

Configuración de la autenticación multifactor nativa ISE 3.3 con DUO

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de flujo](#)

[Configuraciones](#)

[Seleccione las aplicaciones que desea proteger](#)

[Integración de ISE con Active Directory](#)

[Activar API abierta](#)

[Activar origen de identidad de MFA](#)

[Configurar origen de identidad externa de MFA](#)

[Inscribir usuario en DUO](#)

[Configurar conjuntos de políticas](#)

[Limitaciones](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo integrar el parche 1 de Identity Services Engine (ISE) 3.3 con DUO para la autenticación multifactor. Desde la versión 3.3, parche 1, ISE se puede configurar para la integración nativa con servicios DUO, por lo que se elimina la necesidad del proxy de autenticación.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- ISE
- DUO

Componentes Utilizados

La información de este documento se basa en:

- Parche 1 de Cisco ISE versión 3.3
- DUO
- Cisco ASA versión 9.16(4)
- Cisco Secure Client versión 5.0.04032

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de flujo

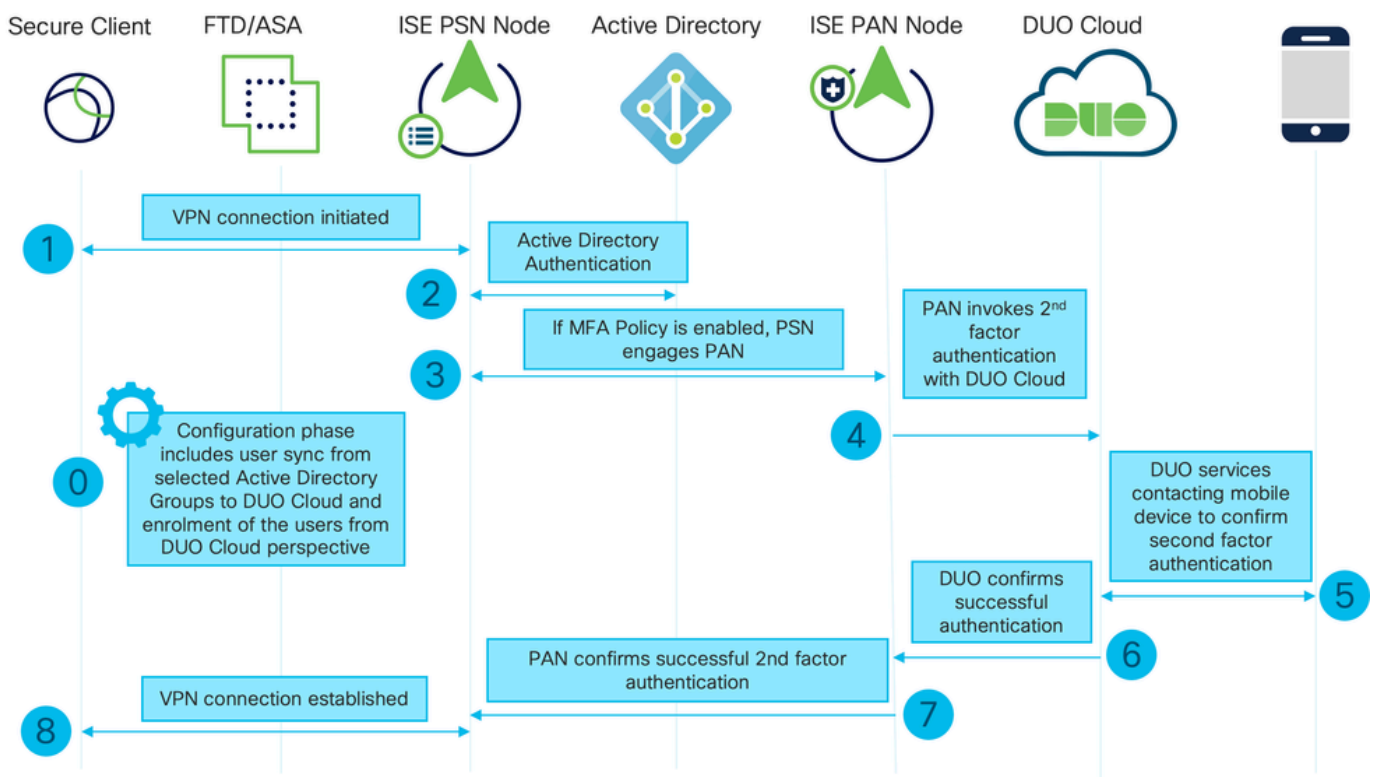


Diagrama de flujo

Pasos

0. La fase de configuración incluye la selección de los grupos de Active Directory, desde los cuales se sincronizan los usuarios, la sincronización se realiza una vez que se completa el asistente de MFA. Consta de dos pasos. Búsquedas en Active Directory para obtener la lista de usuarios y determinados atributos. Se realiza una llamada a DUO Cloud con API de administración para que los usuarios accedan a ella. Los administradores deben inscribir usuarios. La inscripción puede incluir el paso opcional de activar el usuario para Duo Mobile, que permite a los usuarios utilizar la autenticación de un solo toque con Duo Push

1. Se inicia la conexión VPN, el usuario introduce el nombre de usuario y la contraseña y hace clic en Aceptar. El dispositivo de red envía la solicitud de acceso RADIUS y se envía a PSN

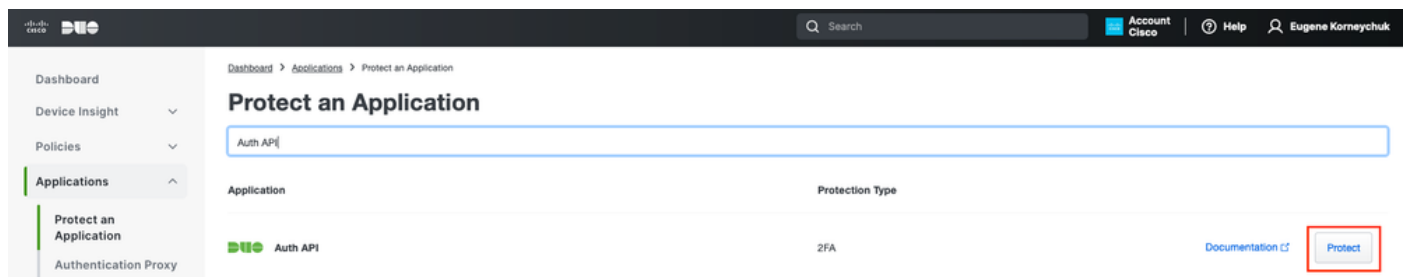
2. El nodo PSN autentica al usuario mediante Active Directory
3. Cuando la autenticación se realiza correctamente y se configura la política MFA, PSN interactúa con PAN para comunicarse con DUO Cloud
4. Se realiza una llamada a DUO Cloud con Auth API para invocar una autenticación de segundo factor con DUO
5. La autenticación de segundo factor tiene lugar. El usuario completa el proceso de autenticación de segundo factor
6. DUO responde a PAN con el resultado de la autenticación de segundo factor
7. PAN responde a PSN con el resultado de la autenticación de segundo factor
8. La aceptación de acceso se envía al dispositivo de red, se establece la conexión VPN

Configuraciones

Seleccione las aplicaciones que desea proteger

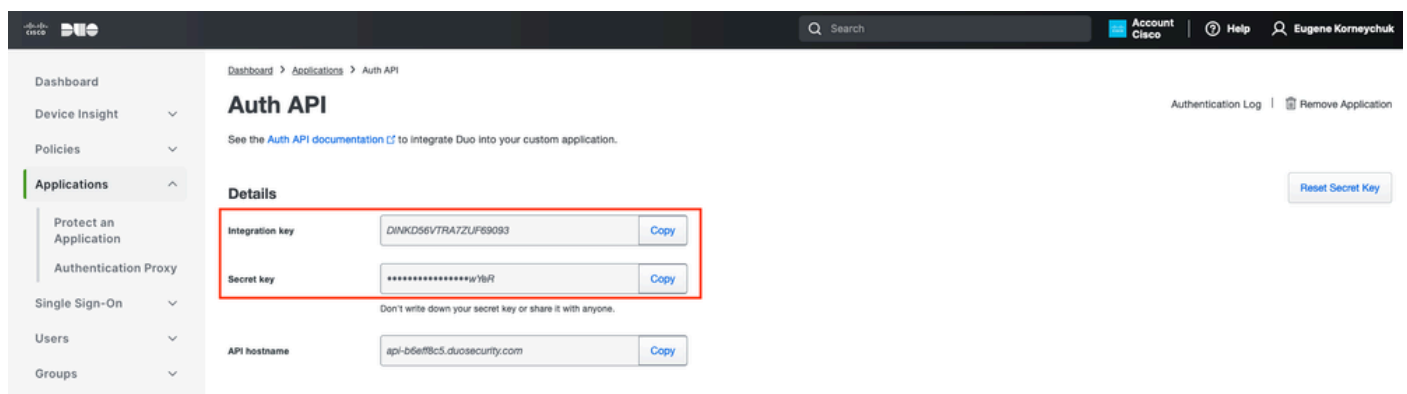
Vaya a DU Admin Dashboard <https://admin.duosecurity.com/login>. Inicie sesión con credenciales de administrador.

Vaya a Panel > Aplicaciones > Proteger una aplicación. Busque Auth API y seleccione Protect.



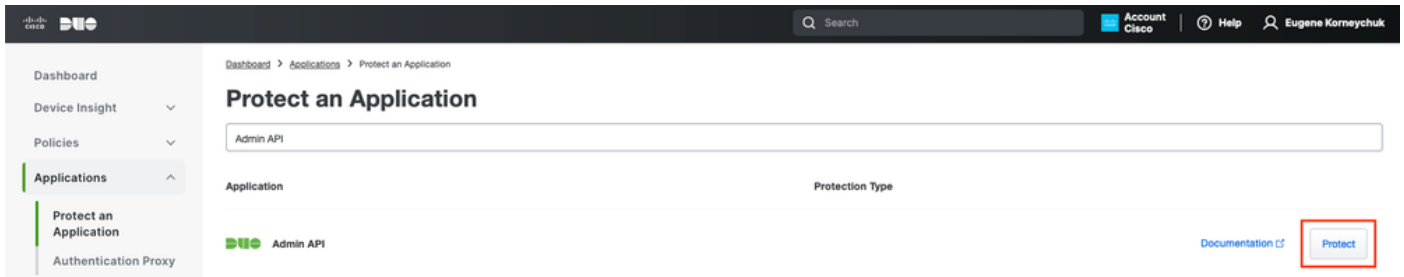
API de autenticación 1

Anote la clave de integración y la clave secreta.



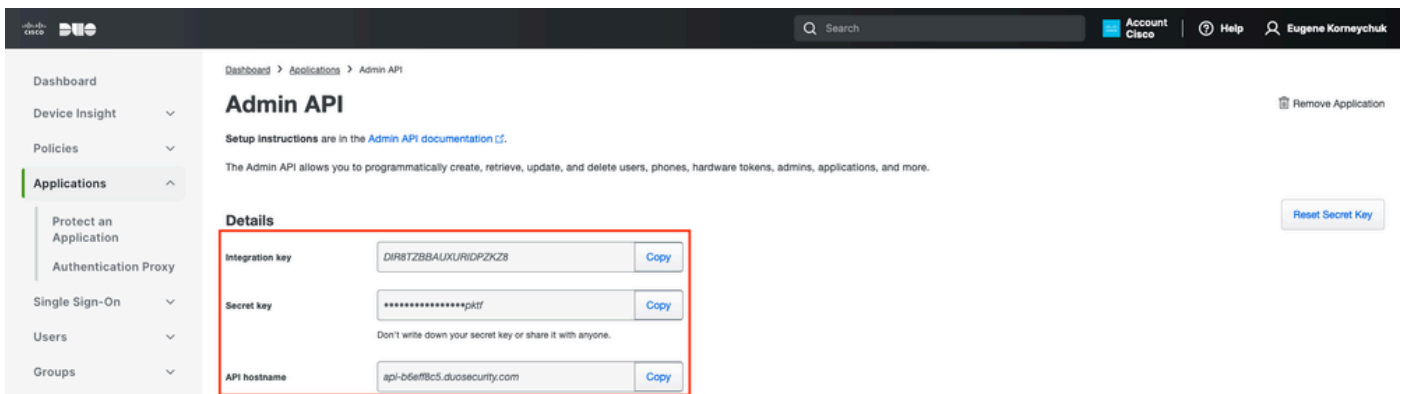
API de autenticación 2

Vaya a Panel > Aplicaciones > Proteger una aplicación. Busque Admin API y seleccione Protect.



API de autenticación 1

Anote la clave de integración, la clave secreta y el nombre de host de la API.



API de administración 2

Configurar permisos de API

Vaya a Panel > Aplicaciones > Aplicación. Seleccione Admin API.

Marque Grant Read Resource y Grant Write Resource permissions. Haga clic en Guardar cambios.

- 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 administración 3

Integración de ISE con Active Directory

1. Vaya a Administration > Identity Management > External Identity Stores > Active Directory > Add. Proporcione el nombre del punto de unión, el dominio de Active Directory y haga clic en Enviar.

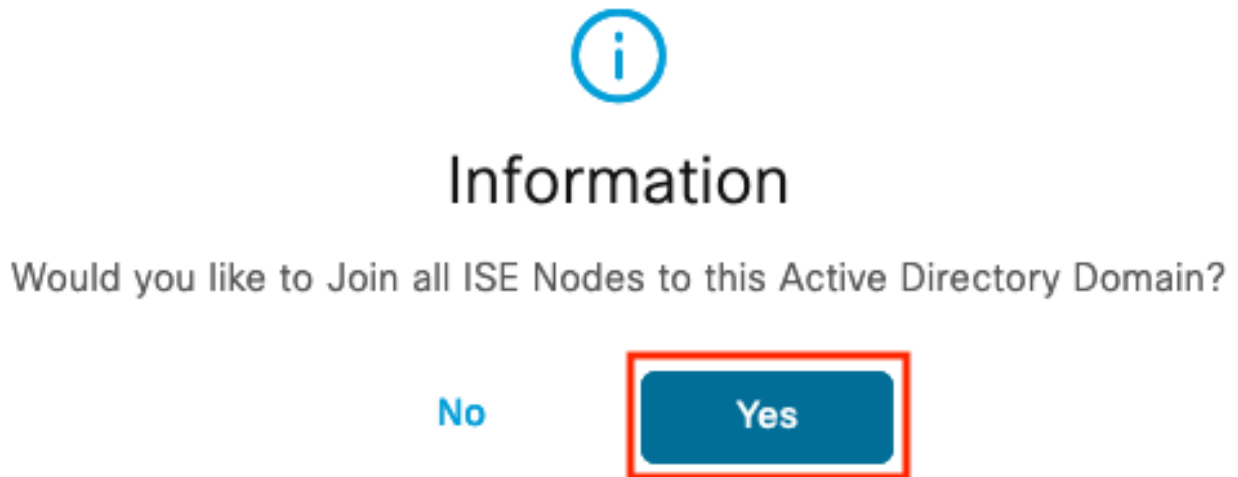
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is Administration / Identity Management. The main menu includes Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The 'External Identity Sources' section is active, and the 'Active Directory' option is selected. The 'Connection' configuration page is displayed, showing the following fields:

- Join Point Name: example
- Active Directory Domain: example.com

At the bottom right of the configuration page, there are 'Submit' and 'Cancel' buttons.

Active Directory 1

2. Cuando se le solicite que una todos los nodos ISE a este dominio de Active Directory, haga clic en Sí.



Information

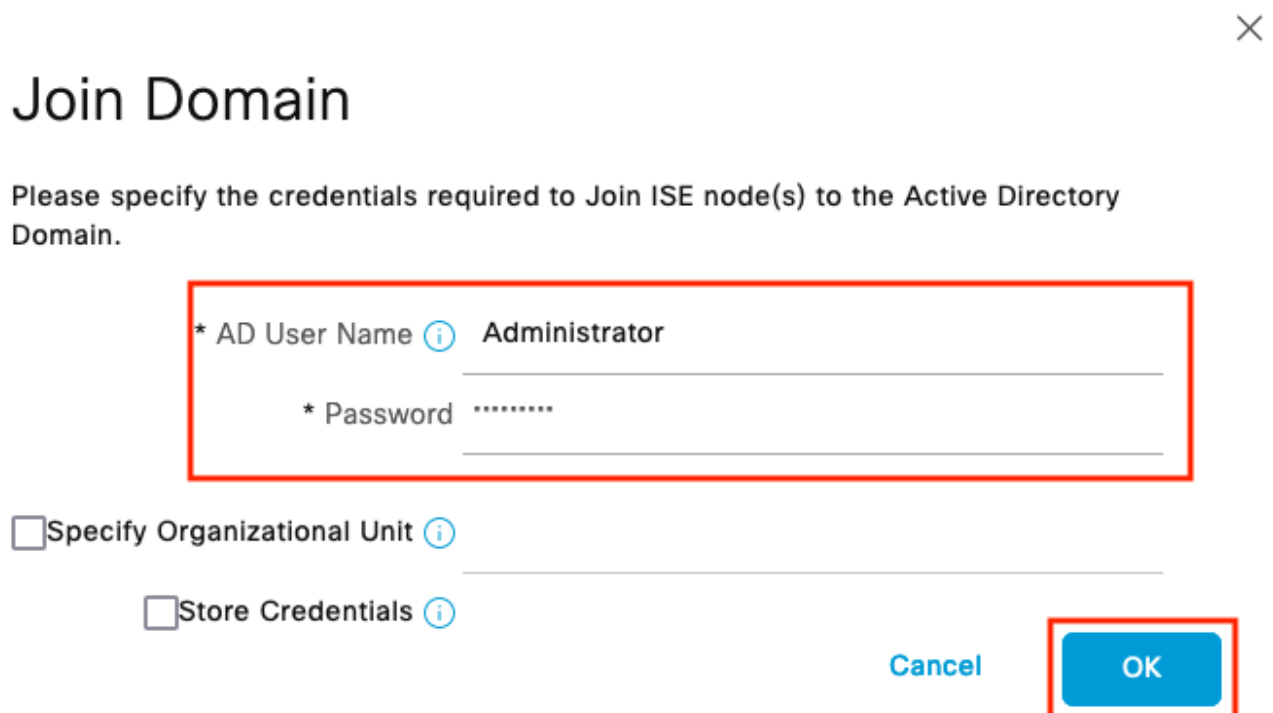
Would you like to Join all ISE Nodes to this Active Directory Domain?

No Yes

The image shows a dialog box with a blue information icon at the top. Below it, the title "Information" is centered. The main text asks "Would you like to Join all ISE Nodes to this Active Directory Domain?". There are two buttons: "No" and "Yes". The "Yes" button is highlighted with a red rectangular border.

Active Directory 2

3. Proporcione el nombre de usuario y la contraseña de AD y haga clic en Aceptar.



Join Domain

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

* AD User Name *i* Administrator

* Password

Specify Organizational Unit *i*

Store Credentials *i*


Cancel OK

The image shows a "Join Domain" dialog box with a close button (X) in the top right corner. The title "Join Domain" is at the top. Below it, the text says "Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.". There are two input fields: "* AD User Name" with the value "Administrator" and "* Password" with masked characters ".....". Below these are two checkboxes: "Specify Organizational Unit" and "Store Credentials", both with information icons. At the bottom right, there are "Cancel" and "OK" buttons. The "OK" button is highlighted with a red rectangular border.

Directorio activo 3

La cuenta de AD necesaria para el acceso al dominio en ISE puede tener cualquiera de estas características:

- Agregar estaciones de trabajo al derecho de usuario del dominio correspondiente
- Crear objetos de equipo o Eliminar objetos de equipo en el contenedor de equipos correspondiente donde se crea la cuenta del equipo ISE antes de que se una al equipo ISE en el dominio

 Nota: Cisco recomienda deshabilitar la política de bloqueo para la cuenta ISE y configurar la infraestructura AD para enviar alertas al administrador si se utiliza una contraseña incorrecta para esa cuenta. Cuando se introduce una contraseña incorrecta, ISE no crea ni modifica su cuenta de equipo cuando es necesario y, por lo tanto, posiblemente deniegue todas las autenticaciones.

4. El estado de AD es operativo.

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

Directorio activo 4

5. Vaya a Grupos > Agregar > Seleccionar grupos del directorio > Recuperar grupos. Active las casillas de verificación de los grupos de AD que desee (que se utilizan para sincronizar usuarios y para la directiva de autorización), como se muestra en esta imagen.

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

Active Directory 5

6. Haga clic en Guardar para guardar los grupos de AD recuperados.

Connection		Allowed Domains	PassiveID	Groups	Attributes	Advanced Settings
Edit + Add Delete Group Update SID Values						
<input type="checkbox"/>	Name	SID				
<input type="checkbox"/>	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-2558713077-...				

Save Reset

Active Directory 6

Activar API abierta

Vaya a Administration > System > Settings > API Settings > API Service Settings. Habilite Open API y haga clic en Save.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System Settings page. The 'API Settings' section is expanded, showing 'API Service Settings for Primary Administration Node' and 'API Service Setting for All Other Nodes'. The 'Open API (Read/Write)' toggle is highlighted with a red box and is turned on. The 'Open API (Read)' toggle is also turned on. The 'CSRF Check (only for ERS Settings)' section is expanded, showing the 'Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)' option selected.

API abierta

Activar origen de identidad de MFA

Vaya a Administration > Identity Management > Settings > External Identity Sources Settings. Habilite MFA y haga clic en Guardar.

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**

ISE MFA 1

Configurar origen de identidad externa de MFA

Vaya a Administration > Identity Management > External Identity Sources. Haga clic en Agregar. En la pantalla Welcome (Bienvenido), haga clic en Let's Do It (Hagámoslo).

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.

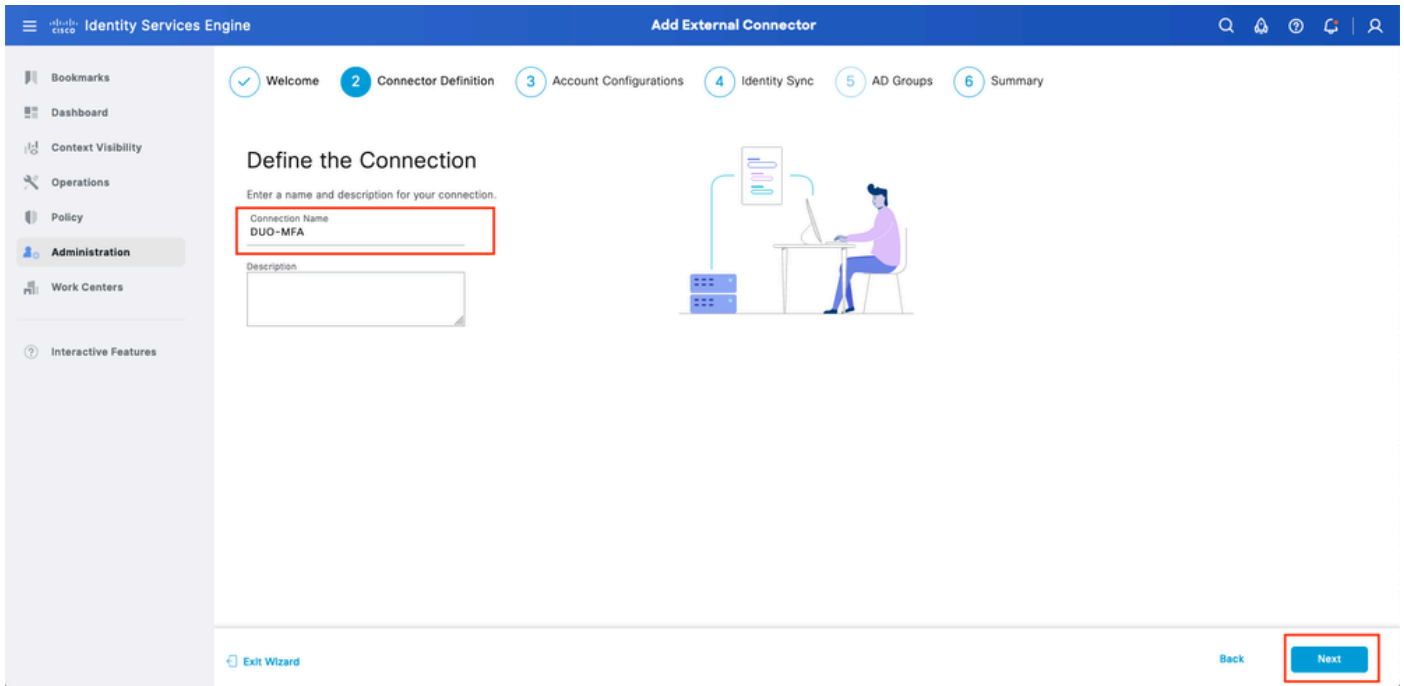
Before you begin, the following prerequisites apply:

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**

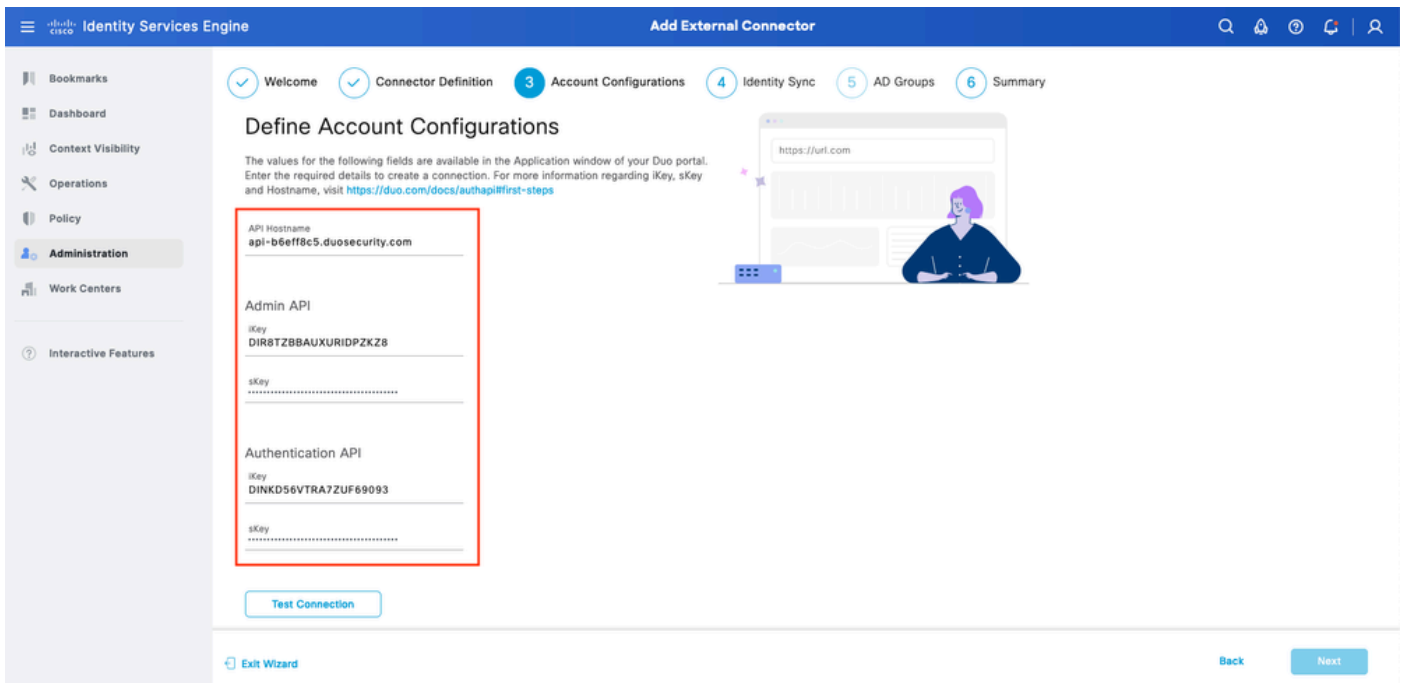
Asistente 1 de ISE DUO

En la siguiente pantalla, configure Connection Name y haga clic en Next.



Asistente 2 de ISE DUO

Configure los valores de Nombre de host de API, Integración de API de administración y Claves secretas, Integración de API de autenticación y Claves secretas desde el paso Select Applications to Protect.



Asistente de ISE DUO 3

Haga clic en Probar conexión. Una vez que la conexión de prueba tenga éxito, puede hacer clic en Next (Siguiente).

Test Connection

MFA Auth and Admin API Integration and Secret Keys are valid


Exit Wizard

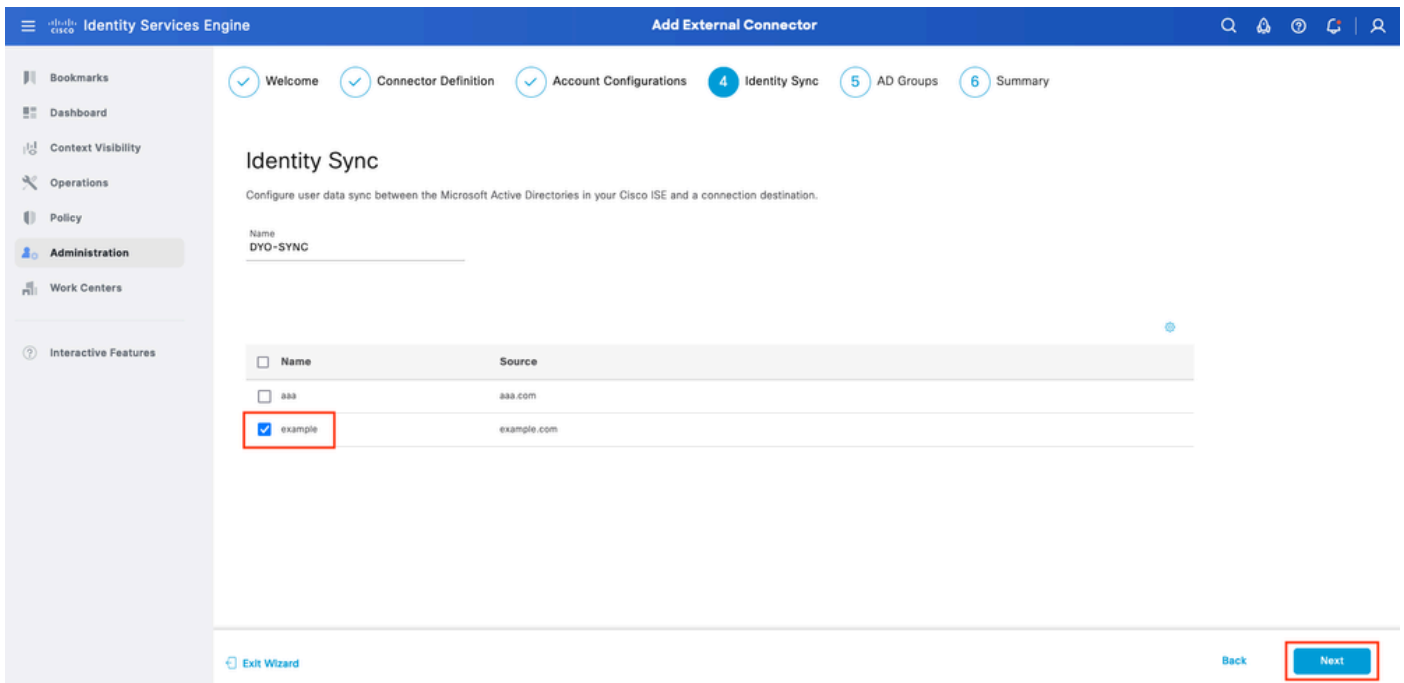
Back

Next

Asistente para ISE DUO 4

Configure Identity Sync. Este proceso sincroniza a los usuarios de los grupos de Active Directory que seleccione en la cuenta DUO mediante las credenciales de la API proporcionadas anteriormente. Seleccione Active Directory Join Point. Haga clic en Next.

 Nota: La configuración de Active Directory está fuera del alcance del documento. Siga este [documento](#) para integrar ISE con 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

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

Exit Wizard Back Next

Asistente para ISE DUO 5

Seleccione Active Directory Groups desde el cual desea que los usuarios se sincronicen con DUO. Haga clic en 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.

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

Exit Wizard Back **Next**

Asistente para ISE DUO 6

Verifique que la configuración sea correcta y haga clic en Finalizado.

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**

Asistente de ISE DUO 7

Inscribir usuario en DUO

 **Nota:** La inscripción de usuarios DUO está fuera del alcance del documento. Considere este [documento](#) para obtener más información sobre la inscripción de usuarios. A los efectos de este documento, se utiliza la inscripción de usuario manual.

Abra el panel de administración de DUO. Vaya a Panel > Usuarios. Haga clic en el usuario

sincronizado desde 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

DUO enroll 1

Desplácese hacia abajo hasta Teléfonos. Haga clic en Agregar teléfono.

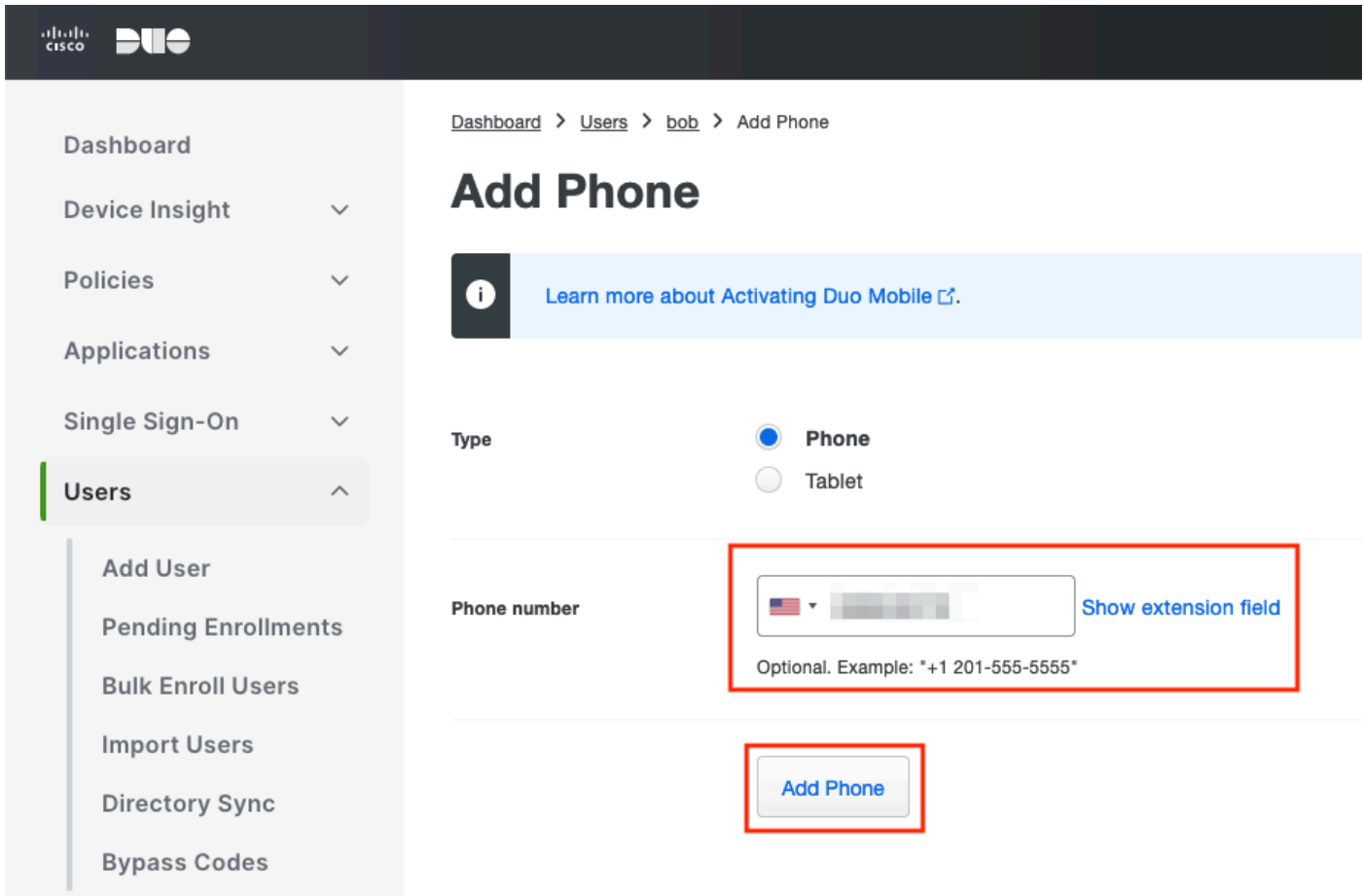
Phones

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](#)

DUO enroll 2

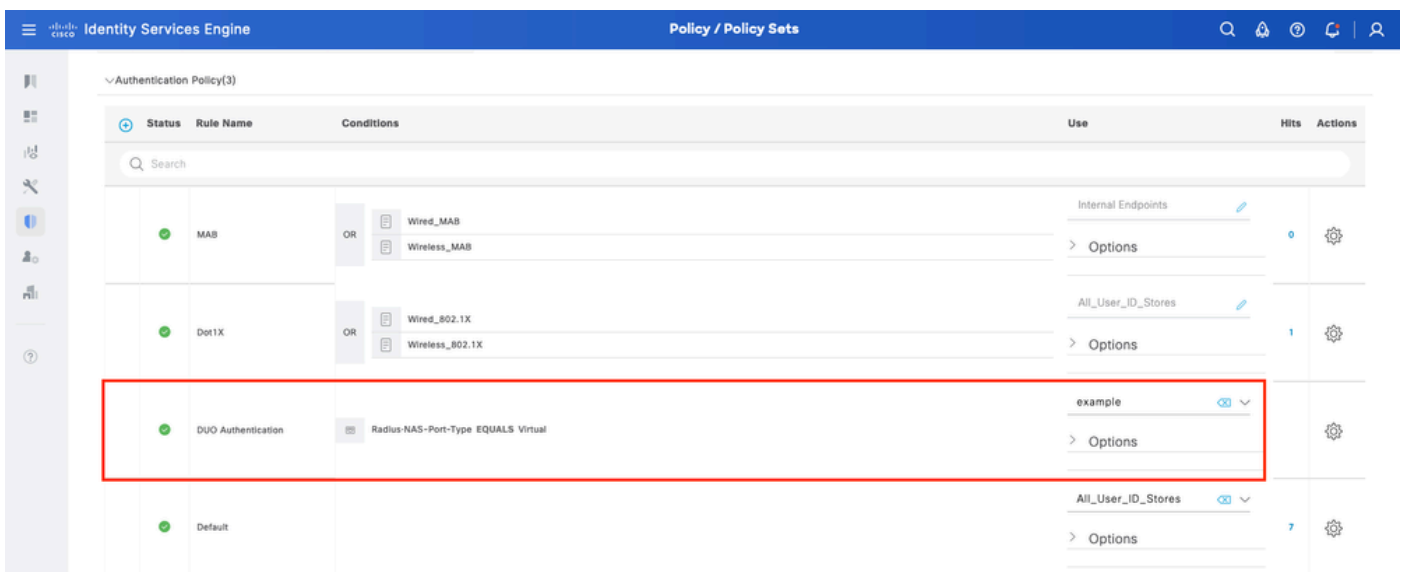
Introduzca el número de teléfono y haga clic en Agregar teléfono.



Configurar conjuntos de políticas

1. Configurar la política de autenticación

Vaya a Policy > Policy Set. Seleccione el conjunto de políticas para el que desea activar MFA. Configure la política de autenticación con el almacén de identidades de autenticación principal como Active Directory.




Conjunto de políticas 1

2. Configuración de la política MFA

Una vez que MFA esté habilitado en ISE, habrá disponible una nueva sección en los conjuntos de políticas de ISE. Expanda Política de MFA y haga clic en + para agregar la Política de MFA. Configure las condiciones MFA de su elección, seleccione DUO-MFA configurado previamente en la sección Use. Haga clic en Guardar.

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

Política de ISE

 Nota: La política configurada anteriormente depende del grupo de túnel denominado RA. Los usuarios conectados al grupo de túnel RA se ven obligados a realizar MFA. La configuración de ASA/FTD está fuera del alcance de este documento. Utilice este [documento](#) para configurar ASA/FTD

3. Configurar directiva de autorización

Configure la directiva de autorización con la condición y los permisos del grupo de Active Directory que elija.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Authorization Policies. The main area displays a table of Authorization Policies, including a 'DUO Authorization Rule' with the condition 'example-ExternalGroups EQUALS example.com/Users/DUO Group' and the 'PermitAccess' profile. The 'Save' button at the bottom right is also highlighted with a red box.

Conjunto de políticas 3

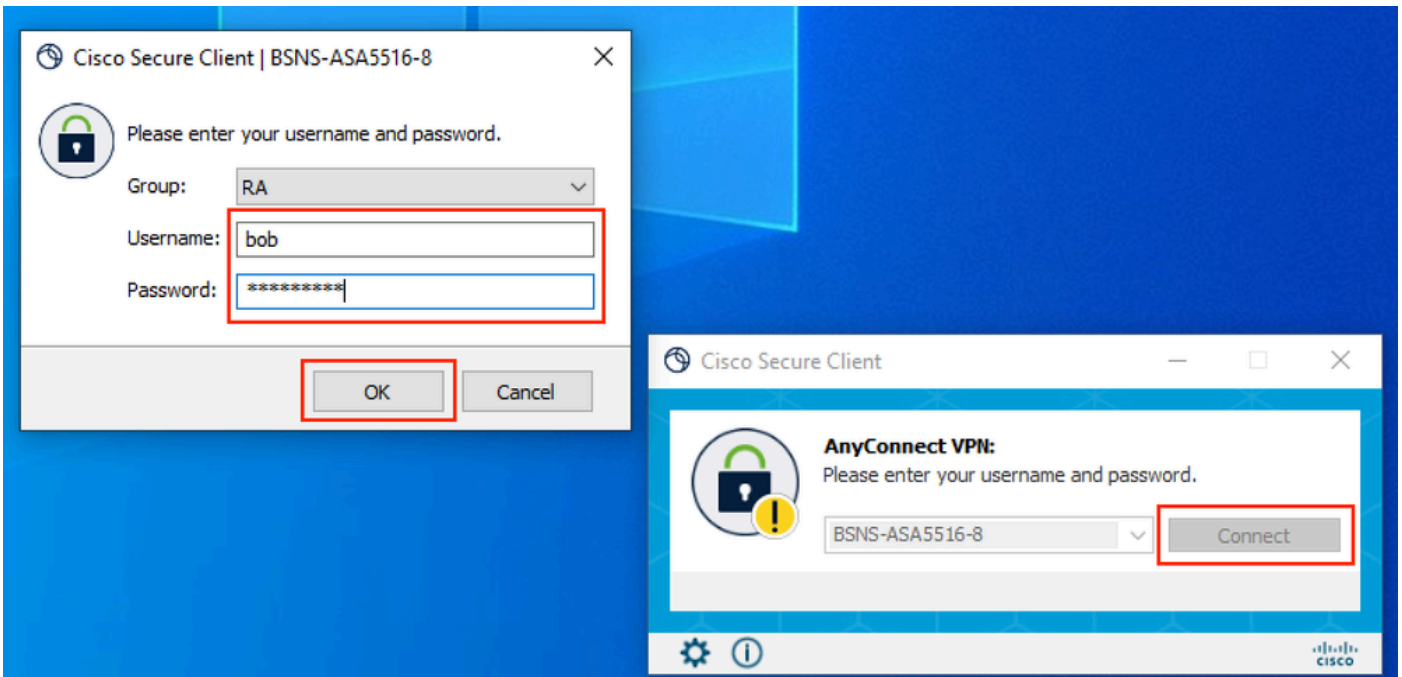
Limitaciones

En el momento de escribir este documento:

1. Solo DUO push y teléfono son compatibles como método de autenticación de segundo factor
2. No se envía ningún grupo a DUO Cloud, solo se admite la sincronización del usuario
3. Solo se admiten los siguientes casos prácticos de autenticación multifactor:
 - Autenticación de usuario VPN
 - Autenticación de acceso de administrador TACACS+

Verificación

Abra Cisco Secure Client, haga clic en Connect. Proporcione Nombre de usuario y Contraseña y haga clic en Aceptar.



Cliente VPN

Los usuarios de dispositivos móviles deben recibir una notificación DUO Push. Aprobar esto. Se ha establecido la conexión VPN.

1:52



Search

Accounts (8)

Add



Cisco
Cisco



Are you logging in to Auth API?

🌐 Cisco

🕒 1:52 PM

👤 bob

Registros relacionados con MFA	motor de políticas	ise-psc.log	DuoMfaAuthApiUtils -::- Solicitud enviada a Duo Client manager DuoMfaAuthApiUtils → Duo response
Registros relacionados con la política	prrt-JNI	port-management.log	RadiusMfaPolicyRequestProcessor TacacsMfaPolicyRequestProcessor
Registros relacionados con la autenticación	Runtime-AAA	prrt-server.log	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
Registros relacionados con autenticación DUO, sincronización de ID		duo-sync-service.log	

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).