通過與Azure AD整合的SAML SSO配置ISE 3.1 ISE GUI管理員登入流

目錄

簡介

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

必要條件

需求

思科建議您瞭解以下主題：

1. Cisco 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. Cisco 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

身份提供程式(IdP)

在此案例中，是Azure AD的授權驗證並宣告使用者身份以及對所請求資源（「服務提供商」）的訪問許可權。

服務提供商(SP)

使用者想要訪問的託管資源或服務，在本例中為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)在身份提供者和服務提供商之間進行標準化通訊。

SAML是使用者身份身份驗證與授權之間用於使用服務的連結。

SAML斷言

SAML斷言是身份提供方傳送到包含使用者授權的服務提供方的XML文檔。

有三種不同型別的SAML斷言 — 身份驗證、屬性和授權決策。

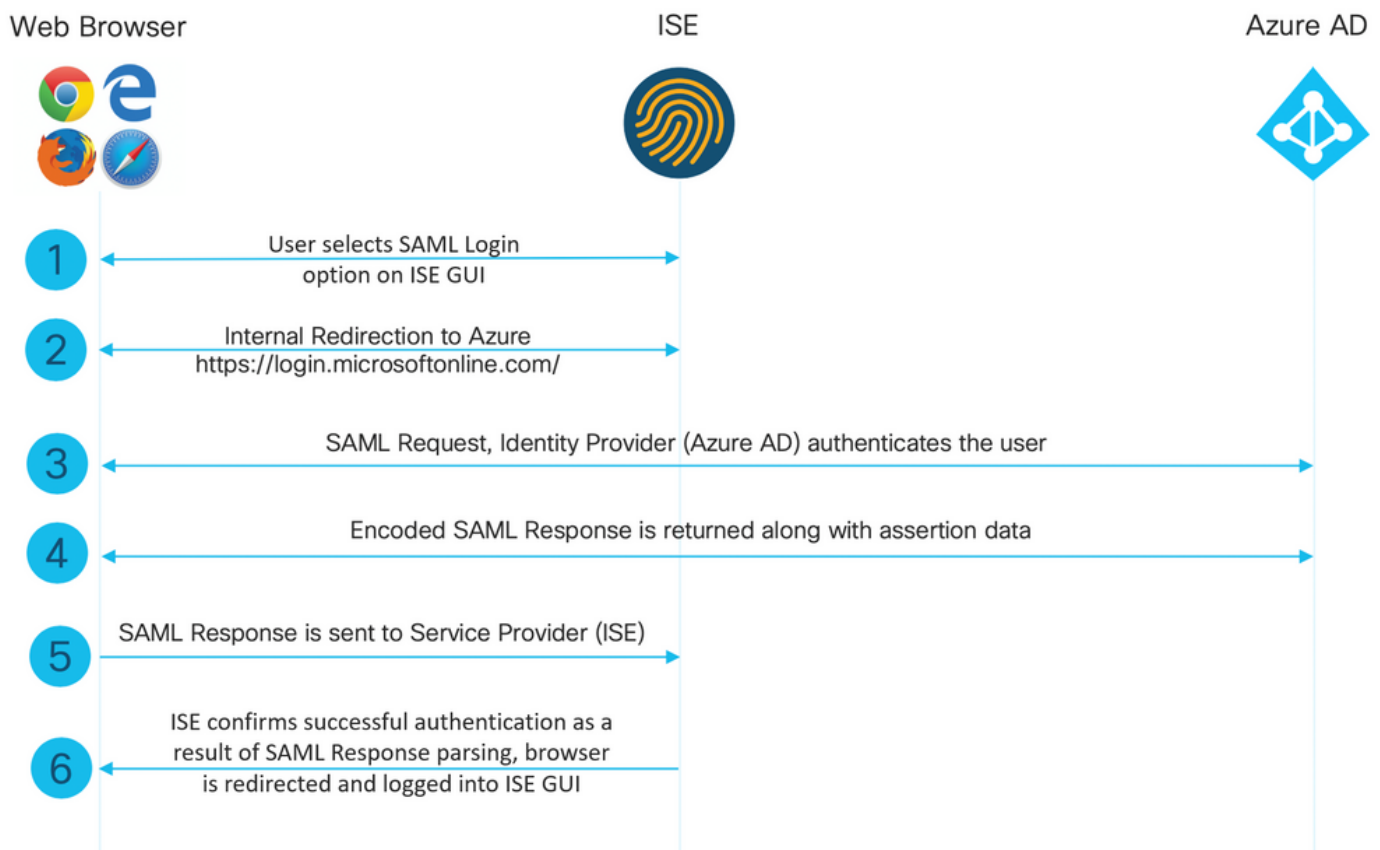- 身份驗證斷言可證明使用者的身份，並提供使用者登入的時間以及他們使用的身份驗證方法

（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段）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權利而拒絕他們的請求。

高級流程圖

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。

每個使用者通過身份提供程式登入一次－一次單點登入(SSO)，然後，當使用者嘗試訪問這些服務時，Azure AD提供程式將SAML屬性傳遞給ISE。

ISE從Azure AD請求授權和身份驗證，如下圖所示。

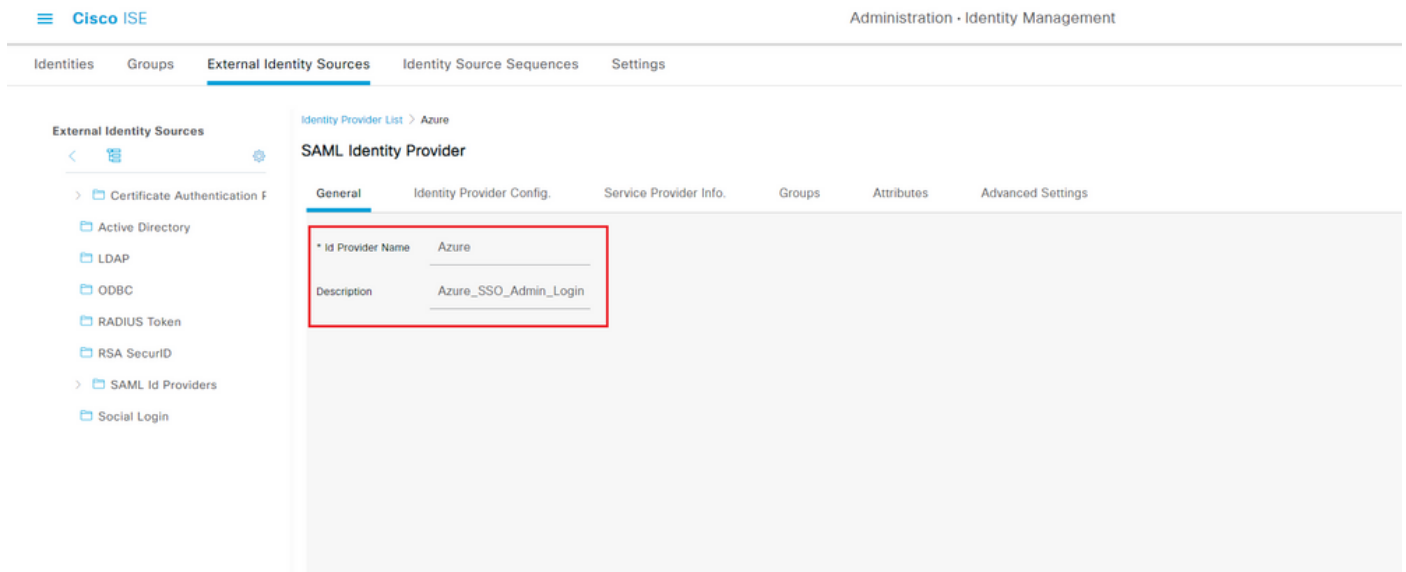# 配置與Azure AD的SAML SSO整合

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

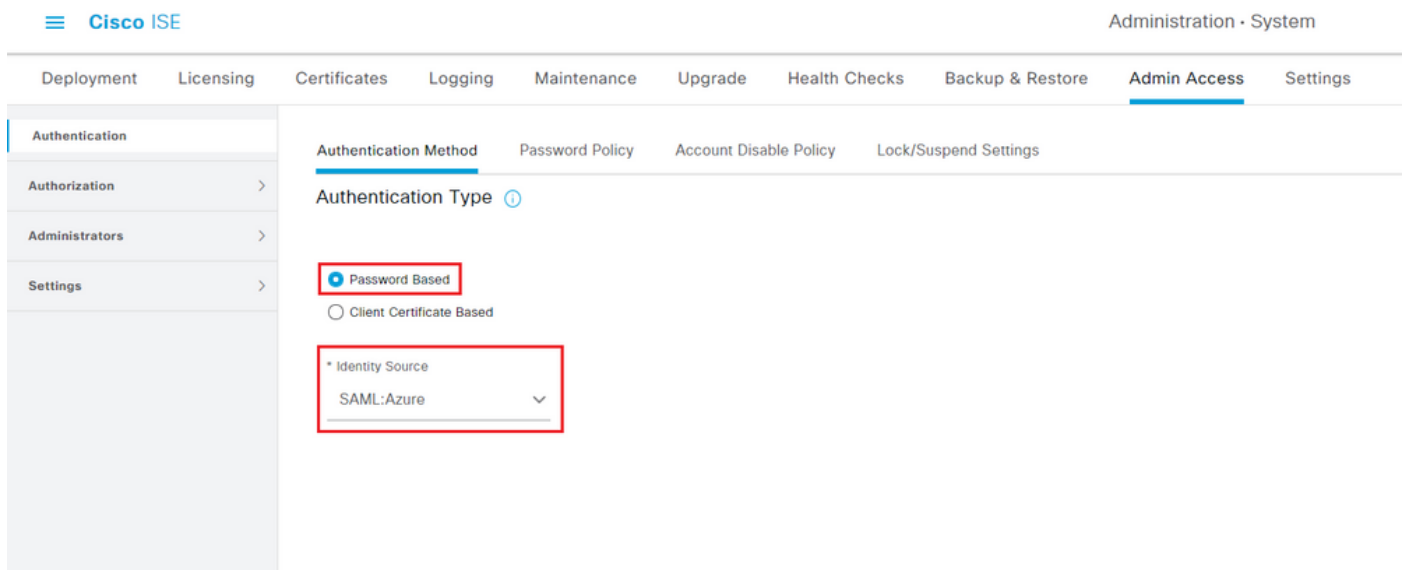在ISE上，導航到Administration > Identity Management > External Identity Sources > SAML Id Providers，然後點選Add按鈕。

輸入Id Provider Name，然後按一下Submit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Administration > System > Admin Access > Authentication > Authentication Method，然後選擇Password Based單選按鈕。

從Identity Source下拉選單中選擇先前建立的所需ID提供程式名稱，如下圖所示。

3.匯出服務提供商資訊

導航到Administration > Identity Management > External Identity Sources > SAML Id Providers > [您的SAML提供程式]。

將頁籤切換到Service Provider Info，然後按一下Export按鈕，如下圖所示。

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" WantAssertionsSign
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amSlL6NAE8FY+tzANBgkqhkiG9w0BAQwFADAlMSMwIQYDVQQDExpT
QU1MX2lzZTMtMSOxOS5ja3VtYXIyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTGlNBTUxfaXNlMy0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAvila4+SOuP3j037yCOXnHAzADupfqcgwcplJQnFxhVfnDdOixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohGOt1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYdlDtE1LMEcGg1mCd56GfrDcJdXOcZJmiDzizyjGKDdPf+1VM5JHCo6UNLFlIFyPmGvcCXnt
NVqsYvxSzF038ciQqlmOsqrVrrYZuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFFlMzybvm1FYu
9h83gL4WJWMizETO6Vs/DOp6BSf2MPxKe790R5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5ROgT7v3CDrdFtRoNYAT+YvO941KzFCSEOsshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNzlFuggaE8tC7uyuQZa2rcmTrXGWCl
sDU4uOvFpFvrcC/lavr9Fnx7LPwXaOasvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWIy+ctbBTO+EMO6Xj1aTI1bV80mN/6LhiS8g7KpFz4RN+ag1iu6pgZ5O58Zot9gqkpFw
kVS9vT4EOzwNGo7pQI8CAwEAAaN9MHswIAYDVRORBBkwF4IVaXNlMy0xLTE5LmNrdW1hcjIuY29t
MAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgLsMB0GA1UdDgQWBBRIkY2z/9H9PpwSnOPGARCj5iaZ
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEMBQADggIBAIE6mnBL
2O6Dkb6fHdgKd9goN8N2bj+34ybwxqvDSwGtn4NA6Hy1q7N6iJzAD/7soZfHgOT2UTgZpRF9FsHn
CGchSHqDt3bQ7g+GWlvcgreC7R46qenaonXVrltRw11vVIdCf8JQFFMxya/rIC4mxVeooOj1Fl9d
rvDBH+XVEt67DnQWkuLp8zPJUuqfa4HOvdm6oF3uBteO/pdUtEi6fObqrOwCyWd9Tjq7KXfd2ITW
hMxaFsv8wWcVuOMDPkP9xUwwt6gfHObE5luT4EYVuuHiwMNGbZqgqb+a4uSkX/EfiDVoLSL6KI31
nf/341cuRTJUmDh9g2mppbBwOcxzoUxDm+HReSe+OJhRCyIJcOvUpdNmYC8cfAZuiV/e3wkOBLZM
lgV8FTVQSnra9LwHP/PgeNAPUcRPXSwaKE4rvjvMcOaS/iYdwZhZiJ8zBdIBanMv5mGu1nvTEt9K
EEwj9yslIHmdqoH3EmOFOgnzRORvsMPbJxAoTFjfoITTMdQXNHhg+wlPOKXS2GCZ29vAM52d8ZCq
UrzOVxNHKWKwER/q1GgaWvh3X/G+z1shUQDrJcBdLcZI1WKUMa6XVDj18byhBM7pFGwg4z9YJZGF
/ncHcoxFY759LA+m7Brp7FFPiGCrPW8EOv7bUMSDmmg/53NoktfJ1CckaWE87myhimj0
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
```

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

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

XML檔案中的相關屬性：

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"

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，然後選擇AD，如下圖所示。
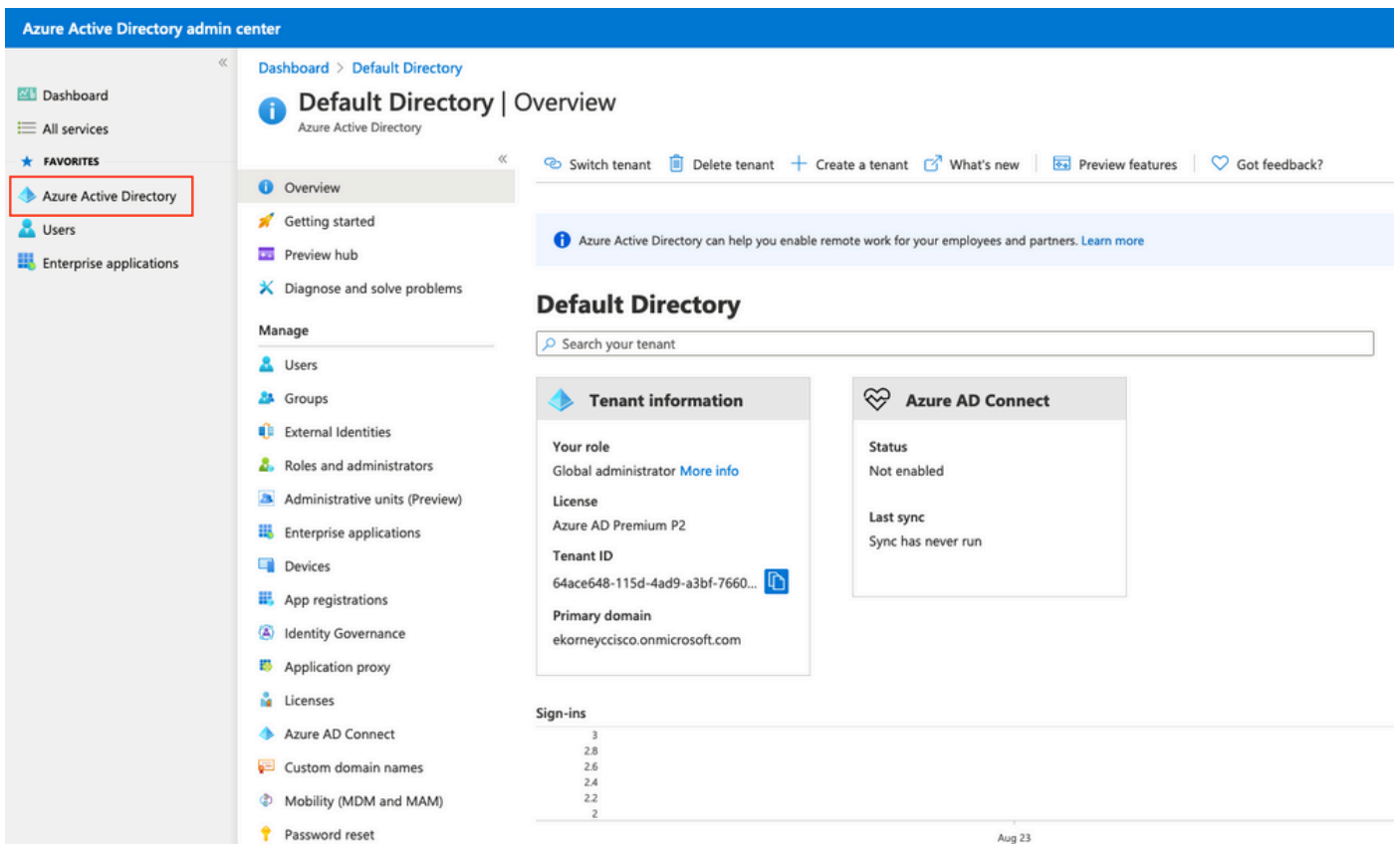
選擇Users，按一下New User，根據需要配置User name、Name和Initial Password。按一下「Create」，如下圖所示。

Identity

User name * ⓘ	mck ✓ @ gdplab2021.onmicrosoft.... ∨ 📋	
	The domain name I need isn't shown here	
Name * ⓘ	mck ✓	
First name		
Last name		

Password

Initial password

◉ Auto-generate password
○ Let me create the 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

將組型別保留為Security。設定Group name，如下圖所示。

3.將Azure AD使用者分配給組

按一下No members selected。選擇使用者並按一下Select。按一下Create以建立已為其分配了User的組。

Add members   ✕

Search ⓘ

🔍 mck   ✕

MC mck
       mck@gdplab2021.onmicrosoft.com

Selected items

No items selected

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

4.建立Azure AD Enterprise應用程式

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

選擇Create your own application。
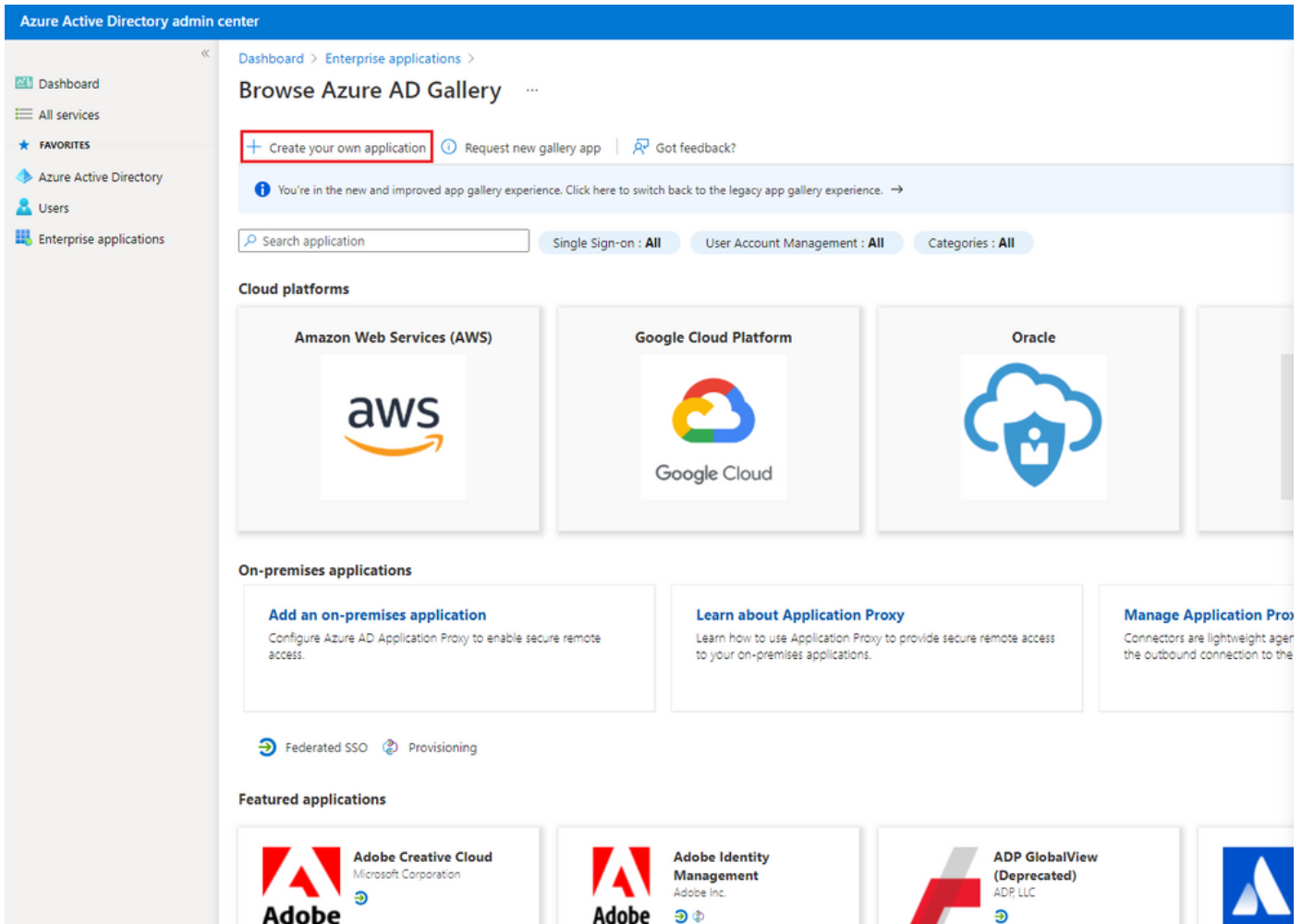
輸入應用程式的名稱，然後選擇Integrate any other application you not found in the gallery(Non-gallery)單選按鈕，然後按一下Create按鈕，如下圖所示。

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.將組新增到應用程式

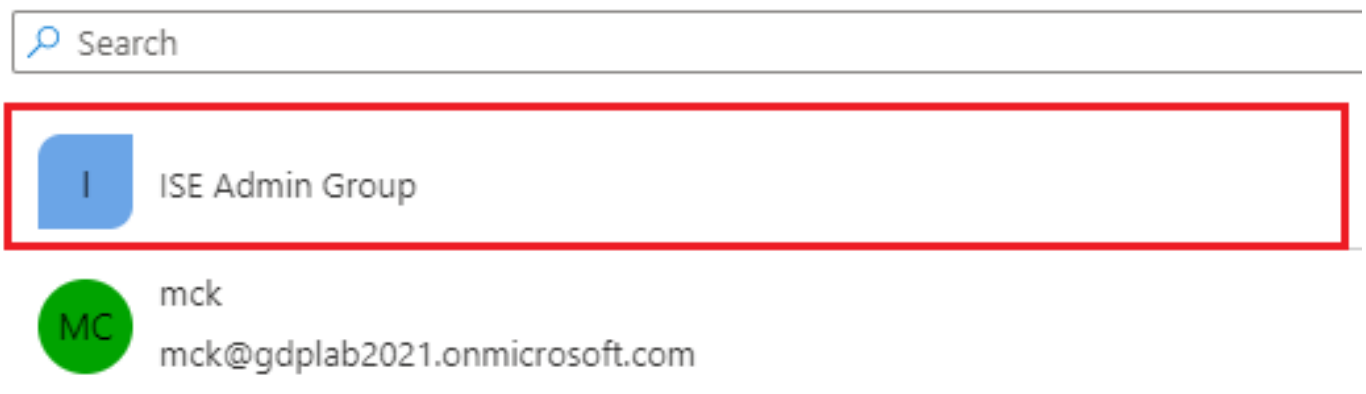選擇Assign users and groups。

按一下Add user/group。
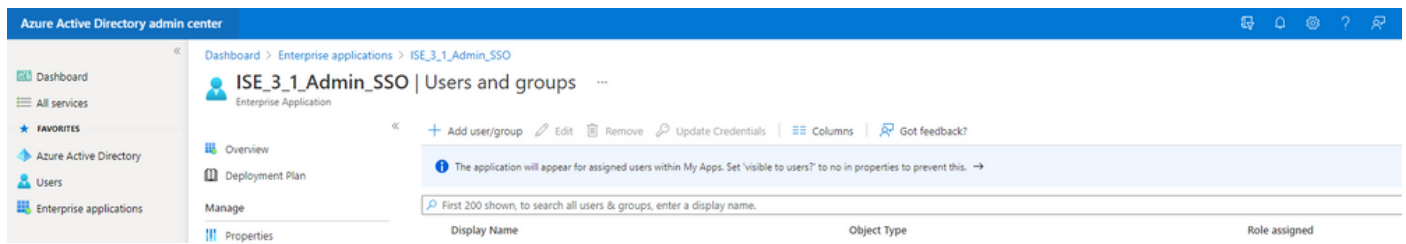
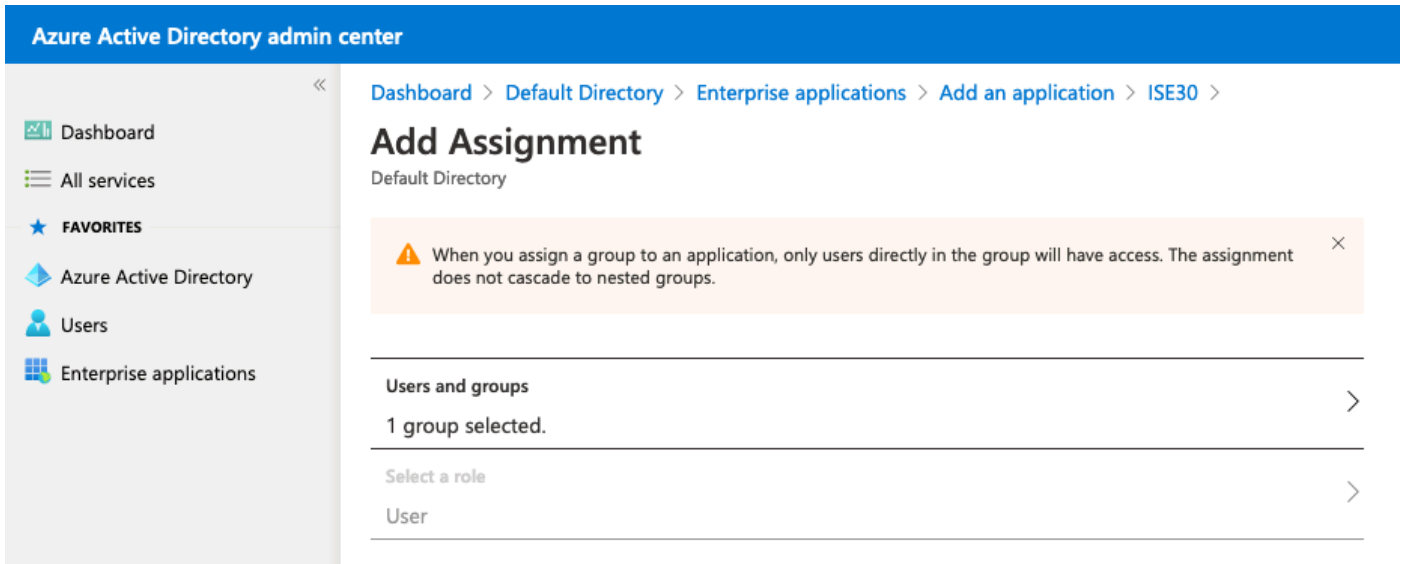按一下Users and groups。
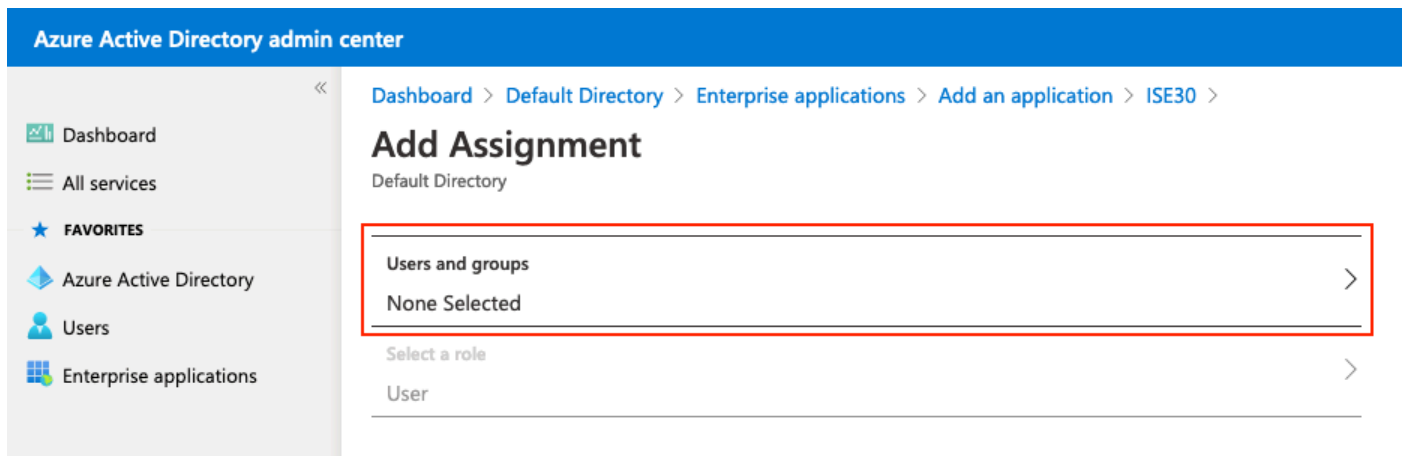
選擇先前配置的組,然後按一下選擇。

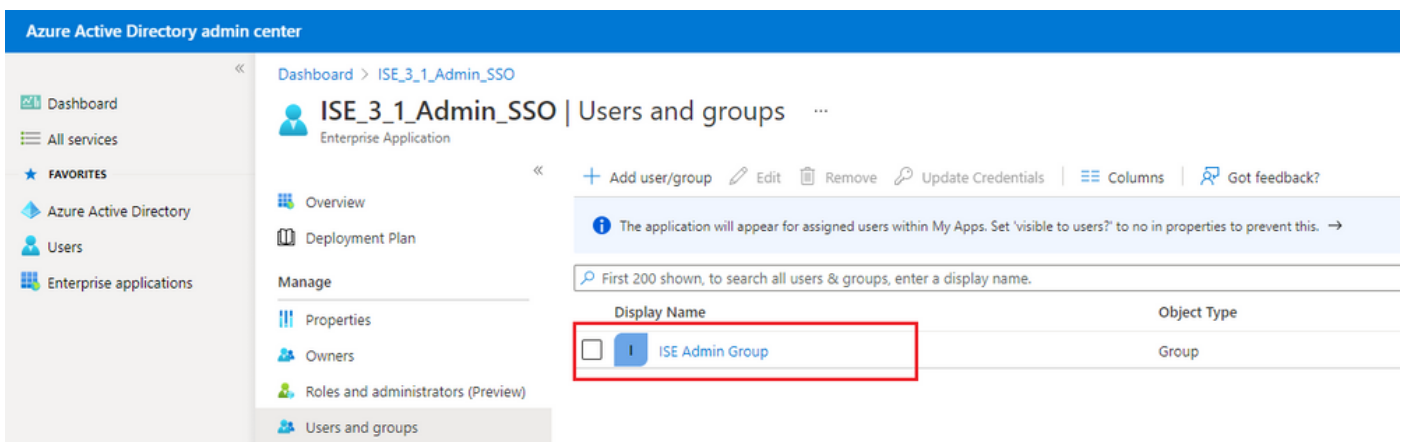📝 附註: 選擇獲得所需訪問許可權的正確使用者或組,因為此處提到的使用者和組在設定完成後即可獲得ISE訪問許可權。

Users and groups

選擇組後,按一下Assign。
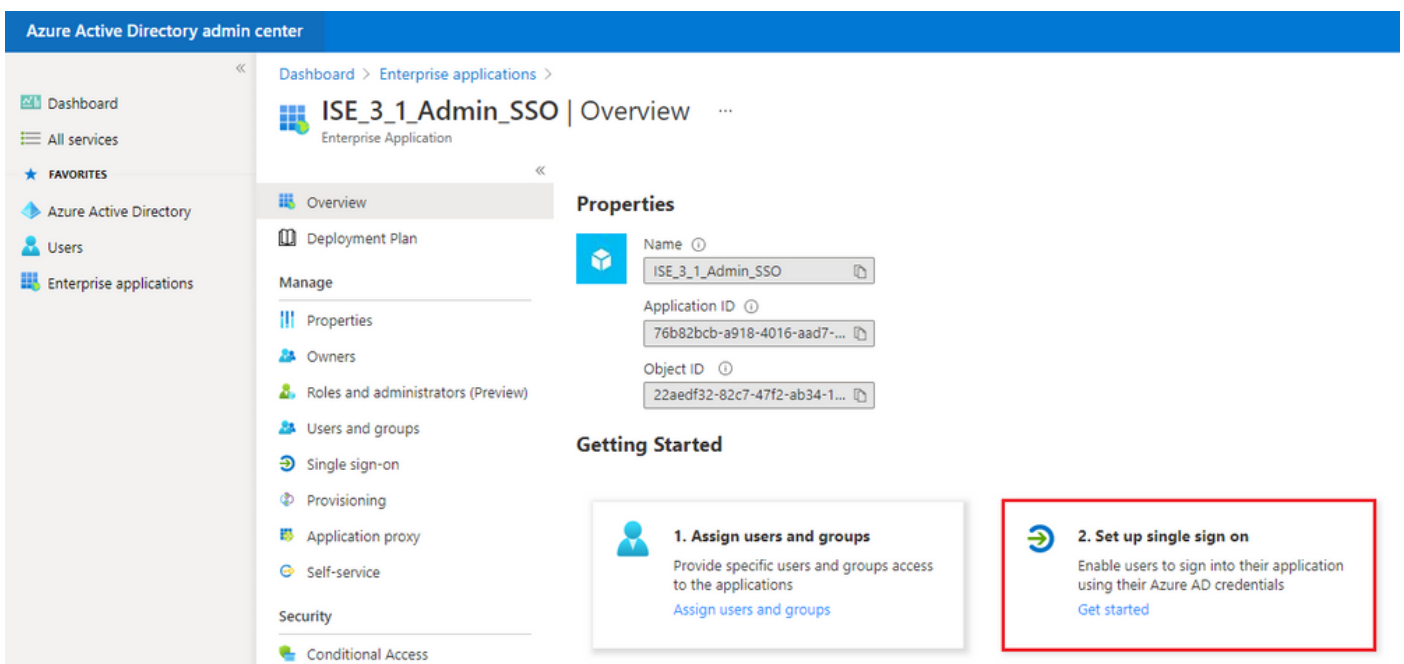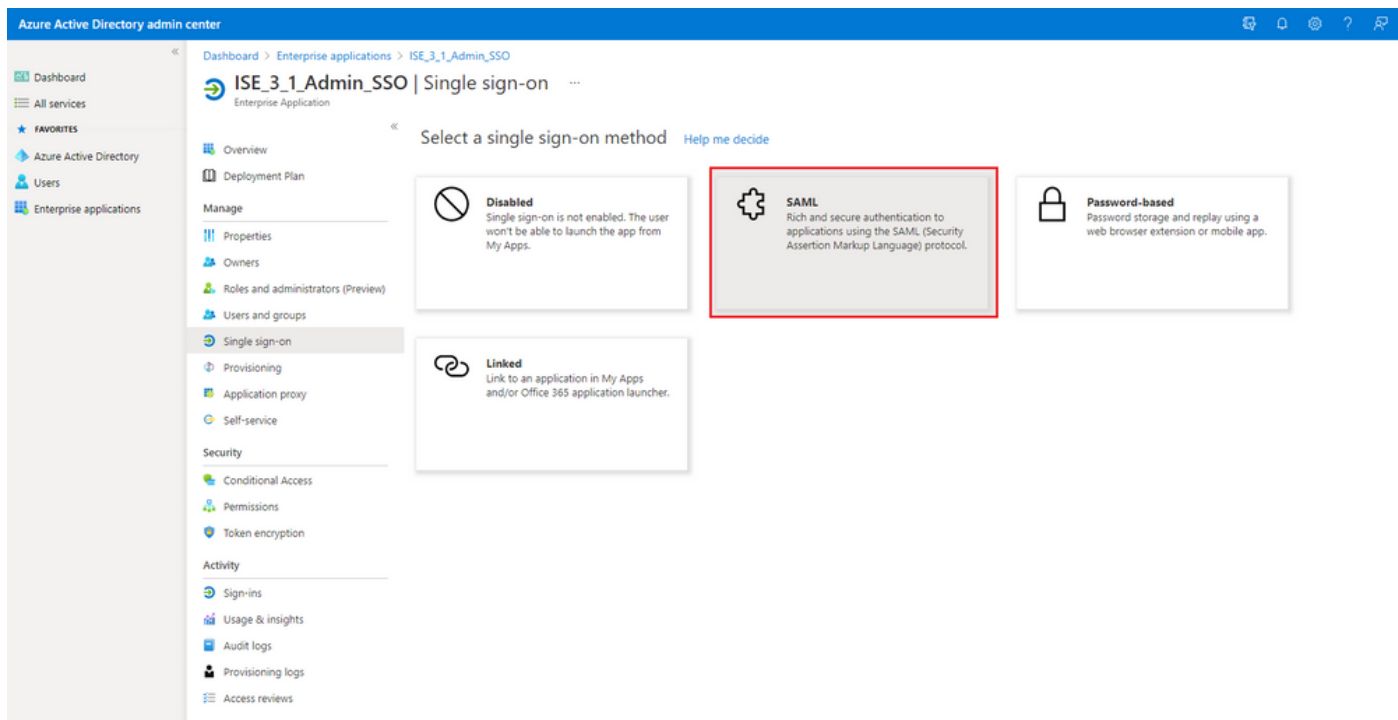
因此，已配置應用程式的使用者和組選單會填充所選的組。

6.配置Azure AD Enterprise應用程式

導航回您的應用程式，然後單擊「設定單一登入」。

在下一個螢幕上選擇SAML。

按一下Basic SAML Configuration旁邊的Edit。

在步驟匯出服務提供商資訊中，使用XML檔案中的entityID值填充識別符號（實體ID）。使用AssertionConsumerService中的Locations值填充Reply URL(Assertion Consumer Service URL)。按一下「Save」。

✎ 附註: 回覆URL用作傳遞清單,允許某些URL在重定向到IdP頁面時用作源。

Basic SAML Configuration

✕

🖫 Save

Identifier (Entity ID) * ⓘ

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

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

Reply URL (Assertion Consumer Service URL) * ⓘ

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

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

Sign on URL ⓘ

Enter a sign on URL

Relay State ⓘ

Enter a relay state

Logout Url ⓘ

Enter a logout url

7.配置Active Directory組屬性

要返回先前配置的組屬性值,請點選使用者屬性和宣告旁邊的編輯。
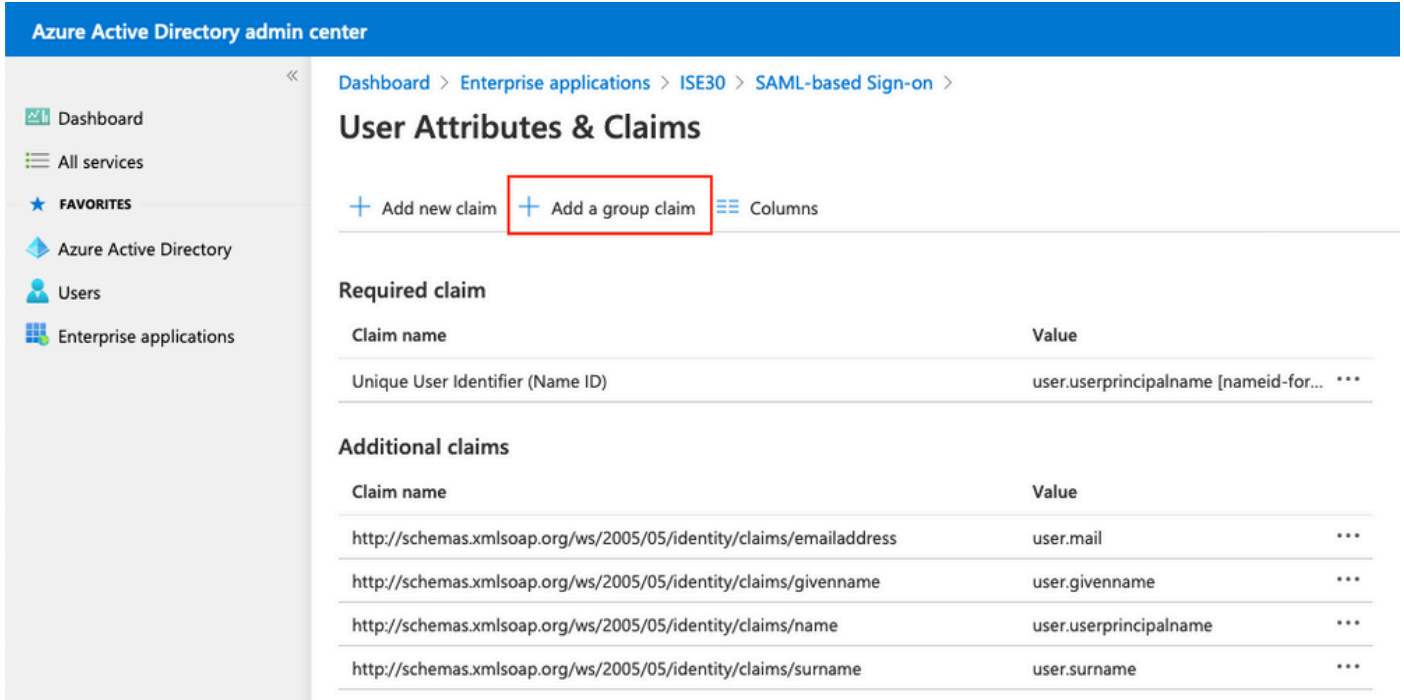
User Attributes & Claims

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

按一下Add a group claim。

選擇Security groups，然後按一下Save。 在Source attribute下拉選單中選擇Group ID。選中此覈取方塊可自定義組宣告的名稱，並輸入名稱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 ⓘ

記下該組的申請名稱。在本例中，它是組。

8.下載Azure聯合後設資料XML檔案

在SAML簽名證書中，按一下Download on Federation Metadata XML。

步驟 3.將後設資料從Azure Active Directory上載到ISE

導航到Administration > Identity Management > External Identity Sources > SAML Id Providers > [您的SAML提供程式]。

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

步驟 4.在ISE上配置SAML組

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

按一下「Add」。使用將Azure Active Directory使用者分配給組時捕獲的ISE管理組的組對象ID值填充Assertion中的Name。

使用下拉選單配置ISE中的名稱(Configure Name in ISE)，並在ISE上選擇適當的組。在本示例中，使用的組是Super Admin。按一下「OK」（確定）。按一下「Save」。

這將在Azure中的組和ISE上的組名稱之間建立對映。

（可選）步驟5。配置RBAC策略

在上一步中，可在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。

此映像是對示例配置的引用。

RBAC Policies

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

驗證

確認您的組態是否正常運作。

✎ 附註: Azure測試功能中的SAML SSO登入測試無法正常工作。SAML請求必須由ISE啟動，Azure SAML SSO才能正常工作。

開啟ISE GUI登入提示螢幕。您將看到一個使用SAML登入的新選項。

1.訪問您的ISE GUI登入頁面，然後按一下使用SAML登入。

2.系統會將您重新導向至Microsoft登入螢幕。如圖所示，輸入對映到ISE的組內帳戶的使用者名稱憑證，然後按一下下一步，如圖所示。

Microsoft

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。

4.現在您將重定向到ISE應用儀表板，該儀表板具有根據之前配置的ISE組配置的相應許可權，如圖所示。
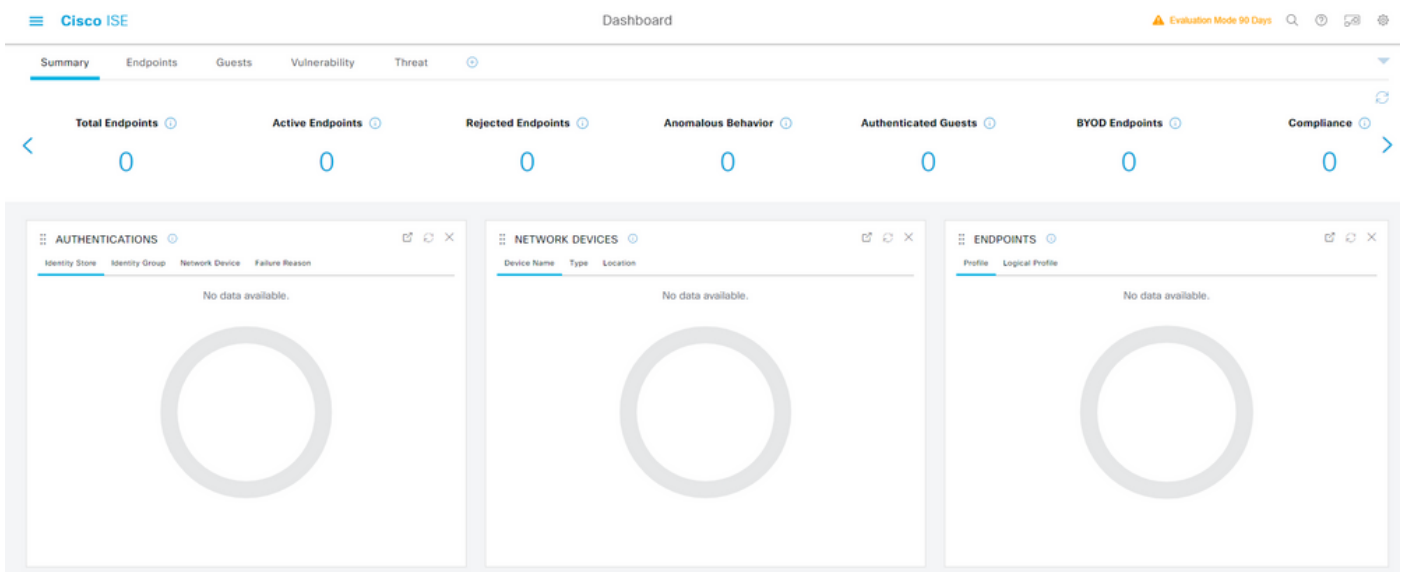
疑難排解

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.輸入憑證後出現「您的帳戶或密碼不正確」錯誤。此時，ISE尚未接收使用者資料，此時進程仍使用IdP(Azure)。

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。

問題2.使用者不屬於應該允許訪問SAML SSO的組。與前面的情況類似，ISE尚未收到使用者資料，此時進程仍採用IdP(Azure)。

要解決此問題：驗證Add group to the Application 配置步驟是否正確執行，如下圖所示。

Microsoft

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.

第三期。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啟動SAML請求時，會發生此問題。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。

第四期。ISE在登入嘗試後顯示「訪問被拒絕」錯誤。當早期在Azure企業應用程式中建立的組的宣告名稱在ISE中不匹配，則會發生此錯誤。

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。

排除ISE故障

必須在ISE上更改此處的元件的日誌級別。導覽至Operations > Troubleshoot > Debug Wizard > Debug Log Configuration。

元件名稱	日誌級別	日誌檔名

門戶	偵錯	guest.log
opensaml	偵錯	ise-psc.log
saml	偵錯	ise-psc.log

包含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)。

✎ 註：注意粗體項目。為了清楚起見，日誌被縮短了。

1.使用者從ISE管理員頁面重定向到IdP URL。

<#root>

2021-07-29 13:48:20,709 INFO   [admin-http-pool46][] api.services.persistance.dao.DistributionDAO -::::-
2021-07-29 13:48:20,712 INFO   [admin-http-pool46][] cpm.admin.infra.spring.ISEAdminControllerUtils -::

forwardStr for: https://10.201.232.19/admin/LoginAction.do

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

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

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

SAML request - spUrlToReturnTo:https://10.201.232.19:8443/portal/SSOLoginResponse.action

2021-07-29 13:48:20,844 DEBUG   [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:20,851 DEBUG   [https-jsse-nio-10.201.232.19-8443-exec-7][] cpm.saml.framework.impl.SAM

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

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

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

-::::- Decoded SAML message

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

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

3.屬性（斷言）分析已啟動。

<#root>

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

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

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

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

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

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

[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.SAN

4.收到值為576c60ec-c0b6-4044-a8ec-d395b1475d6e的組屬性，並進行簽名驗證。

```
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
        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-890
        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.impl.SAM
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAM
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 cach

2021-07-29 13:48:27,368 ERROR  [admin-http-pool50][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::



java.lang.NullPointerException



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



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

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

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

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