将ISE配置为RADIUS服务器的SWA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

网络拓扑

配置

- ISE 配置
- SWA配置

验证

相关内容

简介

本文档介绍使用Cisco ISE®作为RADIUS服务器在安全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：

- 基本RADIUS知识
- Cisco SWA基础知识
- 思科身份服务引擎®(ISE)上的身份验证和授权配置策略知识

思科建议您还应具备以下条件：

- 兼容的SWA和ISE版本
- SWA和ISE管理访问

使用的组件

本文档中的信息基于以下软件版本：

- ISE 3.0.0
- SWA 14.0.2-012

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SWA的管理用户启用外部身份验证时，设备会使用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



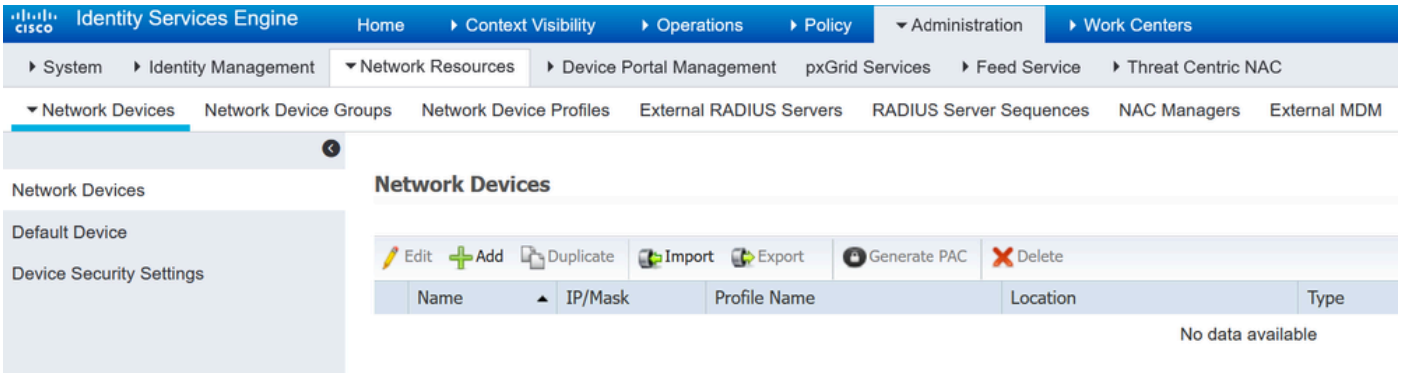
网络拓扑图

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

配置

ISE 配置

1.添加新网络设备并导航到管理>网络资源>网络设备> +添加。

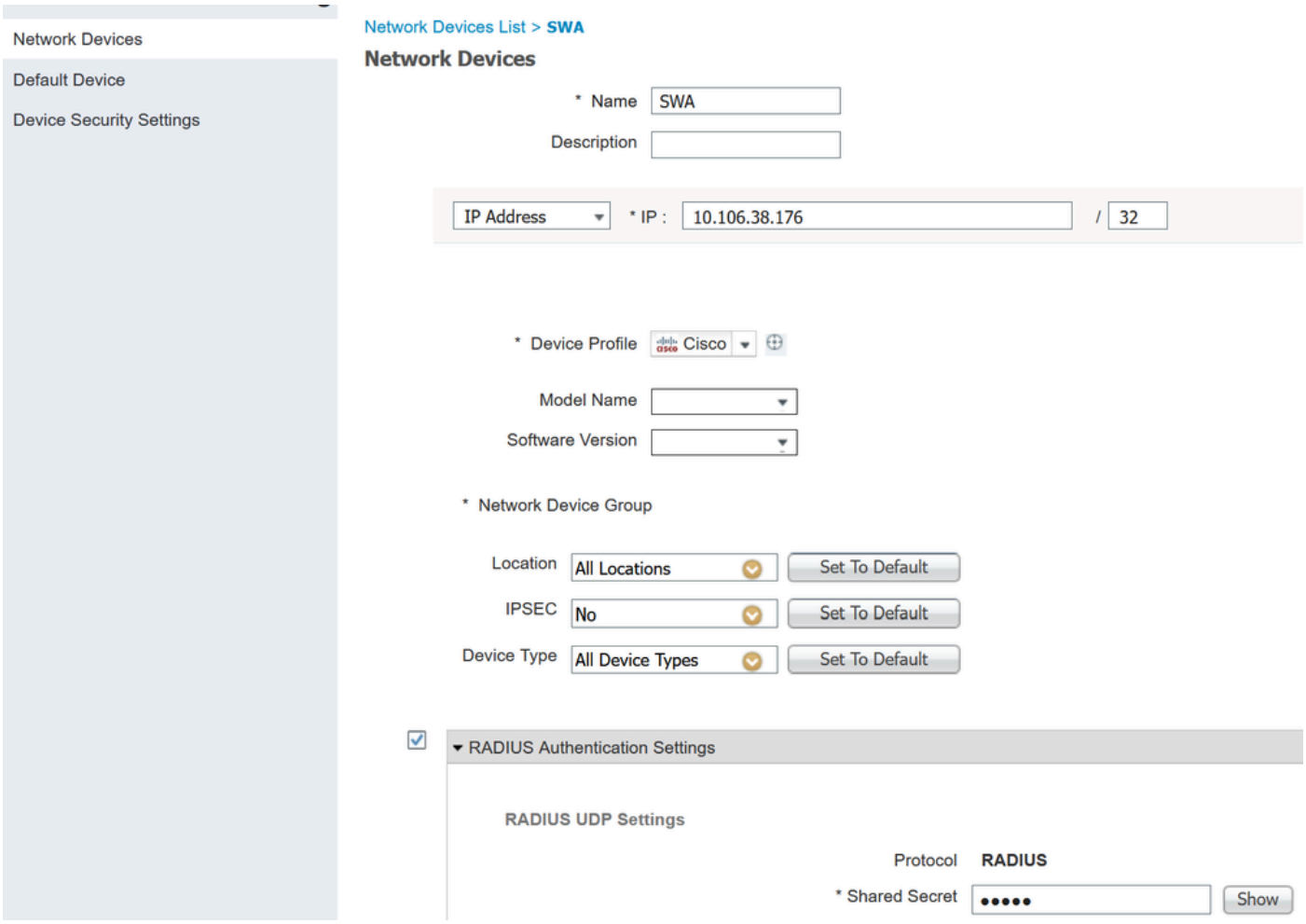


在ISE中将SWA添加为网络设备

2.为网络设备对象分配名称，然后插入SWA IP地址。

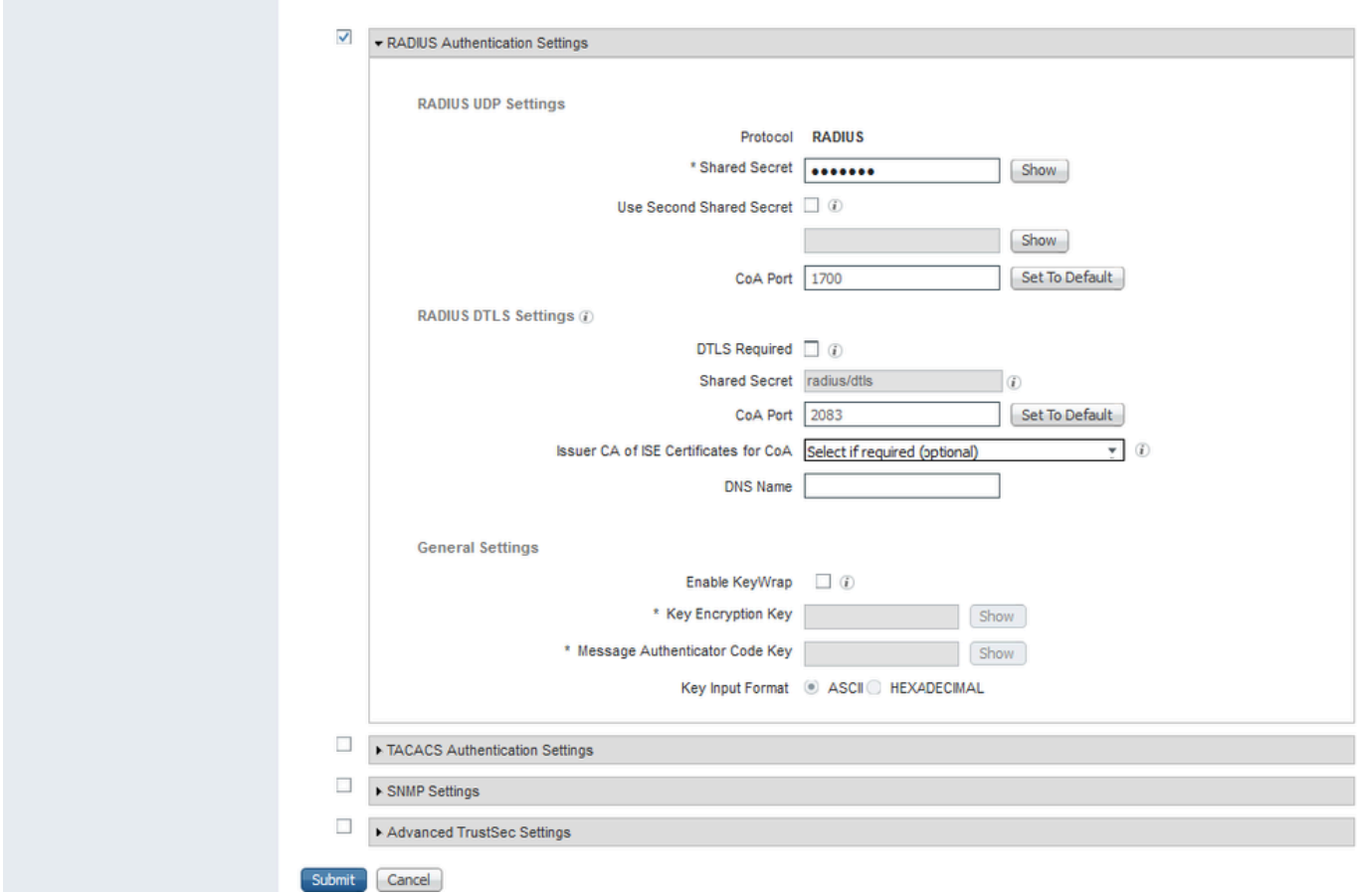
2.1.选中RADIUS复选框并定义共享密钥。

注意：稍后必须在SWA中使用相同的密钥来配置RADIUS服务器。



配置SWA网络设备共享密钥

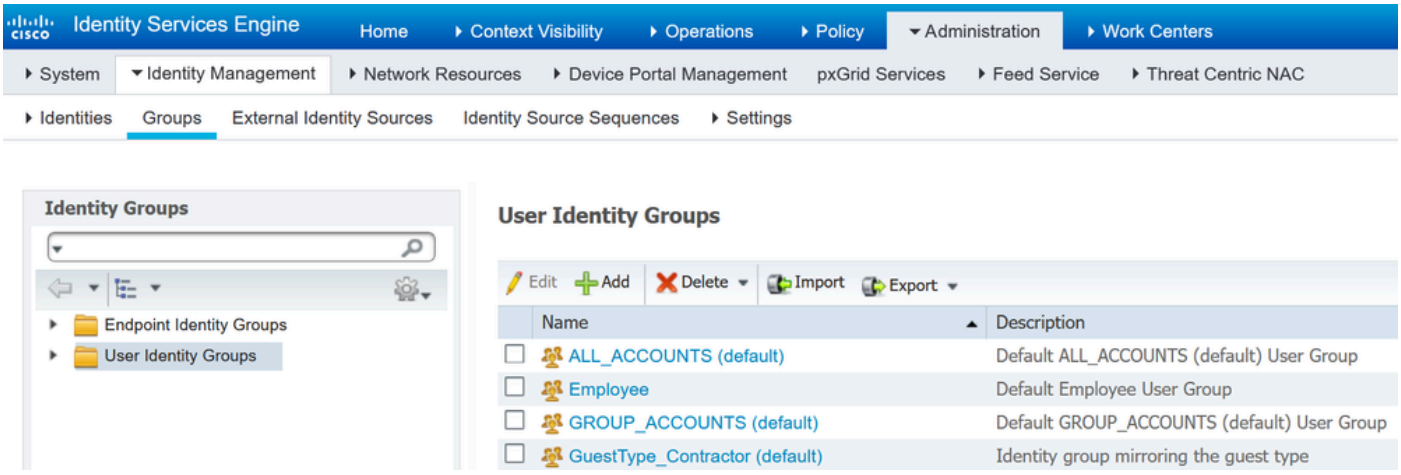
2.2.单击Submit。



提交网络设备配置

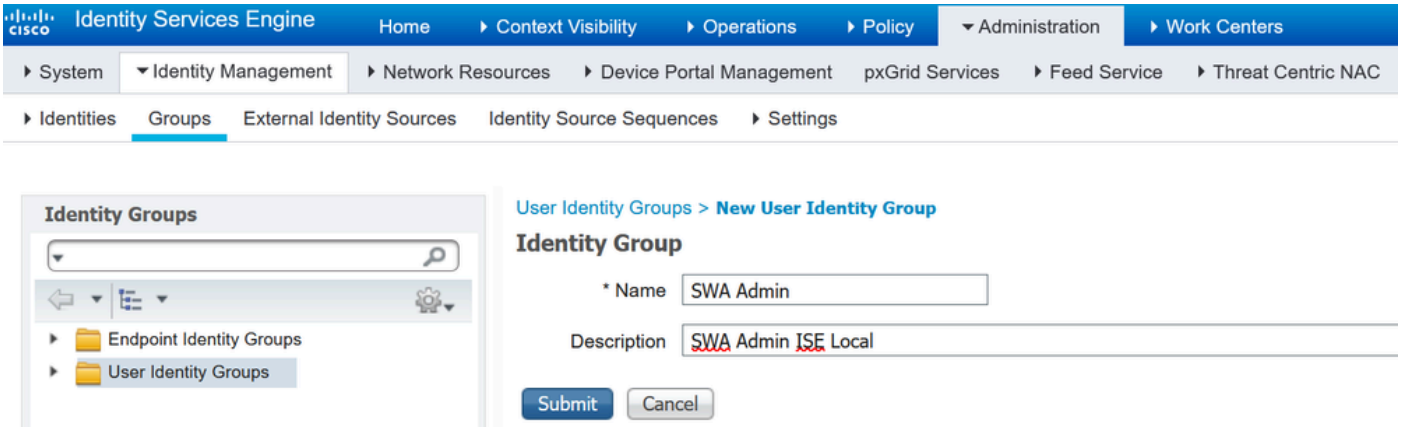
3.创建所需的用户身份组，然后导航到管理>身份管理>组>用户身份组> +Add。

注意：您必须配置不同的用户组以匹配不同类型的用户。

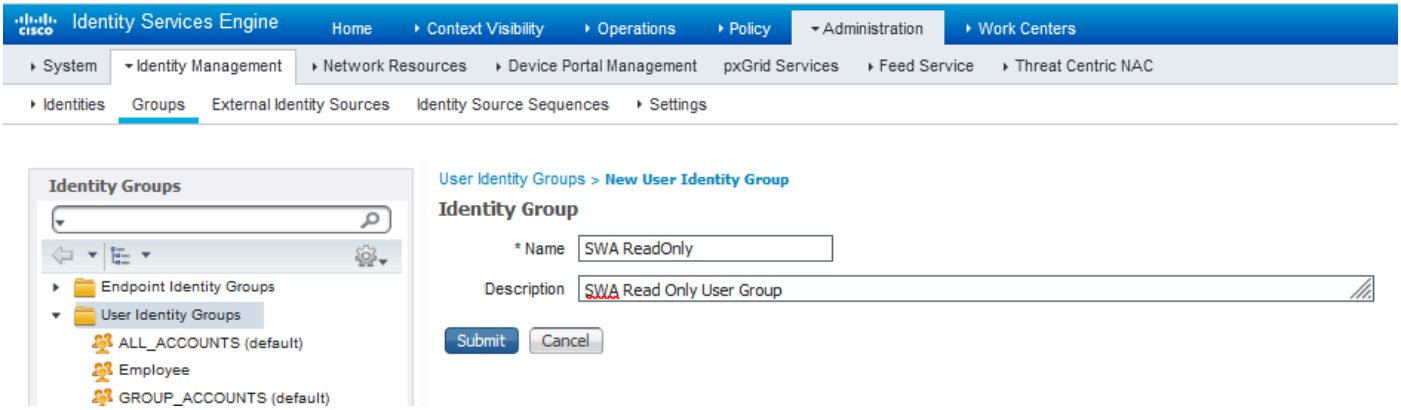


添加用户身份组

4.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，为管理员用户创建一个组，为只读用户创建一个组。



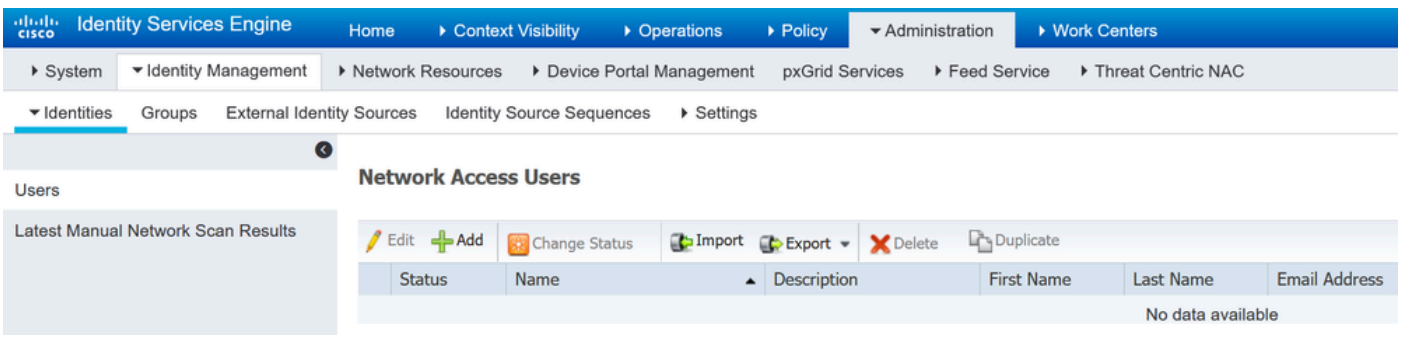
添加用户身份组



为SWA只读用户添加用户身份组

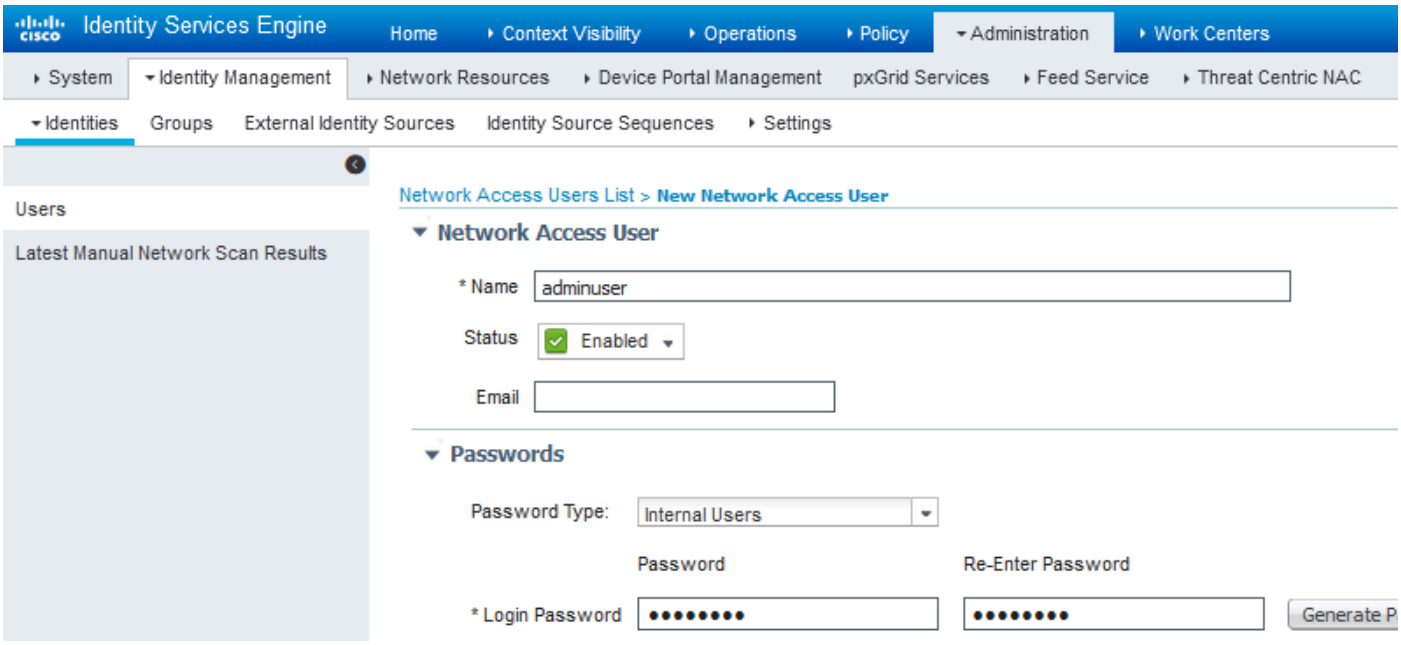
5.您必须创建与SWA中配置的用户名匹配的网络访问用户。

5.1.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> +添加。



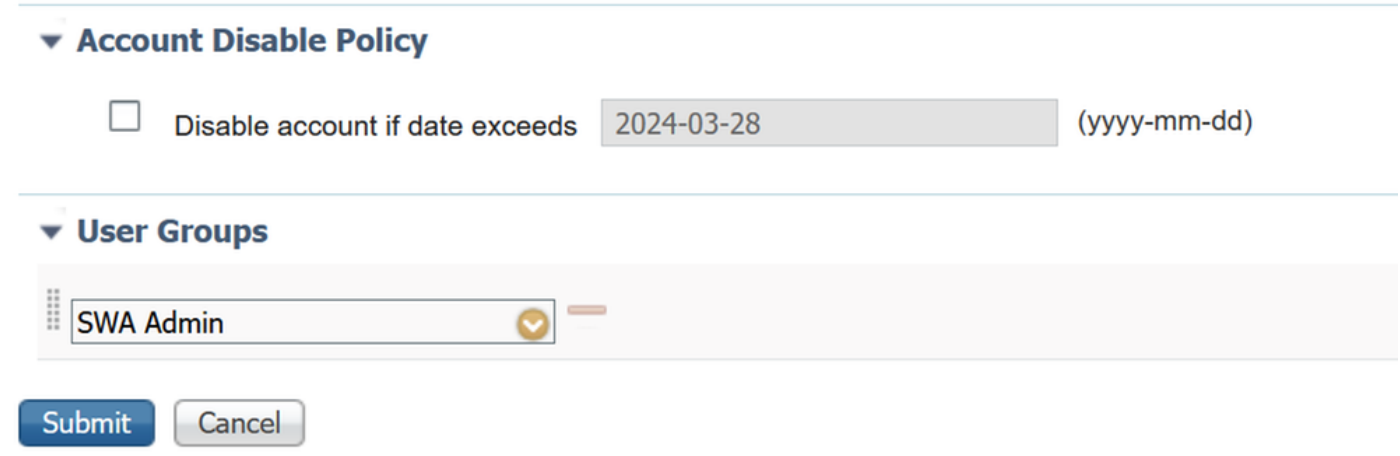
在ISE中添加本地用户

5.2.您必须创建具有管理员权限的网络访问用户，并分配名称和密码。



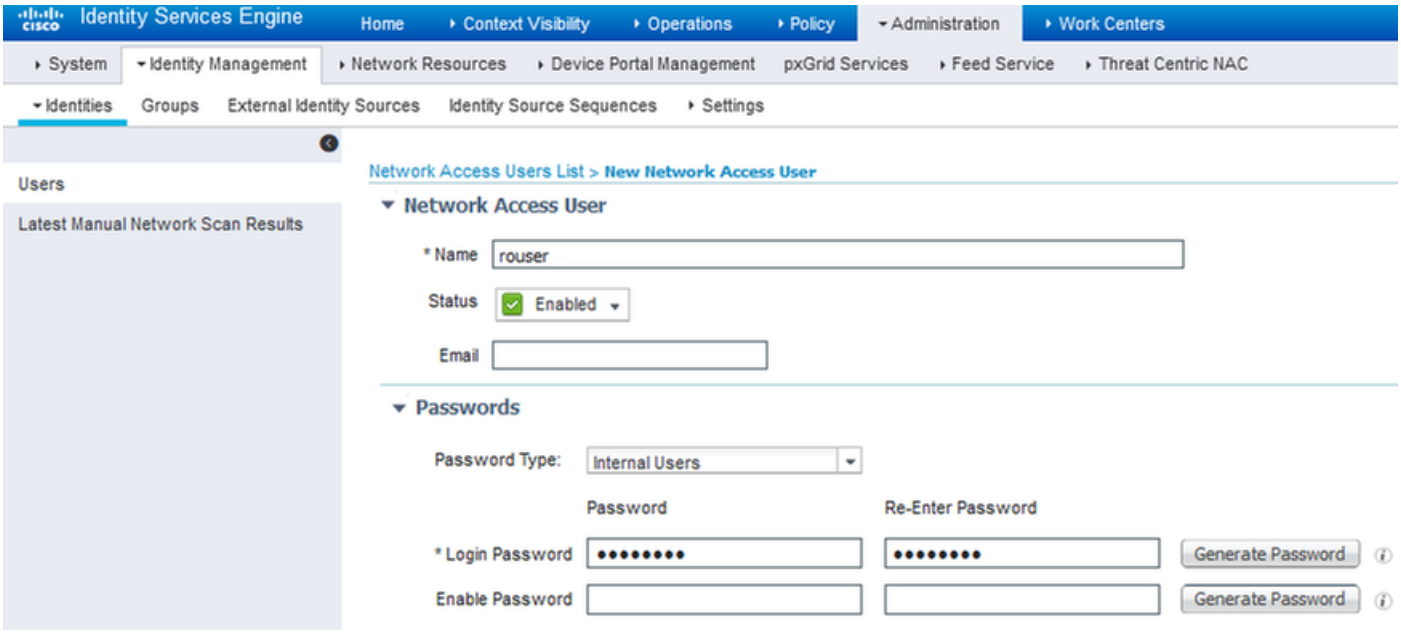
添加管理员用户

5.3.在用户组部分中选择SWA Admin。



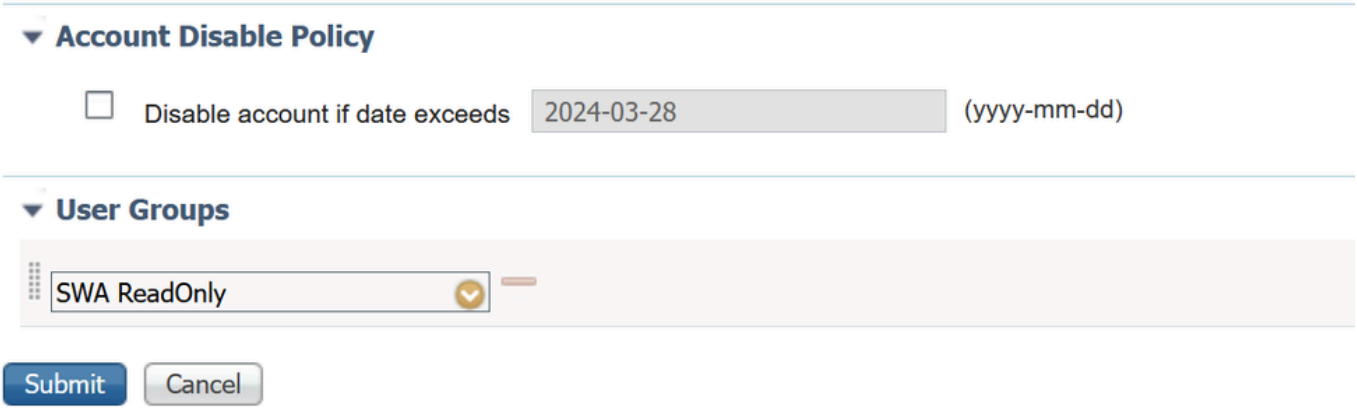
将管理员组分配给管理员用户

5.4.创建具有只读权限的用户，并分配名称和密码。



添加只读用户

5.5.在用户组部分中选择SWA ReadOnly。

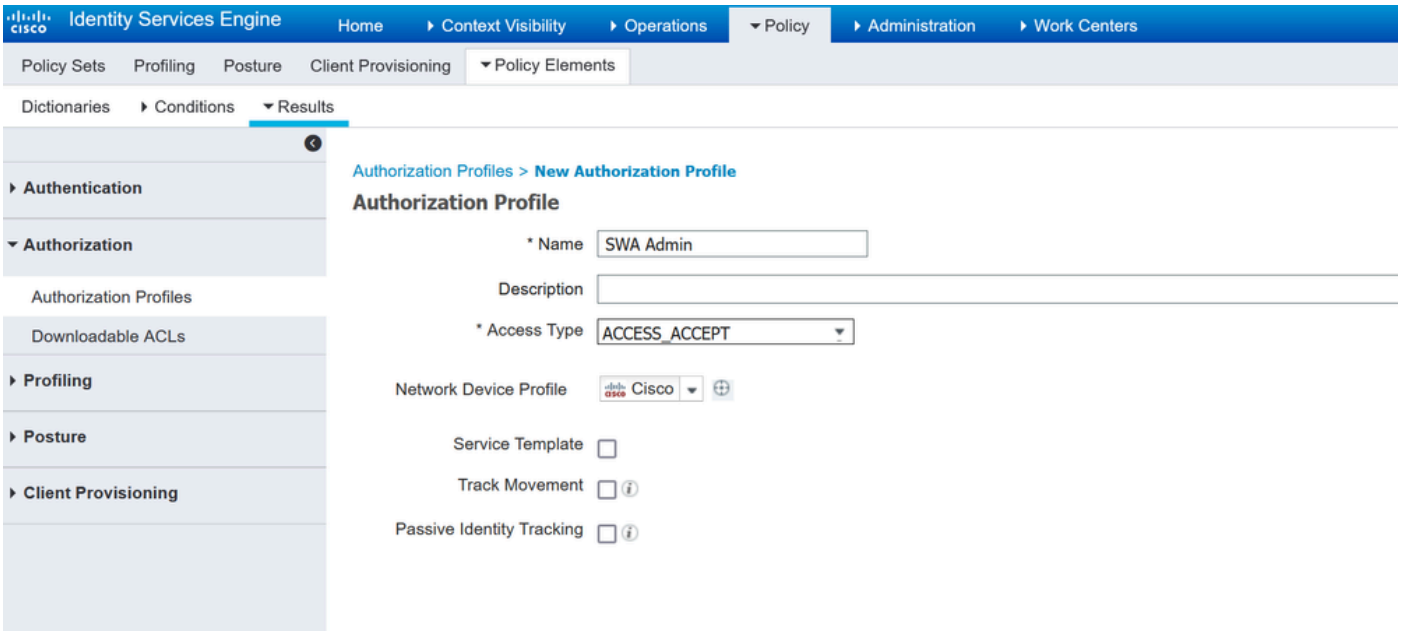


将只读用户组分配给只读用户

6.为管理员用户创建授权配置文件。

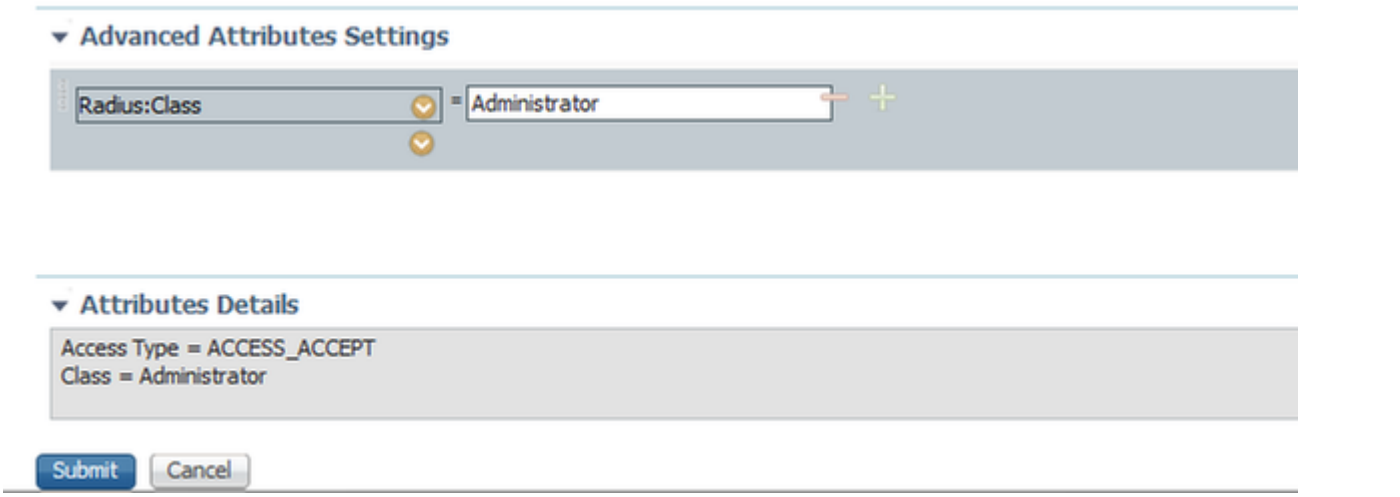
6.1.导航到策略>Policy元素>结果>授权>授权配置文件> +Add。

6.2.定义授权配置文件的名称，并确保访问类型设置为ACCESS_ACCEPT。



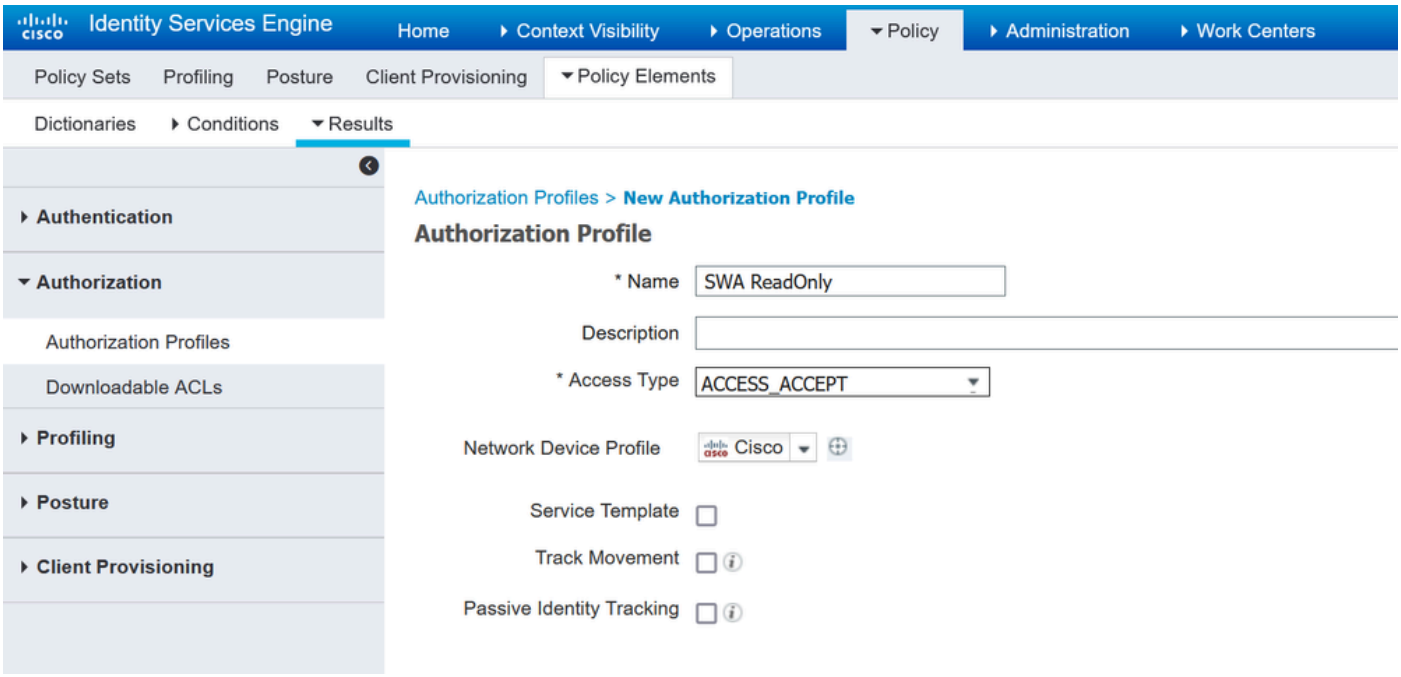
添加管理员用户的授权配置文件

6.3.在“高级属性设置”中，导航到Radius > Class—[25]，然后输入值Administrator，然后单击Submit。



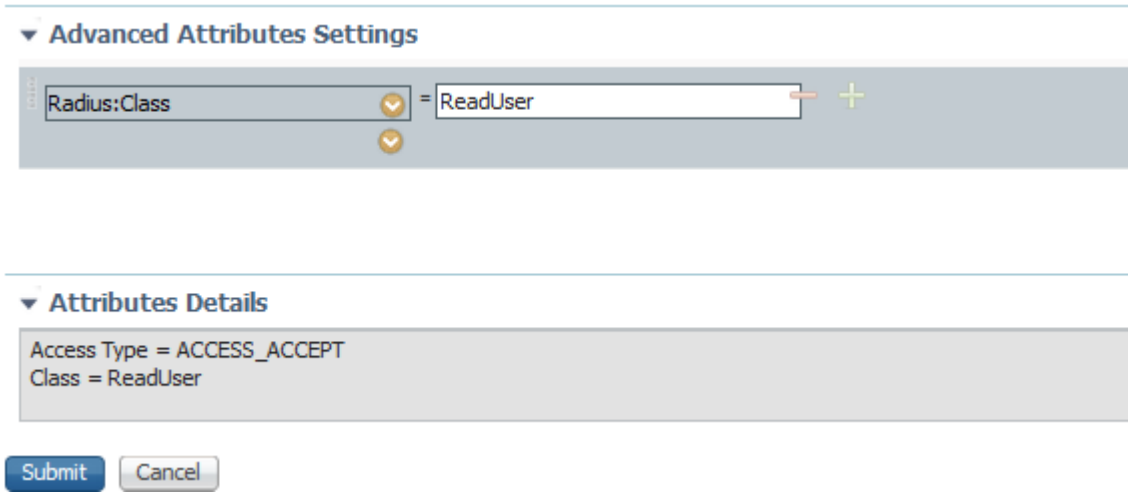
添加管理员用户的授权配置文件

7.重复步骤6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

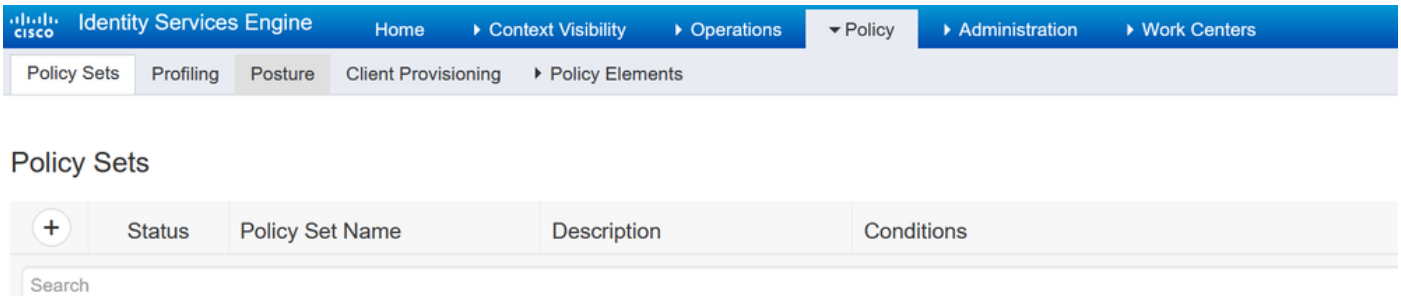
7.1.使用ReadUser而不是Administrator值创建Radius:Class。



为只读用户添加授权配置文件

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。

8.1.导航到Policy > Policy Sets，然后单击位于左上角的+图标。

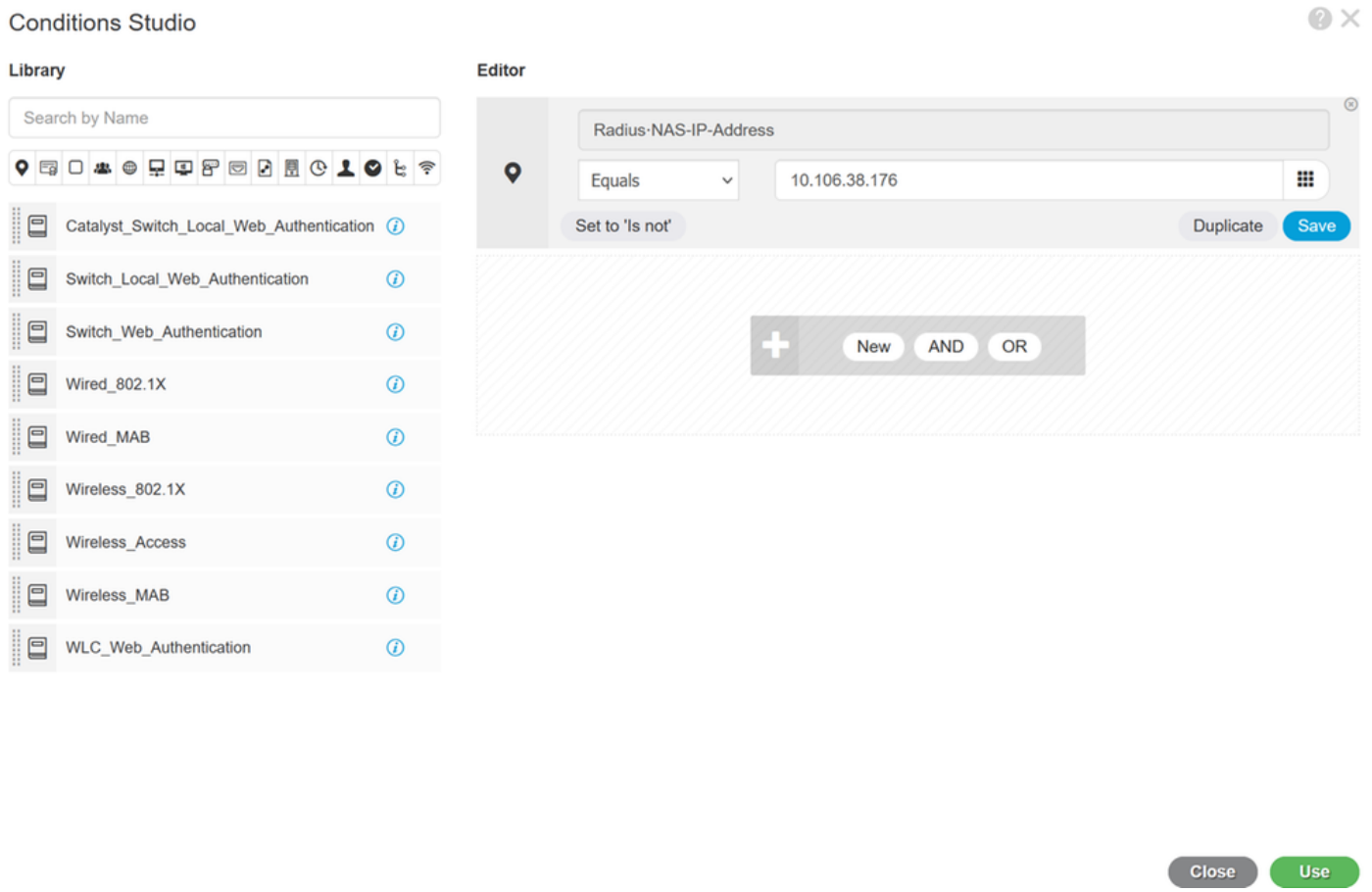


在ISE中添加策略集

8.2.新行位于策略集的顶部。

8.3.输入新策略的名称，并为RADIUS NAS-IP-Address属性添加条件以匹配SWA IP地址。

8.4.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

8.5.单击Save。



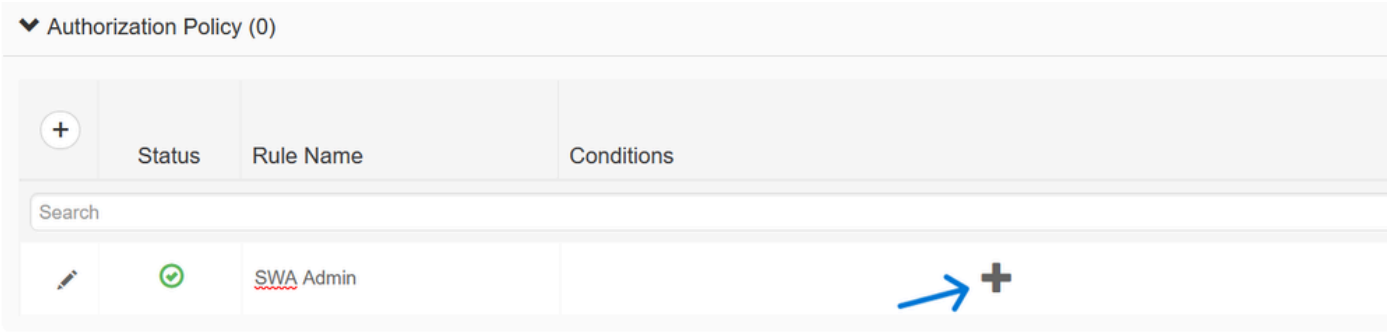
策略保存

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

9.要查看新的策略集，请单击查看列中的>图标。展开Authorization Policy菜单，然后单击+ 图标以添加新的规则，以允许访问具有管理员权限的用户。

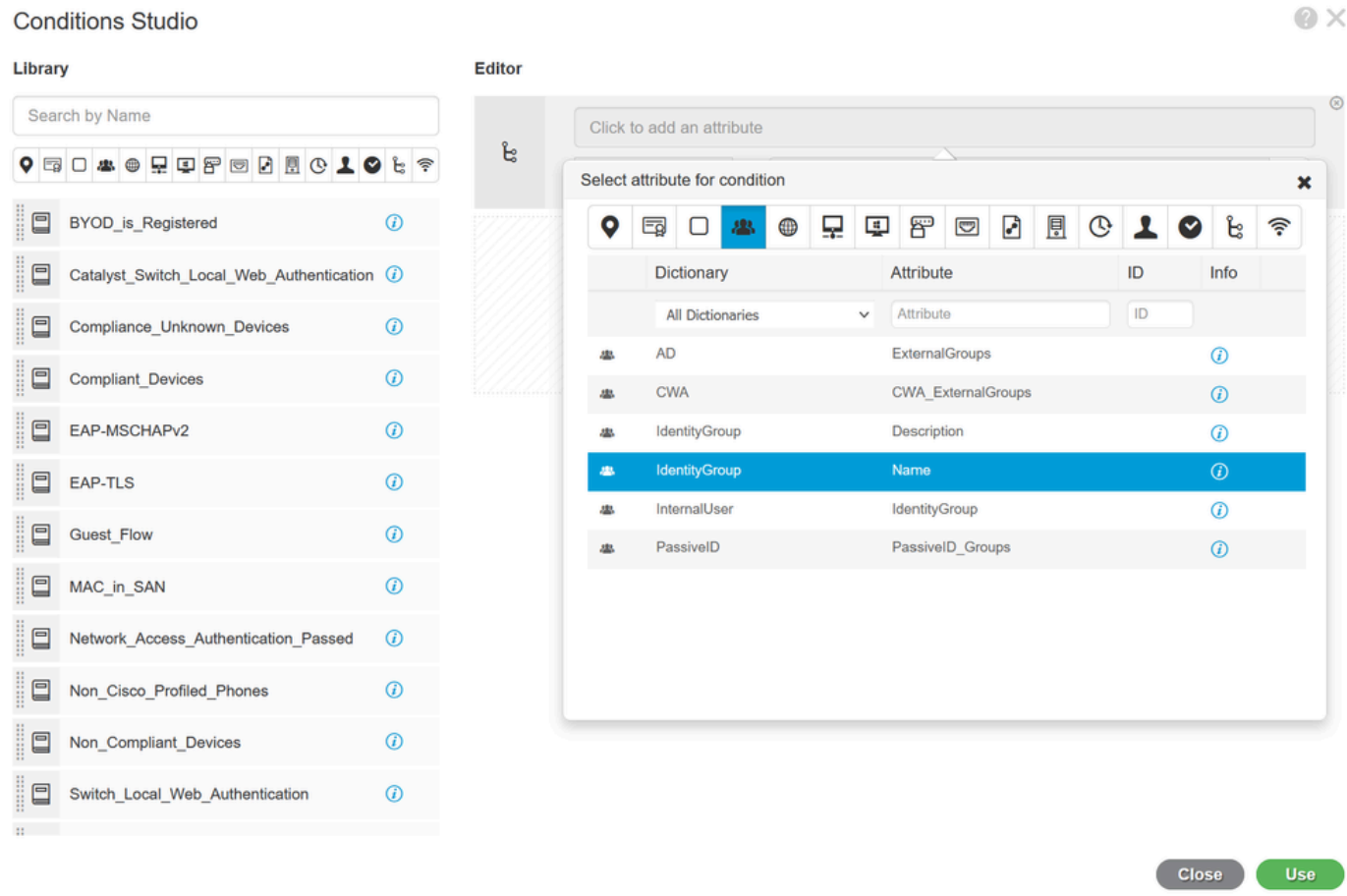
9.1.输入名称。

9.2.要创建匹配管理员用户组的条件，请点击+图标。



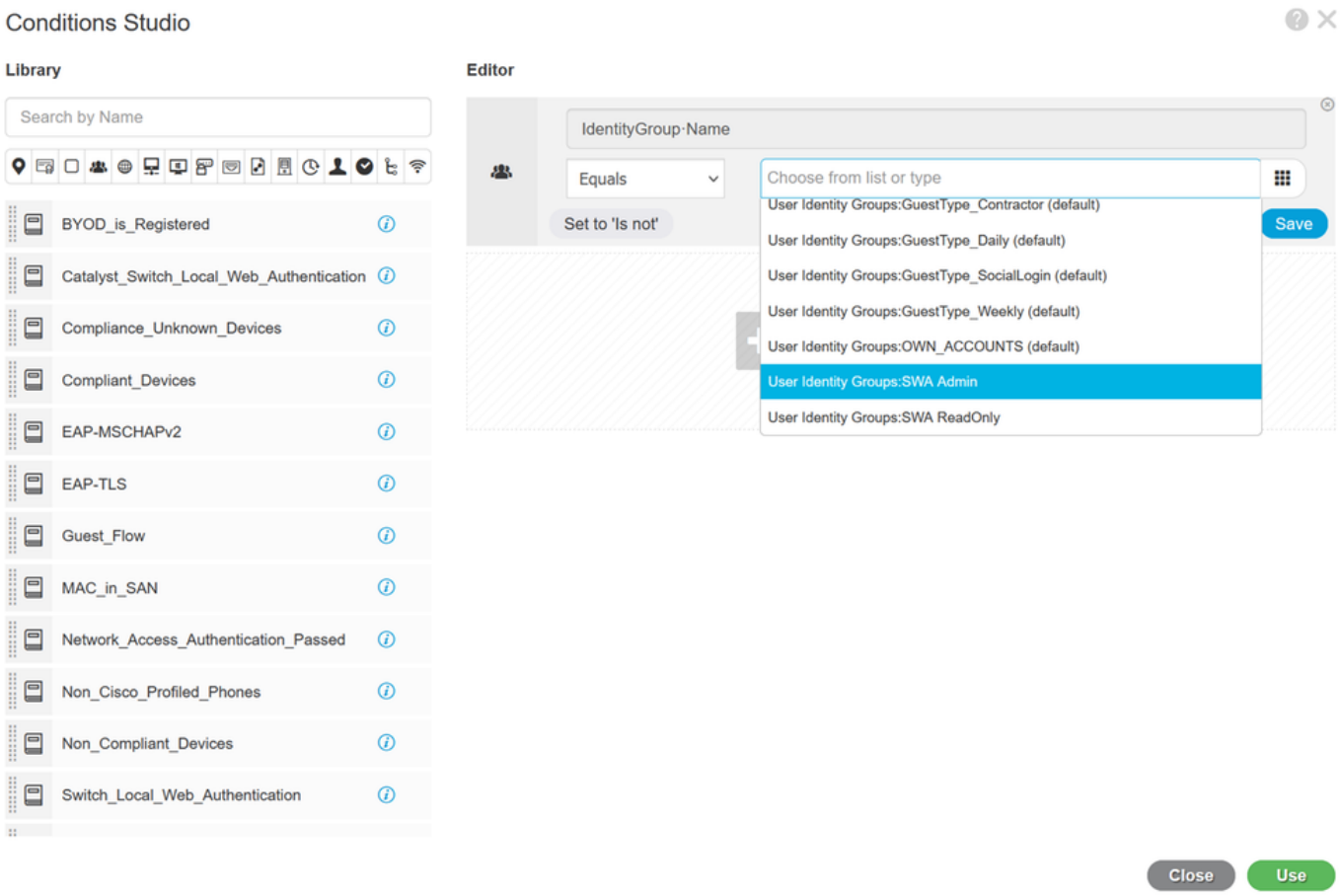
添加授权策略条件

9.3.设置条件以匹配Dictionary Identity Group与Attribute Name Equals User Identity Groups:SWA管理员



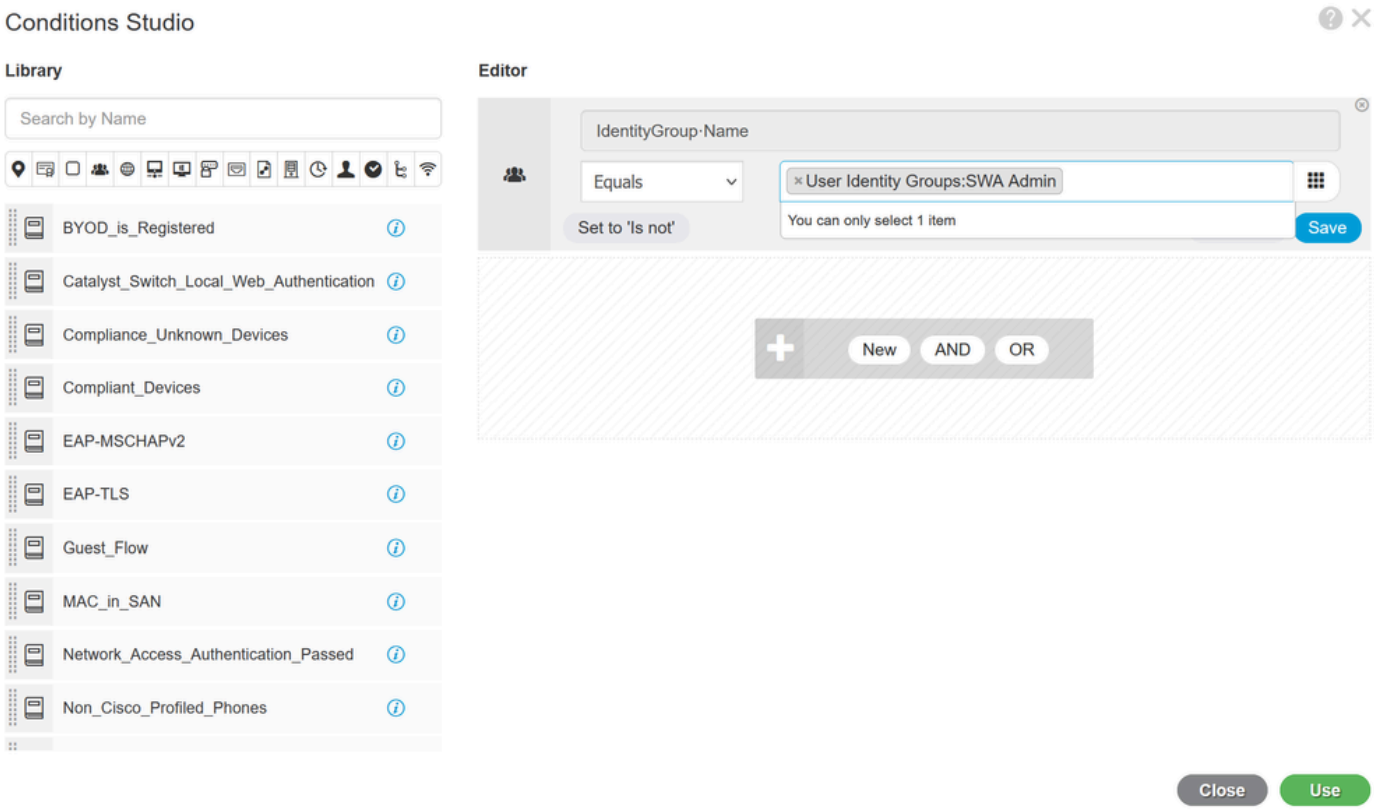
选择身份组作为条件

9.4.向下滚动并选择User Identity Groups:SWA管理员



向下滚动Select Identity Group Name

9.5.单击Use。

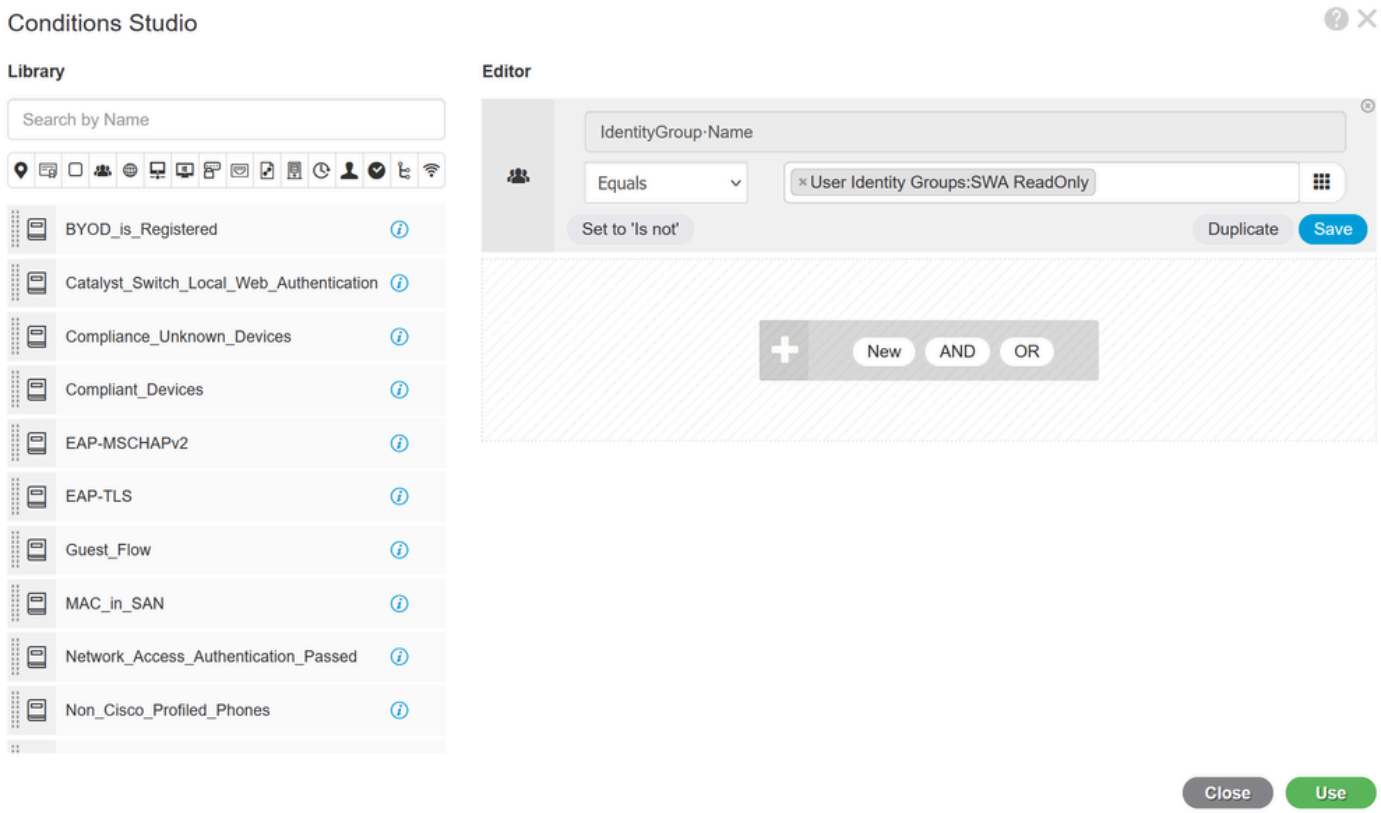


为SWA管理员用户组选择授权策略

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。

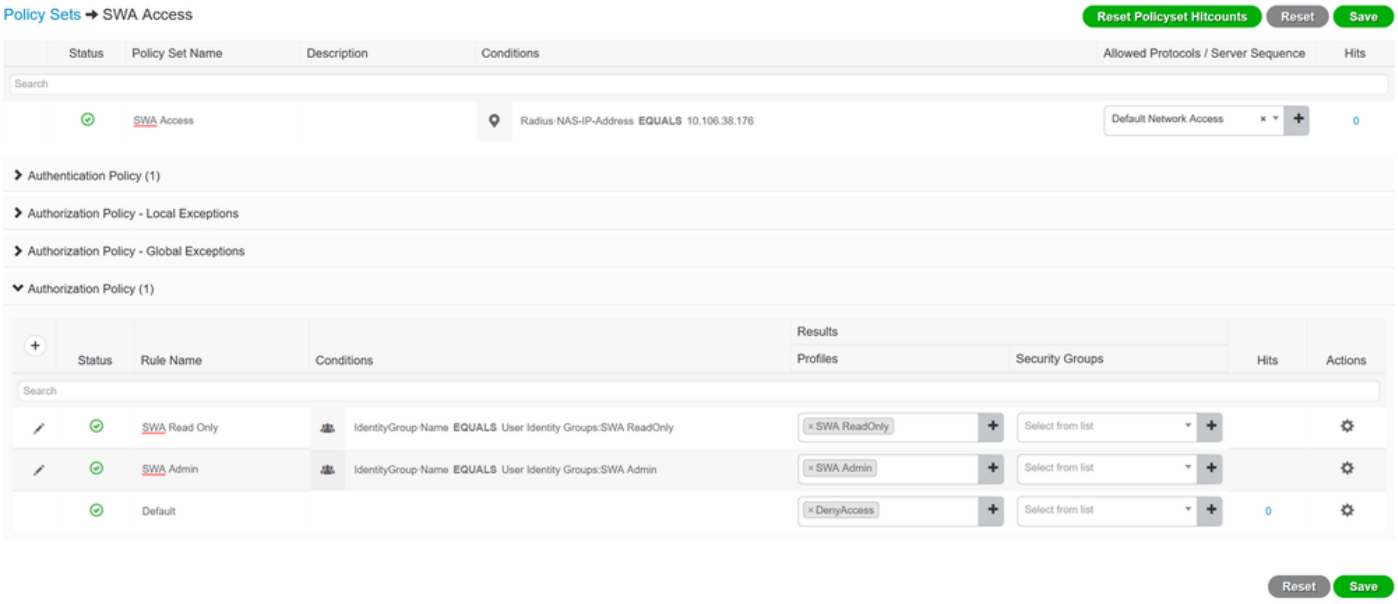
10.1.输入名称。

10.2.设置条件以匹配Dictionary Identity Group with Attribute Name Equals User Identity Groups:SWA只读，然后单击Use。



选择只读用户组的授权策略

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

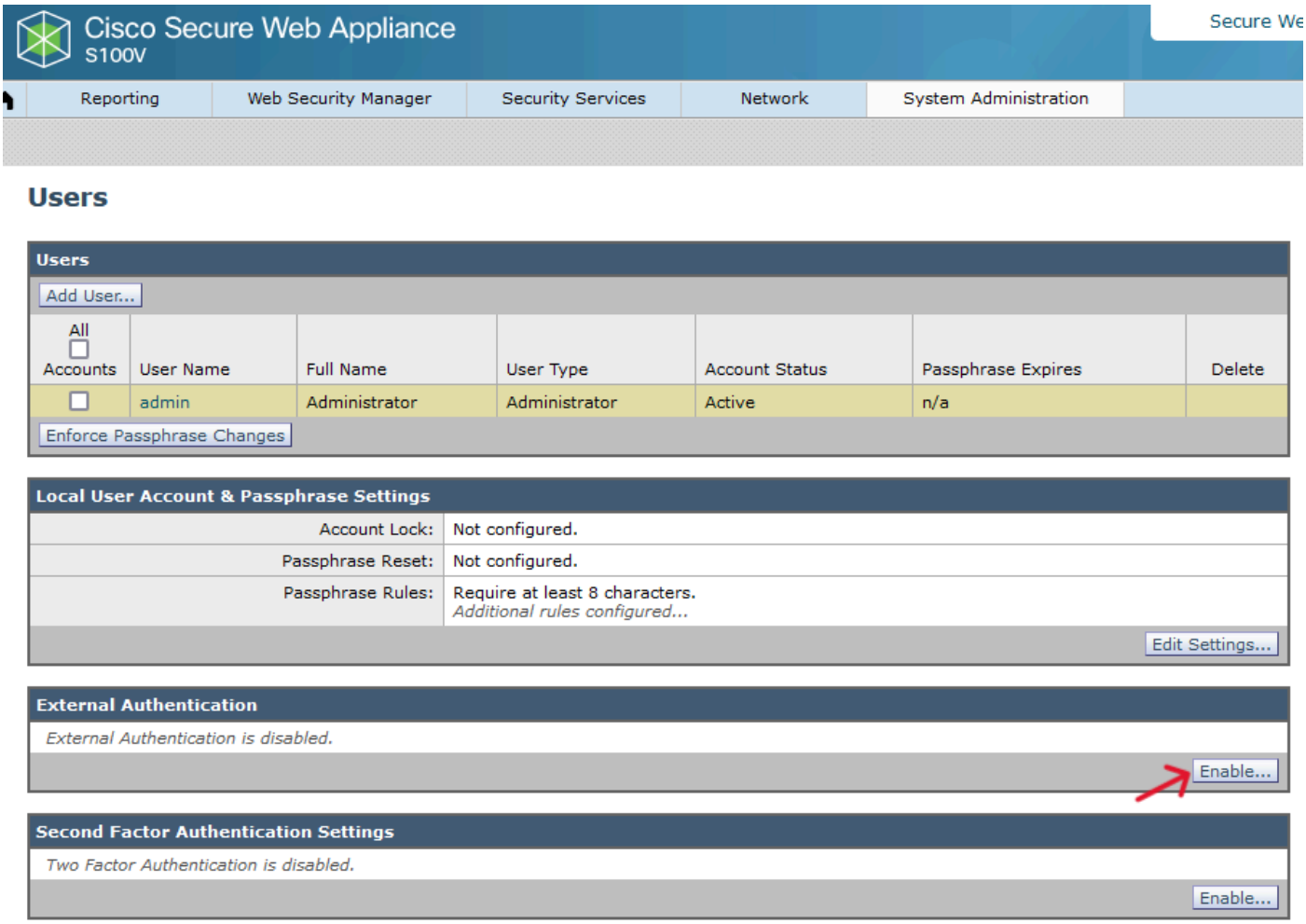


选择授权配置文件

SWA配置

1.从SWA GUI中选择系统管理，然后选择用户。

2.单击外部身份验证中的启用。



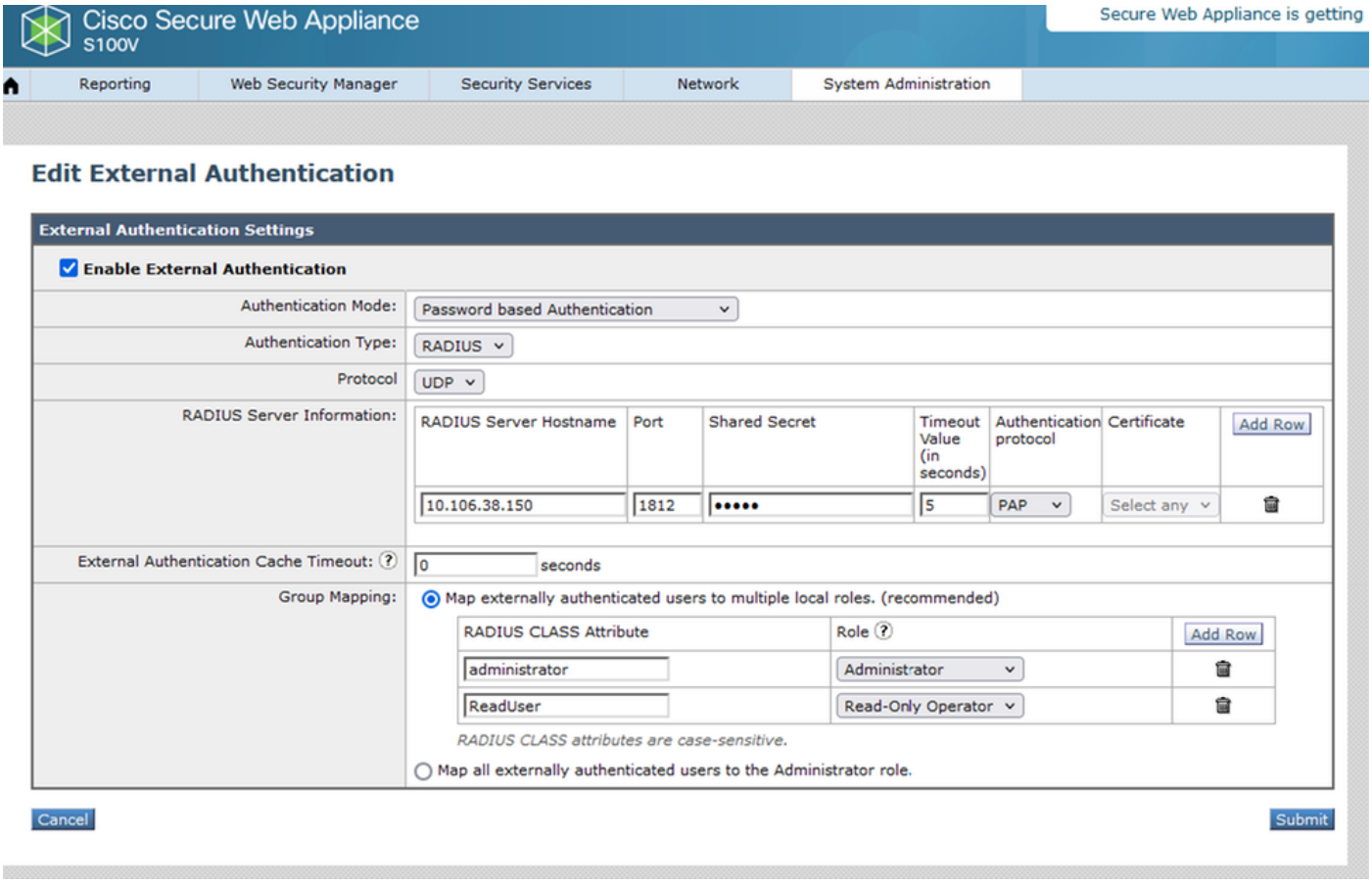
在SWA中启用外部身份验证

3.在RADIUS Server Hostname字段中输入ISE的IP地址或完全限定域名(FQDN)，并输入Shared Secret与Step 2的ISE配置中配置的相同。

4.选择在组映射中将外部身份验证的用户映射到多个本地角色。

4.1.在RADIUS CLASS Attribute字段中输入Administrator，然后选择Role Administrator。

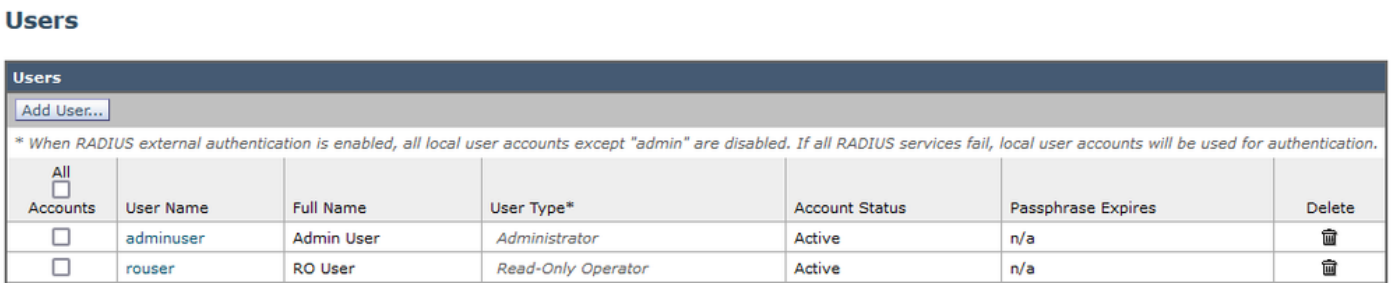
4.2.在RADIUS CLASS Attribute字段中输入ReadUser，然后选择Role Read-Only Operator。



RADIUS服务器的外部身份验证配置

5.要在SWA中配置用户，请单击Add User。输入User Name并选择User Type，这是所需角色所必需的。如果设备无法连接到任何外部RADIUS服务器，请输入Passphrase和Retype Passphrase，这是GUI访问所必需的。

注意：如果设备无法连接到任何外部服务器，则会尝试将用户作为在安全Web设备上定义的本地用户进行身份验证。

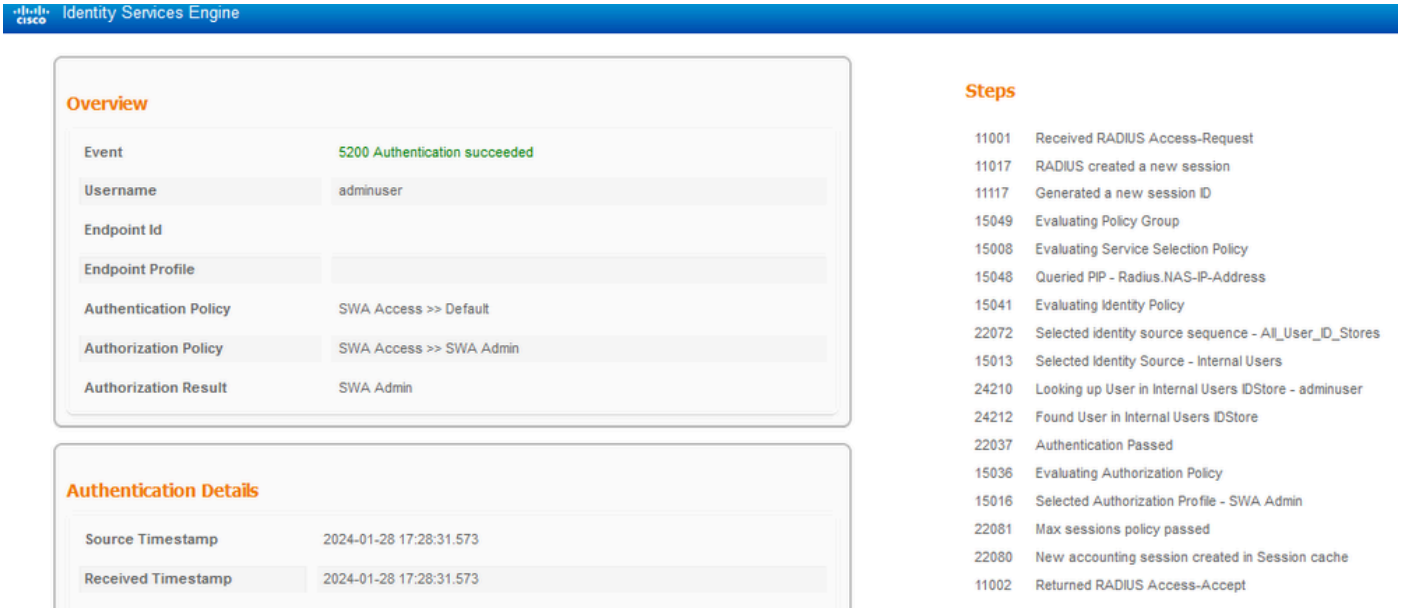


SWA中的用户配置

6.单击Submit和Commit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

相关内容

- 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兼容性矩阵
- 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）。