配置Catalyst 9800无线控制器AP授权列表

目录

简介

本文档介绍如何配置Catalyst 9800无线LAN控制器接入点(AP)身份验证策略。

背景信息

要授权接入点(AP)，需要根据具有9800无线局域网控制器的本地数据库或外部远程身份验证拨入用户服务(RADIUS)服务器来授权AP的以太网MAC地址。

此功能可确保只有经过授权的接入点(AP)才能加入Catalyst 9800无线LAN控制器。本文档不介绍网状（1500系列）AP的情况，这些无线接入点需要mac过滤器条目才能加入控制器，但不会跟踪典型的AP授权流程（请参阅参考资料）。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800 WLC
- 无线控制器的命令行界面(CLI)访问

使用的组件

9800 WLC v16.12

AP 1810W

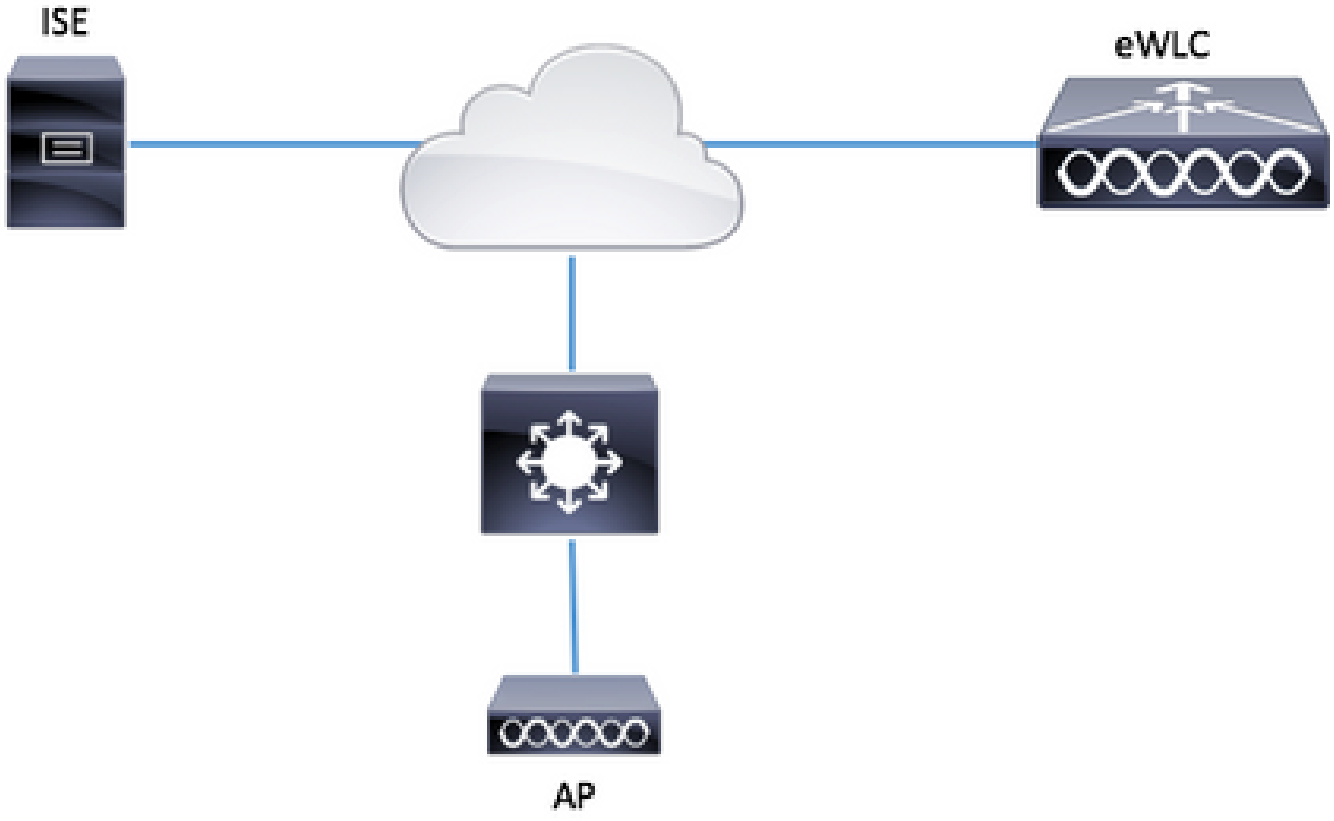
AP 1700

身份服务引擎(ISE)v2.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



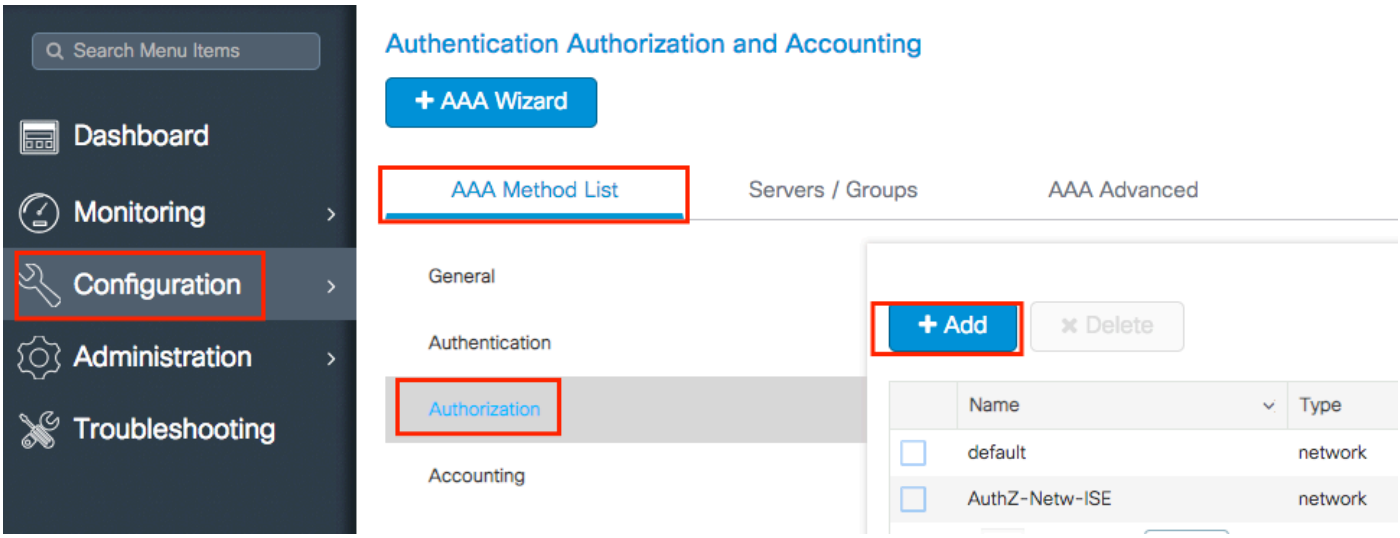
配置

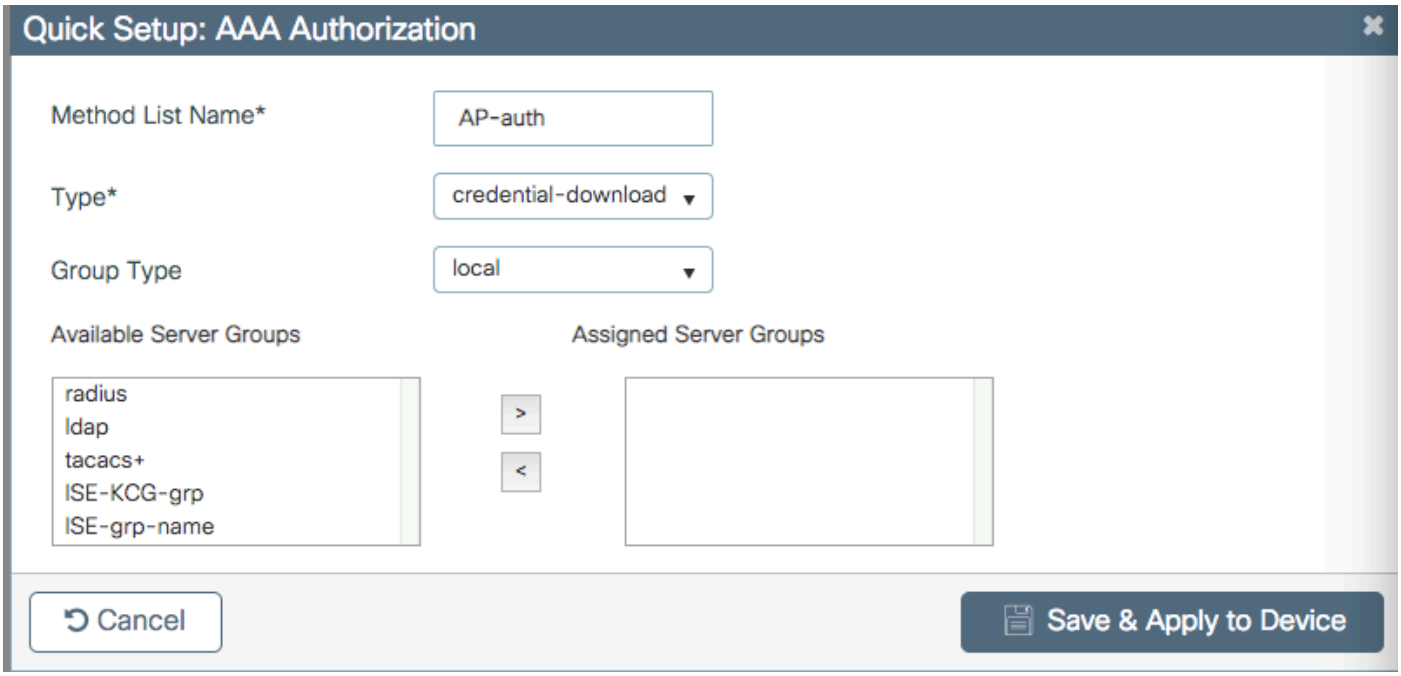
MAC AP授权列表 — 本地

授权AP的MAC地址存储在9800 WLC本地。

步骤1:创建本地授权凭证下载方法列表。

导航到配置>安全> AAA > AAA方法列表>授权> + Add



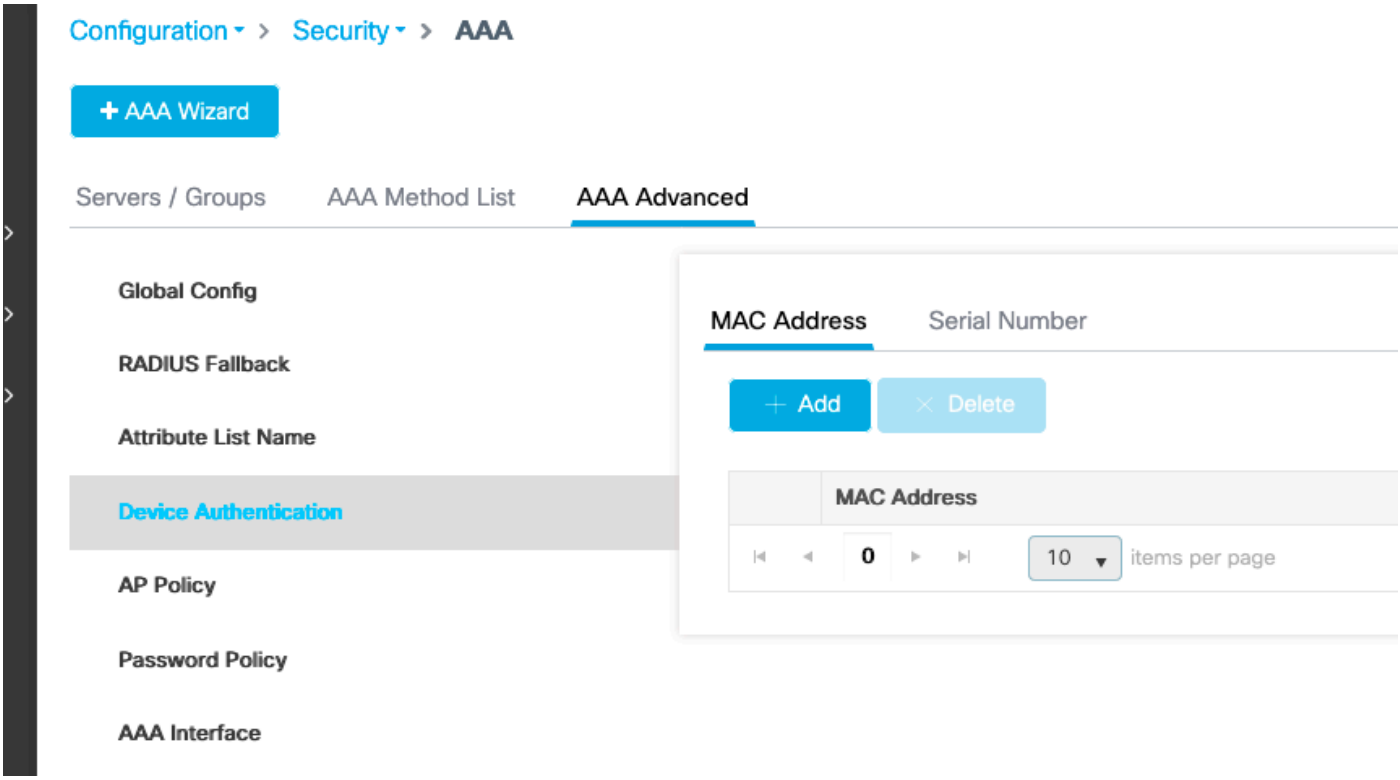


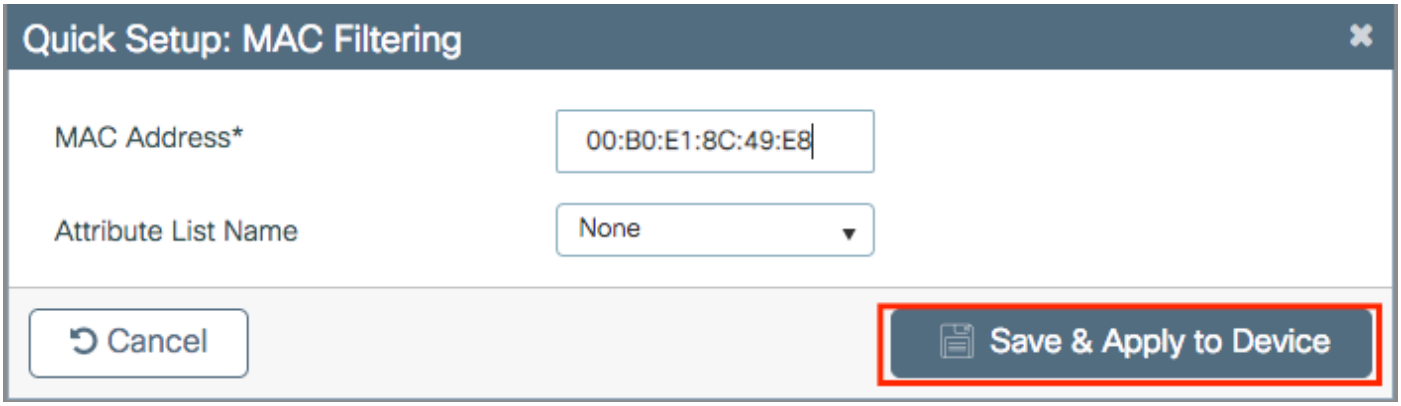
第二步：启用AP MAC授权。

导航至 Configuration > Security > AAA > AAA Advanced > AP Policy。 启用Authorize APs against MAC，并选择第1步中创建的Authorization Method List。

第三步：添加AP以太网mac地址。

导航至 Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add





注意:AP以太网MAC地址必须 在16.12版的Web UI(xx:xx:xx:xx:xx:xx（或）xxxx.xxxx.xxxx（或）xx-xx-xx-xx-xx)中输入以下格式之一。在17.3版中，它们必须是xxxxxxxxxx格式，不带任何分隔符。在任何版本中，CLI格式始终为xxxxxxxxxxx（在16.12中，Web UI会删除配置中的分隔符）。Cisco Bug ID CSCvv43870允许在CLI或Web UI的较新版本中使用任何格式。

CLI：

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local
```

```
# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

MAC AP授权列表 — 外部RADIUS服务器

9800 WLC配置

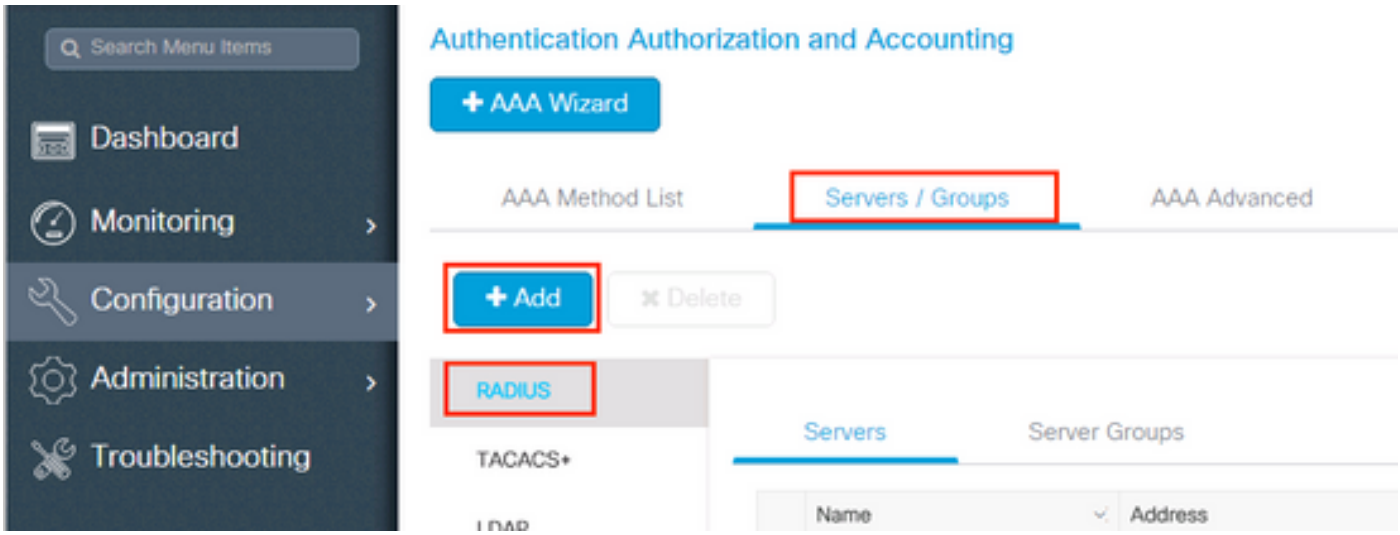
授权AP的MAC地址存储在外部RADIUS服务器（在本例中为ISE）上。

在ISE上，您可以将AP的MAC地址注册为用户名/密码或终端。在步骤中，系统会指导您选择使用其中一种方法。

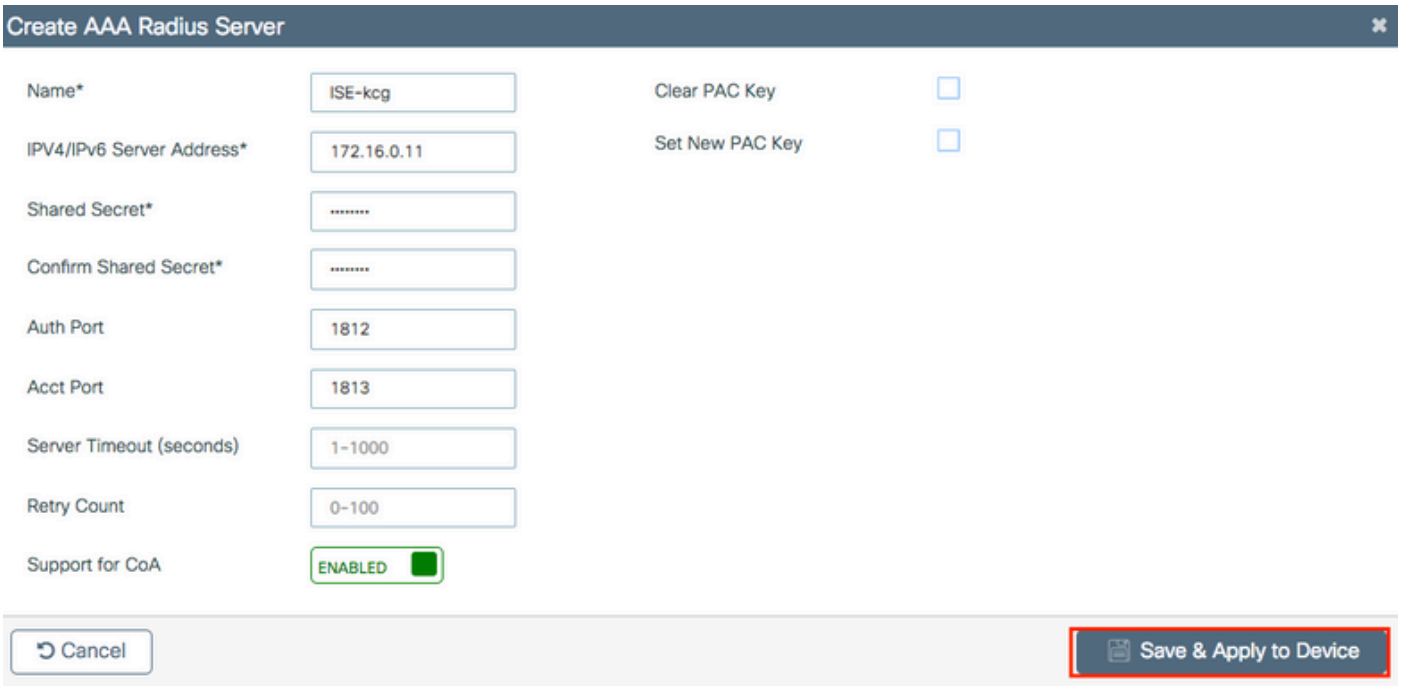
GUI:

步骤1:声明RADIUS服务器

导航到Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add并输入RADIUS服务器信息。



如果您计划将来使用中央 Web 身份验证（或任何一种需要 CoA 的安全措施），请确保已启用对 CoA 的支持。

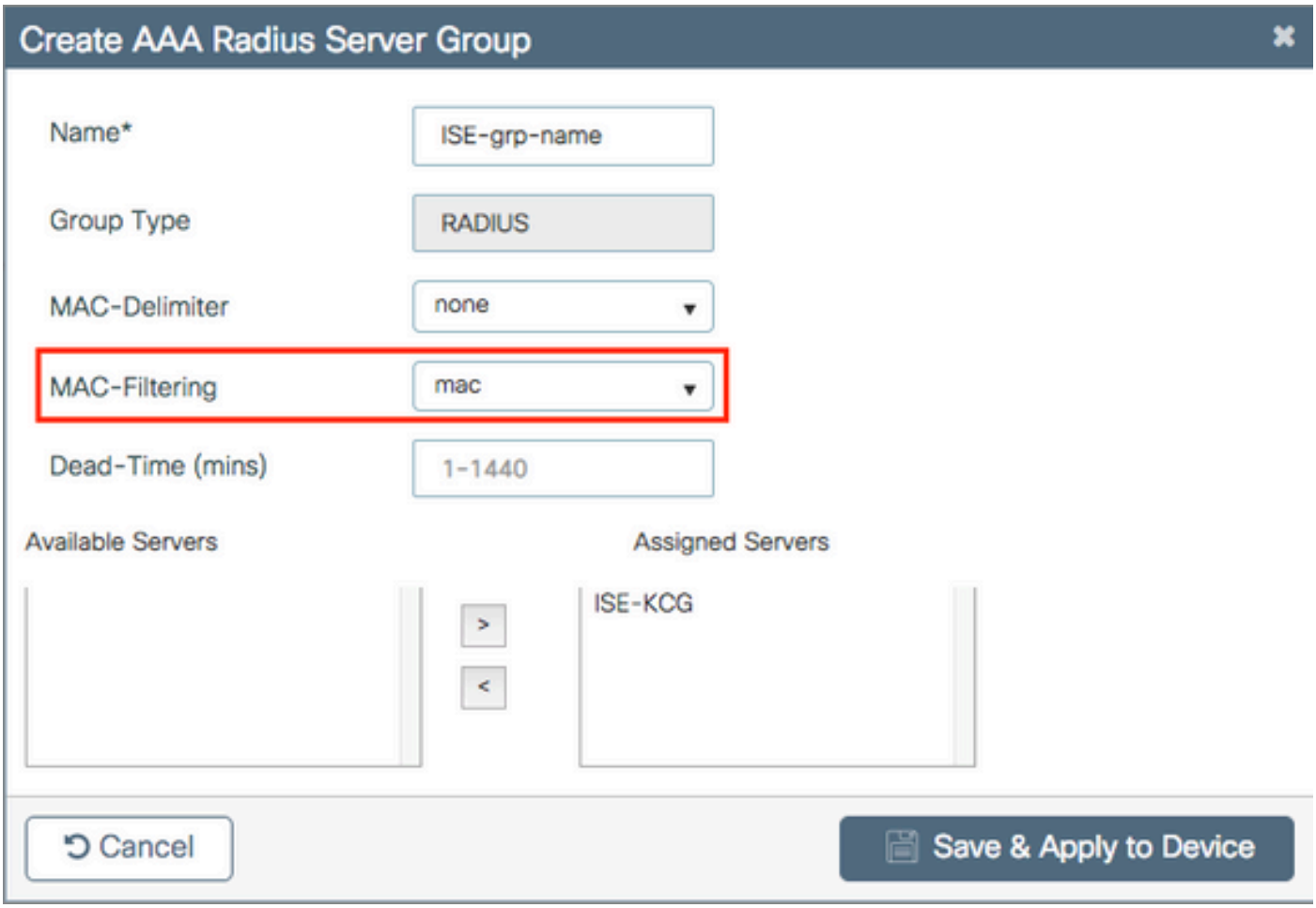


第二步：将RADIUS服务器添加到RADIUS组

导航到配置>安全> AAA >服务器/组> RADIUS >服务器组> + Add

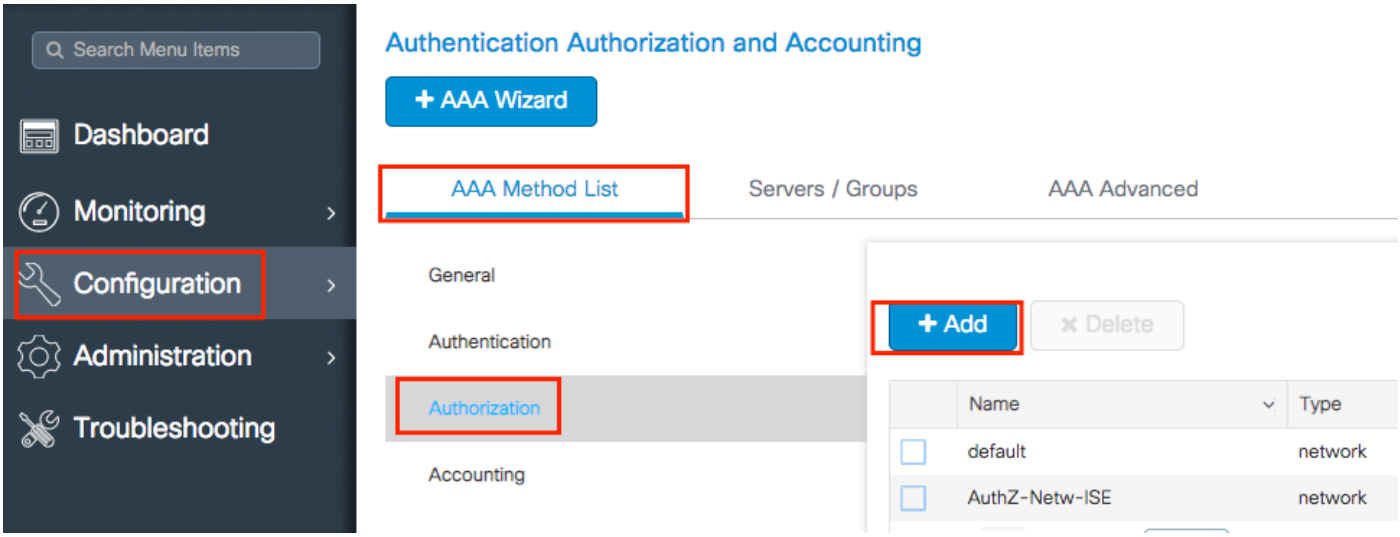
要让ISE将AP MAC地址作为用户名进行身份验证，请将MAC-Filtering保留为none。

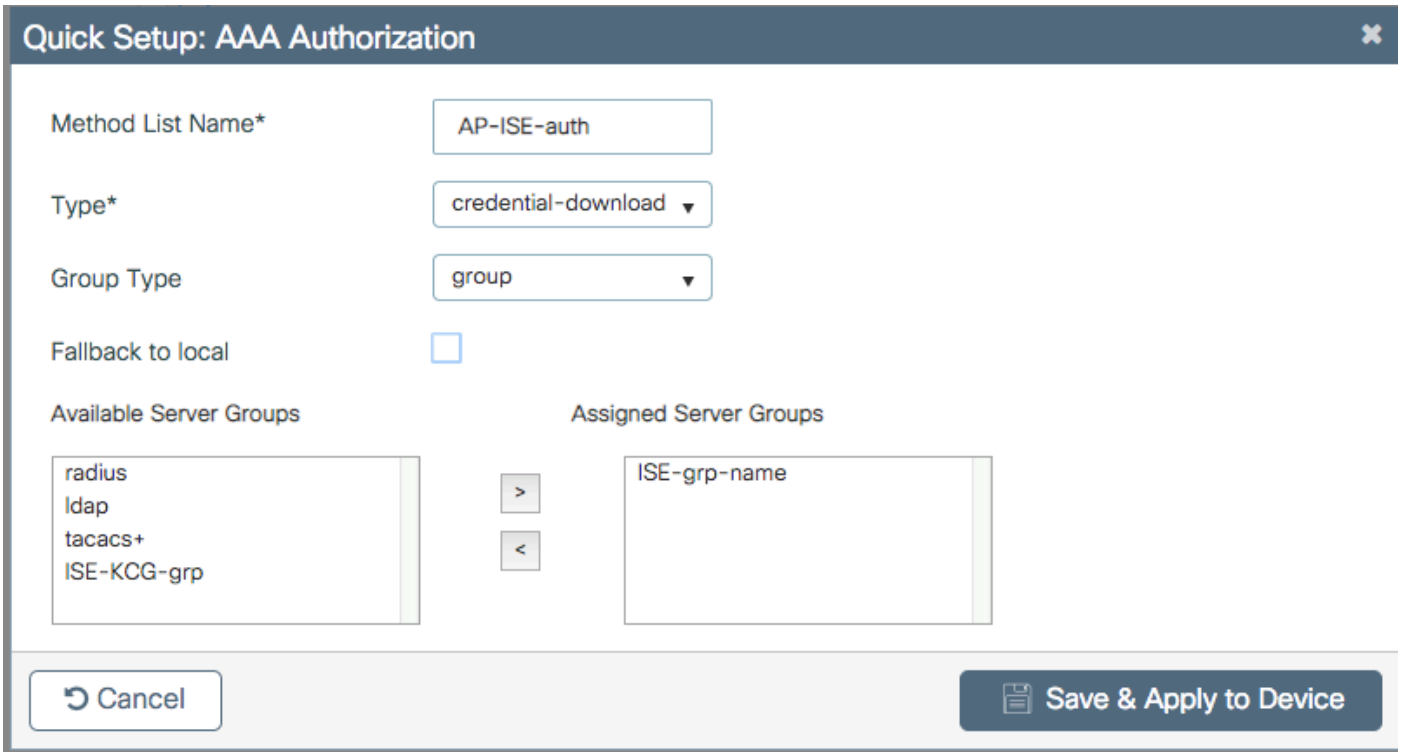
在终端将MAC-Filtering更改为mac时，让ISE对AP MAC地址进行身份验证。



第三步：创建授权凭证下载方法列表。

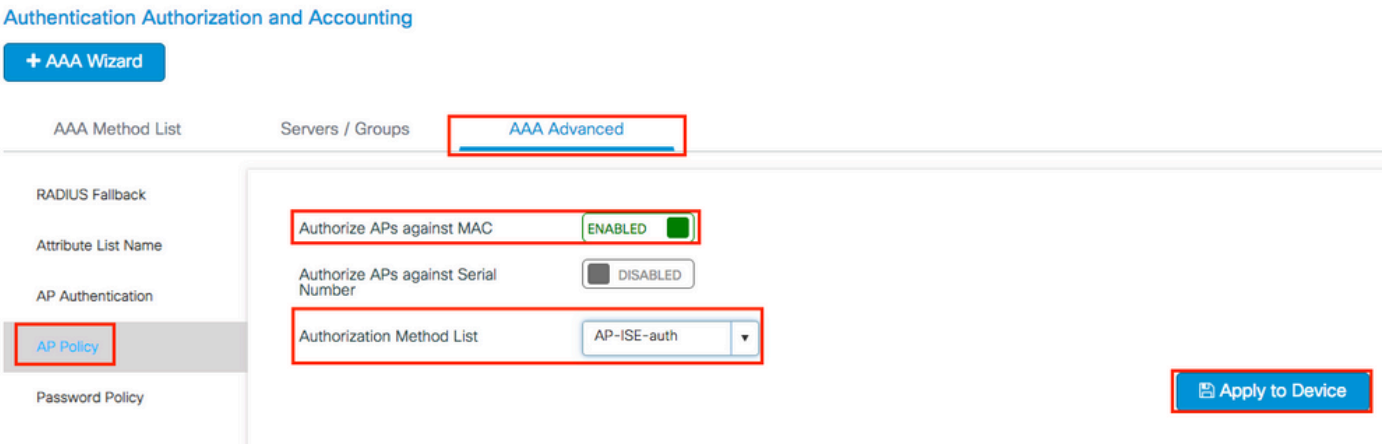
导航到配置>安全> AAA > AAA方法列表>授权> + Add





第四步：启用AP MAC授权。

导航至 Configuration > Security > AAA > AAA Advanced > AP Policy。 启用Authorize APs against MAC，并选择第3步中创建的Authorization Method List。



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 authorization credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

ISE配置

步骤1:要将9800 WLC添加到ISE，请执行以下操作：

在ISE上声明9800 WLC

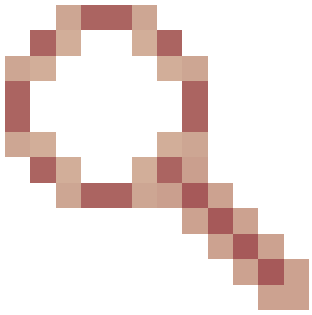
选择根据身份验证配置AP的MAC地址并完成所需的步骤：

配置USE以将MAC地址作为终端进行身份验证

将ISE配置为以用户名/密码身份对MAC地址进行身份验证

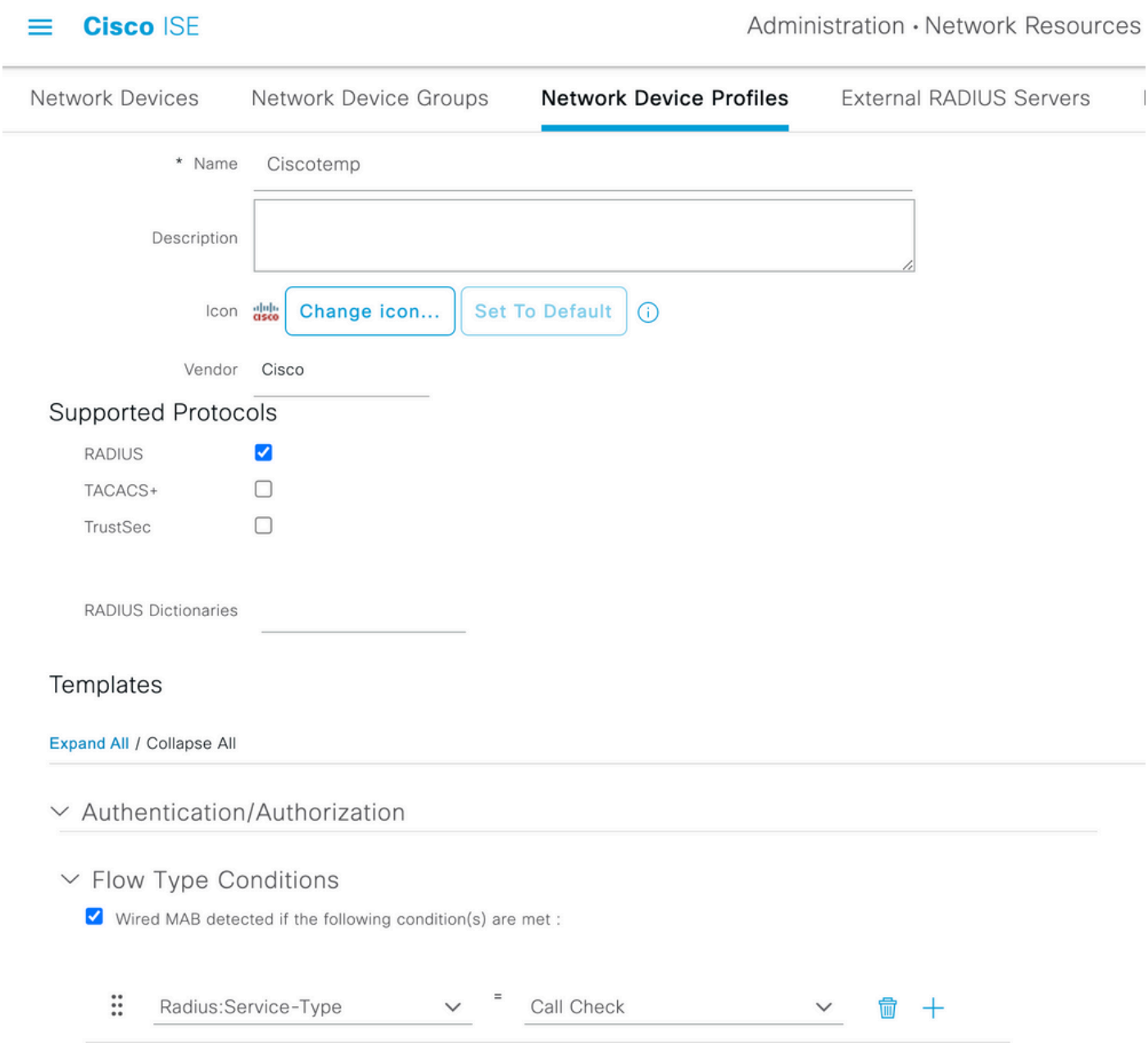
将ISE配置为将MAC地址作为终端进行身份验证

步骤2.（可选）为接入点创建身份组



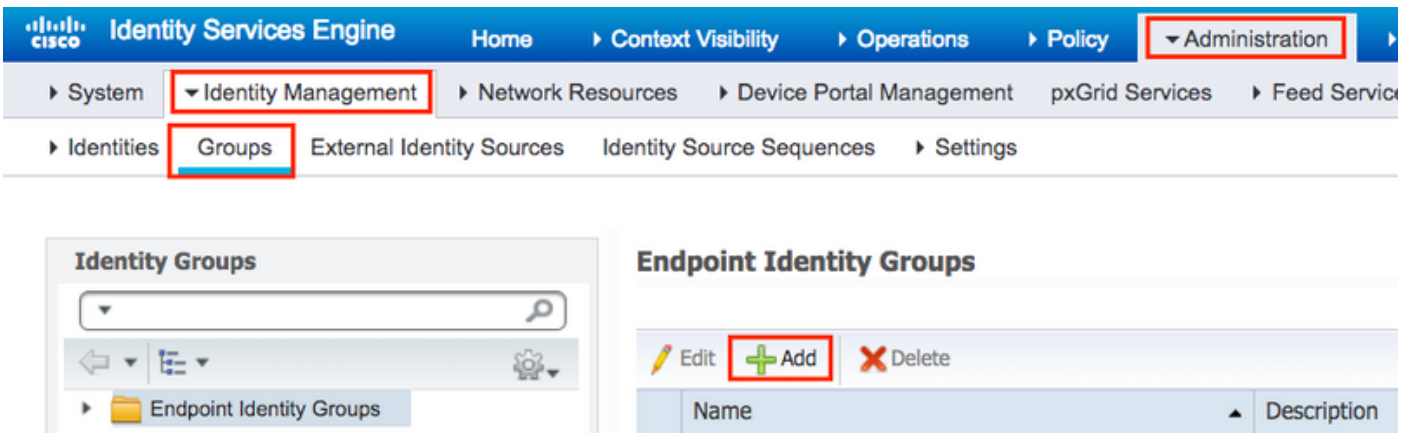
由于9800不发送带有AP授权的NAS-port-Type属性Cisco bug IDCSCvy74904),ISE无法将AP授权识别为MAB工作流程，因此，如果AP的MAC地址位于终端列表中，则无法对AP进行身份验证，除非您将MAB工作流程修改为不需要ISE上的NAS-PORT-type属性。

导航到Administrator > Network device profile并创建新的设备配置文件。启用RADIUS，并为有线MAB添加service-type=call-check。您可以从思科原始配置文件中复制其余部分，其理念是对于有线MAB没有“nas端口类型”条件。

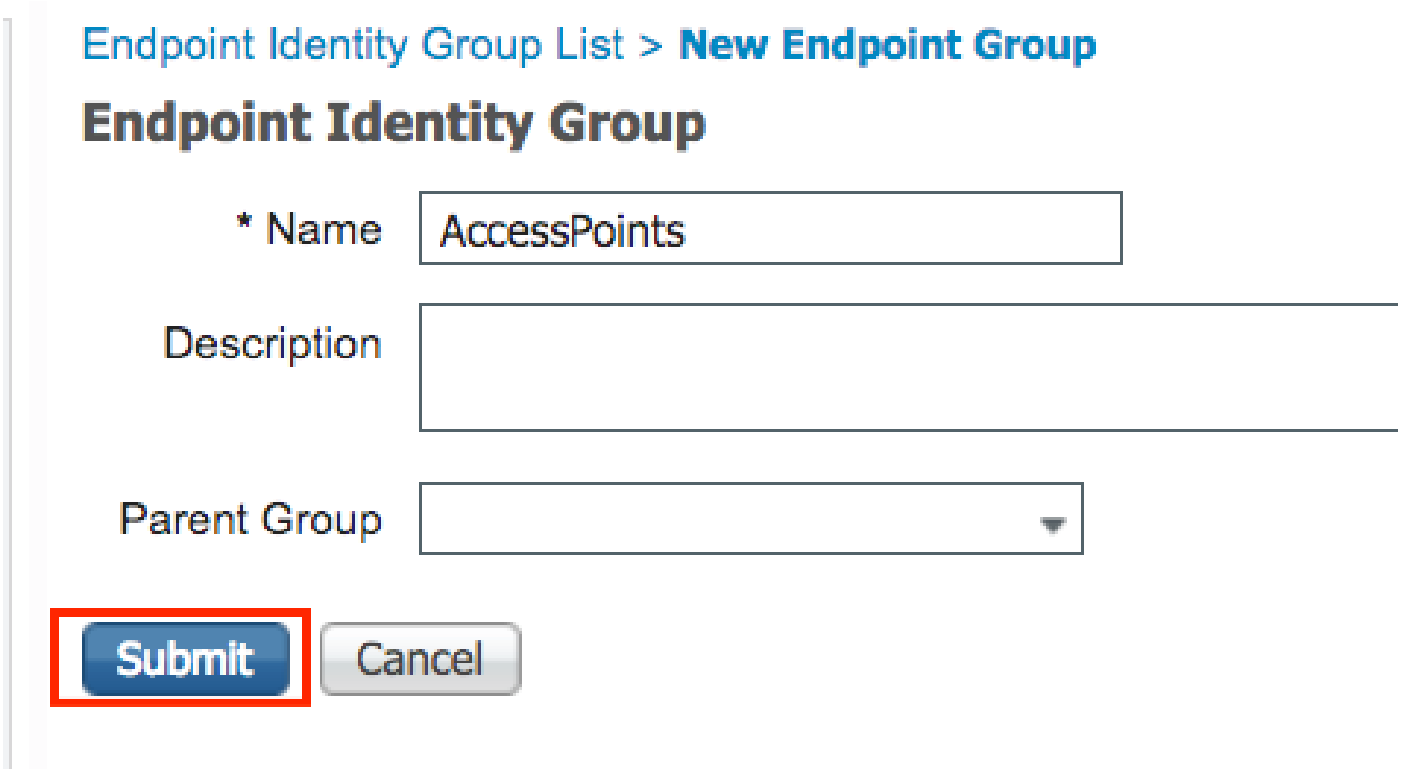


返回到9800的网络设备条目，并将其配置文件设置为新创建的设备配置文件。

导航到管理>身份管理>组>终端身份组> + Add。

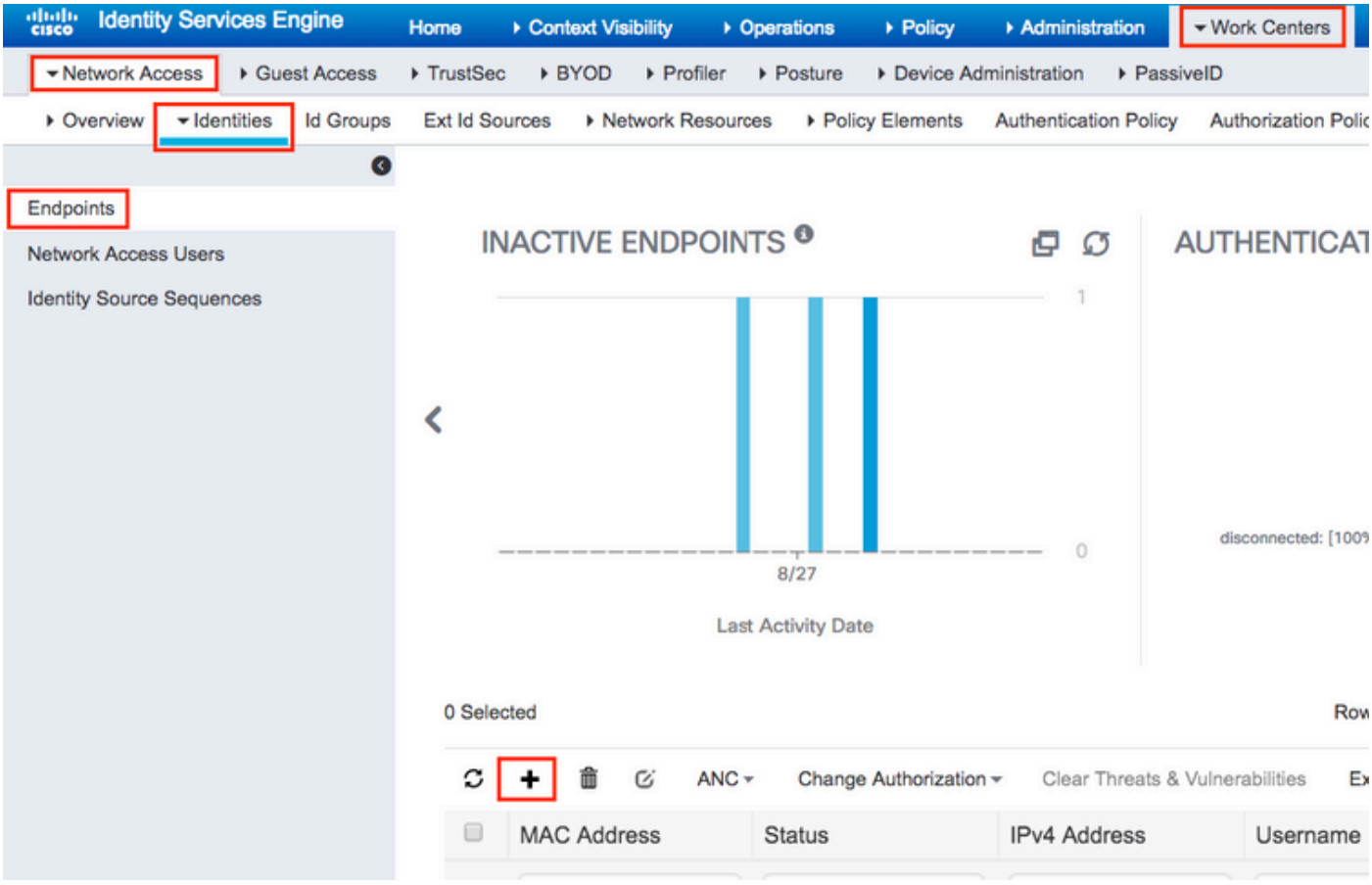


选择一个名称，然后点击提交。

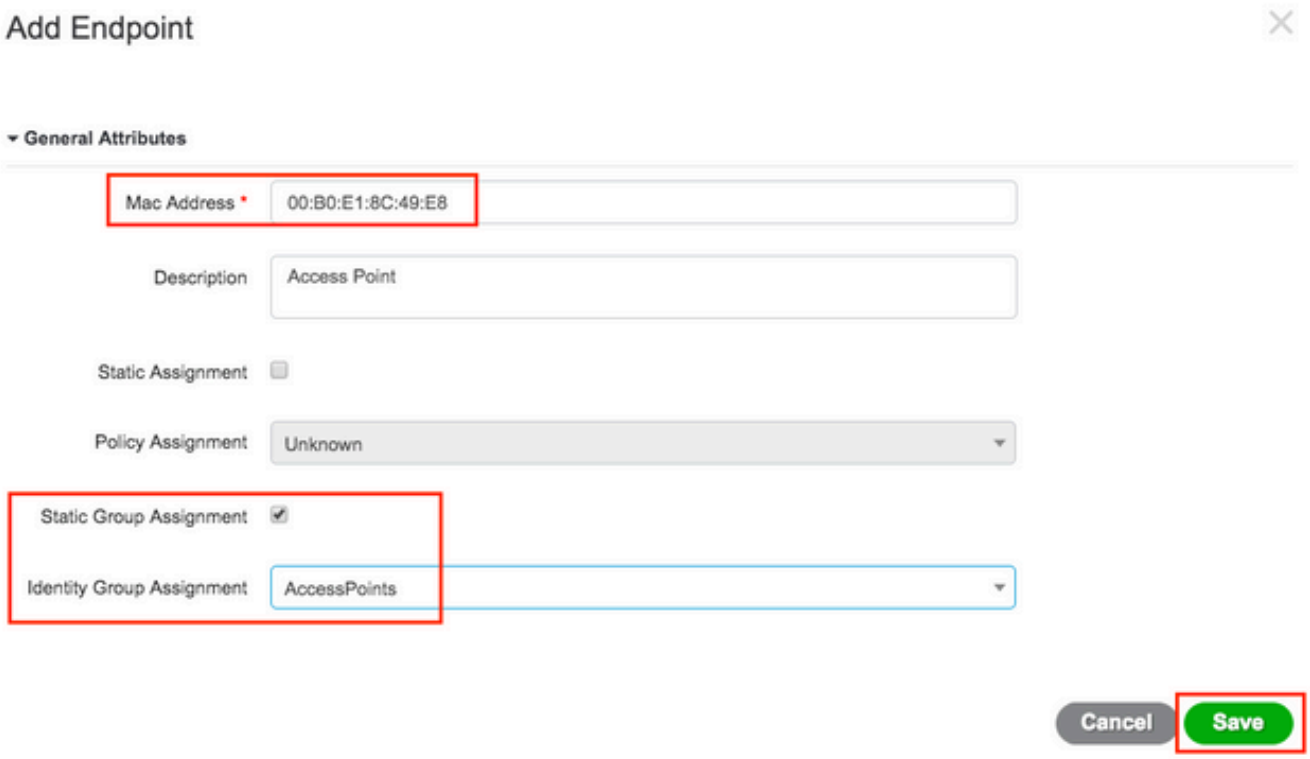


第三步：将AP以太网MAC地址添加到其终端身份组。

导航至工作中心>网络访问>身份>终端> +

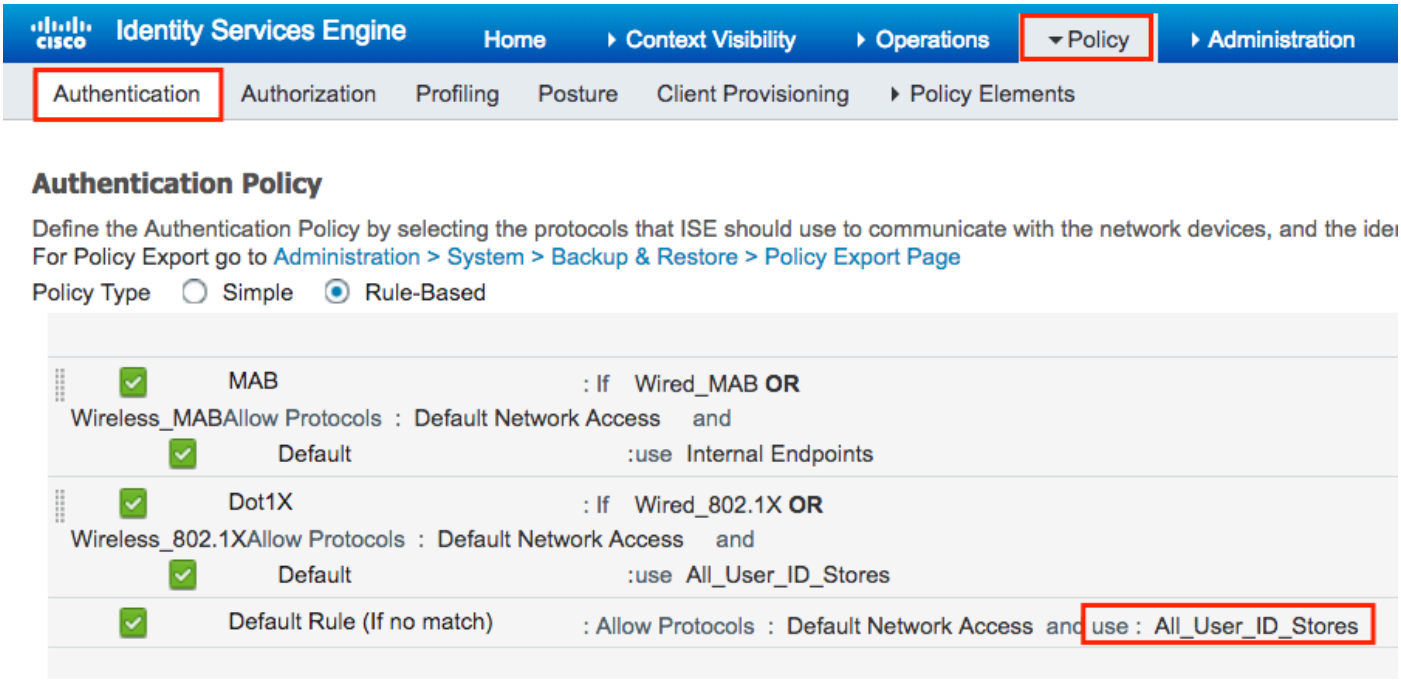


输入所需信息。

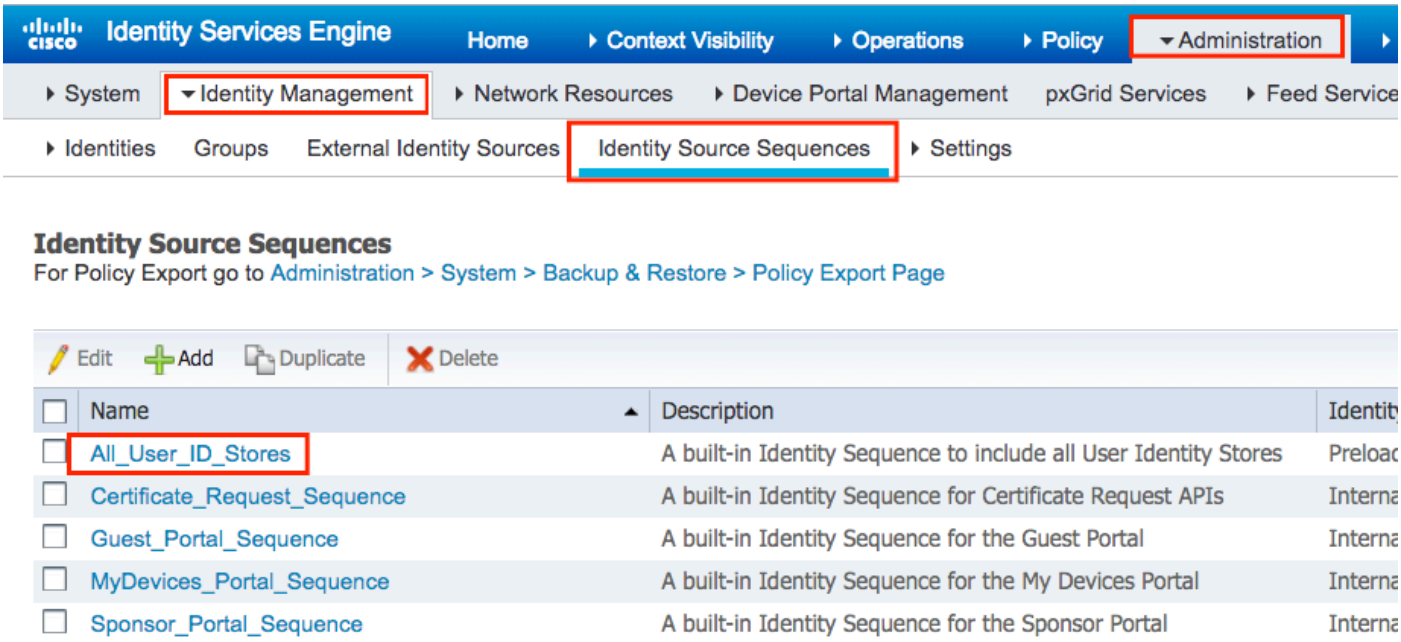


第四步：验证默认身份验证规则上使用的身份库是否包含内部终端。

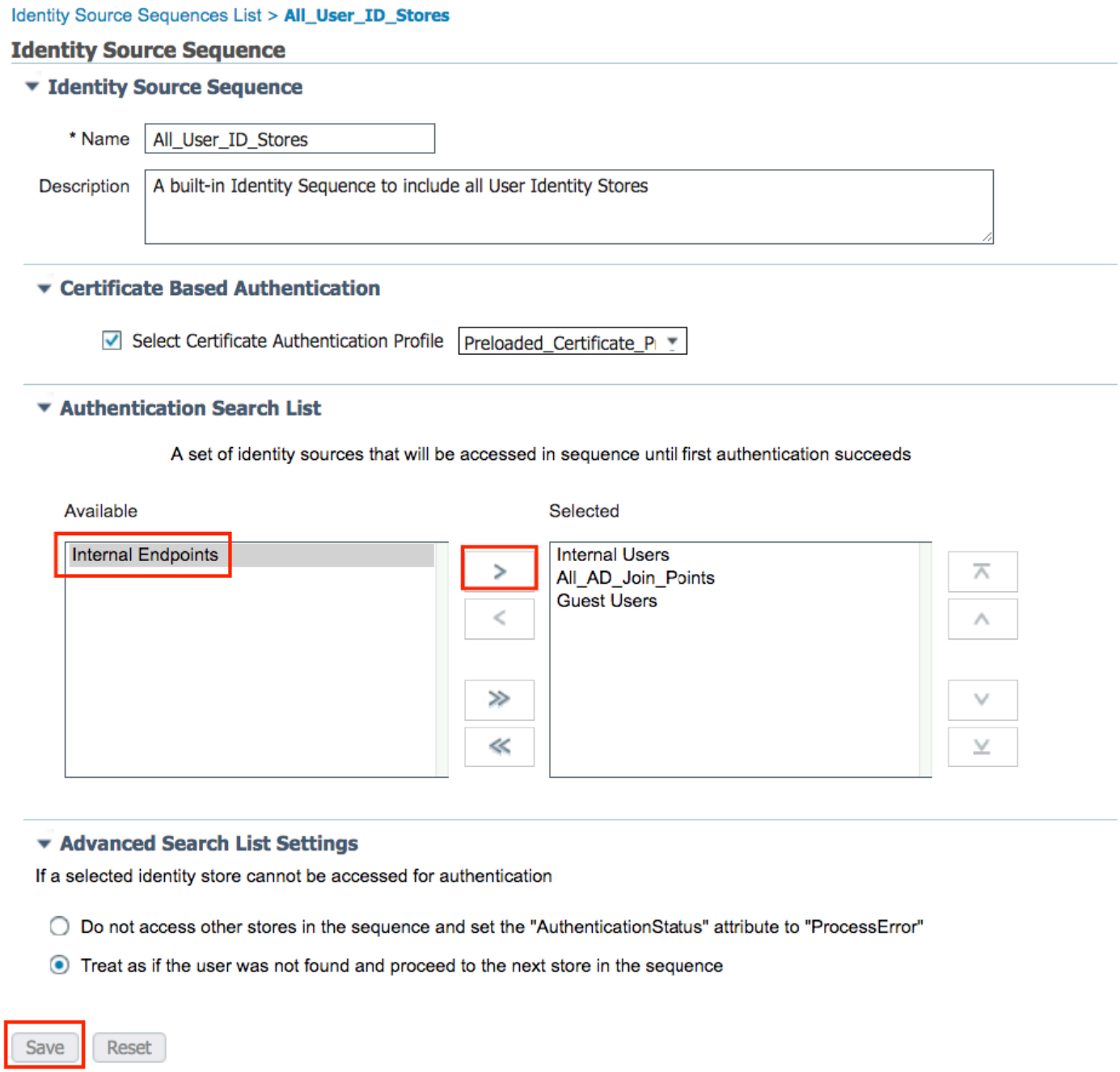
A.导航到Policy > Authentication，并记下身份库。



B.导航到管理>身份管理>身份源序列>身份名称。



C.确保内部终端属于它，如果不是，则添加它。



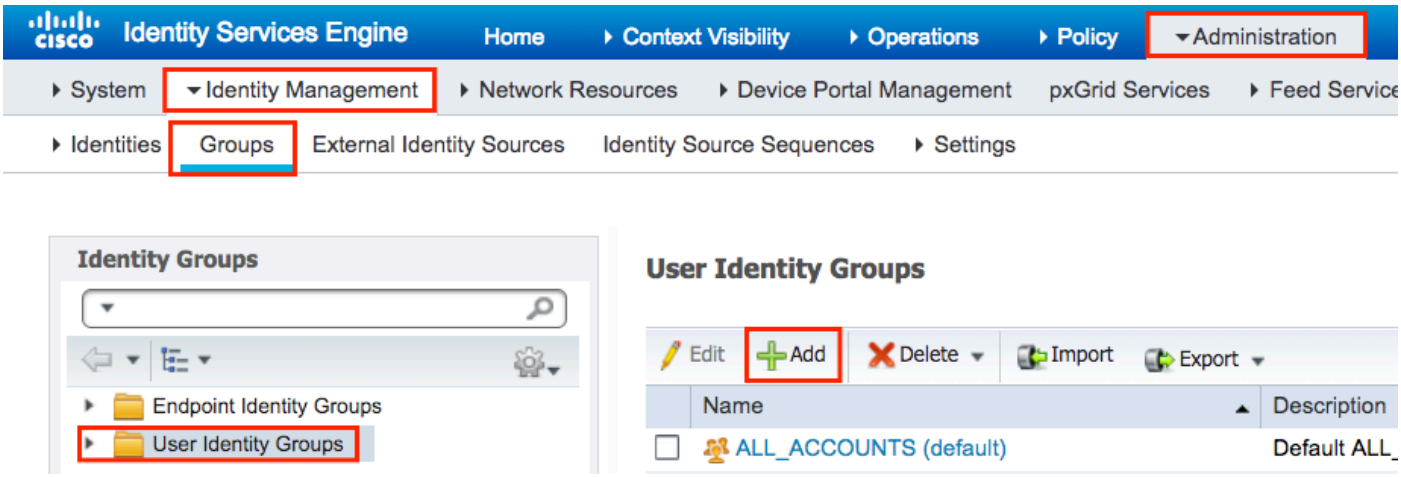
将ISE配置为以用户名/密码身份对MAC地址进行身份验证

不建议使用此方法，因为它需要较低的密码策略以允许与用户名相同的密码。

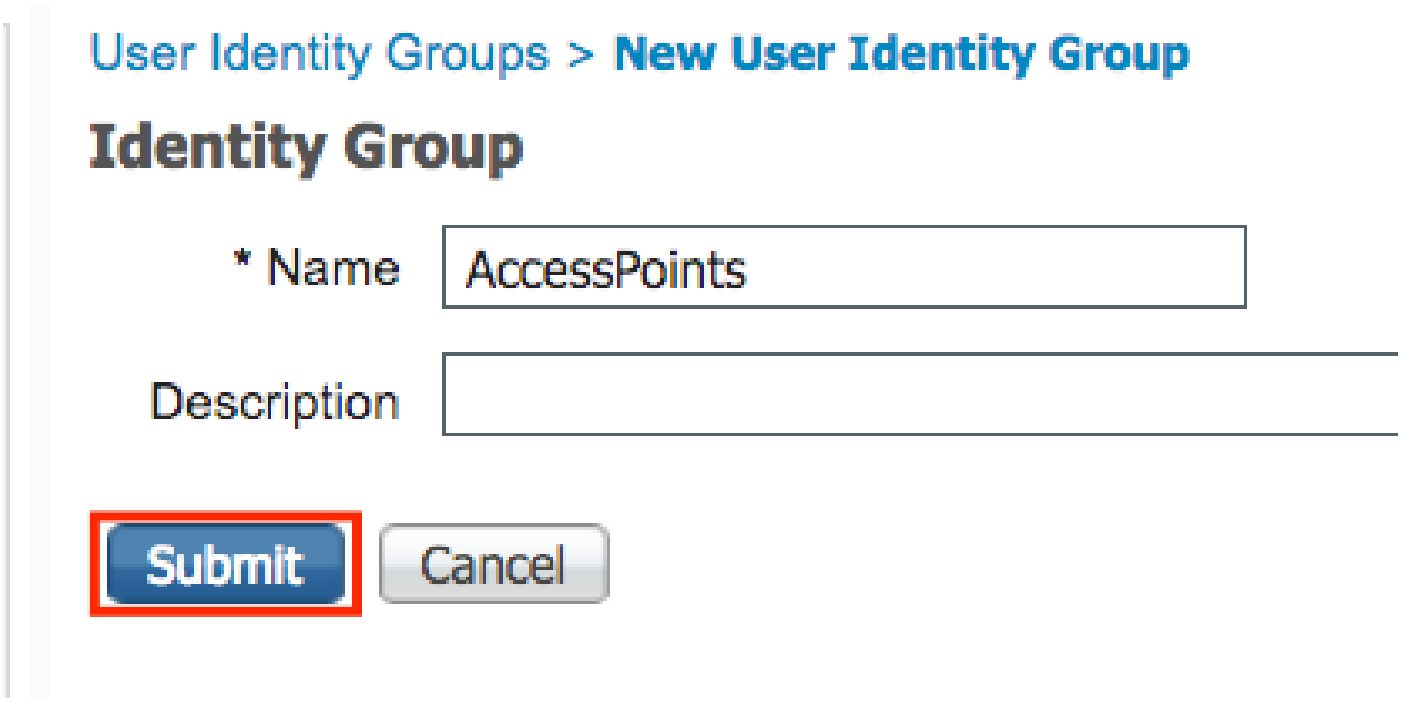
但是，如果无法修改网络设备配置文件，则可以将其作为一种解决方法

步骤2.（可选）为接入点创建身份组

导航到Administration > Identity Management > Groups > User Identity Groups > + Add。

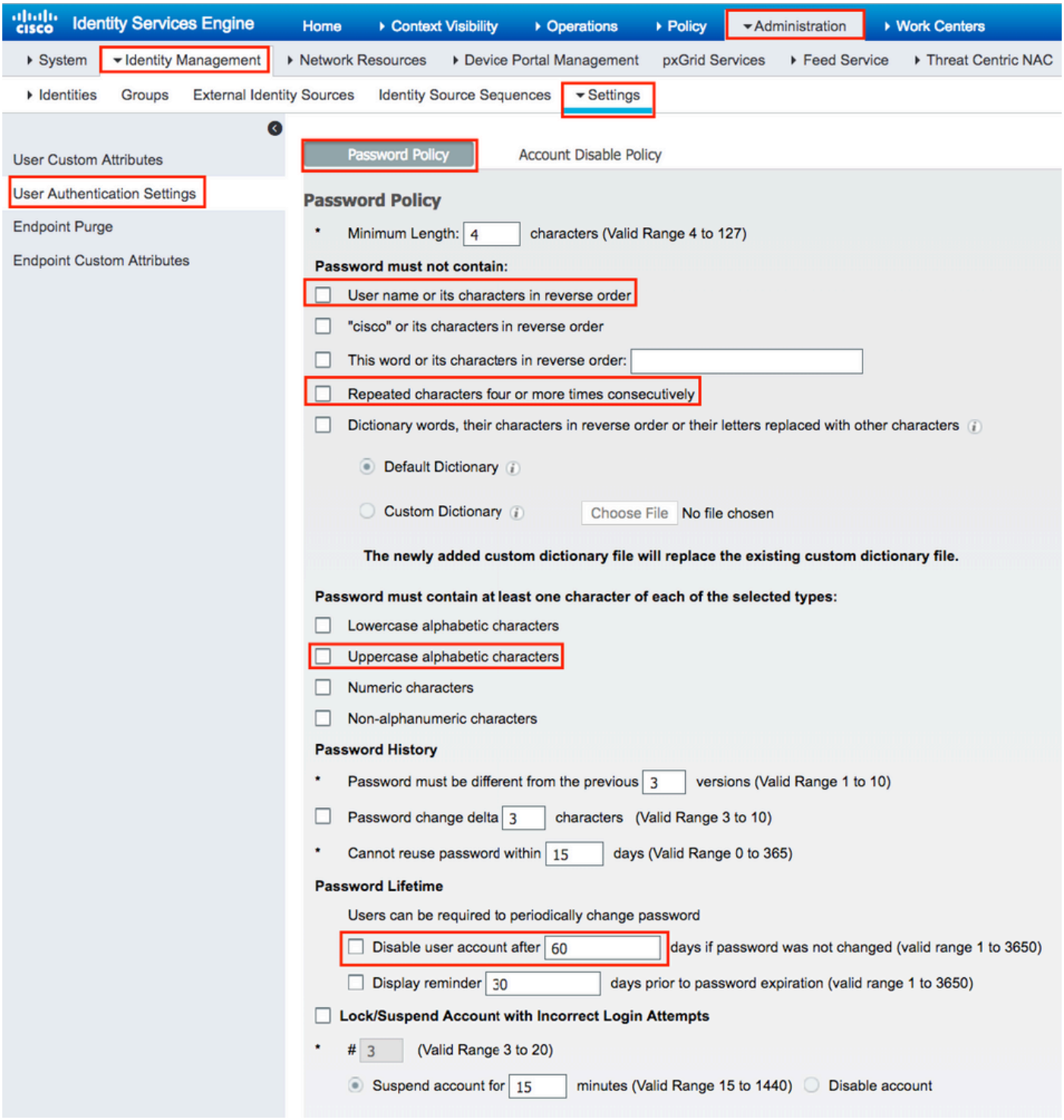


选择一个名称，然后点击提交。



第三步：验证当前密码策略是否允许您将mac地址添加为用户名和密码。

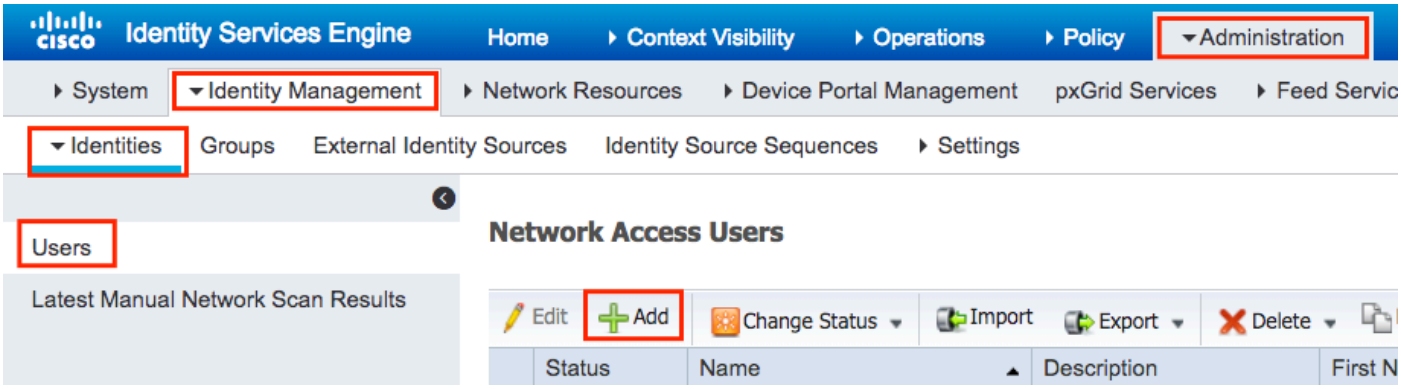
导航到Administration > Identity Management > Settings > User Authentication Settings > Password Policy，并确保至少禁用以下选项：



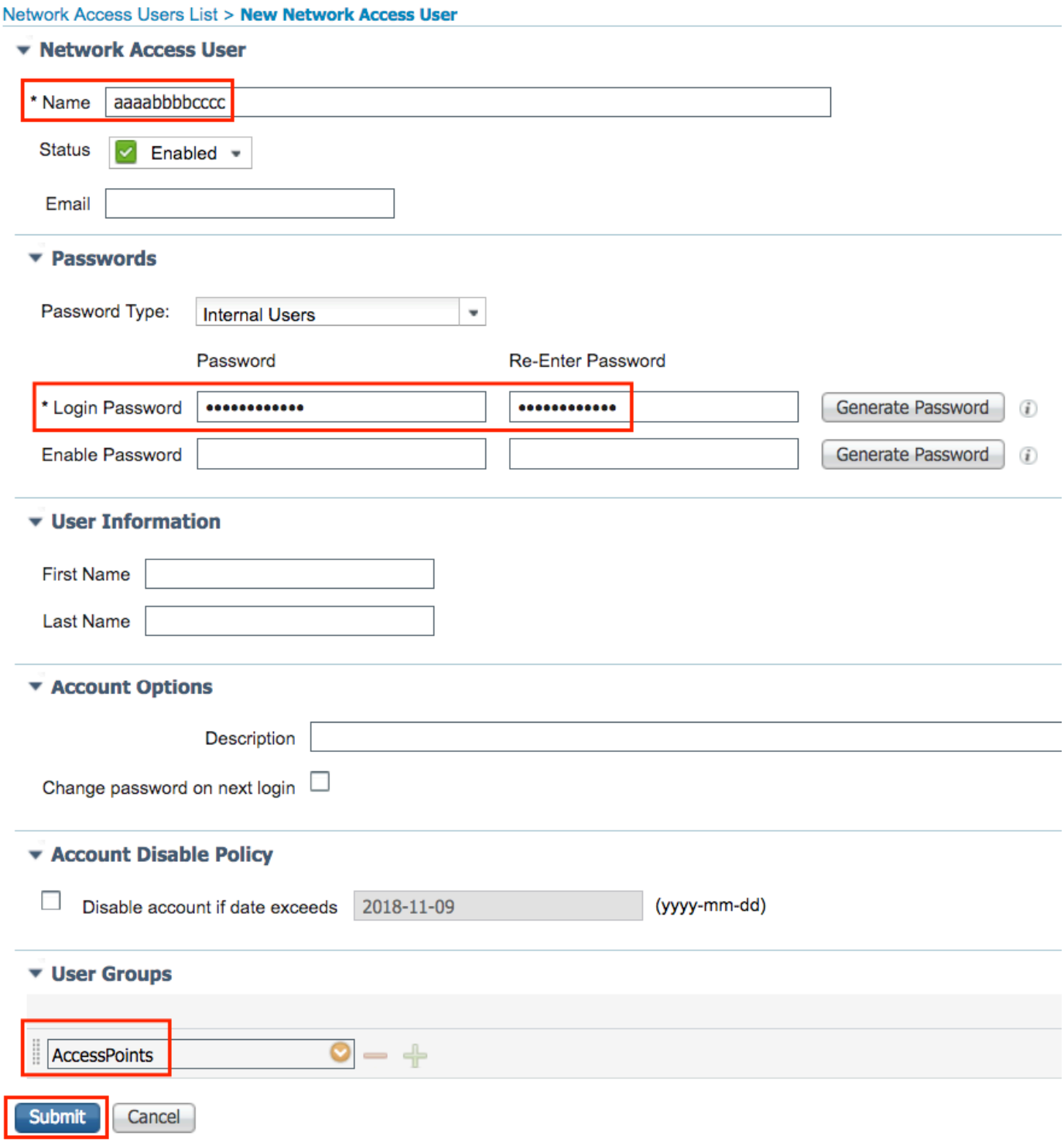
注:如果密码未更改，您也可以禁用在XX天后禁用用户帐户选项。由于这是MAC地址，因此密码永远不会更改。

第四步：添加AP以太网mac地址。

导航到管理>身份管理>身份>用户> + Add


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Servic
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Results
Network Access Users
Edit
Add
Change Status
Import
Export
Delete
Status
Name
Description
First N

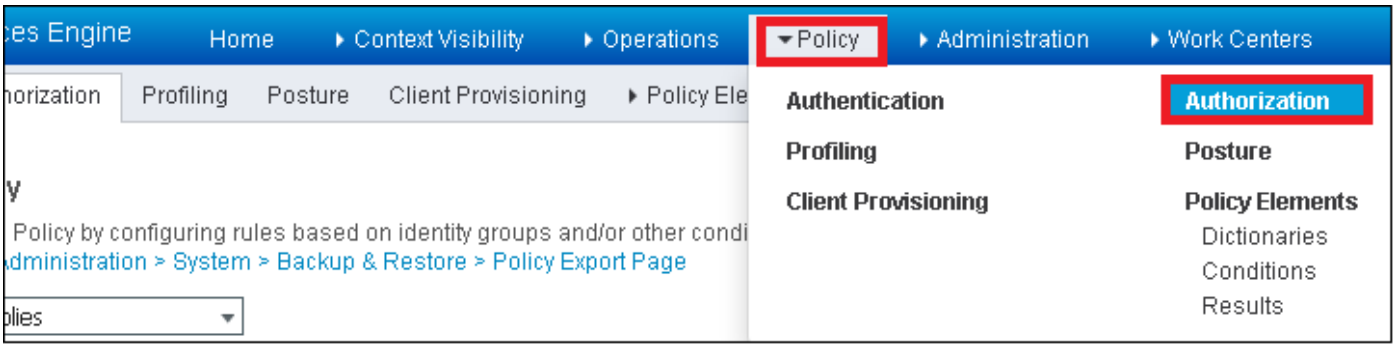
输入所需信息。



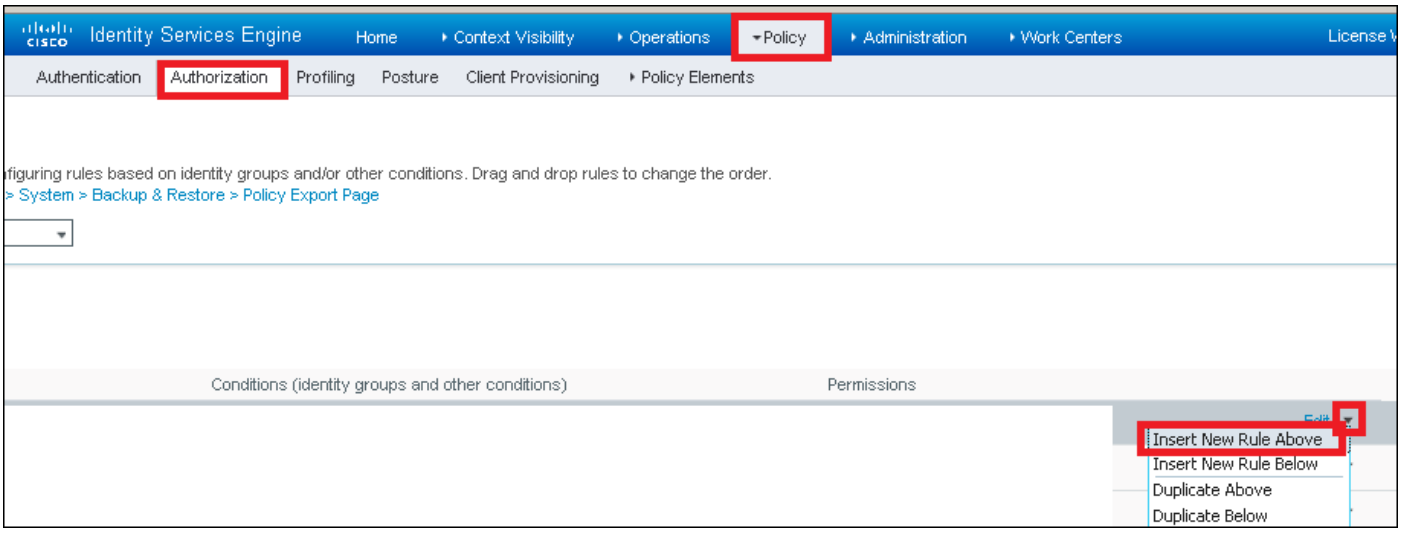
注意: Name 和Login Password字段必须是AP的以太网MAC地址，全部为小写，无分隔符。

对AP进行身份验证的授权策略

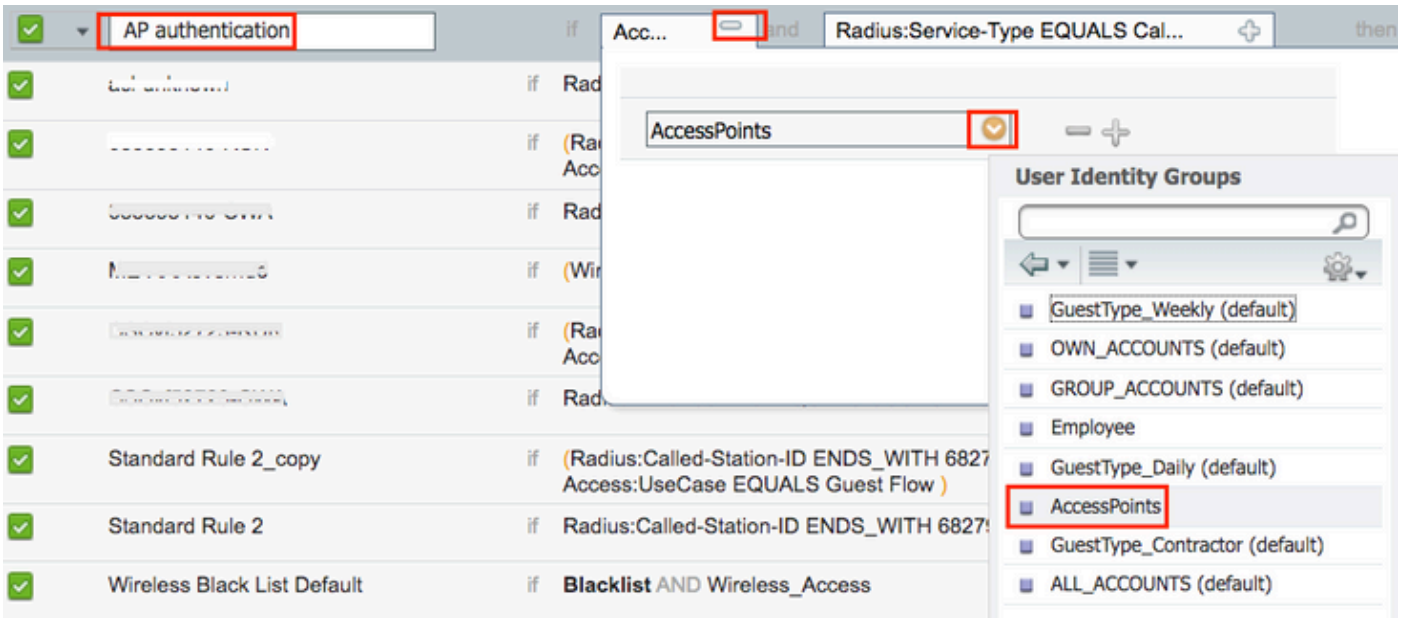
导航至Policy > Authorization，如图所示。



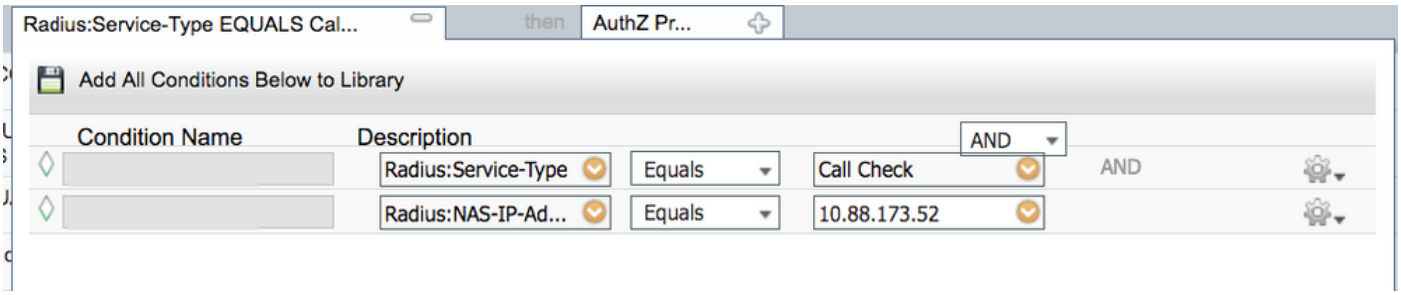
插入新规则，如图所示。



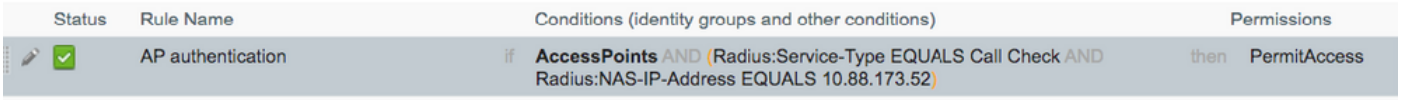
首先，为规则和存储接入点的身份组(AccessPoints)选择一个名称。 如果您决定将MAC地址作为用户名密码进行身份验证，请选择User Identity Groups；如果您选择将AP MAC地址作为终端进行身份验证，请选择Endpoint Identity Groups。



之后，选择执行授权流程的其他条件，使其符合此规则。在本示例中，如果授权进程使用service-type Call Check并且身份验证请求来自IP地址10.88.173.52，则授权进程符合此规则。



最后，选择分配给符合该规则的客户端的授权配置文件，单击Donee并保存它，如图所示。



注：已加入控制器的AP不会失去关联。但是，如果在启用授权列表后，它们会失去与控制器的通信并尝试重新加入，则它们将完成身份验证过程。如果它们的mac地址未在本地或RADIUS服务器中列出，则它们无法重新加入控制器。

验证

验证9800 WLC是否已启用AP身份验证列表

<#root>

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled
Authorize APs against Serial Num : Enabled
Authorization Method List : <auth-list-name>
```

验证radius配置：

<#root>

```
#
show run aaa
```

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与AP加入相关的错误、警告和通知级别消息，并且您可以在发生事故或故障情况后查看其日志。

注意：生成的日志量从几个小时到几天不等。

要查看9800 WLC在默认情况下收集的跟踪，您可以通过以下步骤通过SSH/Telnet连接到9800 WLC（确保您将会话记录到文本文件）。

步骤1:检查控制器当前时间，以便您可以在问题发生之前的时间跟踪日志。

```
# show clock
```

第二步：根据系统配置的指示，从控制器缓冲区或外部系统日志收集系统日志。这样可以快速查看系统运行状况和错误（如有）。

```
# show logging
```

第三步：验证是否启用了任何调试条件。

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Trace Configs:


Packet Infra debugs:

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

注：如果看到列出了任何条件，则意味着所有遇到启用条件的进程（mac地址、ip地址等）的跟踪将记录到调试级别。这会增加日志量。因此，建议在非主动调试时清除所有条件

第四步：假设在步骤3中，未将正在测试的mac地址列为条件，请收集特定无线电mac地址的始终在线通知级别跟踪。

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

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

如果永远在线(always-on)跟踪不能为您提供足够的信息来确定所调查问题的触发器，则可以启用条件调试并捕获无线活动(RA)跟踪，该跟踪为与指定条件（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。

第五步：确保未启用调试条件。

```
# clear platform condition all
```

第六步：为要监控的无线客户端MAC地址启用调试条件。

此命令开始监控提供的mac地址达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:要一次监控多个客户端，请对每个mac地址运行debug wireless mac <aaaa.bbbb.cccc>命令。

注意:您不会看到终端会话上的客户端活动的输出，因为所有内容都在内部缓冲，供以后查看。

步骤 7.重现要监控的问题或行为。

步骤 8如果在默认或配置的监控器时间开启之前重现问题，则停止调试。

```
# 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

步骤 9 收集 MAC 地址活动的文件。 您可以将 ra trace.log 复制到外部服务器，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
```

步骤 10如果根本原因仍不明显，请收集内部日志，这些日志是调试级别日志的更详细视图。您无需再次调试客户端，因为我们只需进一步详细查看已收集并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 r
```

注意：此命令输出返回所有进程的所有日志记录级别的跟踪，而且数量相当大。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
```

步骤 11删除调试条件。

```
# clear platform condition all
```

注意：请确保在故障排除会话后始终删除调试条件。

参考

将网状AP连接到9800 WLC

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）。