透過Azure AD的SAML SSO配置ISE 3.1管理員登入流

目錄

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。

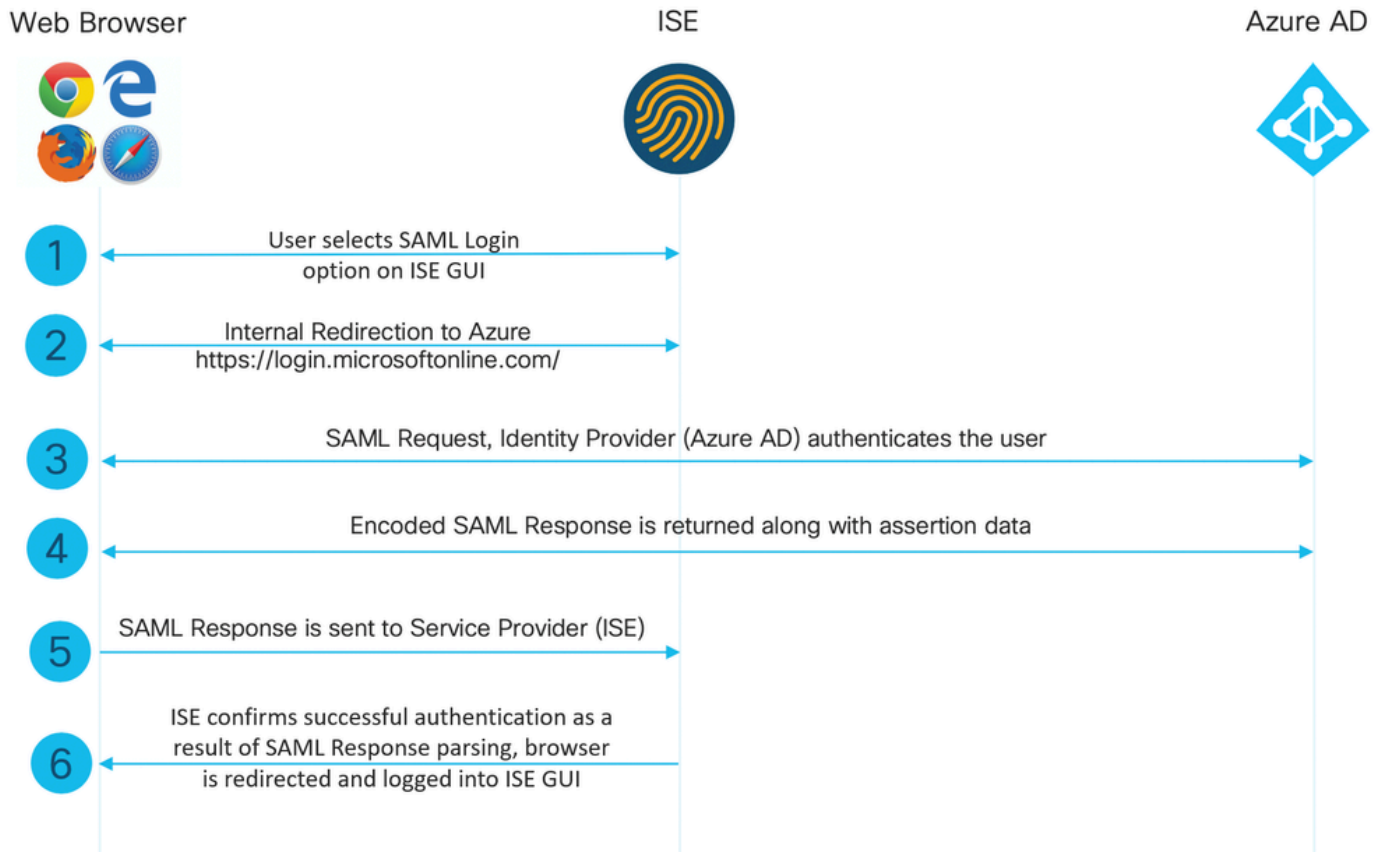
- 身份驗證斷言可證明使用者的身份，並提供使用者登入的時間以及他們使用的身份驗證方法（例如，Kerberos，雙因素）
- 歸屬斷言將SAML屬性（提供有關使用者資訊的特定資料）傳遞給服務提供商。
- 授權決策斷言宣告使用者是否被授權使用服務，或者如果標識提供者由於密碼失敗或缺少對服務的許可權而拒絕他們的請求。

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。



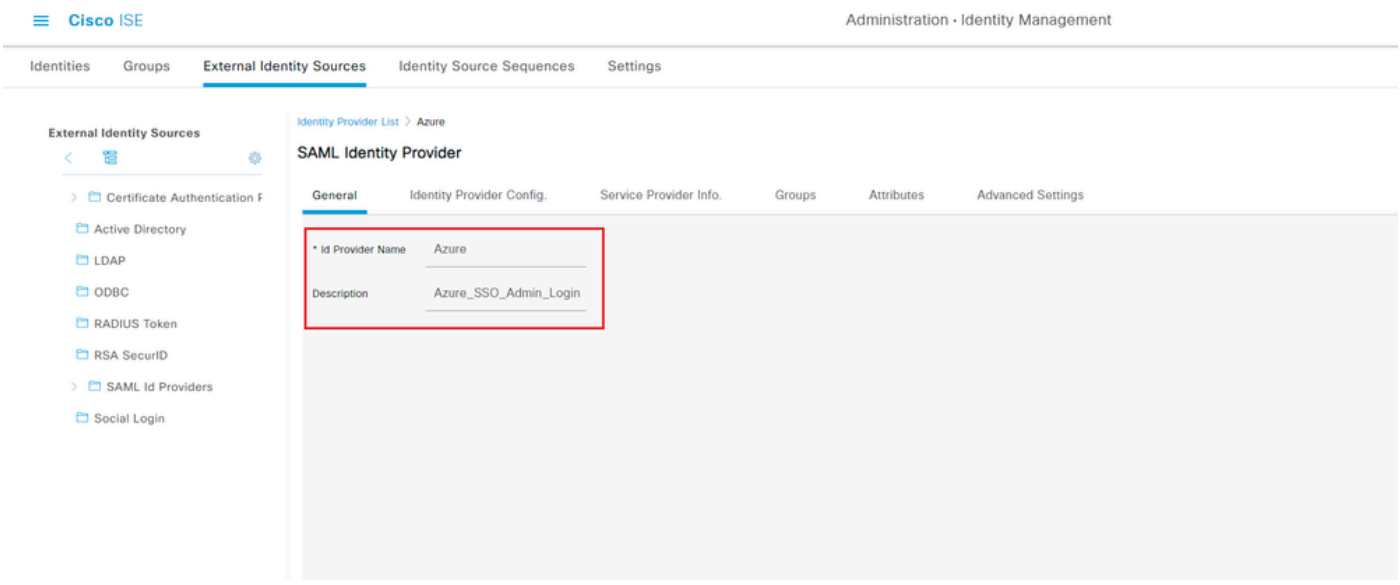
配置與Azure AD的SAML SSO整合

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。

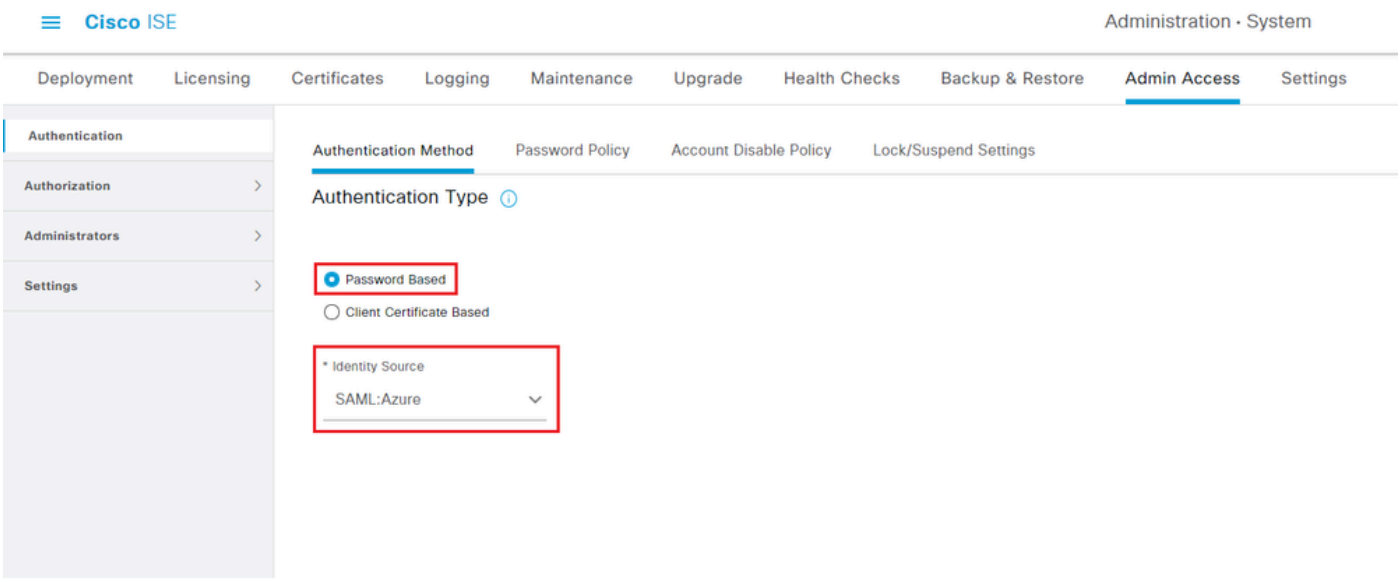
輸入Id Provider Name並按一下Submit以儲存它。Id Provider Name僅對ISE有效，如下圖所示。



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。

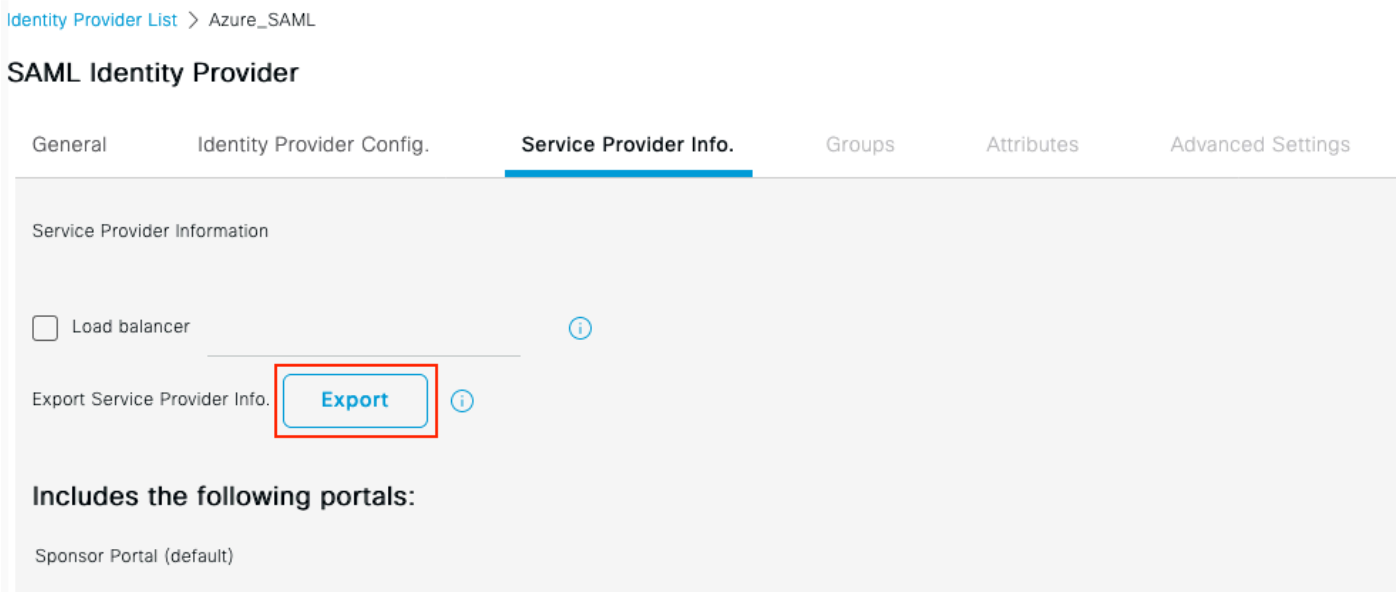
從Identity Source下拉選單選擇之前建立的所需Id Provider Name，如下圖所示。



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。



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:oasi
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSig
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFTjCCAzagAwIBAgINAg2amSlL6NAE8FY+tzANBgkqhkiG9w0BAQwFADAlMSMwIQYDVQQDExpT
QU1MX2lzZTMtMS0xOS5ja3VtYXIyLmNvbTAeFw0yMTA3MTkwMzI4MDBaFw0yNjA3MTgwMzI4MDBa
MCUxIzAhBgNVBAMTGlNBTUxfaXNlMy0xLTE5LmNrdW1hcjIuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAvila4+SOuP3j037yCOXnHAzADupfqcgwcplJQnFxhVfnDdOixGRT8iaQ
1zdKhpwf/BsJeSznXyaPVxFcmMFHbmyt46gQ/jQQEyt7YhyohGOt1op01qDGwtOnWZGQ+ccvqXSL
Ge1HYdlDtE1LMEcGg1mCd56GfrDcJdXOcZJmiDzizyjGKDdPf+1VM5JHCo6UNLFlIFyPmGvcCXnt
NVqsYvxSzFO38ciQqlm0sqrVrrYZuIUAXDWUNUg9pSGzHOFkSsZRPxrQh+3N5DEFFlMzybvm1FYu
9h83gL4WJWMizETO6Vs/DOp6BSf2MPxKe79OR5TfxFqJD9DnYgCnHmGooVmnSSnDsAgWebvF1uhZ
nGGkH5ROgT7v3CDrdFtRoNYAT+YvO941KzFCSEOsshykGSjgVn31XQ5vgDH1PvqNaYs/PWiCvmI/
wYKSTn9/hn7JM1DqOR1PGEkVjg5WbxcViejMrrIzNrIciFNzlFuggaE8tC7uyuQZa2rcmTrXGWCl
sDU4uOvFpFvrcC/lavr9Fnx7LPwXaOasvJd19SPbD+qYgshz9AI/nIXaZdioHzEQwa8pkoNRBwjZ
ef+WFC9dWIy+ctbBTO+EMO6Xj1aTI1bV8OmN/6LhiS8g7KpFz4RN+ag1iu6pgZ5O58Zot9gqkpFw
kVS9vT4EOzwNGo7pQI8CAwEAAaN9MHswIAYDVR0RBBkwF4IVaXNlMy0xLTE5LmNrdW1hcjIuY29t
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"

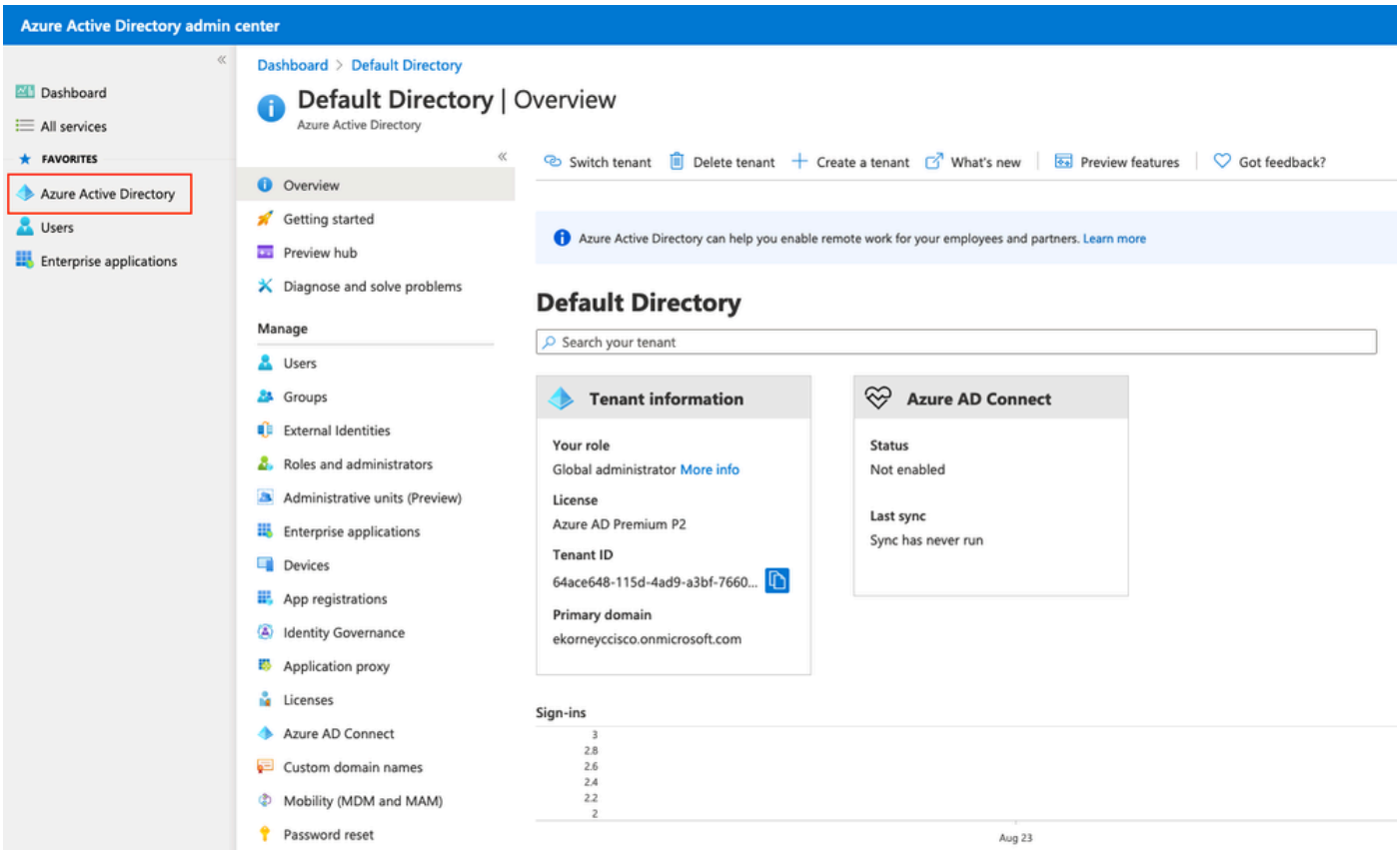
AssertionConsumerService位置="https://10.201.232.19:8443/portal/SSOLoginResponse.action"

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

步驟 2.配置Azure AD IdP設定

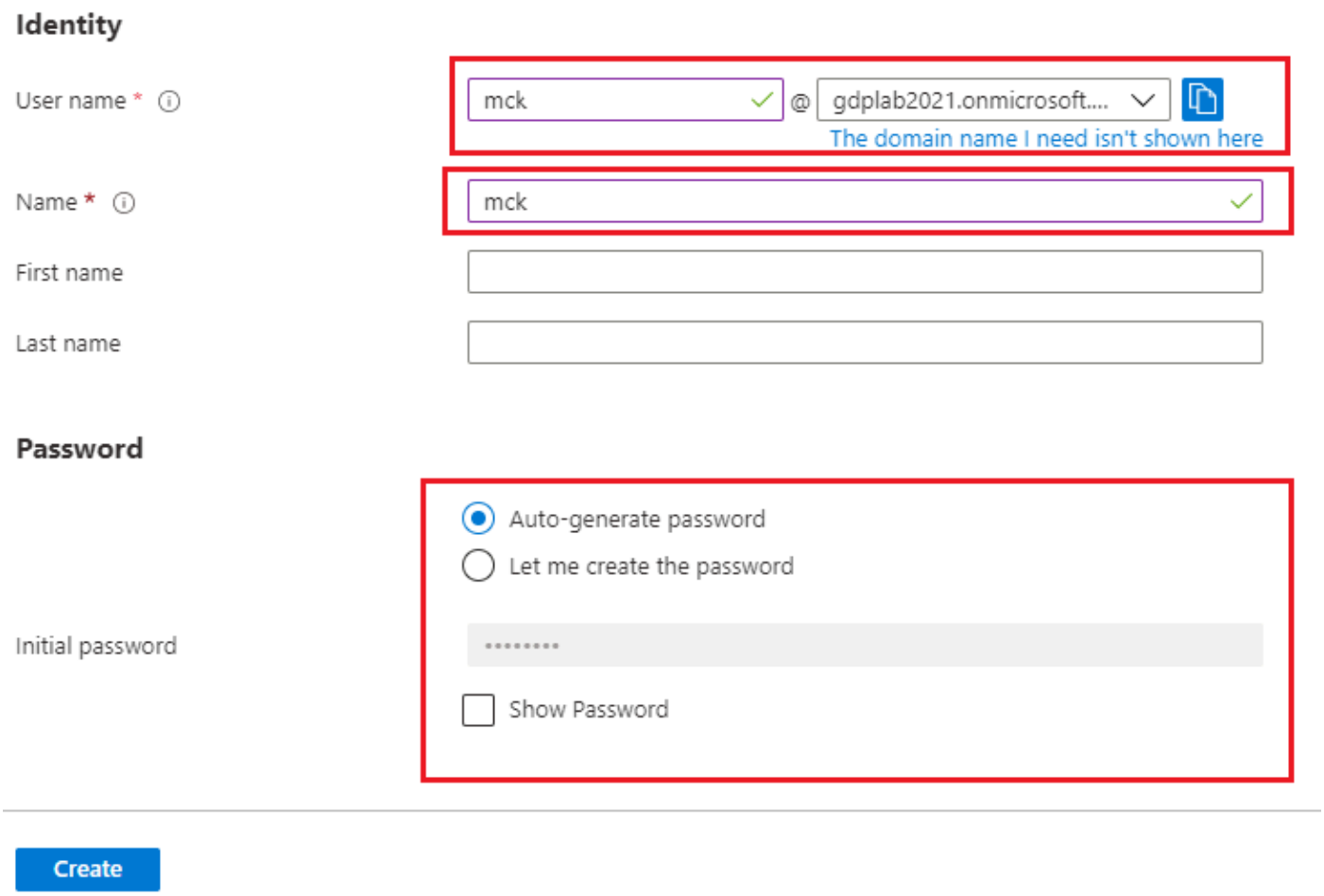
1. 建立Azure AD使用者

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



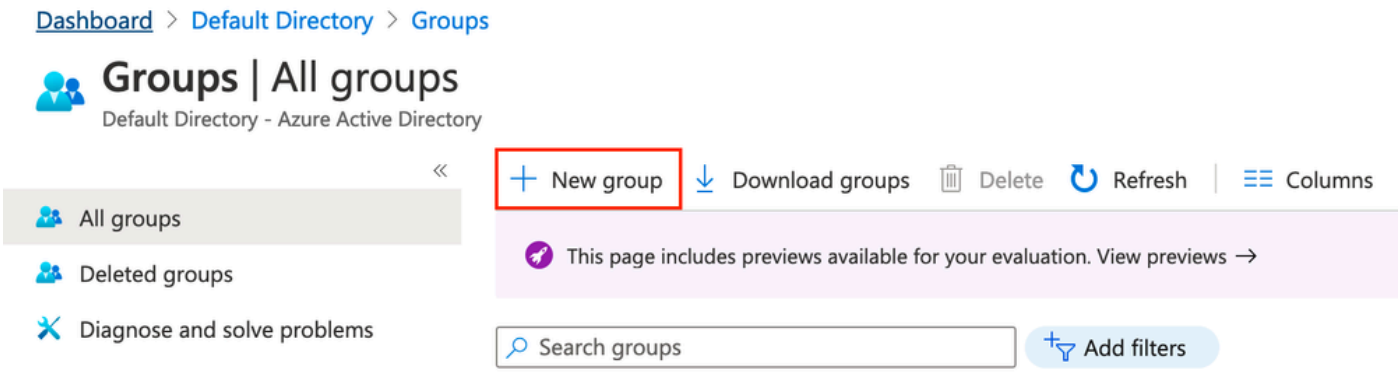
選擇使用者，點選新使用者，根據需要配置使用者名稱、名稱和初始密碼。按一下Create，如圖所

示。

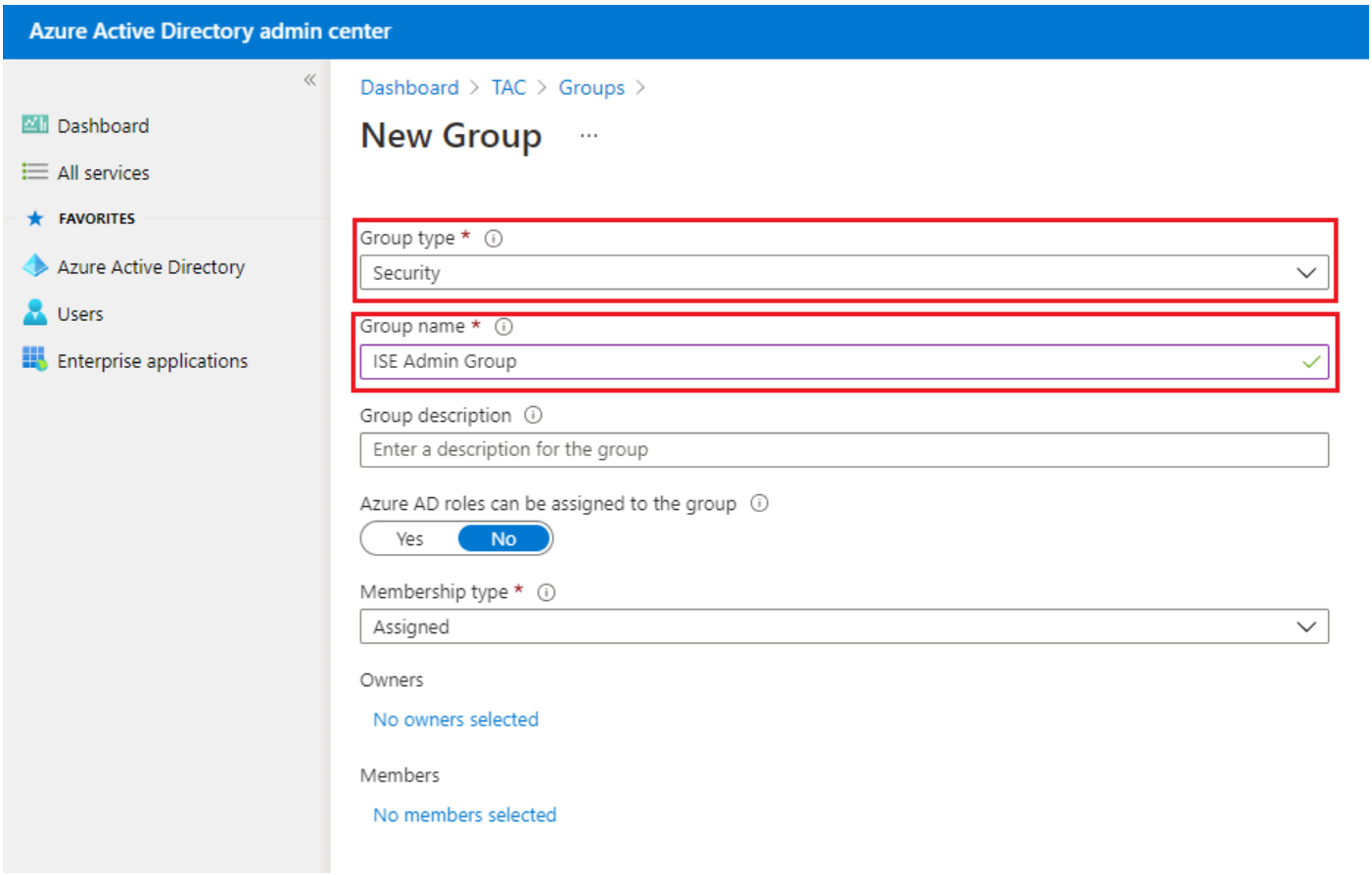


2. 建立Azure AD組

選擇組。按一下New Group。

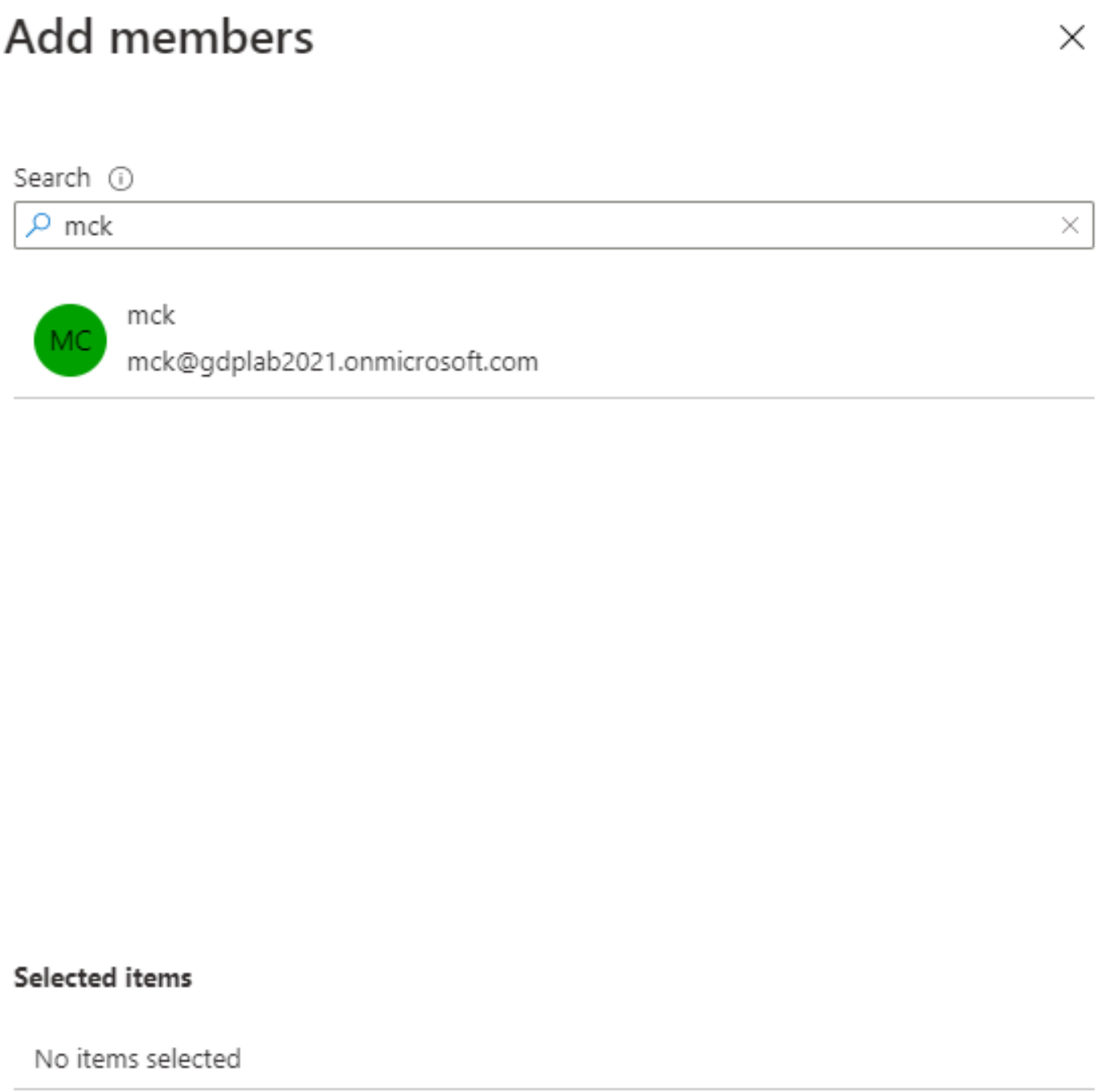


保留Group type為Security。配置Group name，如下圖所示。

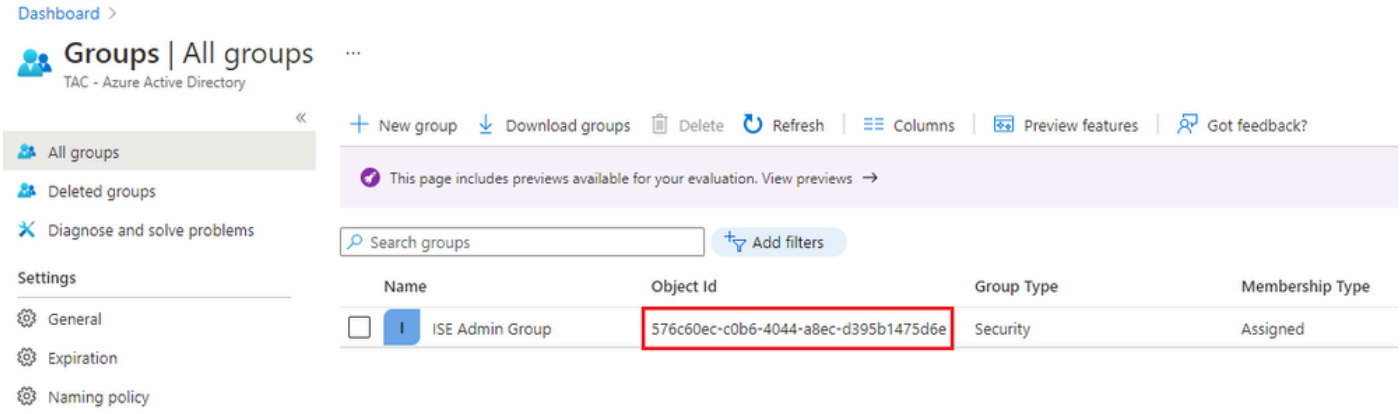


3. 將Azure AD使用者分配到組

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。

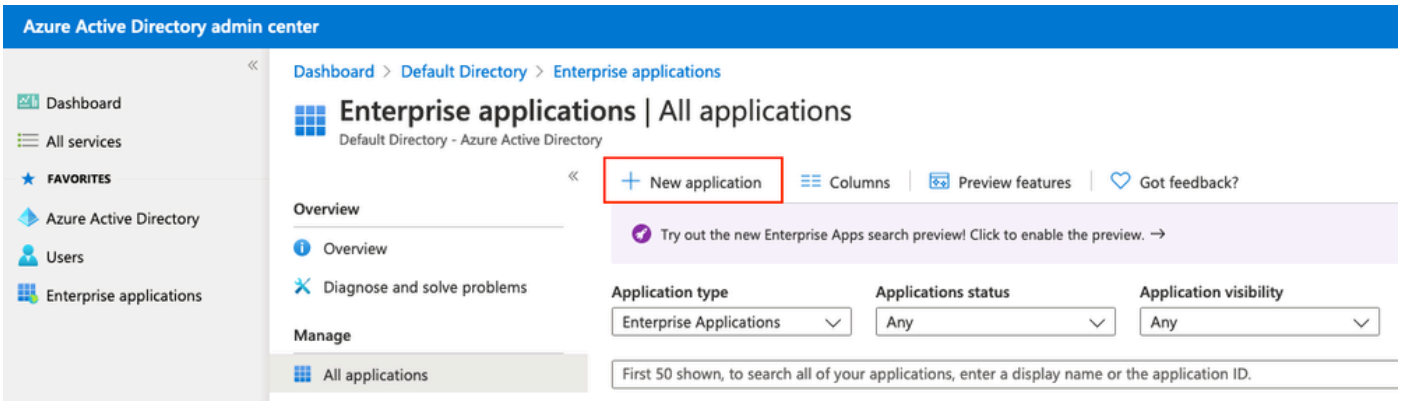


記下Group Object id，在此螢幕中為576c60ec-c0b6-4044-a8ec-d395b1475d6e，用於ISE管理組，如下圖所示。

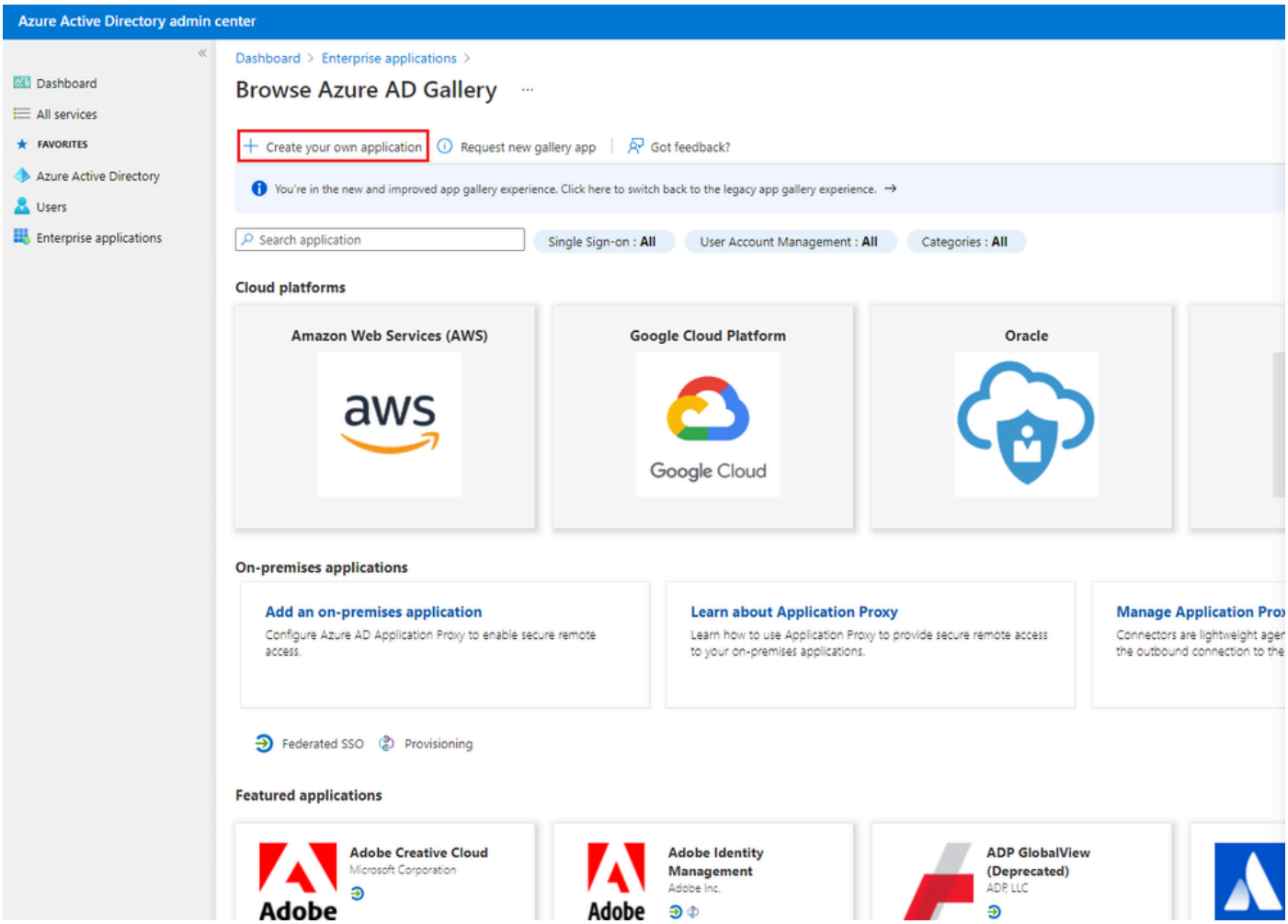


4. 建立Azure AD Enterprise應用程式

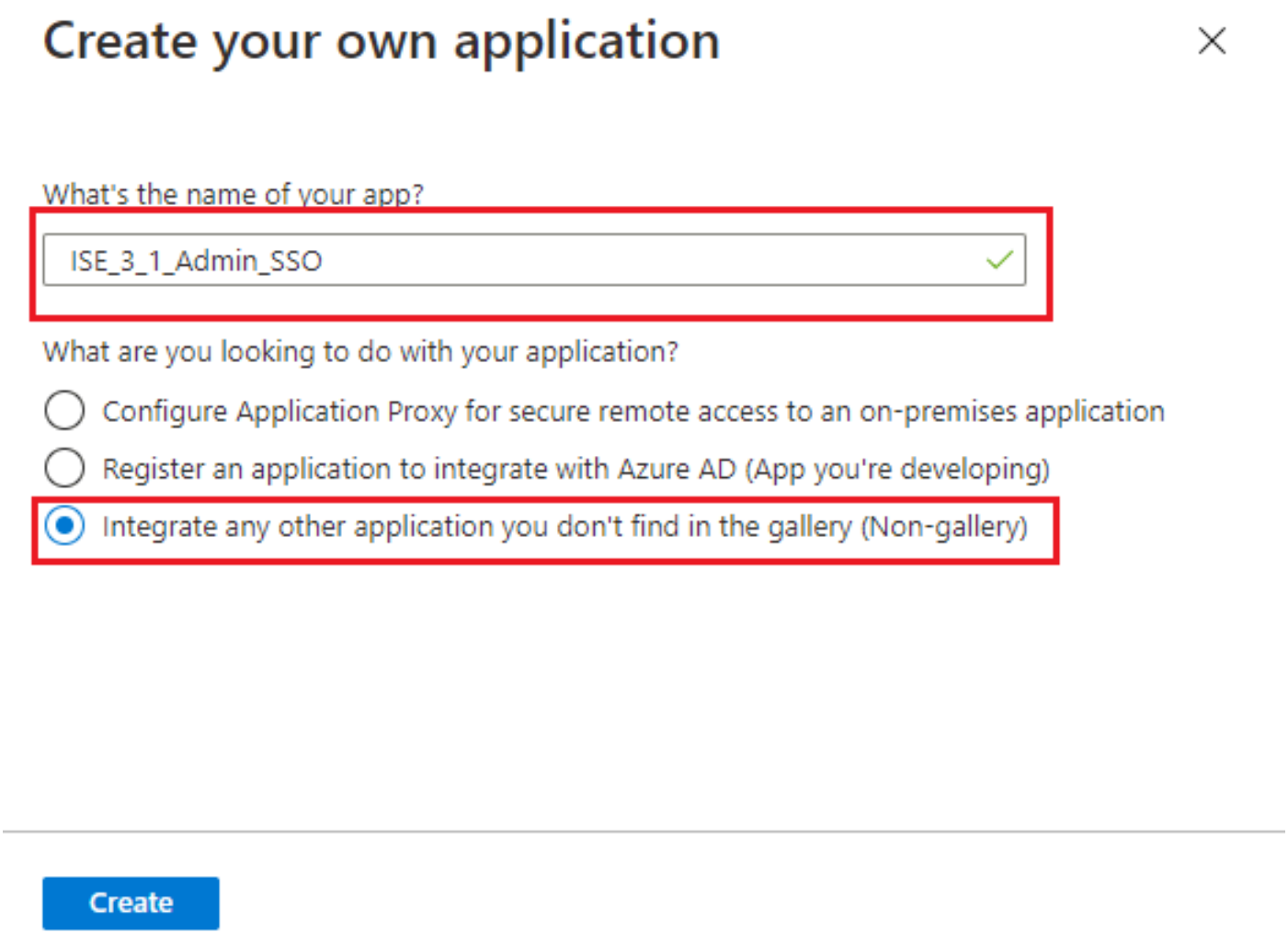
在AD下，選擇Enterprise Applications並按一下New application。



選擇Create your own application。

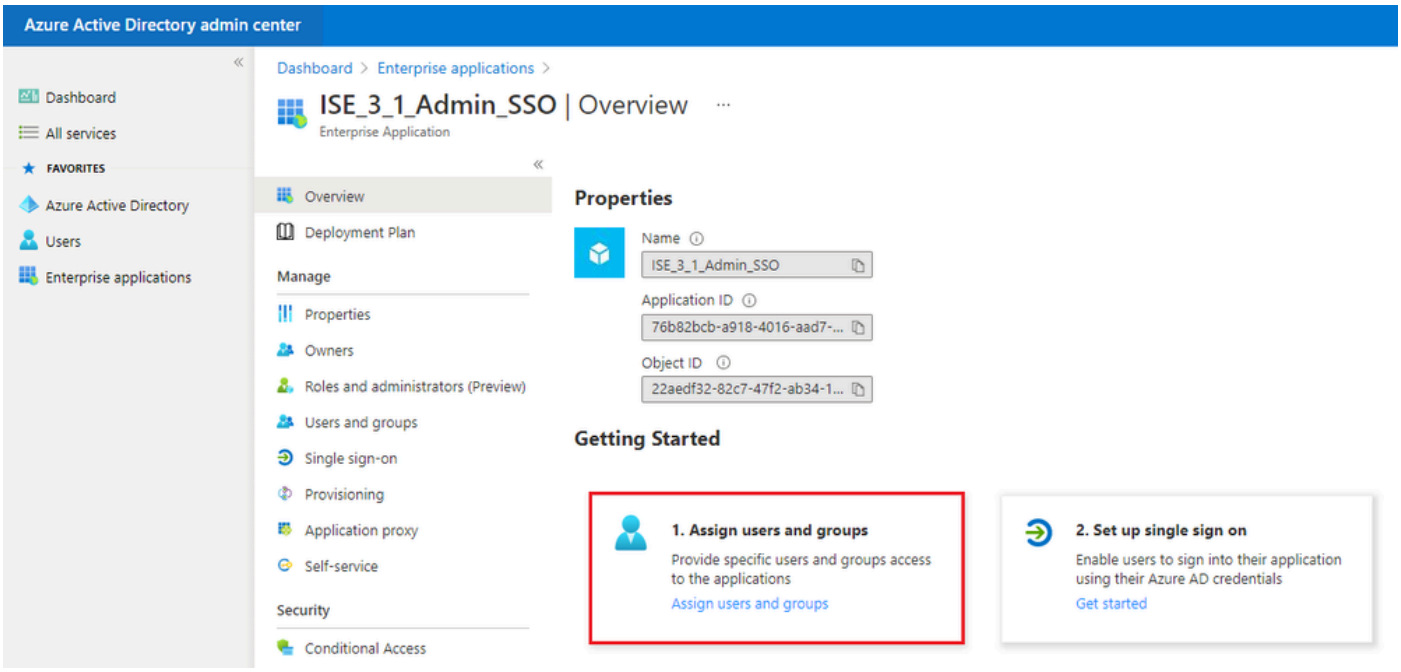


輸入應用程式的名稱，然後選取「整合在收藏館中找不到的任何其他應用程式（非收藏館）」圓鈕，再按一下「建立」按鈕（如圖所示）。

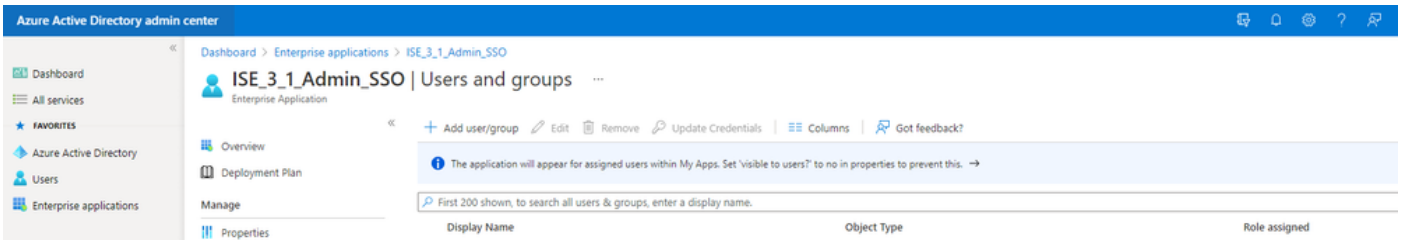


5. 將群組新增至應用程式

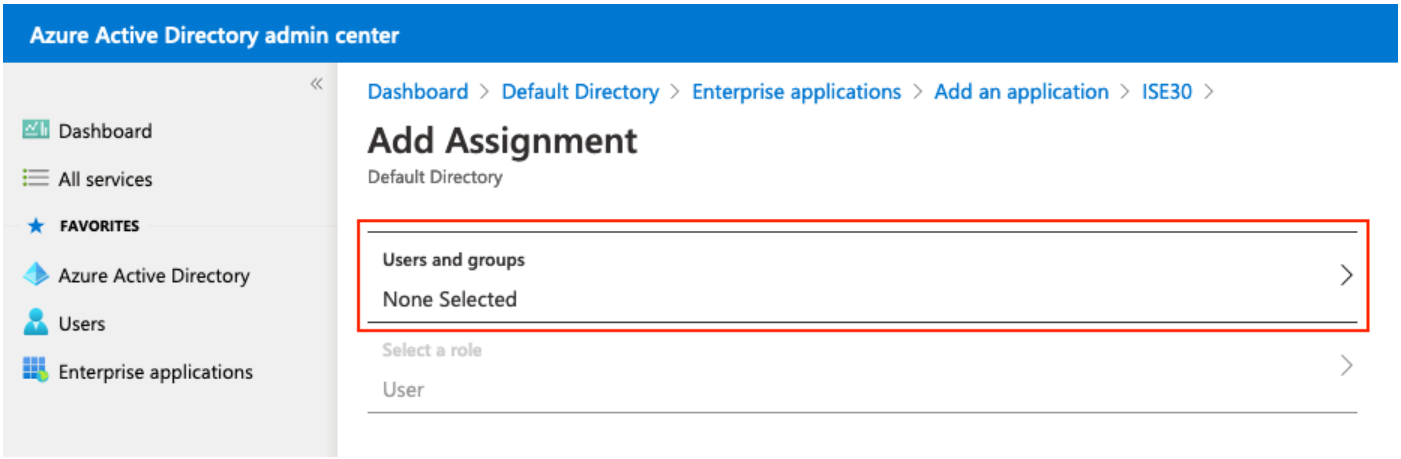
選擇分配使用者和組。



按一下Add user/group。



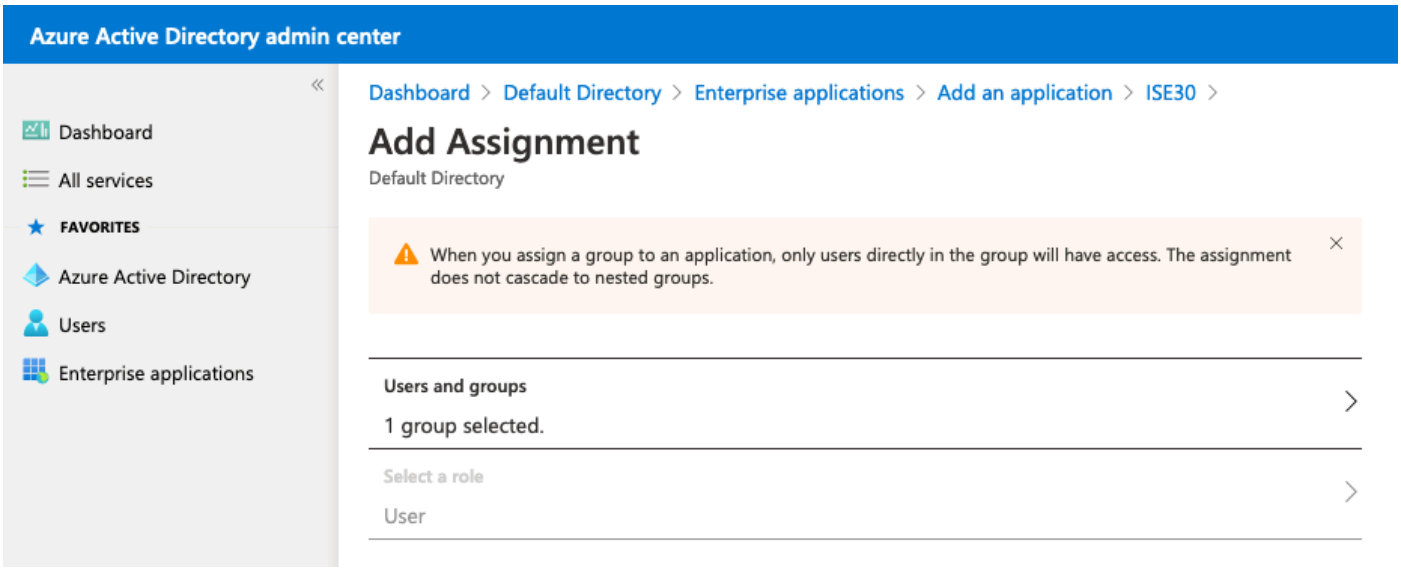
按一下Users and groups。



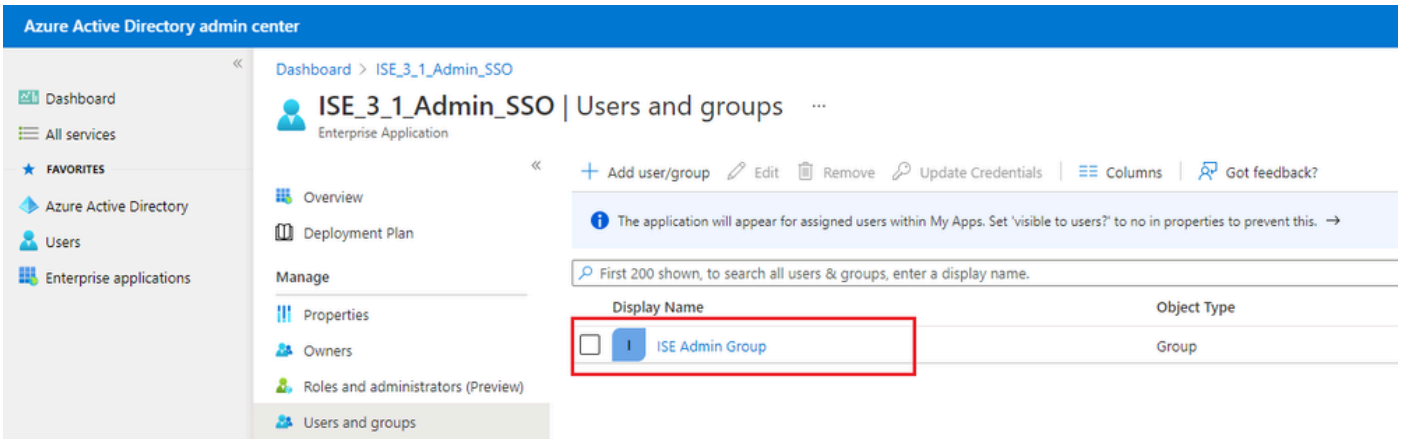
選擇先前配置的組，然後按一下選擇。

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。

選擇組後，按一下Assign。

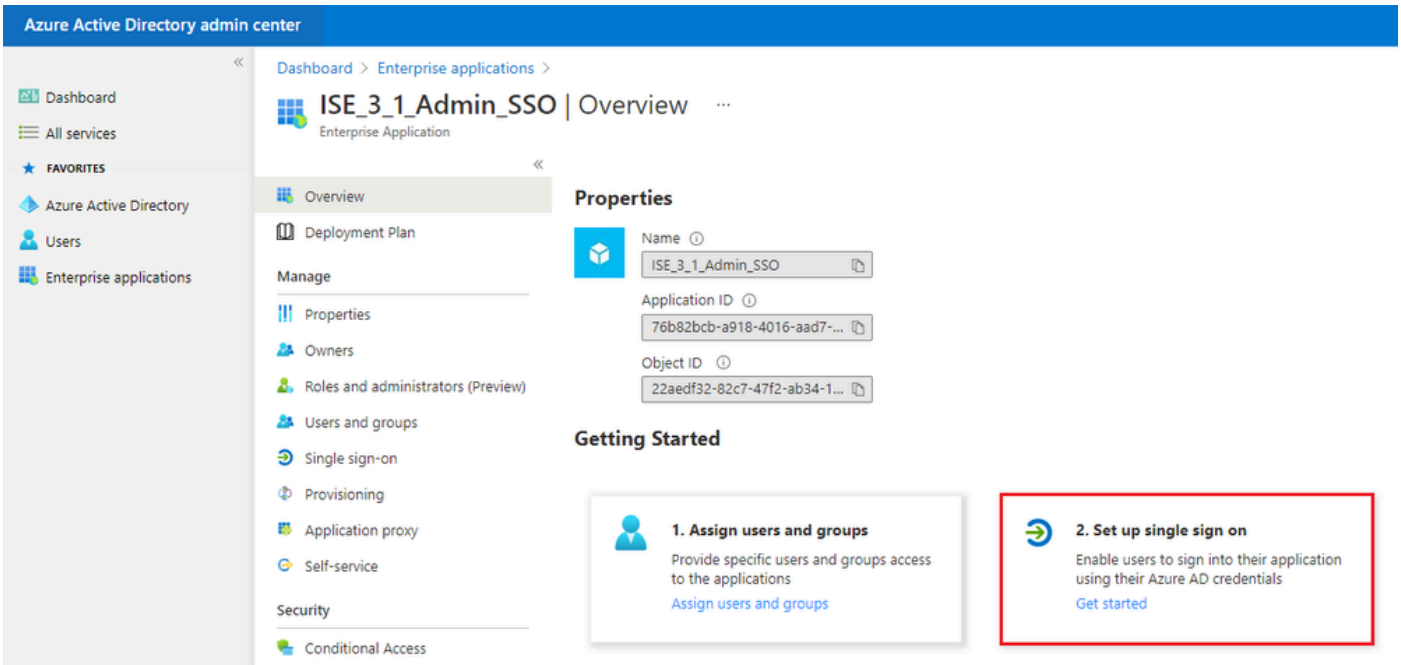


因此，配置的應用程式的使用者和組選單會填充所選的組。

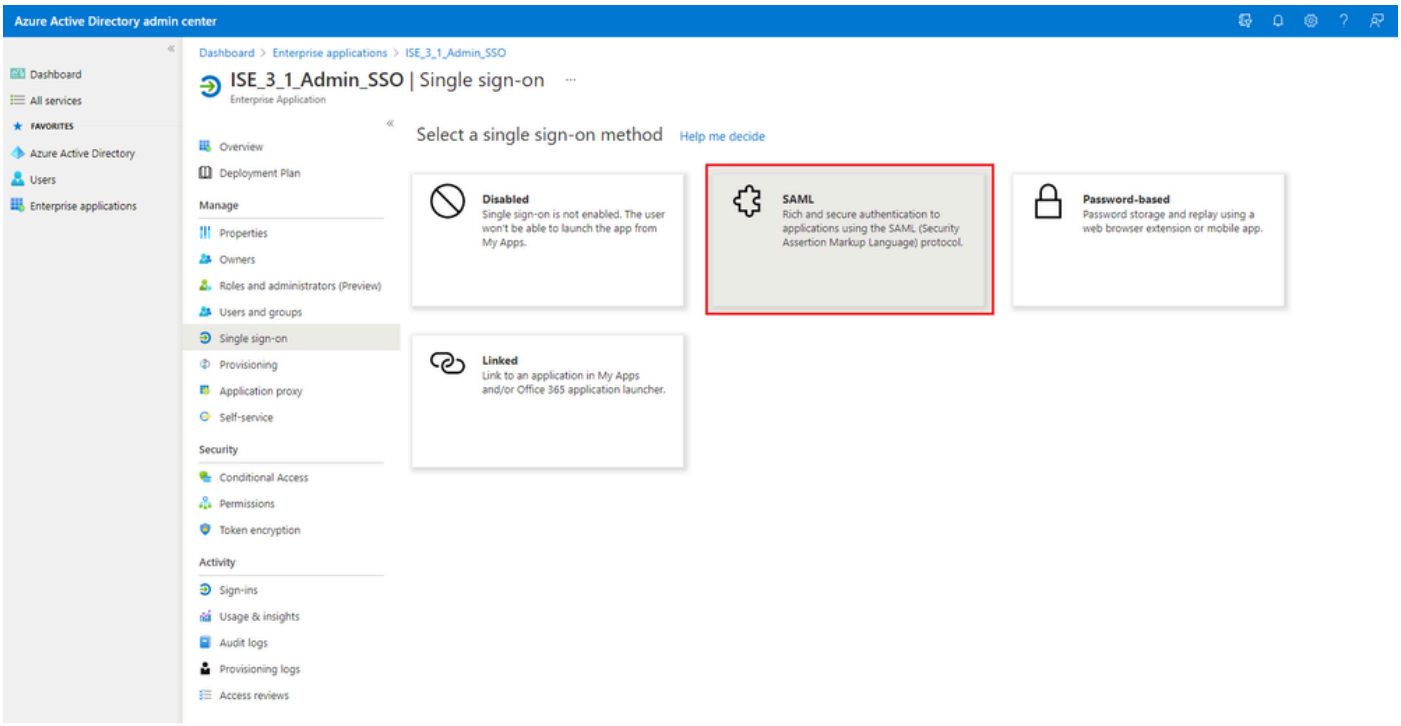


6. 配置Azure AD Enterprise應用程式

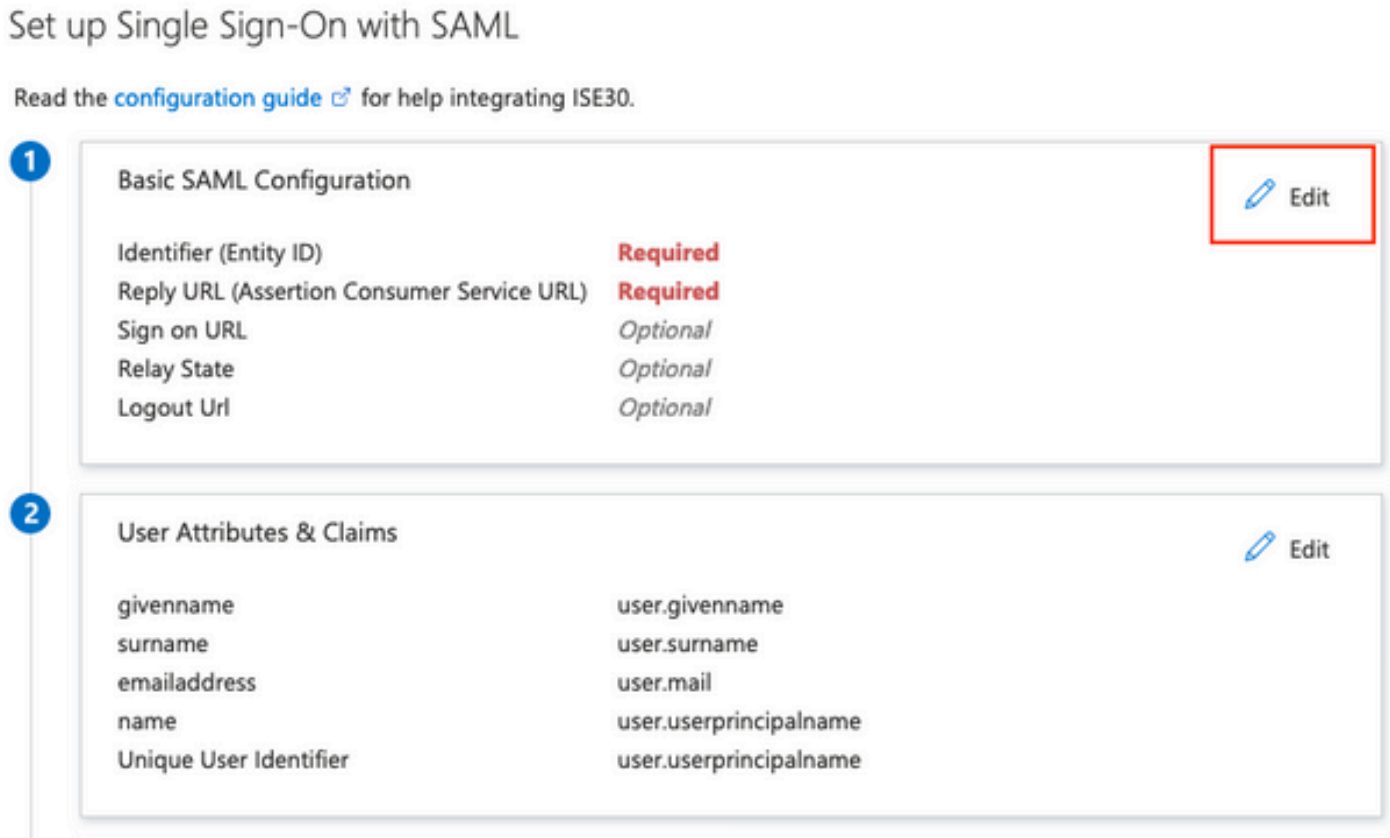
導航回您的應用程式，然後按一下Set up single sign on。



在下一個螢幕中選擇SAML。

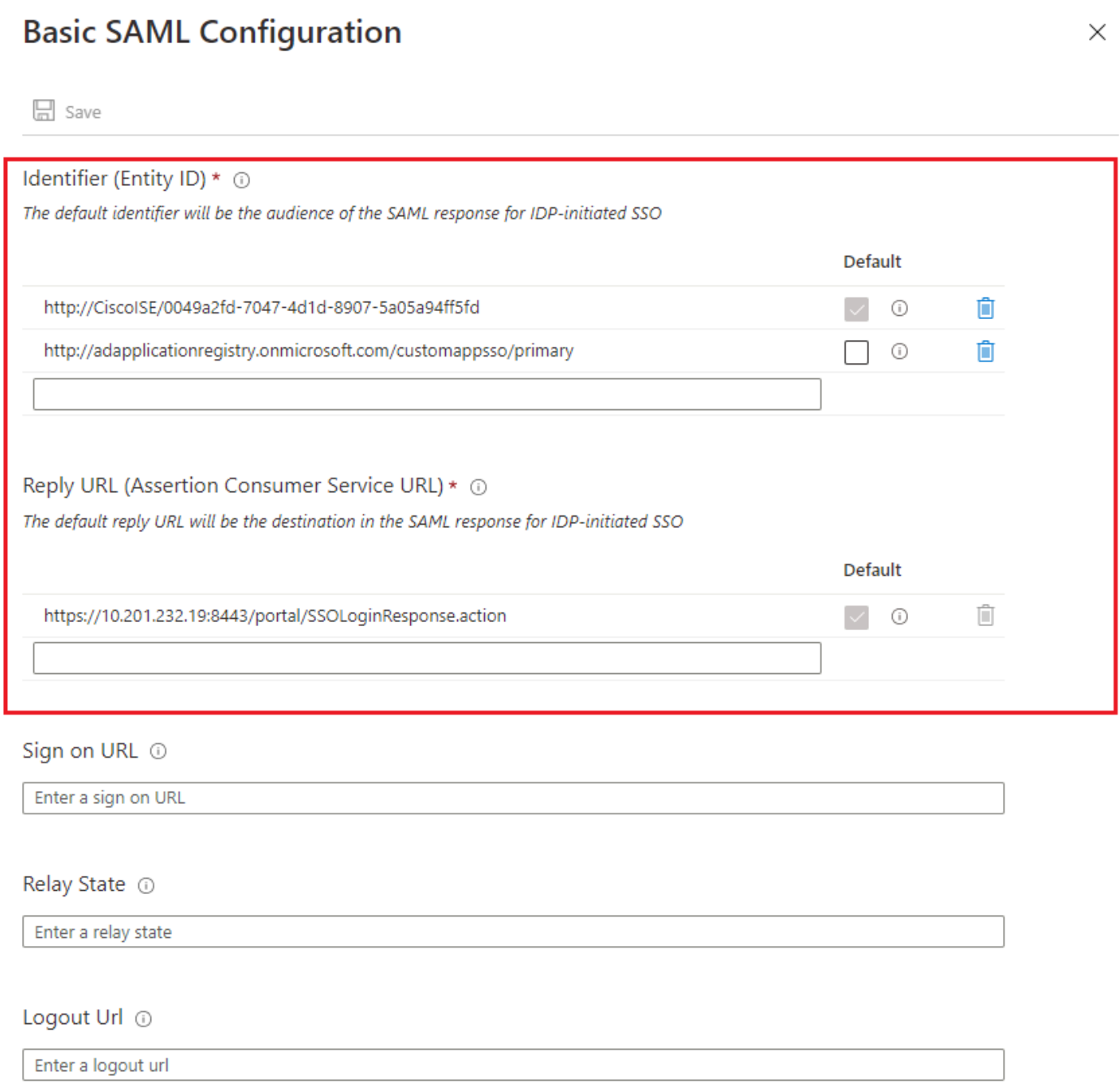


按一下Basic SAML Configuration旁邊的Edit。



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。

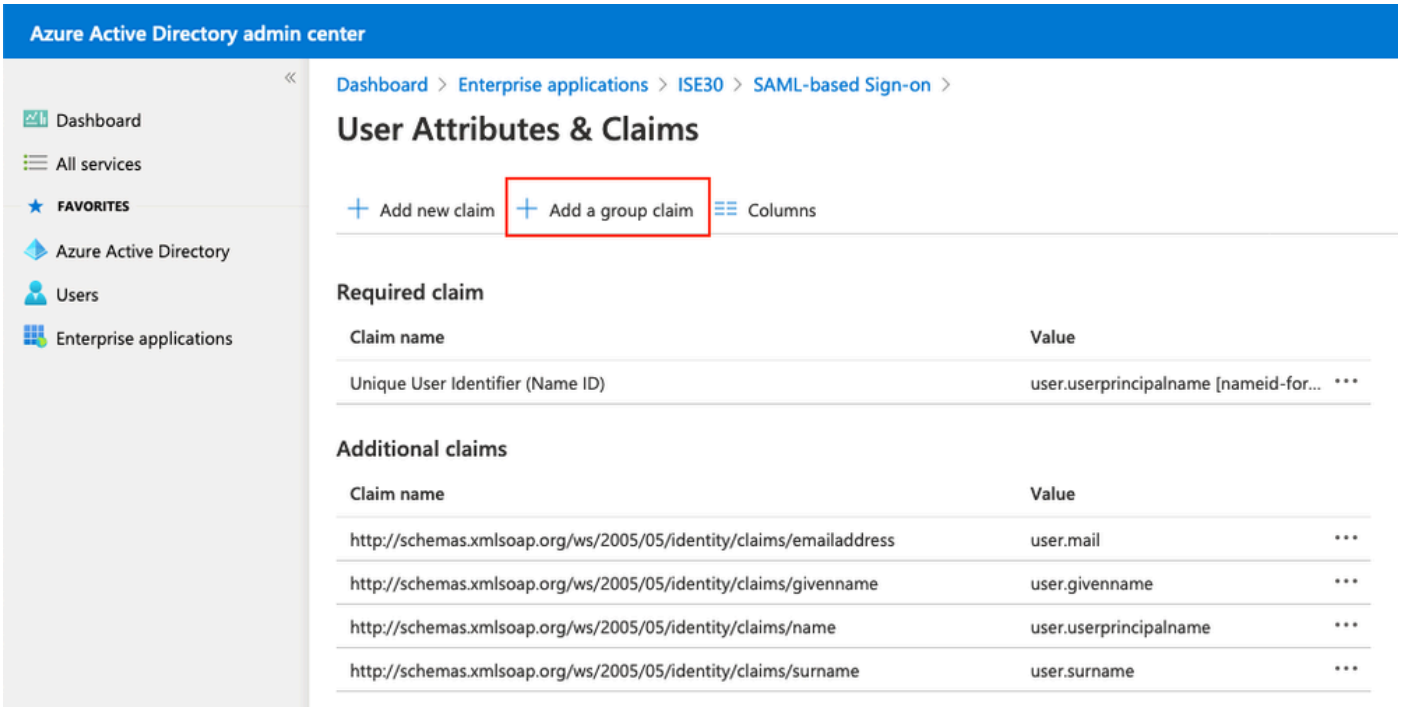
附註：回覆URL會作為傳遞清單，當重新導向至IdP頁面時，允許特定URL作為來源。



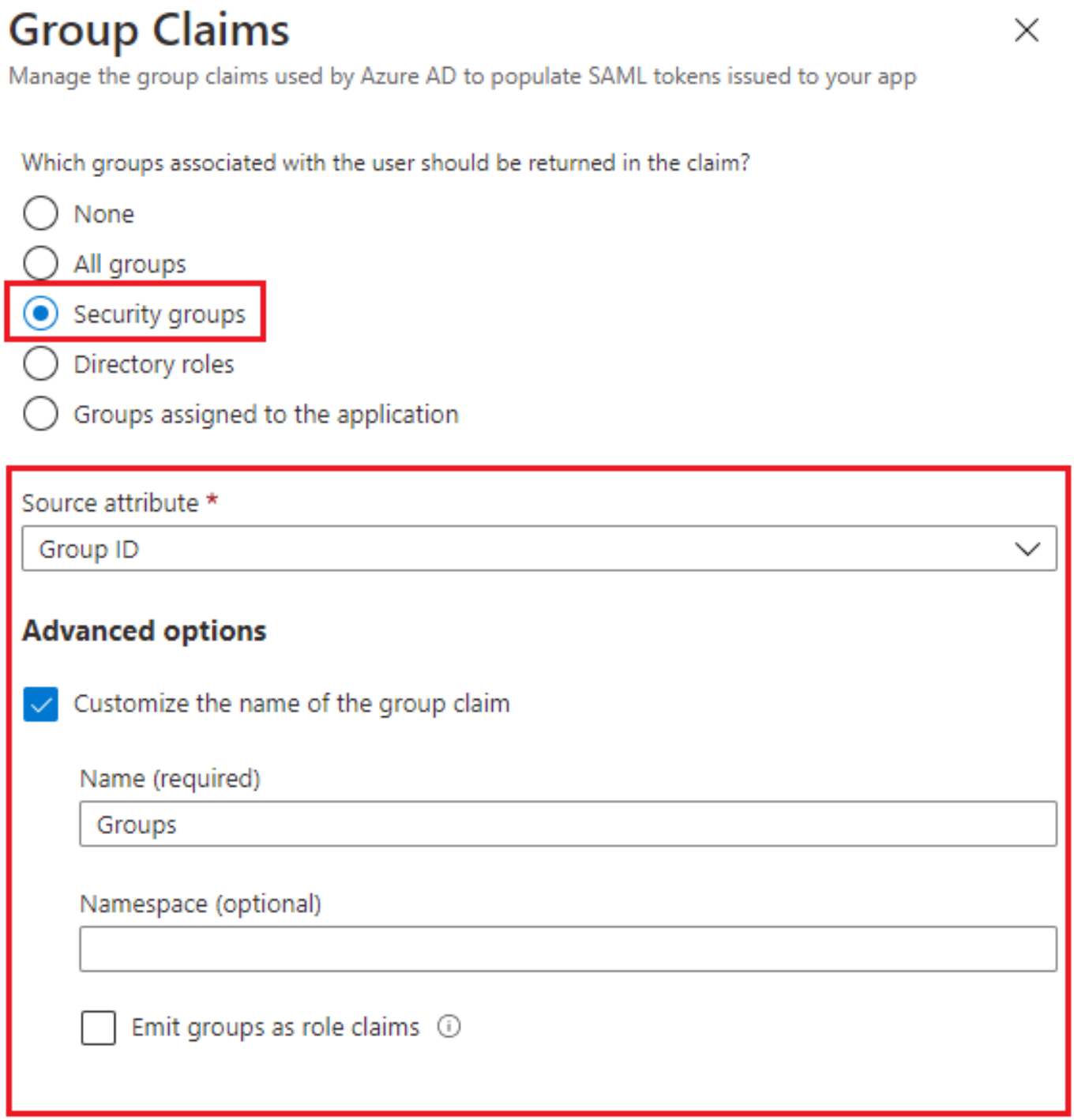
7. 配置Active Directory組屬性

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

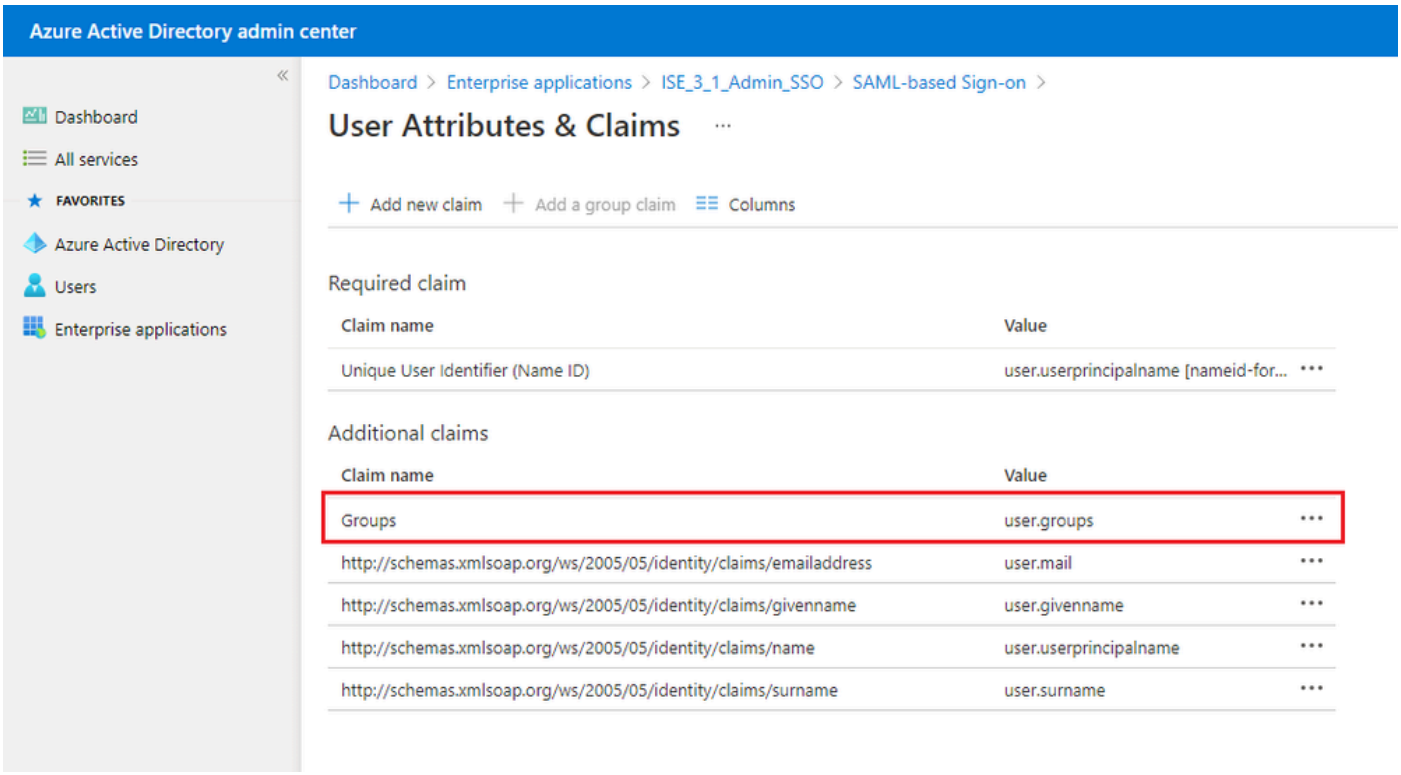
按一下Add a group claim。



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

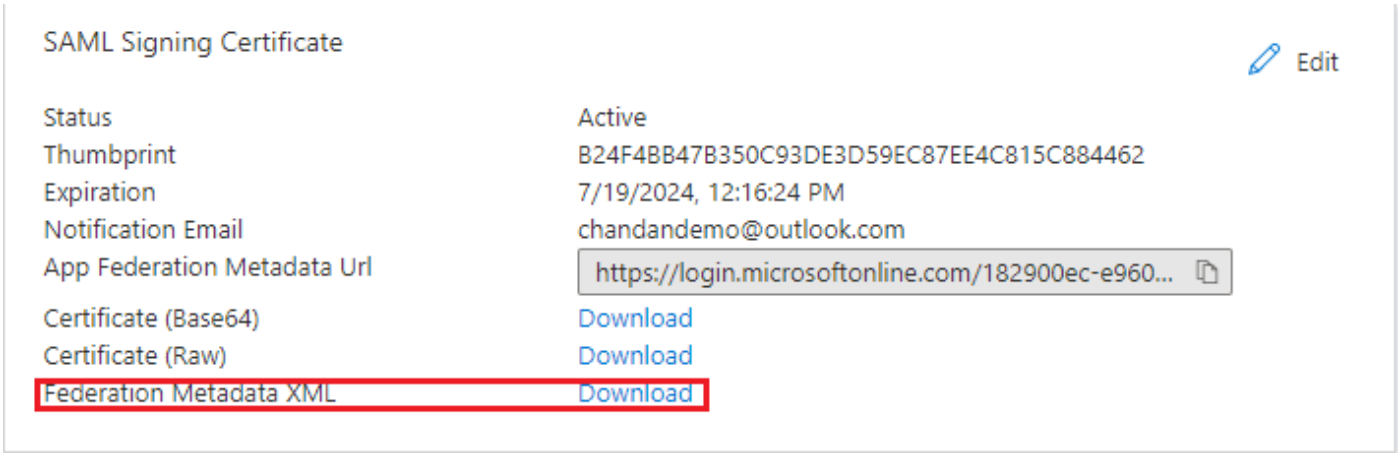


記下該組的領款申請名稱。在本示例中，它是Groups。



8. 下載Azure Federation後設資料XML檔案

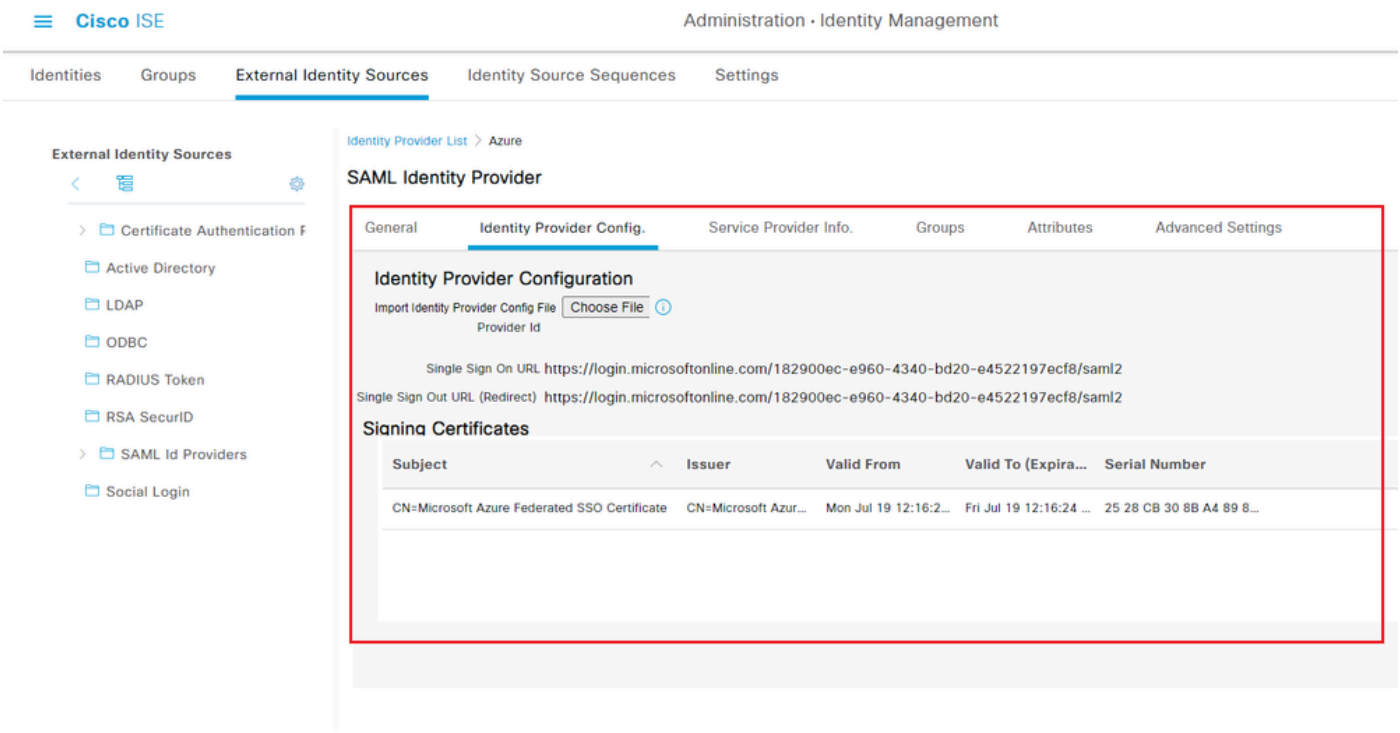
針對SAML簽名證書中的聯合後設資料XML按一下下載。



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

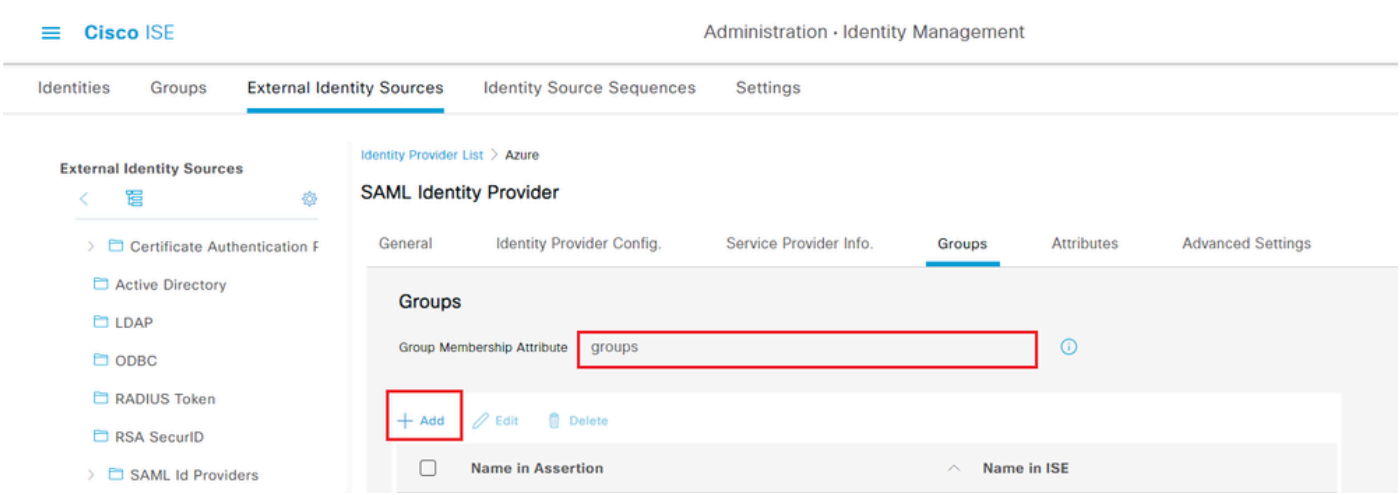
導航到管理>身份管理>外部身份源 > SAML Id提供程式> [您的SAML提供程式]。

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。



步驟 4.在ISE上配置SAML組

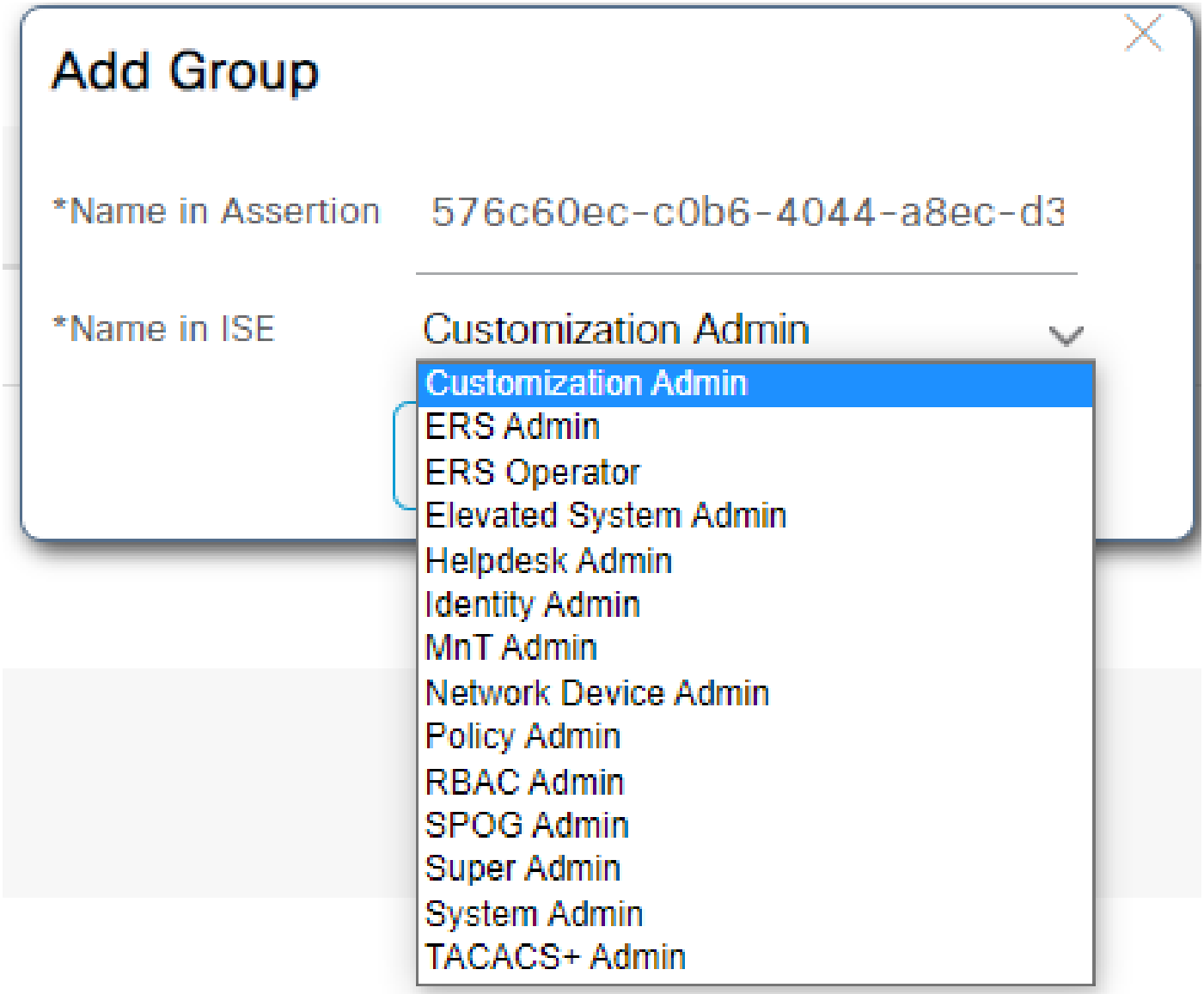
切換到頁籤Groups，然後將Claim name的值從Configure Active Directory Group attribute貼上到Group Membership Attribute。



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。

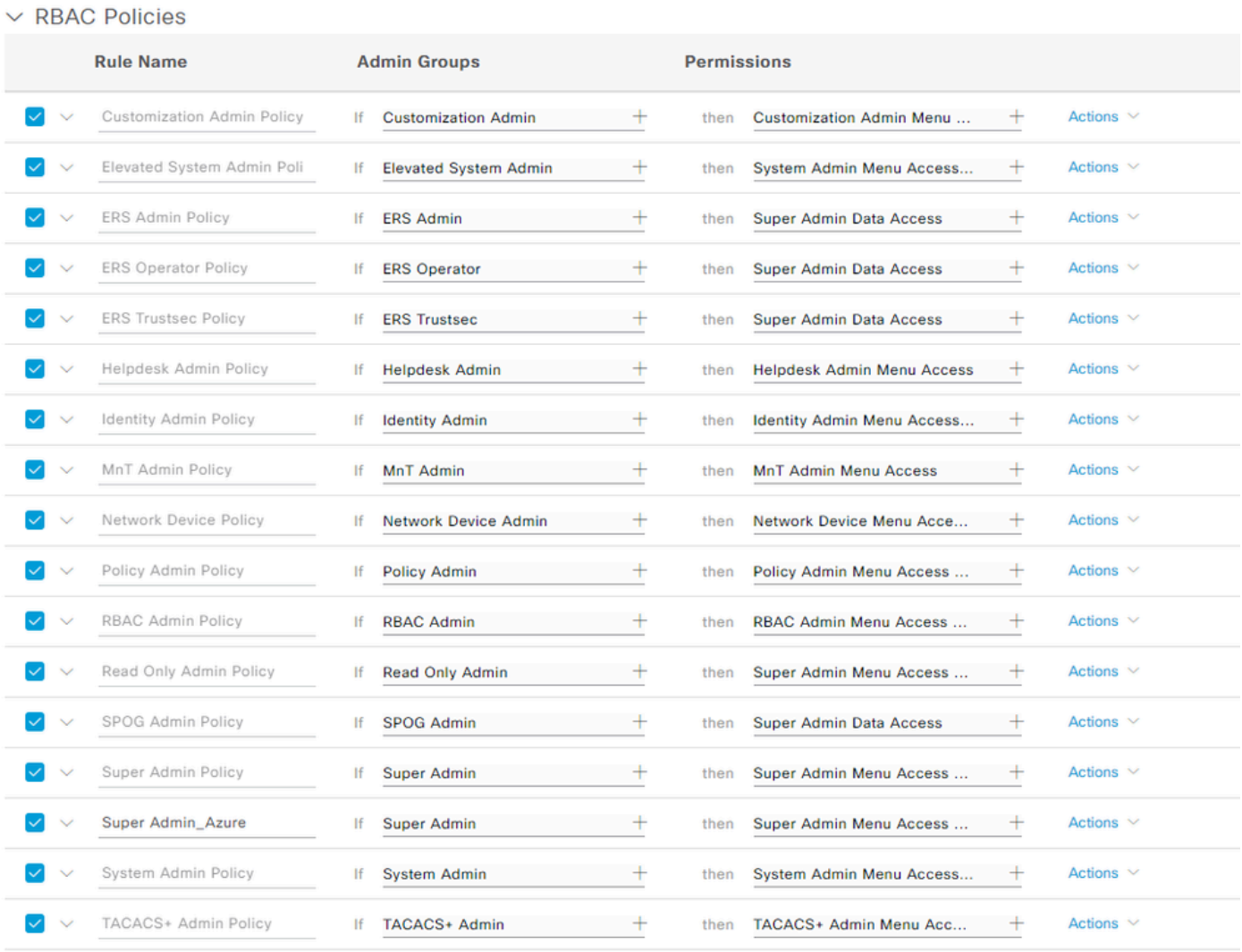


（可選）步驟5。配置RBAC策略

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。



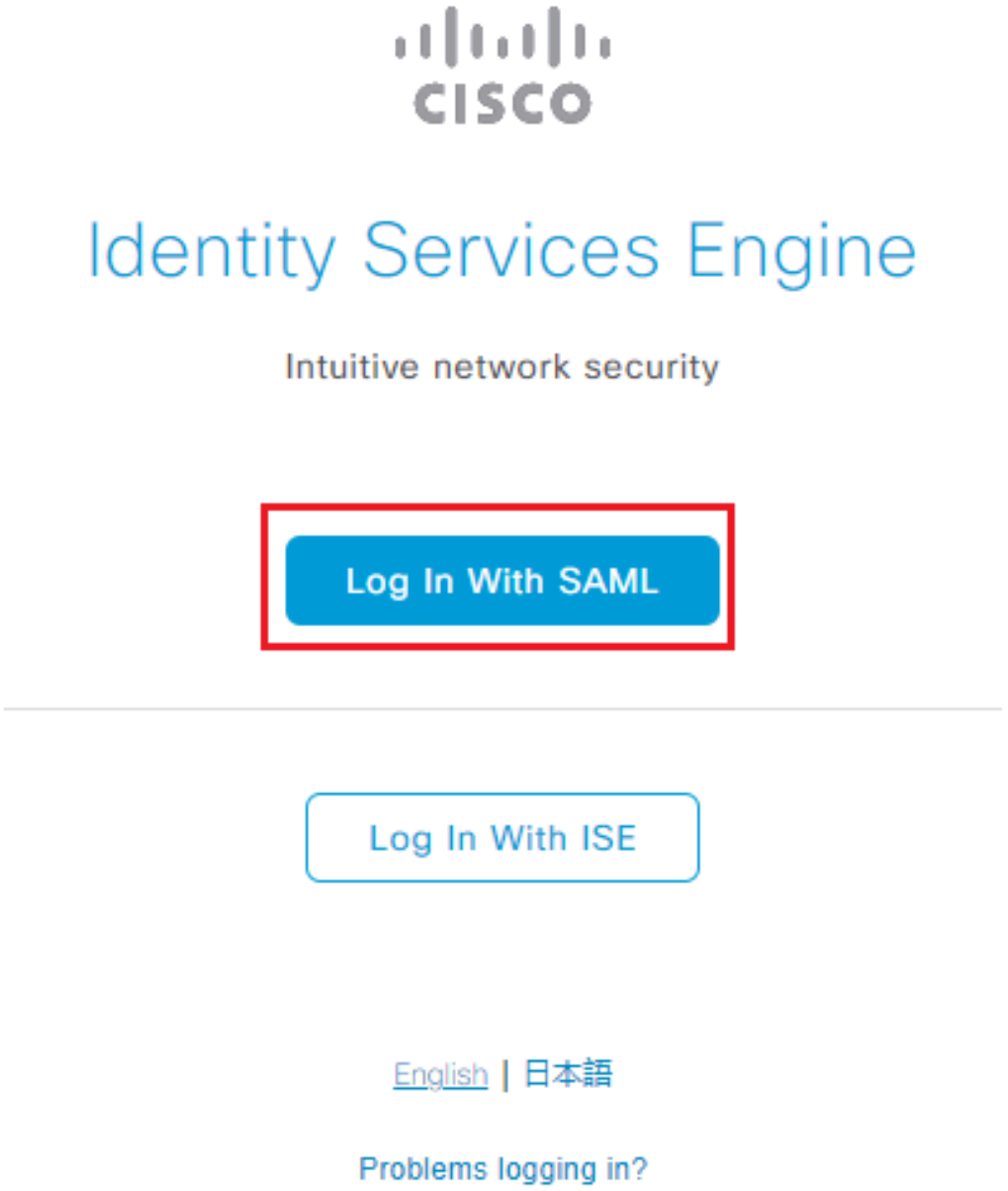
驗證

確認您的組態是否正常運作。

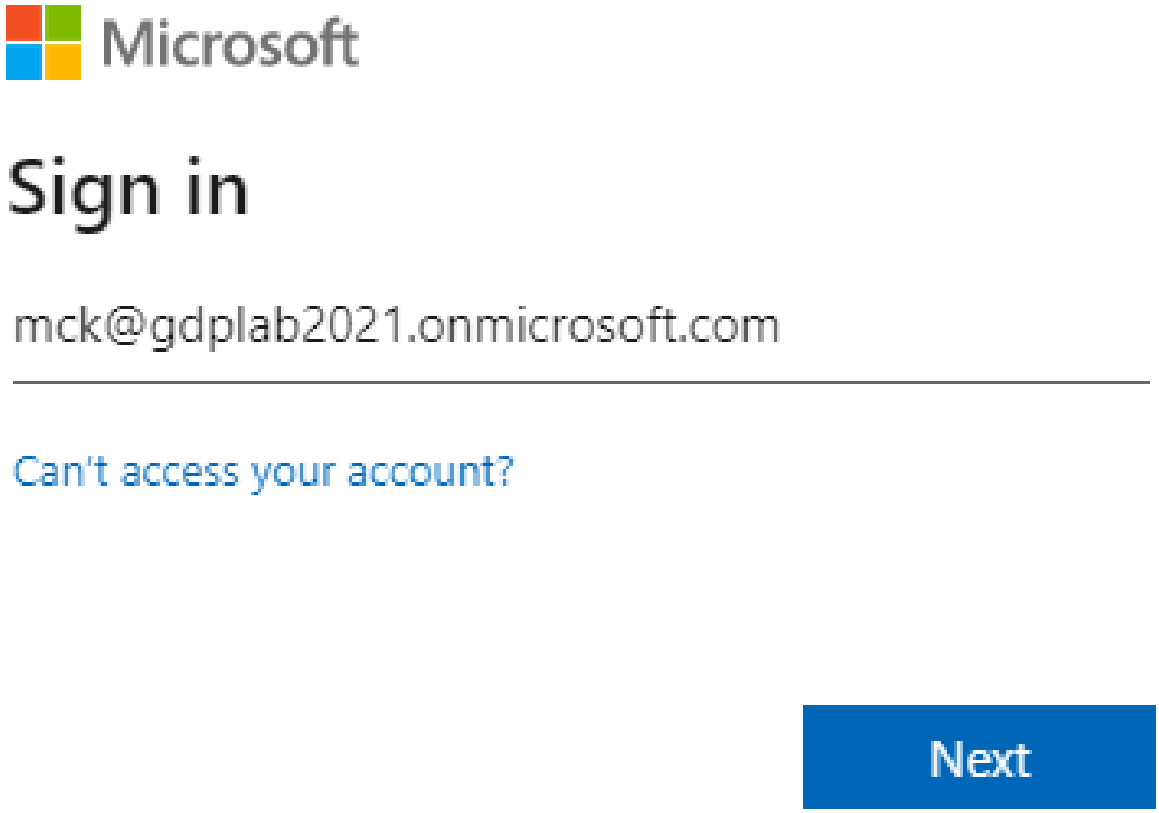
注意：Azure測試功能的SAML SSO登入測試不起作用。SAML請求必須由ISE啟動，Azure SAML SSO才能正常工作。

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。

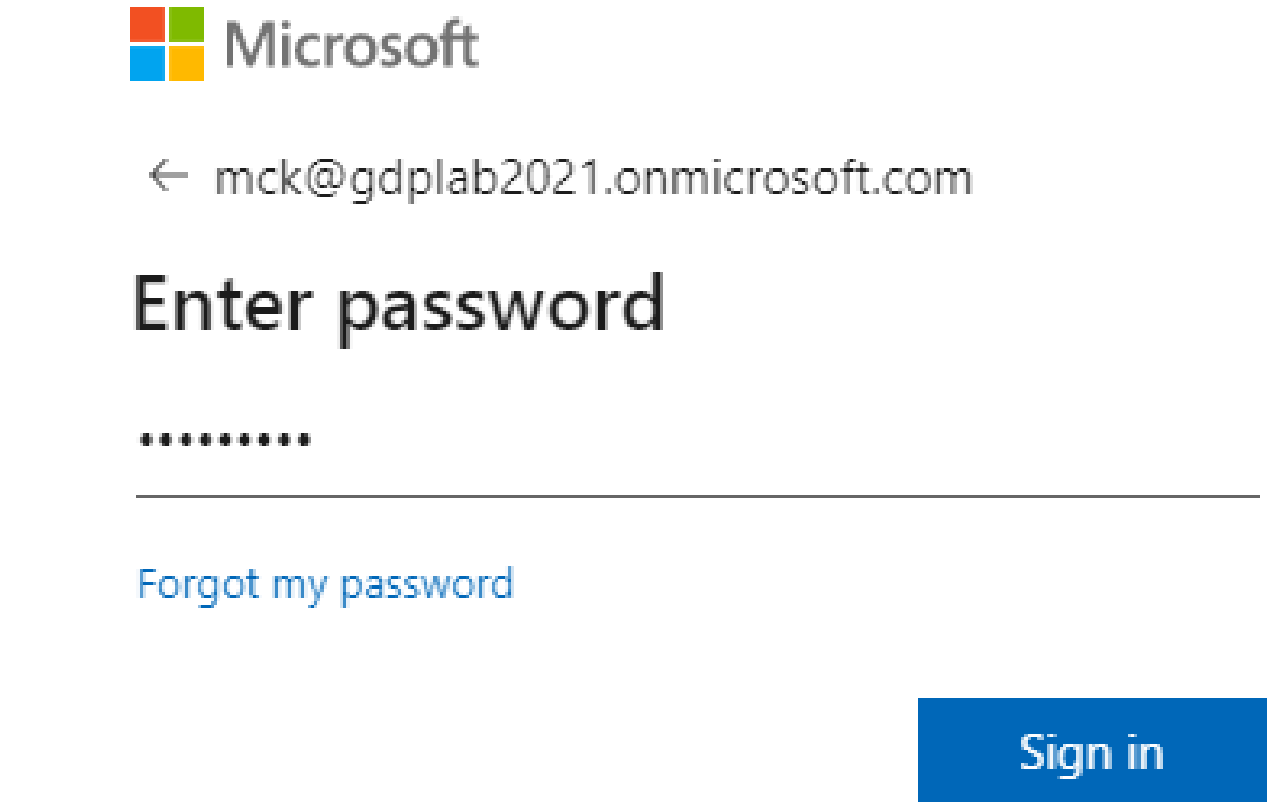
1. 訪問您的ISE GUI登入頁並按一下Log In with SAML。



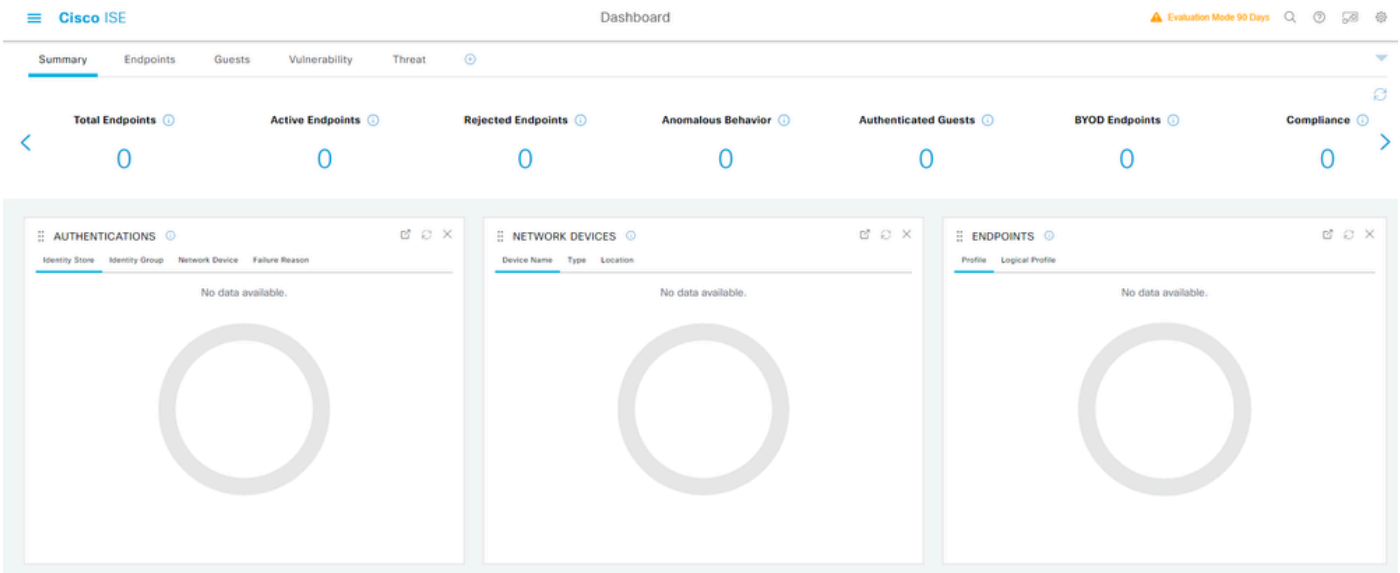
2. 系統會將您重新導向至Microsoft登入畫面。輸入對映到ISE的組中帳戶的使用者名稱憑據（如圖所示），然後按一下Next（如圖所示）。



3. 輸入使用者的密碼，然後按一下「登入」。



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

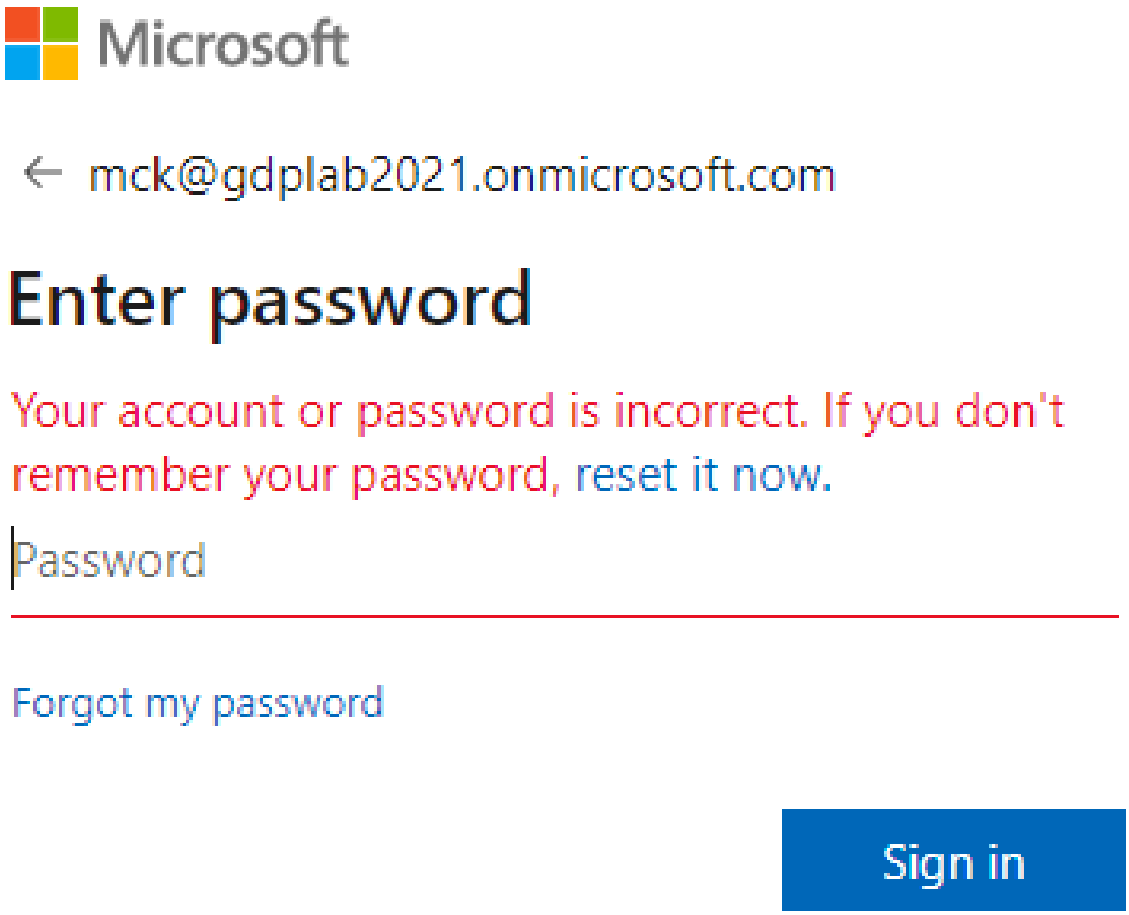
本節提供的資訊可用於對組態進行疑難排解。

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。

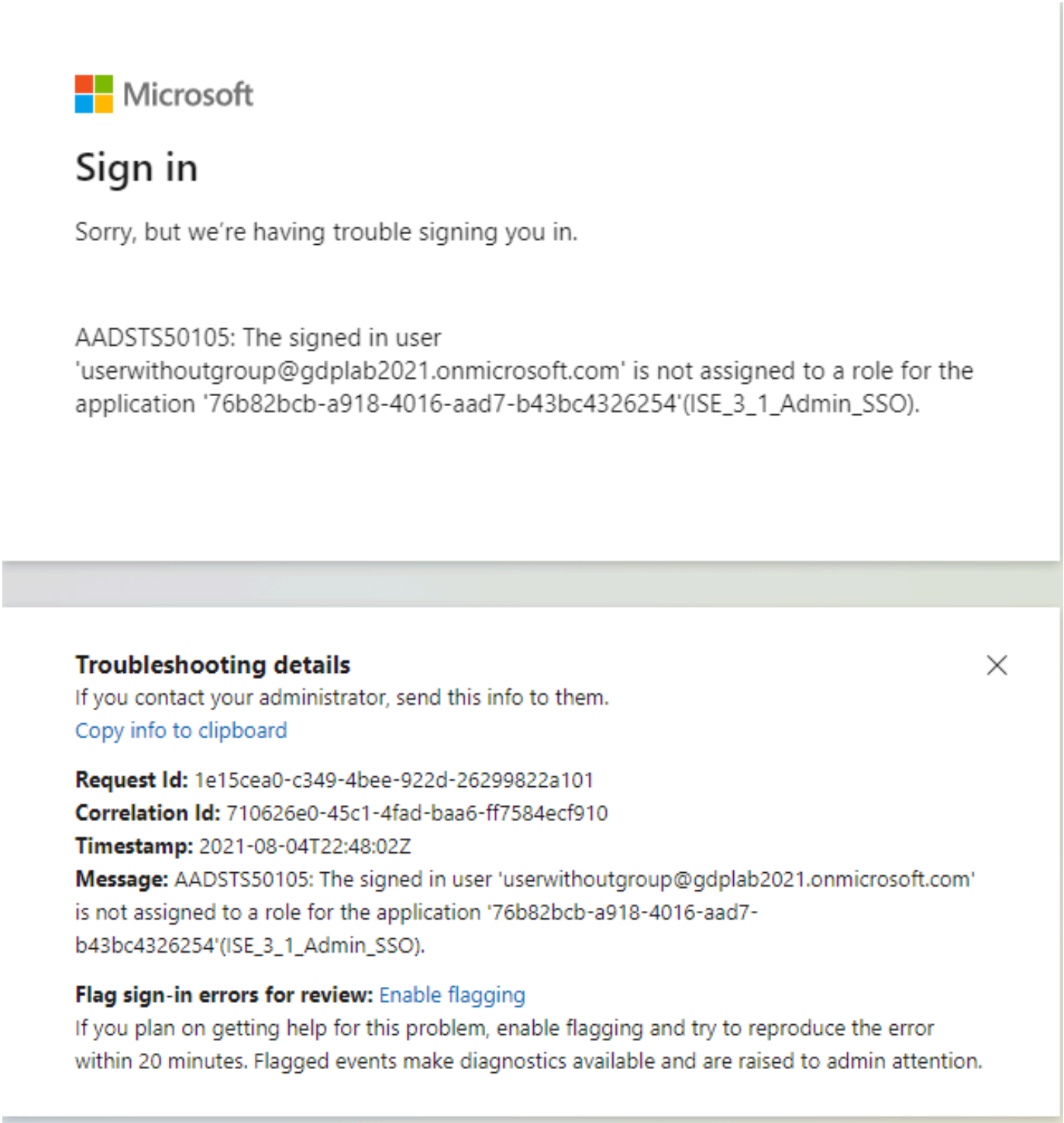
問題1：輸入憑據後出現「您的帳戶或密碼不正確」錯誤。此處，ISE尚未接收使用者資料，此時進程仍保留在IdP (Azure)中。

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。

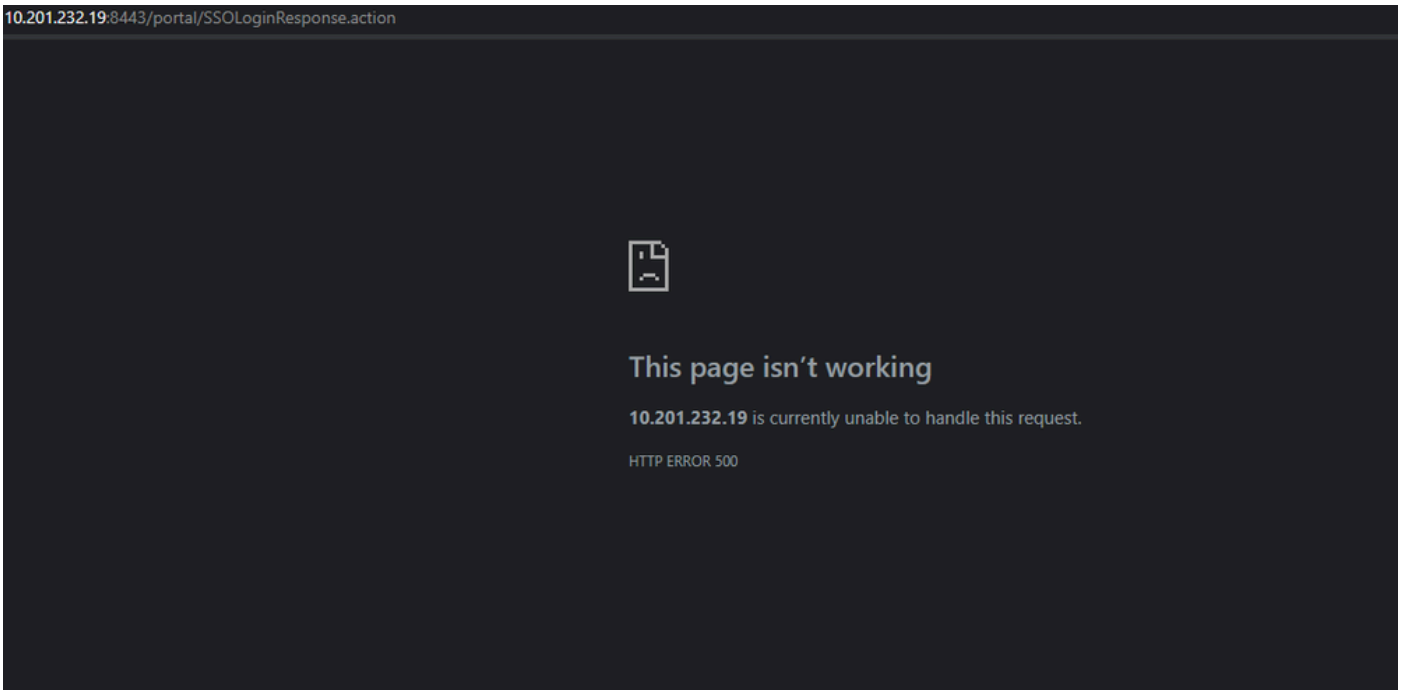


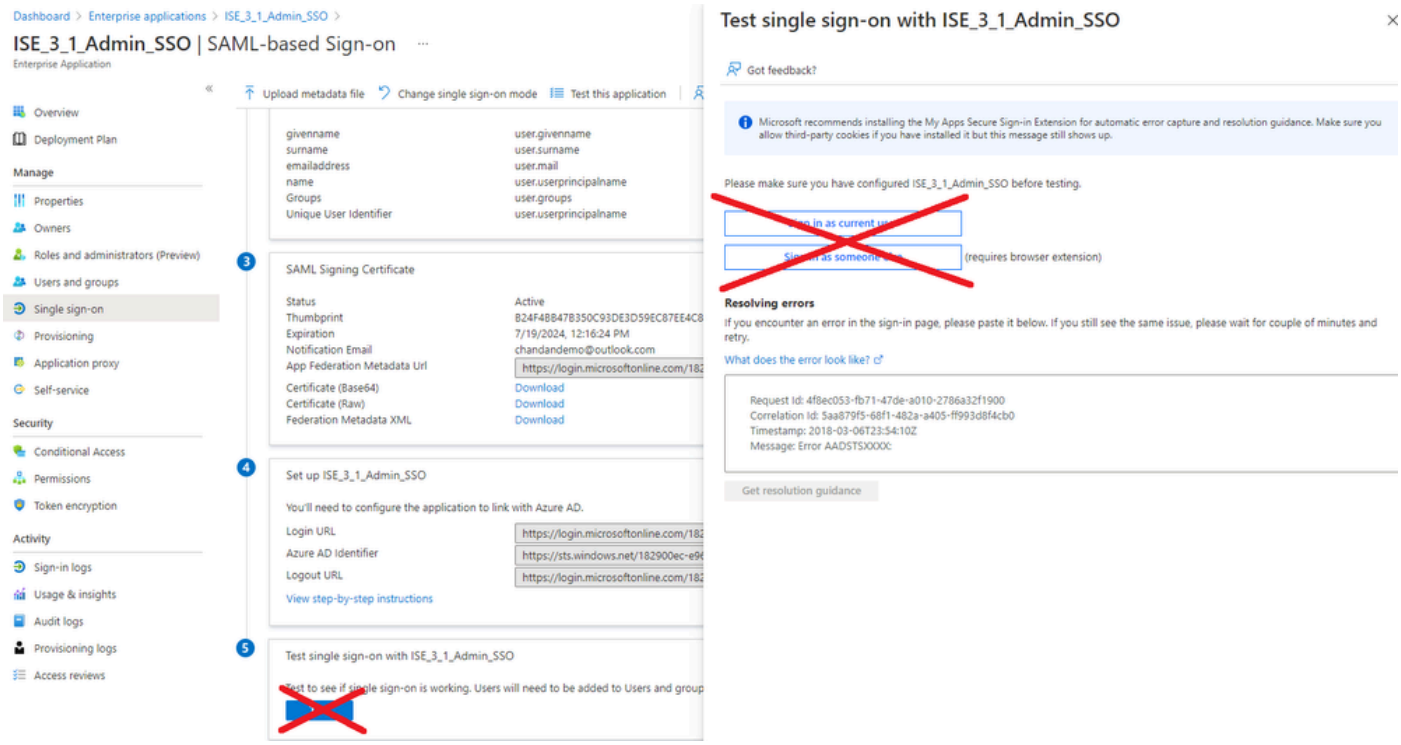
問題2.使用者不屬於應該允許存取SAML SSO的群組。與之前的情況類似，ISE尚未接收使用者資料，此時進程仍使用IdP (Azure)。

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。



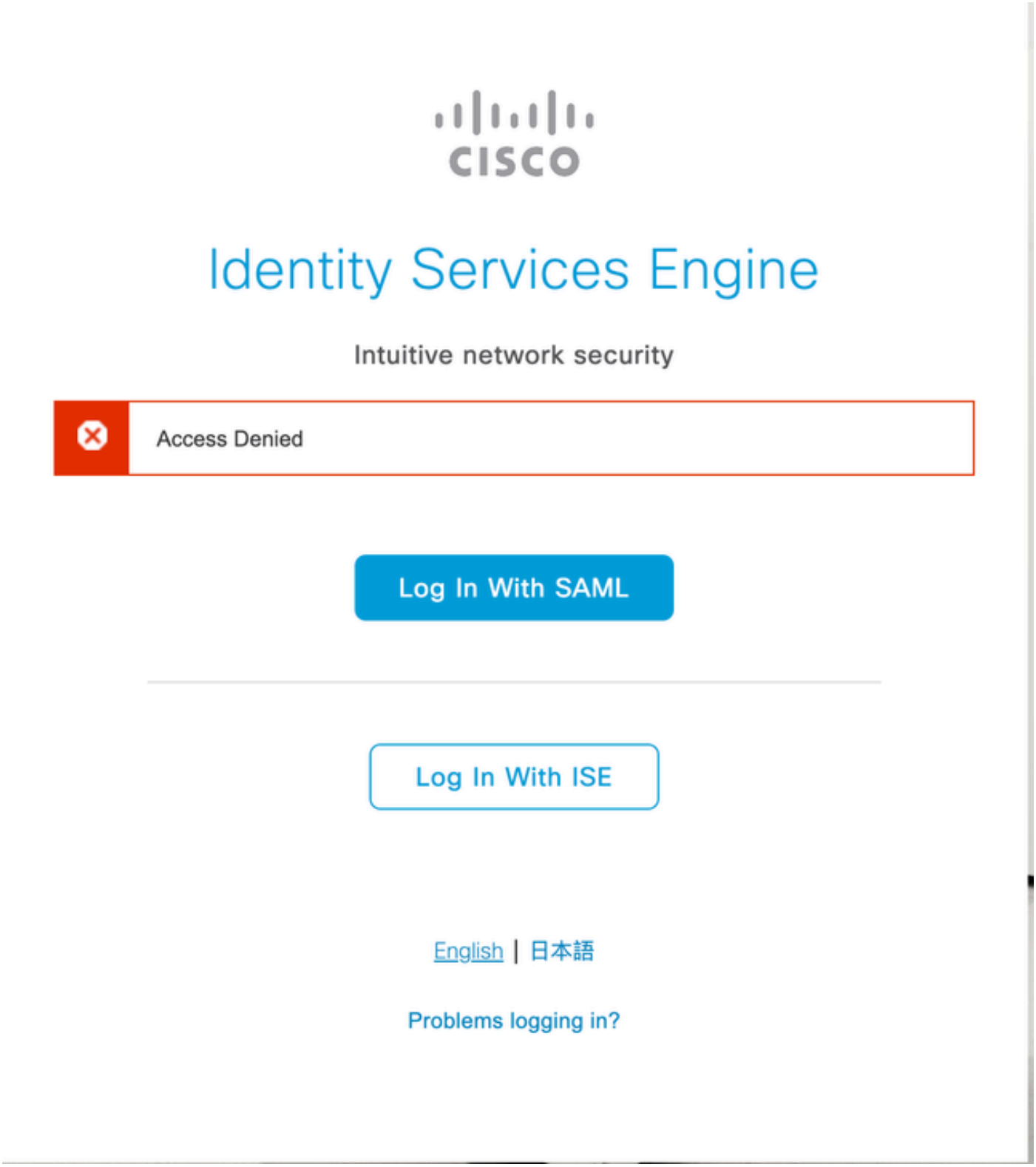
問題3.ISE應用伺服器無法處理SAML登入請求。當從身份提供程式Azure而不是服務提供程式ISE發起SAML請求時，會出現此問題。從Azure AD測試SSO登入不起作用，因為ISE不支援身份提供程式啟動的SAML請求。





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。



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

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

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

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

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

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

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

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

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

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

4. 收到了值為576c60ec-c0b6-4044-a8ec-d395b1475d6e的組屬性，並且簽名驗證。

```
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SA
```

```
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,185 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
        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-89
        Client Address: 10.24.226.171
        Load Balancer: null
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.security.SAML
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,186 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] org.opensaml.xml.signature
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.validat
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,188 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
2021-07-29 13:48:27,189 DEBUG  [https-jsse-nio-10.201.232.19-8443-exec-10][] cpm.saml.framework.impl.SAI
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 -:::

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）。