将ISE配置为RADIUS服务器的SWA外部身份验证

目录

简介

本文档介绍在Cisco ISE作为RADIUS服务器的安全Web访问(SWA)上配置外部身份验证的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全网络设备的基础知识。
- 了解ISE上的身份验证和授权策略配置。
- RADIUS基础知识。

Cisco建议您还应具备：

- SWA和ISE管理访问权限。
- 兼容的WSA和ISE版本。

使用的组件

本文档中的信息基于以下软件版本：

- SWA 14.0.2-012
- ISE 3.0.0

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SWA的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配置中指定的轻型目录访问协议(LDAP)或RADIUS服务器验证用户凭证。

网络拓扑

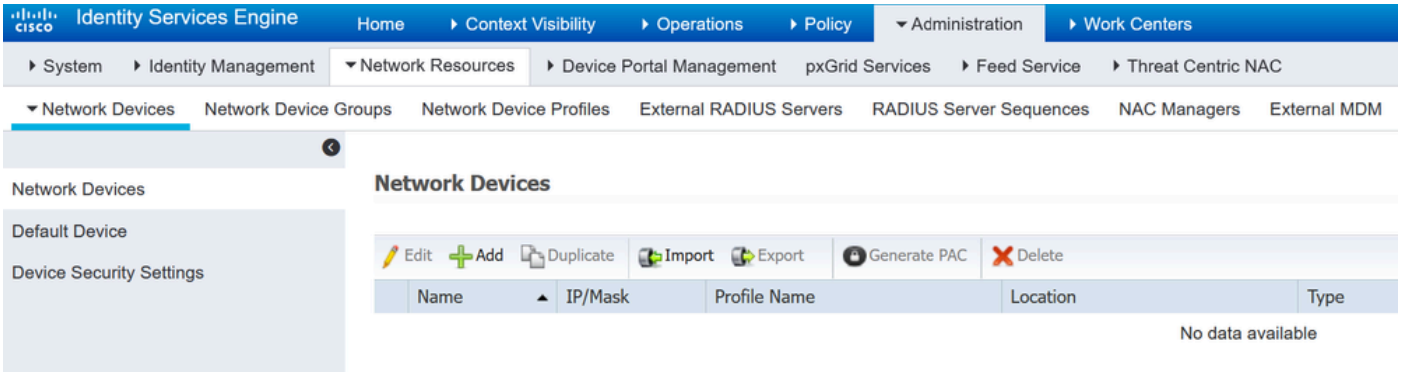
网络拓扑图

管理用户使用其凭证访问端口443上的SWA。SWA使用RADIUS服务器验证凭证。

配置

ISE 配置

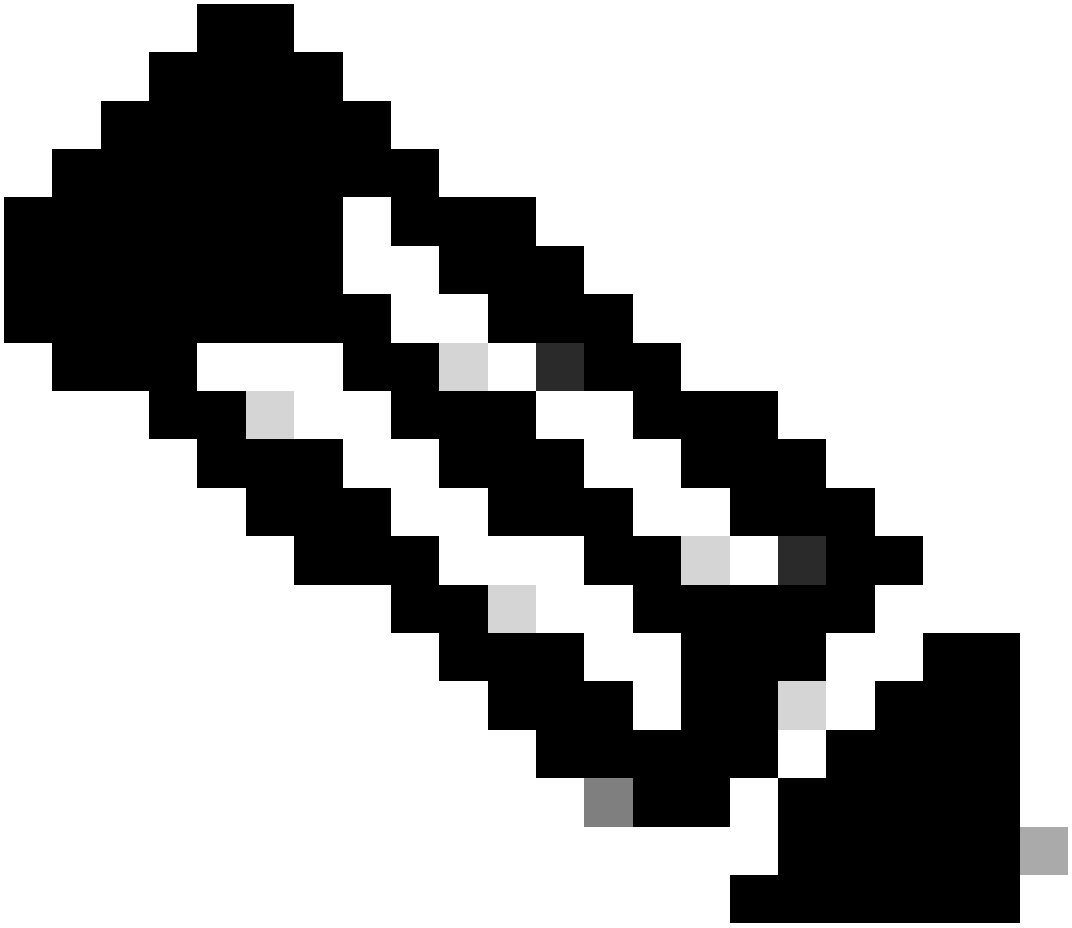
步骤1: 添加新的网络设备。导航到管理>网络资源>网络设备> +Add。



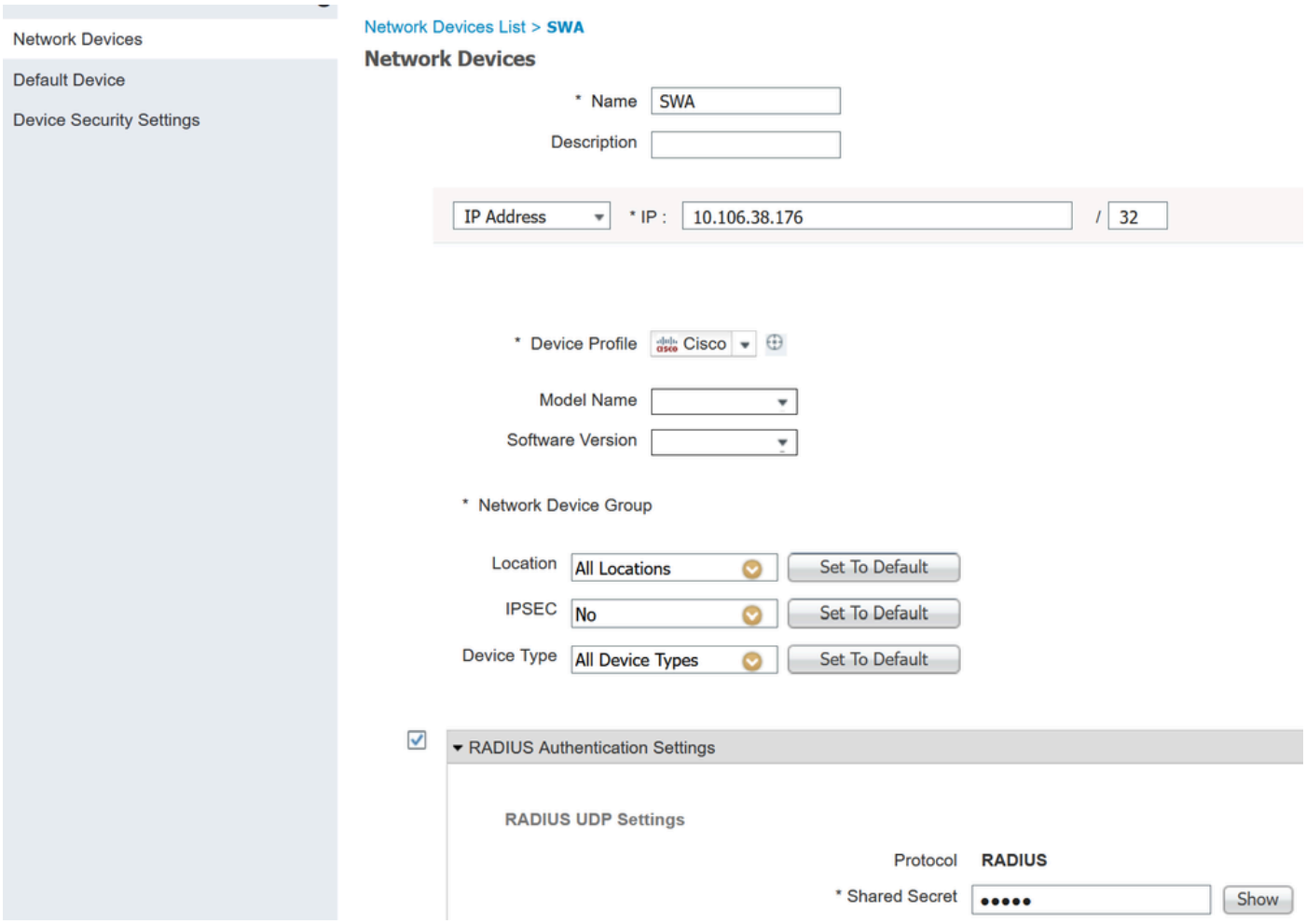
在ISE中添加SWA作为网络设备

第二步： 为网络设备对象分配名称并插入SWA IP地址。

选中RADIUS 复选框并定义共享密钥。

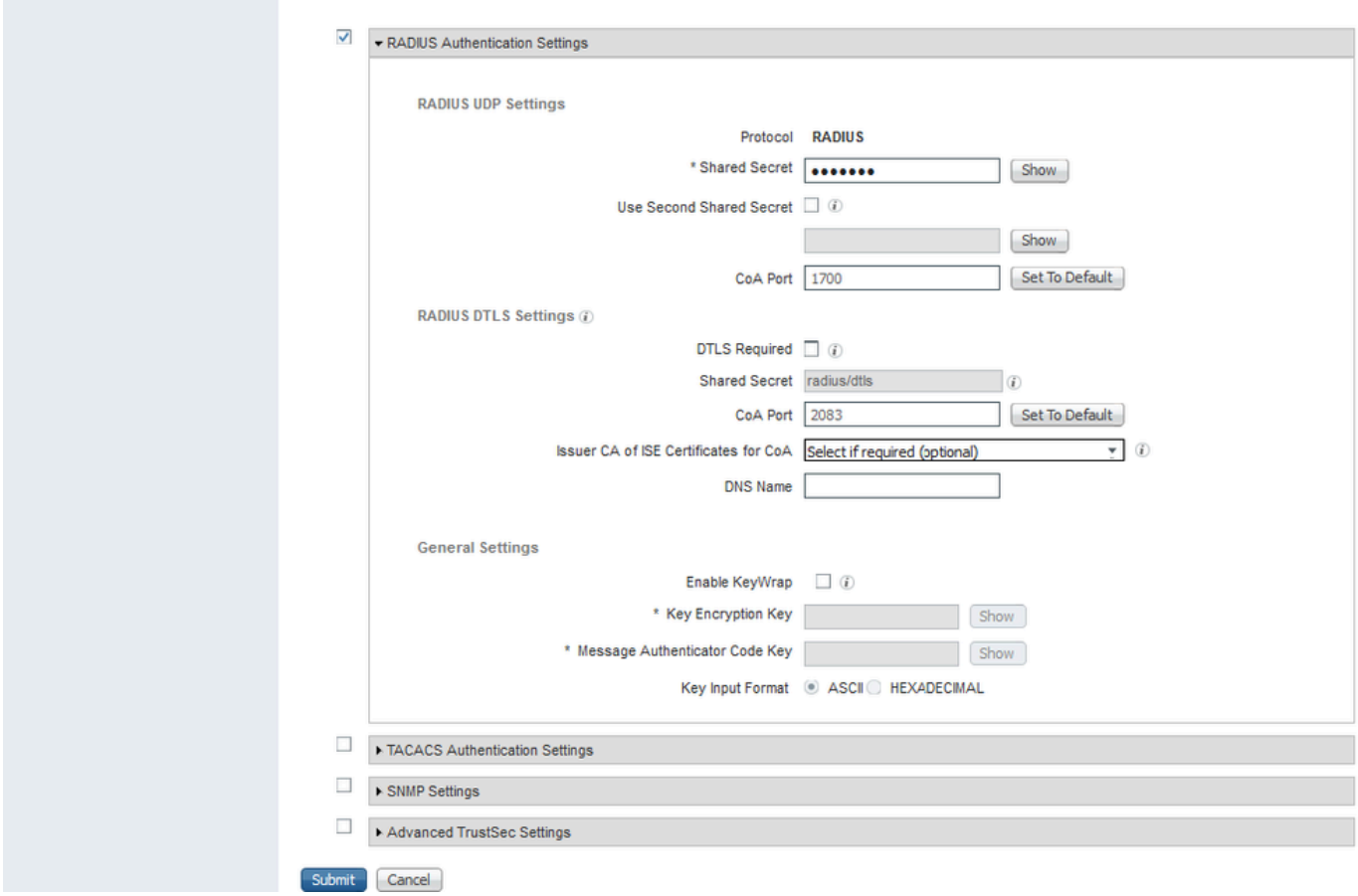


注意：稍后必须在SWA中配置相同的RADIUS服务器密钥。



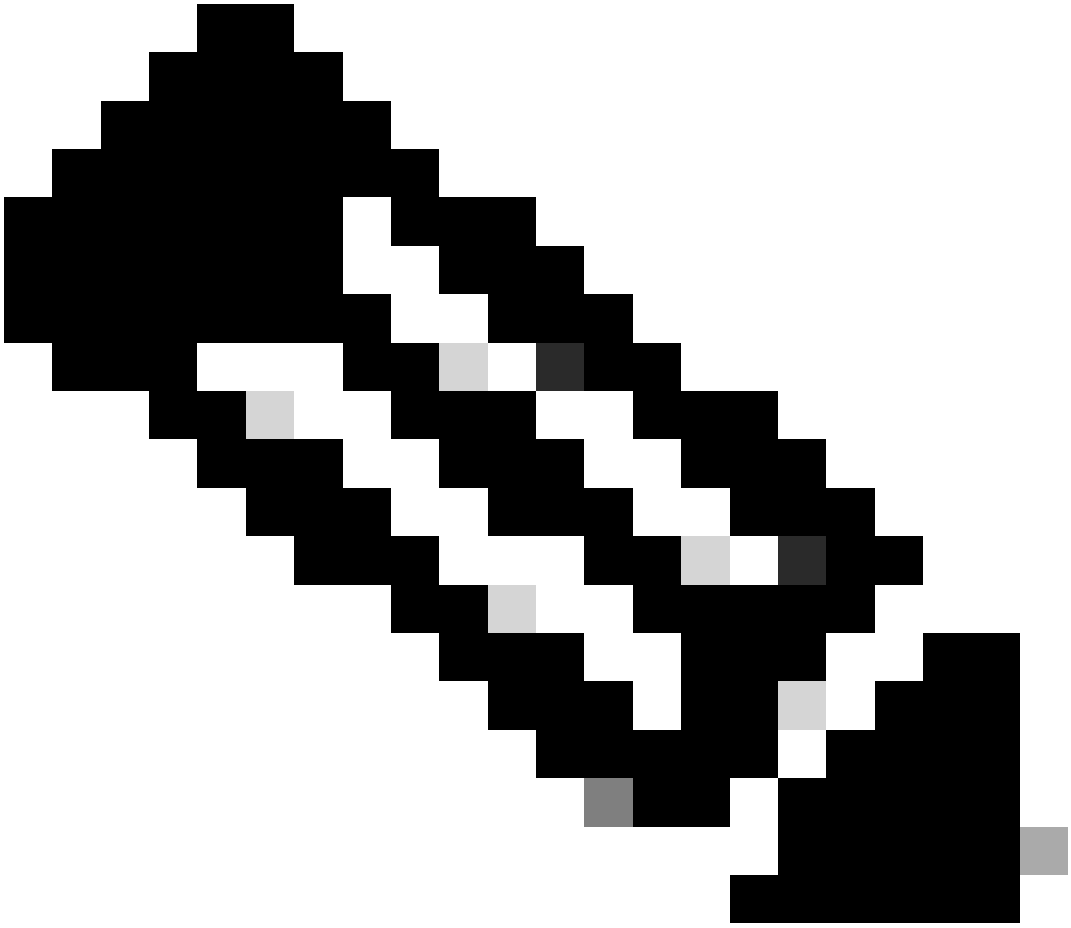
配置SWA网络设备共享密钥

步骤 2.1单击“Submit”。

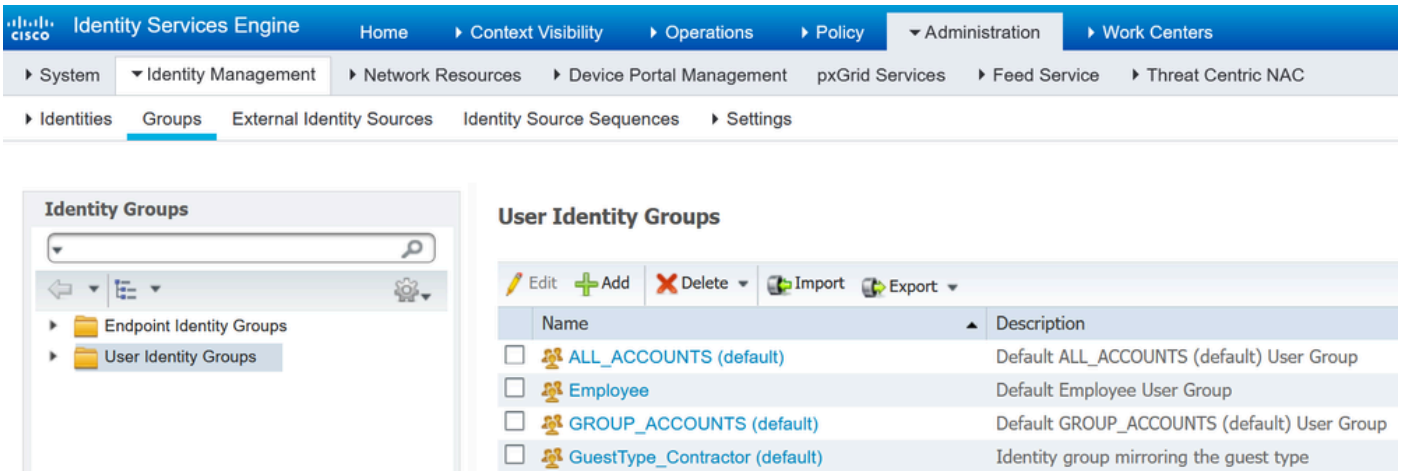


提交网络设备配置

第三步： 创建所需的用户身份组。导航到管理>身份管理> Groups >用户身份组> + Add。

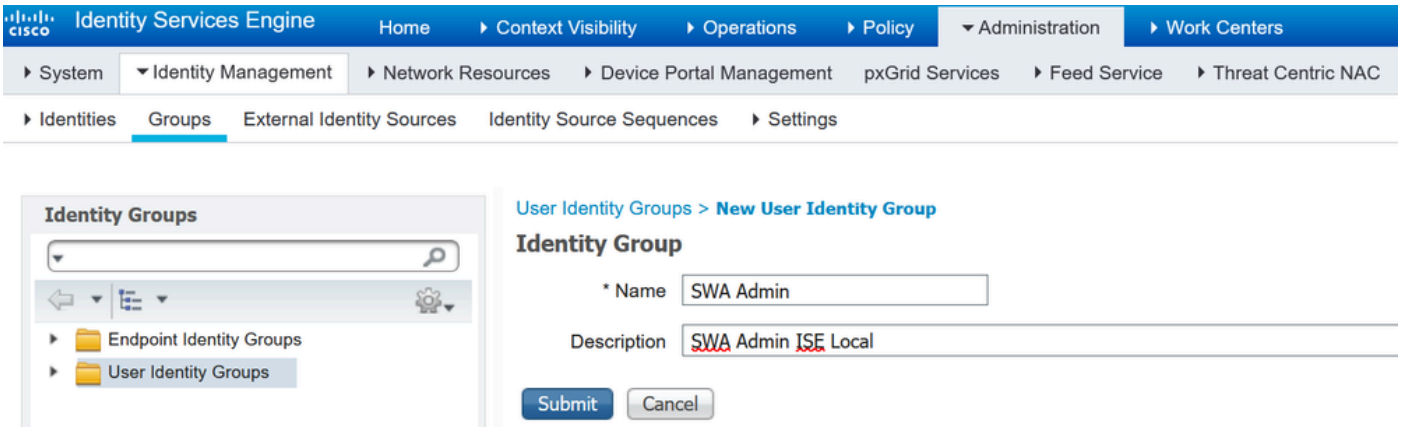


注意：您需要配置不同的用户组以匹配不同类型的用户。

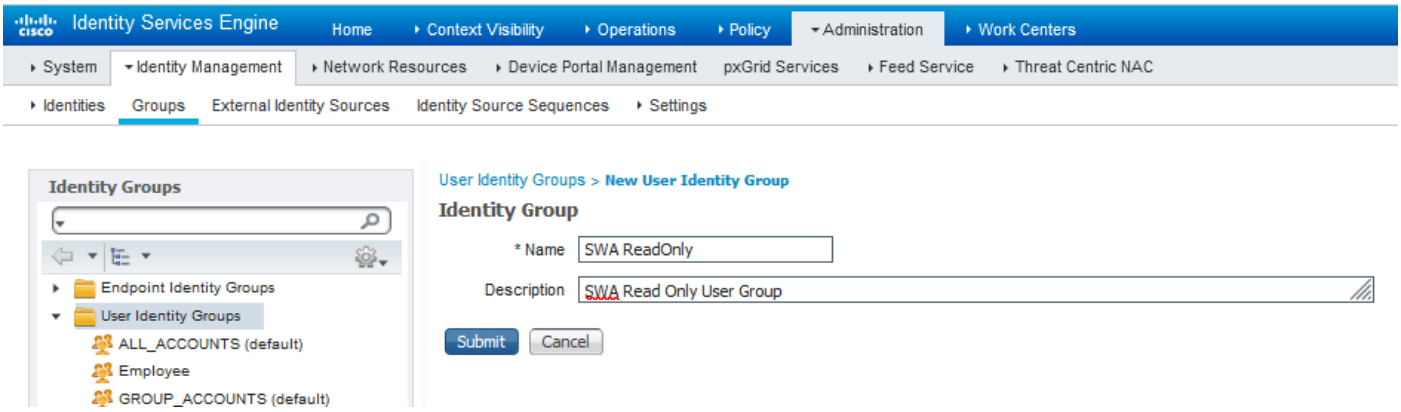


添加用户身份组

第四步：输入组名称、说明（可选）和提交。对每个组重复这些步骤。在本示例中，您为管理员用户创建一个组，为只读用户创建另一个组。



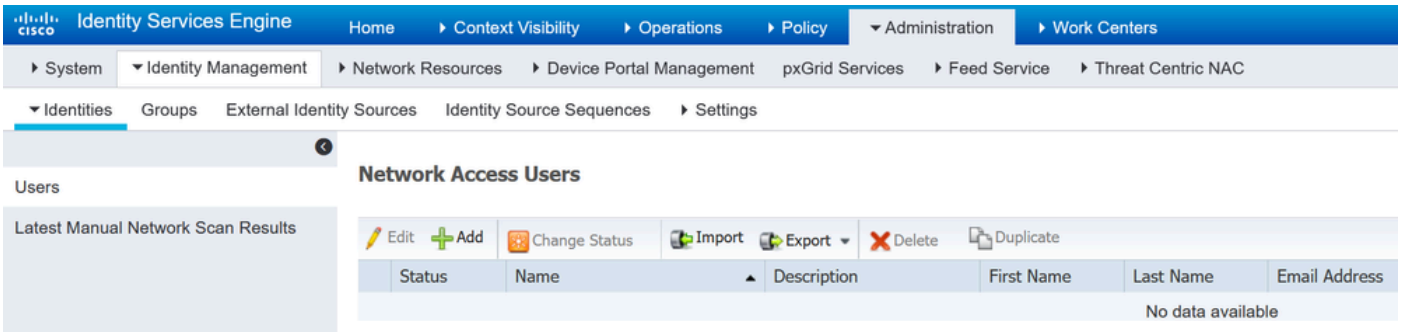
添加用户身份



组为SWA只读用户添加用户身份组

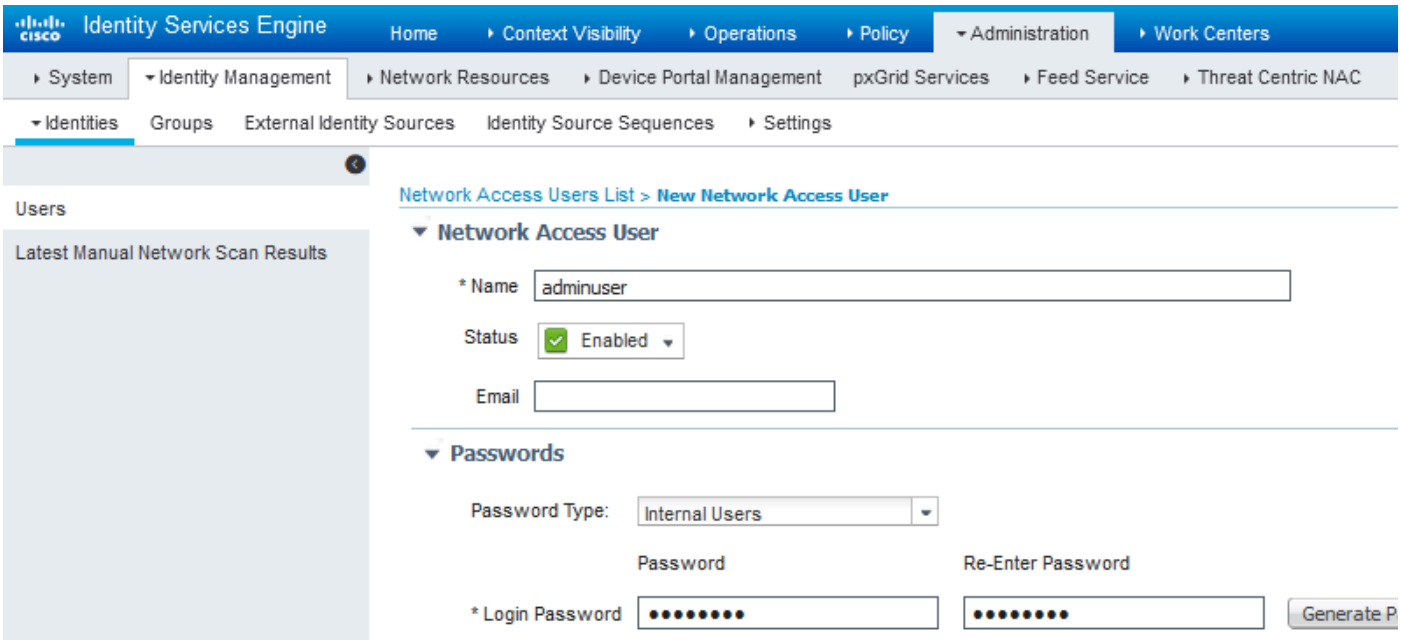
第五步：您需要创建与SWA中配置的用户名匹配的网络访问用户。

创建网络访问用户并将其添加到其对应组。导航到管理>身份管理>身份> + Add。



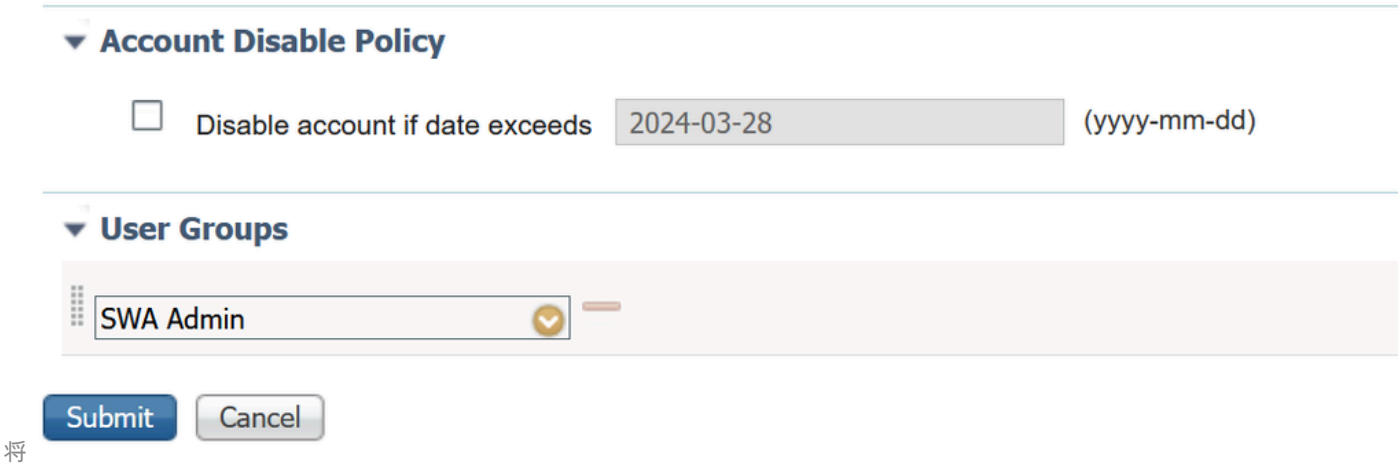
在ISE中添加本地用户

步骤 5.1您需要创建具有管理员权限的网络访问用户。指定名称和密码。



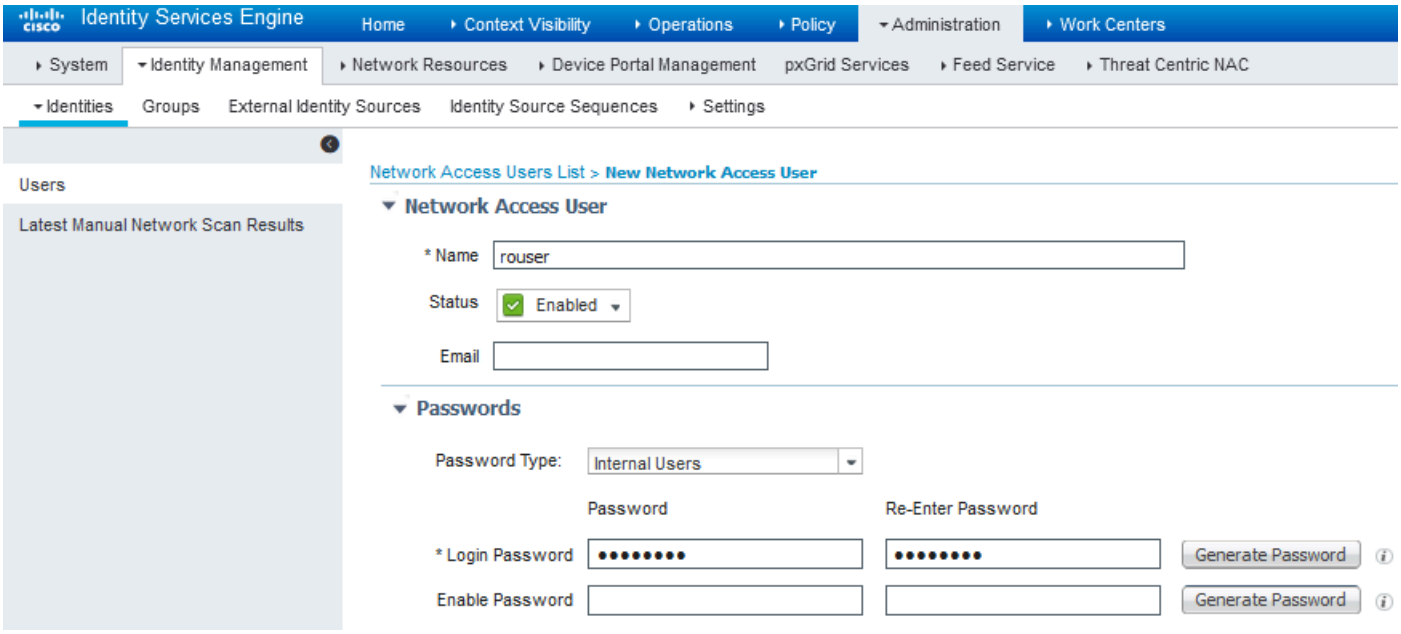
添加管理员用户

步骤 5.2在User Groups部分中选择SWA Admin。



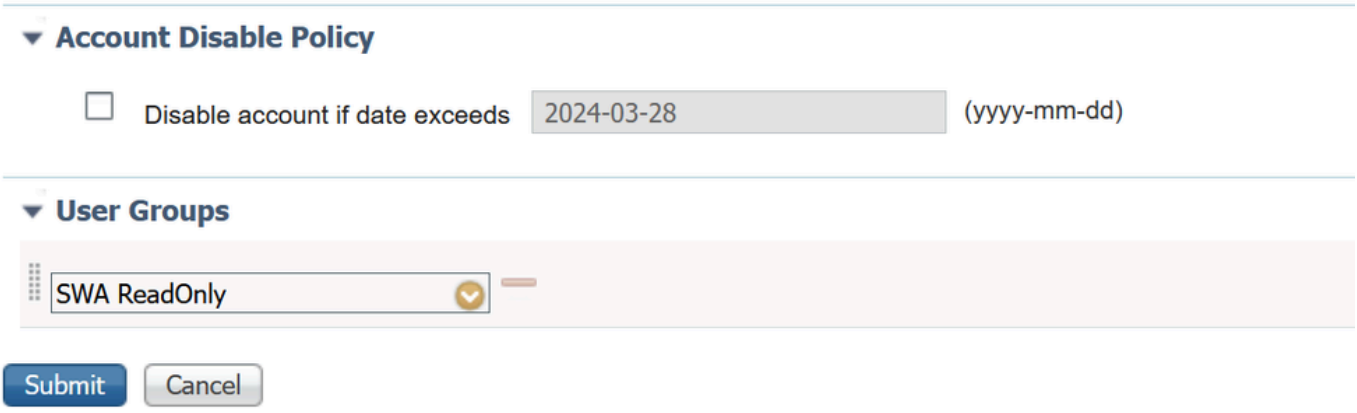
将Admin Group分配给Admin User

步骤 5.3您需要创建具有只读权限的用户。指定名称和密码。



添加只读用户

步骤 5.4在User Groups部分中选择SWA ReadOnly。

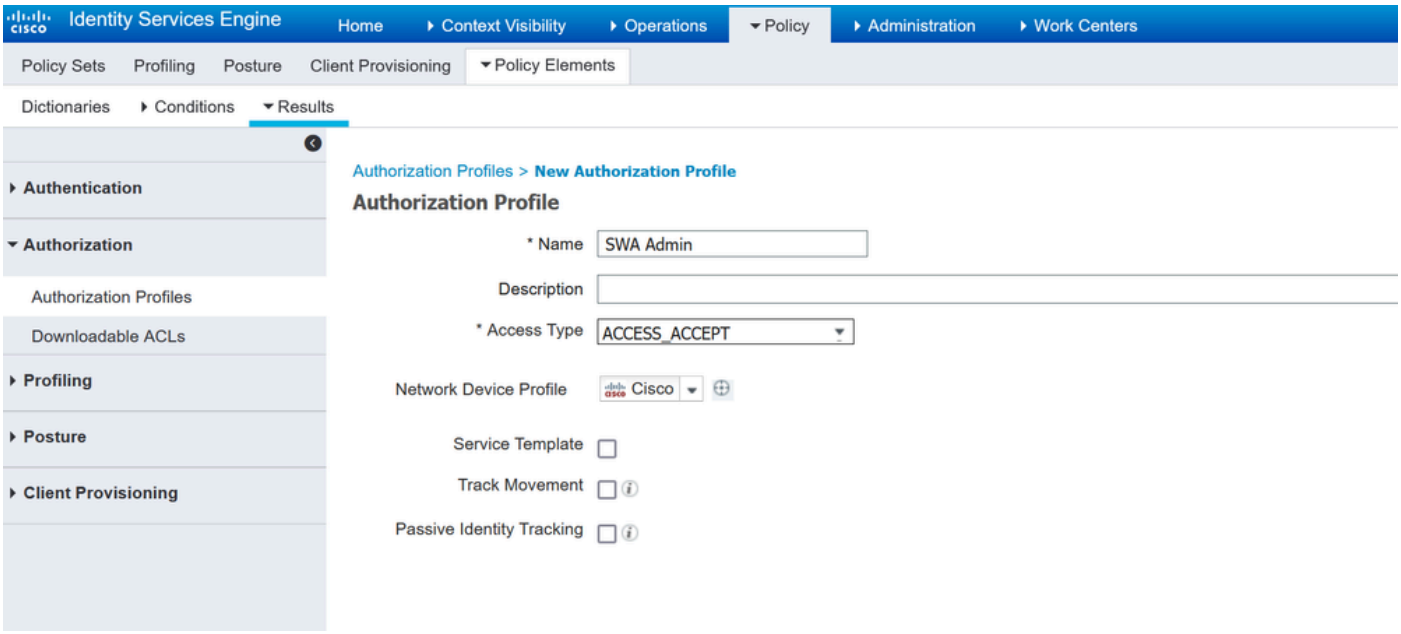


将只读用户组分配给只读用户

第六步： 为管理员用户创建授权配置文件。

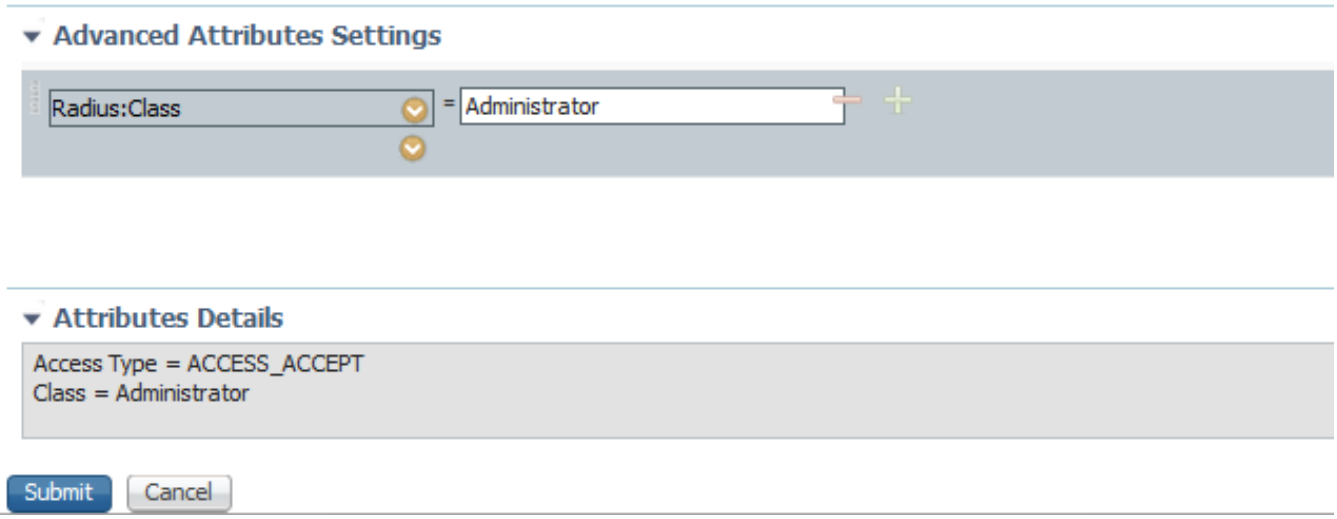
导航到策略>Policy元素>结果>授权>授权配置文件> +Add。

定义授权配置文件的名称，并确保将访问类型设置为ACCESS_ACCEPT。



添加管理员用户的授权配置文件

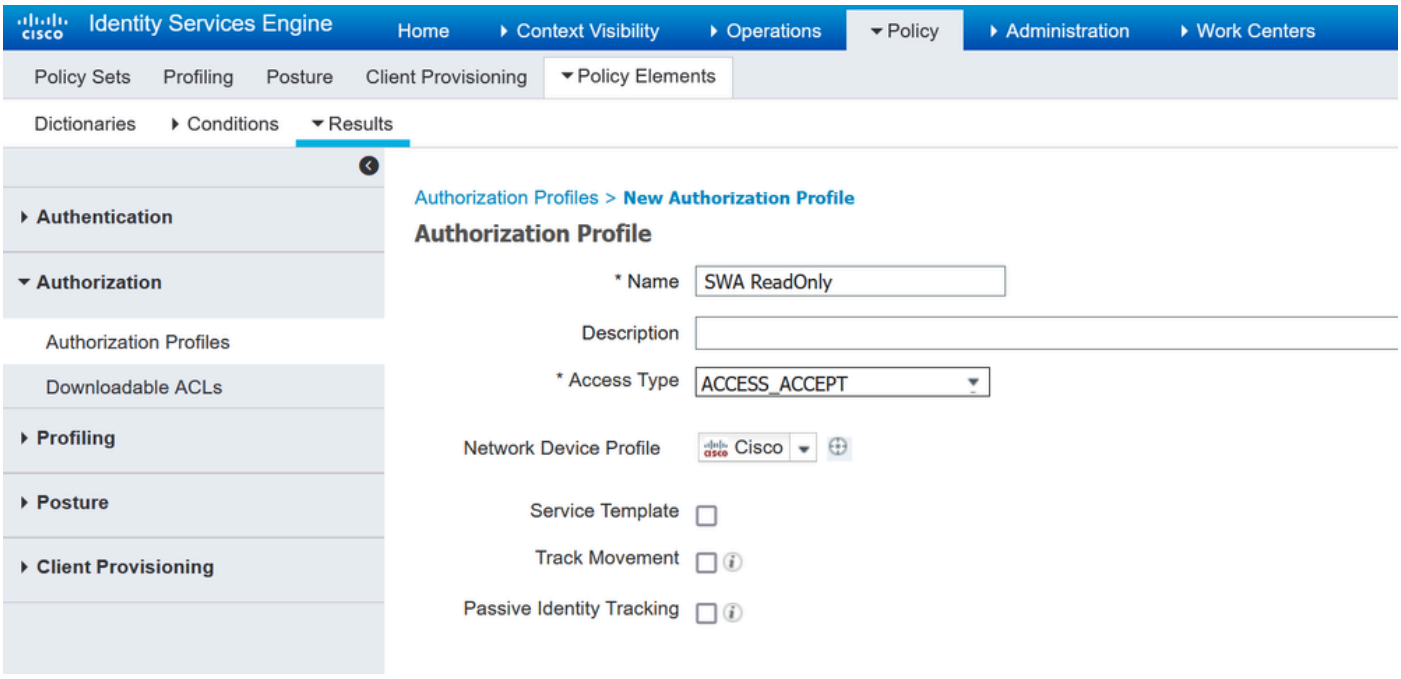
步骤 6.1在“高级属性设置”中，导航到Radius > Class—[25]，输入值Administrator，然后点击提交



。

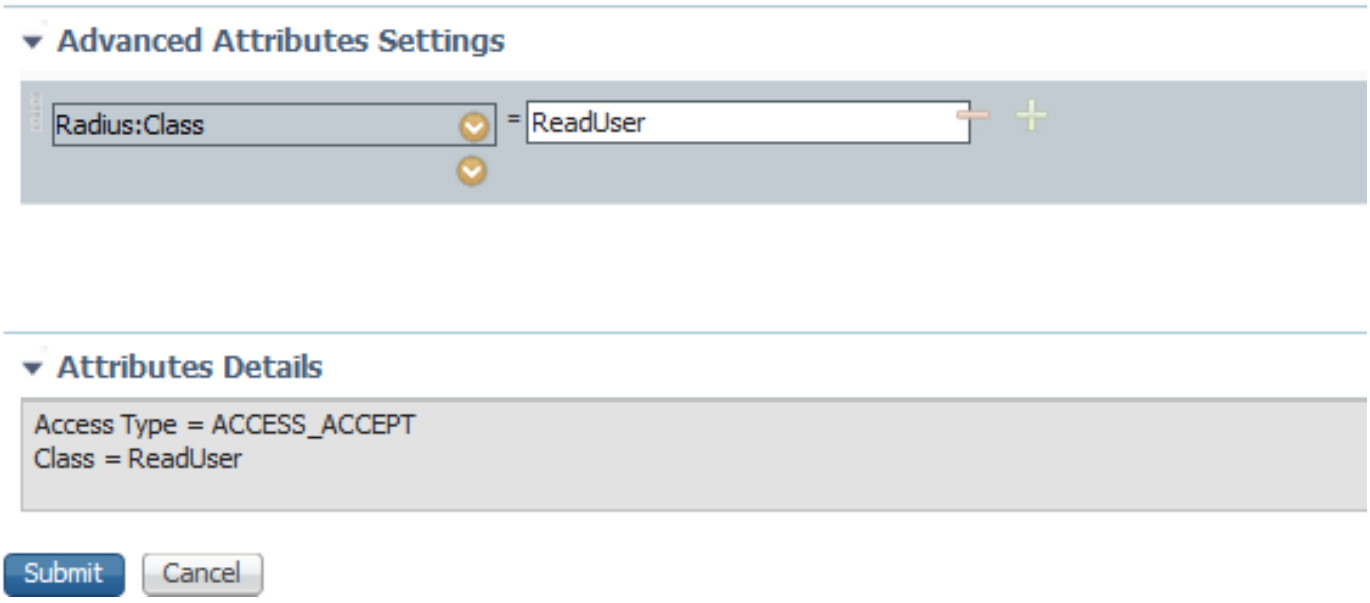
添加管理员用户的授权配置文件

步骤 7. 重复第6步为只读用户创建授权配置文件。



为只读用户添加授权配置文件

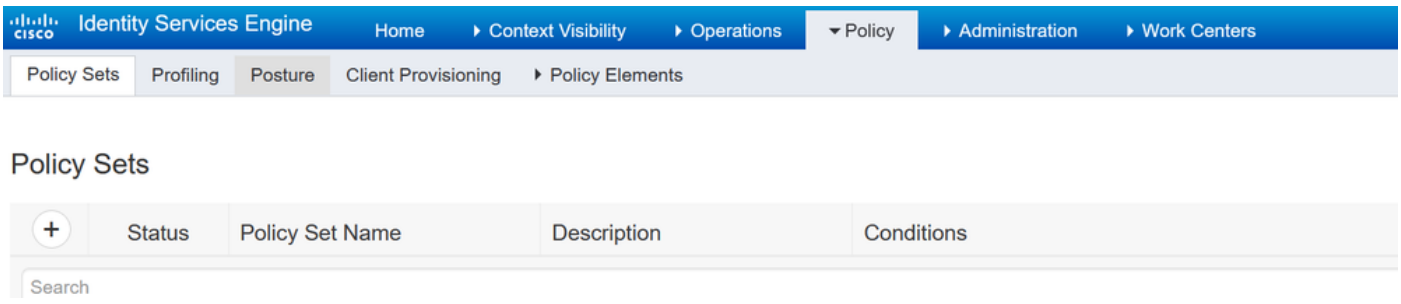
第 7.1 步： 使用值ReadUser创建Radius：Class，这次使用Administrator。



为只读用户添加授权配置文件

步骤 8 创建与SWA IP地址匹配的策略集。这是为了防止使用这些用户凭证访问其他设备。

导航到策略>策略集，点击位于左上角的+图标。

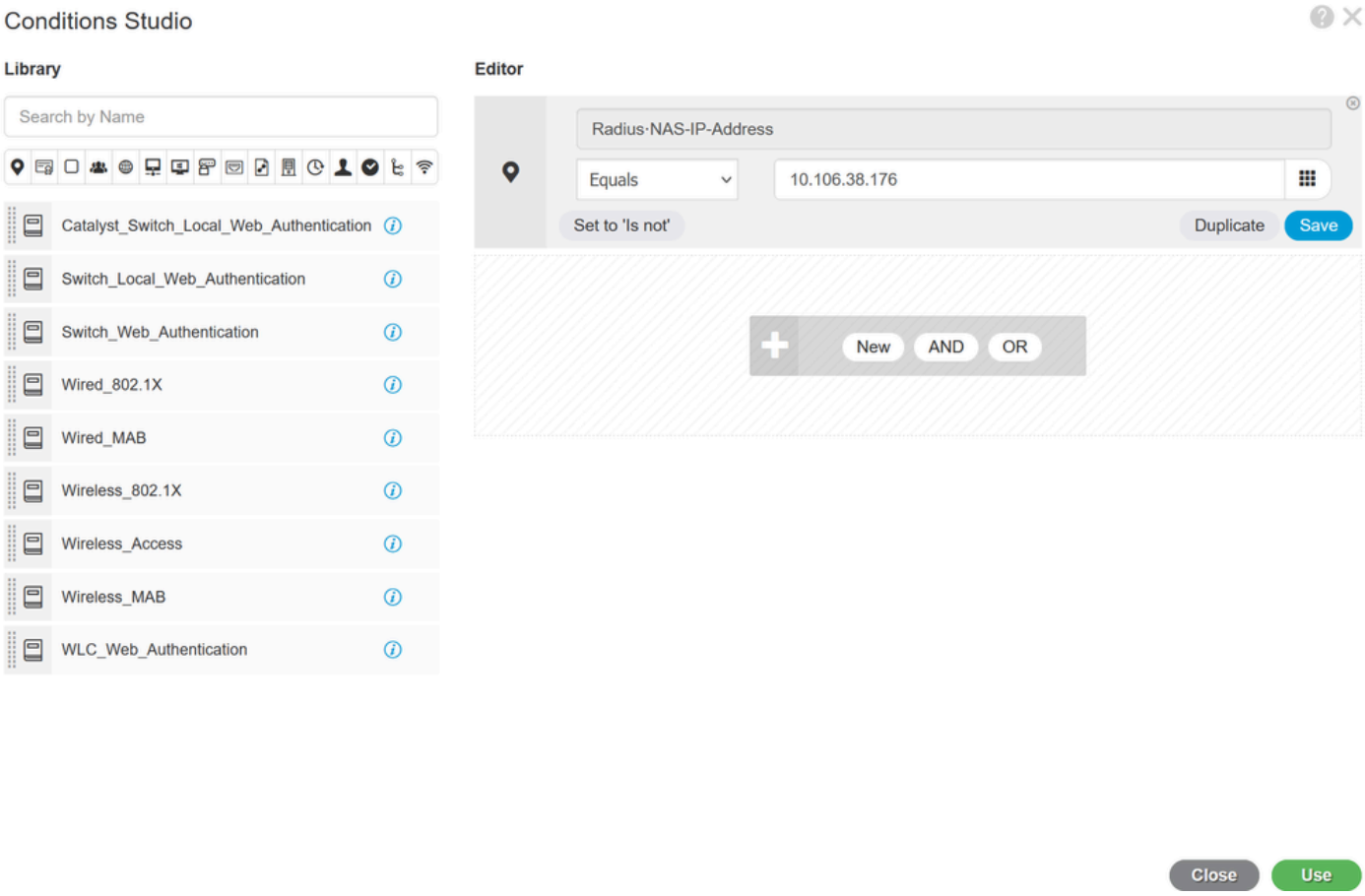


在ISE中添加策略集

步骤 8.1 新行位于策略集的顶部。

为新策略命名并为RADIUS NAS-IP-Address属性添加一个条件以匹配SWA IP地址。

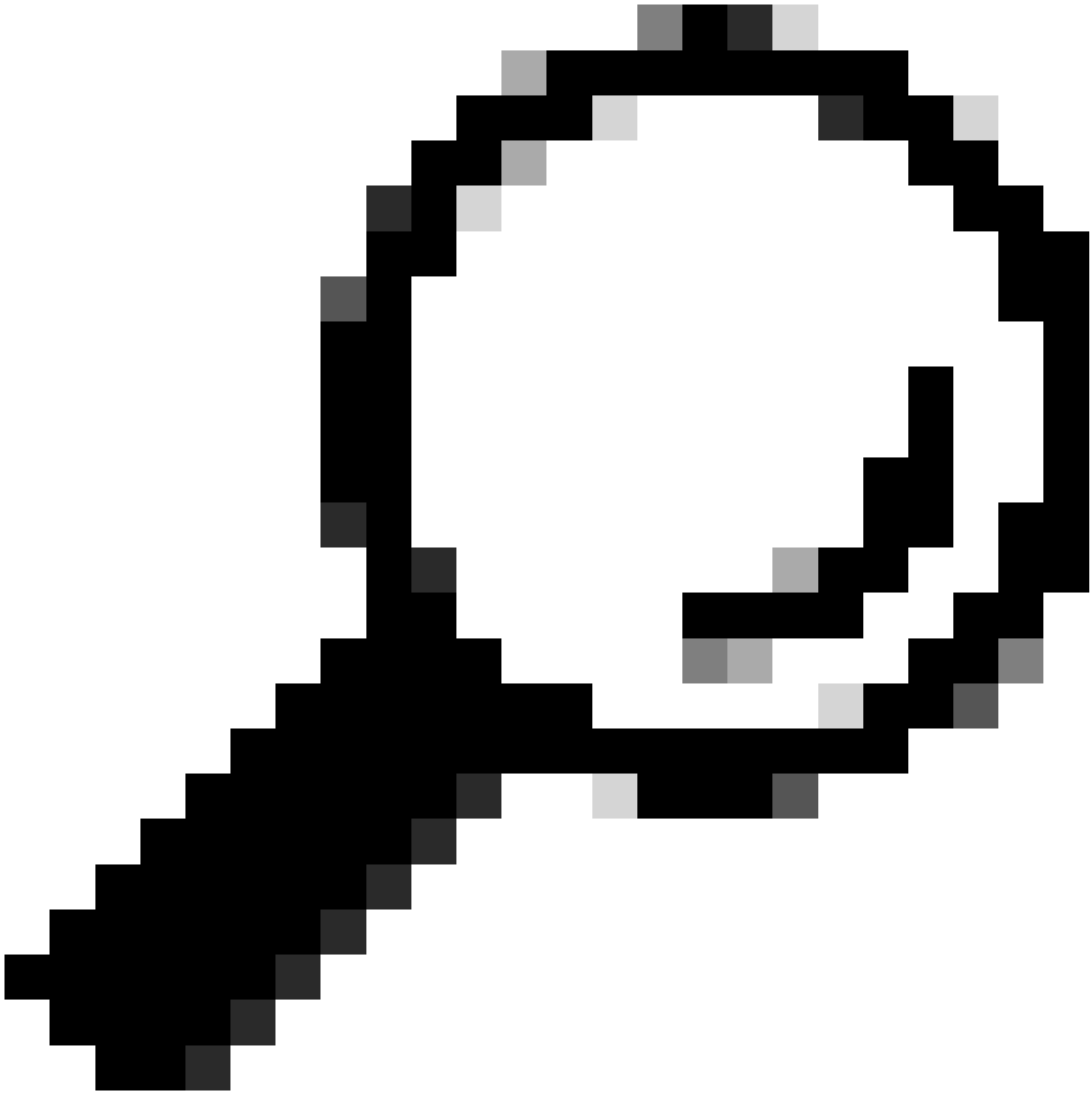
单击Use以保留更改并退出编辑器。



添加策略以映射SWA网络设备

步骤 8.2Click Save.

策略保存



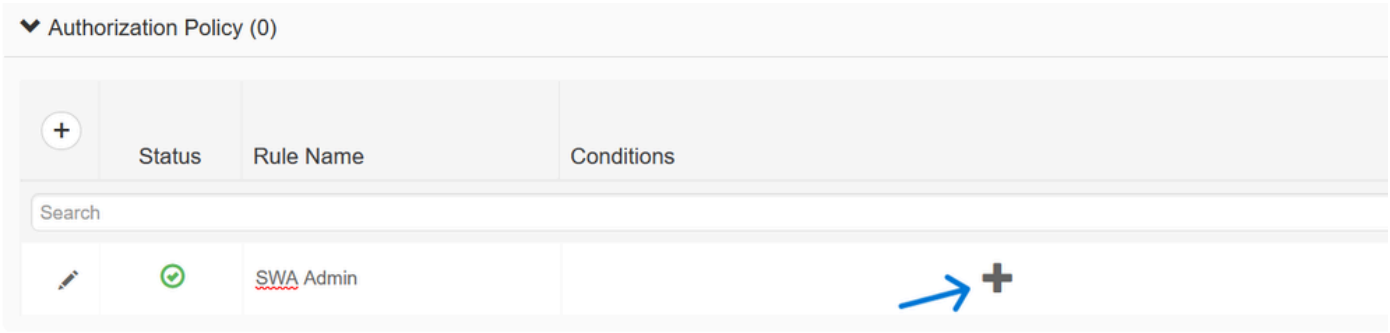
提示：在本文中，默认网络访问协议列表是允许的。您可以创建新列表并根据需要缩小范围。

步骤 9要查看新的策略集，请点击查看列中的> 图标。展开Authorization Policy菜单并单击+图标以添加新规则，从而允许对具有管理员权限的用户进行访问。

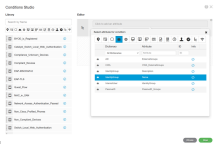
设置名称。

步骤 9.1要创建匹配管理员用户组的条件，请点击+图标。

添

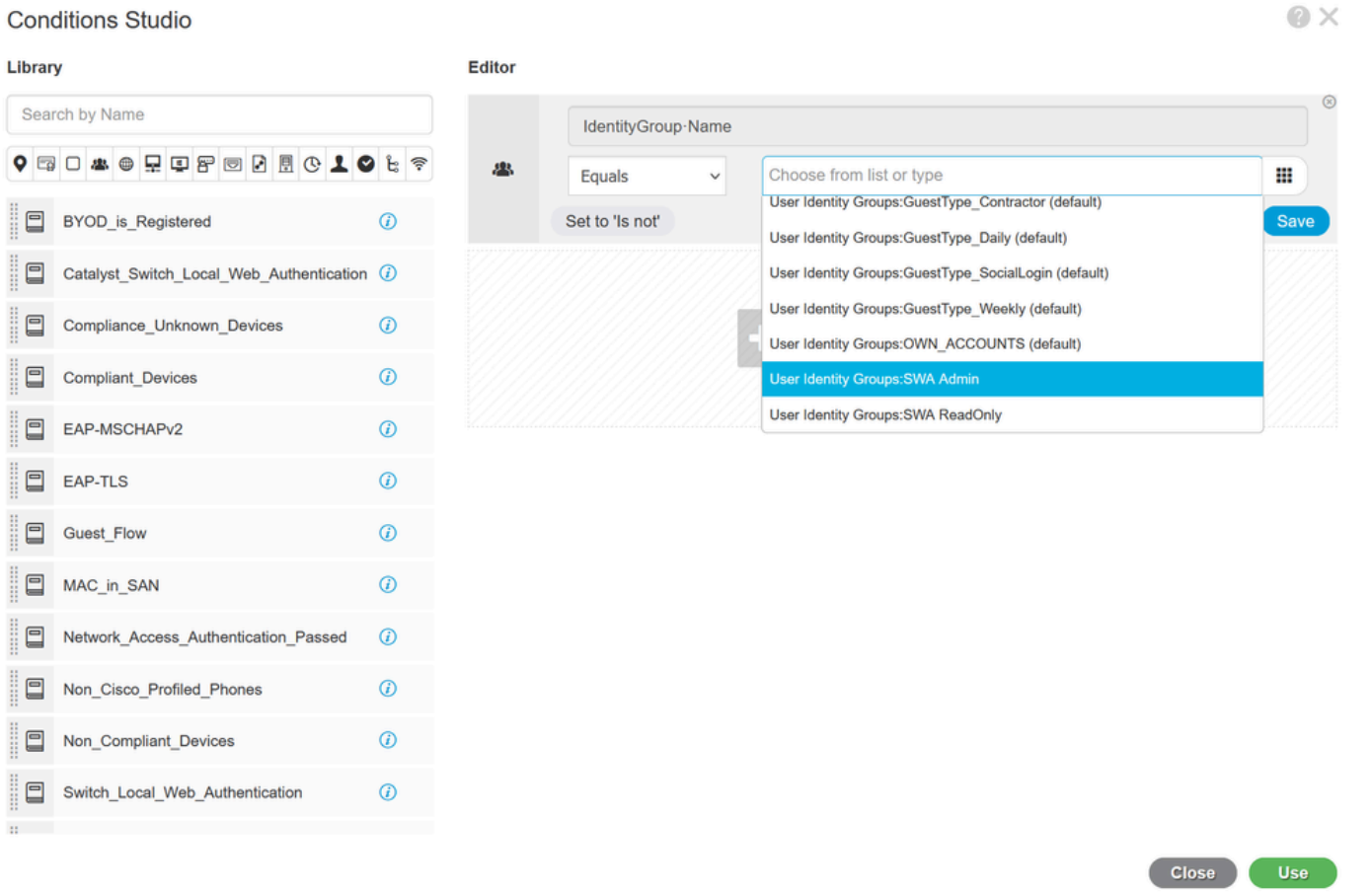


加授权策略条件



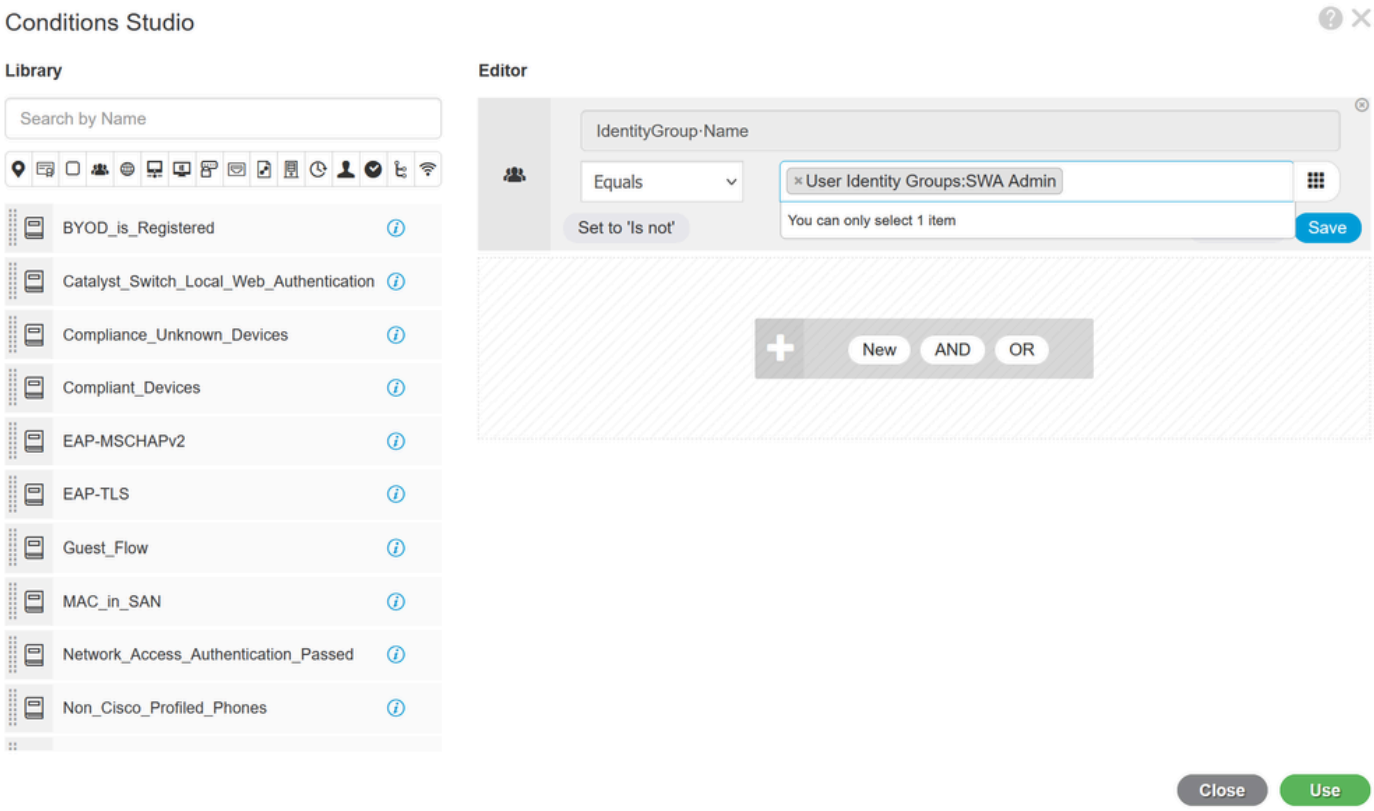
步骤 9.2设置条件以匹配Attribute Name Equals User Identity Groups： SWA admin. Select Identity Group as Condition的字典身份组

步骤 9.3向下滚动并选择User Identity Groups： SWA admin.



Scroll Down abd Select Identity Group Name

步骤 9.4单击Use。

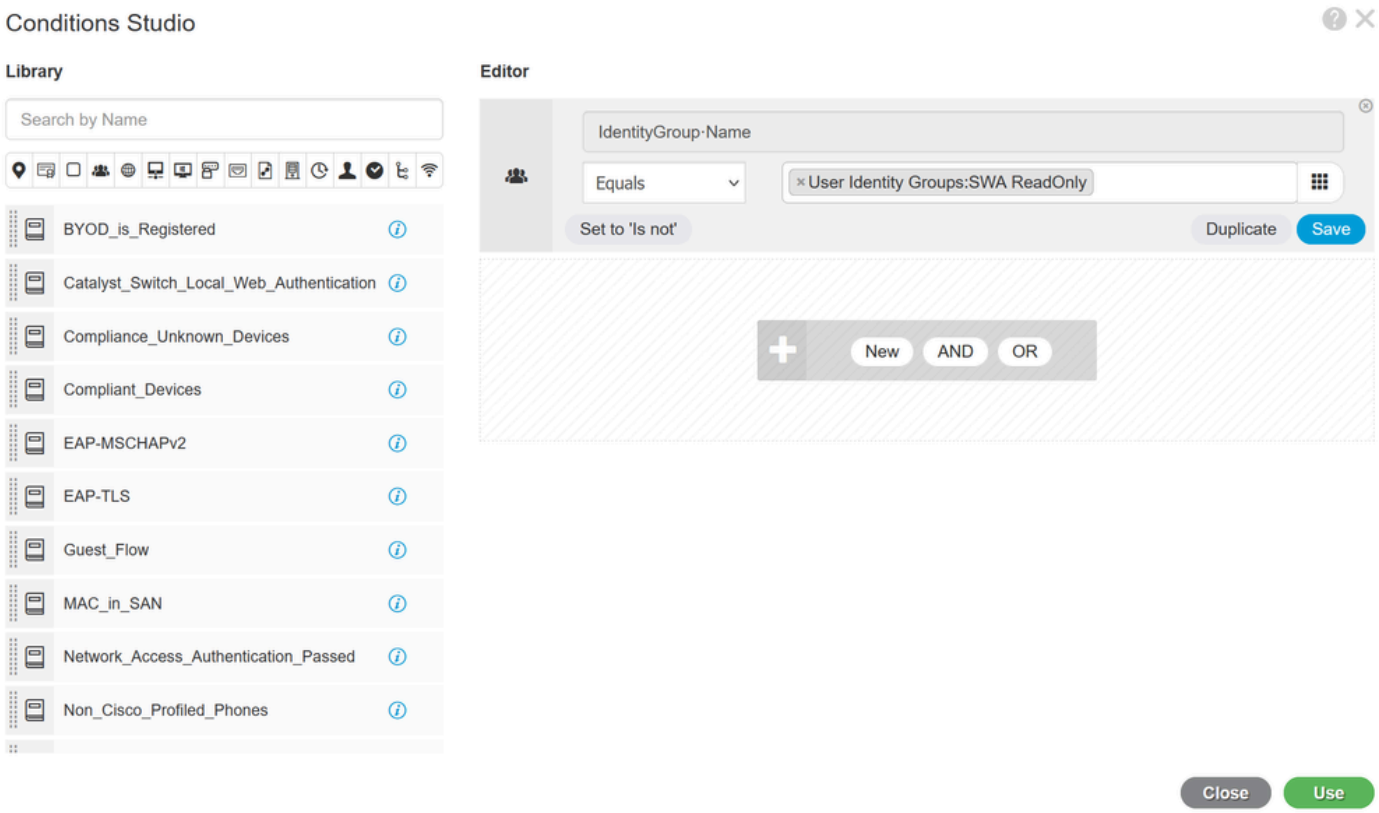


为SWA管理员用户组选择授权策略

步骤 10 单击+图标可添加第二条规则，用于为具有只读权限的用户提供访问权限。

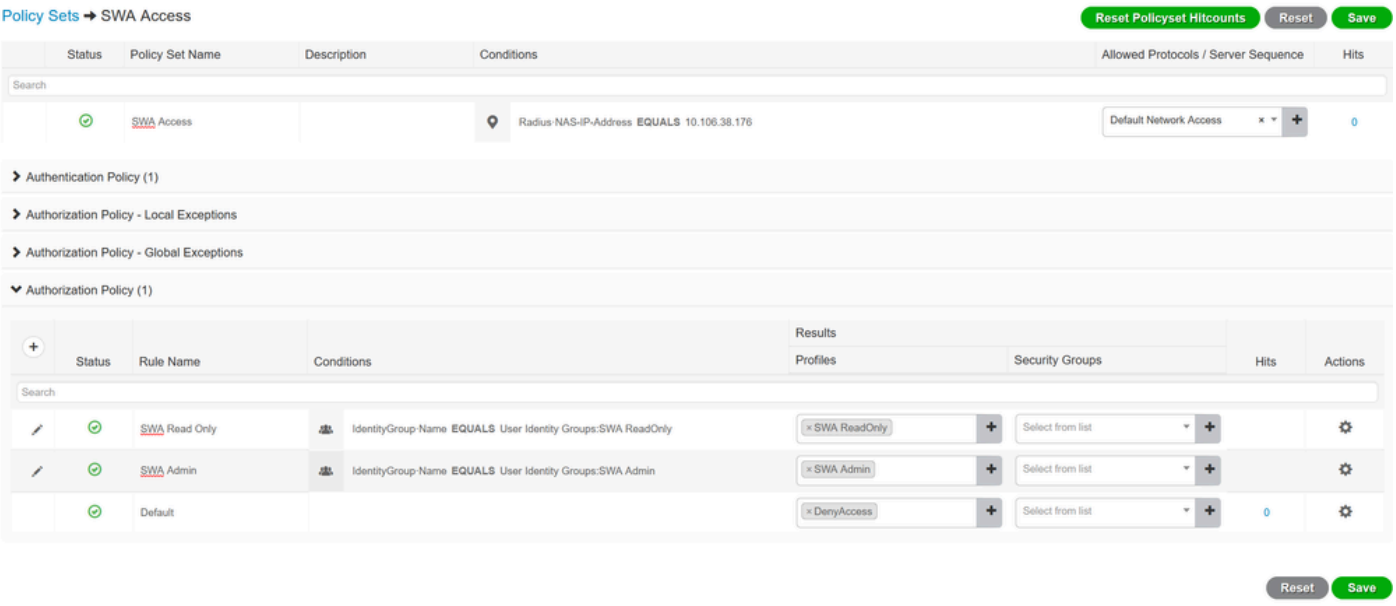
设置名称。

设置条件以匹配Dictionary Identity Group和Attribute Name Equals User Identity Groups： SWA ReadOnly，然后单击Use。



选择只读用户组的授权策略

步骤 11 分别为每个规则设置Authorization Profile，然后单击Save。

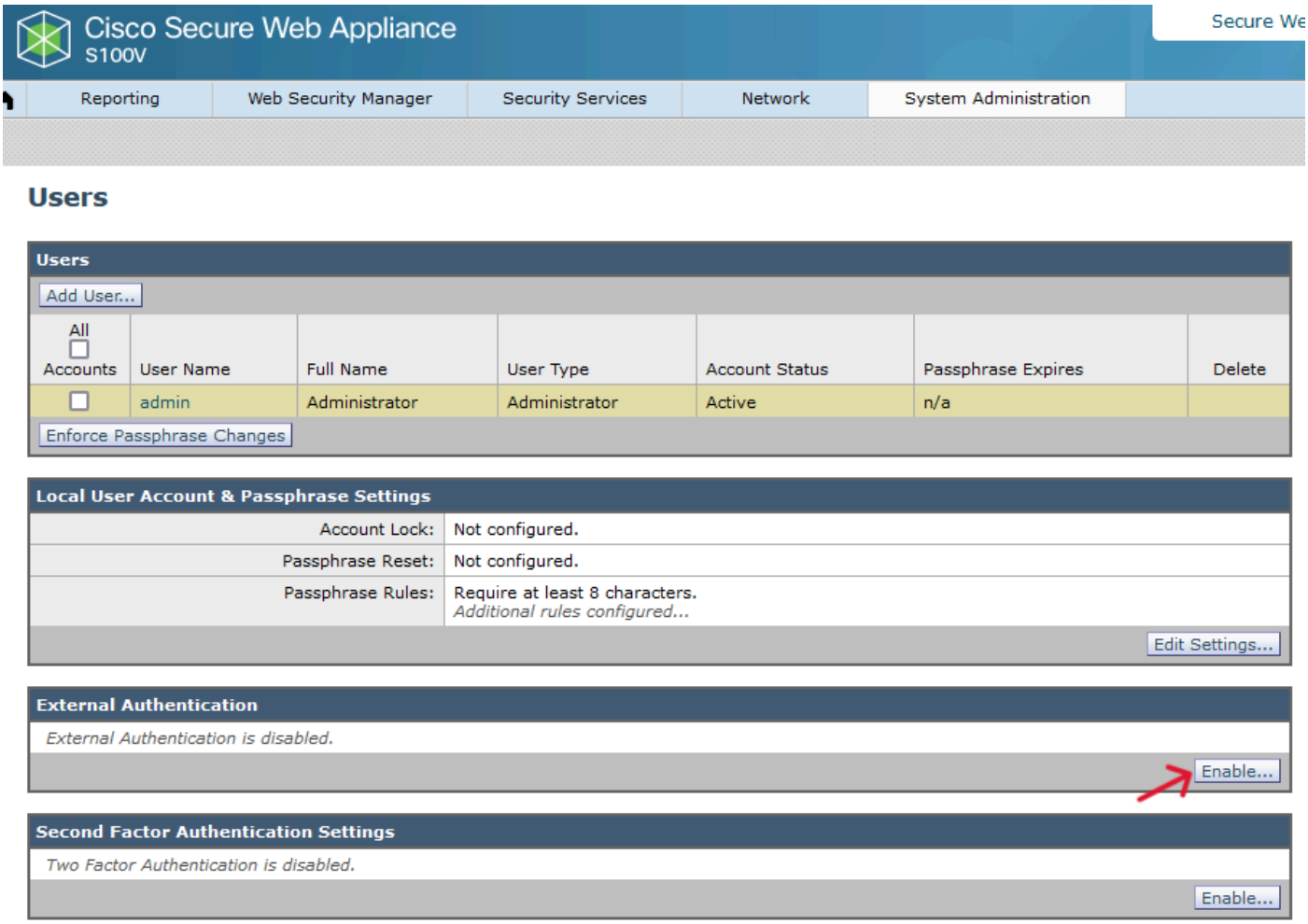


选择授权配置文件

SWA配置

步骤1:从SWA GUI导航至系统管理，然后点击用户。

第二步：在External Authentication中单击Enable。



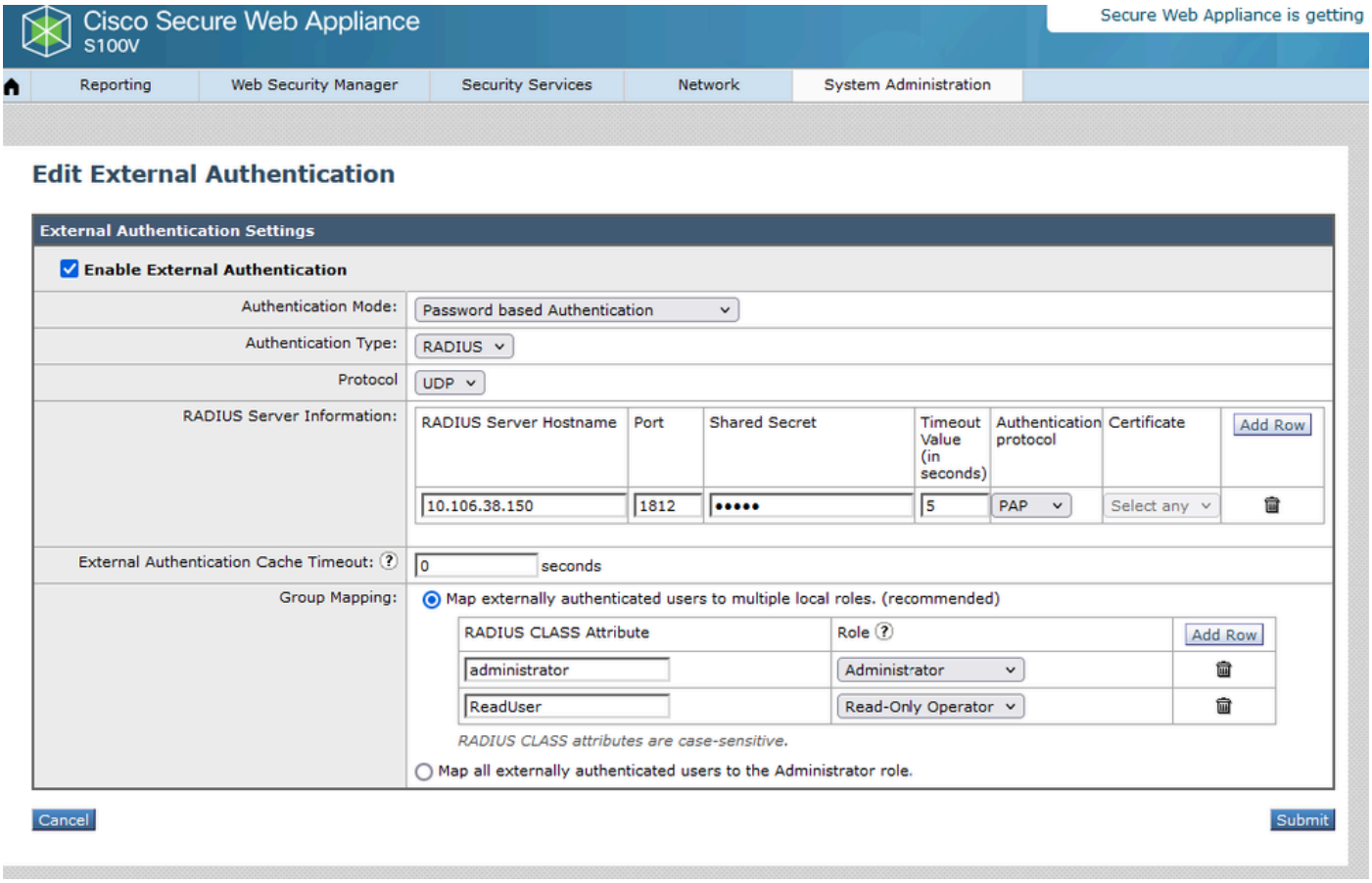
在SWA中启用外部身份验证

第三步：在RADIUS Server Hostname字段中输入ISE的IP地址或FQDN，并输入在步骤2 ISE配置中配置的相同共享密钥。

第四步：在Group Mapping中选择Map external authenticated users to multiple local roles。

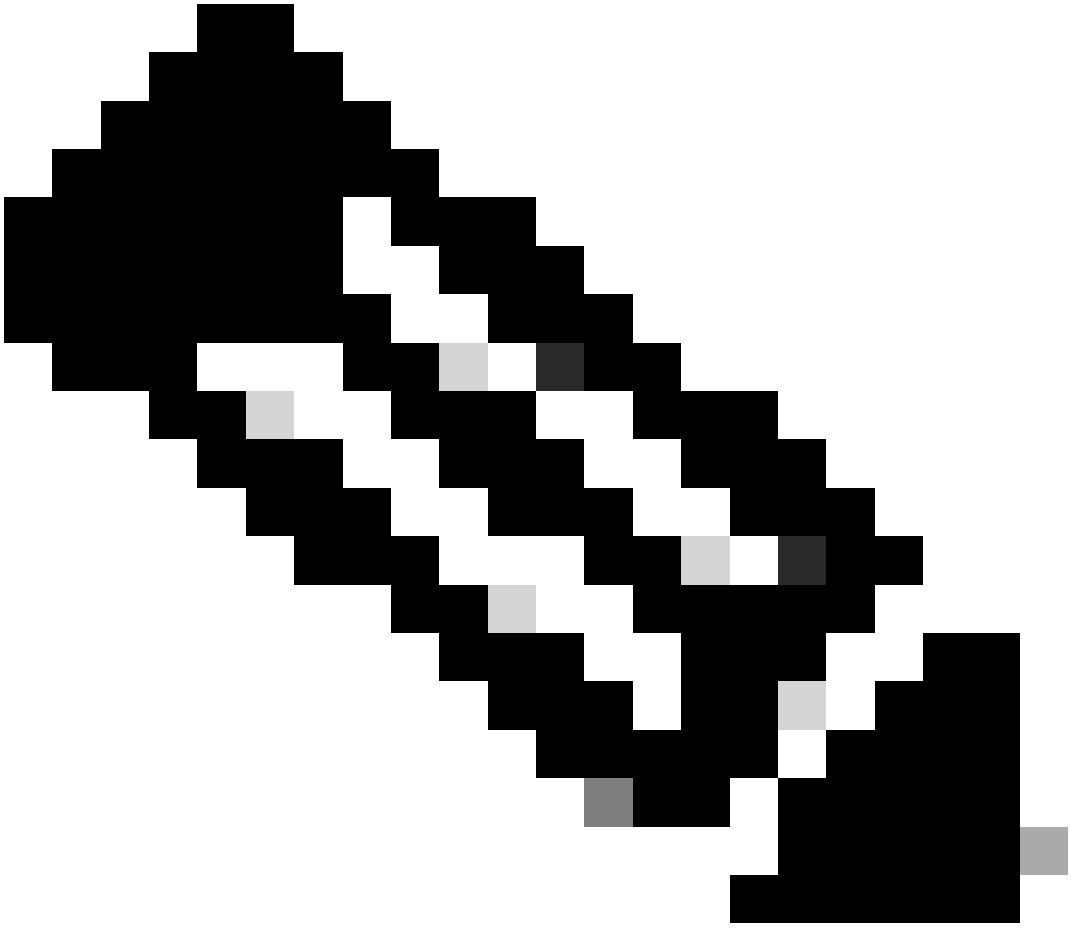
步骤 4.1在RADIUS CLASS Attribute字段中输入Administrator并选择Role Administrator。

步骤 4.2在RADIUS CLASS Attribute字段中输入ReadUser并选择角色Read-Only Operator。



RADIUS服务器的外部身份验证配置

第5步：要在SWA中配置用户，请点击添加用户。输入User Name并选择所需角色所需的User Type。输入Passphrase和Retype Passphrase，如果设备无法连接到任何外部RADIUS服务器，则需要此口令才能进行GUI访问。



注意：如果设备无法连接到任何外部服务器，它会尝试将用户验证为安全Web设备上定义的本地用户。

Users

Users

Add User...

* When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.

All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
☐	adminuser	Admin User	*Administrator*	Active	n/a	🗑
☐	rouser	RO User	*Read-Only Operator*	Active	n/a	🗑

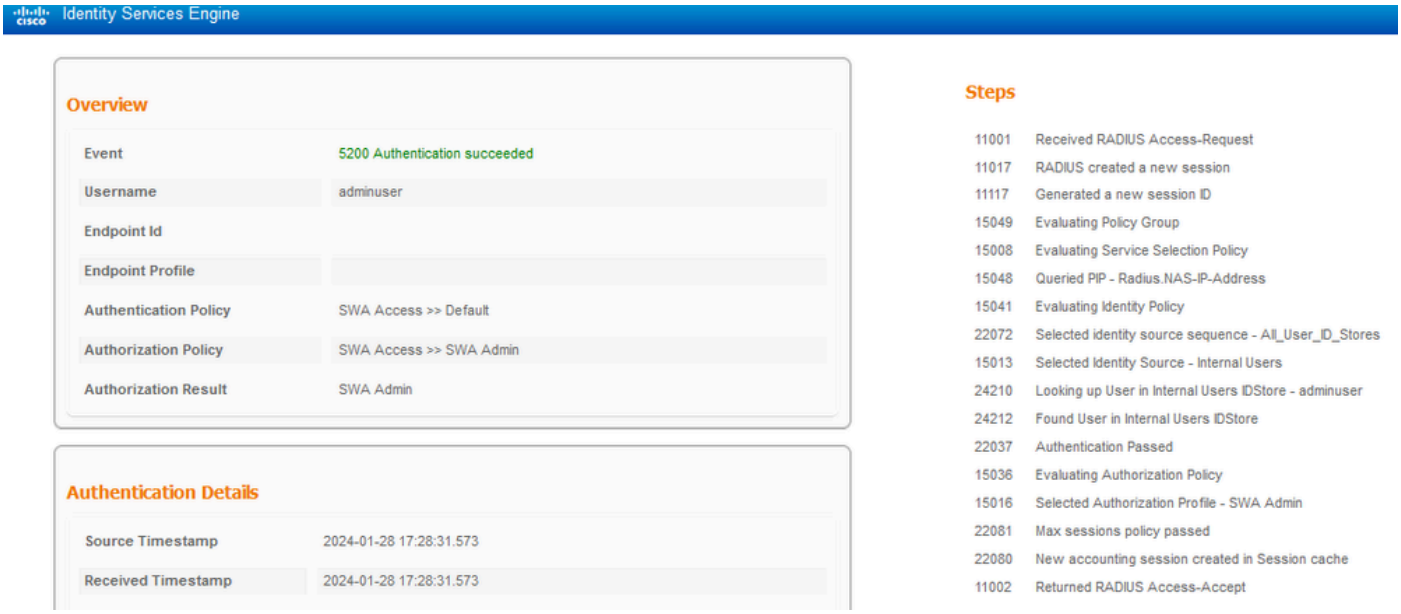
SWA中的用户配置

第6步：点击提交并提交更改。

验证

使用配置的用户凭证访问SWA GUI，并检查ISE中的实时日志。要检查ISE中的实时日志，请导航到

操作>实时日志：



验证用户登录ISE

相关信息

- 思科安全Web设备AsyncOS 14.0用户指南
- ISE 3.0管理员指南
- 安全Web设备的ISE兼容性列表
- 思科技术支持和下载

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）。