在Catalyst 9800無線控制器系列上配置802.1X身份驗證

目錄

簡介

本文說明如何在Cisco Catalyst 9800系列無線控制器上設定具有802.1X安全性的WLAN。

必要條件

需求

思科建議您瞭解以下主題：

- 802.1X

採用元件

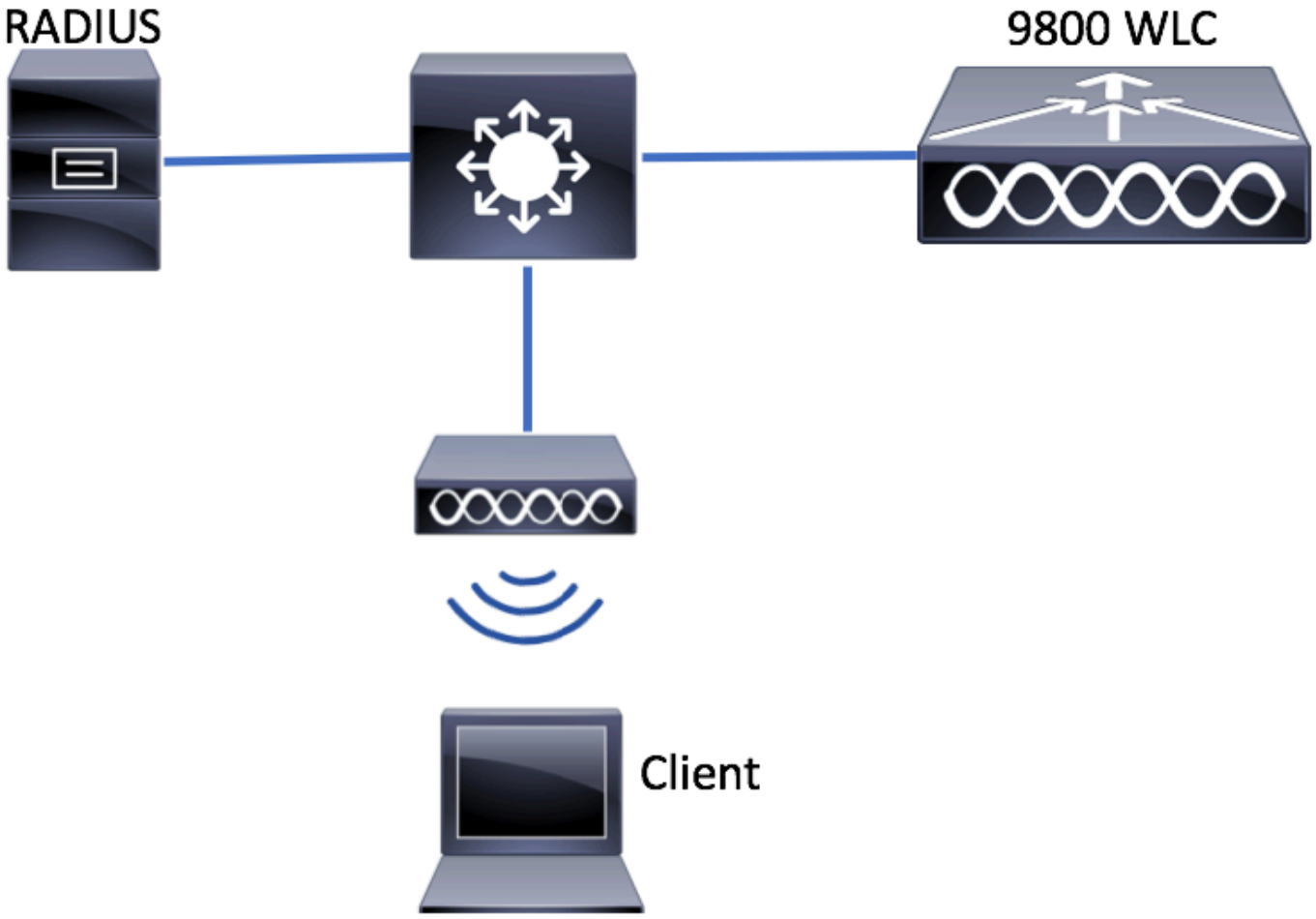
本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9800無線控制器系列(Catalyst 9800-CL)
- Cisco IOS® XE直布羅陀版17.3.x
- Cisco ISE 3.0

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

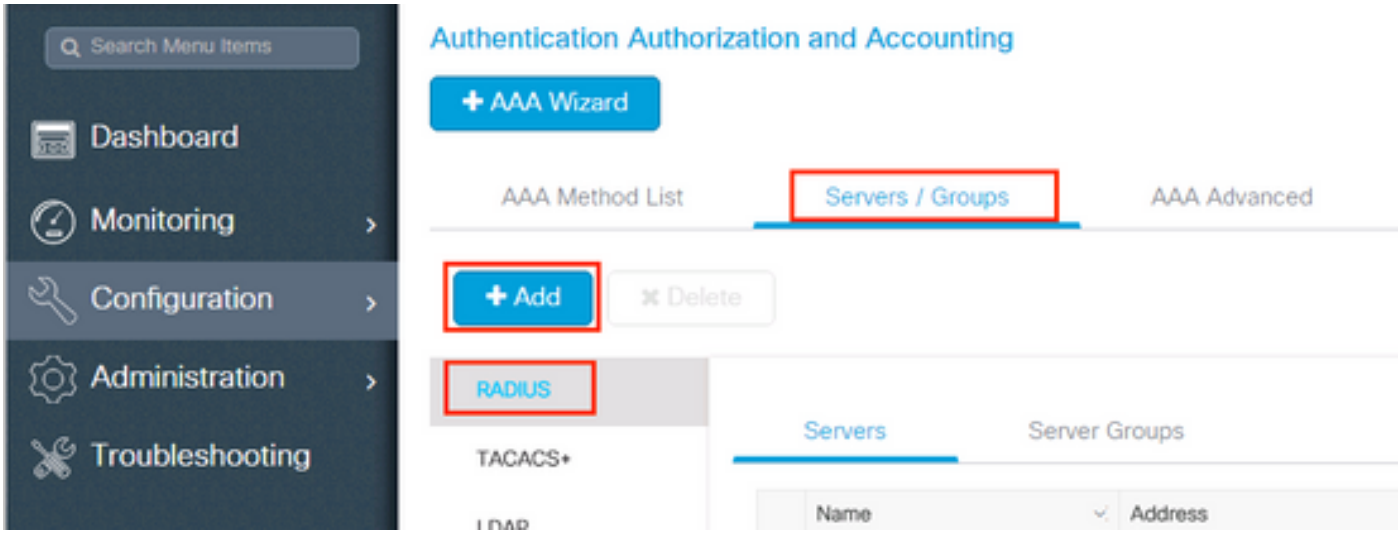


WLC組態

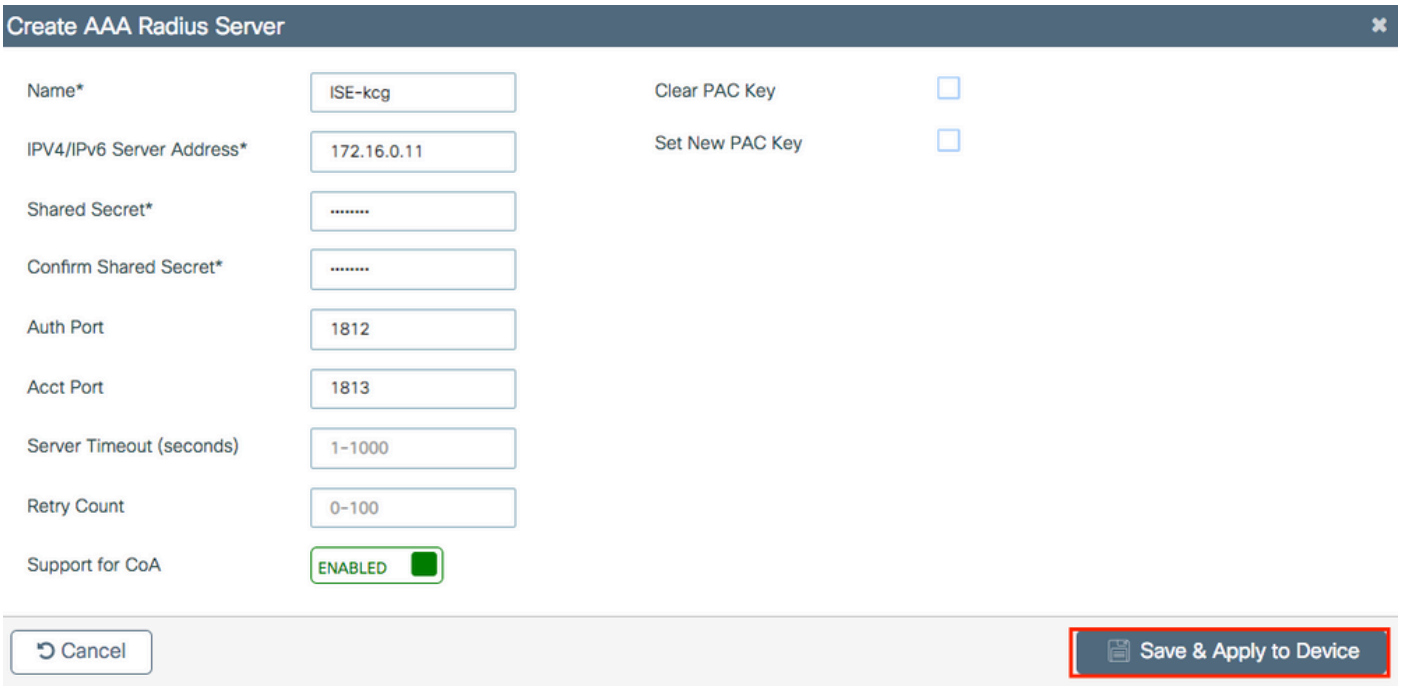
9800 WLC上的AAA組態

GUI:

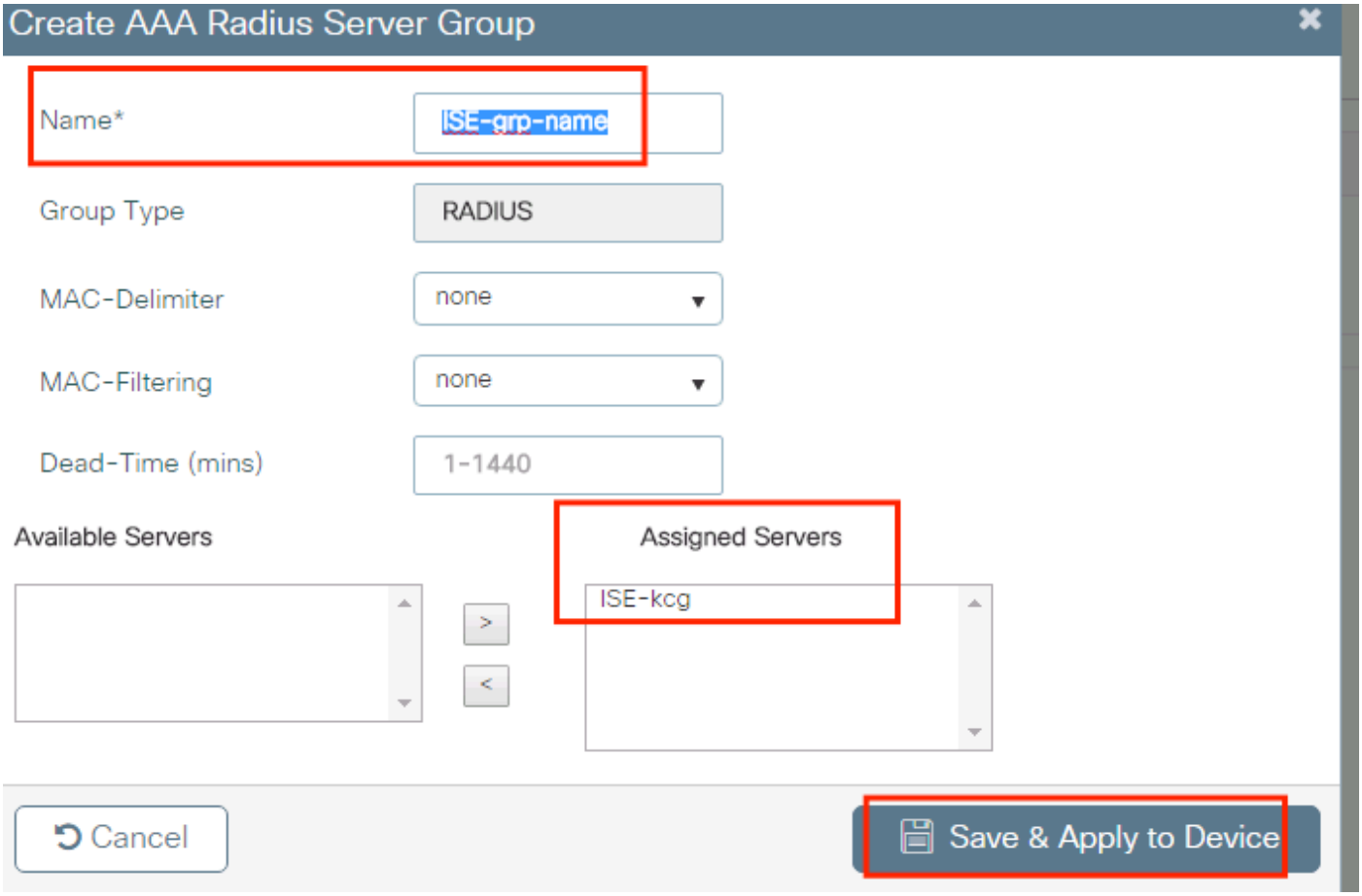
步驟1.宣告RADIUS伺服器。導航至 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** 並輸入RADIUS伺服器資訊。



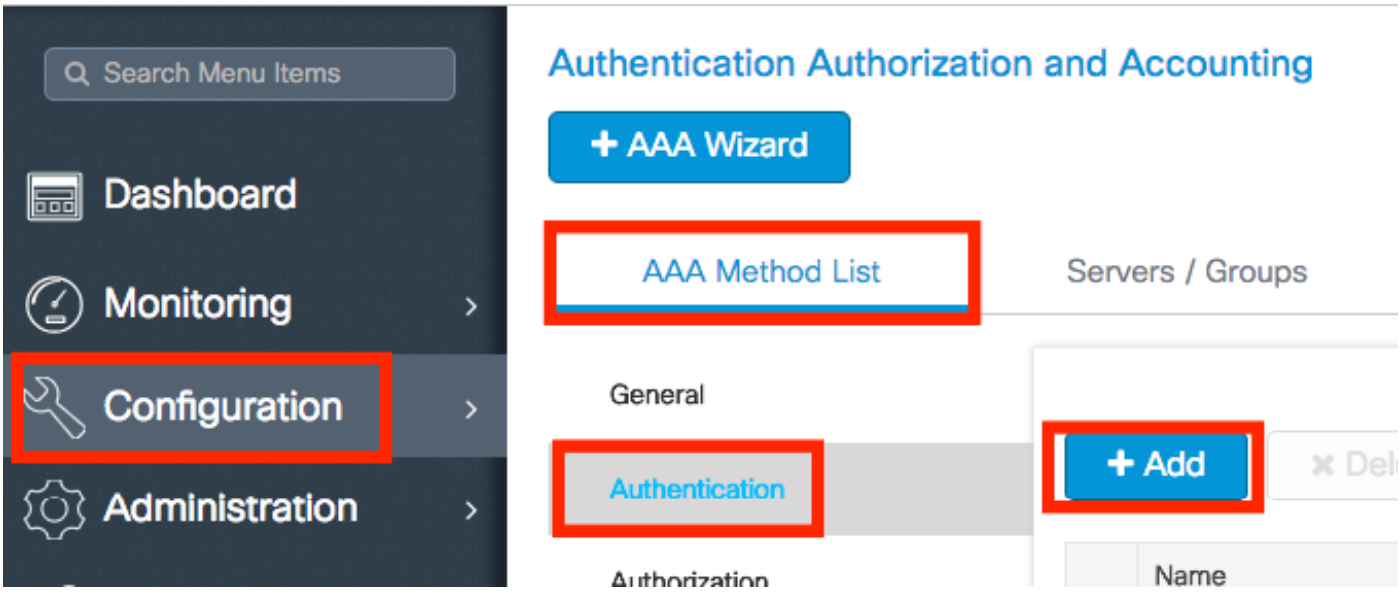
如果您計畫將來使用中央Web驗證（或任何需要授權變更[CoA]的安全型別），請確保**支援CoA**。



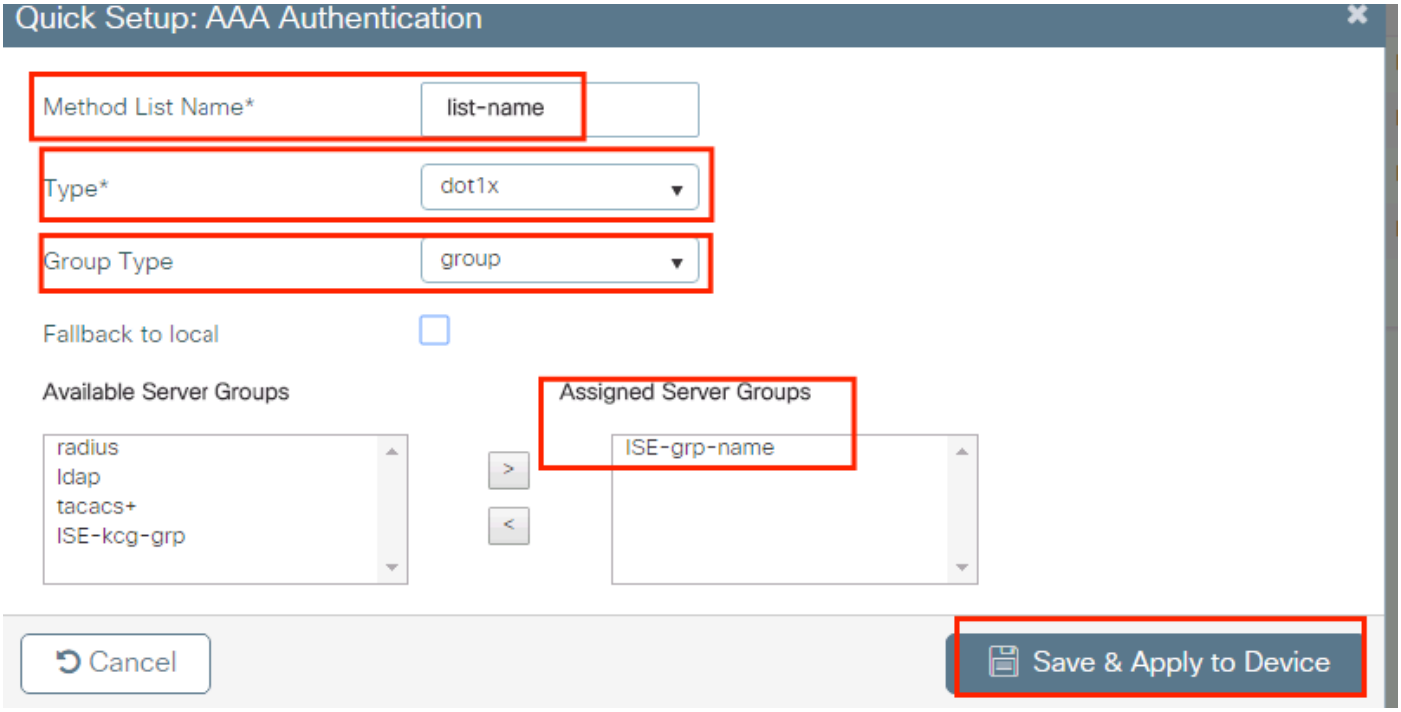
步驟2.將RADIUS伺服器新增到RADIUS組。導航至 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.** 為您的組指定一個名稱，並移動之前在清單中建立的伺服器 **Assigned Servers**.



步驟3.建立身份驗證方法清單。導航至 **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.



輸入以下資訊：



CLI:

```
# 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>
```

關於AAA失效伺服器檢測的註釋

設定RADIUS伺服器後，您就可以檢查它是否被認為是「ALIVE」：

```
#show aaa servers | s WNCD Platform State from WNCD (1) : current UP Platform State from WNCD
(2) : current UP Platform State from WNCD (3) : current UP Platform State from WNCD (4) :
current UP ...
```

您可以配置 **dead criteria**, 以及 **deadtime** 多台RADIUS伺服器時，尤應如此。

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

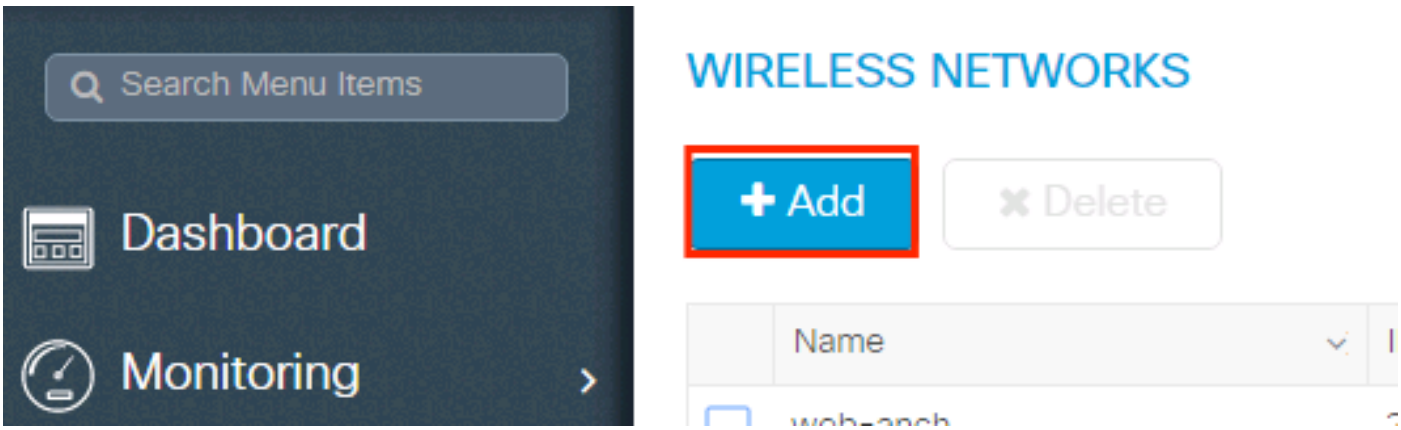
> **註**: **dead criteria** 是用來標籤RADIUS伺服器為宕機的條件。它包括：1.超時（以秒為單位），表示從控制器上次從RADIUS伺服器收到有效封包時間起至伺服器標籤為停用的時間長度。2.一個計數器，表示RADIUS伺服器標籤為失效之前，控制器上必須發生的連續超時數。

註: **deadtime** 指定在死條件將其標籤為死後，伺服器保持死狀態的時間（以分鐘為單位）。一旦死區期滿，控制器會將伺服器標籤為UP(ALIVE)，並通知已註冊的客戶端狀態變化。如果在狀態標籤為UP後伺服器仍然無法訪問，並且滿足dead條件，則在死時間間隔內，伺服器將再次標籤為dead。

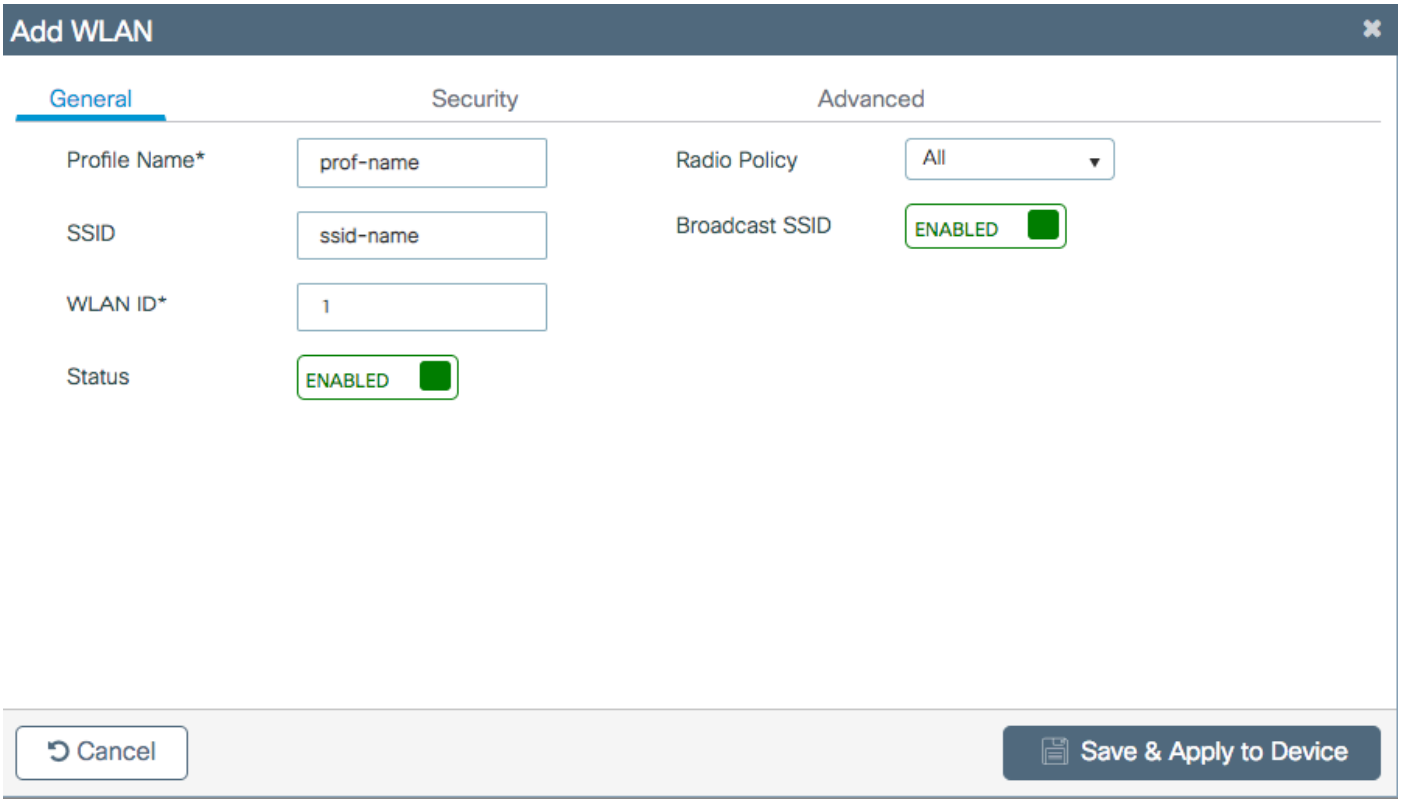
WLAN配置檔案配置

GUI:

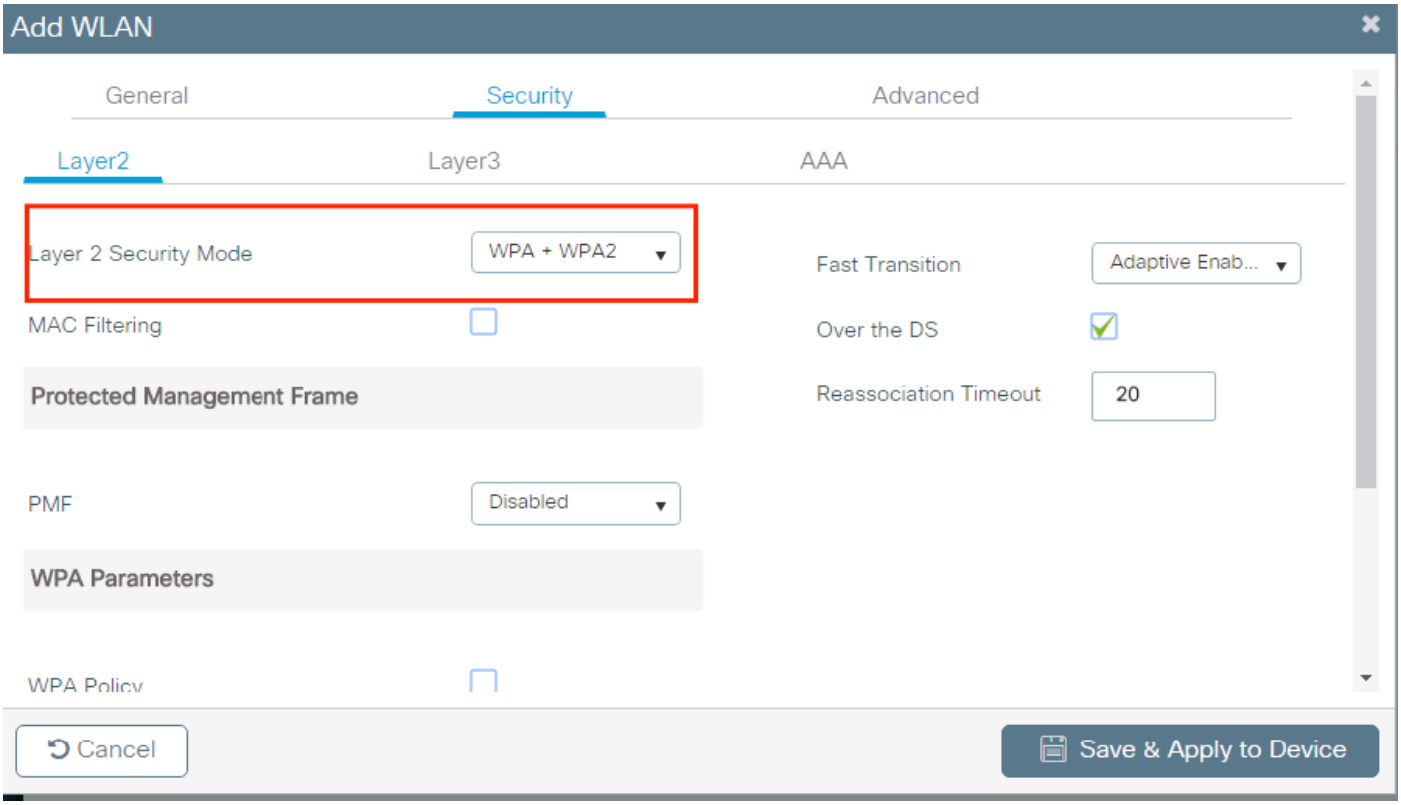
步驟1.建立WLAN。導覽至**Configuration > Wireless > WLANs > + Add**，然後根據需要配置網路。

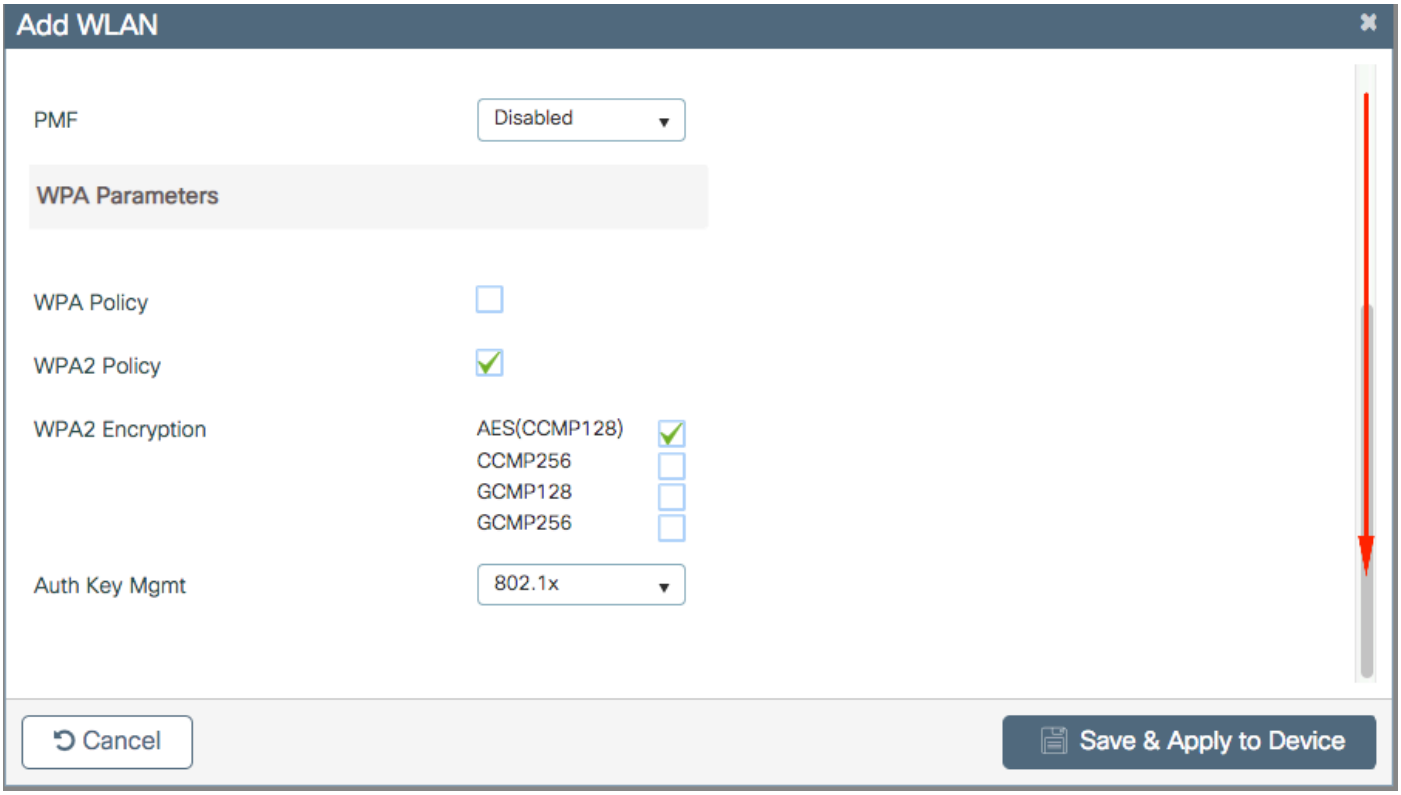


步驟2.輸入無線區域網資訊

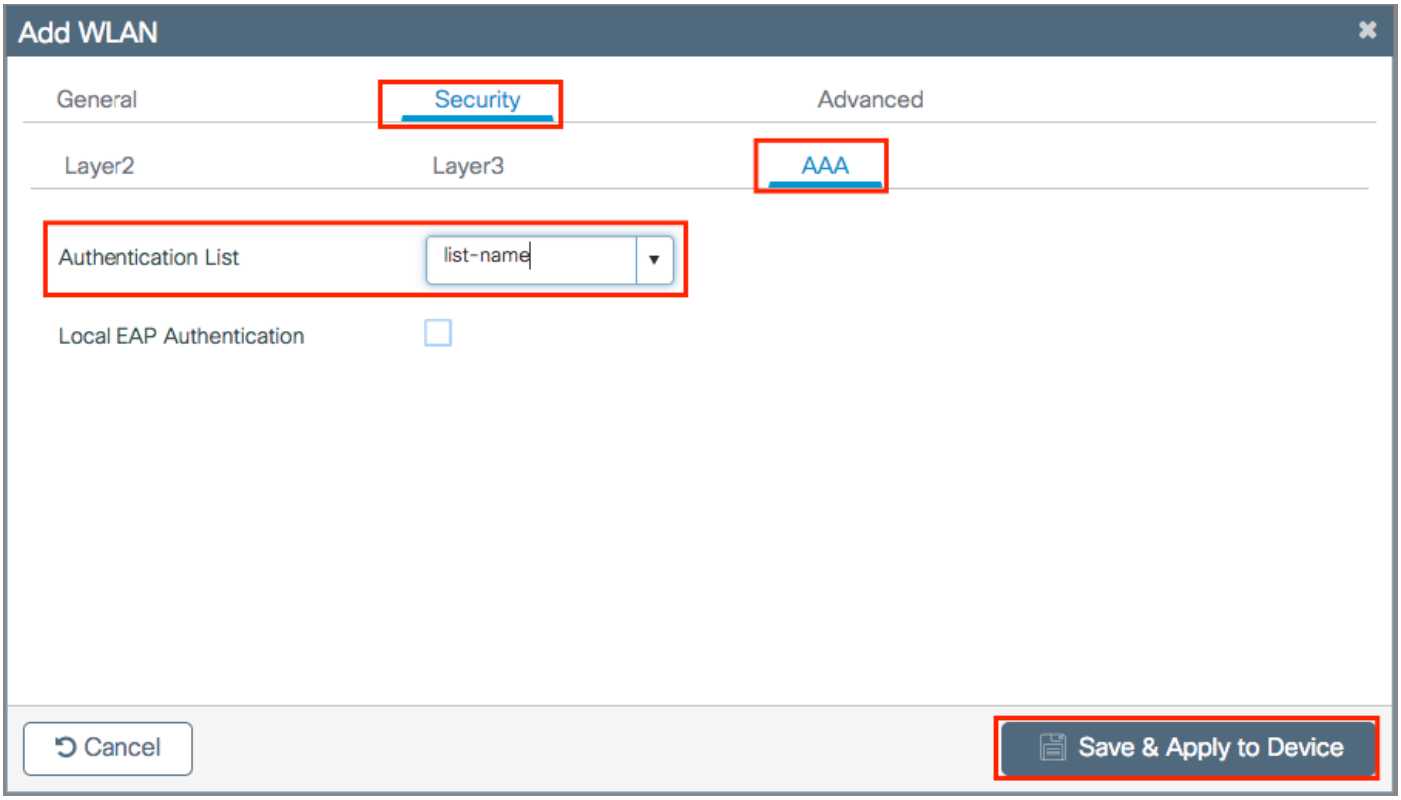


步驟3.導航至 **Security選**項卡，並選擇所需的安全方法。在本例中**WPA2 + 802.1x**。





步驟4.從 **Security > AAA** 頁籤中，從9800 WLC上的AAA配置部分選擇在步驟3中建立的身份驗證方法。



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

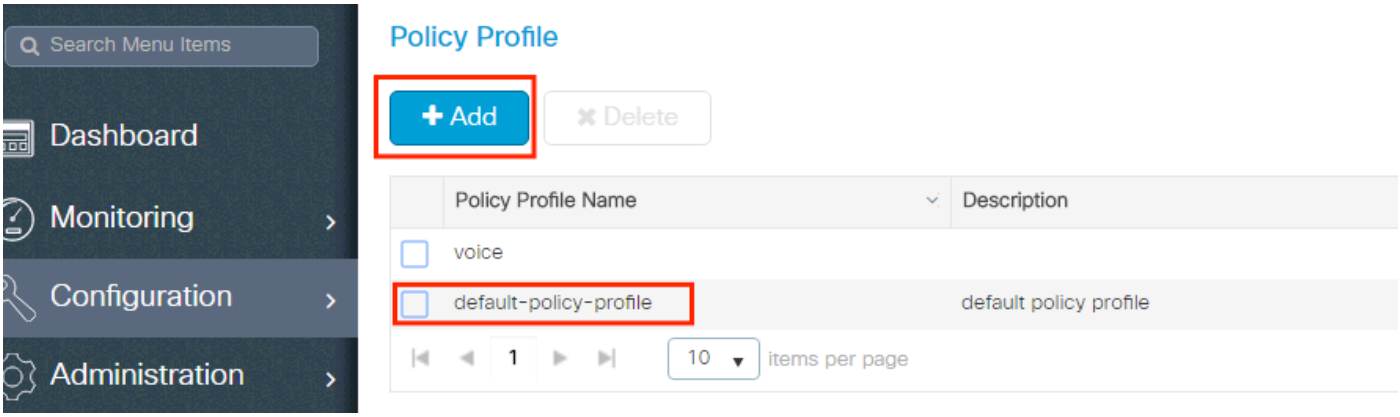
原則設定檔組態

在策略配置檔案中，您可以決定要將客戶端分配到哪個VLAN，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）。

您可以使用預設策略配置檔案，也可以建立新配置檔案。

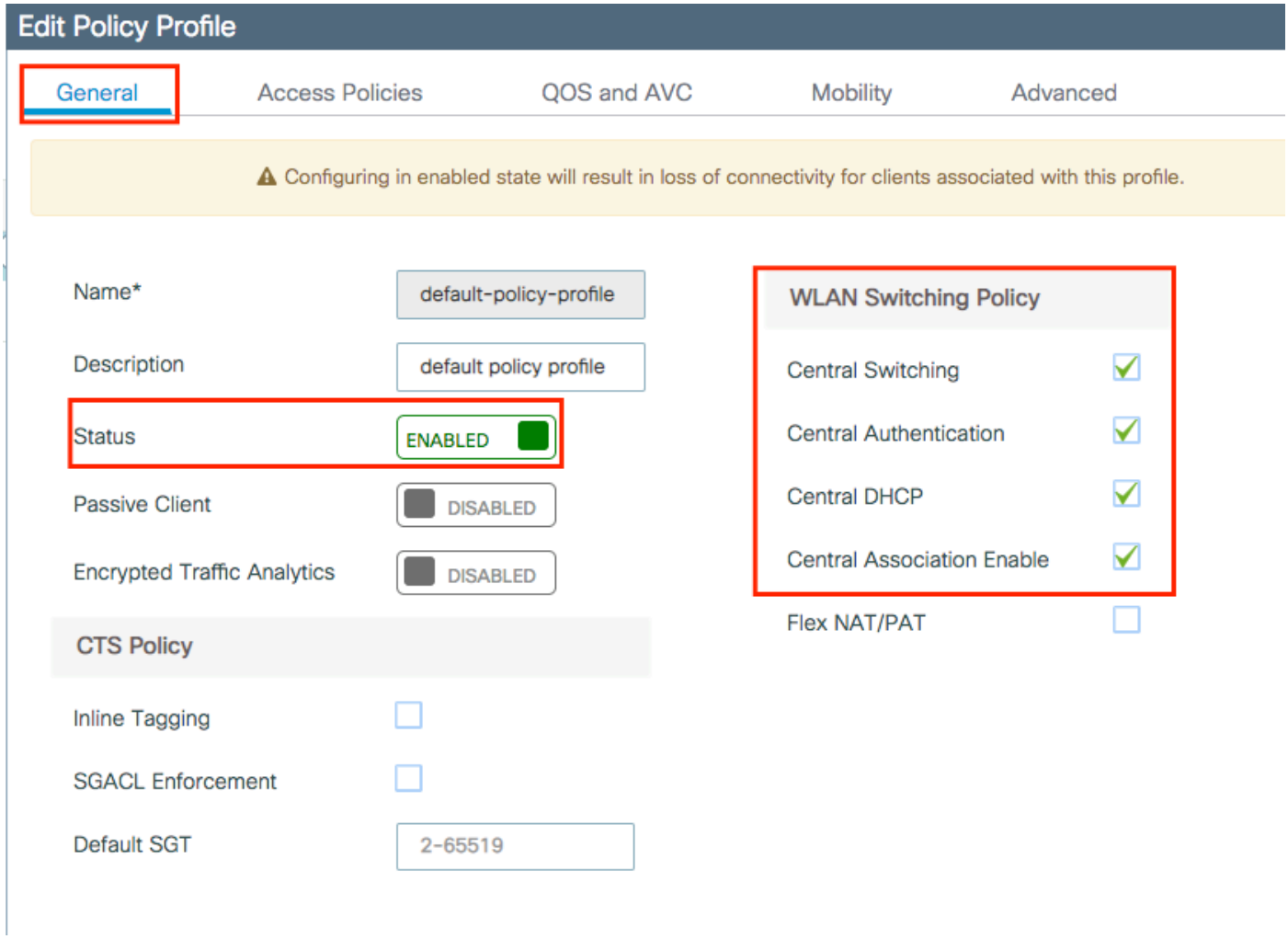
GUI:

導覽至Configuration > Tags & Profiles > Policy Profile ，然後設定default-policy-profile 或建立一個新配置檔案。

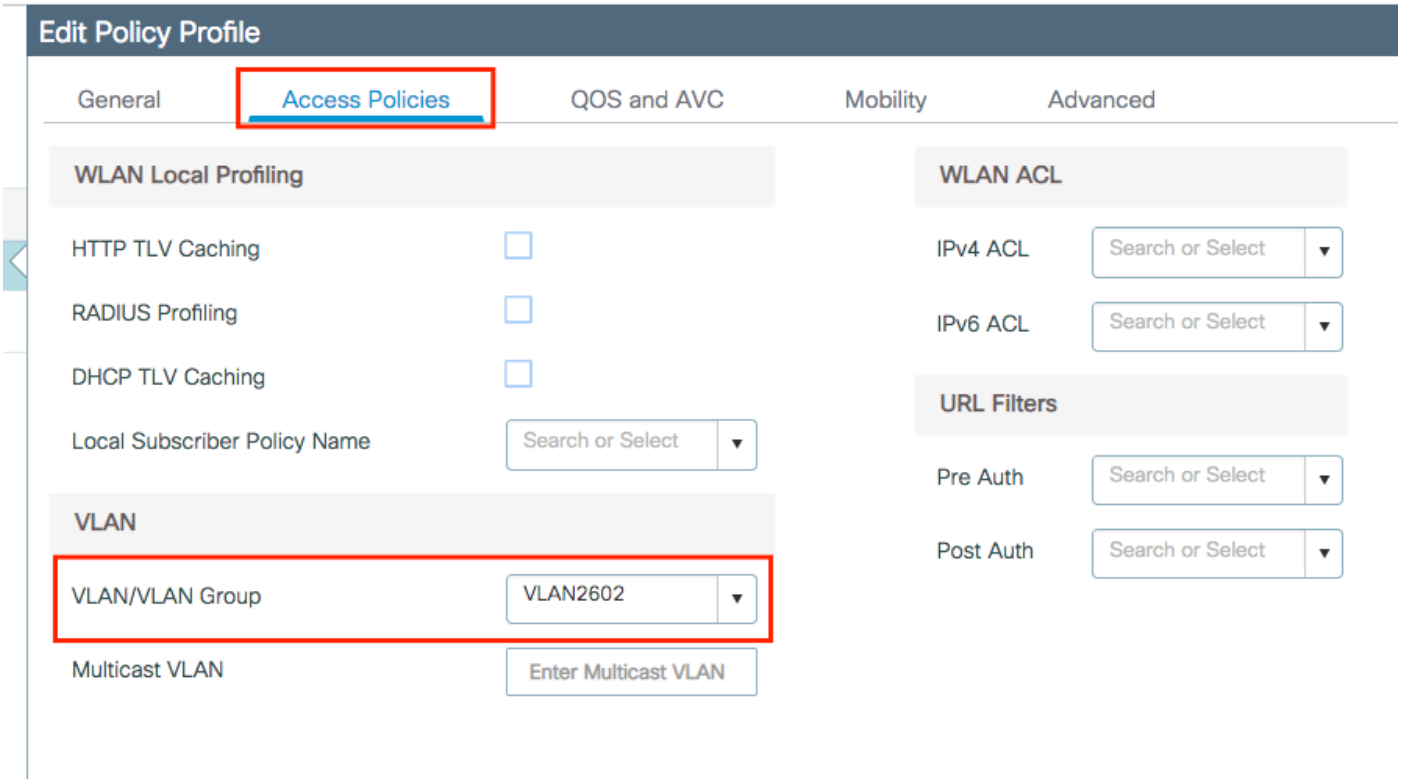


確認設定檔已啟用。

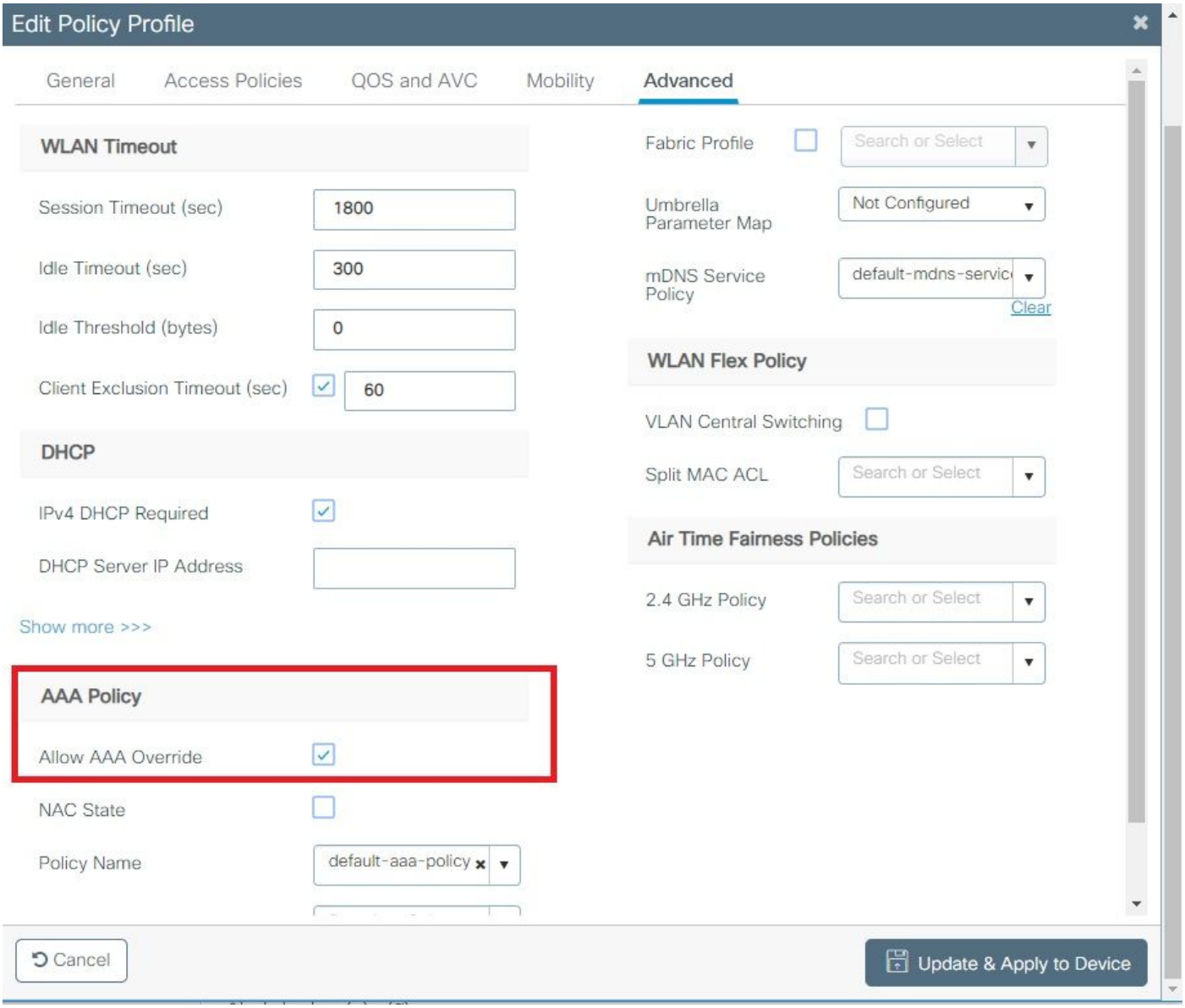
此外，如果您的存取點(AP)處於本機模式，請確保原則設定檔已啟用**中央交換**和**中央驗證**。



在**Access Policies**頁籤中選擇需要分配客戶端的VLAN。



如果您計畫在訪問接受類似於VLAN分配中擁有ISE返回屬性，請在 **Advanced** 頁籤：



CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

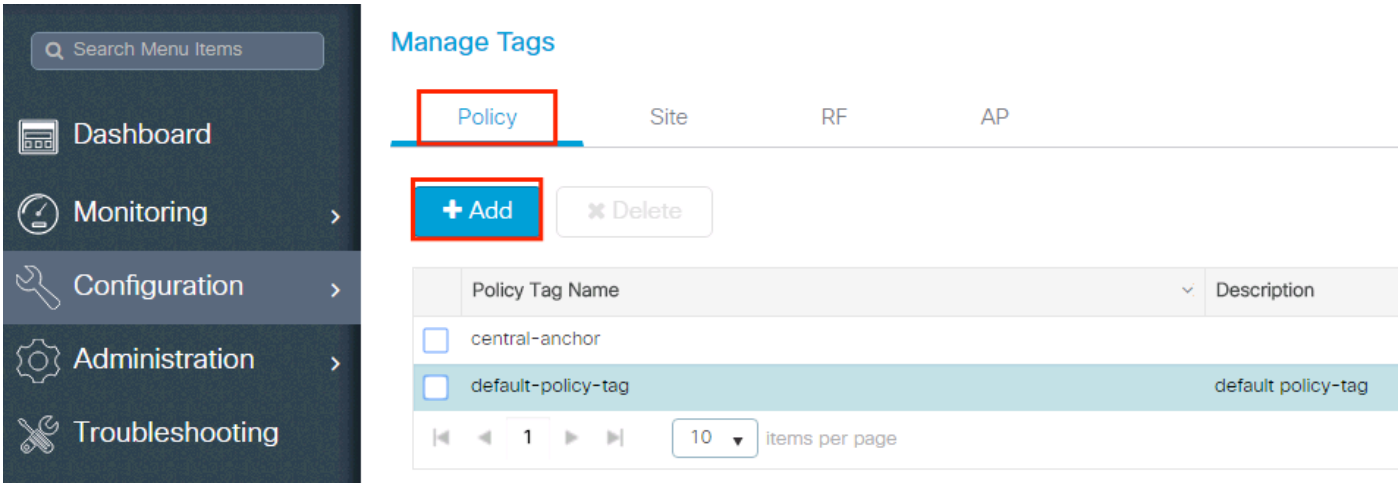
原則標籤組態

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。

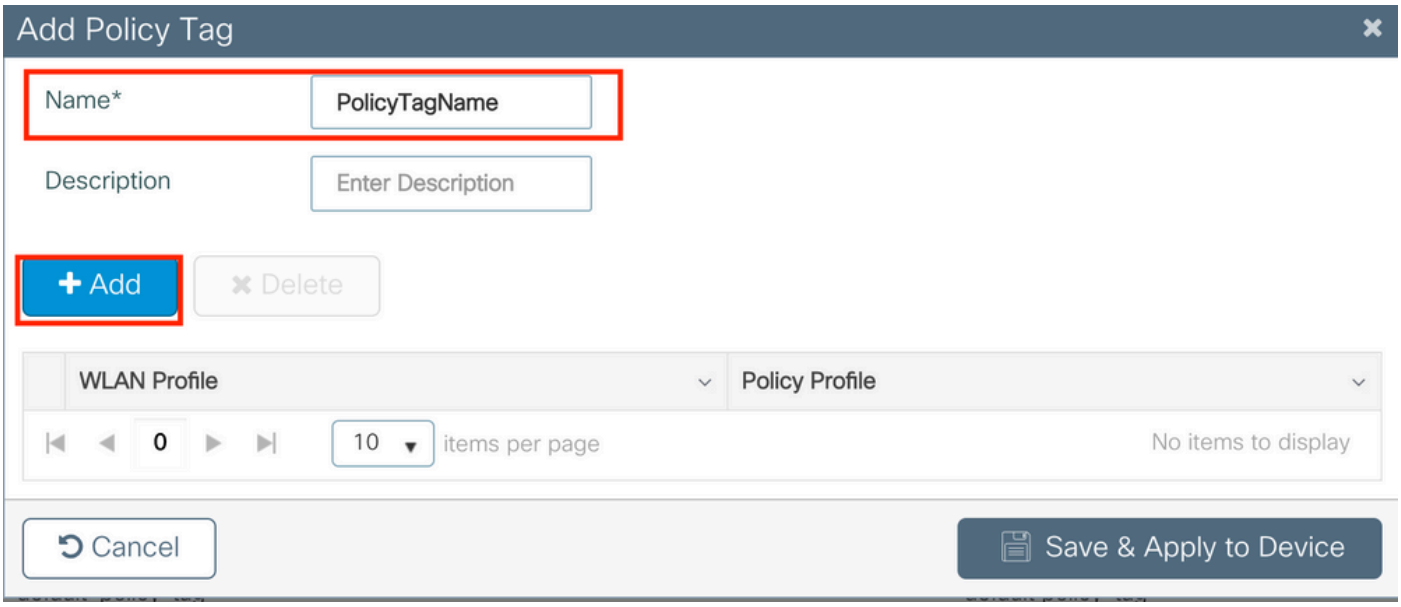
> **注意**:default-policy-tag會自動將WLAN ID介於1和16之間的所有SSID對映到default-policy-profile。不能修改或刪除。 如果您的WLAN的ID為17或更高，則不能使用default-policy-tag。

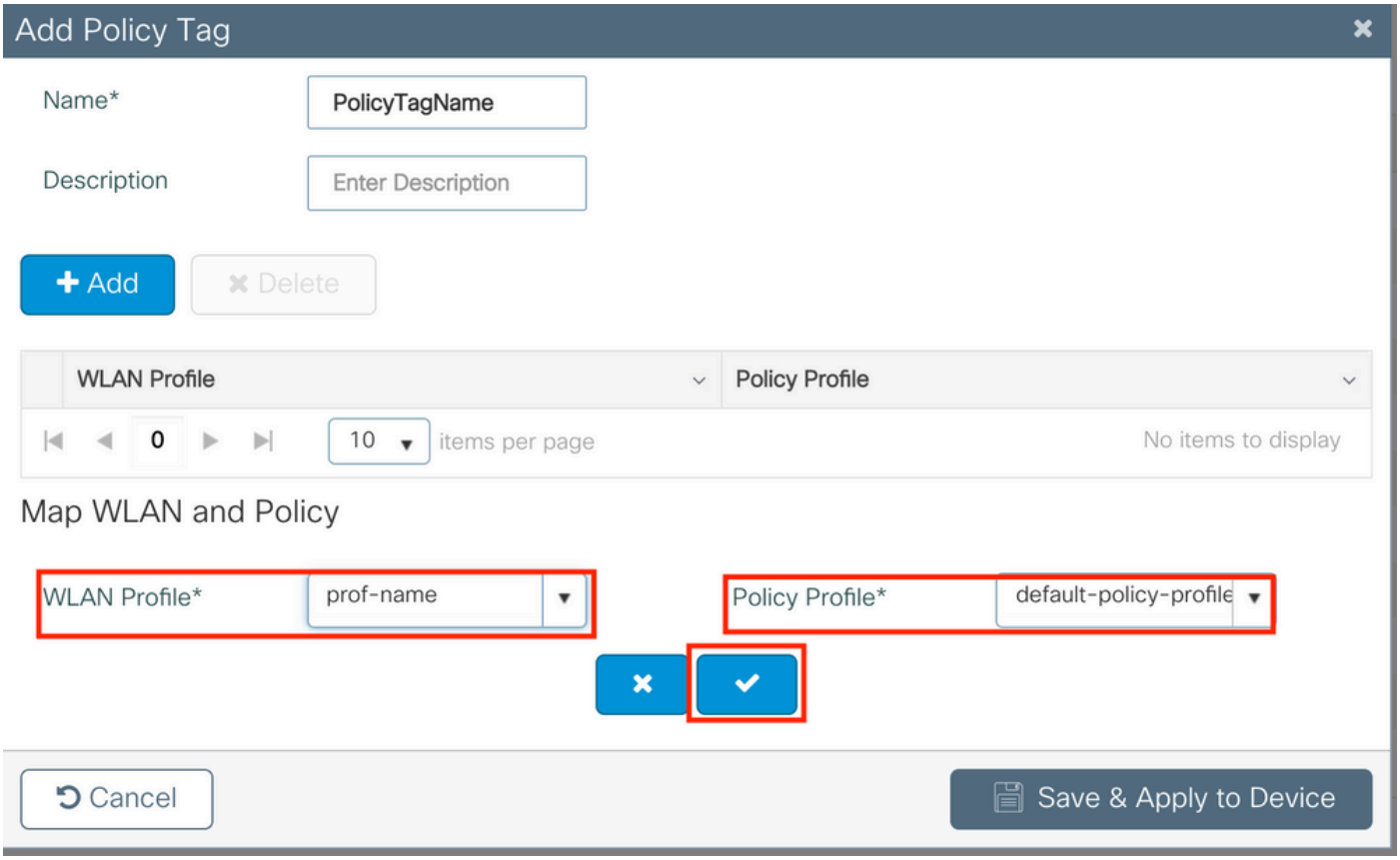
GUI:

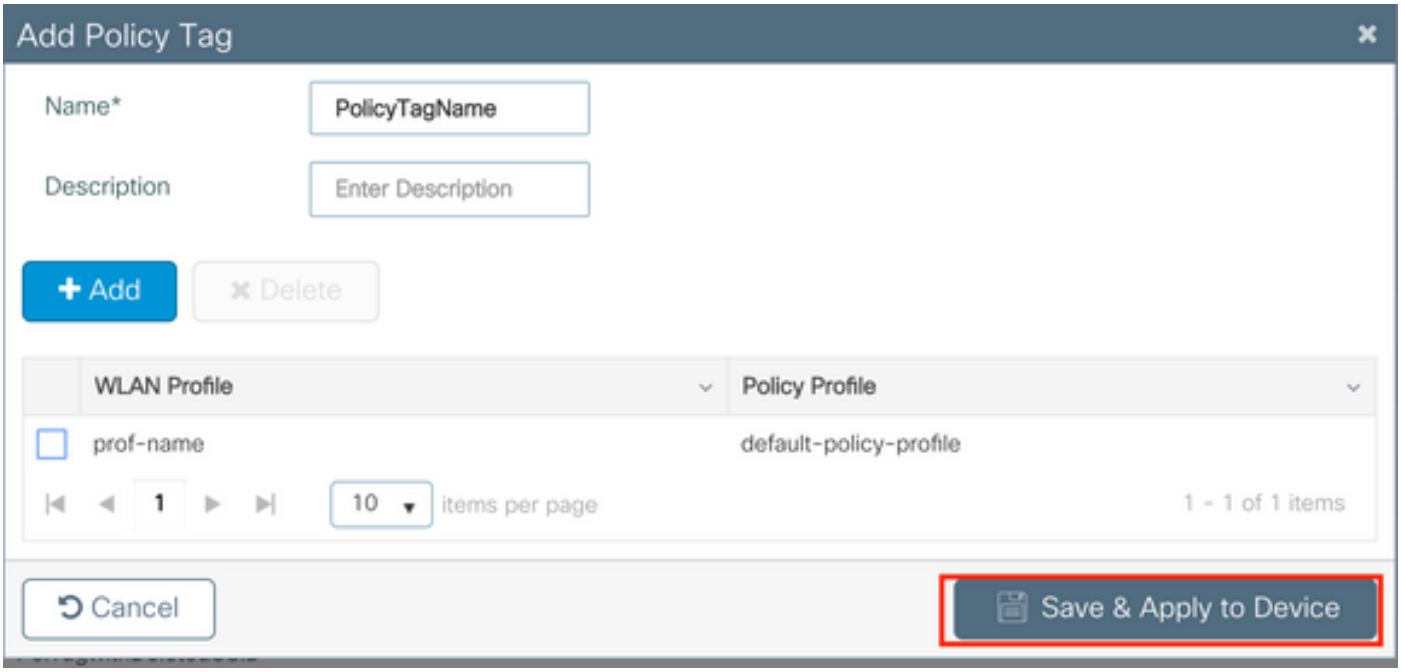
導航至 **Configugation > Tags & Profiles > Tags > Policy** 如果需要，可以新增新的。



將 WLAN 設定檔連結至想要的原則設定檔。







CLI:

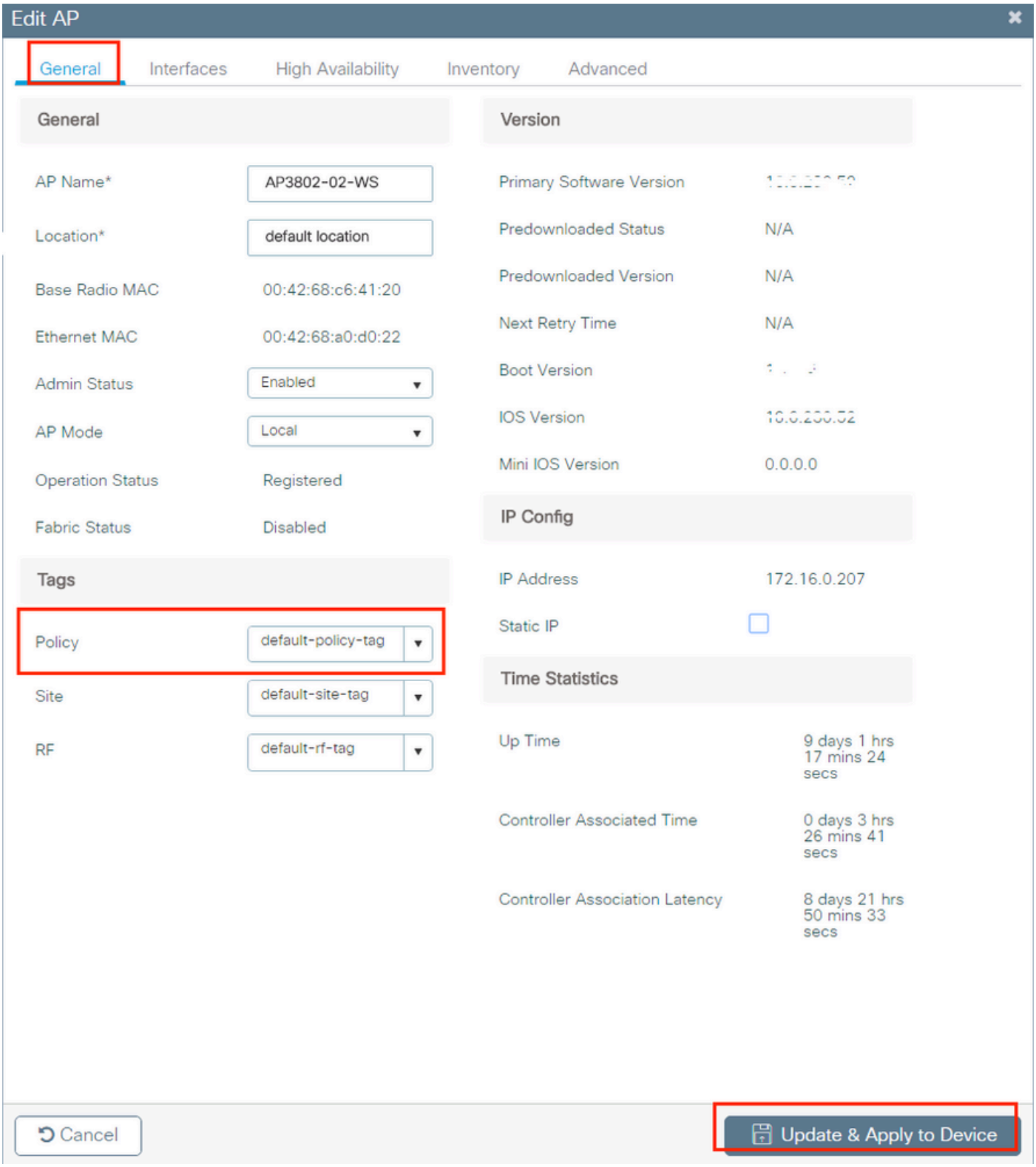
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

策略標籤分配

指派原則標籤至需要的 AP。

GUI:

要將標籤分配給一個AP，請導航至 **Configuration > Wireless > Access Points > AP Name > General Tags**，分配相關的策略標籤，然後按一下 **Update & Apply to Device**.



註意：請注意，當AP上的策略標籤更改時，它會丟棄與9800 WLC的關聯，並在稍後重新連線。

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

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）。