為SMA終端使用者隔離配置Okta SAML SSO

目錄

簡介

本文檔介紹如何將Okta配置為Cisco Secure Email SMA終端使用者隔離訪問的SAML 2.0身份提供程式。

必要條件

- 產品:思科安全電子郵件安全管理裝置(SMA)
- 功能:適用於終端使用者隔離區(EUQ)的SAML SSO
- 標識提供程式：Okta(SAML 2.0)
- 適用於：在虛擬或硬體平台上提供EUQ訪問的SMA部署。用環境中的值替換示例主機名和埠。
- 版本上下文：此過程適用於支援SAML for EUQ的SMA版本。驗證已安裝版本中的可用欄位和選單選項。

附註：本文檔重點介紹SMA EUQ SAML配置。僅當SMA無法生成自簽名證書時，才會引用ESA生成證書。

需求

開始之前，請確認您有：

- 對SMA Web介面的管理訪問。

- Okta中的管理許可權，用於建立SAML 2.0應用程式和分配使用者或組。
- SMA服務提供商配置的證書和私鑰。自簽名證書對於測試是可接受的。
- 終端使用者可以從瀏覽器訪問的可達SMA EUQ完全限定域名(FQDN)和埠。
- SMA SAML斷言URL和SP實體ID值(在建立SP條目後，從系統管理> SAML)。
- 分配給Okta應用程式的Okta中的使用者帳戶。
- 目錄同步使用者（如果部署使用目錄整合）。

附註：Okta是第三方身份提供程式。本檔案將提供範例組態以供客戶參考。

採用元件

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。

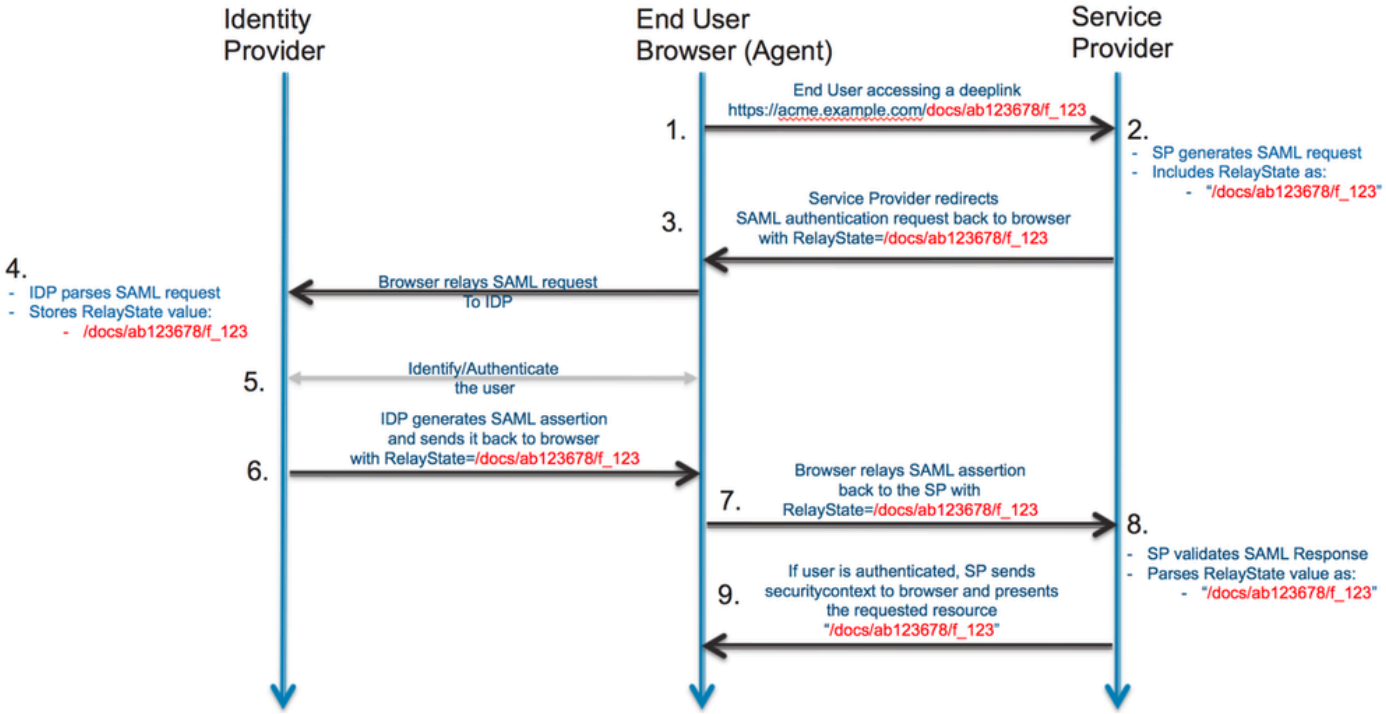
背景資訊

目標是為垃圾郵件隔離區門戶配置單點登入(SSO)，以便使用者重定向到Okta進行身份驗證，如果Okta中啟用了多重身份驗證(MFA)，則完成多重身份驗證(MFA)，然後返回到SMA EUQ門戶。本文檔僅適用於SMA。當SMA無法生成自簽名證書時，僅引用思科安全郵件網關(前身為郵件安全裝置(ESA))生成證書。

問題:使用者必須使用SAML SSO和可選MFA通過Okta向SMA垃圾郵件隔離門戶進行身份驗證。

解析度：將SMA配置為服務提供商，在Okta中配置SAML應用程式，將Okta IdP設定匯入SMA，在Okta中分配使用者，並驗證訪問許可權。

SAML流：



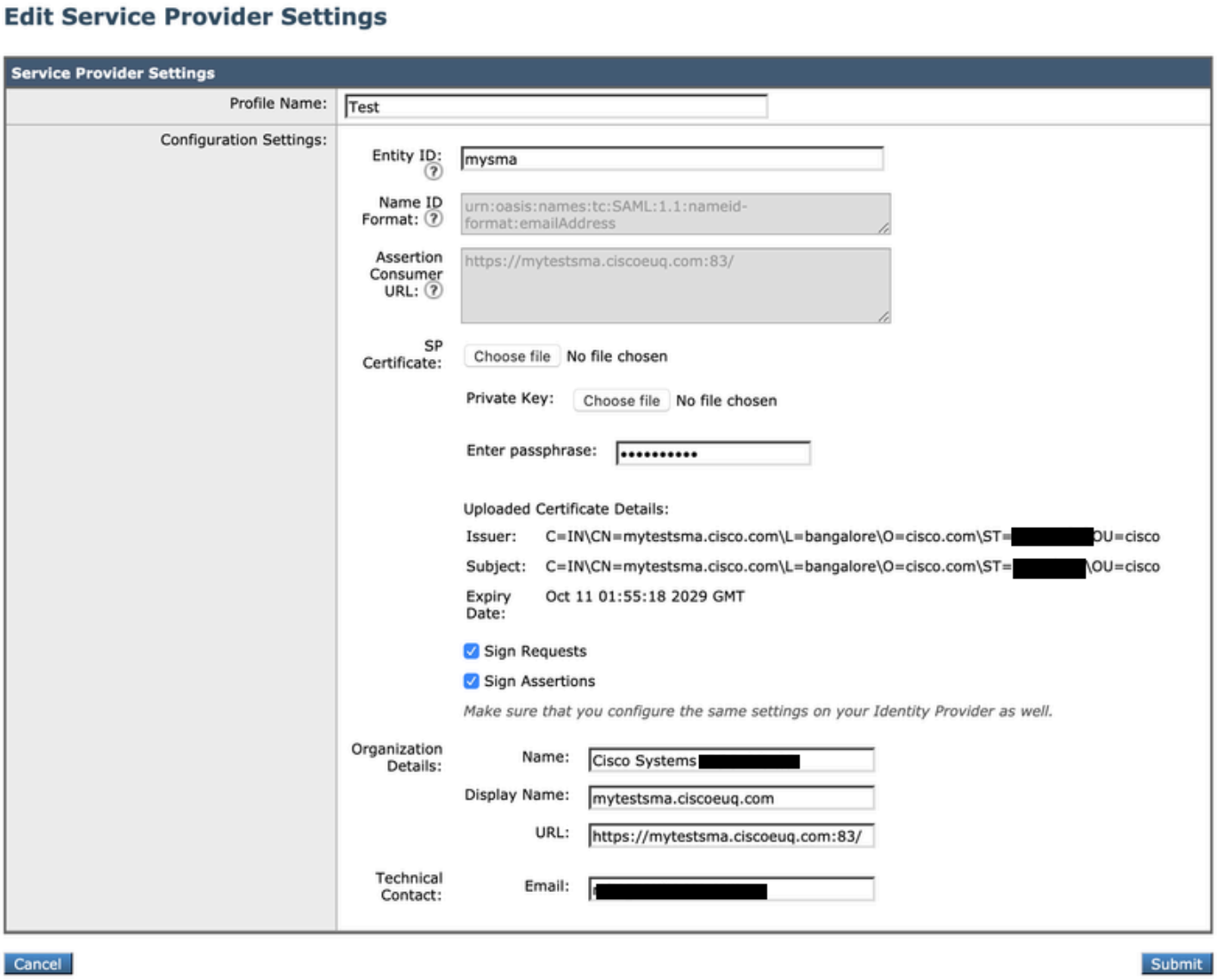
組態

在SMA裝置上配置服務提供商(SP)

要將SMA配置為EUQ訪問的SAML服務提供商，請完成以下步驟：

1. 登入SMA Web介面。
2. 導覽至System Administration > SAML。
3. 選擇Add Service Provider。
4. 在服務提供者實體ID中，輸入實體ID，您也可以在登錄檔中配置。
5. 驗證是否已為EUQ介面填充名稱ID格式和斷言使用者服務(ACS)URL。
6. 在SP證書中，上傳證書以對SAML請求進行簽名。

附註：SMA無法生成自簽名證書。您還可以在ESA上生成證書並匯出該證書以在SMA上使用。

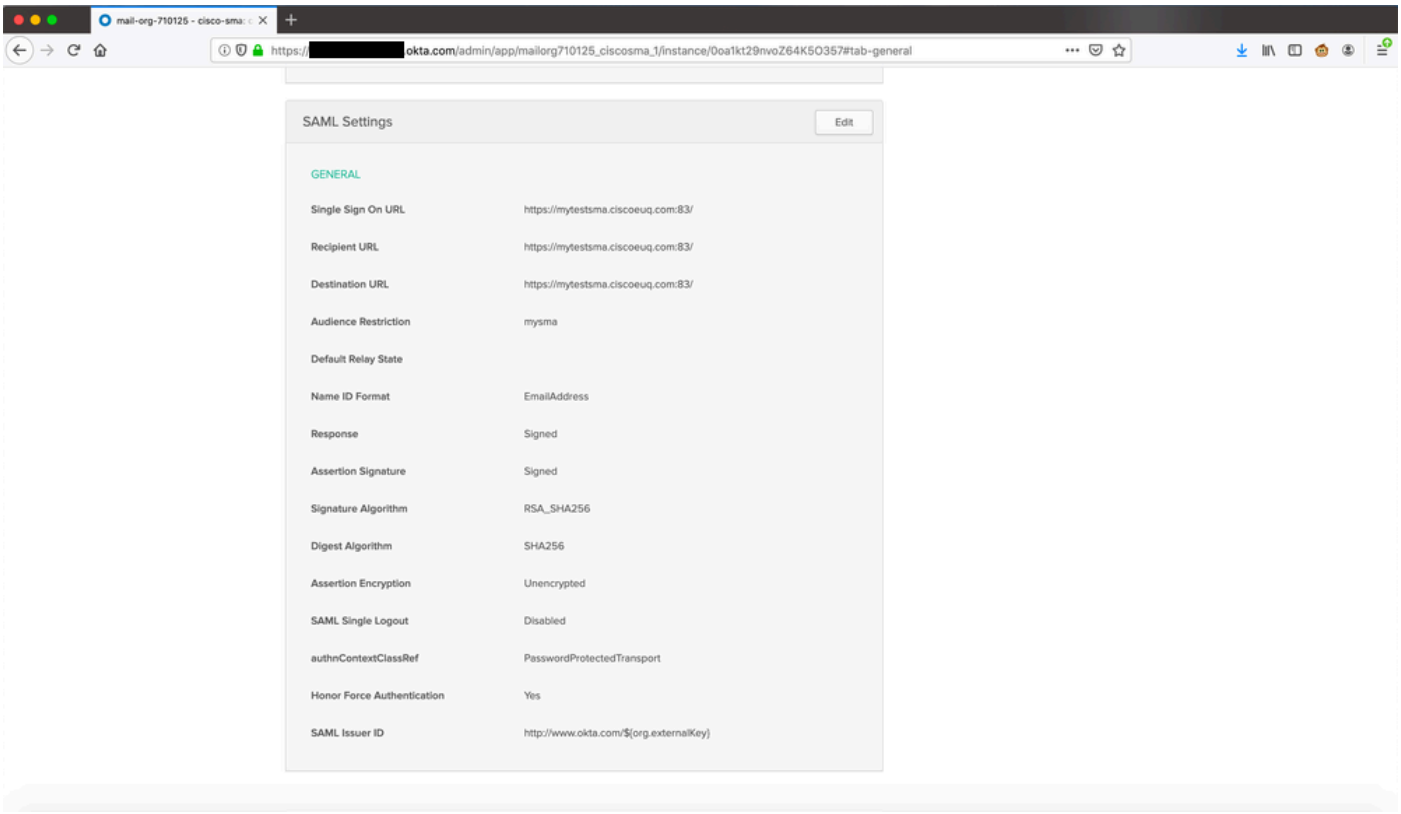


GUI中的服務提供商設定

在Okta中配置SAML應用程式

要在Okta中為SMA EUQ訪問建立SAML 2.0應用程式，請完成以下步驟：

1. 以管理員身份登入Okta。
2. 導航到應用程式>應用程式，然後選擇建立應用程式整合。
3. 選擇SAML 2.0，然後選擇下一步。
4. 輸入App name，例如SMA EUQ，然後選擇Next。
5. 在單點登入URL中，從SMA服務提供商設定輸入SMA ACS URL。
6. 在受眾URI（SP實體ID）中，輸入在SMA上配置的相同實體ID。
7. 對於名稱ID格式，請選擇EmailAddress。
8. 對於Application username，選擇適當的Okta username format以進行部署。
9. 完成嚮導，然後開啟新應用程式，並複製IdP metadata XML檔案或metadataURL。

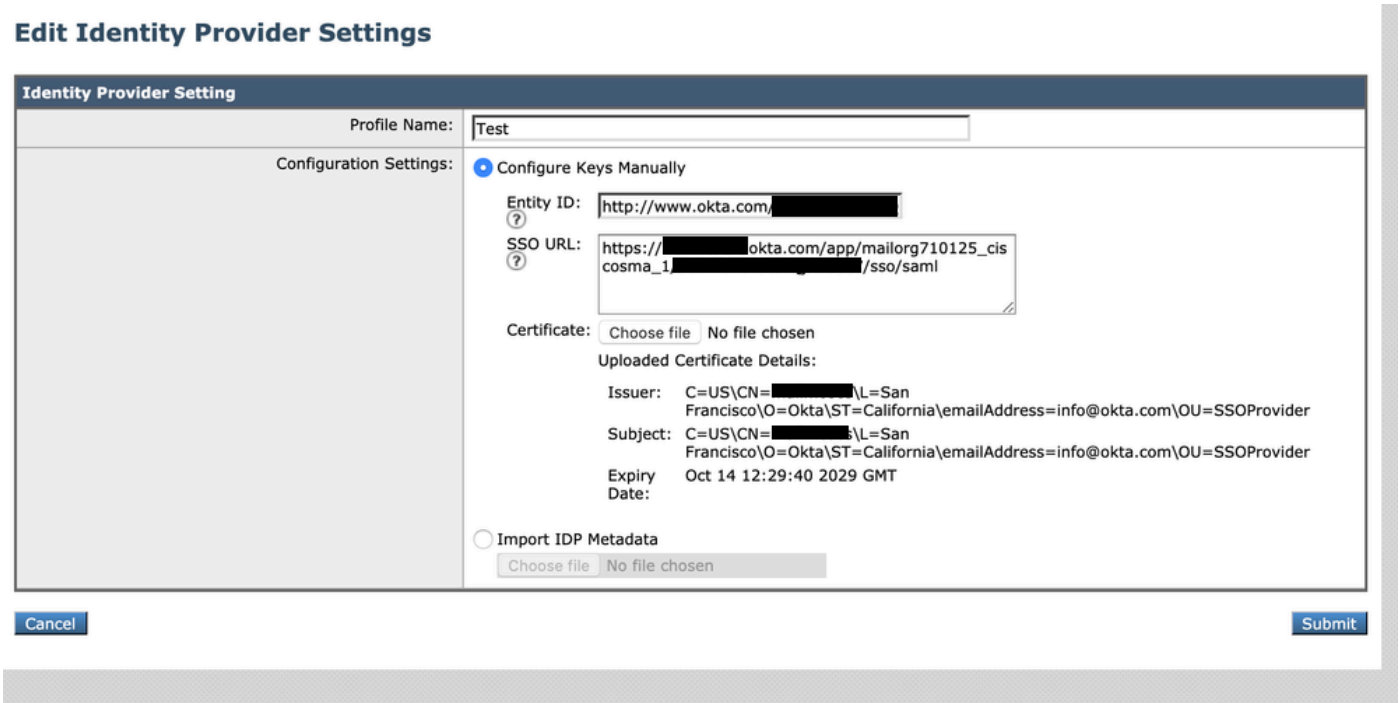


檢視Okta門戶

在SMA裝置上配置身份提供程式(IdP)

要將Okta配置為SMA上的身份提供程式(IdP)，請完成以下步驟：

1. 登入SMA Web介面。
2. 導覽至System Administration > SAML。
3. 在身份提供程式設定下，從上一節匯入Okta IdP後設資料，或手動輸入值。

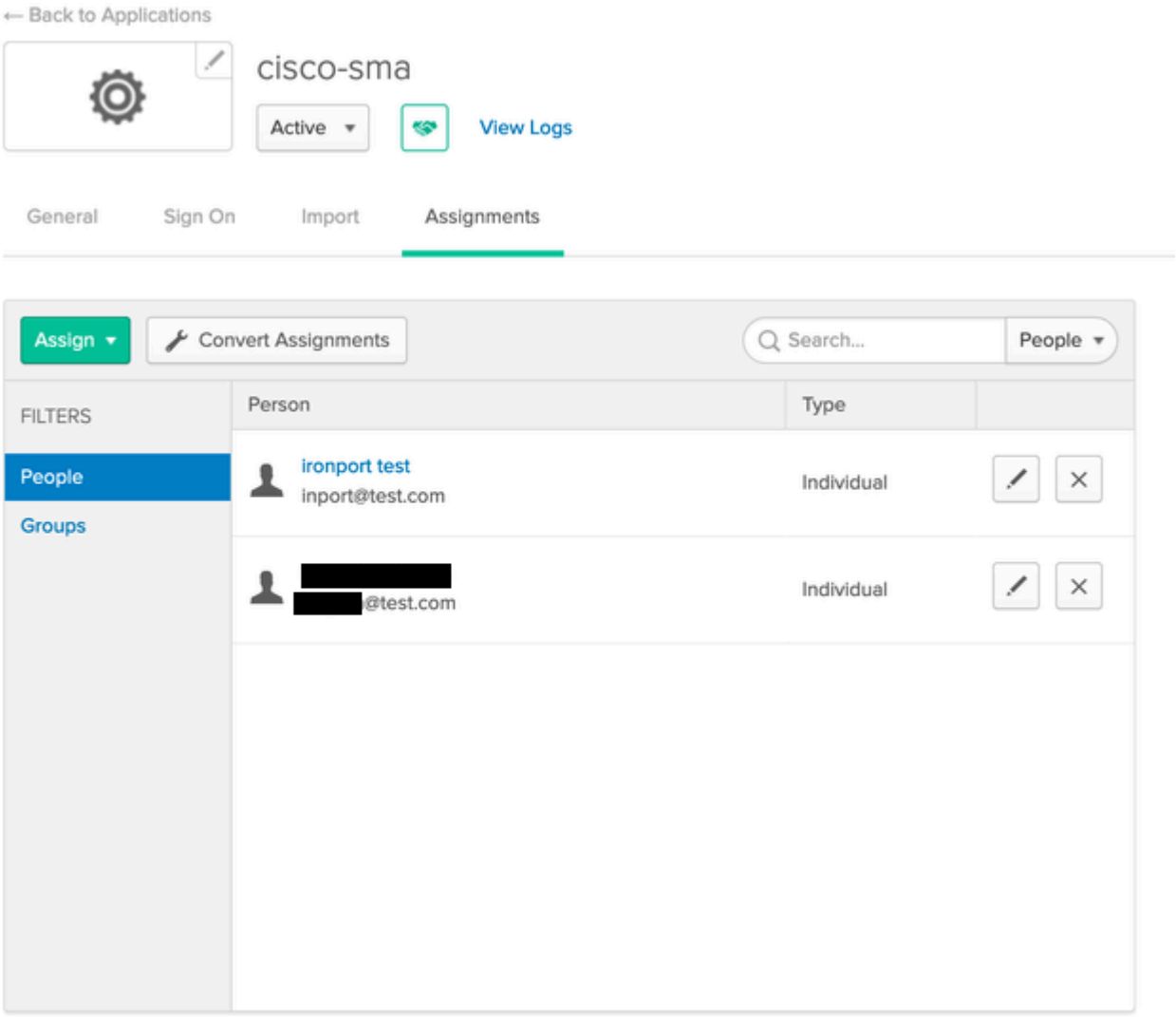


SMA GUI中的IdP配置檔案設定

將使用者分配到Okta應用程式

要允許使用者通過Okta向SMA EUQ進行身份驗證，請向Okta應用程式分配使用者或組：

1. 在Okta中，開啟您創建的應用程式。
2. 定位至分配>人員，然後選擇分配。
3. 選擇每個使用者旁邊的Assign，然後選擇Done。



在Okta門戶中分配使用者

附註：您可以手動分配使用者，從Active Directory同步使用者，或者使用Okta支援的另一個目錄整合。

在Okta中配置MFA（可選）

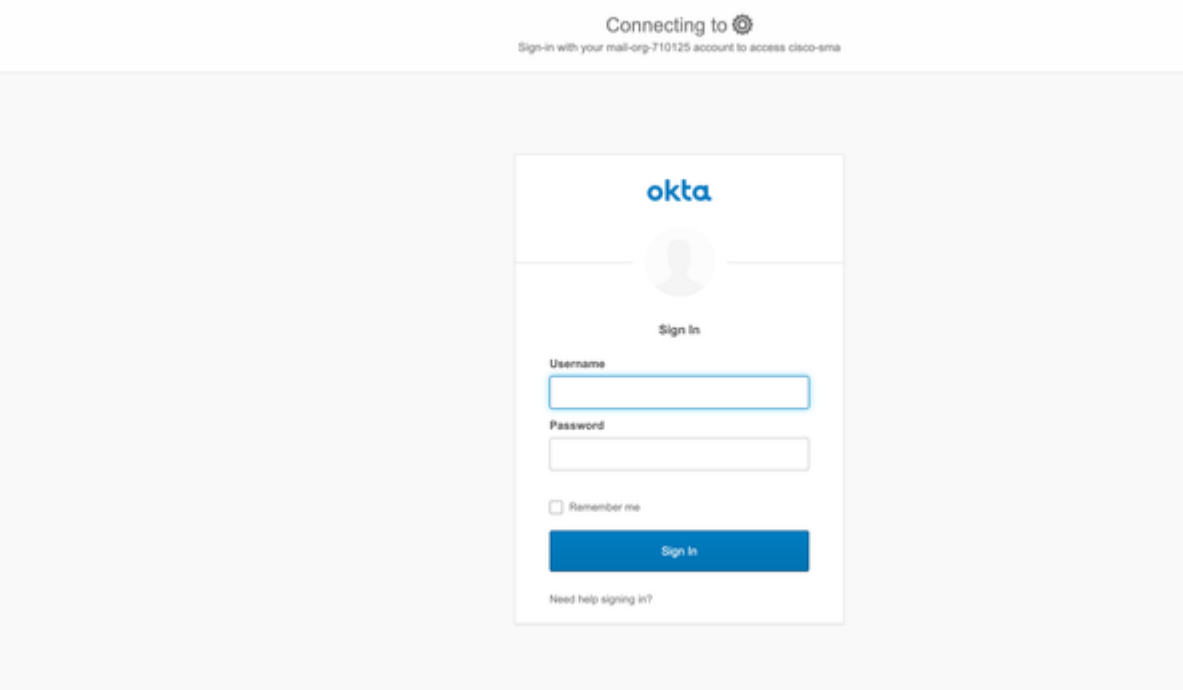
如果要對EUQ訪問進行多重身份驗證(MFA)，請在Okta中為應用程式配置MFA策略：

1. 在Okta Admin中，導航到Security > Authentication。
2. 配置必需的因素，例如Okta Verify、Google Authenticator或SMS，並將策略應用於SMA EUQ應用程式。

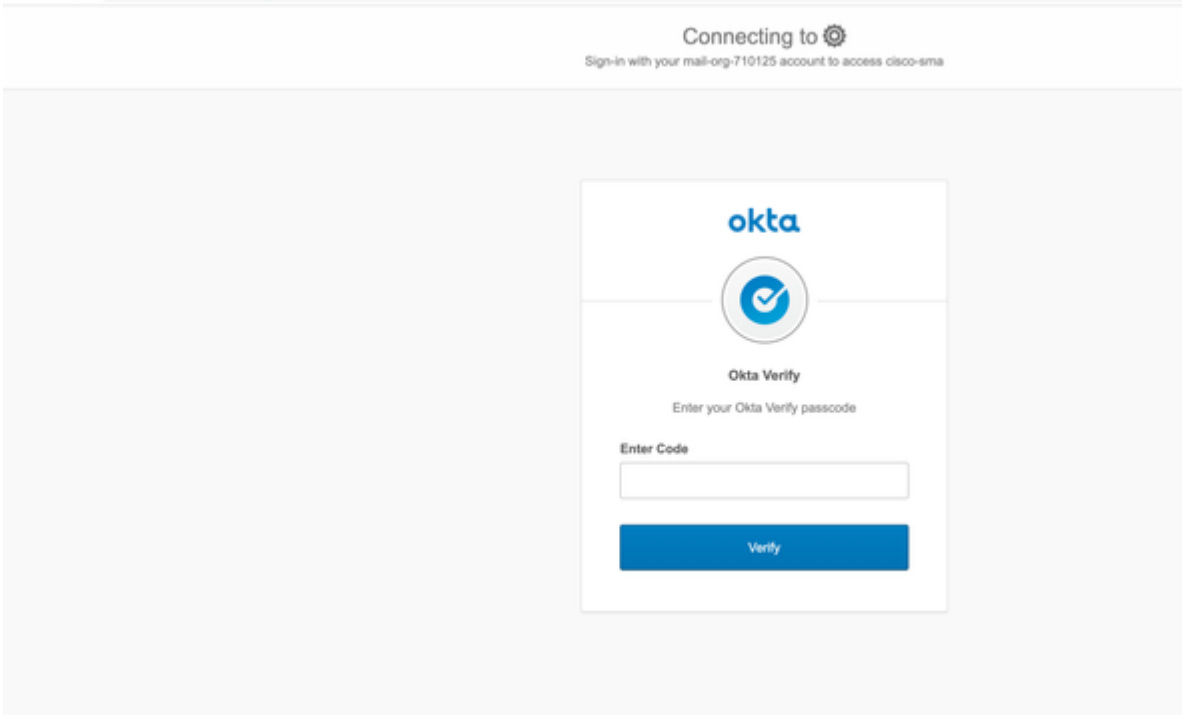
驗證SAML登入

預期結果：若要驗證設定，請完成以下步驟：

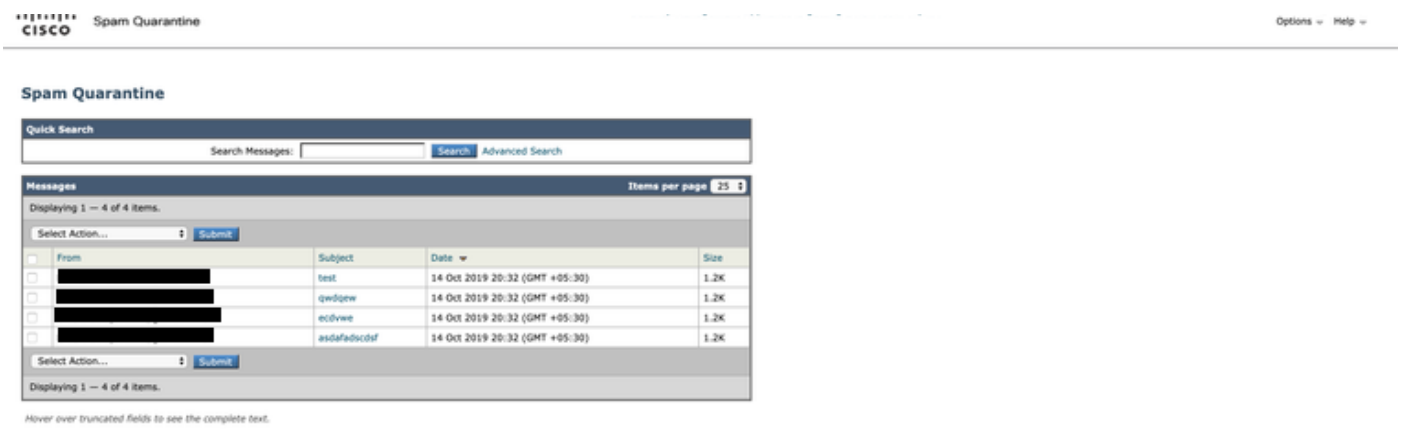
1. 瀏覽到SMA EUQ URL，例如https://<sma-fqdn>:<port>/。
2. 確認瀏覽器重定向至Okta進行身份驗證。
3. 如果已啟用MFA，請完成MFA 練習。
4. 確認已重新定向到SMA垃圾郵件隔離區門戶並有權訪問隔離功能。



使用Okta登入



輸入Okta Verify代碼



使用Okta登入後的垃圾郵件隔離區檢視

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）。