在ASA上使用SAML配置多個隧道組

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

[SAML SP啟動的SSO](#)

[組態](#)

- [從庫中新增Cisco安全防火牆 — 安全客戶端](#)
- [將Azure AD使用者分配給應用](#)
- [通過CLI配置ASA](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹使用Azure身份提供程式對思科ASA上的多個隧道組進行SAML身份驗證。

必要條件

需求

思科建議瞭解以下主題：

- Microsoft Azure

- Adaptive Security Appliance (ASA)
- 安全通訊端層(SSL)憑證
- 安全斷言標籤語言(SAML)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 9.2(1)1
- 思科安全使用者端5.1.7.80
- 使用SAML 2.0的Microsoft Azure Entra ID

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

Microsoft Azure可以支援同一實體ID的多個應用程式。每個應用程式（對映到不同的隧道組）都需要唯一的證書。在ASA上，由於IdP證書功能，可以將多個隧道組配置為使用不同的覆蓋身份提供程式(IdP)保護的應用程式。此功能允許管理員使用每個隧道組的特定IdP證書覆蓋單點登入(SSO)伺服器對象中的主IdP證書。此功能自9.17.1版開始在ASA上引入。

SAML SP啟動的SSO

當終端使用者通過訪問ASA啟動登入時，登入行為按以下方式進行：

1.當VPN使用者訪問或選擇啟用SAML的隧道組時，終端使用者將被重定向到SAML IdP進行身份驗證。系統會提示使用者，除非使用者直接訪問group-url，在這種情況下，重定向是靜默的。

2. ASA生成SAML身份驗證請求，瀏覽器將其重定向到SAML IdP。

3. IdP向終端使用者詢問憑證和終端使用者登入。輸入的憑據必須滿足IdP身份驗證配置。

4. IdP響應被傳送回瀏覽器並發佈到ASA登入URL。ASA驗證響應以完成登入。

組態

從庫中新增Cisco安全防火牆 — 安全客戶端

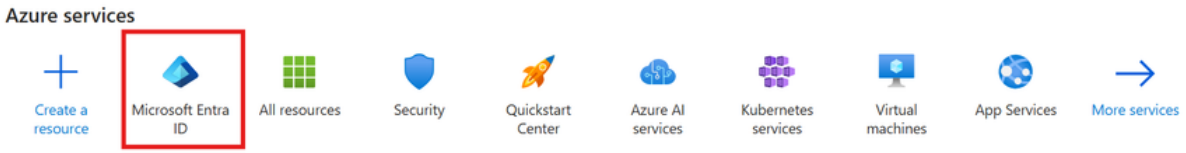
在此示例中，為在ASA上配置的兩個隧道組新增了Microsoft Entra SSO與Cisco安全防火牆 — Azure上的安全客戶端的整合：

- SAML1
- SAML2

要配置思科安全防火牆 — 安全客戶端與Microsoft Entra ID的整合，您必須將庫中的思科安全防火牆 — 安全客戶端新增到託管SaaS應用清單中。

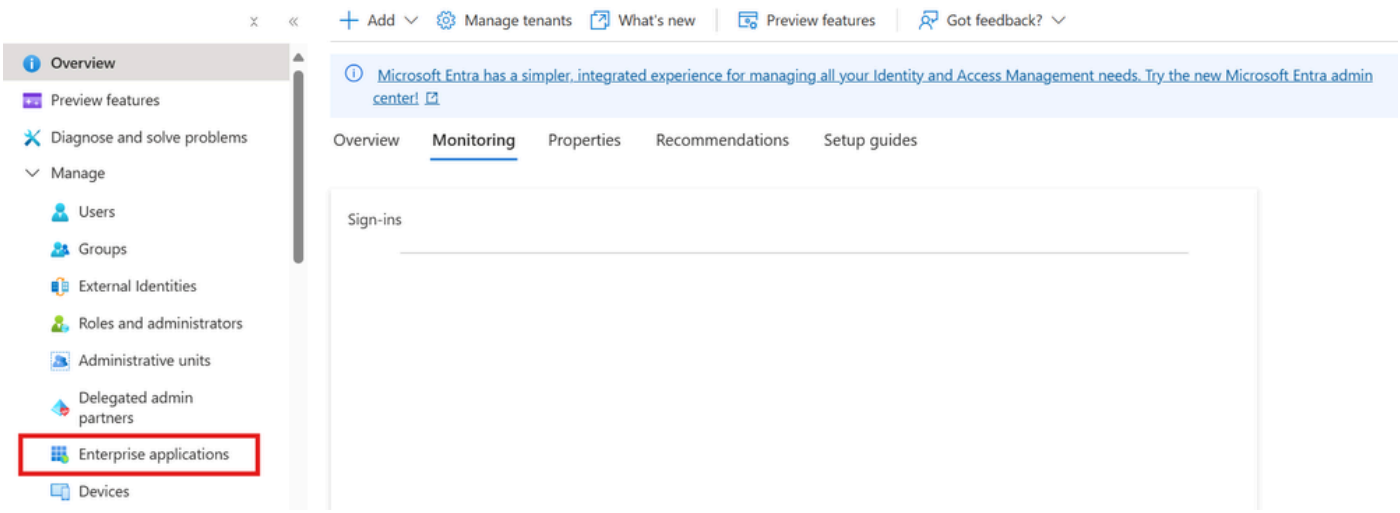
附註：以下步驟用於將思科安全防火牆 — 安全客戶端新增到第一個隧道組SAML1的庫中。

步驟1.登入到Azure門戶並選擇Microsoft Entra ID。



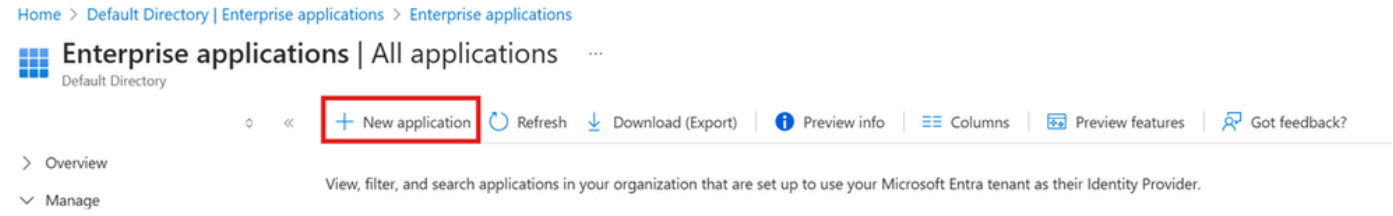
Microsoft Entra ID

步驟2.如圖所示，選擇Enterprise Applications。



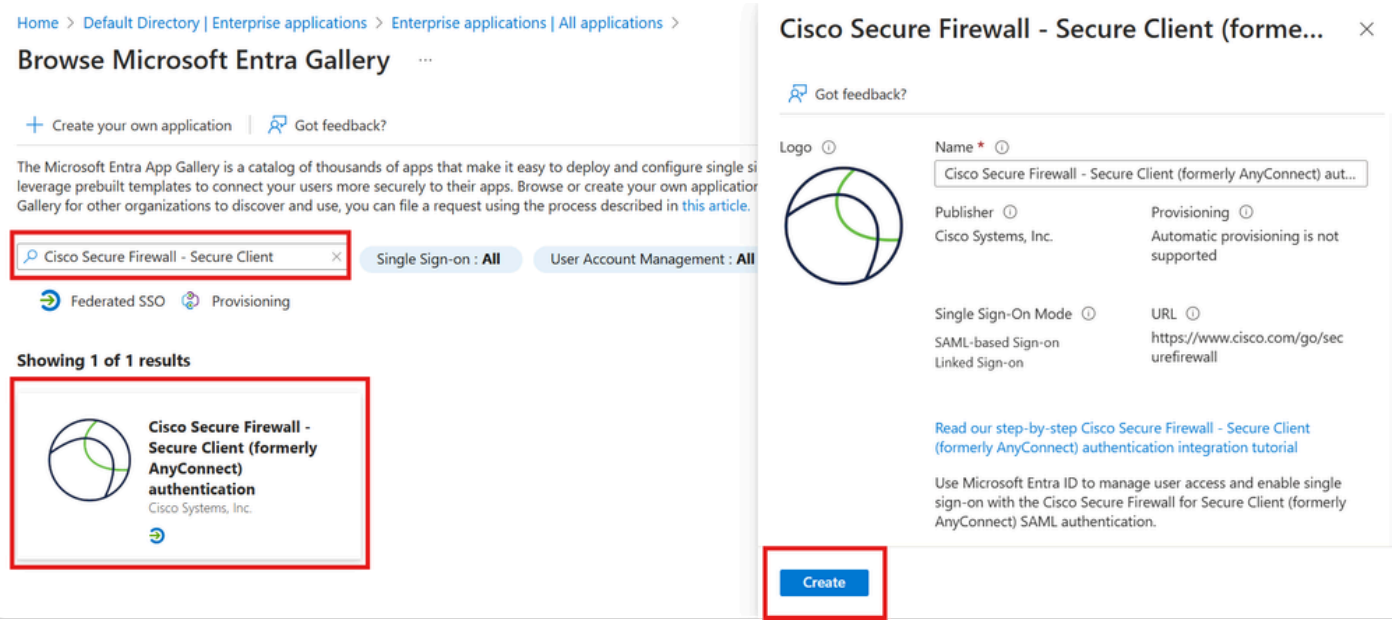
企業應用程式

步驟3.選擇New Application。



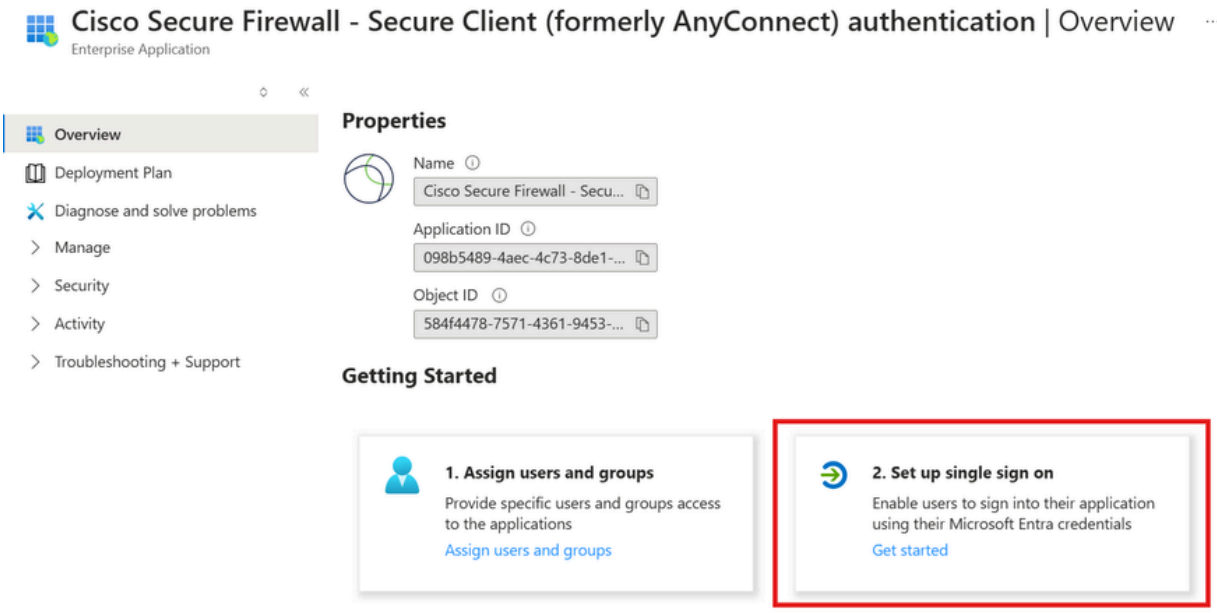
新應用程式

步驟4.在Add from the gallery部分中，在搜尋框中鍵入Cisco Secure Firewall - Secure Client，從結果面板中選擇Cisco Secure Firewall - Secure Client，然後選擇Add應用。



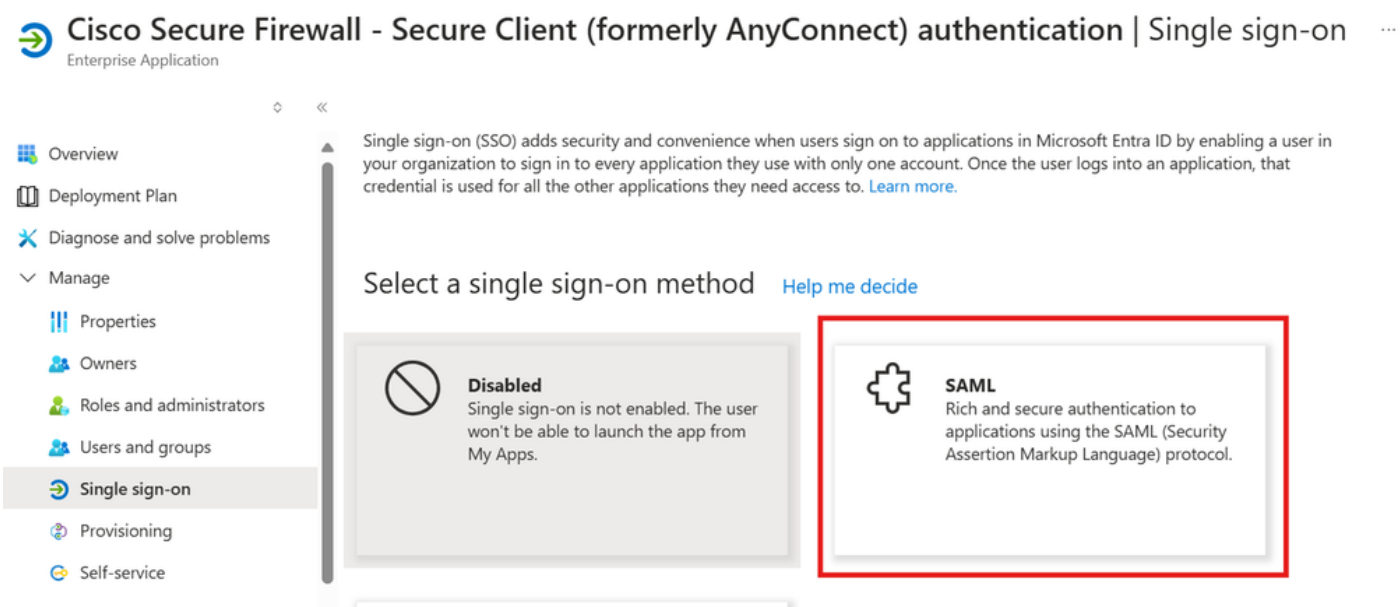
思科安全防火牆 — 安全使用者端

步驟5.選擇單點登入選單項。



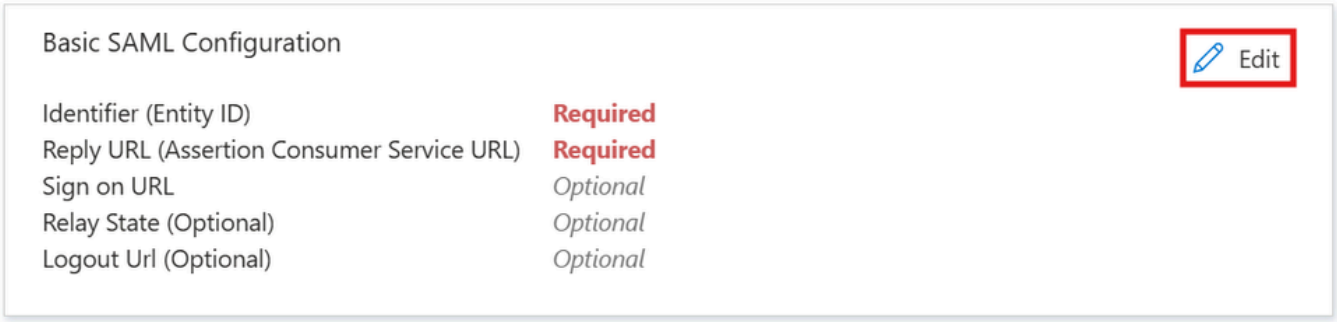
設定單一登入

步驟6.在選擇單點登入方法頁上，選擇SAML。



SAML

步驟7.在「使用SAML設定單一登入」頁上，按一下「基本SAML配置」的「編輯/筆」圖示以編輯設定。



基本Saml配置

步驟8.在「使用SAML設定單一登入」頁上，輸入以下欄位的值：

- 在Identifiertext框中，使用以下模式鍵入URL:

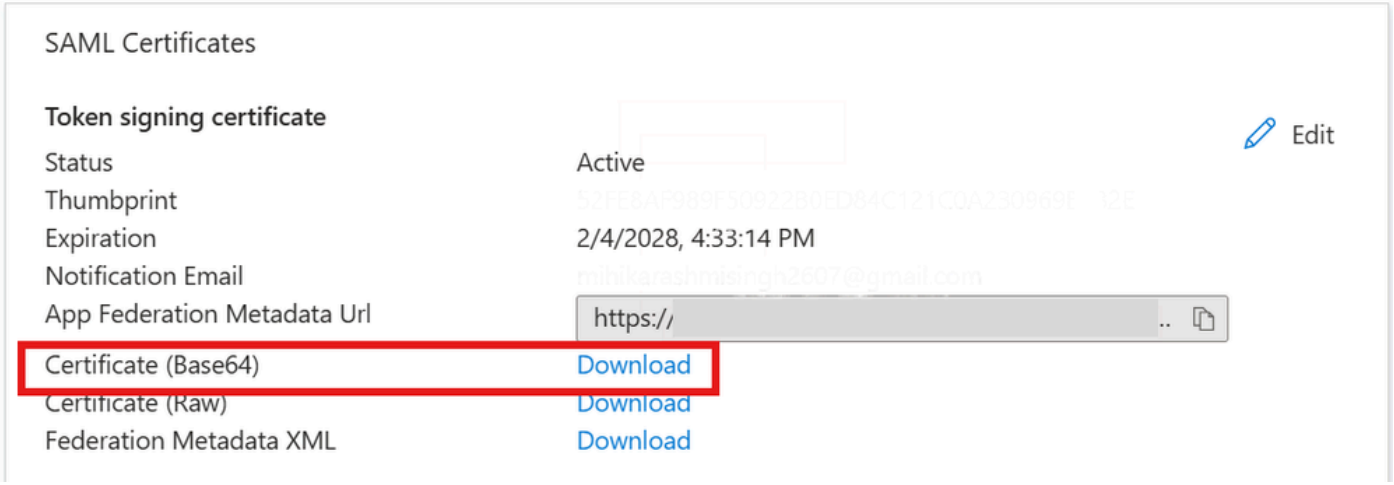
https://<VPN URL>/saml/sp/metadata/<Tunnel_Group_Name>

- 在回覆URL文本框中，鍵入使用以下模式的URL:

https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<Tunnel_Group_Name>
[Tunnel_Group_Name = SAML1]

附註：Tunnel_Group_Name區分大小寫，並且值不得包含點「。」 並斜槓「/」。

步驟9.在使用SAML設定單一登入頁面上，在SAML簽名證書部分中查詢證書(Base64)並選擇Download下載證書檔案並將其儲存在您的電腦上。

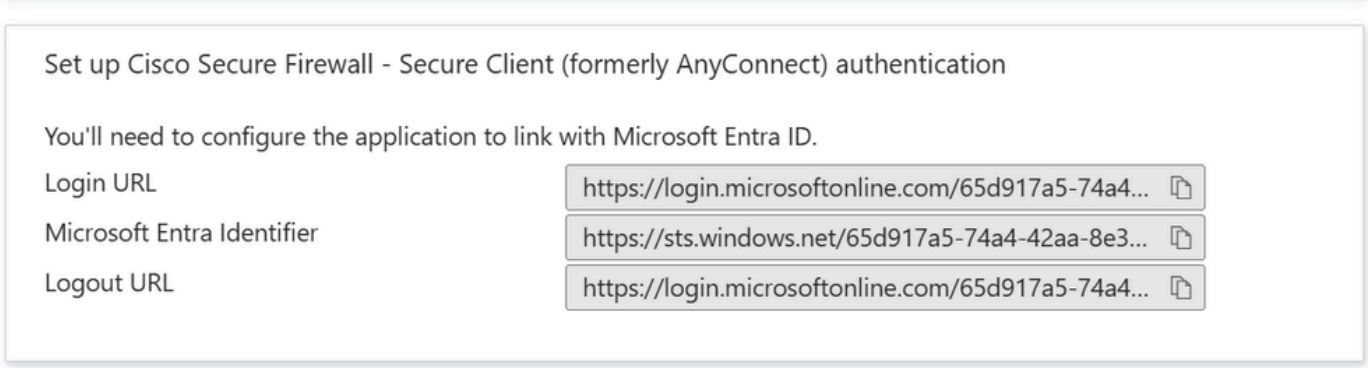


Certificate(Base64)Download

注意：此下載的證書已匯入到ASA信任點AzureAD-AC-SAML1。有關詳細資訊，請參閱「ASA配置」部分。

步驟10.在設定Cisco安全防火牆 — 安全客戶端部分，根據您的要求複製適當的URL。這些URL用於在ASA上配置SSO伺服器對象。

- Microsoft Entra識別符號:這是VPN配置中的SAML IdP。
- 登入URL:這是URL登入。
- 註銷URL:這是URL註銷。



SSO URL

附註：重複前面的配置步驟，從第二個隧道組的庫中新增Cisco Secure Firewall - Secure Client應用。此案例中的第二個隧道組名稱為SAML2。

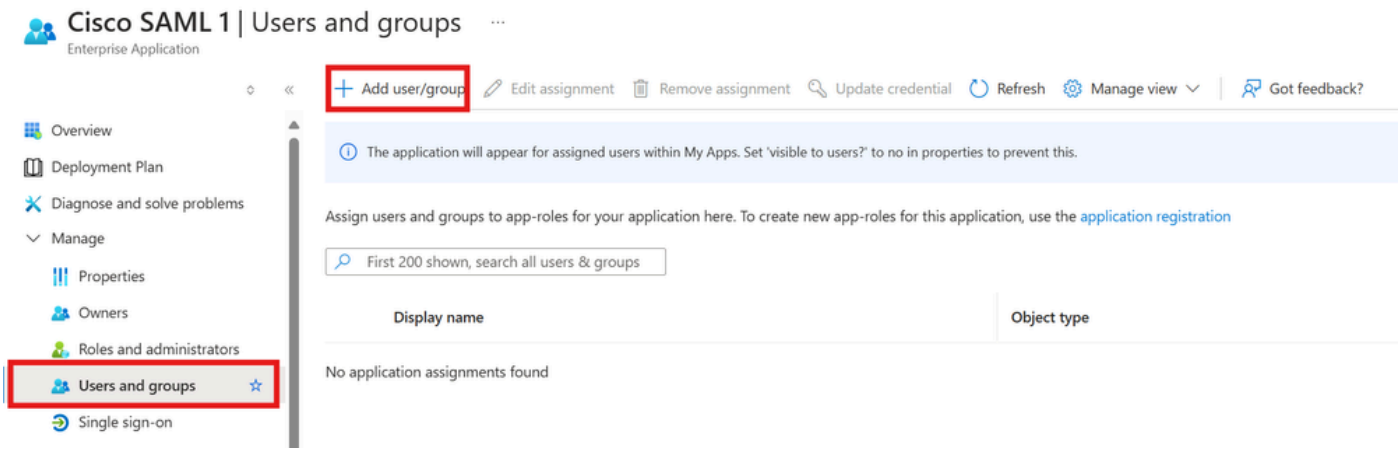
為第二個隧道組(SAML 2)新增思科安全防火牆 — 安全客戶端應用時，將在步驟8中下載的Azure證書匯入到ASA信任點AzureAD-AC-SAML2。

將Azure AD使用者分配給應用

在本節中，Test1和Test2被啟用以使用Azure SSO，因為您授予了對思科安全客戶端應用的訪問許可權。

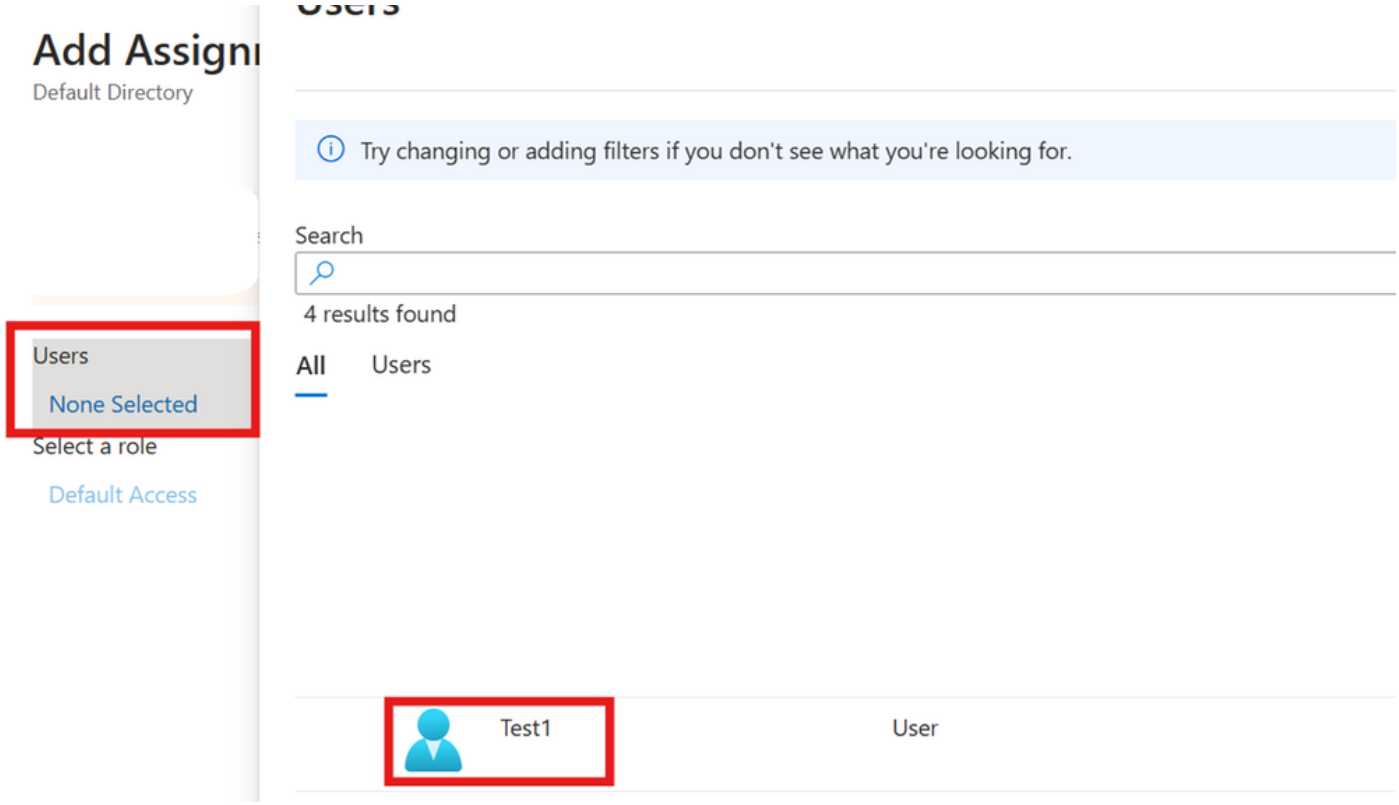
對於第一個IdP應用程式：

步驟1.在第一個IdP應用程式概述頁中，依次選擇Users and groups和Add user。



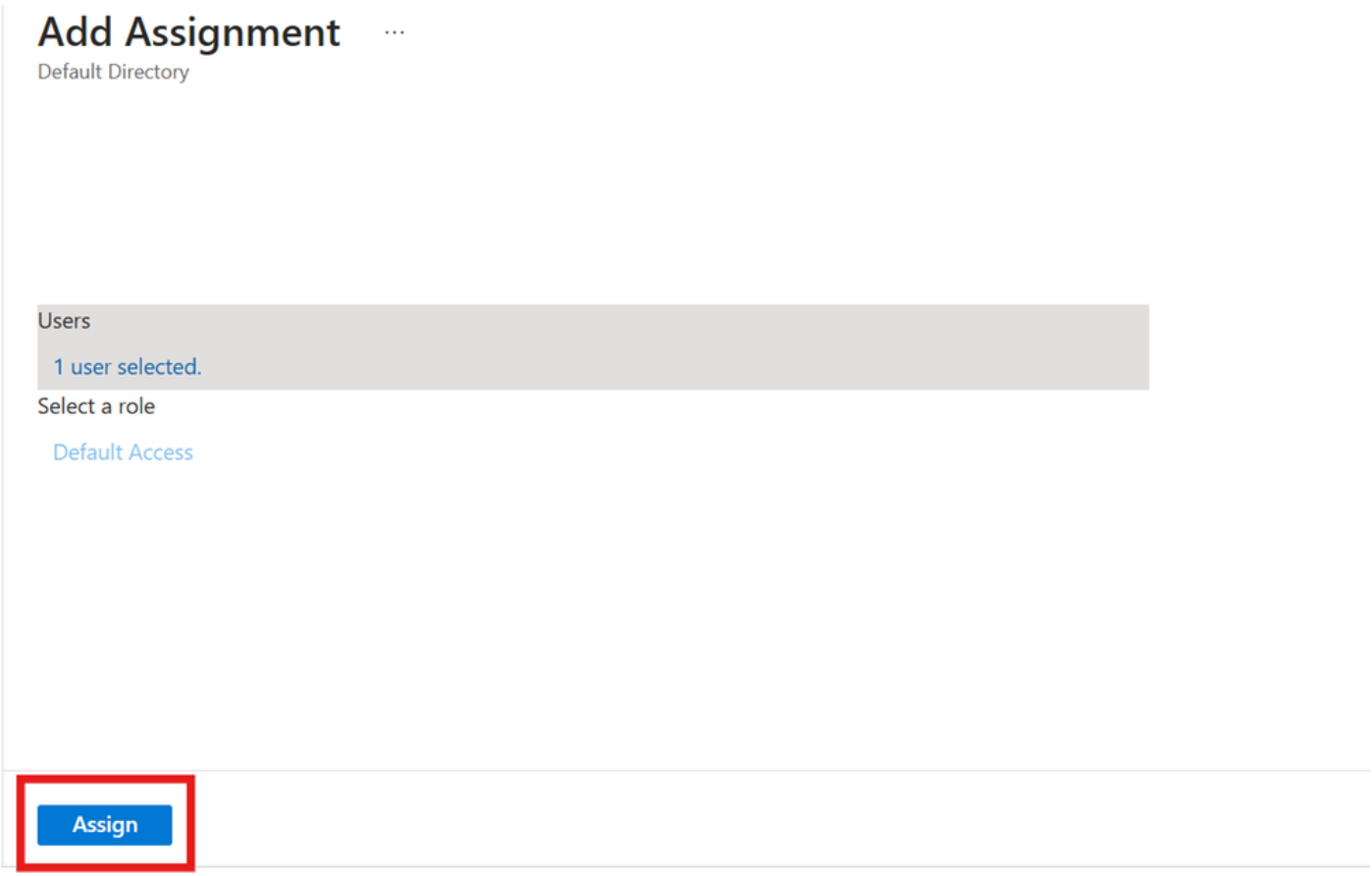
使用者和組

步驟2.在「新增分配」對話框中選擇「使用者」或「組」。



新增作業1

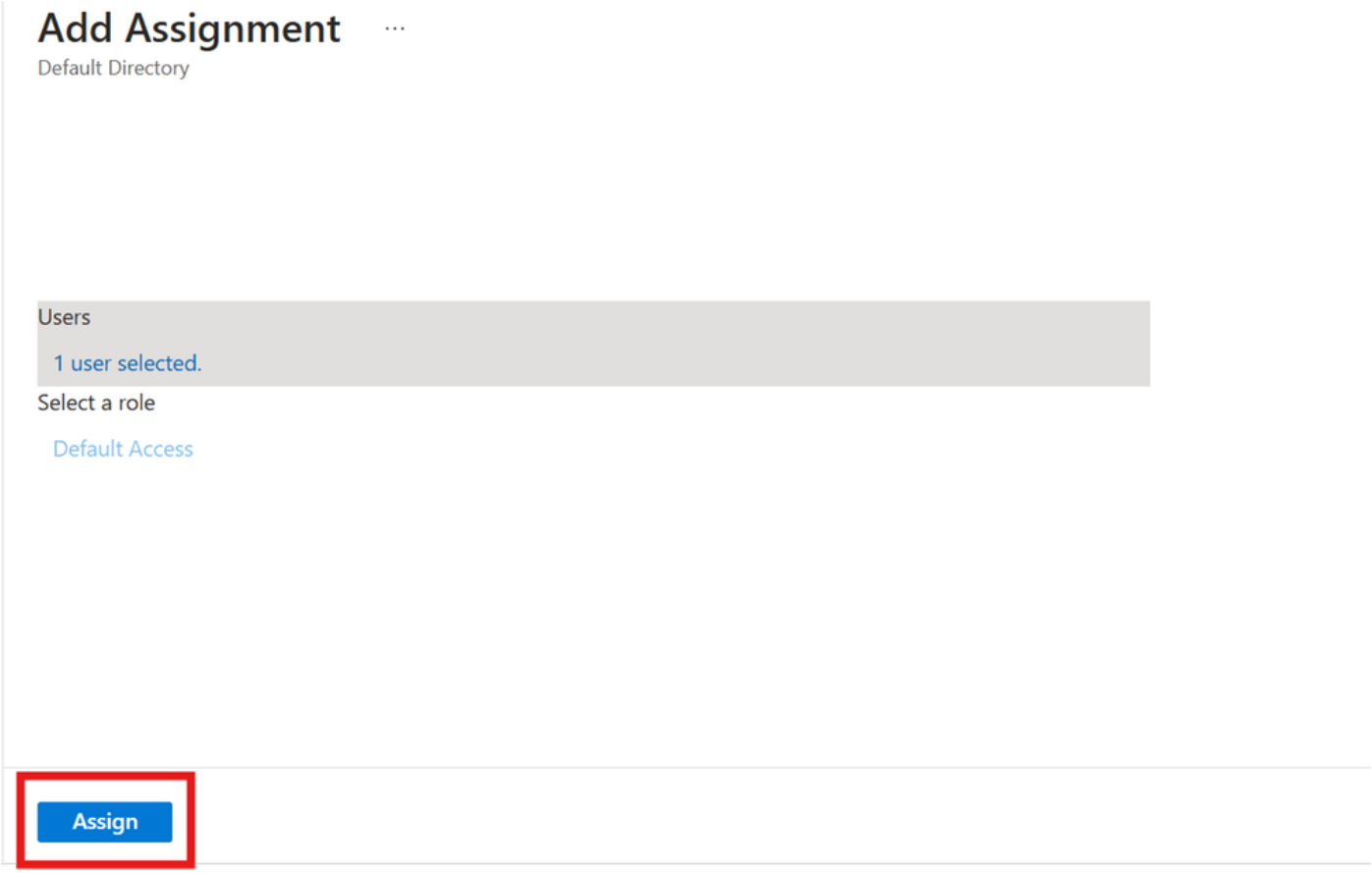
步驟3.在Add Assignment對話框中，按一下Assign按鈕。



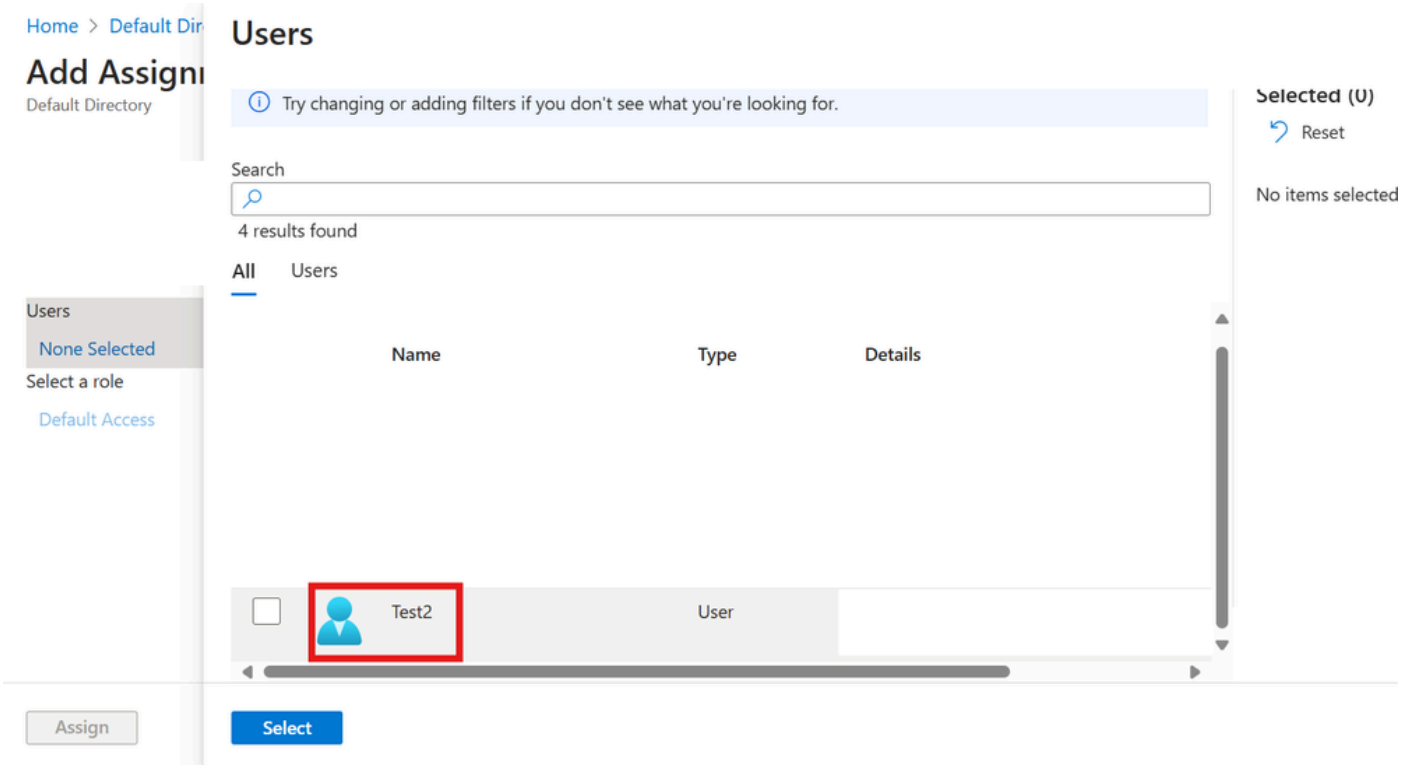
測試1使用者分配

對於第二個IdP應用程式：

對第二個Idp應用程式重複上述步驟，如下圖所示：

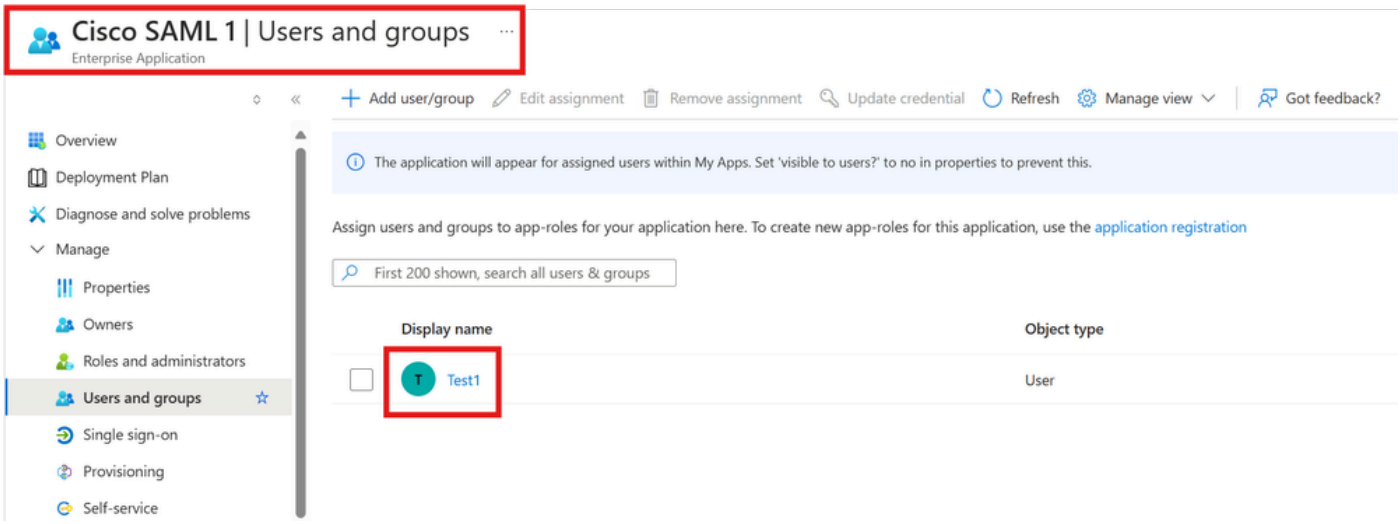


新增作業2



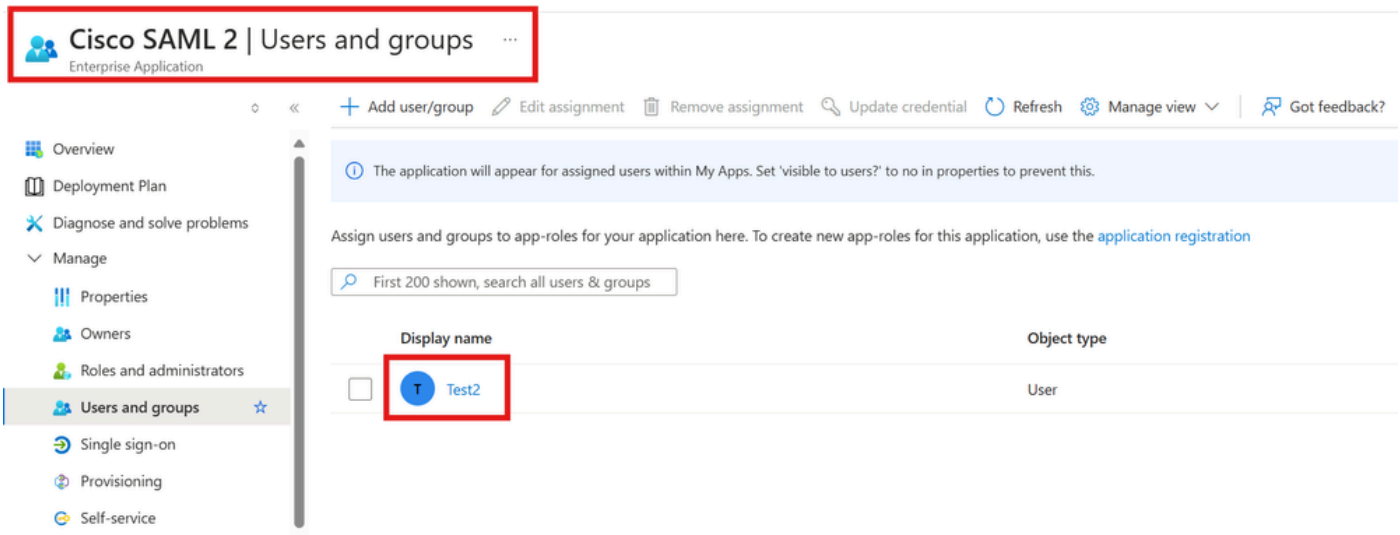
測試2使用者分配

Test1使用者分配：



測試1使用者分配

Test2使用者分配：



測試2使用者分配

通過CLI配置ASA

步驟1.建立信任點並匯入SAML證書。

配置兩個信任點，並為每個隧道組匯入各自的SAML證書:

<#root>

```
config t

 crypto ca trustpoint

AzureAD-AC-SAML1


   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate

AzureAD-AC-SAML1


 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit

!
!
```

```
crypto ca trustpoint
```

AzureAD-AC-SAML2

```
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML2

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit
```

步驟2.配置SAML IdP。

運行這些命令以設定SAML IdP設定。

```
webvpn

 saml idp https://xxx.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2  - [Logout URL]
 trustpoint idp AzureAD-AC-SAML1 - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

步驟3.將SAML身份驗證應用到第一個VPN隧道組。

使用AzureAD-AC-SAML1 IdP信任點配置SAML1隧道組。

<#root>

```
tunnel-group SAML1 webvpn-attributes
authentication saml
group-alias SAML1 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

```
saml idp-trustpoint AzureAD-AC-SAML1 <---- Overrides the primary IDP certificate in the Single Sign-On (
```

步驟4.將SAML身份驗證應用到第二個VPN隧道組。

使用AzureAD-AC-SAML2 IdP信任點配置SAML2隧道組。

<#root>

```
tunnel-group SAML2 webvpn-attributes
authentication saml
group-alias SAML2 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/

saml idp-trustpoint AzureAD-AC-SAML2 <---- Overrides the primary IDP certificate in the Single Sign-On (
```

步驟 5:儲存組態。

```
write memory
```

附註：如果更改IdP配置，則必須從隧道組刪除SAML身份提供程式配置，然後重新應用該配置以使更改生效。

驗證

使用SAML身份驗證測試AnyConnect。

步驟1。連線到您的VPN URL並在Azure AD詳細資訊中輸入您的日誌。

步驟2.（可選）批准登入請求。

步驟3. AnyConnect已連線。

疑難排解

大多數SAML故障排除都涉及配置錯誤，在檢查SAML配置或運行調試時可以發現該錯誤。debug webvpn saml 255可用於排除大多數問題，但是，在此調試不提供有用資訊的情況下，可以運行其他調試，例如：

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

相關資訊

- 技術支援與文件 - Cisco Systems
- 透過 SAML 藉由 Microsoft Azure MFA 設定 ASA AnyConnect VPN

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）。