在 Catalyst 9800 无线控制器系列上配置 802.1X 身份验证

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- WLC 配置
  - 9800 WLC 上的 AAA 配置
  - 关于AAA Dead-Server检测的注释
  - WLAN 配置文件配置
  - 策略配置文件配置
  - 策略标签配置
  - 策略标签分配
- ISE 配置
  - 在 ISE 上声明 WLC
  - 在ISE上创建新用户
  - 创建授权配置文件
  - 创建策略集
  - 创建身份验证策略
  - 创建授权策略

验证

故障排除

- 在 WLC 上进行故障排除
  - 条件调试和无线电主动跟踪
- 在 ISE 上进行故障排除

简介

本文档介绍如何在 Cisco Catalyst 9800 系列无线控制器上设置具备 802.1X 安全性的 WLAN。

先决条件

要求

Cisco 建议您了解以下主题：

- 802.1X

使用的组件

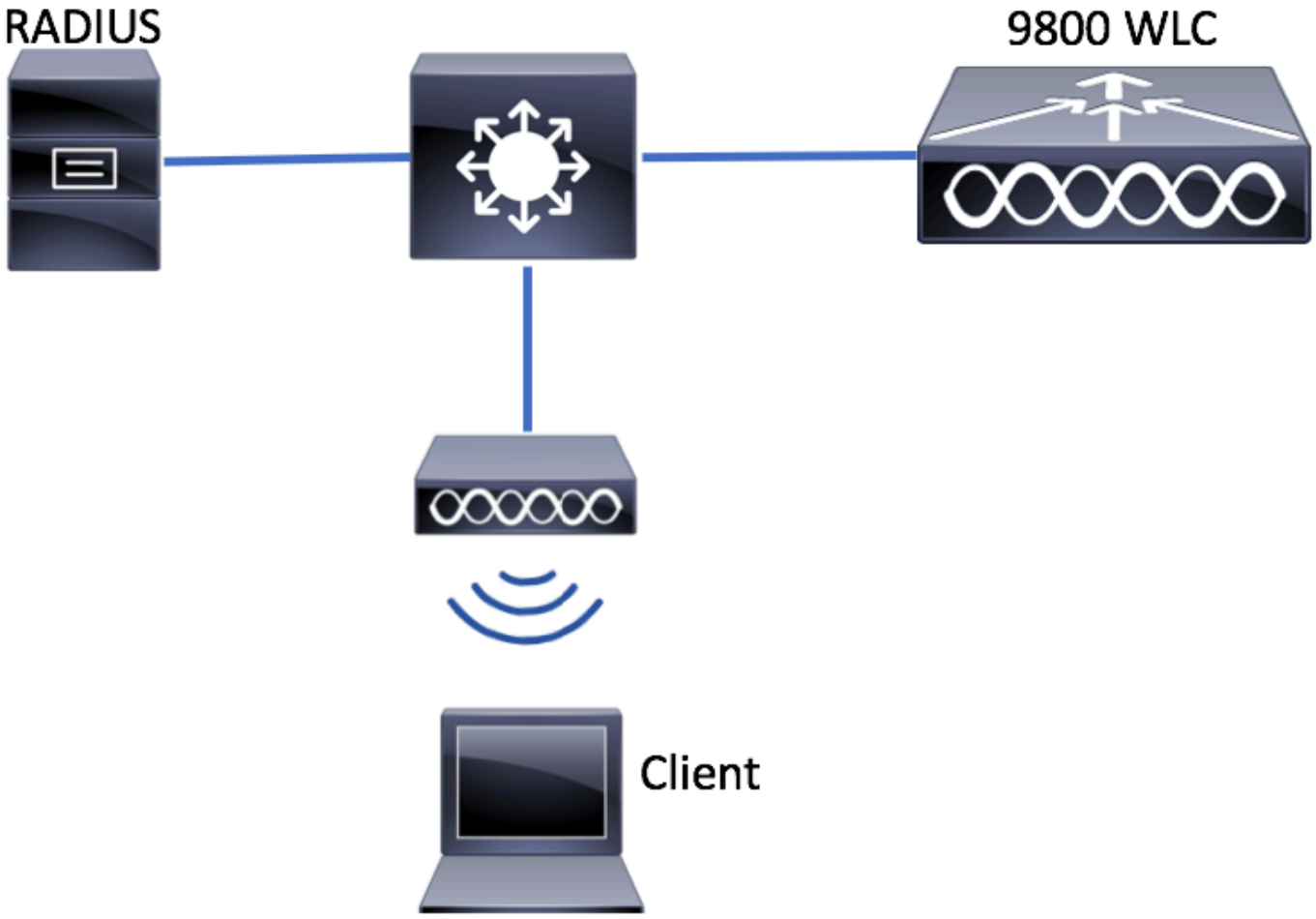
本文档中的信息基于以下软件和硬件版本：

- Catalyst 9800 无线控制器系列 (Catalyst 9800-CL)
- 思科IOS® XE 17.12.5
- Cisco ISE 3.0

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

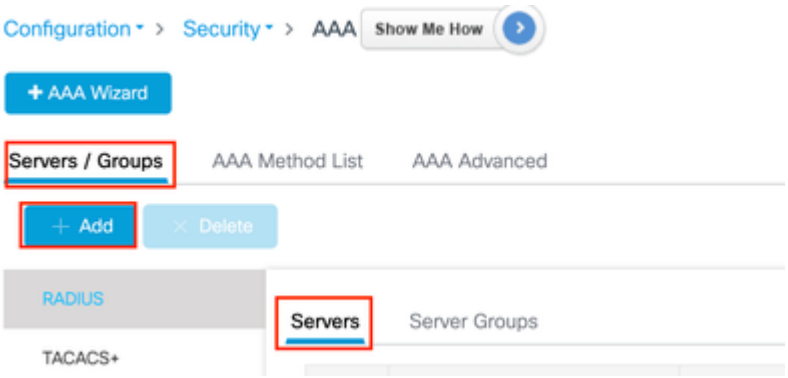


WLC 配置

9800 WLC 上的 AAA 配置

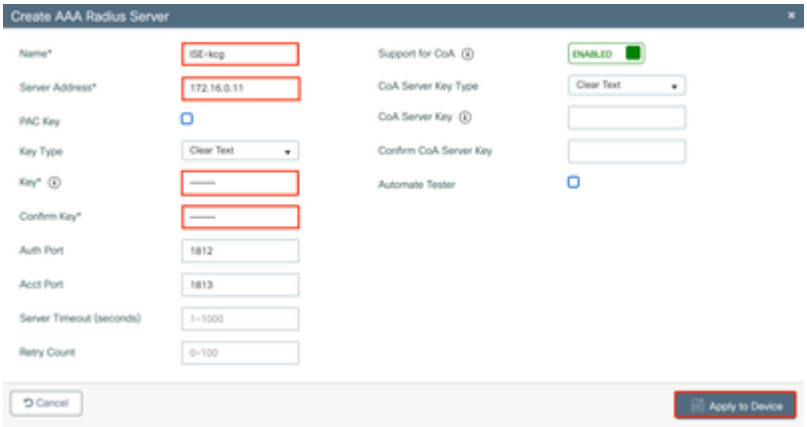
GUI:

第 1 步： 声明 RADIUS 服务器。依次导航至 ，然后输入 RADIUS 服务器信息。 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add**

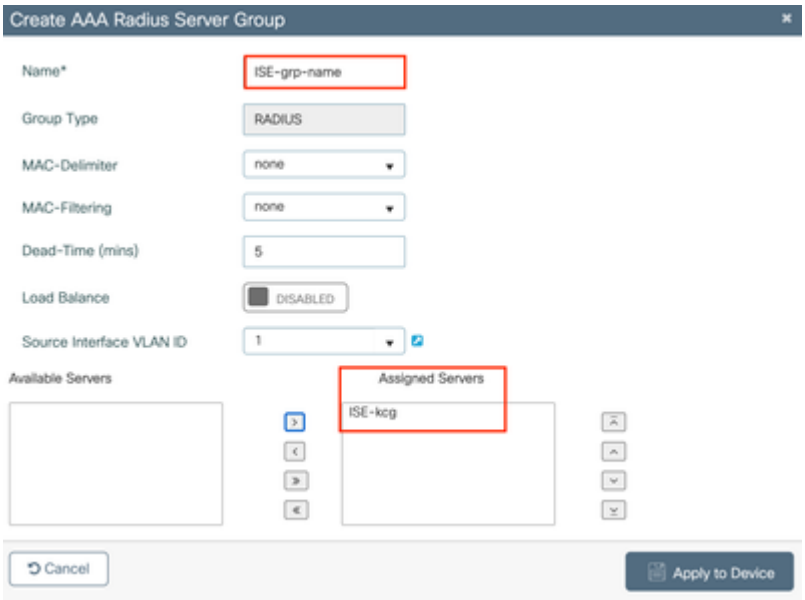


确保启用了CoA支持，并配置CoA服务器密钥(如果您计划将来使用集中式Web身份验证（或任何需要授权更改[CoA]的安全类型）。

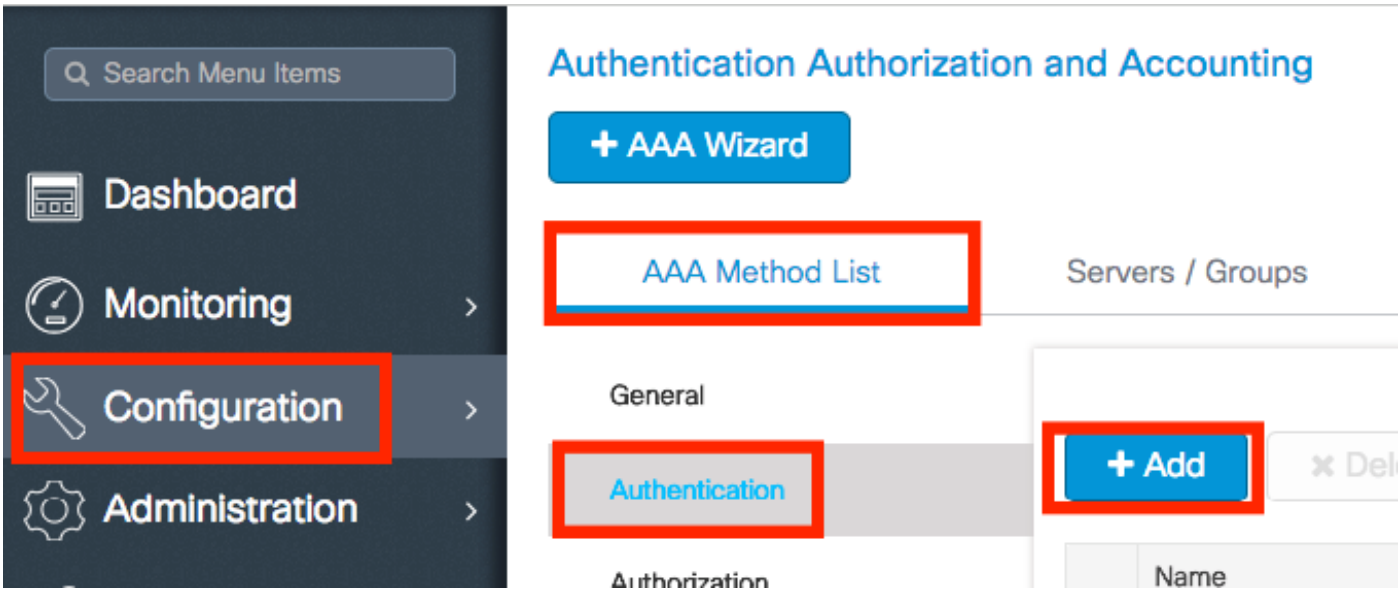
注意：Cisco 9800 WLC上的授权更改(CoA)服务器密钥是用于验证WLC和RADIUS服务器之间的CoA请求的共享密钥。此密钥必须与RADIUS服务器上的CoA配置匹配，以确保成功通信。请确保在所有设备上安全一致地配置CoA服务器密钥，以防止CoA消息被拒绝。



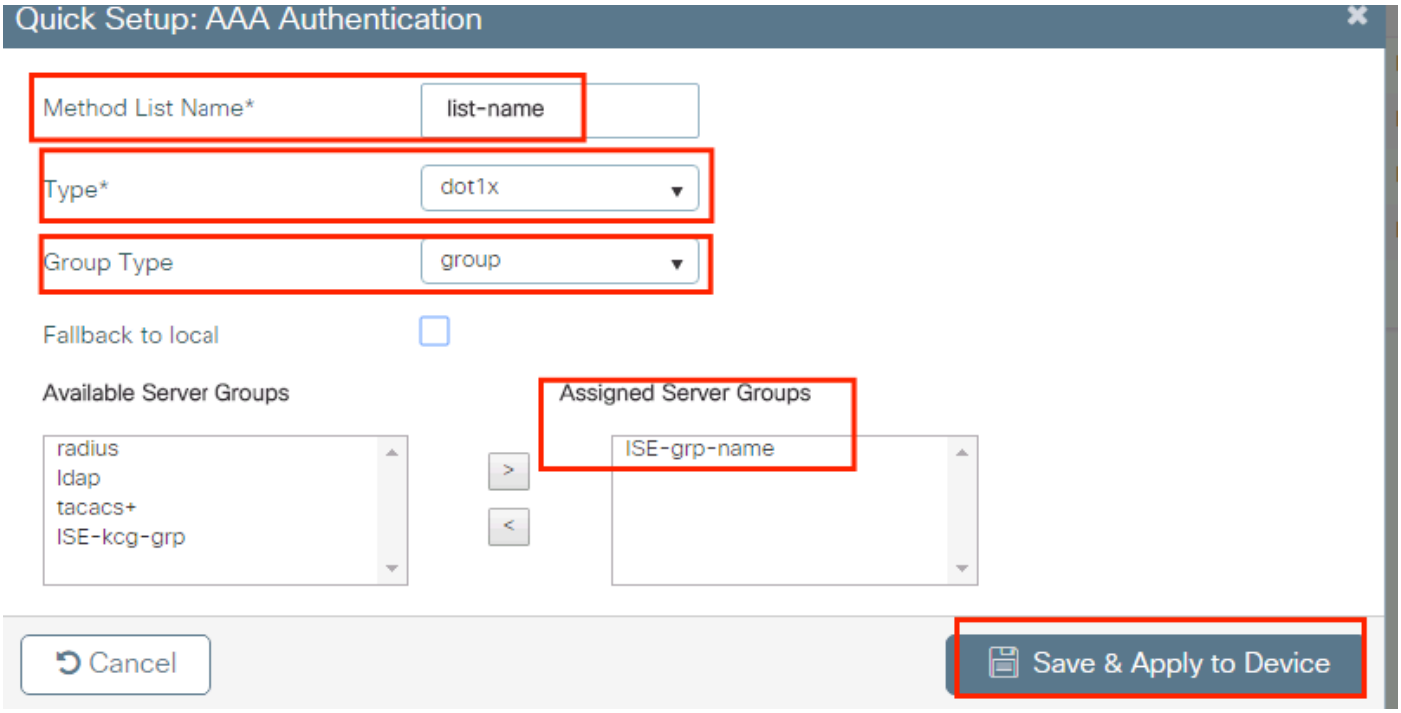
第 2 步： 将 RADIUS 服务器添加到 RADIUS 组。依次导航至 。为组命名，然后将您之前创建的服务器移至 列表中 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add. Assigned Servers**.



第 3 步： 创建身份验证方法列表。依次导航至 **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.



输入相关信息:



CLI：

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

有关 AAA 失效服务器检测的注意事项

配置RADIUS服务器后，可以检查它是否被视为ALIVE:

```
#show aaa servers | s WNCD
     Platform State from WNCD (1) : current UP
     Platform State from WNCD (2) : current UP
     Platform State from WNCD (3) : current UP
```

```
    Platform State from WNCD (4) : current UP
    ...
```

您可以在 WLC 上配置 以及，尤其是在使用多个 RADIUS 服务器的情况下。**dead criteria,deadtime**

```
#radius-server dead-criteria time 5 tries 3
#radius-server deadtime 5
```

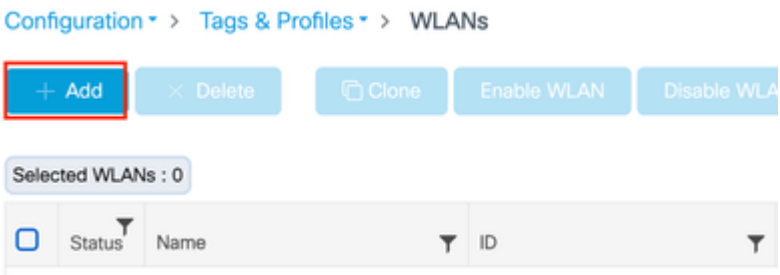
注意： 是用于将 RADIUS 服务器标记为失效的标准。**dead criteria**该标准包括：1. 超时（以秒为单位），表示从控制器上次收到来自 RADIUS 服务器的有效数据包到服务器被标记为“失效”必须经过的时间。2. 计数器，表示在将 RADIUS 服务器标记为“失效”之前控制器上必须发生的连续超时次数。

注意： 指定服务器在按照失效标准将其标记为“失效”之后保持失效状态的时间（以分钟为单位）。**deadtime**失效时间到期后，控制器会将服务器标记为“运行（活动）”，并通知已注册的客户端有关状态更改的信息。如果在将状态标记为“运行”之后仍然无法访问服务器，并且满足失效标准，则服务器会在失效时间间隔内再次被标记为“失效”。

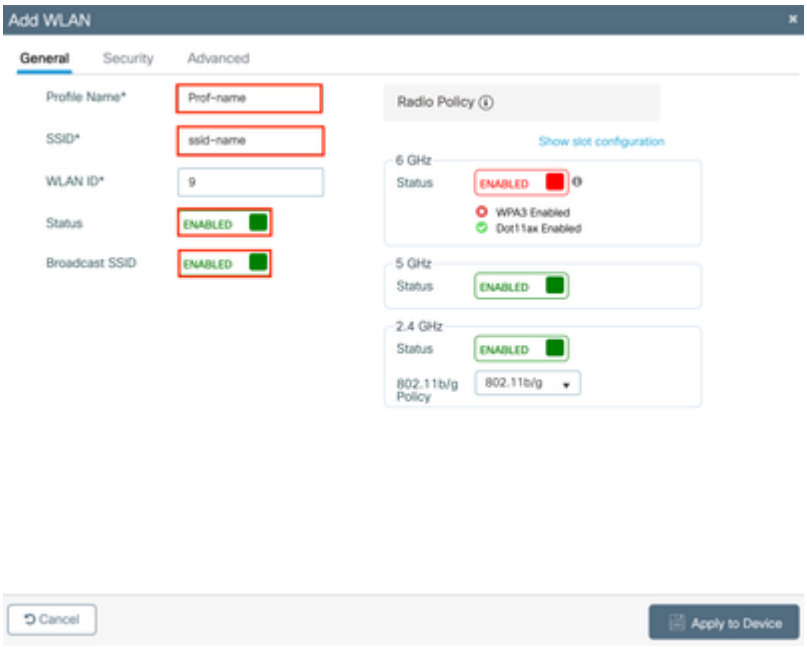
WLAN 配置文件配置

GUI:

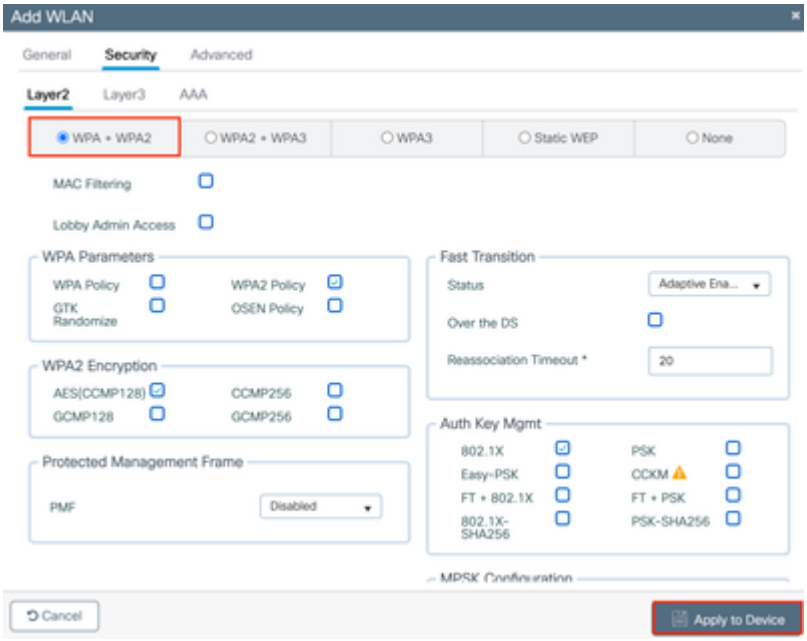
第 1 步： 创建 WLAN.导航到Configuration > Tags&Profiles > WLANs > + Add并根据需要配置网络。



第 2 步： 输入 WLAN 信息:

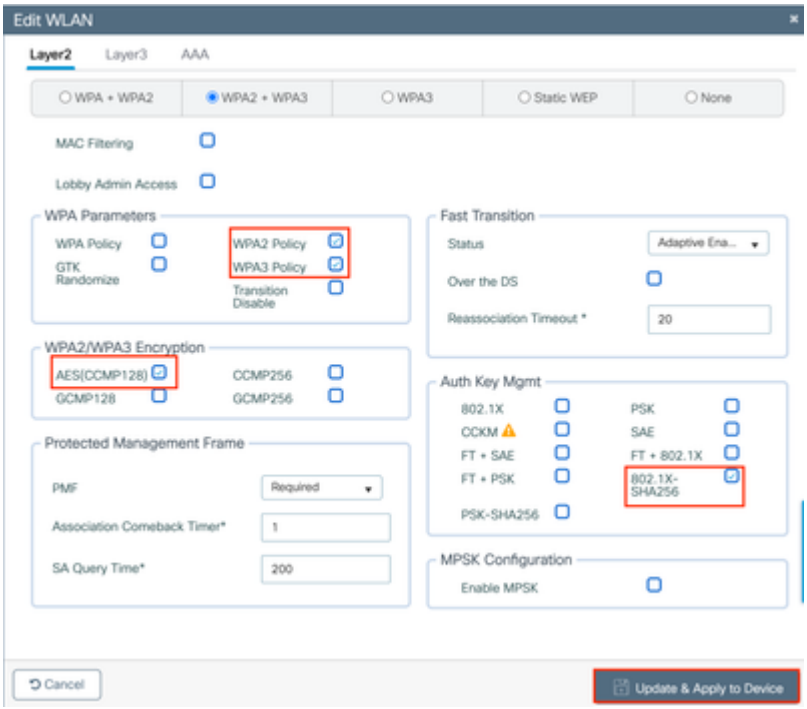


第 3a 步：导航到Security选项卡并选择所需的安全方法。本例中为 WPA2 + 802.1x。

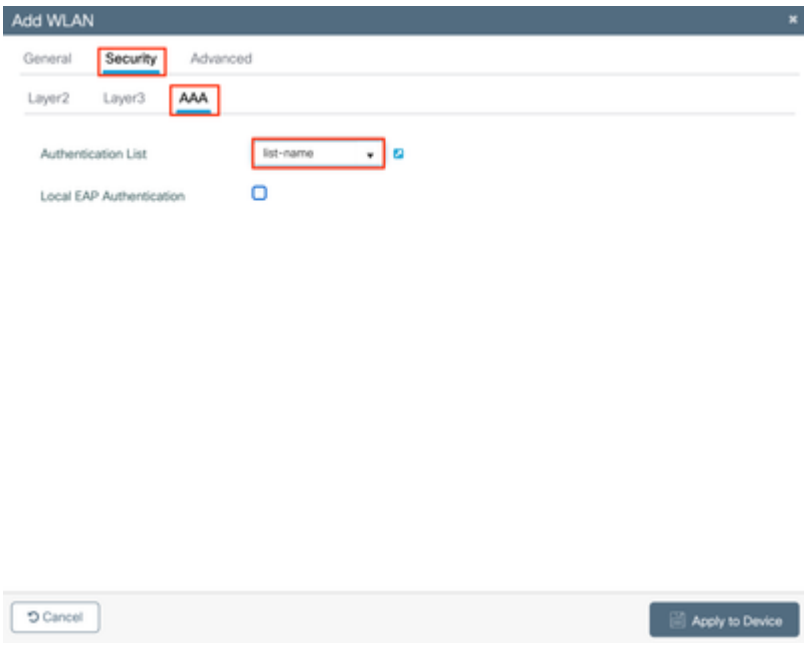


3b. WPA2+WPA3混合模式示例：

注意：Cisco 9800 WLC上的WPA2+WPA3混合模式支持现代WPA3设备和传统WPA2设备的无缝共存，尽可能确保兼容性和增强的安全性。快速过渡(FT)在此场景中是可选的，启用AKM FT+802.1x时成为强制性的。



第4步：从选**Security** > **AAA** 项卡中，从9800 WLC上的AAA配置部分选择在步骤3上创建的身份验证方法。



CLI：

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
```

```
# no shutdown
```

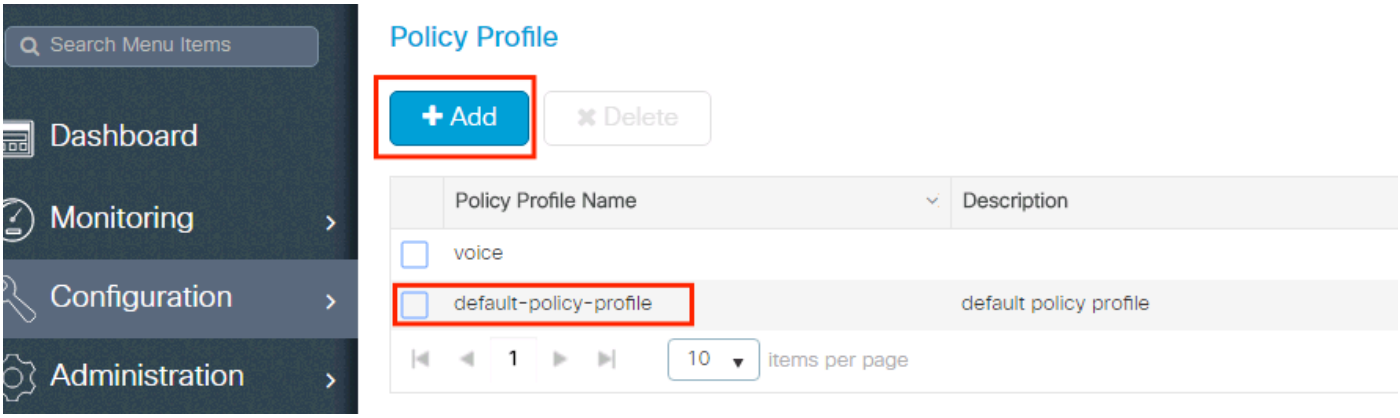
策略配置文件配置

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

您可以使用默认策略配置文件，也可以新建配置文件。

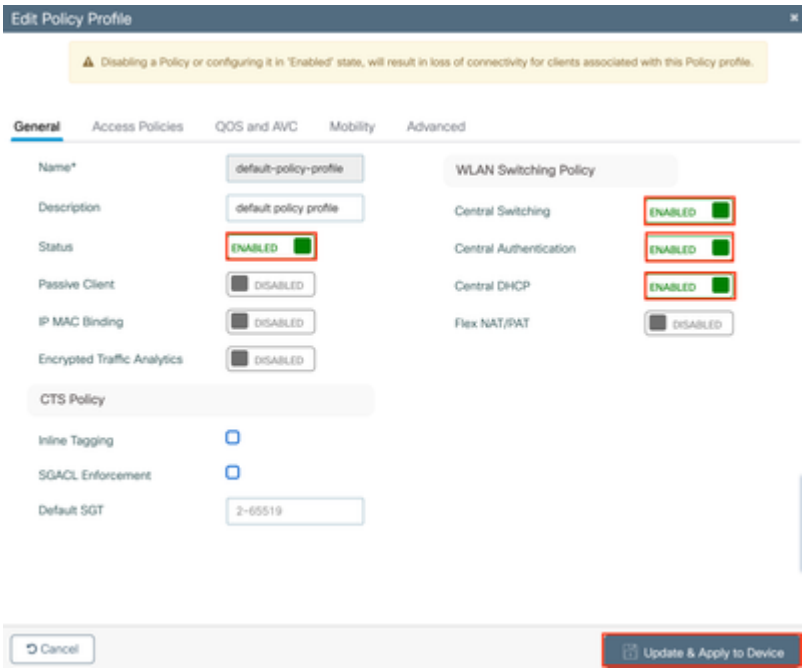
GUI:

依次导航至配置 > 标签和配置文件 > 策略配置文件，然后配置 default-policy-profile 或新建配置文件。

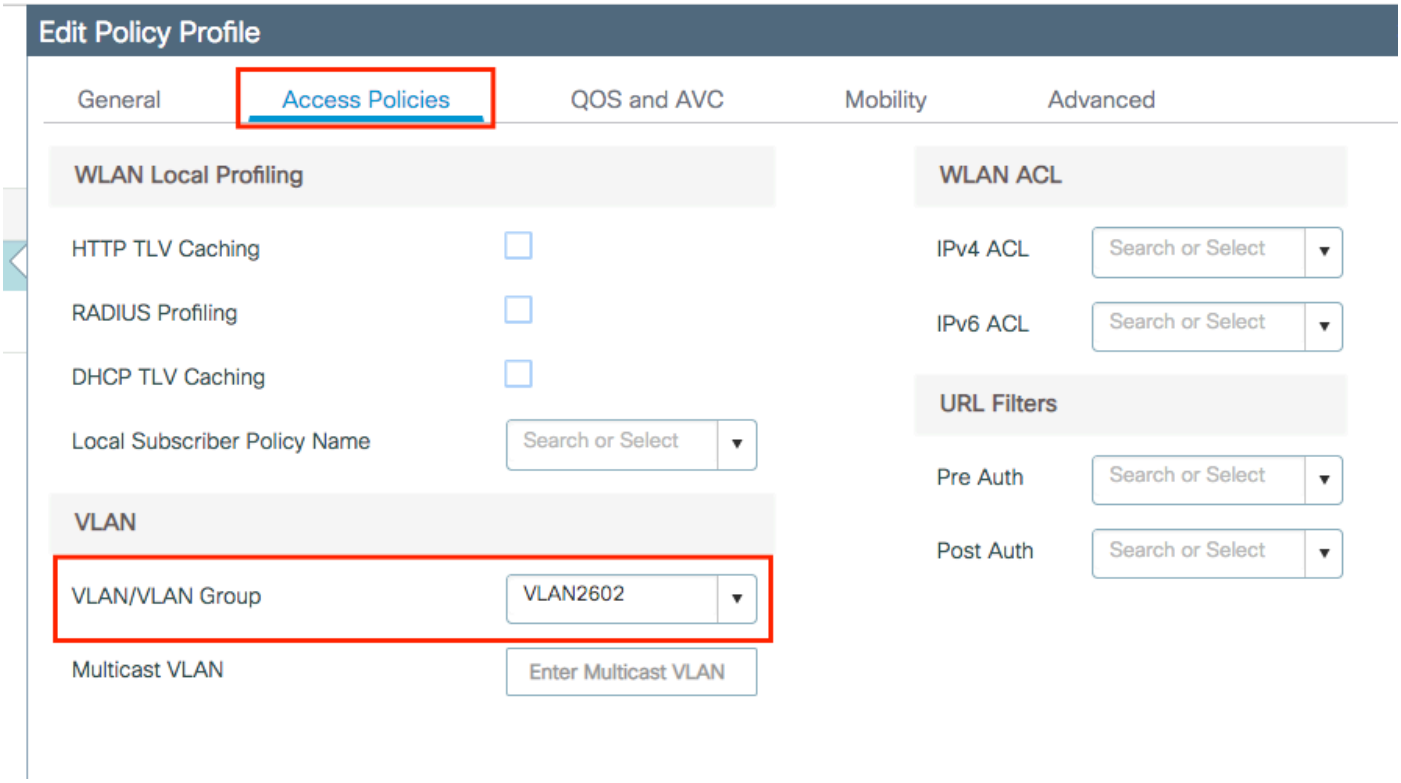


确保已启用配置文件。

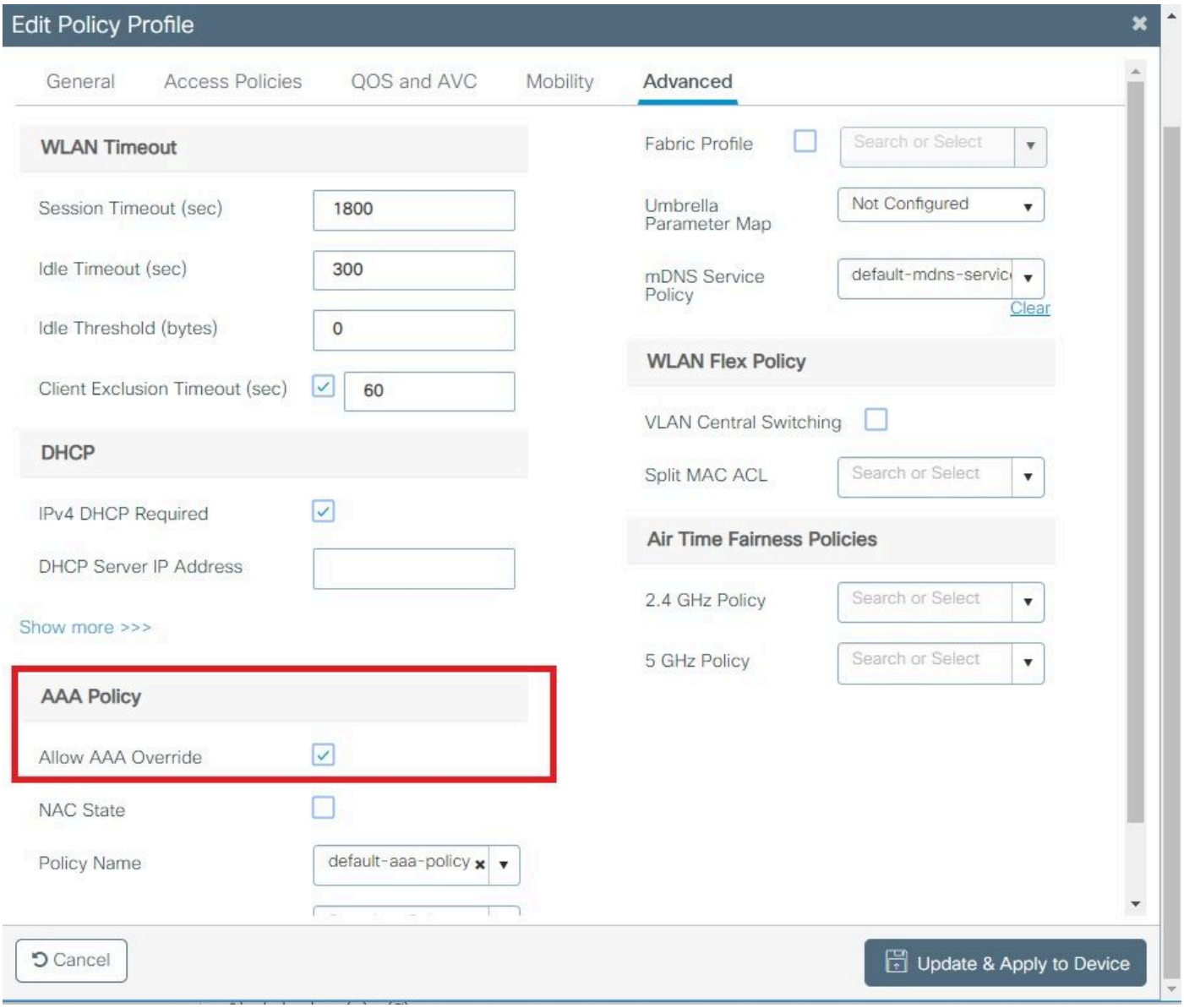
此外，如果接入点(AP)处于本地模式，请确保策略配置文件启用了集中交换、集中身份验证和集中 DHCP。



在访问策略选项卡中，选择需要分配客户端的 VLAN。



如果您计划让 ISE 在 Access-Accept 消息中返回属性（例如 VLAN 分配），请在 选项卡中启用 AAA 覆盖：**Advanced**



CLI：

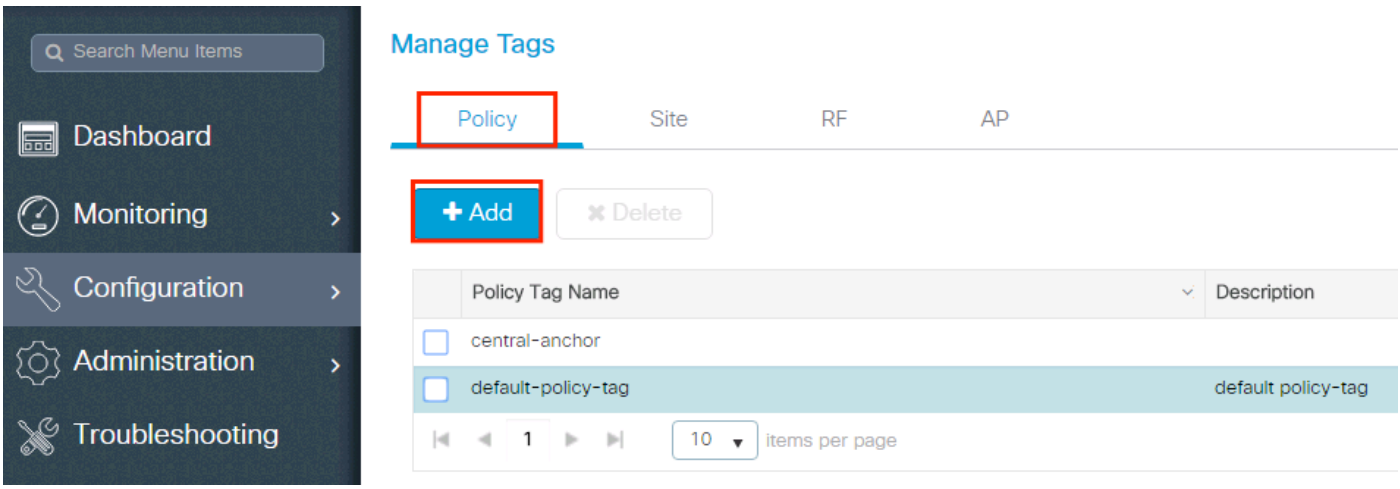
```
# config
# wireless profile policy <policy-profile-name>
# aaa-override
# central switching
# description "<description>"
# vlan <vlanID-or-VLAN_name>
# no shutdown
```

策略标签配置

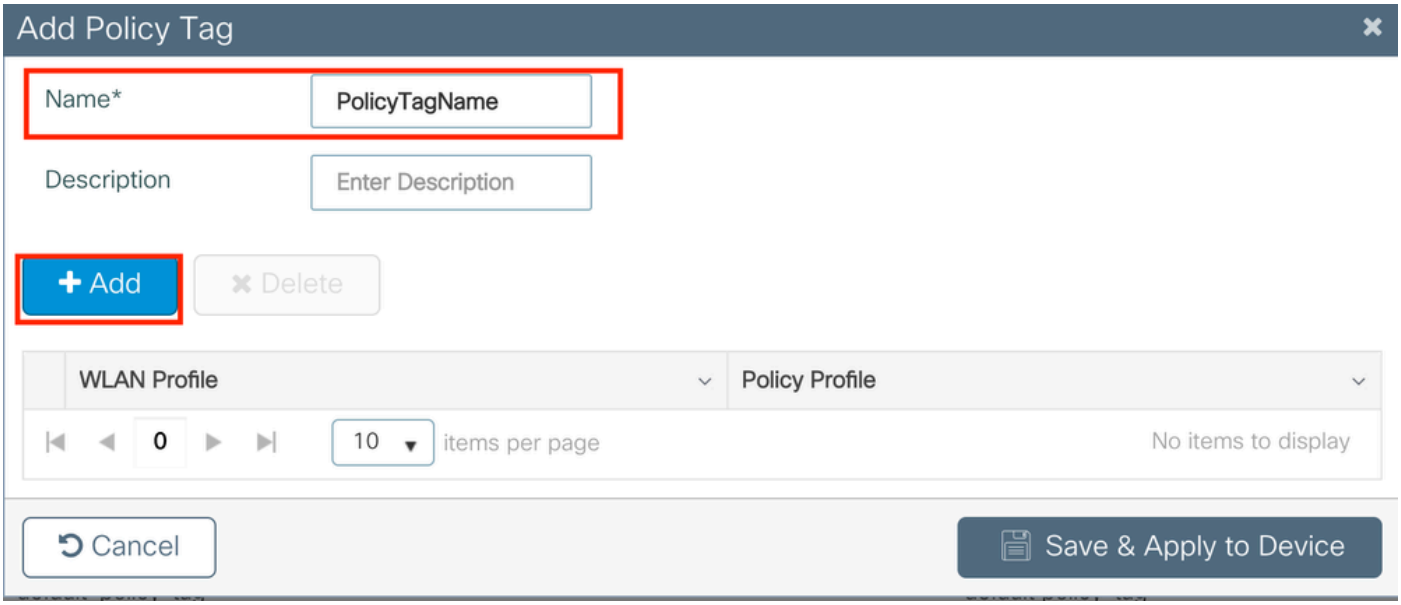
策略标签用于将 SSID 与策略配置文件关联。您可以新建策略标签，也可以使用 default-policy 标签。

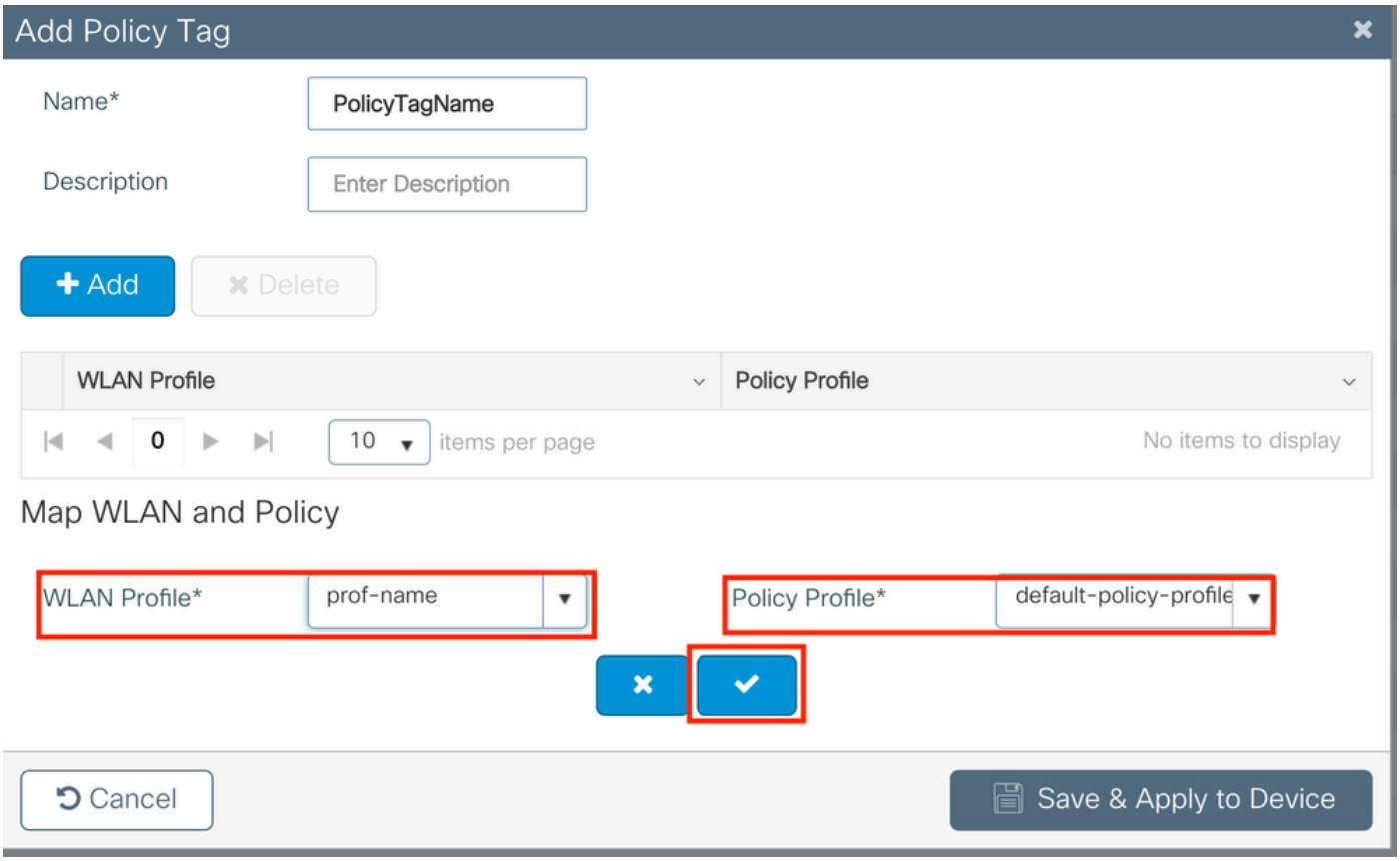
GUI:

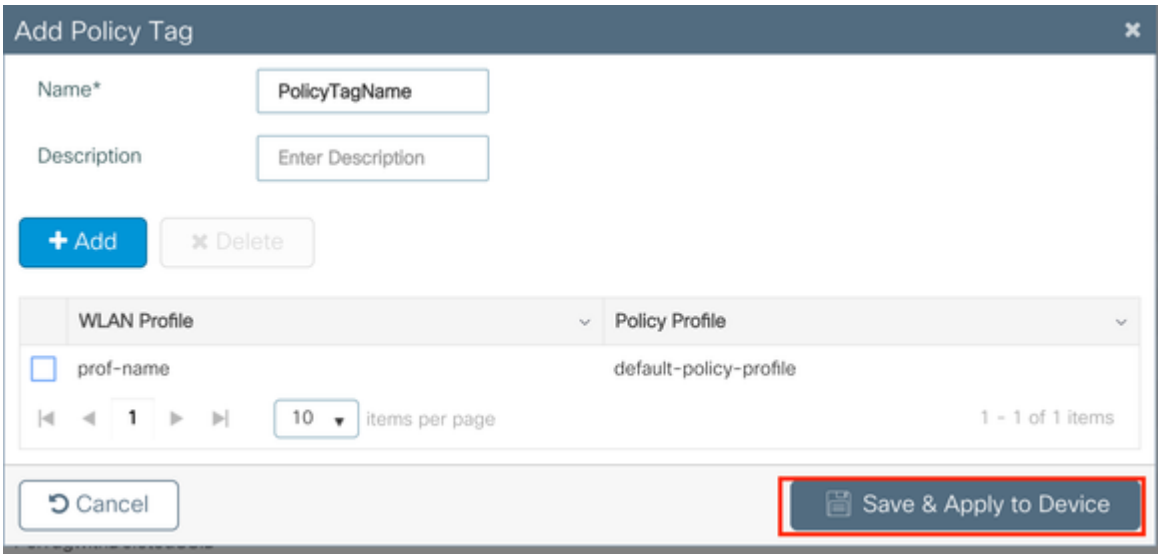
依次导航至 ，然后根据需要添加新的标签。**Configugation > Tags & Profiles > Tags > Policy**



将 WLAN 配置文件关联到所需的策略配置文件。







CLI：

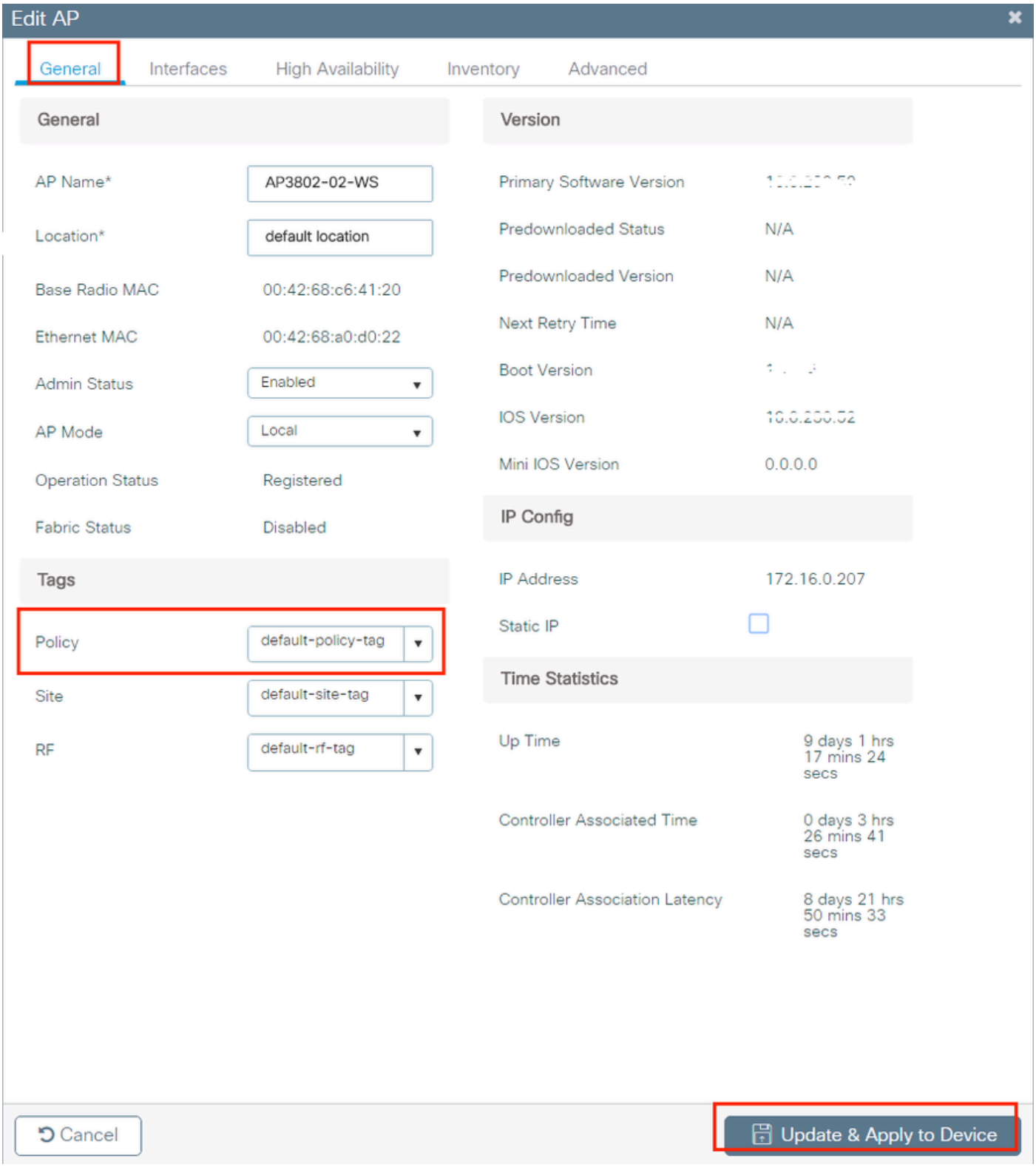
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

策略标签分配

将策略标签分配给所需的 AP。

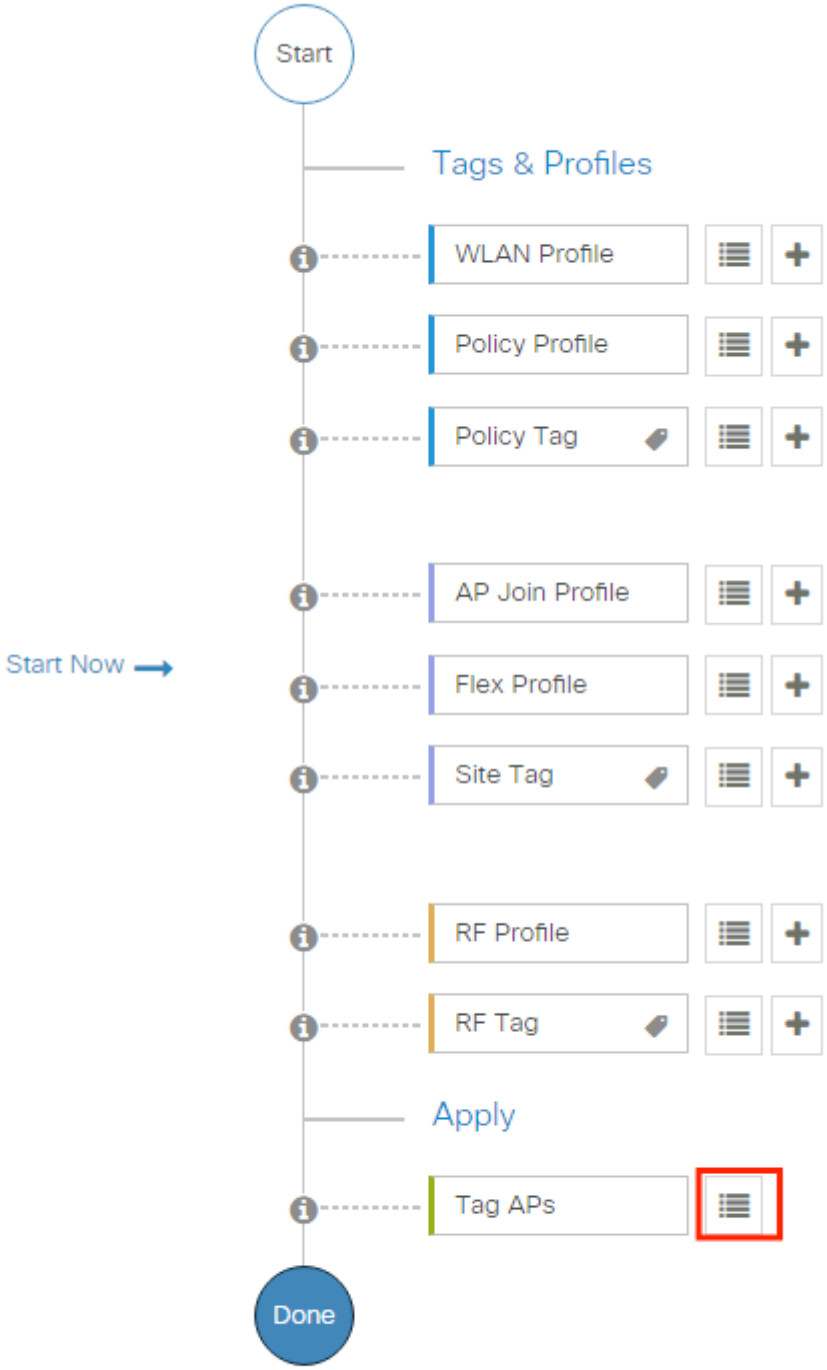
GUI:

要将标签分配给一个无线接入点，请依次导航至 ，分配相关策略标签，然后点击**Configuration > Wireless > Access Points > AP Name > General Tags**, **Update & Apply to Device**.

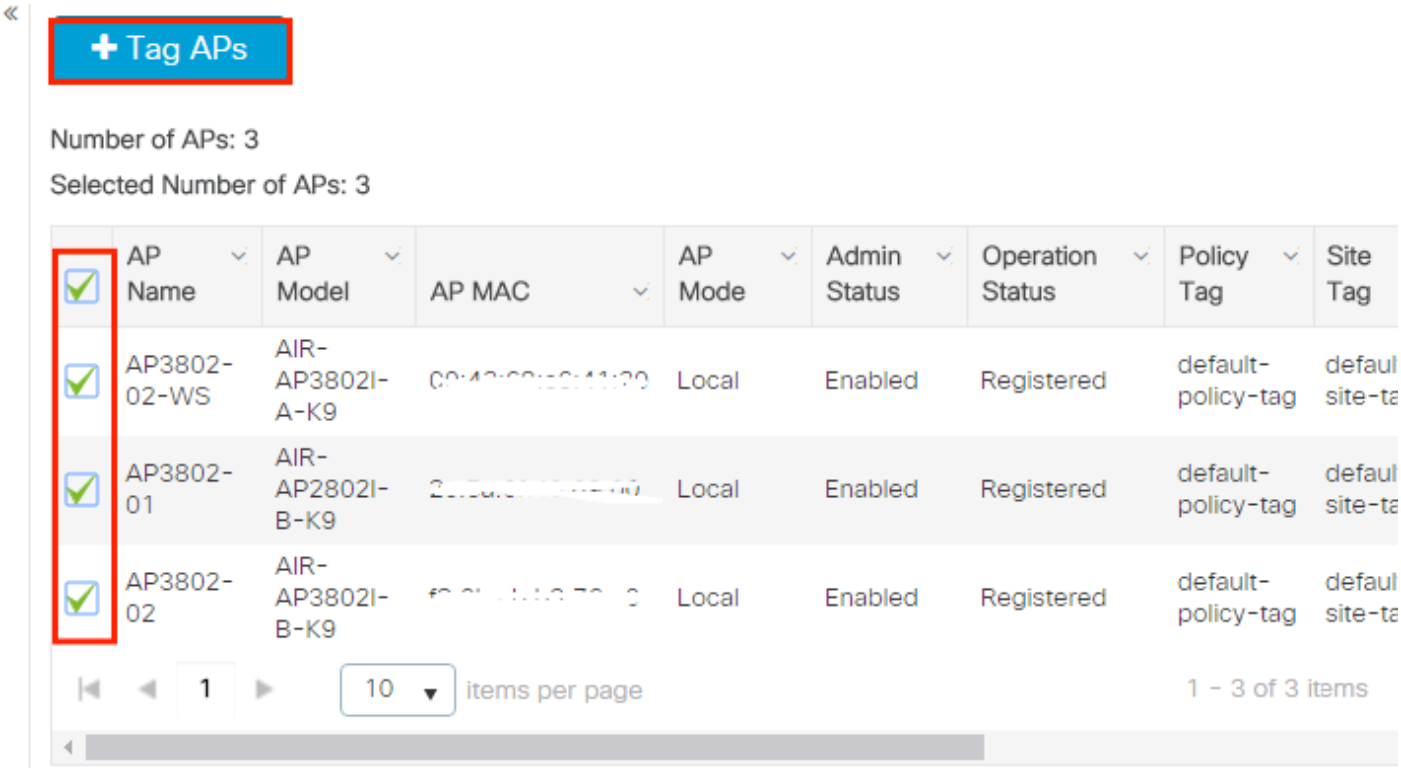


注意：请注意，当无线接入点上的策略标签发生更改时，它将失去与 9800 WLC 的关联，并在几分钟后重新关联。

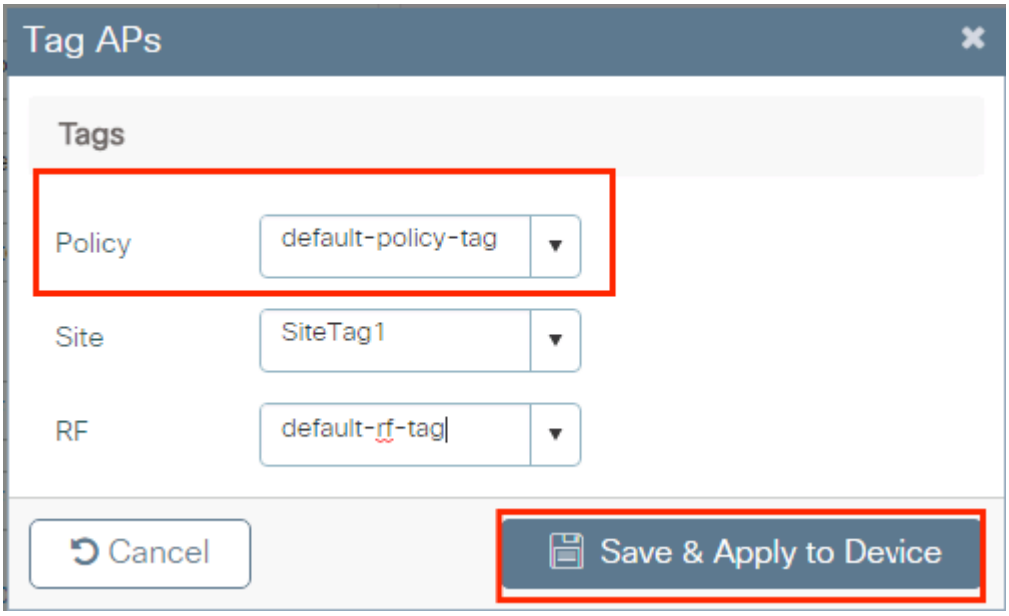
要将相同的策略标签分配给多个无线接入点，请依次导航至 **Configuration > Wireless Setup > Advanced > Start Now > Apply**.



选择要向其分配标签的 AP，然后点击 + Tag APs.



选择适用于策略、站点和RF的标签，然后点击Save & Apply to Device:



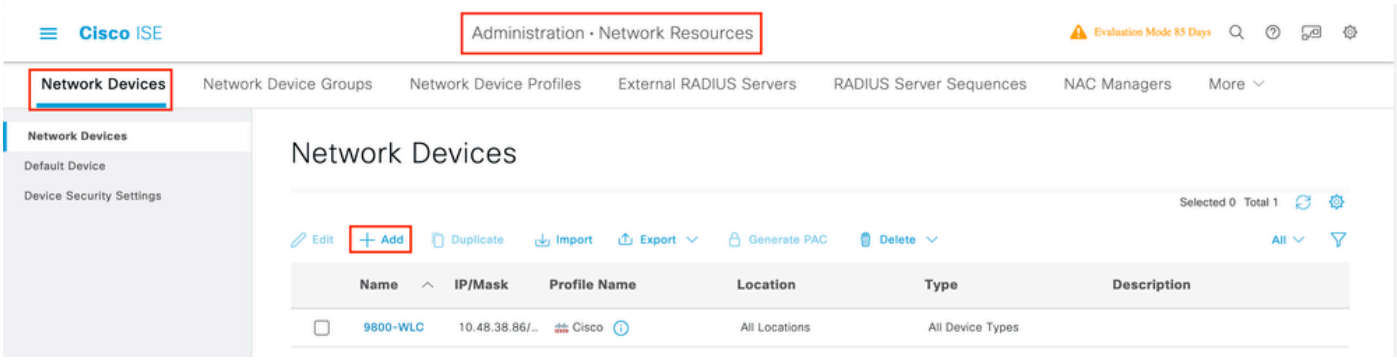
CLI：

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

ISE 配置

在 ISE 上声明 WLC

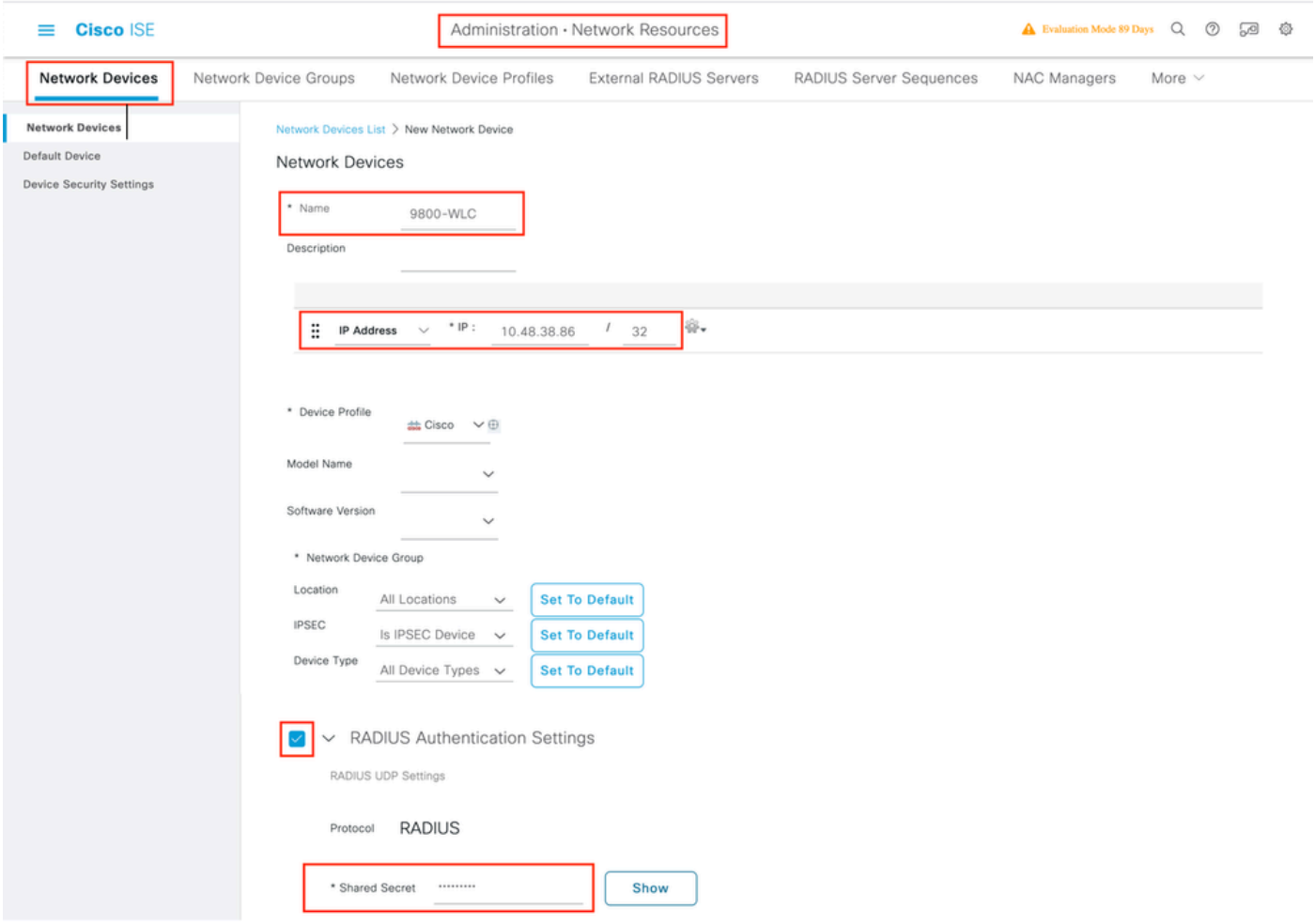
第 1 步： 打开 ISE 控制台，然后依次导航至 ，如图所示。**Administration > Network Resources > Network Devices > Add**



第 2 步： 配置网络设备。

或者，您可以添加指定的型号名称、软件版本、说明，并根据设备类型、位置或 WLC 分配网络设备组。

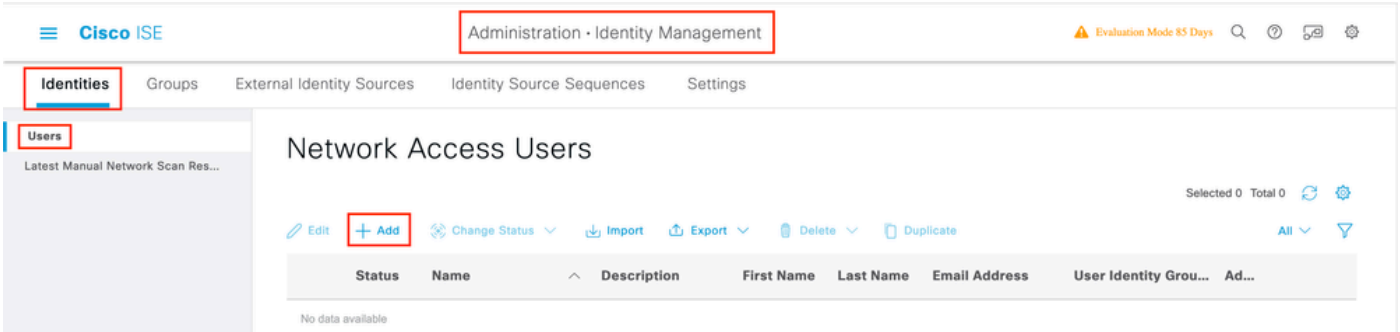
此处的 IP 地址对应于发送身份验证请求的 WLC 接口。默认情况下，它是管理接口，如图所示：



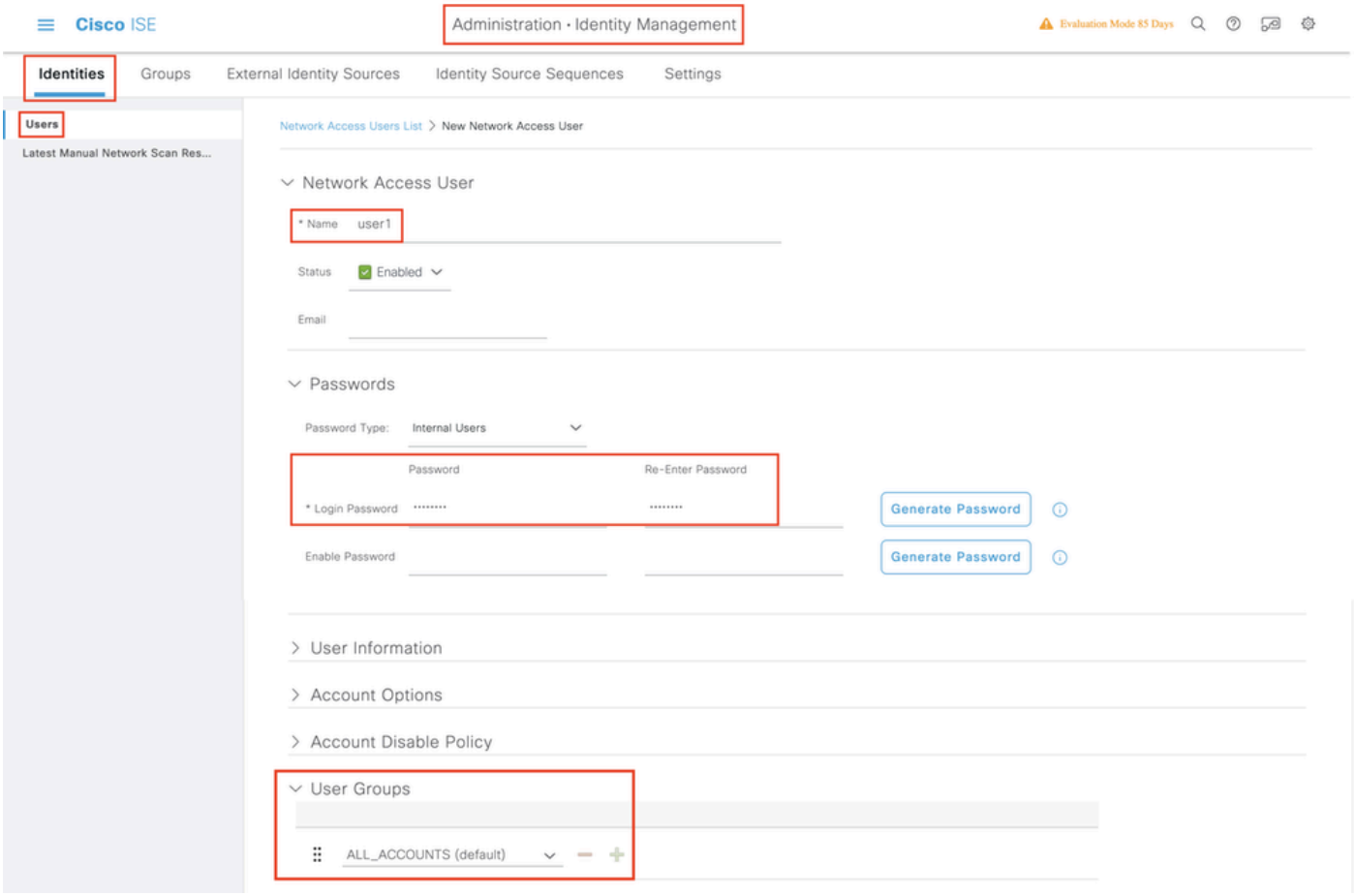
有关 的详细信息，请参阅以下章节： **Network Device Groups**从《思科身份服务引擎管理员指南：网络设备组》管理网络设备。

在 ISE 上创建新用户

步骤1.导 **Administration > Identity Management > Identities > Users > Add** 航至如图所示：



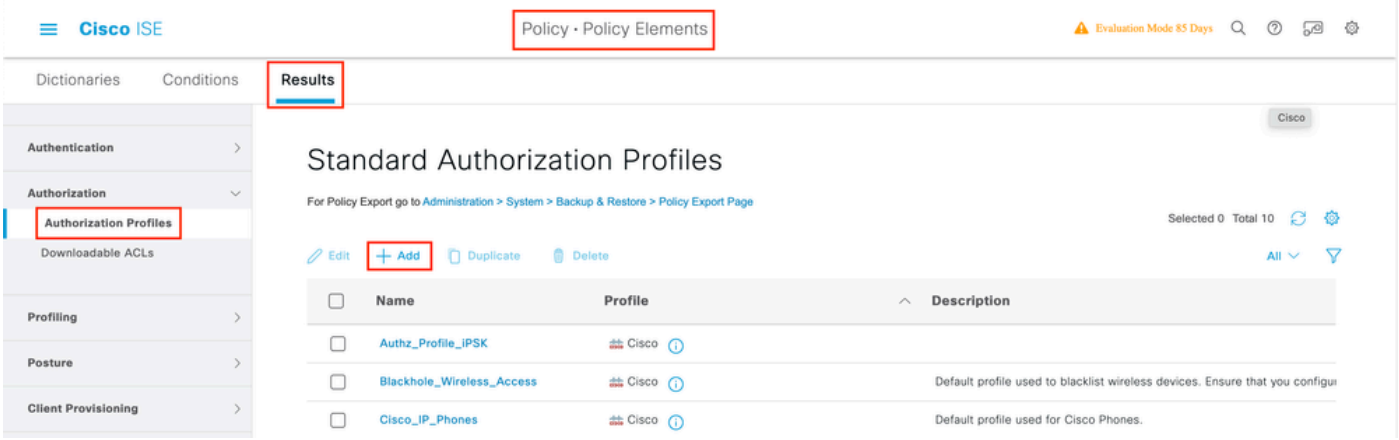
第 2 步： 输入用户的信息。在本例中，用户属于名为 ALL_ACCOUNTS 的组，但可以根据需要进行调整，如图所示：



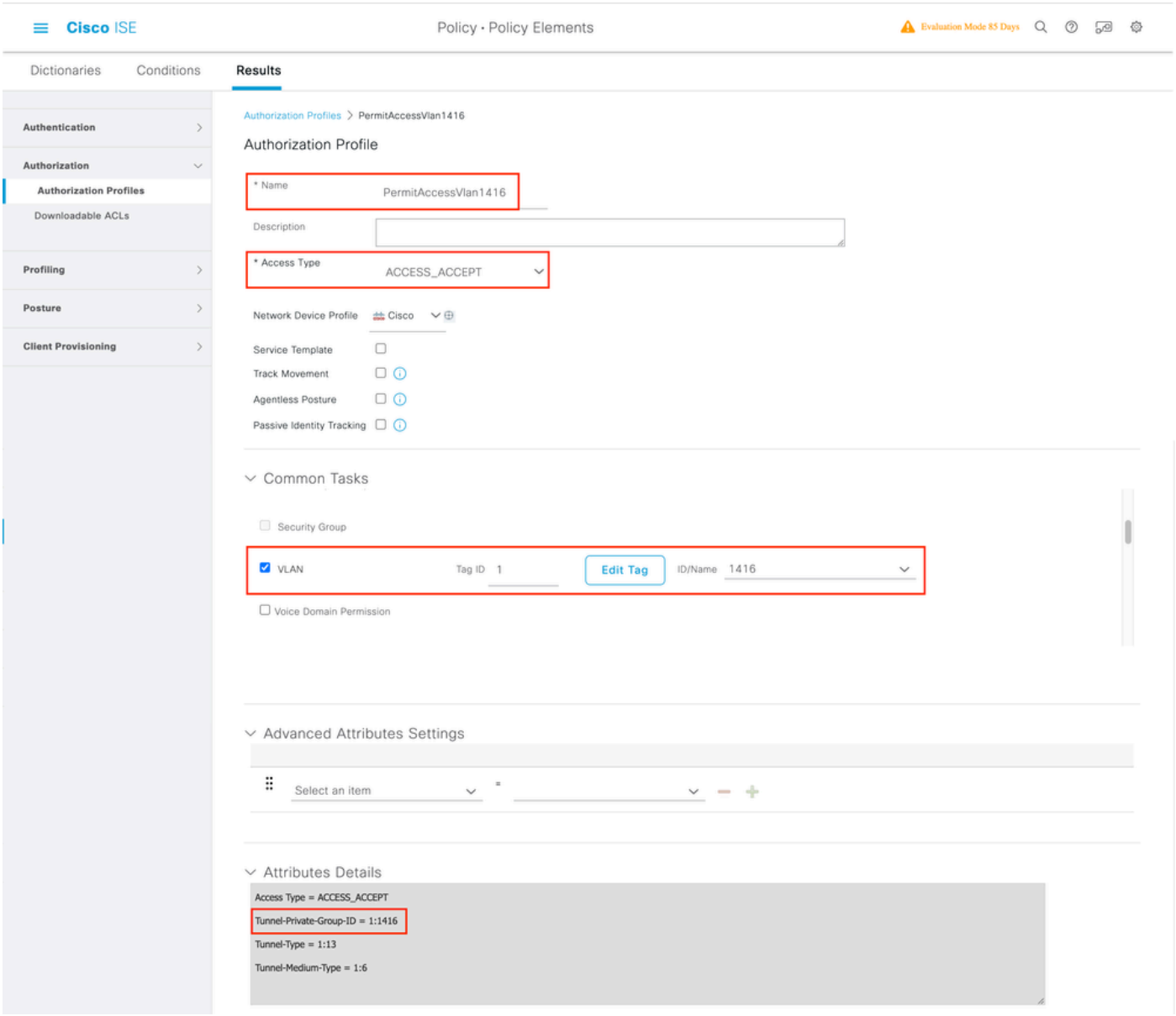
创建授权配置文件

由在满足条件时返回的一组属性组成。**Authorization Profile**授权配置文件确定客户端是否有权访问网络、推送访问控制列表 (ACL)、VLAN 覆盖或任何其他参数。本例中显示的授权配置文件为客户端发送访问接受消息，并将客户端分配给 VLAN 1416。

步骤1.导航到**Policy > Policy Elements > Results > Authorization > Authorization Profiles** 并点击按**Add**钮。

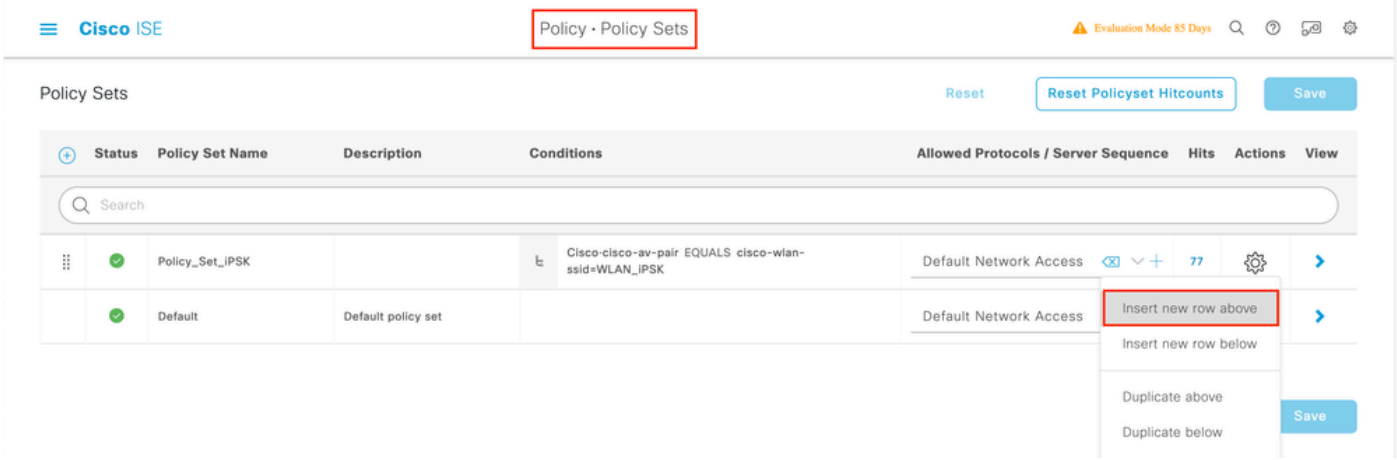


第 2 步： 输入图中所示的值。作为示例，我们可以在此处返回 AAA 覆盖属性，例如 VLAN。WLC 9800 接受使用 VLAN ID 或名称的隧道属性 64、65、81，并且还接受使用 属性。**AirSpace-Interface-Name**



创建策略集

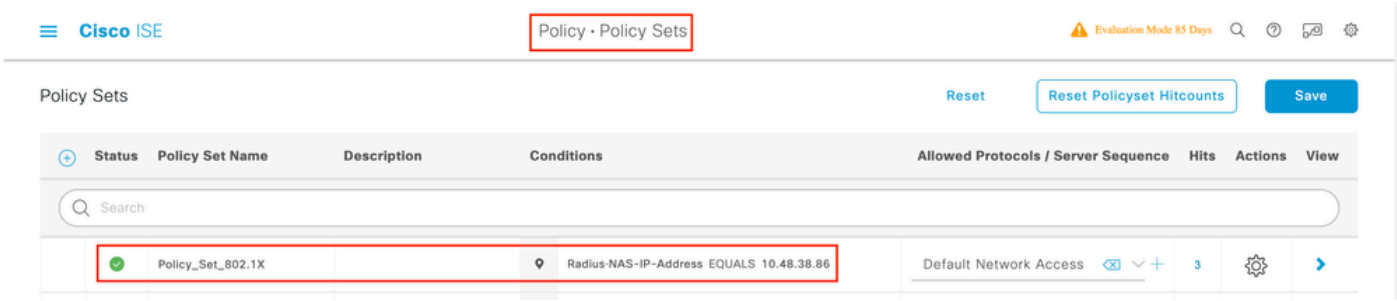
策略集定义一组身份验证和授权规则。要创建策略，请转至，点击列表中的第一个策略集的齿轮，然后选择，如下图所示：**Policy > Policy SetsInsert new row above**



为此策略集配置名称并创建条件。在本例中，该条件指定匹配来自 WLC 的流量：

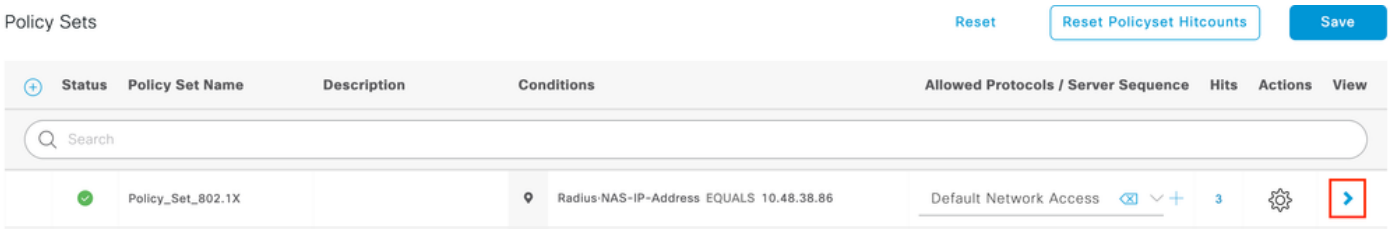
```
Radius:NAS-IP-Address EQUALS X.X.X.X     // X.X.X.X is the WLC IP address
```

确保在 下选择了 。**Default Network AccessAllowed Protocols / Server Sequence**



创建身份验证策略

要配置身份验证和授权策略，您需要进入策略集配置。点击 行右侧的蓝色箭头即可完成此操作：**Policy Set**



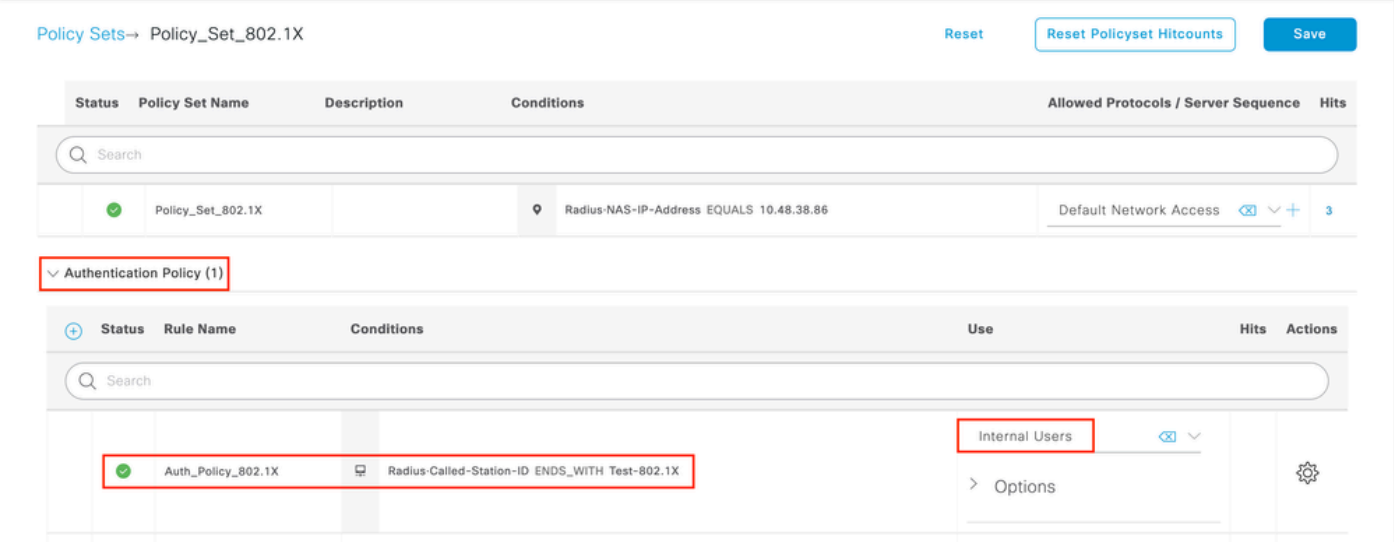
身份验证策略用于验证用户的凭证是否正确（验证用户的身份是否真实）。 在 下，创建身份验证策略并按下图所示进行配置。**Authenticaton Policy**,本例中使用的策略的条件为：

```
RADIUS:Called-Station-ID ENDS_WITH

        //

      is the SSID of your WLAN
```

Use此外，选择Authentication Policy选项卡下的Internal Users。



创建授权策略

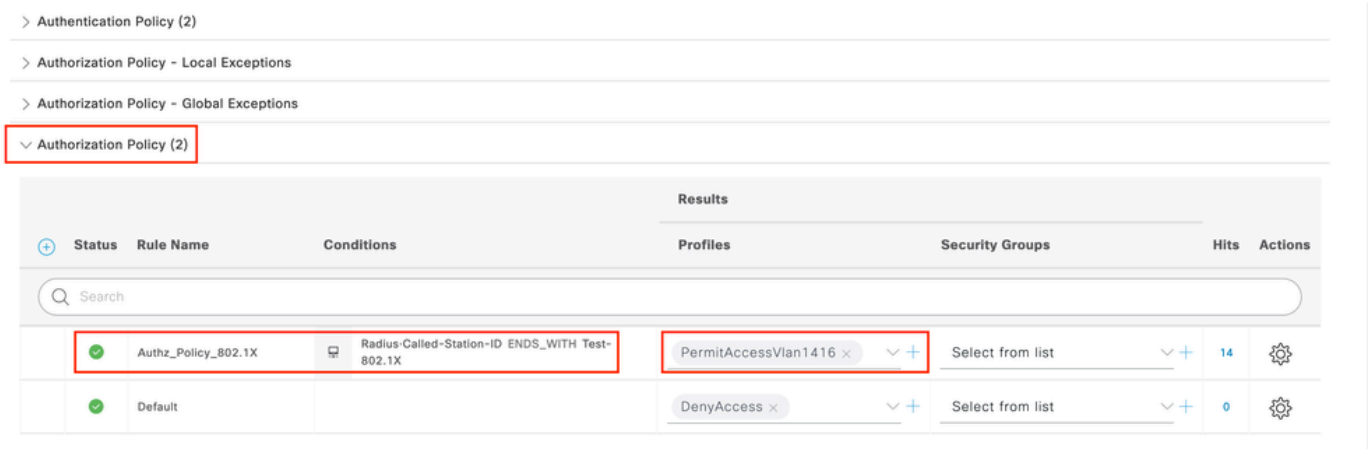
在同一页面上，转至 并新建策略。**Authorization Policy** 此授权策略的条件为：

```
RADIUS:Called-Station-ID ENDS_WITH

        //
```

```
is the SSID of your WLAN
```

在此策略的 选项卡下，选择您之前创建的 。**Result > ProfilesAuthorization Profile**如果用户经过身份验证，这会使 ISE 将正确的属性发送到 WLC。



此时，WLC 和 ISE 的所有配置均已完成，您可以尝试连接客户端。

有关 ISE 允许协议策略的详细信息，请查看以下章节：《思科身份服务引擎管理员指南》中的“管理身份验证策略”：管理身份验证策略

有关 ISE 身份源的详细信息，请查看以下章节：《思科身份服务引擎管理员指南》中的“管理用户和外部身份源”：身份源

验证

您可以使用下列命令验证当前配置：

```
# show run wlan // WLAN configuration
# show run aaa // AAA configuration (server, server group, methods)
# show aaa servers // Configured AAA servers
# show ap config general // AP's configurations
# show ap name <ap-name> config general // Detailed configuration of specific AP
# show ap tag summary // Tag information for AP'S
# show wlan { summary | id | name | all } // WLAN details
# show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
# show wireless profile policy detailed <policy-profile name>// Detailed information on given policy pr
```

故障排除



注意：可以使用外部负载均衡器。但是，请使用 calling-station-id RADIUS 属性来确保负载均衡器在每个客户端上运行。依赖 UDP 源端口平衡来自 9800 的 RADIUS 请求是不受支持的机制。

在 WLC 上进行故障排除

WLC 9800 提供无间断跟踪功能。这可确保持续记录所有客户端连接相关的错误、警告和通知级别消息，并且您可以在事件发生后查看事件或故障情况的日志。这取决于生成的日志量，但通常您可以返回几小时到几天。

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

第 1 步： 检查 WLC 的当前时间，以便追溯到问题发生时的日志。

```
# show clock
```

第 2 步： 根据系统配置，从 WLC 缓冲区或外部系统日志中收集系统日志。这样可以快速查看系统运行状况和错误（如有）。

```
# show logging
```

第 3 步： 验证是否已启用调试条件。

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

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

注意：如果屏幕上列出任何条件，则对于满足这些启用条件（MAC 地址、IP 地址等）的所有进程，其跟踪信息会按调试级别日志进行记录。 这会增加日志量。因此，建议在非主动调试时清除所有条件.

第 4 步： 如果所测试的 MAC 地址未在第 3 步中作为条件列出，请收集特定 MAC 地址的无间断通知级别跟踪信息。

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

您可以显示会话内容，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>
```

条件调试和无线电主动跟踪

如果无间断跟踪未能提供足够的信息来确定所调查问题的触发原因，则可以启用条件调试并捕获无线电主动 (RA) 跟踪，以便为与指定条件（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。 您可以通过 GUI 或 CLI 执行此操作。

CLI：

要启用条件调试，请执行以下步骤。

第 5 步： 确保未启用调试条件。

```
# clear platform condition all
```

第 6 步： 为要监控的无线客户端 MAC 地址启用调试条件。

以下命令用于启动对所提供 MAC 地址的监控，持续时间为 30 分钟（1800 秒）。 您可以选择延长监控时间，最多监控 2085978494 秒。

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

注意：要同时监控多个客户端，请对每个 MAC 地址运行 debug wireless MAC <aaaa.bbbb.cccc> 命令。

注：终端会话中不会显示客户端活动的输出，因为所有内容都在内部缓冲，以备稍后查看。

第 7 步： 重现要监控的问题或行为。

第 8 步： 如果在默认或配置的监控时间已经过之前问题再次出现，请停止调试。

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

监控时间结束或无线网络调试停止后，9800 WLC 会生成一个本地文件，其名称为：

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

第 9 步：收集与 MAC 地址活动相关的文件。 可以将 ra trace.log 复制到外部服务器，也可以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.
```

显示内容：

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

第 10 步： 如果根本原因仍不明显，请收集内部日志，该日志是更为详细的调试级别日志。无需再次调试客户端，因为我们会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
```

注意：此命令输出会返回所有进程的全部日志级别的跟踪信息，因此数量非常庞大。在解析跟踪信息时如需帮助，请联系 Cisco TAC。

您可以将 ra-internal-FILENAME.txt 复制到外部服务器，也可以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
```

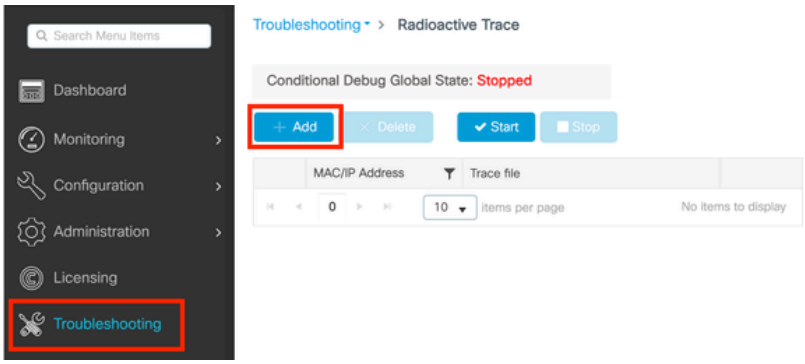
第 11 步： 删除调试条件。

```
# clear platform condition all
```

注意：请务必在故障排除会话结束后移除调试条件。

GUI:

第 1 步： 转至 ，并指定要进行故障排除的客户端的 MAC/IP 地址。**Troubleshooting > Radioactive Trace > + Add**

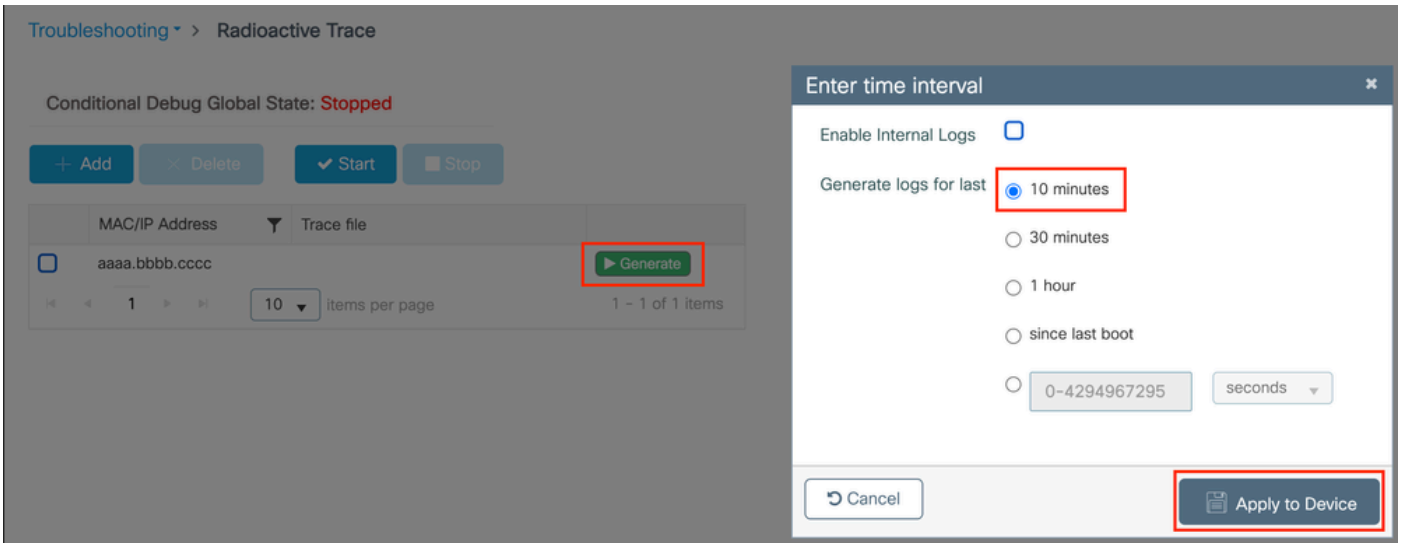


第 2 步： 点击开始。

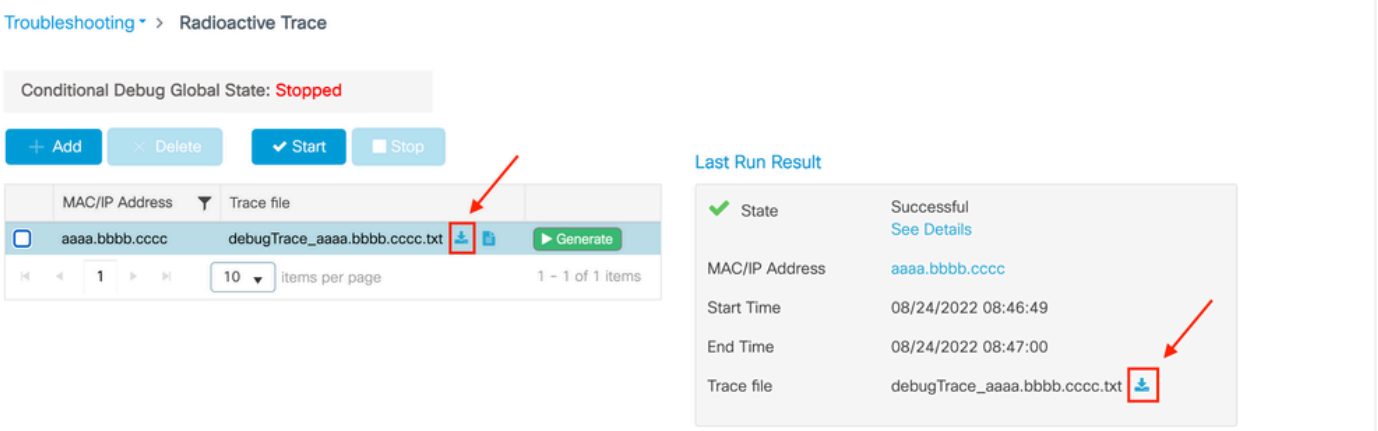
第 3 步： 重现问题。

第 4 步：点击停止。

步骤5.单击**Generate**按钮，选择要获取日志的时间间隔，然后单击 **Apply to Device**. In this example, the logs for the last 10 minutes are requested.

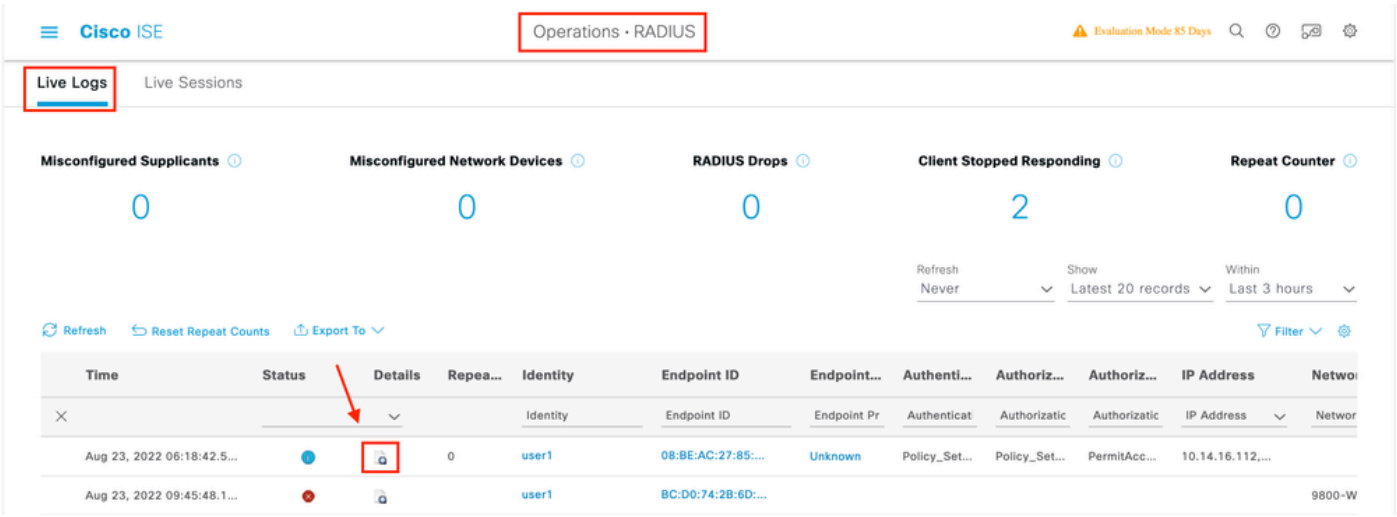


第 6 步： 将无线电主动跟踪文件下载到计算机上，然后点击下载按钮并进行检查。



在 ISE 上进行故障排除

如果遇到客户端身份验证问题，您可以验证 ISE 服务器上的日志。转至，然后您会看到身份验证请求列表以及匹配的策略集、每个请求的结果等。**Operations > RADIUS > Live Logs**点击每行 选项卡下的放大镜，可以获取更多详细信息，如图所示：**Details**



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）。