在Catalyst 9800 WLC上配置OEAP和RLAN

目录

简介

本文档说明如何在9800 WLC上配置Cisco OfficeExtend接入点(OEAP)和远程局域网(RLAN)。

Cisco OfficeExtend接入点(OEAP)提供从控制器到远程位置的Cisco AP的安全通信，通过互联网将公司WLAN无缝扩展到员工住所。用户在家庭办公室的体验与企业办公室的体验完全相同。接入点和控制器之间的数据报传输层安全(DTLS)加密可确保所有通信都具有最高级别的安全性。

远程LAN(RLAN)用于使用控制器对有线客户端进行身份验证。有线客户端成功加入控制器后，LAN端口会在中央或本地交换模式之间交换流量。来自有线客户端的流量被视为无线客户端流量。接入点(AP)中的RLAN发送身份验证请求以对有线客户端进行身份验证。RLAN中有线客户端的身份验证类似于中央身份验证的无线客户端。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800 WLC
- 对无线控制器和接入点的命令行界面(CLI)访问

使用的组件

本文档中的信息基于以下软件和硬件版本：

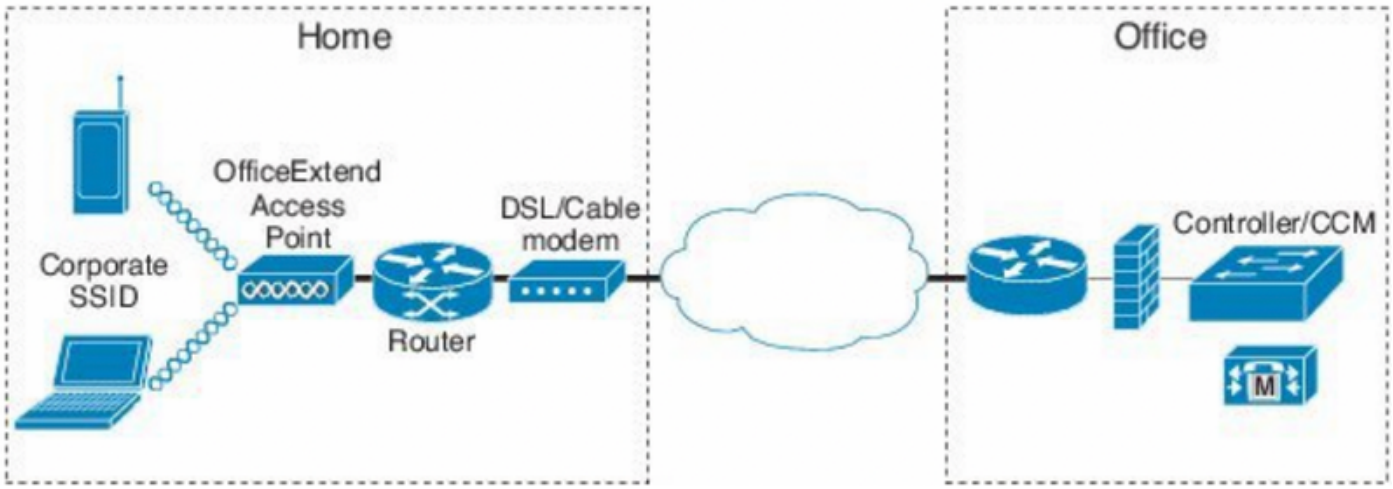
- Catalyst 9800 WLC版本17.02.01
- 1815/1810系列AP

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图

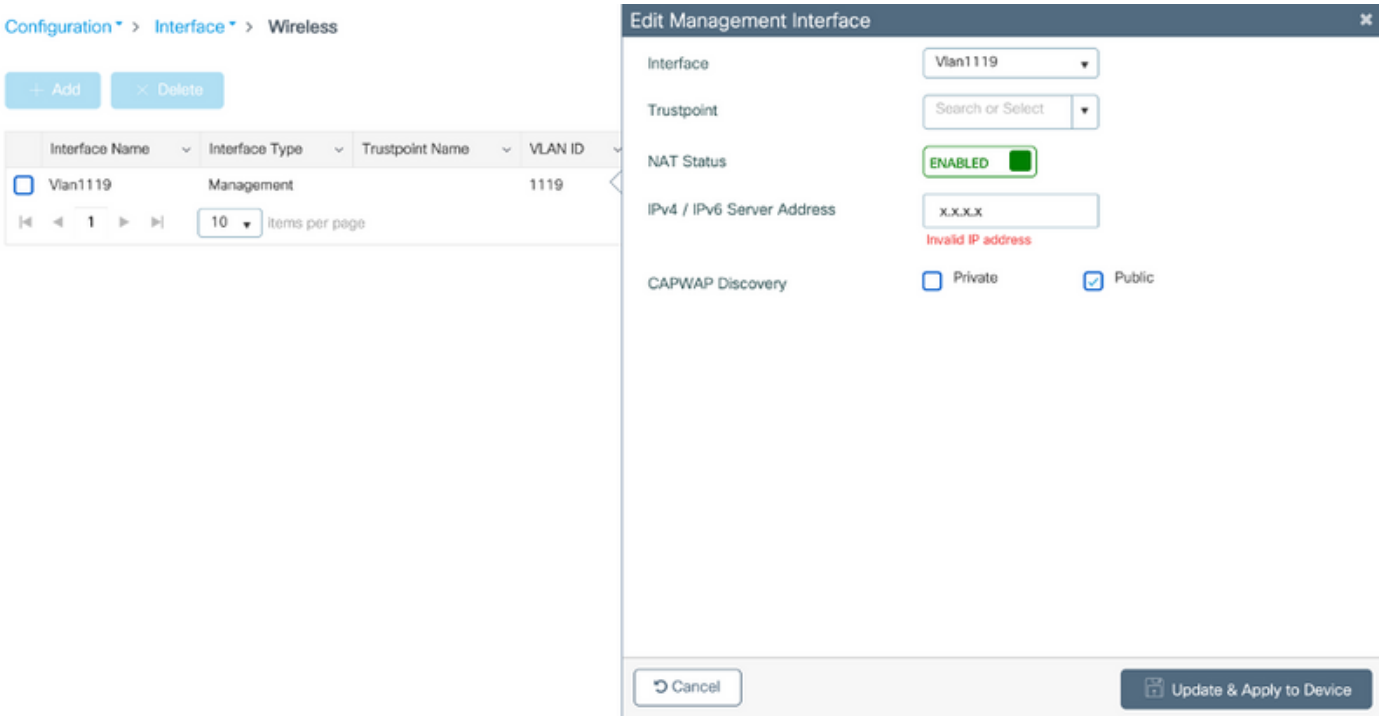


AP在NAT后加入

在16.12.x代码中，您需要从CLI配置NAT IP地址。没有可用的GUI选项。您还可以通过公共或专用IP选择CAPWAP发现。

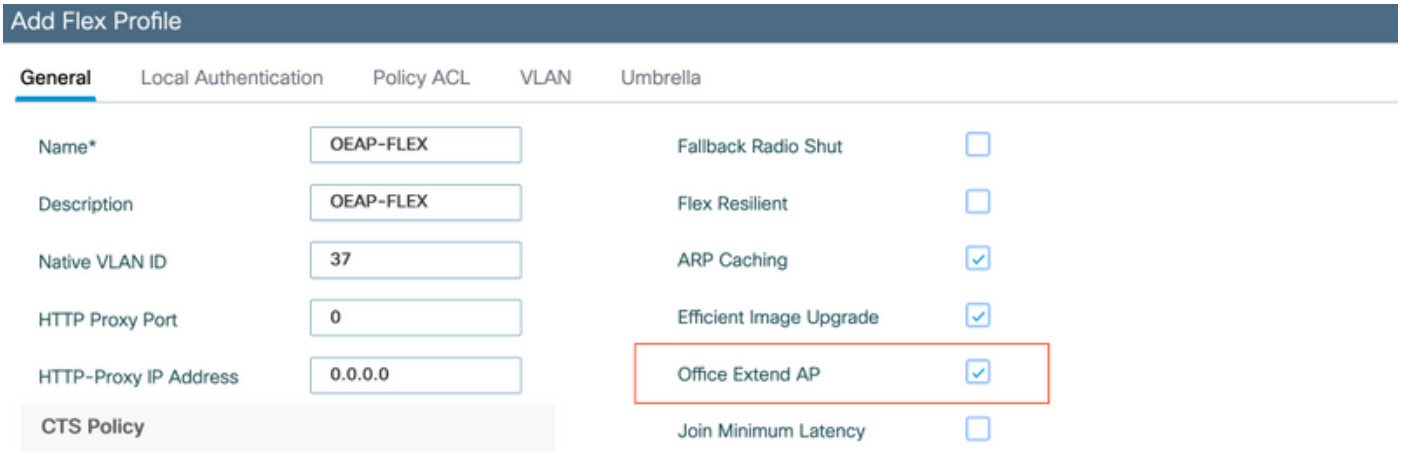
```
(config)#wireless management interface vlan 1114 nat public-ip x.x.x.x
(config-nat-interface)#capwap-discovery ?
  private  Include private IP in CAPWAP Discovery Response

  public   Include public IP in CAPWAP Discovery Response
```

在17.x代码中，导航至**Configuration > Interface > Wireless**，然后单击**Wireless Management Interface**，从GUI中配置NAT IP和CAPWAP发现类型。

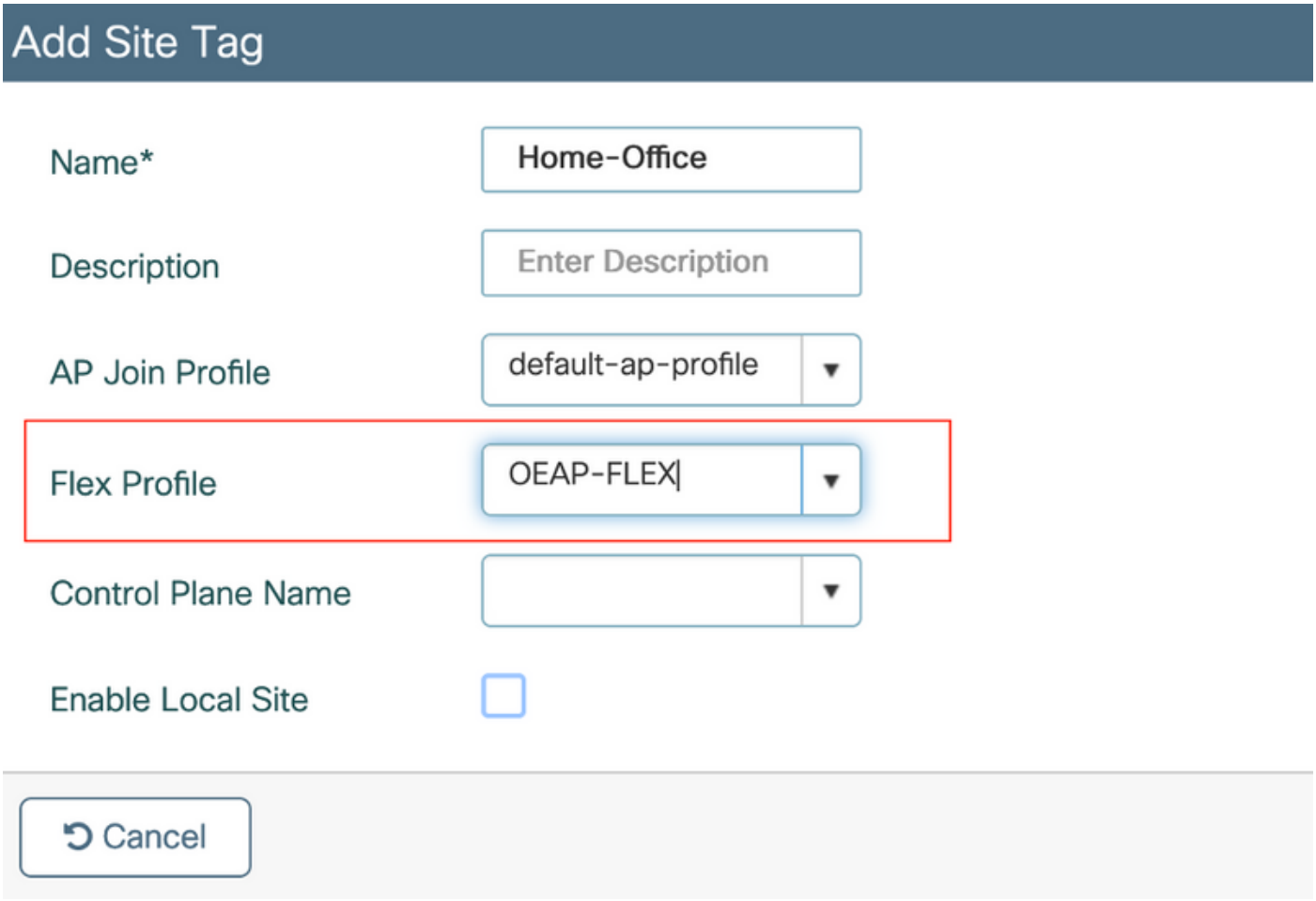


配置

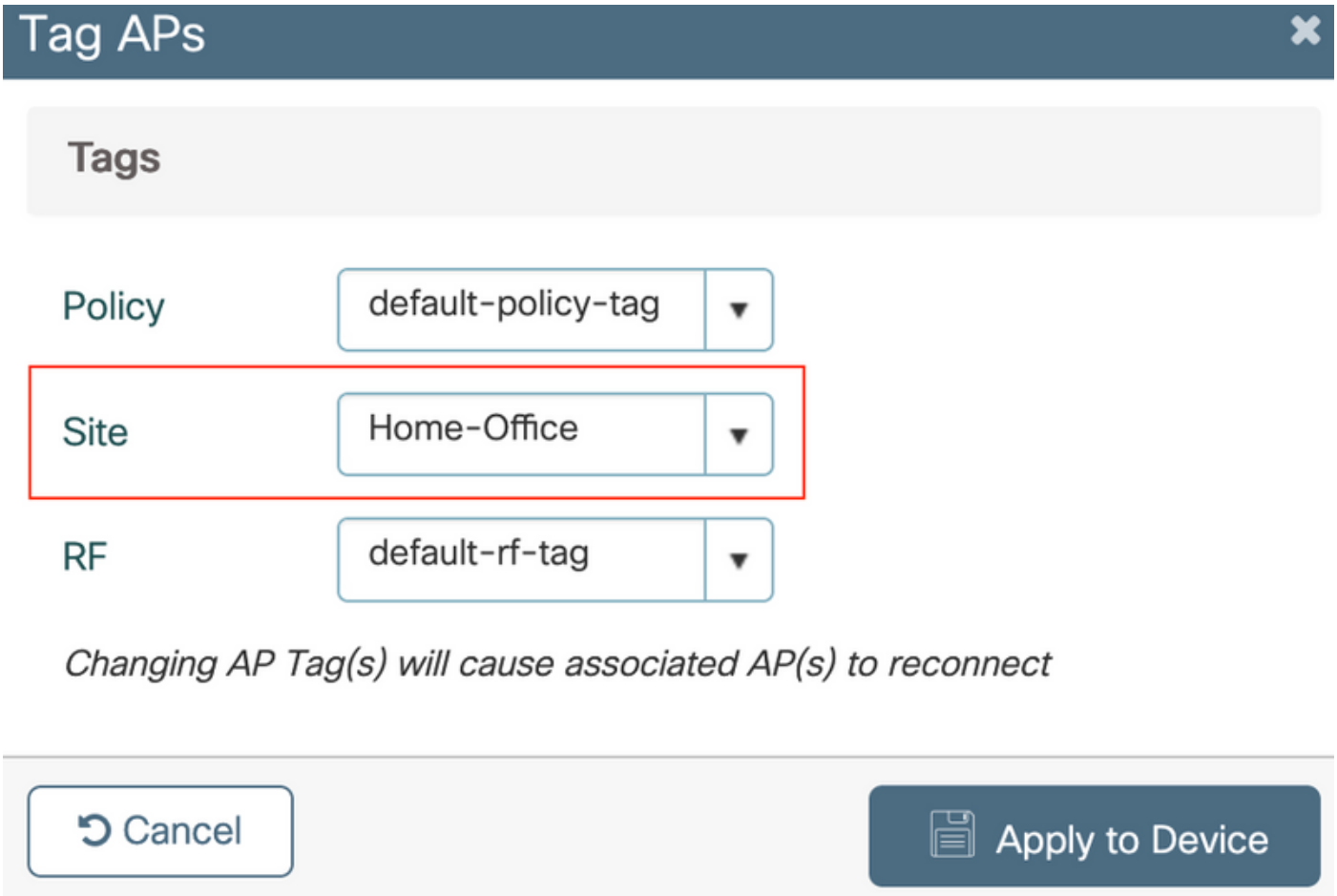
1.要创建Flex配置文件，请启用**Office Extend AP**并导航至**Configuration > Tags & Profiles > Flex。**



2.要创建站点标签并映射Flex Profile，请导航至**配置>标签和配置文件>标签。**



3.导航至使用Configuration > Wireless Setup >Advanced > Tag APs创建的Site Tag（站点标签）**标记1815 AP。**



验证

1815 AP重新加入WLC后，验证以下输出：

```
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
```

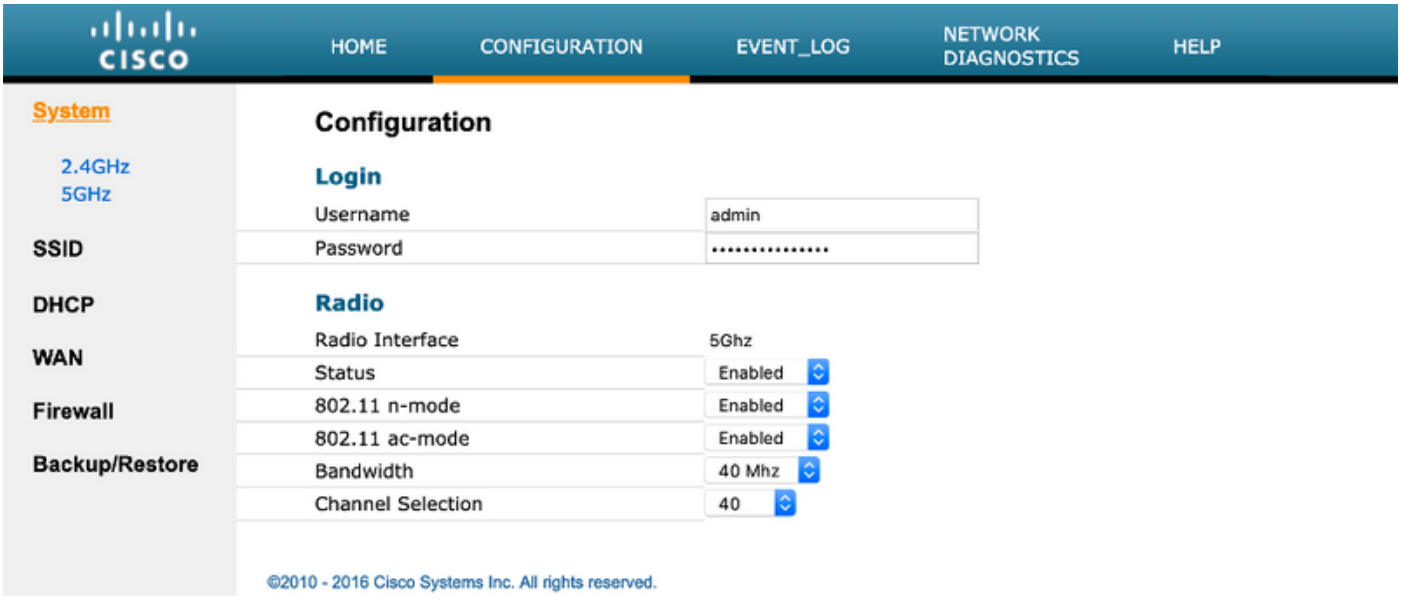
注意：您可以使用ap link-encryption命令为特定接入点或所有接入点启用或禁用DTLS数据加密

```
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
```

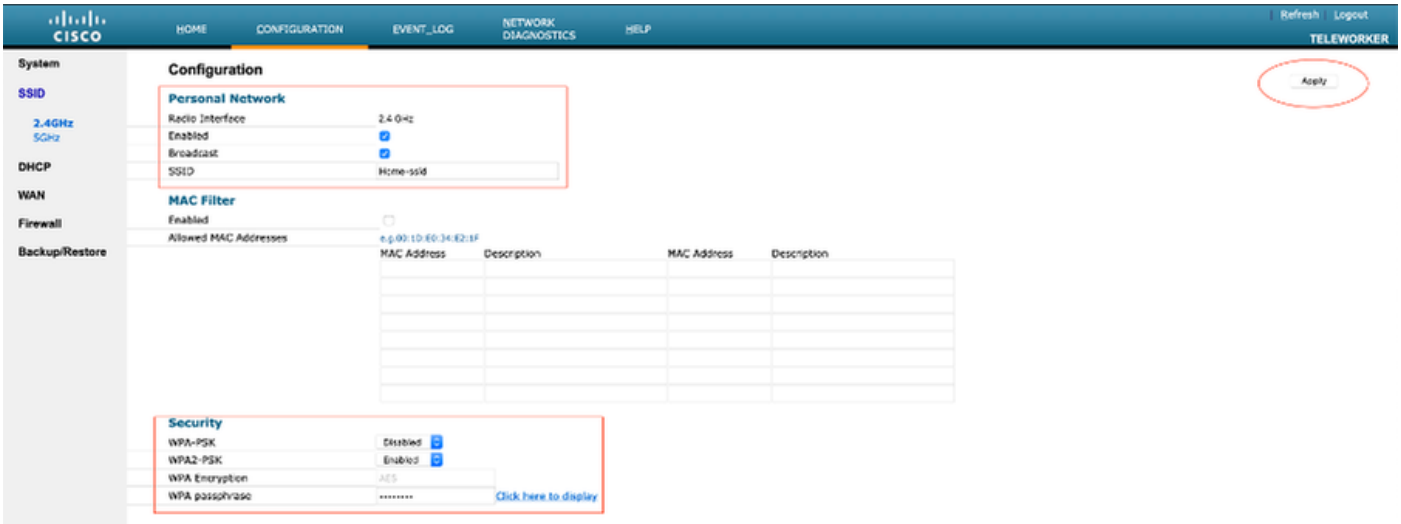
登录OEAP并配置个人SSID

1.您可以使用IP地址访问OEAP的Web界面。要登录的默认凭证是admin和admin。

2.出于安全原因，建议更改默认凭据。



3.导航至**Configuration> SSID> 2.4GHz/5GHz**以配置个人SSID。



4.启用无线电接口。

5.输入SSID并启用广播

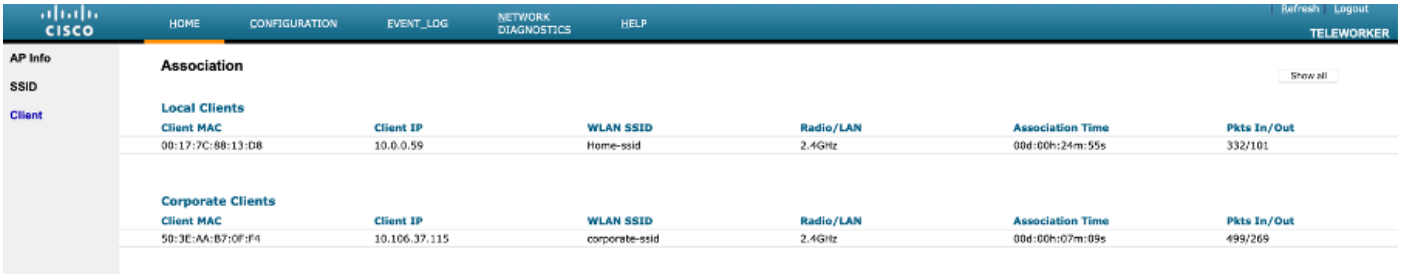
6.对于加密，请选**择WPA-PSK**或**WPA2-PSK**并输入相应安全类型的口令。

7.单击“应用”以使设置生效。

8.默认情况下，连接到个人SSID的客户端从10.0.0.1/24网络获取IP地址。

9.家庭用户可以使用相同的AP连接供家庭使用，并且流量不通过DTLS隧道传输。

10.要检查OEAP上的客户端关联，请导航至“主页”>“**客户端**”。您可以看到与OEAP关联的本地客户端和公司客户端。




```
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上配置RLAN

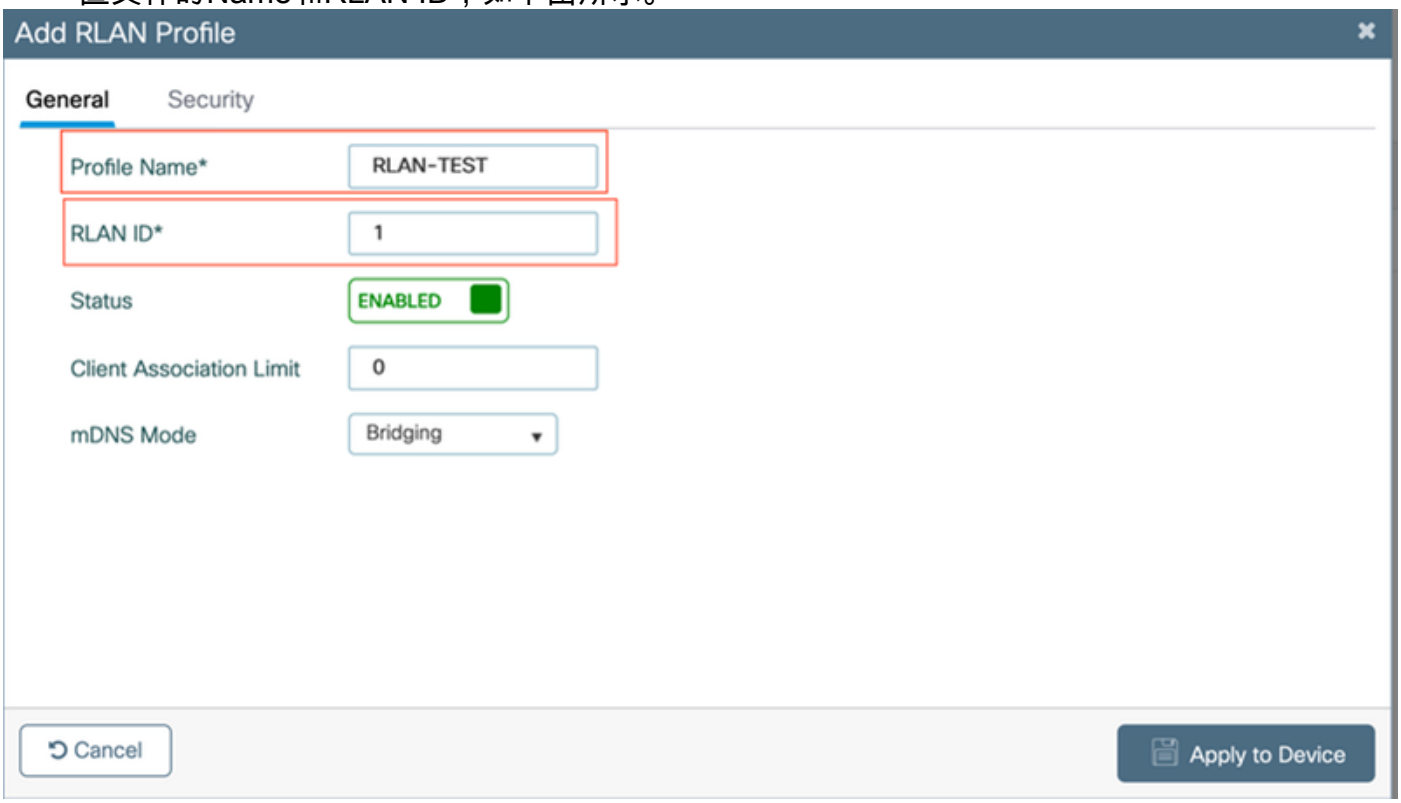
远程LAN(RLAN)用于使用控制器对有线客户端进行身份验证。有线客户端成功加入控制器后，LAN端口会在中央或本地交换模式之间交换流量。来自有线客户端的流量被视为无线客户端流量。接入点(AP)中的RLAN发送身份验证请求以对有线客户端进行身份验证。的

RLAN中有线客户端的身份验证类似于中央身份验证的无线客户端。

> **注意**：本例中，本地EAP用于RLAN客户端身份验证。WLC上必须存在本地EAP配置才能配置以下步骤。它包括aaa authentication & authorization方法、本地EAP配置文件和本地凭证。

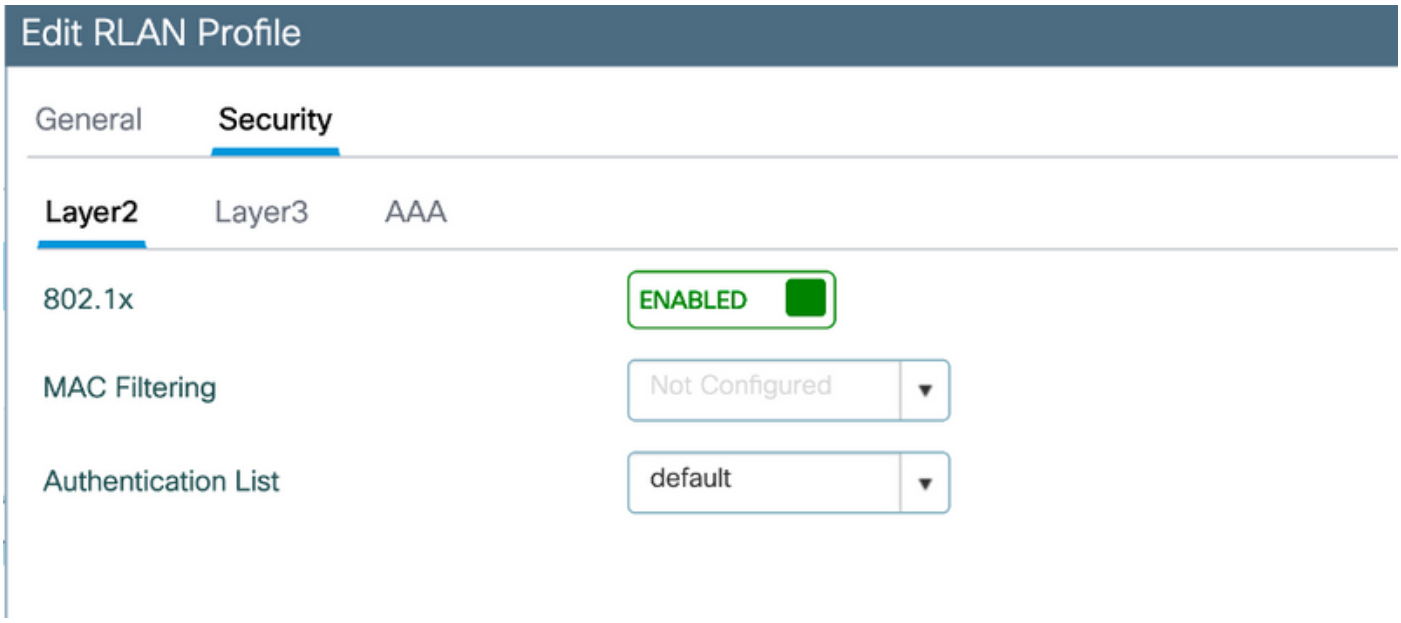
Catalyst 9800 WLC上的本地EAP身份验证配置示例

1. 要创建RLAN配置文件，请导航至**Configuration > Wireless > Remote LAN**，然后输入RLAN配置文件的Name和RLAN ID，如下图所示。

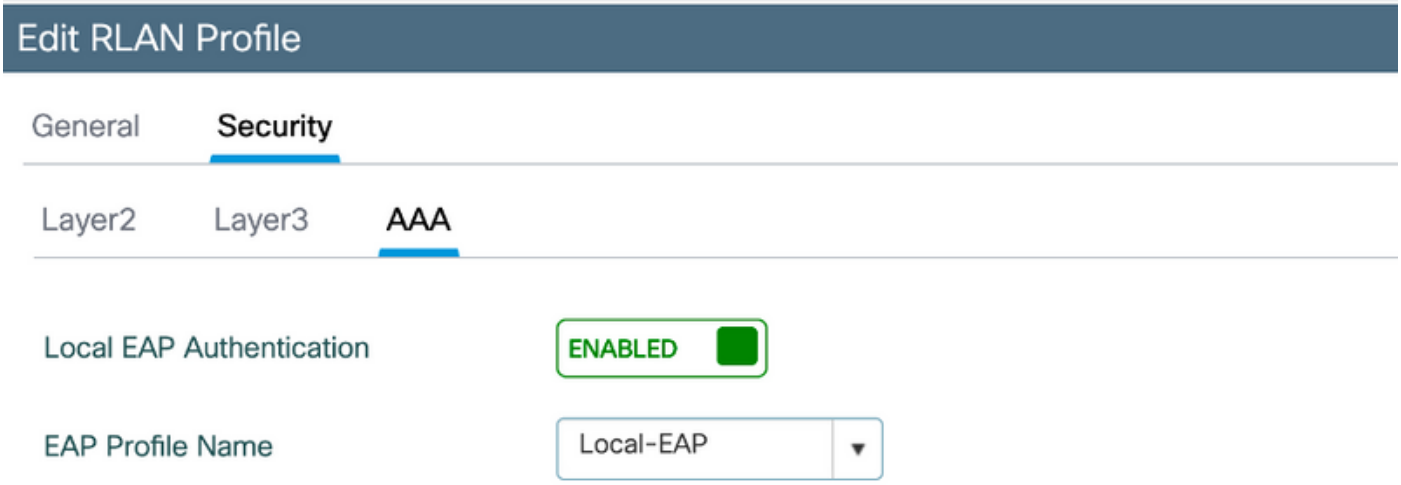


2.导航至**Security > Layer2**，为了为RLAN启用802.1x，请将802.1x状态设置为Enabled，如下图所

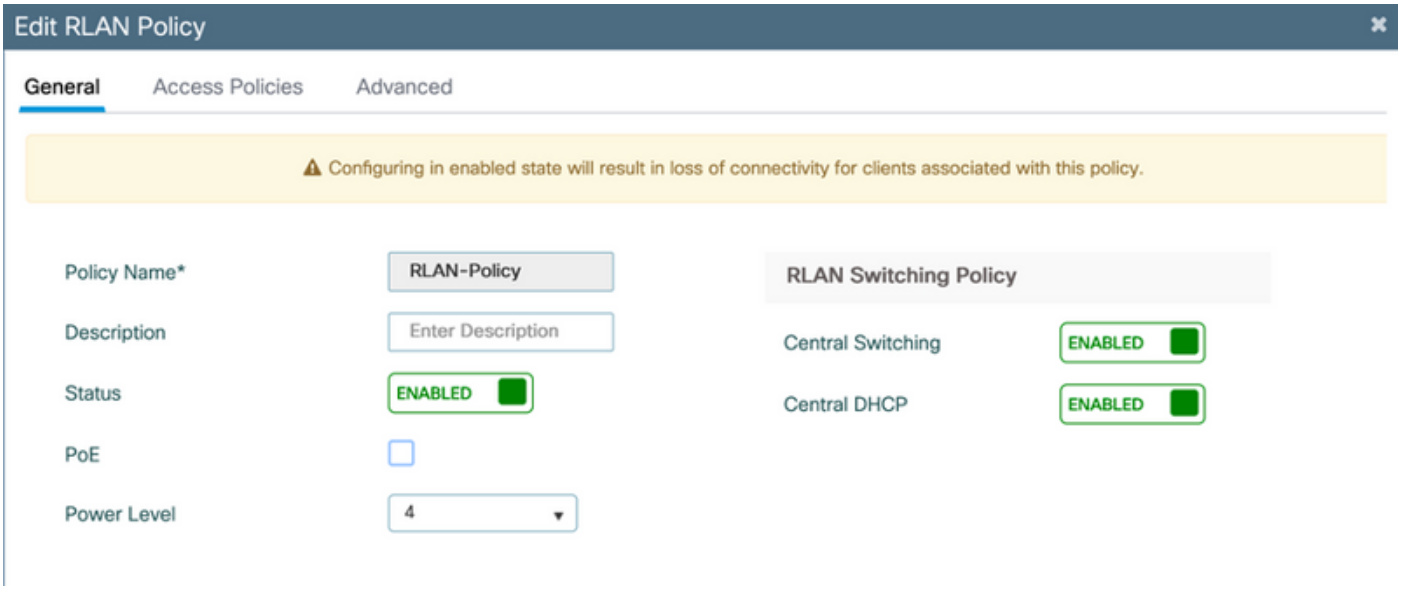
示。



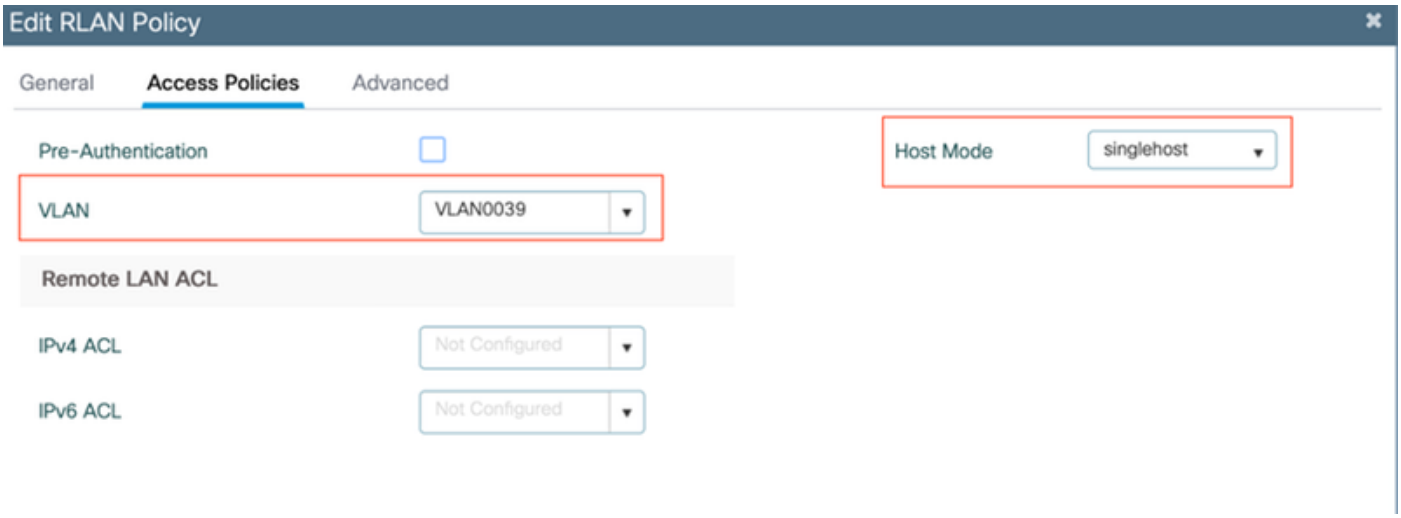
3.导航至**Security > AAA**，将Local EAP Authentication设置为enabled，然后从下拉列表中选择所需的EAP Profile Name，如此图所示。



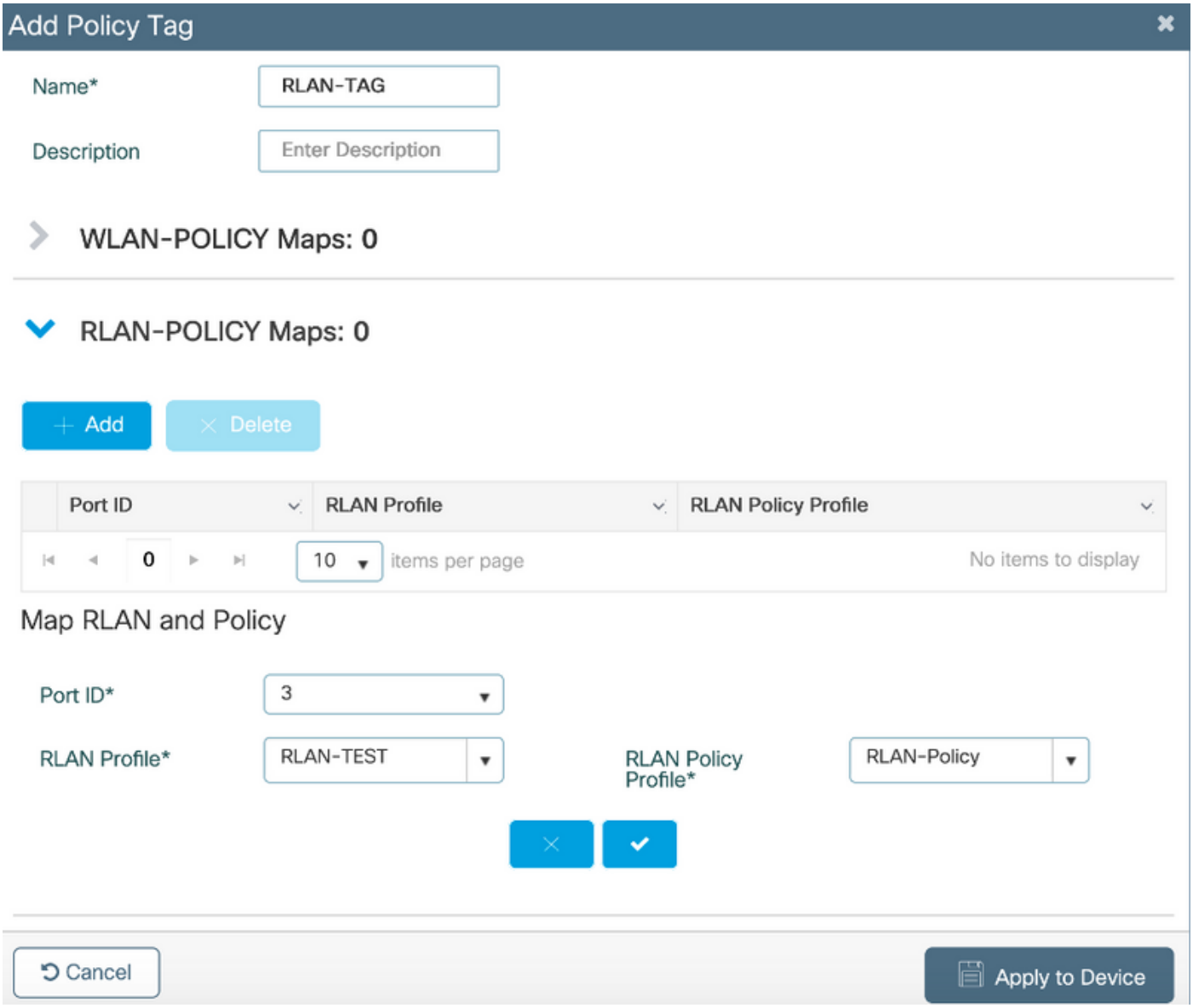
4.要创建RLAN策略，请导航至**Configuration > Wireless > Remote LAN**，然后在“Remote LAN”页上，单击**RLAN Policy**选项卡，如下图所示。

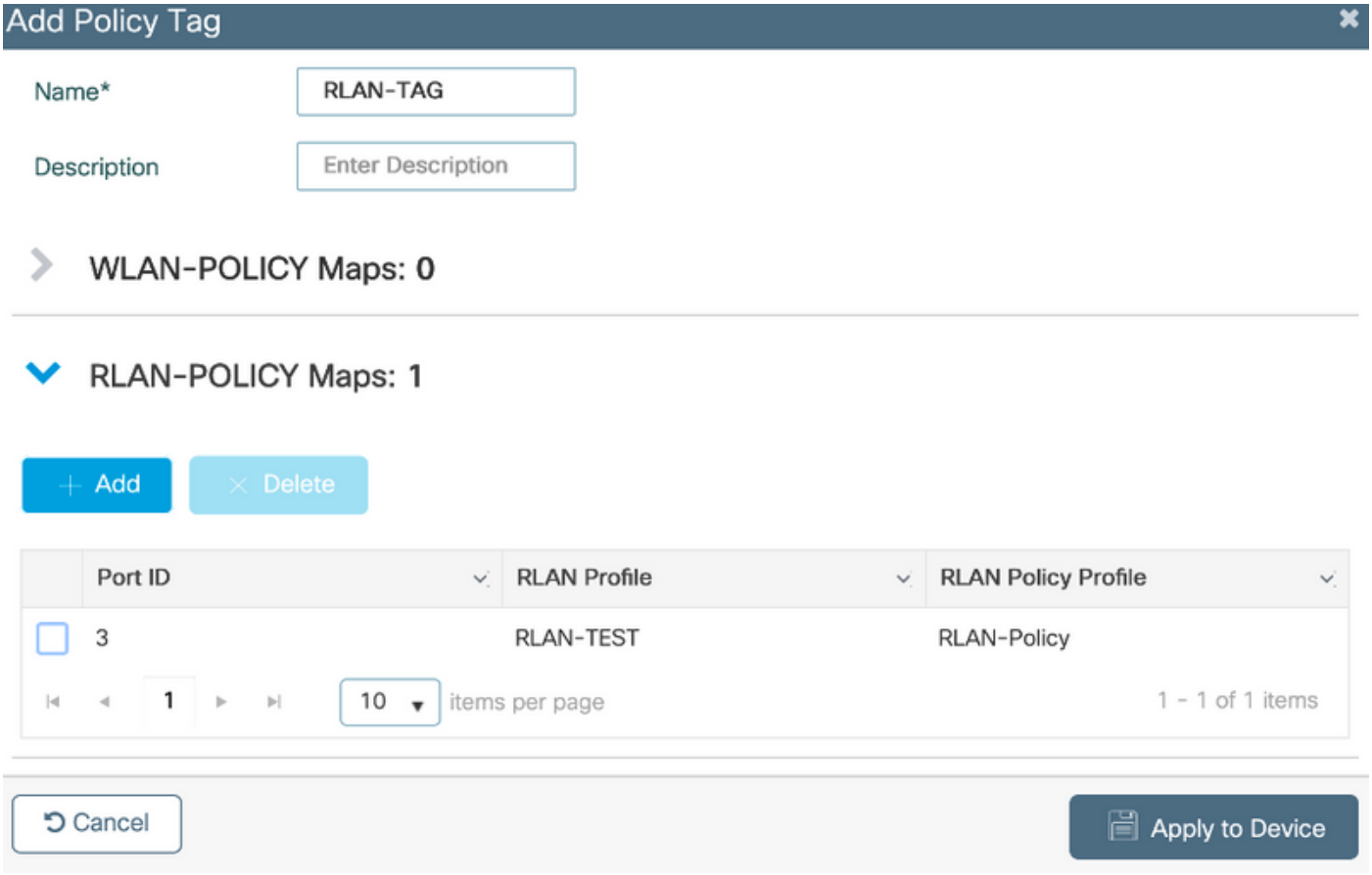


导航至访问策略并配置VLAN和主机模式并应用设置。

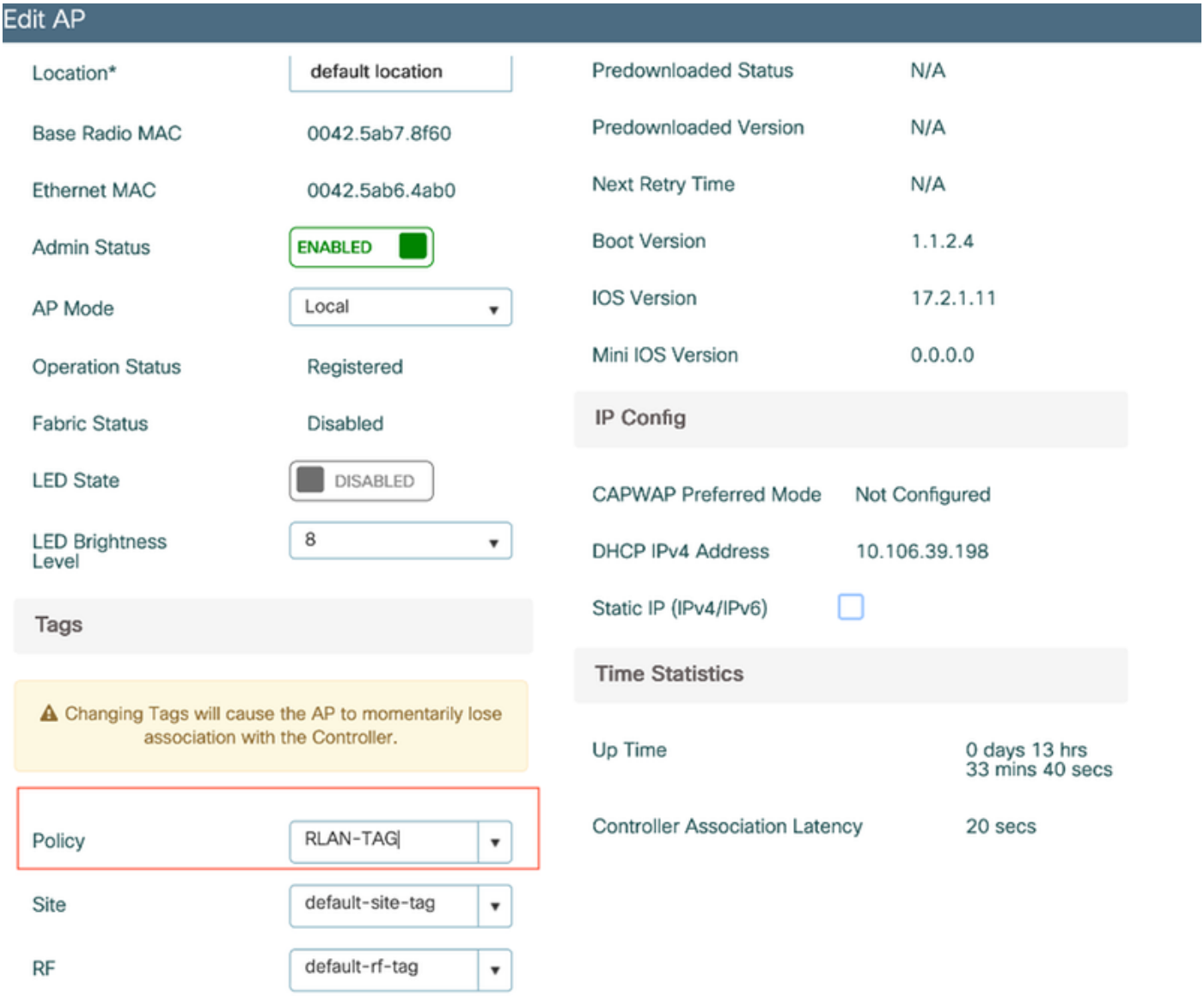


5.要创建策略标记并将RLAN配置文件映射到RLAN策略，请导航至**Configuration > Tags & Profiles > Tags**。

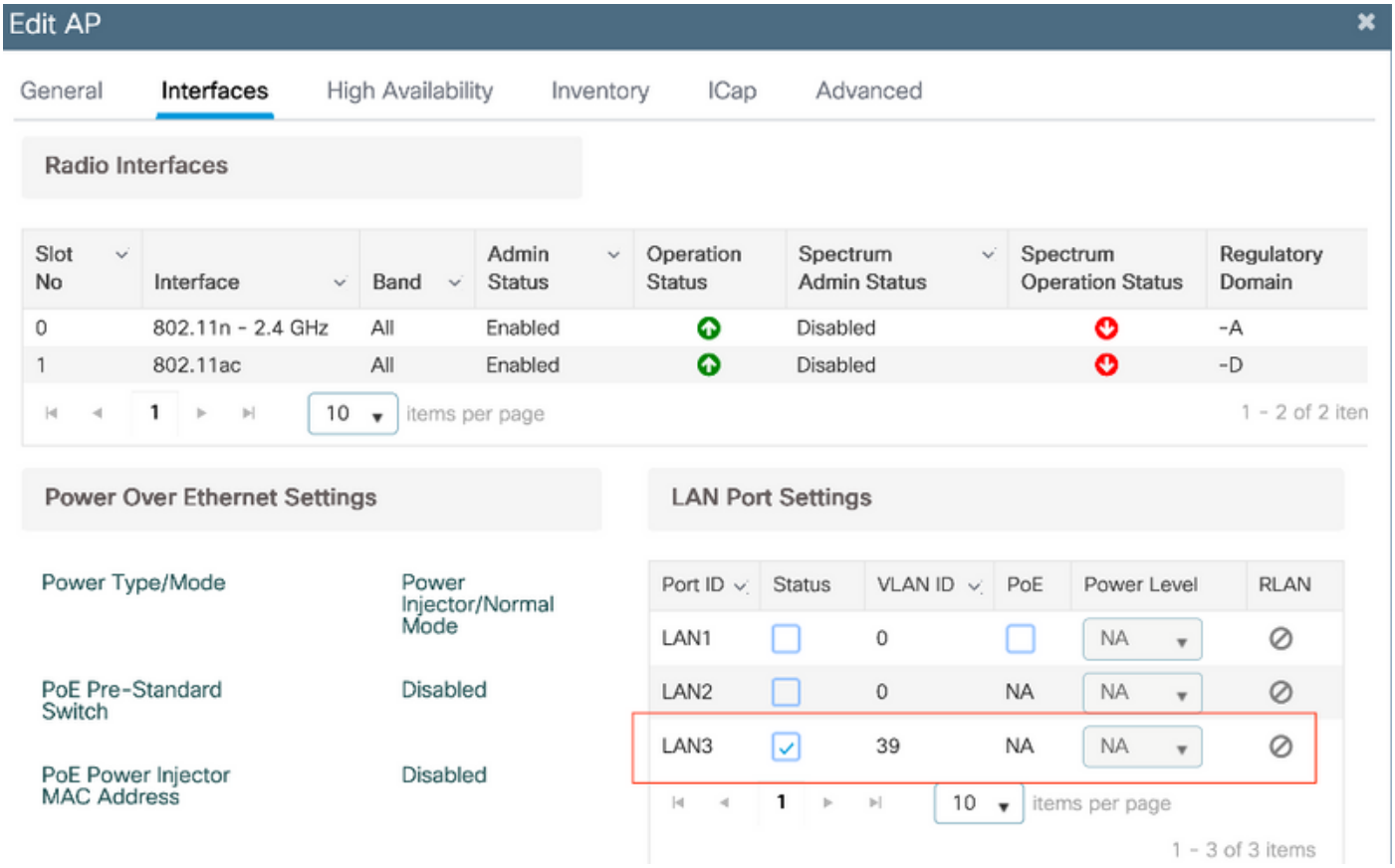

Add Policy Tag
Name*
RLAN-TAG
Description
Enter Description
WLAN-POLICY Maps: 0
RLAN-POLICY Maps: 0
Add
Delete
Port ID
RLAN Profile
RLAN Policy Profile
0
10
items per page
No items to display
Map RLAN and Policy
Port ID*
3
RLAN Profile*
RLAN-TEST
RLAN Policy Profile*
RLAN-Policy
Cancel
Apply to Device



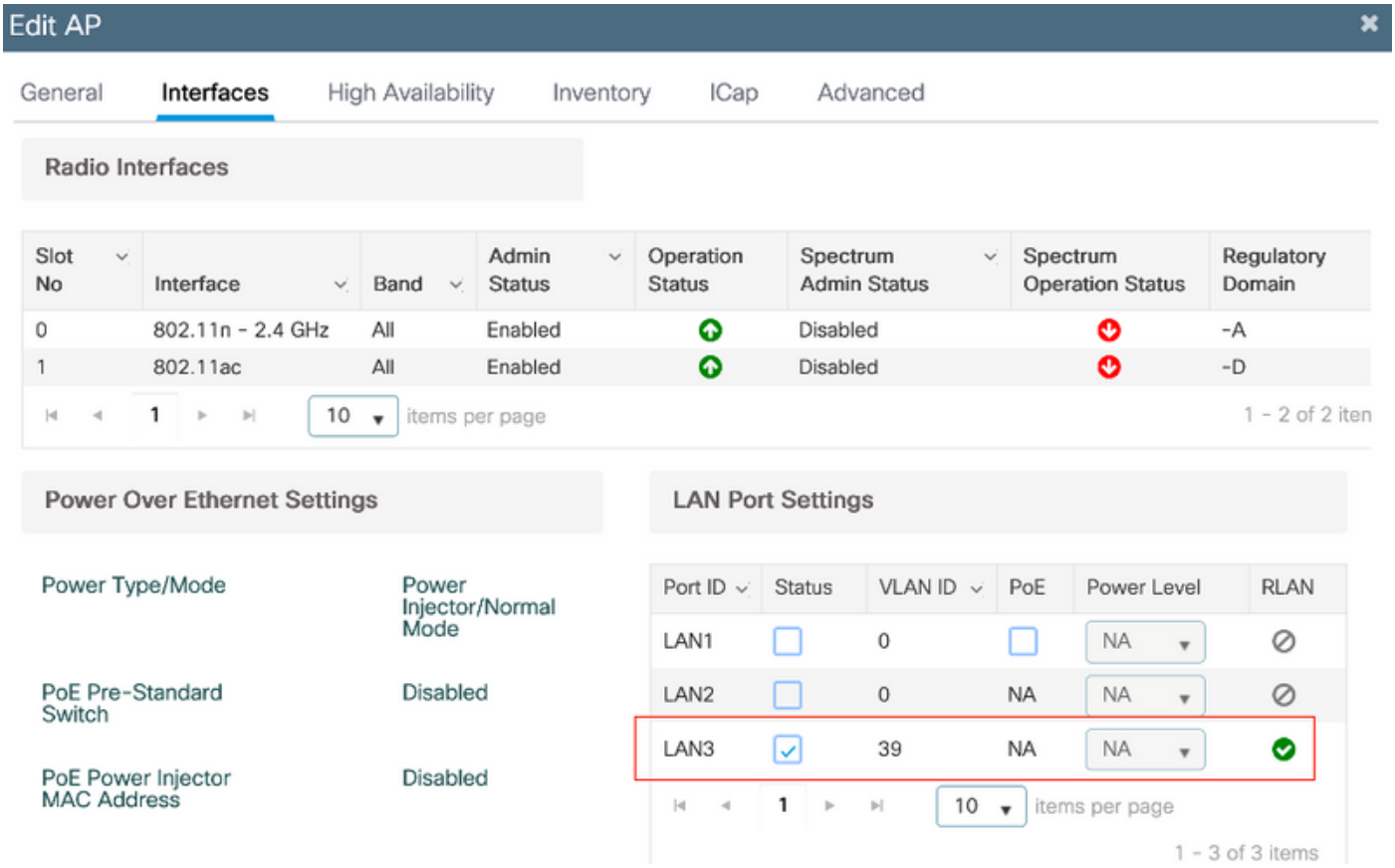
6.启用LAN端口并在AP上应用策略标记。导航至**Configuration > Wireless > Access Points**，然后单击**AP**。



应用设置，AP重新加入WLC。单击AP，然后选择**Interfaces**并启用LAN端口。

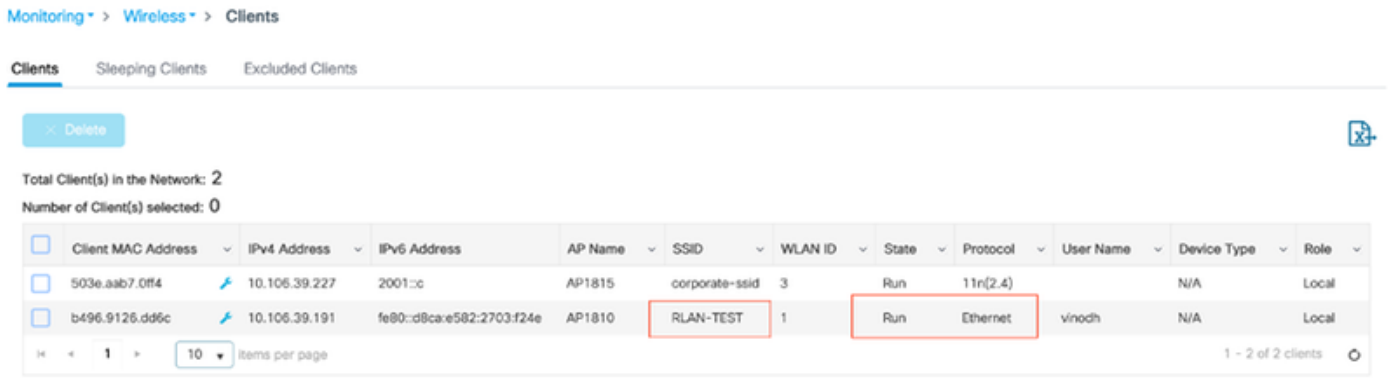


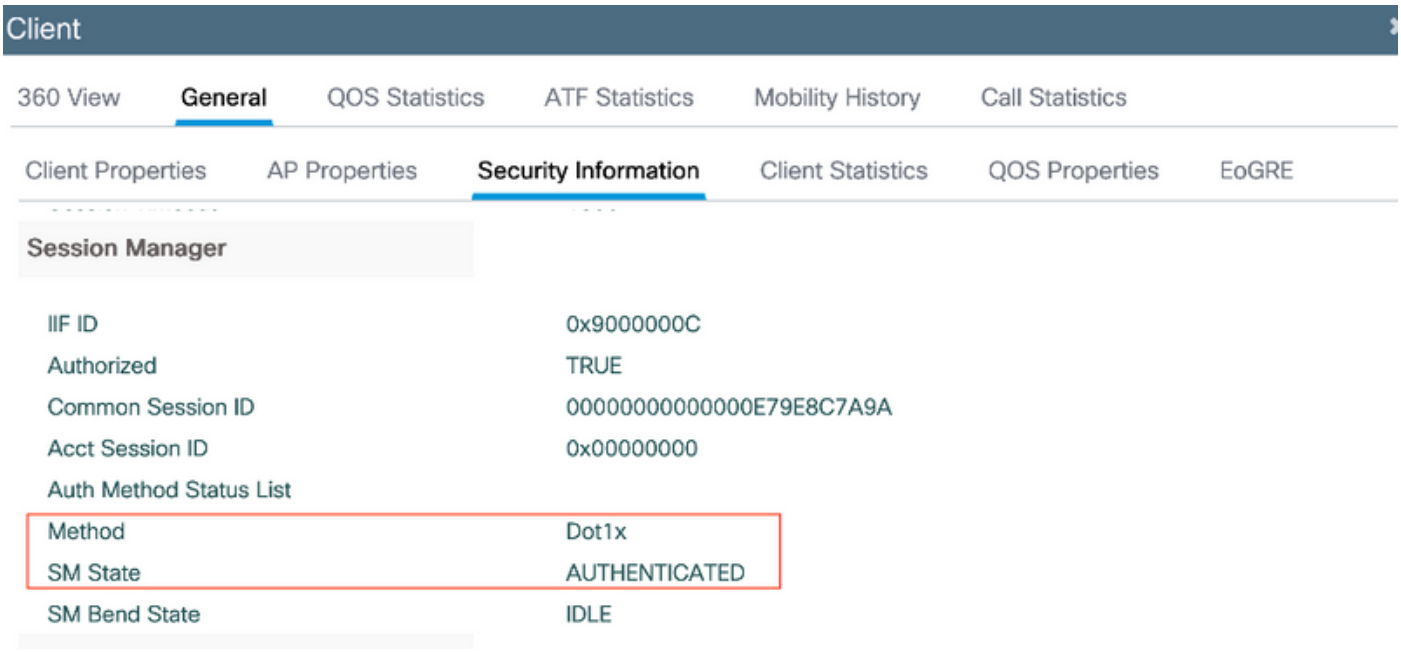
应用设置并验证状态。



7.将PC连接到AP的LAN3端口。PC将通过802.1x进行身份验证，并从已配置的VLAN获取IP地址。

导航至**监控>无线>客**户端以检查客户端状态。






```
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
```

故障排除

常见问题:

- 仅本地SSID的工作，WLC上配置的SSID未被广播：检查AP是否已正确加入控制器。
- 无法访问OEAP GUI:检查ap是否具有IP地址并检验连通性（防火墙、ACL等网内）
- 集中交换无线或有线客户端无法验证或获取IP地址：获取RA跟踪，始终在跟踪等。

有线802.1x客户端的始终在线跟踪示例：

```
[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