FireSIGHT系统与ISE集成，用于RADIUS用户身份验证

目录

简介

本文档介绍将Cisco FireSIGHT管理中心(FMC)或Firepower受管设备与思科身份服务引擎(ISE)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：

- 思科ASA v9.2.1
- ASA FirePOWER模块v5.3.1
- ISE 1.2

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

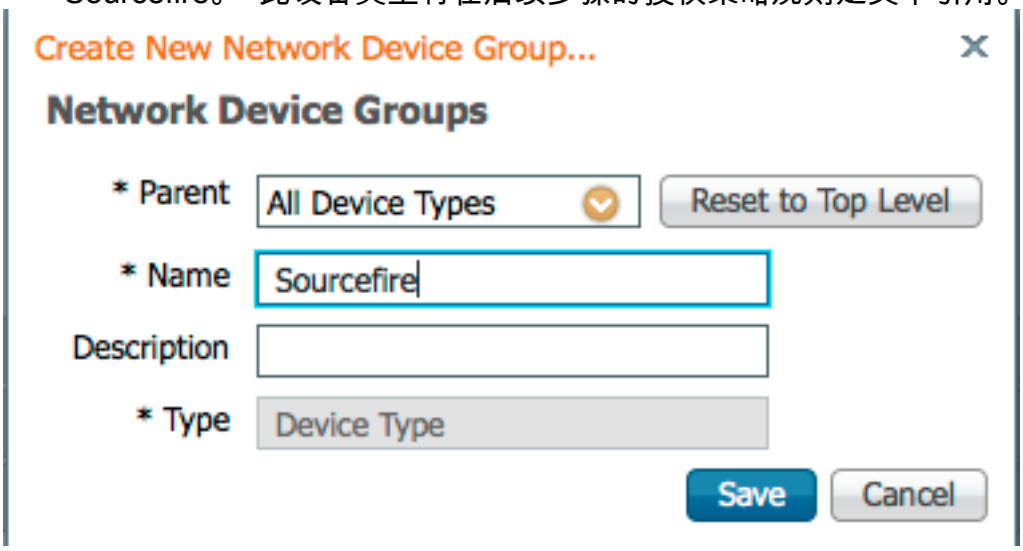
ISE配置

> **提示**：有多种方法可配置ISE身份验证和授权策略，以支持与网络接入设备(NAD)（如Sourcefire）的集成。 以下示例是配置集成的一种方法。 示例配置是参考点，可适应特定部署的需求。 请注意，授权配置是两步过程。 在ISE上定义一个或多个授权策略，ISE将RADIUS属性值对(av-pair)返回到FMC或受管设备。 然后，这些av-pairs会映射到在FMC系统策略配置中定义的本地用户组。

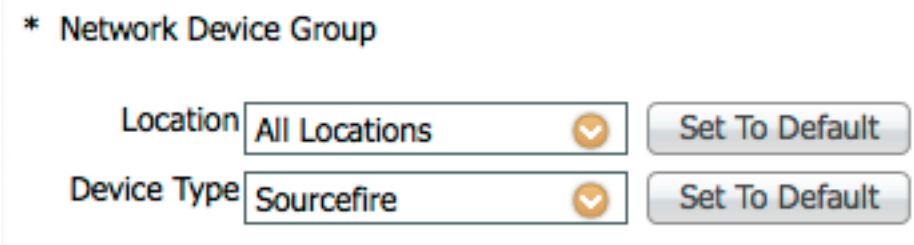
配置网络设备和网络设备组

- 从ISE GUI中，导航至**Administration > Network Resources > Network Devices**。 单击**+**添加以添加新的网络接入设备(NAD)。 提供描述性名称和设备IP地址。 FMC在以下示例中定义。

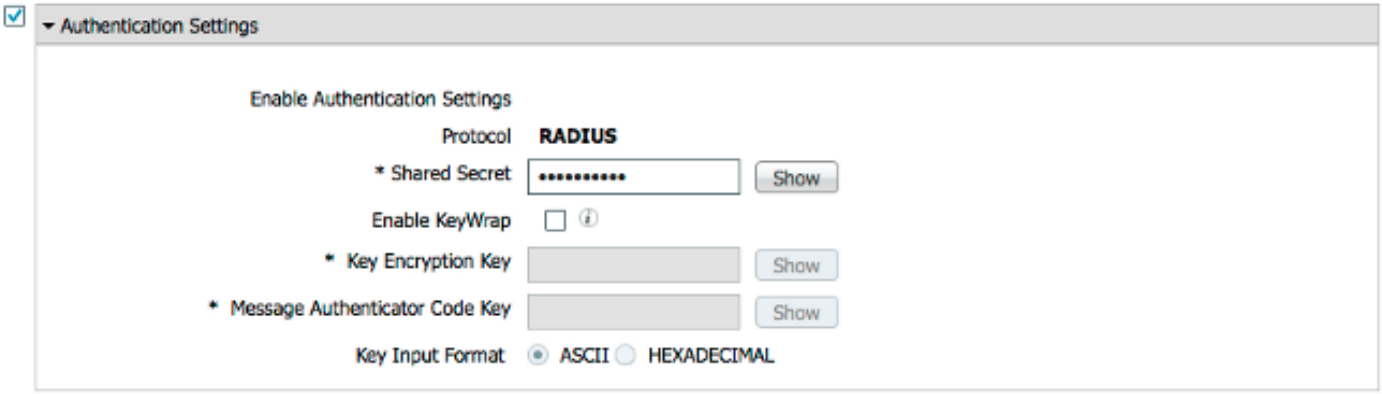
- 在**Network Device Group**下，单击**All Device Types旁的橙色箭头。** 单击图标  ，然后选择**Create New Network Device Group**。 在下面的示例屏幕截图中，配置了Device Type Sourcefire。 此设备类型将在后续步骤的授权策略规则定义中引用。 Click **Save**.



- 再次单击**橙色箭**头，并选择上面步骤中配置的网络设备组



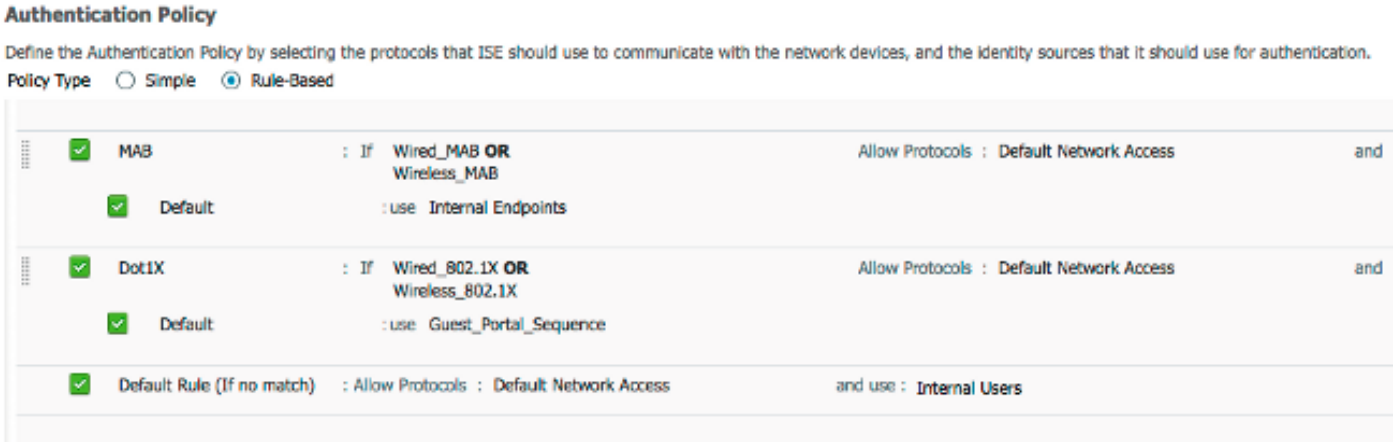
- 选中Authentication Settings旁**的框**。 输入将用于此NAD的RADIUS共享密钥。 请注意，稍后在FireSIGHT MC上配置RADIUS服务器时，将再次使用相同的共享密钥。 要查看纯文本键值，请单击“显**示**”按钮。 Click **Save**.



- 对于需要RADIUS用户身份验证/授权以进行GUI和/或外壳访问的所有FireSIGHT MC和受管设备，重复上述步骤。

配置ISE身份验证策略：

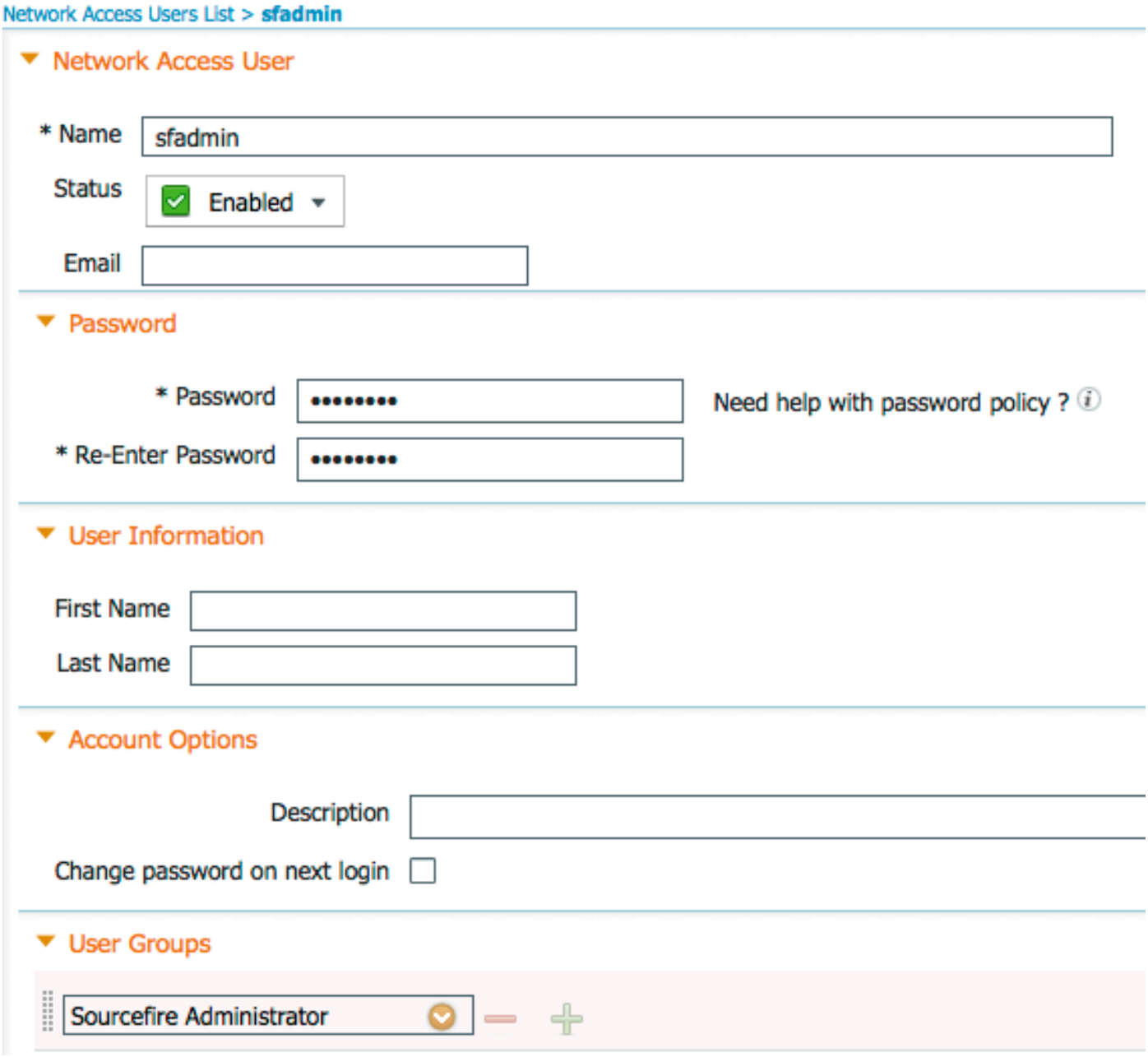
- 从ISE GUI导航到Policy > **Authentication**。 如果使用策略集，请导航至**策略>策略集**。 以下示例取自使用默认身份验证和授权策略接口的ISE部署。 无论采用何种配置方法，身份验证和授权规则逻辑都是相同的。
- **默认规则（如果不匹配）**将用于验证来自NAD的RADIUS请求，其中使用的方法不是MAC身份验证绕行(MAB)或802.1X。 如默认配置，此规则将在ISE的本地内部用户身份源中**查找用**户帐户。 可以修改此配置以引用外部身份源，如Active Directory、LDAP等，如在“管理”>“身份管理”>“外部身份源”**下定义**。 为简单起见，此示例将在ISE本地定义用户帐户，因此无需对身份验证策略进行进一步修改。



将本地用户添加到ISE

- 导航至**管理>身份管理>身份>用户**。 单击 **Add**。 输入有意义的用户名和密码。在“用**户组**”选项

下，选择现有组名称或单击绿色+符号添加新组。 在本例中，用户“sfadmin”被分配给自定义组“Sourcefire管理员”。 此用户组将链接到下面“配置ISE授权策略”步骤中**定义的授权配**置文件。 Click **Save**.

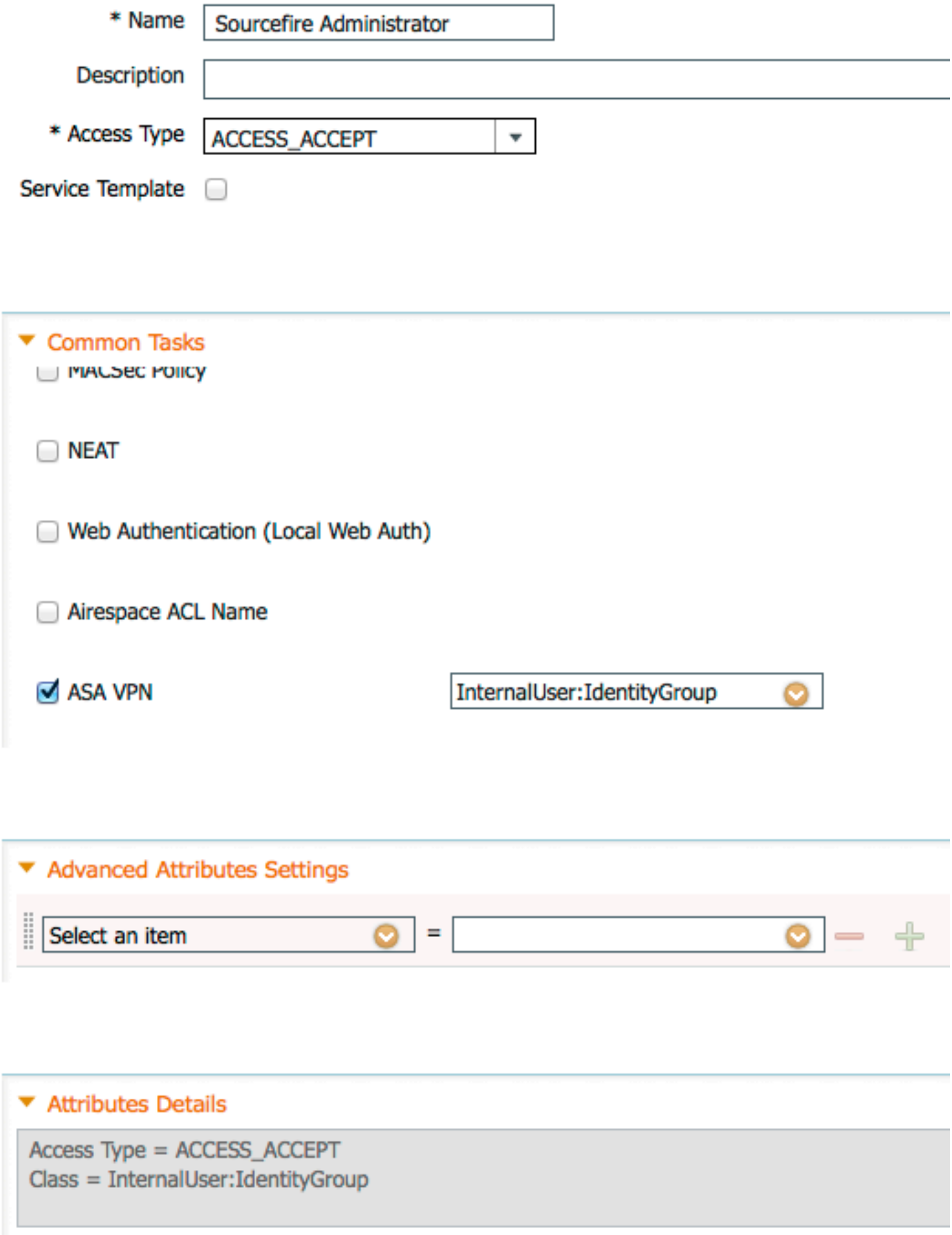


配置ISE授权策略

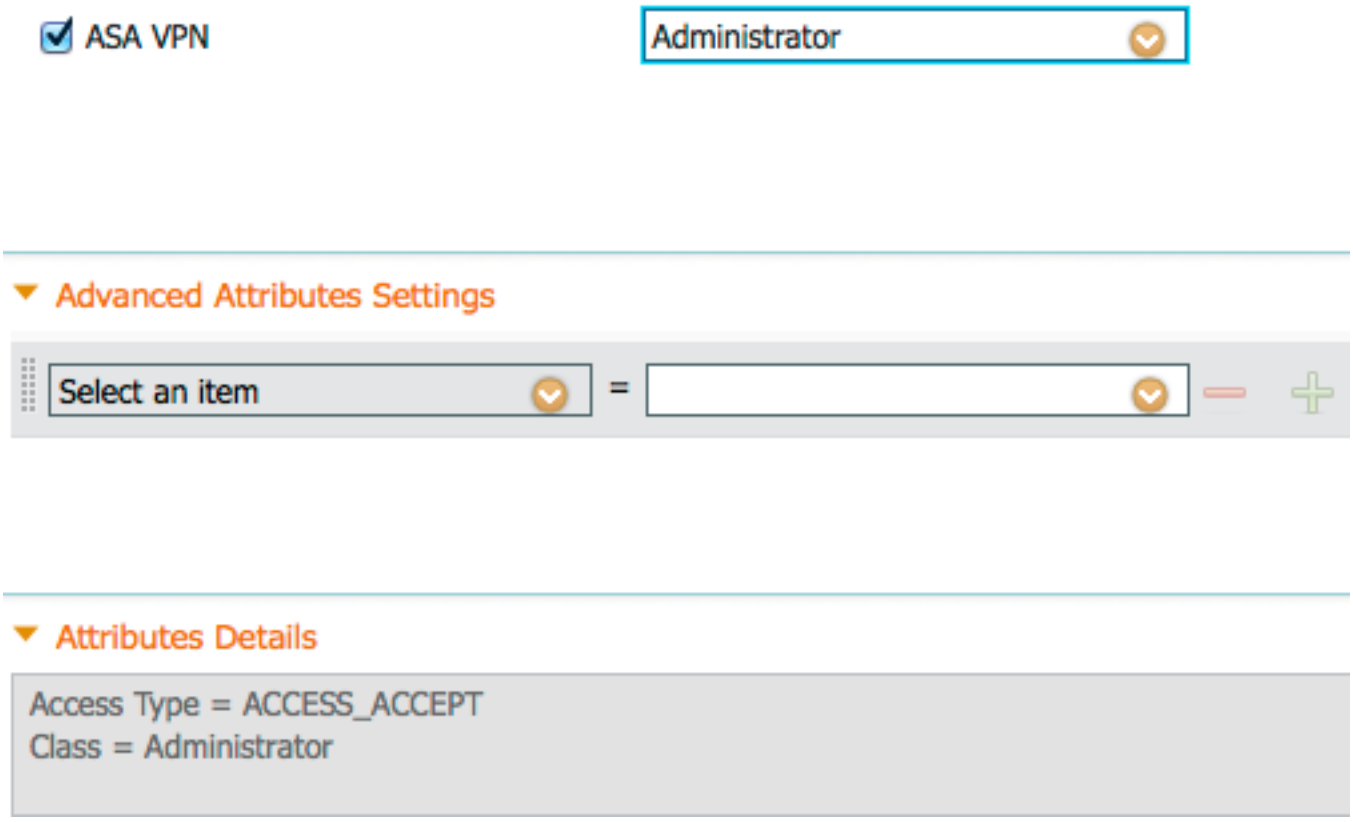
- 导航至**策略>Policy元素>结果>授权>授权配置文件**。 单击绿色+号添加新的授权配置文件。
- 提供描述性名称，如Sourcefire Administrator。 为“访**问类型”**(Access Type)选**择“ACCESS_ACCEPT”**。 在**Common Tasks**下，滚动到底部并选中**ASA VPN**旁边的**复选框。** 单击橙色**箭头，**然后选**择InternalUser:IdentityGroup**。 Click **Save**.

提示：由于此示例使用ISE本地用户身份库，因此InternalUser:IdentityGroup组选项用于简化配置。 如果使用外部身份库，则仍使用ASA VPN授权属性，但是，要返回给Sourcefire设备的值是手动配置的。 例如，在ASA VPN下拉框中手动键入Administrator将导致Class = Administrator的Class-25 av-pair值被发送到Sourcefire设备。 然后，此值可以映射到作为系统策略配置一部分的sourcefire用户组。 对于内部用户，任一配置方法都可接受。

内部用户示例


* Name
Sourcefire Administrator
Description
* Access Type
ACCESS_ACCEPT
Service Template
Common Tasks
NEAT
Web Authentication (Local Web Auth)
Airespace ACL Name
ASA VPN
InternalUser:IdentityGroup
Advanced Attributes Settings
Select an item
=
Attributes Details
Access Type = ACCESS_ACCEPT
Class = InternalUser:IdentityGroup

外部用户示例

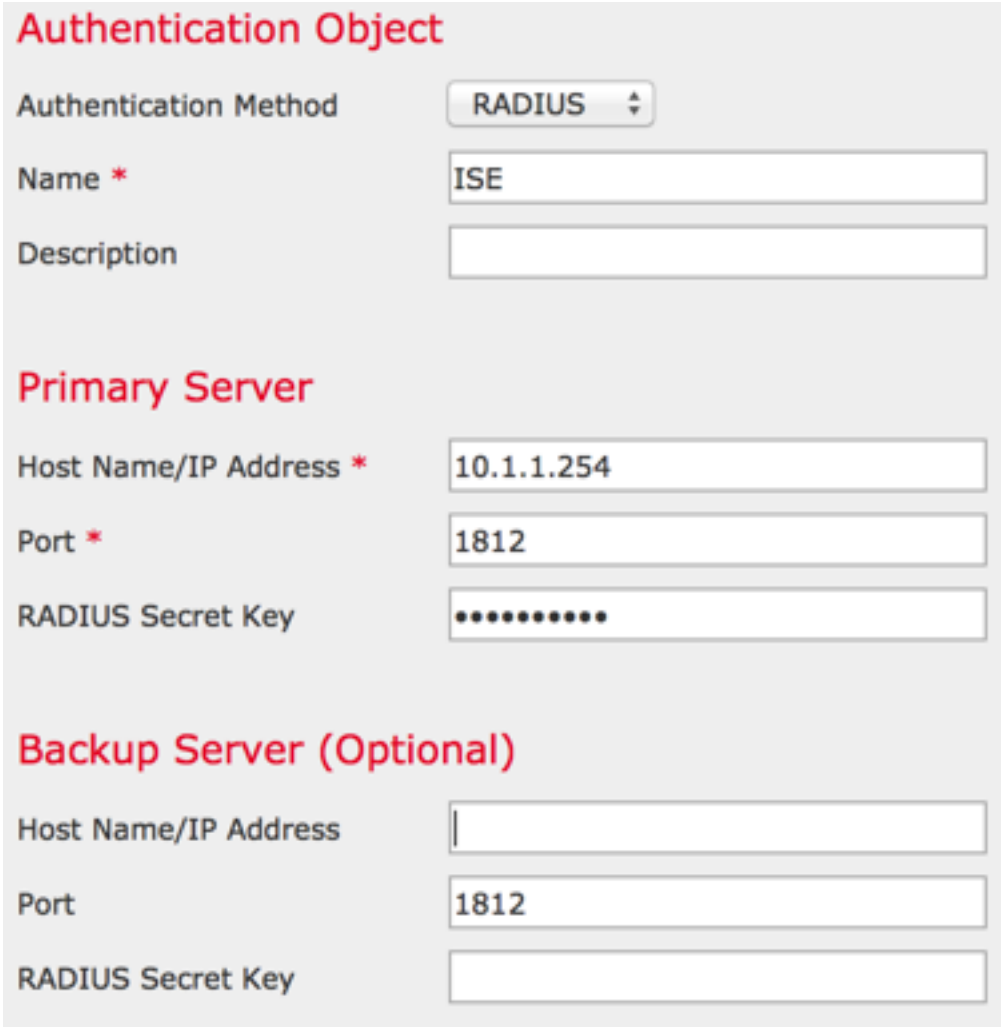


- 导航至**Policy > Authorization**并为Sourcefire管理会话配置新的授权策略。 以下示例使用**DEVICE:Device Type条**件与中配置的设备类型匹配 **上面的"配置网络设备和网络设**备组"部分。 然后，此策略与上面配置的Sourcefire管理员授权配置文件关联。 Click **Save**.

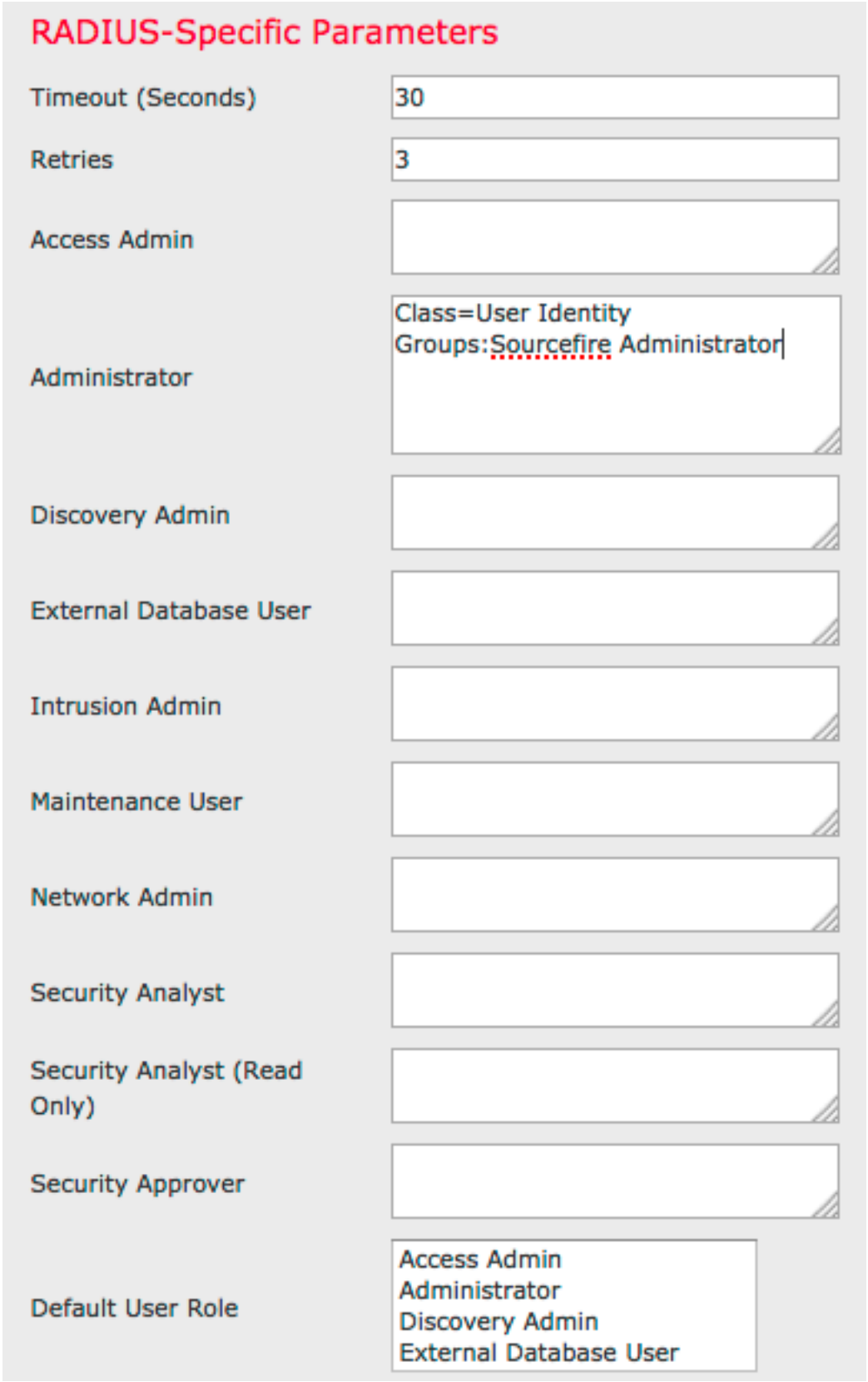
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
✓	Sourcefire Administrator	if	DEVICE:Device Type EQUALS All Device Types#Sourcefire	then	Sourcefire Administrator
✓	CWA-PSN1	if	Network Access:ISE Host Name EQUALS ise12-psn1	then	CWA-PSN1
✓	CWA-PSN2	if	Network Access:ISE Host Name EQUALS ise12-psn2	then	CWA-PSN2

Sourcefire系统策略配置

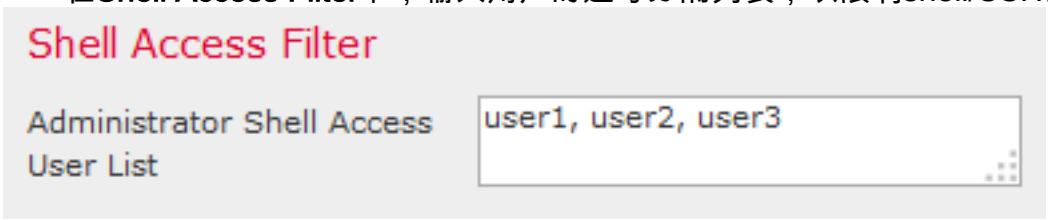
- 登录FireSIGHT MC并导航至System > Local > **User Management**。 单击"Login Authentication(登**录身份验证)**"选项卡。 单击+ Create Authentication Object(**创建身份验**证对象)按钮，为用户身份验证/授权添加新的RADIUS服务器。
- 选择**RADIUS**作为身**份验证方法**。 输入RADIUS服务器的描述性名称。 输入**主机名/IP地址**和**RADIUS密钥**。 密钥应与之前在ISE上配置的密钥匹配。 或者，如果存在备份ISE服**务器主机名/IP**地址，请输入。



- 在**RADIUS特定参数**部分下，在要匹配GUI访问的Sourcefire本地组名称旁的文本框中输入Class-25 av-pair字符串。 在本示例中，Class=User Identity Groups:Sourcefire Administrator值映射到Sourcefire Administrator组。 这是ISE返回的值，作为ACCESS-ACCEPT的一部分。 或者，为未分**配Class-25**组的已验证用户选择默认用户角色。 单击**Save**保存配置，或进入下面的Verify部分以测试ISE的身份验证。



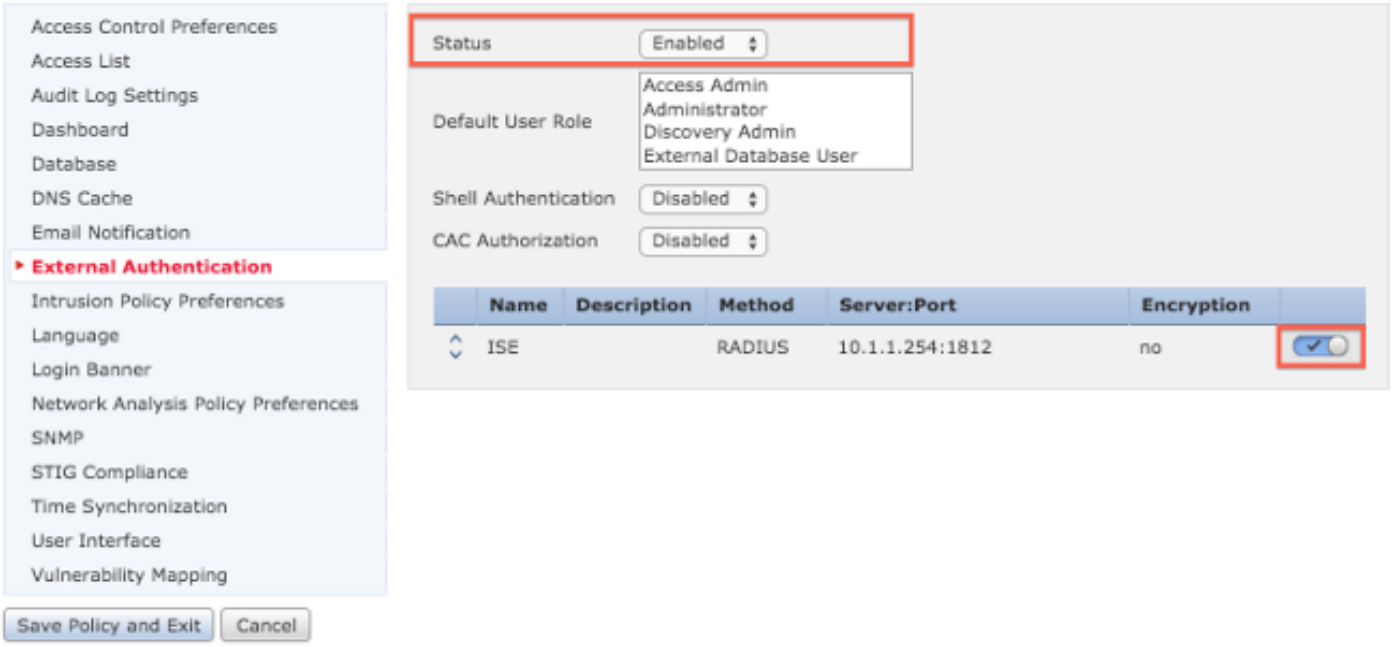
- 在**Shell Access Filter**下，输入用户的逗号分隔列表，以限制shell/SSH会话。



启用外部身份验证

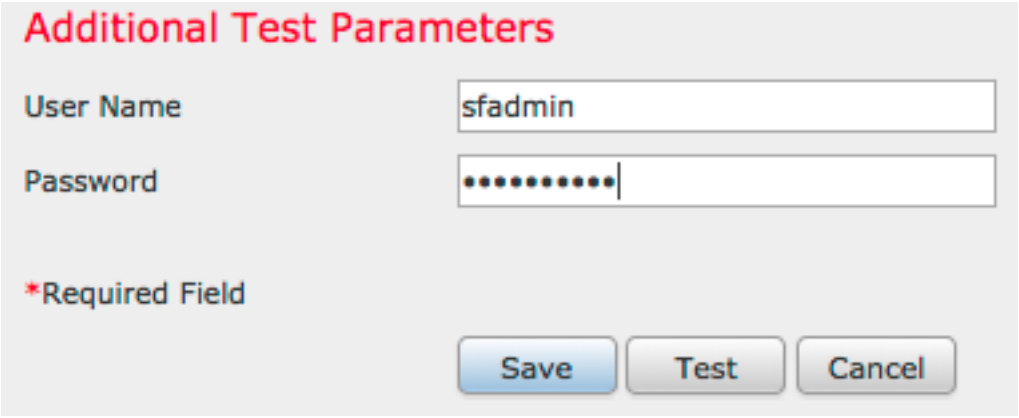
最后，完成以下步骤以在FMC上启用外部身份验证：

1. 导航至 **system > 本地 > 系统策略**。
2. 选择 **外部身份验证** 在左侧面板上。
3. 将状态*更改*为 **启用** （默认禁用）。
4. 启用已添加的ISE RADIUS服务器。
5. 保存策略并在设备上重新应用策略。



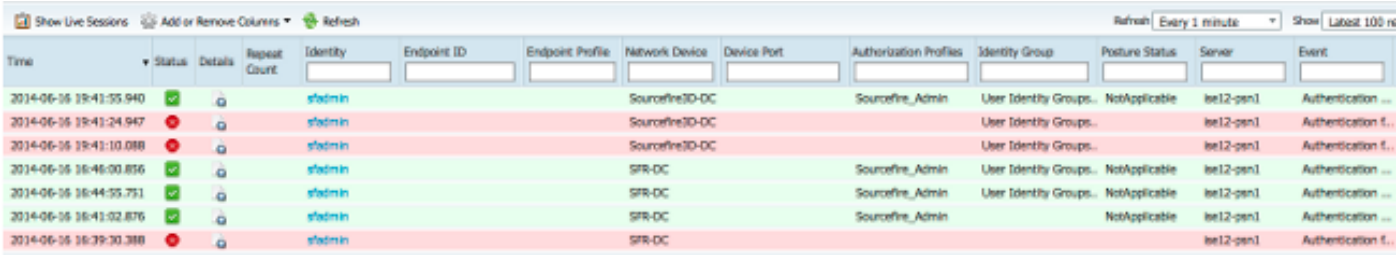
验证

- 要针对ISE测试用户身份验证，请向下滚动到**Additional Test Parameters**部分，并输入ISE用户的用户名和密码。 单击测试。 成功测试将导致绿色成功： 在浏览器窗口顶部测试完成消息。



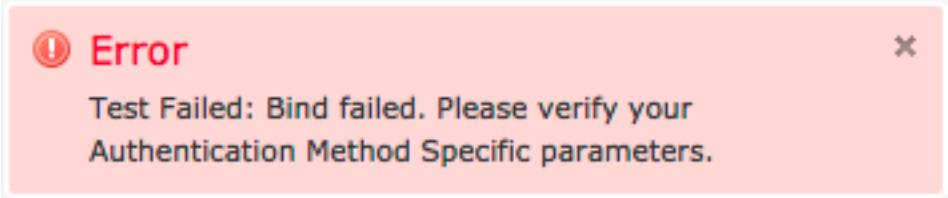
- 要查看测试身份验证的结果，请转至“测试输出”**部分，**然后单击“显示详**细信**息”旁边的**黑色箭头**。 在下面的示例屏幕截图中，请注意“radiusauth - response: |Class=User Identity Groups:Sourcefire Administrator|"值从ISE接收。 这应与与上述FireSIGHT MC上配置的本地Sourcefire组关联的类值匹配。 Click **Save**.

- 从ISE Admin GUI中，导航至**Operations > Authentications**以验证用户身份验证测试的成功或失败。

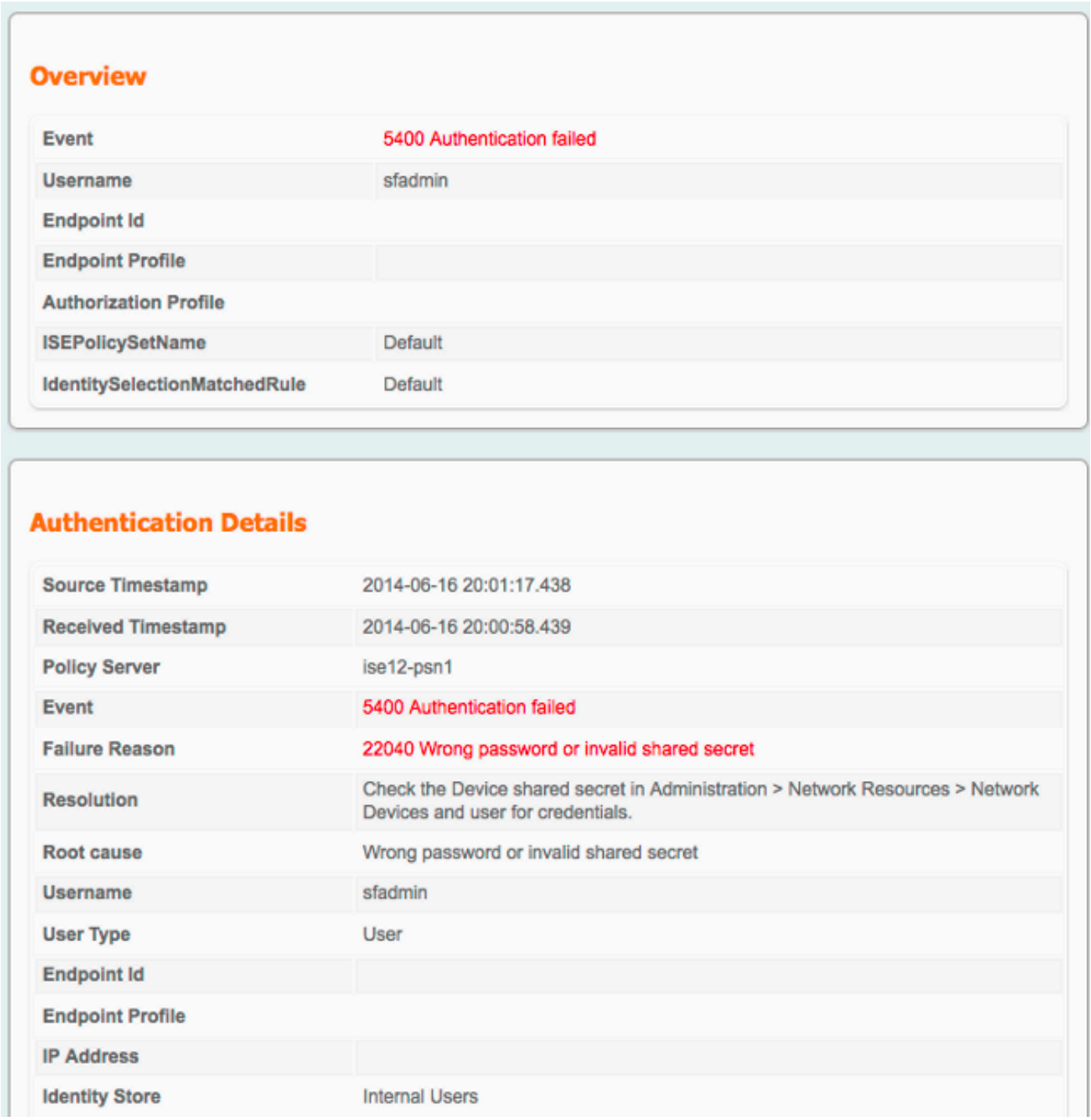


故障排除

- 当根据ISE测试用户身份验证时，以下错误表示RADIUS密钥不匹配或用户名/密码不正确。



- 从ISE管理GUI，导航至**Operations > Authentications**。 红色事件表示失败，而绿色事件表示成功的身份验证/授权/授权更改。 单击图标  查看身份验证事件的详细信息。



Overview

Event	5400 Authentication failed
Username	sfadmin
Endpoint Id	
Endpoint Profile	
Authorization Profile	
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-06-16 20:01:17.438
Received Timestamp	2014-06-16 20:00:58.439
Policy Server	ise12-psn1
Event	5400 Authentication failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	sfadmin
User Type	User
Endpoint Id	
Endpoint Profile	
IP Address	
Identity Store	Internal Users

相关信息

[技术支持和文档 - Cisco Systems]