Configure ISE 3.1 Admin Log in Flow via SAML SSO with Azure AD

Contents

Introduction

This document describes how to configure Cisco ISE 3.1 SAML SSO Integration with an External Identity Provider such as **Azure Active Directory** (AD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

1. Cisco ISE 3.1
2. SAML SSO deployments
3. Azure AD

Components Used

The information in this document is based on these software and hardware versions:

1. Cisco ISE 3.1
2. Azure AD

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

TERMS:

Identity Provider (IdP) :

the authority Azure AD that verifies and asserts a user identity and access privileges to a requested resource (the Service Provider).

Service Provider (SP) :

the hosted resource or service that the user intends to access (the ISE Application Server).

SAML

Security Assertion Markup Language (SAML) is an open standard that allows IdP in order to pass authorization credentials to SP.

SAML transactions use **Extensible Markup Language** (XML) for standardized communications between the identity provider and service providers.

SAML is the link between the authentication of a user identity and the authorization in order to use a service.

SAML Assertion

A SAML Assertion is the XML document that the identity provider sends to the service provider that contains the user authorization.

There are three different types of SAML Assertions – authentication, attribute, and authorization decision.

- Authentication assertions prove the identification of the user and provide the time the user logged in and what method of authentication they used (Kerberos, two-factor, as examples)

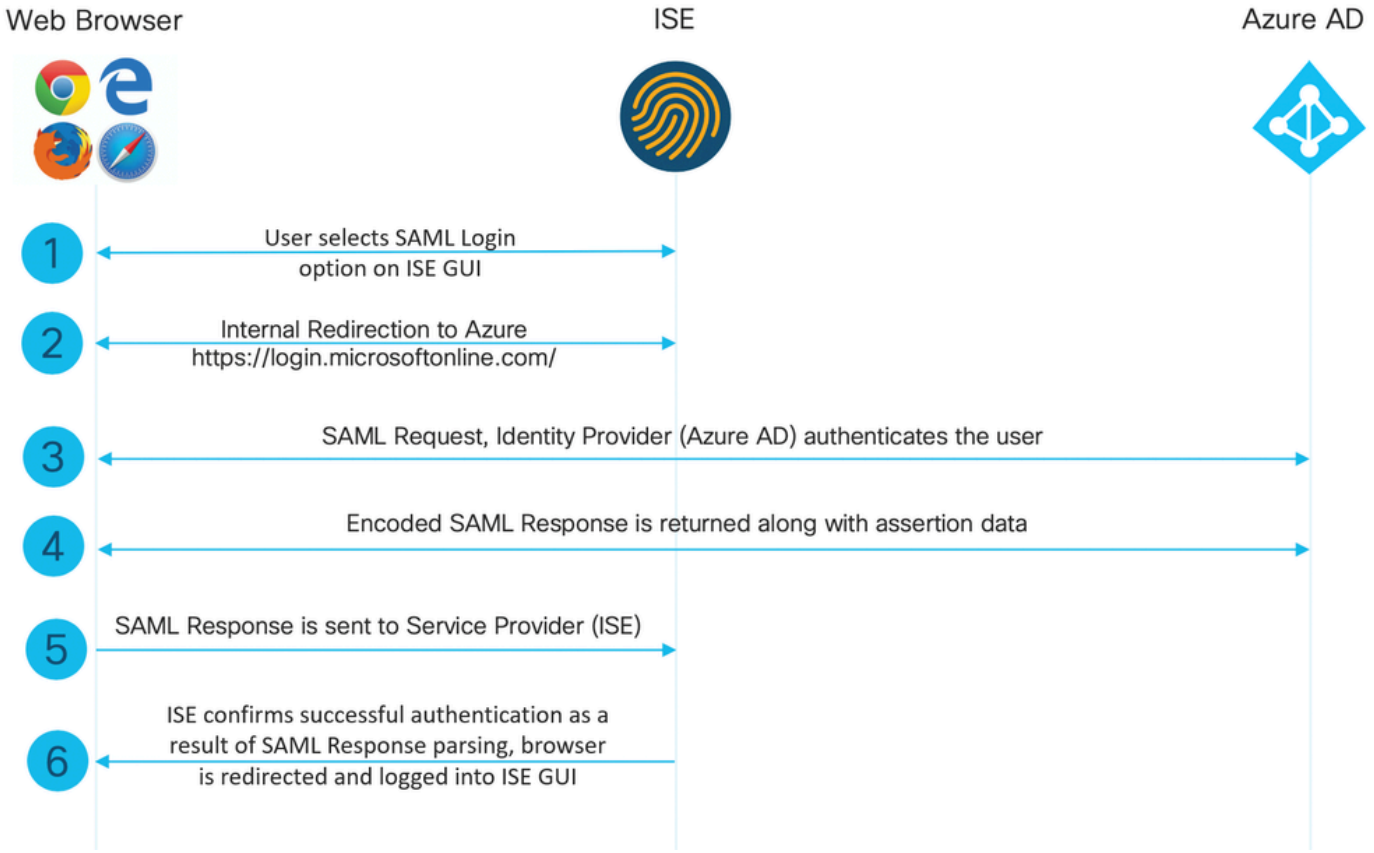
- The attribution assertion passes the SAML attributes, specific pieces of data that provide information about the user, to the service provider.
- An authorization decision assertion declares if the user is authorized to use the service or if the identify provider denied their request due to a password failure or lack of rights to the service.

High-Level Flow Diagram

SAML works by passing information about users, logins, and attributes between the identity provider, Azure AD, and the service provider, ISE.

Each user logs in once to a Single Sign-On (SSO) with the identity provider, then the Azure AD provider passes the SAML attributes to ISE when the user attempts to access those services.

ISE requests authorization and authentication from Azure AD as shown in the image.


Web Browser
ISE
Azure AD
1
User selects SAML Login option on ISE GUI
2
Internal Redirection to Azure https://login.microsoftonline.com/
3
SAML Request, Identity Provider (Azure AD) authenticates the user
4
Encoded SAML Response is returned along with assertion data
5
SAML Response is sent to Service Provider (ISE)
6
ISE confirms successful authentication as a result of SAML Response parsing, browser is redirected and logged into ISE GUI

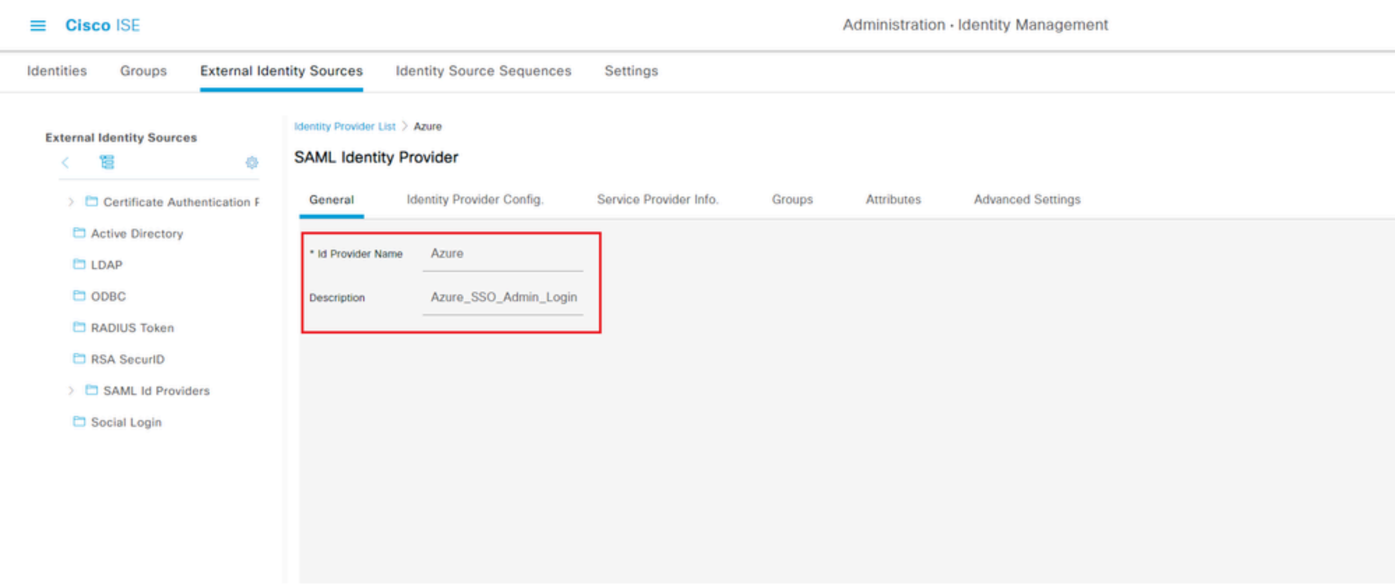
Configure SAML SSO Integration with Azure AD

Step 1. Configure SAML Identity Provider on ISE

1. Configure Azure AD as External SAML Identity Source

On ISE, navigate to **Administration** > **Identity Management** > **External Identity Sources** > **SAML Id Providers** and click the **Add** button.

Enter the **Id Provider Name** and click **Submit** in order to save it. The **Id Provider Name** is significant only for ISE as shown in the image.


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication F
Active Directory
LDAP
ODBC
RADIUS Token
RSA SecurID
SAML Id Providers
Social Login
Identity Provider List > Azure
SAML Identity Provider
General
Identity Provider Config.
Service Provider Info.
Groups
Attributes
Advanced Settings

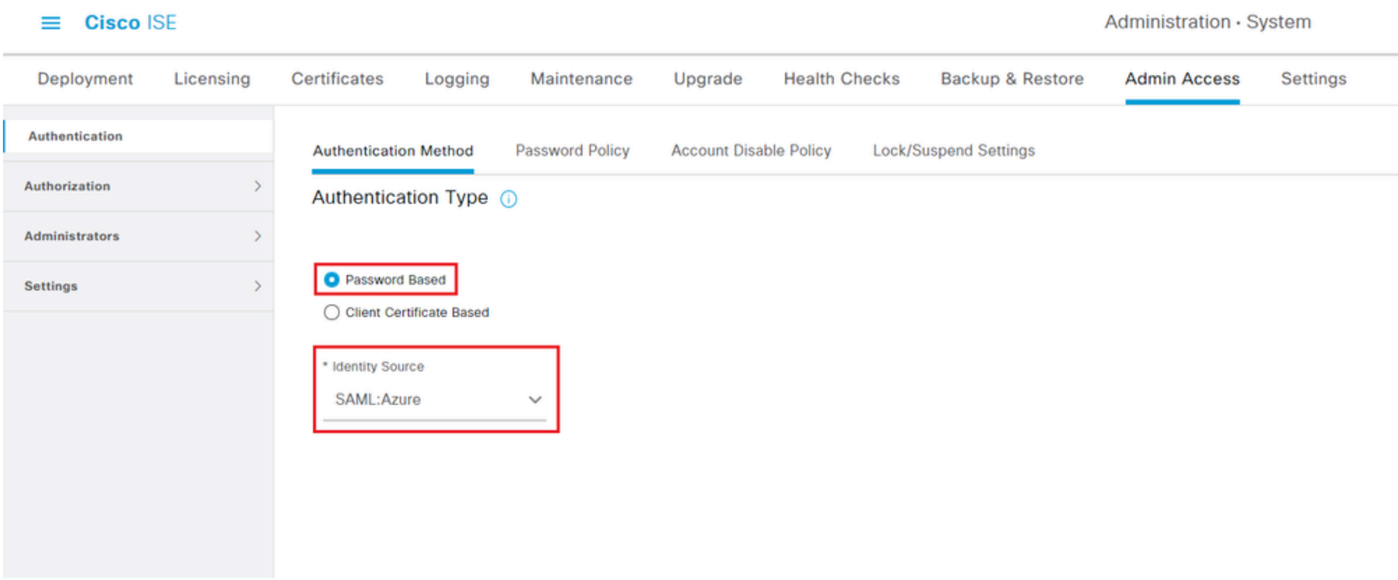
* Id Provider Name: Azure

Description: Azure_SSO_Admin_Login

2. Configure ISE Authentication Method

Navigate to **Administration >System > Admin Access > Authentication > Authentication Method** and select the **Password Based** radio button.

Select the required Id Provider Name created earlier from the **Identity Source** drop-down list as shown in the image.



Authentication Type

● Password Based

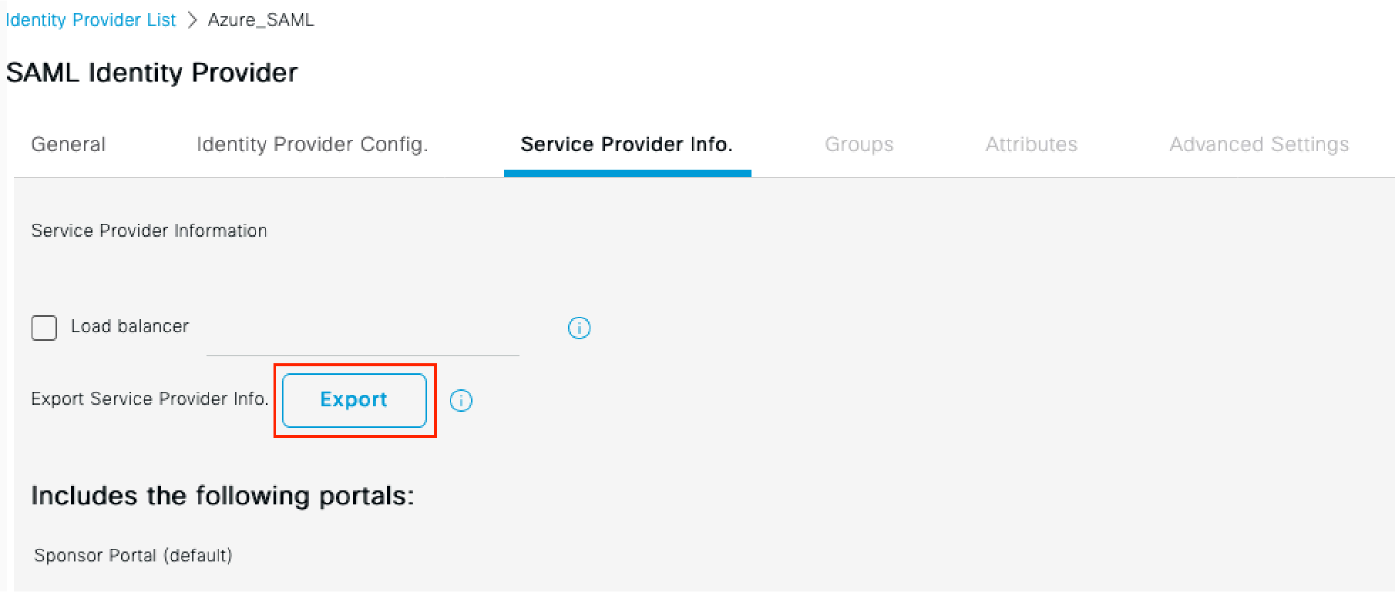
○ Client Certificate Based

* Identity Source: SAML:Azure

3. Export Service Provider Information

Navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider]**.

Switch the tab to **Service Provider Info**. and click the **Export** button as shown in the image.



Service Provider Information

□ Load balancer

Export Service Provider Info. Export

Includes the following portals:

Sponsor Portal (default)

Download the **.xml** file and save it. Make a note of the **Location** URL and **entityID** value.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasi
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSig
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amSlL6NAE8FY+tzANBgkqhkiG9w0BAQwFADAlMSMwIQYDVQQDExpT
QU1MX2lzZTMtMS0xOS5ja3VtYXIyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTGlNBTUxfaXNlMy0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAvila4+SOuP3jO37yCOXnHAzADupfqcgwcplJQnFxhVfnDdOixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohGOt1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYdlDtE1LMEcGg1mCd56GfrDcJdXOcZJmiDzizyjGKDdPf+1VM5JHCo6UNLFlIFyPmGvcCXnt
NVqsYvxSzF038ciQqlm0sqrVrrYZuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFFlMzybvm1FYu
9h83gL4WJWMizETO6Vs/DOp6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5ROgT7v3CDrdFtRoNYAT+YvO941KzFCSE0sshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNzlFuggaE8tC7uyuQZa2rcmTrXGWCl
sDU4uOvFpFvrcC/lavr9Fnx7LPwXaOasvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWIy+ctbBTO+EMO6Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5O58Zot9gqkpFw
kVS9vT4EOzwNGo7pQI8CAwEAAaN9MHswIAYDVR0RBBkwF4IVaXNlMy0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgLsMB0GA1UdDgQWBBRIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
2O6Dkb6fHdgKd9goN8N2bj+34ybwxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GWlvcgreC7R46qenaonXVrltRw11vVIdCf8JQFFMxya/rIC4mxVeooOj1Fl9d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBteO/pdUtEi6fObqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gfHObE5luT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmDh9g2mppbBwOcxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cfAZuiV/e3wkOBLZM
lgV8FTVQSnra9LwHP/PgeNAPUcRPXSwaKE4rvjvMcOaS/iYdwZhZiJ8zBdIBanMv5mGu1nvTEt9K
EEwj9yslIHmdqoH3EmOFOgnzRORvsMPbJxAoTFjfoITTMdQXNHhg+wlPOKXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKwER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8EOv7bUMSDmmg/53NoktfJ1CckaWE87myhimjO
</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.act
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLogin

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

Attributes of interest from the XML file:

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

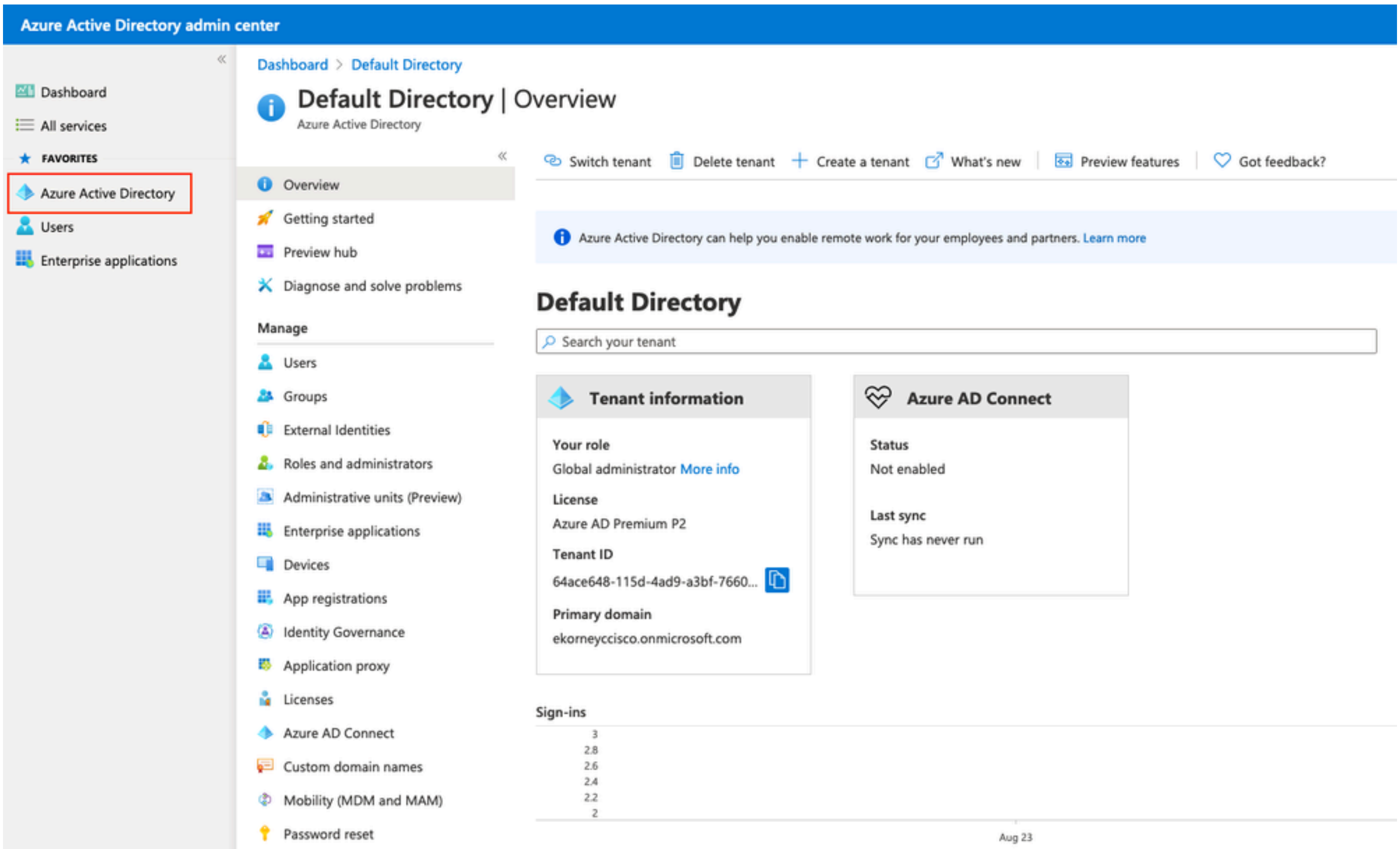
AssertionConsumerService Location="https://10.201.232.19:8443/portal/SSOLoginResponse.action"

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

Step 2. Configure Azure AD IdP Settings

1. Create an Azure AD User

Log in to the Azure Active Directory admin center dashboard and select your **AD** as shown in the image.



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

Your role
Global administrator More info

License
Azure AD Premium P2

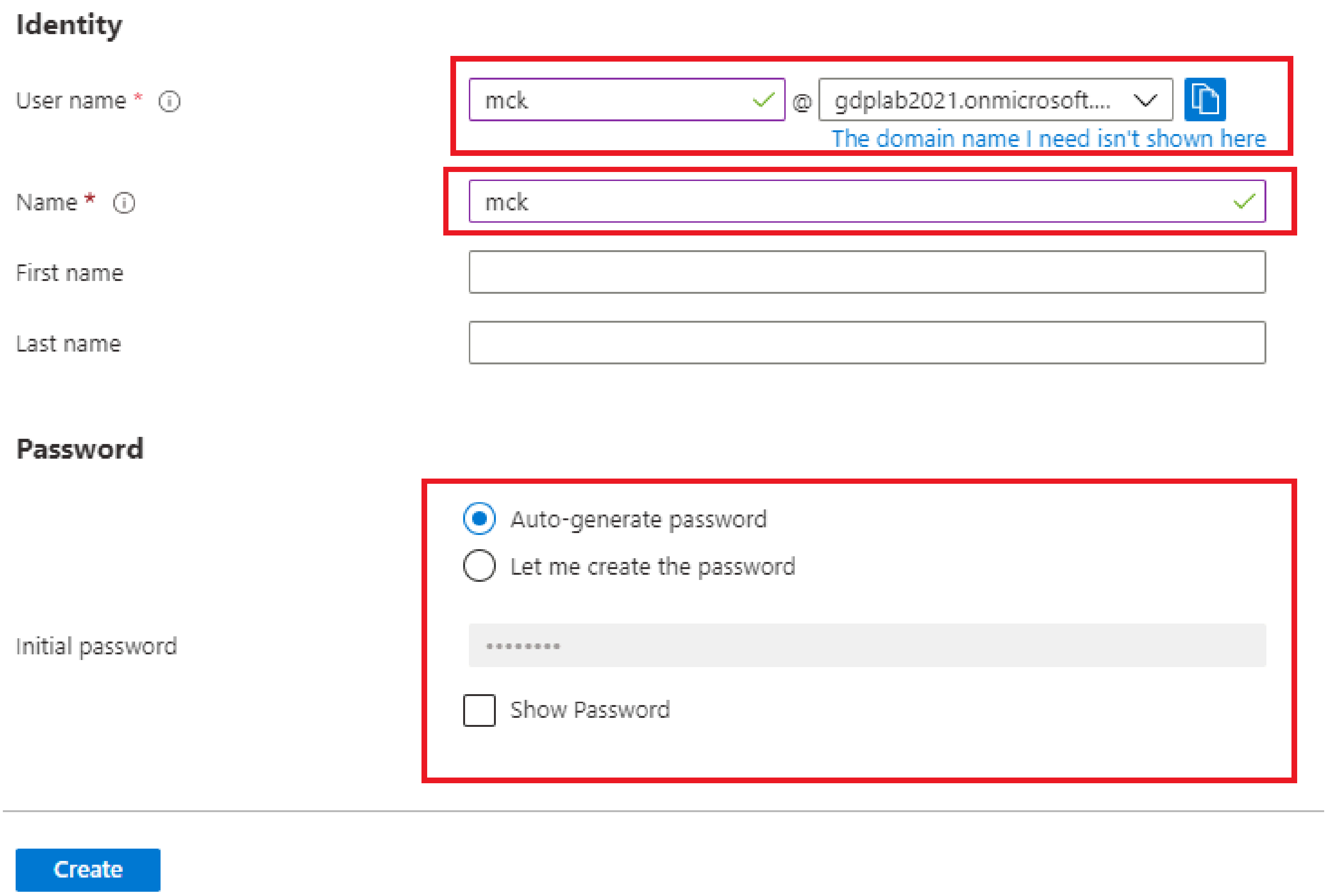
Tenant ID
64ace648-115d-4ad9-a3bf-7660...

Primary domain
ekorneycisco.onmicrosoft.com

Status
Not enabled

Last sync
Sync has never run

Select **Users**, click on **New User**, configure **User name, Name** and **Initial Password** as required. Click on **Create** as shown in the image.



Identity

User name * mck @ gdplab2021.onmicrosoft....

The domain name I need isn't shown here

Name * mck

First name

Last name

Password

Initial password

● Auto-generate password

○ Let me create the password

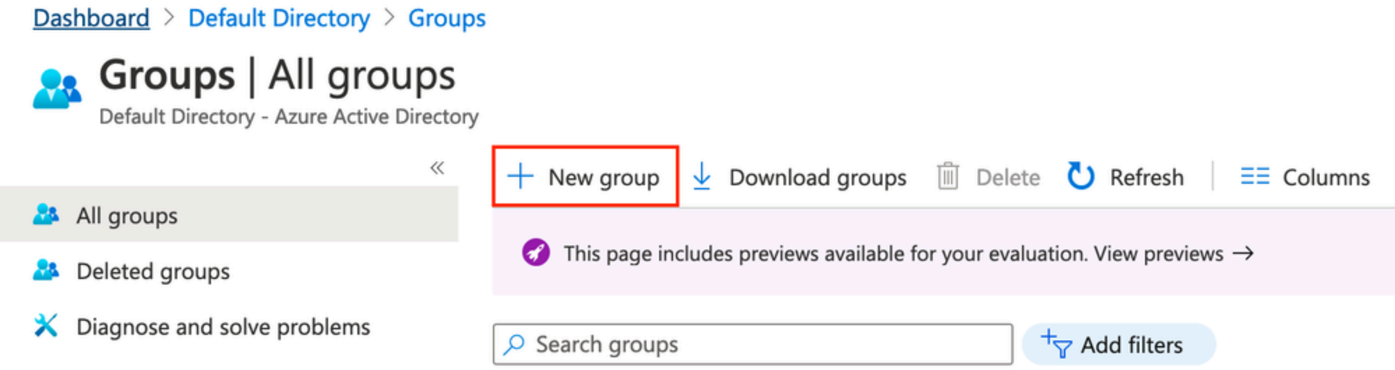
••••••••

□ Show Password

Create

2. Create an Azure AD Group

Select **Groups.** Click **New Group**.



Dashboard > Default Directory > Groups

Groups | All groups

Default Directory - Azure Active Directory

All groups

Deleted groups

Diagnose and solve problems

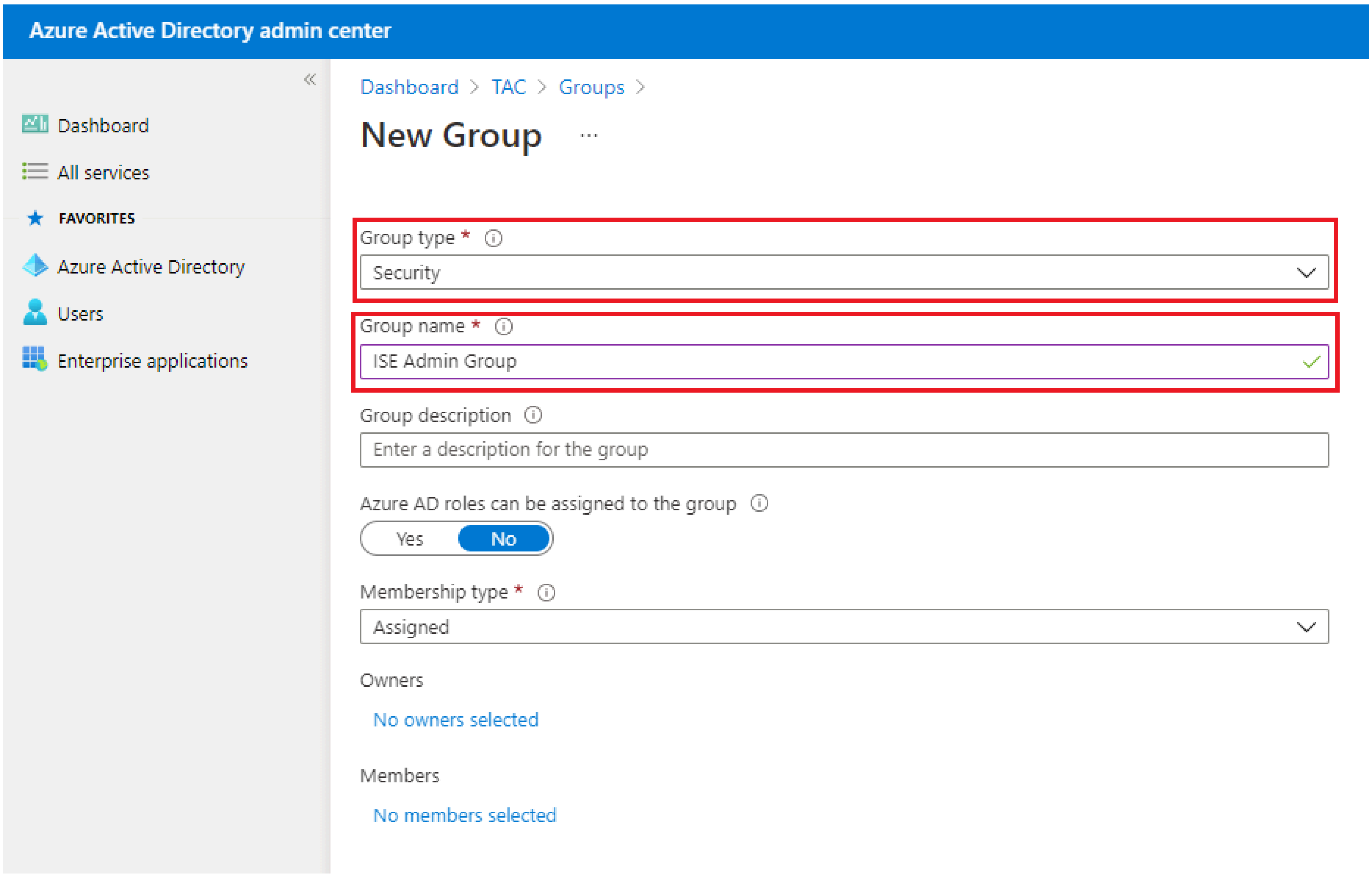
+ New group | Download groups | Delete | Refresh | Columns

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

Search groups

Add filters

Keep Group type as **Security**. Configure the **Group name** as shown in the image.



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]

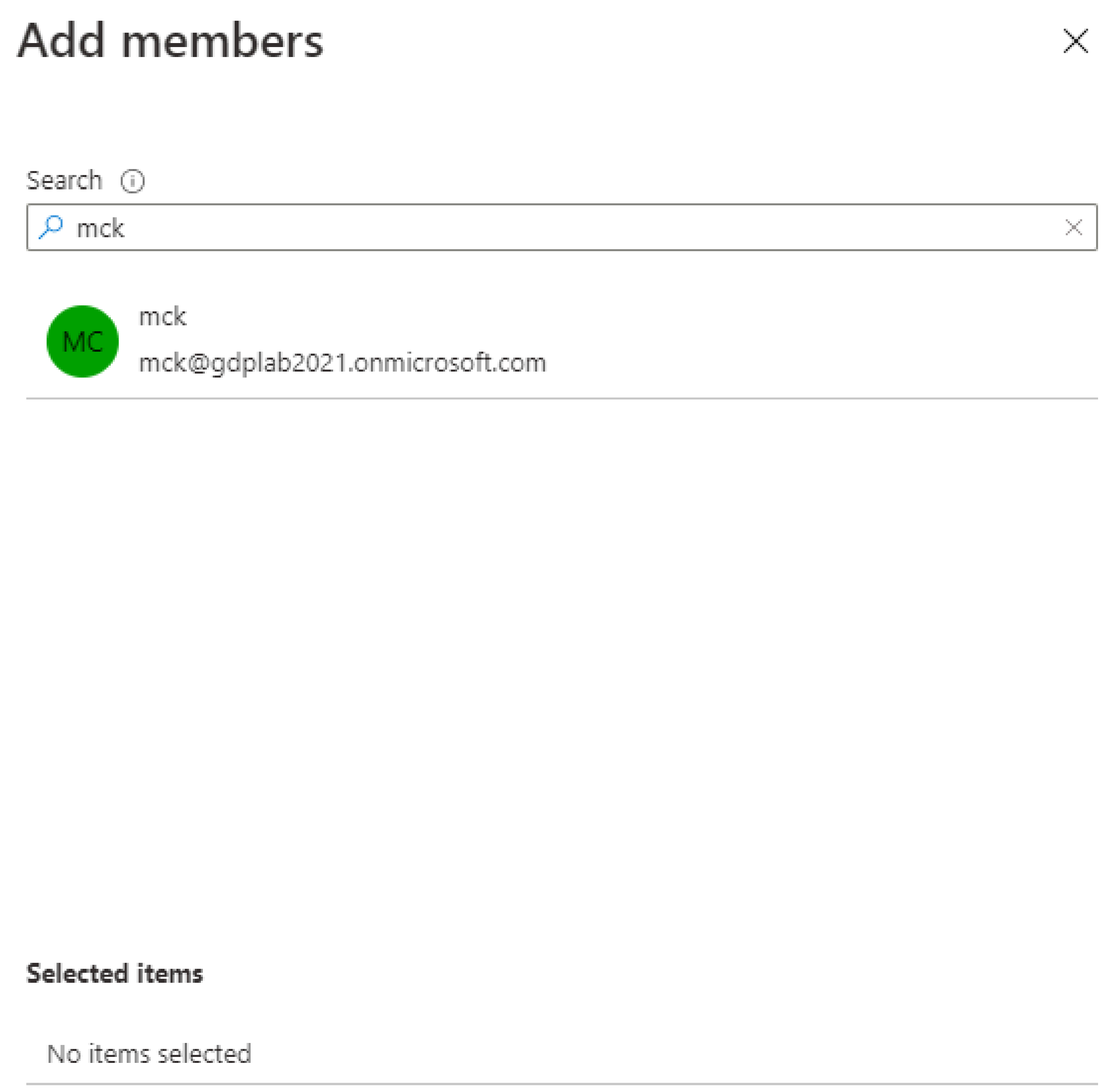
Membership type * ⓘ
Assigned

Owners
No owners selected

Members
No members selected

3. Assign Azure AD User to the Group

Click on **No members selected.** Choose the user and click on **Select.** Click **Create** in order to create the group with a User assigned to it.



Add members

Search

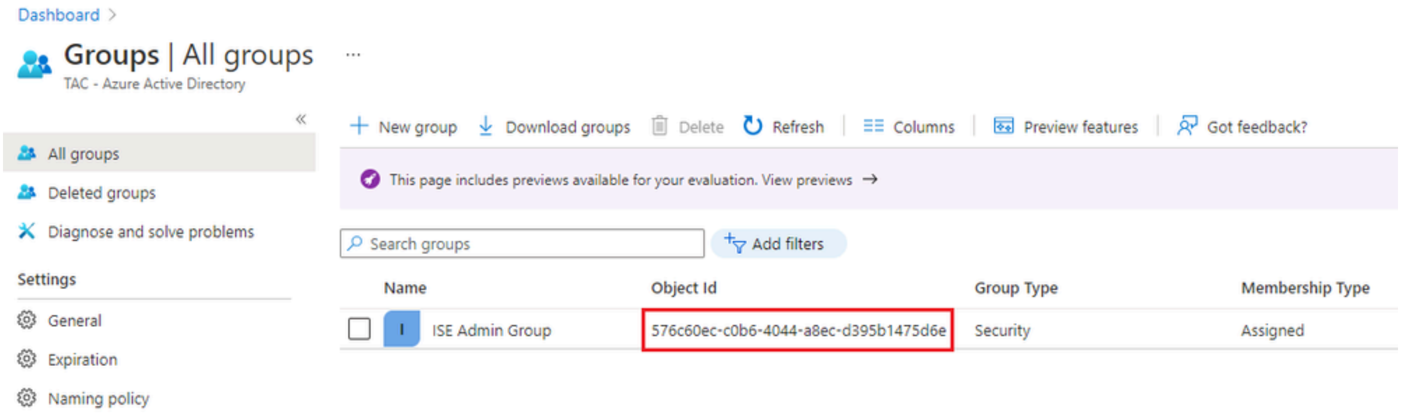
mck

MC mck
mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

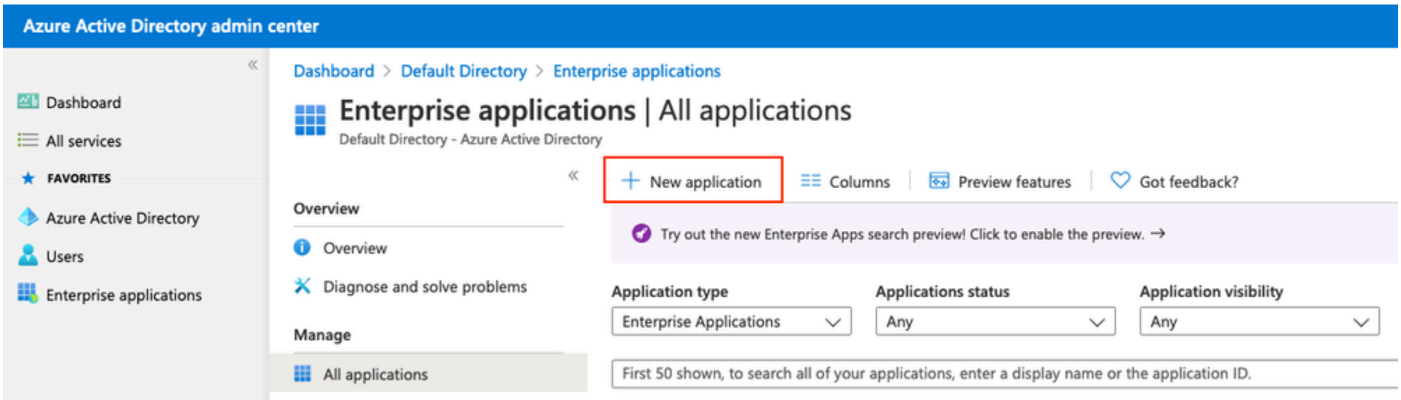
Make a note of **Group Object id**, in this screen, it is **576c60ec-c0b6-4044-a8ec-d395b1475d6e** for **ISE Admin Group** as shown in the image.



	Name	Object Id	Group Type	Membership Type
□	I ISE Admin Group	576c60ec-c0b6-4044-a8ec-d395b1475d6e	Security	Assigned

4. Create an Azure AD Enterprise Application

Under AD, select **Enterprise Applications** and click **New application**.



Enterprise applications | All applications

Default Directory - Azure Active Directory

Try out the new Enterprise Apps search preview! Click to enable the preview. →

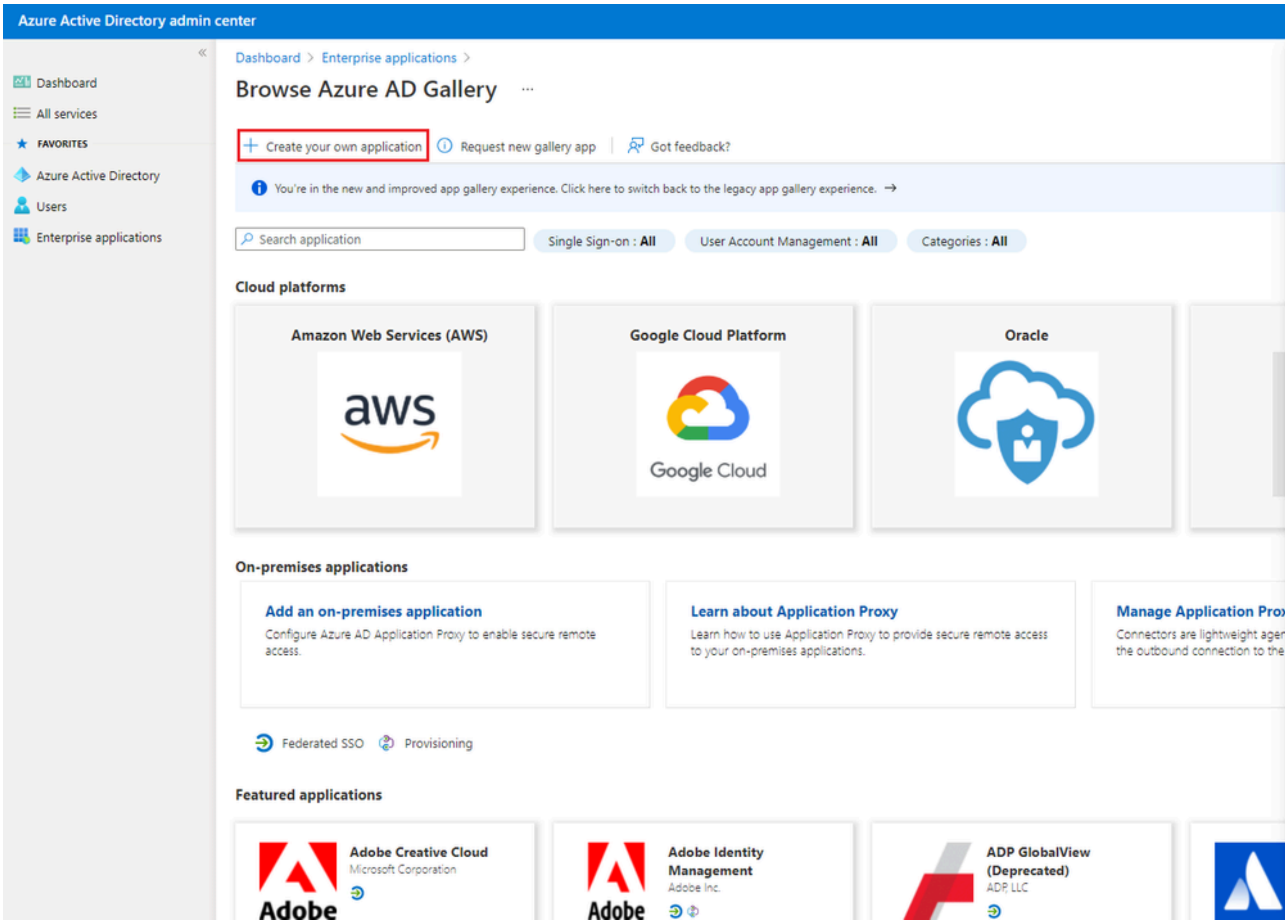
Application type: Enterprise Applications

Applications status: Any

Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Select the **Create your own application**.



Browse Azure AD Gallery

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

Add an on-premises application

Configure Azure AD Application Proxy to enable secure remote access.

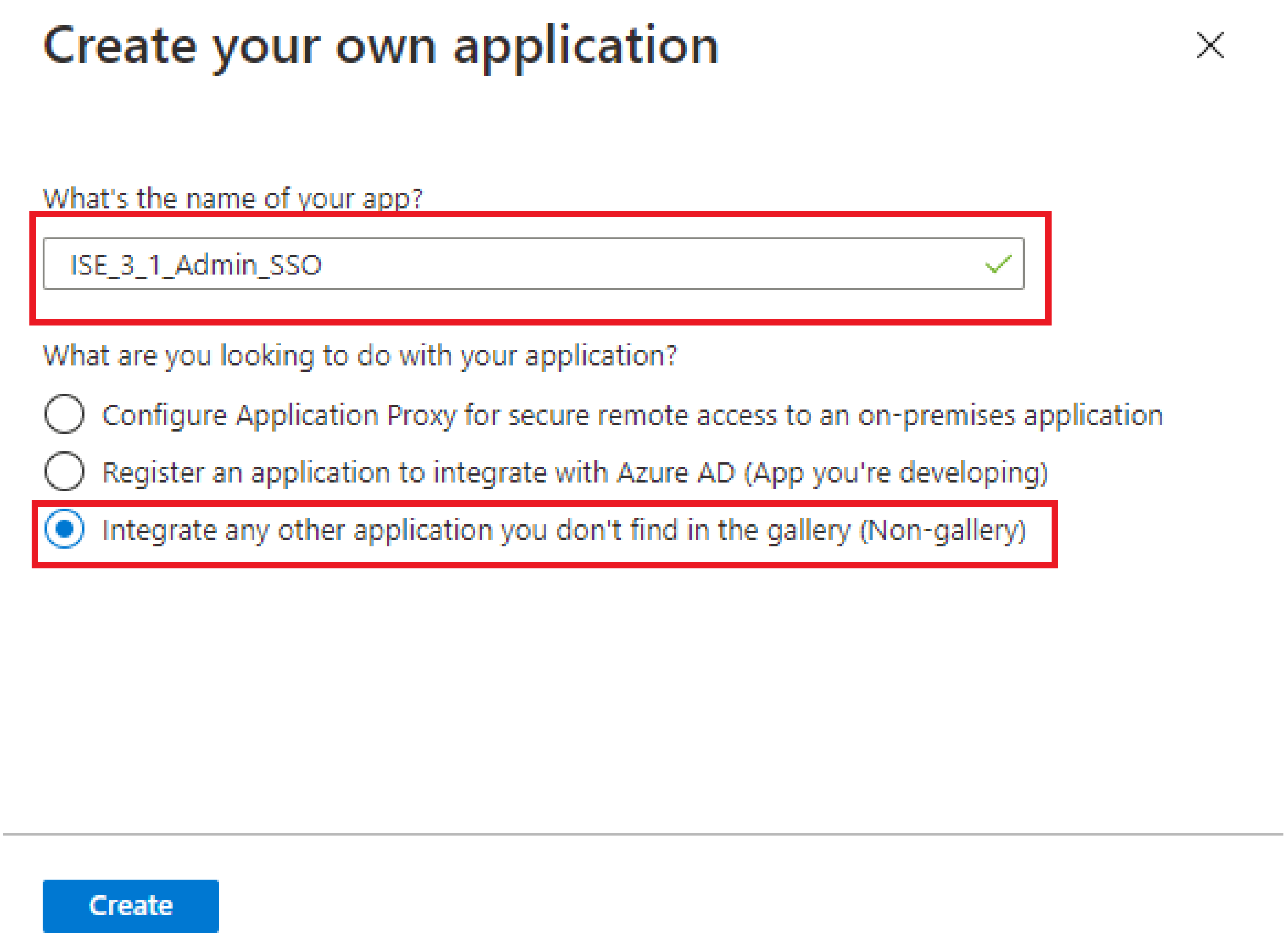
Learn about Application Proxy

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

Manage Application Prox

Connectors are lightweight ager the outbound connection to the

Enter the name of your application and select the **Integrate any other application you do not find in the gallery (Non-gallery)** radio button and click on the **Create** button as shown in the image**.**



Create your own application

What's the name of your app?

ISE_3_1_Admin_SSO

What are you looking to do with your application?

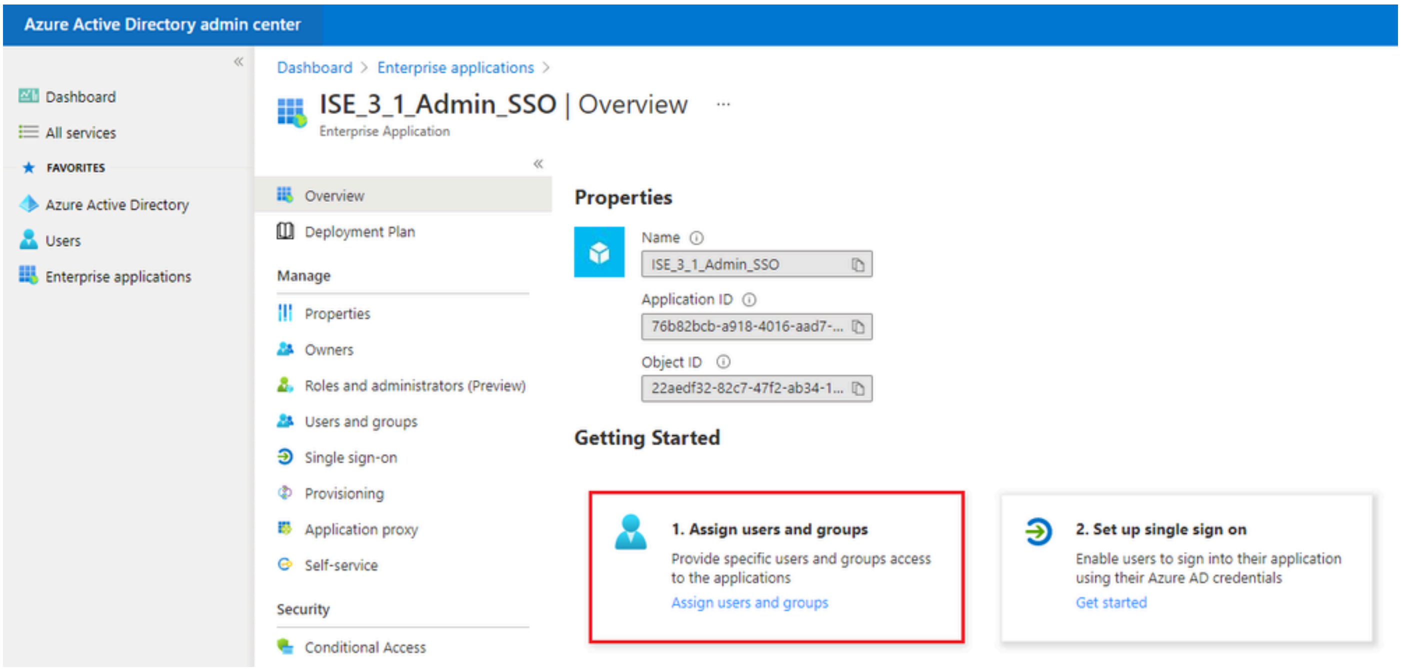
○ Configure Application Proxy for secure remote access to an on-premises application

○ 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)

5. Add Group to the Application

Select **Assign users and groups**.



Name: ISE_3_1_Admin_SSO

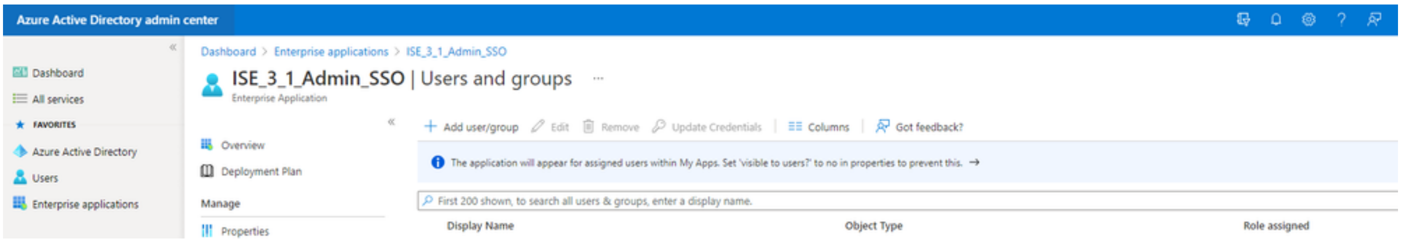
Application ID: 76b82bcb-a918-4016-aad7-...

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

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

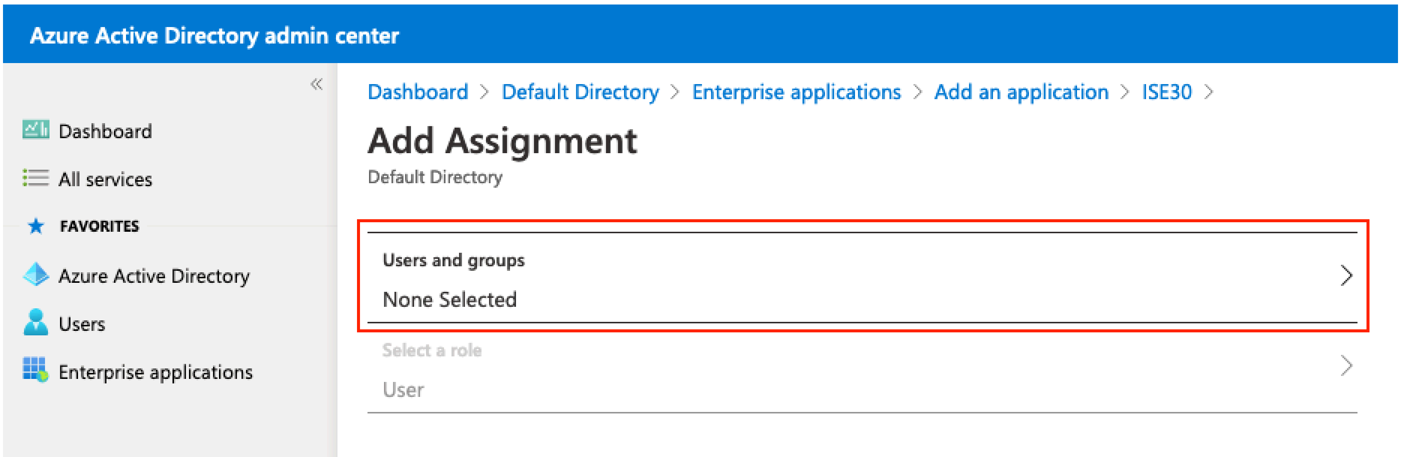
Click **Add user/group**.



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.

Click **Users and groups**.

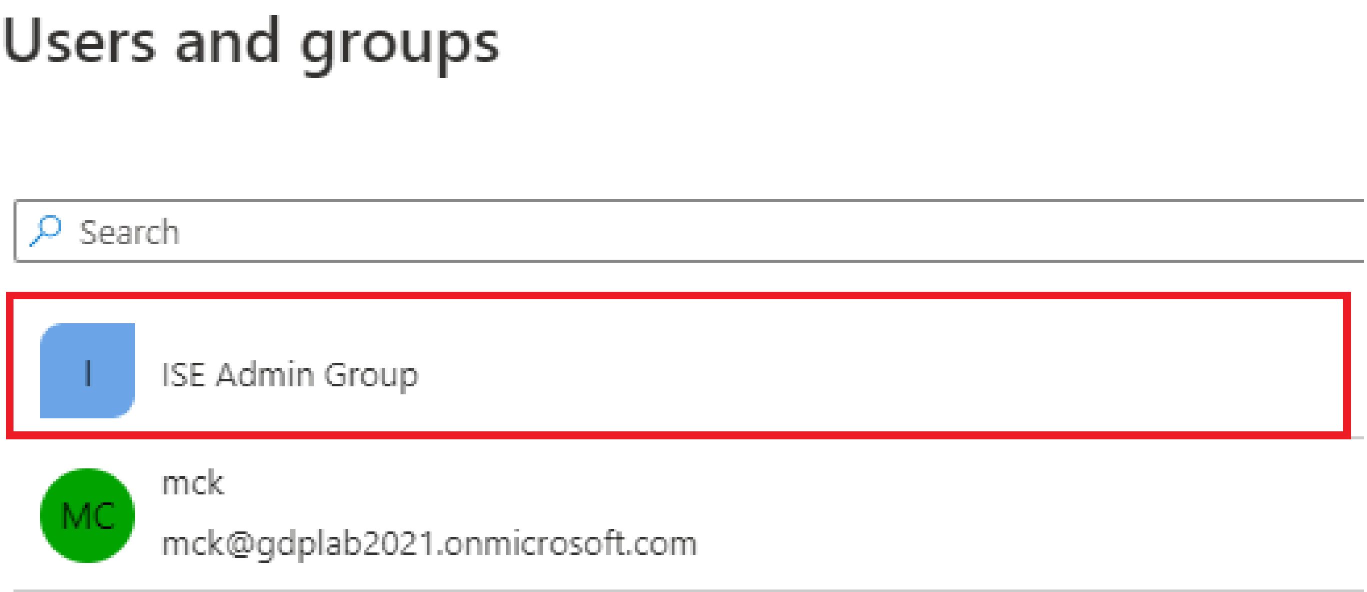

Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Default Directory > Enterprise applications > Add an application > ISE30 >
Add Assignment
Default Directory

Users and groups
None Selected

Select a role
User

Choose the Group configured previously and click **Select.**

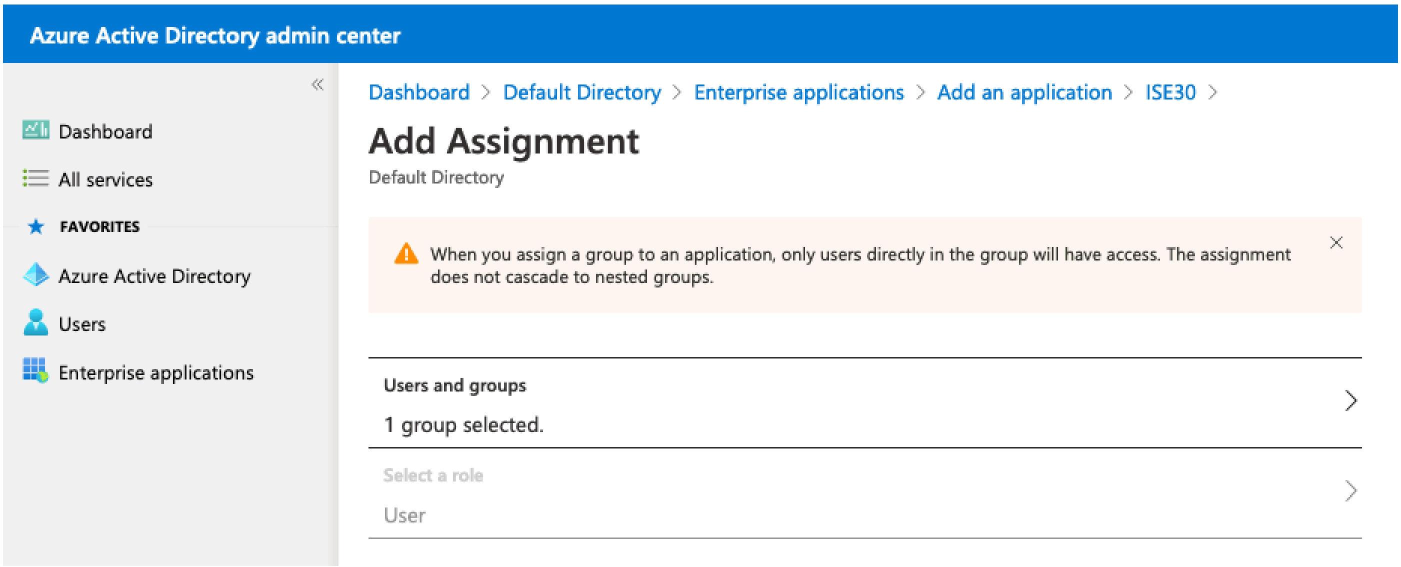
Note: Select the right set of users or groups who get access as intended as the users and groups mentioned here get access to the ISE once the setup is complete.



ISE Admin Group

mck
mck@gdplab2021.onmicrosoft.com

Once the Group is selected, click **Assign**.


Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
Dashboard > Default Directory > Enterprise applications > Add an application > ISE30 >

Add Assignment

Default Directory

When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

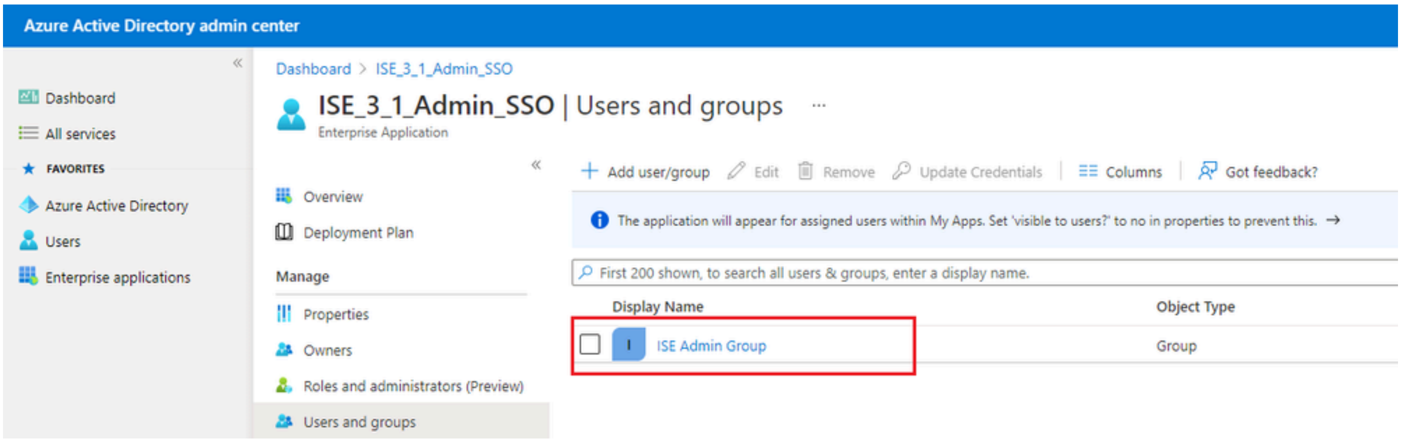
Users and groups

1 group selected.

Select a role

User

As a result, the **Users and groups** Menu for the configured application is populated with the selected Group.



ISE_3_1_Admin_SSO | Users and groups ...

Enterprise Application

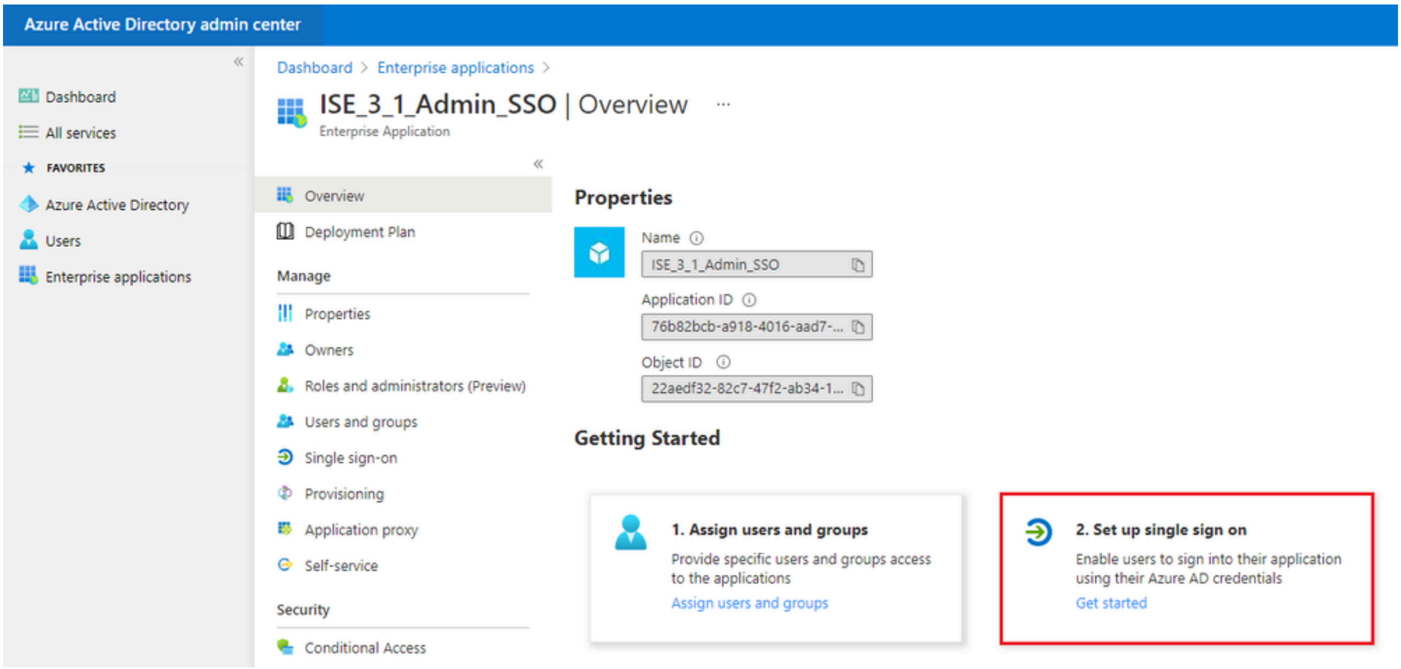
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

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

Display Name	Object Type
□ I ISE Admin Group	Group

6. Configure an Azure AD Enterprise Application

Navigate back to your Application and click **Set up single sign on**.



ISE_3_1_Admin_SSO | Overview ...

Enterprise Application

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

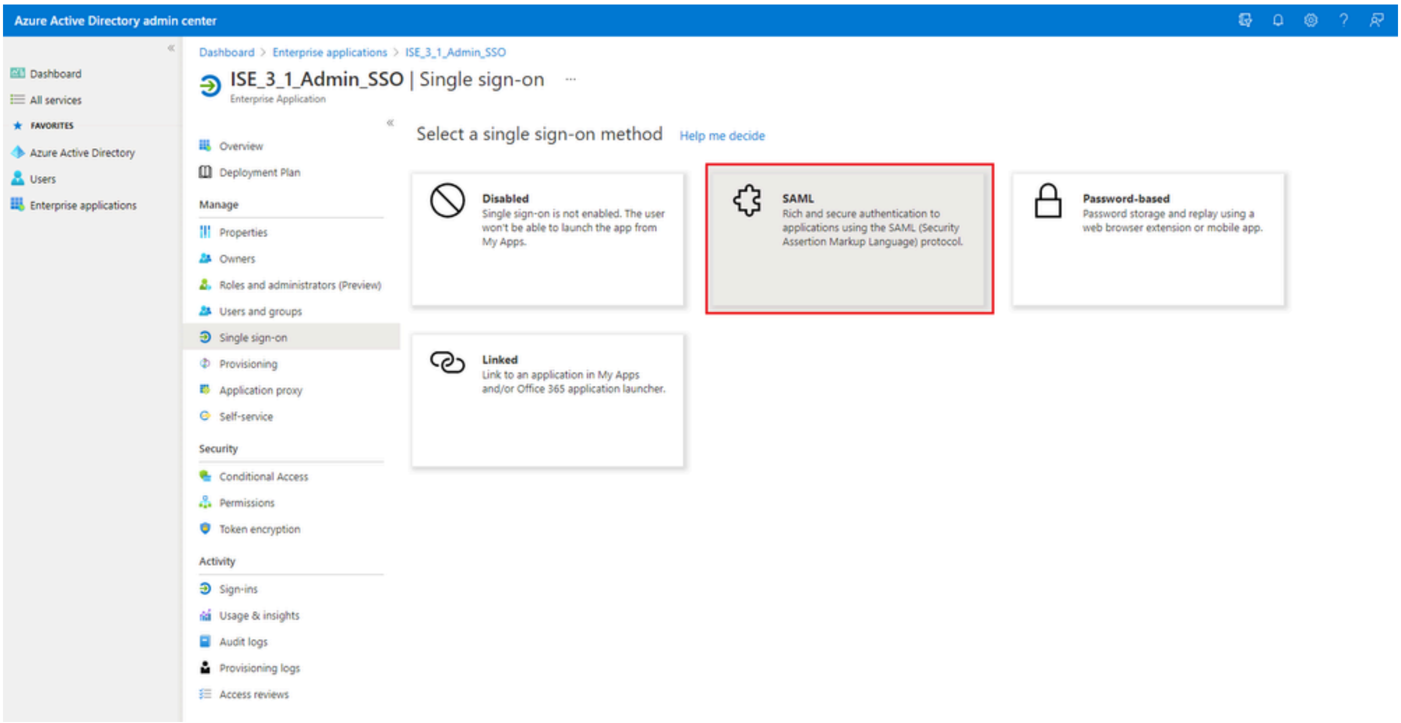
Assign users and groups

2. Set up single sign on

Enable users to sign into their application using their Azure AD credentials

Get started

Select **SAML** on the next screen.



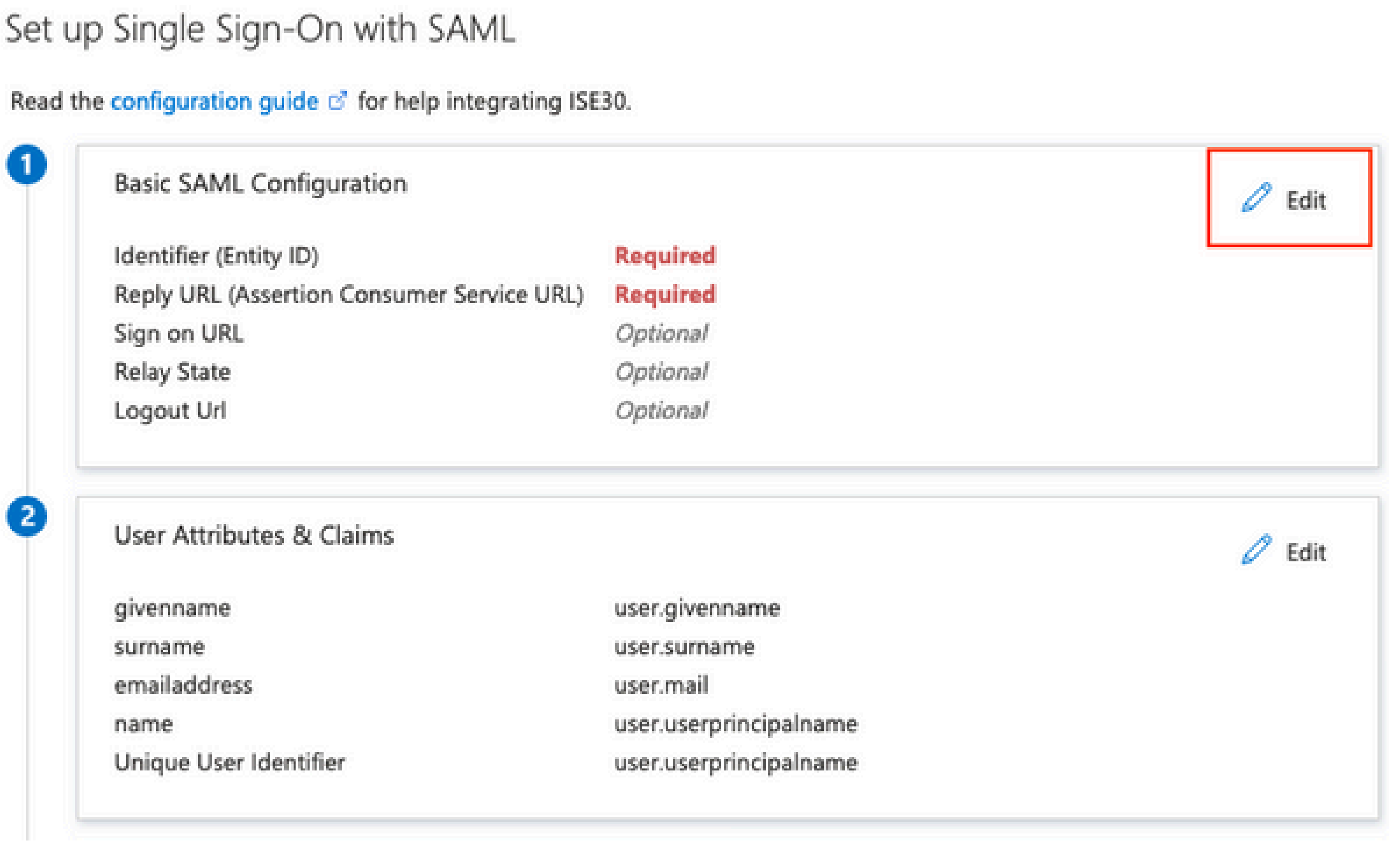
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

Click **Edit** next to **Basic SAML Configuration**.


Set up Single Sign-On with SAML
Read the configuration guide for help integrating ISE30.
1
2
Edit
Edit

Basic SAML Configuration

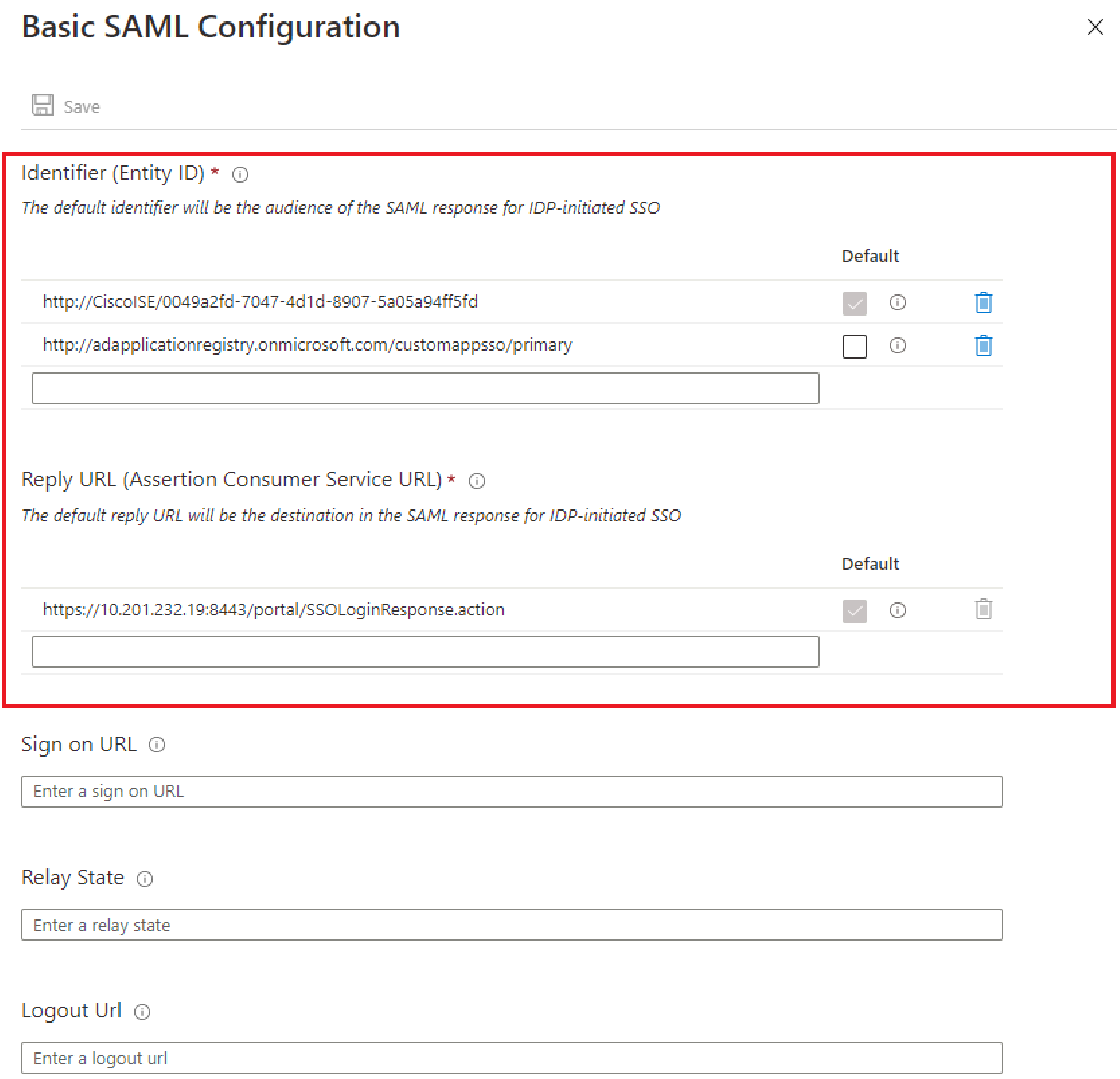
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional

User Attributes & Claims

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

Populate Identifier (Entity ID) with the value of **entityID** from the XML file from step **Export Service Provider Information.** Populate **Reply URL (Assertion Consumer Service URL)** with the value of **Locations** from **AssertionConsumerService.** Click **Save**.

Note: Reply URL acts as a pass list, which allows certain URLs to act as a source when redirected to the IdP page.



Basic SAML Configuration

Identifier (Entity ID) *

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

	Default
http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd	☑
http://adapplicationregistry.onmicrosoft.com/customappsso/primary	□

Reply URL (Assertion Consumer Service URL) *

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

	Default
https://10.201.232.19:8443/portal/SSOLoginResponse.action	☑

Sign on URL

Enter a sign on URL

Relay State

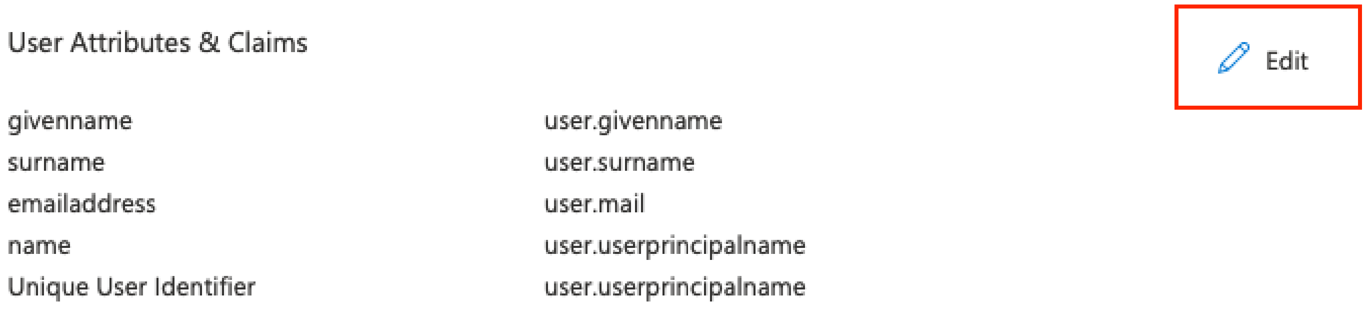
Enter a relay state

Logout Url

Enter a logout url

7. Configure Active Directory Group Attribute

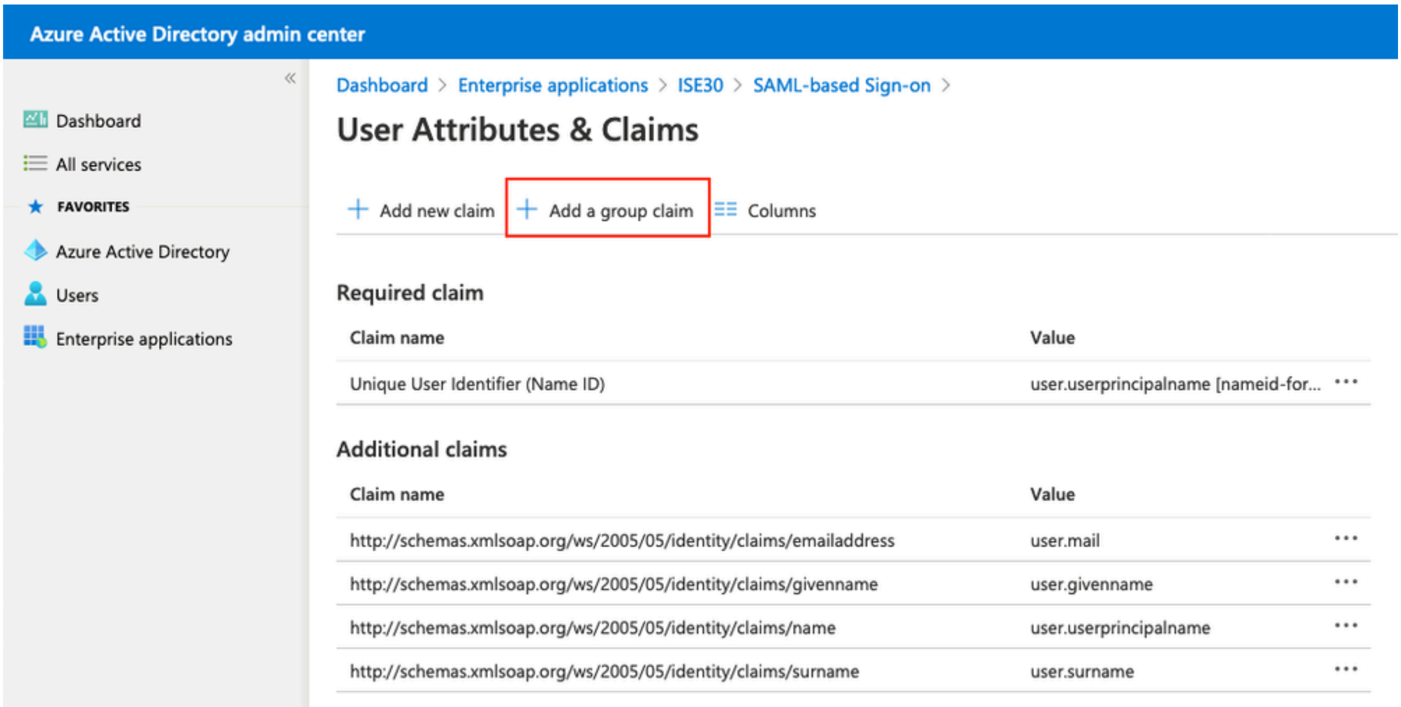
In order to return the group attribute value configured previously, click **Edit** next to the **User Attributes & Claims**.



User Attributes & Claims

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

Click **Add a group claim**.



User Attributes & Claims

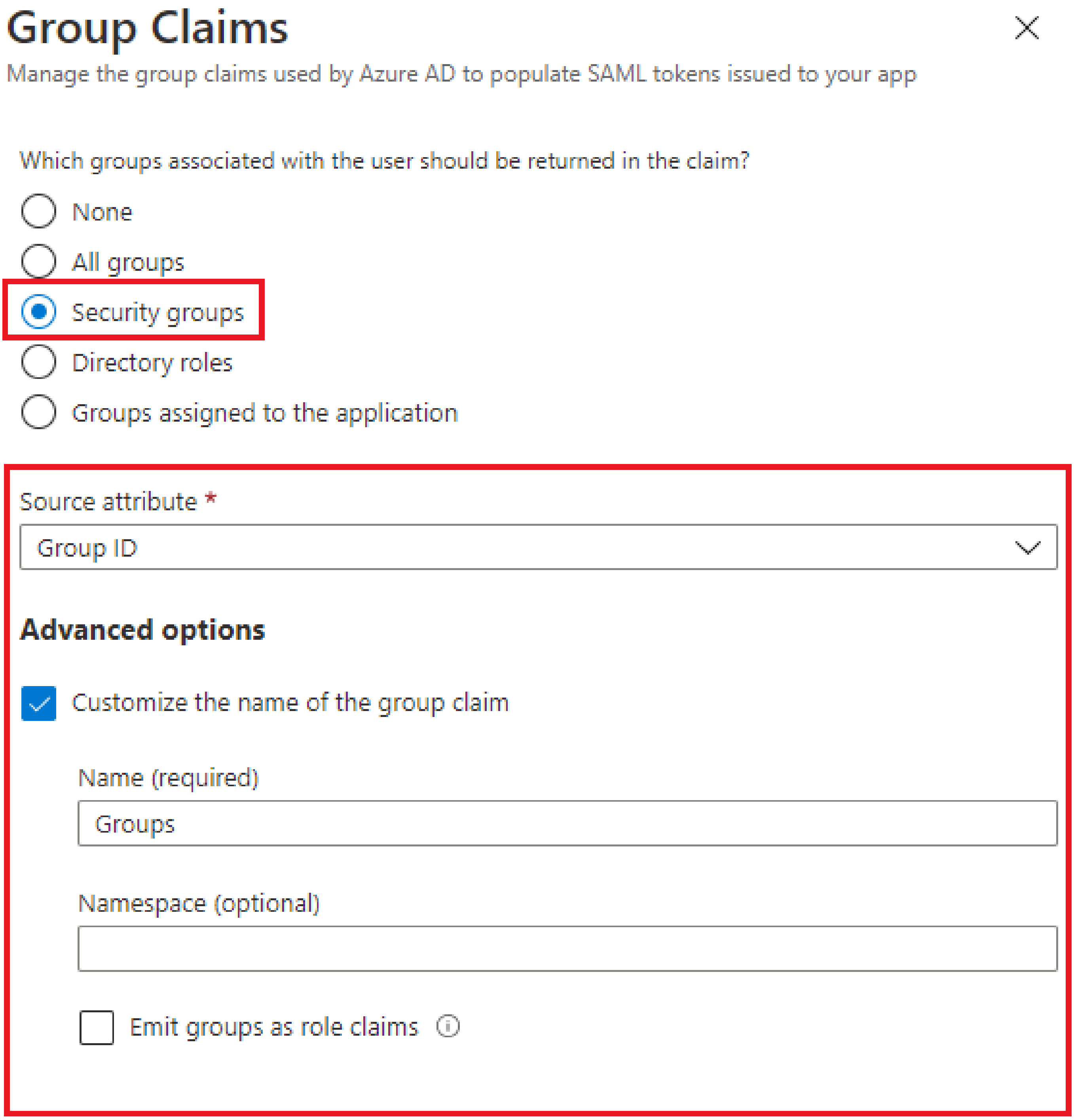
Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Select **Security groups** and click **Save**. Select **Group ID** under the **Source attribute** drop-down menu. Select the checkbox to customize the name of the group claim and enter the name **Groups**.



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

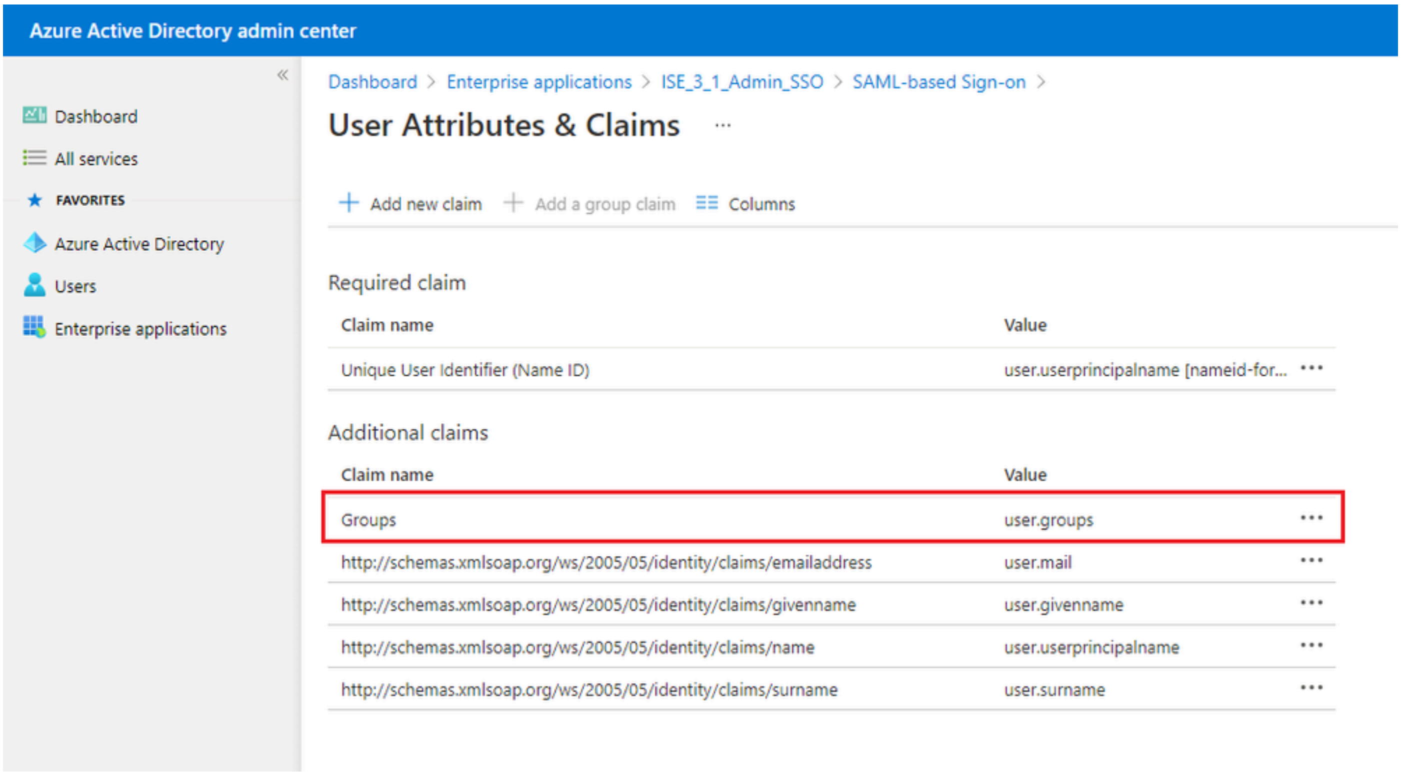
Name (required)

Groups

Namespace (optional)

□ Emit groups as role claims

Make a note of the **Claim name** for the group. In this case, it is **Groups.**


Azure Active Directory admin center
Dashboard
All services
FAVORITES
Azure Active Directory
Users
Enterprise applications
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

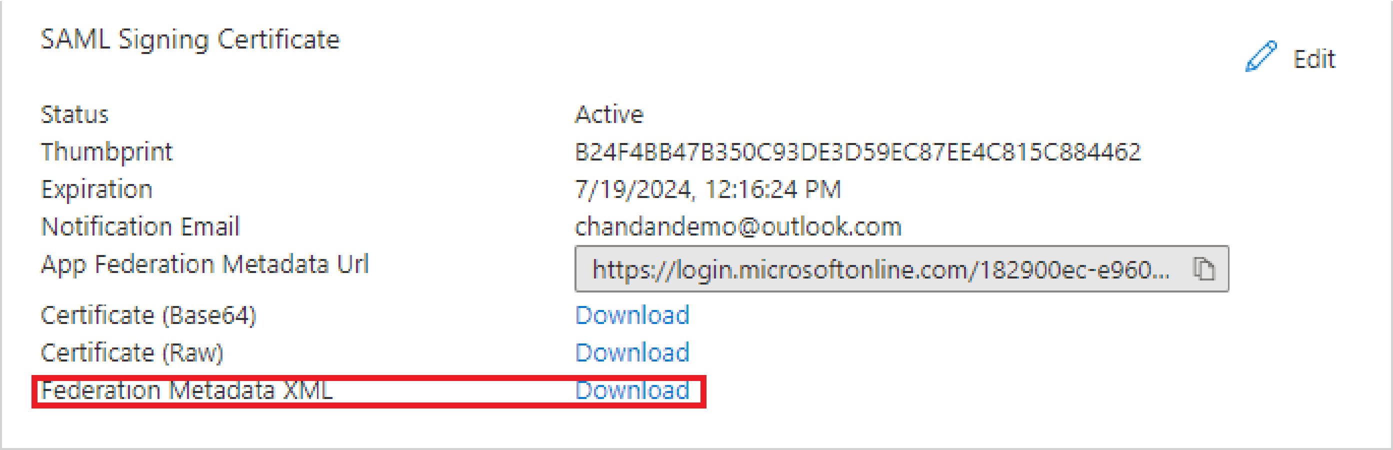
Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...

Additional claims

Claim name	Value
Groups	user.groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

8. Download Azure Federation Metadata XML File

Click **Download** against **Federation Metadata XML** in **SAML Signing Certificate**.

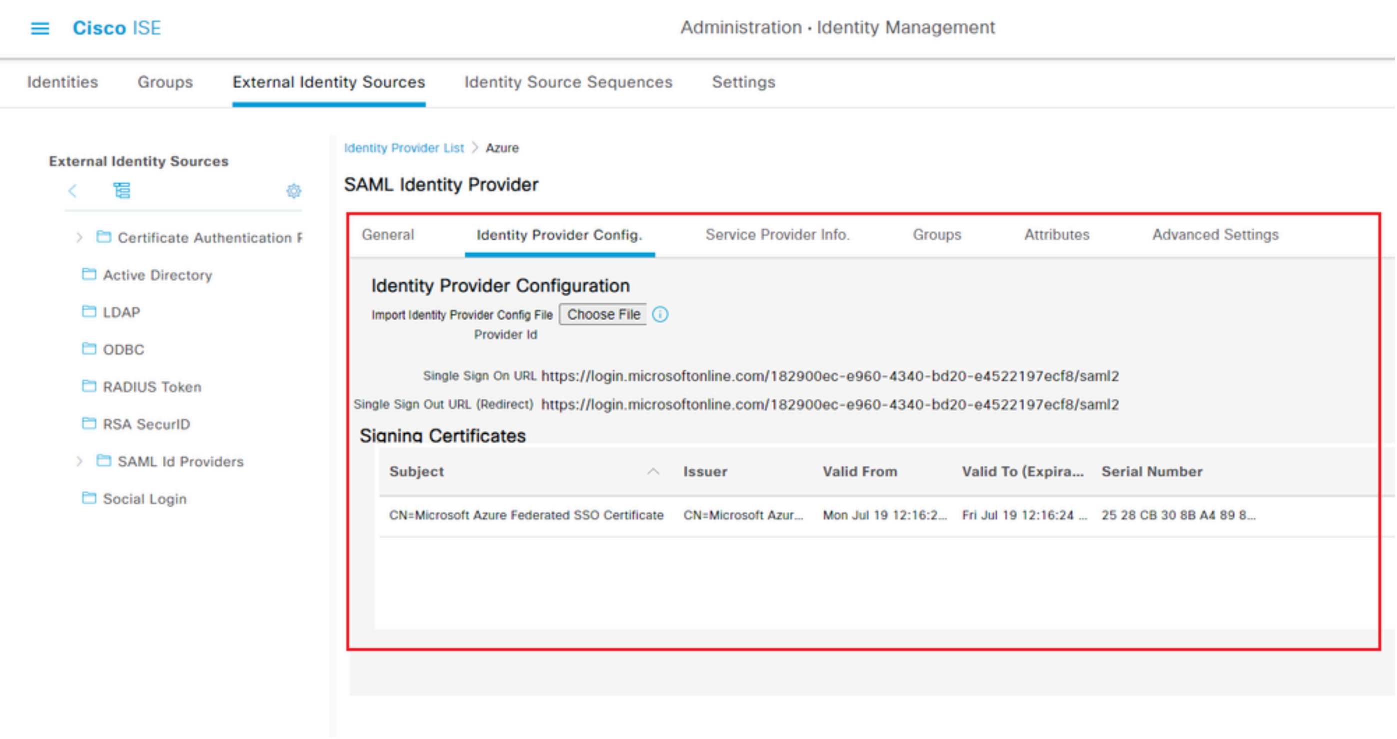


Status	Active
Thumbprint	B24F4BB47B350C93DE3D59EC87EE4C815C884462
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182900ec-e960...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML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

Step 3. Upload MetaData from Azure Active Directory to ISE

Navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider].**

Switch the tab to **Identity Provider Config.** and click **Browse**. Select **Federation Metadata XML** file from step **Download Azure Federation Metadata XML** and click **Save**.


Cisco ISE — Administration · Identity Management

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

External Identity Sources
- Certificate Authentication F
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Identity Provider List > Azure

SAML Identity Provider

General | Identity Provider Config. | Service Provider Info. | Groups | Attributes | Advanced Settings

Identity Provider Configuration

Import Identity Provider Config File: Choose File

Provider Id

Single Sign On URL: https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2

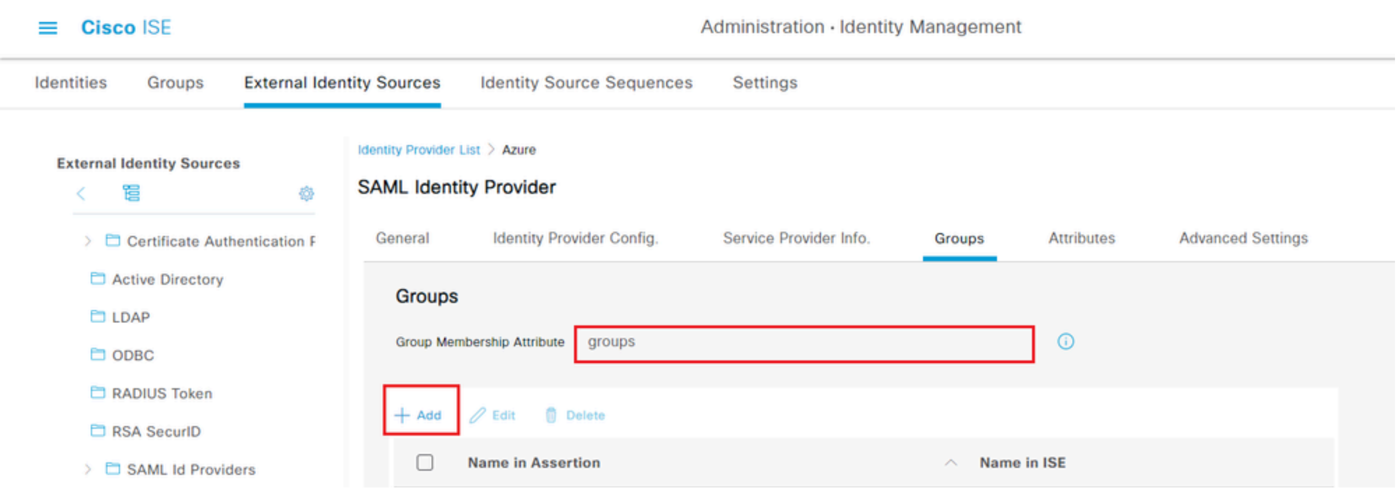
Single Sign Out URL (Redirect): https://login.microsoftonline.com/182900ec-e960-4340-bd20-e4522197ecf8/saml2

Signing Certificates

Subject	Issuer	Valid From	Valid To (Expira...	Serial Number
CN=Microsoft Azure Federated SSO Certificate	CN=Microsoft Azur...	Mon Jul 19 12:16:2...	Fri Jul 19 12:16:24 ...	25 28 CB 30 8B A4 89 8...

Step 4. Configure SAML Groups on ISE

Switch to tab **Groups** and paste the value of **Claim name** from **Configure Active Directory Group attribute** into **Group Membership Attribute**.


Cisco ISE — Administration · Identity Management

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

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 | Attributes | Advanced Settings

Groups

Group Membership Attribute: groups

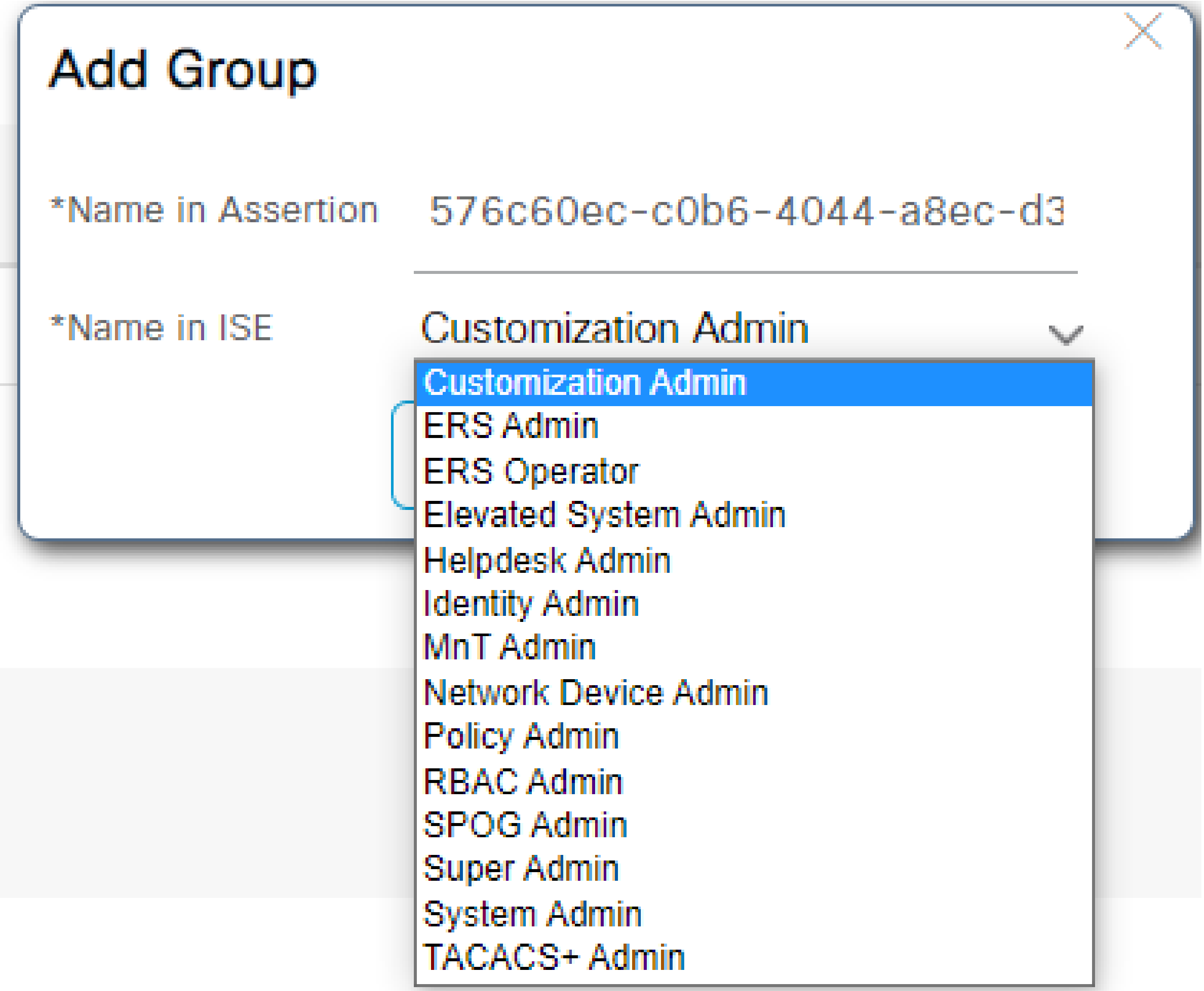
+ Add | Edit | Delete

□	Name in Assertion	Name in ISE

Click on **Add**. Populate **Name in Assertion** with the value of **Group Object id** of **ISE Admin Group** captured in **Assign Azure Active Directory User to the Group.**

Configure **Name in ISE** with the drop-down and select the appropriate group on ISE. In this example, the group used is **Super Admin.** Click **OK.** Click **Save.**

This creates a mapping between Group in Azure and Group name on ISE.



Add Group

*Name in Assertion 576c60ec-c0b6-4044-a8ec-d3

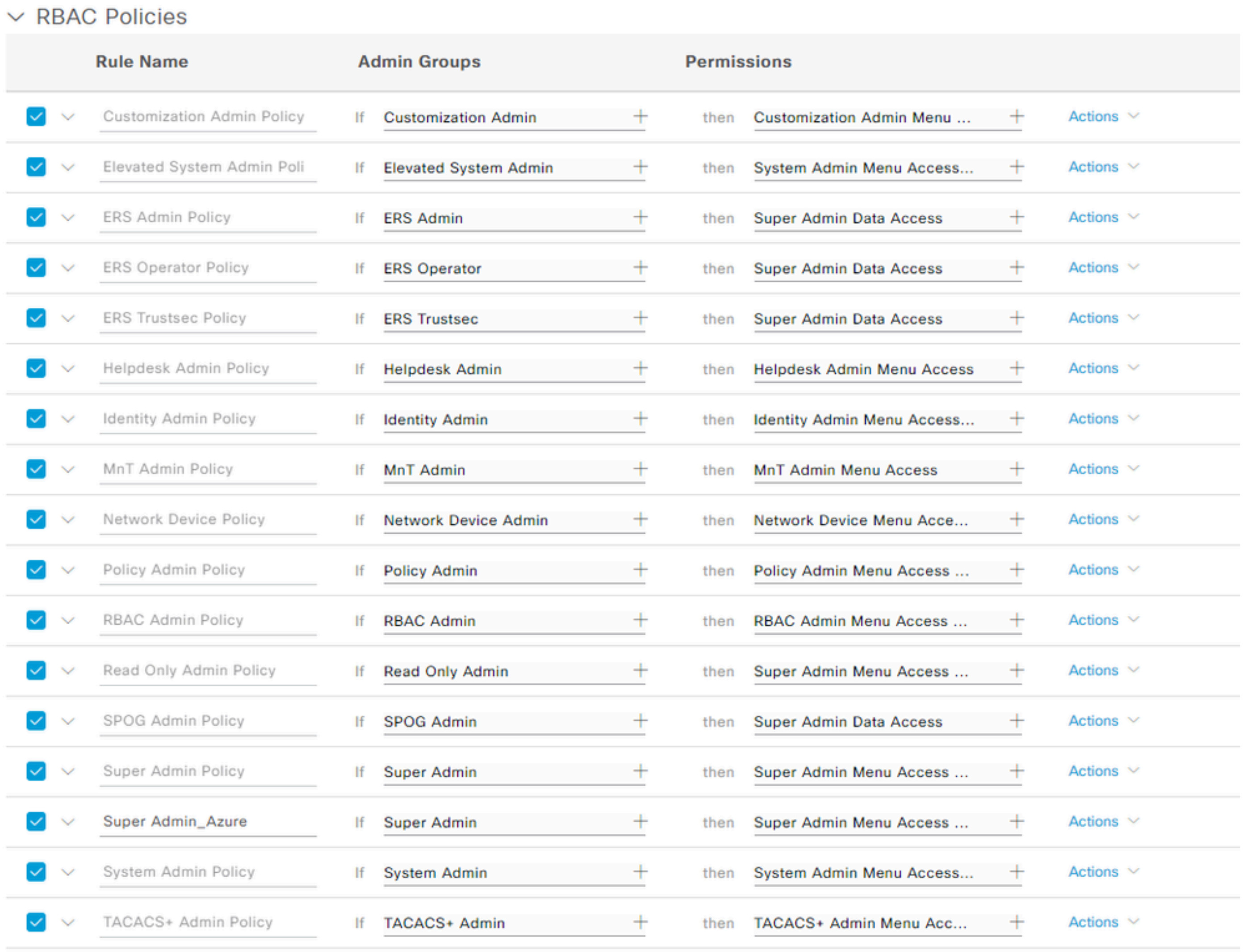
*Name in ISE Customization Admin

(Optional) Step 5. Configure RBAC Policies

From the previous step, there are many different types of user access levels that can be configured on ISE.

To edit Role Based Access Control Policies (RBAC) navigate to **Administration** > **System** > **Admin Access** > **Authorization** > **Permissions** > **RBAC Policies** and configure as needed.

This image is a reference to the sample configuration.



RBAC Policies

	Rule Name		Admin Groups		Permissions	
☑	Customization Admin Policy	If	Customization Admin	then	Customization Admin Menu ...	Actions
☑	Elevated System Admin Poli	If	Elevated System Admin	then	System Admin Menu Access...	Actions
☑	ERS Admin Policy	If	ERS Admin	then	Super Admin Data Access	Actions
☑	ERS Operator Policy	If	ERS Operator	then	Super Admin Data Access	Actions
☑	ERS Trustsec Policy	If	ERS Trustsec	then	Super Admin Data Access	Actions
☑	Helpdesk Admin Policy	If	Helpdesk Admin	then	Helpdesk Admin Menu Access	Actions
☑	Identity Admin Policy	If	Identity Admin	then	Identity Admin Menu Access...	Actions
☑	MnT Admin Policy	If	MnT Admin	then	MnT Admin Menu Access	Actions
☑	Network Device Policy	If	Network Device Admin	then	Network Device Menu Acce...	Actions
☑	Policy Admin Policy	If	Policy Admin	then	Policy Admin Menu Access ...	Actions
☑	RBAC Admin Policy	If	RBAC Admin	then	RBAC Admin Menu Access ...	Actions
☑	Read Only Admin Policy	If	Read Only Admin	then	Super Admin Menu Access ...	Actions
☑	SPOG Admin Policy	If	SPOG Admin	then	Super Admin Data Access	Actions
☑	Super Admin Policy	If	Super Admin	then	Super Admin Menu Access ...	Actions
☑	Super Admin_Azure	If	Super Admin	then	Super Admin Menu Access ...	Actions
☑	System Admin Policy	If	System Admin	then	System Admin Menu Access...	Actions
☑	TACACS+ Admin Policy	If	TACACS+ Admin	then	TACACS+ Admin Menu Acc...	Actions

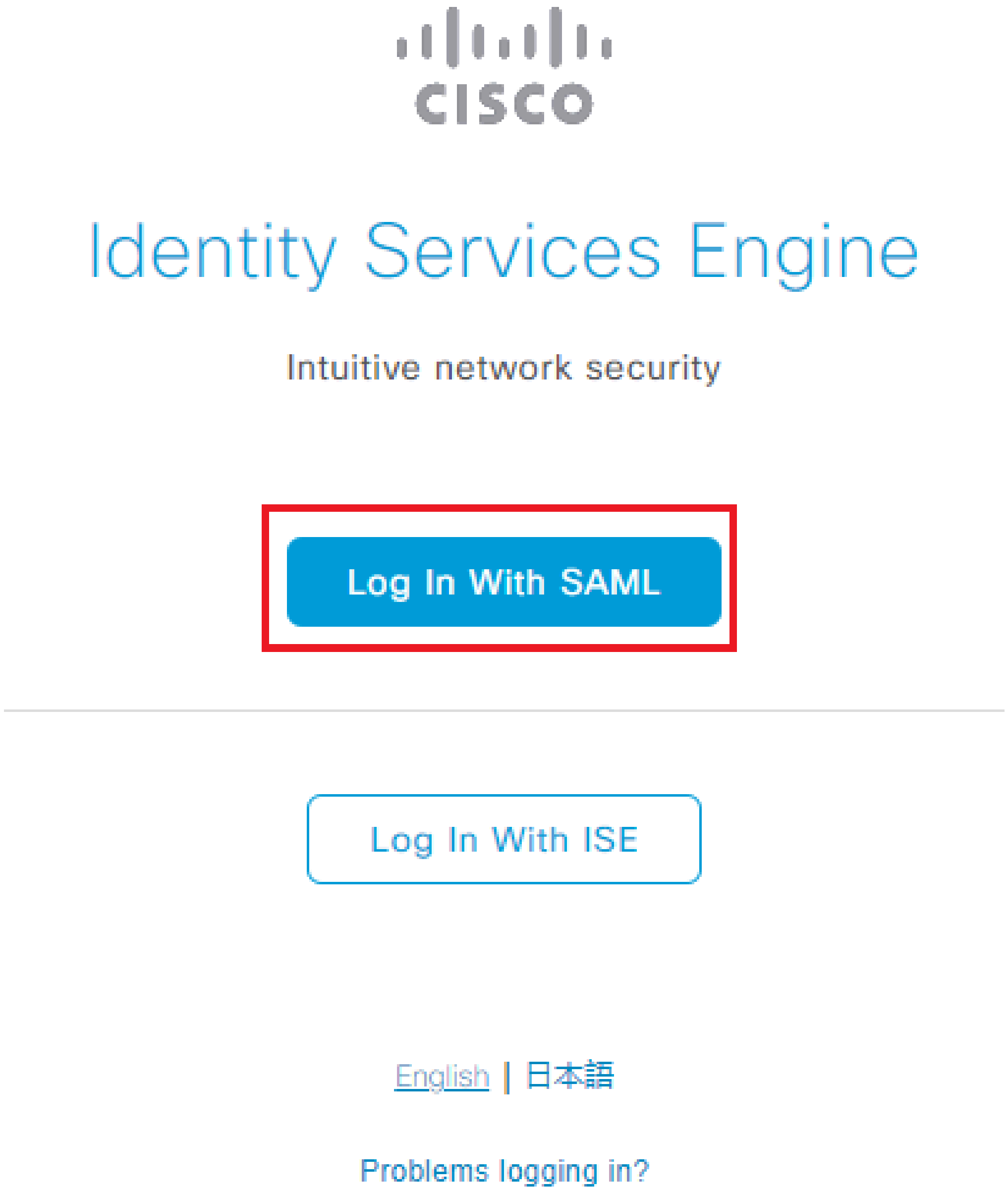
Verify

Confirm that your configuration works properly.

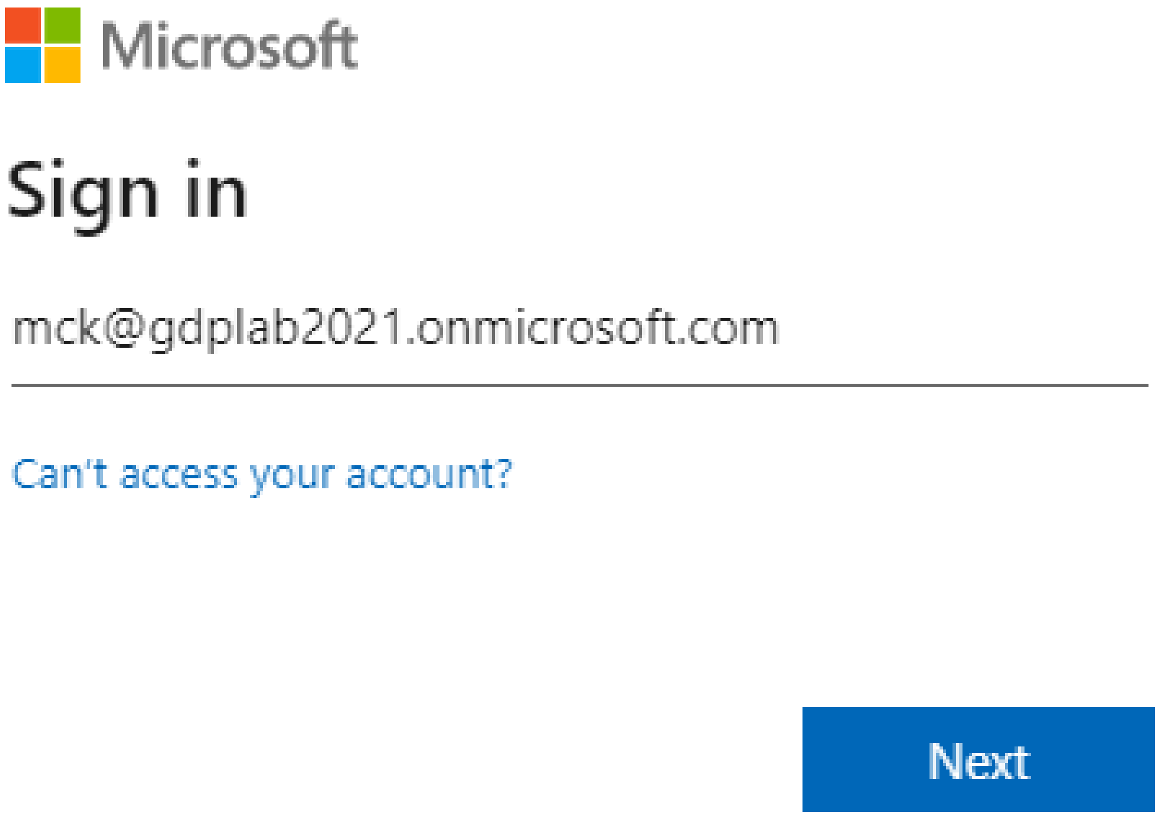
Note: SAML SSO Login test from the Azure test functionality does not work. The SAML request must be initiated by ISE for the Azure SAML SSO to work properly.

Open the ISE GUI Login prompt screen. You are presented with a new option to **Log In with SAML.**

1. Access your ISE GUI Login page and click **Log In with SAML**.



2. You are redirected to the Microsoft login screen. Enter your **Username** credentials of an account in a group mapped to ISE as shown here and click **Next** as shown in the image.

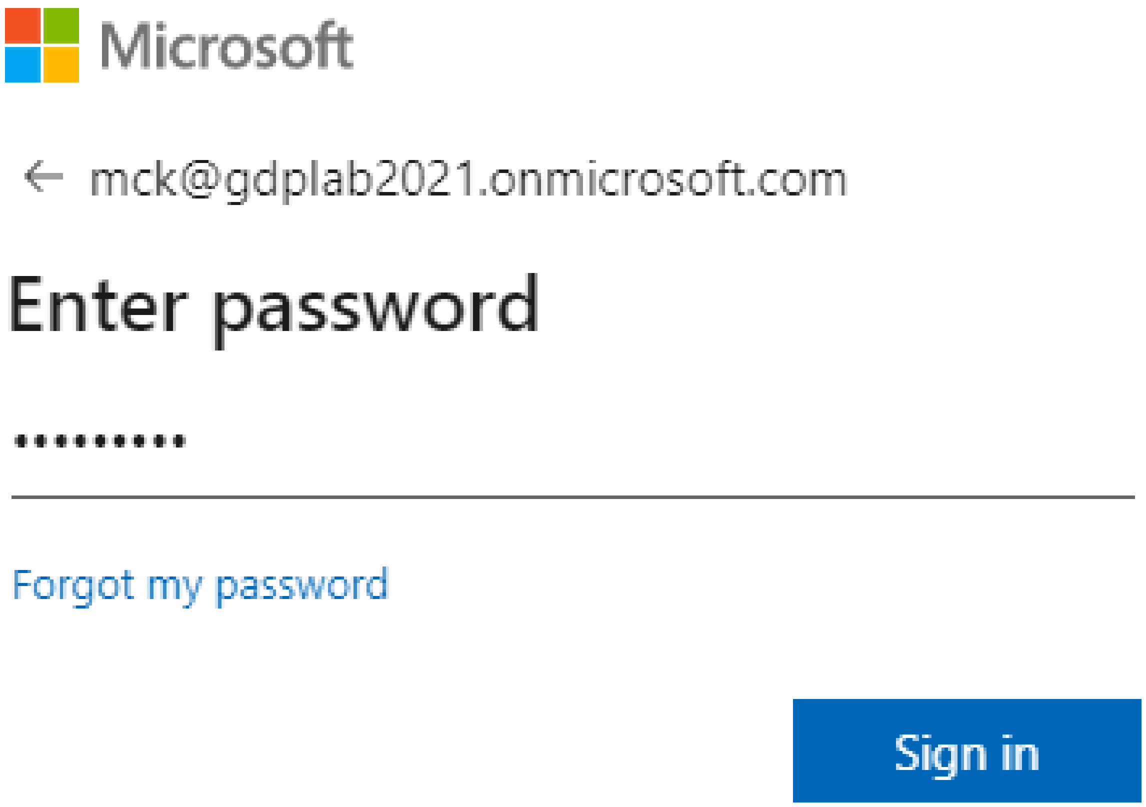


Microsoft

Sign in

mck@gdplab2021.onmicrosoft.com

3. Enter your **Password** for the user and click **Sign In.**

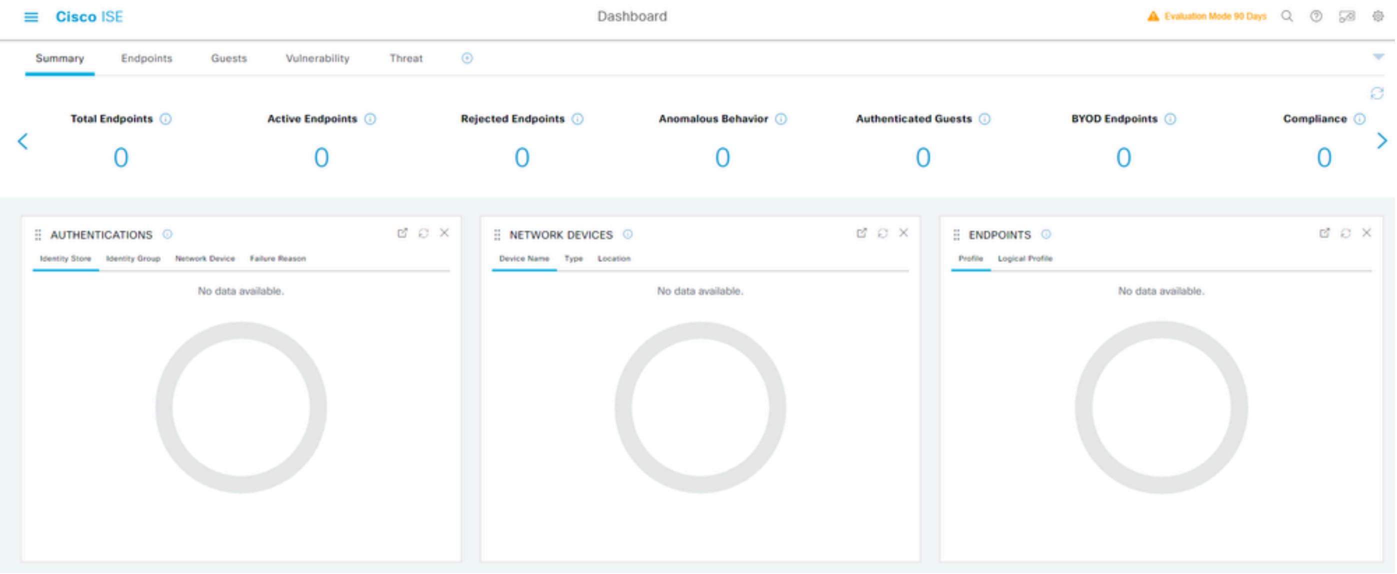


← mck@gdplab2021.onmicrosoft.com

Enter password

••••••••••

4. You are now be redirected to the ISE application dashboard with the appropriate permissions configured based on the ISE group configured previously as shown in the image.



Total Endpoints 0

Active Endpoints 0

Rejected Endpoints 0

Anomalous Behavior 0

Authenticated Guests 0

BYOD Endpoints 0

Compliance 0

No data available.

No data available.

No data available.

Troubleshoot

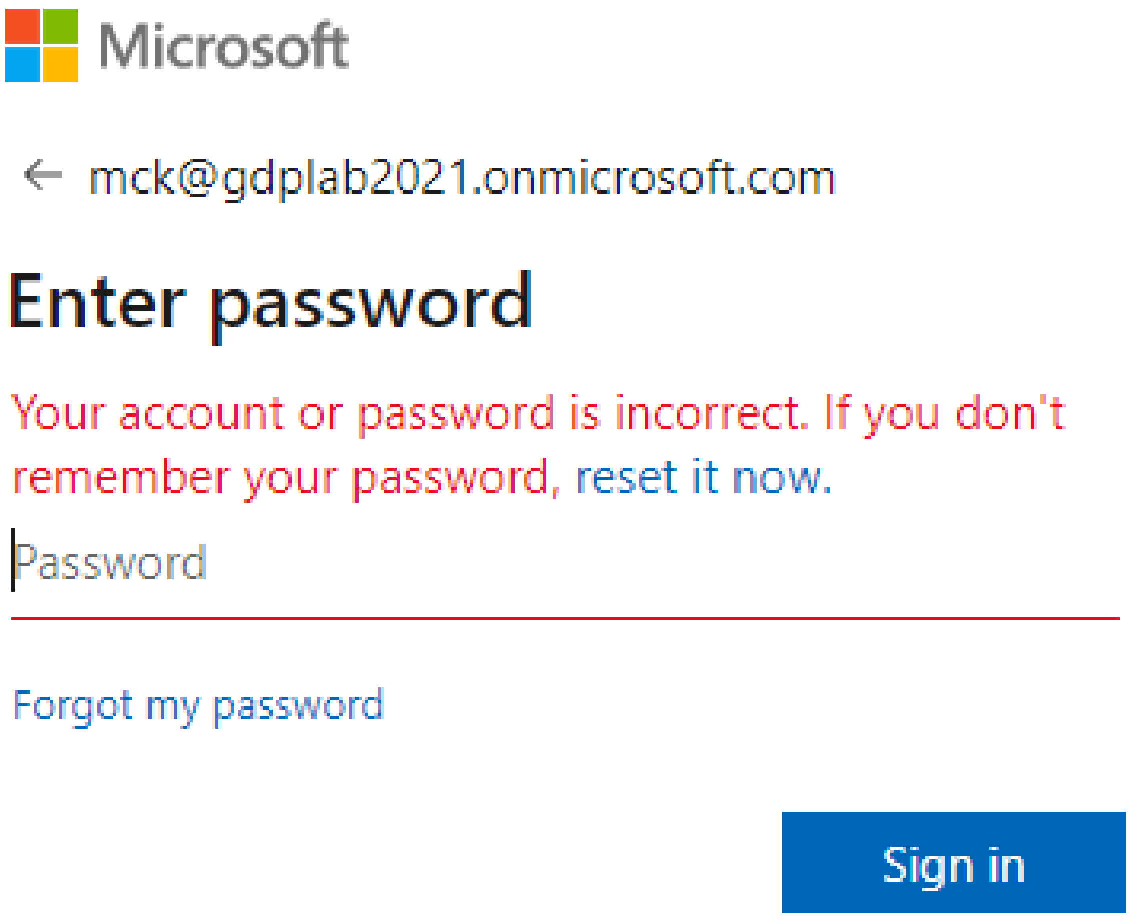
This section provides information you can use to troubleshoot your configuration.

Common Issues

It is vital to understand that SAML authentication is handled between the browser and the Azure Active Directory. Hence, you can get authentication-related errors directly from the Identity Provider (Azure) where ISE engagement has not started yet.

Issue 1. "Your account or password is incorrect" error is seen after you enter the credentials. Here, user data is not yet received by ISE and the process at this point still stays with IdP (Azure).

The most likely reason is that the account information is incorrect or the password is not correct. In order to fix: reset the password or provide the correct password for that account as shown in the image.



Microsoft

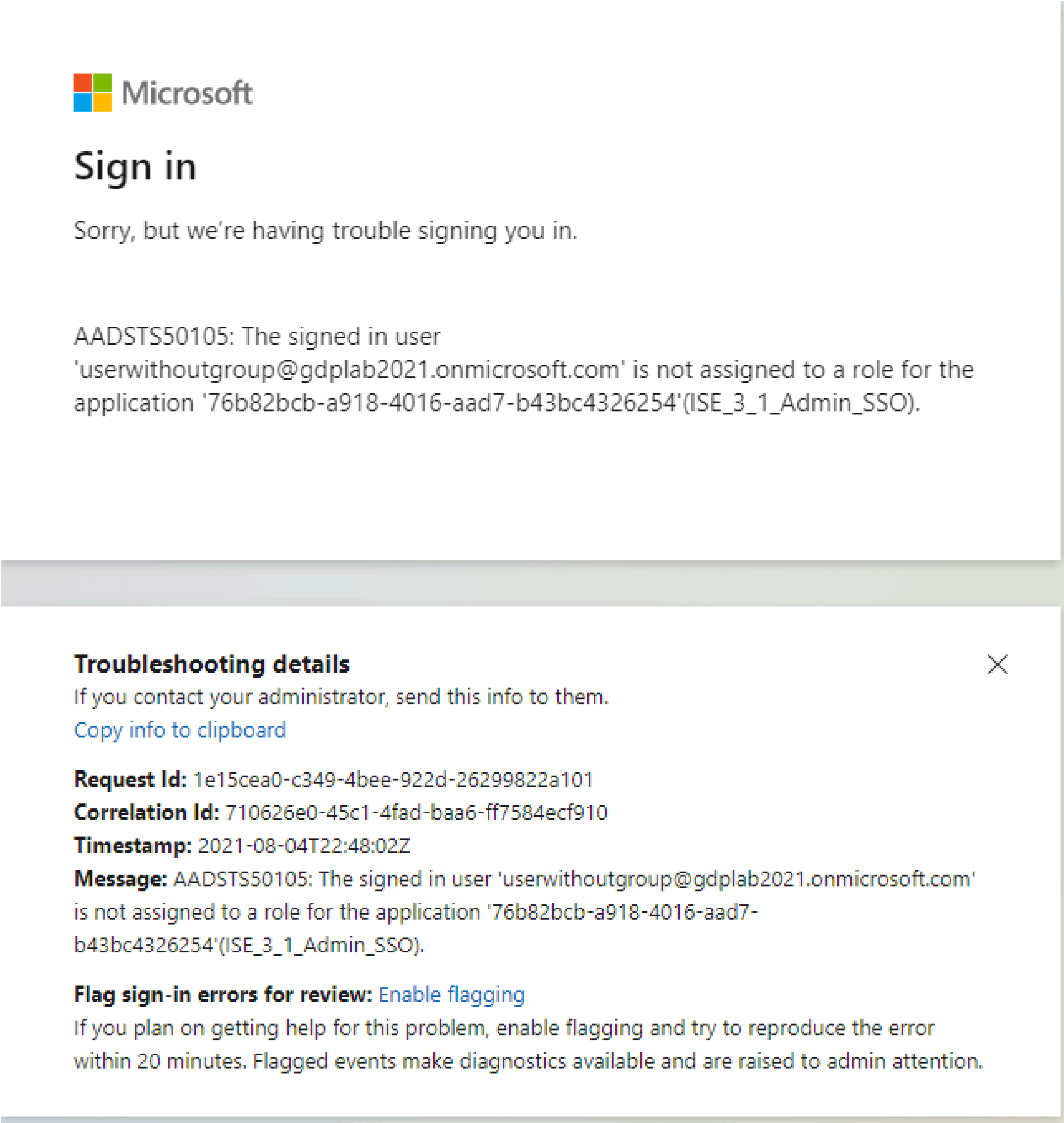
mck@gdplab2021.onmicrosoft.com

Enter password

Your account or password is incorrect. If you don't remember your password, reset it now.

Issue 2. The user is not part of the group which is supposed to be allowed to access SAML SSO. Similar to the previous case, user data is not yet received by ISE and the process at this point still stays with IdP (Azure).

In order to fix this: verify that the **Add group to the Application** configuration step is correctly executed as shown in the image.



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

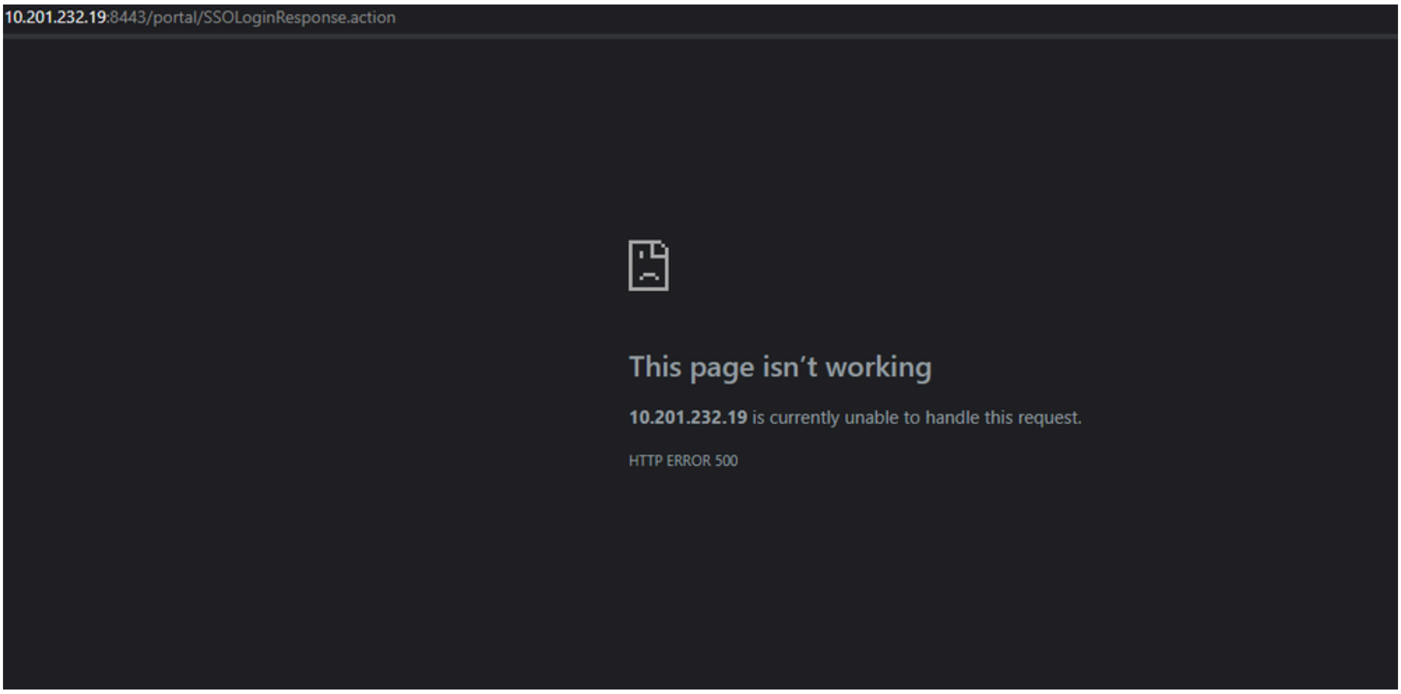
Timestamp: 2021-08-04T22:48:02Z

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.

Issue 3. ISE Application Server is unable to handle SAML login requests. This issue occurs when the SAML request is initiated from the Identity Provider, Azure, instead of the Service Provider, ISE. Testing SSO Login from Azure AD does not work as ISE does not support Identity Provider initiated SAML requests.

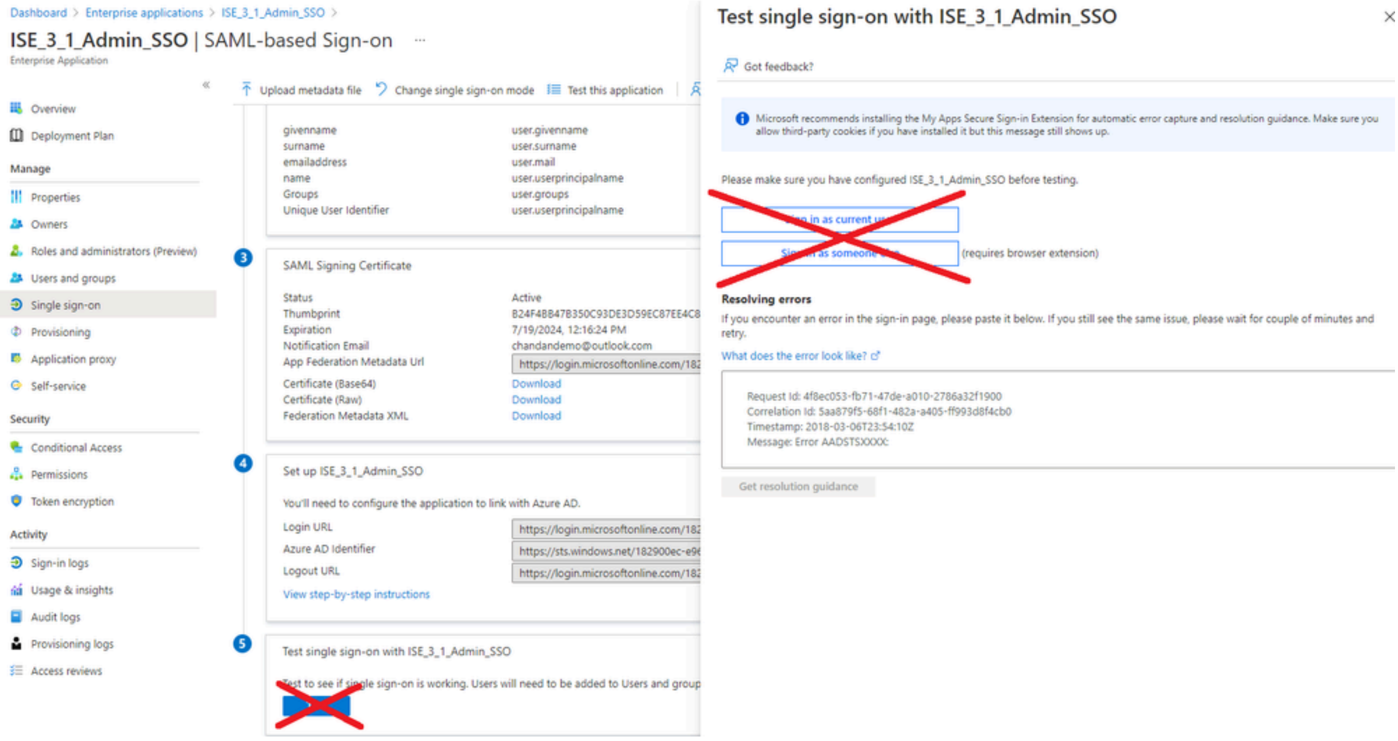


10.201.232.19:8443/portal/SSOLoginResponse.action

This page isn’t working

10.201.232.19 is currently unable to handle this request.

HTTP ERROR 500



Dashboard > Enterprise applications > ISE_3_1_Admin_SSO >

ISE_3_1_Admin_SSO | SAML-based Sign-on ···

Enterprise 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	B24F4BB47B350C93DE3D59EC87EE4C8
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 for automatic error capture and resolution guidance. Make sure you allow third-party cookies if you have installed it but this message still shows up.

Please make sure you have configured ISE_3_1_Admin_SSO before testing.

Sign in as current user

Sign in as someone else (requires browser extension)

Resolving errors

If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

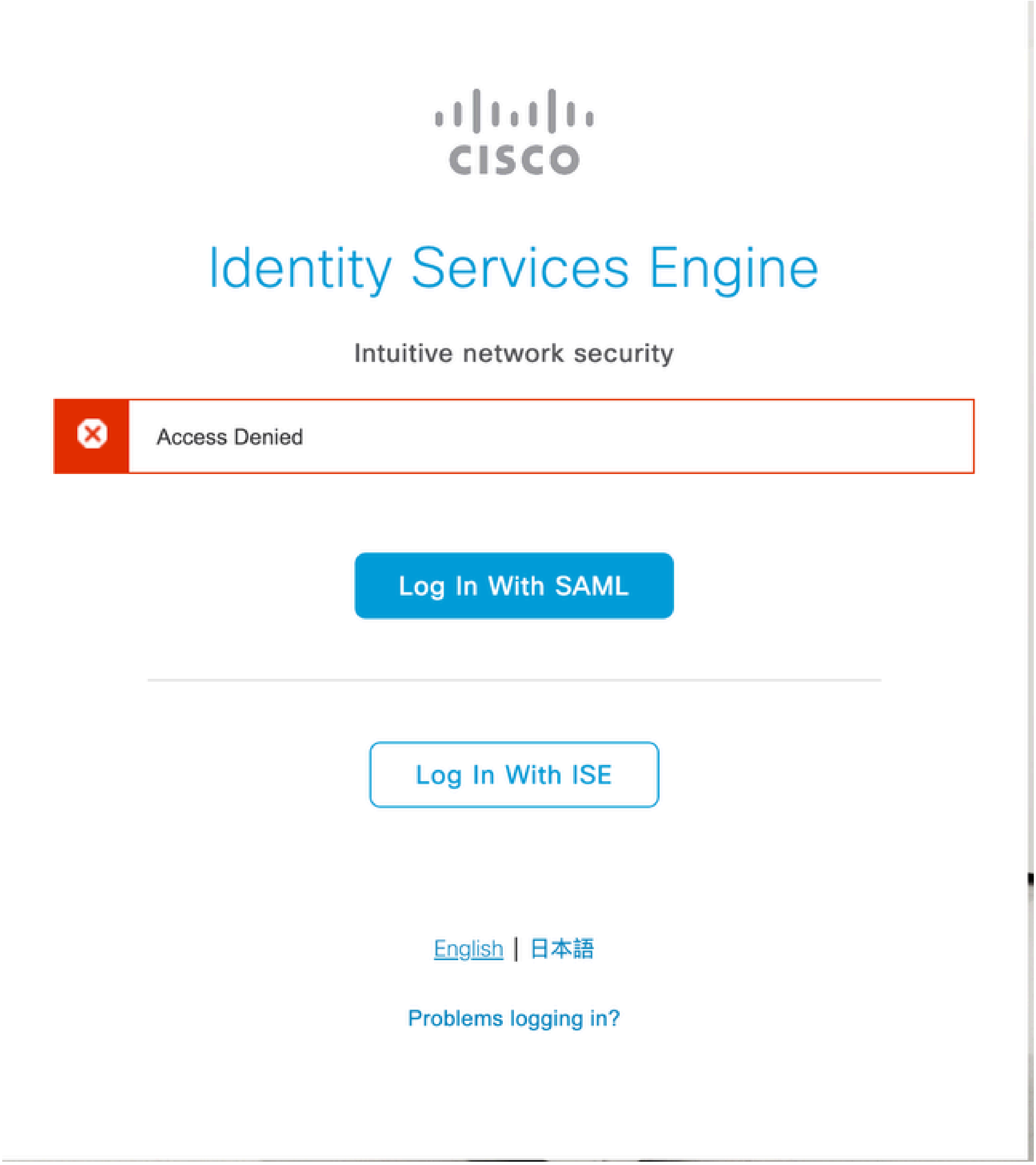
What does the error look like?

```
Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation Id: 5aa879f5-68f1-482a-a405-ff993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXX:
```

Get resolution guidance

Issue 4. ISE displays "Access Denied" error after a login attempt. This error occurs when the claim name of the group created earlier in the Azure Enterprise Application does not match in ISE.

To fix this: ensure the group claim name in Azure andISE under the SAML Identity Provider Groups tab are the same. Refer to steps 2.7. and 4. under the **Configure SAML SSO with Azure AD** section of this document for more details.



Access Denied

Troubleshoot ISE

Log Level of the components here must be changed on **ISE.** Navigate to **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration.**

Component Name	**Log Level**	**Log Filename**
portal	DEBUG	guest.log

opensaml	DEBUG	ise-psc.log
saml	DEBUG	ise-psc.log

Logs with SAML Login and Mismatched Group Claim Names

Set of debugs displaying claim name mismatch troubleshooting scenario at the time of flow execution (ise-psc.log).

Note: Keep an eye out for items in **Bold**. Logs have been shortened down for clarity purposes.

1. User is redirected to IdP URL from ISE Admin Page.

<#root>

```
2021-07-29 13:48:20,709 INFO   [admin-http-pool46][] api.services.persistance.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.SAM
2021-07-29 13:48:20,839 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM

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

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

2. SAML response is received from the browser.

<#root>

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

-::::- Decoded SAML relay state of: _0049a2fd-7047-4d1d-8907-5a05a94ff5fd_DELIMITERportalId_EQUALS0049a

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

-::::- Decoded SAML message
```

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

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

3. Attribute (assertion) parsing is started.

<#root>

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

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


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


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


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


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

[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.SA
```

4. Group attribute is received with the value of **576c60ec-c0b6-4044-a8ec-d395b1475d6e**, signing validation.

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

```
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
        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-89
        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.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
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.validat
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.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,358 INFO   [admin-http-pool50][] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImp
```

5. RBAC authorization validation.

<#root>

```
************************Rbac Log Summary for user samlUser************************
2021-07-29 13:48:27,360 INFO   [admin-http-pool50][] com.cisco.ise.util.RBACUtil -::::- Populating cach

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 -:::
```