

# 通过与Azure AD集成的SAML SSO配置ISE 3.1 ISE GUI管理员登录流

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

### [背景信息](#)

#### [身份提供程序\(IdP\)](#)

#### [服务提供商\(SP\)](#)

#### [SAML](#)

#### [SAML断言](#)

### [高级流程图](#)

### [配置SAML SSO与Azure AD的集成](#)

#### [步骤1:在ISE上配置SAML身份提供程序](#)

- [1.将Azure AD配置为外部SAML身份源](#)
- [2.配置ISE身份验证方法](#)
- [3.导出服务提供商信息](#)

#### [第二步：配置Azure AD IdP设置](#)

- [1.创建Azure AD用户](#)
- [2.创建Azure AD组](#)
- [3.将Azure AD用户分配给组](#)
- [4.创建Azure AD Enterprise应用程序](#)
- [5.将组添加到应用程序](#)
- [6.配置Azure AD Enterprise应用程序](#)
- [7.配置Active Directory组属性](#)
- [8.下载Azure联合身份验证元数据XML文件](#)

#### [第三步：将元数据从Azure Active Directory上传到ISE](#)

#### [第四步：在ISE上配置SAML组](#)

#### [\(可选\) 第五步。配置RBAC策略](#)

### [验证](#)

### [故障排除](#)

#### [常见问题](#)

#### [排除ISE故障](#)

##### [SAML登录和组声明名称不匹配的日志](#)

---

## 简介

本文档介绍如何配置Cisco ISE 3.1 SAML SSO与外部身份提供程序(例如Azure Active Directory(AD))的集成。

# 先决条件

## 要求

Cisco 建议您了解以下主题：

1. 思科ISE 3.1
2. SAML SSO部署
3. Azure AD

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

1. 思科ISE 3.1
2. Azure AD

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

### 身份提供程序(IdP)

在这种情况下是Azure AD的授权机构，用于验证用户身份以及对所请求的资源（“服务提供商”）的访问权限并声明这些权限。

### 服务提供商(SP)

用户想要访问的托管资源或服务，在本例中为ISE应用服务器。

## SAML

安全断言标记语言(SAML)是允许IdP向SP传递授权凭证的开放标准。

SAML事务使用可扩展标记语言(XML)实现身份提供者和服务提供商之间的标准化通信。

SAML是用户身份验证与授权之间的链接，以便使用服务。

### SAML断言

SAML断言是身份提供程序发送到包含用户授权的服务提供商的XML文档。

有三种不同类型的SAML断言 — 身份验证、属性和授权决策。

- 身份验证断言可证明用户的身份，并提供用户登录的时间以及他们使用的身份验证方法（例如

, Kerberos , 双因素 )

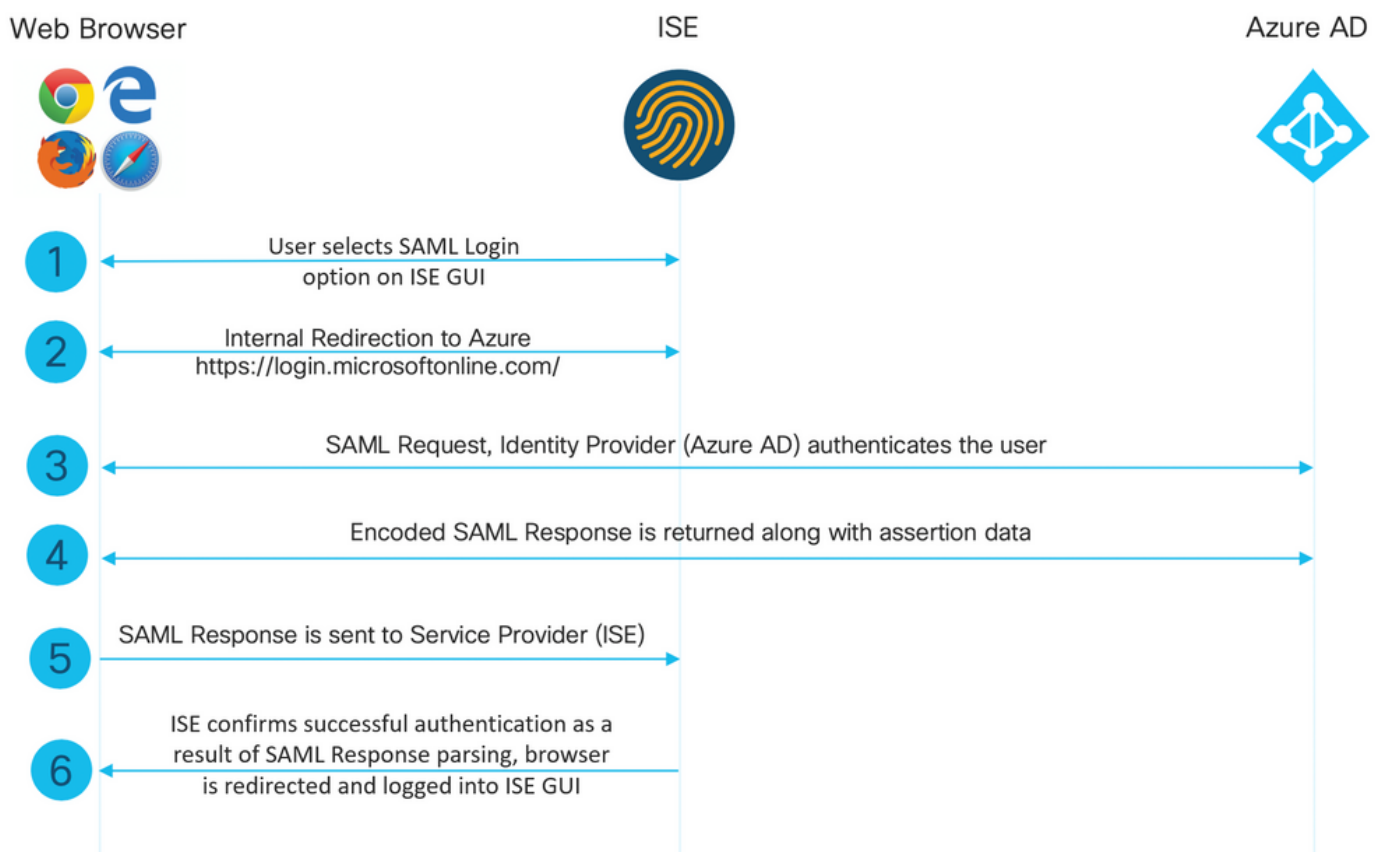
- 归属断言将SAML属性 ( 提供有关用户信息的特定数据片段 ) 传递给服务提供商。
- 授权决策断言声明用户是否被授权使用服务 , 或者如果标识提供者由于密码失败或缺乏对服务的权利而拒绝他们的请求。

## 高级流程图

SAML的工作原理是在身份提供程序、 Azure AD和服务提供程序ISE之间传递有关用户、 登录和属性的信息。

每个用户通过身份提供程序登录一次单点登录(SSO) , 然后Azure AD提供程序在用户尝试访问这些服务时将SAML属性传递给ISE。

ISE从Azure AD请求授权和身份验证 , 如图所示。



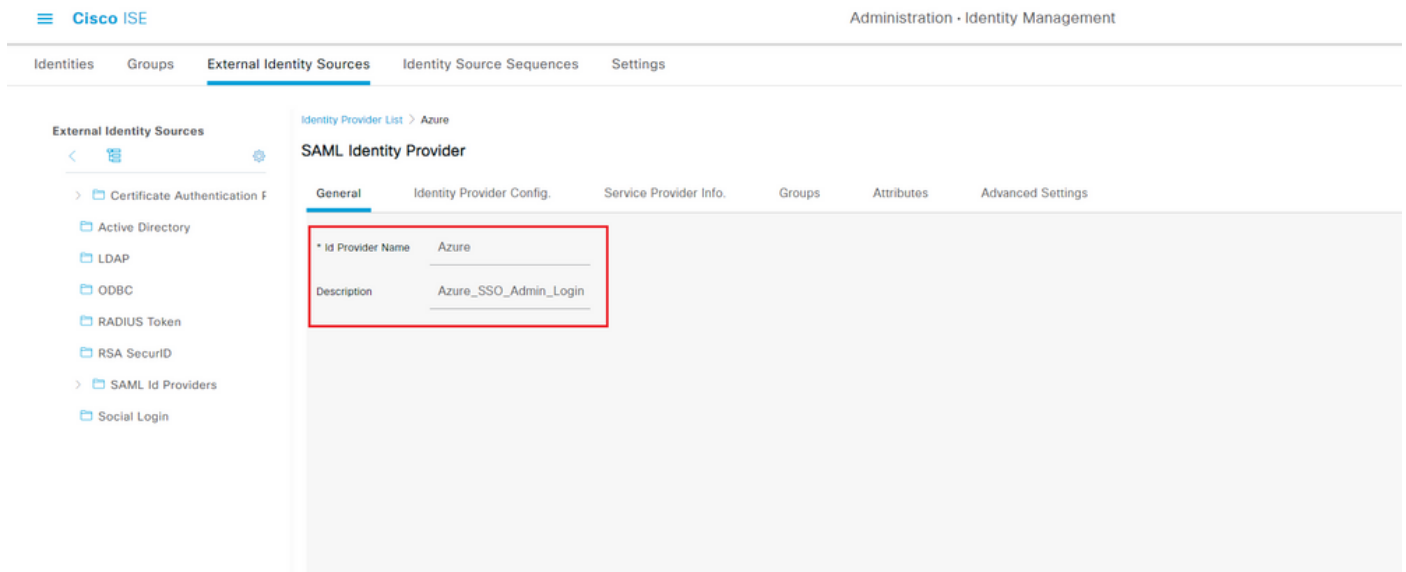
## 配置SAML SSO与Azure AD的集成

### 步骤1:在ISE上配置SAML身份提供程序

#### 1.将Azure AD配置为外部SAML身份源

在ISE上 , 导航到Administration > Identity Management > External Identity Sources > SAML Id Providers , 然后点击Add按钮。

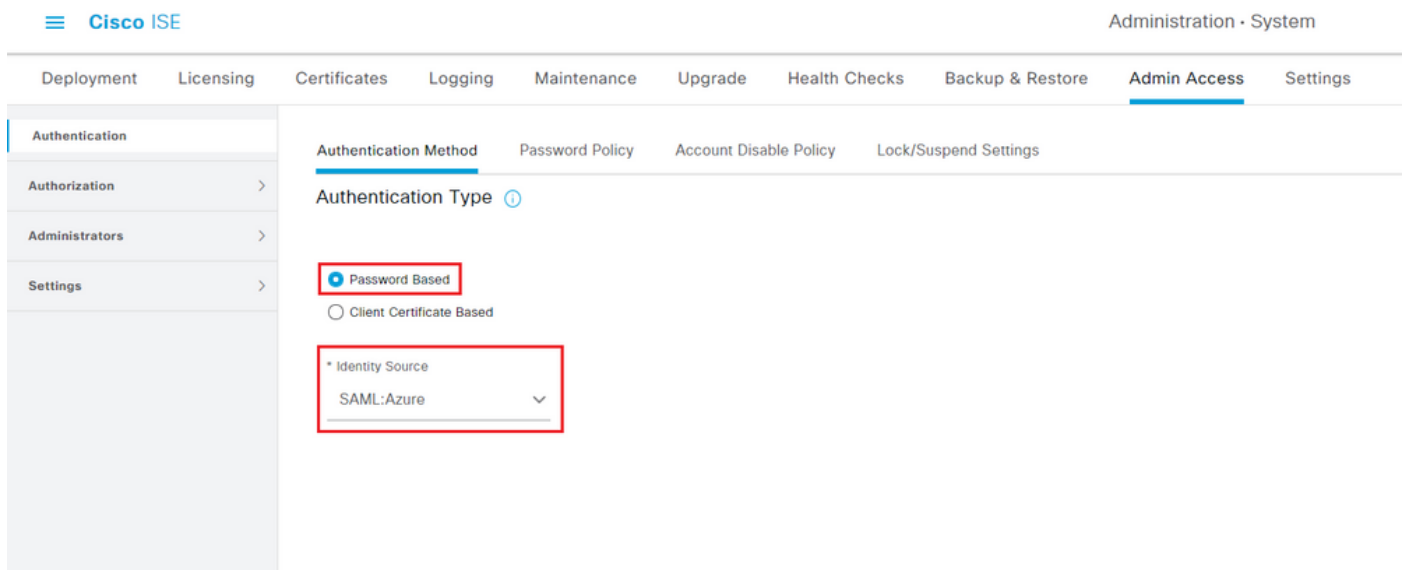
输入Id Provider Name并单击Submit以保存它。Id提供程序名称仅对ISE有效，如图所示。



## 2. 配置ISE身份验证方法

导航到Administration > System > Admin Access > Authentication > Authentication Method，然后选择Password Based单选按钮。

从Identity Source下拉列表中选择之前创建的所需ID提供程序名称，如图所示。



## 3. 导出服务提供商信息

导航到管理>身份管理>外部身份源 > SAML Id提供程序> [您的SAML提供程序]。

将该选项卡切换到Service Provider Info，然后单击Export按钮（如图所示）。

## 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)

下载.xml文件并保存。记录Location URL和entityID值。

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://CiscoISE/0049a2fd-7047-4d1d-8907-5a05a94ff5fd" xmlns:md="urn:oasis:
<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>
MIIFTjCCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDEExpT
QU1MX21zZTMtMS0xOS5ja3VtYXlyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTGNBtUxfaXN1My0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICGKCAgEAvila4+S0uP3j037yCOXnHAzADupfqcgcwcp1JQnFxbVfnDd0ixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohG0t1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYd1DtE1LMEcGg1mCd56GfrDcJdX0cZJmiDziyZyGKdDpf+1VM5JHCo6UNLF1IFyPmGvcCXnt
NVqsYvxSzF038ciQq1m0sqrVrryZuIUAXDWUNUg9pSGzH0FkSsZRPxrQh+3N5DEFF1Mzybvm1FYu
9h83g4LWJWmiZET06Vs/D0p6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5R0gT7v3CDrdFtRoNYAT+Yv0941KzFCSE0sshkGSjgVn31XQ5vgDH1PvqNaYs/PWicvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNz1FuggaE8tC7uyuQZa2rcmTrXGWC1
sDU4u0vFpFvrcC/1avr9Fnx7LPwXa0asvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWiy+ctbBTO+EM06Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5058Zot9gqkpFw
kVS9v4E0zwNGo7pQI8CAwEAAN9MhswIAYDVR0RBkF4IVaXN1My0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAF8wCwYDVR0PBAQDAgLSMB0GA1UdDgQWBBIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHsUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
206Dkb6fHdgKd9goN8N2bj+34ybwqxvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+Gw1vcgreC7R46qenaonXVr1tRw11vVIcF8JQFFMxya/rIC4mxVeoo0j1F19d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4H0vdm6oF3uBte0/pdUteif0bqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwvt6gfH0bE51uT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmdh9g2mppbBw0cxzoUxDm+HReSe+0JhRCyIJc0vUpdNmYC8cFAZuiv/e3wk0BLZM
TgV8FTVQSnra9LwHP/PgeNAPUcRPXSwake4rvjvMc0aS/iYdwZhziJ8zBdIBanMv5mGu1nvTEt9K
EEwj9ys1IHmdqoH3Em0F0gnzR0RvsMPbJxAoTFjfoITTMdQXNHhg+w1POKXS2GCZ29vAM52d8ZCq
Urz0VxNHKWKwER/q1GgaWvh3X/G+z1shUQDRjCbdLcZi1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/nChcoxFY759LA+m7Brp7FFPiGCrPW8E0v7bUMSDmmg/53NoktfJ1CckaWE87myhimj0
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
```

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService index="0" Location="https://10.201.232.19:8443/portal/SSOLoginResponse.act
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLogin

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

XML文件中的相关属性：

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

AssertionConsumerService

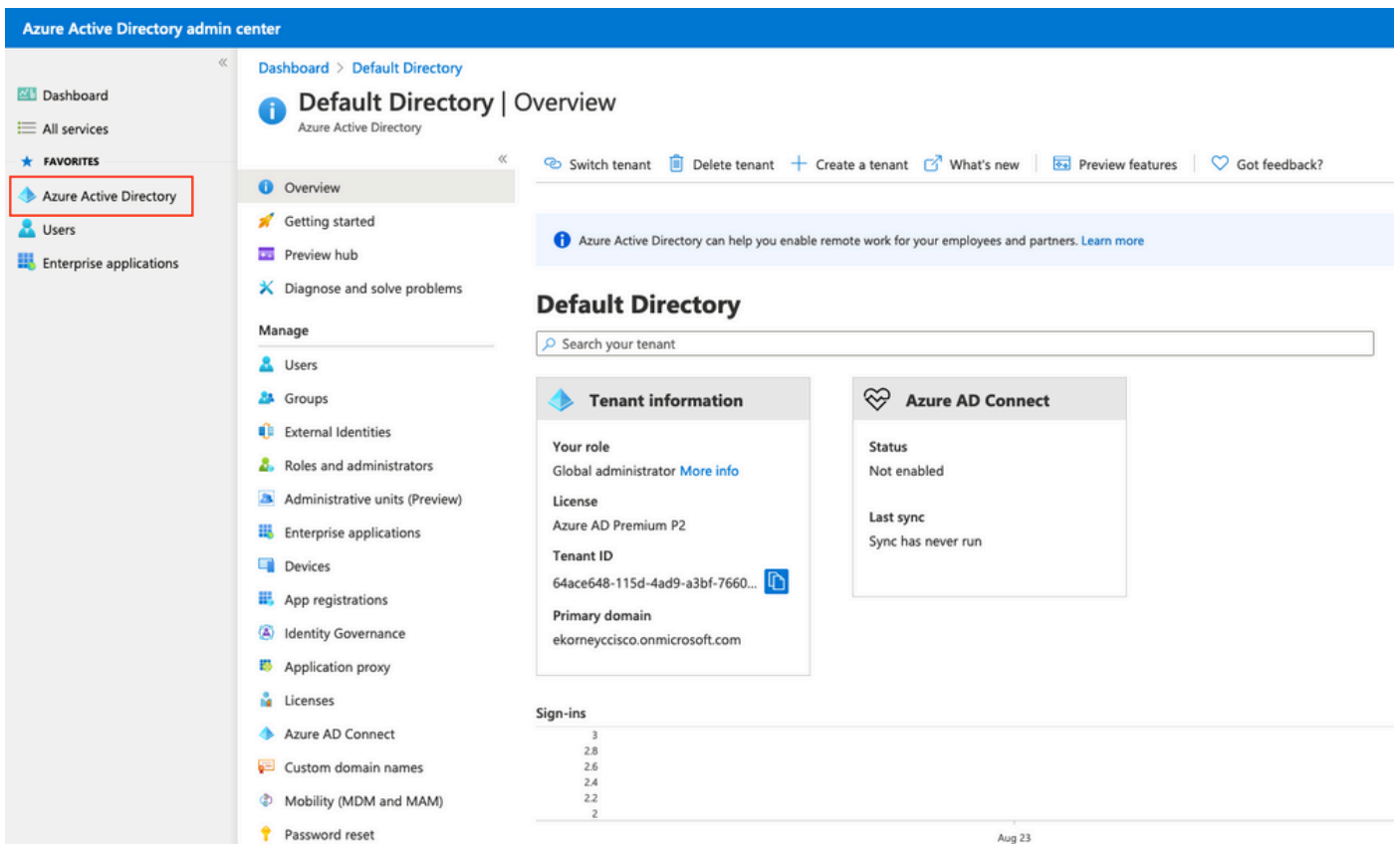
Location="<https://10.201.232.19:8443/portal/SSOLoginResponse.action>"

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

## 第二步：配置Azure AD IdP设置

### 1. 创建Azure AD用户

登录到Azure Active Directory管理中心仪表盘，然后选择您的AD，如图所示。



选择Users，点击New User，根据需要配置User name、Name和Initial Password。单击Create，如图所示。

### 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. 创建Azure AD组


选择组。单击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

[Add filters](#)

 This page includes previews available for your evaluation. [View previews](#) →

将组类型保留为Security。如图所示，配置Group name。

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. 将Azure AD用户分配给组

单击No members selected。选择用户，然后点击选择。单击Create以创建分配有用户的组。



# Add members



Search ⓘ



mck

mck@gdplab2021.onmicrosoft.com

## Selected items

No items selected

请注意Group Object id，在此屏幕中，ISE Admin Group的值为576c60ec-c0b6-4044-a8ec-d395b1475d6e（如图所示）。

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

## 4. 创建Azure AD Enterprise应用程序

在AD下，选择Enterprise Applications，然后单击New application。

Azure Active Directory admin center

Dashboard > Default Directory > Enterprise applications

### Enterprise applications | All applications

Default Directory - Azure Active Directory

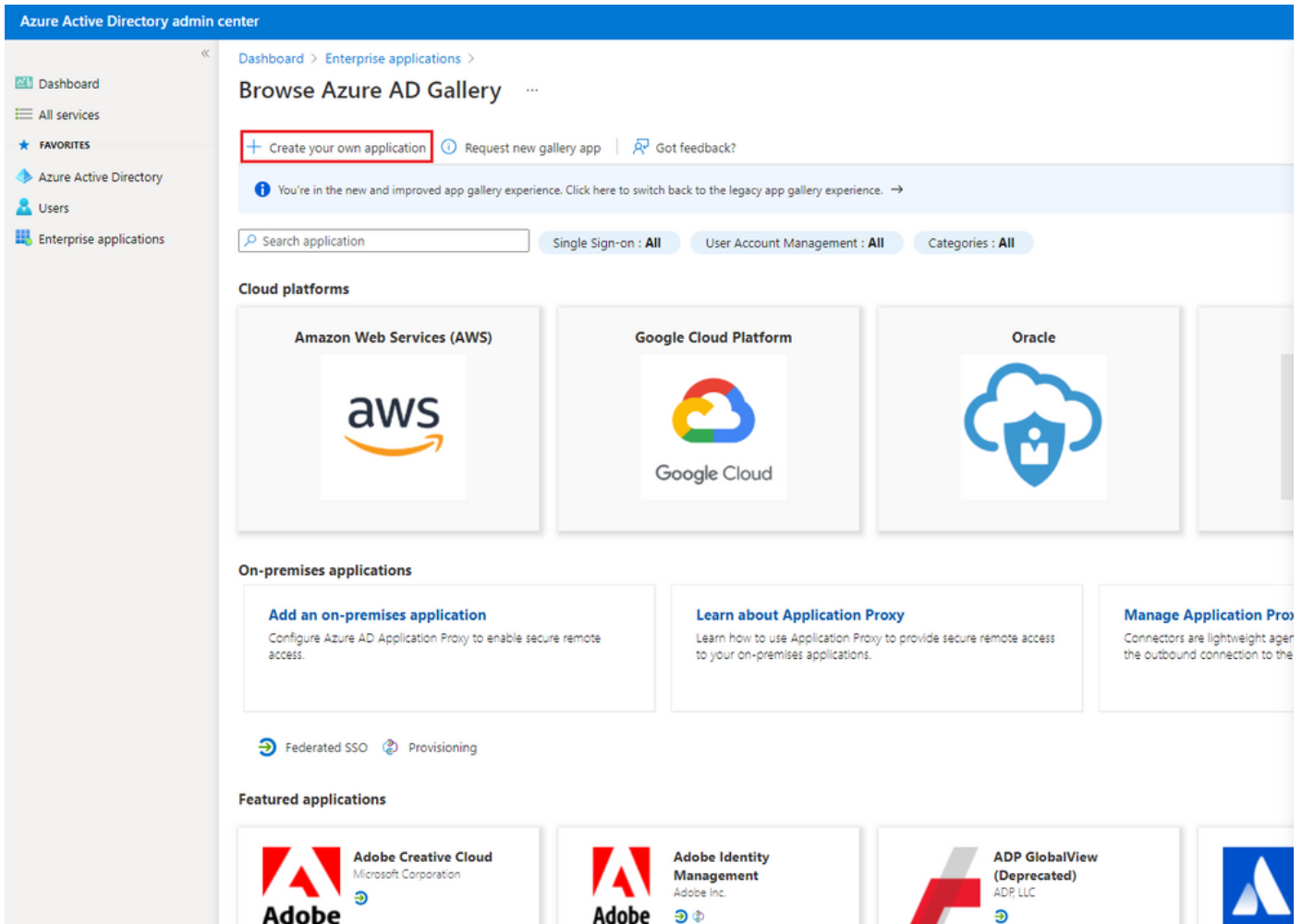
+ New application | Columns | Preview features | Got feedback?

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.

选择Create your own application。



输入应用程序的名称，然后选择Integrate any other application you not found in the gallery(Non-gallery)(集成在图库（非图库）中找不到的所有其他应用程序)单选按钮，然后单击Create按钮（如图所示）。

# Create your own application



What's the name of your app?

What are you looking to do with your application?

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

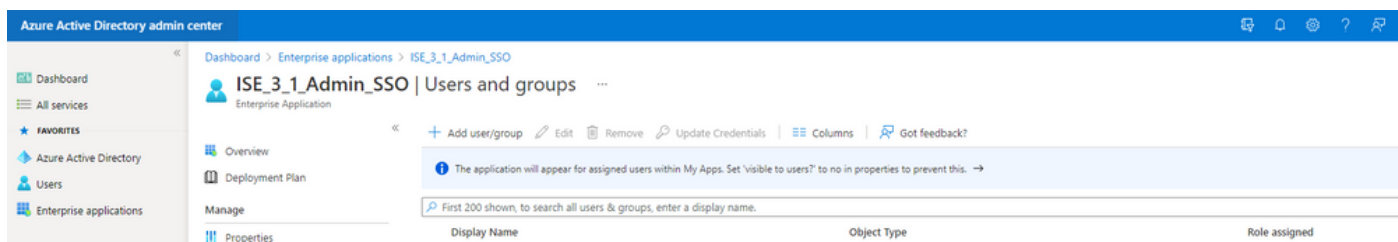
Create

## 5. 将组添加到应用程序

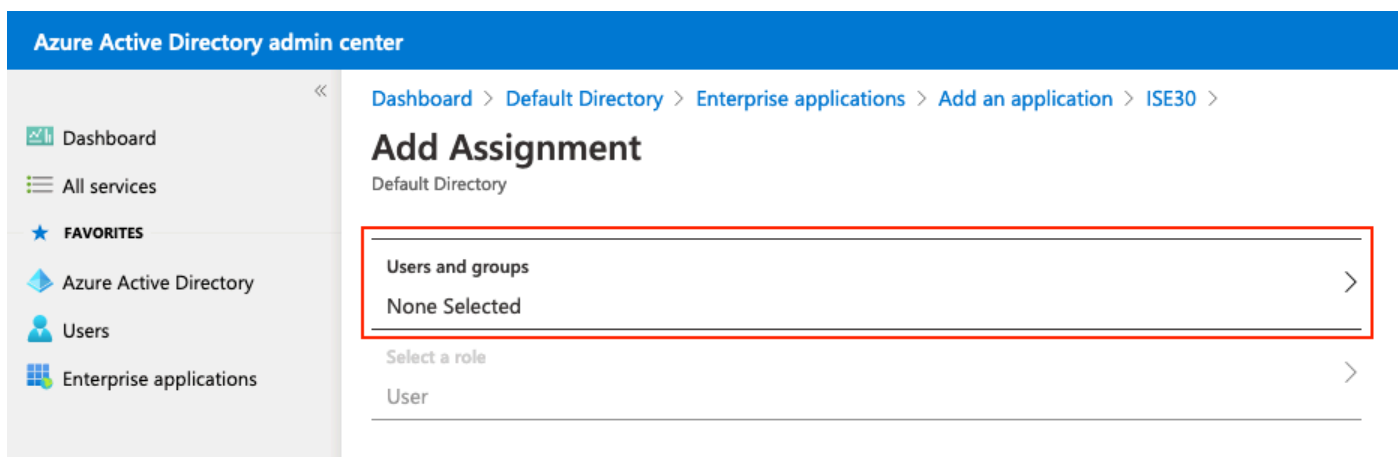
选择分配用户和组。

The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains navigation options like Dashboard, All services, Favorites, Azure Active Directory, Users, and Enterprise applications. The main content area displays the 'Overview' page for the application 'ISE\_3\_1\_Admin\_SSO'. Under the 'Properties' section, the Name, Application ID, and Object ID are listed. The 'Getting Started' section contains two tasks: '1. Assign users and groups' (highlighted with a red box) and '2. Set up single sign on'. The first task includes a description and a link to 'Assign users and groups'.


单击Add user/group。



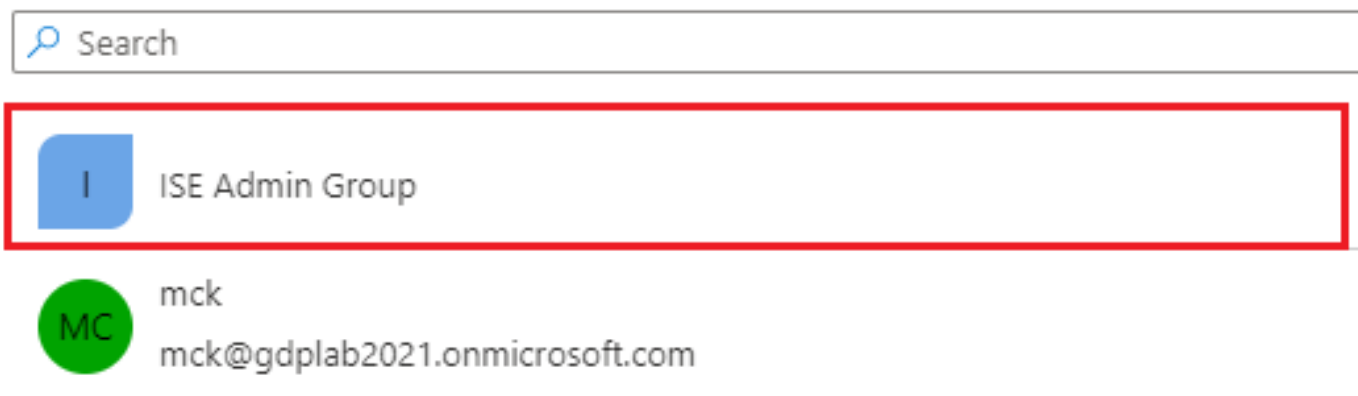
点击用户和组。



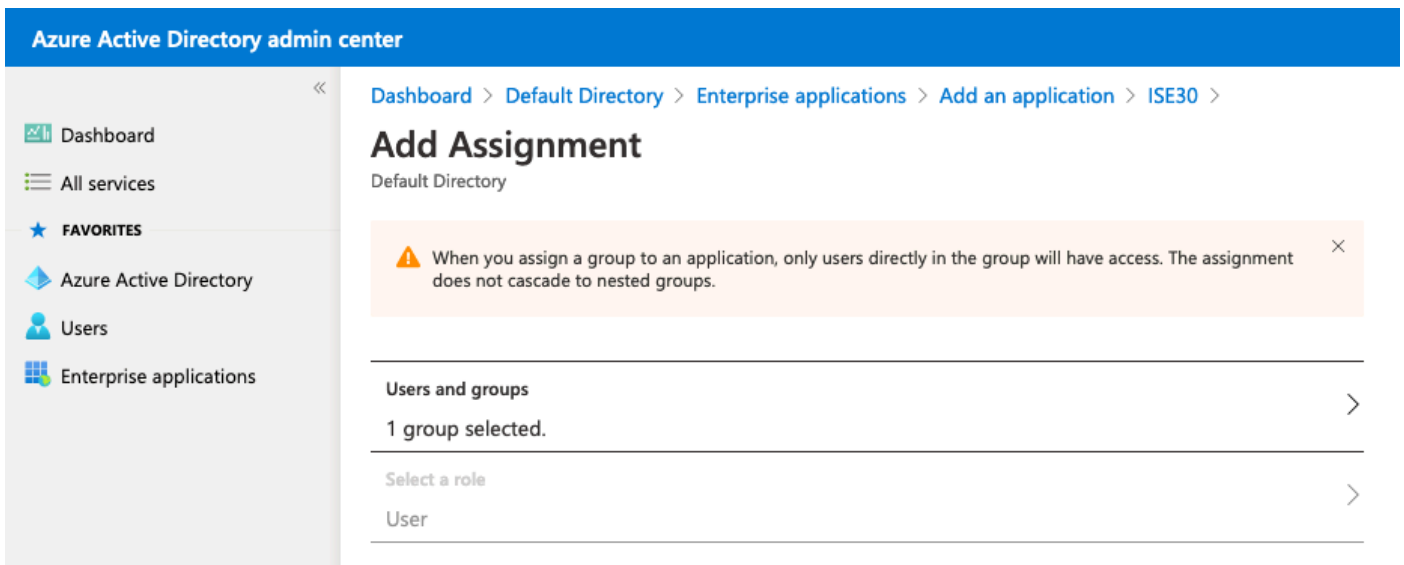
选择之前配置的组，然后点击选择。

 注意：选择获得预期访问权限的正确用户或组，因为此处提到的用户和组在设置完成后即可获得ISE的访问权限。

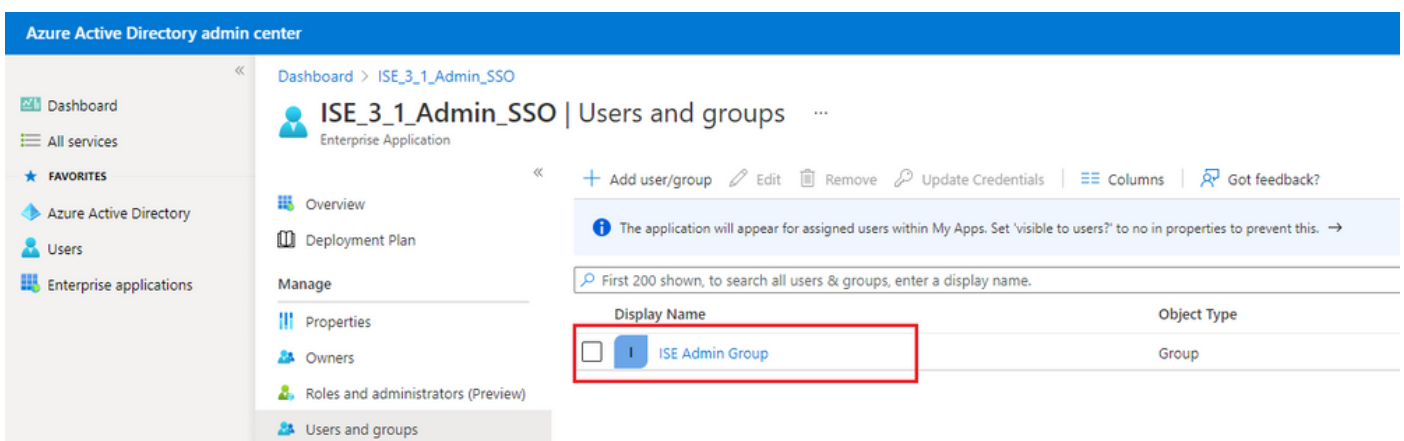
## Users and groups



选择组后，单击Assign。

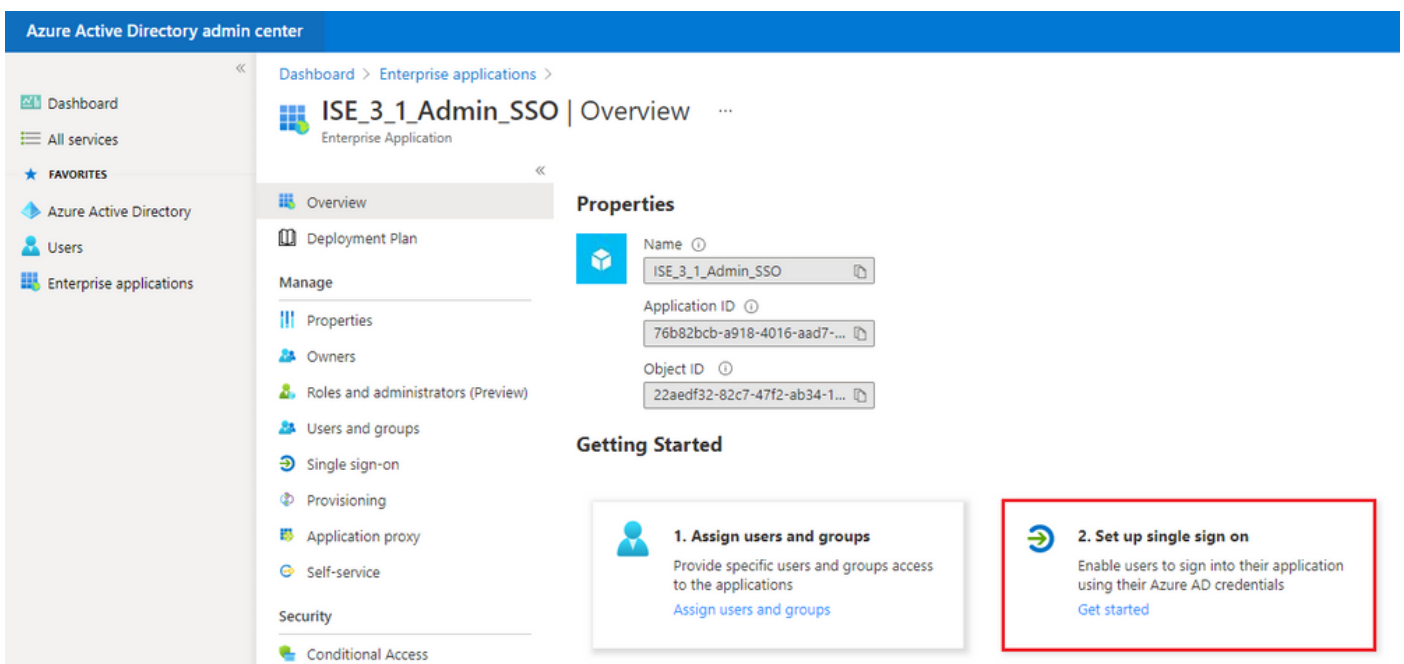


因此，已配置应用的用户和组菜单会填充所选组。

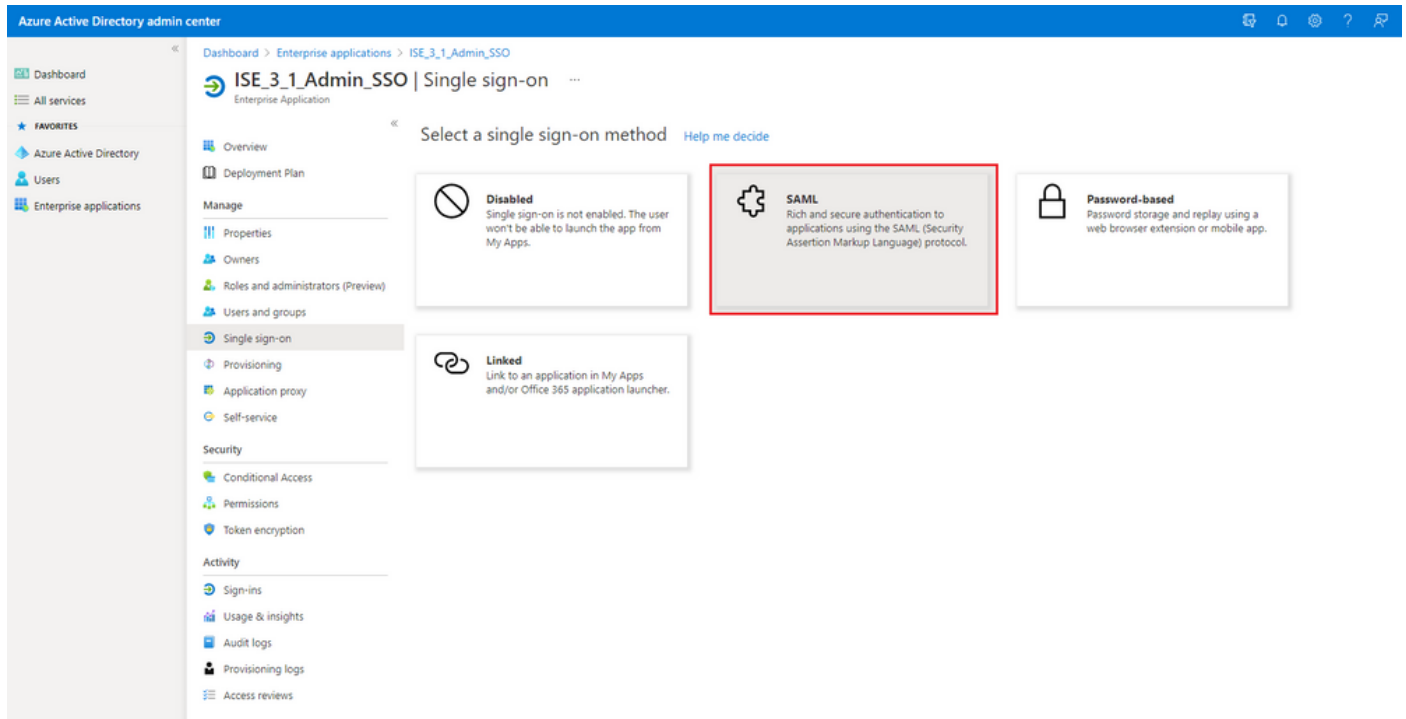


## 6. 配置 Azure AD Enterprise 应用程序

导航回您的应用程序，然后单击 Set up single sign on。



在下一个屏幕中选择SAML。



点击基本SAML配置旁边的编辑。

## Set up Single Sign-On with SAML

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


**1** Basic SAML Configuration Edit

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

**2** User Attributes & Claims Edit

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

使用步骤Export Service Provider Information中XML文件中的entityID值填充标识符(Entity ID)。使用AssertionConsumerService中的Locations 值填充Reply URL(Assertion Consumer Service URL)。 Click Save.

 注意：回复URL用作传递列表，允许某些URL在重定向到IdP页面时用作源。

## Basic SAML Configuration





 Save

### Identifier (Entity ID) \*

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

Default



 

### Reply URL (Assertion Consumer Service URL) \*

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

Default

### Sign on URL

### Relay State

### Logout Url

## 7. 配置Active Directory组属性

要返回先前配置的组属性值，请点击用户属性和领款申请旁边的编辑。

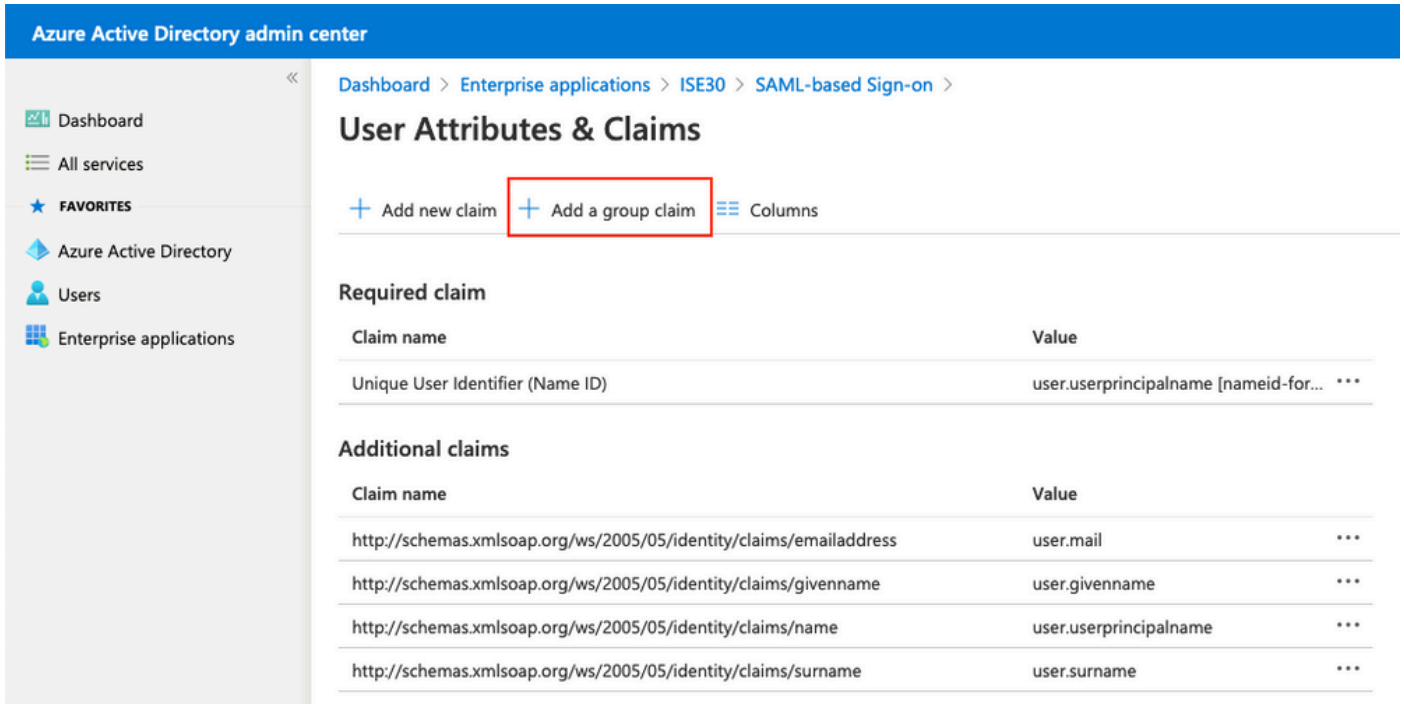


## User Attributes & Claims

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



单击Add a group claim。



Azure Active Directory admin center

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 ***           |

选择Security groups，然后单击Save。在Source attribute下拉菜单中选择Group ID。选中此复选框可自定义组声明的名称，并输入名称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 ⓘ

请记住该组的领款申请名称。在本例中，它是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. 下载Azure联合身份验证元数据XML文件

在SAML签名证书中，单击Download对联合元数据XML。

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

## 第三步：将元数据从Azure Active Directory上载到ISE

导航到管理>身份管理>外部身份源 > SAML Id提供程序> [您的SAML提供程序]。

将选项卡切换到Identity Provider Config，然后单击Browse。从下载Azure联合元数据XML步骤中选择联合元数据XML文件，然后单击保存。

## External Identity Sources

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

Identity Provider List &gt; 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>

### Sianina 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... |

#### 第四步：在ISE上配置SAML组

切换到Groups选项卡，然后将Claim name的值从Configure Active Directory Group attribute粘贴到Group Membership Attribute中。

## External Identity Sources

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

Identity Provider List &gt; Azure

## SAML Identity Provider

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

### Groups

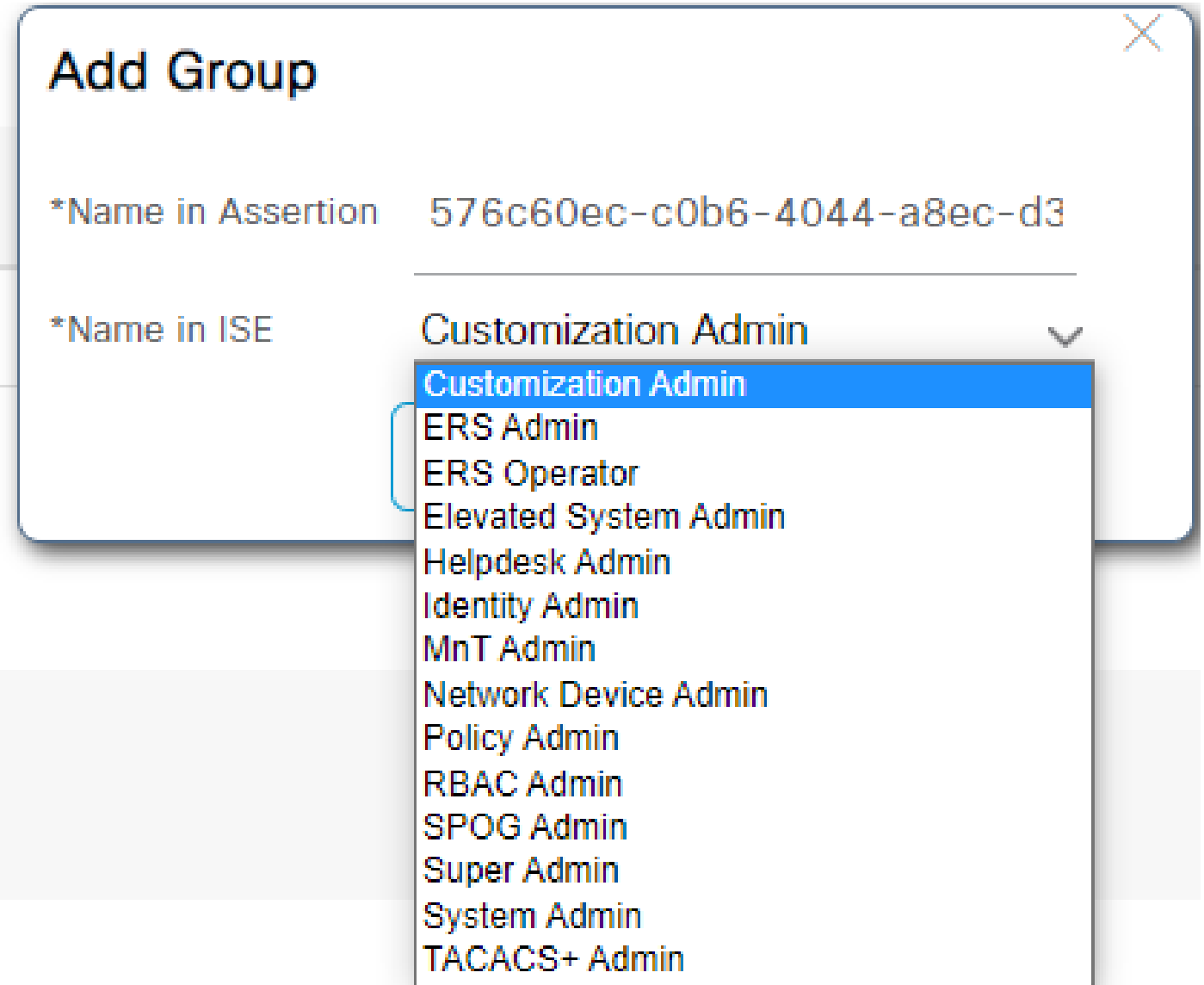
Group Membership Attribute  ⓘ

Name in Assertion  Name in ISE

单击Add。使用在将Azure Active Directory用户分配到组中捕获的ISE管理组的组对象ID值填充Assertion中的名称。

使用下拉列表配置ISE中的名称，并在ISE上选择适当的组。在本示例中，使用的组是Super Admin。Click OK.Click Save.

这会在Azure中的组和ISE上的组名称之间创建映射。



### ( 可选 ) 第5步。配置RBAC策略

从上一步开始，可在ISE上配置许多不同类型的用户访问级别。

要编辑基于角色的访问控制策略(RBAC)，请导航到Administration > System > Admin Access > Authorization > Permissions > RBAC Policies并根据需要进行配置。


此映像是对示例配置的参考。

## ▼ RBAC Policies

| Rule Name   | Admin Groups                      | Permissions   |
|---|-----------------------------------|---|
| <input checked="" type="checkbox"/> <input type="checkbox"/> Customization Admin Policy | If <u>Customization Admin</u> +   | then <u>Customization Admin Menu ...</u> + <a href="#">Actions</a> ▼  |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Elevated System Admin Poli | If <u>Elevated System Admin</u> + | then <u>System Admin Menu Access...</u> + <a href="#">Actions</a> ▼   |
| <input checked="" type="checkbox"/> <input type="checkbox"/> ERS Admin Policy           | If <u>ERS Admin</u> +             | then <u>Super Admin Data Access</u> + <a href="#">Actions</a> ▼       |
| <input checked="" type="checkbox"/> <input type="checkbox"/> ERS Operator Policy        | If <u>ERS Operator</u> +          | then <u>Super Admin Data Access</u> + <a href="#">Actions</a> ▼       |
| <input checked="" type="checkbox"/> <input type="checkbox"/> ERS Trustsec Policy        | If <u>ERS Trustsec</u> +          | then <u>Super Admin Data Access</u> + <a href="#">Actions</a> ▼       |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Helpdesk Admin Policy      | If <u>Helpdesk Admin</u> +        | then <u>Helpdesk Admin Menu Access</u> + <a href="#">Actions</a> ▼    |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Identity Admin Policy      | If <u>Identity Admin</u> +        | then <u>Identity Admin Menu Access...</u> + <a href="#">Actions</a> ▼ |
| <input checked="" type="checkbox"/> <input type="checkbox"/> MnT Admin Policy           | If <u>MnT Admin</u> +             | then <u>MnT Admin Menu Access</u> + <a href="#">Actions</a> ▼         |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Network Device Policy      | If <u>Network Device Admin</u> +  | then <u>Network Device Menu Acce...</u> + <a href="#">Actions</a> ▼   |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Policy Admin Policy        | If <u>Policy Admin</u> +          | then <u>Policy Admin Menu Access ...</u> + <a href="#">Actions</a> ▼  |
| <input checked="" type="checkbox"/> <input type="checkbox"/> RBAC Admin Policy          | If <u>RBAC Admin</u> +            | then <u>RBAC Admin Menu Access ...</u> + <a href="#">Actions</a> ▼    |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Read Only Admin Policy     | If <u>Read Only Admin</u> +       | then <u>Super Admin Menu Access ...</u> + <a href="#">Actions</a> ▼   |
| <input checked="" type="checkbox"/> <input type="checkbox"/> SPOG Admin Policy          | If <u>SPOG Admin</u> +            | then <u>Super Admin Data Access</u> + <a href="#">Actions</a> ▼       |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Super Admin Policy         | If <u>Super Admin</u> +           | then <u>Super Admin Menu Access ...</u> + <a href="#">Actions</a> ▼   |
| <input checked="" type="checkbox"/> <input type="checkbox"/> Super Admin_Azure          | If <u>Super Admin</u> +           | then <u>Super Admin Menu Access ...</u> + <a href="#">Actions</a> ▼   |
| <input checked="" type="checkbox"/> <input type="checkbox"/> System Admin Policy        | If <u>System Admin</u> +          | then <u>System Admin Menu Access...</u> + <a href="#">Actions</a> ▼   |
| <input checked="" type="checkbox"/> <input type="checkbox"/> TACACS+ Admin Policy       | If <u>TACACS+ Admin</u> +         | then <u>TACACS+ Admin Menu Acc...</u> + <a href="#">Actions</a> ▼     |

## 验证

确认您的配置工作正常。

 **注意：** Azure测试功能中的SAML SSO登录测试不起作用。SAML请求必须由ISE发起，Azure SAML SSO才能正常工作。

打开ISE GUI登录提示屏幕。系统将显示一个使用SAML登录的新选项。

1. 访问您的ISE GUI登录页面，然后点击使用SAML登录。



# Identity Services Engine

Intuitive network security

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

2.系统会将您重定向到Microsoft登录屏幕。如图所示，输入映射到ISE的组中的帐户的用户名凭证，然后点击下一步，如图所示。



# Sign in

mck@gdplab2021.onmicrosoft.com

---

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

Next

3.输入用户的密码，然后单击登录。





← mck@gdplab2021.onmicrosoft.com

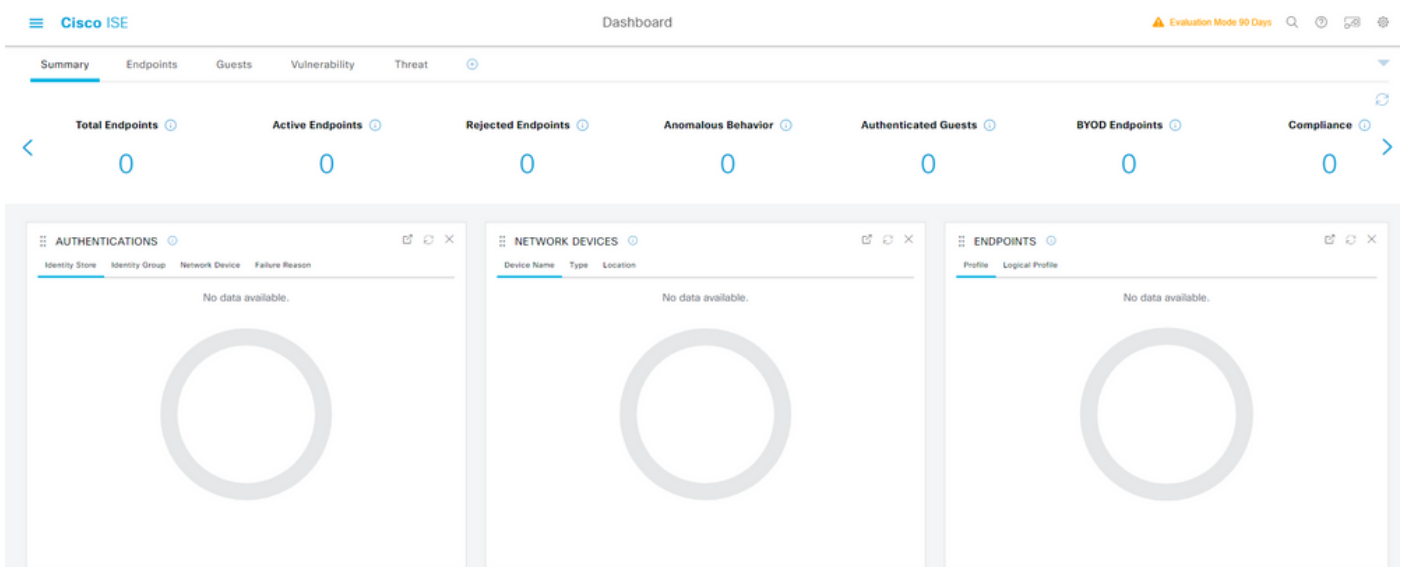
# Enter password

••••••••••

[Forgot my password](#)

Sign in

4.现在您将被重定向到ISE应用仪表板，根据之前配置的ISE组配置相应的权限，如图所示。



## 故障排除

本部分提供的信息可用于对配置进行故障排除。

## 常见问题

了解在浏览器和Azure Active Directory之间处理SAML身份验证至关重要。因此，您可以直接从身份提供程序(Azure)获取与身份验证相关的错误，其中ISE参与尚未启动。

问题1.输入凭证后出现“您的帐户或密码不正确”错误。此时，ISE尚未接收用户数据，此时进程仍采用IdP(Azure)。

最可能的原因是帐户信息不正确或密码不正确。要解决此问题：重置密码或为该帐户提供正确的密码，如图所示。



← 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

问题 2.用户不属于应该允许访问SAML SSO的组。与前面的情况类似，ISE尚未收到用户数据，此时进程仍采用IdP(Azure)。

要解决此问题：验证Add group to the Application配置步骤是否正确执行，如图所示。



## 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.

问题 3. ISE应用服务器无法处理SAML登录请求。当从身份提供程序Azure而不是服务提供程序ISE发起SAML请求时，会发生此问题。从Azure AD测试SSO登录不起作用，因为ISE不支持身份提供程序发起的SAML请求。



## 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                  | 824F4B847B350C93DE3D59EC87EE4C8   |
| Expiration                  | 7/19/2024, 12:16:24 PM  |
| Notification Email          | chandandemo@outlook.com   |
| App Federation Metadata Url | <a href="https://login.microsoftonline.com/182900ce-e99d-4403-8100-41d857100000/...">https://login.microsoftonline.com/182900ce-e99d-4403-8100-41d857100000/...</a> |
| Certificate (Base64)        | <a href="#">Download</a>  |
| Certificate (Raw)           | <a href="#">Download</a>  |
| Federation Metadata XML     | <a href="#">Download</a>  |

4

#### Set up ISE\_3\_1\_Admin\_SSO

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

|                     |   |
|---------------------|---|
| Login URL           | <a href="https://login.microsoftonline.com/182900ce-e99d-4403-8100-41d857100000/...">https://login.microsoftonline.com/182900ce-e99d-4403-8100-41d857100000/...</a> |
| Azure AD Identifier | <a href="https://sts.windows.net/182900ce-e99d-4403-8100-41d857100000/">https://sts.windows.net/182900ce-e99d-4403-8100-41d857100000/</a>                           |
| Logout URL          | <a href="https://login.microsoftonline.com/182900ce-e99d-4403-8100-41d857100000/...">https://login.microsoftonline.com/182900ce-e99d-4403-8100-41d857100000/...</a> |

[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-f993d8f4cb0  
Timestamp: 2018-03-06T23:54:10Z  
Message: Error AADSTSXXXXX

[Get resolution guidance](#)

问题 4. ISE在登录尝试后显示“访问被拒绝”错误。当之前在Azure企业应用中创建的组的声明名称在ISE中不匹配，会发生此错误。

要解决此问题：确保Azure和ISE中“SAML身份提供程序组”(SAML Identity Provider Groups)选项卡下的组声明名称相同。有关详细信息，请参阅本文档的使用Azure AD配置SAML SSO部分下的步骤2.7.和4。



# Identity Services Engine

Intuitive network security



Access Denied

Log In With SAML

Log In With ISE

[English](#) | [日本語](#)

[Problems logging in?](#)

## 排除ISE故障

必须在ISE上更改此处的组件的日志级别。导航到操作>故障排除>调试向导>调试日志配置。

| 组件名称 | 日志级别 | 日志文件名 |
|------|------|-------|
|------|------|-------|

|          |    |             |
|----------|----|-------------|
| 门户       | 调试 | guest.log   |
| opensaml | 调试 | ise-psc.log |
| saml     | 调试 | ise-psc.log |

## SAML登录和组声明名称不匹配的日志

一组调试，显示流执行时的声明名称不匹配故障排除场景(ise-psc.log)。

 注：注意粗体项目。为清楚起见，已将日志缩短。

1.用户从ISE管理员页面重定向到IdP URL。

<#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.从浏览器接收SAML响应。

<#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 13:48:27,182 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.saml2.binding.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.ws.message.decode

2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decode

opensaml.common.binding.decoding.BaseSAMLMessageDecoder -:::- Intended message destination endpoint: [https://schemas.xmlsoap.org/ws/2005/05/identity/](#)

2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decode

2021-07-29 13:48:27,183 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAML

2021-07-29 13:48:27,184 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10][] opensaml.common.binding.decode

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

### 3.属性 ( 断言 ) 分析已启动。

<#root>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### 4.收到组属性，其值为576c60ec-c0b6-4044-a8ec-d395b1475d6e，签名验证。

```

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

```

## 5. RBAC授权验证。

```
<#root>
```

```

*****Rbac Log Summary for user samUser*****
2021-07-29 13:48:27,360 INFO [admin-http-pool50] [] com.cisco.ise.util.RBACUtil -:::- Populating cache
2021-07-29 13:48:27,368 ERROR [admin-http-pool50] [] cpm.admin.infra.utils.PermissionEvaluationUtil -:::-
java.lang.NullPointerException
2021-07-29 13:48:27,369 INFO [admin-http-pool50] [] cpm.admin.infra.action.LoginAction -:::- In Login
2021-07-29 13:48:27,369 INFO [admin-http-pool50] [] cpm.admin.infra.action.LoginAction -:::- In Login

```



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

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

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

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。