将SWA第二因素身份验证配置为ISE作为RADIUS服务器

目录

简介

本文档介绍如何在以Cisco身份服务引擎作为RADIUS服务器的安全Web设备上配置第二因素身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- SWA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：

- 安全网络设备(SWA)和思科身份服务引擎(ISE)管理访问。
- 您的ISE已集成到Active Directory或LDAP。
- Active Directory或LDAP配置为使用用户名“admin”对SWA默认“admin”帐户进行身份验证。
- 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

当您在SWA上为管理用户启用第二因素身份验证时，设备会在验证SWA中配置的凭证后第二次使用RADIUS服务器验证用户凭证。

网络拓扑

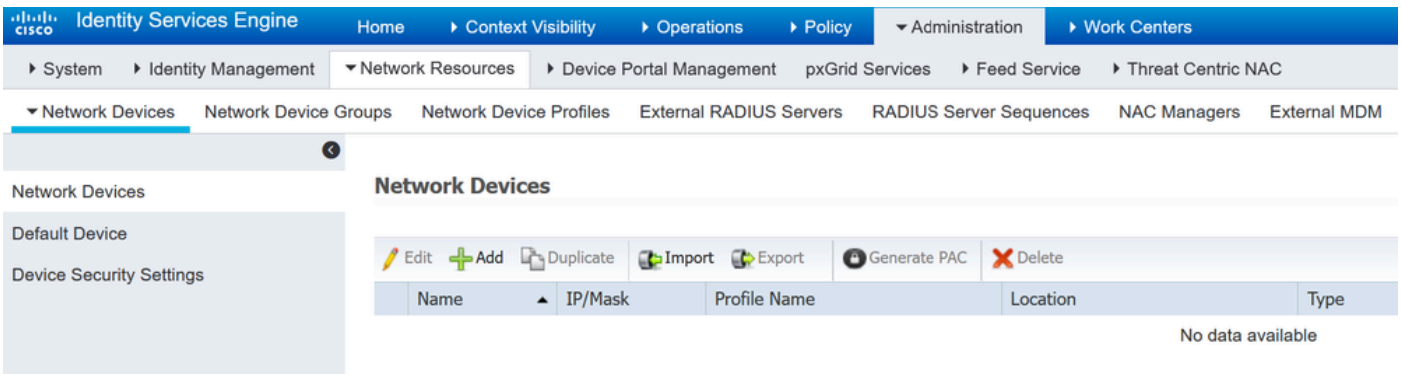
图像-网络拓扑图

管理用户使用其凭证访问端口443上的SWA。SWA验证与RADIUS服务器的凭证以进行第二次因子身份验证。

配置步骤

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

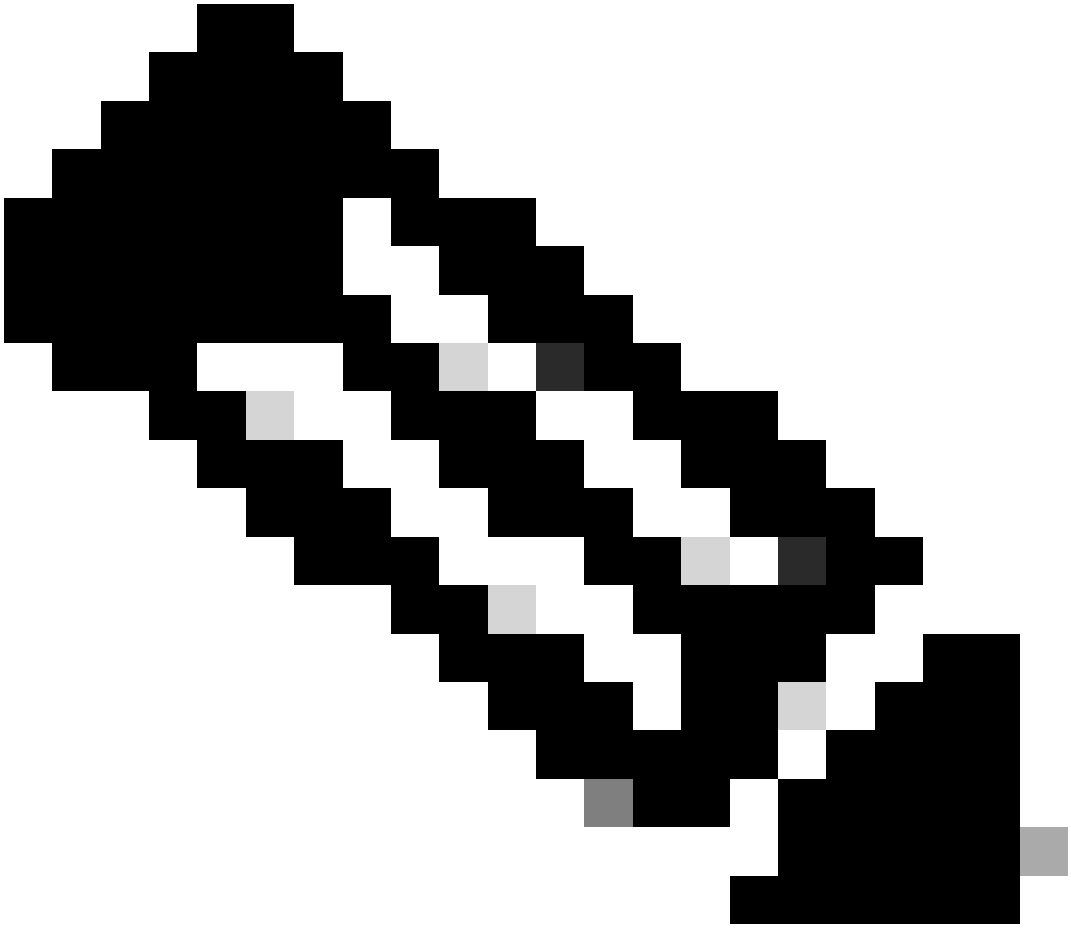
第二步：在ISE中配置网络设备。

步骤 2.1为网络设备对象指定Name。

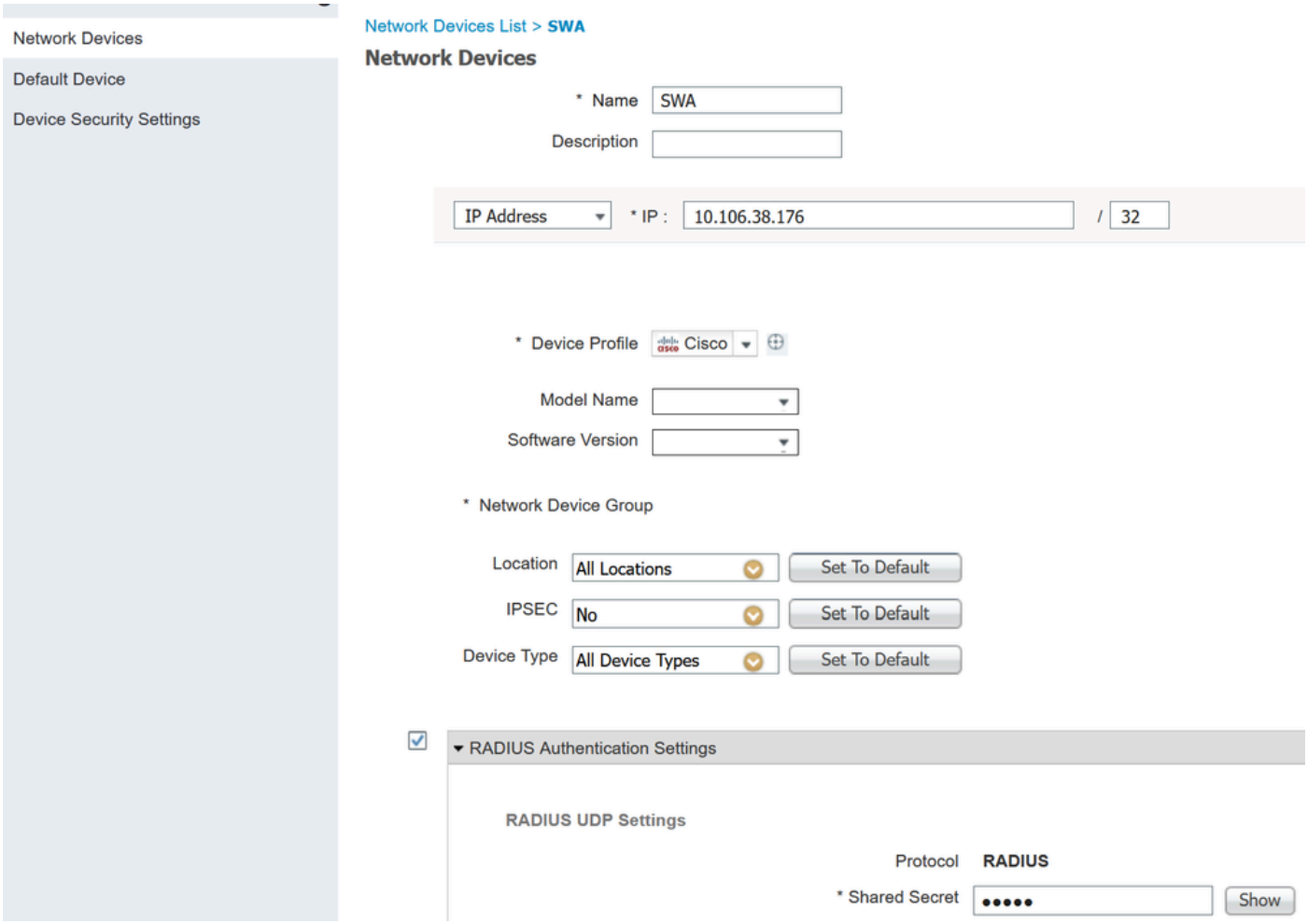
步骤 2.2插入SWA IP地址。

步骤 2.3选中RADIUS复选框。

步骤 2.4定义共享密钥。

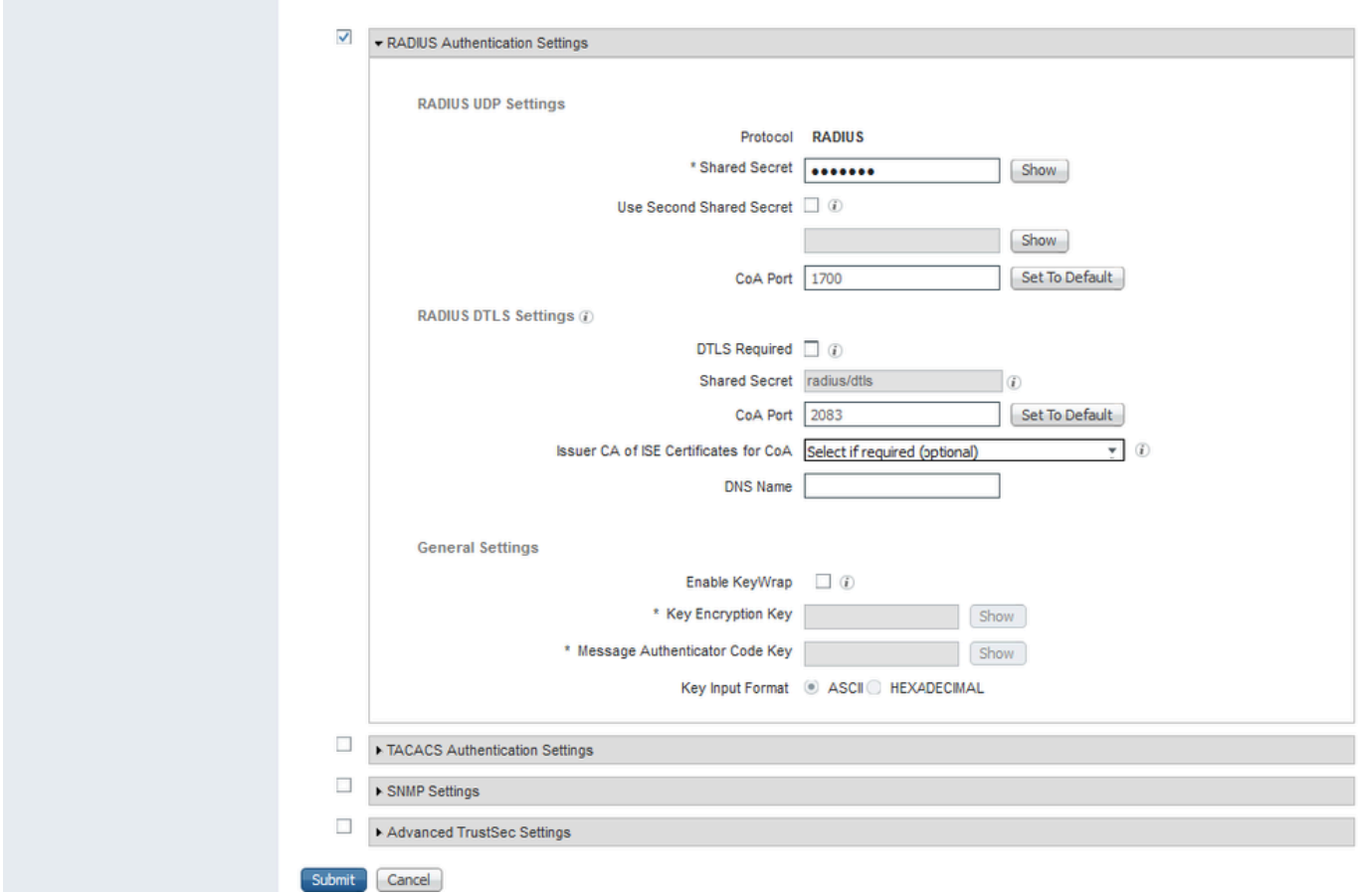


注意：稍后必须使用相同的密钥来配置SWA。



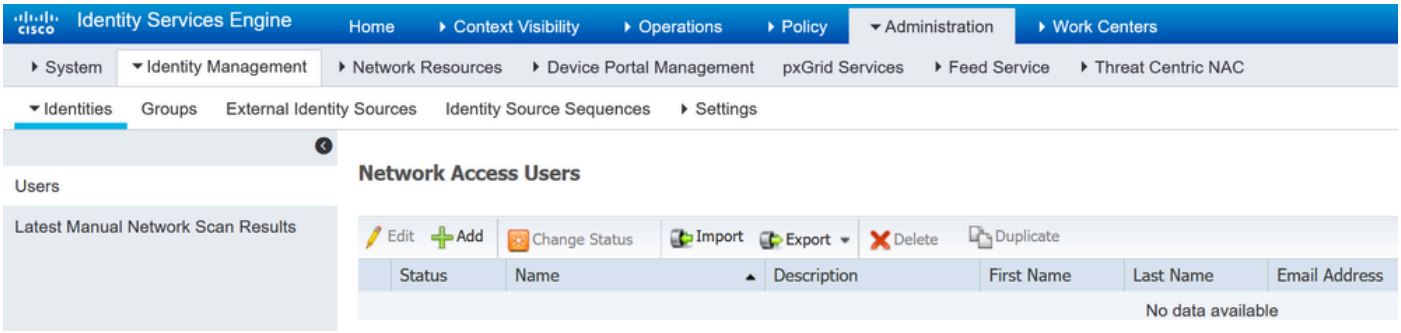
配置SWA网络设备共享密钥

步骤 2.5单击“Submit”。



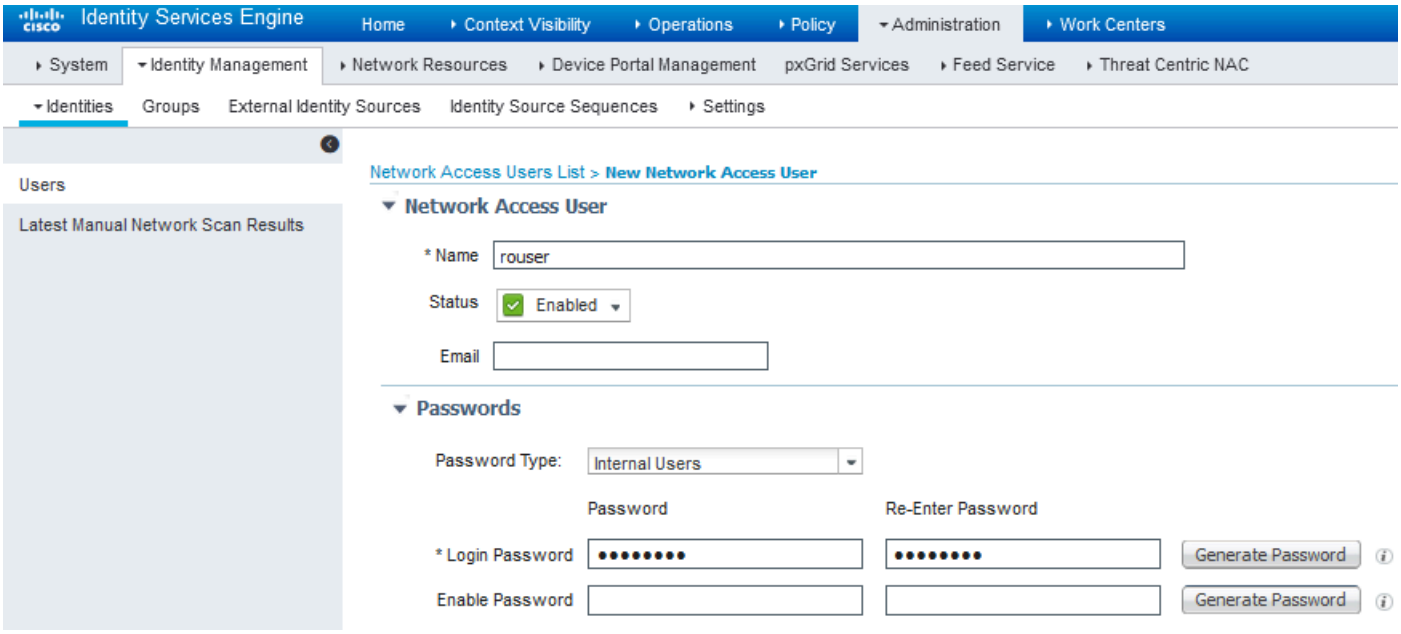
提交网络设备配置

第三步：您需要创建与SWA中配置的用户名匹配的网络访问用户。导航到管理>身份管理>身份> + Add。



在ISE中添加本地用户

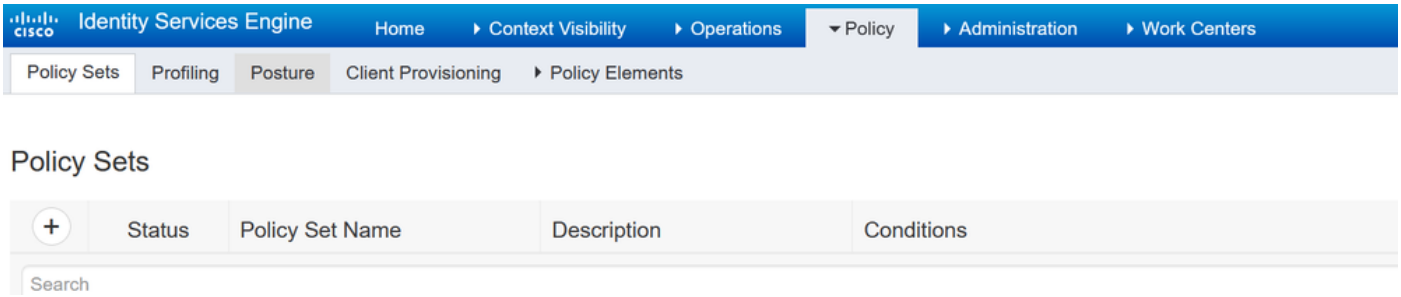
步骤 3.1指定Name。
第3.2步（可选）输入用户的邮件地址。
步骤 3.3设置密码.
步骤 3.4Click Save.



在ISE中添加本地用户

第四步：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。

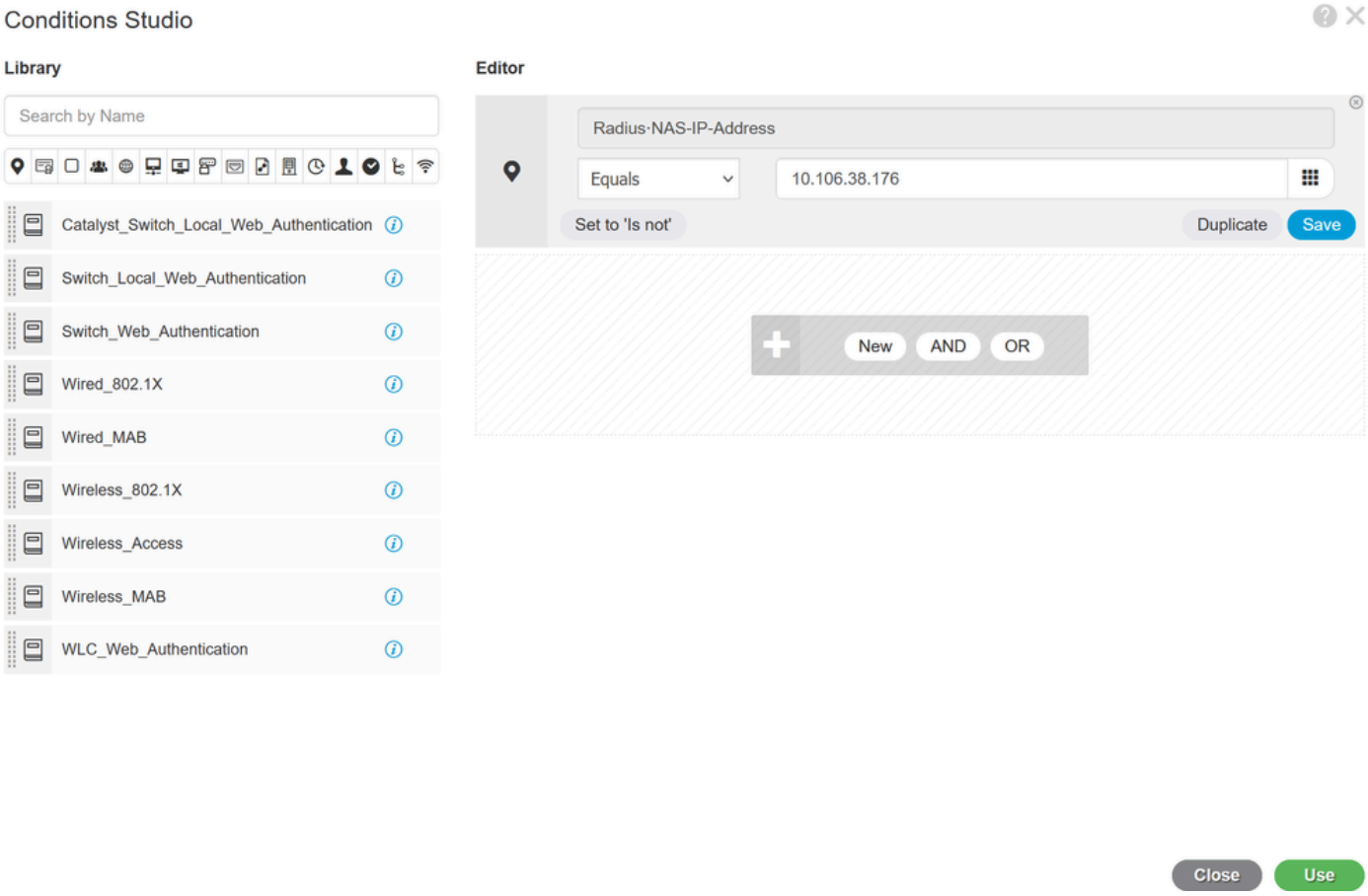


在ISE中添加策略集

步骤 4.1 新行位于策略集的顶部。输入新策略的名称。

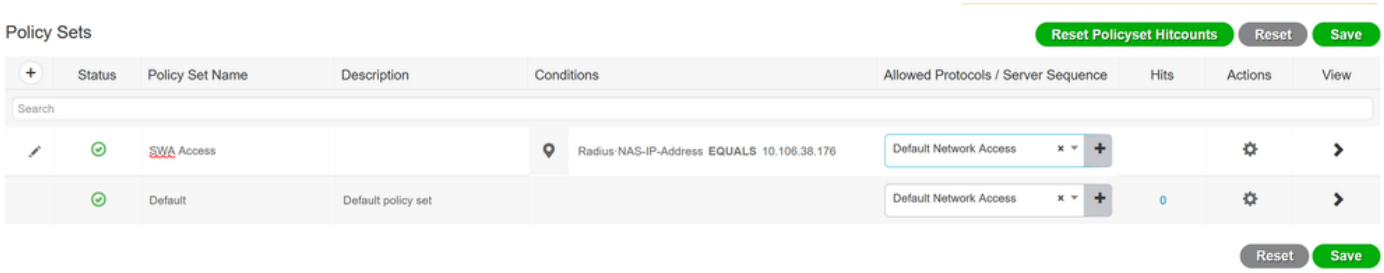
步骤 4.2为RADIUS NAS-IP-Address属性添加一个条件以匹配SWA IP地址。

步骤 4.3单击Use以保留更改并退出编辑器。

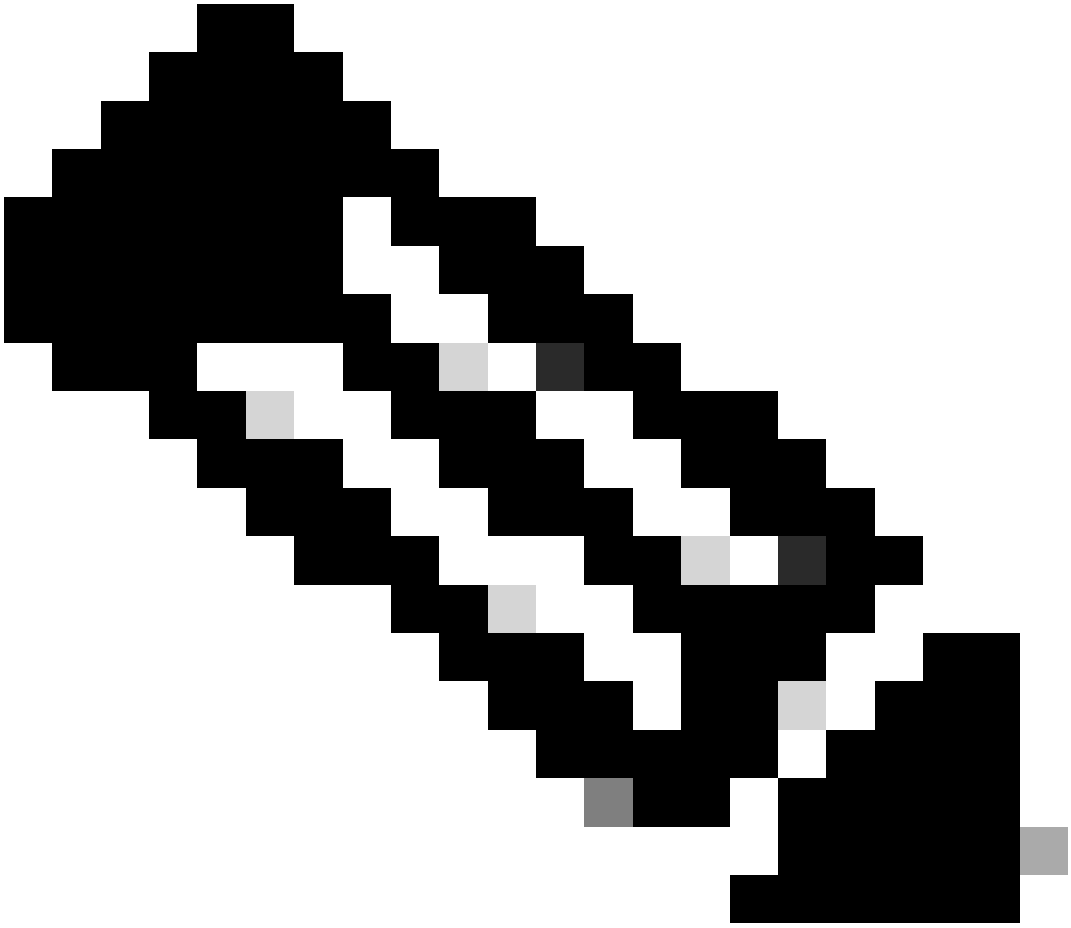


添加策略以映射SWA网络设备

步骤 4.4Click Save.



策略保存



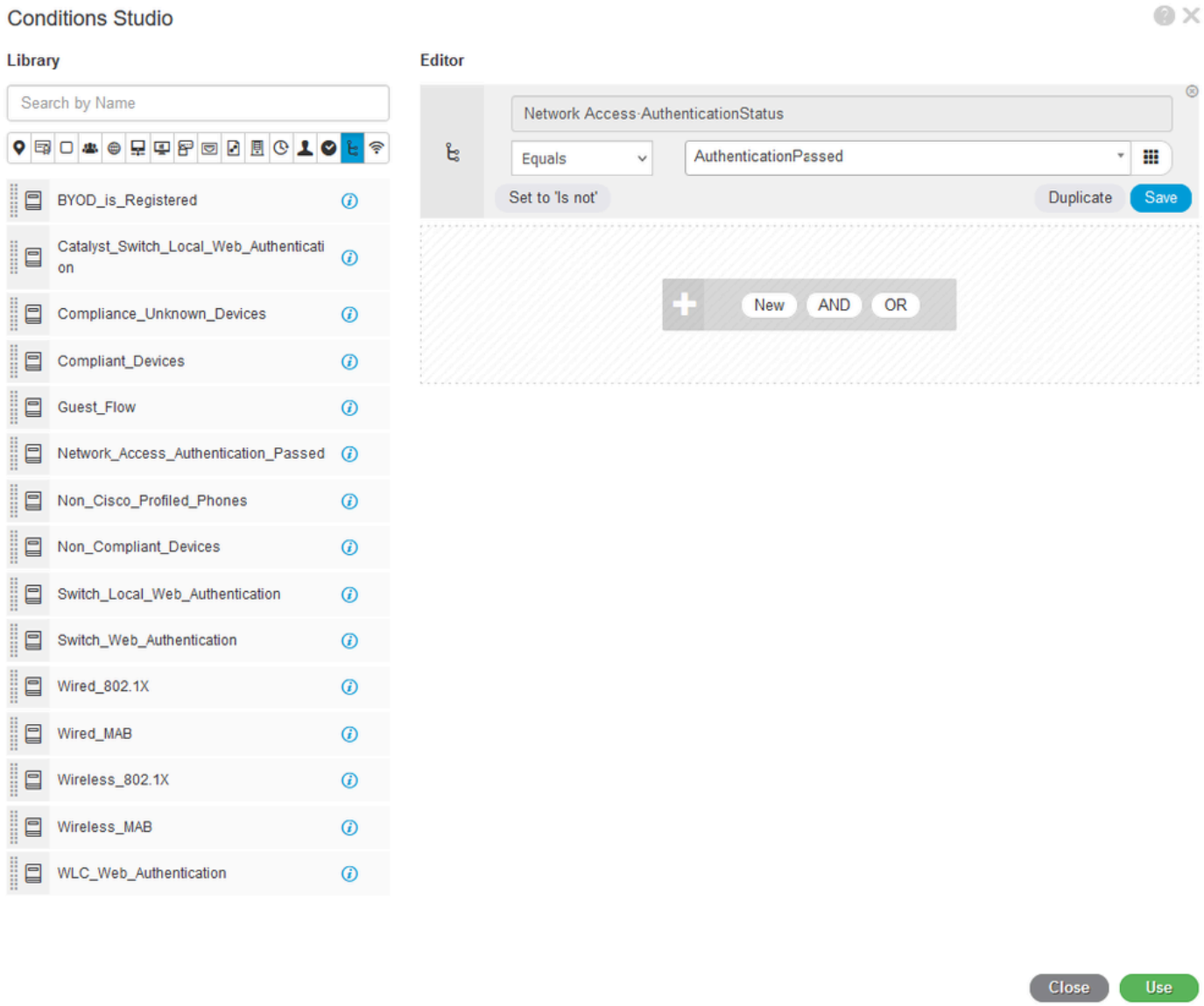
注意：本示例允许使用默认网络访问协议列表。您可以创建一个新列表并根据需要缩小其范围。

第五步：要查看新的策略集，请点击查看列中的“>”图标。

步骤 5.1展开Authorization Policy菜单，然后单击+图标以添加新规则，从而允许所有通过身份验证的用户进行访问。

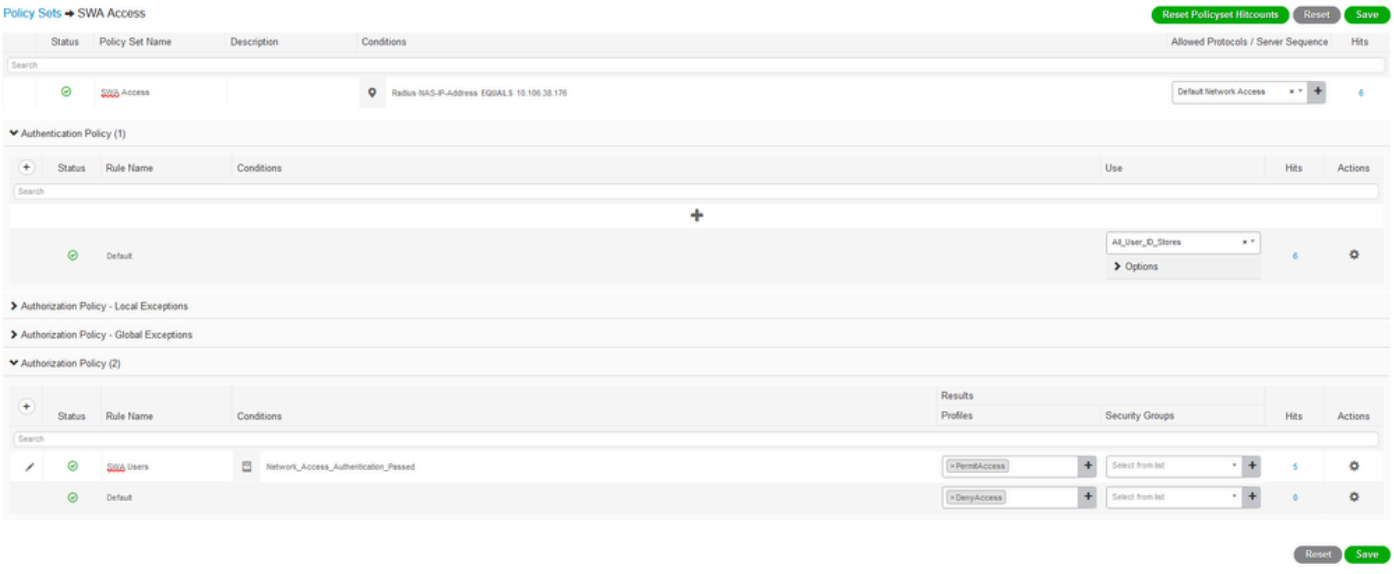
步骤 5.2设置名称。

步骤 5.3设置条件以匹配Dictionary Network Access和属性AuthenticationStatus Equals AuthenticationPassed，然后单击Use。



选择授权条件

第六步： 将默认PermitAccess设置为授权配置文件，并单击Save。

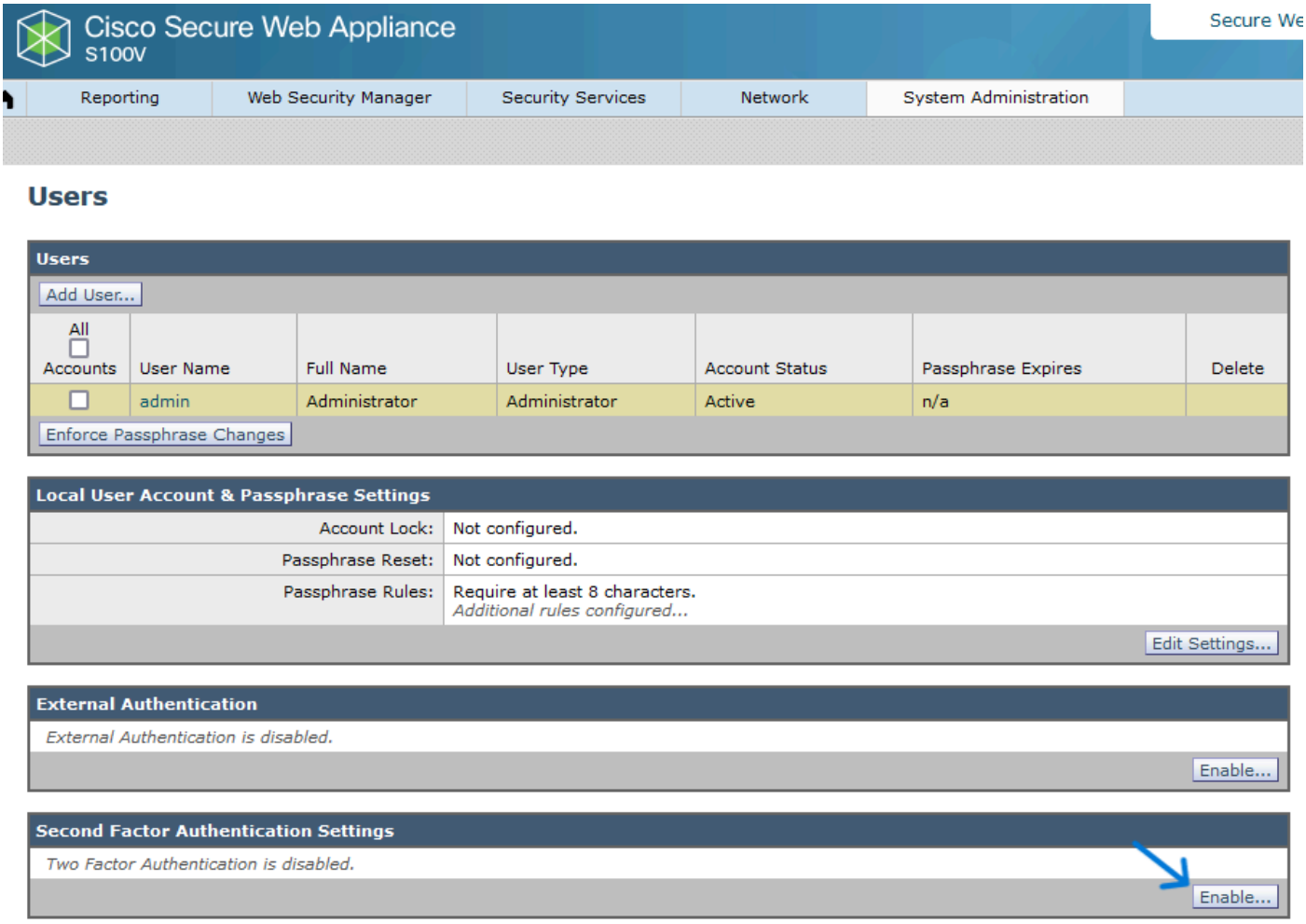


选择授权配置文件

SWA配置

步骤1:从SWA GUI导航至系统管理，然后点击用户。

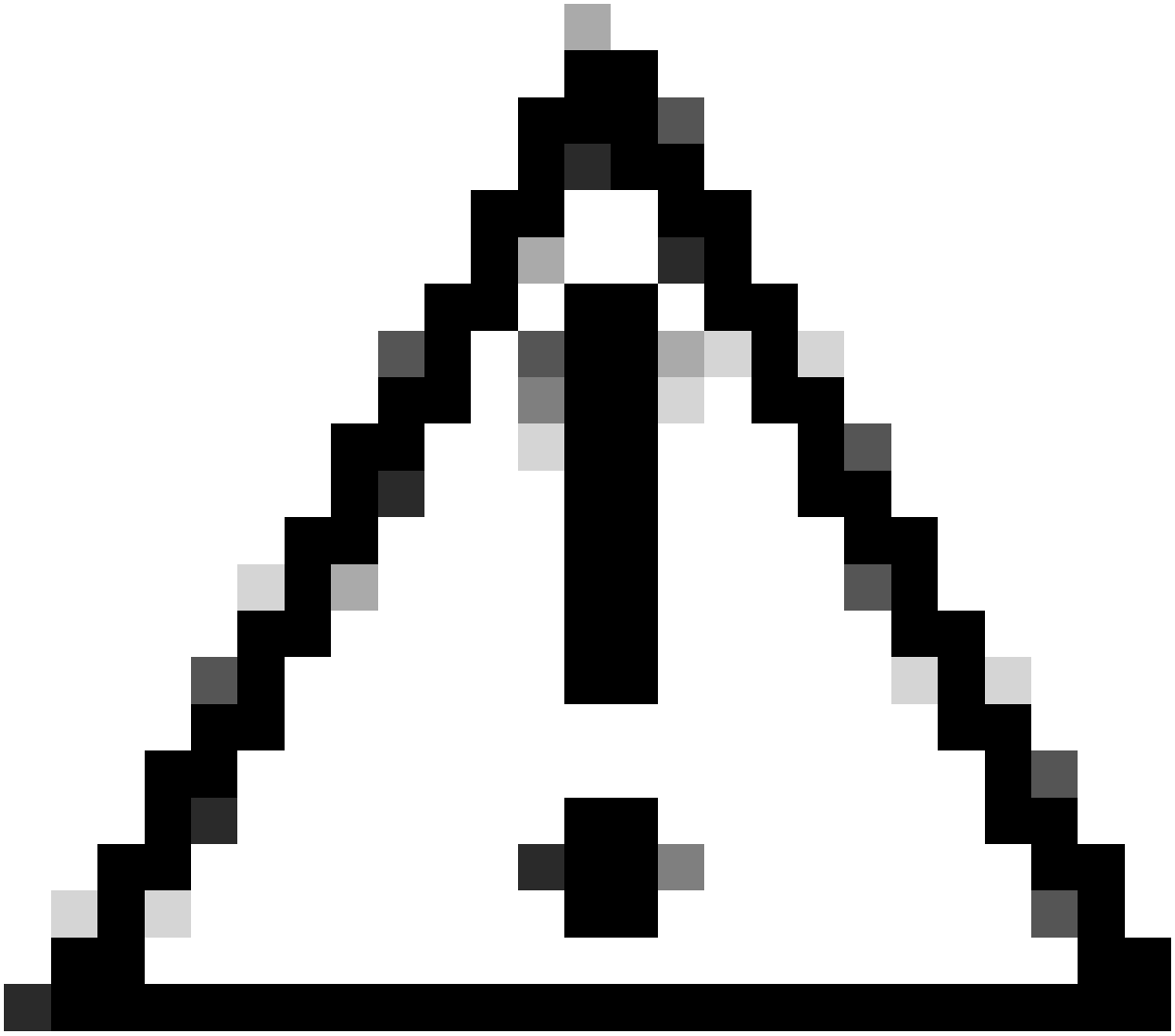
第二步：在Second Factor Authentication Settings中单击Enable。



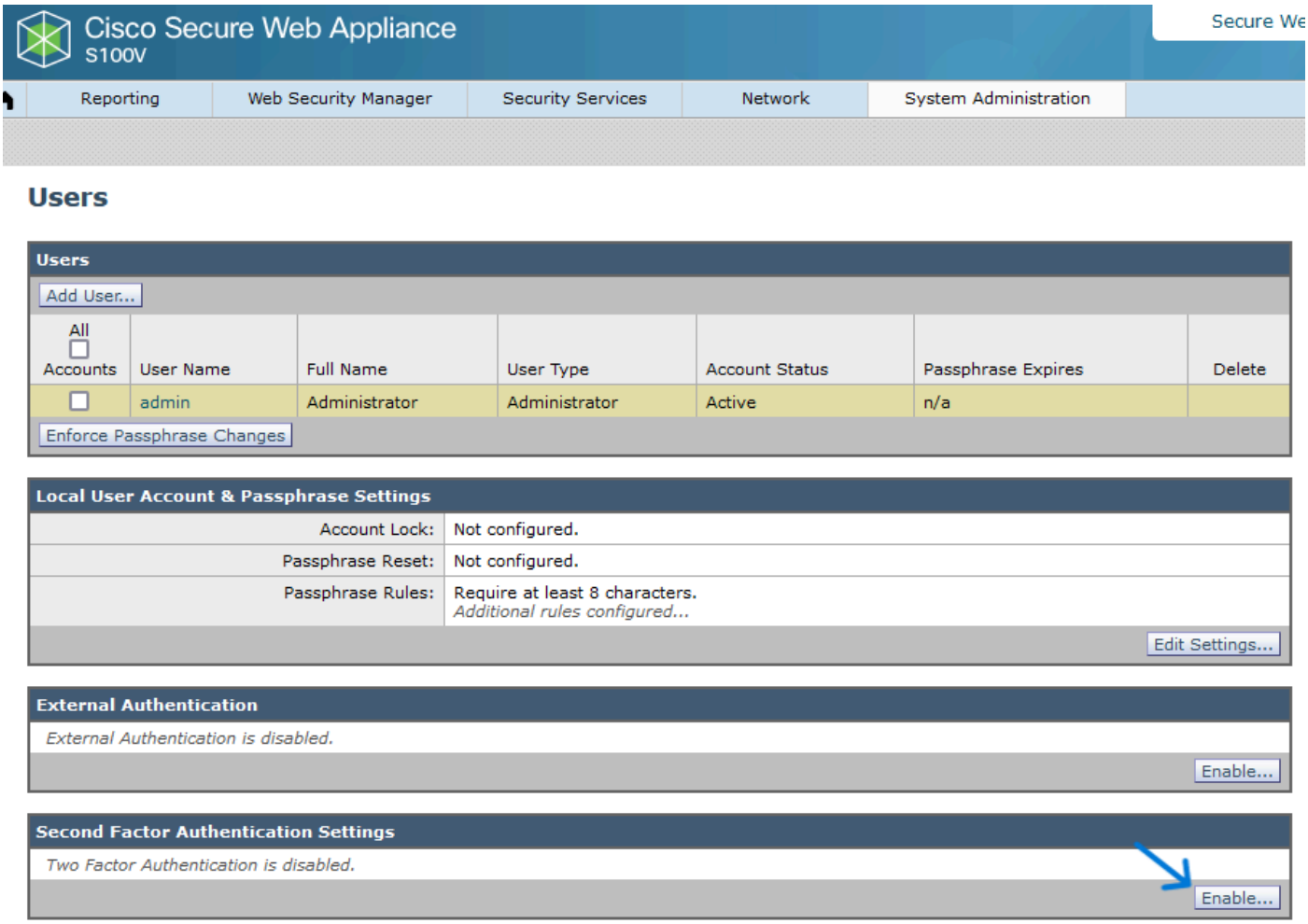
在SWA中启用第二因素身份验证

第三步： 在RADIUS Server Hostname字段中输入ISE的IP地址，并输入在ISE配置的第2步中配置的共享密钥。

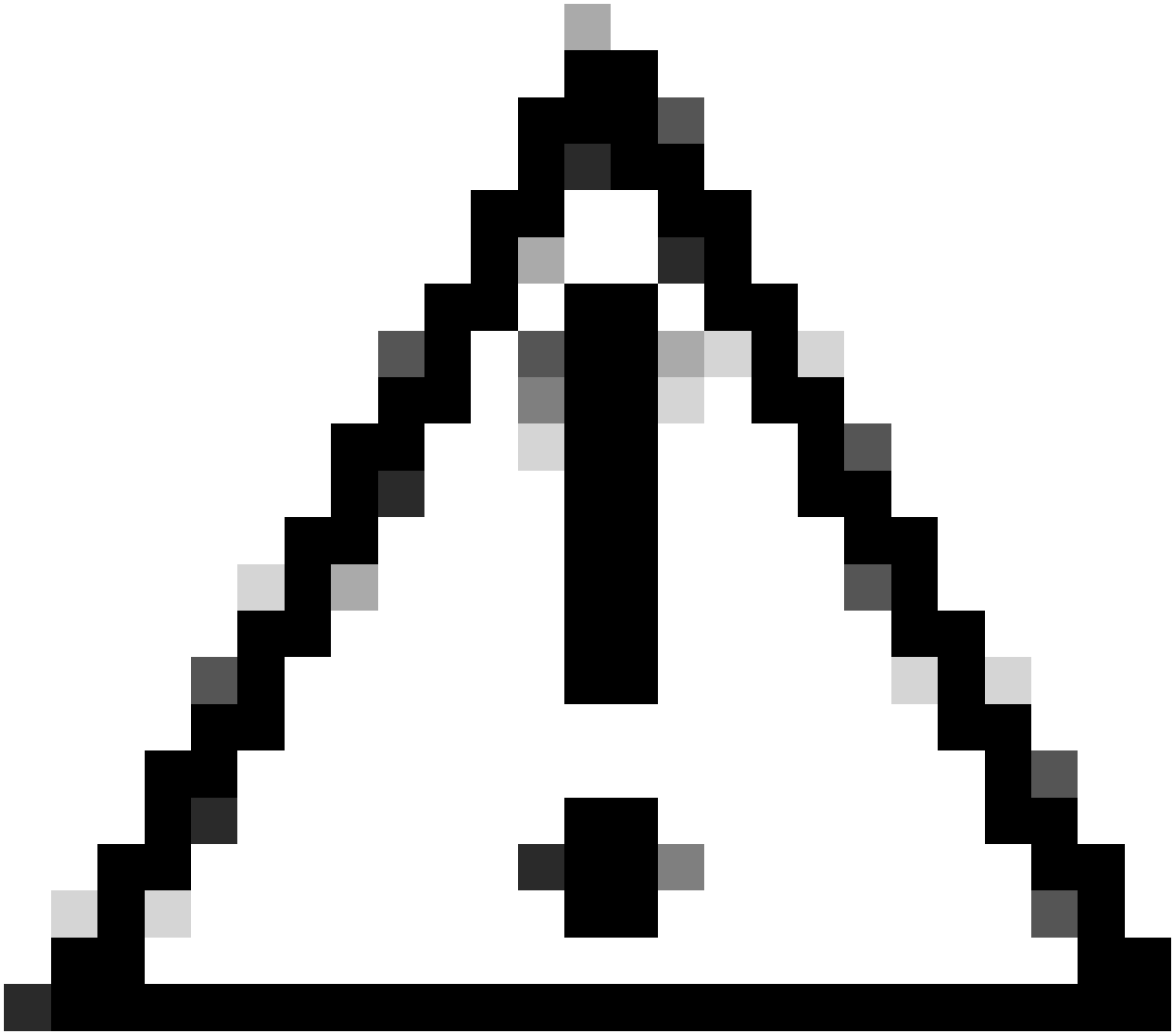
第四步： 选择需要启用“第二因素”实施的必需预定义角色。



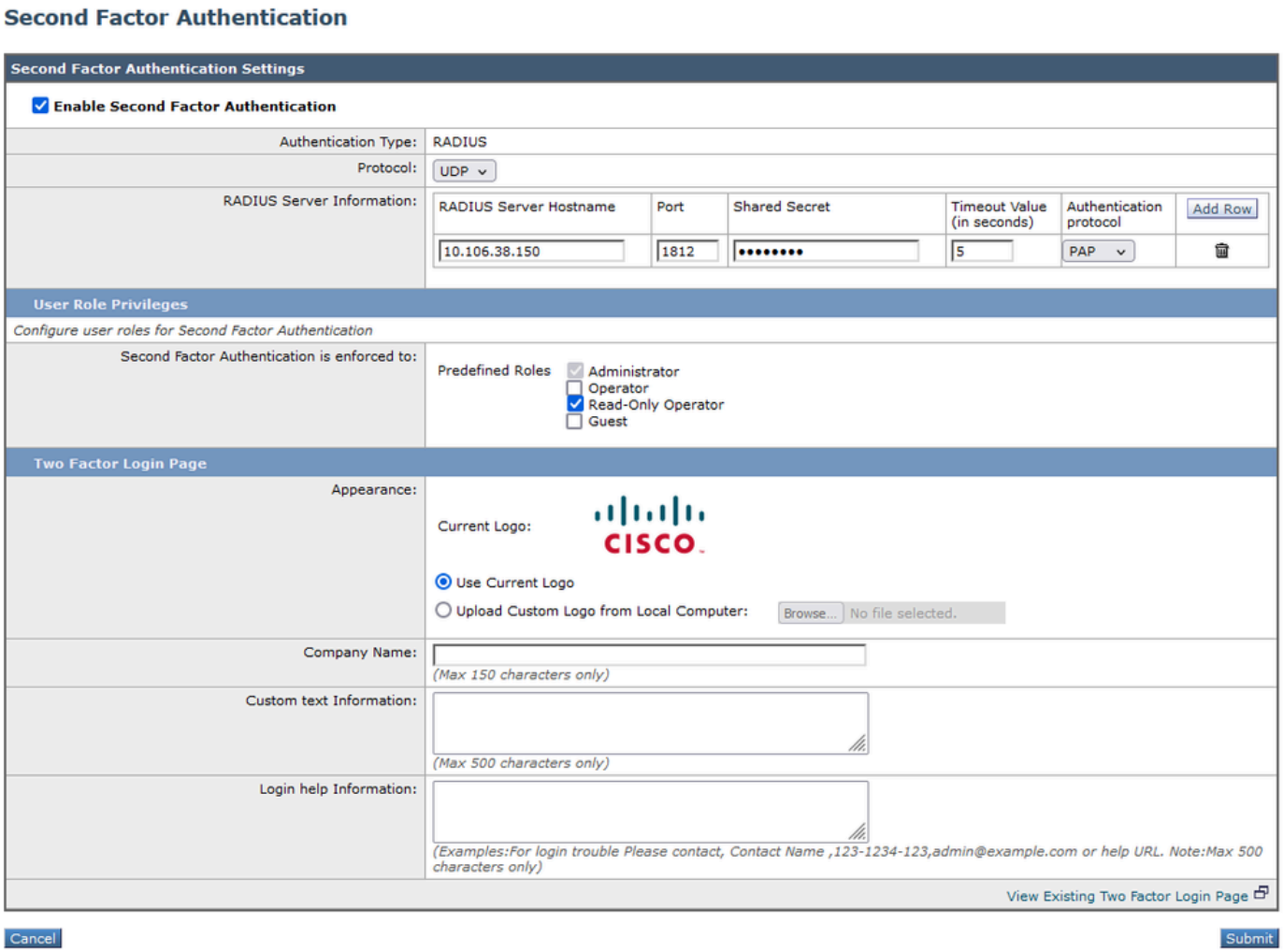
注意：如果在SWA中启用第二因素身份验证，则默认的“admin”帐户也会通过第二因素实施启用。您必须将ISE与LDAP或Active Directory (AD)集成以对“admin”凭证进行身份验证，因为ISE不允许将“admin”配置为网络访问用户。



在SWA中启用第二因素身份验证

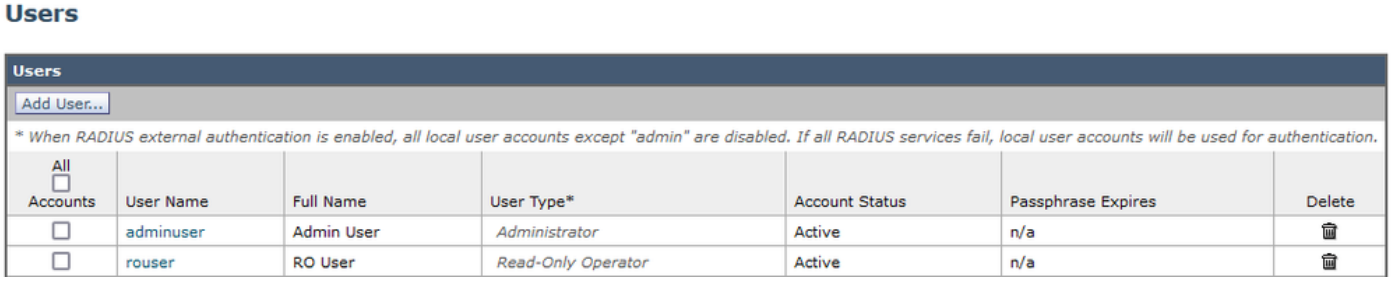


注意：如果在SWA中启用第二因素身份验证，则默认的“admin”帐户也会通过第二因素实施启用。您必须将ISE与LDAP或Active Directory (AD)集成以对“admin”凭证进行身份验证，因为ISE不允许将“admin”配置为网络访问用户。



配置第二因素身份验证

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。

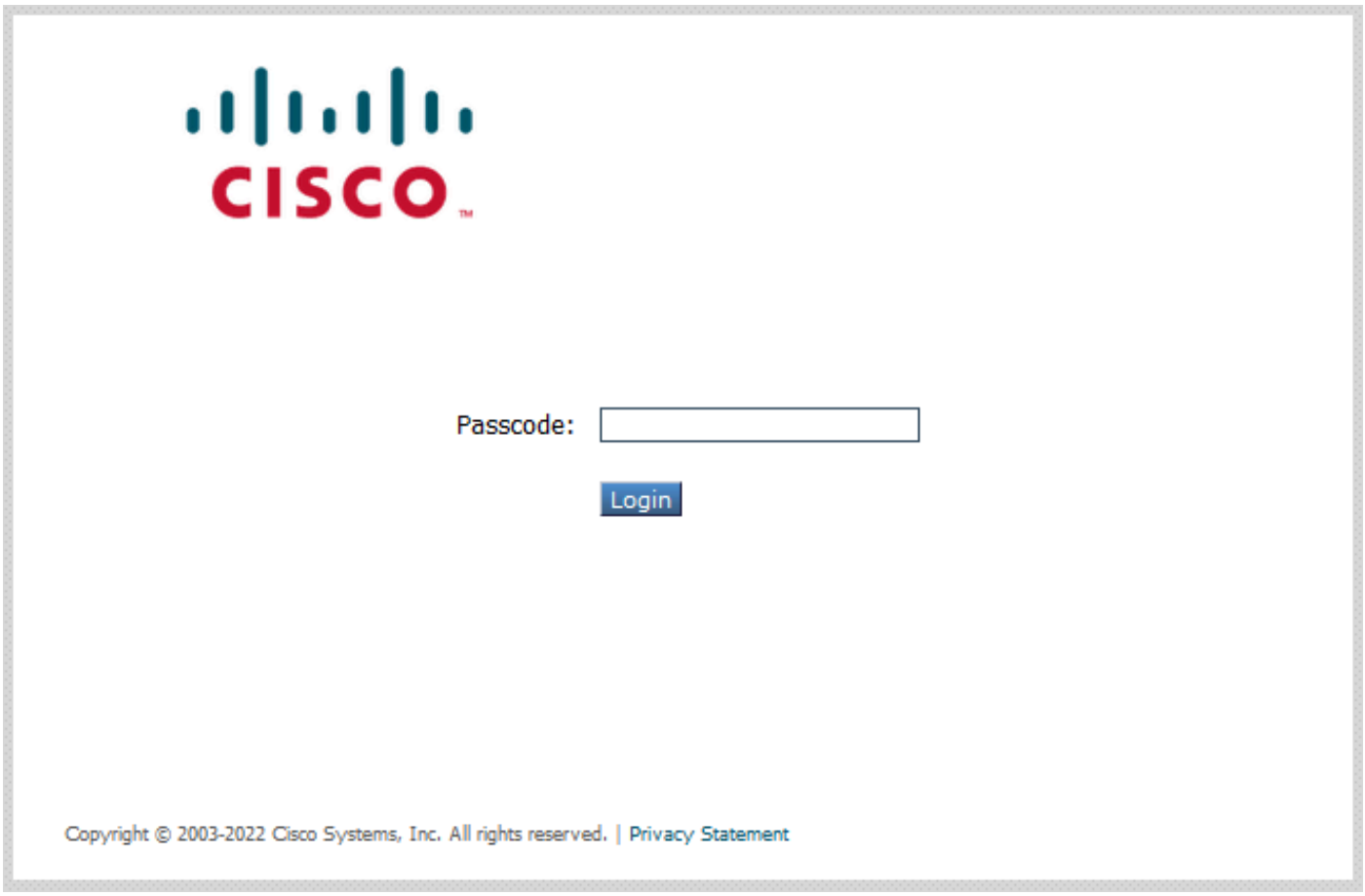


SWA中的用户配置

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。身份验证成功后，您将被重定向到辅助身份验证页面。此处，您需要输入在ISE中配置的辅助身份验证凭证。



验证第二因素登录

参考

- 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
- 集成AD用于ISE GUI和CLI登录

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）。