

Configureer ISE 3.3 Native multi-factor verificatie met DUO

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Stroomdiagram](#)

[Configuraties](#)

[Selecteer te beschermen toepassingen](#)

[Integreer ISE met Active Directory](#)

[Open API inschakelen](#)

[MFA-identiteitsbron inschakelen](#)

[MFA externe identiteitsbron configureren](#)

[Gebruiker inschrijven in DUO](#)

[Beleidssets configureren](#)

[Beperkingen](#)

[Verifiëren](#)

[Problemen oplossen](#)

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

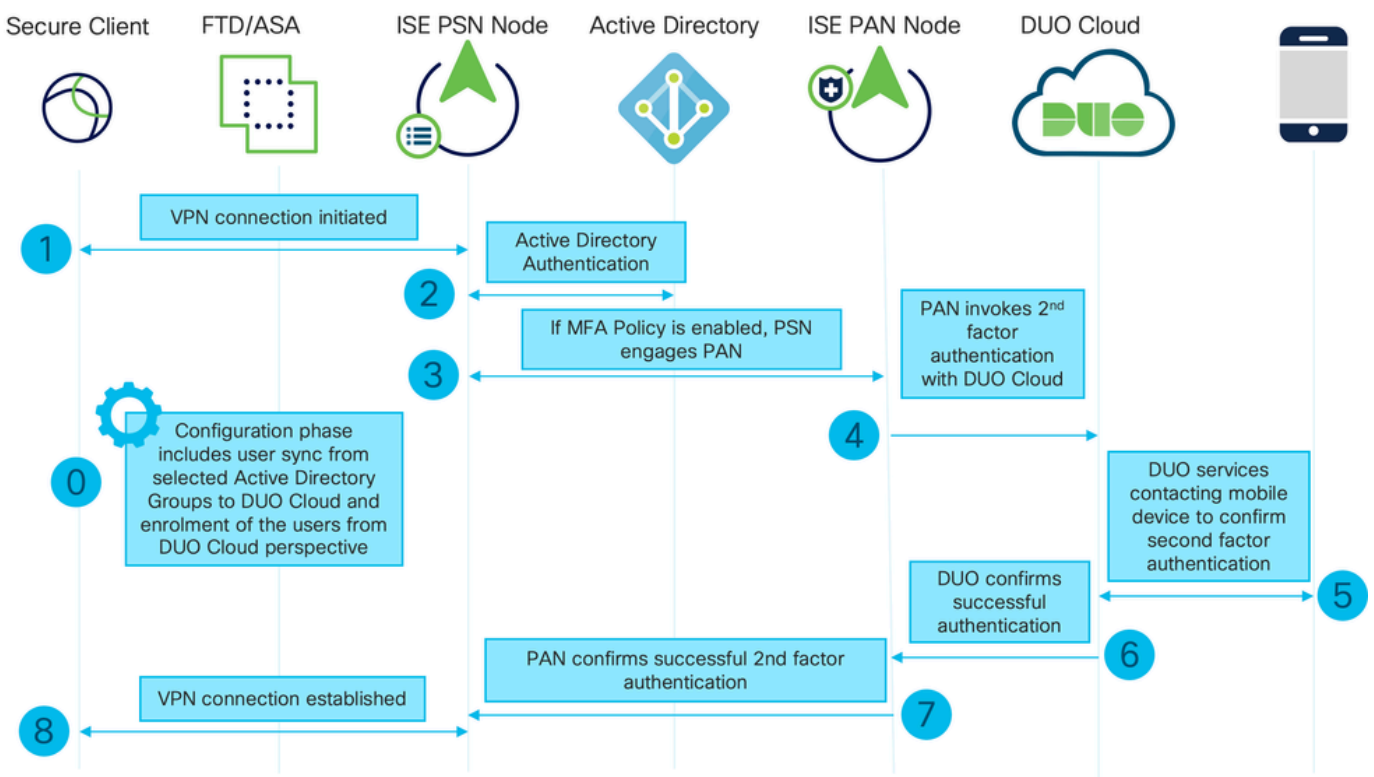
De informatie in dit document is gebaseerd op:

- 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-toegangs aanvraag naar PSN

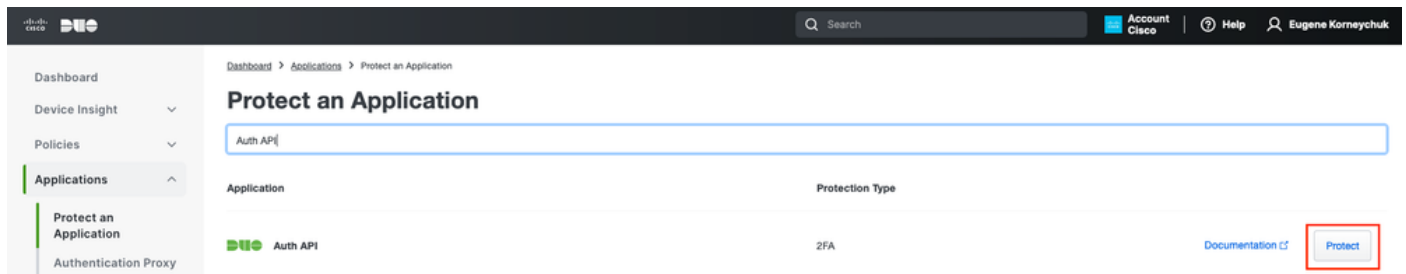
2. PSN-knooppunt verifieert de gebruiker via Active Directory
3. Wanneer de verificatie slaagt en het MFB-beleid is geconfigureerd, neemt PSN PAN aan om contact op te nemen met DUO Cloud
4. Een oproep naar DUO Cloud met Auth API wordt gedaan om een tweede-factor authenticatie met DUO aan te roepen. ISE 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.



Dashboard > Applications > Protect an Application

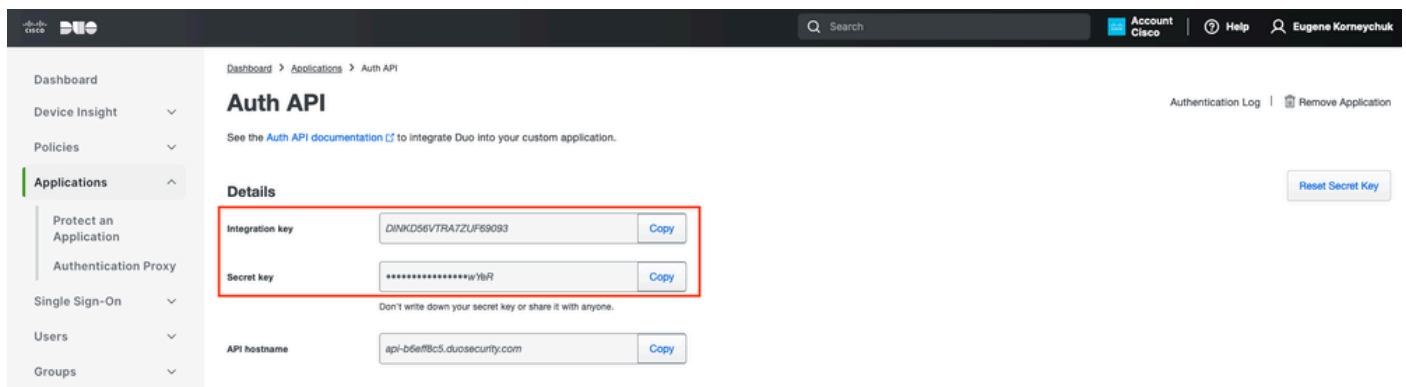
Protect an Application

Auth API

Application	Protection Type	
Auth API	2FA	Documentation ↗ Protect

Autorisatie API 1

Noteer de integratiesleutel en de geheime sleutel.



Dashboard > Applications > Auth API

Auth API

See the [Auth API documentation](#) to integrate Duo into your custom application.

Authentication Log | Remove Application


Reset Secret Key

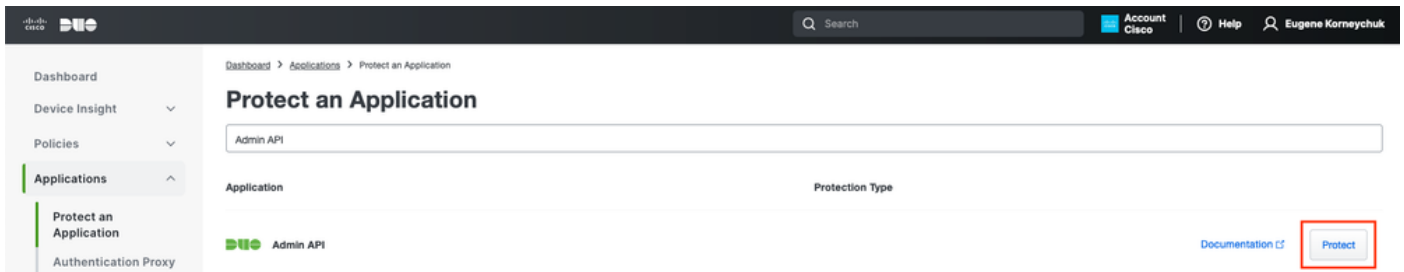
Details

Integration key	DINKD56VTRATZUF89093	Copy
Secret key	*****uY8R	Copy
Don't write down your secret key or share it with anyone.		
API hostname	api-b6e#8c5.duosecurity.com	Copy

Autorisatie API 2

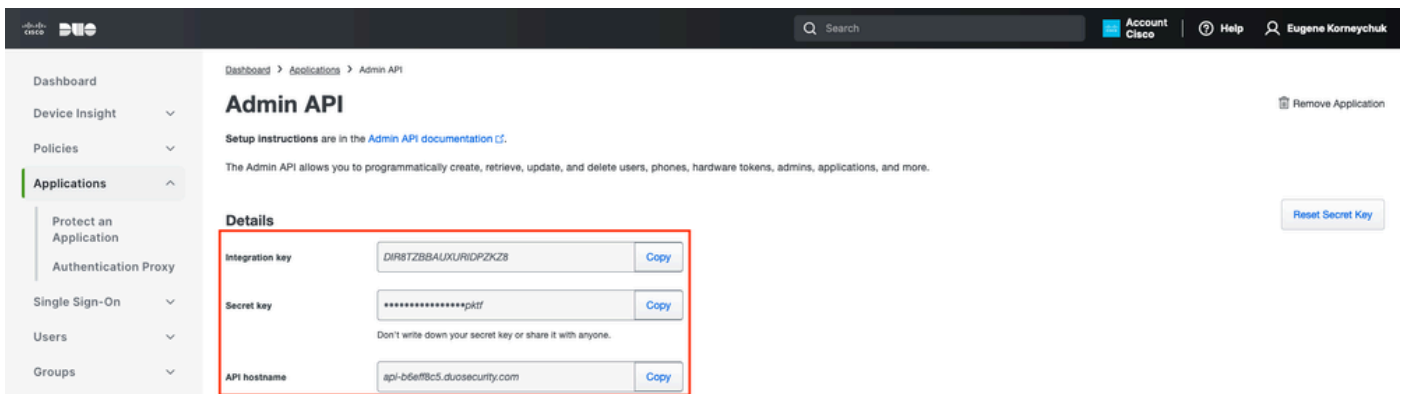
Navigeer naar Dashboard > Toepassingen > Bescherm een toepassing. Zoek Admin API en selecteer Protect.

 **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 schrijfresource modules. Klik op Wijzigingen opslaan.

- 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

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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration / Identity Management > External Identity Sources > Active Directory > Toevoegen. 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'. The 'Submit' button is highlighted with a red box.

Active Directory 1

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



Information

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

No

Yes

Active Directory 2

3. Typ AD Gebruikersnaam en wachtwoord en klik op 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

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.

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. 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.



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

[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

Open API inschakelen

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

The screenshot shows the 'Identity Services Engine Administration / System' interface. The 'Settings' tab is active, and the 'API Settings' section is expanded. Under 'API Service Settings for Primary Administration Node', the 'Open API (Read/Write)' toggle is turned on and highlighted with a red box. Other settings include 'ERS (Read/Write)', 'ERS (Read)', and 'Open API (Read)'. Under 'API Service Setting for All Other Nodes', 'ERS (Read)' and 'Open API (Read)' are also shown. A 'CSRF Check' section is visible at the bottom, with 'Disable CSRF For ERS Request' selected. 'Reset' and 'Save' buttons are at the bottom right.

Open API

MFA-identiteitsbron inschakelen

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

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

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**

MFB 1

MFA externe identiteitsbron configureren

Ga naar Beheer > Identiteitsbeheer > Externe Identiteitsbronnen. Klik op Toevoegen. Klik op het welkomsscherm op 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.

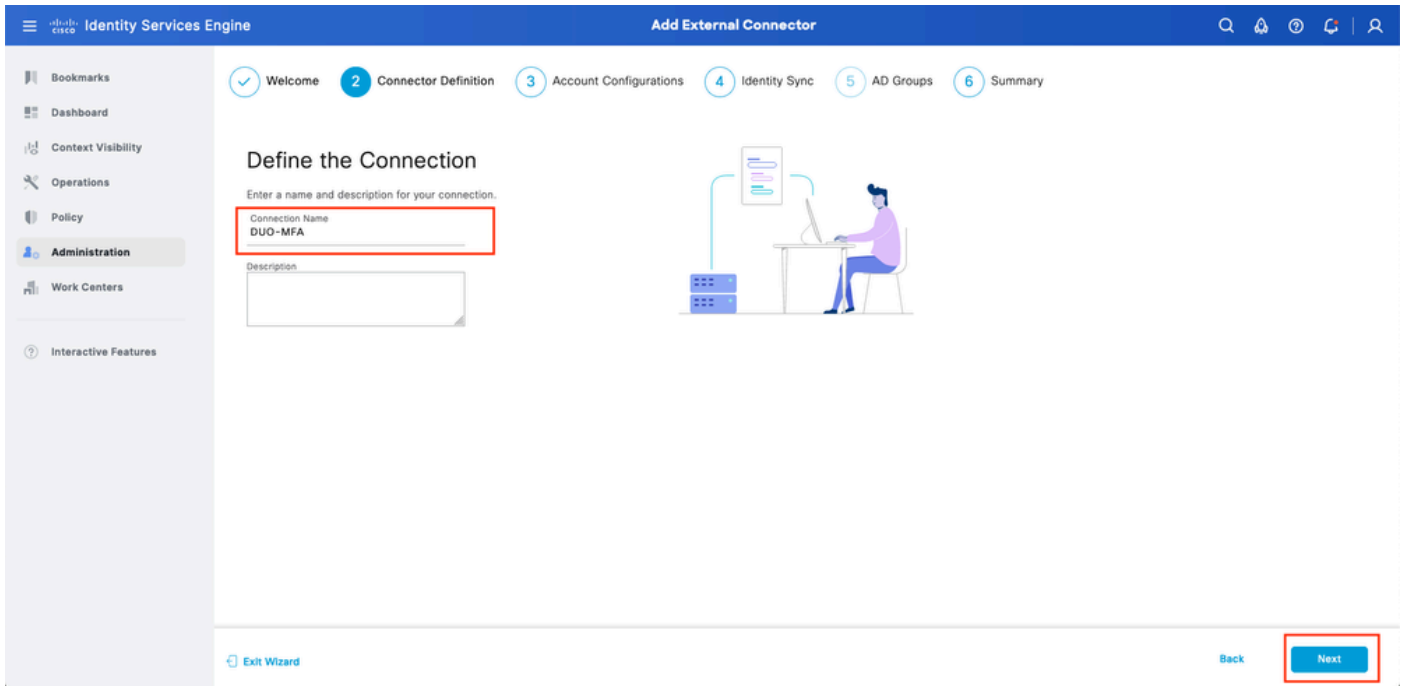
Before you begin, the following prerequisites apply:

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**

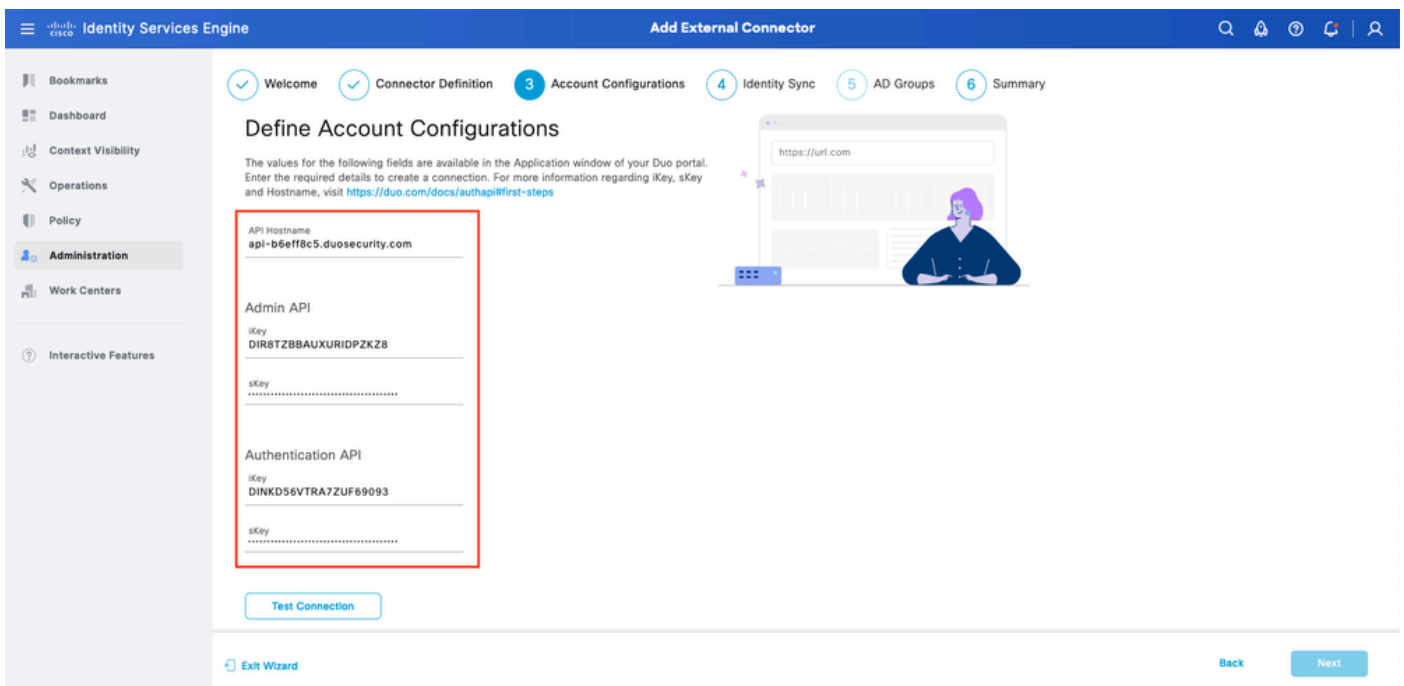
ISE DUO-wizard 1

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.




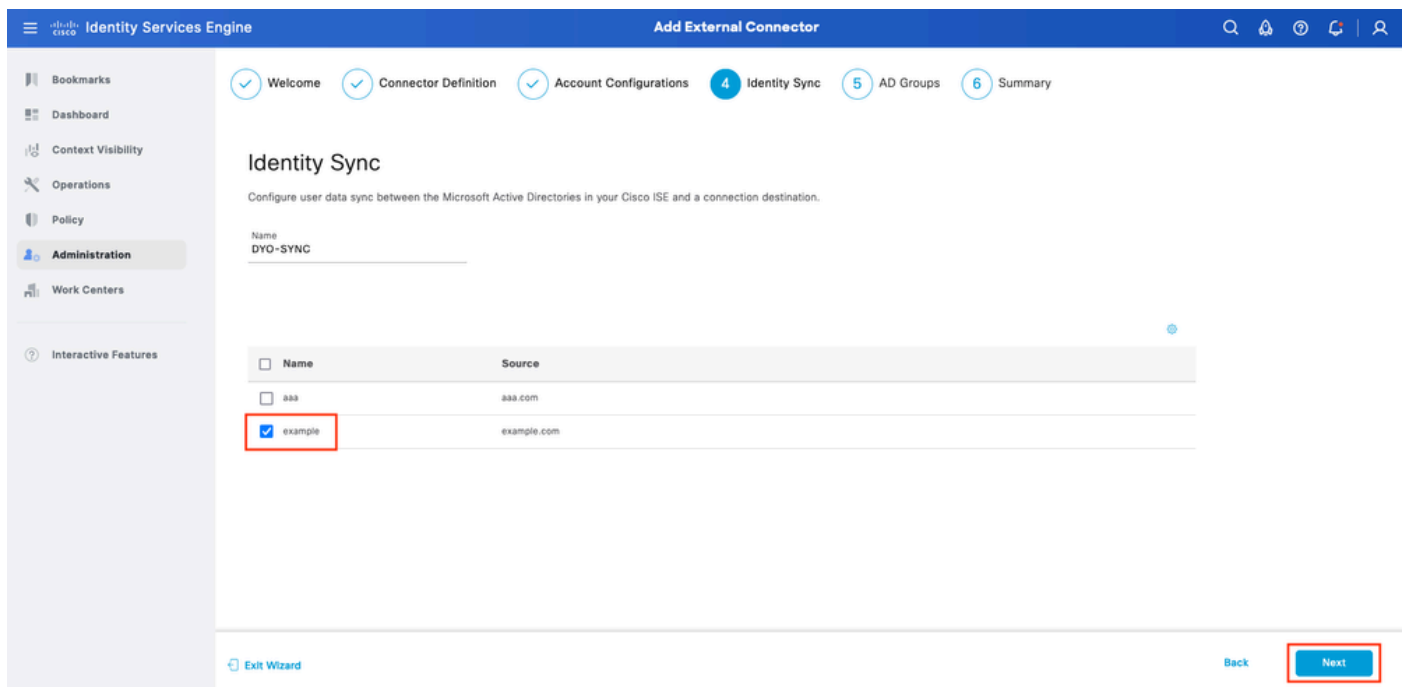
ISE DUO-wizard 3

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



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.



Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations **4 Identity Sync** 5 AD Groups 6 Summary

Identity Sync

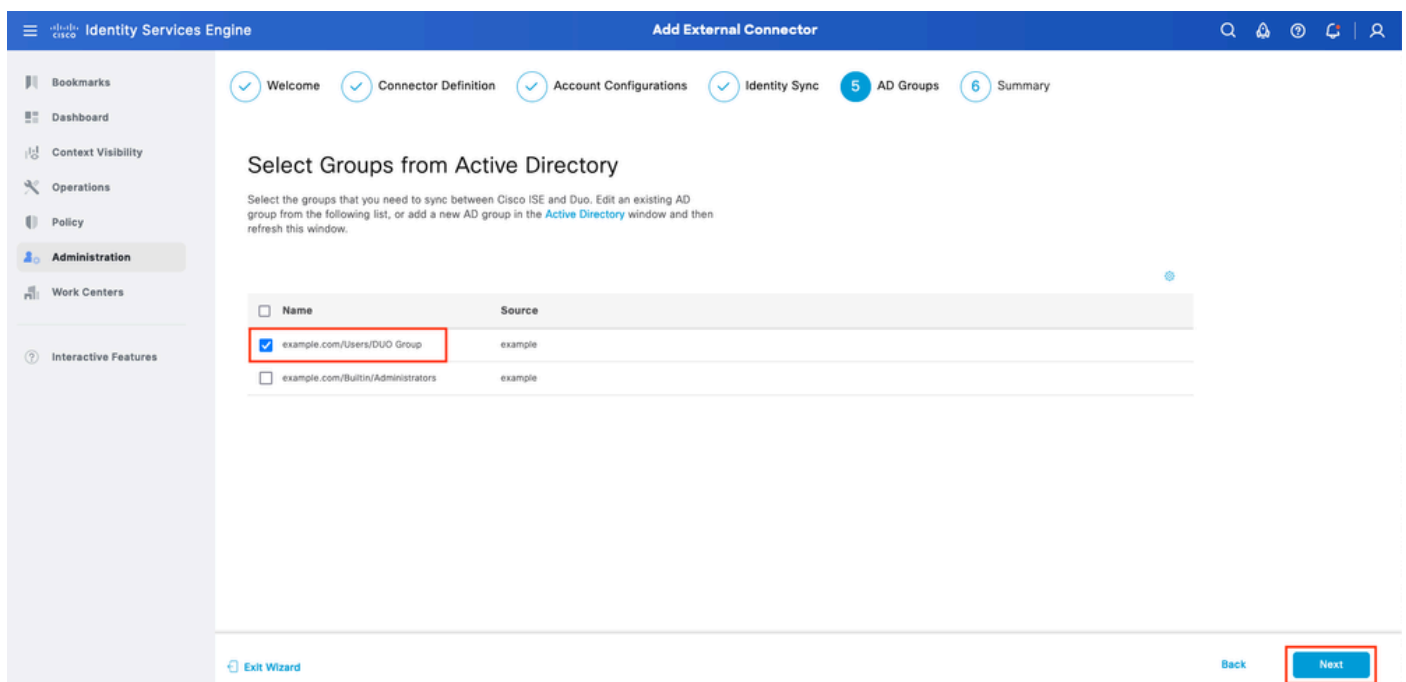
Configure user data sync between the Microsoft Active Directories in your Cisco ISE and a connection destination.

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**

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



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/DOU Group	example
<input type="checkbox"/>	example.com/BuiltIn/Administrators	example

Exit Wizard Back **Next**

Controleer of de instellingen correct zijn en klik op Gereed.

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.

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

DUO-inschrijving 1

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

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-inschrijving 2

Voer het telefoonnummer in en klik op Telefoon toevoegen.

Dashboard > Users > bob > Add Phone

Add Phone

[Learn more about Activating Duo Mobile](#)

Type

Phone

Tablet

Phone number

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

Add Phone

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.

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	⚙️

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The main view is titled 'Policy / Policy Sets'. On the left, there is a navigation menu with options like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area shows a table of Policy Sets. The 'Default' policy set is expanded to show 'MFA Policy(1)'. A table lists the MFA policies, with one row highlighted in red: 'DUO Rule' with conditions 'Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA' and 'Use' set to 'DUO-MFA'. Below this table, there are sections for 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy(15)'. At the bottom right, there are 'Reset' and 'Save' buttons, with the 'Save' button highlighted in red.

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring Authorization Policies. The main view is titled 'Policy / Policy Sets'. On the left, there is a navigation menu with options like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area shows a table of Authorization Policies. The 'DUO Authorization Rule' is highlighted in red. The rule name is 'DUO Authorization Rule', the conditions are 'example-ExternalGroups EQUALS example.com/Users/DUO Group', and the results are 'PermitAccess'. The 'Security Groups' field is set to 'Select from list'. At the bottom right, there are 'Reset' and 'Save' buttons, with the 'Save' button highlighted in red.

Beleidsset 3

Beperkingen

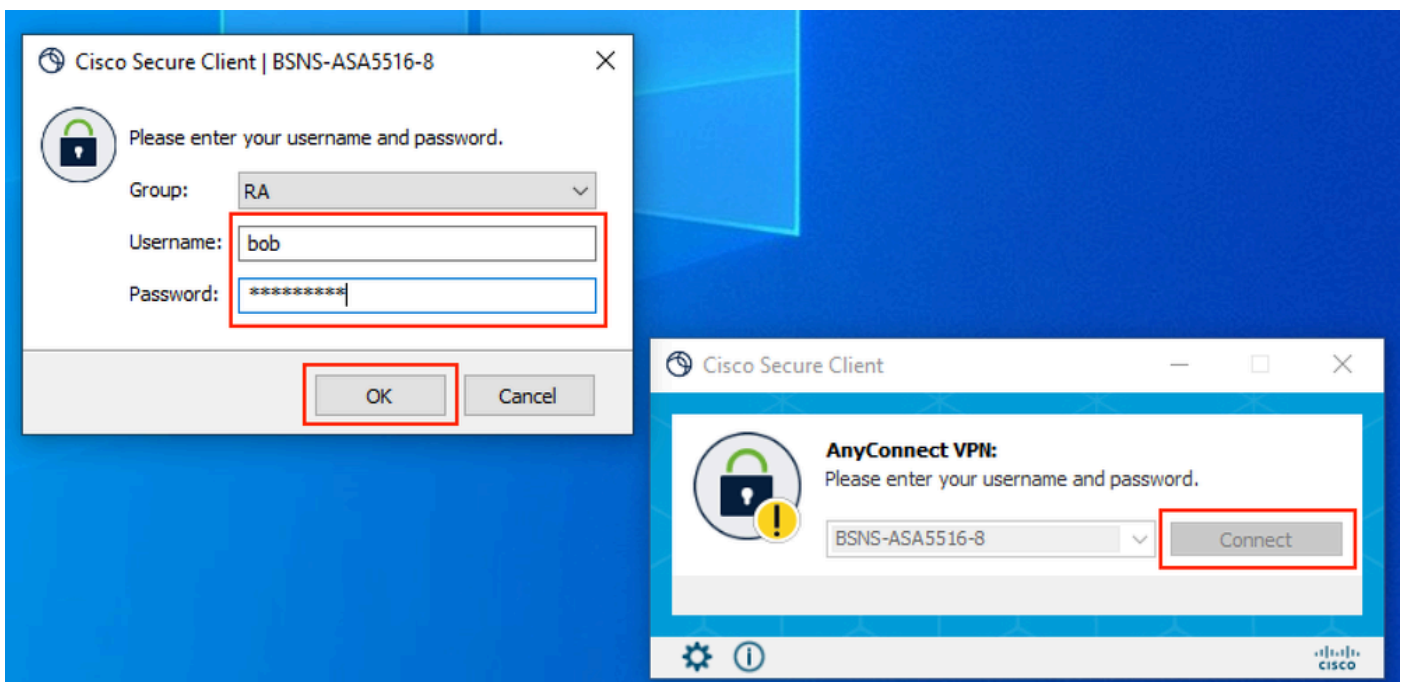
Bij het schrijven van dit document:

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.

1:52



Search

Accounts (8)

Add



Cisco
Cisco



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	MFAAuthenticator:onAuthenticateEvent MFAAuthenticator:sendAuthenticateEvent MFAAuthenticator::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.