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.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances de base sur les sujets suivants :

- ISE
- Duo

Composants utilisés

À partir de la version 3.3 Patch 1, ISE peut être configuré pour des intégrations natives avec les services Duo, éliminant ainsi le besoin de proxy d'authentification.

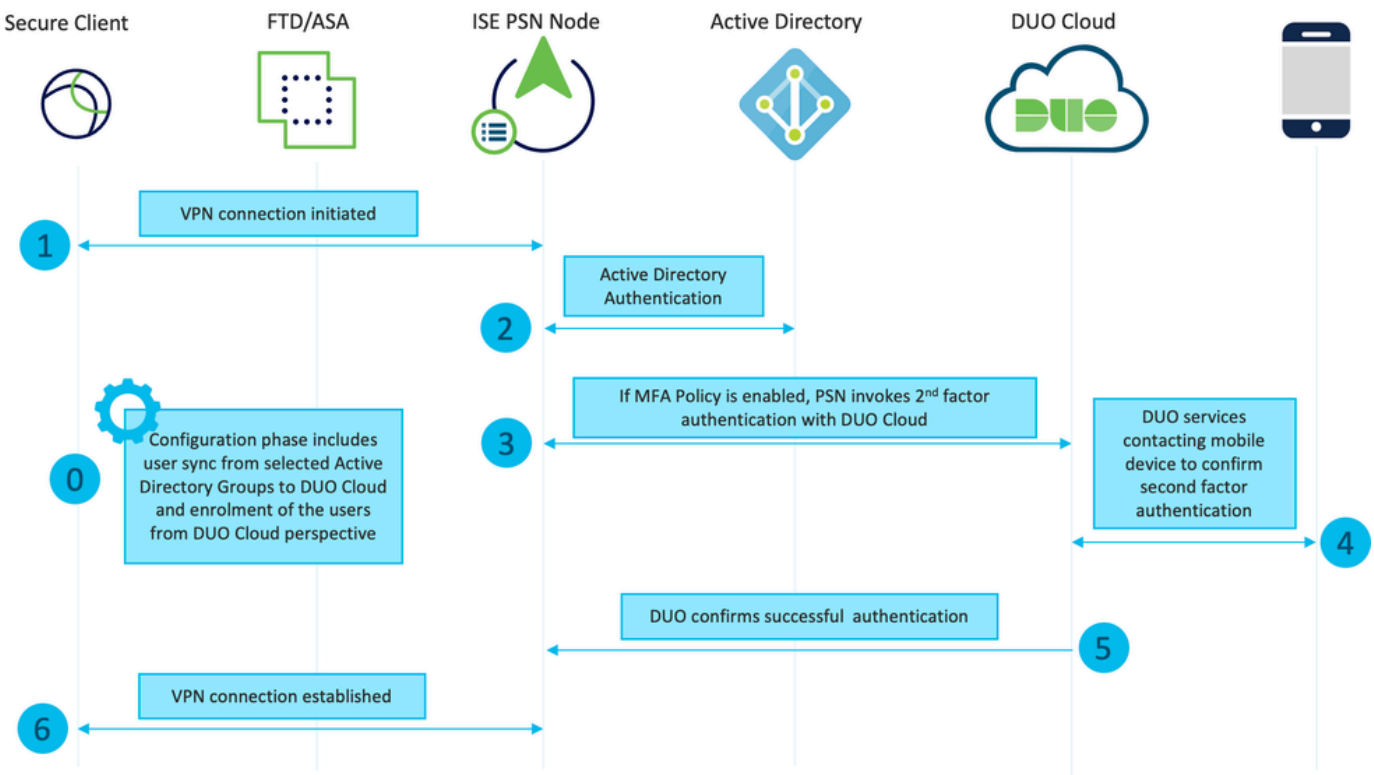
Les informations contenues dans ce document sont basées sur :

- 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



Étapes

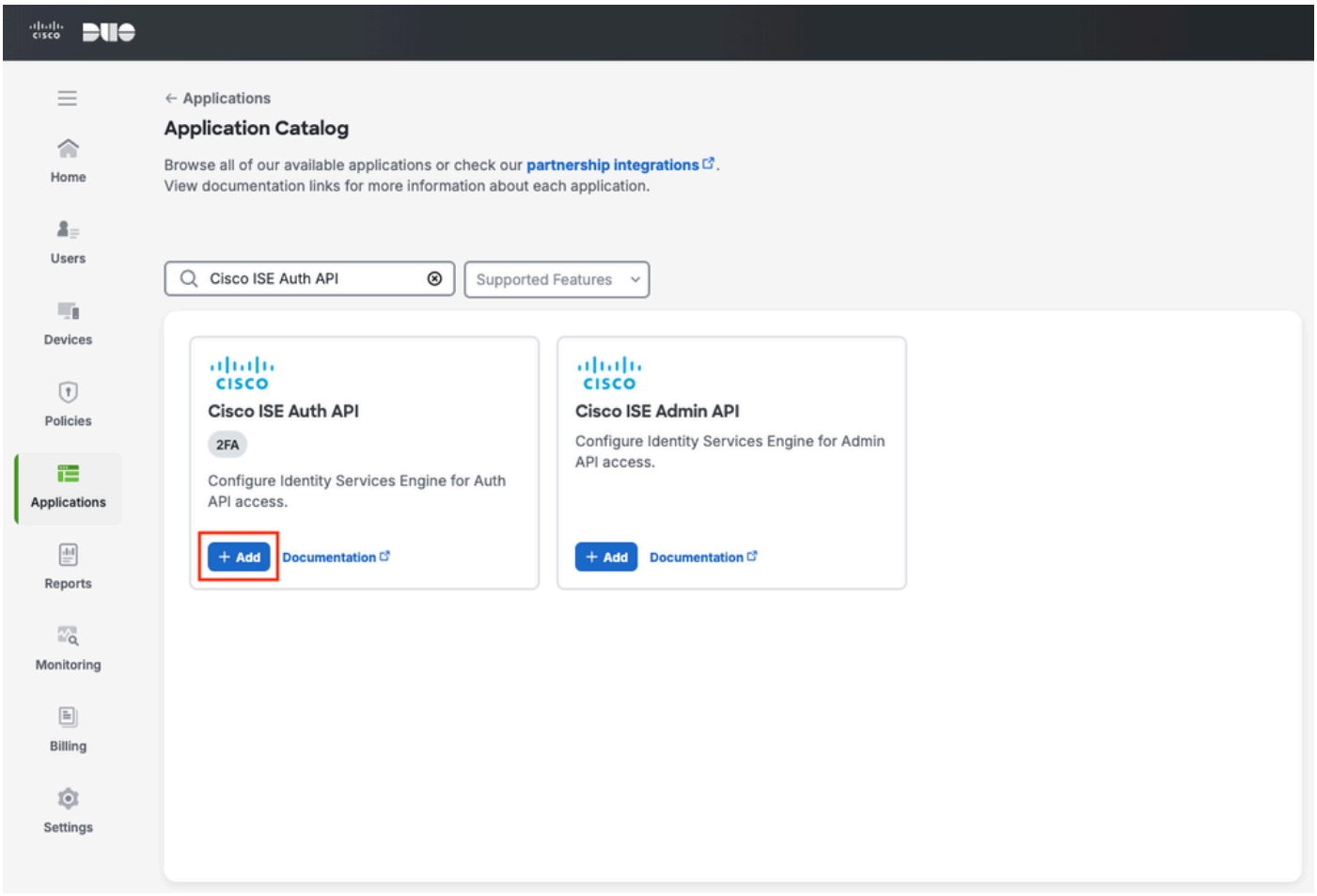
1. La phase de configuration inclut la sélection des groupes Active Directory auxquels les utilisateurs sont synchronisés et cette synchronisation se produit une fois l'assistant MFA terminé. Il se compose de deux étapes. Recherche dans Active Directory pour récupérer la liste des utilisateurs et certains attributs. Un appel vers le cloud Duo avec l'API d'administration ISE de Cisco, qui permet d'y envoyer les utilisateurs (les administrateurs sont tenus d'inscrire les utilisateurs). L'inscription des utilisateurs peut inclure l'étape facultative d'activation de l'utilisateur pour Duo Mobile, qui permet à vos utilisateurs d'utiliser l'authentification en un clic avec Duo Push.
2. Une fois qu'une connexion VPN est initiée, l'utilisateur entre son nom d'utilisateur et son mot de passe et clique sur OK. Le périphérique réseau envoie une requête d'accès RADIUS à PSN.
3. Le noeud PSN authentifie l'utilisateur via Active Directory.
4. Lorsque l'authentification réussit et que la stratégie MFA est configurée, PSN contacte Duo Cloud. Un appel vers Duo Cloud avec l'API d'authentification ISE de Cisco est effectué pour appeler une authentification de second facteur avec Duo. ISE communique avec le service Duos sur le port TCP SSL 443.
5. Une authentification de second facteur a lieu et l'utilisateur termine un processus d'authentification de second facteur.
6. Duo répond à PSN avec le résultat de l'authentification du second facteur.
7. L'acceptation d'accès est envoyée au périphérique réseau et la connexion VPN est établie.

Configurations

Sélectionner les applications à protéger

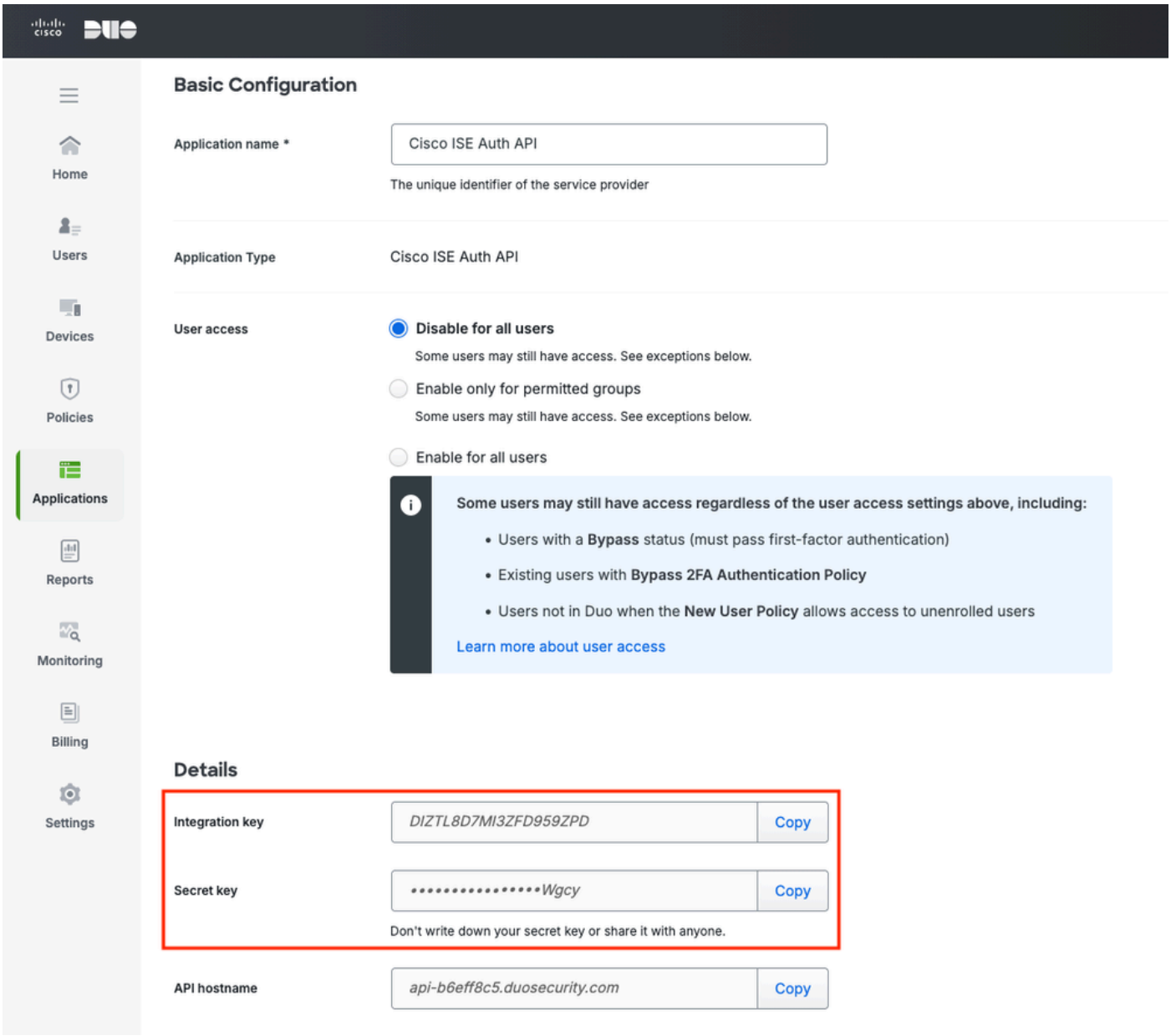
1. Accédez au tableau de bord Admin Duo. Connectez-vous avec les identifiants Admin.

2. Accédez à Tableau de bord > Applications > Catalogue d'applications. Recherchez Cisco ISE Auth API et sélectionnez + Add.



API d'authentification ISE 1

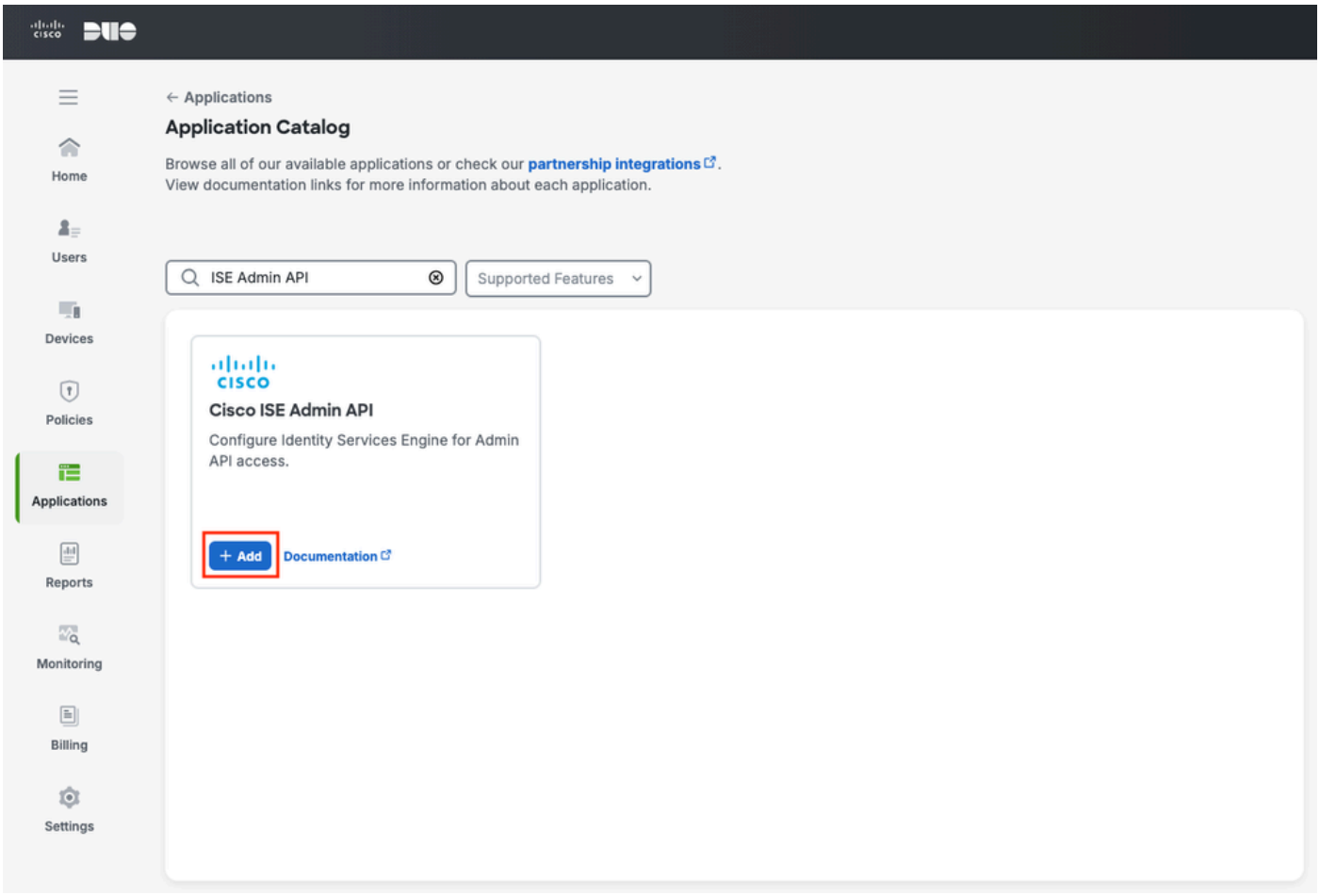
3. Notez la clé d'intégration et la clé secrète.



API d'authentification ISE 2

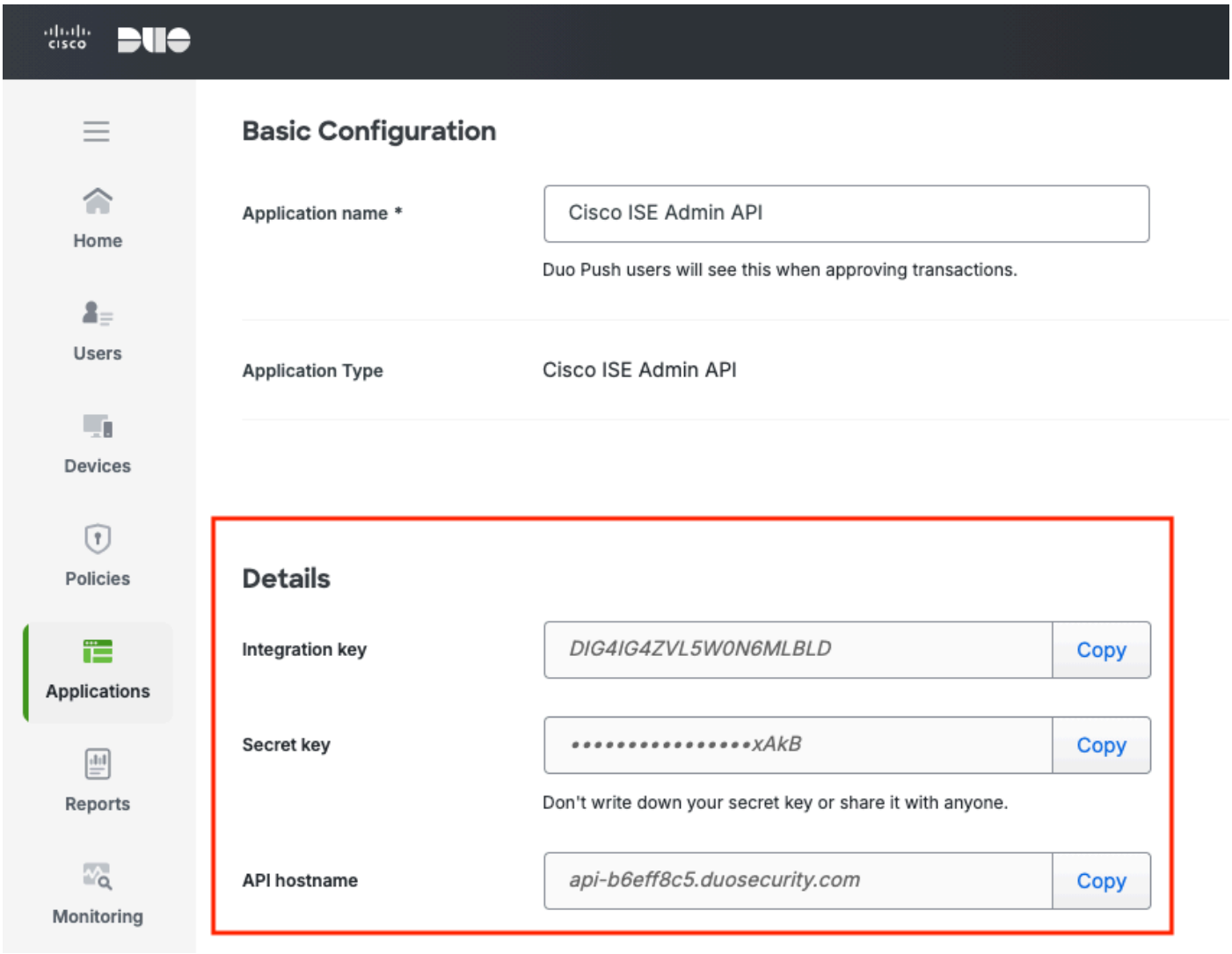
4. Accédez à Tableau de bord > Applications > Catalogue d'applications. Recherchez Cisco ISE Admin API et sélectionnez + Add.

Remarque : Seuls les administrateurs ayant le rôle Propriétaire peuvent créer ou modifier l'application Cisco ISE Admin API dans le panneau d'administration Duo.



API d'administration ISE 1

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

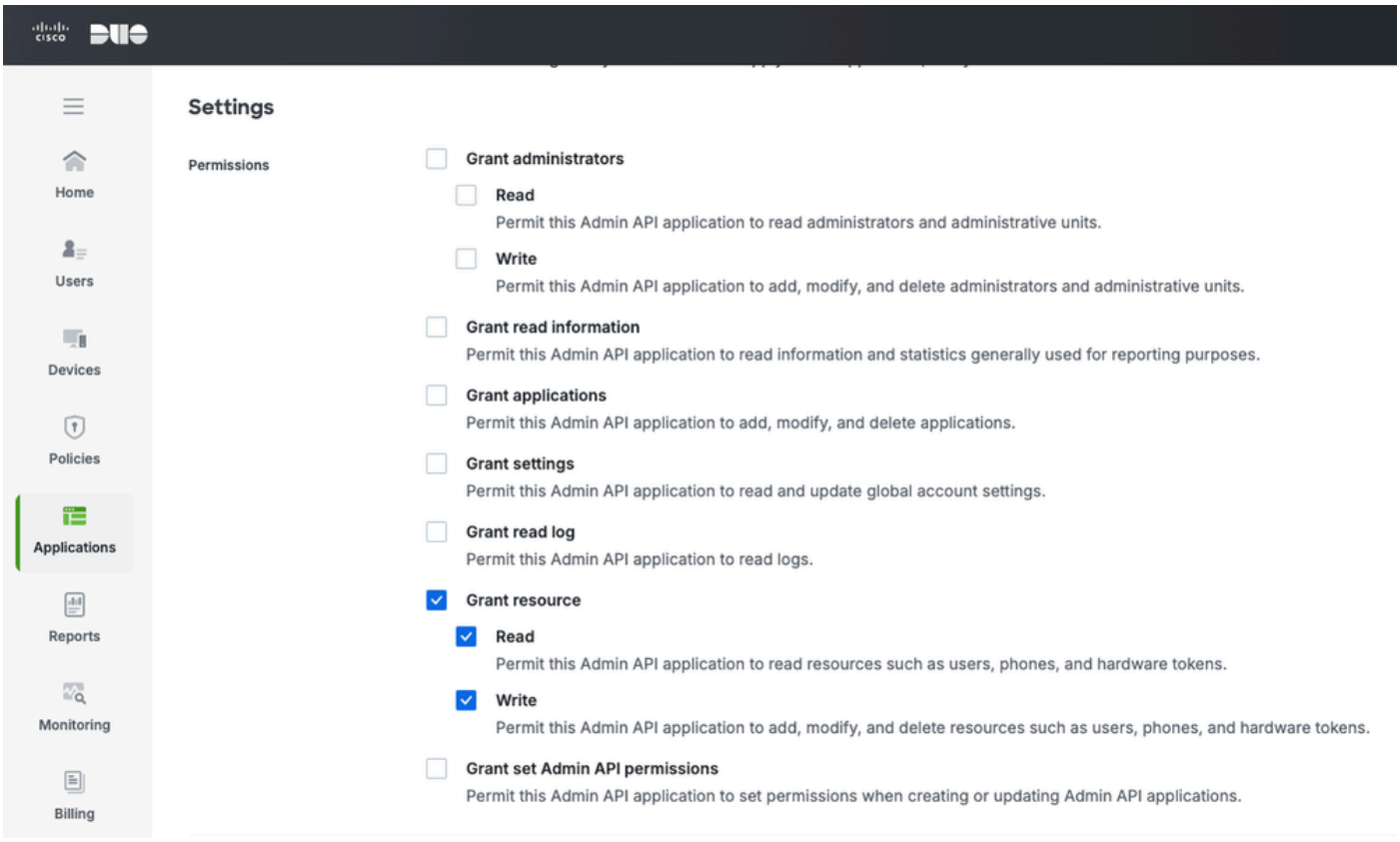


API d'administration ISE 2

Configurer les autorisations API

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

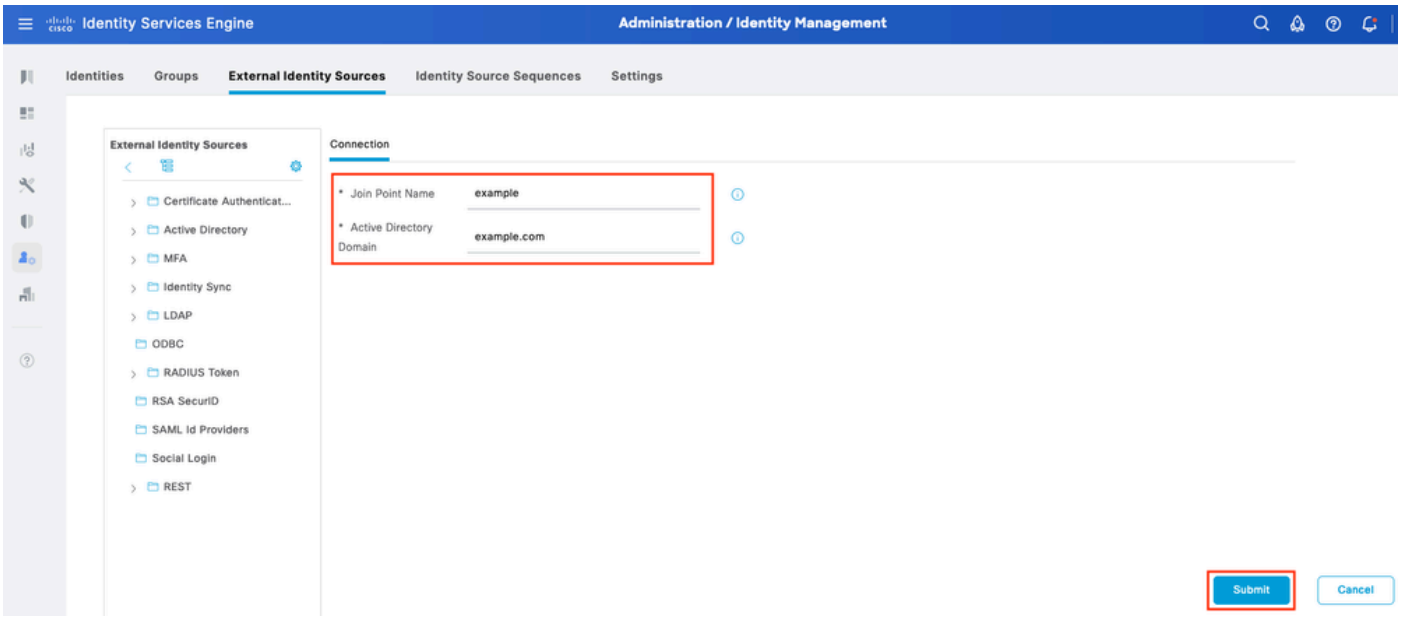
2. Cochez Grant Read Resource et Grant Write Resource permissions. Cliquez sur Enregistrer les modifications.



Autorisations API Admin

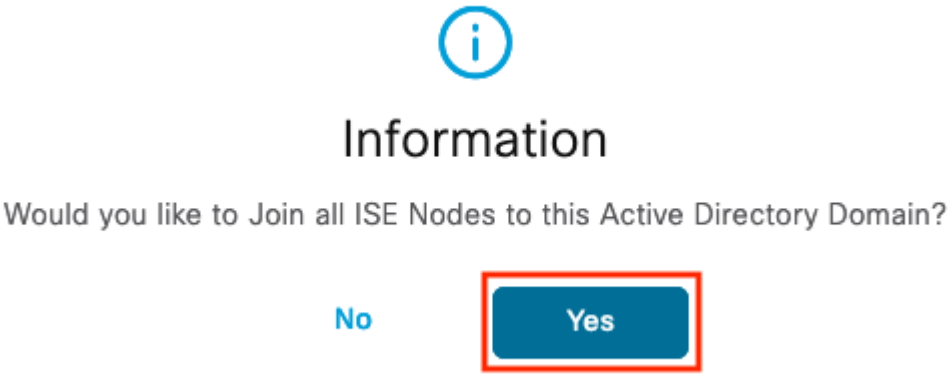
Intégrer ISE à Active Directory

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 Submit.



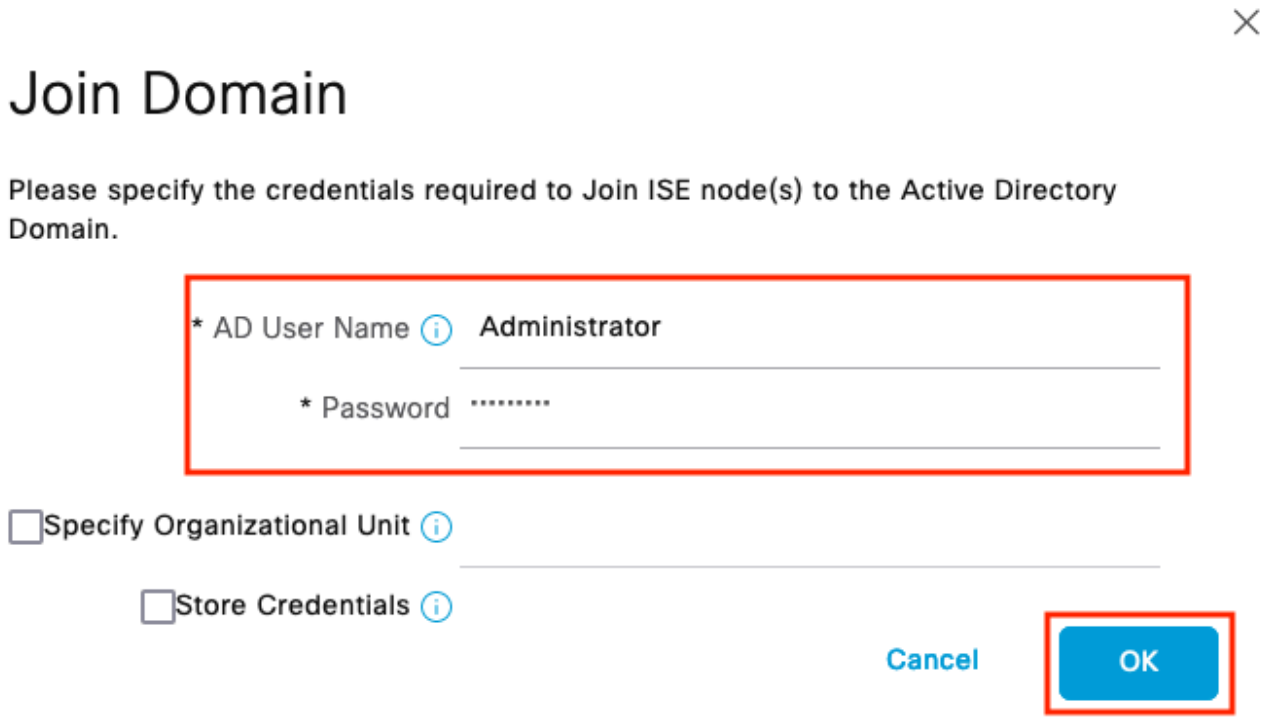
Active Directory 1

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



Active Directory 2

3. Entrez le nom d'utilisateur et le mot de passe Active Directory, puis cliquez sur OK.



Active Directory 3

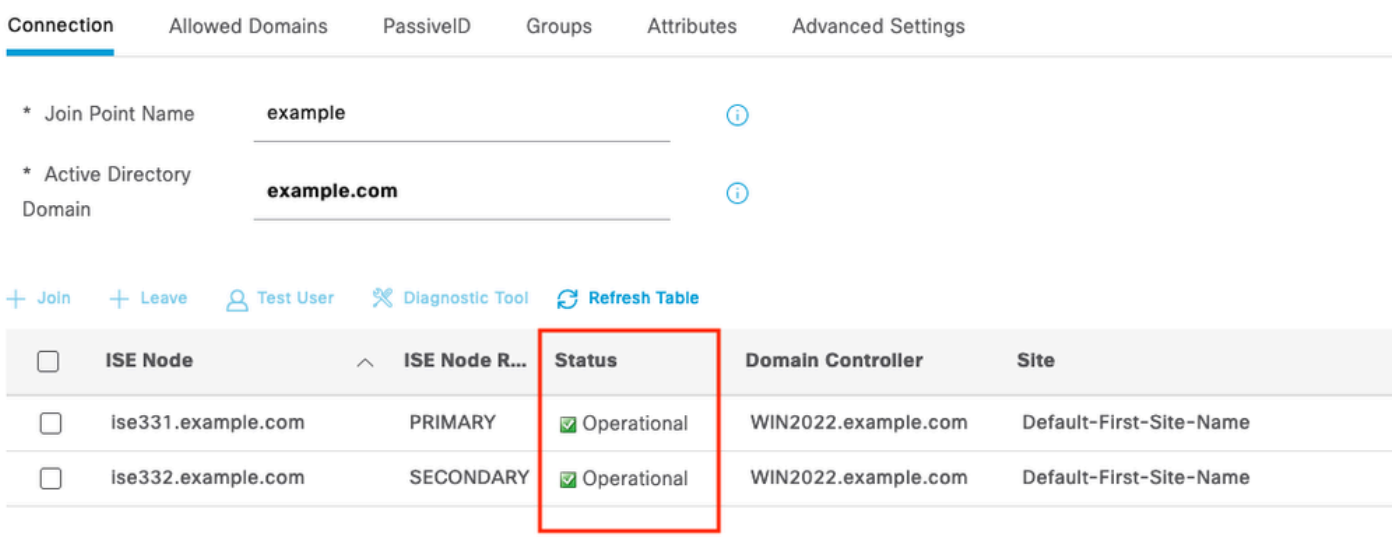
4. Le compte Active Directory requis pour l'accès au domaine dans ISE peut avoir l'un des éléments suivants :

- Ajouter des stations de travail au domaine droit utilisateur dans le domaine respectif.
- L'autorisation Créer des objets ordinateur ou Supprimer des objets ordinateur sur le conteneur d'ordinateurs respectif où le compte d'ordinateurs 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.

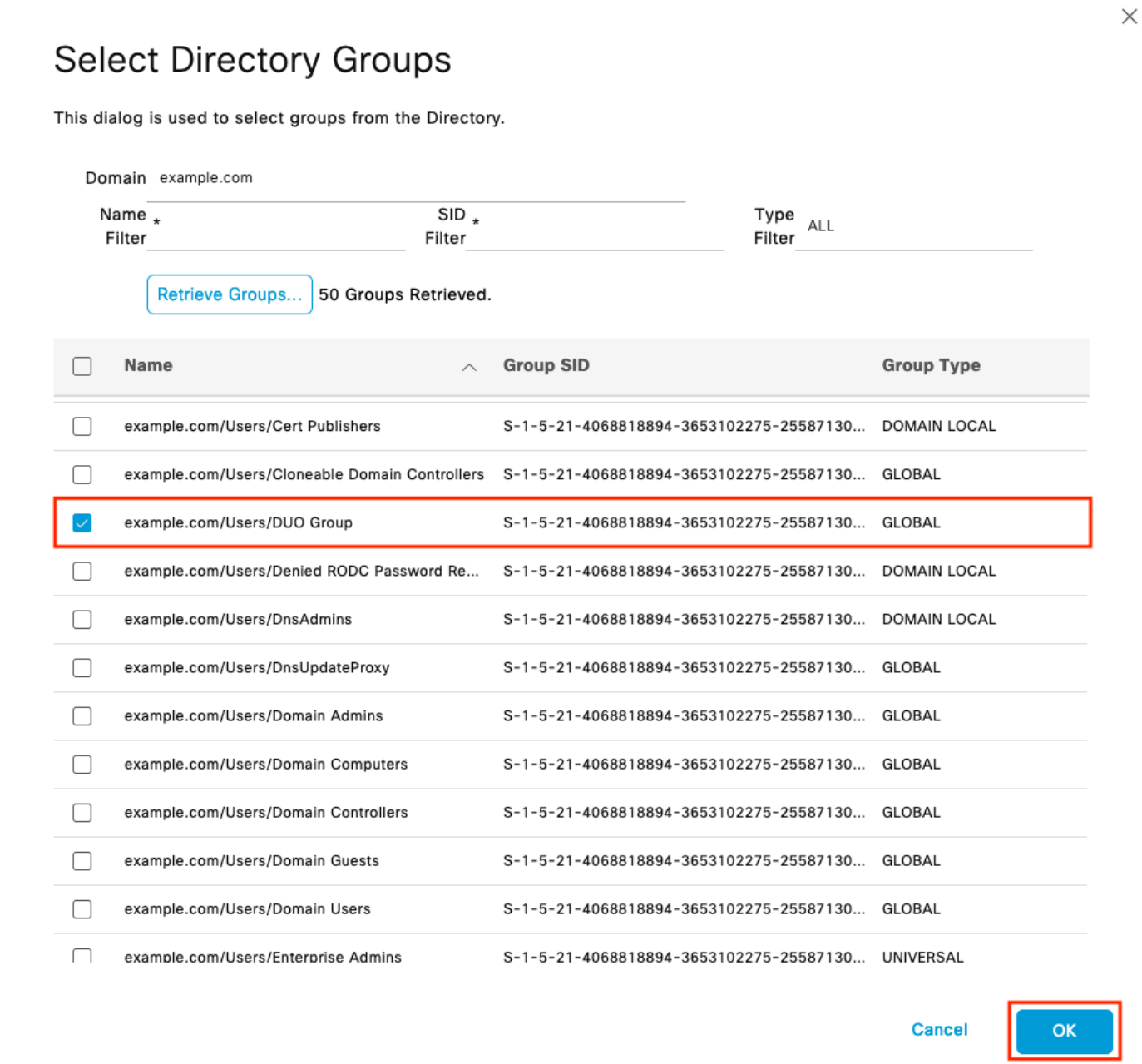
---

5. L'état d'AD est opérationnel.



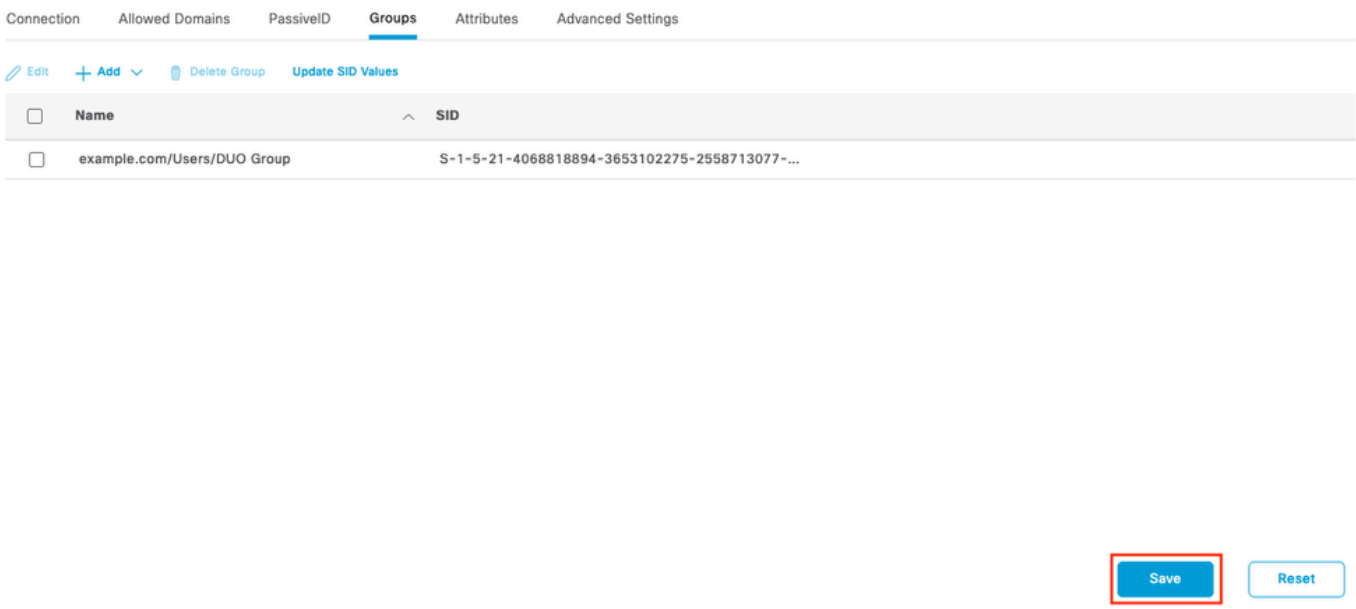
Active Directory 4

6. Accédez à Groupes > Ajouter > Sélectionner des groupes dans le répertoire > Récupérer des groupes. Cochez les cases en regard des groupes AD de votre choix (qui sont utilisés pour synchroniser les utilisateurs et pour la stratégie d'autorisation) :



Active Directory 5

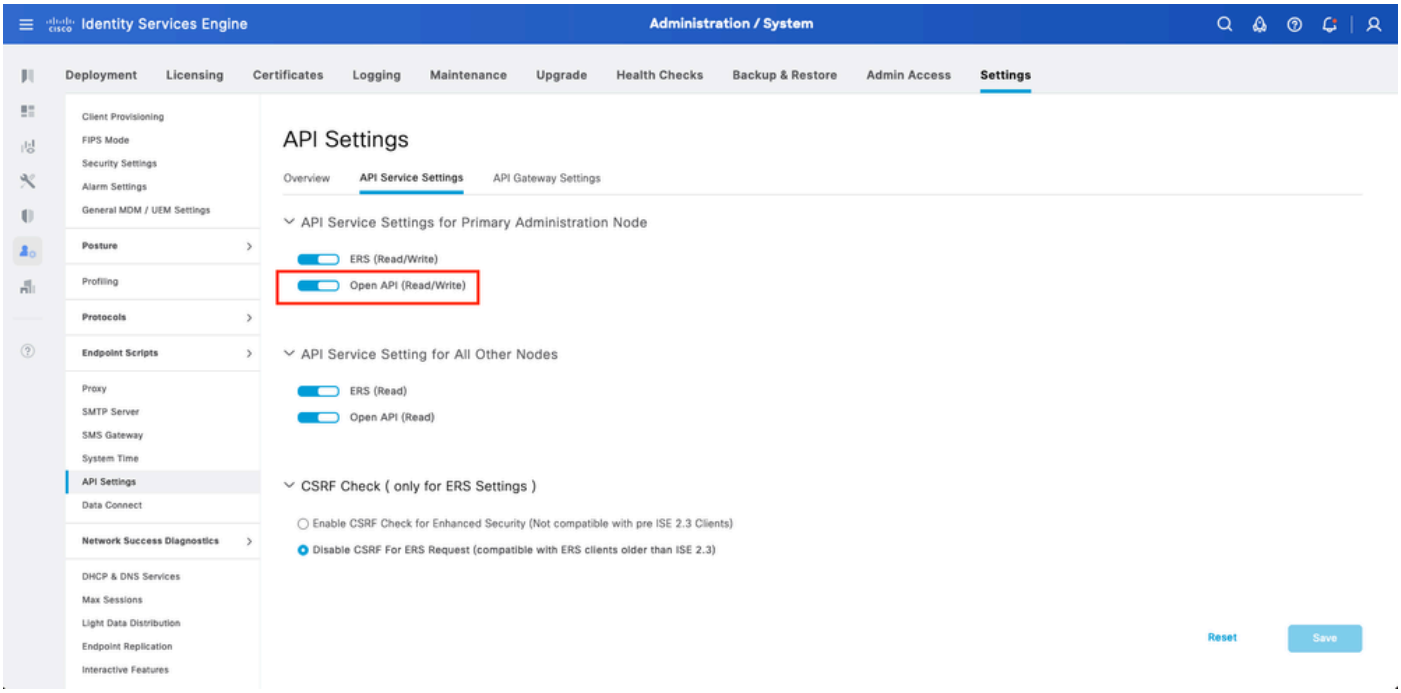
7. Cliquez sur Enregistrer pour enregistrer les groupes AD récupérés.



Active Directory 6

Activer l'API ouverte

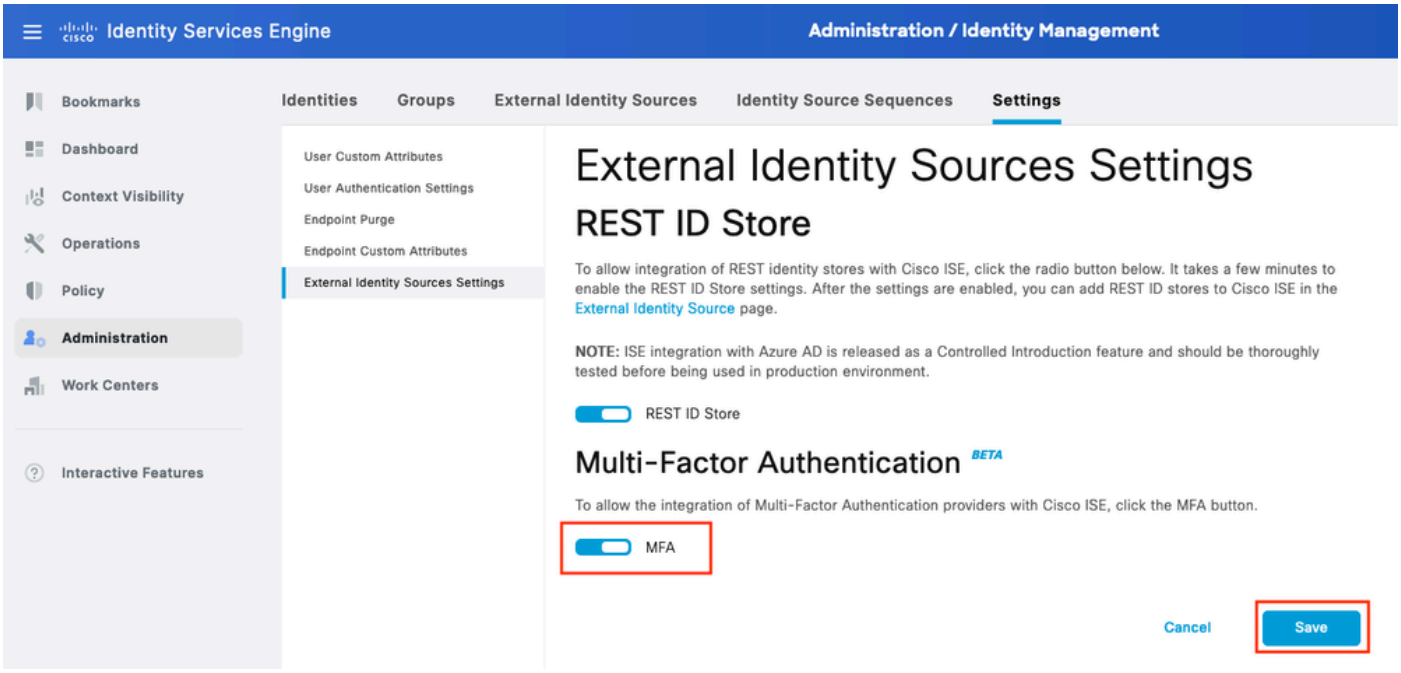
1. Accédez à Administration > System > Settings >API Settings > API Service Settings.Enable Open API et cliquez sur Save.



API ouverte

Activer la source d'identité MFA

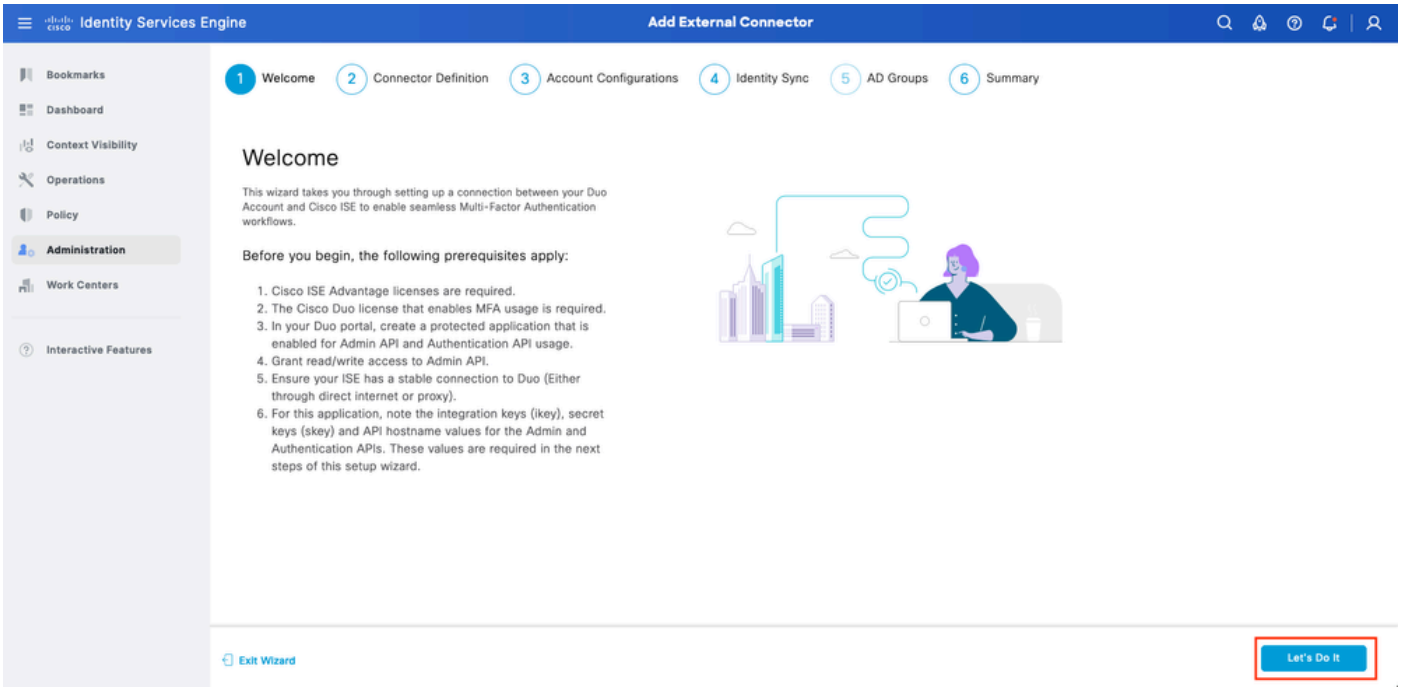
1. Accédez à Administration > Gestion des identités > Paramètres > Paramètres des sources d'identités externes. Activez MFA et cliquez sur Save.



ISE MFA 1

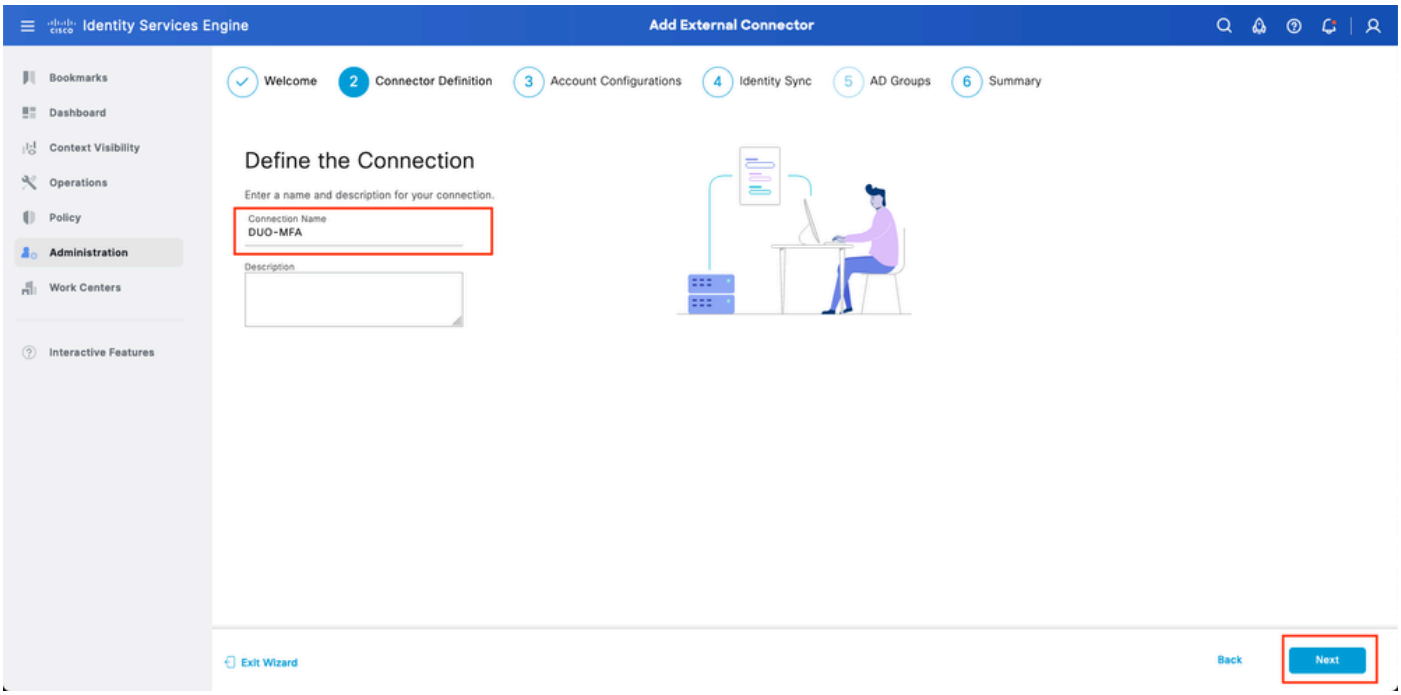
Configurer la source d'identité externe MFA

1. Accédez à Administration > Gestion des identités > Sources d'identités externes. Cliquez sur Add et sur l'écran Welcome cliquez sur Let's Do It.



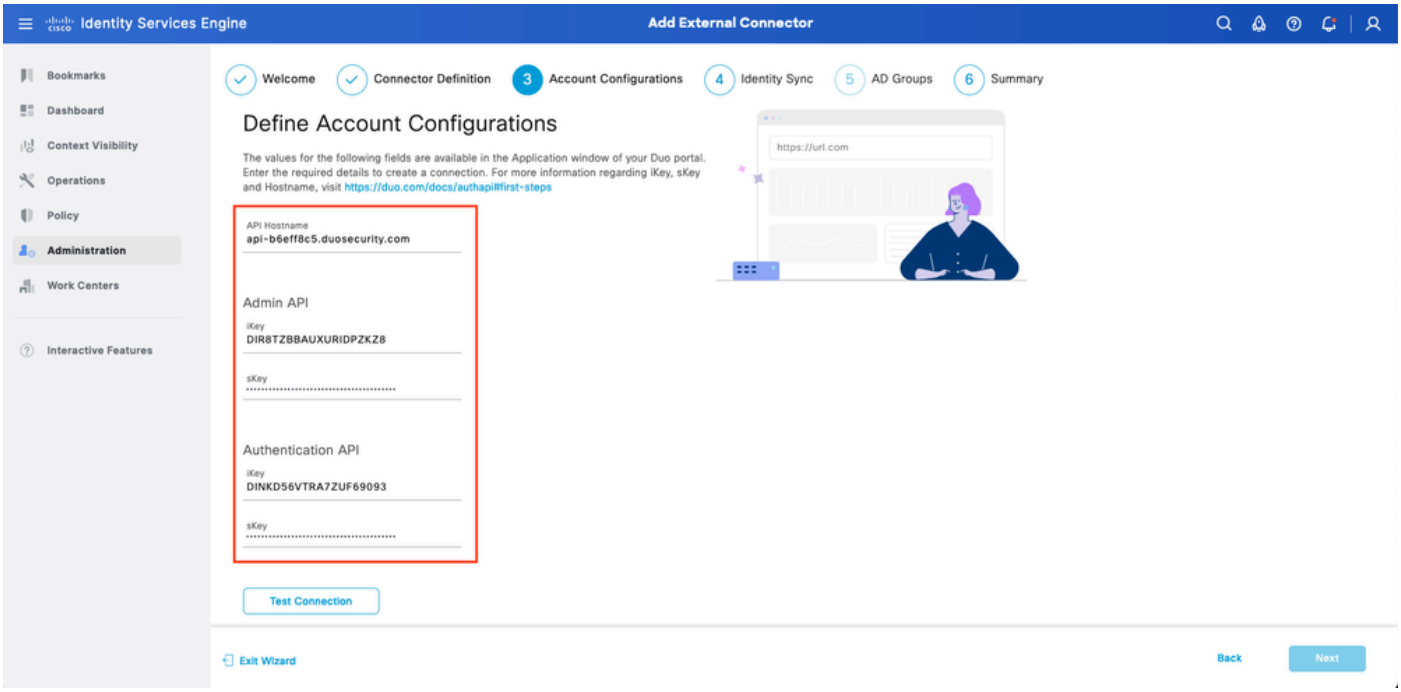
Assistant ISE Duo 1

2. Sur l'écran suivant, configurez le nom de connexion et cliquez sur Suivant.



Assistant ISE Duo 2

3. Configurez les valeurs de l'API Hostname, Cisco ISE Admin API Integration, Secret Keys, Cisco ISE Auth API Integration et Secret Keys de l'étape Select Applications à l'étape Protect.



Assistant ISE Duo 3

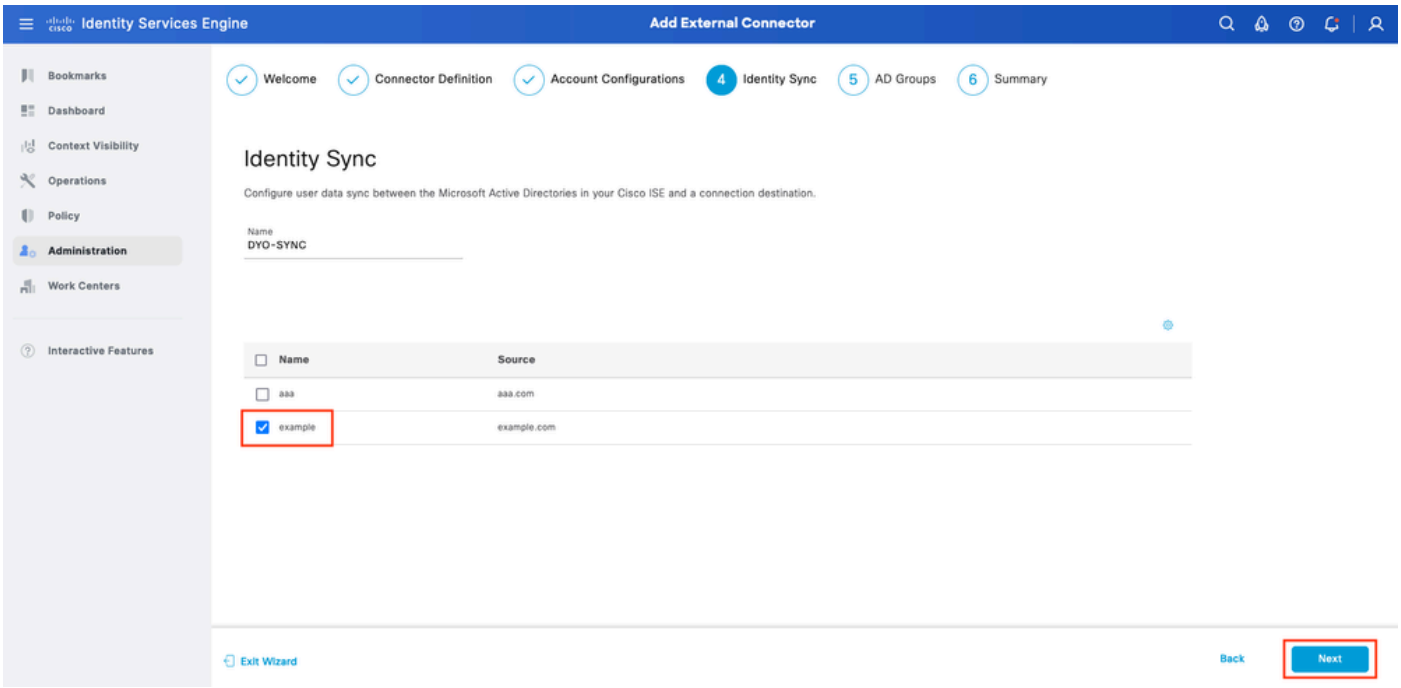
4. Cliquez sur Test Connection et une fois que le test de connexion réussit, cliquez sur Next.



Assistant ISE Duo 4

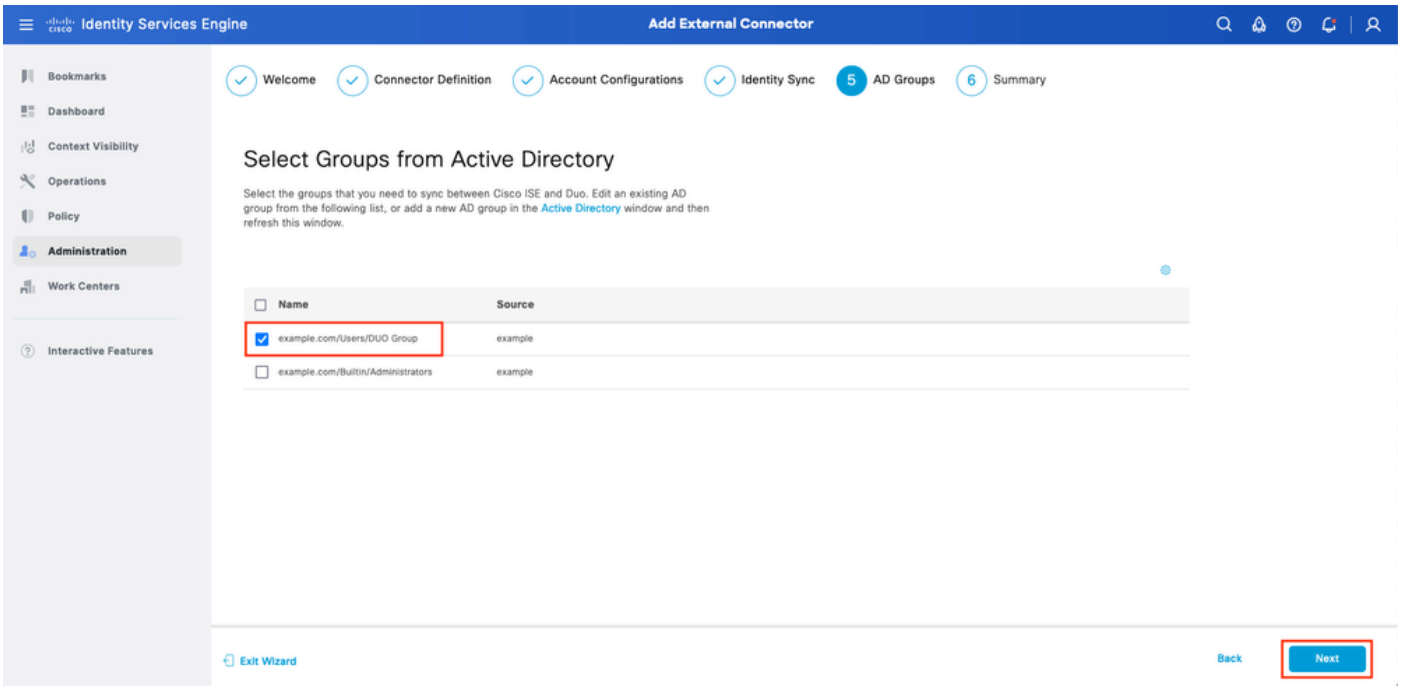
5. Configurez la synchronisation des identités. Ce processus synchronise les utilisateurs des groupes Active Directory que vous avez sélectionnés dans le compte Duo à l'aide des informations d'identification API fournies précédemment. Sélectionnez Point de connexion Active Directory puis cliquez sur Suivant.

Remarque : La configuration d'Active Directory sort du cadre de ce document. Reportez-vous à ce document pour intégrer ISE à Active Directory.



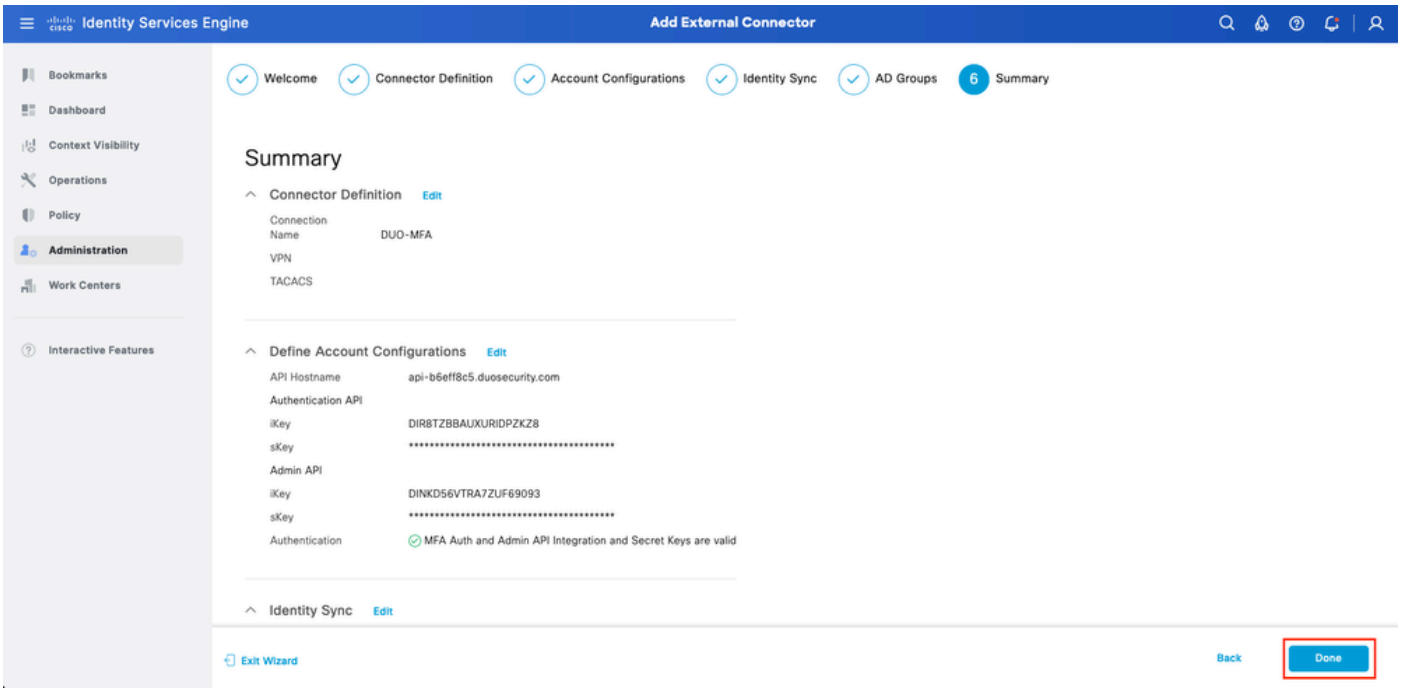
Assistant ISE Duo 5

6. Sélectionnez Groupes Active Directory où vous souhaitez que les utilisateurs se synchronisent avec Duo. Cliquez sur Suivant.



Assistant ISE Duo 6

7. Vérifiez que les paramètres sont corrects et cliquez sur Done.



Assistant ISE Duo 7

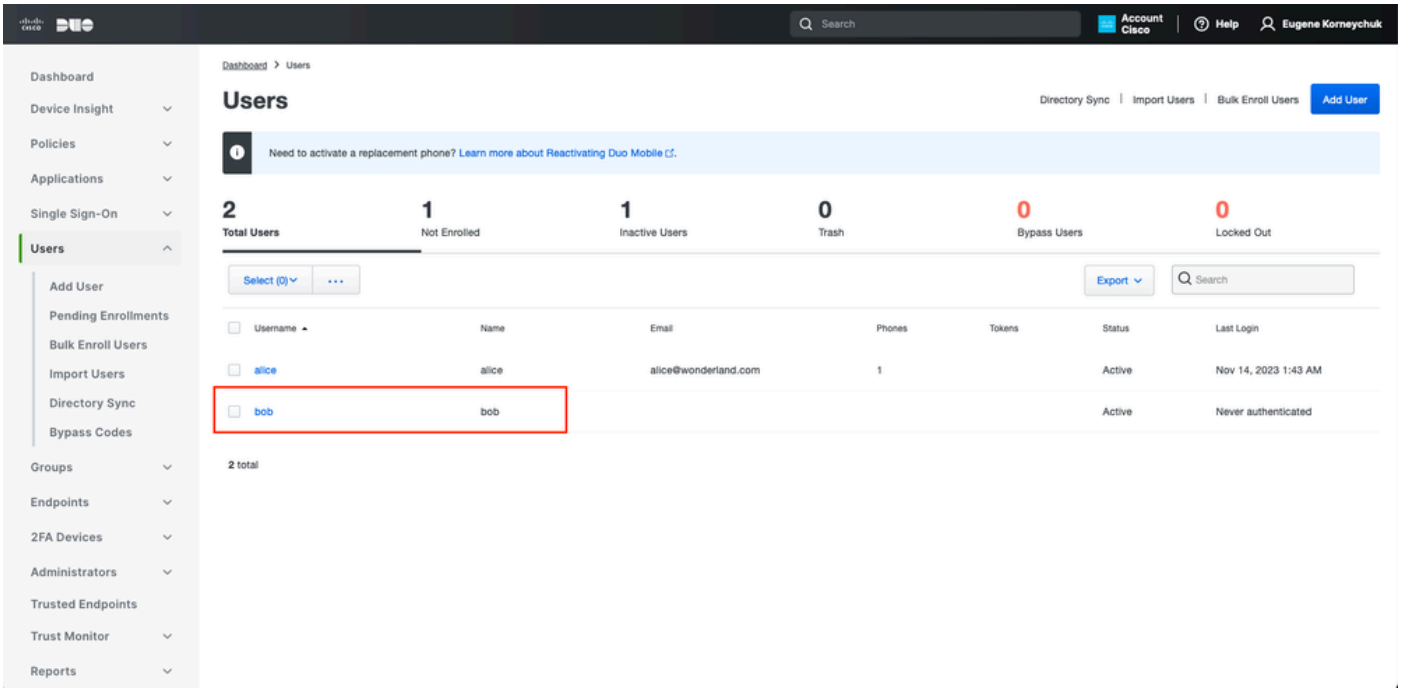
Inscription de l'utilisateur dans Duo

Remarque : L'inscription d'utilisateurs duo sort du cadre de ce document. Consultez ce document pour en savoir plus sur l'inscription d'utilisateurs. Dans le cadre de ce document,

l'inscription manuelle des utilisateurs est utilisée.

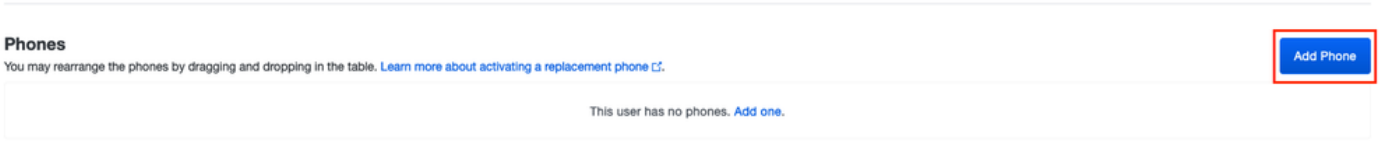
1. Ouvrez le tableau de bord Admin Duo et accédez à Tableau de bord > Utilisateurs.

2. Cliquez sur l'utilisateur synchronisé à partir d'ISE.



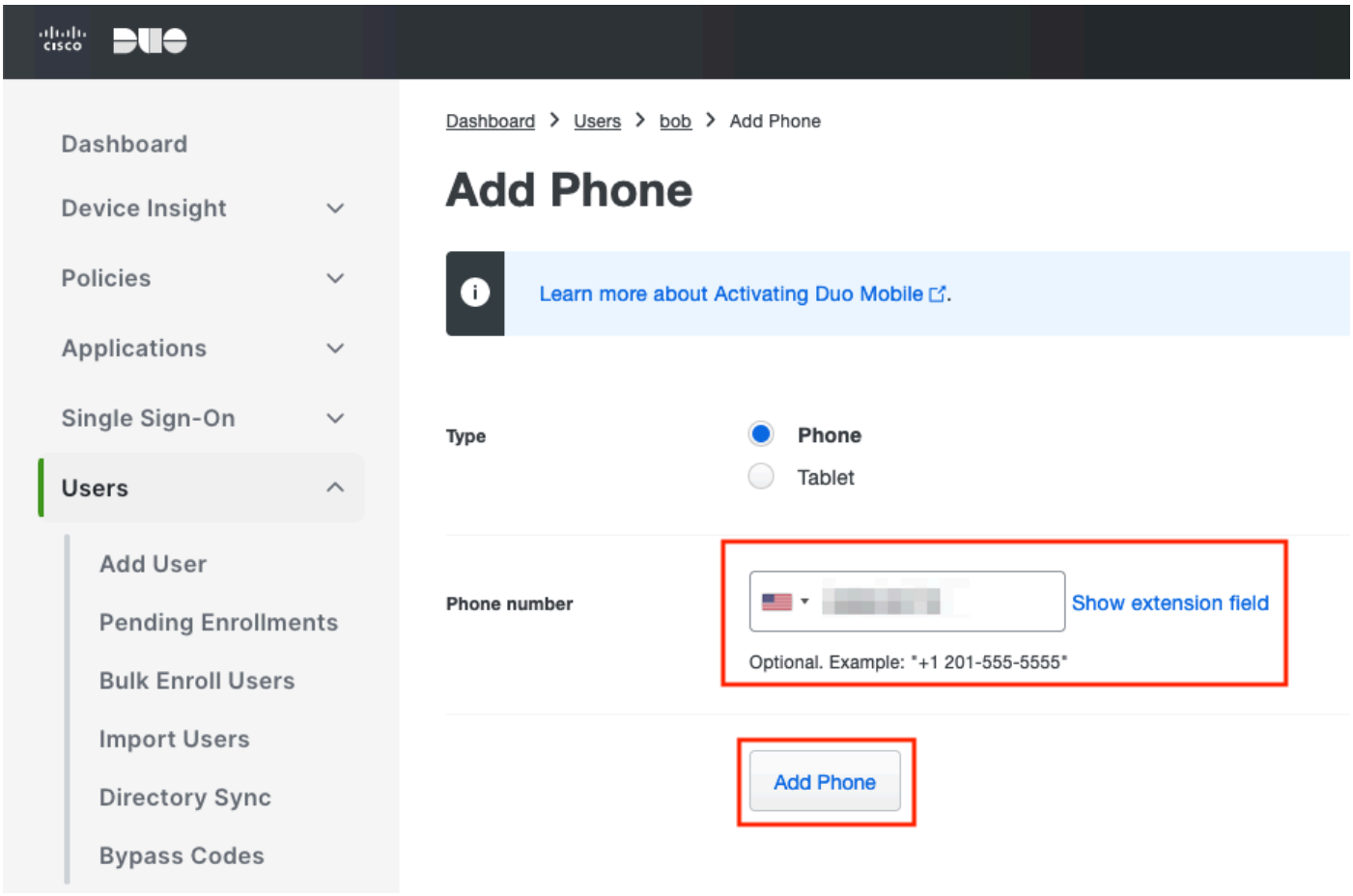
Inscription duo 1

3. Faites défiler jusqu'à Téléphones, puis cliquez sur Ajouter un téléphone.



Inscription Duo 2

4. Entrez le numéro de téléphone et cliquez sur Ajouter un téléphone.

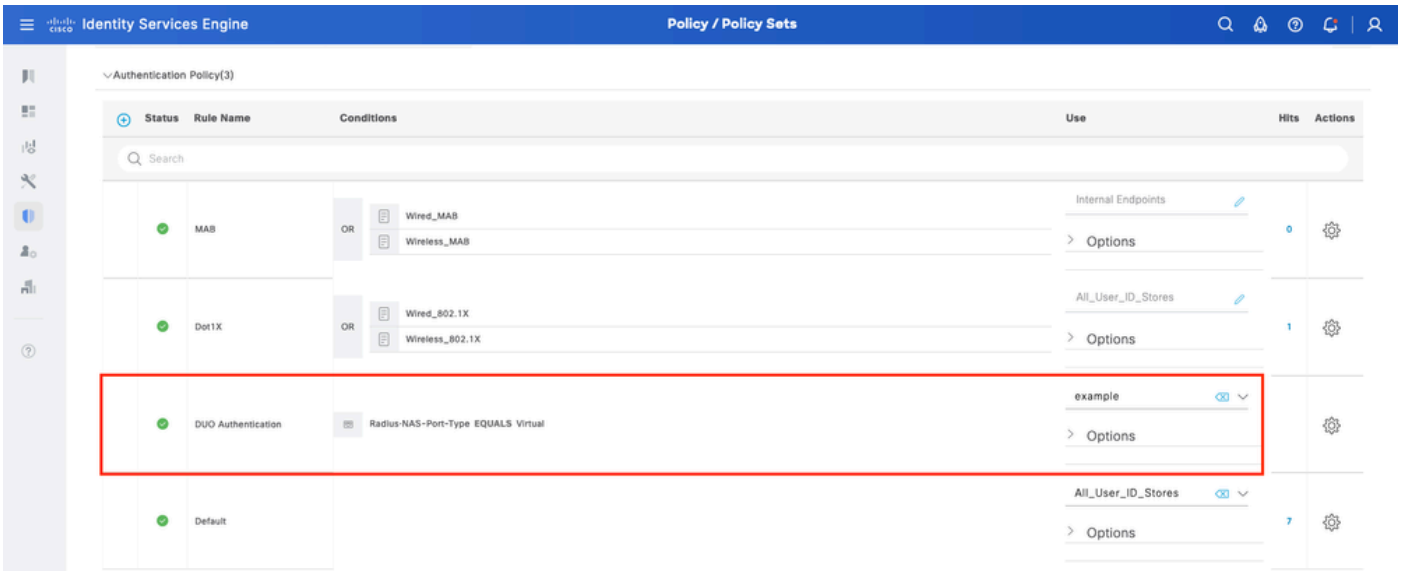


Inscription Duo 3

Configurer les jeux de stratégies

Configurer la stratégie d'authentification

1. Accédez à Policy > Policy Set et sélectionnez le Policy Set où vous souhaitez activer MFA. Configurez la stratégie d'authentification avec le magasin d'identités d'authentification principal comme Active Directory.

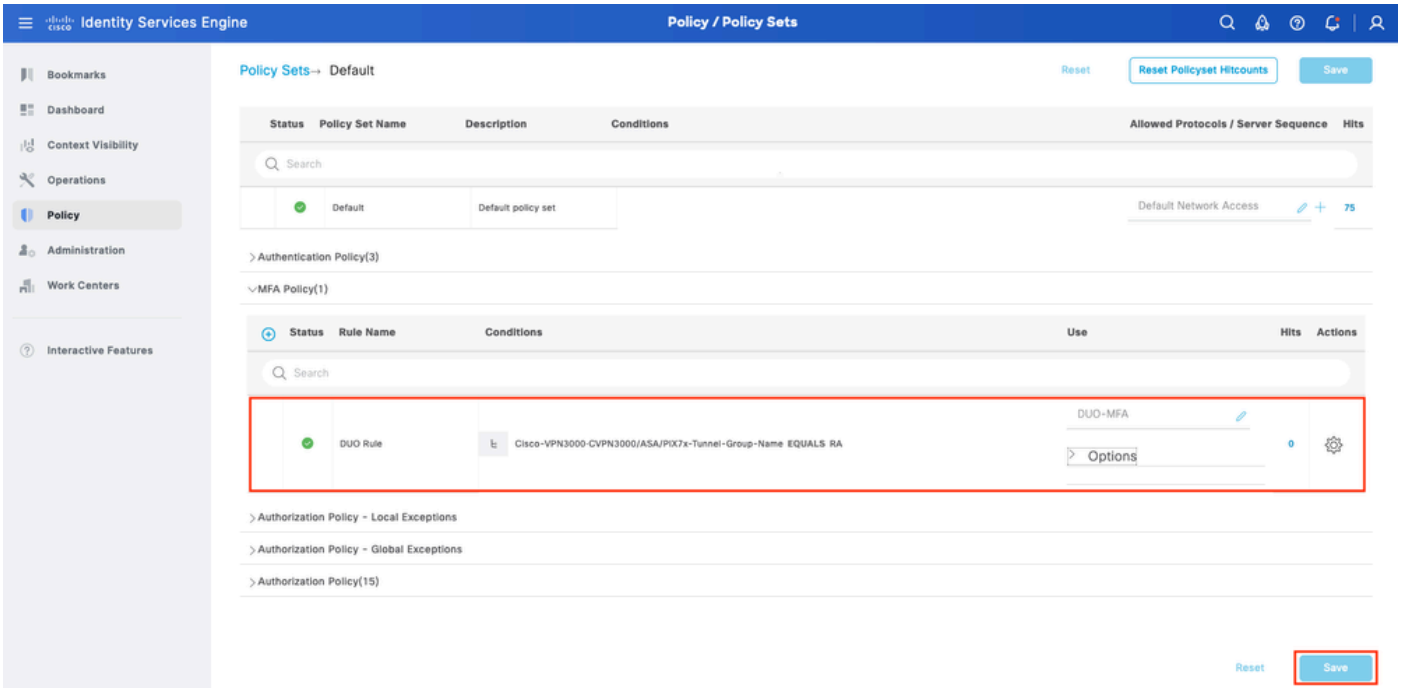


Jeu de stratégies 1

Configurer la stratégie MFA

1. Une fois que l'AMF est activée sur ISE, une nouvelle section des ensembles de stratégies ISE est disponible. Développez la politique d'AMF et cliquez sur le + pour ajouter la politique d'AMF. Configurez les conditions MFA de votre choix en sélectionnant le DUO-MFA configuré précédemment dans la section Use.

2. Cliquez sur Enregistrer.

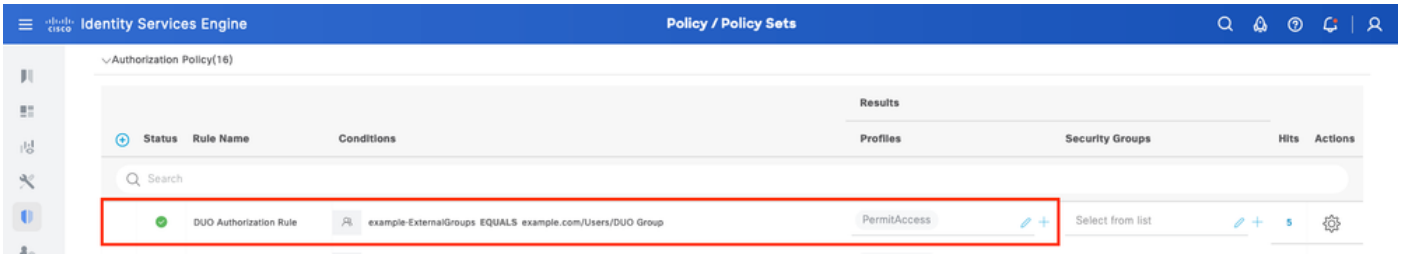


Politique ISE

Remarque : La stratégie configurée précédemment 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. Référez-vous à ce document pour configurer ASA/FTD.

Configurer la stratégie d'autorisation

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



Ensemble de stratégies 3

Limites

Au moment de la rédaction du présent document :

1. Seules les méthodes push et phone Duo sont prises en charge en tant que méthode d'authentification de second facteur

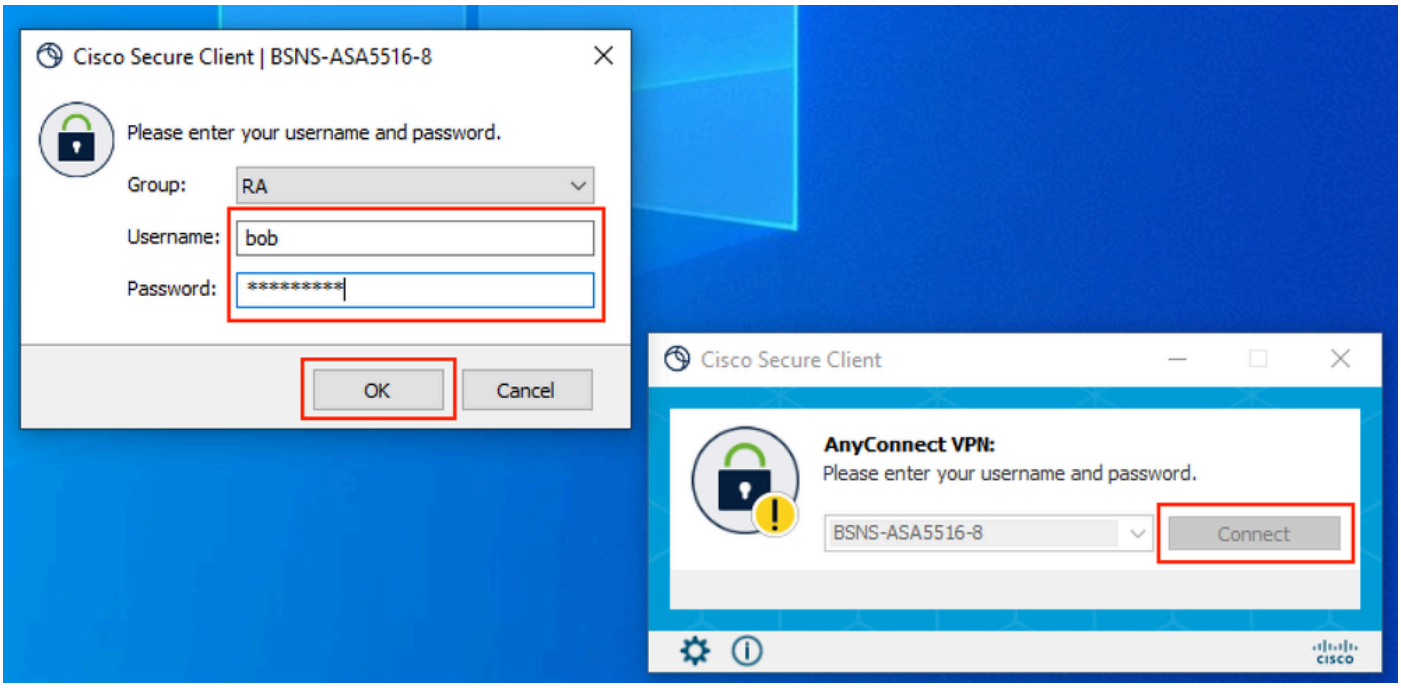
2. Aucun groupe n'est envoyé vers le cloud Duo, seule la synchronisation utilisateur est prise en charge

3. Ces puces sont prises en charge avec l'authentification multifacteur :

- Authentification utilisateur VPN
- Authentification d'accès administrateur TACACS+

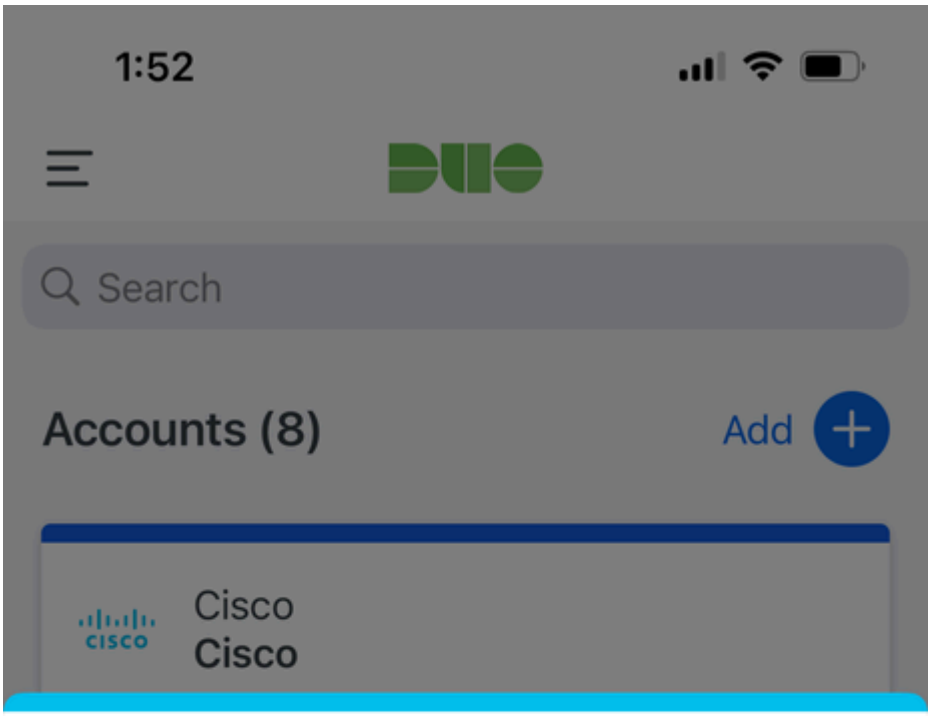
Vérifier

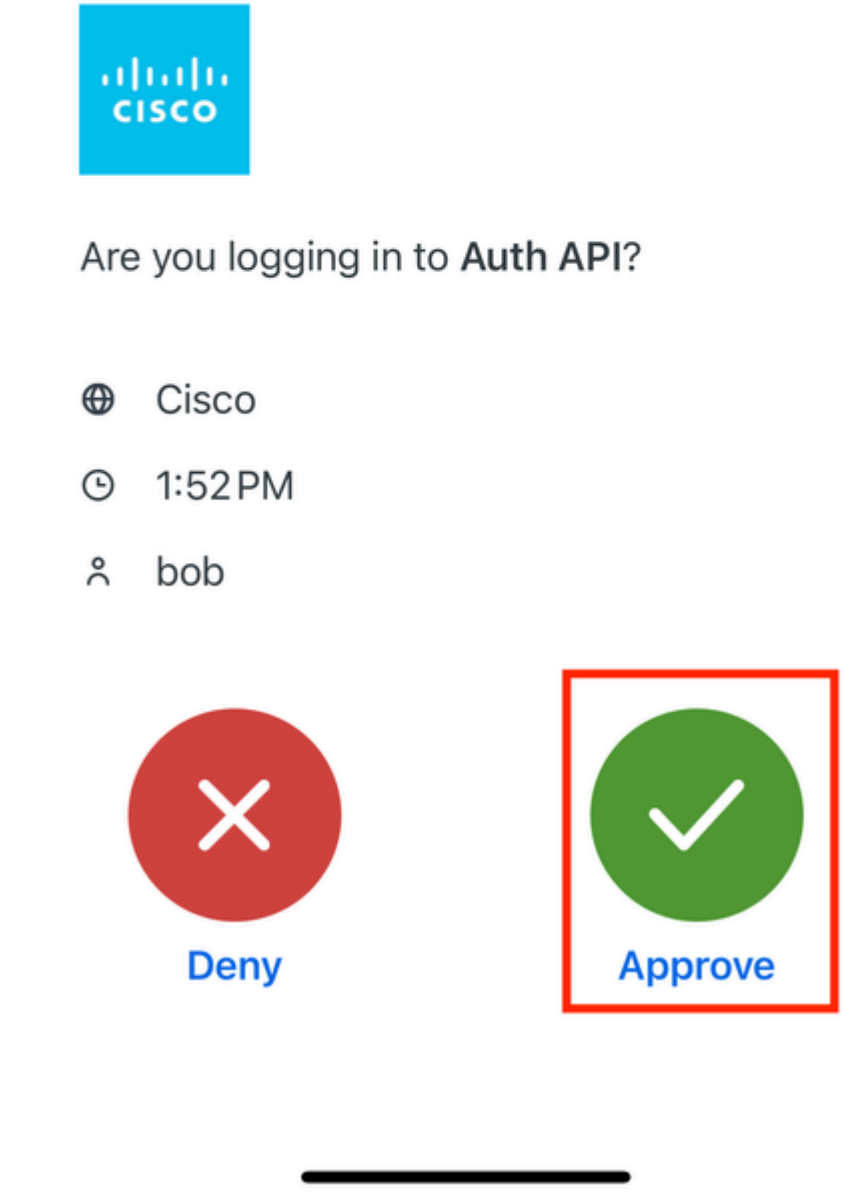
1. Ouvrez Cisco Secure Client, cliquez sur Connect et fournissez le nom d'utilisateur et le mot de passe, puis cliquez sur OK.



Client VPN

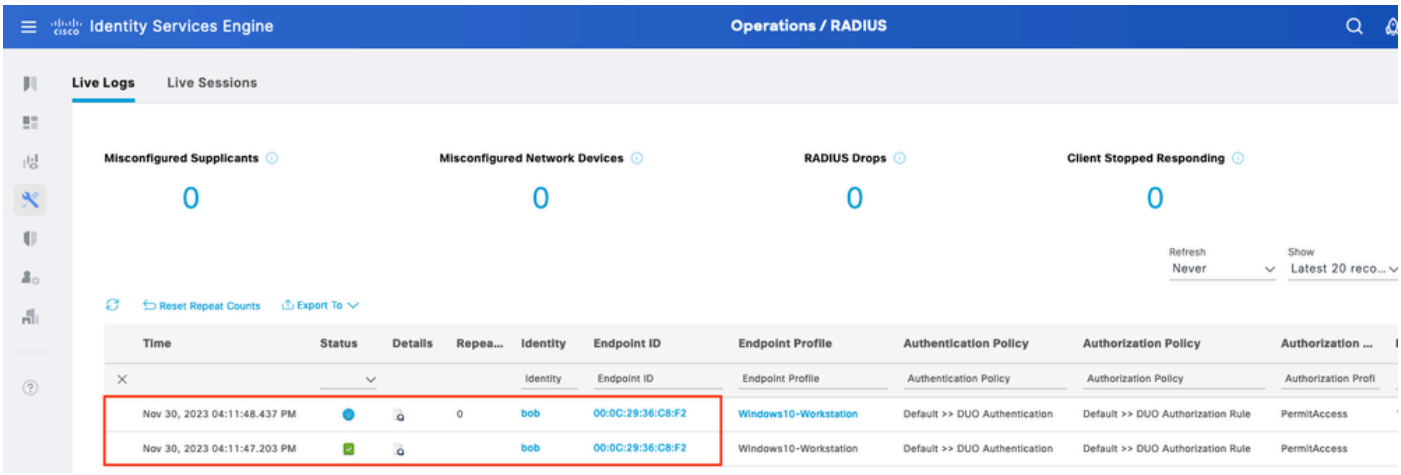
2. L'appareil mobile des utilisateurs doit recevoir une notification de transmission duo. Approuvez-le et la connexion VPN est établie.


1:52
Search
Accounts (8)
Add
Cisco
Cisco


Are you logging in to Auth API?
Cisco
1:52 PM
bob
Deny
Approve

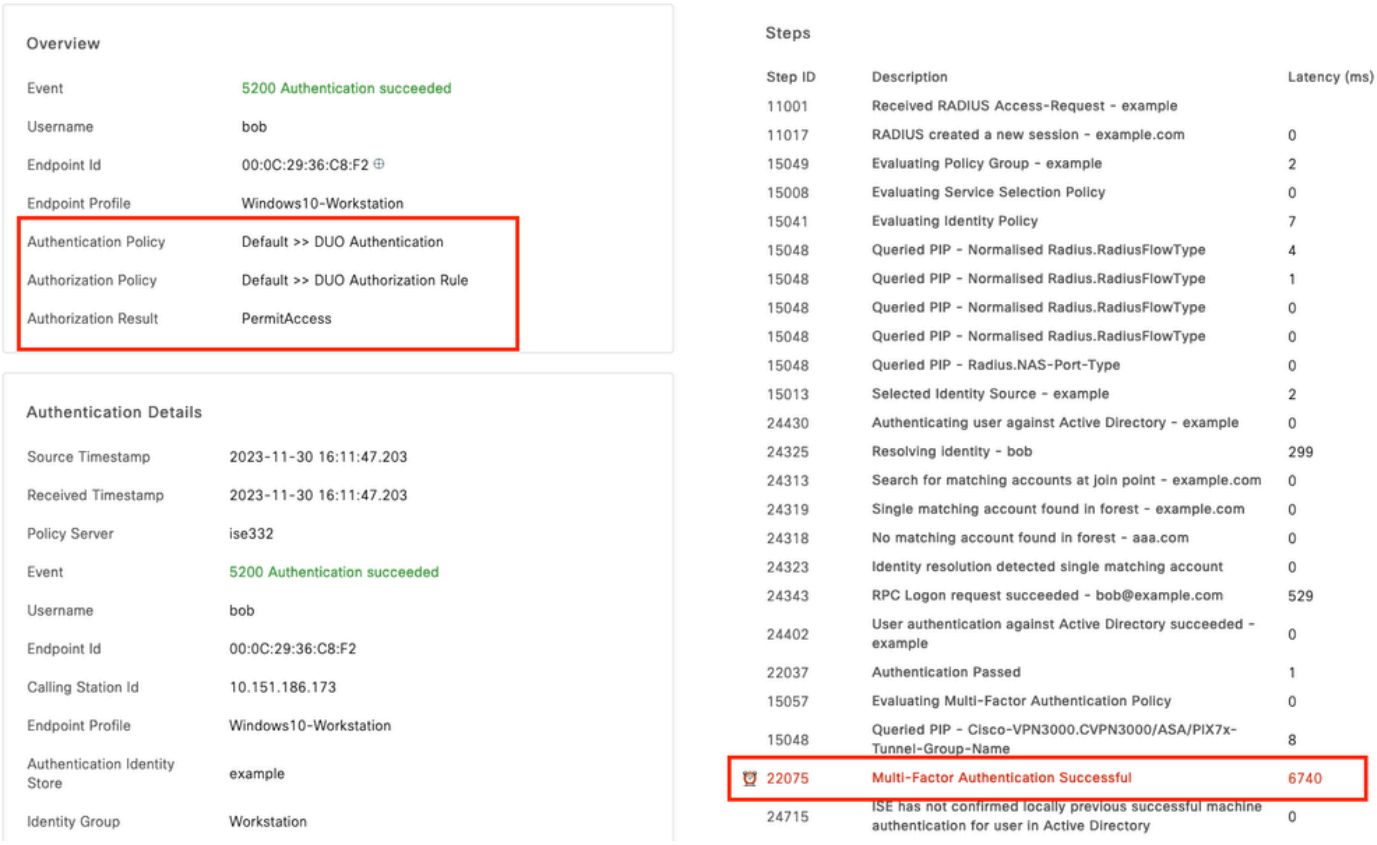
Poussée Duo

3. Accédez à ISE Operations > Live Logs pour confirmer l'authentification de l'utilisateur.



Journaux actifs 1

4. Cliquez sur le rapport d'authentification détaillé, vérifiez la stratégie d'authentification, ainsi que la stratégie d'autorisation et le résultat d'autorisation. Faites défiler les étapes vers la droite. Pour confirmer que MFA a réussi, la ligne MultiFactor Authentication is Successful doit être présente :



Journaux actifs 2

Dépannage

Débogages à activer sur ISE :

Scénario	Composant du journal	Fichier journal	Messages du journal des clés
Journaux MFA associés	moteur politique	ise-psc.log	DuoMfaAuthApiUtils -::::- Demande envoyée au gestionnaire client Duo DuoMfaAuthApiUtils —> Duo response
Journaux liés aux stratégies	port-JNI	prt-management.log	ProcesseurRequêtePolitiqueMfaRadius ProcesseurRequêtePolitiqueMfaTacas
Journaux relatifs à l'authentification	runtime-AAA	prt-server.log	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
Journaux associés à Duo Authentication, 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.