

Configurar a Multi-fator Authentication Nativa do ISE 3.3 com DUO

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de fluxo](#)

[Configurações](#)

[Selecionar aplicativos para proteger](#)

[Integrar o ISE com o Ative Directory](#)

[Habilitar API aberta](#)

[Habilitar fonte de identidade MFA](#)

[Configurar fonte de identidade externa MFA](#)

[Registrar Usuário no DUO](#)

[Configurar conjuntos de políticas](#)

[Limitações](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como integrar o patch 1 do Identity Services Engine (ISE) 3.3 com o DUO para Multi-fator Authentication. A partir da versão 3.3, o patch 1 do ISE pode ser configurado para integração nativa com serviços DUO, eliminando assim a necessidade de proxy de autenticação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- ISE
- DUO

Componentes Utilizados

As informações neste documento são baseadas em:

- Patch 1 do Cisco ISE versão 3.3
- DUO
- Cisco ASA versão 9.16(4)
- Cisco Secure Client versão 5.0.04032

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de fluxo

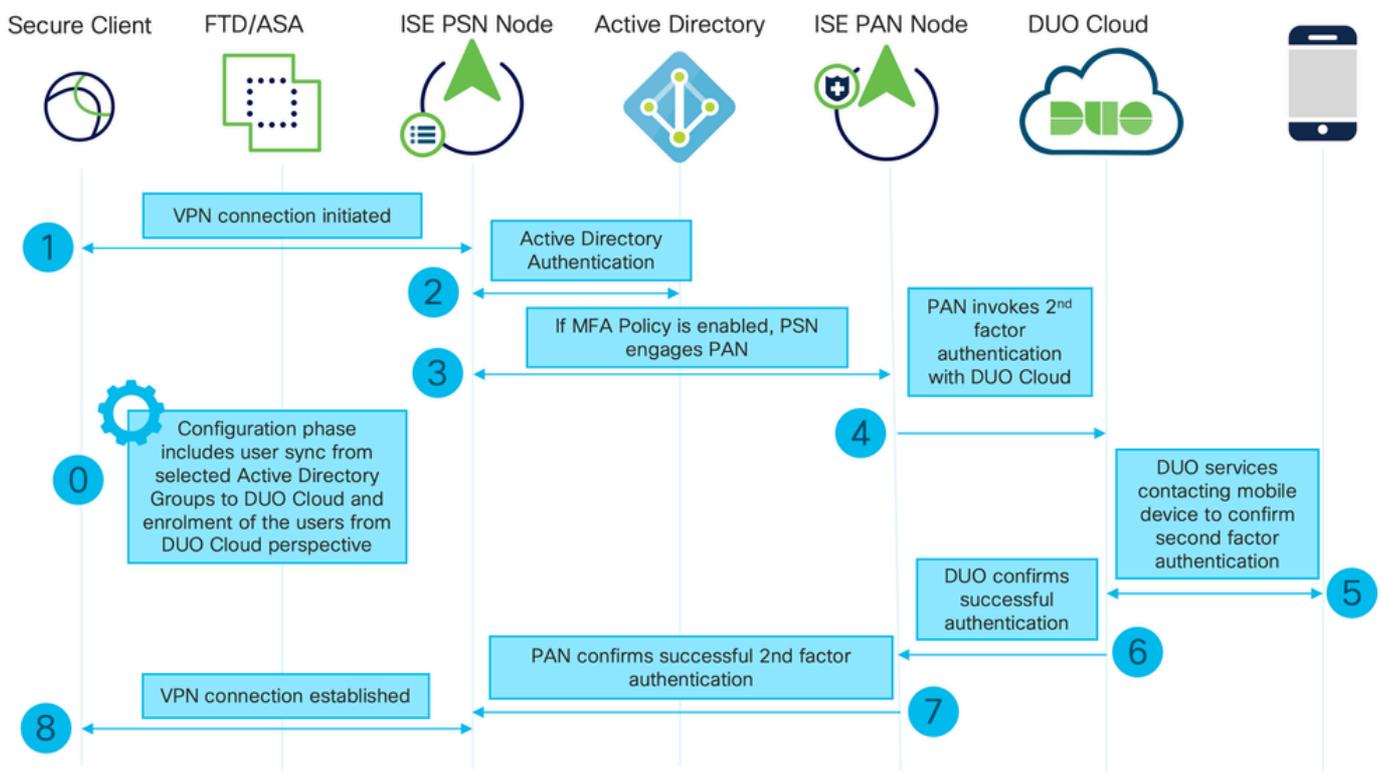


Diagrama de fluxo

Etapas

0. A Fase de Configuração inclui a seleção dos Grupos do Active Directory, a partir dos quais os usuários são sincronizados, e a sincronização ocorre quando o assistente de MFA é concluído. Ele consiste em duas etapas. Pesquisa no Active Directory para obter a lista de usuários e determinados atributos. Uma chamada para o DUO Cloud com API de Administração é feita para enviar os usuários para lá. Os administradores são solicitados a registrar usuários. A inscrição pode incluir a etapa opcional de ativação do usuário do Duo Mobile, que permite que seus usuários usem a autenticação de um toque com o Duo Push

1. A conexão VPN é iniciada, o usuário insere o nome de usuário e a senha e clica em OK. O dispositivo de rede envia a solicitação de acesso RADIUS é enviada à PSN

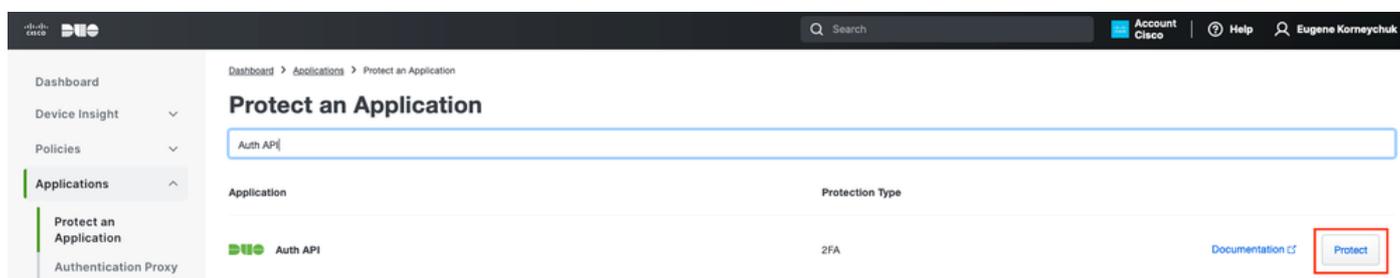
2. O nó PSN autentica o usuário através do Ative Directory
3. Quando a autenticação é bem-sucedida e a política de MFA é configurada, a PSN envolve a PAN para entrar em contato com a nuvem DUO
4. Uma chamada para a nuvem DUO com API Auth é feita para invocar uma autenticação de segundo fator com DUO
5. Ocorre a autenticação de segundo fator. O usuário conclui o processo de autenticação de segundo fator
6. O DUO responde ao PAN com o resultado da autenticação de segundo fator
7. O PAN responde ao PSN com o resultado da autenticação de segundo fator
8. Access-Accept é enviado ao Dispositivo de Rede, a Conexão VPN é estabelecida

Configurações

Selecionar aplicativos para proteger

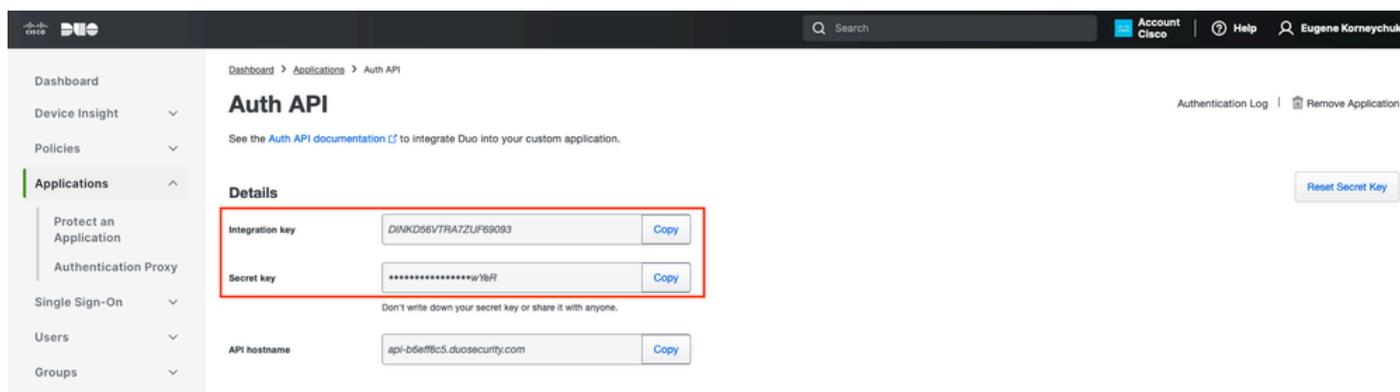
Navegue até Painel de administração do DUO <https://admin.duosecurity.com/login>. Faça login com credenciais de administrador.

Navegue até Painel de Controle > Aplicativos > Proteger um Aplicativo. Procure Auth API e selecione Protect.



API de autenticação 1

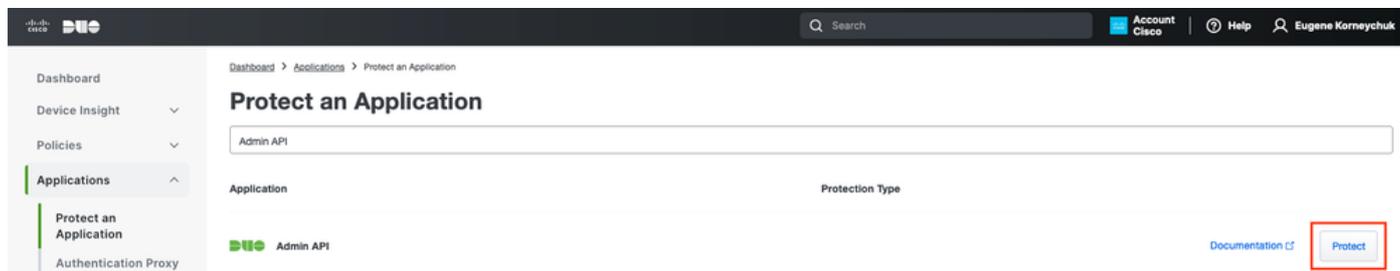
Anote a chave Integration e a chave Secret.



API de autenticação 2

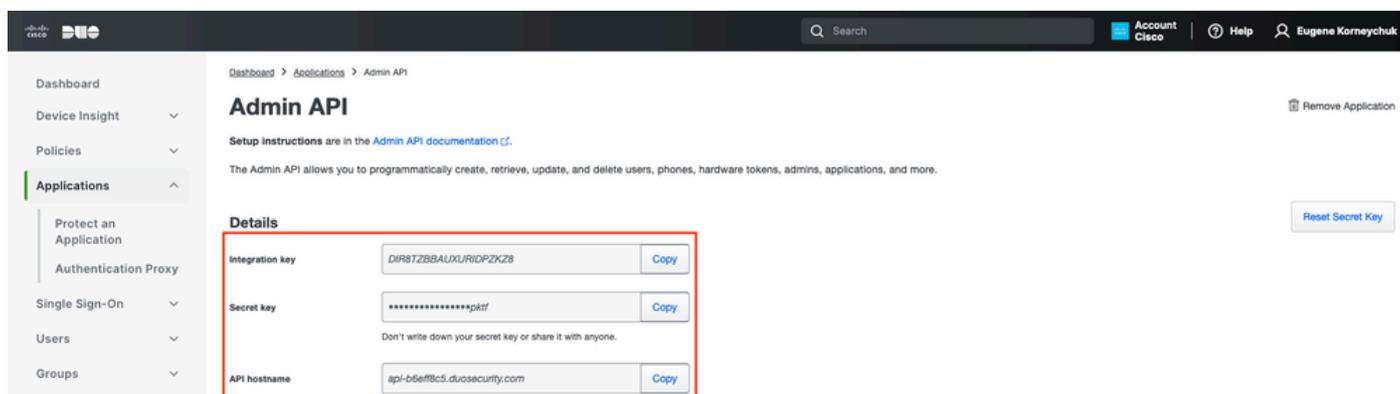
Navegue até Painel de Controle > Aplicativos > Proteger um Aplicativo. Procure Admin API e selecione Proteger.

 Observação: somente administradores com a função Proprietário podem criar ou modificar um aplicativo API de administração no Painel de administração do Duo.



API de autenticação 1

Anote a chave de integração e a chave secreta e o nome de host da API.



API de administração 2

Configurar Permissões de API

Navegue até Painel de Controle > Aplicativos > Aplicativo. Selecione Admin API.

Marque Conceder recursos de leitura e Conceder recursos de gravação. Clique em Save Changes (Salvar alterações).

- Groups ▾
- Endpoints ▾
- 2FA Devices ▾
- Administrators ▾
- Trusted Endpoints
- Trust Monitor ▾
- Reports ▾
- Settings
- Billing ▾

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

[Provide feedback](#)

API hostname [Copy](#)

Settings

Type Admin API

Name

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.

API de administração 3

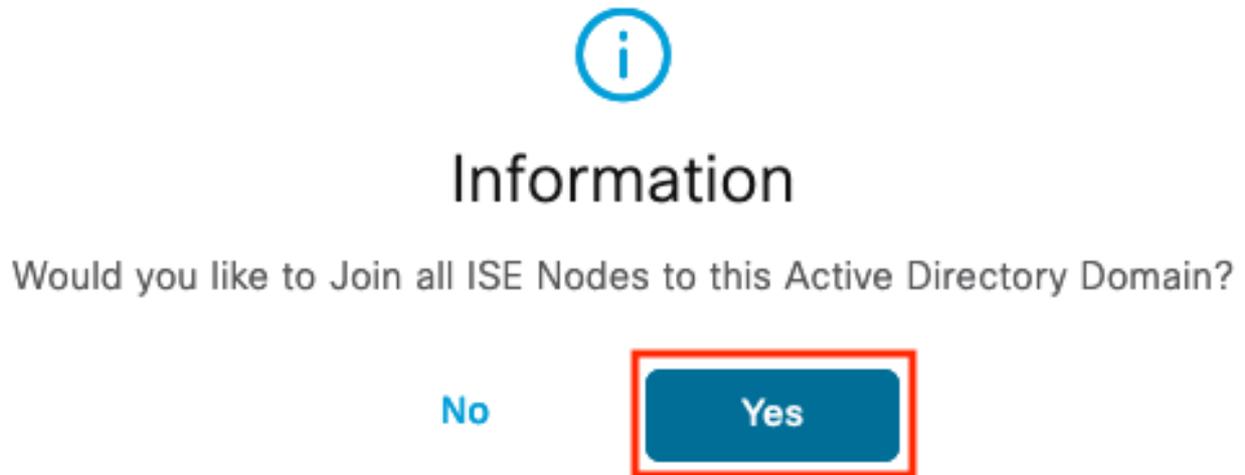
Integrar o ISE com o Active Directory

1. Navegue até Administração > Gerenciamento de identidades > Repositórios de identidades externos > Active Directory > Adicionar. Forneça o Join Point Name (Nome do ponto de ingresso), Active Directory Domain (Domínio do Active Directory) e clique em Submit (Enviar).

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is Administration / Identity Management. The main menu includes Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The 'External Identity Sources' section is active, showing a list of source types on the left: Certificate Authentica..., Active Directory, MFA, Identity Sync, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, Social Login, and REST. The 'Active Directory' source is selected, and the 'Connection' configuration page is displayed. The 'Join Point Name' is set to 'example' and the 'Active Directory Domain' is set to 'example.com'. Both fields are highlighted with a red border. At the bottom right, there are 'Submit' and 'Cancel' buttons, with the 'Submit' button also highlighted with a red border.

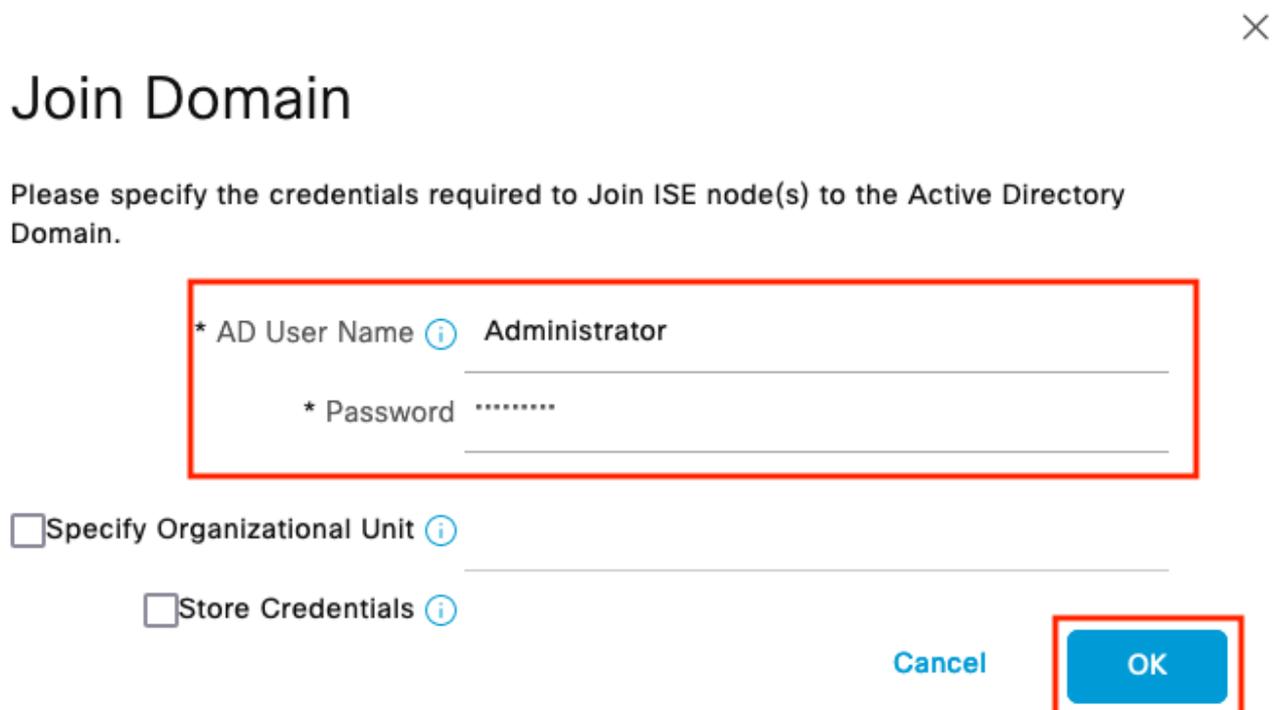
Active Directory 1

2. Quando for solicitado a Ingressar em todos os Nós do ISE neste Domínio do Ative Diretory, clique em Sim.



Ative Diretory 2

3. Forneça o Nome de usuário e a Senha do AD e clique em OK.



Ative Diretory 3

A conta do AD necessária para o acesso ao domínio no ISE pode ter um destes:

- Adicionar estações de trabalho ao domínio do direito do usuário no respectivo domínio

- Criar Objetos do Computador ou Excluir Objetos do Computador no respectivo contêiner de computadores onde a conta da máquina do ISE é criada antes de ela ingressar na máquina do ISE para o domínio

 Observação: a Cisco recomenda desabilitar a política de bloqueio para a conta do ISE e configurar a infraestrutura do AD para enviar alertas ao administrador se uma senha incorreta for usada para essa conta. Quando a senha incorreta é inserida, o ISE não cria nem modifica sua conta de máquina quando necessário e, portanto, possivelmente nega todas as autenticações.

4. O status do AD é Operacional.

Connection Allowed Domains PassiveID Groups Attributes Advanced Settings

* Join Point Name **example** ⓘ

* Active Directory Domain **example.com** ⓘ

+ Join + Leave 👤 Test User 🔧 Diagnostic Tool ↻ Refresh Table

<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	ise331.example.com	PRIMARY	✔ Operational	WIN2022.example.com	Default-First-Site-Name
<input type="checkbox"/>	ise332.example.com	SECONDARY	✔ Operational	WIN2022.example.com	Default-First-Site-Name

Active Directory 4

5. Navegue até Groups > Add > Select Groups From Diretory > Retrieve Groups. Marque as caixas de seleção em Grupos do AD de sua escolha (que são usadas para sincronizar usuários e para Política de autorização), conforme mostrado nesta imagem.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name *
Filter

SID *
Filter

Type
Filter

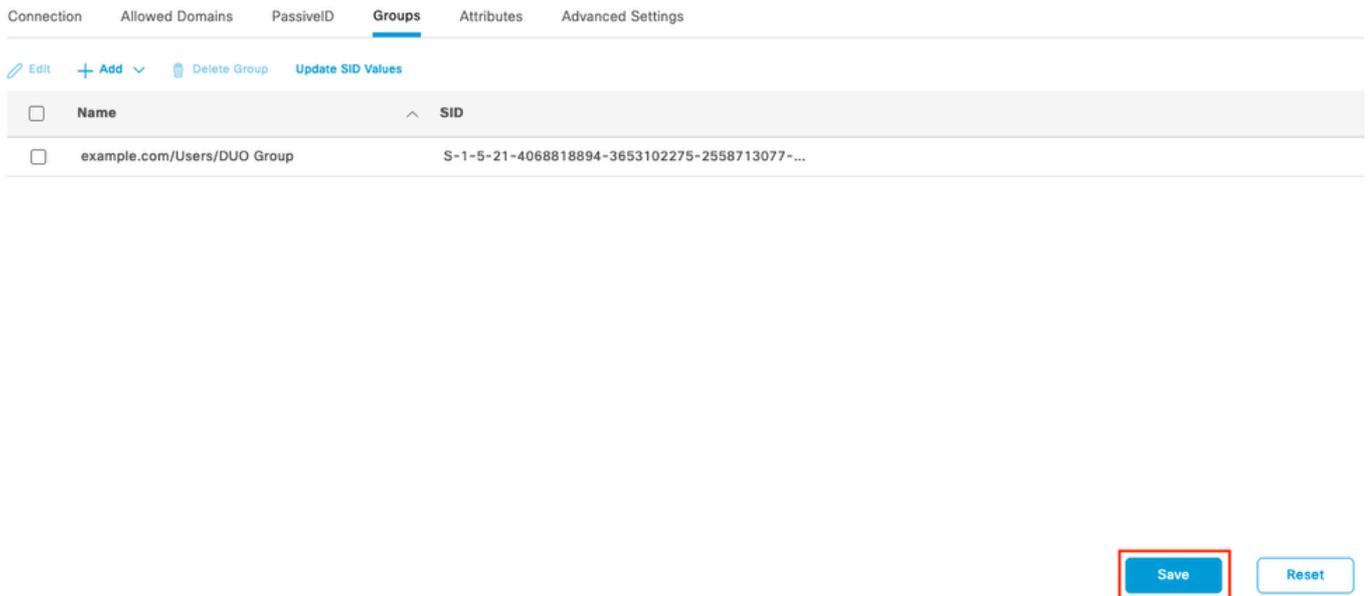
50 Groups Retrieved.

<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	example.com/Users/Cert Publishers	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/Cloneable Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input checked="" type="checkbox"/>	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Denied RODC Password Re...	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/DnsAdmins	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/DnsUpdateProxy	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Admins	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Computers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Guests	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Users	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Enterprise Admins	S-1-5-21-4068818894-3653102275-25587130...	UNIVERSAL

Cancel

Ative Diretory 5

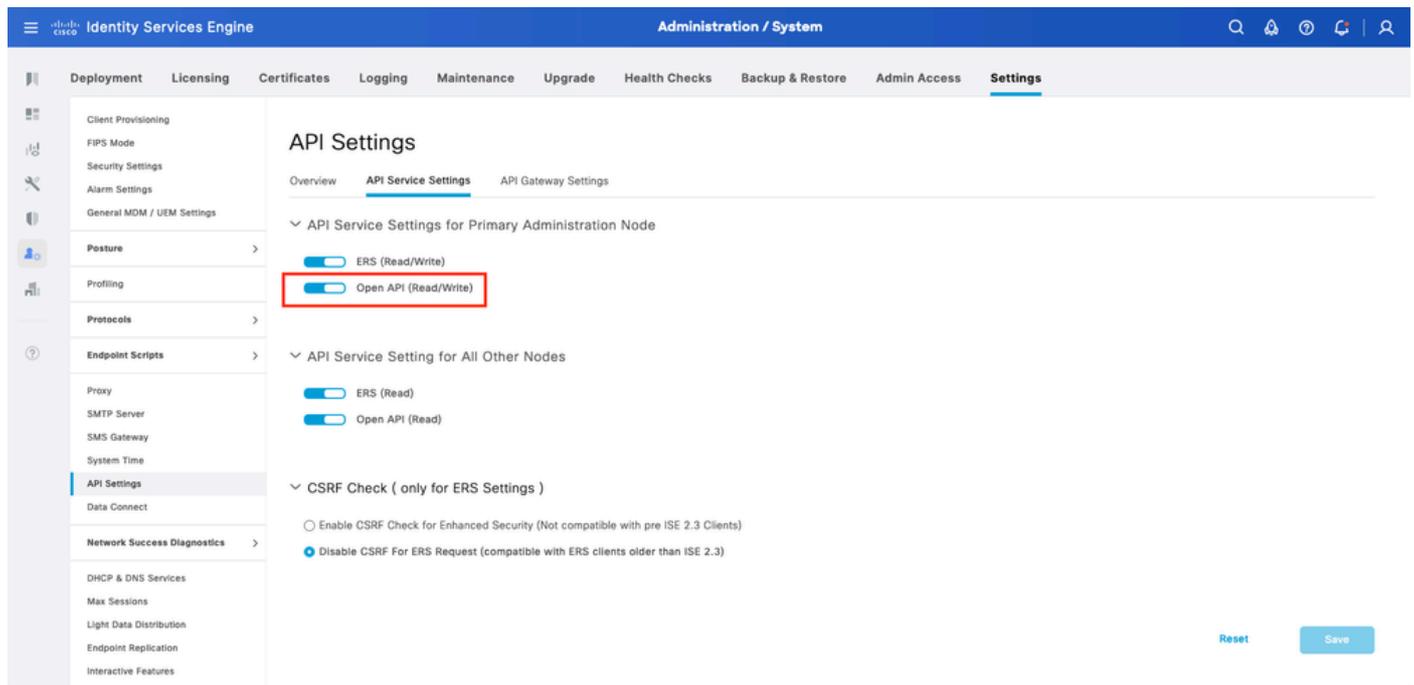
6. Clique em Salvar para salvar os Grupos do AD recuperados.



Ative Diretory 6

Habilitar API aberta

Navegue até Administration > System > Settings > API Settings > API Service Settings. Habilite Open API e clique em Save.



API aberta

Habilitar fonte de identidade MFA

Navegue até Administração > Gerenciamento de identidades > Configurações > Configurações de fontes de identidade externas. Habilite MFA e clique em Save.

Identity Services Engine Administration / Identity Management

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

Identities Groups External Identity Sources Identity Source Sequences Settings

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

Cancel Save

MFA 1 do ISE

Configurar fonte de identidade externa MFA

Navegue até Administração > Gerenciamento de identidades > Fontes de identidade externas. Clique em Add. Na tela Welcome (Bem-vindo), clique em Let's Do It.

Identity Services Engine Add External Connector

1 Welcome 2 Connector Definition 3 Account Configurations 4 Identity Sync 5 AD Groups 6 Summary

Welcome

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

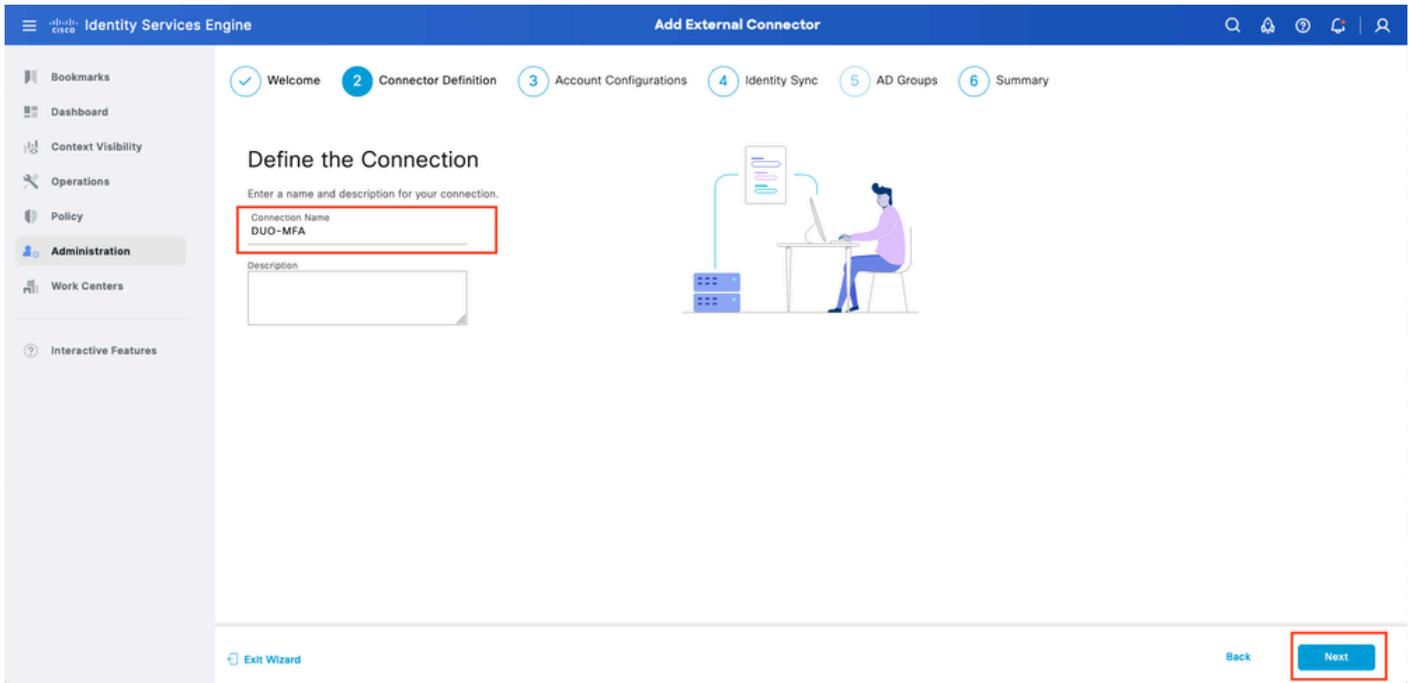
Before you begin, the following prerequisites apply:

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.

Exit Wizard Let's Do It

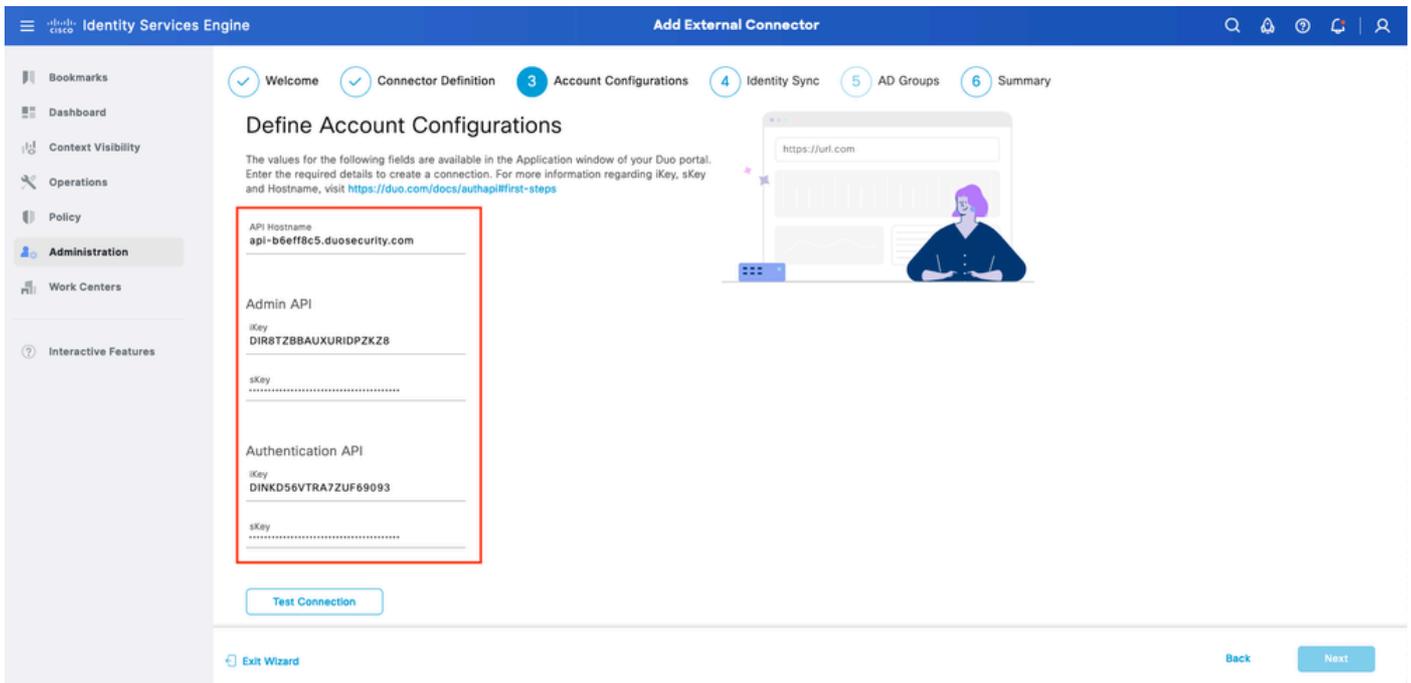
Assistente ISE DUO 1

Na próxima tela, configure Connection Name e clique em Next.



Assistente ISE DUO 2

Etapa Configure os valores de Nome de Host da API, Integração da API de Administração e Chaves Secretas, Integração da API de Autenticação e Chaves Secretas de Seleccionar Aplicativos para Proteger.



Assistente do ISE DUO 3

Clique em Test Connection. Depois que o Teste de conexão for bem sucedido, você pode clicar em Avançar.

Test Connection

MFA Auth and Admin API Integration and Secret Keys are valid

Exit Wizard

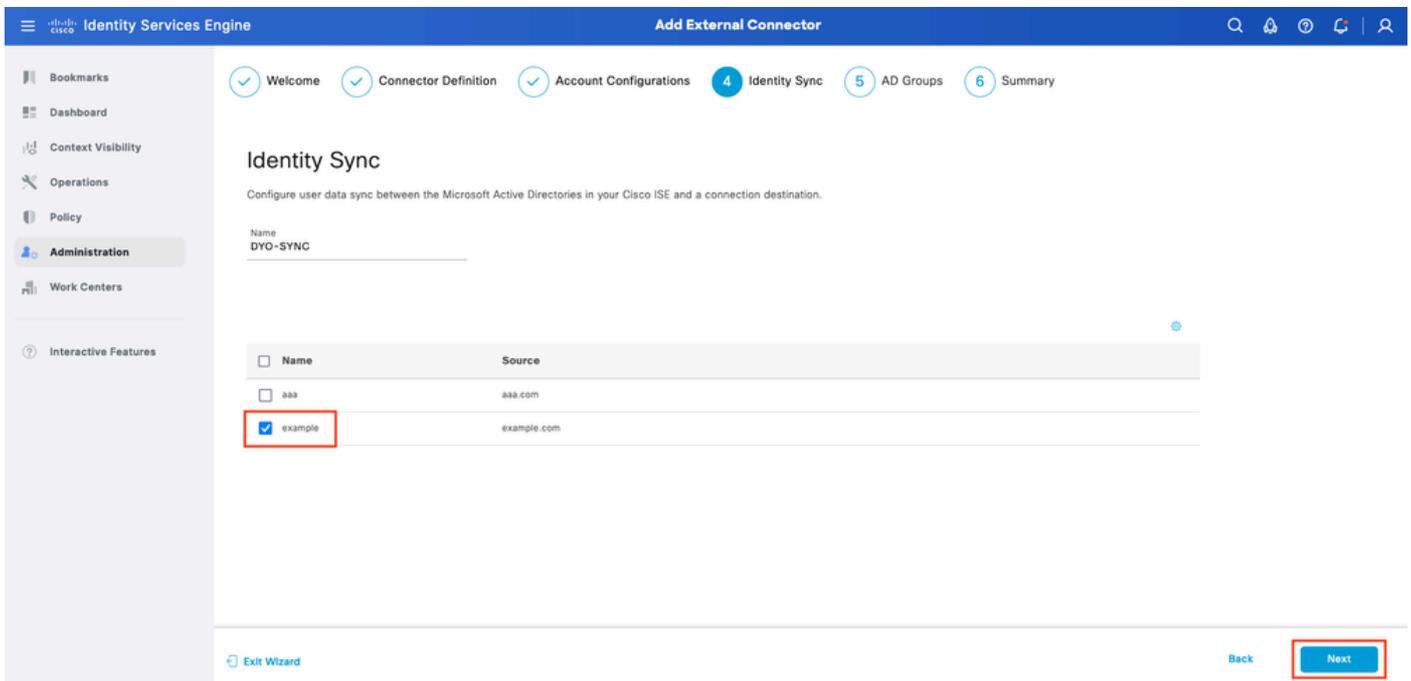
Back

Next

Assistente ISE DUO 4

Configure a Sincronização de Identidades. Este processo sincroniza usuários dos grupos do Active Directory que você selecionou na Conta DUO usando as credenciais de API fornecidas anteriormente. Selecione Active Directory Join Point. Clique em Next.

 Observação: a configuração do Active Directory está fora do escopo do documento. Siga este [documento](#) para integrar o ISE ao Active Directory.



Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations **4 Identity Sync** 5 AD Groups 6 Summary

Identity Sync

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

Name
DYO-SYNC

<input type="checkbox"/> Name	Source
<input type="checkbox"/> aaa	aaa.com
<input checked="" type="checkbox"/> example	example.com

Exit Wizard Back Next

Assistente ISE DUO 5

Selecione Grupos do Active Directory dos quais você deseja que os usuários sejam sincronizados com o DUO. Clique em Next.

Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations Identity Sync 5 AD Groups 6 Summary

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.

<input type="checkbox"/>	Name	Source
<input checked="" type="checkbox"/>	example.com/Users/DUO Group	example
<input type="checkbox"/>	example.com/Builtin/Administrators	example

Exit Wizard Back Next

Assistente ISE DUO 6

Verifique se as configurações estão corretas e clique em Done.

Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations Identity Sync AD Groups 6 Summary

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](#)

Exit Wizard Back Done

Assistente ISE DUO 7

Registrar Usuário no DUO

 **Observação:** a Inscrição de Usuário DUO está fora do escopo do documento. Considere este [documento](#) para saber mais sobre a inscrição dos usuários. Para os fins deste documento, o registro manual de usuário é usado.

Abra o Painel de Administração do DUO. Navegue até Painel > Usuários. Clique no usuário

sincronizado no ISE.

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

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

Select (0) ... Export Search

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/>	alice	alice	alice@wonderland.com	1		Active	Nov 14, 2023 1:43 AM
<input type="checkbox"/>	bob	bob				Active	Never authenticated

2 total

Inscrição DUO 1

Role para baixo até Telefones. Clique em Adicionar telefone.

Phones

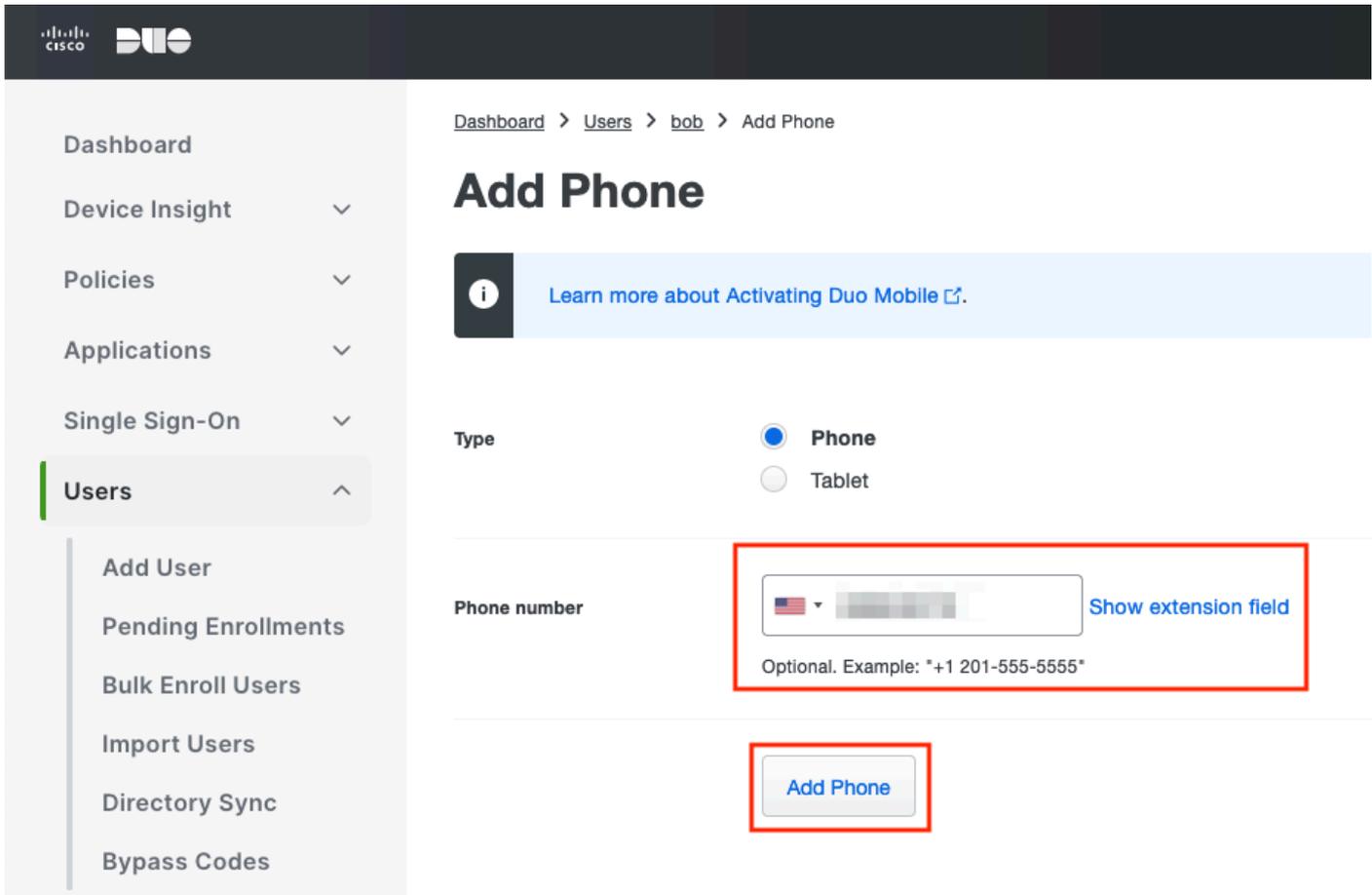
You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#).

This user has no phones. [Add one.](#)

[Add Phone](#)

Inscrição DUO 2

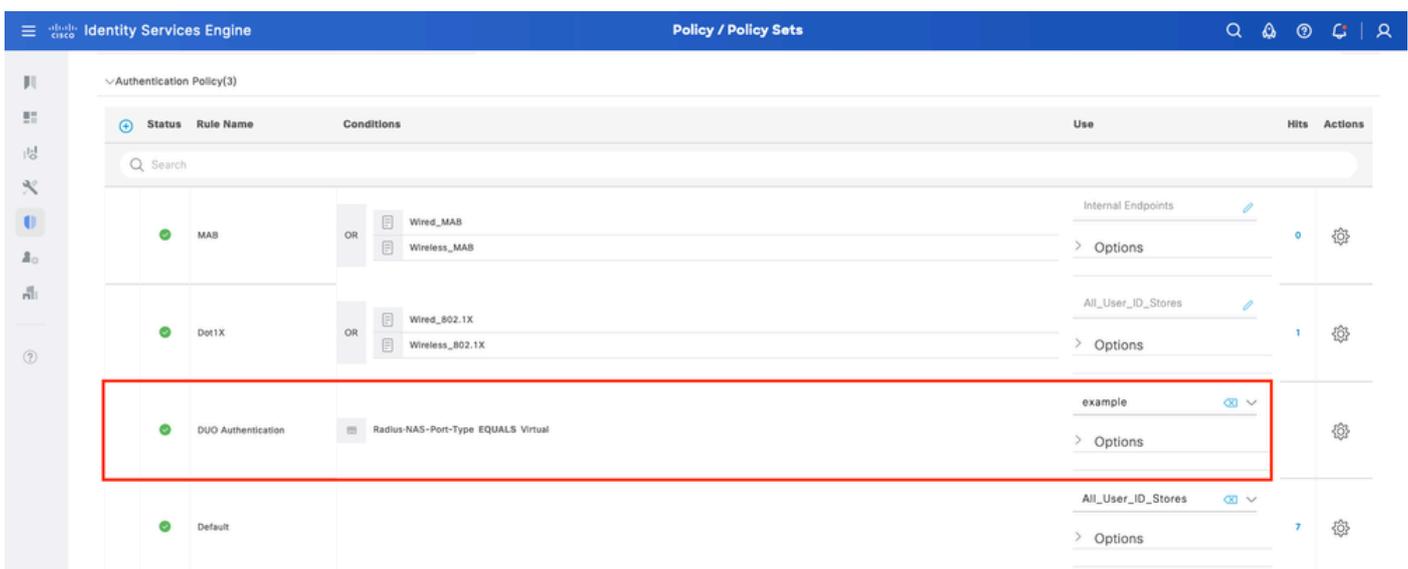
Digite o número de telefone e clique em Add Phone.



Configurar conjuntos de políticas

1. Configurar Política de Autenticação

Navegue até Política > Conjunto de políticas. Selecione o conjunto de políticas para o qual você deseja habilitar a MFA. Configure a Política de Autenticação com o Repositório de Identidades de Autenticação Primária como Ative Directory.



Conjunto de políticas 1

2. Configurar a Política de MFA

Quando o MFA estiver habilitado no ISE, uma nova seção em Conjuntos de políticas do ISE estará disponível. Expanda MFA Policy e clique em + para adicionar MFA Policy. Configure MFA Conditions (Configurar condições de MFA) de sua escolha, selecione DUO-MFA configurado anteriormente na seção Use. Clique em Save.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The main area shows a table of Policy Sets, with the 'MFA Policy(1)' section expanded. A red box highlights the 'DUO Rule' configuration, showing the condition 'Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA', the 'Use' field set to 'DUO-MFA', and the 'Options' dropdown menu. Another red box highlights the 'Save' button at the bottom right of the configuration area.

Política do ISE

 Observação: a política configurada acima depende do grupo de túneis chamado RA. Os usuários conectados ao grupo de túneis RA são forçados a executar o MFA. A configuração do ASA/FTD está fora do escopo deste documento. Use este [documento](#) para configurar o ASA/FTD

3. Configurar Política de Autorização

Configure a Diretiva de Autorização com a condição Grupo do Ative Directory e as permissões de sua escolha.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Authorization Policies. The main area shows a table of Authorization Policies, with the 'DUO Authorization Rule' configuration highlighted by a red box. The configuration shows the condition 'example-ExternalGroups EQUALS example.com/Users/DUO Group', the 'Profiles' field set to 'PermitAccess', and the 'Security Groups' field set to 'Select from list'. The 'Hits' field shows '5'.

Conjunto de políticas 3

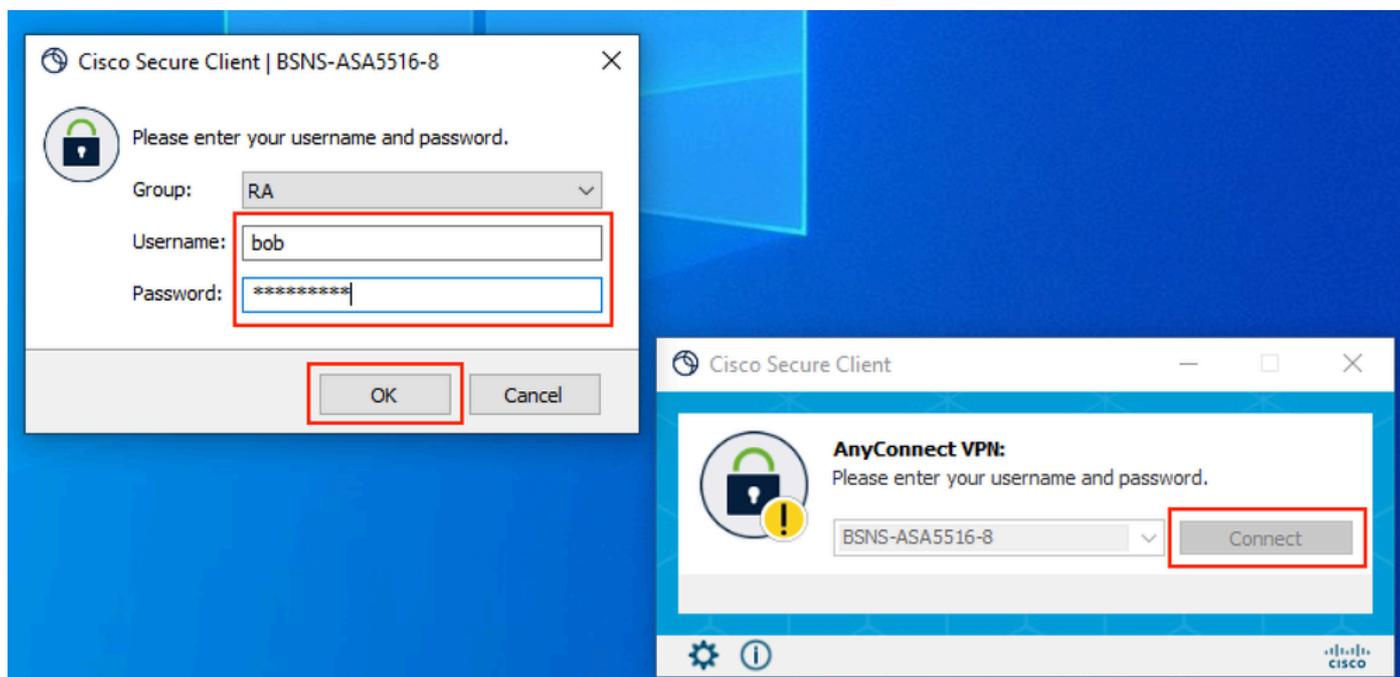
Limitações

No momento em que este documento foi escrito:

1. Apenas push e telefone DUO são suportados como um método de autenticação de segundo fator
2. Nenhum grupo é enviado para a nuvem DUO, somente a sincronização do usuário é suportada
3. Somente os seguintes casos de uso de autenticação multifator são suportados:
 - Autenticação de usuário VPN
 - Autenticação de acesso de administrador TACACS+

Verificar

Abra o Cisco Secure Client, clique em Connect. Forneça Username e Password e clique em OK.



Cliente de VPN

O Dispositivo Móvel do Usuário deve receber uma Notificação por Push DUO. Aprove-o. Conexão VPN estabelecida.

1:52



Search

Accounts (8)

Add



Cisco
Cisco



Are you logging in to Auth API?

🌐 Cisco

🕒 1:52 PM

👤 bob

Logs relacionados a MFA	mecanismo de política	ise-psc.log	DuoMfaAuthApiUtils -:::- Solicitação enviada ao gerenciador de cliente Duo DuoMfaAuthApiUtils → Resposta Duo
Logs relacionados à política	prrt-JNI	prt-management.log	ProcessadorDeSolicitaçãoDePolíticaDeMfaDeRaio TcacacsMfaPolicyRequestProcessor
Logs relacionados à autenticação	runtime-AAA	prt-server.log	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
Autenticação DUO, logs relacionados à Sincronização de ID		duo-sync-service.log	

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.