将ISE配置为RADIUS服务器的FMC和FTD外部身份验证

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- FMC的外部身份验证
- FTD的外部身份验证
- 网络拓扑

配置

- ISE 配置
- FMC配置
- FTD配置

验证

简介

本文档介绍安全防火墙管理中心和防火墙威胁防御的外部身份验证配置示例。

先决条件

要求

建议了解以下主题：

- 通过GUI和/或外壳进行思科安全防火墙管理中心初始配置。
- 在ISE上配置身份验证和授权策略。
- RADIUS基础知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- vFMC 7.2.5
- vFTD 7.2.5。
- ISE 3.2。

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。

背景信息

为安全防火墙系统的管理和管理用户启用外部身份验证时，设备会使用在外部身份验证对象中指定的轻型目录访问协议(LDAP)或RADIUS服务器验证用户凭证。

外部身份验证对象可由FMC和FTD设备使用。您可以在不同设备/设备类型之间共享同一对象，或者创建单独的对象。

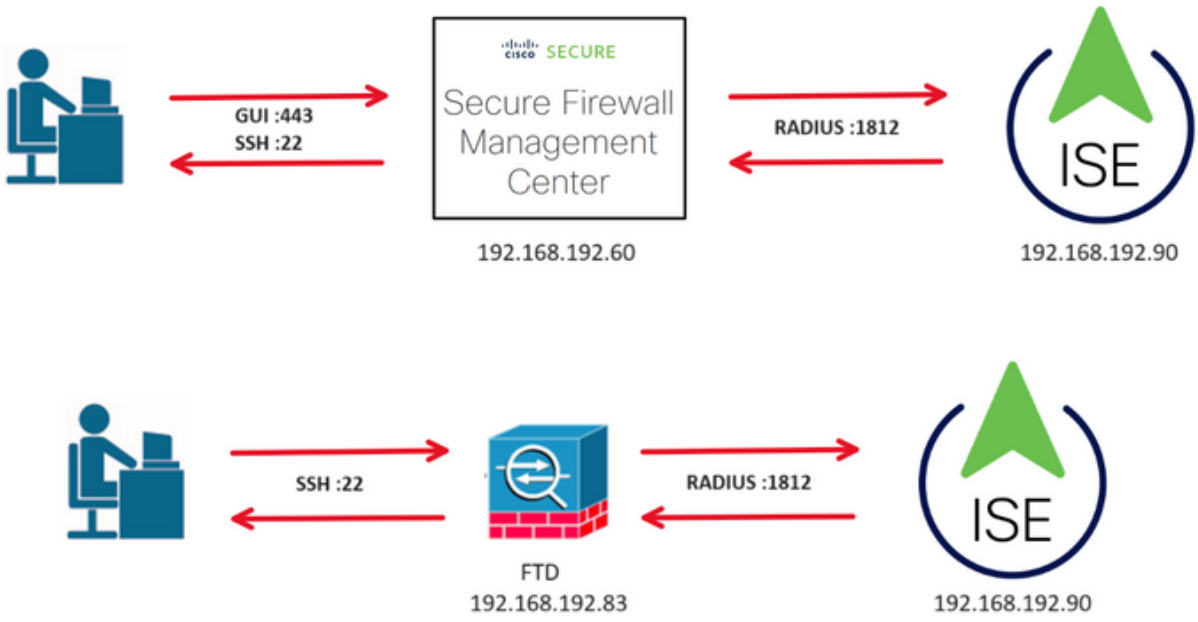
FMC的外部身份验证

您可以配置多个外部身份验证对象以访问Web界面。只有一个外部身份验证对象可用于CLI或外壳访问。

FTD的外部身份验证

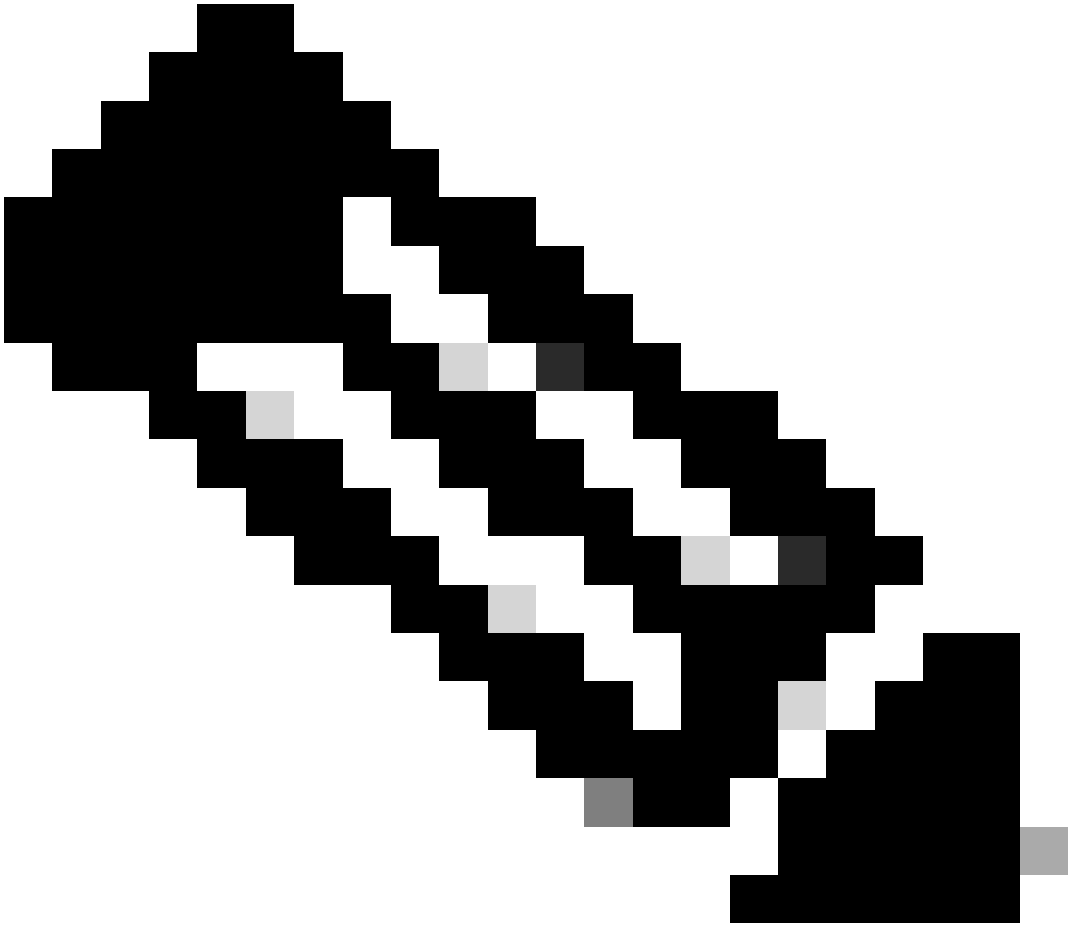
对于FTD，您只能激活一个外部身份验证对象。

网络拓扑



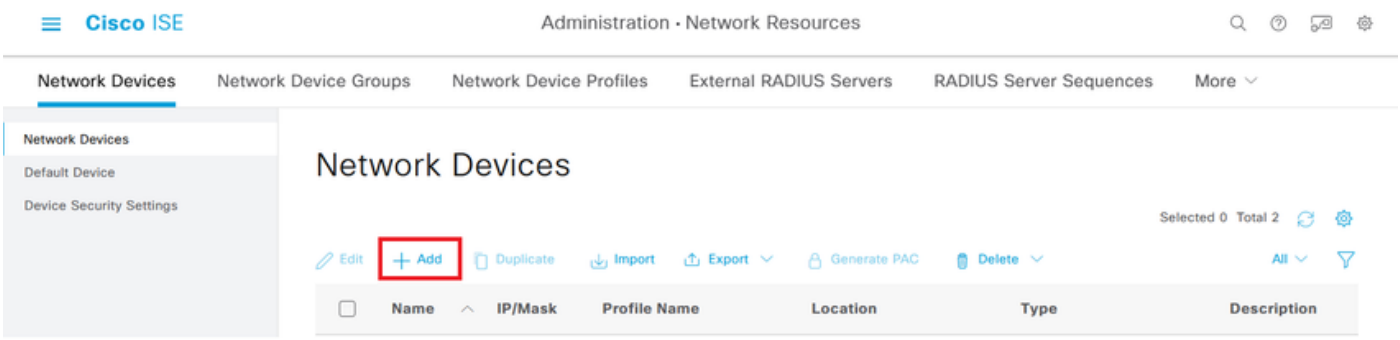
配置

ISE 配置



注意：有多种方法可以为网络接入设备(NAD)（例如FMC）设置ISE身份验证和授权策略。本文档中介绍的示例是一个参考点，我们在其中创建了两个配置文件（一个具有管理员权限，另一个为只读），可以对其进行修改以满足访问网络的基准。可以在ISE上定义一个或多个授权策略，并向FMC返回RADIUS属性值，然后映射到FMC系统策略配置中定义的本地用户组。

步骤1:添加新的网络设备。导航到位于左上角>管理>网络资源>网络设备> +Add的汉堡图标。

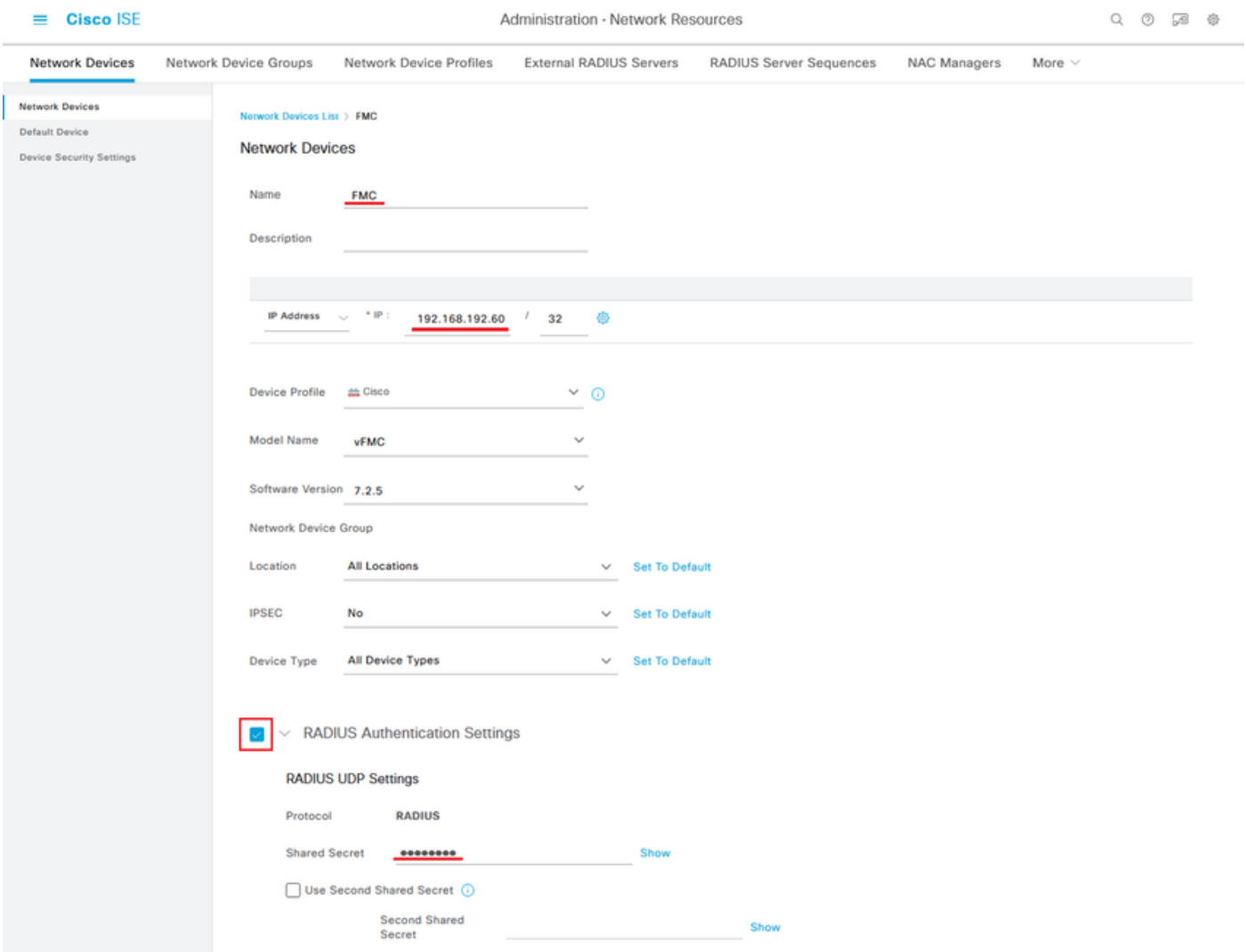


第二步：为网络设备对象分配名称并插入FMC IP地址。

选中RADIUS 复选框并定义共享密钥。

稍后必须使用该密钥来配置FMC。

完成后，单击Save。

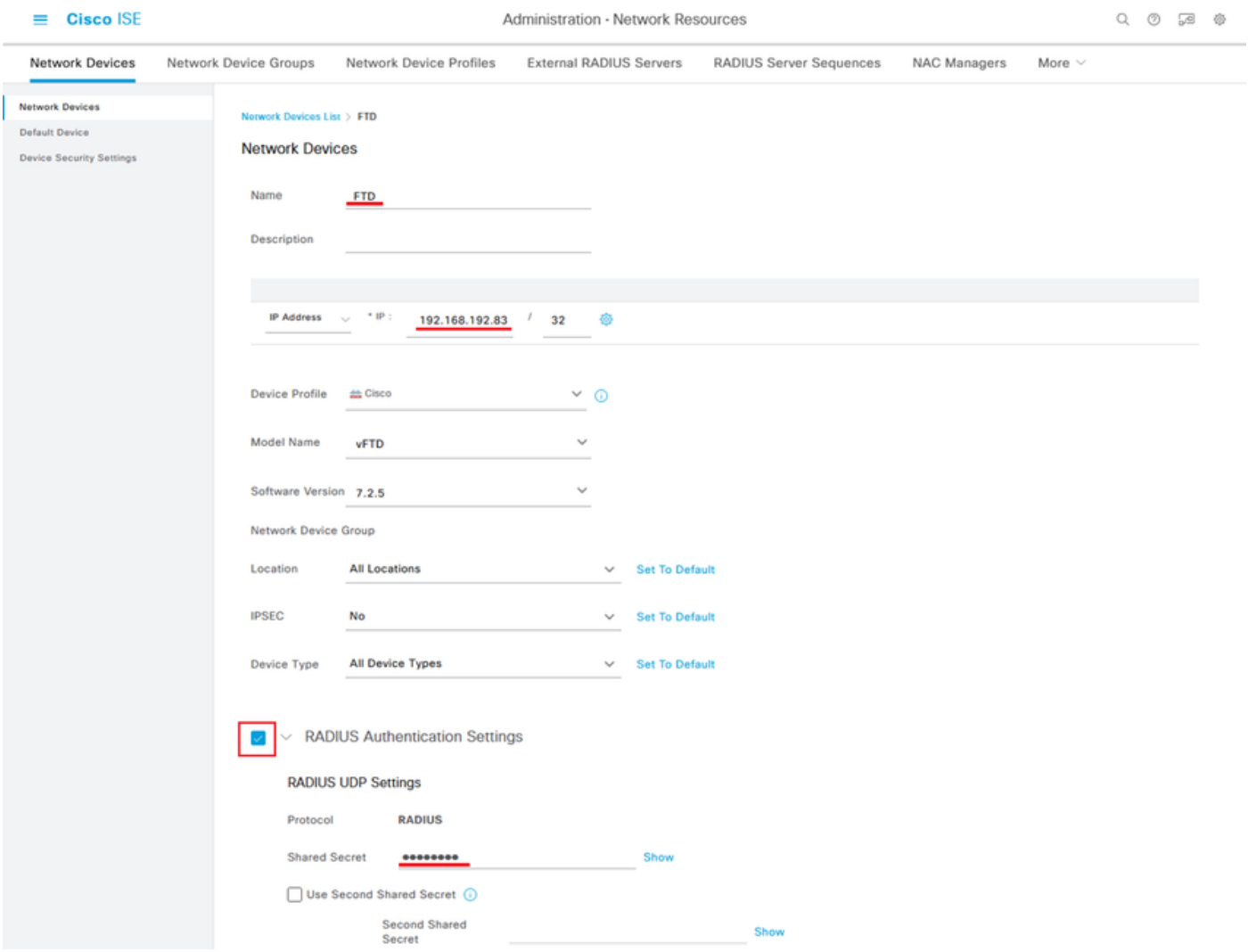


步骤 2.1重复相同操作以添加FTD。

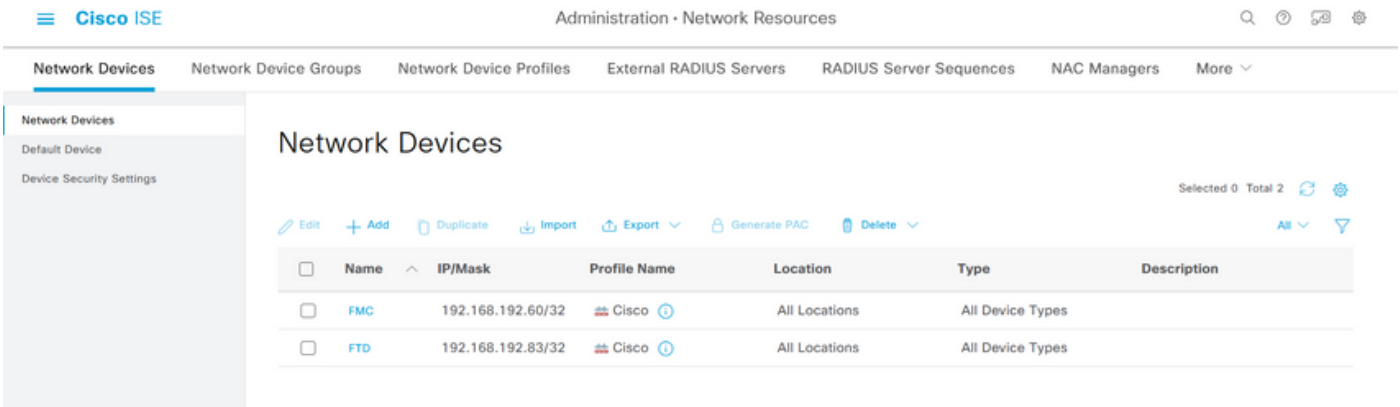
为网络设备对象分配名称并插入FTD IP地址。

选中RADIUS 复选框并定义共享密钥。

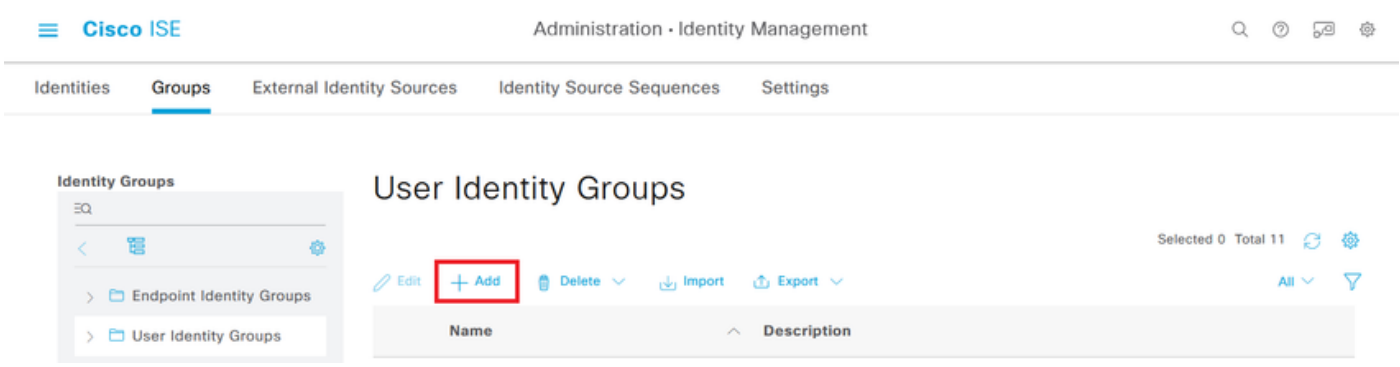
完成后，单击Save。



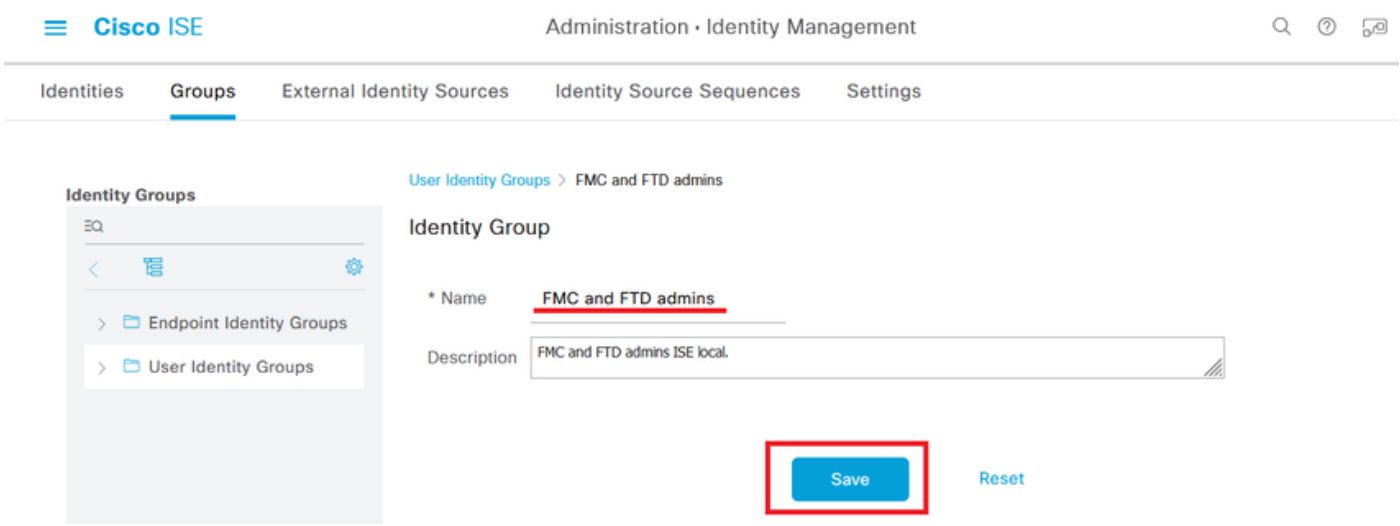
步骤 2.3验证“Network Devices（网络设备）”下显示的两个设备。



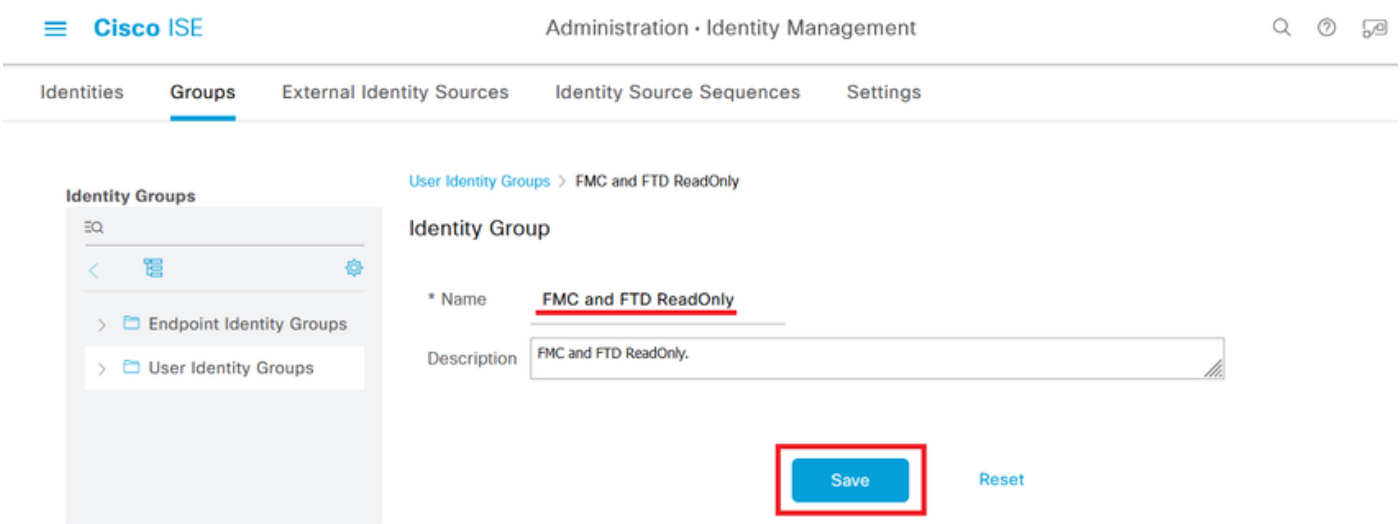
第三步： 创建所需的用户身份组。导航到位于左上角>管理>身份管理>组>用户身份组> +添加的汉堡图标



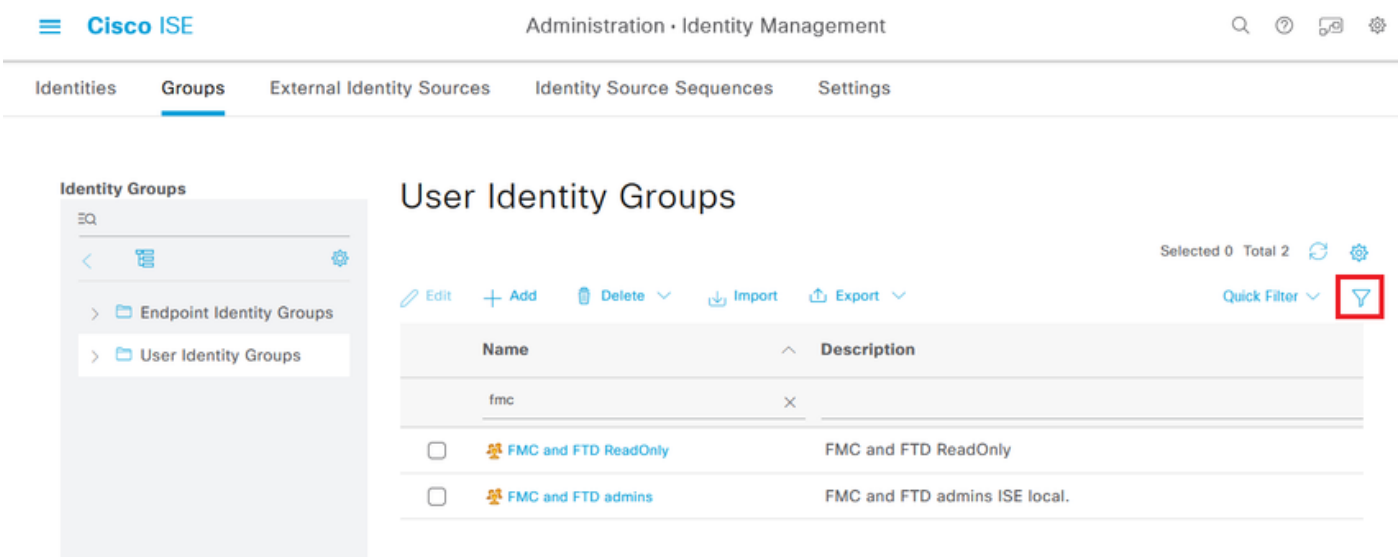
第四步：为每个组指定名称并单独保存。在本例中，我们将为管理员用户创建一个组，为只读用户创建另一个组。首先，为具有管理员权限的用户创建组。



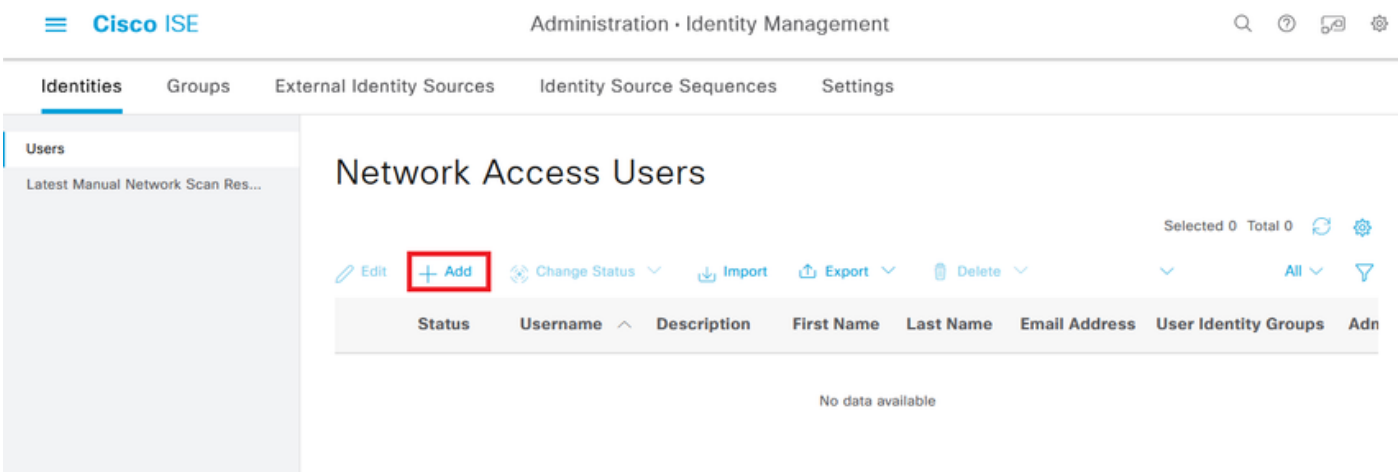
步骤 4.1为只读用户创建第二个组。



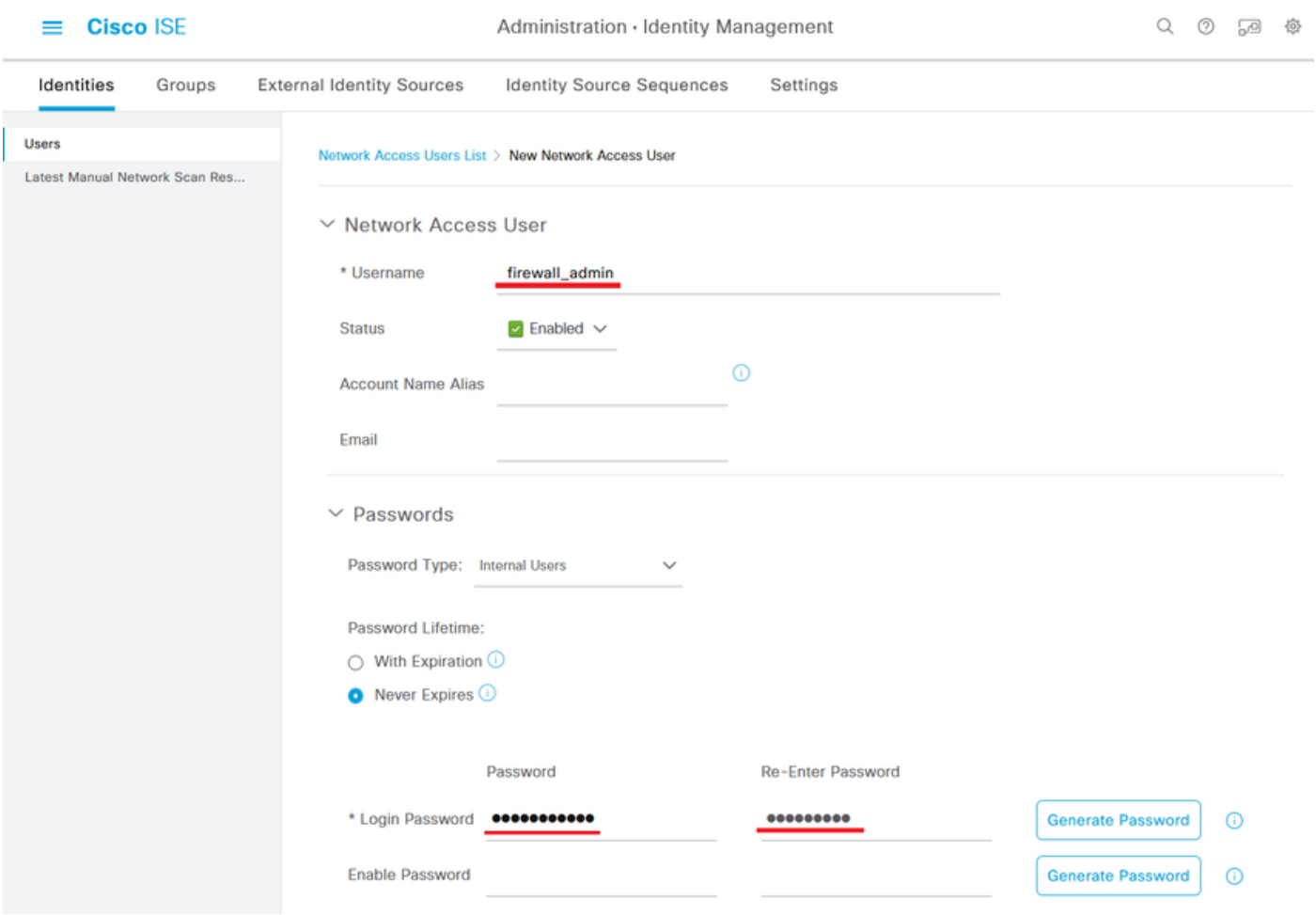
步骤 4.2验证两个组显示在User Identity Groups List下。使用过滤器可以轻松找到它们。

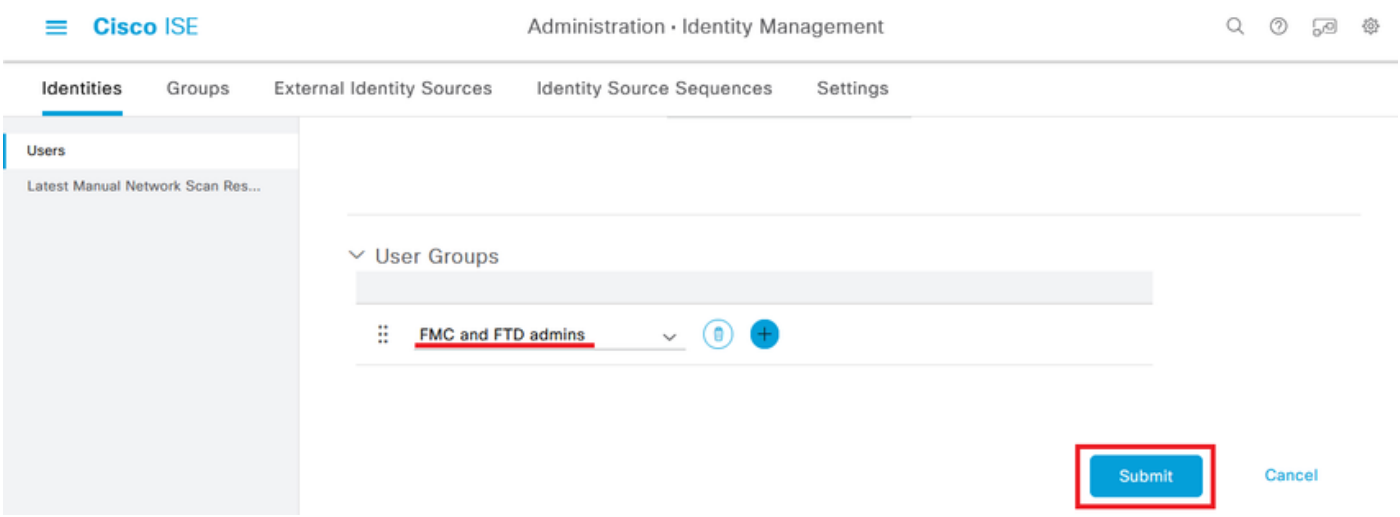


第五步： 创建本地用户并将其添加到其往来行组。导航到>管理>身份管理>身份> + Add。

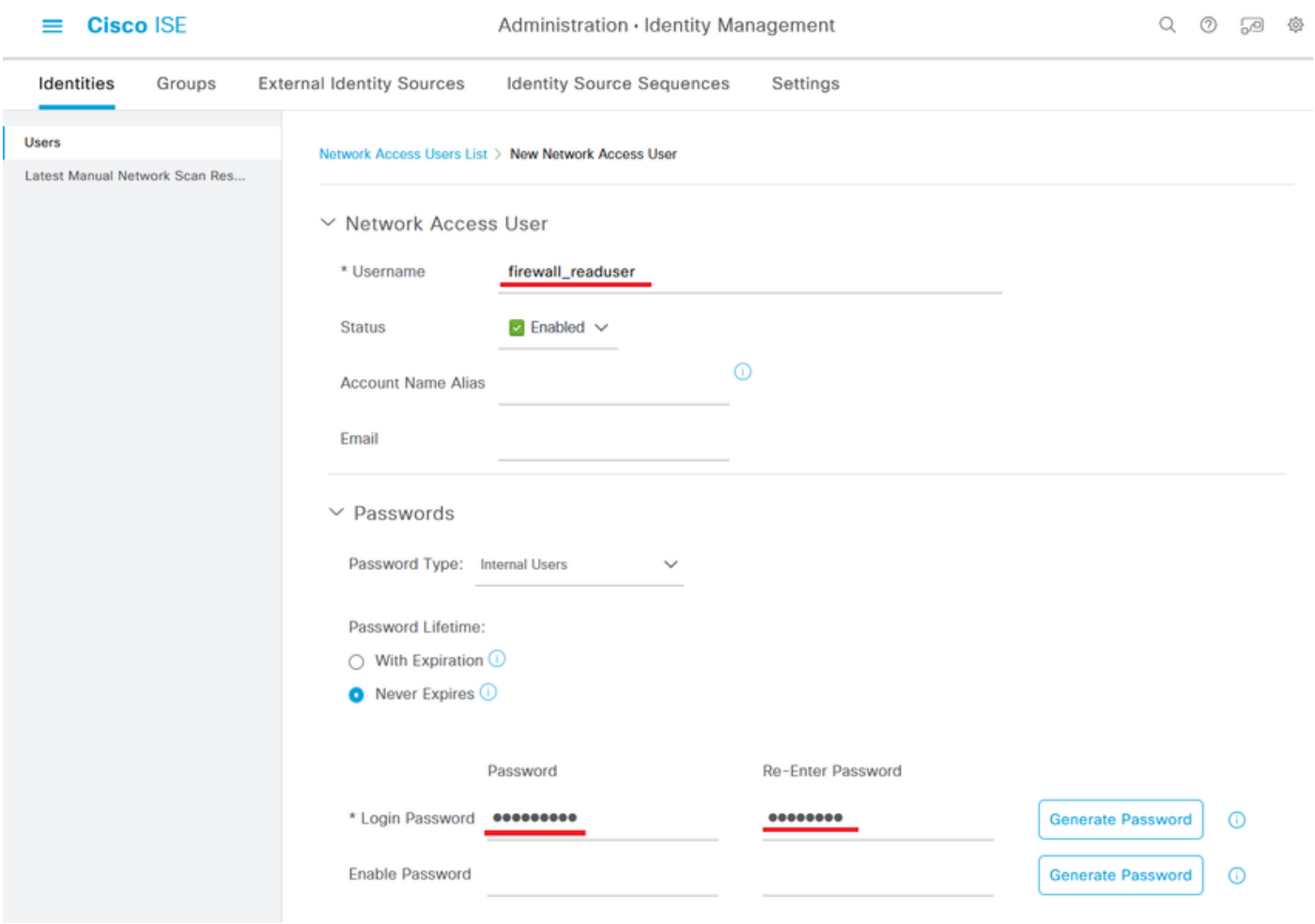


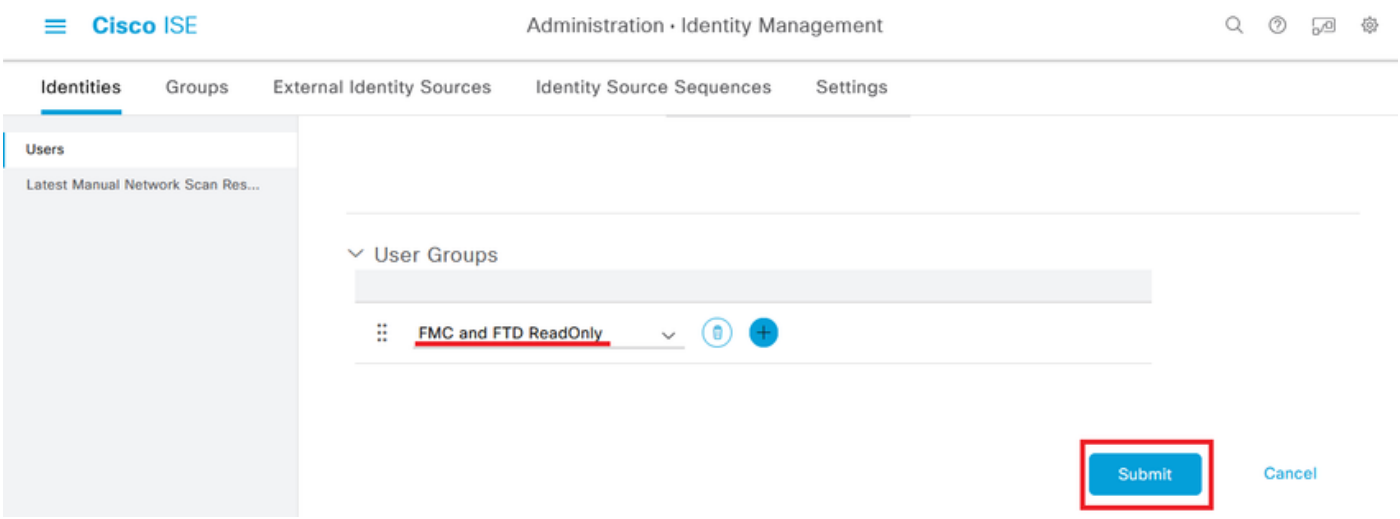
步骤 5.1首先创建具有管理员权限的用户。为其分配名称、密码和组FMC和FTD管理员。





步骤 5.2添加具有只读权限的用户。分配名称、密码和组FMC和FTD ReadOnly。

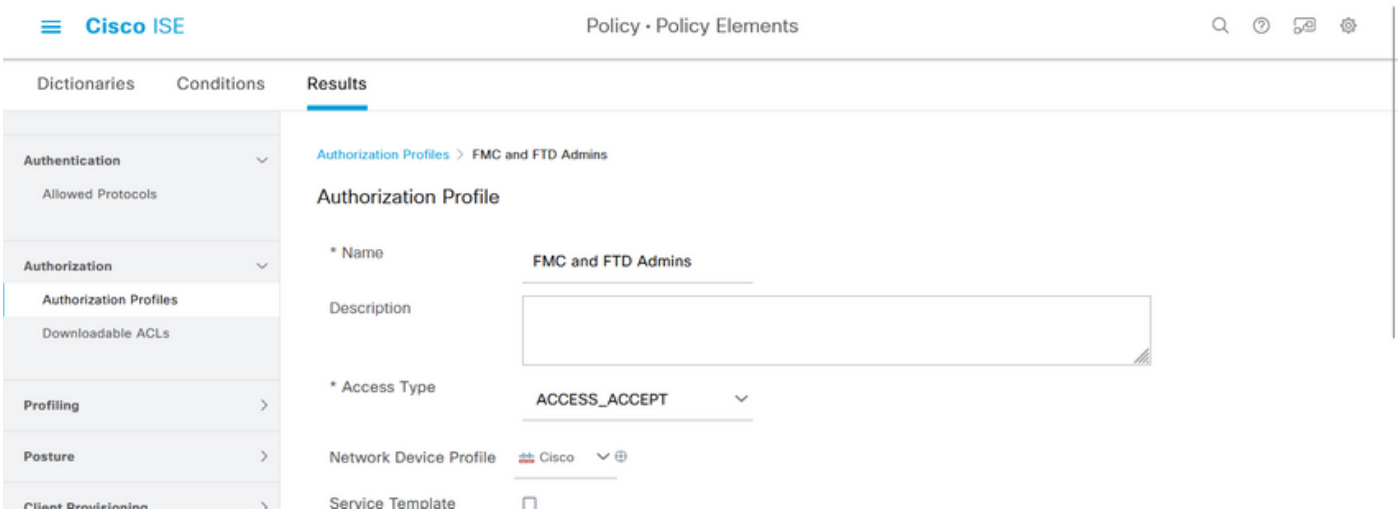


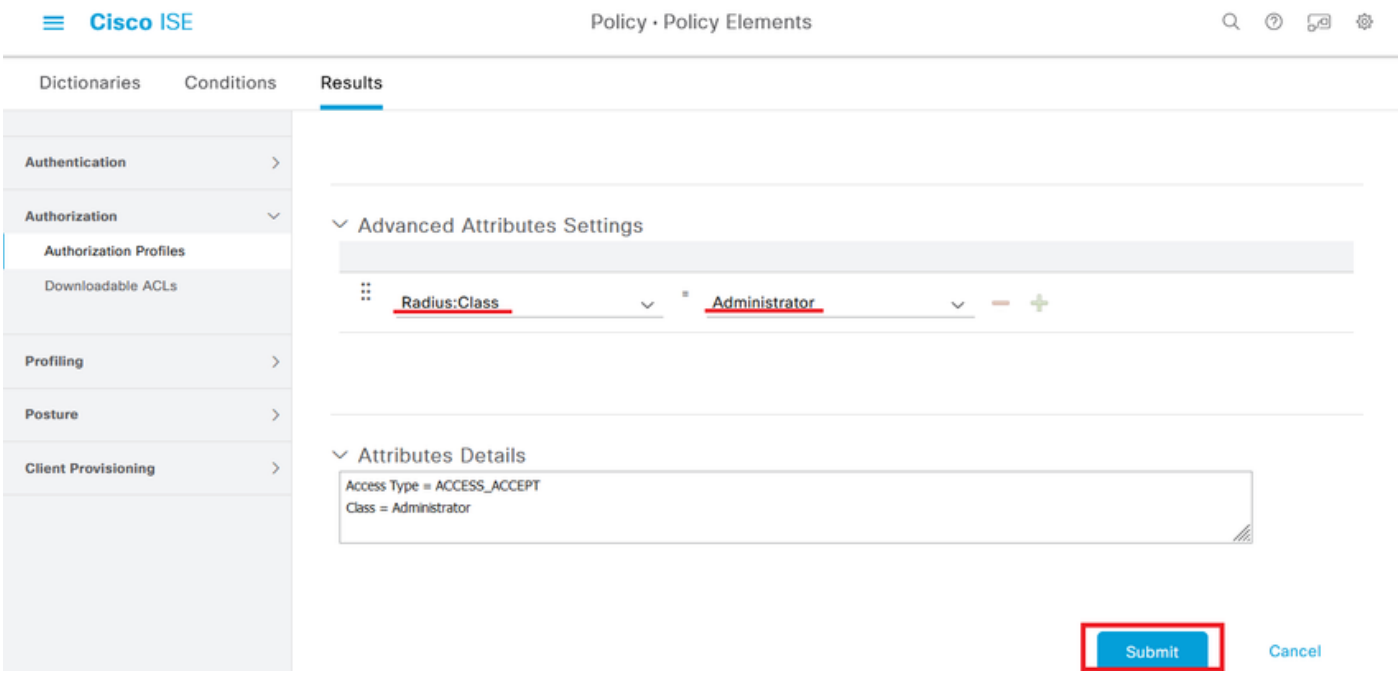


第六步：创建管理员用户的授权配置文件。

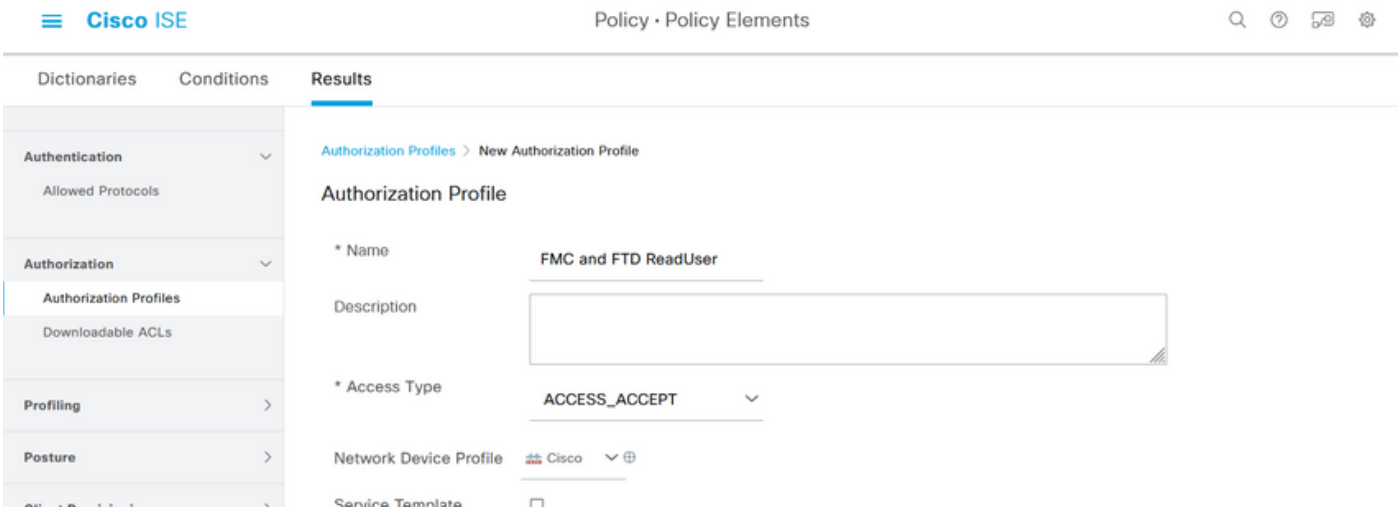
导航到
>策略>Policy元素>结果>授权>授权配置文件> +Add。

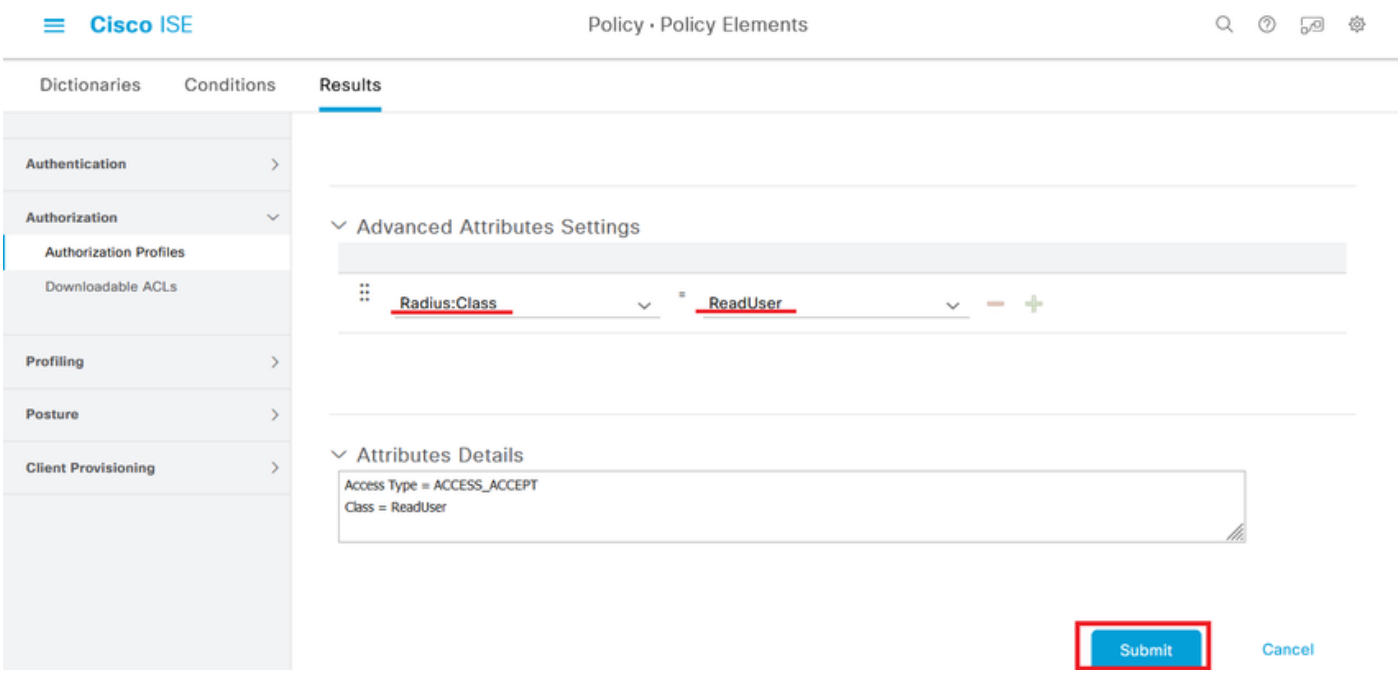
定义授权配置文件的名称，将“访问类型”保留为ACCESS_ACCEPT，并在“高级属性设置”下使用值 Administrator 添加Radius > Class—[25]，然后单击提交。





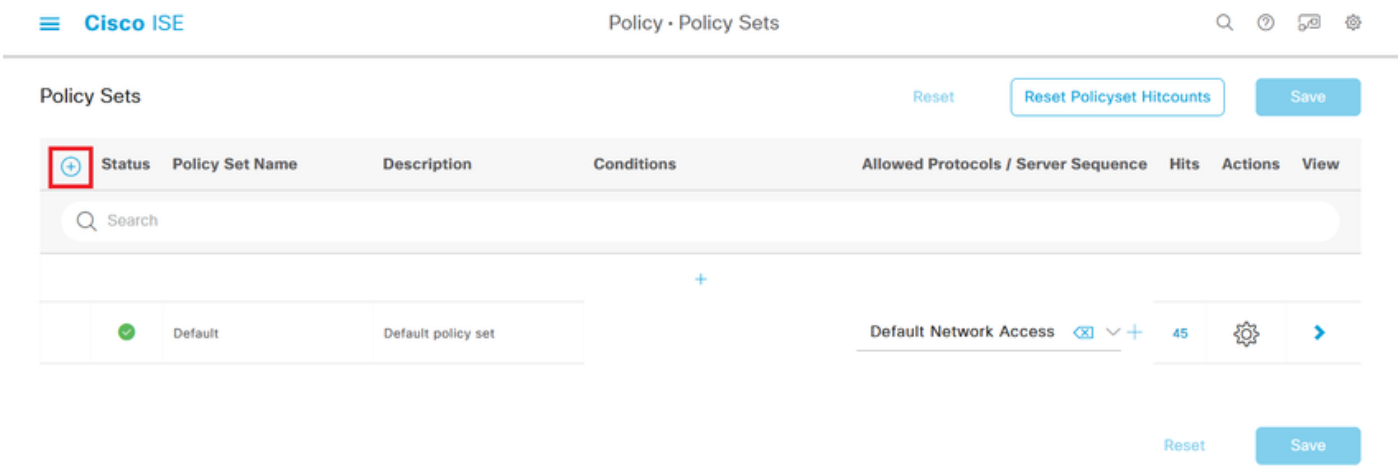
步骤 7.重复上一步为只读用户创建授权配置文件。这次使用值ReadUser而非Administrator创建Radius类。





步骤 8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。

导航到位于左上角的
>策略>策略集> 图标。

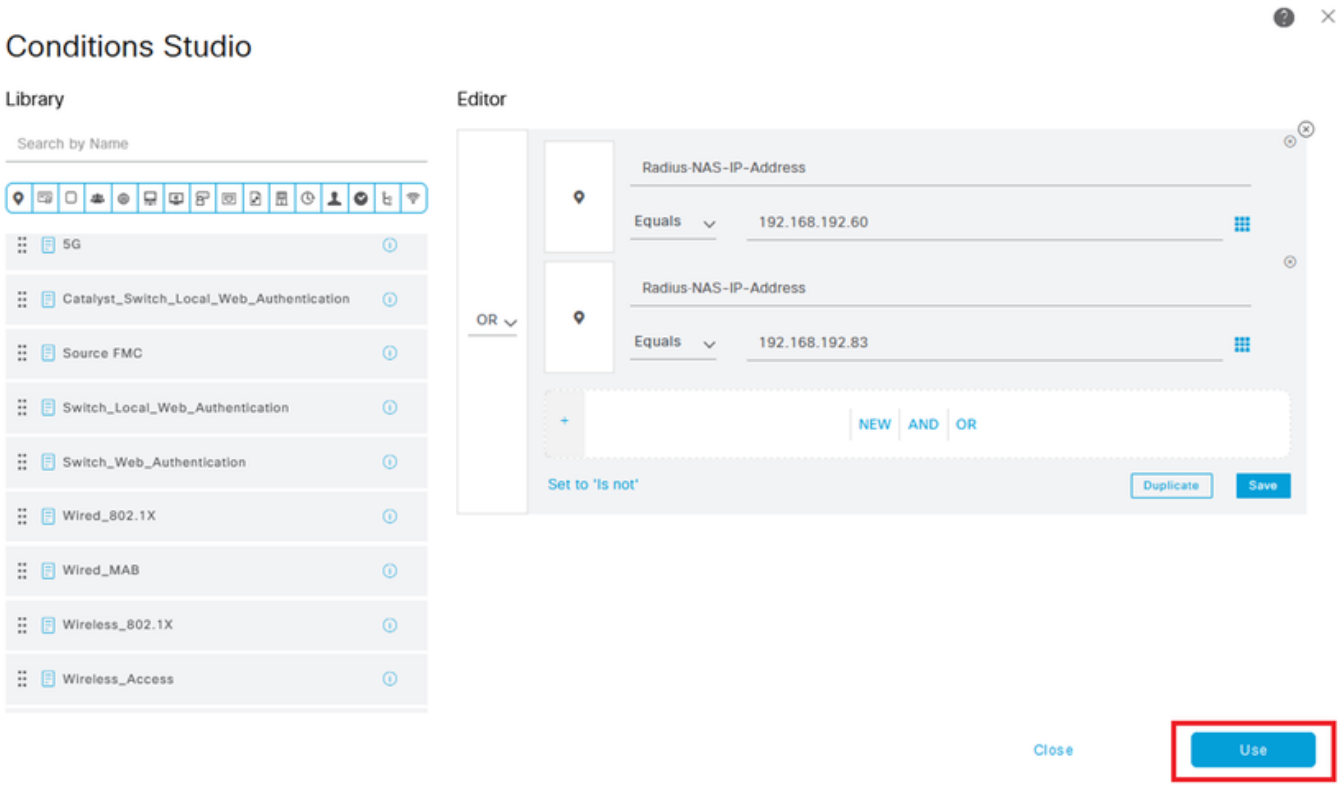


步骤 8.1新行位于策略集的顶部。

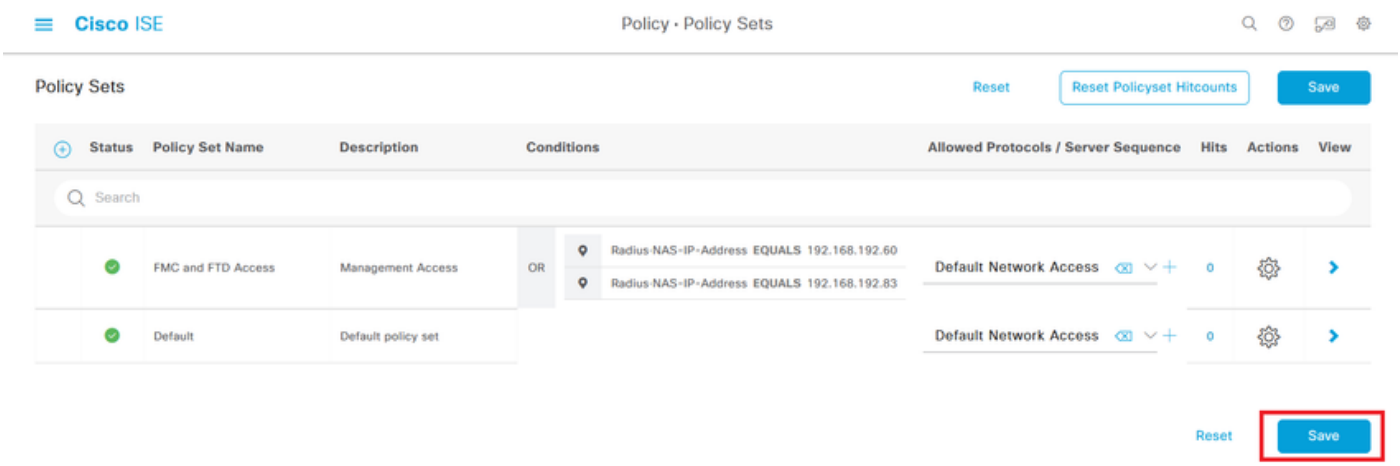
为新策略命名，并为与FMC IP地址匹配的RADIUS NAS-IP-Address属性添加顶级条件。

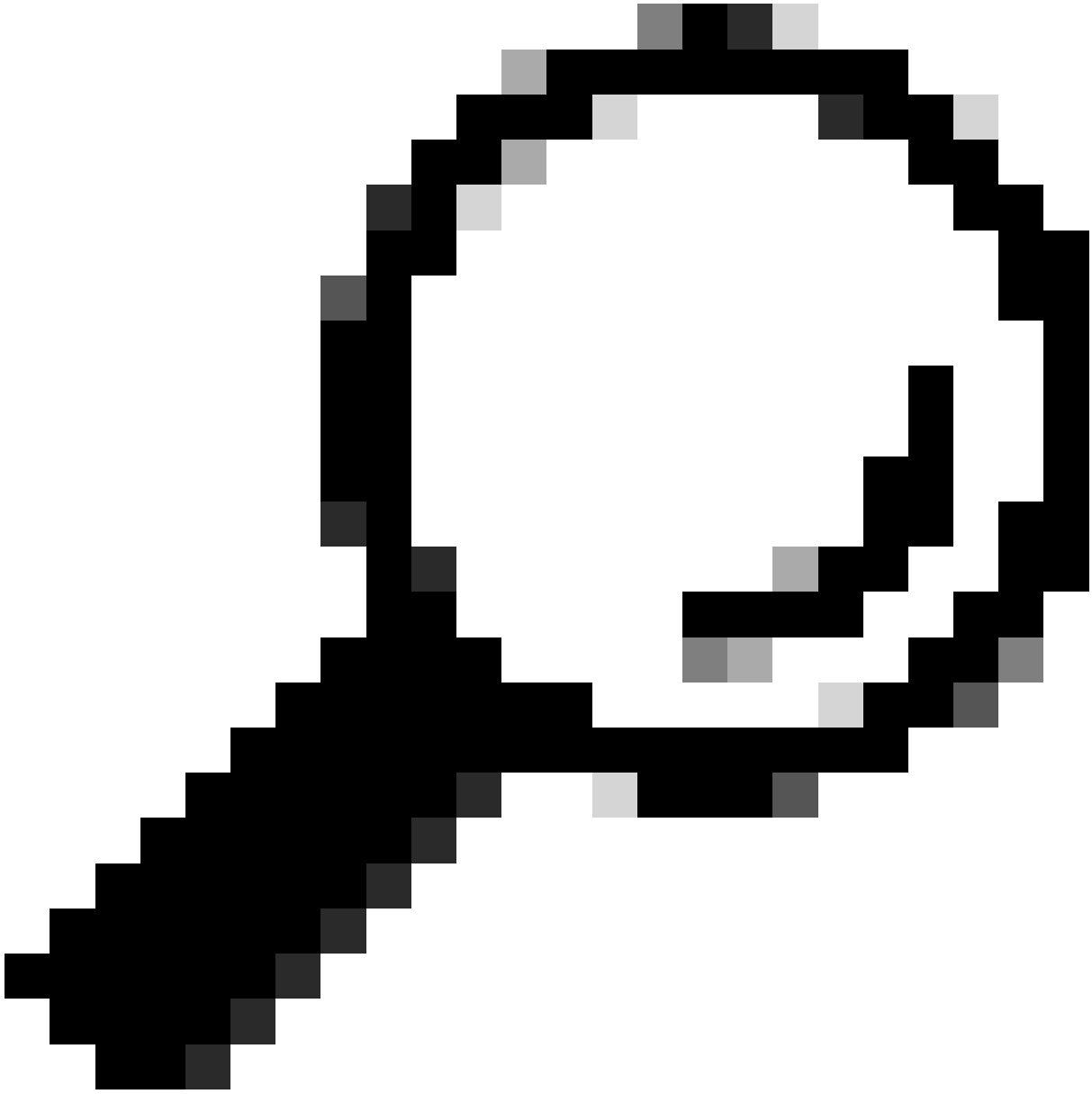
添加第二个带OR条件的值，以包含FTD的IP地址。

单击Use以保留更改并退出编辑器。

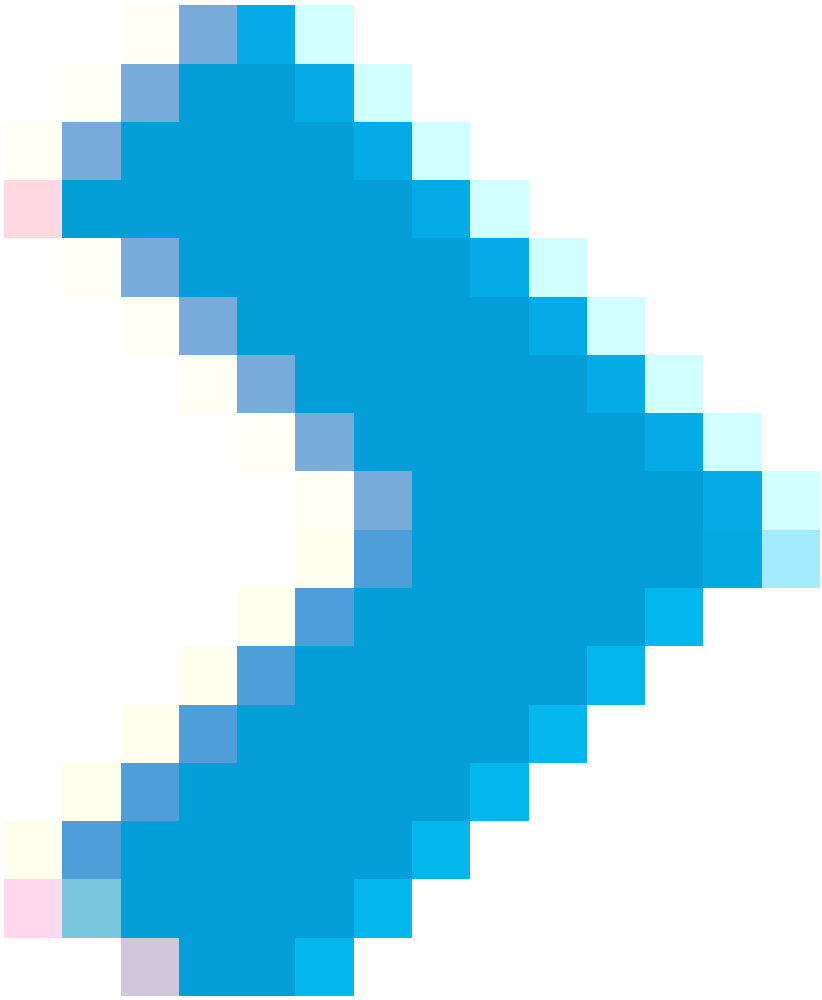


步骤 8.2完成后单击Save。





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。



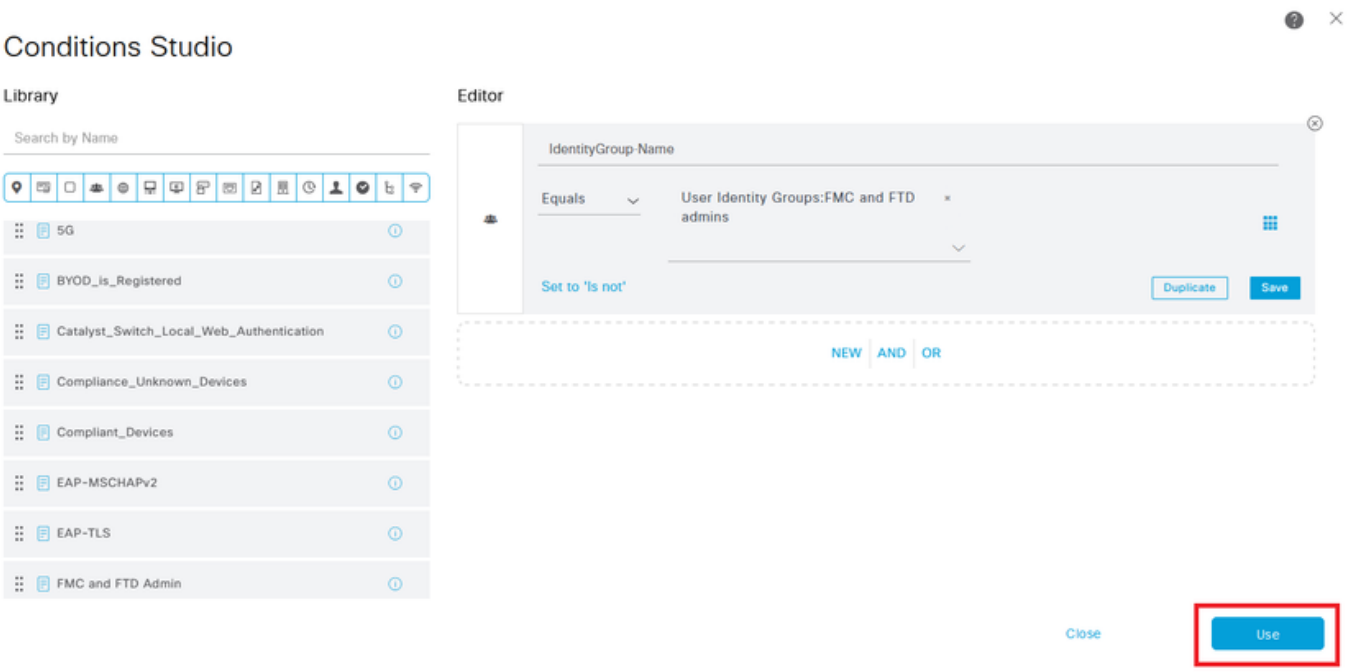
步骤 9通过点击行尾部的
图标查看新的策略集。

展开Authorization Policy菜单并推送

图标以添加新规则，从而允许具有管理员权限的用户访问。

给它一个名字。

设置条件以匹配属性名称等于用户身份组：FMC和FTD管理员（在步骤4中创建的组名）的词典身份组，然后单击使用。

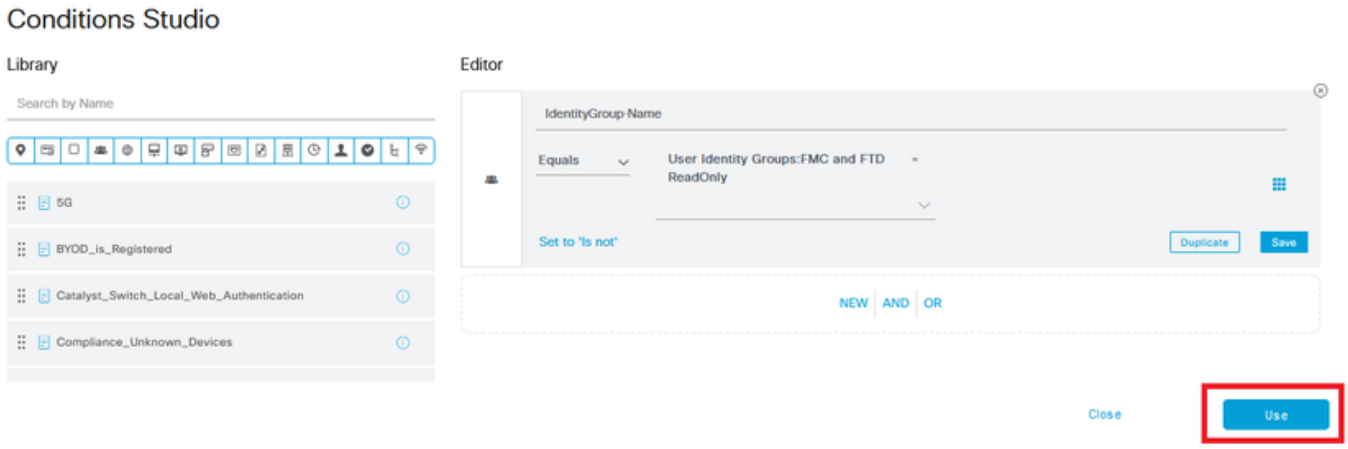

Conditions Studio
Library
Search by Name
5G
BYOD_is_Registered
Catalyst_Switch_Local_Web_Authentication
Compliance_Unknown_Devices
Compliant_Devices
EAP-MSCHAPv2
EAP-TLS
FMC and FTD Admin
Editor
IdentityGroup-Name
Equals
User Identity Groups:FMC and FTD admins
Set to 'Is not'
Duplicate
Save
NEW
AND
OR
Close
Use

步骤 10点击

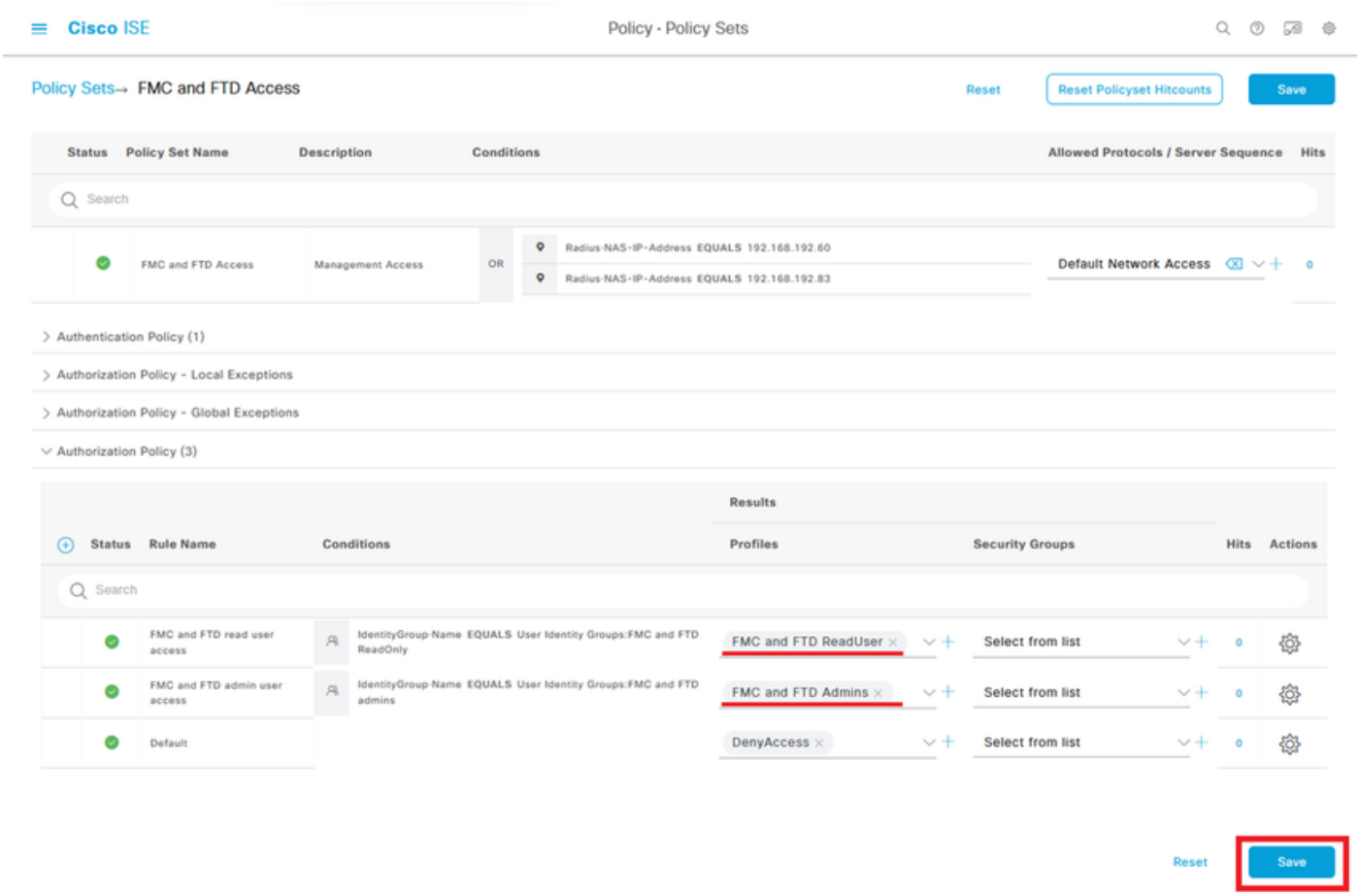
图标，添加第二条规则，以向具有只读权限的用户授予访问权限。

给它一个名字。

设置条件以匹配属性Name Equals User Identity Groups： FMC和FTD ReadOnly（在步骤4中创建的组名）的词典身份组，然后单击Use。



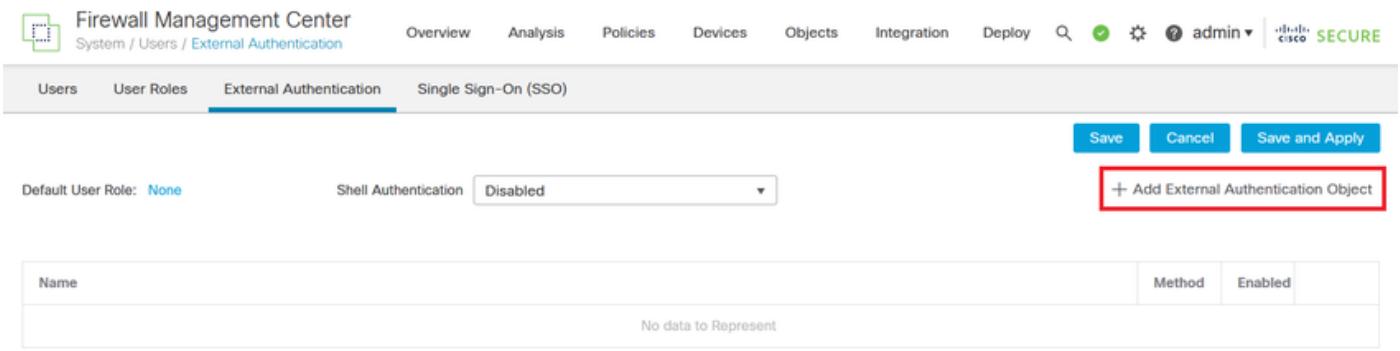
步骤 11分别为每个规则设置授权配置文件，然后单击Save。



FMC配置

步骤1:在System > Users > External Authentication > + Add External Authentication Object下创建

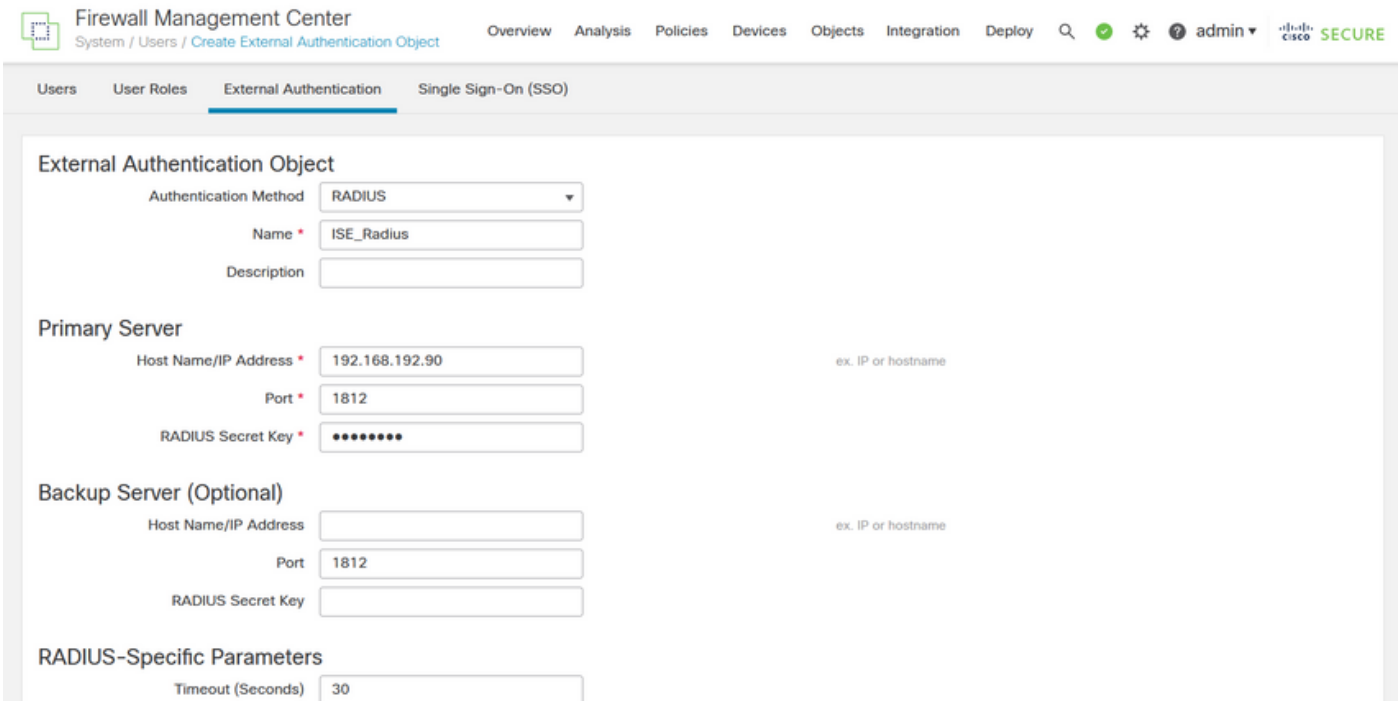
外部身份验证对象。



第二步：选择RADIUS作为身份验证方法。

在External Authentication Object下，为新对象指定Name。

然后，在主服务器设置中，插入ISE IP地址和您在ISE配置的第2步中使用的相同RADIUS密钥。

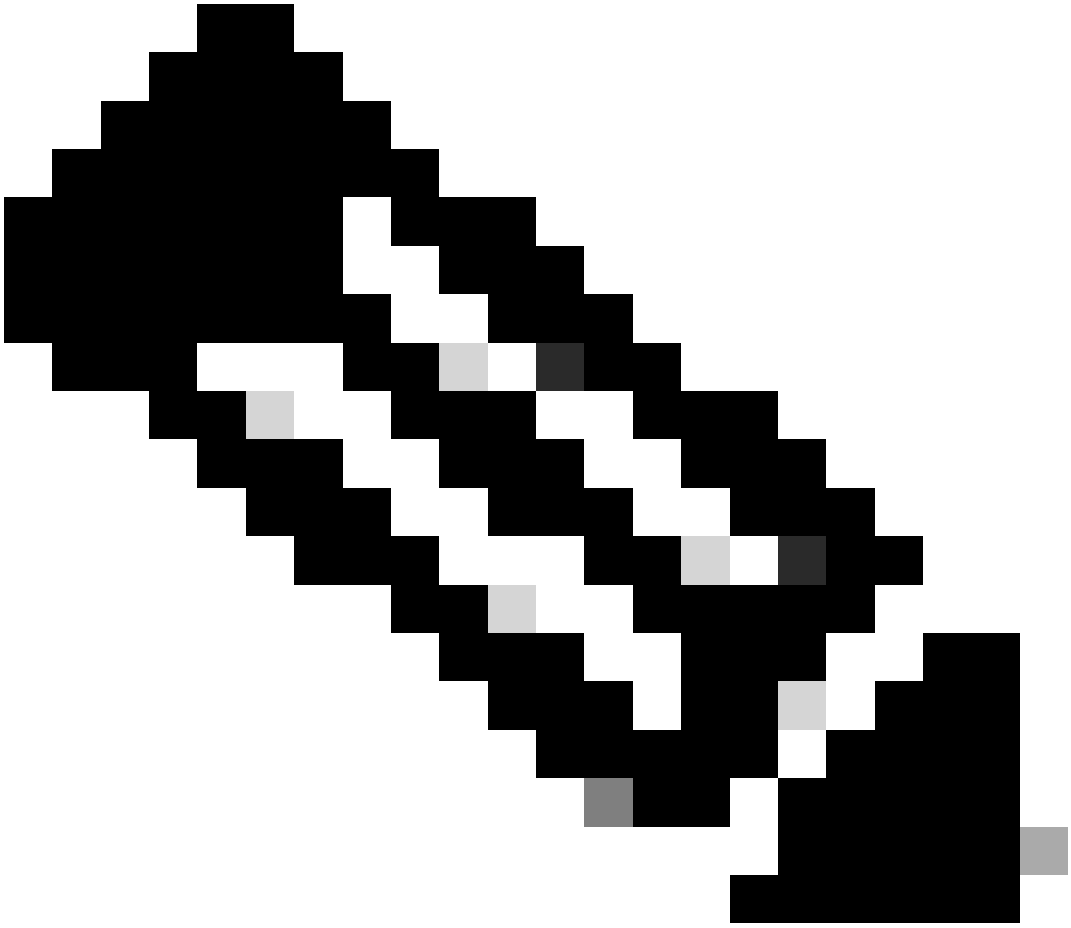


第三步：插入在ISE配置的第6步和第7步中配置的RADIUS Class属性值：分别为管理员和ReadUser的firewall_admin和firewall_readuser。

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Administrator
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	Class=ReadUser
Security Approver	
Threat Intelligence Director (TID) User	
Default User Role	Access Admin Administrator Discovery Admin External Database User

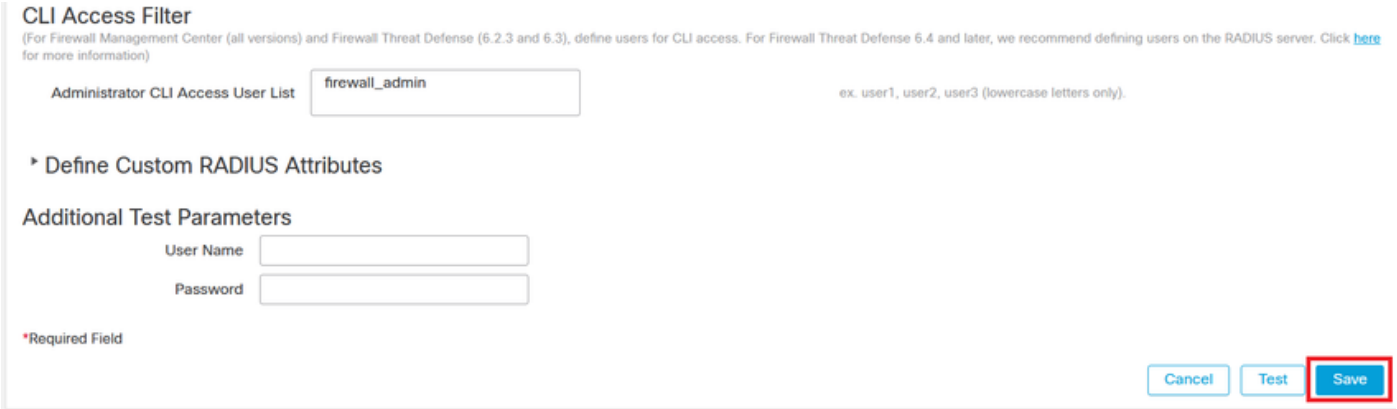
To specify the default user role if user is not found in any group



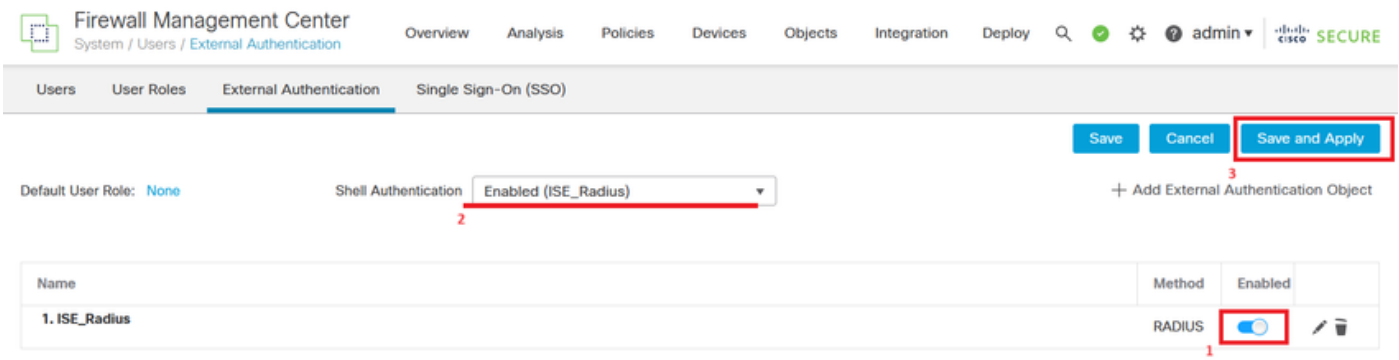
注意：FTD和FMC的超时范围不同，因此如果共享对象并将默认值更改为30秒，请确保不要超出FTD设备的较小超时范围（1-300秒）。如果将超时设置为更高的值，威胁防御RADIUS配置将不起作用。

第四步：用获得CLI访问权限的用户名填充CLI访问过滤器下的管理员CLI访问用户列表。

完成后单击Save。

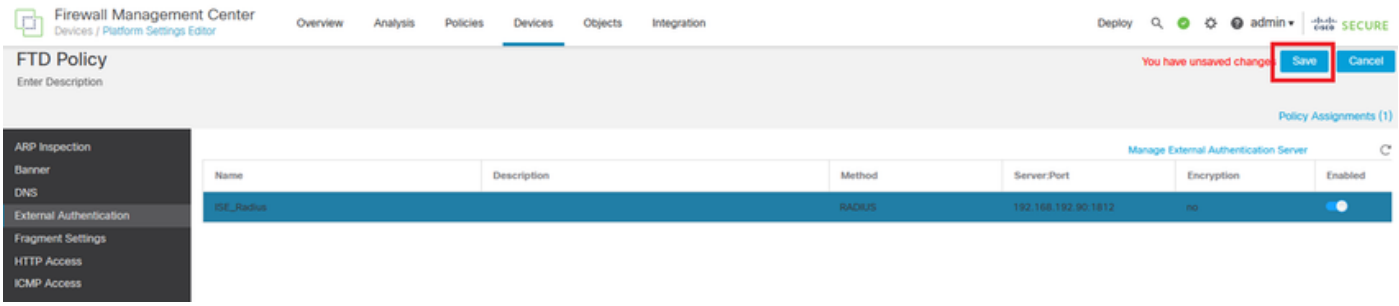


第五步：启用新对象。将其设置为FMC的Shell Authentication（外壳身份验证）方法，然后单击Save and Apply（保存并应用）。

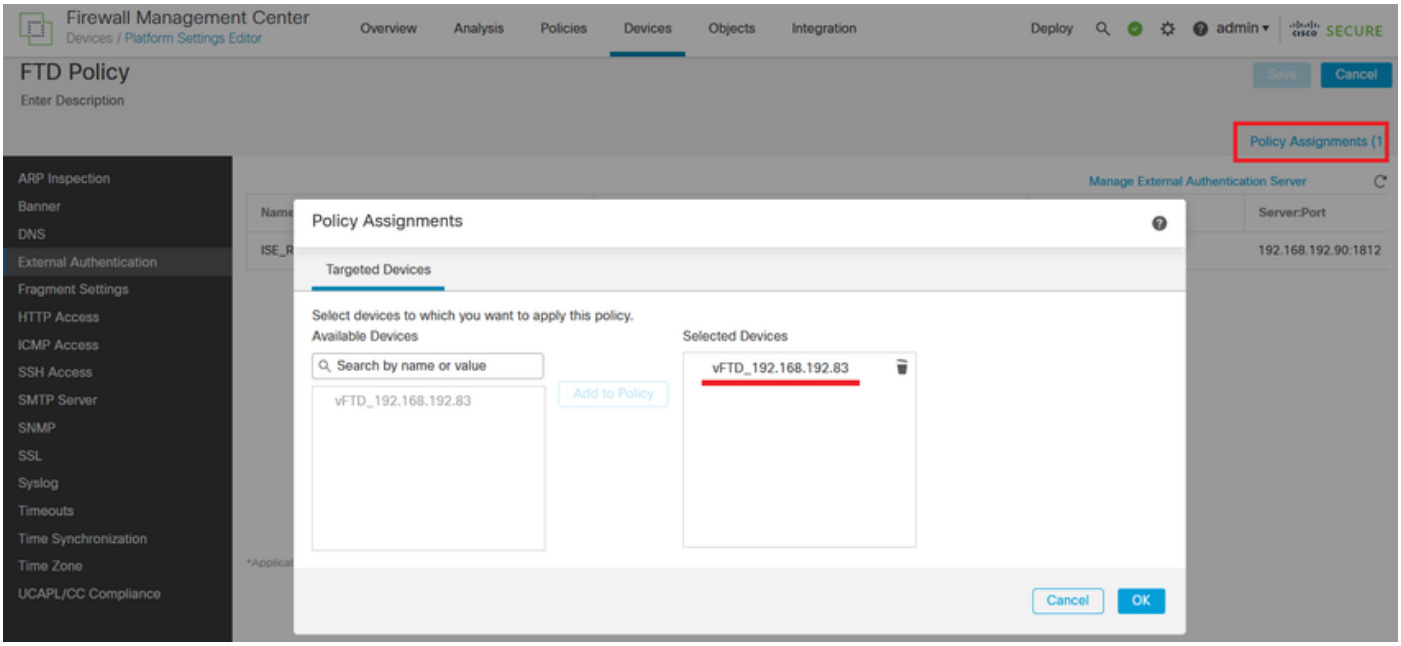


FTD配置

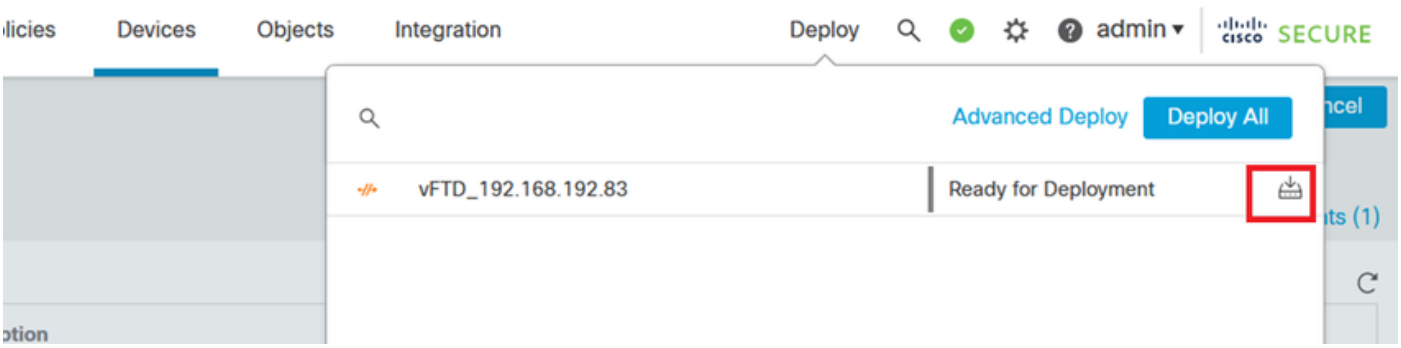
步骤1:在FMC GUI中，导航到设备>平台设置。编辑当前策略或创建新策略（如果没有为需要访问的FTD分配任何策略）。启用External Authentication下的RADIUS服务器，然后单击Save。



第二步：确保您需要获得访问权限的FTD在Policy Assignments as a Selected Device下列出。

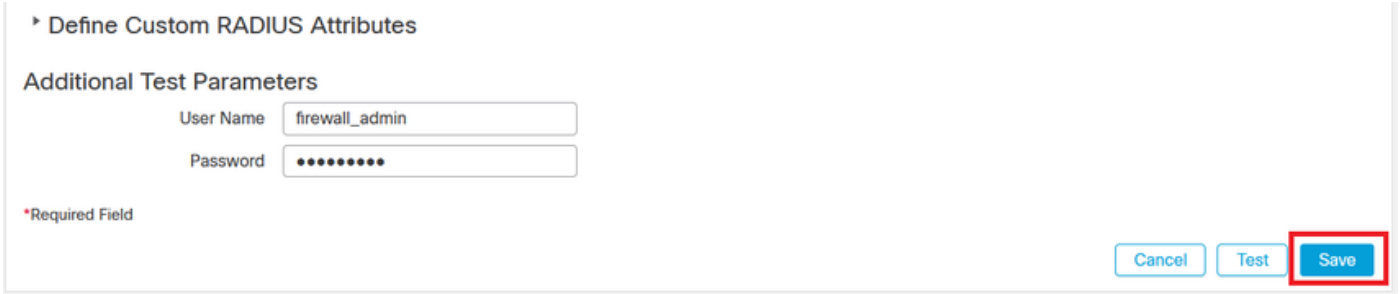


第三步：部署更改。

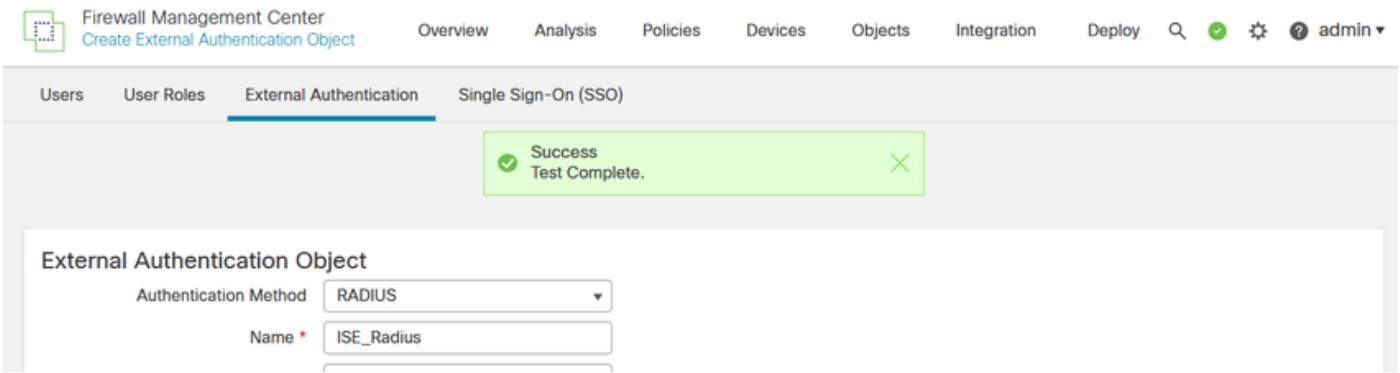


验证

- 测试您的新部署是否正常工作。
- 在FMC GUI中，导航至RADIUS服务器设置并向下滚动至其他测试参数部分。
- 输入ISE用户的用户名和密码，然后点击测试。



- 成功的测试在浏览器窗口的顶部显示绿色的成功测试完成消息。



- 有关详细信息，可以展开测试输出下的Details。

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name: firewall_admin

Password: ••••••••••

Test Output

Show Details ▾

User Test:

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxxhXof/radiusclient_0.conf
radiusauth - response: |User-Name=firewall_admin|
radiusauth - response: |Class=Administrator|
radiusauth - response: |Class=CACS:c0a8c05a_CNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67|
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: |Class=Administrator| - |Class=Administrator| **********
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

Cancel Test Save

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）。