使用ISE配置Catalyst 9800 WLC iPSK

目录

简介

本文档介绍在Cisco 9800无线局域网控制器上配置iPSK安全WLAN，并将Cisco ISE用作RADIUS服务器。

先决条件

要求

本文档假设您已经熟悉9800上WLAN的基本配置，并能根据您的部署调整配置。

使用的组件

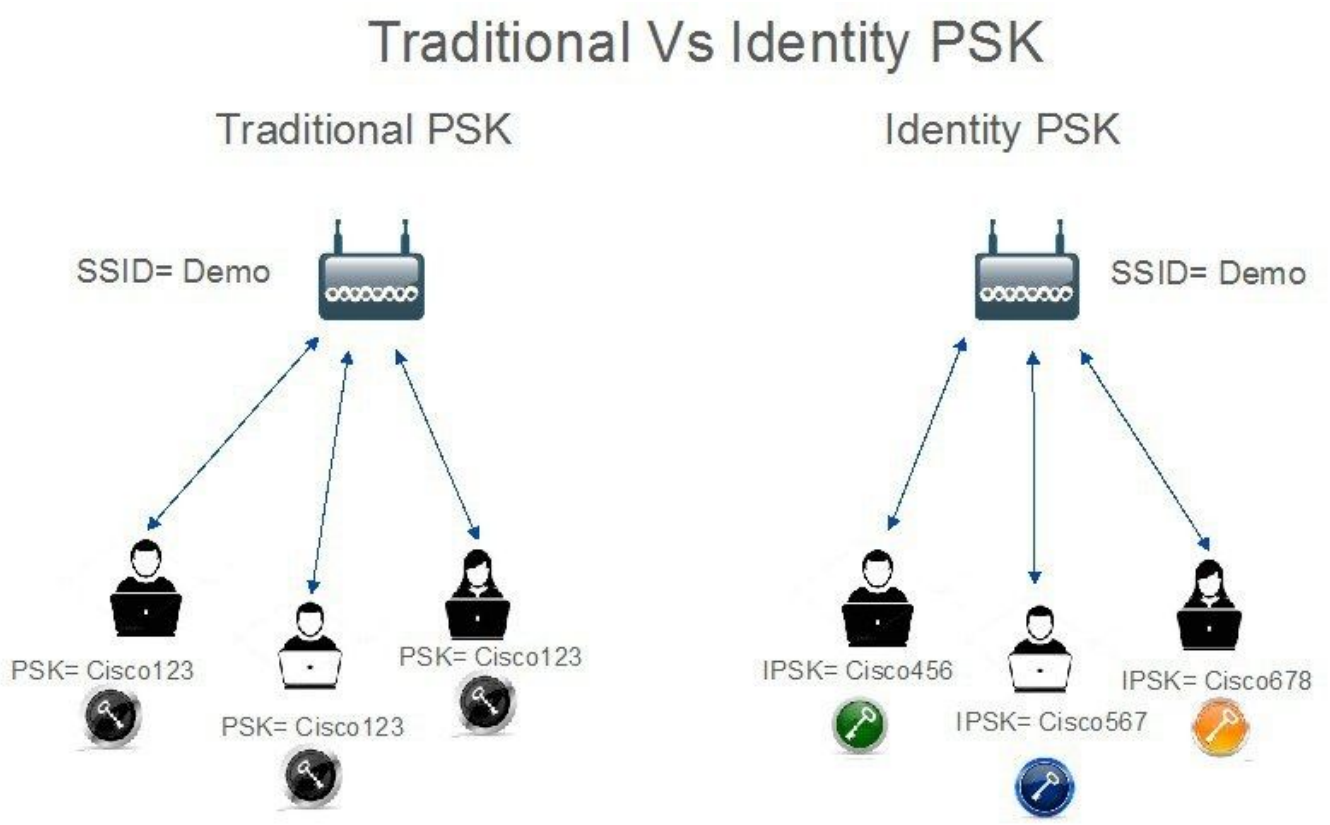
- 运行17.6.3的Cisco 9800-CL WLC
- 思科ISE 3.0

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。

了解iPSK是什么，适合哪些场景

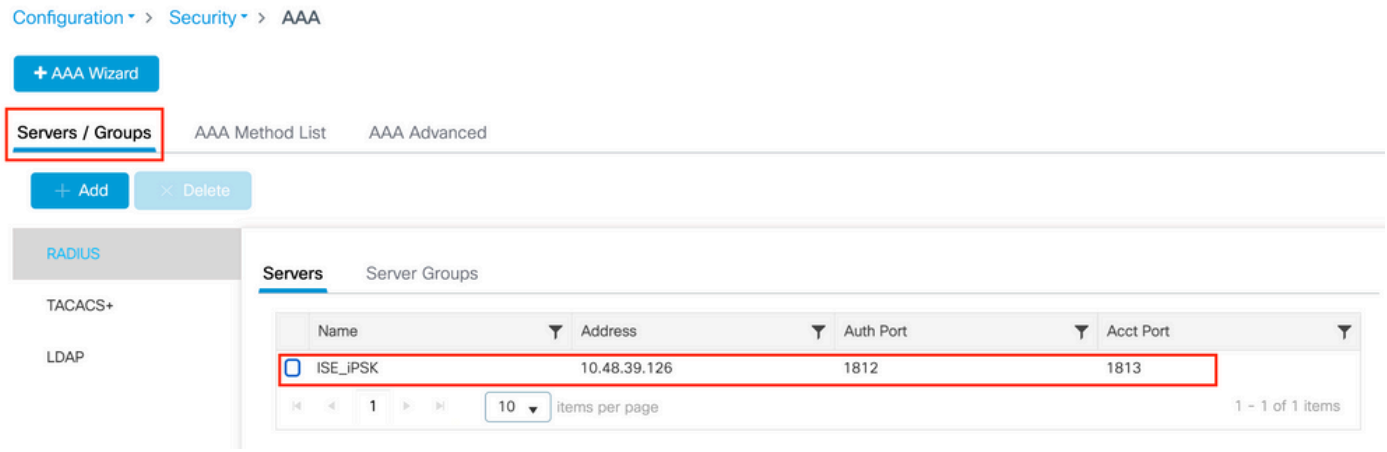
传统预共享密钥(PSK)安全网络对所有连接的客户端使用相同的密码。这可能会导致与未经授权的用户共享密钥，从而造成安全漏洞和未经授权的网络访问。此漏洞最常见的缓解措施是PSK本身的更改，这种更改会影响所有用户，因为许多终端设备需要更新新密钥才能再次访问网络。

通过身份PSK(iPSK)，在RADIUS服务器的帮助下为相同SSID上的个人或用户组创建唯一的预共享密钥。在终端客户端设备不支持dot1x身份验证，但需要更安全和更精细的身份验证方案的网络中，这种设置非常有用。从客户端角度看，此WLAN看起来与传统PSK网络相同。如果其中一个PSK受到危害，则仅受影响的个人或组需要更新其PSK。连接到WLAN的其余设备不受影响。

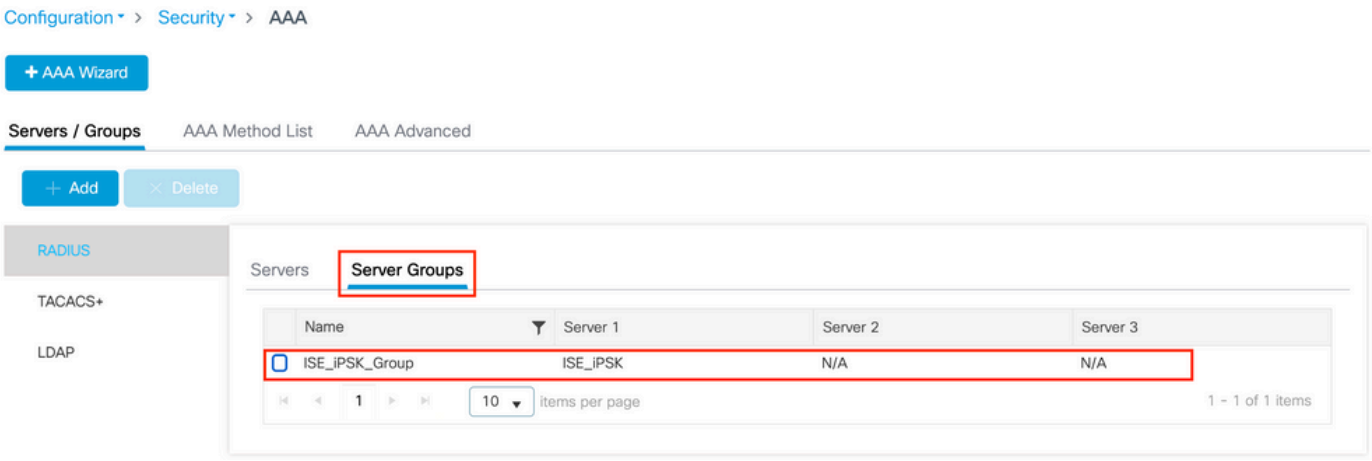


配置9800 WLC

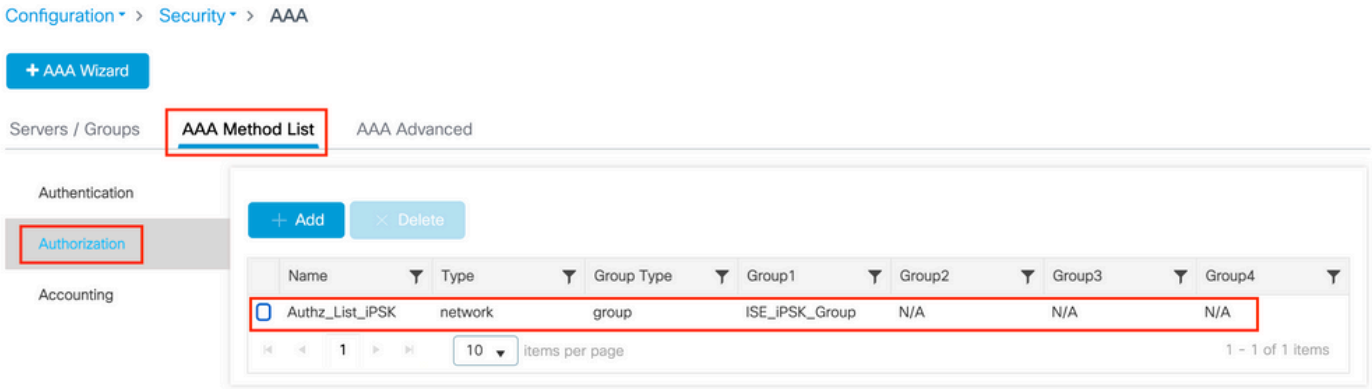
在**Configuration > Security > AAA > Servers/Groups > Servers**下，将ISE添加为RADIUS服务器：



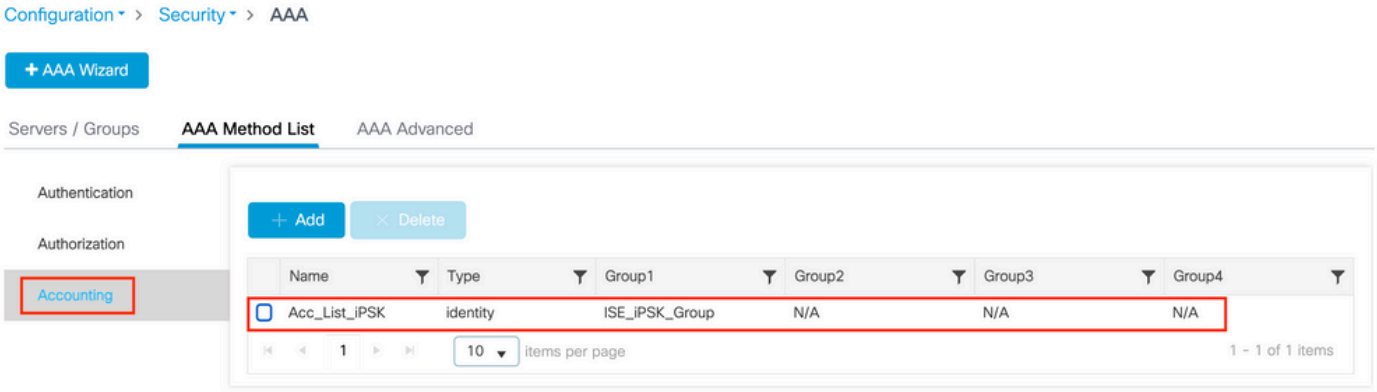
在**Configuration > Security > AAA > Servers/Groups > Server Groups**下，创建RADIUS服务器组并将之前创建的ISE服务器添加到其中：



在**AAA Method List**选项卡中，使用类型“**network**”和组类型“**group**”创建指向以前创建的RADIUS服务器组的**授权列表**：



设置记帐是可选操作，但可以通过将类型配置为“**identity**”并将其指向同一RADIUS服务器组来完成：

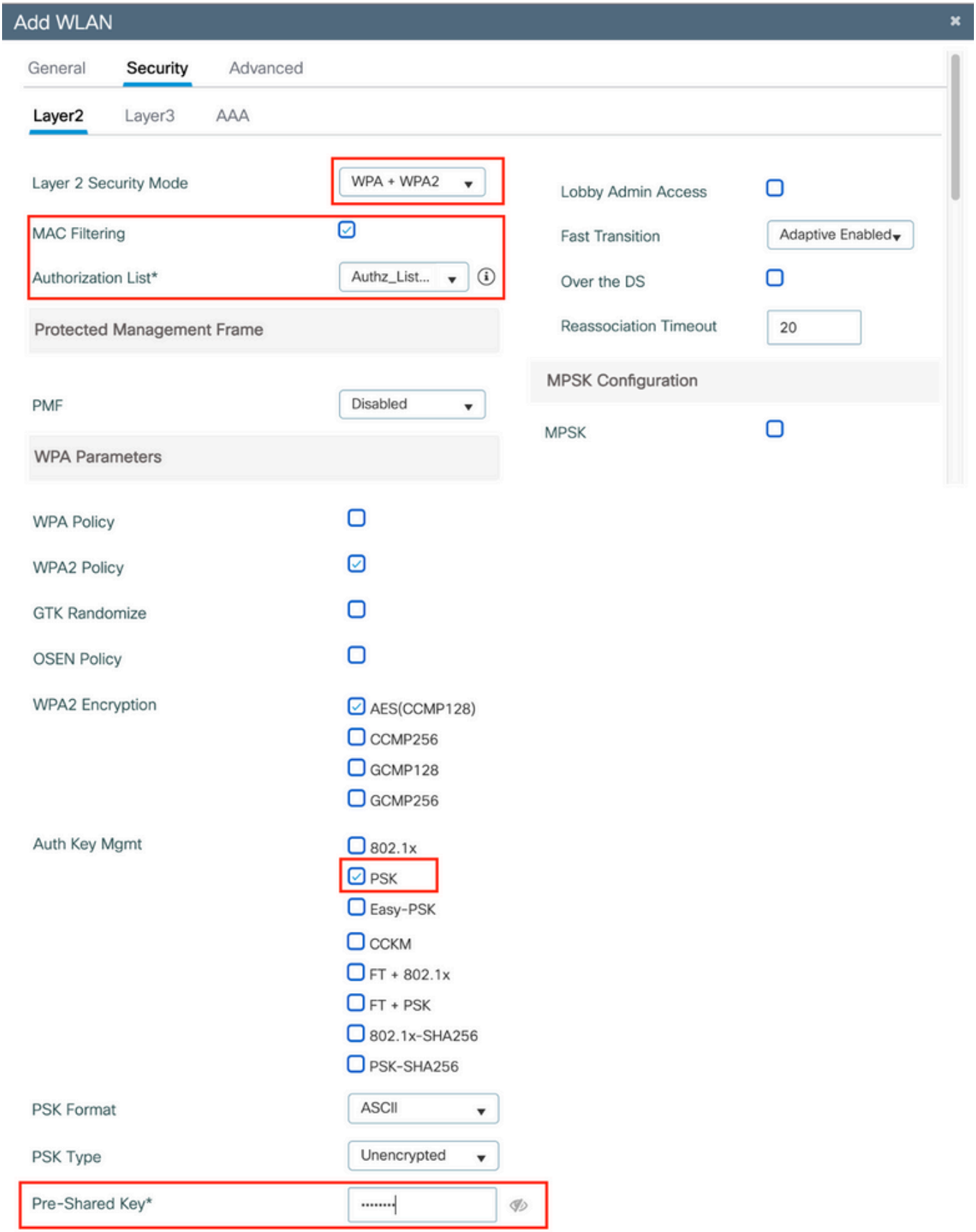


这也可通过命令行使用以下命令执行：

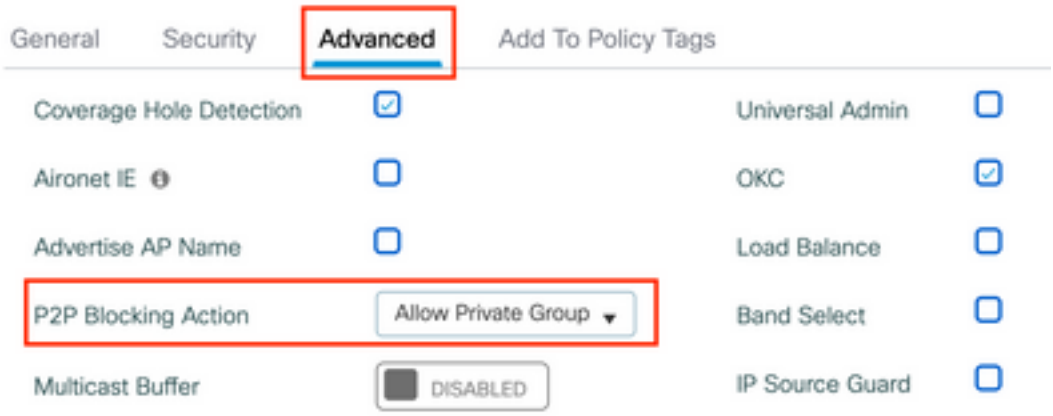
```
radius server
```

在**Configuration > Tags & Profiles > WLANs**下，创建新的WLAN。 在第2层配置下：

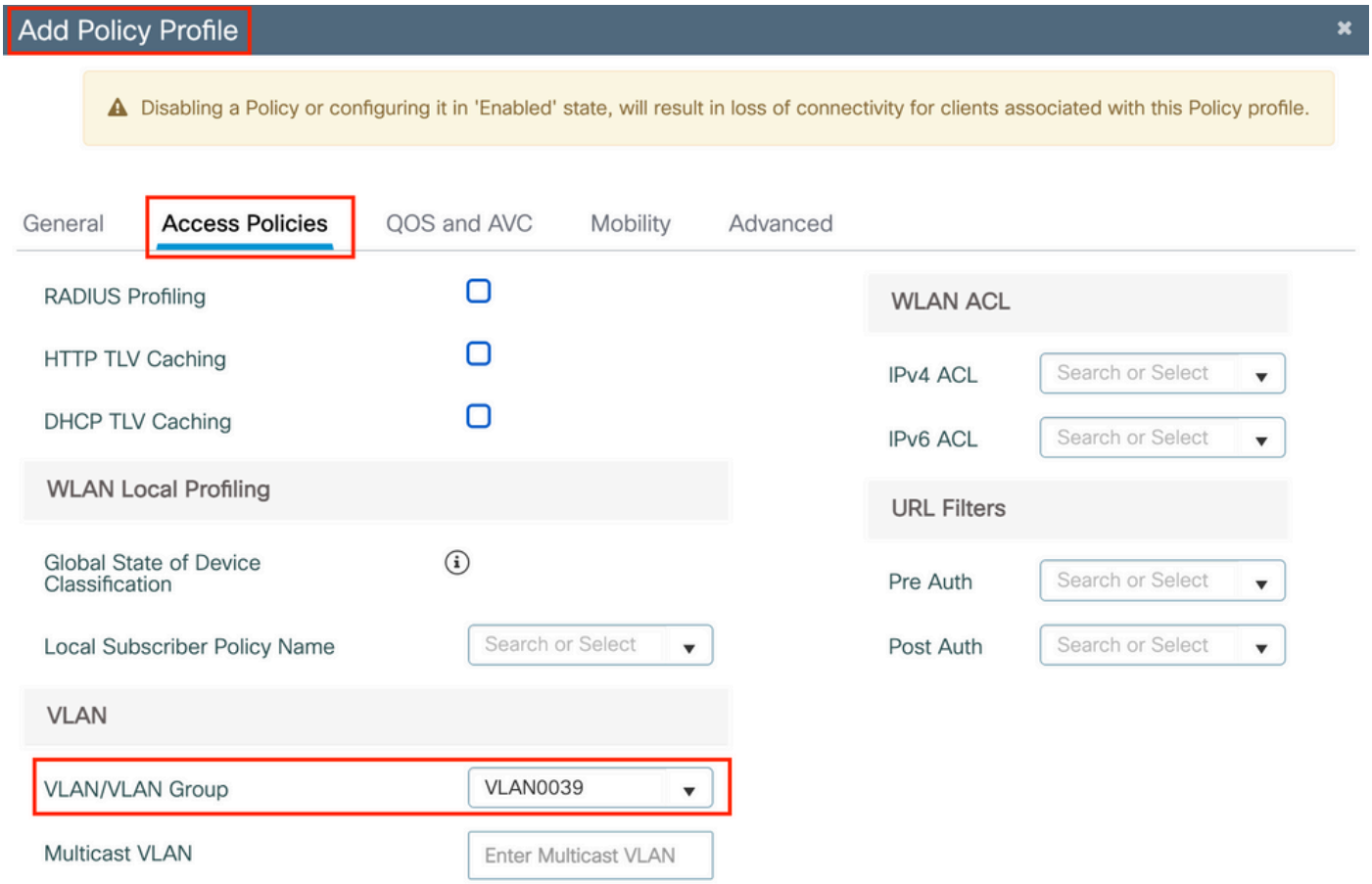
- 启用MAC过滤并将Authorization List（授权列表）设置为之前创建的列表
- 在**Auth Key Mgmt**下启用**PSK**
- 预共享密钥字段可以填充任何值。这样做只是为了满足Web界面设计的要求。没有用户能够使用此密钥进行身份验证。在这种情况下，预共享密钥设置为“12345678”。



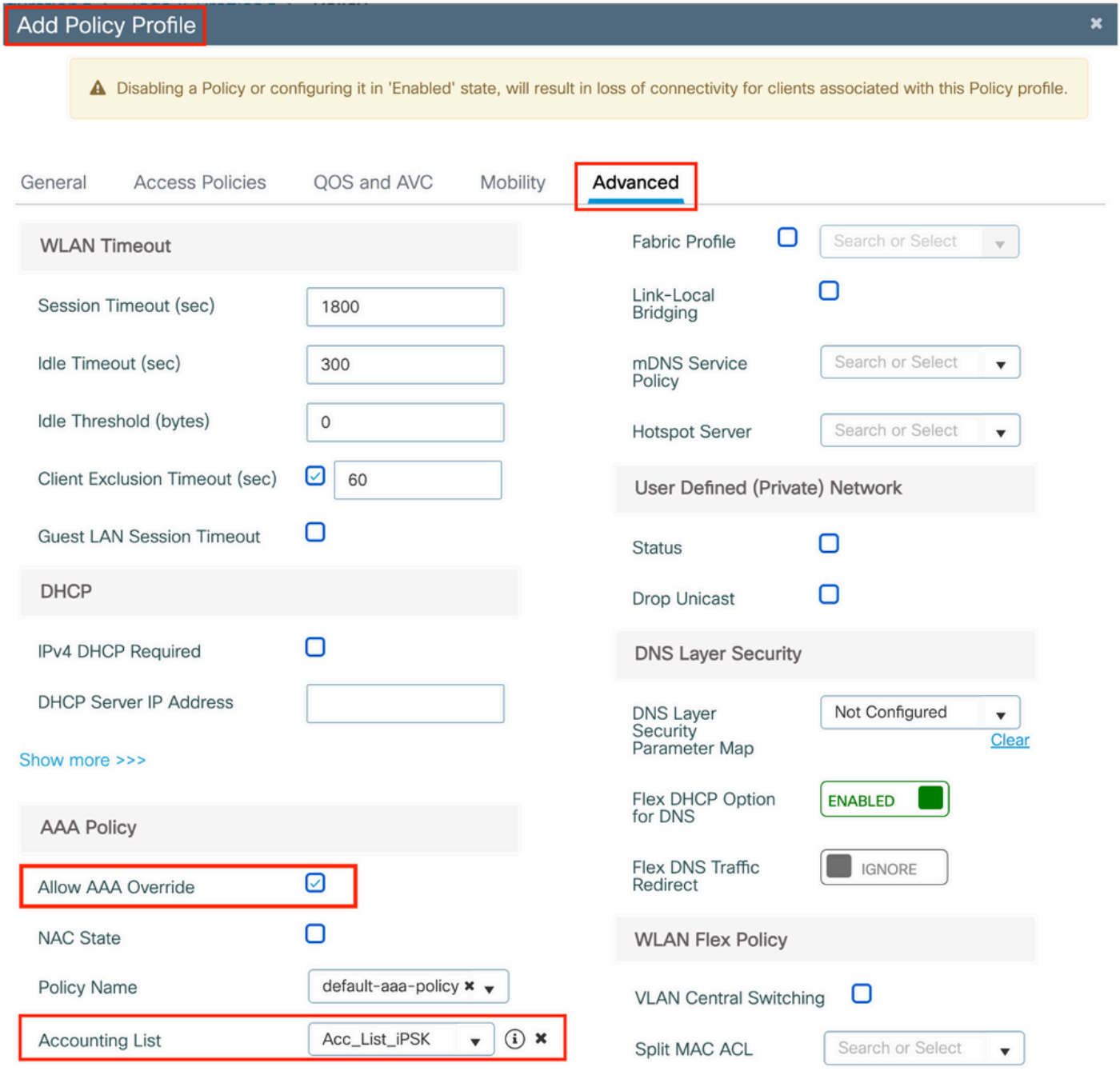
可以在**Advanced**选项卡下实现用户分离。将其设置为Allow Private Group后，使用相同PSK的用户可以相互通信，而使用不同PSK的用户将被阻止：



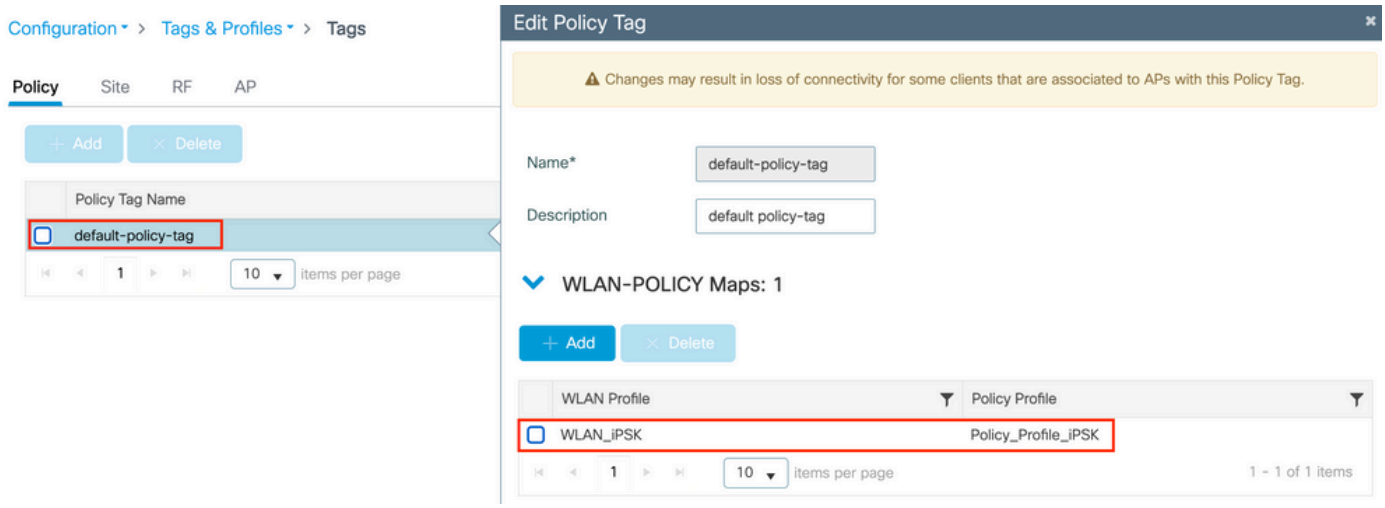
在**Configuration > Tags & Profiles > Policy**下，创建新的策略配置文件。在**访问策略**选项卡中，设置此WLAN正在使用的VLAN或VLAN组：



在**Advanced**选项卡中，启用AAA Override并添加Accounting列表（如果之前已创建）：



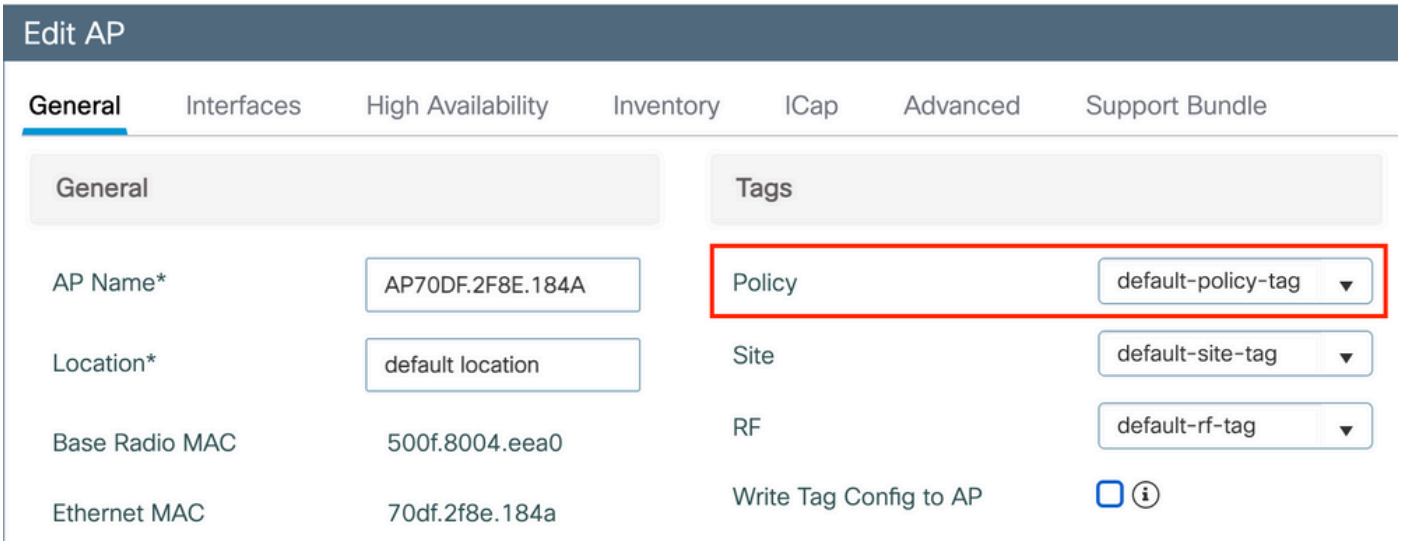
在**Configuration > Tags & Profiles > Tags > Policy**下，确保WLAN映射到您创建的策略配置文件：



这也可通过命令行使用以下命令执行：

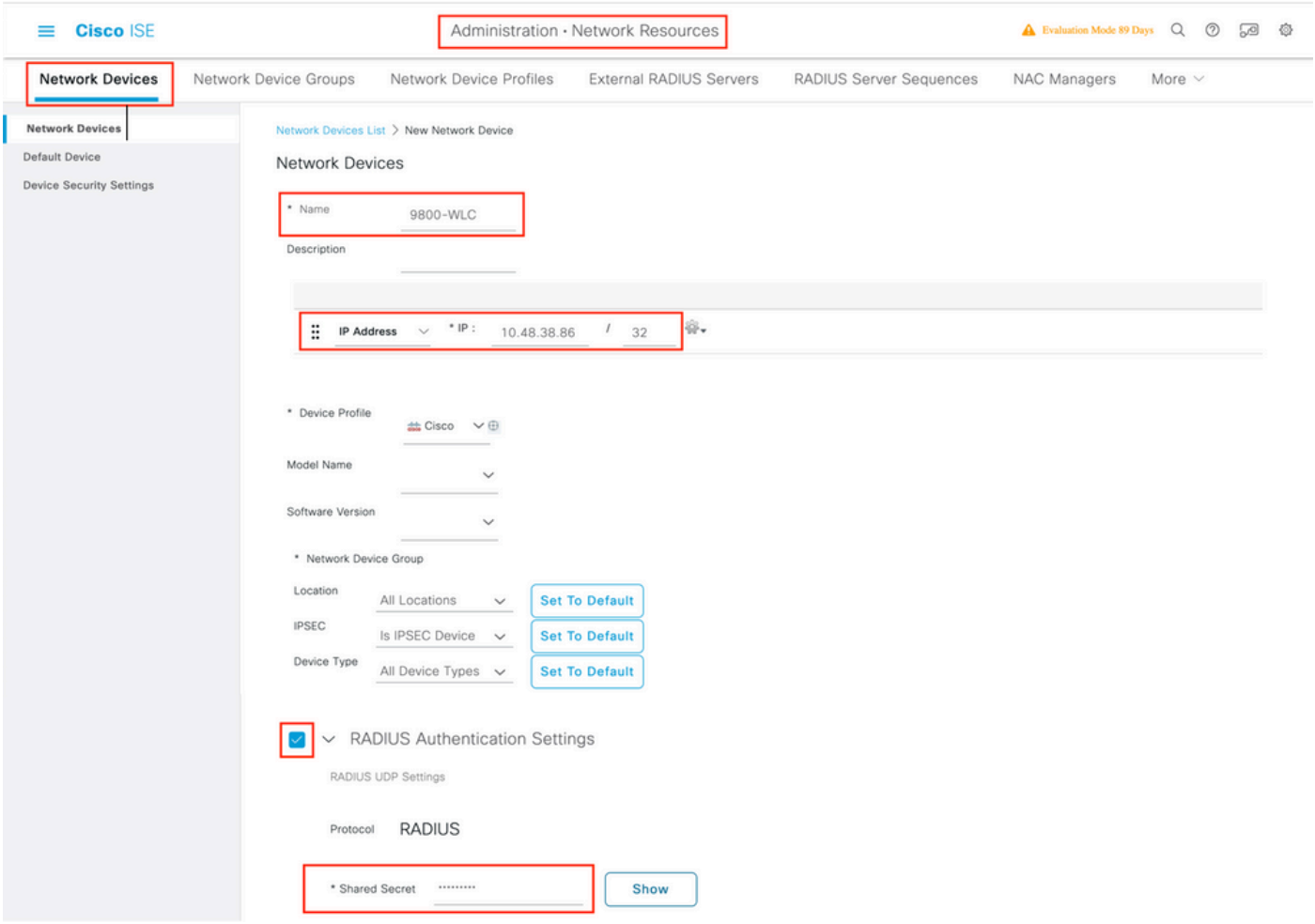
```
wlan
```

在**Configuration > Wireless > Access Points**下，确保此标记已应用于必须在其上广播WLAN的接入点：

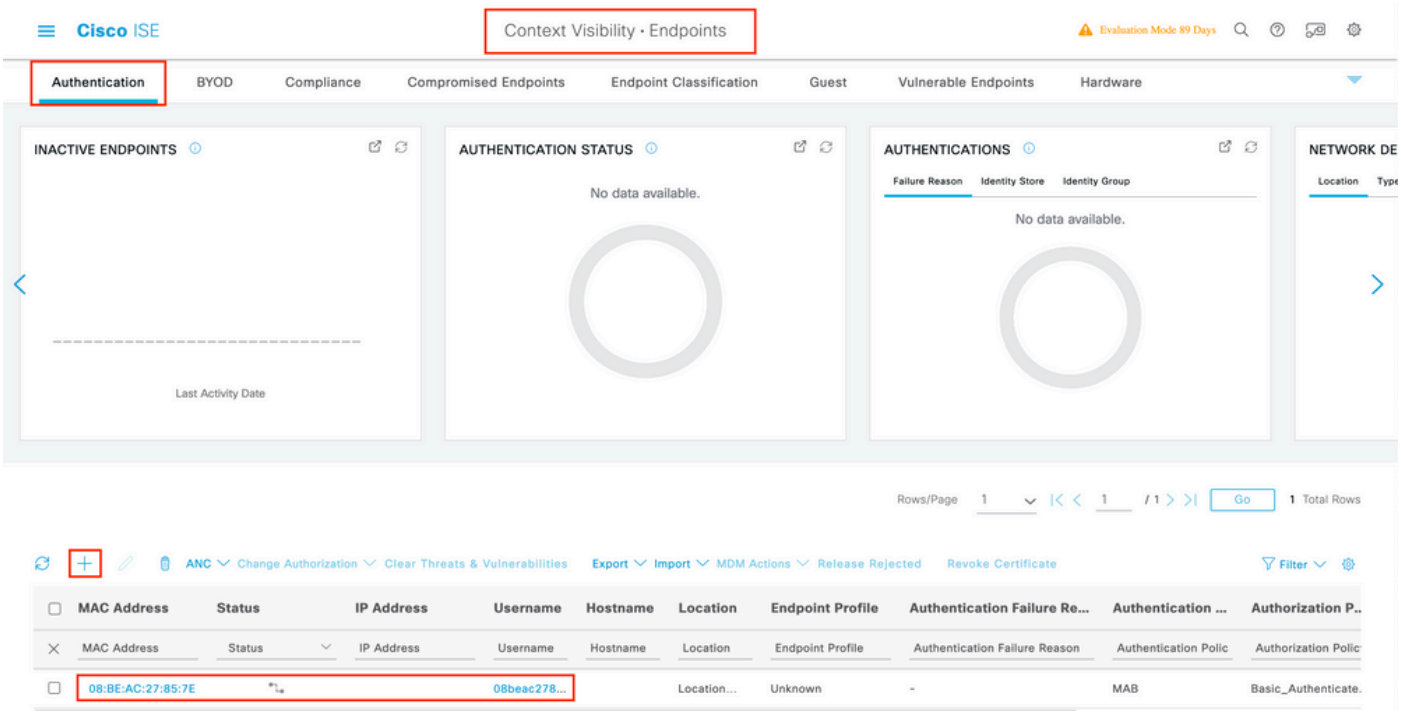


ISE 配置

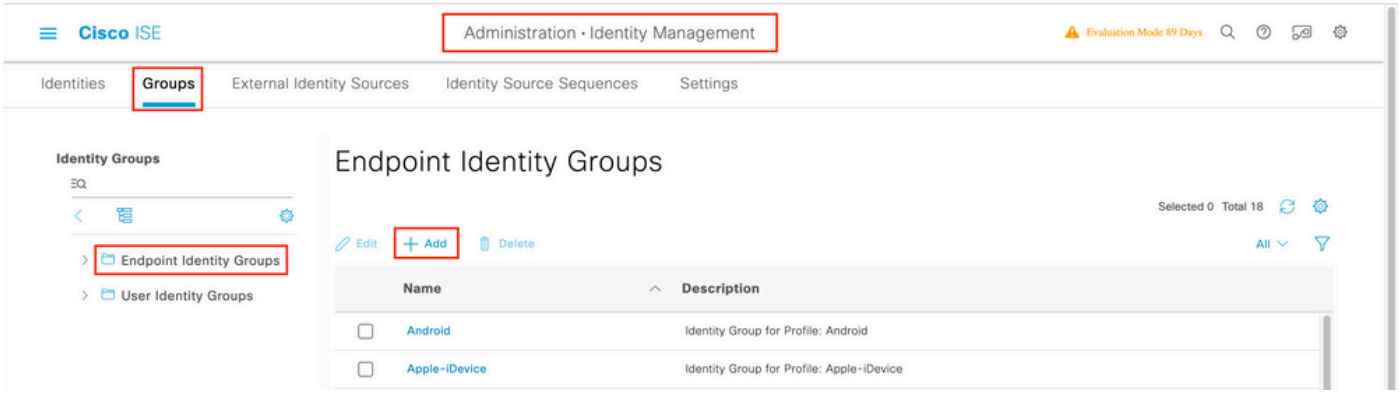
本配置指南介绍根据客户端MAC地址确定设备PSK的场景。在**管理 > 网络资源 > 网络设备**下，添加一个新设备，指定IP地址，启用RADIUS身份验证设置并指定RADIUS共享密钥：

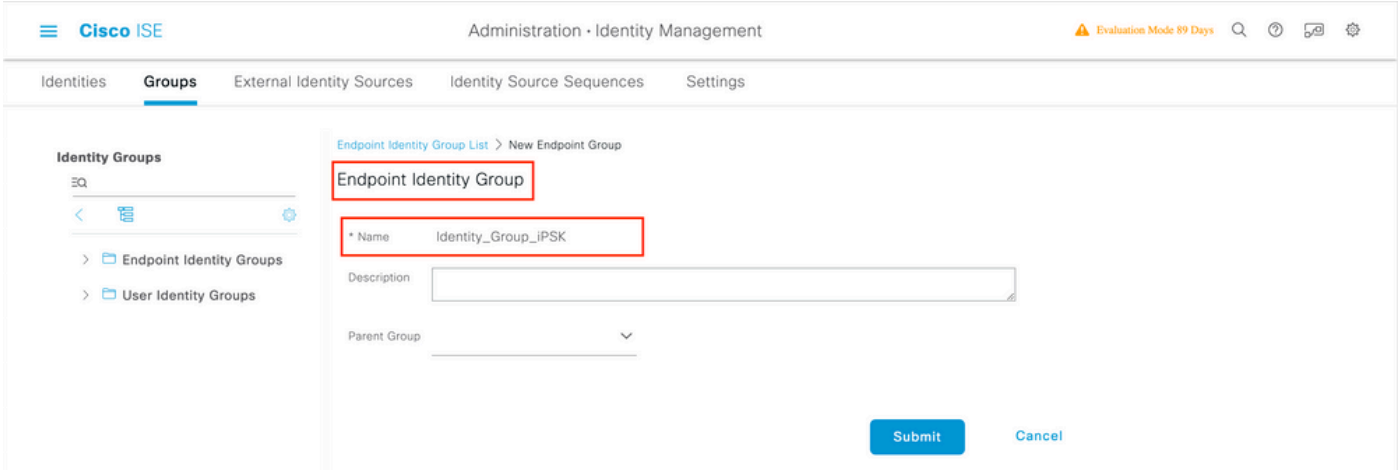


在**Context Visibility > Endpoints > Authentication**下，添加连接到iPSK网络的所有设备（客户端）的MAC地址：

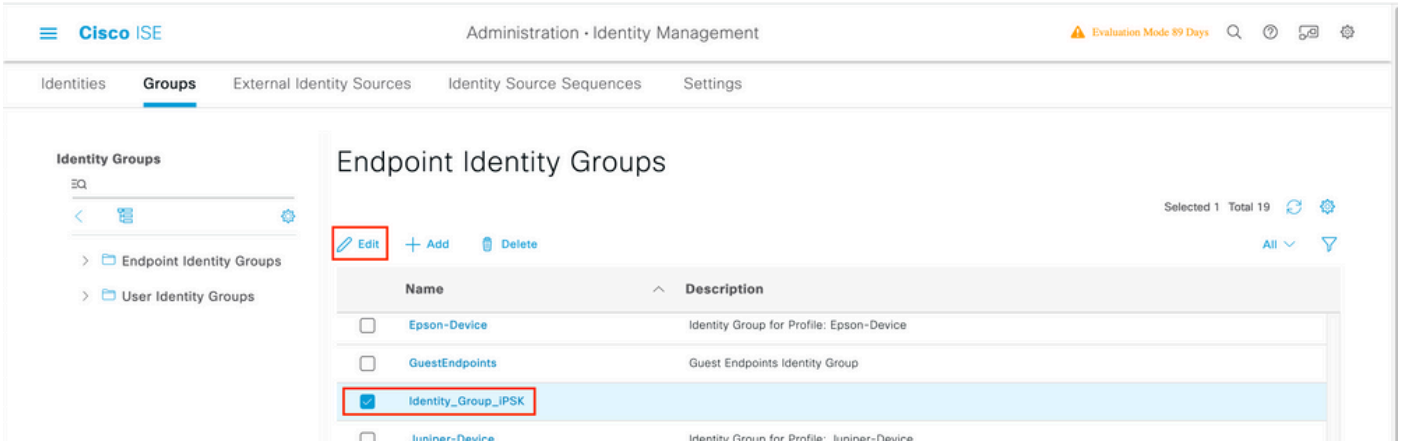


在**Administration > Identity Management** > Groups > **Endpoint Identity Groups**下，创建一个或多个组并向它们分配用户。以后可以将每个组配置为使用不同的PSK连接到网络。

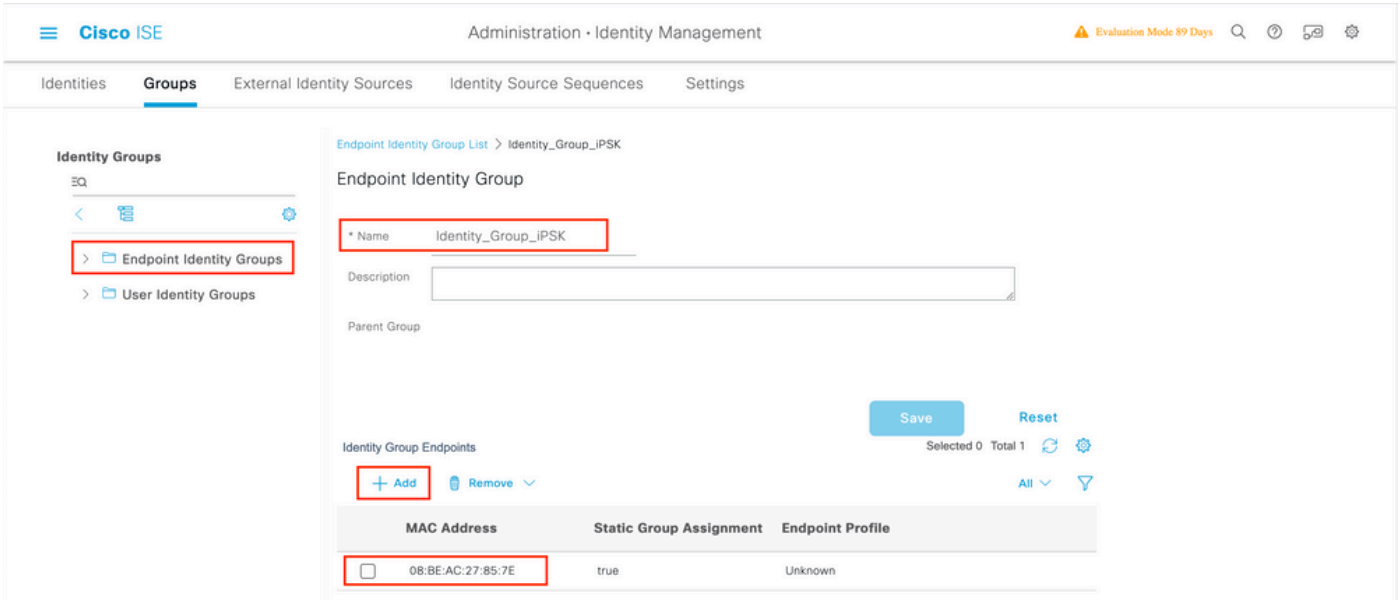




创建组后，即可将用户分配给它们。选择您创建的组，然后单击“编辑”：



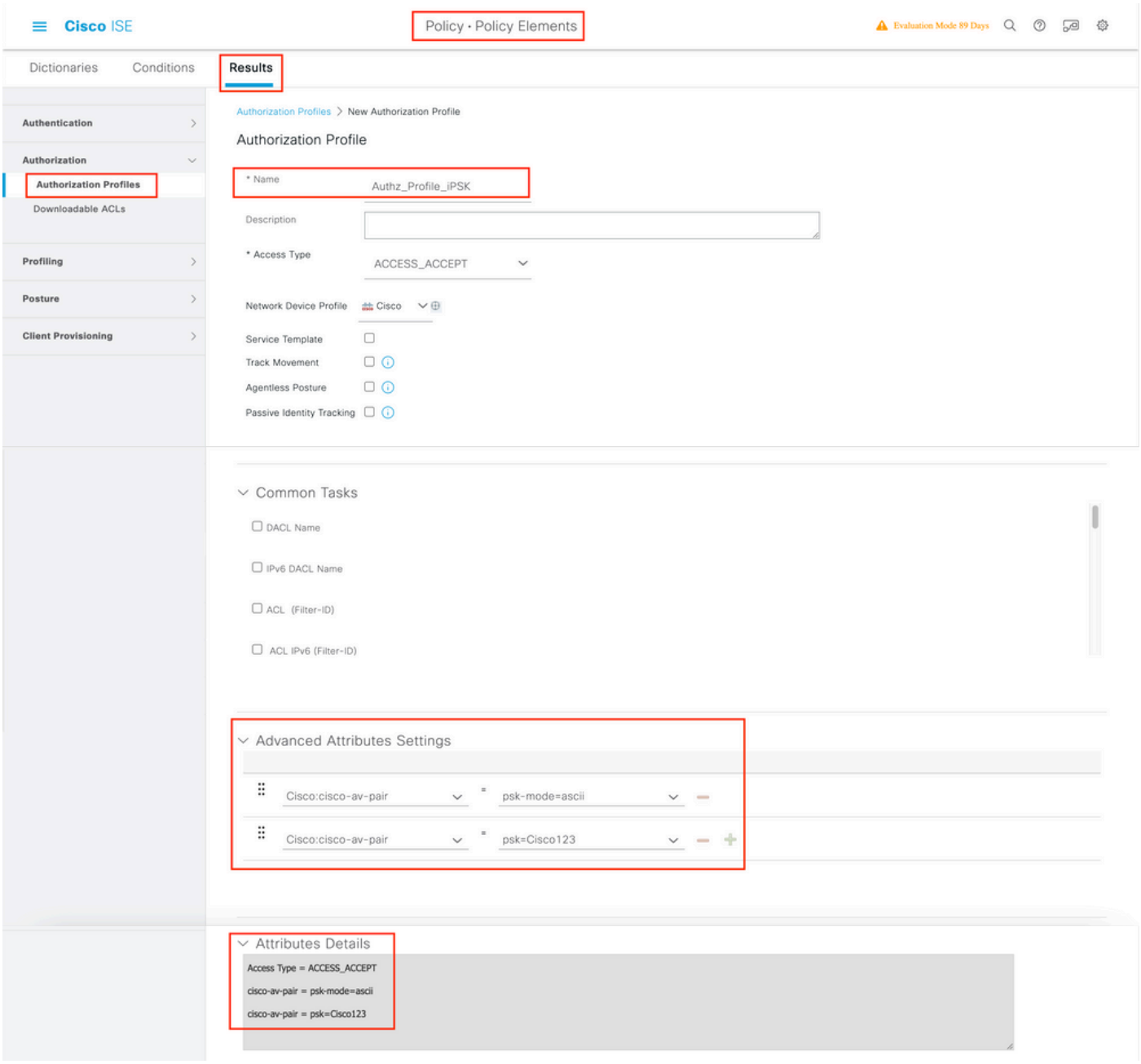
在组配置中，通过点击“添加”按钮添加要分配给该组的客户端的MAC地址：



在Policy > **Policy Elements > Results > Authorization > Authorization Profiles**下，创建新的授权配置文件。将属性设置为：

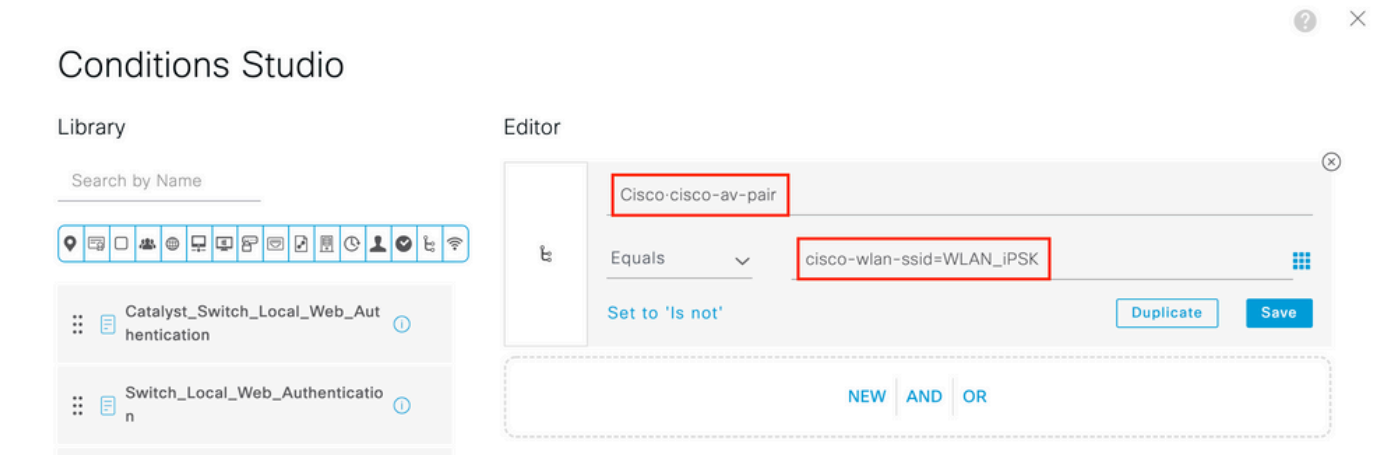
```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

对于必须使用不同PSK的每个用户组，请使用不同的psk av-pair创建附加结果。此处还可以配置ACL和VLAN覆盖等其他参数。

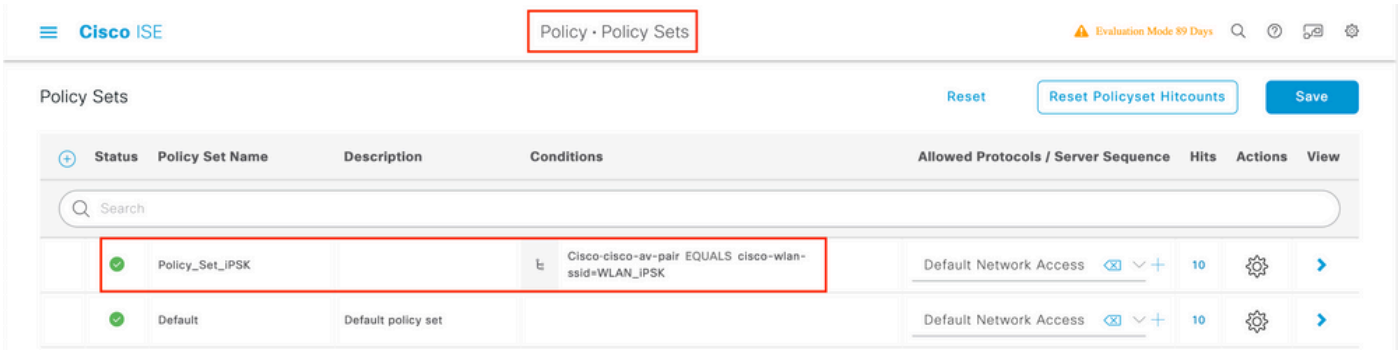


在**Policy > Policy Sets**下，创建一个新策略。要确保客户端与策略集匹配，请使用以下条件：

```
Cisco:cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_iPSK    // "WLAN_iPSK" is WLAN name
```

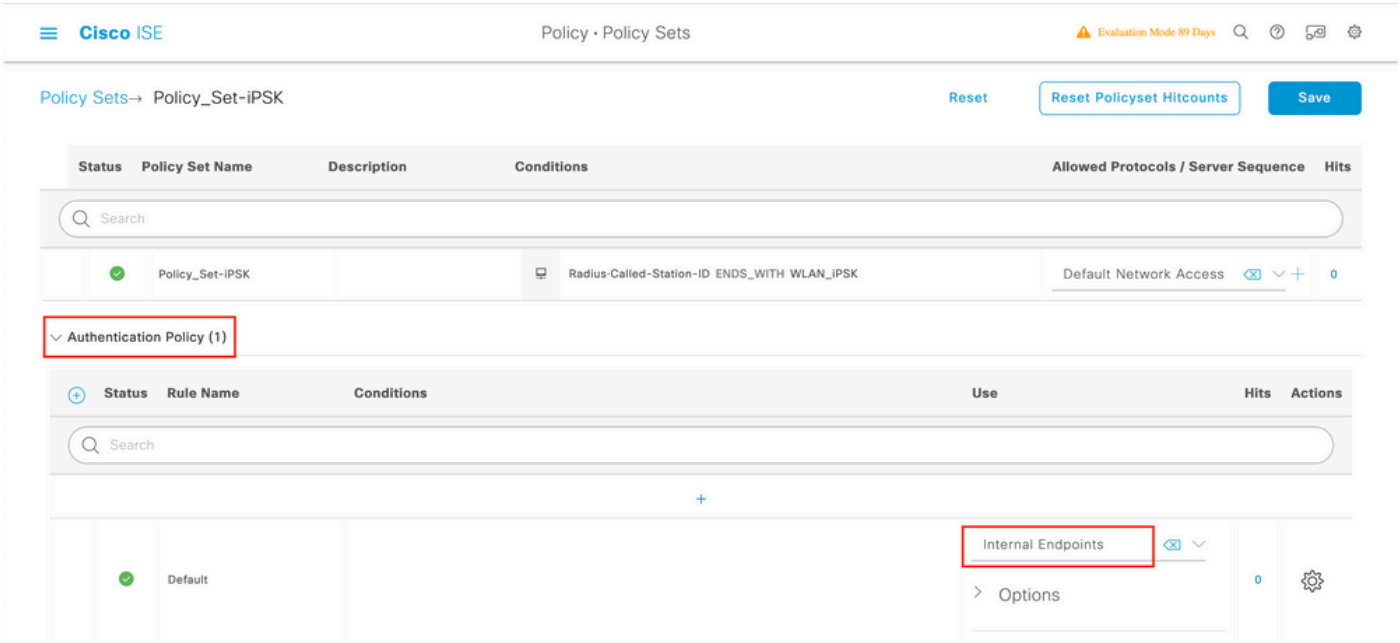


可以添加其他条件以使策略匹配更加安全。



通过点击Policy Set行右侧的蓝色箭头进入新创建的iPSK Policy Set配置：

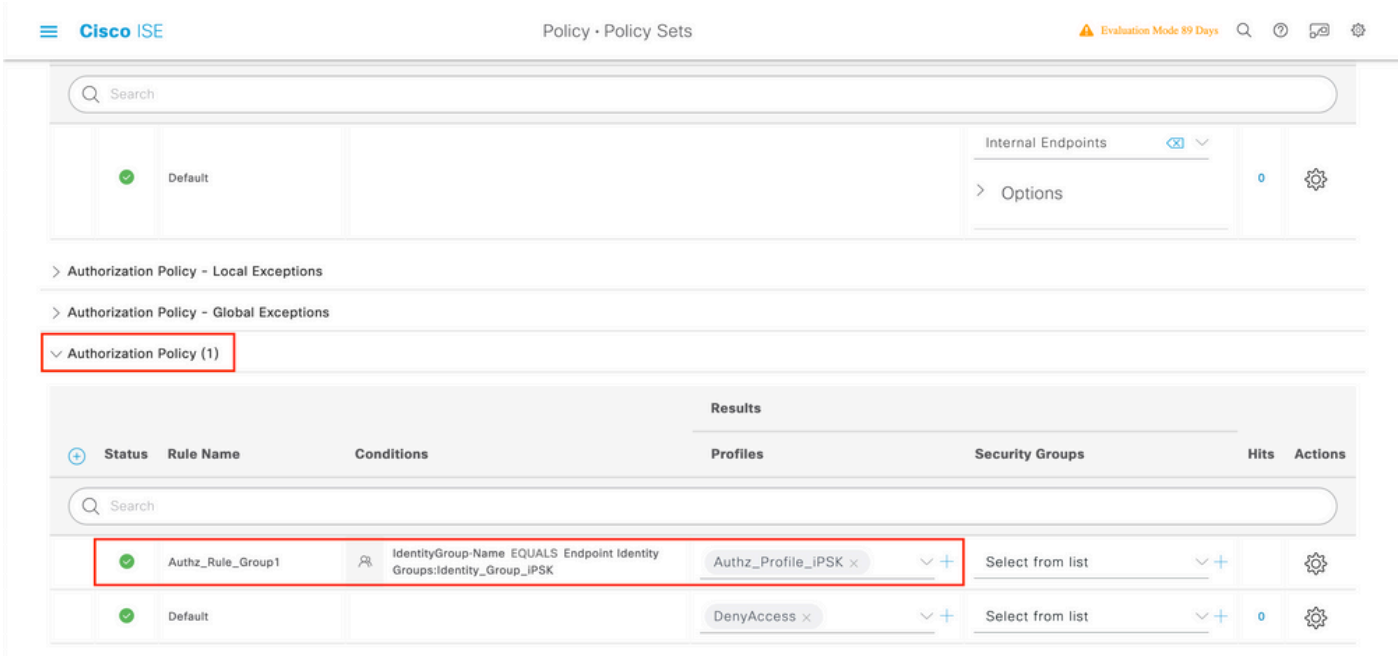
确保将**身份验证策略**设置为“内部终端”：



在**授权策略**下，为每个用户组创建一个新规则。作为条件，请使用：

```
IdentityGroup-Name EQUALS Endpoint Identity Group:Identity_Group_iPSK      //
"Identity_Group_iPSK" is name of the created endpoint group
```

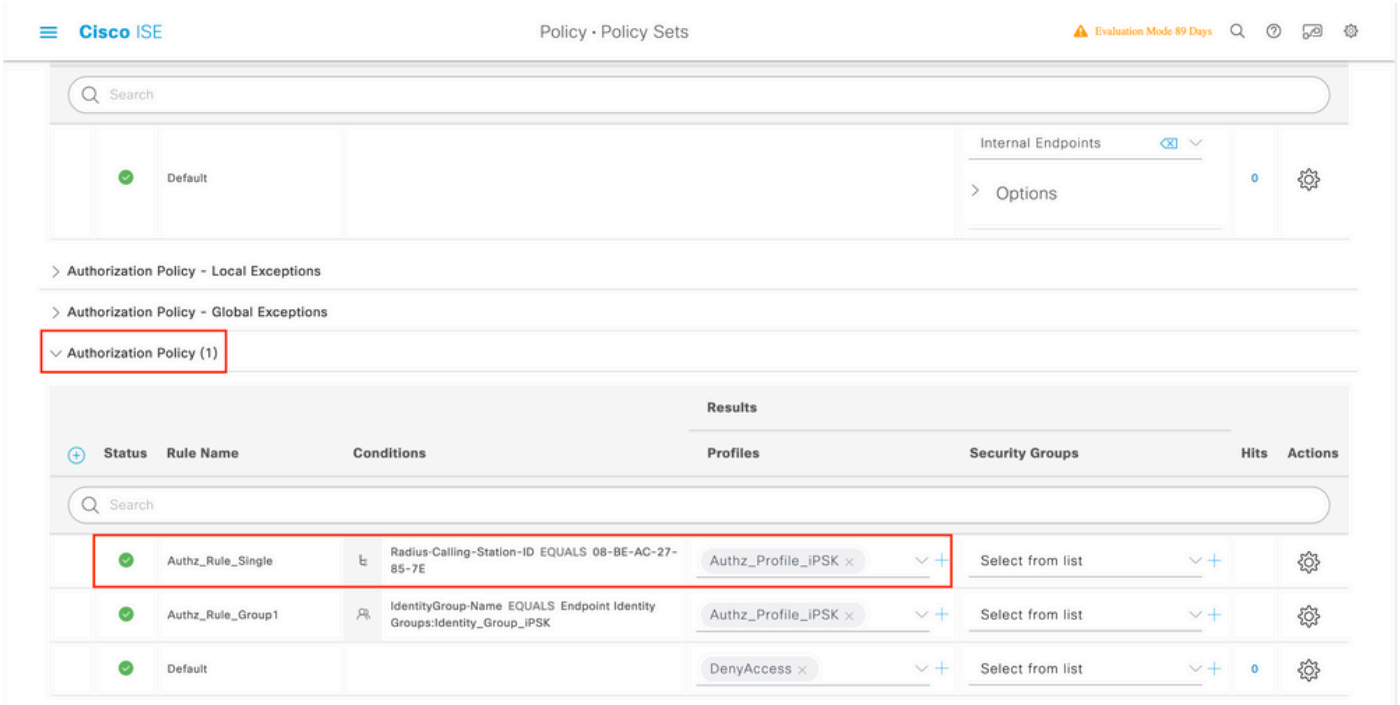
结果是之前创建的**授权配置文件**。确保Default规则位于底部并指向DenyAccess。



如果每个用户将拥有不同的密码，而不是创建与该终端组匹配的终端组和规则，则可以创建具有以下条件的规则：

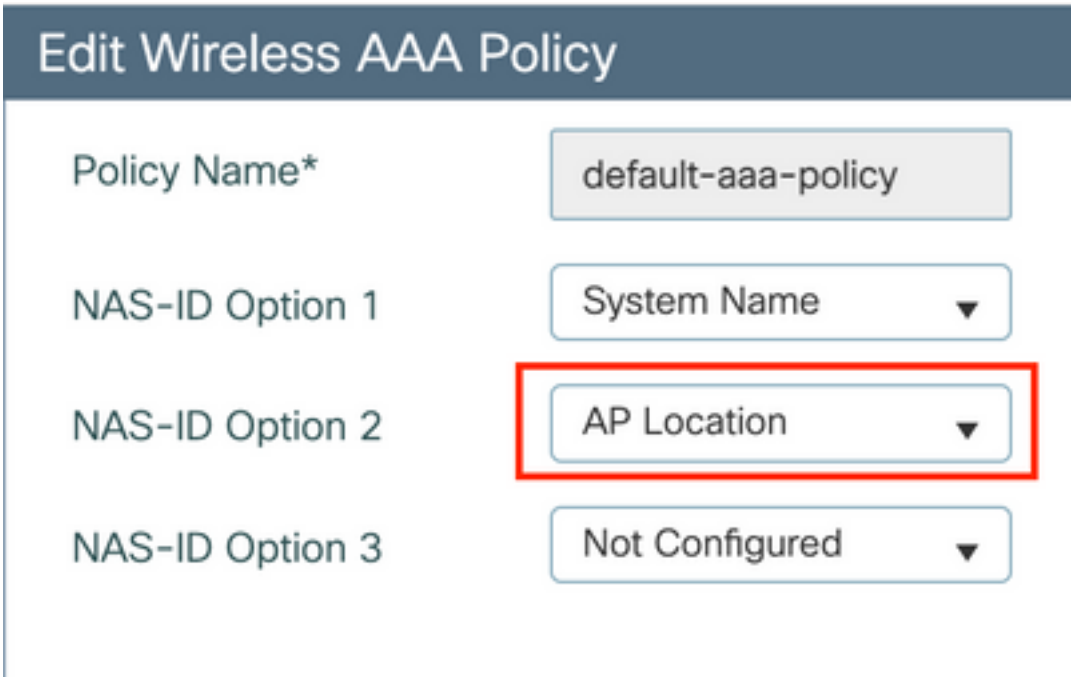
```
Radius-Calling-Station-ID EQUALS <client_mac_addr>
```

注意： MAC地址分隔符可以在WLC上的**AAA > AAA Advanced > Global Config > Advanced Settings下配置**。在本示例中，使用了字符“ — ”。



授权策略的规则允许使用许多其他参数来指定用户正在使用的密码。一些最常用的规则是：

1. **根据用户位置进行匹配**
   在这种情况下，WLC需要将AP位置信息发送到ISE。这允许一个位置的用户使用一个密码，而另一个位置的用户使用不同的密码。可以在**Configuration > Security > Wireless AAA Policy**下配置此项



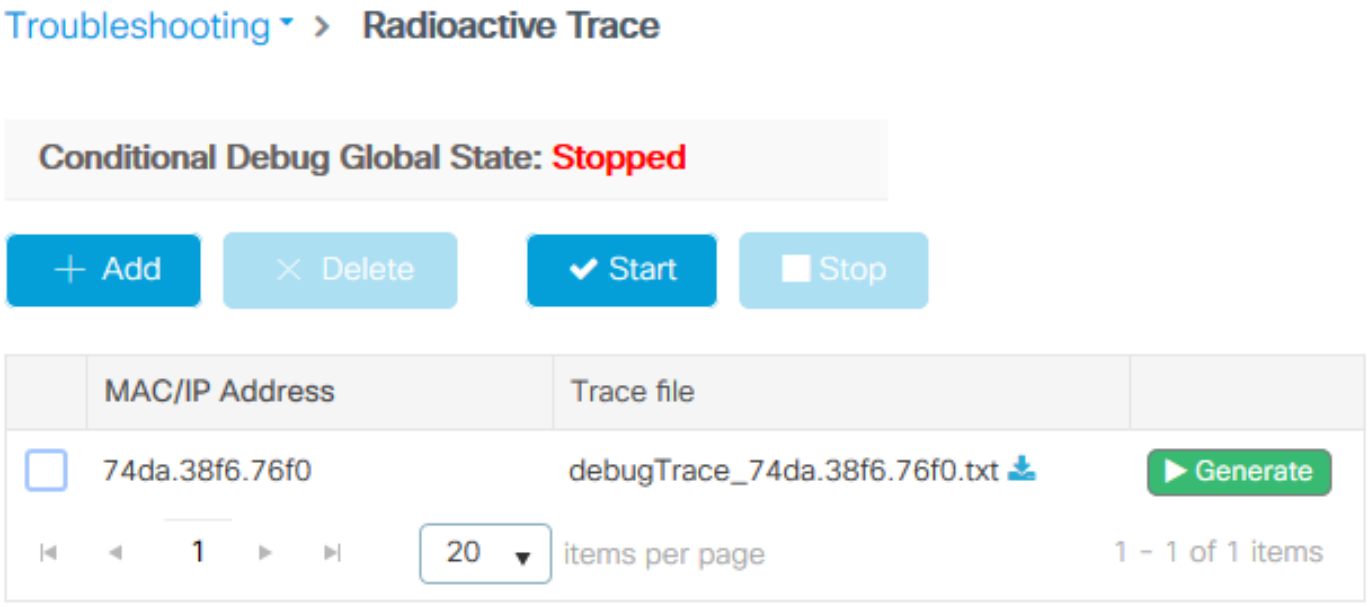
2. **根据设备分析进行匹配**
   在这种情况下，需要配置WLC以全局配置设备。这样，管理员可以为笔记本电脑和电话设备配置不同的密码。全局设备分类可在**Configuration > Wireless > Wireless Global**下启用。有关ISE上的设备分析配置，请参阅ISE分析设计指南。

除了返回加密密钥外，由于此授权发生在802.11关联阶段，因此完全可以从ISE返回其他AAA属性，例如ACL或VLAN id。

故障排除

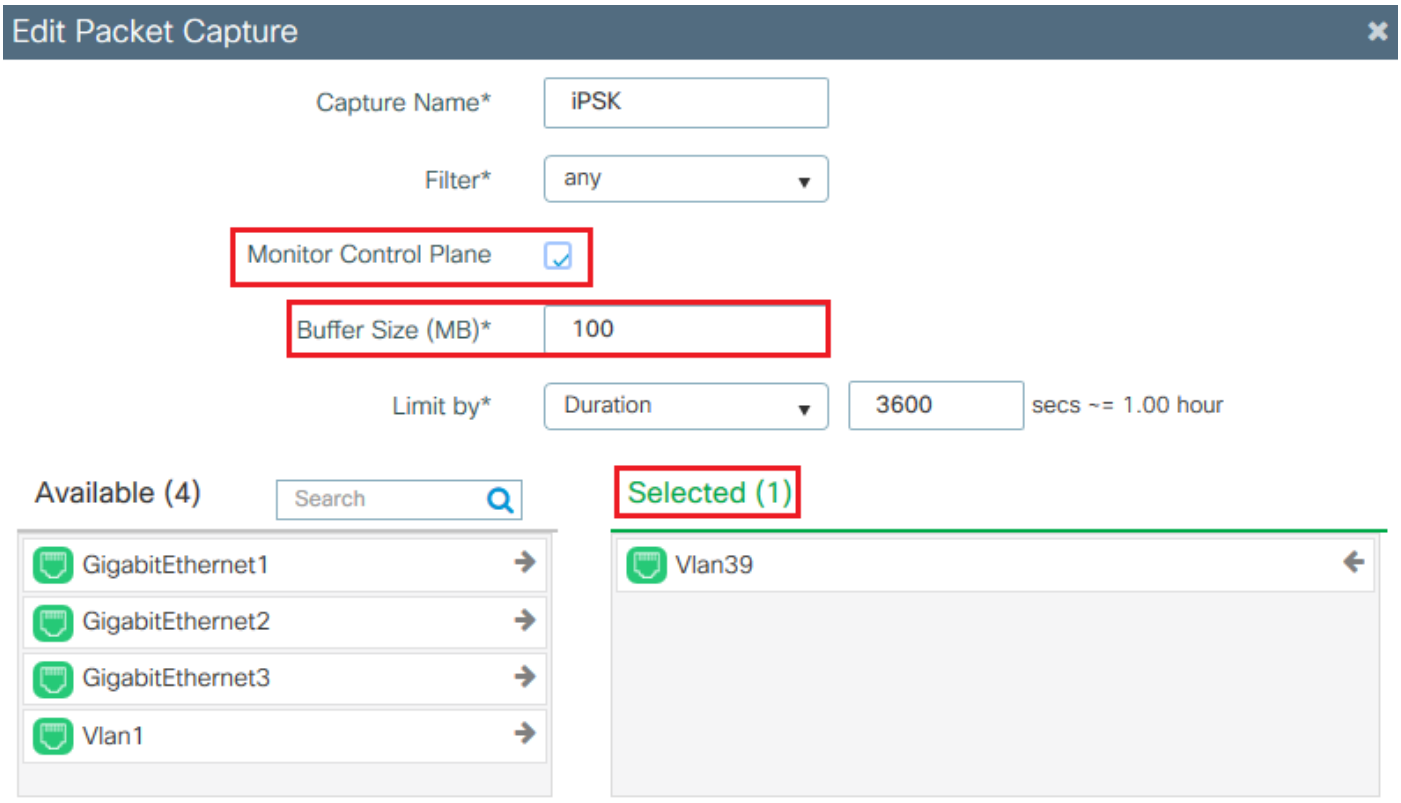
9800 WLC故障排除

在WLC上，收集放射性痕迹必须足以识别大多数问题。这可以在WLC Web界面的**故障排除 > 放射跟踪**下完成。添加客户端MAC地址，按**开始**并尝试重现问题。 单击**Generate**创建并下载文件：

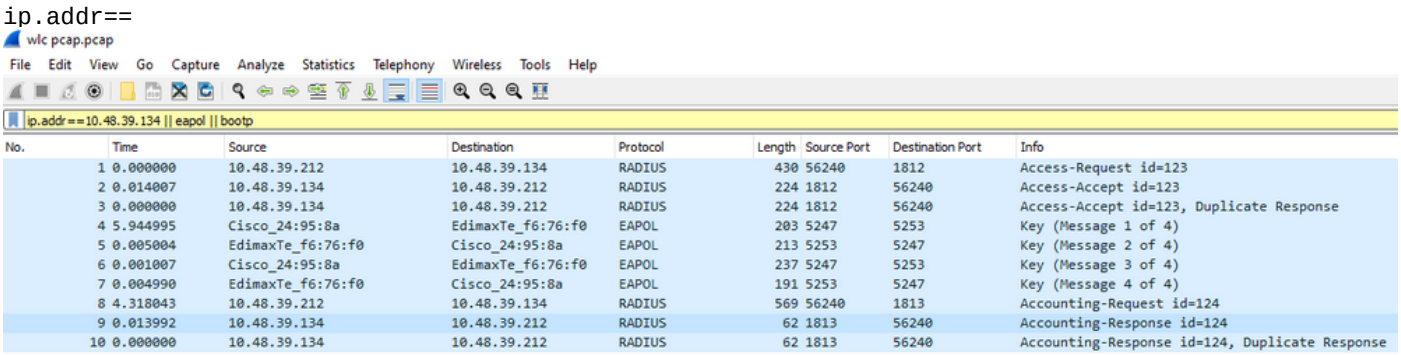


重要:IOS 14和Android 10智能手机上的iPhone在关联网络时使用随机mac地址。此功能可能会完全中断iPSK配置。确保禁用此功能！

如果放射性跟踪不足以识别问题，则可以直接在WLC上收集数据包捕获。在**Troubleshooting > Packet Capture**下，添加捕获点。默认情况下，WLC使用无线管理接口进行所有RADIUS AAA通信。如果WLC有大量客户端，请将缓冲区大小增加到100 MB:

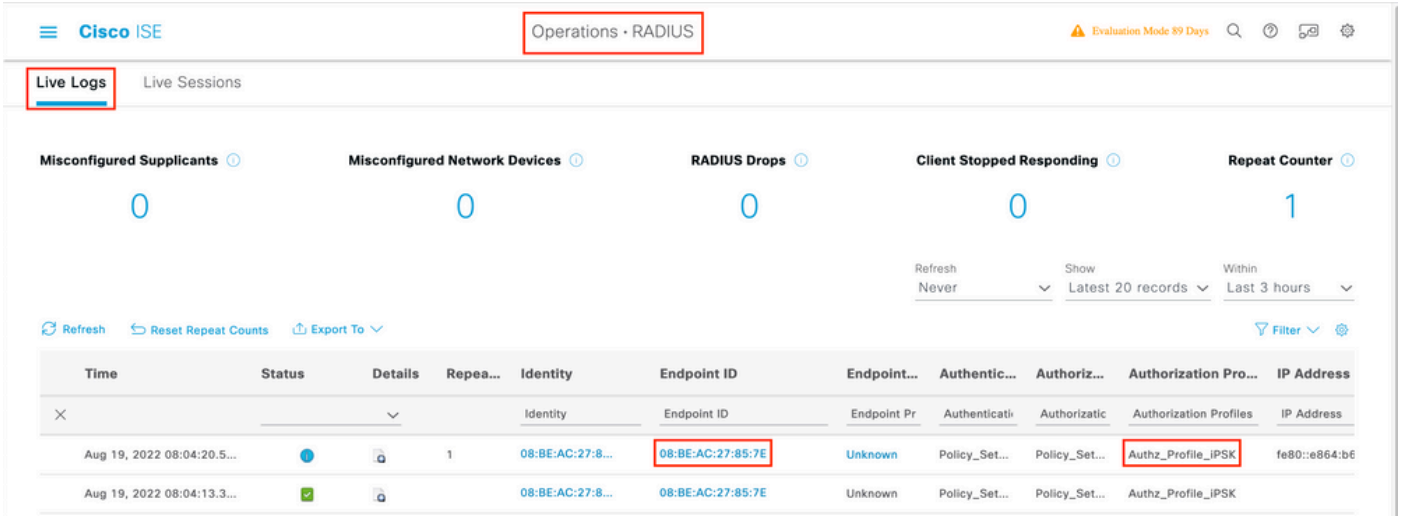


成功进行身份验证和记帐尝试的数据包捕获如下图所示。使用此Wireshark过滤器可过滤出此客户端的所有相关数据包：



排除ISE故障

思科ISE的主要故障排除技术是**实时日志**页面，位于**操作 > RADIUS > 实时日志**下。可以通过将客户端的MAC地址放在Endpoint ID字段中来过滤这些地址。 打开完整的ISE报告可提供有关故障原因的更多详细信息。确保客户端符合正确的ISE策略：


Cisco ISE
Operations · RADIUS
Evaluation Mode 89 Days
Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Repeat Counter
1
Refresh
Never
Show
Latest 20 records
Within
Last 3 hours
Refresh
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repea...
Identity
Endpoint ID
Endpoint...
Authentic...
Authoriz...
Authorization Pro...
IP Address
Identity
Endpoint ID
Endpoint Pr
Authenticati
Authorizatic
Authorization Profiles
IP Address
Aug 19, 2022 08:04:20.5...
1
08:BE:AC:27:8...
08:BE:AC:27:85:7E
Unknown
Policy_Set...
Policy_Set...
Authz_Profile_iPSK
fe80::e864:b6
Aug 19, 2022 08:04:13.3...
08:BE:AC:27:8...
08:BE:AC:27:85:7E
Unknown
Policy_Set...
Policy_Set...
Authz_Profile_iPSK

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）。