

# 透過Azure AD的SAML SSO配置ISE 3.1管理員登入流

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[採用元件](#)

### [背景資訊](#)

[辨識提供者\(IdP\)：](#)

[服務提供者\(SP\)：](#)

[SAML](#)

[SAML斷言](#)

### [概要流程圖](#)

### [配置與Azure AD的SAML SSO整合](#)

#### [步驟 1. 在ISE上配置SAML身份提供程式](#)

- [1. 將Azure AD配置為外部SAML標識源](#)
- [2. 配置ISE身份驗證方法](#)
- [3. 導出服務提供者資訊](#)

#### [步驟 2. 配置Azure AD IdP設定](#)

- [1. 建立Azure AD使用者](#)
- [2. 建立Azure AD組](#)
- [3. 將Azure AD使用者分配到組](#)
- [4. 建立Azure AD Enterprise應用程式](#)
- [5. 將群組新增至應用程式](#)
- [6. 配置Azure AD Enterprise應用程式](#)
- [7. 配置Active Directory組屬性](#)
- [8. 下載Azure Federation後設資料XML檔案](#)

#### [步驟 3. 從Azure Active Directory上傳後設資料到ISE](#)

#### [步驟 4. 在ISE上配置SAML組](#)

[\(可選\) 步驟5. 配置RBAC策略](#)

### [驗證](#)

### [疑難排解](#)

[常見問題](#)

[排除ISE故障](#)

[具有SAML登入名和不匹配的組宣告名稱的日誌](#)

---

## 簡介

本文檔介紹如何配置與外部身份提供程式(例如Azure Active Directory (AD))的Cisco ISE 3.1 SAML SSO整合。

# 必要條件

## 需求

思科建議您瞭解以下主題：

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

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

1. 思科ISE 3.1
2. Azure AD

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

期限：

辨識提供者(IdP)：

用於驗證和宣告對請求的資源（服務提供程式）的使用者標識和訪問許可權的授權Azure AD。

服務提供商(SP)：

使用者要訪問的託管資源或服務（ISE應用伺服器）。

## SAML

安全斷言標籤語言(SAML)是允許IdP向SP傳遞授權憑據的開放標準。

SAML事務使用可擴展標籤語言(XML)實現身份提供方和服務提供商之間的標準化通訊。

SAML是使用者身份身份驗證與使用服務的授權之間的鏈路。

## SAML斷言

SAML斷言是標識提供程式傳送到包含使用者授權的服務提供商的XML文檔。

有三種不同型別SAML斷言-身份驗證、屬性和授權決策。

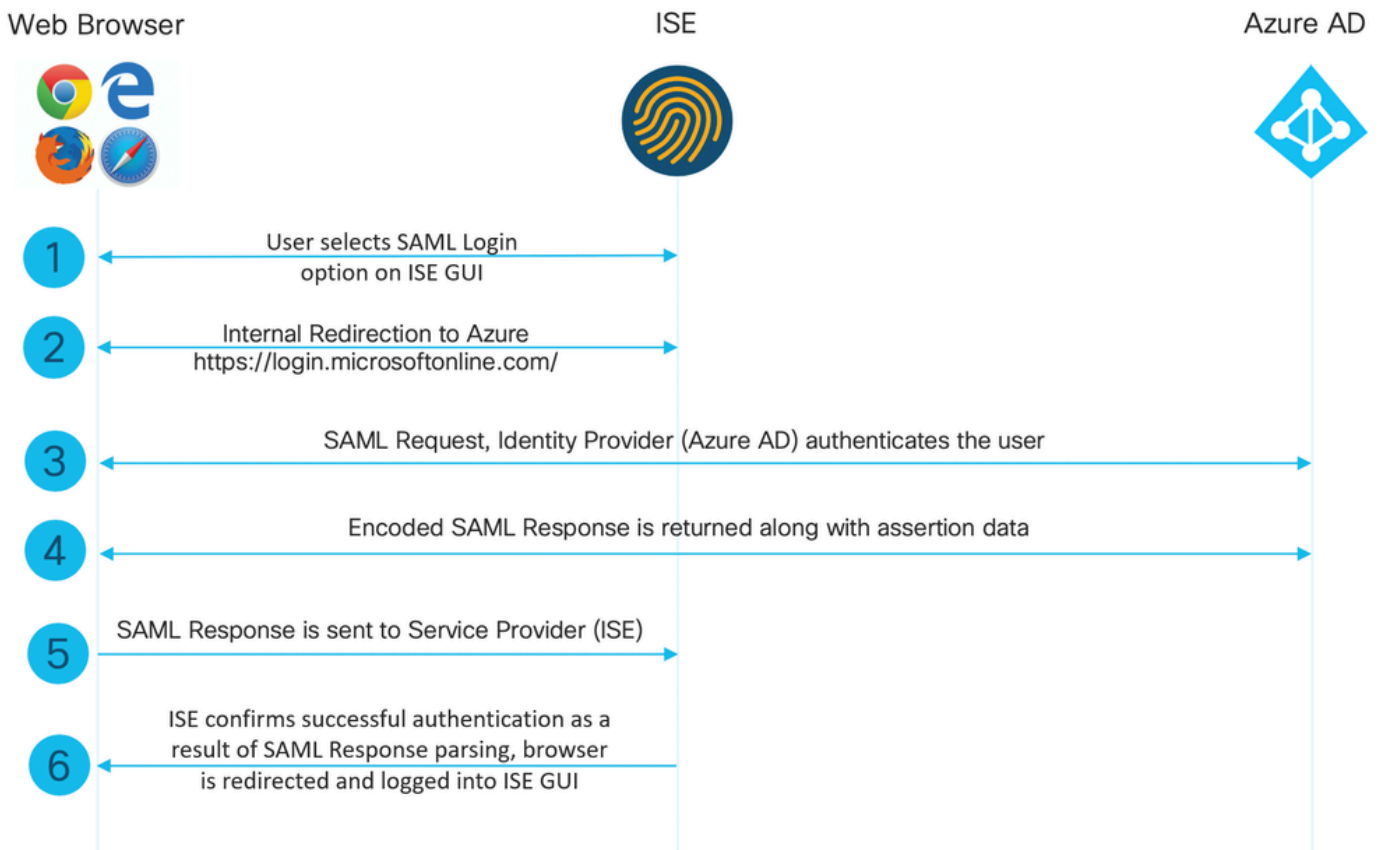
- 身份驗證斷言可證明使用者的身份，並提供使用者登入的時間以及他們使用的身份驗證方法（例如，Kerberos，雙因素）
- 歸屬斷言將SAML屬性（提供有關使用者資訊的特定資料）傳遞給服務提供商。
- 授權決策斷言宣告使用者是否被授權使用服務，或者如果標識提供者由於密碼失敗或缺少對服務的許可權而拒絕他們的請求。

## 概要流程圖

SAML的工作方式是在身份提供程式、Azure AD和服務提供程式ISE之間傳遞有關使用者、登入和屬性的資訊。

每個使用者使用身份提供程式登入一次單一登入(SSO)，然後Azure AD提供程式在使用者嘗試訪問這些服務時將SAML屬性傳遞給ISE。

ISE從Azure AD請求授權和身份驗證，如圖所示。



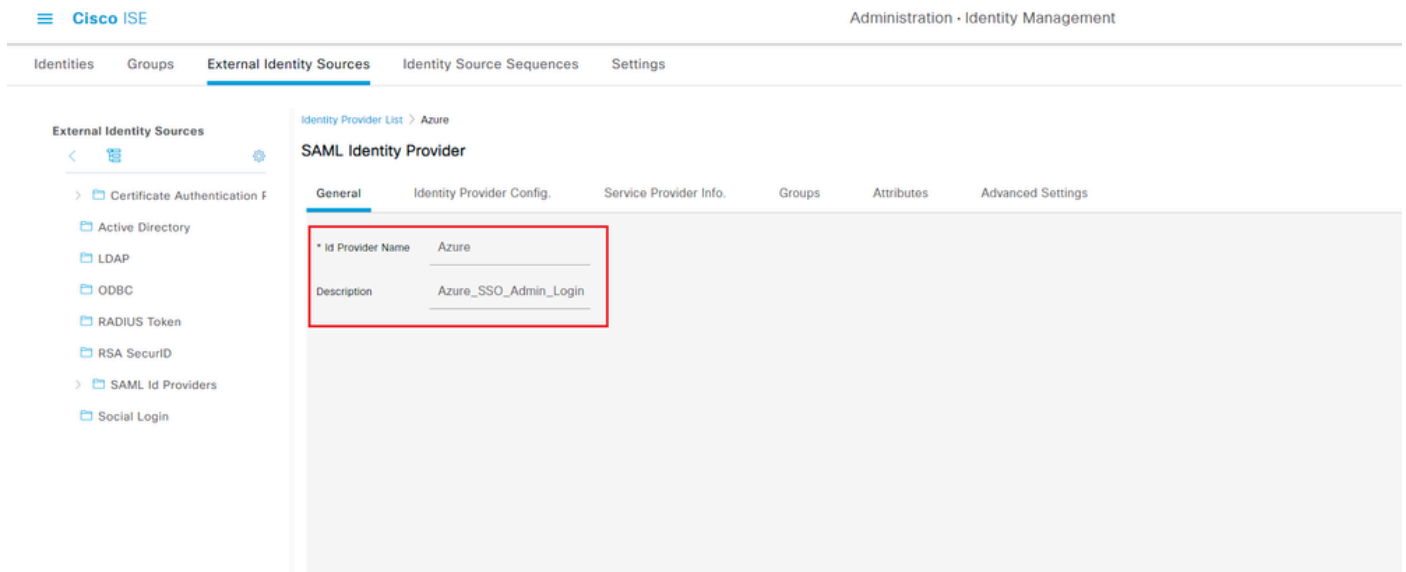
## 配置與Azure AD的SAML SSO整合

### 步驟 1. 在ISE上配置SAML身份提供程式

#### 1. 將Azure AD配置為外部SAML標識源

在ISE上，導航到管理>身份管理>外部身份源 > SAML Id提供程式，然後按一下增加按鈕。

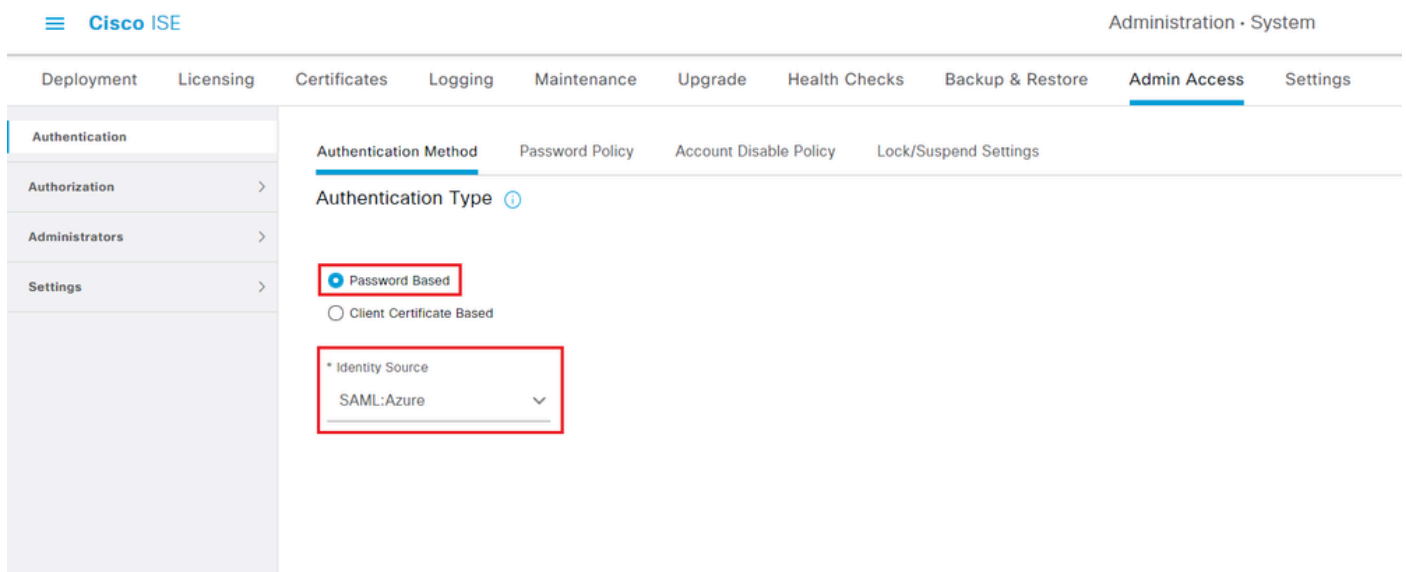
輸入Id Provider Name並按一下Submit以儲存它。Id Provider Name僅對ISE有效，如下圖所示。



## 2. 配置ISE身份驗證方法

導航到管理>系統>管理員訪問許可權>身份驗證>身份驗證方法，然後選擇基於密碼單選按鈕。

從Identity Source下拉選單選擇之前建立的所需Id Provider Name，如下圖所示。



## 3. 導出服務提供商資訊

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

將該頁籤切換到Service Provider Info，然後按一下Export按鈕，如圖所示。

## 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)

下載.xml檔案並儲存。記下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>
MIIFTjCAzagAwIBAgINAg2amS1L6NAE8FY+tzANBgkqhkiG9w0BAQwFADA1MSMwIQYDVQQDExpT
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
kVS9v4E0zwNGo7pQI8CAwEAAa9MHswIAYDVR0RBkF4IVaXN1My0xLTE5LmNrdW1hcjIuY29t
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.action">
<md:AssertionConsumerService index="1" Location="https://ise3-1-19.onmicrosoft.com:8443/portal/SSOLoginResponse.action">
</md:SPSSODescriptor>
</md:EntityDescriptor>
```

XML檔案中的相關屬性：

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

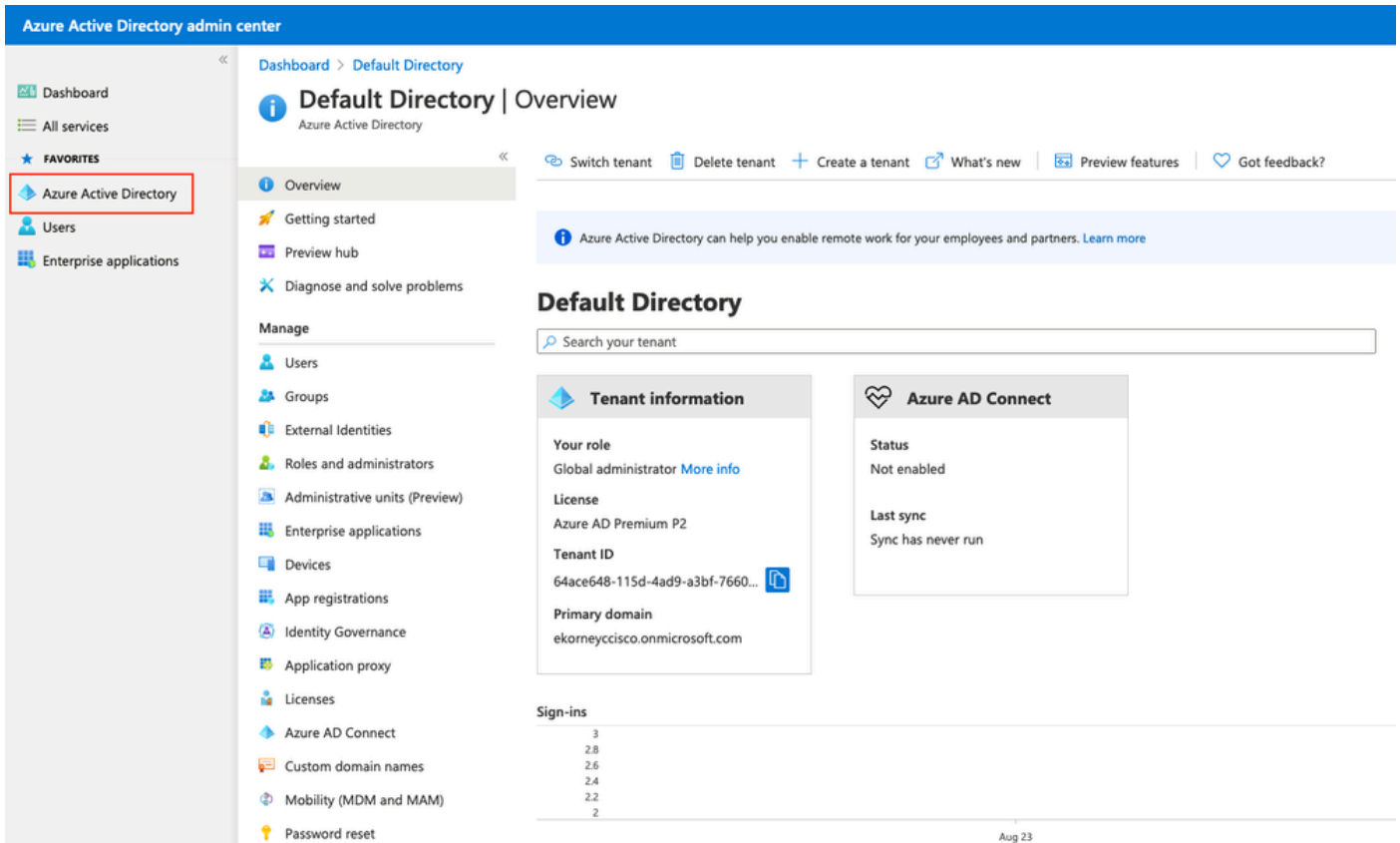
AssertionConsumerService位置="<https://10.201.232.19:8443/portal/SSOLoginResponse.action>"

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

## 步驟 2. 配置 Azure AD IdP 設定

### 1. 建立 Azure AD 使用者

登入到 Azure Active Directory 管理中心儀表板，並選擇你的 AD，如下圖所示。



選擇使用者，點選新使用者，根據需要配置使用者名稱、名稱和初始密碼。按一下 Create，如圖所

示。

## 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. 建立Azure AD組

選擇組。按一下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

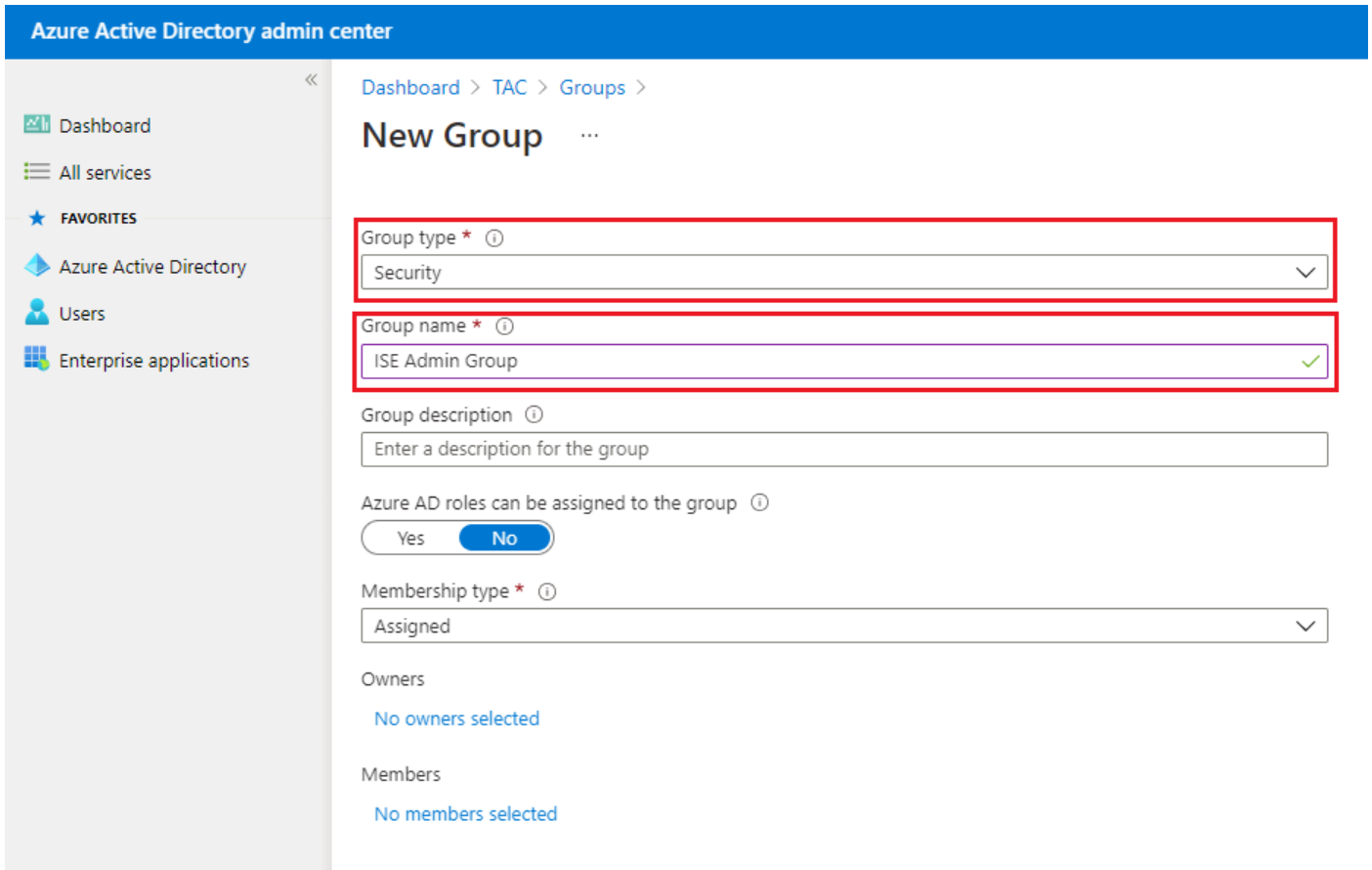


This page includes previews available for your evaluation. View previews →

Search groups

Add filters

保留Group type為Security。配置Group name，如下圖所示。



### 3. 將Azure AD使用者分配到組

按一下No members selected。選擇使用者並按一下Select。按一下Create以建立分配了使用者的組。



# Add members



Search ⓘ



mck  
mck@gdplab2021.onmicrosoft.com

## Selected items

No items selected

記下Group Object id，在此螢幕中為576c60ec-c0b6-4044-a8ec-d395b1475d6e，用於ISE管理組，如下圖所示。

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. 建立Azure AD Enterprise應用程式

在AD下，選擇Enterprise Applications並按一下New application。

Azure Active Directory admin center

Dashboard > Default Directory > Enterprise applications

### Enterprise applications | All applications

Default Directory - Azure Active Directory

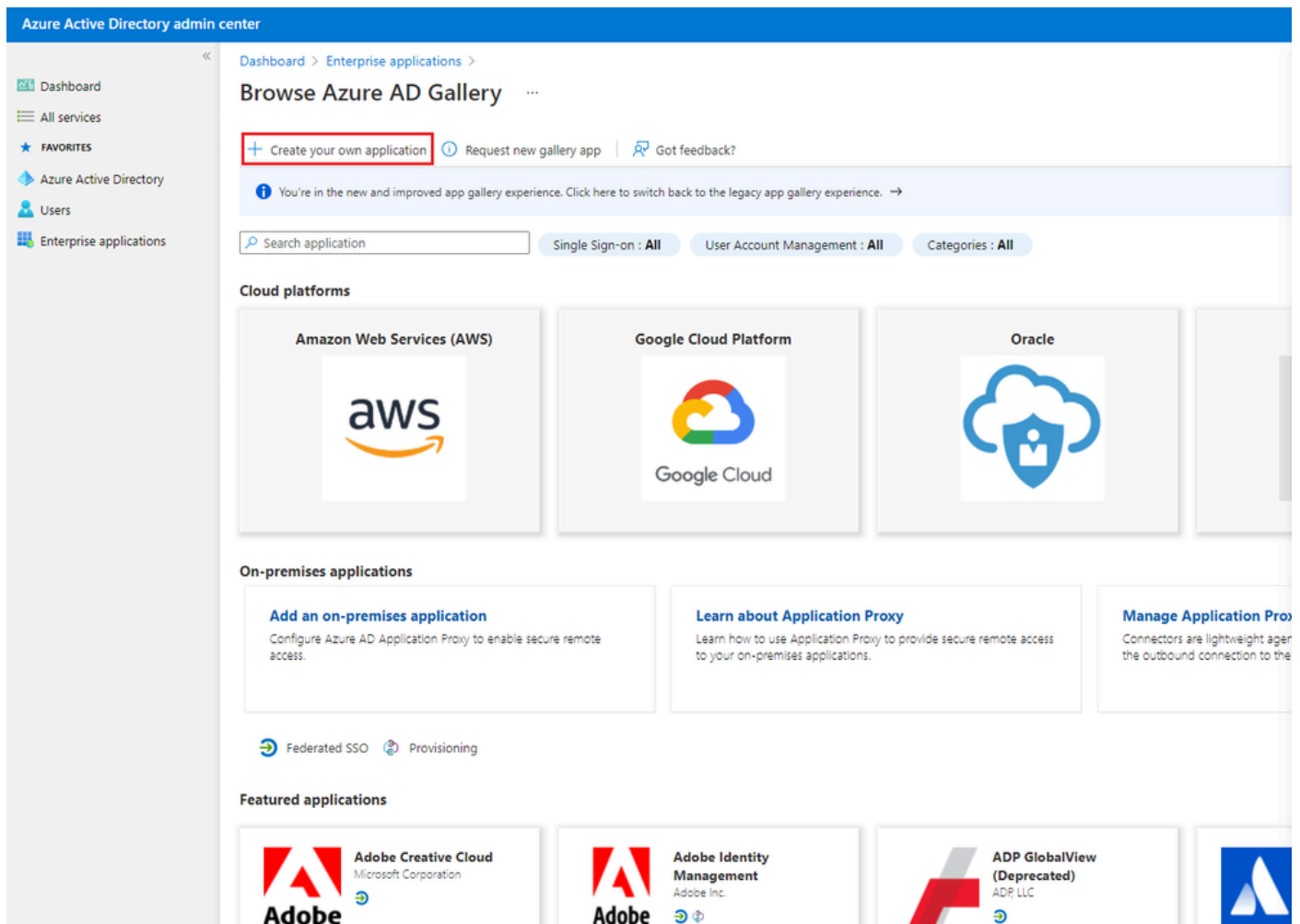
+ New application | Columns | Preview features | Got feedback?

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.

選擇Create your own application。



輸入應用程式的名稱，然後選取「整合在收藏館中找不到的任何其他應用程式（非收藏館）」圓鈕，再按一下「建立」按鈕（如圖所示）。

# 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. 將群組新增至應用程式

選擇分配使用者和組。

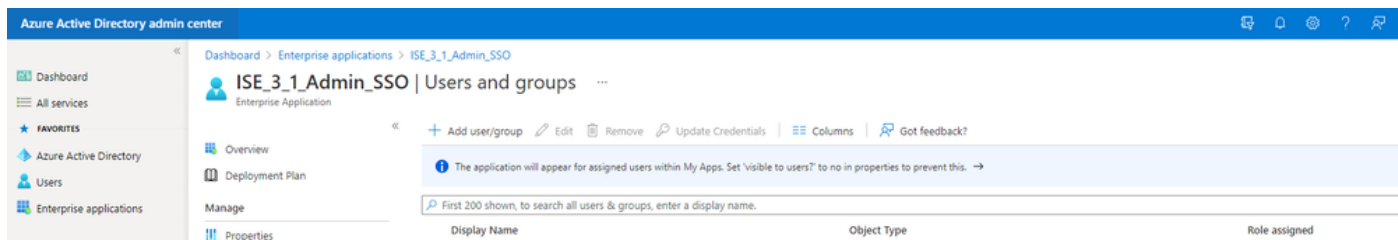
The screenshot shows the Azure Active Directory admin center interface. The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area is titled 'ISE\_3\_1\_Admin\_SSO | Overview' and includes a 'Properties' section with the following details:

- Name: ISE\_3\_1\_Admin\_SSO
- Application ID: 76b82bcb-a918-4016-aad7-...
- Object ID: 22aedf32-82c7-47f2-ab34-1...

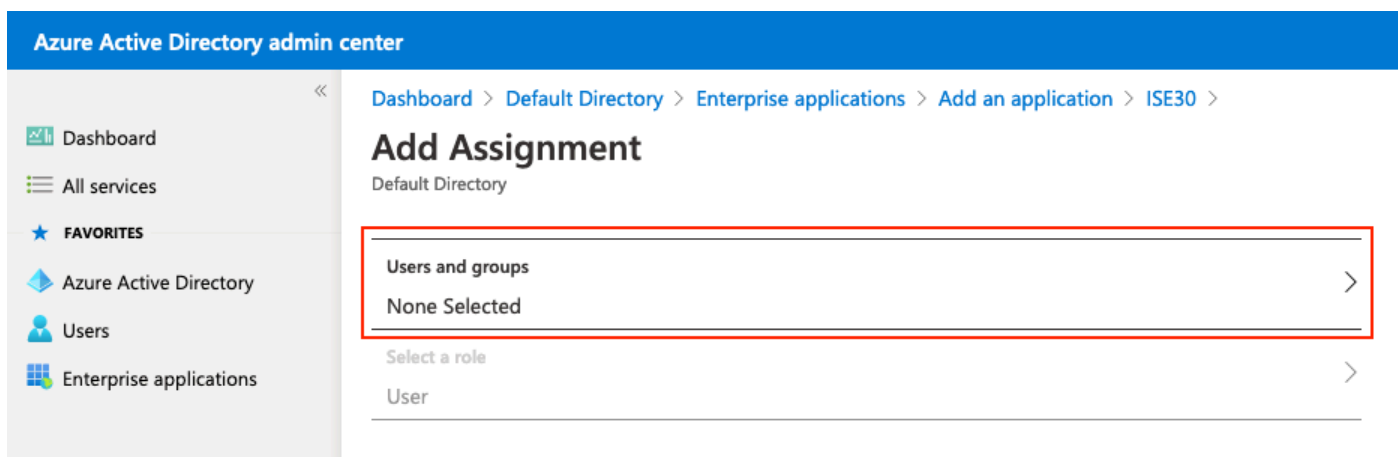
Below the properties, there is a 'Getting Started' section with two steps:

- 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](#)


按一下Add user/group。



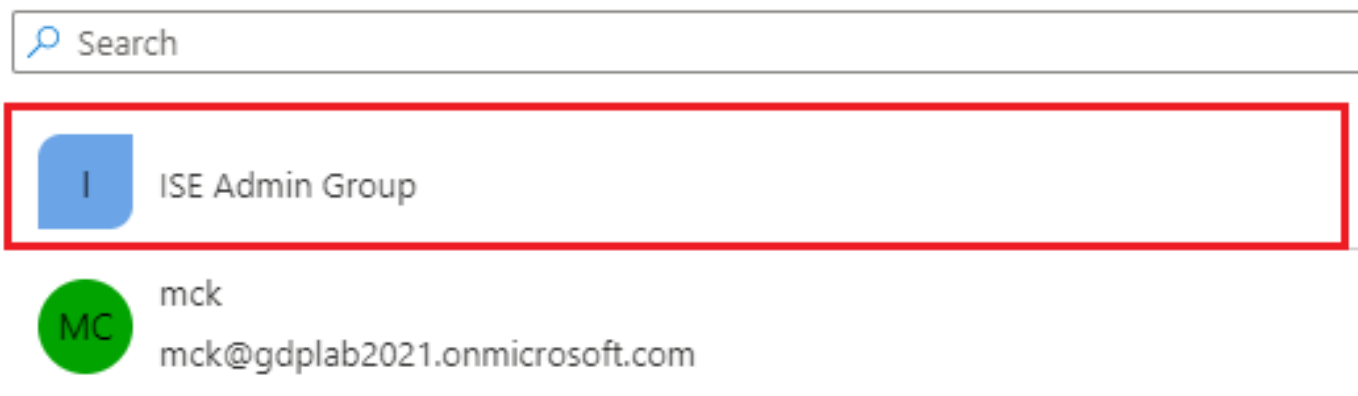
按一下Users and groups。



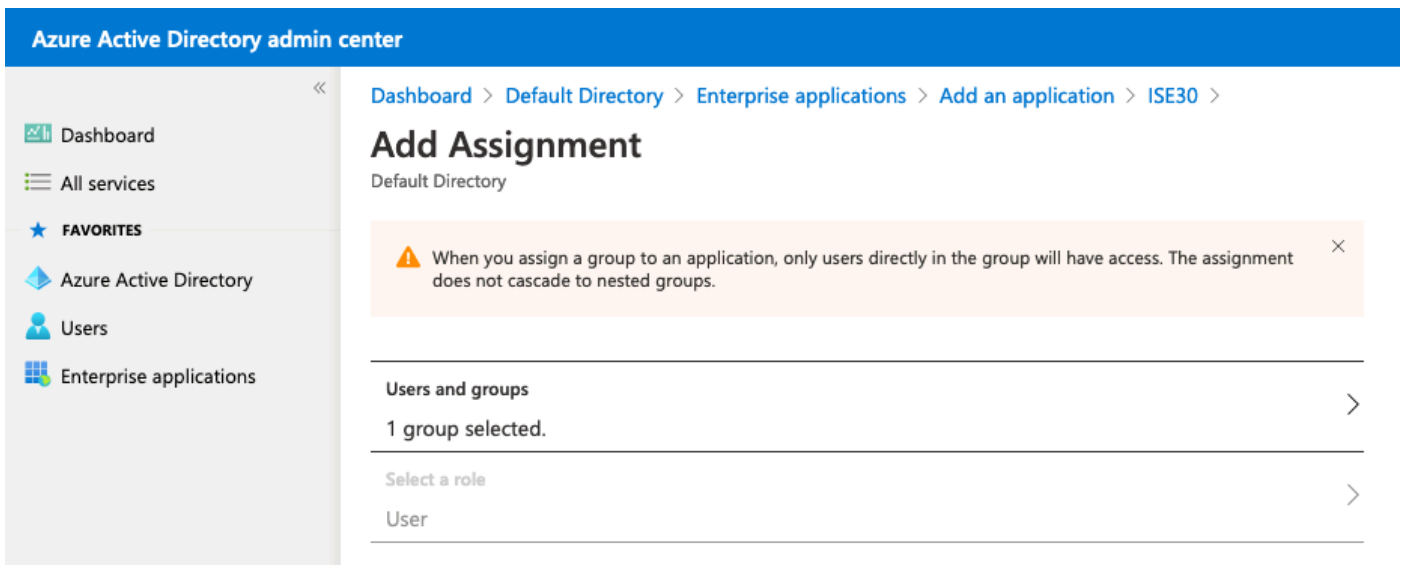
選擇先前配置的組，然後按一下選擇。

 注意：選擇獲得所需訪問許可權的正確使用者或組集，因為此處提及的使用者和組在設定完成後即可獲得ISE訪問許可權。

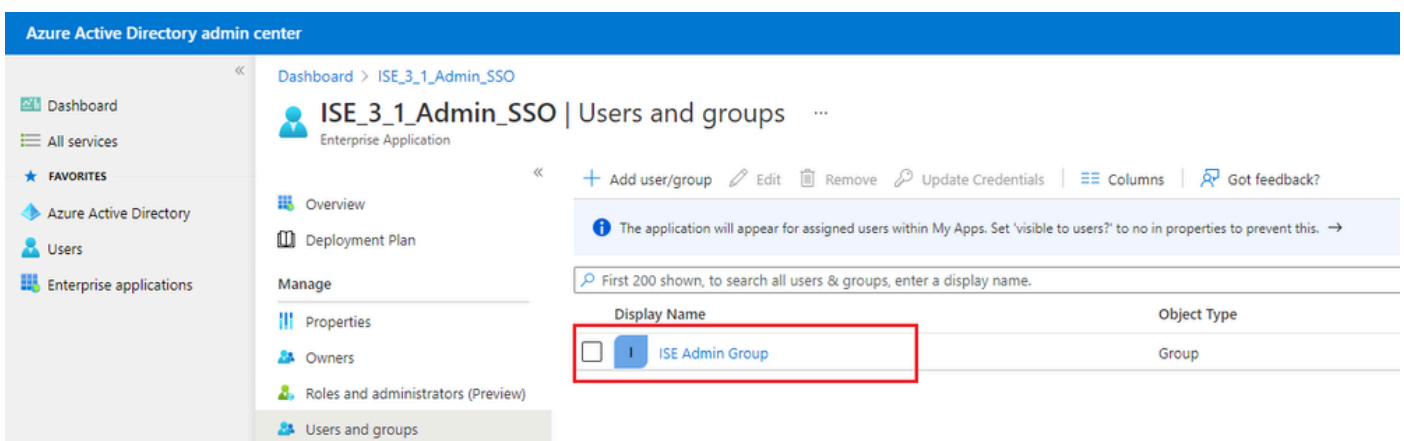
## Users and groups



選擇組後，按一下Assign。

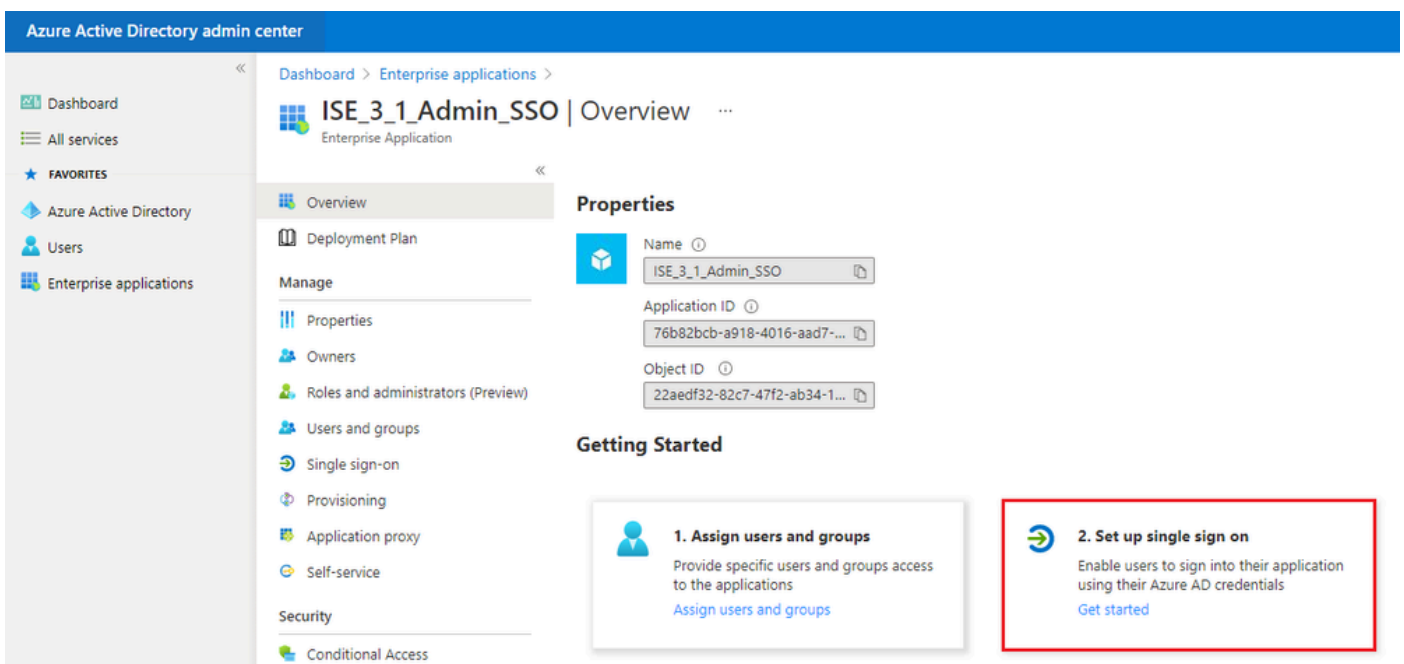


因此，配置的應用程式的使用者和組選單會填充所選的組。

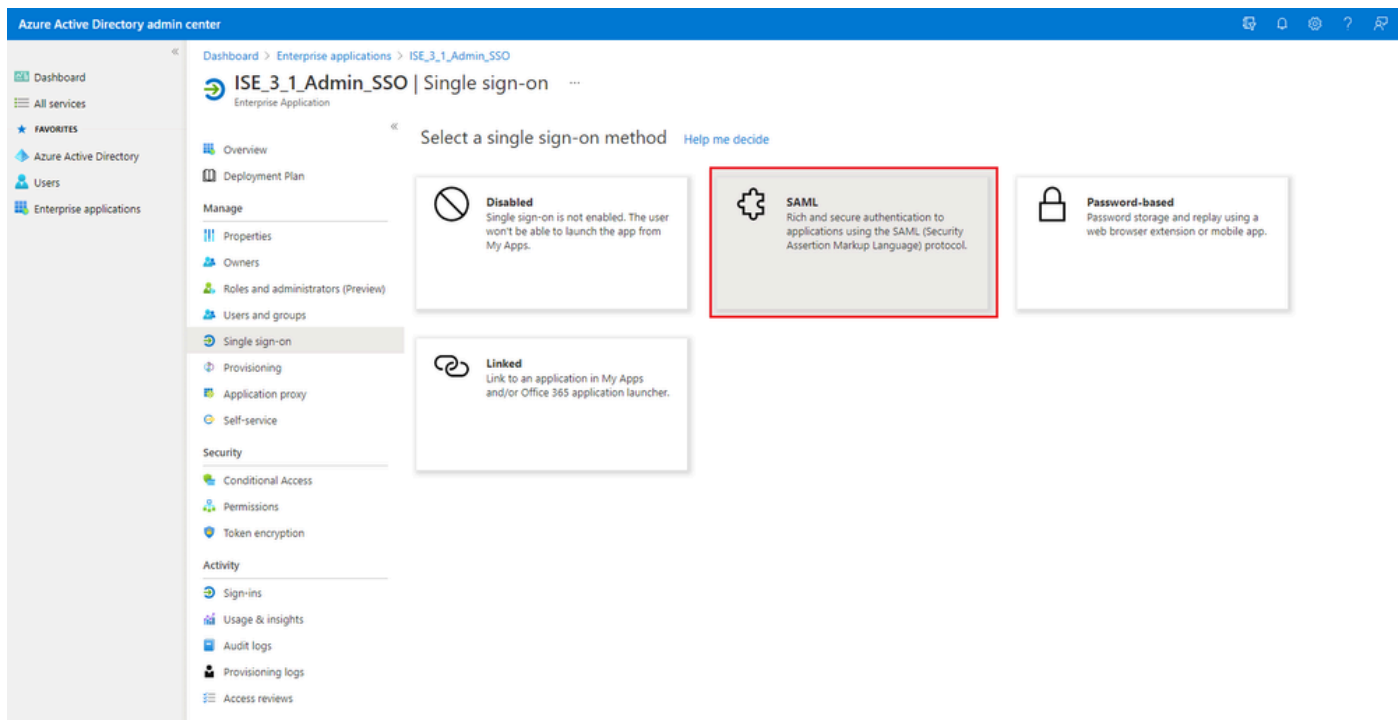


## 6. 配置Azure AD Enterprise應用程式

導航回您的應用程式，然後按一下Set up single sign on。



在下一個螢幕中選擇SAML。



按一下Basic SAML Configuration旁邊的Edit。

## 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

使用步驟匯出服務提供者資訊中XML檔案的entityID值填入辨識碼 (實體ID)。使用 AssertionConsumerService的Locations值填充回覆URL (Assertion Consumer Service URL)。按一下Save。

 附註：回覆URL會作為傳遞清單，當重新導向至IdP頁面時，允許特定URL作為來源。

## 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組屬性

要返回以前配置的組屬性值，請按一下User Attributes & Claims旁邊的Edit。

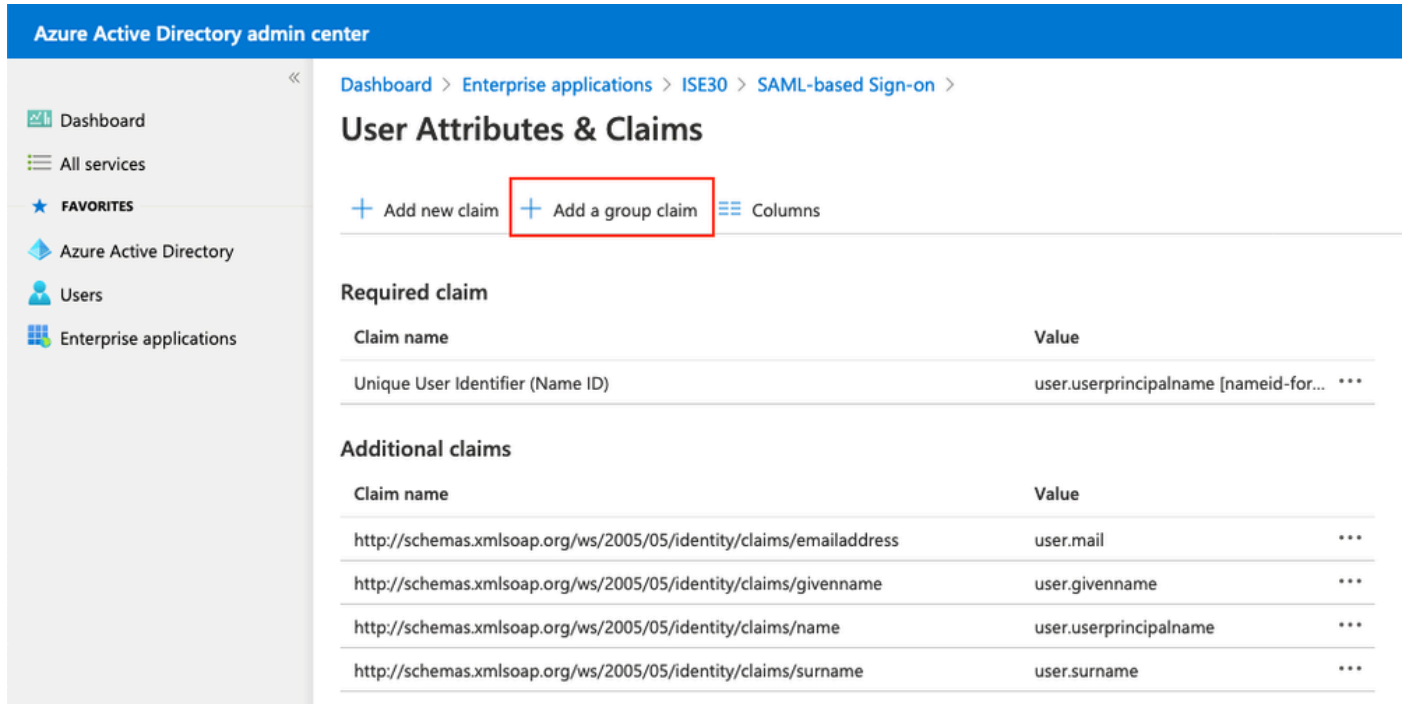


## User Attributes & Claims

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



按一下Add a group claim。



The screenshot shows the Azure Active Directory admin center interface. The breadcrumb navigation is: Dashboard > Enterprise applications > ISE30 > SAML-based Sign-on > User Attributes & Claims. The page title is "User Attributes & Claims". Below the title, there are three buttons: "+ Add new claim", "+ Add a group claim" (highlighted with a red box), and "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 ***

選擇Security groups，然後按一下Save。在Source attribute下拉選單中選擇Group ID。選中該覈取方塊以自定義組宣告的名稱，然後輸入名稱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 ⓘ

記下該組的領款申請名稱。在本示例中，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. 下載Azure Federation後設資料XML檔案

針對SAML簽名證書中的聯合後設資料XML按一下下載。

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>

## 步驟 3. 從Azure Active Directory上傳後設資料到ISE

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

將該頁籤切換到Identity Provider Config，然後按一下Browse。從步驟下載Azure聯合後設資料XML中選擇聯合後設資料XML檔案，然後按一下儲存。

## 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...

## 步驟 4. 在ISE上配置SAML組

切換到頁籤Groups，然後將Claim name的值從Configure Active Directory Group attribute貼上到Group Membership Attribute。

## 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

按一下Add。使用在將Azure Active Directory使用者分配到組中捕獲的ISE管理組的組對象ID值填充斷言中的名稱。

在ISE中配置名稱並從ISE中選擇適當的組。在本示例中，使用的組是Super Admin。按一下「OK」（確定）。點選儲存。

這會在Azure中的組和ISE上的組名之間建立一個對映。

**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

### ( 可選 ) 步驟5。配置RBAC策略

從上一步開始，可以在ISE上配置許多不同型別的使用者訪問級別。

要編輯基於角色的訪問控制策略(RBAC)，請導航到Administration > System > Admin Access > Authorization > Permissions > RBAC Policies，並根據需要進行配置。


此影象是示例配置的參考。

## ▼ RBAC Policies

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

## 驗證

確認您的組態是否正常運作。

 注意：Azure測試功能的SAML SSO登入測試不起作用。SAML請求必須由ISE啟動，Azure SAML SSO才能正常工作。

打開ISE GUI登入提示螢幕。您會看到一個用於使用SAML登入的新選項。

1. 訪問您的ISE GUI登入頁並按一下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. 系統會將您重新導向至Microsoft登入畫面。輸入對映到ISE的組中帳戶的使用者名稱憑據（如圖所示），然後按一下Next（如圖所示）。



# Sign in

mck@gdplab2021.onmicrosoft.com

---

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

Next

3. 輸入使用者的密碼，然後按一下「登入」。





← mck@gdplab2021.onmicrosoft.com

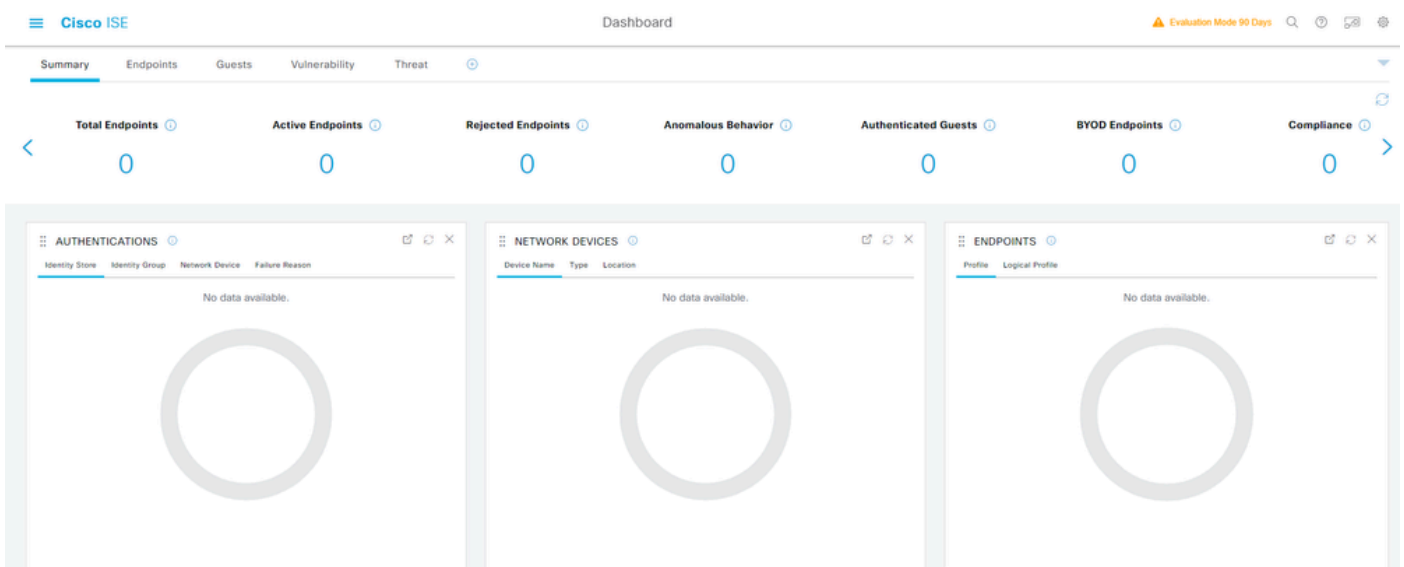
# Enter password

••••••••••

[Forgot my password](#)

Sign in

4. 您現在被重定向到ISE應用控制台，根據之前配置的ISE組配置相應的許可權，如圖所示。



## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

## 常見問題

瞭解在瀏覽器和Azure Active Directory之間處理SAML身份驗證至關重要。因此，您可以直接從身份提供程式(Azure)獲取與身份驗證相關的錯誤，其中ISE參與尚未啟動。

問題1：輸入憑據後出現「您的帳戶或密碼不正確」錯誤。此處，ISE尚未接收使用者資料，此時進程仍保留在IdP (Azure)中。

最可能的原因是帳戶資訊不正確或密碼不正確。若要修正：重設密碼或為該帳戶提供正確的密碼，如下圖所示。



← 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

問題2.使用者不屬於應該允許存取SAML SSO的群組。與之前的情況類似，ISE尚未接收使用者資料，此時進程仍使用IdP (Azure)。

要解決此問題，請驗證是否已正確執行向應用程式增加組配置步驟，如圖所示。



## 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.

問題3. ISE應用伺服器無法處理SAML登入請求。當從身份提供程式Azure而不是服務提供程式ISE發起SAML請求時，會出現此問題。從Azure AD測試SSO登入不起作用，因為ISE不支援身份提供程式啟動的SAML請求。



## 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	824F48B478350C93DE3D59EC87EE4C8
Expiration	7/19/2024, 12:16:24 PM
Notification Email	chandandemo@outlook.com
App Federation Metadata Url	<a href="https://login.microsoftonline.com/182900ec-e99d-4403-9102-000000000000">https://login.microsoftonline.com/182900ec-e99d-4403-9102-000000000000</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/182900ec-e99d-4403-9102-000000000000">https://login.microsoftonline.com/182900ec-e99d-4403-9102-000000000000</a>
Azure AD Identifier	<a href="https://sts.windows.net/182900ec-e99d-4403-9102-000000000000/">https://sts.windows.net/182900ec-e99d-4403-9102-000000000000/</a>
Logout URL	<a href="https://login.microsoftonline.com/182900ec-e99d-4403-9102-000000000000">https://login.microsoftonline.com/182900ec-e99d-4403-9102-000000000000</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: Saa879f5-68f1-482a-a405-f993d8f4cb0  
Timestamp: 2018-03-06T23:54:10Z  
Message: Error AADSTSXXXXX

[Get resolution guidance](#)

問題4. ISE在登入嘗試後顯示「訪問被拒絕」錯誤。當Azure Enterprise Application中以前建立的組的宣告名稱與ISE中的宣告名稱不匹配時，會發生此錯誤。

要解決此問題：確保Azure和ISE中SAML身份提供程式組頁籤下的組宣告名稱相同。有關詳細資訊，請參閱本文檔的使用Azure AD配置SAML SSO部分下的步驟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

必須在ISE上更改此處的元件的日誌級別。導航到操作>故障排除>調試嚮導>調試日誌配置。

元件名稱	記錄層級	記錄檔名
入口網站	除錯	guest.log

opensaml	除錯	ise-psc.log
saml	除錯	ise-psc.log

具有SAML登入名和不匹配的組宣告名稱的日誌

顯示流執行時宣告名稱不匹配故障排除方案的一組調試(ise-psc.log)。



注意：請留意粗體專案。為了清楚起見，已將日誌縮短。

1. 從ISE管理頁面將使用者重定向到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. 從瀏覽器接收SAML響應。

<#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
```



```

2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,185 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.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.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,186 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.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.saml.framework.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.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,188 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.validate
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,189 DEBUG [https-jsse-nio-10.201.232.19-8443-exec-10] [] cpm.saml.framework.impl.SAML
2021-07-29 13:48:27,358 INFO [admin-http-pool50] [] ise.rbac.evaluator.impl.MenuPermissionEvaluatorImp

```

## 5. RBAC授權驗證。

```
<#root>
```

```

*****Rbac Log Summary for user samlUser*****
2021-07-29 13:48:27,360 INFO [admin-http-pool50] [] com.cisco.ise.util.RBACUtil -:::- Populating cache
2021-07-29 13:48:27,368 ERROR [admin-http-pool50] [] cpm.admin.infra.utils.PermissionEvaluationUtil -:::-
java.lang.NullPointerException
2021-07-29 13:48:27,369 INFO [admin-http-pool50] [] cpm.admin.infra.action.LoginAction -:::- In Login
2021-07-29 13:48:27,369 INFO [admin-http-pool50] [] cpm.admin.infra.action.LoginAction -:::- In Login
2021-07-29 13:48:27,369 ERROR [admin-http-pool50] [] cpm.admin.infra.action.LoginAction -:::- Can't save

```



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

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

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。