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

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Terms
- SAML
- SAML Assertion

High-level Flow Diagram

Configure SAML SSO Integration with Azure AD

- Step 1. Configure SAML Identity Provider on ISE
- Step 2. Configure Azure AD IdP Settings
- Step 3. Upload MetaData from Azure Active Directory to ISE
- Step 4. Configure SAML Groups on ISE
- (Optional) Step 5. Configure RBAC Policies

Verify

Troubleshoot

- Common Issues
- Troubleshoot ISE
  - Logs with SAML Login and Mismatched Group Claim Names

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.

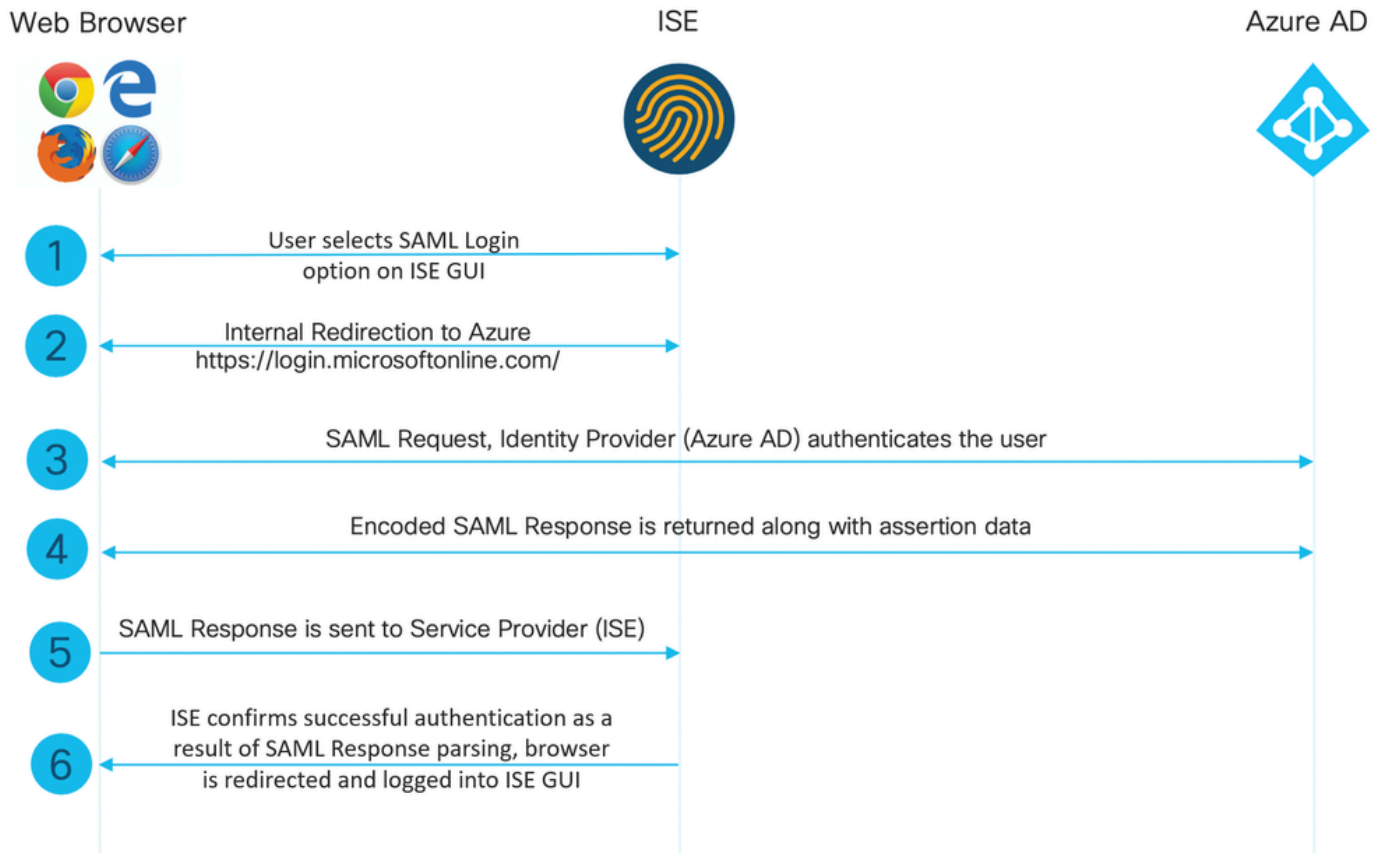
- Authentication assertions prove the identification of the user and provide the time the user logged in and what method of authentication they used (Kerberos, two-factor, as examples)
- The attribution assertion passes the SAML attributes, specific pieces of data that provide information about the user, 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 are as shown in the image:



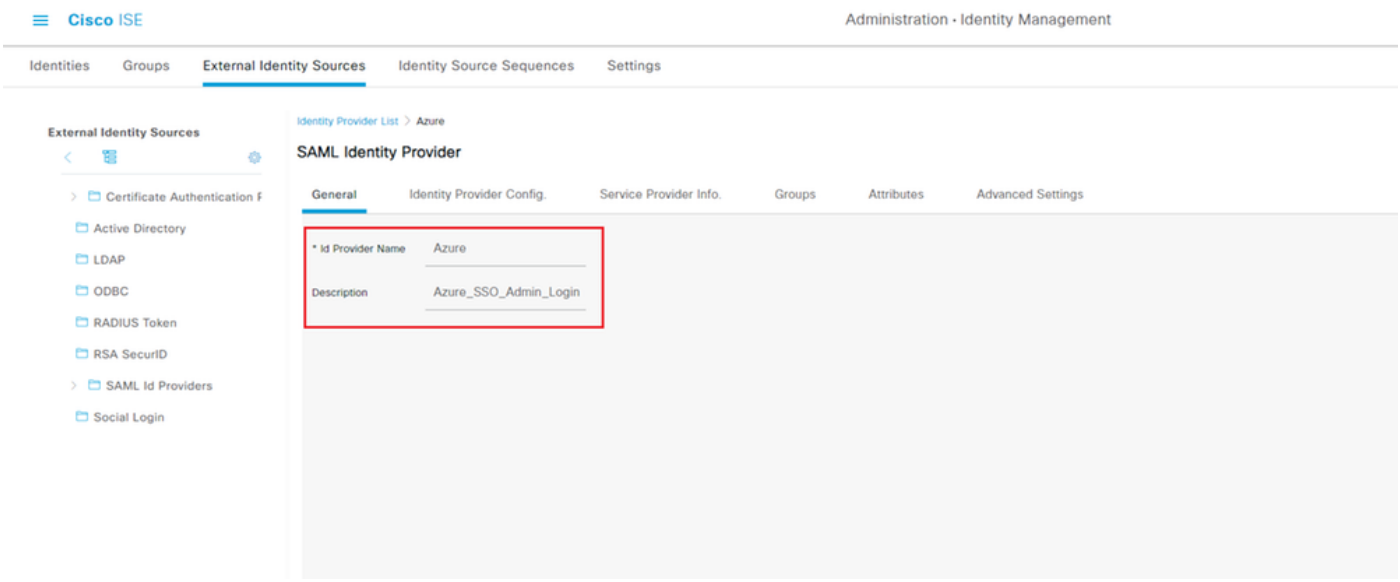
Configure SAML SSO Integration with Azure AD

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.

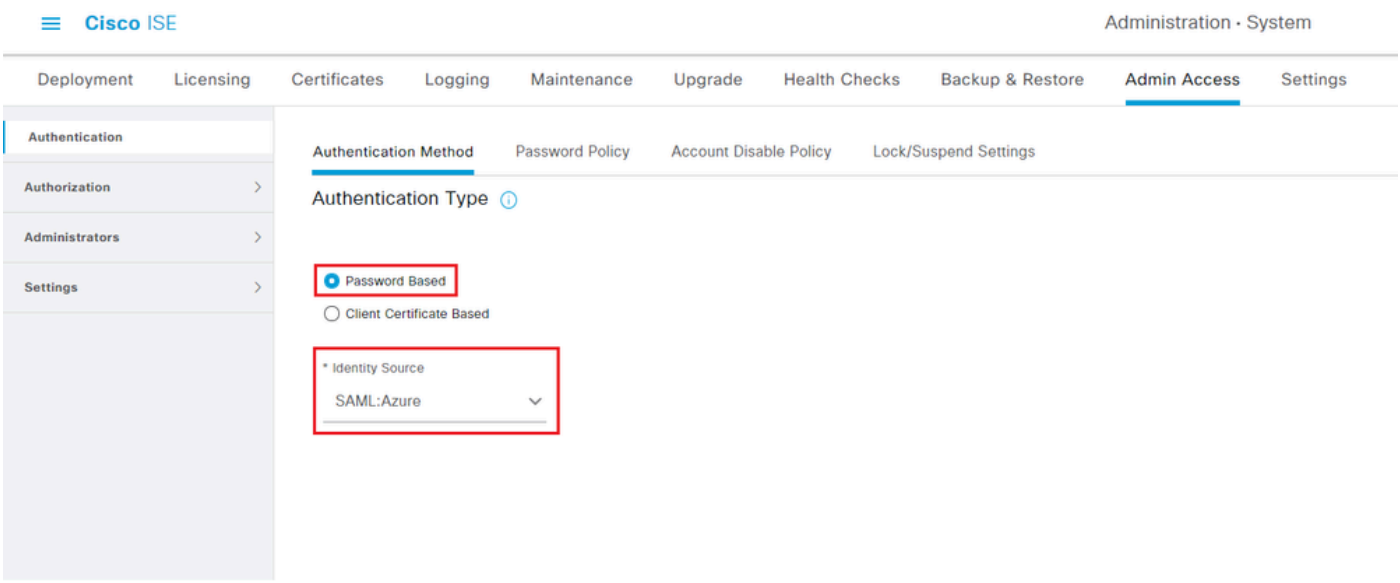
Enter the **Id Provider Name** and click **Submit** in order to save it. The **Id Provider Name** is significant only for ISE as shown in the image.



2. Configure ISE authentication method:

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

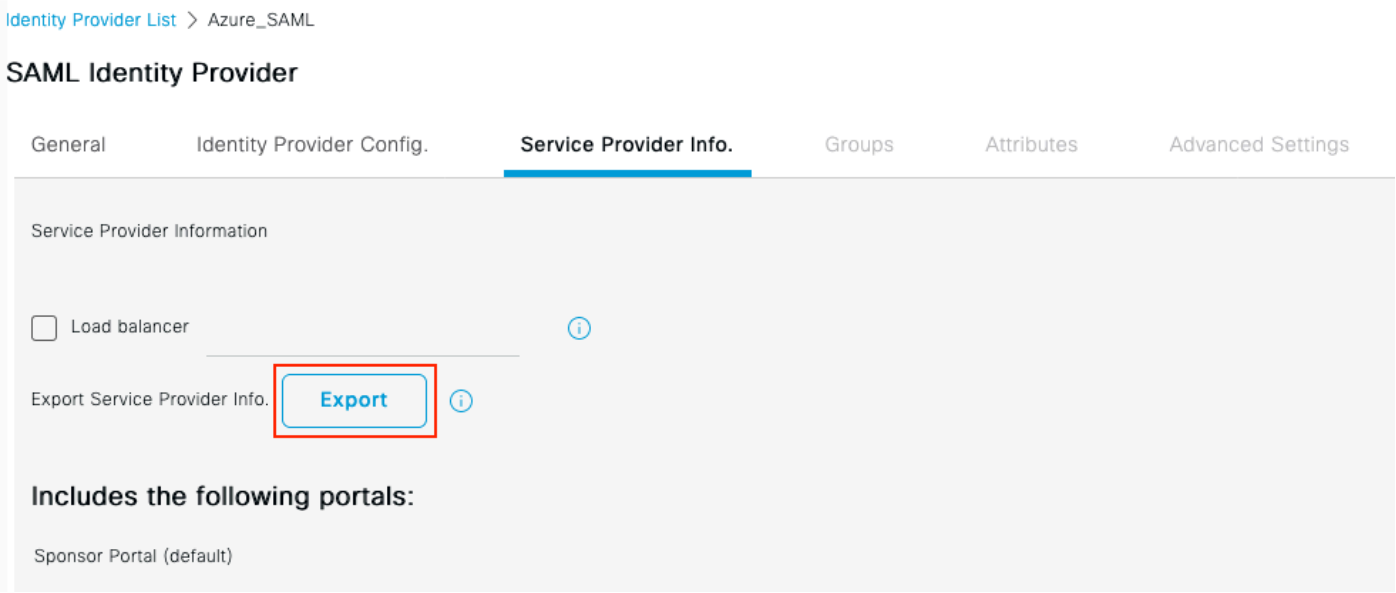
Select the required Id Provider Name created earlier from the **Identity Source** drop-down list as shown in the image.



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.



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+SOuP3j037yCOXnHAzADupfqcgwcplJQnFxhVfnDdOixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohGOt1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYdlDtE1LMEcGg1mCd56GfrDcJdXOcZJmiDzizyjGKDdPf+1VM5JHCo6UNLFlIFyPmGvcCXnt
NVqsYvxSzF038ciQqlm0sqrVrrYZuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFFlMzybvm1FYu
9h83gL4WJWMizETO6Vs/DOp6BSf2MPxKe79OR5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5ROgT7v3CDrdFtRoNYAT+YvO941KzFCSEOsshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNzlFuggaE8tC7uyuQZa2rcmTrXGWCl
sDU4uOvFpFvrcC/lavr9Fnx7LPwXaOasvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWIy+ctbBTO+EMO6Xj1aTI1bV8OmN/6LhiS8g7KpFz4RN+ag1iu6pgZ5O58Zot9gqkpFw
kVS9vT4EOzwNGo7pQI8CAwEAAaN9MHswIAYDVR0RBBkwF4IVaXNlMy0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgLsMB0GA1UdDgQWBBRIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GWlvcgreC7R46qenaonXVrltRw11vVIdCf8JQFFMxya/rIC4mxVeooOj1Fl9d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4HOvdm6oF3uBteO/pdUtEi6fObqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gfHObE5luT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmDh9g2mppbBwOcxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cfAZuiV/e3wkOBLZM
lgV8FTVQSnra9LwHP/PgeNAPUcRPXSwaKE4rvjvMc0aS/iYdwZhZiJ8zBdIBanMv5mGu1nvTEt9K
EEwj9yslIHmdqoH3EmOFOgnzRORvsMPbJxAoTFjfoITTMdQXNHhg+wlPOKXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKwER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8EOv7bUMSDmmg/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.act
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLogin

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

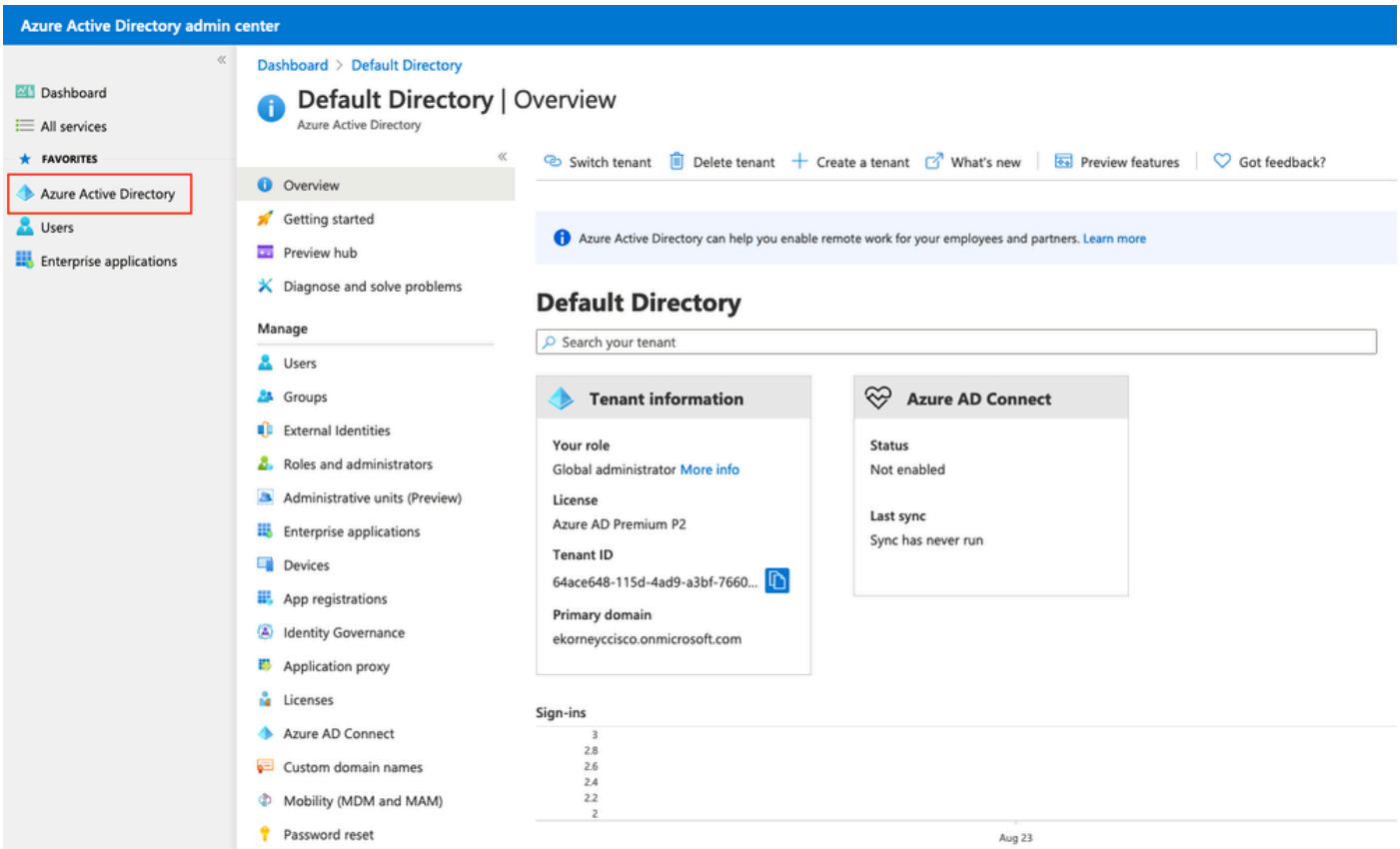
Attributes of interest from the XML file:

- **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"

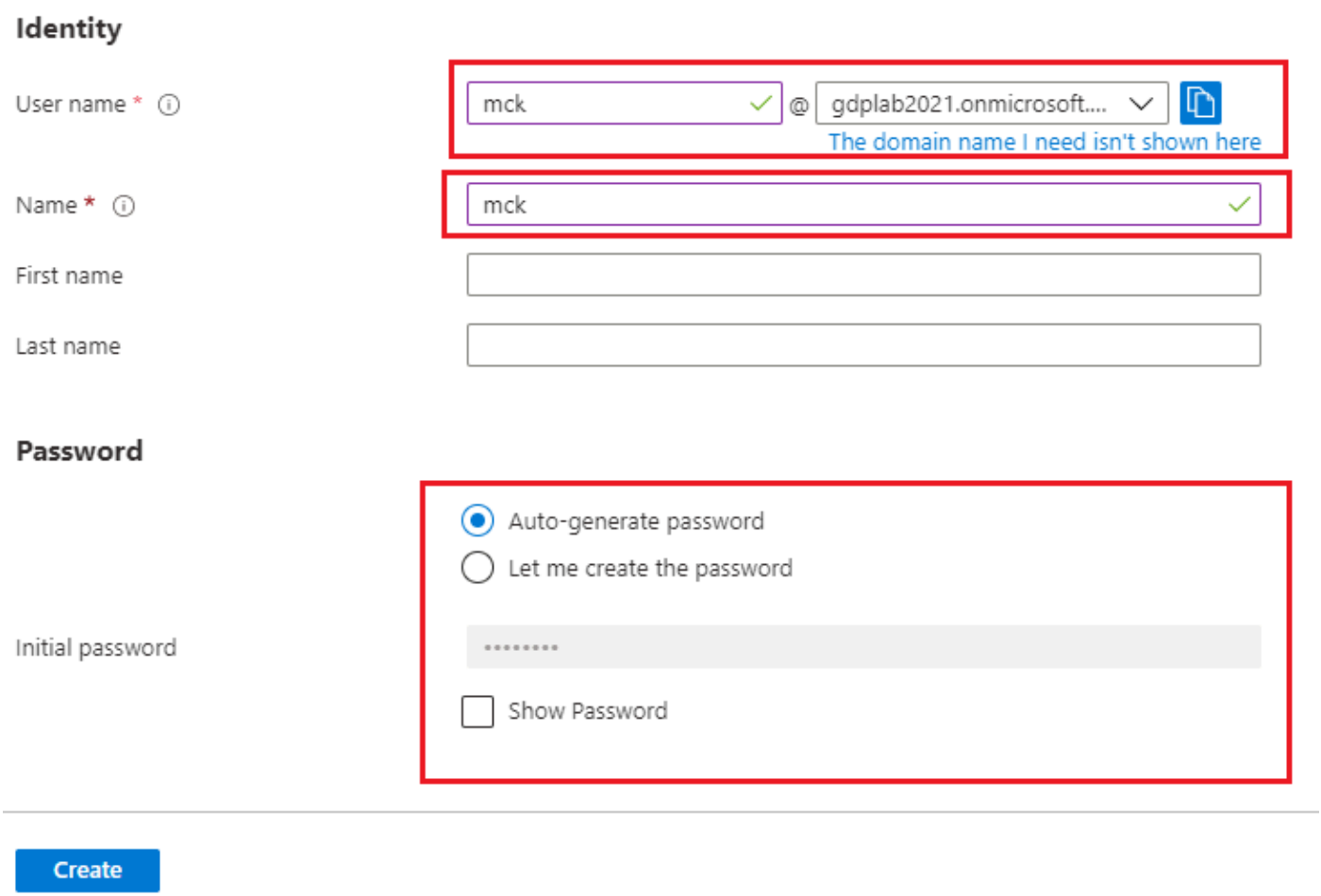
Step 2. Configure Azure AD IdP Settings

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.

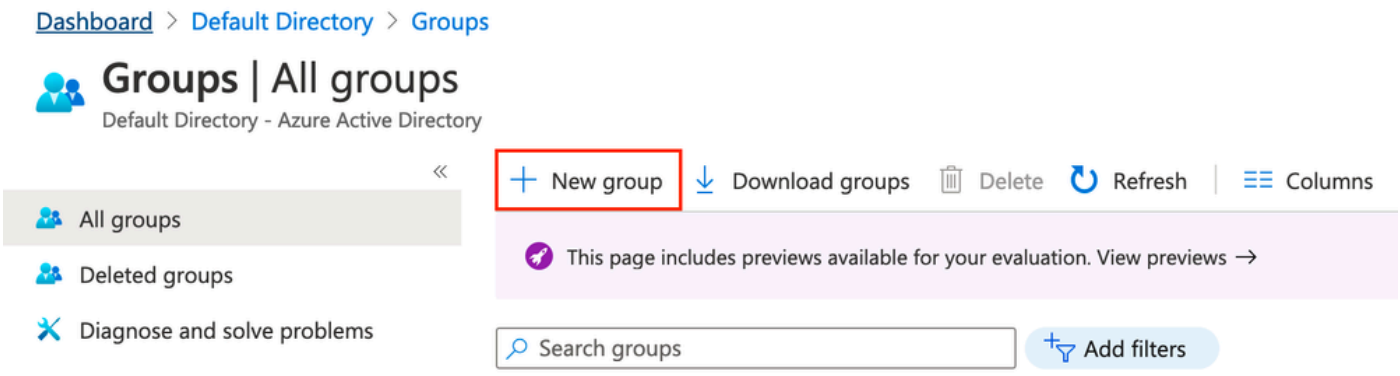


Select **Users**, click on **New User**, configure **User name, Name** and **Initial Password** as required. Click on **Create** as shown in the image.

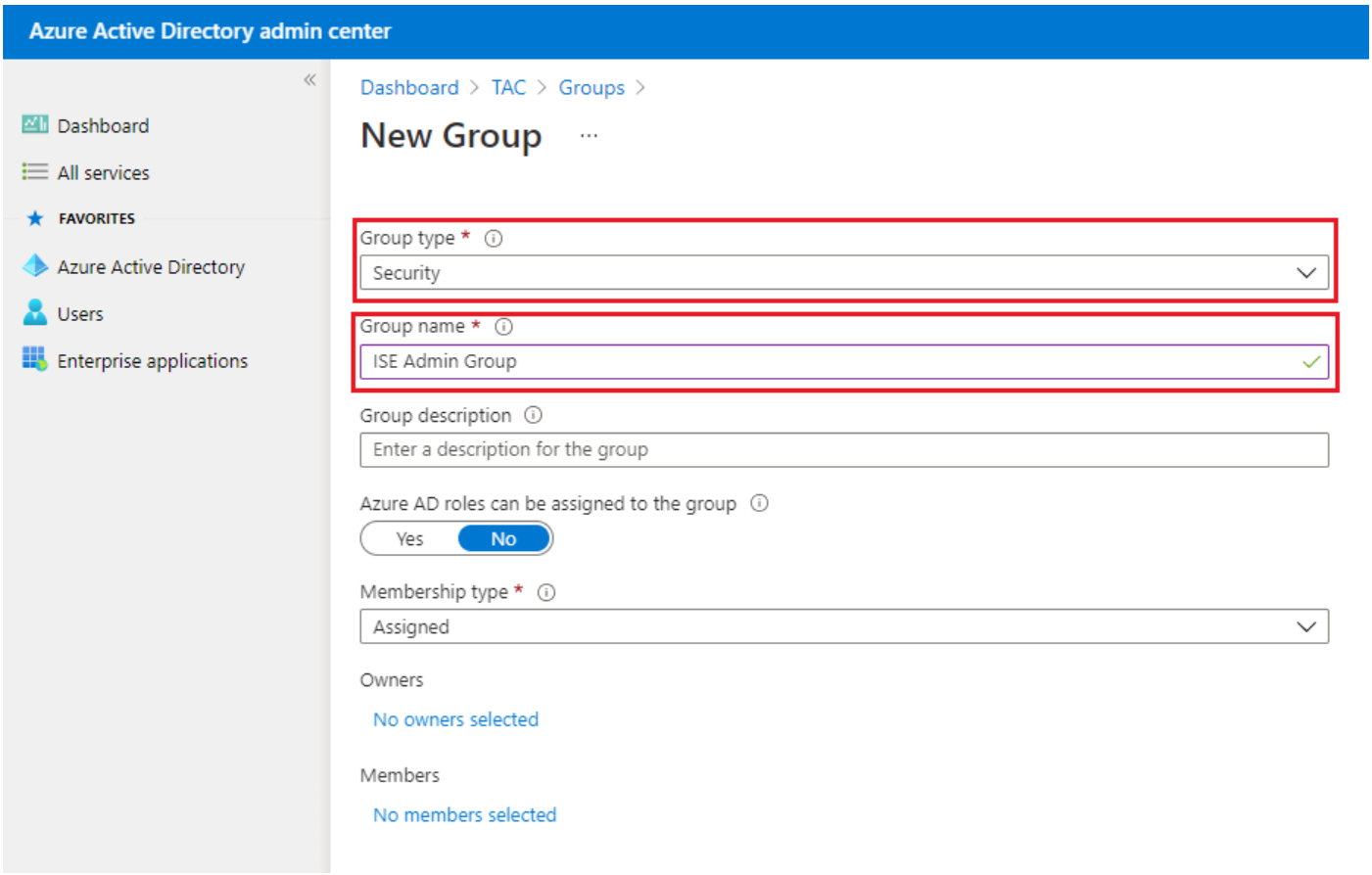


2. Create an Azure AD Group:

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

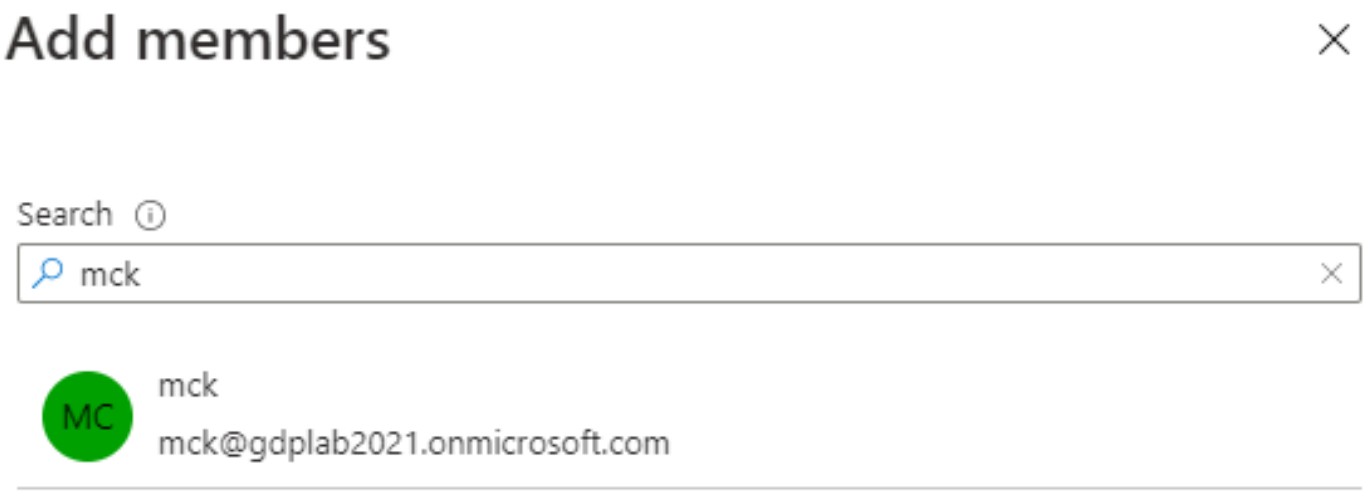


Keep Group type as **Security**. Configure the **Group name** as shown in the image.

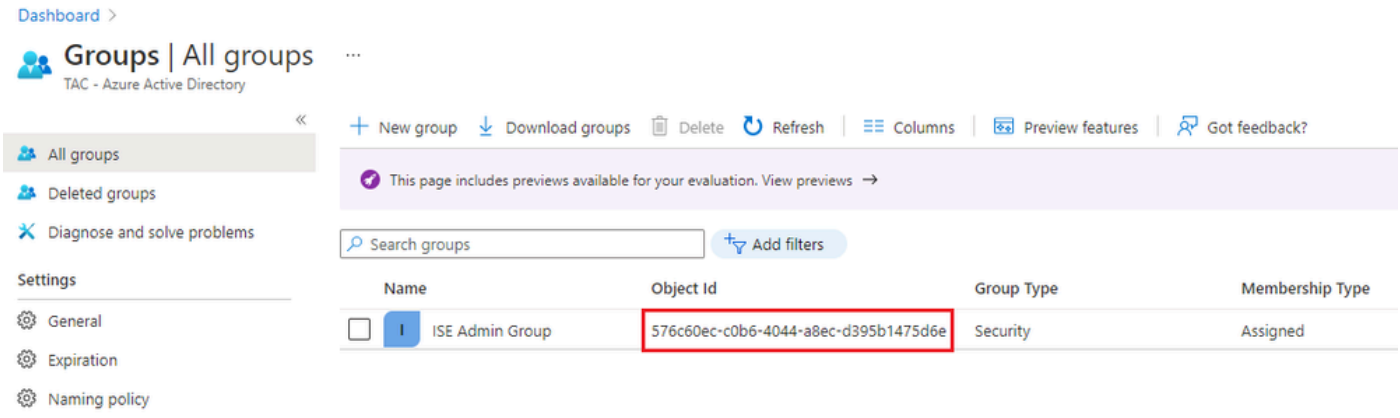


3. Assign Azure AD User to the Group:

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.

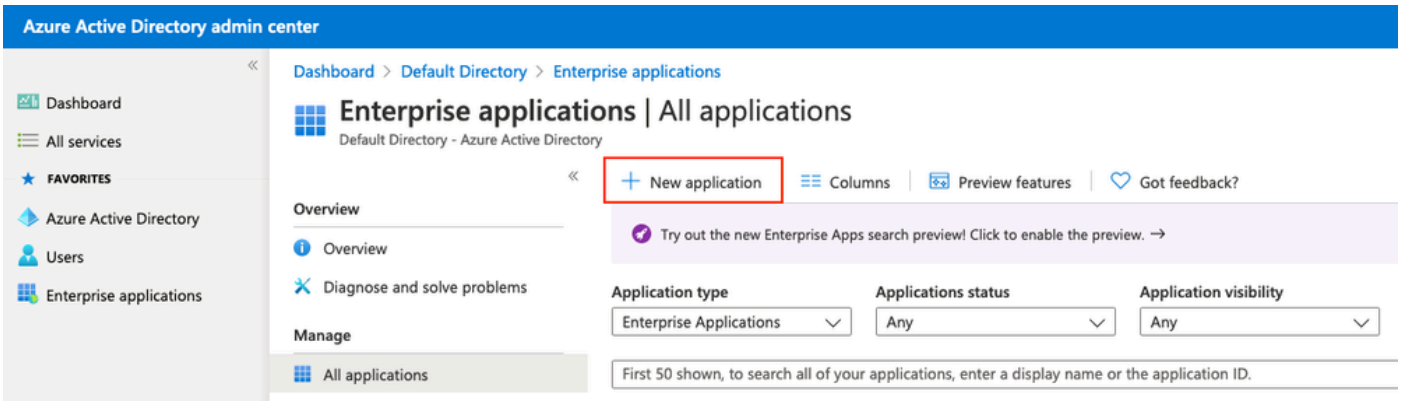


Make a note of **Group Object id**, in this screen, it is **576c60ec-c0b6-4044-a8ec-d395b1475d6e** for **ISE Admin Group** as shown in the image.

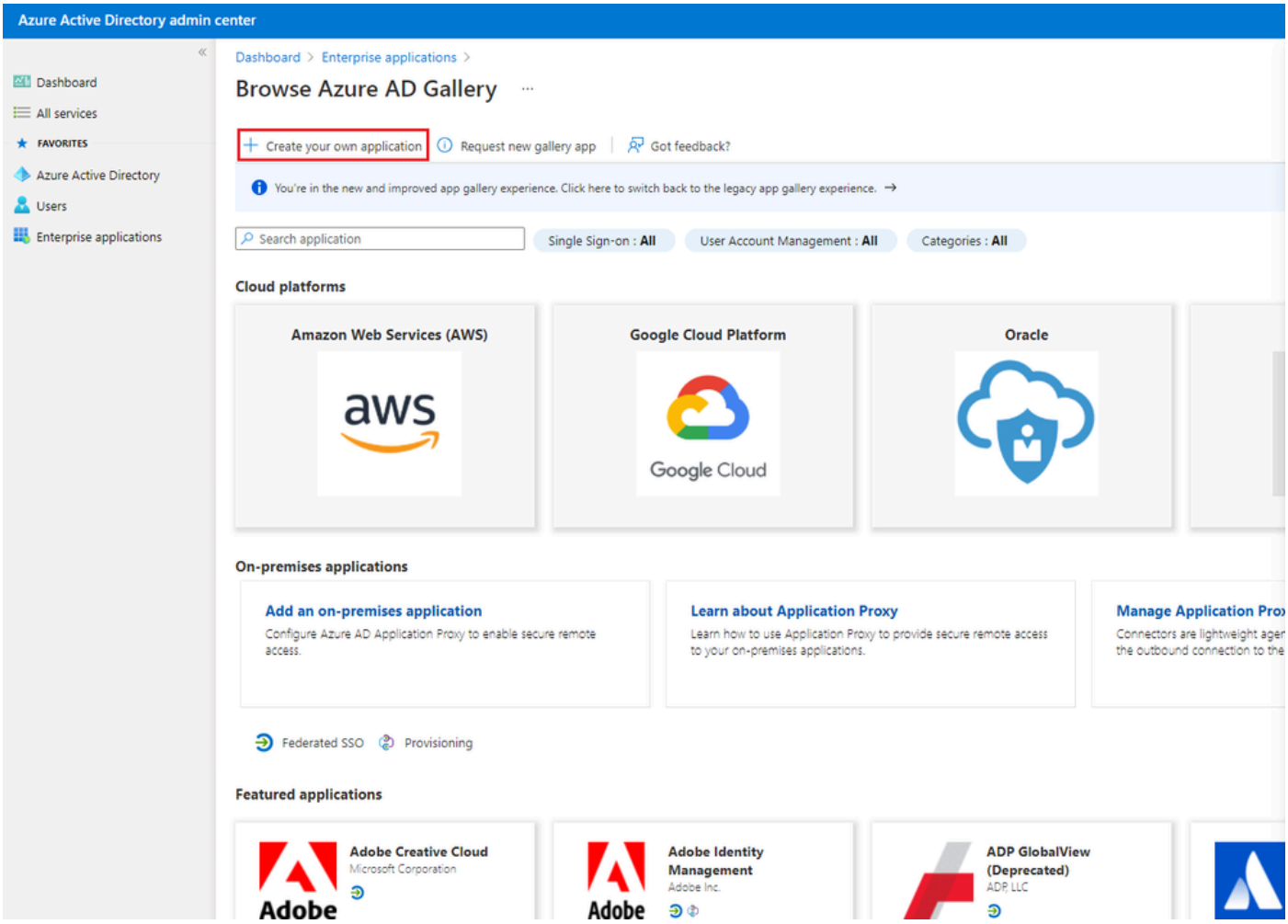


4. Create an Azure AD Enterprise application:

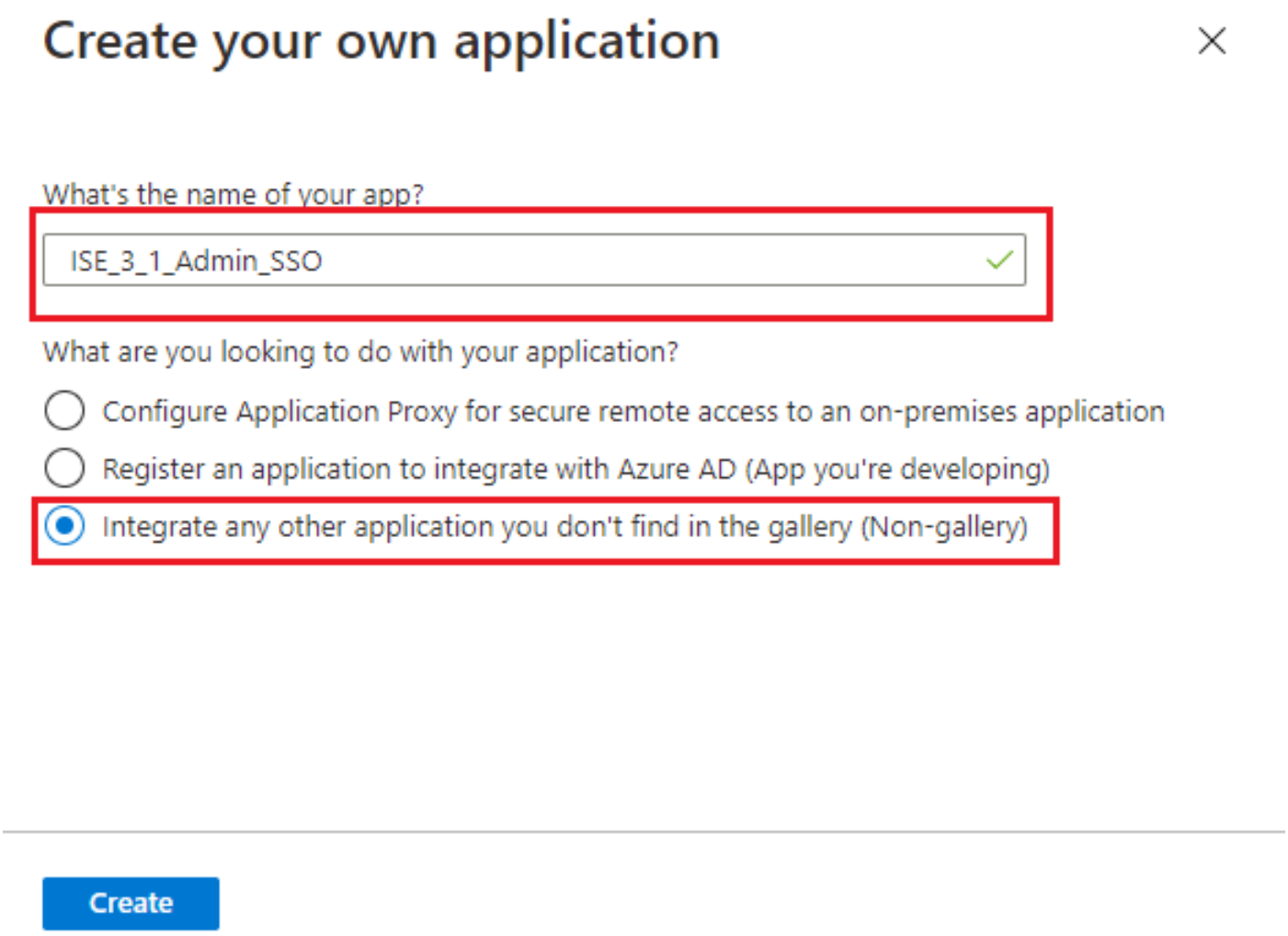
Under AD, select **Enterprise Applications** and click **New application**.



Select the **Create your own application**.

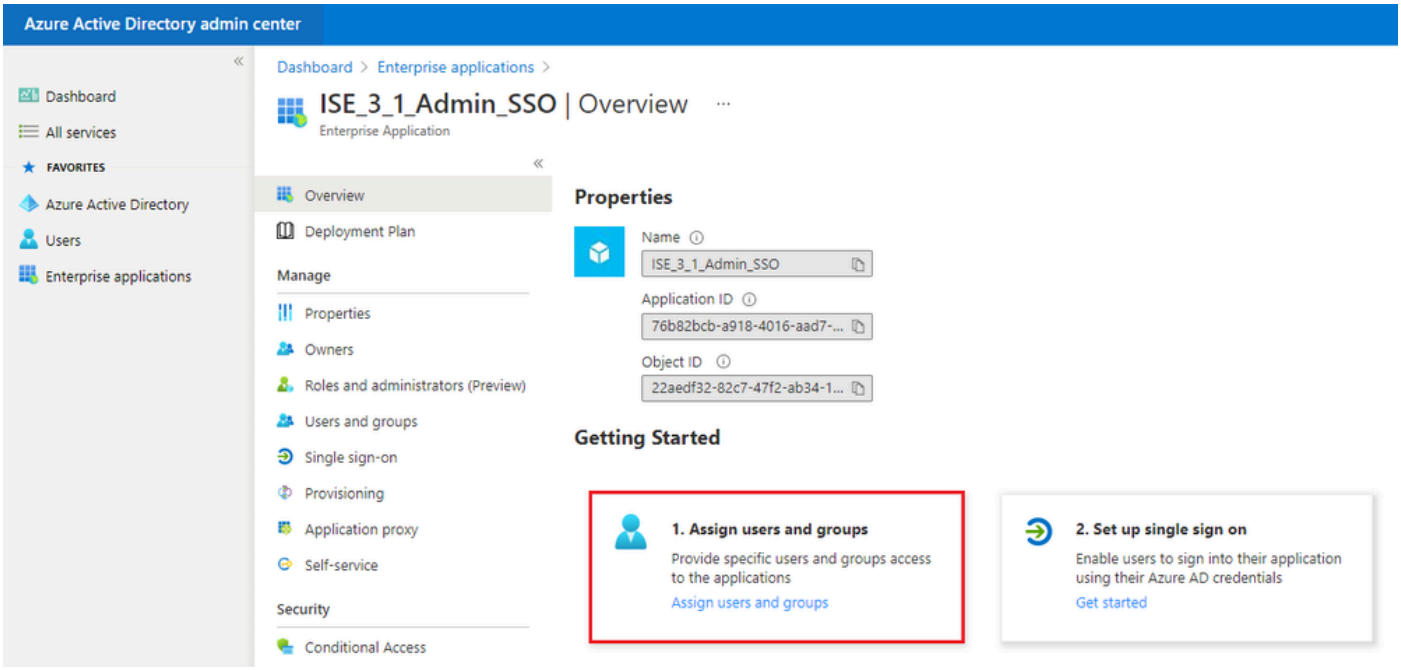


Enter the name of your application and select the **Integrate any other application you do not find in the gallery (Non-gallery)** radio button and click on the **Create** button as shown in the image**.**

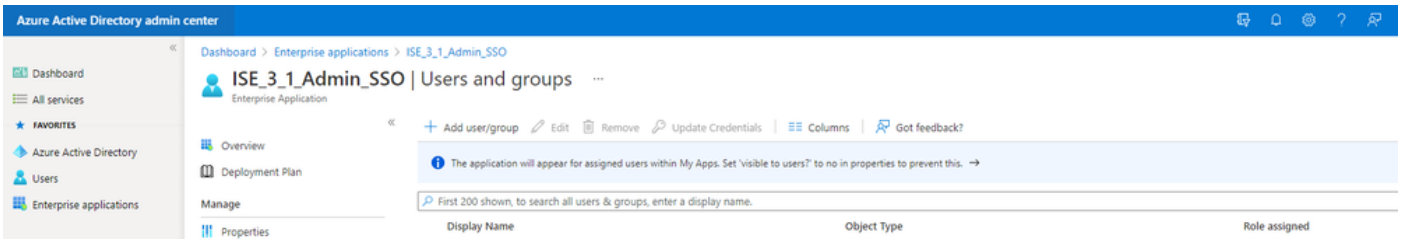


5. Add Group to the application:

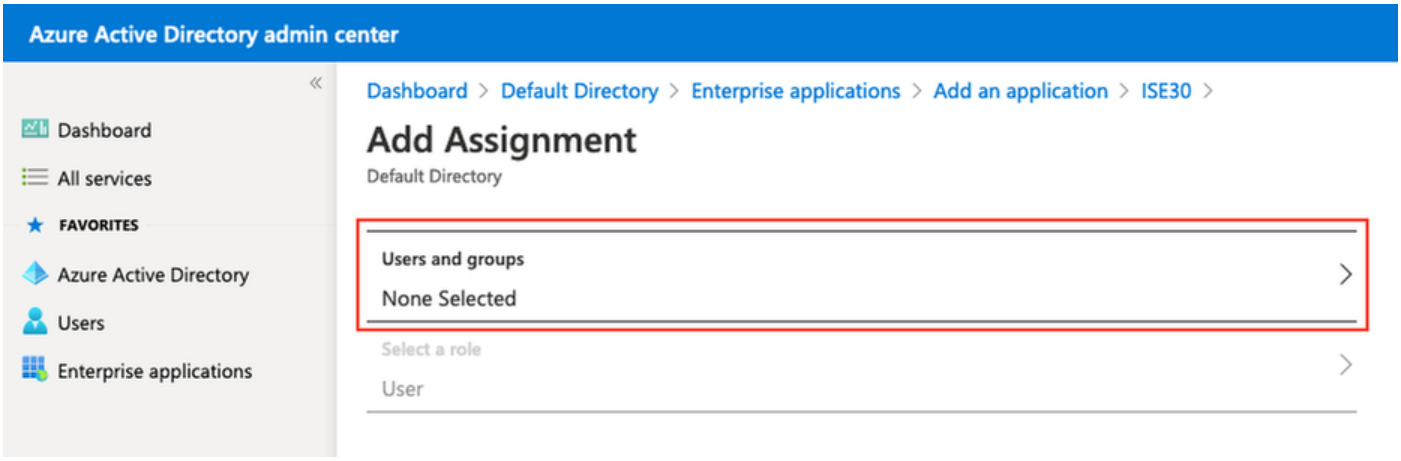
Select **Assign users and groups**.



Click **Add user/group**.



Click **Users and groups**.

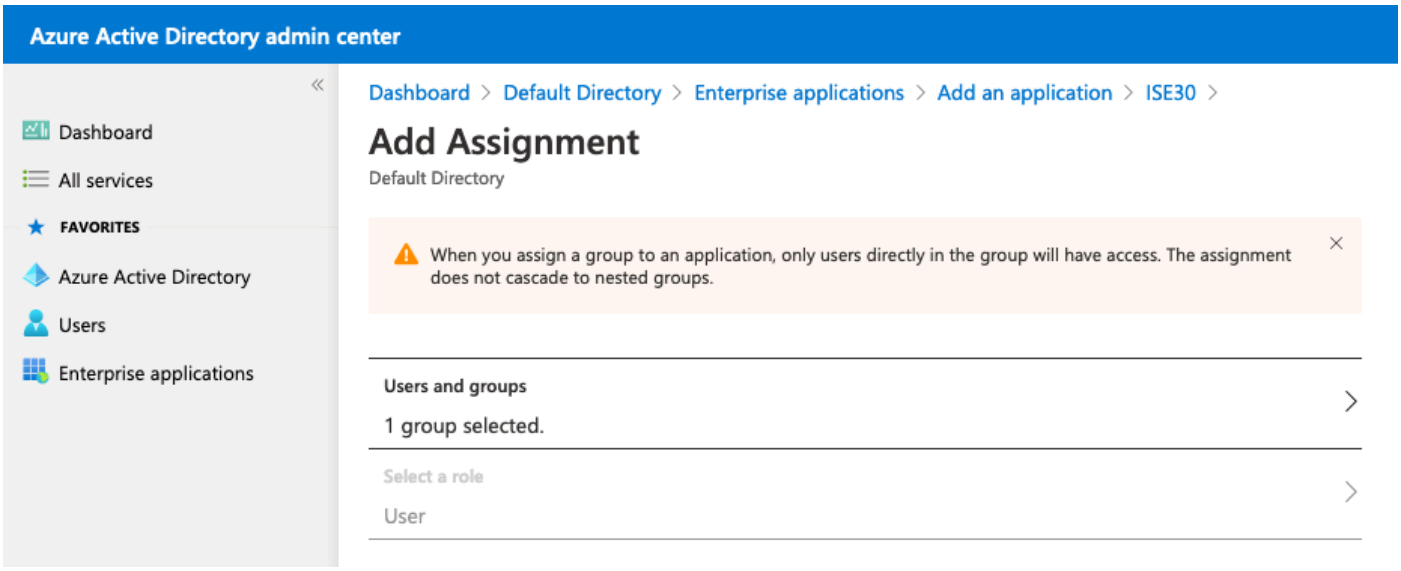


Choose the Group configured previously and click **Select.**

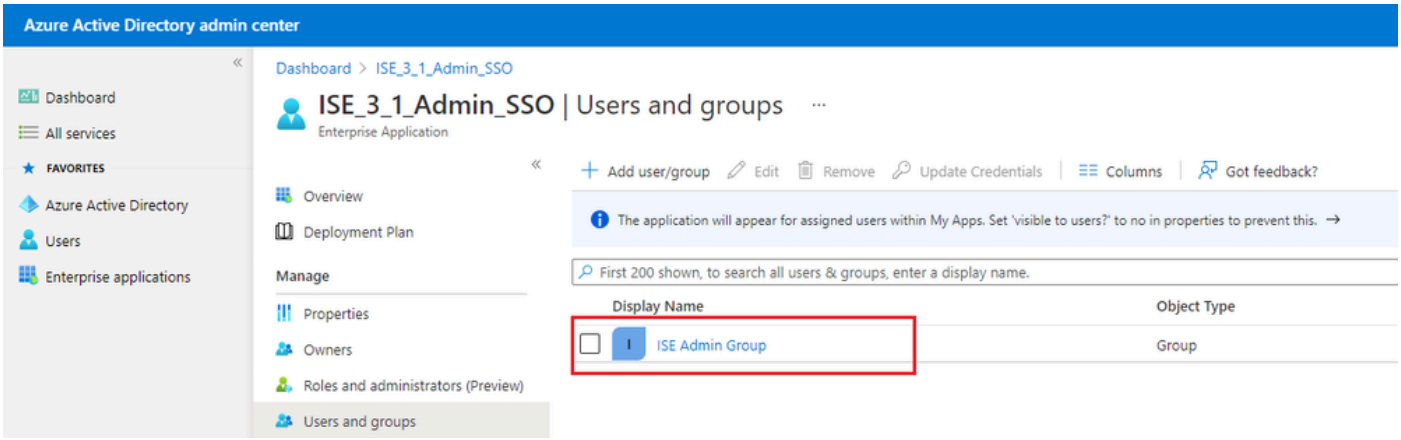
Note: Select the right set of users or groups who get access as intended as the users and groups mentioned here get access to the ISE once the setup is complete.



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

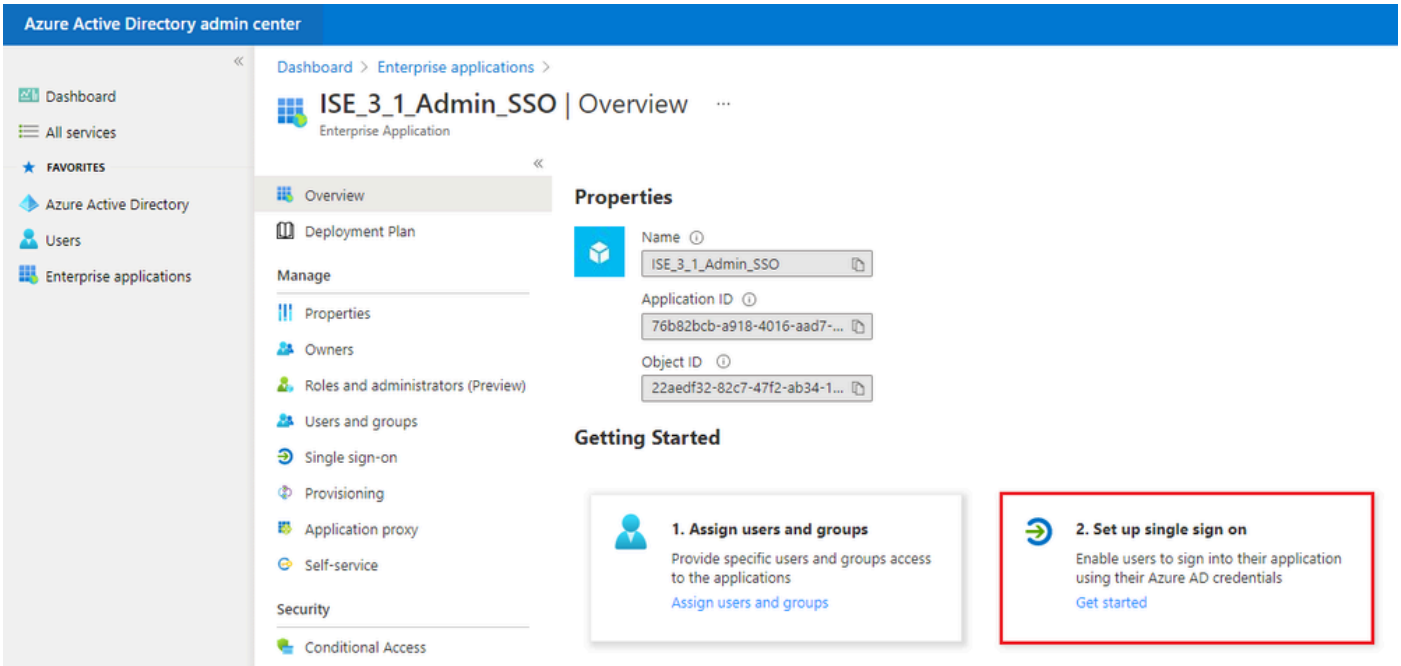


As a result, the **Users and groups** Menu for the configured application is populated with the selected Group.

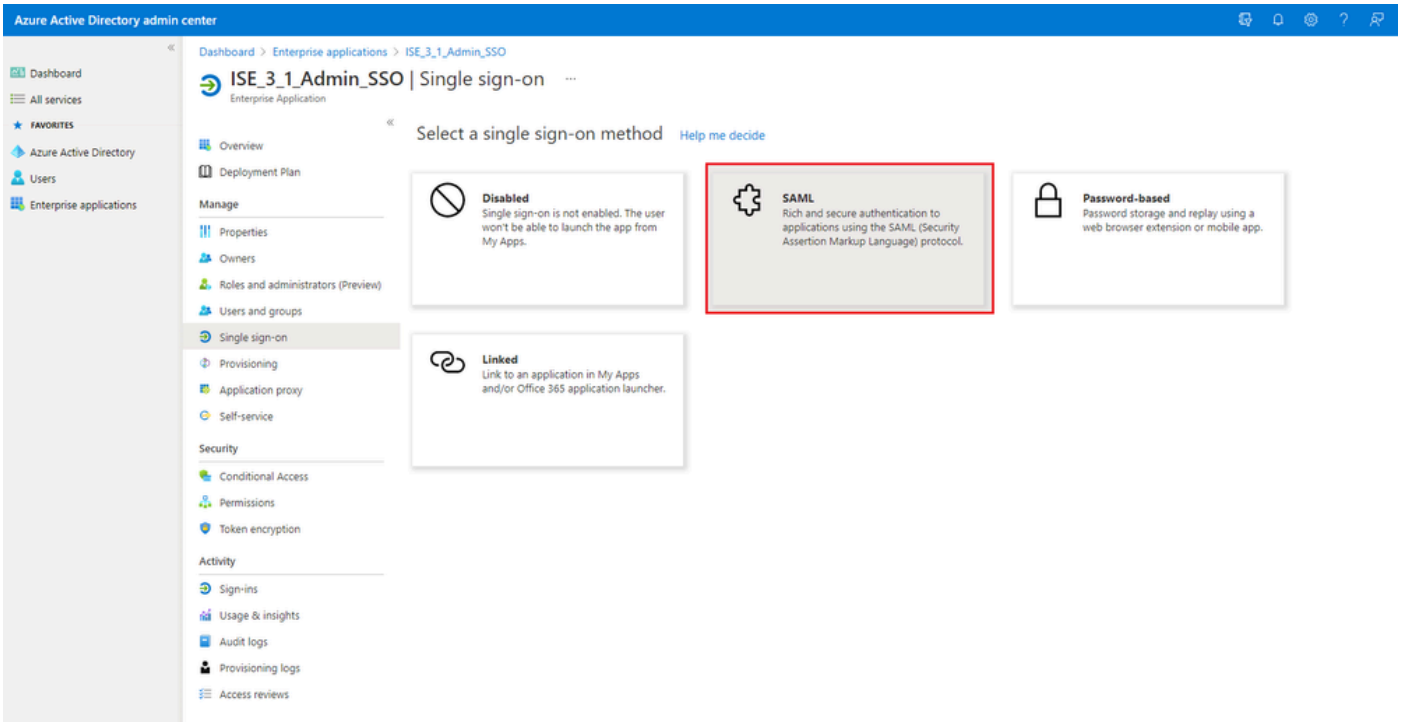


6. Configure an Azure AD Enterprise application:

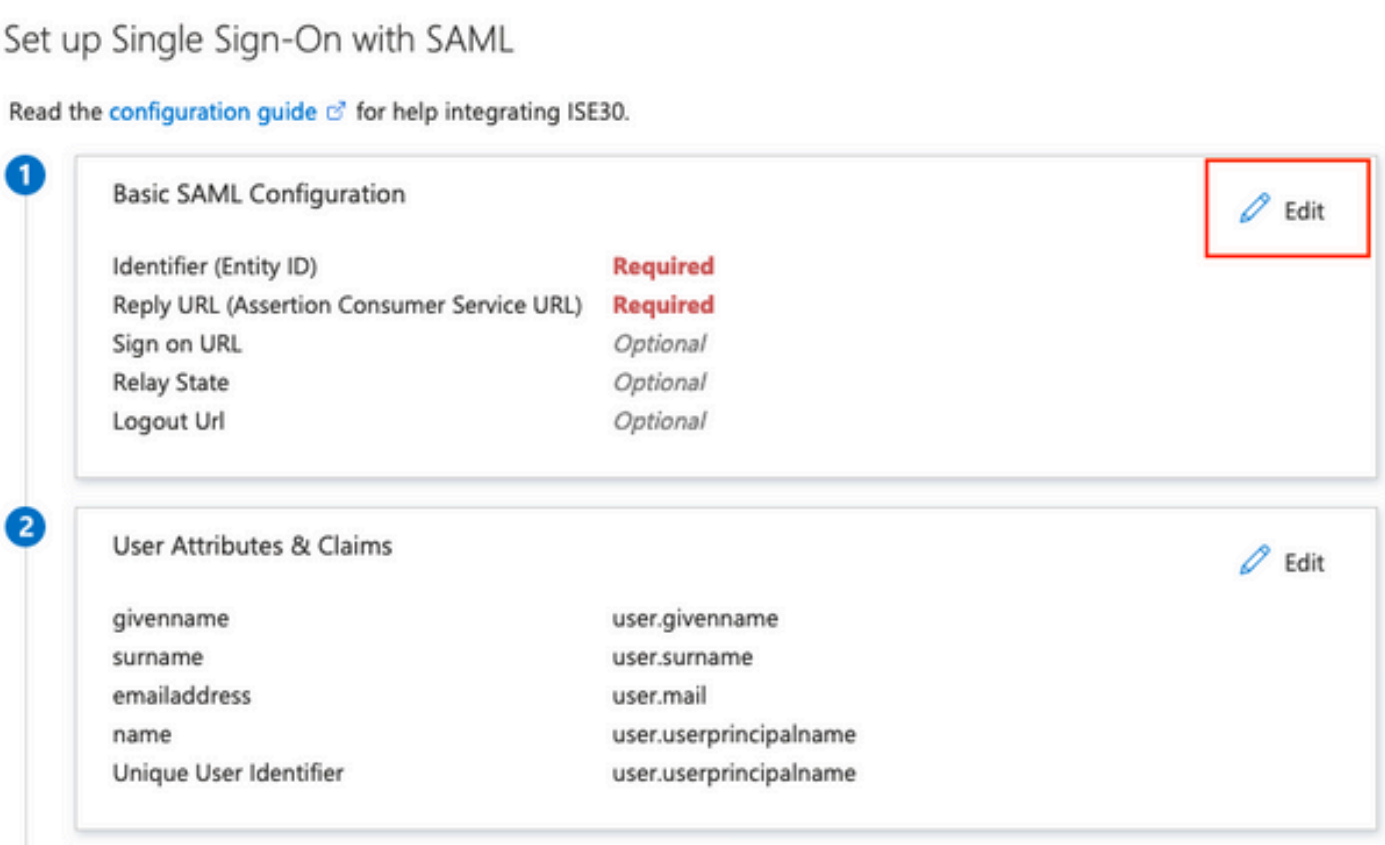
Navigate back to your Application and click **Set up single sign on**.



Select **SAML** on the next screen.

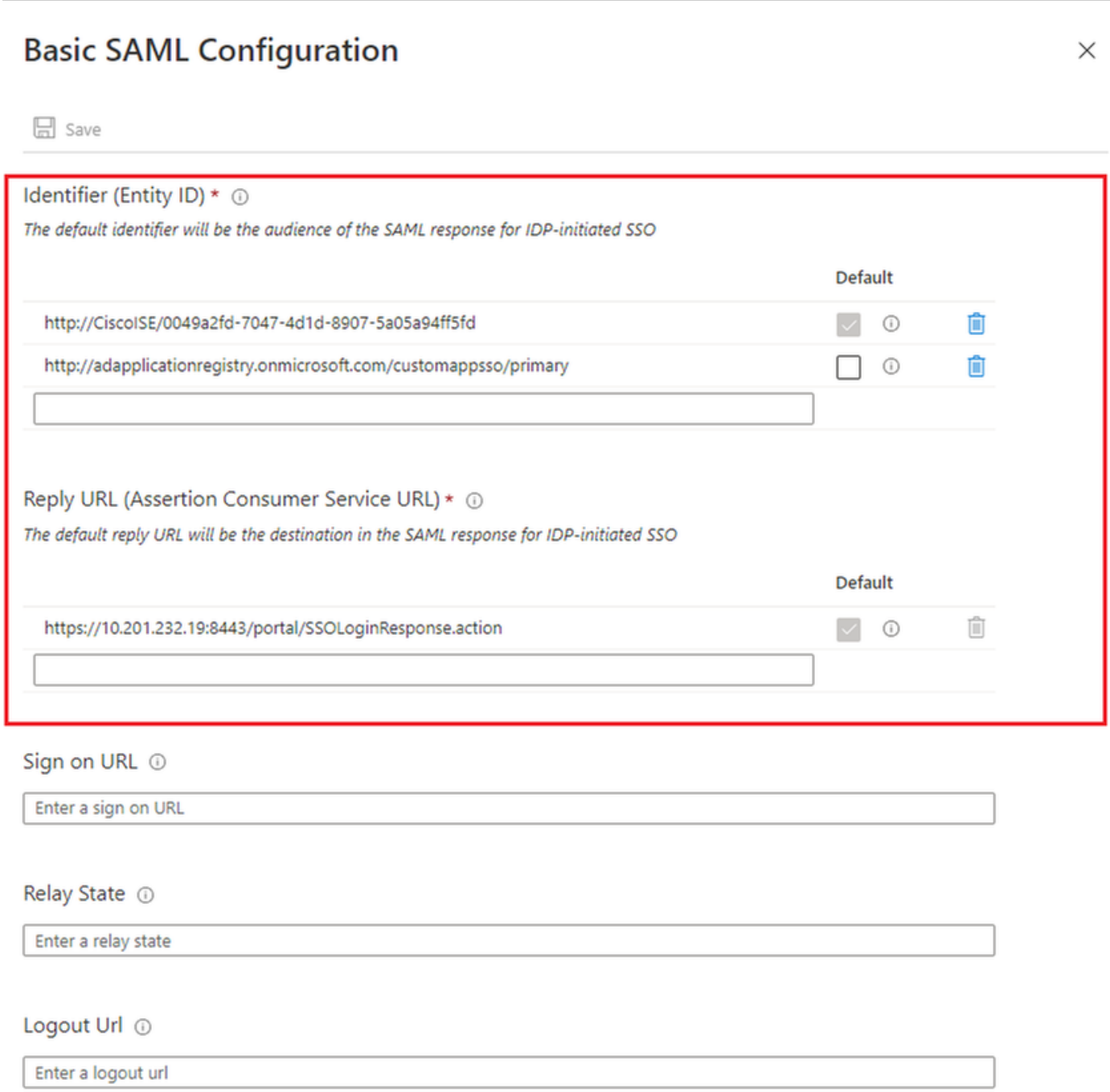


Click **Edit** next to **Basic SAML Configuration**.



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.

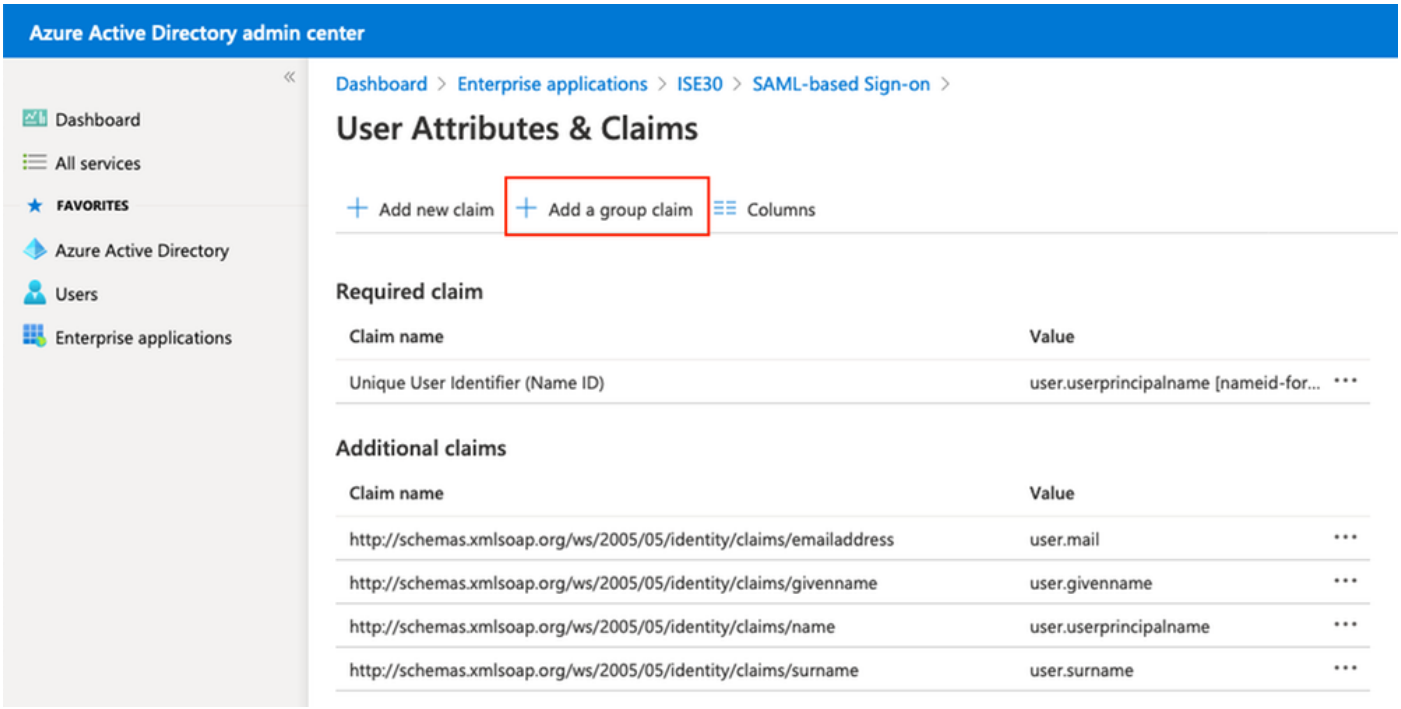


7. Configure Active Directory Group attribute:

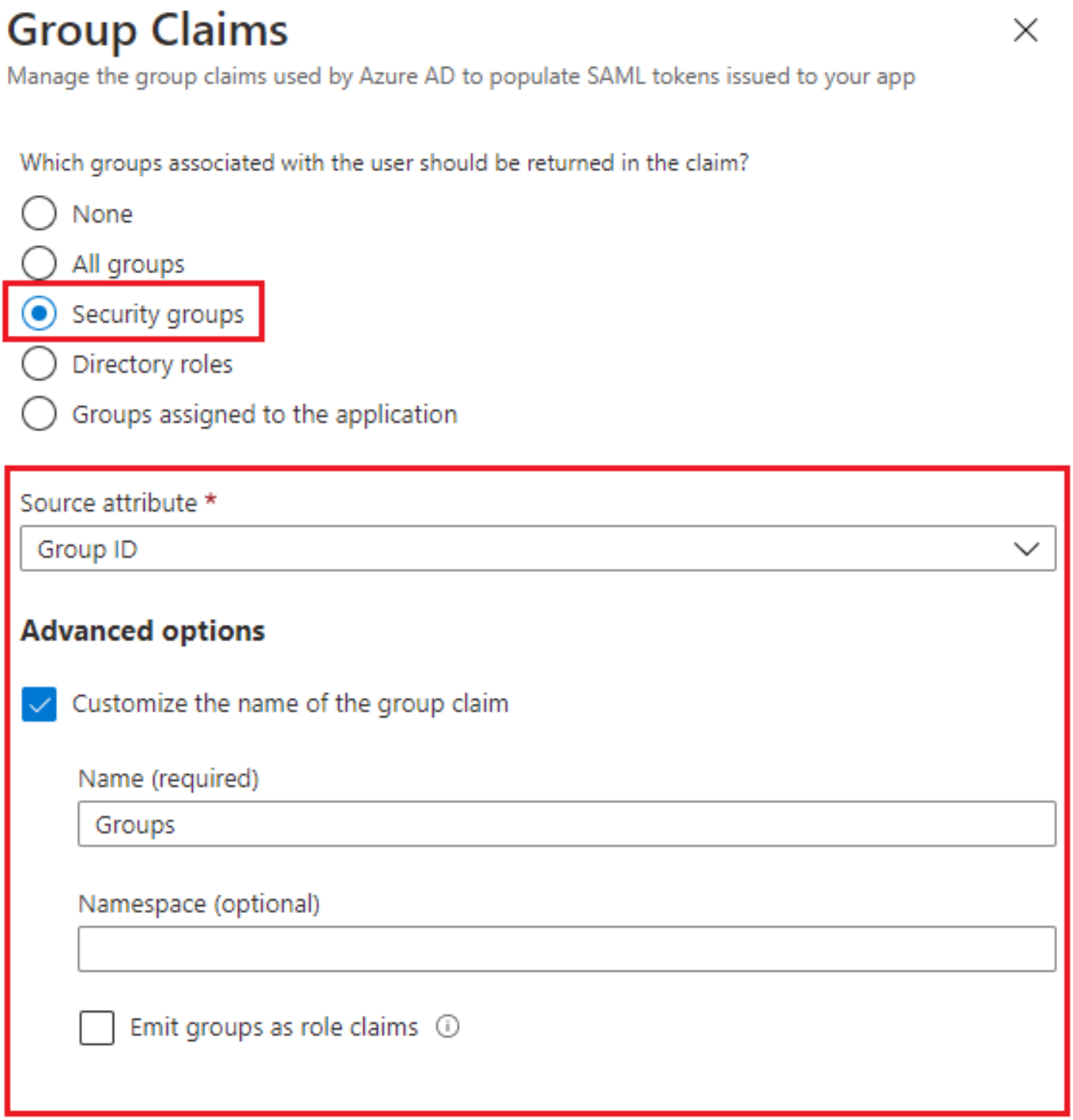
In order to return the group attribute value configured previously, click **Edit** next to the **User Attributes & Claims**.



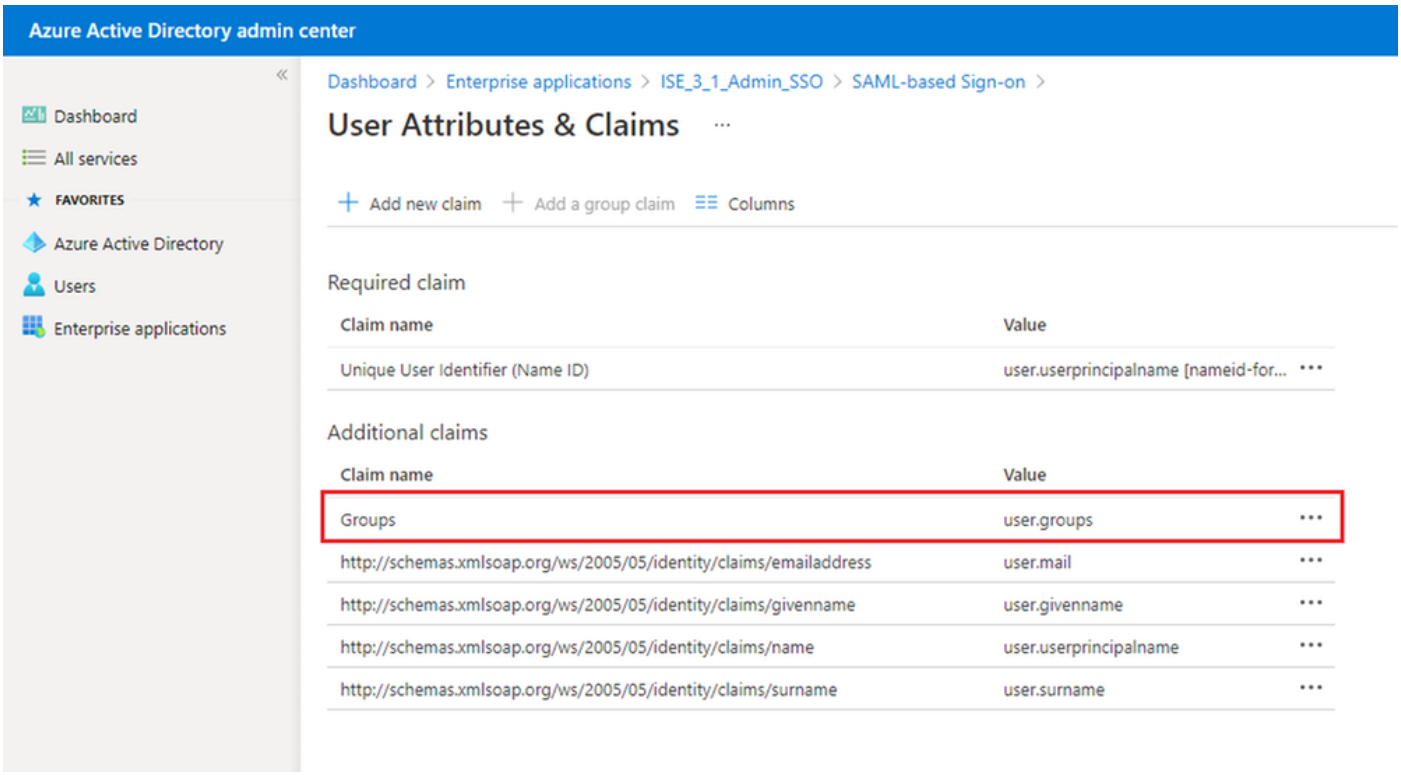
Click **Add a group claim**.



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**.

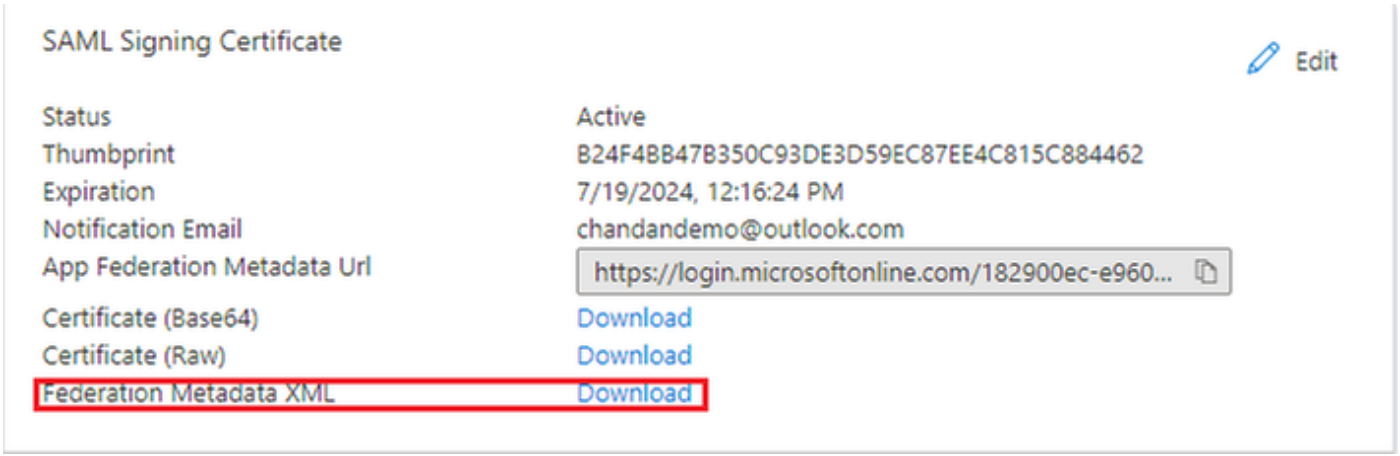


Make a note of the **Claim name** for the group. In this case, it is **Groups.**



8. Download Azure Federation Metadata XML file:

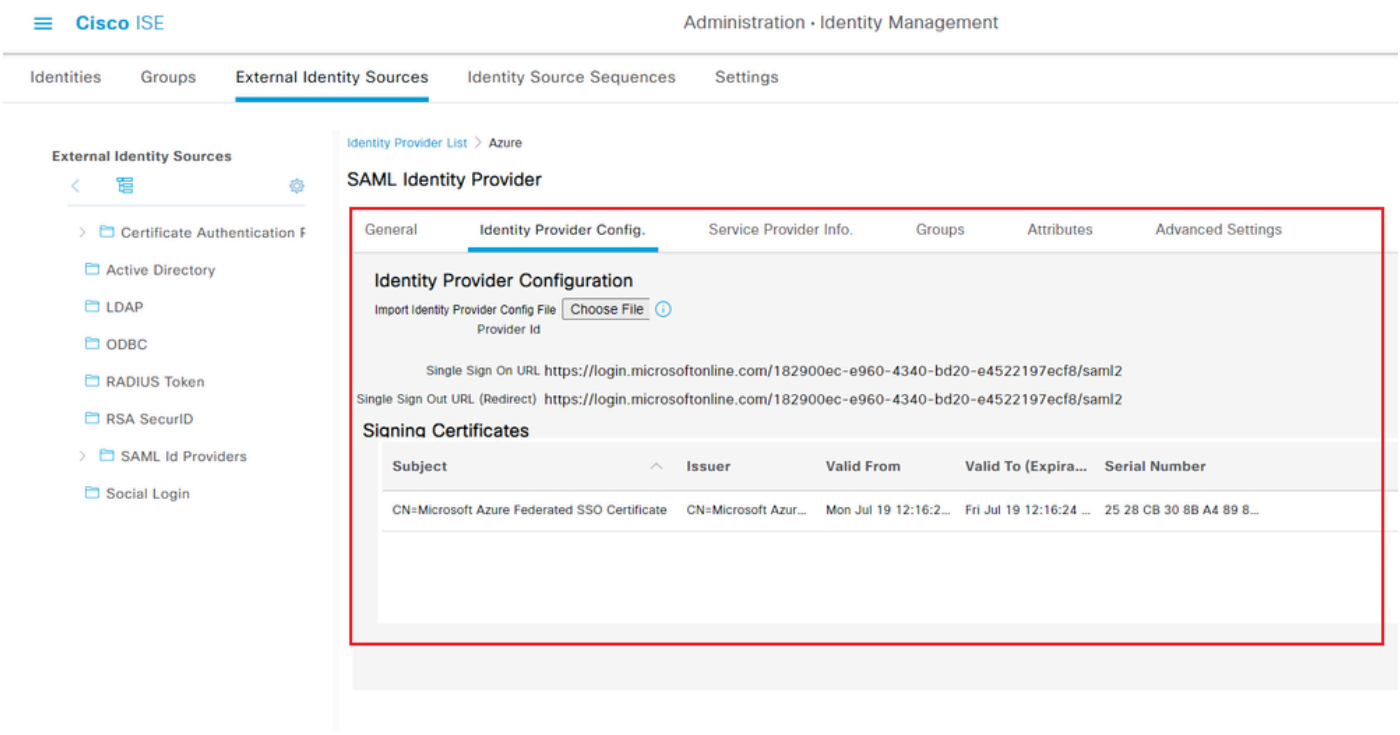
Click **Download** against **Federation Metadata XML** in **SAML Signing Certificate**.



Step 3. Upload MetaData from Azure Active Directory to ISE

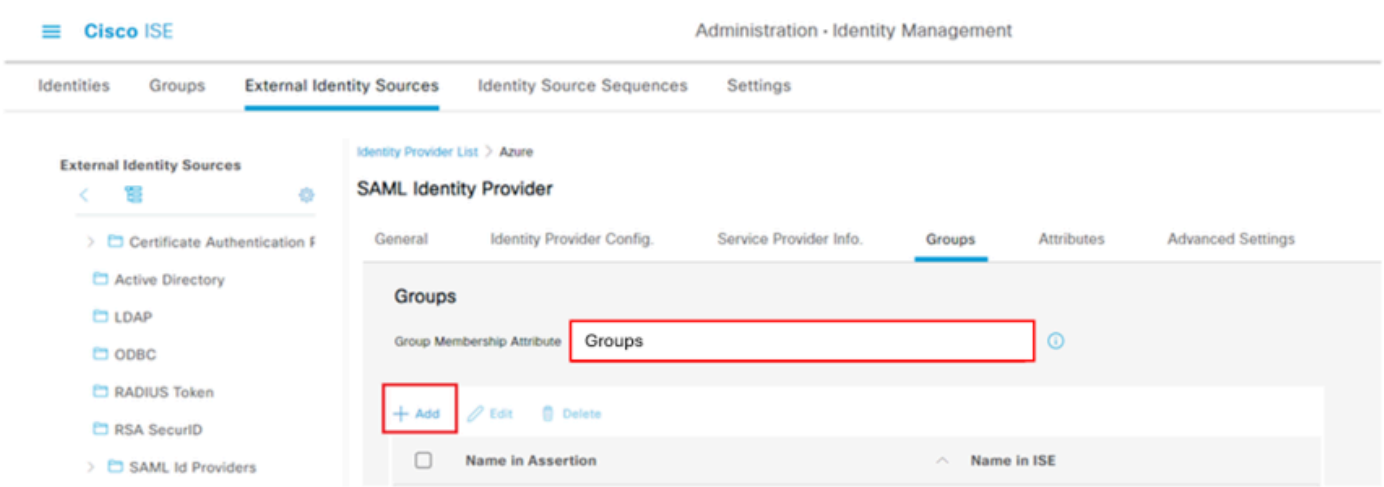
Navigate to **Administration > Identity Management > External Identity Sources > SAML Id Providers > [Your SAML Provider].**

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**.



Step 4. Configure SAML Groups on ISE

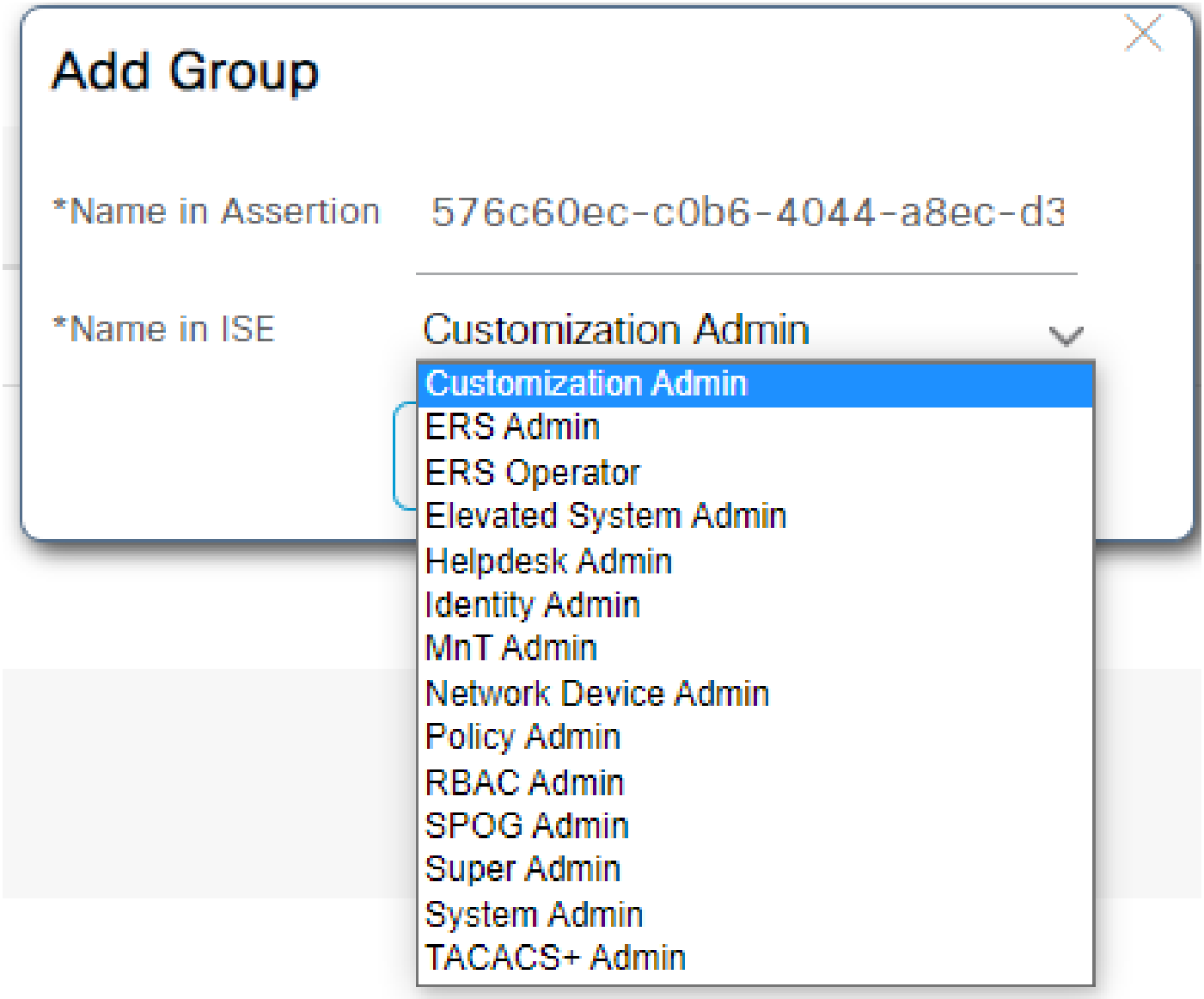
Switch to tab **Groups** and paste the value of **Claim name** from **Configure Active Directory Group attribute** into **Group Membership Attribute**.



Click **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.

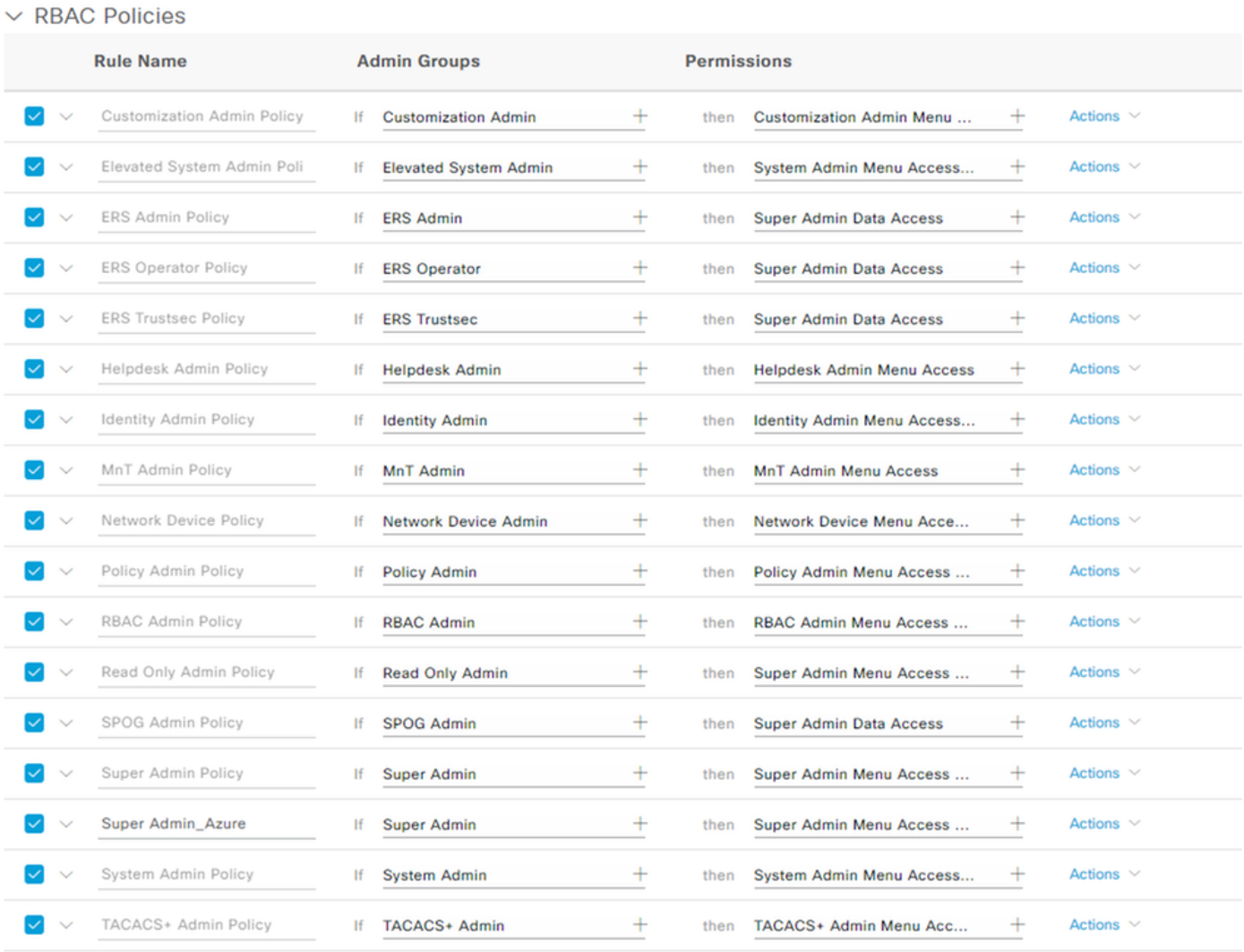


(Optional) Step 5. Configure RBAC Policies

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.



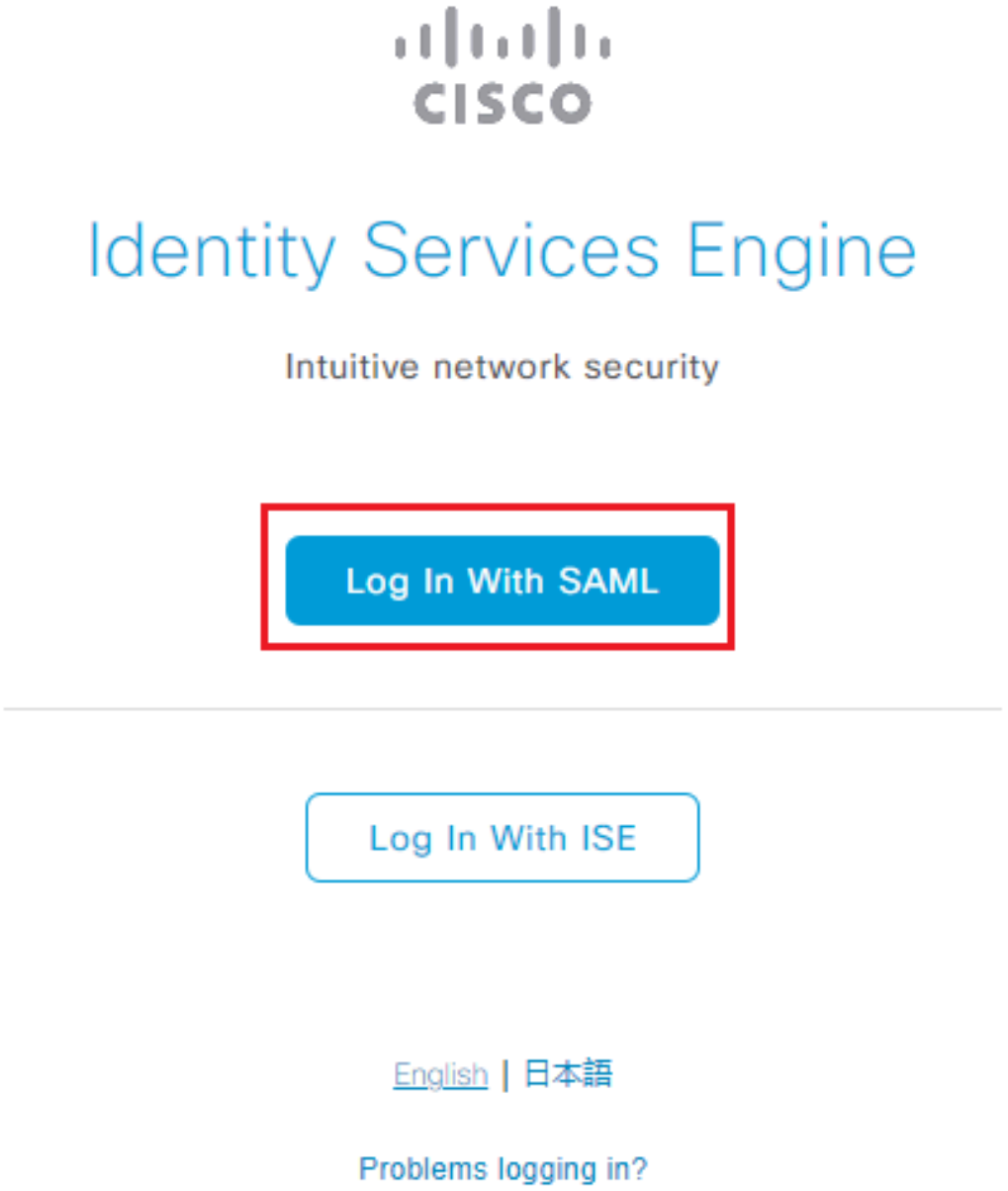
Verify

Confirm that your configuration works properly.

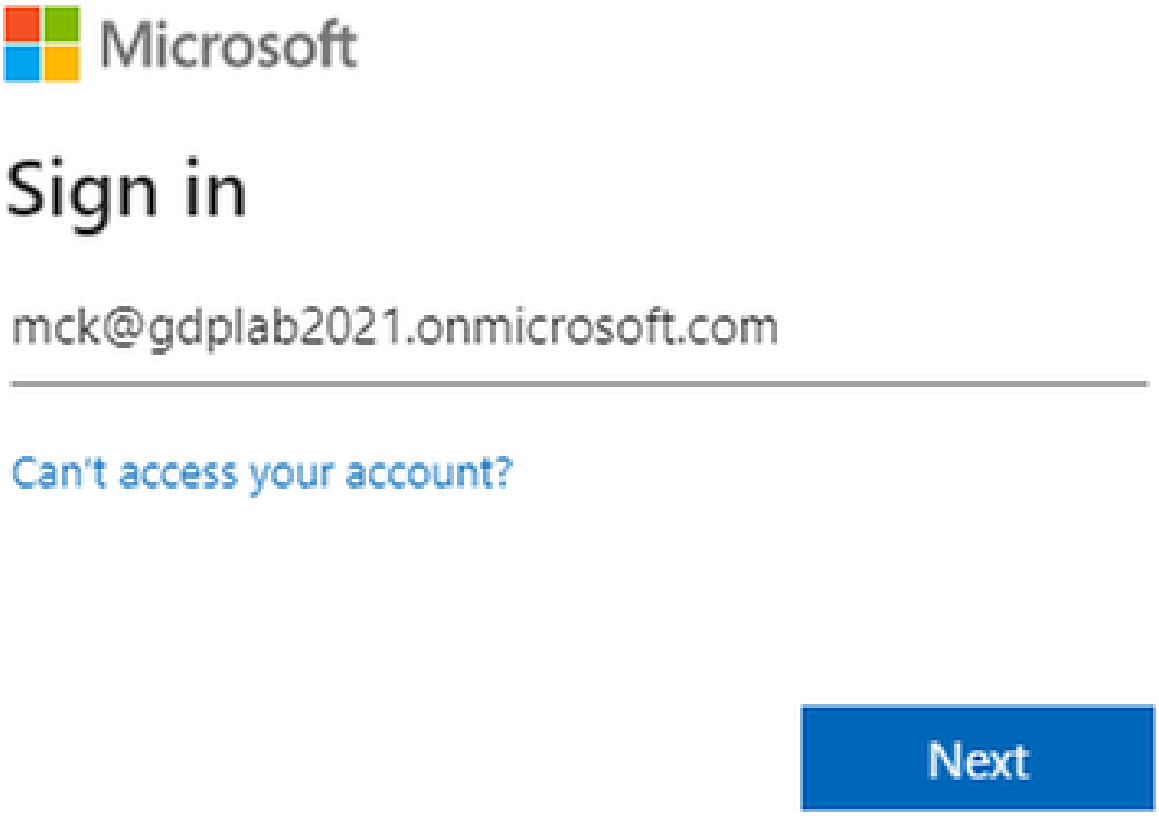
Note: SAML SSO Login test from the Azure test functionality does not work. The SAML request must be initiated by ISE for the Azure SAML SSO to work properly.

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

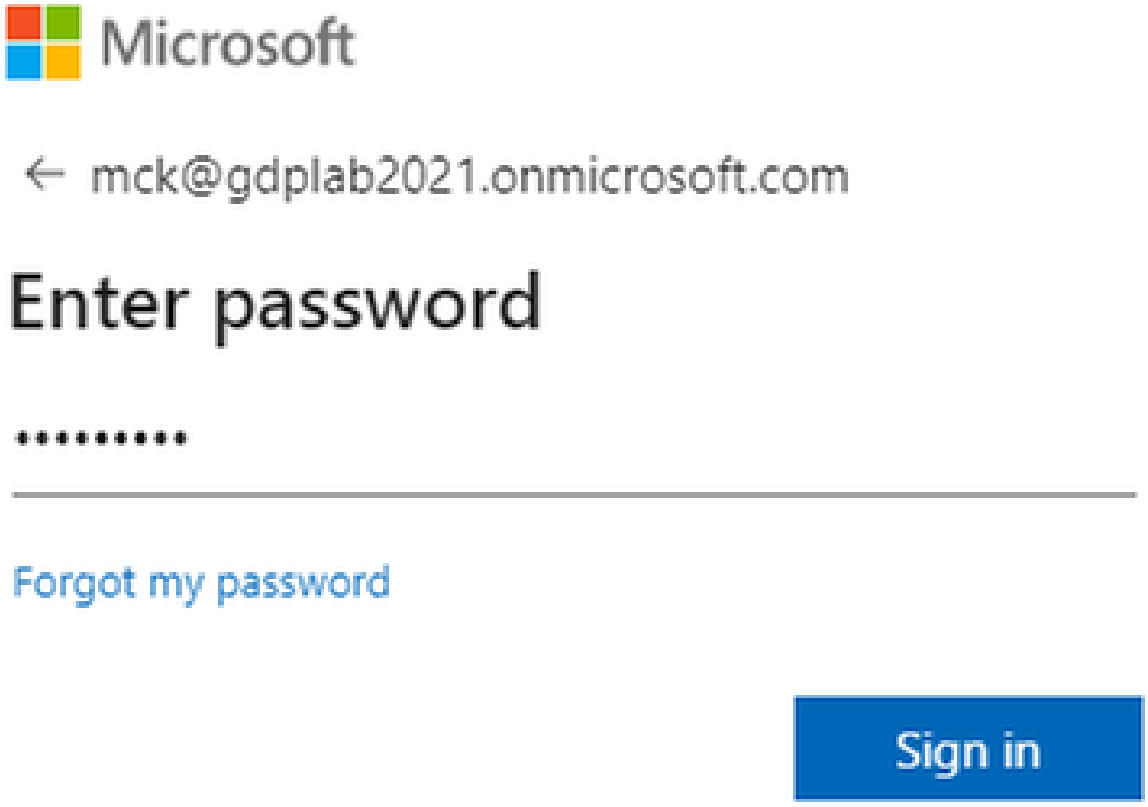
1. Access your ISE GUI Login page and click **Log In with SAML**.



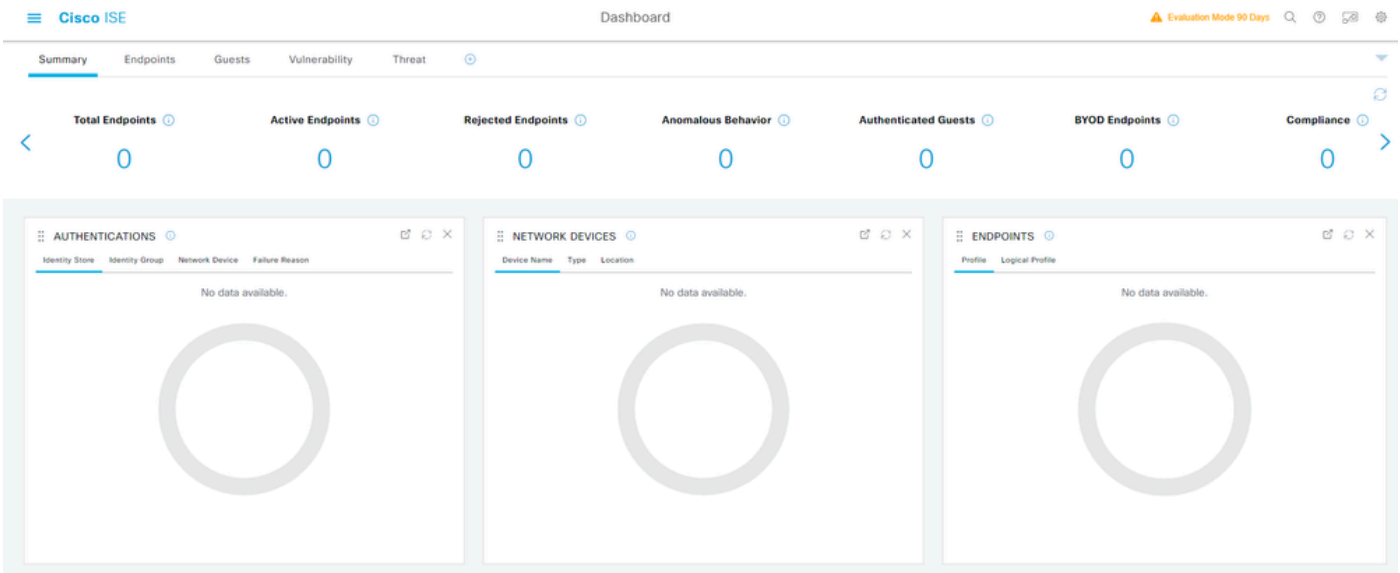
2. You are redirected to the Microsoft login screen. Enter your **Username** credentials of an account in a group mapped to ISE as shown here and click **Next** as shown in the image.



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



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.



Troubleshoot

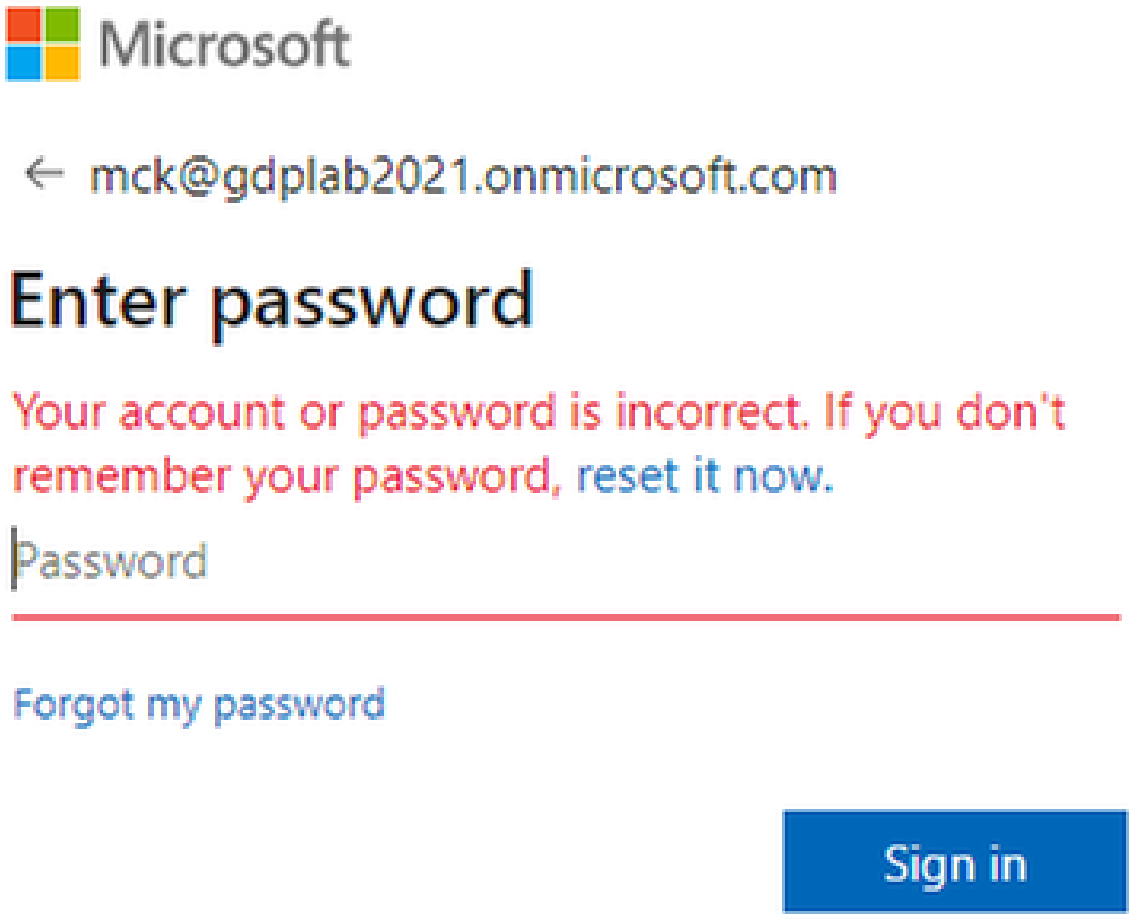
This section provides information you can use to troubleshoot your configuration.

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.

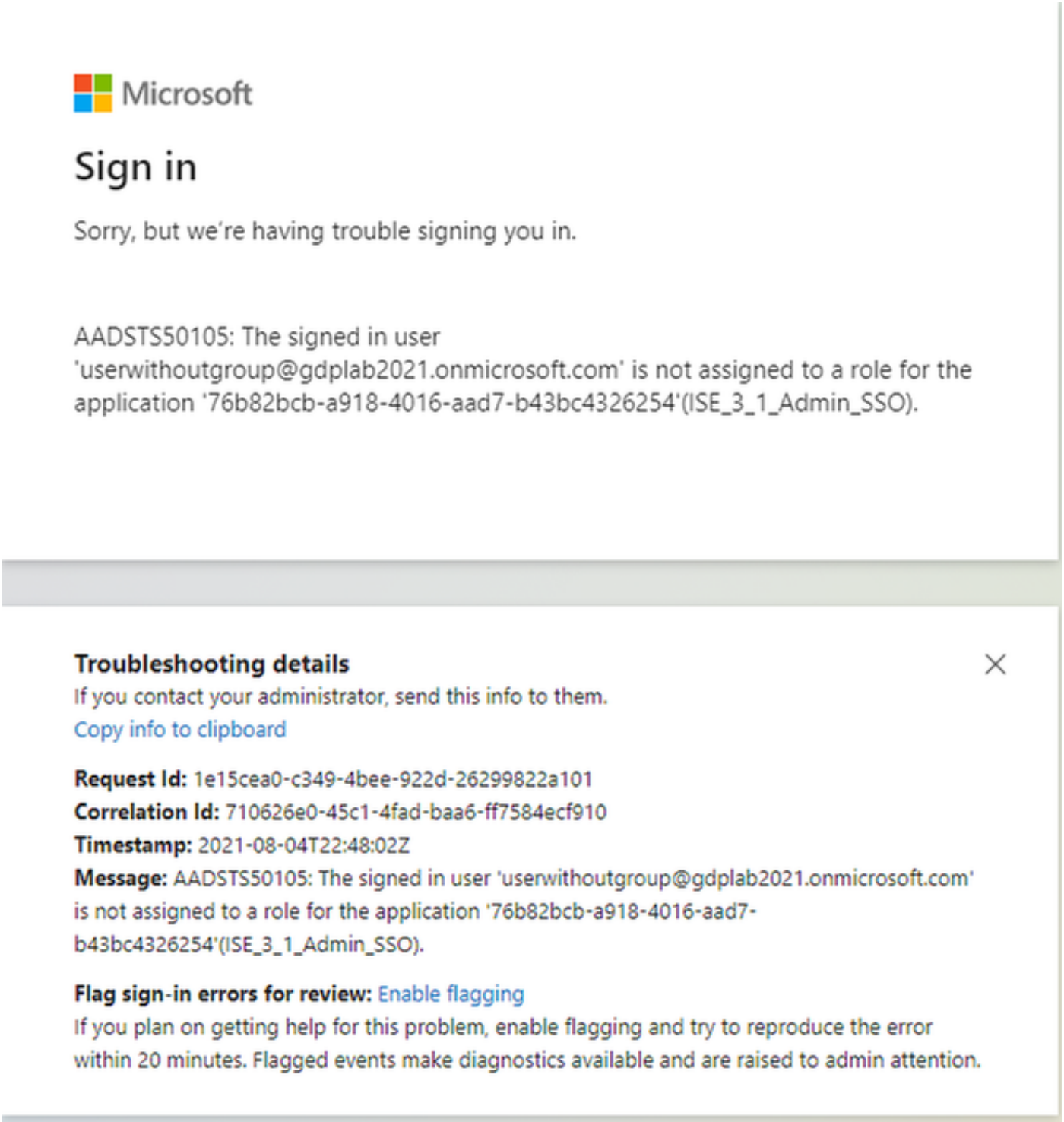
Issue 1. "Your account or password is incorrect" error is seen after you enter the credentials. Here, user data is not yet received by ISE and the process at this point still stays with IdP (Azure).

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.

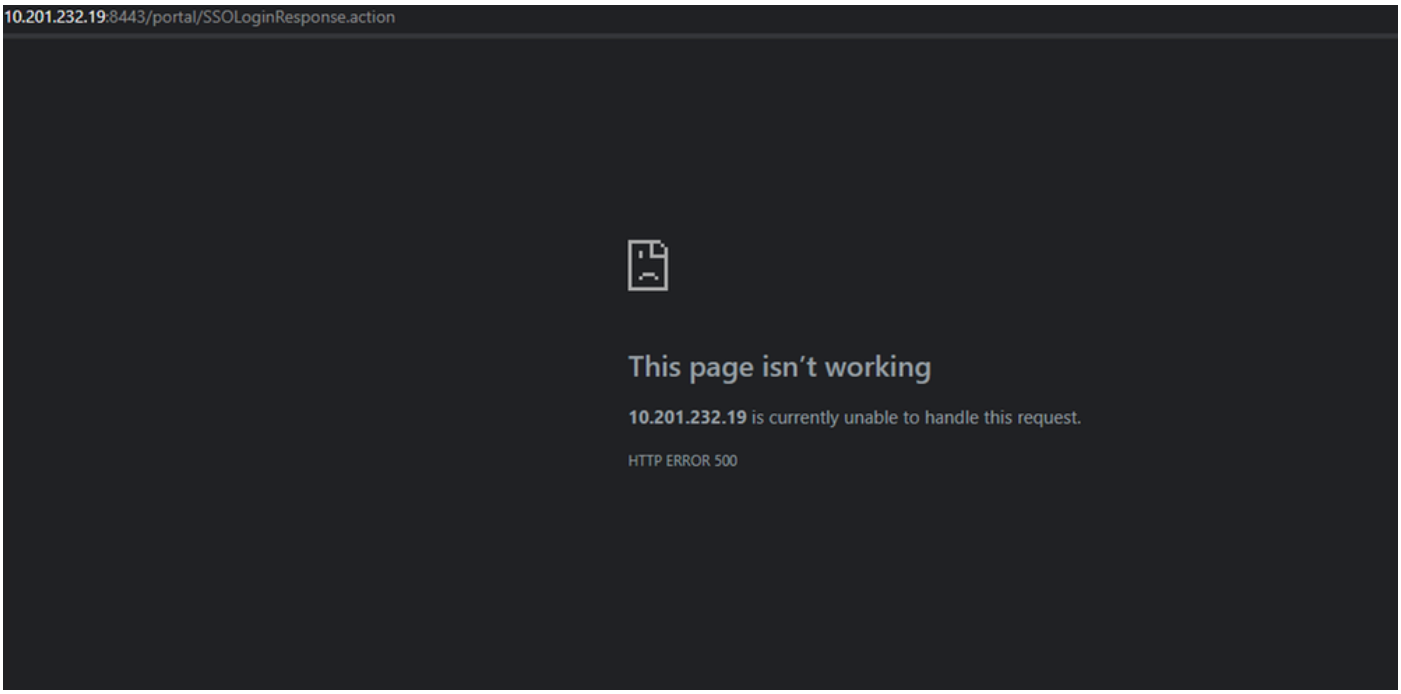


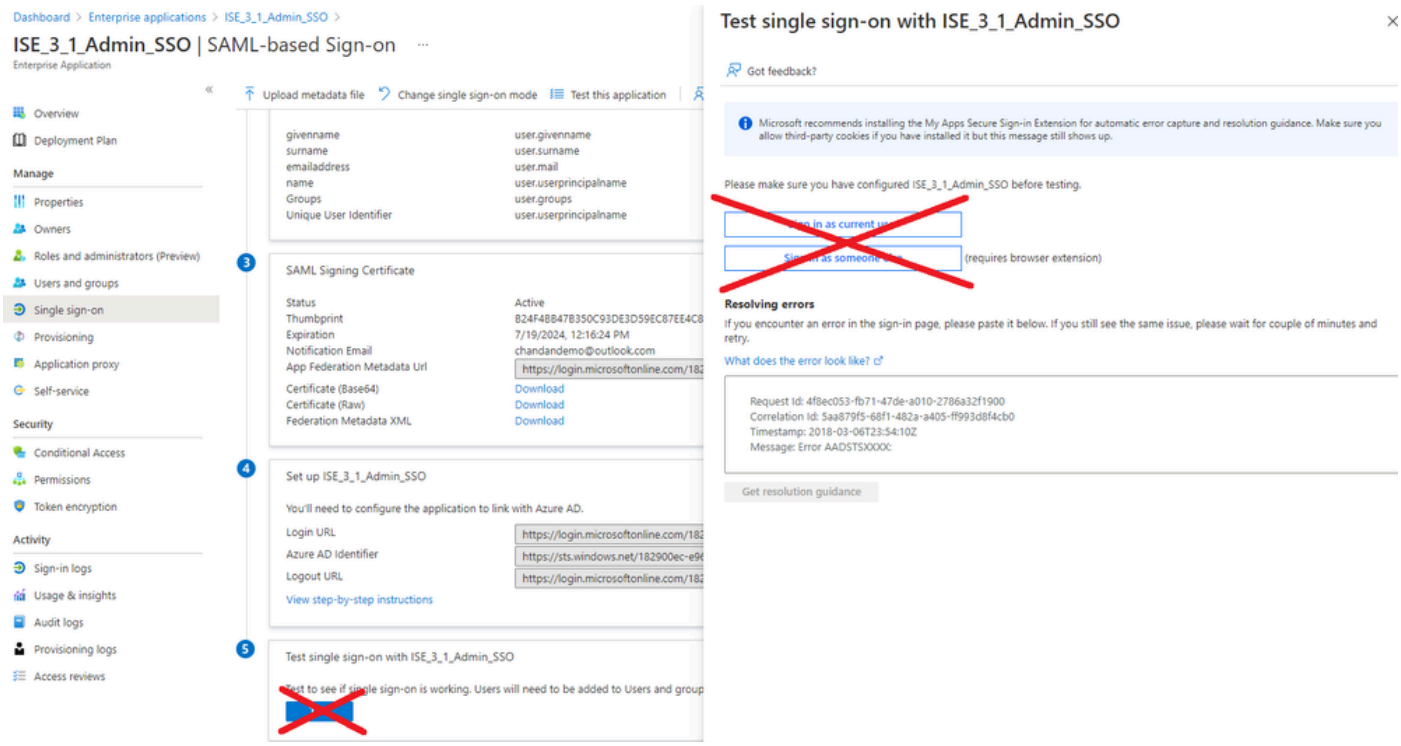
Issue 2. The user is not part of the group which is supposed to be allowed to access SAML SSO. Similar to the previous case, user data is not yet received by ISE and the process at this point still stays with IdP (Azure).

Solution: verify that the **Add group to the Application** configuration step is correctly executed as shown in the image.



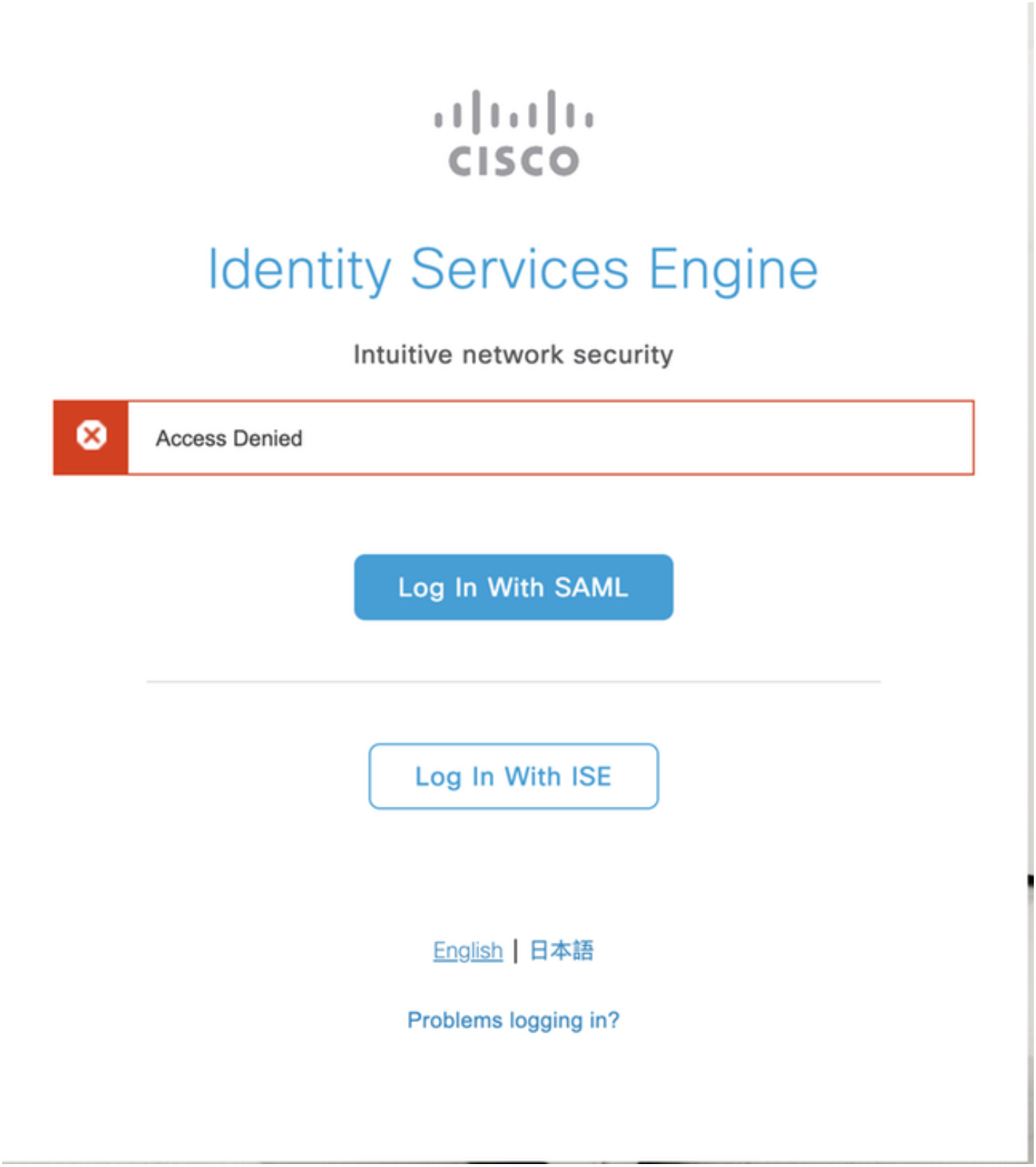
Issue 3. ISE Application Server is unable to handle SAML login requests. This issue occurs when the SAML request is initiated from the Identity Provider, Azure, instead of the Service Provider, ISE. Testing SSO Login from Azure AD does not work as ISE does not support Identity Provider initiated SAML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





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.

Solution: 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.



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.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/18290Oec-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 -:::