使用DUO配置ISE 3.3本机多因素身份验证

目录

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。从版本3.3补丁1开始，ISE可配置为与DUO服务进行本地集成，因此无需身份验证代理。

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

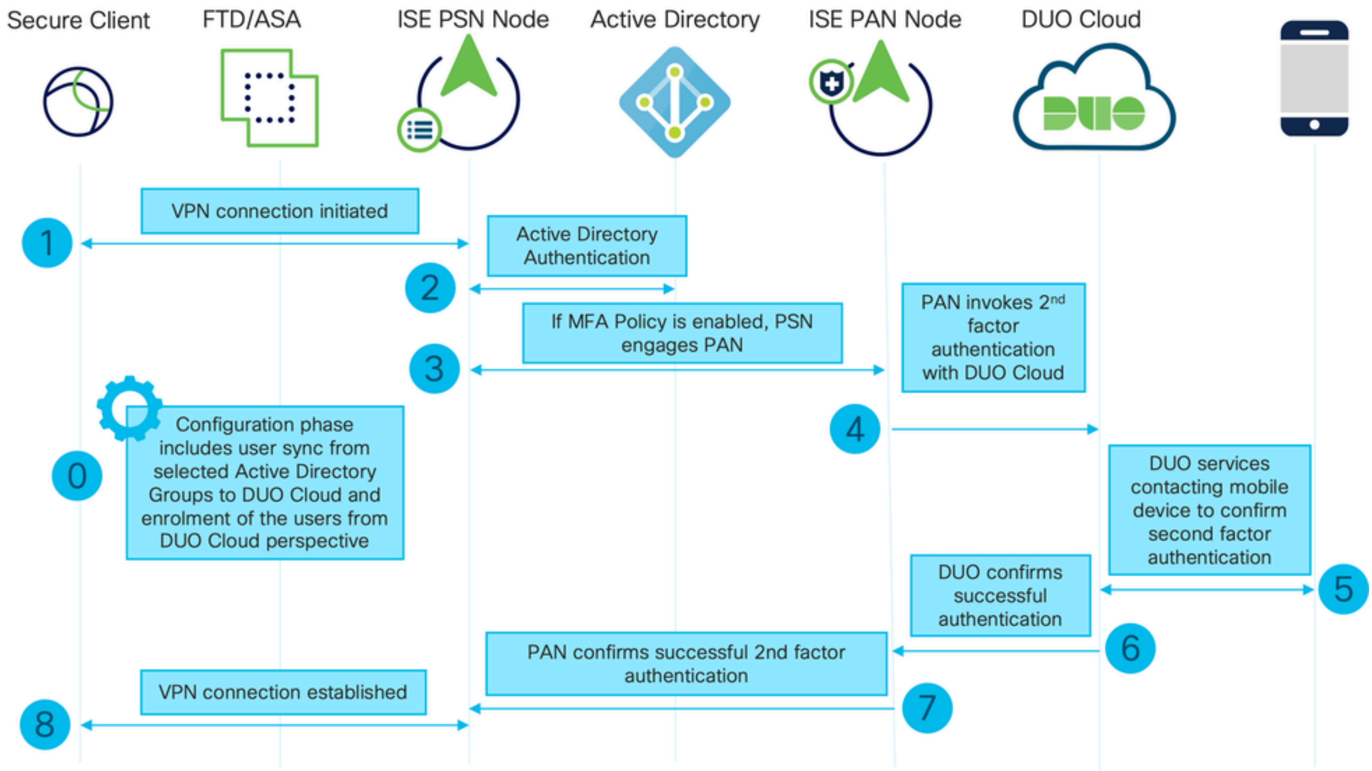
本文档中的信息基于：

- 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


Secure Client
FTD/ASA
ISE PSN Node
Active Directory
ISE PAN Node
DUO Cloud
1
VPN connection initiated
2
Active Directory Authentication
3
If MFA Policy is enabled, PSN engages PAN
PAN invokes 2nd factor authentication with DUO Cloud
4
0
Configuration phase includes user sync from selected Active Directory Groups to DUO Cloud and enrolment of the users from DUO Cloud perspective
DUO services contacting mobile device to confirm second factor authentication
5
DUO confirms successful authentication
6
PAN confirms successful 2nd factor authentication
7
VPN connection established
8

流程图

步骤

0.配置阶段包括选择Active Directory组，用户将从其中进行同步，同步在MFA向导完成之后进行。它由两个步骤组成。查找Active Directory以获取用户和特定属性的列表。通过管理API调用DUO云可将用户推送到那里。管理员需要注册用户。注册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的一键身份验证

1.启动VPN连接，用户输入用户名和密码，然后点击OK。网络设备发送RADIUS访问请求发送到PSN

2. PSN节点通过Active Directory对用户进行身份验证

3.身份验证成功并配置MFA策略后，PSN会与PAN接洽，以便联系DUO云

4.通过身份验证API调用DUO Cloud，以调用使用DUO的二次身份验证。ISE在SSL TCP端口443上与Duo的服务通信。

5.进行第二因素身份验证。用户完成第二因素身份验证过程

6. DUO通过第二因素身份验证的结果响应PAN

7. PAN使用第二因素身份验证的结果响应PSN

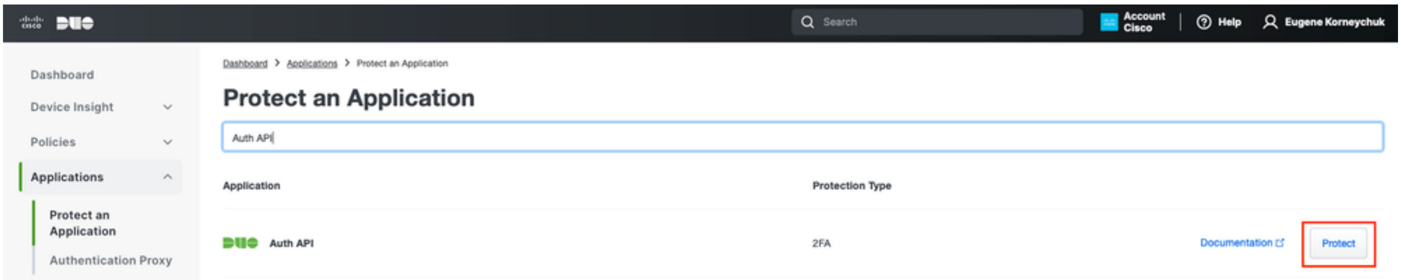
8.将Access-Accept发送到网络设备，建立VPN连接

配置

选择要保护的应用

导航至DUO管理控制面板https://admin.duosecurity.com/login。使用管理员凭证登录。

导航到控制面板>应用>保护应用。查找Auth API并选择Protect。



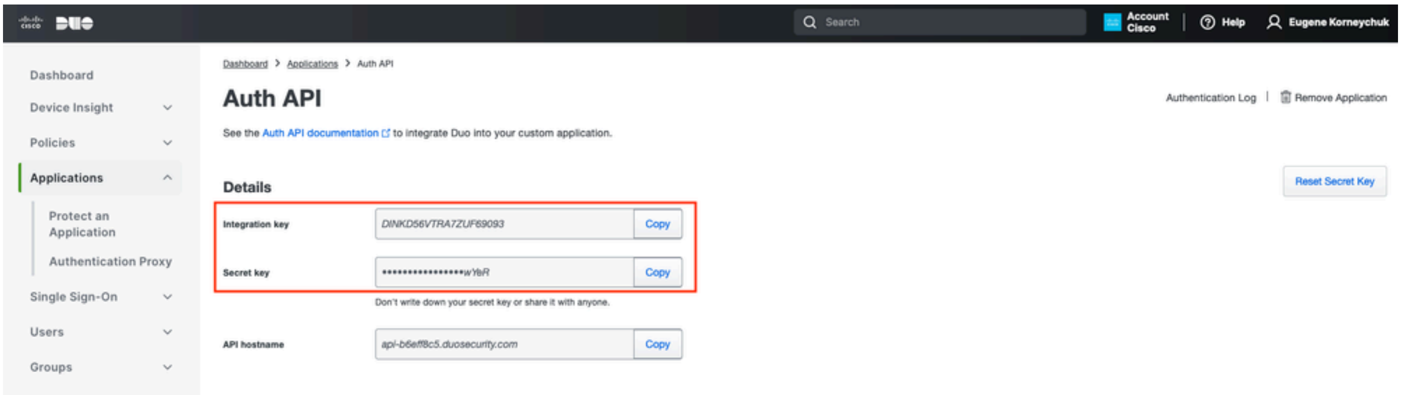
Protect an Application

Auth API

Application	Protection Type		
Auth API	2FA	Documentation	Protect

身份验证API 1

记下Integration密钥和Secret密钥。



Auth API

See the Auth API documentation to integrate Duo into your custom application.

Details

Integration key: DINKD56VTRA7ZUF69093

Secret key: ****************wYbR

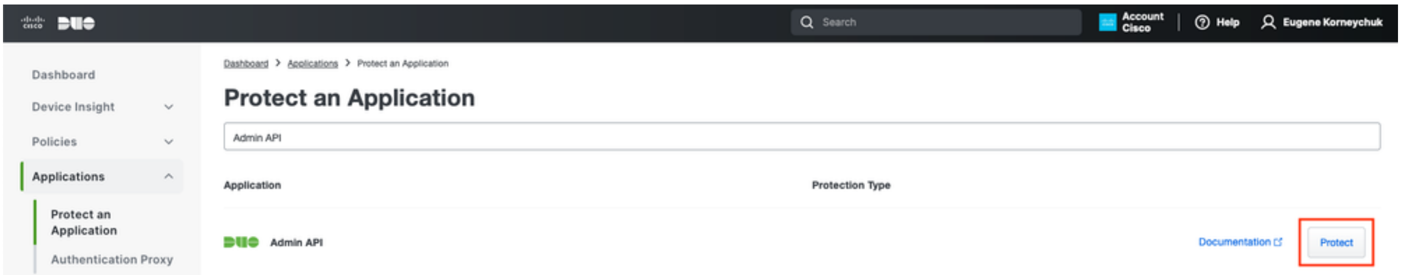
Don't write down your secret key or share it with anyone.

API hostname: api-b6eff8c5.duosecurity.com

身份验证API 2

导航到控制面板>应用>保护应用。查找Admin API并选择Protect。

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



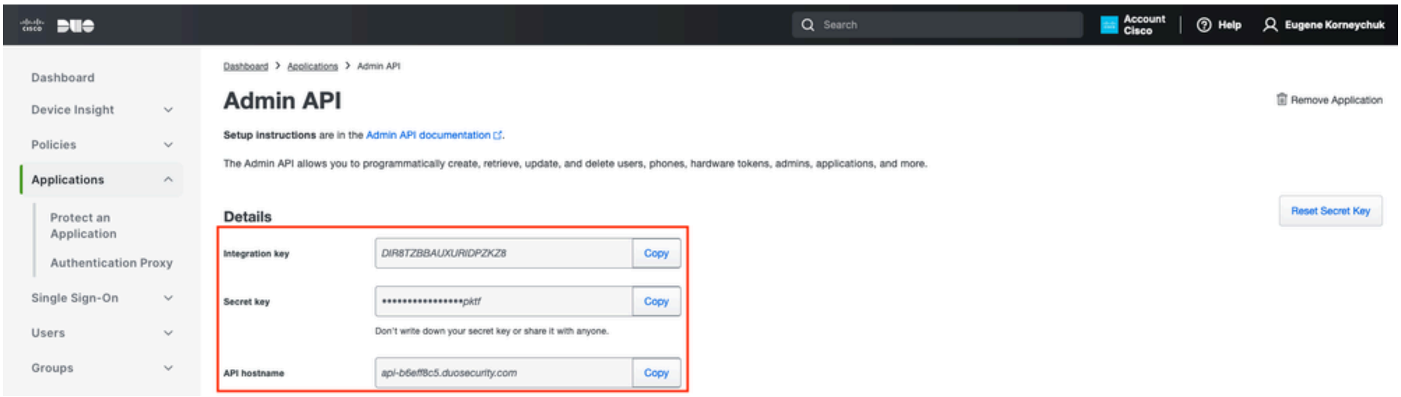
Protect an Application

Admin API

Application	Protection Type		
Admin API		Documentation	Protect

身份验证API 1

记下集成密钥和密钥以及API主机名。



Admin API

Setup instructions are in the Admin API documentation.

The Admin API allows you to programmatically create, retrieve, update, and delete users, phones, hardware tokens, admins, applications, and more.

Details

Integration key: DIR8TZBBAUXURIDPZKZ8

Secret key: ••••••••••••••••pktf

Don't write down your secret key or share it with anyone.

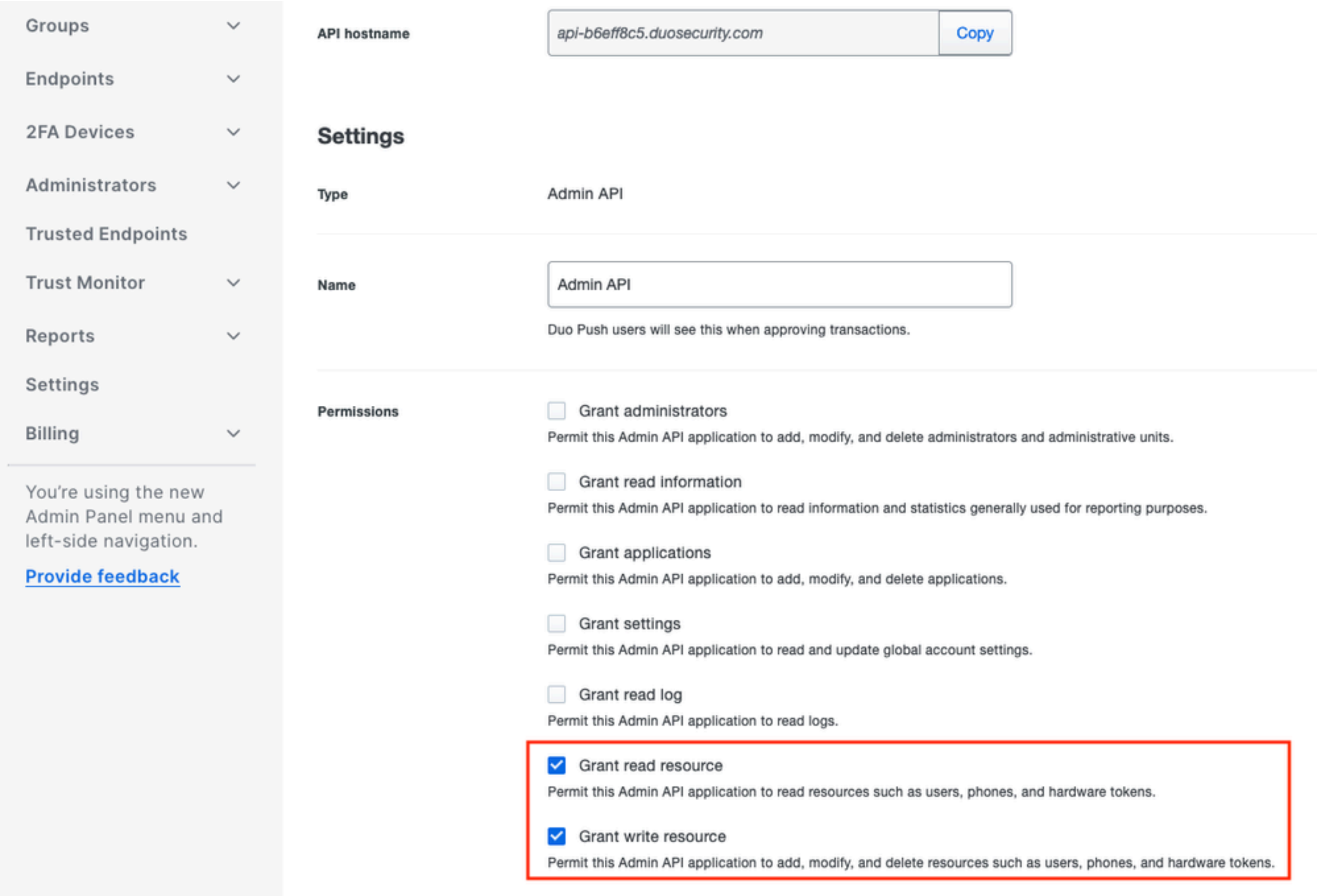
API hostname: api-b6eff8c5.duosecurity.com

管理API 2

配置API权限

导航到控制面板>应用>应用。选择Admin API。

选中授予读取资源和授予写入资源权限。单击Save Changes。



You're using the new Admin Panel menu and left-side navigation.

Provide feedback

API hostname: api-b6eff8c5.duosecurity.com

Settings

Type: Admin API

Name: Admin API

Duo Push users will see this when approving transactions.

Permissions

□ Grant administrators
Permit this Admin API application to add, modify, and delete administrators and administrative units.

□ Grant read information
Permit this Admin API application to read information and statistics generally used for reporting purposes.

□ Grant applications
Permit this Admin API application to add, modify, and delete applications.

□ Grant settings
Permit this Admin API application to read and update global account settings.

□ Grant read log
Permit this Admin API application to read logs.

☑ Grant read resource
Permit this Admin API application to read resources such as users, phones, and hardware tokens.

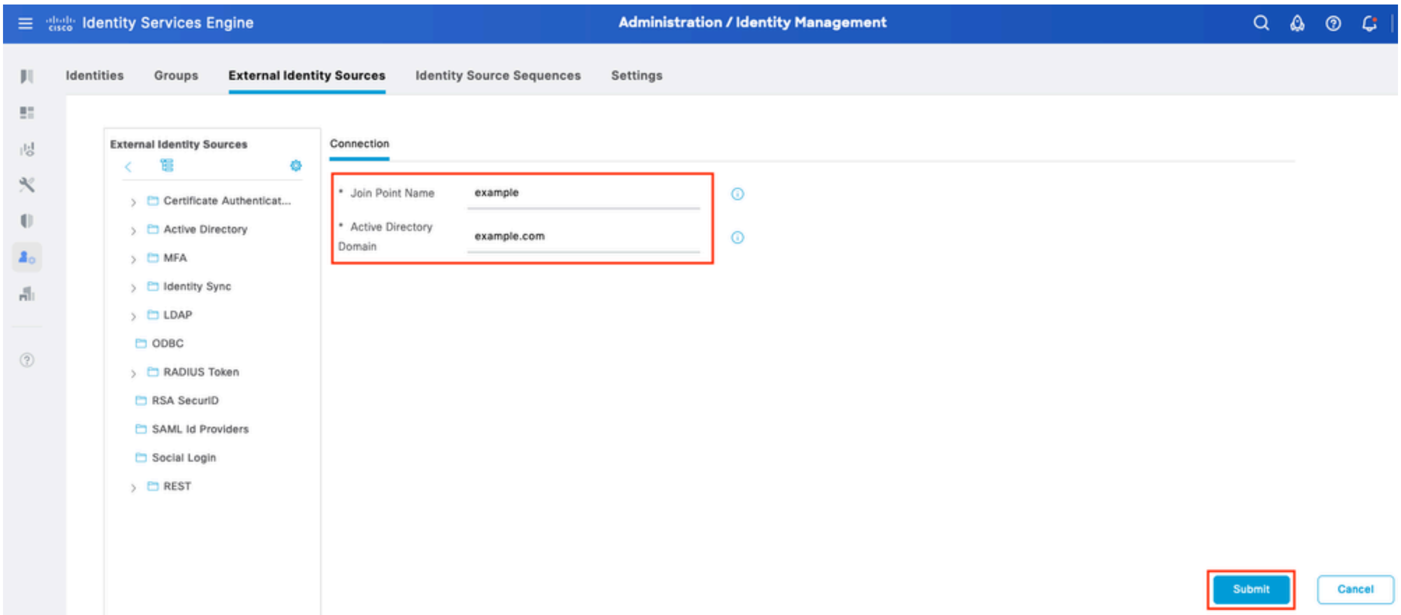
☑ Grant write resource
Permit this Admin API application to add, modify, and delete resources such as users, phones, and hardware tokens.

管理API 3

将ISE与Active Directory集成

1.导航到管理>身份管理>外部身份库> Active Directory >添加。提供加入点名称、Active

Directory域并点击提交。

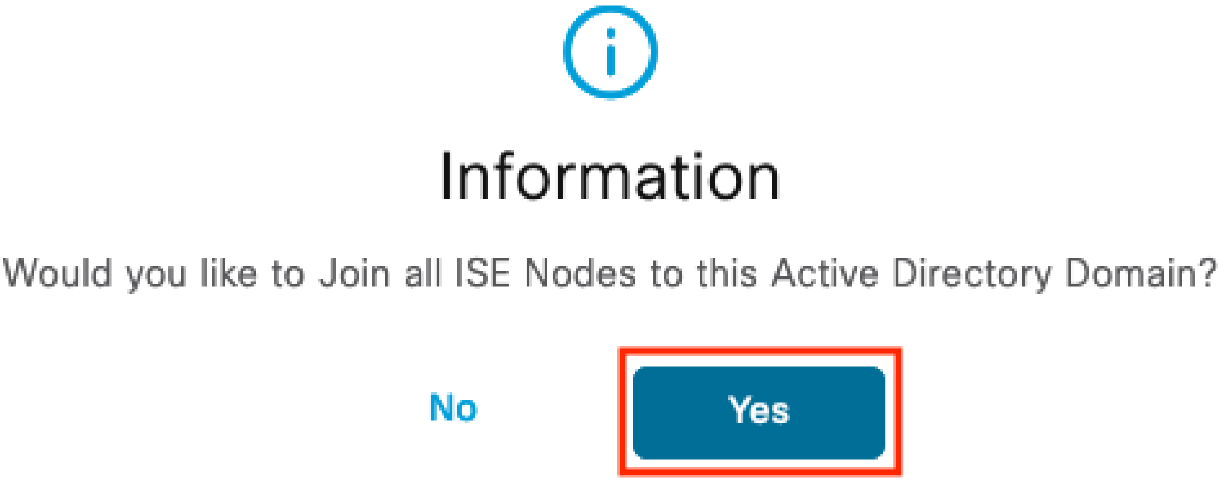


* Join Point Name: example

* Active Directory Domain: example.com

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。

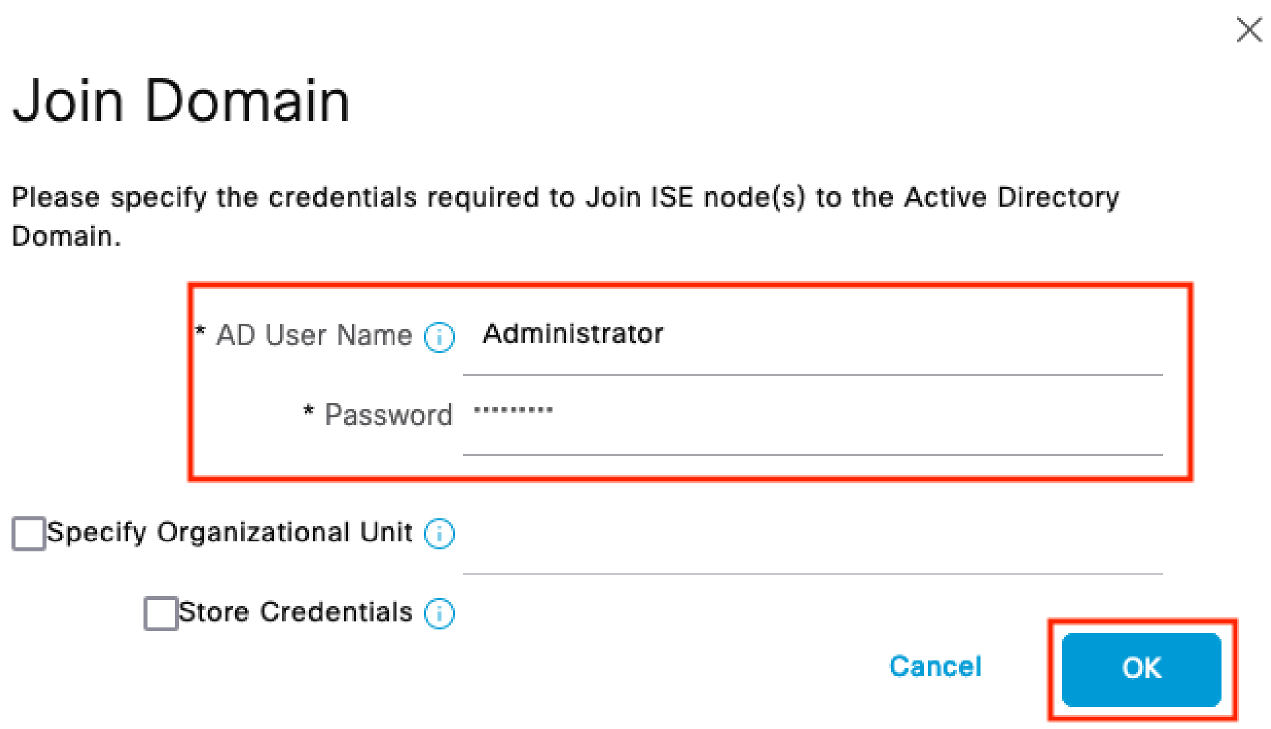


Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

Active Directory 2

3.提供AD用户名和密码，然后点击确定。



Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: Administrator

* Password: ·········

□ Specify Organizational Unit

□ Store Credentials

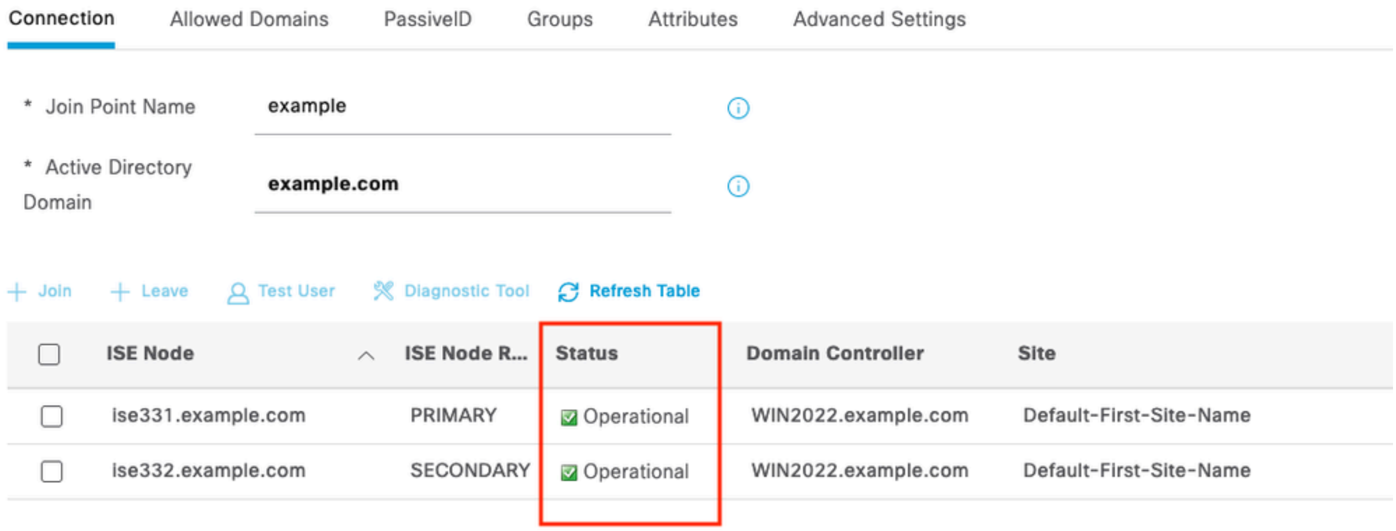
Active Directory 3

在ISE中访问域所需的AD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计算机的帐户后将ISE计算机加入域之前，在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

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。

4. AD状态为运行状态。



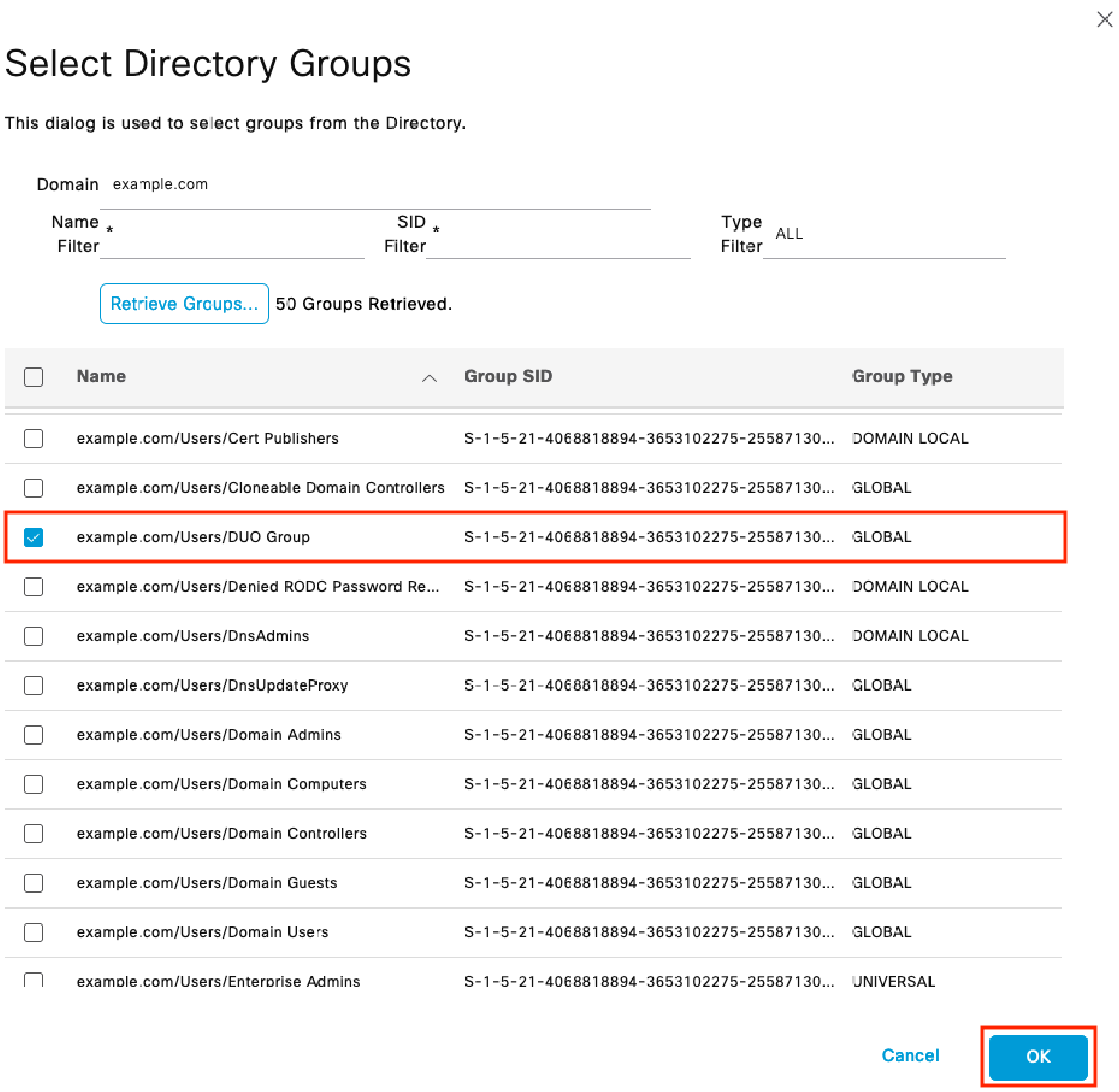
* Join Point Name: example

* Active Directory Domain: example.com

□	ISE Node	ISE Node R...	Status	Domain Controller	Site
□	ise331.example.com	PRIMARY	✓ Operational	WIN2022.example.com	Default-First-Site-Name
□	ise332.example.com	SECONDARY	✓ Operational	WIN2022.example.com	Default-First-Site-Name

Active Directory 4

5.定位至“组”>“添加”>“从目录选择组”>“检索组”。选中与所选的AD组对应的复选框（用于同步用户和授权策略），如下图所示。



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain example.com

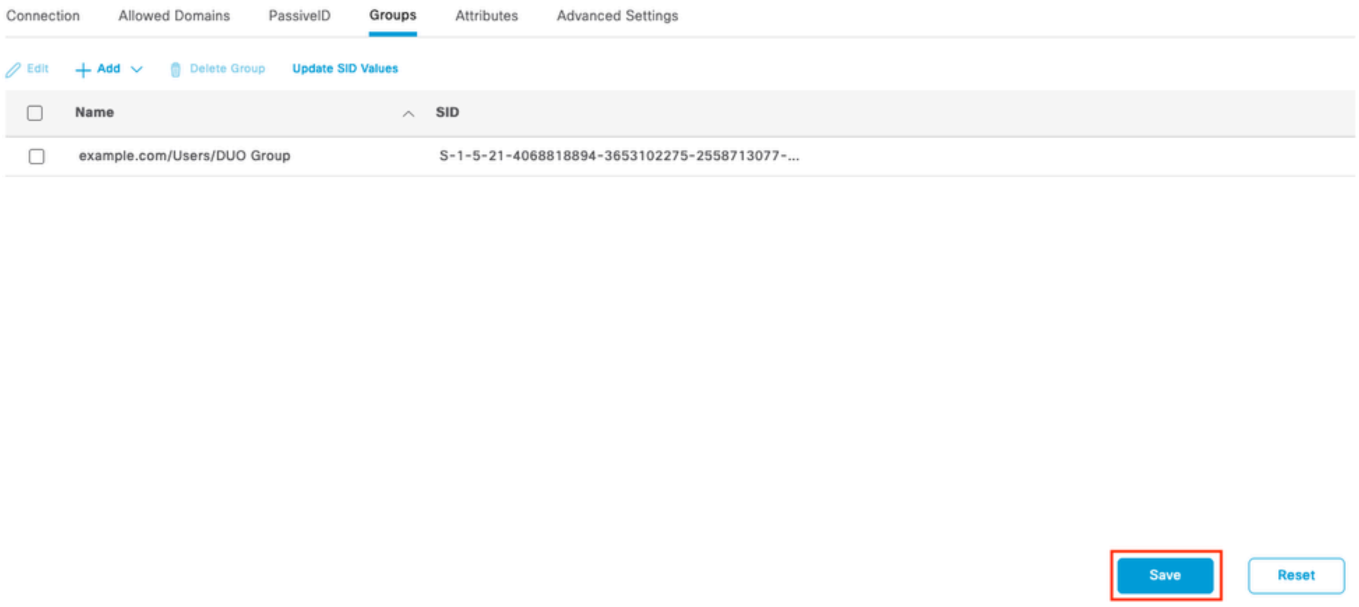
Name Filter *   SID Filter *   Type Filter ALL

Retrieve Groups... 50 Groups Retrieved.

□	Name	Group SID	Group Type
□	example.com/Users/Cert Publishers	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
□	example.com/Users/Cloneable Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
☑	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
□	example.com/Users/Denied RODC Password Re...	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
□	example.com/Users/DnsAdmins	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
□	example.com/Users/DnsUpdateProxy	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
□	example.com/Users/Domain Admins	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
□	example.com/Users/Domain Computers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
□	example.com/Users/Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
□	example.com/Users/Domain Guests	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
□	example.com/Users/Domain Users	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
□	example.com/Users/Enterprise Admins	S-1-5-21-4068818894-3653102275-25587130...	UNIVERSAL

Active Directory 5

6.单击保存以保存检索到的AD组。

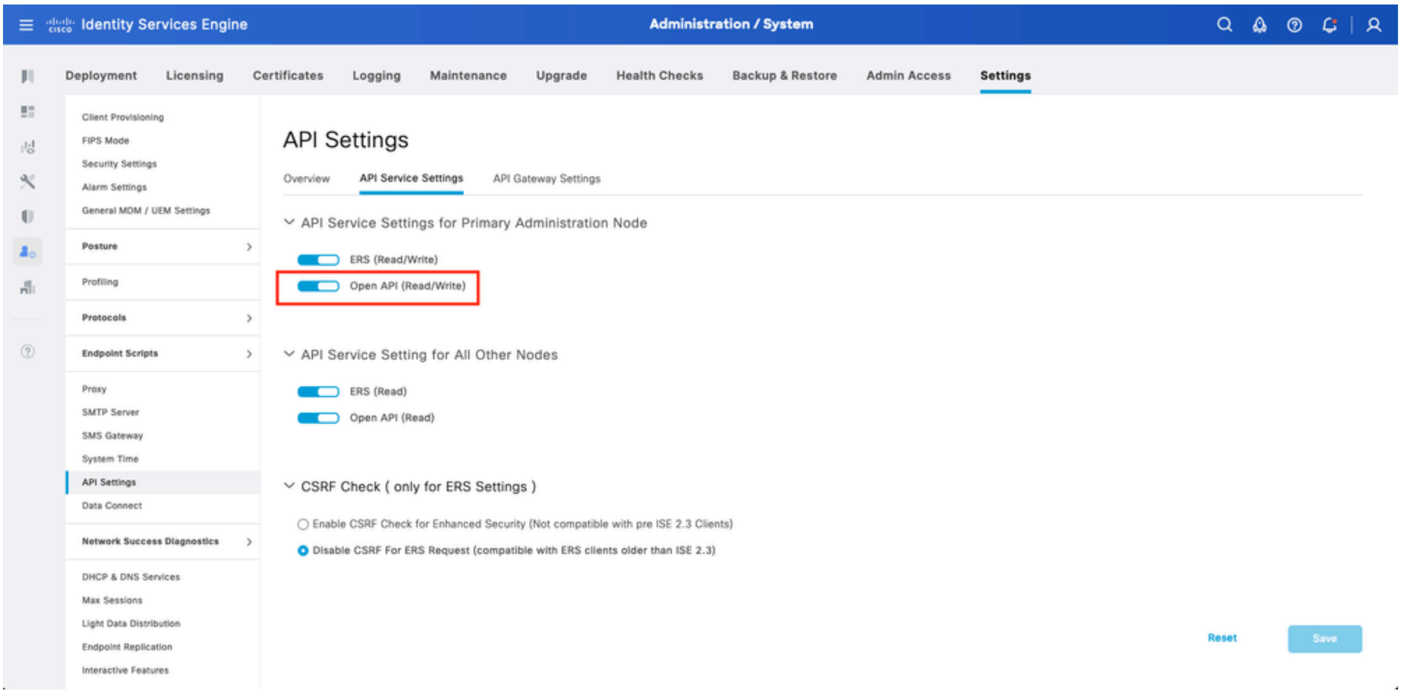


□	Name	SID
□	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-2558713077-...

Active Directory 6

启用开放式API

导航到管理>System >设置> API设置> API服务设置。启用Open API，然后单击Save。



API Settings

Overview | API Service Settings | API Gateway Settings

API Service Settings for Primary Administration Node

- ERS (Read/Write)
- Open API (Read/Write)

API Service Setting for All Other Nodes

- ERS (Read)
- Open API (Read)

CSRF Check (only for ERS Settings)

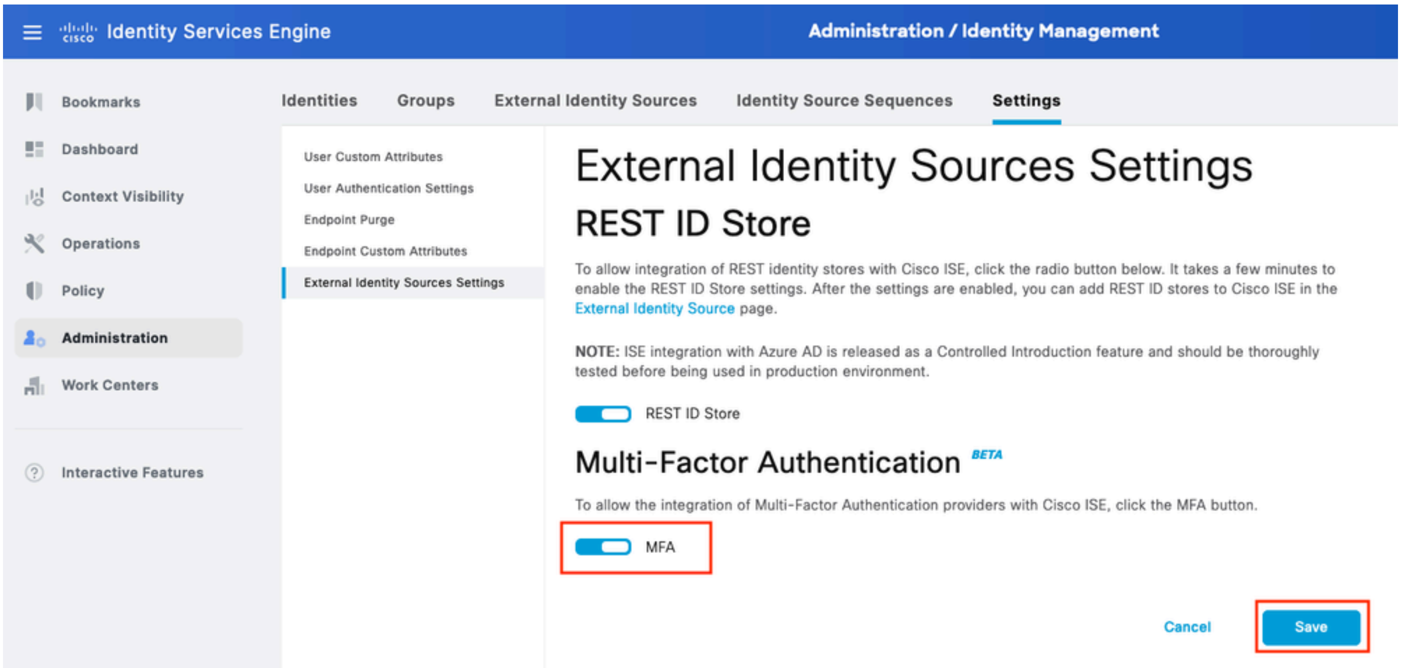
○ Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

● Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

开放式API

启用MFA身份源

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。



External Identity Sources Settings

REST ID Store

To allow integration of REST identity stores with Cisco ISE, click the radio button below. It takes a few minutes to enable the REST ID Store settings. After the settings are enabled, you can add REST ID stores to Cisco ISE in the External Identity Source page.

NOTE: ISE integration with Azure AD is released as a Controlled Introduction feature and should be thoroughly tested before being used in production environment.

REST ID Store

Multi-Factor Authentication BETA

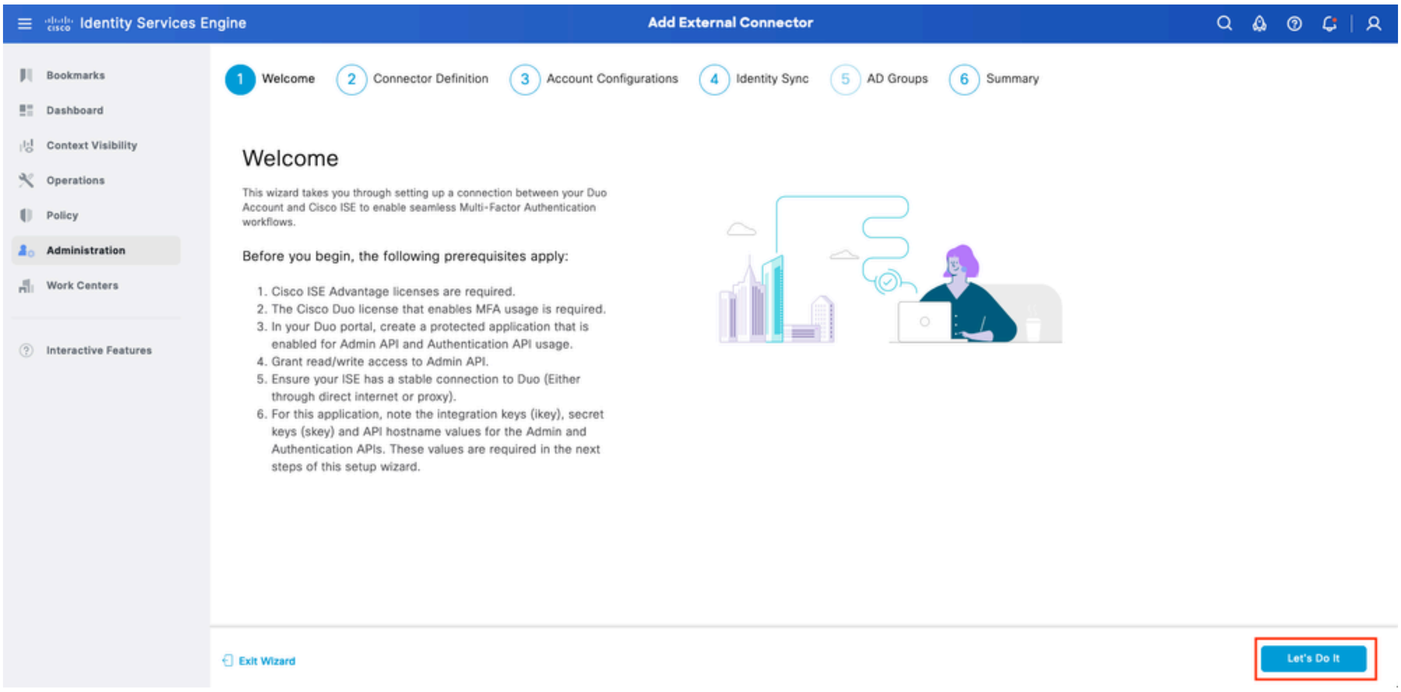
To allow the integration of Multi-Factor Authentication providers with Cisco ISE, click the MFA button.

MFA

ISE MFA 1

配置MFA外部身份源

导航到Administration > Identity Management > External Identity Sources。单击Add。在“欢迎使用”屏幕上，单击开始执行操作。



Welcome

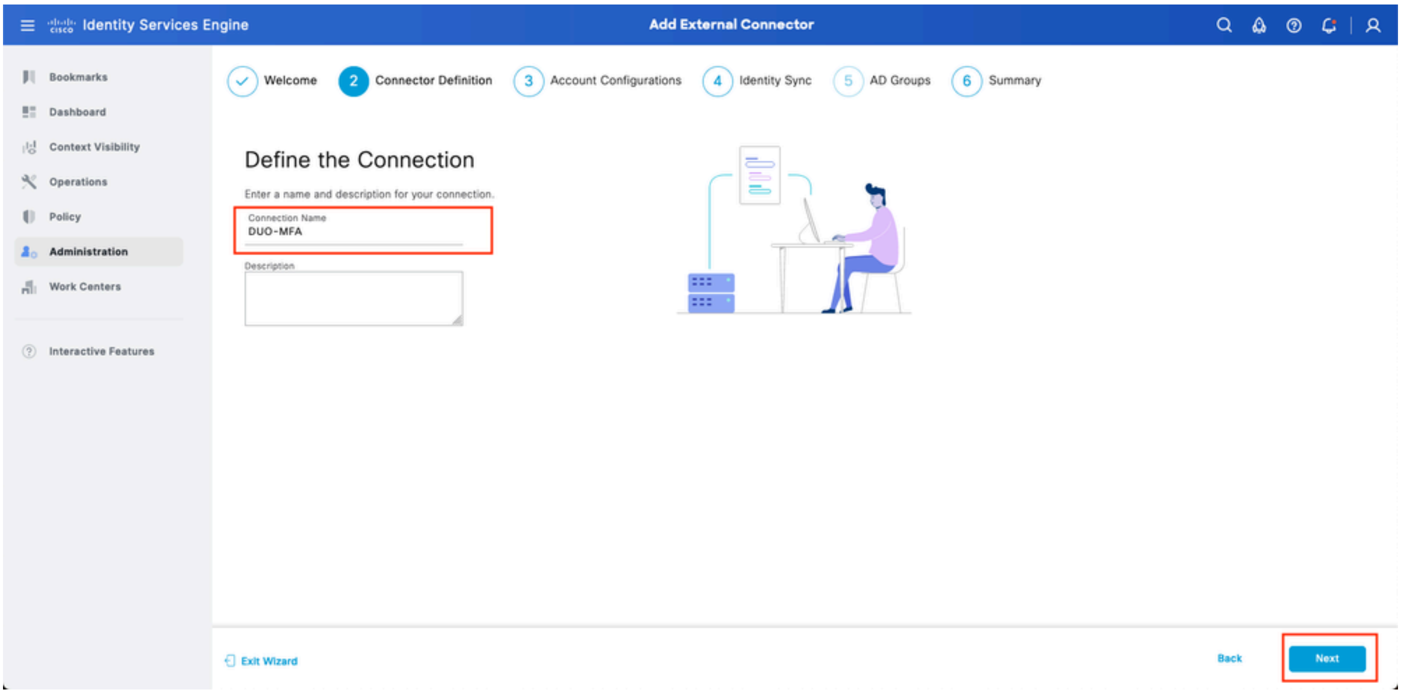
This wizard takes you through setting up a connection between your Duo Account and Cisco ISE to enable seamless Multi-Factor Authentication workflows.

Before you begin, the following prerequisites apply:

1. Cisco ISE Advantage licenses are required.
2. The Cisco Duo license that enables MFA usage is required.
3. In your Duo portal, create a protected application that is enabled for Admin API and Authentication API usage.
4. Grant read/write access to Admin API.
5. Ensure your ISE has a stable connection to Duo (Either through direct internet or proxy).
6. For this application, note the integration keys (ikey), secret keys (skey) and API hostname values for the Admin and Authentication APIs. These values are required in the next steps of this setup wizard.

ISE双功能向导1

在下一个屏幕上，配置Connection Name，然后单击Next。



Define the Connection

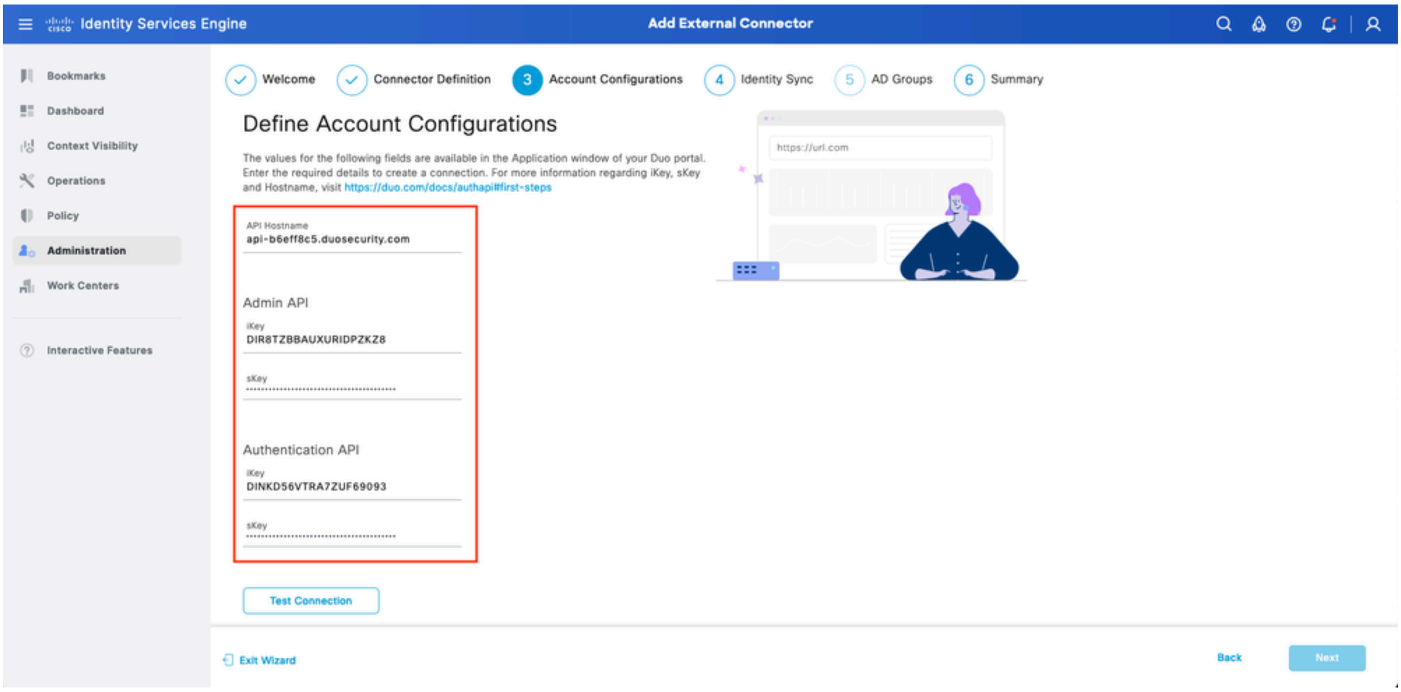
Enter a name and description for your connection.

Connection Name
DUO-MFA

Description

ISE双功能向导2

从Select Applications to Protect步骤配置API主机名、管理API集成和密钥、身份验证API集成和密钥的值。



Define Account Configurations

The values for the following fields are available in the Application window of your Duo portal. Enter the required details to create a connection. For more information regarding iKey, sKey and Hostname, visit https://duo.com/docs/authapi#first-steps

API Hostname
api-b6eff8c5.duosecurity.com

Admin API

iKey
DIR8TZBBAUXURIDPZKZ8

sKey
....

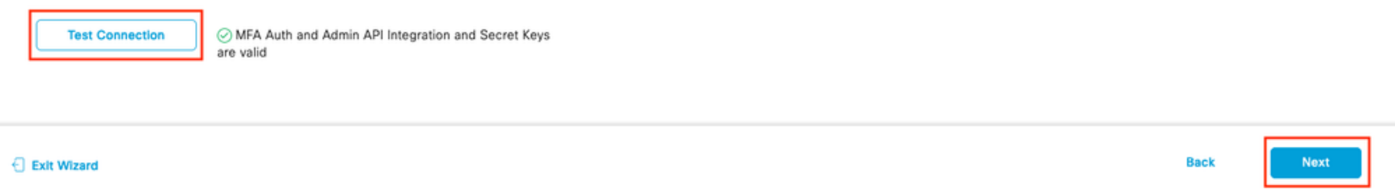
Authentication API

iKey
DINKD56VTRA7ZUF69093

sKey
....

ISE双功能向导3

单击Test Connection。Test Connection成功后，您可以点击Next。

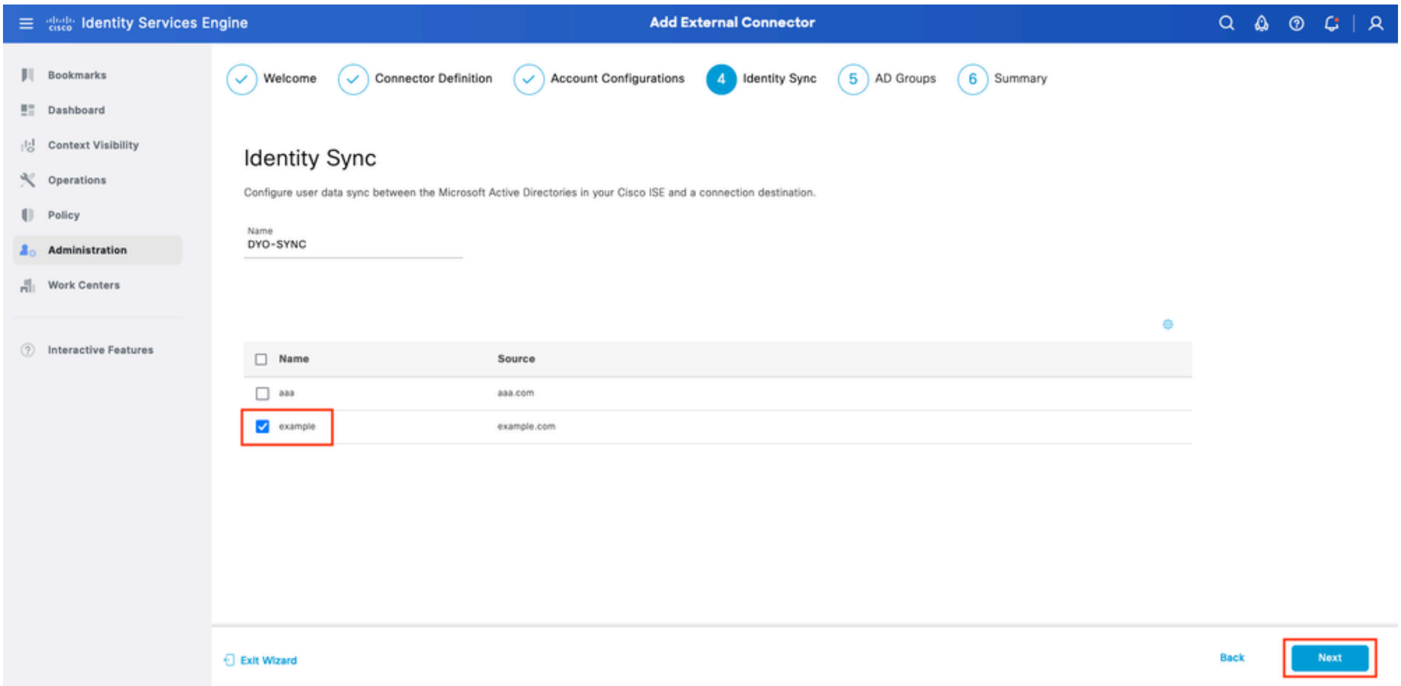


MFA Auth and Admin API Integration and Secret Keys are valid

ISE双功能向导4

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DUO帐户。选择Active Directory加入点。单击Next。

注意：Active Directory配置不在文档范围内，请遵循此文档以将ISE与Active Directory集成。



Identity Sync

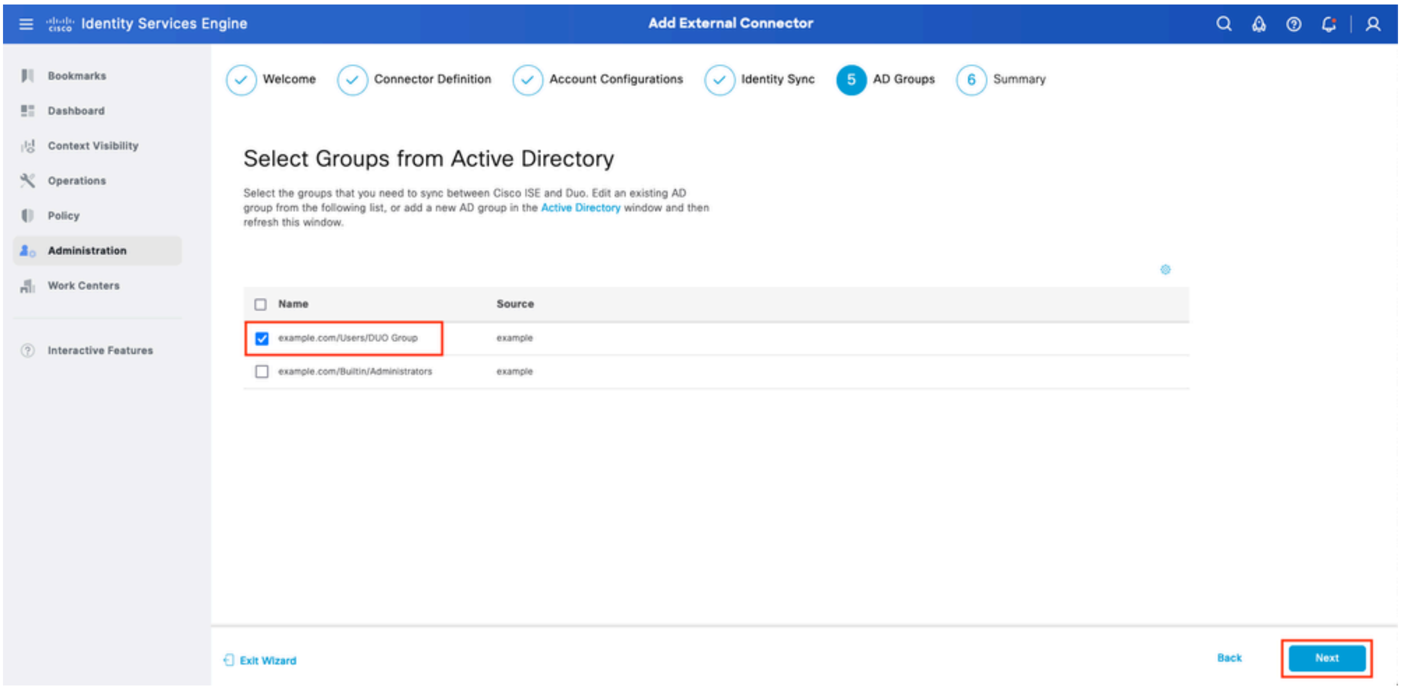
Configure user data sync between the Microsoft Active Directories in your Cisco ISE and a connection destination.

Name
DYO-SYNC

	Name	Source
□	aaa	aaa.com
☑	example	example.com

ISE双功能向导5

选择Active Directory Groups，您希望用户从其中与DUO同步。单击Next。



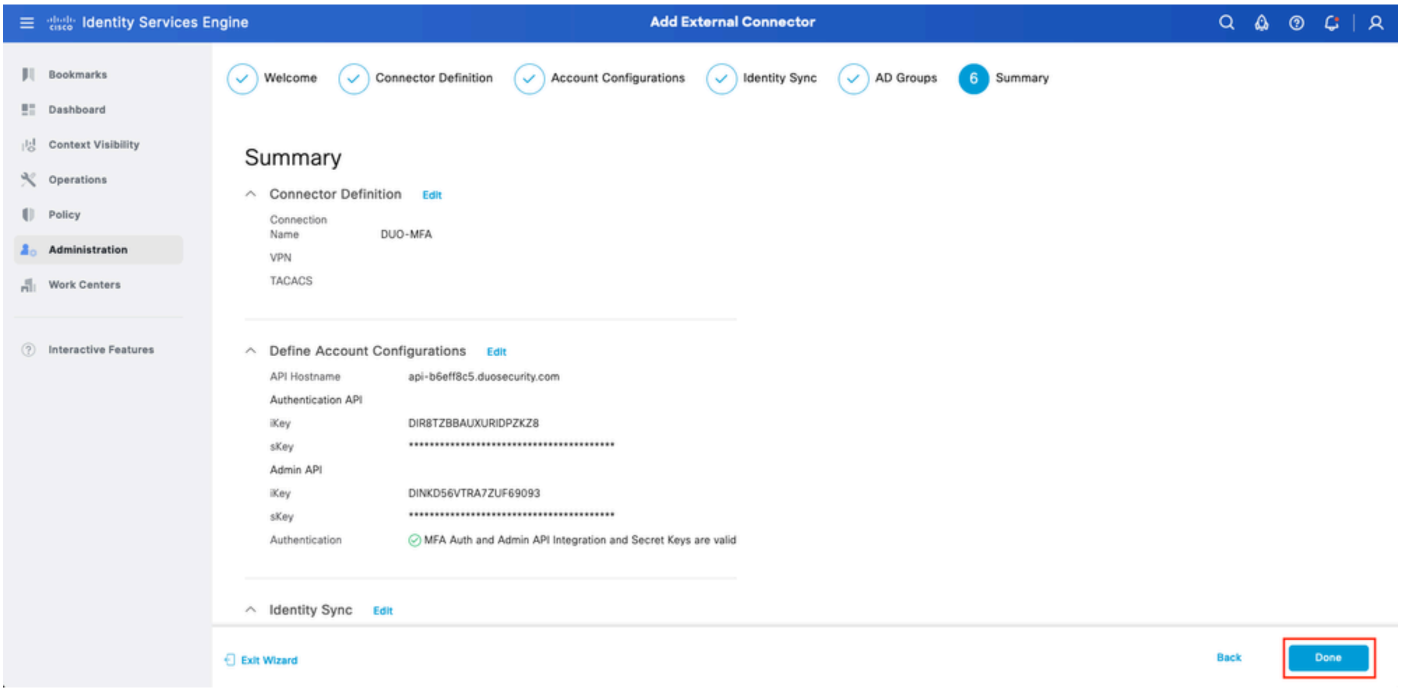
Select Groups from Active Directory

Select the groups that you need to sync between Cisco ISE and Duo. Edit an existing AD group from the following list, or add a new AD group in the Active Directory window and then refresh this window.

	Name	Source
☑	example.com/Users/DUO Group	example
□	example.com/Builtin/Administrators	example

ISE DUO向导6

验证设置是否正确，然后单击Done。



Summary

Connector Definition Edit

Connection Name	DUO-MFA
VPN	
TACACS	

Define Account Configurations Edit

API Hostname	api-b6eff8c5.duosecurity.com
Authentication API	
iKey	DIR8TZBBAUXURIDPZKZ8
sKey	**
Admin API	
iKey	DINKD56VTRA7ZUF69093
sKey	**
Authentication	✓ MFA Auth and Admin API Integration and Secret Keys are valid

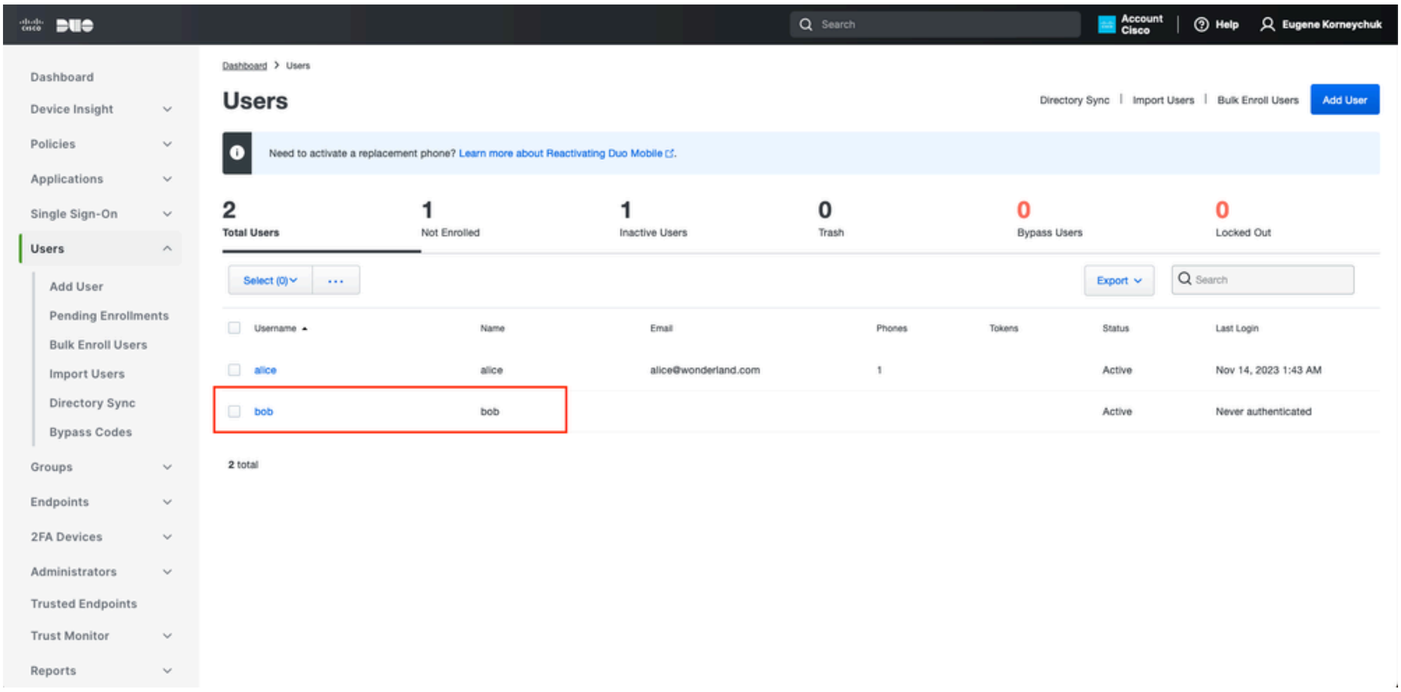
Identity Sync Edit

ISE双功能向导7

将用户注册到DUO

注意：DUO用户注册不属于本文档的范围，请考虑此文档以了解有关用户注册的详细信息。本文档使用手动用户注册。

打开DUO管理控制面板。导航到控制面板>用户。点击从ISE同步的用户。



Users

Need to activate a replacement phone? Learn more about Reactivating Duo Mobile.

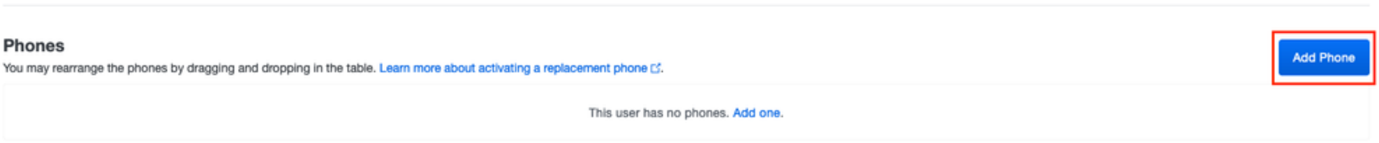
2	1	1	0	0	0
Total Users	Not Enrolled	Inactive Users	Trash	Bypass Users	Locked Out

□	Username	Name	Email	Phones	Tokens	Status	Last Login
□	alice	alice	alice@wonderland.com	1		Active	Nov 14, 2023 1:43 AM
□	bob	bob				Active	Never authenticated

2 total

DUO注册1

向下滚动到Phones。点击Add Phone。



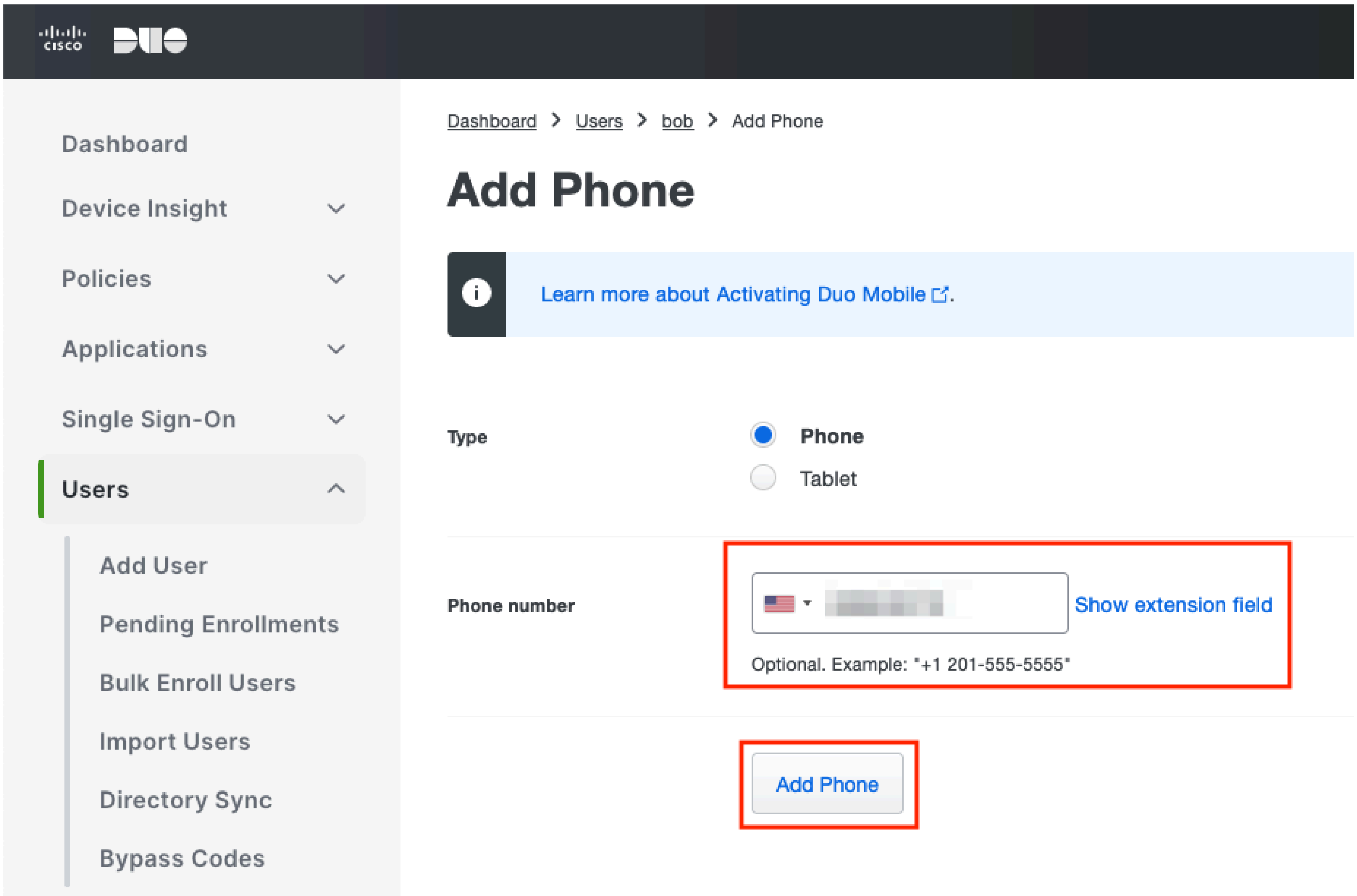
Phones

You may rearrange the phones by dragging and dropping in the table. Learn more about activating a replacement phone.

This user has no phones. Add one.

DUO注册2

输入Phone Number，然后单击Add Phone。



Dashboard > Users > bob > Add Phone

Add Phone

Learn more about Activating Duo Mobile.

Type ● Phone ○ Tablet

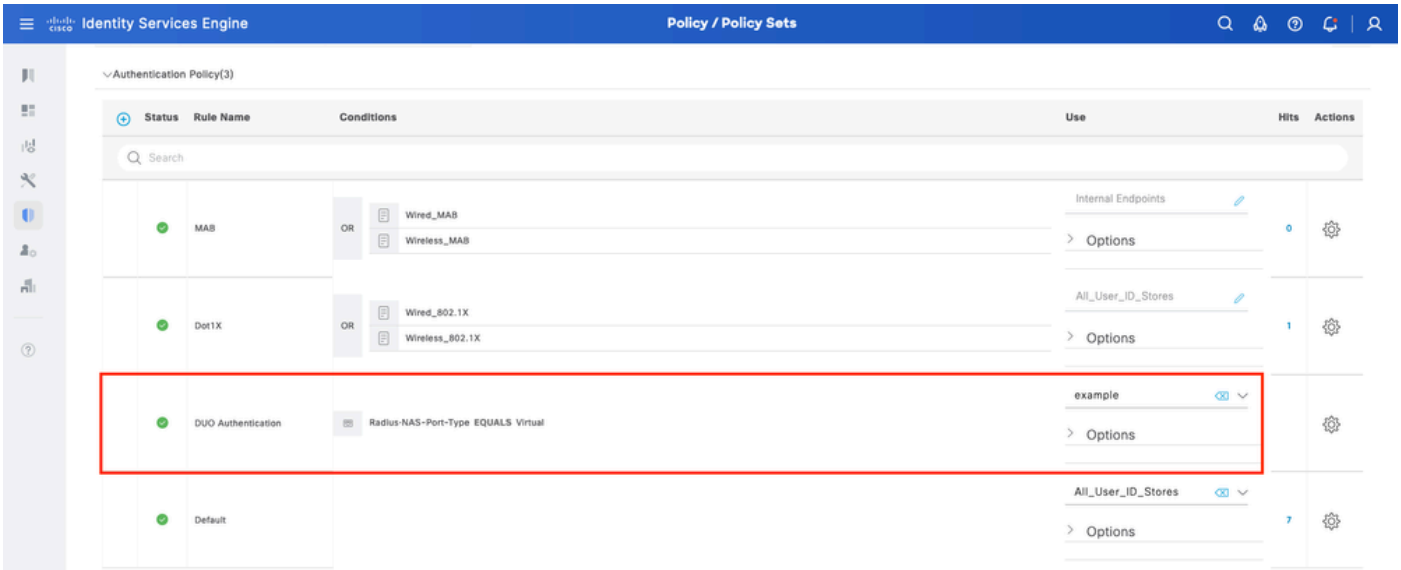
Phone number [redacted] Show extension field

Optional. Example: "+1 201-555-5555"

配置策略集

1.配置身份验证策略

导航到Policy > Policy Set。选择要为其启用MFA的Policy Set。将主身份验证身份库配置为Active Directory的身份验证策略。



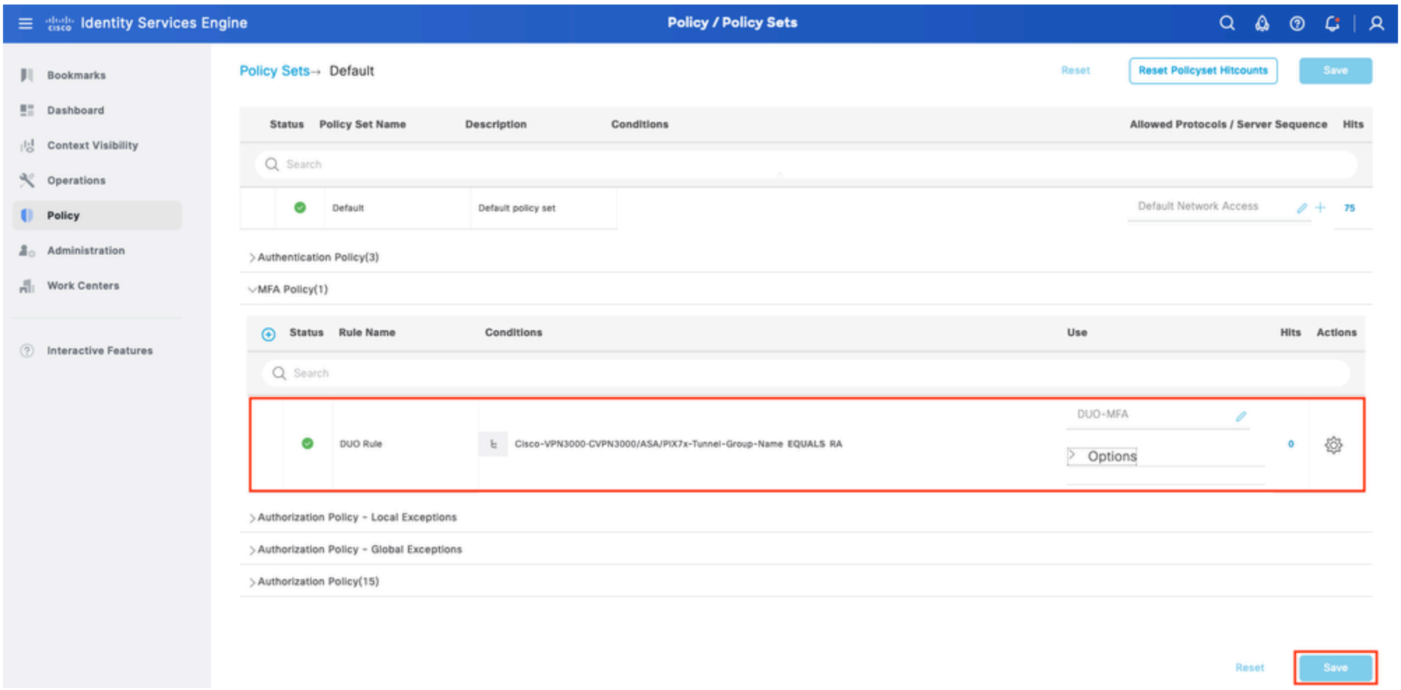
Authentication Policy(3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints Options	0	⚙
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores Options	1	⚙
●	DUO Authentication	Radius-NAS-Port-Type EQUALS Virtual	example Options		⚙
●	Default		All_User_ID_Stores Options	7	⚙

策略集1

2.配置MFA策略

在ISE上启用MFA后，ISE策略集的新部分可用。展开MFA Policy，然后单击+以添加MFA Policy。配置您选择的MFA条件，选择使用部分中以前配置的DUO-MFA。单击Save。



Policy Sets→ Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	75

Authentication Policy(3)

MFA Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
●	DUO Rule	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA	DUO-MFA Options	0	⚙

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

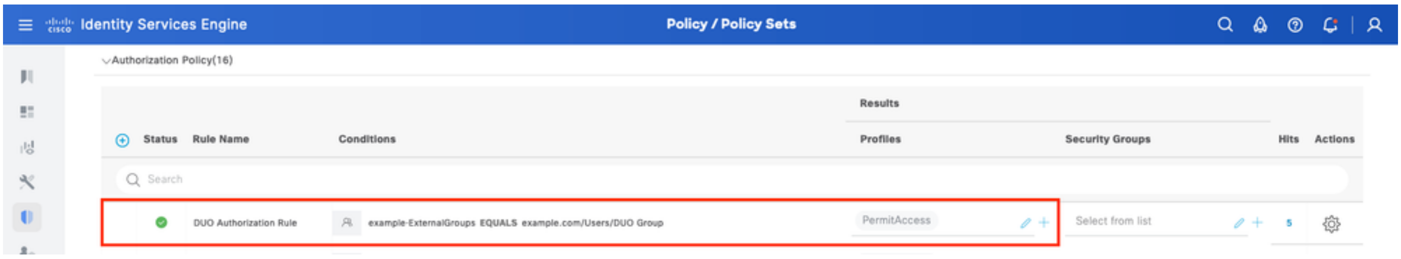
Authorization Policy(15)

ISE策略

注意：以上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。使用此文档配置ASA/FTD

3.配置授权策略

使用Active Directory组条件和您选择的权限配置授权策略。



Authorization Policy(16)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
●	DUO Authorization Rule	example-ExternalGroups EQUALS example.com/Users/DUO Group	PermitAccess	Select from list	5	

策略集3

限制

在撰写本文档时：

1.仅支持DUO推送和电话作为第二因素身份验证方法

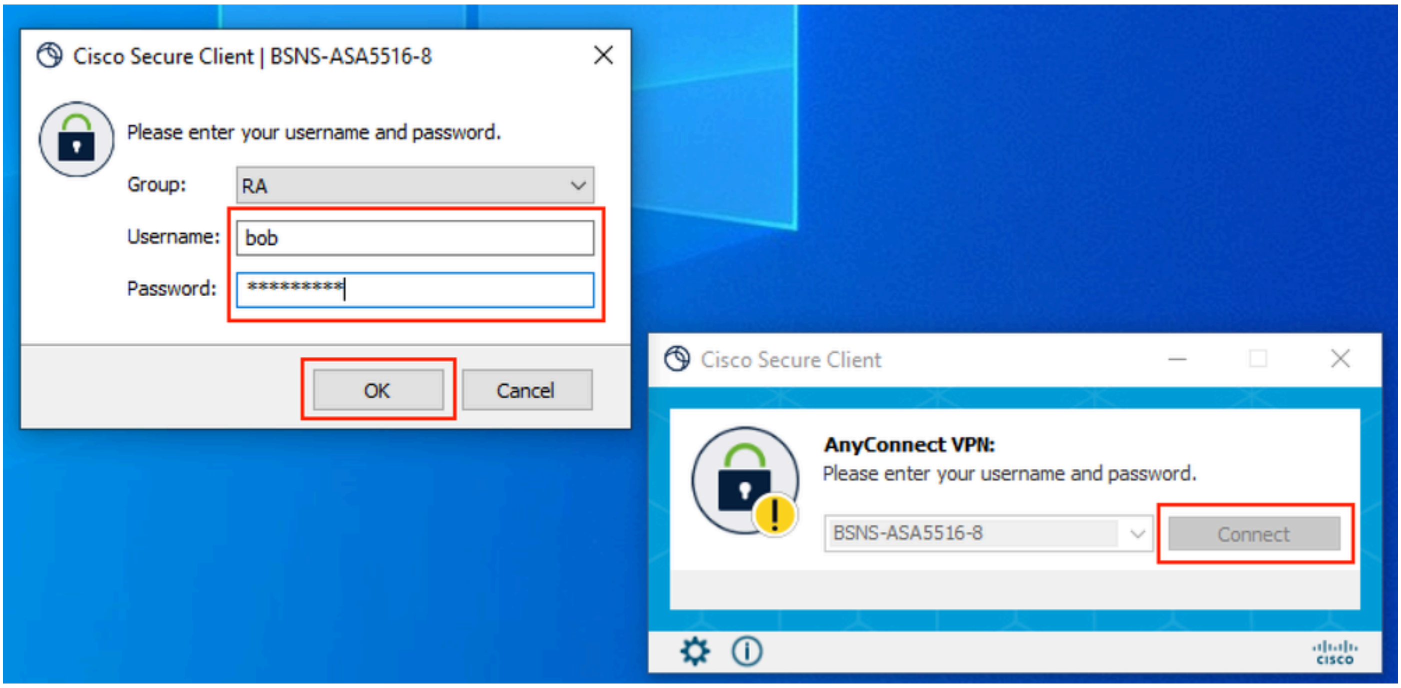
2.没有组被推送到DUO云，仅支持用户同步

3.仅支持以下多重身份验证使用案例：

- VPN用户身份验证
- TACACS+管理员访问身份验证

验证

打开Cisco Secure Client，单击Connect。提供用户名和密码，然后单击确定。



Please enter your username and password.

Group: RA

Username: bob

Password: *********

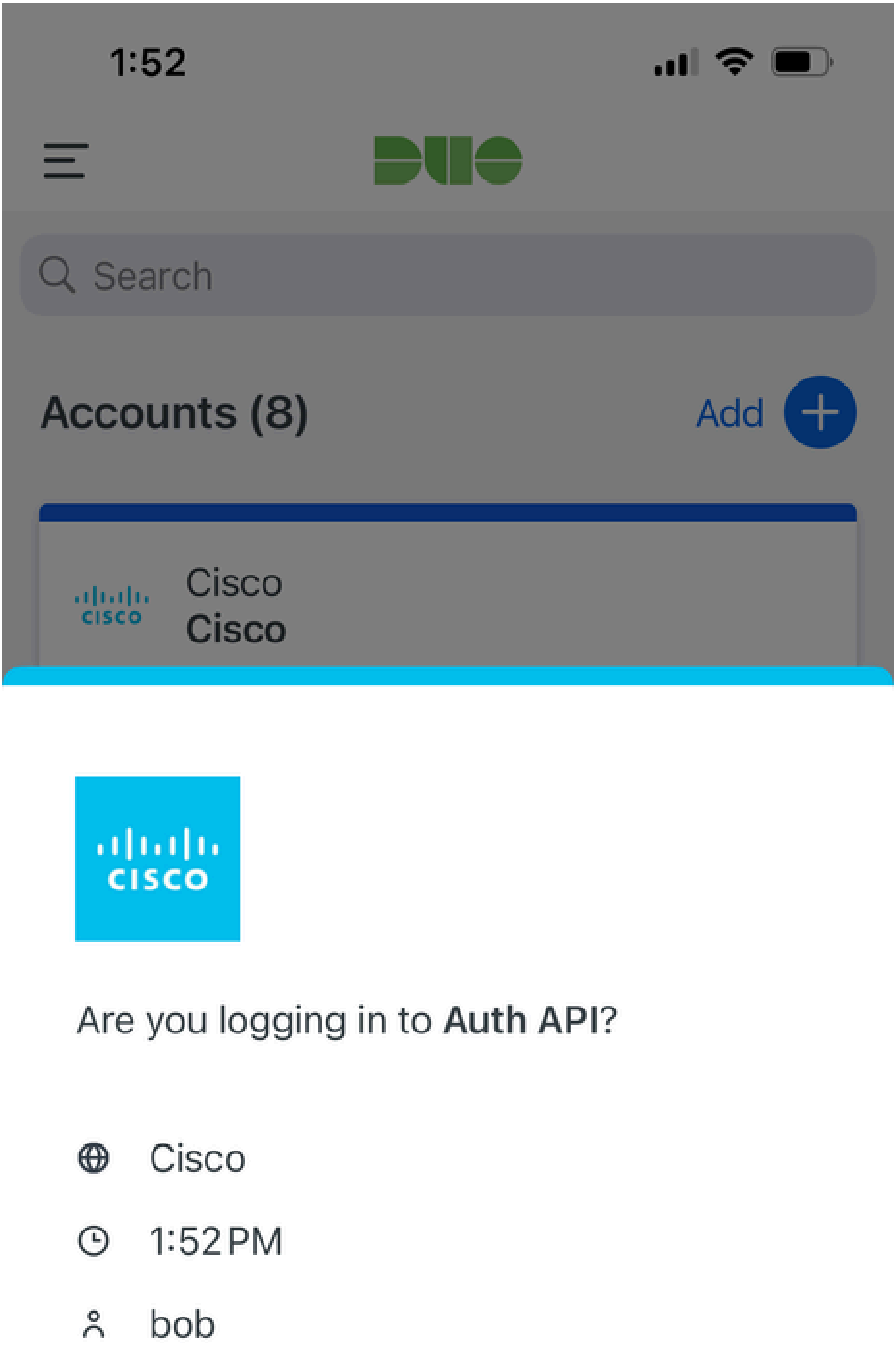
AnyConnect VPN:

Please enter your username and password.

BSNS-ASA5516-8

VPN 客户

用户移动设备必须收到DUO推送通知。批准。已建立VPN连接。



Accounts (8)

Cisco
Cisco

Are you logging in to **Auth API**?

Cisco

1:52 PM

bob

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）。