為ESA和SMA管理配置SAML SSO外部身份驗證

目錄

簡介

本文檔介紹如何為ESA和SMA系統管理配置SAML 2.0 SSO外部身份驗證。

環境

- 產品：電子郵件安全裝置(ESA)、安全管理裝置(SMA)
- 適用於：ESA和SMA系統管理
- 群集行為：在電腦級別配置服務提供商(SP)和IdP配置檔案；在群集級別配置外部身份驗證對映。

必要條件

- 對ESA/SMA Web介面的管理訪問
- X.509證書和私鑰以PKCS #12(PFX)或PEM格式（自簽名或CA簽名）提供
- 訪問第三方身份提供程式(IdP)應用程式及其SAML後設資料/SSO URL

預配置核對表

- 驗證管理員用於訪問裝置的管理介面主機名/FQDN;確認斷言使用者服務(ACS)URL與該主機名匹配。
- 如果裝置在群集中，請在啟用SAML外部身份驗證之前，計畫在計算機級別為每個成員配置SAML。
- 確定IdP是否要求每個裝置有一個單獨的應用程式或領域。
- 確認所需的證書和金鑰可用。
- 確認IdP傳送ESA/SMA角色對映所需的組或角色屬性。

注意：此文檔不適用於終端使用者隔離(EUQ)SAML SSO。

背景資訊

- Cisco TAC不為第三方IdP配置提供技術支援。為常見IdP提供了配置參考示例。

SSO SAML IdPs

- Duo Access Gateway(DAG)增加了二元身份驗證，使用SAML 2.0聯合完成常用雲服務。
- Active Directory聯合身份驗證服務(ADFS) — 使用ADFS 2、3、4、Azure Active Directory(Azure AD)、SecureAUTH和PingFederate進行測試
- 如果IdP在SAML 2.0單點登入框架中支援其他雙因素身份驗證，則可以使用其他雙因素身份驗證。
- Okta支援使用支援服務的IdP進行身份驗證。

將ESA/SMA配置為服務提供商

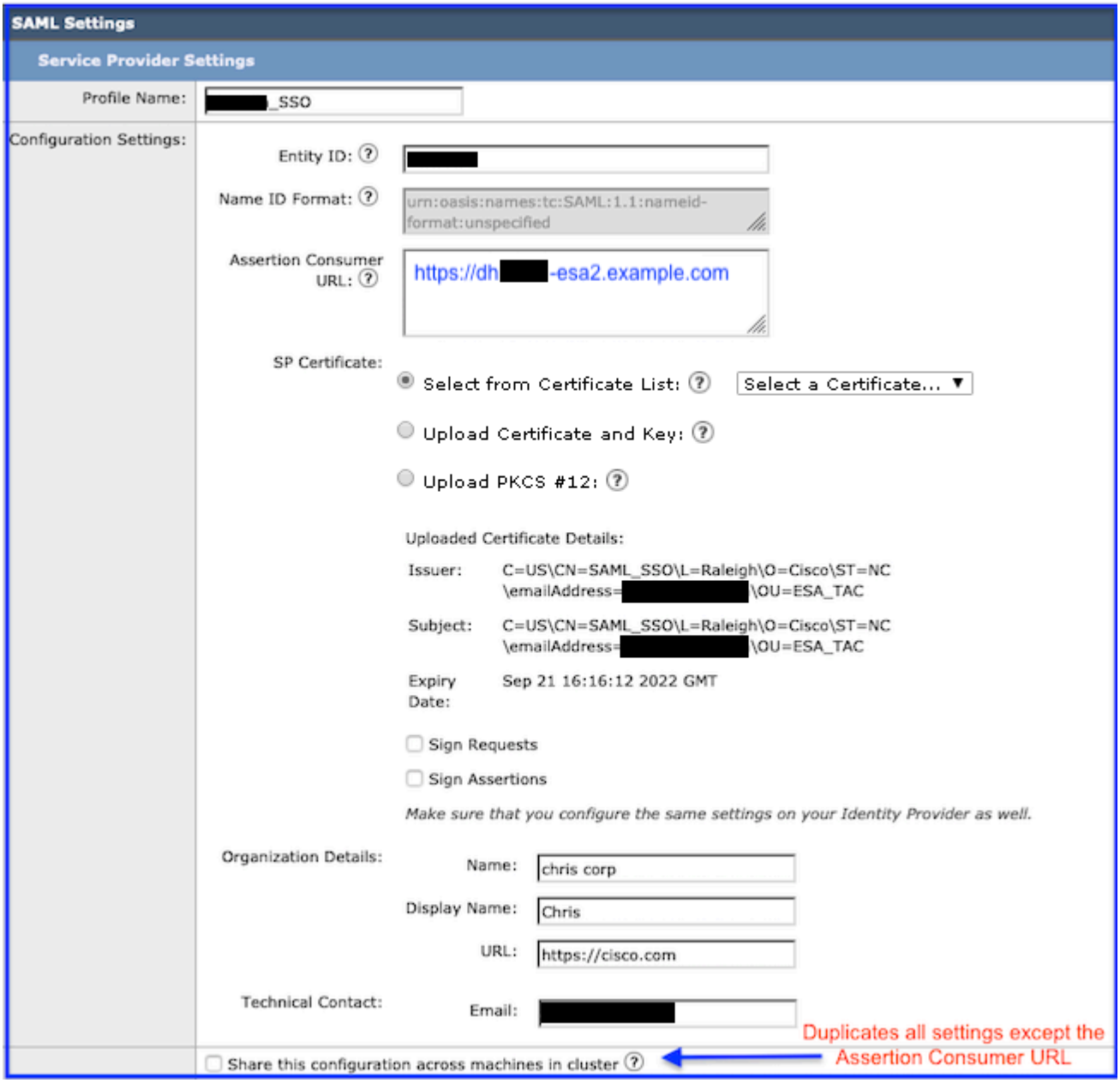
導航到系統管理> SAML >（電腦級別）>新增服務提供商。

附註：在啟用SAML之前，群集中的ESA需要針對群集的所有成員進行電腦級配置。

- 如果選擇了頁面底部的在群集中的電腦間共用此配置選項，則以下條件適用：
  - 除了斷言使用者URL之外，所有欄位都會複製到集群成員。
  - 斷言使用者URL會自動將管理介面的主機名填充為ACS。

- 使用備用主機名訪問主機的環境需要手動配置每台主機，例如CES託管的裝置。
- 配置檔名稱：用於在ESA或SMA介面中標籤SP例項的名稱。
- 實體ID:IdP看到的用於SP例項的名稱。此名稱是IdP用於表示SP的標籤。可以是任意名稱，例如ESA_SP或ESA_SSO。
- 名稱ID格式:不可配置的欄位。
- 斷言使用者URL或斷言使用者服務(ACS):IdP用於與此ESA/SMA主機通訊的URL。
- SP證書:
    - Format:PFX/PKCS12或PEM格式的X.509公共/專用證書。
    - 選項 1:從證書清單中選擇:在Network > Certificates中，從ESA上已建立的證書中進行選擇。
    - 選項 2:上傳憑證和金鑰:上傳PEM格式的證書和金鑰。
    - 選項 3:上傳PKCS #12:上傳PKCS #12檔案。
    - 可選：在ESA/SMA上為SAML單一登入建立自簽名證書。
    - 如果需要，可對私鑰進行密碼保護。

 附註：如果使用PEM格式的證書，請將每個證書和私鑰儲存在不同的檔案中。



「服務提供者設定」頁

「服務提供者設定」頁

- 簽名請求:用於簽署傳送到IdP的ESA/SMA SAML通訊的選項。
- 簽名斷言:選項要求IdP對傳送到ESA/SMA的宣告進行簽名。
- 組織詳細資訊:可以使用相應的公司資料填充。
- 提交和提交更改以保留設定。
- 從「SAML配置」頁下載SP後設資料。

配置身份提供程式(IdP)以與ESA/SMA裝置配合使用

附註：某些IdP要求每個ESA有單獨的應用程式或領域。(例如：DUO)

這些連結在發佈時提供了多個IdP的配置示例。
Cisco TAC不為第三方產品提供技術支援。這些示例作為參考提供。

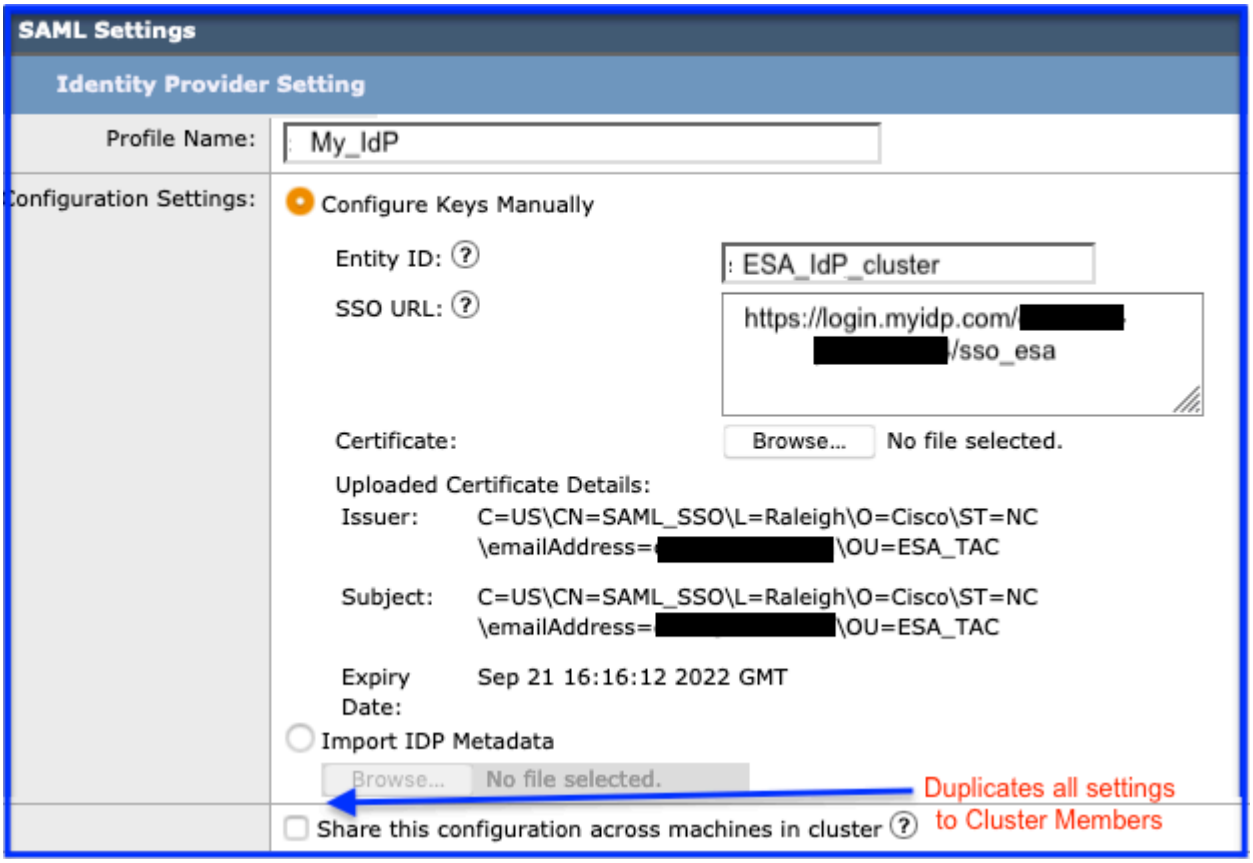
在ESA/SMA上配置IDP設定

1.定位至系統管理> SAML。

2.選擇Add Identity Provider。

- 有兩種可用選項：
- 匯入IdP後設資料
- 手動配置金鑰:
  - 實體ID:可以是用於標識IdP的任何值
  - SSO URL:SP向其傳送SAML身份驗證請求的URL
  - 將私鑰和公共證書上傳到不同的檔案中

3.在群集中的電腦之間共用此配置，以便在群集中的所有ESA之間複製配置：

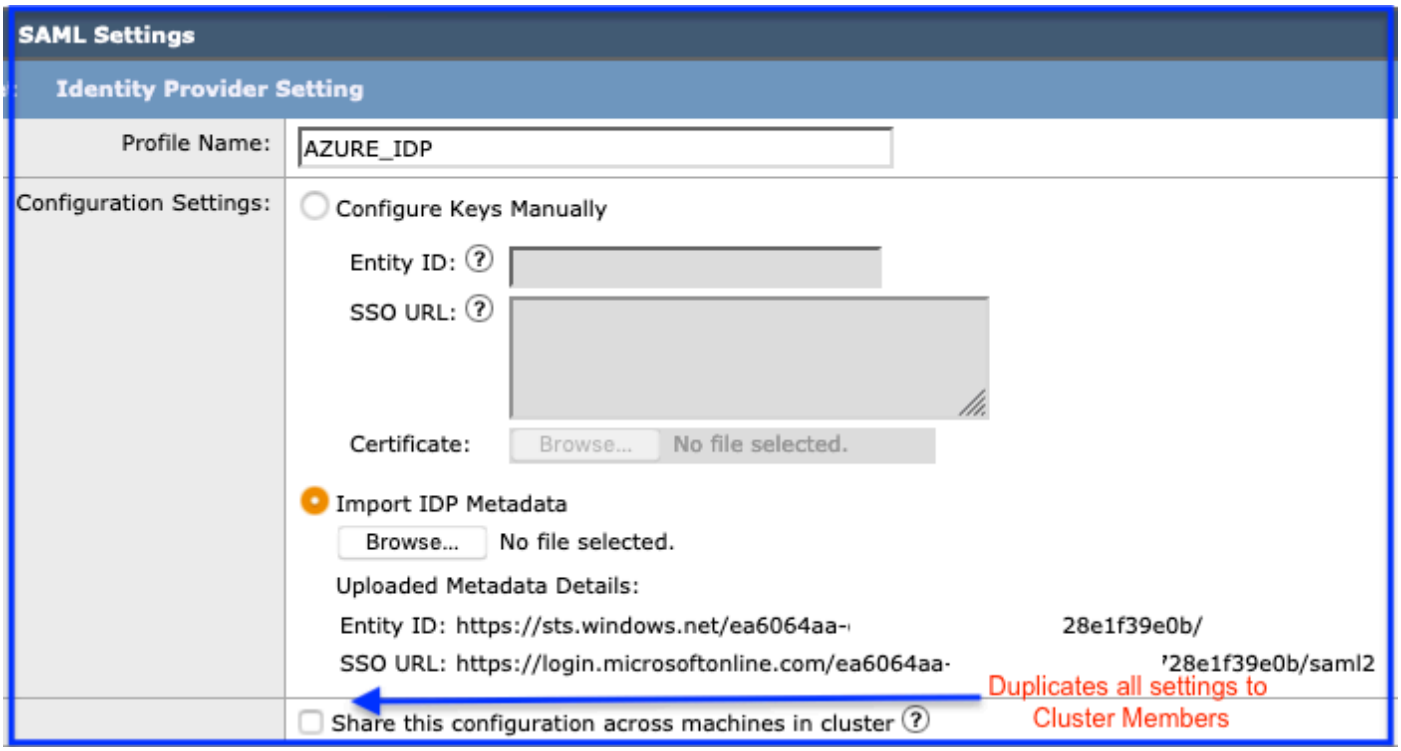


手動輸入IdP內容

手動輸入IdP內容

4.從IdP上載後設資料

- 選擇匯入IdP後設資料。
- 瀏覽到從IdP儲存的後設資料檔案並儲存配置。
- 如果適用於部署，則可以使用在群集中的計算機之間共用此配置的選項。



從Idp上載後設資料

從Idp上載後設資料

在ESA/SMA上使用SAML啟用外部身份驗證

與LDAP外部身份驗證類似，SAML單一登入需要對映將組分配給管理角色。

1.導航到系統管理>使用者（集群級別）>外部身份驗證>啟用。

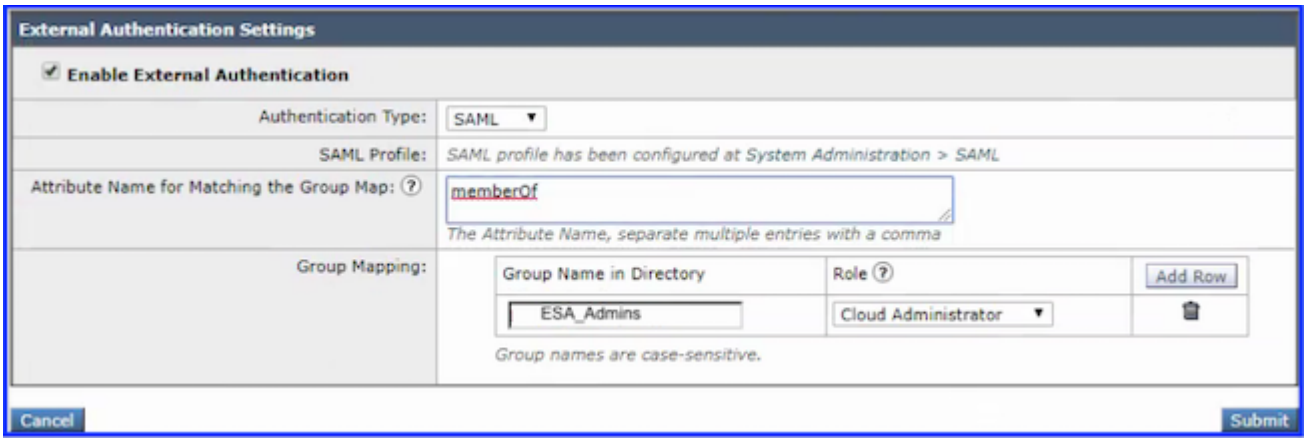
2.選擇Authentication Type:SAML。

3.用於匹配名稱對映的屬性名稱（可選）:輸入要從組對映中搜尋的屬性名稱。

附註：屬性名稱取決於為SAML響應中中繼的身份提供程式配置的屬性。裝置將根據「組對映」欄位中配置的屬性在SAML響應中搜尋指定屬性名稱的匹配條目。如果未配置此欄位，裝置會根據已配置的「組對映」欄位搜尋SAML響應中存在的所有屬性。

4.根據預定義或自定義使用者角色，輸入在SAML目錄中定義的組名屬性。

- Group Mapping欄位必須包含組屬性。可以新增Unspecified Groups屬性來驗證SAML斷言或響應。



外部身份驗證設定

外部身份驗證設定

5.提交和提交更改。

配置成功後，登入頁面底部將顯示一個新連結。ESA/SMA登入頁面顯示使用單一登入連結，該連結將管理員重定向到公司身份提供程式(IdP)。

選擇後，管理員將重定向到公司SAML登入頁面。

使用單一登入連結將重定向到SAML

使用單一登入連結重定向至SAML

疑難排解

使用這些指示符確定問題是與裝置配置還是IdP配置相關。

SSO重定向連結不會顯示在登入頁面上（「使用單一登入」）

確認已配置System Administration > Users > External Authentication > SAML。

重定向返回帶有「單點登入身份驗證失敗！」的ESA/SMA登入頁面請聯絡您的管理員。」

錯誤：「單一登入身份驗證失敗！請聯絡您的管理員。」

- 身份驗證在IdP失敗。
  - 這表示該配置工作到到達「一次登入身份驗證」頁面和提交憑據的點為止。
  - 此故障通常是由於IdP配置而引起的，並且需要對IdP設定進行其他驗證。

重定向返回帶有「授權失敗！」的ESA/SMA登入頁請聯絡您的管理員。」

錯誤：「授權失敗！請聯絡您的管理員。」

- 身份驗證通過，但在ESA/SMA上授權失敗。
  - 重點介紹Users > External Authentication > SAML中的設定。
    - 屬性名稱、組名稱和組對映。

相關資訊

- Cisco Email Security Appliance — 使用手冊
- Cisco Content Security Management Appliance — 使用手冊
- Cisco Web Security — 使用手冊

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）。