為ESA和SMA配置Duo IdP SAML SSO

目錄

簡介

本文檔介紹如何為Cisco ESA和SMA的SAML SSO配置Duo Access Gateway。

環境

- Cisco ESA/SMA:AsyncOS最新版本
- Duo Access Gateway:從ESA/SMA管理介面部署和訪問
- 身份驗證源：Active Directory、OpenLDAP、Azure AD或其他SAML標識提供程式（用於屬性對映）

問題

本文檔僅介紹雙端配置。它不包括Cisco ESA/SMA服務提供商(SP)配置。

必要條件

技術

- 身份提供程式(IdP)
- 單一登入(SSO)
- 電子郵件安全裝置(ESA)
- 安全管理裝置(SMA)
- 斷言使用者服務(ACS)
- 服務提供商(SP)

需求

開始之前：

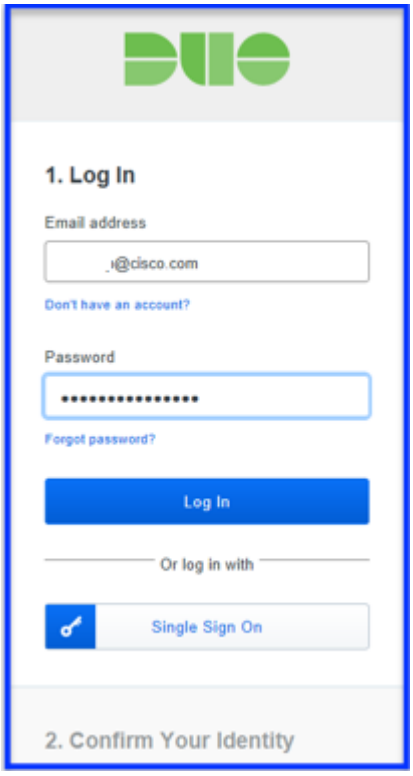
- 確保部署了Duo Access Gateway並具有已配置的身份驗證源。
- 使用已配置的身份驗證源部署Duo Access Gateway。
- 如果不支援多個Assertion Consumer Service(ACS)URL，Duo可能需要為每個ESA提供單獨的應用程式。

該配置包括兩個階段：

1. 配置Duo雲應用。
2. 將新的雲應用程式新增到Duo Access Gateway。

建立雲應用

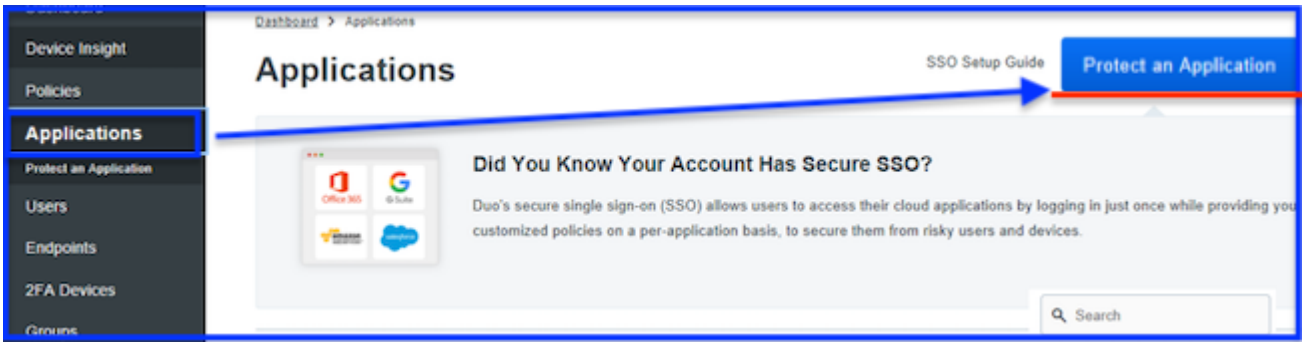
1.登入https://admin.duosecurity.com/。



duo.com

duo.com

2.定位至「應用程式」>「保護應用程式」。

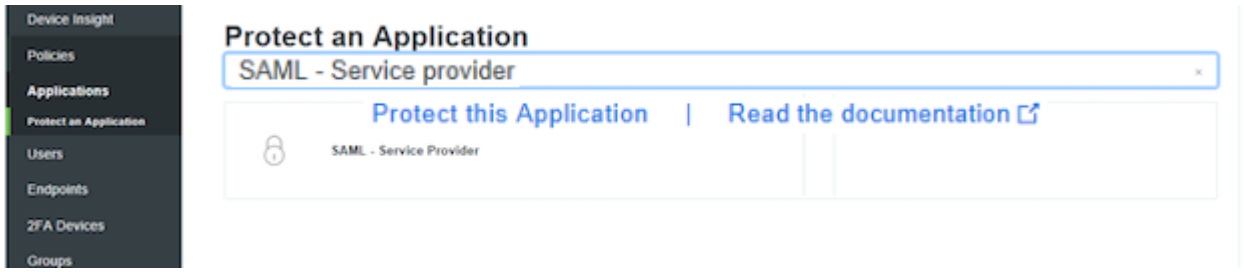


保護應用程式

保護應用程式

3.搜尋SAML -服務提供商。

4.出現SAML圖示時，選擇保護此應用程式。



保護此應用程式

保護此應用程式

5.完成服務提供商配置檔案：

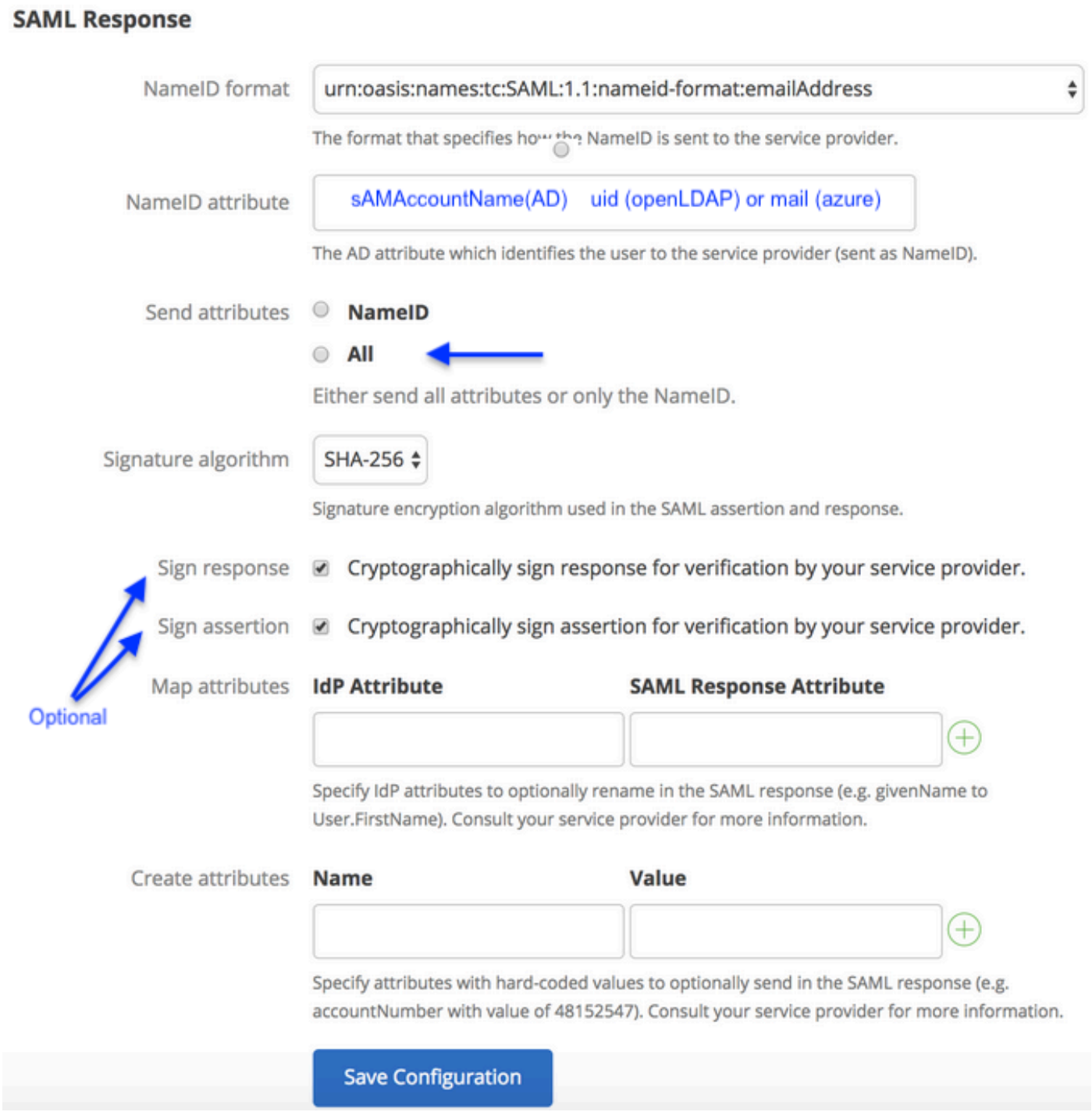
- 服務提供商名稱：輸入您選擇的名稱。
- 實體ID:輸入用於標識ESA/SMA的公用名稱。
- 斷言使用者服務：輸入可訪問的ESA/SMA URL。

6.根據驗證源使用以下NameID屬性值：

屬性	Active Directory	OpenLDAP	SAML身份提供程式(IdP)	Azure AD
郵件屬性	mail	mail	mail	mail
使用者名稱屬性	sAMAccountName	uid	mail	mail
名字屬性	給定名稱	gn	給定名稱	給定名稱
姓氏屬性	sn	sn	sn	姓氏

- 傳送屬性是可選的。選擇NameID或ALL。
- 簽名響應和簽名斷言是可選的。IdP和SP上的這些設定必須匹配。

7.選擇儲存配置。



SAML響應

SAML響應

8.最後，下載配置檔案。

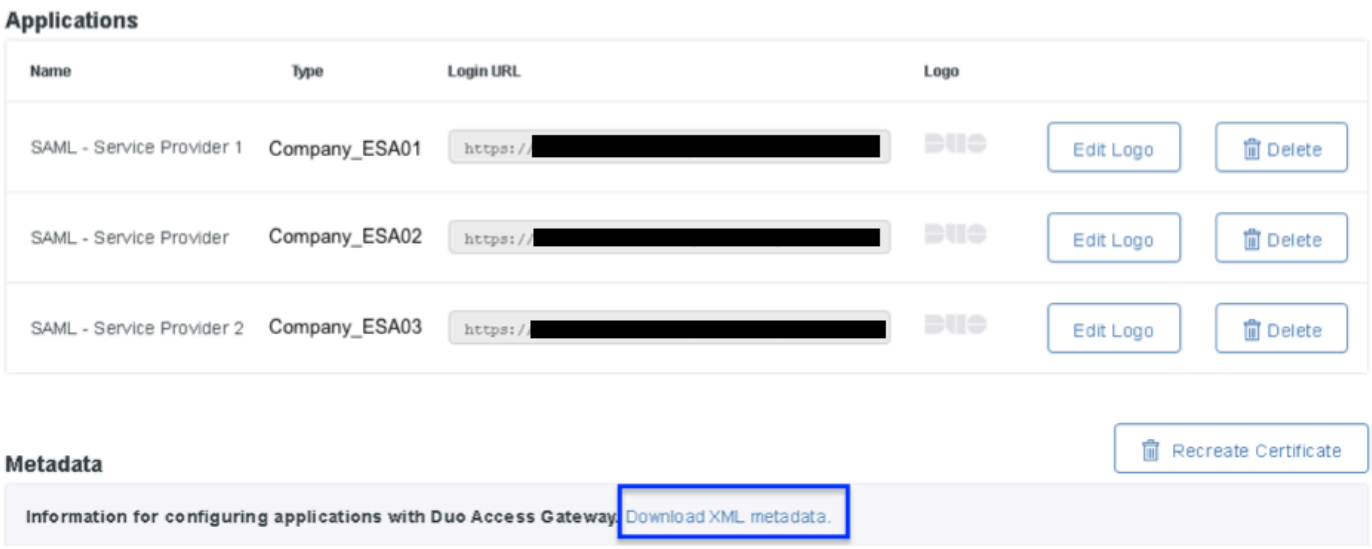
向Duo Access Gateway新增新的雲應用程式

1.登入Duo Access Gateway。

2.定位至「應用程式」>「新增應用」>「配置檔案」>「選擇檔案」。

3.選擇在步驟1中建立的應用程式配置，然後選擇UPLOAD。

4.下載用於SP主機上的XML後設資料作為IdP配置。



應用程式檢視和下載XML後設資料

應用程式檢視和下載XML後設資料

5.返回ESA/SMA以完成SAML SSO配置。

- 預期結果：建立了Duo Access Gateway應用程式，IdP XML後設資料已準備好匯入到ESA/SMA。

6.在後續的ESA/SMA流程中使用下載的後設資料。

後續步驟（ESA/SMA配置）

本文僅介紹Duo-side配置。要完成ESA/SMA上的設定，請按照說明操作。

驗證

- 確認應用程式顯示在Applications下的Duo Access Gateway中。
- 確認IdP XML後設資料已成功下載，並且已準備好在ESA/SMA上匯入。

相關資訊

- SAML SSO的Duo文檔

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）。