

# CRES用のOKTA SSO外部認証の設定

## 内容

[概要](#)

[前提条件](#)

[背景説明](#)

[要件](#)

[設定](#)

[確認](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco Secure Email Encryption Service(CES) (登録済みエンベロープ)へのログイン用にOKTA SSO外部認証を設定する方法について説明します。

## 前提条件

Cisco Secure Email Encryption Service (登録済みエンベロープ)への管理者アクセス。

OKTAへの管理者アクセス。

自己署名またはCA署名 (オプション) PKCS #12またはPEM形式のX.509 SSL証明書 (OKTAから提供)。

## 背景説明

- Cisco Secure Email Encryption Service(Registered Envelope)により、SAMLを使用するエンドユーザのSSOログインが可能になります。
- OKTAは、アプリケーションに認証および許可サービスを提供するアイデンティティマネージャです。
- Cisco Secure Email Encryption Service(Registered Envelope)は、OKTAに接続して認証と認可を行うアプリケーションとして設定できます。
- SAMLは、XMLベースのオープンな標準データ形式で、管理者はいずれかのアプリケーションにサインインした後、定義された一連のアプリケーションにシームレスにアクセスできます。
- SAMLの詳細については、「[SAMLの一般情報](#)」を参照してください。

## 要件

- Cisco Secure Email Encryption Service(Registered Envelope)管理者アカウント
- OKTA管理者アカウント。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリア (デフォルト) 設定で開始されています。ネ

ネットワークが稼働中の場合は、コマンドによる潜在的な影響を十分に理解しておく必要があります。

## 設定

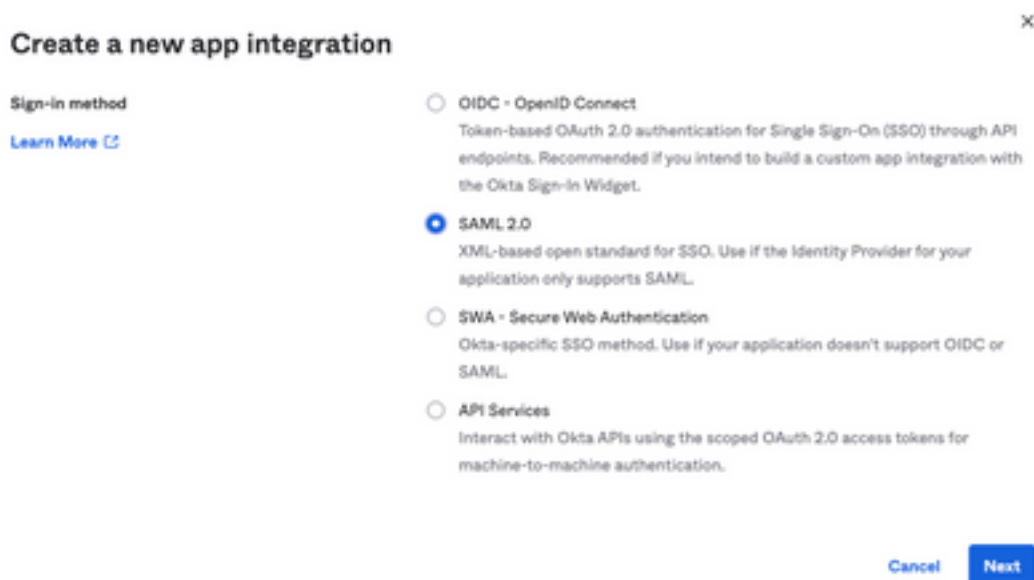
オクタの下で。

1. アプリケーションポータルに移動し、 Create App Integration ( 図を参照 )。

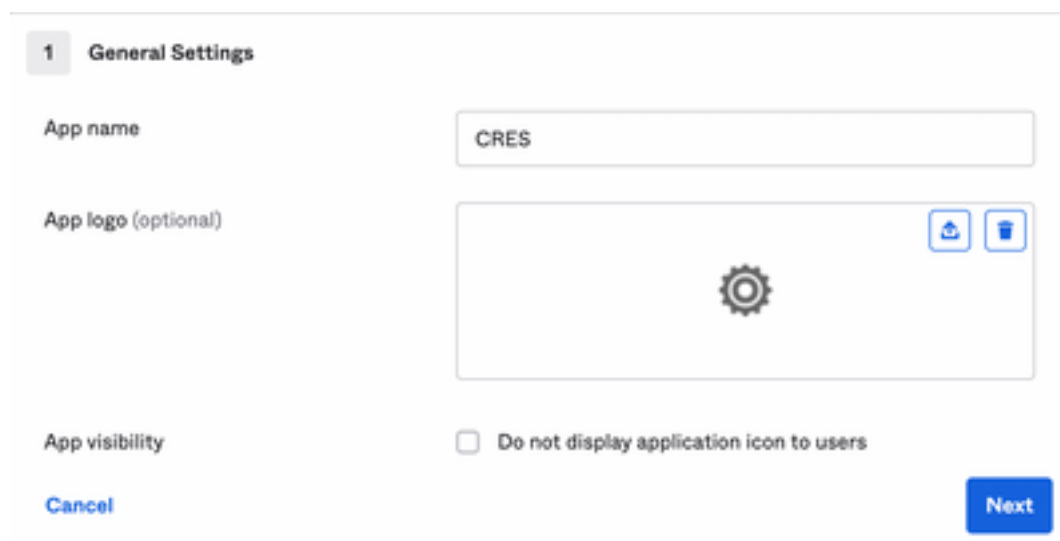
### Applications



2. 選択 SAML 2.0 をアプリケーションタイプとして使用します ( 図を参照 )。



3. アプリ名を入力します CRES を選択し、 Next ( 図を参照 )。



4. SAML settings をクリックして、図に示すようにギャップを埋めます。

- シングルサインオンURL：これは、Cisco Secure Email Encryption Serviceから取得したアサ  
ーションコンシューマサービスです。

- Audience URI(SP Entity ID)：これは、Cisco Secure Email Encryption Serviceから取得したエン  
ティティIDです。

- 名前IDの形式：未指定のままにしておきます。

- アプリケーションユーザ名：電子メール。認証プロセスで電子メールアドレスの入力を求め  
るプロンプトが表示されます。

- アプリケーションのユーザー名の更新：作成および更新。

---

**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](#)

下にスクロールして Group Attribute Statements (optional) ( 図を参照 )。

次の属性文を入力します。

-Name：group

- 名前の形式：Unspecified

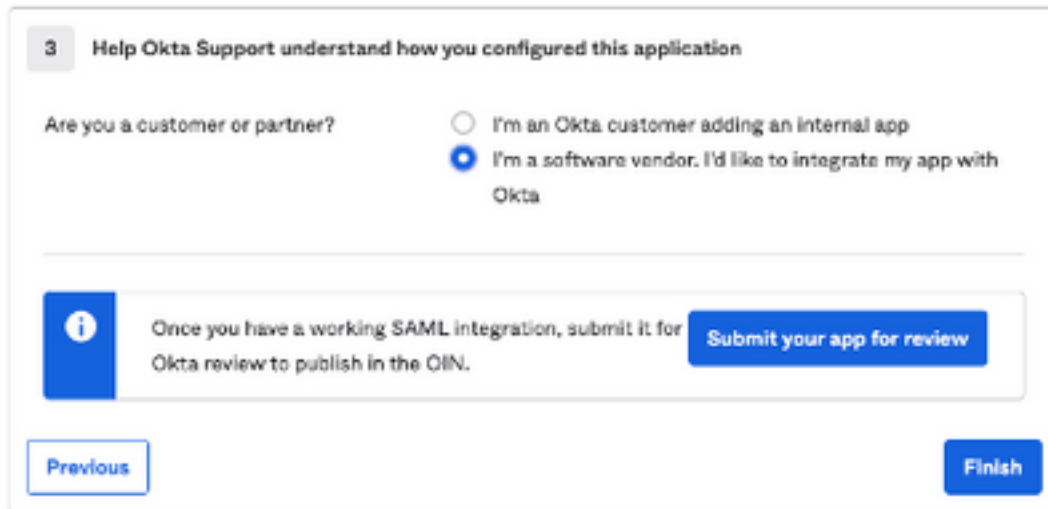
-フィルタ: Equals と OKTA

#### 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"/>

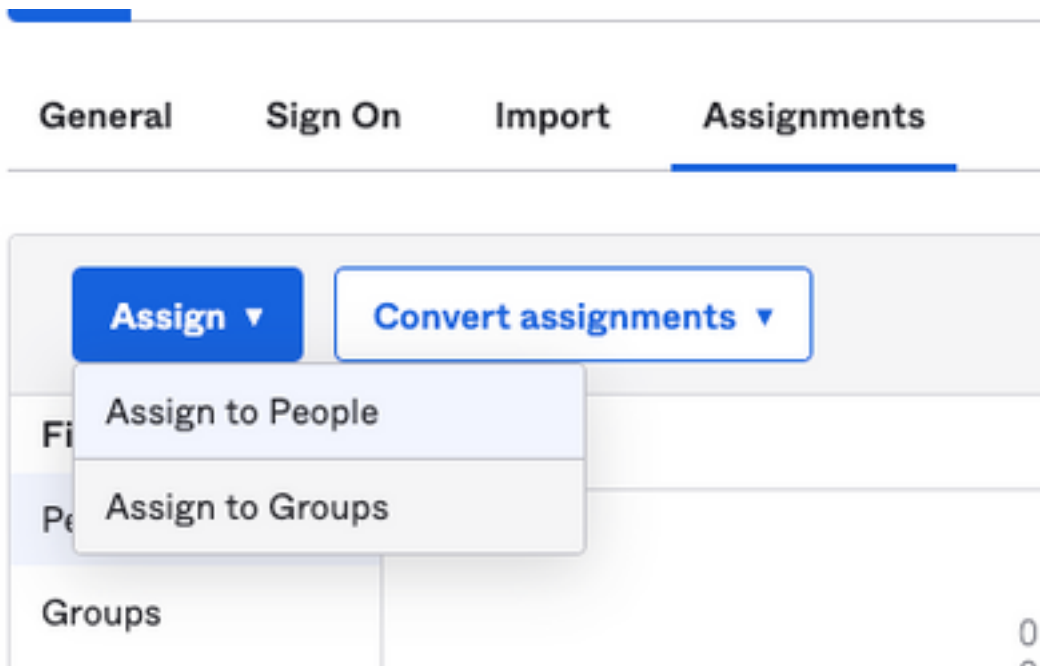
選択 Next .

5.依頼された場合 Help Okta to understand how you configured this application を選択した場合は、次の図に示すように、現在の環境に該当する理由を入力してください。



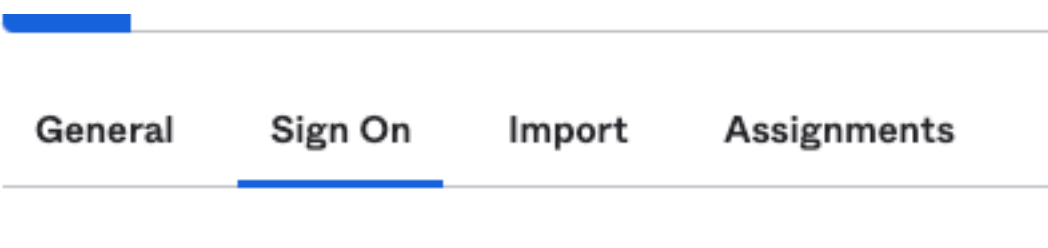
選択 Finish 次のステップに進みます。

6.選択 Assignments タブをクリックし、 Assign > Assign to Groups ( 図を参照 ) 。



7. OKTAグループを選択します。このグループは、環境にアクセスする権限を持つユーザーのグループです。

8.選択 Sign On ( 図を参照 ) 。



9.下にスクロールして右隅に移動し、 View SAML setup instructions オプションを選択します ( 図を参照 )。

## 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.メモ帳に次の情報を保存します。この情報は、 Cisco Secure Email Encryption Service 図に示すように、ポータルは次のようになります。

- アイデンティティプロバイダーのシングルサインオンURL
- アイデンティティプロバイダー発行者
- X.509証明書

## 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. OKTAの設定が完了したら、Cisco Secure Email Encryption Serviceに戻ることができます。

[Cisco Secure Email Encryption Service (Registered Envelope)]:

1. 管理者として組織ポータルにログインします。次の図に示すように、リンクは[CRES Administration Portal](#)です。

### Administration Console Log In

Welcome, please log in:

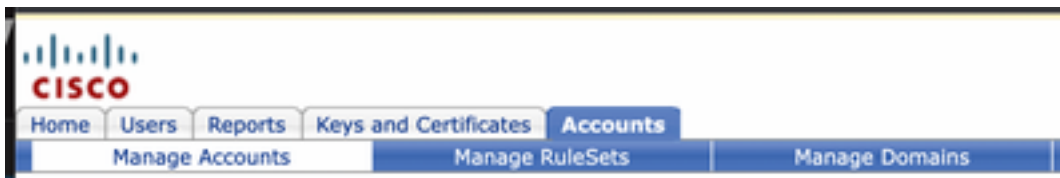
Username

Password

Remember me on this computer.

[Forgot password?](#)

2. Accounts タブをクリックし、 Manage Accounts タブをクリックします ( 図を参照 ) 。



3. アカウント番号をクリックし、Details タブをクリックします ( 図を参照 )。



4. スクロールダウンして、Authentication Method を選択し、SAML 2.0 ( 図を参照 )。

Authentication Method **SAML 2.0** ▾

5. SSO Alternate Email Attribute、図に示すように、空白のままにします。

SSO Alternate Email Attribute Name

6. SSO Service Provider Entity ID\*, <https://res.cisco.com/> ( 図を参照 )。

SSO Service Provider Entity ID\*

7. SSO Customer Service URL\*を入力し、Identity Provider Single Sign-On URL 次の図に示すように、Oktaから提供されます。

SSO Customer Service URL\*

8. SSO Logout URL、図に示すように、空白のままにします。

SSO Logout URL

9. SSO Identity Provider Verification Certificate OKTAから提供されたX.509証明書をアップロードします。

10. 選択 Save 図に示すように、設定を保存するには、次の手順を実行します。

Save

Back to Accounts List

11. 選択 **Activate SAML** 図に示すように、SAML認証プロセスを開始し、SSO認証を適用するには、次の手順を実行します。

Activate  
SAML

Save

Back to  
Accounts List

12. 新しいウィンドウが開き、SAML IDプロバイダーによる認証が成功した後にSAML認証がアクティブになることを通知します。選択 **Continue** ( 図を参照 )。

---

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

Continue

13. OKTAクレデンシャルで認証するための新しいウィンドウが開きます。次を入力します。  
Username を選択し、Next ( 図を参照 )。





## Sign In

Username

Keep me signed in

Next

Help

14. 認証プロセスが成功した場合、SAML Authentication Successful が表示されます。選択 Continue 図に示すように、このウィンドウを閉じるには、次の手順を実行します。

---

SAML Authentication Successful.

Please click continue to close.

Continue

15. 次を確認します。SSO Enable Date は、次の図に示すように、SAML認証が成功した日時に設定されます。

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の設定が完了しました。この時点で、CRES組織に属するユーザは、Eメールアドレスを入力する際にOKTAクレデンシャルを使用するようにリダイレクトされます。

## 確認

1. [Secure Email Encryption Service Portal] に移動します。図に示すように、CRESに登録されている電子メールアドレスを入力します。

# Secure Email Encryption Service

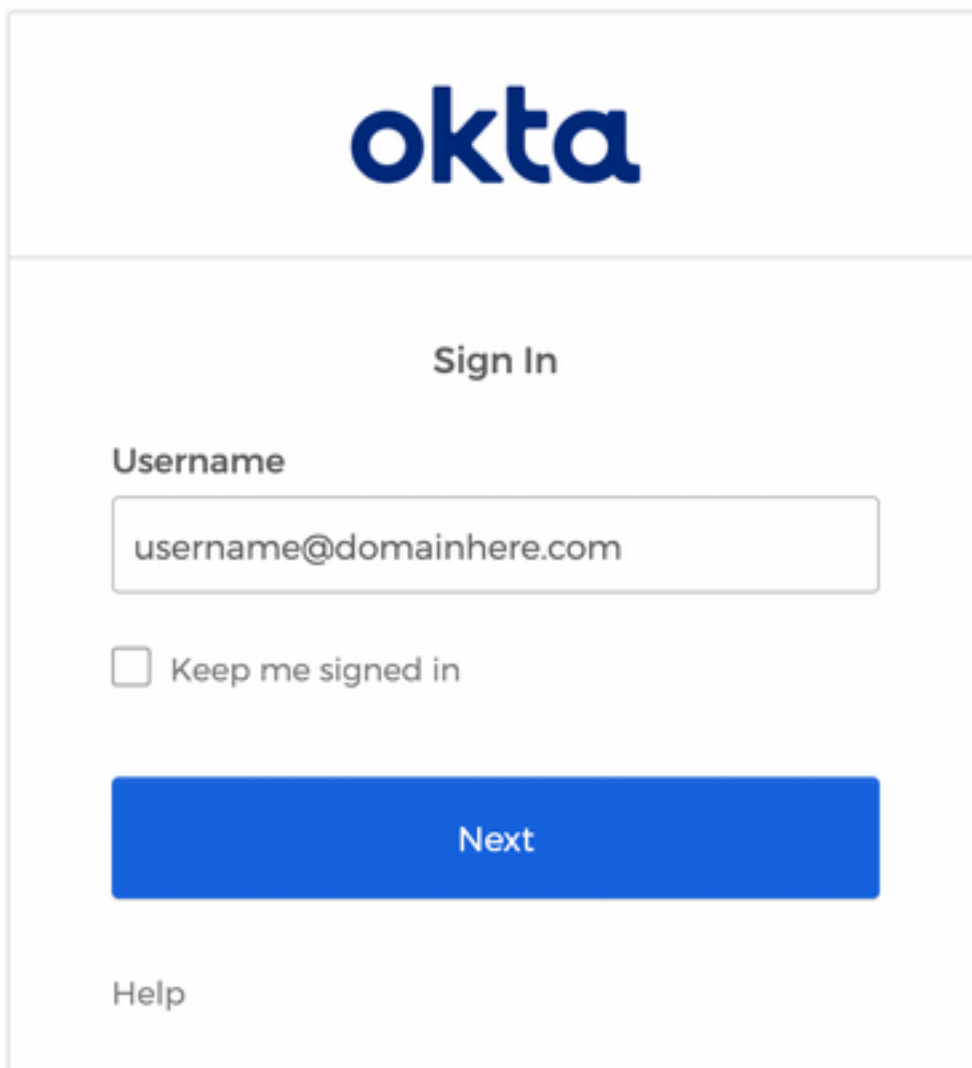
Username\*

Log In

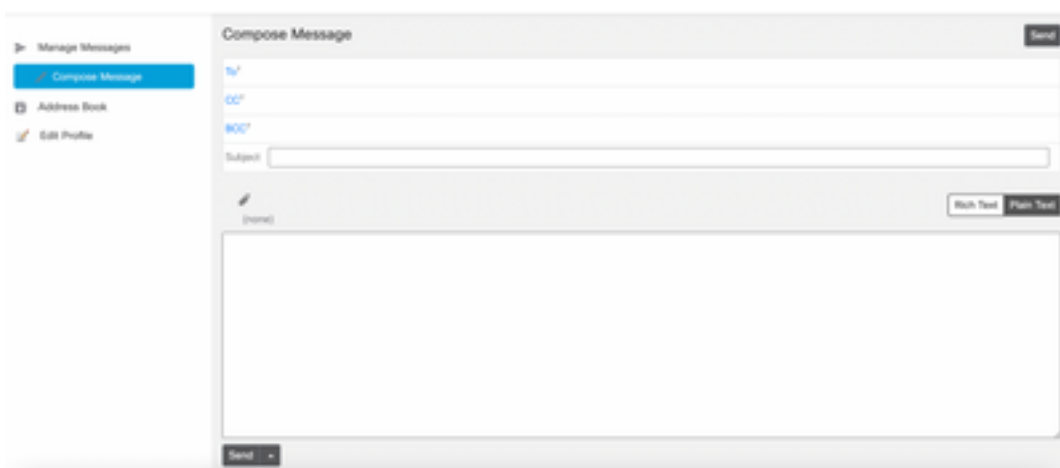
OR

 Sign in with Google

2.次の図に示すように、新しいウィンドウが開き、OKTA認証に進みます。OKTAクレデンシャルでサインインします。



3. 認証が成功すると、Secure Email Encryption Serviceによって Compose Message ウィンドウを開きます ( 次の図を参照 )。



これで、エンドユーザはSecure Email Encryption Serviceポータルにアクセスして、セキュアな電子メールを作成したり、OKTAクレデンシャルを使用して新しいエンベロップを開いたりできるようになります。

## 関連情報

[『Cisco Secure Email Encryption Service 6.2 Account Administrator Guide』](#)

[Cisco Secure Gatewayエンドユーザガイド](#)

[OKTAサポート](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。