

Externe OKTA SSO-Authentifizierung für CRES konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Hintergrundinformationen](#)

[Anforderungen](#)

[Konfigurieren](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration der externen OKTA SSO-Authentifizierung für die Anmeldung beim Cisco Secure Email Encryption Service (Registered Envelope).

Voraussetzungen

Administratorzugriff auf den Cisco Secure Email Encryption Service (registrierter Umschlag)

Administratorzugriff auf OKTA.

Selbstsignierte oder CA-signierte (optional) X.509 SSL-Zertifikate im PKCS #12- oder PEM-Format (von OKTA bereitgestellt).

Hintergrundinformationen

- Der Cisco Secure Email Encryption Service (Registered Envelope) ermöglicht die SSO-Anmeldung für Endbenutzer, die SAML verwenden.
- OKTA ist ein Identitätsmanager, der Authentifizierungs- und Autorisierungsdienste für Ihre Anwendungen bereitstellt.
- Der Cisco Secure Email Encryption Service (Registered Envelope) kann als Anwendung festgelegt werden, die zur Authentifizierung und Autorisierung mit OKTA verbunden ist.
- SAML ist ein XML-basiertes, offenes Standarddatenformat, mit dem Administratoren nach der Anmeldung bei einer dieser Anwendungen nahtlos auf einen definierten Satz von Anwendungen zugreifen können.
- Weitere Informationen zu SAML finden Sie unter: [Allgemeine Informationen zu SAML](#)

Anforderungen

- Administratorkonto für den Cisco Secure Email Encryption Service (registrierter Umschlag)
- OKTA-Administratorkonto.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration. Wenn das Netzwerk aktiv ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Unter Okta.

1. Navigieren Sie zum Anwendungsportal, und wählen Sie **Create App Integration**, wie in der Abbildung dargestellt:

Applications



2. Wählen **SAML 2.0** als Anwendungstyp, wie in der Abbildung dargestellt:

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. Geben Sie den App-Namen ein. **CRES** und wählen **Next**, wie in der Abbildung dargestellt:

1 General Settings

App name

App logo (optional) 

App visibility Do not display application icon to users

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

4. Unter dem SAML settings, füllen Sie die Lücken aus, wie in der Abbildung dargestellt:

- URL für die einmalige Anmeldung: Dies ist der Assertion Consumer Service, der über den Cisco Secure Email Encryption Service bereitgestellt wird.
- Zielgruppen-URI (SP Entity ID): Dies ist die vom Cisco Secure Email Encryption Service erhaltene Entitäts-ID.
- Format der Namens-ID: Beibehalten des Namens "Nicht angegeben".
- Application username (Anwendungsbenutzername): Eine E-Mail, die den Benutzer auffordert, seine E-Mail-Adresse bei der Authentifizierung einzugeben.
- Aktualisieren Sie den Benutzernamen der Anwendung auf: Erstellen und Aktualisieren.

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](#)

Blättern Sie nach unten zu Group Attribute Statements (optional), wie in der Abbildung dargestellt:

Geben Sie die nächste Attributanweisung ein:

- Name: group
- Namensformat: Unspecified
- Filter: Equals und OKTA

Group Attribute Statements (optional)

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

Auswählen Next .

5. Wenn Sie aufgefordert werden, Help Okta to understand how you configured this application, geben Sie bitte den zutreffenden Grund für die aktuelle Umgebung ein, wie in der Abbildung dargestellt:

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

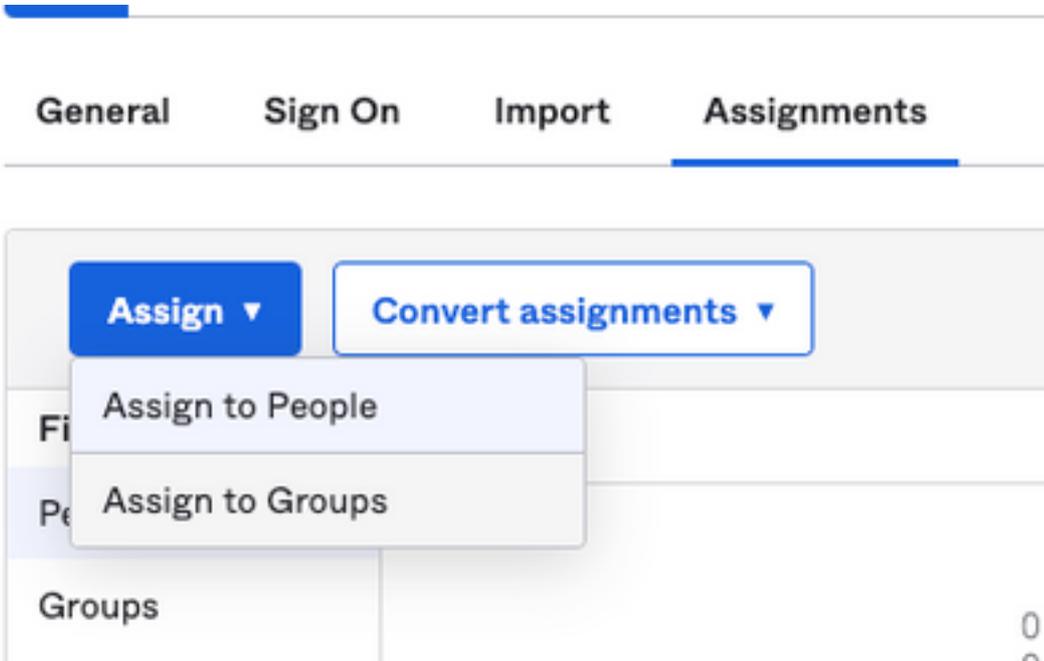
I'm a software vendor. I'd like to integrate my app with Okta

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

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

Auswählen Finish um mit dem nächsten Schritt fortzufahren.

6. Wählen Sie Assignments und anschließend Assign > Assign to Groups, wie in der Abbildung dargestellt:



7. Wählen Sie die OKTA-Gruppe, d. h. die Gruppe mit den autorisierten Benutzern, um auf die Umgebung zuzugreifen.

8. Wählen Sie Sign On, wie in der Abbildung dargestellt:



9. Blättern Sie nach unten, und wählen Sie rechts die View SAML setup instructions Option, wie im Bild gezeigt:

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. Speichern Sie auf einem Notizblock die nächsten Informationen, die notwendig sind, um in die Cisco Secure Email Encryption Service Portal, wie im Bild gezeigt:

- URL für einmalige Anmeldung des Identitätsanbieters

- Aussteller des Identitätsanbieters

- X.509-Zertifikat

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. Nachdem Sie die OKTA-Konfiguration abgeschlossen haben, können Sie zum Cisco Secure Email Encryption Service zurückkehren.

Im Rahmen des Cisco Secure Email Encryption Service (registrierter Umschlag):

1. Melden Sie sich als Administrator bei Ihrem Unternehmensportal an. Der Link lautet: [CRES-Verwaltungsportal](#), wie in der Abbildung dargestellt:

Administration Console Log In

Welcome, please log in:

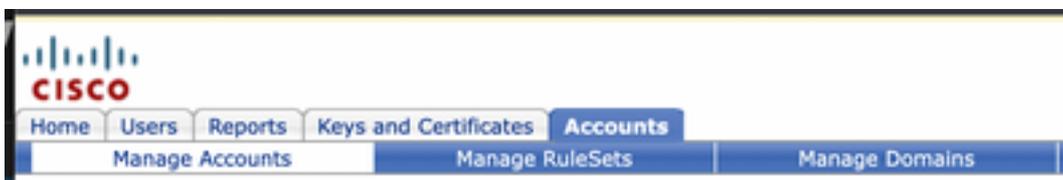
Username

Password

Remember me on this computer.

[Forgot password?](#)

2. Auf dem Accounts Wählen Sie auf der Registerkarte Manage Accounts Registerkarte, wie in der Abbildung dargestellt:



3. Klicken Sie auf eine Kontonummer, und wählen Sie Details Registerkarte, wie in der Abbildung dargestellt:



4. Blättern Sie nach unten zu Authentication Method und wählen SAML 2.0, wie in der Abbildung dargestellt:

Authentication Method

5. Für die SSO Alternate Email Attribute, lassen Sie es leer, wie im Bild gezeigt:

SSO Alternate Email Attribute Name

6. Für die SSO Service Provider Entity ID*, geben <https://res.cisco.com/> , wie in der Abbildung dargestellt:

SSO Service Provider Entity ID*

7. Für die SSO Customer Service URL*, geben Sie Identity Provider Single Sign-On URL bereitgestellt von Okta, wie im Bild zu sehen:

SSO Customer Service URL*

8. Für die SSO Logout URL, lassen Sie es leer, wie im Bild gezeigt:

SSO Logout URL

9. Für die SSO Identity Provider Verification Certificate, laden Sie das von OKTA bereitgestellte X.509 Zertifikat hoch.

10. Wählen Sie **save** um die Einstellungen zu speichern, wie im Bild gezeigt:

Save **Back to Accounts List**

11. Wählen Sie **Activate SAML**. So starten Sie den SAML-Authentifizierungsprozess und erzwingen die SSO-Authentifizierung, wie im Bild gezeigt:

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

12. Es wird ein neues Fenster geöffnet, in dem Sie darüber informiert werden, dass die SAML-Authentifizierung nach der erfolgreichen Authentifizierung beim SAML Identity Provider aktiviert wird. Auswählen **Continue**, wie in der Abbildung dargestellt:

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

Continue

13. Ein neues Fenster wird geöffnet, in dem Sie sich mit OKTA-Anmeldedaten authentifizieren können. Geben Sie **Username** und wählen **Next**, wie in der Abbildung dargestellt:



Sign In

Username

Keep me signed in

Next

Help

14. Wenn der Authentifizierungsprozess erfolgreich verläuft, SAML Authentication Successful wird angezeigt. Auswählen **Continue** um dieses Fenster zu schließen, wie in der Abbildung dargestellt:

SAML Authentication Successful.

Please click continue to close.

Continue

15. Bestätigen Sie die SSO Enable Date wird auf das Datum und die Uhrzeit festgelegt, an dem bzw. zu der die SAML-Authentifizierung erfolgreich war, wie im Bild gezeigt:

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

Die SAML-Konfiguration ist abgeschlossen. Derzeit werden Benutzer, die der CRES-Organisation angehören, zur Verwendung ihrer OKTA-Anmeldeinformationen umgeleitet, wenn sie ihre E-Mail-Adresse eingeben.

Überprüfung

1. Navigieren Sie zum [Secure Email Encryption Service-Portal](#). Geben Sie die bei CRES registrierte E-Mail-Adresse ein, wie im Bild dargestellt:

Secure Email Encryption Service

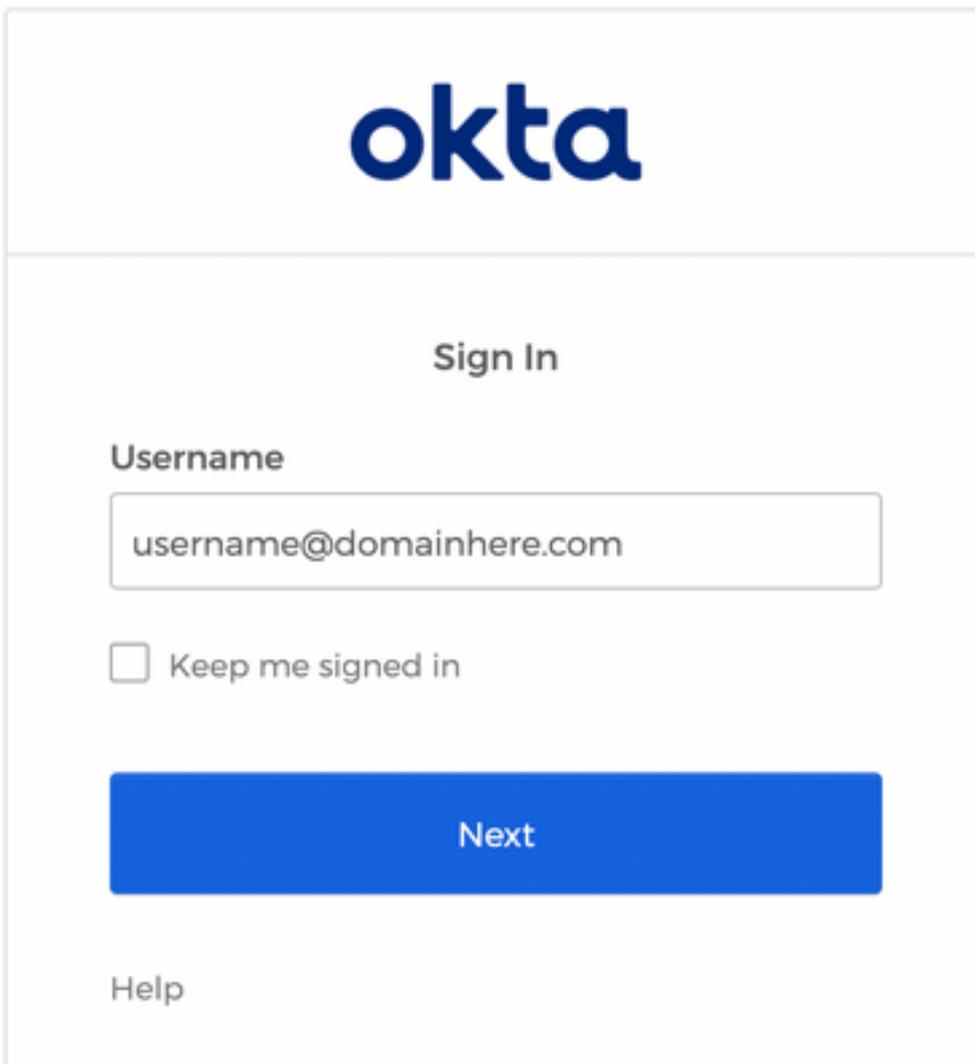
Username*

Log In

OR

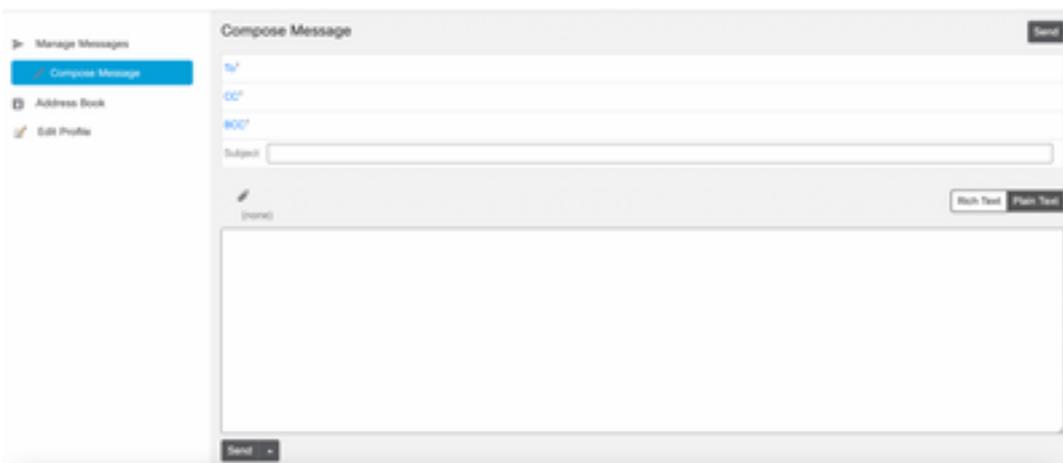
 Sign in with Google

2. Es wird ein neues Fenster geöffnet, in dem Sie mit der OKTA-Authentifizierung fortfahren können. Melden Sie sich mit den **OKTA-Anmeldeinformationen** an, wie im Bild gezeigt:



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. Wenn die Authentifizierung erfolgreich ist, öffnet der sichere E-Mail-Verschlüsselungsdienst die Compose Message Fenster, wie in der Abbildung dargestellt:



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.

Endbenutzer können jetzt auf das Secure Email Encryption Service-Portal zugreifen, um sichere E-Mails zu verfassen oder neue Umschläge mit OKTA-Anmeldeinformationen zu öffnen.

Zugehörige Informationen

[Administratorleitfaden für Cisco Secure Email Encryption Service 6.2](#)

[Cisco Secure Gateway - Benutzerhandbücher](#)

[OKTA-Unterstützung](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.