使用ISE和Catalyst 9800无线局域网控制器配置动态VLAN分配

目录

简介

本文档介绍动态VLAN分配的概念，以及如何配置Catalyst 9800无线LAN控制器(WLC)和思科身份服务引擎(ISE)来分配无线LAN(WLAN)，以便为无线客户端完成此操作。

要求

Cisco 建议您了解以下主题：

- 了解WLC和轻量接入点(LAP)的基本知识。
- 了解AAA服务器（如ISE）的功能知识。
- 深入了解无线网络和无线安全问题。
- 了解动态VLAN分配的功能知识。
- 了解无线接入点控制和调配(CAPWAP)的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本16.12.4a的Cisco Catalyst 9800 WLC(Catalyst 9800-CL)。
- Cisco 2800系列LAP在本地模式下。
- 本地Windows 10请求方。
- 运行版本2.7的思科身份服务引擎(ISE)。
- 运行固件版本16.9.6的Cisco 3850系列交换机。

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。

背景信息

使用 RADIUS 服务器执行动态 VLAN 分配

在大多数无线局域网(WLAN)系统中，每个WLAN都有一个静态策略，该策略适用于与服务集标识符(SSID)关联的所有客户端。 虽然此方法功能强大，但它有其局限性，因为它要求客户端与不同的SSID关联，以继承不同的QoS和安全策略。

然而，Cisco WLAN 解决方案支持网络标识。这允许网络通告单个SSID，并允许特定用户根据用户凭证继承不同的QoS或安全策略。

动态 VLAN 分配便是一项这样的功能，它根据无线用户提供的凭证将该用户置于特定 VLAN 中。将用户分配到特定VLAN的任务由RADIUS身份验证服务器（如Cisco ISE）处理。例如，利用此任务可使无线主机能够在园区网络中移动时保持位于同一 VLAN 中。

因此，当客户端尝试关联到向控制器注册的LAP时，WLC会将用户的凭证传递到RADIUS服务器进行验证。成功执行身份验证后，RADIUS 服务器便会将某些 Internet 工程任务组 (IETF) 属性传递给用户。这些RADIUS属性决定必须分配给无线客户端的VLAN ID。客户端的SSID无关紧要，因为用户始终被分配到此预定VLAN ID。

用于 VLAN ID 分配的 RADIUS 用户属性包括：

- IETF 64（隧道类型）— 将此项设置为 VLAN。
- IETF 65（隧道介质类型） — 将此值设置为802。
- IETF 81（隧道专用组 ID）— 将此项设置为 VLAN ID。

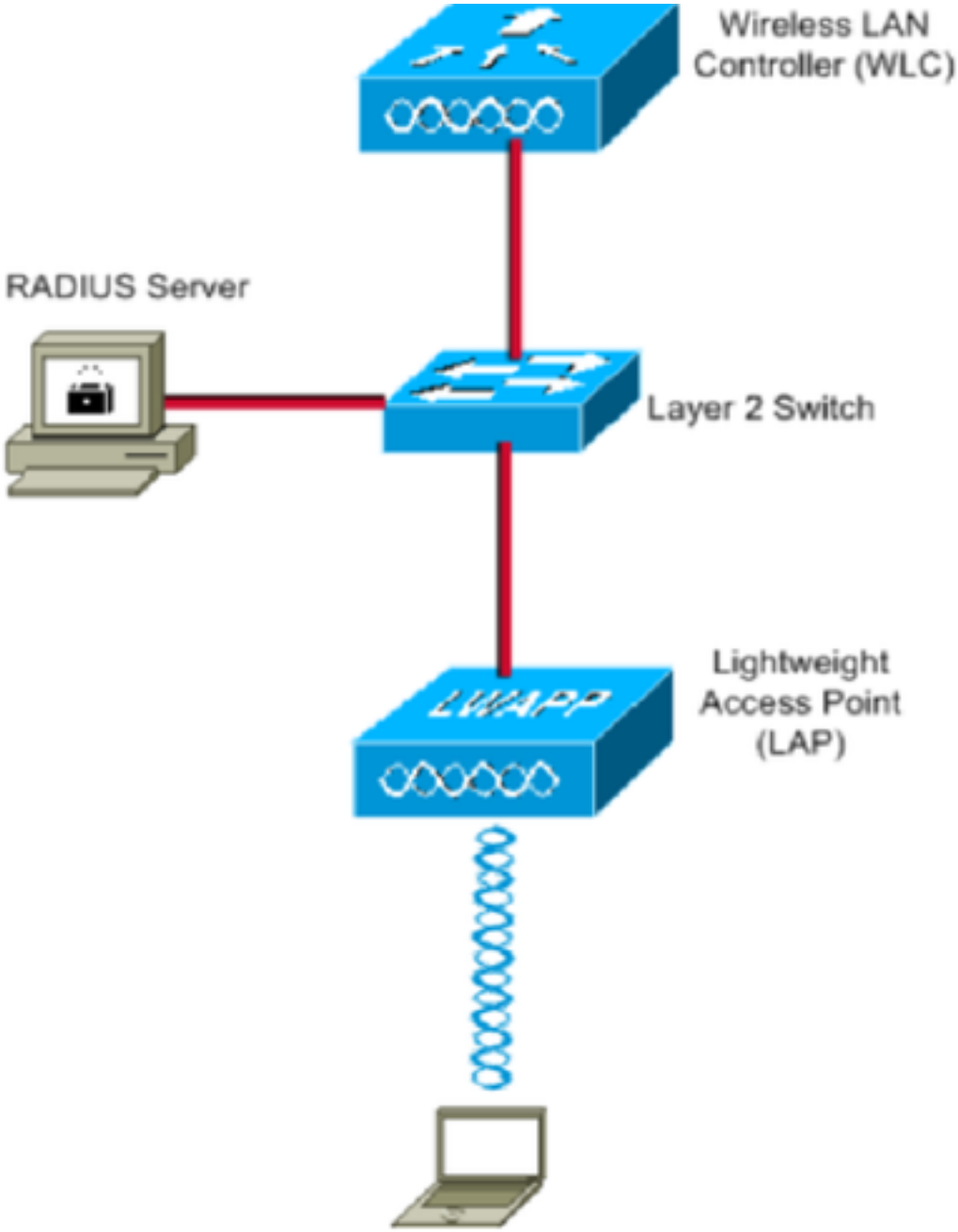
VLAN ID为12位，值介于1和4094之间（含1和4094）。由于隧道专用组 ID 属于字符串类型（如用于 IEEE 802.1X 的 RFC2868 中所定义），因此，VLAN ID 整数值被编码为字符串。发送这些隧道属性时，必须在Tag字段中输入它们。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：



下面是此图中使用的组件的配置详细信息：

- 思科ISE(RADIUS)服务器的IP地址是10.10.1.24。
- WLC 的管理接口地址为 10.10.1.17。
- 控制器上的内部 DHCP 服务器用于将 IP 地址分配给无线客户端。
- 本文档使用802.1x和PEAP作为安全机制。
- VLAN102用于此配置。用户名jonathga-102配置为由RADIUS服务器放入VLAN102。

配置步骤

此配置分为三类：

- 思科ISE配置。
- 为多个 VLAN 配置交换机.
- Catalyst 9800 WLC配置。

思科ISE配置

此配置要求执行下列步骤：

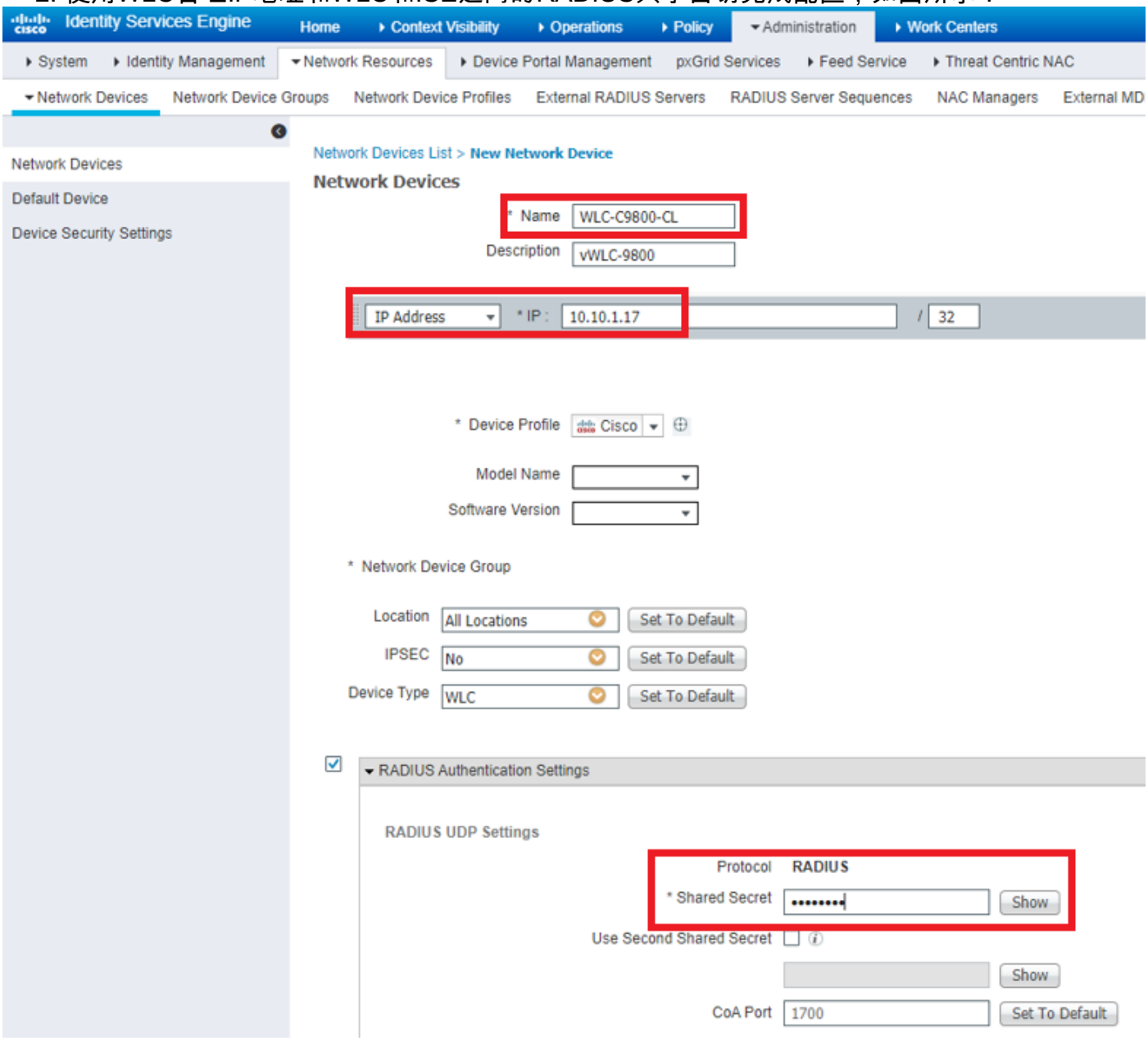
- 将Catalyst WLC配置为Cisco ISE服务器上的AAA客户端。
- 在思科ISE上配置内部用户。
- 在Cisco ISE上配置用于动态VLAN分配的RADIUS(IETF)属性。

步骤1.在Cisco ISE服务器上将Catalyst WLC配置为AAA客户端

此过程说明如何将WLC添加为ISE服务器上的AAA客户端，以便WLC将用户凭证传递给ISE。

请完成以下步骤：

1. 从ISE GUI导航至 **Administration > Network Resources > Network Devices**选择 **Add**。
2. 使用WLC管理IP地址和WLC和ISE之间的RADIUS共享密钥完成配置，如图所示：

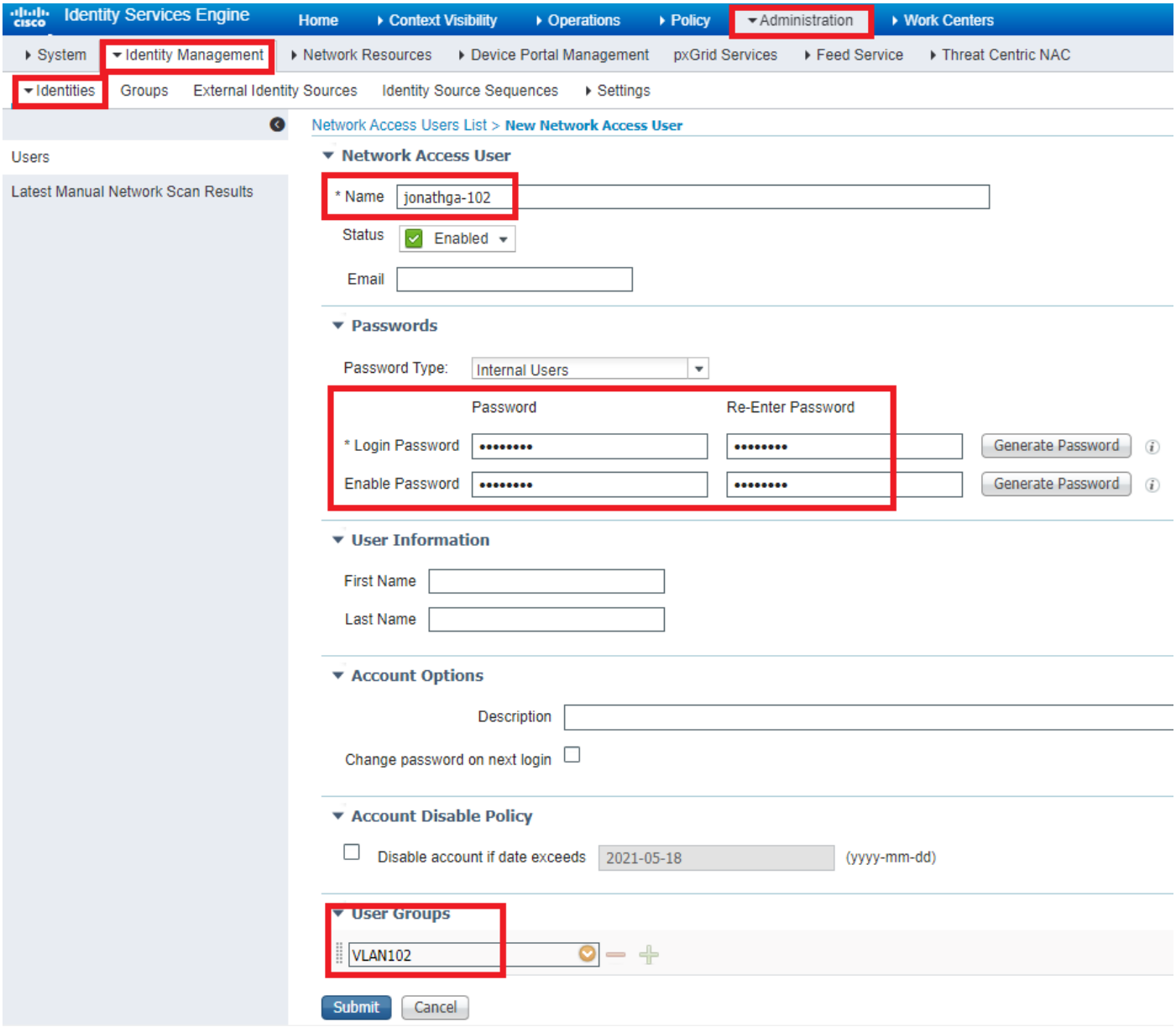


步骤2.在思科ISE上配置内部用户

此过程说明如何在思科ISE的内部用户数据库上添加用户。

请完成以下步骤：

1. 从ISE GUI导航至 **Administration > Identity Management > Identities** 选择 **Add**。
2. 使用用户名、密码和用户组完成配置，如图所示：

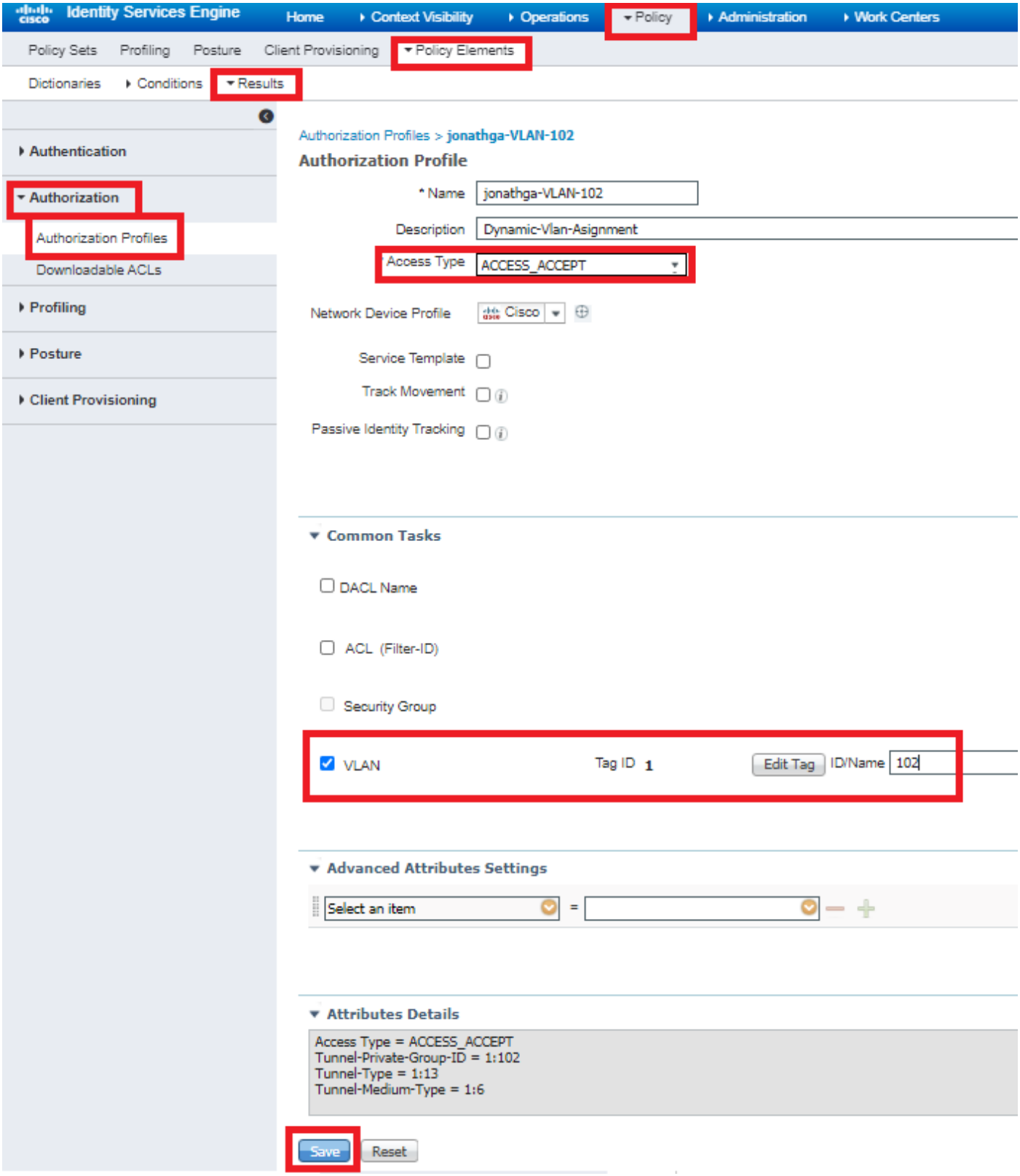


步骤3.配置用于动态VLAN分配的RADIUS(IETF)属性

此过程说明如何为无线用户创建授权配置文件和身份验证策略。

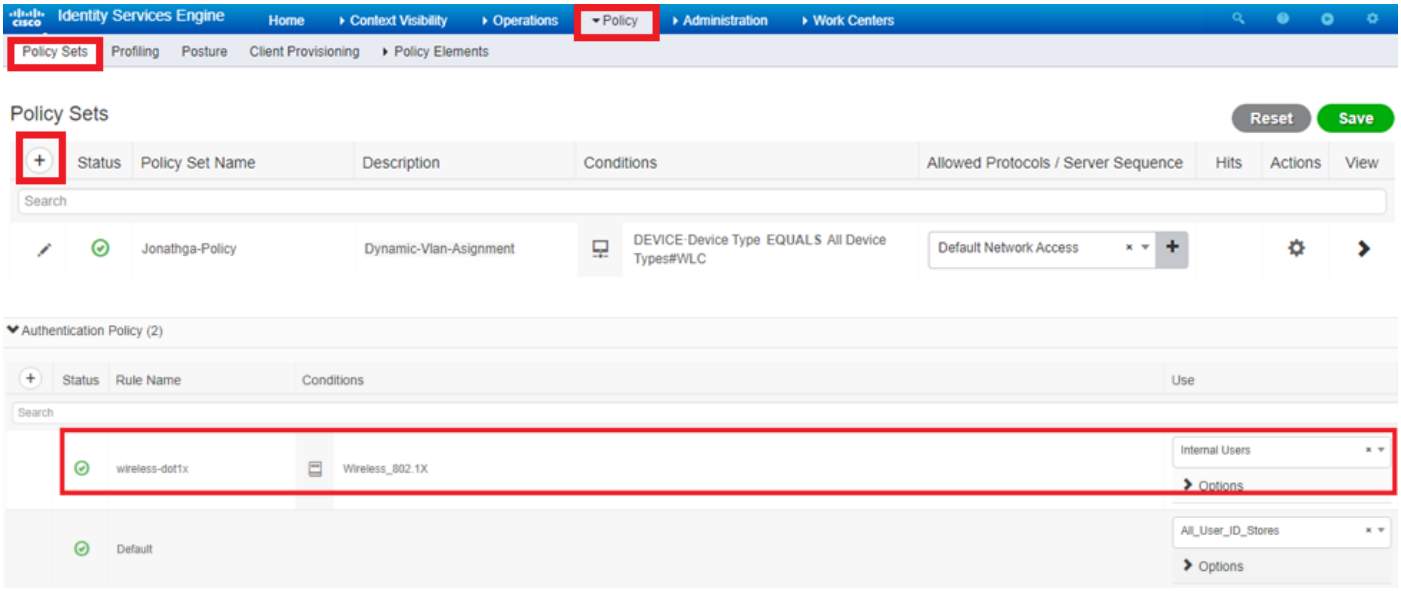
请完成以下步骤：

1. 从ISE GUI导航至 **Policy > Policy Elements > Results > Authorization > Authorization profiles** 选择 **Add** 创建新配置文件。
2. 使用相应组的VLAN信息完成授权配置文件配置。此图显示 **jonathga-VLAN-102** 组配置设置。



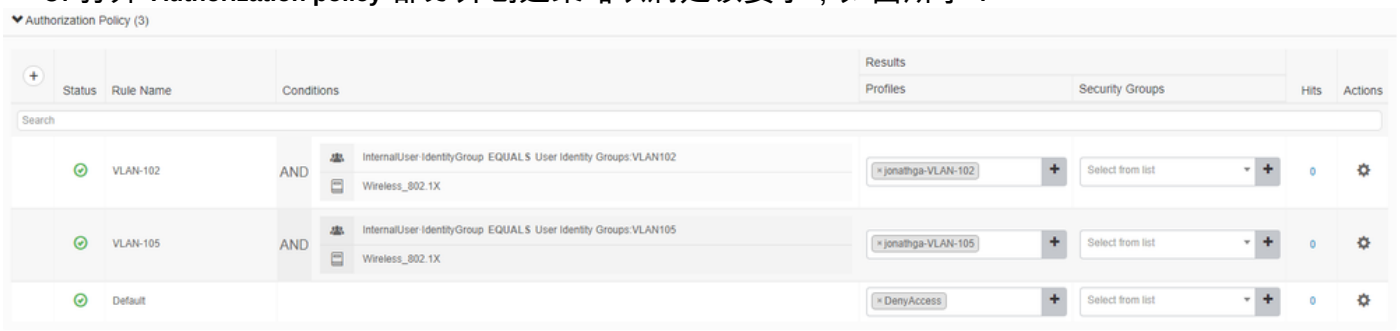
配置授权配置文件后，需要为无线用户创建身份验证策略。您可以使用 **Custom** 策略或修改 **Default** 策略集。在本例中，创建了自定义配置文件。

3. 导航至 **Policy > Policy Sets** 选择 **Add** 要创建新策略，如图所示：



现在，您需要为用户创建授权策略，以便根据组成员身份分配相应的授权配置文件。

5. 打开 **Authorization policy** 部分并创建策略以满足该要求，如图所示：



为多个 VLAN 配置交换机

要允许多个VLAN通过交换机，您需要发出以下命令来配置连接到控制器的交换机端口：

```
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation dot1q
```

> **注意**：默认情况下，大多数交换机都允许在该交换机上通过中继端口创建的所有 VLAN。如果有线网络连接到交换机，则可以将此相同配置应用于连接到有线网络的交换机端口。这样将在位于有线网络和无线网络中的相同 VLAN 之间实现通信。

Catalyst 9800 WLC配置

此配置要求执行下列步骤：

- 用身份验证服务器的详细信息配置 WLC.
- 配置VLAN。
- 配置WLAN(SSID)。
- 配置策略配置文件。

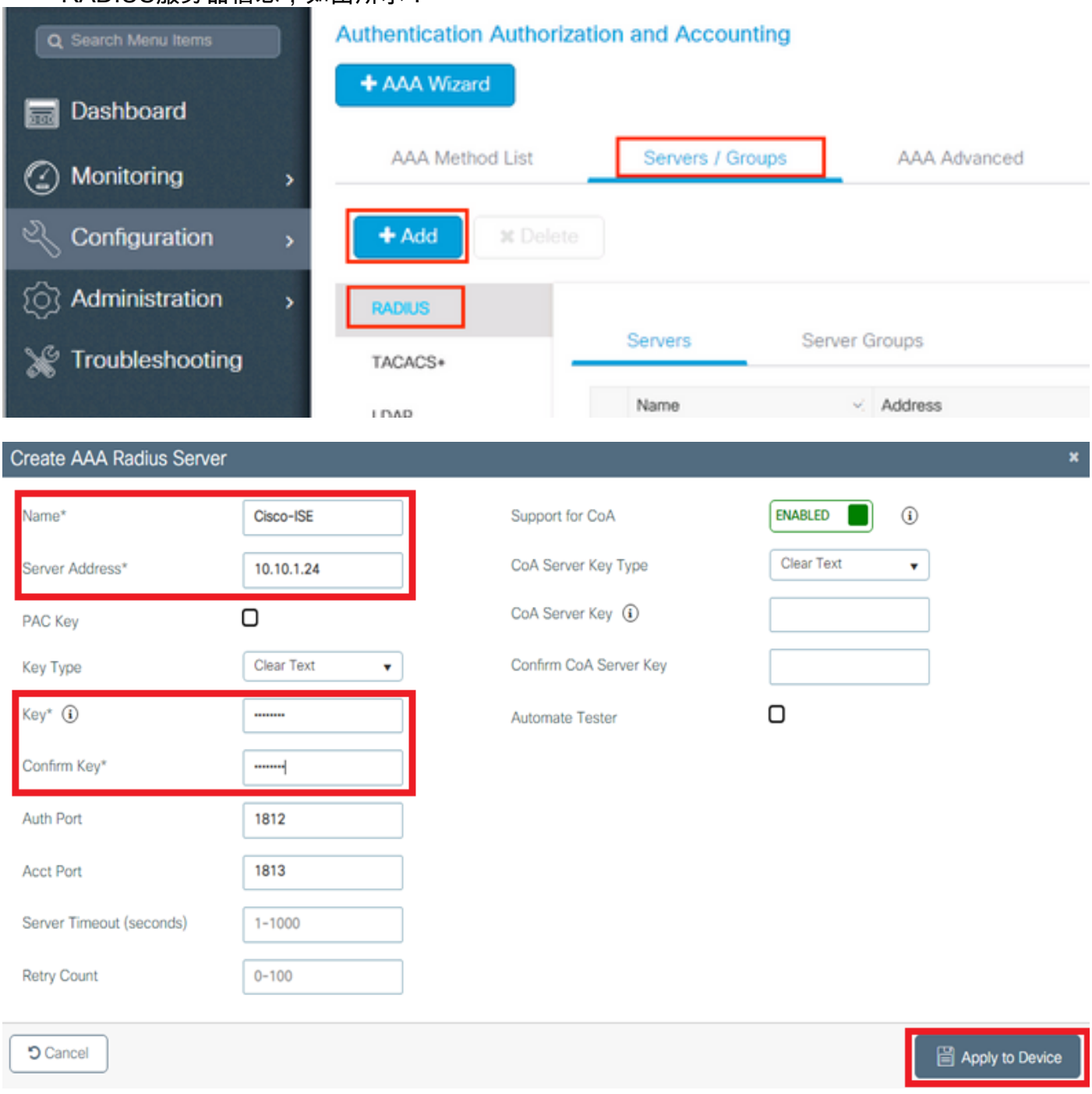
- 配置策略标记。
- 将策略标记分配给AP。

步骤1.使用身份验证服务器的详细信息配置WLC

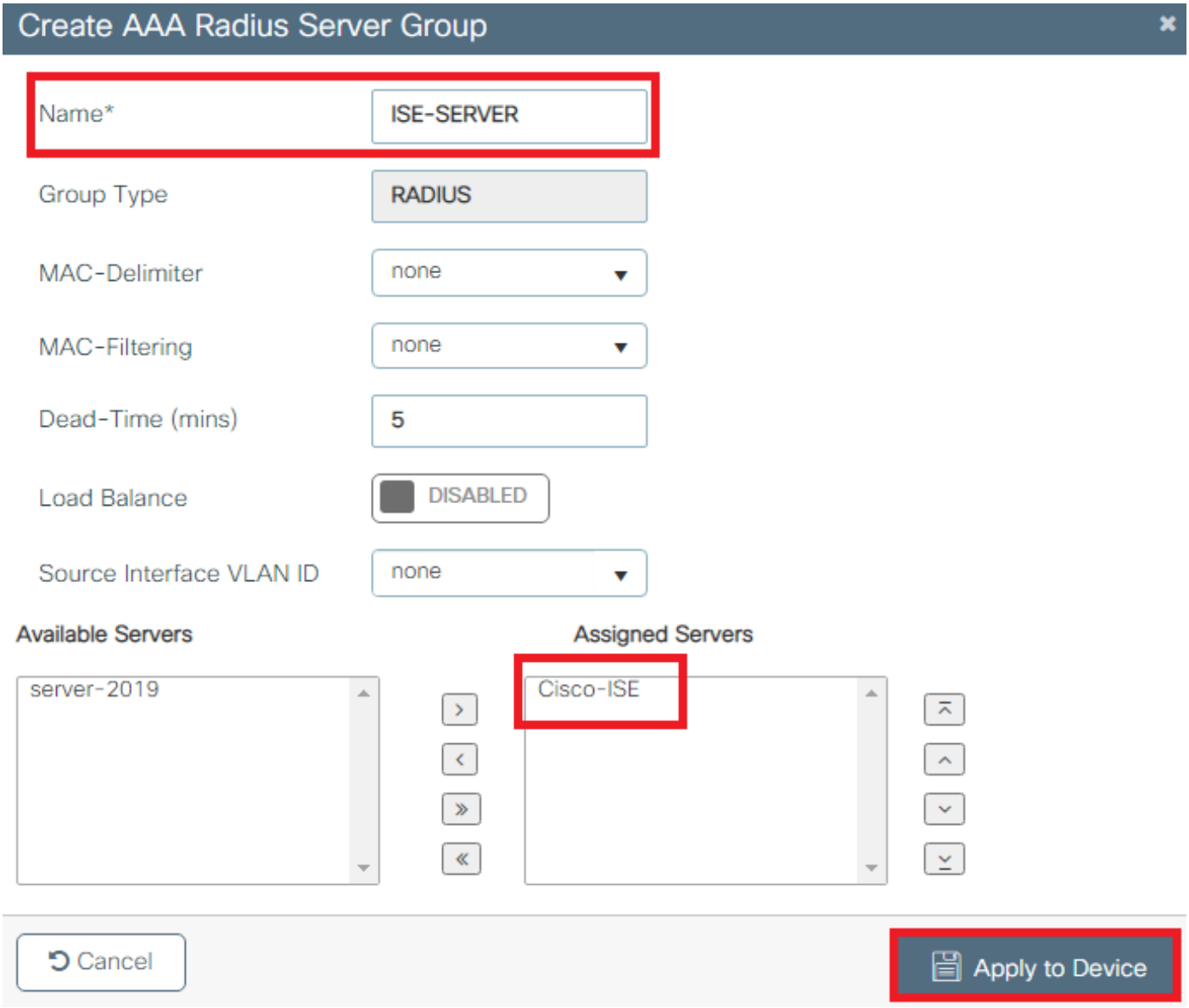
必须配置WLC，以便它能够与RADIUS服务器通信以验证客户端。

请完成以下步骤：

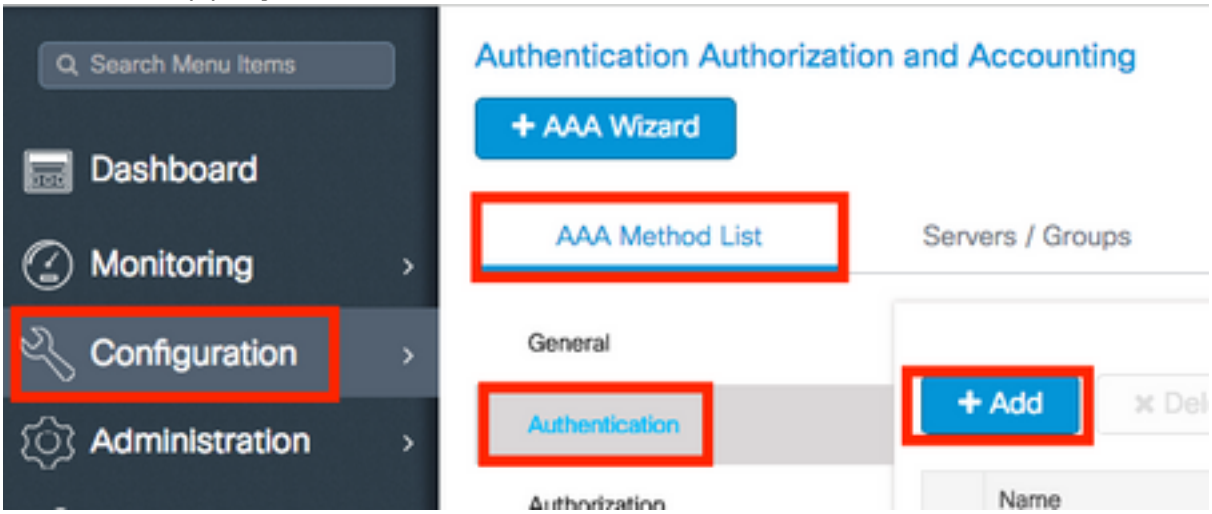
1. 从控制器GUI导航至 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** 并输入RADIUS服务器信息，如图所示：

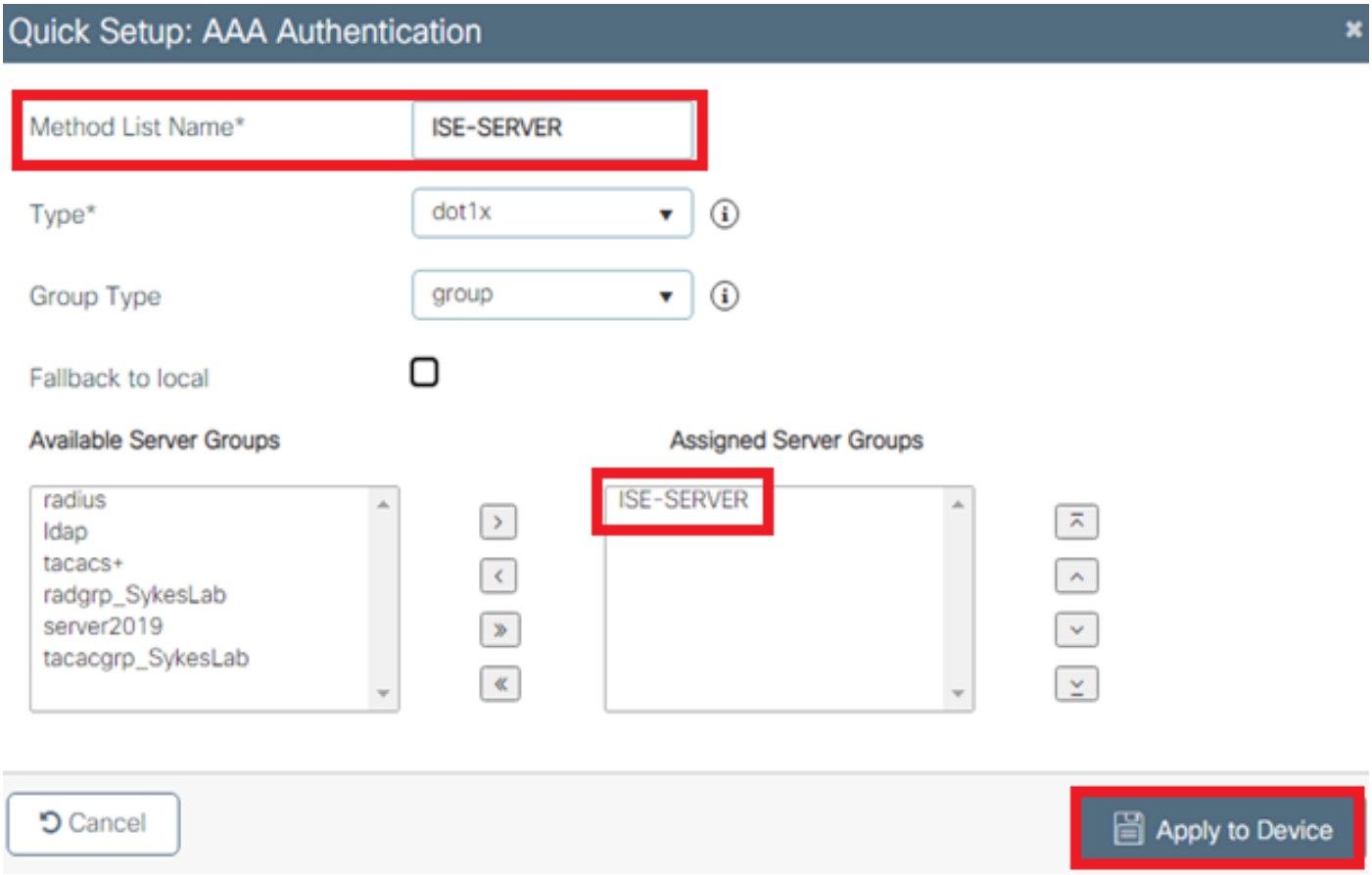


2. 要将RADIUS服务器添加到RADIUS组，请导航至 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** 如图所示:



3. 要创建身份验证方法列表，请导航至 **Configuration > Security > AAA > AAA Method List > Authentication > + Add** 如图所示：



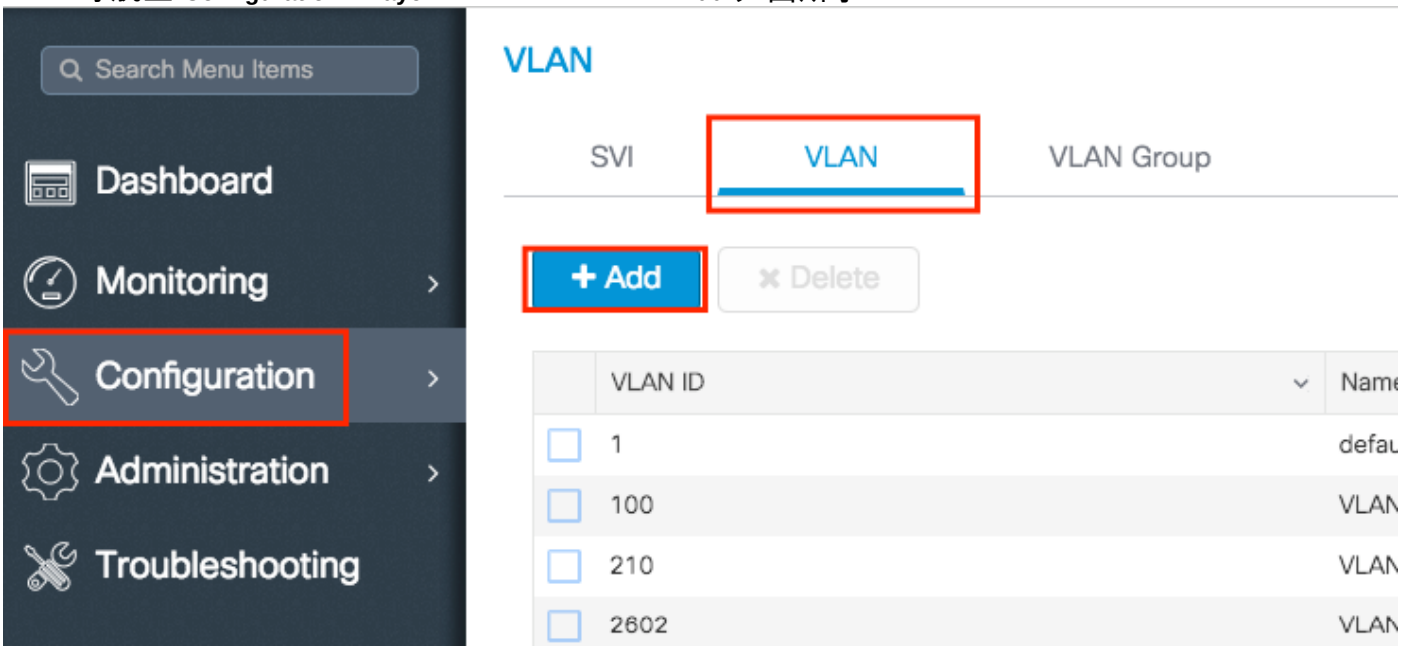


步骤2.配置VLAN

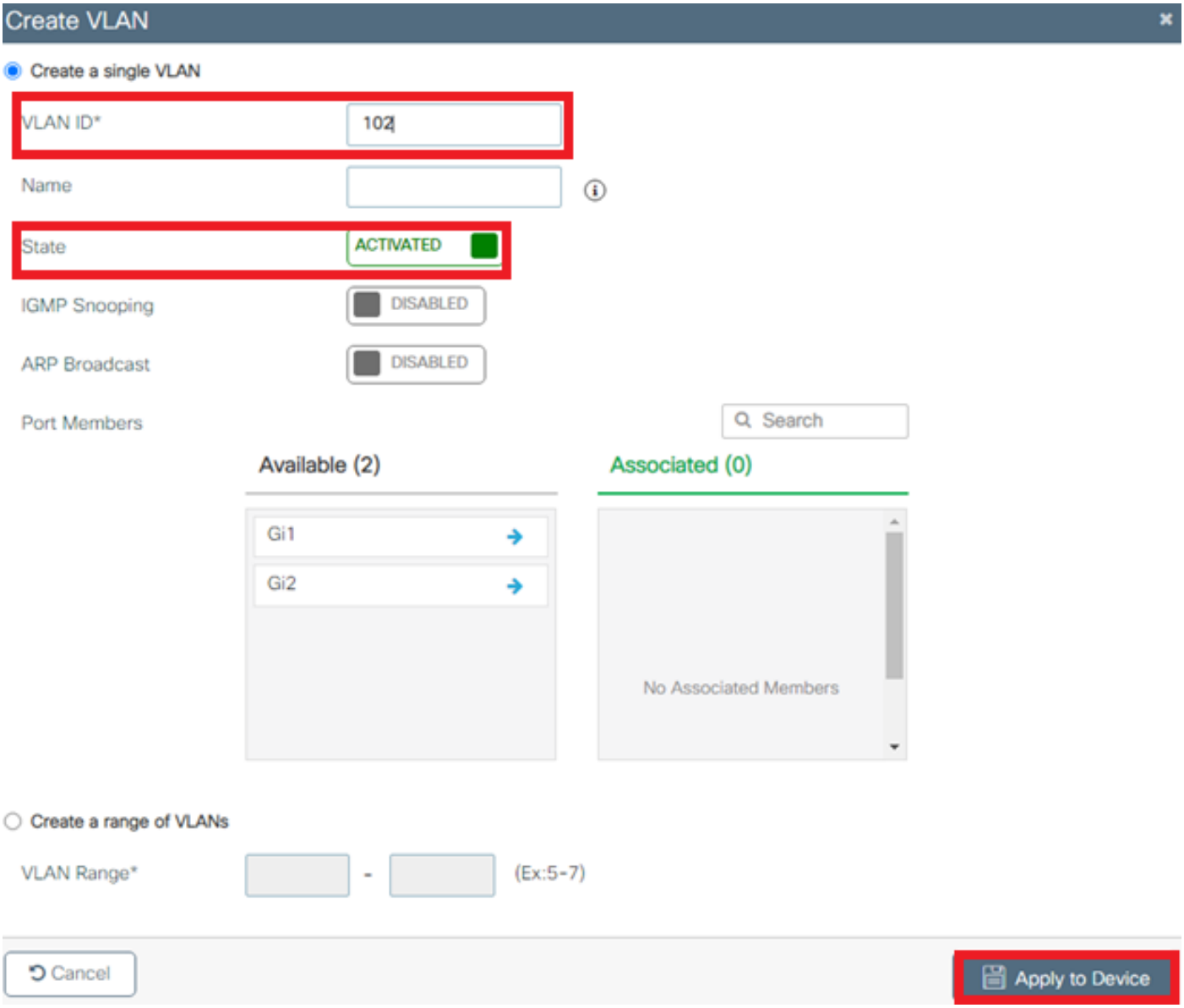
此步骤说明如何在Catalyst 9800 WLC上配置VLAN。如本文档中上文所述，WLC 中也必须具有在 RADIUS 服务器的 Tunnel-Private-Group ID 属性下指定的 VLAN ID。

在本例中，用户jonathga-102使用 **Tunnel-Private-Group ID of 102 (VLAN =102)** 在RADIUS服务器上。

1. 导航至 **Configuration > Layer2 > VLAN > VLAN > + Add** 如图所示:



2. 输入所需信息，如图所示：



注意：如果不指定名称，VLAN将自动获得VLANXXX的名称，其中XXXX是VLAN ID。

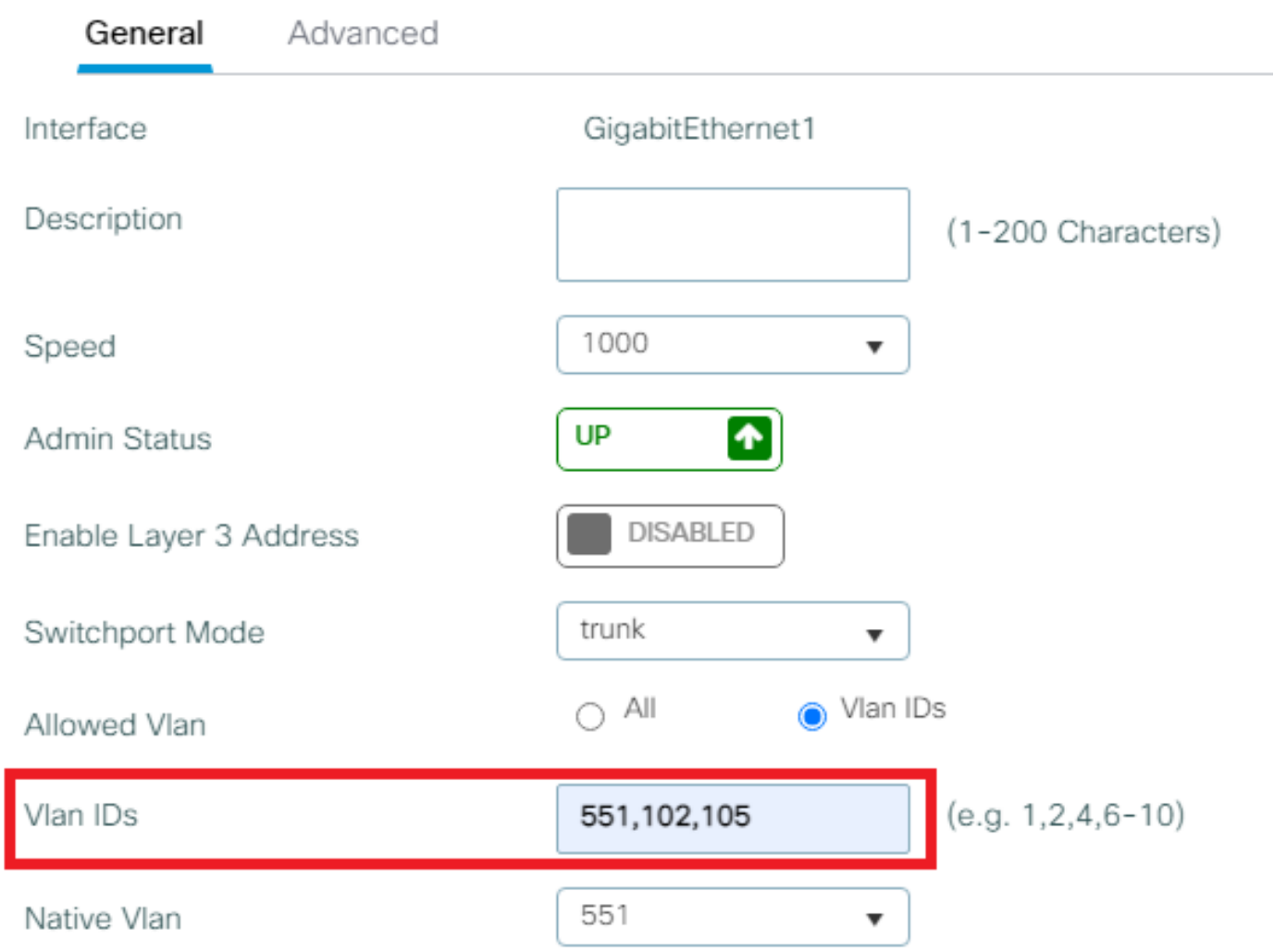
对所有需要的VLAN重复步骤1和2，完成后，您可以继续步骤3。

3. 验证数据接口中是否允许VLAN。 如果您正在使用端口通道，请导航至 **Configuration > Interface > Logical > PortChannel name > General**。如果您看到它配置为 **Allowed VLAN = All** 配置完成。如果您看到 **Allowed VLAN = VLANs IDs**，添加所需的VLAN，然后选择 **Update & Apply to Device**。如果没有使用端口通道，请导航至 **Configuration > Interface > Ethernet > Interface Name > General**。如果您看到它配置为 **Allowed VLAN = All** 配置完成。如果您看到 **Allowed VLAN = VLANs IDs**，添加所需的VLAN，然后选择 **Update & Apply to Device**。

如果使用All或特定VLAN ID，此图像显示与接口设置相关的配置。

General Advanced

Interface	GigabitEthernet3
Description	(1-200 Characters)
Admin Status	UP
Port Fast	disable
Enable Layer 3 Address	DISABLED
Switchport Mode	trunk
Allowed Vlan	All / Vlan IDs
Native Vlan	

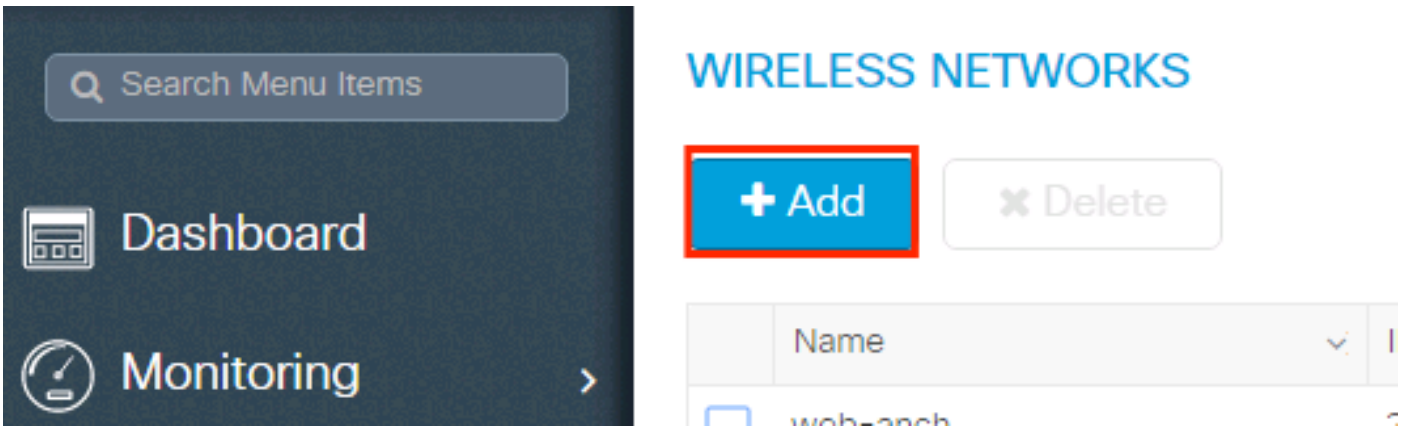


步骤3.配置WLAN(SSID)

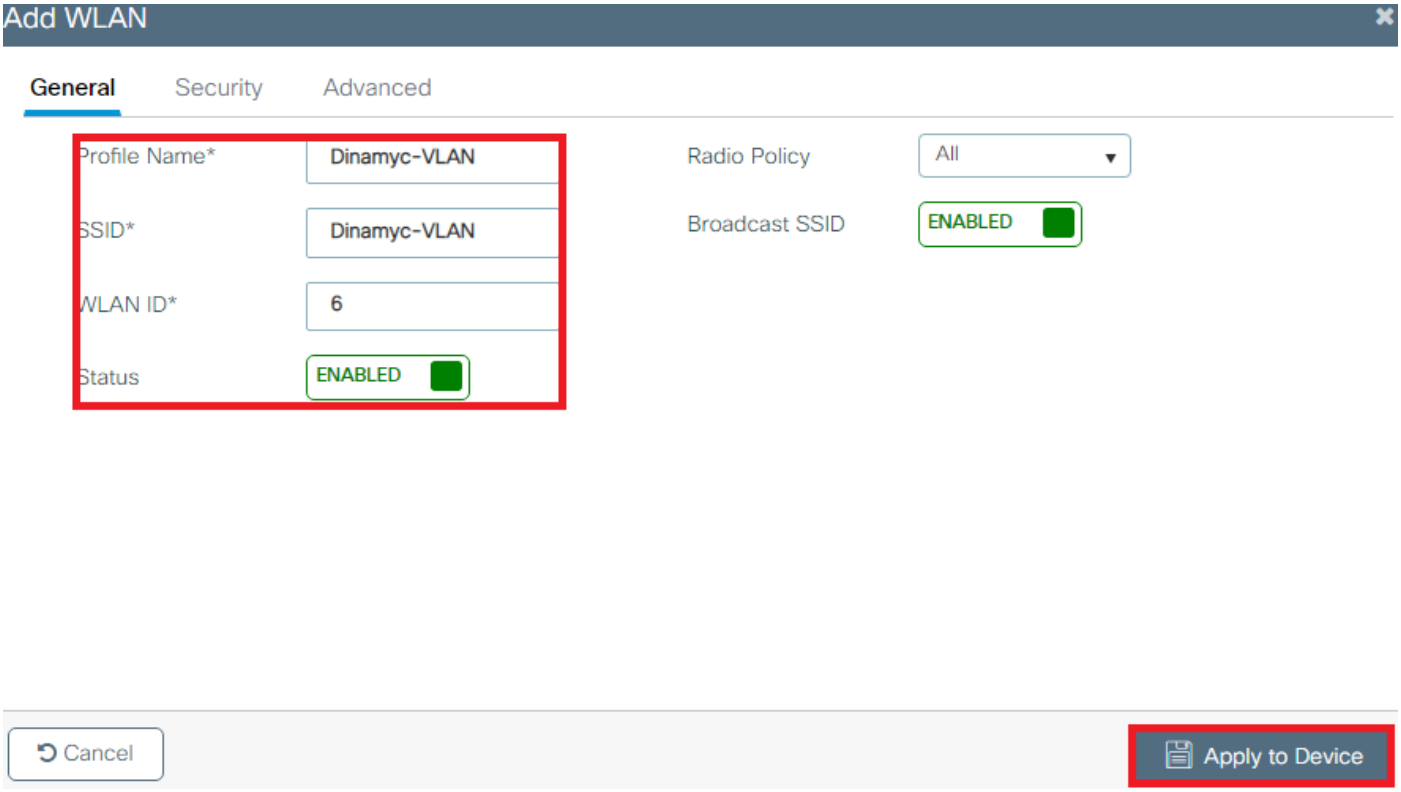
此过程说明如何在 WLC 中配置 WLAN。

请完成以下步骤：

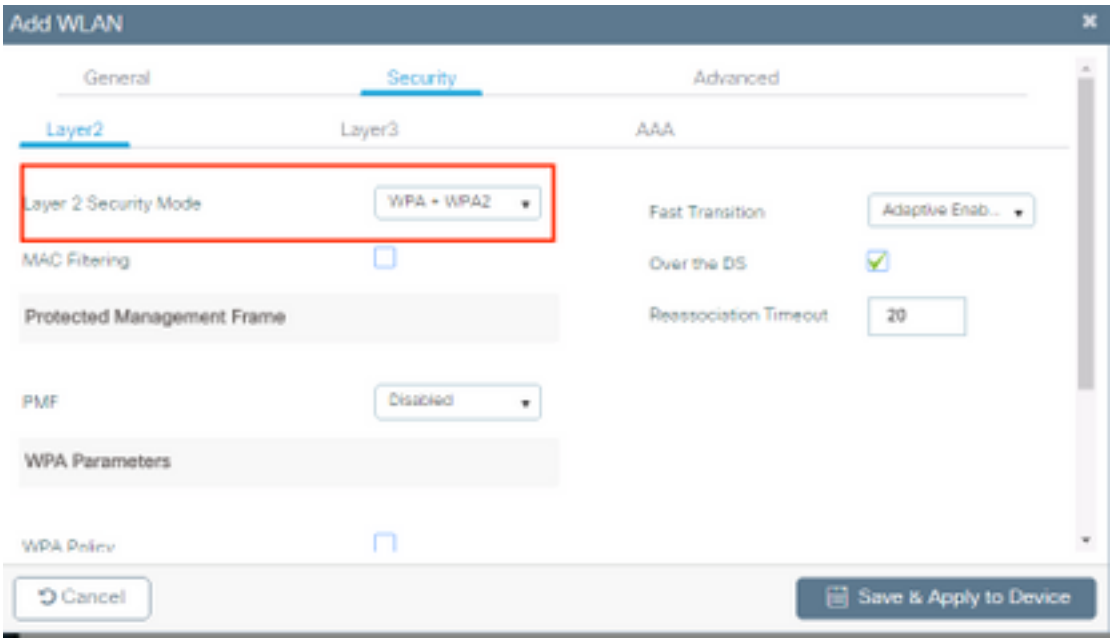
1. 以创建WLAN。导航至 **Configuration > Wireless > WLANs > + Add** 并根据需要配置网络，如图所示：

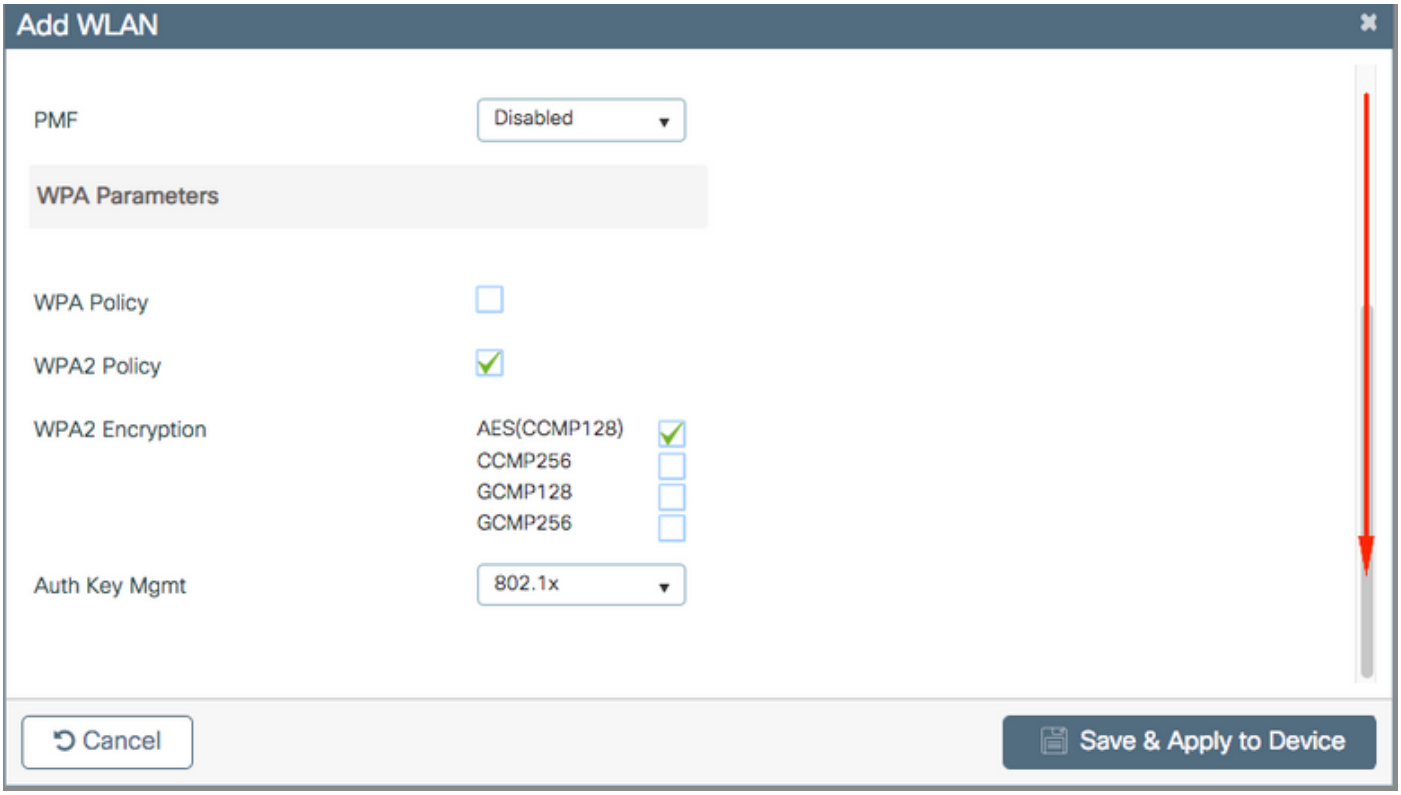


2. 输入WLAN信息，如图所示：

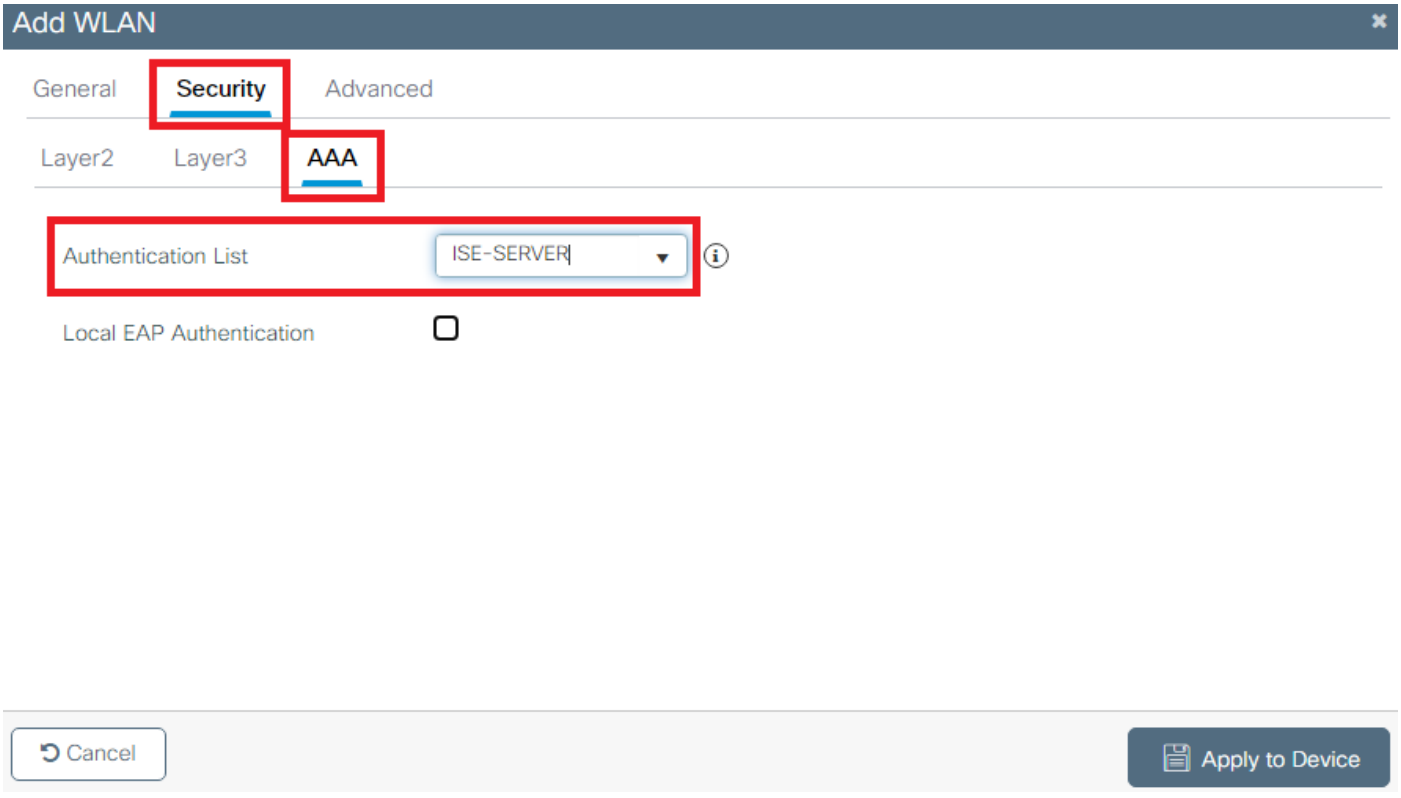


3. 导航至 **Security** 选项卡，然后选择所需的安全方法。在本例中，WPA2 + 802.1x如图所示：





发件人**Security > AAA** 选项卡，从 **Configure the WLC with the Details of the Authentication Server** 部分，如图所示：



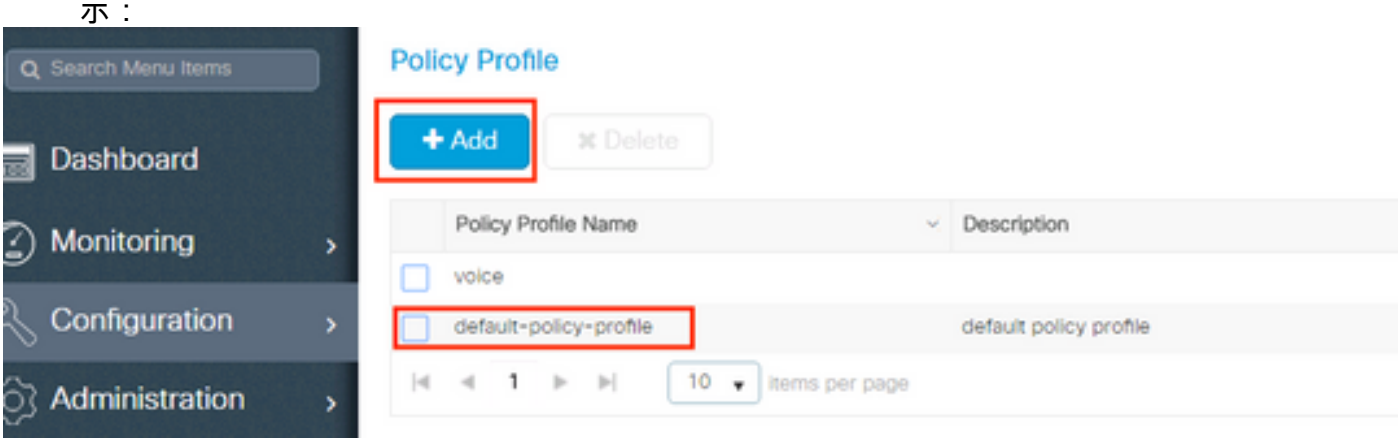
步骤4.配置策略配置文件

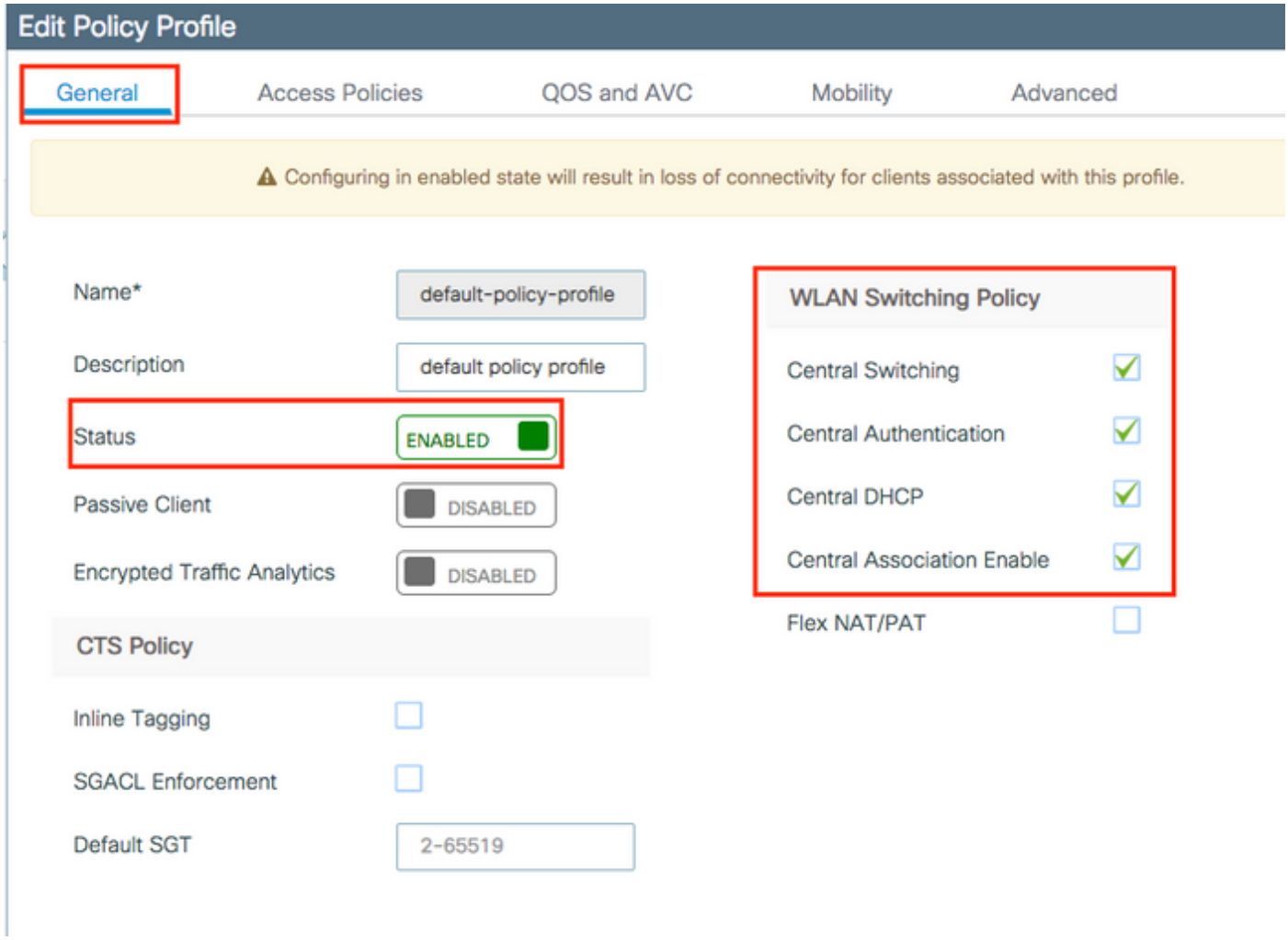
此过程说明如何在WLC中配置策略配置文件。

请完成以下步骤：

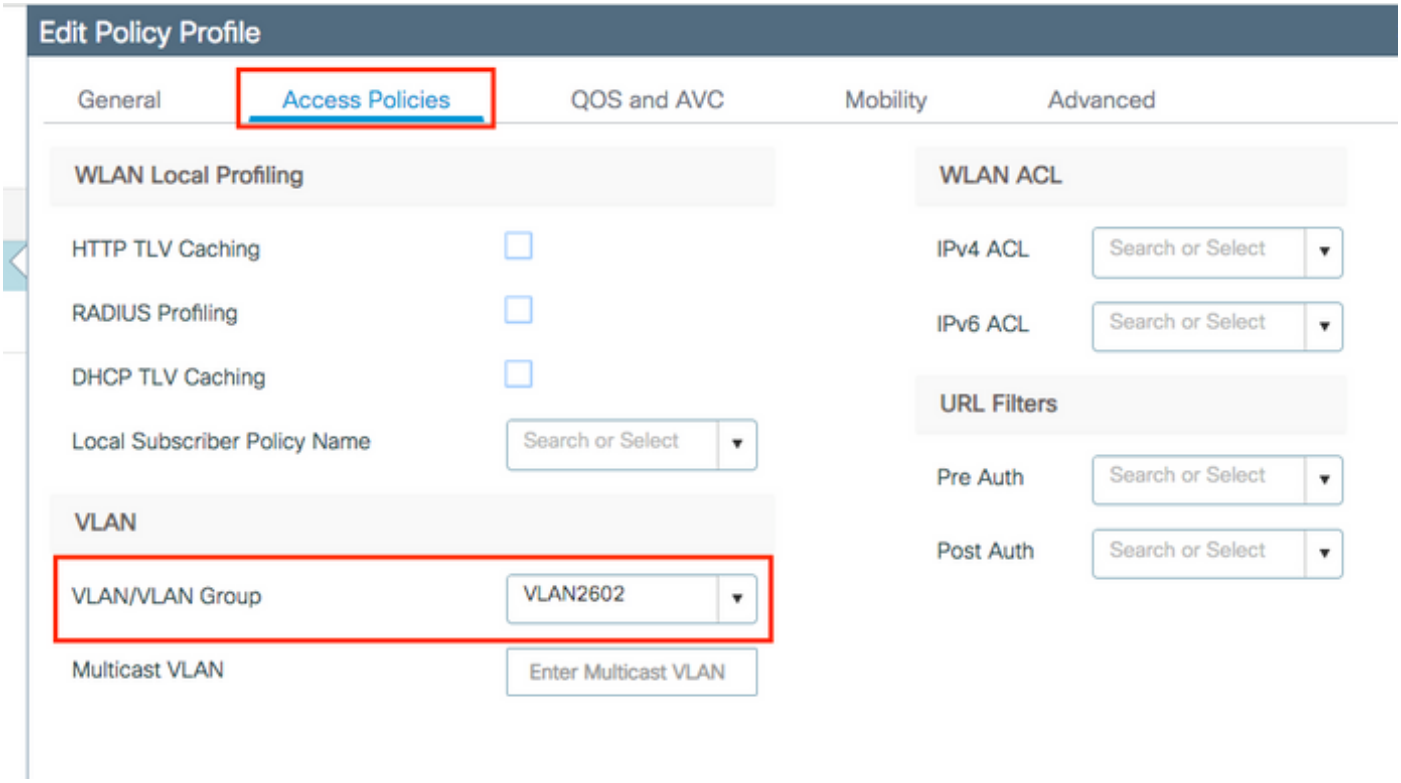
1. 导航至 **Configuration > Tags & Profiles > Policy Profile** 配置 **default-policy-profile** 或创建新映像，如图所

示：



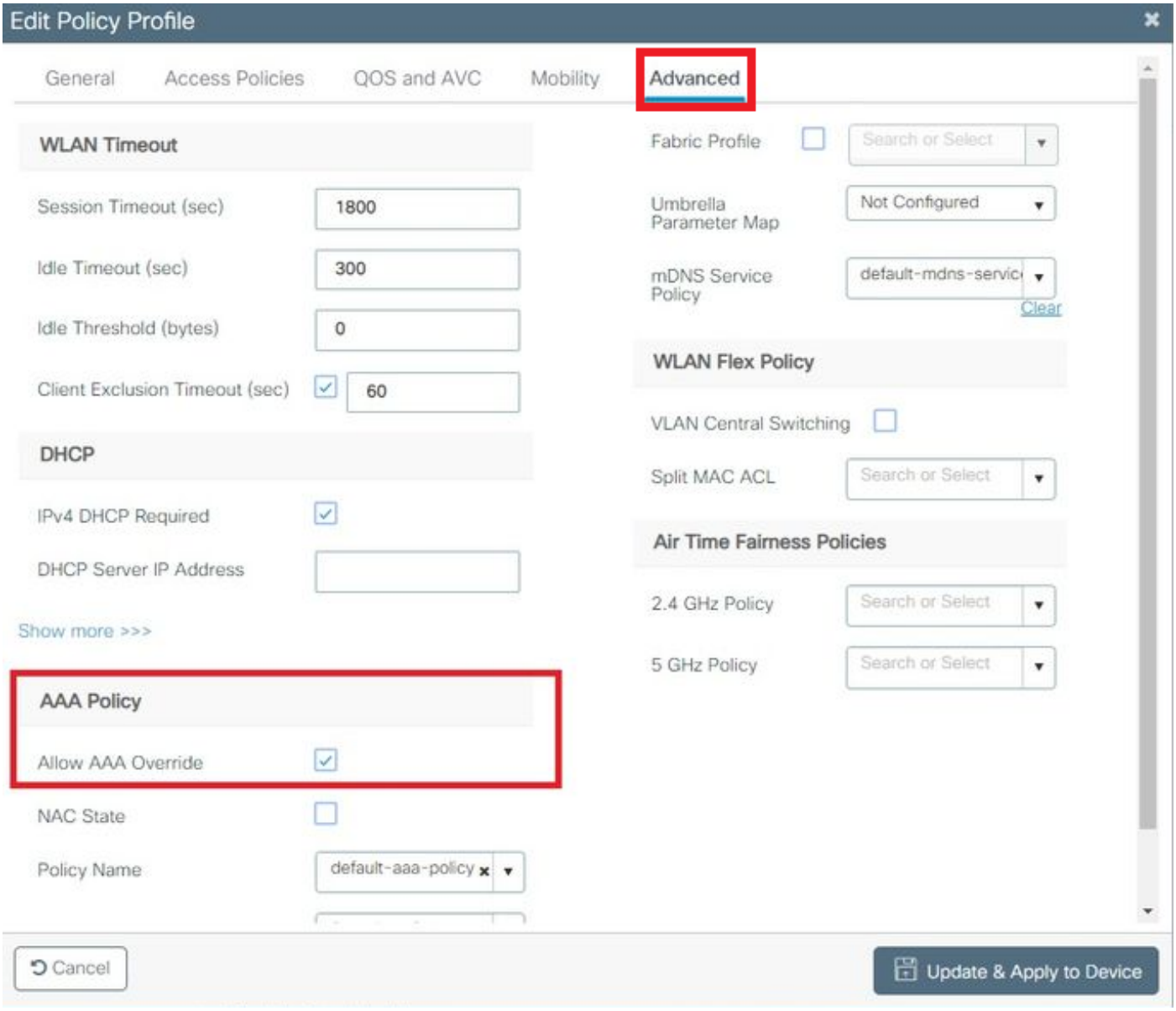


2. 从 **Access Policies** 选项卡分配无线客户端在默认情况下连接到此WLAN时分配到的VLAN，如图所示：



注意：在提供的示例中，RADIUS服务器的工作是在身份验证成功后将无线客户端分配给特定VLAN，因此策略配置文件上配置的VLAN可以是黑洞VLAN，RADIUS服务器会覆盖此映射，并将通过该WLAN的用户分配给RADIUS服务器中用户Tunnel-Group-Private-ID字段下指定的VLAN。

3. 从 **Advance** 选项卡 **Allow AAA Override** 复选框以覆盖WLC配置，当RADIUS服务器返回将客户端置于正确VLAN所需的属性时，如图所示：

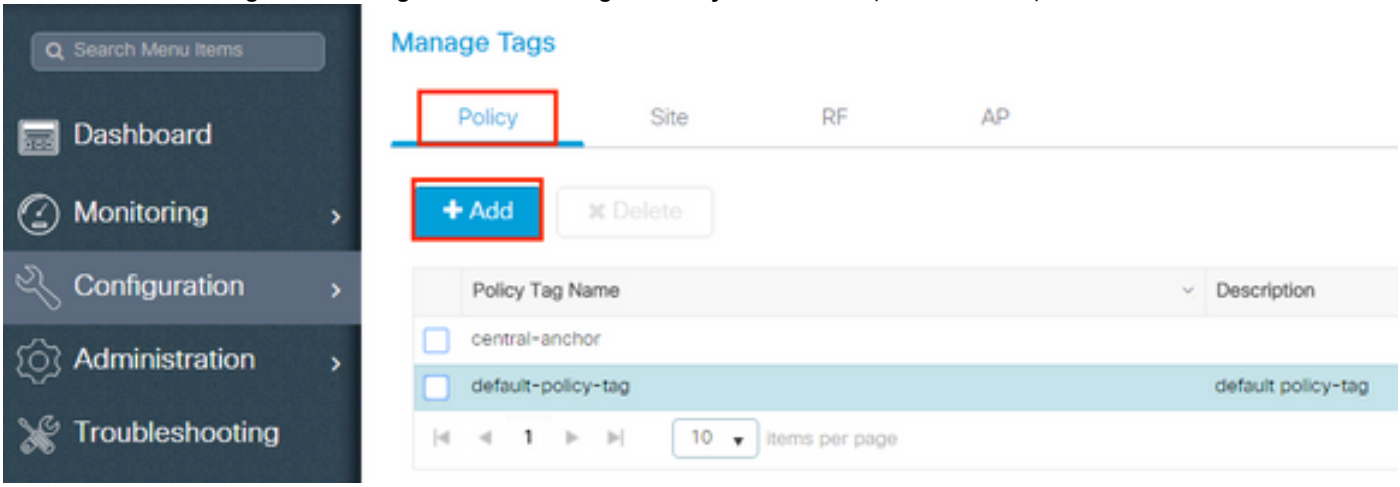


步骤5.配置策略标记

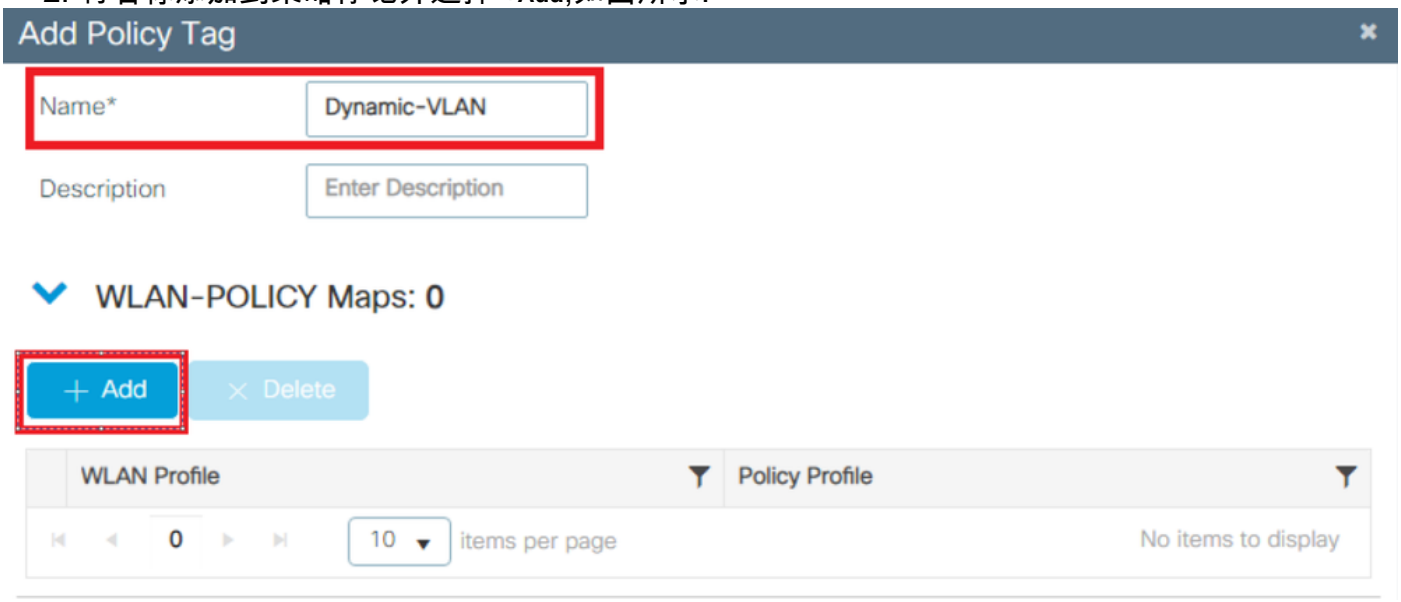
此过程说明如何在WLC中配置策略标记。

请完成以下步骤：

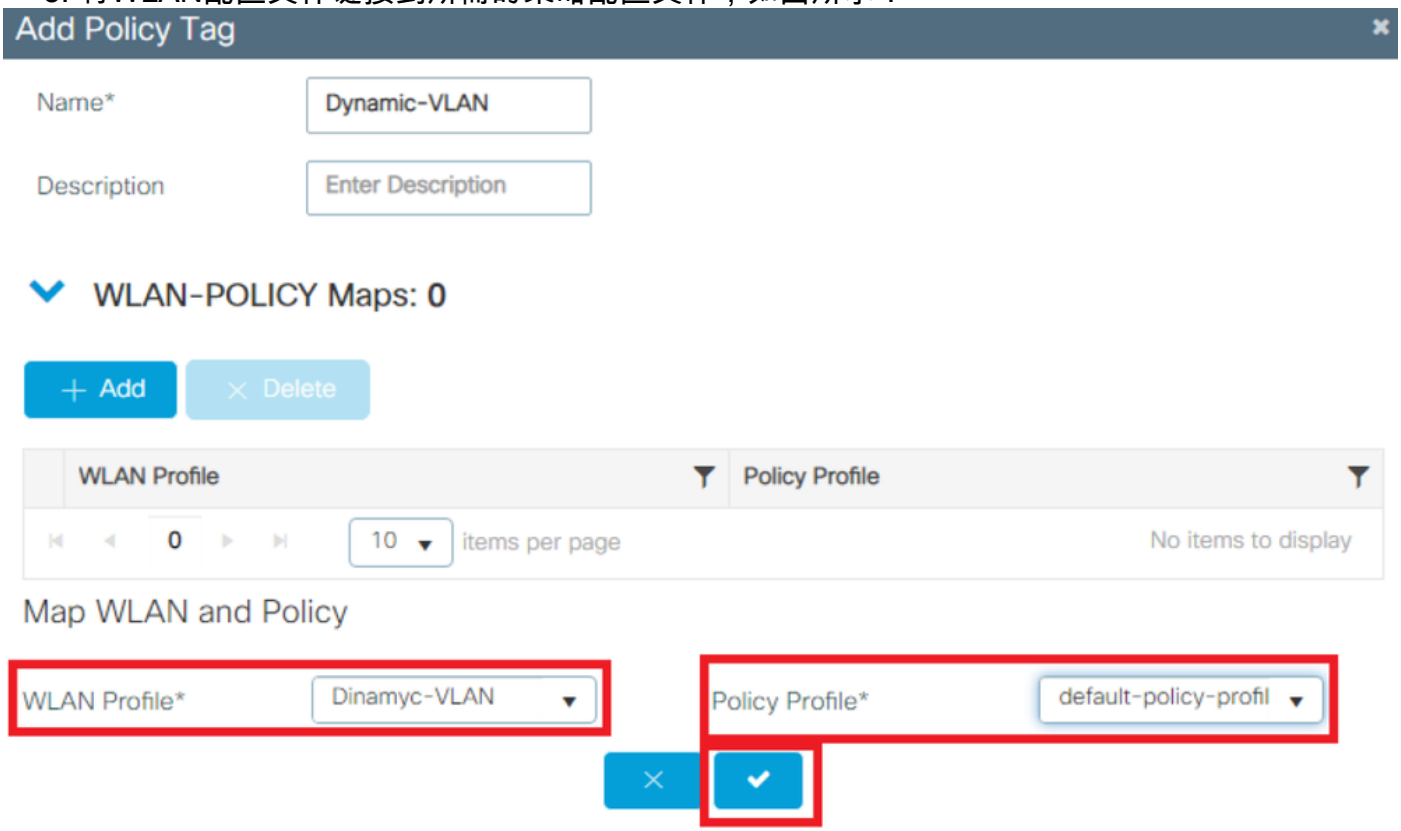
1. 导航至 **Configuration > Tags & Profiles > Tags > Policy** 如图所示，如果需要，添加一个新的：

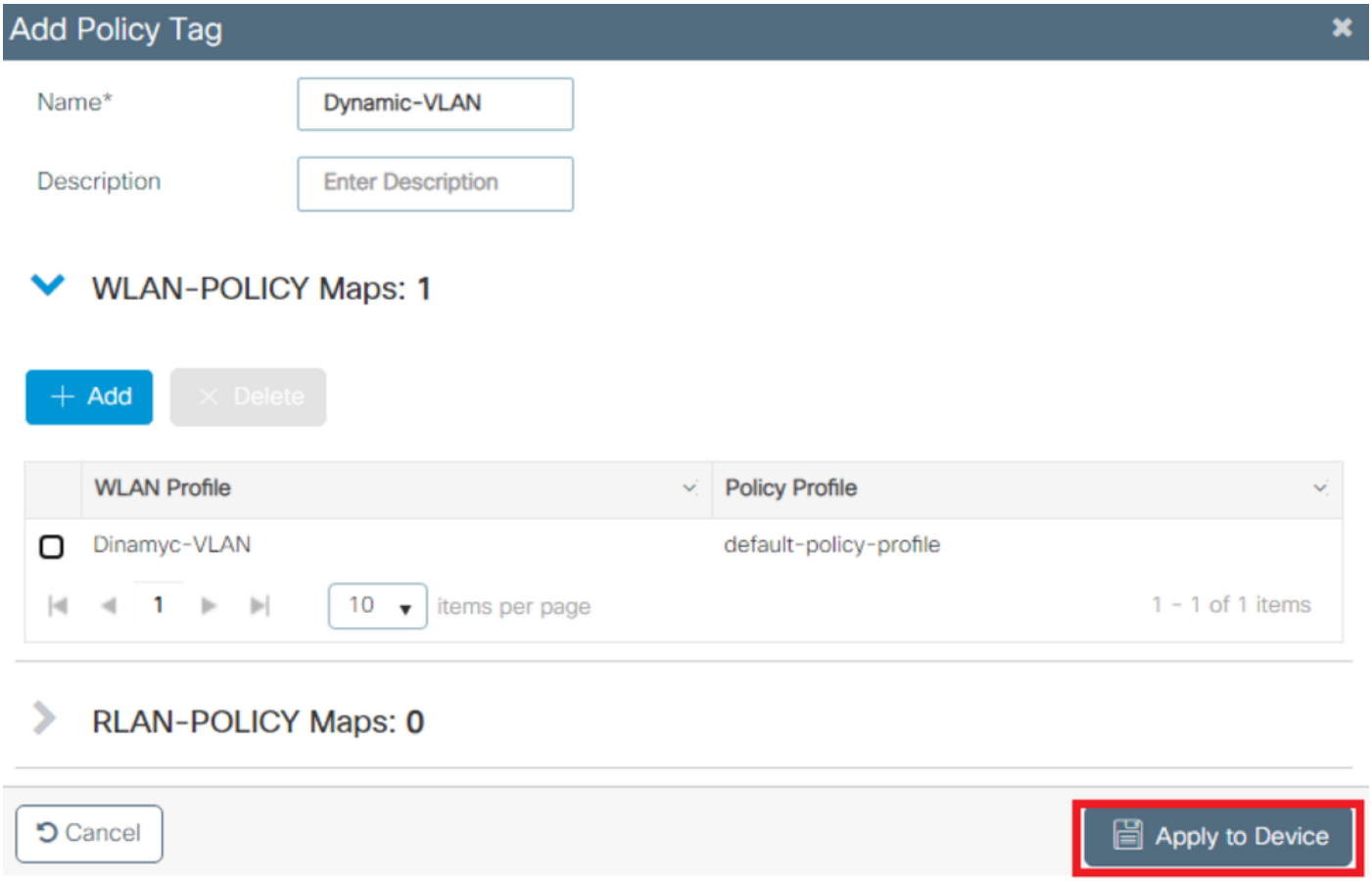


2. 将名称添加到策略标记并选择 **+Add**,如图所示:



3. 将WLAN配置文件链接到所需的策略配置文件，如图所示：



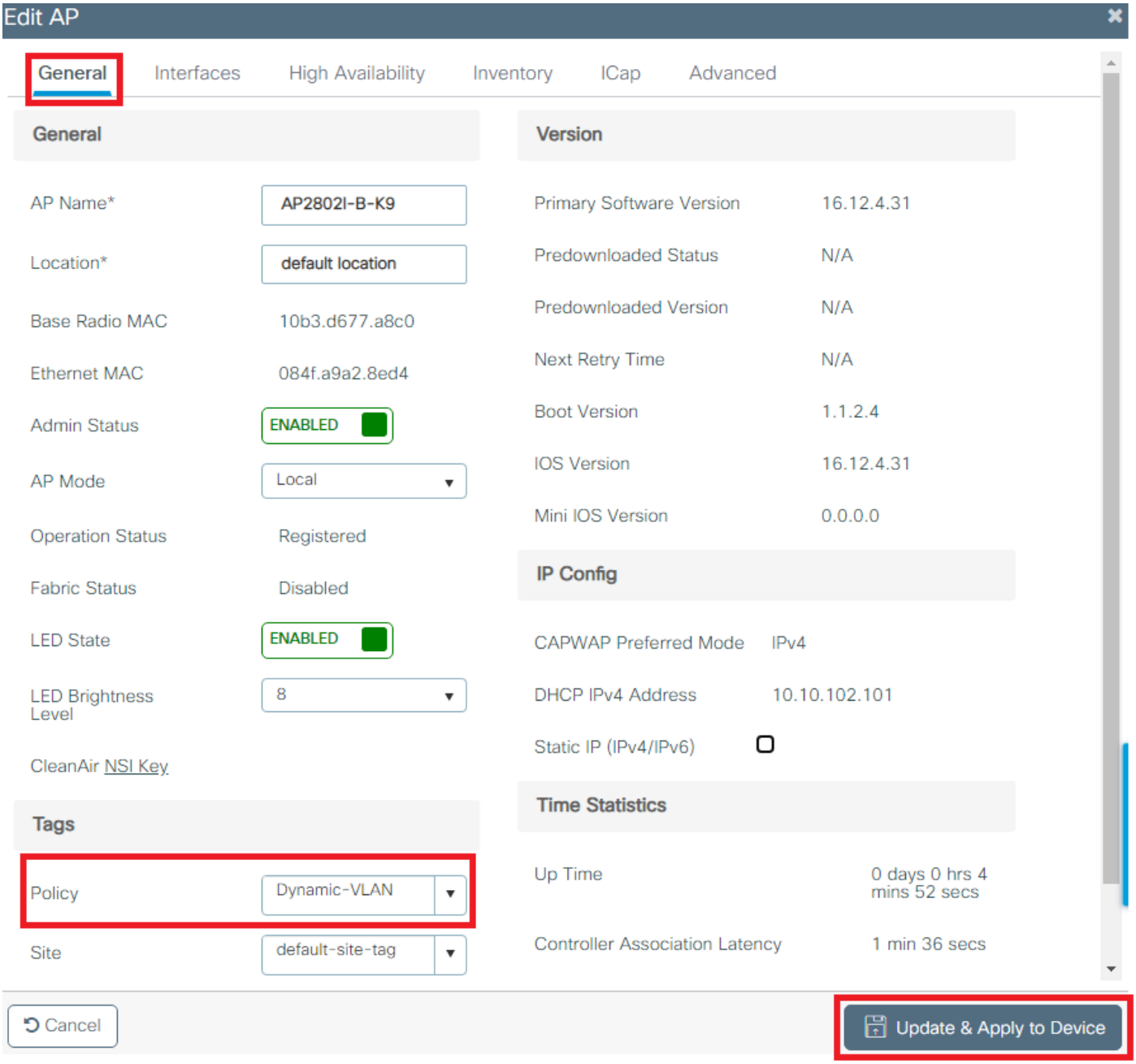


步骤6.将策略标记分配给AP

此过程说明如何在WLC中配置策略标记。

请完成以下步骤：

1. 导航至 **Configuration > Wireless > Access Points > AP Name > General Tags** 分配相关策略标记，然后选择 **Update & Apply to Device** 如图所示:



警告：请注意，当AP上的策略标记更改时，它会丢弃与WLC的关联并重新加入。

验证

使用本部分可确认配置能否正常运行。

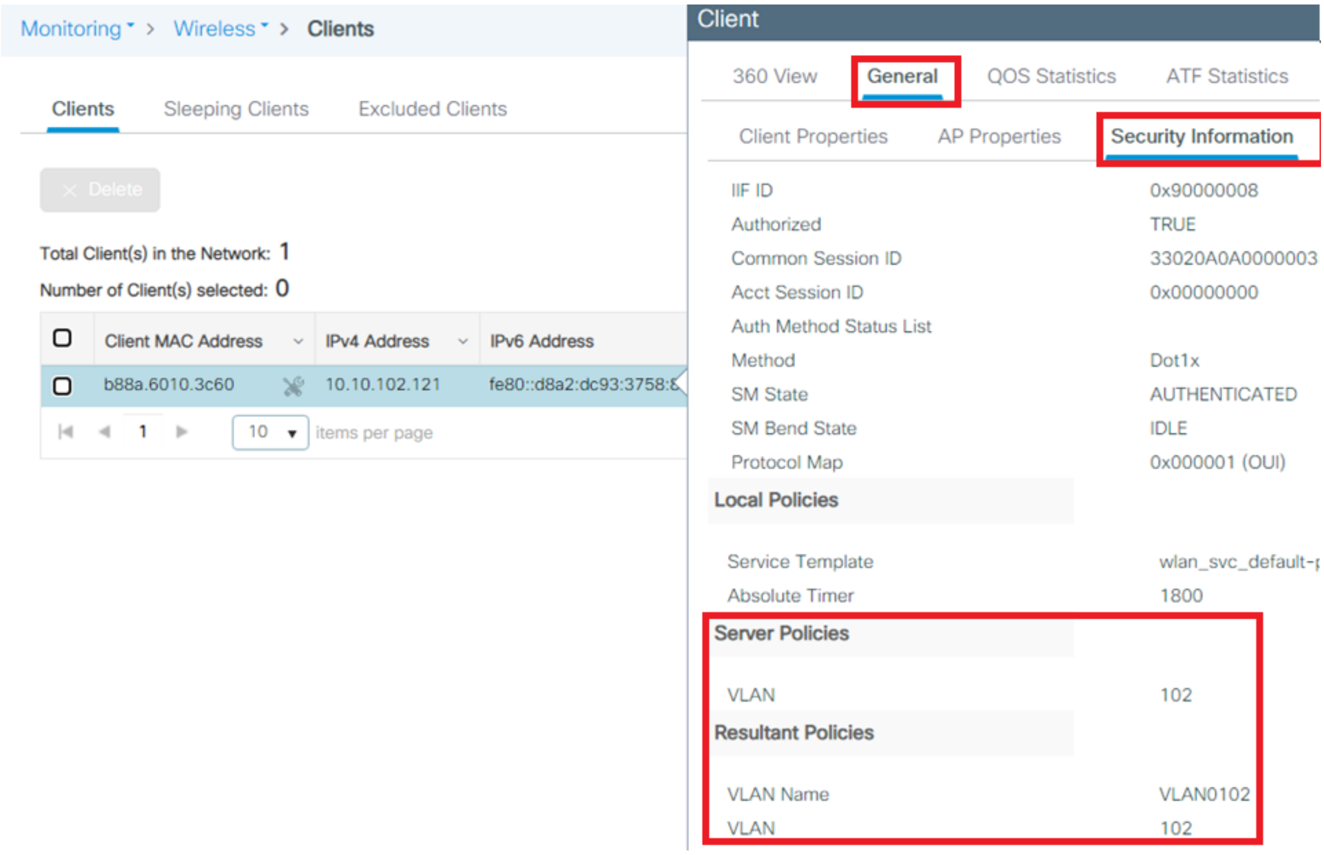
测试与Windows 10和本地请求方的连接，当系统提示您输入用户名和密码后，输入ISE上映射到VLAN的用户信息。

在上一个示例中，请注意jonathga-102已分配给RADIUS服务器中指定的VLAN102。本示例使用此用户名接收身份验证，并由RADIUS服务器分配给VLAN:

完成身份验证后，您需要根据发送的RADIUS属性验证是否将客户端分配到正确的VLAN。完成以下步骤以完成此任务：

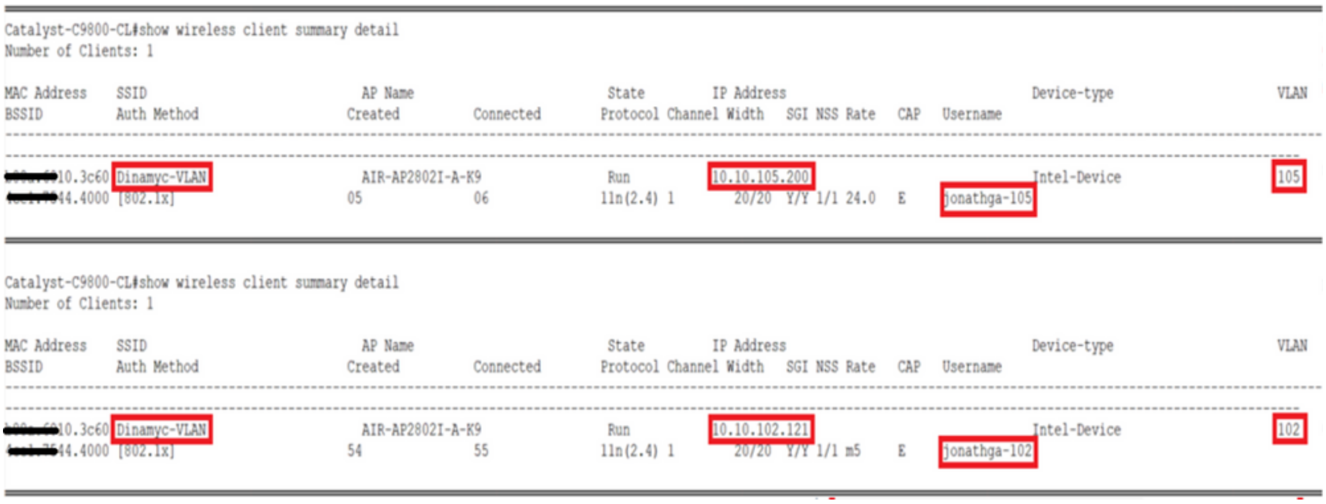
1. 从控制器GUI导航至 **Monitoring > Wireless > Clients > Select the client MAC address > General > Security**

Information 并查找VLAN字段，如图所示：



在此窗口中，您可以观察到此客户端根据RADIUS服务器上配置的RADIUS属性分配给VLAN102。在CLI中，您可以使用 **show wireless client summary detail** 要查看与图中所示相同的信息

：


```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1

MAC Address    SSID           AP Name          Connected    State    IP Address                         Device-type    VLAN
BSSID          Auth Method    Created                       Protocol Channel Width  SGI NSS Rate  CAP  Username
------------------------------------------------------------------------------------------------------------------------
[redacted]10.3c60 Dinamyc-VLAN  AIR-AP2802I-A-K9              Run      10.10.105.200                      Intel-Device   105
[redacted]44.4000 [802.1x]      05               06           11n(2.4) 1  20/20   Y/Y 1/1 24.0  E    jonathga-105

Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1

MAC Address    SSID           AP Name          Connected    State    IP Address                         Device-type    VLAN
BSSID          Auth Method    Created                       Protocol Channel Width  SGI NSS Rate  CAP  Username
------------------------------------------------------------------------------------------------------------------------
[redacted]10.3c60 Dinamyc-VLAN  AIR-AP2802I-A-K9              Run      10.10.102.121                      Intel-Device   102
[redacted]44.4000 [802.1x]      54               55           11n(2.4) 1  20/20   Y/Y 1/1 m5    E    jonathga-102
```

2. 可以启用 **Radioactive traces** 确保RADIUS属性成功传输到WLC。为此，请执行以下步骤： 从控制器GUI导航至 **Troubleshooting > Radioactive Trace > +Add**。输入无线客户端的Mac地址。选择 **Start**。将客户端与WLAN连接。导航至 **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log**。

跟踪输出的这一部分确保RADIUS属性成功传输：

```
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id
1812/60 10.10.1.24:0, Access-Accept, len 352
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  authenticator e5 5e
58 fa da 0a c7 55 - 53 55 7d 43 97 5a 8b 17
```

```
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  User-Name
[1]     13  "jonathga-102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  State
[24]    40  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Class
[25]    54  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Type
       [64]     6  VLAN                    [13]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Medium-Type
[65]     6  ALL_802                [6]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  EAP-Message
[79]     6  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Message-
Authenticator[80]    18  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Private-
Group-Id[81]     6  "102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  EAP-Key-Name
 [102]   67  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Send-Key
[16]    52  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Recv-Key
[17]    52  *
2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method
name: PEAP on handle 0x0C000008

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:            username   0 "jonathga-102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:               class   0 43 41 43 53 3a 33 33 30 32 30 41 30 41 30 30 30 30 30 30 33 35 35 36
45 32 32 31 36 42 3a 49 53 45 2d 32 2f 33 39 33 33 36 36 38 37 32 2f 31 31 32 36 34 30  ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:         tunnel-type   1 13 [vlan] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute :
tunnel-medium-type   1 6 [ALL_802] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:tunnel-private-group-id   1 "102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:             timeout   0 1800 (0x708) ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [25253]: (info):
[0000.0000.0000:unknown] AAA override is enabled under policy profile
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 最终用户指南