配置Catalyst 9800和FlexConnect OEAP拆分隧道

目录

简介

本文档介绍如何将室内接入点(AP)配置为FlexConnect Office Extend(OEAP)，以及如何启用分割隧道，以便您可以定义哪些流量可以在家庭办公室本地交换，哪些流量必须在WLC中集中交换。

先决条件

要求

本文档中的配置假设WLC已在启用了NAT的DMZ中配置，并且AP能够从家庭办公室加入WLC。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS-XE 17.3.1软件的无线LAN控制器9800。
- Wave1 AP:1700/2700/3700 的多播地址发送一次邻居消息。
- 第2波AP:1800/2800/3800/4800和Catalyst 9100系列。

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。

概述

Cisco OfficeExtend接入点(Cisco OEAP)提供从Cisco WLC到远程位置的Cisco AP的安全通信，通过互联网无缝地将企业WLAN扩展到员工住所。用户在家庭办公室的体验与在公司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。 FlexConnect模式下的任何室内AP都可以充当OEAP。

背景信息

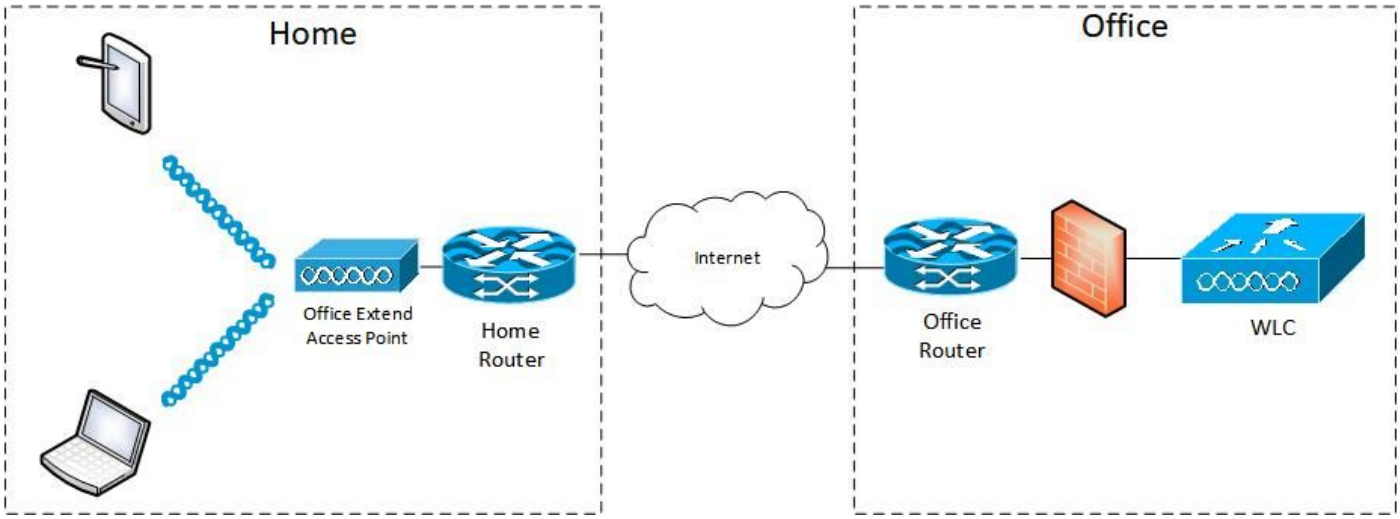
FlexConnect是指接入点(AP)在远程位置（例如广域网）上运行时处理无线客户端的功能。他们还可以决定来自无线客户端的流量是直接放在AP级（本地交换）网络上，还是将流量集中到9800控制器（中央交换），然后根据WLAN通过WAN发回。

有关FlexConnect的详细信息，请查看本文档了解Catalyst 9800无线控制器上的FlexConnect。

OEAP模式是FlexConnect AP中提供的选项，可允许其他功能，例如个人本地SSID用于家庭访问，还可提供分割隧道功能，以更大的粒度定义哪些流量必须在家庭办公室本地交换，哪些流量必须在WLC上通过单个WLAN集中交换

配置

网络图



配置

定义分割隧道的访问控制列表

步骤1.选择Configuration > Security > ACL。选择添加。

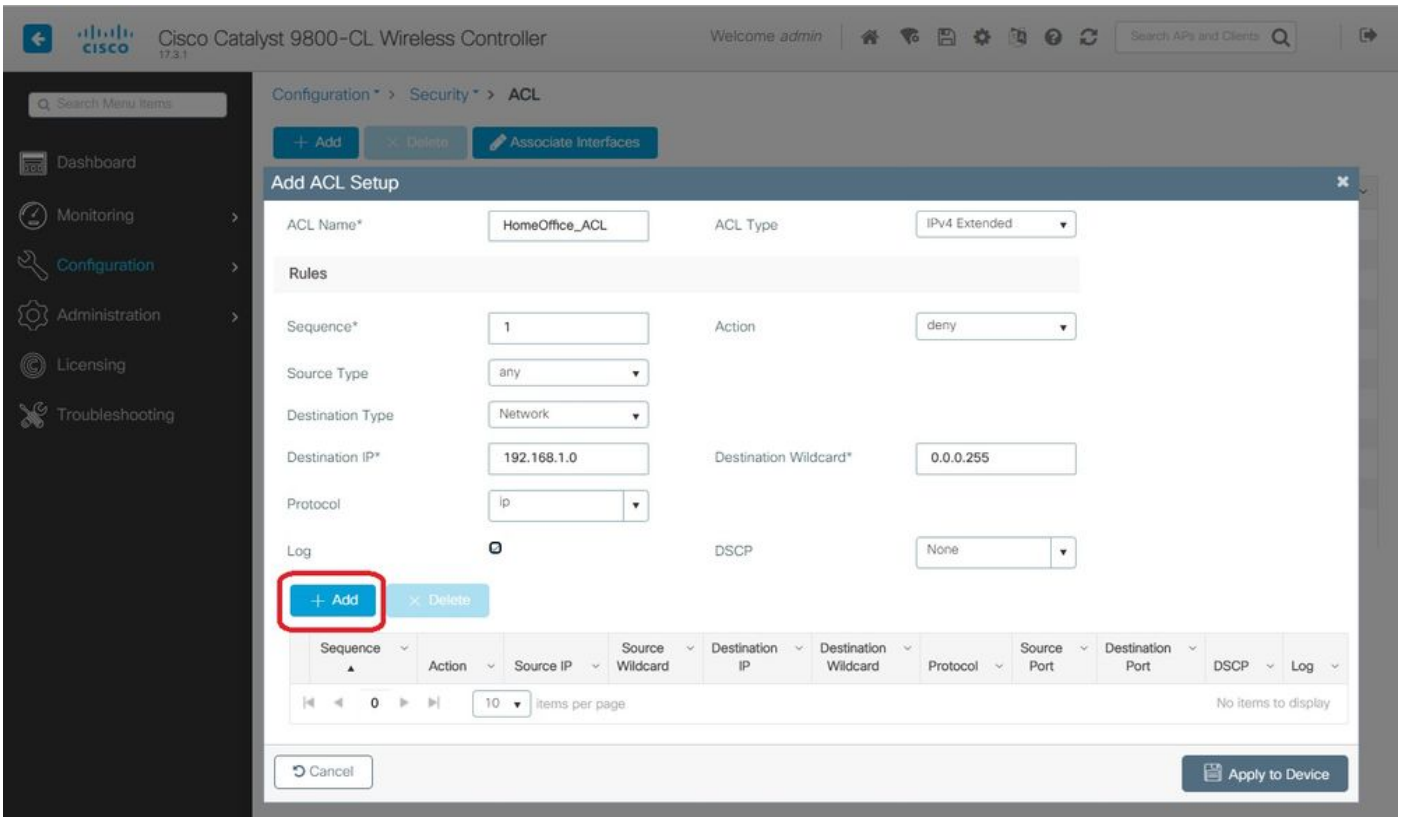
步骤2.在Add ACL Setup（添加ACL设置）对话框中，输入ACL Name（ACL名称），从ACL Type下拉列表中选择ACL类型，然后在Rules（规则）设置下，输入Sequence number（序列号）。然后，选择Action（操作）作为permit或deny。

步骤3.从Source Type下拉列表中选择所需的源类型。

如果选择源类型作为主机，则必须输入主机名/IP。

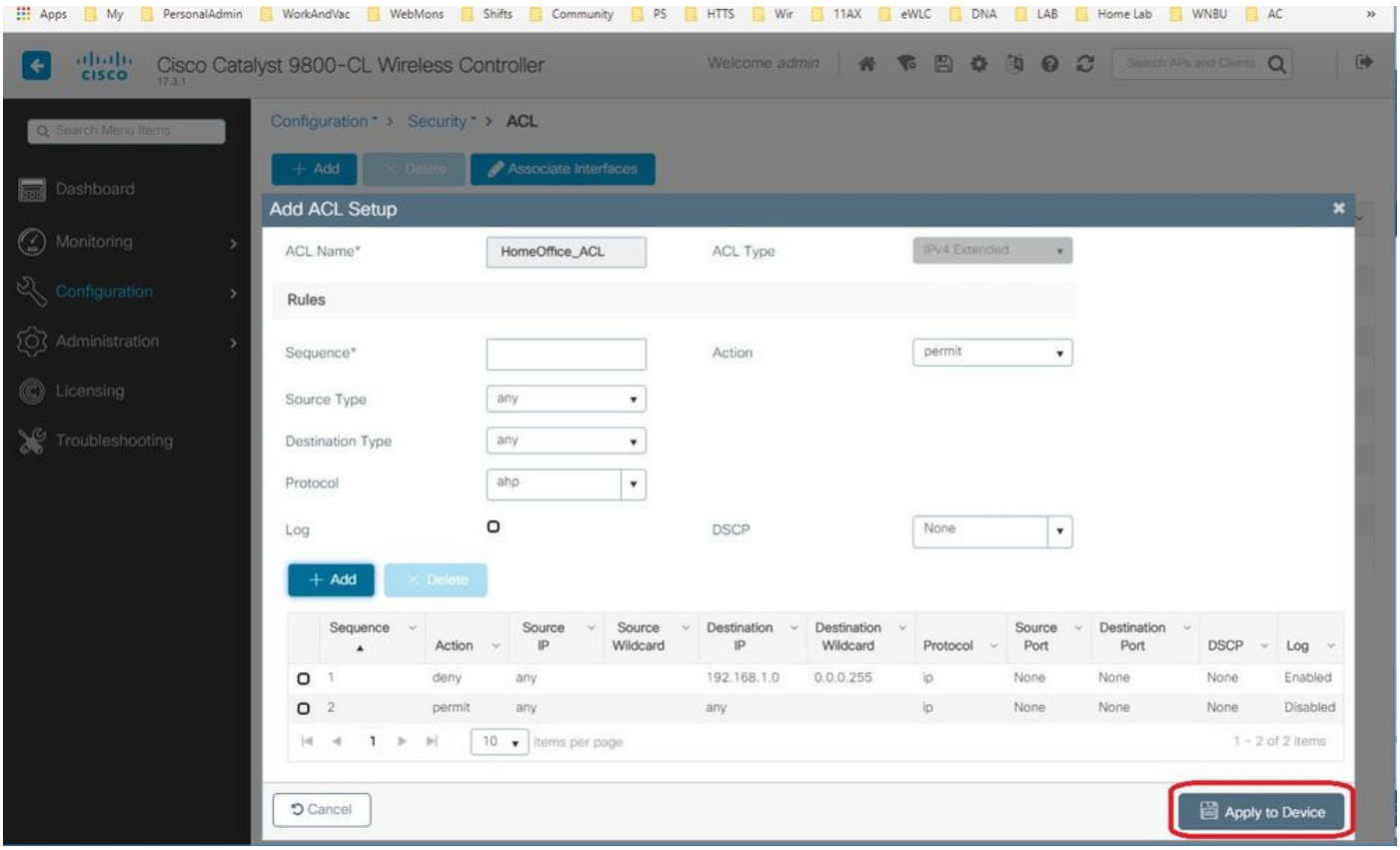
如果选择源类型为网络，则必须指定源IP地址和源通配符掩码。

在本例中，从任何主机到子网192.168.1.0/24的所有流量都集中交换（拒绝），其余所有流量都在本地交换（允许）。



步骤4.如果需要日志，请选中Log复选框，然后选择Add。

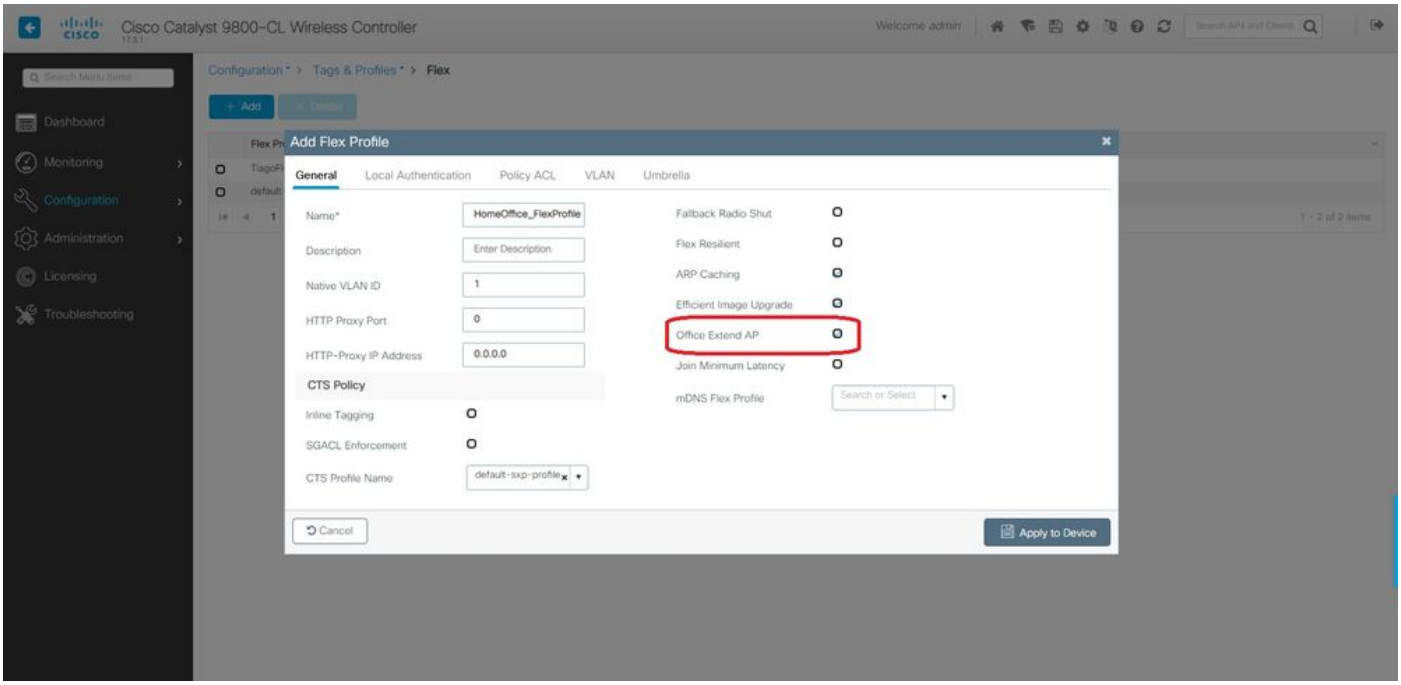
步骤5.添加其余规则并选择Apply to Device。



将ACL策略链接到已定义的ACL

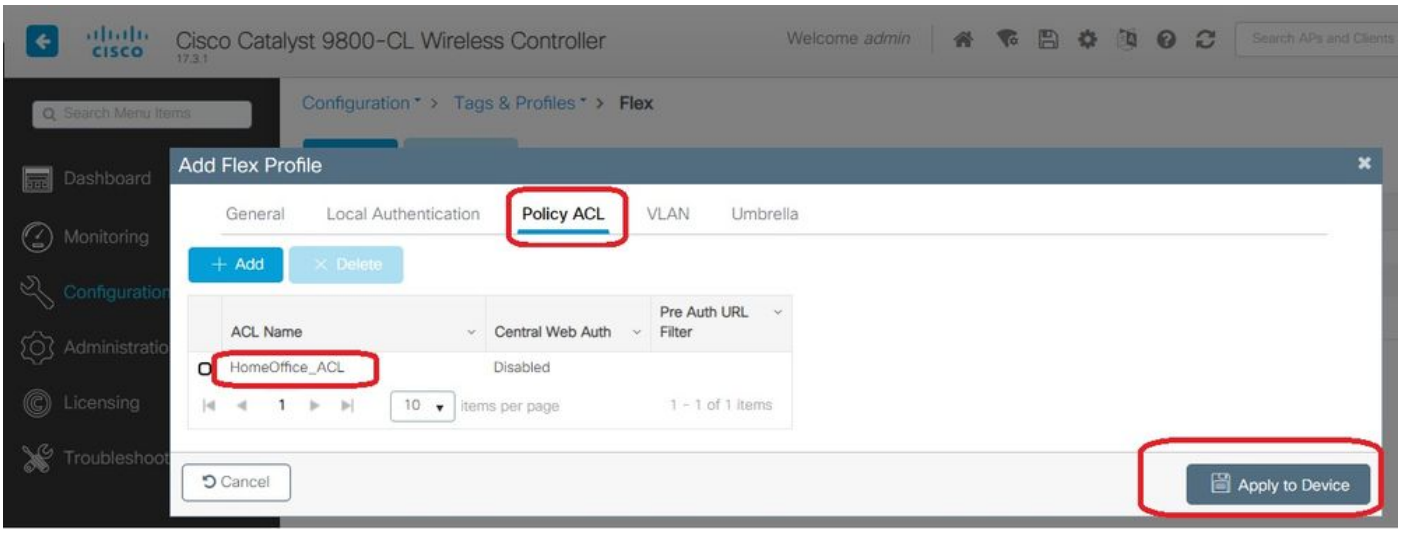
步骤1.创建新的Flex Profile。转至Configuration > Tags & Profiles > Flex。选择Add。

步骤2.输入名称并启用OEAP。另外，确保本征VLAN ID是AP交换机端口中的VLAN ID。



注意：启用Office-Extend模式时，链路加密也默认启用，即使在AP加入配置文件中禁用链路加密，也无法更改。

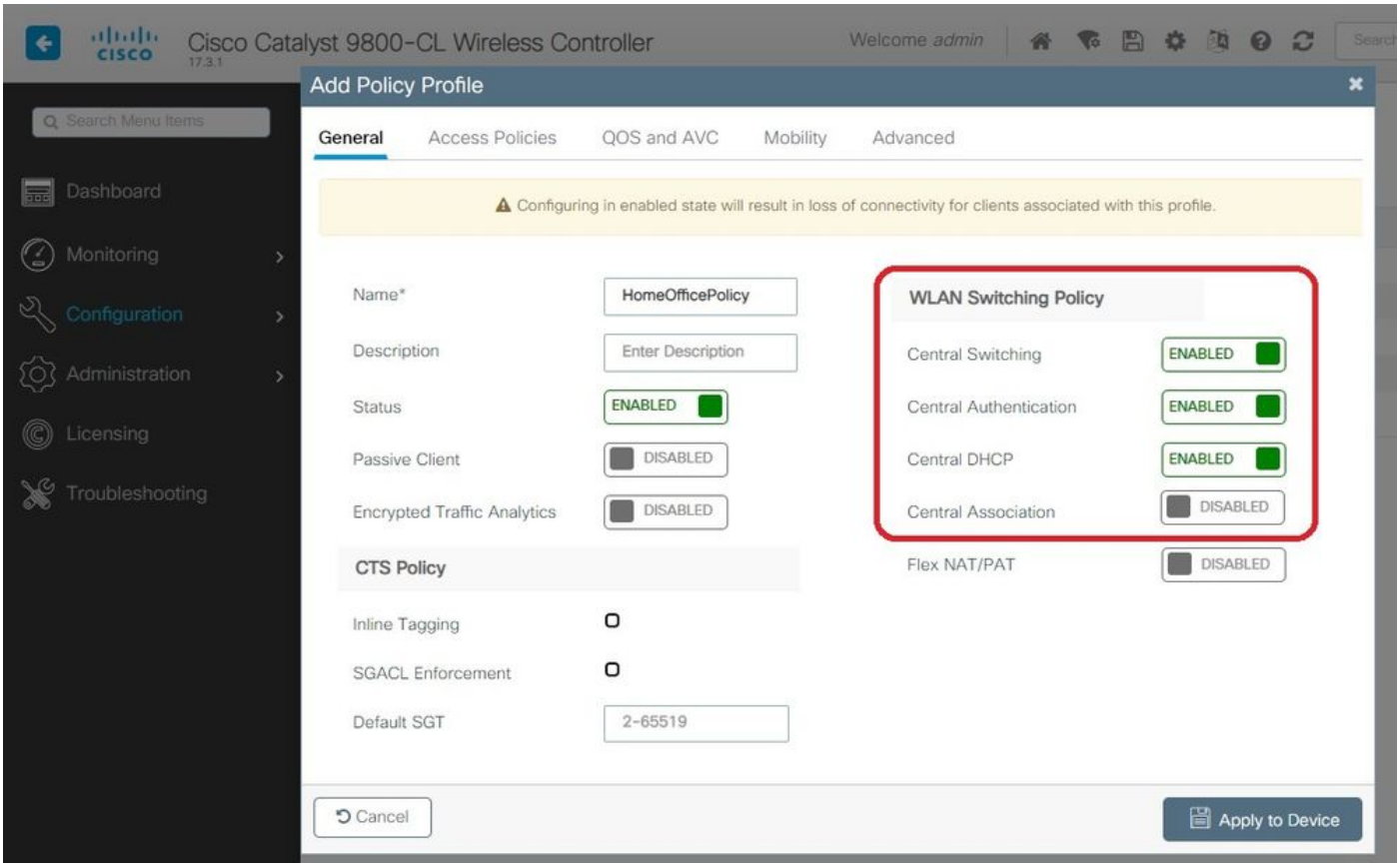
步骤3.移至Policy ACL选项卡并选择Add。此处将ACL添加到配置文件并应用到设备。



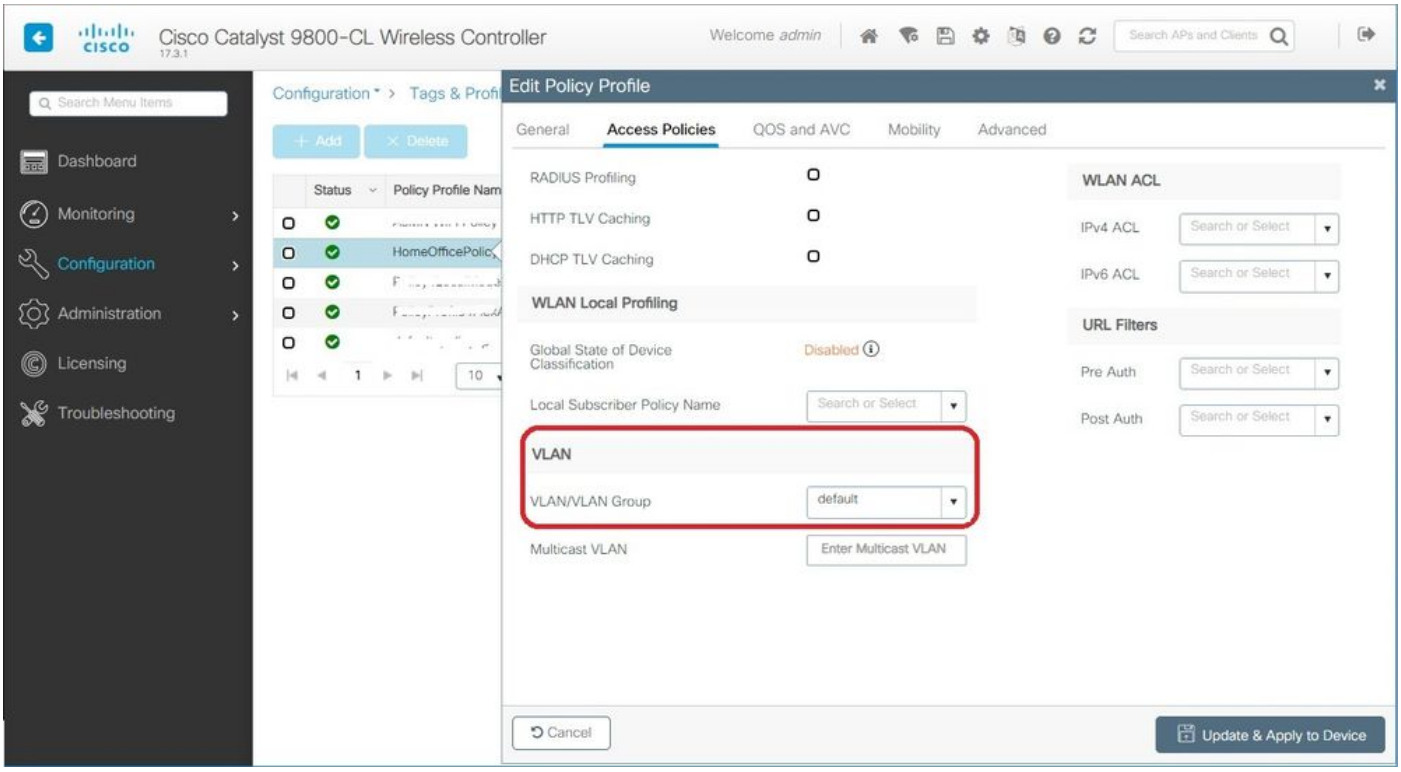
配置无线配置文件策略和拆分MAC ACL名称

步骤1.创建WLAN配置文件。在本示例中，它使用名为HomeOffice的SSID和WPA2-PSK安全。

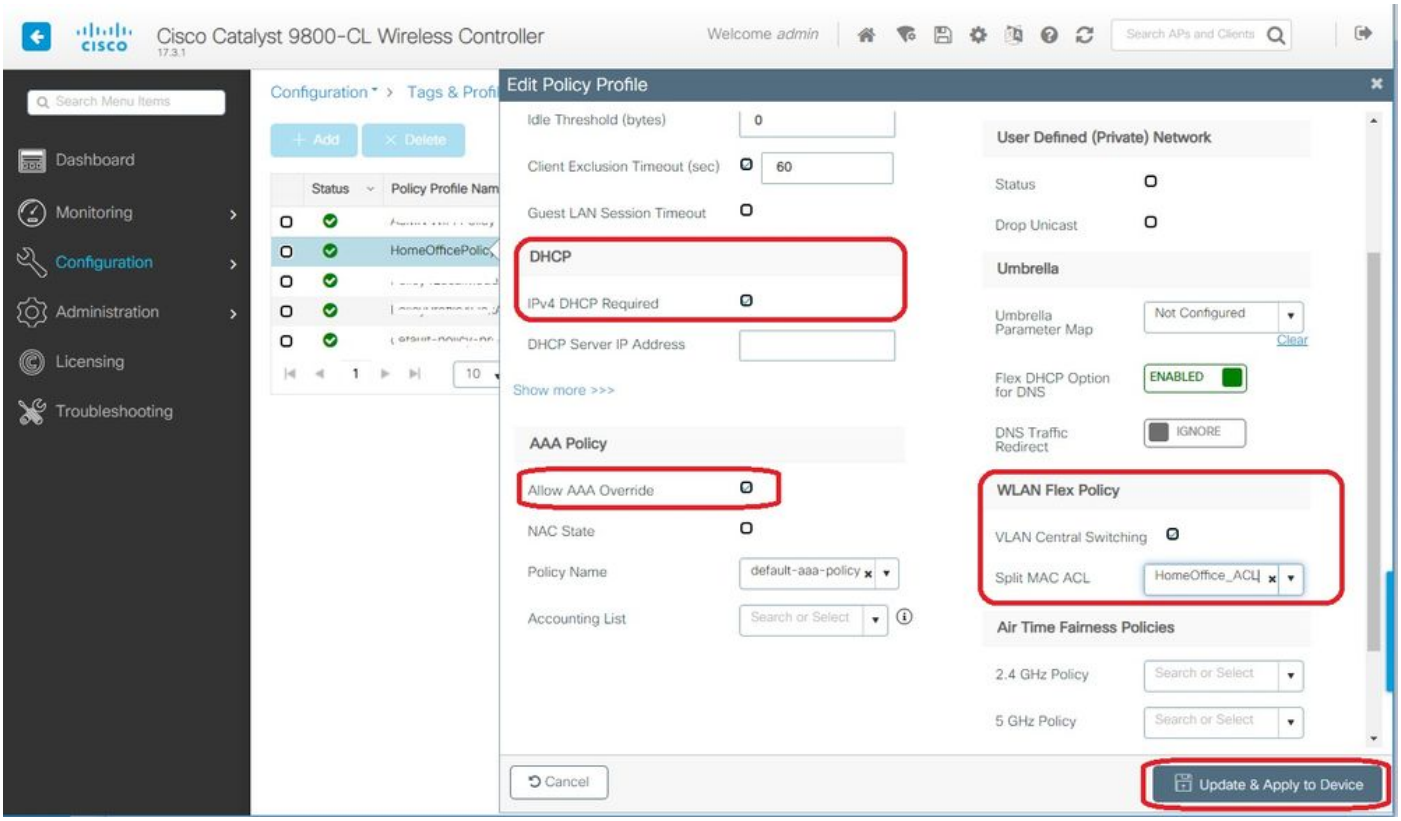
步骤2.创建策略配置文件。转到配置>标记>策略，并选择添加。在常规下，确保此配置文件是集中交换的策略，如本例所示：



步骤3.在Policy Profile中，转到Access Policies并定义要集中交换的流量的VLAN。客户端在分配给此VLAN的子网中获取IP地址。



步骤4.要在AP上配置本地拆分隧道，您需要确保已在WLAN上启用DCHP Required。这可确保与拆分WLAN关联的客户端执行DHCP。您可以在Advanced选项卡下的Policy Profile中启用此选项。启用IPv4 DHCP Required复选框。在WLAN Flex Policy设置下，从Split MAC ACL下拉列表中选择之前创建的拆分MAC ACL。选择Apply to Device:



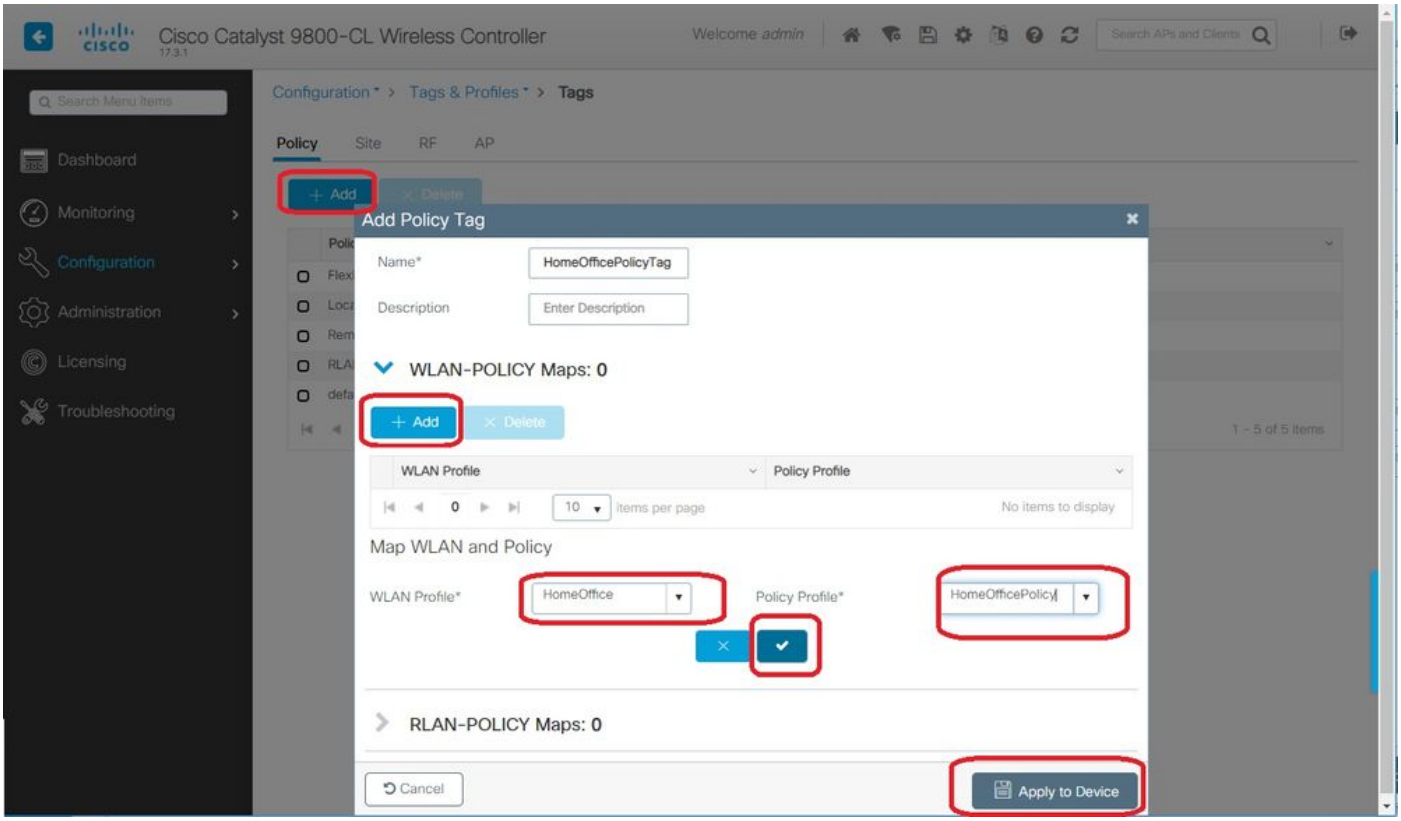
注意：Apple iOS客户端需要在DHCP提供中设置选项6(DNS)，以便切分隧道工作。

将WLAN映射到策略配置文件

步骤1.选择Configuration > Tags & Profiles > Tags。在Policy选项卡中，选择Add。

步骤2.输入Tag Policy的Name，在WLAN-POLICY Maps选项卡下，选择Add。

步骤3.从WLAN配置文件下拉列表中选择WLAN配置文件，然后从策略配置文件下拉列表中选择策略配置文件。选择刻度图标，然后选择应用到设备。

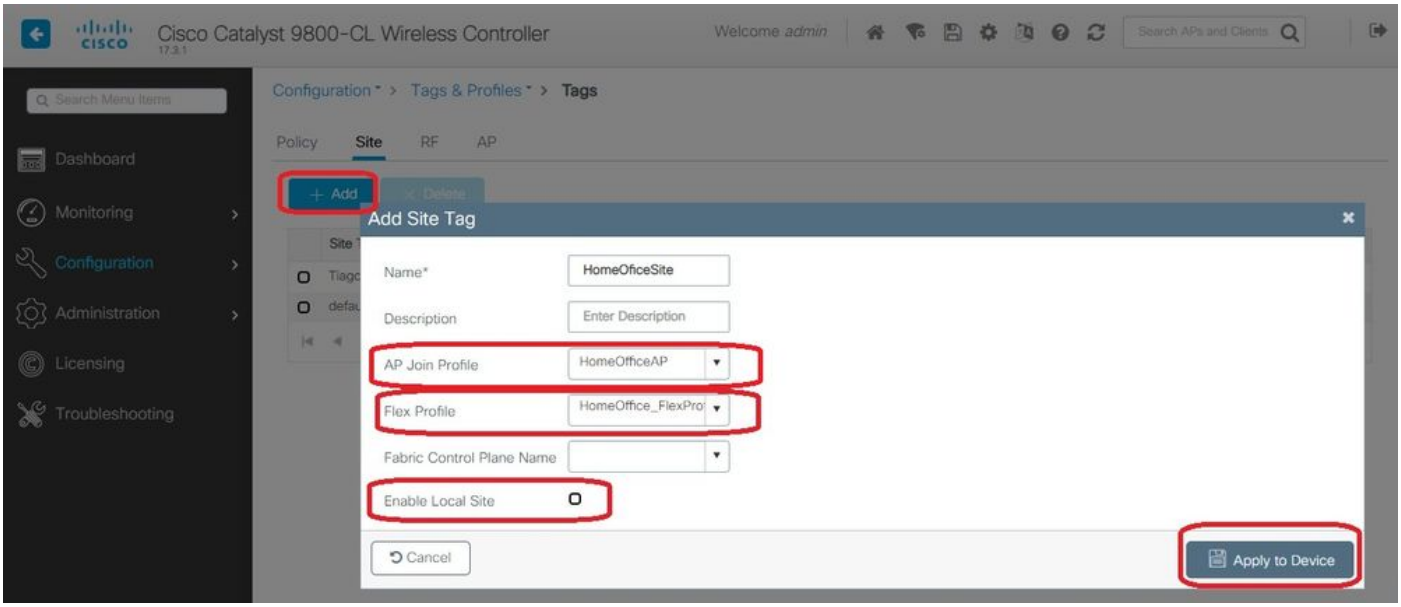


配置AP加入配置文件并与站点标记关联

步骤1.导航至Configuration > Tags & Profiles > AP Join，然后选择Add。输入名称。或者，您可以启用SSH以允许进行故障排除，然后在不需要时禁用它。

步骤2.选择Configuration > Tags & Profiles > Tags。在“站点”选项卡中，选择“添加”。

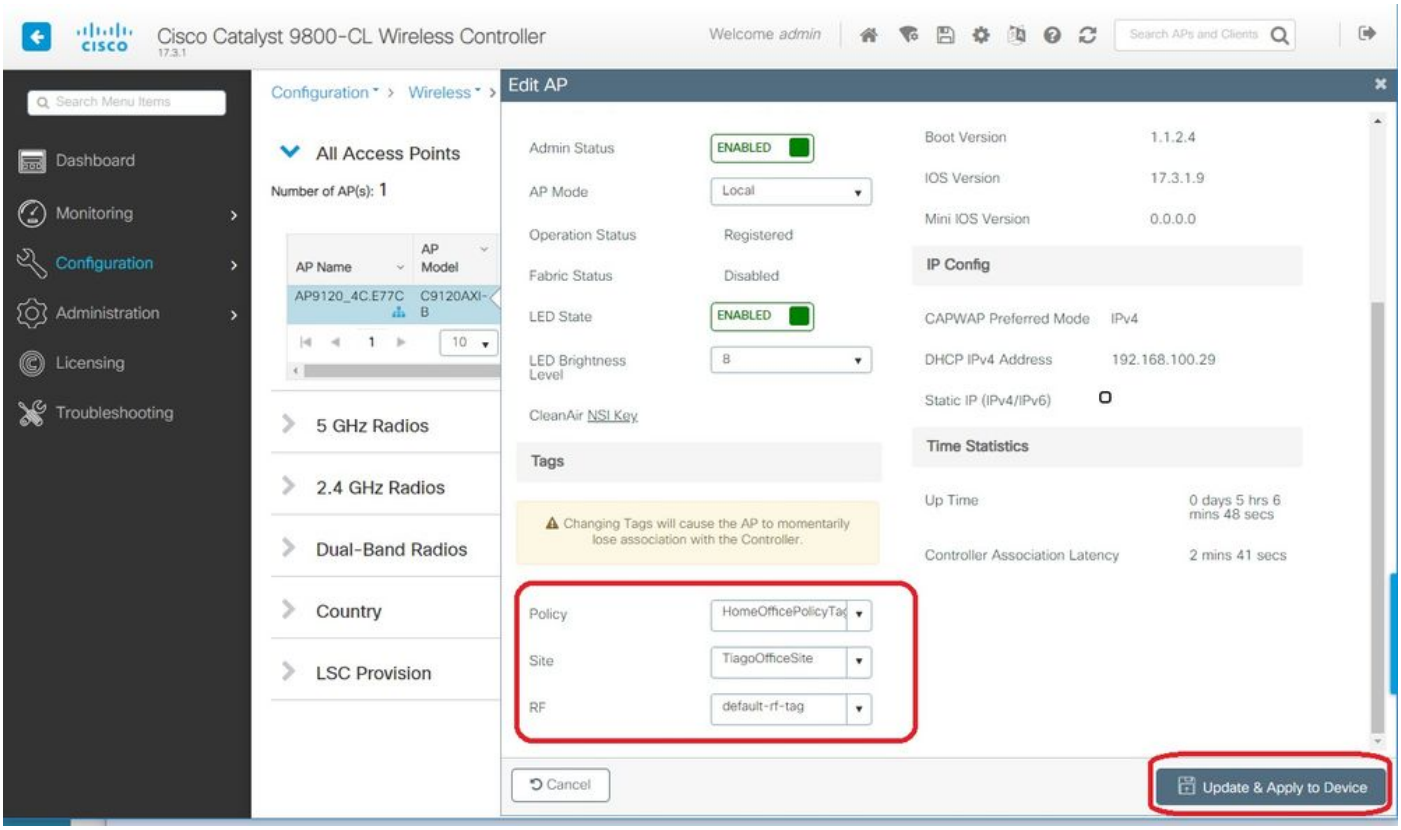
步骤3.输入站点标签的名称，取消选中启用本地站点，然后从下拉列表中选择AP加入配置文件和弹性配置文件（之前创建）。然后应用到设备。



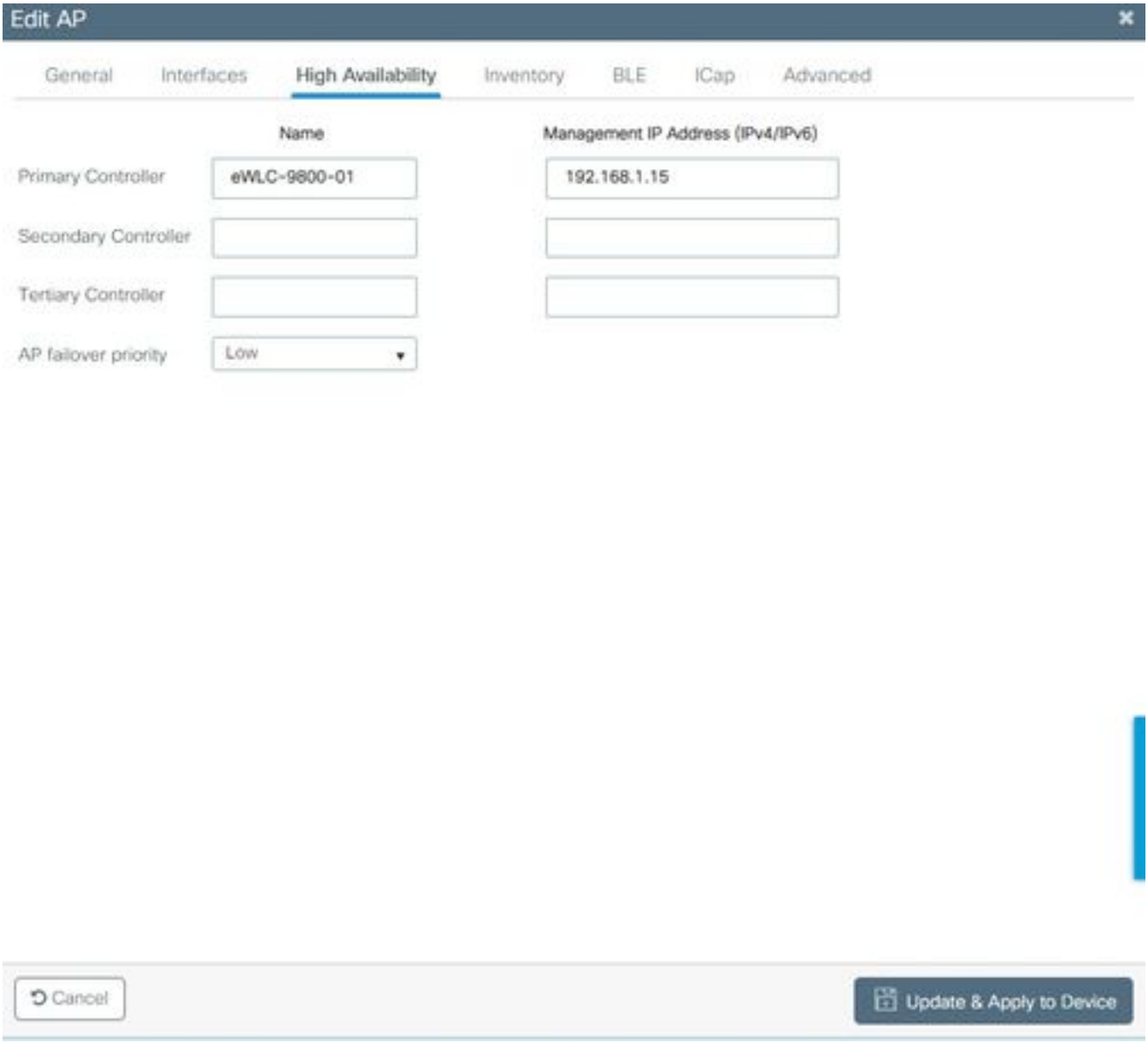
将策略标记和站点标记附加到接入点

选项1.此选项要求您一次配置1个AP。转至Configuration > Wireless > Access Points。选择要移动

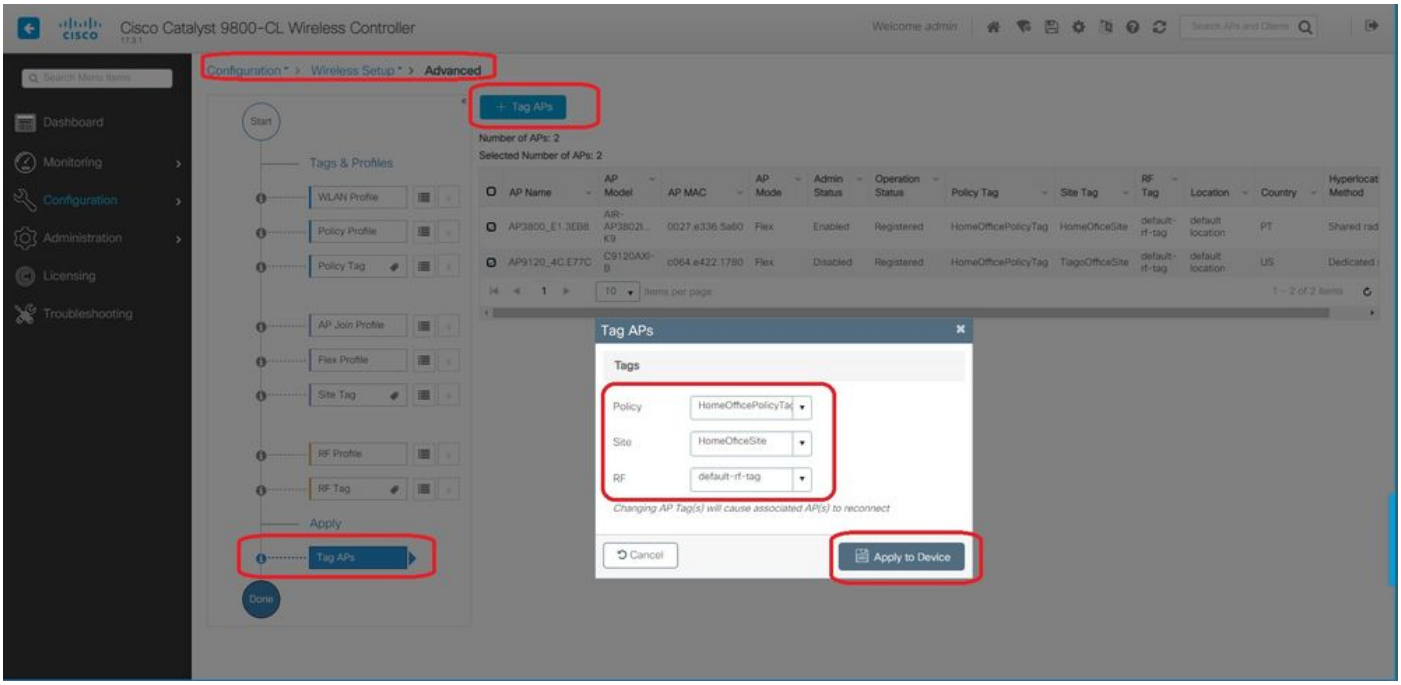
到家庭办公室的AP，然后选择家庭办公室标签。选择更新并应用到设备：



还建议配置主控制器，以便AP知道WLC在部署到家庭办公室后要到达的IP/名称。您可以直接编辑AP到高可用性选项卡：



选项2.此选项允许您同时配置多个AP。导航至Configuration > Wireless Setup > Advanced > Tag APs。选择之前创建的标记，然后选择应用到设备。



AP将重新启动，并使用新设置重新加入WLC。

验证

您可以通过GUI或CLI验证配置。以下是CLI中的结果配置：

```
!
ip access-list extended HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255 log
2 permit ip any any log
!
wireless profile flex HomeOffice_FlexProfile
acl-policy HomeOffice_ACL
office-extend
!
wireless profile policy HomeOfficePolicy
no central association
aaa-override
flex split-mac-acl HomeOffice_ACL
flex vlan-central-switching
ipv4 dhcp required
vlan default
no shutdown
!
wireless tag site HomeOficeSite
flex-profile HomeOffice_FlexProfile
no local-site
!
wireless tag policy HomeOfficePolicyTag
wlan HomeOffice policy HomeOfficePolicy
!
wlan HomeOffice 5 HomeOffice
security wpa psk set-key ascii 0 xxxxxxx
no security wpa akm dot1x
security wpa akm psk
no shutdown
!
ap 70db.98e1.3eb8
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
ap c4f7.d54c.e77c
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
```

检查AP配置：

```
eWLC-9800-01#show ap name AP3800_E1.3EB8 config general

Cisco AP Name : AP3800_E1.3EB8
=====================================================

Cisco AP Identifier : 0027.e336.5a60
...
MAC Address : 70db.98e1.3eb8
IP Address Configuration : DHCP
IP Address : 192.168.1.99
IP Netmask : 255.255.255.0
```

```
Gateway IP Address : 192.168.1.254
...
SSH State : Enabled
Cisco AP Location : default location
Site Tag Name : HomeOficeSite
RF Tag Name : default-rf-tag
Policy Tag Name : HomeOfficePolicyTag
AP join Profile : HomeOfficeAP
Flex Profile : HomeOffice_FlexProfile
Primary Cisco Controller Name : eWLC-9800-01
Primary Cisco Controller IP Address : 192.168.1.15
...
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
...
```

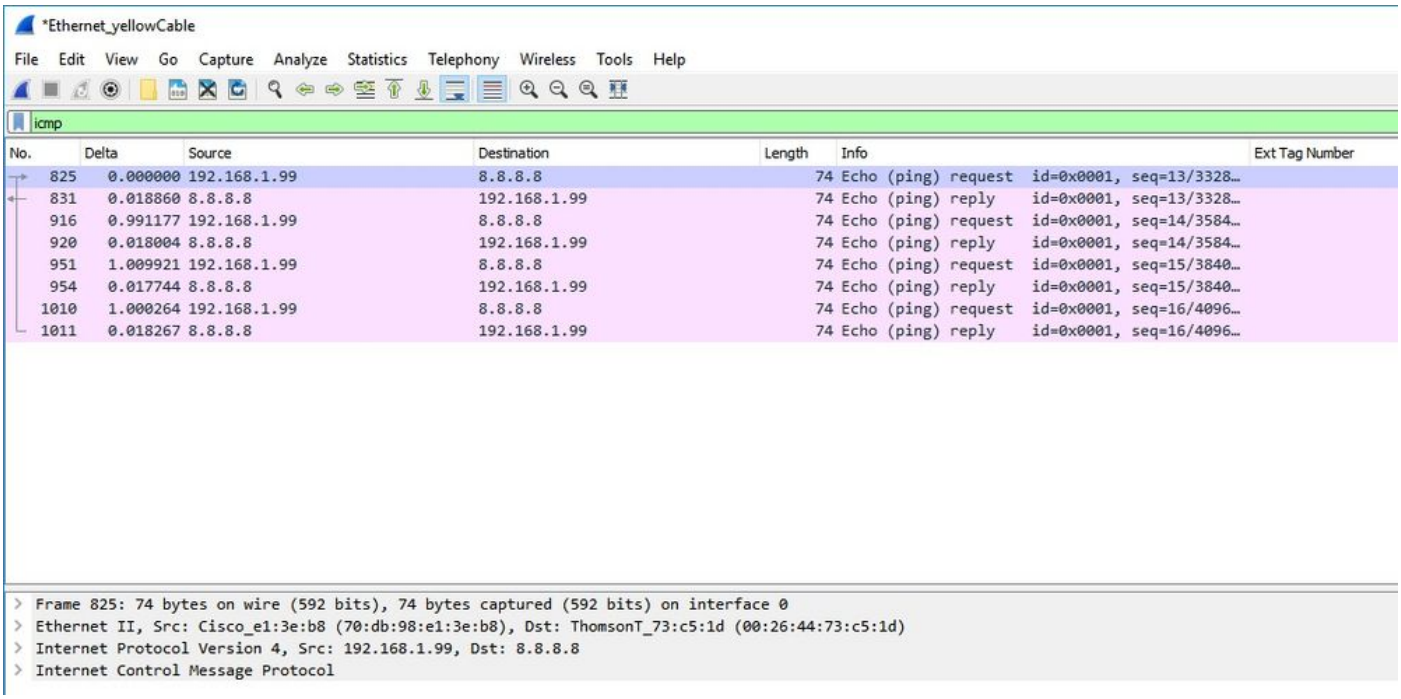
您可以直接连接到AP，也可以验证配置：

```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

AP3800_E1.3EB8#show capwap client detailrcb
SLOT 0 Config

SSID : HomeOffice
Vlan Id : 0
Status : Enabled
...
otherFlags : DHCP_REQUIRED VLAN_CENTRAL_SW
...
Profile Name : HomeOffice
...
```

```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name :
ssh status : Enabled
ApMode : FlexConnect
ApSubMode : Not Configured
Link-Encryption : Enabled
OfficeExtend AP : Enabled
Discovery Timer : 10
Heartbeat Timer : 30
...
```

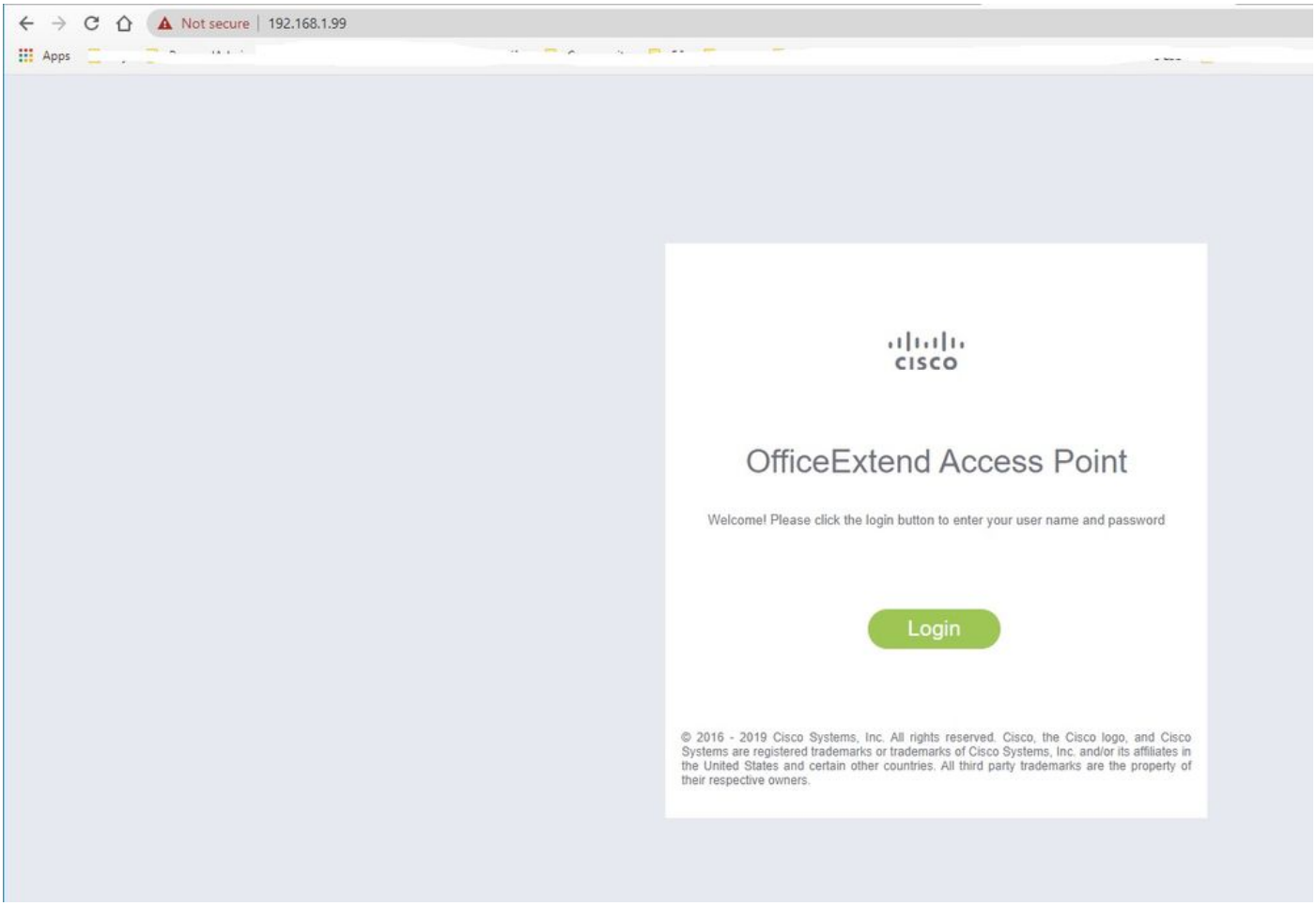
以下是数据包捕获的示例，显示本地交换的流量。在此，测试是从IP为192.168.1.98的客户端对Google DNS服务器执行“ping”操作，然后对192.168.1.254执行ping操作。您可以看到IP地址为192.168的ICMP。1.99由于AP NAT在本地传输流量而发送到Google DNS。由于流量在DTLS隧道

中进行加密，并且仅显示应用数据帧，因此没有icmp到192.168.1.254。

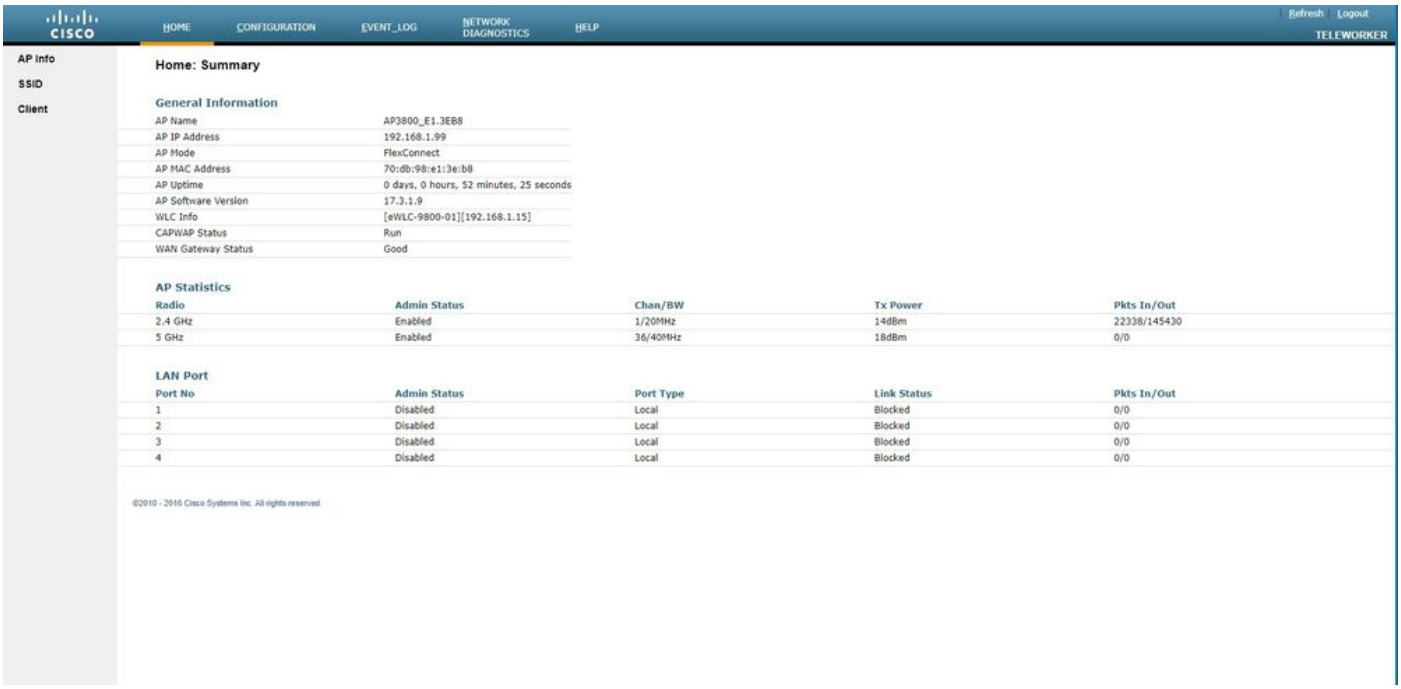


注意：本地交换的流量由AP进行NAT，因为在正常情况下，客户端子网属于Office网络，而家庭办公室的本地设备不知道如何到达客户端子网。AP使用本地家庭办公室子网中的AP IP地址转换客户端流量。

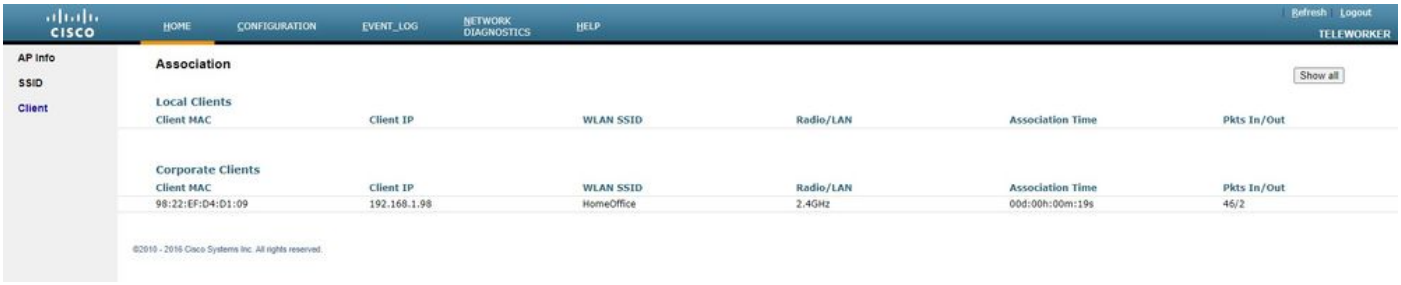
您可以访问OEAP GUI打开浏览器并在URL中键入AP IP地址。默认凭证是admin/admin，您必须在初始登录时更改这些凭证。



登录后，您可以访问GUI:



您可以访问OEAP中的典型信息，如AP信息、SSID和连接的客户端：



相关文档

[了解Catalyst 9800无线控制器上的FlexConnect]

[FlexConnect的分割隧道]

[在Catalyst 9800 WLC上配置OEAP和RLAN]