

# ISE 3.0 REST-id configureren met Azure Active Directory

## Inhoud

- [Inleiding](#)
- [Achtergrondinformatie](#)
- [Voorwaarden](#)
- [Vereisten](#)
- [Gebruikte componenten](#)
- [Configureren](#)
- [Flow-overzicht op hoog niveau](#)
- [Azure AD voor integratie configureren](#)
- [Configureren ISE voor integratie](#)
- [ISE-beleidsvoorbeelden voor verschillende gebruikscases](#)
- [Verifiëren](#)
- [Problemen oplossen](#)
- [Problemen met de rest van de autorisatieservice](#)
- [Problemen met REST ID-verificatie](#)
- [Werken met de logbestanden](#)

## Inleiding

Dit document beschrijft de integratie van Cisco ISE 3.0 met Azure AD die is geïmplementeerd via REST Identity Service met Resource Owner Password Credentials.

## Achtergrondinformatie

In dit document wordt beschreven hoe u de integratie van Identity Services Engine (ISE) 3.0 met Microsoft (MS) Azure Active Directory (AD) kunt configureren en oplossen, geïmplementeerd via de Representational State Transfer (REST) Identity (ID)-service met behulp van Resource Owner Password Credentials (ROPC).

## Voorwaarden

### Vereisten

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

- ISE
- MS Azure AD
- Inzicht in de implementatie en beperkingen van het ROPC-protocol; [link](#)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 3.0
- MS Azure AD

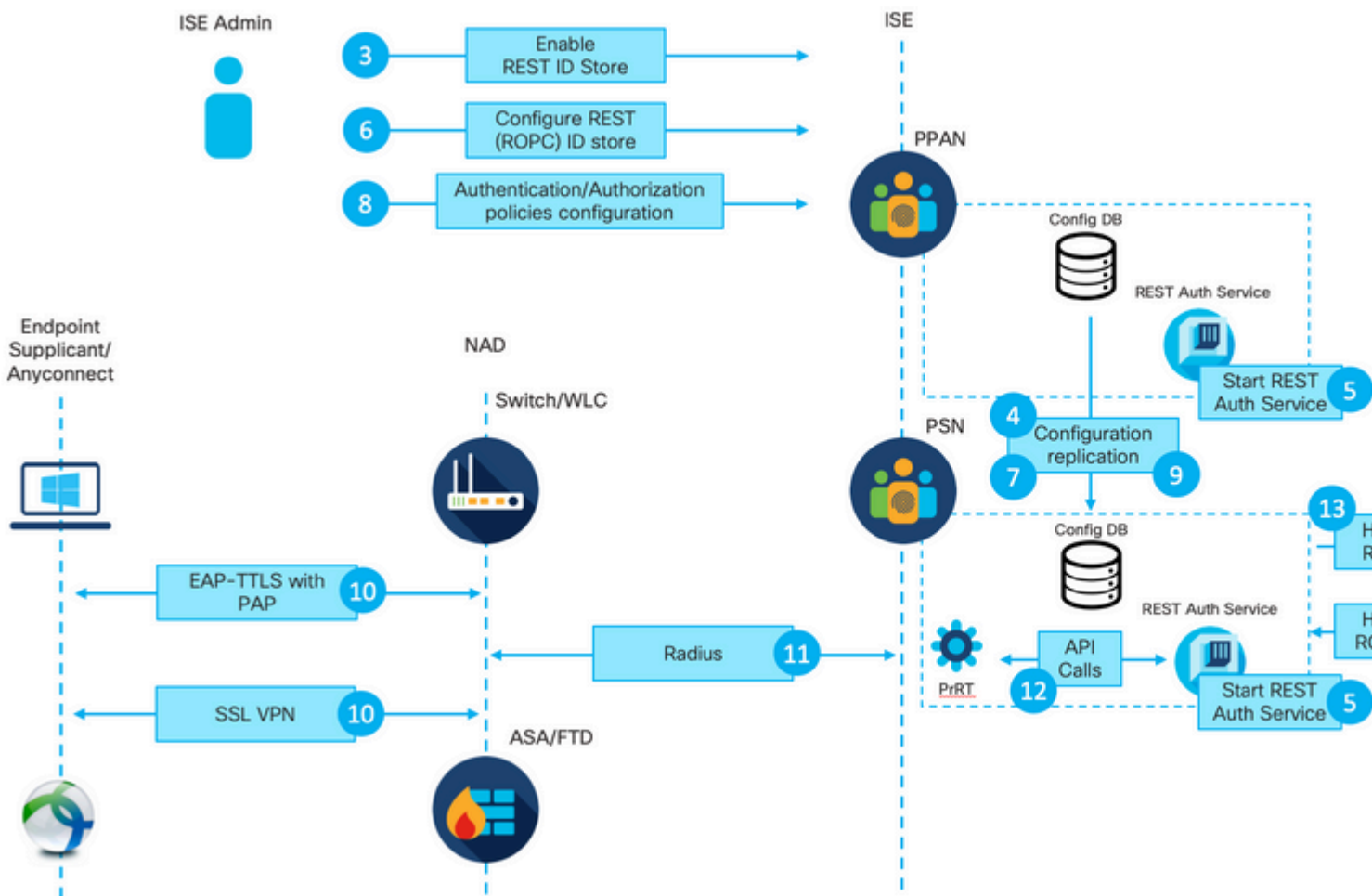
- WS-C3850-24P met s/w 16.9.2
- ASA v met 9,10 (1)
- Windows 10.0.18363

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

ISE REST ID-functionaliteit is gebaseerd op de nieuwe service die in ISE 3.0 - REST Auth Service is geïntroduceerd. Deze service is verantwoordelijk voor de communicatie met Azure AD over Open Authorisation (OAuth) ROPC-uitwisselingen om gebruikersverificatie en groepsherstel uit te voeren. De rest Auth Service is standaard uitgeschakeld en nadat de beheerder deze heeft ingeschakeld, wordt deze op alle ISE-knooppunten in de implementatie uitgevoerd. Aangezien REST Auth Service communicatie met de cloud gebeurt wanneer op het moment van de gebruikersverificatie, eventuele vertragingen op het pad extra latentie in de verificatie/autorisatie stroom brengen. Deze latentie valt buiten de ISE-controle en elke implementatie van REST Auth moet zorgvuldig worden gepland en getest om impact op andere ISE-diensten te voorkomen.

## Flow-overzicht op hoog niveau



1. Azure-cloudbeheerder maakt een nieuwe toepassing (App)-registratie aan. Details van deze app worden later op ISE gebruikt om een verbinding met de Azure AD tot stand te brengen.

2. Azure Cloud-beheerder moet de app configureren met:

- Een clientgeheim maken
- ROPC inschakelen
- Groepsclaims toevoegen
- Toepassingsprogrammeerinterfacerechten (API) definiëren

3. ISE-beheerder schakelt de REST-autorisatieservice in. Dit moet gebeuren voordat enige andere actie kan worden uitgevoerd.

4. Wijzigingen worden in de configuratiedatabase geschreven en over de gehele ISE-implementatie gerepliceerd.

5. REST Auth Service start op alle knooppunten.

6. ISE-beheerder configureert de REST-ID-winkel met gegevens uit stap 2.

7. De veranderingen worden geschreven in het configuratiegegevensbestand en over de volledige plaatsing van ISE herhaald.

8. ISE-beheerder maakt een nieuwe sequentie voor identiteitsopslag of wijzigt de sequentie die al bestaat en configureert beleid voor verificatie/autorisatie.

9. De veranderingen worden geschreven in het configuratiegegevensbestand en over de volledige plaatsing van ISE herhaald.

10. Endpoint initieert verificatie. Volgens de ROPC-protocolspecificatie moet het gebruikerswachtwoord aan het Microsoft Identity Platform worden gegeven in duidelijke tekst via een versleutelde HTTP-verbinding. Vanwege dit feit zijn de enige beschikbare verificatieopties die vanaf nu door ISE worden ondersteund:

- Extensible Verification Protocol-Tunnelling Transport Layer Security (EAP-TTLS) met Password Verification Protocol (PAP) als binnenste methode
- AnyConnect SSL VPN-verificatie met PAP

11. Uitwisseling met het Knooppunt van de Dienst van het Beleid van ISE (PSN) over Straal.

12. Process Runtime (PrRT) stuurt een verzoek naar REST ID-service met gebruikersgegevens (gebruikersnaam/wachtwoord) via interne API.

13. REST ID-service stuurt OAuth ROPC-aanvraag naar Azure AD via HyperText Transfer Protocol Secure (HTTPS).

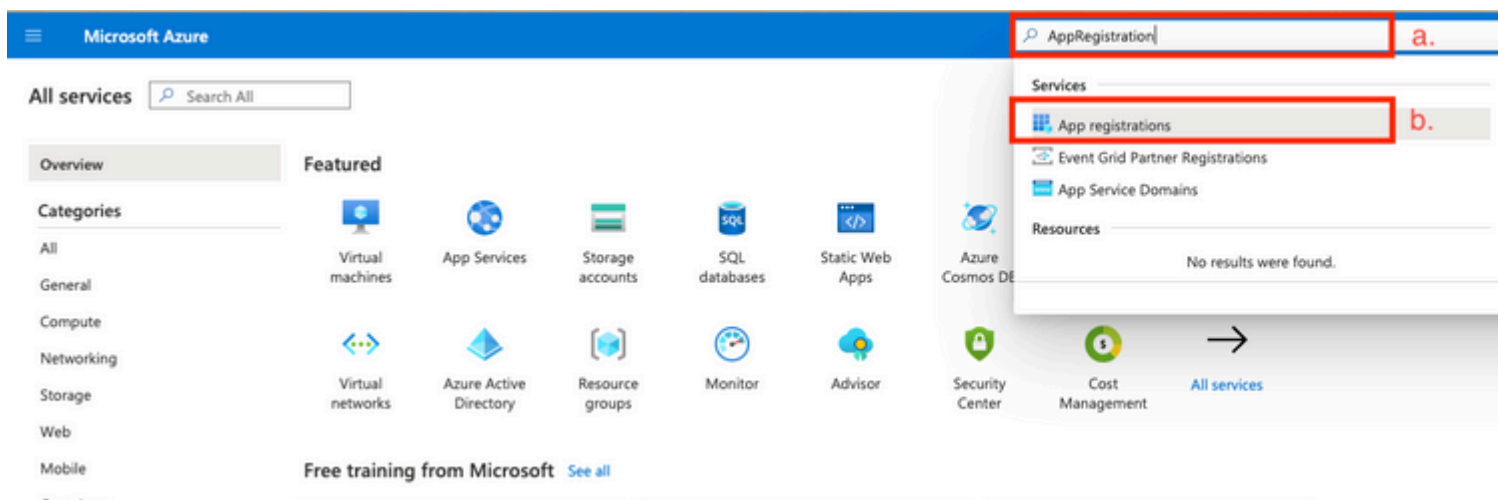
14. Azure AD voert gebruikersverificatie uit en haalt gebruikersgroepen op.

15. Resultaat van verificatie/autorisatie teruggestuurd naar ISE.

Na punt 15 zijn het authenticatieresultaat en de opgehaalde groepen teruggekeerd naar PrRT, waarbij de stroom van beleidsevaluaties wordt gebruikt en het definitieve resultaat van verificatie/autorisatie wordt toegewezen. Ofwel Access-Accept met eigenschappen uit het autorisatieprofiel of Access-Reject dat is teruggestuurd naar Network Access Device (NAD).

## Azure AD voor integratie configureren

1. Zoek de AppRegistration Service zoals in de afbeelding.



Afbeelding 2.

a. Type AppRegistration in de algemene zoekbalk.

b. Klik op de App-registratieservice.

2. Maak een nieuwe app-registratie.



[All services](#) >

# App registrations

[+ New registration](#)

[Endpoints](#)

[Troubleshooting](#)

[Download \(Preview\)](#)

[Got feedback?](#)

 Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed.

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure

[All applications](#)

[Owned applications](#)

Afbeelding 3.

3. Registreer een nieuwe app.

## Register an application

\* Name

The user-facing display name for this application (this can be changed later).

Azure-AD-ISE-APP

a.

### Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (DEMO only - Single tenant)

b.

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

e.g. https://myapp.com/auth

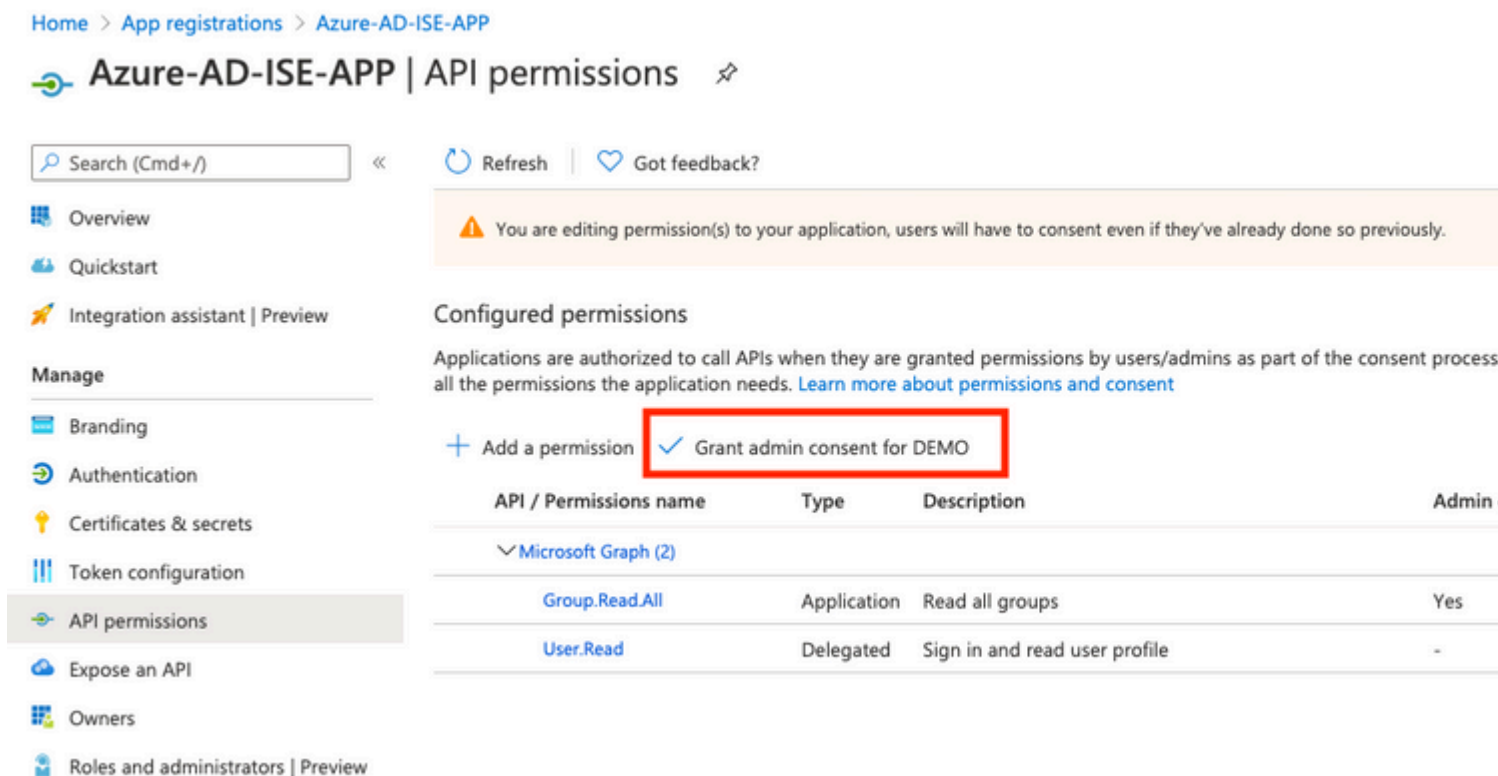
By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

c.

: Gebruikersgroepgegevens kunnen op meerdere manieren uit Azure AD worden gehaald met behulp van verschillende API-rechten. De methode die in dit voorbeeld wordt beschreven, is succesvol gebleken in het Cisco TAC-lab. Gebruik andere API-rechten voor het geval uw Azure AD-beheerder dit aanraadt.

## 16. Grant admin consent voor API-rechten.



Home > App registrations > Azure-AD-ISE-APP

### Azure-AD-ISE-APP | API permissions

Search (Cmd+/) Refresh Got feedback?

**Warning:** You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

#### Configured permissions

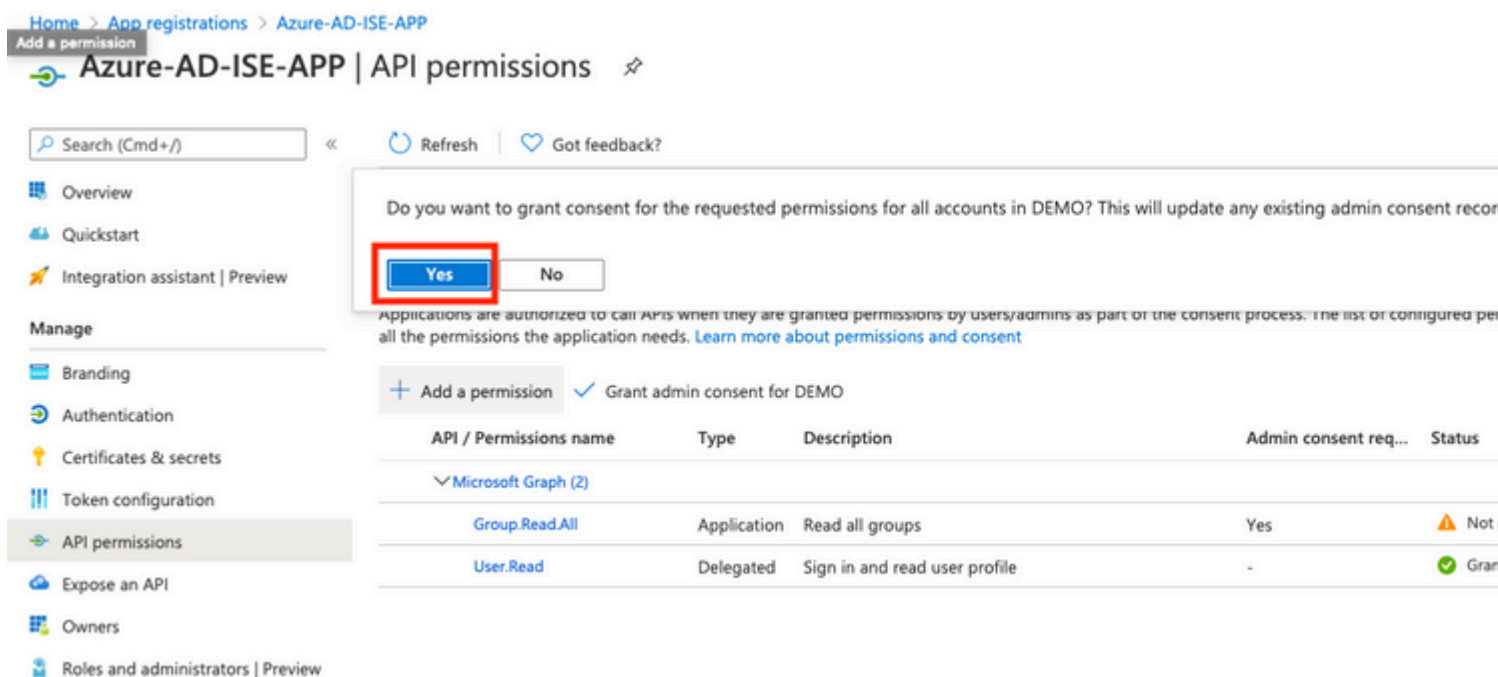
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. All the permissions the application needs. [Learn more about permissions and consent](#)

Grant admin consent for DEMO

API / Permissions name	Type	Description	Admin
Microsoft Graph (2)			
Group.Read.All	Application	Read all groups	Yes
User.Read	Delegated	Sign in and read user profile	-

Afbeelding 17.

## 17. Bevestig de toestemming van de beheerder.



Home > App registrations > Azure-AD-ISE-APP

### Azure-AD-ISE-APP | API permissions

Search (Cmd+/) Refresh Got feedback?

**Dialog:** Do you want to grant consent for the requested permissions for all accounts in DEMO? This will update any existing admin consent records. [Learn more about permissions and consent](#)

Grant admin consent for DEMO

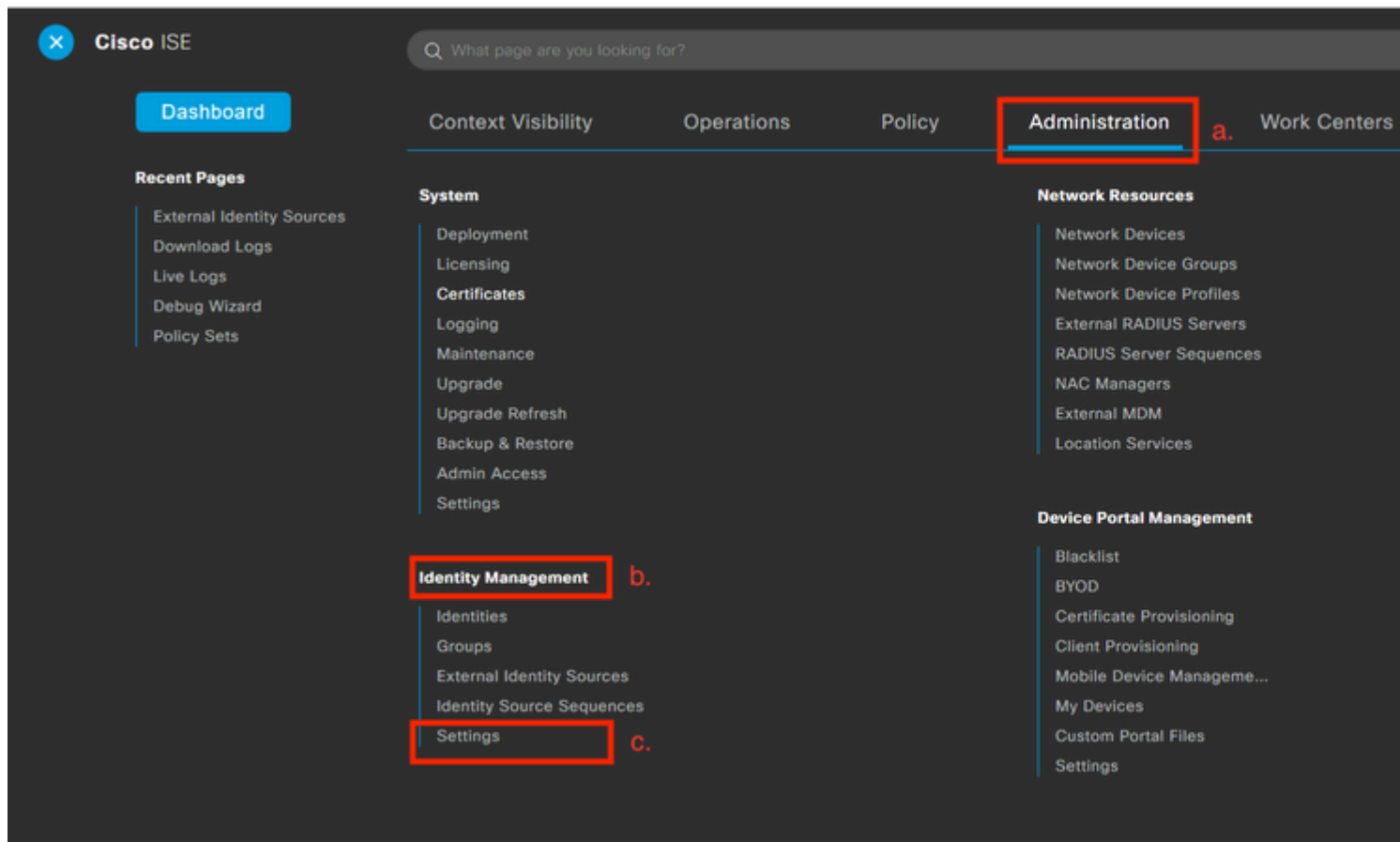
API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
Group.Read.All	Application	Read all groups	Yes	Not granted
User.Read	Delegated	Sign in and read user profile	-	Granted

Afbeelding 18.

Op dit punt kunt u overwegen integratie volledig geconfigureerd aan de kant van Azure AD.

## Configureren ISE voor integratie

1. Navigeer naar instellingen voor identiteitsbeheer.

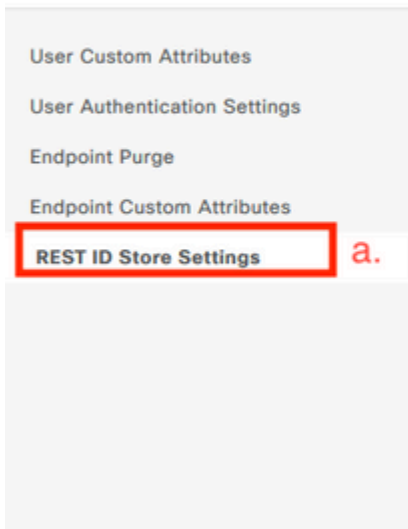


Afbeelding 19.

Naar navigeren Administration > Identity Management > Settings .

2. Schakel de REST ID-service in (standaard uitgeschakeld).





## REST ID Store Settings

Status

Enabled

b.

Disabled

Cancel

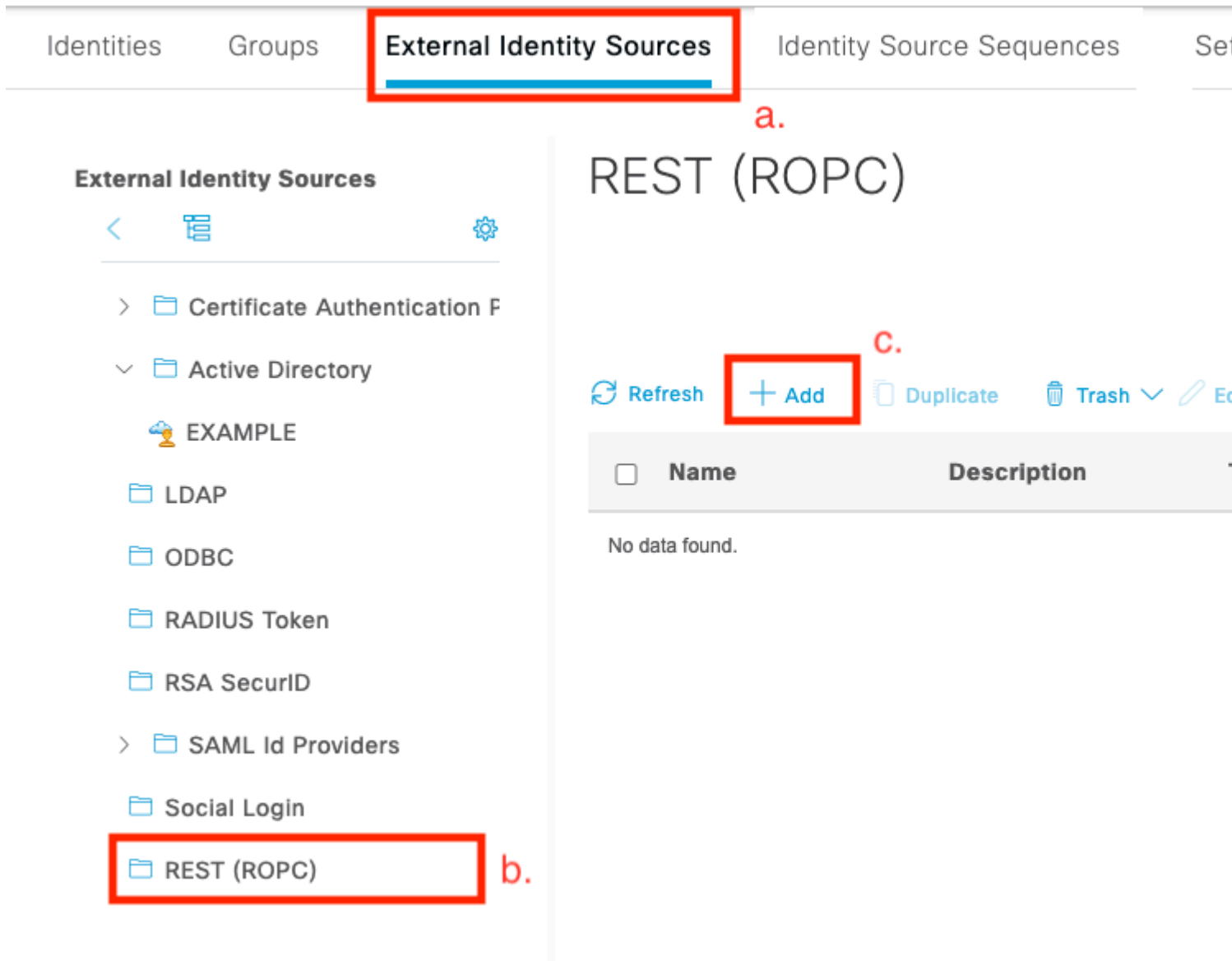
Submit

c.

Afbeelding 20.

Naar navigeren REST ID Store Settings en de status van de instellingen van de REST ID Store te wijzigen om Enable, dan Submit uw wijzigingen.

3. Maak een REST ID-winkel.



Afbeelding 21.

Switch aan de External Identity Sources tabblad klikt u op REST (ROPC) en klik op **Toevoegen**.

4. Configureer de REST ID store.

**External Identity Sources**



> Certificate Authentication F

∨ Active Directory

EXAMPLE

LDAP

ODBC

RADIUS Token

RSA SecurID

> SAML Id Providers

Social Login

REST (ROPC)

REST (ROPC) > New

Name \*

Azure\_AD

a.

Description

REST Identity Provider \*

Azure

Client ID \*

b.

Client Secret \*

c.

Tenant ID \*

Test c

d.

Groups

Load c

Username Suffix

@skuchere.onmicrosoft.com

e.

Cancel



Afbeelding 22.

- a. Bepaal de naam van de ID-winkel. Later kan deze naam in de lijst van woordenboeken van ISE worden gevonden wanneer u vergunningsbeleid vormt. Deze naam wordt ook weergegeven in de lijst met ID-opslagsystemen die beschikbaar zijn in de instellingen voor het verificatiebeleid en in de lijst met ID-opslagsystemen die beschikbaar zijn in de configuratie van de Identity Store-reeks.
- b. Geef client-ID (overgenomen uit Azure AD in stap 8 van het gedeelte Azure AD-integratieconfiguratie).
- c. Verstrek cliëntgeheim (genomen van Azure AD in Stap 7. van het gedeelte Azure AD-integratieconfiguratie).
- d. Verstrek huurder-ID (overgenomen uit Azure AD in stap 8. van de integratiesectie Azure AD).
- e. Gebruikersnaam instellen Suffix - Standaard maakt ISE PSN gebruik van een gebruikersnaam die door de eindgebruiker is opgegeven, die in de sAMAaccountName-indeling wordt verstrekt (korte gebruikersnaam, bijvoorbeeld bob); in een dergelijk geval kan Azure AD de gebruiker niet vinden. Gebruikersnaam Suffix is de waarde die aan de gebruikersnaam wordt toegevoegd die door de gebruiker wordt geleverd om de gebruikersnaam naar het UPN-formaat te brengen.

---

**Opmerking:** ROPC is beperkt tot gebruikersverificatie omdat het zich tijdens de verificatie baseert op het kenmerk Gebruikersnaam. Apparaatobjecten in Azure AD hebben geen gebruikerskenmerken.

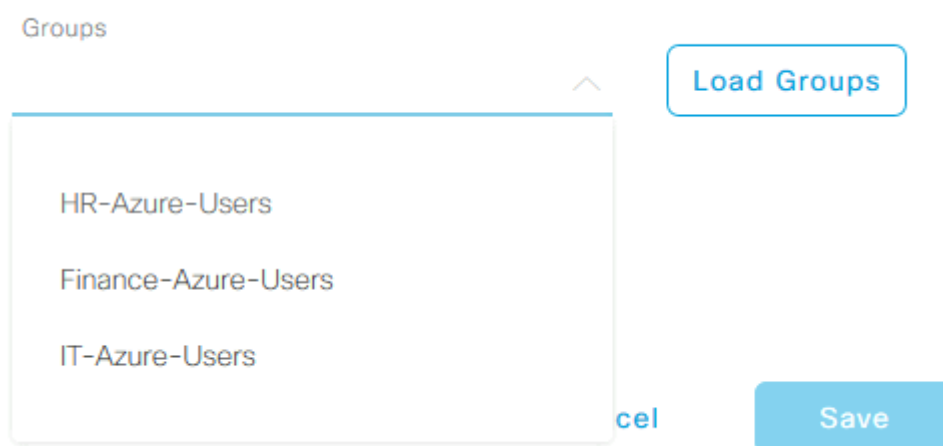
---

- f. Druk op Test-verbinding om te bevestigen dat ISE de geleverde App-gegevens kan gebruiken om een verbinding met Azure AD tot stand te brengen.
- g. Druk op Laadgroepen om groepen toe te voegen die beschikbaar zijn in de Azure AD naar REST ID-winkel. Het voorbeeld hier laat zien hoe admin ervaring eruit ziet.

---

**Opmerking:** houd rekening met het defect dat Cisco bug-id [CSCvx00345](#) veroorzaakt doordat groepen niet worden geladen. Het defect is verholpen in ISE 3.0 patch 2.

---

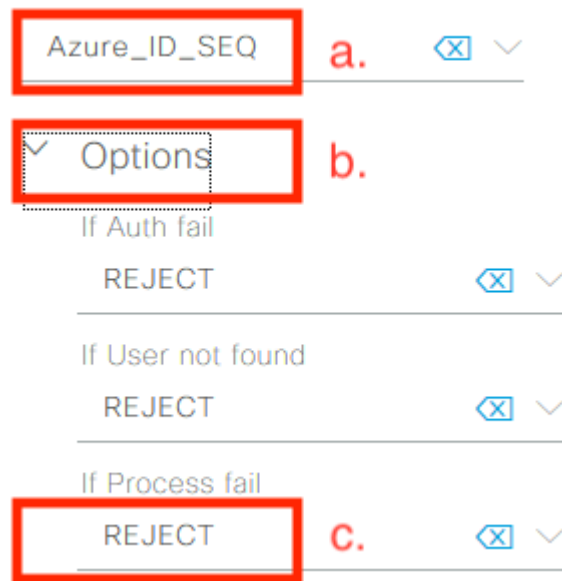


Afbeelding 23.

- h. Verzend uw wijzigingen.

5. Overweeg in deze fase de creatie van een nieuwe Identity Store Sequence, die een nieuw gecreëerde REST ID-winkel omvat.

6. Op het moment dat de REST-ID-opslag of Identity Store-sequentie die deze bevat, is toegewezen aan het verificatiebeleid, wijzigt u een standaardactie voor procesfout van DALEN naar AFWIJZEN zoals in de afbeelding.



Afbeelding 24.

- a. Zoek een verificatiebeleid dat gebruikmaakt van de REST-ID-opslag.
- b. Open de vervolgkeuzelijst Opties.
- c. De standaardinstelling voor het proces is mislukt van droppen naar WEIGEREN.

Dit is nodig om te voorkomen dat PSN aan de NADs-kant als dood aangemerkt wordt op het moment dat specifieke fouten optreden in de REST ID-winkel, zoals:

- De gebruiker is geen lid van een groep in Azure AD.
- Het gebruikerswachtwoord moet worden gewijzigd.

7. Voeg het opslagwoordenboek van REST-ID toe aan het autorisatiebeleid.

## Editor

Click to add an attribute

Equals Attribute val

### Select attribute for condition

Dictionary	Attribute
All Dictionaries	Attribute <b>a.</b>
All Dictionaries	
Airspace	Aire-Data-Bandwidth-Aver... 7
Alcatel-Lucent	Aire-Data-Bandwidth-Aver... 1
Aruba	
<b>Azure_AD</b> <b>b.</b>	Aire-Data-Bandwidth-Burs... 9
Brocade	Aire-Data-Bandwidth-Burs... 1
CERTIFICATE	
CWA	Aire-Data-Bandwidth-Burs... 1
Cisco-BBSM	
Cisco-VPN3000	Aire-Real-Time-Bandwidth... 8
Cisco	
DEVICE	Aire-Real-Time-Bandwidth... 1
EXAMPLE	
EndPoints	Aire-Real-Time-Bandwidth... 1
Guest	
H3C	
HP	
IdentityGroup	
InternalUser	
Juniper	

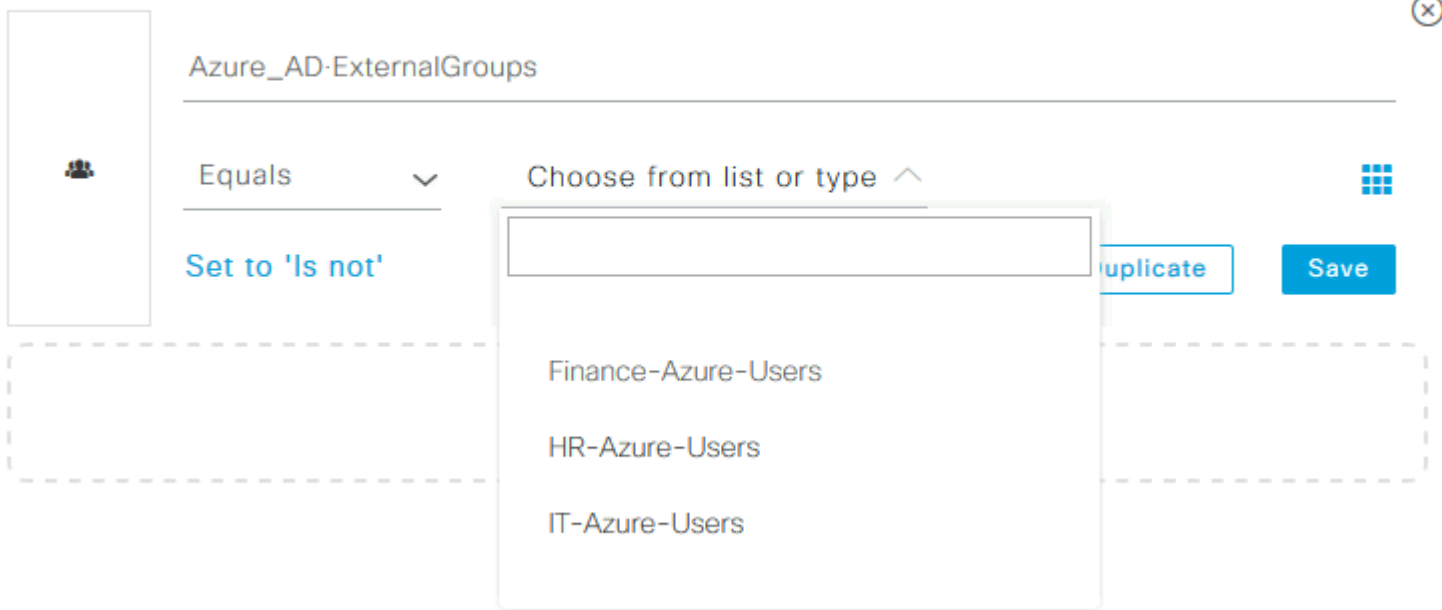
Afbeelding 25.

a. Open de vervolgkeuzelijst Alle woordenboeken.

b. Zoek het genoemde woordenboek op dezelfde manier als uw REST ID-winkel.

8. Voeg externe identiteitsgroepen toe (vanaf ISE 3.0 is het enige kenmerk dat in het woordenboek REST-ID-opslag beschikbaar is een externe groep).

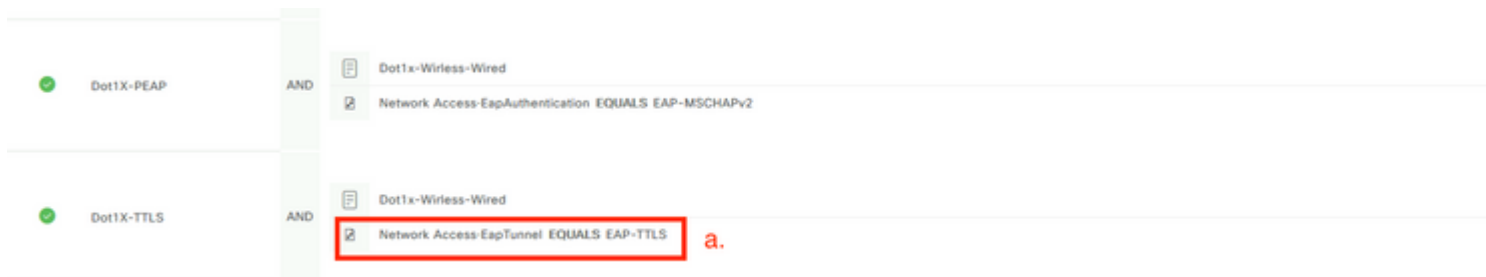
## Editor



Afbeelding 26.

## ISE-beleidsvoorbeelden voor verschillende gebruikscases

In het geval van Dot1x-verificatie kan de EAP-tunnelvoorwaarde uit het woordenboek voor netwerktoegang worden gebruikt om EAP-TTLS-pogingen aan te passen zoals in de afbeelding.



Afbeelding 27.

a. Definieer EAP Tunnel GELIJK aan EAP-TTLS om pogingen aan te passen die aan de REST ID-opslag moeten worden doorgestuurd.

b. Selecteer dit in het vak REST ID direct of Identity Store Sequence, dat het in de kolom Gebruik bevat.

Binnen het individuele vergunningsbeleid kunnen externe groepen van Azure AD samen met het EAP-tunneltype worden gebruikt:

✓	Dot1X-TTLS-Azure-Finance	AND	<ul style="list-style-type: none"> <li>Dot1x-Wireless-Wired</li> <li>Network Access-EapTunnel EQUALS EAP-TTLS</li> <li>Azure_AD-ExternalGroups EQUALS Finance-Azure-Users</li> </ul>
✓	Dot1X-TTLS-Azure-HR	AND	<ul style="list-style-type: none"> <li>Dot1x-Wireless-Wired</li> <li>Network Access-EapTunnel EQUALS EAP-TTLS</li> <li>Azure_AD-ExternalGroups EQUALS HR-Azure-Users</li> </ul>
✓	Dot1X-TTLS-Azure-IT	AND	<ul style="list-style-type: none"> <li>Dot1x-Wireless-Wired</li> <li>Network Access-EapTunnel EQUALS EAP-TTLS</li> <li>Azure_AD-ExternalGroups EQUALS IT-Azure-Users</li> </ul>

Afbeelding 28.

Voor VPN gebaseerde flow kunt u een tunnelgroepnaam als differentiator gebruiken:

Verificatiebeleid:

Status	Rule Name	Conditions
✓	Azure-AD	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS skuchere

Vergunningsbeleid:

✓	VPN-Azure-Finance	AND	<ul style="list-style-type: none"> <li>Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name</li> <li>Azure_AD-ExternalGroups EQUALS Finance-Azure-Users</li> </ul>
✓	VPN-Azure-HR	AND	<ul style="list-style-type: none"> <li>Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name</li> <li>Azure_AD-ExternalGroups EQUALS HR-Azure-Users</li> </ul>
✓	VPN-Azure-IT	AND	<ul style="list-style-type: none"> <li>Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name</li> <li>Azure_AD-ExternalGroups EQUALS IT-Azure-Users</li> </ul>

Afbeelding 29.



# Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

1. Bevestig dat de REST Auth Service op het ISE-knooppunt wordt uitgevoerd.

Om dit te controleren, moet u de opdracht **status** van de **showtoepassing** in de Secure Shell (SSH)-shell van een doel ISE-knooppunt uitvoeren:

```
<#root>
```

```
skuchere-ise30-1/admin# show application status ise
```

```
ISE PROCESS NAME STATE PROCESS ID
```

```
-----
```

```
Database Listener running 101790
Database Server running 92 PROCESSES
Application Server running 39355
Profiler Database running 107909
ISE Indexing Engine running 115132
AD Connector running 116376
M&T Session Database running 107694
M&T Log Processor running 112553
Certificate Authority Service running 116226
EST Service running 119875
SXP Engine Service disabled
Docker Daemon running 104217
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 104876
ISE API Gateway Database Service running 106853
ISE API Gateway Service running 110426
Segmentation Policy Service disabled
```

```
REST Auth Service running 63052
```

```
SSE Connector disabled
```

2. Controleer of de REST-ID-opslag wordt gebruikt op het moment van de verificatie (controleer de stappen.-sectie van het gedetailleerde verificatierapport).

```

15013 Selected Identity Source - Azure_AD
25103 Perform plain text password authentication in external REST ID store server - Azure_AD a.
25100 Connecting to external REST ID store server - Azure_AD b.
25101 Successfully connected to external REST ID store server - Azure_AD (🕒 Step latency=1660 ms) c.
25104 Plain text password authentication in external REST ID store server succeeded - Azure_AD d.
25107 REST ID store server respond with groups - Azure_AD e.
25110 User groups inserted to session cache - Azure_AD f.
22037 Authentication Passed

```

- a. PSN start verificatie van onbewerkte tekst met geselecteerde REST-ID-opslag.
  - b. Verbinding gemaakt met Azure Cloud.
  - c. Feitelijke authenticatiestap - let op de hier gepresenteerde latentiewaarde. In het geval dat al uw authenticaties met de Aure Cloud worstelen van aanzienlijke latentie, dit beïnvloedt de andere ISE-flow, en als gevolg daarvan wordt de gehele ISE-implementatie instabiel.
  - d. Bevestiging van succesvolle verificatie.
  - e. Bevestiging van in antwoord gepresenteerde groepsgegevens.
  - f. Sessiecontext gevuld met gebruikersgroepgegevens. Voor meer details over het ISE-sessiebeheerproces, kunt u een herziening van deze [link](#) van artikel overwegen.
3. Bevestig dat verwacht wordt dat het beleid voor verificatie/autorisatie wordt geselecteerd (voor dit te onderzoeken overzicht sectie van het gedetailleerde verificatierapport).

## Overview

Event 5200 Authentication succeeded

Username bob

Endpoint Id ED:37:E1:08:57:15 📶

### Endpoint Profile

Authentication Policy SPRT-Policy-Set >> Azure-AD

Authorization Policy SPRT-Policy-Set >> Azure-Finance

Authorization Result PermitAccess

Afbeelding 30.

## Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

### Problemen met de rest van de autorisatieservice

Om problemen met REST Auth Service op te lossen, moet u beginnen met de beoordeling van het **ADE.log**-bestand. Ondersteuning bundellocatie - **/support/adeos/ade**

Een zoekterm voor REST Auth Service is - **ROPC-control**.

Dit voorbeeld laat zien hoe de REST Auth Service begint:

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] St
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] in
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Im
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Do
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Lo
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Ex
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Lo
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Do
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Se
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] in
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Co
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Co
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Co
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Cr
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info: [application:operation:ROPC-control.sh] Co
```

In gevallen waarin de dienst niet start of onverwacht daalt, is het altijd zinvol om te beginnen door het **ADE.log** rond een problematisch tijdschema te bekijken.

### Problemen met REST ID-verificatie

In het geval van verificatiefouten wanneer de REST-ID-opslag wordt gebruikt, moet u altijd beginnen met een gedetailleerd verificatierapport. In het gebied Andere kenmerken kunt u een sectie zien - **RestAuthErrorMsg** die een fout bevat die door Azure cloud wordt geretourneerd:

RestAuthErrorMsg

Error Key - invalid\_client | Error Description - AADSTS7000218: The request body must contain the following parameter: 'client\_assertion' or 'client\_secret'. Error Code: 519641db-a8ea-49df-85aa-ddd2b53a0000 | Error Codes - 2020-09-13 19:11:47Z | Error Codes -  
- <https://login.microsoftonline.com/error>

Afbeelding 31.

## Werken met de logbestanden

In ISE 3.0 vanwege de Controlled Introduction of REST ID-functie, debuggen voor deze standaard ingeschakeld. Alle aan REST ID gerelateerde logbestanden worden opgeslagen in ROPC-bestanden die via CLI kunnen worden bekeken:

```
skuchere-ise30-1/admin# sh logging application | i ropc
755573 Oct 04 2020 09:10:29 ropc/ropc.log
```

```
skuchere-ise30-1/admin# sh logging application ropc/ropc.log
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
```

Merk op dat op ISE 3.0 met de geïnstalleerde patch de bestandsnaam rest-id-store.log is en niet ropc.log. Het vorige zoekvoorbeeld heeft gewerkt omdat de mapnaam niet is gewijzigd.

Of die bestanden kunnen worden afgeleid uit de ISE-ondersteuningsbundel.

Hier zijn een paar logboekvoorbeelden die verschillende het werken en niet-werkende scenario's tonen:

1. Certificaatfout wanneer de Azure Graph niet wordt vertrouwd door de ISE-knooppunt. Deze fout kan worden gezien wanneer groepen niet laden in de REST ID winkel instelling.

```
20:44:54.420 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https://graph.microsoft.com/v1.0/groups'
20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch application certificate
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate found
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1946)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

Dit probleem duidt erop dat het Microsoft grafiek API-certificaat niet wordt vertrouwd door ISE. ISE 3.0.0.458 heeft geen DigiCert Global Root G2 CA geïnstalleerd in de vertrouwde winkel. Dit wordt in het defect gedocumenteerd

- Cisco bug-id [CSCv80297](https://tools.cisco.com/bugcenter/bug/?bugID=CSCv80297) Om dit probleem op te lossen, moet u DigiCert Global Root G2 CA in een ISE-vertrouwde winkel installeren en markeren als vertrouwd voor Cisco-services.

Het certificaat kan hier worden gedownload - <https://www.digicert.com/kb/digicert-root-certificates.htm>

## 2. Onjuiste aanvraag geheim.

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client se
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentityF
```

## 3. Verkeerde APP-ID.

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with i
Trace ID: 6dbd0 added-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

## 4. Gebruiker niet gevonden.

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Stat
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvider
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

5. Gebruikerswachtwoord verlopen - dit kan doorgaans gebeuren voor de nieuwe gebruiker, aangezien het wachtwoord dat door Azure admin is gedefinieerd, moet worden gewijzigd bij de aanmelding bij Office365.

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Status: 400
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_description":"The client is not authorized to use this token."}
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProviderFacade.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

## 6. Groepen kunnen niet worden geladen vanwege verkeerde API-rechten.

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Status: 403
{"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

## 7. Verificatie mislukt wanneer ROPC niet is toegestaan aan de Azure-zijde.

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with trustManager
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Status: 400
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_client","error_description":"The client is not authorized to use this token."}
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProviderFacade.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

## 8. Verificatie mislukt omdat de gebruiker niet tot een groep aan de kant van Azure behoort.

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with trustManager
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "roles"
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPCController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id token: "roles"
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

## 9. Succesvolle gebruikersverificatie en groepsherstel.

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filter
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https:
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168.
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials t
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.2
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```

## 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.