在FlexConnect模式下配置本地身份驗證

目錄

簡介

- 背景資訊
  - FlexConnect概述和要求
  - 操作模式
  - 快速安全漫遊
  - FlexConnect高擴展模式
  - Wi-Fi 7 FlexConnect支援
  - FlexConnect恢復能力方案

必要條件

- 需求
- 採用元件

設定

- 網路圖表
- 配置AAA伺服器
- 在遠端站點上配置FlexConnect模式
- 使用外部RADIUS伺服器配置帶有本地身份驗證的802.1x WLAN
- 配置ISE
- 使用本地身份驗證配置PSK WLAN

驗證

疑難排解

- 獨立方案

相關資訊

簡介

本檔案將說明FlexConnect本機驗證如何運作，以及如何使用Cisco Catalyst 9800系列無線控制器(WLC)對其進行設定

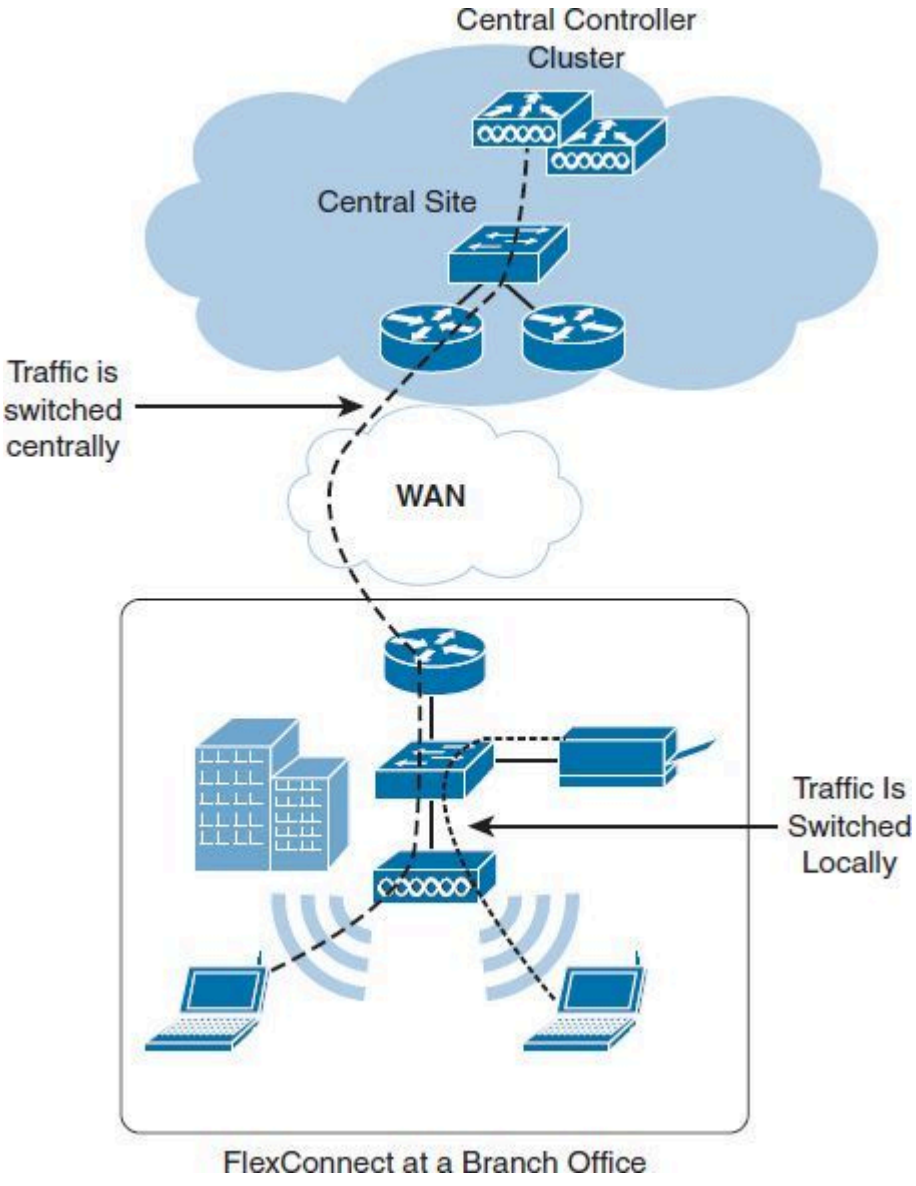
背景資訊

FlexConnect概述和要求

FlexConnect使遠端或分支機構的接入點(AP)能夠連線到集中式控制器，同時允許對無線流量進行本地處理。與使用CAPWAP（無線接入點的控制和調配）將所有無線流量通過隧道傳輸到控制器的傳統集中式無線部署不同，FlexConnect允許流量在本地進行交換，並由分支AP直接處理。此本地

交換為AP提供一定程度的自主權，使安全、漫遊和服務品質(QoS)等關鍵服務能夠獨立於控制器運行。

雖然FlexConnect主要是為本地流量交換而設計的，但它也提供了根據需要集中交換特定SSID（服務集識別符號）的靈活性。例如，如果某些流量必須通過中央防火牆，則這些SSID可以通過CAPWAP發回控制器，以進行集中交換。這種雙重功能允許單個FlexConnect AP同時支援本地和集中交換的WLAN（無線區域網）。



在分支機構部署的FlexConnect AP本地交換一個SSID，而另一個集中交換

操作模式

FlexConnect AP以兩種模式運行：connected mode和standalone mode。

- 在連線模式下，AP通過CAPWAP控制通道保持與控制器的活動連線。
- 獨立模式是回退狀態，當AP失去與控制器的連線時會發生此狀態。

在正常情況下，FlexConnect AP在連線模式下工作，控制器管理集中身份驗證、客戶端分析和無線電資源管理(RRM)等關鍵服務。 雖然預計AP大多數時間都保持此模式，但是如果與控制器的通訊丟失，它會自動切換到獨立模式。在獨立模式下，AP繼續運行，在本地交換流量並允許客戶端保持連線。AP獨立驗證客戶端，而不向中央控制器轉發驗證請求。但是，某些與控制器相關的服務（如RRM和集中客戶端身份驗證）暫時不可用。

例如，如果WAN（廣域網）中斷中斷AP與控制器之間的連線，但Internet訪問仍然處於活動狀態，則AP將轉換到獨立模式，繼續處理本地交換的流量而不中斷。現有客戶端保持連線，但需要集中身份驗證的新客戶端無法加入網路，除非配置了本地身份驗證。可以將FlexConnect AP設定為在WAN故障期間執行本地身份驗證，確保即使在控制器不可訪問時也能繼續提供服務。

在獨立模式下，AP無法使用這些功能：

- 客戶端Web驗證
- 訪客身份驗證（門戶重定向）
- 任何集中交換SSID
- RRM
- IPv6第3層移動性
- 本機分析
- 策略分類
- 服務探索閘道
- 配置更新

有關獨立模式（本地身份驗證）支援的功能和WLAN配置的完整清單，請參閱功能表：思科無線接入點的功能表

常見的FlexConnect故障情況包括WAN完全丟失或顯著降低，這會中斷CAPWAP控制通道。當AP由於WAN問題而失去與控制器的連線時，它會立即切換到獨立模式。

WAN故障期間，主要目標是儘快恢復與控制器的通訊以恢復全部功能。

當FlexConnect AP因WAN故障而進入獨立模式時，活動客戶端保持連線並可在FlexConnect域/站點標籤內的AP之間無縫漫遊，但不同FlexConnect站點標籤之間的漫遊可能需要完全重新身份驗證。

但是，嘗試加入本地交換WLAN的新客戶端無法進行身份驗證，因為無法訪問中心位置的AAA伺服器（身份驗證、授權和記帳伺服器）。

快速安全漫遊

EAP（可擴展身份驗證協定）身份驗證與PSK（預共用金鑰）身份驗證相比，由於與AAA伺服器交換EAP幀，引入了更高的延遲。但是，藉助快速安全漫遊，客戶端僅在其與網路的初始關聯期間接受完整的802.1X/EAP身份驗證。在隨後到相鄰AP的漫遊中，EAP交換被繞過，僅留下四路握手，這要快得多，因為它不涉及AAA伺服器。下表概述在本機模式和FlexConnect部署中9800 WLC支援的各種快速安全漫遊方法。

功能	本地模式	FlexConnect(連線模式；集中身份驗證)	FlexConnect（連線模式 — 本地身份驗證）	FlexConnect(獨立)
粘滯金鑰快取(SKC)	不支援	不支援	不支援	不支援
機會式金鑰快取(OKC)	支援	支援	支援	支援（直到客戶端會話過期）
思科集中式金鑰管理(CCKM)	支援	支援	支援	不支援
FT-802.11r/自適應11r（快速過渡）（空中）	支援	支援	支援	支援（直到客戶端會話過期）
FT-802.11r/自適應11r（快速過渡）（通過DS）	支援	支援	不支援	不支援

在獨立模式下，快速漫遊取決於快取的金鑰材料是否仍然有效。當快取的PMK（成對主金鑰）/會話到期時，AP無法獲取新的控制器派生的金鑰資訊，直到恢復控制器連線。

FlexConnect高擴展模式

從Cisco IOS XE 17.8.1開始，靈活站點站點容量已擴展到可容納300個AP和3000個802.1x客戶端。

PMK傳播允許同一FlexConnect站點中的AP共用PMK資訊，減少漫遊期間對完整EAP交換的需求。預設情況下未啟用PMK傳播。

使用以下命令驗證PMK傳播並啟用PMK:

- show wireless stats pmk-propagation
- pmk傳播

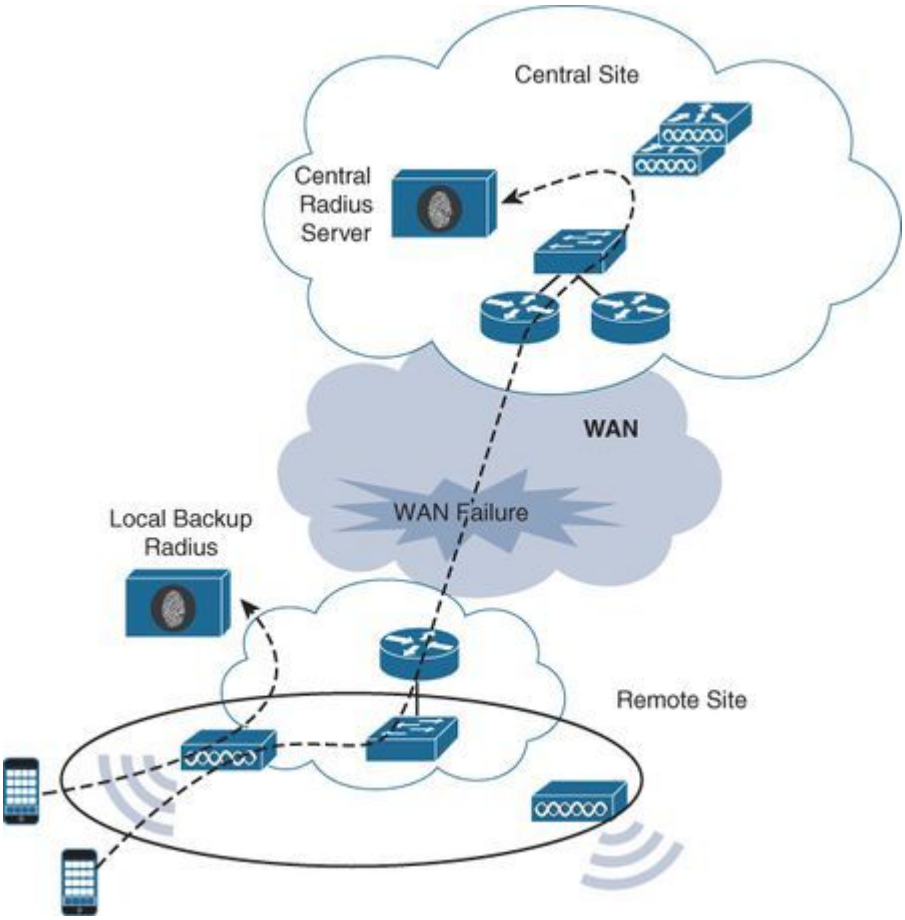
Wi-Fi 7 FlexConnect支援

下表彙總了CW917x Wi-Fi 7 AP系列支援的FlexConnect功能。

功能	支援
本地交換	支援
中央交換	支援
WLAN-VLAN對應	支援
使用外部RADIUS的本地驗證	支援
WPA3-Enterprise	支援
FT-802.11r快速漫遊	支援
多重連結操作(MLO)	支援
使用內部RADIUS的本地驗證	不支援
WPA3-Enterprise-192	不支援

FlexConnect恢復能力方案

1. 在N+1恢復設定中，多個活動控制器共用一個通用備份控制器，在任何活動控制器出現故障時該控制器將接管該備用控制器。當主控制器離線時，FlexConnect接入點會立即切換到獨立模式，並開始搜尋備份控制器。在此斷開連線期間，集中交換客戶端與AP斷開。一旦AP找到並與備份控制器同步，需要訪問集中交換SSID的客戶端就會重新連線。同時，本地交換客戶端仍然不受影響，並在不注意到服務中斷的情況下繼續運行。
2. 在遠端位置提供可由FlexConnect組訪問的備份AAA伺服器。啟用本地身份驗證後，此備份RADIUS伺服器僅在AP進入獨立模式時使用 — 當AP處於連線模式時，該伺服器保持非活動狀態。當FlexConnect AP使用本地備份AAA伺服器進行身份驗證時，身份驗證金鑰會分發到FlexConnect組中的所有AP，就像集中式AAA伺服器一樣。這可確保即使使用備份RADIUS伺服器，新客戶端仍可以在AP之間無縫漫遊，而無需重新進行身份驗證。
3. Feature Matrix for Cisco Wireless Access Points中允許本地身份驗證的任何方法。



當中央AAA伺服器因WAN故障而變得不可用時，客戶端根據本地備份AAA伺服器進行身份驗證

必要條件

需求

本文件沒有特定需求。

採用元件

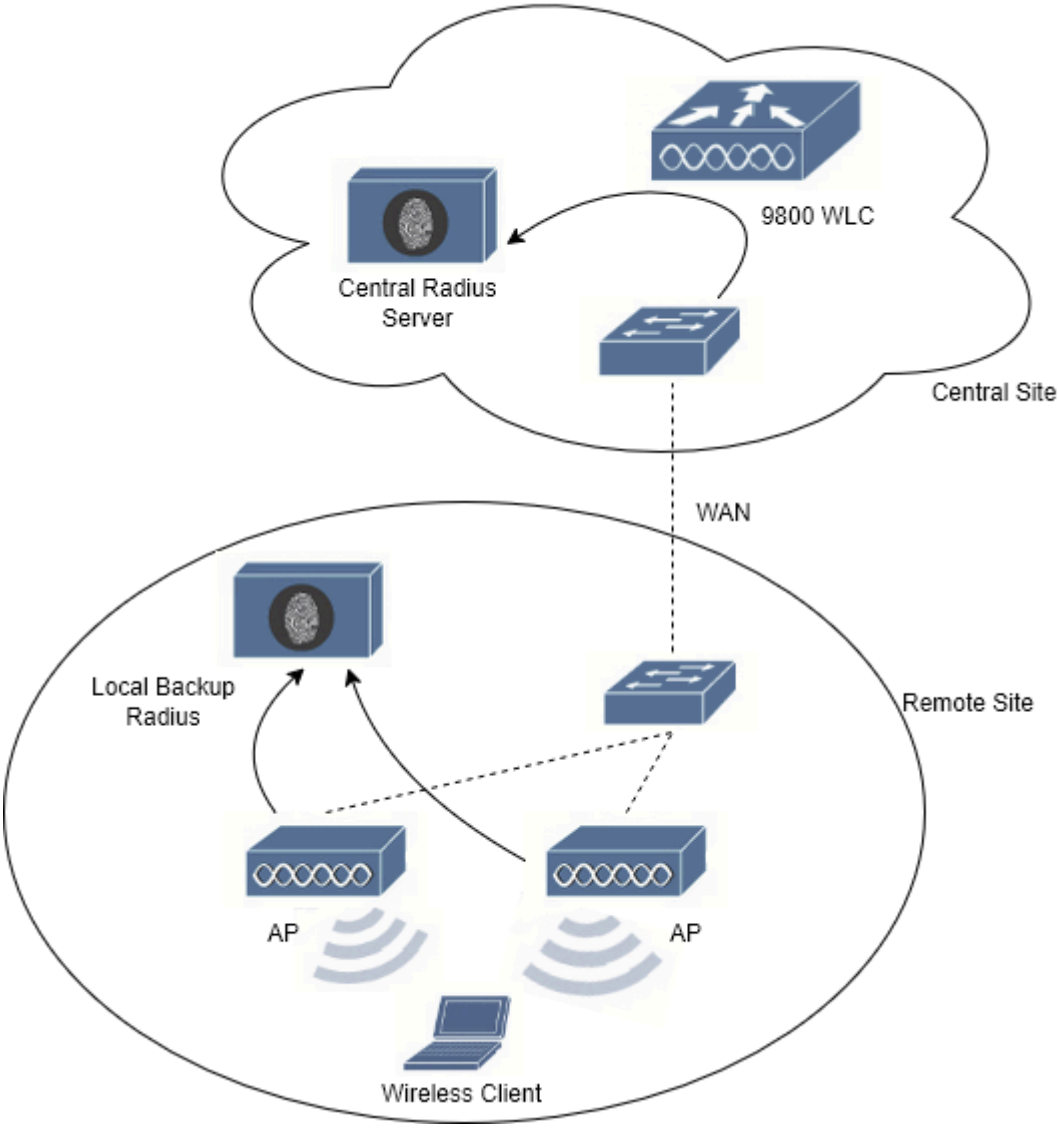
本文中的資訊係根據以下軟體和硬體版本：

- 適用於雲端的Catalyst C9800-CL無線控制器(含Cisco IOS® XE都柏林17.18.3)
- Catalyst CW9164I-ROW接入點v17.18.3.18
- Aironet® AIR-AP2802I-E-K9接入點v17.18.3.18
- 2個身份服務引擎v3.2.0.542

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



網路圖表

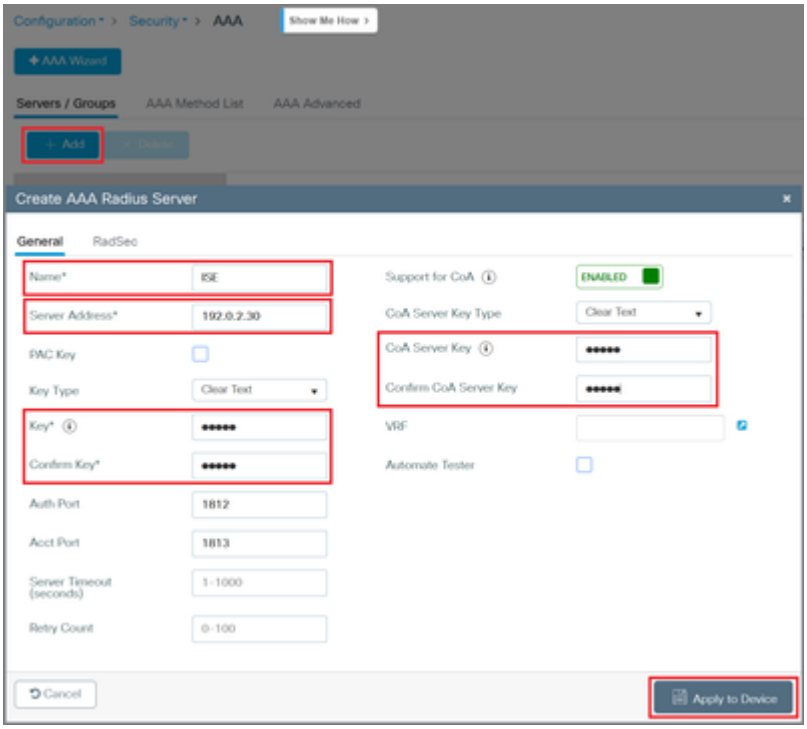
配置AAA伺服器

步驟1。若要設定802.1x WLAN，您需要在9800 WLC上建立AAA伺服器群組。

為每個站點建立一個AAA伺服器 — 一個在中心站點，另一個在遠端站點。

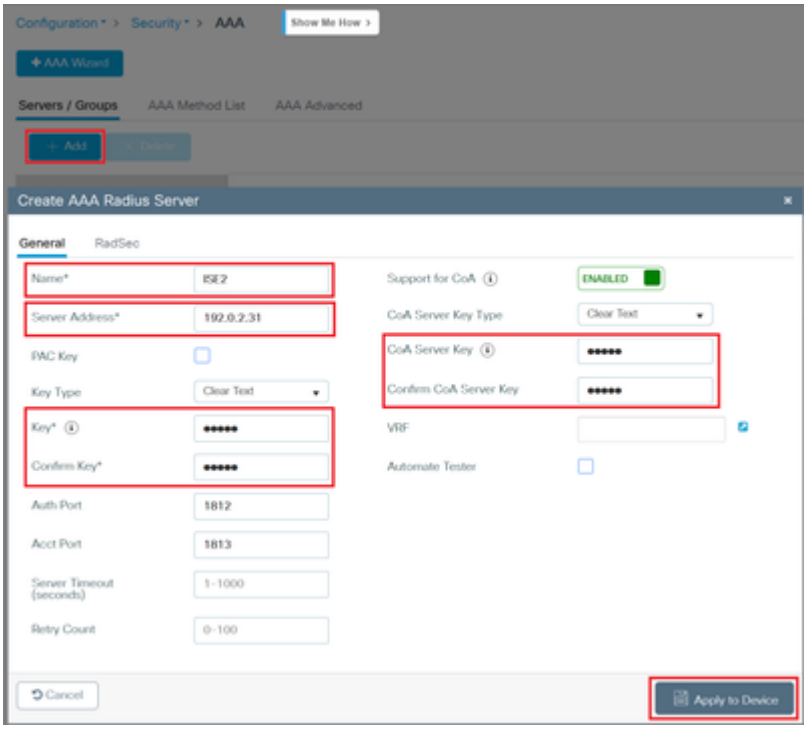
導航到Configuration > Security > AAA > Server/Groups > Servers，然後選擇+Add。為伺服器指定

名稱、其IP地址、金鑰（和確認金鑰）、啟用CoA（授權更改）支援，並輸入CoA伺服器金鑰（並確認CoA伺服器金鑰）。 金鑰必須相同。



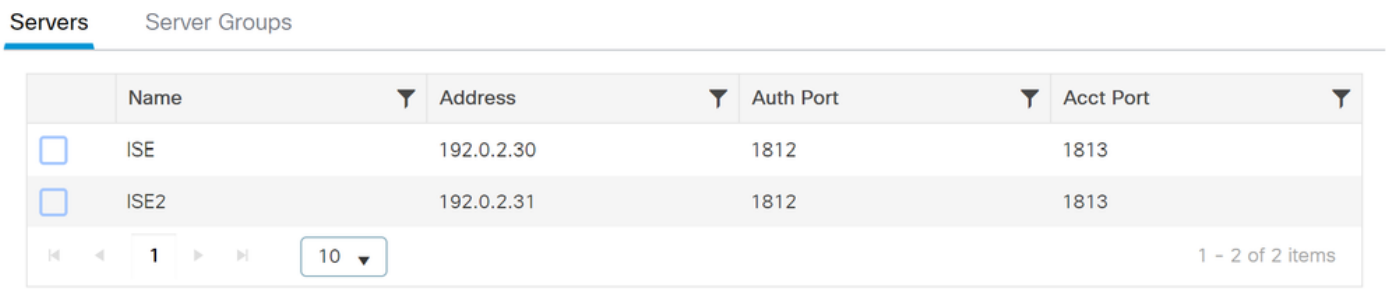
按一下Apply to Device。

步驟2.建立其他AAA伺服器：

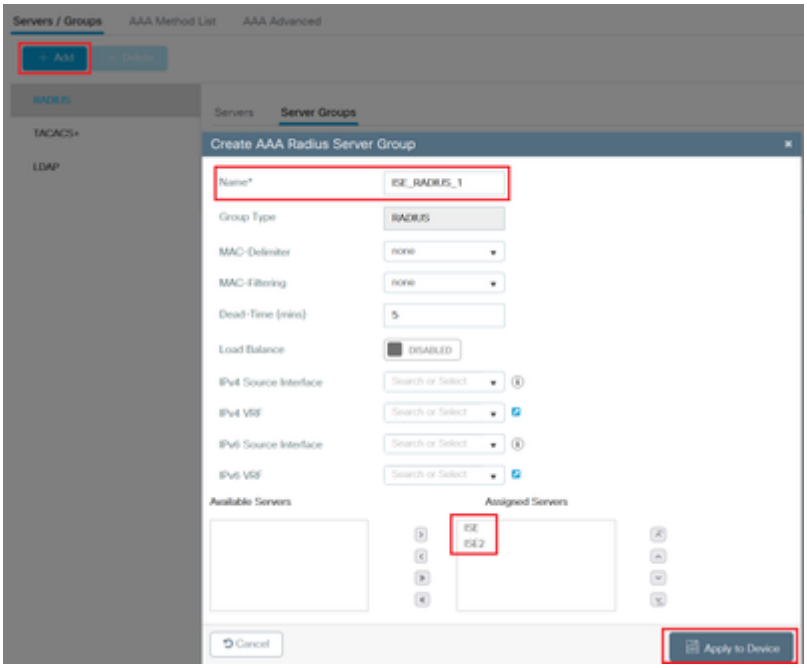


按一下Apply to Device。

現在您會看到您的AAA伺服器已配置：

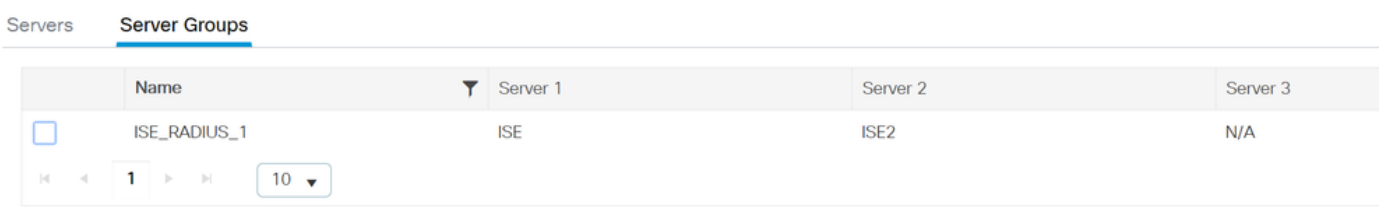


步驟3.導航到Configuration > Security > AAA > Server/Groups > Server Groups，然後選擇+Add。為組伺服器指定一個名稱，然後將先前建立的AAA伺服器選擇到Assigned Servers列：



按一下Apply to Device。

然後您會看到已配置的AAA伺服器組：



CLI:

```
aaa new-model
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

在遠端站點上配置FlexConnect模式

步驟1.第一步是在遠端站點上配置FlexConnect。

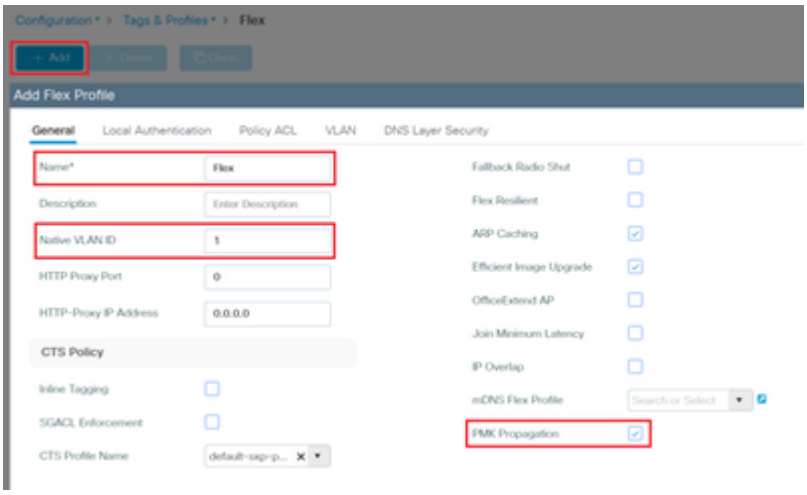
使用本指南將AP模式更改為Flex：瞭解Catalyst 9800無線控制器上的FlexConnect。

本指南/實驗室中的AP使用相同的Flex配置檔案。

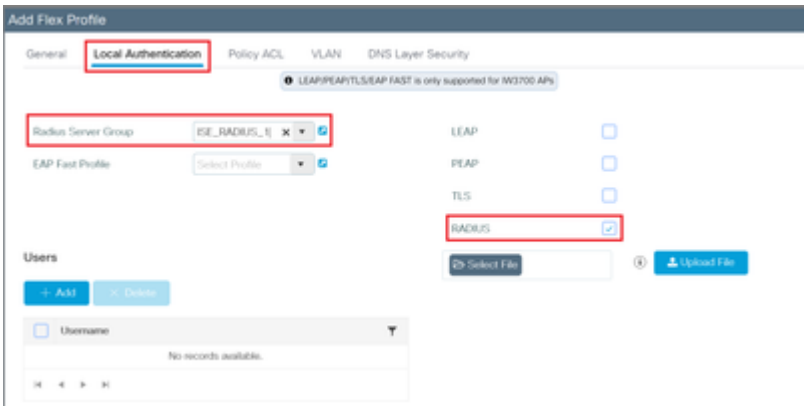
步驟2.導覽至Configuration > Tags & Profiles > Flex。

使用+Add建立一個新的Flex配置檔名稱。在General頁籤上，為配置檔案指定名稱，輸入本徵VLAN（虛擬區域網）ID，然後啟用PMK傳播。

啟用PMK傳播，通過在單個站點內的AP之間共用PMK資訊，促進無縫無線客戶端漫遊。

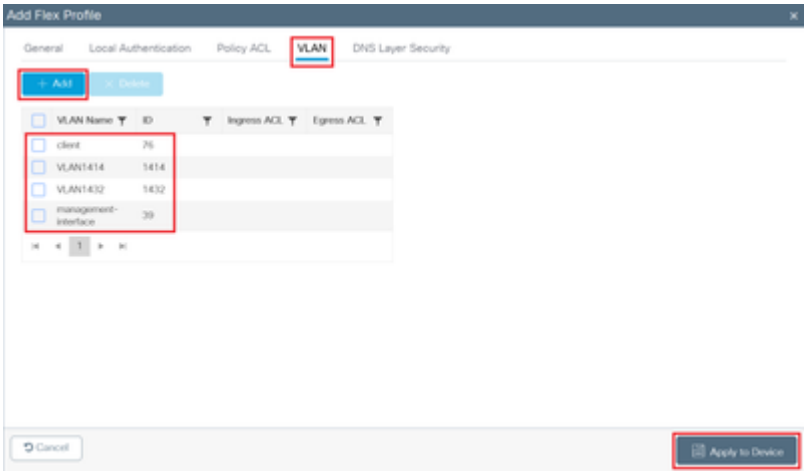


步驟3.對於802.1x WLAN，在Local Authentication頁籤上選擇Radius伺服器組並啟用RADIUS:



提示：對於PSK WLAN，您無需在此頁籤中新增任何內容。

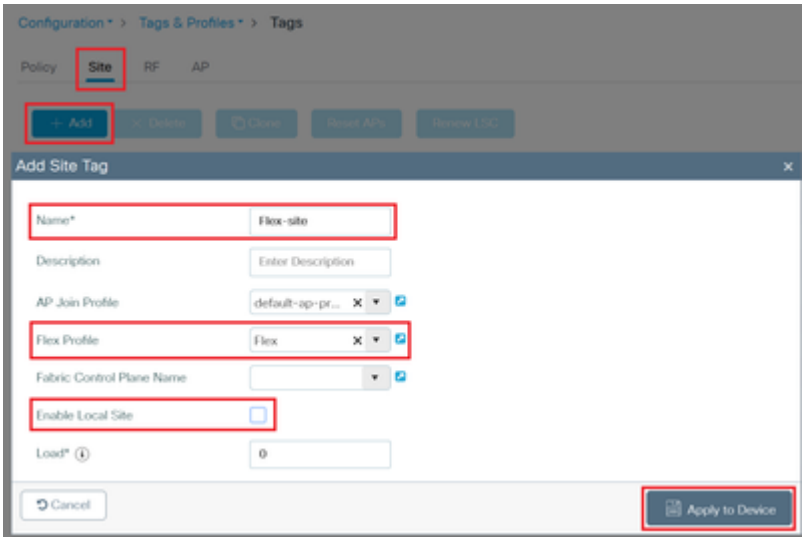
步驟4.在VLAN索引標籤上新增使用者端、AP和RADIUS伺服器使用的所有VLAN。確保將每個VLAN名稱與正確的VLAN ID正確對應：



最後點選Update & Apply to Device。

步驟5.導覽至Configuration > Tags & Profiles > Tags > Site，然後選擇+Add。

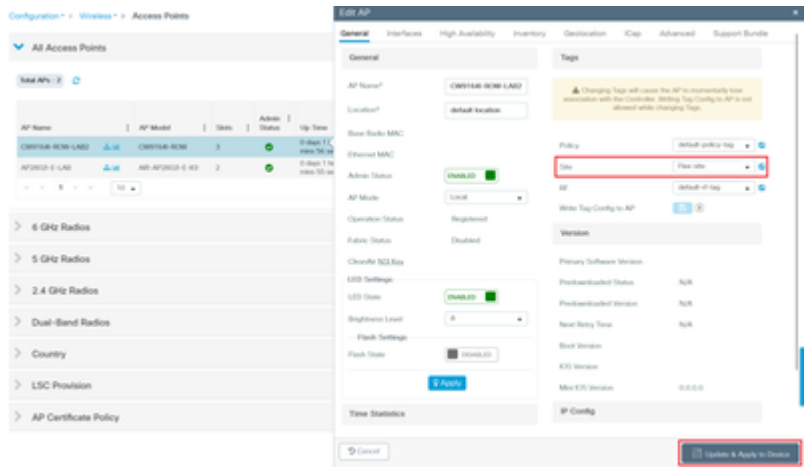
使用之前建立的Flex Profile建立站點標籤。為其指定一個名稱，選擇正確的Flex配置檔案，然後禁用啟用本地站點。確保AP加入配置檔案是正確的。



按一下Apply to Device。

步驟6.導覽至Configuration > Wireless > Access Points。

在General > Tags上選擇您的AP，將Site Tag更改為先前配置的標籤：



按一下Update & Apply to Device。

AP與WLC斷開連線並使用Flex AP模式重新連線。

在同一頁上，當AP重新加入時，您可以檢查AP模式列上的AP模式。

如果選擇AP，則會顯示新的站點標籤：



CLI:

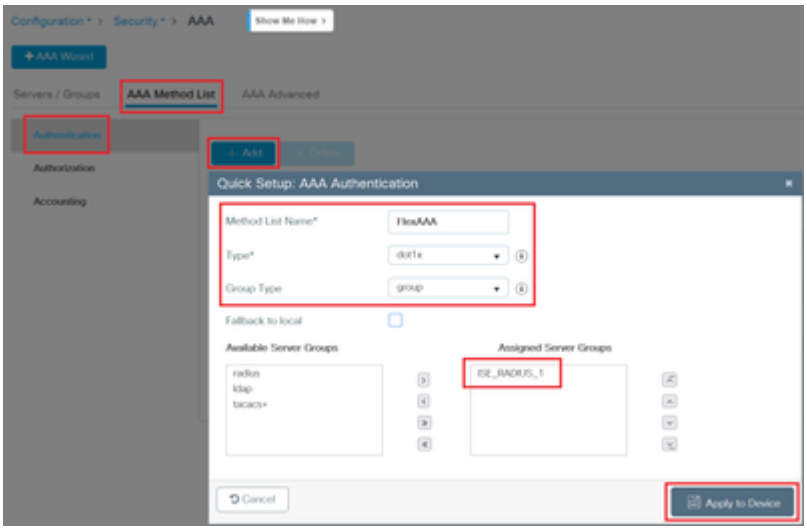
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

使用外部RADIUS伺服器配置使用本地身份驗證的802.1x WLAN

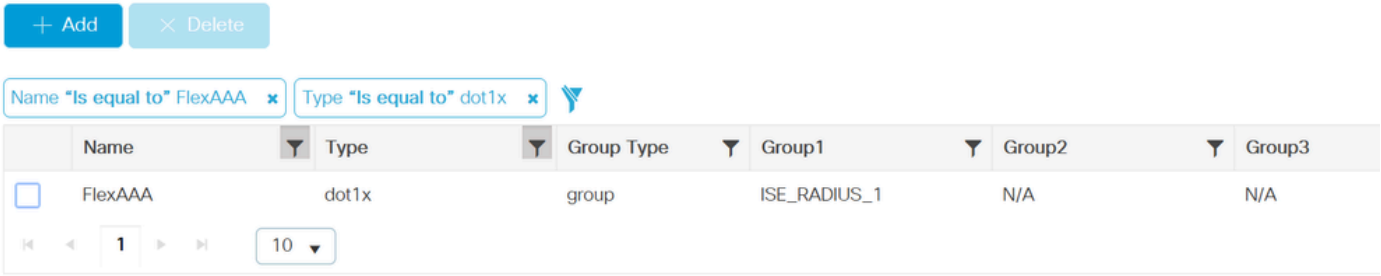
步驟1.建立身份驗證方法清單。

在AAA Method List > Authentication頁籤上導航到Configuration > Security > AAA。

選擇+Add，為方法清單名稱指定名稱，選擇dot1x作為型別，選擇group作為組型別，並在Assigned Server Groups列上分配AAA伺服器組：



現在可以看到建立的AAA方法清單：



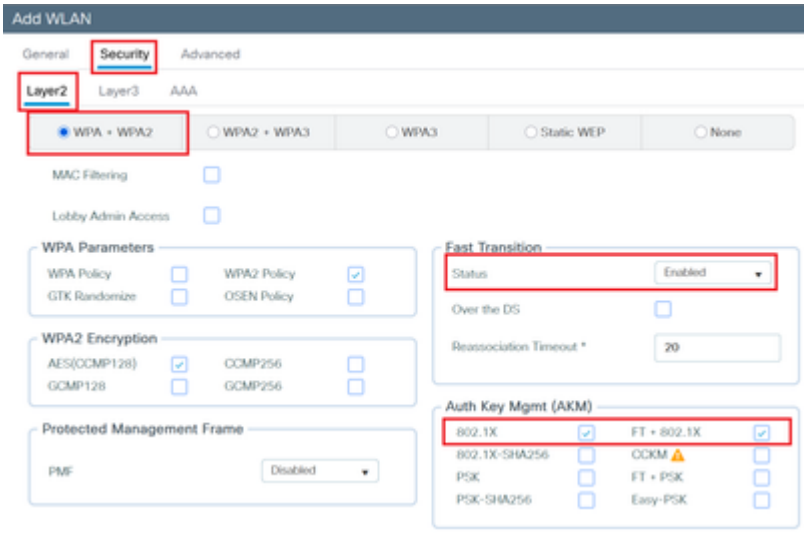
步驟2.建立WLAN。

導覽至Configuration > Tags & Profiles > WLANs，然後選擇+Add。

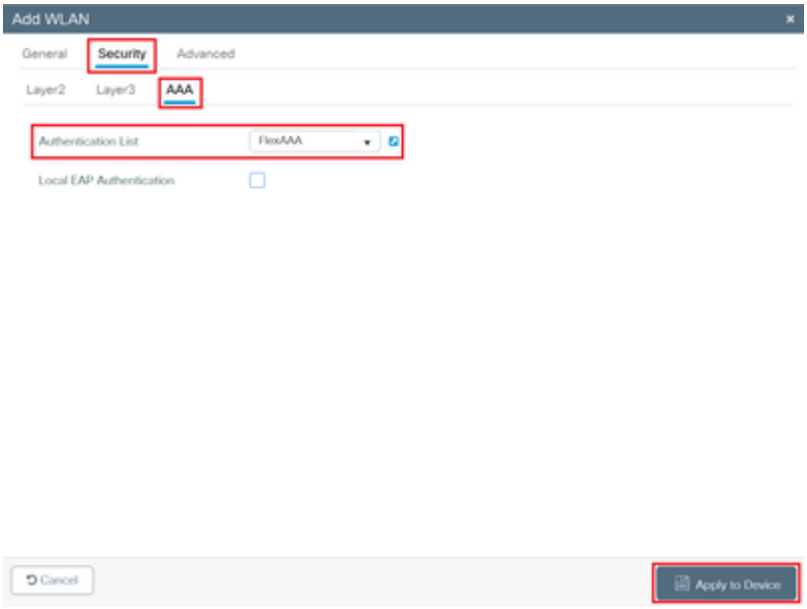
在General標籤上，為配置檔名稱、SSID和啟用狀態建立一個名稱：



步驟3.導航到安全> Layer 2頁籤，選擇WPA+WPA2（Wi-Fi保護訪問）、快速轉換作為啟用、身份驗證金鑰管理802.1X和FT+802.1X:



步驟4.導航至安全> AAA頁籤，在「身份驗證清單」下拉選單中選擇之前建立的清單：



按一下Update & Apply to Device。

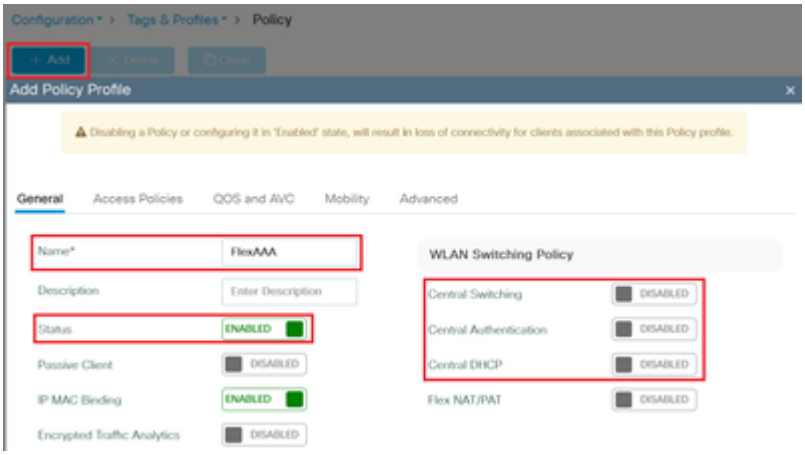
接著您會看到建立的WLAN:



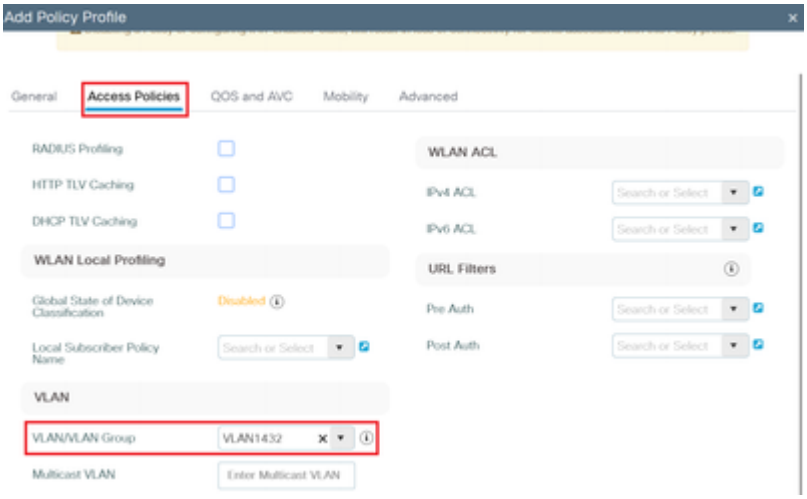
步驟5.建立策略配置檔案。

導覽至Configuration > Tags & Profiles > Policy。

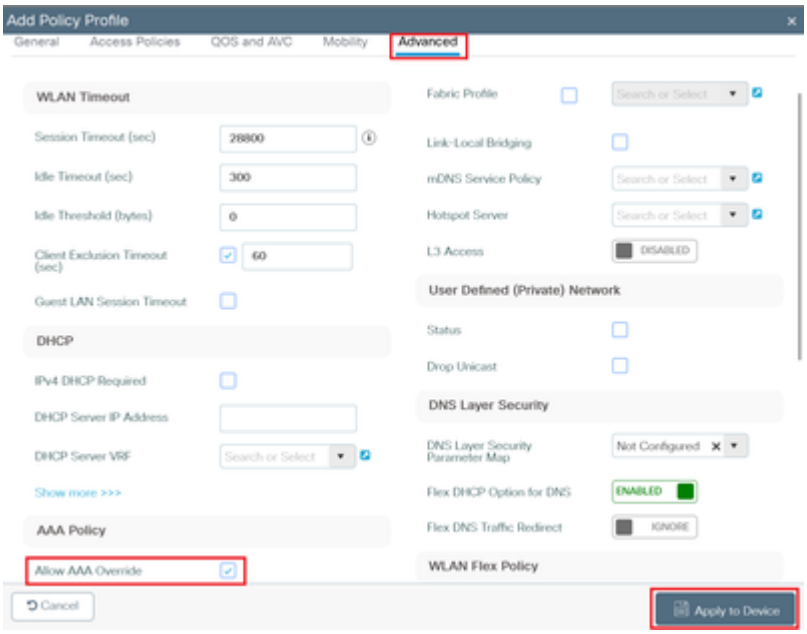
選擇+Add，然後在General頁籤上為策略配置檔案指定名稱，啟用狀態，並禁用集中交換、集中身份驗證和集中DHCP（動態主機配置協定）：



步驟6.導航到Access Policies選項卡，選擇VLAN:

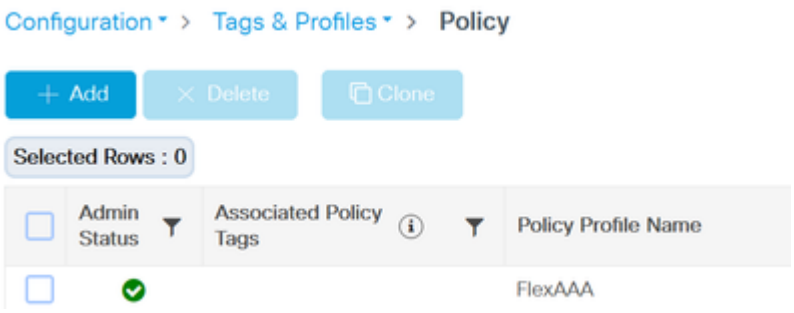


步驟7.導航到Advanced頁籤，啟用Allow AAA Override:



按一下「Update & Apply to Device」。

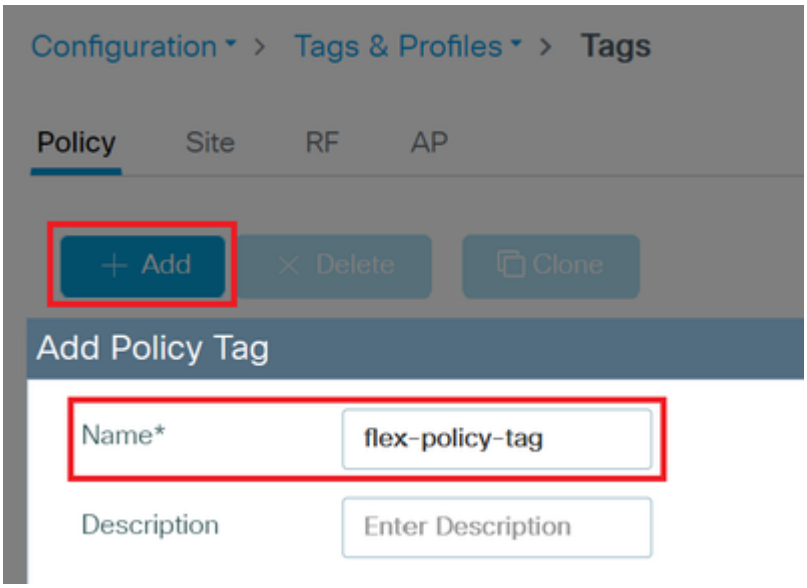
您可以在清單中看到策略配置檔案：



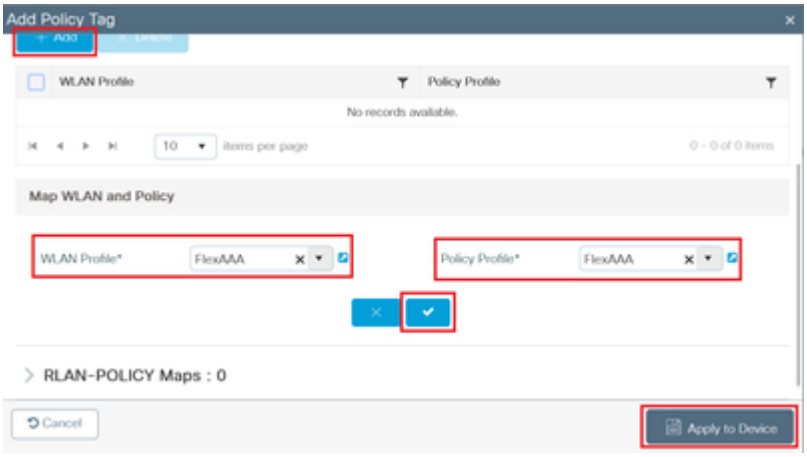
步驟8.建立策略標籤。

導航到Configuration > Tags & Profiles > Tags

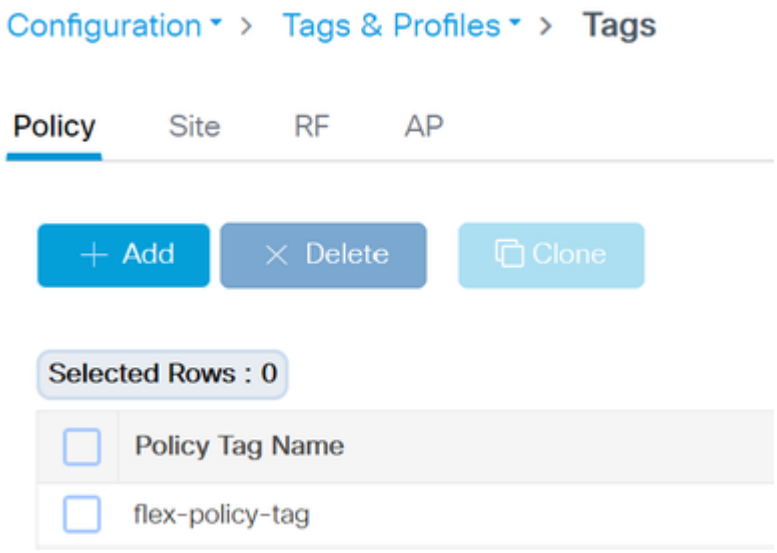
在Policy頁籤上，選擇+Add。為策略標籤指定名稱：



向下滾動並選擇WLAN-POLICY Maps下的+Add。在WLAN Profile中，從下拉選單中選擇之前建立的WLAN。在Policy Profile中，從下拉選單中選擇之前建立的策略配置檔案。按一下檢查按鈕，然後按一下Apply to Device:

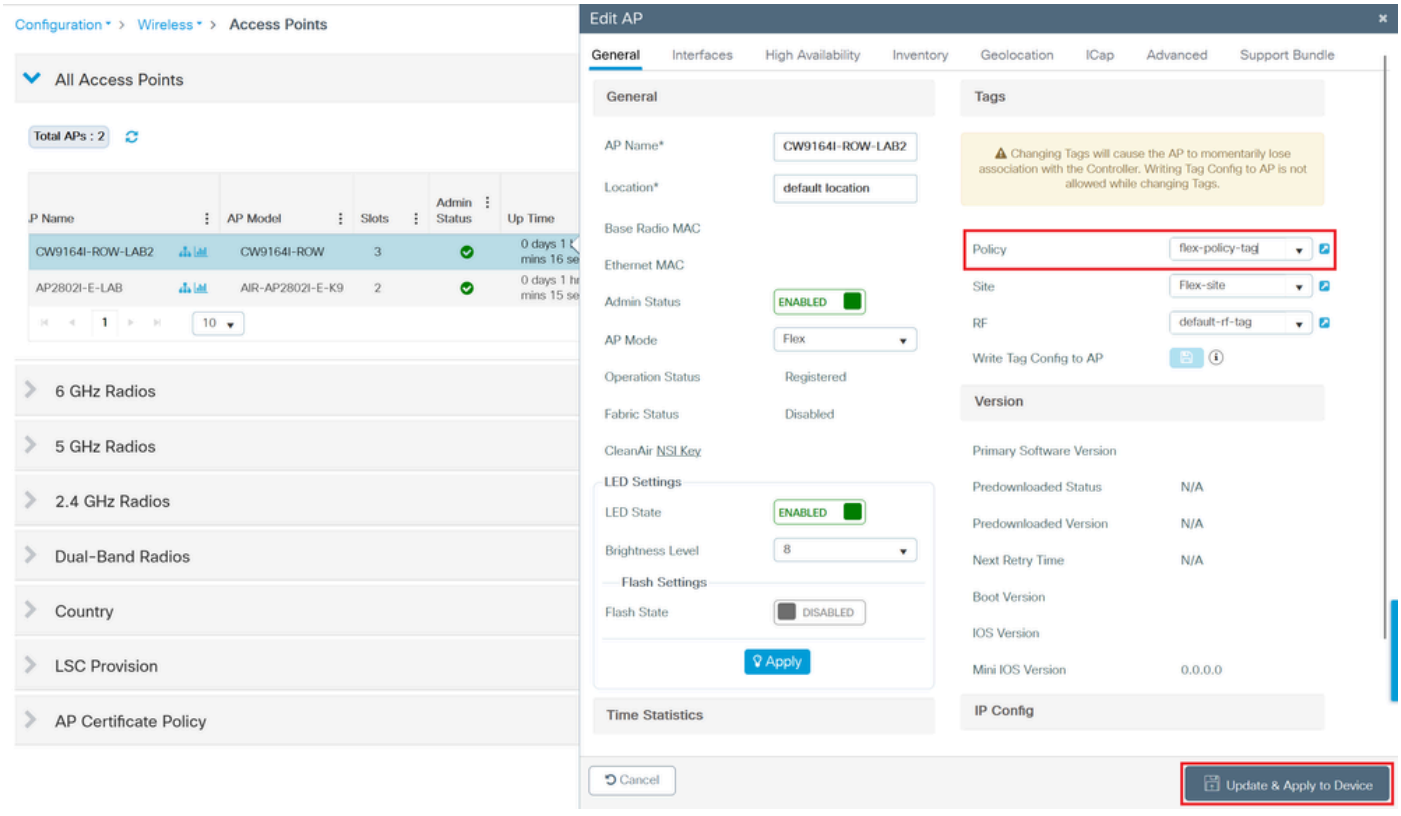


您可以在清單中看到策略標籤：



步驟9.在AP標籤上分配策略標籤。

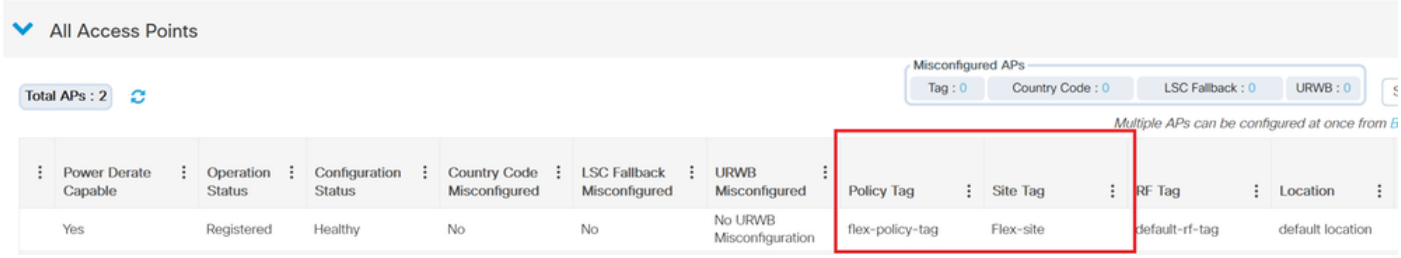
導覽至Configuration > Wireless > Access Points。選擇AP以更改標籤。



按一下Update & Apply to Device。

AP斷開連線，然後使用新的策略標籤重新連線。

當AP返回時，您可以檢查Access Points清單，確認AP處於Flex模式，以及指定的標籤：



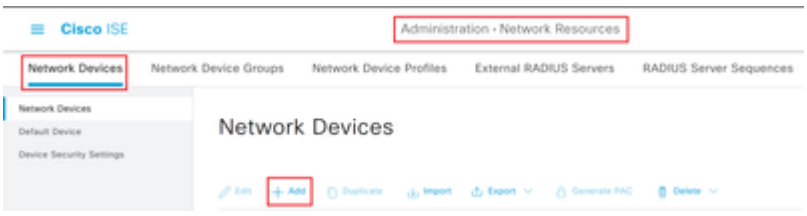
CLI:

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

配置ISE

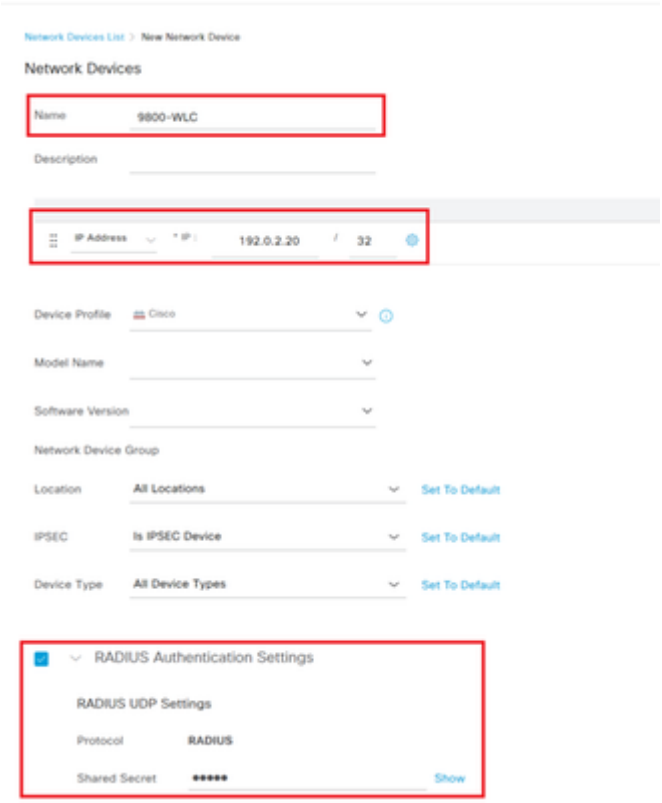
現在，您需要配置ISE才能在客戶端處於本地身份驗證時對其進行身份驗證。

步驟1.導覽至Administration > Network Resources > Network Devices。選擇+Add。



步驟2.新增9800 WLC。為其指定一個名稱，新增其IP地址，啟用RADIUS身份驗證設定，然後新增

共用金鑰。此金鑰必須與之前在9800 WLC上建立AAA伺服器時設定的金鑰相同。



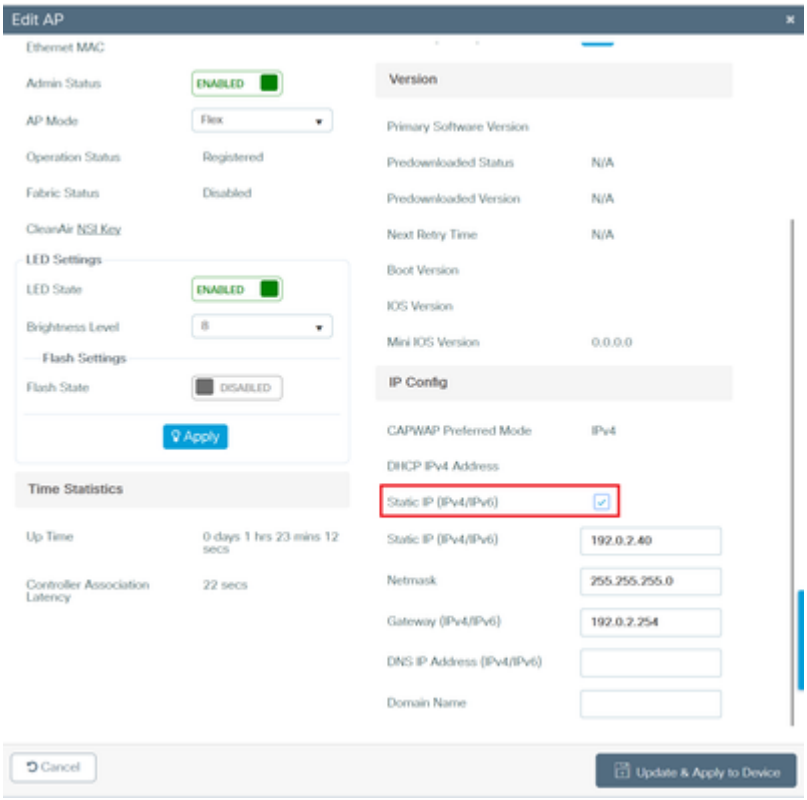
在右下角，按一下Save。

步驟3.我們需要將AP新增到「網路裝置」清單中，以便在遠端站點丟失WAN鏈路（以及AP移動到獨立模式時）時充當AAA身份驗證器/轉發器。

在9800 WLC GUI上導覽至Configuration > Wireless > Access Points，並記下每個AP IP位址。

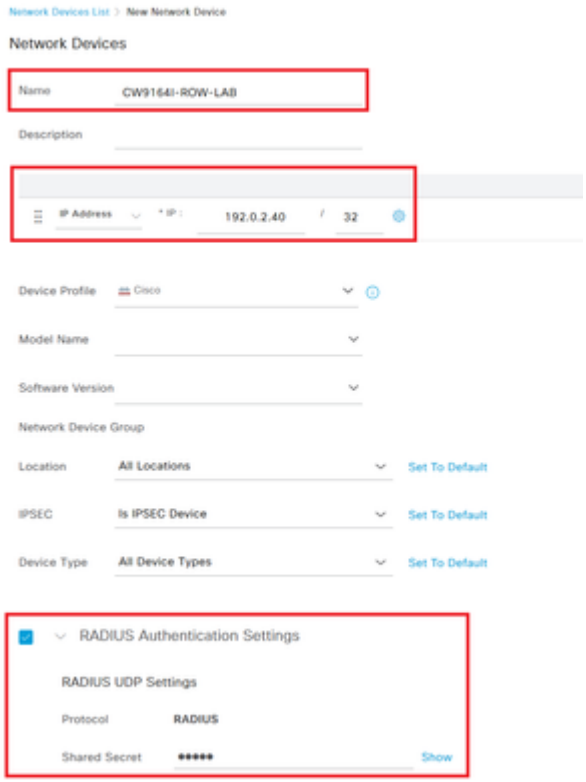
附註：將每個Flex AP的IP地址配置為靜態。當AP鬆動並重新恢復到9800 WLC的連線時，它們可能會返回一個與DHCP不同的IP地址，從而失去與ISE的通訊。

啟用靜態IP(IPv4/IPv6)。 按一下Update & Apply to Device:



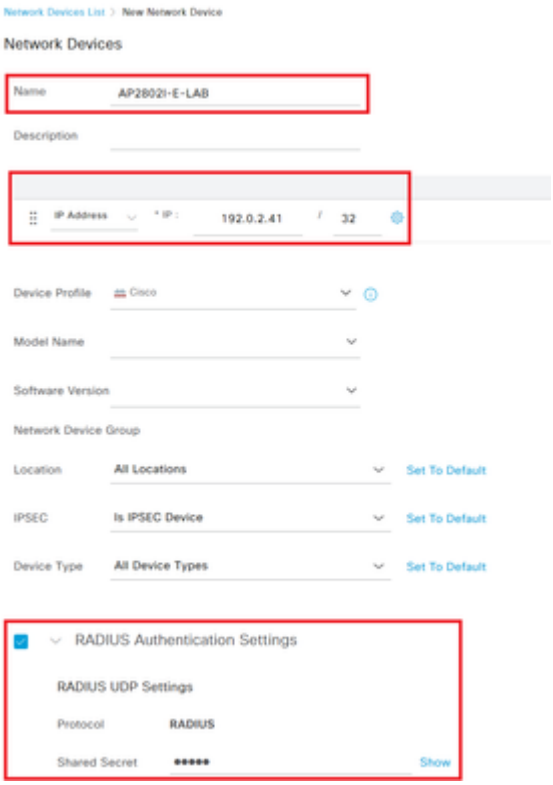
步驟4.返回ISE，導航到Administration > Network Resources > Network Devices。選擇+Add。

將存取點新增為網路裝置，其組態與9800 WLC相同：



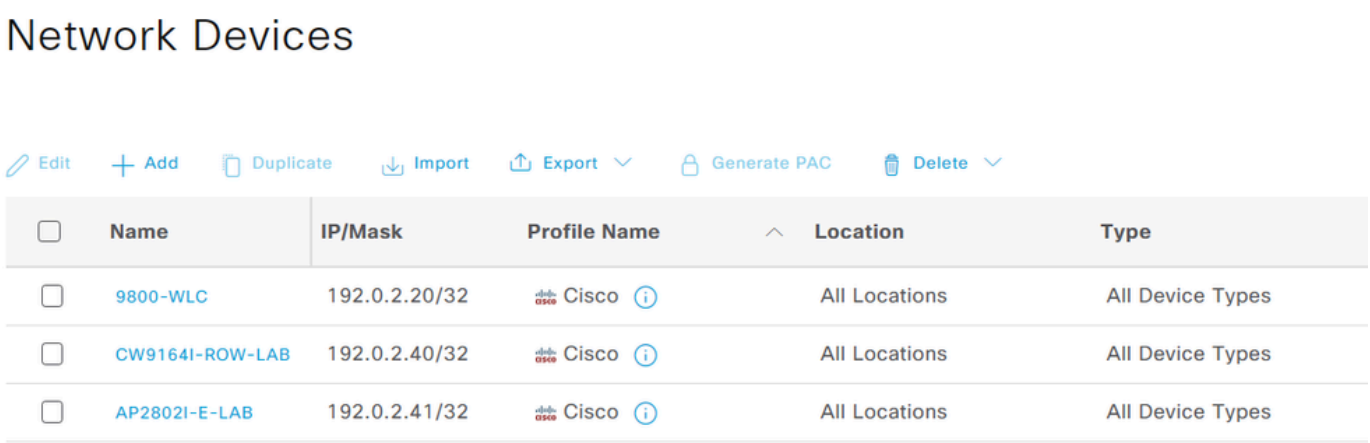
在右下角，按一下Save。

對於第二個AP:



在右下角，按一下Save。

您可以看到以下網路裝置清單：



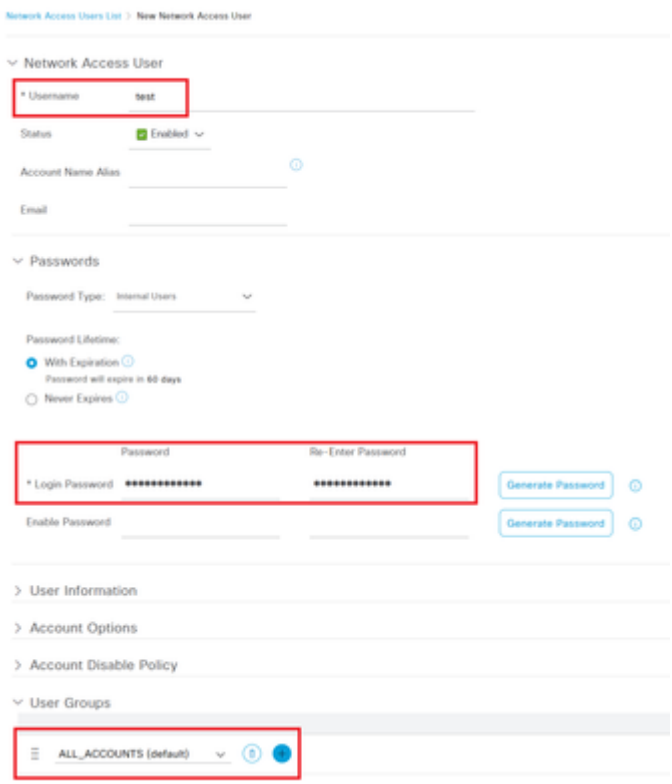
如果您的AP位於連續的IP範圍內，您可以使用掩碼功能配置單個條目，該條目為整個AP組（如果不是全部）定義共用金鑰。在ISE中，實際上不需要為每個AP配置一個網路裝置。但是請注意，通

過使用萬用字元和掩碼，可為欺詐裝置留出一些空間來嘗試作為ISE的轉發器。

步驟5.在Users頁籤上導航到Administration > Identity Management > Identities，然後建立用於802.1x身份驗證的使用者。選擇+Add:

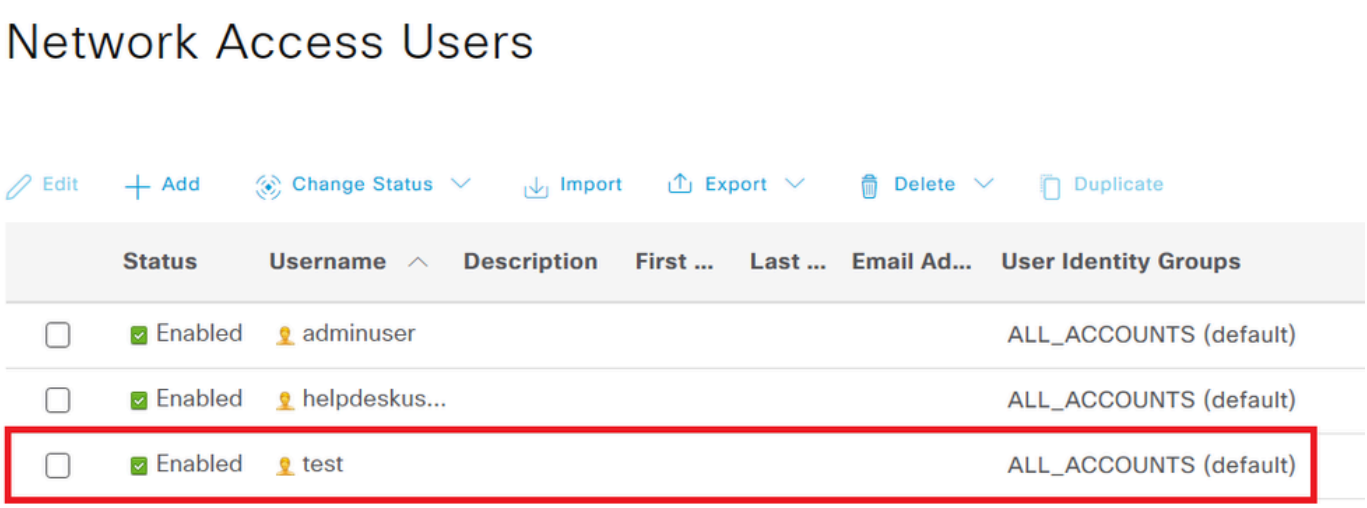


建立使用者名稱、密碼（並在重新輸入密碼時鍵入相同的密碼），然後從「使用者組」下拉選單中選擇ALL_ACCOUNTS（預設值）：



在右下角，按一下Submit。

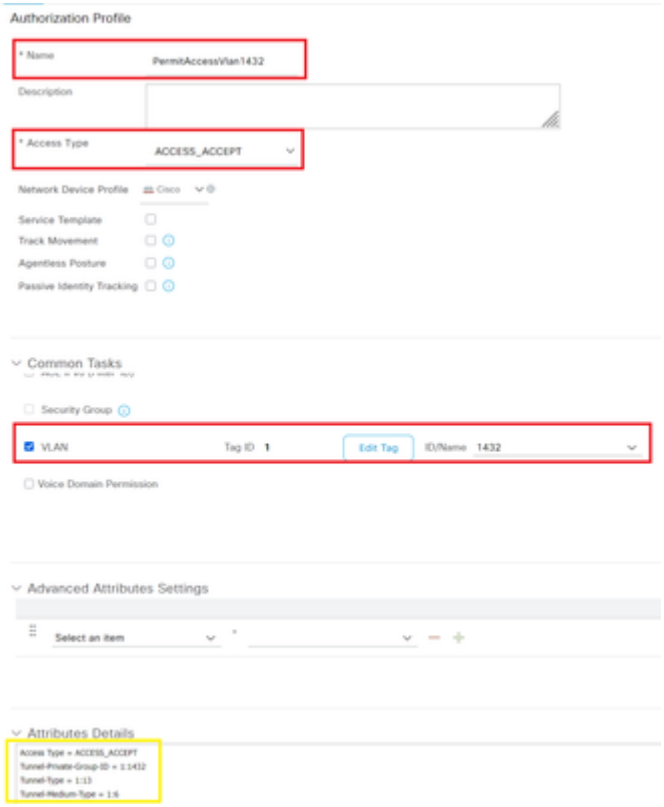
您可以在Network Access Users清單中看到使用者：



步驟6.導覽至Policy > Policy Elements > Results。在Authorization > Authorization Profiles頁籤上，選擇+Add。



為分配給本地身份驗證客戶端的VLAN建立授權配置檔案：

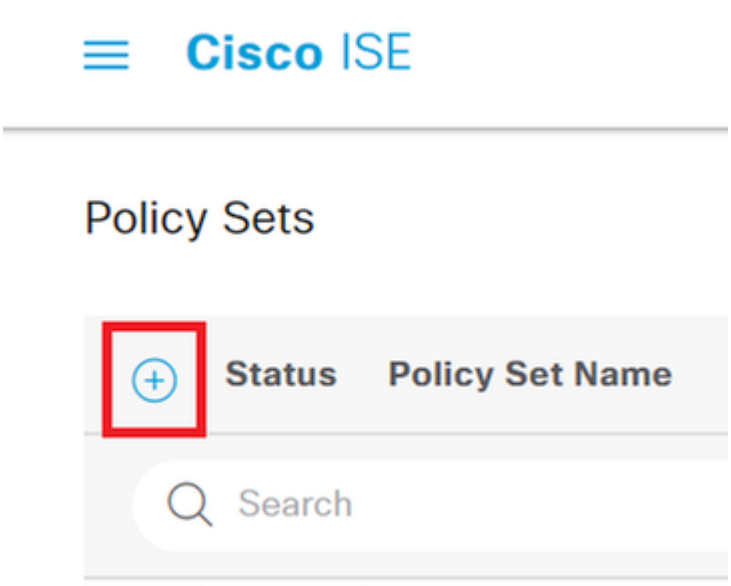


在右下角，按一下Submit。

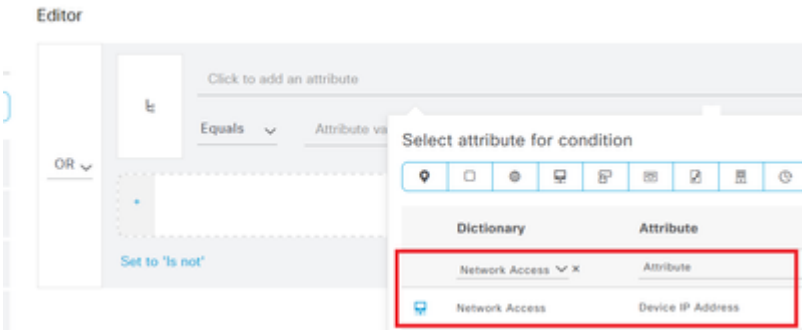
在成功案例中，您會看到ISE傳送到WLC/AP的屬性詳細資訊。

步驟7.導覽至Policy > Policy Sets。建立新的策略集。

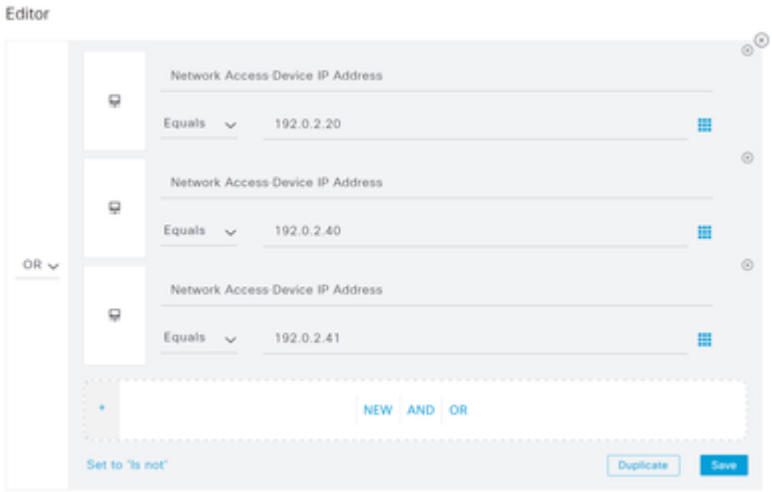
按一下+sign:



為策略集指定一個名稱。在Conditions列中，新增OR規則並新增詞典Network Access，在Attribute Device IP Address中選擇Equals:

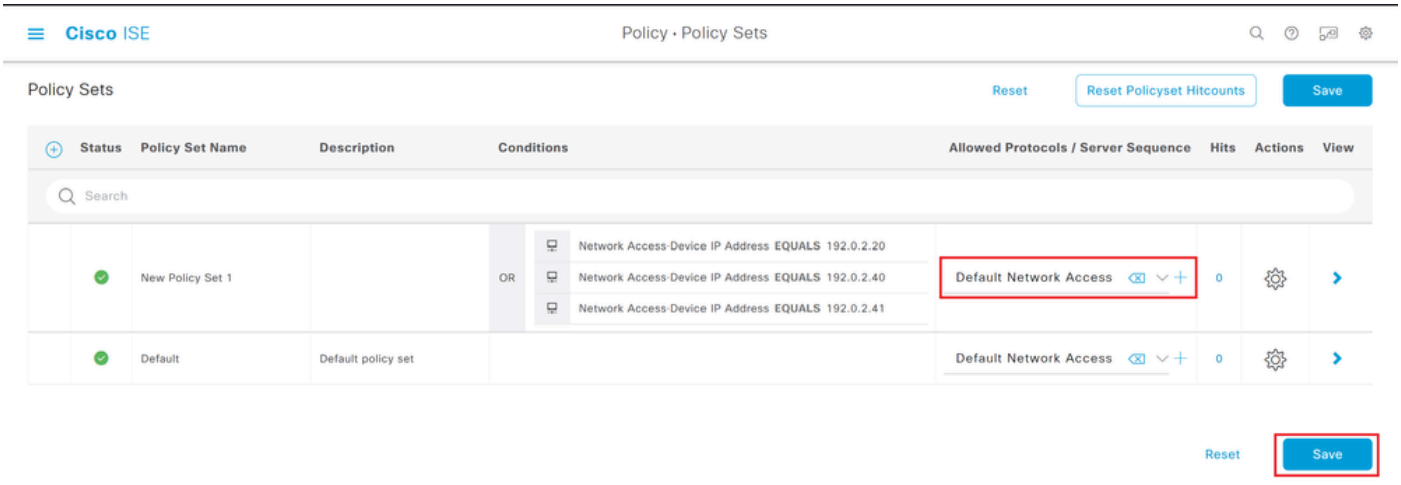


新增9800 WLC和AP的IP地址：

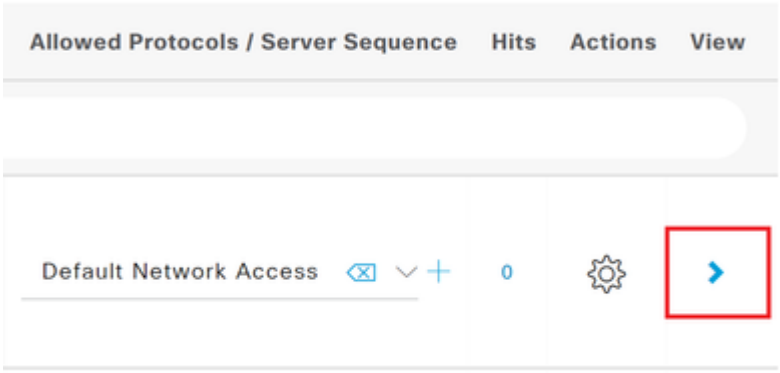


在右下角，按一下Use。

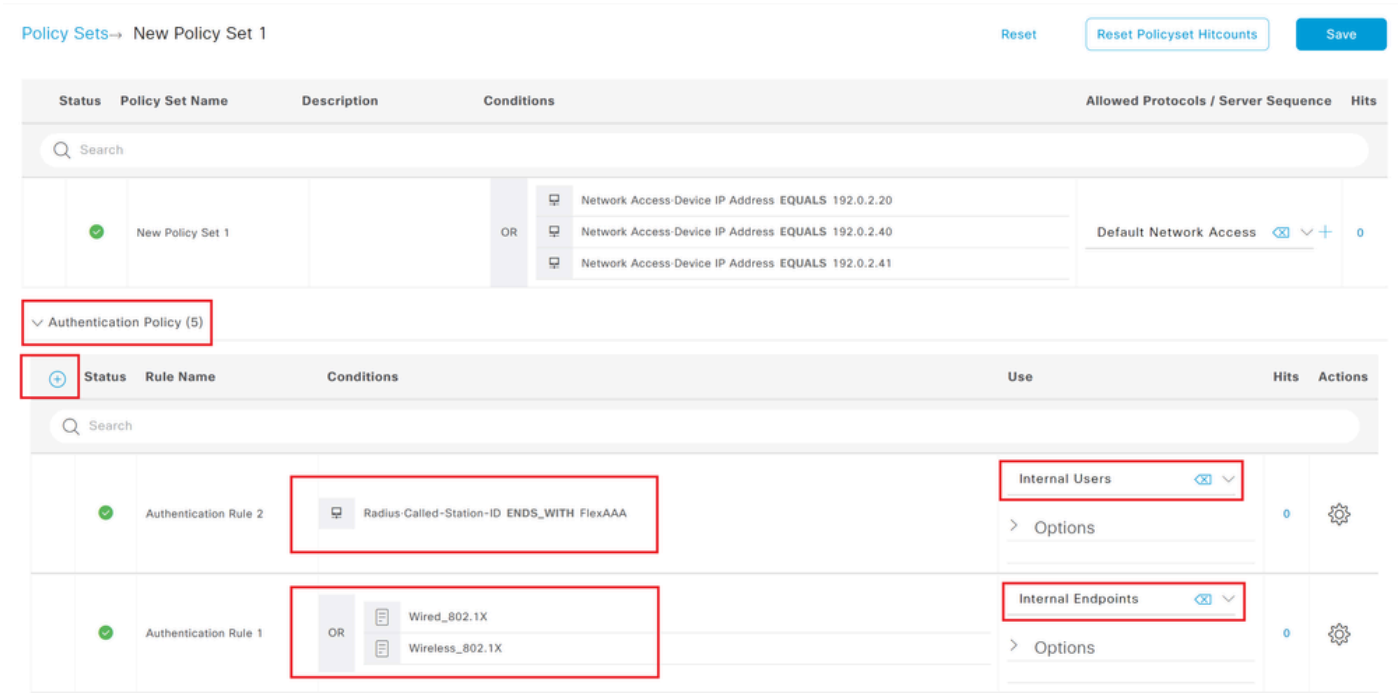
步驟8.在Allowed Protocols列中選擇Default Network Access。最後，按一下Save:



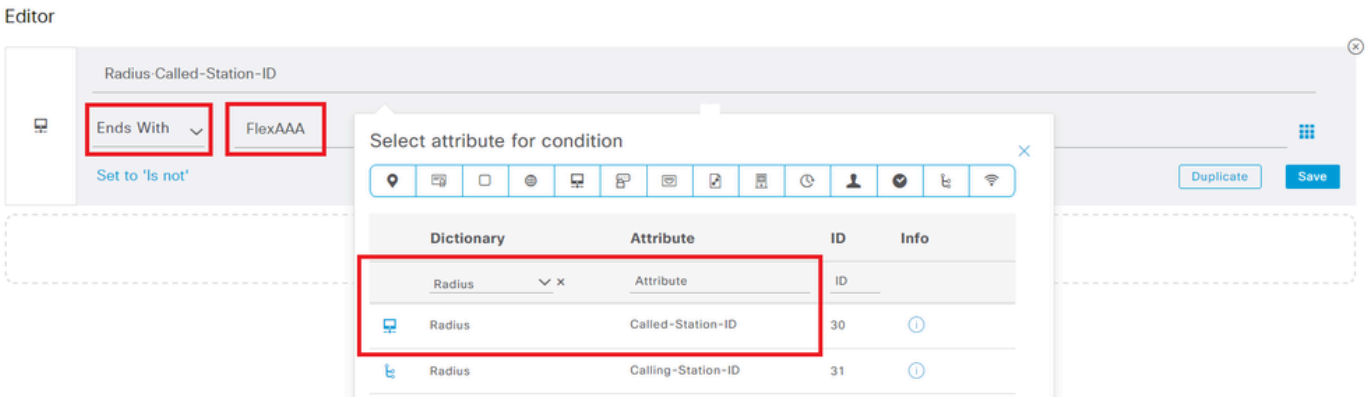
步驟9.在View列中，按一下箭頭符號：



步驟10.展開Authentication Policy，建立兩個新策略：一個用於WLAN名稱，另一個用於802.1X配置：

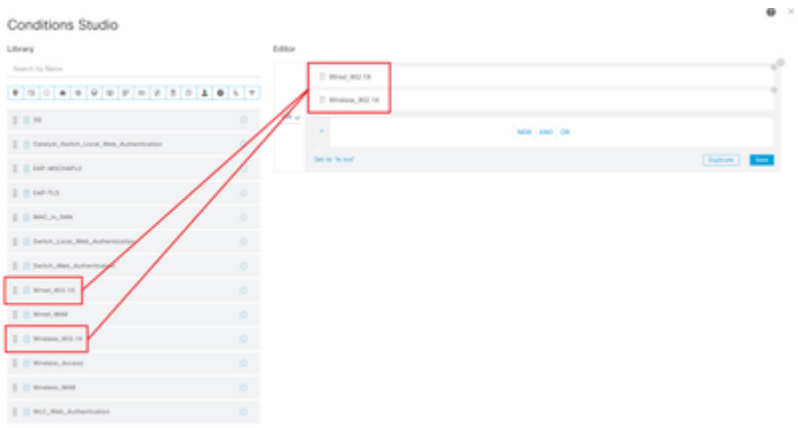


對於WLAN名稱，使用字典Radius和屬性Called-Station-ID建立Condition。選擇Ends With並鍵入WLAN名稱：



在右下角，按一下Use。對於此策略，在Use列上，選擇Internal Users。

步驟11.對於802.1X策略，使用ISE上可用的Wired_802.1X和Wireless_802.1X庫建立Condition。您可以拖放這些專案，並選擇條件或：



在右下角，按一下Use。對於此策略，在Use列上，選擇Internal Endpoints。

步驟12.向下滾動到Authorization Policy並建立新策略。為其指定一個名稱，然後建立與身份驗證策略上為WLAN名稱建立的相同條件。

在Profiles列上，從下拉選單中選擇配置檔案PermitAccessVlan1432:



在右下角，按一下Save。

使用本地身份驗證配置PSK WLAN

步驟1.首先按照在遠端站點上配置FlexConnect模式一節所述在Flex模式下配置AP。

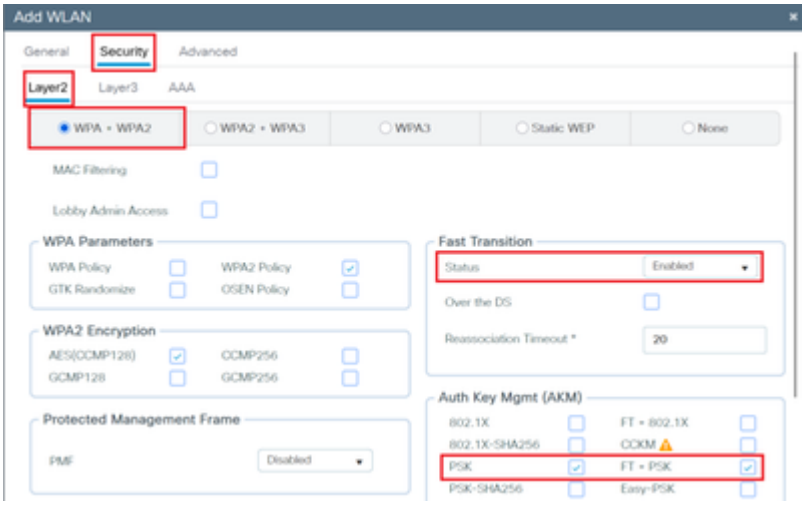
步驟2.建立WLAN。

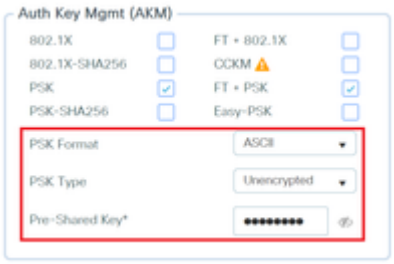
導覽至Configuration > Tags & Profiles > WLANs，然後選擇+Add。

在General標籤上，為配置檔名稱、SSID和啟用狀態建立一個名稱：



步驟3.導航到安全>第2層頁籤，選擇WPA+WPA2、快速轉換已啟用、身份驗證金鑰管理PSK和FT+PSK，選擇所需的PSK格式和PSK型別，然後鍵入希望客戶端使用的預共用金鑰：





按一下Update & Apply to Device。

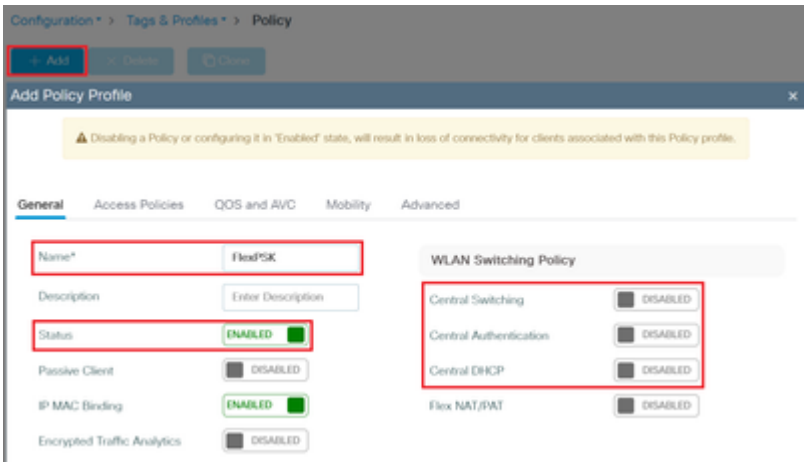
您可以看到建立的WLAN:



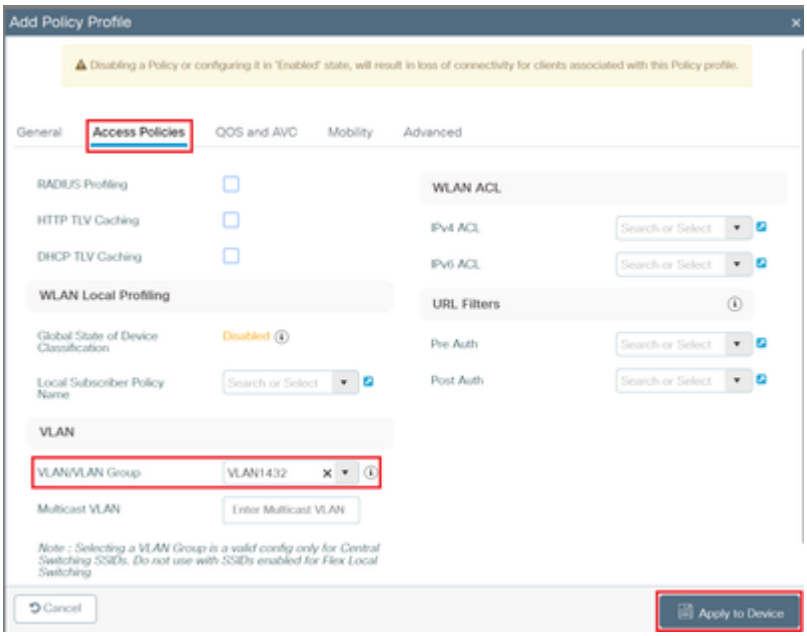
步驟4.建立策略配置檔案。

導航到Configuration > Tags & Profiles > Policy。

選擇+Add並在General頁籤上為策略配置檔案指定名稱，啟用狀態，並禁用集中交換、集中身份驗證和集中DHCP:

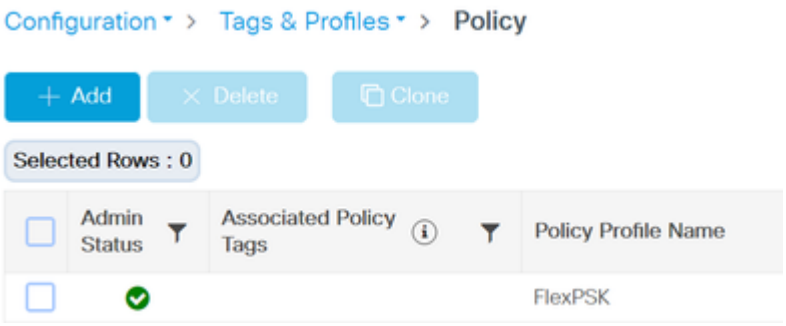


步驟5.導覽至Access Policies頁籤，選擇VLAN:



按一下Update & Apply to Device。

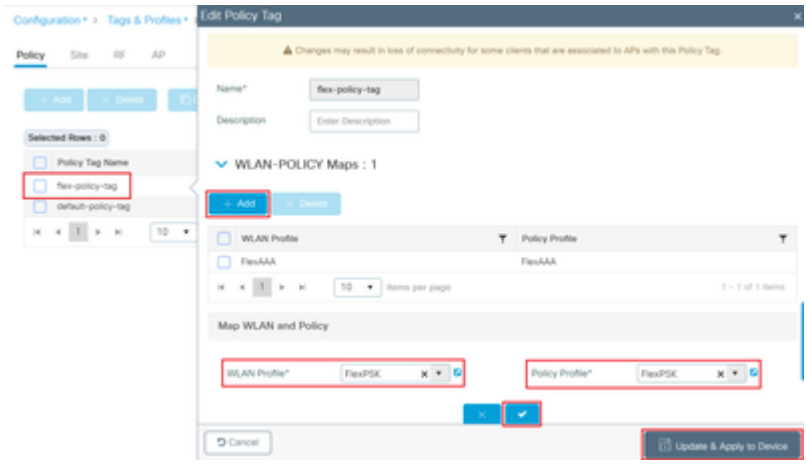
您可以在清單中看到策略配置檔案：



步驟6.您可以建立新的策略標籤，也可以編輯現有策略標籤。

導航到Configuration > Tags & Profiles > Tags以編輯現有策略標籤。選擇要編輯的標籤。

在WLAN-POLICY Maps下選擇+Add。在WLAN Profile中，從下拉選單中選擇之前建立的WLAN。在Policy Profile中，從下拉選單中選擇之前建立的策略配置檔案。按一下檢查按鈕，然後按一下Apply to Device:



如果在AP上已分配策略標籤，則無需執行其他操作。

如果不是，請在AP標籤上分配策略標籤。導航到Configuration > Wireless > Access Points。選擇AP以更改策略標籤，然後按一下「更新並應用到裝置」。

AP會分離並使用新的策略標籤重新連線。

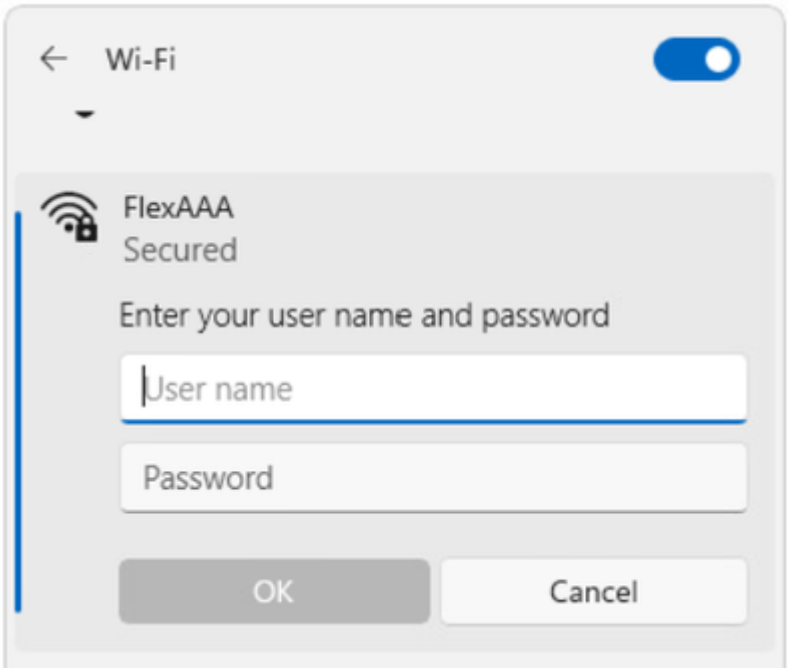
當AP返回時，您可以檢查Access Points清單，確認AP處於Flex模式，並且它有正確的分配標籤。

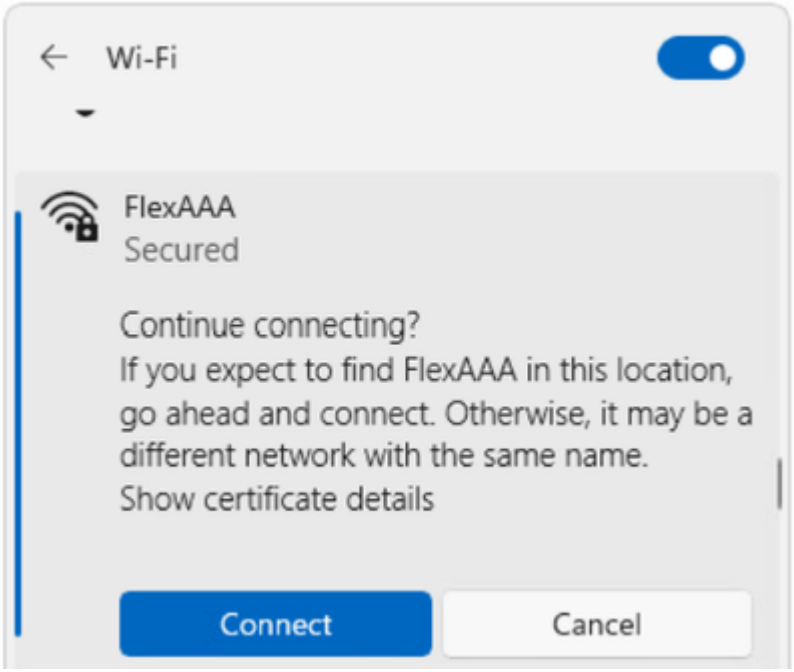
CLI:

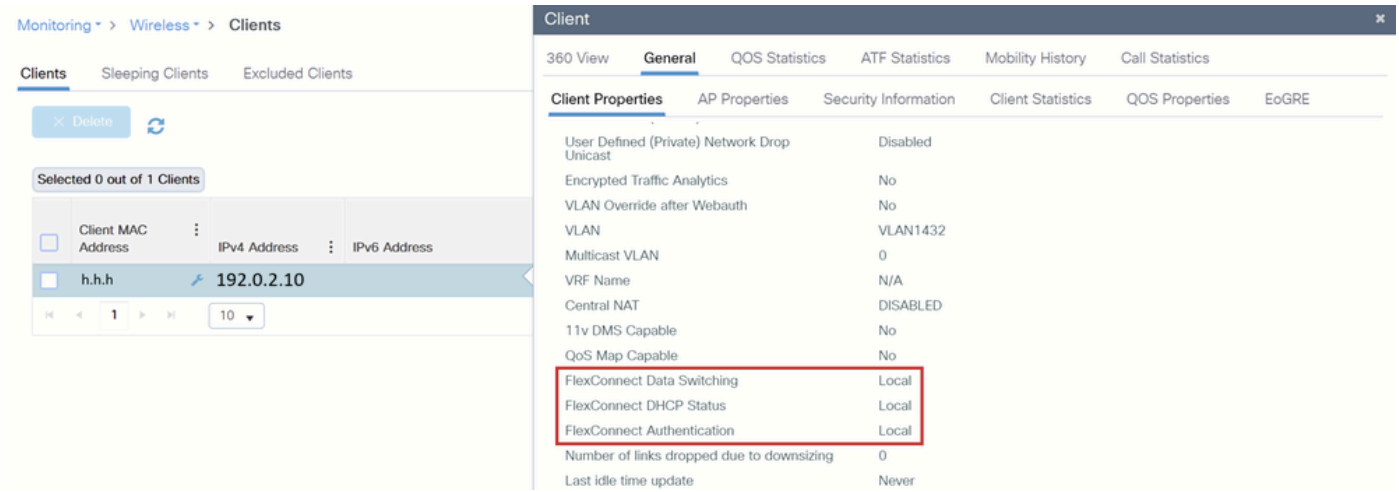
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

驗證

對於802.1x WLAN:







CLI:

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

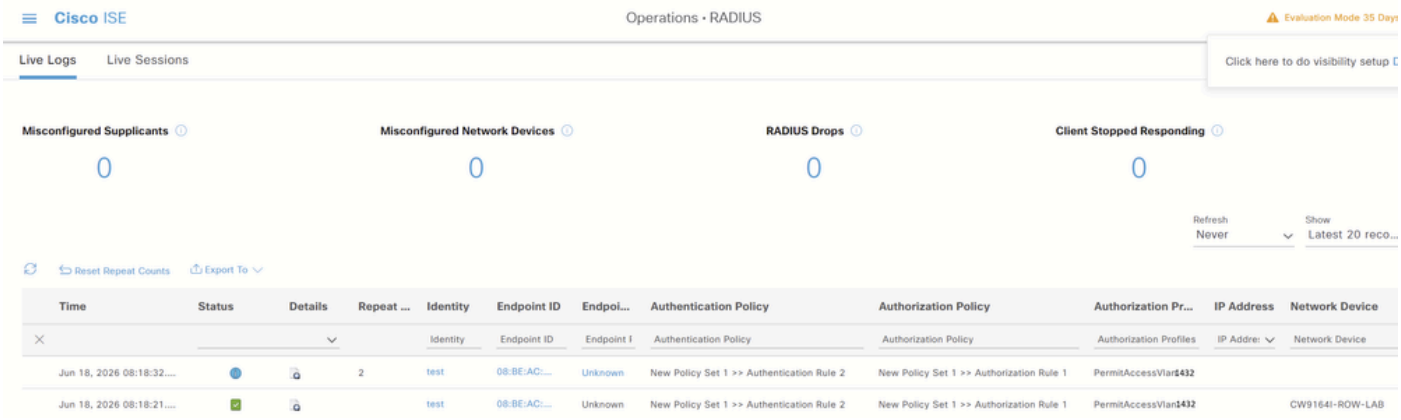
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

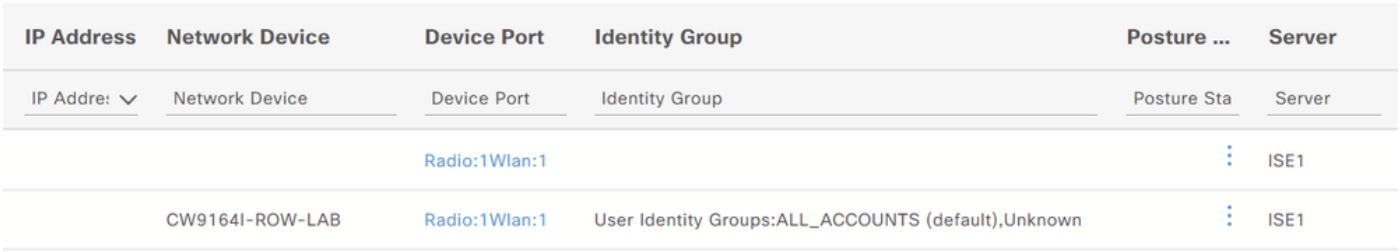
在AP CLI上：

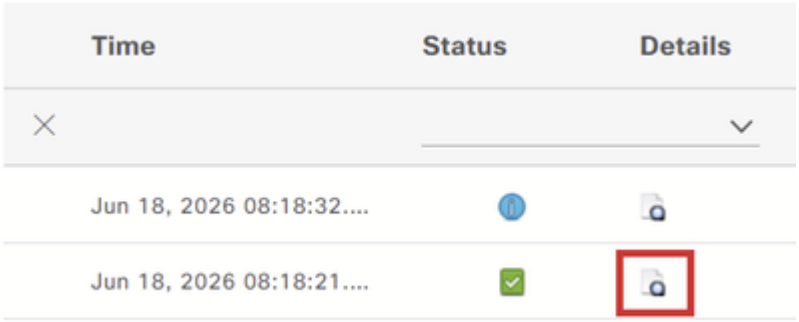
```
CW9164I-ROW-LAB#show dot11 clients

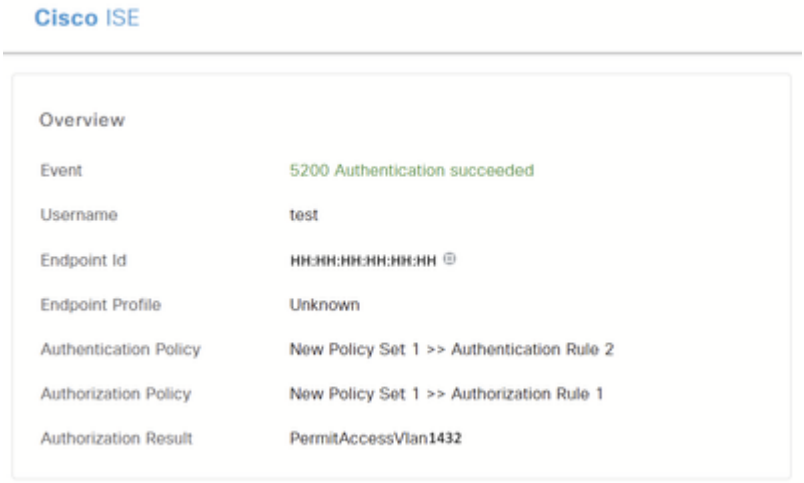
Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH          1       1  33   FlexAAA  -45 MCS9ISS           No          No
```

在ISE上


Cisco ISE
Operations · RADIUS
Evaluation Mode 35 Days
Live Logs
Live Sessions
Click here to do visibility setup
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Refresh
Never
Show
Latest 20 reco...
Reset Repeat Counts
Export To
Time
Status
Details
Repeat ...
Identity
Endpoint ID
Endpoi...
Authentication Policy
Authorization Policy
Authorization Pr...
IP Address
Network Device
Jun 18, 2026 08:18:32....
2
test
08:BE:AC:...
Unknown
New Policy Set 1 >> Authentication Rule 2
New Policy Set 1 >> Authorization Rule 1
PermitAccessVlan1432
Jun 18, 2026 08:18:21....
test
08:BE:AC:...
Unknown
New Policy Set 1 >> Authentication Rule 2
New Policy Set 1 >> Authorization Rule 1
PermitAccessVlan1432
CW9164I-ROW-LAB

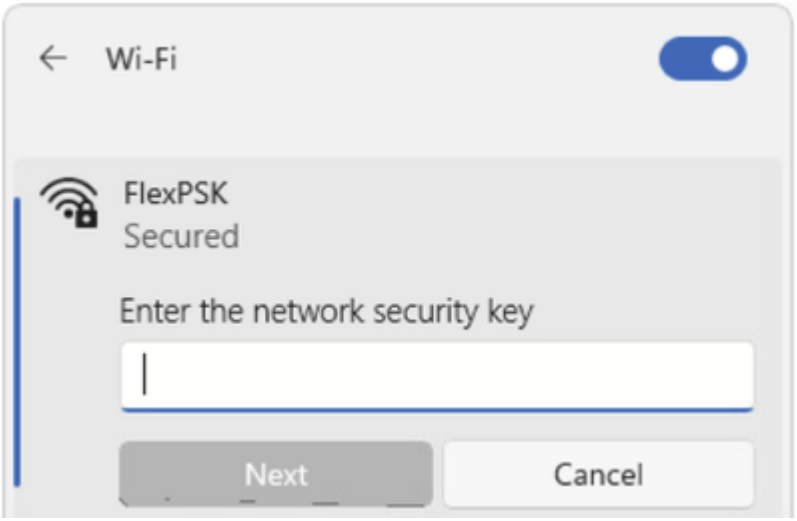

IP Address
Network Device
Device Port
Identity Group
Posture ...
Server
IP Addre:
Network Device
Device Port
Identity Group
Posture Sta
Server
Radio:1Wlan:1
ISE1
CW9164I-ROW-LAB
Radio:1Wlan:1
User Identity Groups:ALL_ACCOUNTS (default),Unknown
ISE1

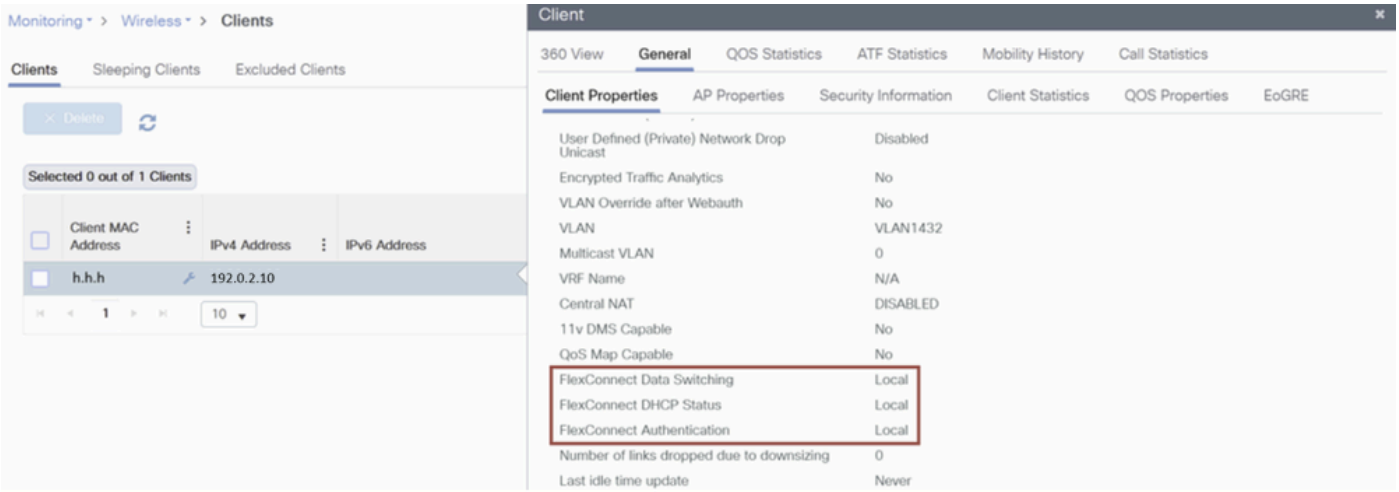

Time
Status
Details
Jun 18, 2026 08:18:32....
Jun 18, 2026 08:18:21....


Cisco ISE
Overview
Event
5200 Authentication succeeded
Username
test
Endpoint Id
HH:HH:HH:HH:HH:HH
Endpoint Profile
Unknown
Authentication Policy
New Policy Set 1 >> Authentication Rule 2
Authorization Policy
New Policy Set 1 >> Authorization Rule 1
Authorization Result
PermitAccessVlan1432

Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

對於PSK WLAN:





CLI:

```
C9800-1#show wireless client mac-address      h.h.h      detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

在AP CLI上：

```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
  xxxxxxxxxxxx          1       2  33   FlexPSK  -45 MCS9iSS          No          No
```

疑難排解

啟用同步使用客戶端MAC地址的AP調試和RA跟蹤。

在AP上啟用以下調試：

debug flexconnect event
debug flexconnect pmk
debug flexconnect dot11r
debug dot11 client management information
debug dot11 client management critical
debug dot11 client management errors
debug dot11 client management events

對於802.1x WLAN:

AP調試成功身份驗證的日誌：

AP處理802.11狀態機和本地金鑰管理。
AP處理關聯並準備客戶端進行身份驗證。

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

AP處理授權，應用VLAN覆蓋，並將客戶端移動到FWD（轉發）狀態。

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

相同成功身份驗證的RA跟蹤日誌：

RA追蹤記錄了WLC的作業階段編排。WLC驗證使用者端身分和原則。
WLC可識別FlexConnect關聯。

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

WLC將策略推送到AP。

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
```

```
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

授權成功。

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

客戶端引數。
2026/06/19 06:49:20.939394217 {wncd_x_R0-1}{1}:[dot11] [18318]:（註）：MAC:hhhh.hhh.hhh客戶端資料路徑條目引數 — ssid:FlexAAA，slot_id:1 bssid ifid:0x0, radio_ifid:0x90400008, wlan_ifid:0xf0400004

WLC通過本地DHCP/ARP獲取IP。
2026/06/19 06:49:21.001000218 {wncd_x_R0-1}{1}:[client-iplearn] [18318]:（註）：MAC:hhhh.hhh.hhh客戶端IP學習成功。方法：IP窺探IP:192.0.2.10

客戶端已完全連線。
2026/06/19 06:49:21.002363496 {wncd_x_R0-1}{1}:[errmsg] [18318]:（資訊）：%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE:R0/1:wncd:使用MAC的裝置使用者名稱條目（測試）與ssid(FlexAAA)加入：hhhh.hhh.hhhh在通道上(48)
2026/06/19 06:49:21.002795009 {wncd_x_R0-1}{1}:[client-orch-state] [18318]:（註）：MAC:hhhh.hhh.hhh客戶端狀態轉換：S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

獨立方案

AP-WLC連線丟失和後續恢復期間的行為。

AP已加入WLC。客戶端成功執行802.1X身份驗證，然後AP將客戶端轉換為FWD（轉發）狀態。

在ISE RADIUS即時日誌中，我們看到客戶端會話。

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

AP無法到達WLC，耗盡其重新傳輸計數，然後切換到獨立模式。現有客戶端在本地保持連線。

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

但是使用者端仍舊連線：

CW9164I-ROW-LAB2#show dot11客戶端

Dot11客戶端總數：1
客戶端MAC插槽ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7否否

當客戶端在獨立模式下漫遊到另一個AP時，由於無法訪問RADIUS伺服器，EAP握手失敗。客戶端已取消授權並從AP中刪除。

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

AP將客戶端會話傳送到備份RADIUS伺服器。

AP重新連線到WLC。AP切換回連線模式，並將本地客戶端會話資訊與WLC同步。

客戶端會話根據AP連線狀態在主和備份ISE節點之間轉換。

AP和客戶端在WLC上顯示為已連線，並且當AP和WLC之間的連線關閉時，客戶端未發現任何斷開或翻動。

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, m
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASS
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD

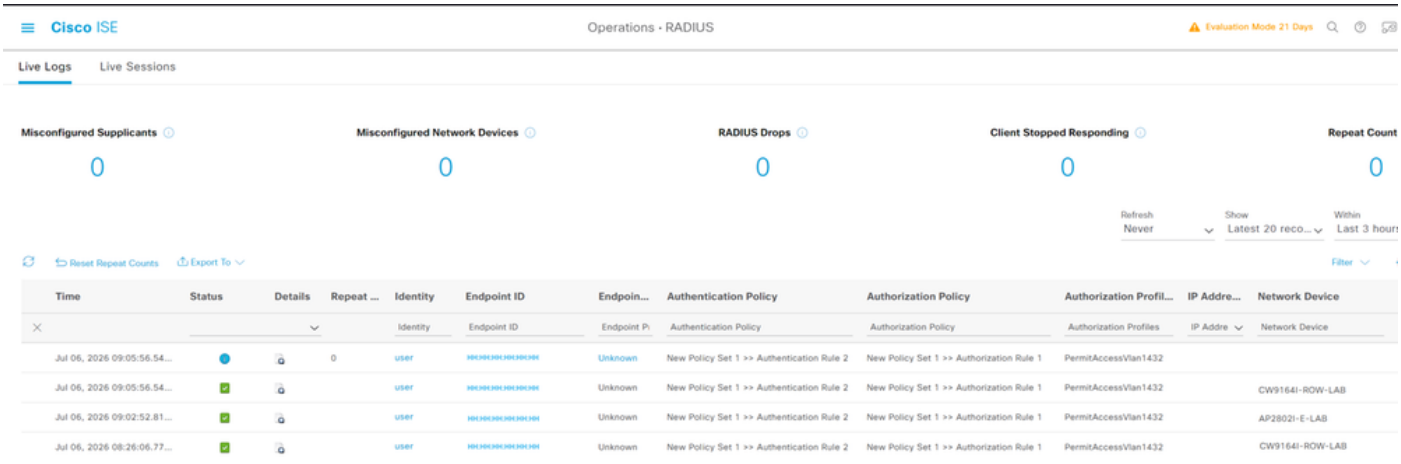

CW9164I-ROW-LAB2#show dot11 clients
```

```
Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No
```

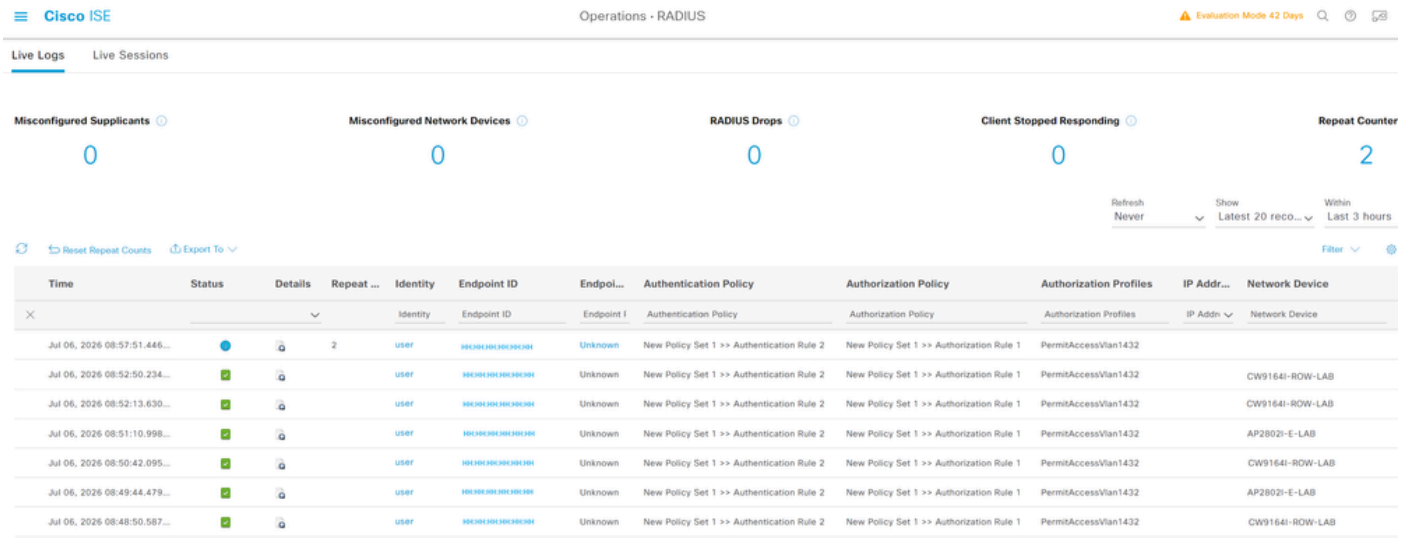
```
*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
```

```
CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



主ISE:記錄WLC連線恢復後的初始會話(08:26:06)和續會(09:02:52)。



備份ISE:捕獲AP在獨立模式下運行時發生的會話活動(08:48:50 - 08:57:51)。

第一個會話在08:26:06，之後AP失去與WLC的連線並移至獨立模式。

會話09:02:52是AP與WLC重新建立連線後的第一個會話。

相關資訊

- CCNP企業無線設計ENWLSD 300-425和實施ENWLSI 300-430官方認證指南，第2版
- Cisco Catalyst 9800系列無線控制器軟體配置指南，Cisco IOS XE 17.8.x — 章節：FlexConnect
- Cisco Catalyst 9800系列無線控制器、Cisco IOS XE Cupertino版本17.8.x的版本說明
- 思科無線接入點的功能表
- 思科技術支援與下載

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）。