

# Configuration de l'authentification multifacteur native ISE 3.3 avec DUO

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme De Flux](#)

[Configurations](#)

[Sélectionner les applications à protéger](#)

[Intégrer ISE à Active Directory](#)

[Activer l'API ouverte](#)

[Activer la source d'identité MFA](#)

[Configurer la source d'identité externe MFA](#)

[Inscription de l'utilisateur dans DUO](#)

[Configurer les jeux de stratégies](#)

[Limites](#)

[Vérifier](#)

[Dépannage](#)

---

## Introduction

Ce document décrit comment intégrer Identity Services Engine (ISE) 3.3 patch 1 avec DUO pour l'authentification multifacteur. À partir de la version 3.3, le patch 1 ISE peut être configuré pour une intégration native avec les services DUO, éliminant ainsi le besoin d'un proxy d'authentification.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE
- DUO

### Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Correctif 1 de Cisco ISE version 3.3

- DUO
- Cisco ASA version 9.16(4)
- Client sécurisé Cisco 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configurer

### Diagramme De Flux

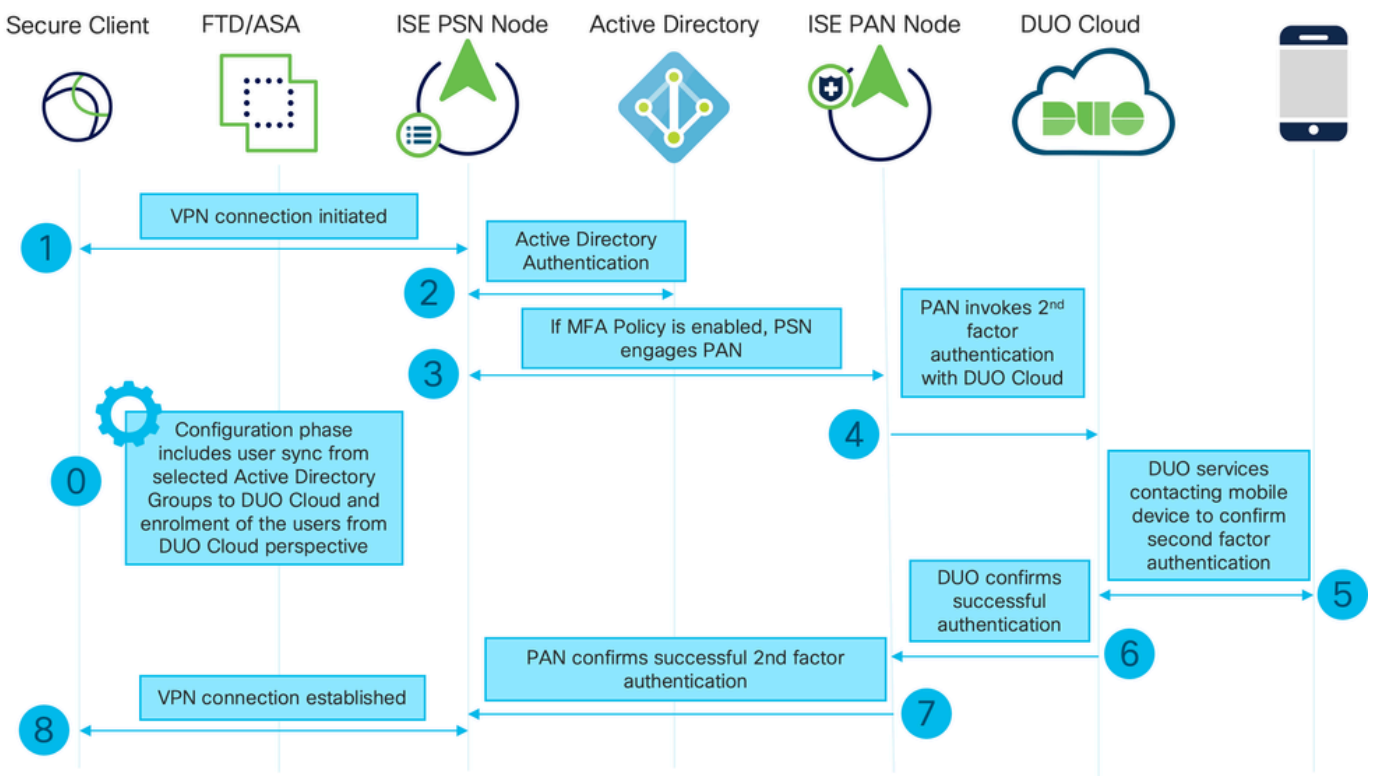


Diagramme De Flux

### Étapes

0. La phase de configuration inclut la sélection des groupes Active Directory à partir desquels les utilisateurs sont synchronisés. La synchronisation se produit une fois l'assistant MFA terminé. Il se compose de deux étapes. Recherche dans Active Directory la liste des utilisateurs et certains attributs. Un appel au cloud DUO avec l'API d'administration est effectué pour y pousser les utilisateurs. Les administrateurs doivent inscrire des utilisateurs. L'inscription peut inclure l'étape facultative d'activation de l'utilisateur pour Duo Mobile, ce qui permet à vos utilisateurs d'utiliser l'authentification en une seule pression avec Duo Push

1. La connexion VPN est initiée, l'utilisateur saisit le nom d'utilisateur et le mot de passe et clique sur OK. Le périphérique réseau envoie la requête d'accès RADIUS à PSN

2. Le noeud PSN authentifie l'utilisateur via Active Directory

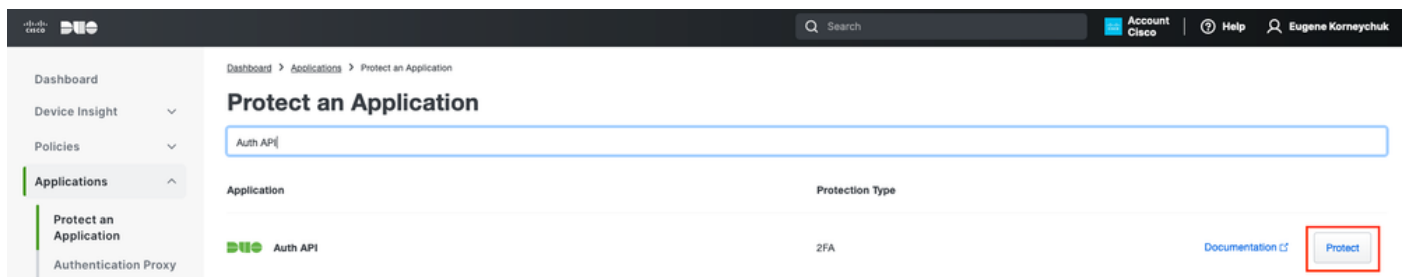
3. Lorsque l'authentification réussit et que la stratégie MFA est configurée, PSN engage le PAN afin de contacter DUO Cloud
4. Un appel vers le cloud DUO avec l'API d'authentification est effectué pour appeler une authentification de second facteur avec DUO. ISE communique avec le service de Duo sur le port TCP SSL 443.
5. L'authentification de second facteur a lieu. L'utilisateur termine le processus d'authentification du second facteur
6. DUO répond au PAN avec le résultat de l'authentification de second facteur
7. Le PAN répond à PSN avec le résultat de l'authentification de second facteur
8. Access-Accept est envoyé au périphérique réseau, la connexion VPN est établie

## Configurations

Sélectionner les applications à protéger

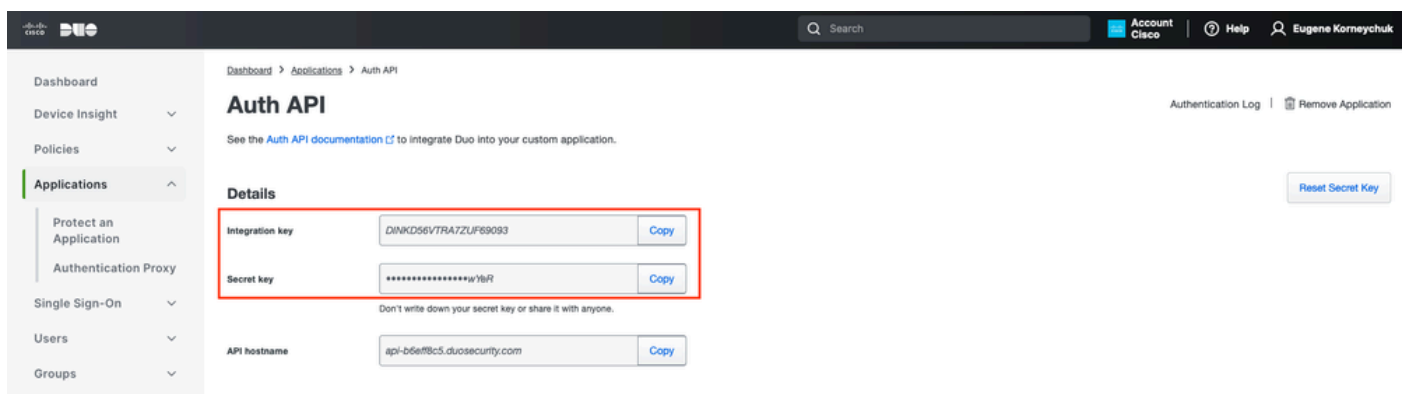
Accédez à DUO Admin Dashboard <https://admin.duosecurity.com/login>. Connectez-vous avec les identifiants Admin.

Accédez à Tableau de bord > Applications > Protéger une application. Recherchez Auth API et sélectionnez Protect.




API d'authentification 1

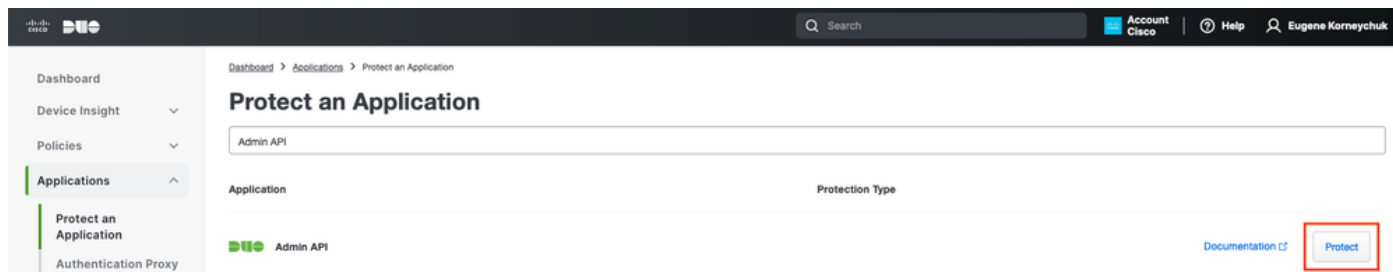
Notez la clé d'intégration et la clé secrète.



API d'authentification 2

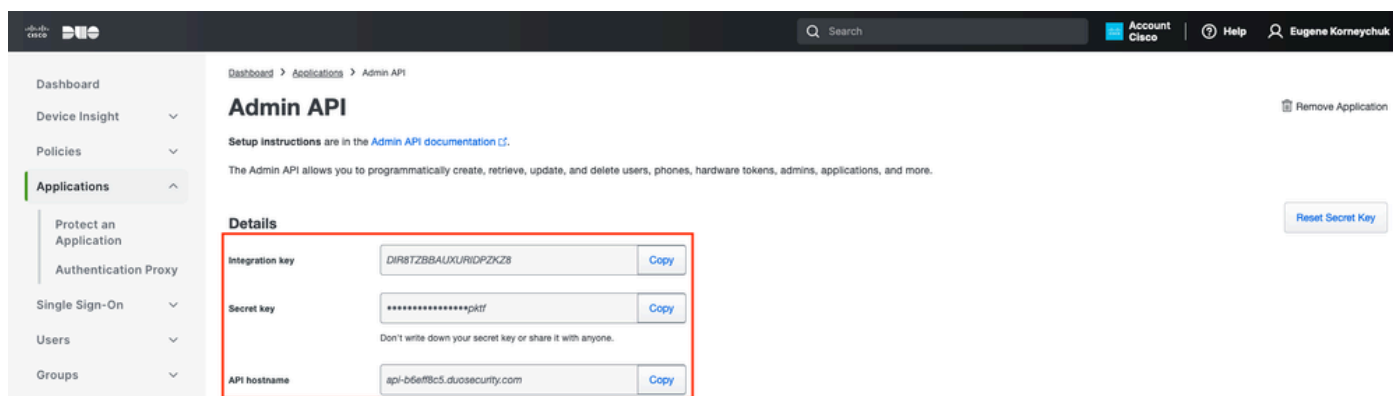
Accédez à Tableau de bord > Applications > Protéger une application. Recherchez Admin API et sélectionnez Protect.

 Remarque : seuls les administrateurs dotés du rôle Propriétaire peuvent créer ou modifier une application API Admin dans le panneau d'administration Duo.



API d'authentification 1

Notez la clé d'intégration, la clé secrète et le nom d'hôte de l'API.



API d'administration 2

Configurer les autorisations API

Accédez à Tableau de bord > Applications > Application. Sélectionnez Admin API.

Cochez Grant Read Resource et Grant Write Resource. Cliquez sur Enregistrer les modifications.

- 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 d'administration 3

## Intégrer ISE à Active Directory

1. Accédez à Administration > Gestion des identités > Magasins d'identités externes > Active Directory > Ajouter. Fournissez le nom du point de jonction, le domaine Active Directory et cliquez sur Envoyer.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration / Identity Management > External Identity Sources > Active Directory. The 'External Identity Sources' list on the left includes Certificate Authentication, 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 is shown. 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 box. At the bottom right, there are 'Submit' and 'Cancel' buttons, with 'Submit' also highlighted by a red box.

Active Directory 1

2. Lorsque vous êtes invité à joindre tous les noeuds ISE à ce domaine Active Directory, cliquez sur Oui.



## Information

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

No

Yes

Active Directory 2

3. Fournissez un nom d'utilisateur et un mot de passe AD, puis cliquez sur OK.



## Join Domain

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

\* AD User Name ⓘ Administrator

\* Password .....

Specify Organizational Unit ⓘ

Store Credentials ⓘ

Cancel


OK

Active Directory 3

Le compte AD requis pour l'accès au domaine dans ISE peut avoir l'un des éléments suivants :

- Ajouter des stations de travail au droit utilisateur de domaine dans le domaine respectif

- Autorisation Créer des objets ordinateur ou Supprimer des objets ordinateur sur le conteneur d'ordinateurs respectif où le compte de l'ordinateur ISE est créé avant qu'il ne joigne l'ordinateur ISE au domaine

 Remarque : Cisco recommande de désactiver la stratégie de verrouillage pour le compte ISE et de configurer l'infrastructure AD pour envoyer des alertes à l'administrateur si un mot de passe incorrect est utilisé pour ce compte. Lorsque le mauvais mot de passe est entré, ISE ne crée pas ou ne modifie pas son compte d'ordinateur lorsqu'il est nécessaire et peut donc refuser toutes les authentifications.

#### 4. L'état d'AD est opérationnel.

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. Accédez à Groups > Add > Select Groups From Directory > Retrieve Groups. Cochez les cases correspondant aux groupes AD de votre choix (qui sont utilisés pour synchroniser les utilisateurs et pour la stratégie d'autorisation), comme illustré dans cette image.

# Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name \*  
Filter

SID \*  
Filter

Type  
Filter

50 Groups Retrieved.

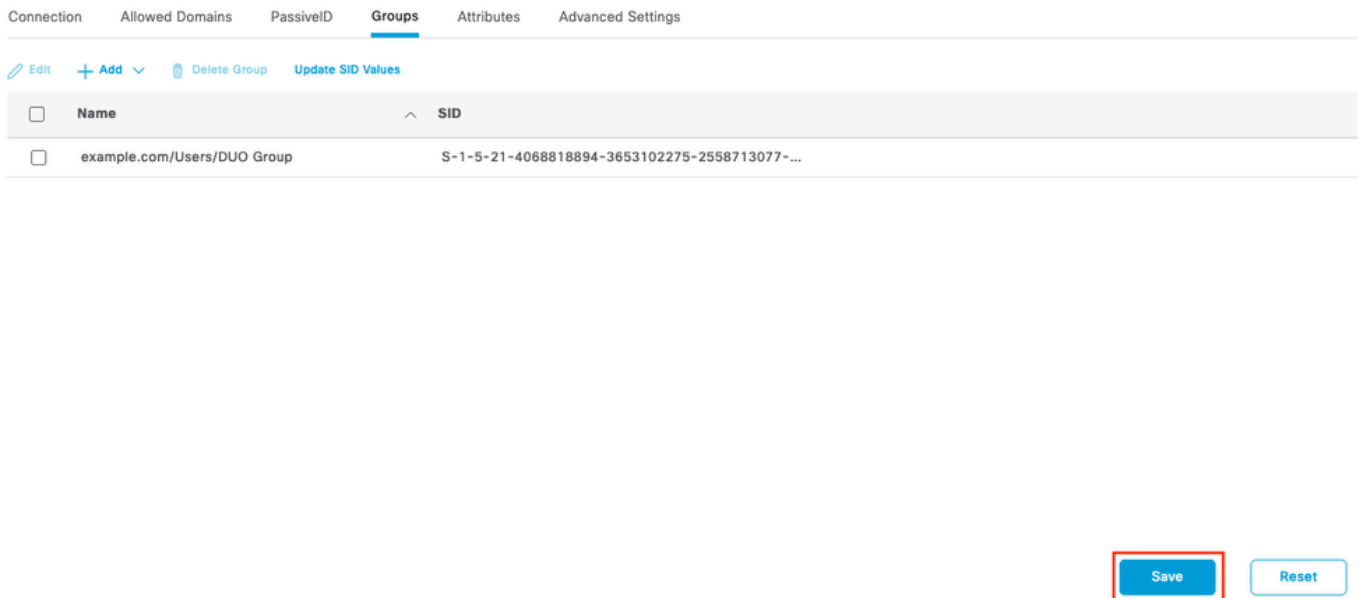
<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	example.com/Users/Cert Publishers	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/Cloneable Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input checked="" 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

Active Directory 5

6. Cliquez sur Enregistrer pour enregistrer les groupes AD récupérés.

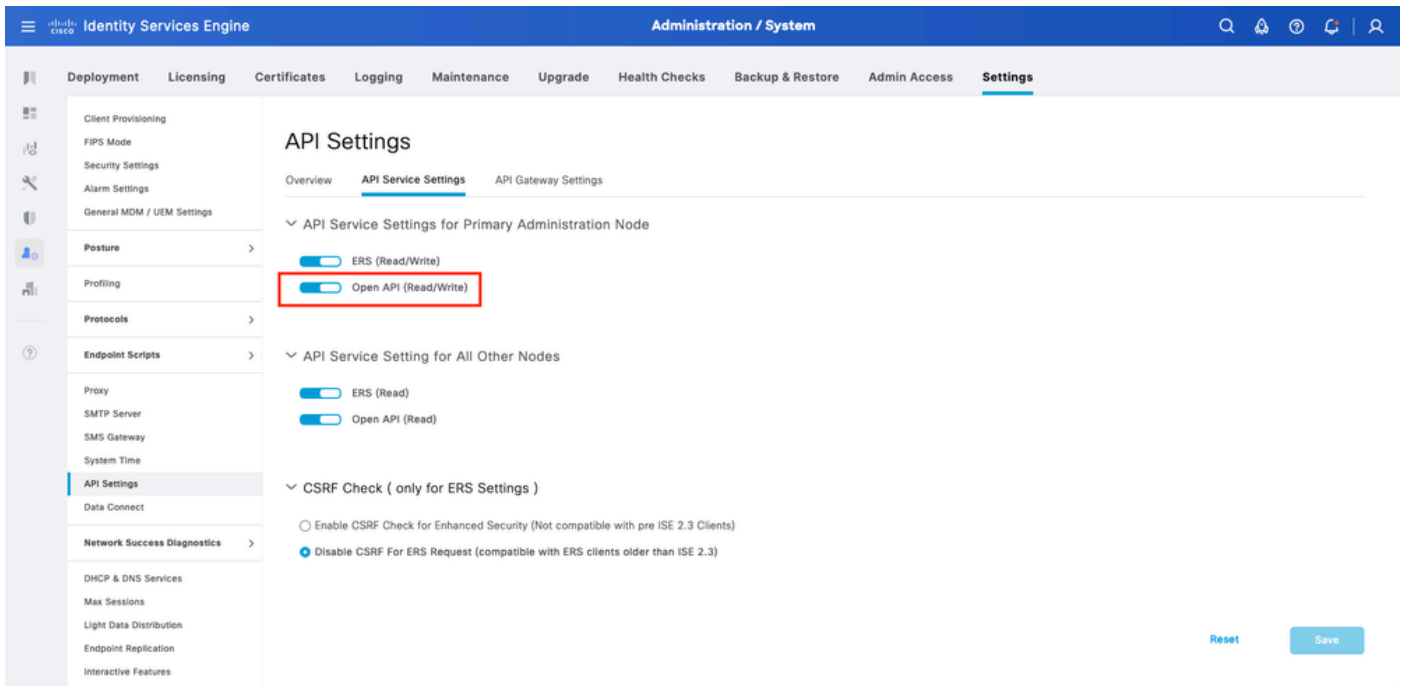




Active Directory 6

## Activer l'API ouverte

Accédez à Administration > System > Settings > API Settings > API Service Settings. Activez Open API et cliquez sur Save.



API ouverte

## Activer la source d'identité MFA

Accédez à Administration > Identity Management > Settings > External Identity Sources Settings. Activez MFA et cliquez sur 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 <sup>BETA</sup>

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

MFA

Cancel **Save**

ISE MFA 1

## Configurer la source d'identité externe MFA

Accédez à Administration > Identity Management > External Identity Sources. Cliquez sur Ajouter. Dans l'écran Welcome (Bienvenue), cliquez sur 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.

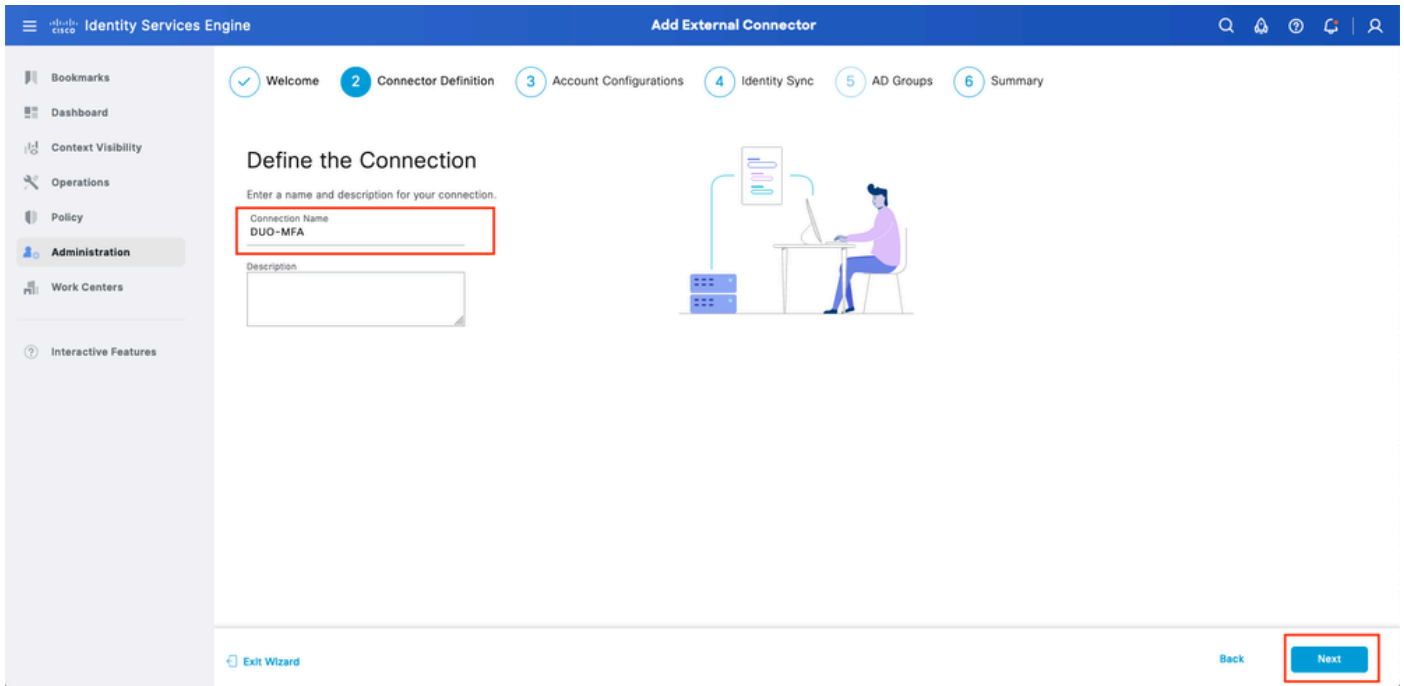
Before you begin, the following prerequisites apply:

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**

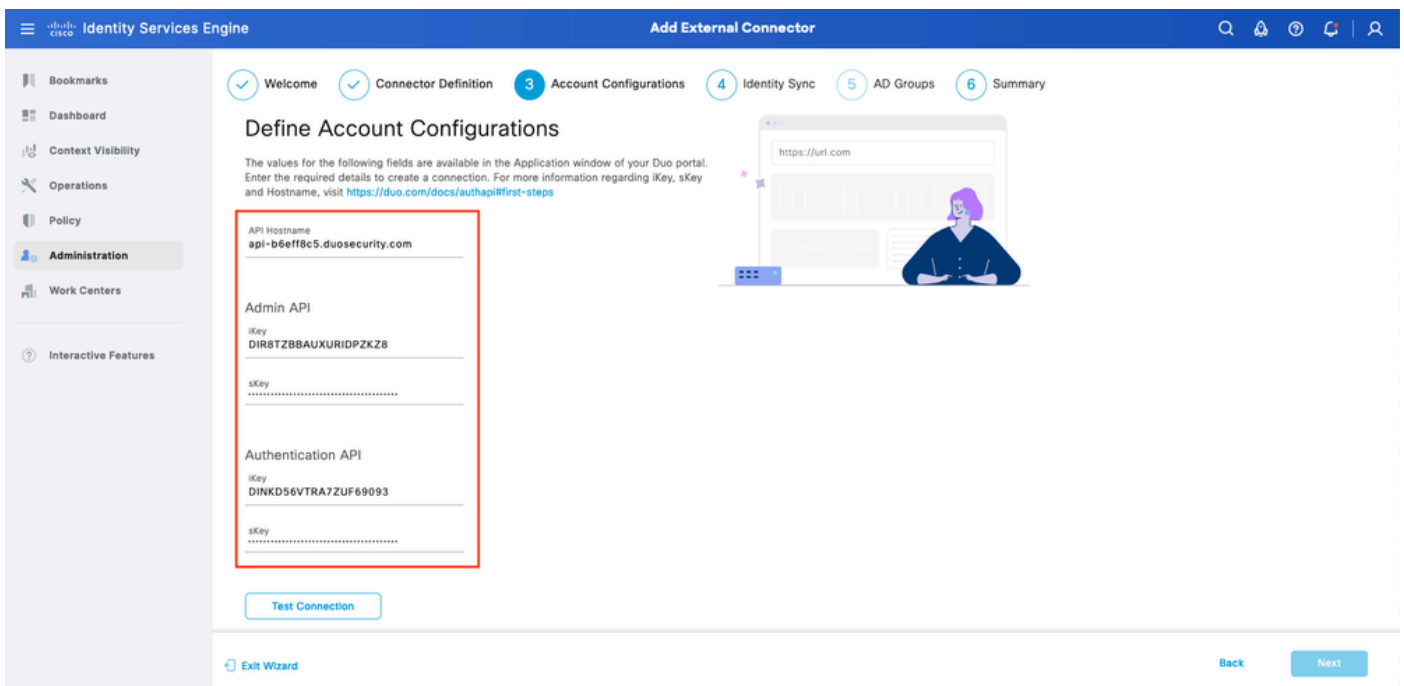
Assistant ISE DUO 1

Dans l'écran suivant, configurez Connection Name et cliquez sur Next.



Assistant ISE DUO 2

Configurez les valeurs de Nom d'hôte de l'API, Intégration de l'API Admin et Clés secrètes, Intégration de l'API Auth et Clés secrètes de l'étape Sélectionner les applications à protéger.



Assistant ISE DUO 3

Cliquez sur Test Connection. Une fois que le test de connexion réussit, vous pouvez cliquer sur Suivant.

[Test Connection](#)

MFA Auth and Admin API Integration and Secret Keys are valid

[Exit Wizard](#)

[Back](#)

[Next](#)

#### Assistant ISE DUO 4

Configurez la synchronisation des identités. Ce processus synchronise les utilisateurs des groupes Active Directory sélectionnés dans le compte DUO à l'aide des informations d'identification API fournies précédemment. Sélectionnez Point de jonction Active Directory. Cliquez sur Suivant.



Remarque : la configuration d'Active Directory sort du cadre du document. Suivez ce [document](#) afin d'intégrer ISE à 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](#)

#### Assistant ISE DUO 5

Sélectionnez Groupes Active Directory à partir desquels vous souhaitez que les utilisateurs soient synchronisés avec DUO. Cliquez sur Suivant.

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**

Assistant ISE DUO 6

Vérifiez que les paramètres sont corrects et cliquez sur 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**

Assistant ISE DUO 7

## Inscription de l'utilisateur dans DUO

Remarque : l'inscription des utilisateurs DUO n'est pas couverte par le document. Examinez ce [document](#) pour en savoir plus sur l'inscription des utilisateurs. Dans le cadre de ce document, l'inscription manuelle des utilisateurs est utilisée.

Ouvrez le tableau de bord DUO Admin. Accédez à Tableau de bord > Utilisateurs. Cliquez sur

l'utilisateur synchronisé à partir d'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

Inscription DUO 1

Faites défiler jusqu'aux téléphones. Cliquez sur Ajouter un téléphone.

### 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](#)

Inscription DUO 2

Saisissez le numéro de téléphone et cliquez sur 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](#)

## Configurer les jeux de stratégies

### 1. Configurer la stratégie d'authentification

Accédez à Policy > Policy Set. Sélectionnez l'ensemble de stratégies pour lequel vous souhaitez activer l'AMF. Configurez la stratégie d'authentification avec le magasin d'identités d'authentification principal comme 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		⚙️
●	Default		All_User_ID_Stores > Options	7	⚙️

## 2. Configurez la politique MFA


Une fois que l'AMF est activée sur ISE, une nouvelle section des ensembles de stratégies ISE est disponible. Développez MFA Policy et cliquez sur + afin d'ajouter MFA Policy. Configurez les conditions MFA de votre choix, sélectionnez DUO-MFA configuré précédemment dans la section Use. Cliquez sur Enregistrer.

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

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

Politique ISE

 Remarque : la stratégie configurée ci-dessus repose sur l'autorité de résolution nommée Tunnel-Group. Les utilisateurs connectés au groupe de tunnels RA sont forcés d'exécuter MFA. La configuration ASA/FTD sort du cadre de ce document. Utilisez ce [document](#) afin de configurer ASA/FTD

## 3. Configurer la stratégie d'autorisation

Configurez la stratégie d'autorisation avec la condition de groupe Active Directory et les autorisations de votre choix.

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

Ensemble de stratégies 3

## Limites

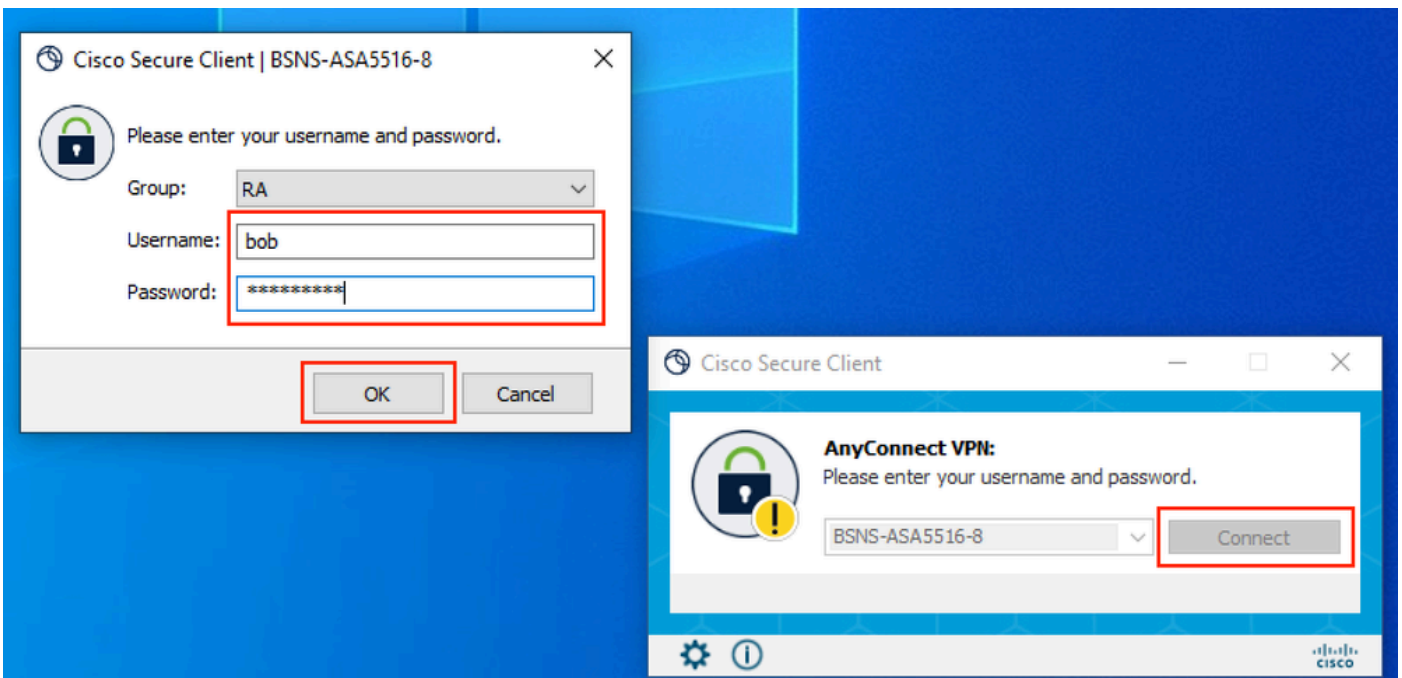
Au moment de la rédaction de ce document :



1. Seules les méthodes push et phone DUO sont prises en charge en tant que méthode d'authentification de second facteur
2. Aucun groupe n'est envoyé vers le cloud DUO, seule la synchronisation utilisateur est prise en charge
3. Seuls les cas d'utilisation d'authentification multifacteur suivants sont pris en charge :
  - Authentification utilisateur VPN
  - Authentification d'accès administrateur TACACS+

## Vérifier

Ouvrez Cisco Secure Client, cliquez sur Connect. Saisissez Username et Password, puis cliquez sur OK.



Client VPN

Les utilisateurs du périphérique mobile doivent recevoir une notification de transmission DUO. Approuvez-le. Connexion VPN établie.

1:52



Search

Accounts (8)

Add



Cisco  
Cisco



Are you logging in to Auth API?

🌐 Cisco

🕒 1:52 PM

👤 bob

Journaux MFA associés	moteur politique	ise-psc.log	DuoMfaAuthApiUtils -:::- Demande envoyée au gestionnaire client Duo DuoMfaAuthApiUtils → Duo response
Journaux liés aux stratégies	port-JNI	pvt-management.log	ProcesseurRequêtePolitiqueMfaRadius ProcesseurRequêtePolitiqueMfaTacas
Journaux relatifs à l'authentification	runtime-AAA	pvt-server.log	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
Authentification DUO, journaux associés à ID Sync		duo-sync-service.log	

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.