配置OKTA SSO外部身份驗證以實現高級網路釣魚防護

目錄

簡介

本文檔介紹如何配置OKTA SSO外部身份驗證以登入思科高級網路釣魚防護。

必要條件

管理員有權訪問思科高級網路釣魚防護門戶。

對Okta idP的管理員訪問許可權。

自簽名或CA簽名（可選）的X.509 SSL證書，採用PKCS #12或PEM格式。

背景資訊

- Cisco高級網路釣魚防護允許管理員使用SAML啟用SSO登入。
- OKTA是一個身份管理器，為您的應用程式提供身份驗證和授權服務。
- 思科高級網路釣魚防護可以設定為連線到OKTA進行身份驗證和授權的應用程式。
- SAML是一種基於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之後，無縫地訪問一組定義的應用程式。
- 要瞭解有關SAML的更多資訊，可以訪問下一個連結:SAML一般資訊

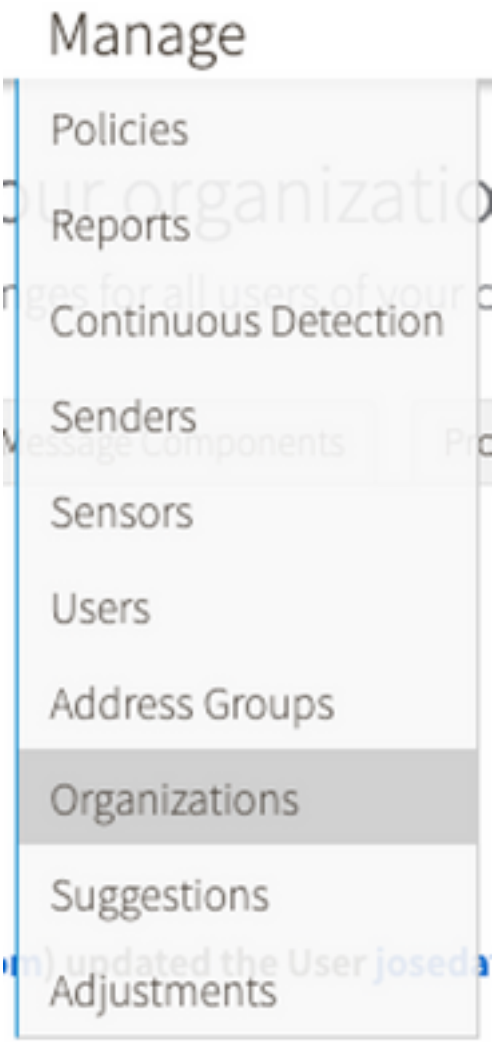
需求

- 思科高級網路釣魚防護門戶。
- OKTA管理員帳戶。

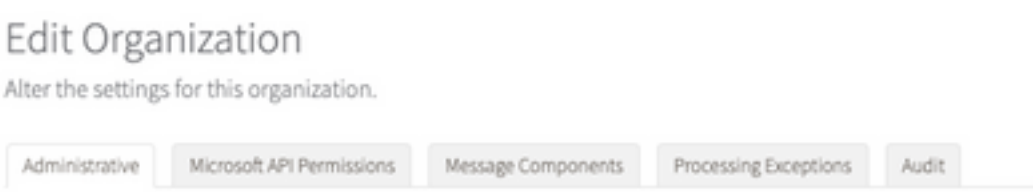
設定

在思科高級網路釣魚防護門戶下：

1.登入到組織門戶，然後選擇**管理 > 組織**，如下圖所示：



2.選擇您的組織名稱**編輯組織**，如下圖所示：



3.在**Administrative**頁籤上，向下滾動到**User Account Settings**，然後在SSO下選擇**Enable**，如下圖所示：

4.下一個視窗提供要在OKTA SSO配置下輸入的資訊。將以下資訊貼上到記事本，使用它配置OKTA設定：

— 實體ID:apcc.cisco.com

— 斷言消費者服務：此資料是為您的組織量身定製的。

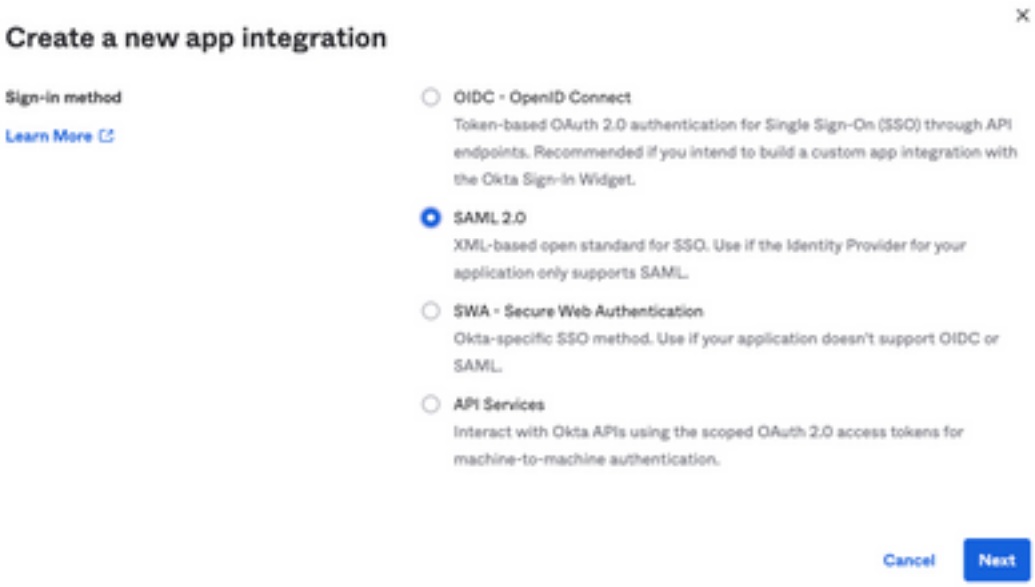
選擇要使用**電子郵**件地址登入的命名格式電子郵件，如下圖所示：

5.此時將思科高級網路釣魚防護配置降至最低，因為您需要先在OKTA中設定應用程式，然後再繼續下一步。

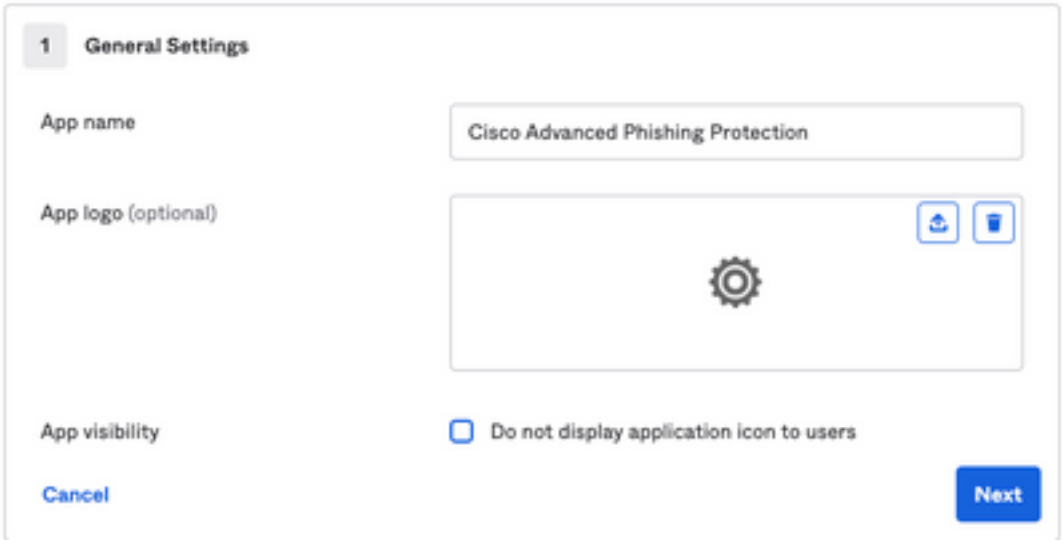
在Okta下。

1.定位至「應用程式」門戶，然後選擇**「建立應用程式整合」**，如下圖所示：

2.選擇**SAML 2.0**作為應用型別，如下圖所示：



3.輸入應用名稱**Advanced Phishing Protection**並選擇**Next**，如下圖所示：



4.在SAML設定下，填充間隙，如下圖所示：

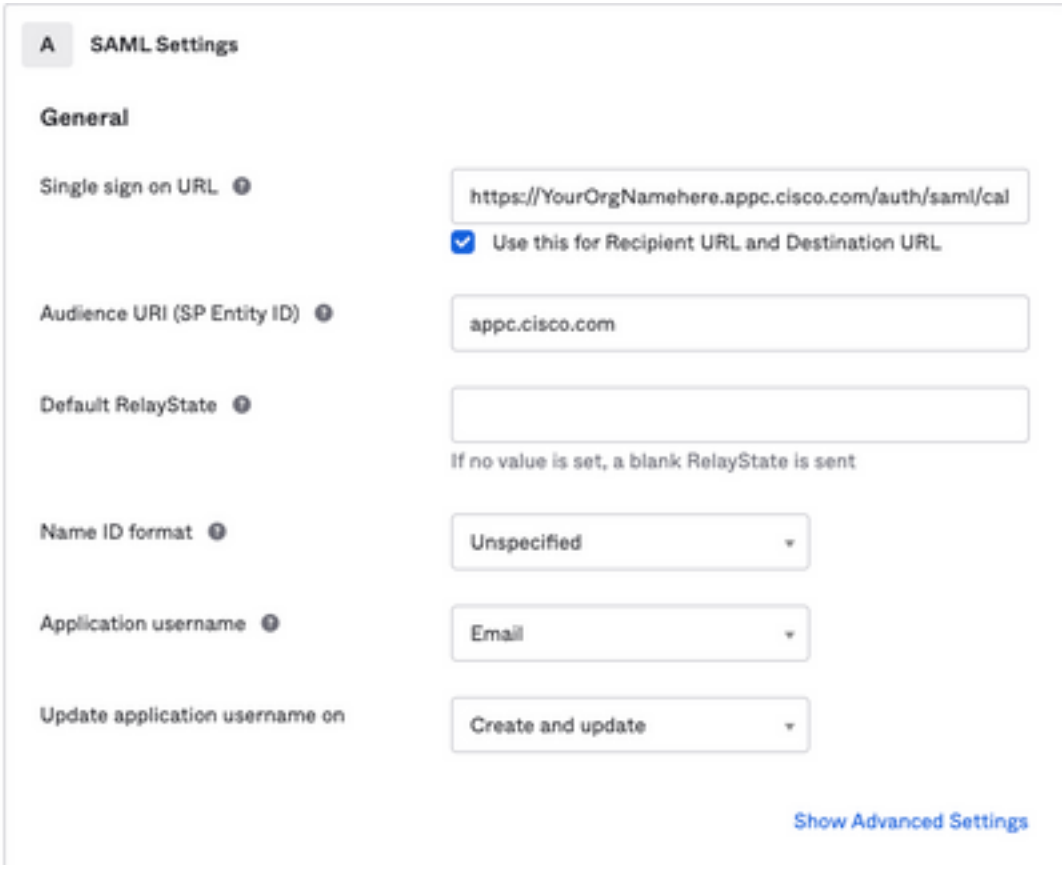
— 單點登入URL:這是通過思科高級網路釣魚防護獲得的斷言消費者服務。

— 收件人URL:這是從思科高級網路釣魚防護獲取的實體ID。

— 名稱ID格式：將其保留為「未指定」(Unspecified)。

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

— 更新應用程式使用者名稱：建立和更新。



向下滾動到**Group Attributes Statements（可選）**，如下圖所示：

輸入下一個屬性語句：

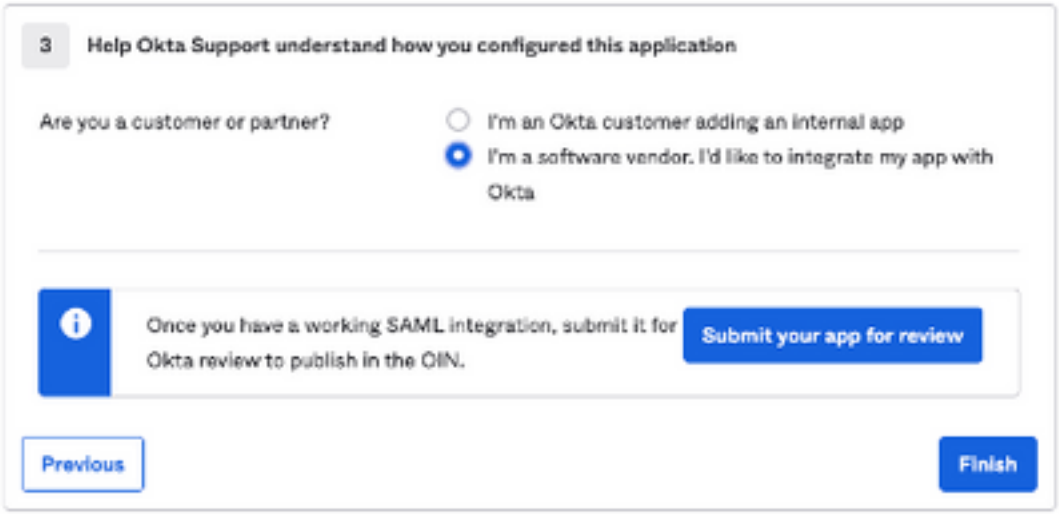
-名稱:群組

— 名稱格式：未指定。

— 篩選器：「等於」和「OKTA」

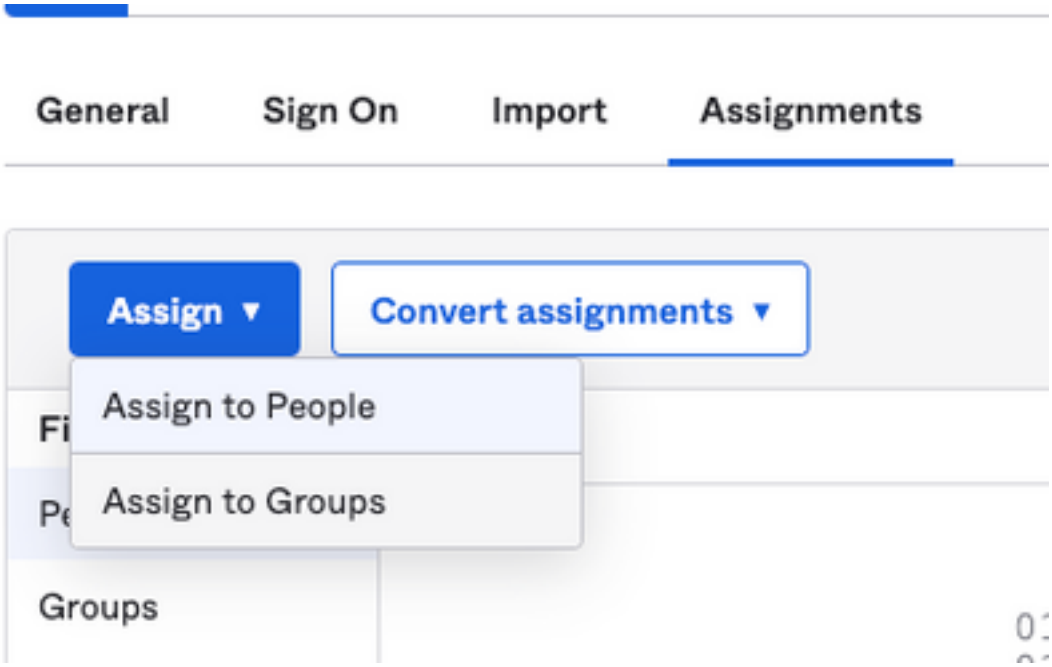
選擇「下一步」。

5.當要求幫助Okta瞭解您如何配置此應用程式時，請輸入當前環境適用的原因，如下圖所示：



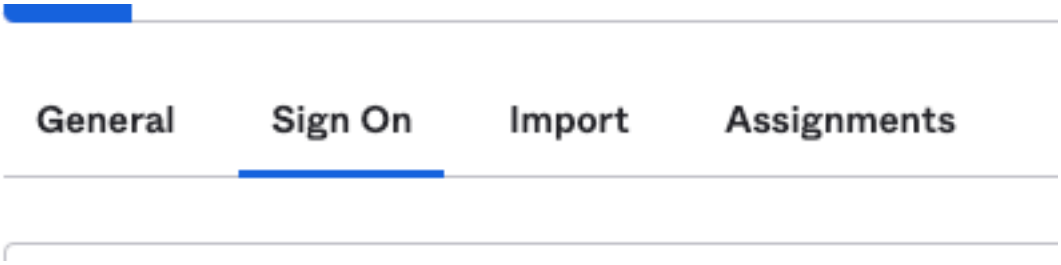
選擇Finish以繼續執行下一步。

6.選擇「**分配**」標籤，然後選擇「**分配**」>「**分配給組**」，如下圖所示：

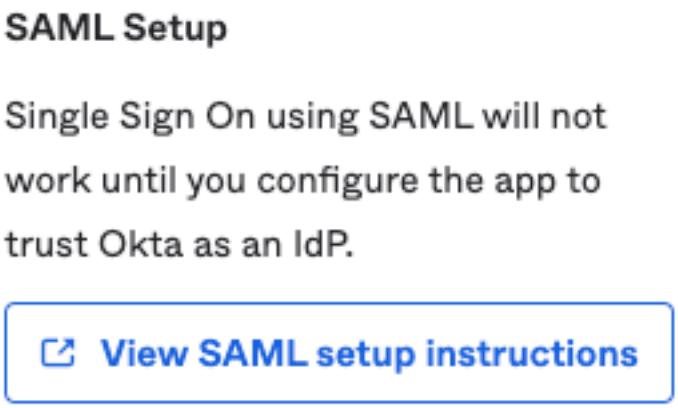


7.選擇OKTA組，該組是有權訪問環境的使用者的組

8.選擇**Sign On**，如下圖所示：



9.向下滾動到右角，輸入**檢視SAML設定說明**選項，如下圖所示：

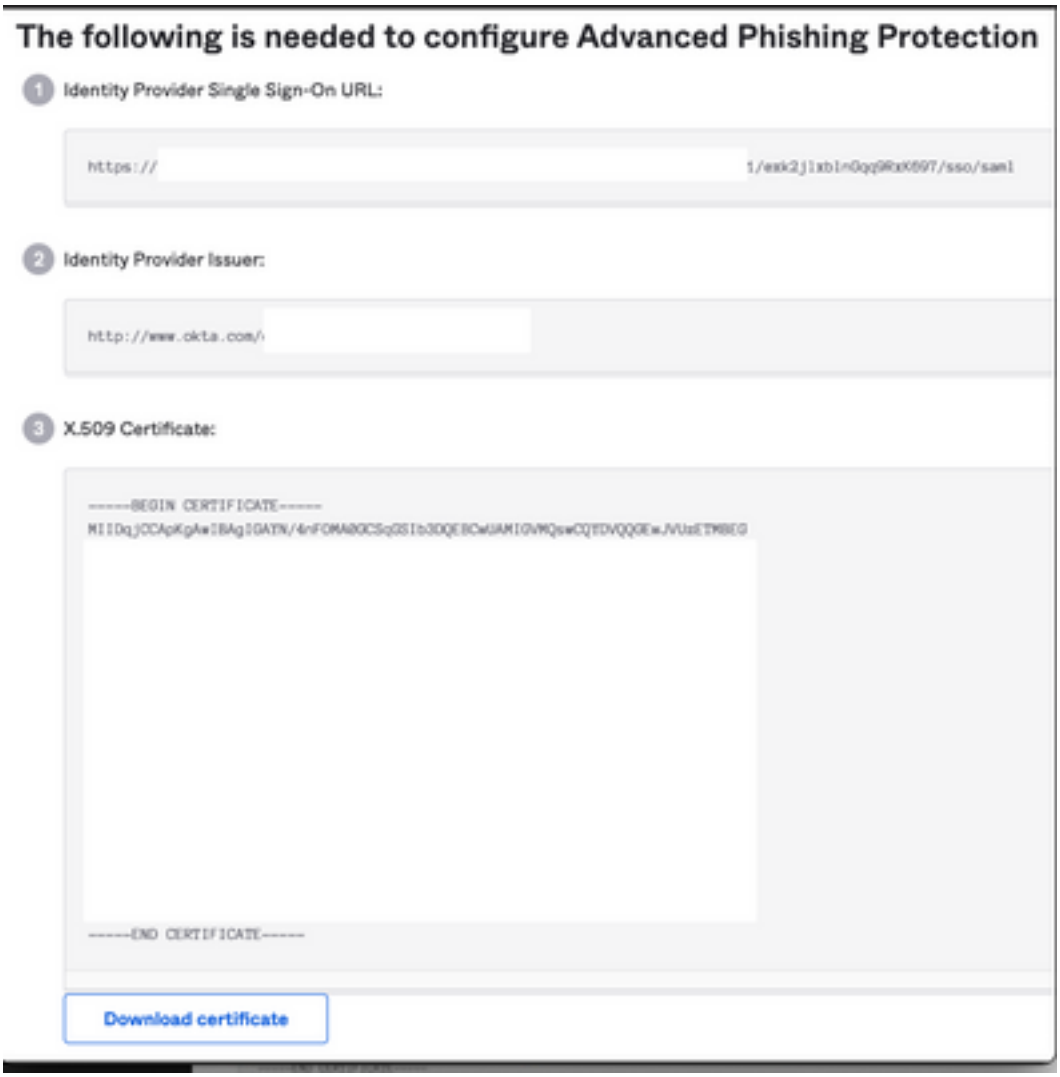


9.將輸入思科高級網路釣魚防護門戶所需的下一個資訊儲存到記事本，如下圖所示：

— 身份提供程式單一登入URL。

— 確定提供商頒發者（對於思科高級網路釣魚防護來說不是必需的，但對於其他應用程式來說則是必需的）。

- X.509憑證。



10.完成OKTA配置後，您可以返回到思科高級網路釣魚防護

在思科高級網路釣魚防護門戶下：

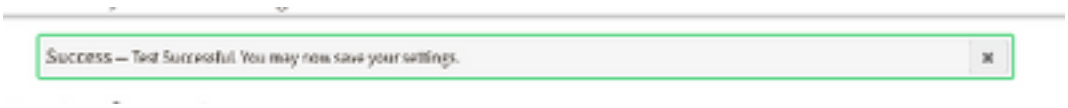
1.使用名稱識別符號格式，輸入以下資訊：

- SAML 2.0終結點（HTTP重定向）：Okta提供的識別提供程式單點登入URL。

— 公共證書：輸入Okta提供的X.509證書。

2.選擇**測試設定**以驗證配置是否正確

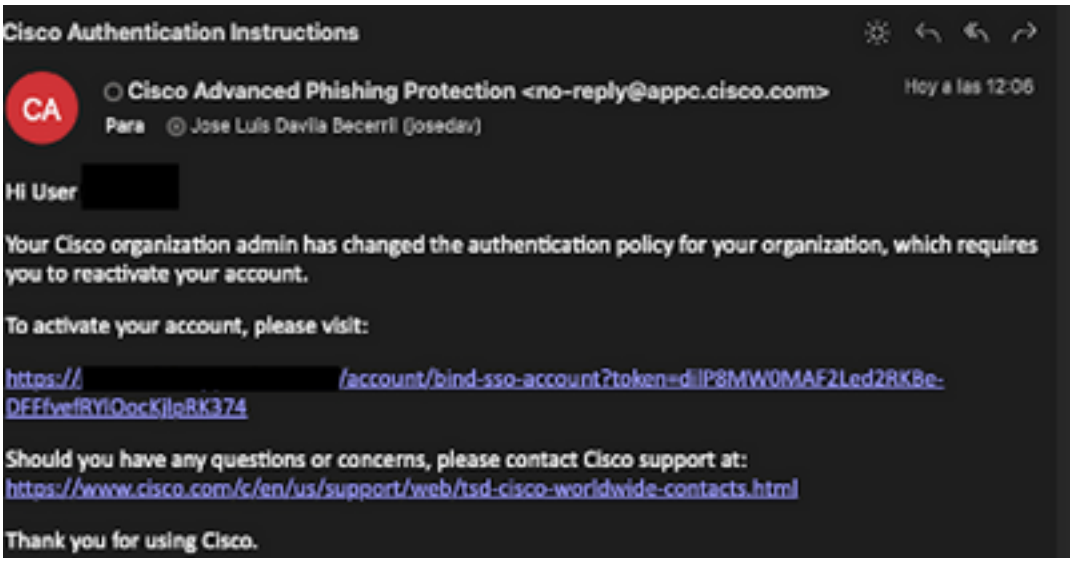
如果配置中沒有錯誤，您會看到「測試成功」條目，現在可以儲存您的設定，如下圖所示：



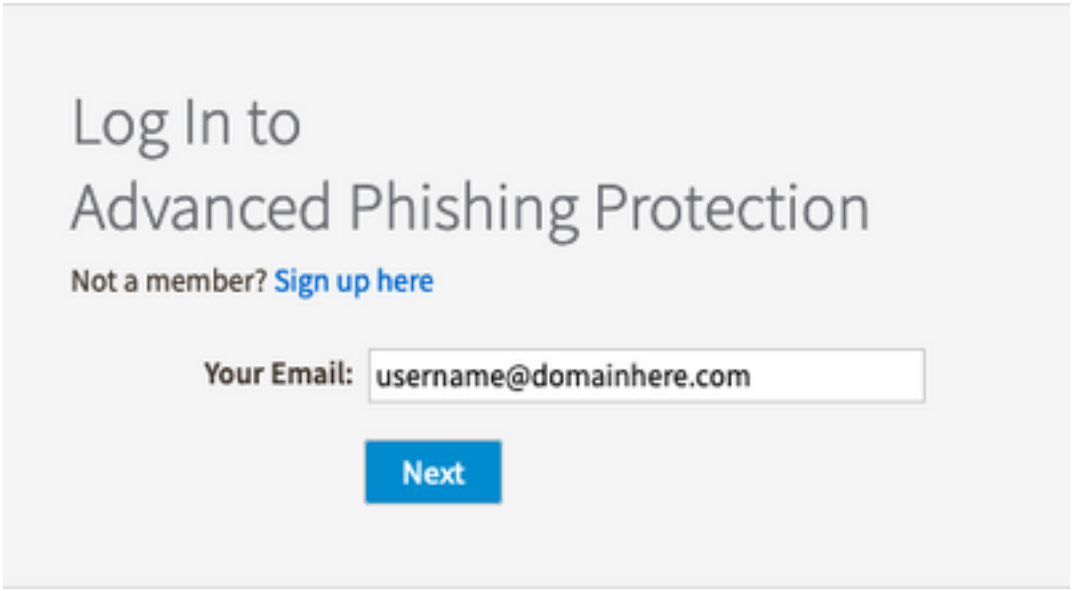
3.儲存設定

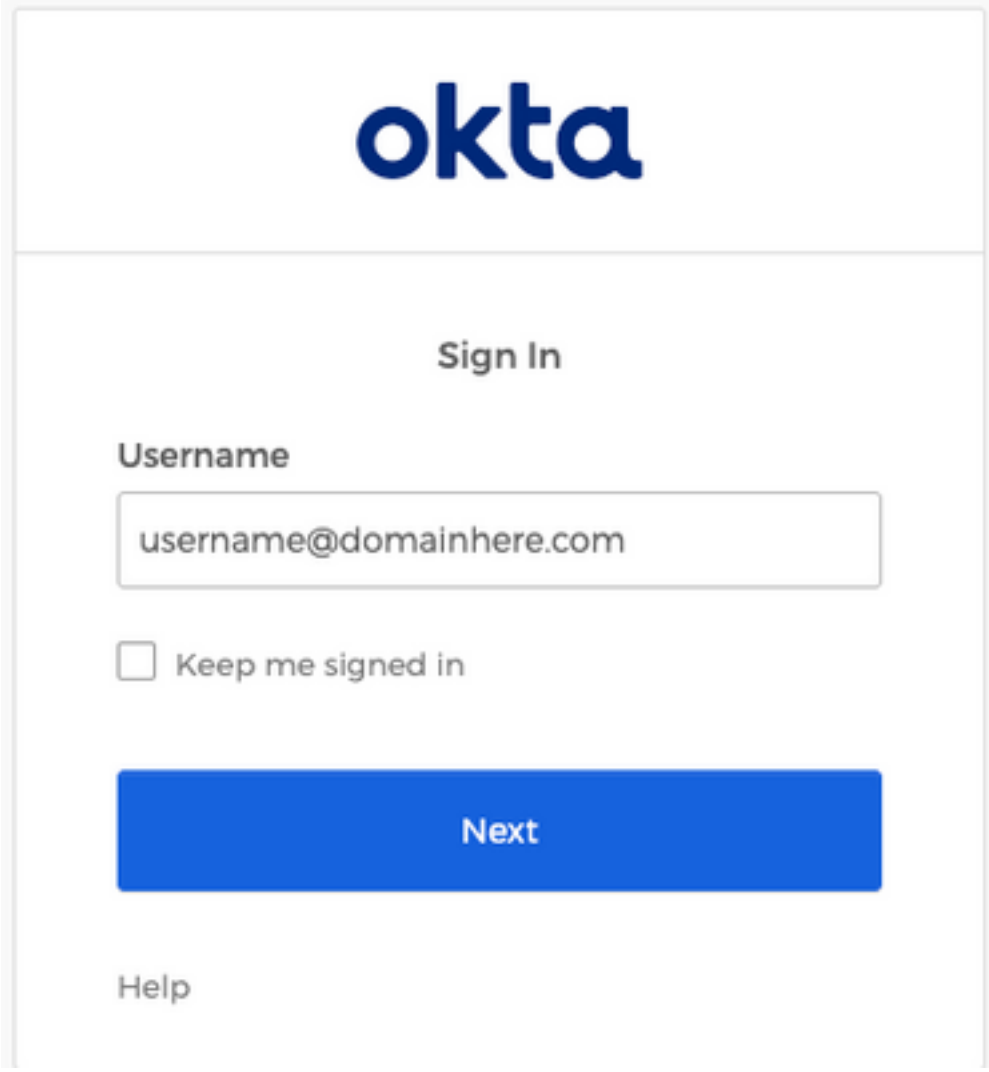
驗證

1.對於不使用SSO的任何現有管理員，系統會通過電子郵件通知他們組織的身份驗證策略已更改，並要求管理員使用外部連結啟用其帳戶，如下圖所示：

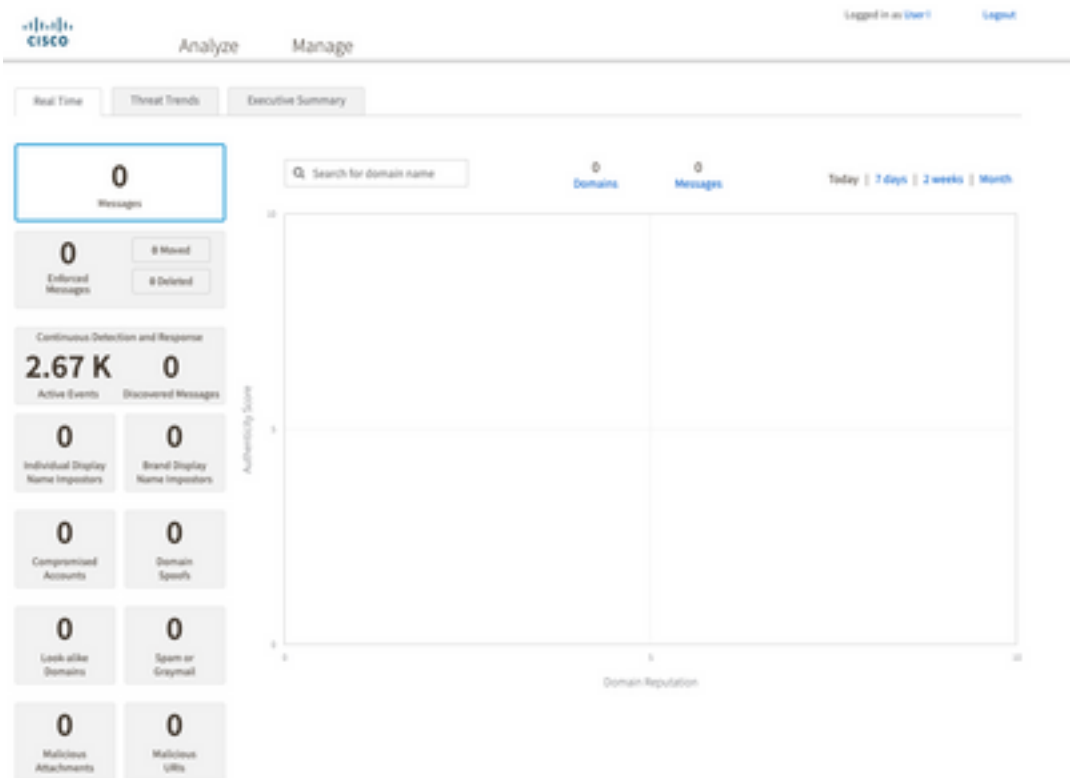


2.帳戶啟用後，請輸入您的電子郵件地址，然後重定向至OKTA登入網站進行登入，如下圖所示：





3. OKTA登入過程完成後，登入思科高級網路釣魚防護門戶，如下圖所示：



相關資訊

思科高級網路釣魚防護 — 產品資訊

思科高級網路釣魚防護 — 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）。