

# Externe verificatie OKTA SSO configureren voor CRES

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Achtergrondinformatie](#)

[Vereisten](#)

[Configureren](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u OKTA SSO Externe Verificatie kunt configureren voor aanmelding bij Cisco Secure Email Encryption Service (Registered Envelope).

## Voorwaarden

Beheerderstoegang tot Cisco Secure Email Encryption Service (geregistreerde envelop).

Beheerder toegang tot OKTA.

Zelfondertekende of CA-ondertekende (facultatieve) X.509 SSL-certificaten in PKCS #12- of PEM-formaat (geleverd door OKTA).

## Achtergrondinformatie

- Cisco Secure Email Encryption Service (Registered Envelope) maakt SSO-aanmelding mogelijk voor eindgebruikers die SAML gebruiken.
- OKTA is een identiteitsmanager die authenticatie- en autorisatieservices biedt voor uw applicaties.
- Cisco Secure Email Encryption Service (Registered Envelope) kan worden ingesteld als een toepassing die is aangesloten op OKTA voor verificatie en autorisatie.
- SAML is een op XML gebaseerd open standaard dataformaat dat beheerders in staat stelt om naadloos na het teken toegang te krijgen tot een gedefinieerde set toepassingen in een van die toepassingen.
- Voor meer informatie over SAML, raadpleegt u: [SAML General Information](#)

## Vereisten

- Beheerdersaccount voor Cisco Secure Email Encryption Service (Registered Envelope).
- OKTA-beheerdersaccount.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een ontruimde (standaard) configuratie. Als het netwerk actief is, zorg er dan voor dat u de potentiële impact van een opdracht begrijpt.

## Configureren

Onder Okta.

1. Navigeer naar het portaal Toepassingen en selecteer **Create App Integration**, zoals aangegeven op de afbeelding:

### Applications



2. Selecteer **SAML 2.0** als het toepassingstype, zoals in de afbeelding:

#### 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. Voer de naam van de app in **CRES** en selecteer **Next**, zoals aangegeven op de afbeelding:

**1 General Settings**

App name

App logo (optional) 

App visibility  Do not display application icon to users


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


4. Volgens de SAML settings Vul de gaten in, zoals in de afbeelding:


- Enkelvoudige aanmelding op URL: dit is de Assertion Consumer Service die is verkregen van de Cisco Secure Email Encryption Service.
- URI met publiek (SP Entity ID): Dit is de entiteit-ID die is verkregen van de Cisco Secure Email Encryption Service.
- Naam ID formaat: Bewaar het als Niet gespecificeerd.
- Toepassingsgebruikersnaam: E-mail, die de gebruiker vraagt om zijn e-mailadres in te voeren in het verificatieproces.
- Gebruikersnaam voor toepassing bijwerken op: Aanmaken en bijwerken.


**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 naar beneden Group Attribute Statements (optional), zoals aangegeven op de afbeelding:

Voer de volgende attribuutverklaring in:

- Name: group
- Naamformaat: Unspecified
- filteren: Equals en OKTA

#### Group Attribute Statements (optional)

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

Kiezen Next .

5. Wanneer Help Okta to understand how you configured this application Geef ook de reden op die van toepassing is op de huidige omgeving, zoals aangegeven op de afbeelding:

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

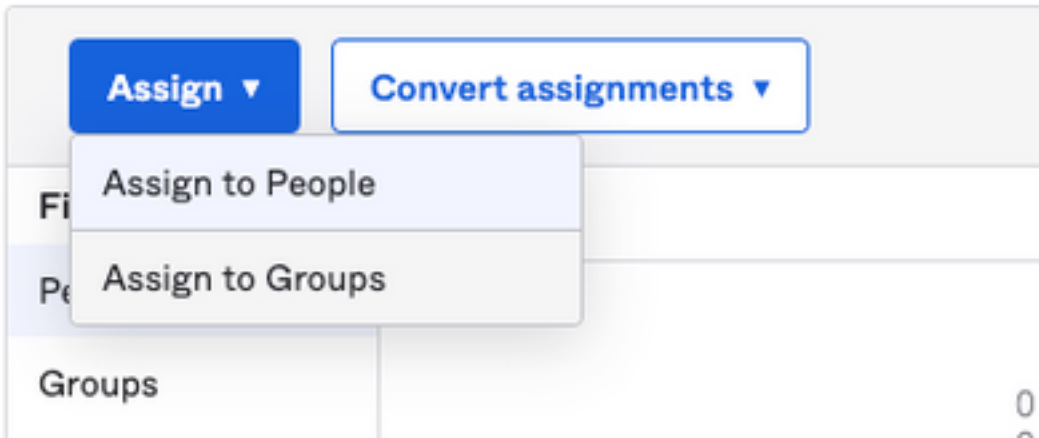
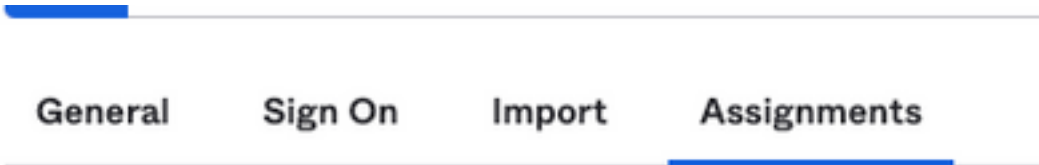
I'm a software vendor. I'd like to integrate my app with Okta

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

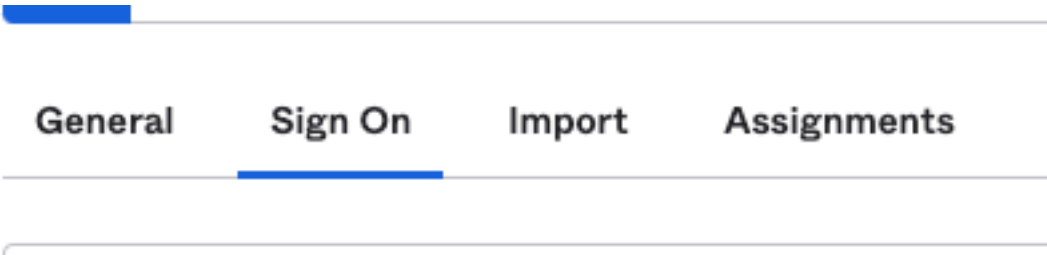
[Previous](#) [Finish](#)

Kiezen Finish om verder te gaan naar de volgende stap.

6. Selecteer Assignments tabblad en selecteer vervolgens Assign > Assign to Groups, zoals aangegeven op de afbeelding:



7. Selecteer de OKTA-groep, die de groep is met de geautoriseerde gebruikers voor toegang tot de omgeving.
8. Selecteer Sign On, zoals aangegeven op de afbeelding:



9. Blader naar beneden en selecteer de optie View SAML setup instructions optie, zoals in de afbeelding:

### 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. Sla de volgende informatie die nodig is om deze in de Cisco Secure Email Encryption Service portal, zoals in de afbeelding:

- Identity Provider Single Sign-On URL

- uitgever van identiteitsbewijzen

- X.509-certificaat

---

## 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](#)

1. Zodra u de OKTA-configuratie hebt voltooid, kunt u terugkeren naar de Cisco Secure Email Encryption Service.

### Onder Cisco Secure Email Encryption Service (geregistreerde encryptie):

1. Log in op uw organisatieportal als beheerder, de link is: [CRES Administration Portal](#), zoals getoond in de afbeelding:

**Administration Console Log In**

Welcome, please log in:

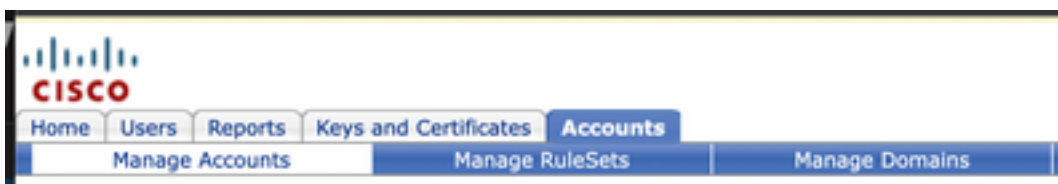
Username

Password

Remember me on this computer.

[Forgot password?](#)

2. Op de Accounts tabblad selecteert u de Manage Accounts tabblad, zoals in de afbeelding:



3. Klik op een accountnummer en selecteer de Details tabblad, zoals in de afbeelding:



4. Scroll naar beneden Authentication Method en selecteer **SAML 2.0**, zoals aangegeven op de afbeelding:

Authentication Method

5. Voor de SSO Alternate Email Attribute Laat het leeg, zoals in de afbeelding:

SSO Alternate Email Attribute Name

6. Voor de SSO Service Provider Entity ID\*, voer in <https://res.cisco.com/>, zoals aangegeven op de afbeelding:

SSO Service Provider Entity ID\*

7. Voor de SSO Customer Service URL\*, de Identity Provider Single Sign-On URL verstrekt door Okta, zoals weergegeven in de afbeelding:

SSO Customer Service  
URL\*

https:// .okta.com/app/

8. Voor de SSO Logout URL Laat het leeg, zoals in de afbeelding:

SSO Logout URL

9. Voor de SSO Identity Provider Verification Certificate, upload het X.509-certificaat dat is geleverd door OKTA.

10. Selecteer **save** Zo slaat u de instellingen op, zoals in de afbeelding:

Save

Back to Accounts List

1. Selecteer **Activate SAML** om het SAML-verificatieproces te starten en de SSO-verificatie uit te voeren, zoals in de afbeelding wordt getoond:

Activate  
SAML

Save

Back to  
Accounts List

12. Er wordt een nieuw venster geopend om aan te geven dat SAML-verificatie actief wordt nadat de verificatie bij de SAML Identity Provider is geslaagd. Kiezen **Continue**, zoals aangegeven op de afbeelding:

---

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

Continue

13. Er wordt een nieuw venster geopend voor verificatie met OKTA Credentials. Voer het **Username** en selecteer **Next**, zoals aangegeven op de afbeelding:





## Sign In

Username

Keep me signed in

Next

Help

14. Als het verificatieproces succesvol is, kan de SAML Authentication Successful wordt weergegeven. Kiezen Continue om dit venster te sluiten, zoals wordt getoond in de afbeelding:

---

SAML Authentication Successful.

**Please click continue to close.**

Continue

15. Bevestig de SSO Enable Date Deze instelling is ingesteld op de datum en het tijdstip waarop de SAML-verificatie is uitgevoerd, zoals aangegeven in de afbeelding:

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	<a href="#">Download</a>
SSO Binding	HTTP-Redirect, HTTP-POST
SSO Assertion Consumer URL	https://res.cisco.com/websafe/ssourl
Current Certificate	

De SAML-configuratie is voltooid. Vanaf dit moment worden gebruikers die lid zijn van de CRES-organisatie omgeleid om hun OKTA-referenties te gebruiken wanneer ze hun e-mailadres invoeren.

## Verifiëren


1. Navigeer naar [Secure Email Encryption Service Portal](#). Voer het e-mailadres in dat bij CRES is geregistreerd, zoals in de afbeelding wordt getoond:

# Secure Email Encryption Service

Username\*

Log In

OR

 Sign in with Google

2. Er wordt een nieuw venster geopend om verder te gaan met de authenticatie van OKTA. Meld u aan met de **referenties van OKTA**, zoals in de afbeelding:

# okta

## Sign In

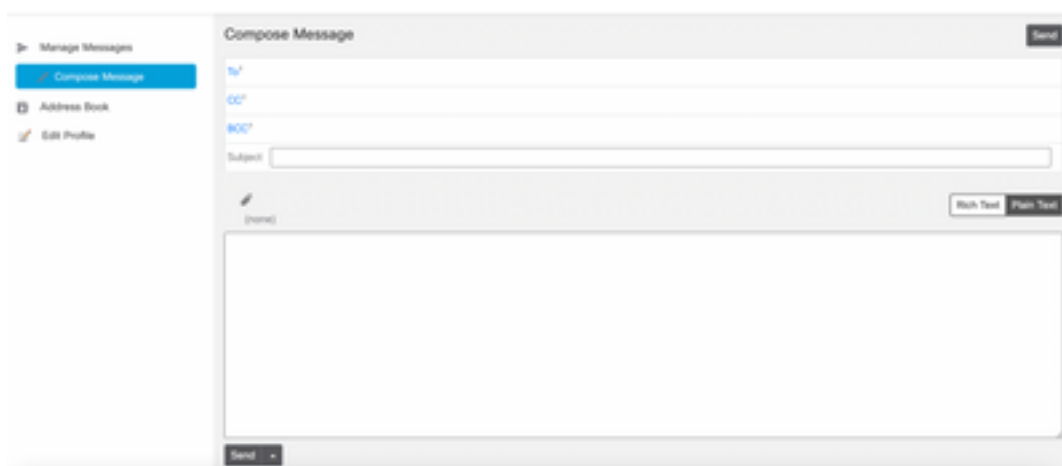
Username

Keep me signed in

Next

Help

3. Als de verificatie succesvol is, opent de Secure Email Encryption Service de Compose Message venster, zoals in de afbeelding:



Nu kan de eindgebruiker toegang krijgen tot het Secure Email Encryption Service portal om beveiligde e-mails samen te stellen of nieuwe enveloppen te openen met OKTA-referenties.

## Gerelateerde informatie

[Cisco Secure Email Encryption Service 6.2-accountbeheerdershandleiding](#)

[Cisco Secure Gateway-eindgebruikershandleidingen](#)

[Ondersteuning van OKTA](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.