配置 FMC 和 FTD 使用 ISE 作为 RADIUS 服务器进行外部身份验证

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
  - 添加网络设备
  - 创建本地用户身份组和用户
  - 创建授权配置文件
  - 添加新策略集
- FMC配置
  - 添加用于FMC身份验证的ISE RADIUS服务器
- FTD配置
  - 添加用于FTD身份验证的ISE RADIUS服务器
  - 启用RADIUS服务器

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/或外壳对Cisco安全防火墙管理中心进行初始配置。
- 在ISE上配置身份验证和授权策略。
- 基本RADIUS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 7.4.2
- vFTD 7.4.2
- ISE 3.3

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

当您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。

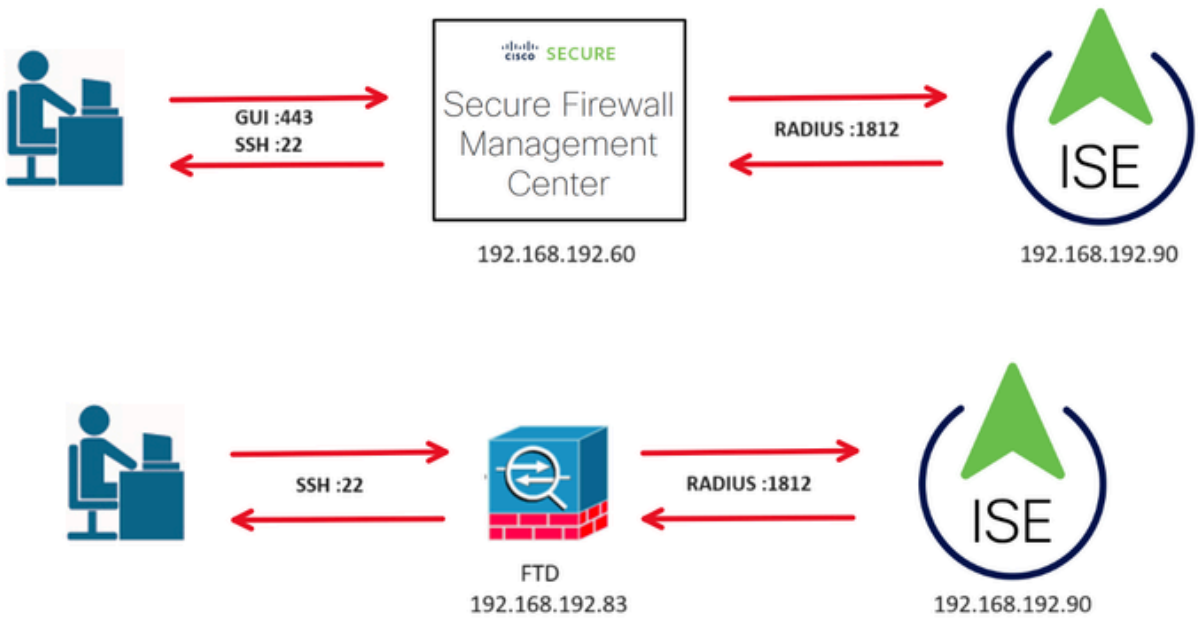
FMC的外部身份验证

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，只能激活一个外部身份验证对象。

网络拓扑



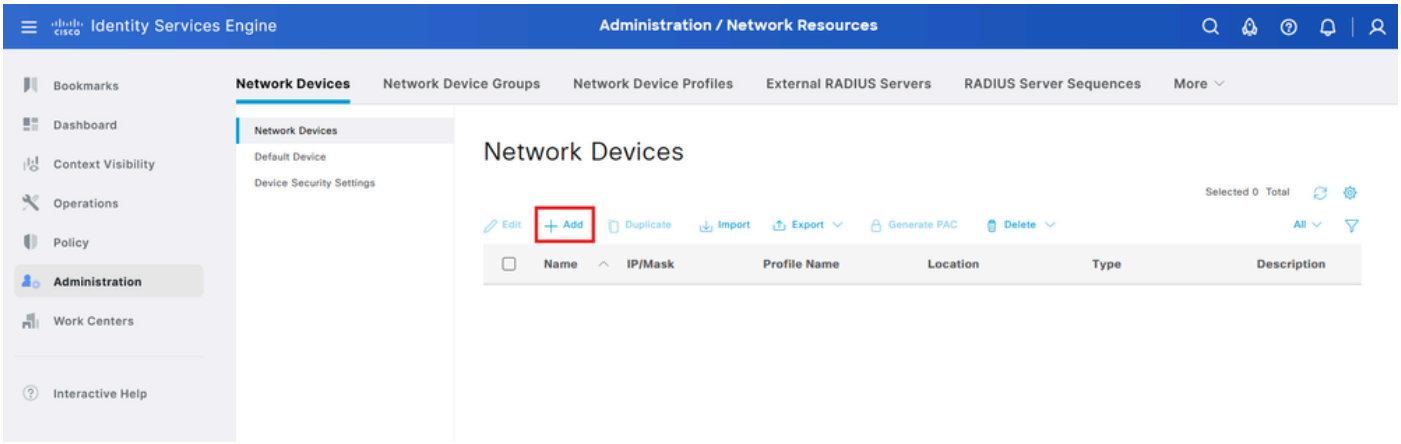
配置

ISE 配置

注意：设置网络接入设备(NAD)（例如FMC）的ISE身份验证和授权策略的方法有多种。本文档中介绍的示例是一个参考点，在该参考点中，我们创建了两个配置文件（一个具有管理员权限，另一个为只读），并可根据基线进行调整以访问您的网络。可以在ISE上定义一个或多个授权策略，将RADIUS属性值返回到FMC，然后映射到FMC系统策略配置中定义的本地用户组。

添加网络设备

步骤1.导航到burger图标 ☰ 位于左上角Administration > Network Resources > Network Devices > +Add。

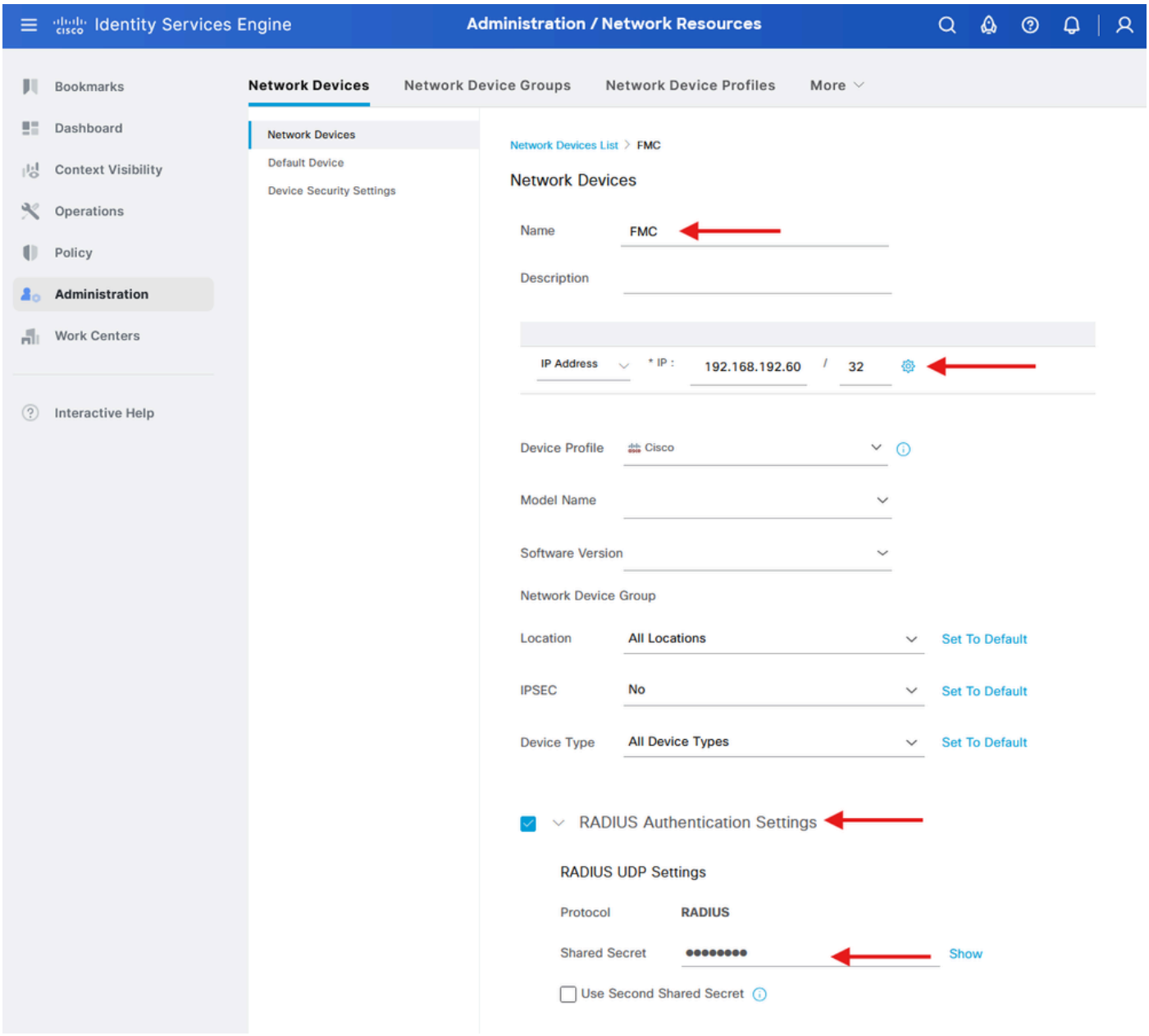


步骤2.为网络设备对象分配名称，并插入FMC IP地址。

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。

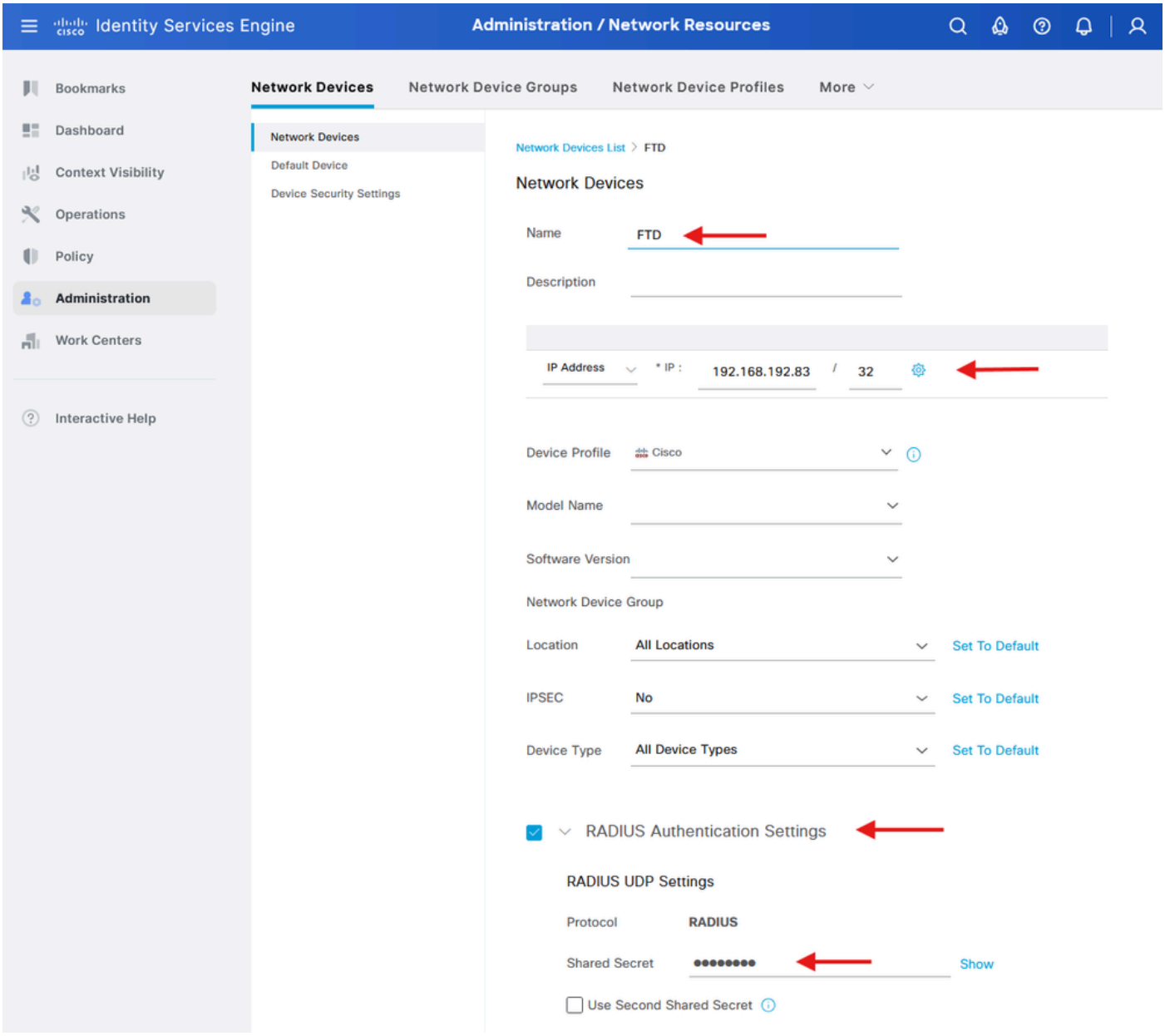


步骤2.1.重复上述步骤以添加FTD。

为网络设备对象分配Name并插入FTD IP地址。

选中RADIUS复选框并定义一个共享密钥。

完成后，单击Save。

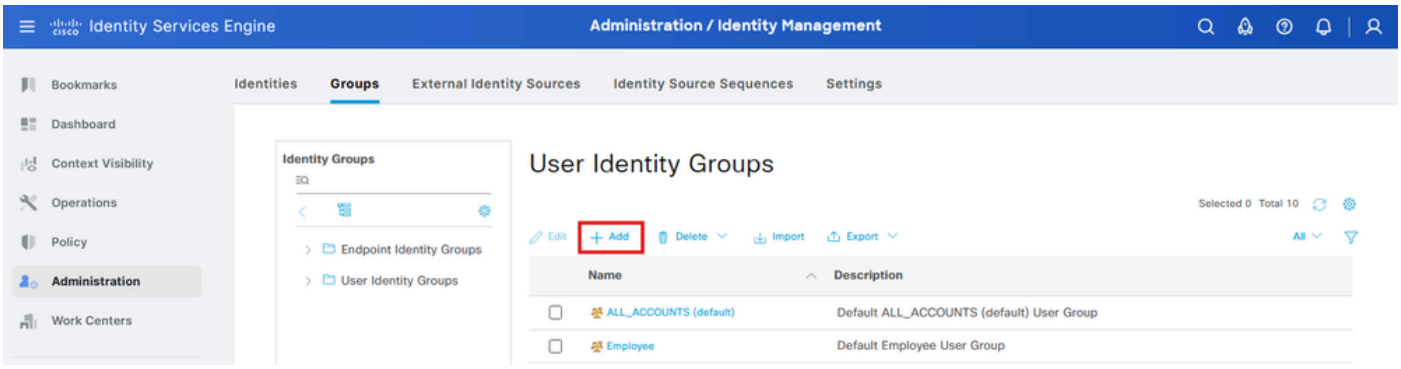


步骤2.2.验证Network Devices下显示的两个设备。

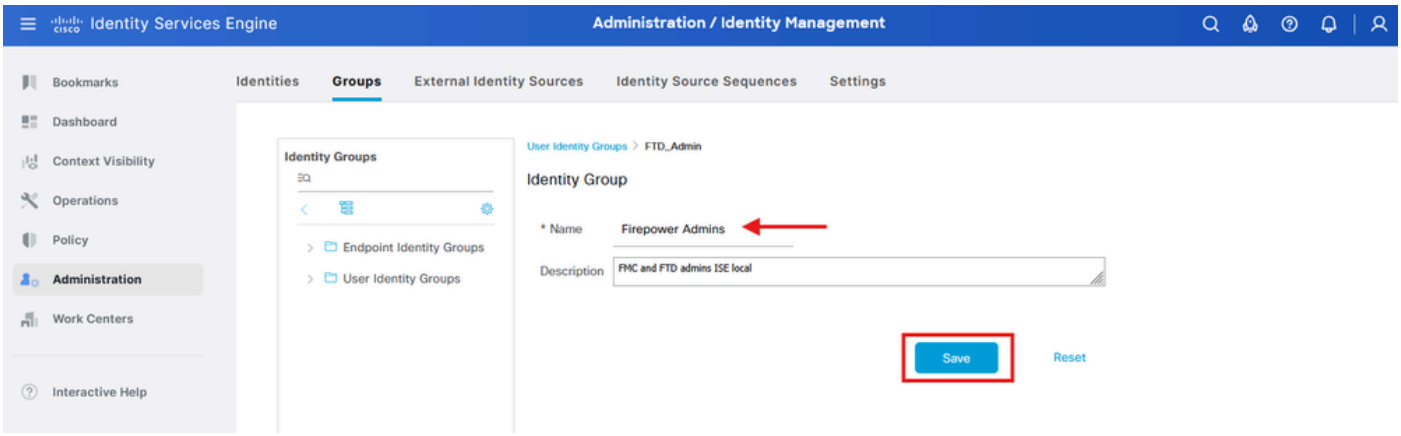


创建本地用户身份组和用户

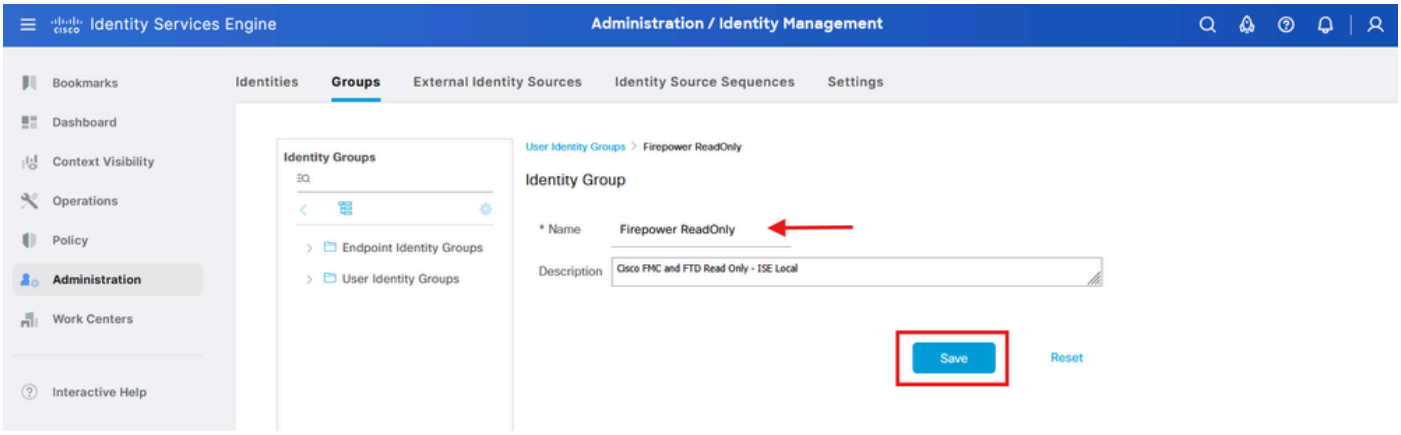
步骤3.创建所需的用户身份组。导航到Burger图标 ☰ 位于左上角Administration > Identity Management > Groups > User Identity Groups > + Add



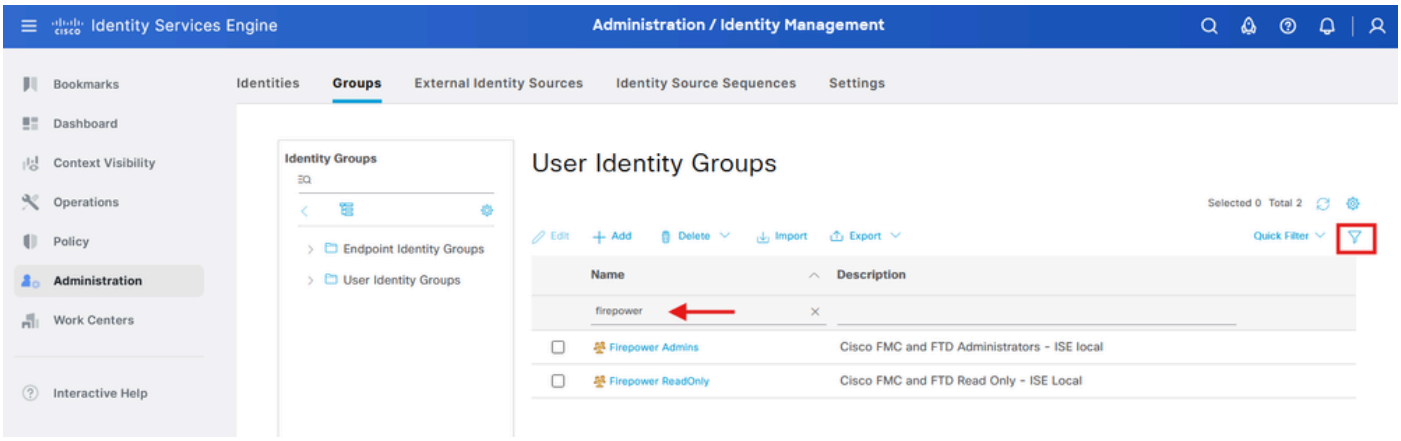
步骤4.为每个组指定一个名称并单独保存。在本示例中，您正在为管理员用户创建一个组，为只读用户创建另一个组。首先，为具有管理员权限的用户创建组。



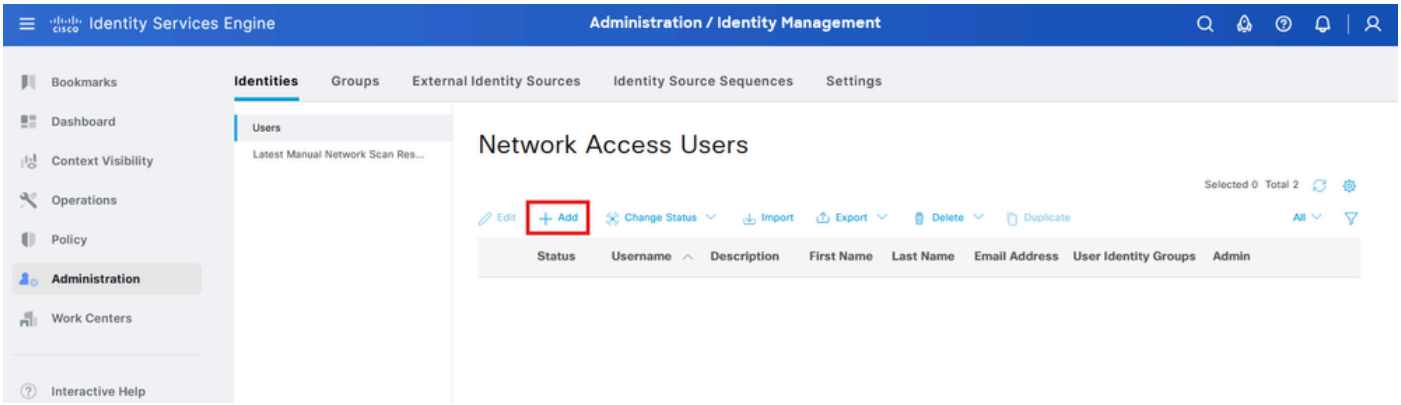
步骤4.1.为只读用户创建第二个组。



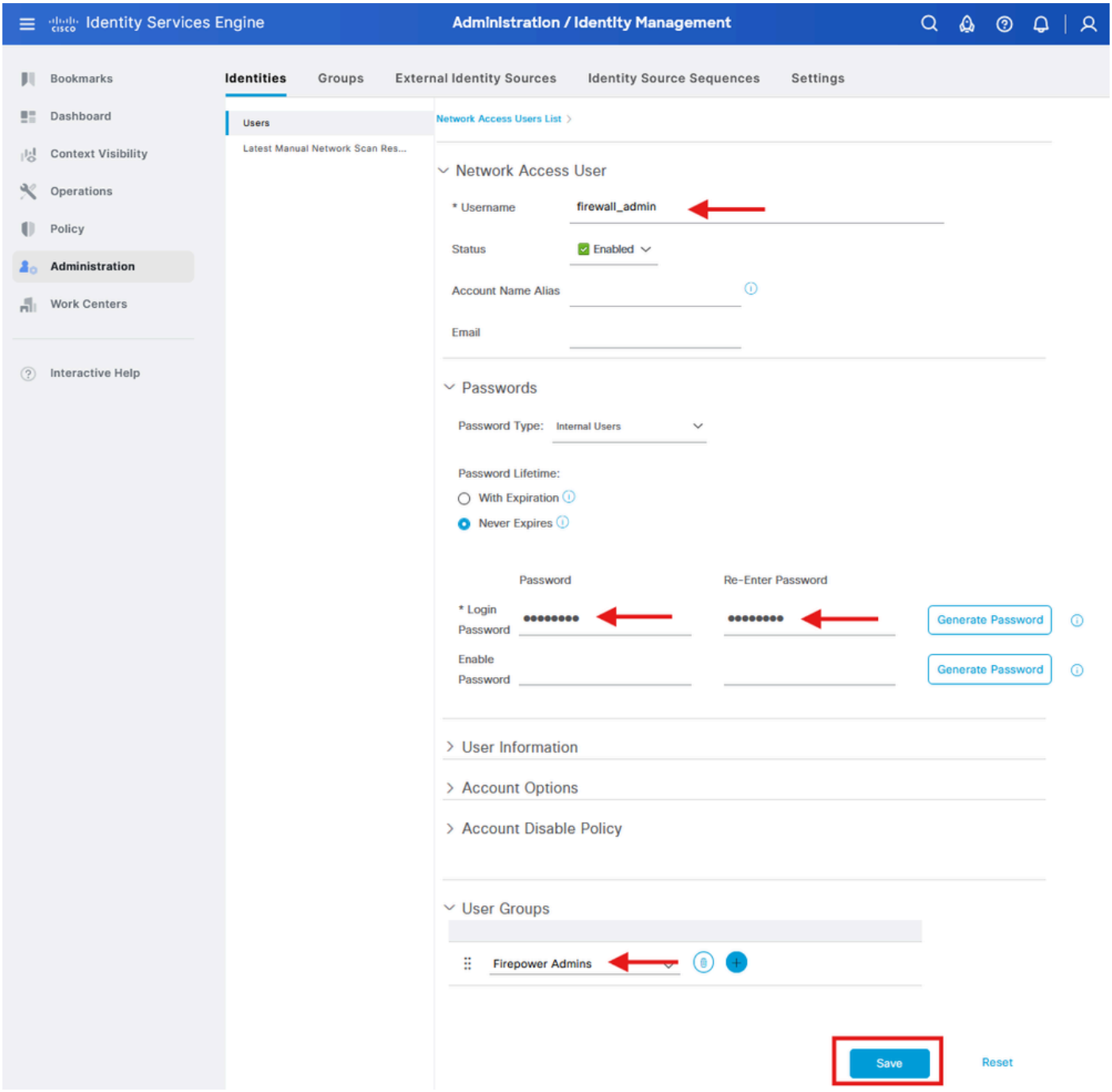
步骤4.2.验证两个组显示在User Identity Groups List下。使用过滤器可以轻松找到它们。



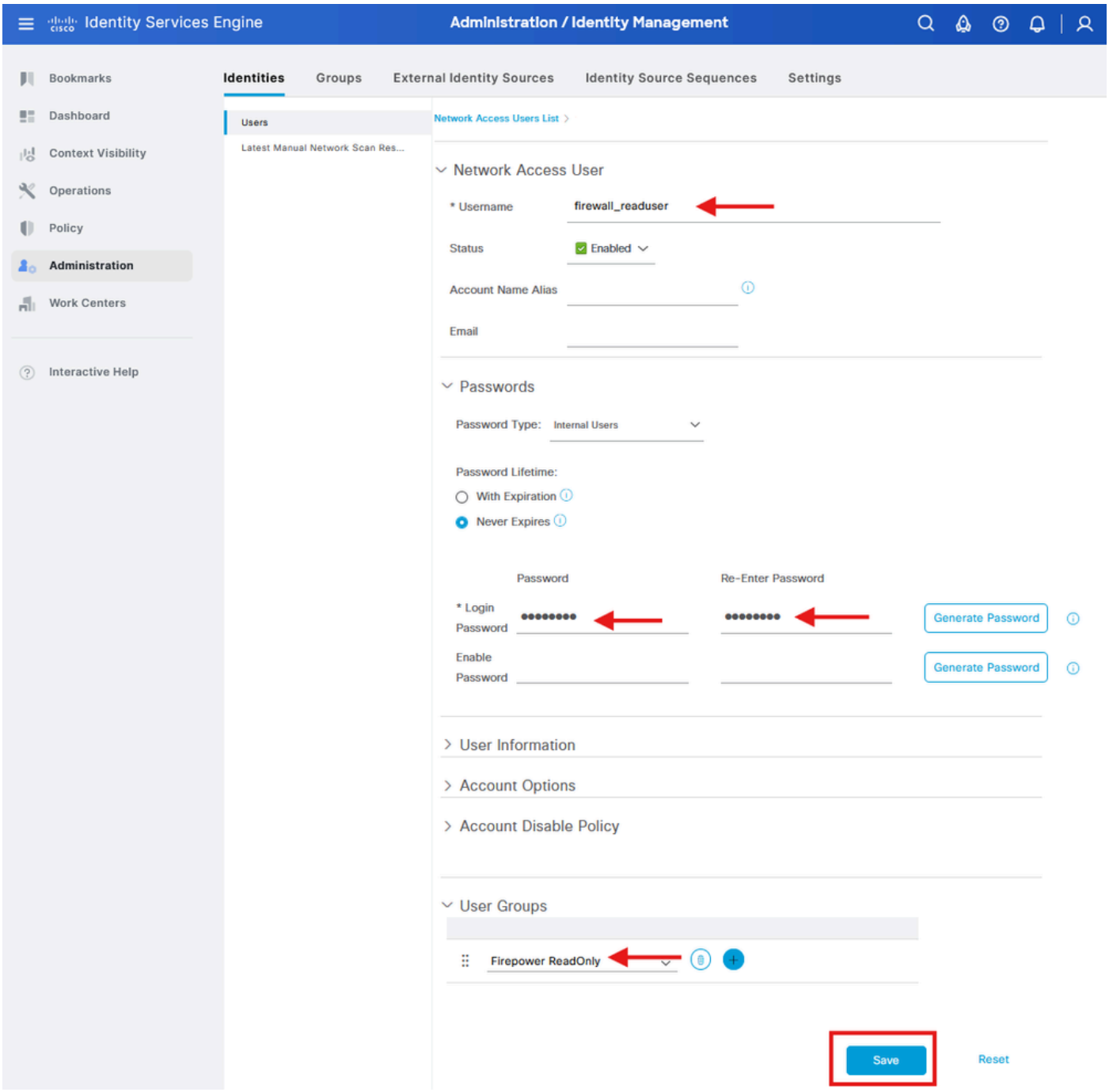
步骤5.创建本地用户并将他们添加到对应组中。依次导航至 ☰ > Administration > Identity Management > Identities > + Add。



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Firepower Admins组。



步骤5.2.添加具有只读权限的用户。分配名称、密码和Firepower ReadOnly组。



创建授权配置文件

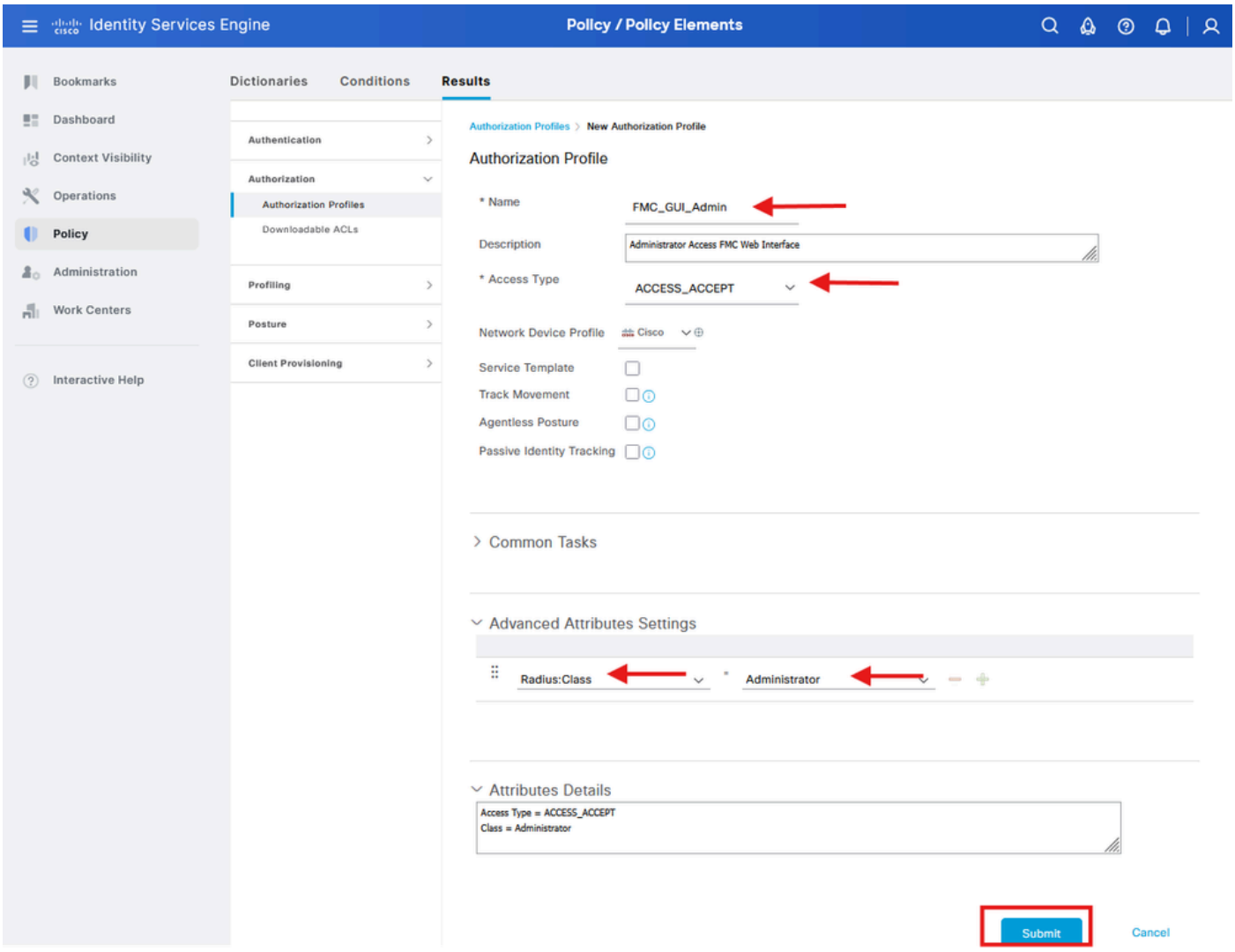
步骤6.为FMC Web界面管理员用户创建授权配置文件。

依次导航至 ☰ >Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add。

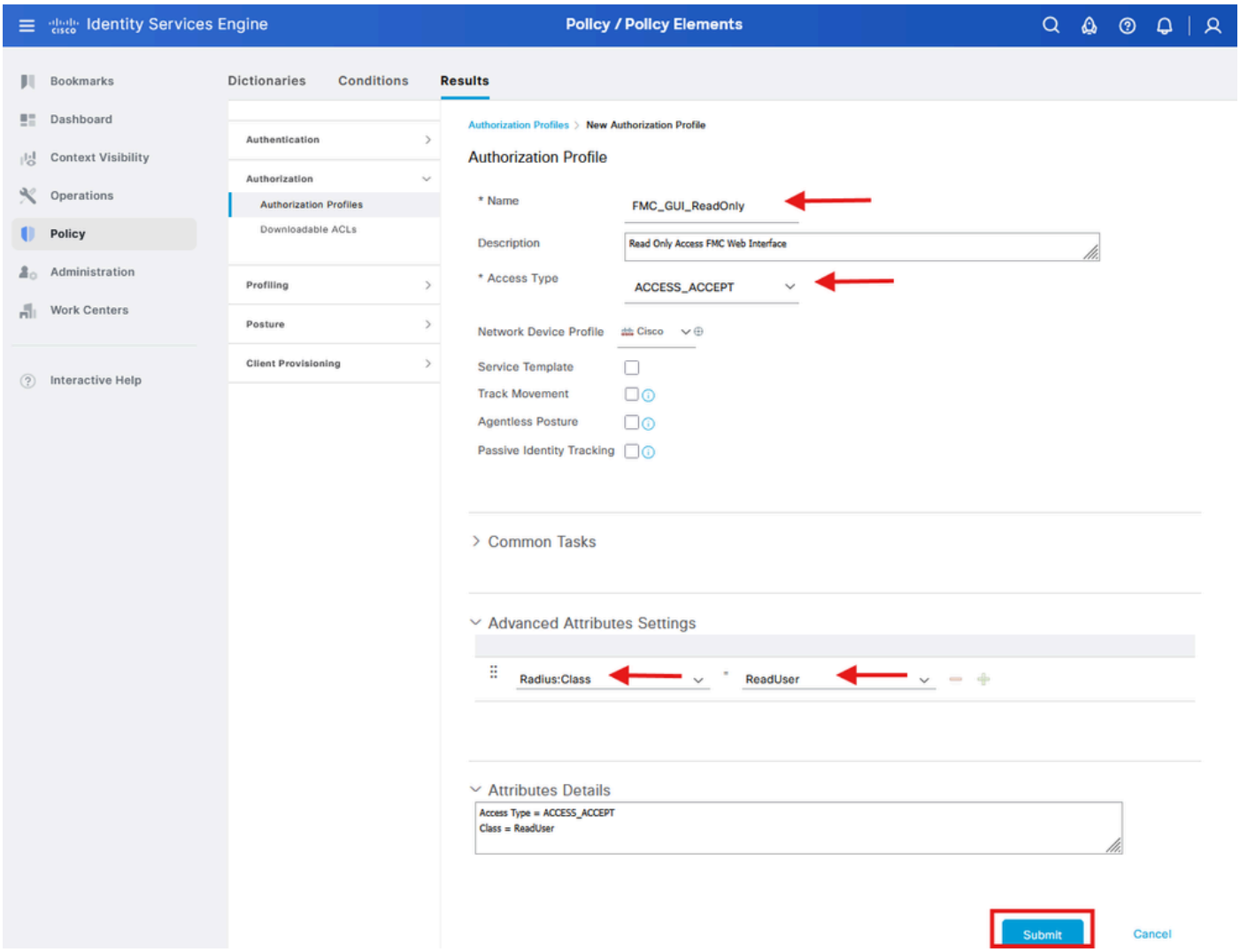
定义授权配置文件的名称，将Access Type保留为ACCESS_ACCEPT。

在“高级属性设置”(Advanced Attributes Settings)下，添加Radius > Class— [25]和值

Administrator，然后单击提交。



步骤6.1.重复上述步骤，为FMC Web界面只读用户创建授权配置文件。这次使用值ReadUser代替Administrator创建Radius类。



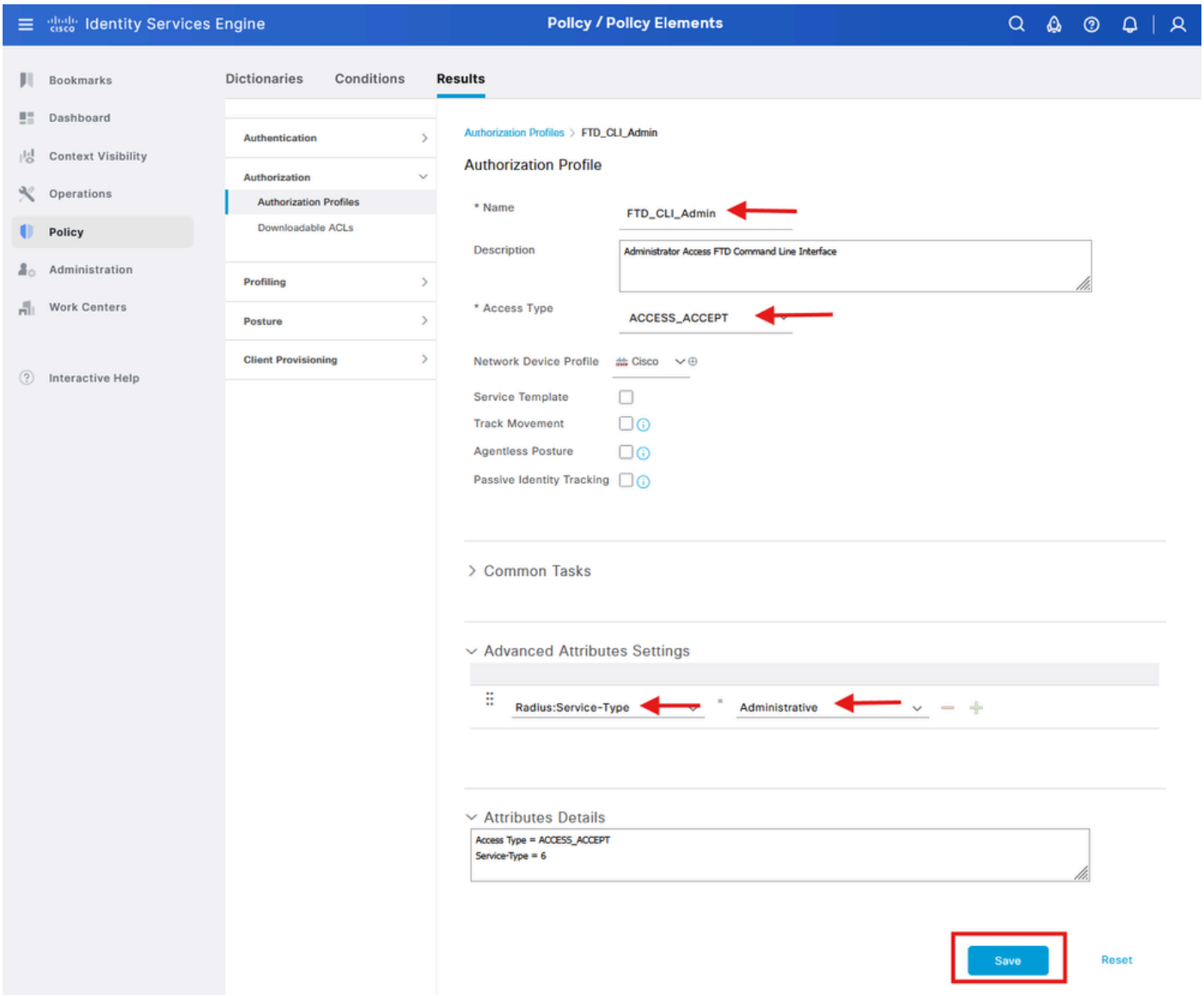
注意：对于FMC（所有版本）和FTD（6.2.3和6.3），必须在FMC外部身份验证对象中定义命令行界面(CLI)访问用户，如步骤4中的FMC配置程序所示。对于FTD 6.4及更高版本，建议在RADIUS服务器上定义用户，如下一步所示。

步骤7.创建具有管理员权限的FTD CLI用户的授权配置文件。

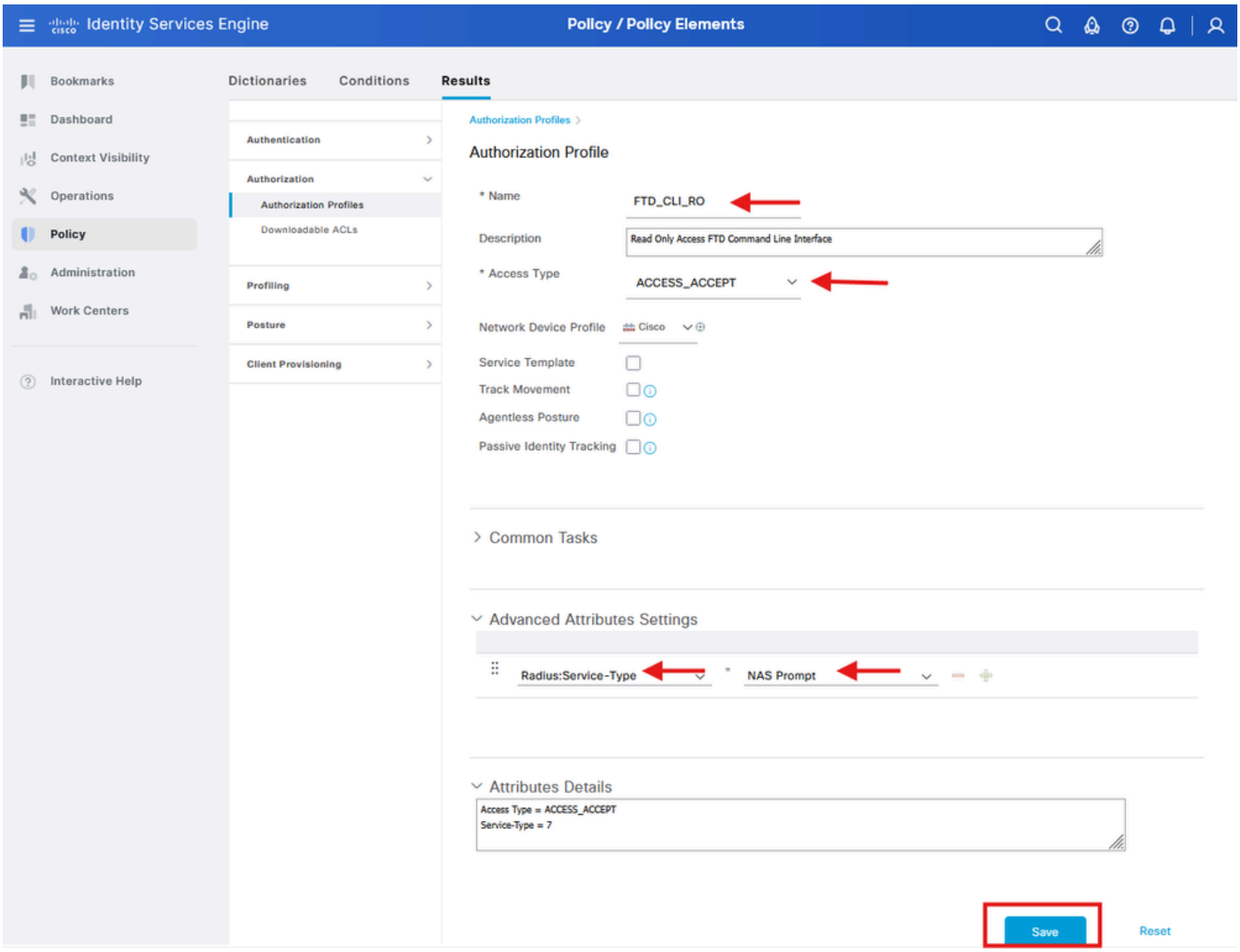
依次导航至 ☰ >Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add。

定义授权配置文件的名称，将Access Type保留为ACCESS_ACCEPT。

在Advanced Attributes Settings下，添加值为Administrative 的Radius > Service-Type - [6]，然后单击Submit。



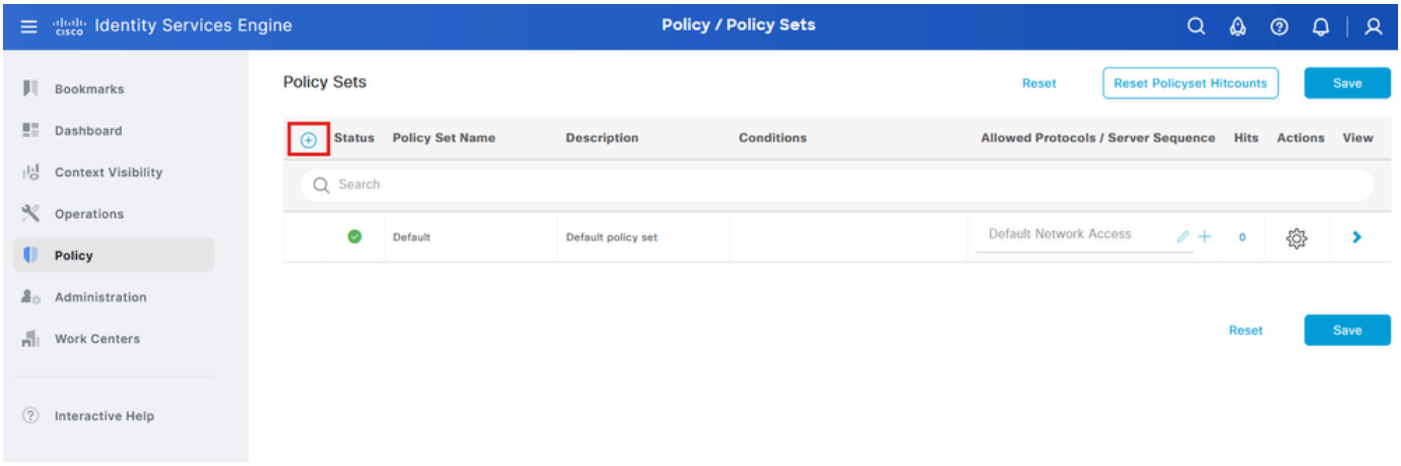
步骤7.1.重复上一步为FTD CLI只读用户创建授权配置文件。这次改为使用NAS Prompt值创建Radius > Service-Type -[6]。



添加新策略集

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。

依次导航至 ☰ >策略>策略集> ⊕ 图标位于左上角。

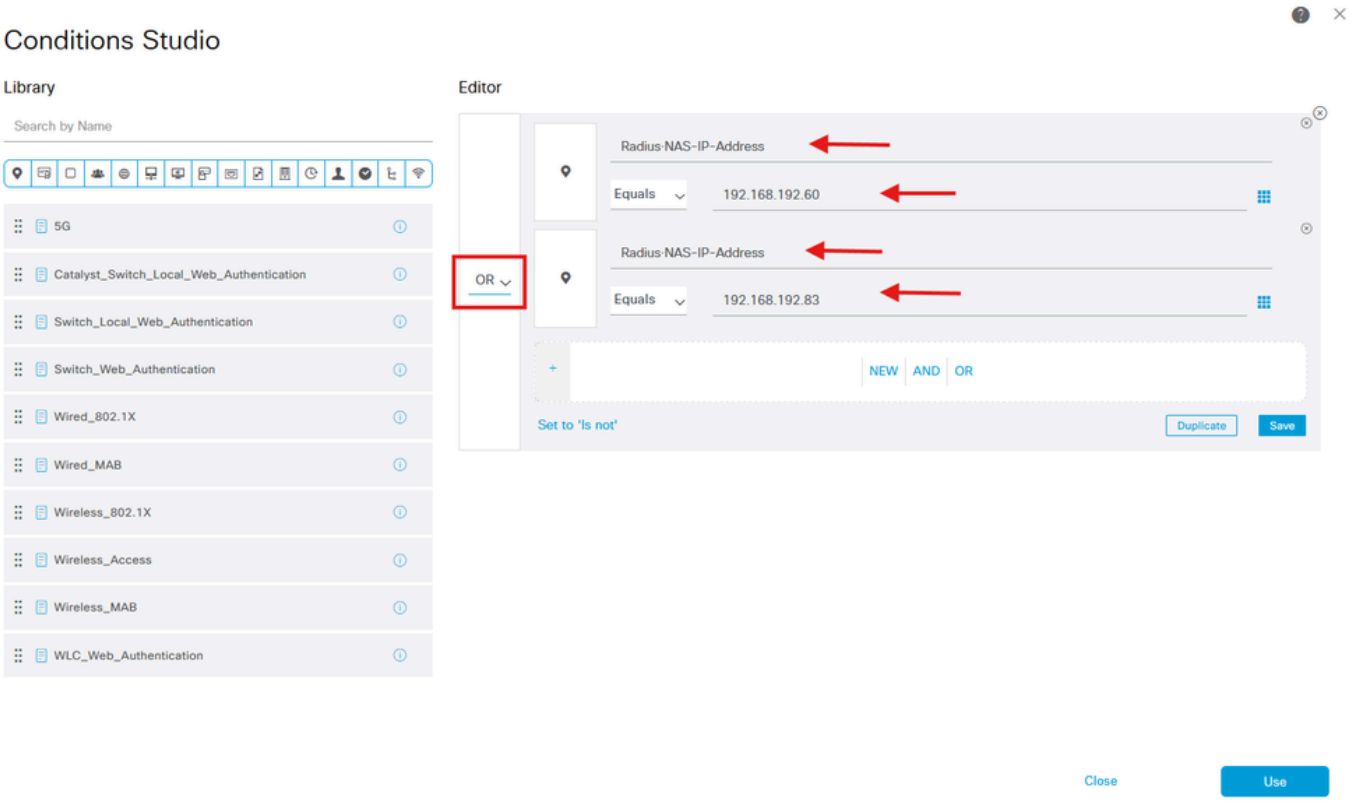


步骤8.1.新行位于策略集的顶部。

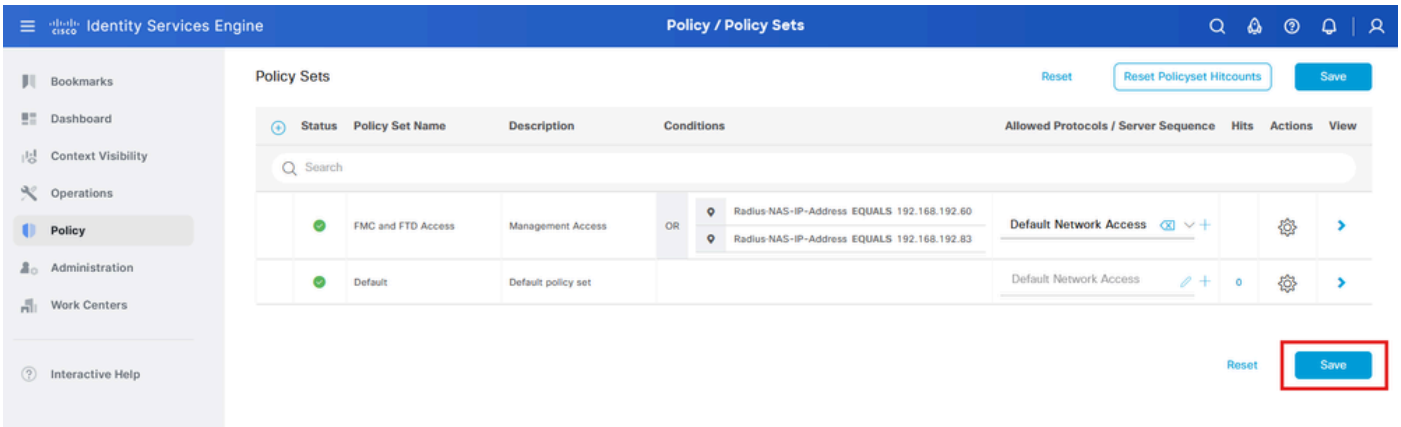
为新的策略命名，并为与FMC IP地址匹配的RADIUS NAS-IP-Address属性添加一个顶部条件。

添加带或的第二个条件，以包括FTD的IP地址。

单击Use以保留更改并退出编辑器。



第8.2步：完成后，选择保存。

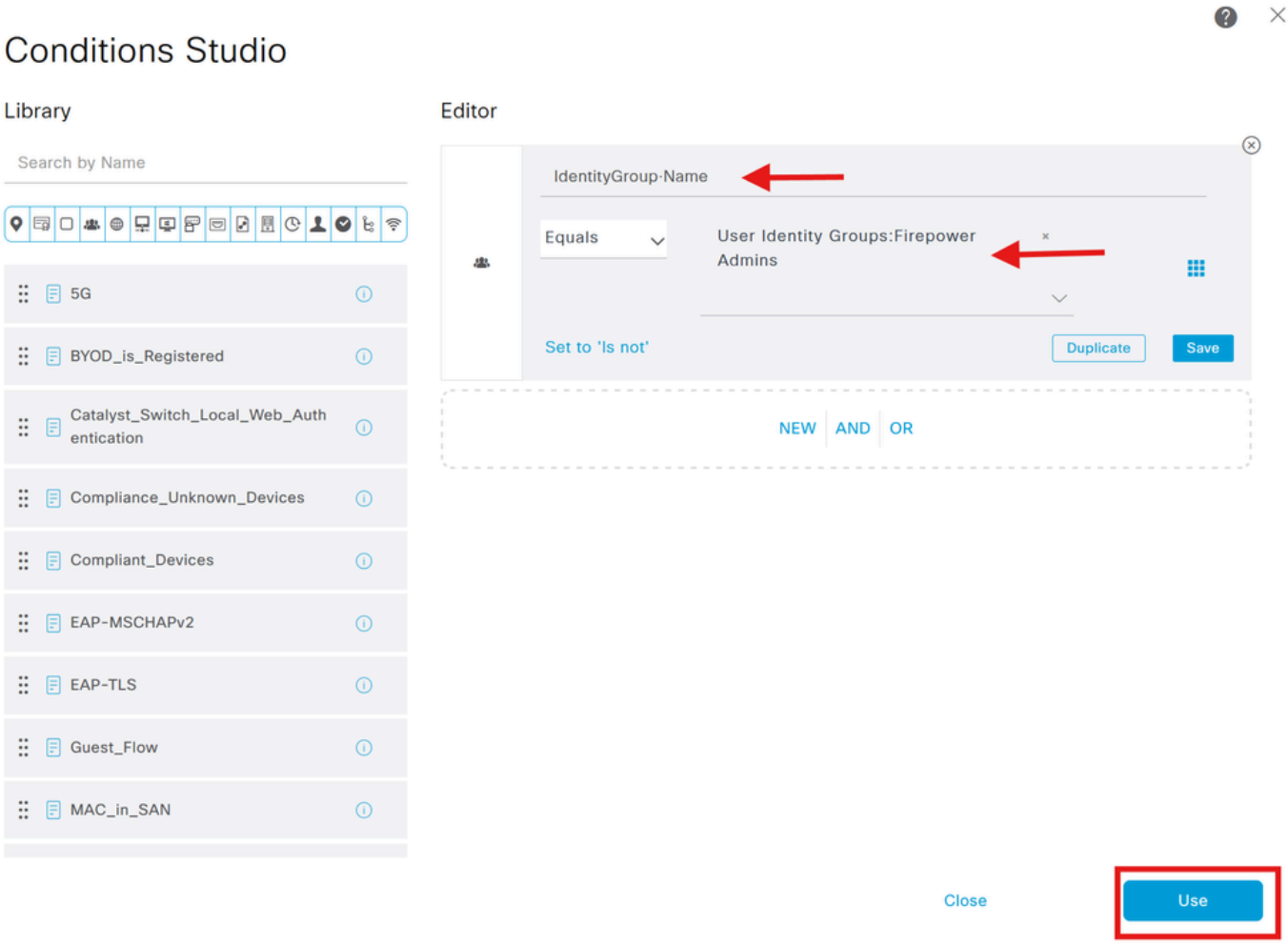


提示：在本练习中，允许从Default Network Access Protocols列表执行该操作。您可以创建新列表并根据需要缩小其范围。

步骤9.通过选择 位于行尾的图标。

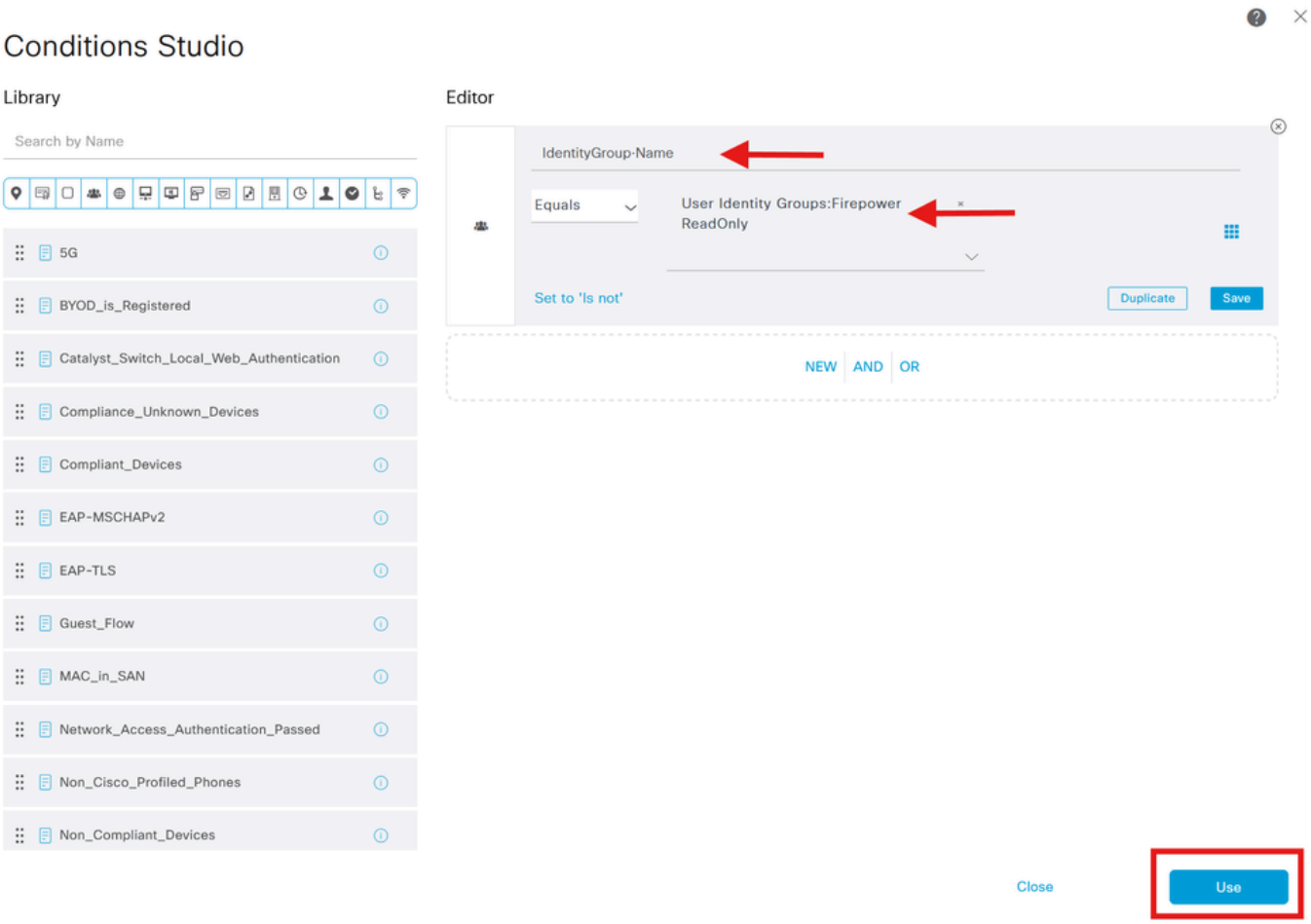
展开Authorization Policy菜单并推送 图标添加新的规则，以允许访问具有管理员权限的用户。为其指定名称。

设置条件以匹配Dictionary Identity Group with Attribute Name Equals，然后选择User Identity Groups:Firepower管理员（步骤4中创建的组名称），然后点击使用。

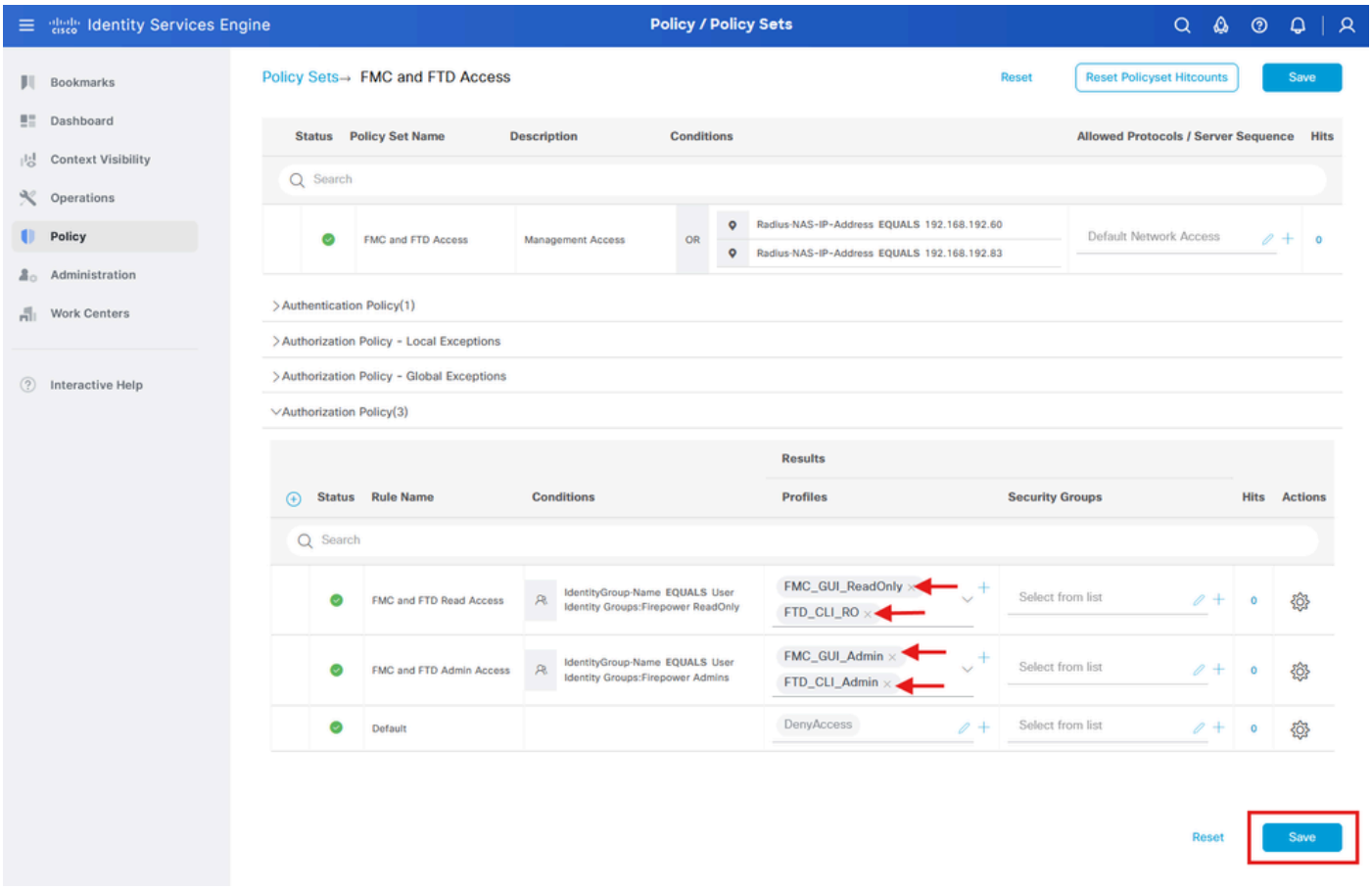


步骤10.单击 图标添加第二条规则，以允许访问具有只读权限的用户。为其指定名称。

设置条件以匹配Dictionary Identity Group with Attribute Name Equals User Identity Groups:Firepower只读（在步骤4.1中创建的组名称），然后点击使用。



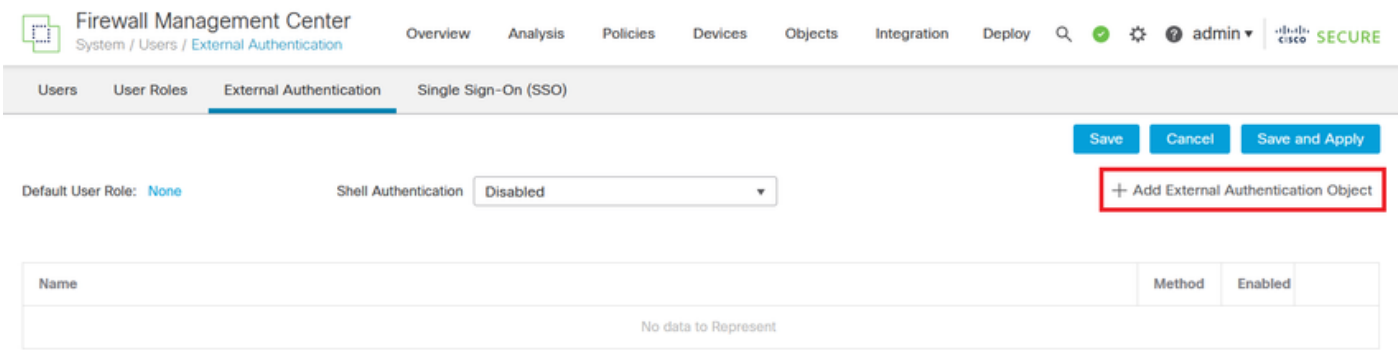
步骤11.分别为每个规则设置Authorization Profiles，然后点击Save。



FMC配置

添加用于FMC身份验证的ISE RADIUS服务器

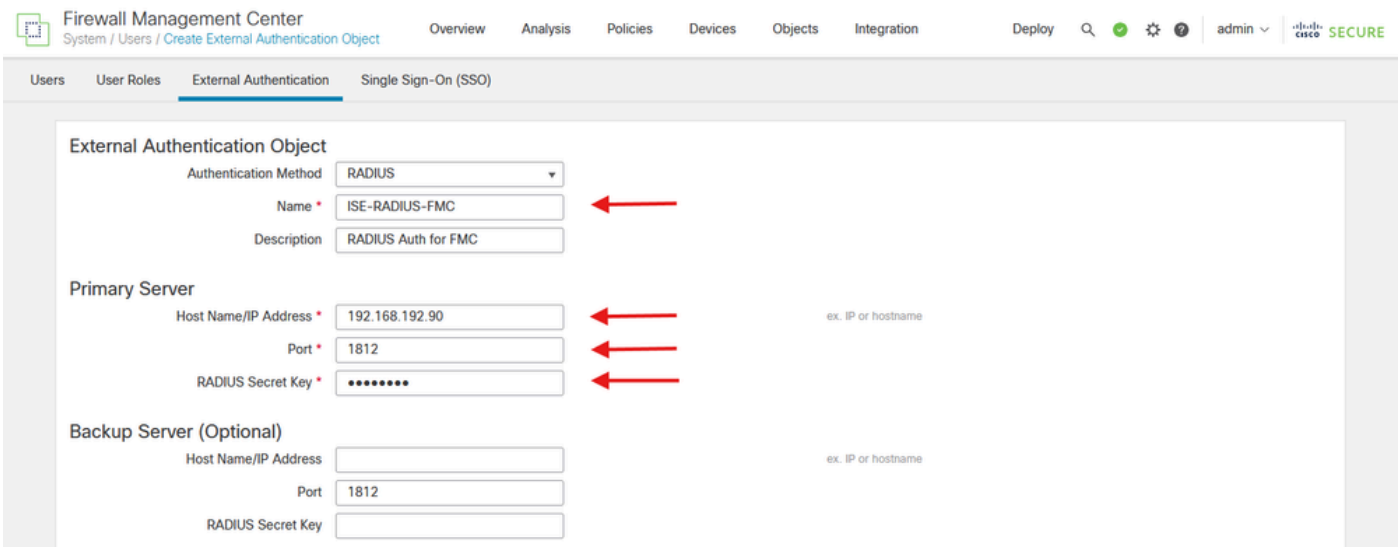
步骤1.在System > Users > External Authentication > + Add External Authentication Object下创建外部身份验证对象。



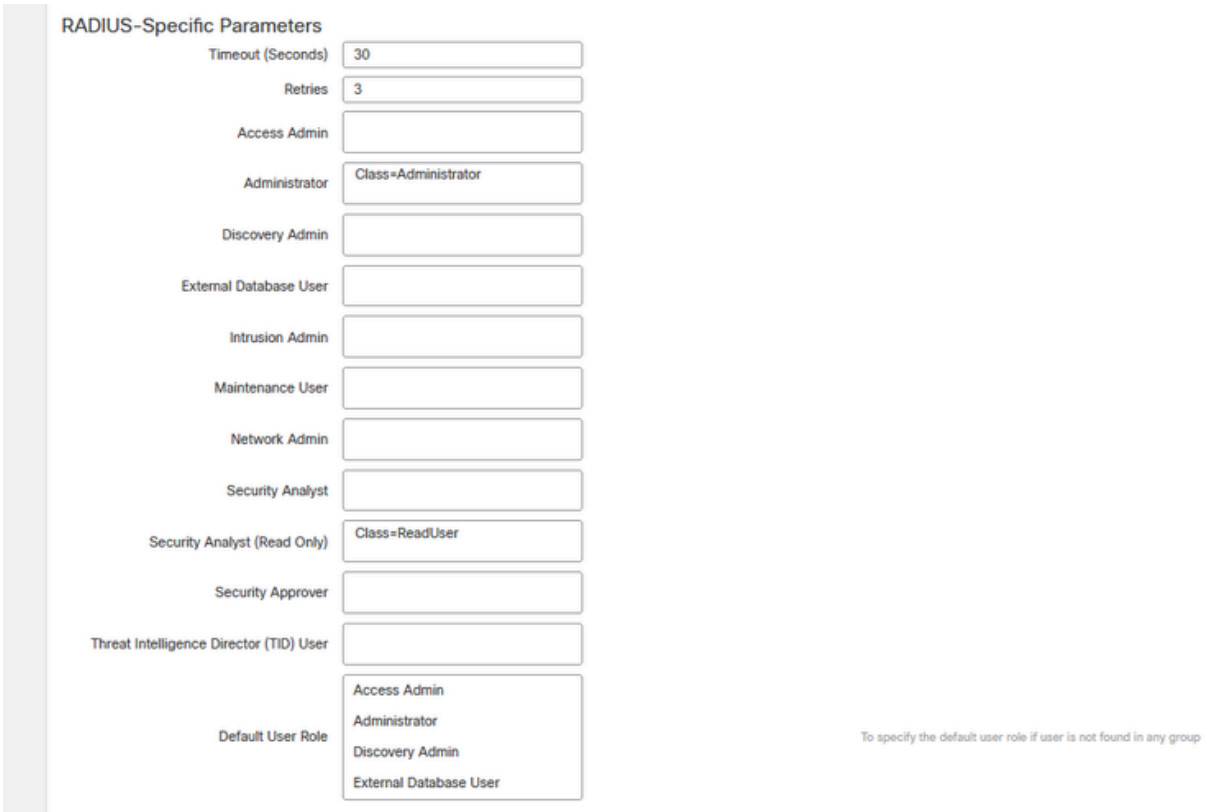
步骤2.选择RADIUS作为身份验证方法。

在External Authentication Object下为新对象指定Name。

接下来，在Primary Server设置中，插入ISE IP地址和您在ISE配置的第2步中使用的RADIUS密钥。

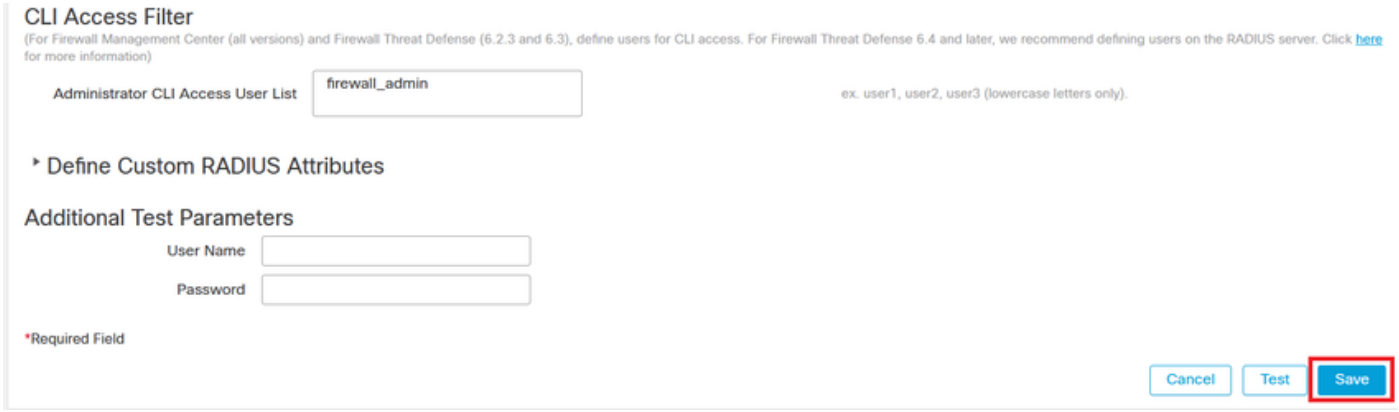


第3步：插入ISE配置的第6步和第7步配置的RADIUS Class属性值：分别用于firewall_admin和firewall_readuser的Administrator和ReadUser。



步骤4.使用必须对FMC具有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。

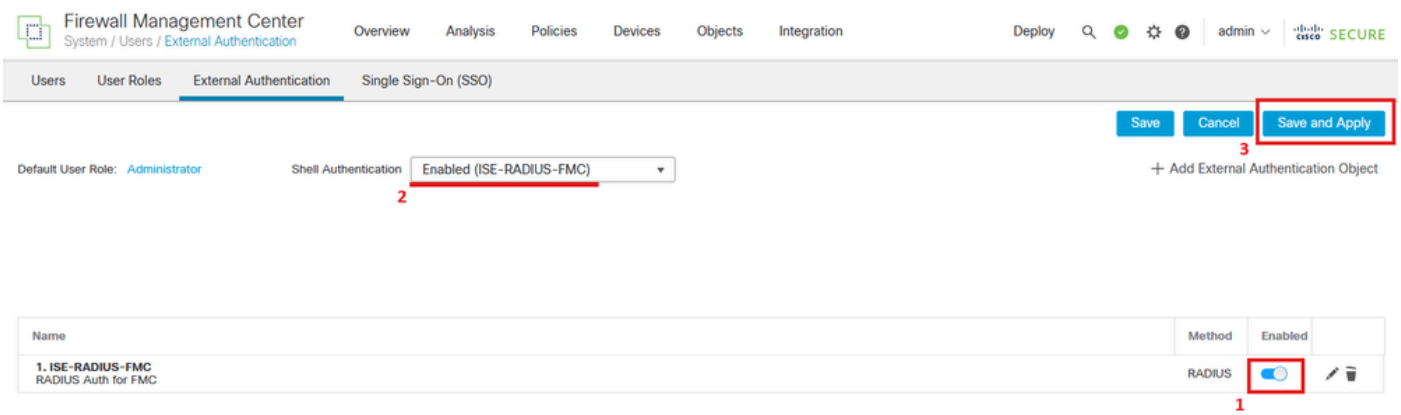
完成后单击Save。



注意：对于FMC CLI访问，必须使用此用户列表。要在防火墙威胁防御使用服务类型属性方法时对FTD和FMC使用同一RADIUS服务器，必须创建两个标识同一RADIUS服务器的外部身份验证对象：一个对象包括预定义的CLI访问过滤器用户（用于FMC），另一个对象将CLI访问过滤器留空（用于FTD）。

警告：使用expert命令，任何具有CLI访问FMC的用户都可以获得Linux shell访问权限。Linux shell用户可以获得root权限，这会带来安全风险。确保使用CLI或Linux外壳访问限制用户列表。

步骤5.启用新对象。将其设置为FMC的Shell身份验证方法，然后单击Save和Apply。

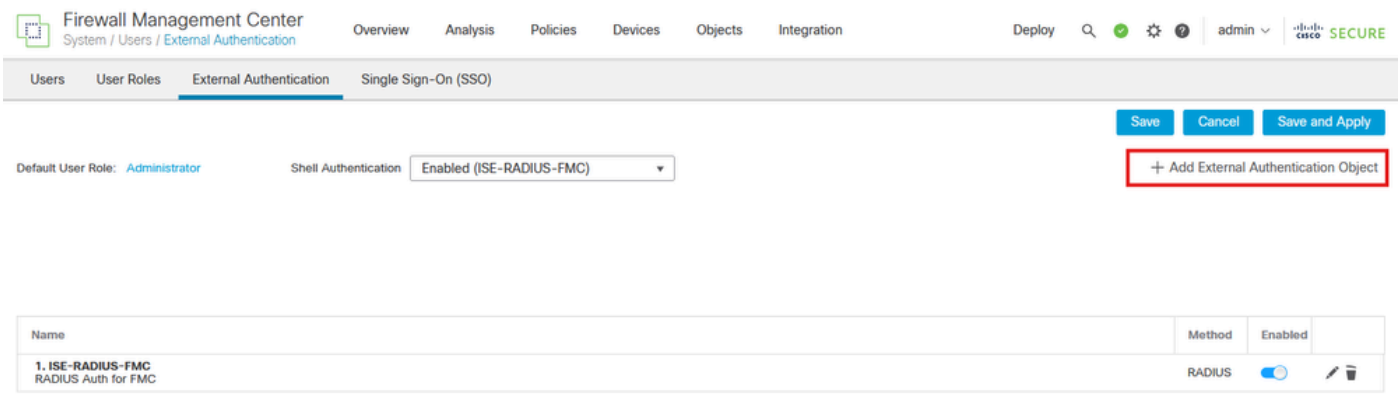


FTD配置

添加用于FTD身份验证的ISE RADIUS服务器

注意：您可以在管理中心和设备之间共享同一对象，也可以创建单独的对象，具体取决于您要定义用户的位置及其必须具有的授权级别。在此场景中，您是在RADIUS服务器上定义用户，因此您需要为威胁防御和管理中心创建单独的对象。

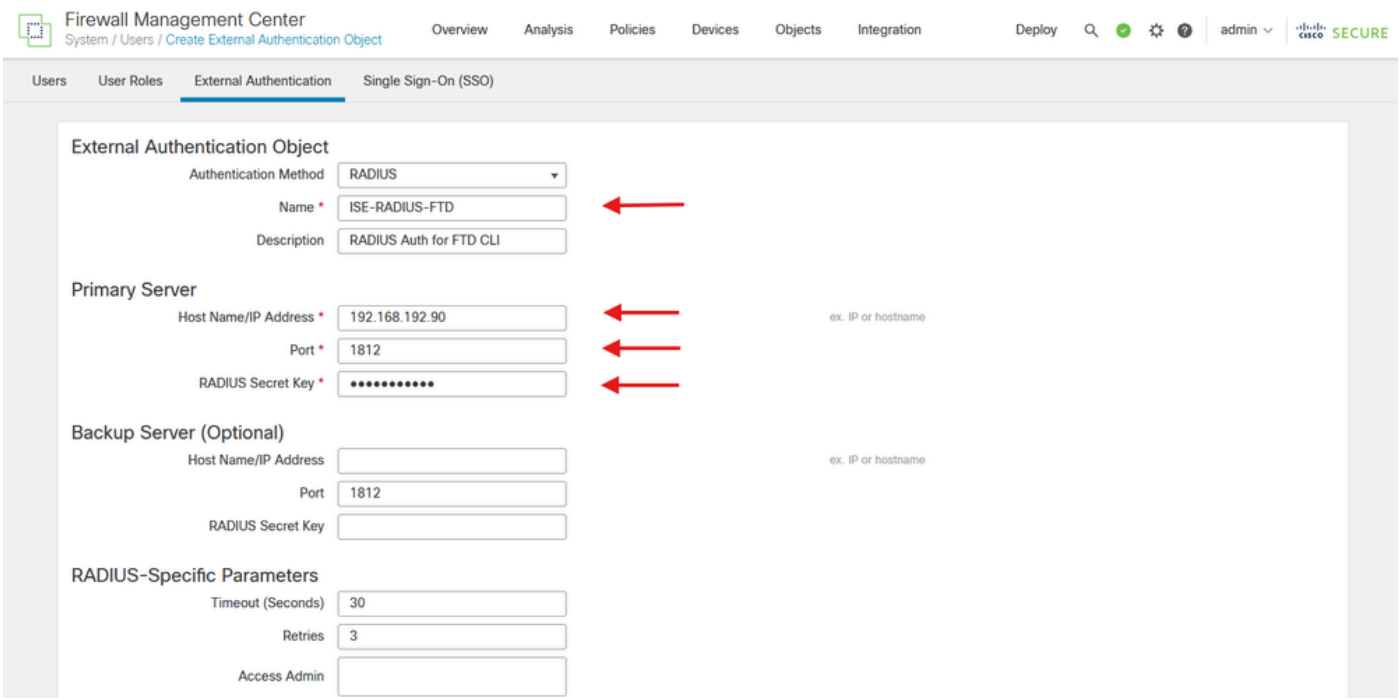
步骤1.与对FMC所做的相同，在System > Users > External Authentication > + Add External Authentication Object下创建External Authentication Object。



步骤2.选择RADIUS作为身份验证方法。

在External Authentication Object下为新对象指定Name。

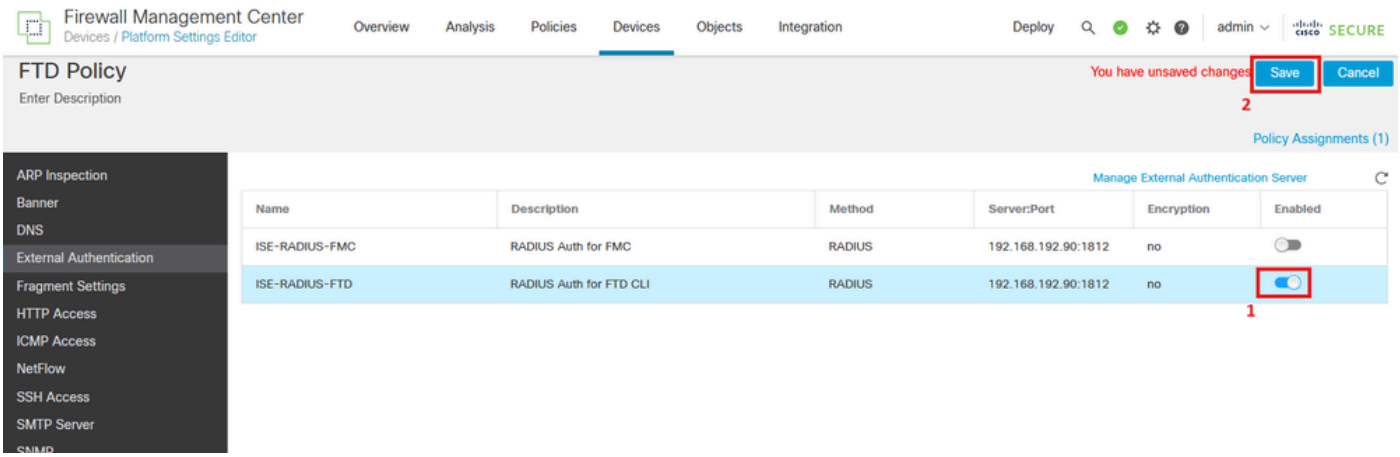
接下来，在Primary Server设置中，插入ISE IP地址和您在ISE配置的第2.1步中使用的RADIUS密钥。点击保存



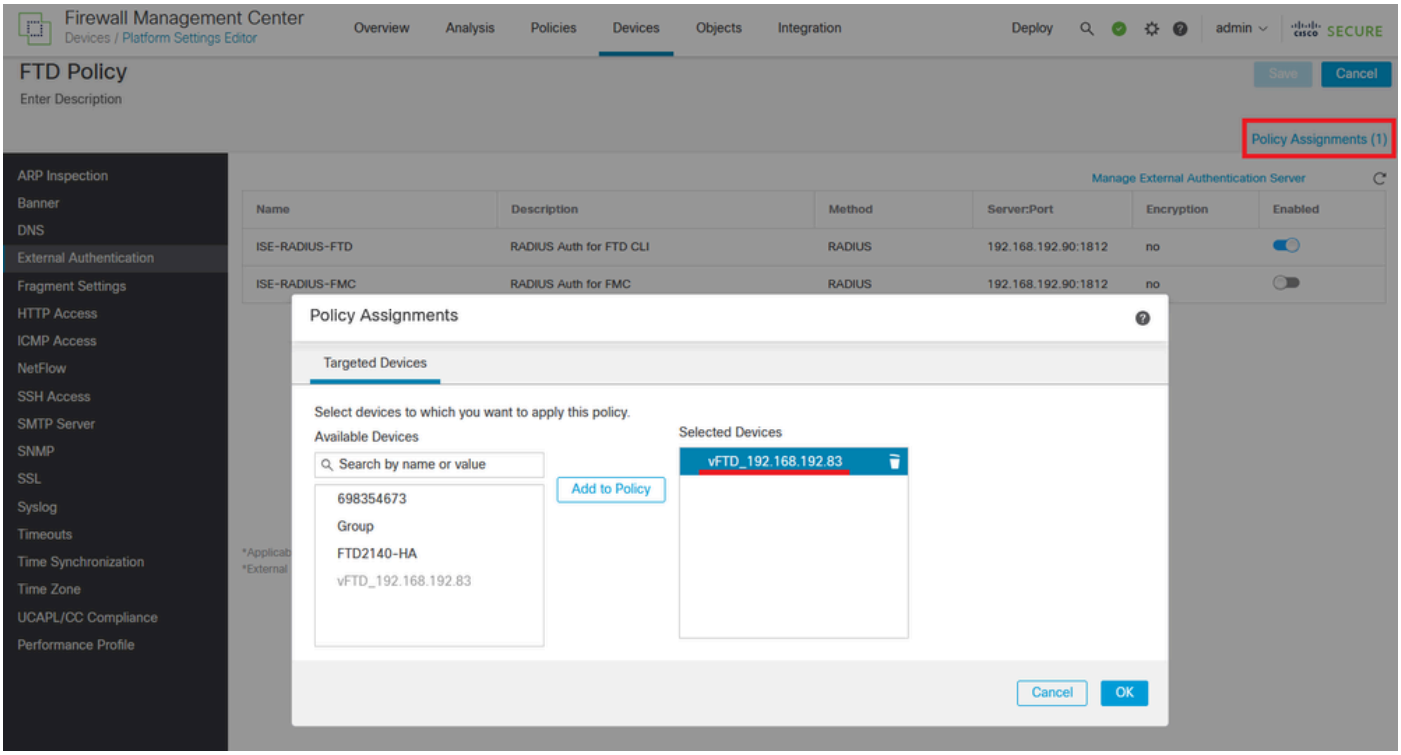
警告：FTD和FMC的超时范围不同，因此，如果您共享对象并更改默认值30秒，请确保不要超过FTD设备的较小超时范围（1-300秒）。如果将超时设置为更高的值，威胁防御RADIUS配置将不起作用。

启用RADIUS服务器

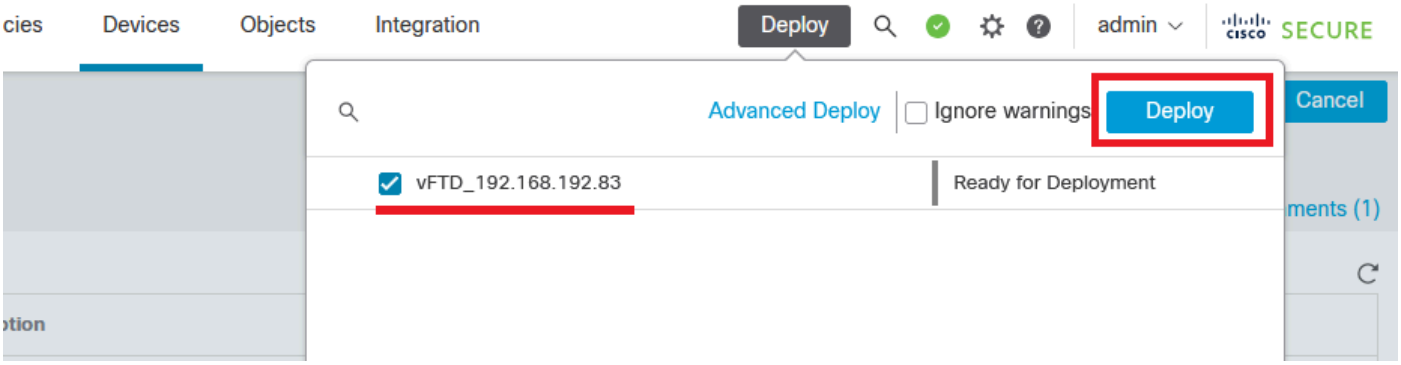
第1步：在FMC GUI中，导航到设备>平台设置>编辑当前策略，或者创建新的策略（如果您未将任何策略分配给需要访问的FTD）。在External Authentication下启用RADIUS服务器，然后单击Save。



步骤2.确保您需要获得访问权限的FTD列在“Policy Assignments as a Selected Device”下。



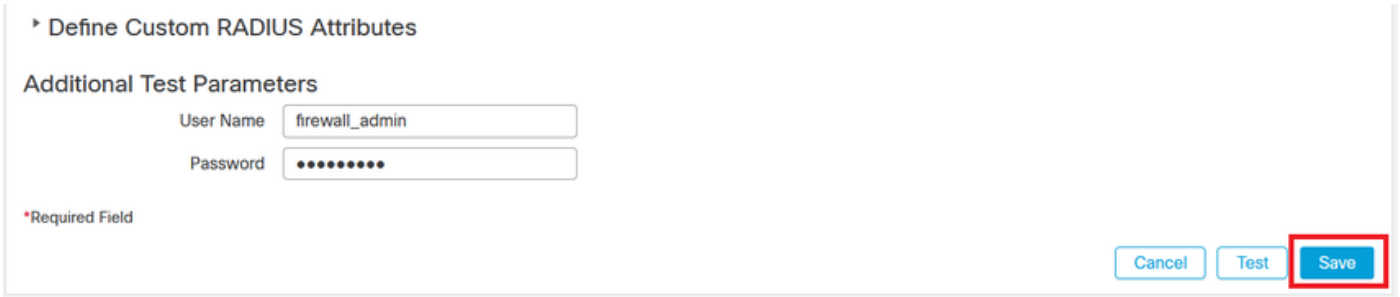
步骤3.部署更改。



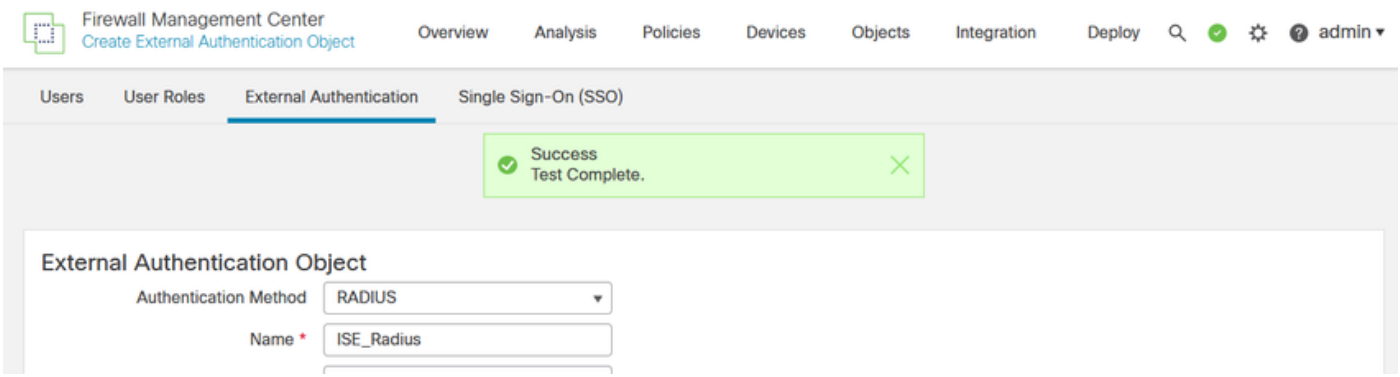
注意：如果以前使用configure user add命令将某个现有的外部用户名配置为内部用户，则威胁防御会首先针对内部用户检查密码，如果检查失败，则检查RADIUS服务器。以后无法添加与外部用户同名的内部用户，因为部署可能会失败；仅支持预先存在的内部用户。

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Additional Test Parameters部分。
- 输入ISE用户的用户名和密码，然后单击测试。



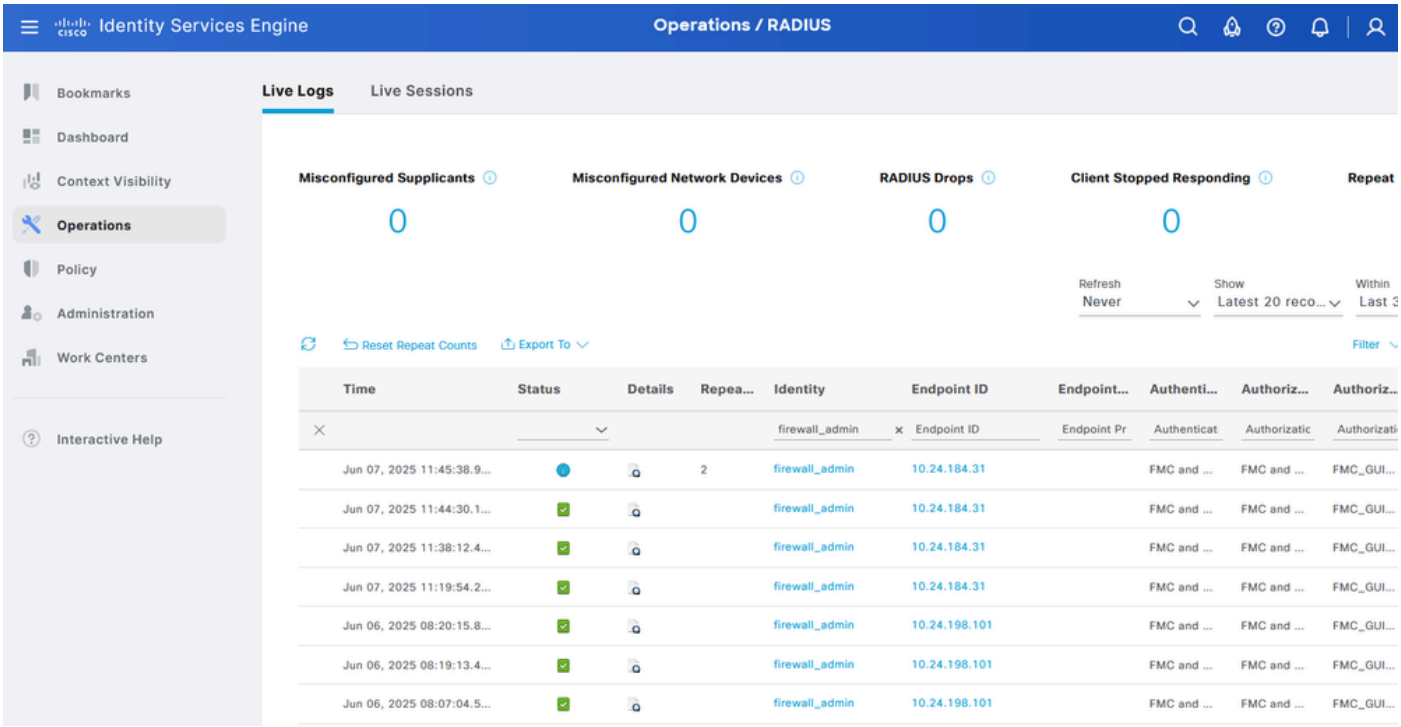
- 成功的测试在浏览器窗口的顶部显示绿色的Success Test Complete消息。



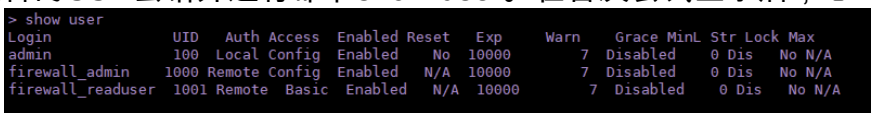
- 有关详细信息，可以展开测试输出下的详细信息。



- 在操作> RADIUS >实时日志下，检查ISE RADIUS中的身份验证请求和响应。



- 对于FTD身份验证，请打开与设备的SSH会话并运行命令show user。在首次尝试登录后，您会看到外部用户及其访问级别。



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）。