為終端使用者垃圾郵件隔離區配置OKTA SSO

目錄

簡介

本文檔介紹如何配置OKTA SSO以登入到安全管理裝置的終端使用者垃圾郵件隔離區。

必要條件

- 管理員對思科安全管理裝置的訪問許可權。
- OKTA的管理員訪問許可權。
- 自簽名或CA簽名（可選）PKCS #12或PEM格式（由OKTA提供）的X.509 SSL證書。

背景資訊

思科安全管理裝置為使用終端使用者垃圾郵件隔離區的終端使用者啟用SSO登入，並與OKTA整合，OKTA是一個為應用程式提供身份驗證和授權服務的身份管理器。思科終端使用者垃圾郵件隔離區可以設定為連線OKTA進行身份驗證和授權的應用程式，並使用SAML（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定義的應用程式。

要瞭解有關SAML的詳細資訊，請參閱:SAML一般資訊

元件

- 思科安全管理裝置雲管理員帳戶。
- OKTA管理員帳戶。

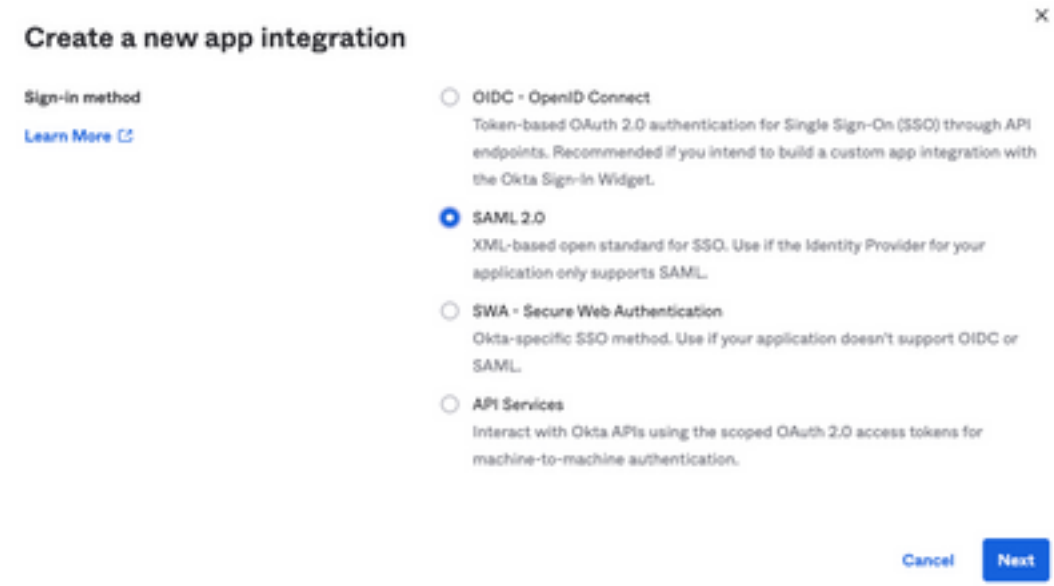
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果網路運作中，請確保您已瞭解任何指令可能造成的影響。

設定

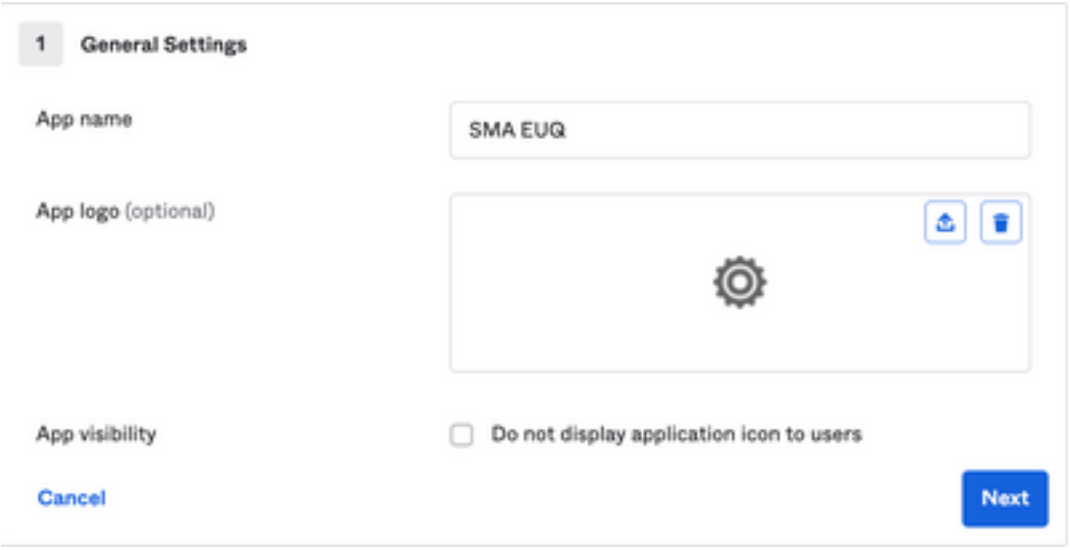
在Okta下。

1.定位至「應用程式」門戶，然後選擇 Create App Integration 中，如下圖所示：

2.選擇 SAML 2.0 作為應用程式型別，如下圖所示：



3.輸入應用程式名稱 SMA EUQ 選擇 Next中，如下圖所示：



4.在 SAML settings，填補空白，如下圖所示：

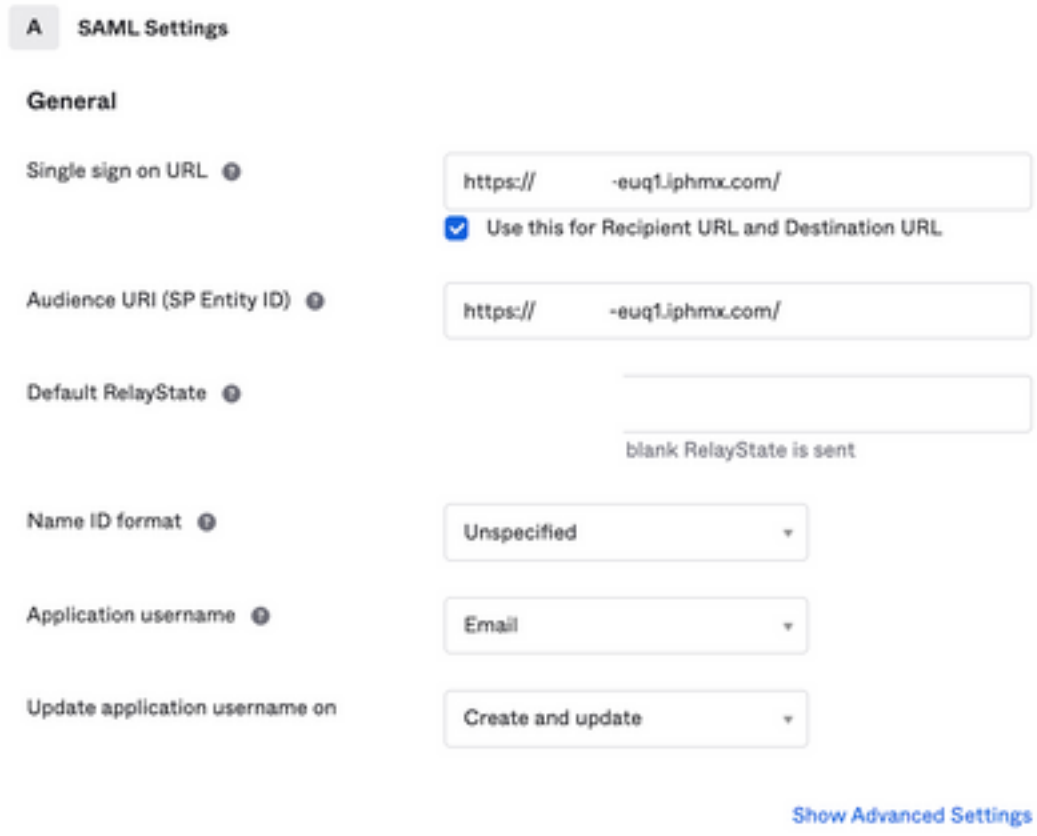
— 單點登入URL：這是從SMA EUQ介面獲得的宣告使用者服務。

— 受眾URI（SP實體ID）：這是從SMA EUQ實體ID獲取的實體ID。

— 名稱ID格式：保留為「未指定」(Unspecified)。

— 應用程式使用者名稱：提示使用者在身份驗證過程中輸入其電子郵件地址的電子郵件。

— 更新上的應用程式使用者名稱：建立和更新。



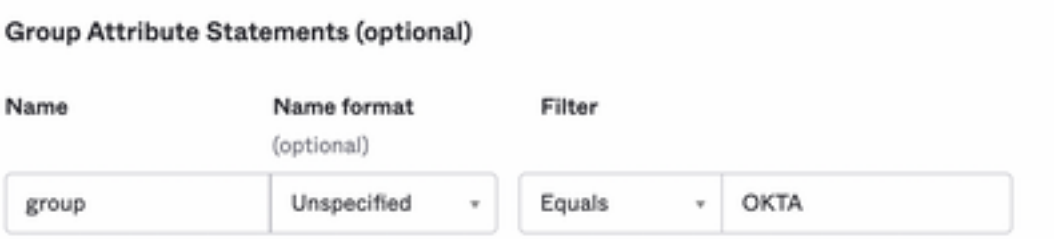
向下滾動到 Group Attibute Statements (optional) 中，如下圖所示：

輸入下一個屬性語句：

-名稱: group

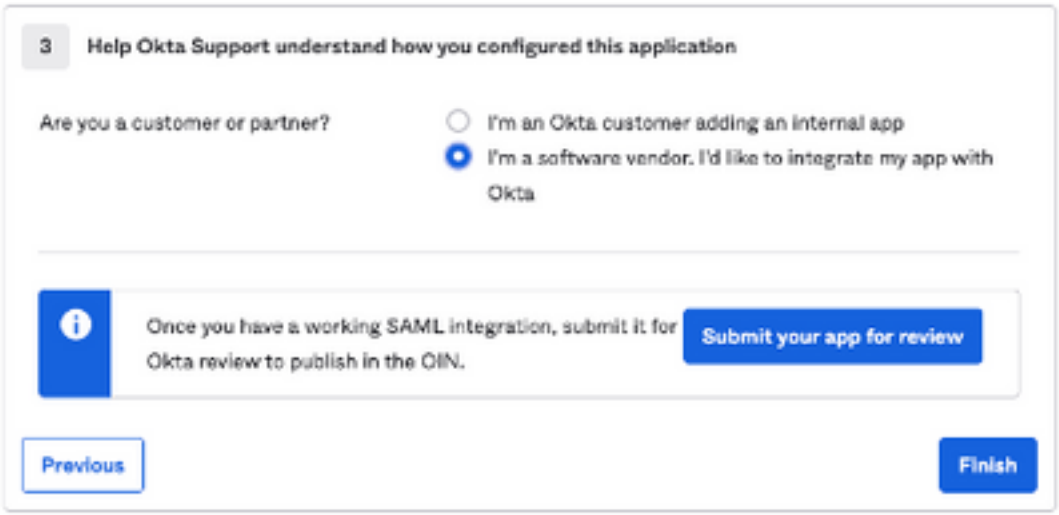
— 名稱格式： Unspecified

— 篩選器： Equals 和 OKTA



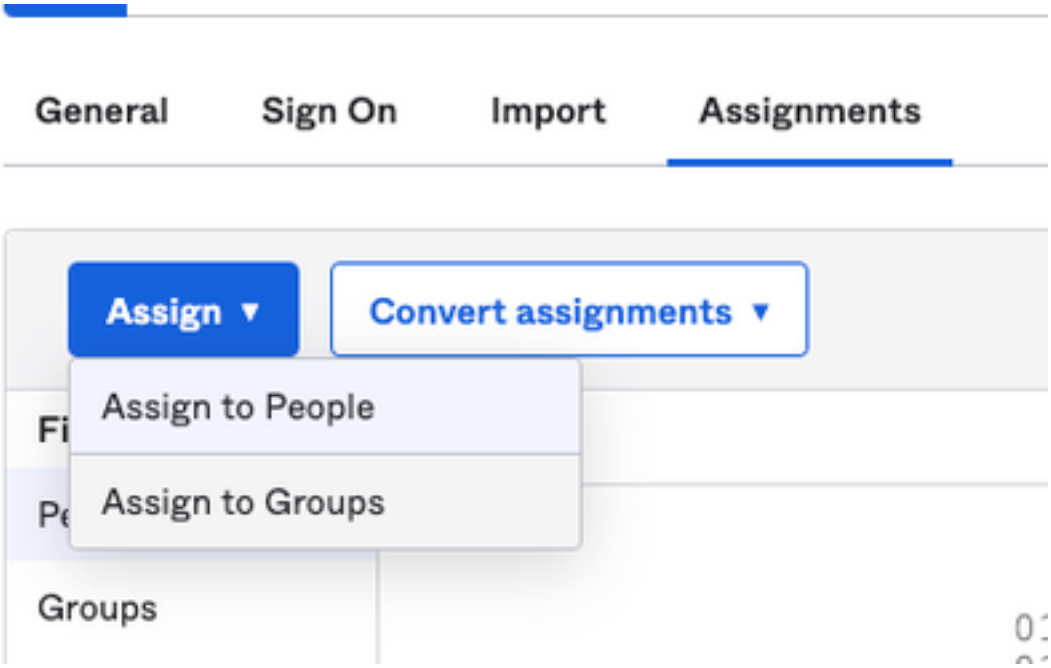
選擇 Next .

5.當被要求時 Help Okta to understand how you configured this application，請輸入當前環境的適用原因，如下圖所示：



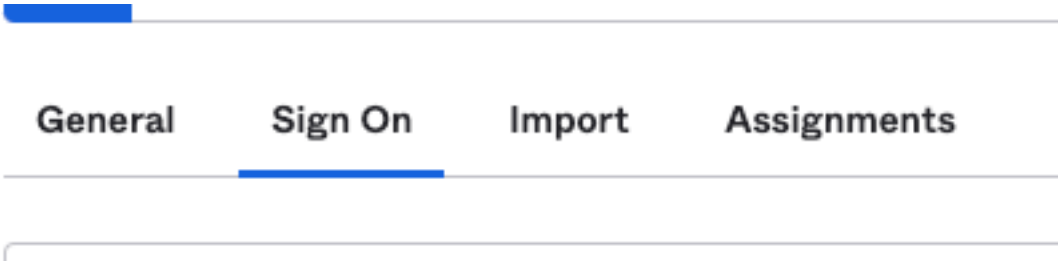
選擇 Finish 繼續下一步。

6.選擇 Assignments 頁籤，然後選擇 Assign > Assign to Groups中，如下圖所示：

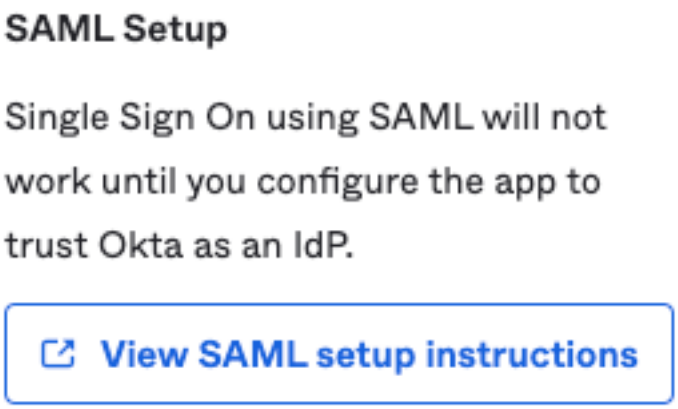


7.選擇OKTA組，該組具有訪問環境的授權使用者

8.選擇 Sign On 中，如下圖所示：



9.向下滾動到右角，選擇 View SAML setup instructions 選項，如下圖所示：

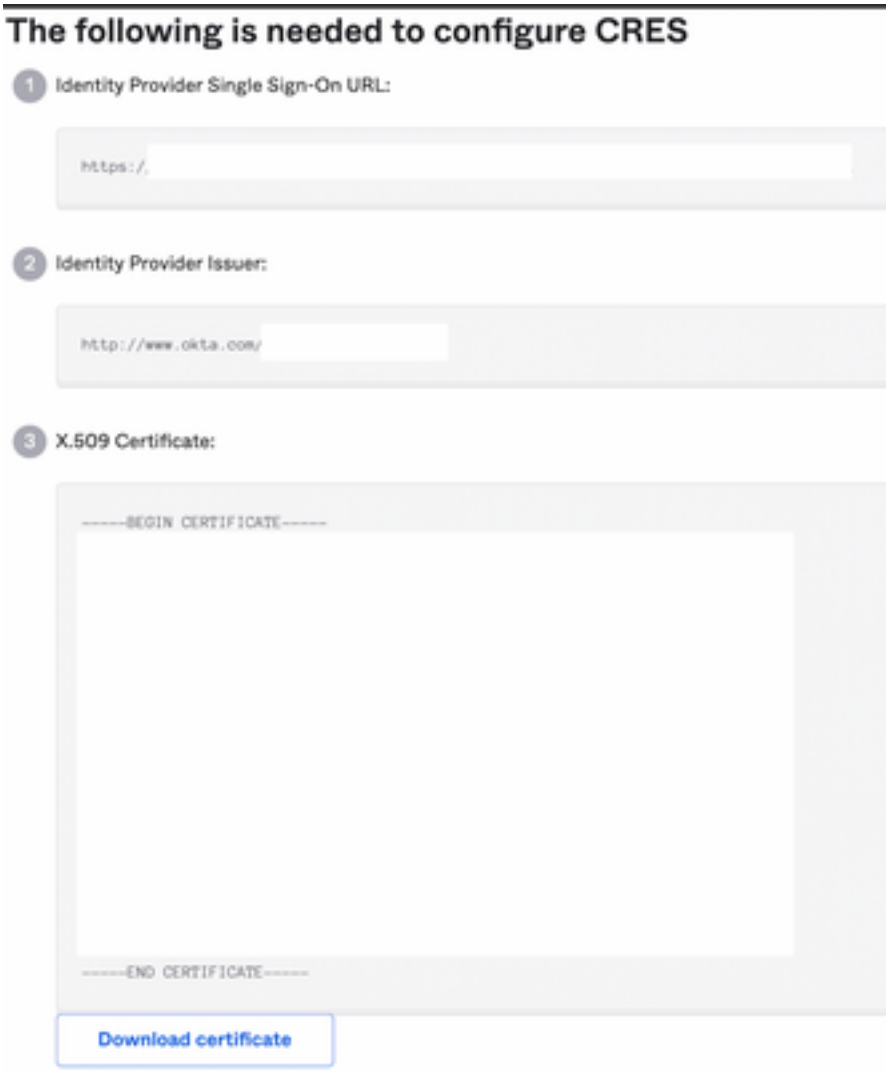


10.將此資訊儲存到記事本，需要放入 Cisco Security Management Appliance SAML配置，如下圖所示：

— 身份提供程式單一登入URL

— 身份提供程式頒發者

- X.509憑證

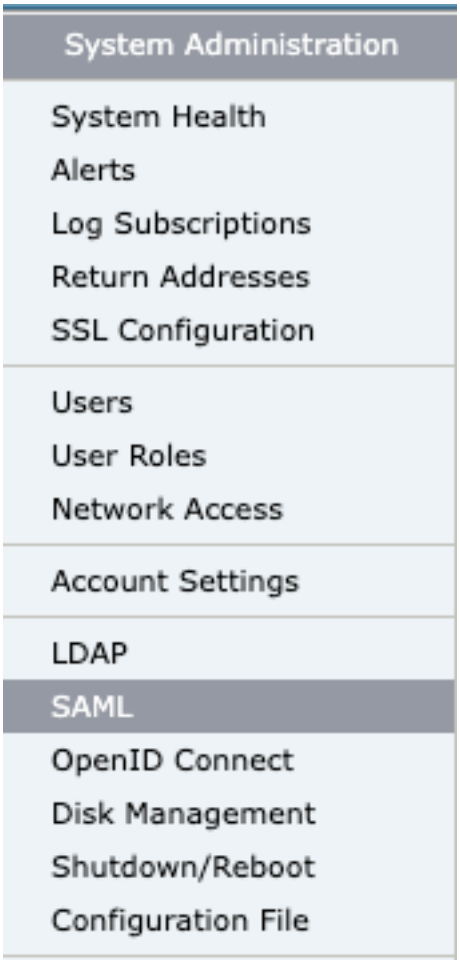


11.完成OKTA配置後，您可以返回思科安全管理裝置。

在思科安全管理裝置下：

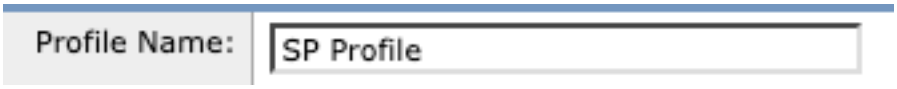
1.以雲管理員身份登入思科安全管理裝置，如下圖所示：

2.在 System Administration頁籤中，選擇 SAML 選項，如下圖所示：



3.開啟新視窗以配置SAML。在 SAML for End-User Quarantine，按一下 Add Service Provider 中，如下圖所示：

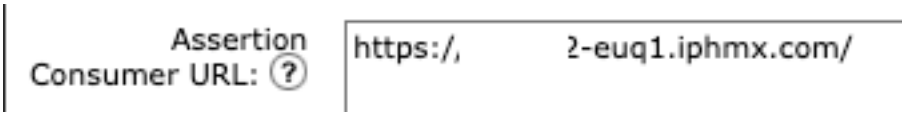
4.不足 Profile Name ，輸入服務提供商配置檔案的配置文件名稱，如下圖所示：



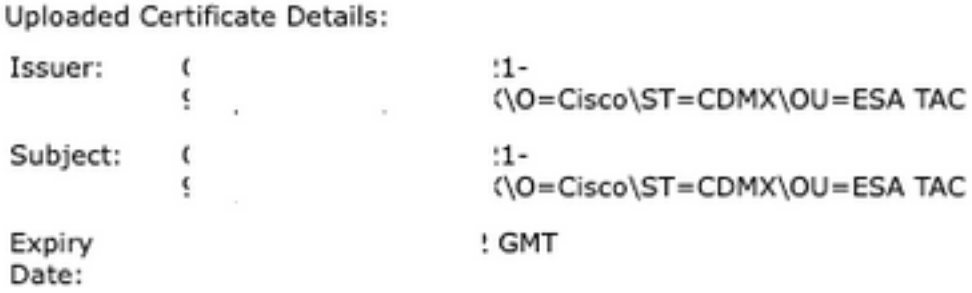
5.對於 Entity ID ,輸入服務提供商（在本例中為裝置）的全域性唯一名稱。服務提供商實體ID的格式通常是URI，如下圖所示：

6.對於 **Name ID Format** ,此欄位不可配置。在配置身份提供程式時需要此值，如下圖所示：

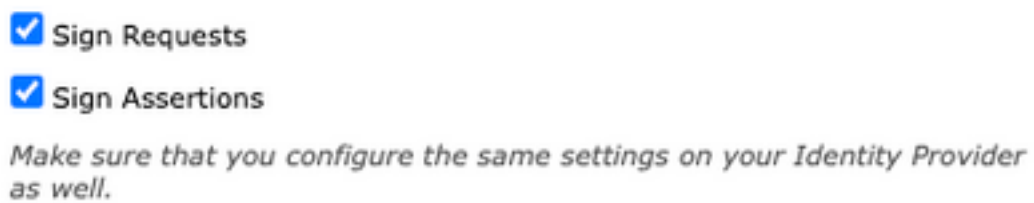
7.對於 **Assertion Consumer URL**，輸入身份驗證成功完成後，身份提供程式將SAML宣告傳送到的URL。在這種情況下，這是垃圾郵件隔離區的URL。



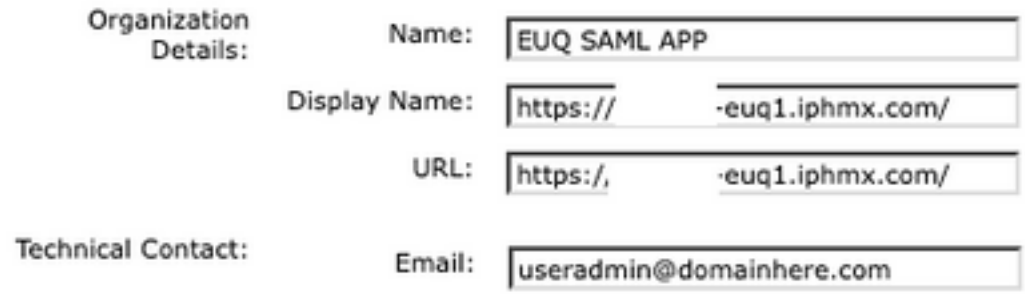
8.對於 SP Certificate 上傳證書和金鑰，或上傳PKCS #12檔案。上傳後， Uploaded Certificate Details 顯示，如下圖所示：



9.對於 Sign Requests and Sign Assertions ，如果要對SAML請求和斷言進行簽名，請選中這兩個覈取方塊。如果選擇選中這些選項，請確保在OKTA上配置相同的設定，如下圖所示：

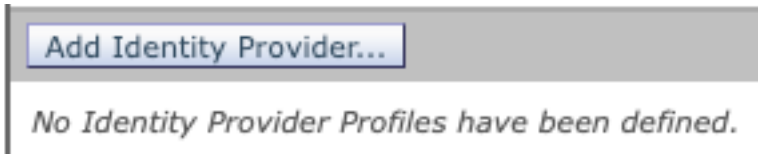


10.對於 Organization Details，輸入組織的詳細資訊，如下圖所示：



11. Submit 和 Commit 在繼續配置之前進行更改 Identity Provider Settings .

12.不足 SAML ，按一下 Add Identity Provider中，如下圖所示：



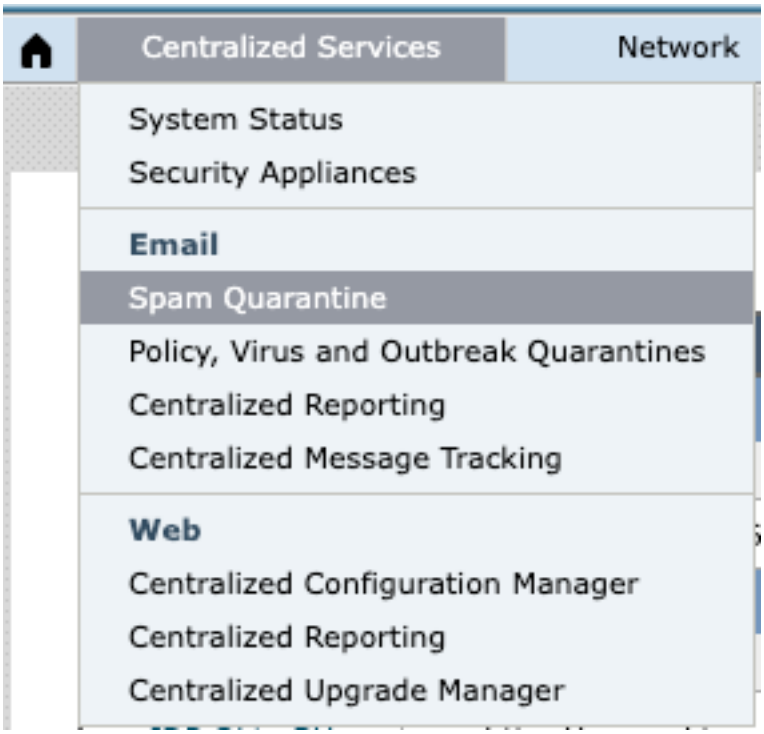
13.不足 Profile Name: 輸入身份提供程式配置檔案的名稱，如下圖所示：

14.選擇 Configure Keys Manually 並輸入以下資訊，如下圖所示：

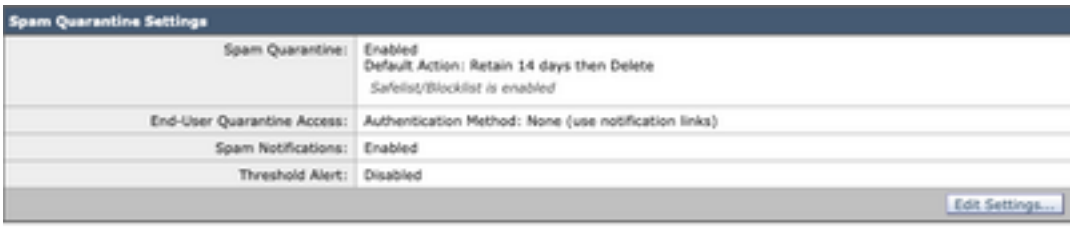
- 實體ID:身份提供程式實體ID用於唯一標識身份提供程式。它是在前面的步驟中通過OKTA設定獲得的。
- SSO URL:SP應向其傳送SAML身份驗證請求的URL。它是在前面的步驟中通過OKTA設定獲得的。
- 證書：由OKTA提供的證書。

15. Submit 和 Commit 更改以繼續SAML登入啟用。

16.不足 Centralized Services > Email ，按一下 Spam Quarantine中，如下圖所示：



17.不足 Spam Quarantine -> Spam Quarantine Settings ，按一下 Edit Settings ，as shown in the image:



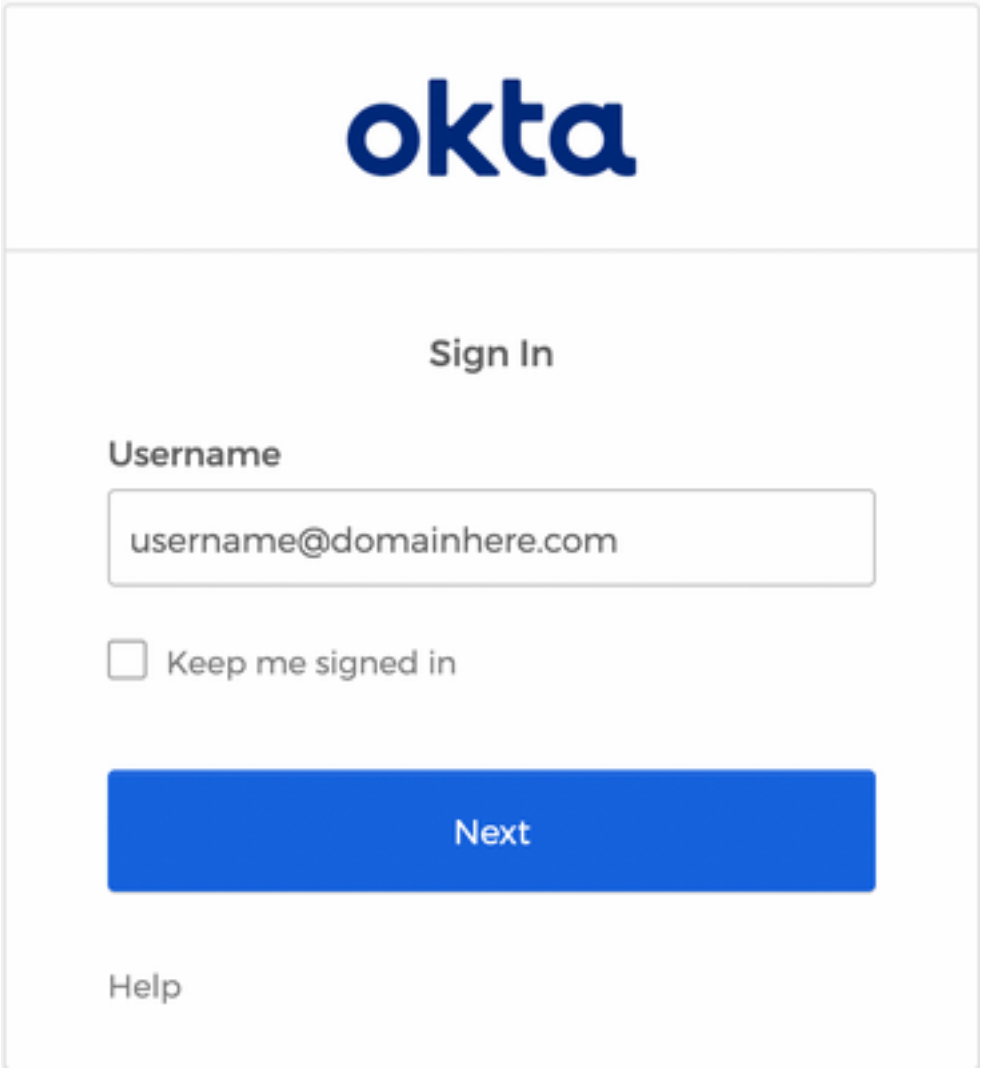
18.向下滾動到 End-User Quarantine Access > End-User Authentication ，選擇 SAML 2.0 中，如下圖所示：

19. Submit 和 Commit 更改以啟用SAML身份驗證 **End User Spam Quarantine** .

驗證

1.在任何Web瀏覽器中，輸入貴公司的終端使用者垃圾郵件隔離區的URL，如下圖所示：

2.開啟一個新視窗以繼續OKTA身份驗證。使用**OKTA憑據**登入，如下圖所示：



3.如果驗證成功，則 End User Spam Quarantine 為登入使用者開啟垃圾郵件隔離區的內容，如下圖所示：

現在，終端使用者可以使用OKTA憑證訪問終端使用者垃圾郵件隔離區。.

相關資訊

[Cisco Secure Email and Web Manager最終使用手冊]

[OKTA支援]

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）。