在Catalyst 9800 WLC上設定OEAP和RLAN

目錄

簡介

本檔案將說明如何在9800 WLC上設定Cisco OfficeExtend存取點(OEAP)和遠端區域網路(RLAN)。

Cisco OfficeExtend接入點(OEAP)提供從控制器到遠端位置的Cisco AP的安全通訊，從而通過網際網路將公司WLAN無縫擴展至員工住所。使用者在家庭辦公室中的體驗與在公司辦公室中的體驗完全相同。接入點和控制器之間的資料包傳輸層安全(DTLS)加密可確保所有通訊具有最高級別的安全性。

遠端LAN(RLAN)用於使用控制器驗證有線使用者端。有線使用者端成功加入控制器後，LAN連線埠會在中央或本地交換模式之間交換流量。來自有線客戶端的流量被視為無線客戶端流量。存取點(AP)中的RLAN會傳送驗證要求，以驗證有線使用者端。RLAN中有線使用者端的驗證與中央驗證無線使用者端的驗證類似。

必要條件

需求

思科建議您瞭解以下主題：

- 9800 WLC
- 對無線控制器和接入點的命令列介面(CLI)訪問

採用元件

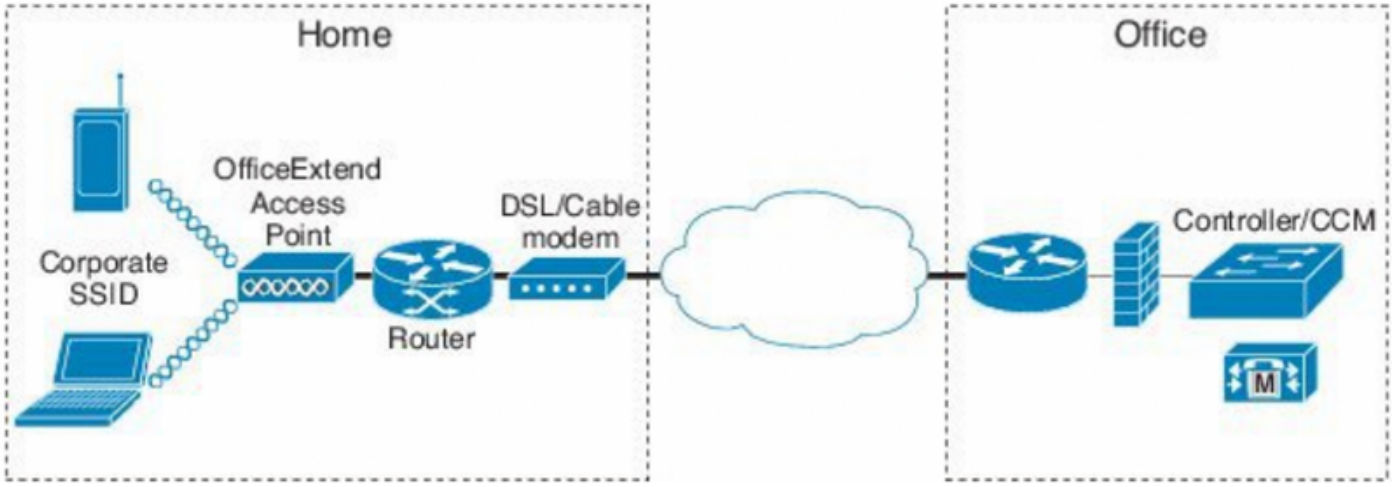
本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9800 WLC版本17.02.01
- 1815/1810系列AP

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

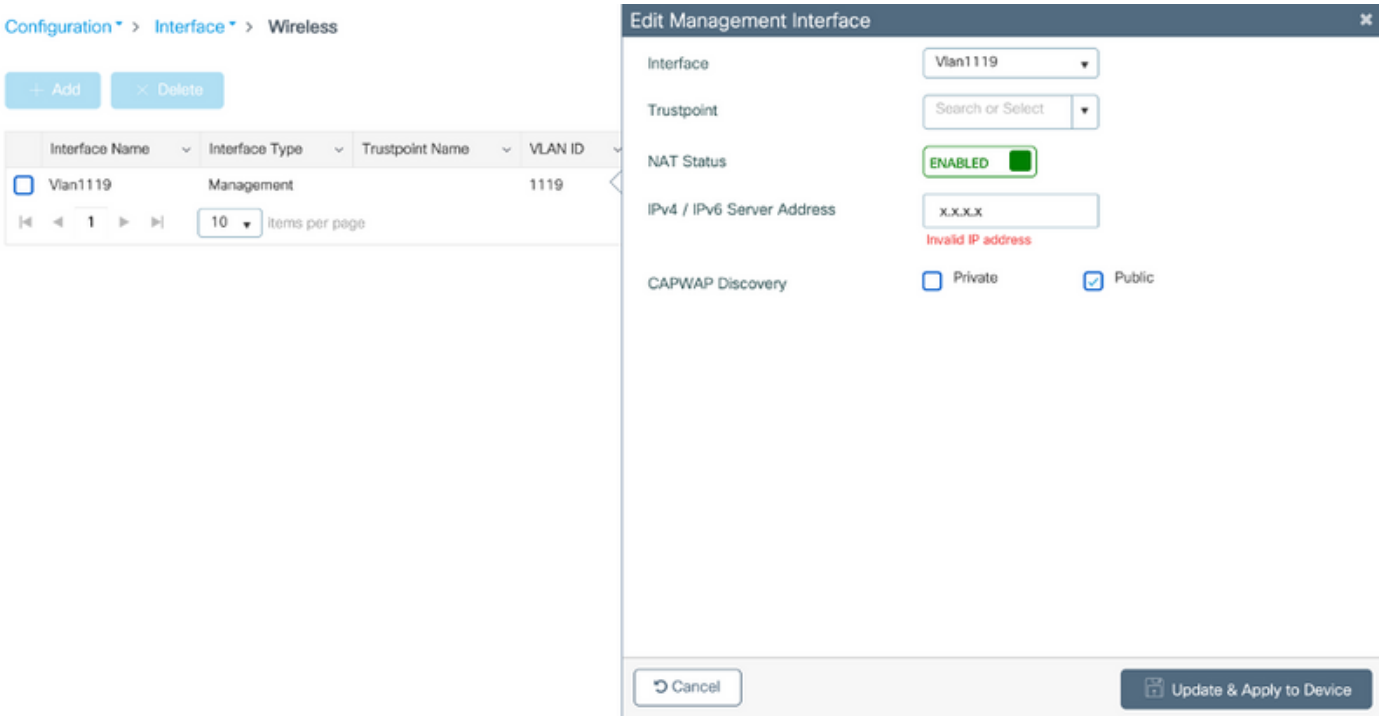


AP在NAT後加入

在16.12.x代碼中，您需要從CLI配置NAT IP地址。沒有GUI選項可用。您還可以通過公共或專用IP選擇CAPWAP發現。

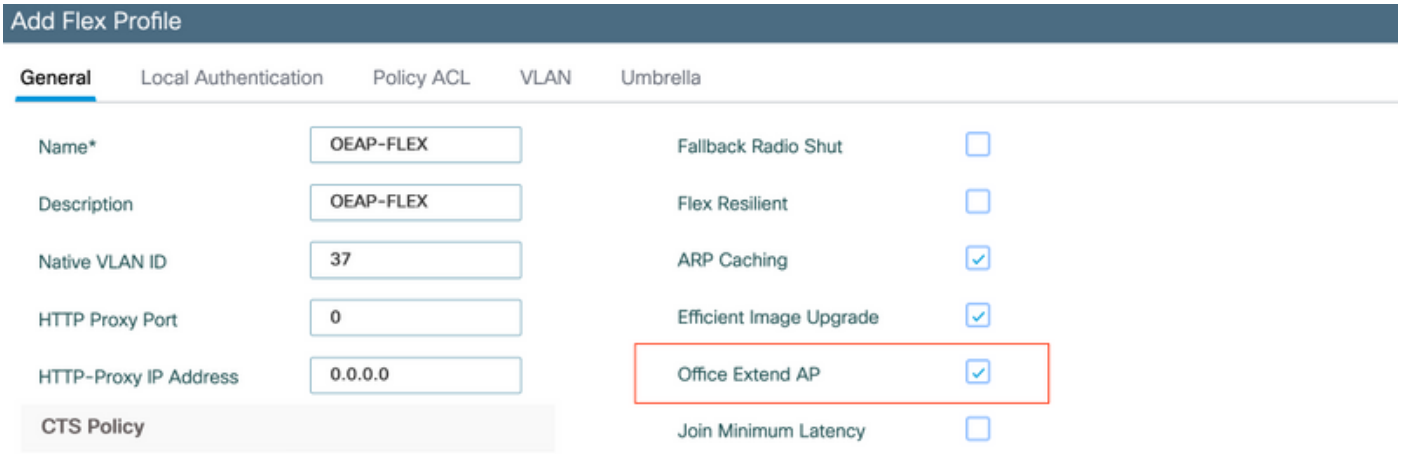
```
(config)#wireless management interface vlan 1114 nat public-ip x.x.x.x
(config-nat-interface)#capwap-discovery ?
  private  Include private IP in CAPWAP Discovery Response

  public   Include public IP in CAPWAP Discovery Response
```

在17.x代碼中，導航到**Configuration > Interface > Wireless**，然後按一下**Wireless Management Interface**，從GUI配置NAT IP和CAPWAP發現型別。

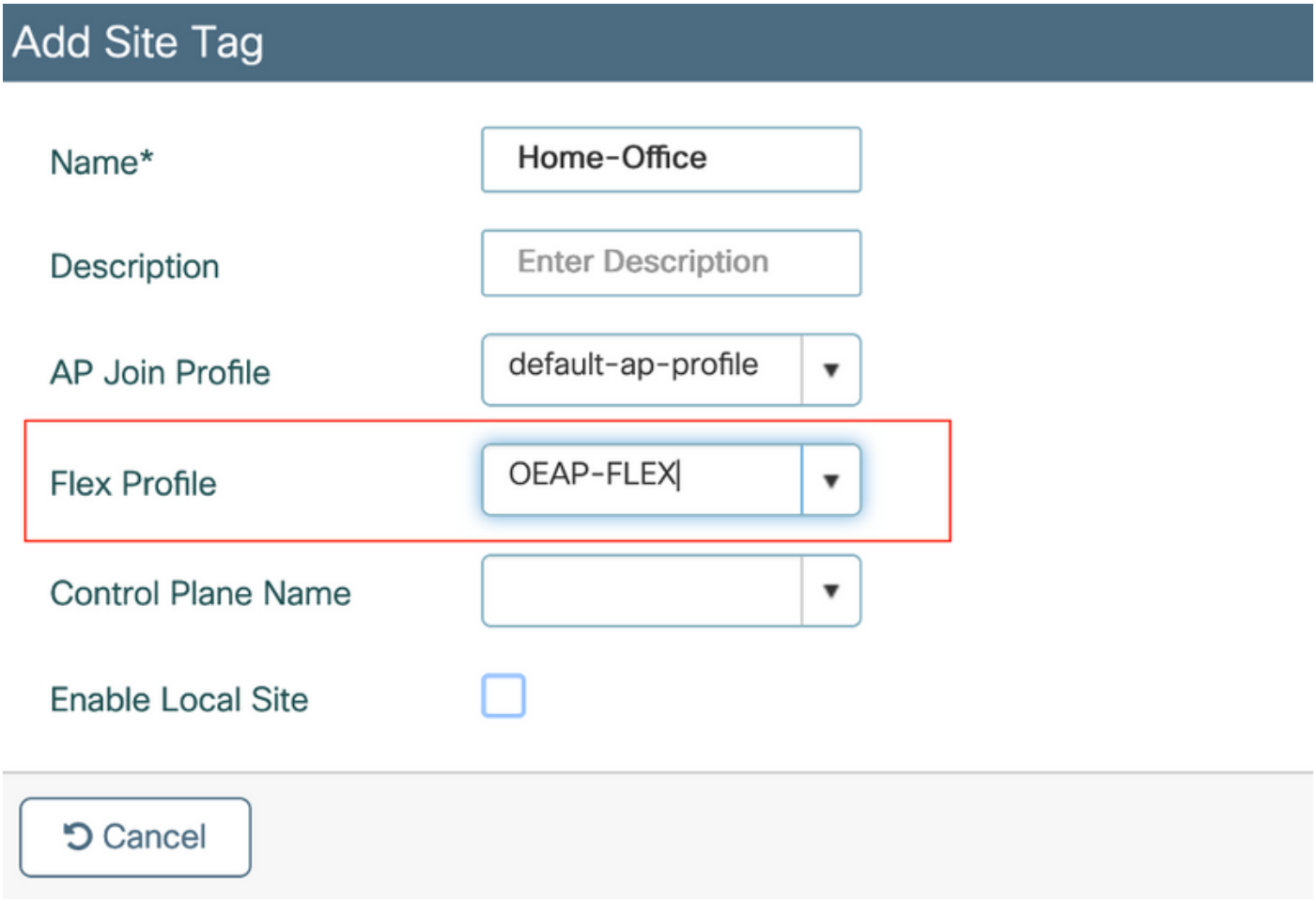


組態

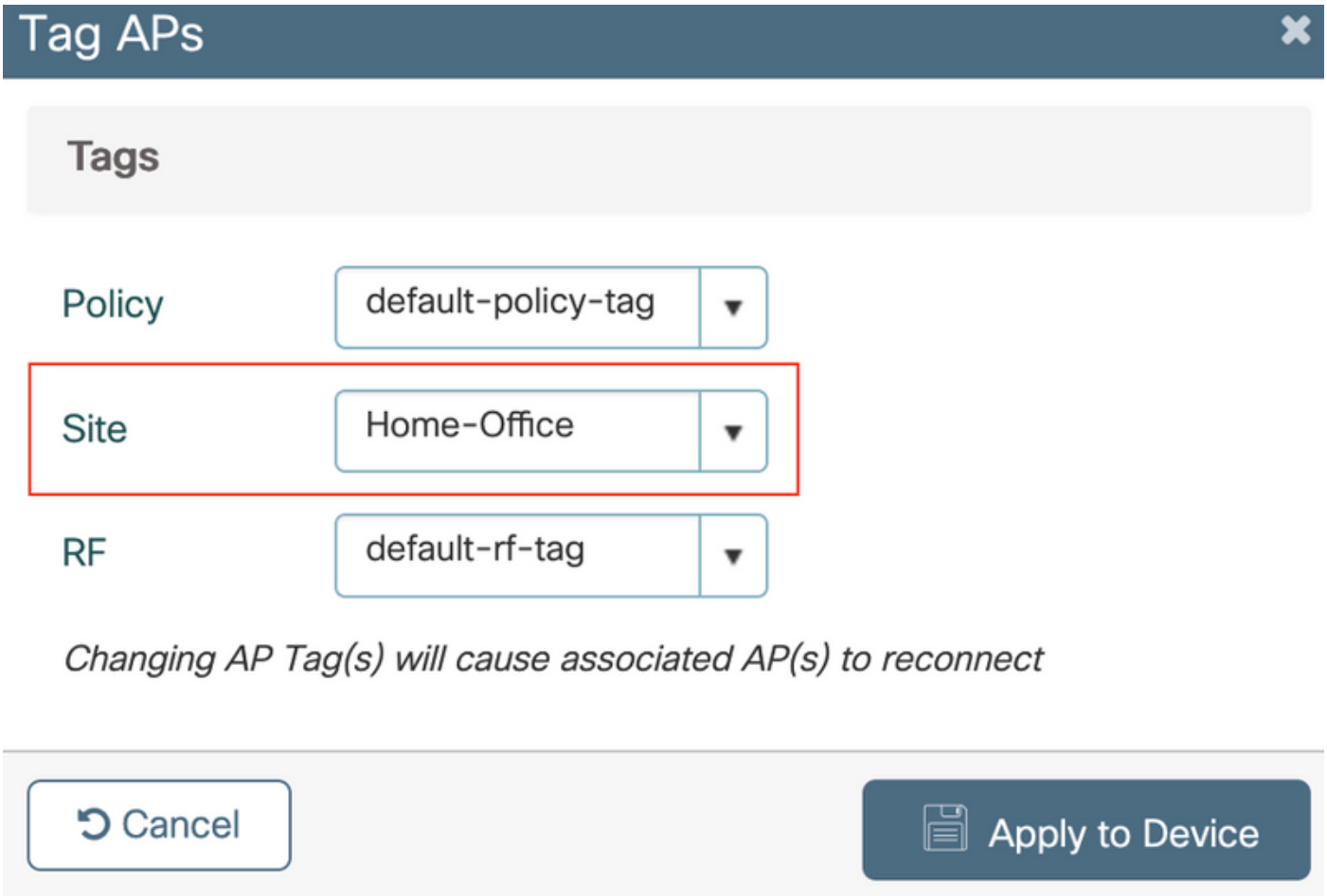
1.要建立Flex配置檔案，請啟用**Office Extend AP**，然後導航到**配置>標籤和配置檔案> Flex。**



2.要建立站點標籤和對映Flex配置檔案，請導航至**配置>標籤和配置檔案>標籤。**



3.導航到1815 AP的標籤，該標籤使用由**Configuration > Wireless Setup > Advanced > Tag AP**建立的**Site Tag**。



驗證

1815 AP重新加入WLC後，驗證以下輸出：

```
vk-9800-1#show ap name AP1815 config general

Cisco AP Name   : AP1815
================================================

Cisco AP Identifier                             : 002c.c8de.3460

Country Code                                    : Multiple Countries : IN,US

Regulatory Domain Allowed by Country            : 802.11bg:-A   802.11a:-ABDN

AP Country Code                                 : US  - United States

Site Tag Name                                   : Home-Office

RF Tag Name                                     : default-rf-tag

Policy Tag Name                                 : default-policy-tag

AP join Profile                                 : default-ap-profile

Flex Profile                                    : OEAP-FLEX

Administrative State                            : Enabled

Operation State                                 : Registered

AP Mode                                         : FlexConnect

AP VLAN tagging state                           : Disabled

AP VLAN tag                                     : 0

CAPWAP Preferred mode                           : IPv4

CAPWAP UDP-Lite                                 : Not Configured

AP Submode                                      : Not Configured

Office Extend Mode                              : Enabled

Dhcp Server                                     : Disabled

Remote AP Debug                                 : Disabled


vk-9800-1#show ap link-encryption

                           Encryption      Dnstream    Upstream     Last

AP Name                    State           Count       Count        Update

-----------------------------------------------------------------------

N2                          Disabled        0           0           06/08/20 00:47:33
```

```
AP1815                          Enabled         43          865         06/08/20 00:46:56
```

```
when you enable the OfficeExtend mode for an access point DTLS data encryption is enabled
automatically.
```

```
AP1815#show capwap client config

AdminState                          : ADMIN_ENABLED(1)

Name                                : AP1815

Location                            : default location

Primary controller name             : vk-9800-1

ssh status                          : Enabled

ApMode                              : FlexConnect

ApSubMode                           : Not Configured

Link-Encryption                     : Enabled

OfficeExtend AP                     : Enabled

Discovery Timer                     : 10

Heartbeat Timer                     : 30

Syslog server                       : 255.255.255.255

Syslog Facility                     : 0

Syslog level                        : informational
```

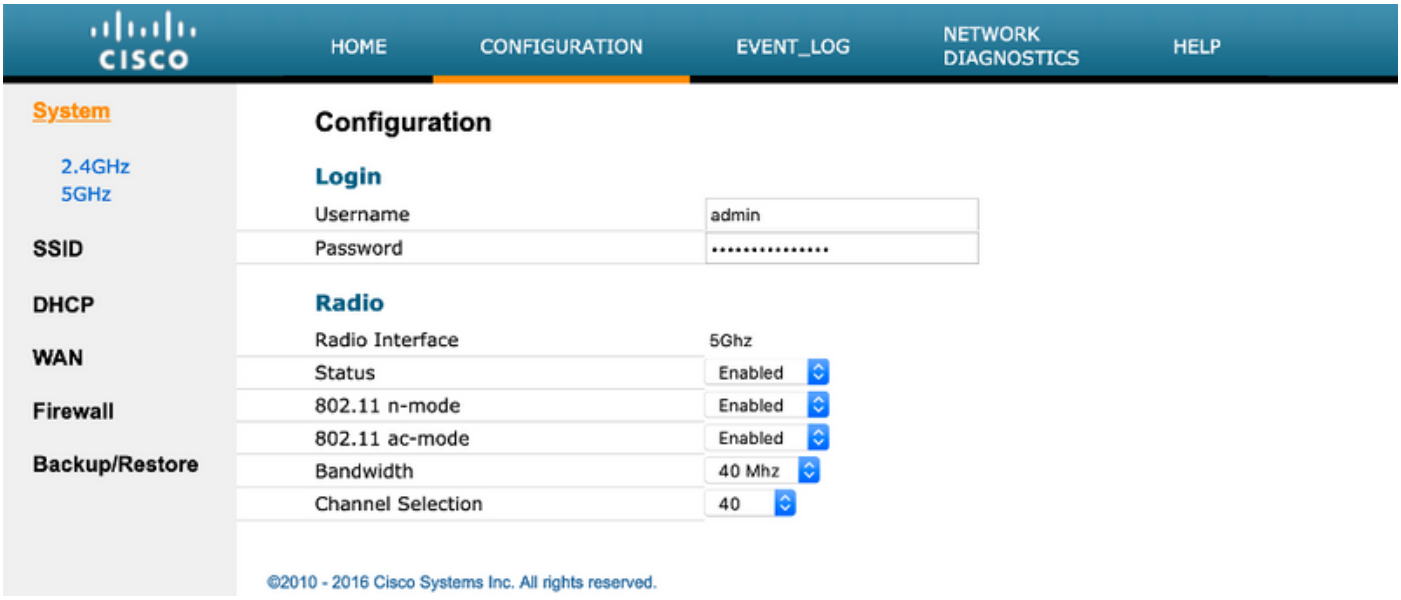
附註：您可以使用ap link-encryption命令為特定接入點或所有接入點啟用或禁用DTLS資料加密

```
vk-9800-1(config)#ap profile default-ap-profile

vk-9800-1(config-ap-profile)#no link-encryption

Disabling link-encryption globally will reboot the APs with link-encryption.

Are you sure you want to continue? (y/n)[y]:y
```

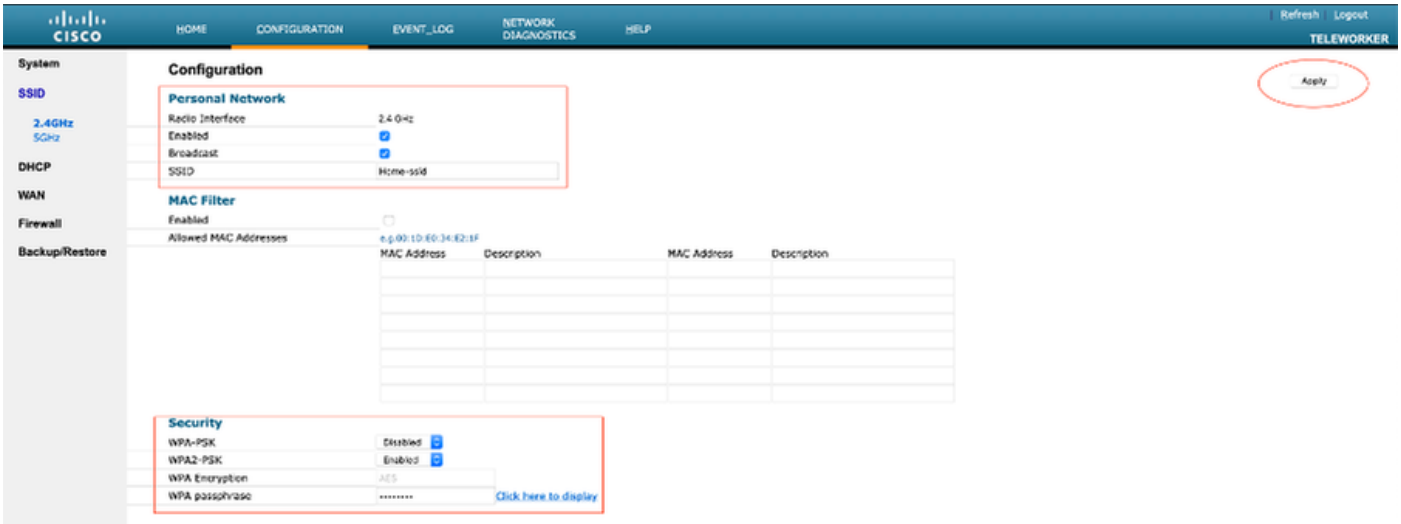
登入OEAP並配置個人SSID

1.您可以使用其IP地址訪問OEAP的Web介面。登入的預設憑據為**admin**和**admin**。

2.出於安全原因，建議更改預設憑據。



3.導航至**Configuration> SSID> 2.4GHz/5GHz**以配置個人SSID。



4.啟用無線電介面。

5.輸入SSID並啟用Broadcast

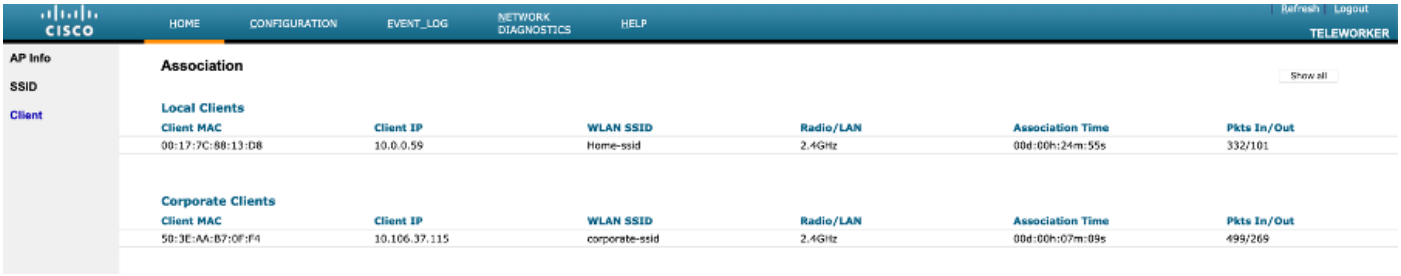
6.對於加密，請選擇**WPA-PSK**或**WPA2-PSK**，然後輸入相應安全型別的密碼。

7.按一下「應用」以使設定生效。

8.預設情況下，連線到個人SSID的客戶端會從10.0.0.1/24網路獲取IP地址。

9.家庭使用者可以使用同一個AP連線家庭，並且流量不會通過DTLS隧道傳遞。

10.要檢查OEAP上的客戶端關聯，請導航到**Home > Client**。您可以看到與OEAP關聯的本地客戶端和企業客戶端。




```
To clear personal ssidfrom office-extend ap

ewlc#ap name cisco-ap clear-personalssid-config

clear-personalssid-config Clears the Personal SSID config on an OfficeExtend AP
```

在9800 WLC上設定RLAN

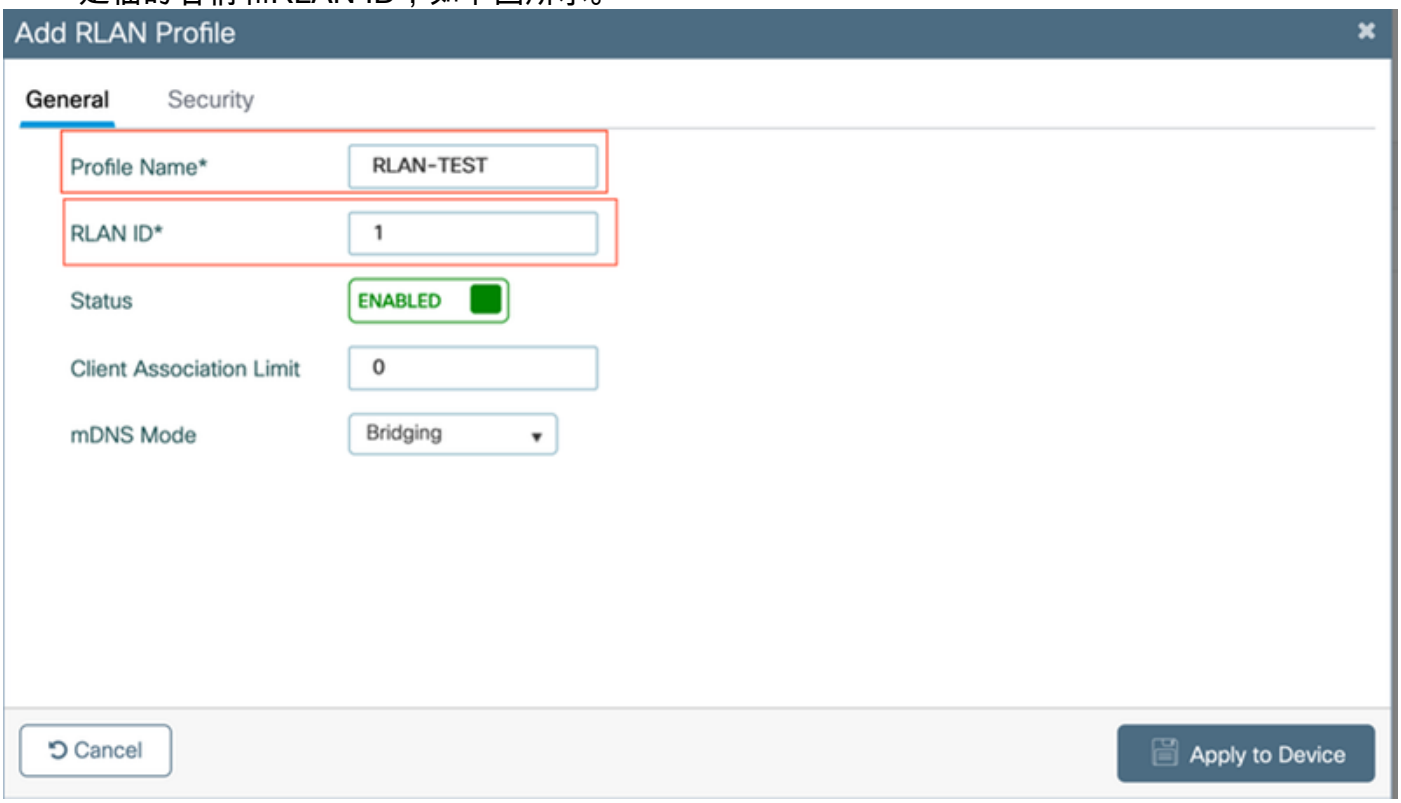
遠端LAN(RLAN)用於使用控制器驗證有線使用者端。有線使用者端成功加入控制器後，LAN連線埠會在中央或本地交換模式之間交換流量。來自有線客戶端的流量被視為無線客戶端流量。存取點(AP)中的RLAN會傳送驗證要求，以驗證有線使用者端。其

RLAN中有線使用者端的驗證與中央驗證無線使用者端的驗證類似。

> **附註**：在本示例中，本地EAP用於RLAN客戶端身份驗證。WLC上必須存在本地EAP配置才能配置以下步驟。它包括aaa身份驗證和授權方法、本地EAP配置檔案和本地憑證。

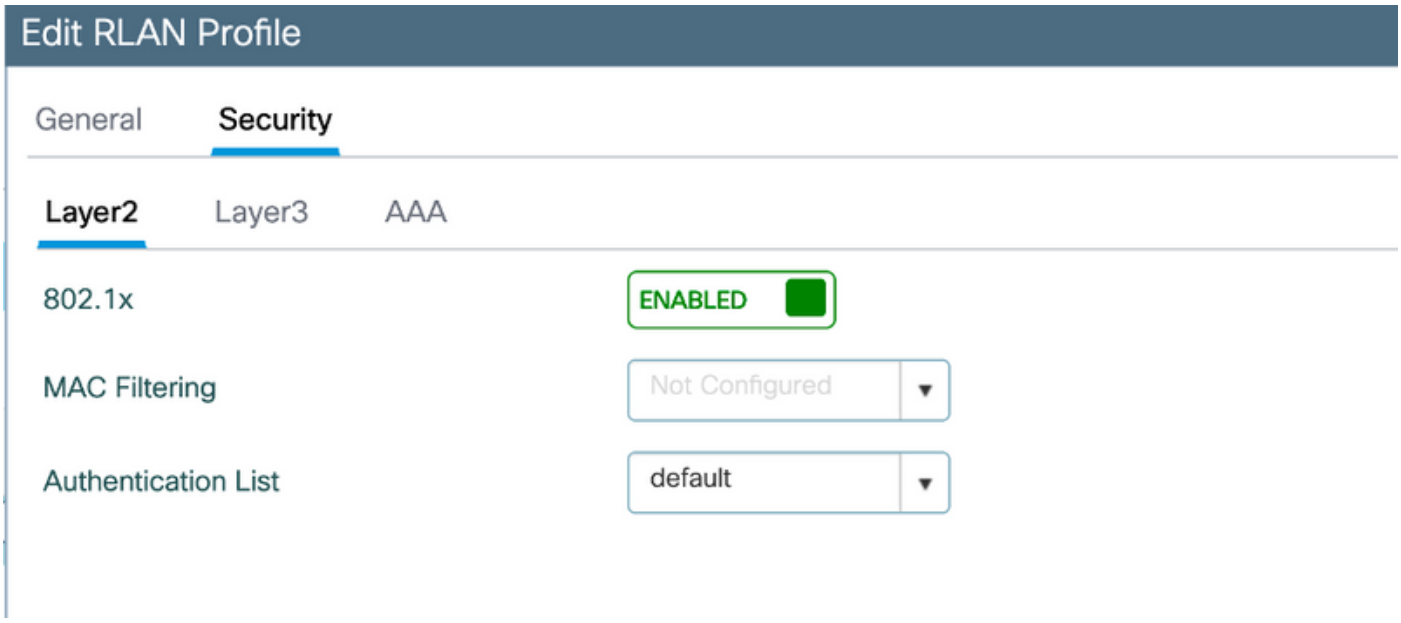
[Catalyst 9800 WLC上的本地EAP驗證組態範例]

1. 若要建立RLAN設定檔，請導覽至**Configuration > Wireless > Remote LAN**，然後輸入RLAN設定檔的名稱和RLAN ID，如下圖所示。

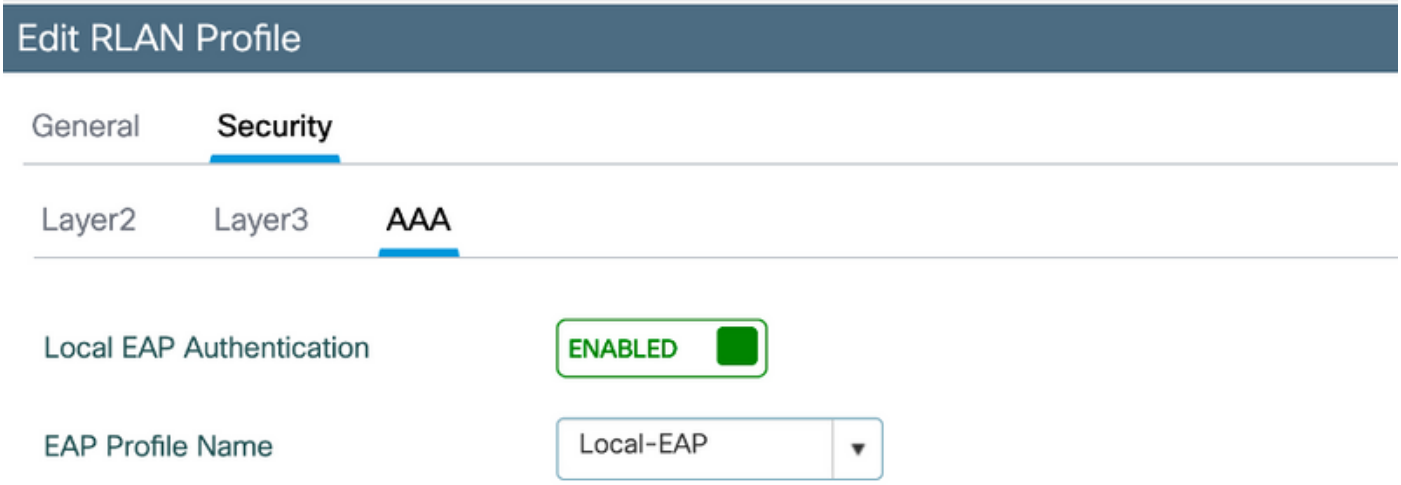


2.導覽至**Security > Layer2**，若要為RLAN啟用802.1x，請將802.1x狀態設定為Enabled，如下圖所

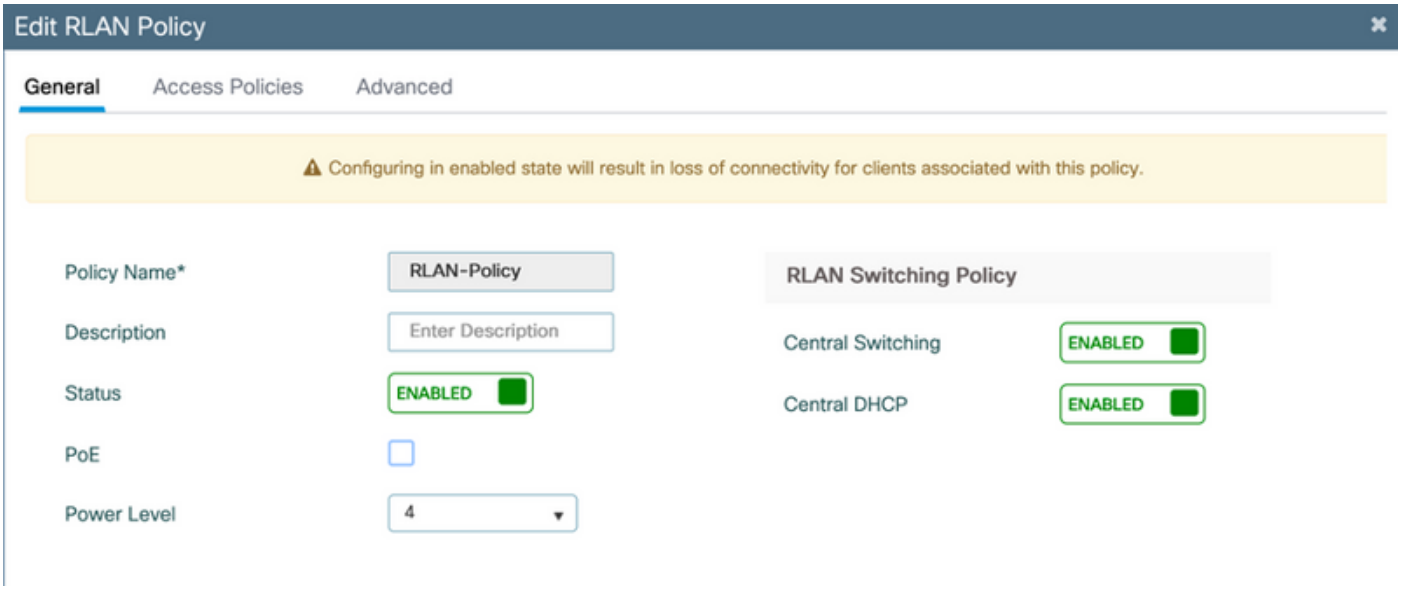
示。



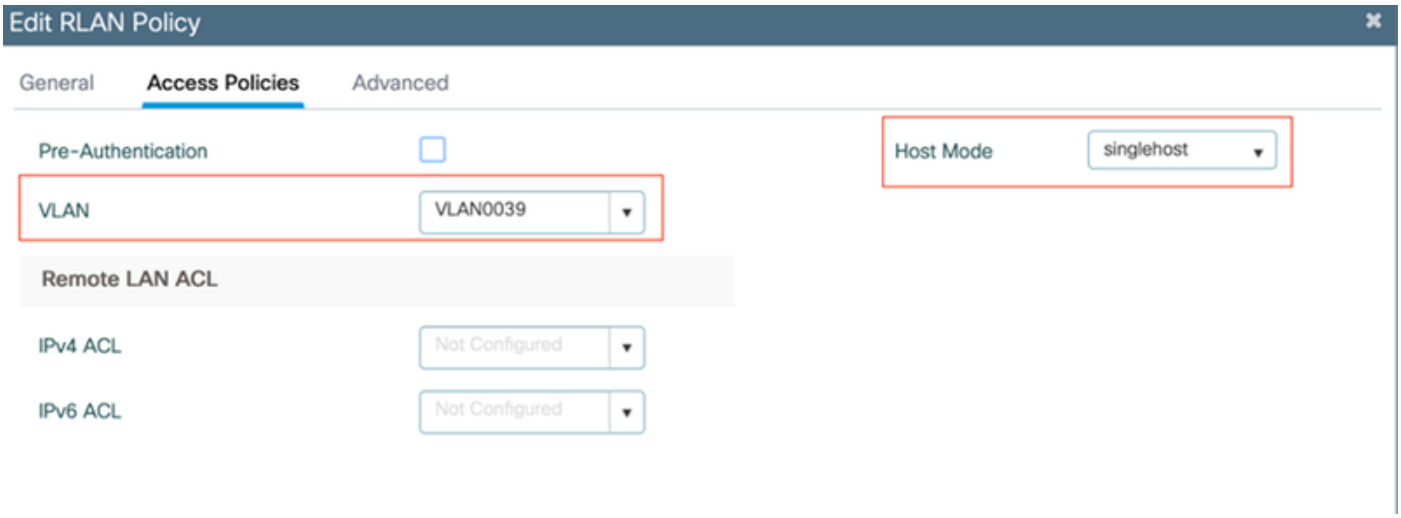
3.導航到**Security > AAA**，將Local EAP Authentication設定為enabled，然後從下拉選單中選擇所需的EAP配置檔名稱，如下圖所示。



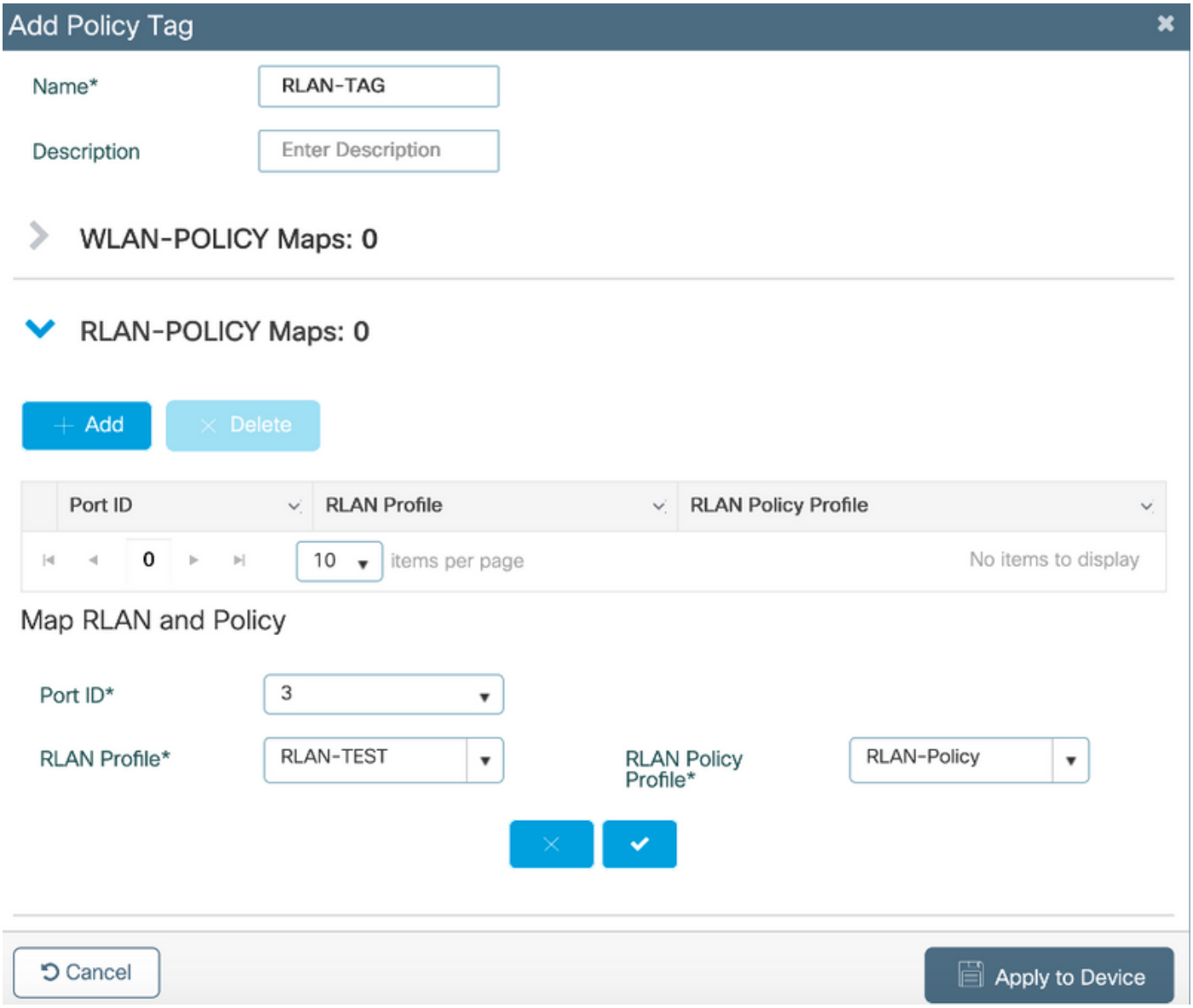
4.若要建立RLAN原則，請導覽至**Configuration > Wireless > Remote LAN**，然後在「Remote LAN」頁面上按一下**RLAN Policy**標籤，如下圖所示。

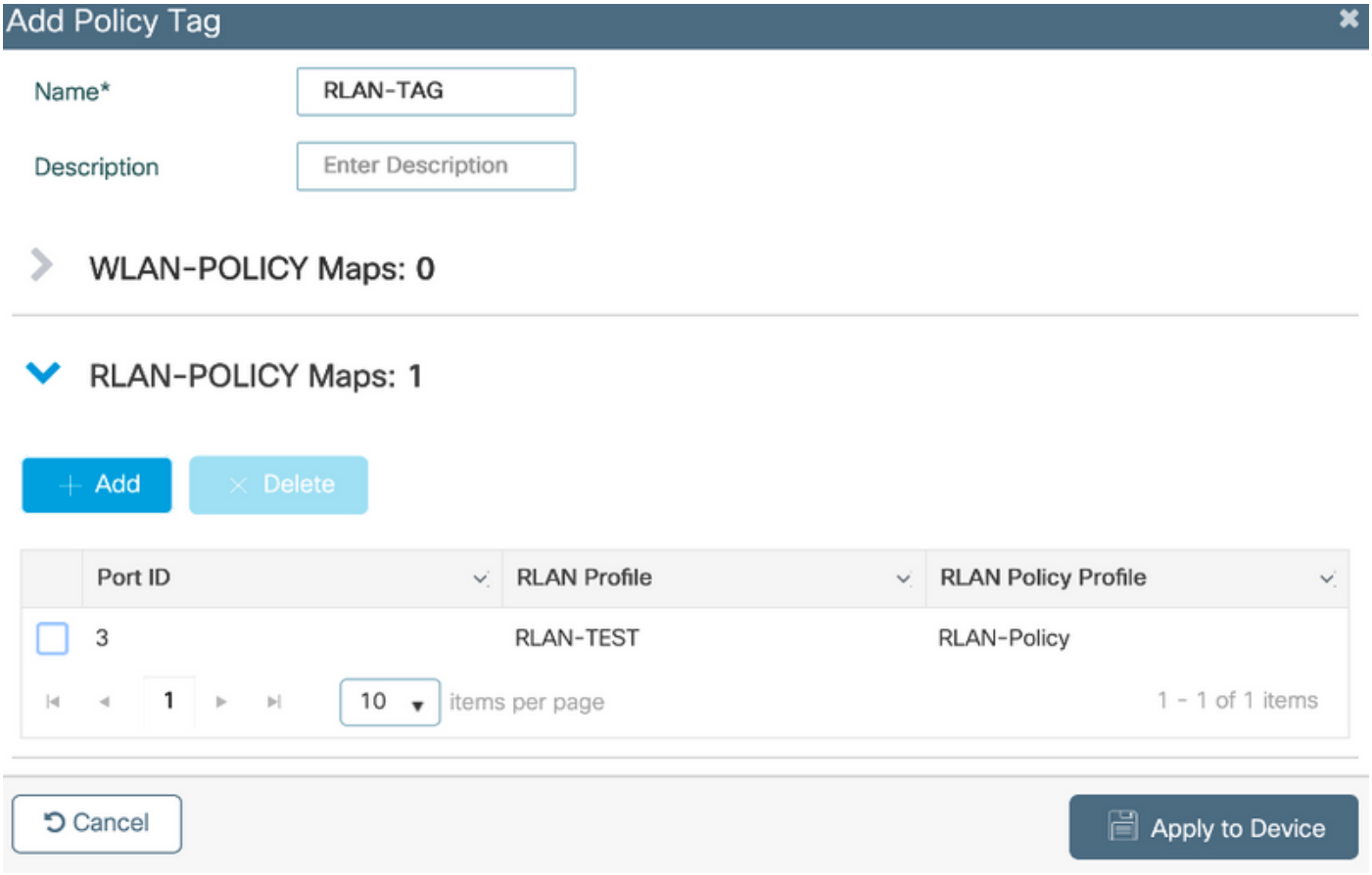


導航到訪問策略，配置VLAN和主機模式並應用設定。

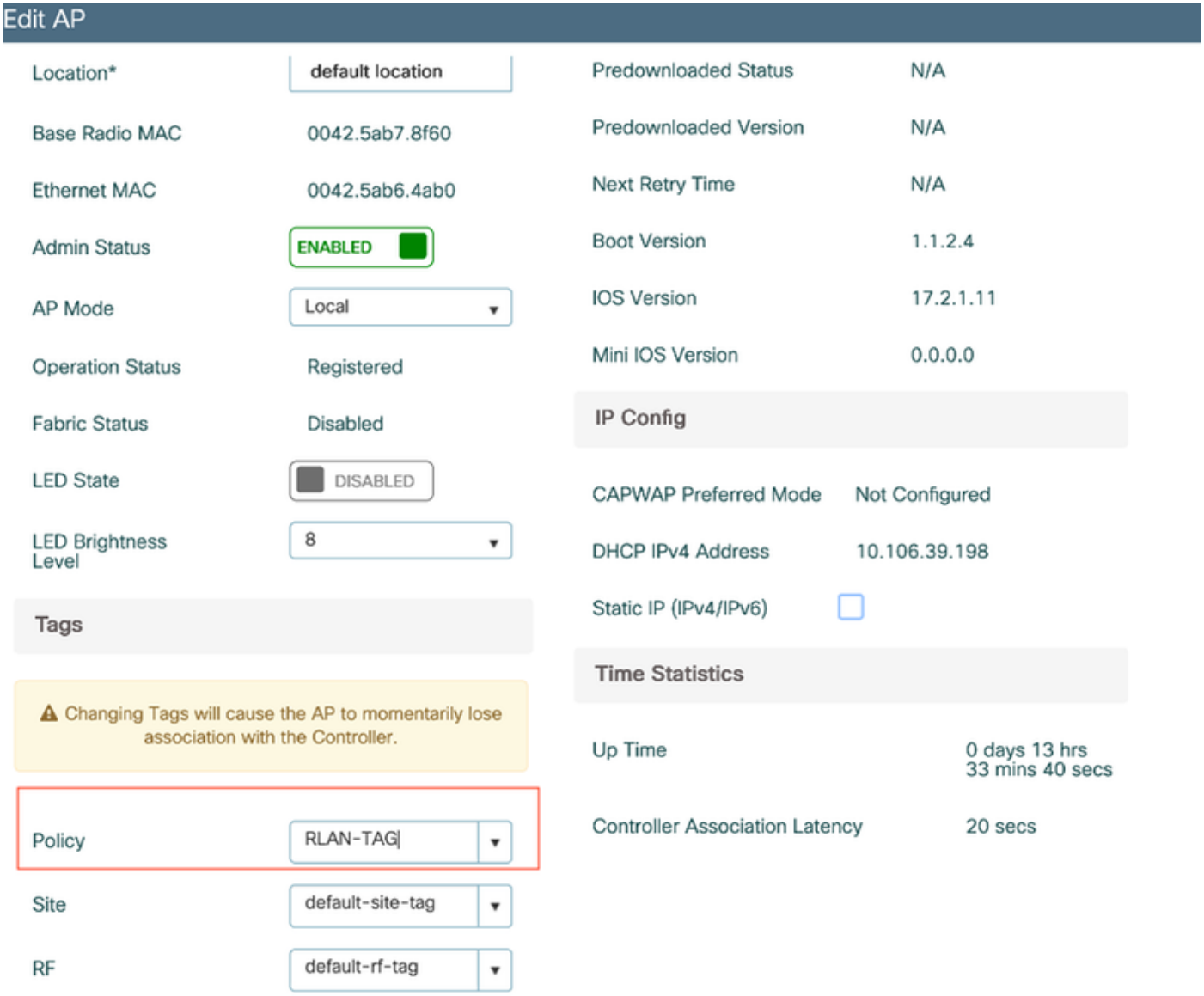


5.要建立策略標籤並將RLAN配置檔案對映到RLAN策略，請導航到**配置>標籤與配置檔案>標籤。**

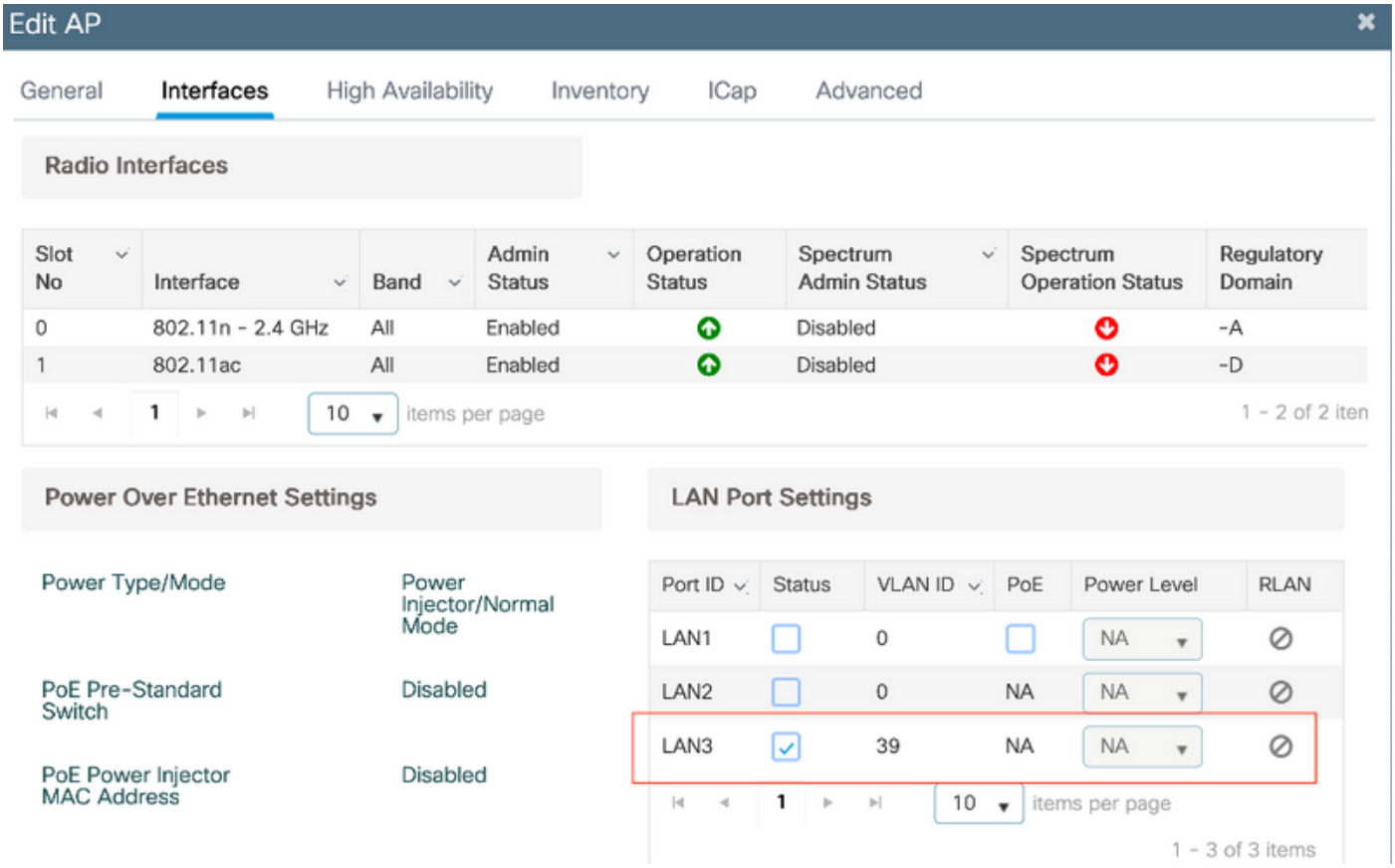

Add Policy Tag
Name*
RLAN-TAG
Description
Enter Description
WLAN-POLICY Maps: 0
RLAN-POLICY Maps: 0
Add
Delete
Port ID
RLAN Profile
RLAN Policy Profile
0
10
items per page
No items to display
Map RLAN and Policy
Port ID*
3
RLAN Profile*
RLAN-TEST
RLAN Policy Profile*
RLAN-Policy
Cancel
Apply to Device



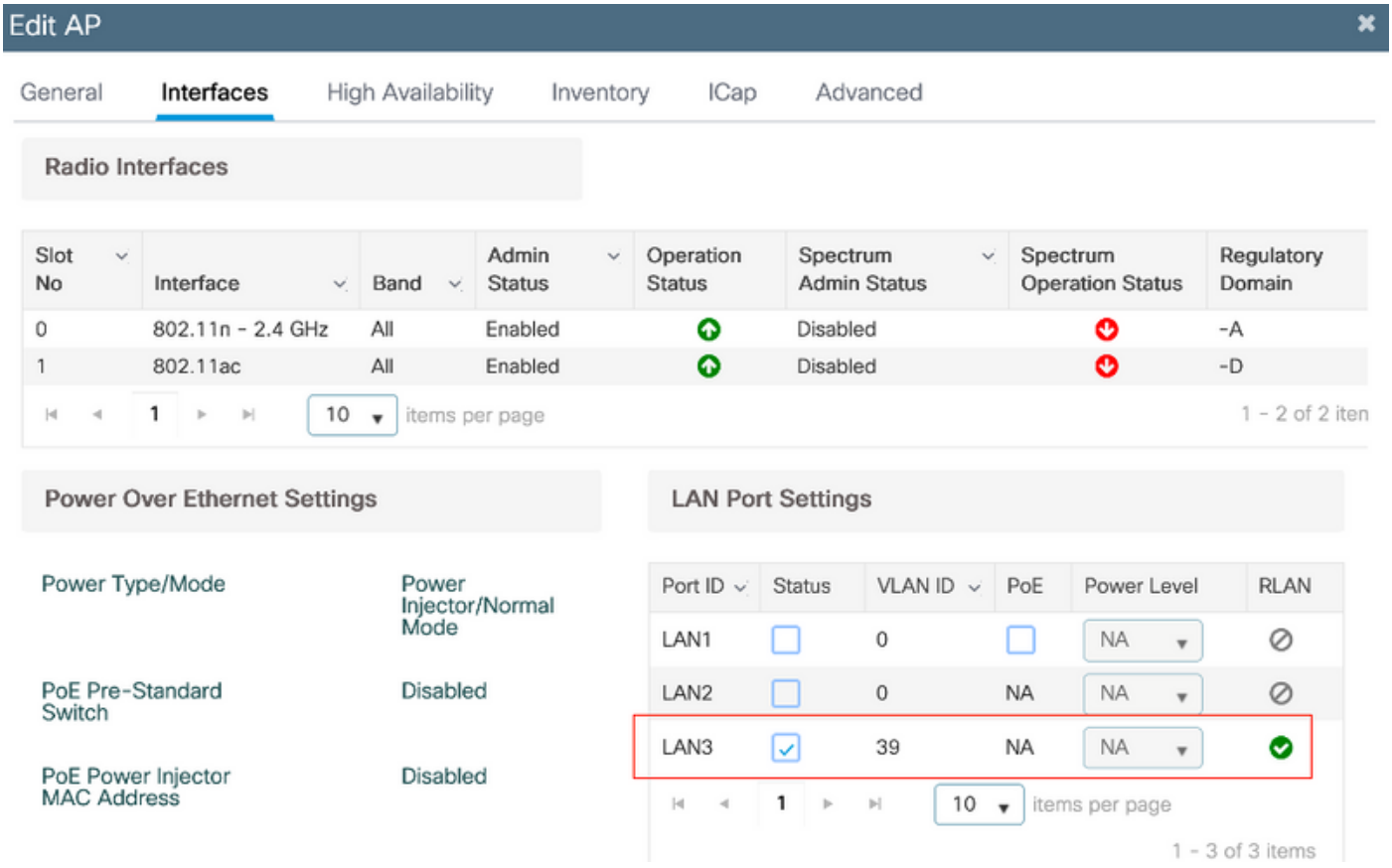
6.啟用LAN埠並在AP上應用策略標籤。導覽至**Configuration > Wireless > Access Points**，然後按一下**AP**。



套用設定，AP會重新加入WLC。按一下**AP**，然後選擇**Interfaces**並啟用LAN埠。

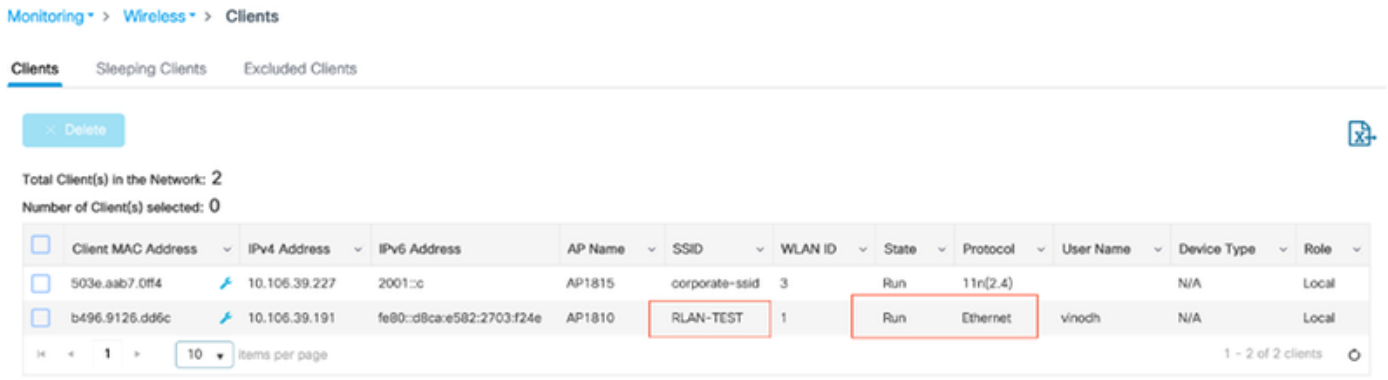


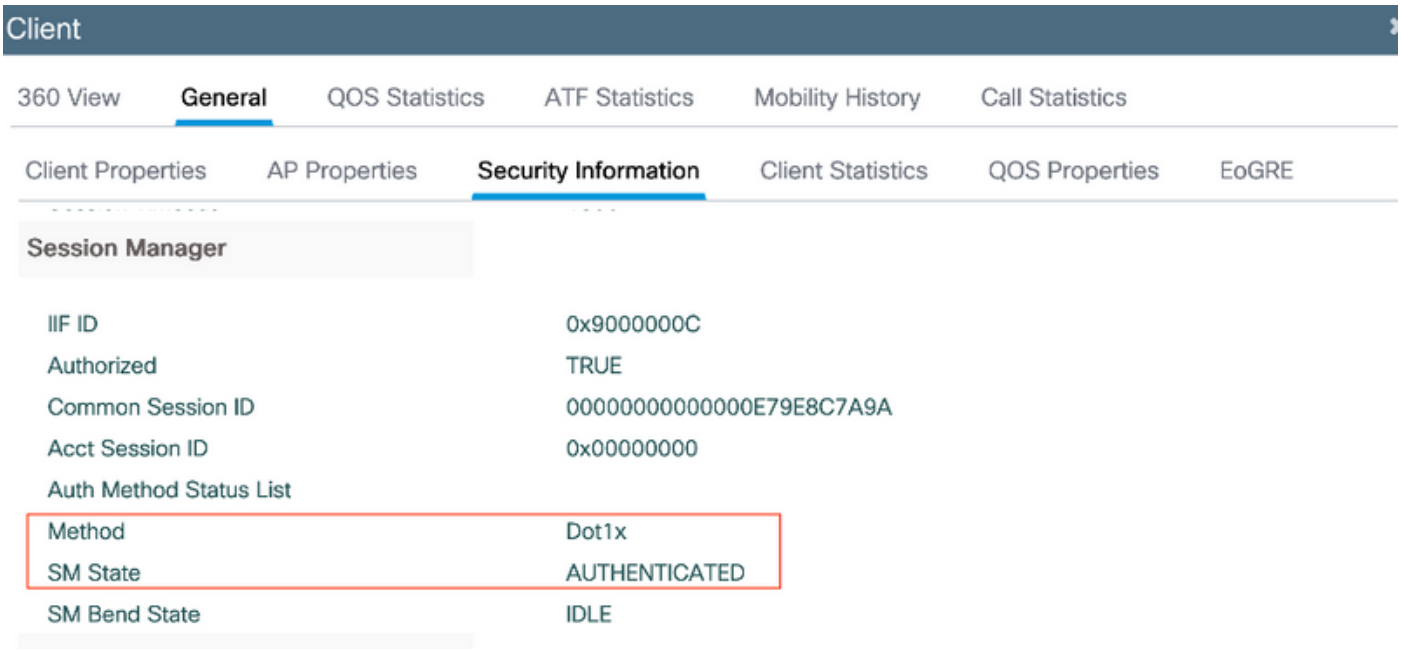
應用設定並驗證狀態。



7.將PC連線到AP的LAN3埠。PC將通過802.1x進行身份驗證，並從配置的VLAN獲取IP地址。

導覽至**Monitoring > Wireless > Clients**，檢查客戶端狀態。






```
vk-9800-1#show wireless client summary
Number of Clients: 2
MAC Address    AP Name                                          Type ID   State
Protocol Method     Role
--------------------------------------------------------------------------------------------------
-------------------------
503e.aab7.0ff4 AP1815                                           WLAN 3    Run
11n(2.4) None       Local
b496.9126.dd6c AP1810                                           RLAN 1    Run
Ethernet Dot1x      Local
Number of Excluded Clients: 0
```

疑難排解

常見問題：

- 僅本地SSID工作，未廣播WLC上配置的SSID：檢查AP是否正確加入控制器。
- 無法訪問OEAP GUI:檢查AP是否具有IP地址並驗證可達性（防火牆、ACL等）
- 集中交換無線或有線客戶端無法驗證或獲取IP地址：進行RA跟蹤，始終跟蹤等。

有線802.1x客戶端的「永遠線上」跟蹤示例：

```
[client-orch-sm] [18950]: (note): MAC: <client-mac>  Association received. BSSID 00b0.e187.cfc0,
old BSSID 0000.0000.0000, WLAN test_rlan, Slot 2 AP 00b0.e187.cfc0, Ap_1810
```

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_INIT -> S_CO_ASSOCIATING

[dot11-validate] [18950]: (ERR): MAC: <client-mac> Failed to dot11 determine ms physical radio type. Invalid radio type :0 of the client.

[dot11] [18950]: (ERR): MAC: <client-mac> Failed to dot11 send association response. Encoding of assoc response failed for client reason code: 14.

[dot11] [18950]: (note): MAC: <client-mac> Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False AID list: 0x1| 0x0| 0x0| 0x0

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-auth] [18950]: (note): MAC: <client-mac> L2 Authentication initiated. method DOT1X, Policy VLAN 1119,AAA override = 0 , NAC = 0

[ewlc-infra-evq] [18950]: (note): Authentication Success. Resolved Policy bitmap:11 for client <client-mac>

[client-orch-sm] [18950]: (note): MAC: <client-mac> Mobility discovery triggered. Client mode: Local

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS

[mm-client] [18950]: (note): MAC: <client-mac> Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_NONE, Previous BSSID MAC: 0000.0000.0000   Client IFID: 0xa0000003, Client Role: Local PoA: 0x90000012 PoP: 0x0

[client-auth] [18950]: (note): MAC: <client-mac> ADD MOBILE sent. Client state flags: 0x72 BSSID: MAC: 00b0.e187.cfc0 capwap IFID: 0x90000012

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS

[dot11] [18950]: (note): MAC: <client-mac> Client datapath entry params - ssid:test_rlan,slot_id:2 bssid ifid: 0x0, radio_ifid: 0x90000006, wlan_ifid: 0xf0404001

[dpath_svc] [18950]: (note): MAC: <client-mac> Client datapath entry created for ifid 0xa0000003

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS

[client-iplearn] [18950]: (note): MAC: <client-mac> Client IP learn successful. Method: DHCP IP: <Cliet-IP>

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Get ATF policy name from WLAN profile:: Failed to get wlan profile. Searched wlan profile test_rlan

[apmgr-db] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name

[apmgr-bssid] [18950]: (ERR): 00b0.e187.cfc0 Failed to get ATF policy name from WLAN profile name: No such file or directory

[client-orch-sm] [18950]: (ERR): Failed to get client ATF policy name: No such file or directory

[client-orch-state] [18950]: (note): MAC: <client-mac> Client state transition:

S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN