FireSIGHT系统与用于RADIUS用户身份验证的ACS 5.x集成

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[配置](#)

- [ACS 5.x配置](#)
  - [配置网络设备和网络设备组](#)
  - [在ACS中添加身份组](#)
  - [将本地用户添加到ACS](#)
  - [配置ACS策略](#)
- [FireSight管理中心配置](#)
  - [FireSight管理器系统策略配置](#)
  - [启用外部身份验证](#)

[确认](#)

[相关的思科支持社区讨论](#)

简介

本文档介绍将Cisco FireSIGHT管理中心(FMC)或Firepower受管设备与思科安全访问控制系统5.x (ACS)集成以进行远程身份验证拨入用户服务(RADIUS)用户身份验证所需的配置步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 通过GUI和/或外壳进行FireSIGHT系统和受管设备的初始配置
- 在ACS 5.x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：

- 思科安全访问控制系统5.7 (ACS 5.7)
- 思科FireSight管理器中心5.4.1

以上版本是当前可用的最新版本。所有ACS 5.x版本和FMC 5.x版本均支持此功能。

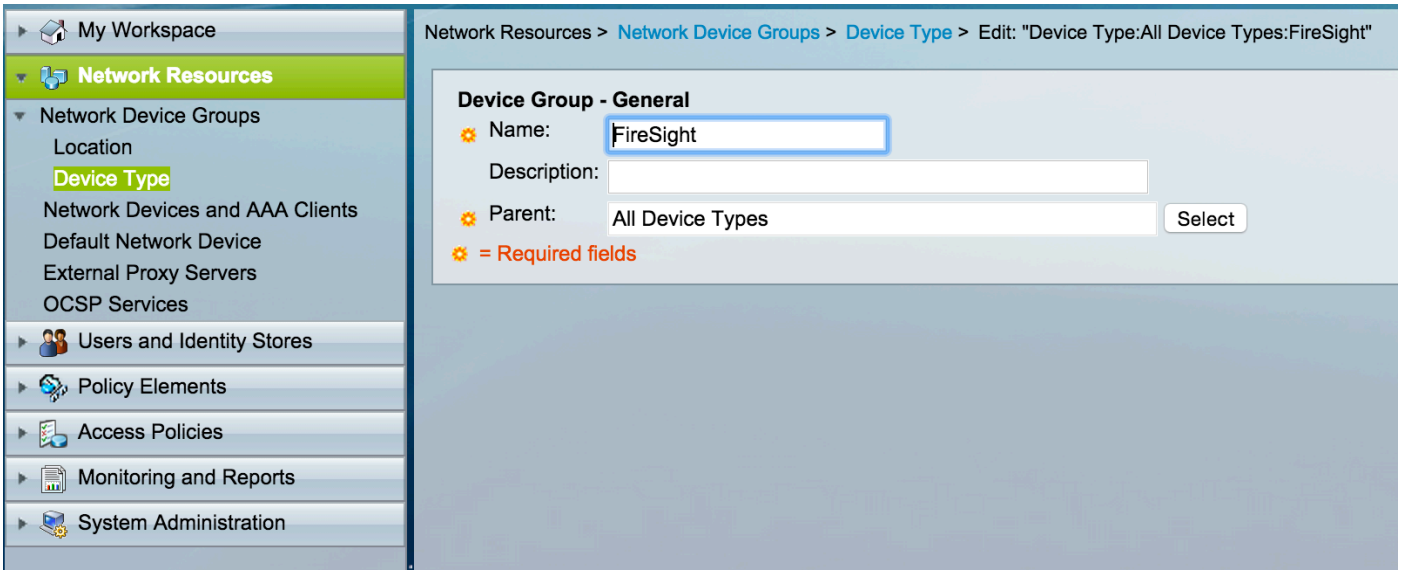
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

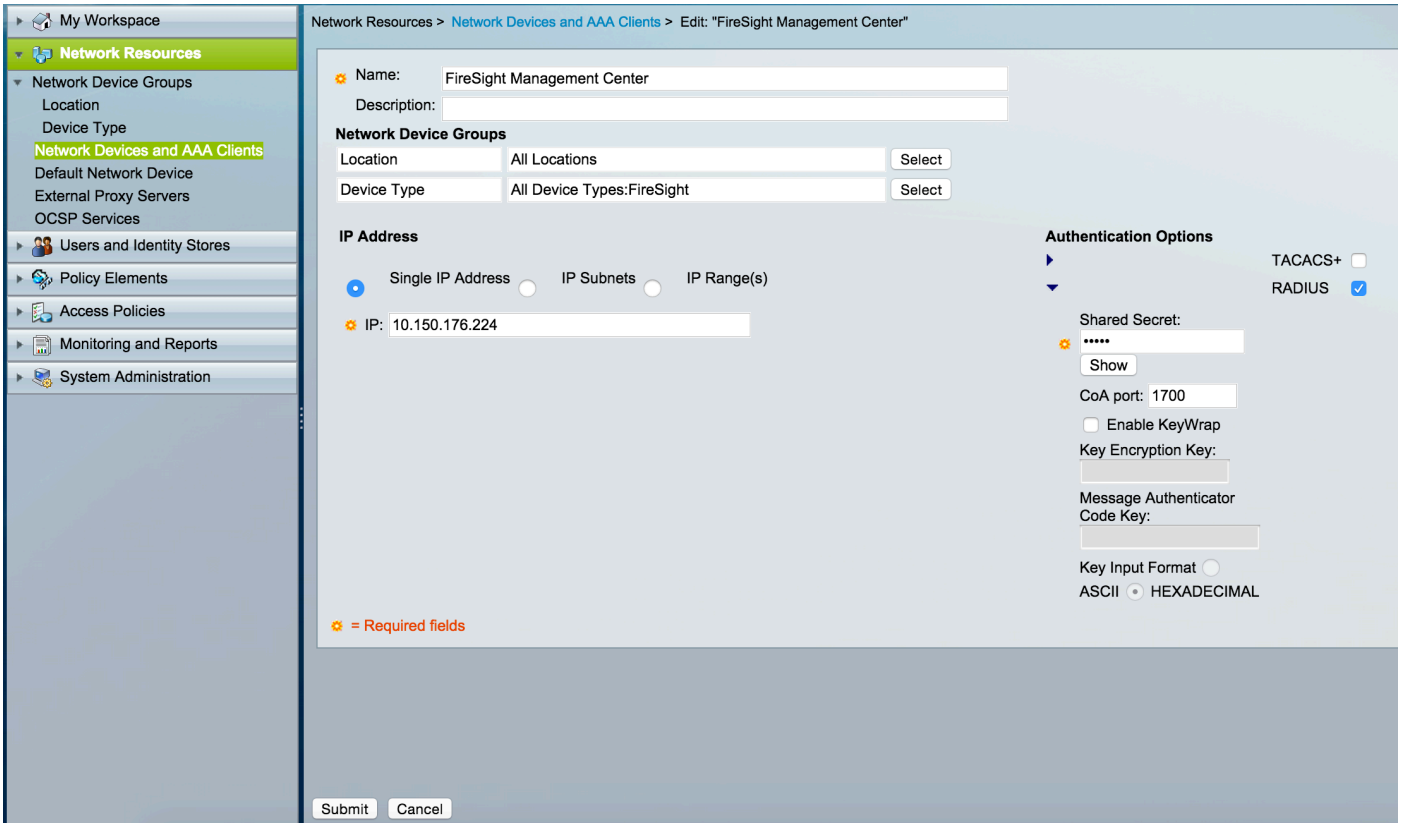
ACS 5.x配置

配置网络设备和网络设备组

- 从ACS GUI中，导航到网络设备组，单击设备类型并创建设备组。在下面的示例屏幕截图中，已配置设备类型FireSight。 此设备类型将在后续步骤的授权策略规则定义中引用。 Click Save.



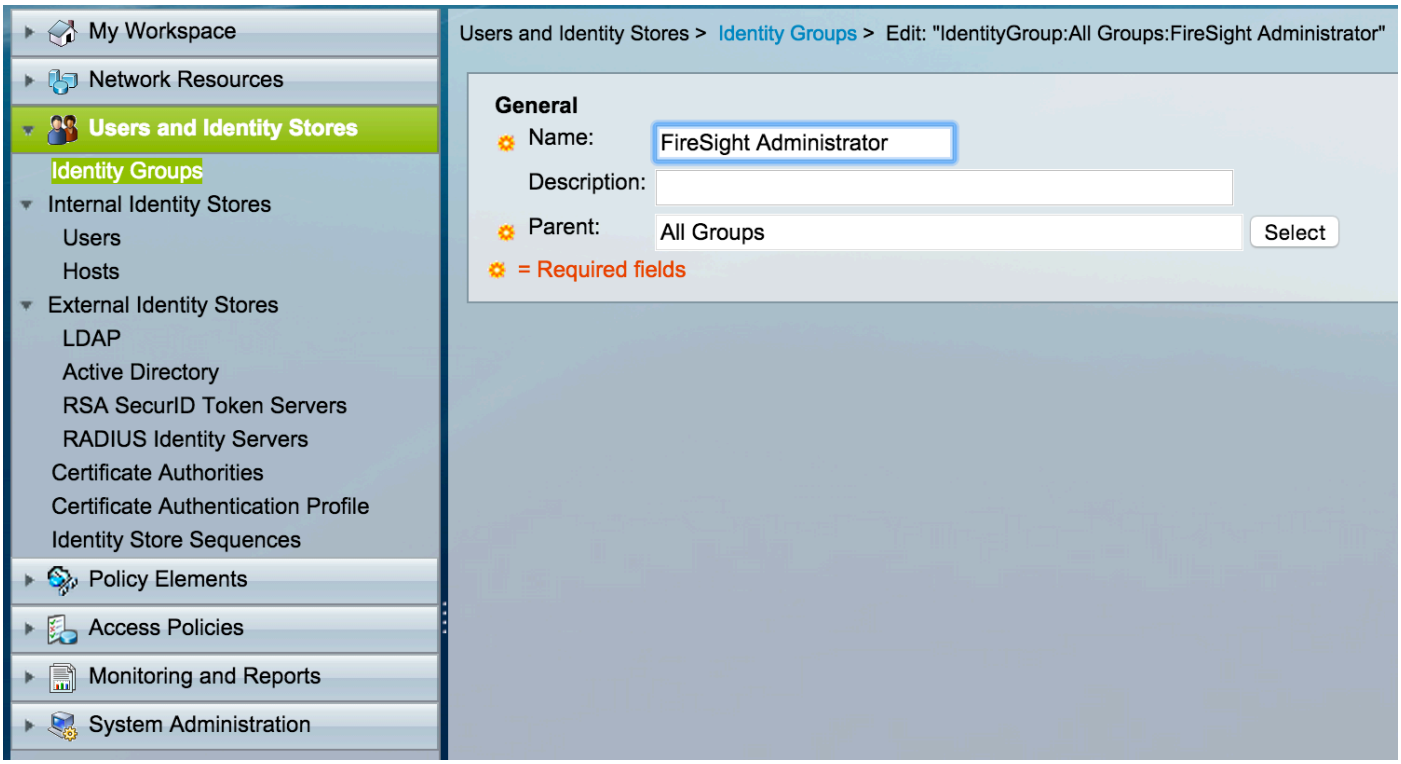
- 在ACS GUI中，导航至网络设备组，点击网络设备和AAA客户端，然后添加设备。 提供描述性名称和设备IP地址。 FireSIGHT管理中心在以下示例中进行定义。



- 在网络设备组中，配置与上一步中创建的设备组相同的设备类型。
- 选中Authentication Options旁边的框，选中RADIUS复选框，然后输入将用于此NAD的共享密钥。请注意，稍后在FireSIGHT管理中心上配置RADIUS服务器时，将再次使用相同的共享密钥。 要查看纯文本键值，请单击Show按钮。 单击“Submit”。
- 对需要RADIUS用户身份验证/授权以进行GUI和/或外壳访问的所有FireSIGHT管理中心和受管设备重复上述步骤。

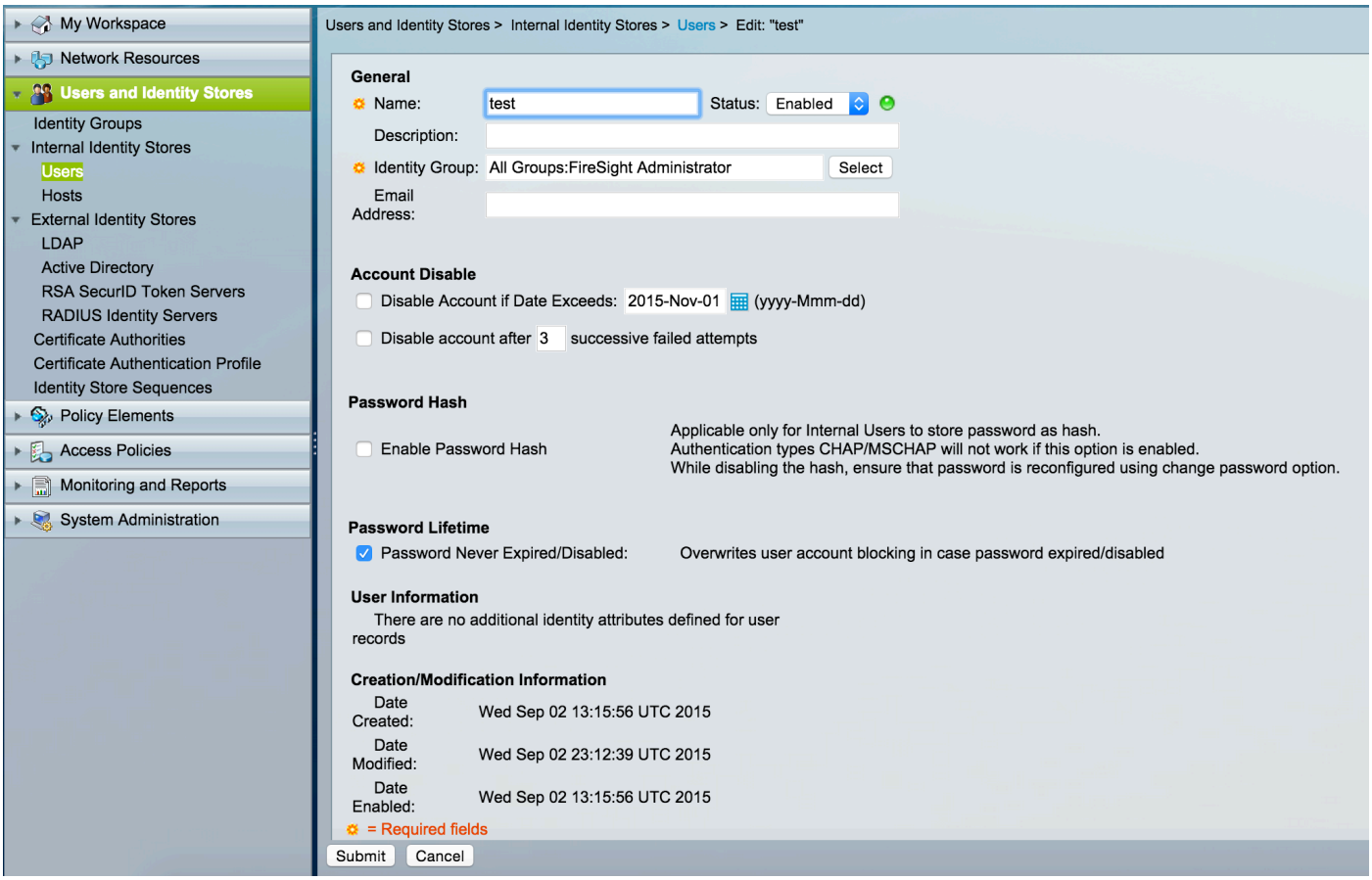
在ACS中添加身份组

- 导航到用户和身份库，配置身份组。 在本示例中，创建的身份组是“FireSight Administrator”。 此组将链接到以下步骤中定义的授权配置文件。



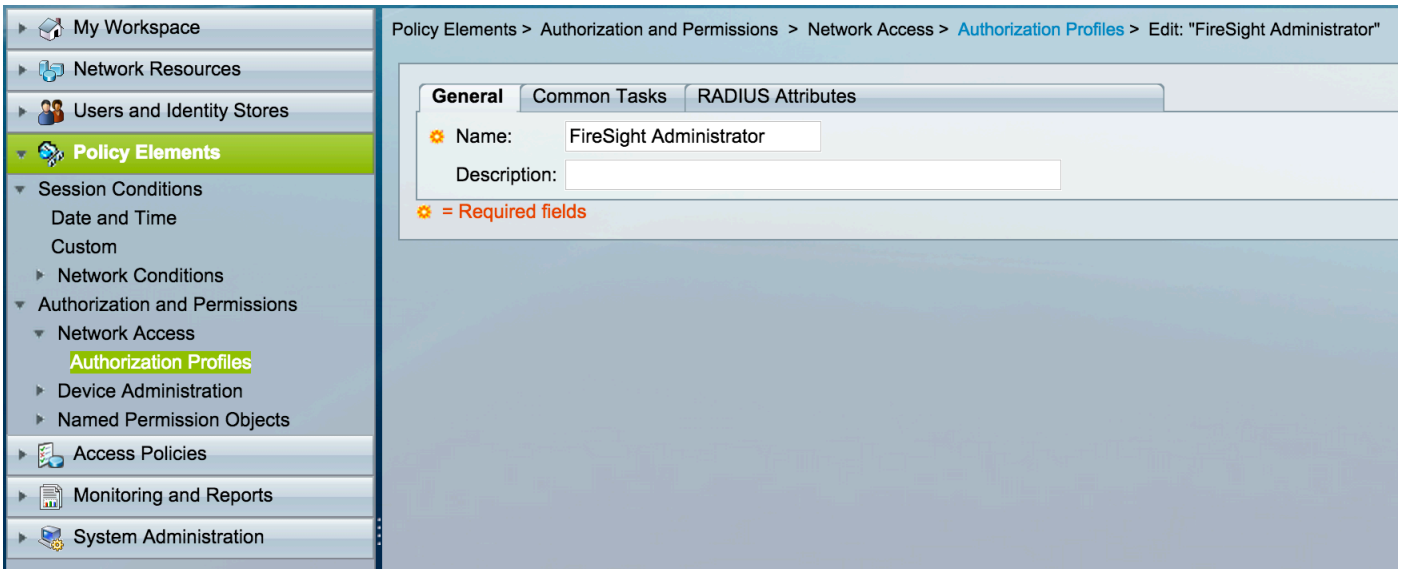
将本地用户添加到ACS

- 导航到用户和身份库，在内部身份库部分中配置用户。输入创建本地用户所需的信息，选择在上一步中创建的身份组，然后点击提交。

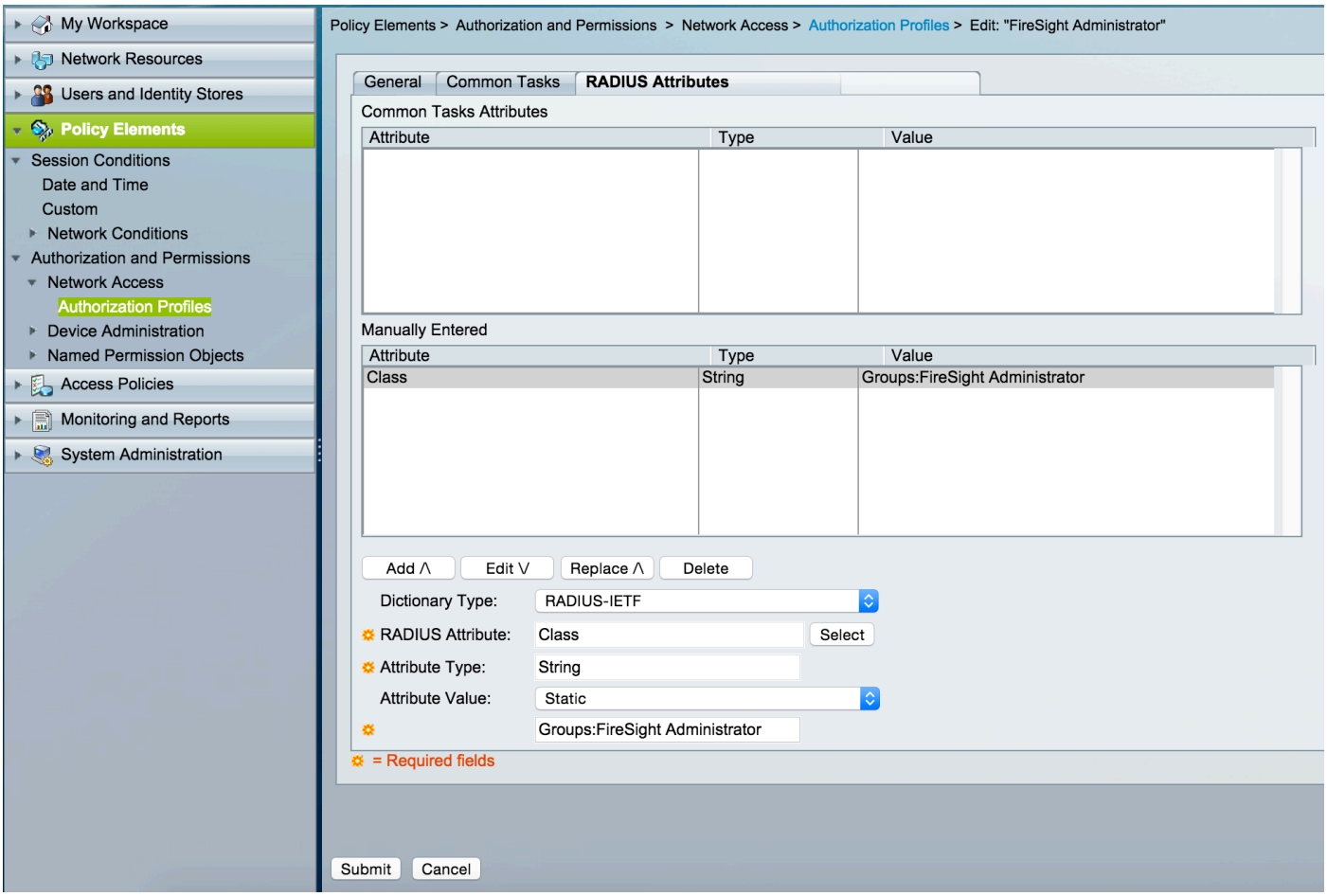


配置ACS策略

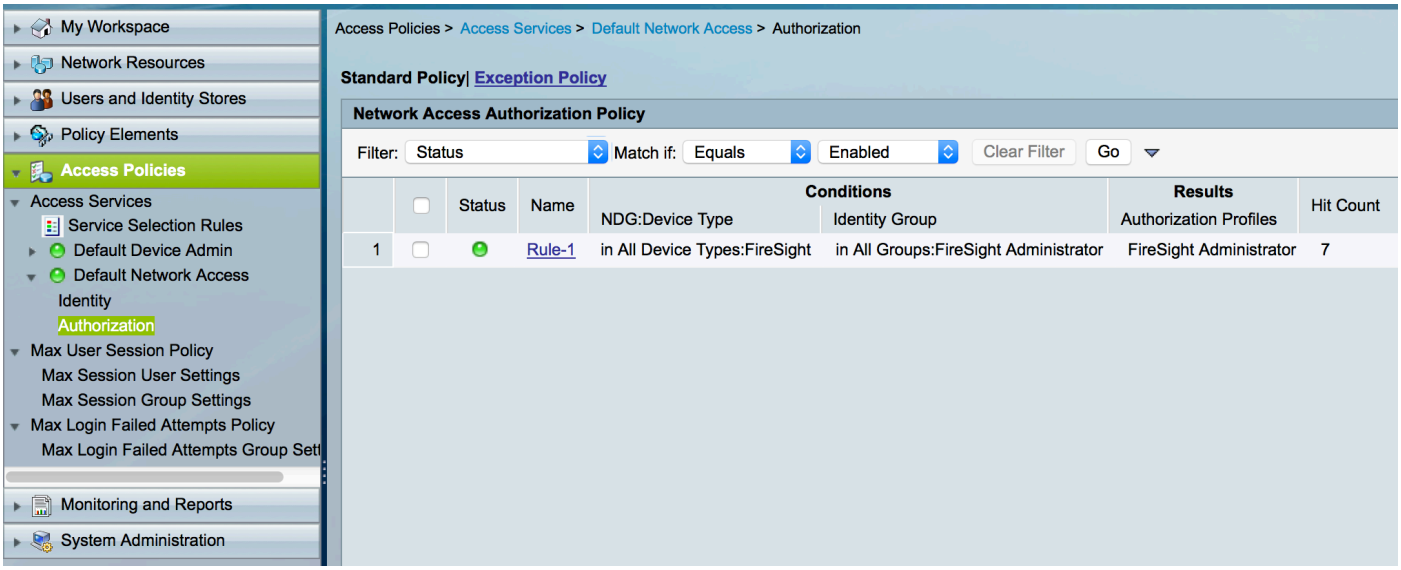
- 在ACS GUI中，导航到Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles。 使用描述性名称创建新的授权配置文件。在下面的示例中，创建的策略是FireSight管理员。



- 在RADIUS attributes选项卡中，添加用于为以上创建的身份组进行授权的手动属性，然后单击Submit



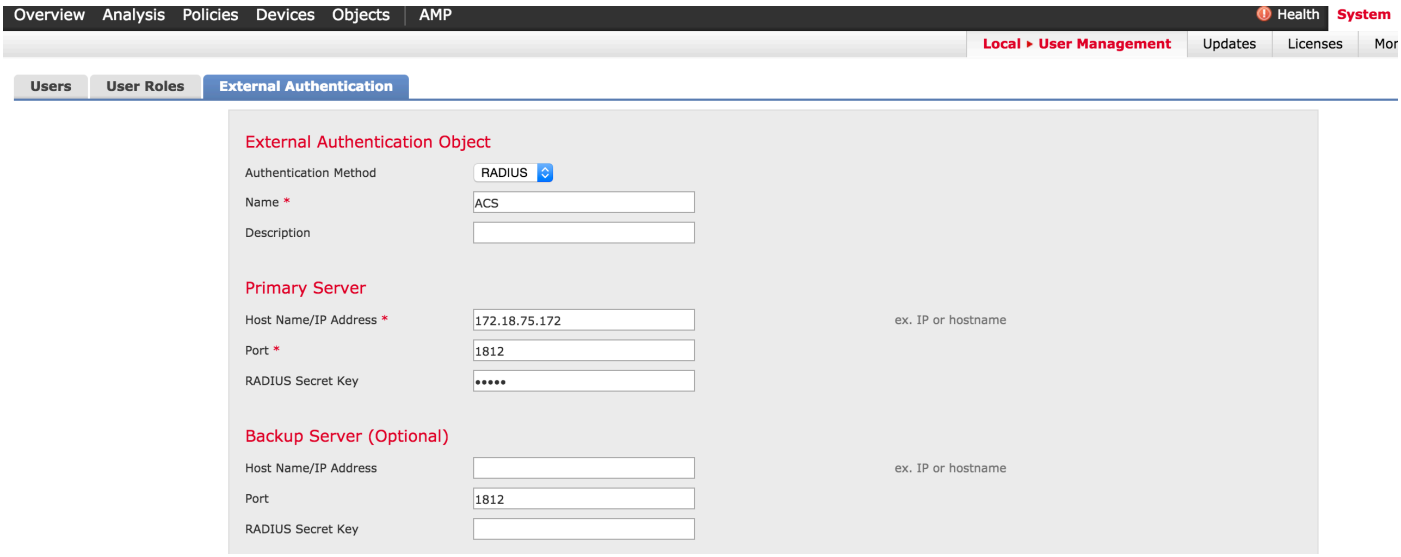
- 导航到访问策略>访问服务>默认网络访问>授权，然后为FireSight管理中心管理会话配置新的授权策略。 以下示例使用NDG：Device Type & Identity Group 条件匹配上一步中配置的设备类型和身份组。
- 此策略随后与上面配置的FireSight管理员授权配置文件关联作为结果。 单击“Submit”。



FireSight管理中心配置

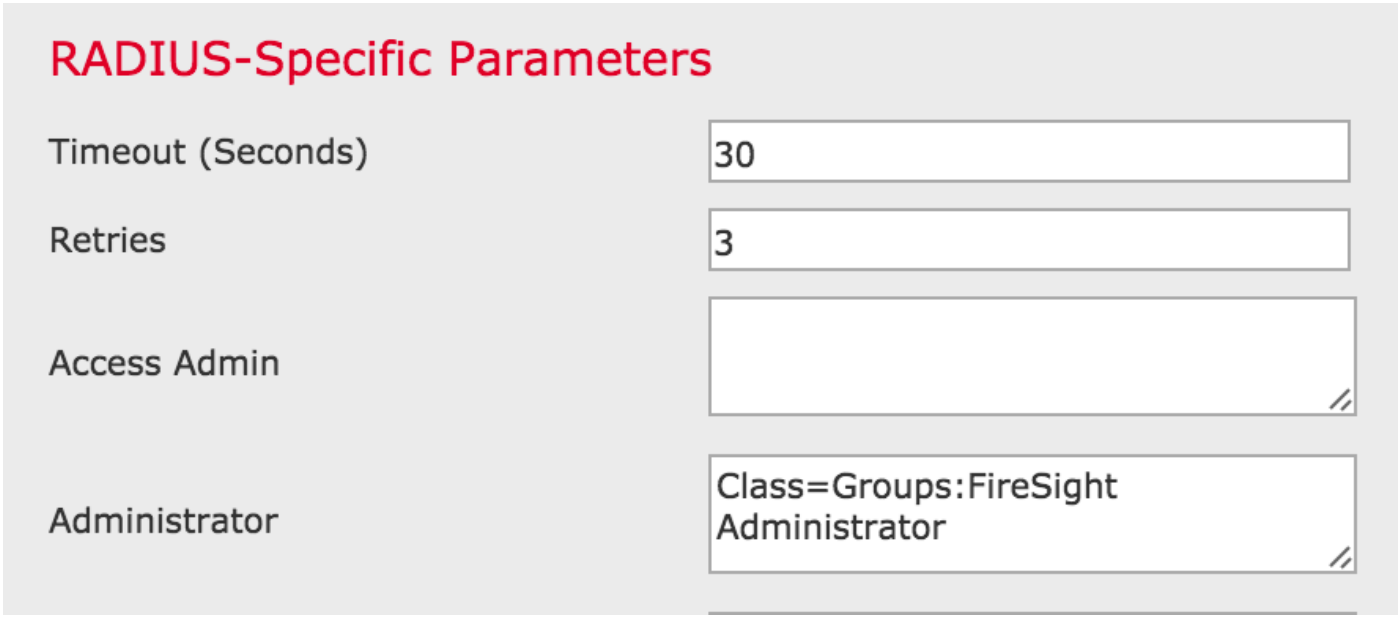
FireSight管理器系统策略配置

- 登录FireSIGHT MC并导航到System > Local > User Management。 点击外部身份验证选项卡。 单击+ Create Authentication Object按钮添加新的RADIUS服务器以进行用户身份验证/授权。
- 为Authentication Method选择RADIUS。 输入RADIUS服务器的描述性名称。 输入Host Name/IP Address和RADIUS Secret Key。 密钥应与以前在ACS上配置的密钥相匹配。也可以输入备份ACS服务器主机名/IP地址（如果存在）。

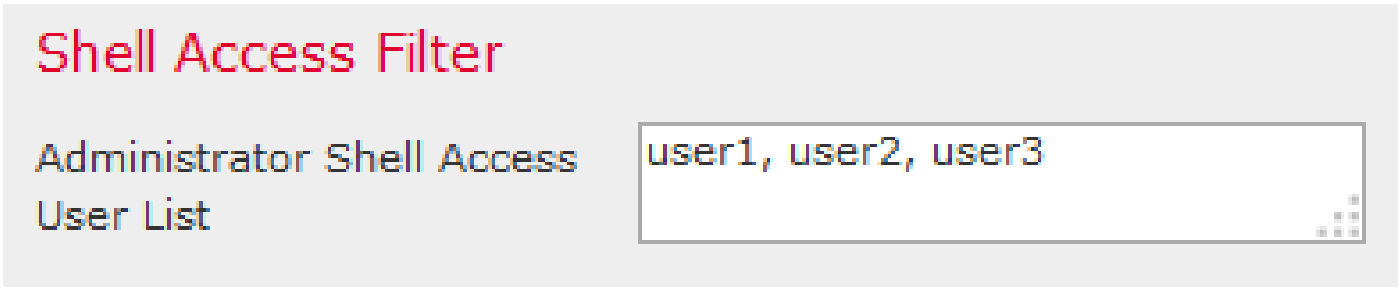


- 在本示例中，在RADIUS-Specific Parameters部分下，Class=Groups：FireSight Administrator值将映射到FireSight管理员组。 这是ACS作为ACCESS-ACCEPT的一部分返回

的值。单击Save保存配置，或者前进到下面的“验证”部分以测试通过ACS的身份验证。



- 在Shell Access Filter下，输入以逗号分隔的用户列表以限制Shell/SSH会话。



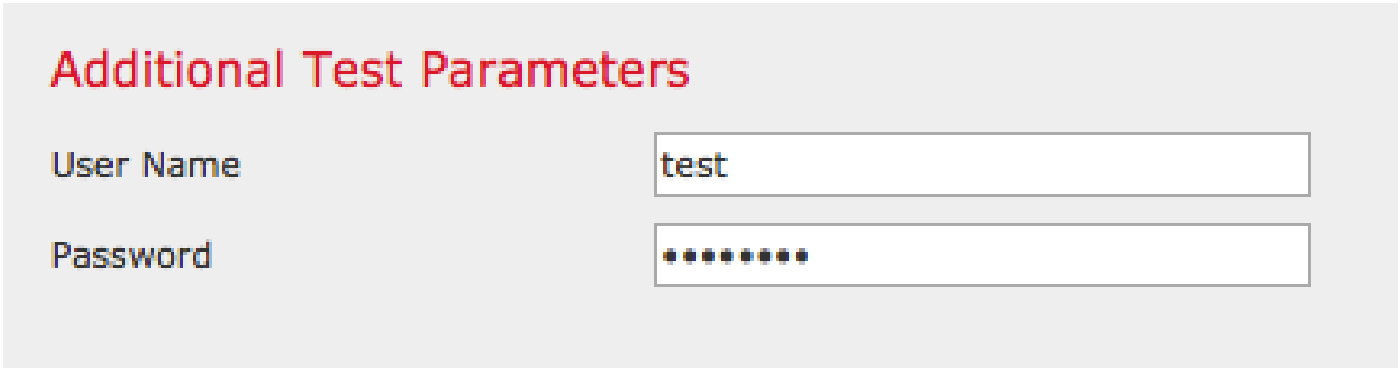
启用外部身份验证

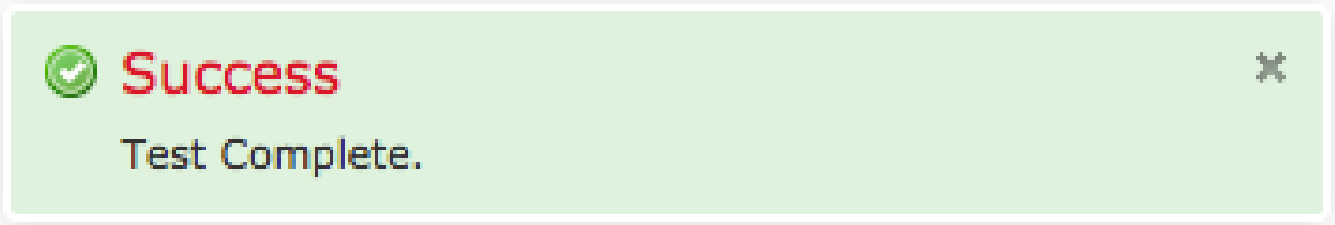
最后，完成以下步骤以便在FMC上启用外部身份验证：

1. 导航到System > Local > System Policy。
2. 在左窗格中选择External Authentication。
3. 将Status更改为Enabled（默认为禁用）。
4. 启用添加的ACS RADIUS服务器。
5. 保存策略并在设备上重新应用策略。

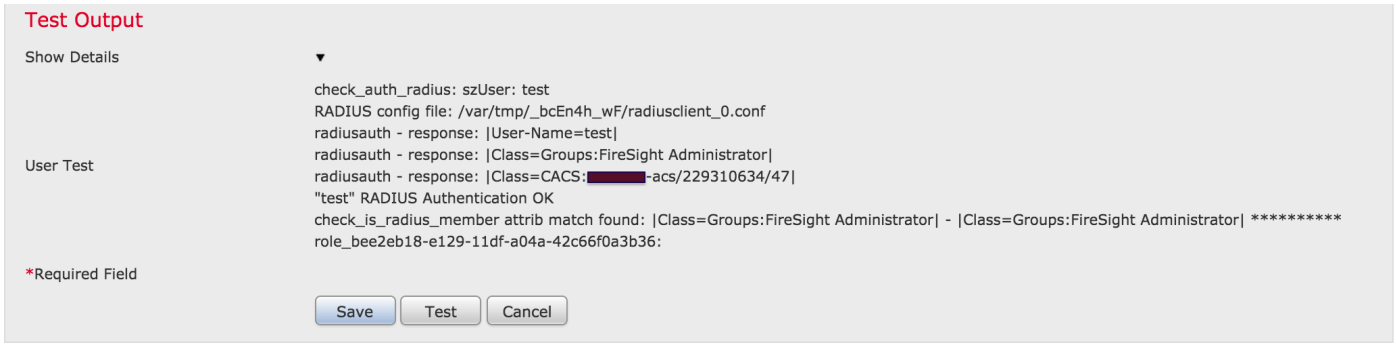
确认

- 要针对ACS测试用户身份验证，请向下滚动到Additional Test Parameters 部分，并输入ACS用户的用户名和口令。 单击测试。 成功测试将导致浏览器窗口顶部显示green Success： Test Complete消息。





- 要查看测试身份验证的结果，请转到测试输出部分，然后单击显示详细信息旁边的黑色箭头。 在下面的示例屏幕截图中，请注意“radiusauth - response： 从ACS接收的 |Class=Groups：FireSight Administrator|”值。这应该与上面在FireSIGHT MC上配置的本地FireSight组相关联的Class值匹配。 Click 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）。

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）。