

Configuración de la Autenticación Externa SSO de OKTA para CRES

Contenido

[Introducción](#)

[Prerequisites](#)

[Antecedentes](#)

[Requirements](#)

[Configurar](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la autenticación externa SSO de OKTA para iniciar sesión en el Servicio de cifrado de correo electrónico seguro de Cisco (sobre registrado).

Prerequisites

Acceso de administrador al servicio Cisco Secure Email Encryption (sobre registrado).

Acceso de administrador a OKTA.

Certificados SSL X.509 autofirmados o firmados por CA (opcional) en formato PKCS #12 o PEM (proporcionados por OKTA).

Antecedentes

- Cisco Secure Email Encryption Service (sobre registrado) permite el inicio de sesión SSO para los usuarios finales que utilizan SAML.
- OKTA es un gestor de identidades que proporciona servicios de autenticación y autorización a sus aplicaciones.
- Cisco Secure Email Encryption Service (Registered Envelope) se puede establecer como una aplicación conectada a OKTA para la autenticación y autorización.
- SAML es un formato de datos estándar abierto basado en XML que permite a los administradores acceder a un conjunto definido de aplicaciones sin problemas después de iniciar sesión en una de esas aplicaciones.
- Para obtener más información sobre SAML, consulte: [Información general sobre SAML](#)

Requirements

- Cuenta de administrador del Servicio de cifrado de correo electrónico seguro de Cisco (sobre registrado).

- Cuenta de administrador OKTA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos utilizados en este documento se iniciaron con una configuración desactivada (predeterminada). si la red está activa, asegúrese de comprender el impacto potencial de cualquier comando.

Configurar

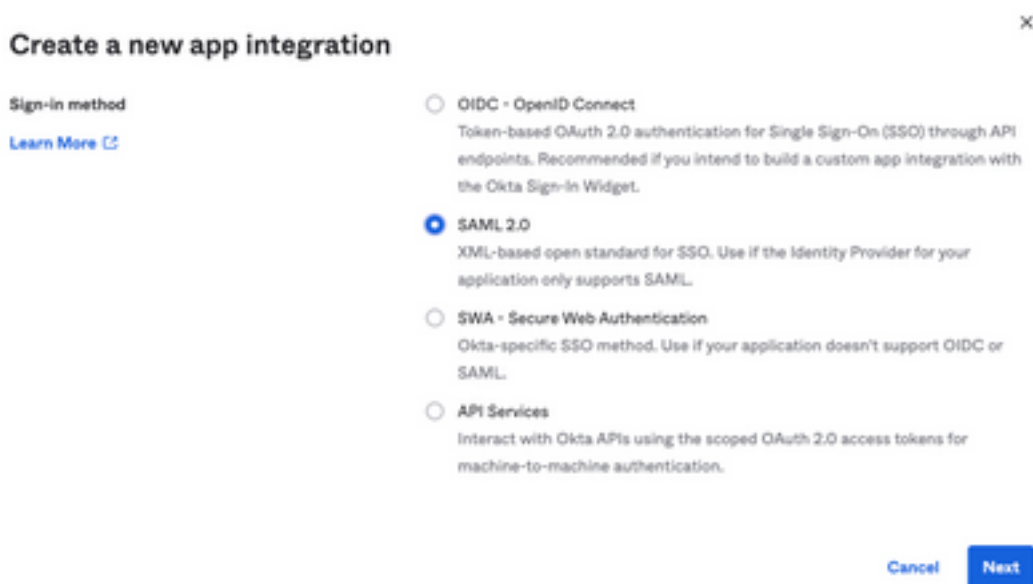
Bajo Okta.

1. Acceda al portal de aplicaciones y seleccione Create App Integration, como se muestra en la imagen:

Applications




2. Seleccione SAML 2.0 como tipo de aplicación, como se muestra en la imagen:



3. Introduzca el nombre de la aplicación CRES y seleccione Next, como se muestra en la imagen:

1 General Settings

App name

App logo (optional) 

App visibility Do not display application icon to users


[Cancel](#) [Next](#)


4. En virtud del SAML settings, rellene los espacios, como se muestra en la imagen:


- URL de inicio de sesión único: se trata del servicio de consumidor de aserción que se obtiene del servicio Cisco Secure Email Encryption.
- URI de destinatario (ID de entidad SP): es la ID de entidad obtenida del servicio Cisco Secure Email Encryption.
- Formato de ID de nombre: mantenerlo como Sin especificar.
- Nombre de usuario de la aplicación: Correo electrónico que solicita al usuario que introduzca su dirección de correo electrónico en el proceso de autenticación.
- Actualizar nombre de usuario de aplicación en: Crear y actualizar.


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](#)

Desplácese hasta **Group Attribute Statements (optional)**, como se muestra en la imagen:

Introduzca la siguiente sentencia de atributo:

- Nombre: group
- Formato del nombre: Unspecified
- Filtro: Equals y OKTA

Group Attribute Statements (optional)

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

Seleccionar **Next** .

5. Cuando se le solicite **Help Okta to understand how you configured this application**, introduzca el motivo aplicable al entorno actual, como se muestra en la imagen:

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

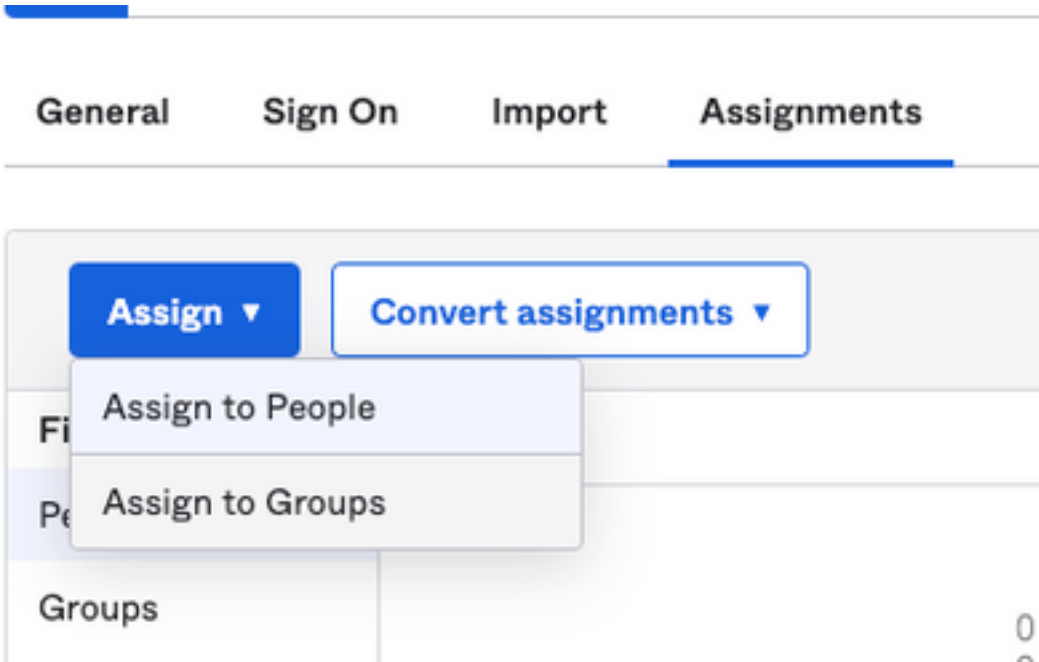
I'm a software vendor. I'd like to integrate my app with Okta

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**

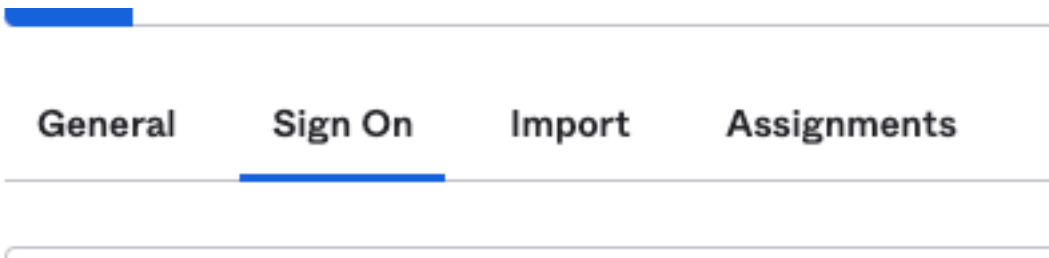
Seleccionar **Finish** para continuar con el paso siguiente.

6. Seleccione **Assignments** y, a continuación, seleccione **Assign > Assign to Groups**, como se muestra en la imagen:



7. Seleccione el grupo OKTA, que es el grupo con los usuarios autorizados para acceder al entorno.

8. Seleccione Sign On, como se muestra en la imagen:



9. Desplácese hacia abajo y a la esquina derecha, seleccione el View SAML setup instructions , como se muestra en la imagen:

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. Guarde en un bloc de notas la siguiente información, que es necesaria para poner en el Cisco Secure Email Encryption Service portal, como se muestra en la imagen:

- URL de inicio de sesión único del proveedor de identidad

- Emisor del proveedor de identidad

- 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-----

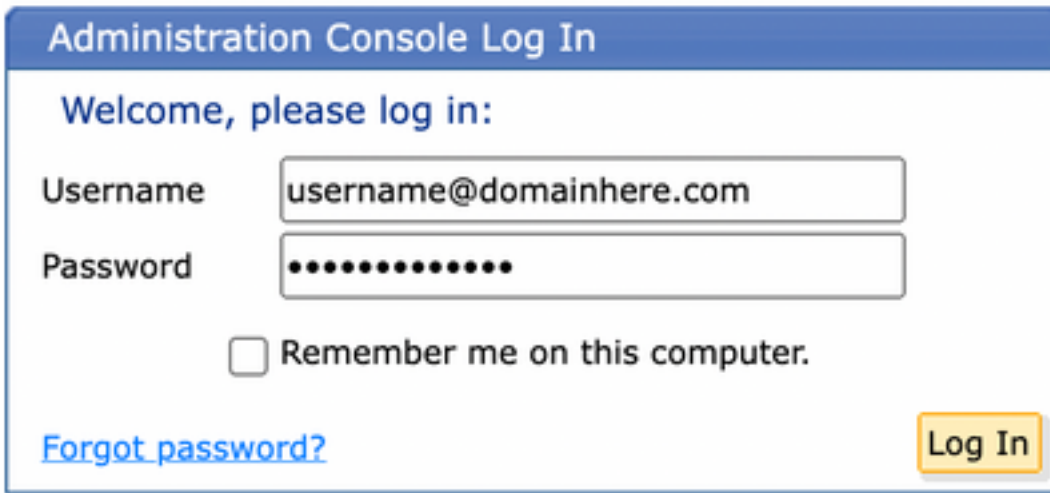
-----END CERTIFICATE-----

[Download certificate](#)

11. Una vez completada la configuración de OKTA, puede volver al servicio Cisco Secure Email Encryption.

En Cisco Secure Email Encryption Service (Sobre Registrado):

1. Inicie sesión en el portal de su organización como administrador. El enlace es: [Portal de administración de CRES](#), como se muestra en la imagen:



Administration Console Log In

Welcome, please log in:

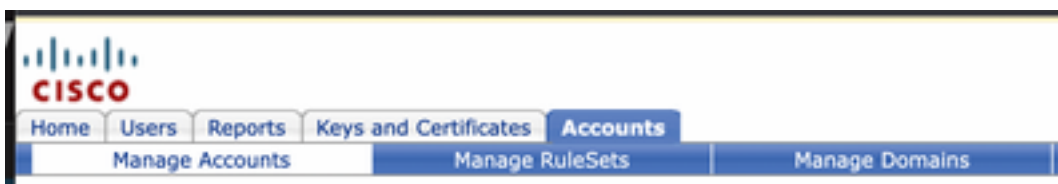
Username

Password

Remember me on this computer.

[Forgot password?](#)

2. En el Accounts seleccione la ficha Manage Accounts , como se muestra en la imagen:



3. Haga clic en un número de cuenta y seleccione el Details , como se muestra en la imagen:



4. Desplácese hasta Authentication Method y seleccione SAML 2.0, como se muestra en la imagen:

Authentication Method

5. Para el SSO Alternate Email Attribute, déjelo en blanco, como se muestra en la imagen:

SSO Alternate Email Attribute Name

6. Para el SSO Service Provider Entity ID*, ingrese <https://res.cisco.com/> , como se muestra en la imagen:

SSO Service Provider Entity ID*

7. Para el SSO Customer Service URL*, escriba el Identity Provider Single Sign-On URL proporcionada por Okta, como se muestra en la imagen:

SSO Customer Service
URL*

https:// .okta.com/app/

8. Para el SSO Logout URL, déjelo en blanco, como se muestra en la imagen:

SSO Logout URL

9. Para el SSO Identity Provider Verification Certificate, cargue el certificado X.509 proporcionado por OKTA.

10. Seleccione **save** para guardar la configuración, como se muestra en la imagen:

Save

Back to Accounts List

11. Seleccione **Activate SAML** para iniciar el proceso de autenticación SAML y aplicar la autenticación SSO, como se muestra en la imagen:

**Activate
SAML**

Save

**Back to
Accounts List**

12. Se abre una nueva ventana para informar que la autenticación SAML se activa después de una autenticación exitosa con el proveedor de identidad SAML. Seleccionar **Continue**, como se muestra en la imagen:

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

Continue

13. Se abre una nueva ventana para autenticar con credenciales OKTA. Escriba el **Username** y seleccione **Next**, como se muestra en la imagen:



Sign In

Username

Keep me signed in

Next

Help

14. Si el proceso de autenticación se realiza correctamente, el SAML Authentication Successful se muestra. Seleccionar Continue para cerrar esta ventana, como se muestra en la imagen:

SAML Authentication Successful.

Please click continue to close.

Continue

15. Confirme el SSO Enable Date se establece en la fecha y hora en que la autenticación SAML fue exitosa, como se muestra en la imagen:

Authentication Method	<input type="text" value="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	<input type="button" value="Download"/>
SSO Binding	HTTP-Redirect, HTTP-POST
SSO Assertion Consumer URL	https://res.cisco.com/websafe/ssourl
Current Certificate	

La configuración de SAML se ha completado. A partir de este momento, los usuarios que pertenecen a la organización de CRES son redirigidos a usar sus credenciales de OKTA cuando ingresan su dirección de correo electrónico.

Verificación

1. Acceda al [portal del servicio de cifrado de correo electrónico seguro](#). Introduzca la dirección de correo electrónico registrada en CRES, como se muestra en la imagen:

Secure Email Encryption Service

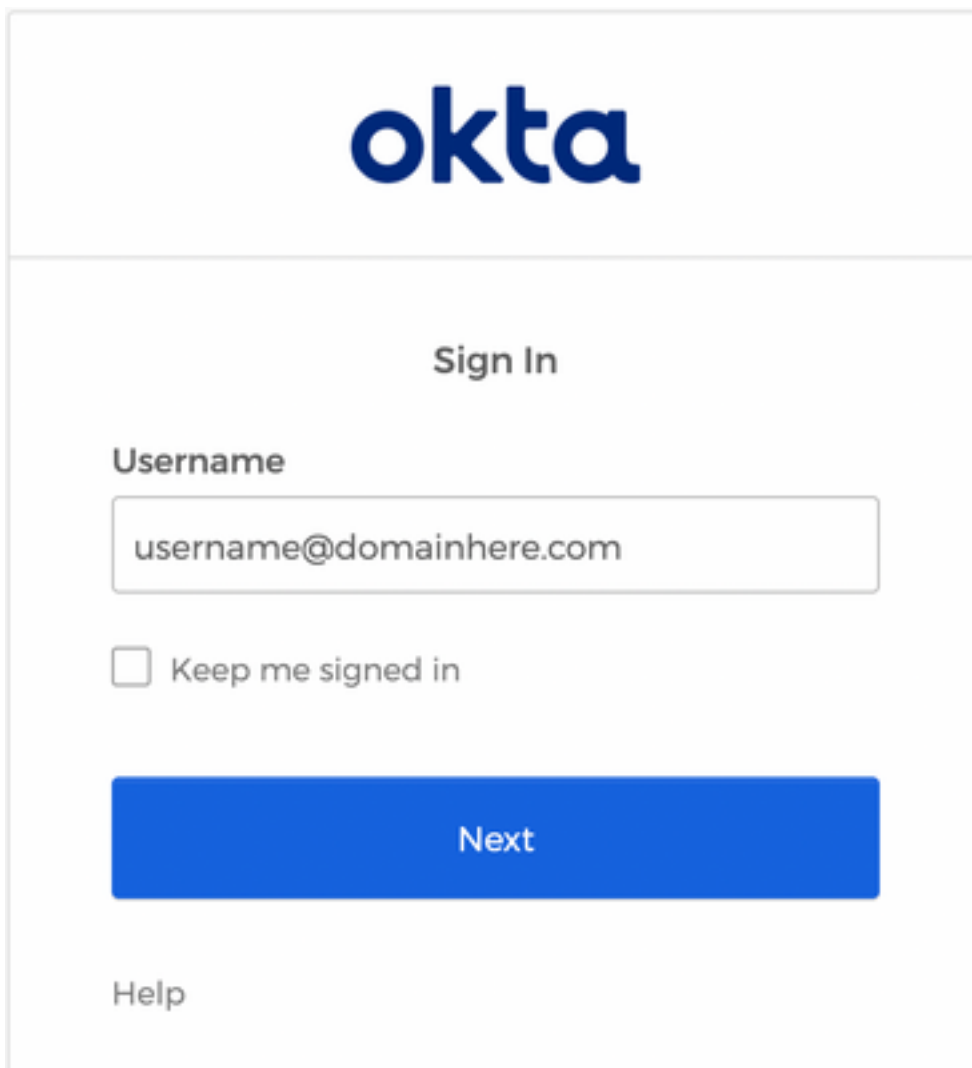
Username*

Log In

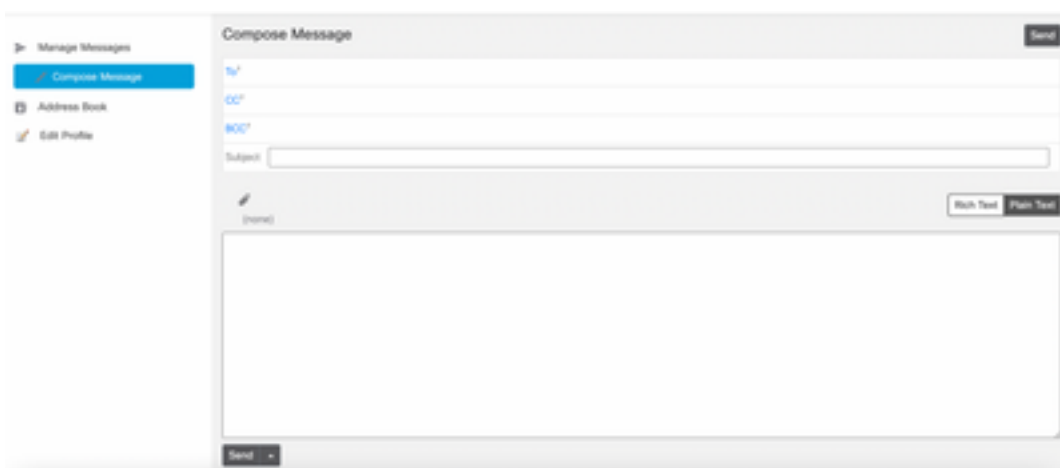
OR

 Sign in with Google

2. Se abre una nueva ventana para continuar con la autenticación de OKTA Iniciar sesión con las **credenciales de OKTA**, como se muestra en la imagen:



3. Si la autenticación se realiza correctamente, el servicio de cifrado de correo electrónico seguro abre el Compose Message , como se muestra en la imagen:



Ahora el usuario final puede acceder al portal del Servicio de cifrado de correo electrónico seguro para redactar correos electrónicos seguros o abrir nuevos sobres con credenciales de OKTA.

Información Relacionada

[Guía para administradores de cuentas de Cisco Secure Email Encryption Service 6.2](#)

[Guías de usuario final de Cisco Secure Gateway](#)

[Asistencia para OKTA](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).