为 Catalyst 9800 无线控制器配置 MAC 身份验证 SSID

目录

简介

本文档介绍如何在Cisco Catalyst 9800 WLC上设置具有MAC身份验证安全性的无线局域网(WLAN)。

先决条件

要求

Cisco 建议您了解以下主题：

- Mac 地址
- Cisco Catalyst 9800 系列无线控制器
- 身份服务引擎(ISE)

使用的组件

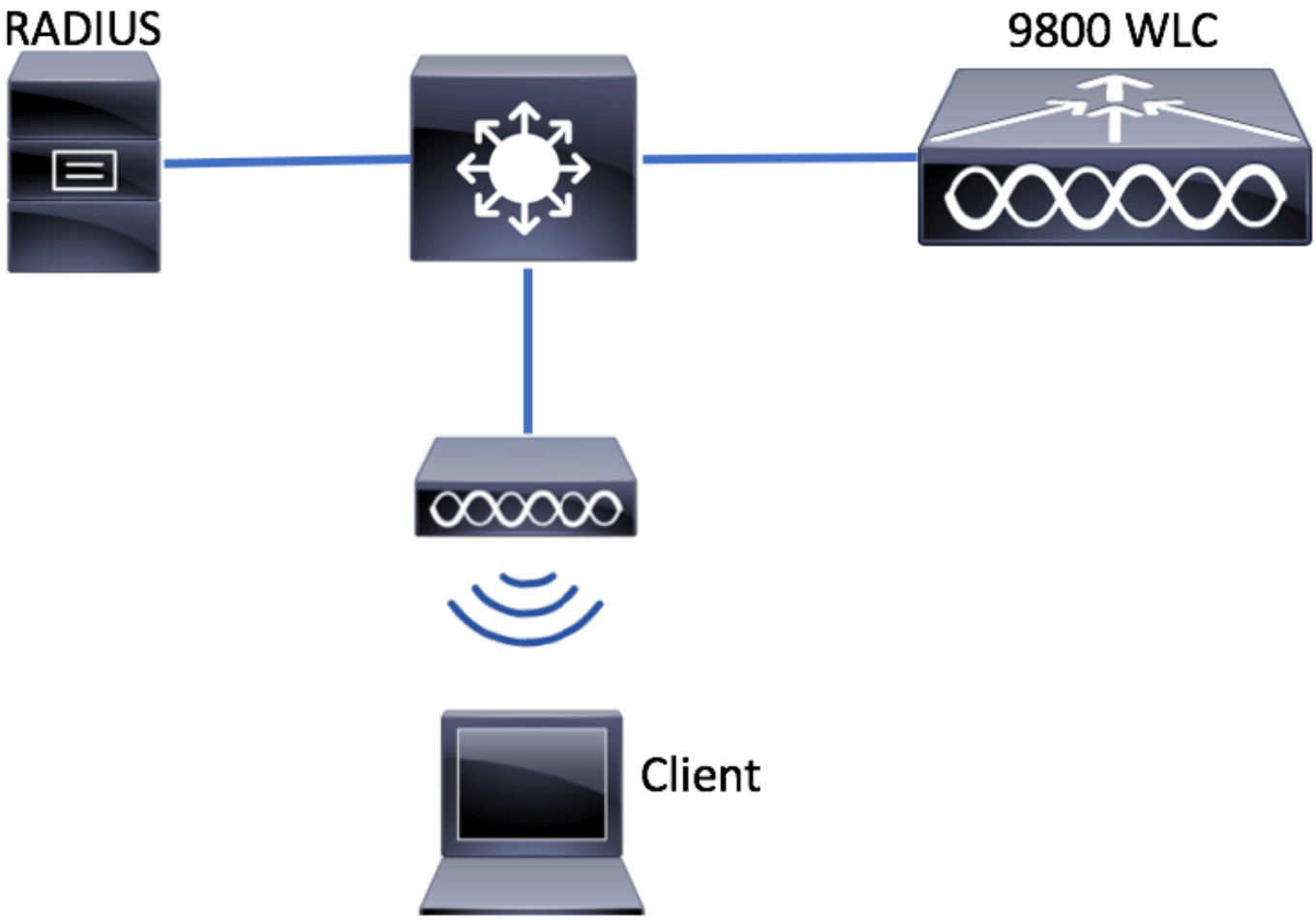
本文档中的信息基于以下软件和硬件版本：

- 思科IOS® XE直布罗陀v16.12
- 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



9800 WLC 上的 AAA 配置

使用外部服务器对客户端进行身份验证

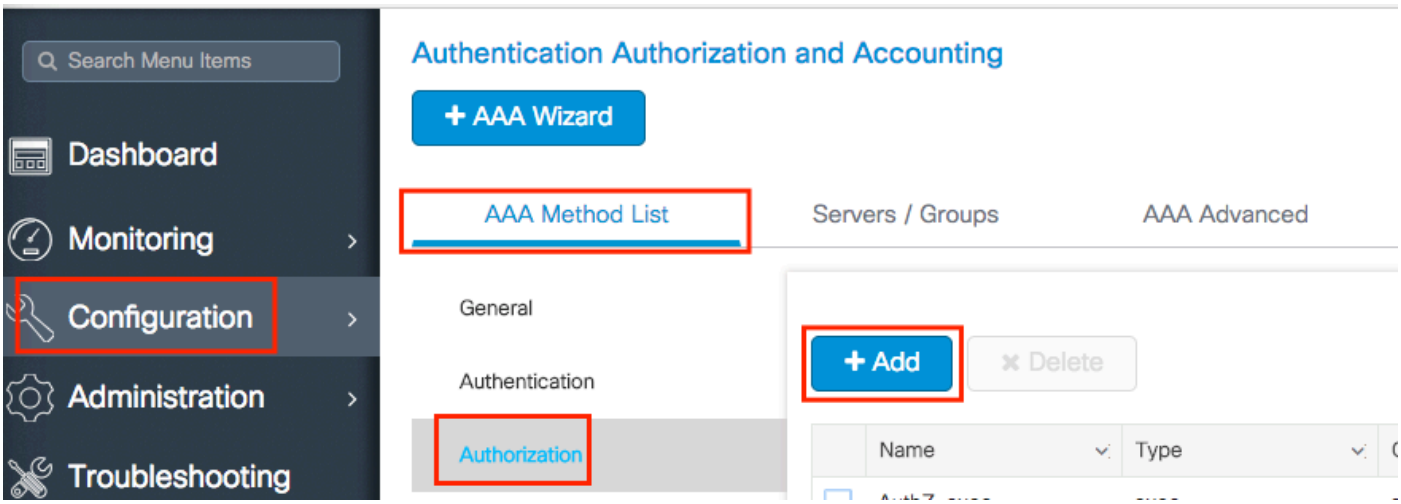
GUI:

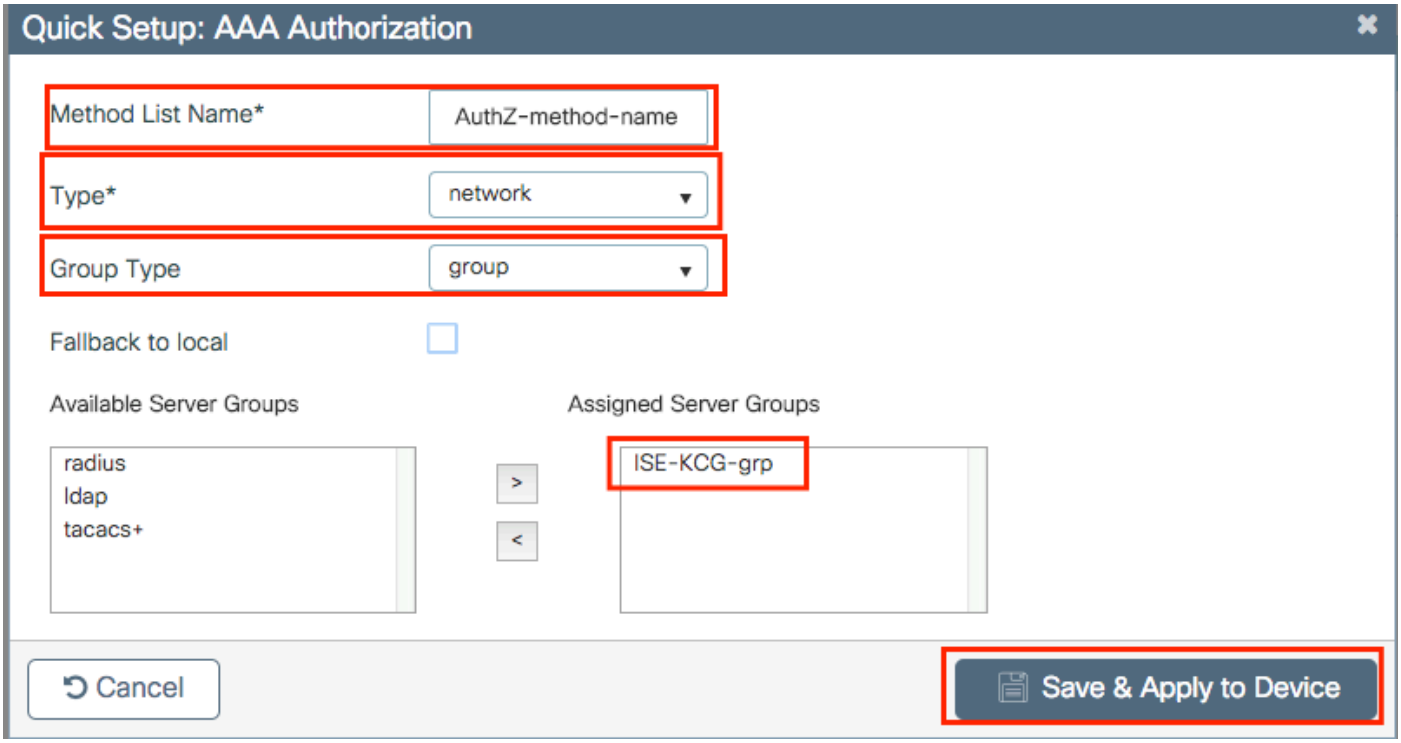
从此链接阅读“9800 WLC上的AAA配置”一节中的步骤1-3:

9800系列WLC上的AAA配置

第四步：创建授权网络方法。

导航到Configuration > Security > AAA > AAA Method List > Authorization > + Add并创建它。





CLI：

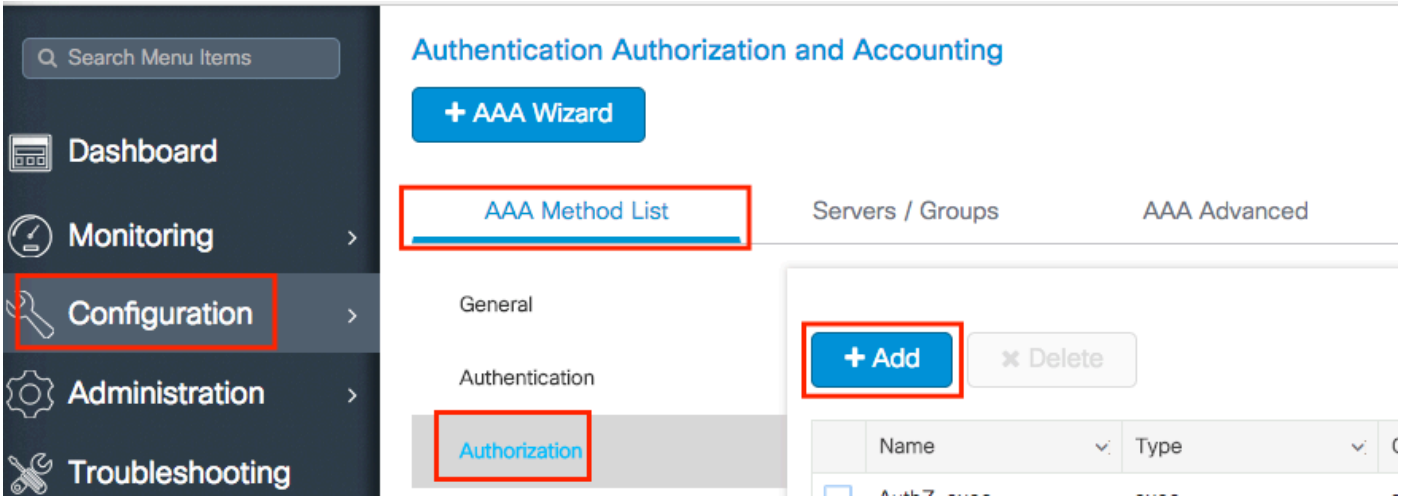
```
# config t
# aaa new-model

# 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
```

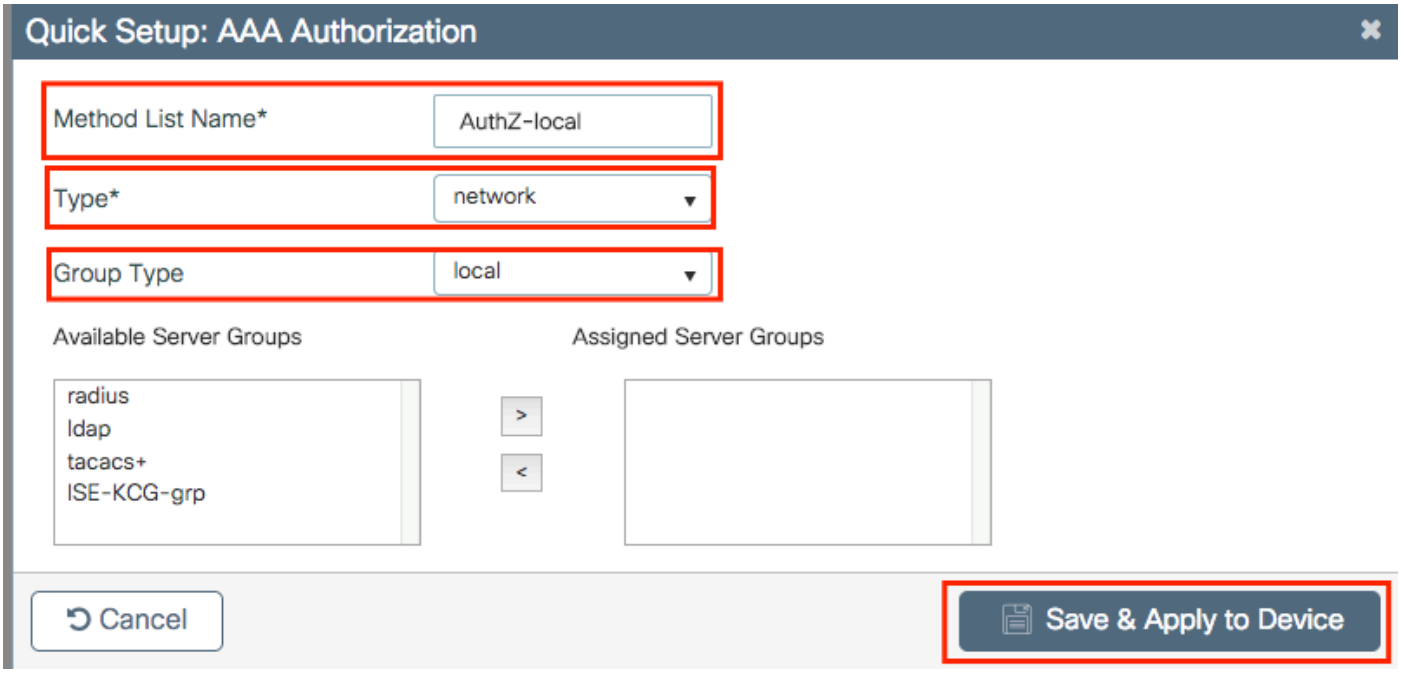
```
# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authorization network <AuthZ-method-name> group <radius-grp-name>
```

本地验证客户端

创建本地授权网络方法。

导航到Configuration > Security > AAA > AAA Method List > Authorization > + Add并创建它。





CLI：

```
# config t
```

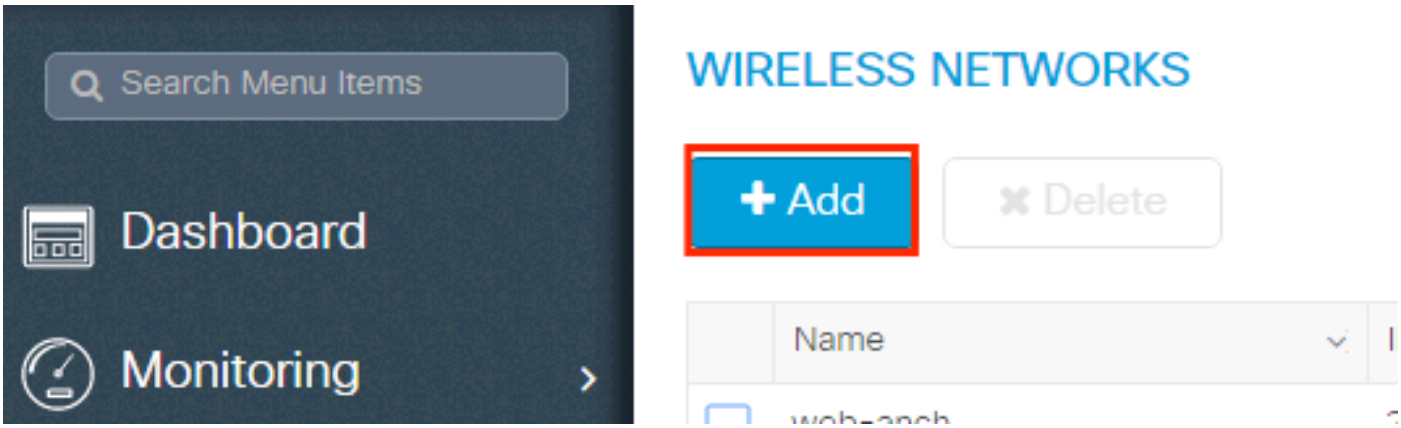
```
# aaa new-model
# aaa authorization network AuthZ-local local
```

WLAN 配置

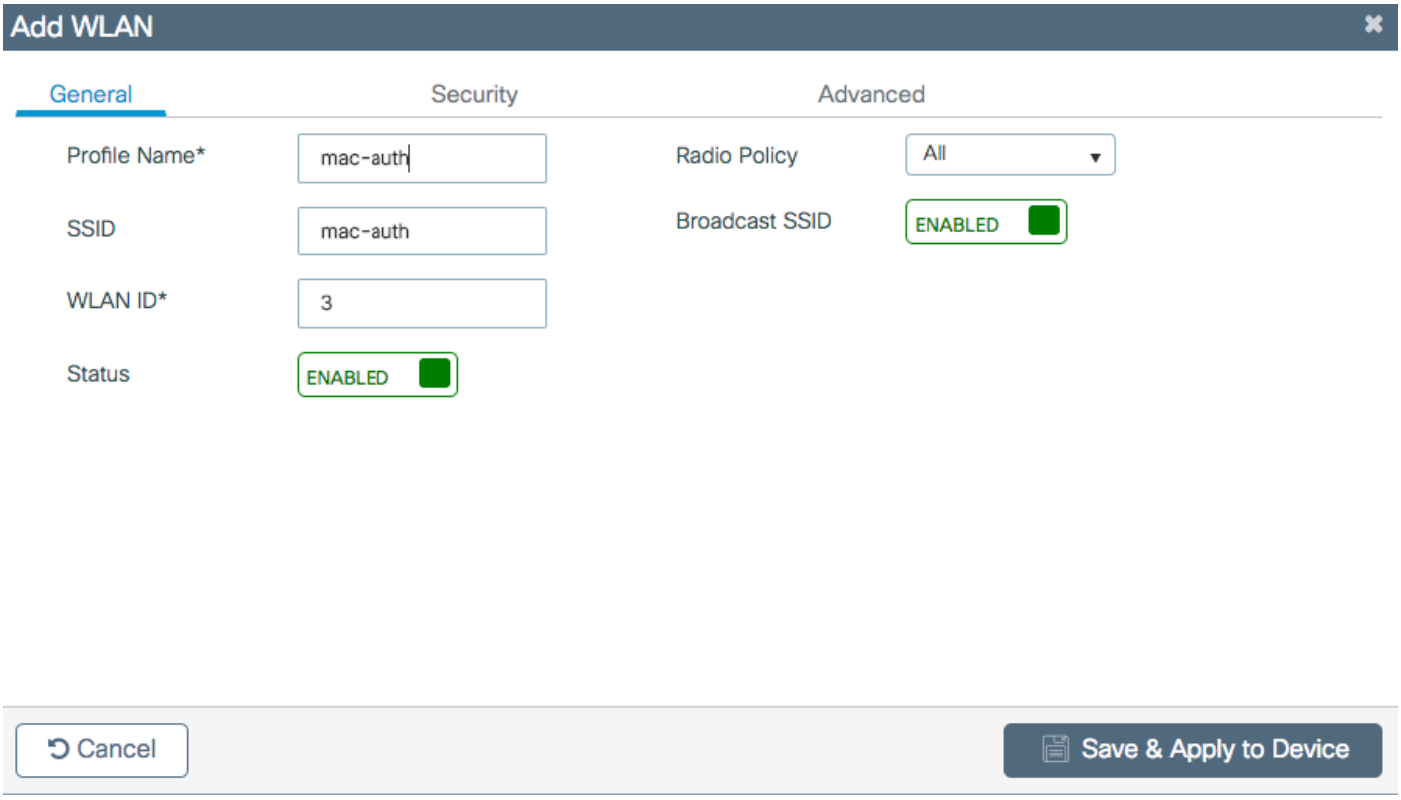
GUI:

步骤1:创建WLAN。

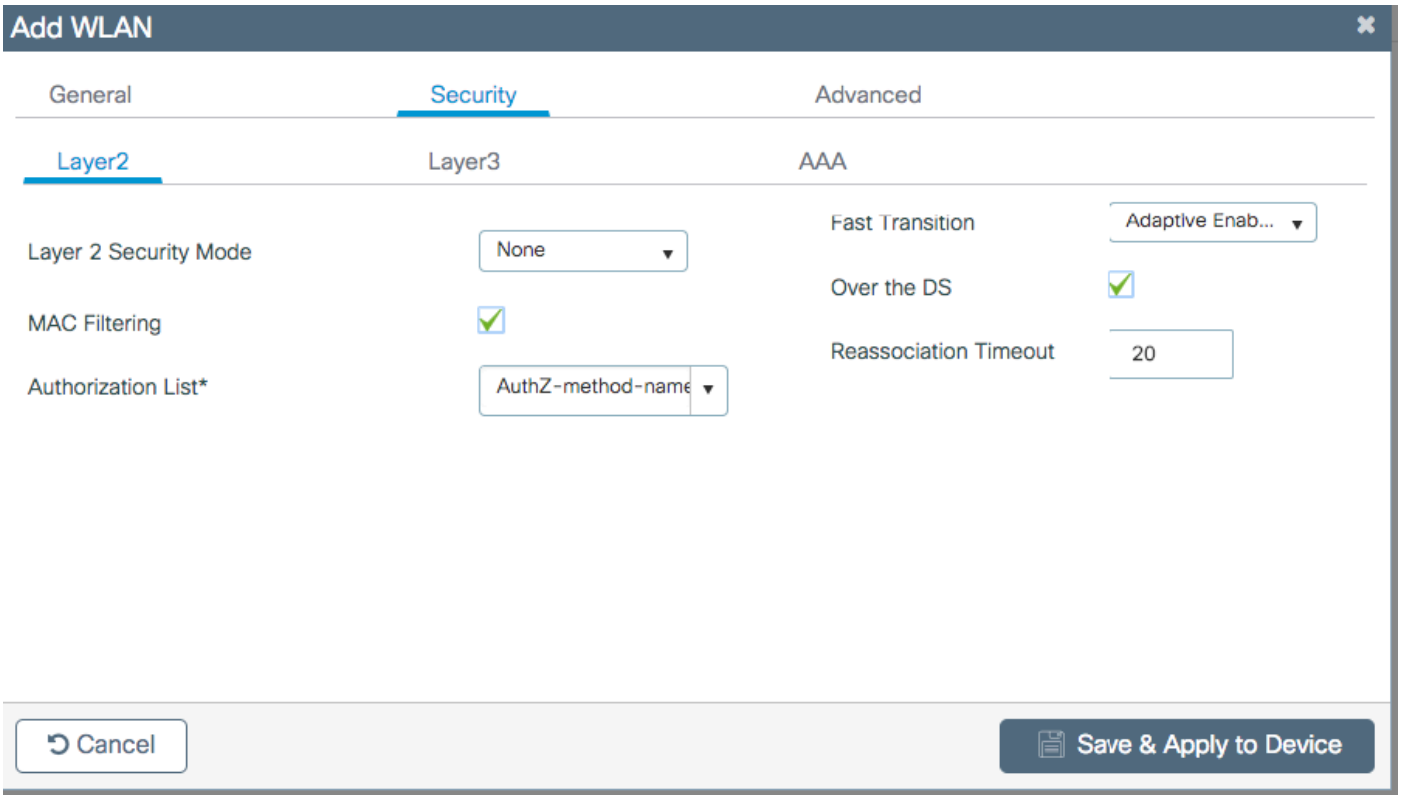
根据需Configuration > Wireless > WLANs > + Add要导航到并配置网络。



第二步：输入WLAN信息。



第三步：导航到选Security项卡并禁用Layer 2 Security Mode和启用MAC Filtering。从Authorization List ，选择上一步中创建的授权方法。？？然后单击.Save & Apply to Device



CLI：

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

策略配置文件配置

必须在策略配置文件中启用aaa-override，以确保每个SSID的mac过滤正常工作。

9800 WLC上的策略配置文件配置

策略标签配置

9800 WLC上的策略标签

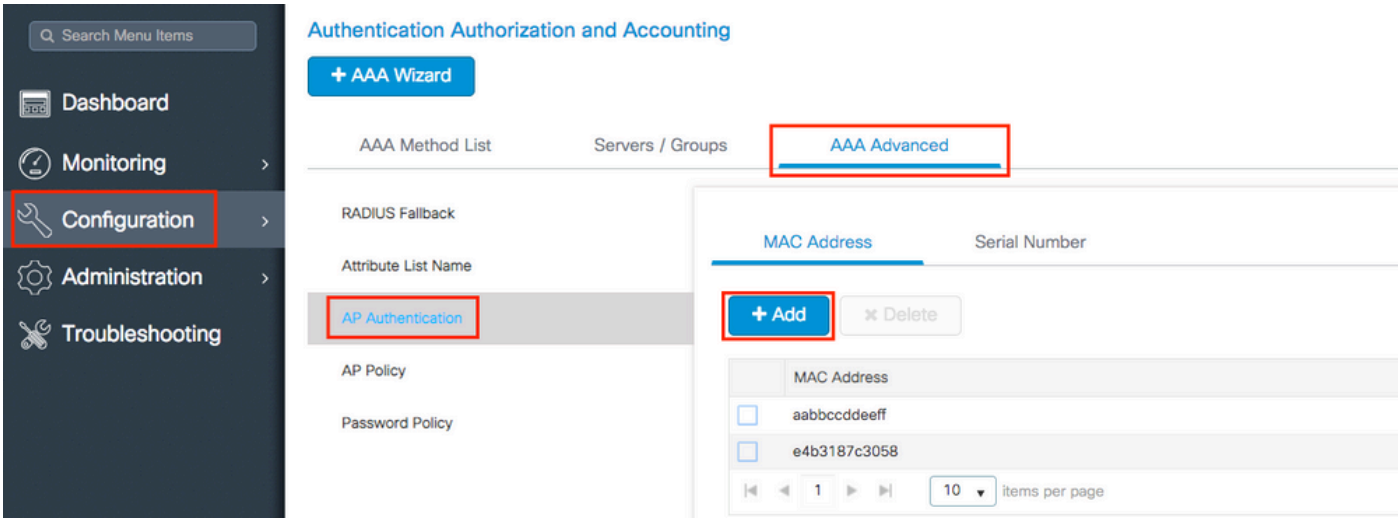
策略标记分配

9800 WLC上的策略标记分配

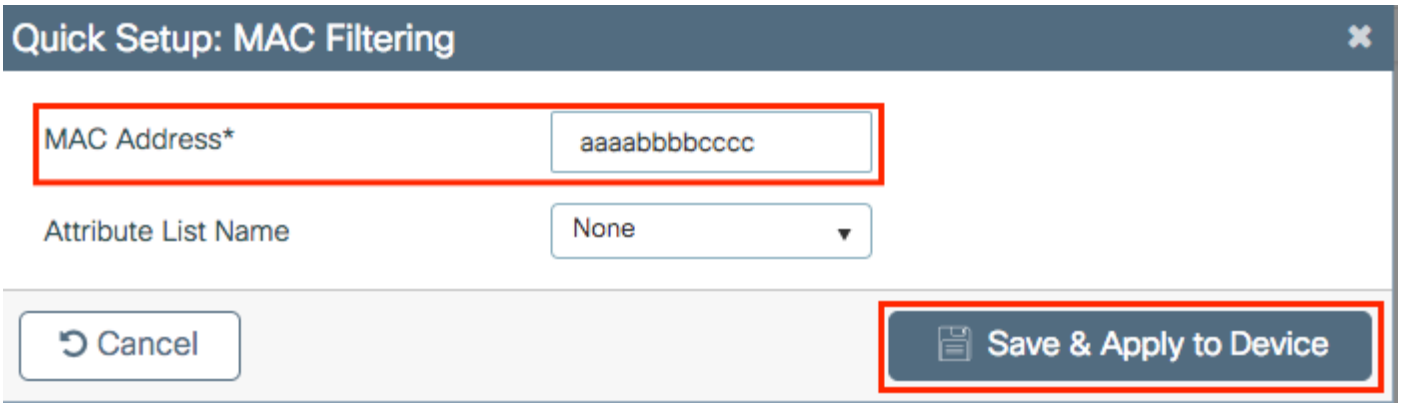
注册允许的MAC地址。

在WLC上本地注册MAC地址以进行本地身份验证

导航至Configuration > Security > AAA > AAA Advanced > AP Authentication > + Add。



写下不带分隔符的所有小写形式的mac地址，然后单击Save & Apply to Device。



注意：在17.3之前的版本中，Web UI将您键入的任何MAC格式更改为图中所示的“无分隔符”格式。在17.3及更高版本中，Web UI尊重您输入的任何设计，因此，不输入任何分隔符至关重要。增强漏洞Cisco Bug ID CSCvv43870跟踪对MAC身份验证的多种格式的支持。

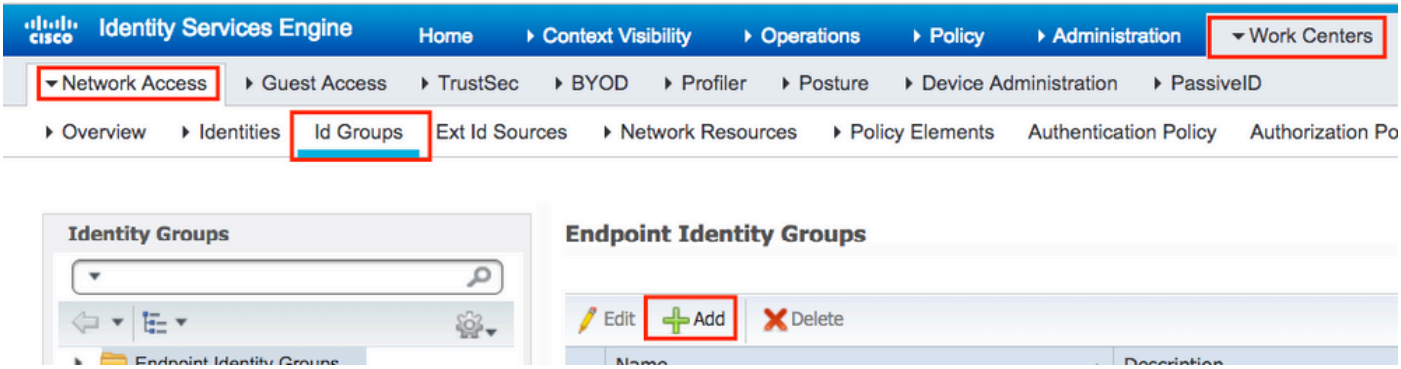
CLI：

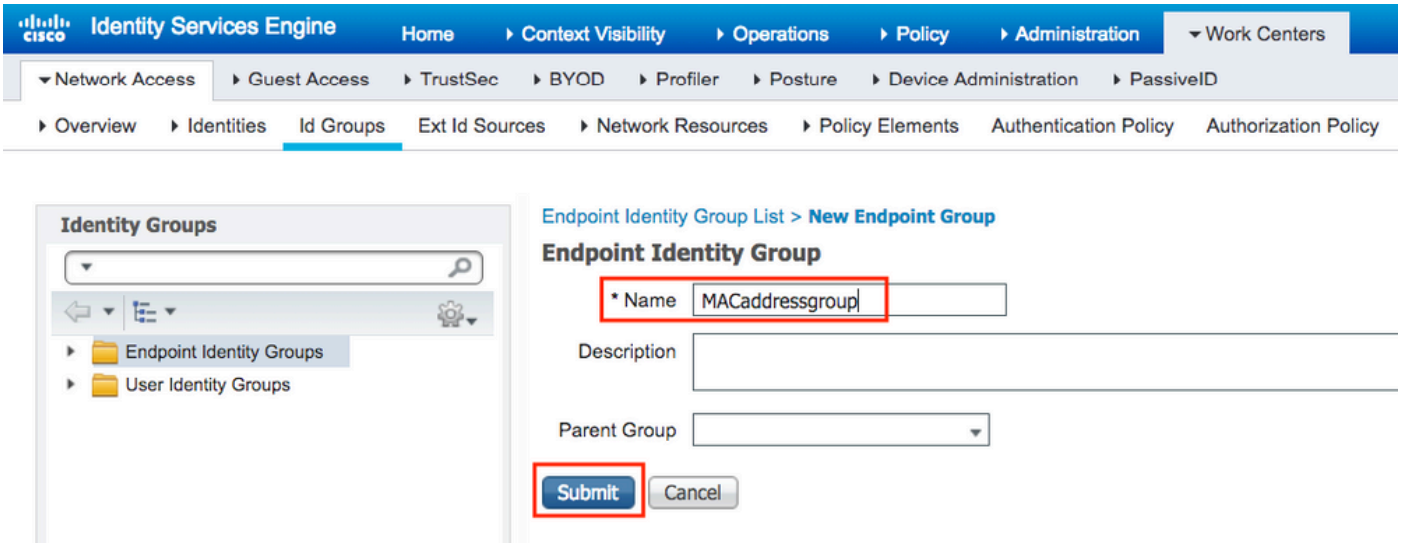
```
# config t
# username <aabbccddeeff> mac
```

在ISE终端数据库上输入MAC地址

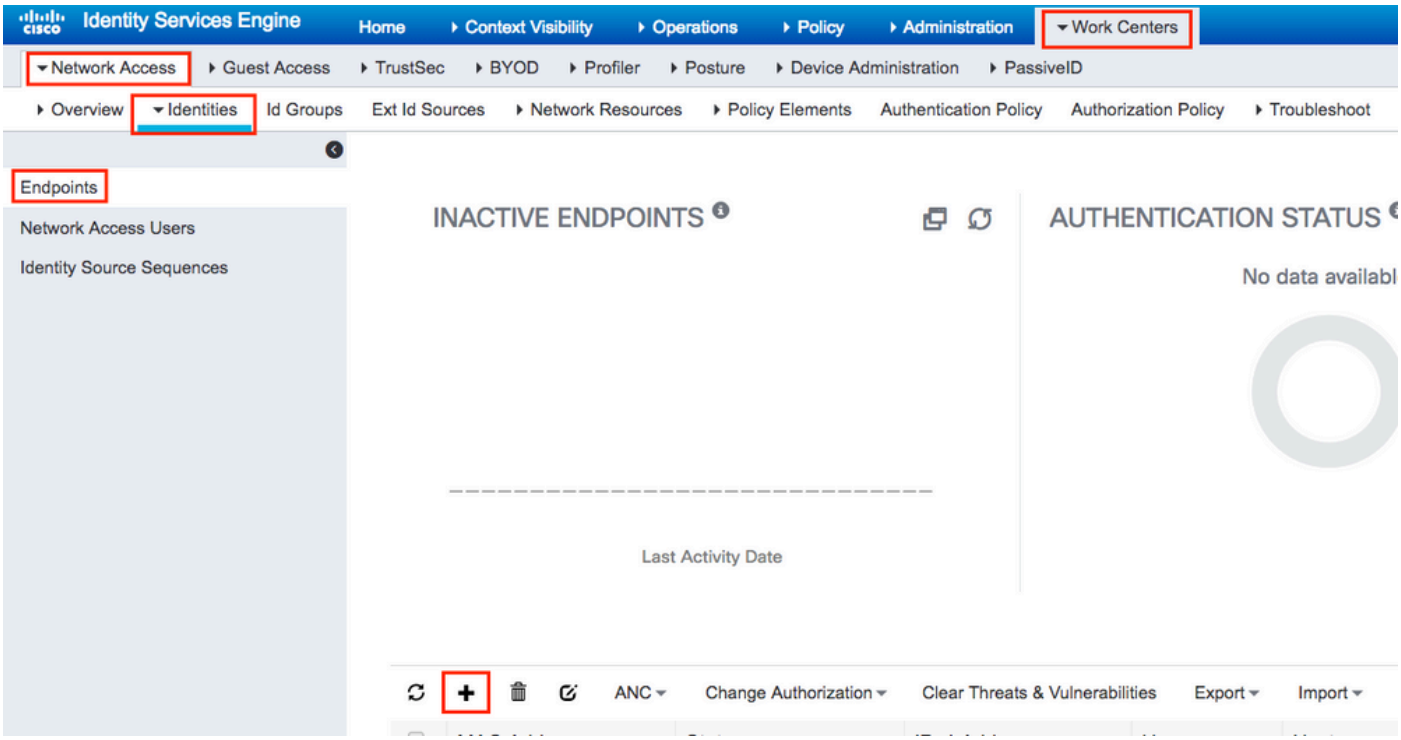
步骤1.（可选）创建新的终端组。

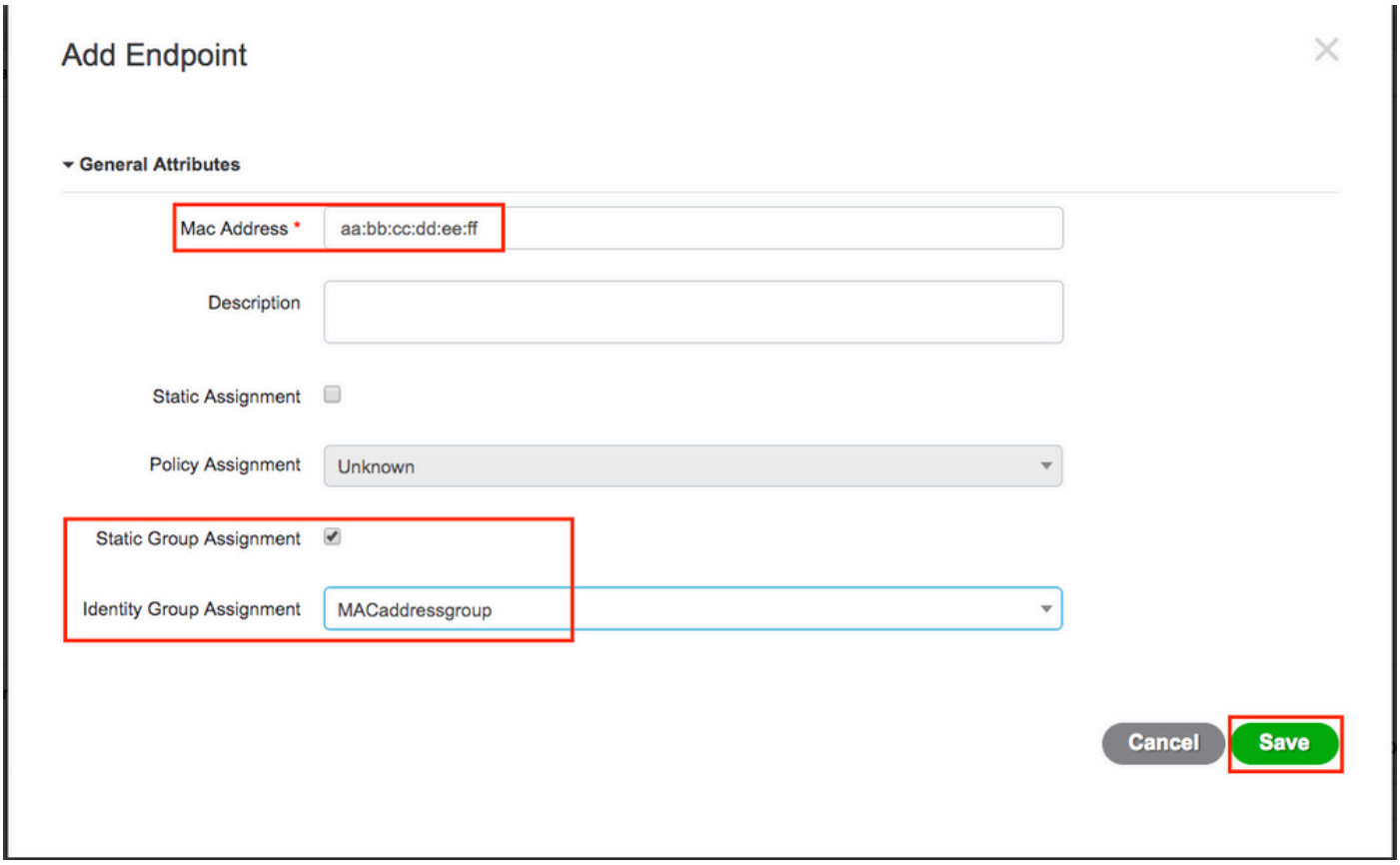
导航至Work Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add。





第二步：导航至Work Centers > Network Access > Identities > Endpoints > +Add。





ISE 配置

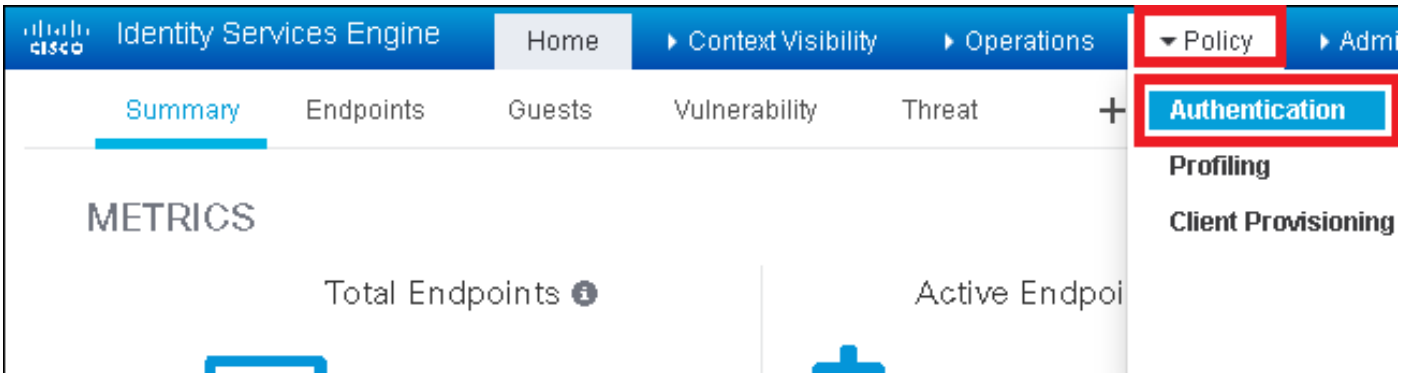
将 9800 WLC 添加到 ISE.

请阅读以下链接中的说明：向ISE声明WLC。

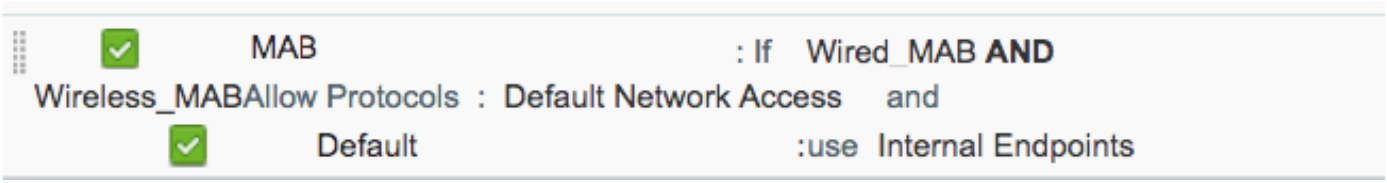
创建身份验证规则

身份验证规则用于验证用户的凭证是否正确（验证用户是否真的如其所言）并限制允许其使用的身份验证方法。

步骤1:导航至Policy > Authentication ，如图所示。
确认ISE上存在默认MAB规则。



第二步：验证MAB的默认身份验证规则已存在：

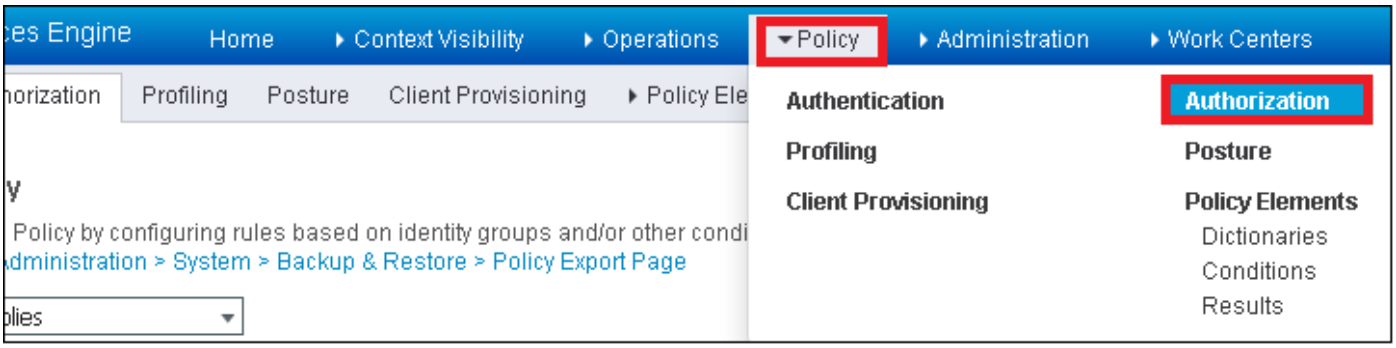


如果没有，您可以在点击时添加一个新链接Insert new row above。

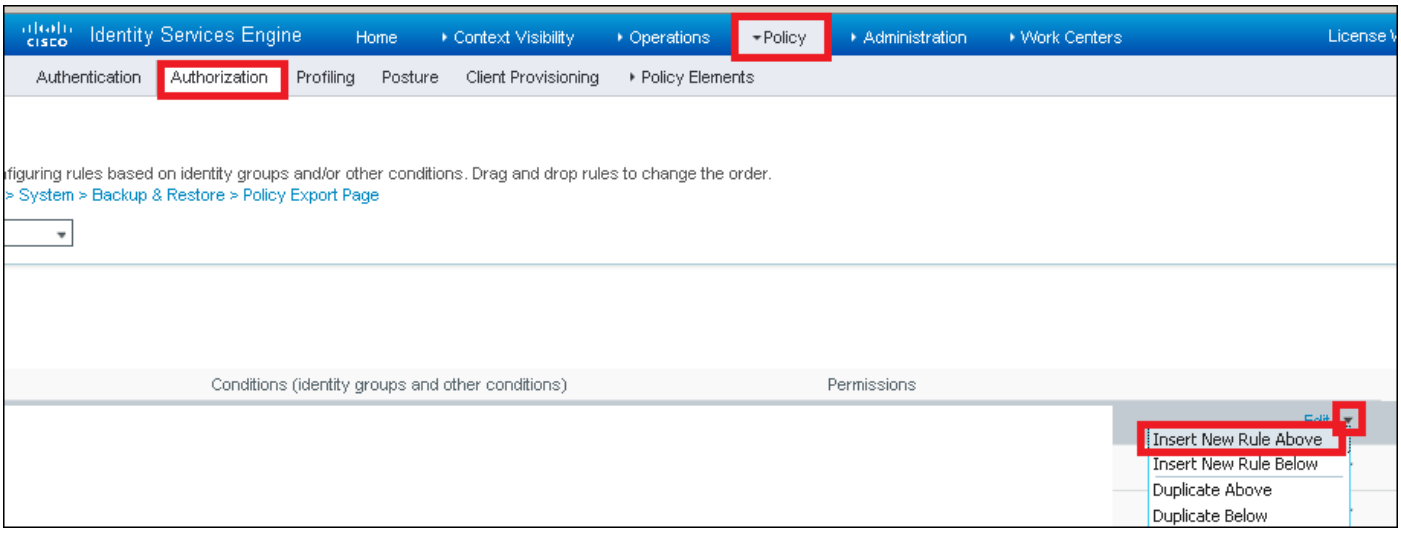
授权规则创建

授权规则负责确定将哪些权限（哪个授权配置文件）结果应用于客户端。

步骤1:导航至Policy > Authorization ，如图所示。

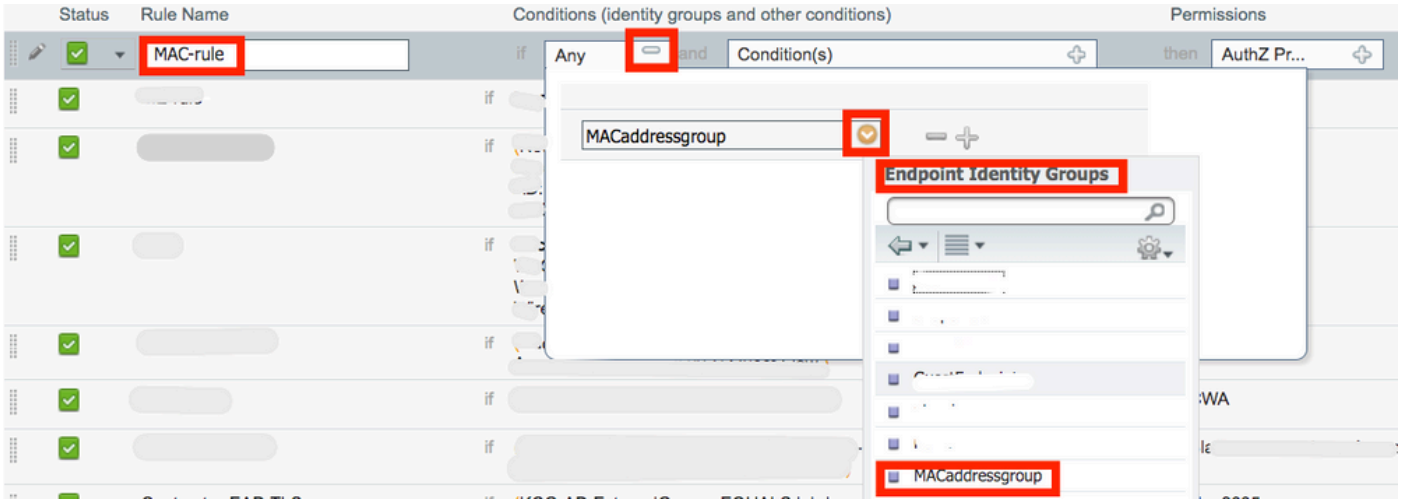


第二步：插入新规则，如图所示。

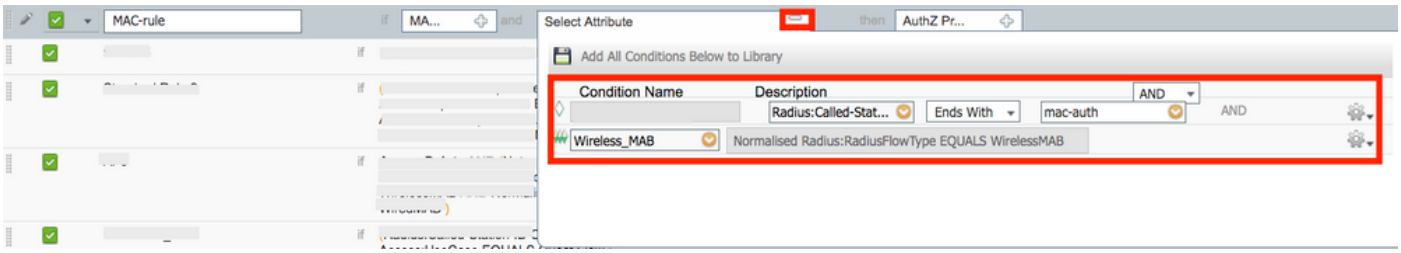


第三步：输入值。

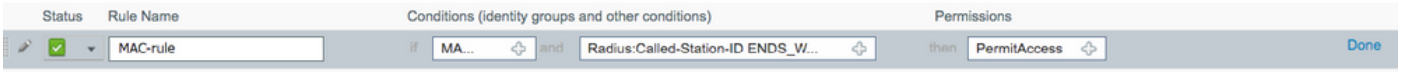
首先，选择规则的名称以及终端存储位置(MACaddressgroup)的身份组，如图所示。



之后，选择执行授权流程的其他条件以属于此规则。在本示例中，如果授权进程使用无线MAB，并且其被叫站ID（SSID的名称）以图中所示结mac-auth尾，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Authorization profilePermitAccess（在本例中）。单击Done并保存它。



验证

您可以使用以下命令验证当前配置：

```
# show wlan { summary | id | name | all }
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

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，并且您可以在发生事故或故障情况后查看其日志。

注：虽然这取决于生成的日志量，但您可以返回几小时到几天。

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

步骤1:检查控制器的当前时间，以便跟踪从问题发生时开始的日志。

```
# 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的运行状况和错误（如果有）。

```
# 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 Tracing Configs:


Packet Infra debugs:

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

> 注：如果看到列出了任何条件，则意味着遇到启用条件（MAC地址、IP地址等）的所有进程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：如果测试中的MAC地址未作为步骤3.中的条件列出，请收集特定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。要启用条件调试，请阅读以下步骤。

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。

这些命令用于开始监控所提供的 MAC 地址，持续 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： 要一次监控多个客户端，请对每个mac地址运行debug wireless mac 命令。

注意:您不会在终端会话上看到客户端活动的输出，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>
```

一旦监控时间过长或调试无线停止，9800 WLC将生成一个本地文件，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。 您可以将复制到ra trace .log外部服务器，或者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，因为您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。与Cisco TAC联系，以帮助分析这些跟踪。

您可以将复制到ra-internal-FILENAME.txt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。

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）。