

# 为CRES配置OKTA SSO外部身份验证

## 目录

[简介](#)

[先决条件](#)

[背景信息](#)

[要求](#)

[配置](#)

[验证](#)

[相关信息](#)

## 简介

本文档介绍如何配置OKTA SSO外部身份验证以登录思科安全邮件加密服务（注册信封）。

## 先决条件

管理员有权访问思科安全邮件加密服务（注册信封）。

OKTA的管理员访问权限。

自签名或CA签名（可选）PKCS #12或PEM格式（由OKTA提供）的X.509 SSL证书。

## 背景信息

- 思科安全邮件加密服务（注册信封）为使用SAML的最终用户启用SSO登录。
- OKTA是一个身份管理器，为您的应用提供身份验证和授权服务。
- 思科安全邮件加密服务（注册信封）可以设置为连接到OKTA进行身份验证和授权的应用。
- SAML是基于XML的开放标准数据格式，使管理员能够在登录其中一个应用后无缝访问一组已定义的应用。
- 要了解有关SAML的详细信息，请参阅[SAML一般信息](#)

## 要求

- 思科安全邮件加密服务（注册信封）管理员帐户。
- OKTA管理员帐户。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备都以清除（默认）配置开头。如果网络处于活动状态，请确保您了解任何命令的潜在影响。

## 配置

在Okta下。

1.定位至“应用程序”门户，然后选择 Create App Integration,如图所示：

## Applications

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

2.选择 SAML 2.0 作为应用类型，如图所示：

### 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.输入应用名称 CRES 并选择 Next,如图所示：

#### 1 General Settings

App name

CRES

App logo (optional)



App visibility

Do not display application icon to users

Cancel

Next

4.在 SAML settings，如图所示，填空隙：

— 单点登录URL：这是从思科安全邮件加密服务获取的断言消费者服务。

— 受众URI ( SP实体ID )：这是从思科安全邮件加密服务获取的实体ID。

— 名称ID格式：保留为未指定。

— 应用用户名：邮件，提示用户在身份验证过程中输入其邮件地址。

— 更新上的应用程序用户名：创建和更新。

## 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](#)

向下滚动到 Group Attribute Statements (optional), 如图所示:

输入下一个属性语句:

-姓名: group

-姓名格式: Unspecified

— 过滤器: Equals 和 OKTA

### Group Attribute Statements (optional)

Name	Name format (optional)	Filter
<input type="text" value="group"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Equals"/> <input type="text" value="OKTA"/>

选择 Next .

5. 当被要求时 Help Okta to understand how you configured this application , 请输入当前环境的适用原因 , 如图所示:

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](#)

选择 Finish 继续下一步。

6.选择 Assignments 选项卡，然后选择 Assign > Assign to Groups,如图所示:

General Sign On Import **Assignments**

[Assign](#) [Convert assignments](#)

Assign to People

Assign to Groups

Groups

7.选择OKTA组，该组为具有有权访问环境的用户的组。

8.选择 Sign On,如图所示:

General **Sign On** Import Assignments

9.向下滚动至右下角，选择 View SAML setup instructions 选项，如图所示：

## 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.将下一个需要输入的信息保存到记事本 Cisco Secure Email Encryption Service 门户，如图所示：

- 身份提供程序单点登录URL
- 身份提供程序颁发者
- X.509证书

### 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配置后，您可以返回思科安全邮件加密服务。

在思科安全邮件加密服务（注册信封）下：

1.以管理员身份登录您的组织门户，链接为：[CRES Administration Portal](#)，如图所示：



Administration Console Log In

Welcome, please log in:

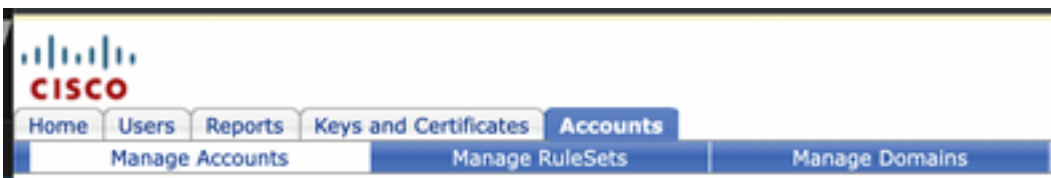
Username

Password

Remember me on this computer.

[Forgot password?](#)

2.在 Accounts 选项卡，选择 Manage Accounts 选项卡，如图所示：



CISCO

Home Users Reports Keys and Certificates Accounts

Manage Accounts Manage RuleSets Manage Domains

3.单击帐号并选择 Details 选项卡，如图所示：



Details Groups Tokens

4.向下滚动到 Authentication Method 并选择 SAML 2.0,如图所示:



Authentication Method

5.对于 SSO Alternate Email Attribute，将其留空，如图所示：



SSO Alternate Email Attribute Name

6.对于 SSO Service Provider Entity ID\*，输入 <https://res.cisco.com/> ,如图所示:



SSO Service Provider Entity ID\*

7.对于 SSO Customer Service URL\* , 输入 Identity Provider Single Sign-On URL 由Okta提供 , 如图所示 :

SSO Customer Service URL\*

8.对于 SSO Logout URL , 将其留空 , 如图所示 :

SSO Logout URL

9.对于 SSO Identity Provider Verification Certificate上传OKTA提供的X.509证书。

10.选择 **Save** 要保存设置 , 如图所示 :

**Save** **Back to Accounts List**

11.选择 **Activate SAML** 要启动SAML身份验证过程并实施SSO身份验证 , 如图所示 :

**Activate SAML** **Save** **Back to Accounts List**

12.将打开一个新窗口 , 通知SAML身份验证在与SAML身份提供方成功身份验证后变为活动状态。选择 **Continue**, 如图所示:

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

**Continue**

13.将打开一个新窗口 , 以使用OKTA凭证进行身份验证。输入 Username 并选择 **Next**, 如图所示:



## Sign In

Username

Keep me signed in

Next

Help

14.如果身份验证过程成功， SAML Authentication Successful 显示。选择 Continue 要关闭此窗口，如图所示：

---

SAML Authentication Successful.

Please click continue to close.

Continue

15.确认 SSO Enable Date 设置为SAML身份验证成功的日期和时间，如图所示：



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:// i.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。从此时起，属于CRES组织的用户在输入其电子邮件地址时，将被重定向以使用其OKTA凭证。

## 验证

1.导航到[安全邮件加密服务门户](#)。输入注册到CRES的邮件地址，如图所示：

# Secure Email Encryption Service

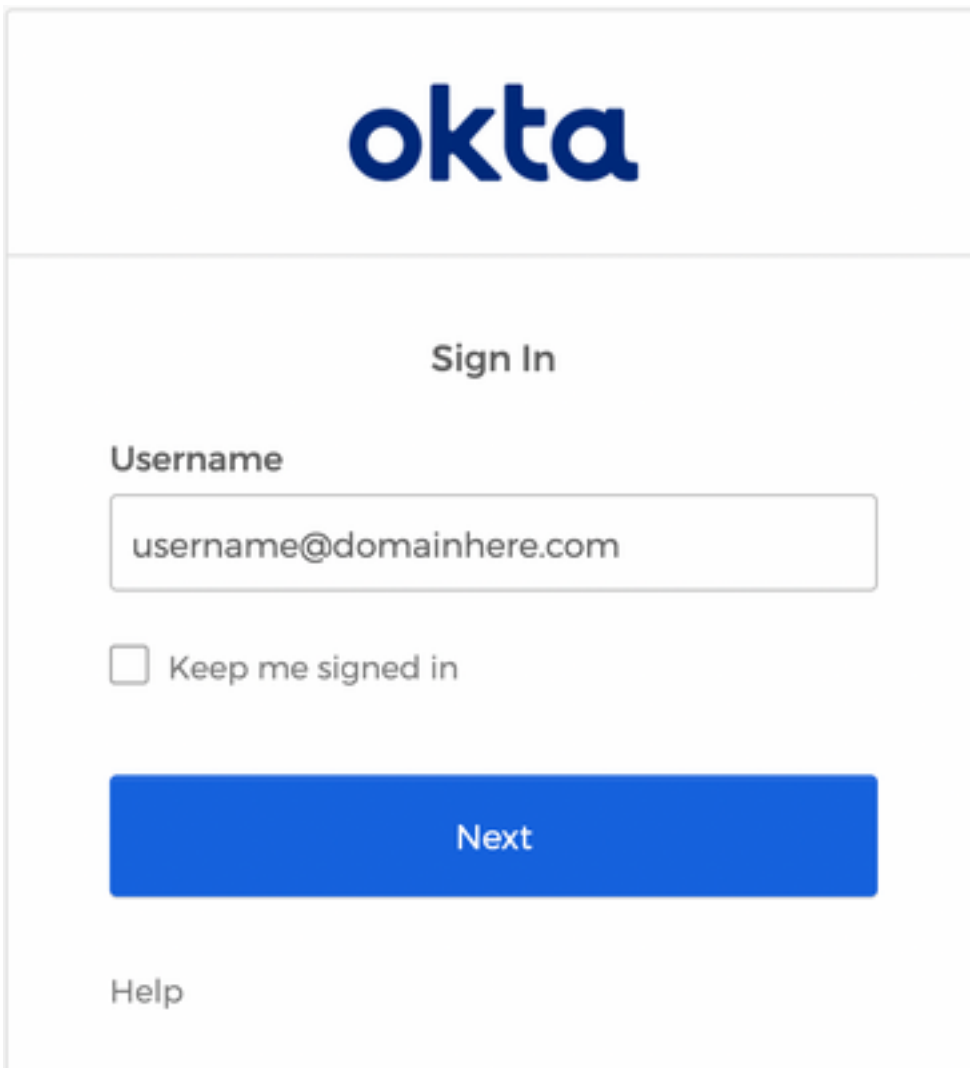
Username\*

Log In

OR

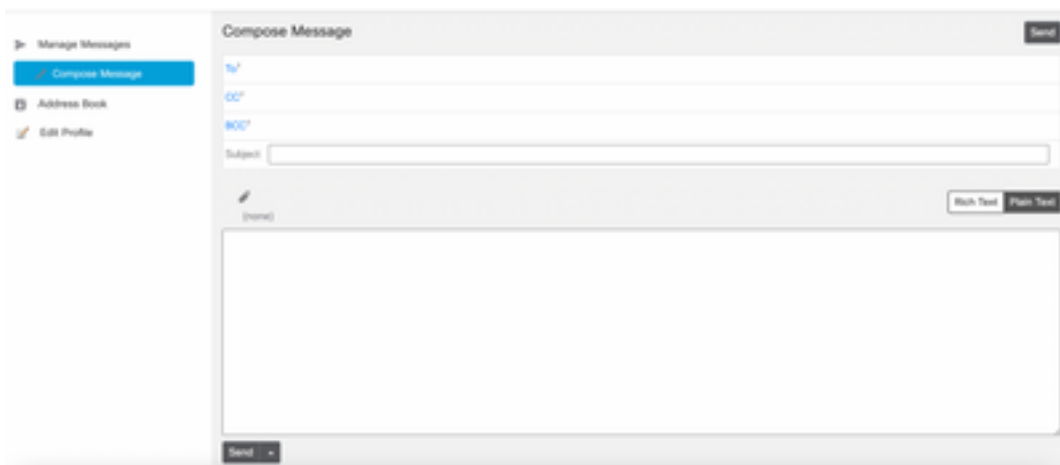
 Sign in with Google

2.打开一个新窗口，以使用OKTA凭证进行OKTA身份验证登录，如图所示：



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.如果身份验证成功，安全邮件加密服务会打开 Compose Message 窗口，如图所示：



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

现在，最终用户可以访问安全邮件加密服务门户，以撰写安全邮件或使用OKTA凭证打开新信封。

## 相关信息

[思科安全邮件加密服务6.2帐户管理员指南](#)

[思科安全网关最终用户指南](#)

[OKTA支持](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。