

# 為CRES配置OKTA SSO外部身份驗證

## 目錄

[簡介](#)

[必要條件](#)

[背景資訊](#)

[需求](#)

[設定](#)

[驗證](#)

[相關資訊](#)

## 簡介

本文檔介紹如何配置OKTA SSO外部身份驗證以登入思科安全郵件加密服務 ( 註冊信封 ) 。

## 必要條件

對思科安全郵件加密服務 ( 註冊信封 ) 的管理員訪問許可權。

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

- Cisco Secure Email Encryption Service(Registered Envelope)為使用SAML的終端使用者啟用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。
- 思科安全電子郵件加密服務 ( 註冊信封 ) 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的詳細資訊，請參閱：[SAML一般資訊](#)

## 需求

- 思科安全電子郵件加密服務 ( 註冊信封 ) 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：

## Applications

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

2.選擇 SAML 2.0 作為應用程式型別，如下圖所示：

### Create a new app integration ✕

Sign-in method

[Learn More](#)

OIDC - OpenID Connect

Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

SAML 2.0

XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

SWA - Secure Web Authentication

Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

API Services

Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

3.輸入應用程式名稱 CRES 並選取 Next中，如下圖所示：

#### 1 General Settings

App name

CRES

App logo (optional)



App visibility

Do not display application icon to users

Cancel

Next

4.在 SAML settings，填補空白，如下圖所示：

— 單點登入URL：這是從思科安全郵件加密服務獲取的宣告使用者服務。

— 受眾URI ( SP實體ID )：這是從思科安全電子郵件加密服務獲取的實體ID。

— 名稱ID格式：保留為「未指定」(Unspecified)。

— 應用程式使用者名稱：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。

— 更新上的應用程式使用者名稱：建立和更新。

**A SAML Settings**

**General**

Single sign on URL   
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID)

Default RelayState   
If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

向下滾動到 Group Attribute 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

#### Group Attribute Statements (optional)

Name	Name format (optional)	Filter
group	Unspecified	Equals 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：

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

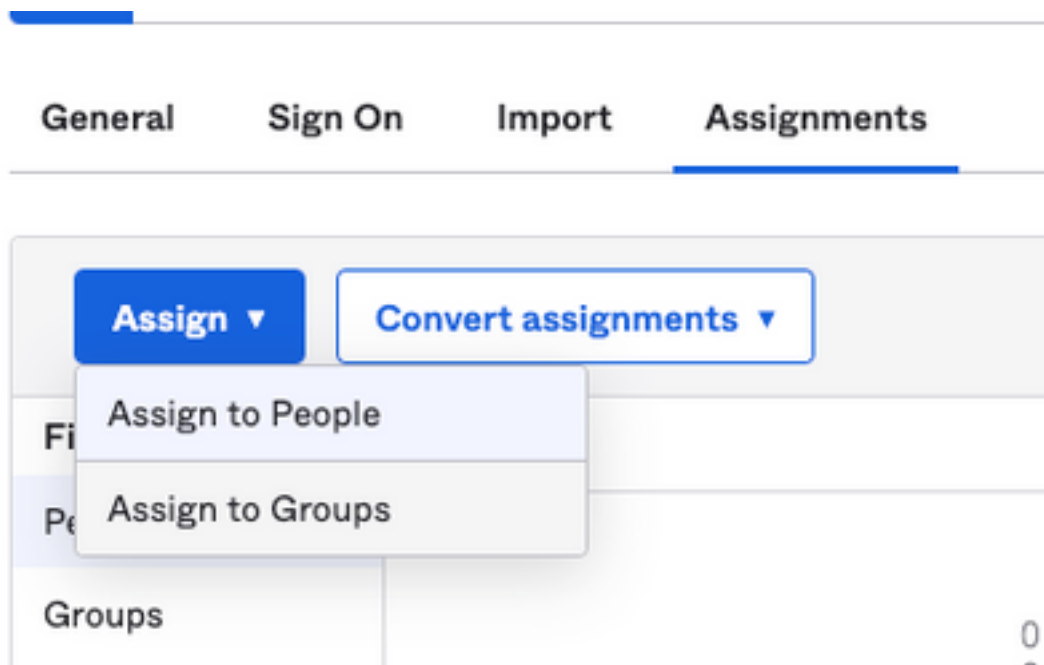
I'm a software vendor. I'd like to integrate my app with Okta

Once you have a working SAML integration, submit it for Okta review to publish in the OIN. [Submit your app for review](#)

[Previous](#) [Finish](#)

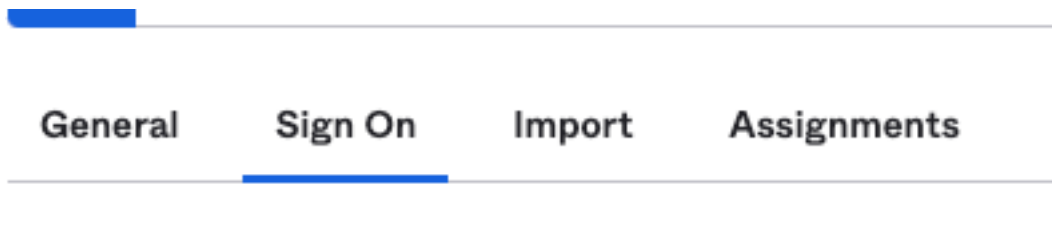
選擇 Finish 繼續下一步。

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，該組是有權訪問環境的使用者的組。

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：

## SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

10.將所需的下一個資訊儲存到記事本，以放入 Cisco Secure Email Encryption Service 輸入網站，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

### The following is needed to configure CRES

1 Identity Provider Single Sign-On URL:

https://

2 Identity Provider Issuer:

http://www.okta.com/

3 X.509 Certificate:

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

[Download certificate](#)

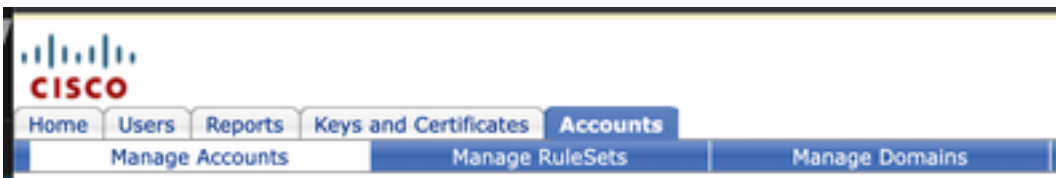
11.完成OKTA配置後，您可以返回思科安全郵件加密服務。

在Cisco Secure Email Encryption Service ( 註冊信封 ) 下：

1.以管理員身份登入您的組織門戶，連結為：[CRES管理門戶](#)，如下圖所示：



2.在 Accounts 頁籤中，選擇 Manage Accounts 頁籤，如下圖所示：



3.按一下帳號，然後選擇 Details 頁籤，如下圖所示：



4.向下滾動到 Authentication Method 並選取 SAML 2.0中，如下圖所示：

Authentication Method **SAML 2.0** ▾

5.對於以下方面：SSO Alternate Email Attribute，將其留空，如下圖所示：

SSO Alternate Email Attribute Name

6.就本集團而言，SSO Service Provider Entity ID\*，請輸入 <https://res.cisco.com/> 中，如下圖所示：

SSO Service Provider  
Entity ID\*

7.對於 SSO Customer Service URL\*，請輸入 Identity Provider Single Sign-On URL 由Okta提供，如下圖所示：

SSO Customer Service  
URL\*

8.對於 SSO Logout URL，將其留空，如下圖所示：

SSO Logout URL

9.對於 SSO Identity Provider Verification Certificate上傳由OKTA提供的X.509證書。

10.選擇 **Save** 要儲存設定，如下圖所示：

**Save**

**Back to Accounts List**

11.選擇 **Activate SAML** 要啟動SAML身份驗證過程並實施SSO身份驗證，如下圖所示：

**Activate  
SAML**

**Save**

**Back to  
Accounts List**

12.開啟一個新視窗，通知SAML身份驗證在成功通過SAML身份提供程式身份驗證後變為活動狀態。選擇 **Continue**中，如下圖所示：

---

SAML authentication will be active after a successful authentication with the SAML Identity  
Provider.  
Please click continue to authenticate.

**Continue**

13.開啟一個新視窗，以使用OKTA憑證進行身份驗證。輸入 Username 並選取 **Next**中，如下圖所示：



## Sign In

Username

Keep me signed in

Next

Help

14. 如果驗證過程成功，則 SAML Authentication Successful 顯示。選擇 Continue 如圖所示，關閉此視窗：

---

SAML Authentication Successful.

Please click continue to close.

Continue

15. 確認 SSO Enable Date 設定為SAML身份驗證成功的日期和時間，如下圖所示：



Authentication Method	SAML 2.0 ▾
SSO Enable Date	10/18/2022 15:21:07 CDT
SSO Email Name ID Format	transient
SSO Alternate Email Attribute Name	<input type="text"/>
SSO Service Provider Entity ID*	<input type="text" value="https://res.cisco.com/"/>
SSO Customer Service URL*	<input type="text" value="https://"/> <input type="text" value="t.okta.com/app/"/>
SSO Logout URL	<input type="text"/>
SSO Service Provider Verification Certificate	<a href="#">Download</a>
SSO Binding	HTTP-Redirect, HTTP-POST
SSO Assertion Consumer URL	https://res.cisco.com/websafe/ssourl
Current Certificate	

SAML配置已完成。從此時起，CRES組織的使用者將被重定向到使用他們的OKTA憑據輸入其電子郵件地址。

## 驗證

1. 導航到[安全電子郵件加密服務門戶](#)。輸入註冊到CRES的電子郵件地址，如下圖所示：

# Secure Email Encryption Service

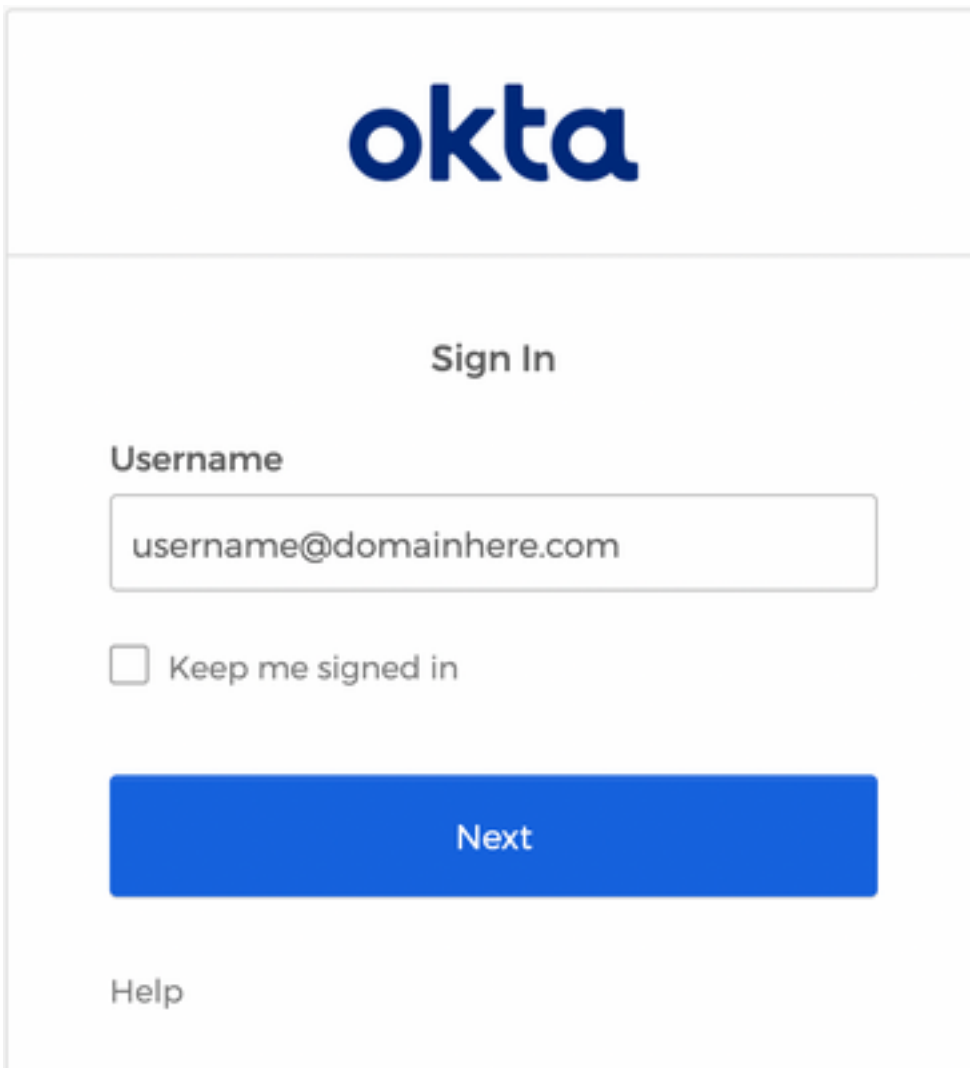
Username\*

Log In

OR

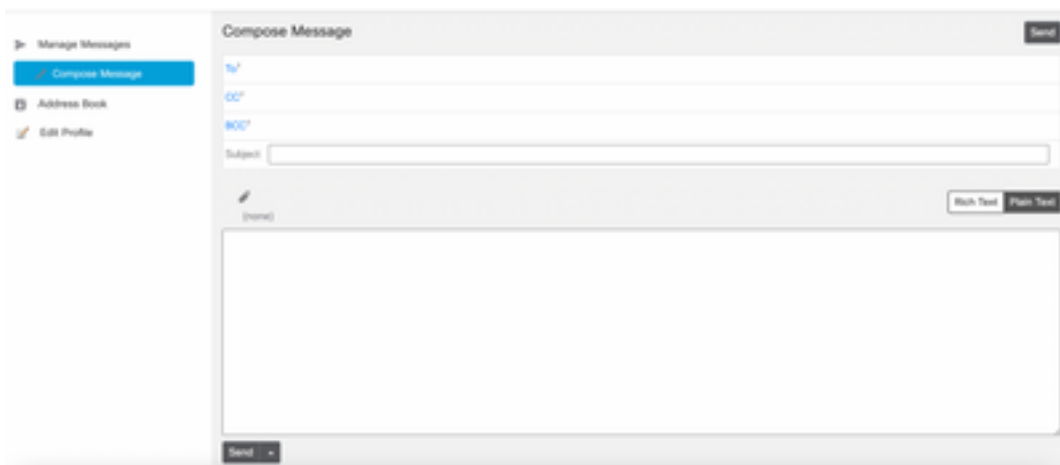
 Sign in with Google

2. 開啟一個新視窗，繼續使用OKTA憑證進行OKTA身份驗證登入，如下圖所示：



The image shows the Okta Sign In interface. At the top is the Okta logo. Below it is the text "Sign In". There is a "Username" label followed by a text input field containing "username@domainhere.com". Below the input field is a checkbox labeled "Keep me signed in". A large blue button labeled "Next" is positioned below the checkbox. At the bottom left, there is a "Help" link.

3.如果驗證成功，安全郵件加密服務將開啟 Compose Message 視窗，如下圖所示：



The image shows a "Compose Message" window. On the left is a sidebar with navigation options: "Manage Messages", "Compose Message" (highlighted), "Address Book", and "Edit Profile". The main area is titled "Compose Message" and contains fields for "To:", "CC:", "BCC:", and "Subject:". Below these fields is a rich text editor with a "Rich Text" button and a "Plain Text" button. A "Send" button is located at the bottom right of the window.

現在，終端使用者可以訪問安全郵件加密服務門戶，以撰寫安全電子郵件或開啟具有OKTA憑據的信封。

## 相關資訊

[思科安全電子郵件加密服務6.2帳戶管理員指南](#)

[Cisco Secure Gateway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）。