為DMP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域保護門戶的身份。

必要條件

需求

思科建議您瞭解以下主題：

- 思科網域保護
- 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

- 思科域保護管理員訪問許可權
- 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

- 思科域保護通過SAML 2.0協定為終端使用者啟用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。

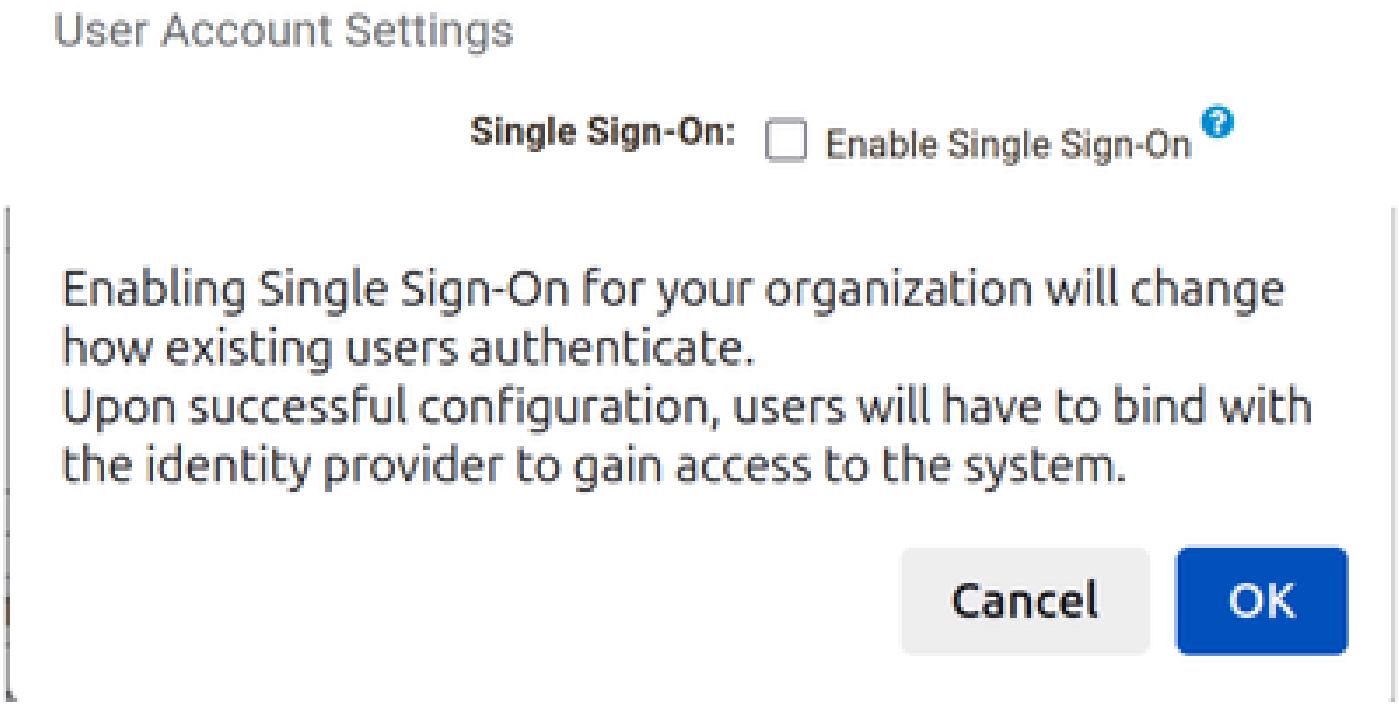
- 思科域保護可以設定為通過身份驗證方法連線到Microsoft Entra的託管身份應用，這些身份驗證方法包括多重身份驗證，因為僅密碼身份驗證不安全，也不建議使用。
- SAML是基於XML的開放式標準資料格式，使管理員能夠在登入到其中某個應用程式後無縫訪問一組已定義的應用程式。
- 要瞭解有關SAML的詳細資訊，請參閱：什麼是SAML?

設定

思科網域保護（第1部分）

1.登入到Cisco Domain Protection管理員門戶，然後導航到Admin > Organization。單擊Edit Organization Details按鈕，如下圖所示：

2.導航至使用者帳戶設定部分，然後按一下EnableSingle Sign-On覈取方塊。系統會顯示訊息，如下圖所示：

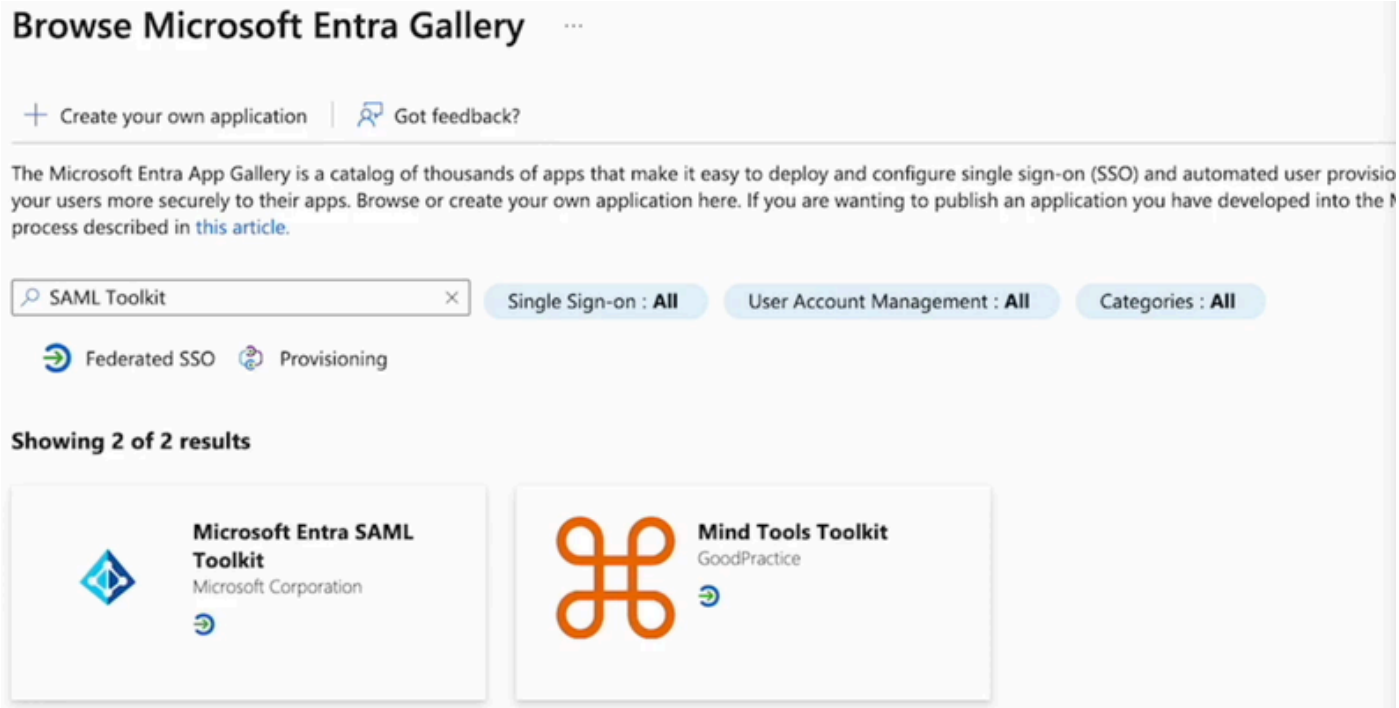


3.按一下OK按鈕，並複製實體ID和斷言使用者服務(ACS)URL引數。必須在Microsoft Entra ID基本SAML身份驗證中使用這些引數。稍後返回以設定名稱識別符號格式、SAML 2.0終端和公共證書引數。

- 實體ID:dmp.cisco.com
- 斷言使用者服務URL:https://<dmp_id>.dmp.cisco.com/auth/saml/callback

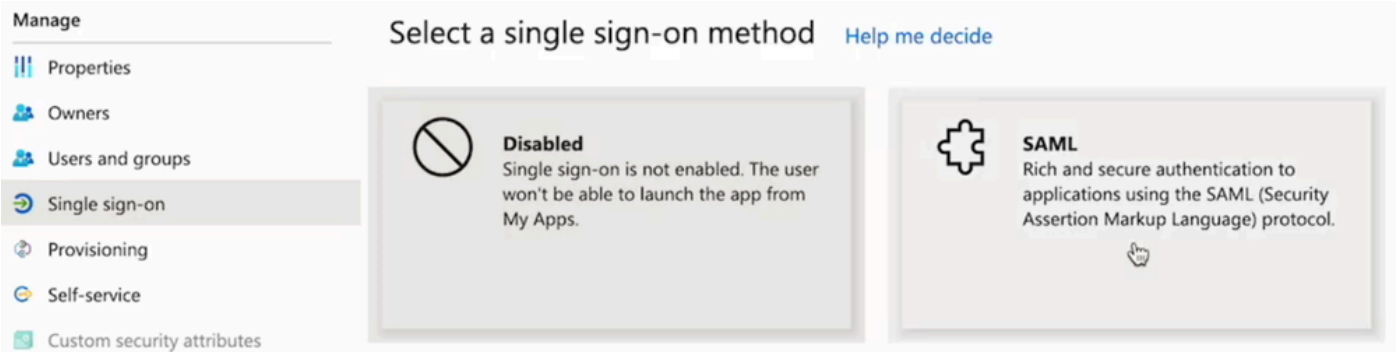
Microsoft Entra ID

1.導航到Microsoft Entra ID管理中心，然後按一下Add按鈕。選擇Enterprise Application，然後搜尋Microsoft Entra SAML Toolkit，如下圖所示：



2.使用有意義的值命名它，然後按一下建立。例如，域保護登入。

3.導航至管理部分下的左側面板。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，然後填寫引數：

- 識別符號（實體ID）：dmp.cisco.com
- 回覆URL（斷言使用者服務URL）：https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- 登入URL:https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- 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。

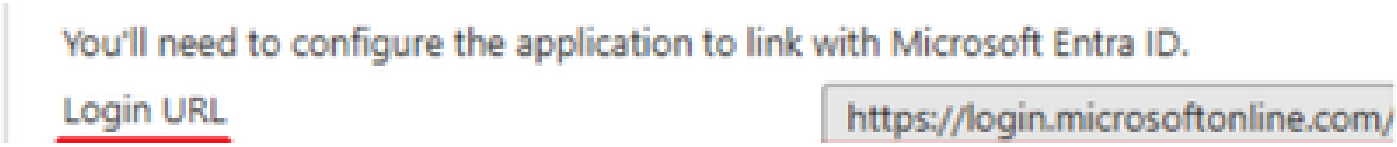
- 將Source attribute欄位設定為user.userprincipalname。這假設user.userprincipalname的值表示有效的電子郵件地址。如果不是，請將Source設定為user.primaryauthoritiveemail。
- 在Additional Claims面板下，按一下Edit，建立Microsoft Entra ID使用者屬性和SAML屬性之間的對映。

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。

- 儲存登入URL。

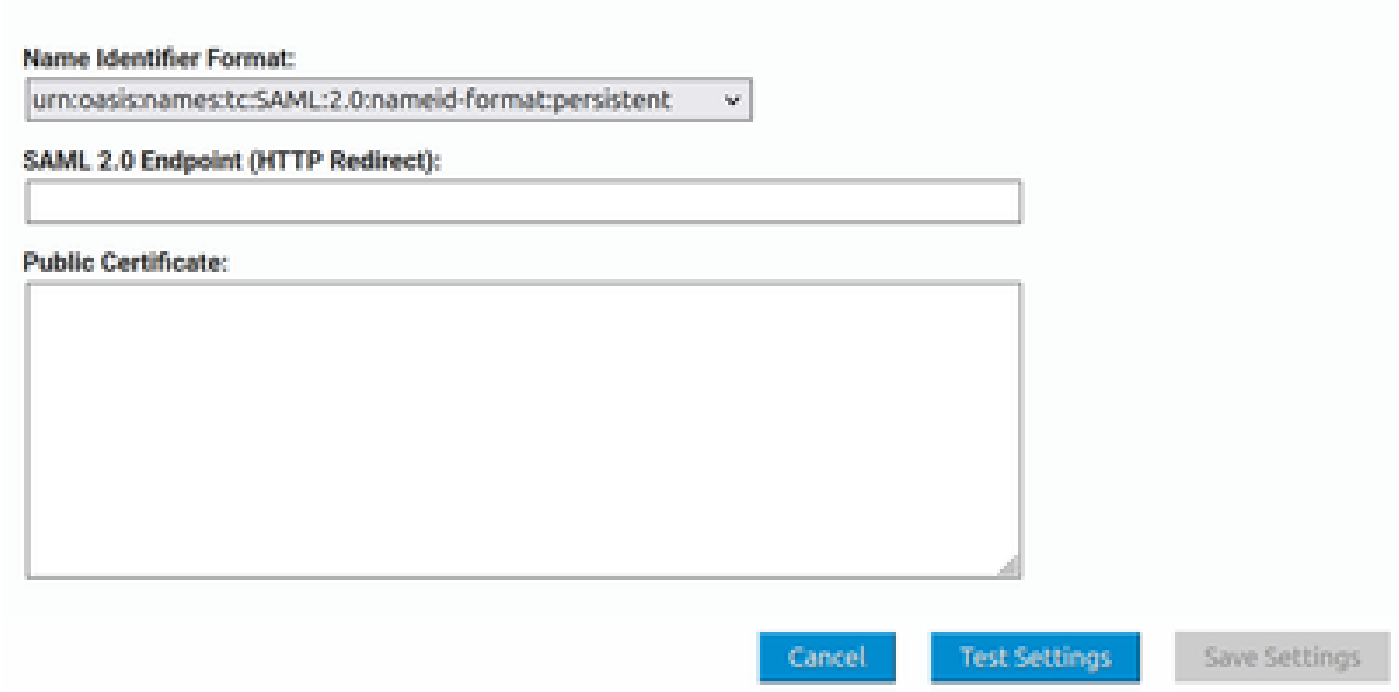


- 儲存證書(Base64)。

思科網域保護（第2部分）

返回Cisco Domain Protection > Enable Single Sign-On 部分。

- 名稱識別符號格式: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- SAML 2.0終結點（HTTP重定向）：Microsoft Entra ID提供的登入URL
- 公共證書:Microsoft Entra ID提供的證書(Base64)



驗證

按一下測試設定。它將您重定向到您的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 Settings」。

疑難排解

```
Error - Error parsing X509 certificate
```

- 確保證書位於Base64中。

```
Error - Please enter a valid URL
```

- 確保Microsoft Entra ID提供的登入URL正確。

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）。