

Configure OKTA SSO External Authentication for CRES

Contents

[Introduction](#)

[Prerequisites](#)

[Background Information](#)

[Requirements](#)

[Configure](#)

[Verify](#)

[Related Information](#)

Introduction

This document describes how to configure OKTA SSO External Authentication for login to Cisco Secure Email Encryption Service (Registered Envelope).

Prerequisites

Administrator access to Cisco Secure Email Encryption Service (Registered Envelope).

Administrator access to OKTA.

Self-Signed or CA Signed (optional) X.509 SSL certificates in PKCS #12 or PEM format (provided by OKTA).

Background Information

- Cisco Secure Email Encryption Service (Registered Envelope) enables SSO login for end users who use SAML.
- OKTA is an identity manager that provides authentication and authorization services to your applications.
- Cisco Secure Email Encryption Service (Registered Envelope) can be set as an application which is connected to OKTA for authentication and authorization.
- SAML is an XML-based open standard data format that enables administrators to access a defined set of applications seamlessly after the sign into one of those applications.
- To learn more about SAML, refer to: [SAML General Information](#)

Requirements

- Cisco Secure Email Encryption Service (Registered Envelope) administrator account.
- OKTA administrator account.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. if the network is live, ensure that you understand the potential impact of any command.

Configure

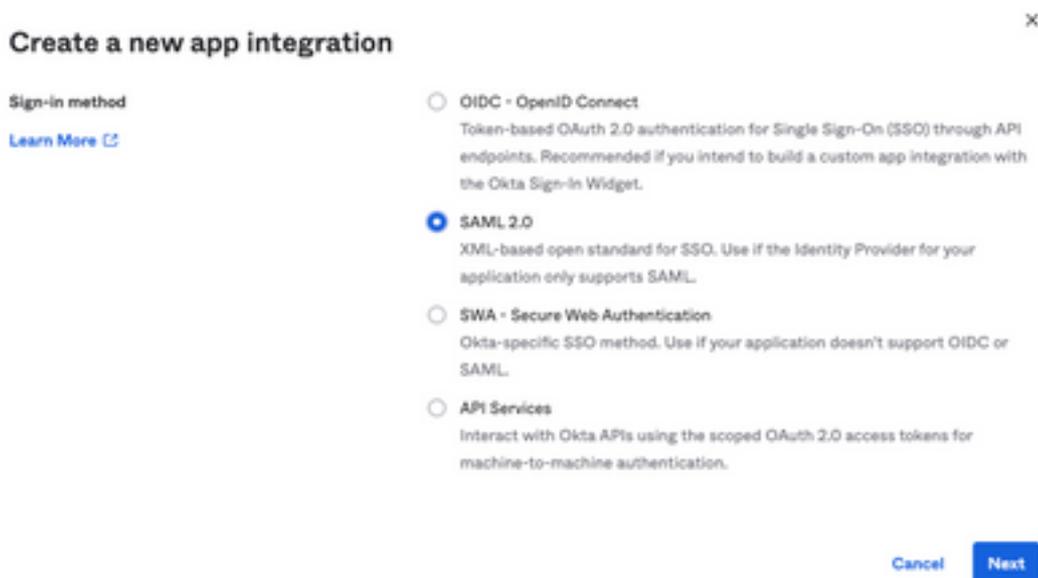
Under Okta.

1. Navigate to Applications portal and select Create App Integration, as shown in the image:

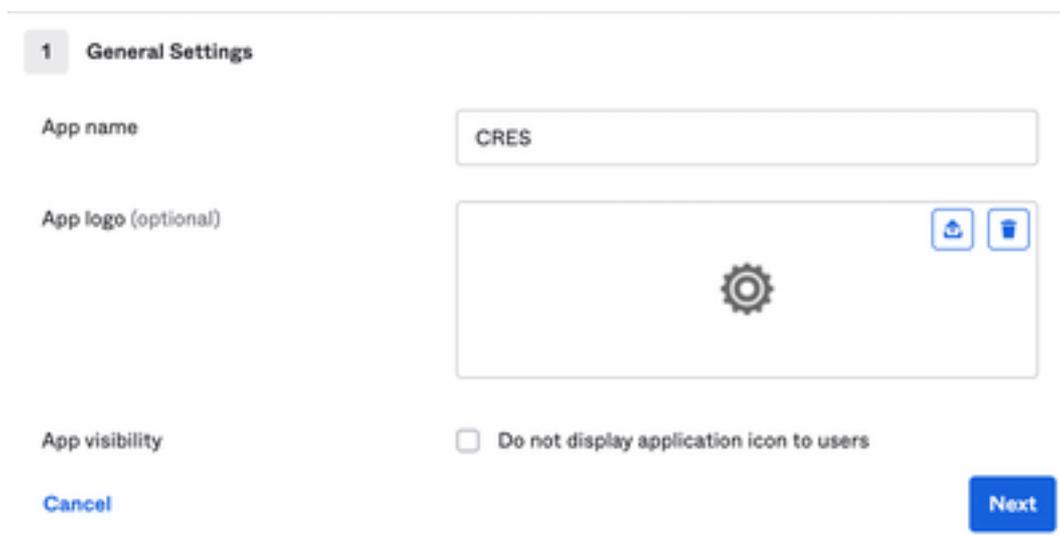
Applications



2. Select SAML 2.0 as the application type, as shown in the image:



3. Enter the App name CRES and select Next, as shown in the image:



4. Under the SAML settings, fill in the gaps, as shown in the image:

- Single sign on URL: This is the Assertion Consumer Service obtained from the Cisco Secure Email Encryption Service.

- Audience URI (SP Entity ID): This is the Entity ID obtained from the Cisco Secure Email Encryption Service.

- Name ID format: keep it as Unspecified.

- Application username: Email, that prompts user to enter their Email address in the authentication process.

- Update application username on: Create and Update.

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](#)

Scroll down to Group Attribute Statements (optional), as shown in the image:

Enter the next attribute statement:

- Name: group
- Name format: Unspecified
- Filter: Equals and 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"/>

Select Next .

5. When asked to Help Okta to understand how you configured this application, please enter the applicable reason to the current environment, as shown in the image:

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

Select Finish to proceed to the next step.

6. Select Assignments tab and then select Assign > Assign to Groups, as shown in the image:

General Sign On Import Assignments

Assign Convert assignments

Assign to People

Assign to Groups

Groups

7. Select the OKTA group, which is the group with the authorized users to access the environment.

8. Select Sign On, as shown in the image:

General Sign On Import Assignments

9. Scroll down and to the right corner, select the [View SAML setup instructions](#) option, as shown in the image:

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. Save to a notepad the next information, that is necessary to put into the [Cisco Secure Email Encryption Service](#) portal, as shown in the image:

- Identity Provider Single Sign-On URL
- Identity Provider Issuer
- X.509 Certificate

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. Once you complete the OKTA configuration, you can go back to the Cisco Secure Email Encryption Service.

Under Cisco Secure Email Encryption Service (Registered Envelope) :

1. Log in to your organization portal as an administrator, the link is: [CRES Administration Portal](#), as shown in the image:



Administration Console Log In

Welcome, please log in:

Username

Password

Remember me on this computer.

[Forgot password?](#)

2. On the Accounts tab, select the Manage Accounts tab, as shown in the image:



3. Click an Account Number and select the **Details** tab, as shown in the image:



4. Scroll down to **Authentication Method** and select **SAML 2.0**, as shown in the image:



5. For the **SSO Alternate Email Attribute Name**, leave it blank, as shown in the image:

SSO Alternate Email Attribute Name

6. For the **SSO Service Provider Entity ID***, enter <https://res.cisco.com/>, as shown in the image:

SSO Service Provider Entity ID*

7. For the **SSO Customer Service URL***, enter the Identity Provider Single Sign-On URL provided by Okta, as shown in the image:

SSO Customer Service URL*

8. For the **SSO Logout URL**, leave it blank, as shown in the image:

SSO Logout URL

9. For the **SSO Identity Provider Verification Certificate**, upload the X.509 Certificate provided by OKTA.

10. Select **save** to save settings, as shown in the image:

Save

Back to Accounts List

11. Select `Activate SAML` to start the SAML authentication process and enforce SSO authentication, as shown in the image:

Activate
SAML

Save

Back to
Accounts List

12. A new window opens to inform SAML authentication becomes active after successful authentication with the SAML Identity Provider. Select `Continue`, as shown in the image:

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

Continue

13. A new window opens to authenticate with OKTA Credentials. Enter the `Username` and select `Next`, as shown in the image:



Sign In

Username

Keep me signed in

Next

Help

14. If the Authentication process is successful, the SAML Authentication Successful is displayed. Select Continue to close this window, as shown in the image:

SAML Authentication Successful.

Please click continue to close.

Continue

15. Confirm the SSO Enable Date is set to the date and time the SAML Authentication was successful, as shown in the image:

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	

The SAML configuration is completed. As of this moment, users who belong to the CRES organization are redirected to use their OKTA credentials when they enter their email address.

Verify

1. Navigate to [Secure Email Encryption Service Portal](#). Enter the email address registered to CRES, as shown in the image:

Secure Email Encryption Service

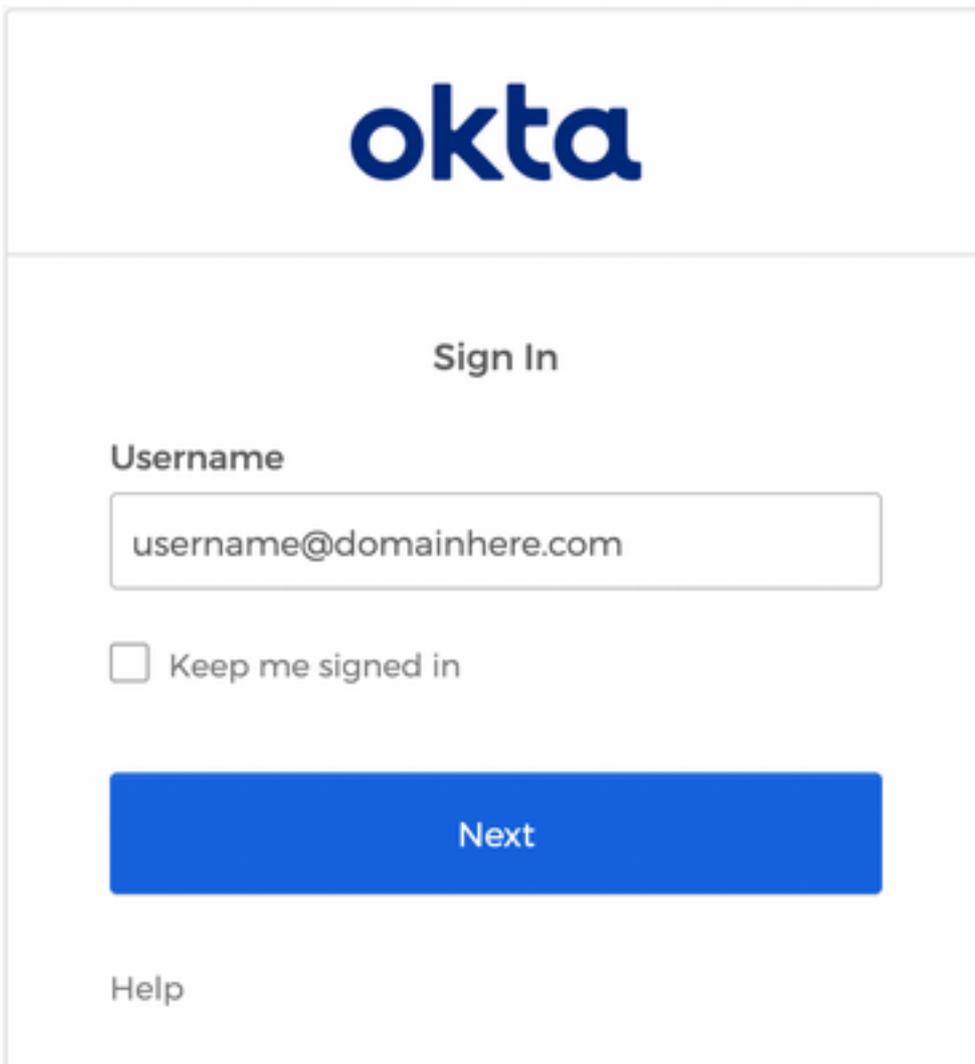
Username*

Log In

OR

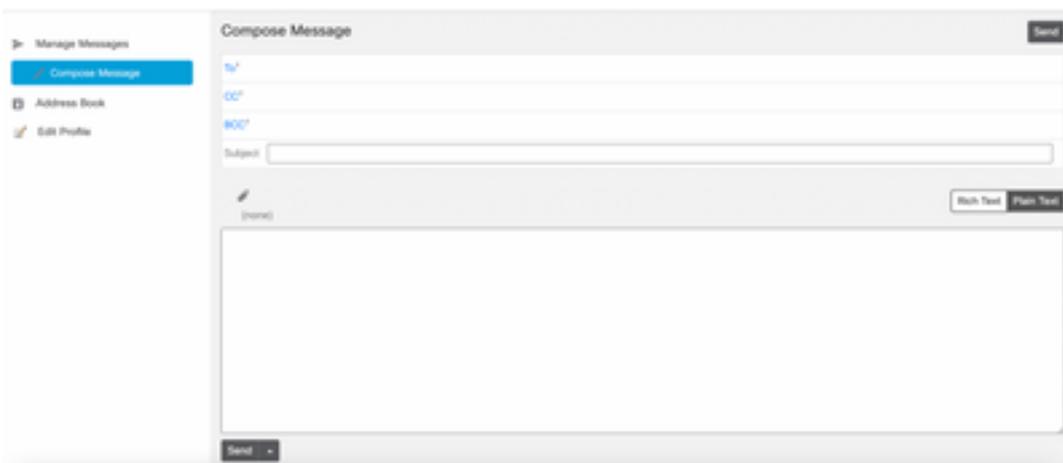
 Sign in with Google

2. A new window opens to proceed with the OKTA authentication Sign in with the **OKTA credentials**, as shown in the image:



The image shows the Okta Sign In page. At the top is the Okta logo. Below it is the heading "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. If the Authentication is successful, the Secure Email Encryption Service opens the Compose Message window, as shown in the image:



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 large text area for the message body. At the bottom right of the text area are "Rich Text" and "Plain Text" buttons. A "Send" button is located at the bottom right of the window.

Now the end user can access the Secure Email Encryption Service portal to compose secure emails or open new envelopes with OKTA credentials.

Related Information

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

[Cisco Secure Gateway End User Guides](#)

[OKTA Support](#)