

为安全防火墙机箱管理器(FCM)配置ISE RADIUS身份验证

目录

简介

本文档介绍如何为带有ISE的Secure Firewall Chasis Manager配置RADIUS授权/身份验证访问的过程。

先决条件

要求

思科建议了解以下主题：

- 安全防火墙机箱管理器(FCM)
- 思科身份服务引擎(ISE)
- RADIUS 身份验证

使用的组件

- 思科Firepower 4110安全设备FXOS v2.12
- 思科身份服务引擎(ISE) v3.2补丁4

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。

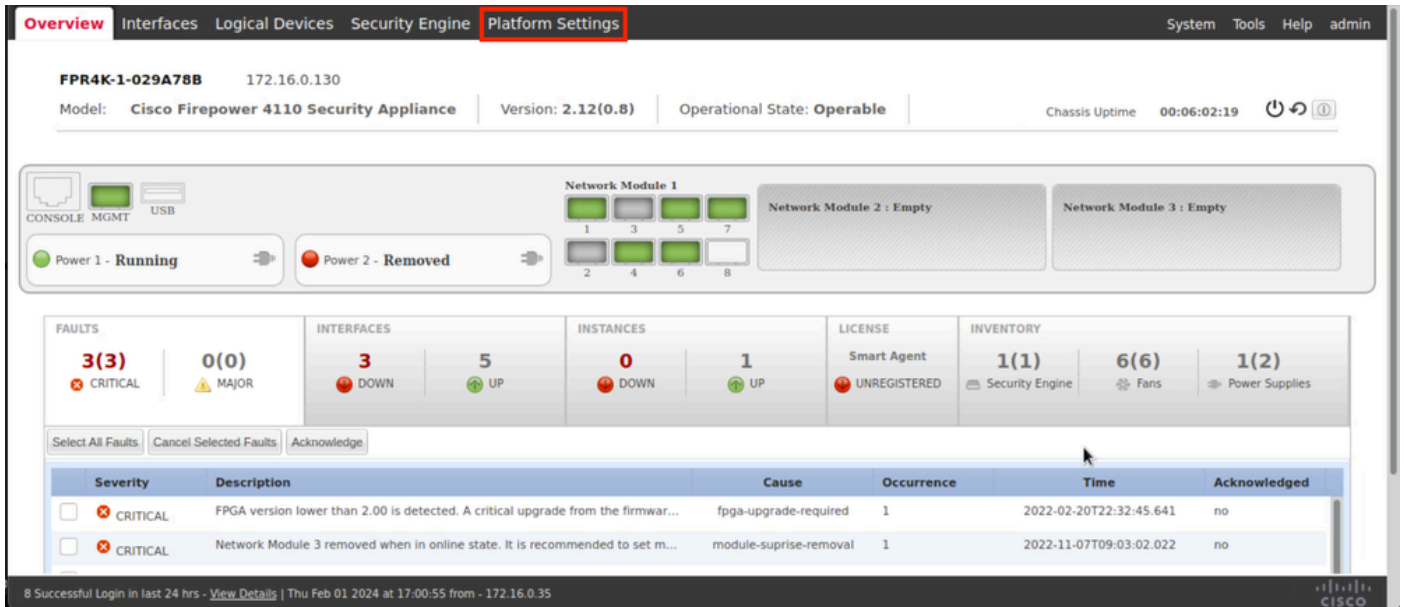
配置

配置

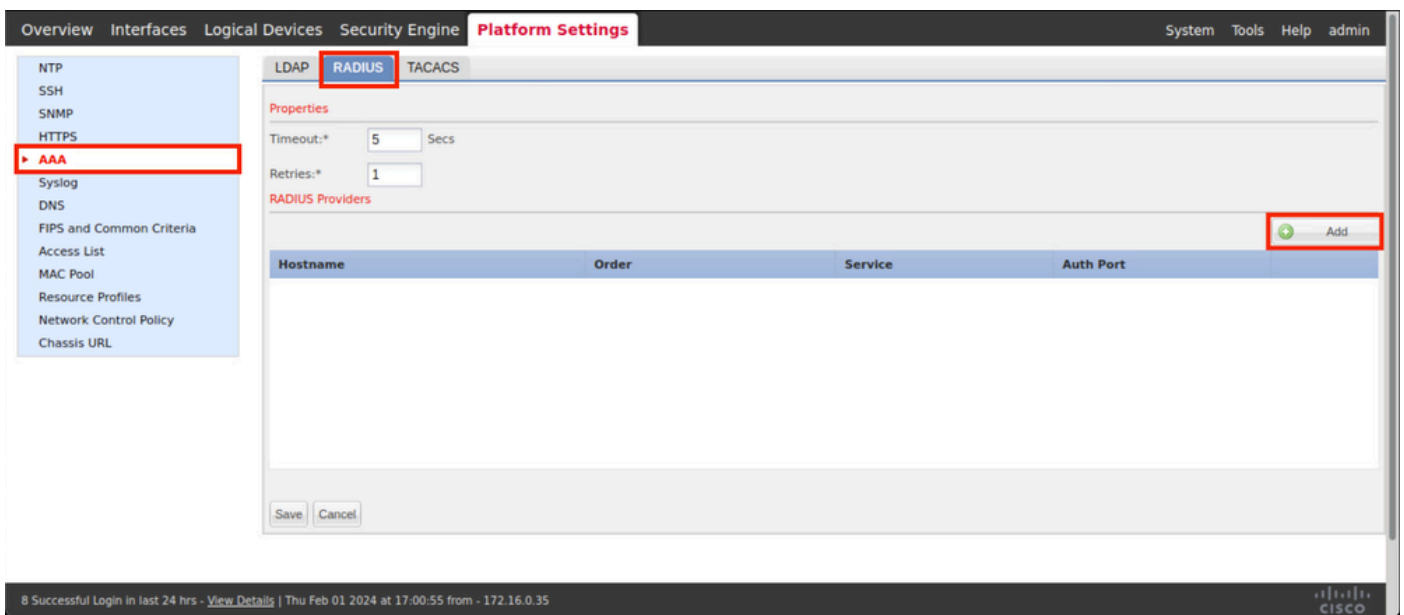
安全防火墙机箱管理器

步骤1:登录到Firepower机箱管理器GUI。

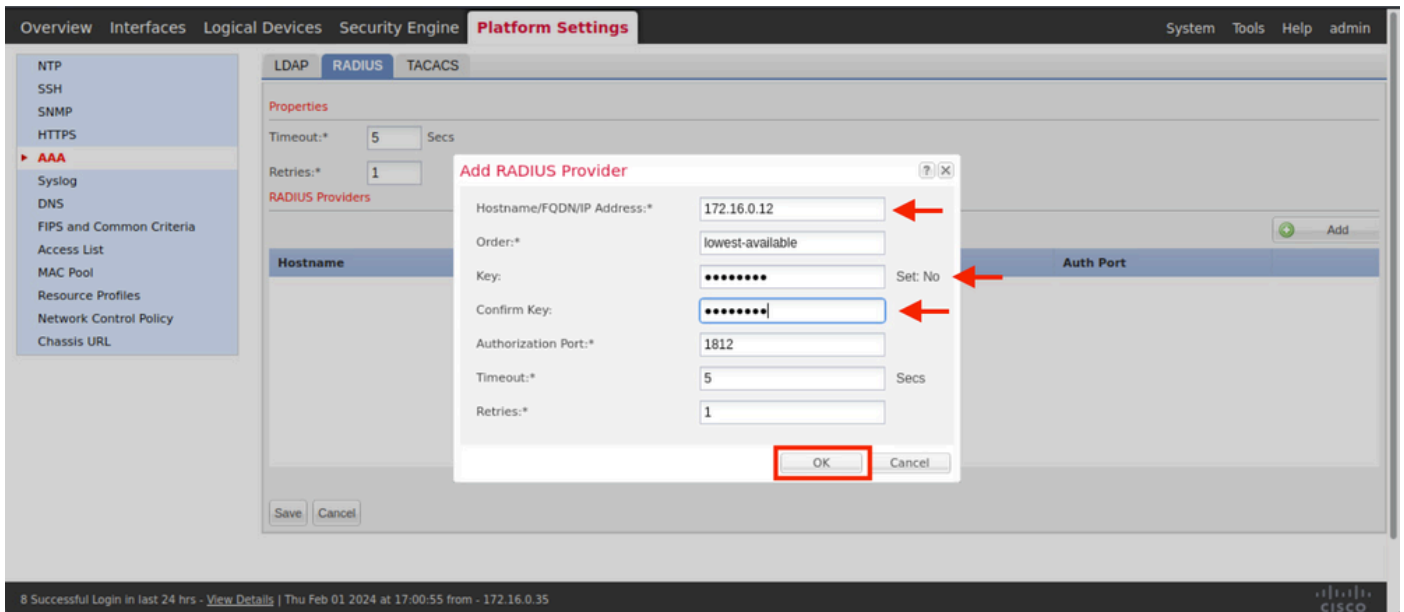
第二步：导航到平台设置



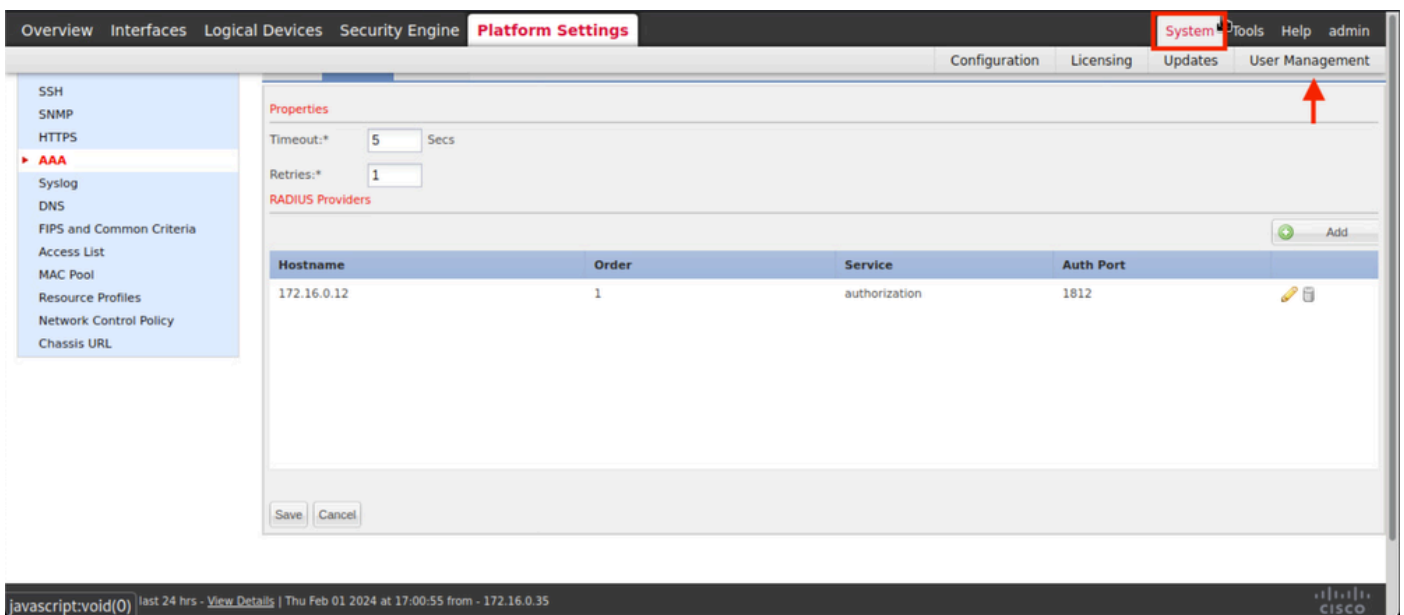
第三步：从左侧菜单中单击over AAA。选择Radius并Add一个新的RADIUS提供程序。



第四步：使用Radius提供程序的请求信息填写提示菜单。Click OK.



第五步：导航到系统>用户管理



第六步：点击Settings选项卡，将下拉菜单中的Default Authentication设置为Radius，然后向下滚动并保存配置。


Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication

Local *Local is fallback authentication method

Local
RADIUS 
LDAP
TACACS
None

Console Authentication

Remote User Settings

Remote User Role Policy

Local User Settings

Password Strength Check Enable

History Count (0-disabled,1-15)

Change Interval (1-730 hours)

Change Count (1-10)

No Change Interval (1-730 hours)

Days until Password Expiration (0-never,1-9999 days)

Password Expiration Warning Period (0-9999 days)

Expiration Grace Period (0-9999 days)

Password Reuse Interval (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet) (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

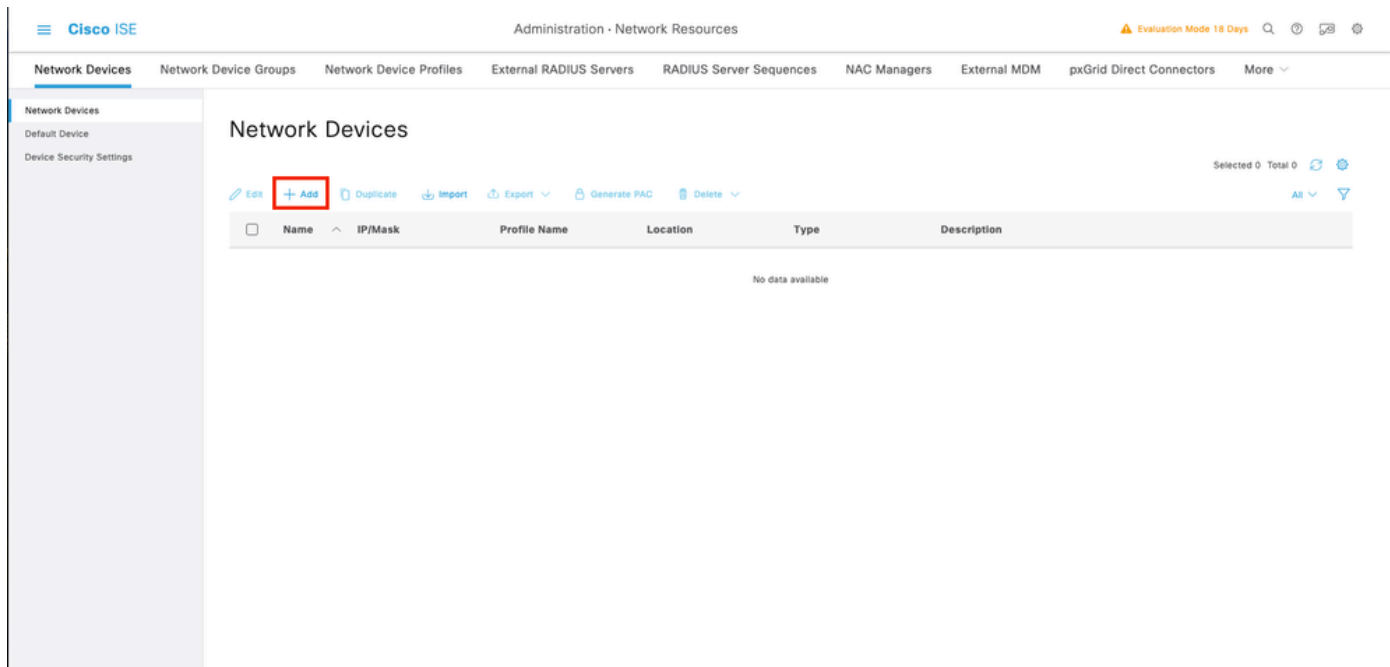
CISCO

注意：FCM配置此时已完成。

身份服务引擎

步骤1: 添加新的网络设备。

导航到位于左上角≡汉堡图标> Administration > Network Resources > Network Devices > +Add。

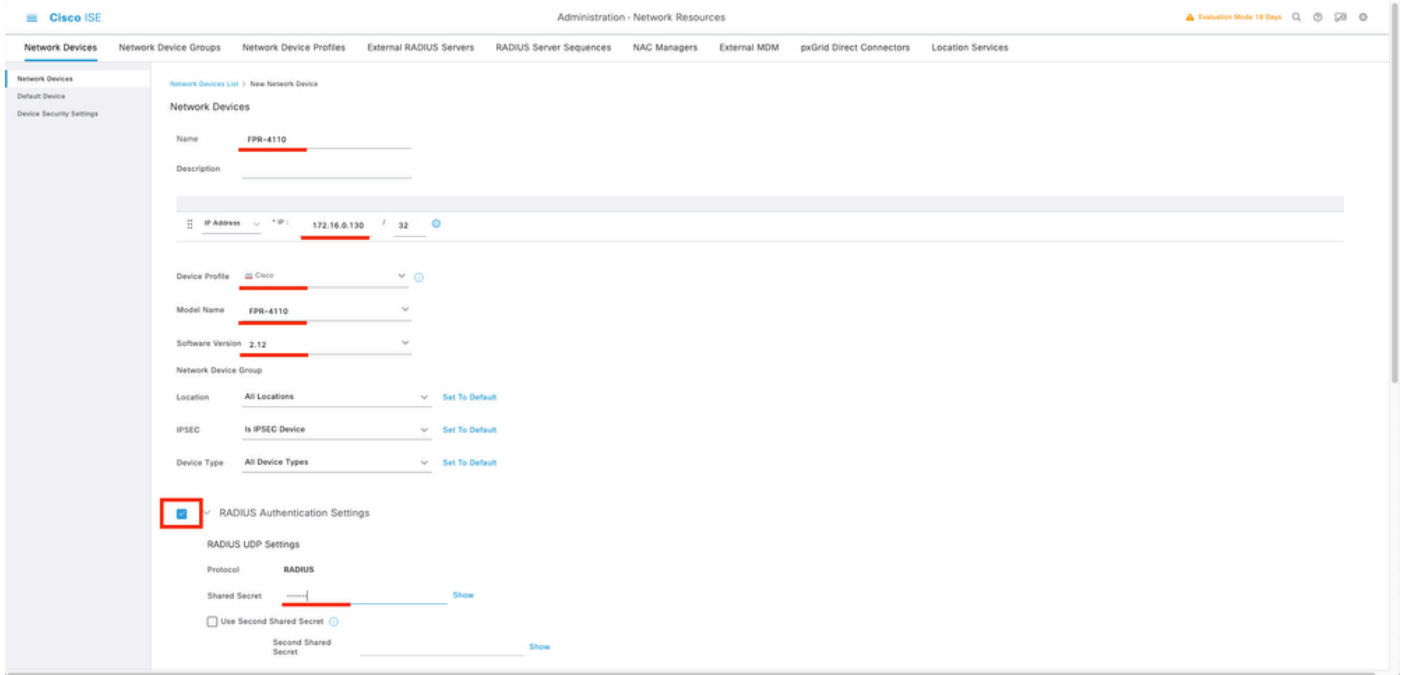


第二步：填写有关新网络设备信息的请求参数。

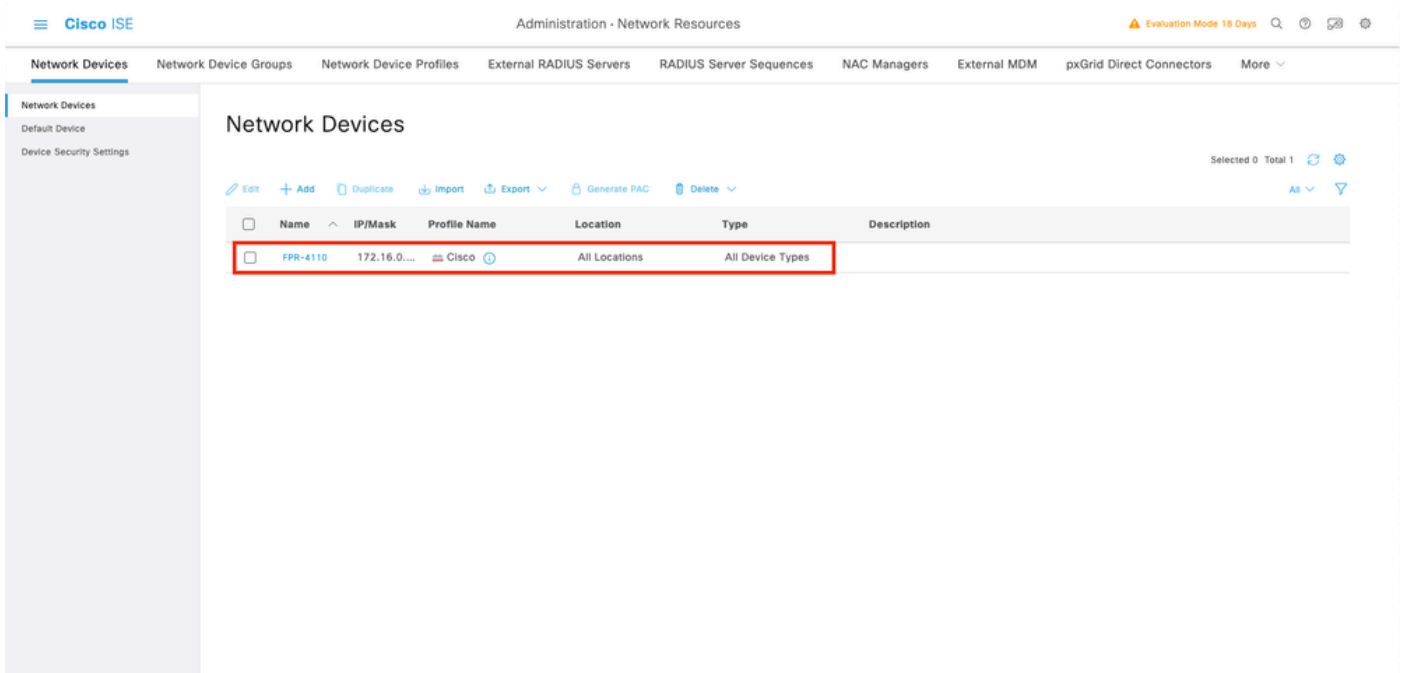
2.1选中RADIUS复选框

2.2配置与FCM Radius配置相同的共享密钥。

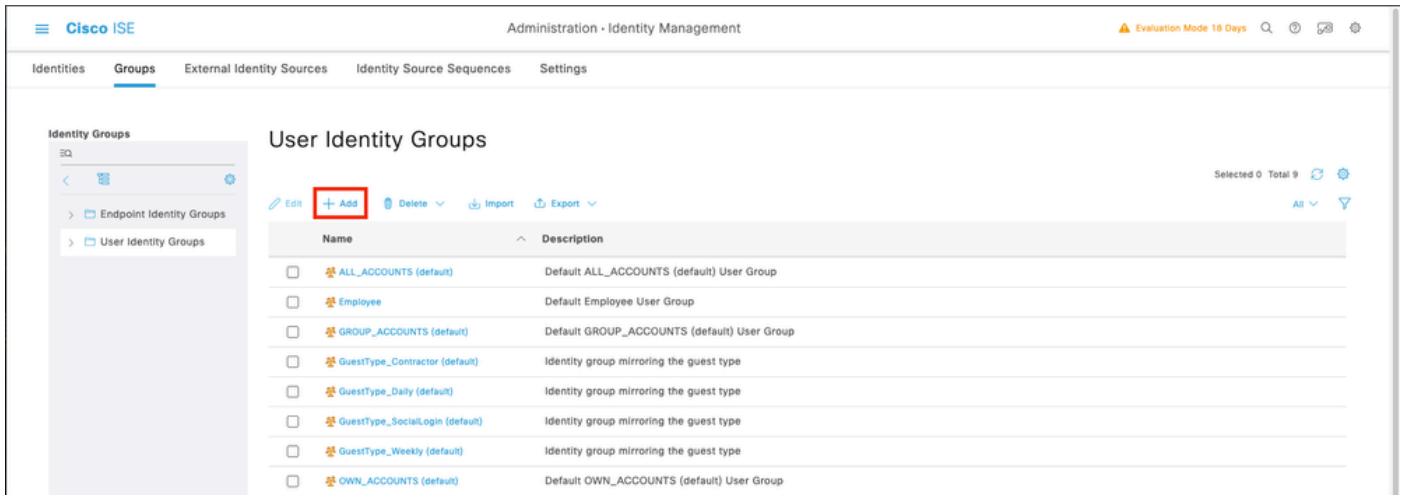
2.1向下滚动并点击Submit。



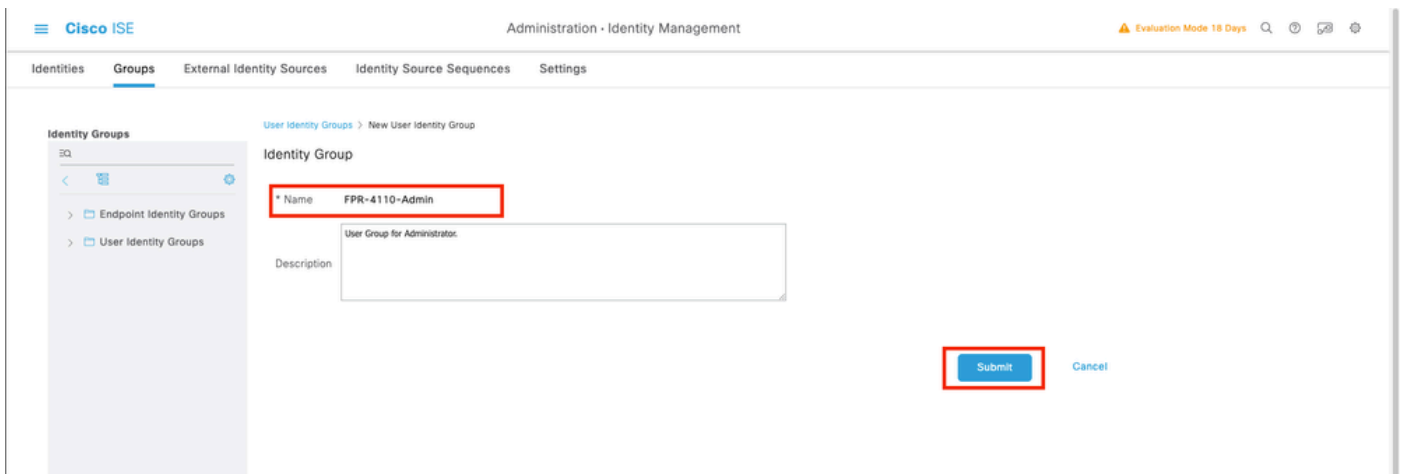
第三步：验证新设备是否显示在Network Devices下。



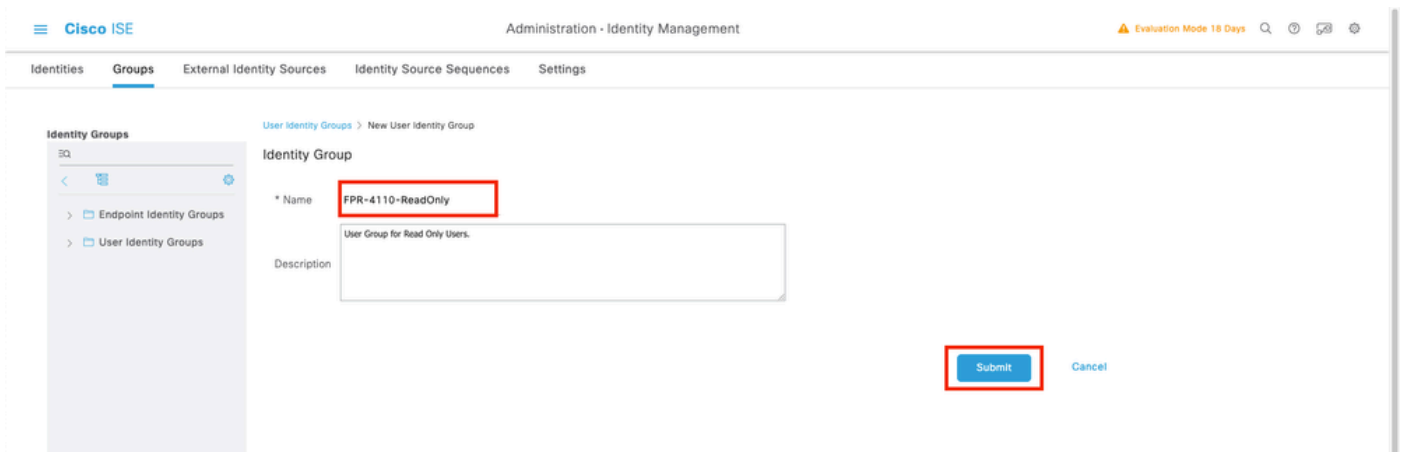
第四步：创建所需的用户身份组。导航到位于左上角≡汉堡图标> Administration > Identity Management > Groups > User Identity Groups > + Add



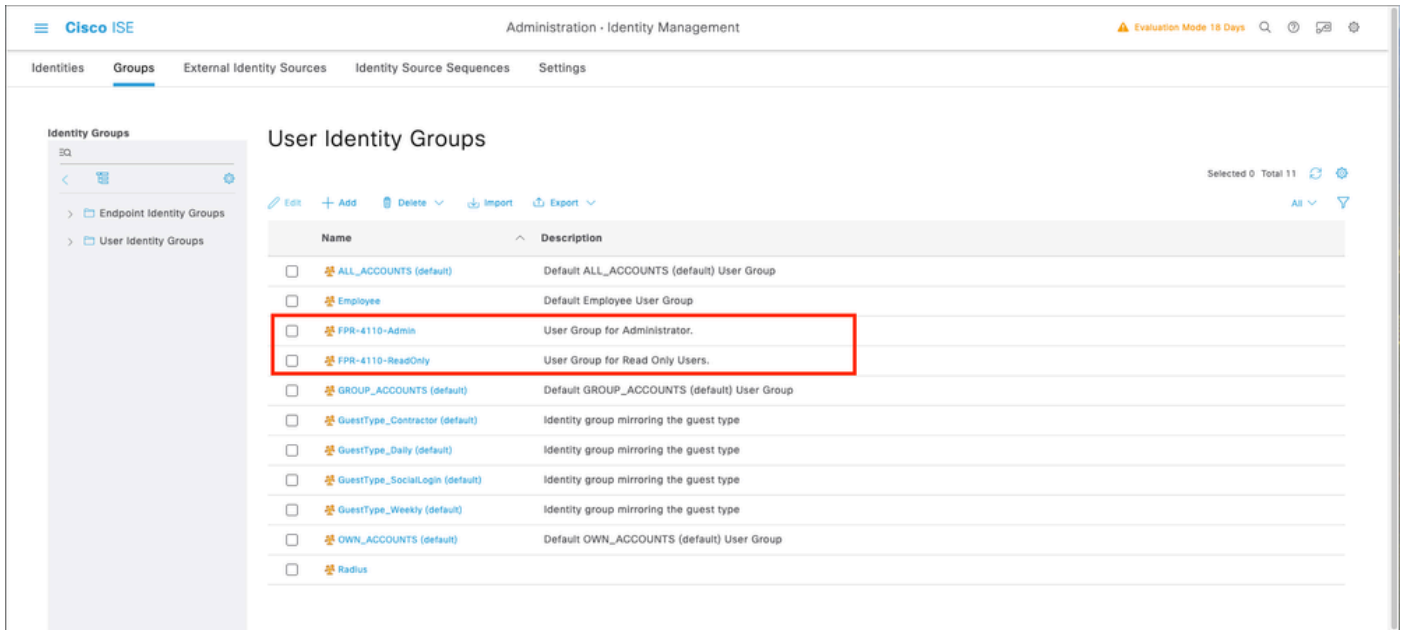
第五步：为管理员用户身份组设置名称，然后点击提交以保存配置。



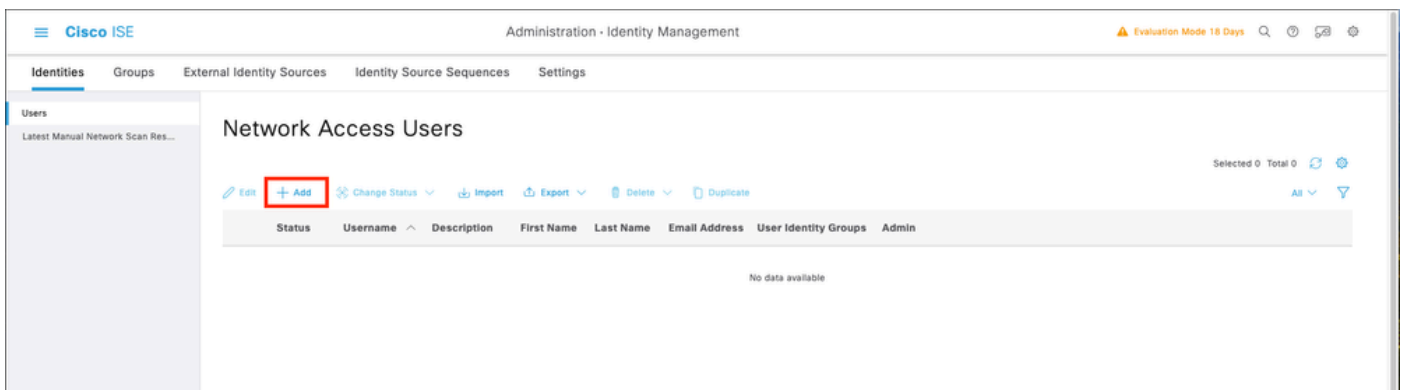
5.1对只读用户重复相同的过程。



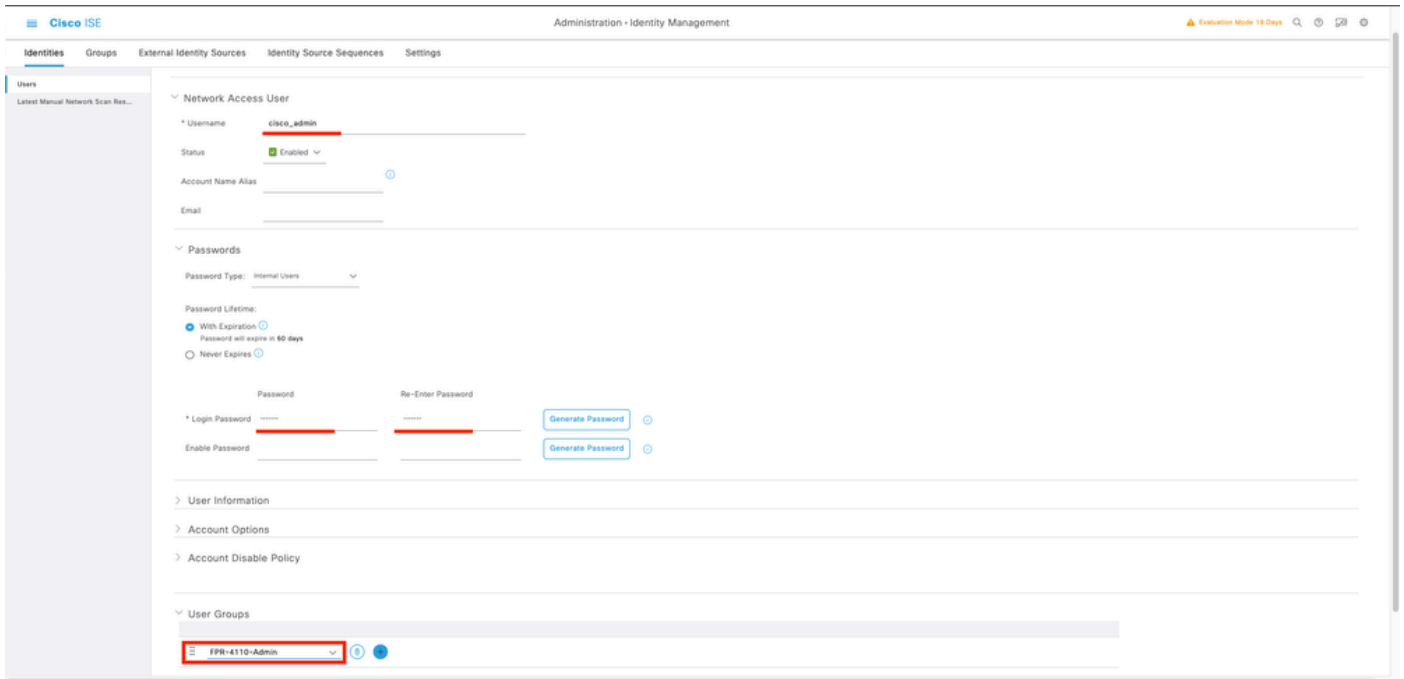
第六步：验证新的用户组显示在User Identity Groups下。



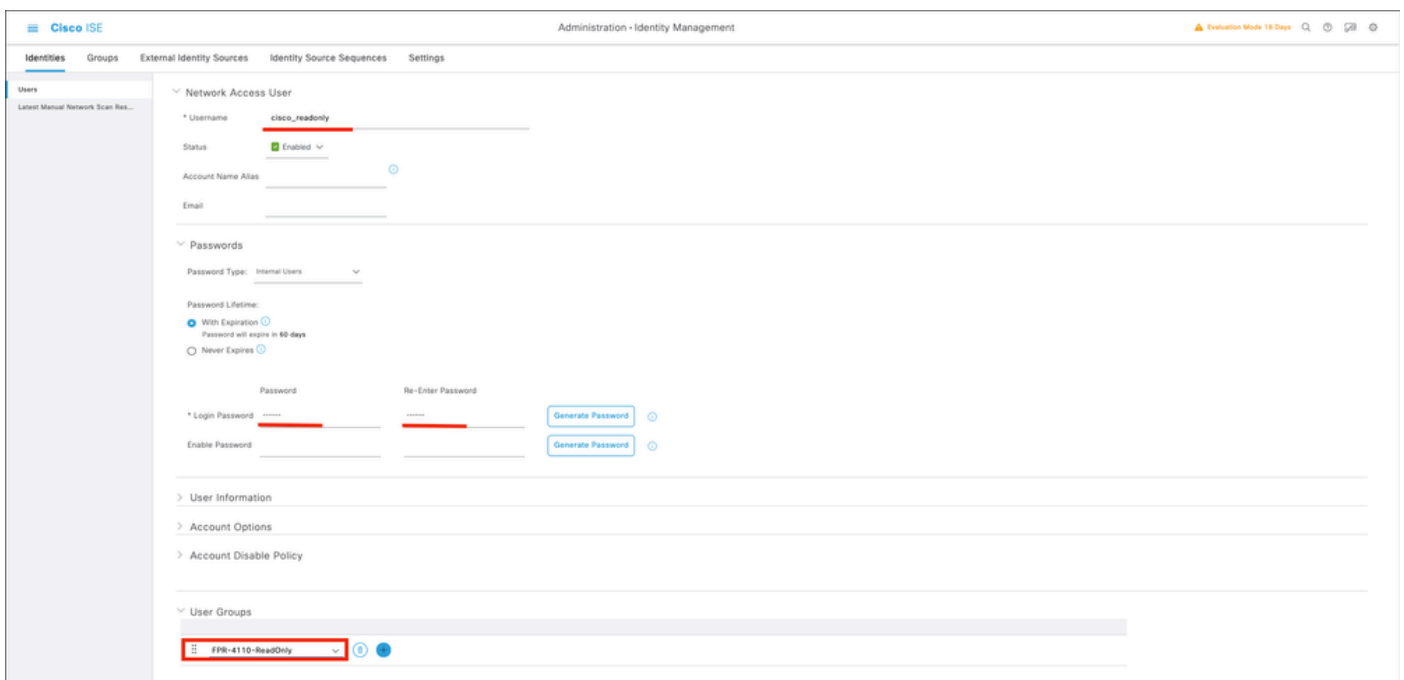
步骤 7. 创建本地用户并将其添加到其往来行组。 导航到汉堡图标≡ > Administration > Identity Management > Identities > + Add。



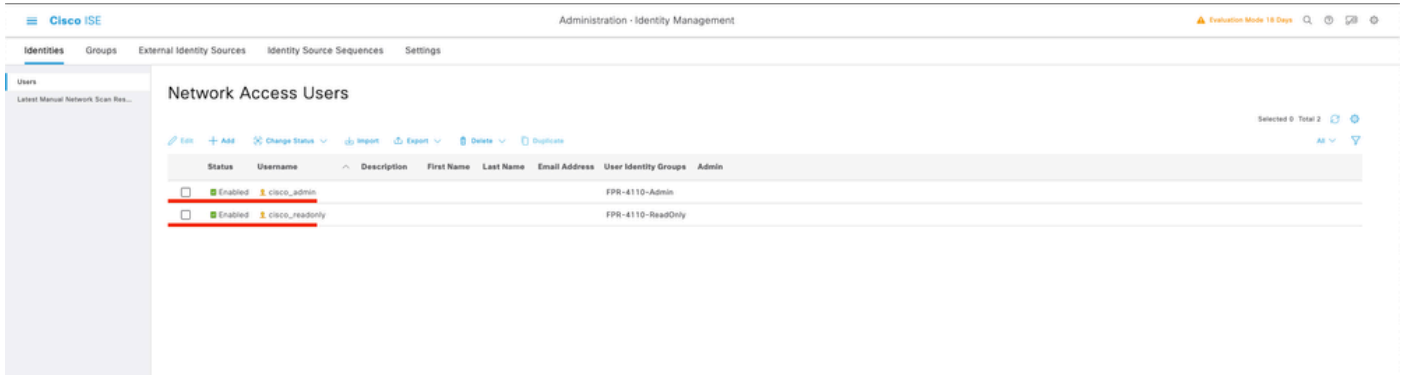
7.1 添加具有管理员权限的用户。设置名称和口令，并将其分配给FPR-4110-Admin，然后向下滚动并单击Submit以保存更改。



7.2添加具有只读权限的用户。设置名称和口令，并将其分配给FPR-4110-ReadOnly，然后向下滚动并单击Submit以保存更改。



7.3验证用户是否处于网络访问用户下。



第8步：创建管理员用户的授权配置文件。

FXOS机箱包括以下用户角色：

- Administrator —对整个系统的完全读写访问权限。默认情况下，为默认管理员帐户分配此角色，且无法更改。
- 只读-对系统配置的只读访问权限，没有修改系统状态的权限。
- 操作-对NTP配置、智能许可的Smart Call Home配置和系统日志（包括系统日志服务器和故障）的读写访问权限。对系统的其余部分具有读取访问权限。
- AAA -对用户、角色和AAA配置的读写访问。对系统其余部分的读取权限

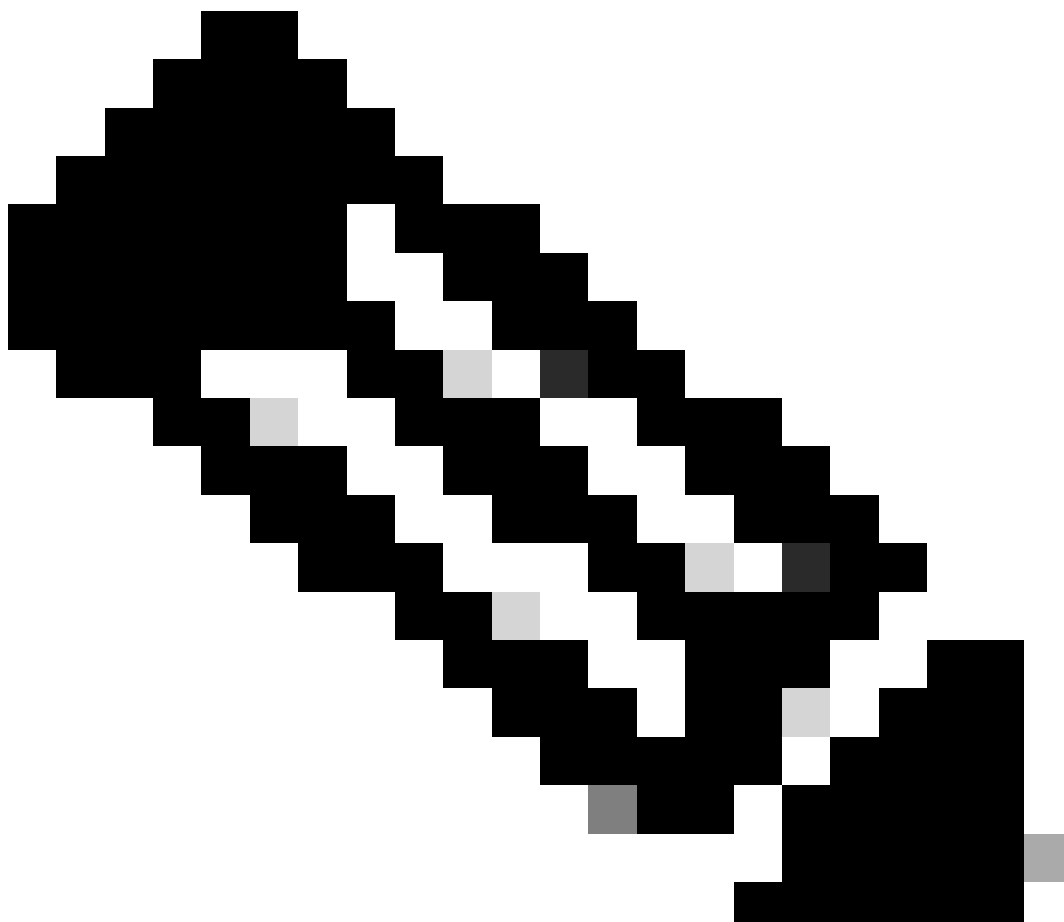
每个角色的属性：

```
cisco-av-pair=shell : roles="admin"
```

```
cisco-av-pair=shell : roles="aaa"
```

```
cisco-av-pair=shell : roles="operations"
```

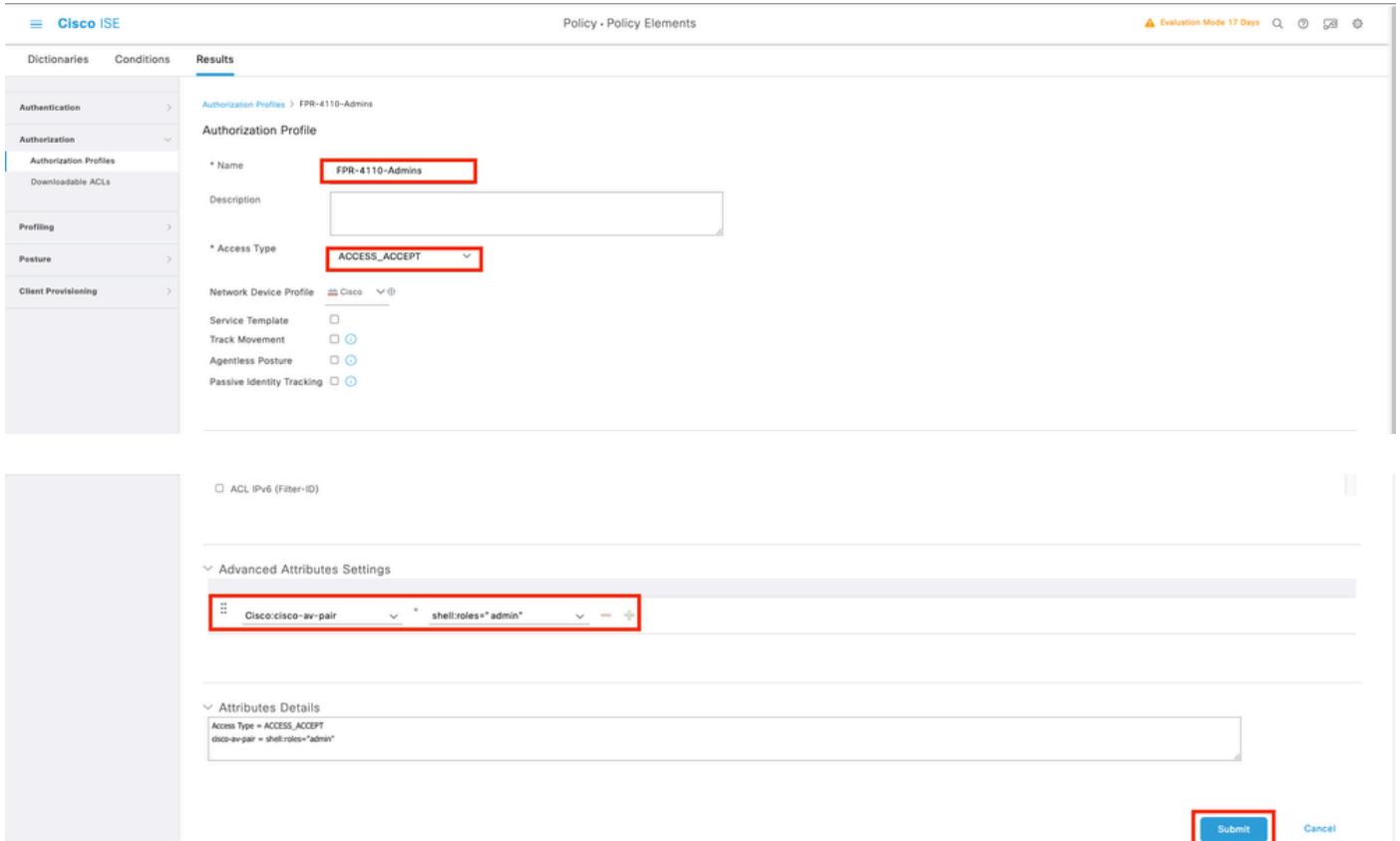
```
cisco-av-pair=shell : roles="read-only"
```



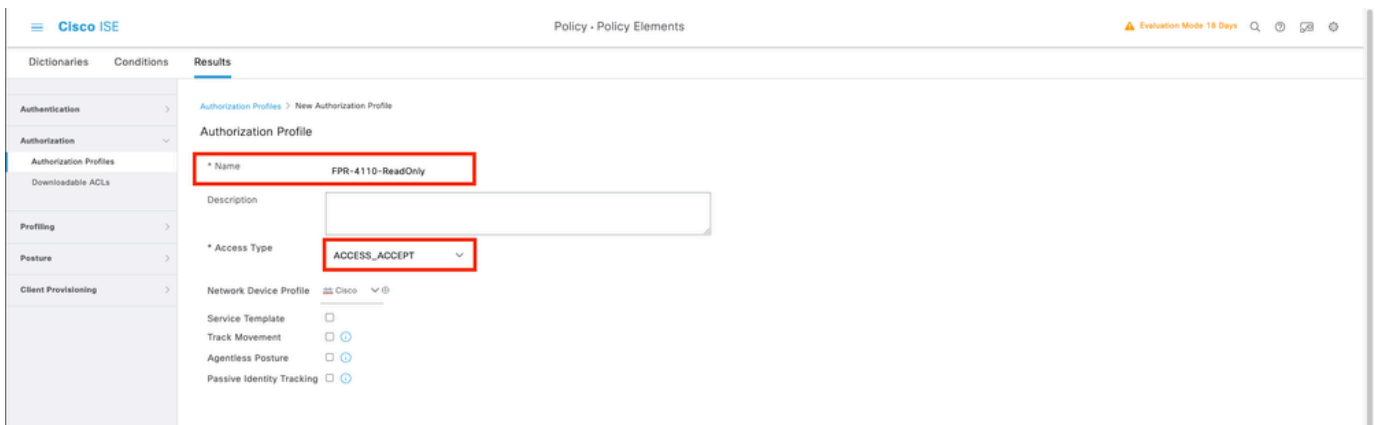
注意：此文档仅定义管理员和只读属性。

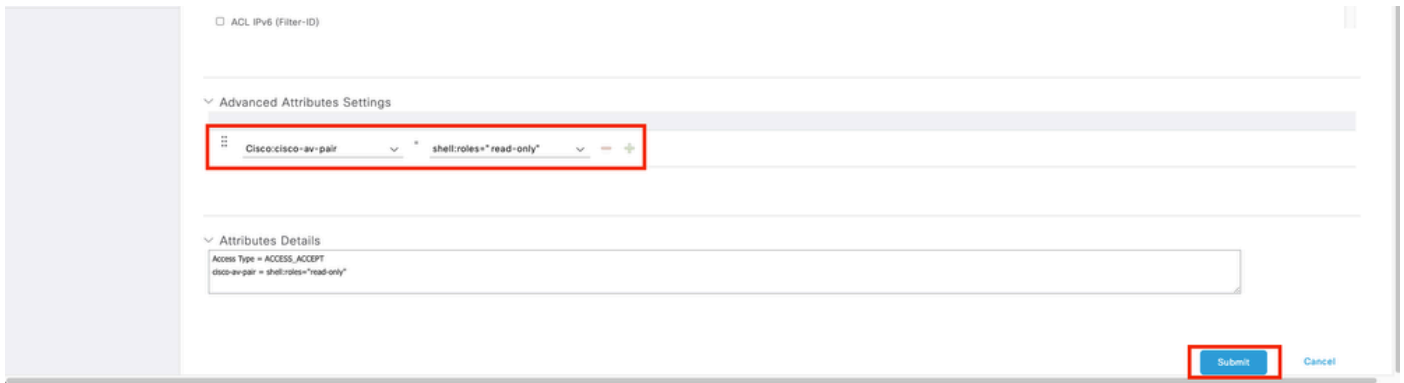
导航到汉堡图标 ≡ >策略>Policy元素>结果>授权>授权配置文件> +Add。

定义授权配置文件的名称，将访问类型保留为ACCESS_ACCEPT，然后在Advanced Attributes Settings下添加cisco-av-pair=shell : roles="admin"，然后点击Submit。

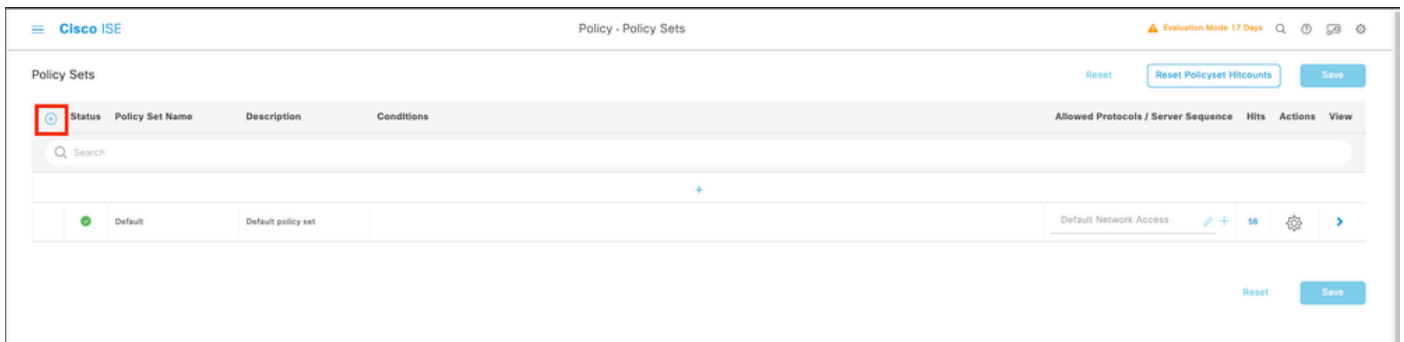


8.1 重复上述步骤为只读用户创建授权配置文件。这次使用值read-only Administrator创建RADIUS类。

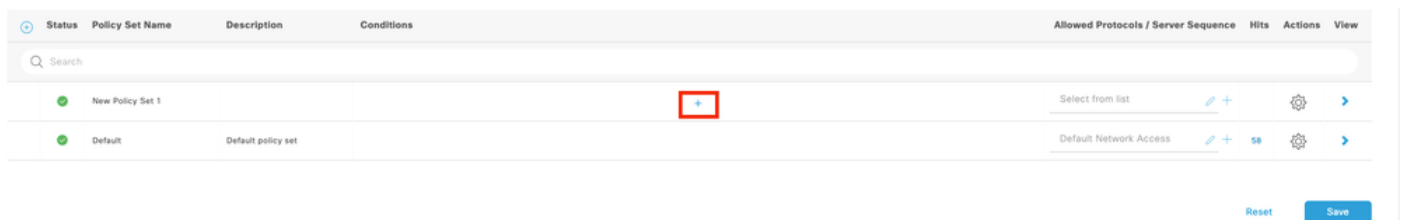




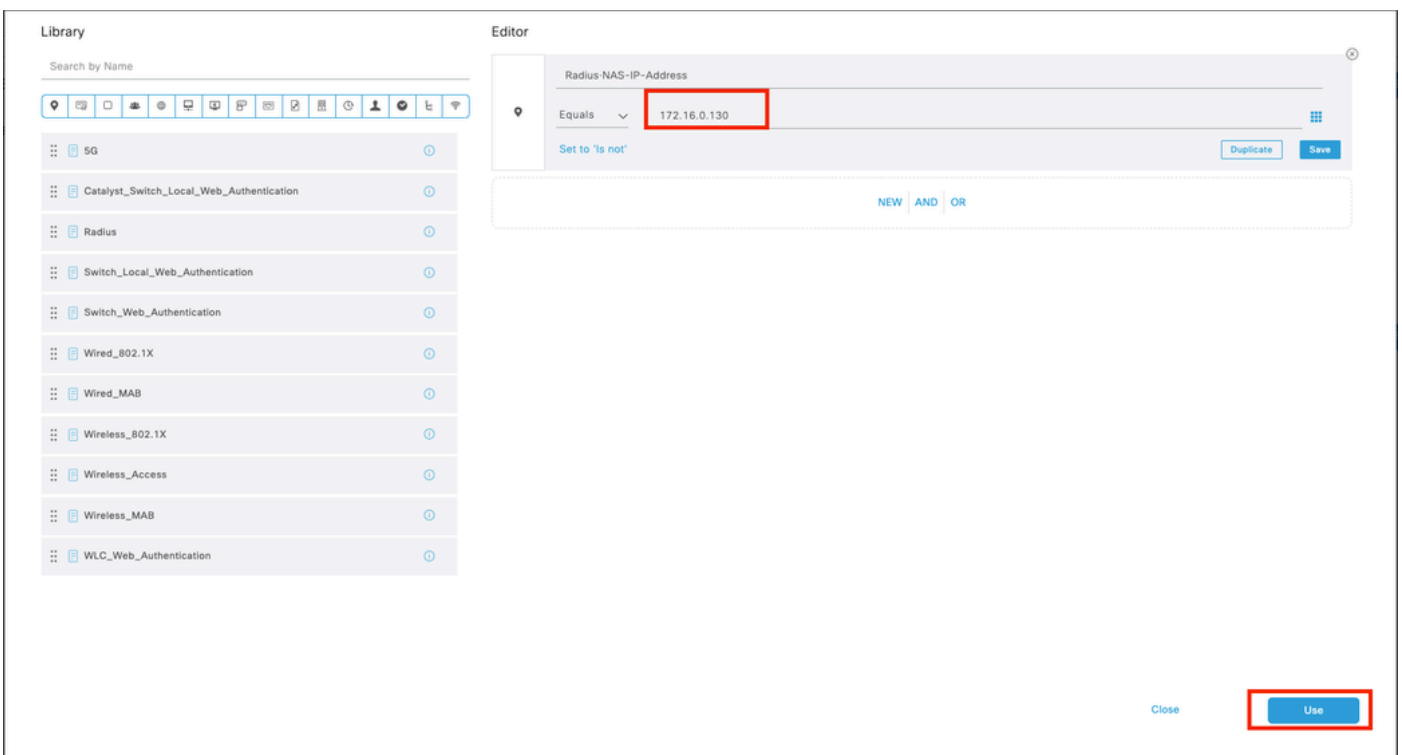
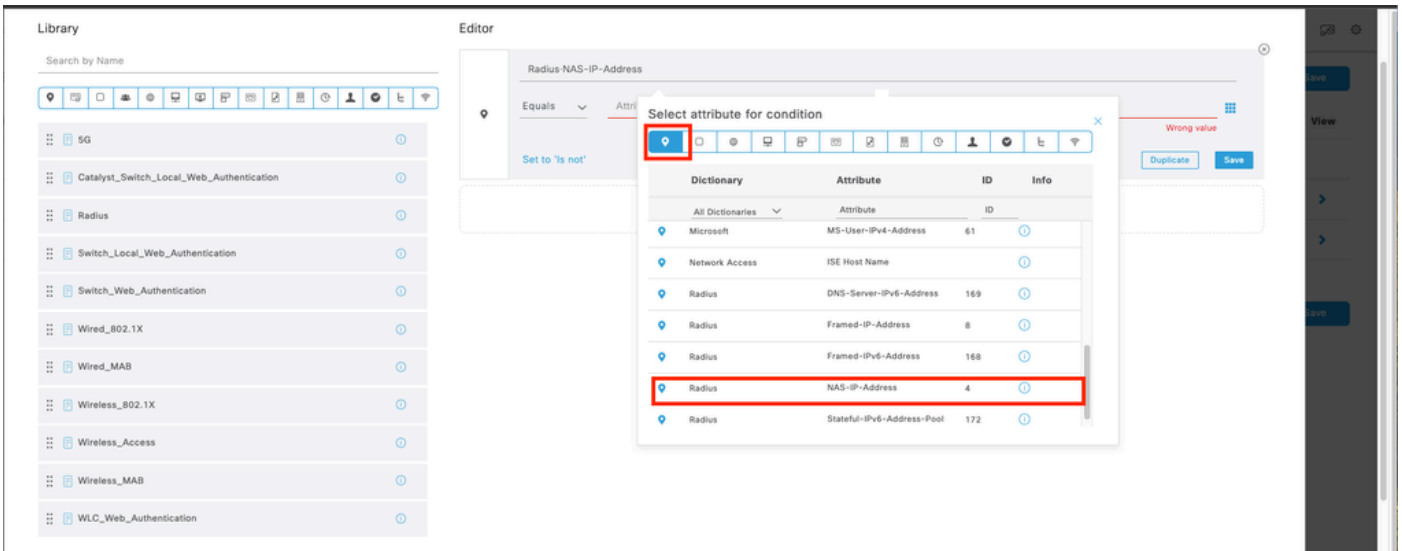
第9步：创建与FMC IP地址匹配的策略集。这是为了防止其他设备向用户授予访问权限。
导航到左上角的☰ > Policy > Policy Sets > Add图标符号。



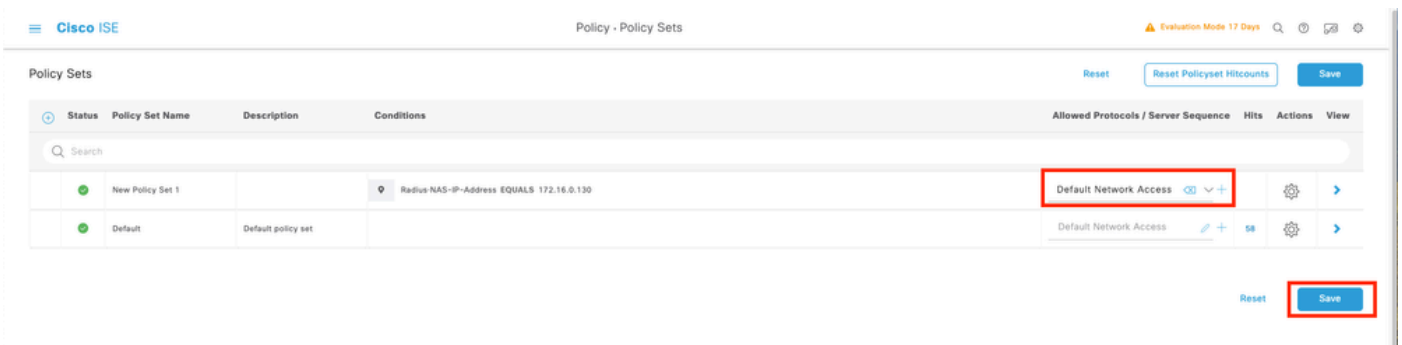
9.1 新行位于策略集的顶部。单击Add 图标以配置新条件。

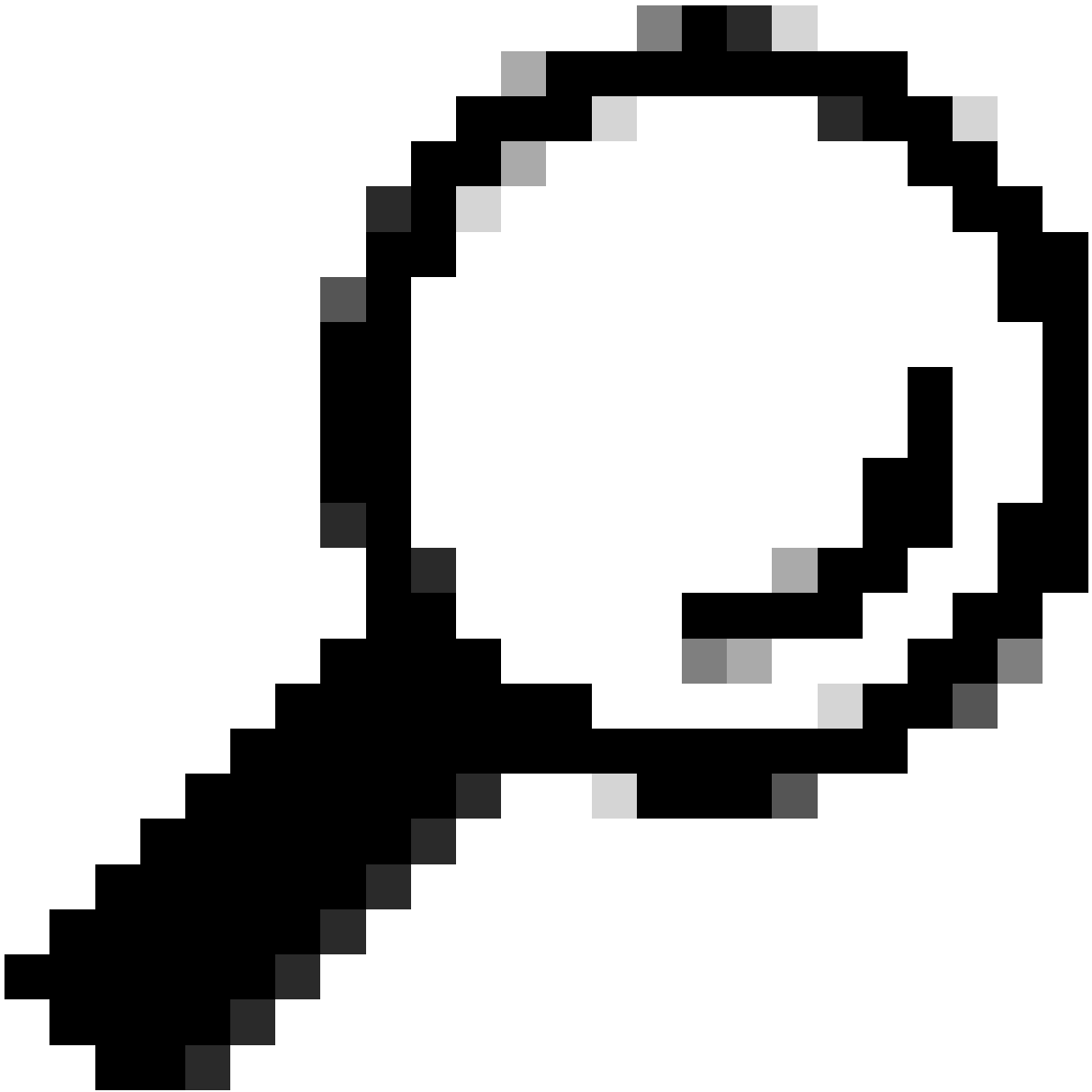


9.2 为RADIUS NAS-IP-Addressattribute添加与FCM IP地址匹配的顶部条件，然后点击使用。



9.3完成后单击Save。



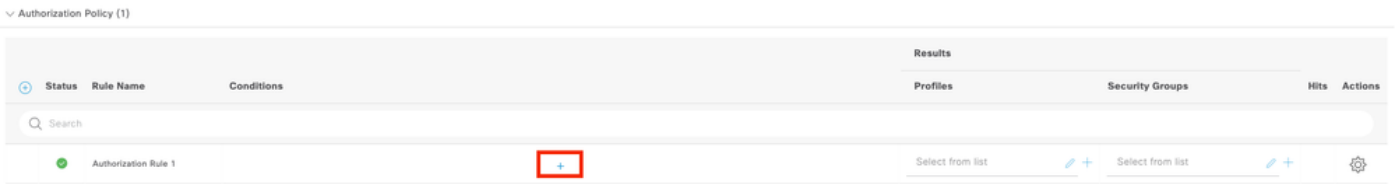


提示：在本练习中，我们允许使用默认网络访问协议列表。您可以创建一个新列表并根据需要缩小其范围。

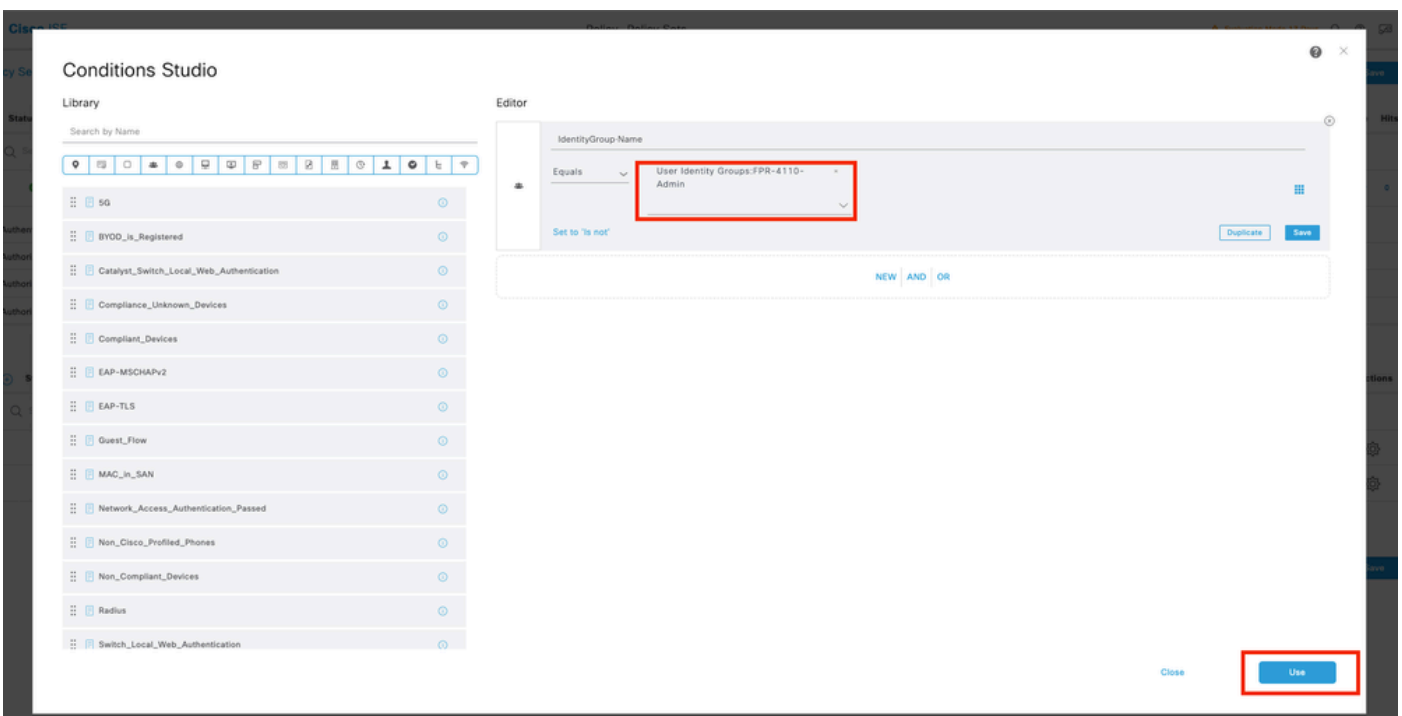
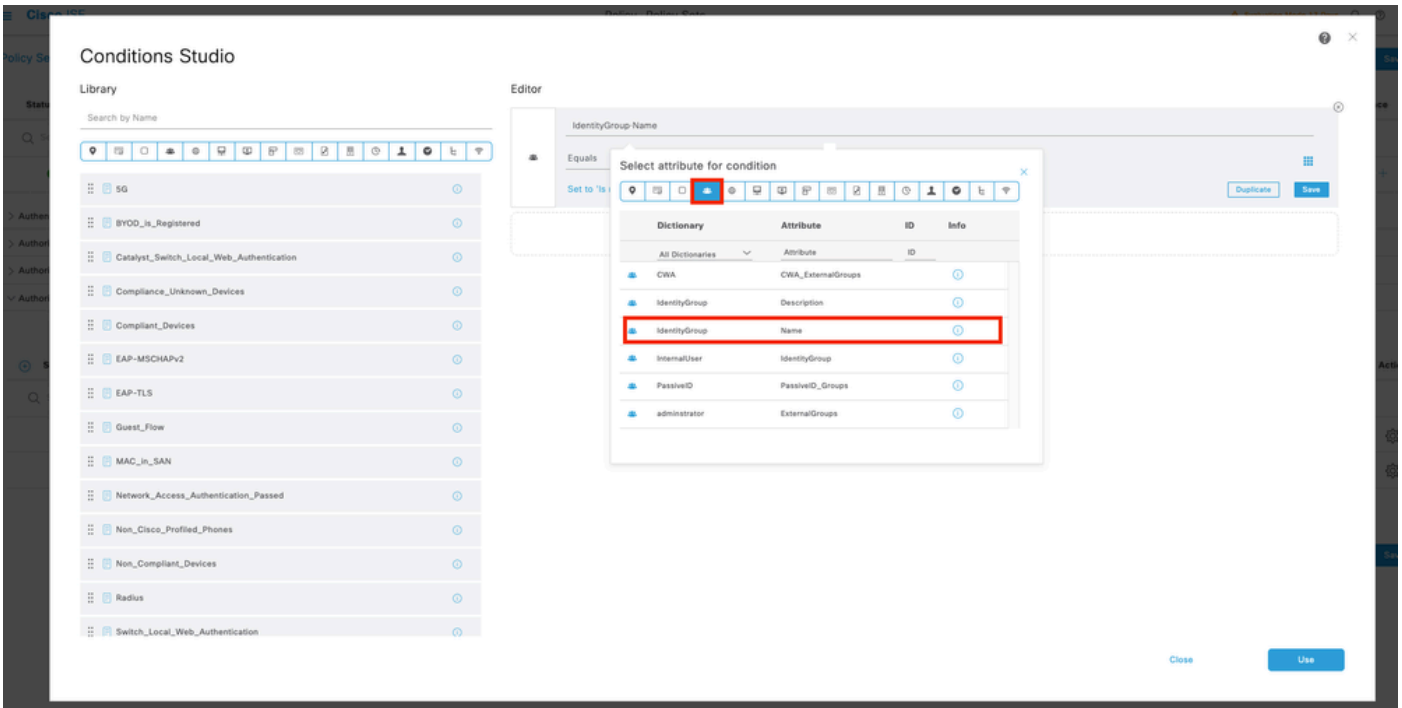
步骤 10 通过点击行尾部的>图标来查看新的策略集。



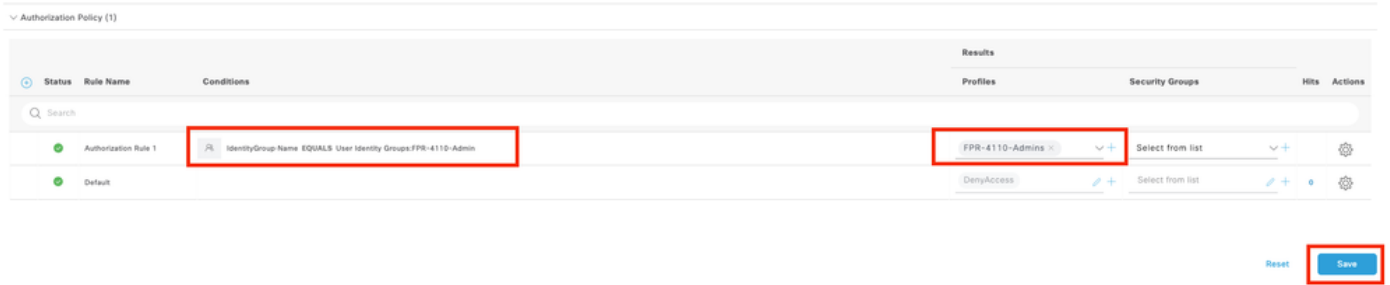
10.1 展开 Authorization Policy 菜单并单击(+)添加新条件。



10.2设置条件以匹配DictionaryIdentity组与AttributeName Equals User Identity Groups : FPR-4110-Admins (在步骤7中创建的组名) 并单击Use。



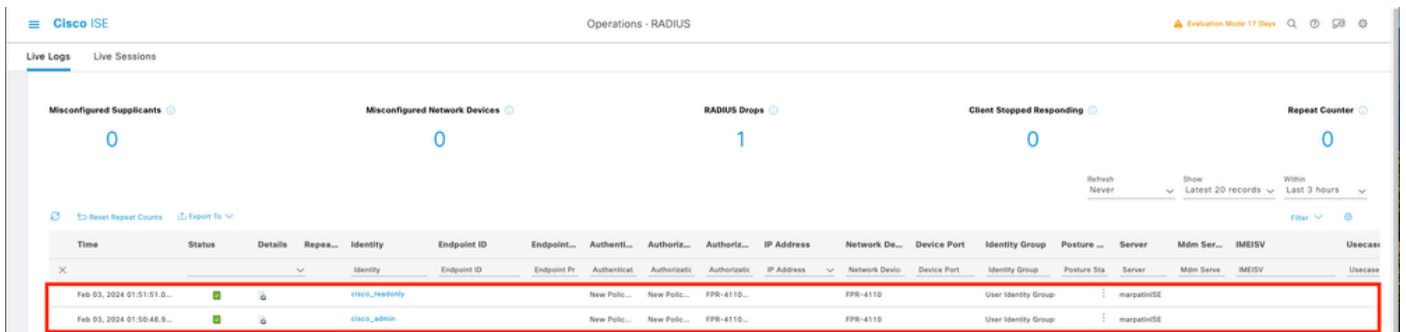
第10.3步验证在授权策略中配置的新条件，然后在配置文件下添加用户配置文件。



步骤 11对只读用户重复步骤9中的相同过程，然后点击保存。

验证

1. 尝试使用新的Radius凭证登录FCM GUI
2. 导航至>工序> Radius >实时日志=的汉堡图标。
3. 显示的信息显示用户是否成功登录。



4. 从安全防火墙机箱CLI验证已记录的用户角色。

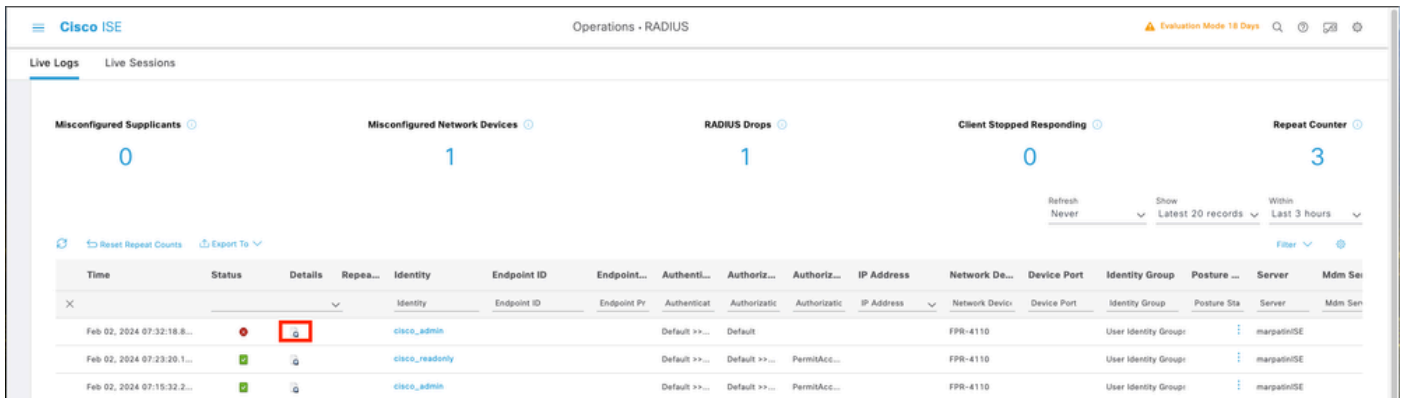
```
FPR4K-1-029A78B# scope se
security          server          service-profile

FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
  Description:
  User Roles:
    Name: admin
    Name: read-only
FPR4K-1-029A78B /security #
```

故障排除

1. 在ISE GUI上，导航至汉堡图标=> Operations > Radius > Live logs。

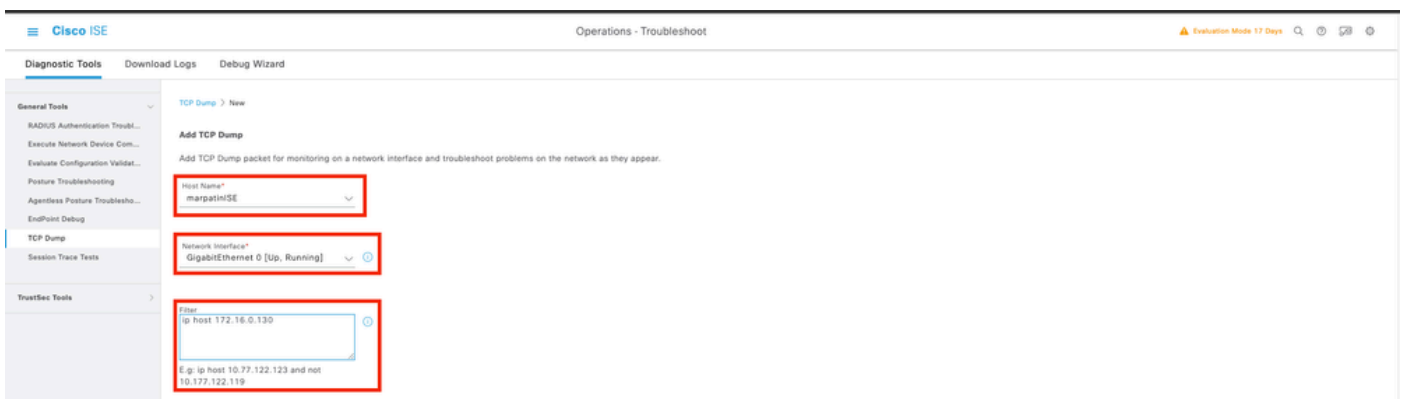
- 1.1验证日志会话请求是否到达ISE节点。
- 1.2对于失败状态，请查看会话详细信息。



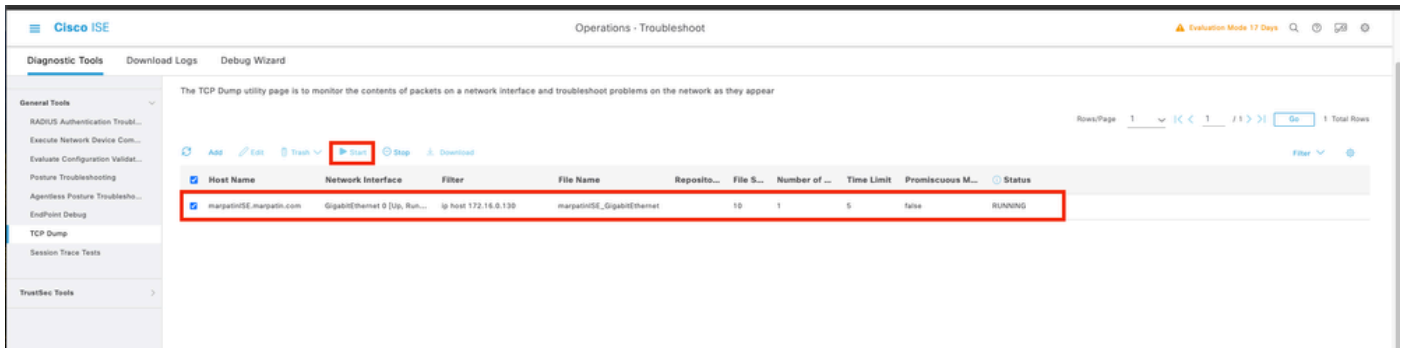
2. 对于未显示在RADIUS实时日志中的请求，请查看UDP请求是否通过数据包捕获到达ISE节点。

导航到>操作>故障排除>诊断工具> TCP转储=>的汉堡图标。添加新的捕获并将文件下载到本地计算机，以查看UDP数据包是否到达ISE节点。

2.1请填写所需信息，向下滚动并单击Save。



2.2选择并启动捕获。



2.3当ISE捕获运行时，尝试记录到安全防火墙机箱

2.4停止ISE中的TCP转储并将文件下载到本地计算机。

2.5查看流量输出。

预期输出：

数据包编号1。从安全防火墙通过端口1812 (RADIUS)向ISE服务器发出的请求
数据包No2。ISE服务器回复接受初始请求。

No.	Time	Source	Destination	Length	Protocol	Message Transaction ID	Info
1	2024-02-02 20:21:52.999276	172.16.0.130	172.16.0.12	128	RADIUS		Access-Request id=22
2	2024-02-02 20:21:53.090894	172.16.0.12	172.16.0.130	186	RADIUS		Access-Accept id=22

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）。