

# Konfigurieren von ISE 3.1 ISE-GUI-Admin-Anmeldeablauf über SAML SSO-Integration mit Azure AD

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Identitätsanbieter \(IdP\)](#)

[Service Provider](#)

[SAML](#)

[SAML-Assertion](#)

[Übergeordnetes Flussdiagramm](#)

[Konfigurieren der SAML-SSO-Integration mit Azure AD](#)

[Schritt 1: Konfiguration des SAML Identity Providers auf der ISE](#)

[1. Azure AD als externe SAML-Identitätsquelle konfigurieren](#)

[2. Konfigurieren der ISE-Authentifizierungsmethode](#)

[3. Exportieren von Informationen zu Service Providern](#)

[Schritt 2: Azure AD IDp-Einstellungen konfigurieren](#)

[1. Erstellen Sie einen Azure AD-Benutzer](#)

[2. Erstellen einer Azure AD-Gruppe](#)

[3. Azure AD-Benutzer der Gruppe zuweisen](#)

[4. Erstellen einer Azure AD-Enterprise-Anwendung](#)

[5. Gruppe zur Anwendung hinzufügen](#)

[6. Konfigurieren einer Azure AD-Enterprise-Anwendung](#)

[7. Active Directory-Gruppenattribut konfigurieren](#)

[8. Azure Federation Metadaten-XML-Datei herunterladen](#)

[Schritt 3: Hochladen von Metadaten aus Azure Active Directory in die ISE](#)

[Schritt 4: Konfigurieren von SAML-Gruppen auf der ISE](#)

[\(Optional\) Schritt 5: RBAC-Richtlinien konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Häufige Probleme](#)

[Fehlerbehebung bei ISE](#)

[Protokolle mit SAML-Anmeldung und nicht übereinstimmenden Gruppenansprachenamen](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie die Cisco ISE 3.1 SAML SSO-Integration mit einem externen Identitätsanbieter wie Azure Active Directory (AD) konfigurieren.

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

## **Verwendete Komponenten**

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

1. Cisco ISE 3.1
2. Azure AD

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## **Hintergrundinformationen**

### **Identitätsanbieter (IdP)**

In diesem Fall überprüft und bestätigt Azure AD eine Benutzeridentität und Zugriffsrechte für eine angeforderte Ressource (den "Dienstanbieter").

### **Service Provider**

Die gehostete Ressource oder der gehostete Dienst, auf die bzw. den der Benutzer zugreifen möchte, in diesem Fall der ISE-Anwendungsserver.

### **SAML**

Security Assertion Markup Language (SAML) ist ein offener Standard, der IdP zum Übergeben von Autorisierungsdaten an SP zulässt.

SAML-Transaktionen verwenden Extensible Markup Language (XML) für die standardisierte Kommunikation zwischen Identitätsanbieter und Dienstanbieter.

SAML ist die Verbindung zwischen der Authentifizierung einer Benutzeridentität und der Autorisierung zur Nutzung eines Dienstes.

### **SAML-Assertion**

Eine SAML-Assertion ist das XML-Dokument, das der Identitätsanbieter an den Dienstanbieter sendet, der die Benutzerautorisierung enthält.

Es gibt drei verschiedene Arten von SAML-Assertionen: Authentifizierung, Attribut und Autorisierungsentscheidung.

- Authentifizierungsassertionen belegen die Identifizierung des Benutzers und geben die Zeit an, zu der sich der Benutzer angemeldet hat, sowie die verwendete Authentifizierungsmethode (z. B. Kerberos, zweistufig).

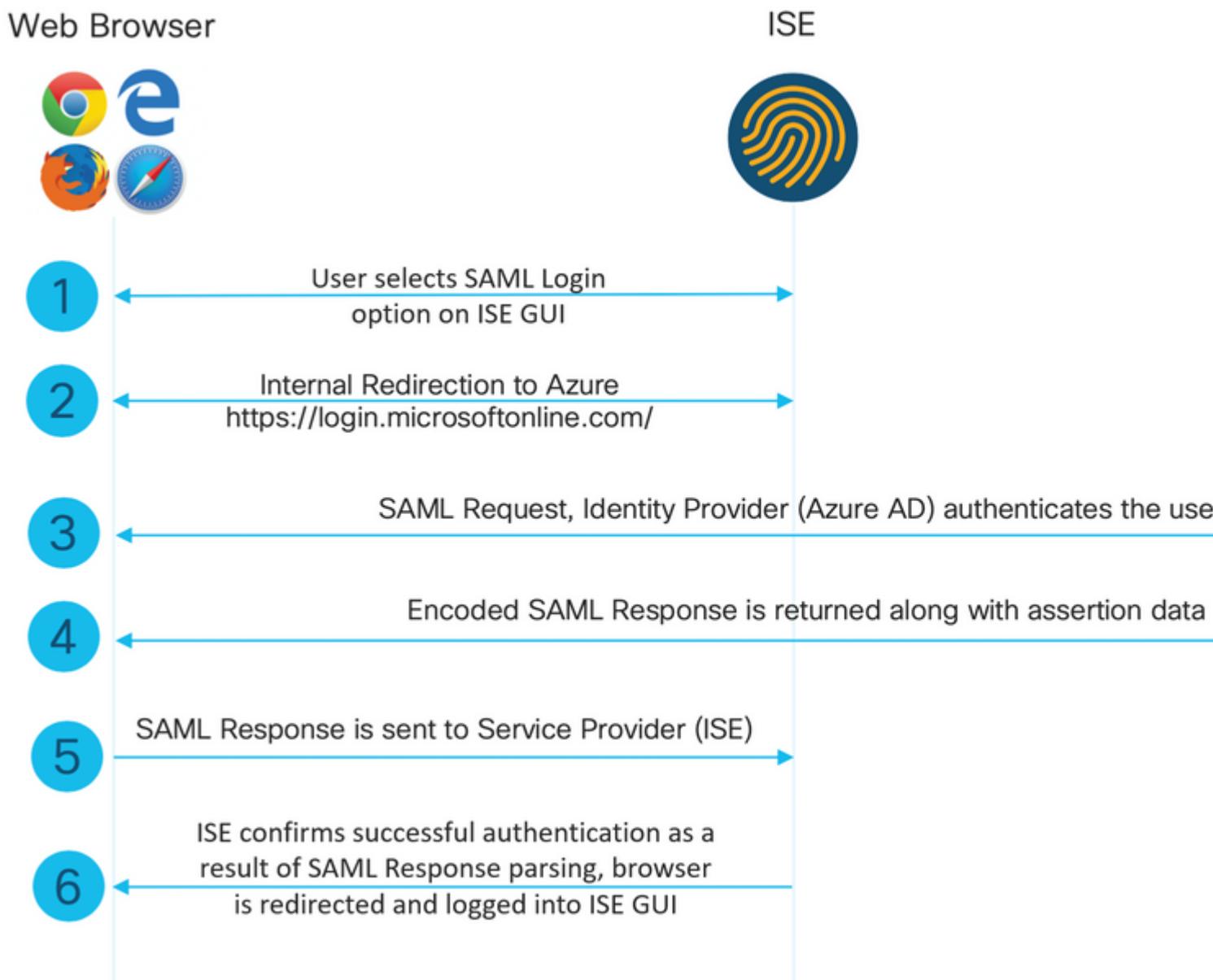
- Die Attributassertion übergibt die SAML-Attribute, d. h. bestimmte Datenelemente, die Informationen über den Benutzer bereitstellen, an den Service Provider.
- Eine Autorisierungsentscheidungsbestätigung gibt an, ob der Benutzer zur Nutzung des Dienstes autorisiert ist oder ob der identifizierende Anbieter seine Anfrage aufgrund eines Kennwortfehlers oder fehlender Rechte für den Dienst abgelehnt hat.

## Übergeordnetes Flussdiagramm

SAML übergibt Informationen über Benutzer, Anmeldungen und Attribute zwischen dem Identitätsanbieter Azure AD und dem Dienstanbieter ISE.

Jeder Benutzer meldet sich einmal bei einer einmaligen Anmeldung (Single Sign-On, SSO) beim Identitätsanbieter an. Anschließend übergibt der Azure AD-Anbieter die SAML-Attribute an die ISE, wenn der Benutzer versucht, auf diese Dienste zuzugreifen.

ISE fordert Autorisierung und Authentifizierung von Azure AD an, wie im Bild dargestellt.



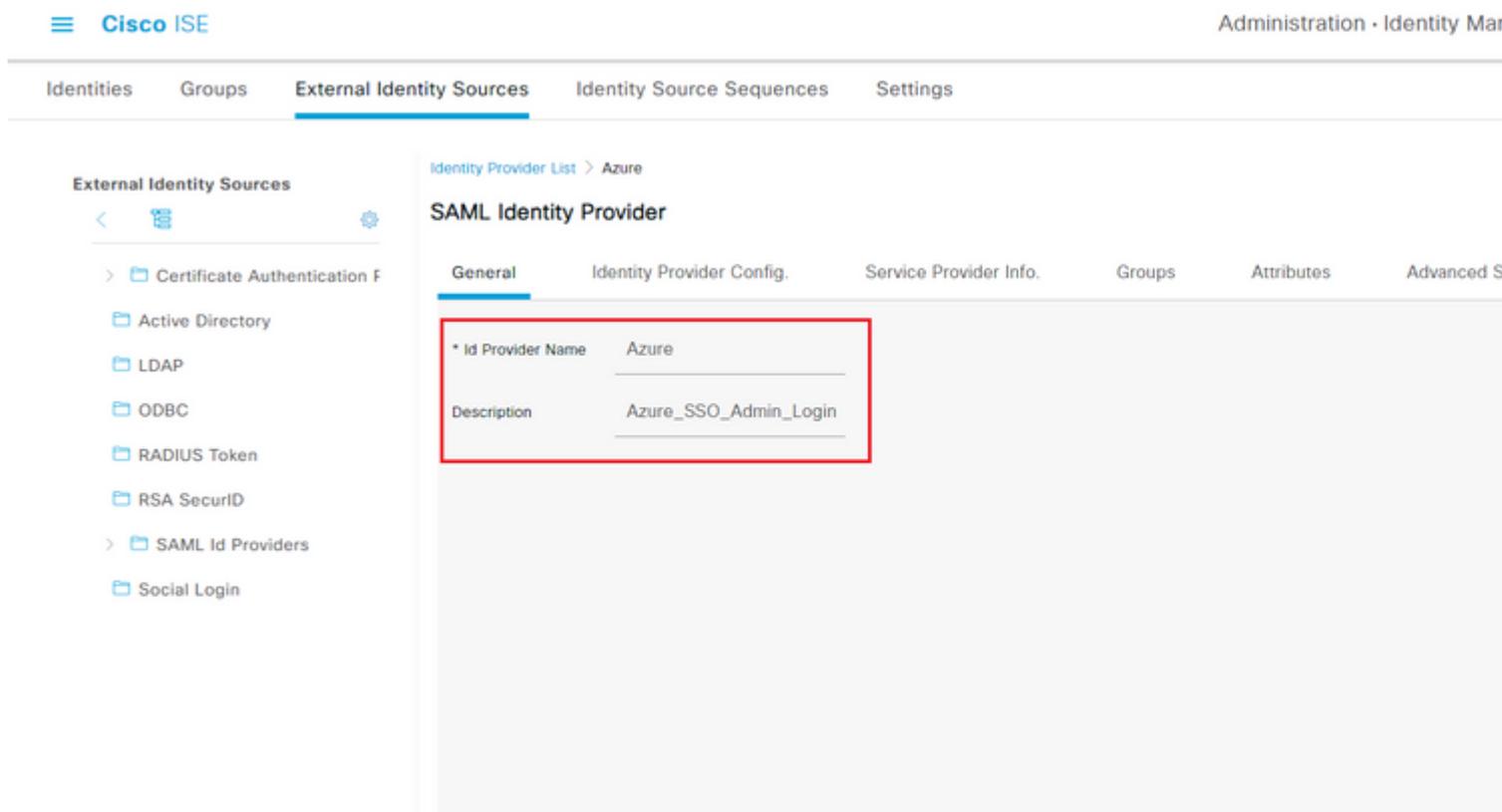
# Konfigurieren der SAML-SSO-Integration mit Azure AD

## Schritt 1: Konfiguration des SAML Identity Providers auf der ISE

### 1. Azure AD als externe SAML-Identitätsquelle konfigurieren

Navigieren Sie auf der ISE zu **Administration > Identity Management > External Identity Sources > SAML Id Providers**, und klicken Sie auf die Schaltfläche **Add (Hinzufügen)**.

Geben Sie den **ID-Anbiaternamen ein**, und klicken Sie auf **Senden**, um ihn zu speichern. Der **ID-Anbietername** ist nur für die ISE relevant, wie im Bild gezeigt.



### 2. Konfigurieren der ISE-Authentifizierungsmethode

Navigieren Sie zu **Administration > System > Admin Access > Authentication > Authentication Method**, und wählen Sie das Optionsfeld **Password Based (Passwortbasiert)** aus.

Wählen Sie den zuvor erstellten erforderlichen ID-Anbiaternamen aus der Dropdown-Liste **Identitätsquelle** aus, wie im Bild dargestellt.

- Authentication
- Authorization >
- Administrators >
- Settings >

Authentication Type ⓘ

Password Based

Client Certificate Based

\* Identity Source

SAML:Azure



### 3. Exportieren von Informationen zu Service Providern

Navigieren Sie zu **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]**.

Wechseln Sie zur Registerkarte **Service Provider Info.**, und klicken Sie auf die Schaltfläche **Exportieren**, wie in der Abbildung dargestellt.

## SAML Identity Provider

General Identity Provider Config. **Service Provider Info.** Groups Attribute

Service Provider Information

Load balancer i

---

Export Service Provider Info. Export i

**Includes the following portals:**

Sponsor Portal (default)

Laden Sie die **.xml**-Datei herunter, und speichern Sie sie. Notieren Sie sich die **Standort**-URL und den **entityID**-Wert.

```
<?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" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:2.0:protocol.xsd">
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:2.0:protocol.xsd">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDEExpT
QU1MX21zZTMtMS0xOS5ja3VtYXlYLnNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yMTA3MTkwMzI4MDBa
MCUxIzAhBgNVBAMTG1NBTUxfaXNlMy0xLkTE5LmNrdW1hcjIuYy29tMIICijANBgkqhkiG9w0BAQEF
AAOCAg8AMIICGKCAgEAvila4+S0uP3j037yCOXnHAzADupfqcgcwplJQnFxfvfnDd0ixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohG0t1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0czJmiDzizyJGKDDPf+1VM5JHCo6UNLFIIfyPmGvcCXnt
NVqsYvxSzF038ciQlmsqrVrryZuIUAXDWUNUg9pSGzH0FkSsZRPxrQh+3N5DEFF1Mzybvm1FYu
9h83gL4WJWmizET06Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0sshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
sDU4u0vFpFvrcC/lavr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBT0+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
kVS9vT4E0zwNGo7pQI8CAwEAAAN9MhswIAYDVR0RBbkwF4IVaXNlMy0xLkTE5LmNrdW1hcjIuYy29t
MAwGA1UdEwQFMAMBAF8wCwYDVR0PBAQDAgLSMB0GA1UdDgQWBBRikY2z/9H9PpwSn0PGARCj5iaZ
oDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEMBQADggIBAIE6mNB
L206Dkb6fHdgKd9goN8N2bj+34ybwxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+Gw1vcgreC7R46qenaonXVr1tRw11vVIIdCf8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUtEi6f0bqr0wCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gfH0bE5luT4EYVuuHiwMNGbZqqqb+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>
```

Interessante Attribute aus der XML-Datei:

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

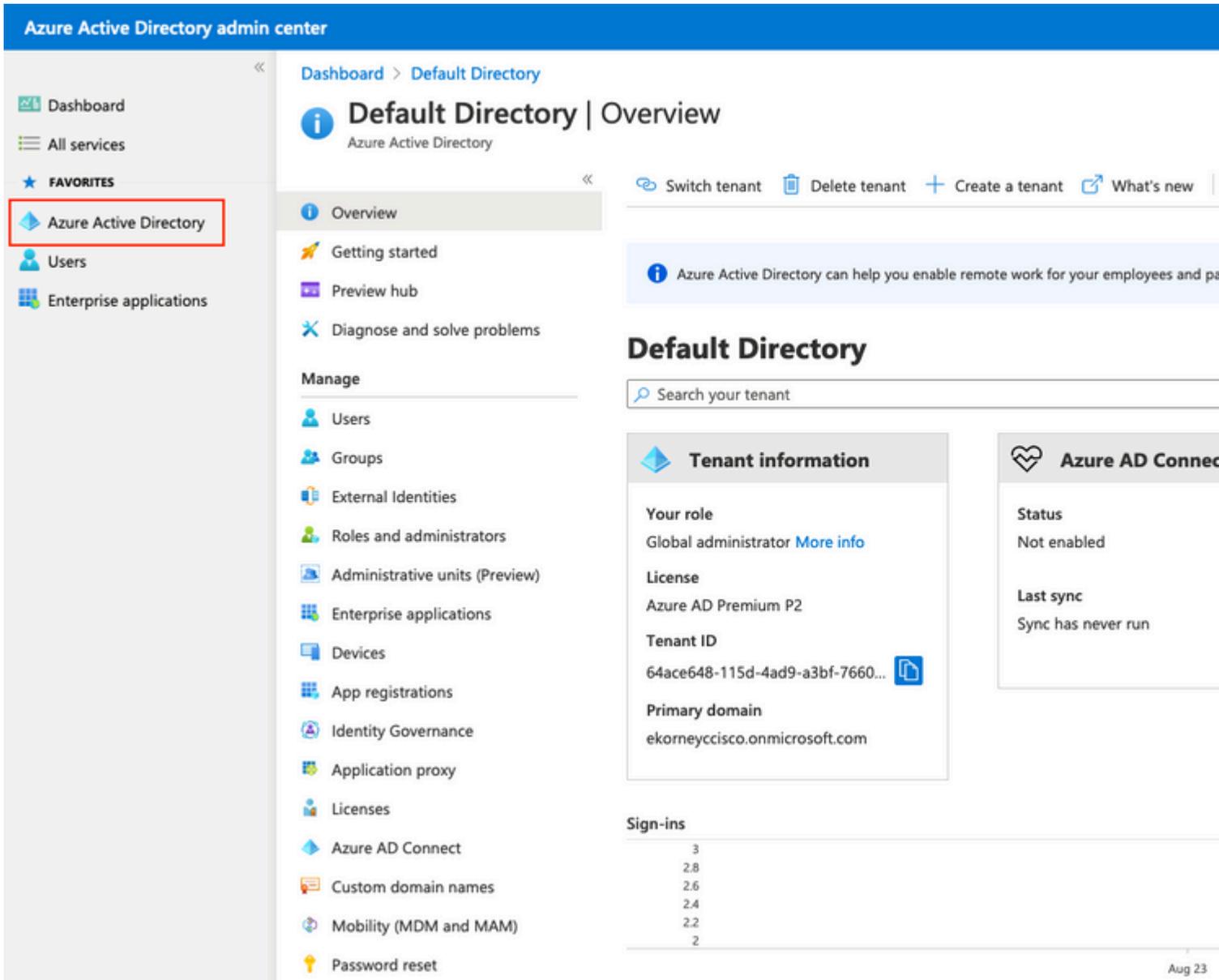
**AssertionConsumerService Location**="<https://10.201.232.19:8443/portal/SSOLoginResponse.action>"

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

## Schritt 2: Azure AD IDp-Einstellungen konfigurieren

### 1. Erstellen Sie einen Azure AD-Benutzer

Melden Sie sich beim Azure Active Directory-Admin-Center-Dashboard an, und wählen Sie Ihr **AD** wie im Bild dargestellt aus.



Wählen Sie **Benutzer aus**, klicken Sie auf **Neuer Benutzer**, konfigurieren Sie **Benutzername**, **Name** und **Anfangskennwort**, wie erforderlich. Klicken Sie auf **Erstellen**, wie im Bild gezeigt.

## 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. Erstellen einer Azure AD-Gruppe

Wählen Sie **Gruppen aus**. Klicken Sie auf **Neue Gruppe**.

[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

Behalten Sie Gruppentyp als **Sicherheit bei**. Konfigurieren Sie den **Gruppennamen** wie im Bild dargestellt.

Navigation sidebar with items: 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. Azure AD-Benutzer der Gruppe zuweisen

Klicken Sie auf **Keine Mitglieder ausgewählt**. Wählen Sie den Benutzer aus, und klicken Sie auf **Auswählen**. Klicken Sie auf **Erstellen**, um die Gruppe mit einem zugewiesenen Benutzer zu erstellen.

# Add members



Search ⓘ



mck  
mck@gdplab2021.onmicrosoft.com

## Selected items

No items selected

Notieren Sie sich die **Gruppenobjekt-ID**. In diesem Bildschirm ist dies **576c60ec-c0b6-4044-a8ec-d395b1475d6e** für die **ISE-Admin-Gruppe**, wie im Bild gezeigt.

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. Erstellen einer Azure AD-Enterprise-Anwendung

Wählen Sie unter AD die Option **Enterprise Applications** aus, und klicken Sie auf **New application**.

The screenshot shows the Azure Active Directory admin center interface. The top navigation bar is blue and contains the text "Azure Active Directory admin center". Below this, the breadcrumb path is "Dashboard > Default Directory > Enterprise applications". The main heading is "Enterprise applications | All applications" with the subtitle "Default Directory - Azure Active Directory". On the left side, there is a navigation menu with options: "Dashboard", "All services", "FAVORITES", "Azure Active Directory", "Users", and "Enterprise applications". The "Enterprise applications" option is selected. In the main content area, there is a "New application" button with a plus sign, which is highlighted with a red rectangular box. To the right of this button are "Columns" and "Preview feat" options. Below the "New application" button, there is a purple banner that says "Try out the new Enterprise Apps search preview! Click to ena". Further down, there are two dropdown menus: "Application type" set to "Enterprise Applications" and "Applications status" set to "Any". At the bottom, there is a text box that says "First 50 shown, to search all of your applications, enter a displ".

Wählen Sie die Option **Eigene Anwendung erstellen aus**.

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

Dashboard > Enterprise applications >

## 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.](#) →

Search application

Single Sign-on : All

User Account Management : All

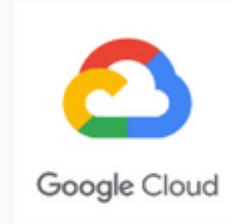
Catego

### Cloud platforms

#### Amazon Web Services (AWS)



#### Google Cloud Platform



### 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



Adobe Creative Cloud  
Microsoft Corporation



Adobe Identity Management  
Adobe Inc.

Geben Sie den Namen Ihrer Anwendung ein, und wählen Sie das Optionsfeld **Andere Anwendung integrieren, die Sie nicht in der Galerie finden (Nicht-Galerie)** und klicken Sie auf die Schaltfläche **Erstellen**, wie im Bild dargestellt.

# 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. Gruppe zur Anwendung hinzufügen

Wählen Sie **Benutzer und Gruppen** zuweisen aus.

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](#)

Klicken Sie auf **Benutzer/Gruppe hinzufügen**.

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
--------------	-------------

Klicken Sie auf **Benutzer und Gruppen**.

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

## Add Assignment

Default Directory

Users and groups

None Selected

Select a role

User

Wählen Sie die zuvor konfigurierte Gruppe aus, und klicken Sie auf **Auswählen**.

**Anmerkung:** Wählen Sie die richtigen Benutzer oder Gruppen aus, die wie vorgesehen auf die ISE zugreifen können, da die hier erwähnten Benutzer und Gruppen nach Abschluss der Einrichtung Zugriff auf die ISE erhalten.

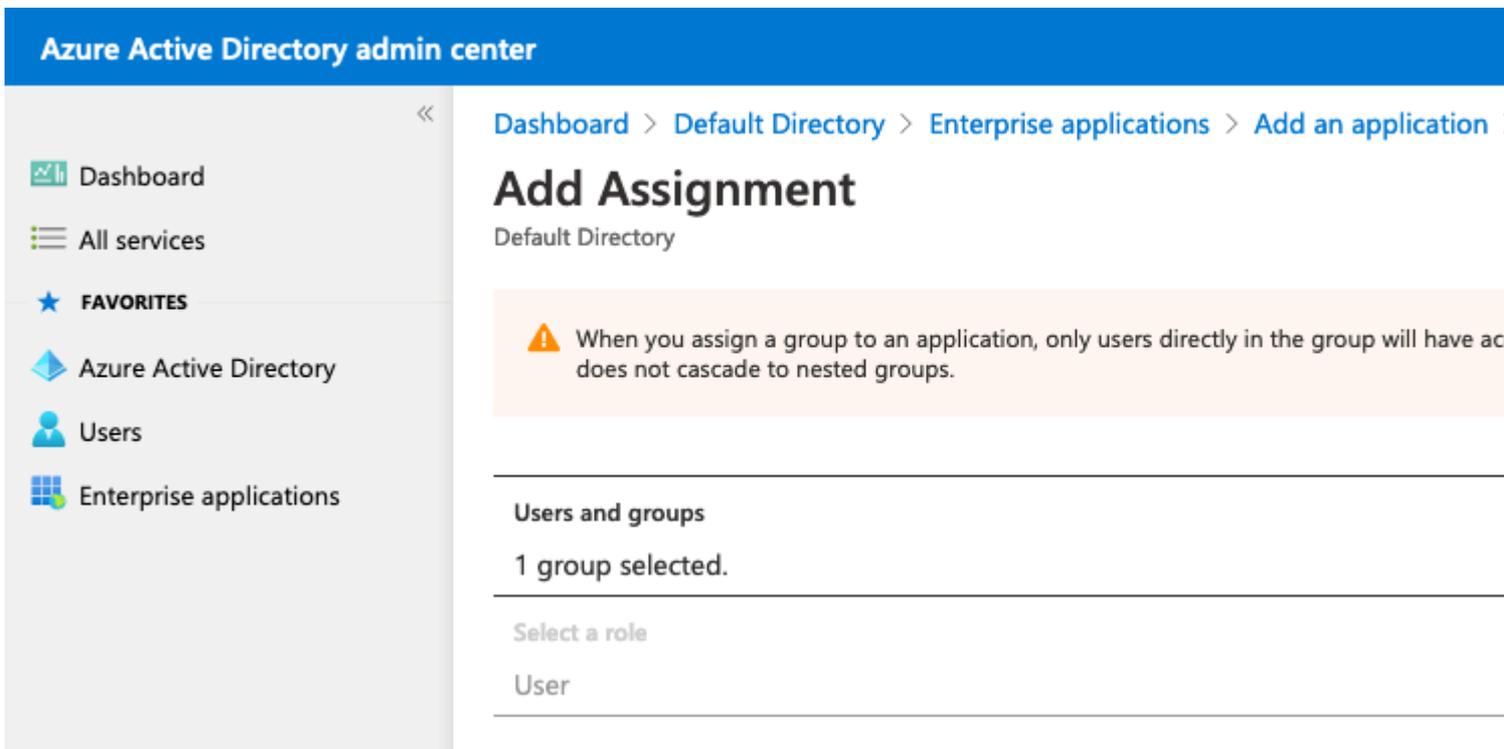
## Users and groups

Search

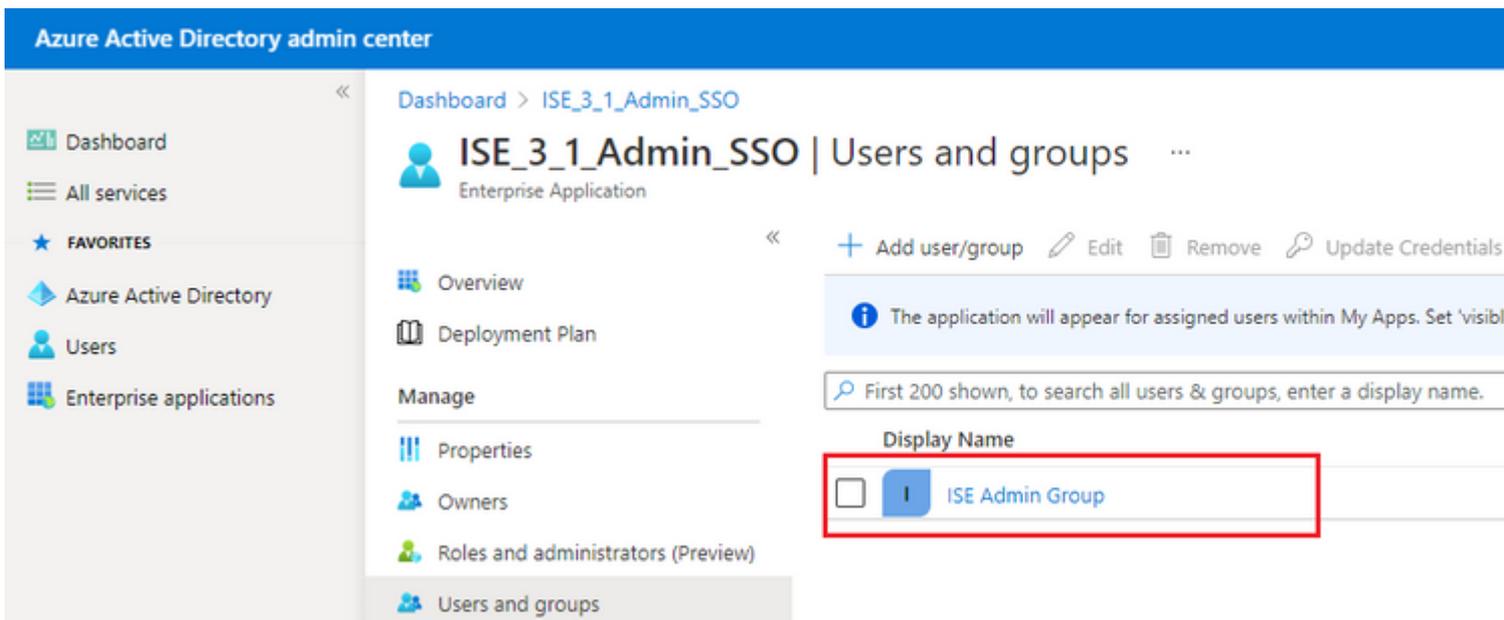
I ISE Admin Group

MC mck  
mck@gdplab2021.onmicrosoft.com

Klicken Sie nach Auswahl der Gruppe auf **Zuweisen**.



Daher wird das Menü **Benutzer und Gruppen** für die konfigurierte Anwendung mit der ausgewählten Gruppe gefüllt.



## 6. Konfigurieren einer Azure AD-Enterprise-Anwendung

Navigieren Sie zurück zu Ihrer Anwendung, und klicken Sie auf **einmalige Anmeldung einrichten**.

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

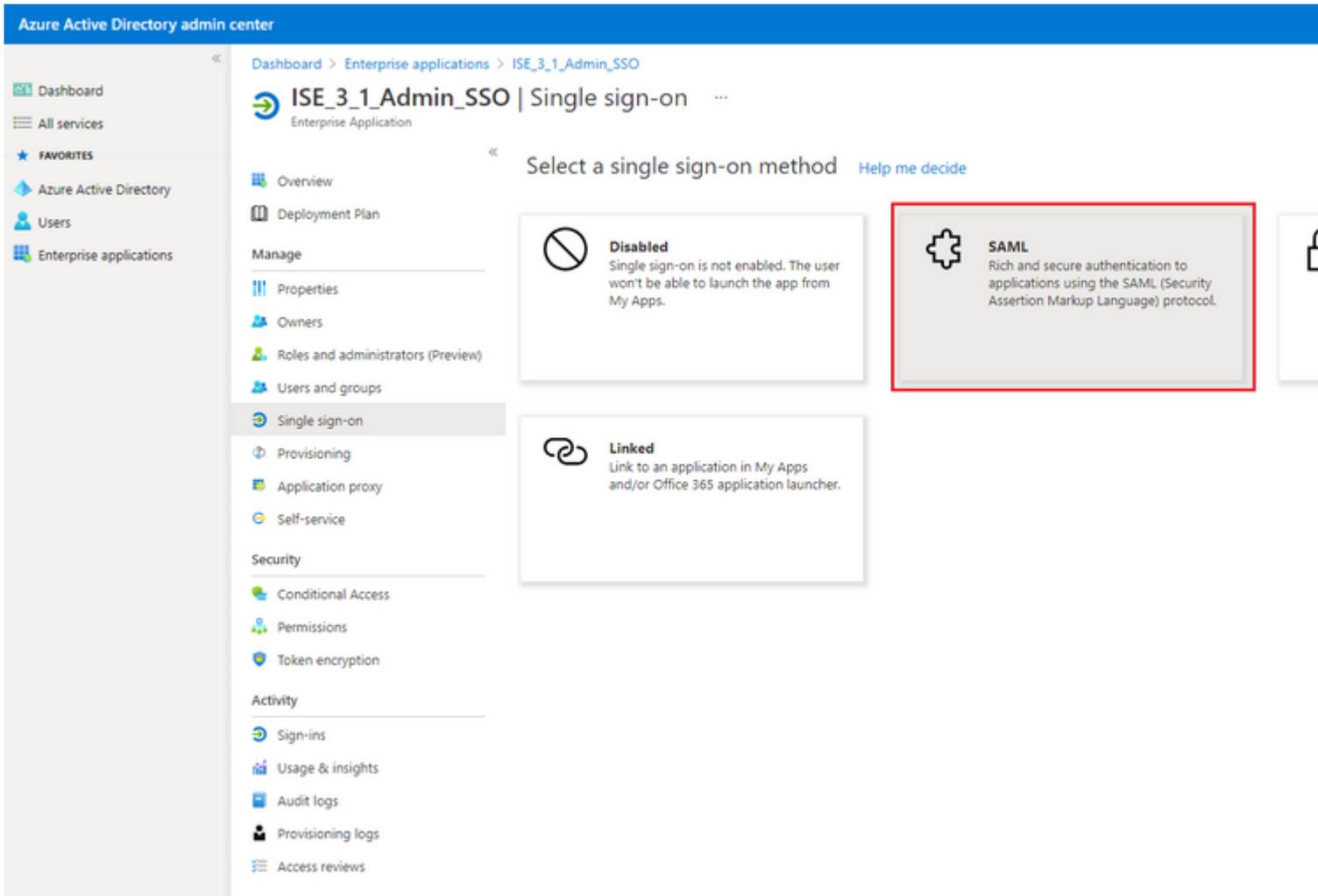
## Properties

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](#)

Wählen Sie auf dem nächsten Bildschirm **SAML** aus.



Klicken Sie neben "SAML-Basiskonfiguration" auf **Bearbeiten**.

## Set up Single Sign-On with SAML

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

**1** Basic SAML Configuration Edit

Identifier (Entity ID)	<b>Required</b>
Reply URL (Assertion Consumer Service URL)	<b>Required</b>
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

Geben Sie in Identifier (Entity ID) den Wert **entityID** aus der XML-Datei aus Schritt **Export Service Provider Information** ein. Füllen Sie die **Antwort-URL (Assertion Consumer Service URL)** mit dem

Wert von **Locations** von **AssertionConsumerService** aus. Klicken Sie auf **Speichern**.

**Anmerkung:** Antwort-URL fungiert als Übergabeliste, die es bestimmten URLs ermöglicht, als Quelle zu fungieren, wenn sie auf die IdP-Seite umgeleitet werden.

## 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

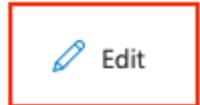
### Relay State

### Logout Url

## 7. Active Directory-Gruppenattribut konfigurieren

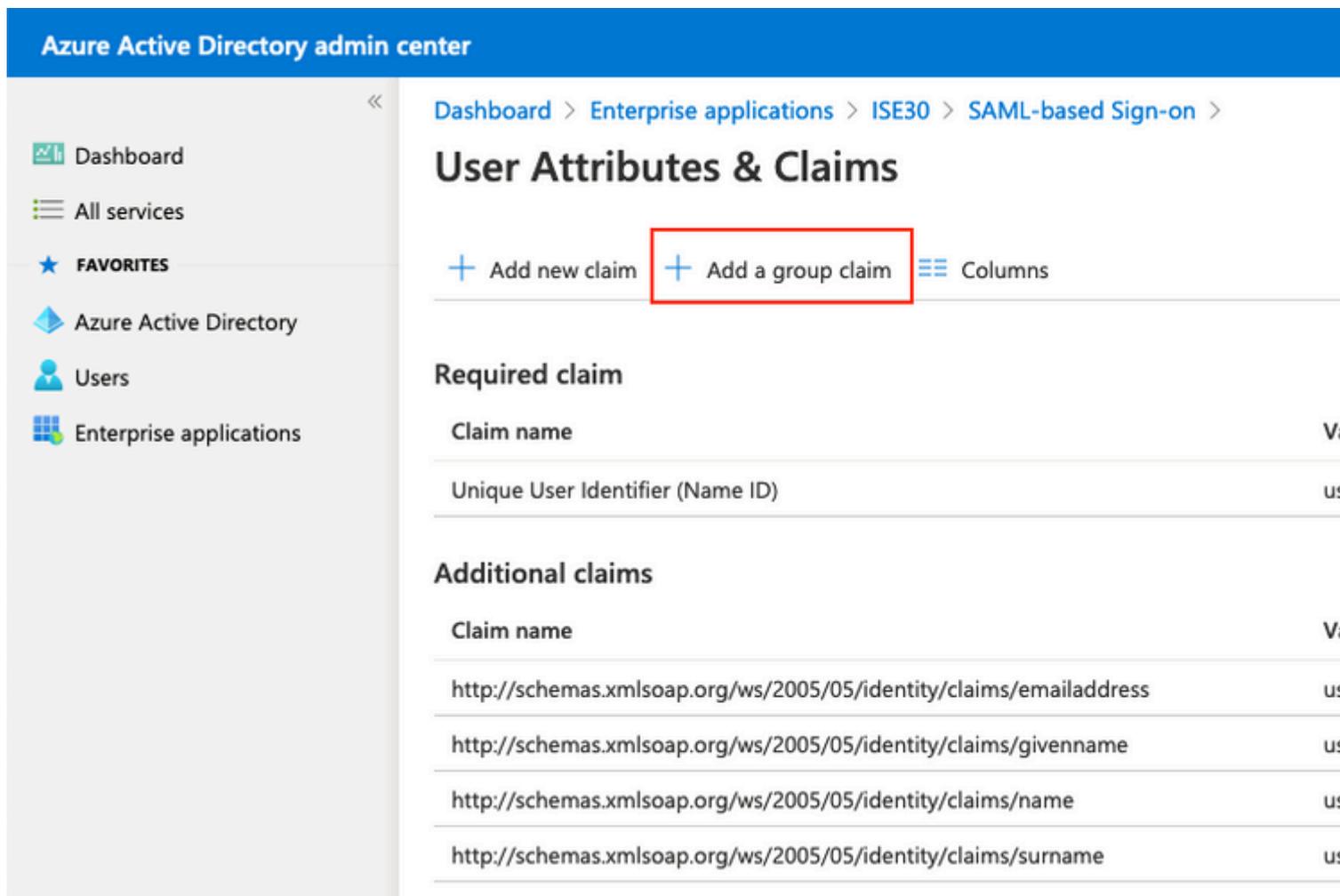
Um den zuvor konfigurierten Gruppenattributwert zurückzugeben, klicken Sie neben "**Benutzerattribute & Ansprüche**" auf **Bearbeiten**.

### User Attributes & Claims



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

Klicken Sie auf **Gruppenanspruch hinzufügen**.

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 breadcrumb, there are three buttons: "Add new claim", "Add a group claim" (highlighted with a red box), and "Columns". The "Required claim" section shows a table with one row: "Unique User Identifier (Name ID)". The "Additional claims" section shows a table with four rows, each with a claim name and a source URL: "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname", "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name", and "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname".

Wählen Sie **Sicherheitsgruppen aus**, und klicken Sie auf **Speichern**. Wählen Sie im Dropdown-Menü "**Quellattribut**" die Option **Gruppen-ID aus**. Aktivieren Sie das Kontrollkästchen, um den Namen des Gruppenanspruchs anzupassen, und geben Sie den Namen **Gruppen ein**.

# 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 ⓘ

Notieren Sie sich den **Forderungsnamen** für die Gruppe. In diesem Fall sind es **Gruppen**.

**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 Metadaten-XML-Datei herunterladen

Klicken Sie auf **Download** für **Verbundmetadaten-XML** im **SAML-Signaturzertifikat**.

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	<a href="https://login.microsoftonline.com/182900ec-e960...">https://login.microsoftonline.com/182900ec-e960...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
<b>Federation Metadata XML</b>	<b><a href="#">Download</a></b>

## Schritt 3: Hochladen von Metadaten aus Azure Active Directory in die ISE

Navigieren Sie zu **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]**.

Wechseln Sie von der Registerkarte zu **Identity Provider Config**, und klicken Sie auf **Durchsuchen**. Wählen Sie **Verbundmetadaten-XML**-Datei aus Schritt **Azure-Verbundmetadaten-XML herunterladen** aus, und klicken Sie auf **Speichern**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration · Identity Management'. Below this are tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' tab is selected, and the left sidebar shows a tree view of external identity sources, including 'SAML Id Providers'. The main content area is titled 'SAML Identity Provider' and shows the configuration for an Azure provider. The 'Identity Provider Config.' tab is active, 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 this is a section for 'Signing Certificates' with a table listing certificates.

Subject	Issuer	Valid From	Valid To (Ex
CN=Microsoft Azure Federated SSO Certificate	CN=Microsoft Azur...	Mon Jul 19 12:16:2...	Fri Jul 19 12:

#### Schritt 4: Konfigurieren von SAML-Gruppen auf der ISE

Wechseln Sie zu Registerkarte **Gruppen**, und fügen Sie den Wert des **Anspruchsnamens** aus **Active Directory-Gruppenattribut konfigurieren** in **Gruppenmitgliedschaft-Attribut ein**.

## External Identity Sources

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

Identity Provider List &gt; Azure

## SAML Identity Provider

General

Identity Provider Config.

Service Provider Info.

Groups

## Groups

Group Membership Attribute    Name in Assertion ^ Name in

Klicken Sie auf **Hinzufügen**. Geben Sie **in Assertion** den Wert der **Gruppenobjekt-ID** der **ISE-Admin-Gruppe** ein, die in **Azure Active Directory-Benutzer der Gruppe** zuweisen erfasst wurde.

Konfigurieren Sie **Name in ISE** mit dem Dropdown-Menü, und wählen Sie die entsprechende Gruppe auf ISE aus. In diesem Beispiel wird die Gruppe **"Super Admin"** verwendet. Klicken Sie auf **OK**. Klicken Sie auf **Speichern**.

Dadurch wird eine Zuordnung zwischen der Gruppe in Azure und dem Gruppennamen auf der ISE erstellt.

### Add Group

\*Name in Assertion

\*Name in ISE

- Customization Admin
- ERS Admin
- ERS Operator
- Elevated System Admin
- Helpdesk Admin
- Identity Admin
- MnT Admin
- Network Device Admin
- Policy Admin
- RBAC Admin
- SPOG Admin
- Super Admin
- System Admin
- TACACS+ Admin

### (Optional) Schritt 5: RBAC-Richtlinien konfigurieren

Im vorherigen Schritt gibt es viele verschiedene Arten von Benutzerzugriffsebenen, die auf der ISE konfiguriert werden können.

Um rollenbasierte Zugriffskontrollrichtlinien (RBAC) zu bearbeiten, navigieren Sie zu **Administration > System > Admin Access > Authorization > Permissions > RBAC Policies**, und konfigurieren Sie sie nach Bedarf.

Dieses Bild dient als Referenz für die Beispielkonfiguration.

### ▼ 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</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 Acce</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>

## Überprüfung

Bestätigen Sie, dass Ihre Konfiguration ordnungsgemäß funktioniert.

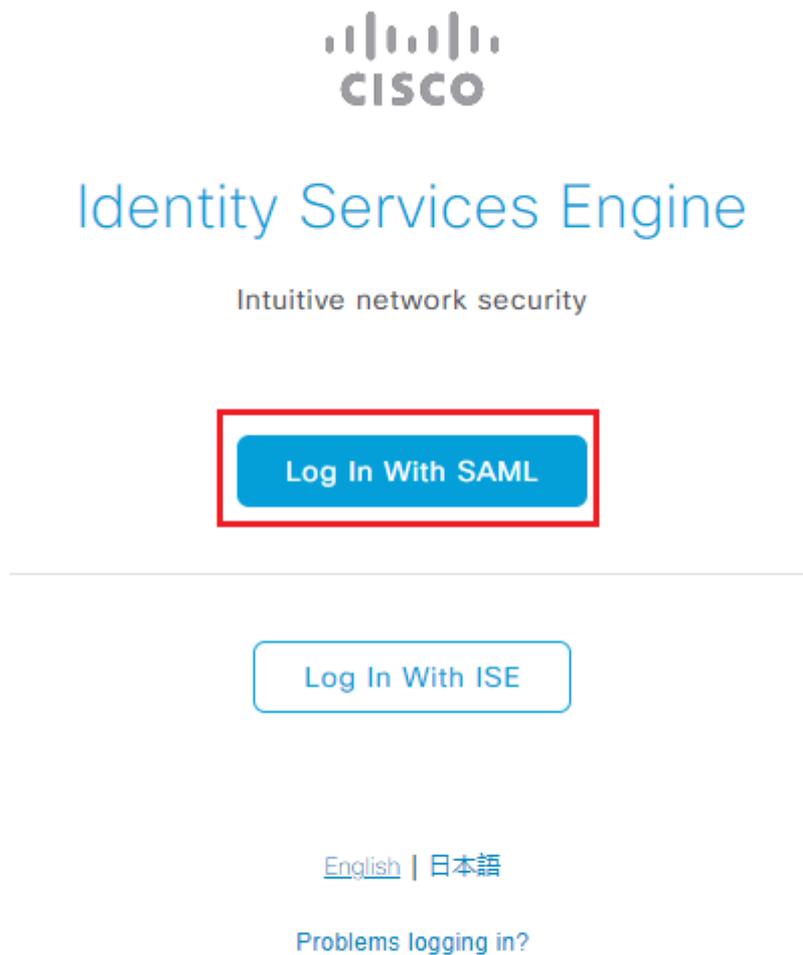
---

**Anmerkung:** Der SAML SSO-Anmeldetest von der Azure-Testfunktion funktioniert nicht. Die SAML-Anforderung muss von ISE initiiert werden, damit die Azure SAML-SSO ordnungsgemäß funktioniert.

---

Öffnen Sie den Anmeldeaufforderungsbildschirm der ISE-GUI. Es wird eine neue Option für die **Anmeldung mit SAML** angezeigt.

1. Rufen Sie Ihre ISE GUI-Anmeldeseite auf, und klicken Sie auf **Anmelden mit SAML**.



2. Sie werden zum Microsoft-Anmeldebildschirm weitergeleitet. Geben Sie Ihre **Benutzernamen-**Anmeldeinformationen für ein Konto in einer Gruppe ein, die der ISE zugeordnet ist, wie hier dargestellt, und klicken Sie auf **Weiter**, wie im Bild gezeigt.



## Sign in

mck@gdplab2021.onmicrosoft.com

---

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

Next

3. Geben Sie Ihr **Kennwort** für den Benutzer ein, und klicken Sie auf **Anmelden**.



← mck@gdplab2021.onmicrosoft.com

## Enter password

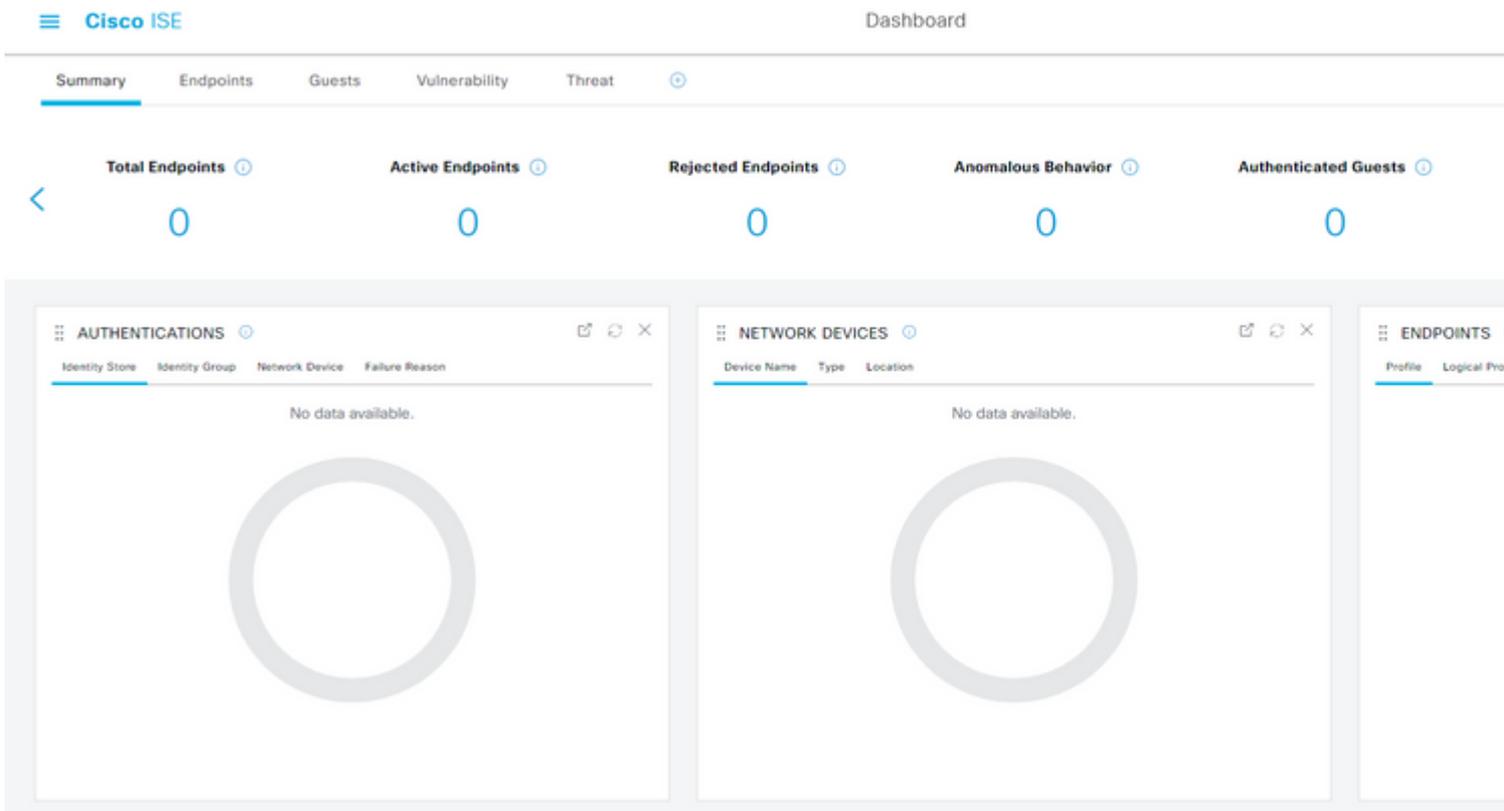
.....

---

[Forgot my password](#)

Sign in

4. Sie werden jetzt zum ISE-Anwendungs-Dashboard mit den entsprechenden Berechtigungen umgeleitet, die basierend auf der zuvor konfigurierten ISE-Gruppe konfiguriert wurden, wie im Bild gezeigt.



## Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

### Häufige Probleme

Es ist wichtig zu wissen, dass die SAML-Authentifizierung zwischen dem Browser und Azure Active Directory durchgeführt wird. Daher können Sie authentifizierungsbezogene Fehler direkt vom Identity Provider (Azure) abrufen, bei dem die ISE-Einbindung noch nicht gestartet wurde.

Problem 1. Der Fehler "Ihr Konto oder Kennwort ist falsch" wird angezeigt, nachdem Sie die Anmeldeinformationen eingegeben haben. Hier werden Nutzerdaten noch nicht von der ISE empfangen und der Prozess bleibt an dieser Stelle noch bei IdP (Azure).

Der wahrscheinlichste Grund ist, dass die Kontoinformationen falsch sind oder das Kennwort falsch ist. Um zu beheben: Setzen Sie das Kennwort zurück, oder geben Sie das richtige Kennwort für das Konto ein, wie im Bild gezeigt.



← 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

Ausgabe 2. Der Benutzer ist nicht Teil der Gruppe, die Zugriff auf SAML SSO erhalten soll. Ähnlich wie im vorherigen Fall werden Benutzerdaten noch nicht von der ISE empfangen und der Prozess bleibt an dieser Stelle noch bei IdP (Azure).

Um dies zu beheben, stellen Sie sicher, dass die **Gruppe "Hinzufügen" zum Konfigurationsschritt "Anwendung"** korrekt ausgeführt wird, wie im Bild gezeigt.



## 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.

Ausgabe 3. Der ISE-Anwendungsserver kann SAML-Anmeldeanforderungen nicht verarbeiten. Dieses Problem tritt auf, wenn die SAML-Anforderung vom Identitätsanbieter Azure statt vom Dienstanbieter ISE initiiert wird. Das Testen der SSO-Anmeldung von Azure AD funktioniert nicht, da ISE vom Identitätsanbieter initiierte SAML-Anforderungen nicht unterstützt.



## 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)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

**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

~~Sign in as current user~~  
~~Sign in as someone else~~ (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](#)

Ausgabe 4: ISE zeigt nach einem Anmeldeversuch den Fehler "Zugriff verweigert" an. Dieser Fehler tritt auf, wenn der Anspruchsname der zuvor in der Azure Enterprise-Anwendung erstellten Gruppe in ISE nicht übereinstimmt.

So beheben Sie dies: Stellen Sie sicher, dass der Gruppenanspruchsname in Azure und ISE auf der Registerkarte SAML Identity Provider Groups (SAML-Identitätsanbietergruppen) identisch ist. Weitere Informationen finden Sie in den Schritten 2.7 und 4 im Abschnitt **Konfigurieren von SAML SSO mit Azure AD** dieses Dokuments.



# Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

## Fehlerbehebung bei ISE

Die Protokollstufe der hier aufgeführten Komponenten muss für die **ISE** geändert werden. Navigieren Sie zu **Operationen > Fehlerbehebung > Debugassistent > Debugprotokollkonfiguration**.

Komponentenname	Protokollstufe	Protokolldateiname
Portal	DEBUG	guest.log

opensaml	DEBUG	ise-psc.log
Kleine	DEBUG	ise-psc.log

## Protokolle mit SAML-Anmeldung und nicht übereinstimmenden Gruppenanspruchenamen

Satz von Debugs, die ein Fehlerbehebungsszenario mit nicht übereinstimmenden Anspruchsamen zum Zeitpunkt der Ausführung des Datenflusses anzeigen (ise-psc.log).

---

**Hinweis:** Achten Sie auf **fett gedruckte** Elemente. Die Protokolle wurden zur Verdeutlichung gekürzt.

---

1. Der Benutzer wird von der ISE-Admin-Seite zur IdP-URL umgeleitet.

<#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
```

**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. Die SAML-Antwort wird vom Browser empfangen.

<#root>

```
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://10.201.232.19:8443/identity/
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.SAMLMessageDecoder
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.SAMLMessageDecoder
```

### 3. Die Analyse von Attributen (Assertionen) wird gestartet.

<#root>

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

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

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

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

[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.SAMLMessageDecoder
```

### 4. Gruppenattribut wird mit dem Wert **576c60ec-c0b6-4044-a8ec-d395b1475d6e** empfangen, Signaturvalidierung.

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

```

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][] 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 13:48:27,188 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.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. Validierung der RBAC-Autorisierung.

```
<#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 save
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 -:::

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.