在Catalyst 9800无线控制器上具有802.1x AAA覆盖的FlexConnect WLAN

目录

简介

本文档介绍如何设置弹性无线LAN控制器(9800 WLC)和FlexConnect模式接入点(AP)以及使用虚拟局域网(VLAN)身份验证、授权和记帐(AAA)本地交换的802.1x无线局域网(WLAN)。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800 WLC配置模式
- FlexConnect

使用的组件

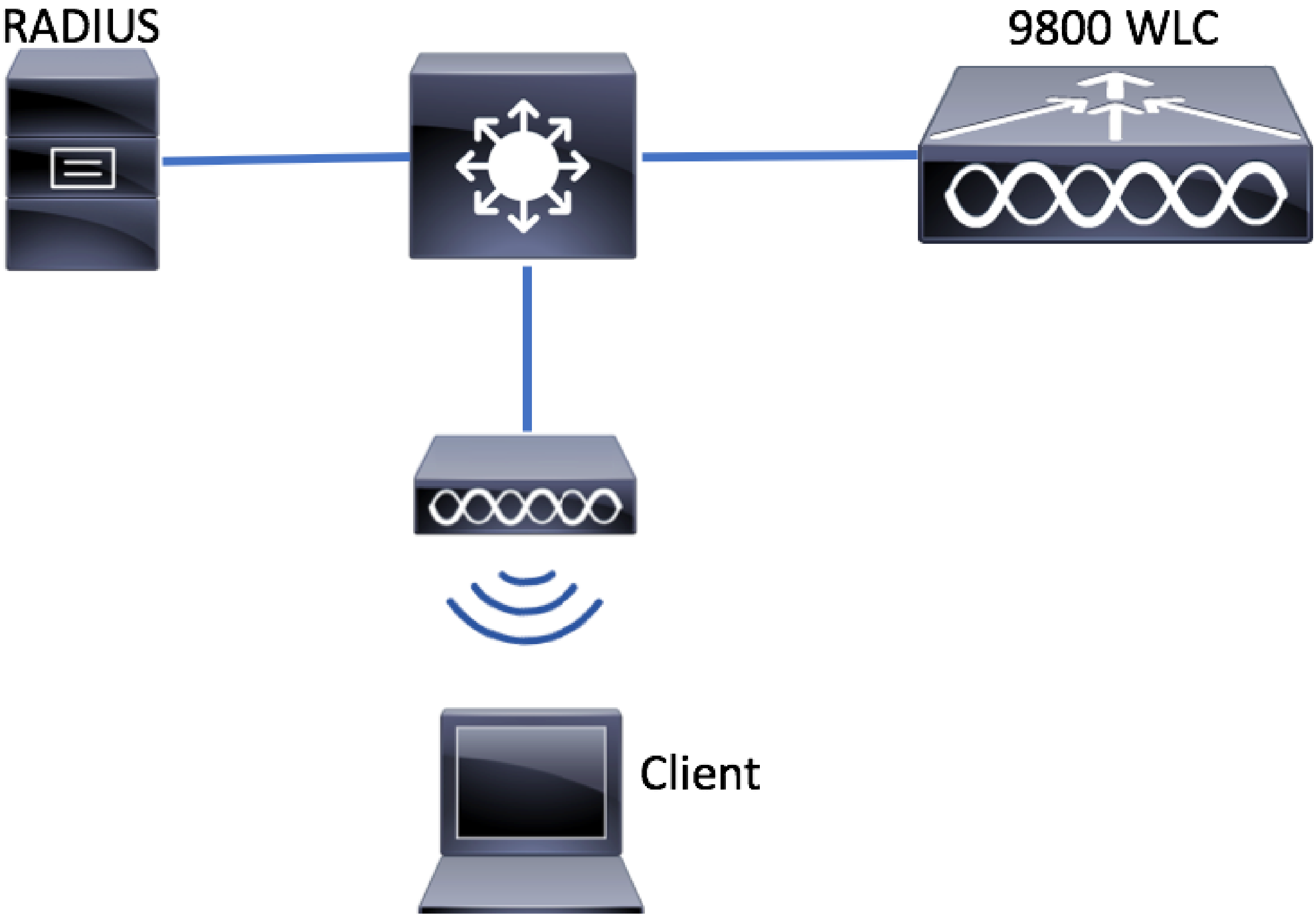
本文档中的信息基于以下软件和硬件版本：

- 9800 WLC v16.10

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



配置

9800 WLC上的AAA配置

您可以按照以下链接的说明进行操作：

9800 WLC上的AAA配置

WLAN 配置

您可以按照以下链接的说明进行操作：

WLAN 配置

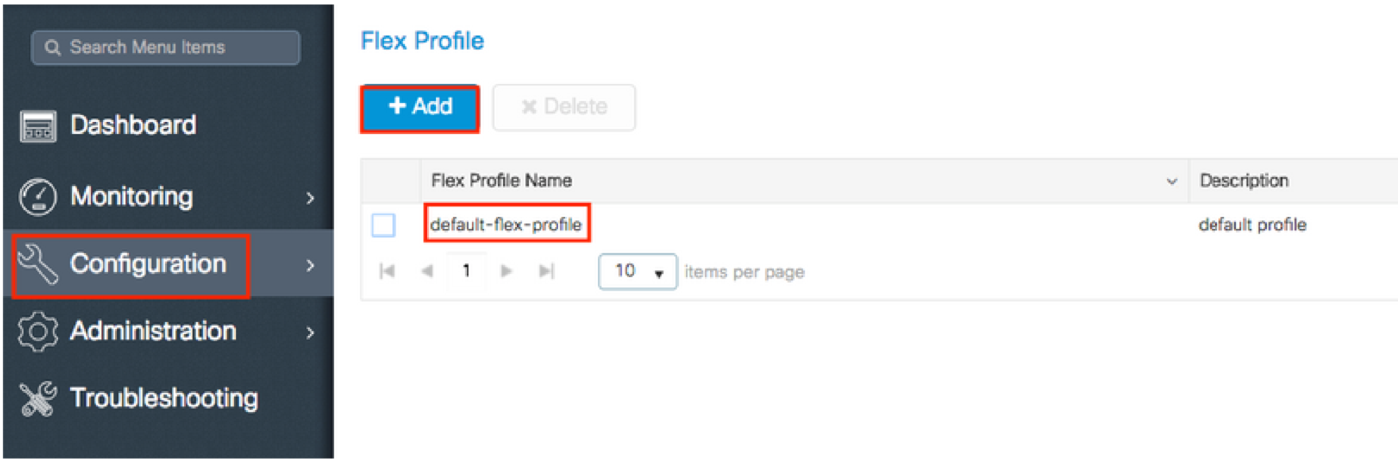
将AP设置为FlexConnect模式

与AireOS配置不同，在9800 WLC上，无法直接从AP配置AP本地模式或flexconnect模式。按照以下步骤在FlexConnect模式下配置AP。

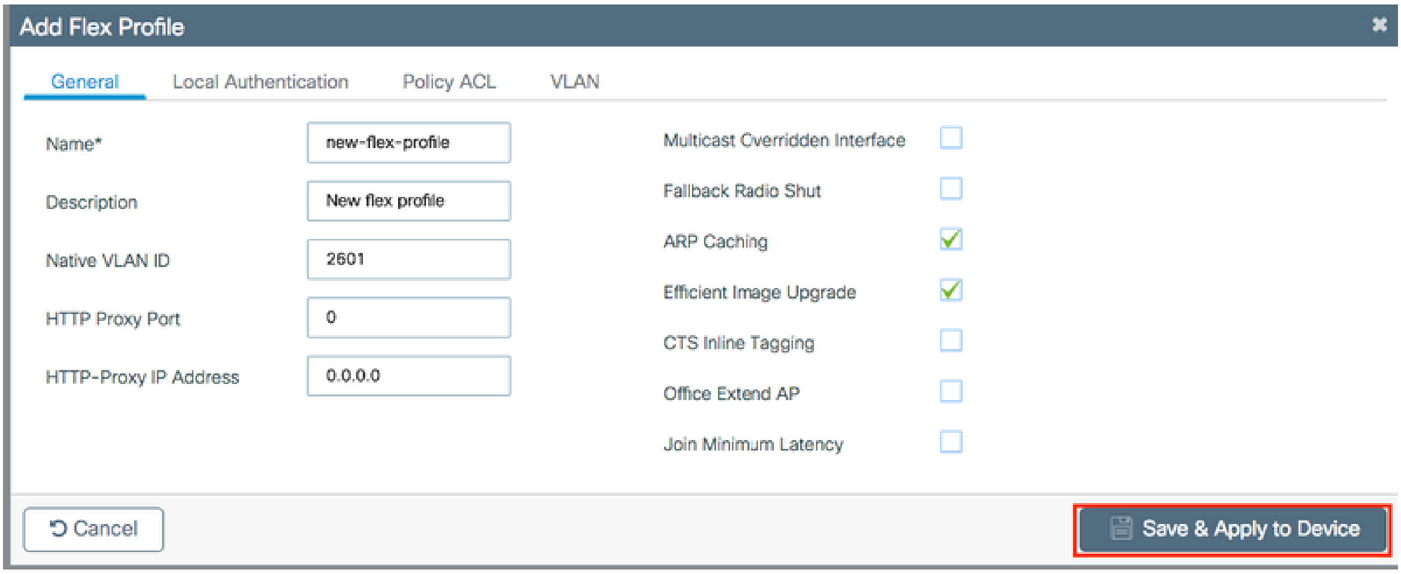
GUI

步骤1.配置Flex Profile。

导航至 **配置>标记和配置文件>Flex** 并修改默认**Flex配置文件**或单击**+Add**创建新配置文件。



	Flex Profile Name	Description
□	default-flex-profile	default profile

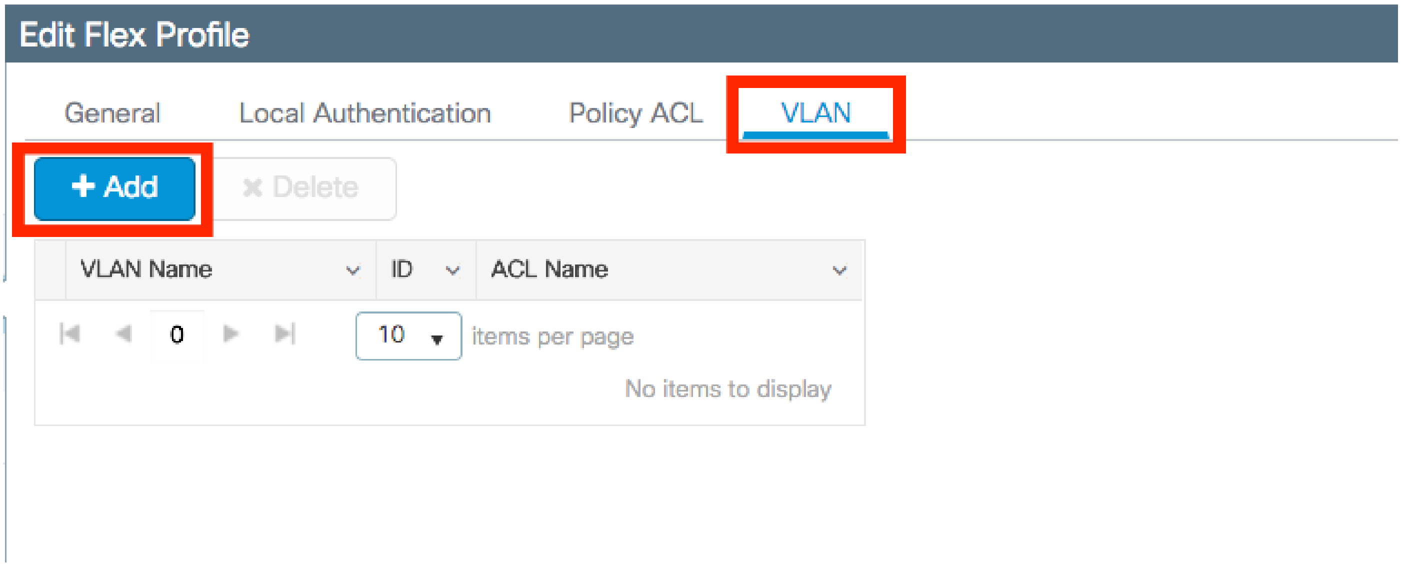


Name*	new-flex-profile
Description	New flex profile
Native VLAN ID	2601
HTTP Proxy Port	0
HTTP-Proxy IP Address	0.0.0.0

Multicast Overridden Interface	□
Fallback Radio Shut	□
ARP Caching	☑
Efficient Image Upgrade	☑
CTS Inline Tagging	□
Office Extend AP	□
Join Minimum Latency	□

步骤2.添加所需的VLAN（默认WLAN的VLAN或从ISE推送的VLAN）。

> **注意**：在策略配置文**件配置**部分的步骤3中，选择分配给SSID的默认VLAN。如果在该步骤中使用VLAN名称，请确保在Flex Profile配置中使用相同的VLAN名称，否则客户端将无法连接到WLAN。

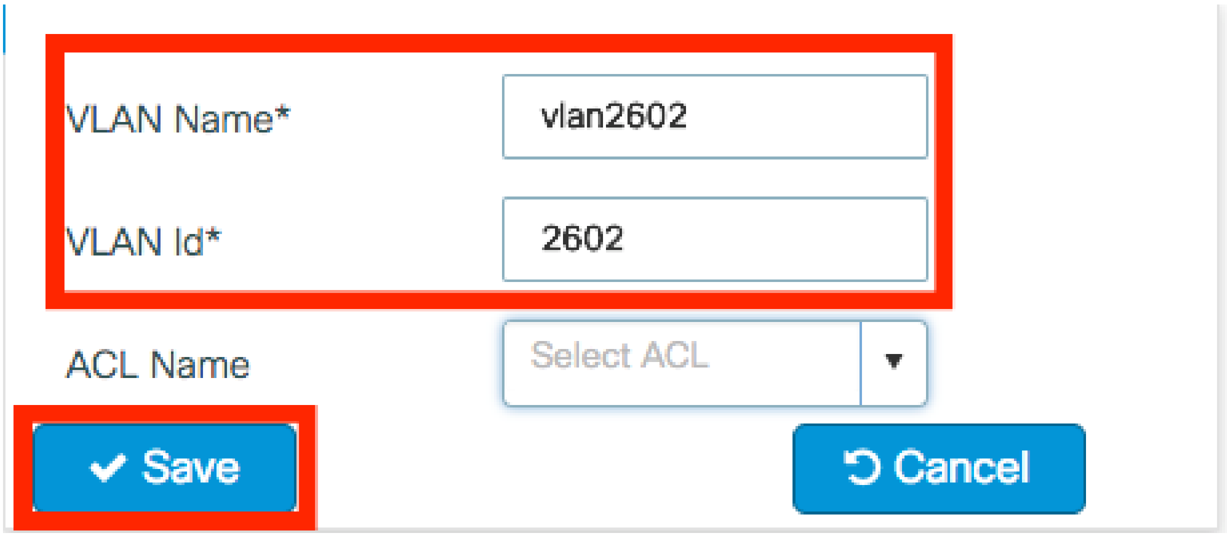


Edit Flex Profile

VLAN Name	ID	ACL Name

No items to display

您可以选择为每个VLAN添加特定ACL。

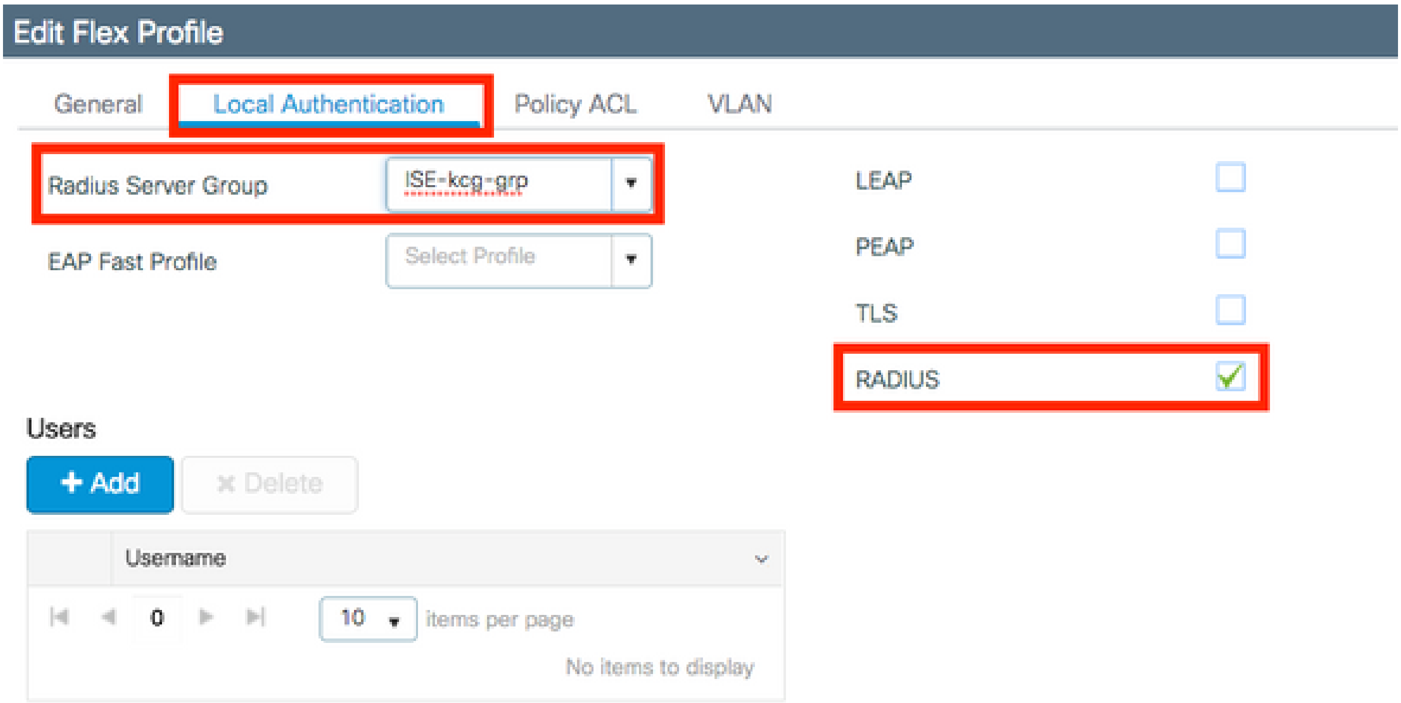


VLAN Name*: vlan2602

VLAN Id*: 2602

ACL Name: Select ACL

或者，分配Radius服务器组以允许FlexConnect AP执行本地身份验证。



Radius Server Group: ISE-kcg-grp

EAP Fast Profile: Select Profile

LEAP □

PEAP □

TLS □

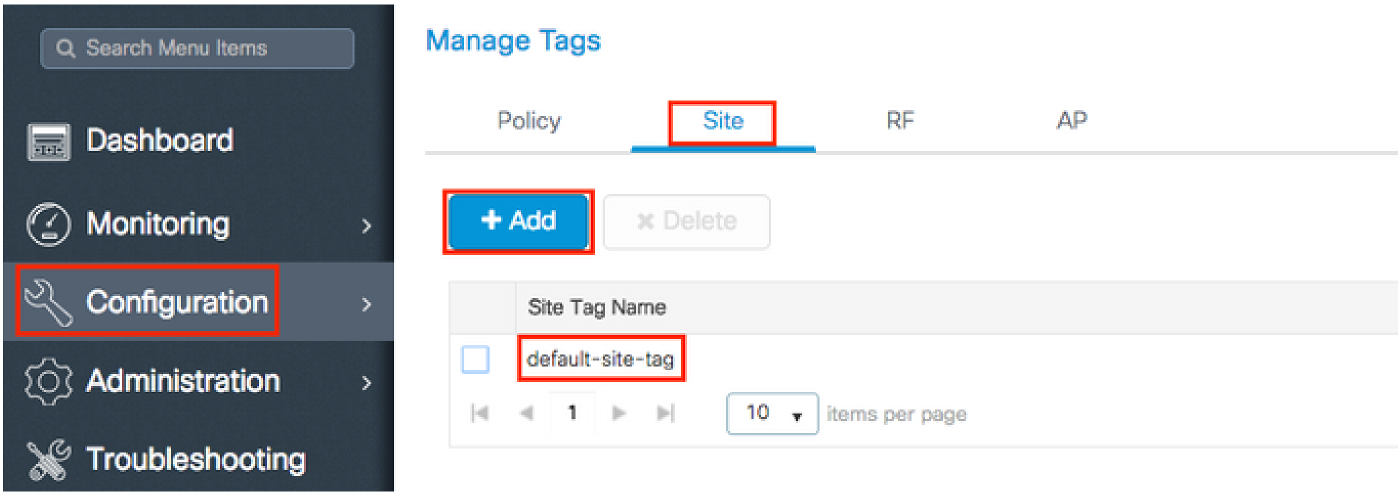
RADIUS ☑

	Username

No items to display

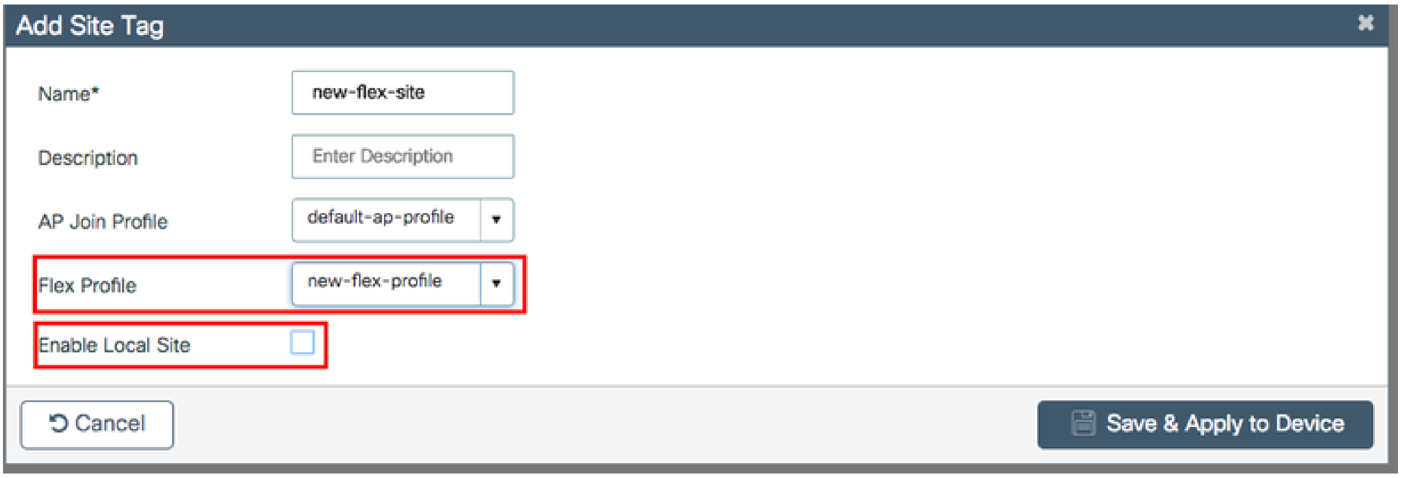
步骤3.配置站点标记。

导航**至配置>标记和配置文件>标记>站点**。修改**default-site-tag**（默认为分配给所有AP的标记）或创建新标记(单击**+添加**以创建新标记)。



	Site Tag Name
□	default-site-tag

确保禁用“**启用本地站**点”选项，否**则“Flex**配置文件”选项不可用。



Name*: new-flex-site

Description: Enter Description

AP Join Profile: default-ap-profile

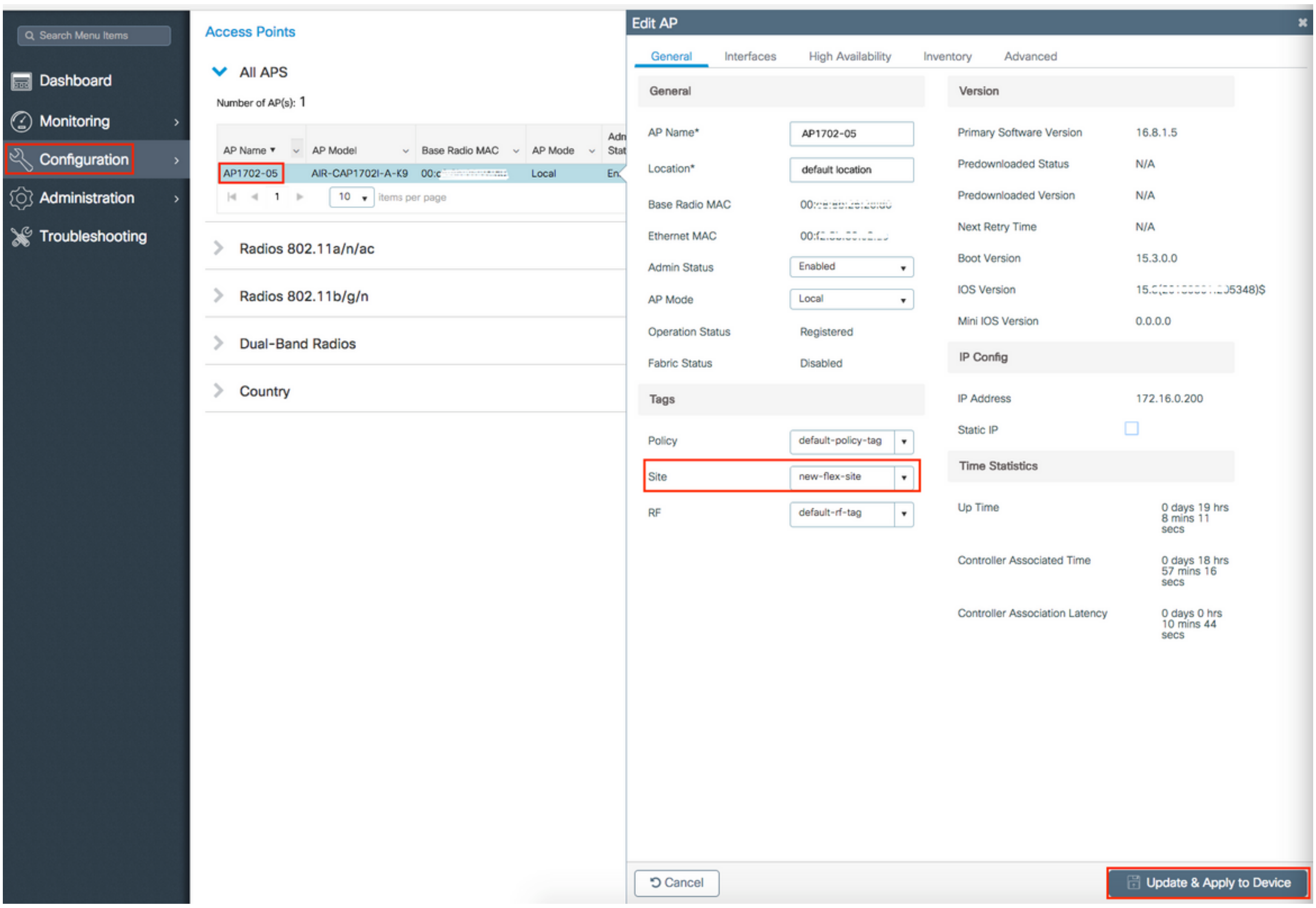
Flex Profile: new-flex-profile

Enable Local Site □

注意：任何获取已启用启用本地站点**的站点标**记的AP都配置为本地模式。同样，任何获取站点标记且禁用**启用本地站**点的AP都配置为flexconnect模式。

步骤4.使AP关联到9800 WLC并分配步骤2中配置的站点标记。

导航至**Configuration > Wireless > Access Points > AP name**并设置Site标记。然后单**击更新并应用到设**备以设置更改。



Number of AP(s): 1

AP Name	AP Model	Base Radio MAC	AP Mode	Admin Status
AP1702-05	AIR-CAP1702I-A-K9	00:[redacted]	Local	En

10 items per page

General

AP Name*	AP1702-05
Location*	default location
Base Radio MAC	00:[redacted]
Ethernet MAC	00:[redacted]
Admin Status	Enabled
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled

Tags

Policy	default-policy-tag
Site	new-flex-site
RF	default-rf-tag

Version

Primary Software Version	16.8.1.5
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	15.3.0.0
IOS Version	15.[redacted]5348)$
Mini IOS Version	0.0.0.0

IP Config

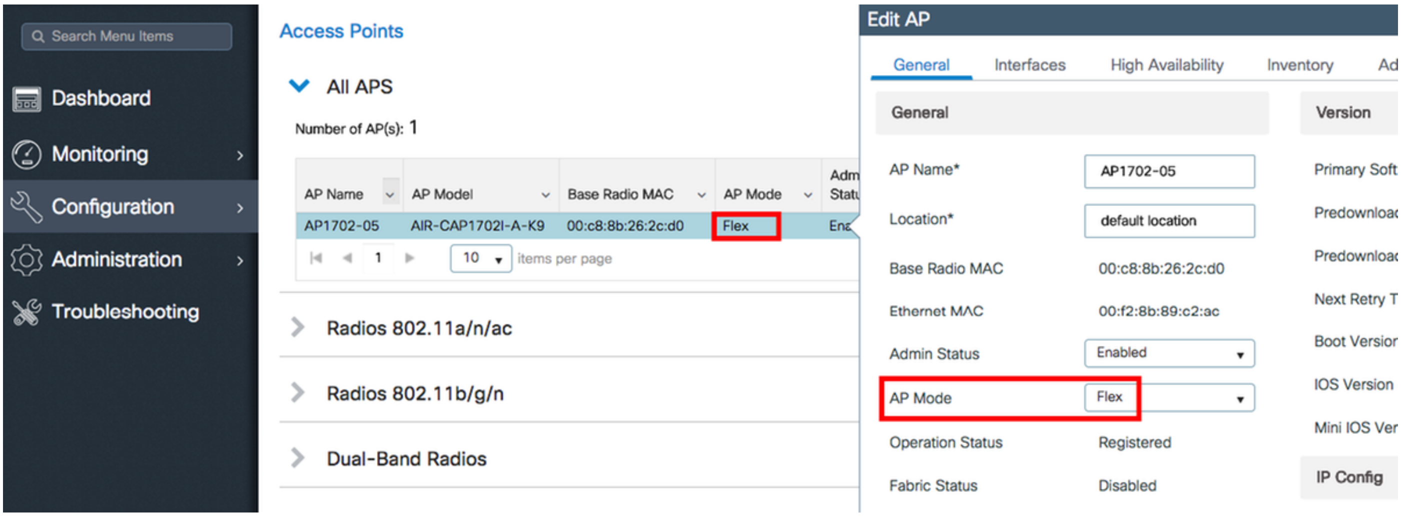
IP Address	172.16.0.200
Static IP	□

Time Statistics

Up Time	0 days 19 hrs 8 mins 11 secs
Controller Associated Time	0 days 18 hrs 57 mins 16 secs
Controller Association Latency	0 days 0 hrs 10 mins 44 secs

注意: **请注意，在更改AP上的标记后，它将失去与9800 WLC的关联，并在大约1分钟内重新加入。**

步骤5. AP重新加入后，请注意AP模式为Flex



Number of AP(s): 1

AP Name	AP Model	Base Radio MAC	AP Mode	Adm Statu
AP1702-05	AIR-CAP1702I-A-K9	00:c8:8b:26:2c:d0	Flex	Ena

General

AP Name*	AP1702-05
Location*	default location
Base Radio MAC	00:c8:8b:26:2c:d0
Ethernet MAC	00:f2:8b:89:c2:ac
Admin Status	Enabled
AP Mode	Flex
Operation Status	Registered
Fabric Status	Disabled

CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                                          : FlexConnect
```

交换机配置

配置AP所连接的交换机接口。

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

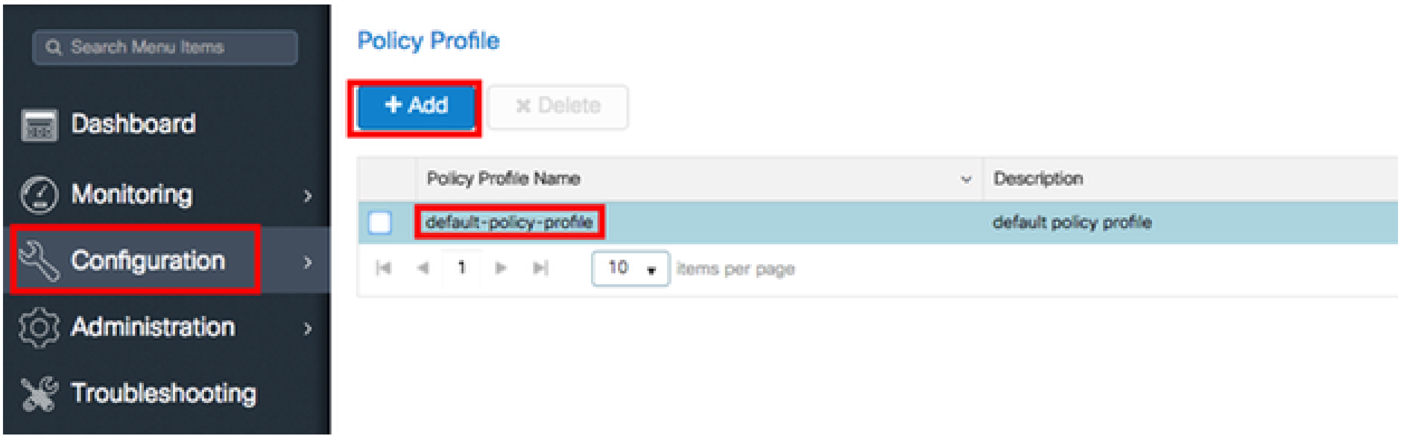
策略配置文件配置

在策略配置文件中，您可以决定将客户端分配到哪个VLAN，以及其他设置（如访问控制列表[ACL]、服务质量[QoS]、移动锚点、计时器等）。

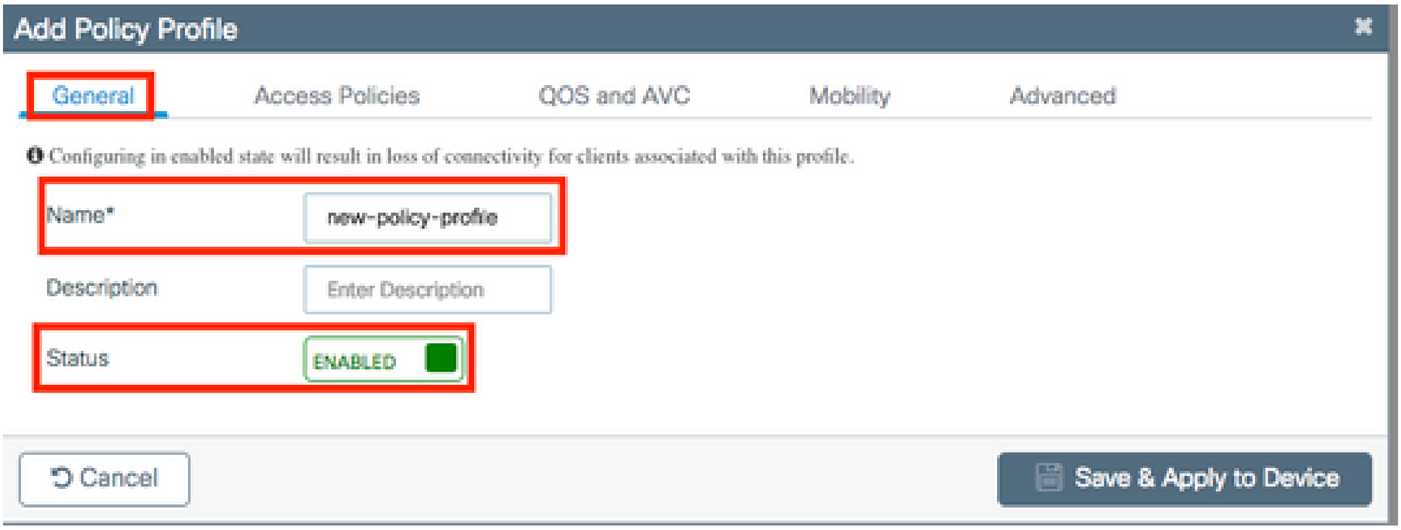
GUI

步骤1.配置要分配给WLAN的策略配置文件。

导航至**Configuration > Tags & Profiles > Policy**，然后创建新策略或修改**default-policy-profile。**



步骤2.从General选**项卡，**为Policy Profile分配名称，并将其状态更改为**ENABLED。**



Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*: new-policy-profile

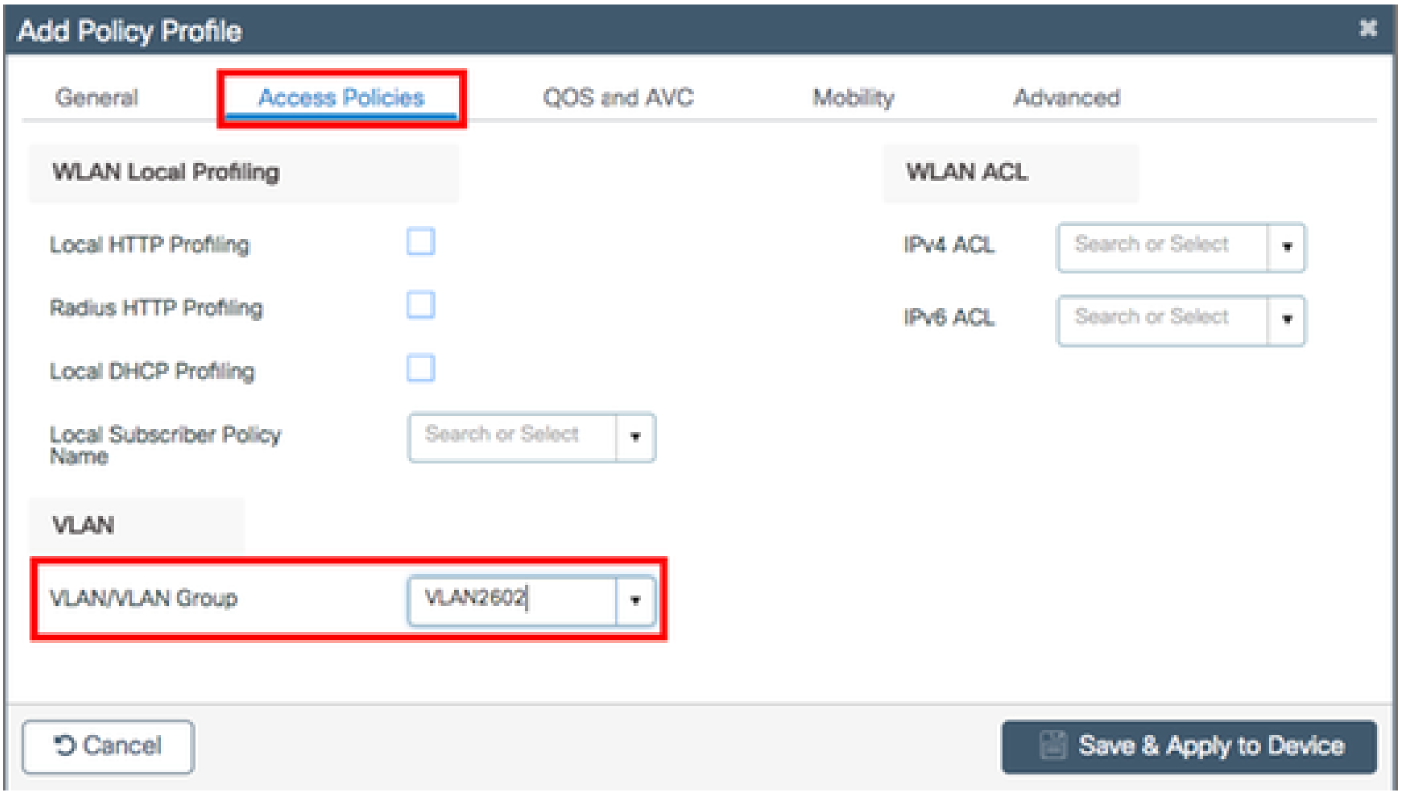
Description: Enter Description

Status: ENABLED

步骤3.从Access Policies选**项卡**分配无线客户端在默认情况下连接到此WLAN时分配给的VLAN。

您可以从下拉列表中选择一个VLAN名称，或手动键入vlan id。

> **注意**:如果从下拉列表中选择VLAN名称，请确保它与“将AP设置为FlexConnect模式”一节中第2步中**使用的VLAN名称匹配。**



WLAN Local Profiling

Local HTTP Profiling □

Radius HTTP Profiling □

Local DHCP Profiling □

Local Subscriber Policy Name: Search or Select

VLAN

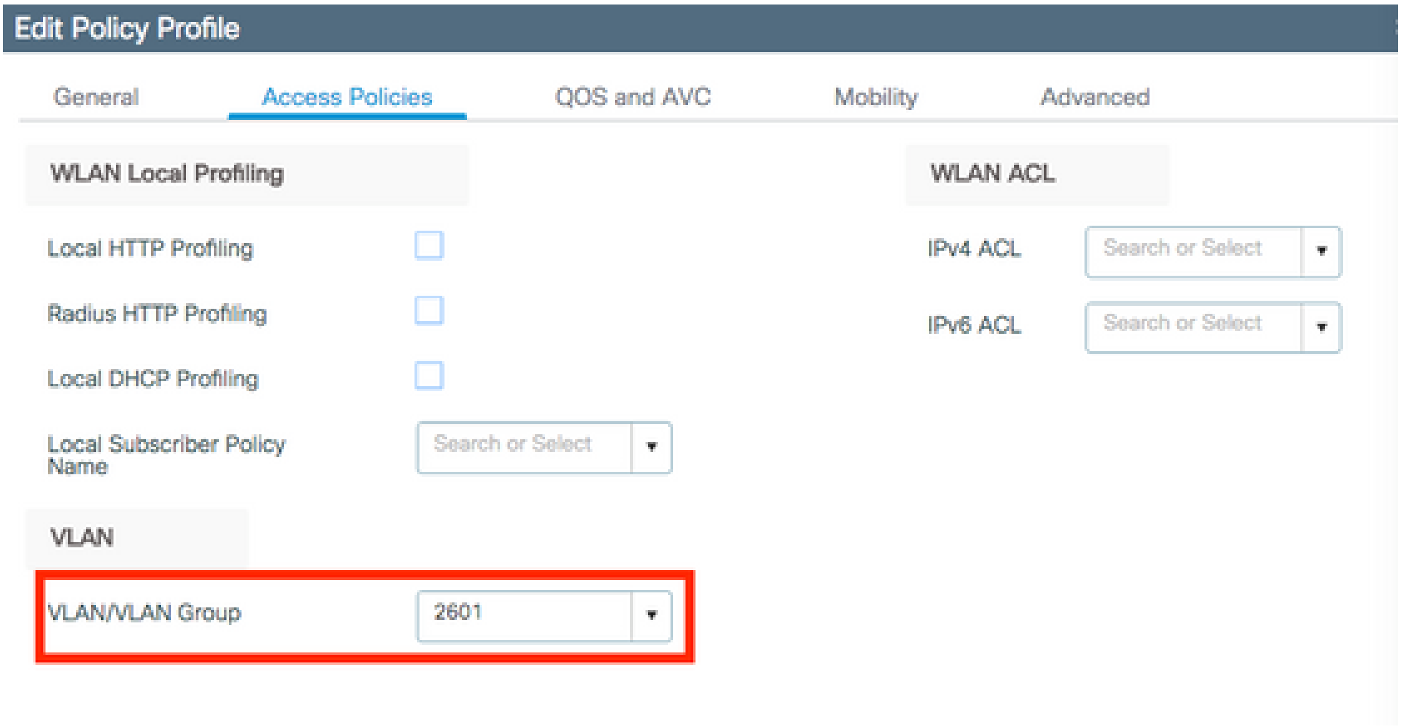
VLAN/VLAN Group: VLAN2602

WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

或



WLAN Local Profiling

Local HTTP Profiling □

Radius HTTP Profiling □

Local DHCP Profiling □

Local Subscriber Policy Name: Search or Select

VLAN

VLAN/VLAN Group: 2601

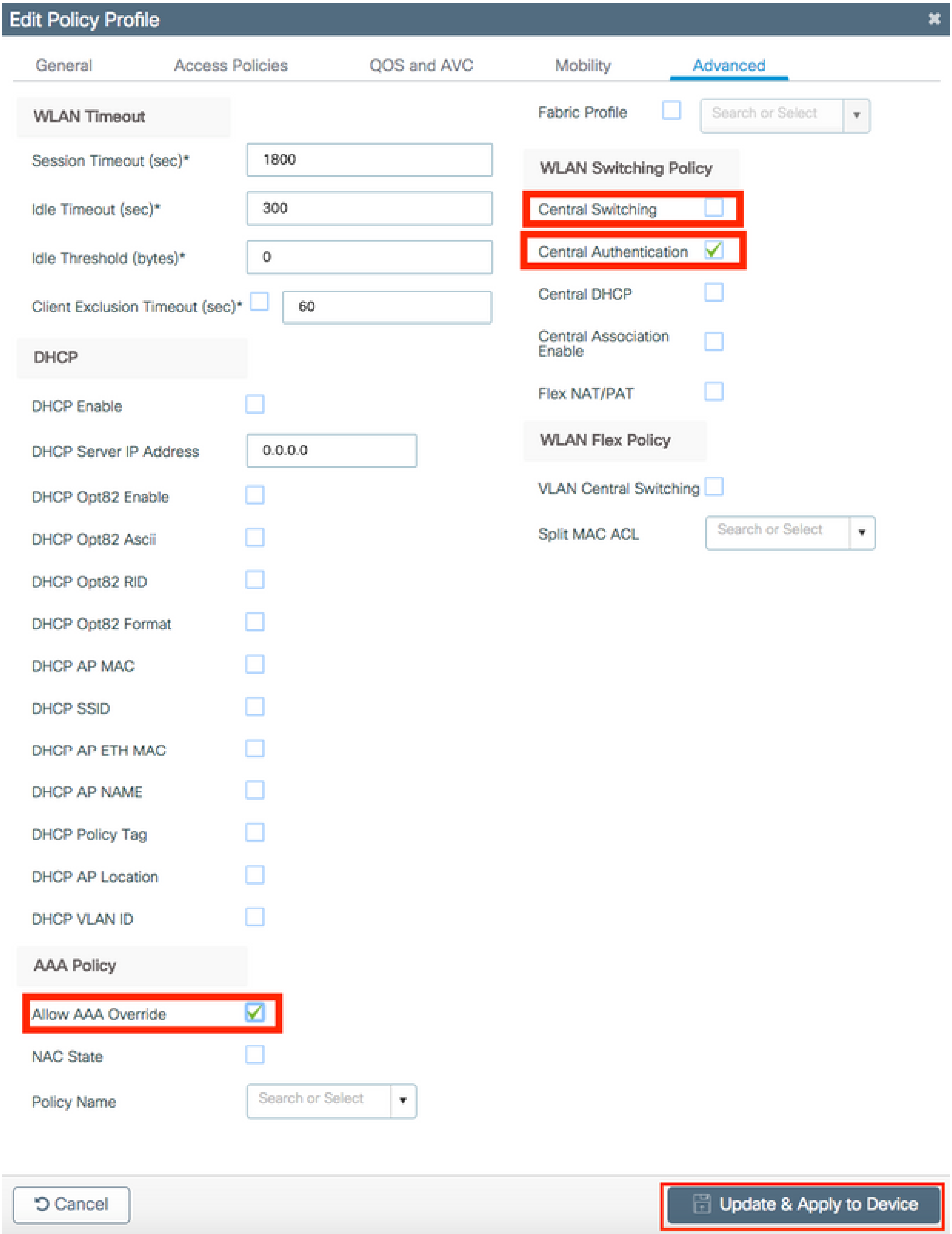
WLAN ACL

IPv4 ACL: Search or Select

IPv6 ACL: Search or Select

步骤4.导航至“高级”**选项卡，**并启用**Central Authentication Enable和**Allow AAA Overrideoptions。**必须禁**用中央交换。

如果希望9800 WLC集中执行身份验证过程，则必须启用集中身份验证。如果希望FlexConnect AP对无线客户端进行身份验证，请禁用它。



WLAN Timeout

Session Timeout (sec)* 1800

Idle Timeout (sec)* 300

Idle Threshold (bytes)* 0

Client Exclusion Timeout (sec)* □ 60

DHCP

DHCP Enable □

DHCP Server IP Address 0.0.0.0

DHCP Opt82 Enable □

DHCP Opt82 Ascii □

DHCP Opt82 RID □

DHCP Opt82 Format □

DHCP AP MAC □

DHCP SSID □

DHCP AP ETH MAC □

DHCP AP NAME □

DHCP Policy Tag □

DHCP AP Location □

DHCP VLAN ID □

AAA Policy

Allow AAA Override ☑

NAC State □

Policy Name Search or Select

Fabric Profile □ Search or Select

WLAN Switching Policy

Central Switching □

Central Authentication ☑

Central DHCP □

Central Association Enable □

Flex NAT/PAT □

WLAN Flex Policy

VLAN Central Switching □

Split MAC ACL Search or Select

CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
# no shutdown
```

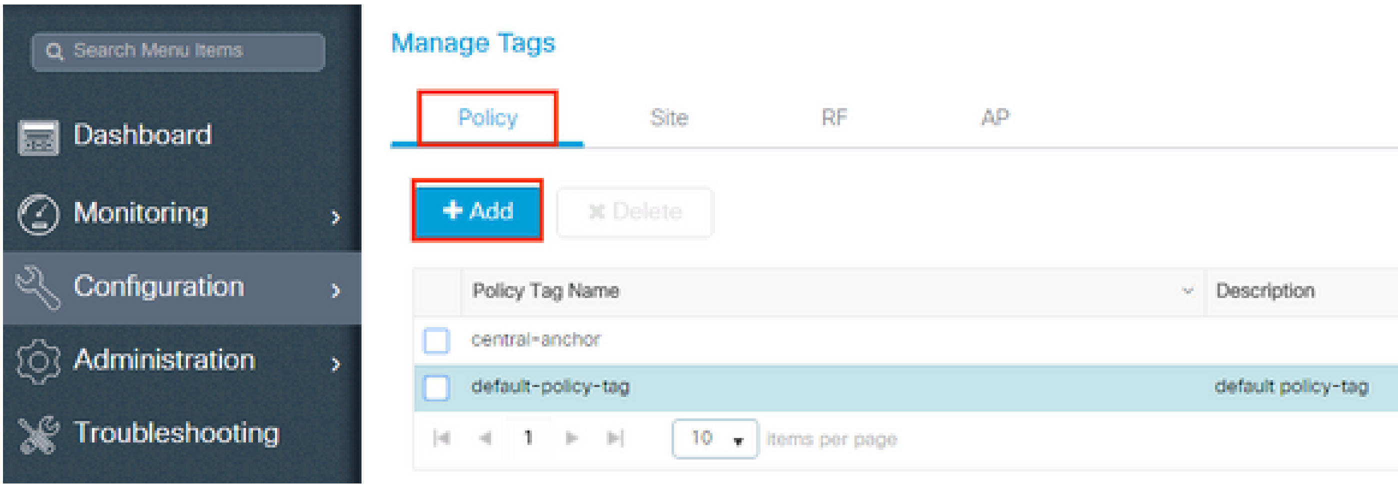
策略标记配置

策略标记用于将SSID与策略配置文件链接。您可以创建新的策略标记或使用默认策略标记。

> 注意: **default-policy-tag会自动将WLAN ID在1到16之间的任何SSID映射到default-policy-profile。**无法修改或删除它。如果您有ID为17或更高的WLAN，则无法使用default-policy-tag。

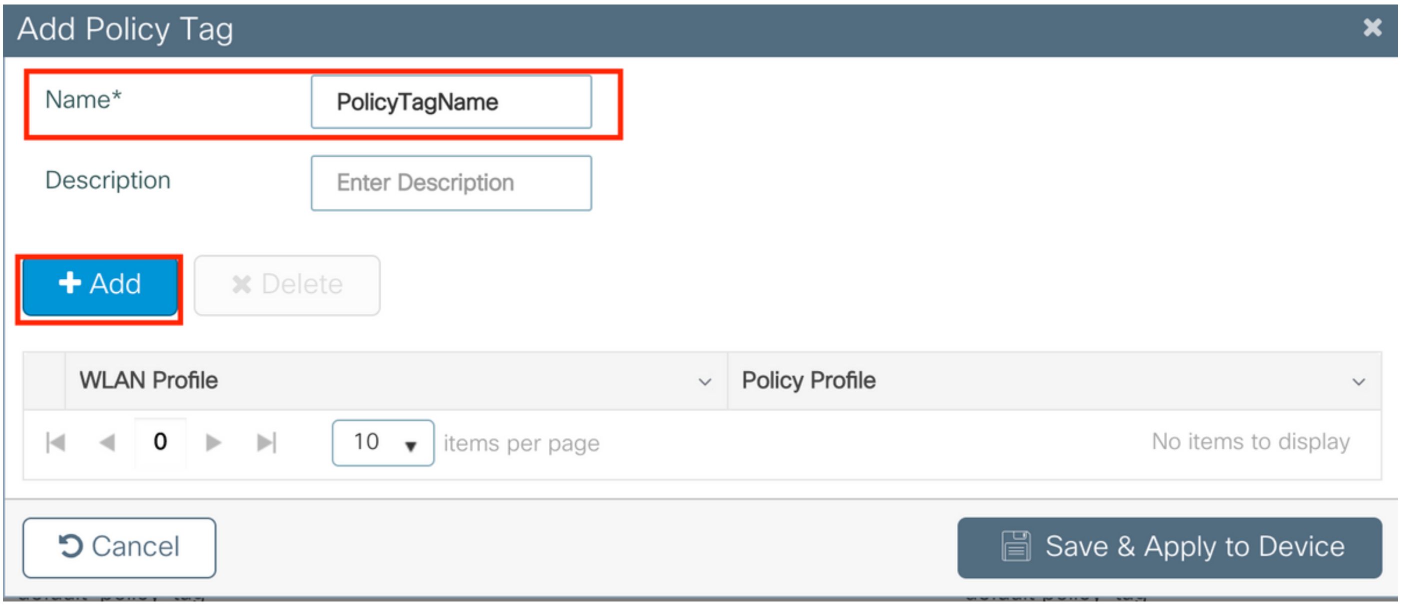
GUI:

导航至**Configuration > Tags & Profiles > Tags > Policy**，并在需要时添加新的。



	Policy Tag Name	Description
□	central-anchor	
□	default-policy-tag	default policy-tag

将您的WLAN配置文件链接到所需的策略配置文件。

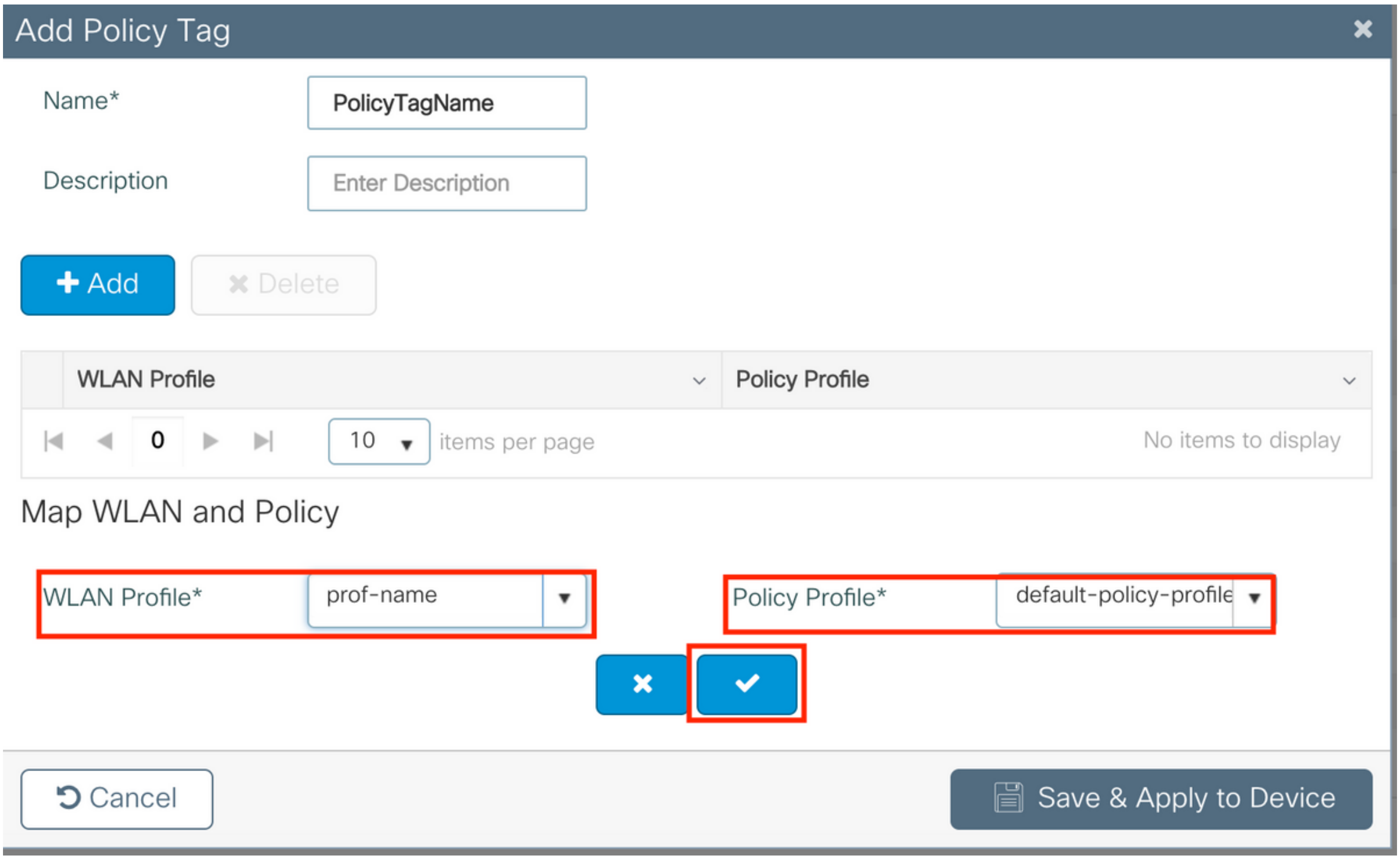


Name*: PolicyTagName

Description: Enter Description

	WLAN Profile	Policy Profile

No items to display



Add Policy Tag

Name*: PolicyTagName

Description: Enter Description

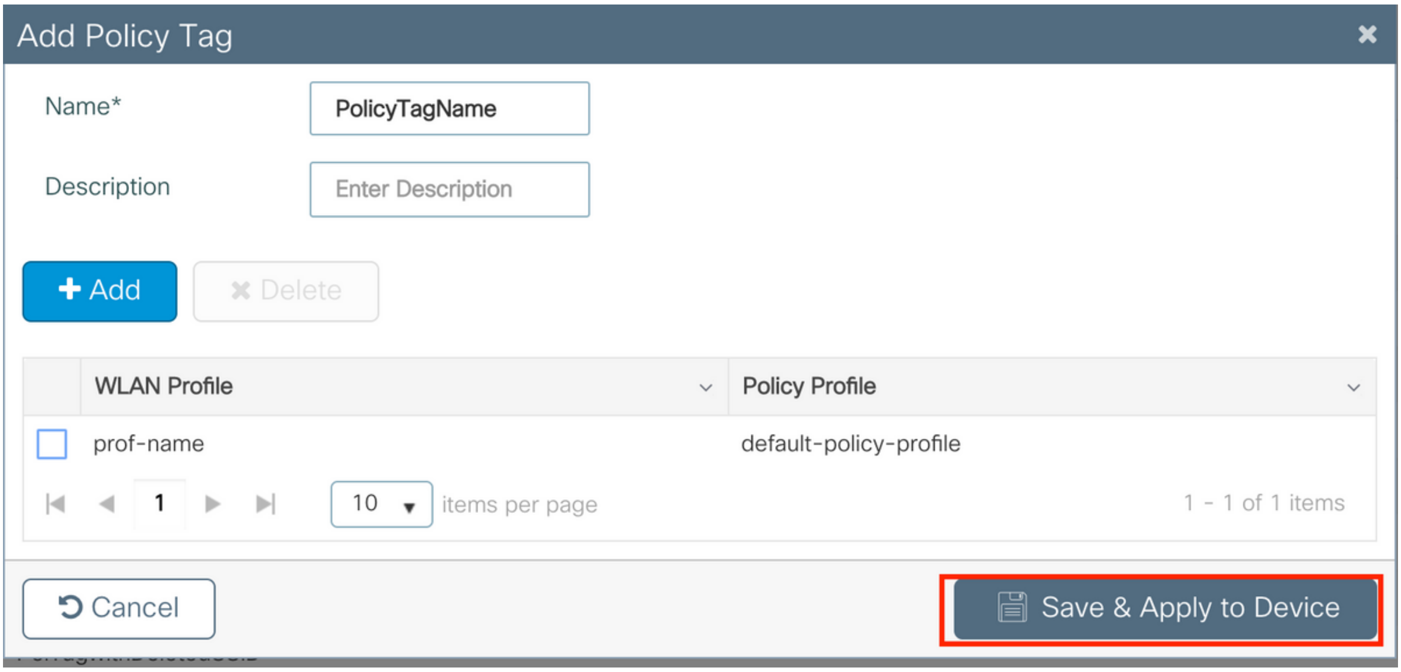
WLAN Profile	Policy Profile

0 — 10 items per page — No items to display

Map WLAN and Policy

WLAN Profile*: prof-name

Policy Profile*: default-policy-profile



Add Policy Tag

Name*: PolicyTagName

Description: Enter Description

	WLAN Profile	Policy Profile
□	prof-name	default-policy-profile

1 — 10 items per page — 1 - 1 of 1 items

CLI：

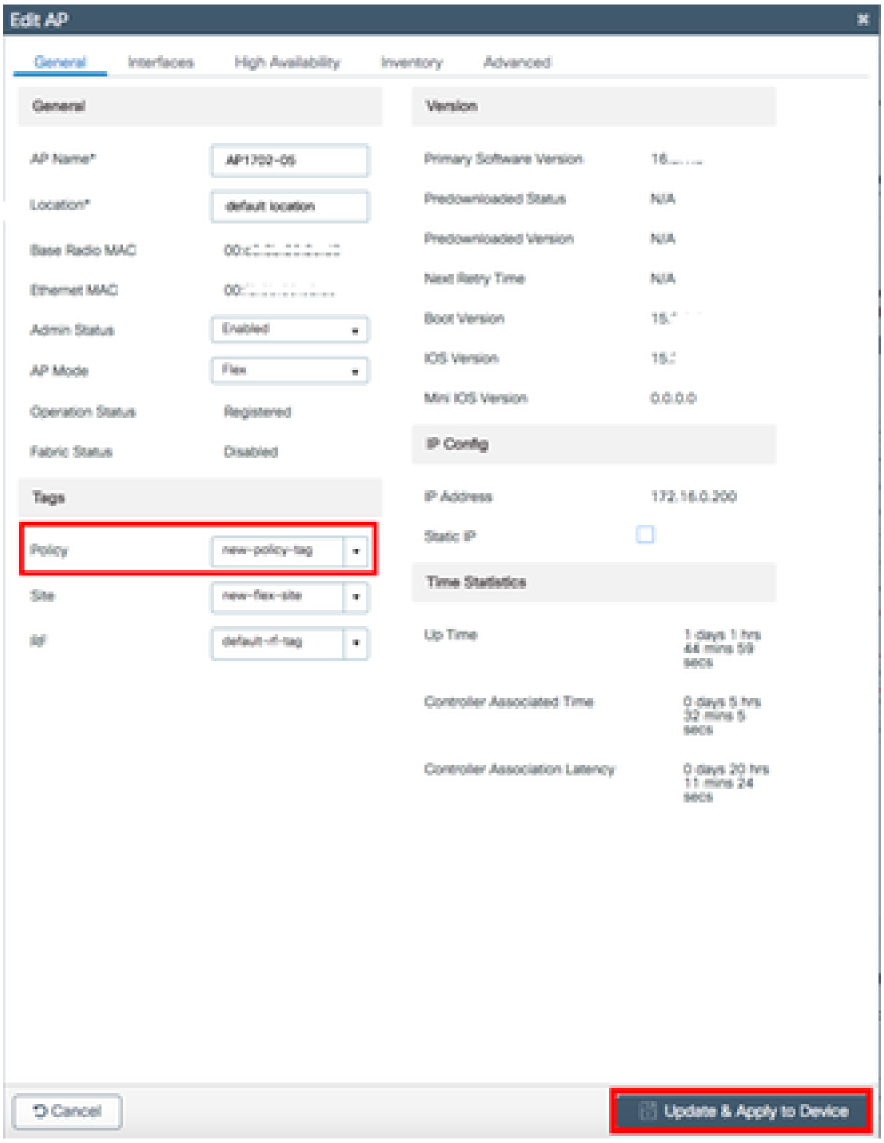
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

策略标记分配

将策略标记分配给AP

GUI

要将标记分配给一个AP，请导航至**Configuration > Wireless > Access Points > AP Name > General Tags**，进行所需的分配，然后单击**Update & Apply to Device**。



General

AP Name*	AP1702-05
Location*	default location
Base Radio MAC	00:c
Ethernet MAC	00:
Admin Status	Enabled
AP Mode	Flex
Operation Status	Registered
Fabric Status	Disabled

Tags

Policy	new-policy-tag
Site	new-flex-site
RF	default-rf-tag

Version

Primary Software Version	16.
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	15.
IOS Version	15.
Mini IOS Version	0.0.0.0

IP Config

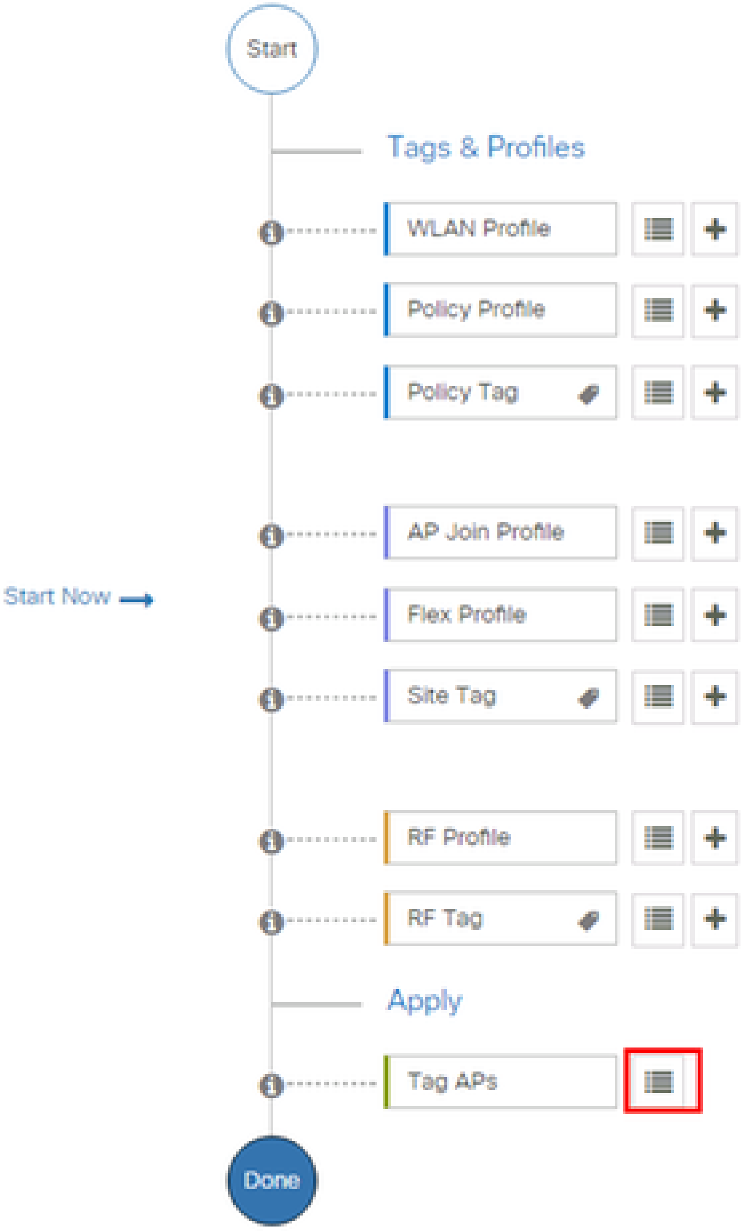
IP Address	172.16.0.200
Static IP	□

Time Statistics

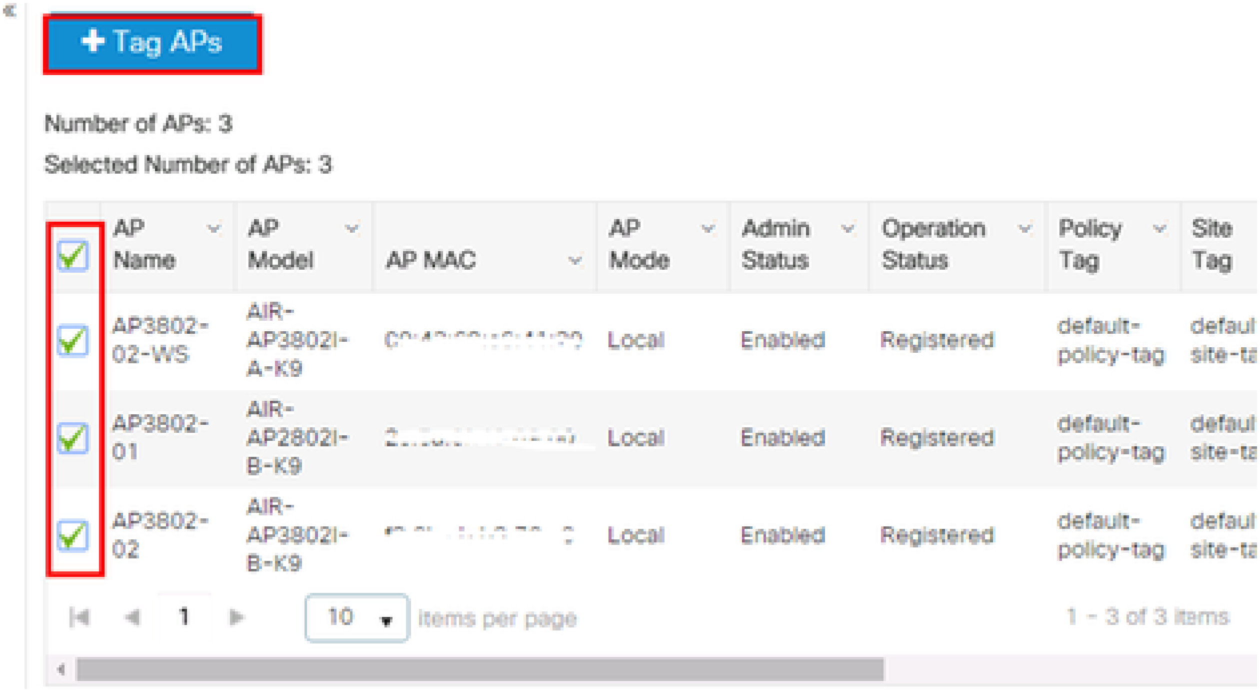
Up Time	1 days 1 hrs 44 mins 59 secs
Controller Associated Time	0 days 5 hrs 32 mins 5 secs
Controller Association Latency	0 days 20 hrs 11 mins 24 secs

注意: **请注意，在更改AP上的策略标记后，它将失去与9800 WLC的关联，并在大约1分钟内重新加入。**

要向多个AP分配相同的策略标记，请导航至**Configuration > Wireless > Wireless Setup > Start Now > Apply**。



选择要向其分配标签的AP，然后单击**+ Tag AP**



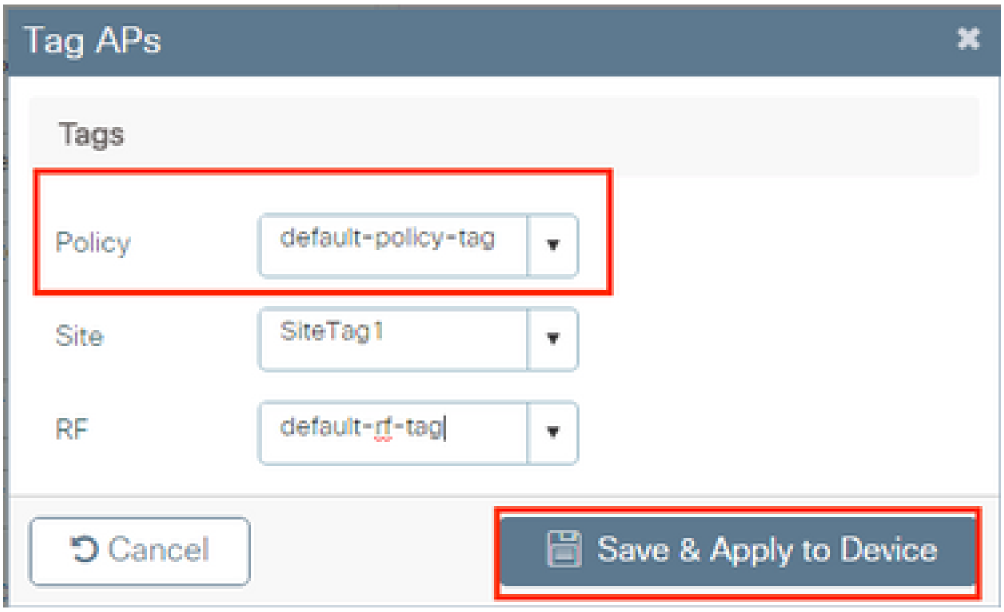
+ Tag APs

Number of APs: 3

Selected Number of APs: 3

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag
☑	AP3802-02-WS	AIR-AP3802I-A-K9	[redacted]	Local	Enabled	Registered	default-policy-tag	defaul site-ta
☑	AP3802-01	AIR-AP2802I-B-K9	[redacted]	Local	Enabled	Registered	default-policy-tag	defaul site-ta
☑	AP3802-02	AIR-AP3802I-B-K9	[redacted]	Local	Enabled	Registered	default-policy-tag	defaul site-ta

选择已清除的标记，然后单**击保存并应用到设备**



Tag APs

Tags

Policy: default-policy-tag

Site: SiteTag1

RF: default-rf-tag

CLI

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

ISE配置

对于ISE v1.2配置，请检查以下链路：

ISE配置

验证

您可以使用这些命令验证当前配置

```
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

故障排除

WLC 9800提供ALWAYS-ON跟踪功能。这可确保持续记录所有与客户端连接相关的错误、警告和通知级别消息，并且您可以查看发生事故或故障情况的日志。

> **注意：**根据生成的日志数量，您可以返回数小时到数天。

要查看默认情况下收集的9800 WLC的跟踪，您可以通过SSH/Telnet连接到9800 WLC并执行以下步骤（确保将会话记录到文本文件）。

步骤1.检查控制器的当前时间，以便在发生问题时跟踪日志。

```
# show clock
```

步骤2.从控制器缓冲区或外部系统日志收集系统日志，如系统配置所述。这可快速查看系统运行状况和错误（如果有）。

```
# show logging
```

步骤3.检验是否启用了任何调试条件。

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                               Port
------------------------------------------------------|----------
```

> **注意：**如果您看到列出的任何条件，这意味着跟踪记录到遇到启用条件（mac地址、ip地址等）的所有进程的调试级别。 这将增加日志的数量。因此，建议在非主动调试时清除所有条件

步骤4.假设测试中的mac地址未列为步骤3中的条件，请收集特定mac地址的始终在线通知级别跟踪。

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file
always-on-<FILENAME.txt>
```

您可以显示会话中的内容，也可以将文件复制到外部TFTP服务器。

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

条件调试和无线电活动跟踪

如果始终在线跟踪没有提供足够的信息来确定所调查问题的触发因素，您可以启用条件调试并捕获活动无线电(RA)跟踪，这将为与指定条件（本例中为客户端mac地址）交互的所有进程提供调试级别跟踪。 要启用条件调试，请执行以下步骤。

步骤5.确保未启用调试条件。

```
# clear platform condition all
```

步骤6.为要监控的无线客户端mac地址启用调试条件。

此命令开始监控提供的MAC地址30分钟（1800秒）。 您可以选择将此时间增加到2085978494秒。

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

注意: **要一次监控多个客户端，请按mac地址运行debug wireless mac <aaaa.bbbb.cccc>命令。**

注意:**您看不到终端会话上客户端活动的输出，因为所有内容都在内部缓冲，以备以后查看。**

步骤7.重现要监控的问题或行为。

步骤8.如果问题在默认或配置的监控时间开启之前重现，请停止调试。

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

监控时间过去或调试无线停止后，9800 WLC将生成名为：

ra_trace_MAC_aaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

步骤9.收集MAC地址活动的文件。您可以将ra trace .log复制到外部服务器或直接在屏幕上显示输出。

检查RA跟踪文件的名称

```
# dir bootflash: | inc ra_trace
```

将文件复制到外部服务器：

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

显示内容：

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步骤10.如果根本原因仍不明显，请收集内部日志，这些日志是调试级别日志的更详细视图。您无需再次调试客户端，因为我们只是进一步详细查看已收集和内部存储的调试日志。

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }
to-file ra-internal-<FILENAME>.txt
```

> **注意：**此命令输出返回所有进程的所有日志记录级别的跟踪，并且相当庞大。请联系思科TAC，帮助解析这些跟踪。

您可以将ra-internal-FILENAME.txt复制到外部服务器，或直接在屏幕上显示输出。

将文件复制到外部服务器：

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

显示内容：

```
# more bootflash:ra-internal-<FILENAME>.txt
```

步骤11.删除调试条件。

```
# clear platform condition all
```

> **注意：**确保在故障排除会话后始终删除调试条件。