使用ISE RADIUS配置SWA双因素身份验证

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

网络拓扑

配置步骤

- ISE 配置
  - 2.在ISE中配置网络设备
- SWA配置

验证

相关内容

简介

本文档介绍如何配置安全网络设备上的第二因素身份验证，将Cisco ISE®用作RADIUS服务器。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本RADIUS知识
- SWA基础知识
- 了解思科身份服务引擎(ISE)上的身份验证和授权策略配置

思科建议您还应具备以下条件：

- 兼容的WSA和ISE版本
- 您的ISE已集成到Active Directory或LDAP
- 安全网络设备(SWA)和思科身份服务引擎(ISE)管理访问

- Active Directory或LDAP配置用户名“Admin”以验证SWA默认“Admin”帐户

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

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中配置的凭证后再次验证与RADIUS服务器的用户凭证。

网络拓扑



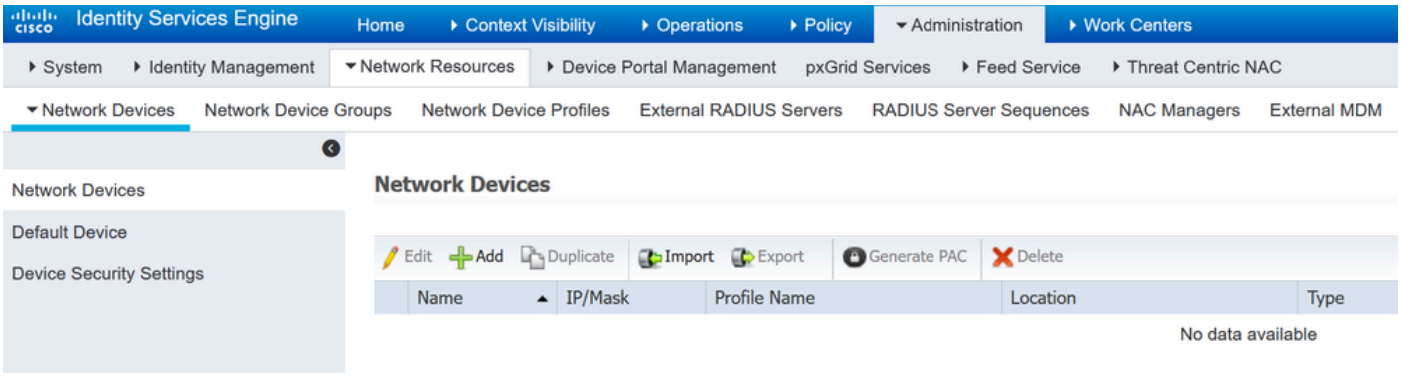
图像 — 网络拓扑图

管理用户使用其凭证访问端口443上的SWA，SWA通过RADIUS服务器验证凭证以进行第二次身份验证。

配置步骤

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.在ISE中配置网络设备

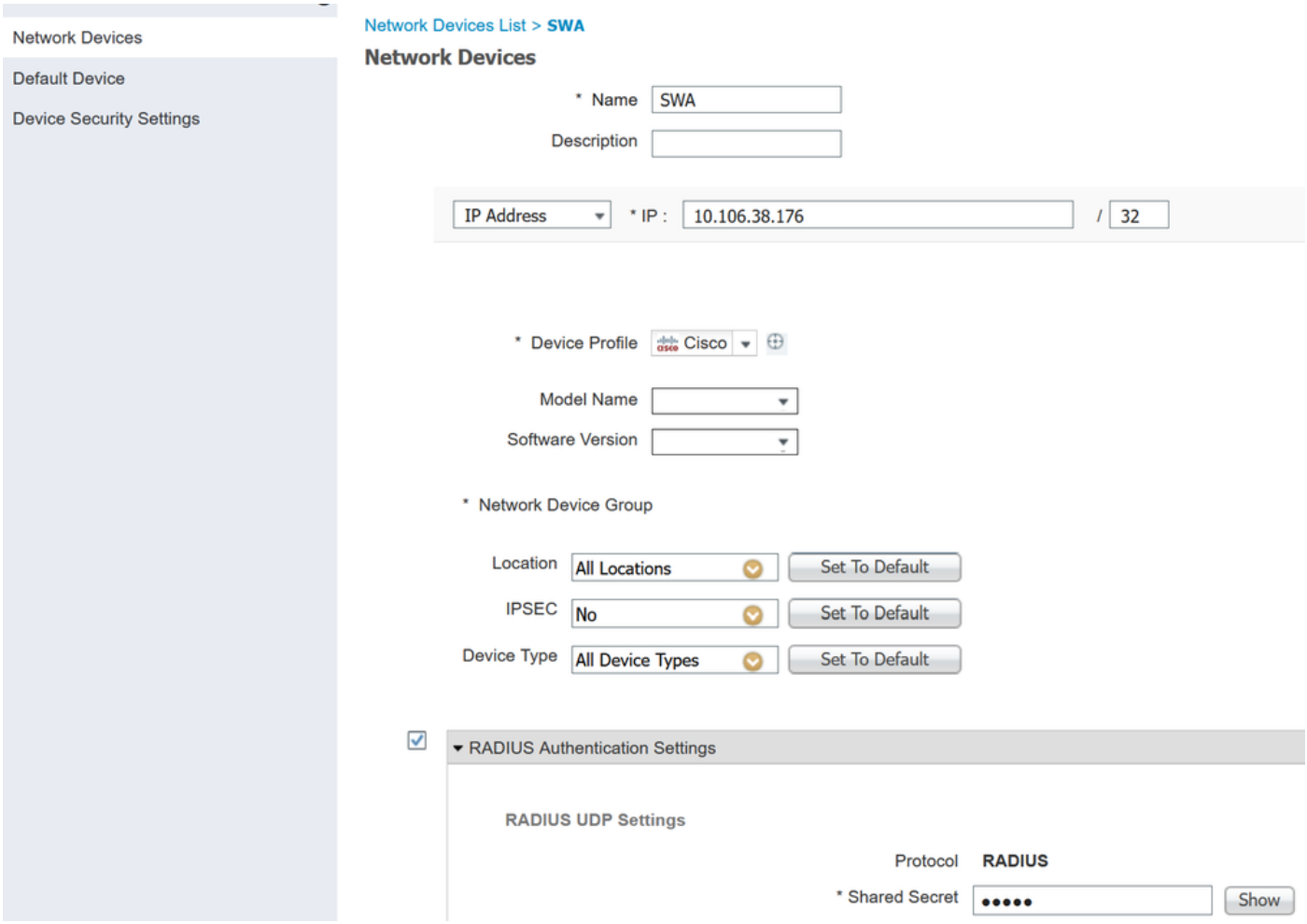
2.1.为网络设备对象指定Name。

2.2.插入SWA IP地址。

2.3.选中RADIUS复选框。

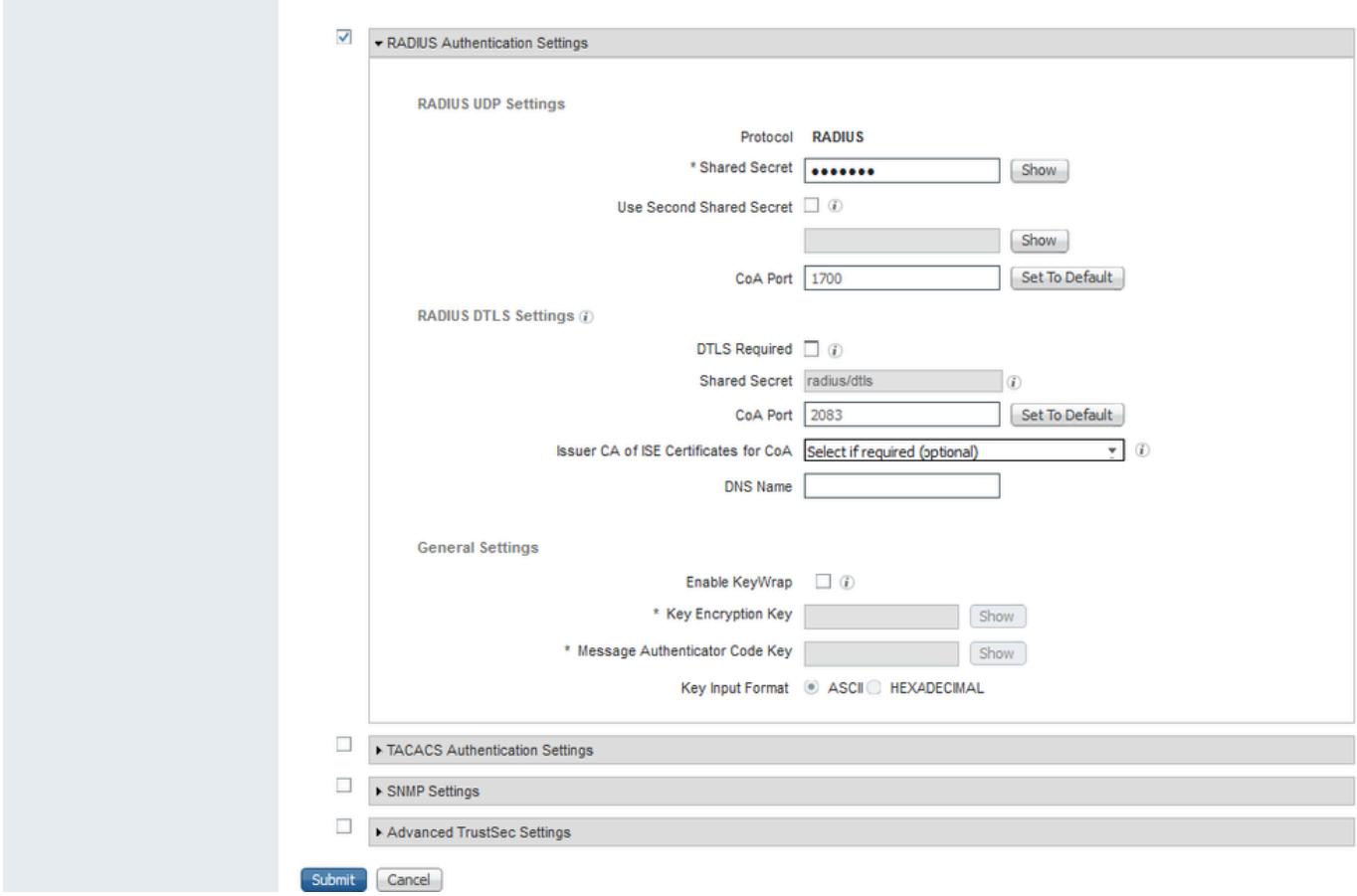
2.4.定义共享密钥。

注意：稍后必须使用该密钥来配置SWA。



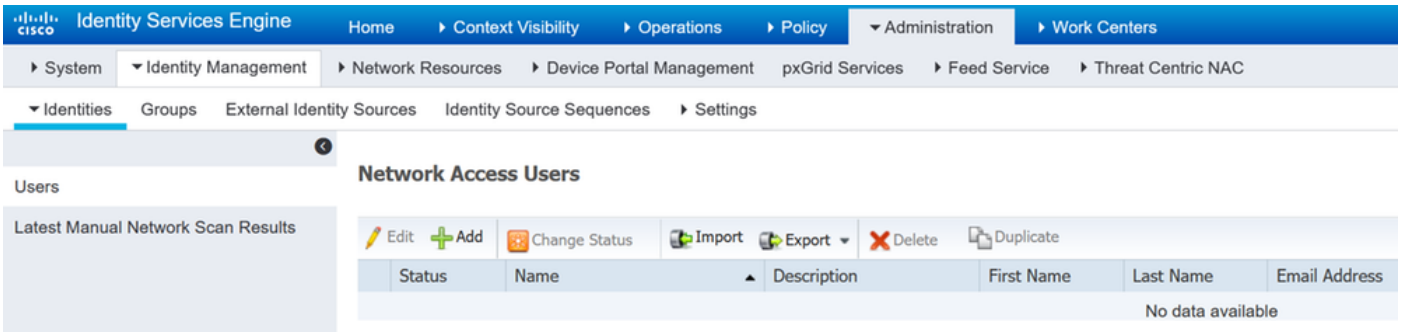
配置SWA网络设备共享密钥

2.5.单击Submit。



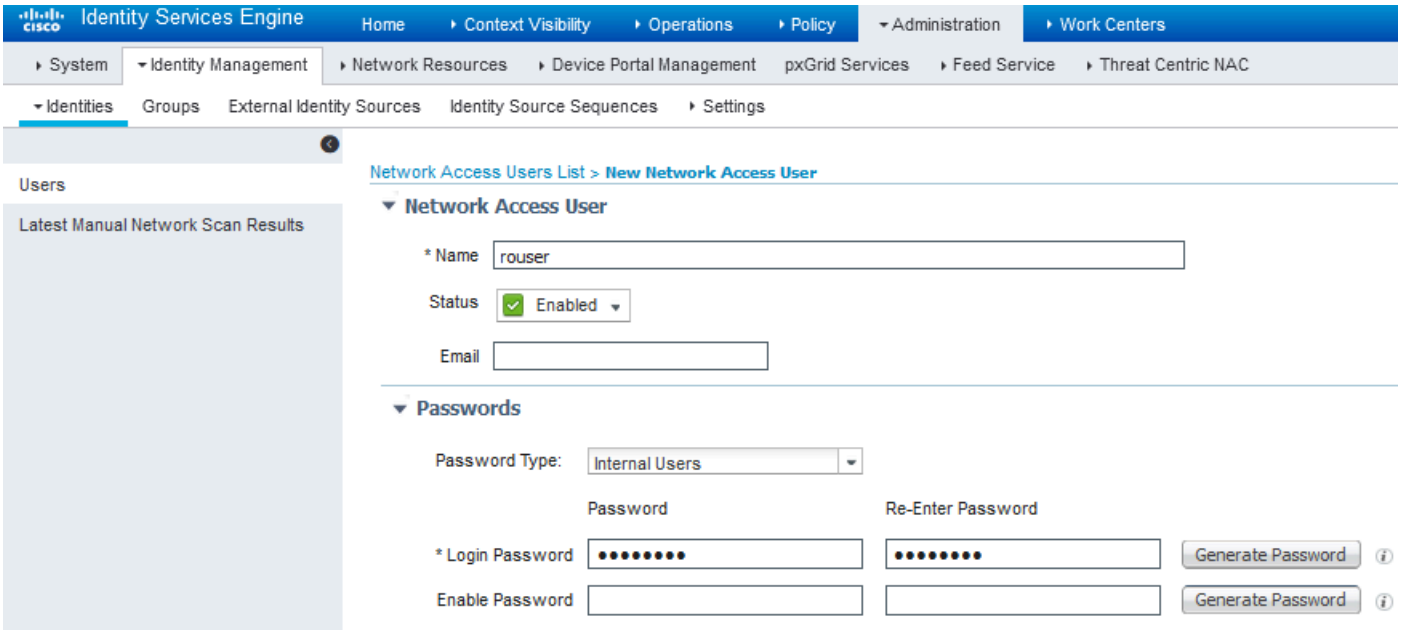
提交网络设备配置

3.您必须创建与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> +添加。



在ISE中添加本地用户

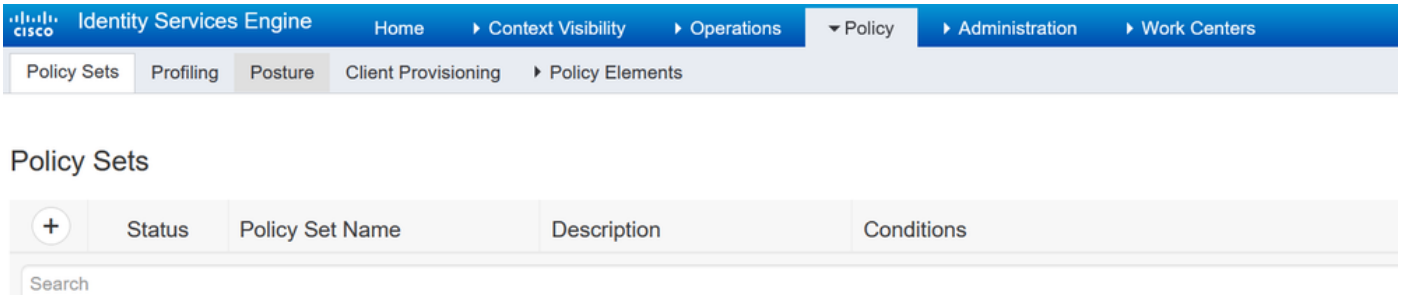
3.1.指定名称。
3.2.（可选）输入用户的邮件地址。
3.3.设置密码。
3.4.单击Save。



在ISE中添加本地用户

4.创建与SWA IP地址匹配的策略集。这可以阻止使用这些用户凭证访问其他设备。

4.1.导航到Policy > Policy Sets，然后点击位于左上角的+图标。

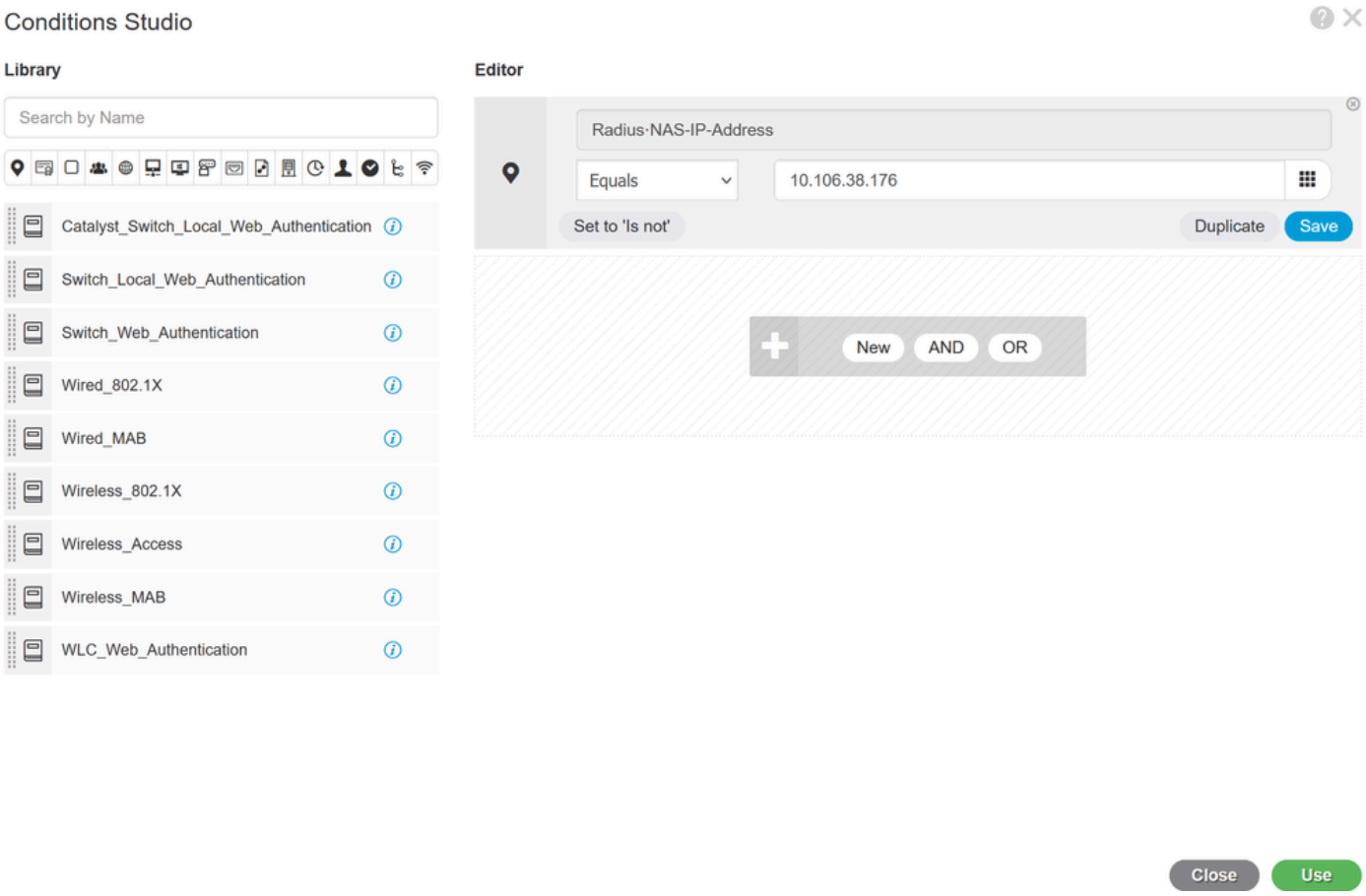


在ISE中添加策略集

4.2.新行位于策略集的顶部。输入新策略的Name。

4.3.为RADIUS NAS-IP-Address属性添加条件以匹配SWA IP地址。

4.4.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

4.5.单击Save。



策略保存

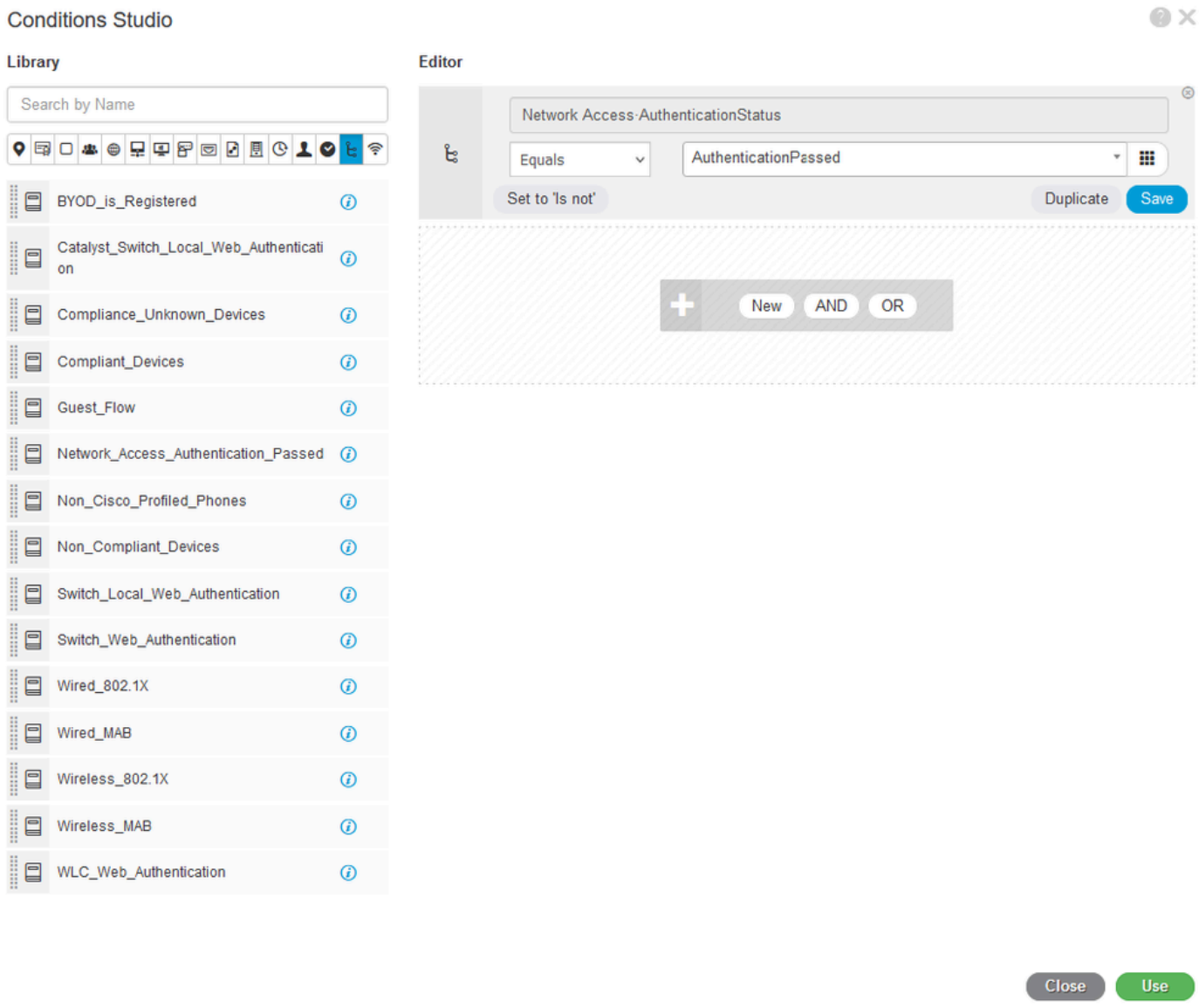
注意：本示例使用Default Network Access Protocols列表。您可以创建新列表并根据需要缩小其范围。

5.要查看新的策略集，请单击查看列中的>图标。

5.1.展开Authorization Policy菜单，然后单击+图标以添加允许访问所有已验证用户的新规则。

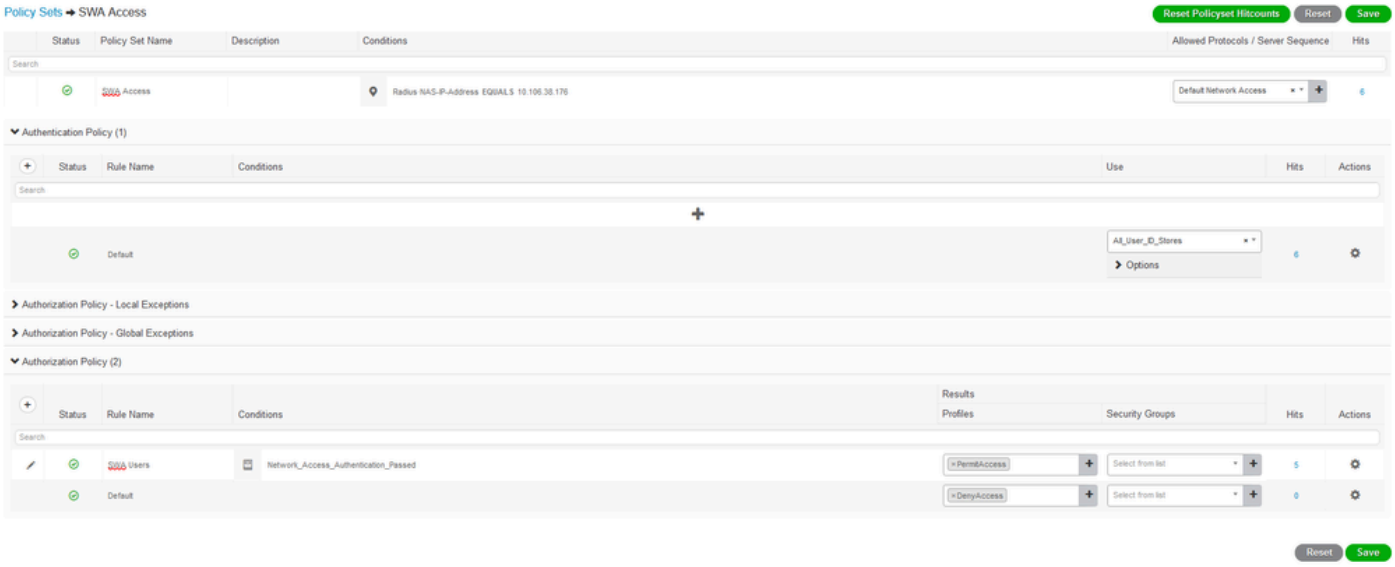
5.2.输入名称。

5.3.设置条件以匹配Attribute AuthenticationStatus Equals AuthenticationPassed的Dictionary Network Access，然后单击Use。



选择授权条件

6.将默认PermitAccess设置为Authorization Profile，然后单击Save。

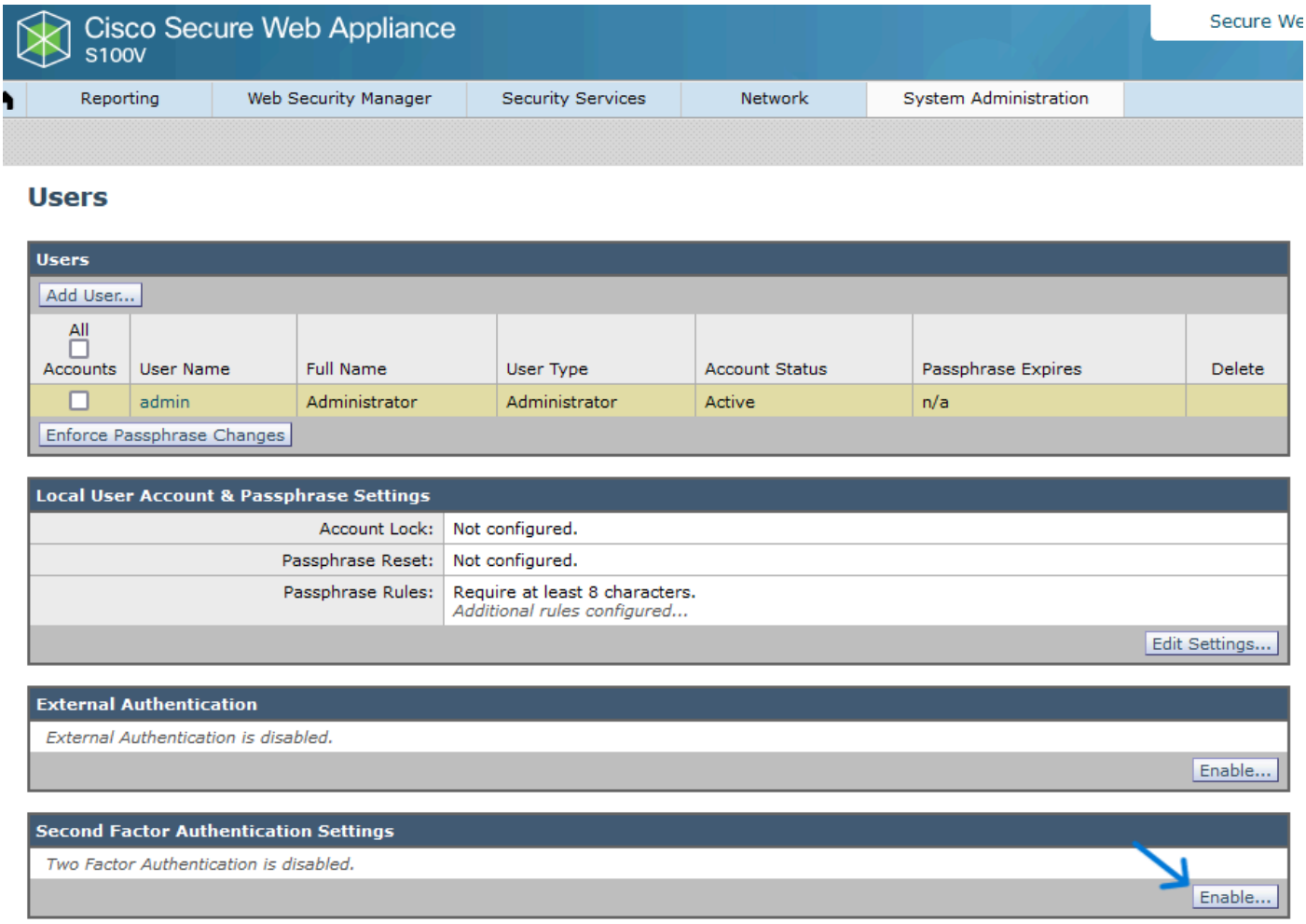


选择授权配置文件

SWA配置

1.从SWA GUI导航到系统管理，然后选择用户。

2.单击第二个因素身份验证设置中的启用。

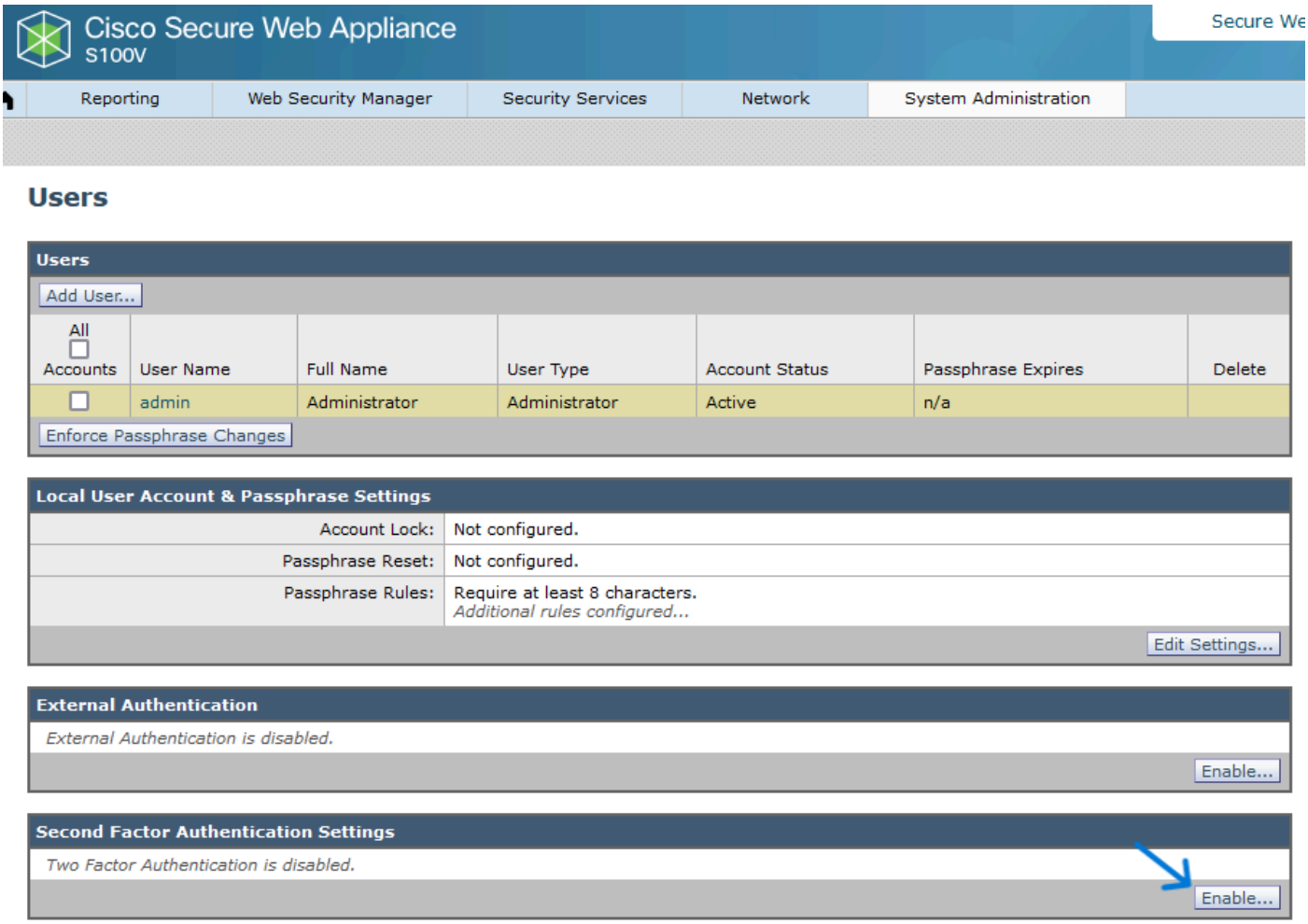


在SWA中启用第二因素身份验证

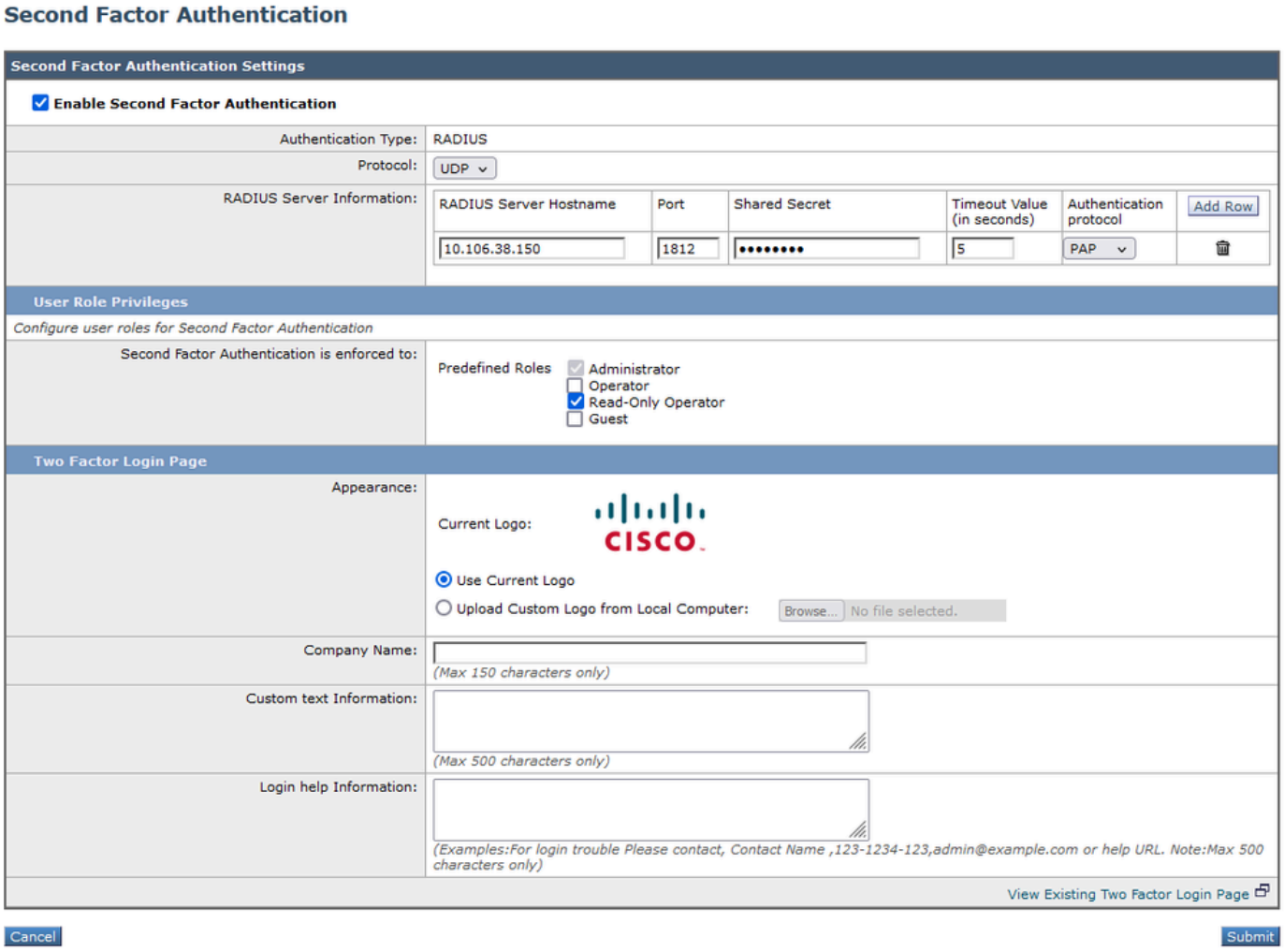
3.在RADIUS Server Hostname（RADIUS服务器主机名）字段中输入ISE的IP地址，并输入ISE配置步骤2中配置的Shared Secret。

4.选择要启用第二要素实施的预定义角色。

⚠ 警告：如果在SWA中启用第二因素身份验证，则还会为第二因素实施启用默认Admin帐户。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Network Access User。

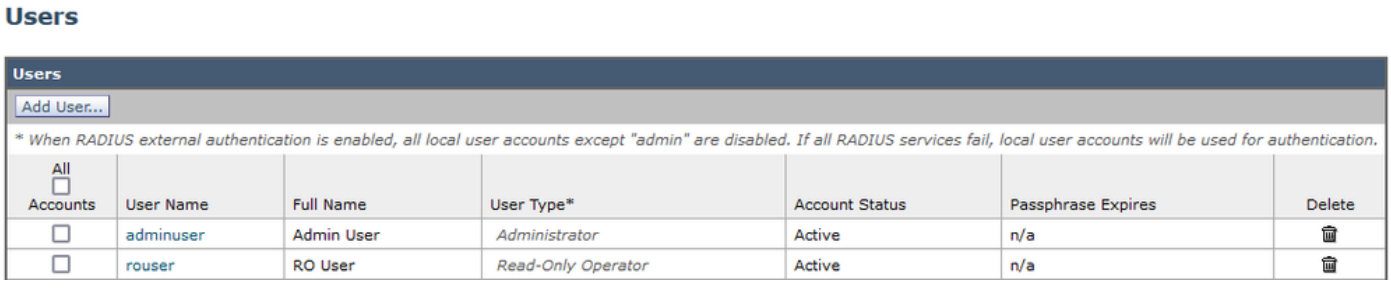


在SWA中启用第二因素身份验证



配置第二因素身份验证

5.要在SWA中配置用户，请单击添加用户。输入User Name并选择所需角色所需的User Type。输入Passphrase并重新键入密码。

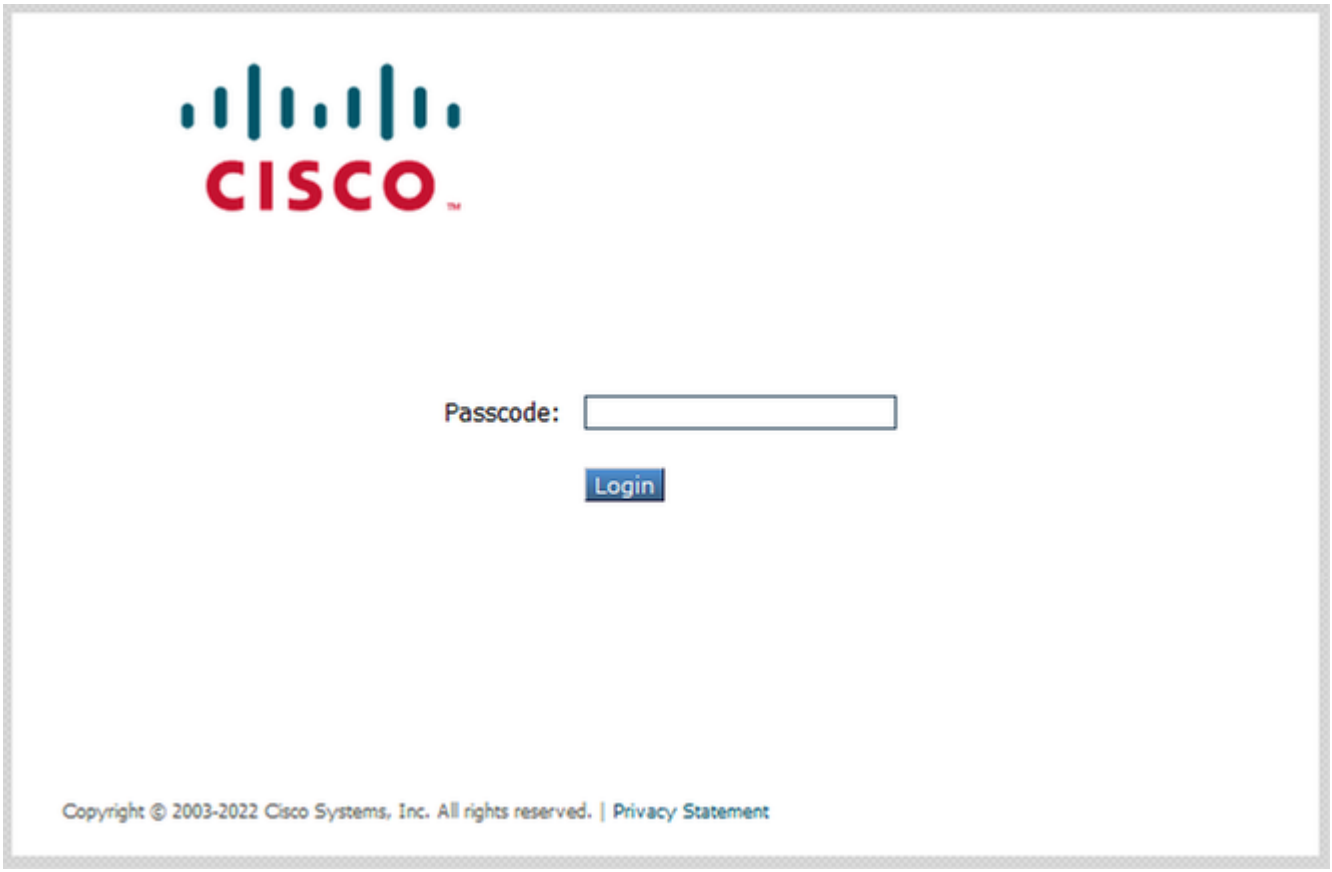


SWA中的用户配置

6.单击提交和提交更改。

验证

使用配置的用户凭证访问SWA GUI。身份验证成功后，您将重定向到辅助身份验证页面。您必须输入在ISE中配置的辅助身份验证凭证。



验证第二次因子登录

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
- 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）。