

Configurar a autenticação externa OKTA SSO para CRES

Contents

[Introduction](#)

[Prerequisites](#)

[Informações de Apoio](#)

[Requirements](#)

[Configurar](#)

[Verificar](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar a Autenticação externa de SSO OKTA para fazer login no Cisco Secure Email Encryption Service (Envelope registrado).

Prerequisites

Acesso de administrador ao Cisco Secure Email Encryption Service (Envelope registrado).

Acesso de administrador ao OKTA.

Certificados SSL X.509 com assinatura automática ou CA (opcional) no formato PKCS #12 ou PEM (fornecido pelo OKTA).

Informações de Apoio

- O Cisco Secure Email Encryption Service (Envelope registrado) permite o login SSO para usuários finais que usam SAML.
- O OKTA é um gerenciador de identidades que fornece serviços de autenticação e autorização para seus aplicativos.
- O Cisco Secure Email Encryption Service (Registered Envelope) pode ser definido como um aplicativo conectado ao OKTA para autenticação e autorização.
- O SAML é um formato de dados padrão aberto baseado em XML que permite que os administradores acessem um conjunto definido de aplicativos perfeitamente após o login em um desses aplicativos.
- Para saber mais sobre SAML, consulte: [Informações Gerais de SAML](#)

Requirements

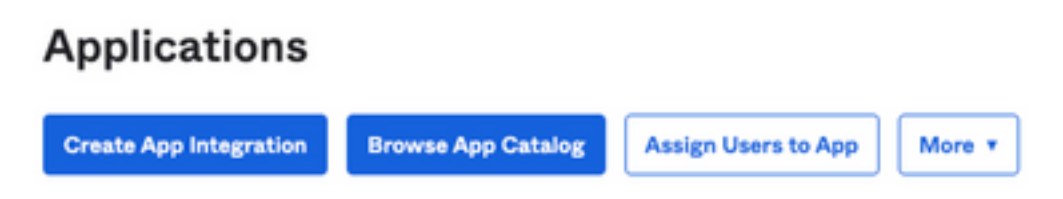
- Conta de administrador do Cisco Secure Email Encryption Service (Registered Envelope).
- Conta de administrador OKTA.

The information in this document was created from the devices in a specific lab environment. Todos os dispositivos usados neste documento foram iniciados com uma configuração limpa (padrão). se a rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando.

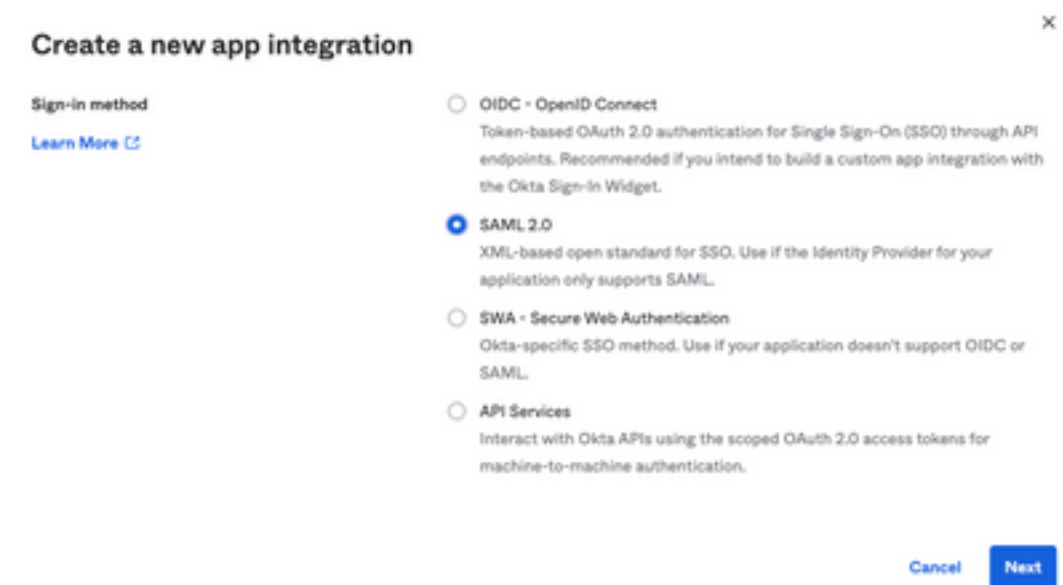
Configurar

Sob Okta.

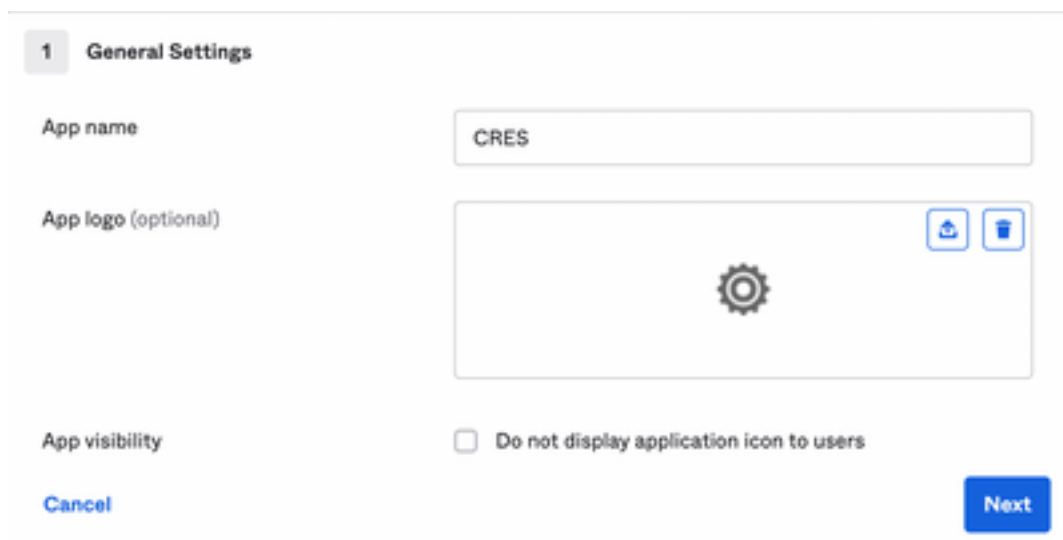
1. Navegue até o portal Aplicativos e selecione **Create App Integration**, conforme mostrado na imagem:



2. Selecione **SAML 2.0** como o tipo de aplicativo, conforme mostrado na imagem:



3. Informe o nome do Aplicativo **CRES** e selecione **Next**, conforme mostrado na imagem:



4. Nos termos do SAML settings, preencha as lacunas, conforme mostrado na imagem:

- URL de logon único: este é o Assertion Consumer Service obtido do Cisco Secure Email Encryption Service.

- URI do público (ID da entidade SP): é a ID da entidade obtida do Cisco Secure Email Encryption Service.


- Formato de ID do nome: mantenha-o como Não especificado.


- Nome de usuário do aplicativo: e-mail que solicita que o usuário insira seu endereço de e-mail no processo de autenticação.


- Atualizar nome de usuário do aplicativo em: Criar e Atualizar.


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](#)

Role para baixo até Group Attribute Statements (optional), conforme mostrado na imagem:

Insira a próxima instrução de atributo:

-Nome: group

- Formato do nome: Unspecified

-Filtro: Equals e OKTA

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
group	Unspecified ▾	Equals ▾ OKTA

Selecionar Next .

5. Quando solicitado a Help Okta to understand how you configured this application, insira o motivo aplicável para o ambiente atual, como mostrado na imagem:

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

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

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

Selecionar Finish para prosseguir para a próxima etapa.

6. Selecione Assignments e selecione Assign > Assign to Groups, conforme mostrado na imagem:

General **Sign On** **Import** **Assignments**

Assign ▾ **Convert assignments ▾**

- Assign to People
- Assign to Groups

Groups

7. Selecione o grupo OKTA, que é o grupo com os usuários autorizados a acessar o ambiente.

8. Selecione Sign On, conforme mostrado na imagem:

General

Sign On

Import

Assignments

9. Role para baixo e, para o canto direito, selecione a *View SAML setup instructions* , como mostrado na imagem:

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. Salve em um bloco de notas as próximas informações, que são necessárias para colocar no Cisco Secure Email Encryption Service como mostrado na imagem:

- URL de Logon Único do Provedor de Identidade
- Emissor do provedor de identidade
- Certificado X.509

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. Depois de concluir a configuração do OKTA, você pode voltar para o Cisco Secure Email Encryption Service.

No Cisco Secure Email Encryption Service (Envelope registrado):

1. Faça login no portal da sua organização como administrador, o link é: [Portal de administração do CRES](#), como mostrado na imagem:



Administration Console Log In

Welcome, please log in:

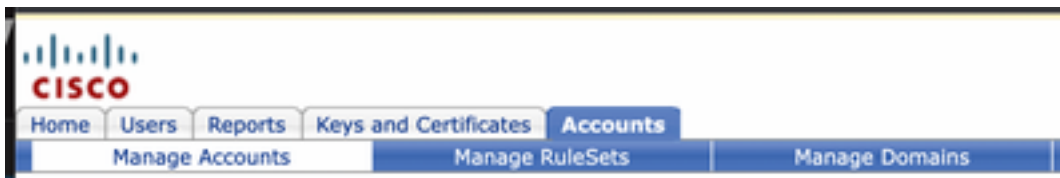
Username

Password

Remember me on this computer.

[Forgot password?](#) [Log In](#)

2. No Accounts selecione a guia Manage Accounts , como mostrado na imagem:



3. Clique em um Número de Conta e selecione o Details , como mostrado na imagem:



4. Role para baixo até Authentication Method e selecione SAML 2.0, conforme mostrado na imagem:

Authentication Method **SAML 2.0** ▾

5. Para efeitos da SSO Alternate Email Attribute, deixe-o em branco, como mostrado na imagem:

SSO Alternate Email Attribute Name

6. Para efeitos da SSO Service Provider Entity ID*, enter <https://res.cisco.com/> , conforme mostrado na imagem:

SSO Service Provider Entity ID*

7. Para efeitos da SSO Customer Service URL*, digite o Identity Provider Single Sign-On URL fornecido pela Okta, como mostrado na imagem:

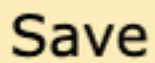
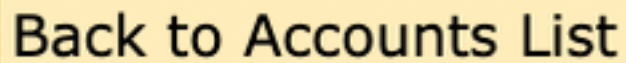
SSO Customer Service URL*

8. Para efeitos da SSO Logout URL, deixe-o em branco, como mostrado na imagem:


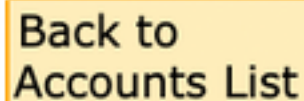
SSO Logout URL

9. Para efeitos da SSO Identity Provider Verification Certificate, carregue o Certificado X.509 fornecido pelo OKTA.

10. Selecione save para salvar as configurações, como mostrado na imagem:

A rectangular button with a yellow background and a thin orange border, containing the text "Save" in black.A rectangular button with a yellow background and a thin orange border, containing the text "Back to Accounts List" in black.

11. Selecione **Activate SAML** para iniciar o processo de autenticação SAML e aplicar a autenticação SSO, como mostrado na imagem:

A rectangular button with a yellow background and a thin orange border, containing the text "Activate SAML" in black.A rectangular button with a yellow background and a thin orange border, containing the text "Save" in black.A rectangular button with a yellow background and a thin orange border, containing the text "Back to Accounts List" in black.

12. Uma nova janela é aberta para informar que a autenticação SAML se torna ativa após a autenticação bem-sucedida com o Provedor de Identidade SAML. Selecionar **Continue**, conforme mostrado na imagem:

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

A small rectangular button with a yellow background and a thin orange border, containing the text "Continue" in black.

13. Uma nova janela é aberta para autenticar com Credenciais OKTA. Digite o Username e selecione **Next**, conforme mostrado na imagem:



Sign In

Username

Keep me signed in

Next

Help

14. Se o processo de autenticação for bem-sucedido, o SAML Authentication Successful é exibido. Selecionar **Continue** para fechar esta janela, como mostrado na imagem:

SAML Authentication Successful.

Please click continue to close.

Continue

15. Confirme a SSO Enable Date está definido como a data e a hora em que a Autenticação SAML foi bem-sucedida, conforme mostrado na imagem:

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	Download
SSO Binding	HTTP-Redirect, HTTP-POST
SSO Assertion Consumer URL	https://res.cisco.com/websafe/ssourl
Current Certificate	

A configuração SAML foi concluída. A partir deste momento, os usuários que pertencem à organização do CRES são redirecionados para usar suas credenciais OKTA quando inserirem seu endereço de e-mail.

Verificar

1. Navegue até [Secure Email Encryption Service Portal](#). Insira o endereço de e-mail registrado no CRES, como mostrado na imagem:

Secure Email Encryption Service

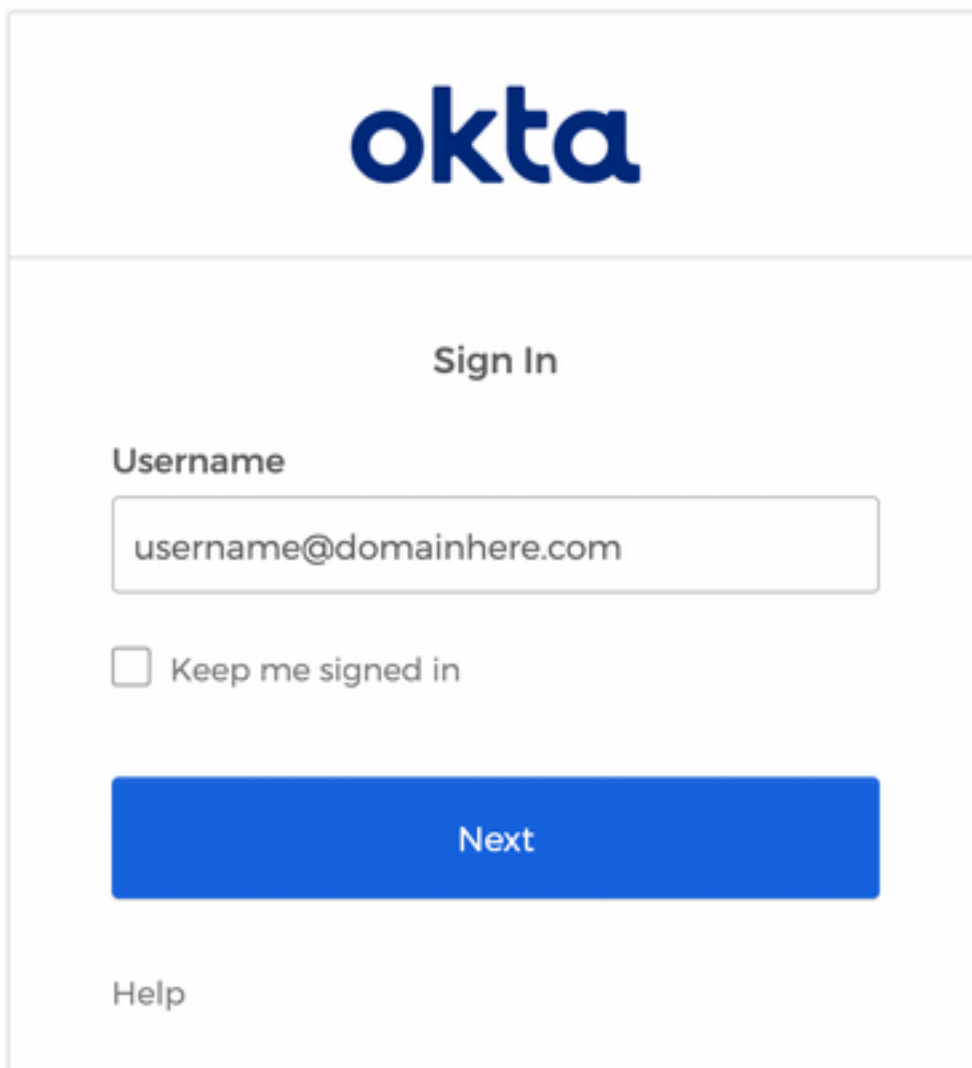
Username*

Log In

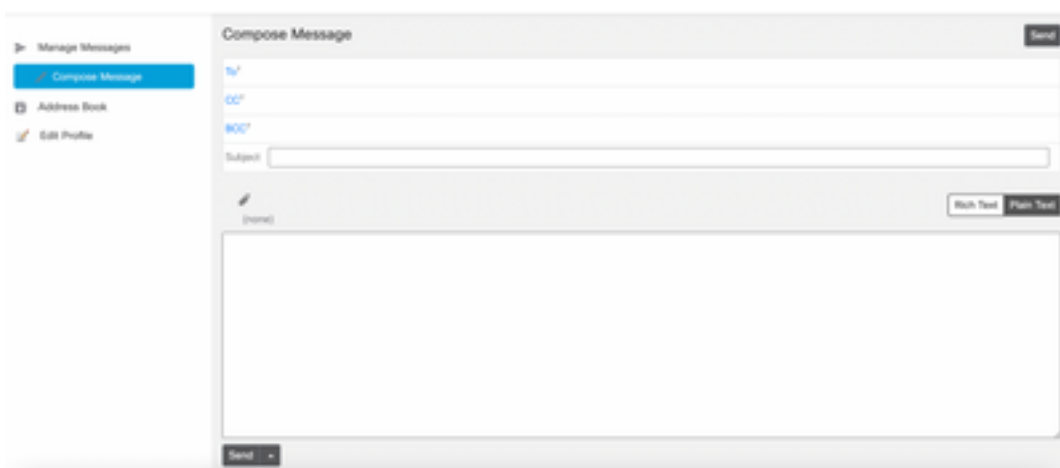
OR

 Sign in with Google

2. Uma nova janela é aberta para continuar com a autenticação OKTA. Entre com as **credenciais OKTA**, conforme mostrado na imagem:



3. Se a Autenticação for bem-sucedida, o Serviço de Criptografia Segura de E-mail abrirá a Compose Message como mostrado na imagem:



Agora, o usuário final pode acessar o portal Secure Email Encryption Service para redigir e-mails seguros ou abrir novos envelopes com credenciais OKTA.

Informações Relacionadas

[Guia do administrador de contas do Cisco Secure Email Encryption Service 6.2](#)

[Guias do Usuário Final do Cisco Secure Gateway](#)

[Suporte a OKTA](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.