

Configure ISE 3.3 Native Multi-factor Authentication with Duo

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Flow Diagram](#)

[Configurations](#)

[Select Applications to Protect](#)

[Integrate ISE with Active Directory](#)

[Enable Open API](#)

[Enable MFA Identity Source](#)

[Configure MFA External Identity Source](#)

[Enroll User into Duo](#)

[Configure Policy Sets](#)

[Limitations](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to integrate Identity Services Engine (ISE) 3.3 patch 1 with Duo for Multi-factor Authentication. From version 3.3 patch 1 ISE can be configured for native integration with Duo services hence eliminating the need for Authentication Proxy.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- ISE
- Duo

Components Used

The information in this document is based on:

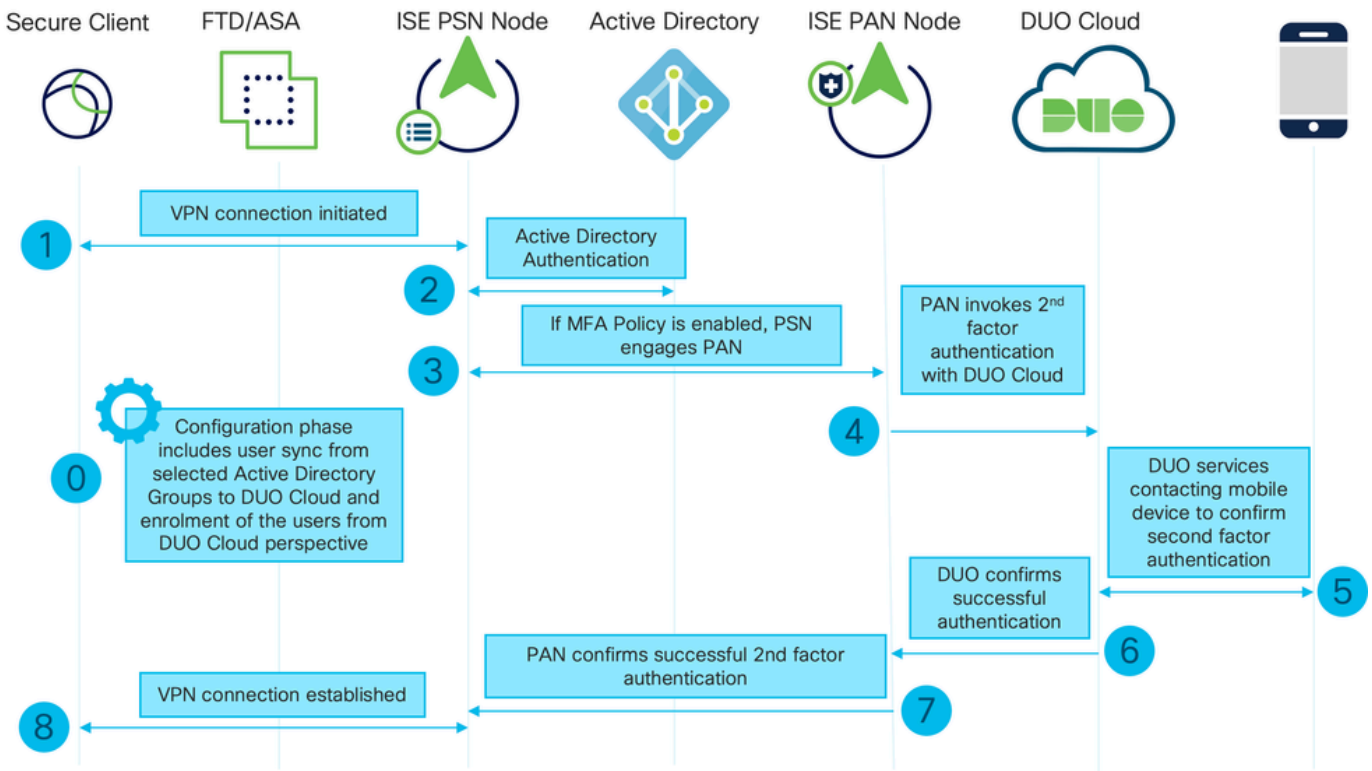
- Cisco ISE Version 3.3 patch 1
- Duo
- Cisco ASA version 9.16(4)

- Cisco Secure Client version 5.0.04032

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Flow Diagram



Flow Diagram

Steps

0. Configuration Phase includes the selection of the Active Directory Groups, from which users are synced up, the sync happens once the MFA wizard is completed. It consists of two steps. Lookups to Active Directory to get the list of users and certain attributes. A call to Duo Cloud with Cisco ISE Admin API is made to push users there. Administrators are required to enroll users. Enrolling can include the optional step of activating the user for Duo Mobile, which allows your users to use one-tap authentication with Duo Push

1. VPN connection is initiated, user inputs the username and password and clicks on OK. Network device sends RADIUS Access-Request is sent to PSN

2. PSN node authenticates the user via Active Directory

3. When authentication succeeds and MFA Policy is configured, PSN engages PAN in order to contact Duo Cloud

4. A call to Duo Cloud with Cisco ISE Auth API is made to invoke a second-factor authentication with Duo. ISE communicates with Duo's service on SSL TCP port 443.

5. Second-factor authentication takes place. User completes the second-factor authentication process

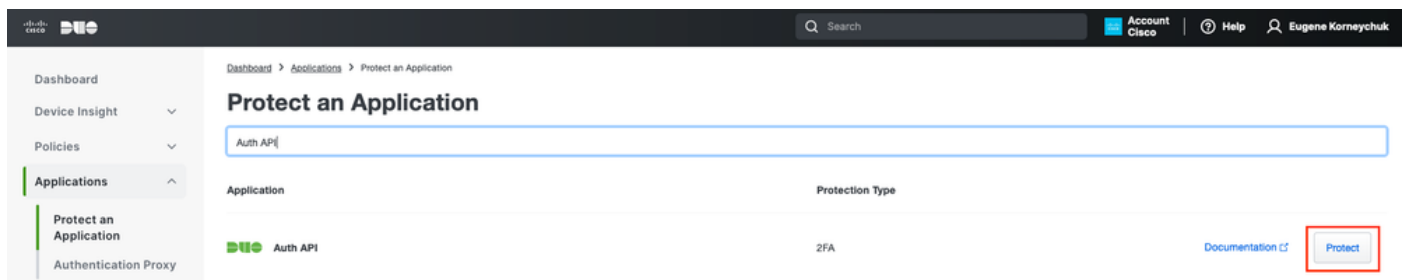
6. Duo responds to PAN with the result of the second-factor authentication
7. PAN responds to PSN with the result of the second-factor authentication
8. Access-Accept is sent to the Network Device, VPN Connection is established

Configurations

Select Applications to Protect

Navigate to Duo Admin Dashboard <https://admin.duosecurity.com/login>. Login with Admin credentials.

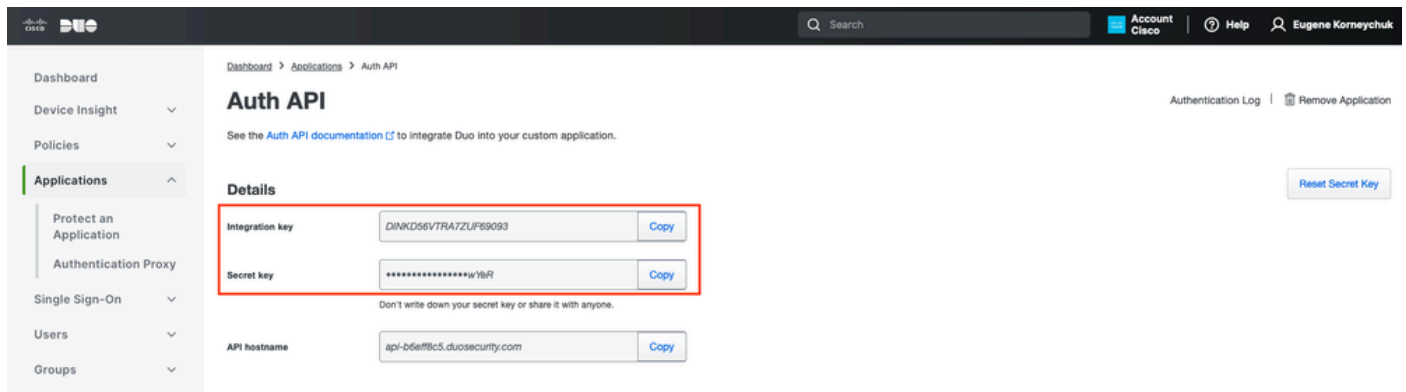
Navigate to **Dashboard > Applications > Protect an Application**. Look for **Cisco ISE Auth API** and select **Protect**.



Application	Protection Type
Auth API	2FA

Auth API 1

Make a note of **Integration key** and **Secret key**.



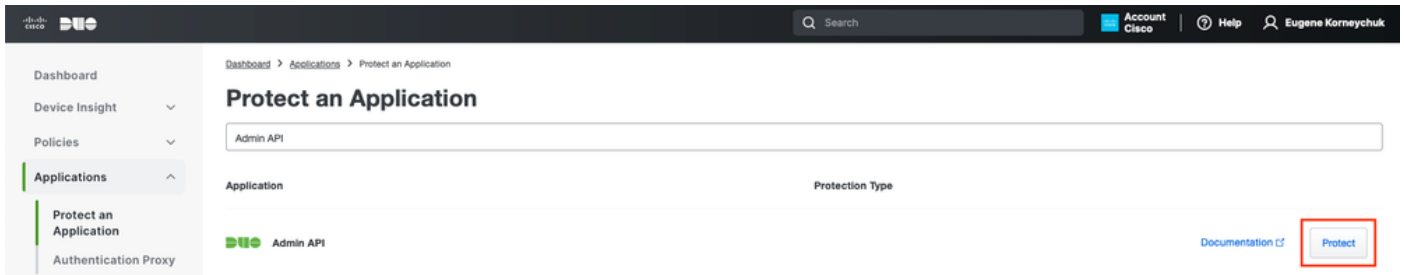
Details		
Integration key	DINKD56V7RA7ZUF69093	Copy
Secret key	*****'Y8R	Copy
API hostname	api-b6e#bc5.duosecurity.com	Copy

Auth API 2

Navigate to **Dashboard > Applications > Protect an Application**. Look for **Cisco ISE Admin API** and select **Protect**.

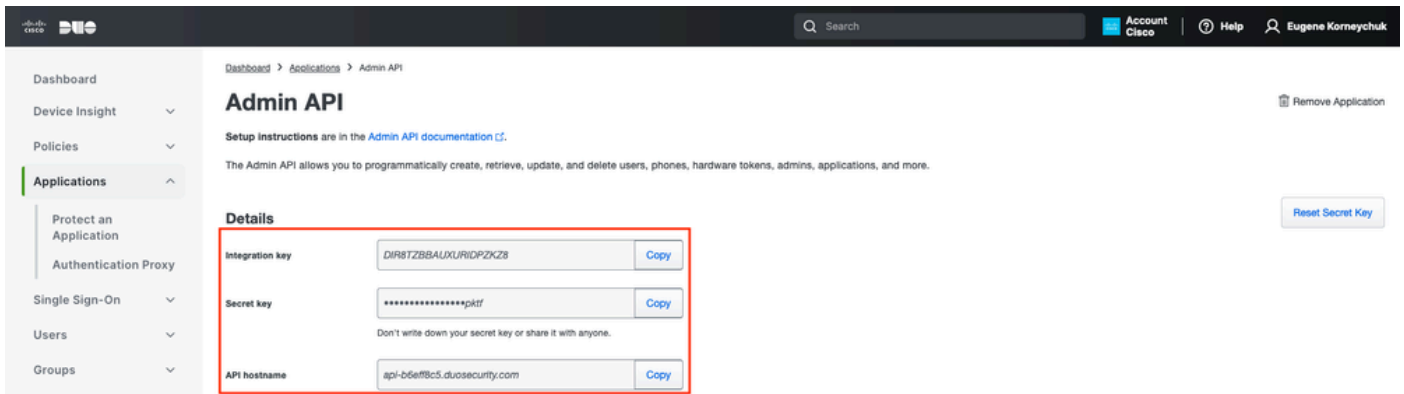


Note: Only administrators with the **Owner** role can create or modify Cisco ISE Admin API application in the Duo Admin Panel.



Auth API 1

Make a note of **Integration key** and **Secret key** and **API hostname**.



Admin API 2

Configure API Permissions

Navigate to **Dashboard > Applications > Application**. Select **Cisco ISE Admin API**.

Check **Grant Read Resource** and **Grant Write Resource** permissions. Click on **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

Integrate ISE with Active Directory

1. Navigate to **Administration > Identity Management > External Identity Stores > Active Directory > Add**. Provide the Join Point Name, Active Directory Domain and click **Submit**.

Identity Services Engine Administration / Identity Management

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources

- > Certificate Authentica...
- > Active Directory
- > MFA
- > Identity Sync
- > LDAP
- > ODBC
- > RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- > REST

Connection

- * Join Point Name ○
- * Active Directory Domain ○

[Submit](#) [Cancel](#)

Active Directory 1

2. When prompted to Join all ISE Nodes to this Active Directory Domain, click **Yes**.



Information

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

No

Yes

Active Directory 2

3. Provide AD User Name and Password, click **OK**.



Join Domain

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

* AD User Name	<input type="text" value="Administrator"/>
* Password	<input type="password" value="*****"/>

Specify Organizational Unit

Store Credentials


Cancel

OK

Active Directory 3

AD account required for domain access in ISE can have either of these:

- Add workstations to domain user right in respective domain
- Create Computer Objects or Delete Computer Objects permission on respective computers container where ISE machine's account is created before it joins ISE machine to the domain

 **Note:** Cisco recommends to disable the lockout policy for the ISE account and configure the AD infrastructure to send alerts to the admin if a wrong password is used for that account. When the wrong password is entered, ISE does not create or modify its machine account when it is necessary and therefore possibly deny all authentications.

4. Status of AD is Operational.

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. Navigate to **Groups > Add > Select Groups From Directory > Retrieve Groups**. Select checkboxes against AD Groups of your choice (which are used to sync users and for Authorization Policy), as shown in this image.

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

6. Click **Save** to save retrieved AD Groups.

Connection Allowed Domains PassivelD **Groups** Attributes Advanced Settings

Edit + Add Delete Group Update SID Values

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

Active Directory 6

Enable Open API

Navigate to **Administration > System > Settings > API Settings > API Service Settings**. Enable **Open API** and click on **Save**.

Identity Services Engine Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
General MDM / UEM Settings
Posture
Profiling
Protocols
Endpoint Scripts
Proxy
SMTP Server
SMS Gateway
System Time
API Settings
Data Connect
Network Success Diagnostics
DHCP & DNS Services
Max Sessions
Light Data Distribution
Endpoint Replication
Interactive Features

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)

Open API

Enable MFA Identity Source

Navigate to **Administration > Identity Management > Settings > External Identity Sources Settings**. Enable **MFA** and click on **Save**.

Identity Services Engine Administration / Identity Management

Settings

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 Save

ISE MFA 1

Configure MFA External Identity Source

Navigate to **Administration > Identity Management > External Identity Sources**. Click on **Add**. On the Welcome Screen click on **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.

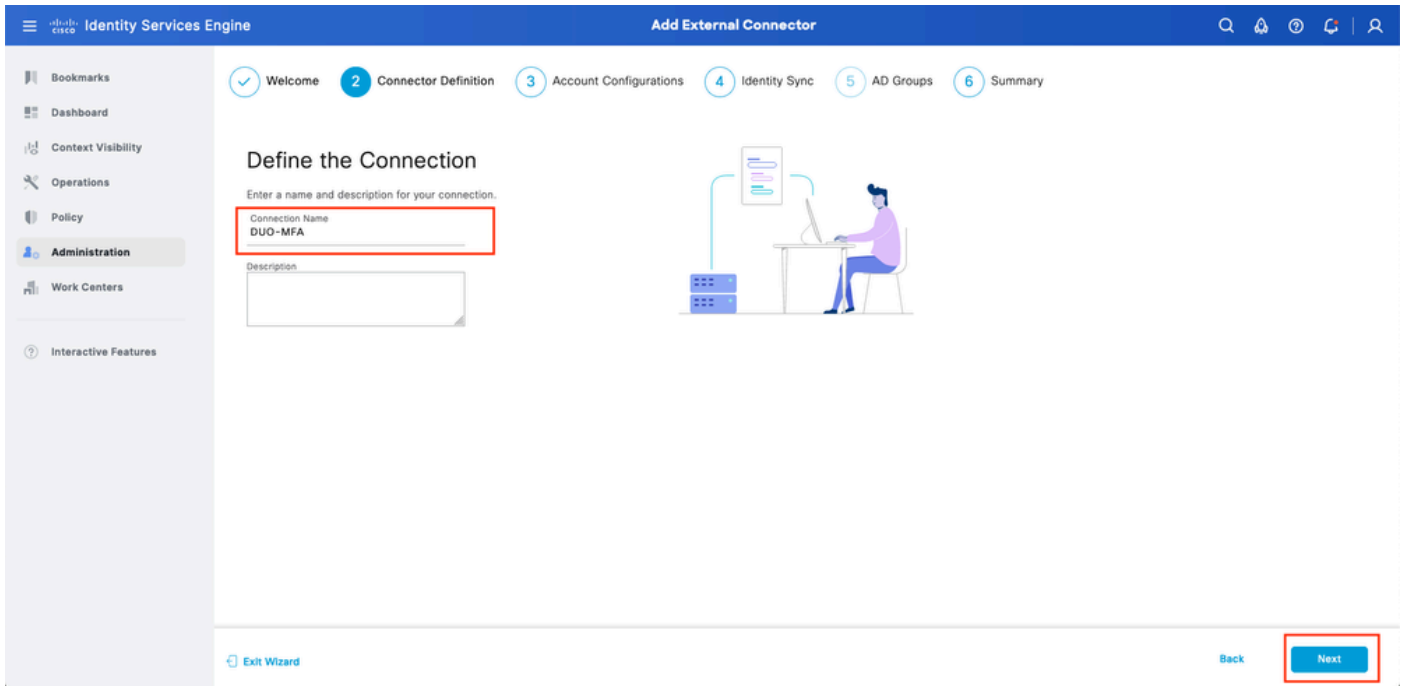
Before you begin, the following prerequisites apply:

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

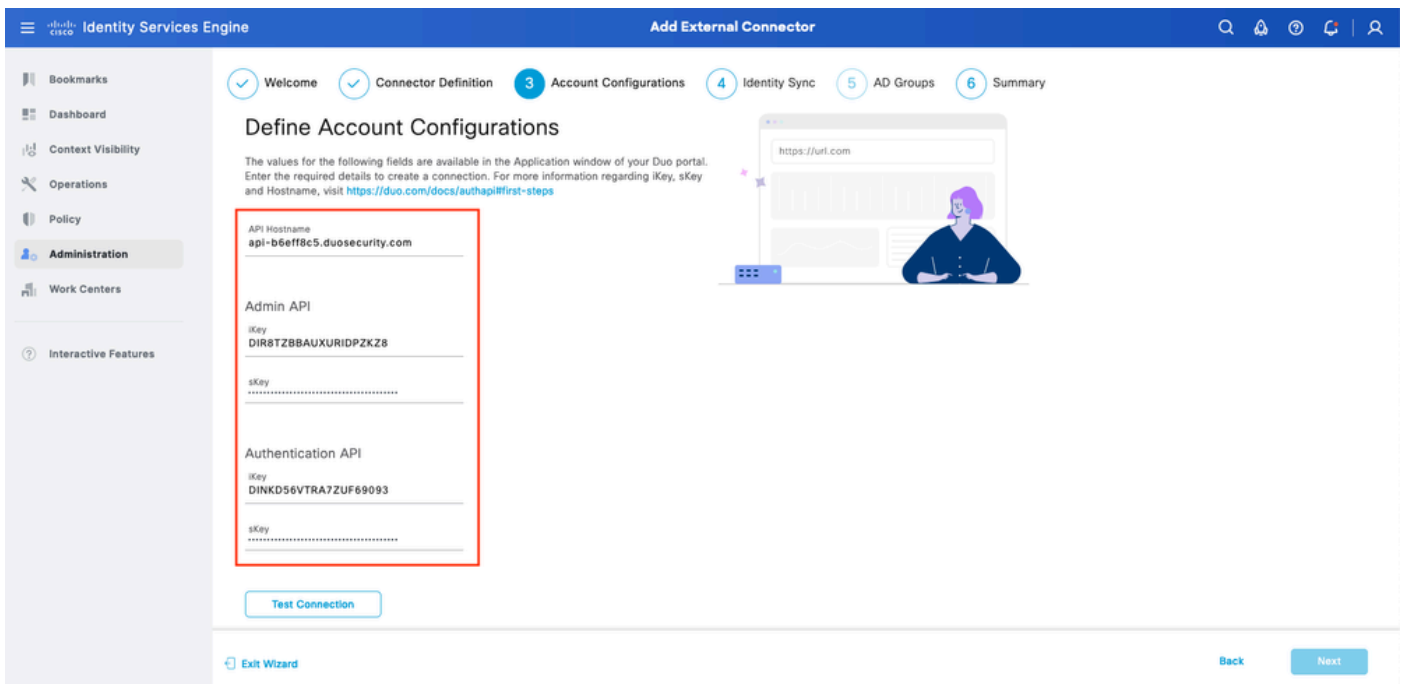
ISE Duo wizard 1

On the next screen configure **Connection Name** and click on **Next**.



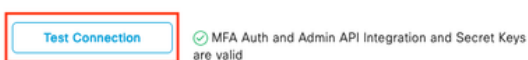
ISE Duo wizard 2

Configure the values of **API Hostname**, **Cisco ISE Admin API Integration** and **Secret Keys**, **Cisco ISE Auth API Integration** and **Secret Keys** from **Select Applications to Protect** step.




ISE Duo wizard 3

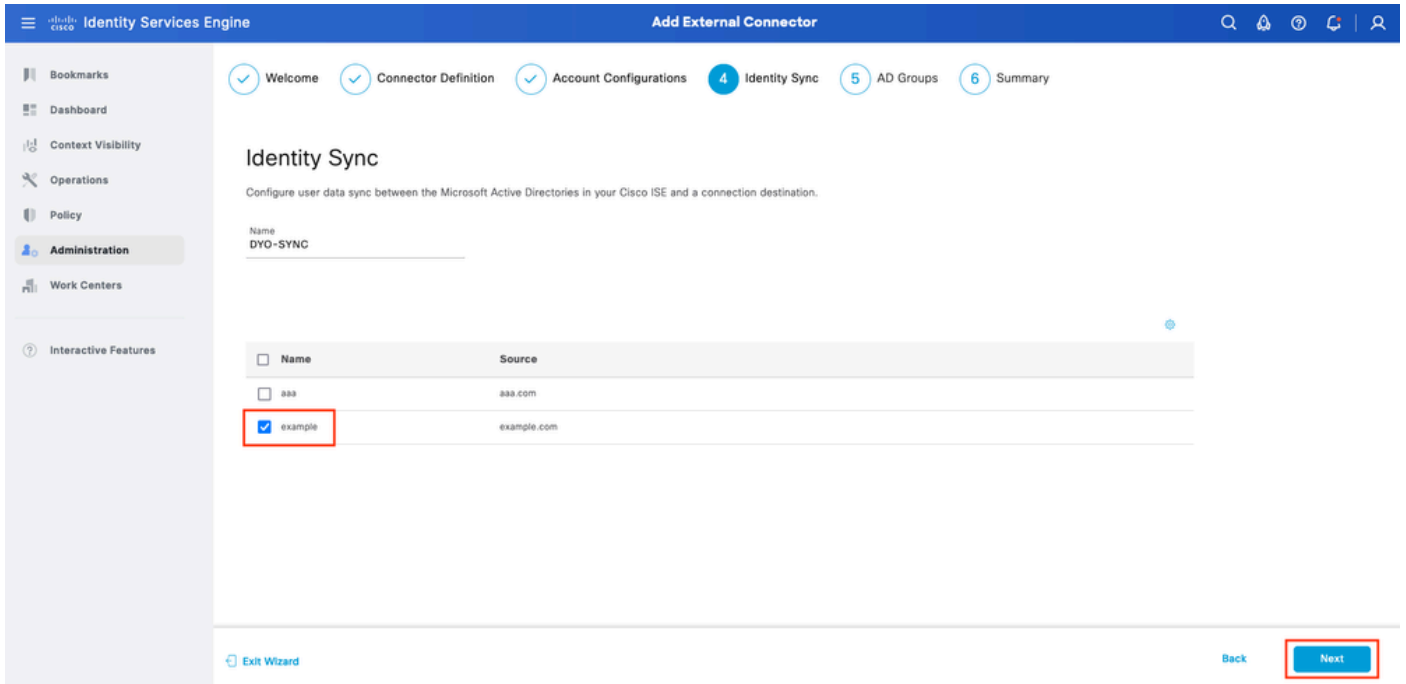
Click on **Test Connection**. Once the **Test Connection** succeeds you can click on **Next**.



ISE Duo wizard 4

Configure **Identity Sync**. This process synchronizes users from the Active Directory groups you select into Duo Account using API credentials provided earlier. Select **Active Directory Join Point**. Click on **Next**.

 **Note:** Active Directory configuration is outside of the scope of the document, Follow this [document](#) in order to integrate ISE with Active Directory.

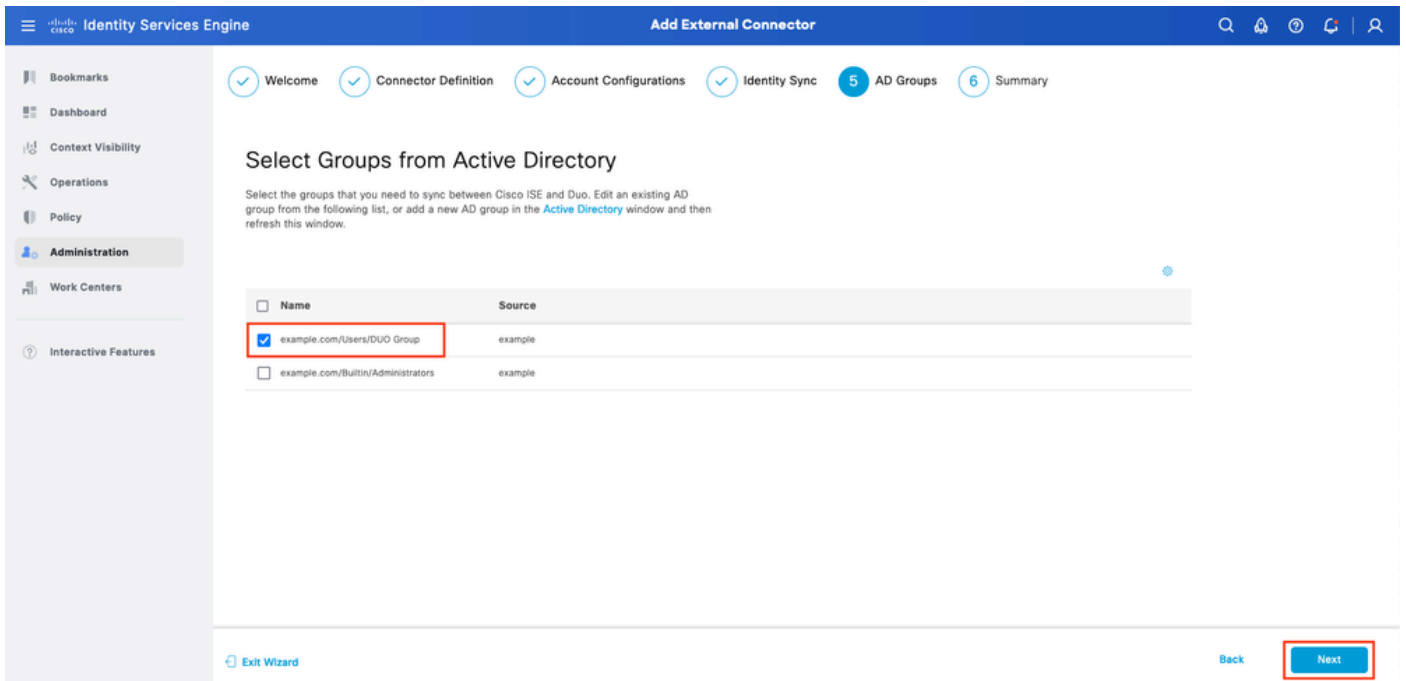


The screenshot shows the 'Identity Sync' configuration page in the Cisco Identity Services Engine. The breadcrumb trail is: Welcome > Connector Definition > Account Configurations > **4 Identity Sync** > 5 AD Groups > 6 Summary. The page title is 'Identity Sync' with the subtitle 'Configure user data sync between the Microsoft Active Directories in your Cisco ISE and a connection destination.' There is a text input field for 'Name' containing 'DYO-SYNC'. Below it is a table with columns 'Name' and 'Source'. The table contains two rows: one with 'aaa' and 'aaa.com' (checkbox unchecked), and one with 'example' and 'example.com' (checkbox checked). At the bottom right, there are 'Back' and 'Next' buttons, with 'Next' highlighted by a red box.

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

ISE Duo wizard 5

Select **Active Directory Groups** from which you would like users to be synchronized with Duo. Click on **Next**.



The screenshot shows the 'Select Groups from Active Directory' page in the Cisco Identity Services Engine. The breadcrumb trail is: Welcome > Connector Definition > Account Configurations > Identity Sync > **5 AD Groups** > 6 Summary. The page title is 'Select Groups from Active Directory' with the subtitle '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.' Below it is a table with columns 'Name' and 'Source'. The table contains two rows: one with 'example.com/Users/DUO Group' and 'example' (checkbox checked), and one with 'example.com/Builtin/Administrators' and 'example' (checkbox unchecked). At the bottom right, there are 'Back' and 'Next' buttons, with 'Next' highlighted by a red box.

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

ISE Duo wizard 6

Verify the settings are correct and click on **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](#)

ISE Duo wizard 7

Enroll User into Duo

 **Note:** Duo User Enrollment is outside of the scope of the document, consider this [document](#) to learn more about enrolling the users. For the purpose of this document, manual user enrolment is used.

Open Duo Admin Dashboard. Navigate to **Dashboard > Users**. Click on the user synchronized from ISE.

Dashboard > Users

Users

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

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 enroll 1

Scroll down to the **Phones**. Click on **Add Phone**.

Phones

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

Add Phone

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

Duo enroll 2

Enter the **Phone Number** and click on **Add Phone**.

Dashboard > Users > bob > Add Phone

Add Phone

[Learn more about Activating Duo Mobile](#).

Type Phone Tablet

Phone number [Show extension field](#)

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

Add Phone

Duo Enroll 3

Configure Policy Sets

1. Configure Authentication Policy

Navigate to **Policy > Policy Set**. Select the **Policy Set** for which you would like to enable MFA. Configure Authentication Policy with Primary Authentication Identity Store as Active Directory.

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	0	⚙️
●	Default		All_User_ID_Stores > Options	7	⚙️

Policy Set 1

2. Configure MFA Policy

Once MFA is enabled on ISE, a new section in ISE Policy Sets is available. Expand **MFA Policy** and click on + in order to add MFA Policy. Configure MFA Conditions of your choice, select **DUO-MFA** configured previously in **Use** section. Click on **Save**.

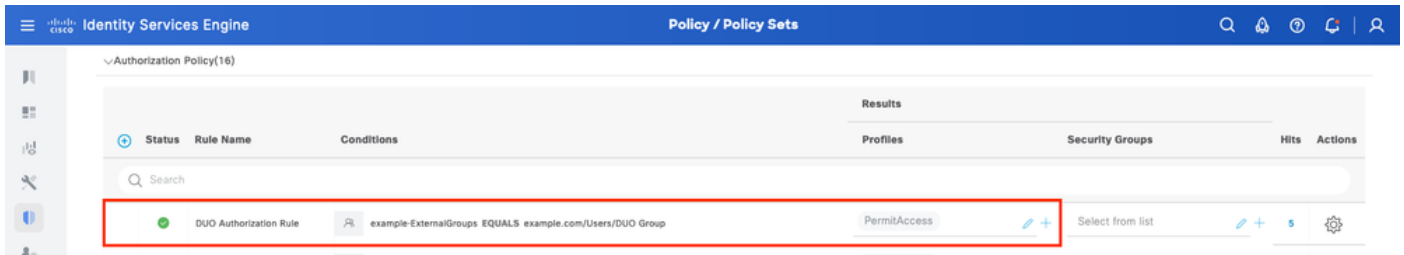
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits												
●	Default	Default policy set		Default Network Access	75												
<table border="1"> <thead> <tr> <th>Status</th> <th>Rule Name</th> <th>Conditions</th> <th>Use</th> <th>Hits</th> <th>Actions</th> </tr> </thead> <tbody> <tr style="border: 2px solid red;"> <td>●</td> <td>DUO Rule</td> <td>Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA</td> <td>DUO-MFA > Options</td> <td>0</td> <td>⚙️</td> </tr> </tbody> </table>						Status	Rule Name	Conditions	Use	Hits	Actions	●	DUO Rule	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA	DUO-MFA > Options	0	⚙️
Status	Rule Name	Conditions	Use	Hits	Actions												
●	DUO Rule	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA	DUO-MFA > Options	0	⚙️												

ISE Policy

Note: Policy configured above relies on the Tunnel-Group Named RA. Users connected to RA tunnel group are forced to perform MFA. ASA/FTD configuration is outside of the scope of this document. Use this [document](#) in order to configure ASA/FTD

3. Configure Authorization Policy

Configure Authorization Policy with Active Directory Group condition and permissions of your choice.



Policy Set 3

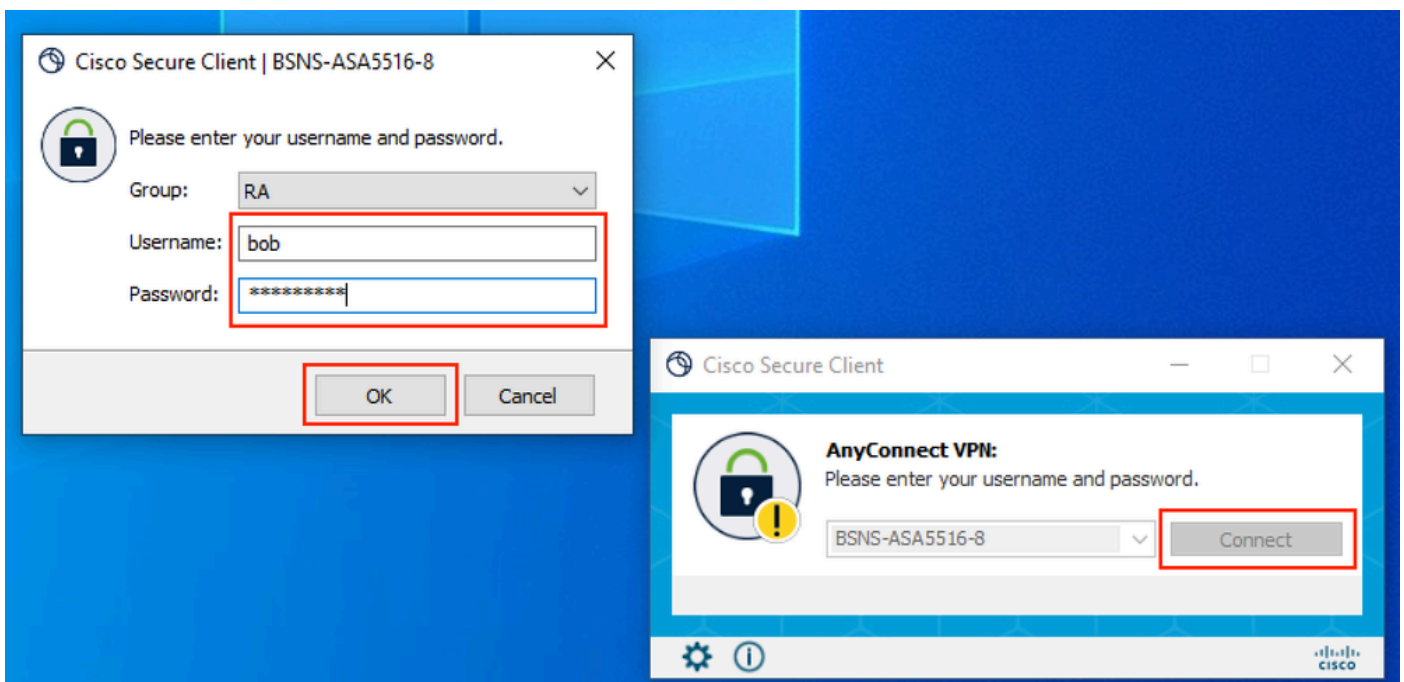
Limitations

At the time of writing this document:

1. Only Duo push and phone are supported as a second-factor authentication method
2. No Groups are pushed to Duo Cloud, only User sync is supported
3. Only the following multifactor authentication use cases are supported:
 - VPN user authentication
 - TACACS+ admin access authentication

Verify

Open **Cisco Secure Client**, click on **Connect**. Provide **Username** and **Password** and click **OK**.



VPN Client

Users Mobile Device must receive a Duo Push Notification. **Approve** it. VPN Connection is Established.

1:52



Search

Accounts (8)

Add



Cisco
Cisco



Are you logging in to Auth API?

🌐 Cisco

🕒 1:52 PM

👤 bob

MFA related logs	policy-engine	ise-psc.log	DuoMfaAuthApiUtils -:::- Submitted request to Duo Client manager DuoMfaAuthApiUtils --> Duo response
Policy related logs	prrt-JNI	prrt-management.log	RadiusMfaPolicyRequestProcessor TacacsMfaPolicyRequestProcessor
Authentication related logs	runtime-AAA	prrt-server.log	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
Duo Authentication, ID Sync related logs		duo-sync-service.log	