

Konfigurieren der nativen Multi-Factor-Authentifizierung mit DUO für ISE 3.3

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Flussdiagramm](#)

[Konfigurationen](#)

[Zu schützende Anwendungen auswählen](#)

[Integration der ISE mit Active Directory](#)

[Offene API aktivieren](#)

[MFA-Identitätsquelle aktivieren](#)

[Externe MFA-Identitätsquelle konfigurieren](#)

[Benutzer für DUO registrieren](#)

[Konfigurieren von Richtlinienansätzen](#)

[Einschränkungen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Integration von Identity Services Engine (ISE) 3.3 Patch 1 mit DUO für Multi-Factor Authentication beschrieben. Ab Version 3.3 Patch 1 kann ISE für die native Integration in DUO-Dienste konfiguriert werden, sodass der Authentifizierungsproxy nicht mehr erforderlich ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- ISE
- DUO

Verwendete Komponenten

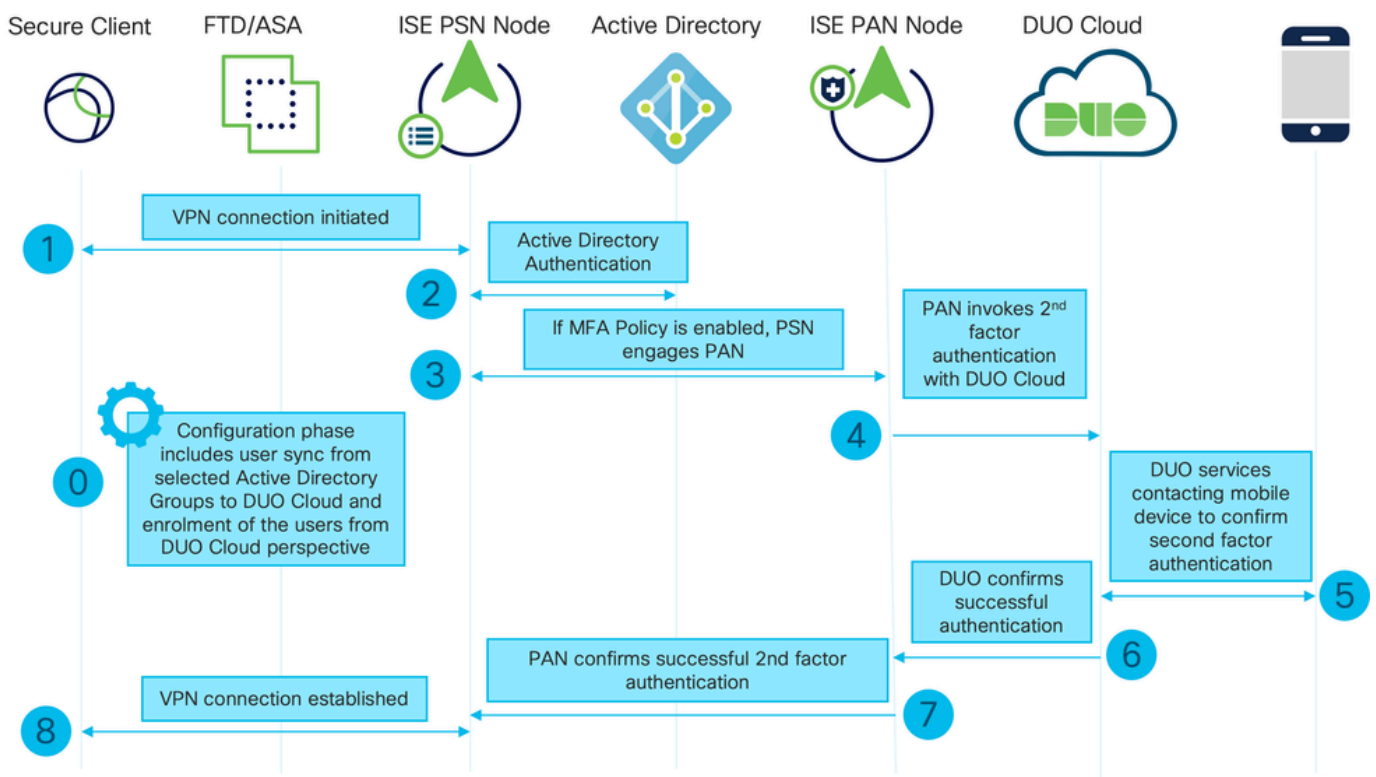
Die Informationen in diesem Dokument basieren auf:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Flussdiagramm



Flussdiagramm

Schritte

0. Die Konfigurationsphase umfasst die Auswahl der Active Directory-Gruppen, von denen die Benutzer synchronisiert werden. Die Synchronisierung erfolgt, sobald der MFA-Assistent abgeschlossen ist. Es besteht aus zwei Schritten. Sucht in Active Directory nach der Liste der Benutzer und bestimmten Attributen. Ein Anruf bei DUO Cloud mit Admin-API dient dazu, Benutzer dorthin zu lotsen. Administratoren müssen Benutzer registrieren. Die Registrierung kann den optionalen Schritt der Aktivierung des Benutzers für Duo Mobile umfassen, der es Ihren Benutzern ermöglicht, eine One-Tap-Authentifizierung mit Duo Push zu verwenden

1. VPN-Verbindung wird initiiert, der Benutzer gibt den Benutzernamen und das Passwort ein und klickt auf OK. Netzwerkgerät sendet RADIUS-Zugriffsanforderung wird an PSN gesendet

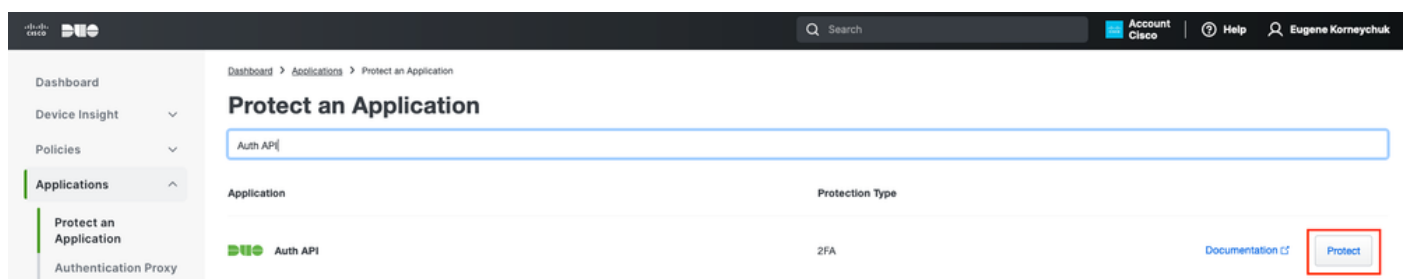
2. Der PSN-Knoten authentifiziert den Benutzer über Active Directory
3. Wenn die Authentifizierung erfolgreich ist und die MFA-Richtlinie konfiguriert ist, aktiviert PSN PAN, um DUO Cloud zu kontaktieren.
4. Ein Aufruf an DUO Cloud mit Auth API wird durchgeführt, um eine zweite Faktor Authentifizierung mit DUO aufzurufen
5. Second-Factor-Authentifizierung erfolgt. Der Benutzer schließt den Authentifizierungsprozess mit dem zweiten Faktor ab.
6. DUO reagiert auf PAN mit dem Ergebnis der zweiten Faktor Authentifizierung
7. PAN antwortet auf PSN mit dem Ergebnis der zweiten Faktor-Authentifizierung
8. Access-Accept wird an das Netzwerkgerät gesendet, VPN-Verbindung wird hergestellt

Konfigurationen

Zu schützende Anwendungen auswählen

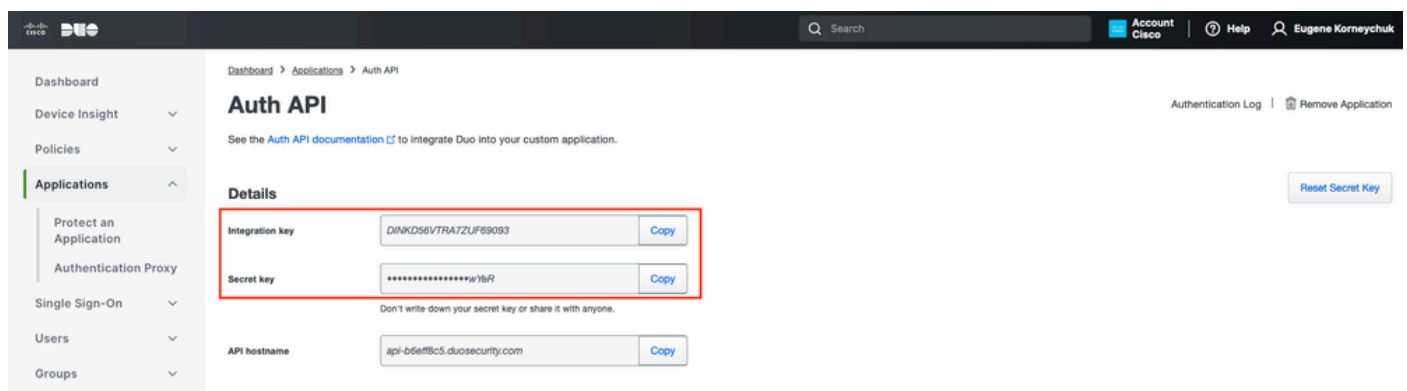
Navigieren Sie zu DUO Admin Dashboard <https://admin.duosecurity.com/login>. Melden Sie sich mit Administratorrechten an.

Navigieren Sie zu Dashboard > Anwendungen > Eine Anwendung schützen. Suchen Sie nach Auth API, und wählen Sie Schützen aus.



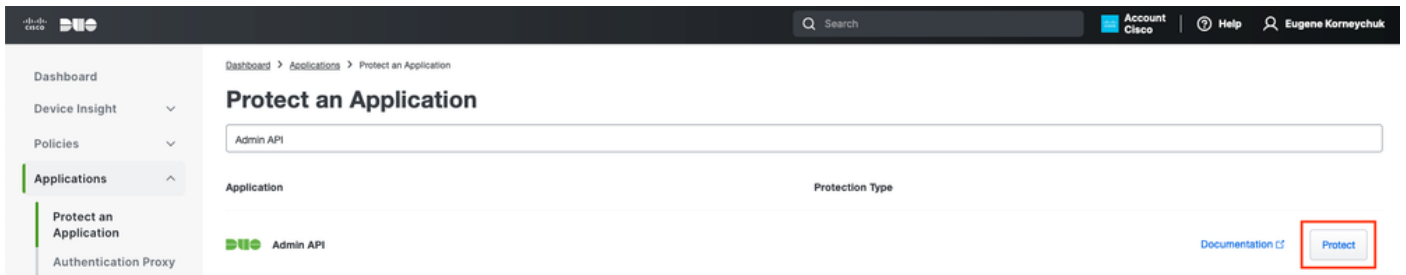
Auth-API 1

Notieren Sie sich den Integrationsschlüssel und den geheimen Schlüssel.



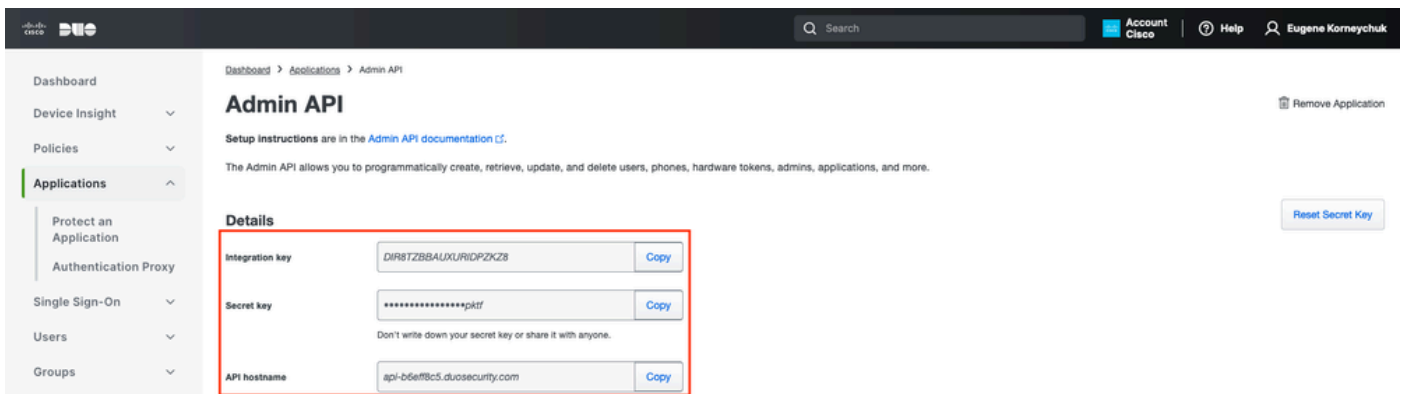
Auth-API 2

Navigieren Sie zu Dashboard > Anwendungen > Eine Anwendung schützen. Suchen Sie nach der Admin-API, und wählen Sie Schützen aus.



Auth-API 1

Notieren Sie sich den Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen.



Admin-API 2

Konfigurieren von API-Berechtigungen

Navigieren Sie zu Dashboard > Anwendungen > Anwendung. Wählen Sie Admin API aus.

Aktivieren Sie Leseressourcen gewähren und Schreibressourcenberechtigungen gewähren. Klicken Sie auf Save Changes.

- 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.

Admin-API 3

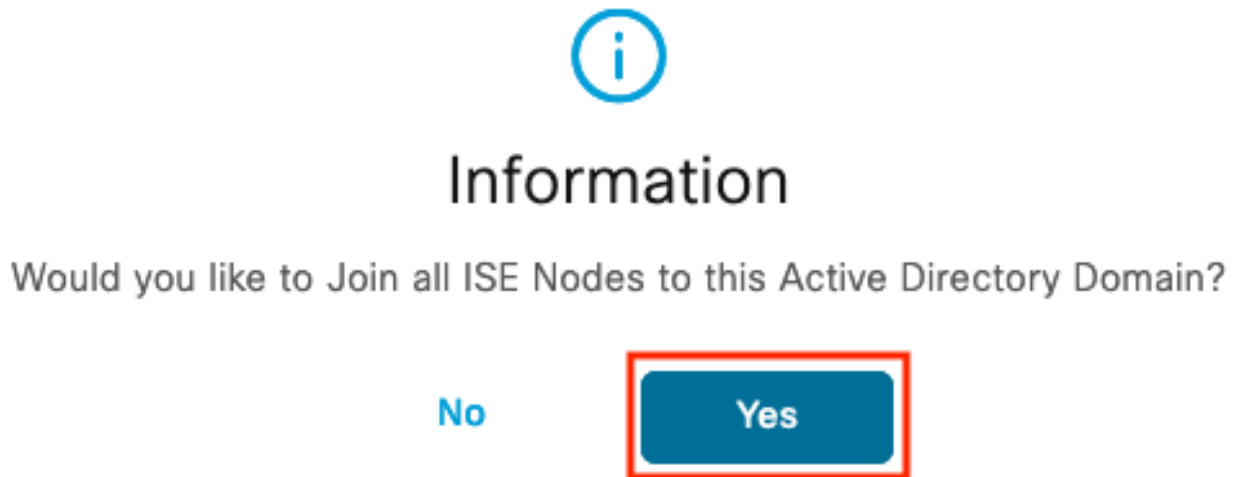
Integration der ISE mit Active Directory

1. Navigieren Sie zu Administration > Identity Management > External Identity Stores > Active Directory > Add. Geben Sie den Namen des Join Points und die Active Directory-Domäne an, und klicken Sie auf Submit (Senden).

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 'Submit' also highlighted with a red border.

Active Directory 1

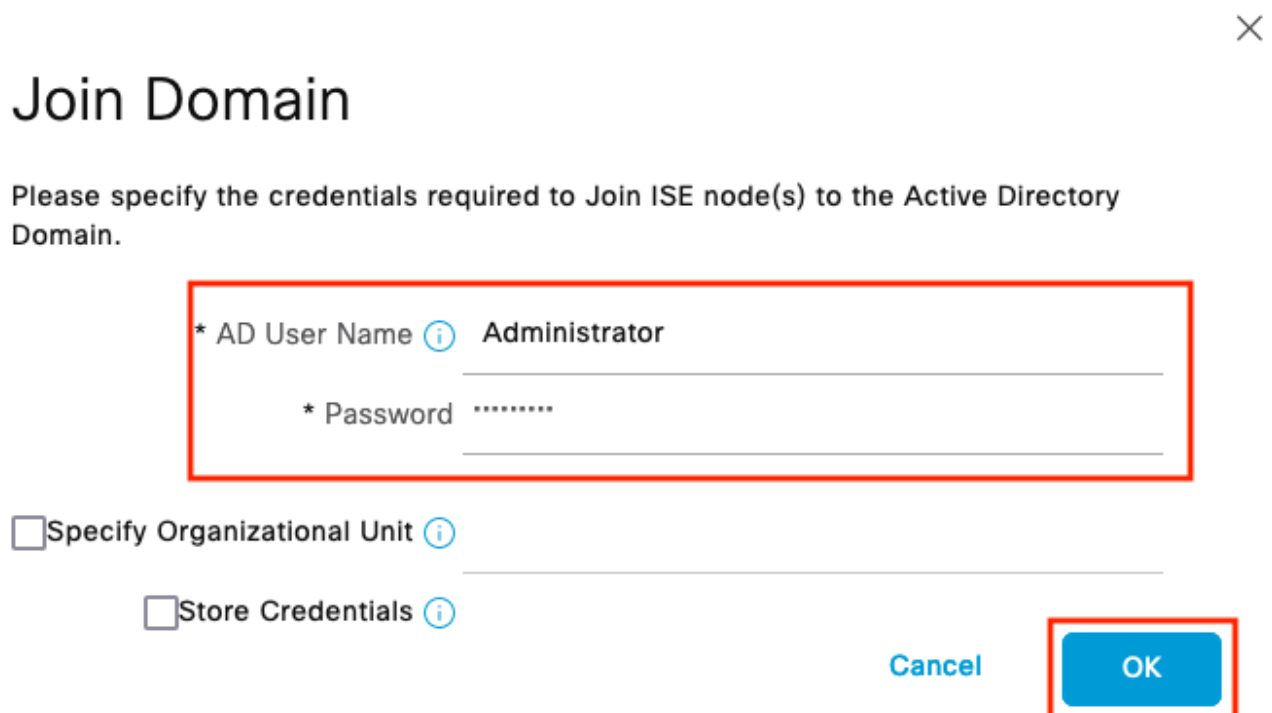
2. Wenn Sie aufgefordert werden, allen ISE-Knoten dieser Active Directory-Domäne beizutreten, klicken Sie auf Ja.



An information dialog box with a blue circular icon containing a lowercase 'i' at the top center. Below the icon is the title 'Information' in a large, bold, black font. Underneath the title is the question 'Would you like to Join all ISE Nodes to this Active Directory Domain?' in a smaller black font. At the bottom of the dialog, there are two buttons: a blue 'No' button on the left and a blue 'Yes' button on the right. The 'Yes' button is highlighted with a red rectangular border.

Active Directory 2

3. Geben Sie den AD-Benutzernamen und das AD-Kennwort ein, und klicken Sie auf OK.




A 'Join Domain' dialog box with a close button (X) in the top right corner. The title 'Join Domain' is in a large, bold, black font. Below the title is the instruction 'Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.' in a smaller black font. The main input area is enclosed in a red rectangular border and contains two fields: '* AD User Name' with an information icon and the text 'Administrator' entered, and '* Password' with a masked password '*****' entered. Below these fields are two checkboxes: 'Specify Organizational Unit' and 'Store Credentials', both with information icons. At the bottom right of the dialog, there are two buttons: a blue 'Cancel' button and a blue 'OK' button. The 'OK' button is highlighted with a red rectangular border.

Active Directory 3

Das für den Domänenzugriff in der ISE erforderliche AD-Konto kann einen der folgenden Werte aufweisen:

- Hinzufügen von Workstations zur Domänenbenutzerrechte in der entsprechenden Domäne
- Berechtigung "Computerobjekte erstellen" oder "Computerobjekte löschen" für den entsprechenden Computer-Container, in dem das Konto des ISE-Computers erstellt wird, bevor er dem ISE-Computer zur Domäne beitrifft

 Hinweis: Cisco empfiehlt, die Sperrrichtlinie für das ISE-Konto zu deaktivieren und die AD-Infrastruktur so zu konfigurieren, dass Warnmeldungen an den Administrator gesendet werden, wenn ein falsches Kennwort für das Konto verwendet wird. Bei Eingabe eines falschen Passworts erstellt oder ändert die ISE ihr Computerkonto nicht, wenn dies erforderlich ist, und verweigert daher möglicherweise alle Authentifizierungen.

4. AD-Status: "Operativ".

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	<input checked="" type="checkbox"/> Operational	WIN2022.example.com	Default-First-Site-Name
<input type="checkbox"/>	ise332.example.com	SECONDARY	<input checked="" type="checkbox"/> Operational	WIN2022.example.com	Default-First-Site-Name

Active Directory 4

5. Navigieren Sie zu Gruppen > Hinzufügen > Gruppen auswählen aus Verzeichnis > Gruppen abrufen. Aktivieren Sie die Kontrollkästchen für die gewünschten AD-Gruppen (die zum Synchronisieren von Benutzern und für Autorisierungsrichtlinien verwendet werden), wie in diesem Bild gezeigt.

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. Klicken Sie auf Speichern, um abgerufene AD-Gruppen zu speichern.

[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

Offene API aktivieren

Navigieren Sie zu Administration > System > Settings > API Settings > API Service Settings. Aktivieren Sie Open API und klicken Sie auf Speichern.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration / System > Settings > API Settings > API Service Settings. The 'Open API (Read/Write)' toggle is highlighted with a red box. Other settings include ERS (Read/Write), ERS (Read), and Open API (Read). The CSRF Check section is also visible, with the option 'Disable CSRF For ERS Request' selected.

Offene API

MFA-Identitätsquelle aktivieren

Navigieren Sie zu Administration > Identity Management > Settings > External Identity Sources Settings. Aktivieren Sie MFA, und klicken Sie auf Speichern.

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

User Custom Attributes
User Authentication Settings
Endpoint Purge
Endpoint Custom Attributes
External Identity Sources 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

ISE MFA 1

Externe MFA-Identitätsquelle konfigurieren

Navigieren Sie zu Administration > Identity Management > External Identity Sources. Klicken Sie auf Hinzufügen. Klicken Sie im Willkommensbildschirm auf 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.

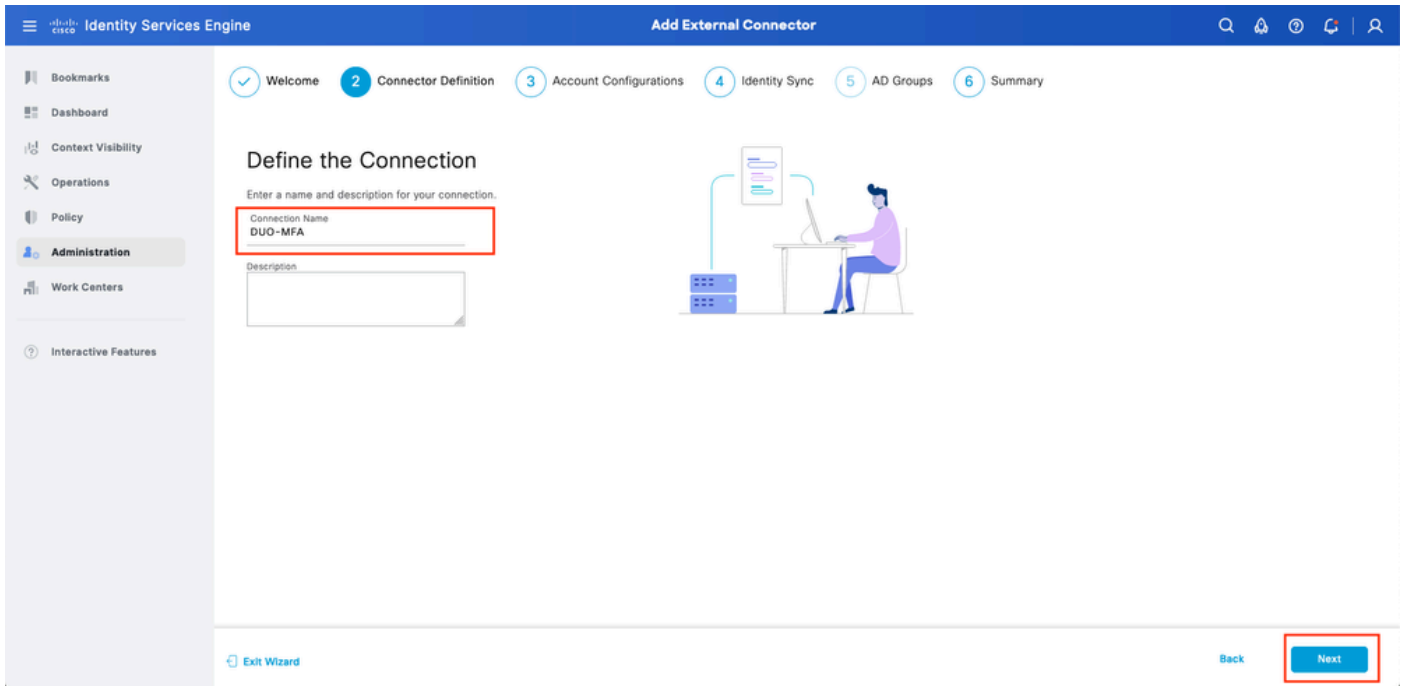
Before you begin, the following prerequisites apply:

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

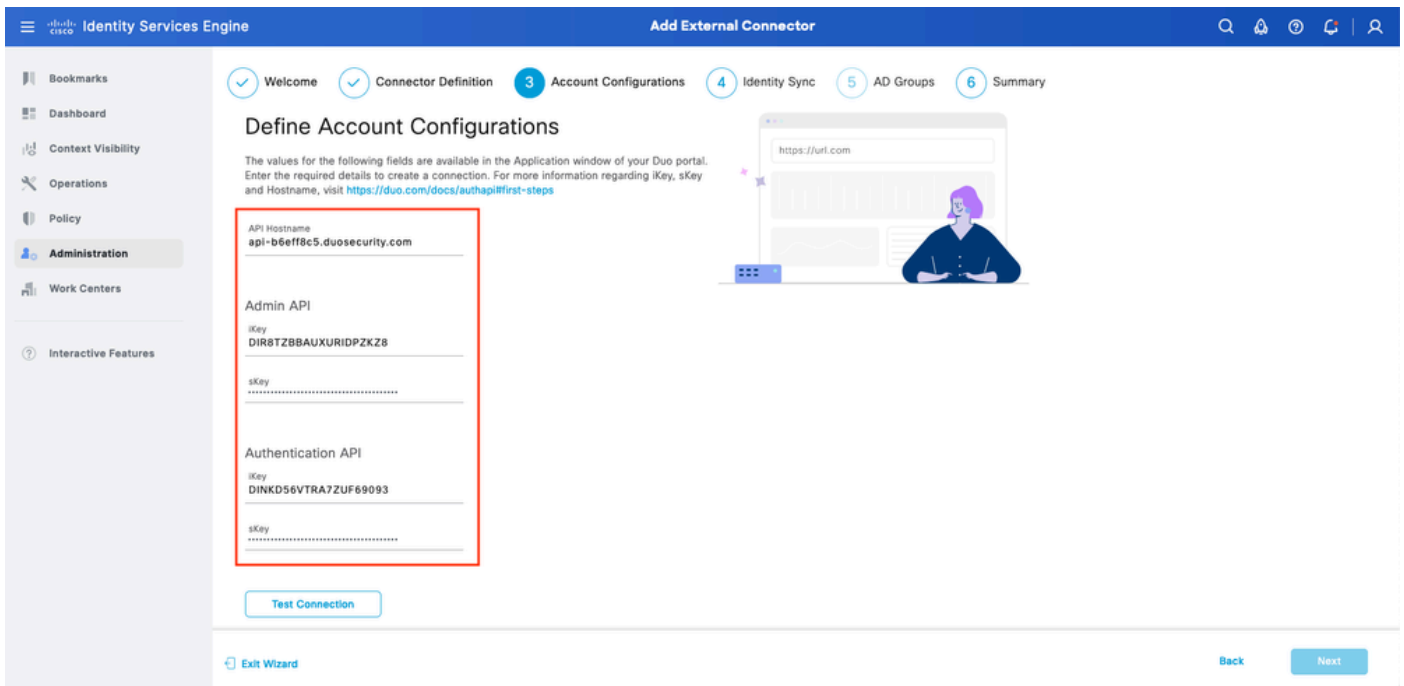
ISE DUO Assistent 1

Konfigurieren Sie auf dem nächsten Bildschirm den Verbindungsnamen, und klicken Sie auf "Weiter".



ISE DUO Assistent 2

Konfigurieren Sie die Werte für API-Hostname, Admin-API-Integration und geheime Schlüssel, Auth-API-Integration und geheime Schlüssel von Select Applications to Protect (Anwendungen zum Schutz auswählen).



ISE DUO-Assistent 3

Klicken Sie auf Verbindung testen. Wenn die Testverbindung erfolgreich hergestellt wurde, können Sie auf "Weiter" klicken.

Test Connection

MFA Auth and Admin API Integration and Secret Keys are valid


Exit Wizard

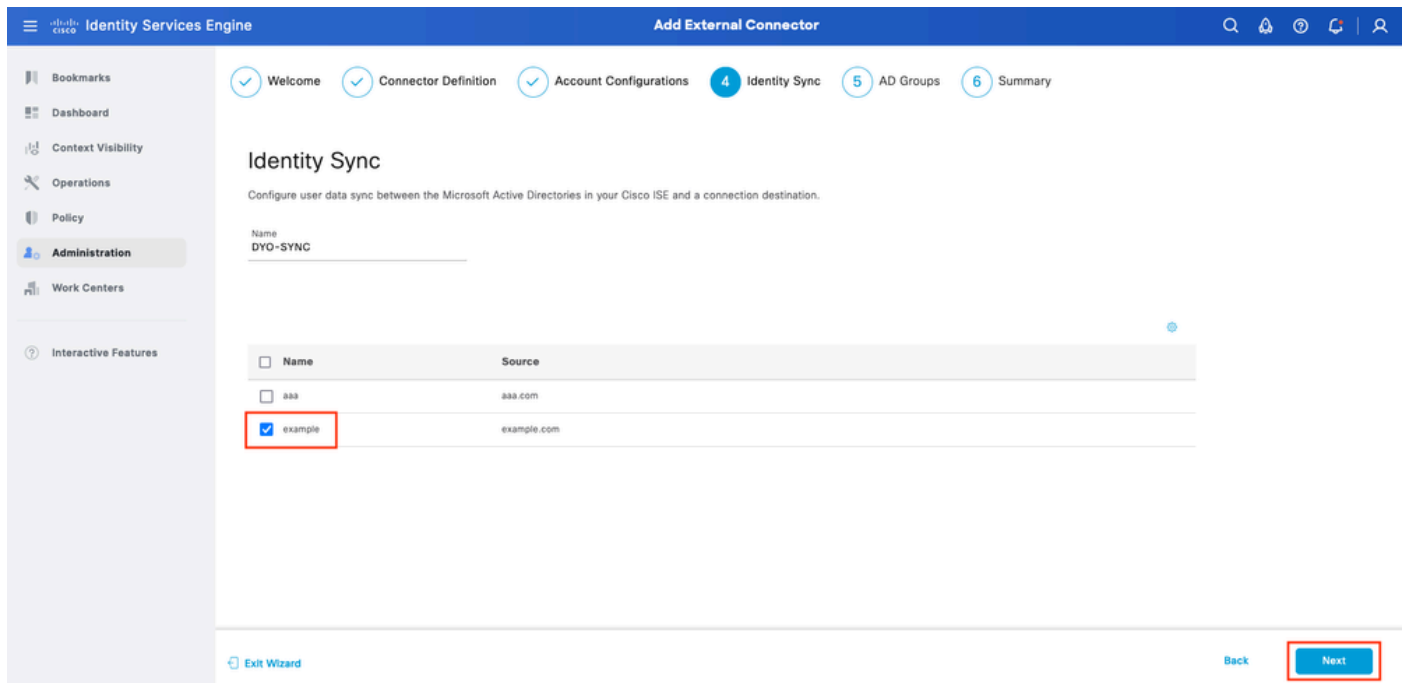
Back

Next

ISE DUO-Assistent 4

Identitätssynchronisierung konfigurieren. Dieser Prozess synchronisiert Benutzer aus den Active Directory-Gruppen, die Sie für das DUO-Konto auswählen, mithilfe der zuvor bereitgestellten API-Anmeldeinformationen. Wählen Sie Active Directory Join Point aus. Klicken Sie auf "Weiter".

 Hinweis: Die Active Directory-Konfiguration ist nicht Bestandteil des Dokuments. Folgen Sie diesem [Dokument](#), um die ISE in Active Directory zu integrieren.



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

ISE DUO-Assistent 5

Wählen Sie Active Directory-Gruppen aus, aus denen Benutzer mit DUO synchronisiert werden sollen. Klicken Sie auf "Weiter".

The screenshot shows the 'Add External Connector' wizard in Cisco Identity Services Engine. The current step is '5 AD Groups'. The page title is 'Select Groups from Active Directory'. Below the title, there is a brief instruction: '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

At the bottom of the wizard, there are 'Exit Wizard', 'Back', and 'Next' buttons. The 'Next' button is highlighted with a red box.

ISE DUO-Assistent 6

Überprüfen Sie die Einstellungen, und klicken Sie auf Fertig.


The screenshot shows the 'Add External Connector' wizard in Cisco Identity Services Engine, step 6: 'Summary'. The page title is 'Summary'. The wizard is divided into three sections:

- 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):

At the bottom of the wizard, there are 'Exit Wizard', 'Back', and 'Done' buttons. The 'Done' button is highlighted with a red box.

ISE DUO-Assistent 7

Benutzer für DUO registrieren

 Hinweis: DUO User Enrollment (DUO-Benutzerregistrierung) ist nicht Bestandteil des Dokuments. In diesem [Dokument](#) erfahren Sie mehr über die Registrierung der Benutzer. Für dieses Dokument wird die manuelle Benutzerregistrierung verwendet.

DUO Admin Dashboard öffnen Navigieren Sie zu Dashboard > Benutzer. Klicken Sie auf den von

der ISE synchronisierten Benutzer.

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

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-Anmeldung 1

Blättern Sie nach unten zu den Telefonen. Klicken Sie auf Telefon hinzufügen.

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-Anmeldung 2

Geben Sie die Telefonnummer ein, und klicken Sie auf Telefon hinzufügen.

Konfigurieren von Richtlinienätzen

1. Authentifizierungsrichtlinie konfigurieren

Navigieren Sie zu Richtlinie > Richtlinienatz. Wählen Sie den Richtlinienatz aus, für den Sie MFA aktivieren möchten. Konfigurieren der Authentifizierungsrichtlinie mit dem primären Authentifizierungsidentitätsspeicher als Active Directory

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


Richtliniensatz 1

2. Konfigurieren der MFA-Richtlinie

Sobald MFA auf der ISE aktiviert ist, steht ein neuer Abschnitt in den ISE-Richtliniensätzen zur Verfügung. Erweitern Sie die MFA-Richtlinie, und klicken Sie auf +, um die MFA-Richtlinie hinzuzufügen. Konfigurieren Sie die gewünschten MFA-Bedingungen, und wählen Sie DUO-MFA aus, das zuvor im Abschnitt Verwendung konfiguriert wurde. Klicken Sie auf Speichern.

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)' section is expanded, showing a table of rules. A red box highlights the 'DUO Rule' configuration, which has a status of 'On' and a condition of 'Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA'. The action is set to 'DUO-MFA'. A 'Save' button is highlighted with another red box at the bottom right of the configuration area.

ISE-Richtlinie

 Hinweis: Die oben konfigurierte Richtlinie basiert auf der Tunnelgruppen-RA. Benutzer, die mit einer RA-Tunnelgruppe verbunden sind, müssen MFA durchführen. Die ASA-/FTD-Konfiguration wird in diesem Dokument nicht behandelt. Verwenden Sie dieses [Dokument](#) zum Konfigurieren von ASA/FTD.

3. Autorisierungsrichtlinie konfigurieren

Konfigurieren Sie die Autorisierungsrichtlinie mit den Bedingungen und Berechtigungen der Active Directory-Gruppe Ihrer Wahl.

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

Richtliniensatz 3

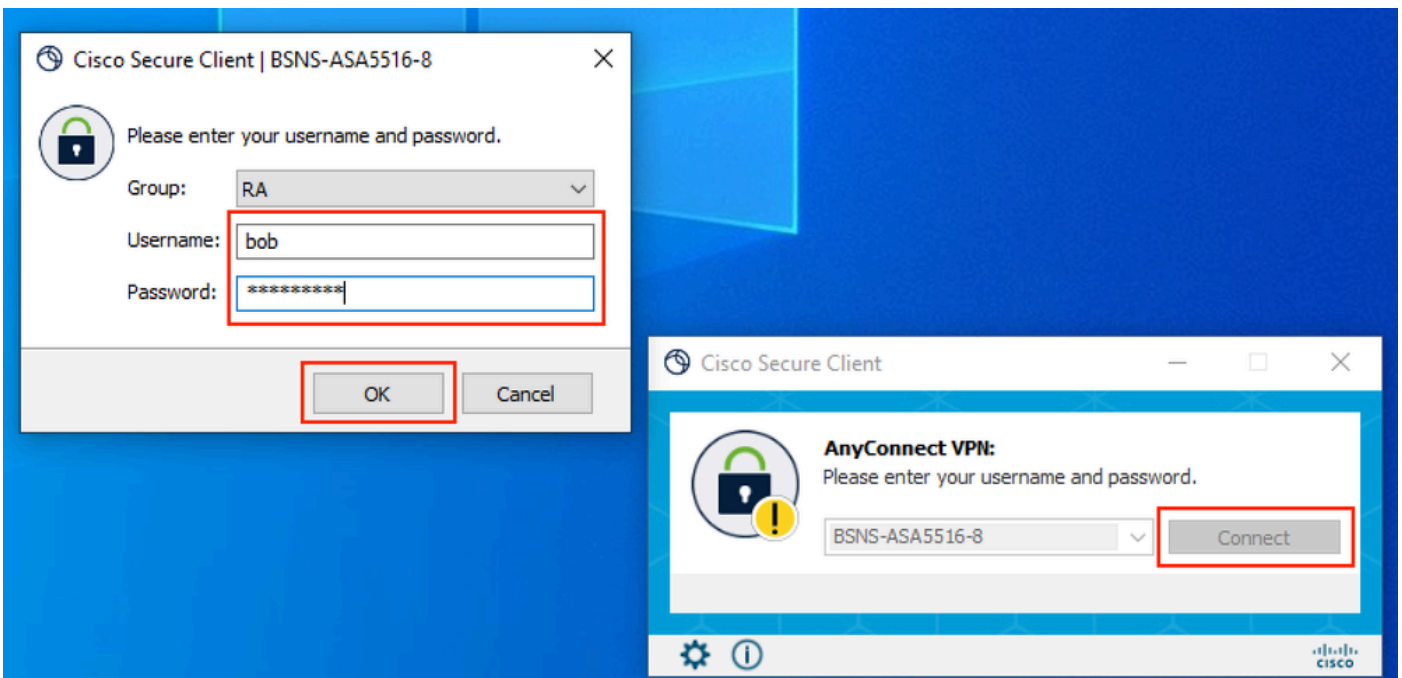
Einschränkungen

Zum Zeitpunkt der Erstellung dieses Dokuments:

1. Nur DUO-Push und Telefon werden als Authentifizierungsmethode des zweiten Faktors unterstützt.
2. Es werden keine Gruppen an DUO Cloud weitergeleitet, nur die Benutzersynchronisierung wird unterstützt
3. Nur die folgenden Anwendungsfälle für die mehrstufige Authentifizierung werden unterstützt:
 - VPN-Benutzerauthentifizierung
 - TACACS+-Administrator-Zugriffsauthentifizierung

Überprüfung

Öffnen Sie Cisco Secure Client, und klicken Sie auf Verbinden. Geben Sie Benutzernamen und Kennwort ein, und klicken Sie auf OK.



VPN-Client

Benutzer des Mobilgeräts müssen eine DUO-Push-Benachrichtigung erhalten. Genehmigen Sie es. Die VPN-Verbindung wurde hergestellt.

1:52



Search

Accounts (8)

Add



Cisco
Cisco



Are you logging in to Auth API?

🌐 Cisco

🕒 1:52 PM

👤 bob

MFA-bezogene Protokolle	Policy-Engine	ise-psc.log	DuoMfaAuthApiUtils -:::- Anfrage an D Manager gesendet DuoMfaAuthApiUtils —> Duo-Antwort
Richtlinienbezogene Protokolle	Port-JNI	prrt- management.log	RadiusMfaPolicyRequestProzessor TACACSmfaPolicyRequestProcessor
Authentifizierungsbezogene Protokolle	Laufzeit-AAA	prrt-server.log	MfaAuthenticator::onAuthenticateEver MfaAuthenticator::sendAuthenticateEv MfaAuthenticator::onResponseEvalua
DUO-Authentifizierung, ID- Synchronisierung - Protokolle		duo-sync- service.log	

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.