP AP ETH MAC □

DHCP AP NAME □

DHCP Policy Tag □

DHCP AP Location □

DHCP VLAN ID □

AAA Policy

Allow AAA Override ☑

NAC State □

Policy Name Search or Select

Fabric Profile □ Search or Select

WLAN Switching Policy

Central Switching □

Central Authentication ☑

Central DHCP □

Central Association Enable □

Flex NAT/PAT □

WLAN Flex Policy

VLAN Central Switching □

Split MAC ACL Search or Select

CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
# no shutdown
```

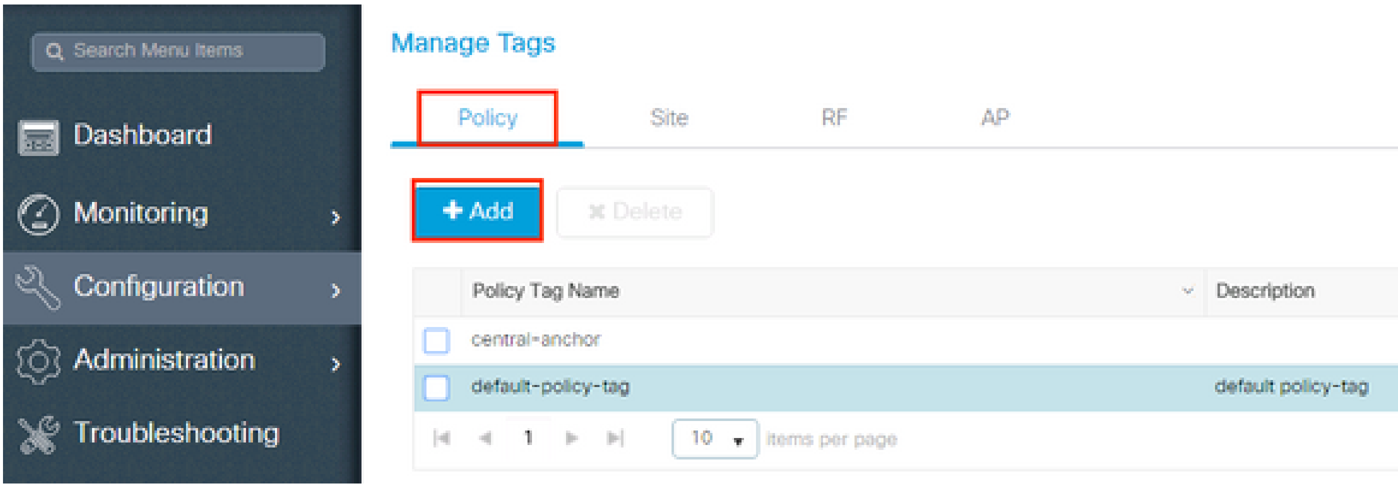
原則標籤組態

策略標籤用於將SSID與策略配置檔案連結。您可以建立新的原則標籤，或使用 default-policy-tag。

> **注意**:default-policy-tag會自動將WLAN ID介於1到16之間的所有SSID對映到default-policy-profile。無法修改或刪除它。如果您的WLAN的ID為17或更高，則不能使用default-policy-tag。

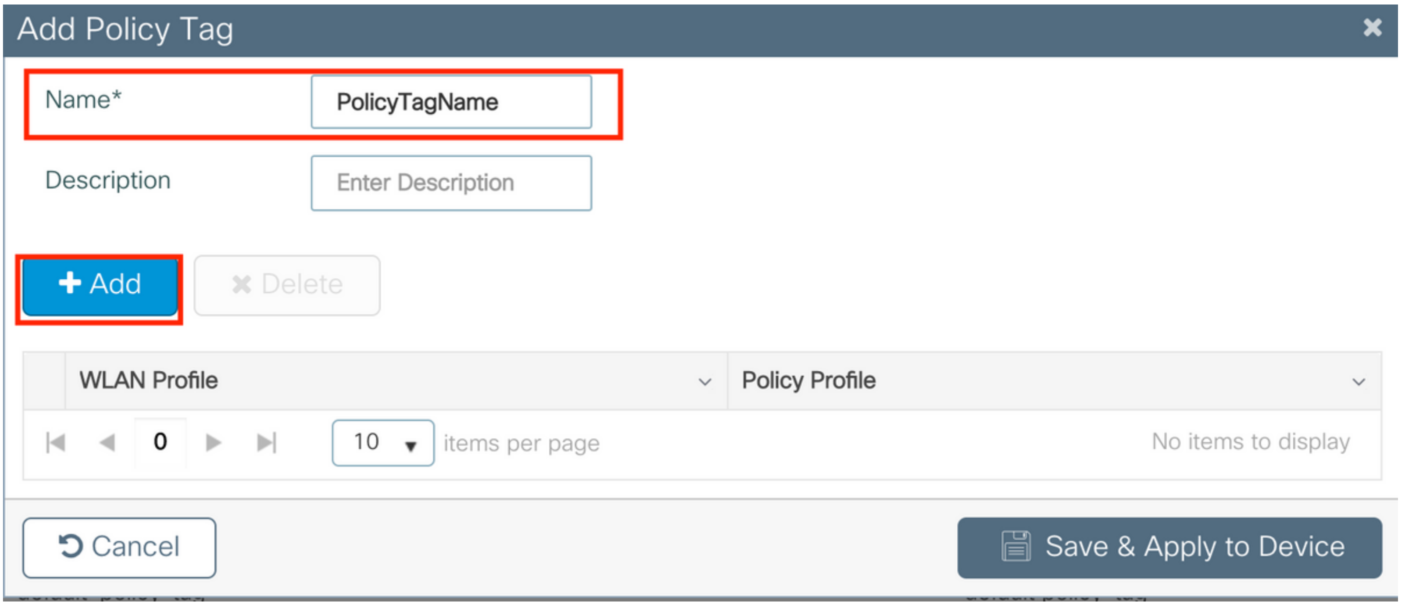
GUI:

如果需要，請導航到**Configuration > Tags & Profiles > Tags > Policy**，然後新增一個新檔案。



	Policy Tag Name	Description
□	central-anchor	
□	default-policy-tag	default policy-tag

將 WLAN 設定檔連結至想要的原則設定檔。

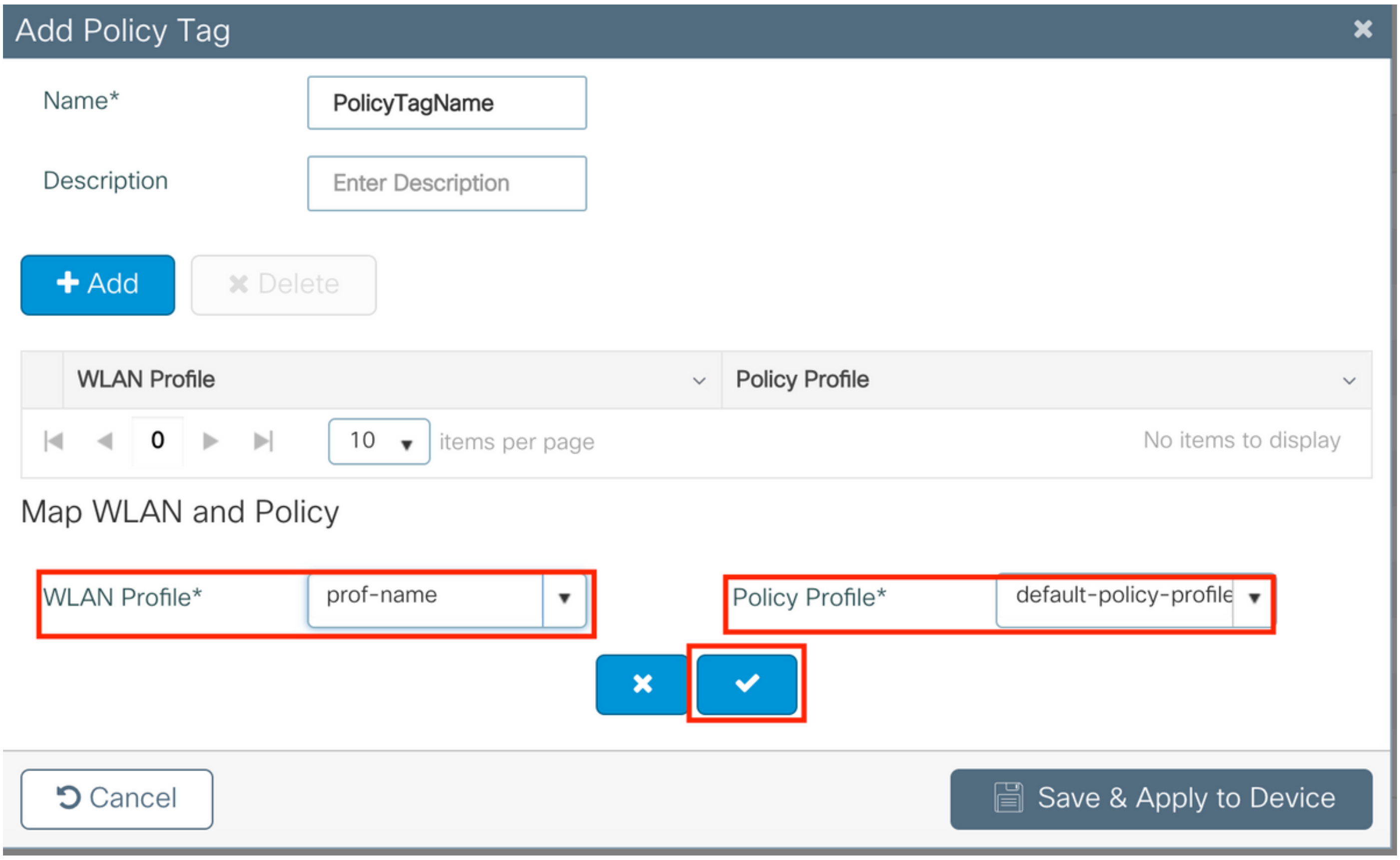


Name* PolicyTagName

Description Enter Description

WLAN Profile	Policy Profile

No items to display



Add Policy Tag

Name* PolicyTagName

Description Enter Description

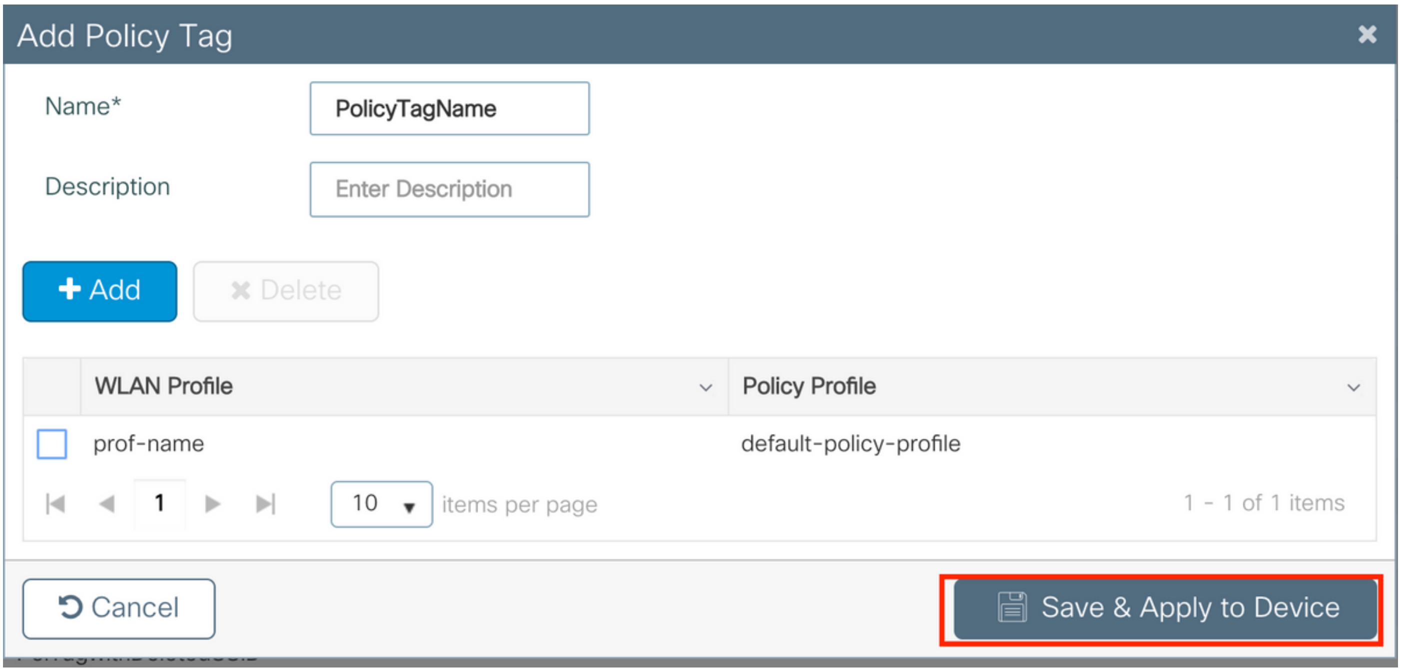
WLAN Profile	Policy Profile

No items to display

Map WLAN and Policy

WLAN Profile* prof-name

Policy Profile* default-policy-profile



Add Policy Tag

Name* PolicyTagName

Description Enter Description

	WLAN Profile	Policy Profile
□	prof-name	default-policy-profile

1 - 1 of 1 items

CLI:

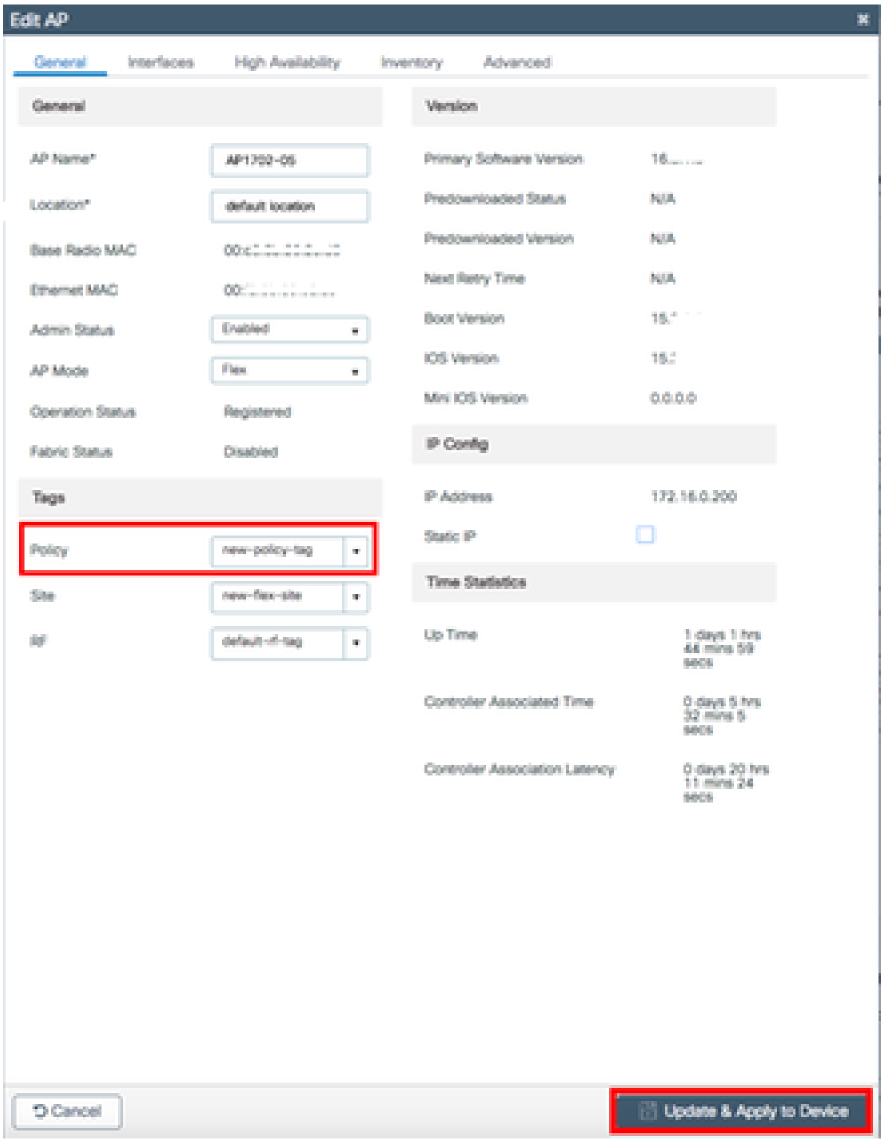
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

策略標籤分配

為AP分配策略標籤

GUI

要將標籤分配給一個AP，請導航到**Configuration > Wireless > Access Points > AP Name > General Tags**，進行所需的分配，然後點選**Update & Apply to Device**。



Edit AP

General

AP Name*	AP1702-05
Location*	default location
Base Radio MAC	00:c[redacted]
Ethernet MAC	00:[redacted]
Admin Status	Enabled
AP Mode	Flex
Operation Status	Registered
Fabric Status	Disabled

Tags

Policy	new-policy-tag
Site	new-flex-site
RF	default-rf-tag

Version

Primary Software Version	16.[redacted]
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	15.[redacted]
IOS Version	15.[redacted]
Mini IOS Version	0.0.0.0

IP Config

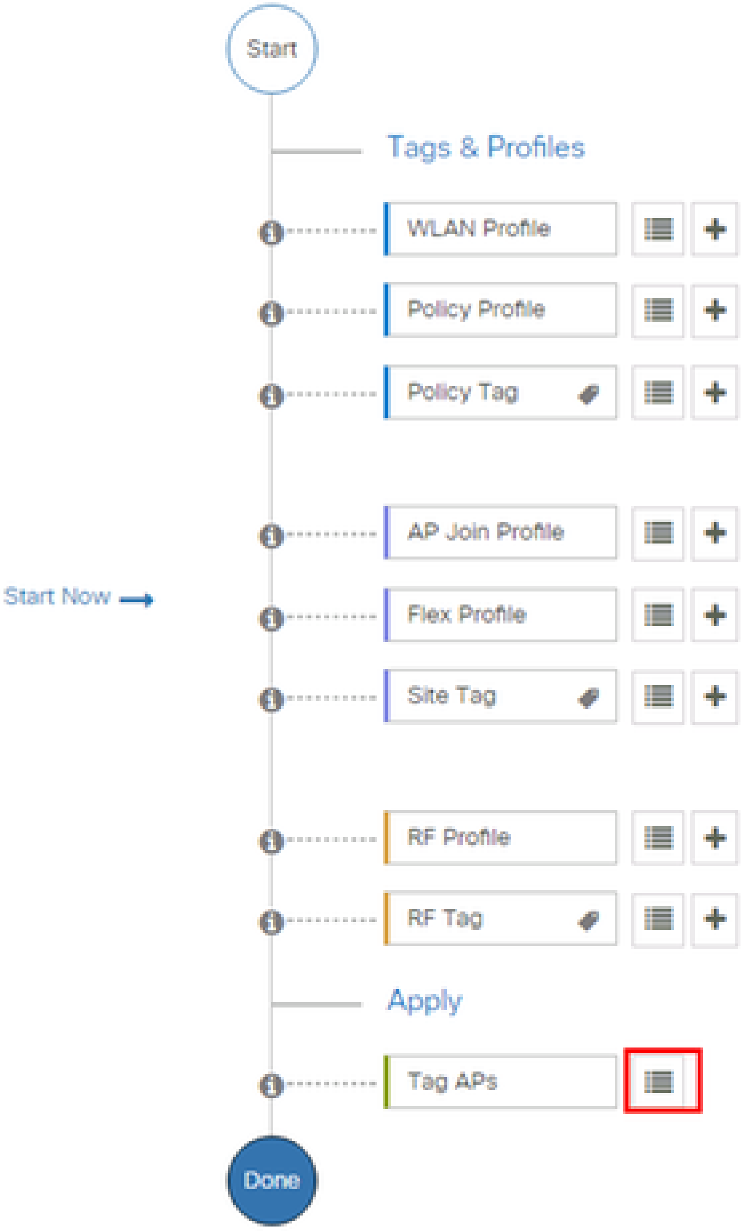
IP Address	172.16.0.200
Static IP	□

Time Statistics

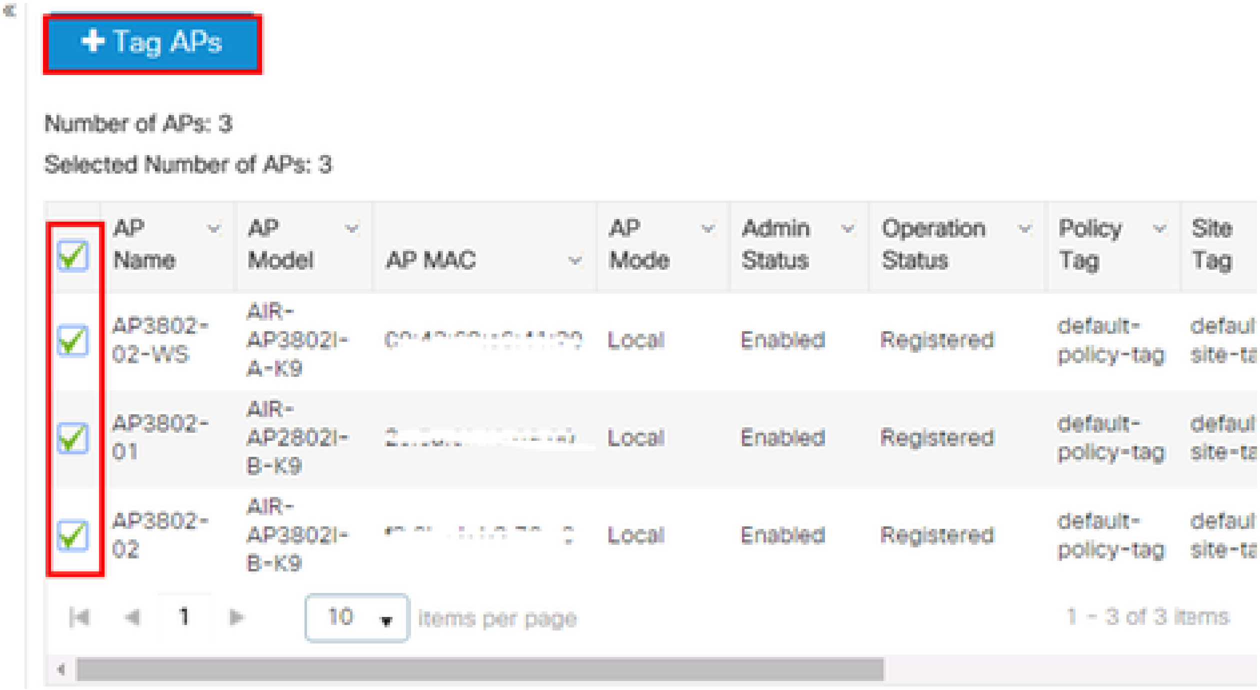
Up Time	1 days 1 hrs 44 mins 59 secs
Controller Associated Time	0 days 5 hrs 32 mins 5 secs
Controller Association Latency	0 days 20 hrs 11 mins 24 secs

注意:請注意，變更AP上的原則標籤後，AP會失去與9800 WLC的關聯，並在約1分鐘內重新加入。

要將相同的策略標籤分配給多個AP，請導航至**Configuration > Wireless > Wireless Setup > Start Now > Apply**。



選擇要為其分配標籤的AP，然後按一下**+ Tag AP**

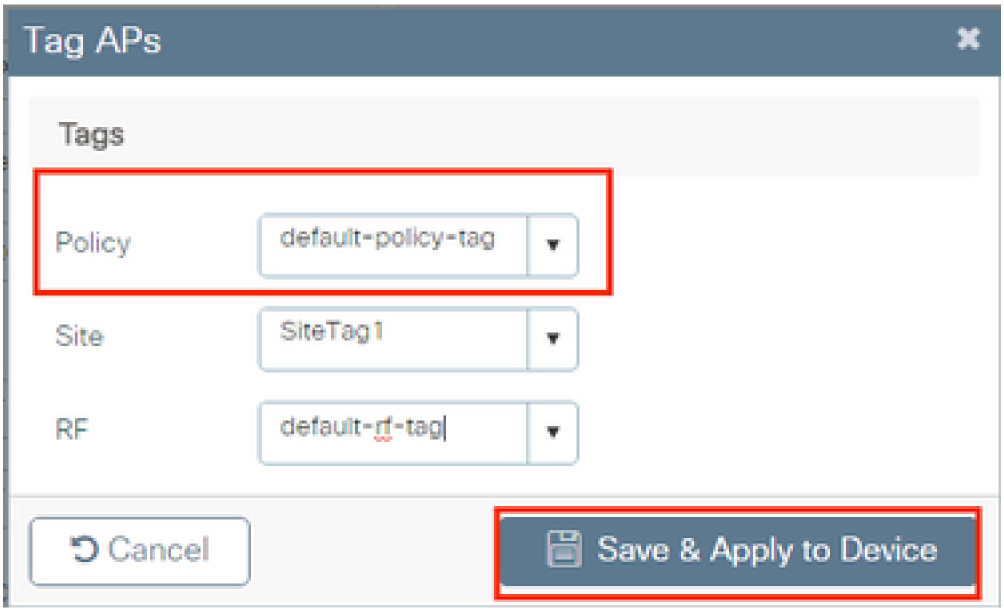


Number of APs: 3

Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag
☑	AP3802-02-WS	AIR-AP3802I-A-K9	[redacted]	Local	Enabled	Registered	default-policy-tag	defaul site-ta
☑	AP3802-01	AIR-AP2802I-B-K9	[redacted]	Local	Enabled	Registered	default-policy-tag	defaul site-ta
☑	AP3802-02	AIR-AP3802I-B-K9	[redacted]	Local	Enabled	Registered	default-policy-tag	defaul site-ta

選擇完成的標籤，然後按一下**儲存並應用到裝置**



Policy: default-policy-tag

Site: SiteTag1

RF: default-rf-tag

CLI

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

ISE 組態

對於ISE v1.2配置，請檢查此連結：

ISE 組態

驗證

您可以使用這些命令驗證當前配置

```
# 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 提供永不間斷的追蹤功能。如此可確保所有與錯誤相關的用戶端連線、警告及通知層級訊息皆持續受到記錄，且您可在事件或故障情況發生後檢視相關記錄。

> **附註**：根據正在生成的日誌量，您可以將時間返回幾小時到幾天。

若要檢視 9800 WLC 依預設收集的追蹤，您可透過 SSH/Telnet 連接至 9800 WLC，並遵循以下步驟執行（請確認您將作業階段記錄至文字檔）。

步驟1.檢查控制器的當前時間，以便您可以跟蹤問題發生時的記錄時間。

```
# show clock
```

步驟 2. 從控制器的緩衝區或系統組態指定的外部系統日誌來收集系統日誌。如此可快速檢視系統健全狀況和錯誤（如有）。

```
# show logging
```

步驟 3. 確認所有偵錯條件是否已啟用。

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

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

> **附註**：如果您看見任何列出的條件，這表示追蹤已記錄至所有遭遇啟用條件（MAC 位址、IP 位址等）之程序的偵錯層級。 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. 假設在步驟 3 中，測試之下的 MAC 位址未列為條件，請針對特定 MAC 位址收集永不間斷

之通知層級的追蹤。

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

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。

```
# 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式追蹤

如果全天候運作的追蹤未提供充足資訊，使您在調查之下無法判斷問題的觸發原因，則您可啟用條件式偵錯並擷取無線電主動式 (RA) 追蹤，如此可將偵錯層級追蹤提供給所有與指定條件（在此案例中為用戶端 MAC 位址）互動的所有程序。 若要啟動條件式偵錯，請遵循以下步驟執行。

步驟 5. 確認未啟用任何偵錯條件。

```
# clear platform condition all
```

步驟 6. 針對您想要監控的無線用戶端 MAC 位址啟用偵錯條件。

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。

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

> **注意**:為了同時監控多個客戶端，請對每個mac地址運行debug wireless mac <aaaa.bbb.cccc>命令。

> **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. 重現您想要監控的問題或行為。

步驟 8. 如果問題在預設或設定的監控時間結束之前重現，請停止偵錯。

```
# 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地址活動的檔案。您可以將ra跟蹤.log複製到外部伺服器，也可以直接在螢幕上顯示輸出。

檢查RA跟蹤檔案的名稱

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

將檔案複製到外部伺服器：

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

顯示內容：

```
# 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，請收集內部記錄，該記錄為較詳細的偵錯層級記錄檢視。您無需再次調試客戶端，因為我們只是進一步詳細檢視已收集並內部儲存的調試日誌。

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

> **附註**：此命令輸出會傳回所有程序之所有記錄層級的追蹤，且資訊相當大量。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：

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

顯示內容：

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

步驟 11. 移除偵錯條件。

```
# clear platform condition all
```

> **附註**：疑難排解作業階段後，請務必移除偵錯條件。