使用Microsoft Entra ID為SD-WAN配置SSO

目錄

簡介

本檔案介紹如何使用Microsoft Entra ID為Cisco Catalyst軟體定義廣域網(SD-WAN)設定單一登入(SSO)。

必要條件

需求

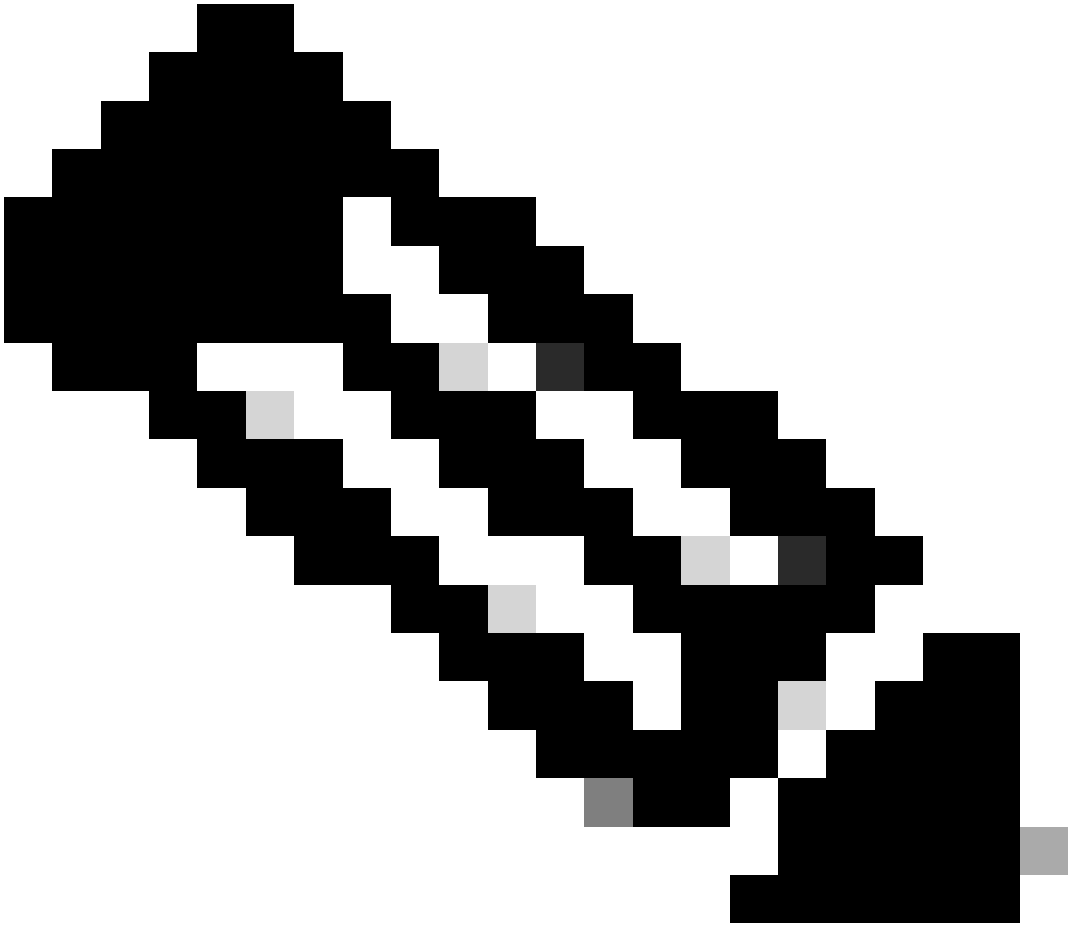
思科建議您瞭解以下主題的一般知識：

- 單一登入
- Cisco Catalyst SD-WAN解決方案

採用元件

本檔案中的資訊是根據：

- Cisco Catalyst SD-WAN管理器版本20.15.3.1
- Microsoft Entra ID



附註：以前稱為Azure Active Directory(Azure AD)的解決方案現在稱為Microsoft 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

單一登入是一種身份驗證方法，允許使用者使用一組憑據安全訪問多個獨立的應用程式或網站。使用SSO，使用者不再需要分別登入到每個應用程式 — 經過身份驗證後，他們就可以無縫訪問所有允許的資源。

實現SSO的一種常見方法是使用聯合身份驗證，它使用諸如SAML 2.0、WS-Federation或OpenID Connect等協定在身份提供程式(IdP)和服務提供程式(SP)之間建立信任。聯合通過集中身份驗證提高安全性、可靠性和使用者體驗。

Microsoft Entra ID是一種廣泛使用的基於雲的身份提供程式，支援這些聯合協定。在使用Cisco Catalyst SD-WAN的SSO設定中，Microsoft Entra ID充當IdP，Cisco SD-WAN Manager充當

Service Provider。

整合工作如下：

1. 網路管理員嘗試登入到Cisco SD-WAN Manager。
2. Cisco SD-WAN Manager向Microsoft Entra ID傳送身份驗證請求。
3. Microsoft Entra ID提示管理員使用其Entra ID(Microsoft)帳戶進行身份驗證。
4. 驗證憑證後，Microsoft Entra ID會將安全響應傳送回Cisco SD-WAN Manager，以確認身份驗證。
5. Cisco SD-WAN Manager無需單獨的憑證即可授予訪問許可權。

在此模型中：

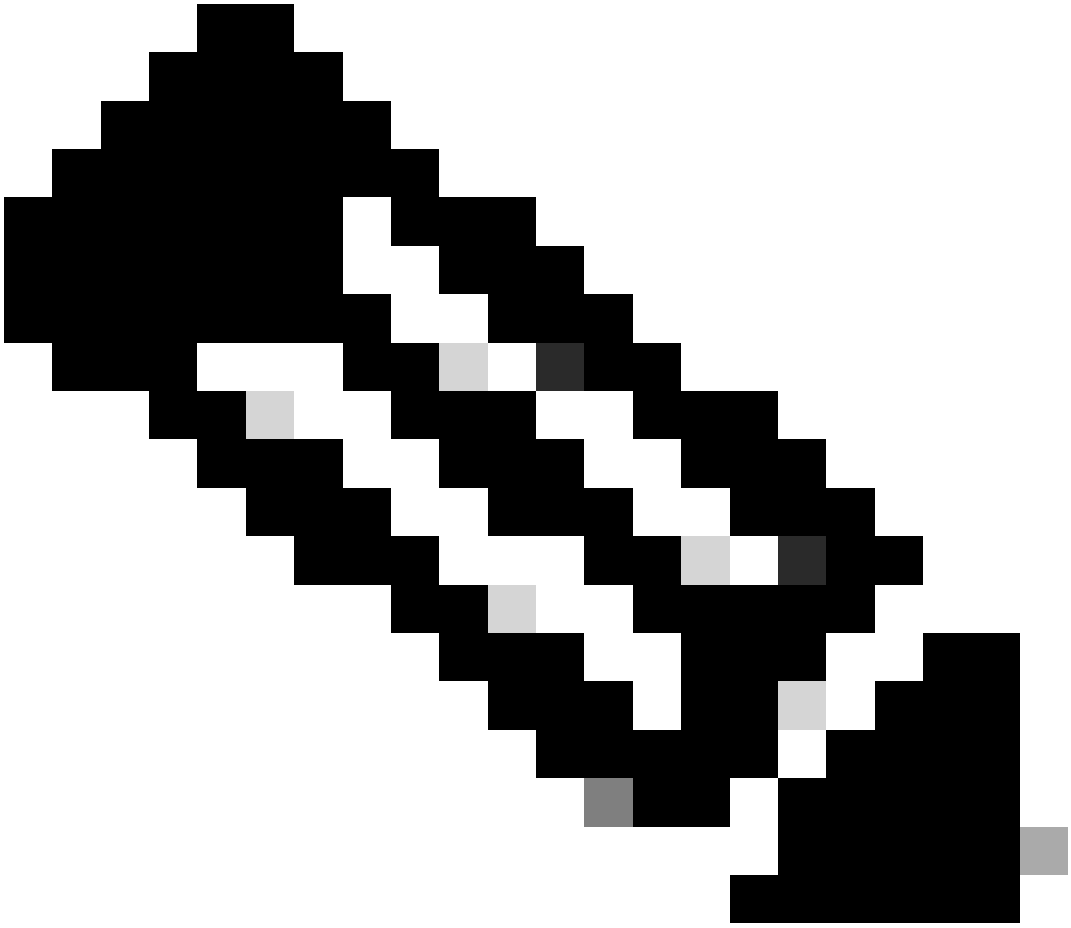
- 身份提供程式(IdP) — 儲存使用者資料，驗證憑據（例如，Microsoft Entra ID、Okta、PingID、ADFS）。
- 服務提供商 — 託管要訪問的應用程式（例如Cisco SD-WAN Manager）。
- Users — 在IdP目錄中擁有帳戶並有權訪問服務提供商。

根據行業標準配置時，Cisco Catalyst SD-WAN與任何符合SAML 2.0的IdP相容。

使用單一登入的優勢

- 通過身份提供程式集中憑據管理。
- 通過消除多個弱密碼加強身份驗證安全。
- 簡化管理員的安全訪問。
- 啟用對Cisco Catalyst SD-WAN Manager和其他授權應用程式的一鍵訪問。

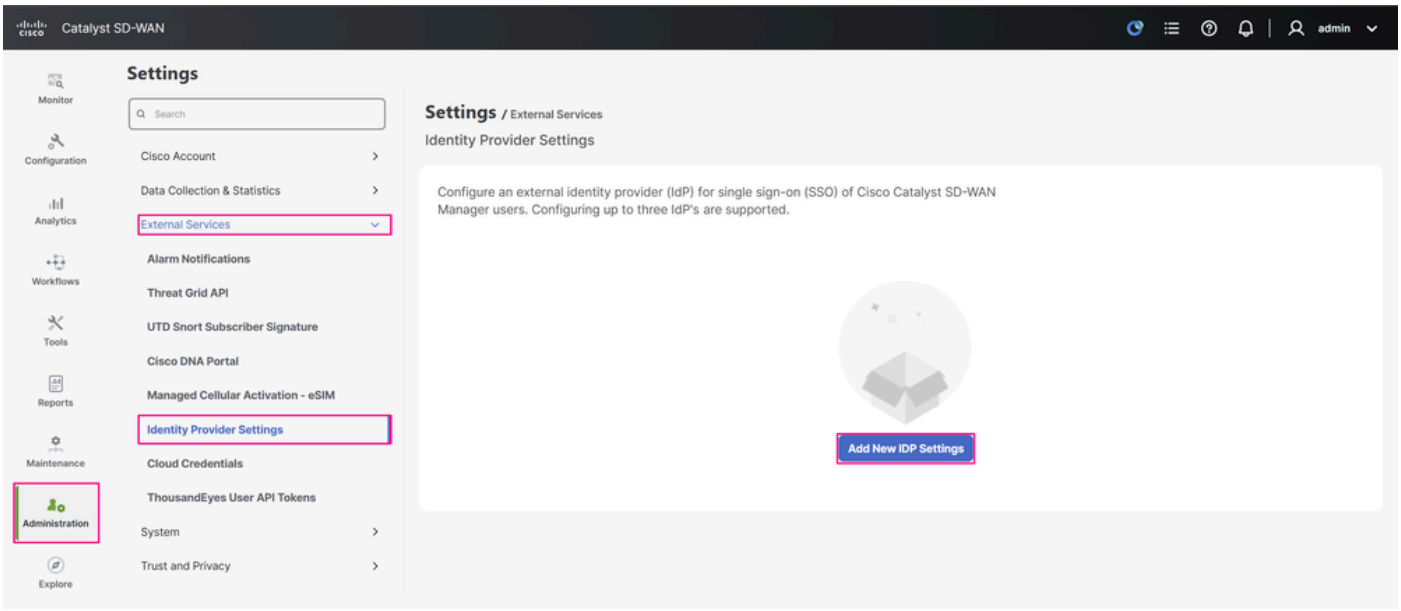
設定



附註：支援的最低版本：Cisco Catalyst SD-WAN管理器版本20.8.1。

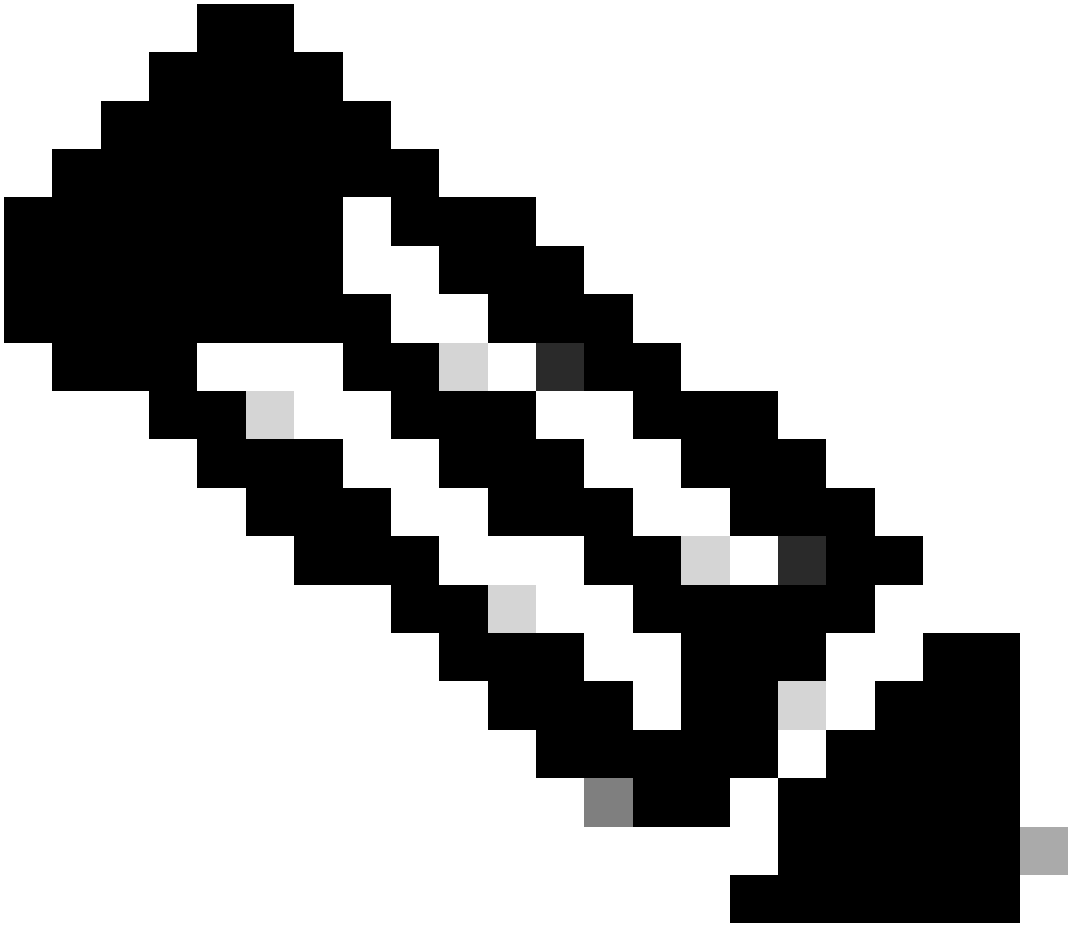
步驟1.獲取Cisco SD-WAN Manager SAML後設資料

- 在Cisco SD-WAN Manager中，導航到管理>設定>外部服務>身份提供程式設定，然後按一下新增新IDP設定。



Cisco SD-WAN管理員UI

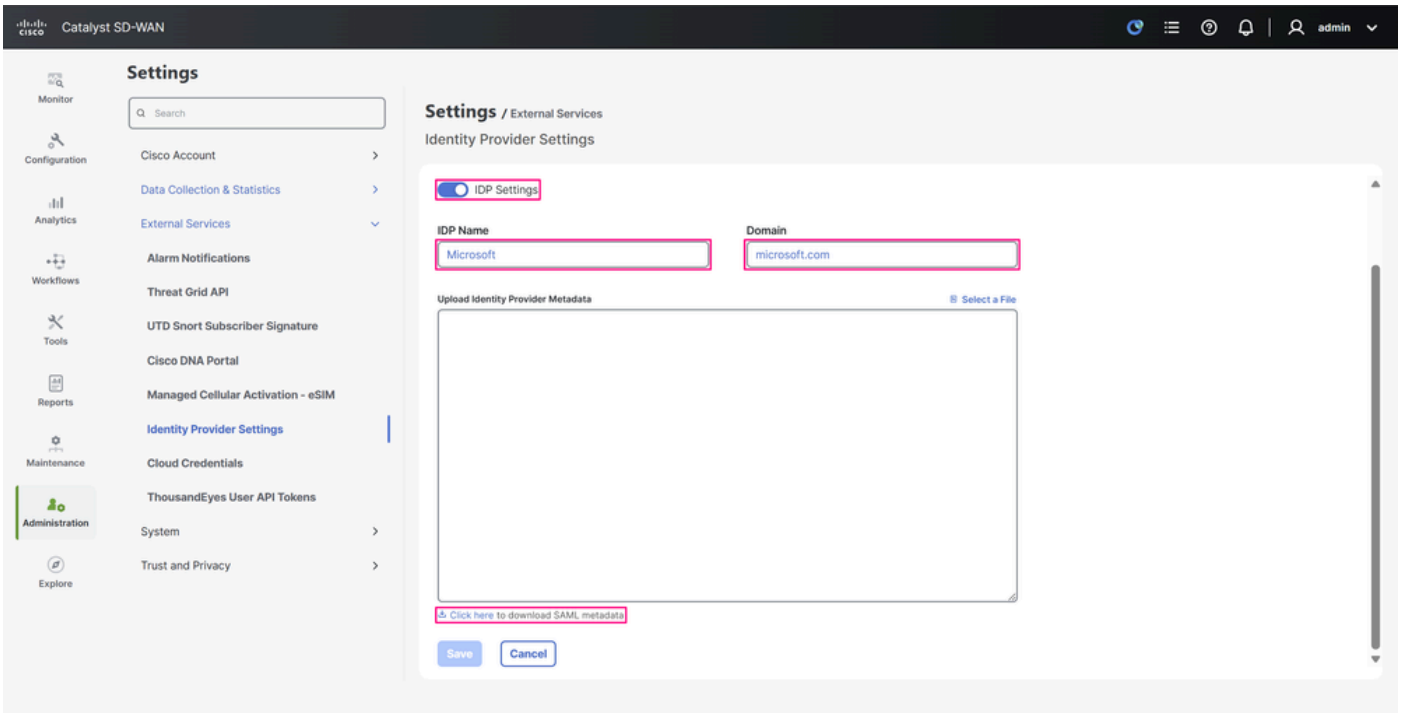
- 切換IDP設定以啟用身份提供程式設定。在IDP Name欄位中，輸入引用您正在使用的IdP的name，然後在Domain欄位中，輸入與組織企業應用程式中的使用者使用的域名匹配的域。按一下按一下此處下載SAML後設資料並將後設資料XML檔案保存到電腦。在下一步中，此檔案用於在Microsoft Entra ID中配置SSO。



附註：在此示例中，後設資料XML檔案直接指向Cisco SD-WAN Manager的IP地址，但在許多生產環境中，它指向其完全限定的域名(FQDN)。 對於獨立的Cisco SD-WAN Manager，後設資料中包含的實體ID與下載時用於登入Cisco SD-WAN Manager的URL匹配。這表示它使用IP地址或FQDN運行，因為它是單節點設定。

對於Cisco SD-WAN Manager集群，相同的原理適用於FQDN指向其中一個集群節點，並且後設資料包括此域作為實體ID。不同之處在於，無論您是使用群集的FQDN還是使用來自使用其IP地址的特定節點的後設資料，在成功完成與Microsoft Entra ID的SSO整合後，其他節點也會重定向到IdP登入提示。

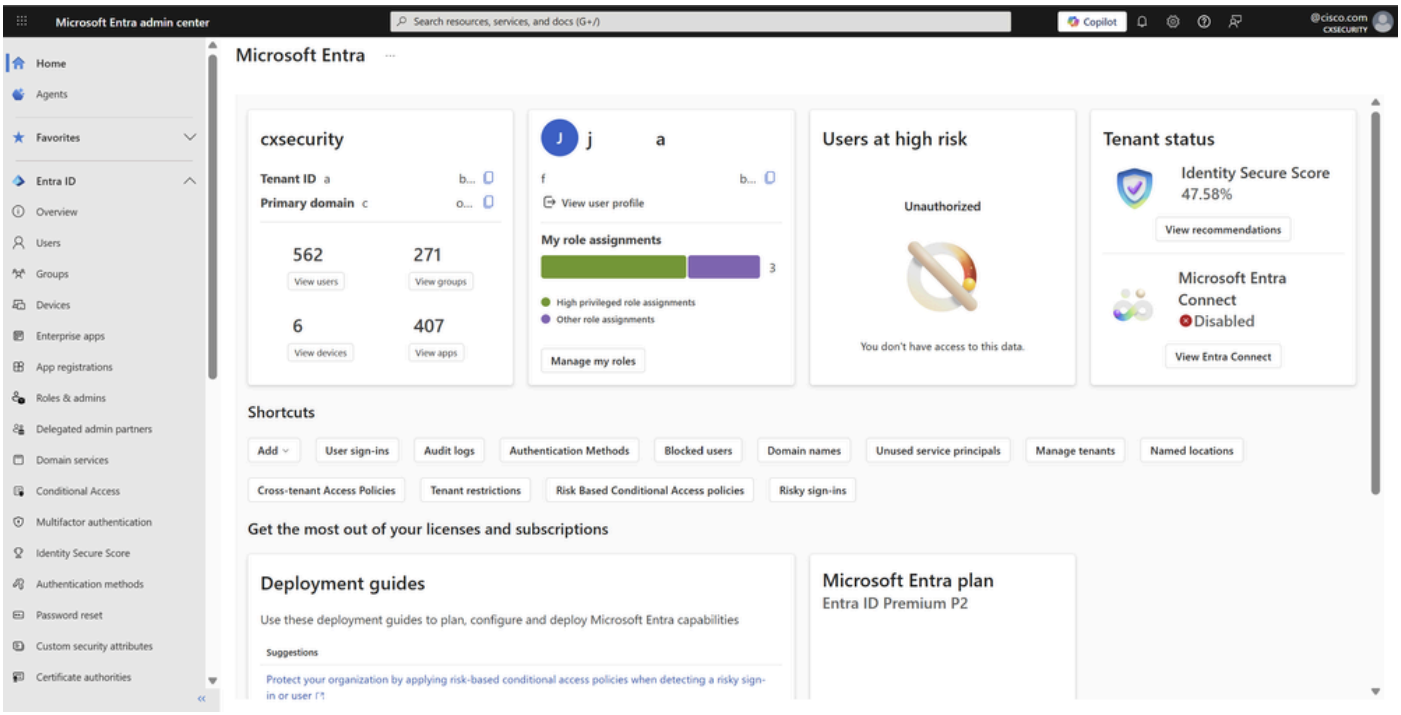
這兩種方案的主要要求是，您在Cisco SD-WAN Manager中使用的實體ID（無論是IP地址還是FQDN）與IdP端配置的識別符號相匹配。



「IdP設定：配置」頁

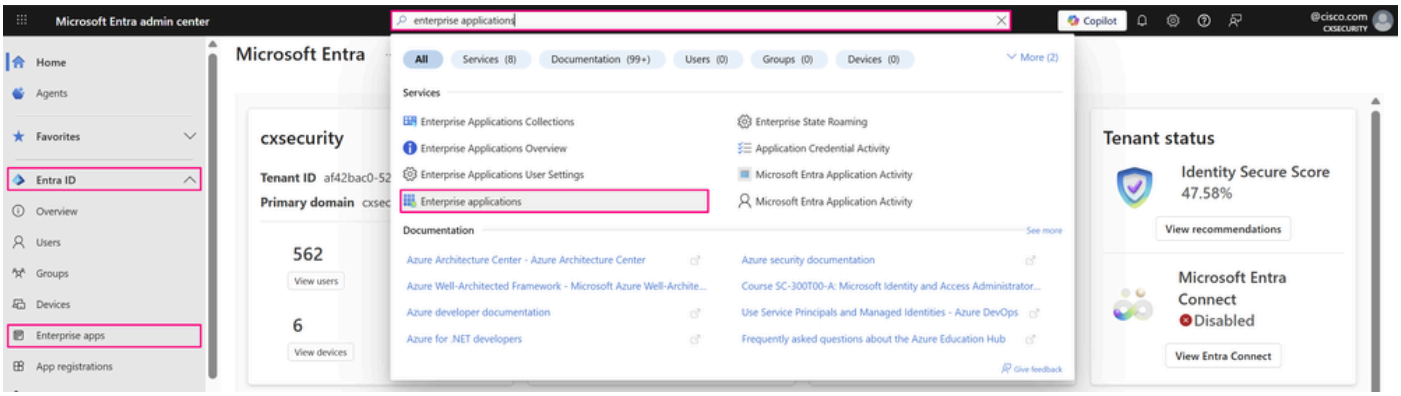
步驟2.在Microsoft Entra ID中配置用於SSO的企業應用程式

- 使用以下角色之一登錄Microsoft Entra管理中心門戶：雲應用程式管理員、應用程式管理員或服務主體的所有者。



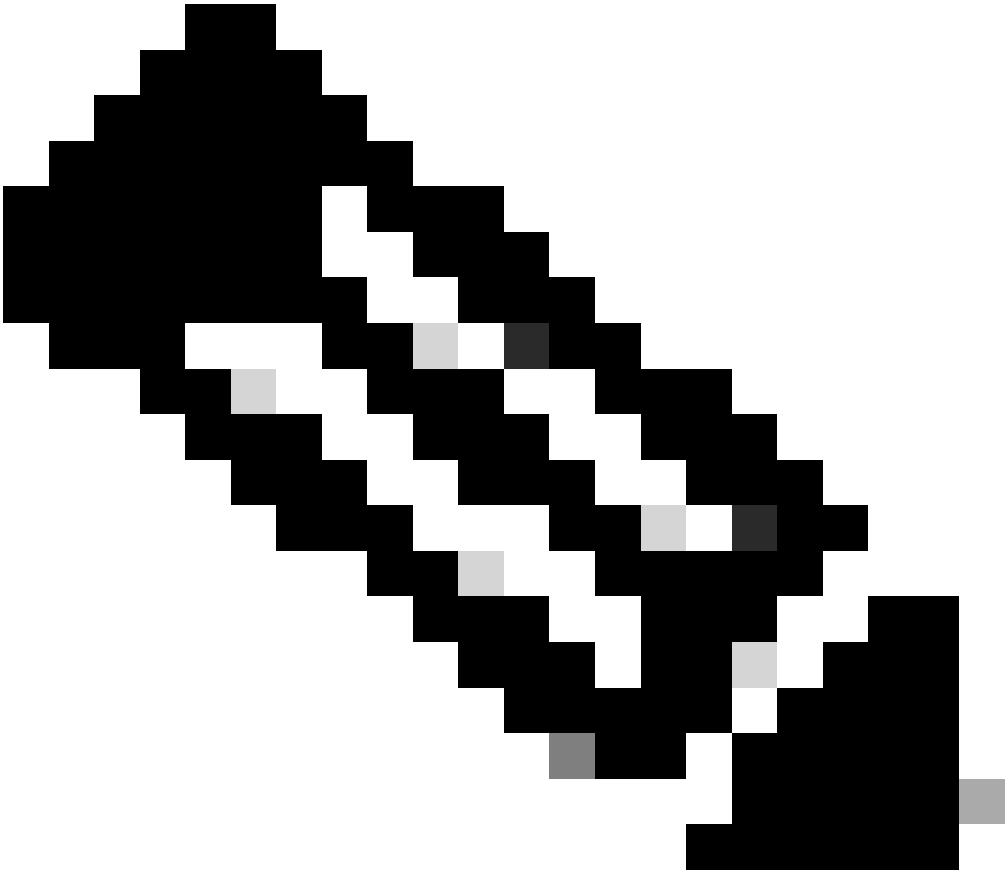
Microsoft Entra管理中心門戶

- 導航到Entra ID > Enterprise apps，或者也可以在您在門戶頂部的搜尋欄中輸入enterprise applications，然後選擇Enterprise Applications時訪問此服務。

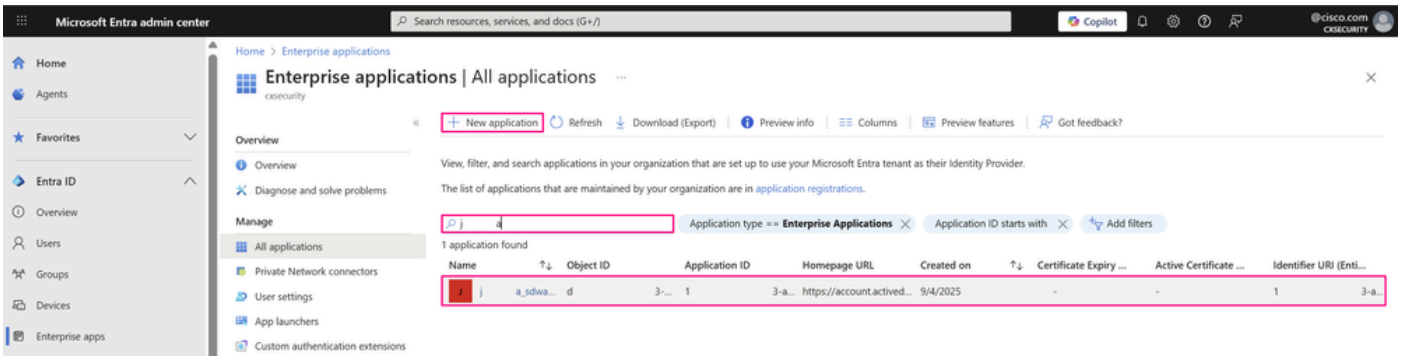


Microsoft Entra管理中心門戶

- 將開啟「所有應用程式」頁面。在搜尋框中輸入現有應用程式的名稱，然後從搜尋結果中選擇應用程式。

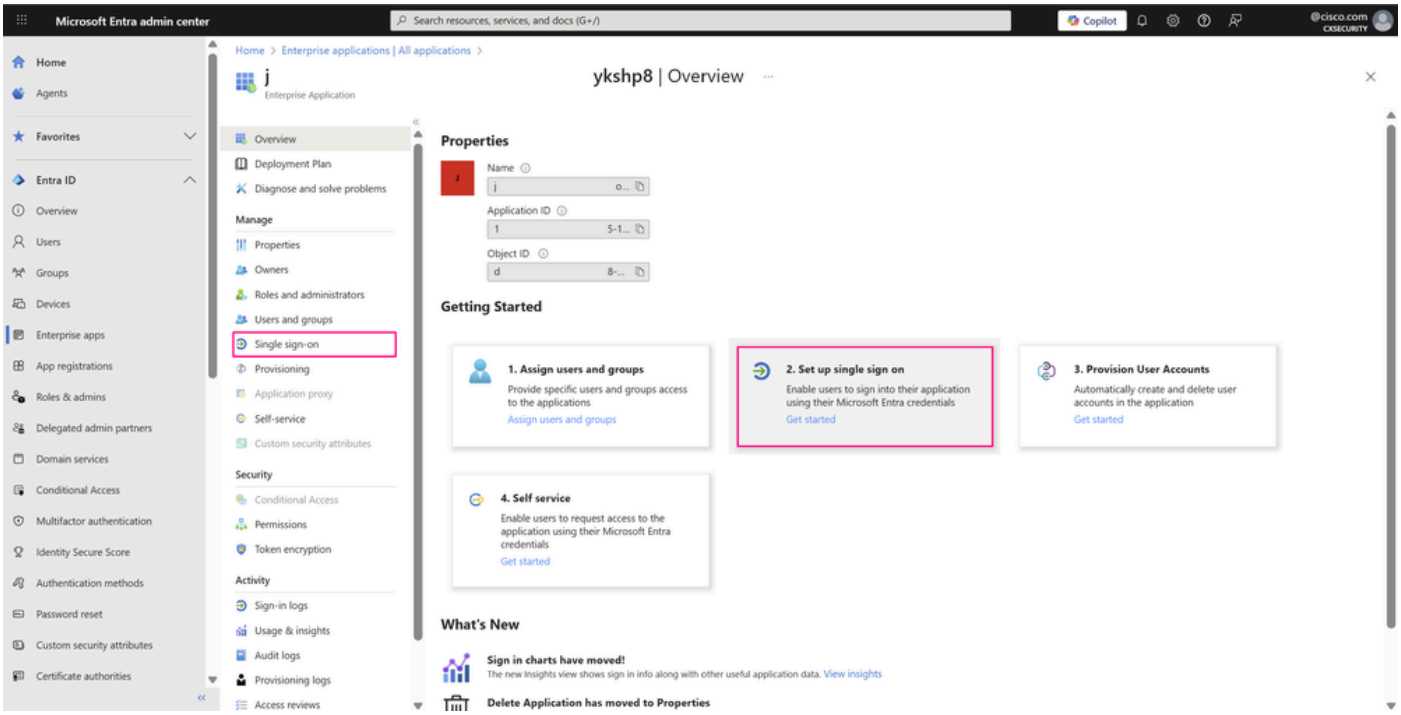


附註：在此頁面上，您可以根據組織的要求建立自定義企業應用程式，並在按一下New application時，使用SSO身份驗證（如果尚未進行）對其進行配置。



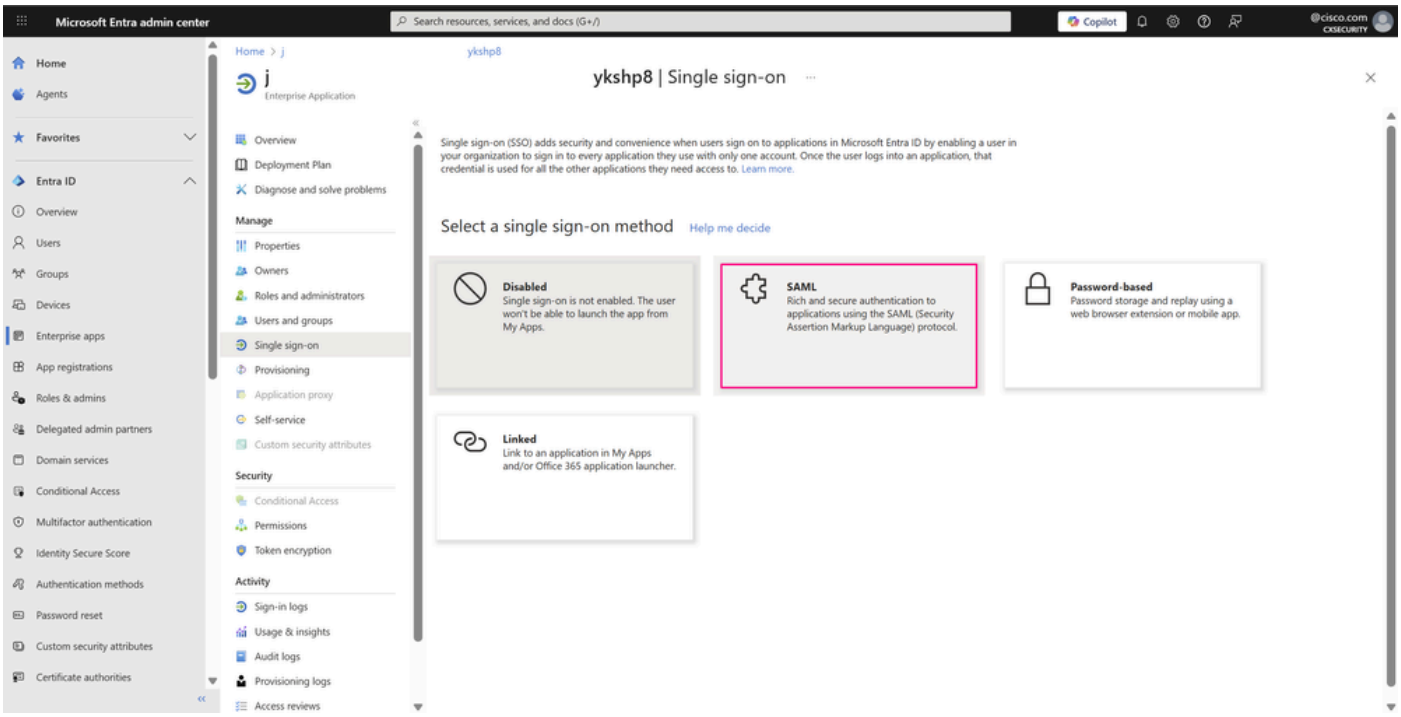
企業應用程式控制面板

- 在左側選單的「管理」部分，按一下「一次登入」，或在「概述」部分的「入門」窗格中，單擊「2」。設定一次登入，開啟Single sign-on窗格進行編輯。



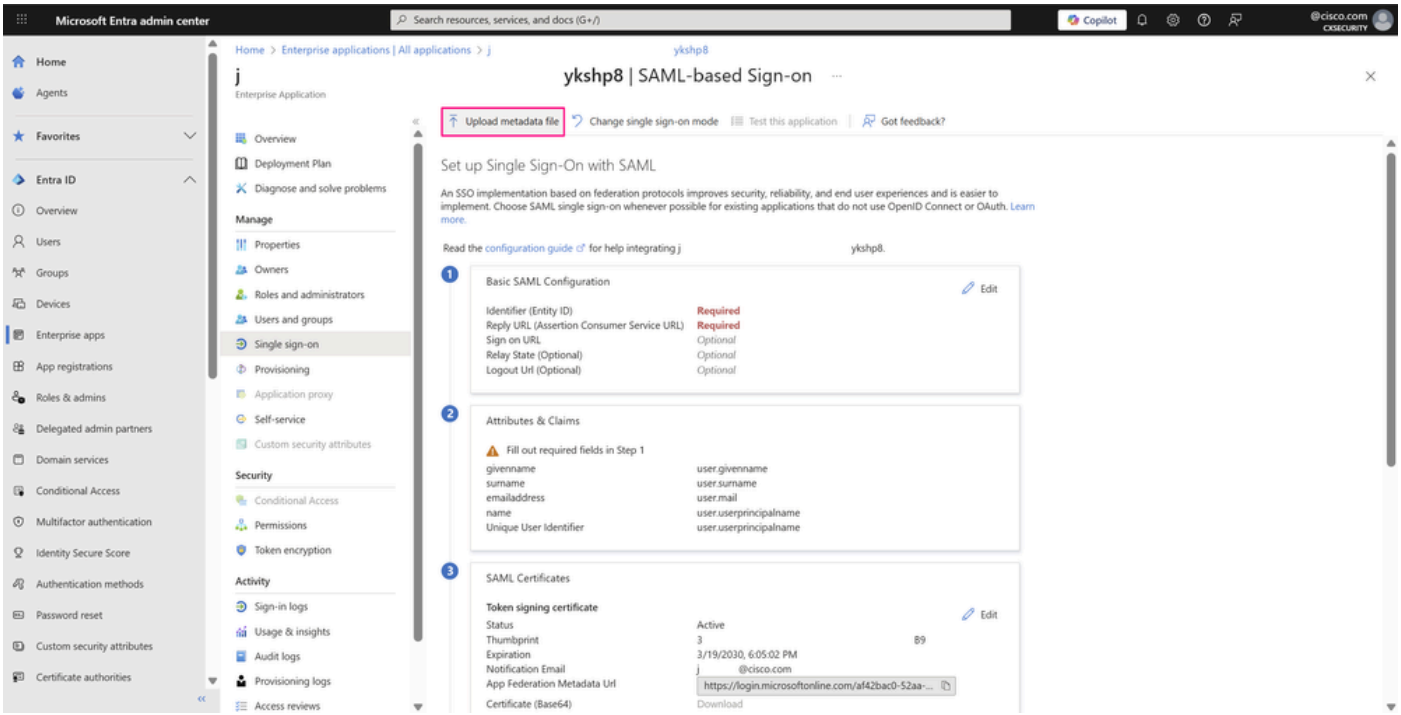
企業應用程式概述

- 選擇SAML以開啟SSO配置頁。



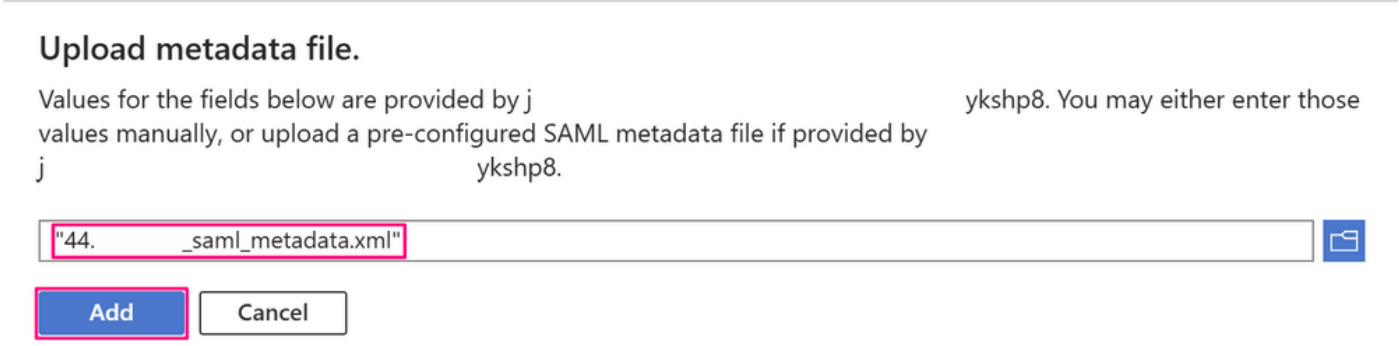
單一登入窗格

- 在「使用SAML設定單一登入」頁上，按一下上傳後設資料檔案。



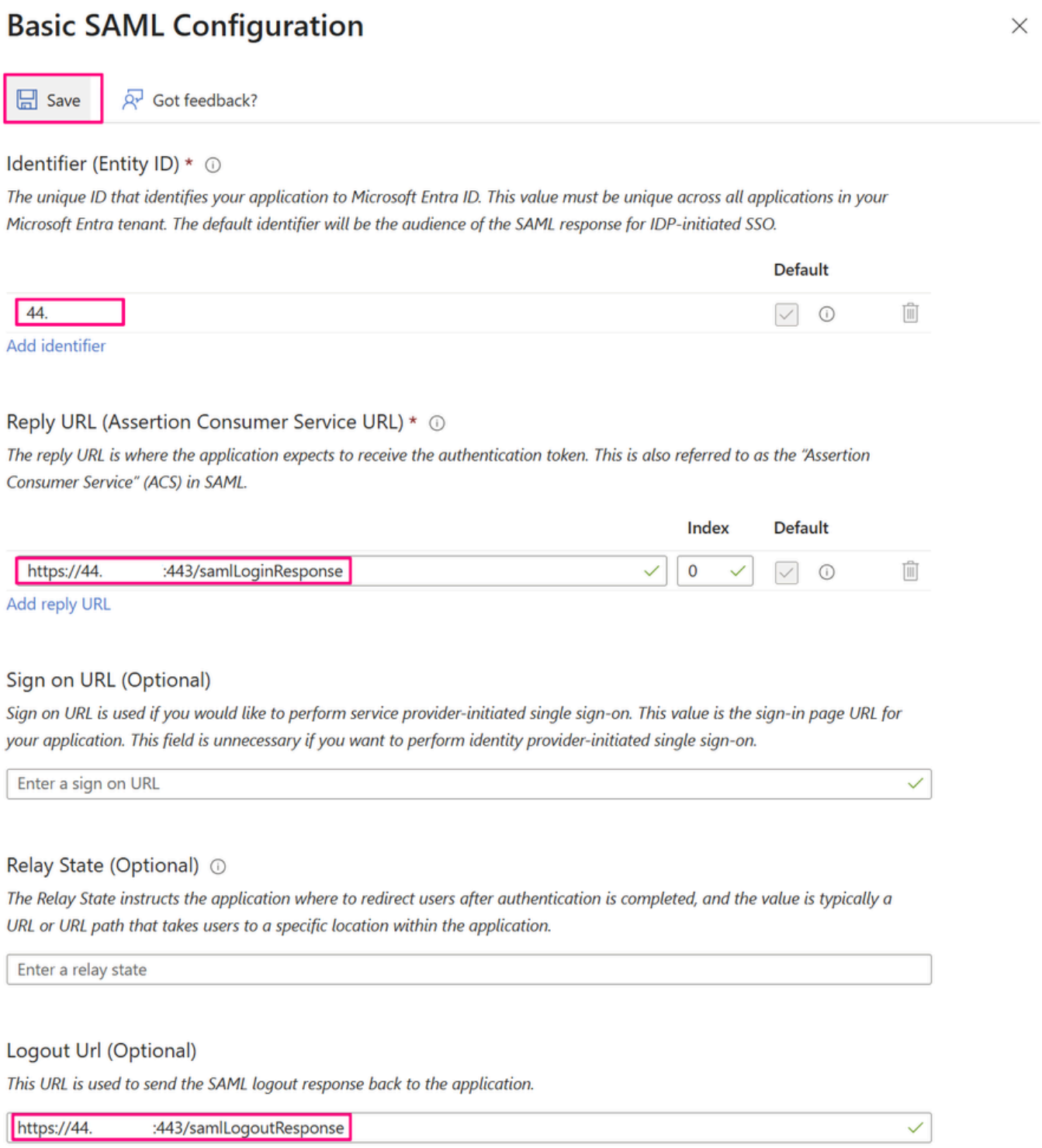
「使用SAML的SSO配置」頁

- 在Upload metadata file視窗中，瀏覽並點選之前下載的metadata XML檔案，然後按一下Add。



上載後設資料檔案視窗

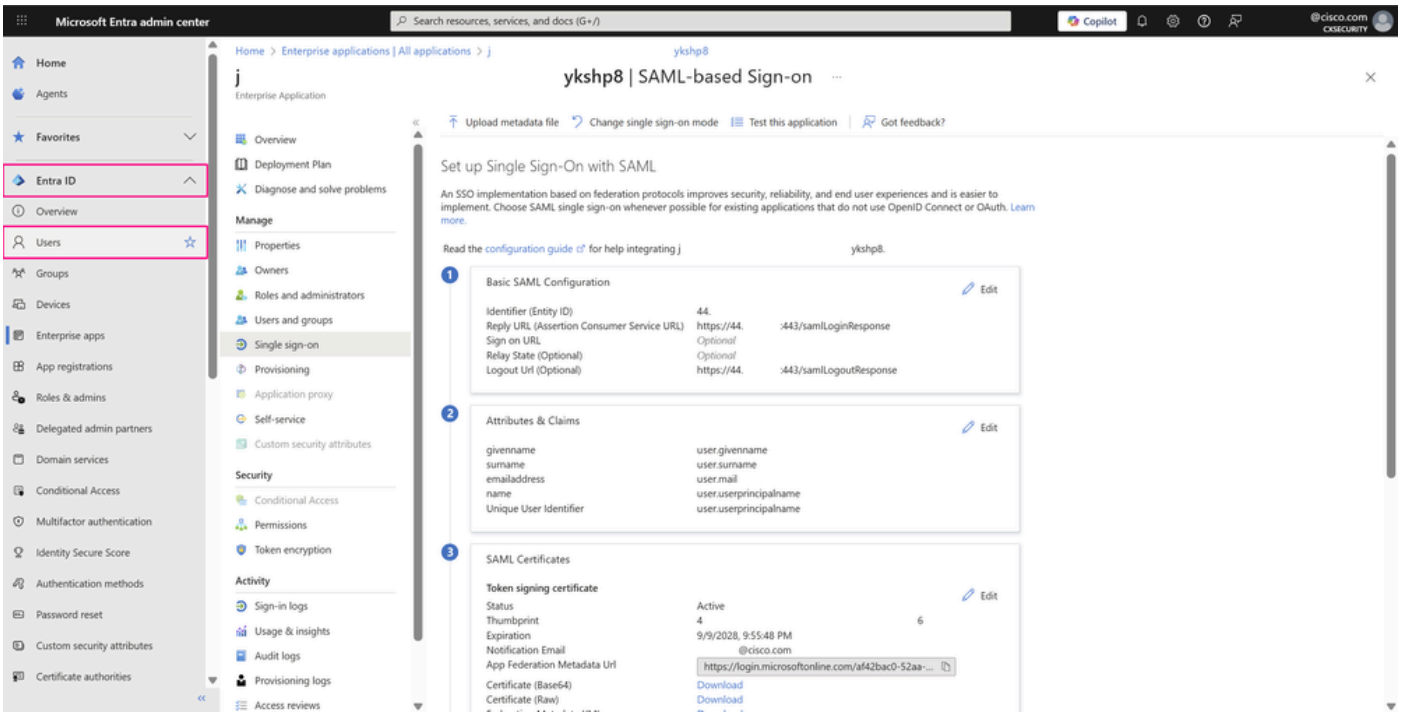
- 在基本SAML配置視窗中，識別符號(實體ID)通常是應用程式特定的URL（在本例中為Cisco SD-WAN管理器），您將與其整合（如前面的步驟所述）。 成功上載檔案後，回覆URL和註銷URL值將自動填充。要繼續，請按一下Save。



基本SAML配置視窗

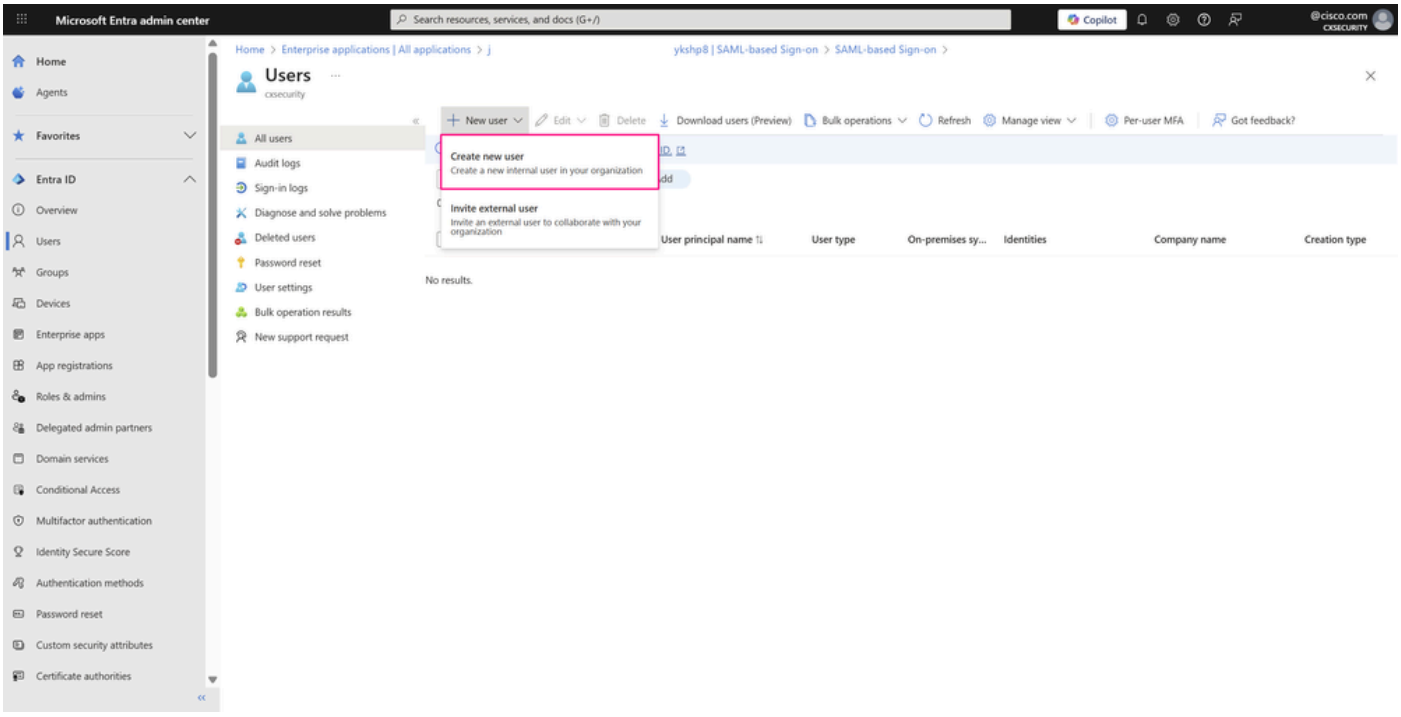
步驟3.將使用者或組帳戶新增到企業應用程式

- 在定義應用程式的SAML配置引數後，可以繼續將登入到該應用程式的使用者或組新增到企業應用程式中。為此，請首先導航到Entra ID > Users，或在門戶頂部的搜尋欄中搜尋服務名稱時也可以訪問此服務，如上一步所示。



「使用SAML的SSO配置」頁

- 建立與組關聯的使用者，以說明使用Cisco SD-WAN Manager及其使用者組之一netadmin（在生產環境中最常見）進行SSO身份驗證。為此，請導航到Entra ID > Users。接下來，單擊New user，然後選擇Create new user。

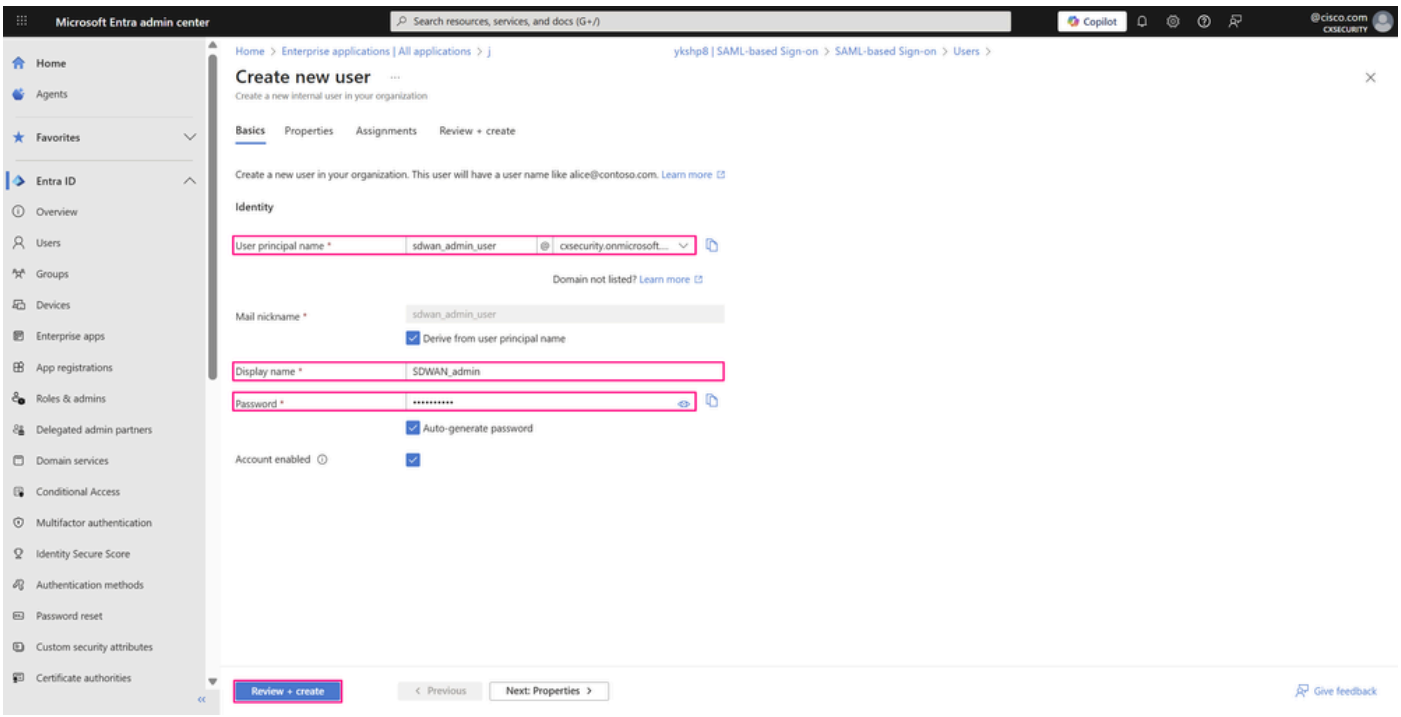


使用者控制面板

- Basics頁籤包含建立新使用者所需的核心欄位。
  - 對於User principal name，輸入唯一使用者名稱，然後從組織中可用的域下拉選單中選擇域。
  - 輸入用戶的顯示名稱。
  - 如果要輸入自定義密碼，請取消選中Auto-generate password，或者選中此選項以自動

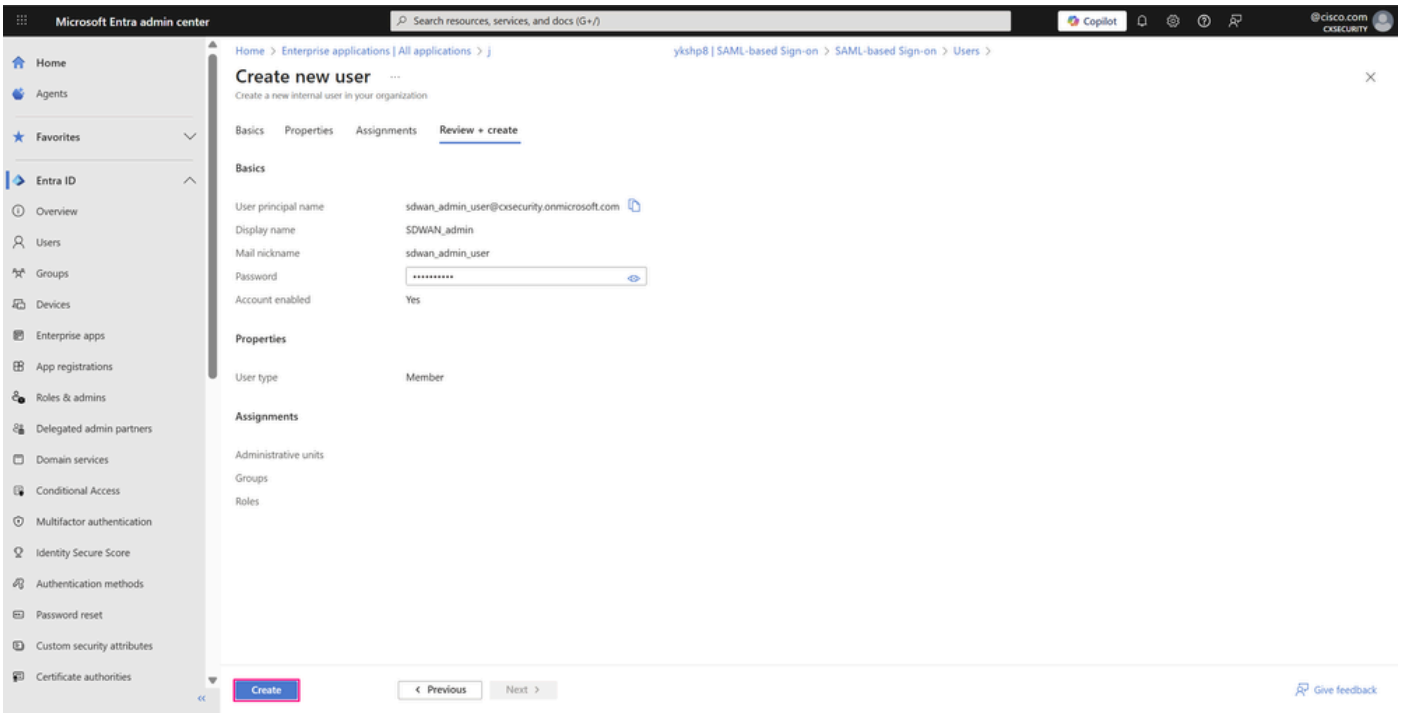
生成密碼。

- 您可以將該使用者新增到Assignments頁籤中的組，但由於尚未建立組成員身份，請單擊Review + create。



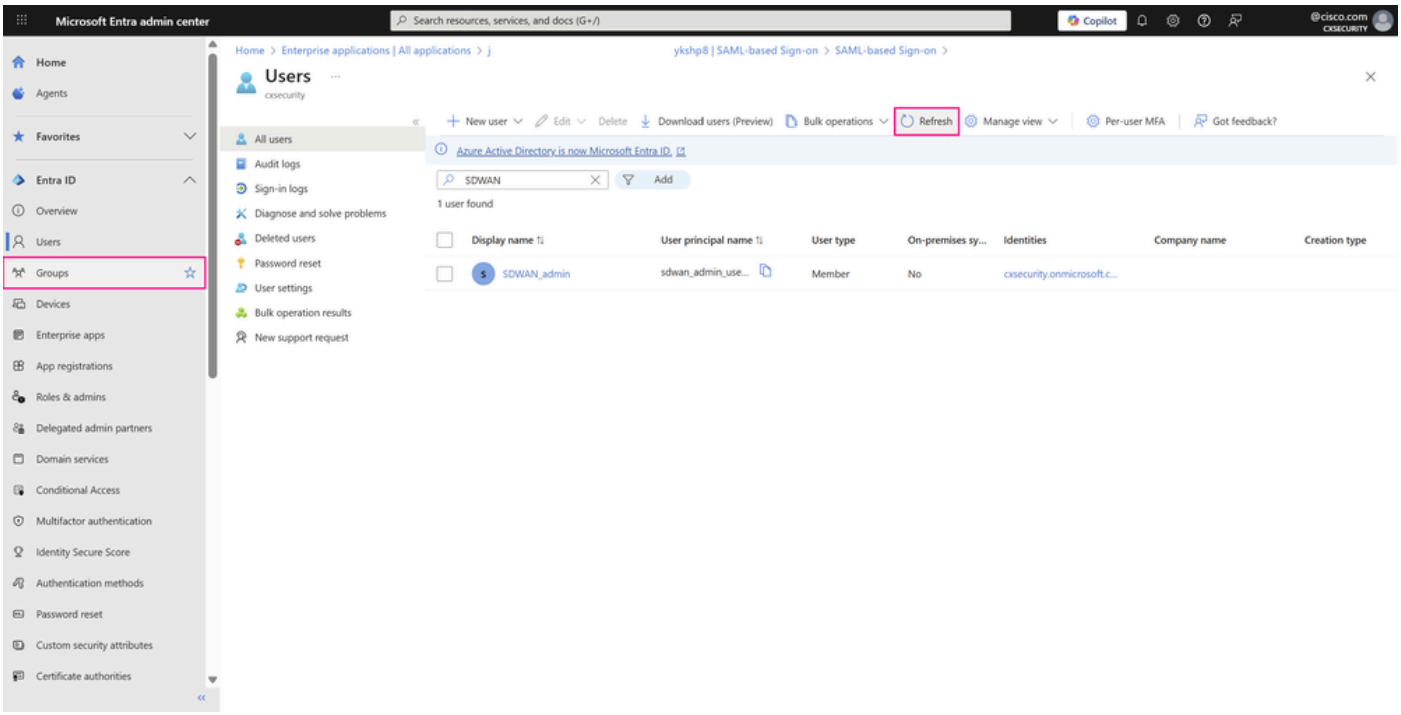
「使用者建立」頁

- 最後一個頁籤顯示使用者建立工作流程中的關鍵詳細資訊。檢視詳細資訊，然後按一下Create完成該過程。



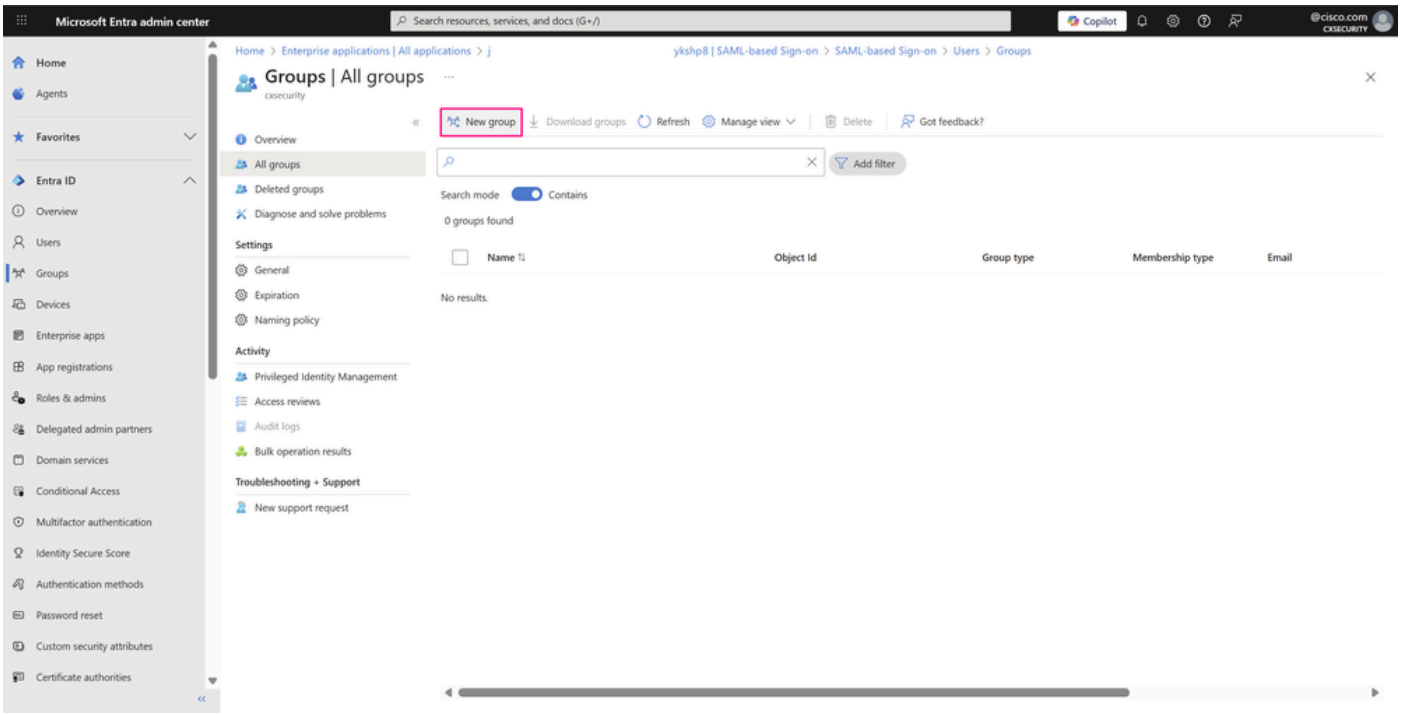
「使用者建立」頁

- 新使用者將在稍後顯示。如果沒有，則按一下Refresh並使用服務中的搜尋欄搜尋使用者。接下來，導航到Entra ID > Groups > All groups，以建立新組。



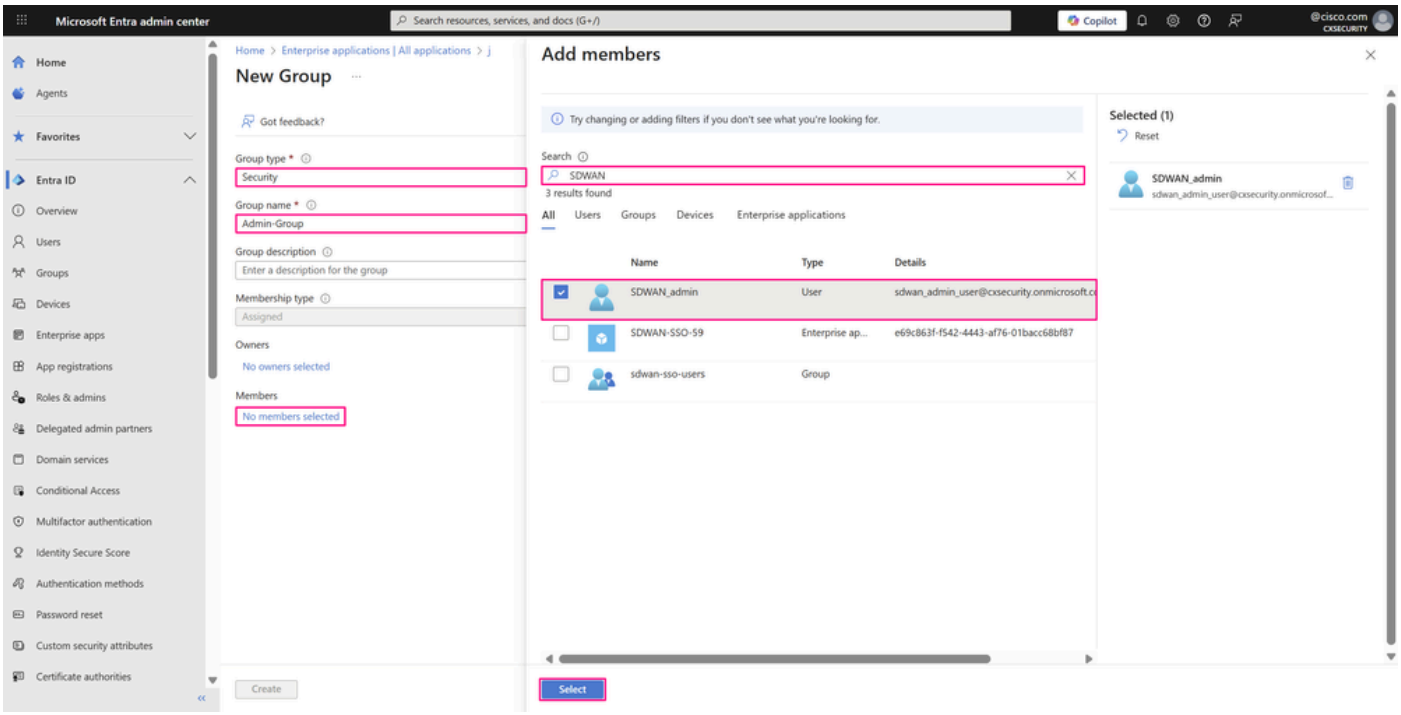
使用者控制面板

- 在此頁上，可以管理組織中的不同組及其許可權。單擊「新建組」以建立具有網路管理員許可權的組。



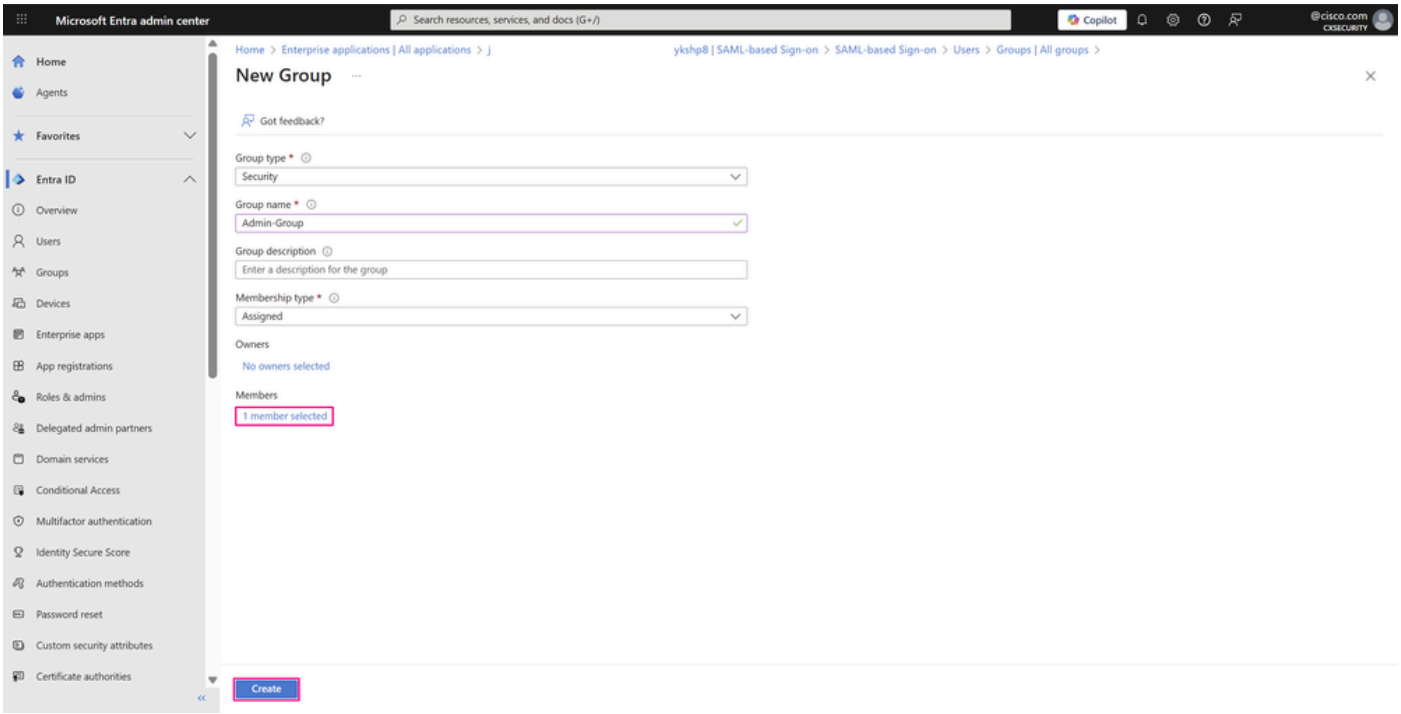
「所有組」頁

- 從下拉選單中選擇Group type — 在本例中為Security，因為只需要訪問共用資源。輸入您選擇的引用該組的角色或許可權的組名稱。此時，當您按一下「成員」欄位中的選定成員時，將使用者與該組相關聯。
    - 在「Add members」視窗中，瀏覽並選擇要新增的使用者（在我們的示例中，為剛建立的使用者），然後按一下Select。



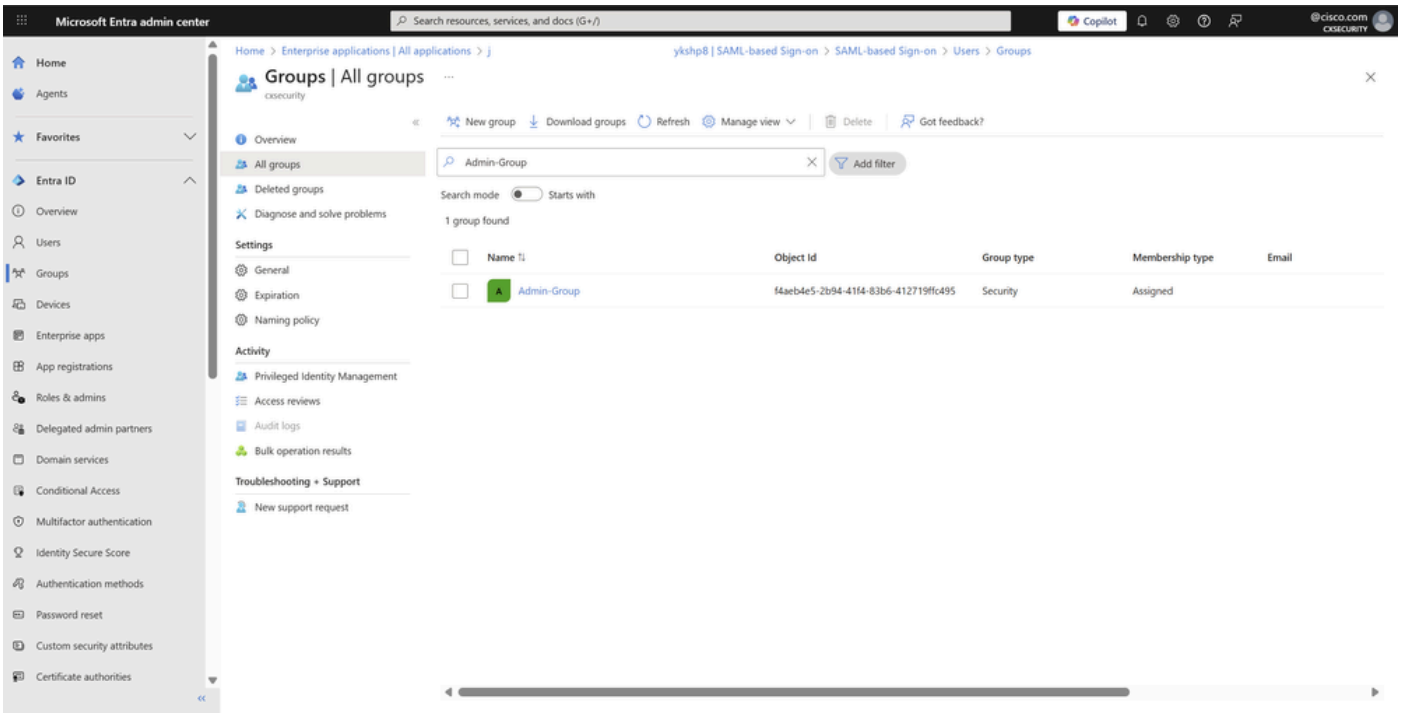
「組建立」頁

- 按一下建立以建立組。



「組建立」頁

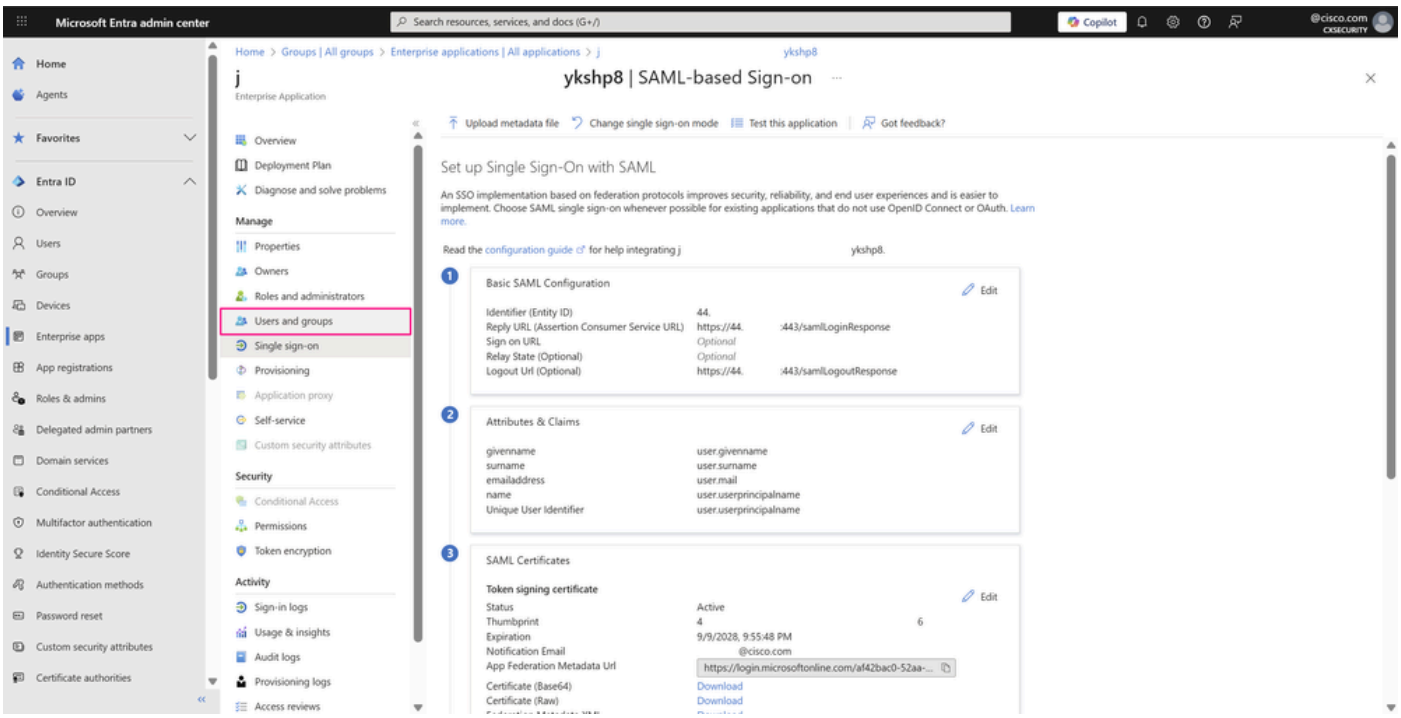
- 新組將在稍後顯示。如果沒有，請按一下刷新，然後使用服務中的搜尋欄搜尋組名。重複前面的步驟以建立其他使用者並將其新增到其他組成員身份，以驗證應用程式及其其他使用者組（如操作員）的SSO登入。



「所有組」頁

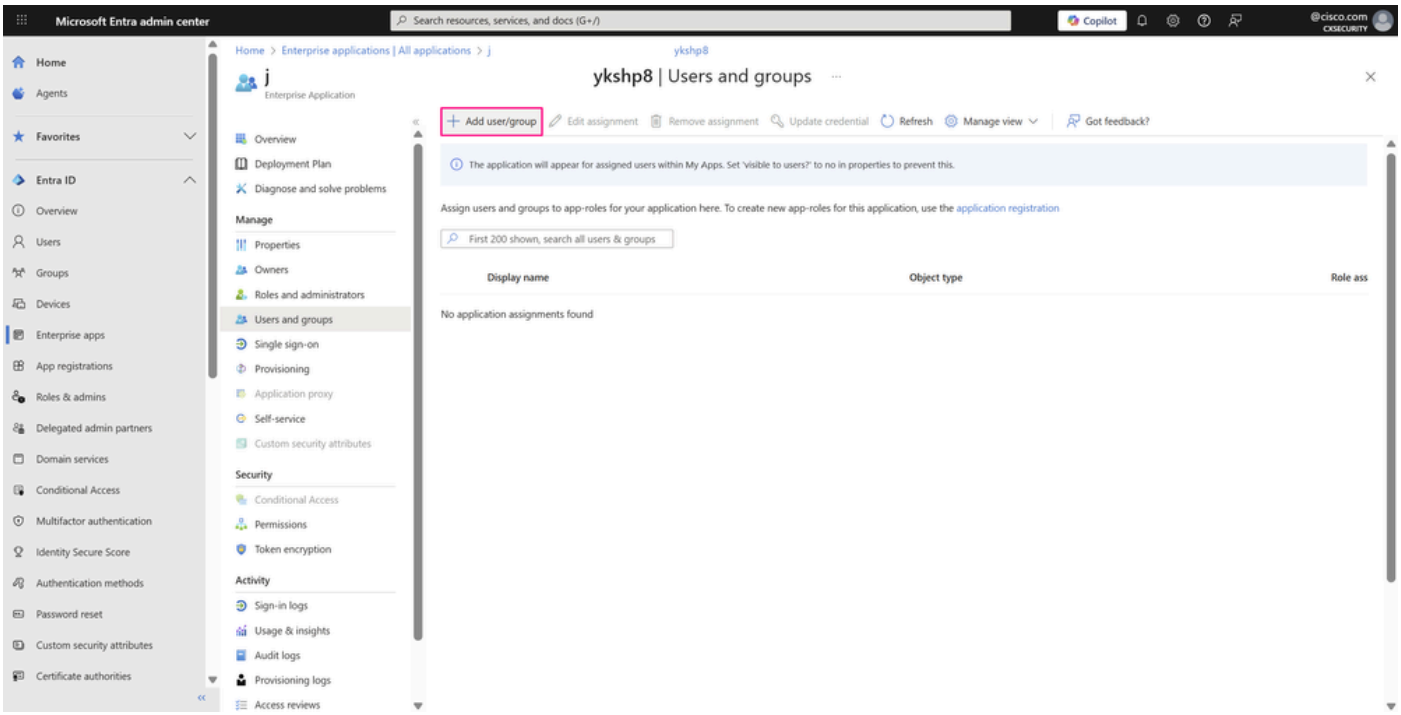
步驟4.為Microsoft Entra ID配置SAML組設定

- 要預配SAML配置中與其關聯的組或使用者，您需要將它們分配給您的企業應用程式，以便它們擁有您的應用程式（例如Cisco SD-WAN Manager）的登入許可權。導航回Entra ID > Enterprise apps，然後開啟您的企業應用程式。在左側選單的Manage部分中，按一下Users and groups。



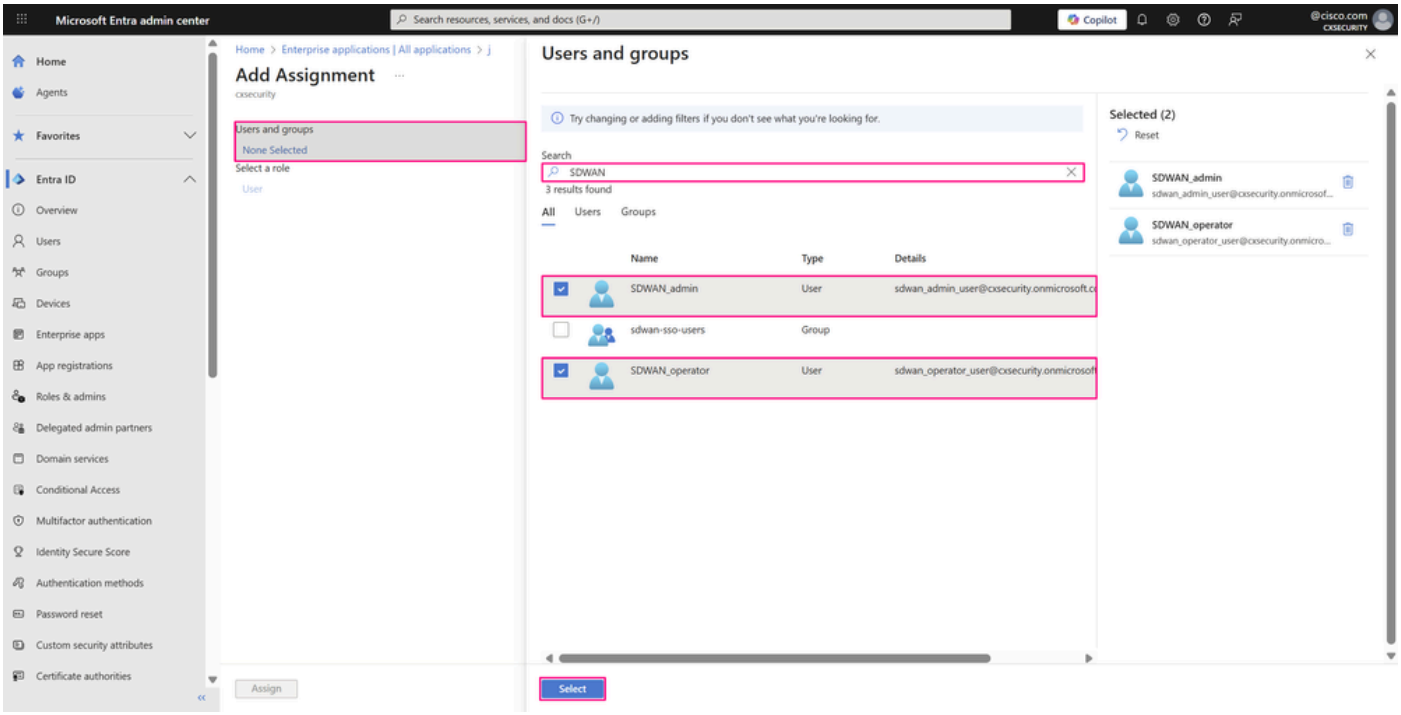
「使用SAML的SSO配置」頁

- 接下來，按一下Add user/group。



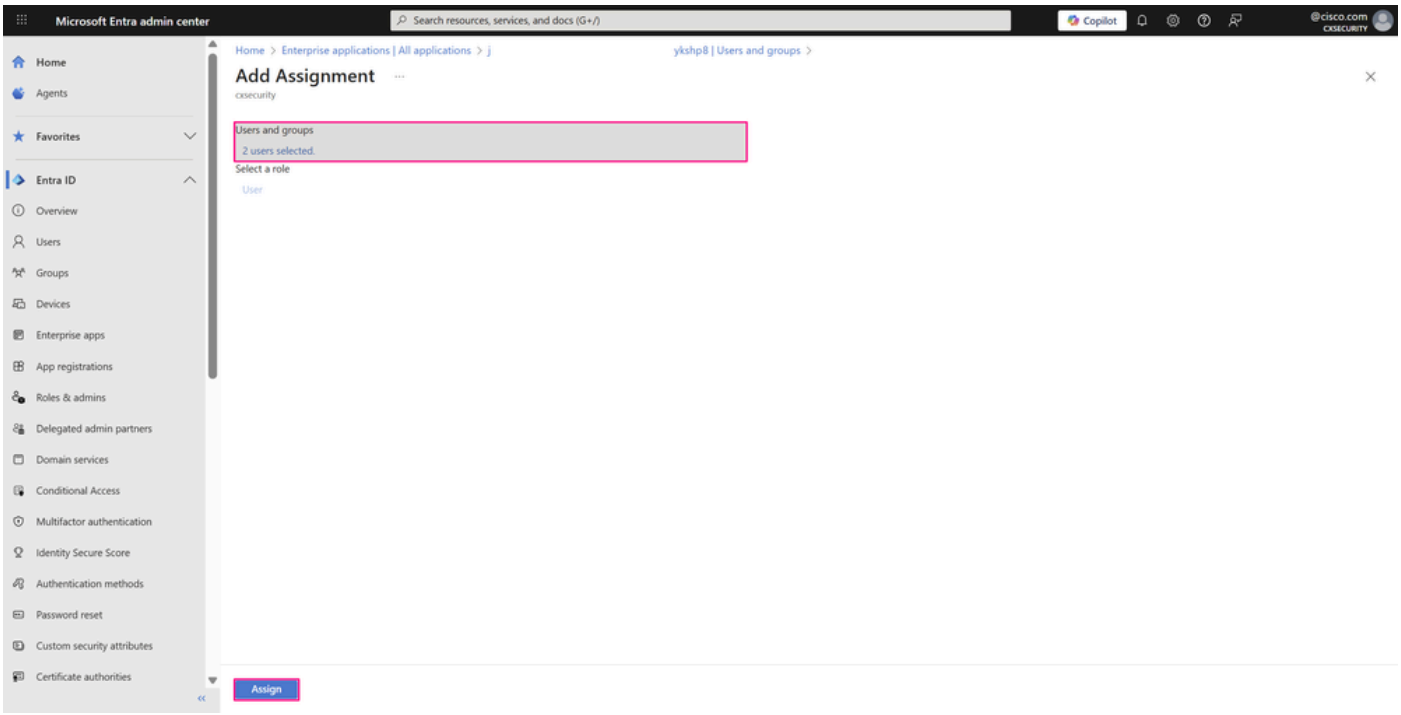
「使用者和組」頁

- 在Add Assignment窗格中，按一下Users and groups欄位下的None Selected。搜尋並選擇要分配給應用程式的使用者或組(在我們的示例中，是在前面步驟中建立的兩個使用者)，然後按一下選擇。



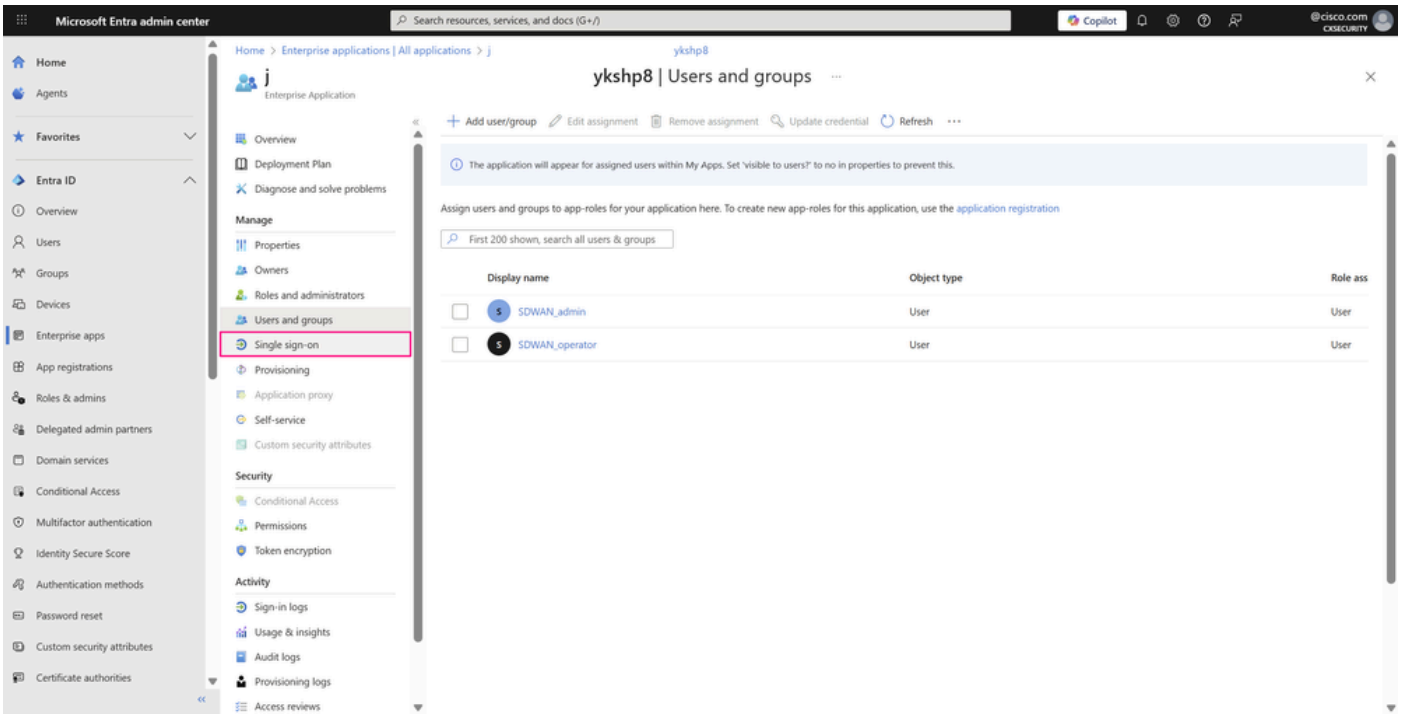
使用者/組分配窗格

- 按一下Assign將使用者或組分配給應用程式。



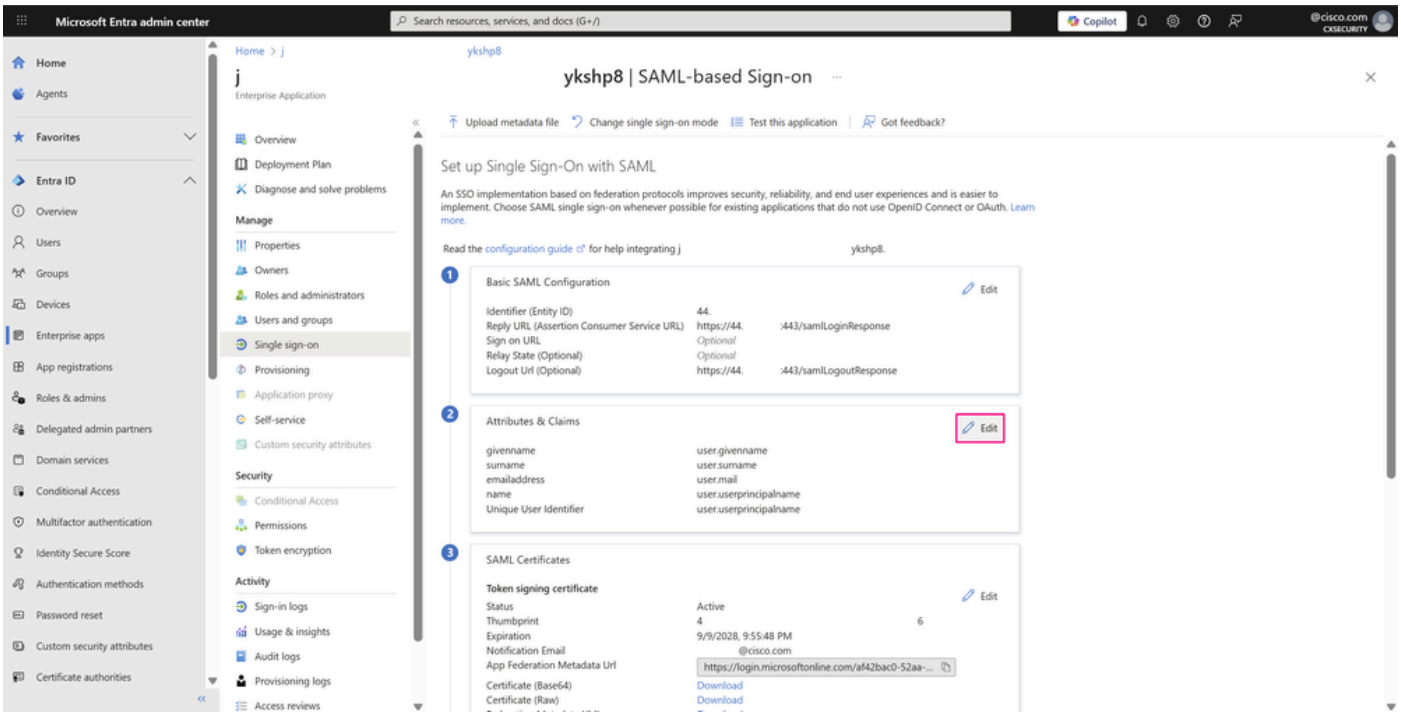
使用者/組分配窗格

- 分配給您的企業應用程式的使用者會在分配後不久列出。在左側選單的Manage部分中按一下Single sign-on，訪問應用程式的SSO SAML配置，並完成其餘必需的配置。



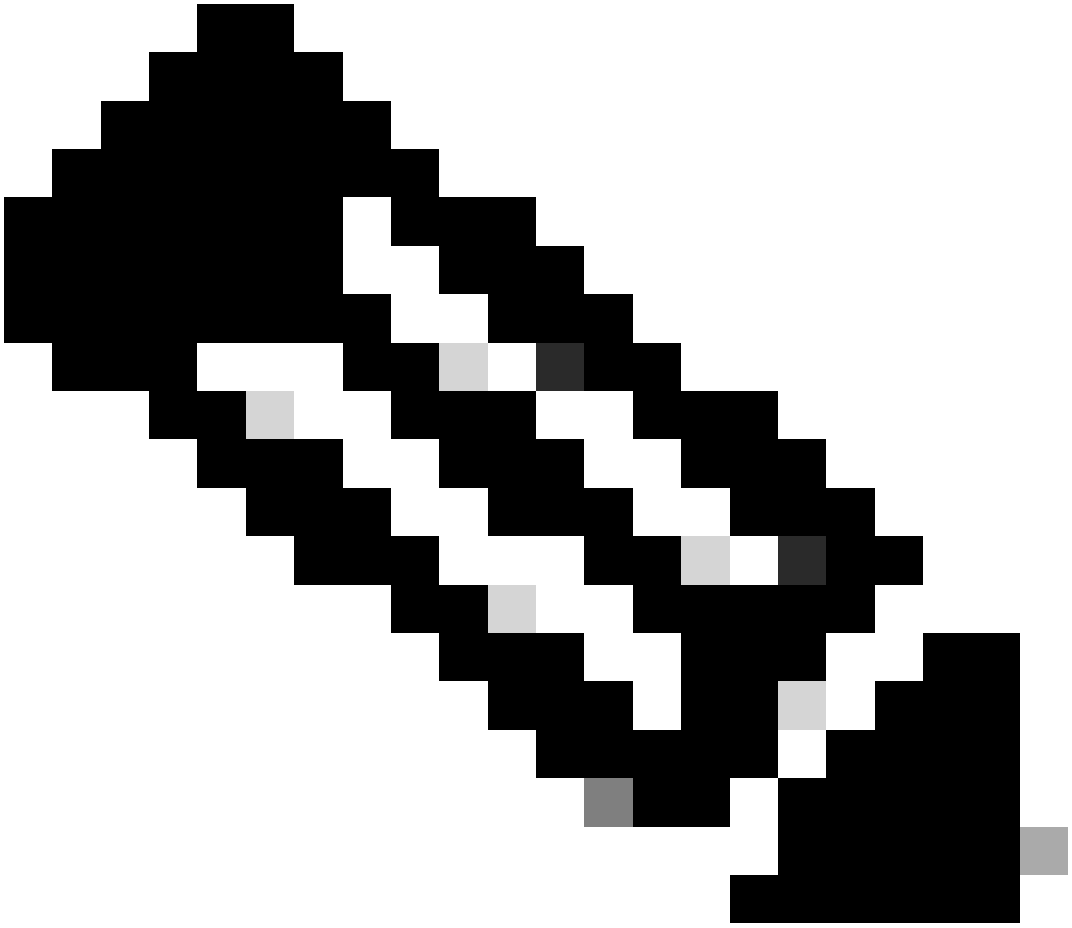
「使用者和組」頁

- 在使用SAML設定單一登入頁面的Attributes & Claims下，按一下Edit。

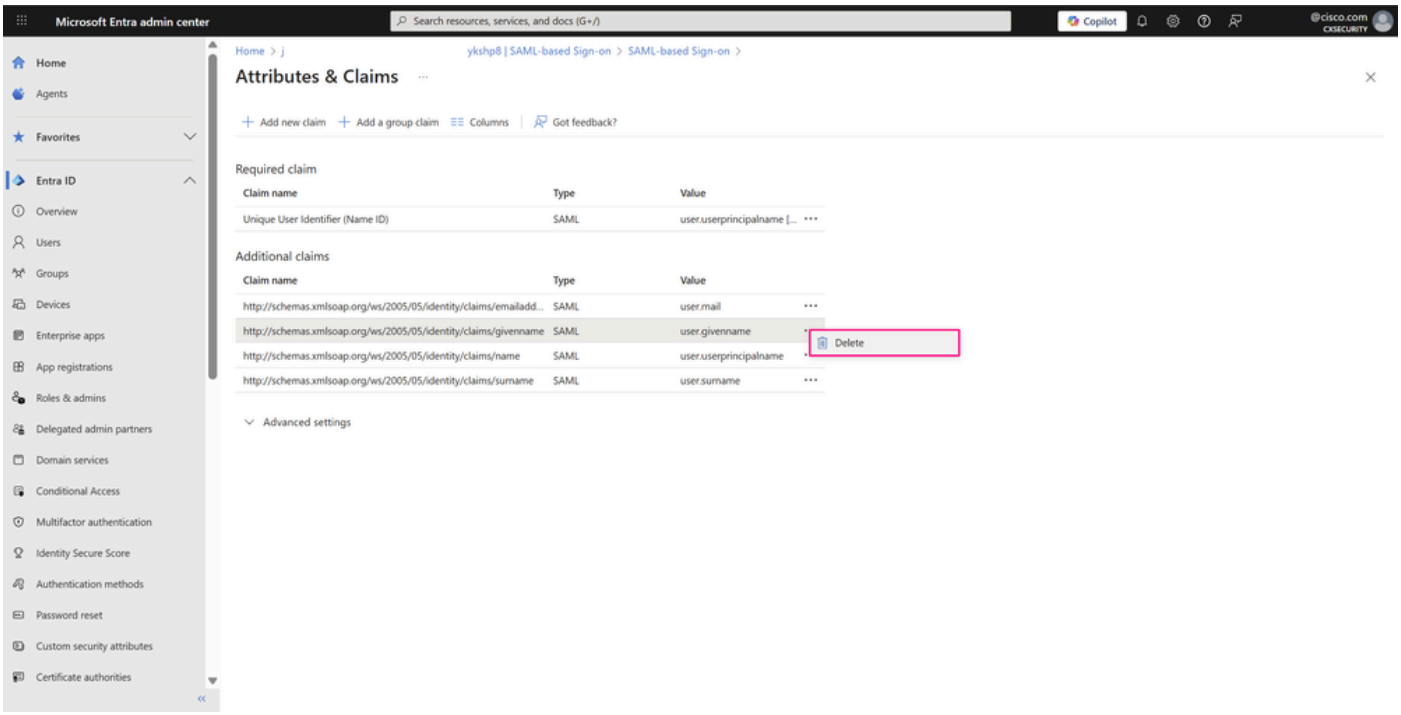


「使用SAML的SSO配置」頁

- 在「屬性和宣告」(Attributes & Claims)頁面上，按一下三點圖標，然後按一下刪除以刪除值為user.givenname的宣告和值為user.surname的宣告，因為本示例不需要這些宣告。對於應用程式的基本的SSO身份驗證，僅需要下一個宣告：
    - user-user.mail的電子郵件地址
    - user-user.userprincipalname的使用者主體名稱(UPN)

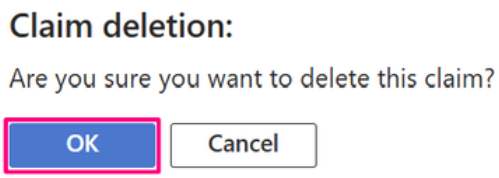


附註：您的組織可能根據自身的特定需求要求其他索賠。



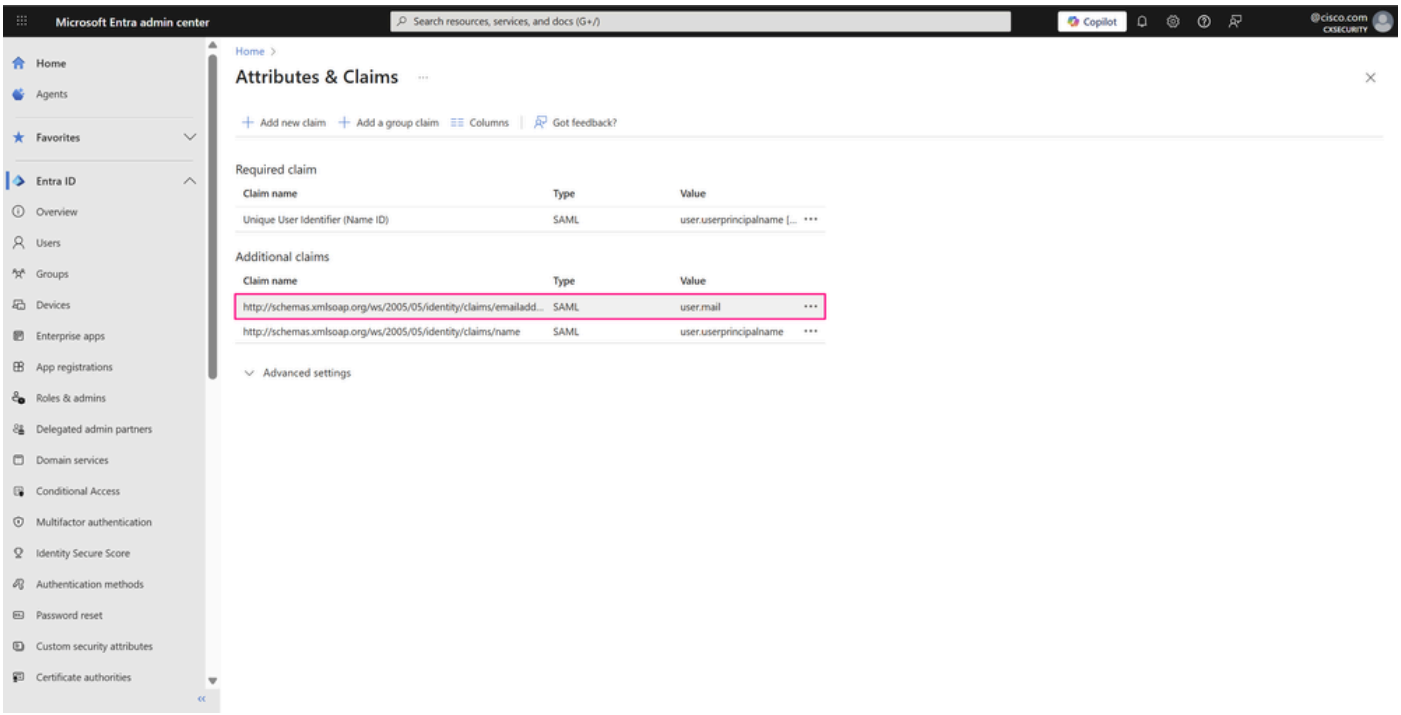
屬性和宣告頁

- 在「Claim deletion」視窗中，按一下OK以刪除該索賠。



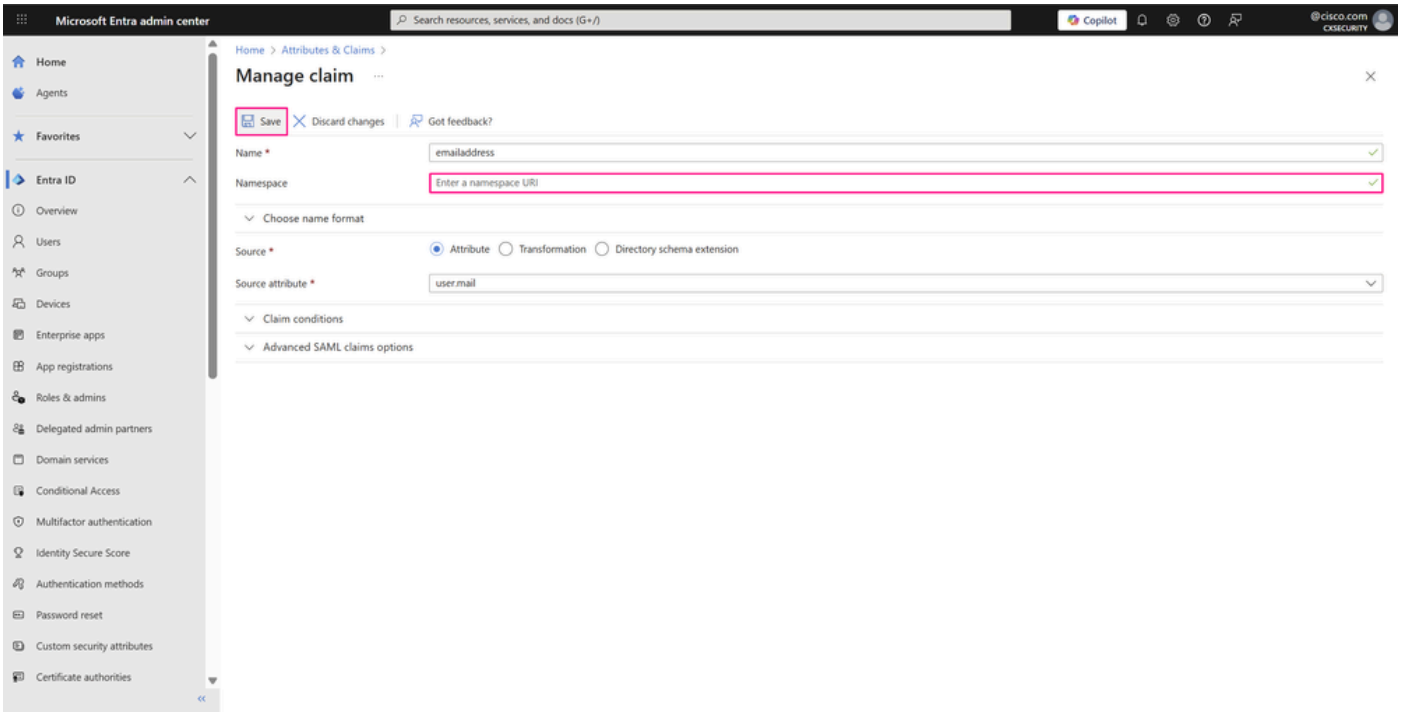
報銷申請刪除視窗

- 接下來，從其餘兩個宣告中的宣告名稱中刪除名稱空間，因為此欄位是可選的。此更改允許在此頁面上顯示每個的實際名稱，以便於識別。將滑鼠懸停在每個宣告上，然後按一下它以訪問其設定。



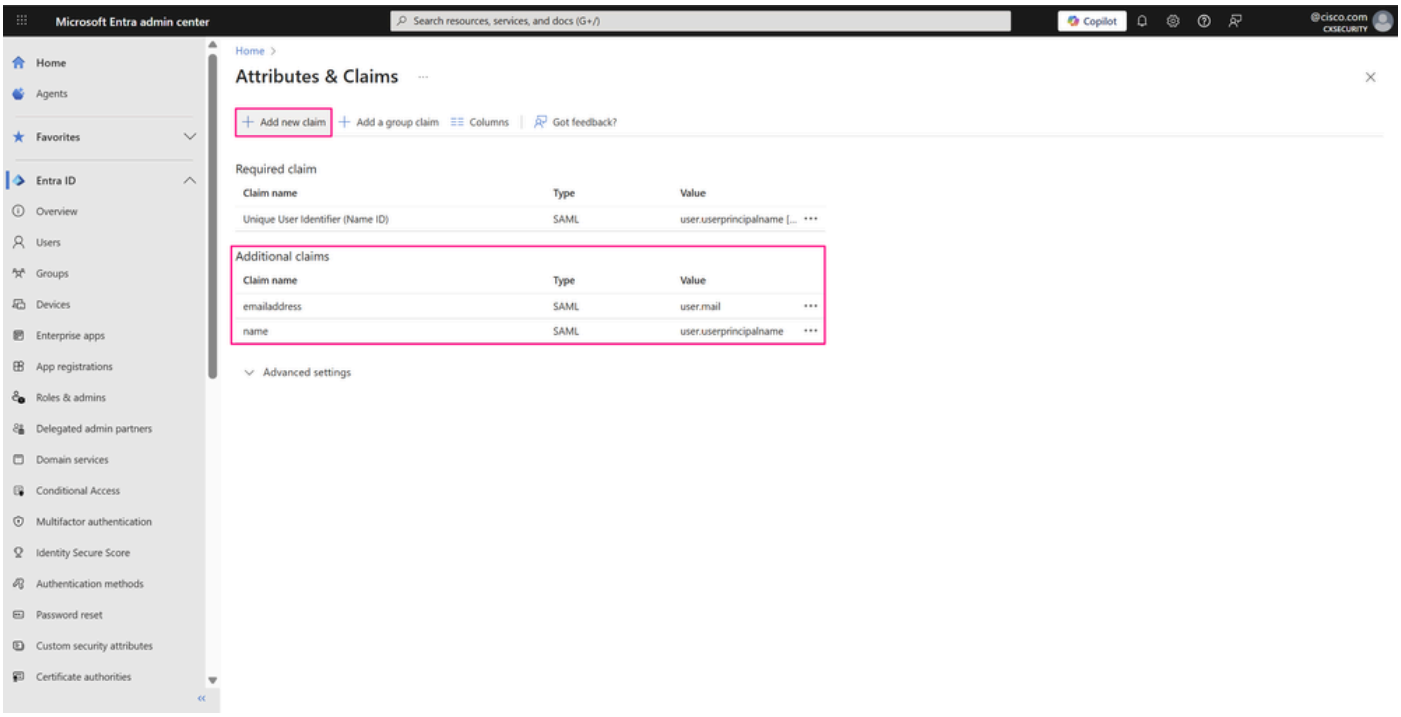
屬性和宣告頁

- 在Manage claim頁面上，刪除Namespace欄位，然後按一下Save以應用更改。



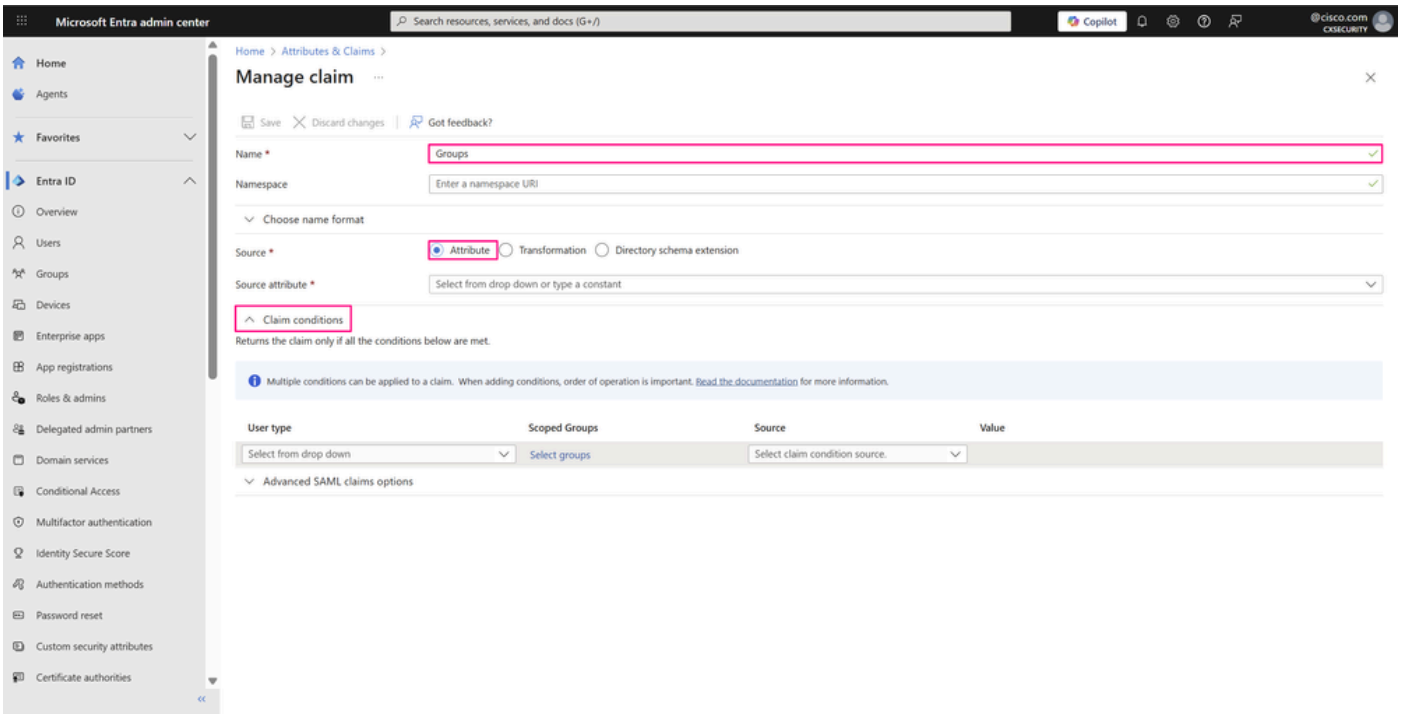
管理報銷申請頁面

- 現在可以看到兩個所需宣告的名稱。但是，還需要一個附加宣告，以定義使用者所屬的組和授權訪問應用程式資源的組。為此，請按一下新增新宣告。



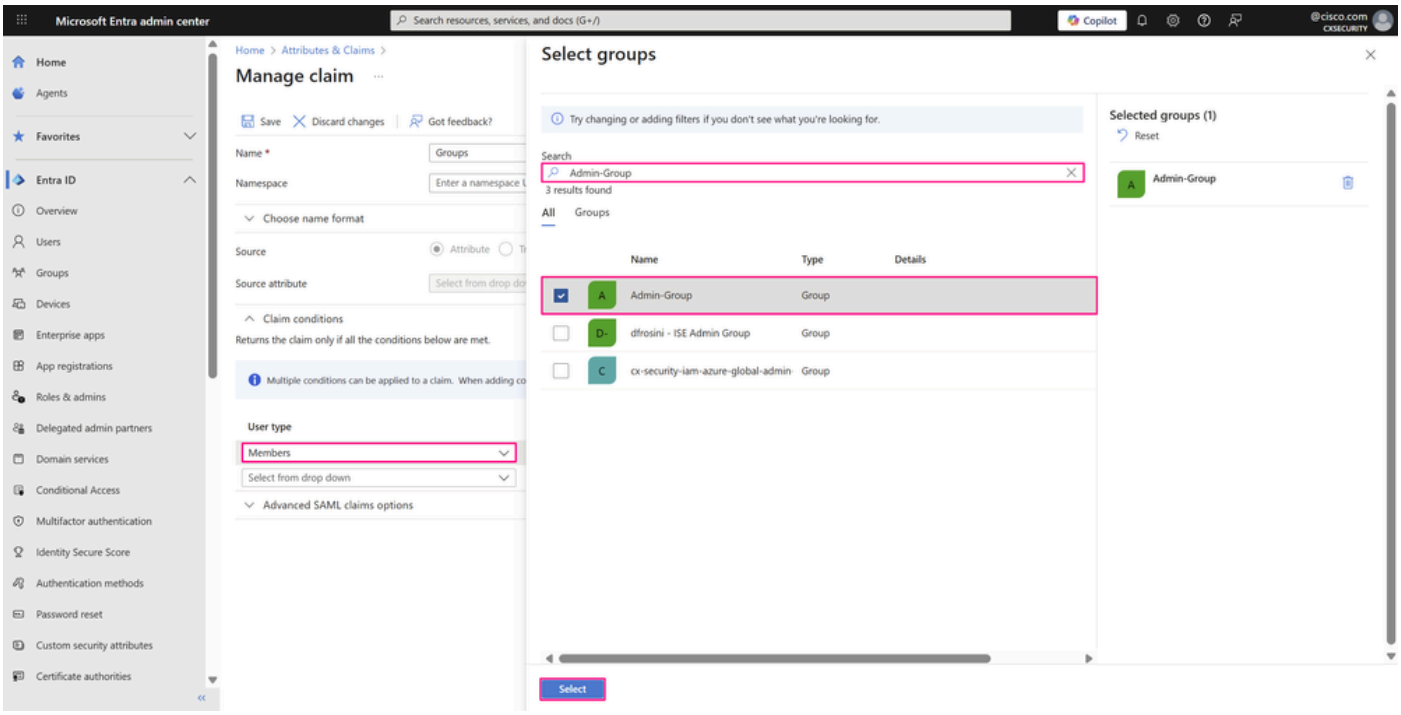
屬性和宣告頁

- 輸入名稱以標識此宣告。在Source旁邊，選擇Attribute。然後按一下Claim conditions展開選項並配置多個條件。



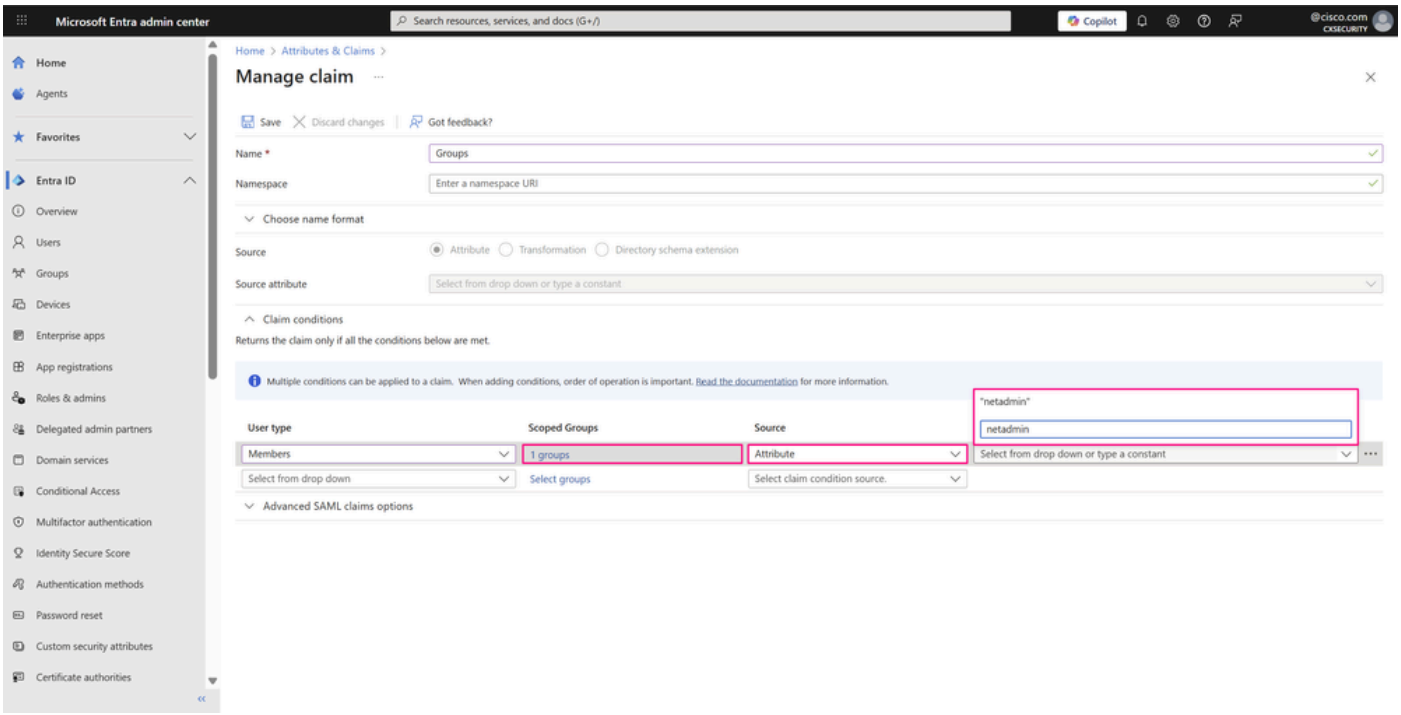
管理報銷申請頁面

- 在宣告條件中，從User type下拉選單中選擇Members，然後按一下Select Groups以選擇使用者必須所屬的組，然後按一下Select。



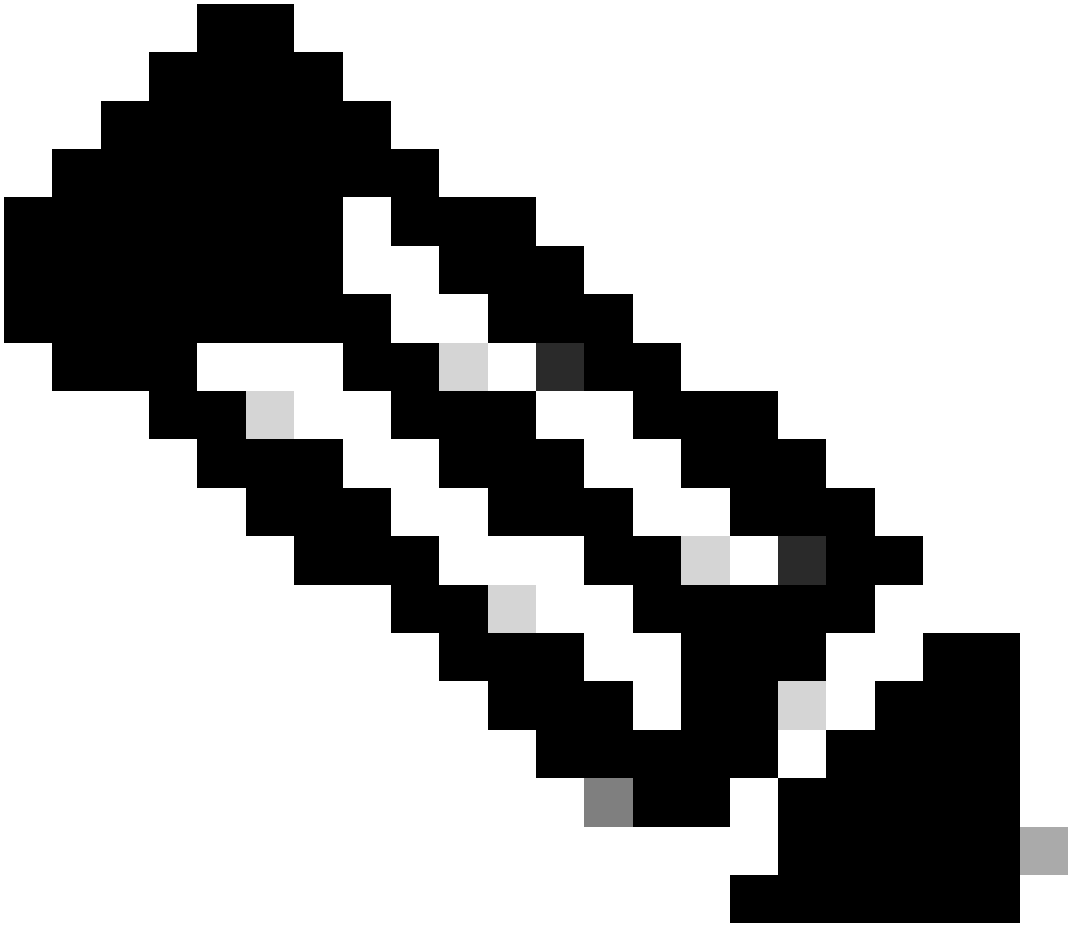
管理報銷申請頁面

- 從Source下拉選單中選擇Attribute，在此項宣告中檢索其值。在值欄位中，輸入引用應用程式中定義的使用者組的自定義屬性。在本例中，netadmin是Cisco SD-WAN Manager中的標準使用者組之一。請輸入屬性值（不含引號）並按Enter。

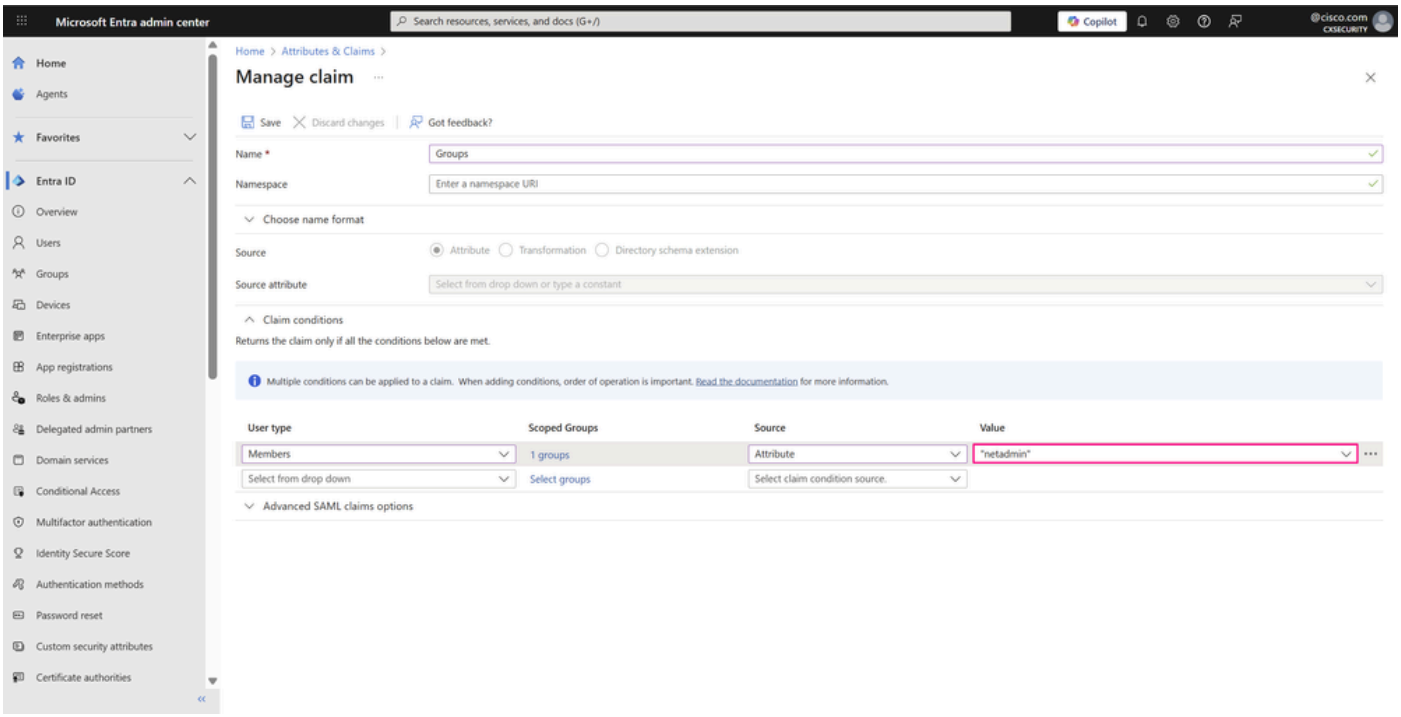


管理報銷申請頁面

- 緊接之後，屬性值會帶引號出現，因為Microsoft Entra ID將此值處理為字串。

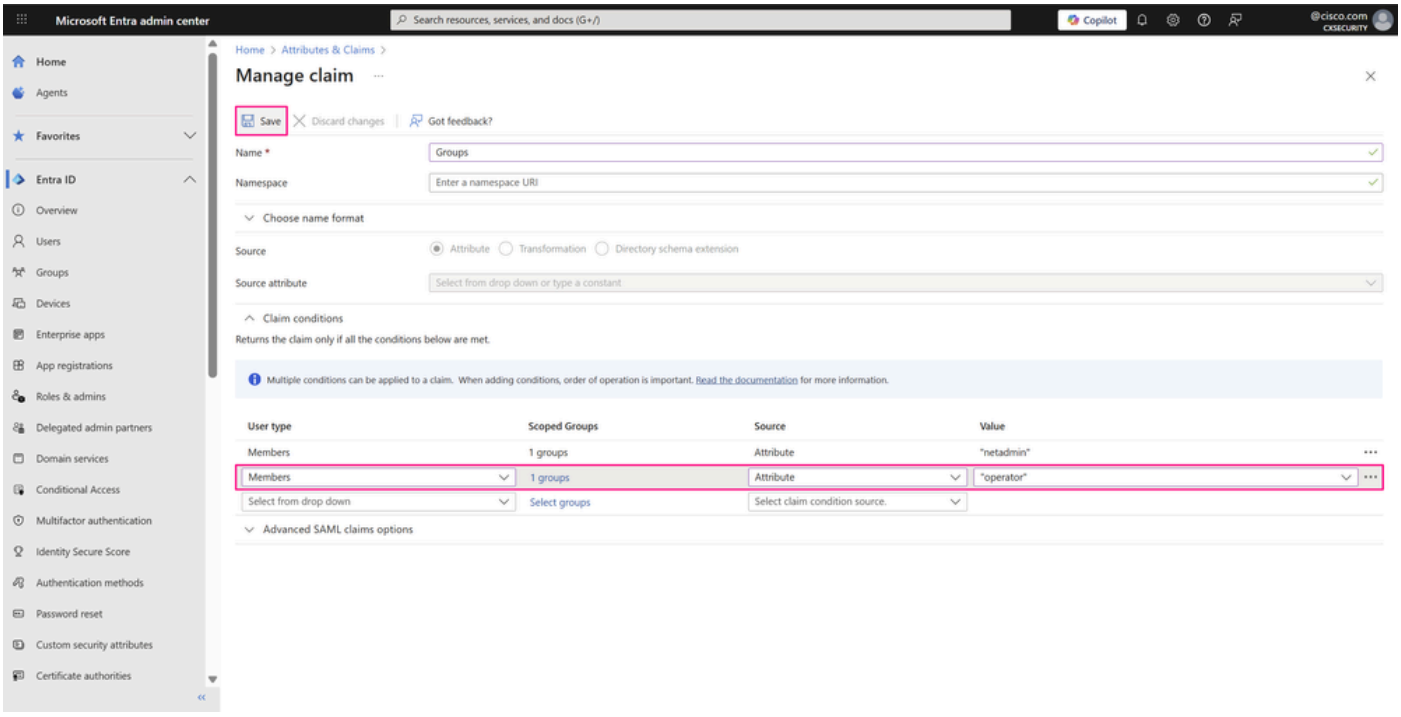


附註：宣告條件中的這些引數在企業應用程式的SSO SAML配置中高度相關，因為這些自定義屬性必須始終與Cisco SD-WAN Manager中定義的使用者組匹配。此匹配項根據使用者所屬的Microsoft Entra ID組確定授予使用者的許可權或許可權。



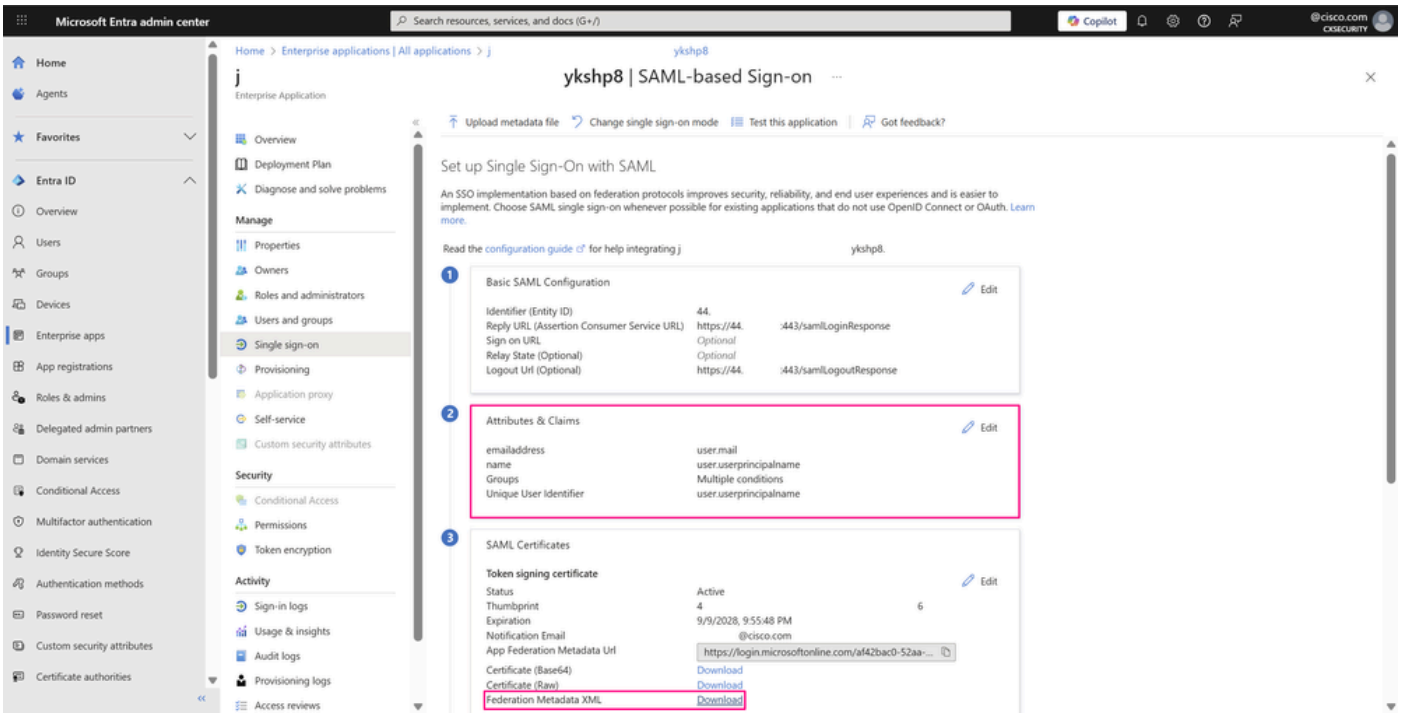
管理報銷申請頁面

- 為所建立的第二個組(該組對映到Cisco SD-WAN Manager中的operator使用者組)重複相同步驟。每個具有要登入到應用程式的特定許可權的不同組都需要此過程。您還可以在單個條件中新增多個組。按一下「Save」以儲存變更。



管理報銷申請頁面

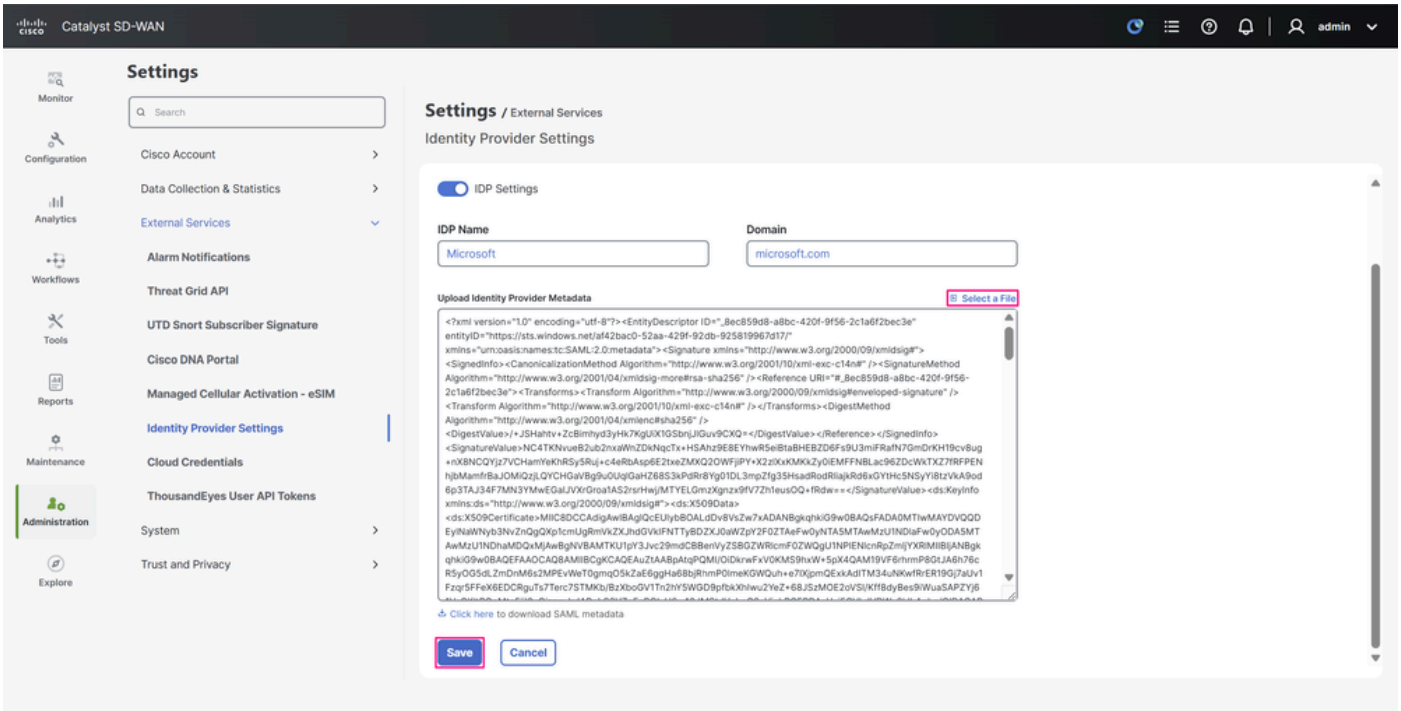
- 在使用SAML設定單一登入頁面上，Attributes & Claims部分顯示所做的新更改。要完成Microsoft Entra ID中的配置，請在SAML Certificates下，按一下Federation Metadata XML旁邊的Download，將提供身份服務的XML檔案下載到應用程式。



「使用SAML的SSO配置」頁

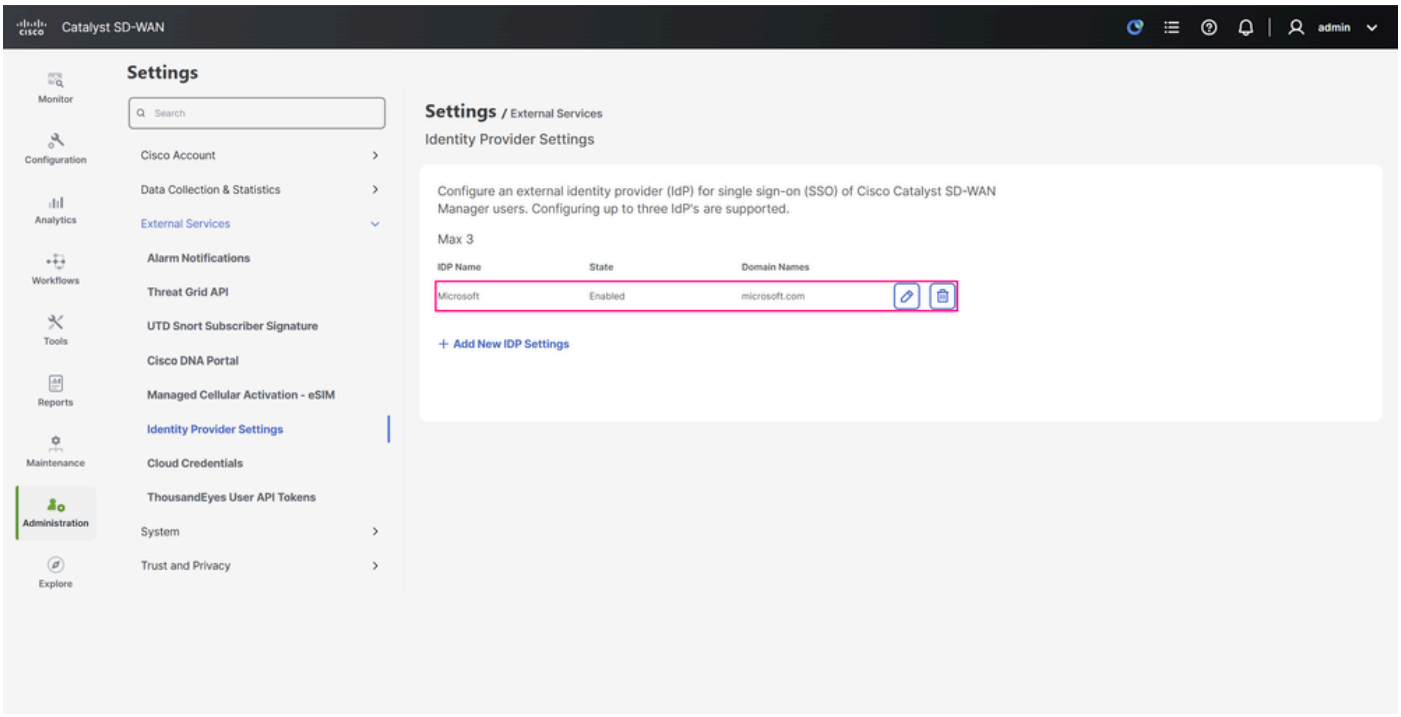
步驟5.將Microsoft Entra ID SAML後設資料檔案匯入Cisco SD-WAN Manager

- 要將聯合後設資料上傳到Cisco SD-WAN Manager，請導航到Administration > Settings > External Services > Identity Provider Settings，然後點選Select a file。選擇剛從Microsoft Entra ID下載的檔案，然後按一下Save。



「IdP設定：配置」頁

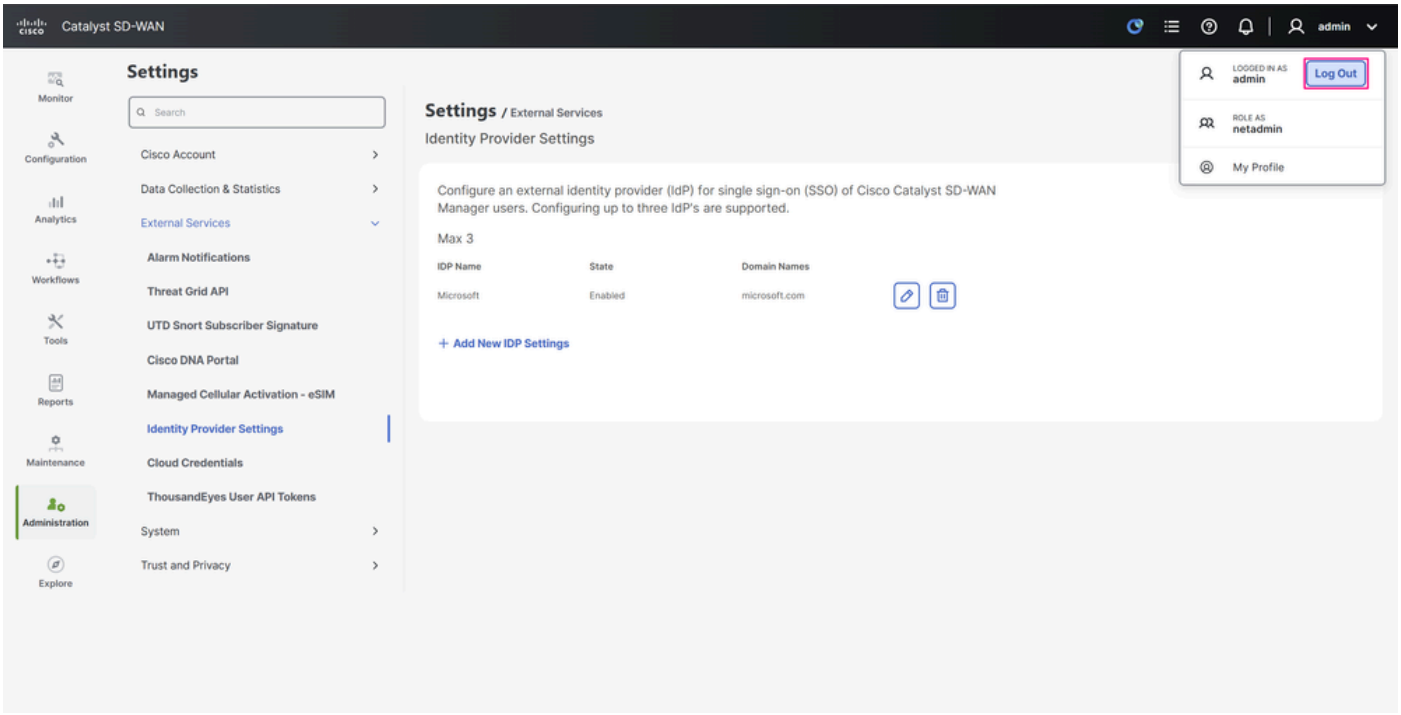
- IdP設定和後設資料現在已儲存。



「IdP設定：配置」頁

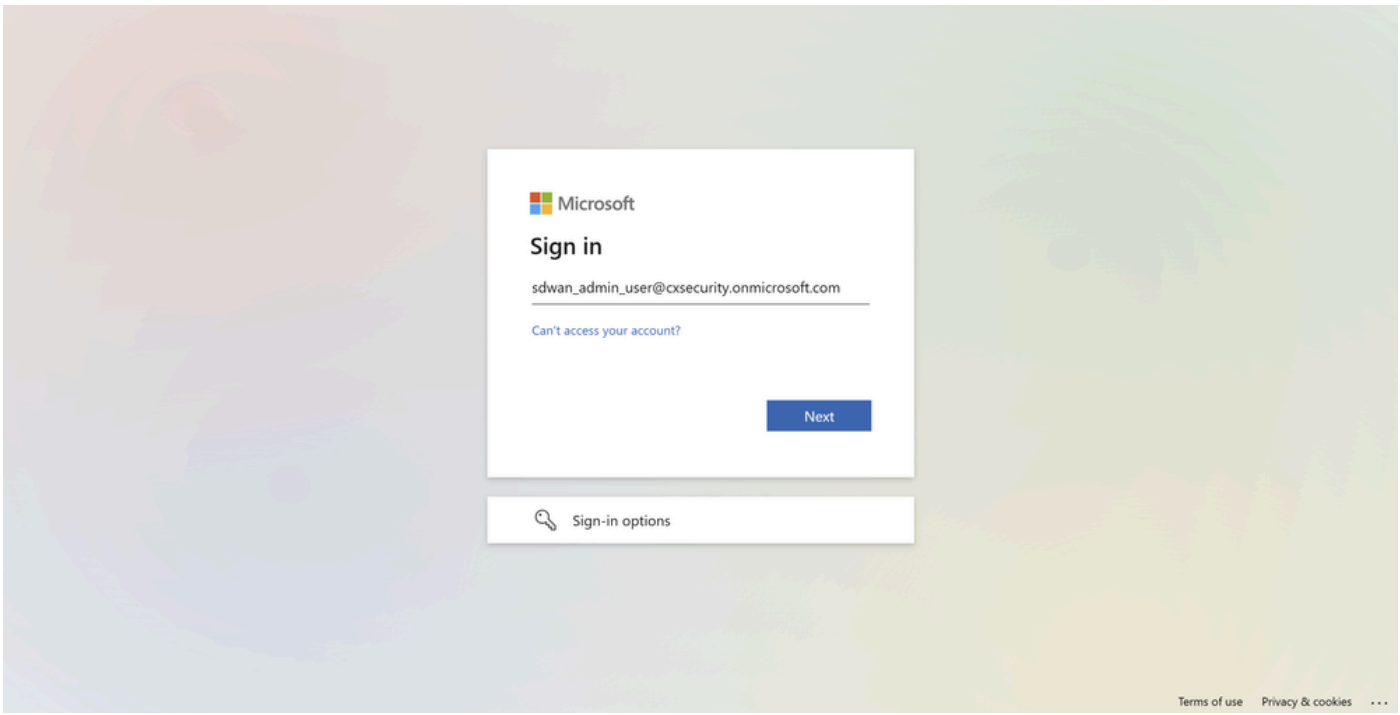
驗證

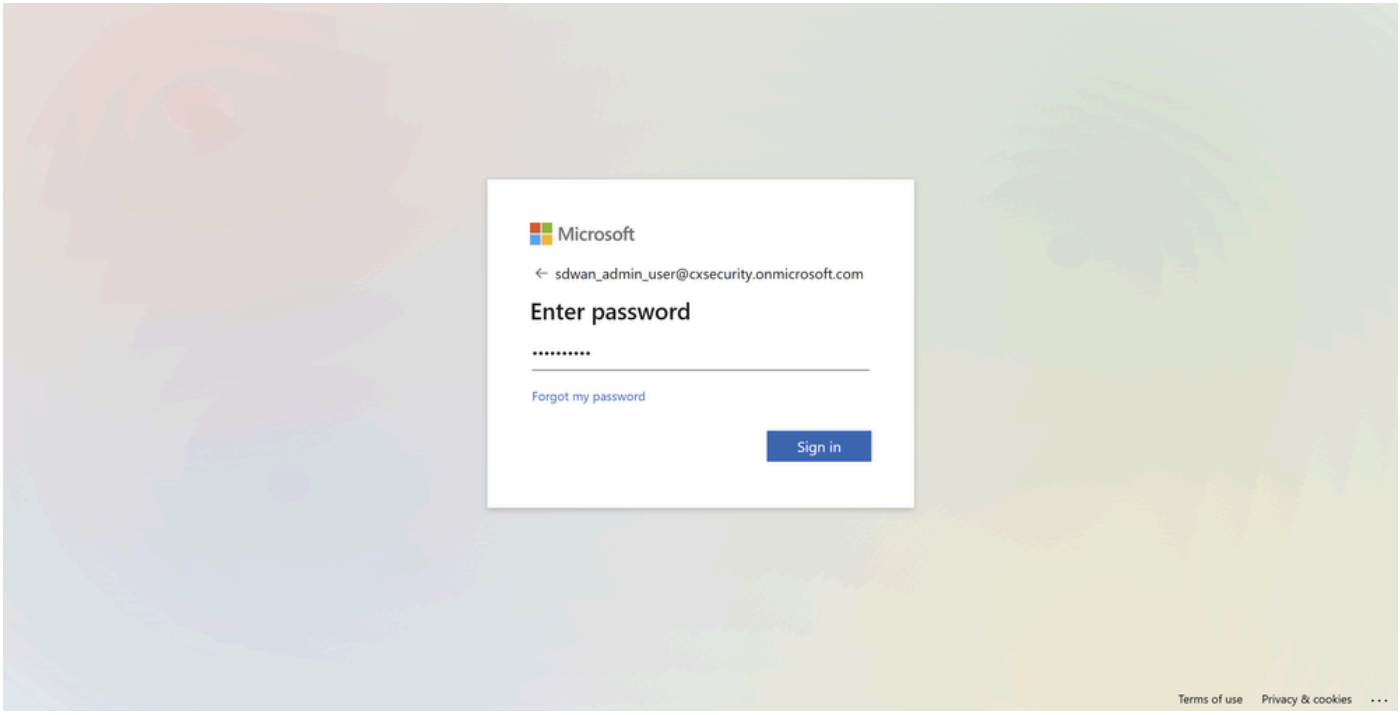
- 按一下UI右上角的配置檔名稱以展開選項，從那裡按一下Log Out以註銷門戶。



配置檔案選單

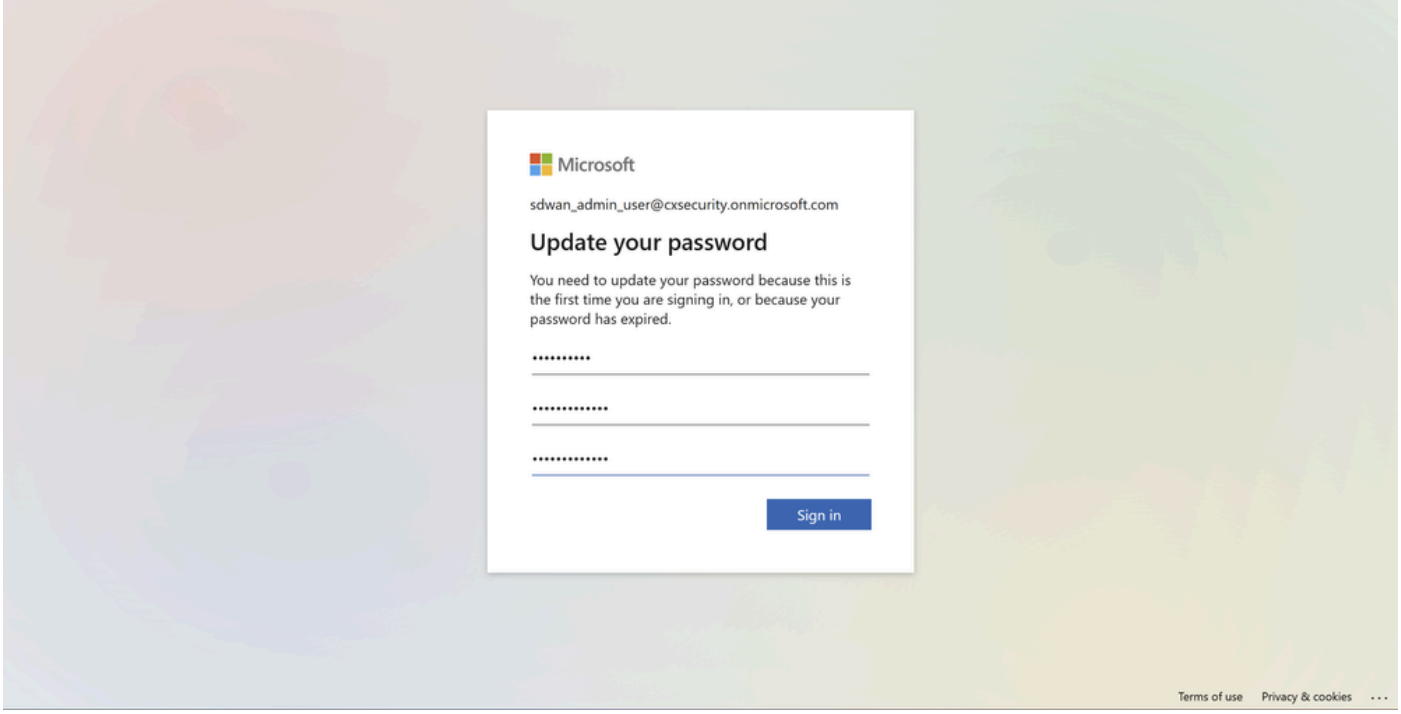
- 您將立即重定向到Microsoft身份驗證螢幕，在該螢幕中使用Microsoft Entra ID SSO使用者的憑據登入。





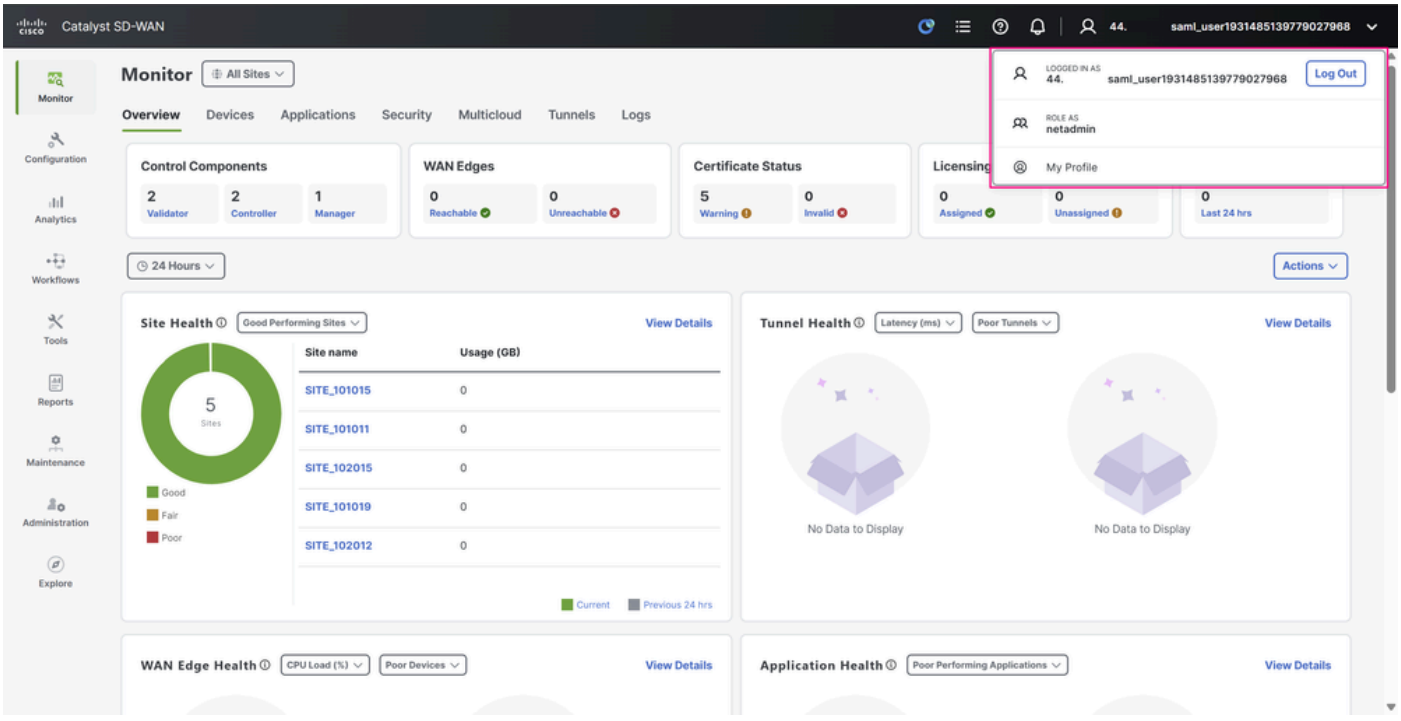
Microsoft登入螢幕

- 由於這是SSO使用者首次登入，因此提示會請求更改密碼。



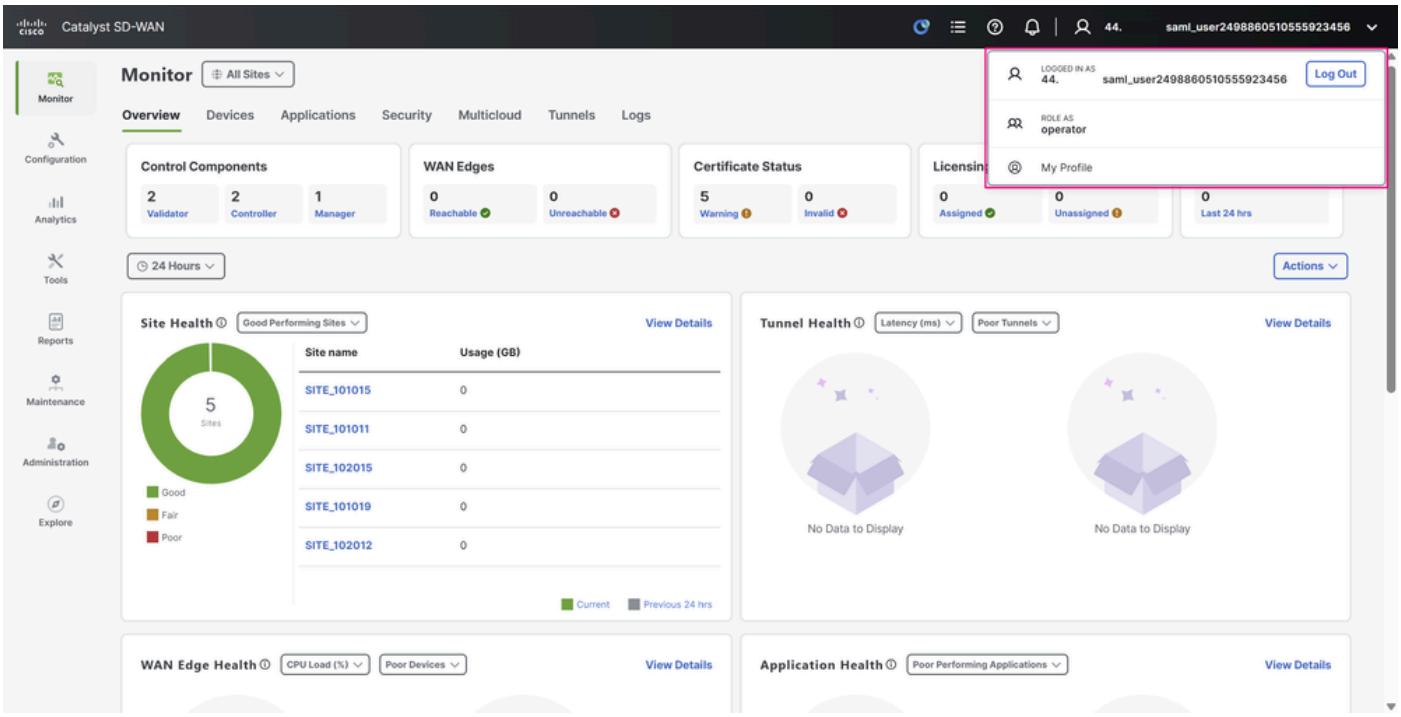
Microsoft登入螢幕

- 成功登入後，在儀表板右上角再次展開您的配置檔案的詳細信息，您可以確認檢測到使用者具有netadmin角色，完全如Microsoft Entra ID中配置的。



Cisco SD-WAN管理員UI

- 最後，與其他使用者執行相同的登入測試。您會看到相同的行為 — 現在使用者已標識為operator角色。



Cisco SD-WAN管理員UI

相關資訊

- [在Cisco IOS XE Catalyst SD-WAN上配置單點登入]

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）。