配置ISE 3.3本地多因素身份验证与双核

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 流程图
- 配置
  - 选择要保护的应用
  - 将ISE与Active Directory集成
  - 启用开放式API
  - 启用MFA身份源
  - 配置MFA外部身份源
  - 将用户注册到Duo
  - 配置策略集
- 限制

验证

故障排除

简介

本文档介绍如何将身份服务引擎(ISE)3.3补丁1与Duo集成以实现多重身份验证。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- ISE
- Duo

使用的组件

从版本3.3补丁1开始，可以将ISE配置为与双核服务进行本地集成，无需身份验证代理。

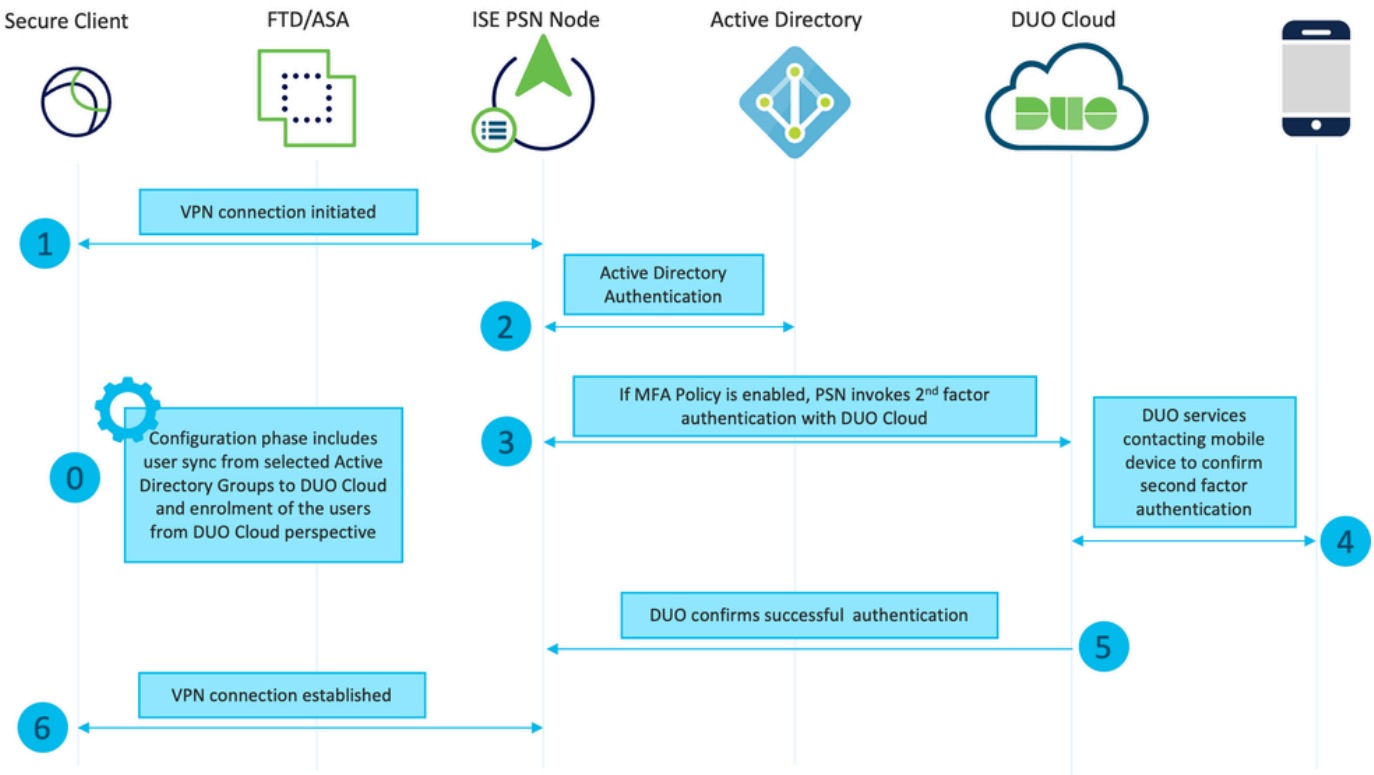
本文档中的信息基于：

- 思科ISE版本3.3补丁1
- Duo
- Cisco ASA 9.16(4) 版
- 思科安全客户端5.0.04032版

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。

配置

流程图



步骤

1. 配置阶段包括选择Active Directory组，用户将同步到该组，并且此同步在MFA向导完成后进行。它由两个步骤组成。查找Active Directory以检索用户和特定属性的列表。通过思科ISE管理API调用Duo Cloud，将用户推送到那里（管理员需要注册用户）。 注册用户可包括激活用

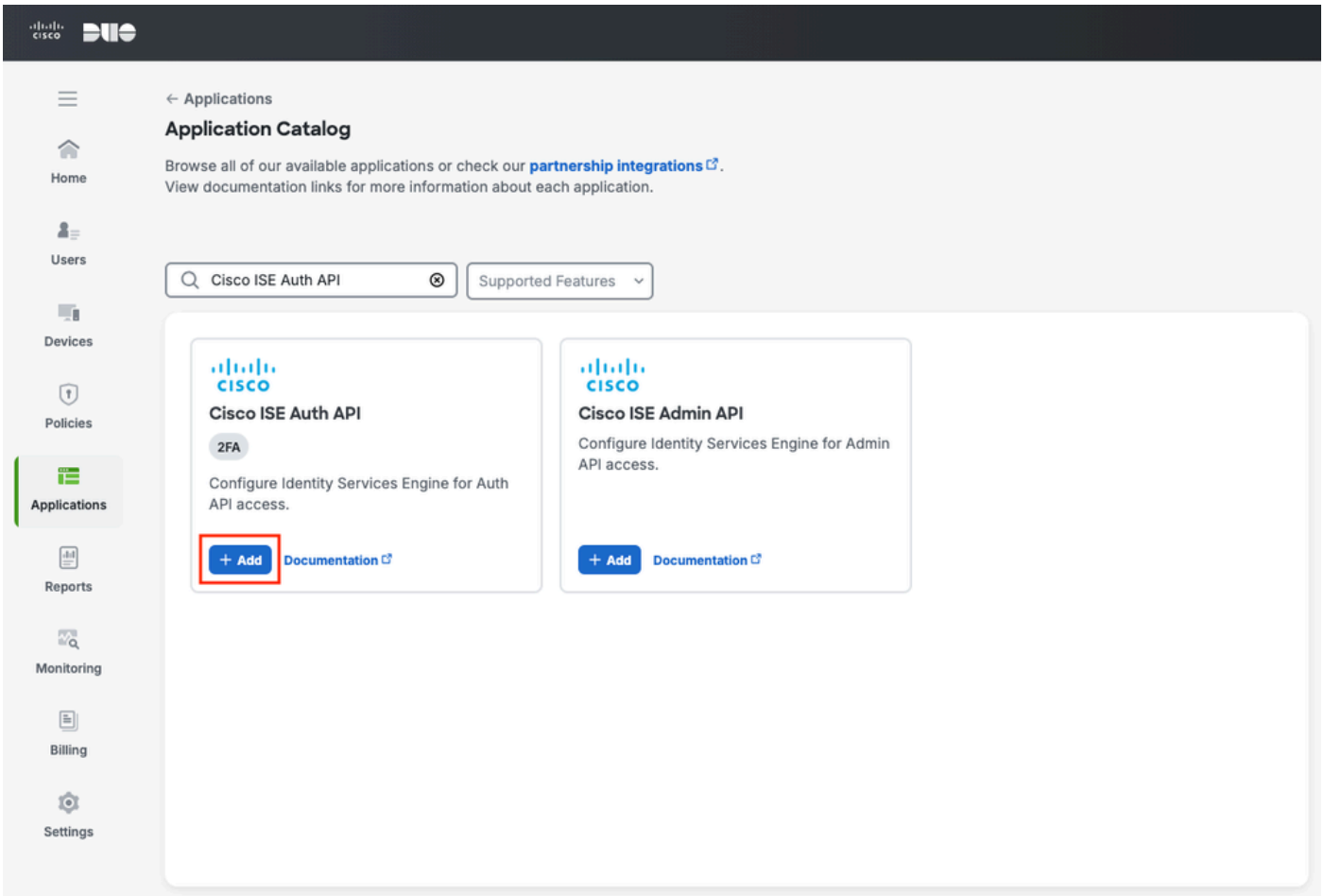
户使用Duo Mobile的可选步骤，这允许用户使用Duo Push的一键式身份验证。
2. 启动VPN连接后，用户输入其用户名和密码，然后点击OK。网络设备向PSN发送RADIUS访问请求。
3. PSN节点通过Active Directory对用户进行身份验证。
4. 当身份验证成功且配置了MFA策略时，PSN会与Duo Cloud联系。通过思科的ISE身份验证API调用Duo Cloud，以使用Duo调用第二因素身份验证。ISE在SSL TCP端口443上与Duos服务通信。
5. 第二因素身份验证发生，用户完成第二因素身份验证过程。
6. Duo对PSN做出响应并提供第二因素身份验证的结果。
7. Access-Accept将发送到网络设备并建立VPN连接。

配置

选择要保护的应用

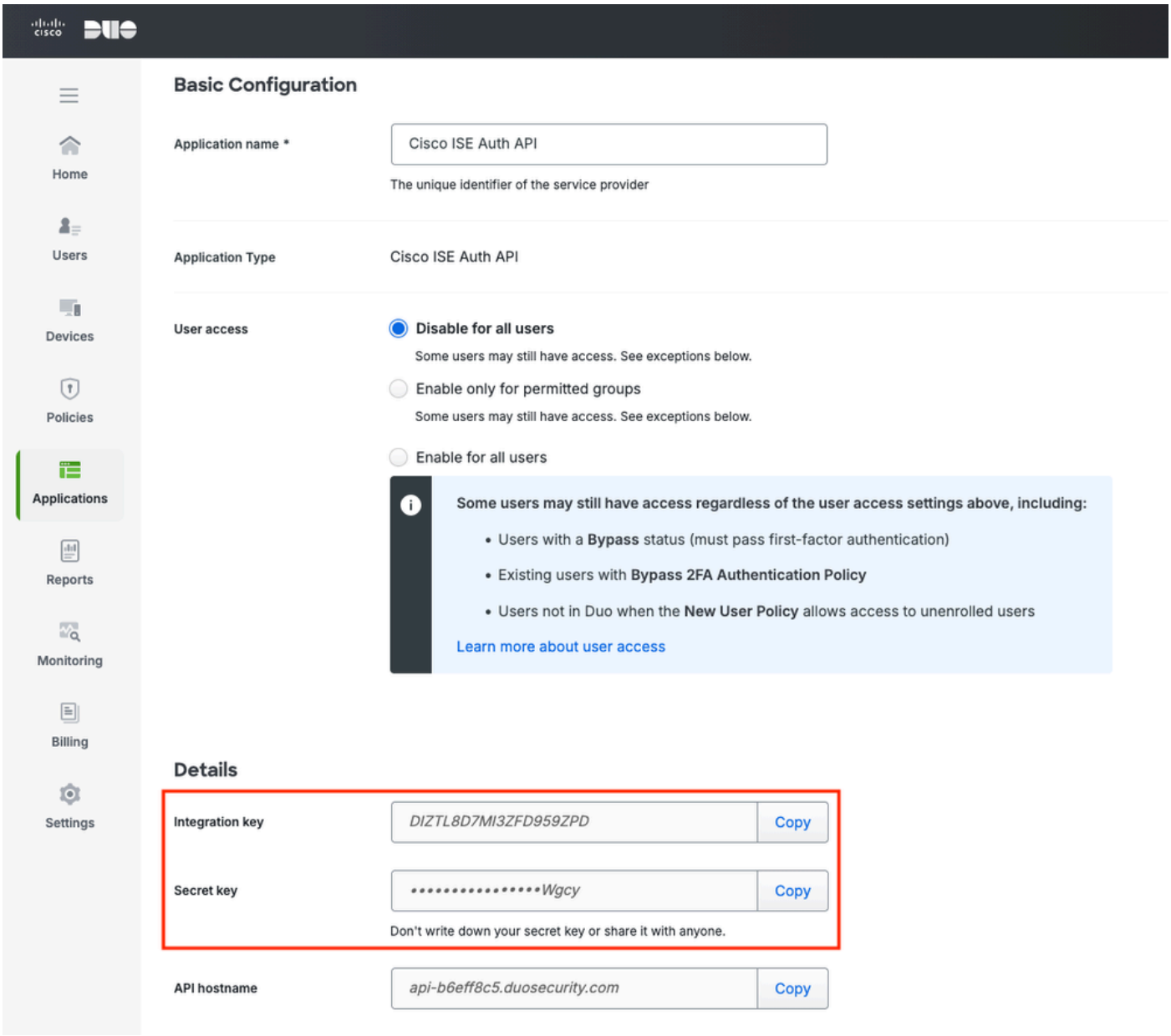
1.导航至Duo Admin Dashboard。使用管理员凭证登录。

2.定位至控制面板>应用>应用目录。查找Cisco ISE Auth API并选择+ Add。



ISE身份验证API 1

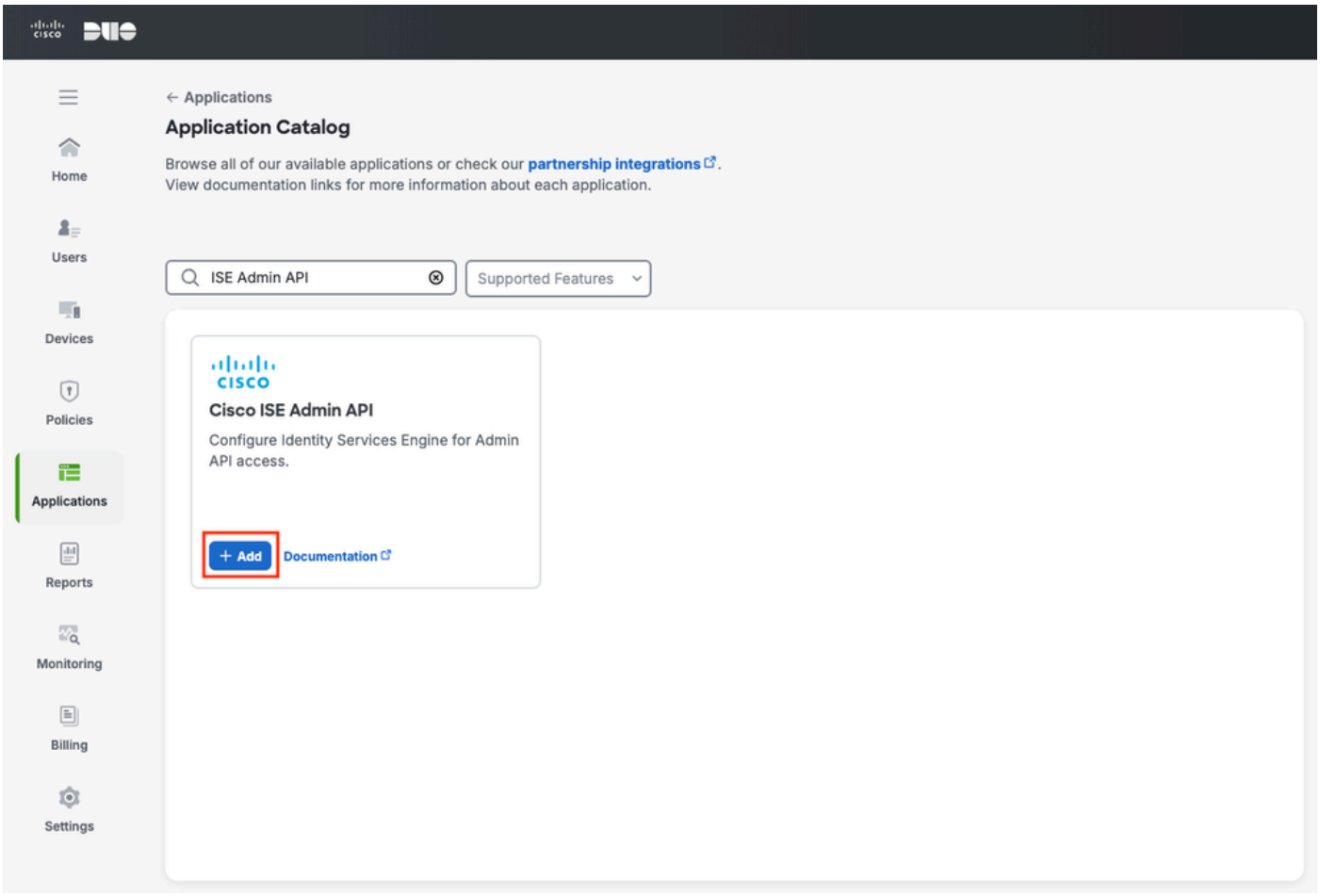
3.记下Integrationkey和Secret密钥。



ISE身份验证API 2

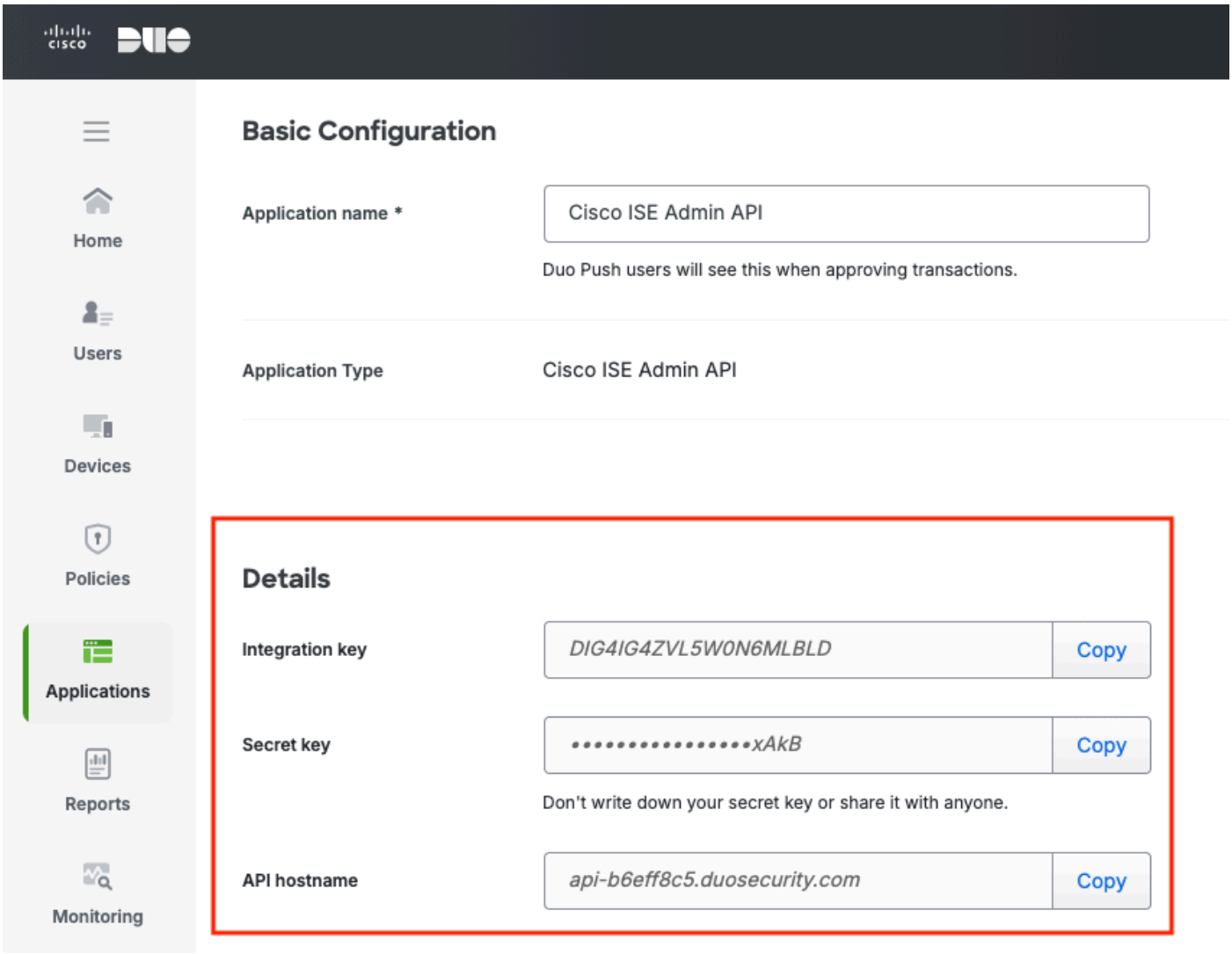
4.定位至控制面板>应用>应用目录。查找Cisco ISE管理API并选择+添加。

注意：只有具有Owner角色的管理员才能在Duo Admin Panel中创建或修改思科ISE管理员API应用。



ISE管理API 1

5.记下Integration密钥、Secret密钥和API主机名。

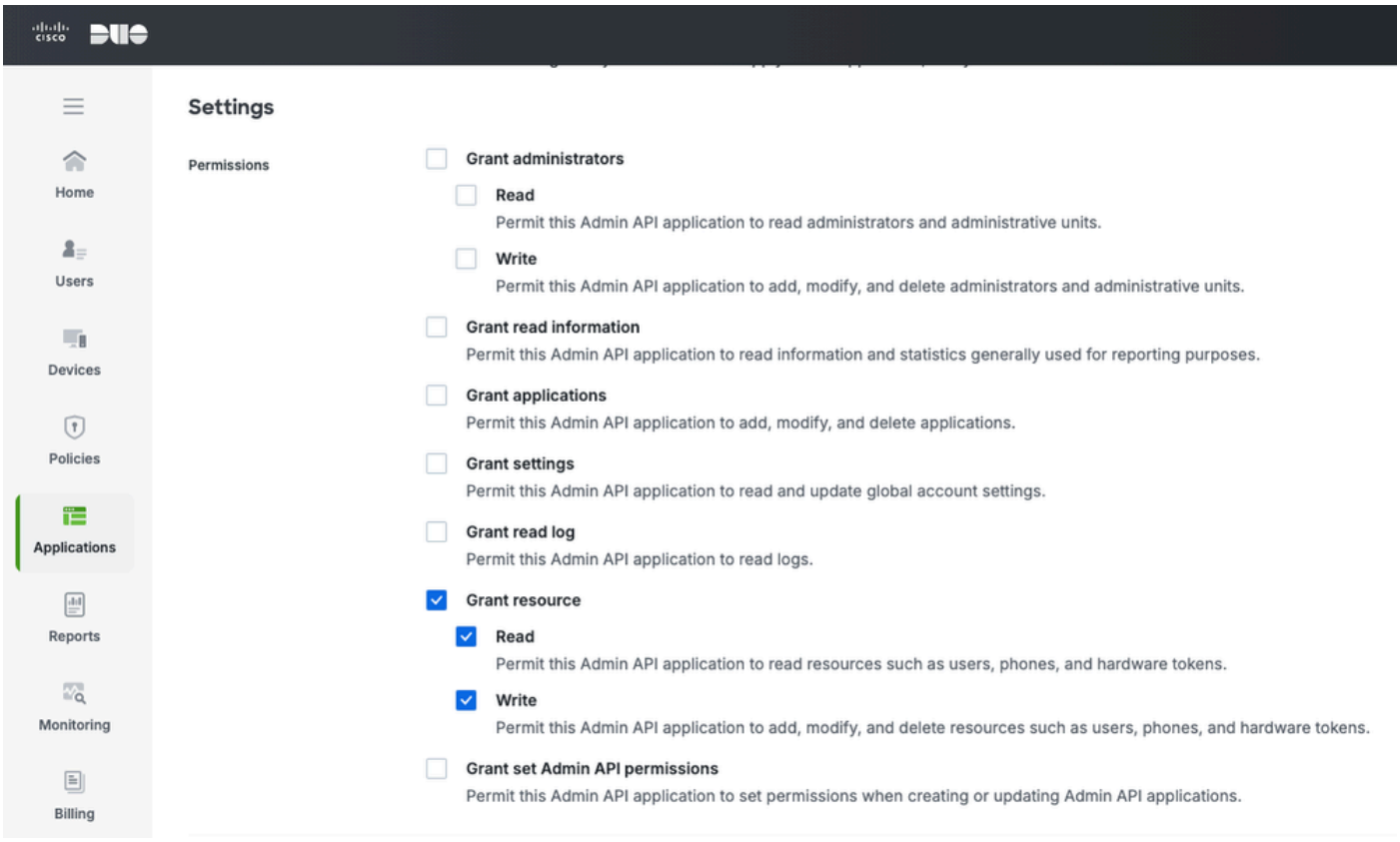


ISE管理API 2

配置API权限

1.定位至控制面板>应用>应用。选择Cisco ISE管理API。

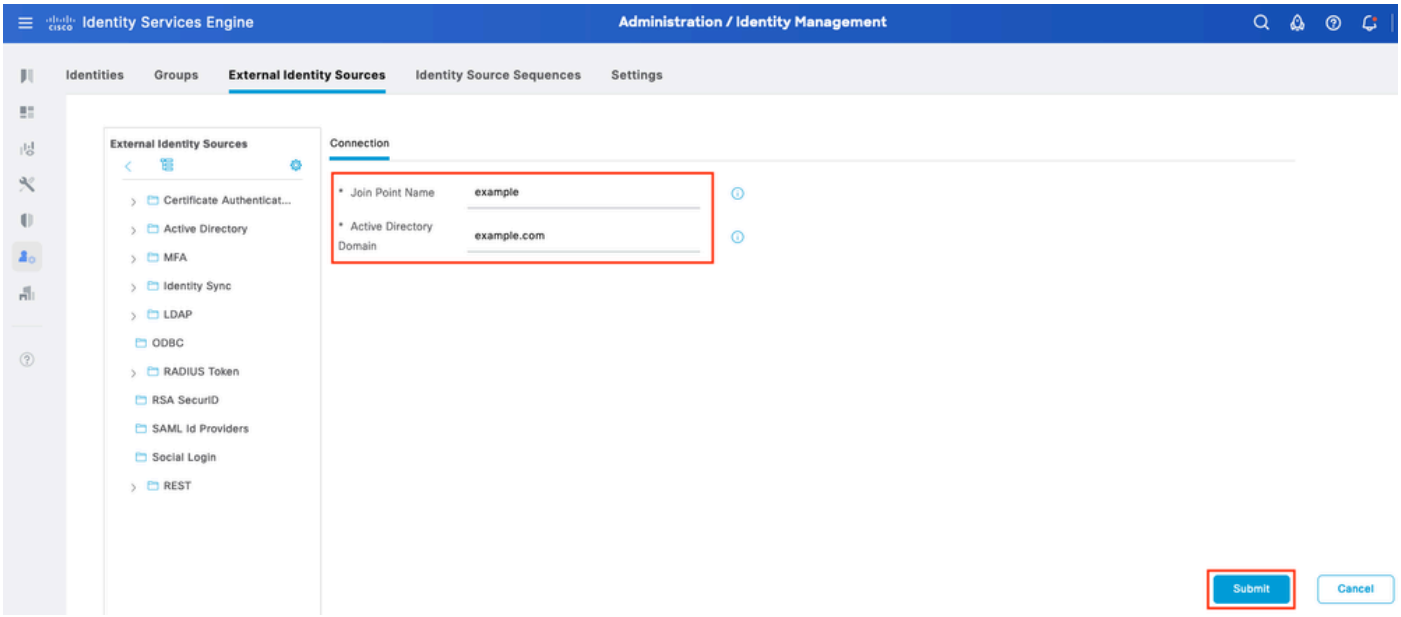
2.选中授予读取资源和授予写入资源权限。点击Save Changes。



管理员API权限

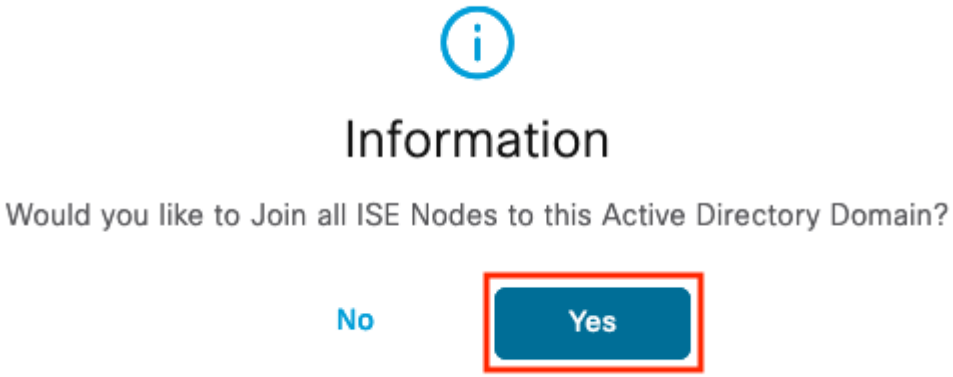
将ISE与Active Directory集成

1.导航到Administration > Identity Management > External Identity Stores > Active Directory > Add。提供加入点名称、Active Directory域并点击提交。



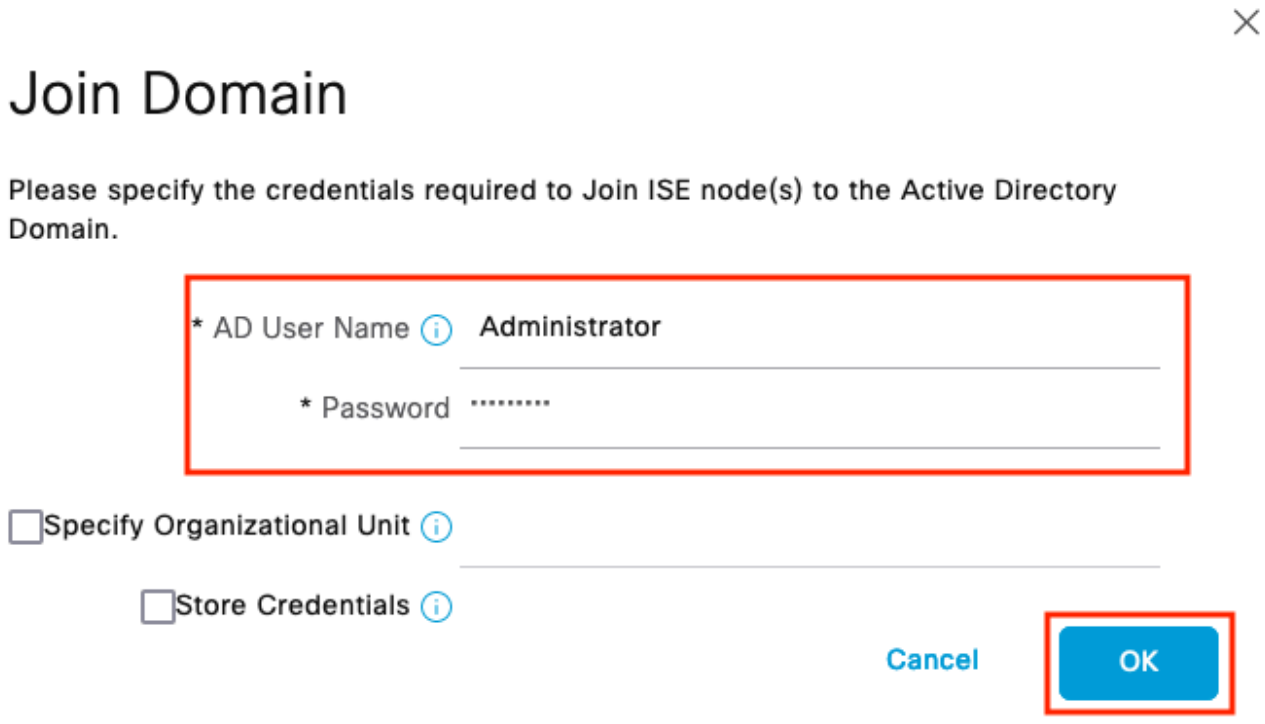
Active Directory 1

2.当系统提示将所有ISE节点加入此Active Directory域时，点击是。



Active Directory 2

3.提供AD用户名和密码，然后单击OK。



Active Directory 3

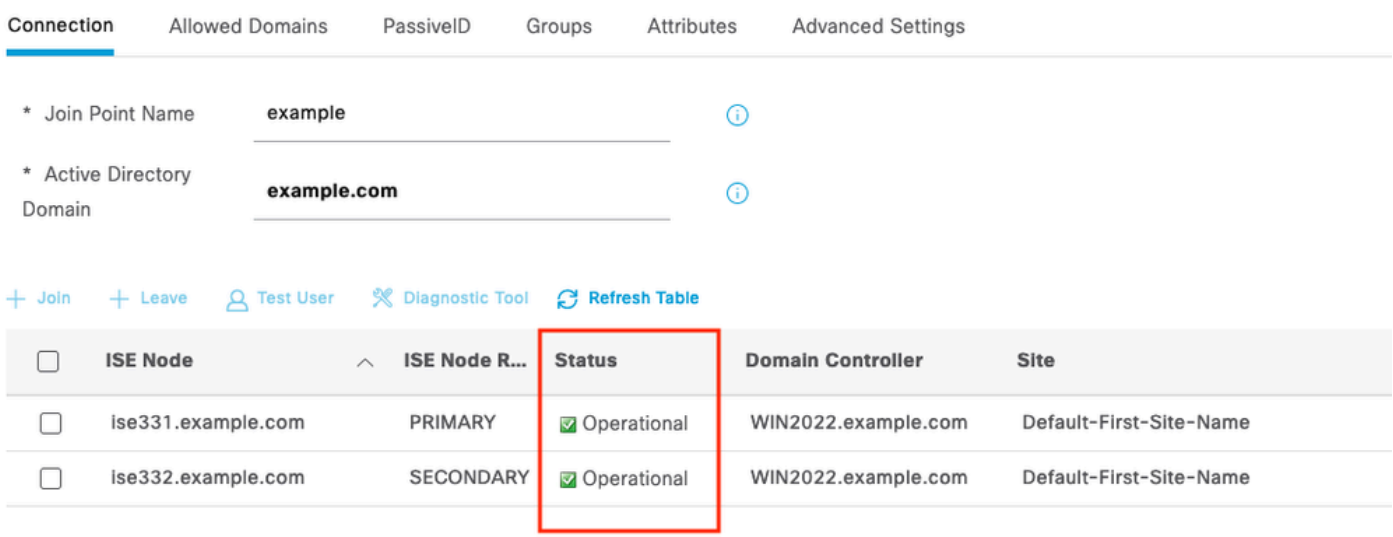
4.在ISE中访问域所需的Active Directory帐户可以具有下列任一项：

- 将工作站添加到相应域中的域用户权限。

- 在创建ISE计算机帐户的相应计算机容器上创建计算机对象或删除计算机对象权限，然后将ISE计算机加入域。

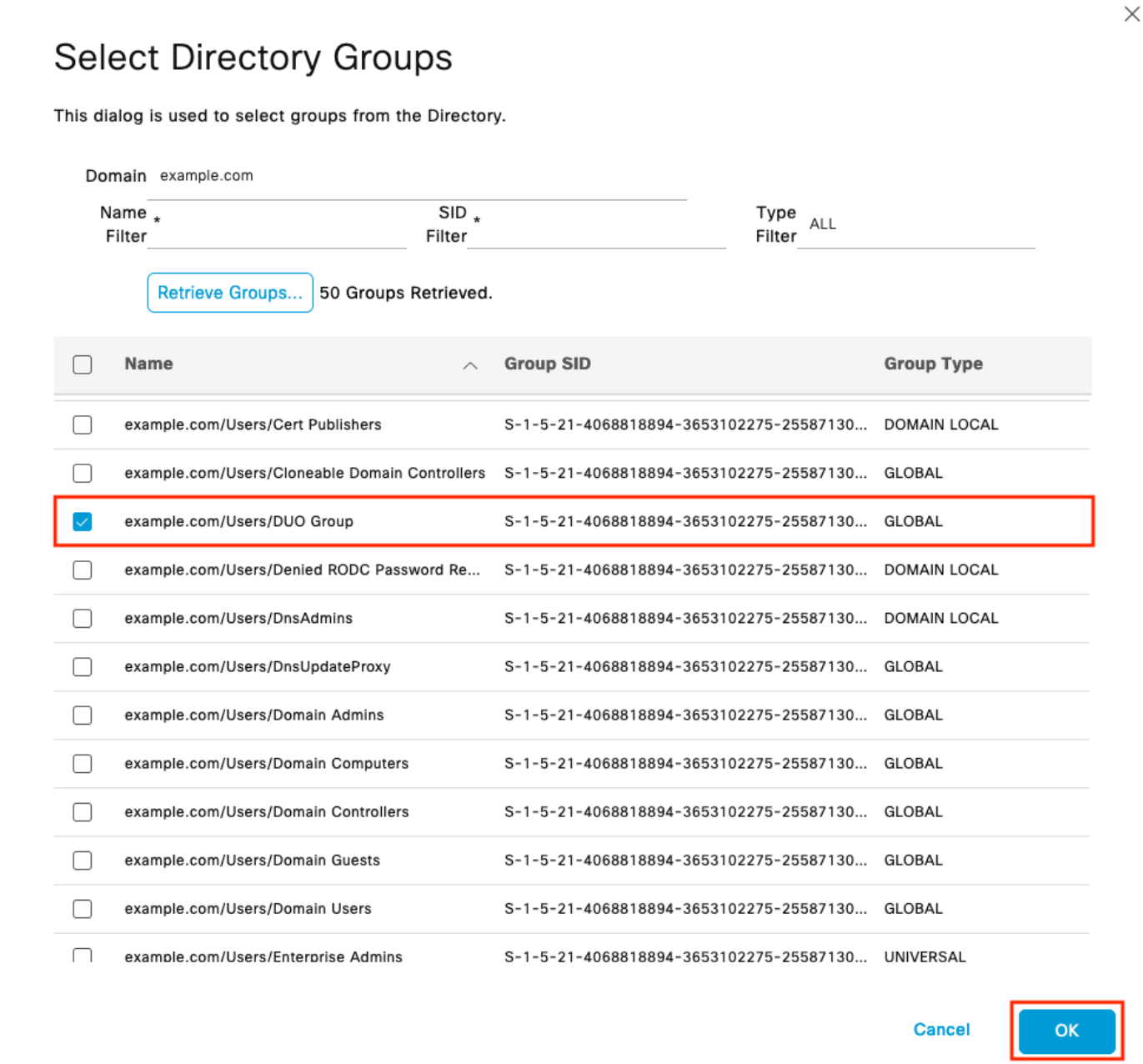
注意：思科建议禁用ISE帐户的锁定策略，并配置AD基础设施，以便在为该帐户使用错误密码时向管理员发送警报。输入错误密码时，ISE不会在必要时创建或修改其计算机帐户，因此可能会拒绝所有身份验证。

5. AD状态为运行状态。



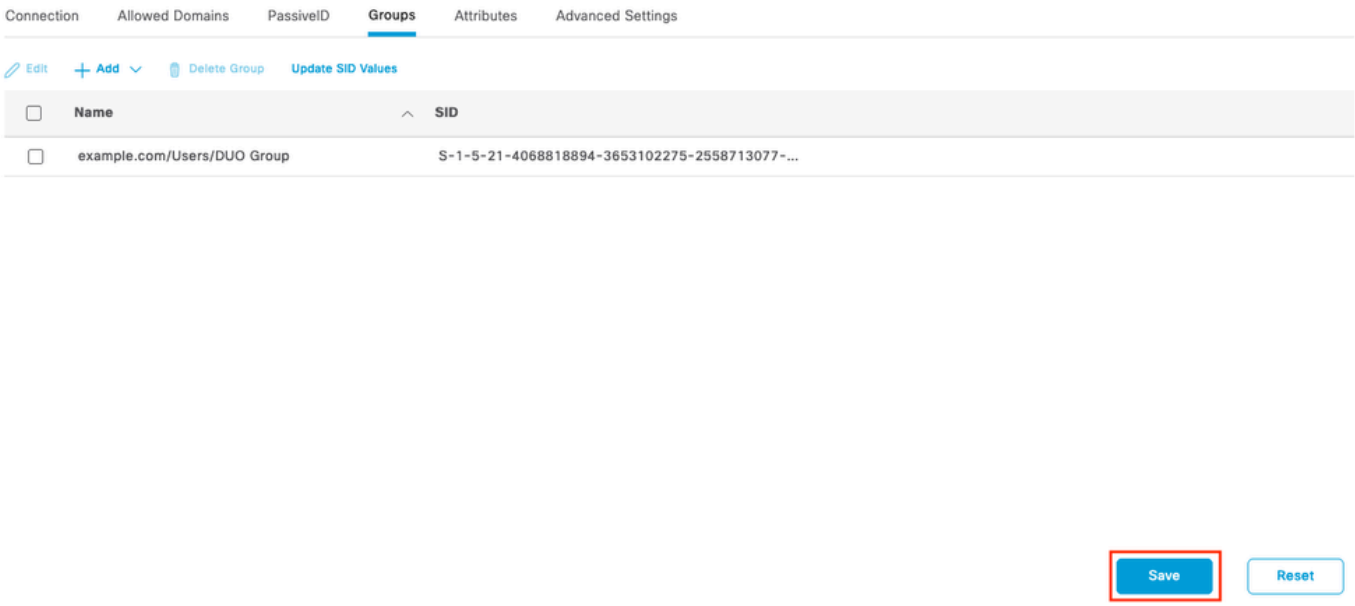
Active Directory 4

6.定位至组>添加>从目录选择>检索组。选中您选择的AD组的复选框（用于同步用户和授权策略）：



Active Directory 5

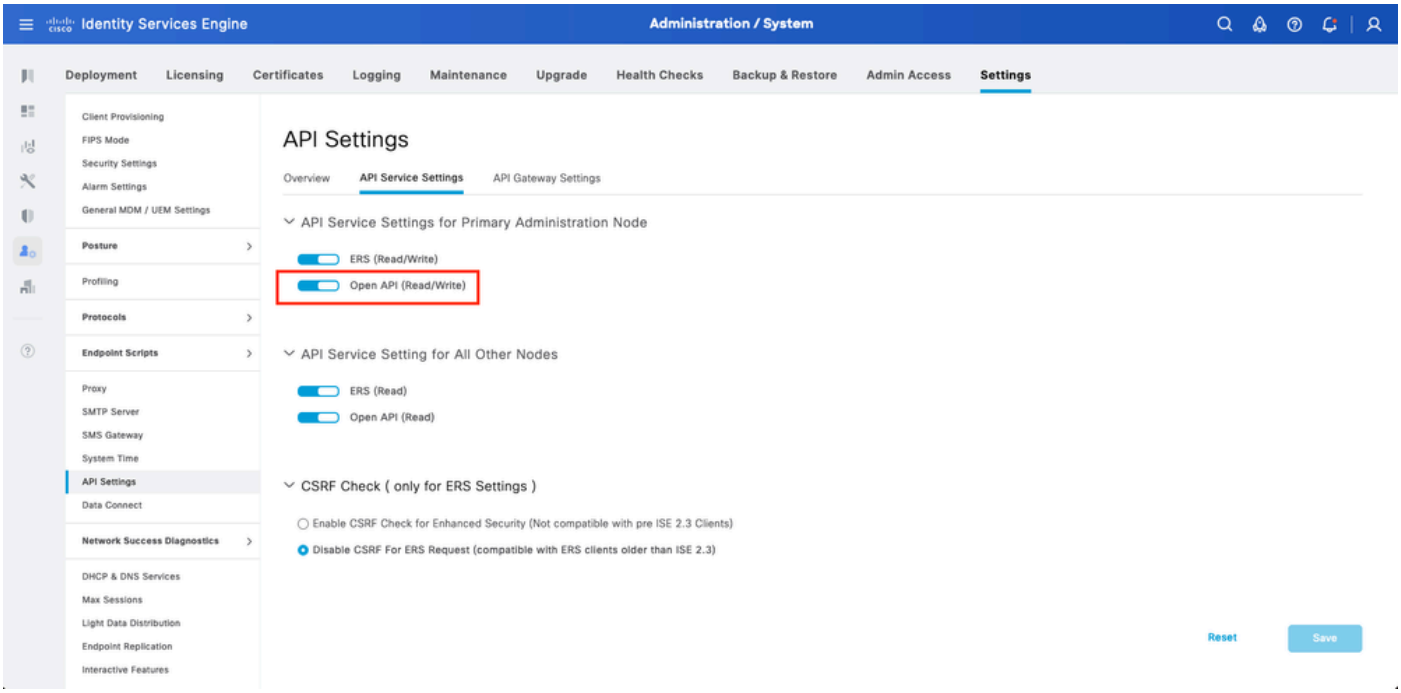
7.单击保存以保存检索到的AD组。



Active Directory 6

启用开放式API

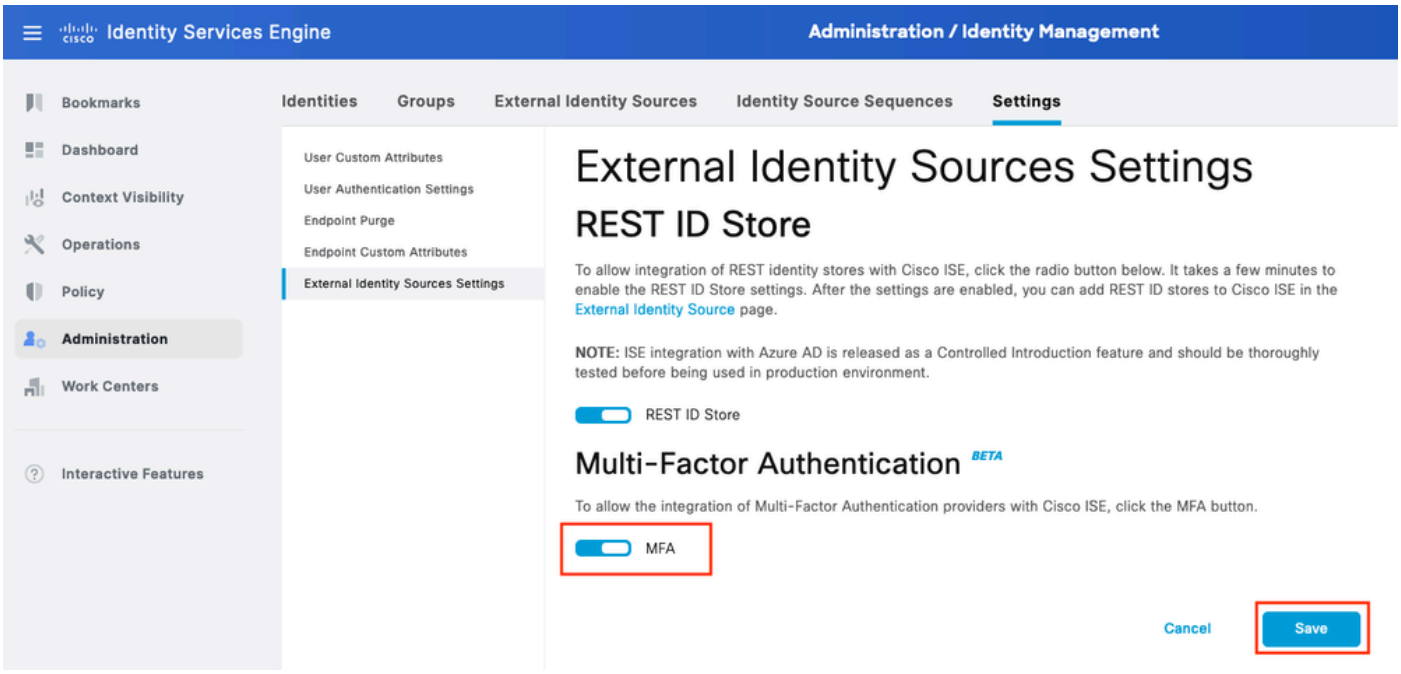
1. 导航到Administration > System > Settings > API Settings > API Service Settings。启用Open API并点击Save。



开放式API

启用MFA身份源

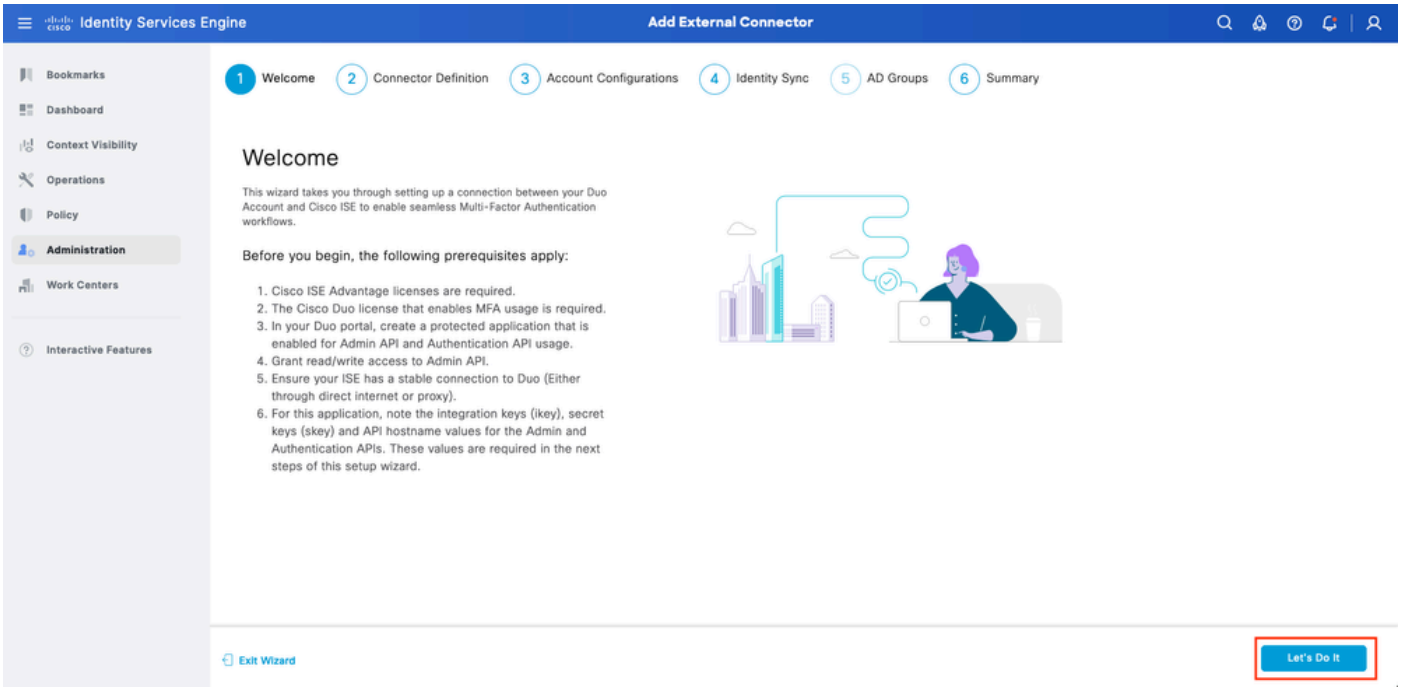
1. 导航到管理>身份管理>设置> 外部身份源设置。启用MFA，然后单击Save。



ISE MFA 1

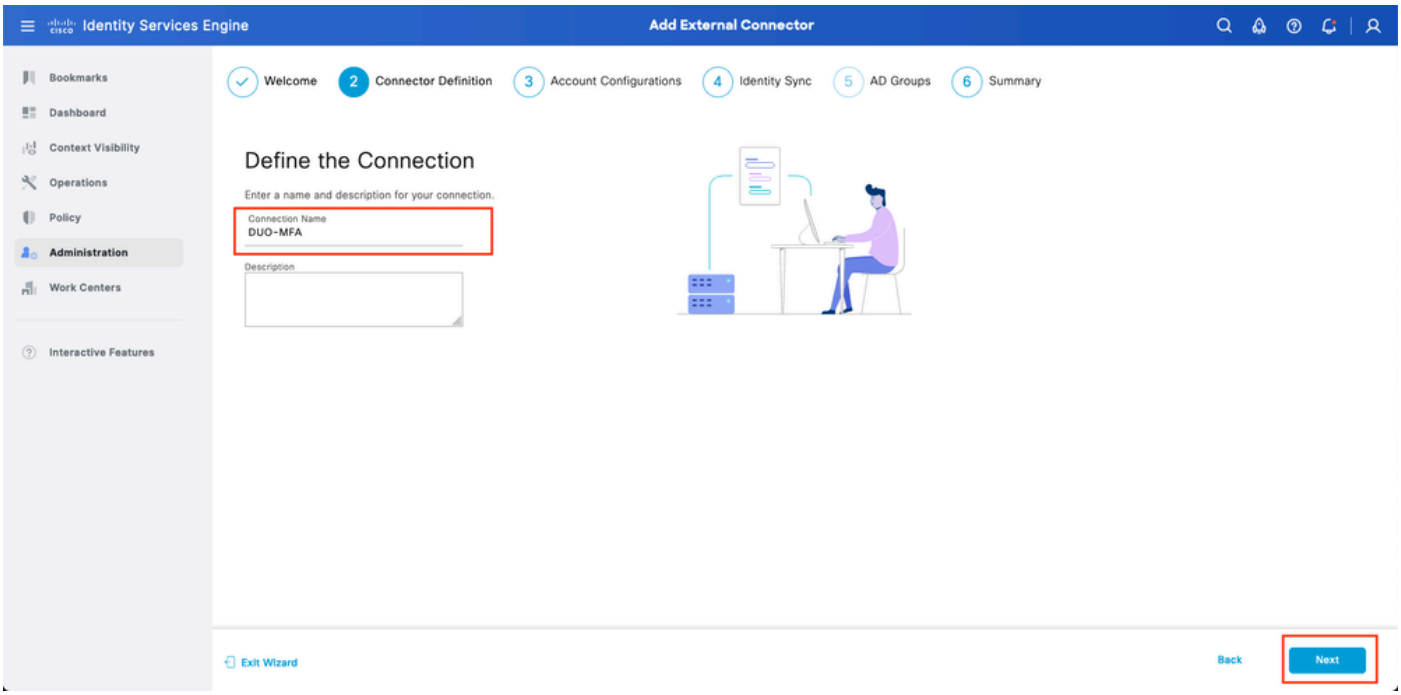
配置MFA外部身份源

1. 导航到管理>身份管理>外部身份源。单击Add，然后在“Welcome Screen”中单击Let's Do It。



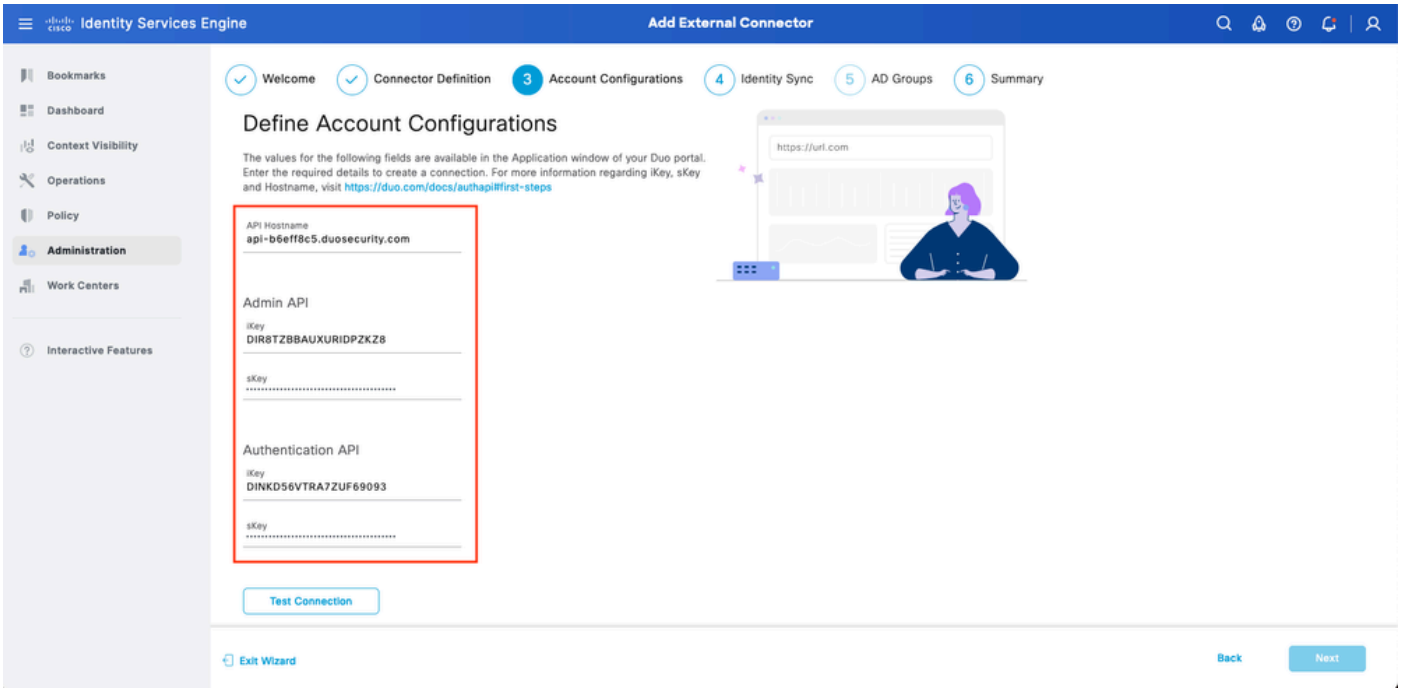
ISE Duo向导1

2.在下一个屏幕上，配置Connection Name并单击Next。



ISE Duo向导2

3.配置API主机名、Cisco ISE管理API集成、密钥、Cisco ISE身份验证API集成和密钥的值(从选择应用到Protect步骤)。



ISE Duo向导3

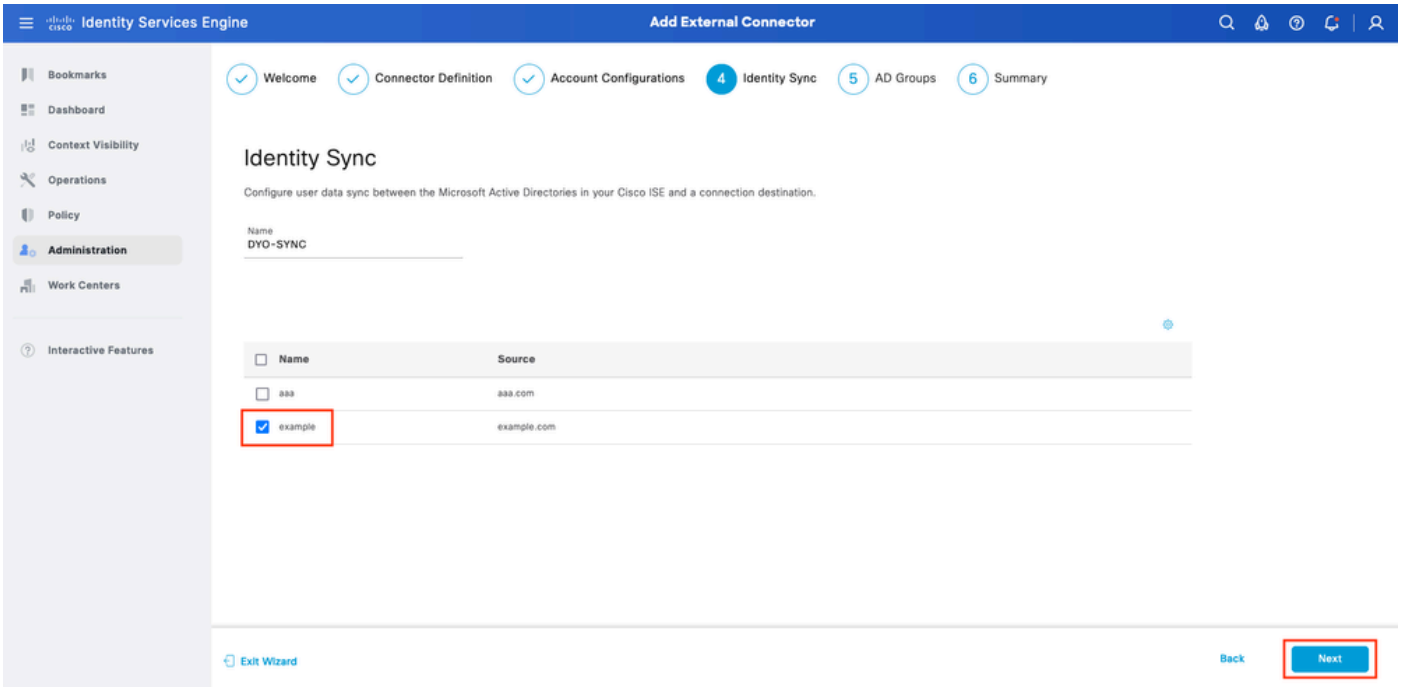
4.单击测试连接，一旦测试连接成功，请单击下一步。



ISE Duo向导4

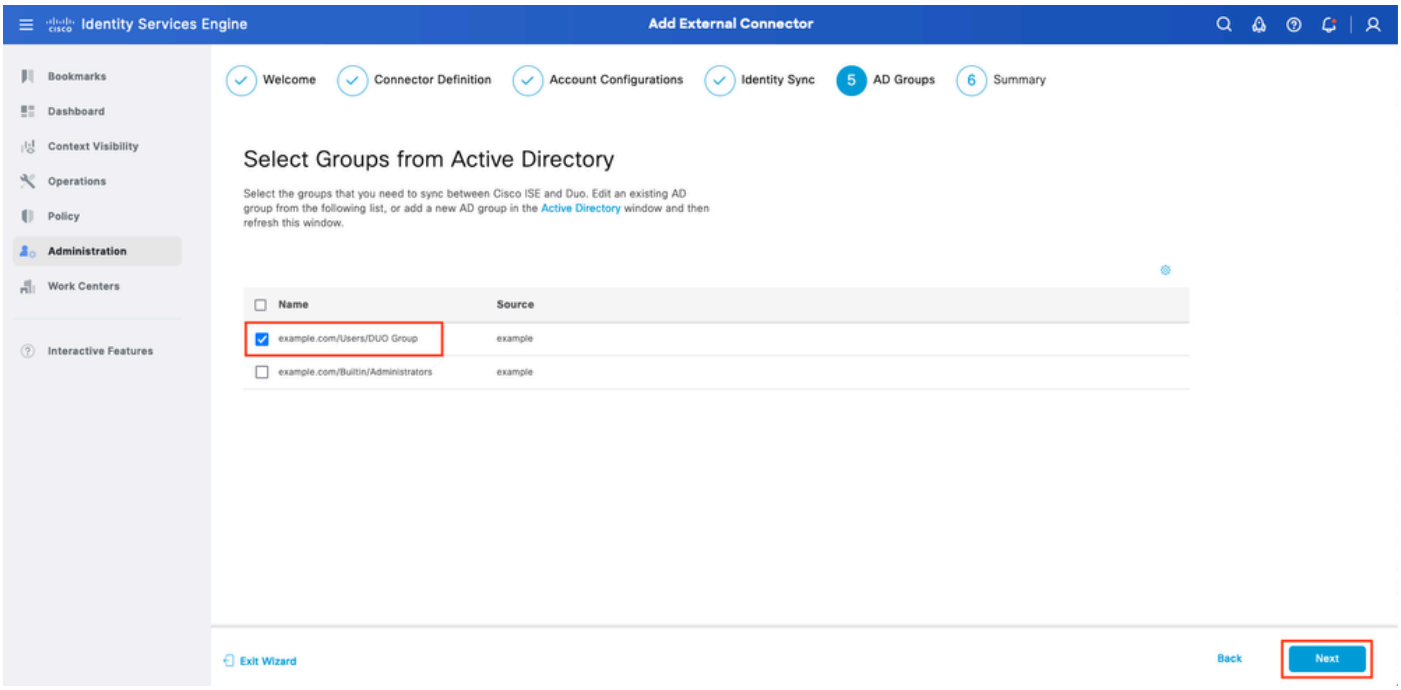
5.配置身份同步。此过程将使用之前提供的API凭证将您选择的Active Directory组中的用户同步到双核帐户。选择Active Directory加入点，然后单击下一步。

注意：Active Directory配置不在本文档范围内，请参阅此文档将ISE与Active Directory集成。



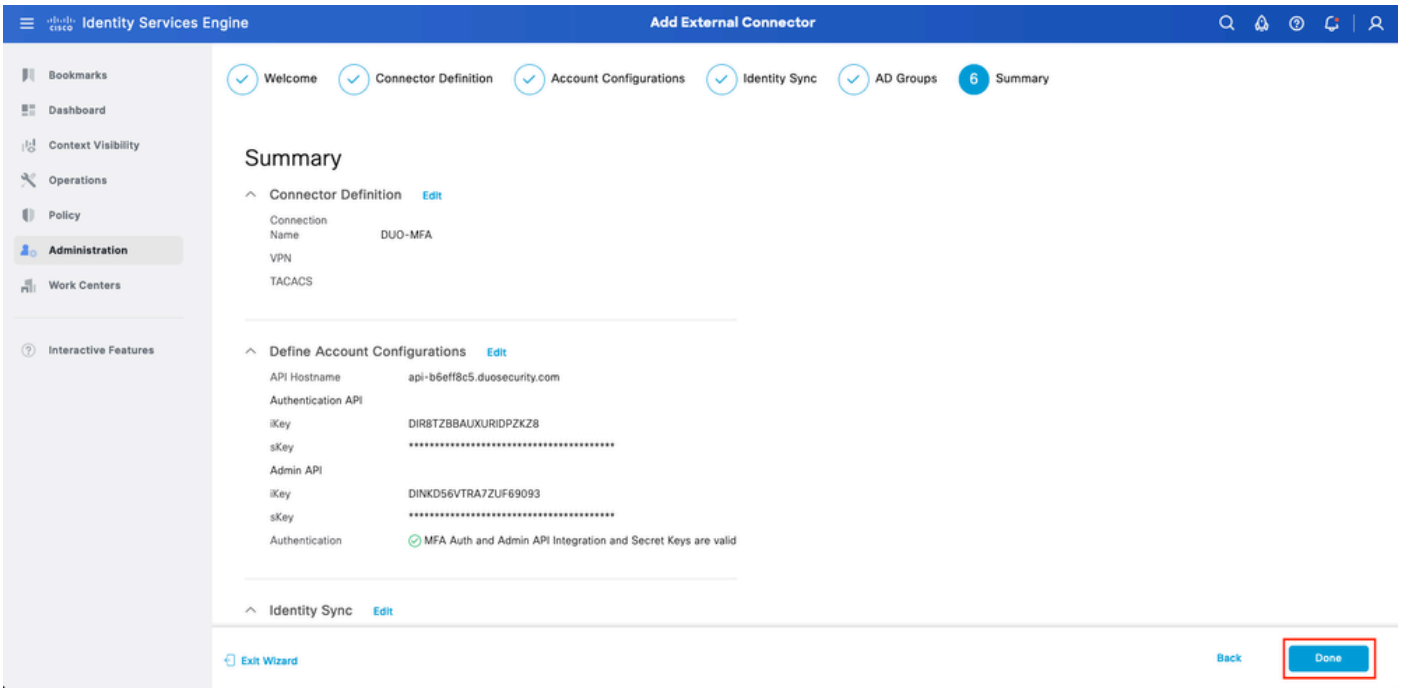
ISE Duo向导5

6.选择Active Directory Groups，用户要在其中与Duo同步。单击 Next。



ISE Duo向导6

7.验证设置是否正确，然后单击完成。



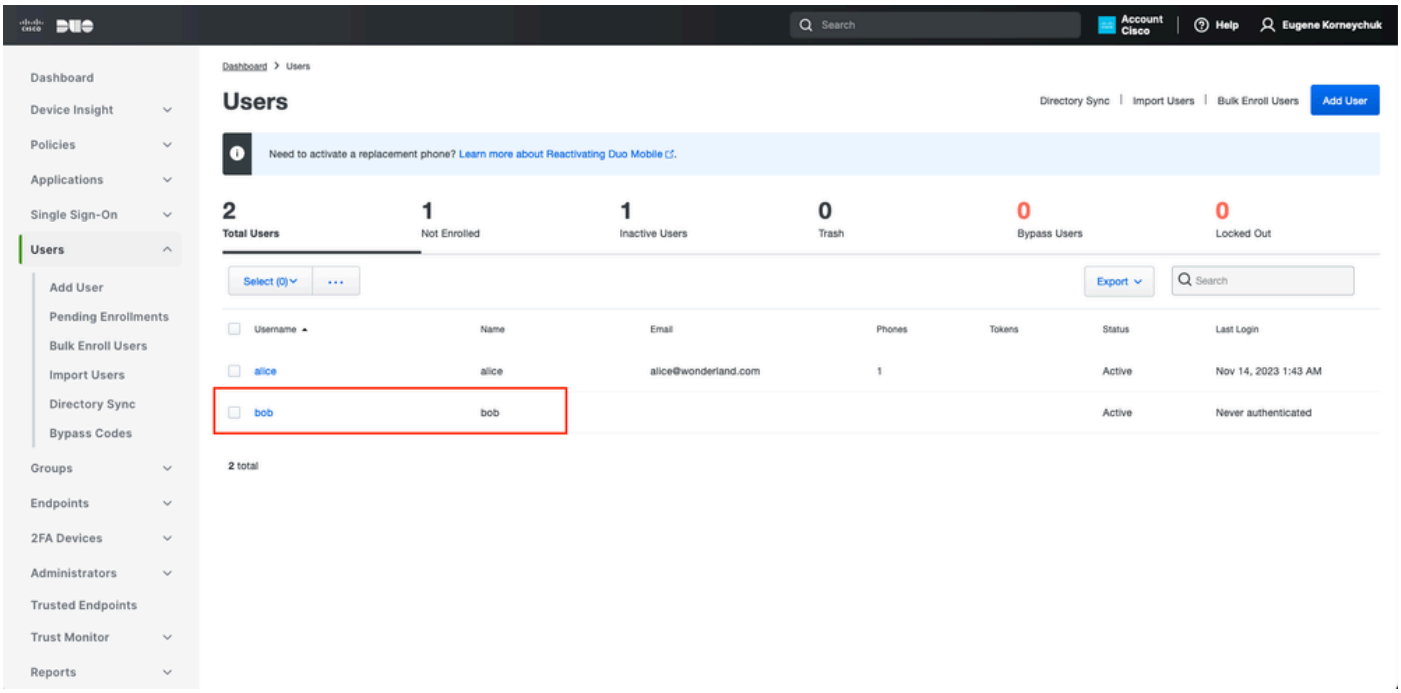
ISE Duo向导7

将用户注册到Duo

注意：双用户注册不在本文档的讨论范围之内，请参阅本文档以了解有关注册用户的更多信息。本文档使用手动用户注册。

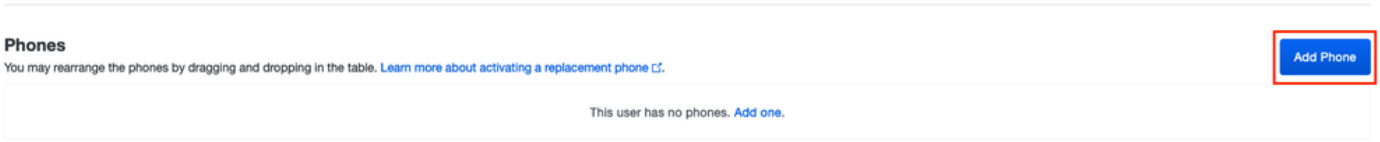
1.打开Duo Admin Dashboard并导航到Dashboard > Users。

2.点击从ISE同步的用户。



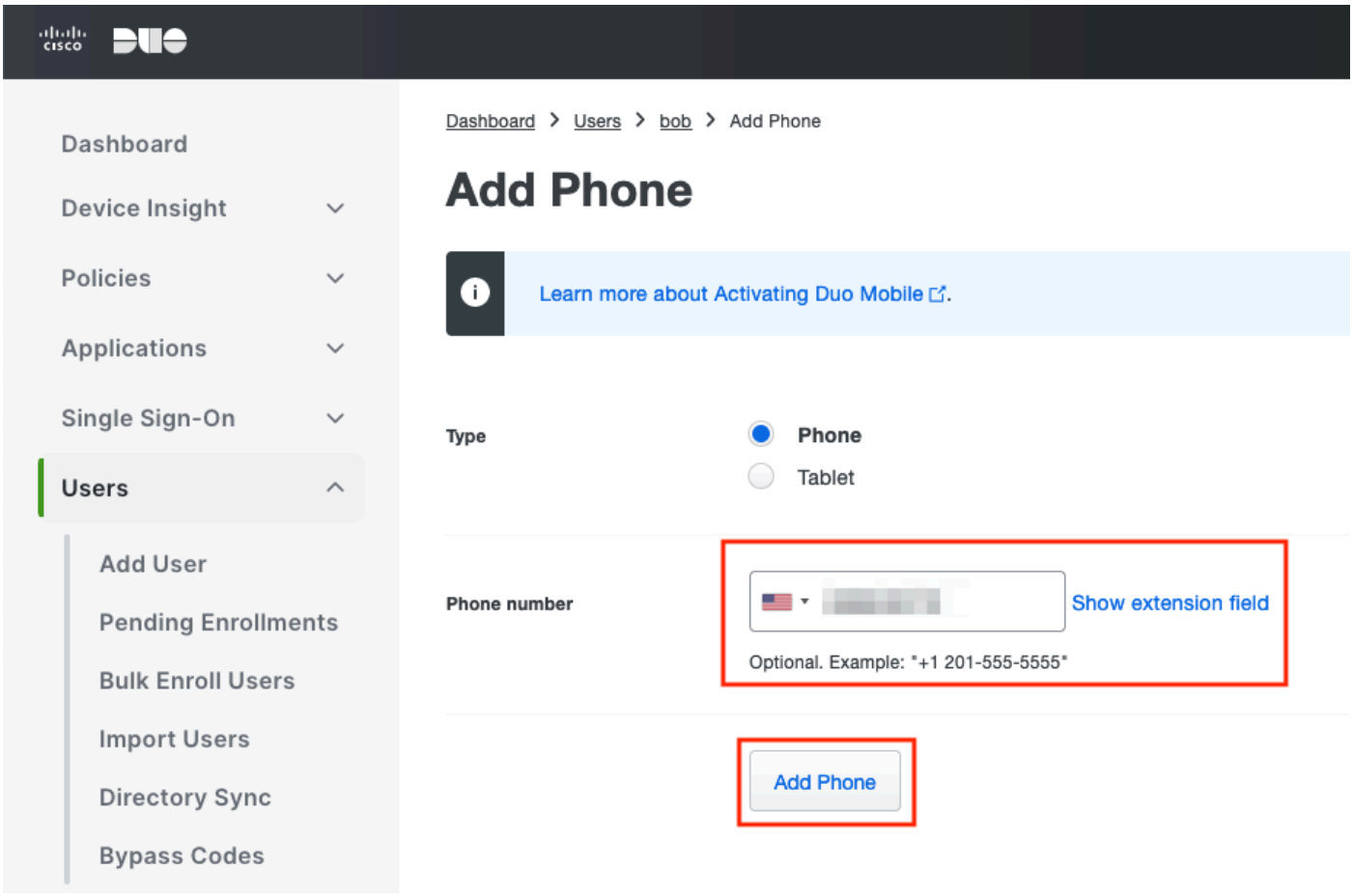
Duo注册1

3.向下滚动到Phones，然后单击Add Phone。



Duo注册2

4.输入电话号码，然后单击添加电话。

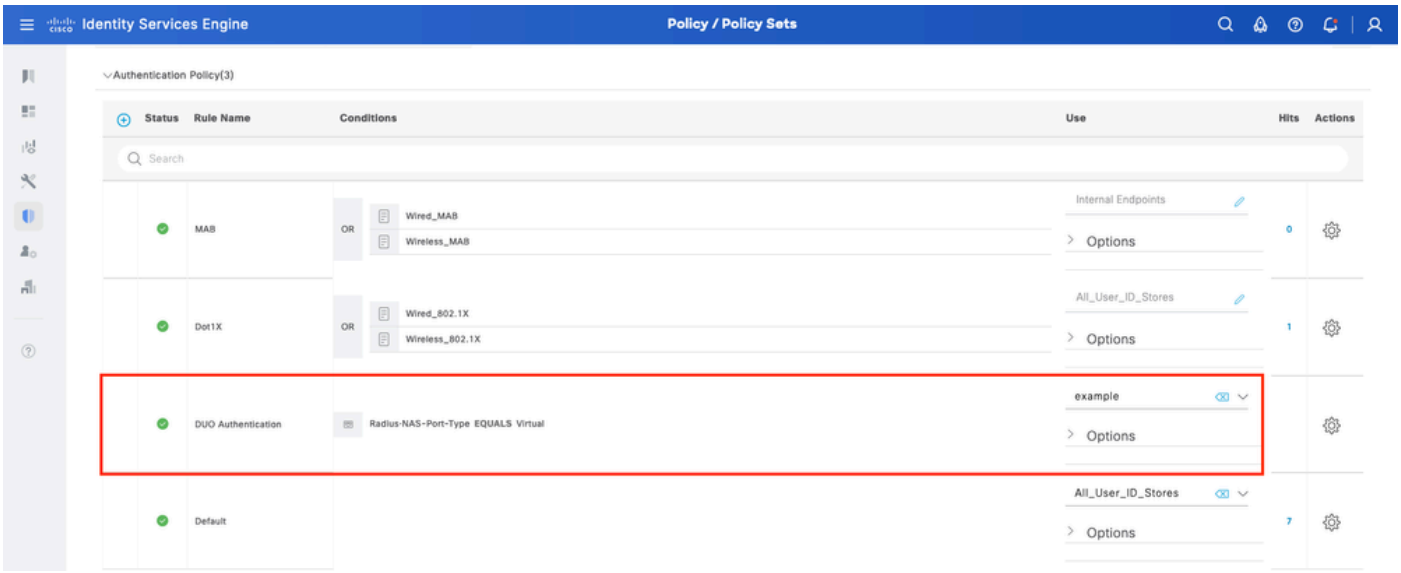


Duo注册3

配置策略集

配置身份验证策略

1.定位至策略>策略集，然后选择要在其中启用MFA的策略集。将主身份验证身份库配置为Active Directory的身份验证策略。

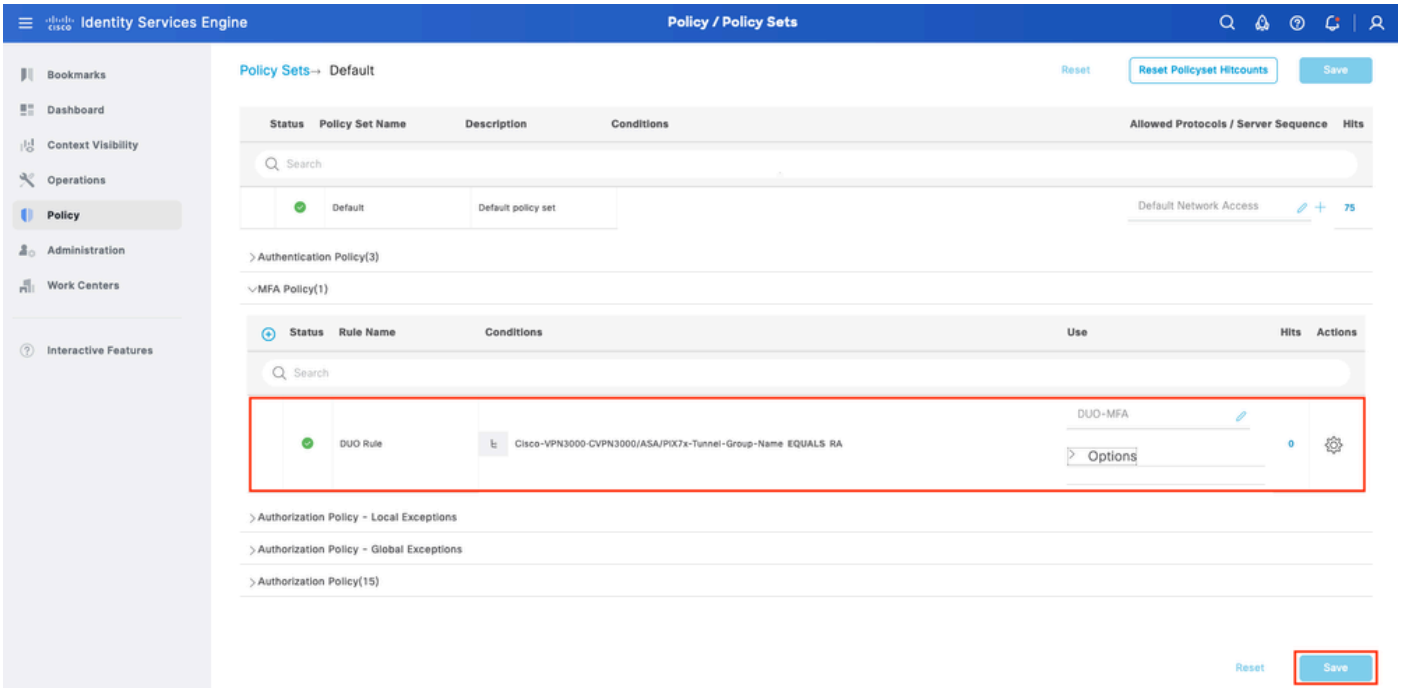


策略集1

配置MFA策略

1.在ISE上启用MFA后，ISE策略集中会出现一个新部分。展开MFA Policy，然后单击+以添加MFA Policy。通过选择之前在使用部分配置的DUO-MFA配置您选择的MFA条件。

2.单击Save。

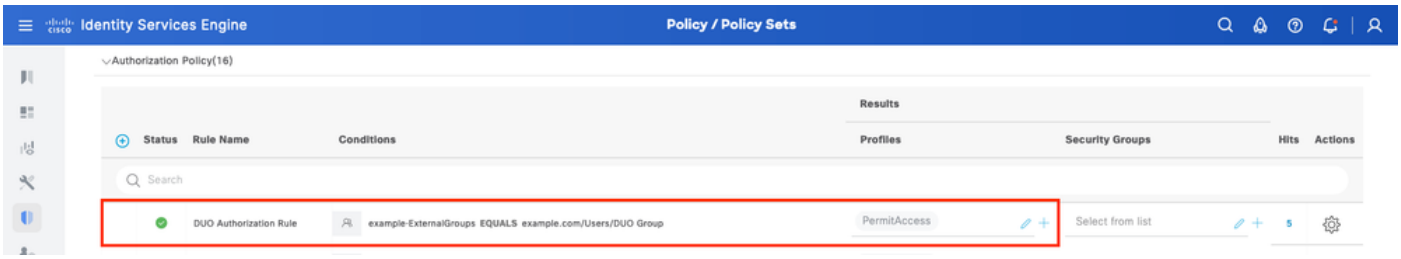


ISE策略

注意：以前配置的策略依赖于名为RA的隧道组。连接到RA隧道组的用户将被强制执行MFA。ASA/FTD配置不在本文档的讨论范围之内。请参阅此文档以配置ASA/FTD。

配置授权策略

1.使用您选择的Active Directory组条件和权限配置授权策略。



策略集3

限制

在本文档中：

1.仅支持Duo推送和电话作为第二因素身份验证方法

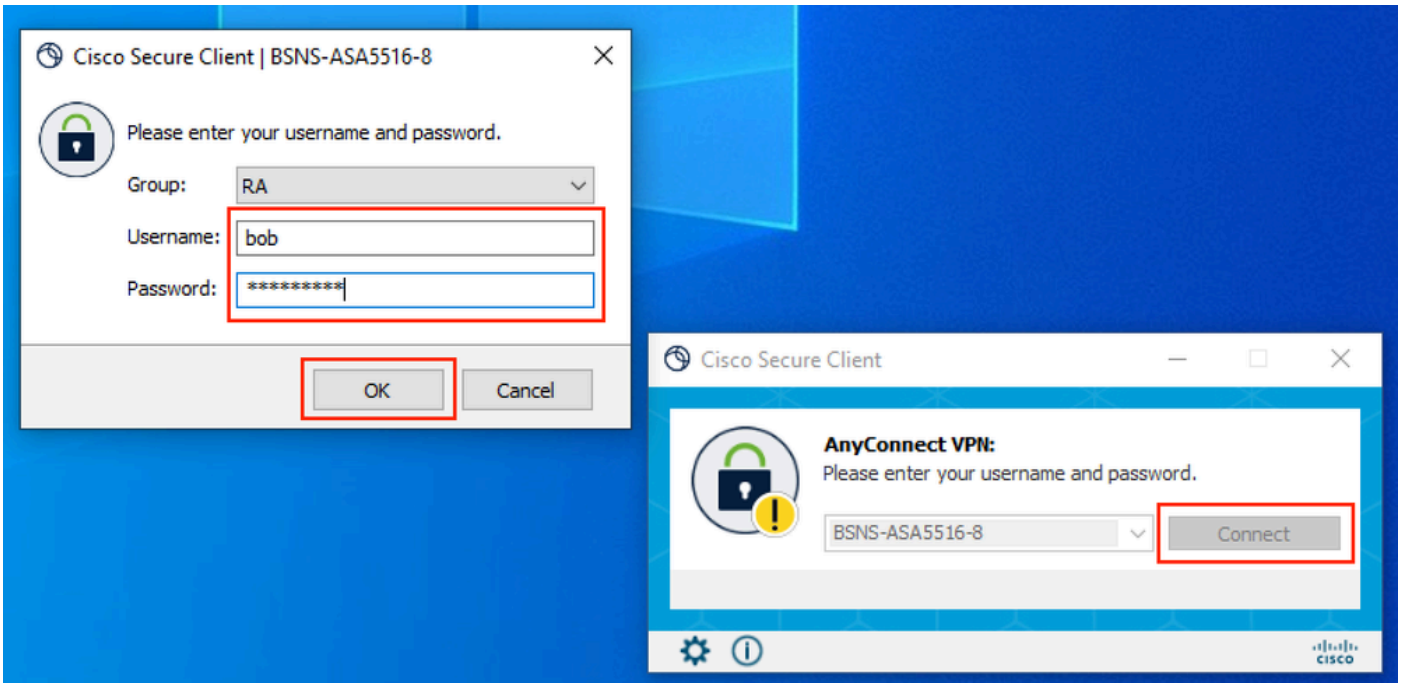
2.未将组推送到双核云，仅支持用户同步

3.这些因素支持多重身份验证：

- VPN用户身份验证
- TACACS+管理员访问身份验证

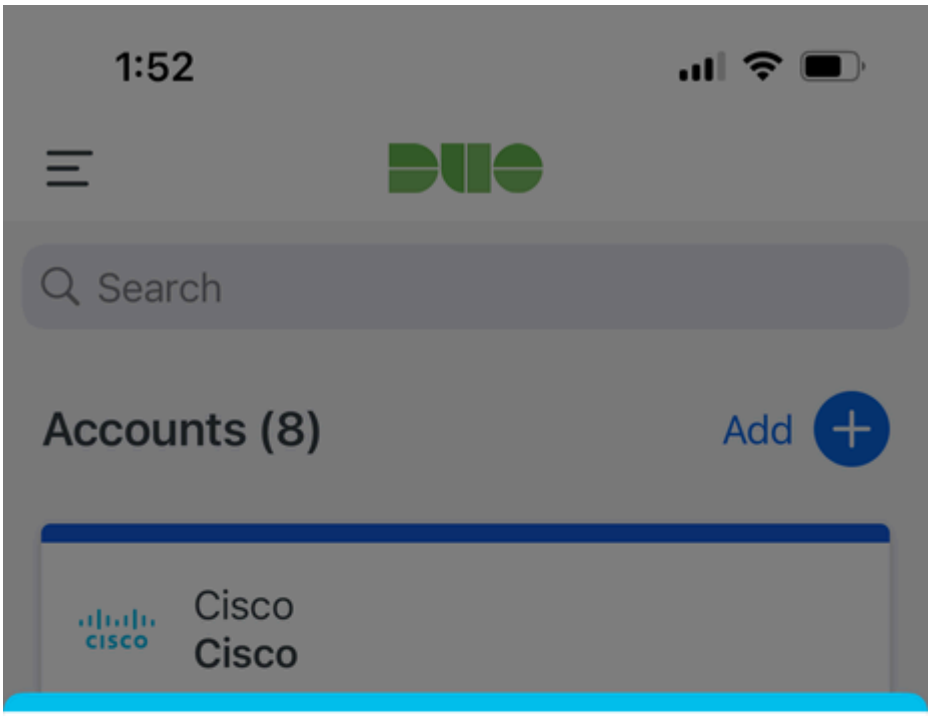
验证

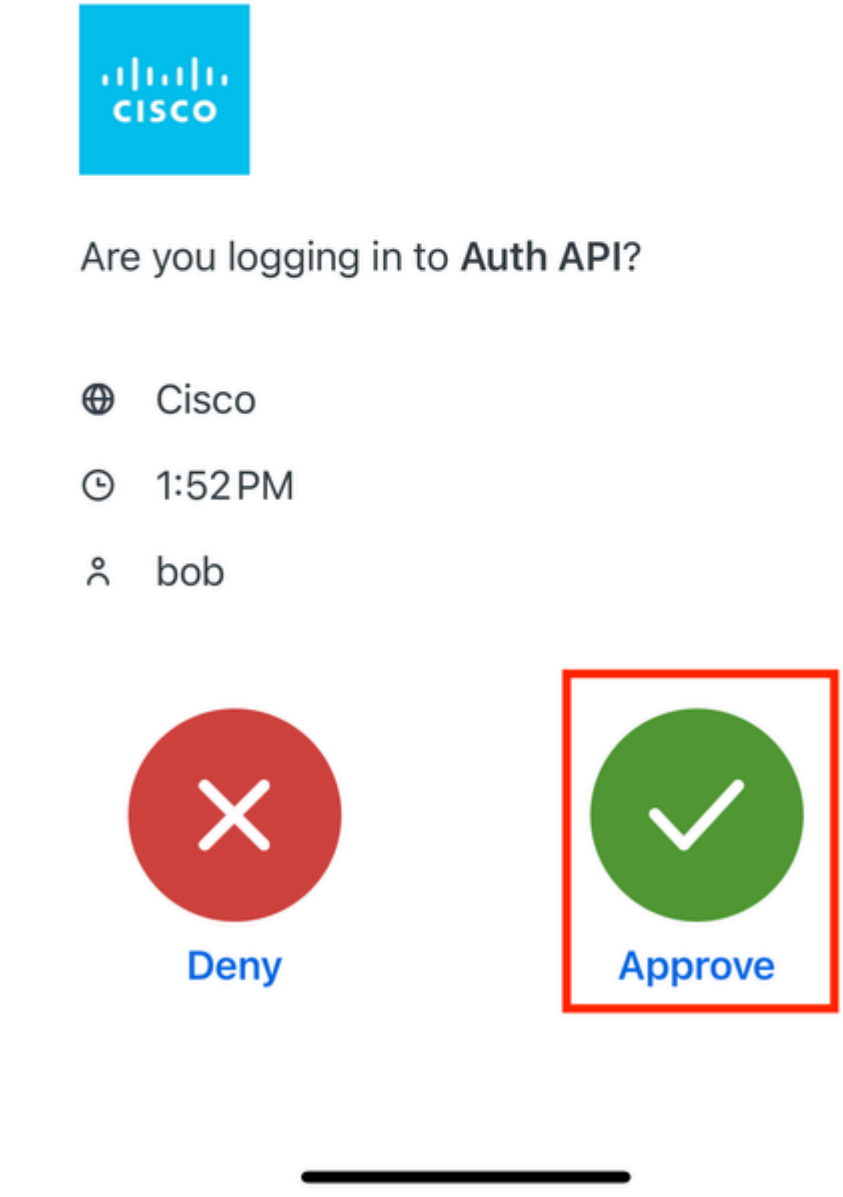
1.打开Cisco Secure Client，单击Connect，并提供Username和Password，然后单击OK。



VPN 客户

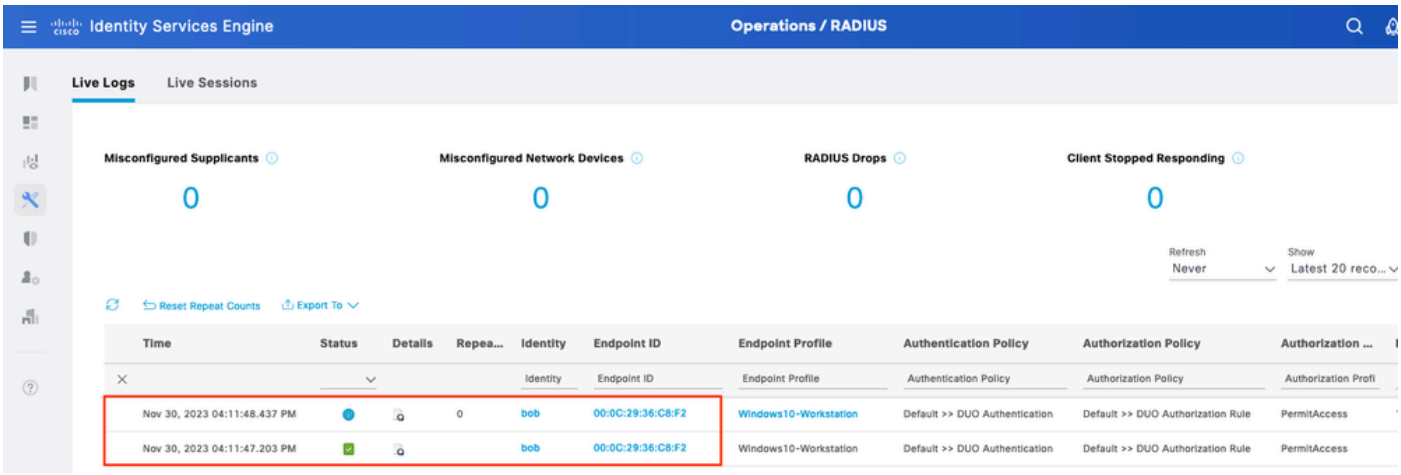
2.用户的移动设备必须收到Duo Push通知。审批并建立VPN连接。


1:52
Search
Accounts (8)
Add
Cisco
Cisco


Are you logging in to Auth API?
Cisco
1:52 PM
bob
Deny
Approve

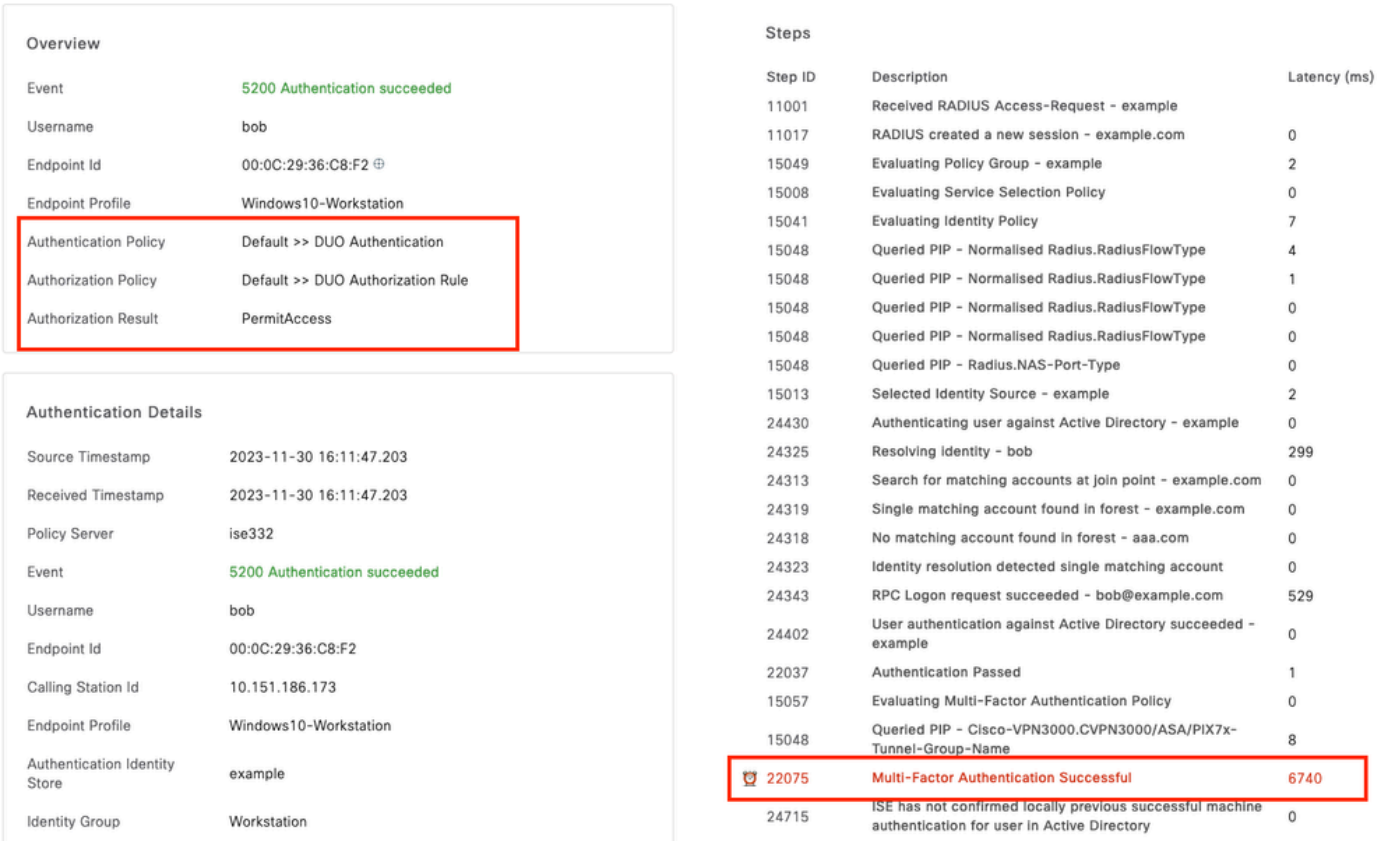
Duo推送

3.导航至ISE Operations > Live Logs以确认用户身份验证。



实时日志1

4.单击“详细信息身份验证报告”，验证身份验证策略、授权策略和授权结果。滚动浏览右侧的步骤。要确认MFA成功，必须存在MultiFactor Authentication is Successful行：



实时日志2

故障排除

在ISE上启用的调试：

使用案例	日志组件	日志文件	关键日志消息
MFA相关日志	策略引擎	ise-psc.log	DuoMfaAuthApiUtils -::: — 已向Duo Client Manager提交请求 DuoMfaAuthApiUtils —> Duo响应
策略相关日志	prrt-JNI	prrt-management.log	RadiusMfaPolicyRequestProcessor TacacsMfaPolicyRequestProcessor
身份验证相关日志	运行时AAA	prrt-server.log	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
Duo身份验证、ID同步相关日志		duo-sync-service.log	

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）。