在FlexConnect模式下配置本地身份验证

目录

- 简介
  - 背景信息
    - FlexConnect概述和要求
    - 运行模式
    - 快速安全漫游
    - FlexConnect高扩展模式
    - Wi-Fi 7 FlexConnect支持
    - FlexConnect恢复能力方案
- 先决条件
  - 要求
  - 使用的组件
- 配置
  - 网络图
  - 配置AAA服务器
  - 在远程站点上配置FlexConnect模式
  - 使用外部RADIUS服务器配置802.1x WLAN进行本地身份验证
  - 配置ISE
  - 使用本地身份验证配置PSK WLAN
- 验证
- 故障排除
  - 独立方案
- 相关信息

简介

本文档介绍FlexConnect本地身份验证的工作原理以及如何使用Cisco Catalyst 9800系列无线控制器(WLC)对其进行配置

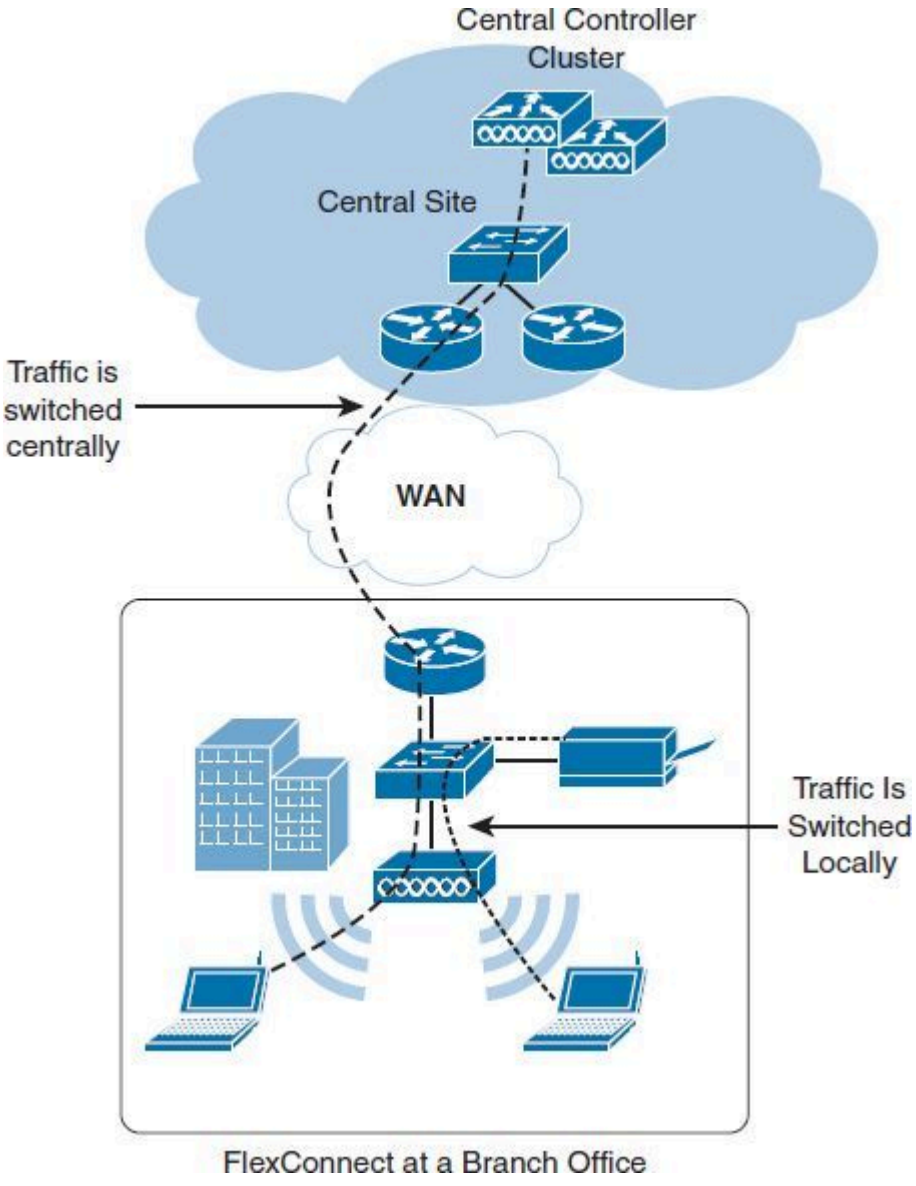
背景信息

FlexConnect概述和要求

FlexConnect使远程或分支机构的接入点(AP)能够连接到集中式控制器，同时允许对无线流量进行本地处理。与传统的集中式无线部署不同，传统的集中式无线部署使用CAPWAP（无线接入点的控制和调配）将所有无线流量通过隧道传输到控制器，而FlexConnect允许流量在本地进行交换，并

由分支机构AP直接进行处理。此本地交换为AP提供一定程度的自治权，使安全、漫游和服务质量(QoS)等关键服务能够独立于控制器运行。

虽然FlexConnect主要用于本地流量交换，但它也提供了根据需要集中交换特定SSID（服务集标识符）的灵活性。例如，如果某些流量必须通过中央防火墙，则这些SSID可以通过CAPWAP发回控制器进行集中交换。这种双重功能允许单个FlexConnect AP同时支持本地和集中交换WLAN（无线局域网）。



在分支机构部署的FlexConnect AP本地交换一个SSID，同时集中交换另一个SSID

运行模式

FlexConnect AP在两种模式下运行：连接模式和独立模式。

- 在连接模式下，AP通过CAPWAP控制通道保持与控制器的活动连接。
- 独立模式是当AP失去与控制器的连接时发生的回退状态。

在正常情况下，FlexConnect AP在连接模式下运行，控制器在此模式下管理关键服务，例如集中身份验证、客户端分析和无线电资源管理(RRM)。 虽然AP预计大部分时间都保持此模式，但如果与控制器的通信丢失，它会自动切换到独立模式。在独立模式下，AP继续运行，在本地交换流量并允许客户端保持连接。AP独立对客户端进行身份验证，而不向中央控制器转发身份验证请求。但是，某些与控制器相关的服务（例如RRM和集中客户端身份验证）暂时不可用。

例如，如果WAN（广域网）中断中断AP和控制器之间的连接，但Internet访问保持活动状态，则AP将转换到独立模式，继续处理本地交换的流量而不中断。现有客户端保持连接，但需要集中身份验证的新客户端无法加入网络，除非配置了本地身份验证。可以将FlexConnect AP设置为在WAN故障期间执行本地身份验证，确保即使在控制器不可达时也能继续提供服务。

当处于独立模式时，AP无法使用这些功能：

- 客户端Web身份验证
- 访客身份验证（门户重定向）
- 任何集中交换SSID
- RRM
- IPv6第3层移动性
- 本地分析
- 策略分类
- 服务发现网关
- 配置更新

有关独立模式（本地身份验证）支持的功能和WLAN配置的完整列表，请参阅功能表：思科无线接入点的功能表

常见的FlexConnect故障场景包括WAN完全丢失或显着下降，这会中断CAPWAP控制信道。当AP因WAN问题失去与控制器的连接时，它会立即切换到独立模式。

WAN故障期间的主要目标是尽快恢复与控制器的通信，以恢复全部功能。

当FlexConnect AP因WAN故障而进入独立模式时，活动客户端保持连接并可在FlexConnect域/站点标记内的AP之间无缝漫游，但不同FlexConnect站点标记之间的漫游可能需要完全重新身份验证。

但是，尝试加入本地交换WLAN的新客户端无法进行身份验证，因为无法访问中心位置的AAA服务器（身份验证、授权和记帐服务器）。

快速安全漫游

由于与AAA服务器交换EAP帧，EAP（可扩展身份验证协议）身份验证与PSK（预共享密钥）身份验证相比，引入更高的延迟。但是，使用快速安全漫游时，客户端仅在其与网络的初始关联期间接受完整的802.1X/EAP身份验证。在随后到相邻AP的漫游中，EAP交换被绕过，只留下四向握手，这要快得多，因为它不涉及AAA服务器。此表概述了本地模式和FlexConnect部署中9800 WLC支持的各种快速安全漫游方法。

功能	本地模式	FlexConnect(连接模式；集中身份验证)	FlexConnect（连接模式 — 本地身份验证）	FlexConnect（独立）
粘滞密钥缓存(SKC)	Not Supported	Not Supported	Not Supported	Not Supported
机会密钥缓存(OKC)	受支持	受支持	受支持	支持（直到客户端会话过期）
思科集中密钥管理(CCKM)	受支持	受支持	受支持	Not Supported
FT-802.11r/自适应11r（快速转换）（空中）	受支持	受支持	受支持	支持（直到客户端会话过期）
FT-802.11r/自适应11r（快速转换）（通过DS）	受支持	受支持	Not Supported	Not Supported

在独立模式下，快速漫游取决于缓存的密钥材料是否仍然有效。当缓存的PMK（成对主密钥）/会话到期时，AP无法获取新的控制器派生密钥信息，直到恢复控制器连接。

FlexConnect高扩展模式

从Cisco IOS XE 17.8.1开始，灵活站点站点容量已扩展到可容纳300个AP和3000个802.1x客户端。

PMK传播允许同一FlexConnect站点内的AP共享PMK信息，从而减少在漫游期间进行完整EAP交换的需要。默认情况下，PMK传播未启用。

使用以下命令验证PMK传播并启用PMK:

- show wireless stats pmk-propagation
- pmk传播

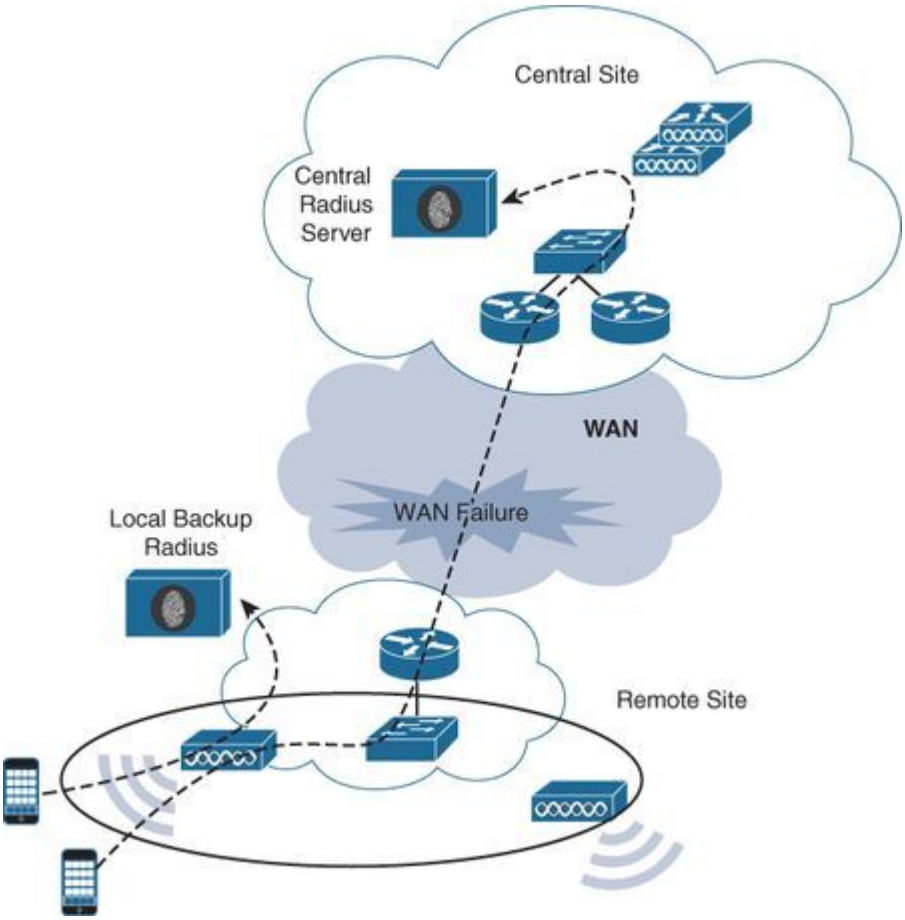
Wi-Fi 7 FlexConnect支持

此表汇总了CW917x Wi-Fi 7 AP系列支持的FlexConnect功能。

功能	支持
本地交换	受支持
中心交换	受支持
WLAN-VLAN映射	受支持
使用外部RADIUS的本地身份验证	受支持
WPA3 — 企业	受支持
FT-802.11r快速漫游	受支持
多链路操作(MLO)	受支持
使用内部RADIUS的本地身份验证	Not Supported
WPA3-Enterprise-192	Not Supported

FlexConnect恢复能力方案

1. 在N+1恢复力设置中，多个活动控制器共享一个通用备用控制器，该备用控制器可在任何活动控制器发生故障时进行接管。当主控制器离线时，FlexConnect AP立即切换到独立模式，并开始搜索备用控制器。在此断开期间，集中交换的客户端会与AP断开连接。一旦AP定位并与备用控制器同步，需要访问集中交换SSID的客户端就会重新连接。同时，本地交换的客户端仍然不受影响，并在不注意到服务中断的情况下继续运行。
2. 在远程位置提供可由FlexConnect组访问的备份AAA服务器。启用本地身份验证后，此备用RADIUS服务器仅在AP进入独立模式时使用 — 当AP处于连接模式时，该服务器保持非活动状态。当FlexConnect AP使用本地备份AAA服务器进行身份验证时，身份验证密钥会分布在FlexConnect组中的所有AP上，就像集中式AAA服务器一样。这样可确保新客户端仍然能够无缝地在AP之间漫游，而无需重新进行身份验证，即使在使用备份RADIUS服务器时也是如此。
3. 思科无线接入点功能表上允许本地身份验证的任何方法。



当中央AAA服务器因WAN故障而变得不可用时，客户端根据本地备份AAA服务器进行身份验证

先决条件

要求

本文档没有任何特定的要求。

使用的组件

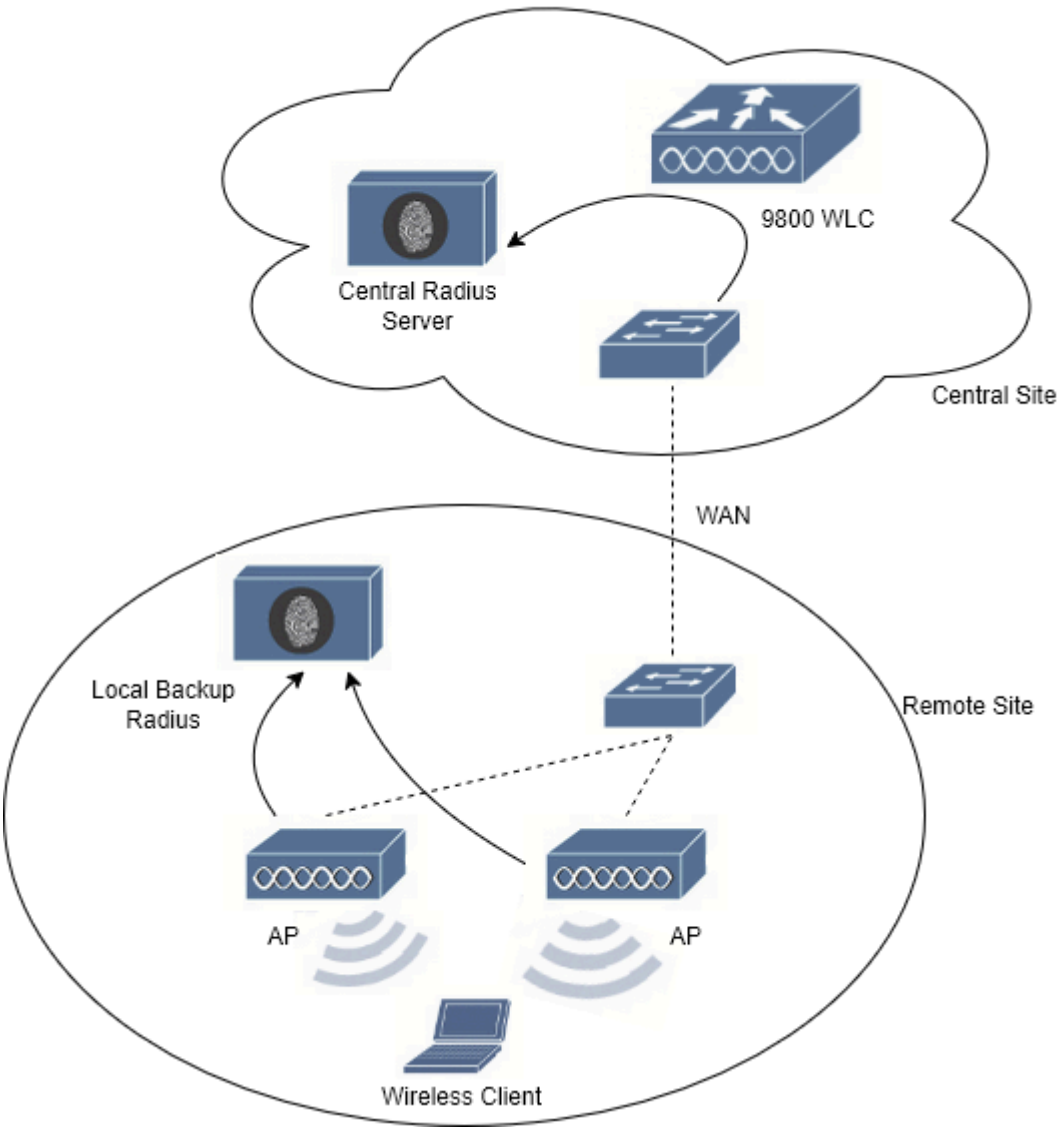
本文档中的信息基于以下软件和硬件版本：

- 适用于云的Catalyst C9800-CL无线控制器，带Cisco IOS® XE都柏林17.18.3
- Catalyst CW9164I-ROW接入点v17.18.3.18
- Aironet® AIR-AP2802I-E-K9无线接入点v17.18.3.18
- 2个身份服务引擎v3.2.0.542

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



网络图

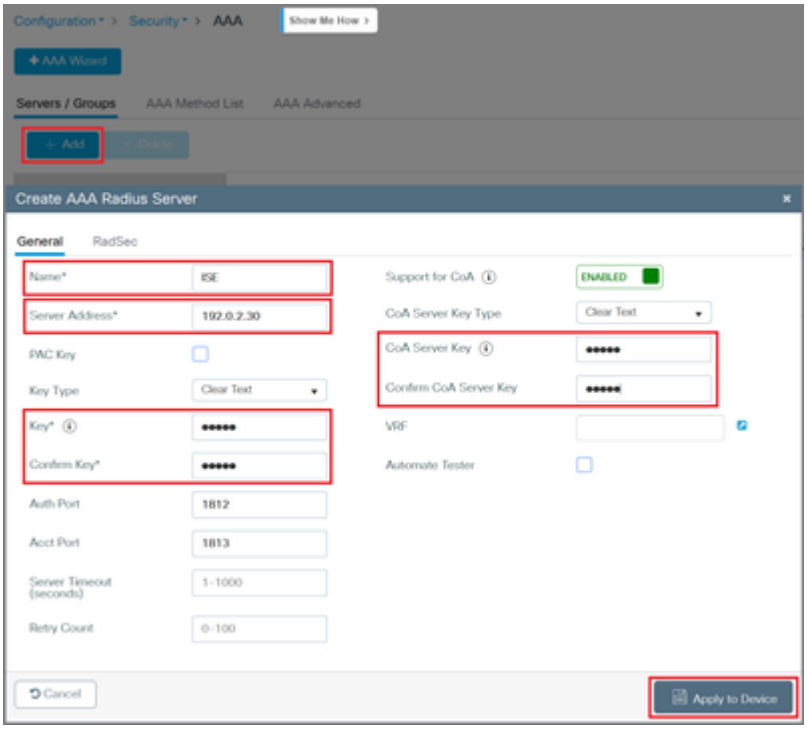
配置AAA服务器

步骤1.要配置802.1x WLAN，您需要在9800 WLC上创建AAA服务器组。

为每个站点创建一个AAA服务器 — 一个在中心站点上，另一个在远程站点上。

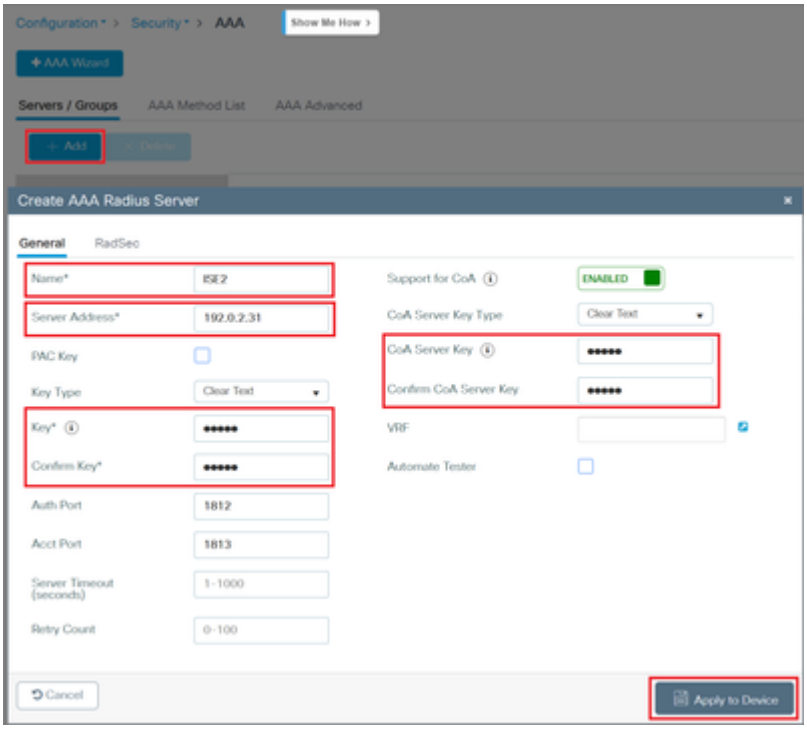
导航到Configuration > Security > AAA > Server/Groups > Servers，然后选择+Add。为服务器命名

、其IP地址、密钥（和确认密钥）、启用CoA（授权更改）支持，并输入CoA服务器密钥（并确认CoA服务器密钥）。 密钥必须相同。



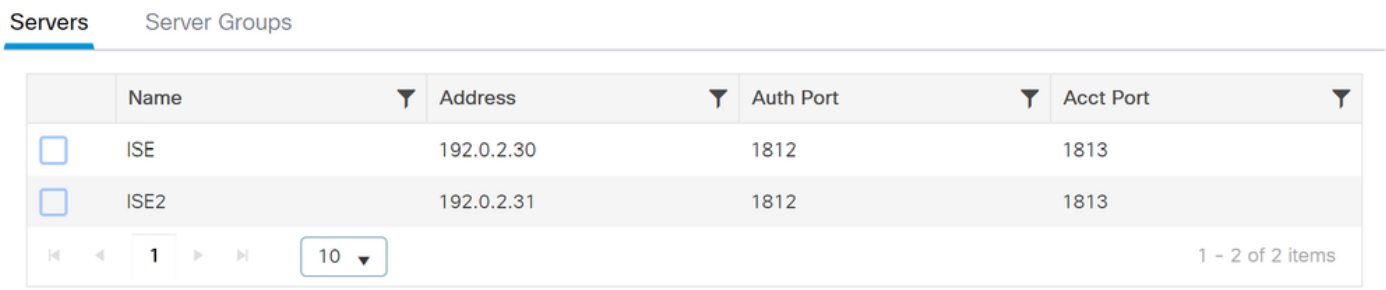
单击Apply to Device。

步骤2.创建其他AAA服务器：

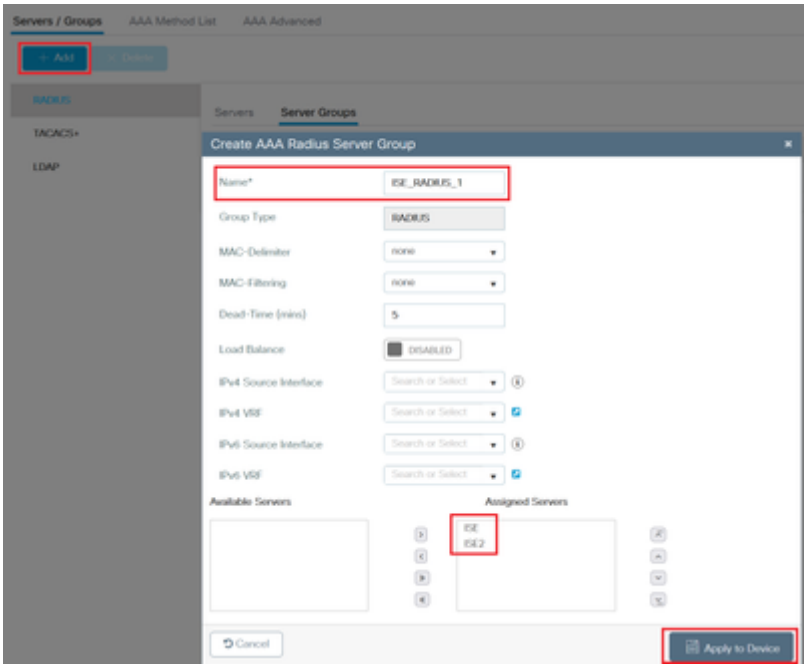


单击Apply to Device。

现在您会看到已配置的AAA服务器：

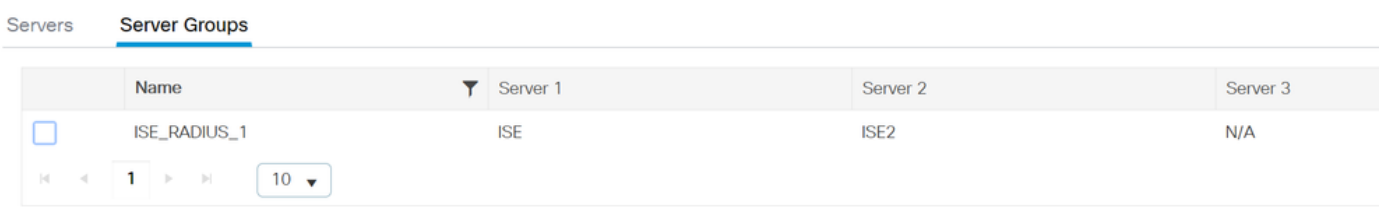


第3步：导航到配置>安全> AAA >服务器/组>服务器组，然后选择+添加。为组服务器指定名称，并选择之前创建的AAA服务器到分配的服务器列：



单击Apply to Device。

然后您会看到配置的AAA服务器组：



CLI：

```
aaa new-model
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

在远程站点上配置FlexConnect模式

步骤1.第一步是在远程站点上配置FlexConnect。

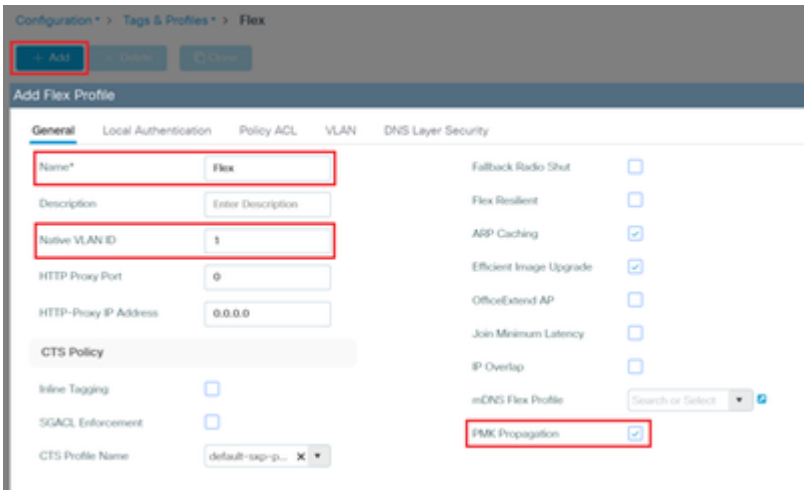
使用此指南将您的AP模式更改为Flex：了解Catalyst 9800无线控制器上的FlexConnect。

本指南/实验中的AP使用相同的Flex配置文件。

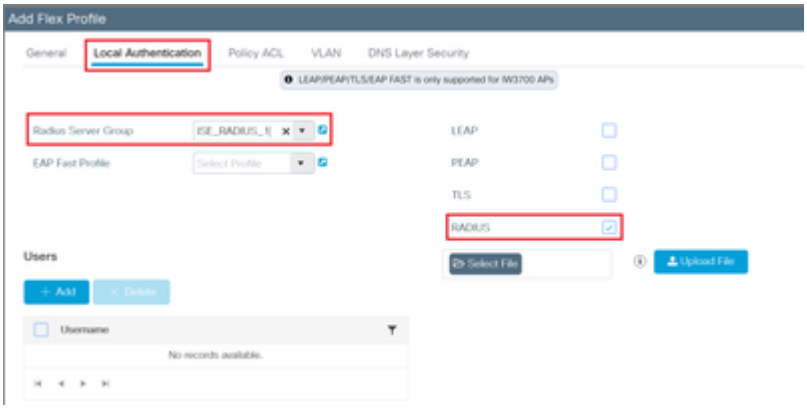
步骤2.导航到配置>标记和配置文件> Flex。

使用+Add创建新的Flex配置文件名称。在General选项卡上，为配置文件指定名称，输入本地VLAN（虚拟局域网）ID，并启用PMK传播。

启用PMK传播，通过在单个站点内的AP之间共享PMK信息，促进无缝无线客户端漫游。

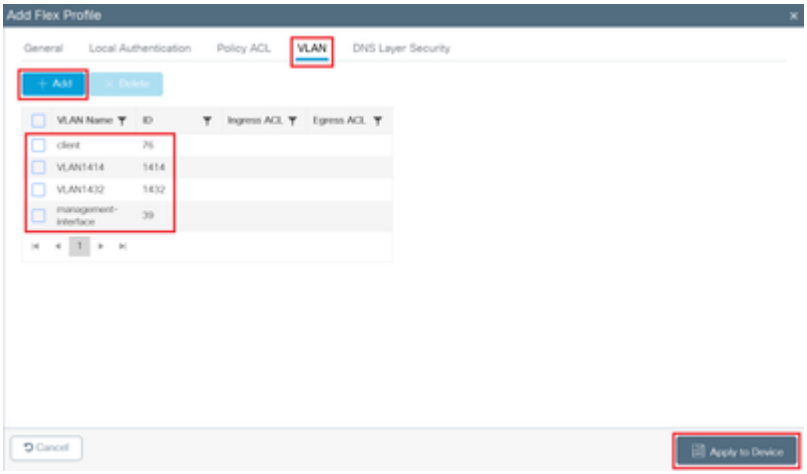


步骤3.对于802.1x WLAN，在Local Authentication选项卡上选择Radius Server Group并启用RADIUS:



提示：对于PSK WLAN，您无需在此选项卡中添加任何内容。

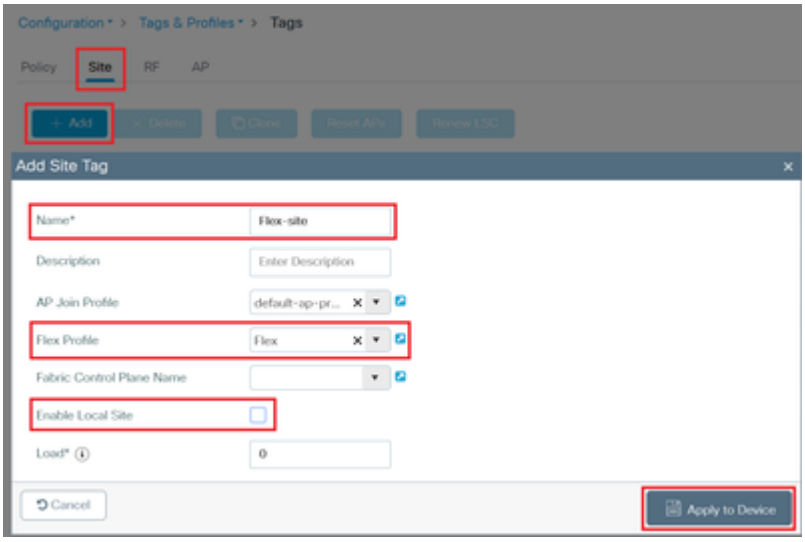
步骤4.在VLAN选项卡上，添加客户端、AP和RADIUS服务器使用的所有VLAN。确保将每个VLAN名称正确对应到正确的VLAN ID:



最后，点击Update & Apply to Device。

第5步：导航到配置>标签和配置文件>标签>站点，然后选择+添加。

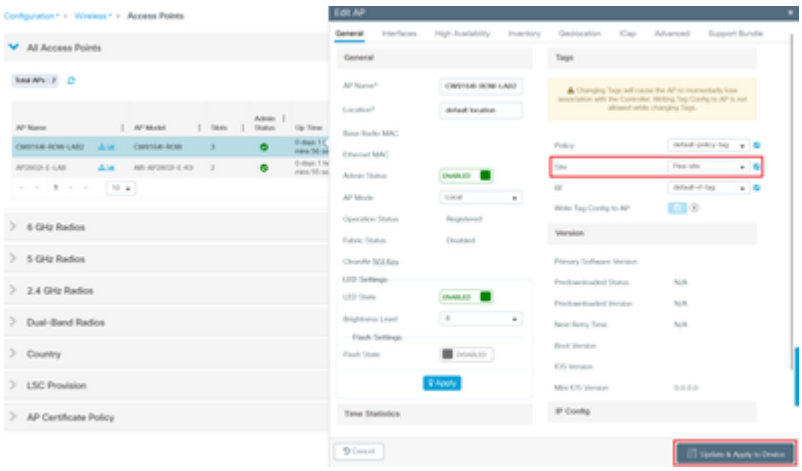
使用之前创建的Flex Profile创建站点标签。为其指定一个名称，选择正确的Flex配置文件，并禁用启用本地站点。确保AP加入配置文件正确。



点击应用到设备。

步骤6.导航到配置>无线>接入点。

选择AP，在General > Tags上，将Site Tag更改为先前配置的标记：



单击Update & Apply to Device。

AP与WLC断开连接并使用Flex AP模式重新加入。

在同一页上，当AP重新加入时，您可以在AP Mode列上检查AP模式。

如果选择AP，则会显示新的站点标记：



CLI：

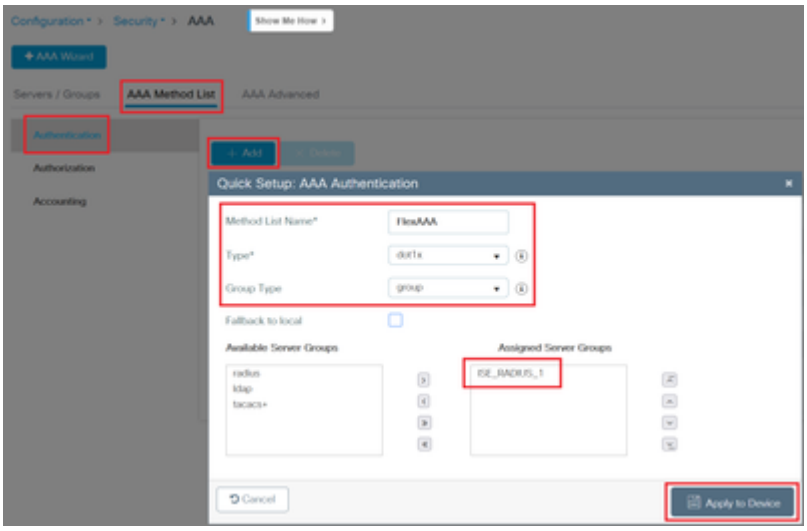
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

使用外部RADIUS服务器配置802.1x WLAN的本地身份验证

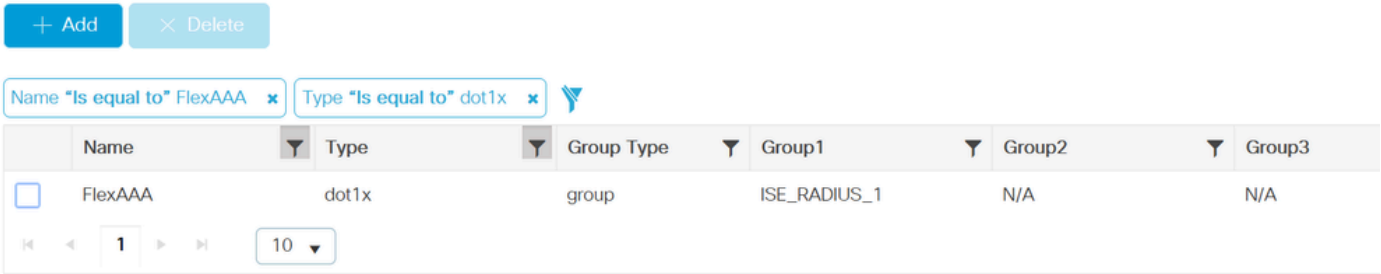
步骤1.创建身份验证方法列表。

导航到AAA Method List > Authentication选项卡上的Configuration > Security > AAA。

选择+Add，为方法列表名称指定名称，选择dot1x作为类型，选择group作为组类型，并在Assigned Server Groups列上分配AAA服务器组：



现在您会看到创建的AAA方法列表：



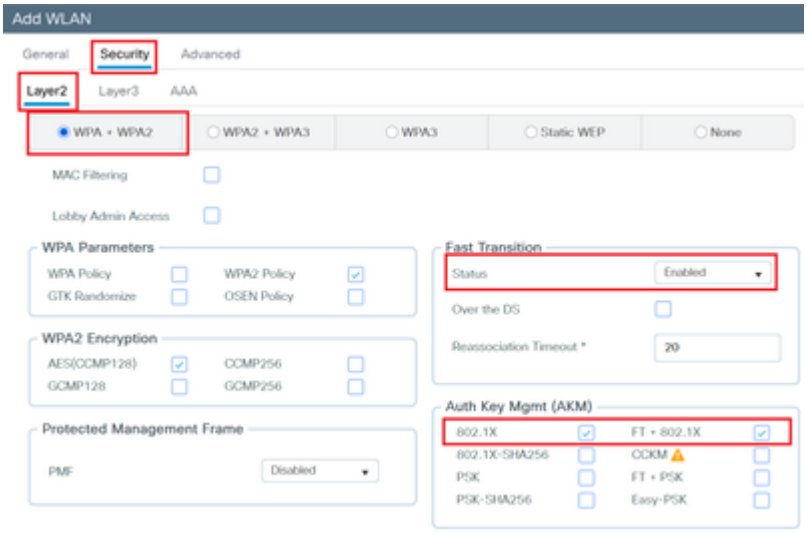
第 2 步： 创建 WLAN.

导航到Configuration > Tags & Profiles > WLANs，选择+Add。

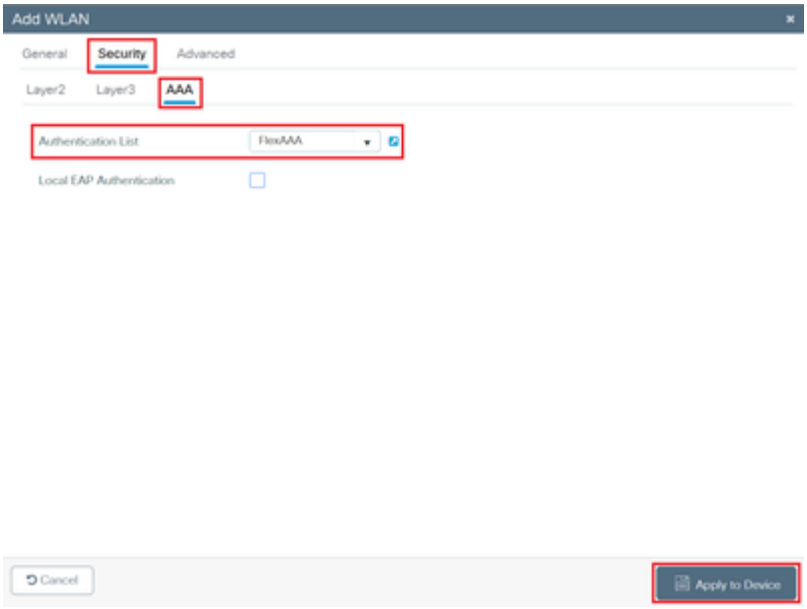
在General标记上，为配置文件名称、SSID创建一个名称，并启用状态：



第3步：导航到安全> Layer 2选项卡，选择WPA+WPA2（Wi-Fi保护访问），快速过渡为已启用，身份验证密钥管理802.1X和FT+802.1X:



第4步：导航到Security > AAA选项卡，在Authentication List下拉菜单中选择之前创建的列表：



单击Update & Apply to Device。

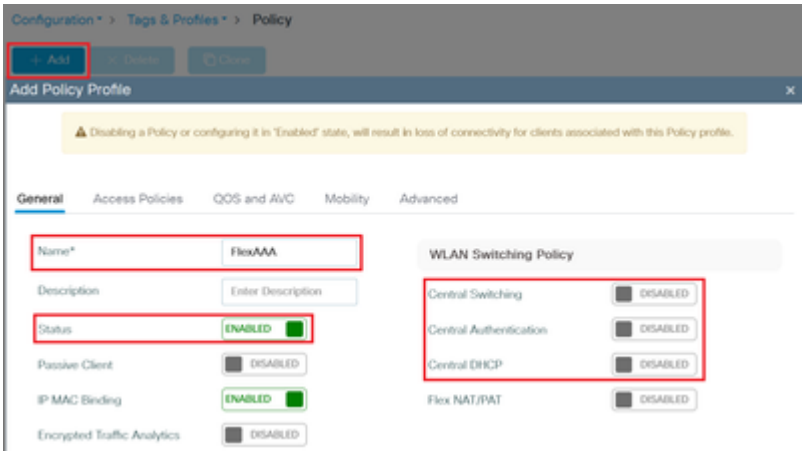
然后您会看到创建的WLAN:



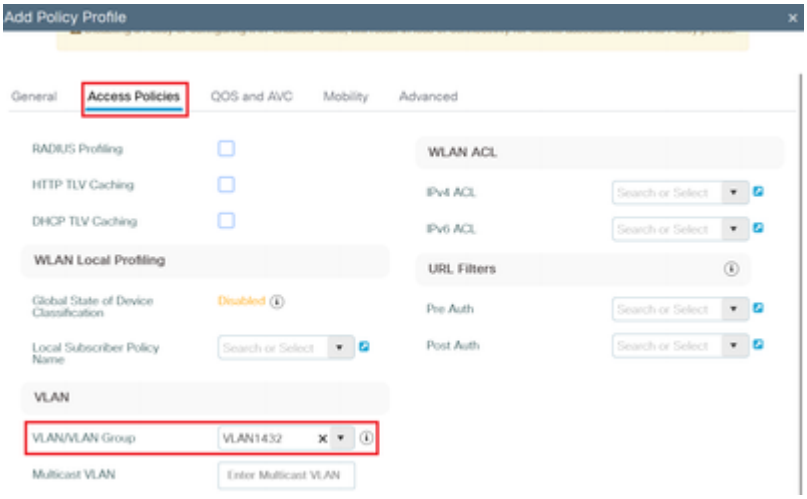
步骤5.创建策略配置文件。

导航至配置 > 标签和配置文件 > 策略。

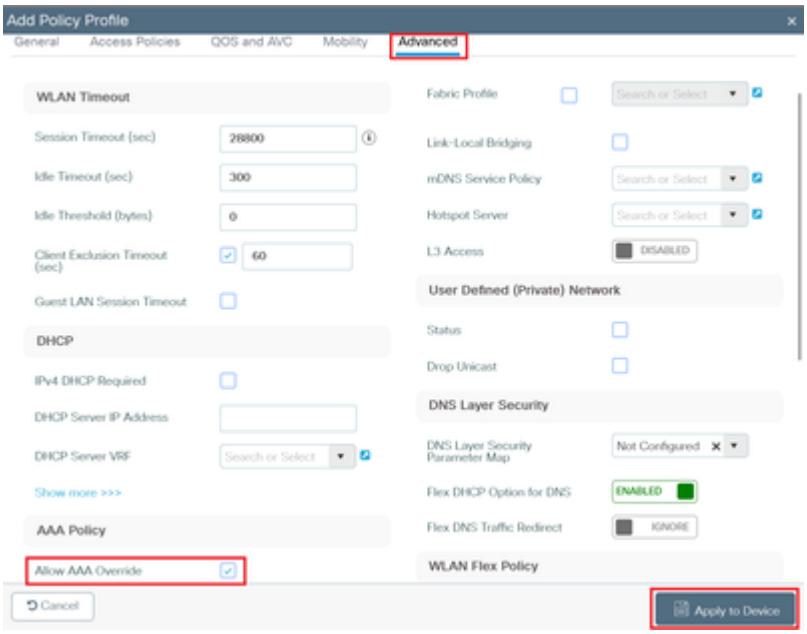
选择+Add，并在General选项卡上为策略配置文件命名，启用状态，并禁用集中交换、集中身份验证和集中DHCP（动态主机配置协议）：



步骤6.导航到Access Policies选项卡，选择VLAN:

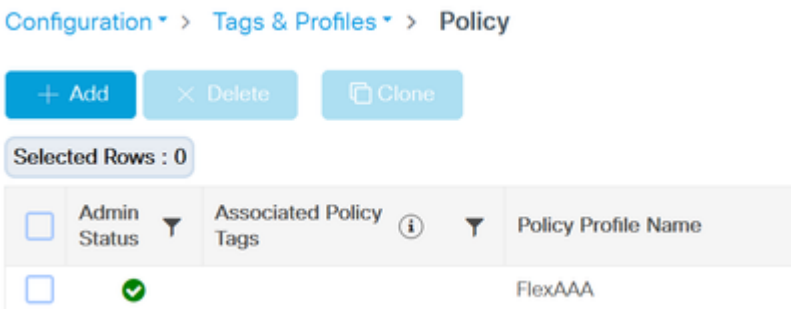


步骤7.导航到高级选项卡，启用允许AAA覆盖：



单击Update & Apply to Device。

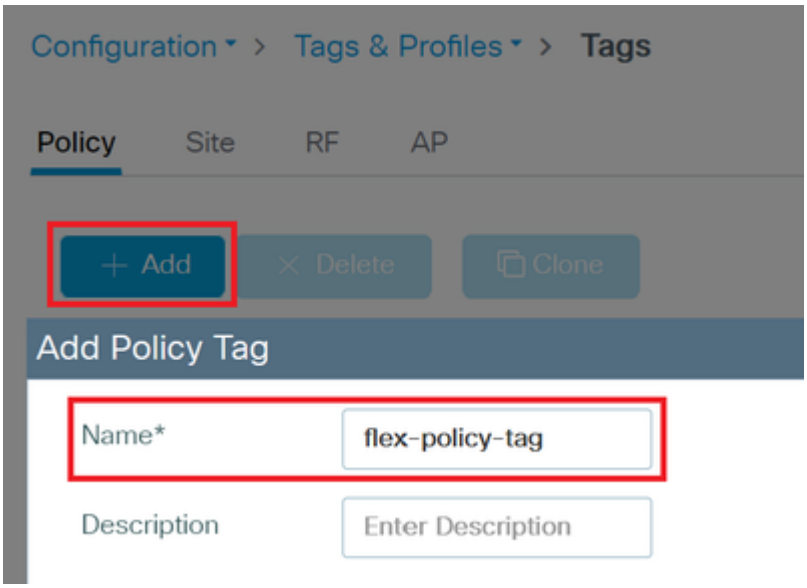
您可以在列表中看到策略配置文件：



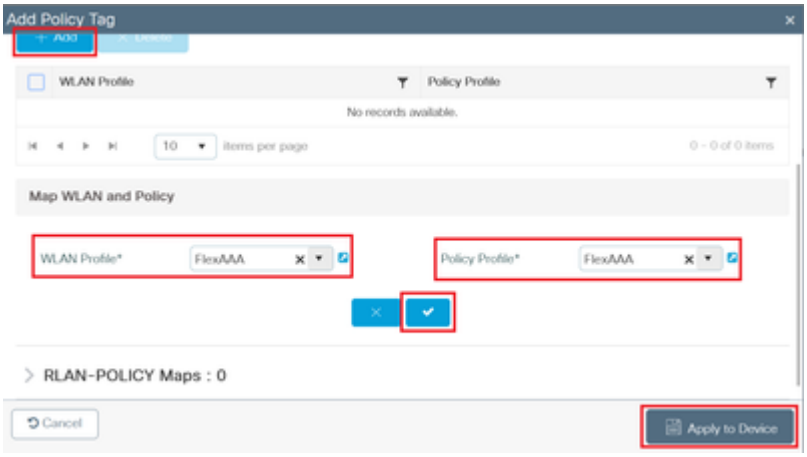
步骤8.创建策略标记。

导航到配置>标签和配置文件>标签

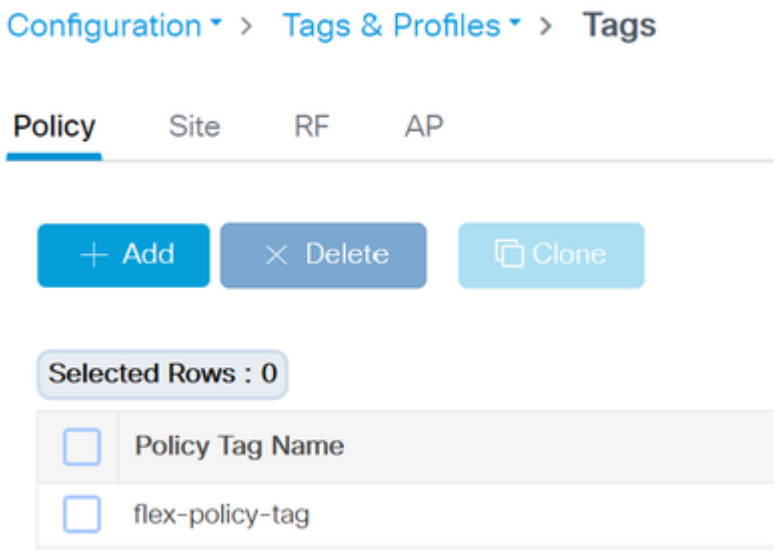
在Policy选项卡上，选择+Add。为策略标记指定名称：



向下滚动并选择WLAN-POLICY Maps下的+Add。在WLAN配置文件上，从下拉菜单中选择之前创建的WLAN。在Policy Profile上，从下拉菜单中选择之前创建的策略配置文件。单击check（检查）按钮，然后单击Apply to Device:

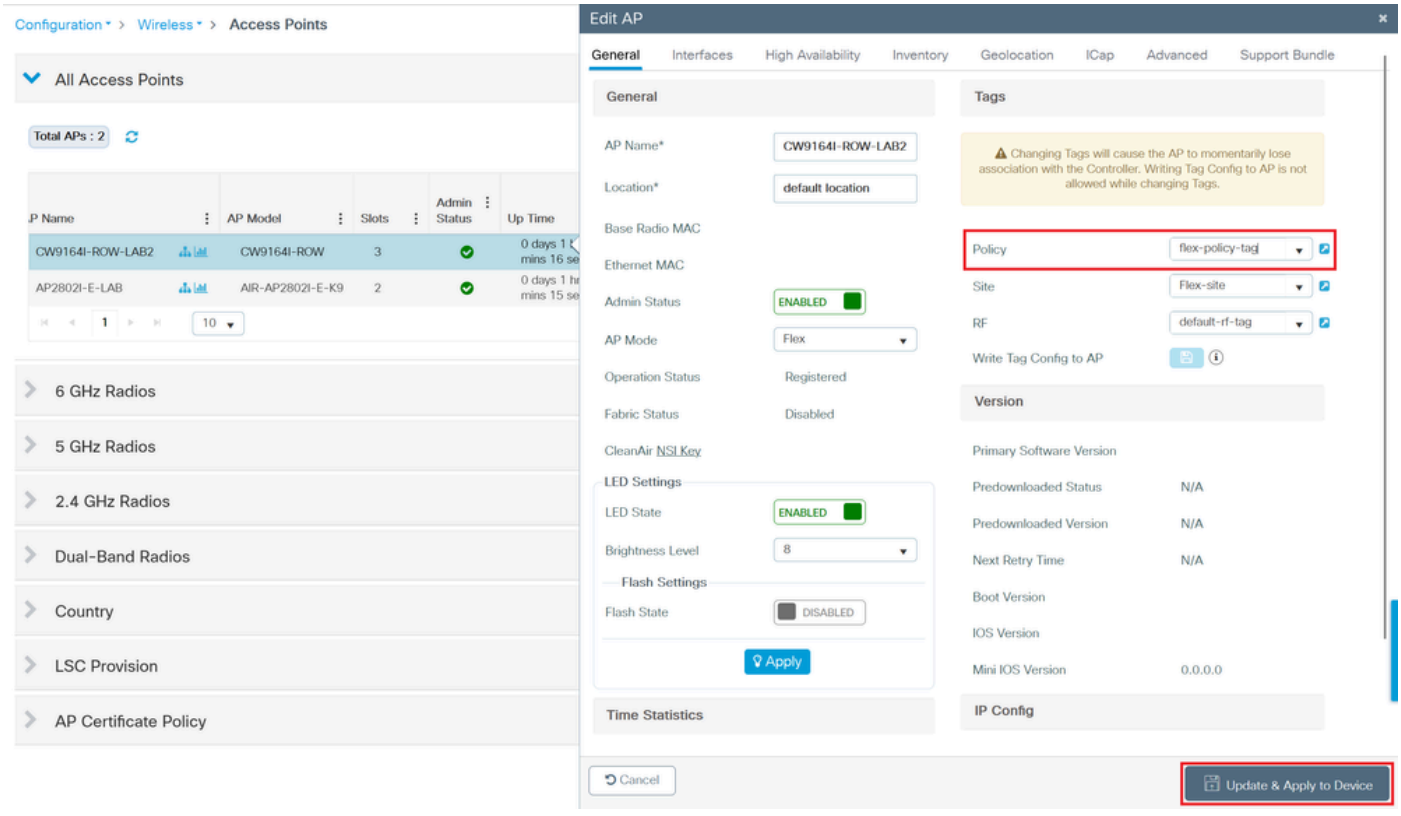


您可以在列表中看到策略标记：



步骤9.在AP标记上分配策略标记。

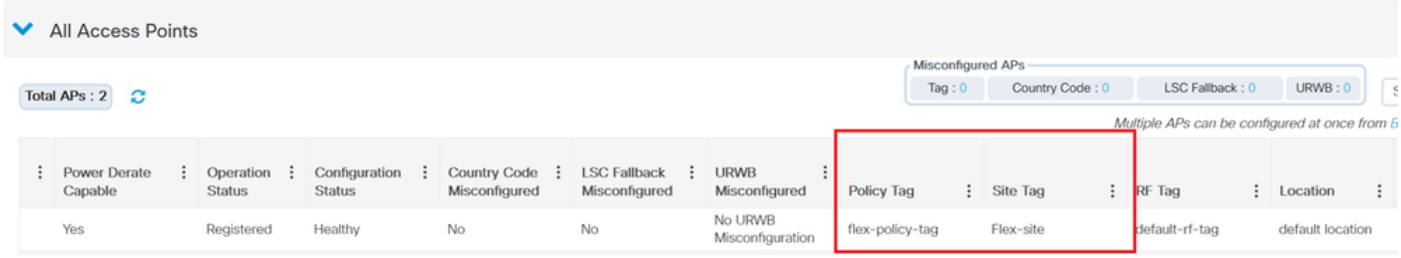
导航到配置>无线>接入点。选择AP以更改标记。



单击Update & Apply to Device。

AP将解除，然后使用新的策略标记重新加入。

当AP重新加入时，您可以检查Access Points列表，确认AP处于Flex模式，以及分配的标记：



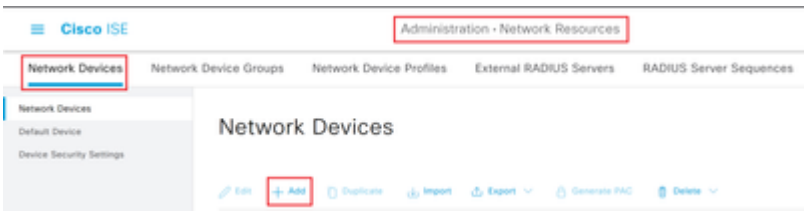
CLI：

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

配置ISE

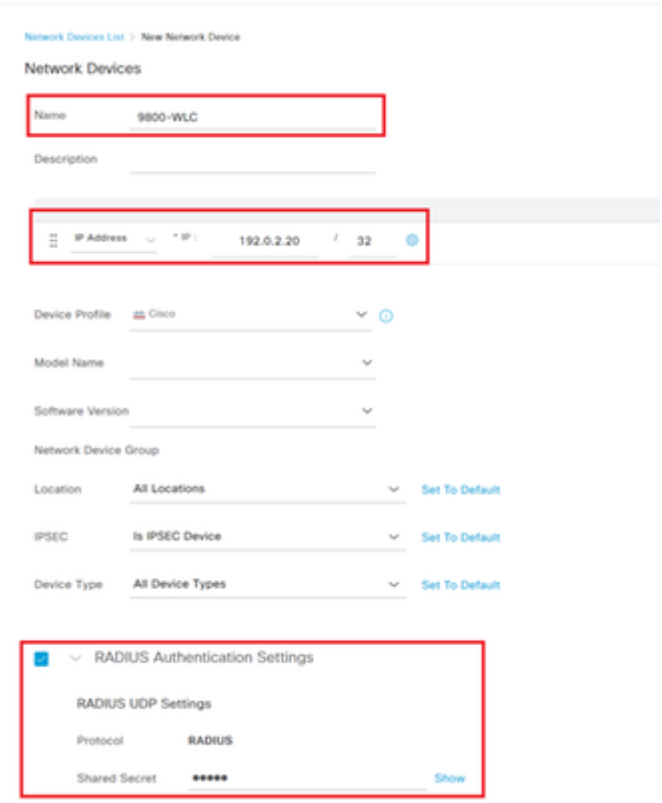
现在，您需要配置ISE才能在客户端处于本地身份验证时对其进行身份验证。

第1步：导航到管理>网络资源>网络设备。选择+Add。



步骤2.添加9800 WLC。为其指定一个名称，添加其IP地址，启用RADIUS身份验证设置，并添加共

享密钥。此密钥必须与之前在9800 WLC上创建AAA服务器时配置的密钥相同。



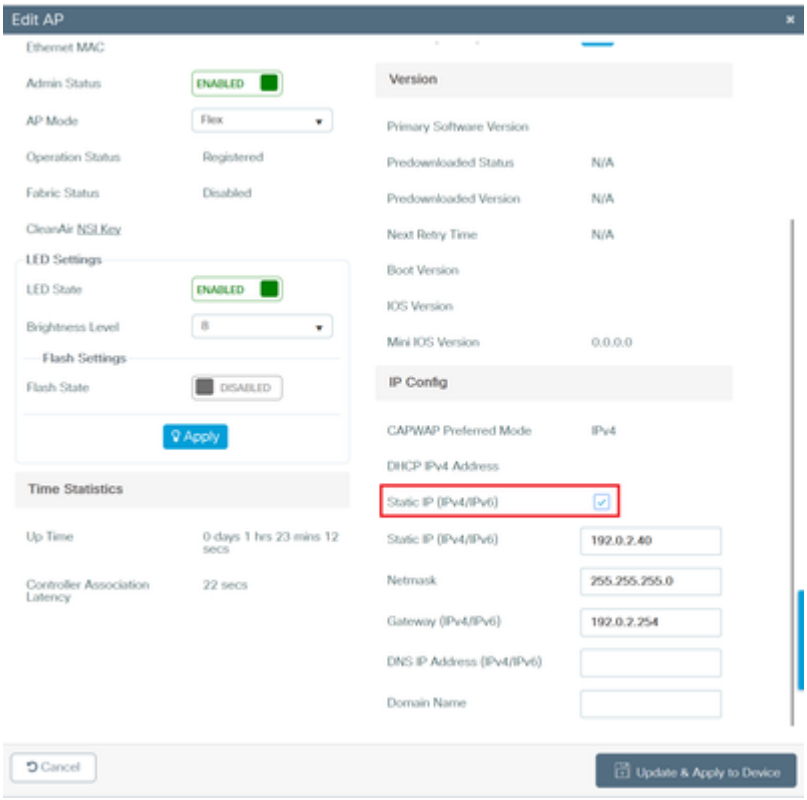
在右下角，单击Save。

步骤3.我们需要将AP添加到“网络设备”列表中，以便在远程站点丢失WAN链路时（以及AP移动到独立模式时），AP能够充当AAA身份验证器/转发器。

在9800 WLC GUI上导航到Configuration > Wireless > Access Points，并记录每个AP IP地址。

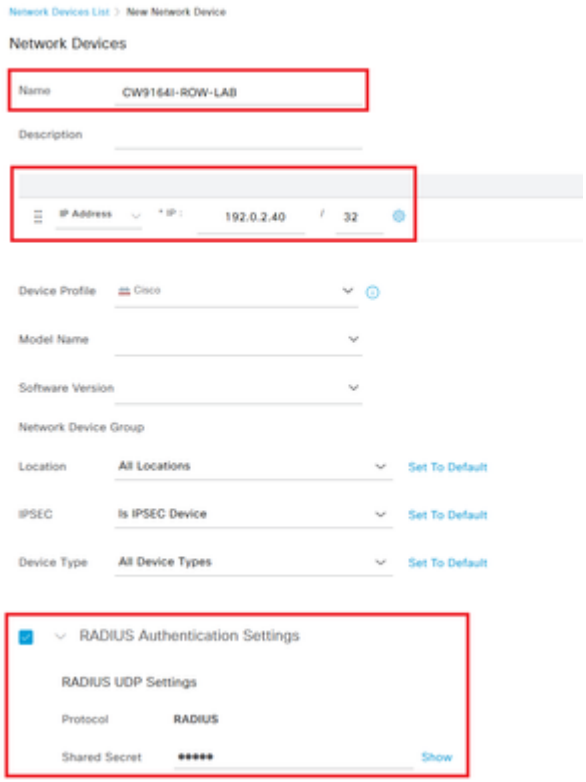
注意：将每个Flex AP的IP地址配置为Static。当AP松动并重新连接到9800 WLC时，它们可能会返回一个与DHCP不同的IP地址，从而丢失与ISE的通信。

启用静态IP(IPv4/IPv6)。 单击Update & Apply to Device:



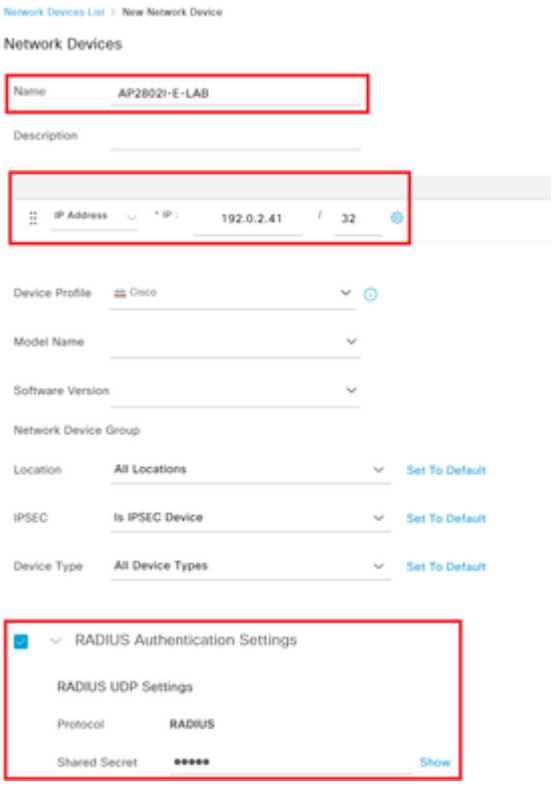
第4步：返回ISE，导航到管理>网络资源>网络设备。选择+Add。

将您的AP添加为网络设备，配置与9800 WLC相同：



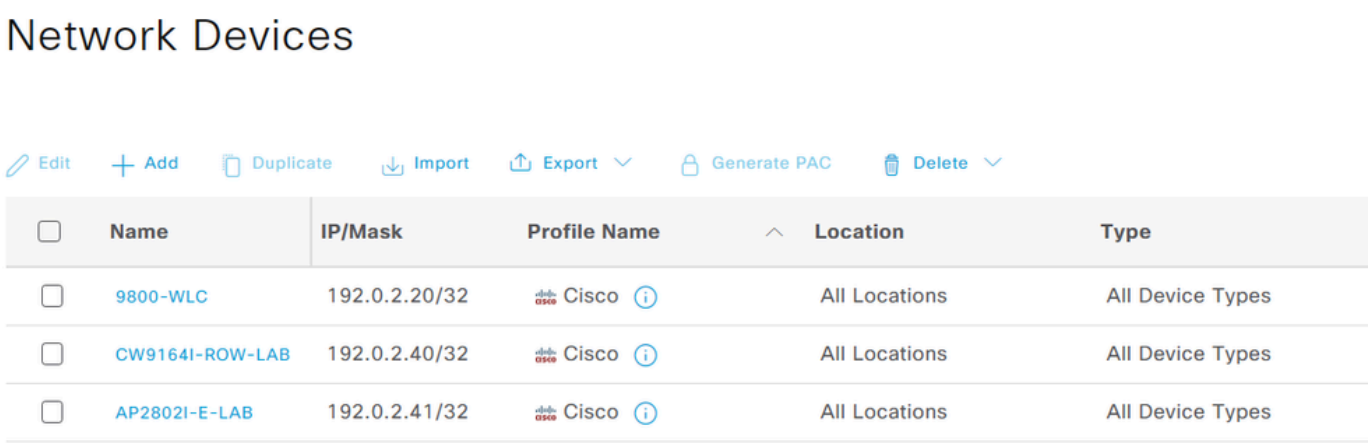
在右下角，单击Save。

对于第二个AP:



在右下角，单击Save。

您可以看到以下网络设备列表：



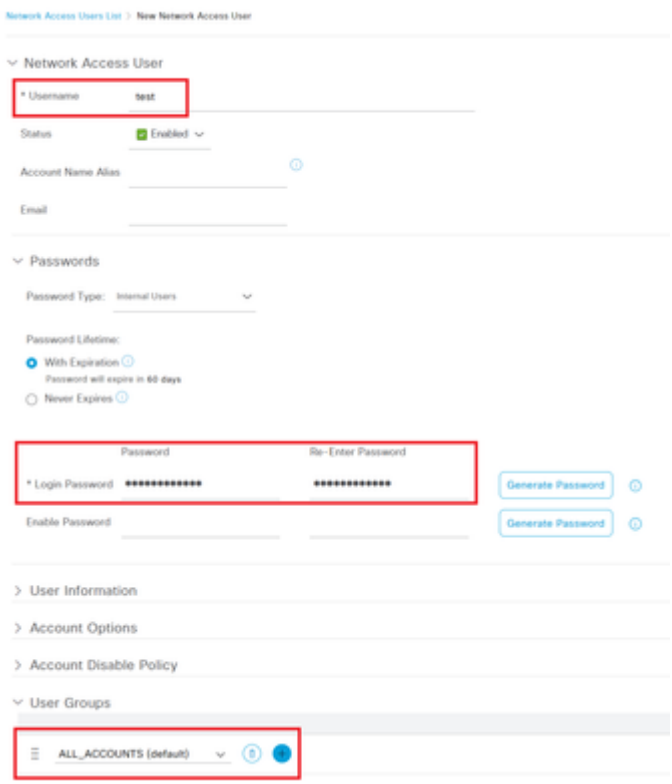
如果AP在连续的IP范围内，您可以使用掩码功能配置单个条目，该条目为整个AP组（如果不是全部）定义共享密钥。在ISE中，实际上不需要为每个AP配置一个网络设备。但请注意，通过使用通

配符和掩码，可为非法设备留出一些空间来尝试作为ISE的转发器。

第5步：在用户选项卡上导航到管理>身份管理>身份，并创建用于802.1x身份验证的用户。选择+添加:

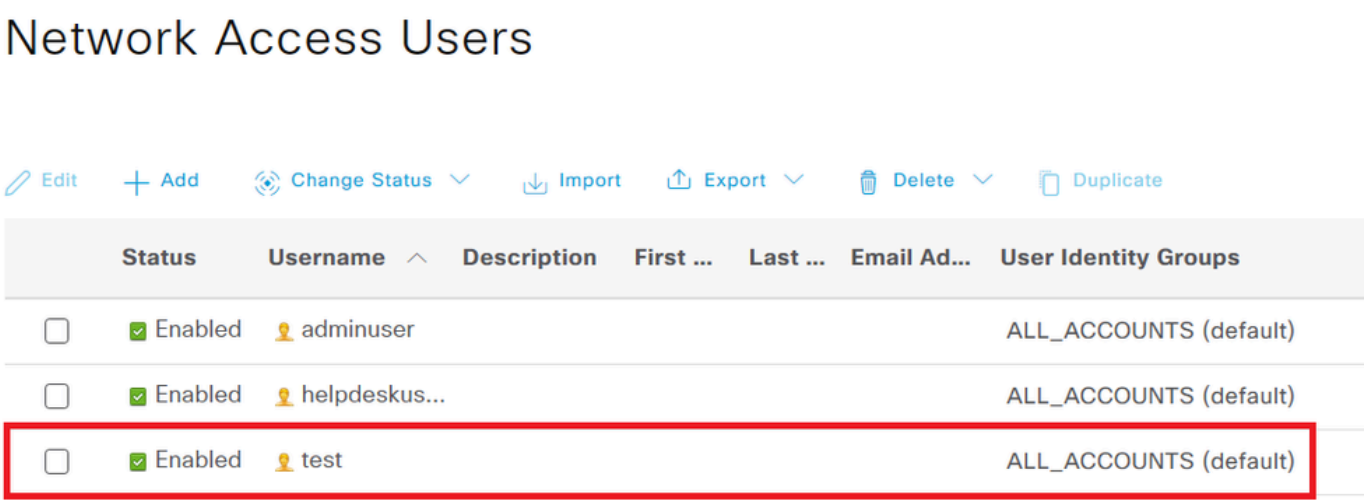


创建用户名、密码（并在重新输入密码时键入相同的密码），然后从User Groups下拉菜单中选择ALL_ACCOUNTS（默认值）：



在右下角，单击Submit。

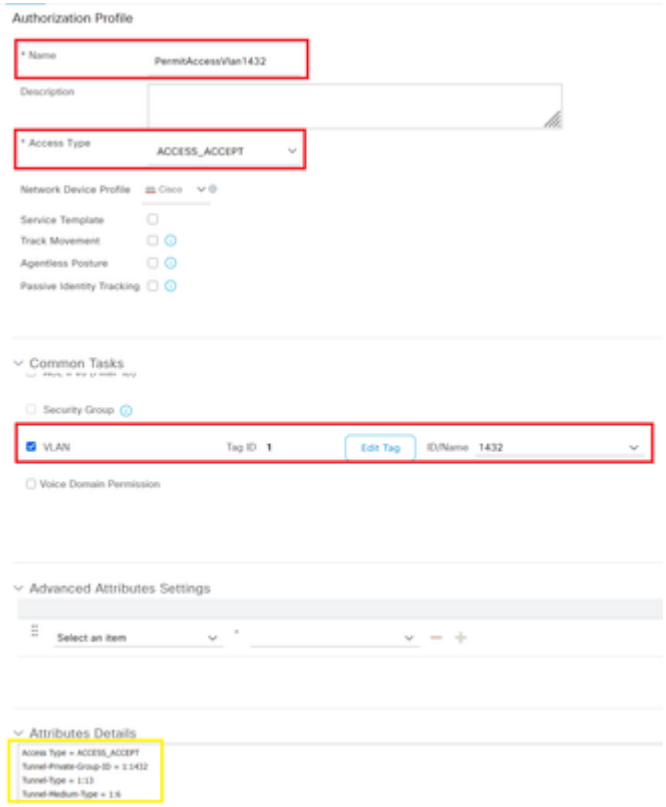
您可以在Network Access Users列表中看到用户：



步骤6.导航到策略>策略元素>结果。在Authorization > Authorization Profiles选项卡上，选择+Add。



为分配了本地身份验证客户端的VLAN创建授权配置文件：

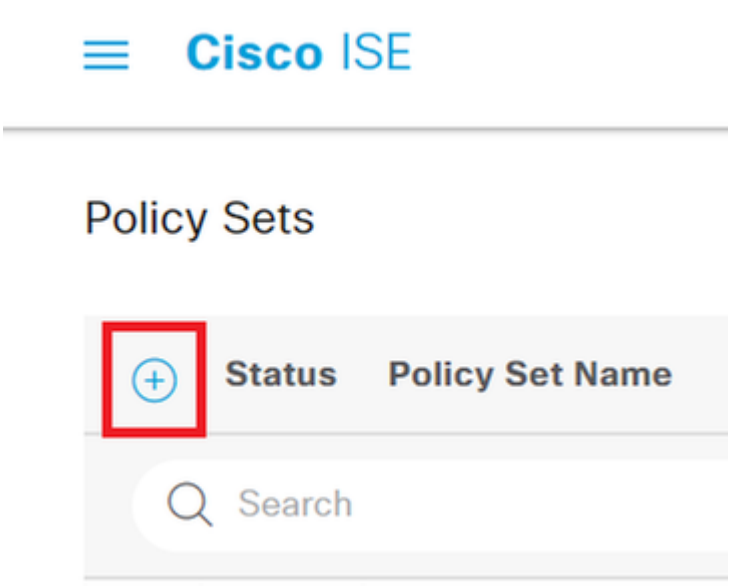


在右下角，单击Submit。

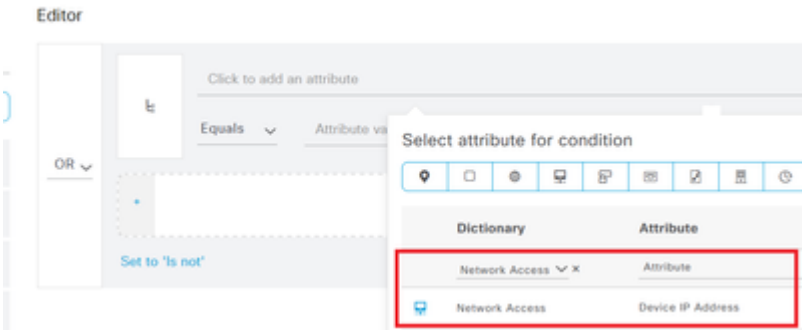
您会看到ISE在成功场景中发送到WLC/AP的属性详细信息。

第 7 步： 导航至策略 > 策略集。创建新策略集。

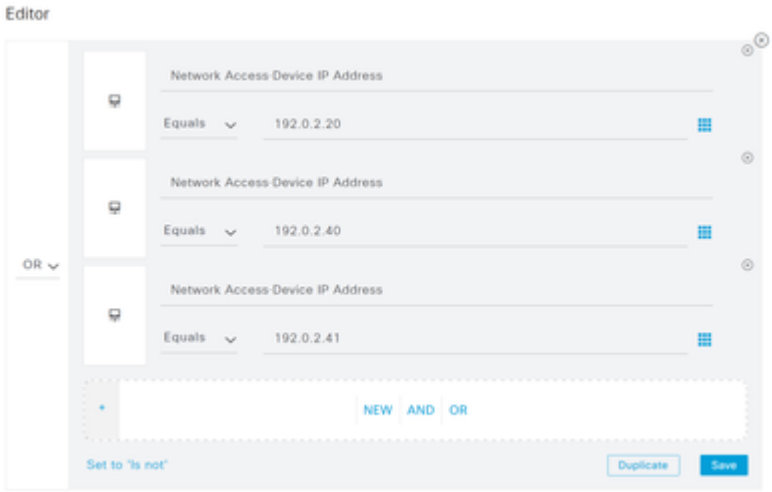
单击+符号：



为策略集命名。在Conditions列上，添加OR规则并添加词典Network Access，在Attribute Device IP Address中选择Equals:

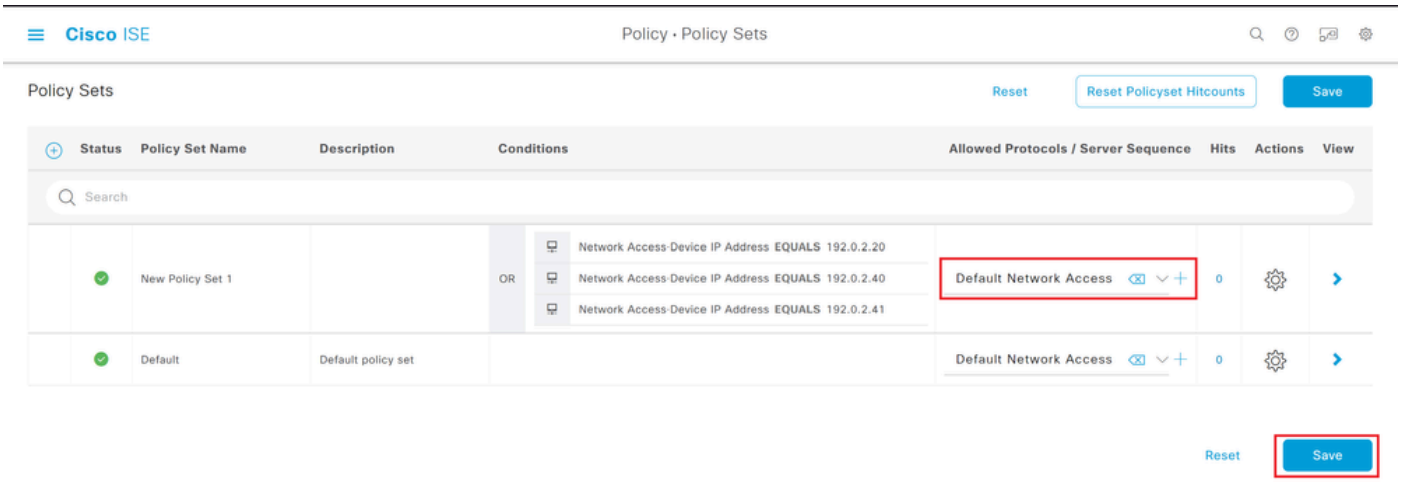


添加9800 WLC和AP的IP地址：

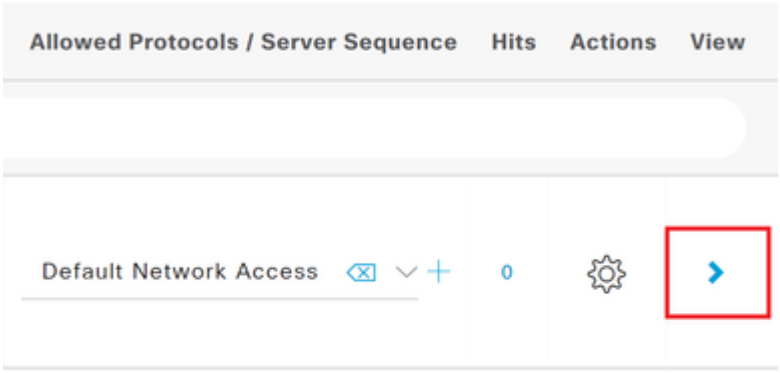


在右下角，单击Use。

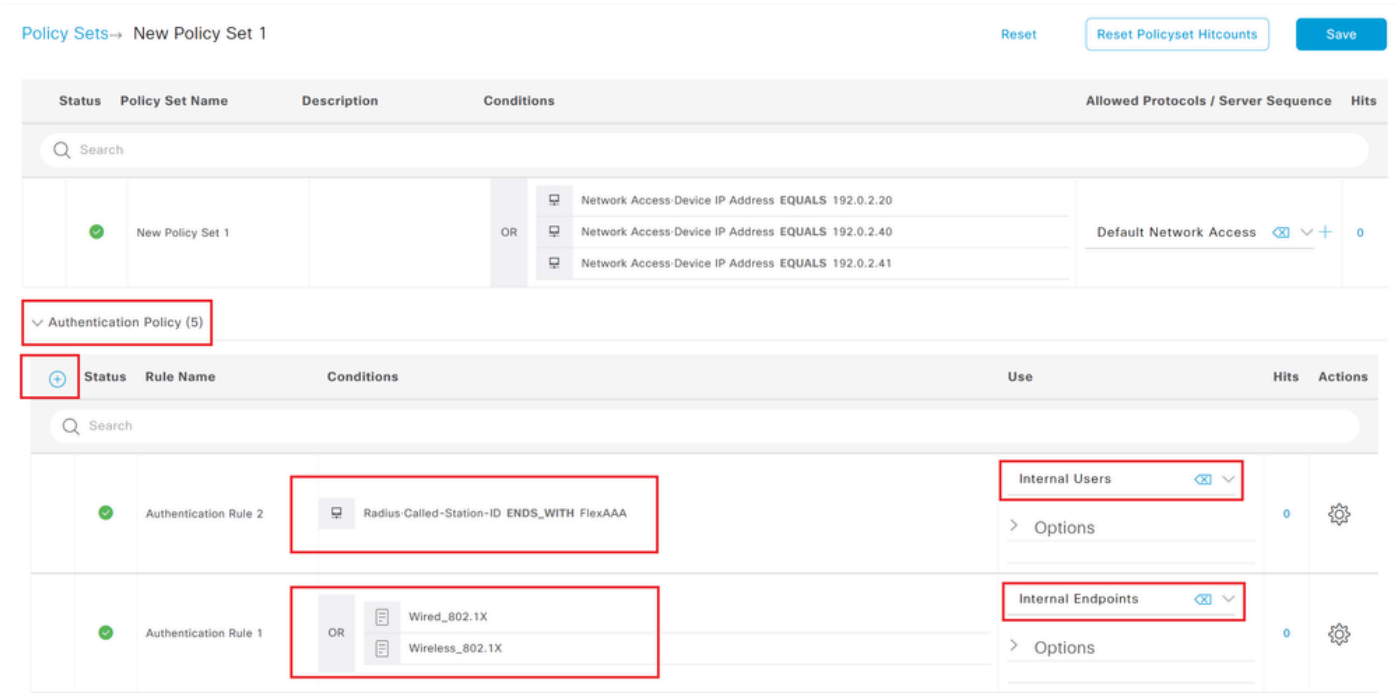
步骤8.在Allowed Protocols列中，选择Default Network Access。最后，单击Save:



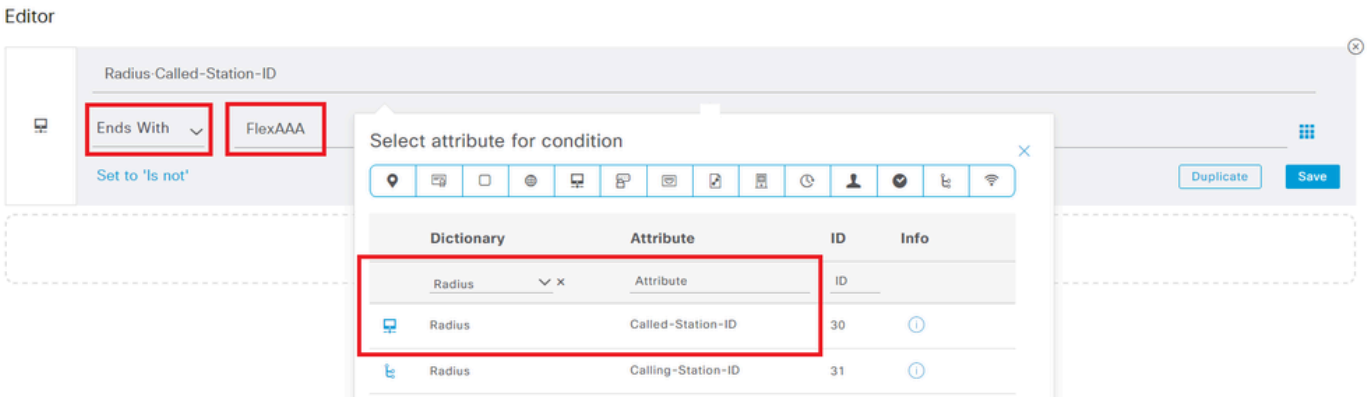
步骤9.在View列中，单击箭头符号：



步骤10.展开Authentication Policy，创建两个新策略：一个用于WLAN名称，另一个用于802.1X配置：

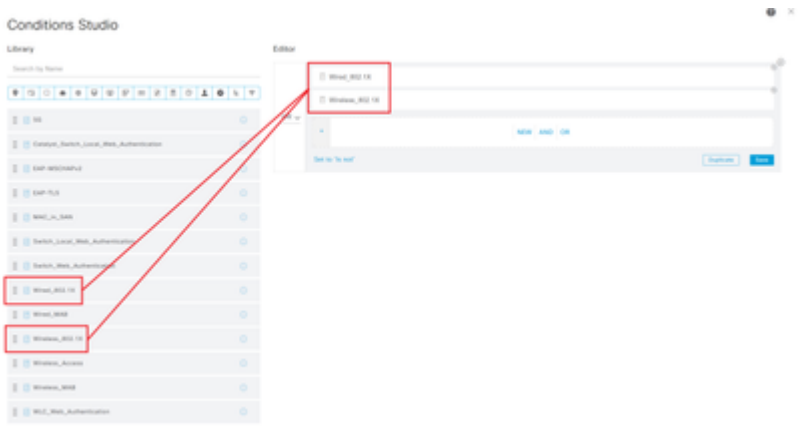


对于WLAN名称，使用字典Radius和属性Called-Station-ID创建Condition。选择Ends With并键入WLAN名称：



在右下角，单击Use。对于此策略，在Use列上，选择Internal Users。

步骤11.对于802.1X策略，使用ISE上可用的Wired_802.1X和Wireless_802.1X库创建Condition。您可以拖放这些项目，然后选择条件或：



在右下角，单击Use。对于此策略，在Use列上，选择Internal Endpoints。

步骤12.向下滚动到Authorization Policy并创建新策略。为其指定一个名称，并创建与身份验证策略上为WLAN名称创建的相同条件。

在Profiles列上，从下拉菜单中选择配置文件PermitAccessVlan1432:



在右下角，单击Save。

使用本地身份验证配置PSK WLAN

步骤1.首先按照“在远程站点上配置FlexConnect模式”一节所述配置AP。

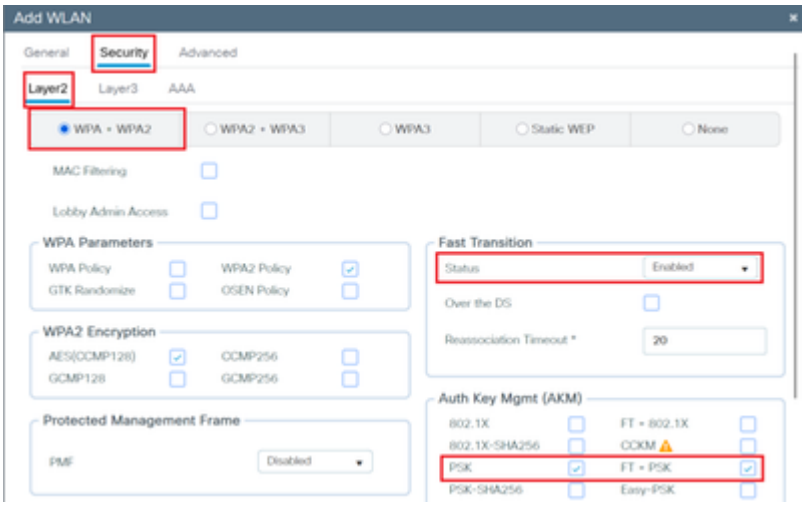
第 2 步： 创建 WLAN.

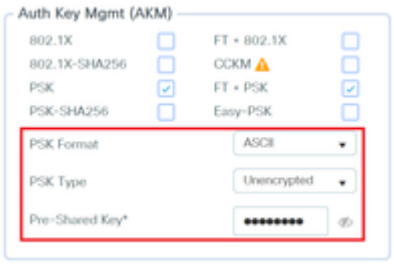
导航到Configuration > Tags & Profiles > WLANs，选择+Add。

在General标记上，为配置文件名称、SSID创建一个名称，并启用状态：



第3步：导航到安全>第2层选项卡，选择WPA+WPA2、快速转换已启用、身份验证密钥管理PSK和FT+PSK，选择所需的PSK格式和PSK类型，并键入希望客户端使用的预共享密钥：





单击Update & Apply to Device。

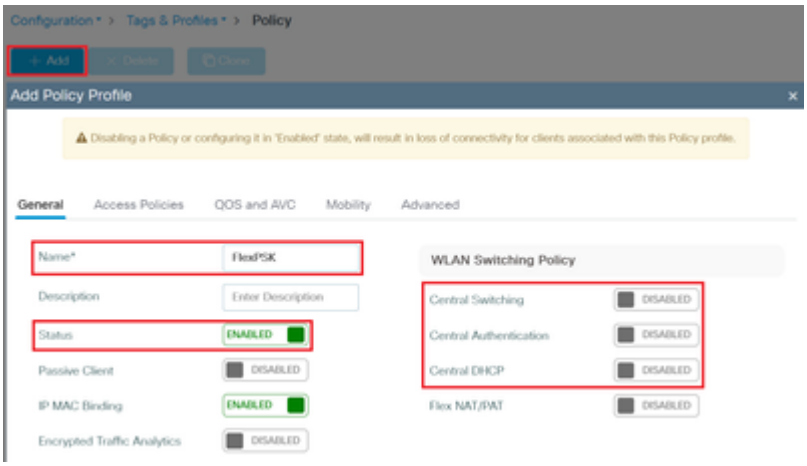
您可以看到创建的WLAN:



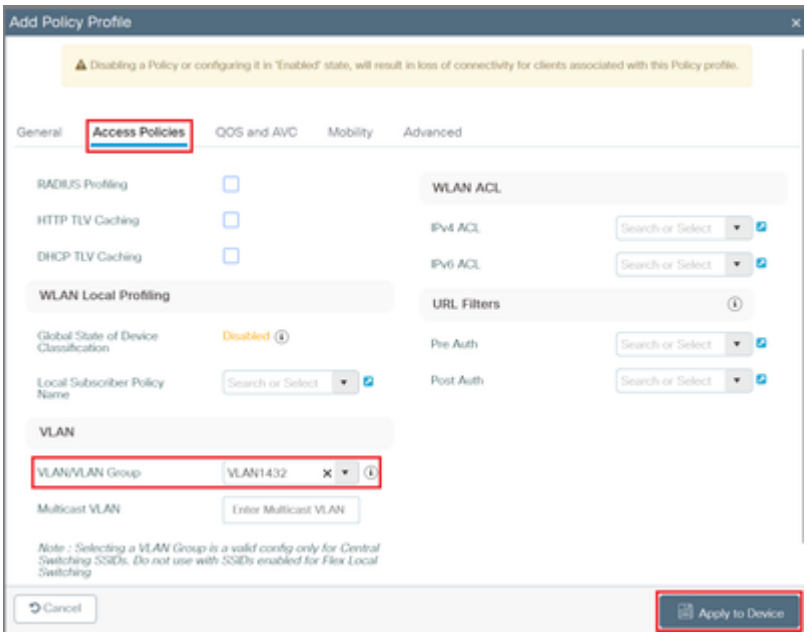
步骤4.创建策略配置文件。

导航至配置 > 标签和配置文件 > 策略。

选择+Add，并在General选项卡上为策略配置文件命名，启用状态，并禁用集中交换、集中身份验证和集中DHCP:

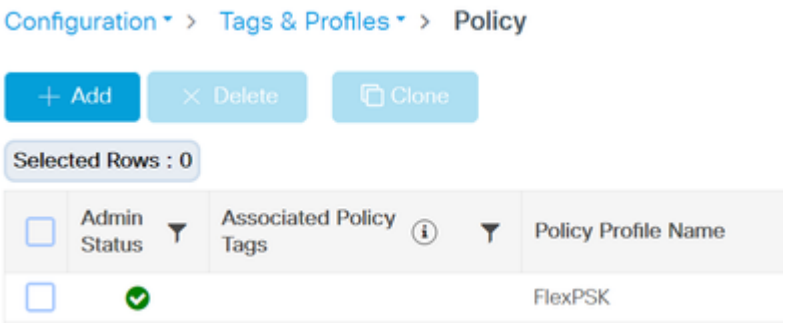


步骤5.导航到访问策略选项卡，选择VLAN:



单击Update & Apply to Device。

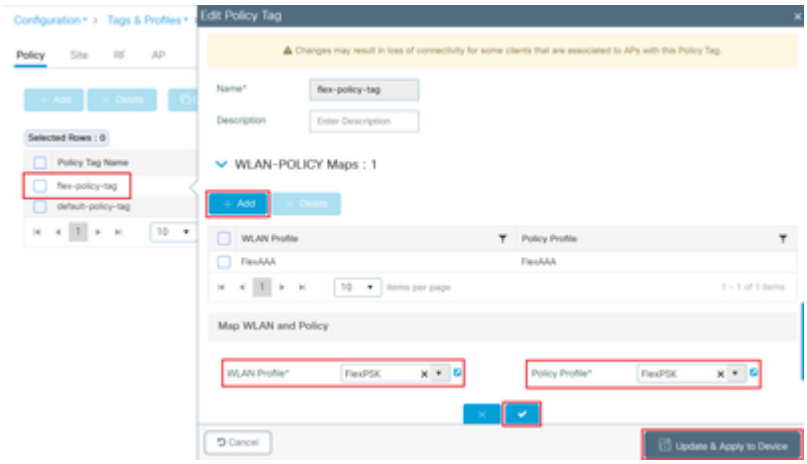
您可以在列表中看到策略配置文件：



步骤6.可以创建新的策略标记，也可以编辑现有策略标记。

导航到Configuration > Tags & Profiles > Tags以编辑现有策略标记。选择要编辑的标记。

在WLAN-POLICY Maps下选择+Add。在WLAN配置文件上，从下拉菜单中选择之前创建的WLAN。在Policy Profile上，从下拉菜单中选择之前创建的策略配置文件。单击check（检查）按钮，然后单击Apply to Device:



如果在AP上已分配策略标记，则无需执行其他操作。

如果不是，请在AP标记上分配策略标记。导航到“配置”>“无线”>“接入点”。选择AP以更改策略标记，然后点击“更新并应用到设备”。

AP会断开连接，然后使用新的策略标记重新连接。

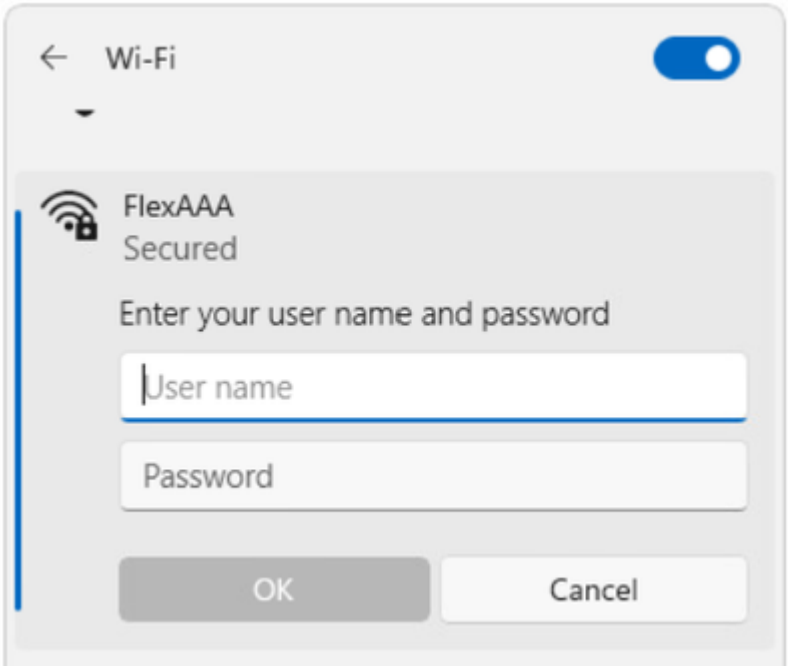
当AP重新加入时，您可以检查Access Points列表，确认AP处于Flex模式，并且它具有正确的分配标记。

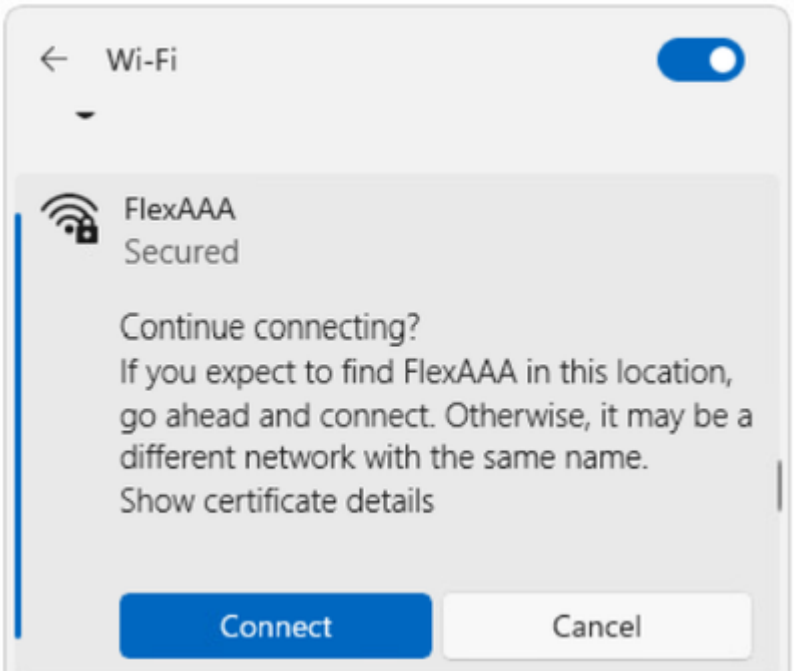
CLI：

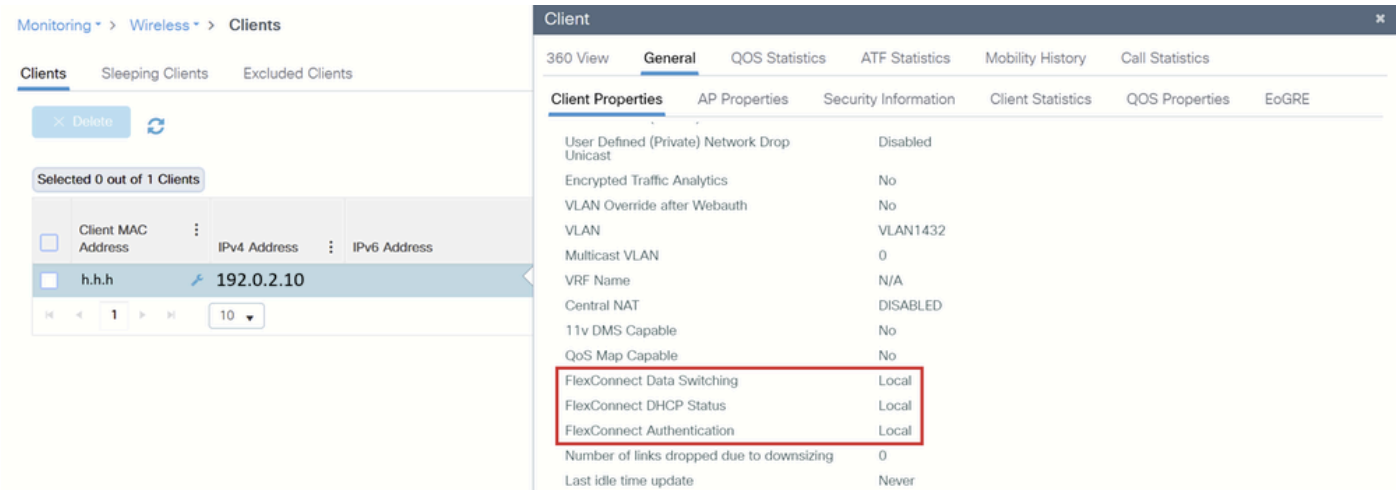
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

验证

对于802.1x WLAN:







CLI：

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

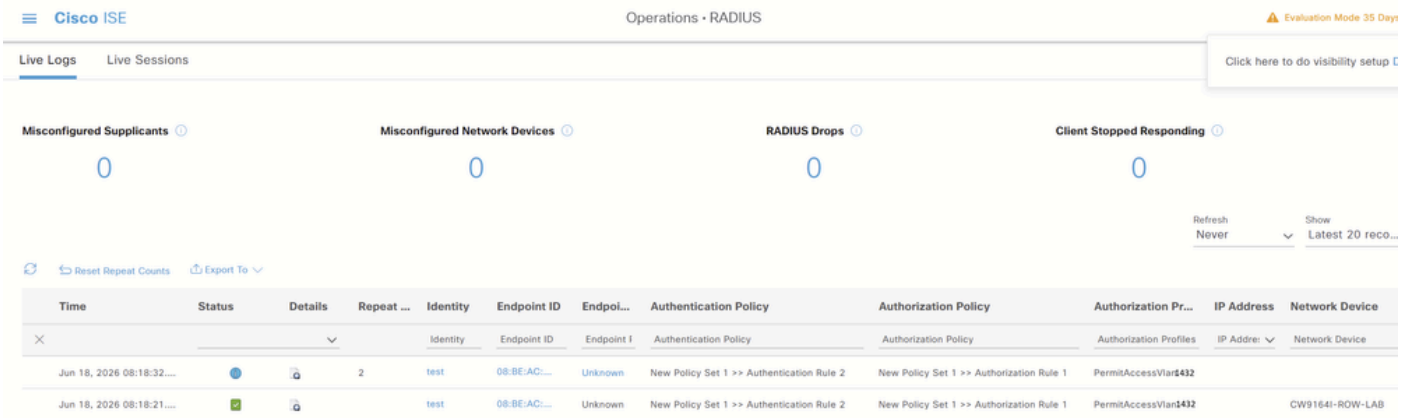
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

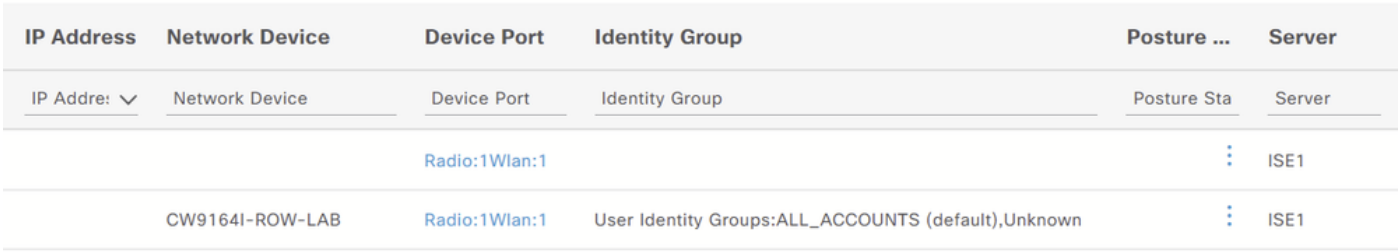
在AP CLI上：

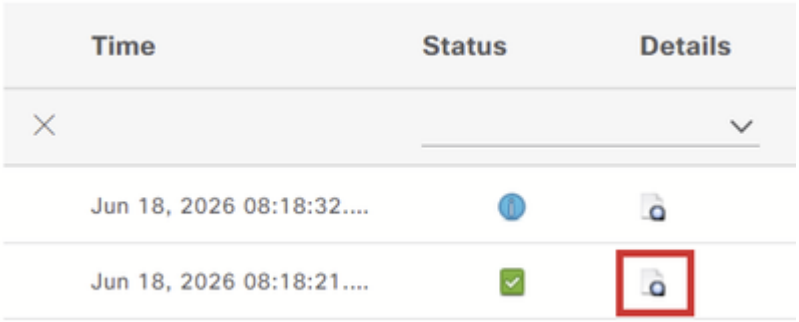
```
CW9164I-ROW-LAB#show dot11 clients

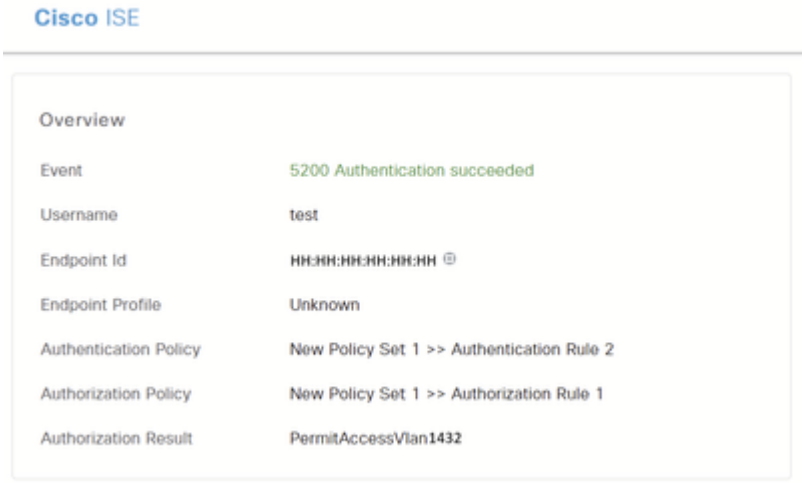
Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH          1       1  33   FlexAAA  -45 MCS9ISS           No          No
```

在ISE上


Cisco ISE
Operations · RADIUS
Evaluation Mode 35 Days
Live Logs
Live Sessions
Click here to do visibility setup
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Refresh
Never
Show
Latest 20 reco...
Reset Repeat Counts
Export To
Time
Status
Details
Repeat ...
Identity
Endpoint ID
Endpoi...
Authentication Policy
Authorization Policy
Authorization Pr...
IP Address
Network Device
Jun 18, 2026 08:18:32....
2
test
08:BE:AC:...
Unknown
New Policy Set 1 >> Authentication Rule 2
New Policy Set 1 >> Authorization Rule 1
PermitAccessVlan1432
Jun 18, 2026 08:18:21....
test
08:BE:AC:...
Unknown
New Policy Set 1 >> Authentication Rule 2
New Policy Set 1 >> Authorization Rule 1
PermitAccessVlan1432
CW9164I-ROW-LAB

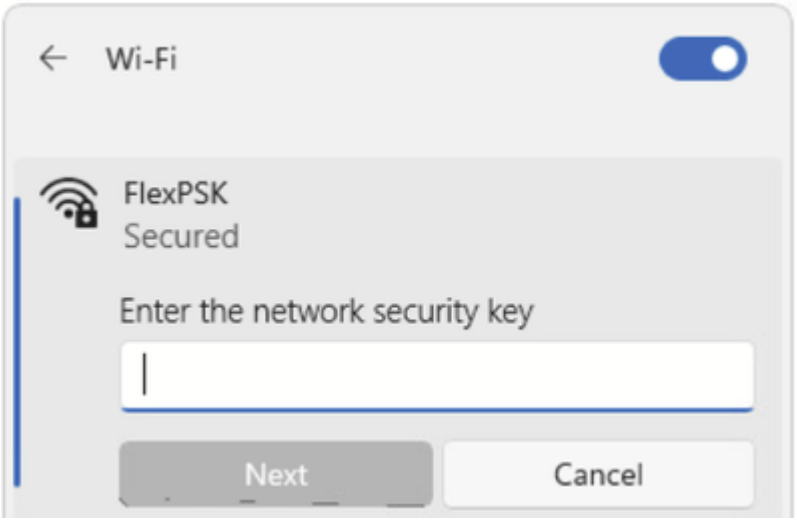

IP Address
Network Device
Device Port
Identity Group
Posture ...
Server
IP Addre:
Network Device
Device Port
Identity Group
Posture Sta
Server
Radio:1Wlan:1
ISE1
CW9164I-ROW-LAB
Radio:1Wlan:1
User Identity Groups:ALL_ACCOUNTS (default),Unknown
ISE1

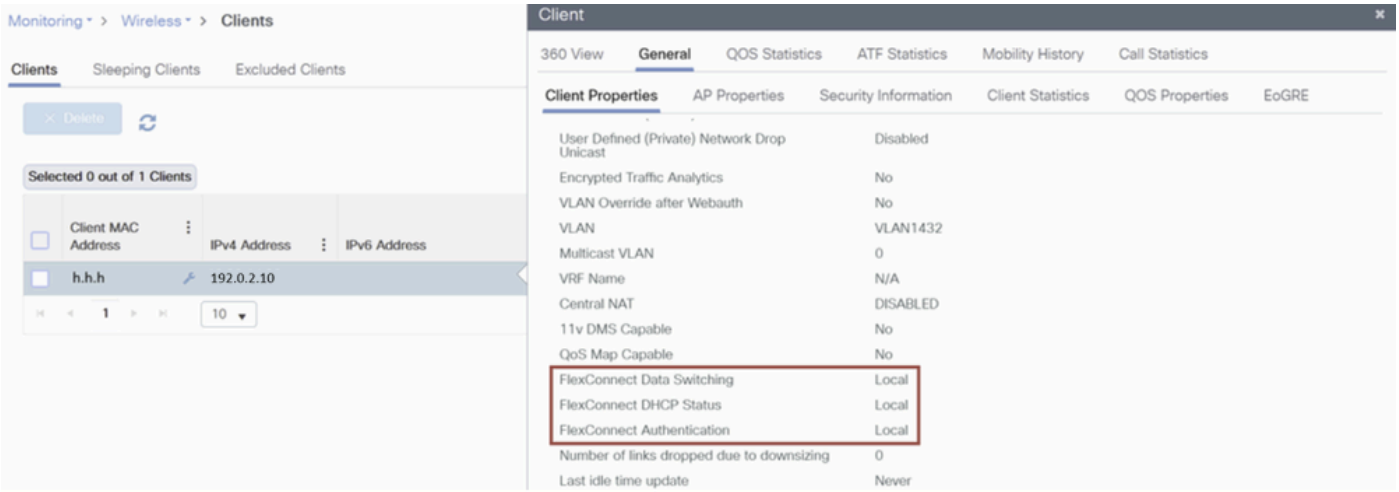

Time
Status
Details
Jun 18, 2026 08:18:32....
Jun 18, 2026 08:18:21....


Cisco ISE
Overview
Event
5200 Authentication succeeded
Username
test
Endpoint Id
HH:HH:HH:HH:HH:HH
Endpoint Profile
Unknown
Authentication Policy
New Policy Set 1 >> Authentication Rule 2
Authorization Policy
New Policy Set 1 >> Authorization Rule 1
Authorization Result
PermitAccessVlan1432

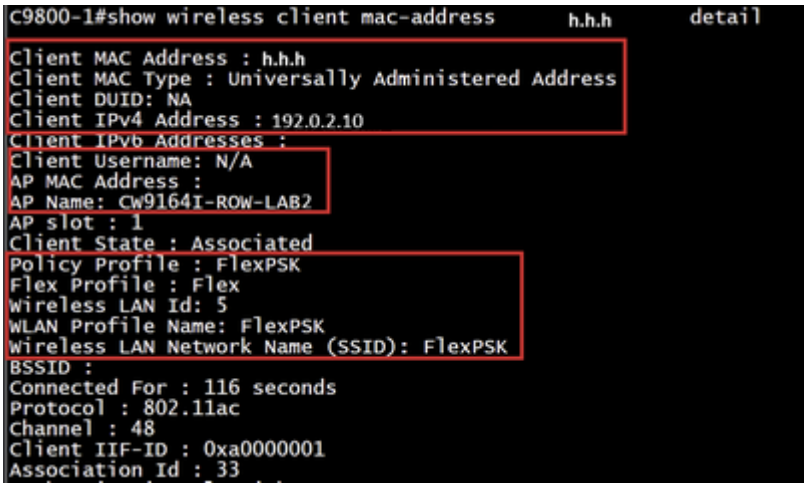
Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

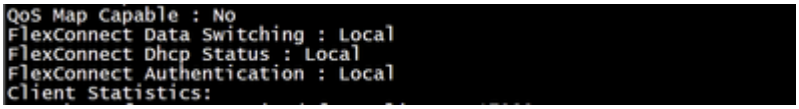
对于PSK WLAN:



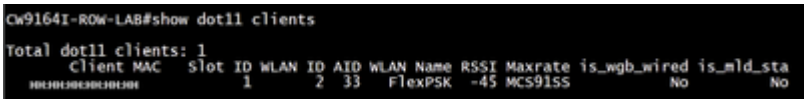


CLI：





在AP CLI上：



故障排除

使用客户端MAC地址同步启用AP调试和RA跟踪。

在AP上启用以下调试：

debug flexconnect event
debug flexconnect pmk
debug flexconnect dot11r
debug dot11 client management information
debug dot11 client management critical
debug dot11 client management errors
debug dot11 client management events

对于802.1x WLAN:

AP调试成功身份验证的日志：

AP处理802.11状态机和本地密钥管理。
AP处理关联并准备客户端进行身份验证。

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

AP处理授权，应用VLAN覆盖，并将客户端移至FWD（转发）状态。

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

相同成功身份验证的RA跟踪日志：

RA跟踪记录会话的WLC协调。WLC验证客户端身份和策略。
WLC识别FlexConnect关联。

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

WLC将策略推送到AP。

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
```

```
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

授权成功。

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

客户端参数。
2026/06/19 06:49:20.939394217 {wncd_x_R0-1}{1}:[dot11] [18318]:（注）：MAC :hhhh.hhh.hhh客户端数据路径条目参数 — ssid:FlexAAA，slot_id:1 bssid ifid:0x0,radio_ifid:0x90400008,wlan_ifid:0xf0400004

WLC通过本地DHCP/ARP获取IP。
2026/06/19 06:49:21.001000218 {wncd_x_R0-1}{1}:[client-iplearn] [18318]:（注）：MAC :hhhh.hhh.hhhh客户端IP学习成功。方法：IP监听IP:192.0.2.10

客户端已完全连接。
2026/06/19 06:49:21.002363496 {wncd_x_R0-1}{1}:[errmsg] [18318]:（信息）%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE:R0/1:wncd:使用MAC的设备的ssid(FlexAAA)加入的用户名条目（测试）：hhhh.hhhh.hhhh on channel(48)
2026/06/19 06:49:21.002795009 {wncd_x_R0-1}{1}:[客户端工作状态] [18318]:（注）：MAC :hhhh.hhh.hhhh客户端状态转换：S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

独立方案

AP-WLC连接丢失和后续恢复期间的行为。

AP已加入WLC。客户端成功执行802.1X身份验证，AP将客户端转换为FWD（转发）状态。

在ISE RADIUS实时日志中，我们看到客户端会话。

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

AP无法到达WLC，耗尽其重新传输计数，然后切换到独立模式。现有客户端在本地保持连接。

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

但客户端仍然处于连接状态：

CW9164I-ROW-LAB2#show dot11 clients

Dot11客户端总数：1
客户端MAC插槽ID WLAN ID AID WLAN名称RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7否否

当客户端在独立模式下漫游到另一个AP时，由于无法到达RADIUS服务器，EAP握手失败。客户端已取消授权并从AP中删除。

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

AP将客户端会话发送到备份RADIUS服务器。

AP重新连接到WLC。AP切换回连接模式，并将本地客户端会话信息与WLC同步。

客户端会话根据AP连接状态在主和备份ISE节点之间转换。

AP和客户端显示为在WLC上已连接，并且当AP和WLC之间的连接关闭时，客户端未发现任何断开或抖动。

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, m
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASS
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD

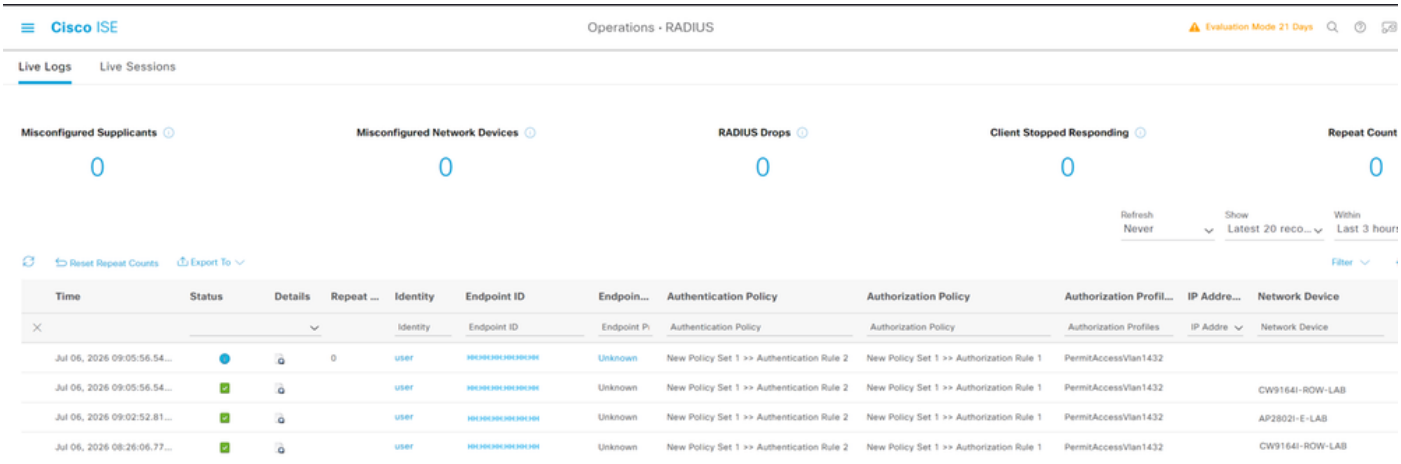

CW9164I-ROW-LAB2#show dot11 clients
```

```
Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No
```

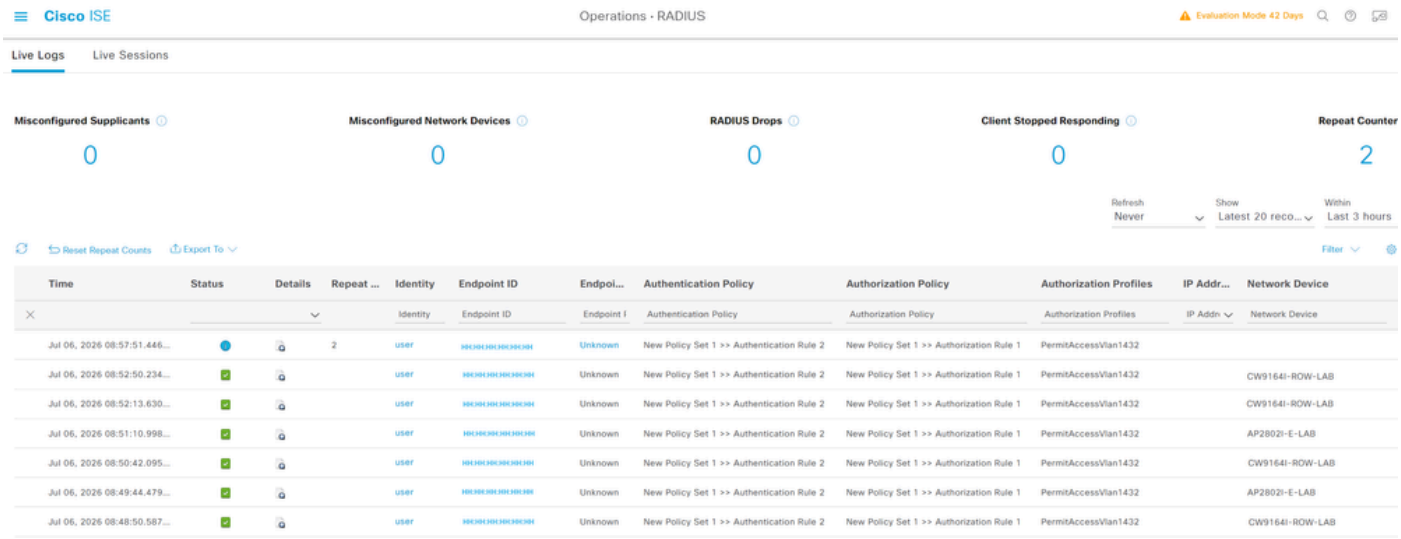
```
*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
```

```
CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



主ISE:记录WLC连接恢复后的初始会话(08:26:06)和续约会话(09:02:52)。



备份ISE:在AP以独立模式运行时捕获会话活动(08:48:50 - 08:57:51)。

第一个会话在08:26:06，之后AP失去与WLC的连接并移至独立模式。

会话09:02:52是AP与WLC重新建立连接后的第一个会话。

相关信息

- CCNP企业无线设计ENWLSD 300-425和实施ENWLSI 300-430官方认证指南，第2版
- Cisco Catalyst 9800系列无线控制器软件配置指南，Cisco IOS XE 17.8.x — 章节：FlexConnect
- Cisco Catalyst 9800系列无线控制器、Cisco IOS XE Cupertino版本17.8.x的发行版本注释
- 思科无线接入点的功能表
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。