

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.

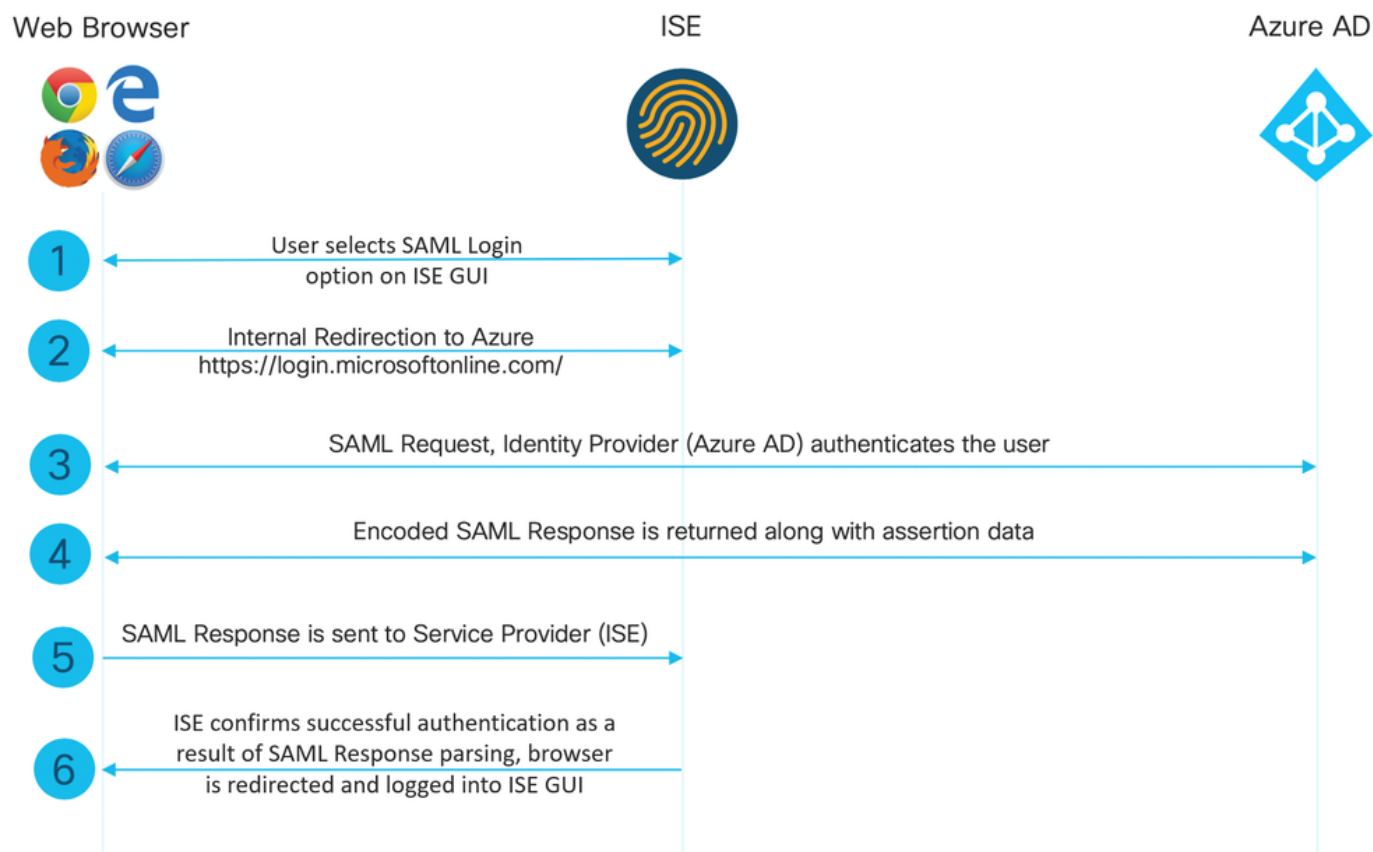
- Authentication assertions prove the identification of the user and provide the time the user logged in and what method of authentication they used (Kerberos, two-factor, as examples)
- The attribution assertion passes the SAML attributes, specific pieces of data that provide information about the user, to the service provider.
- An authorization decision assertion declares if the user is authorized to use the service or if the identity 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:



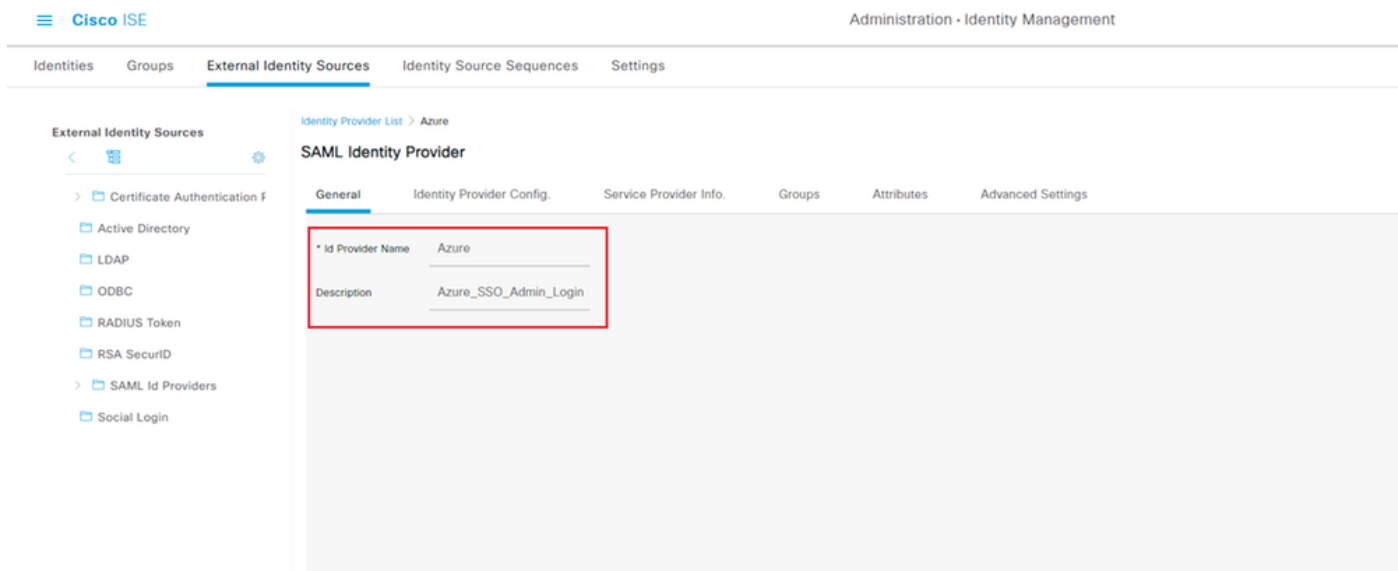
Configure SAML SSO Integration with Azure AD

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.

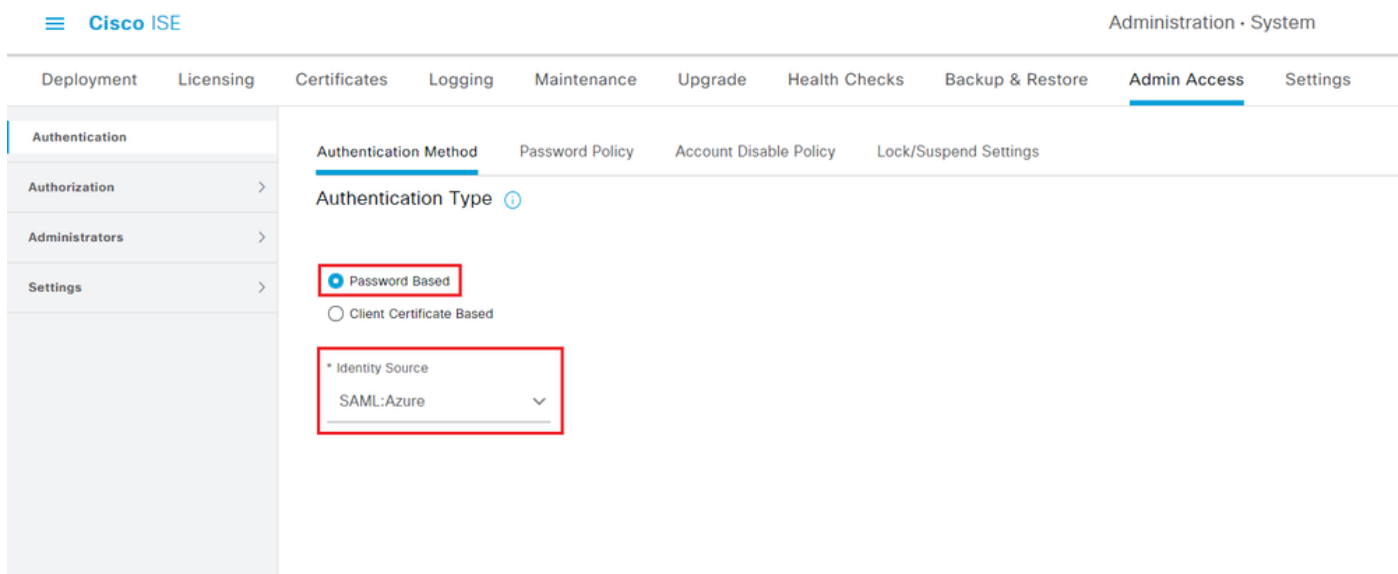
Enter the **Id Provider Name** and click **Submit** in order to save it. The **Id Provider Name** is significant only for ISE as shown in the image.



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.

SAML Identity Provider

General	Identity Provider Config.	Service Provider Info.	Groups	Attributes	Advanced Settings
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:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
            MIIITjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpT
            QU1MX21zZTMtMS0xOS5ja3VtYXJyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
            MCUxIzAhBgNVBAMTG1NBUTxfaXN1My0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
            AAOCAg8AMIICGKCAgEAvila4+S0uP3j037yCOXnHAzADupfqcgcwcp1JQnFxbVfnDd0ixGRT8iaQ
            1zdKhpwF/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohG0t1op01qDGwtOnwZGQ+ccvqXSL
            Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDzizyJGKdPf+1VM5JHCo6UNLF1IFyPmGvcCXnt
            NVqsYvxSzF038ciQq1m0sqvVrryZuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFF1Mzybvm1FYu
            9h83gl4WJWmiZETO6Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
            nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0sshkGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
            wYKSTn9/hn7JM1DqOR1PGEKvjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
            sDU4u0vFpFvrcC/lav9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
            ef+WFC9dWiy+ctbBTO+EM06Xj1aTi1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
            kVS9vT4EOzwNGo7pQI8CAwEAaA9MHswIAYDVRORBBkwF4IVaXN1My0xLTE5LmNrdW1hcjIuY29t
            MAwGA1UdEwQFMAMBAF8wCwYDVR0PBAQDAgLSMBOGA1UdDgQWBBIKjY2z/9H9PpwSnOPGARCj5iaZ
            oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
            206Dkb6fHdgKd9goN8N2bj+34ybwXqvDSwGtn4NA6Hy1q7N6iJzAD/7soZFhgOT2UTgZpRF9FsHn
            CGchSHqDt3bQ7g+Gw1vcgreC7R46qenaonXVr1tRw11vVIDcF8JQFFMxya/rIC4mxVeoo0j1F19d
            rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUteif0bqrOwCyWd9Tjg7KXfd2ITW
            hMxaFsv8wWcVuOMDPkP9xUwvt6gfH0bE51uT4EYVuuHwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
            nf/341cuRTJUmDh9g2mppbBw0cxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cfAZuiV/e3wk0BLZM
            1gV8FTVQSnra9LwHP/PgeNAPUCRPXSwake4rvjvMc0aS/iYdwZhziJ8zBdIBanMv5mGu1nvTet9K
            EEwj9ys1IHmdqoh3EmOF0gnzR0RvsMPbJxAoTfjfoITTMdQXNHhg+w1P0KXS2GC29vAM52d8ZCq
            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:SPSSODescriptor>
</md:EntityDescriptor>
```

```

<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>

```

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.

The screenshot shows the Azure Active Directory admin center interface. On the left, the 'FAVORITES' section has 'Azure Active Directory' highlighted. The main content area is titled 'Default Directory | Overview'. Below this, there's a search bar for the tenant. The 'Tenant information' card shows the user's role as 'Global administrator', the license as 'Azure AD Premium P2', the tenant ID as '64ace648-115d-4ad9-a3bf-7660...', and the primary domain as 'ekorneyccisco.onmicrosoft.com'. The 'Azure AD Connect' card shows the status as 'Not enabled' and the last sync as 'Sync has never run'. At the bottom, the 'Sign-ins' section displays a bar chart with the following values: 3, 2.8, 2.6, 2.4, 2.2, and 2.

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

☒ Auto-generate password

☐ Let me create the password

Initial 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



+ New group



Download groups



Delete



Refresh



Columns



All groups



Deleted groups



Diagnose and solve problems



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.

Azure Active Directory admin center

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. 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 



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.

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

🖨 Preview features

🗨 Got feedback?

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

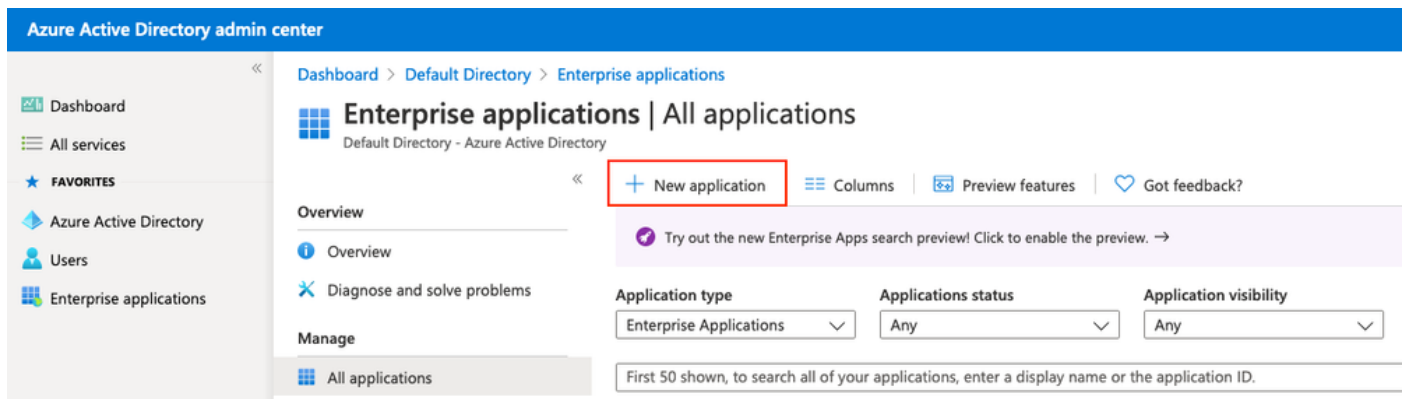
🔍 Search groups

+ Add filters

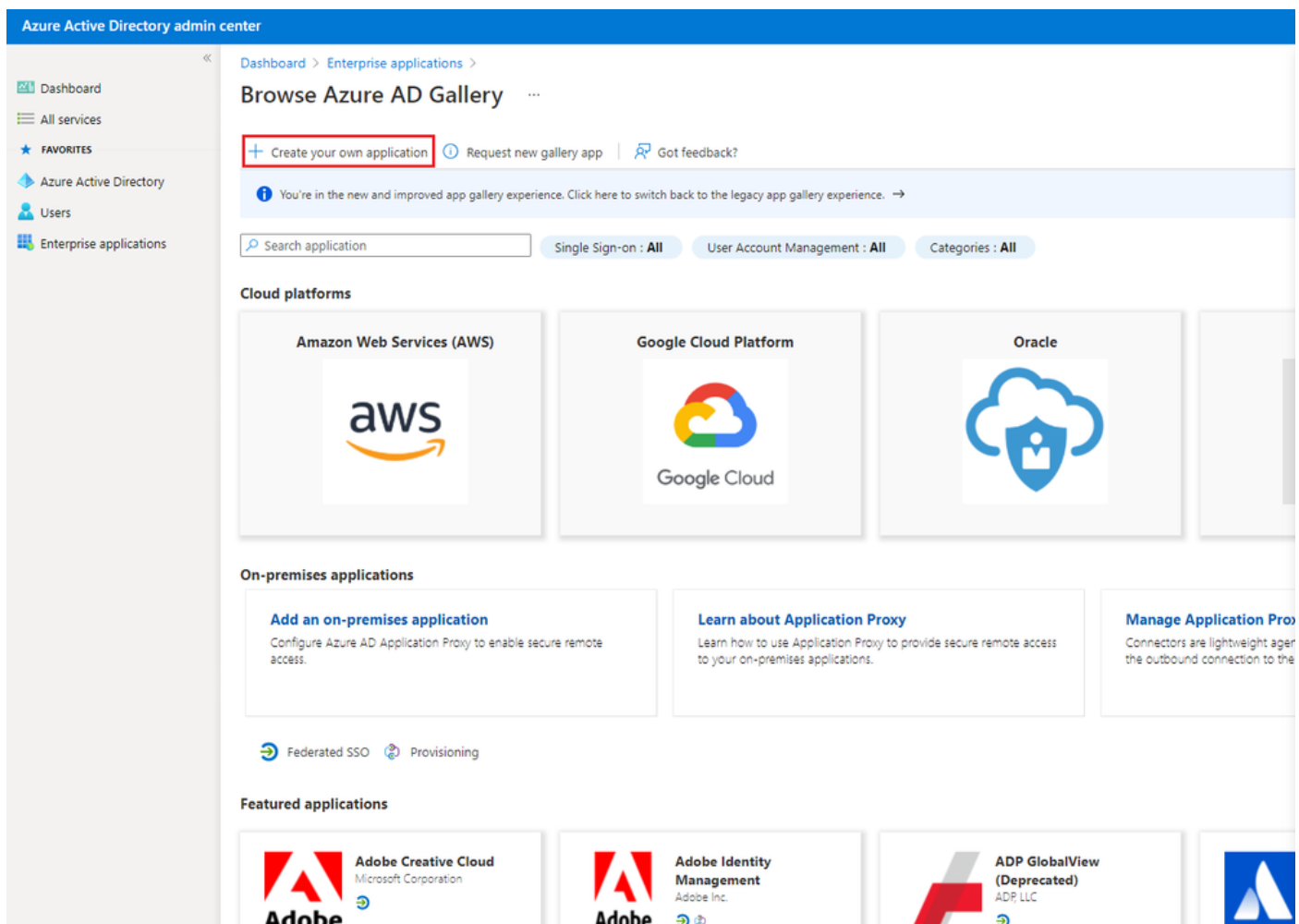
	Name	Object Id	Group Type	Membership Type
☐	 ISE Admin Group	576c60ec-c0b6-4044-a8ec-d395b1475d6e	Security	Assigned

4. Create an Azure AD Enterprise application:

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



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.

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)

Create

5. Add Group to the application:

Select **Assign users and groups**.

Azure Active Directory admin center

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

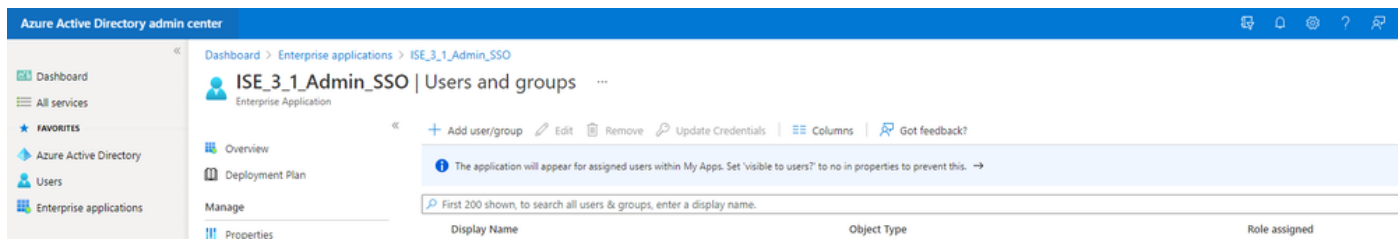
Application ID: 76b82bcb-a918-4016-aad7-...

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

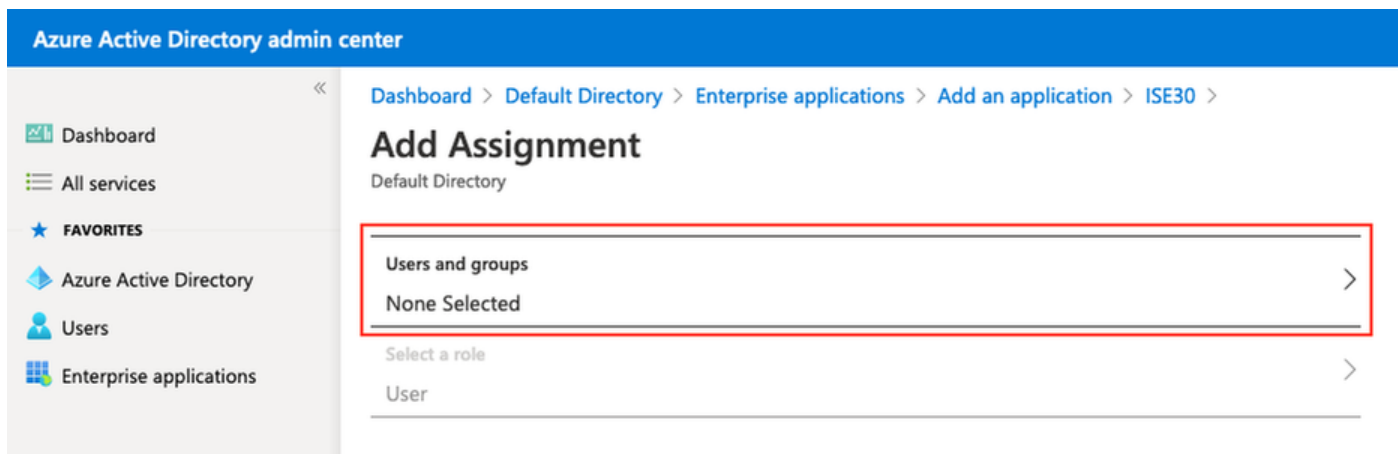
Getting Started

- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)

Click **Add user/group**.



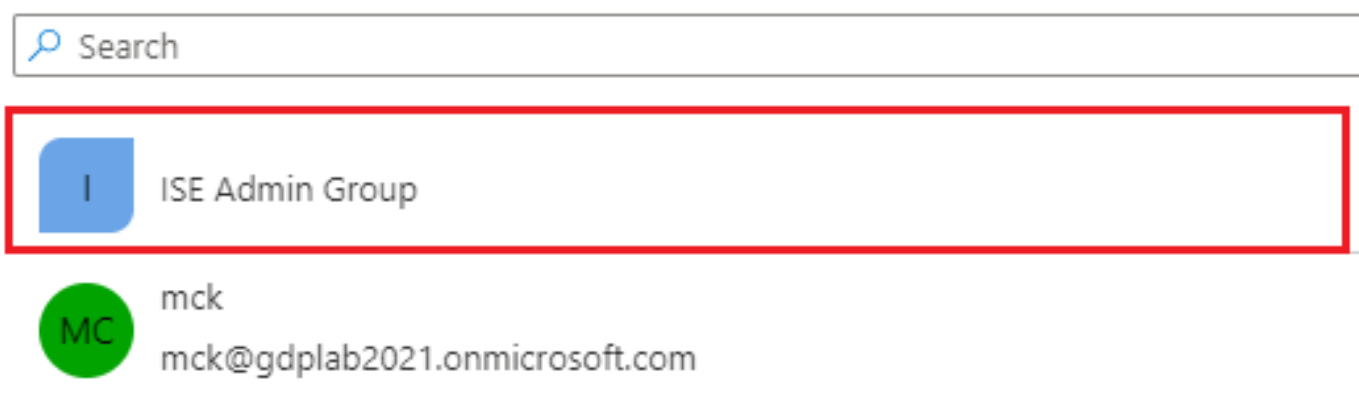
Click **Users and groups**.



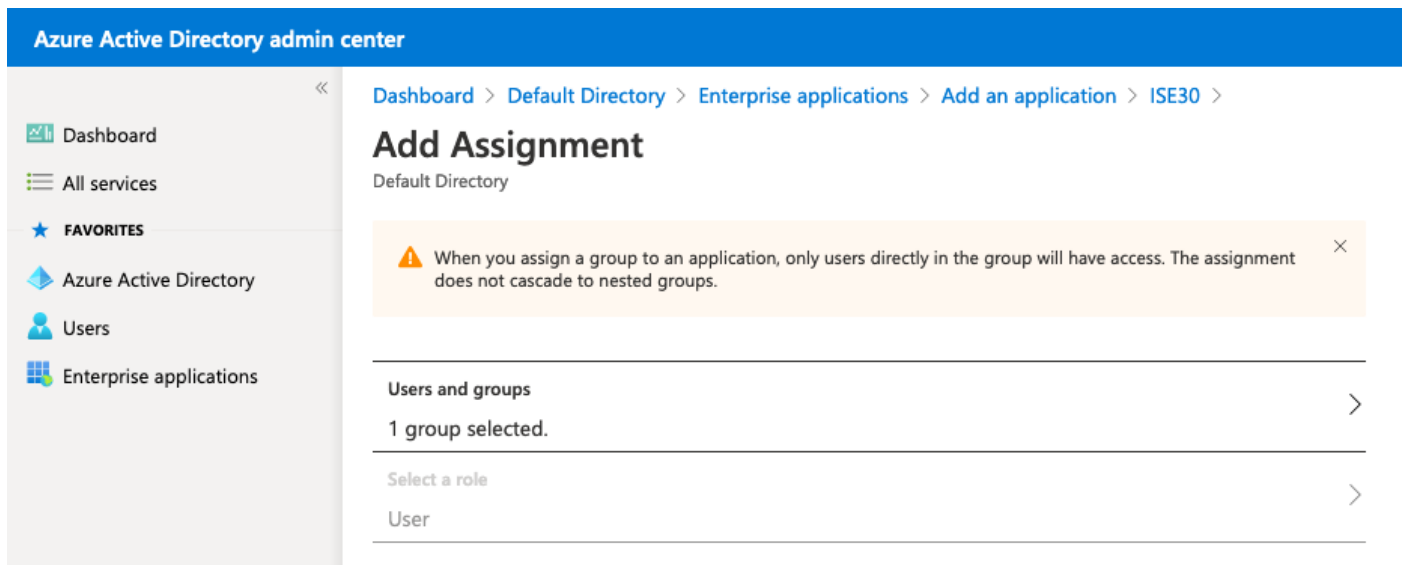
Choose the Group configured previously and click **Select**.

 **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.

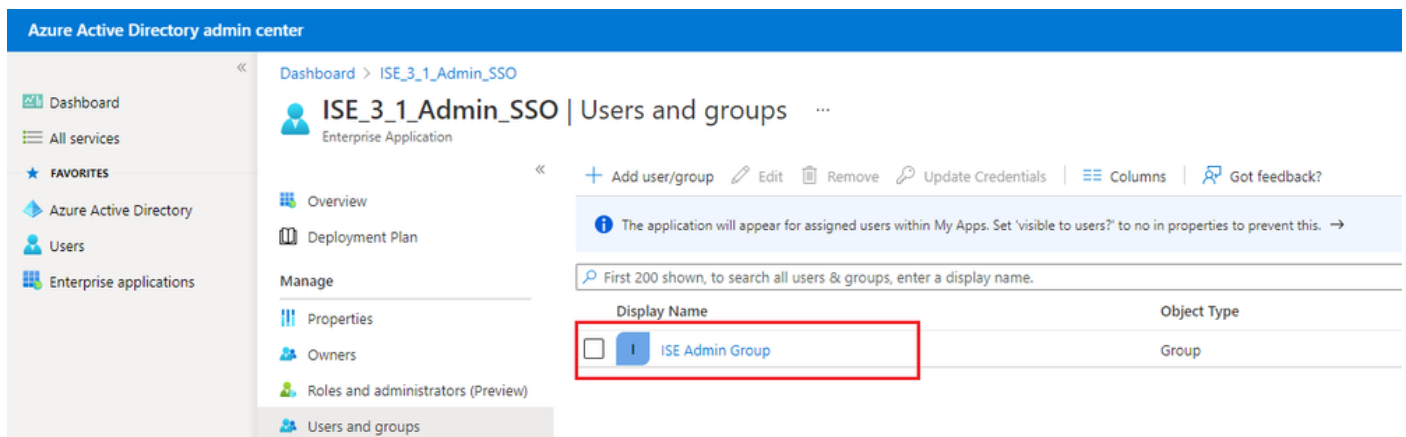
Users and groups



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

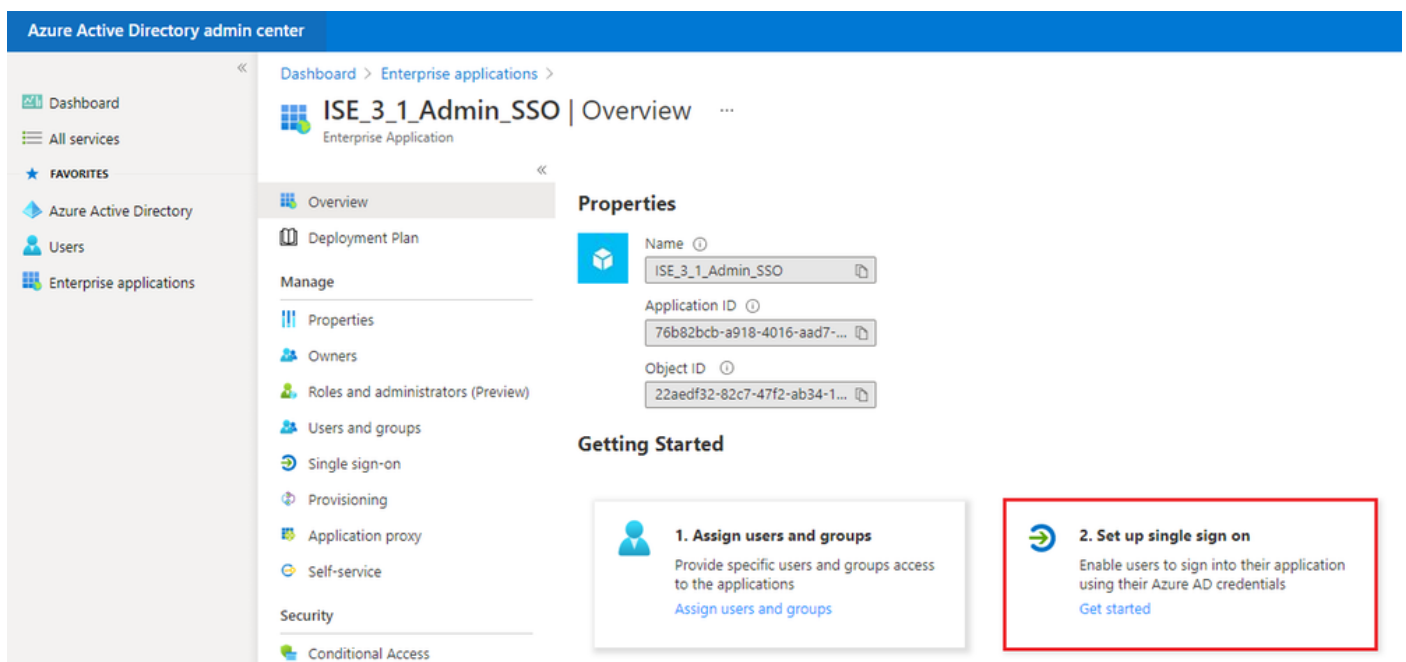


As a result, the **Users and groups** Menu for the configured application is populated with the selected Group.

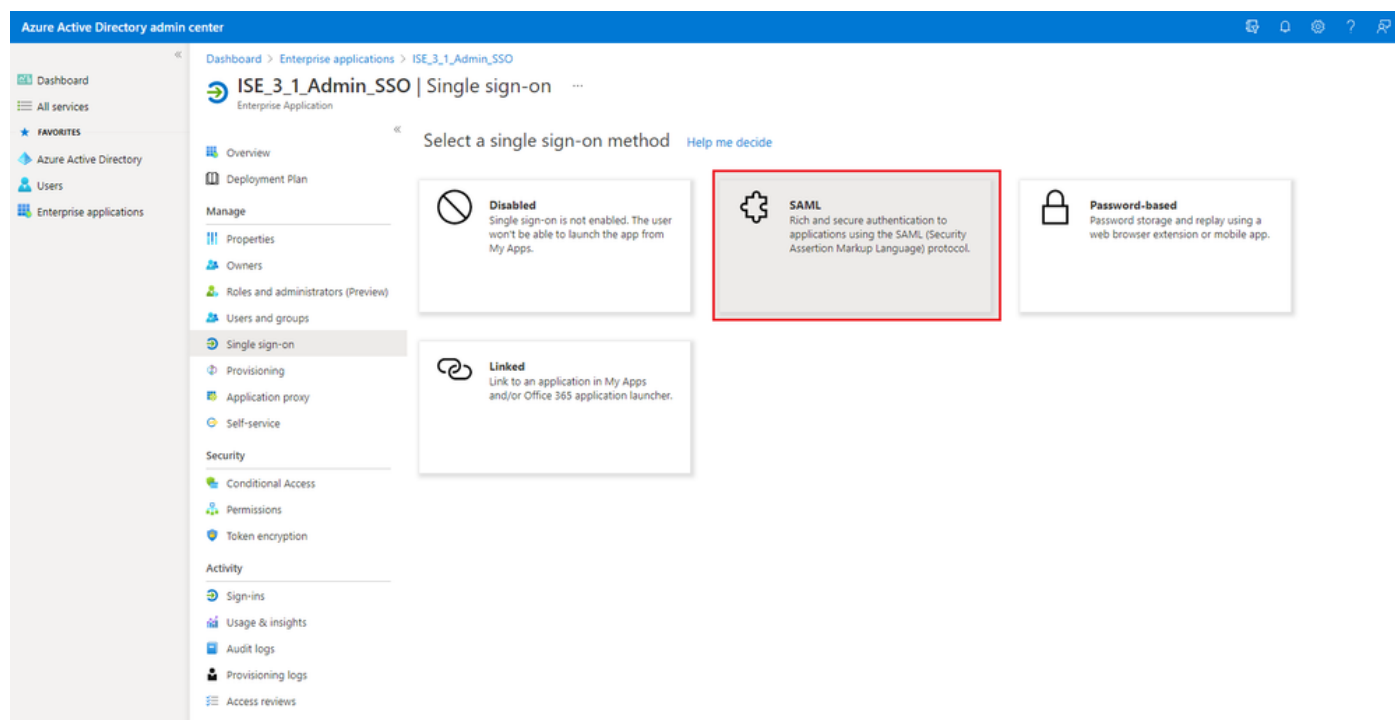


6. Configure an Azure AD Enterprise application:

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**.

Set up Single Sign-On with SAML

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

1

Basic SAML Configuration

Edit

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

2

User Attributes & Claims

Edit

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

Populate Identifier (Entity ID) 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 ×

 Save

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 ⓘ

Relay State ⓘ

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**.

Azure Active Directory admin center

Dashboard

All services

FAVORITES

Azure Active Directory

Users

Enterprise applications

Dashboard > Enterprise applications > ISE30 > 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
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 > 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**.

SAML Signing Certificate Edit

Status	Active
Thumbprint	B24F48B47B350C93DE3D59EC87EE4C815C884462
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 ⓘ

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
 - Social Login

Identity Provider List > Azure

SAML Identity Provider

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

Groups

Group Membership Attribute ⓘ

☐ Name in Assertion

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

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) 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 <u>Customization Admin</u> +	then <u>Customization Admin Menu ...</u> +	Actions ▼
☒ ▼	Elevated System Admin Poli	If <u>Elevated System Admin</u> +	then <u>System Admin Menu Access...</u> +	Actions ▼
☒ ▼	ERS Admin Policy	If <u>ERS Admin</u> +	then <u>Super Admin Data Access</u> +	Actions ▼
☒ ▼	ERS Operator Policy	If <u>ERS Operator</u> +	then <u>Super Admin Data Access</u> +	Actions ▼
☒ ▼	ERS Trustsec Policy	If <u>ERS Trustsec</u> +	then <u>Super Admin Data Access</u> +	Actions ▼
☒ ▼	Helpdesk Admin Policy	If <u>Helpdesk Admin</u> +	then <u>Helpdesk Admin Menu Access</u> +	Actions ▼
☒ ▼	Identity Admin Policy	If <u>Identity Admin</u> +	then <u>Identity Admin Menu Access...</u> +	Actions ▼
☒ ▼	MnT Admin Policy	If <u>MnT Admin</u> +	then <u>MnT Admin Menu Access</u> +	Actions ▼
☒ ▼	Network Device Policy	If <u>Network Device Admin</u> +	then <u>Network Device Menu Acce...</u> +	Actions ▼
☒ ▼	Policy Admin Policy	If <u>Policy Admin</u> +	then <u>Policy Admin Menu Access ...</u> +	Actions ▼
☒ ▼	RBAC Admin Policy	If <u>RBAC Admin</u> +	then <u>RBAC Admin Menu Access ...</u> +	Actions ▼
☒ ▼	Read Only Admin Policy	If <u>Read Only Admin</u> +	then <u>Super Admin Menu Access ...</u> +	Actions ▼
☒ ▼	SPOG Admin Policy	If <u>SPOG Admin</u> +	then <u>Super Admin Data Access</u> +	Actions ▼
☒ ▼	Super Admin Policy	If <u>Super Admin</u> +	then <u>Super Admin Menu Access ...</u> +	Actions ▼
☒ ▼	Super Admin_Azure	If <u>Super Admin</u> +	then <u>Super Admin Menu Access ...</u> +	Actions ▼
☒ ▼	System Admin Policy	If <u>System Admin</u> +	then <u>System Admin Menu Access...</u> +	Actions ▼
☒ ▼	TACACS+ Admin Policy	If <u>TACACS+ Admin</u> +	then <u>TACACS+ Admin Menu Acc...</u> +	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**.



Identity Services Engine

Intuitive network security

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

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.



Sign in

mck@gdplab2021.onmicrosoft.com

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

Next

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



← mck@gdplab2021.onmicrosoft.com

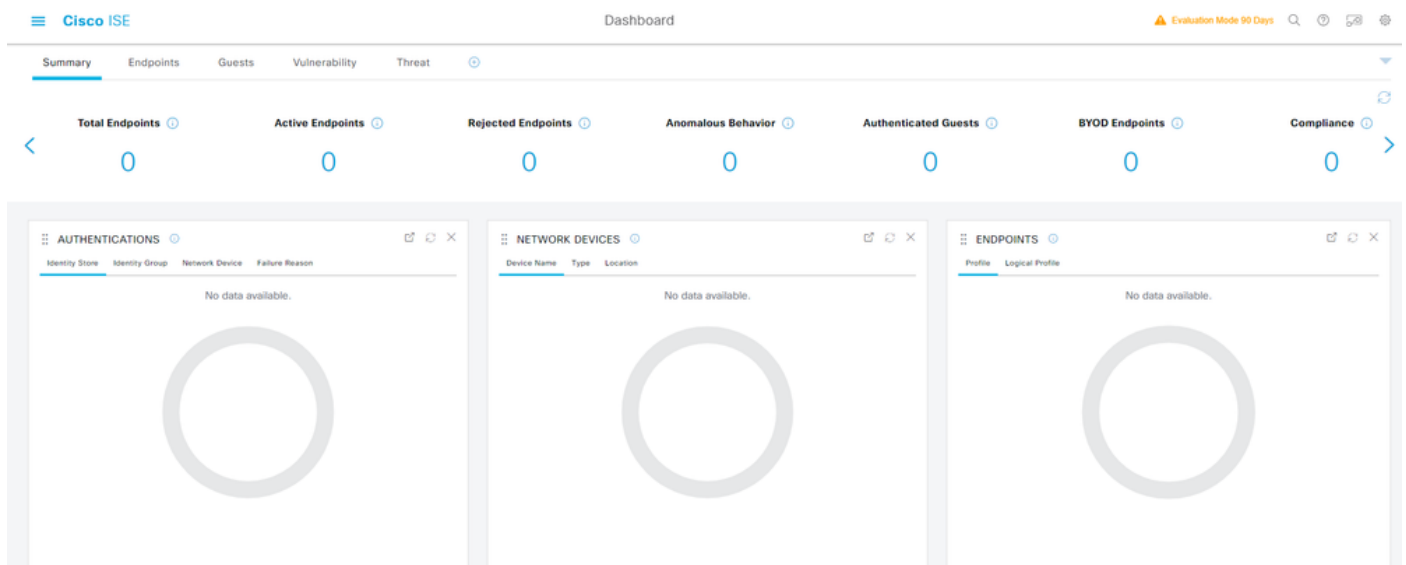
Enter password

••••••••

[Forgot my password](#)

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.



← 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

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.



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.



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

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	824F48B478350C93DE3D59EC87EE4C8
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	https://login.microsoftonline.com/182900ec-e99e-4b41-b0f0-6a2103200000/...
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/182900ec-e99e-4b41-b0f0-6a2103200000/...
Azure AD Identifier	https://sts.windows.net/182900ec-e99e-4b41-b0f0-6a2103200000/...
Logout URL	https://login.microsoftonline.com/182900ec-e99e-4b41-b0f0-6a2103200000/...

[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? c?

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

[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.

Solution: ensure the group claim name in Azure and ISE 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.



Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

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

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