Configureer ISE 3.3 Native multi-factor verificatie met DUO

Inhoud

Inleiding

In dit document wordt beschreven hoe u Identity Services Engine (ISE) 3.3-patch 1 met DUO voor multi-factor verificatie kunt integreren. Vanaf versie 3.3 patch 1 ISE kan worden geconfigureerd voor native integratie met DUO-services, waardoor de noodzaak voor verificatie proxy wordt geëlimineerd.

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis te hebben van deze onderwerpen:

- ISE
- DUO

Gebruikte componenten

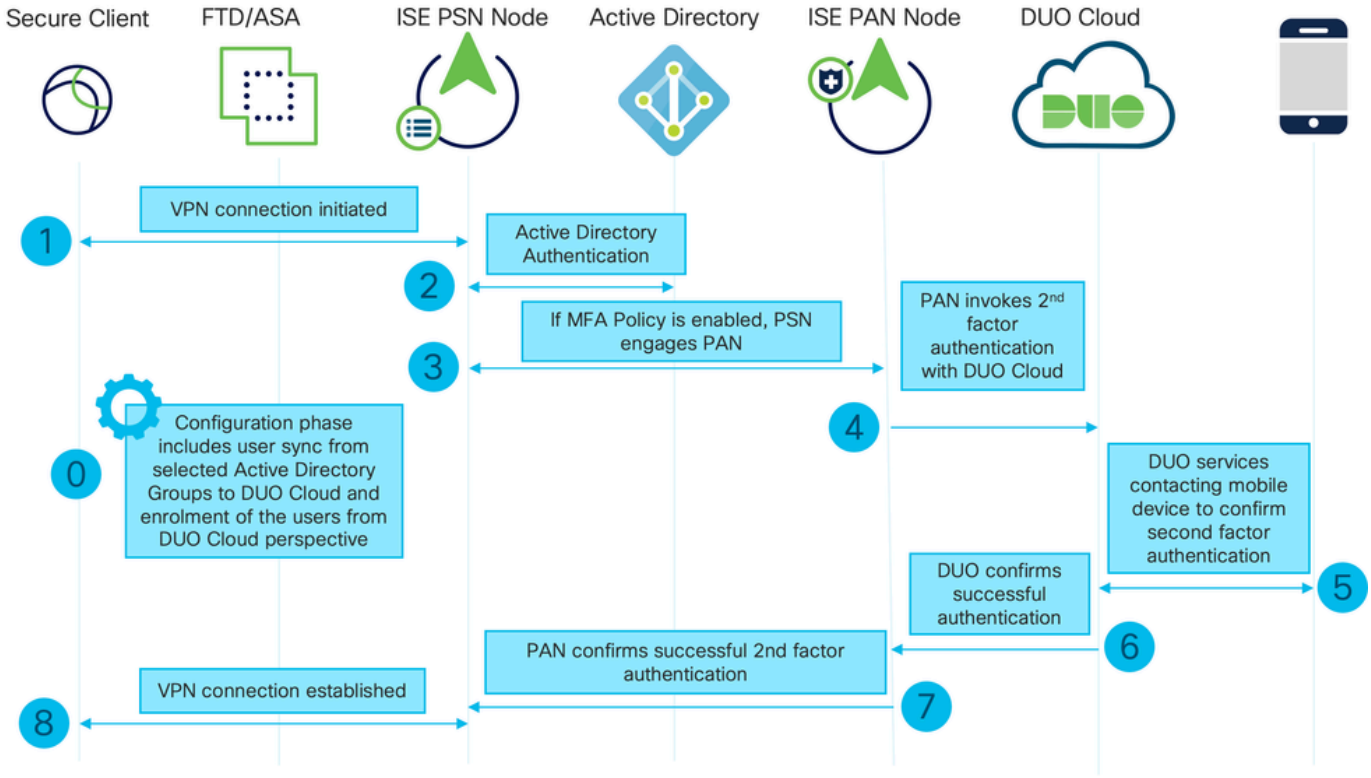
De informatie in dit document is gebaseerd op:

- Cisco ISE versie 3.3 patch 1
- DUO
- Cisco ASA versie 9.16(4)
- Cisco Secure-clientversie 5.0.04032

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Stroomdiagram



Stroomdiagram

Stappen

0. De configuratiefase omvat de selectie van de Active Directory-groepen, waaruit gebruikers gesynchroniseerd zijn, de synchronisatie gebeurt zodra de MFA-wizard is voltooid. Het bestaat uit twee stappen. Zoekopdrachten naar Active Directory om de lijst van gebruikers en bepaalde eigenschappen. Er wordt een oproep gedaan naar DUO Cloud met Admin API om gebruikers daar te duwen. Beheerders moeten gebruikers inschrijven. U kunt zich aanmelden met de optionele stap van het activeren van de gebruiker voor Duo Mobile, waarmee uw gebruikers eenmalige verificatie met Duo Push kunnen gebruiken

1. De VPN-verbinding wordt geïnitieerd, de gebruiker voert de gebruikersnaam en het wachtwoord in en klikt op OK. Het netwerkapparaat verzendt RADIUS-toegangsaanvraag naar PSN

2. PSN-knooppunt verifieert de gebruiker via Active Directory

3. Wanneer de verificatie slaagt en het MFB-beleid is geconfigureerd, neemt PSN PAN aan om contact op te nemen met DUO Cloud

4. Een oproep naar DUO Cloud met Auth API wordt gedaan om een tweede-factor authenticatie met DUO aan te roepen. ISE communiceert met Duo's service via SSL TCP poort 443.

5. De authenticatie van de tweede factor vindt plaats. De gebruiker voltooit het verificatieproces van de tweede factor

6. DUO reageert op PAN met het resultaat van de tweede-factor-authenticatie

7. PAN reageert op PSN met het resultaat van de tweede-factorverificatie

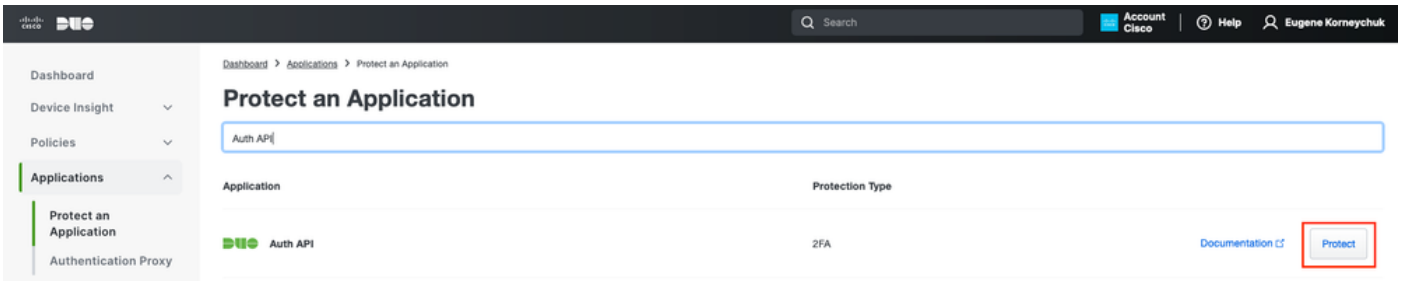
8. Access-Accept wordt naar het netwerkapparaat verzonden, VPN-verbinding wordt tot stand gebracht

Configuraties

Selecteer te beschermen toepassingen

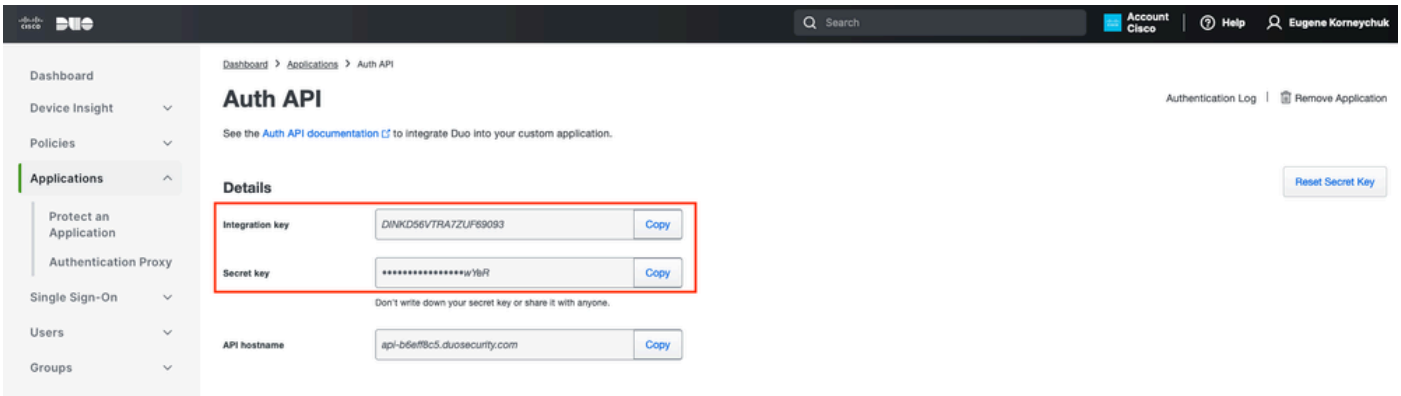
Navigeer naar DUO Admin Dashboard https://admin.duosecurity.com/login. Aanmelden met beheerdersreferenties.

Navigeer naar Dashboard > Toepassingen > Bescherm een toepassing. Zoek naar Auth API en selecteer Protect.



Autorisatie API 1

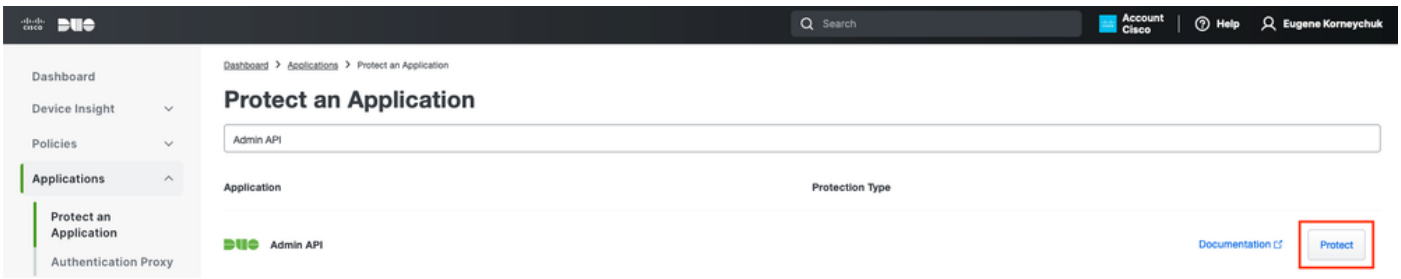
Noteer de integratiesleutel en de geheime sleutel.



Autorisatie API 2

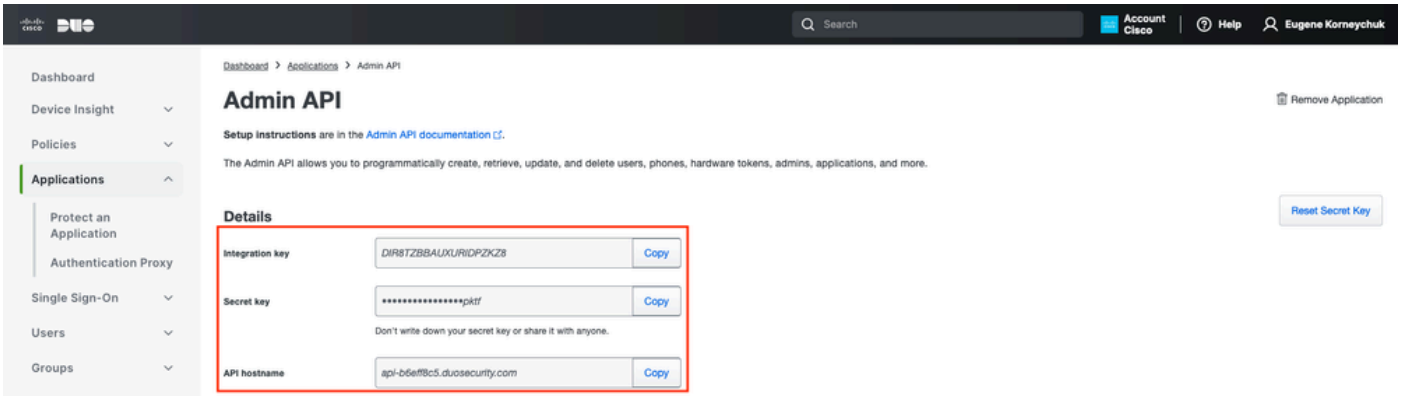
Navigeer naar Dashboard > Toepassingen > Bescherm een toepassing. Zoek Admin API en selecteer Protect.

Opmerking: alleen beheerders met de rol Eigenaar kunnen een Admin API-toepassing maken of wijzigen in het Duo Admin Panel.



Autorisatie API 1

Noteer de integratiesleutel en geheime sleutel en API-hostnaam.

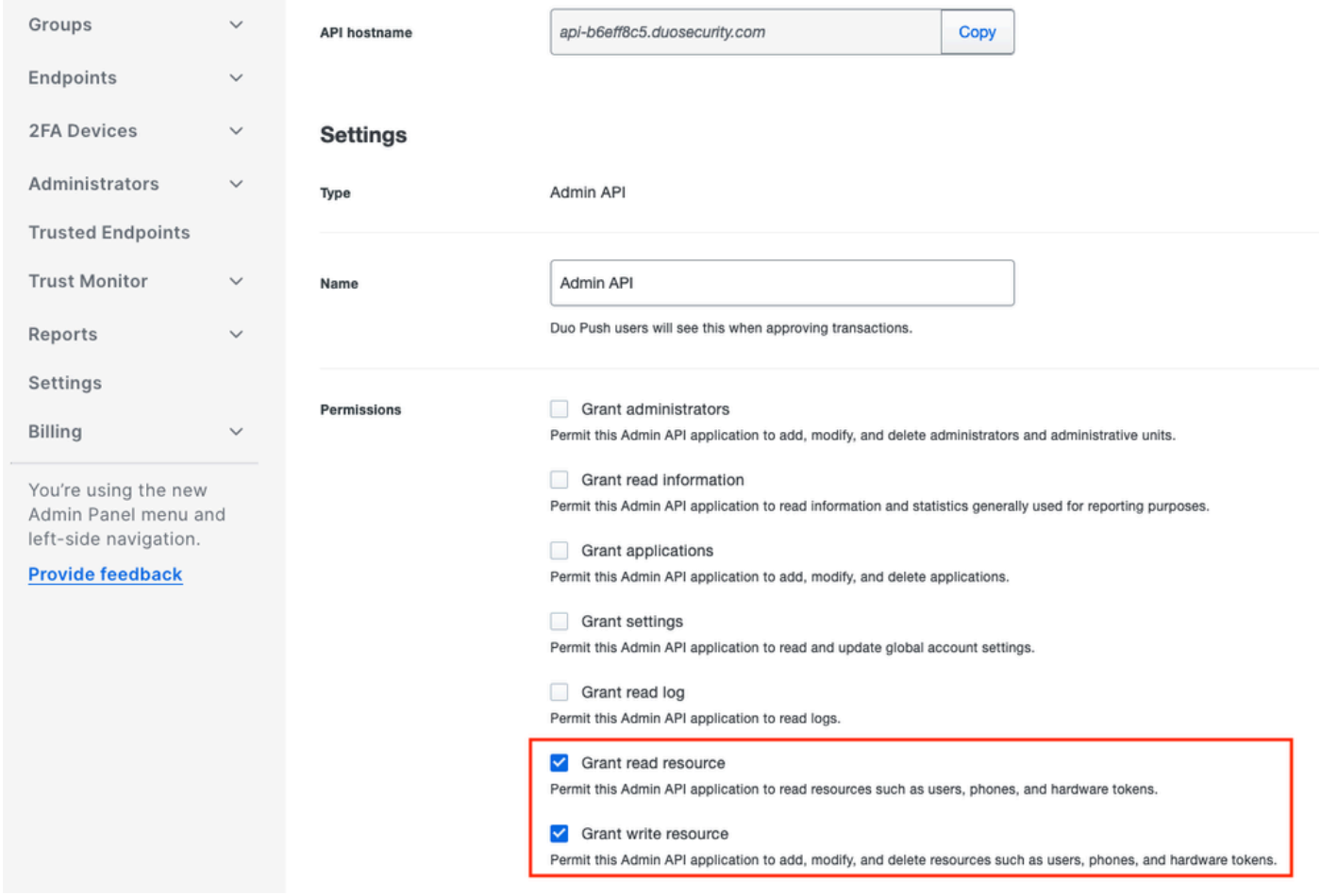


Admin API 2

API-toegangsrechten configureren

Navigeer naar Dashboard > Toepassingen > Toepassing. Selecteer Beheerder-API.

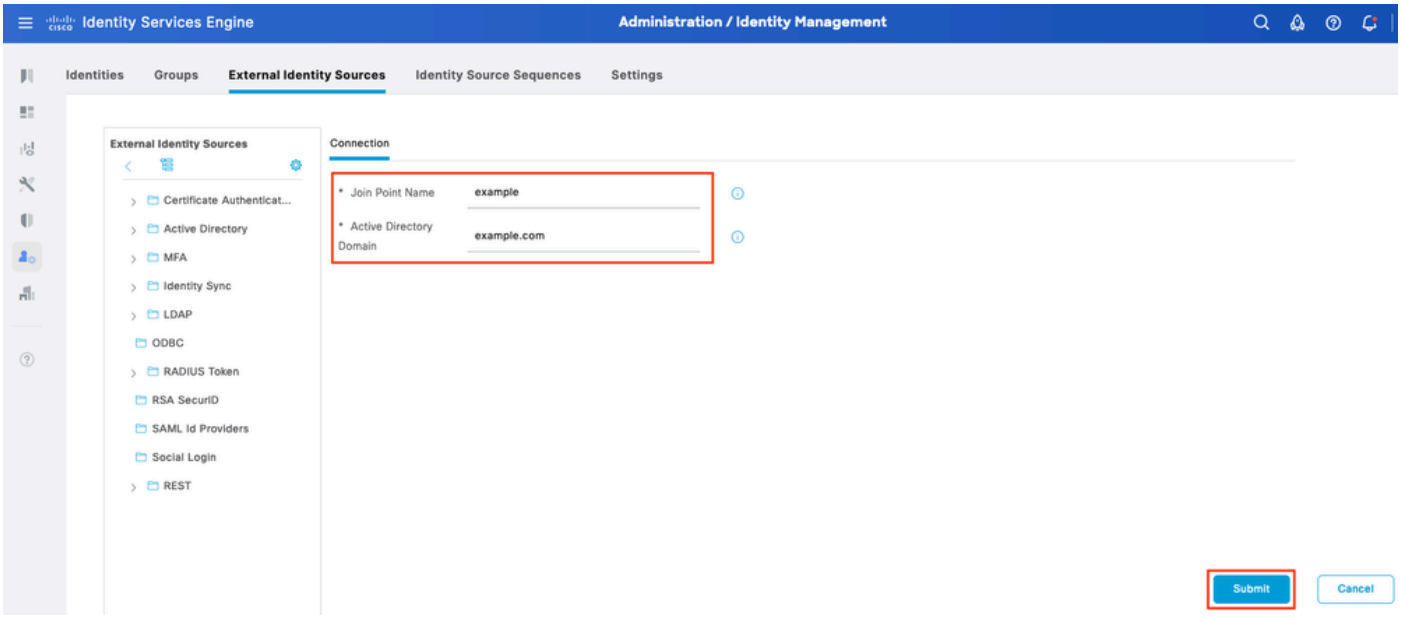
Controleer de toegang tot lees- en schrijfresourcemodules. Klik op Wijzigingen opslaan.



Admin API 3

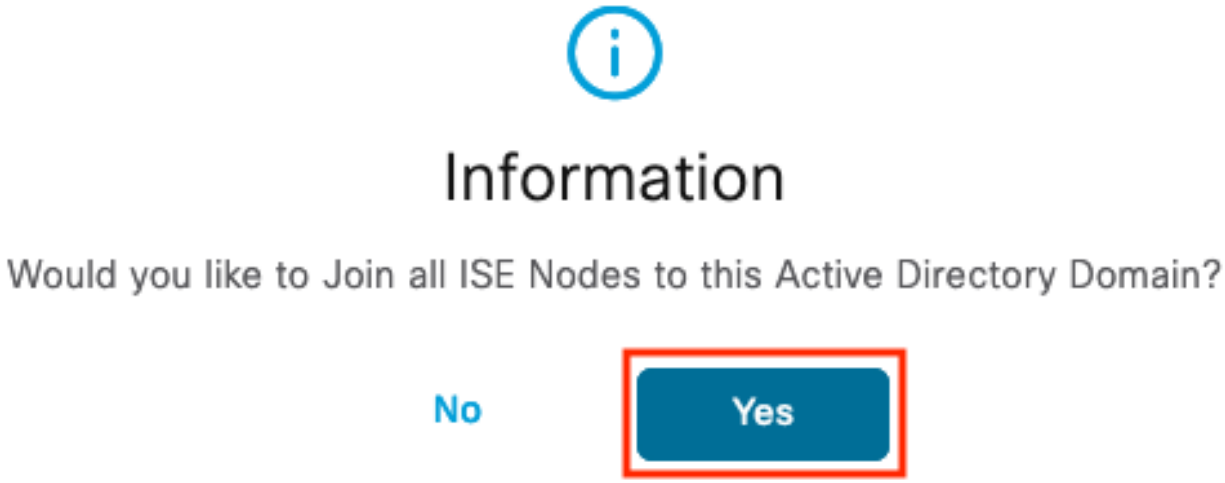
Integreer ISE met Active Directory

1. Ga naar Beheer > Identiteitsbeheer > Externe identiteitsopslag > Active Directory > Toevoegen. Geef de Join Point Name, Active Directory Domain en klik op Indienen.



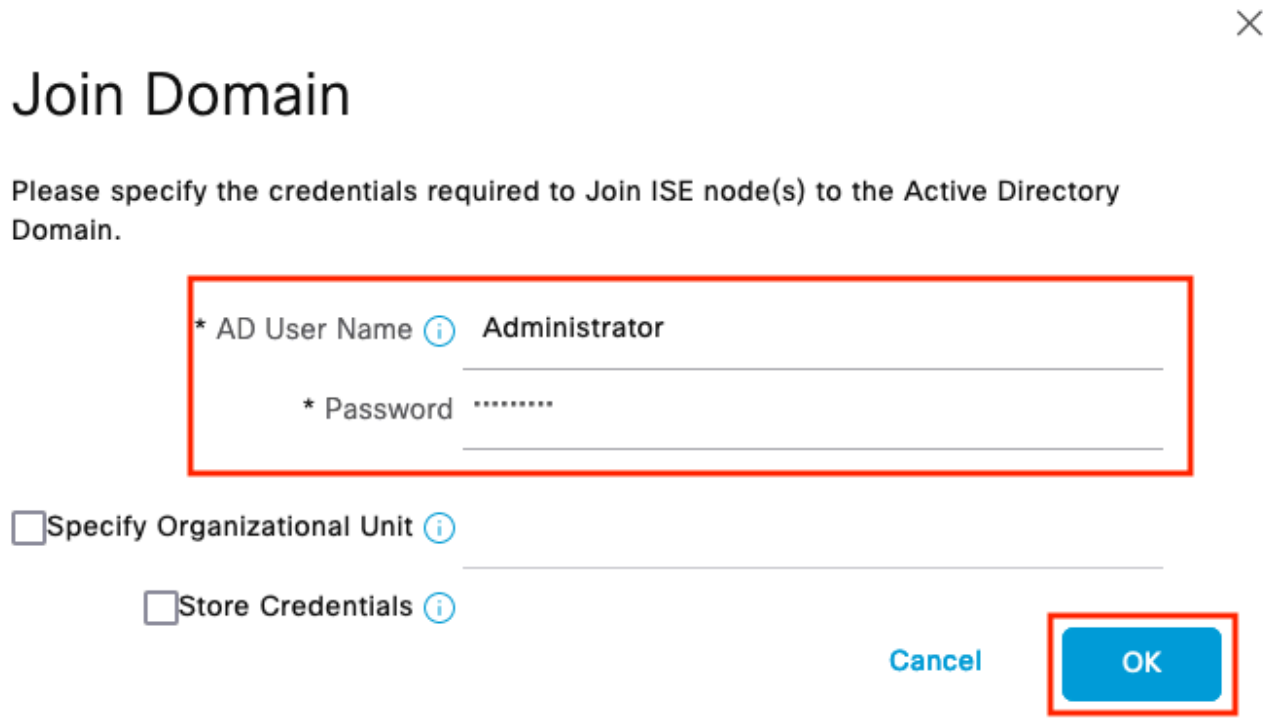
Active Directory 1

2. Klik op Ja wanneer u wordt gevraagd om toe te treden tot alle ISE-knooppunten in dit Active Directory-domein.



Active Directory 2

3. Typ AD Gebruikersnaam en wachtwoord en klik op OK.



Active Directory 3

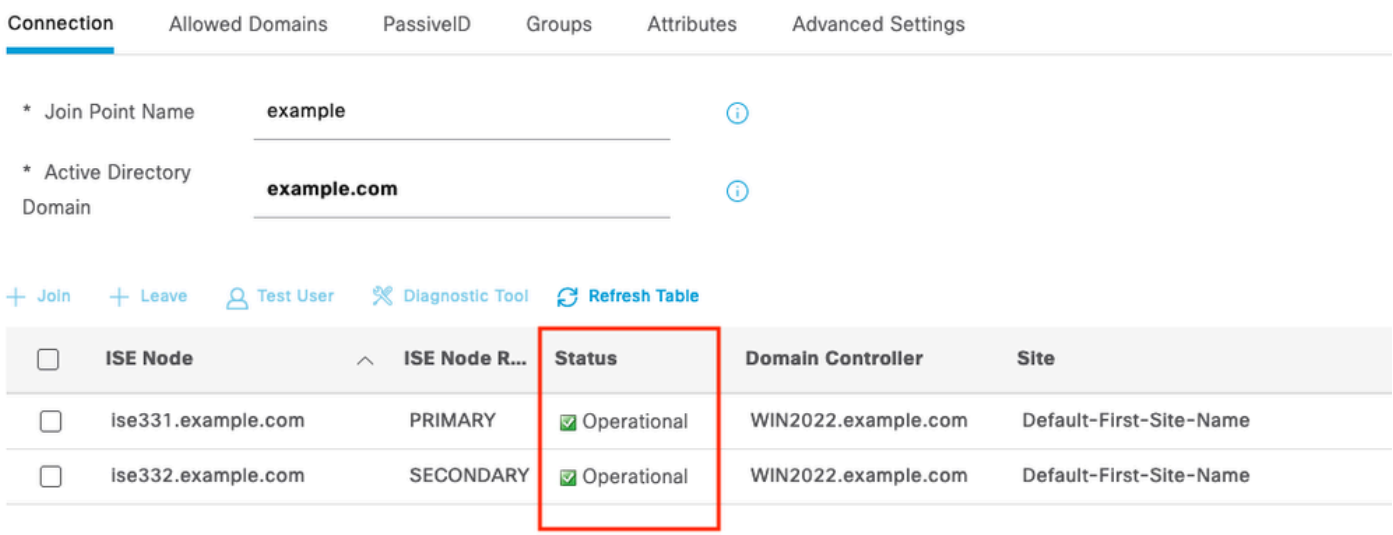
Een AD-account dat vereist is voor domeintoegang in ISE kan een van de volgende waarden hebben:

- Voeg werkstations toe aan domeingebruikersrecht in het betreffende domein
- Computer Objects maken of Computer Objects toestemming verwijderen op de respectievelijke computers container waar de account van de ISE-machine is gemaakt voordat deze zich bij de ISE-machine aansluit.

Opmerking: Cisco raadt aan het uitsluiting-beleid voor de ISE-account uit te schakelen en de AD-infrastructuur te configureren om waarschuwingen naar de beheerder te sturen als er een verkeerd wachtwoord voor die account wordt gebruikt. Wanneer het verkeerde wachtwoord is ingevoerd, maakt of wijzigt ISE de machinerekening niet wanneer dit nodig is en ontkent zij daarom mogelijk alle verificaties.

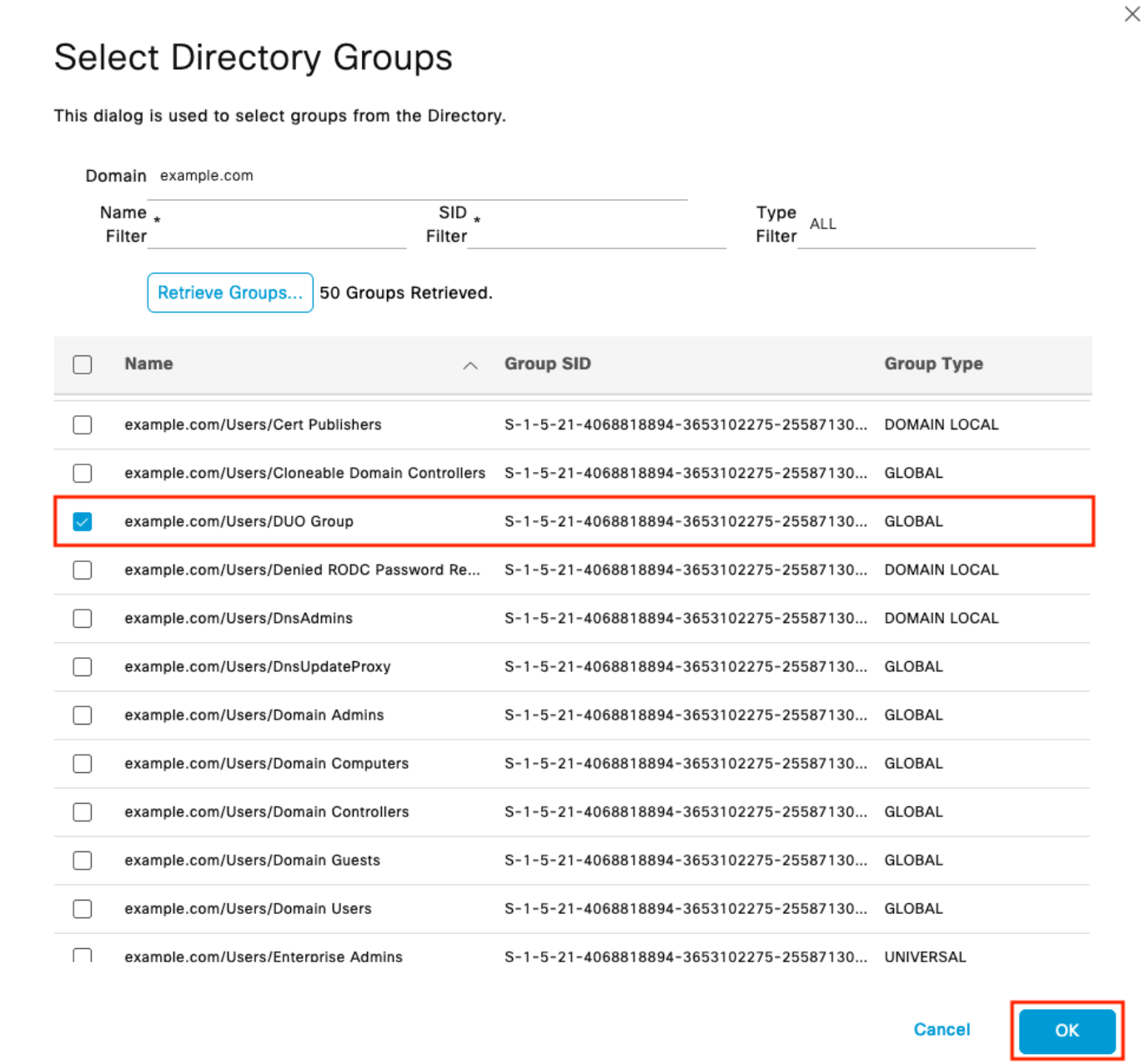
---

4. De AD-status is operationeel.



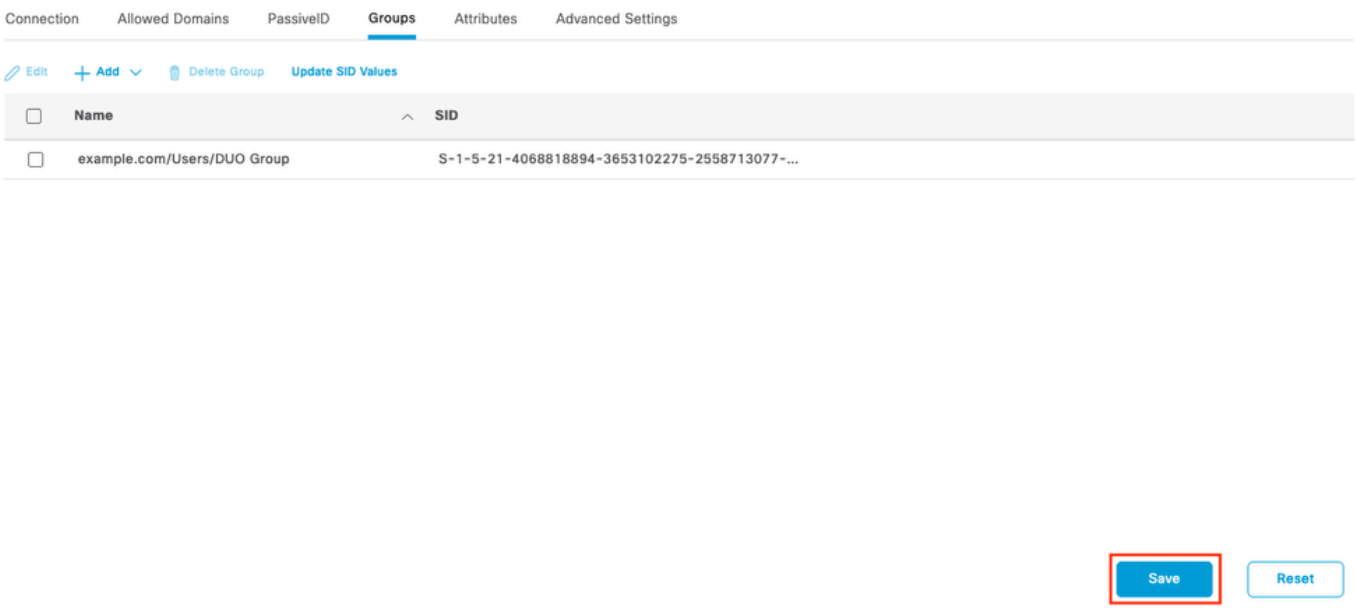
Active Directory 4

5. Navigeer naar Groepen > Toevoegen > Groepen selecteren uit map > Groepen ophalen. Selecteer selectievakjes in AD-groepen naar keuze (die worden gebruikt om gebruikers te synchroniseren en voor autorisatiebeleid), zoals in deze afbeelding.



Active Directory 5

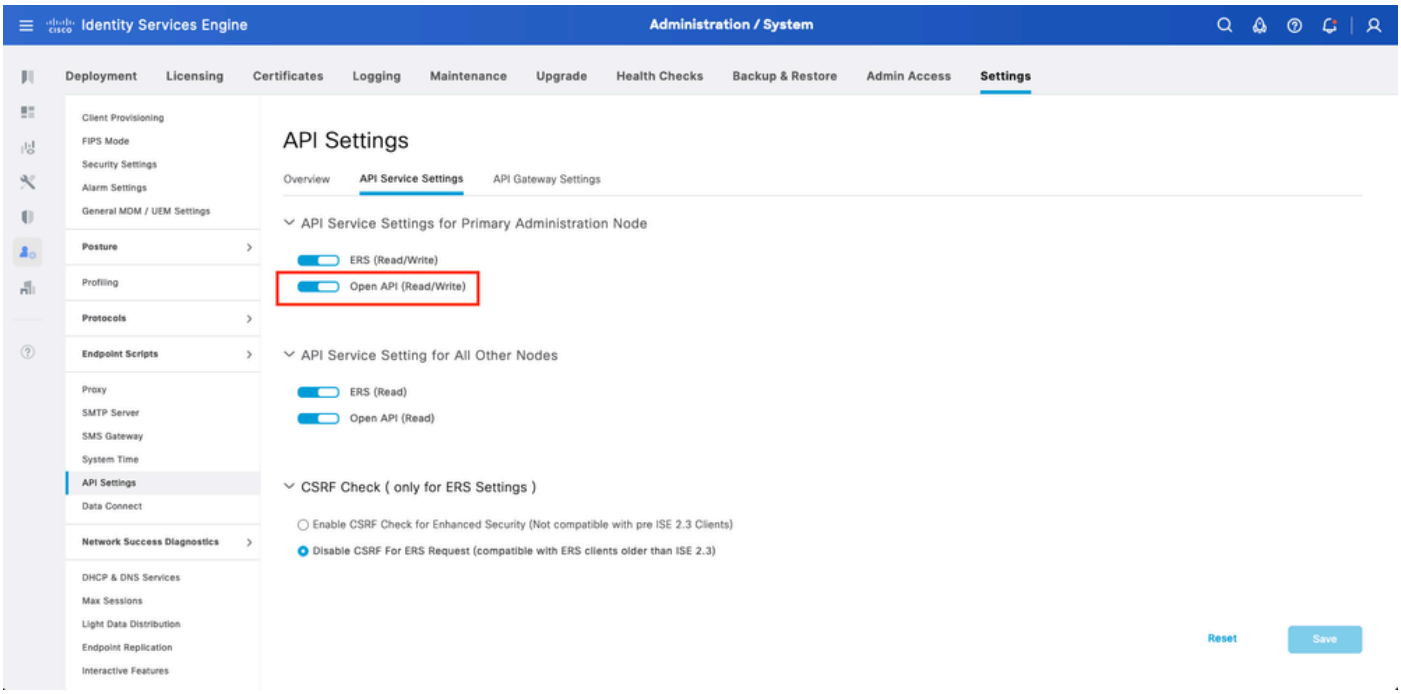
6. Klik op Opslaan om teruggewonnen AD-groepen op te slaan.



Active Directory 6

Open API inschakelen

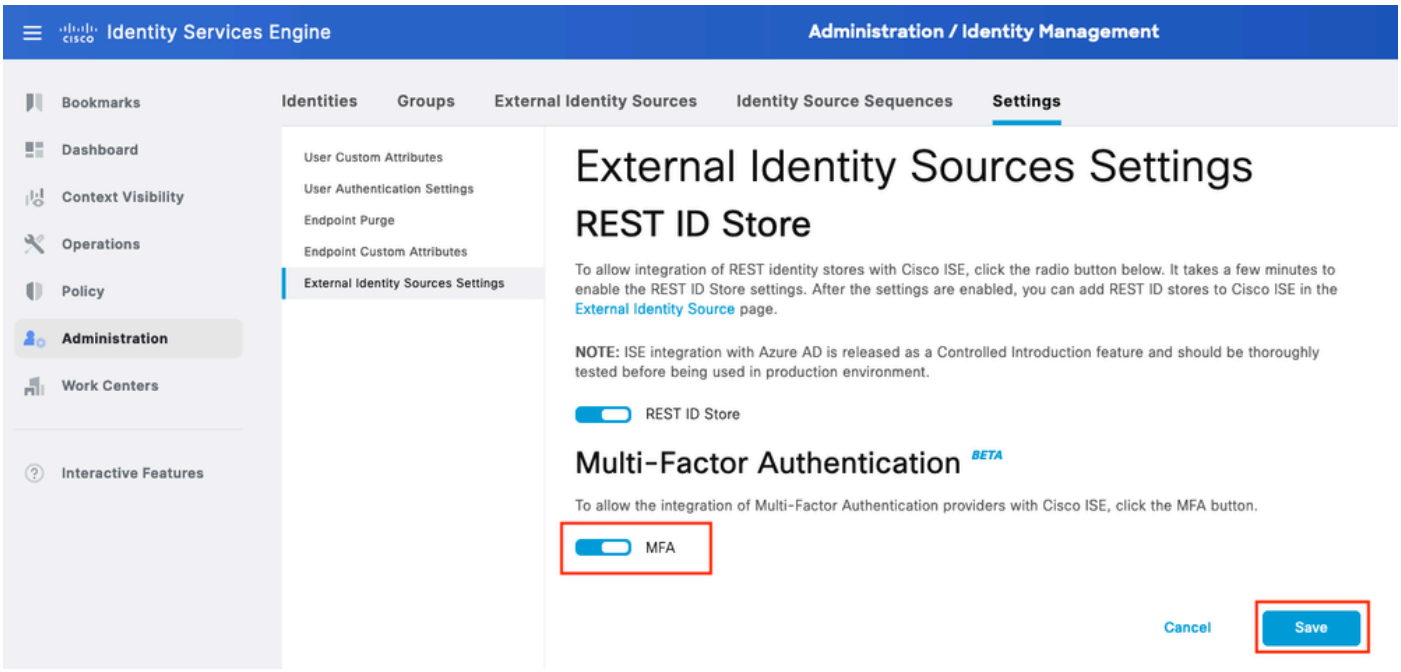
Ga naar Beheer > Systeem > Instellingen > API-instellingen > API-servicesinstellingen. Open API inschakelen en op Opslaan klikken.



Open API

MFA-identiteitsbron inschakelen

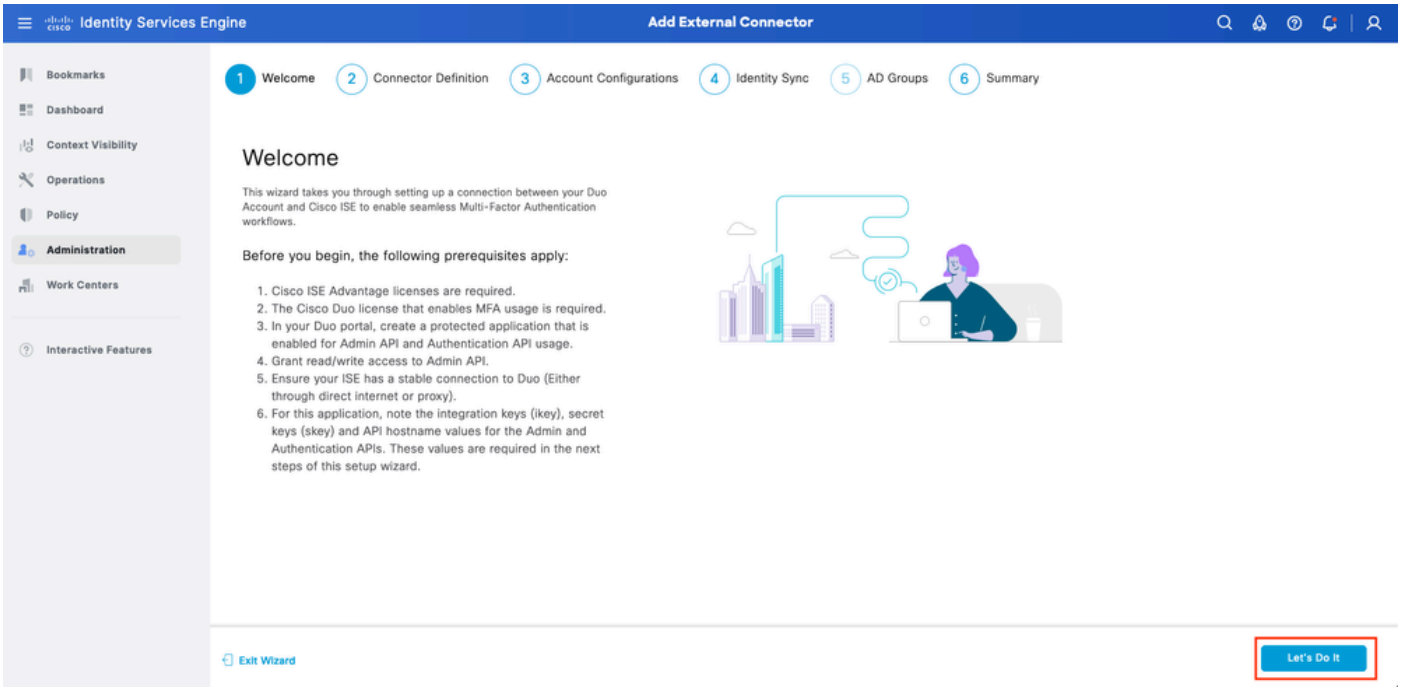
Ga naar Beheer > Identity Management > Instellingen > Externe Identity Source Settings. MFA inschakelen en op Opslaan klikken.



MFB 1

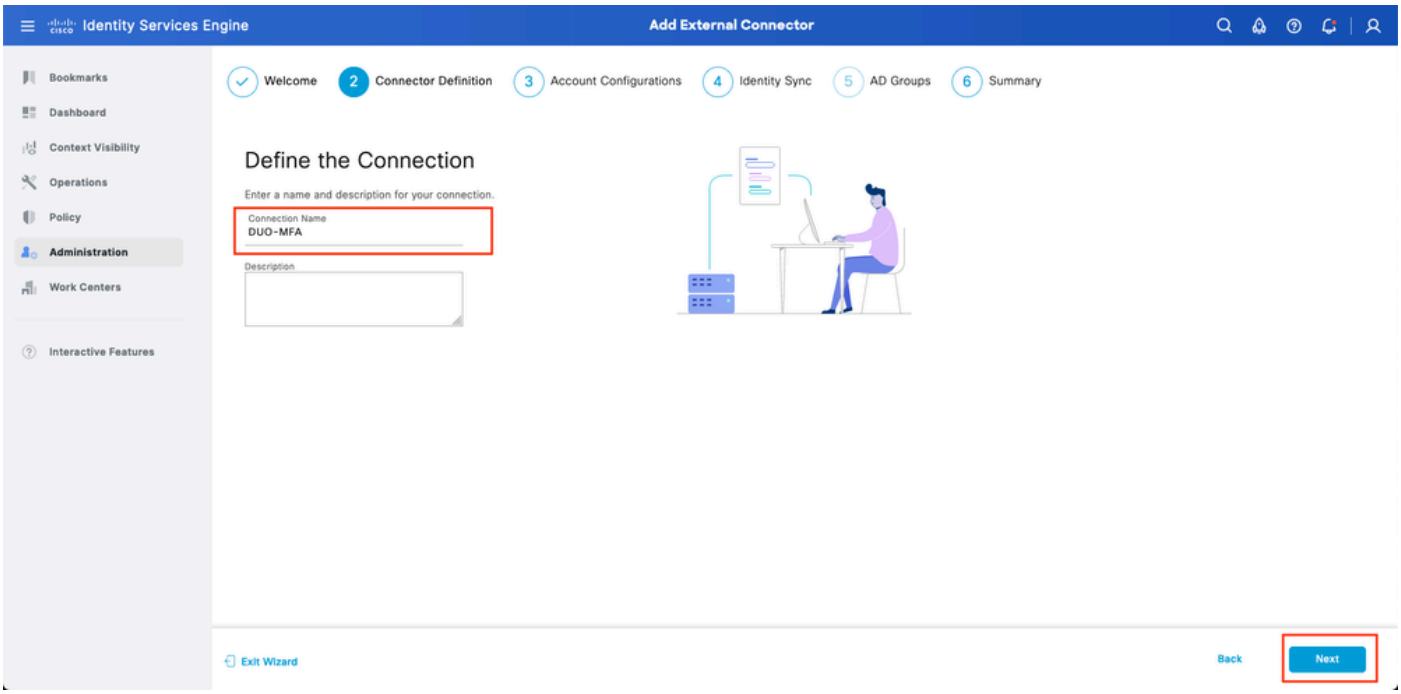
MFA externe identiteitsbron configureren

Ga naar Beheer > Identiteitsbeheer > Externe Identiteitsbronnen. Klik op Toevoegen. Klik op het welkomstscherm op Let's Do It.



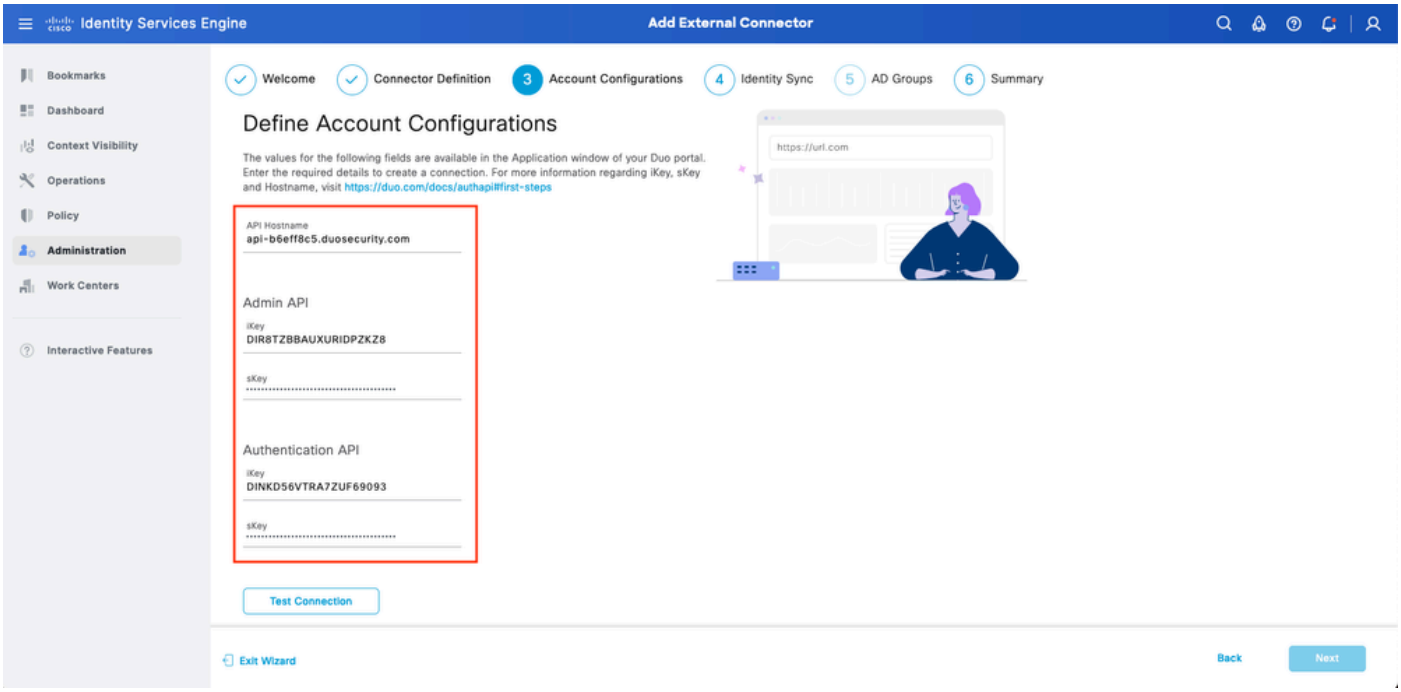
ISE DUO-wizard 1

Configureer in het volgende scherm de verbindingsnaam en klik op Volgende.



ISE DUO-wizard 2

Configureer de waarden van API Hostname, Admin API Integration en Secret Keys, Auth API Integration en Secret Keys van Select Toepassingen om stap te beschermen.



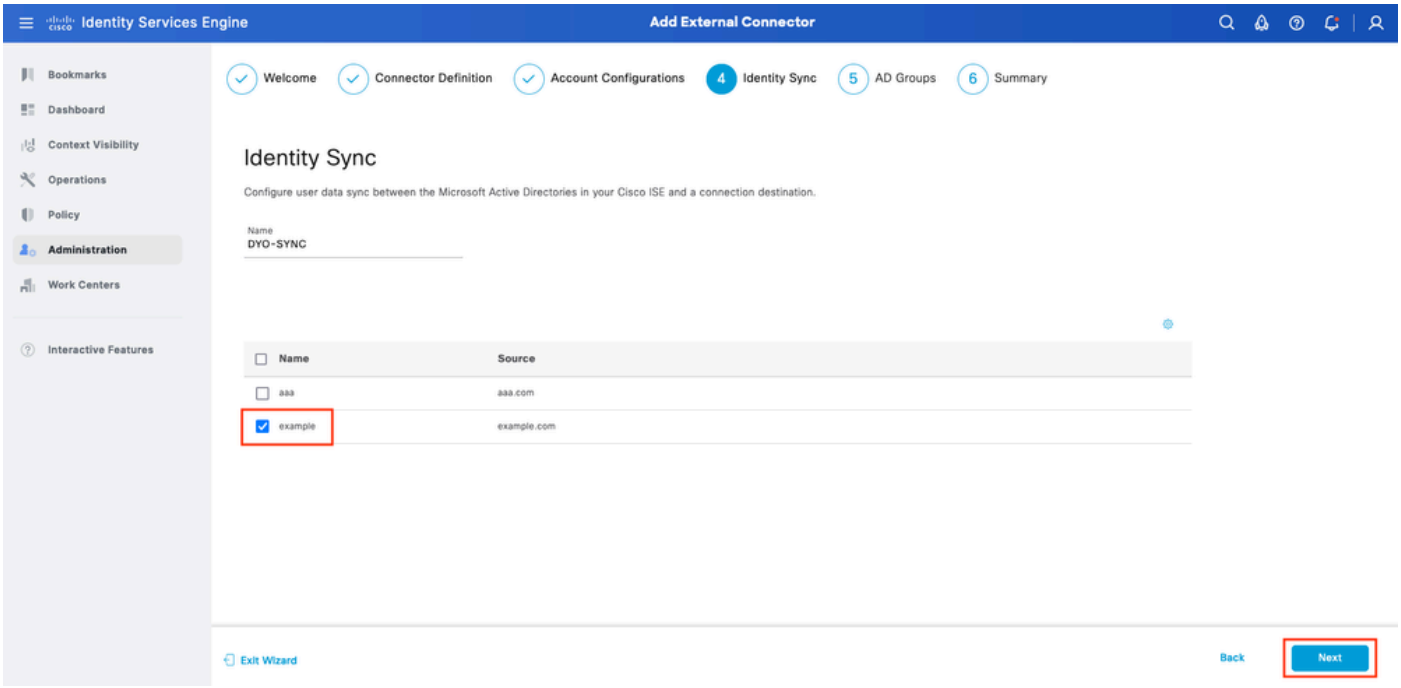
ISE DUO-wizard 3

Klik op Verbinding testen. Als de Test Connection succesvol is, kunt u op Volgende klikken.

ISE DUO-wizard 4

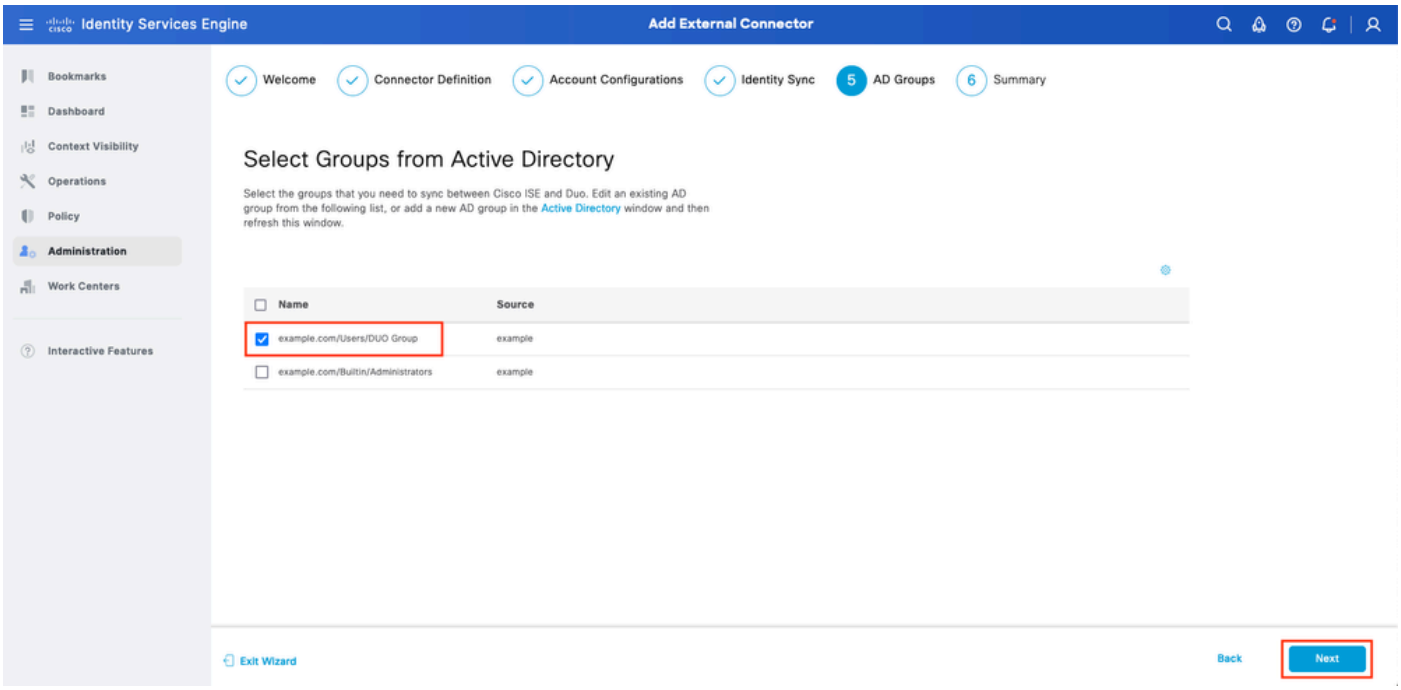
Configureer Identity Sync. Dit proces synchroniseert gebruikers van de Active Directory-groepen die u in DUO-account selecteert met behulp van API-referenties die eerder worden verstrekt. Selecteer Active Directory Join Point. Klik op Volgende.

Opmerking: de configuratie van de actieve map valt buiten het bereik van het document. Volg dit document om ISE in de actieve map te integreren.



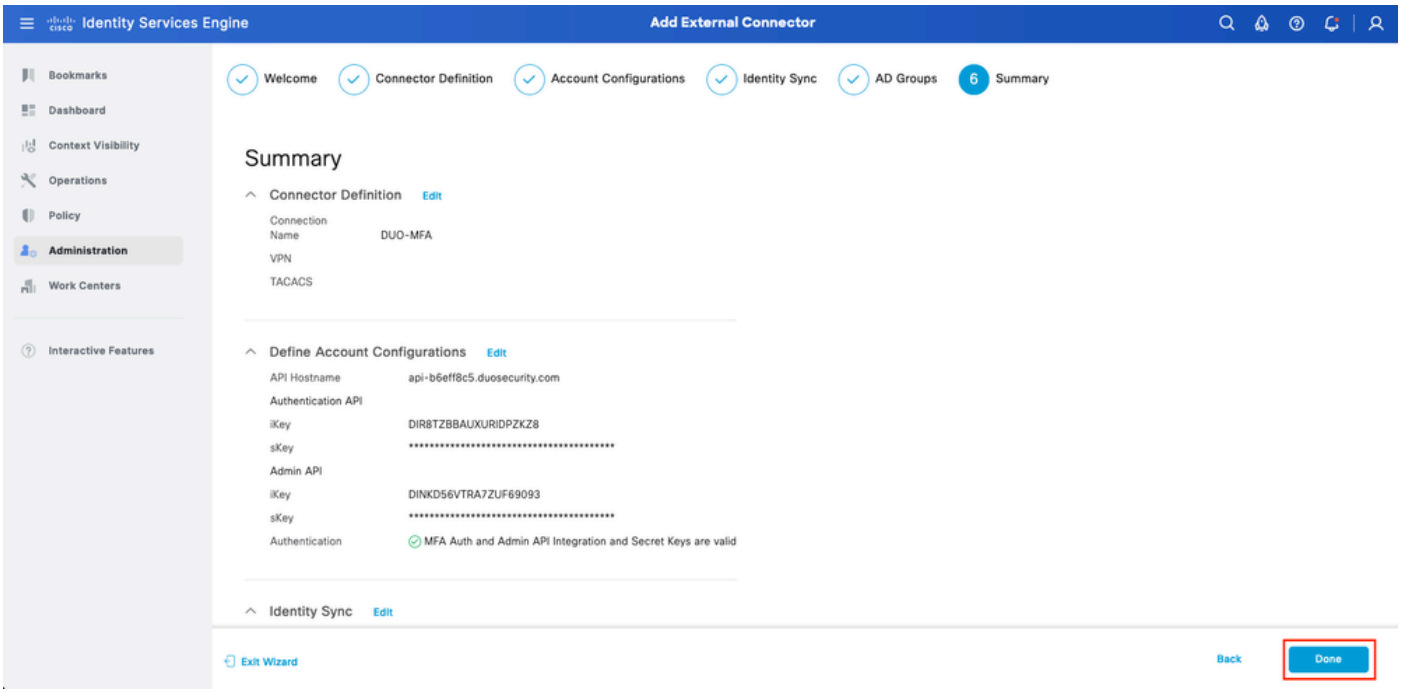
ISE DUO-wizard 5

Selecteer Active Directory-groepen waaruit u wilt dat gebruikers worden gesynchroniseerd met DUO. Klik op Volgende.



ISE DUO-wizard 6

Controleer of de instellingen correct zijn en klik op Gereed.

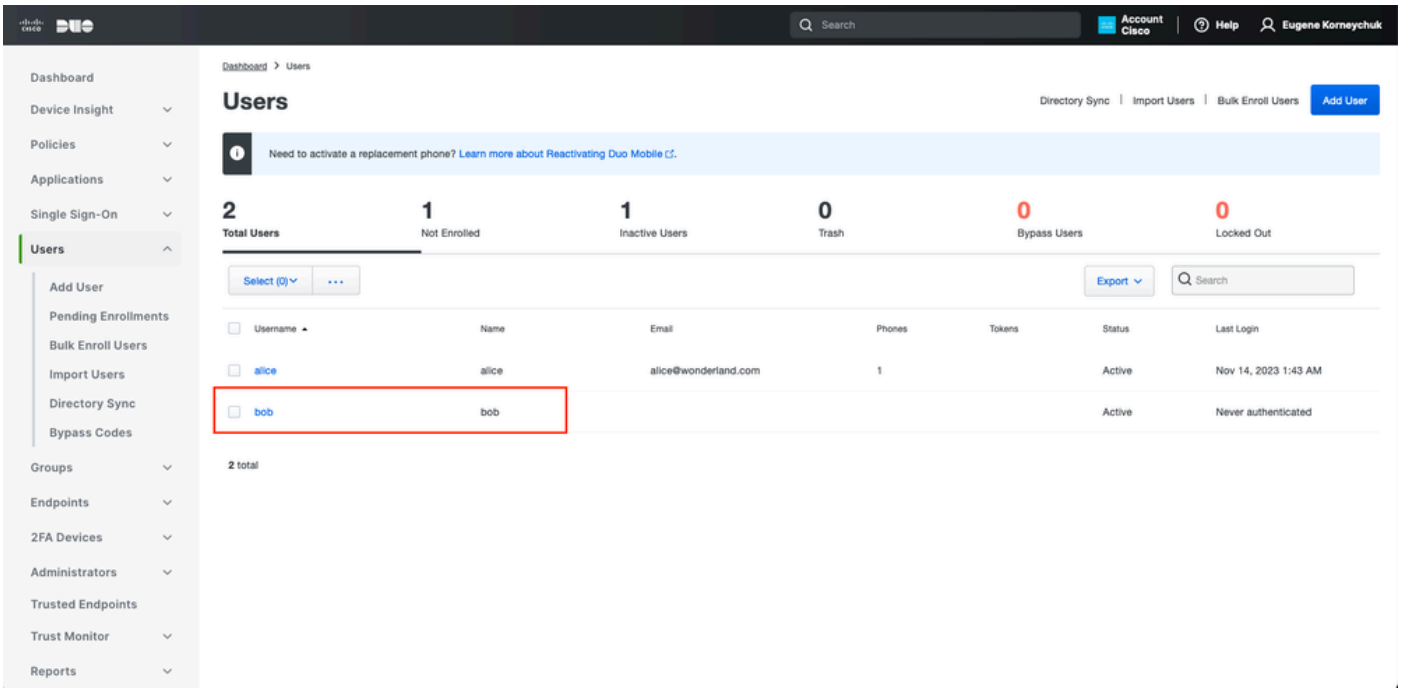


ISE DUO-wizard 7

Gebruiker inschrijven in DUO

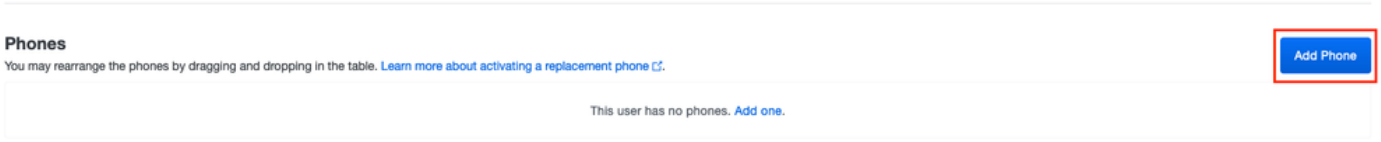
Opmerking: DUO User Enrollment valt buiten het bereik van het document, overweeg dit document om meer te weten te komen over het inschrijven van de gebruikers. Voor dit document wordt handmatige inschrijving door de gebruiker gebruikt.

Open het Dashboard van DUO Admin. Navigeer naar Dashboard > Gebruikers. Klik op de gebruiker die van ISE gesynchroniseerd is.



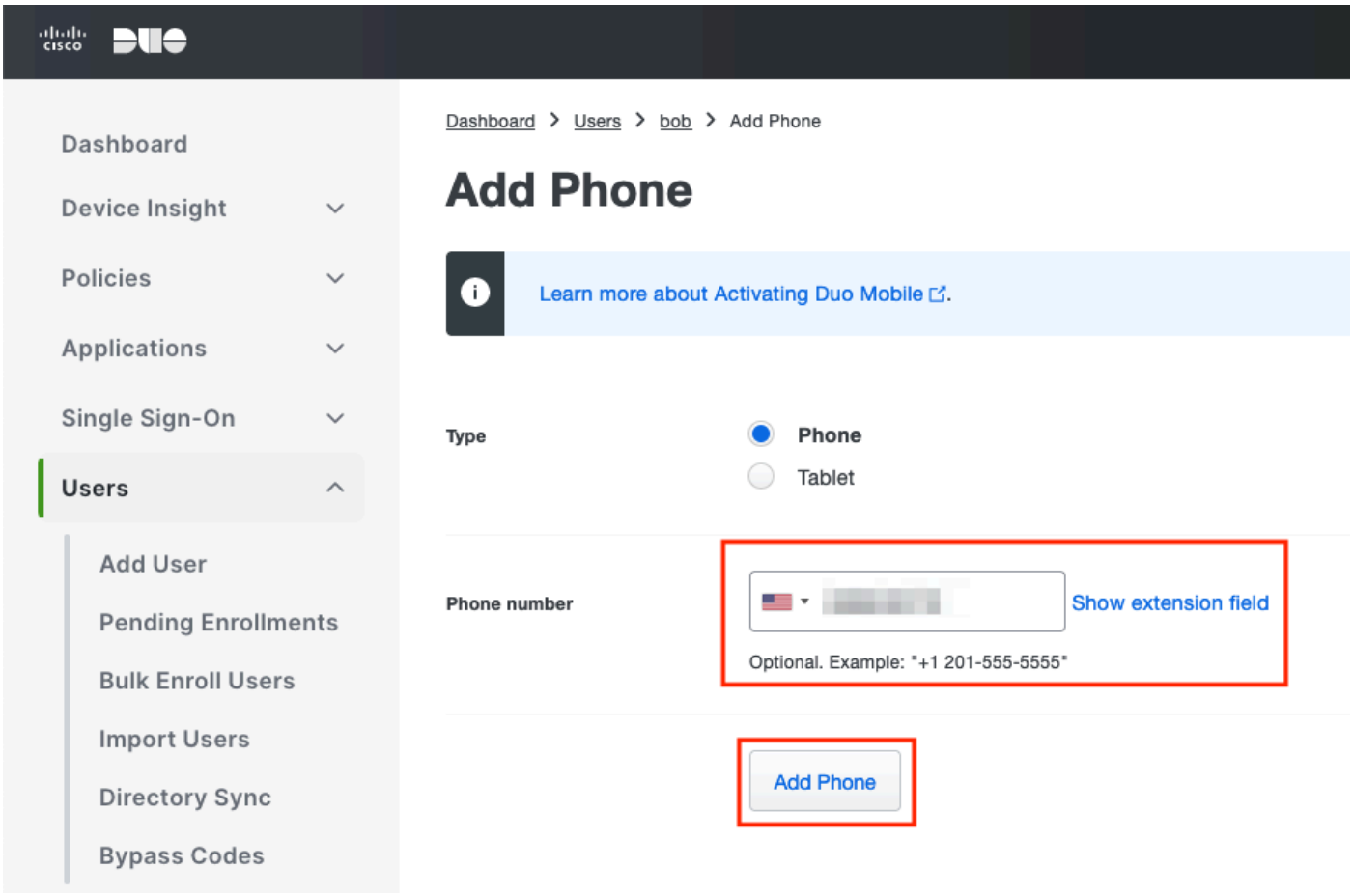
DUO-inschrijving 1

Scroll naar beneden naar de telefoons. Klik op Telefoon toevoegen.



DUO-inschrijving 2

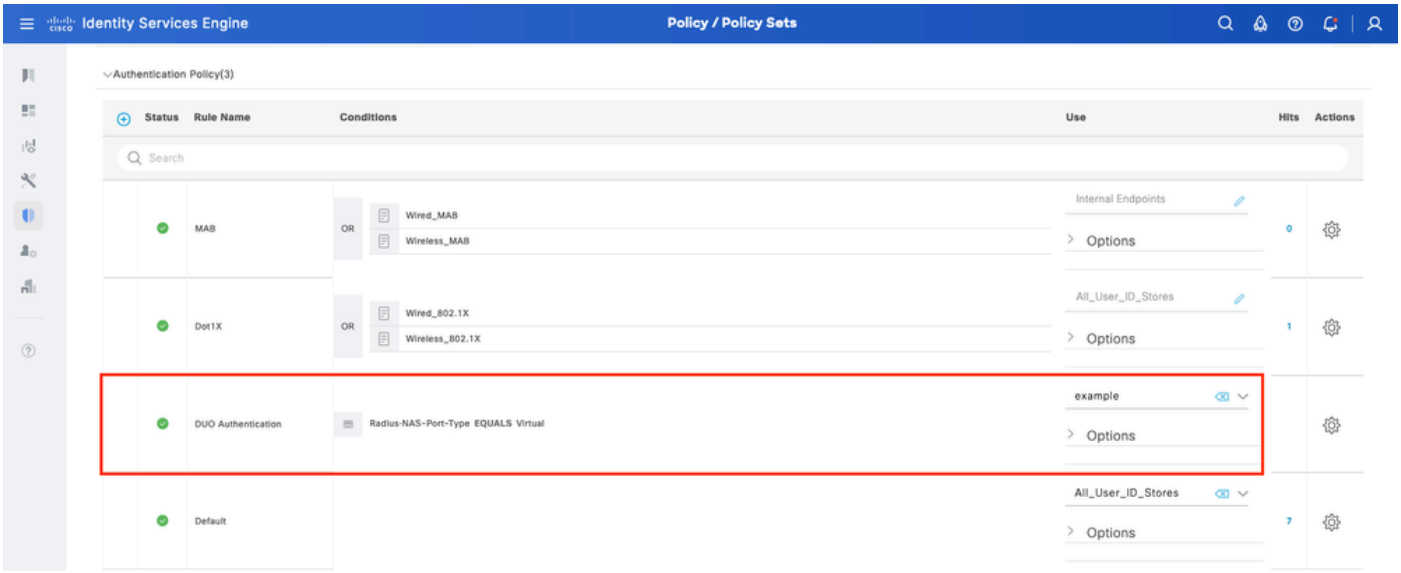
Voer het telefoonnummer in en klik op Telefoon toevoegen.



Beleidssets configureren

1. Verificatiebeleid configureren

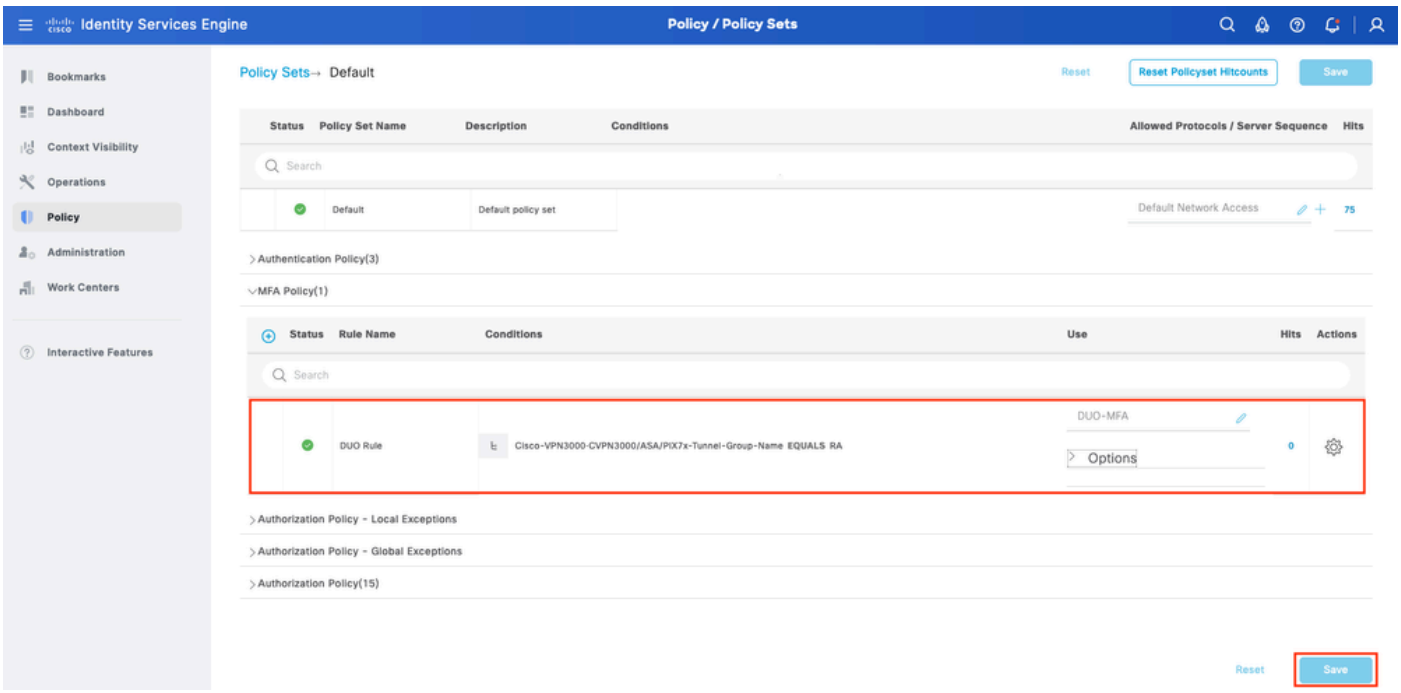
Ga naar Policy > Policy Set. Selecteer de Beleidsset waarvoor u MFB wilt inschakelen. Configureer het verificatiebeleid met Primaire verificatie Identity Store als actieve map.



Beleidsset 1

2. MFB-beleid configureren

Zodra MFA is ingeschakeld op ISE, is er een nieuwe sectie in ISE Policy Sets beschikbaar. Breid MFB-beleid uit en klik op + om MFB-beleid toe te voegen. Configureer de voorwaarden van uw keuze en selecteer DUO-MFA die eerder in de sectie Gebruik is geconfigureerd. Klik op Opslaan.

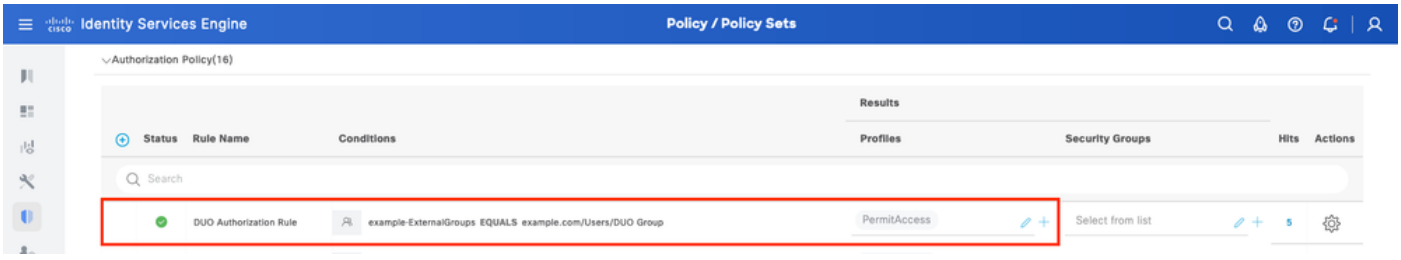


ISE-beleid

Opmerking: het beleid dat hierboven is geconfigureerd, is gebaseerd op de Tunnel-groep Named RA. Gebruikers verbonden met RA tunnelgroep worden gedwongen om MFA uit te voeren. ASA/FTD-configuratie valt buiten het bereik van dit document. Gebruik dit document om ASA/FTD te configureren

3. Vergunningsbeleid configureren

Configureer het autorisatiebeleid met de voorwaarde en rechten van de Active Directory-groep van uw keuze.



Beleidsset 3

Beperkingen

Bij het schrijven van dit document:

1. Alleen DUO-push en -telefoon worden ondersteund als een tweede-factor-verificatiemethode

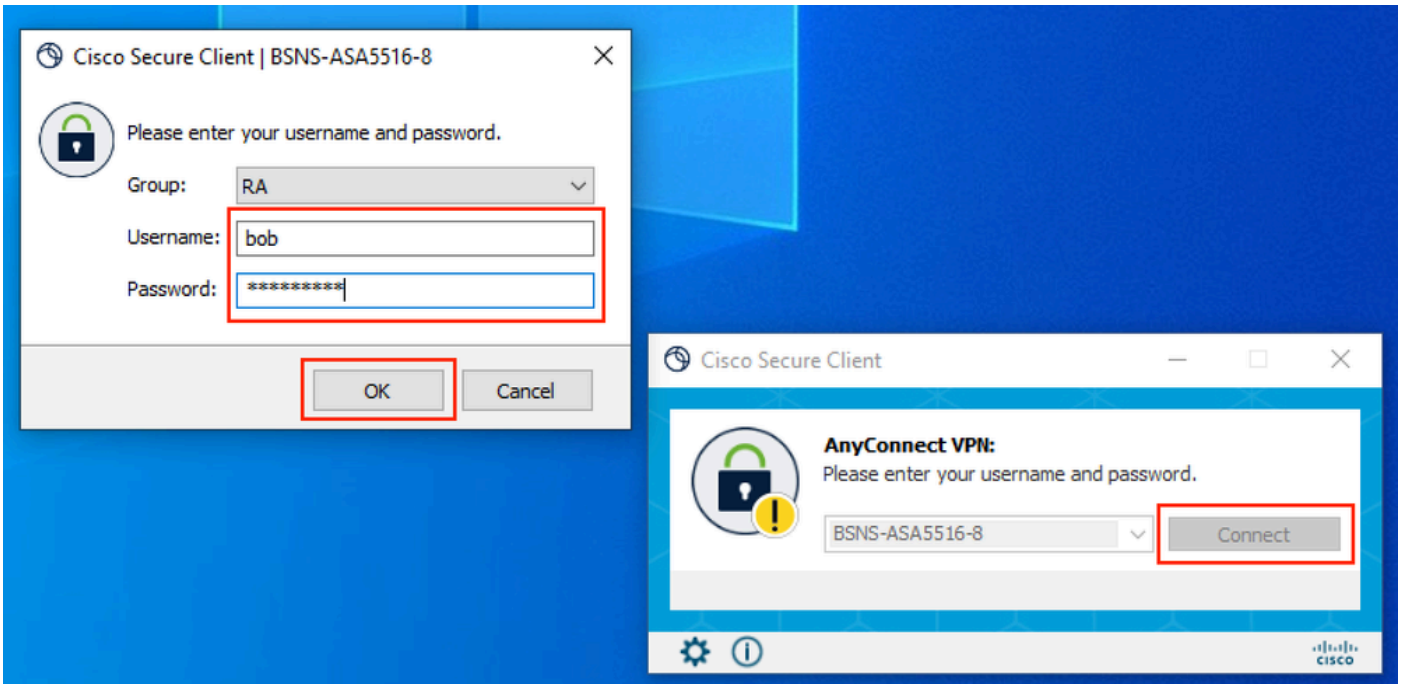
2. Er worden geen groepen naar DUO Cloud gedrukt, alleen gebruikerssync wordt ondersteund

3. Alleen de volgende gebruikscases voor multifactorverificatie worden ondersteund:

- VPN-gebruikersverificatie
- Verificatie van TACACS+ beheertoegang

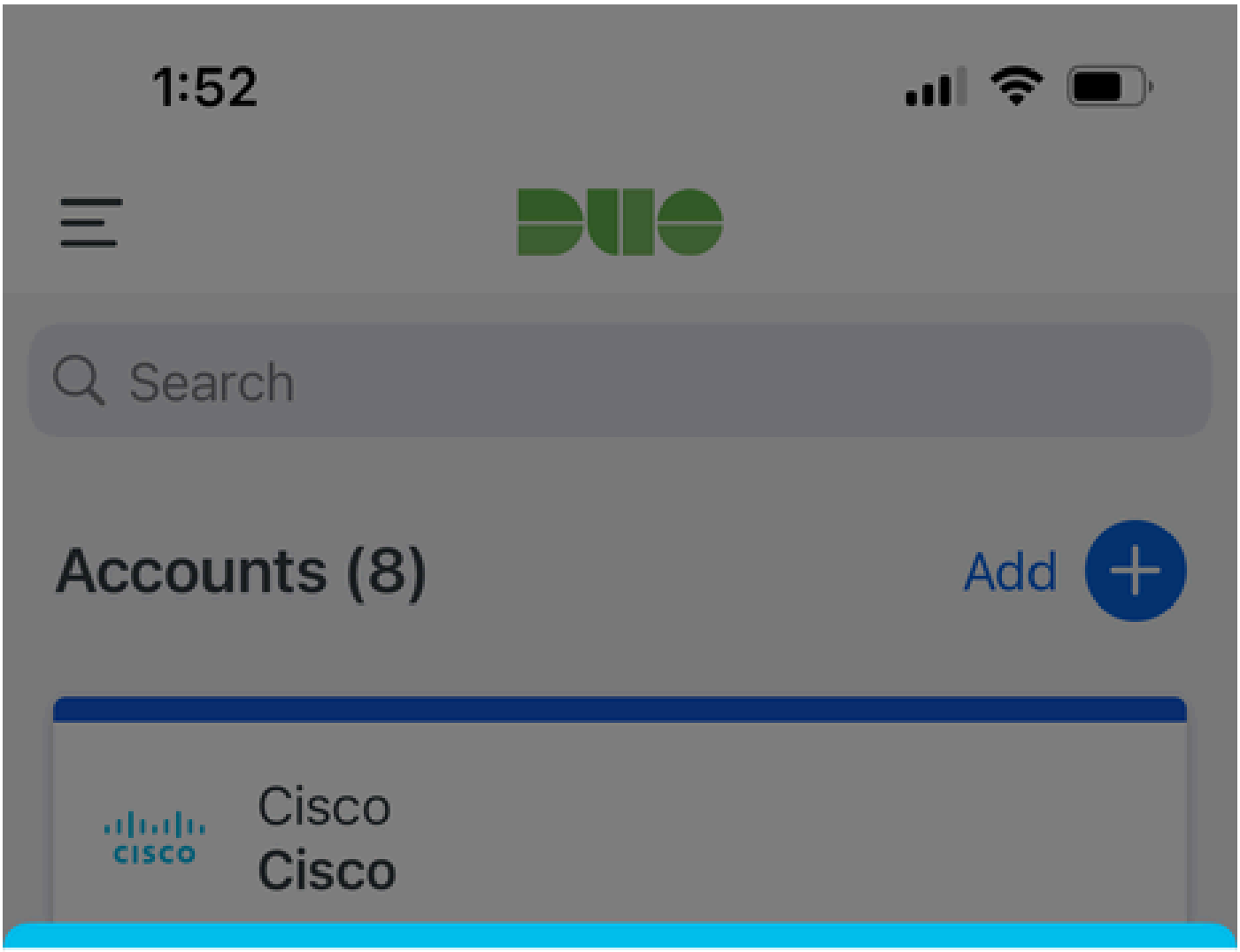
Verifiëren

Open Cisco Secure-client en klik op Connect. Gebruikersnaam en wachtwoord opgeven en op OK klikken.



VPN-client

Gebruikers mobiele apparaat moeten een DUO Push Notification ontvangen. Goedkeuren. VPN-verbinding is tot stand gebracht.



Are you logging in to **Auth API**?

Cisco

1:52 PM

bob

MFA gerelateerde logbestanden	beleidsinstrument	ise-psc.log	DuoMfaAuthApiUtils -::::- Ingezonden aanvraag b Duo Client Manager DuoMaxAuthAputils —> Duo-respons
Beleidsgerelateerde logbestanden	prt-JNI	prt-management.log	Radius MFbeleidsaanvraagprocessor Tacacs MFA-beleidsaanvraagprocessor
Met verificatie verband houdende logbestanden	runtime-AAA	prtserver.log	MFAuthenticator:onAuthenticateEvent MFAuthenticator:sendAuthenticateEvent MFAuthenticator::onResponseEvaluatePolicyEve
DUO-verificatie, ID-synchronisatie-logbestanden		duo-sync-service.log	

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.