

ISE 3.1 ISE GUI Admin inlogstroom configureren via SAML SSO-integratie met Azure AD

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Identity Provider \(IDP\)](#)

[Serviceprovider \(SP\)](#)

[SAML](#)

[SAML Assertion](#)

[Flow Diagram op hoog niveau](#)

[SAML SSO-integratie configureren met Azure AD](#)

[Stap 1. SAML Identity Provider configureren op ISE](#)

[1. Azure AD configureren als externe SAML Identity Source](#)

[2. ISE-verificatiemethode configureren](#)

[3. Informatie over exportserviceproviders](#)

[Stap 2. Instellingen voor Azure AD IDP configureren](#)

[1. Een Azure AD-gebruiker maken](#)

[2. Een Azure AD-groep maken](#)

[3. Wijs Azure AD-gebruiker toe aan de groep](#)

[4. Een Azure AD Enterprise-toepassing maken](#)

[5. Voeg groep toe aan de toepassing](#)

[6. Een Azure AD Enterprise-toepassing configureren](#)

[7. Active Directory-groepskenmerk configureren](#)

[8. Azure Federation Metadata XML-bestand downloaden](#)

[Stap 3. MetaData uploaden van Azure Active Directory naar ISE](#)

[Stap 4. SAML-groepen op ISE configureren](#)

[\(Optioneel\) Stap 5. RBAC-beleid configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Veelvoorkomende problemen](#)

[Probleemoplossing ISE](#)

[Logbestanden met SAML Login en Mismatched Group Claim Names](#)

Inleiding

In dit document wordt beschreven hoe u de integratie van Cisco ISE 3.1 SAML SSO kunt configureren met een externe identiteitsprovider zoals Azure Active Directory (AD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

1. Cisco ISE-lijnkaart 3.1
2. SAML SSO-implementaties
3. Azure AD

Gebruikte componenten

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

1. Cisco ISE-lijnkaart 3.1
2. Azure AD

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.

Achtergrondinformatie

Identity Provider (IDP)

Het is de autoriteit Azure AD in dit geval, die een gebruikersidentiteit en toegangsrechten tot een gevraagde bron (de "Serviceprovider") verifieert en bevestigt.

Serviceprovider (SP)

De gehoste bron of service waartoe de gebruiker toegang wil krijgen, in dit geval de ISE Application Server.

SAML

Security Assertion Markup Language (SAML) is een open standaard die IdP toestaat om aanmeldingsgegevens door te geven aan SP.

SAML-transacties maken gebruik van Extensible Markup Language (XML) voor gestandaardiseerde communicatie tussen de identiteitsprovider en serviceproviders.

SAML is de koppeling tussen de authenticatie van een gebruikersidentiteit en de autorisatie voor het gebruik van een dienst.

SAML Assertion

Een SAML Assertion is het XML-document dat de identiteitsprovider verstuurt naar de serviceprovider die de gebruikersautorisatie bevat.

Er zijn drie verschillende typen SAML Assertions - authenticatie, attribuut en autorisatiebesluit.

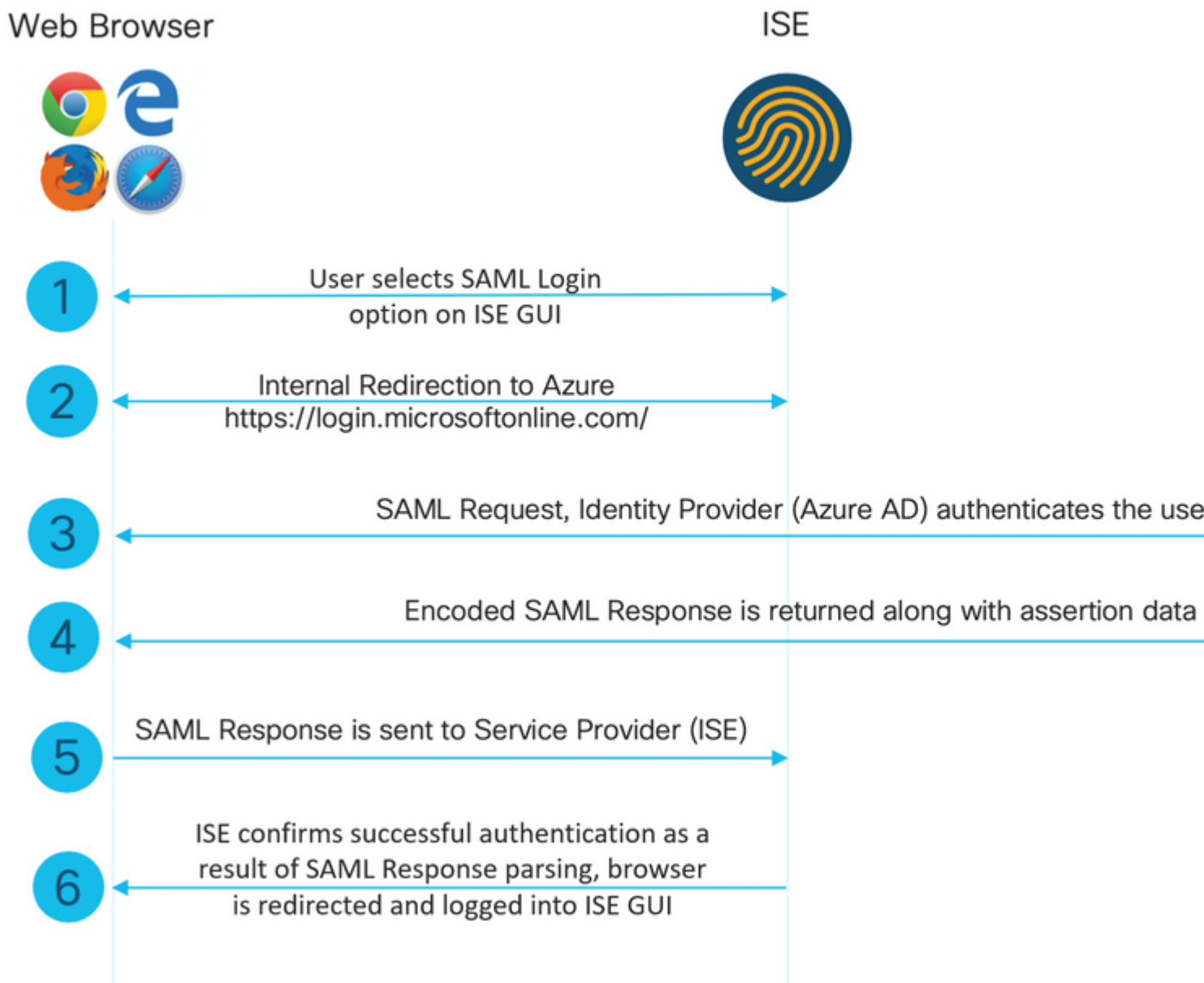
- Verificatiebeweringen bewijzen de identificatie van de gebruiker en geven de tijd aan dat de gebruiker is ingelogd en welke verificatiemethode hij heeft gebruikt (Kerberos, twee-factor, als voorbeelden)
- De attributie bewering geeft de SAML attributen, specifieke stukken gegevens die informatie over de gebruiker geven, door aan de dienstverlener.
- In een autorisatiebesluit wordt verklaard of de gebruiker geautoriseerd is om de service te gebruiken of of dat de identificatieprovider hun verzoek heeft afgewezen vanwege een wachtwoordfout of gebrek aan rechten op de service.

Flow Diagram op hoog niveau

SAML werkt door informatie over gebruikers, logins en attributen door te geven tussen de identiteitsprovider, Azure AD en de serviceprovider, ISE.

Elke gebruiker logt eenmaal in bij een Single Sign-On (SSO) met de identiteitsprovider, dan geeft de Azure AD-provider de SAML-kenmerken door aan ISE wanneer de gebruiker probeert toegang te krijgen tot die diensten.

ISE vraagt autorisatie en verificatie aan bij Azure AD zoals in de afbeelding.



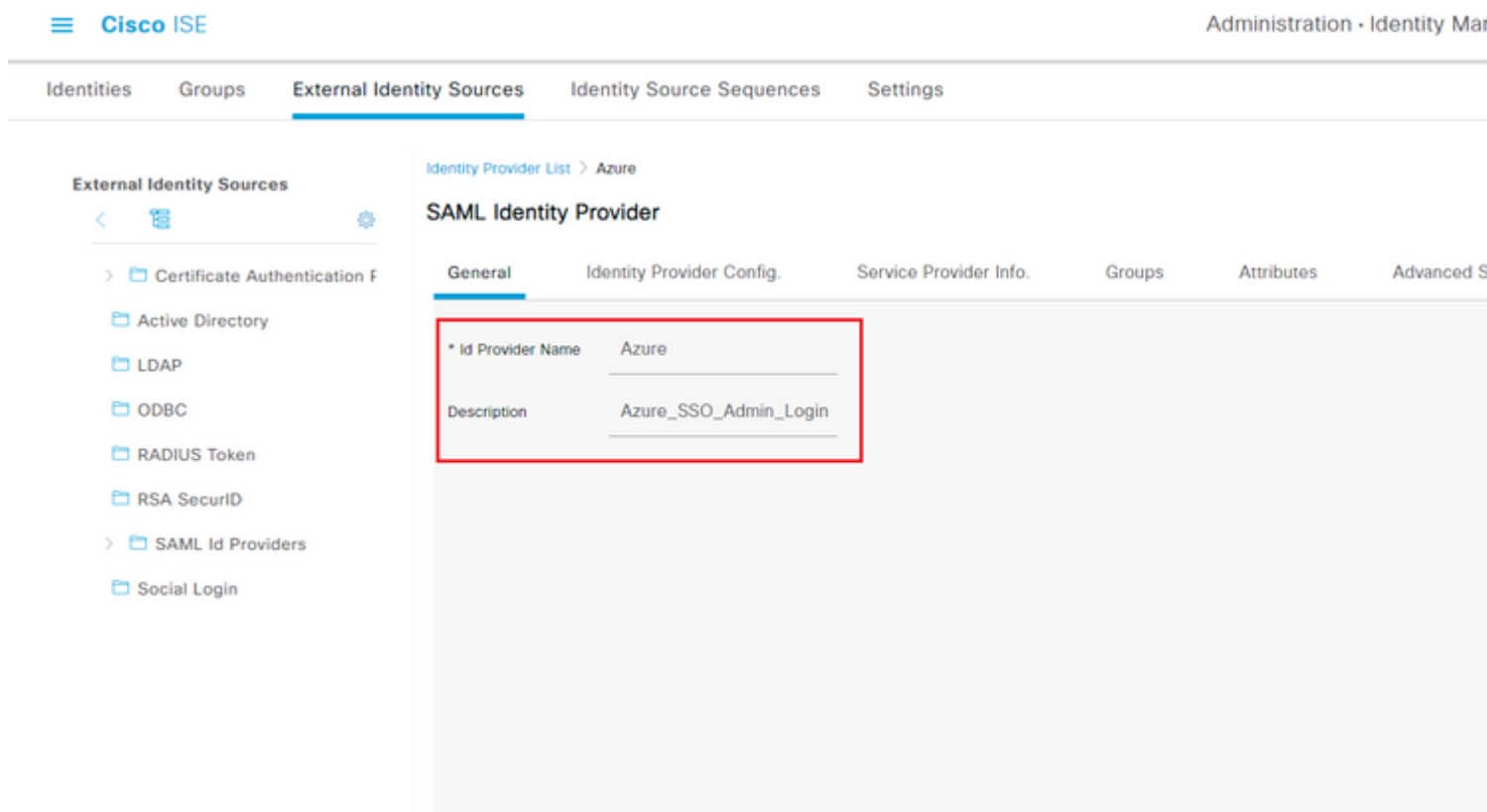
SAML SSO-integratie configureren met Azure AD

Stap 1. SAML Identity Provider configureren op ISE

1. Azure AD configureren als externe SAML Identity Source

Ga op ISE naar **Administration > Identity Management > Externe Identity Sources > SAML ID Providers** en klik op de knop **Add**.

Voer de **naam** van de **ID-provider** in en klik op **Indienen** om deze op te slaan. De **naam van de ID-provider** is alleen belangrijk voor ISE zoals in de afbeelding.



2. ISE-verificatiemethode configureren

Navigeer naar **Beheer >Systeem > Admin Access > Verificatie > Verificatiemethode** en selecteer de keuze **Wachtwoord gebaseerd**.

Selecteer de gewenste naam van de ID-provider die eerder is gemaakt in de vervolgkeuzelijst **Identity Source** zoals in de afbeelding.

- Authentication
- Authorization >
- Administrators >
- Settings >

Authentication Type ⓘ

Password Based

Client Certificate Based

* Identity Source

SAML:Azure



3. Informatie over exportserviceproviders

Ga naar **Beheer > Identiteitsbeheer > Externe Identiteitsbronnen > SAML ID Providers > [Uw SAML Provider]**.

Switch het tabblad naar **Serviceprovider Info.** en klik op de knop **Exporteren** zoals in de afbeelding.

SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

Attribute

Service Provider Information

 Load balancer (i)Export Service Provider Info. (i)[Export](#)

Includes the following portals:

Sponsor Portal (default)

Download het **.xml**-bestand en sla het op. Noteer de URL van de **locatie** en de waarde van **entityID**.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" >
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" >
    <md:KeyDescriptor use="signing" >
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#" >
        <ds:X509Data >
          <ds:X509Certificate >
MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBqkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpT
QU1MX21zZTMtMS0xOjU5a3VtYXN1bWVtAEFw0yMTA3MTkwMzI4MDBaFw0yMTA3MTkwMzI4MDBa
MCUxIzAhBgNVBAMTG1NBTUxfaXN1My0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAG8AMIICGKCAgEAvila4+S0uP3j037yCOXnHAzADupfqcwcp1JQnFxfhVfnDd0ixGRt8iaQ
1zdKhpwF/BsJeSznXyaPVxFcmMFHbmyt46gQ/jjQEyt7YhyohG0t1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDzizyJGKdDPf+1VM5JHCo6UNLFIIfyPmGvcCXnt
NVqsYvxSzF038ciQq1m0sqvrrYzuIUAXDWUNUg9pSGzH0fKsSsZRPxrQh+3N5DEFF1Mzybvm1FYu
9h83g14WJWmizET06Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0ssshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
sDU4u0vFpFvrcC/lavr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBT0+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
kVS9vT4E0zwnGo7pQI8CAwEAAAN9MHswIAAYDVR0RBbkwF4IVaXN1My0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEQUFMAMBAF8wCwYDVR0PBAQDAgLSMB0GA1UdDgQWBBIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwXqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHg0T2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GwlvvcgreC7R46qenaonXVr1tRw11vVIdcf8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUtEi6f0bqr0wCyd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwvt6gFH0bE5luT4EYVuuHwMNGbZqqqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmdh9g2mppbBw0cxzoUxDm+HReSe+0JhRCyIJC0vUpdNmYC8cfAZuiV/e3wk0BLZM
lgV8FTVQSNra9LwHP/PgeNAPUCRPXSwake4rvjvMc0aS/iYdwZhziJ8zBdIBanMv5mGu1nvTET9K
EEwj9ys1IHmdqoH3Em0F0gnzR0RvsMPbJxAoTFjfoITTMdQXNHhg+w1POKXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKWER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMA6XVDj18byhBM7pFGwg4z9YJZGF
```

```
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8E0v7bUMSDmmg/53NoktfJ1CckaWE87myhimj0
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService index="0" Location="https://10.201.232.19:8443/portal/SSOLoginResponse.action" />
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action" />

</md:SPSSODescriptor>
</md:EntityDescriptor>
```

Attributen van belang uit het XML-bestand:

entityID="<http://CiscoISE/100d02da-9457-41e8-87d7-0965b0714db2>"

AssertionConsumer Service Location="<https://10.201.232.19:8443/portal/SSOLoginResponse.action>"

AssertionConsumer Service Location="<https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action>"

Stap 2. Instellingen voor Azure AD IDP configureren

1. Een Azure AD-gebruiker maken

Log in op het Azure Active Directory-beheerdersdashboard en selecteer uw **AD** zoals in de afbeelding.

Azure Active Directory admin center

Dashboard > Default Directory

Default Directory | Overview

Azure Active Directory

Switch tenant Delete tenant Create a tenant What's new

Azure Active Directory can help you enable remote work for your employees and partners.

Default Directory

Search your tenant

Tenant information

Your role
Global administrator [More info](#)

License
Azure AD Premium P2

Tenant ID
64ace648-115d-4ad9-a3bf-7660... [Copy](#)

Primary domain
ekorneyccisco.onmicrosoft.com

Azure AD Connect

Status
Not enabled

Last sync
Sync has never run

Sign-ins

| |
|-----|
| 3 |
| 2.8 |
| 2.6 |
| 2.4 |
| 2.2 |
| 2 |

Aug 23

Selecteer **Gebruikers**, klik op **Nieuwe Gebruiker**, configureer **Gebruikersnaam**, **Naam** en **Eerste Wachtwoord** zoals vereist. Klik op **Maken** zoals in de afbeelding.

Identity

User name * ⓘ

mck ✓

@ gdplab2021.onmicrosoft... ▾



The domain name I need isn't shown here

Name * ⓘ

mck ✓

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password

.....

Show Password

Create

2. Een Azure AD-groep maken

Selecteer **Groepen**. Klik op **Nieuwe groep**.

[Dashboard](#) > [Default Directory](#) > [Groups](#)



Groups | All groups

Default Directory - Azure Active Directory



+ New group



Download groups



Delete



All groups



Deleted groups



Diagnose and solve problems



This page includes previews available for your evaluation



Search groups

Groepstype behouden als **security**. Configureer de **groepsnaam** zoals in de afbeelding.

Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications

Dashboard > TAC > Groups >

New Group

Group type * ⓘ

Security

Group name * ⓘ

ISE Admin Group

Group description ⓘ

Enter a description for the group

Azure AD roles can be assigned to the group ⓘ

Yes

No

Membership type * ⓘ

Assigned

Owners

No owners selected

Members

No members selected

3. Wijs Azure AD-gebruiker toe aan de groep

Klik op **Geen leden geselecteerd**. Kies de gebruiker en klik op **Selecteren**. Klik op **Aanmaken** om de groep te maken waaraan een gebruiker is toegewezen.

Add members



Search ⓘ



mck
mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

Maak een notitie van **Group Object id**, in dit scherm, het is **576c60ec-c0b6-4044-a8ec-d395b1475d6e** voor **ISE Admin Group** zoals in de afbeelding.

Dashboard >

Groups | All groups

TAC - Azure Active Directory

- All groups
- Deleted groups
- Diagnose and solve problems

Settings

- General
- Expiration
- Naming policy

+ New group | Download groups | Delete | Refresh | Columns | Pre

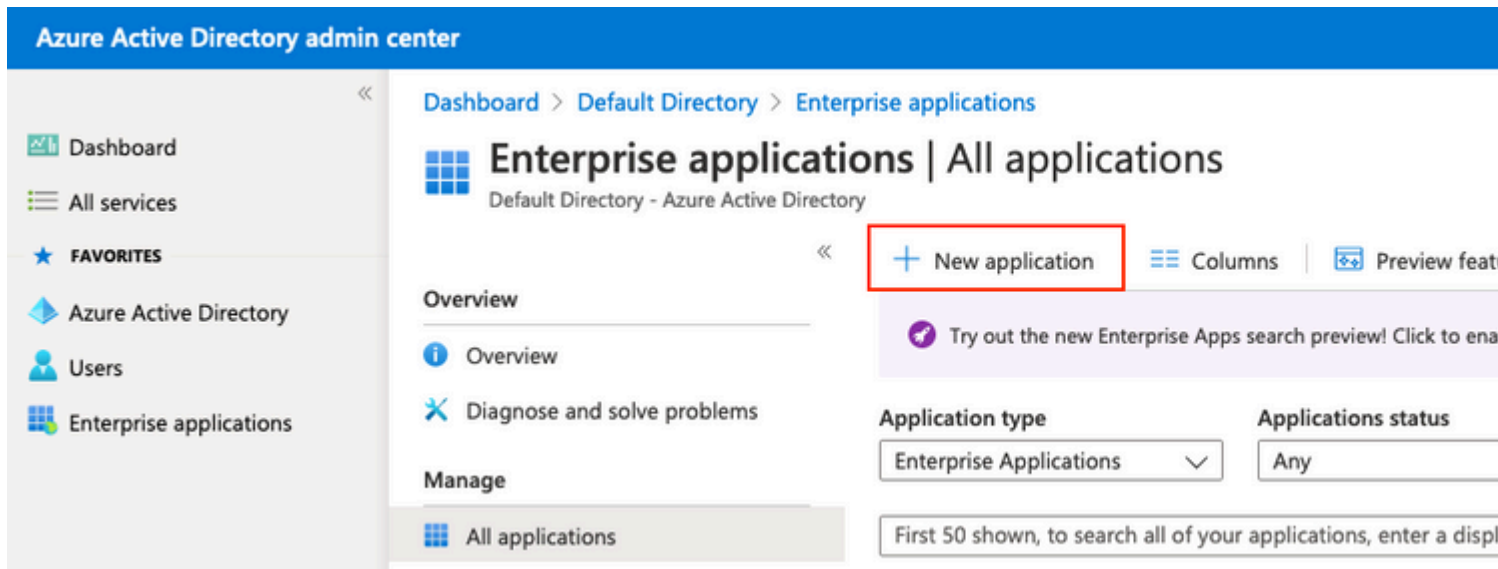
This page includes previews available for your evaluation. View previews →

Search groups | Add filters

| | Name | Object Id | Group Type |
|--------------------------|-----------------|--------------------------------------|------------|
| <input type="checkbox"/> | ISE Admin Group | 576c60ec-c0b6-4044-a8ec-d395b1475d6e | Security |

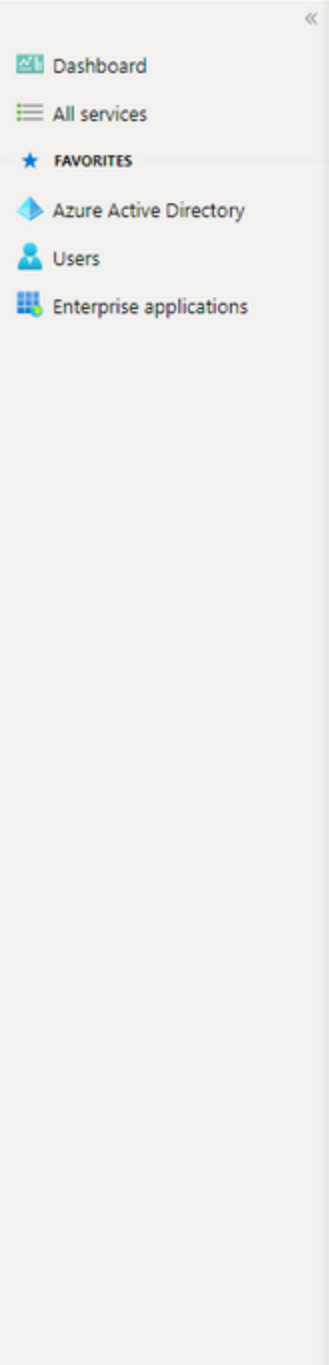
4. Een Azure AD Enterprise-toepassing maken

Selecteer onder AD de optie **Enterprise Application (Enterprise-toepassingen)** en klik op **New application (Nieuwe toepassing)**.



The screenshot shows the Azure Active Directory admin center interface. The left-hand navigation pane includes 'Dashboard', 'All services', 'FAVORITES', 'Azure Active Directory', 'Users', and 'Enterprise applications'. The main content area is titled 'Enterprise applications | All applications' and includes a breadcrumb trail: 'Dashboard > Default Directory > Enterprise applications'. A red box highlights the '+ New application' button. Below this, there are filters for 'Application type' (set to 'Enterprise Applications') and 'Applications status' (set to 'Any'). A notification banner at the top right encourages trying out the new Enterprise Apps search preview.

Selecteer de optie **Uw eigen toepassing maken**.



Browse Azure AD Gallery

[+ Create your own application](#) | [Request new gallery app](#) | [Got feedback?](#)

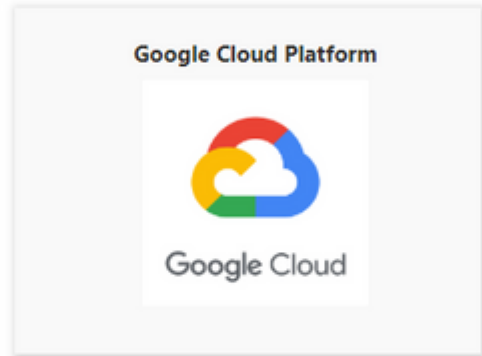
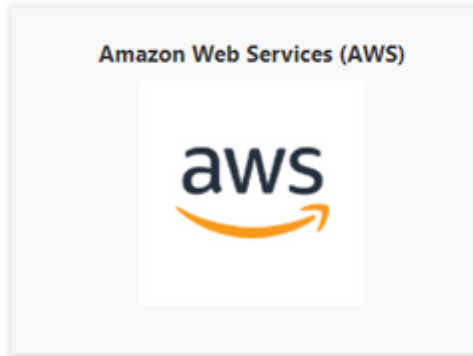
[You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience.](#) →

Single Sign-on : All

User Account Management : All

Category

Cloud platforms



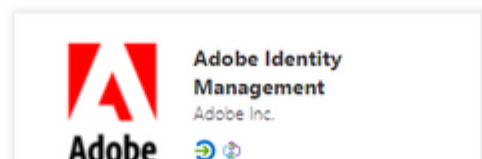
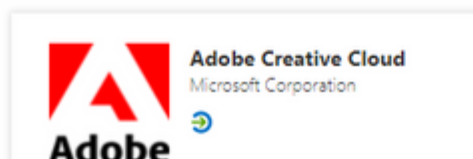
On-premises applications

Add an on-premises application
Configure Azure AD Application Proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure access to your on-premises applications.

[Federated SSO](#) | [Provisioning](#)

Featured applications



Voer de naam van uw toepassing in en selecteer de knop **Integrate een andere toepassing die u niet vindt in de galerij (Non-gallery)** en klik op de knop **Create** zoals getoond in de afbeelding.

Create your own application



What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

Create

5. Voeg groep toe aan de toepassing

Selecteer **Gebruikers en groepen toewijzen**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO | Overview

ISE_3_1_Admin_SSO | Overview

Enterprise Application

Overview

Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access

Properties

Name: ISE_3_1_Admin_SSO

Application ID: 76b82bcb-a918-4016-aad7-...

Object ID: 22aedf32-82c7-47f2-ab34-1...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)

Klik op **Gebruiker/groep toevoegen**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO

ISE_3_1_Admin_SSO | Users and groups

Enterprise Application

+ Add user/group | Edit | Remove | Update Credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

First 200 shown, to search all users & groups, enter a display name.

| Display Name | Object Type |
|--------------|-------------|
|--------------|-------------|

Klik op **Gebruikers en groepen**.

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Add Assignment

Default Directory

Users and groups

None Selected

Select a role

User

Kies de groep die u eerder hebt ingesteld en klik op **Selecteren**.

Opmerking: Selecteer de juiste set gebruikers of groepen die toegang krijgen zoals bedoeld, aangezien de hier genoemde gebruikers en groepen toegang krijgen tot de ISE zodra de installatie is voltooid.

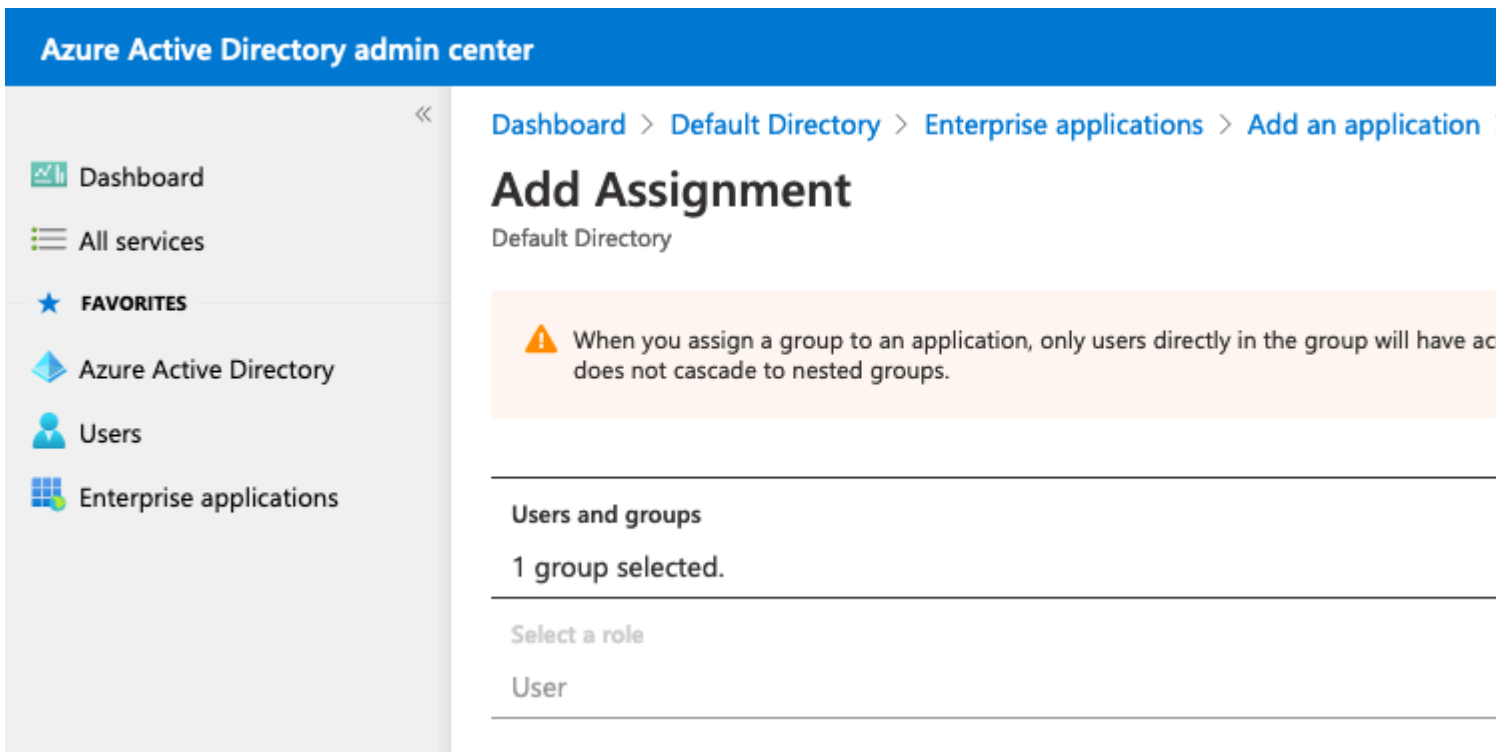
Users and groups

Search

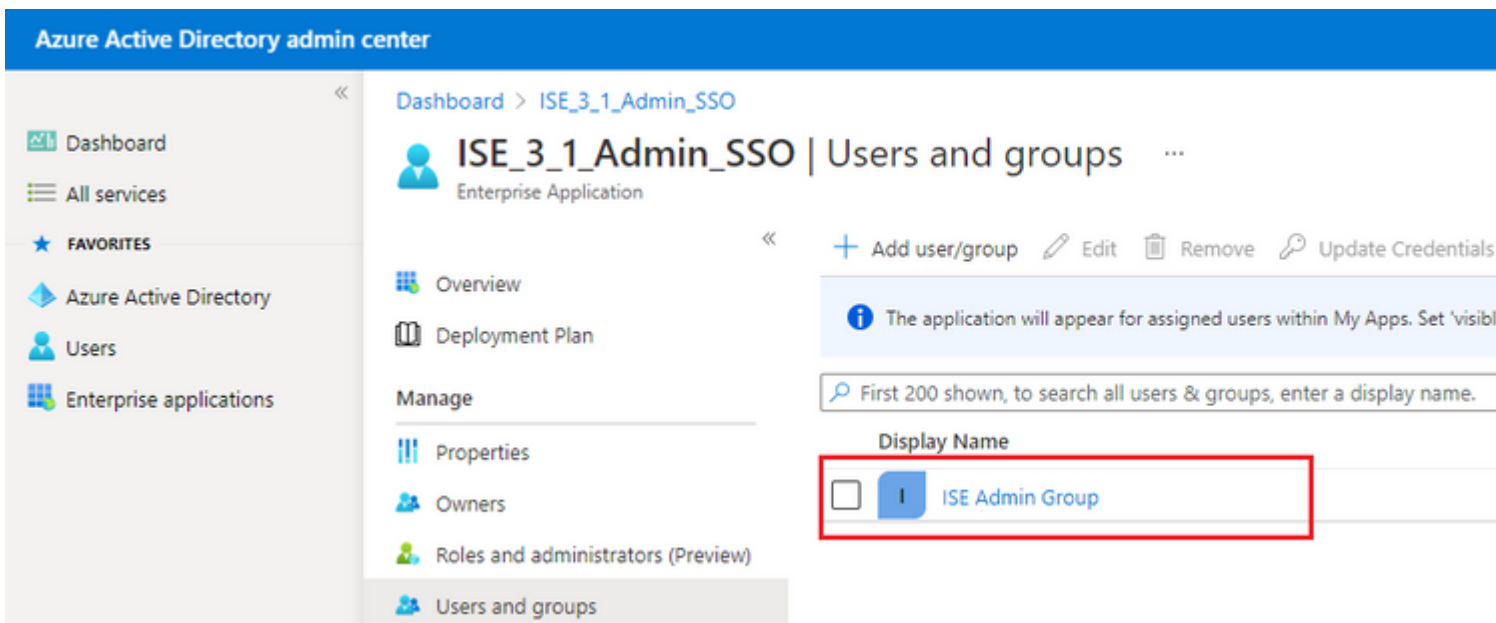
I ISE Admin Group

MC mck
mck@gdplab2021.onmicrosoft.com

Klik op **Toewijzen** nadat de groep is geselecteerd.



Hierdoor wordt het menu **Gebruikers en groepen** voor de geconfigureerde toepassing gevuld met de geselecteerde groep.



6. Een Azure AD Enterprise-toepassing configureren

Navigeer terug naar uw Applicatie en klik op **Enkelvoudige aanmelding instellen**.

Dashboard > Enterprise applications >

ISE_3_1_Admin_SSO | Overview

Enterprise Application

- Overview
- Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access

Properties

| | |
|------------------|------------------------------|
| Name ⓘ | ISE_3_1_Admin_SSO |
| Application ID ⓘ | 76b82bcb-a918-4016-aad7-... |
| Object ID ⓘ | 22aedf32-82c7-47f2-ab34-1... |

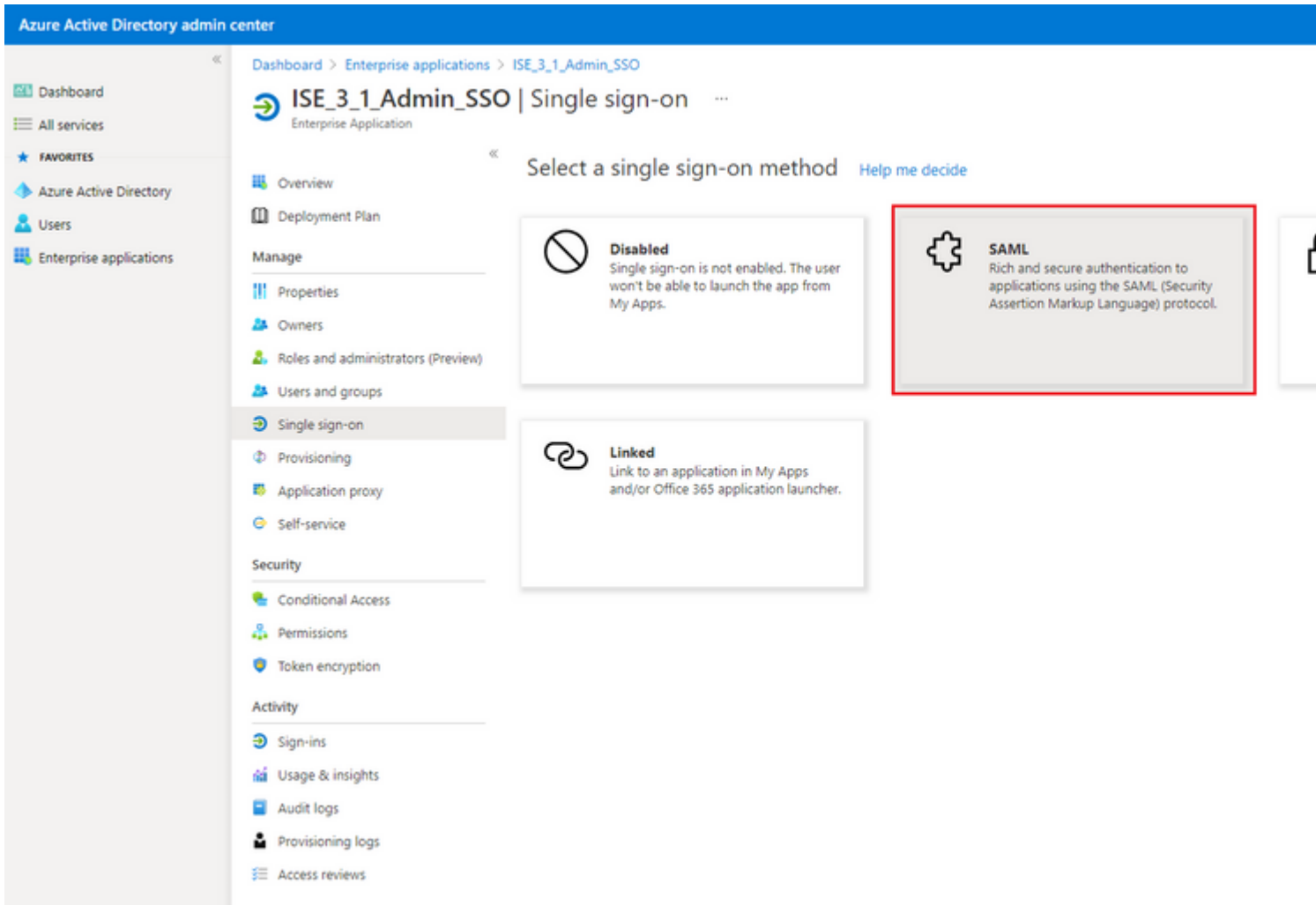
Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)


Selecteer **SAML** op het volgende scherm.




Klik op **Bewerken** naast **Basis SAML Configuration**.

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating ISE30.

1 Basic SAML Configuration  Edit

| | |
|--|-----------------|
| Identifier (Entity ID) | Required |
| Reply URL (Assertion Consumer Service URL) | Required |
| Sign on URL | <i>Optional</i> |
| Relay State | <i>Optional</i> |
| Logout Url | <i>Optional</i> |

2 User Attributes & Claims  Edit

| | |
|------------------------|------------------------|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |

Populate Identifier (Entity ID) met de waarde van **entityID** uit het XML-bestand uit de stap **Export Service Provider Information**. Populate **Reply URL (Assertion Consumer Service URL)** met de waarde van

Locaties van AssertionConsumerService. Klik op Save (Opslaan).

Opmerking: Antwoord URL fungeert als een pass list, die bepaalde URL's toestaat om als bron te fungeren wanneer deze wordt doorgestuurd naar de IdP pagina.

Basic SAML Configuration



 Save

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default



 

Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

Sign on URL

Relay State

Logout Url

7. Active Directory-groepskenmerk configureren

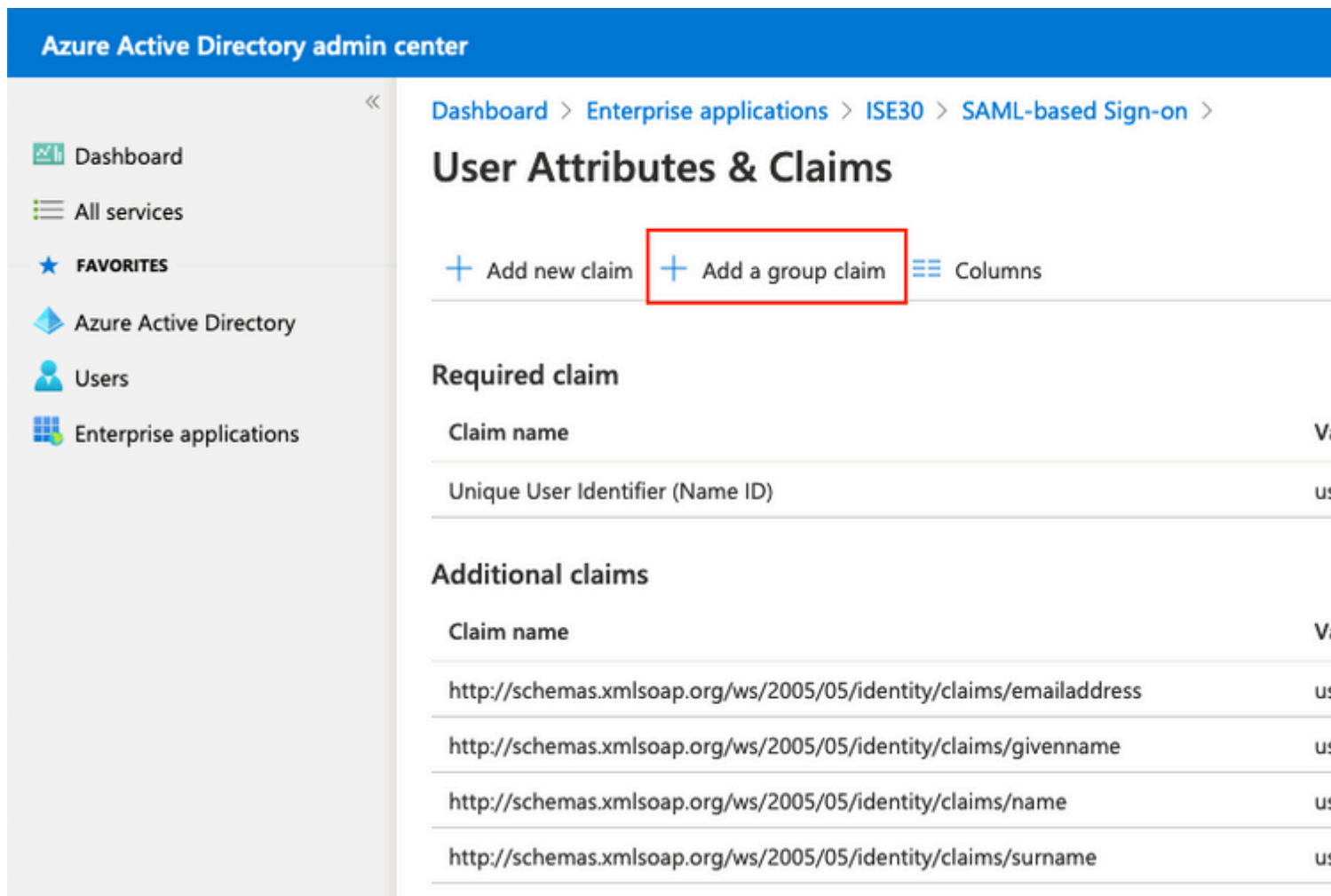
Klik op **Bewerken** naast de **Gebruikerskenmerken & claims** om de eerder ingestelde waarde voor groepsattributen terug te geven.

User Attributes & Claims



| | |
|------------------------|------------------------|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |

Klik op **Een groepsclaim toevoegen**.

A screenshot of the Azure Active Directory admin center interface. The top navigation bar is blue with the text "Azure Active Directory admin center". The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area shows the breadcrumb "Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on > User Attributes & Claims". Below the title, there are two buttons: "Add new claim" and "Add a group claim", with the latter highlighted by a red box. To the right of these buttons is a "Columns" button. Below the buttons, there are two sections: "Required claim" and "Additional claims". The "Required claim" section has a table with one row: "Unique User Identifier (Name ID)". The "Additional claims" section has a table with four rows, each with a claim name and a value type (partially visible as "us").

| Claim name | Value type |
|----------------------------------|------------|
| Unique User Identifier (Name ID) | us |

| Claim name | Value type |
|--|------------|
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | us |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | us |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | us |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | us |

Selecteer **Beveiligingsgroepen** en klik op **Opslaan**. Selecteer **Groep-ID** onder het vervolgkeuzemenu **Bronkenmerken**. Selecteer het aanvinkvakje om de naam van de groepsclaim aan te passen en voer de naam **Groepen in**.

Group Claims



Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

- None
- All groups
- Security groups
- Directory roles
- Groups assigned to the application

Source attribute *

Group ID

Advanced options

- Customize the name of the group claim

Name (required)

Groups

Namespace (optional)

- Emit groups as role claims ⓘ

Noteer de **naam** van de **claim** voor de groep. In dit geval gaat het om **Groepen**.

Azure Active Directory admin center

Dashboard > Enterprise applications > ISE_3_1_Admin_SSO > SAML-based Sign-on > **User Attributes & Claims**

+ Add new claim + Add a group claim Columns

Required claim

| Claim name | Value |
|----------------------------------|--------|
| Unique User Identifier (Name ID) | user.o |

Additional claims

| Claim name | Value |
|--|--------|
| Groups | user.g |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | user.m |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | user.g |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | user.r |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | user.s |

8. Azure Federation Metadata XML-bestand downloaden

Klik op **Downloaden** tegen **Federatie Metadata XML** in **SAML Signing Certificate**.

SAML Signing Certificate Edit

| | |
|--------------------------------|---|
| Status | Active |
| Thumbprint | B24F4BB47B350C93DE3D59EC87EE4C815C884462 |
| Expiration | 7/19/2024, 12:16:24 PM |
| Notification Email | chandandemo@outlook.com |
| App Federation Metadata Url | https://login.microsoftonline.com/182900ec-e960... |
| Certificate (Base64) | Download |
| Certificate (Raw) | Download |
| Federation Metadata XML | Download |

Stap 3. MetaData uploaden van Azure Active Directory naar ISE

Ga naar **Beheer > Identity Management > Externe Identity Resources > SAML ID Providers > [Uw SAML Provider]**.










Switch het tabblad naar **Identity Provider Config.** en klik op **Bladeren**. Selecteer **Federatie Metadata XML** bestand uit stap **Download Azure Federation Metadata XML** en klik op **Opslaan**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - Identity Management'. Below this, there are tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' tab is active, and a sidebar on the left lists various source types: Certificate Authentication F, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The main content area is titled 'SAML Identity Provider' and shows the configuration for an 'Azure' provider. The 'Identity Provider Config.' tab is selected, displaying fields for 'Import Identity Provider Config File' (with a 'Choose File' button), 'Provider Id', 'Single Sign On URL', and 'Single Sign Out URL (Redirect)'. Below these fields is a table titled 'Sianina Certificates' with columns for 'Subject', 'Issuer', 'Valid From', and 'Valid To (Ex)'. One certificate is listed with the subject 'CN=Microsoft Azure Federated SSO Certificate' and an issuer 'CN=Microsoft Azur...'. The table also shows validity dates: 'Mon Jul 19 12:16:2...' and 'Fri Jul 19 12:...'.

Stap 4. SAML-groepen op ISE configureren

Switch naar tab **Groepen** en plak de waarde van **Claim naam** van **Configure Active Directory Group** attribuut in **Group Membership Attribute**.

External Identity Sources

- <  
- >  Certificate Authentication F
-  Active Directory
-  LDAP
-  ODBC
-  RADIUS Token
-  RSA SecurID
- >  SAML Id Providers


Identity Provider List > Azure

SAML Identity Provider

General Identity Provider Config. Service Provider Info. Groups

Groups

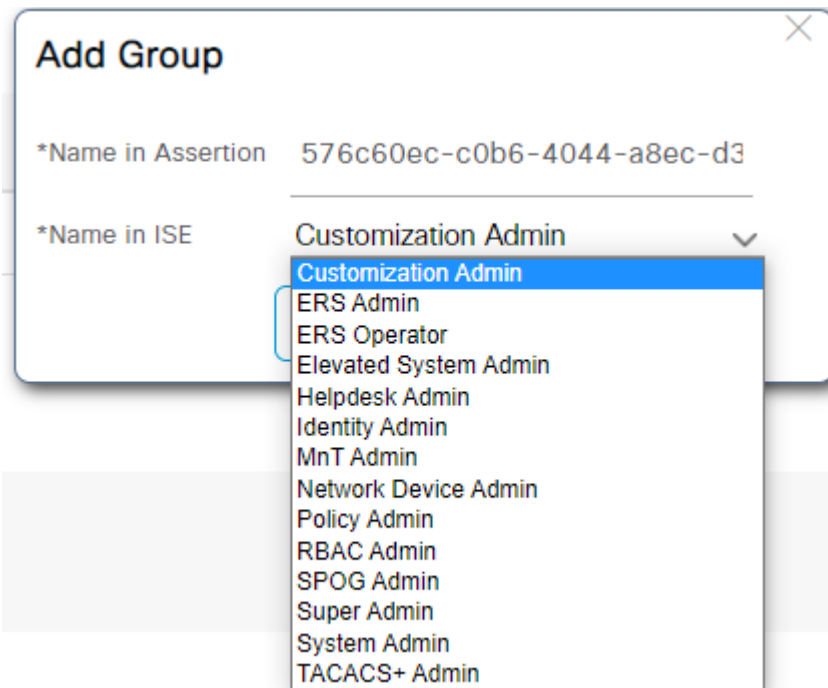
Group Membership Attribute groups

 + Add  Edit  Delete Name in Assertion  Name in

Klik op **Toevoegen**. Naam invullen in **Assertion** met de waarde van **Group Object ID** van **ISE Admin Group** opgenomen in **Toewijzen Azure Active Directory-gebruiker aan de groep**.

Configureer **Naam in ISE** met de vervolgkeuzelijst en selecteer de juiste groep op ISE. In dit voorbeeld is de gebruikte groep **Super Admin**. Klik op **OK**. Klik op **Save (Opslaan)**.

Hiermee wordt een koppeling gemaakt tussen Groep in Azure en Groepsnaam op ISE.



(Optioneel) Stap 5. RBAC-beleid configureren

Van de vorige stap, zijn er vele verschillende types van de niveaus van de gebruikerstoegang die op ISE kunnen worden gevormd.

Als u op rol gebaseerde toegangscontroleregelingen (RBAC) wilt bewerken, gaat u naar **Beheer > Systeem**

> **Admin Access** > **Autorisatie** > **Rechten** > **RBAC-beleid** en configureert u het **beleid** naar wens.

Dit beeld is een verwijzing naar de steekproefconfiguratie.

∨ RBAC Policies

| | Rule Name | Admin Groups | Permissions |
|---------------------------------------|-----------------------------------|-----------------------------------|------------------------------------|
| <input checked="" type="checkbox"/> ∨ | <u>Customization Admin Policy</u> | If <u>Customization Admin</u> + | then <u>Customization Admin M</u> |
| <input checked="" type="checkbox"/> ∨ | <u>Elevated System Admin Poli</u> | If <u>Elevated System Admin</u> + | then <u>System Admin Menu Ac</u> |
| <input checked="" type="checkbox"/> ∨ | <u>ERS Admin Policy</u> | If <u>ERS Admin</u> + | then <u>Super Admin Data Acce</u> |
| <input checked="" type="checkbox"/> ∨ | <u>ERS Operator Policy</u> | If <u>ERS Operator</u> + | then <u>Super Admin Data Acce</u> |
| <input checked="" type="checkbox"/> ∨ | <u>ERS Trustsec Policy</u> | If <u>ERS Trustsec</u> + | then <u>Super Admin Data Acce</u> |
| <input checked="" type="checkbox"/> ∨ | <u>Helpdesk Admin Policy</u> | If <u>Helpdesk Admin</u> + | then <u>Helpdesk Admin Menu A</u> |
| <input checked="" type="checkbox"/> ∨ | <u>Identity Admin Policy</u> | If <u>Identity Admin</u> + | then <u>Identity Admin Menu Ac</u> |
| <input checked="" type="checkbox"/> ∨ | <u>MnT Admin Policy</u> | If <u>MnT Admin</u> + | then <u>MnT Admin Menu Acces</u> |
| <input checked="" type="checkbox"/> ∨ | <u>Network Device Policy</u> | If <u>Network Device Admin</u> + | then <u>Network Device Menu A</u> |
| <input checked="" type="checkbox"/> ∨ | <u>Policy Admin Policy</u> | If <u>Policy Admin</u> + | then <u>Policy Admin Menu Acc</u> |
| <input checked="" type="checkbox"/> ∨ | <u>RBAC Admin Policy</u> | If <u>RBAC Admin</u> + | then <u>RBAC Admin Menu Acc</u> |
| <input checked="" type="checkbox"/> ∨ | <u>Read Only Admin Policy</u> | If <u>Read Only Admin</u> + | then <u>Super Admin Menu Acc</u> |
| <input checked="" type="checkbox"/> ∨ | <u>SPOG Admin Policy</u> | If <u>SPOG Admin</u> + | then <u>Super Admin Data Acce</u> |
| <input checked="" type="checkbox"/> ∨ | <u>Super Admin Policy</u> | If <u>Super Admin</u> + | then <u>Super Admin Menu Acc</u> |
| <input checked="" type="checkbox"/> ∨ | <u>Super Admin_Azure</u> | If <u>Super Admin</u> + | then <u>Super Admin Menu Acc</u> |
| <input checked="" type="checkbox"/> ∨ | <u>System Admin Policy</u> | If <u>System Admin</u> + | then <u>System Admin Menu Ac</u> |
| <input checked="" type="checkbox"/> ∨ | <u>TACACS+ Admin Policy</u> | If <u>TACACS+ Admin</u> + | then <u>TACACS+ Admin Menu</u> |

Verifiëren

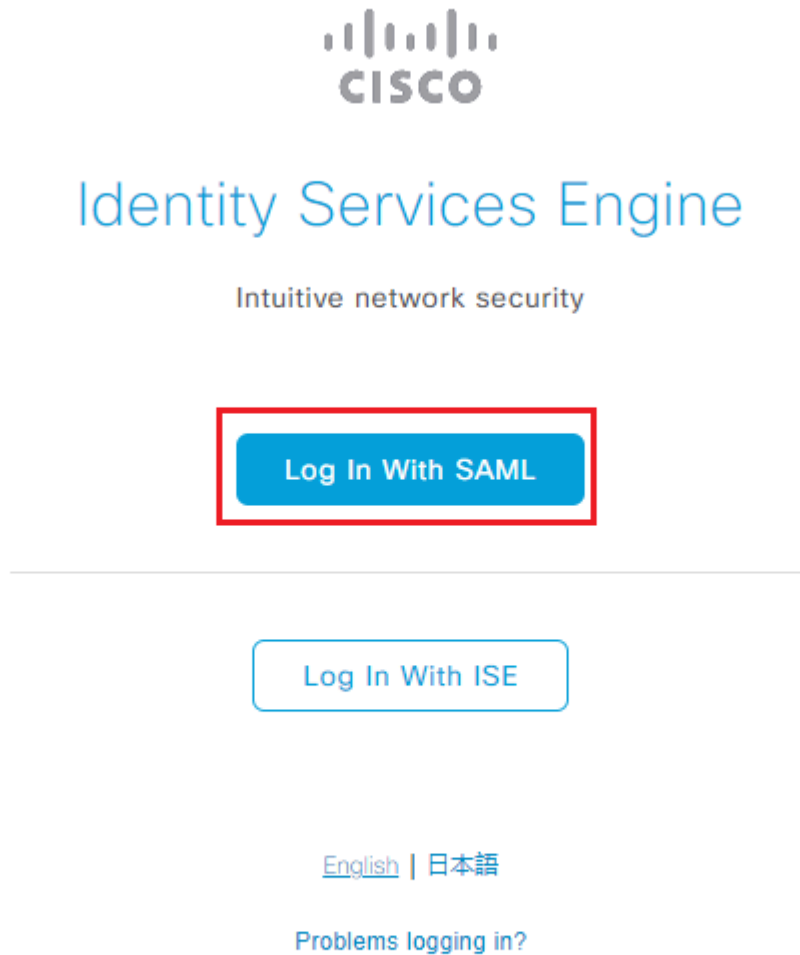
Bevestig dat uw configuratie correct werkt.

Opmerking: SAML SSO Login test van de Azure testfunctionaliteit werkt niet. Het SAML-verzoek

moet door ISE worden geïnitieerd om de Azure SAML SSO correct te laten werken.

Open het aanloopscherm voor ISE GUI. U krijgt een nieuwe optie om in te **loggen met SAML**.

1. Open de inlogpagina van de ISE GUI en klik op **Inloggen met SAML**.



2. U wordt omgeleid naar het Microsoft-inlogscherm. Voer uw **gebruikersnaam** in voor een account in een groep die is toegewezen aan ISE, zoals hier wordt getoond, en klik op **Volgende** zoals in de afbeelding.



Sign in

mck@gdplab2021.onmicrosoft.com

[Can't access your account?](#)

Next

3. Voer uw **wachtwoord** voor de gebruiker in en klik op **Inloggen**.



← mck@gdplab2021.onmicrosoft.com

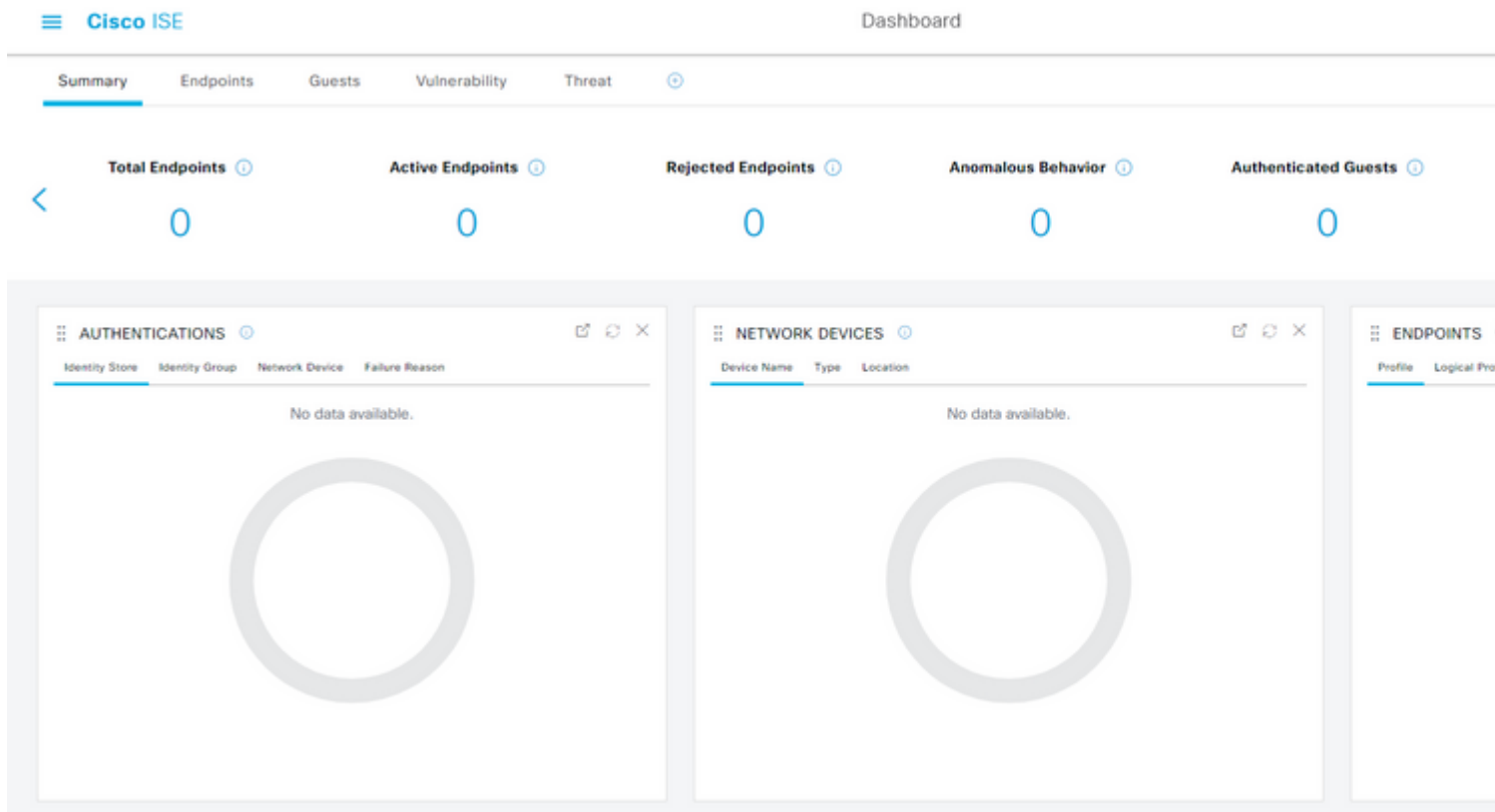
Enter password

.....

[Forgot my password](#)

Sign in

4. U wordt nu doorgestuurd naar het ISE-toepassingsdashboard met de juiste rechten die zijn ingesteld op basis van de eerder geconfigureerde ISE-groep zoals in de afbeelding.



Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Veelvoorkomende problemen

Het is belangrijk om te begrijpen dat SAML-verificatie wordt afgehandeld tussen de browser en de Azure Active Directory. Daarom kunt u verificatiegerelateerde fouten rechtstreeks opvragen bij de Identity Provider (Azure), waar de ISE-overeenkomst nog niet is gestart.

Probleem 1. "Uw account of wachtwoord is onjuist" fout wordt gezien nadat u de aanmeldingsgegevens hebt ingevoerd. Hier worden gebruikersgegevens nog niet door ISE ontvangen en blijft het proces op dit punt nog steeds bij IdP (Azure).

De meest waarschijnlijke reden is dat de accountinformatie onjuist is of dat het wachtwoord niet juist is. Om te repareren: stel het wachtwoord opnieuw in of geef het juiste wachtwoord op voor die account zoals in de afbeelding.



← mck@gdplab2021.onmicrosoft.com

Enter password

Your account or password is incorrect. If you don't remember your password, [reset it now](#).

Password

[Forgot my password](#)

Sign in

Probleem 2. De gebruiker maakt geen deel uit van de groep die toegang zou moeten krijgen tot SAML SSO. Net als bij de vorige case worden gebruikersgegevens nog niet door ISE ontvangen en blijft het proces op dit punt nog steeds bij IdP (Azure).

Om dit op te lossen: controleer of de **Add groep aan de Application** configuratie stap correct wordt uitgevoerd zoals in het afbeelding.



Sign in

Sorry, but we're having trouble signing you in.

AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Troubleshooting details ✕

If you contact your administrator, send this info to them.

[Copy info to clipboard](#)

Request Id: 1e15cea0-c349-4bee-922d-26299822a101

Correlation Id: 710626e0-45c1-4fad-baa6-ff7584ecf910

Timestamp: 2021-08-04T22:48:02Z

Message: AADSTS50105: The signed in user 'userwithoutgroup@gdplab2021.onmicrosoft.com' is not assigned to a role for the application '76b82bcb-a918-4016-aad7-b43bc4326254'(ISE_3_1_Admin_SSO).

Flag sign-in errors for review: [Enable flagging](#)

If you plan on getting help for this problem, enable flagging and try to reproduce the error within 20 minutes. Flagged events make diagnostics available and are raised to admin attention.

Probleem 3. ISE Application Server kan geen SAML-aanmeldingsverzoeken verwerken. Dit probleem doet zich voor wanneer het SAML-verzoek wordt geïnitieerd door de Identity Provider, Azure, in plaats van de Service Provider, ISE. Het testen van SSO Login van Azure AD werkt niet omdat ISE geen ondersteuning biedt voor door SAML geïnitieerde identiteitsprovider-verzoeken.



This page isn't working

10.201.232.19 is currently unable to handle this request.

HTTP ERROR 500

ISE_3_1_Admin_SSO | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators (Preview)
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews

Upload metadata file | Change single sign-on mode | Test this application

| | |
|------------------------|------------------------|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Groups | user.groups |
| Unique User Identifier | user.userprincipalname |

3 SAML Signing Certificate

| | |
|-----------------------------|---------------------------------------|
| Status | Active |
| Thumbprint | 824F4BB47B350C93DE3D59EC87EE4C8 |
| Expiration | 7/19/2024, 12:16:24 PM |
| Notification Email | chandandemo@outlook.com |
| App Federation Metadata Url | https://login.microsoftonline.com/182 |
| Certificate (Base64) | Download |
| Certificate (Raw) | Download |
| Federation Metadata XML | Download |

4 Set up ISE_3_1_Admin_SSO

You'll need to configure the application to link with Azure AD.

| | |
|---------------------|---------------------------------------|
| Login URL | https://login.microsoftonline.com/182 |
| Azure AD Identifier | https://sts.windows.net/182900ec-e96 |
| Logout URL | https://login.microsoftonline.com/182 |

[View step-by-step instructions](#)

5 Test single sign-on with ISE_3_1_Admin_SSO

Test to see if single sign-on is working. Users will need to be added to Users and group

Test single sign-on with ISE_3_1_Admin_SSO

Got feedback?

Microsoft recommends installing the My Apps Secure Sign-in Extension to allow third-party cookies if you have installed it but this message

Please make sure you have configured ISE_3_1_Admin_SSO before

(requires browser)

Resolving errors
If you encounter an error in the sign-in page, please paste it below and retry.

What does the error look like? [?](#)

```
Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation Id: Saa879f5-68f1-482a-a405-ff993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXX
```

[Get resolution guidance](#)

Probleem 4. ISE geeft "Access Denied"-fout weer na een inlogpoging. Deze fout doet zich voor wanneer de claimnaam van de groep die eerder in de Azure Enterprise Application is gemaakt, niet overeenkomt in ISE.

Om dit te verhelpen: zorg ervoor dat de naam van de groepsclaim in Azure en ISE onder het tabblad SAML Identity Provider Groups hetzelfde zijn. Raadpleeg de stappen 2.7 en 4. onder het gedeelte **SAML SSO configureren met Azure AD** van dit document voor meer informatie.



Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

Probleemoplossing ISE

Log niveau van de componenten hier moet worden gewijzigd op **ISE**. Navigeer naar **Operations > Probleemoplossing > Wizard Debug > Configuratie debug log**.

| Naam van component | Logniveau | Logbestandsnaam |
|--------------------|-----------|-----------------|
| deuropening | DEBUGGEN | guest.log |

| | | |
|----------|----------|-------------|
| opensaml | DEBUGGEN | ise-psc.log |
| klein | DEBUGGEN | ise-psc.log |

Logbestanden met SAML Login en Mismatched Group Claim Names

De reeks van debugs toont de wanverhouding van de eisennaam het oplossen van probleemscenario op het tijdstip van stroomuitvoering (ise-psc.log).

Opmerking: Houd **vetgedrukte** items in de gaten. Logbestanden zijn ingekort omwille van de duidelijkheid.

1. Gebruiker wordt doorgestuurd naar IDp URL vanaf ISE-beheerpagina.

<#root>

```
2021-07-29 13:48:20,709 INFO [admin-http-pool46][] api.services.persistence.dao.DistributionDAO -:::
2021-07-29 13:48:20,712 INFO [admin-http-pool46][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::
```

forwardStr for: <https://10.201.232.19/admin/LoginAction.do>

```
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
```

IDP URL: <https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2>

```
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,839 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
```

SAML request - spUrlToReturnTo:<https://10.201.232.19:8443/portal/SSOLoginResponse.action>

```
2021-07-29 13:48:20,844 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:20,851 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAML
```

2. SAML-antwoord wordt ontvangen van de browser.

<#root>

```
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,172 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
```

-:::- Decoded SAML relay state of: `_0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2`

```
2021-07-29 13:48:27,177 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decoder
```

-:::- Decoded SAML message

```
2021-07-29 13:48:27,182 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.saml2.binding.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.ws.message.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
opensaml.common.binding.decoder.BaseSAMLMessageDecoder -:::- Intended message destination endpoint: https://...
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decoder
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
```

3. Het ontleden van een kenmerk (bewering) is gestart.

<#root>

```
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
```

[parseAttributes] Set on IdpResponse object - attribute<<http://schemas.xmlsoap.org/ws/2005/05/identity/>>

```
2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
```

4. Het kenmerk Group wordt ontvangen met de waarde **576c60ec-c0b6-4044-a8ec-d395b1475d6e**, ondertekening validatie.

```
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML
```

```

2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
    IdP URI: https://sts.windows.net/182900ec-e960-4340-bd20-e4522197ecf8/
    SP URI: http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd
    Assertion Consumer URL: https://10.201.232.19:8443/portal/SSOloginResponse.action
    Request Id: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a2fd-7047-4d1d-8907-5a05a94ff5fd
    Client Address: 10.24.226.171
    Load Balancer: null
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validato
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,358 INFO [admin-http-pool50][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImpl

```

5. validering van RBAC-vergunningen.

```
<#root>
```

```

*****Rbac Log Summary for user samlUser*****
2021-07-29 13:48:27,360 INFO [admin-http-pool50][] com.cisco.ise.util.RBACUtil -:::- Populating cache
2021-07-29 13:48:27,368 ERROR [admin-http-pool50][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::-

java.lang.NullPointerException

2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.action.LoginAction -:::- In Login
2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.action.LoginAction -:::- In Login
2021-07-29 13:48:27,369 ERROR [admin-http-pool50][] cpm.admin.infra.action.LoginAction -:::- Can't sav
2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.action.LoginActionResultHandler -:::-

```

2021-07-29 13:48:27,369 INFO [admin-http-pool50][] cpm.admin.infra.spring.ISEAdminControllerUtils -:::

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.