為CRES配置Microsoft Entra ID SSO外部身份驗證

目錄

簡介

本文檔介紹如何配置Microsoft Entra ID單一登入以驗證思科安全郵件加密服務的身份。

必要條件

需求

思科建議您瞭解以下主題：

- 安全電子郵件加密服務（註冊信封）
- Microsoft Entra ID
- 自簽名或CA簽名（可選）PEM格式的X.509 SSL證書

採用元件

- 安全電子郵件加密服務（註冊信封）管理員訪問許可權
- Microsoft Entra ID管理中心管理員訪問許可權

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。

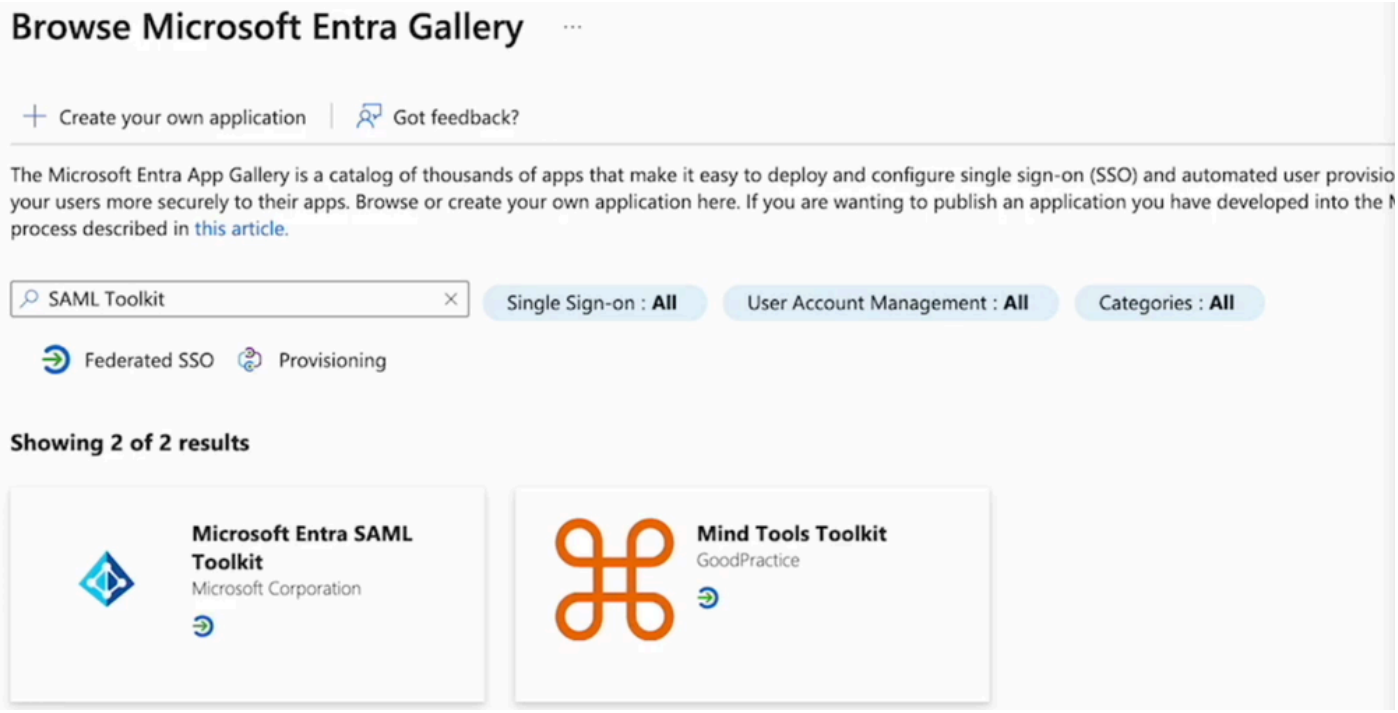
背景資訊

- 註冊信封為使用SAML的終端使用者啟用SSO登入。
- Microsoft Entra SSO允許和控制通過單點登入從任何位置訪問軟體即服務(SaaS)應用、雲應用或本地應用。
- 註冊信封可以設定為通過身份驗證方法連線到Microsoft Entra的託管身份應用程式，這些身份驗證方法包括多重身份驗證，因為純密碼身份驗證不安全，也不建議使用。
- SAML是基於XML的開放式標準資料格式，使管理員能夠在登入到其中某個應用程式後無縫訪問一組已定義的應用程式。
- 要瞭解有關SAML的詳細資訊，請參閱：什麼是SAML?

設定

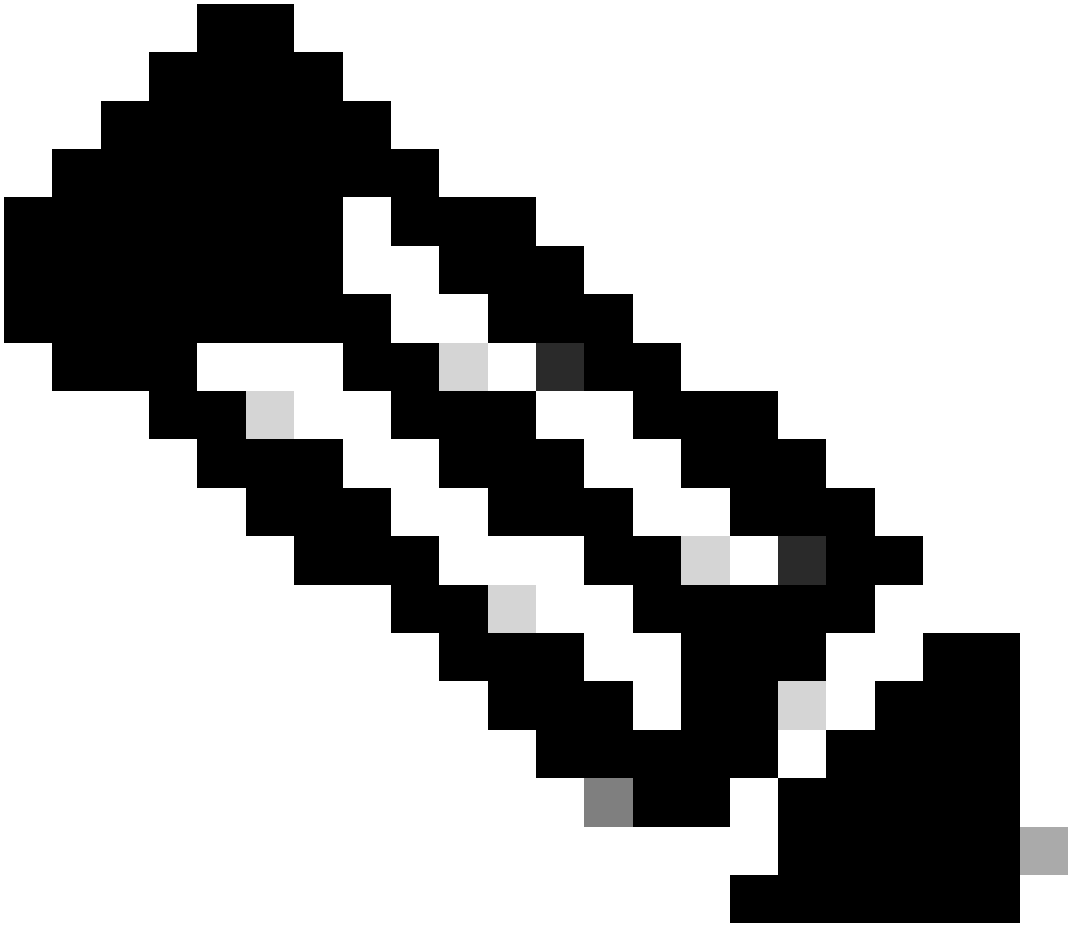
Microsoft Entra ID

1.導航到Microsoft Entra ID管理中心，然後點選Add按鈕。選擇「Enterprise Application」，然後搜尋「Microsoft Entra SAML Toolkit」，如下圖所示：



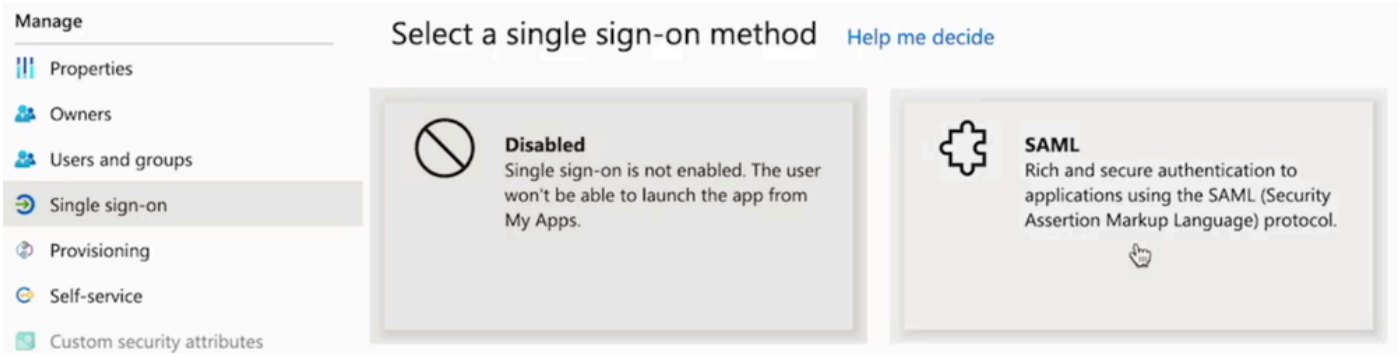
瀏覽Microsoft Entra Gallery

2.使用有意義的值命名它，然後按一下建立。例如，CRES Single Sign On。



附註：要允許所有使用者登入到CRES門戶，您需要在CRES Sign On(SAML toolkit)屬性下手動禁用Required Assignment，對於Assignment Required，請選擇No。

3.導航到左側面板，在Manage部分下按一下Single sign-on，然後選擇SAML。



4.在「基本SAML配置」面板中，按一下編輯，然後按如下方式填寫屬性：

- 識別符號（實體ID）：https://res.cisco.com/

- 回覆URL（斷言使用者服務URL）：https://res.cisco.com/websafe/ssourl
- 登入URL:https://res.cisco.com/websafe/ssourl
- 按一下「Save」。

5.在「屬性和宣告」面板中，按一下編輯。

在Required下，按一下Unique User Identifier(Name ID)宣告以對其進行編輯。

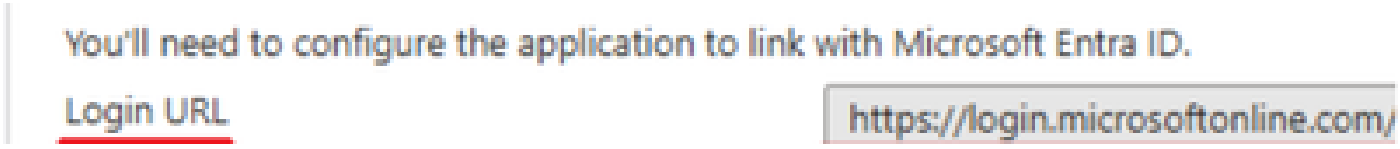
- 將Source attribute欄位設定為user.userprincipalname。這假設user.userprincipalname的值表示有效的電子郵件地址。如果不是，請將Source設定為user.primaryauthoritiveemail。
- 在Additional Claims面板下，按一下Edit，建立Microsoft Entra ID使用者屬性和SAML屬性之間的對映。

名稱	名稱空間	源屬性
電郵地址	無值	user.userprincipalname
名字	無值	user.givenname
姓氏	無值	user.surname

請務必清除每個宣告的Namespace欄位，如下所示：

6.一旦填寫了「屬性和索賠」部分，就會填寫最後一部分SAML簽名證書。在CRES門戶中根據需要儲存下一個值:

- 儲存登入URL。



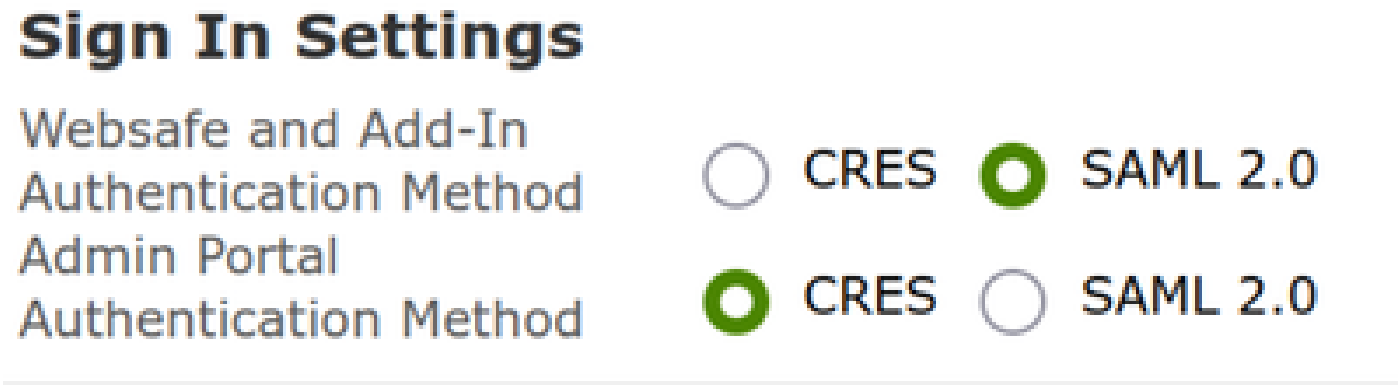
- 選擇Certificate(Base64)Download連結。

思科電子郵件加密服務

1.以管理員身份登入到您的安全郵件加密服務組織門戶。

2.在Accounts頁籤上，選擇Manage Accounts頁籤，然後按一下您的Account Number。

3.在Details頁籤中，滾動到Authentication Method，然後選擇SAML 2.0。



4. — 按如下方式填寫屬性：

- SSO備用EmailAttribute名稱：電郵地址
- SSO服務提供商實體ID*:https://res.cisco.com/
- SSO客戶服務URL*:此連結由Entra ID提供，位於
- SSO註銷URL:留空

5. — 按一下啟用SAML。

驗證

出現一個新視窗，確認登入成功後已啟用SAML身份驗證。按一下下一步。它會將您重定向到身份提供程式的登入頁。使用您的SSO憑據登入。成功登入後，可以關閉視窗。按一下「Save」。

疑難排解

如果視窗沒有將您重定向到您的身份提供程式的登入頁，則會返回跟蹤記錄，為您提供錯誤。請複查屬性和宣告，確保使用與「CRES驗證方法」部分相同的名稱配置它。SAML登入中使用的使用者電子郵件地址必須與CRES中的電子郵件地址匹配。請勿使用別名。

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）。