

Configurer l'authentification externe OKTA SSO pour CRES

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Informations générales](#)

[Exigences](#)

[Configurer](#)

[Vérifier](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification externe OKTA SSO pour la connexion au service Cisco Secure Email Encryption (recommandé).

Conditions préalables

Accès administrateur au service Cisco Secure Email Encryption (enveloppe inscrite).

Accès administrateur à OKTA.

Certificats SSL X.509 auto-signés ou CA-signés (facultatif) au format PKCS #12 ou PEM (fournis par OKTA).

Informations générales

- Cisco Secure Email Encryption Service (recommandé) permet aux utilisateurs finaux qui utilisent SAML d'ouvrir une session SSO.
- OKTA est un gestionnaire d'identité qui fournit des services d'authentification et d'autorisation à vos applications.
- Cisco Secure Email Encryption Service (recommandé) peut être défini comme une application connectée à OKTA pour l'authentification et l'autorisation.
- SAML est un format de données standard ouvert basé sur XML qui permet aux administrateurs d'accéder à un ensemble défini d'applications en toute transparence après la connexion à l'une de ces applications.
- Pour en savoir plus sur le langage SAML, reportez-vous à : [Informations générales du langage SAML](#)

Exigences

- Compte d'administrateur Cisco Secure Email Encryption Service (recommandé).

- Compte administrateur OKTA.

The information in this document was created from the devices in a specific lab environment. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si le réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande.

Configurer

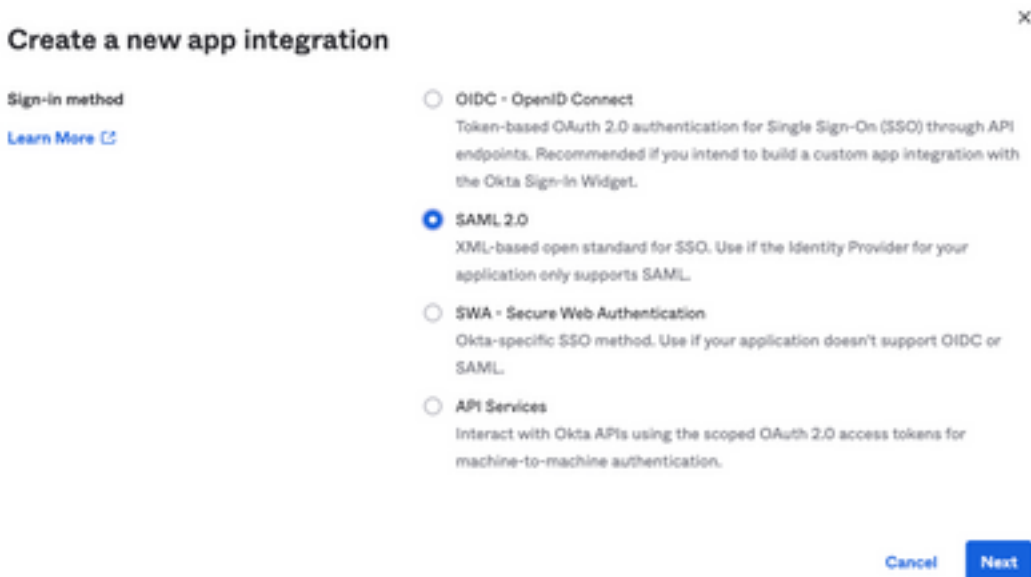
Sous Okta.

1. Accédez au portail Applications et sélectionnez Create App Integration, comme l'illustre l'image :

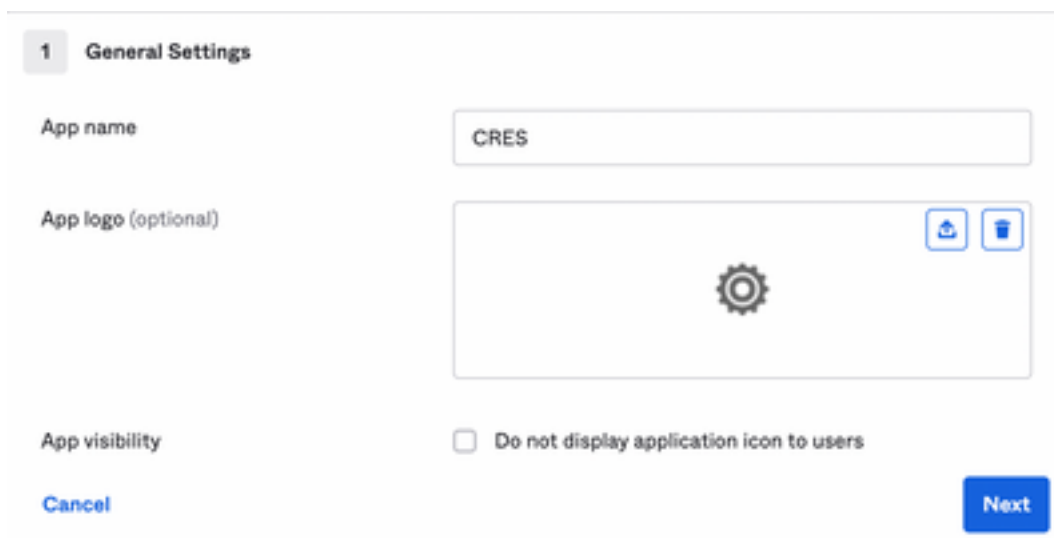
Applications



2. Sélectionnez SAML 2.0 comme type d'application, comme illustré dans l'image :



3. Entrez le nom de l'application CRES et sélectionnez Next, comme l'illustre l'image :



4. Dans la section SAML settings, remplissez les espaces vides, comme indiqué dans l'image :

- URL d'authentification unique : il s'agit du service client d'assertion obtenu auprès du service de chiffrement sécurisé des e-mails de Cisco.

- URI d'auditoire (ID d'entité SP) : ID d'entité obtenu auprès du service de chiffrement sécurisé des e-mails de Cisco.

- Format d'ID de nom : conservez-le comme Non spécifié.

- Nom d'utilisateur de l'application : e-mail, qui invite l'utilisateur à saisir son adresse e-mail dans le processus d'authentification.

- Mettre à jour le nom d'utilisateur de l'application sur : Créer et mettre à jour.

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](#)

Faites défiler jusqu'à Group Attribute Statements (optional), comme l'illustre l'image :

Entrez l'instruction d'attribut suivante :

-Name : group

- Format du nom : Unspecified

- Filtre : Equals et OKTA

Group Attribute Statements (optional)

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

Sélectionner **Next** .

5. Lorsqu'il est demandé Help Okta to understand how you configured this application, veuillez saisir la raison applicable à l'environnement actuel, comme indiqué dans l'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

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](#)

Sélectionner **Finish** pour passer à l'étape suivante.

6. Sélectionnez **Assignments** , puis sélectionnez **Assign > Assign to Groups**, comme l'illustre l'image :

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

Assign ▾ **Convert assignments** ▾

- Assign to People
- Assign to Groups

Fi

Pe

Groups

0:

0:

7. Sélectionnez le groupe OKTA, c'est-à-dire le groupe avec les utilisateurs autorisés à accéder à l'environnement.

8. Sélectionnez **Sign On**, comme l'illustre l'image :

General

Sign On

Import

Assignments

9. Faites défiler vers le bas et, dans le coin droit, sélectionnez [View SAML setup instructions](#) , comme l'illustre l'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. Enregistrez sur un bloc-notes les informations suivantes, qui sont nécessaires pour mettre dans le [Cisco Secure Email Encryption Service](#) portail, comme l'illustre l'image :

- URL d'authentification unique du fournisseur d'identité
- Émetteur du fournisseur d'identité
- Certificat 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. Une fois la configuration OKTA terminée, vous pouvez revenir au service Cisco Secure Email Encryption.

Sous Cisco Secure Email Encryption Service (Enveloppe inscrite) :

1. Connectez-vous au portail de votre organisation en tant qu'administrateur, le lien est : [CRES Administration Portal](#), comme indiqué dans l'image :



Administration Console Log In

Welcome, please log in:

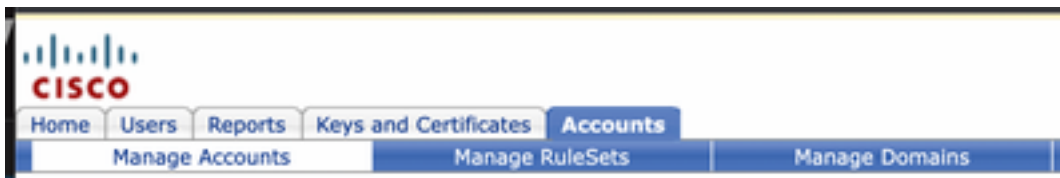
Username

Password

Remember me on this computer.

[Forgot password?](#)

2. Sur la page Accounts , sélectionnez l'option Manage Accounts , comme l'illustre l'image :



3. Cliquez sur un numéro de compte et sélectionnez le **Details** , comme l'illustre l'image :



4. Faites défiler jusqu'à **Authentication Method** et sélectionnez **SAML 2.0**, comme l'illustre l'image :



5. Pour la **SSO Alternate Email Attribute Name**, laissez ce champ vide, comme illustré dans l'image :



6. Pour la **SSO Service Provider Entity ID***, saisissez <https://res.cisco.com/> , comme l'illustre l'image :



7. Pour la **SSO Customer Service URL***, entrez la commande **Identity Provider Single Sign-On URL** fournie par Okta, comme le montre l'image :

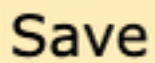
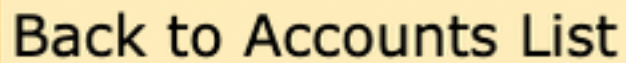


8. Pour la **SSO Logout URL**, laissez ce champ vide, comme illustré dans l'image :


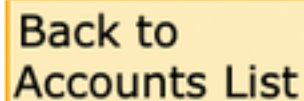


9. Pour la **SSO Identity Provider Verification Certificate**, téléchargez le certificat X.509 fourni par OKTA.

10. Sélectionnez **save** pour enregistrer les paramètres, comme indiqué dans l'image :

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. Sélectionnez `Activate SAML` pour démarrer le processus d'authentification SAML et appliquer l'authentification SSO, comme indiqué dans l'image :

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. Une nouvelle fenêtre s'ouvre pour informer que l'authentification SAML devient active après une authentification réussie avec le fournisseur d'identité SAML. Sélectionner `Continue`, comme l'illustre l'image :

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. Une nouvelle fenêtre s'ouvre pour authentifier les informations d'identification OKTA. Saisissez la commande `Username` et sélectionnez `Next`, comme l'illustre l'image :



Sign In

Username

Keep me signed in

Next

Help

14. Si le processus d'authentification réussit, le SAML Authentication Successful s'affiche. Sélectionner Continue pour fermer cette fenêtre, comme illustré dans l'image :

SAML Authentication Successful.

Please click continue to close.

Continue

15. Confirmez la SSO Enable Date est défini sur la date et l'heure auxquelles l'authentification SAML a réussi, comme indiqué dans l'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	

La configuration SAML est terminée. À partir de ce moment, les utilisateurs qui appartiennent à l'organisation CRES sont redirigés pour utiliser leurs identifiants OKTA lorsqu'ils saisissent leur adresse e-mail.

Véifier

1. Accédez au [portail Secure Email Encryption Service](#). Saisissez l'adresse e-mail enregistrée auprès de CRES, comme indiqué dans l'image :

Secure Email Encryption Service

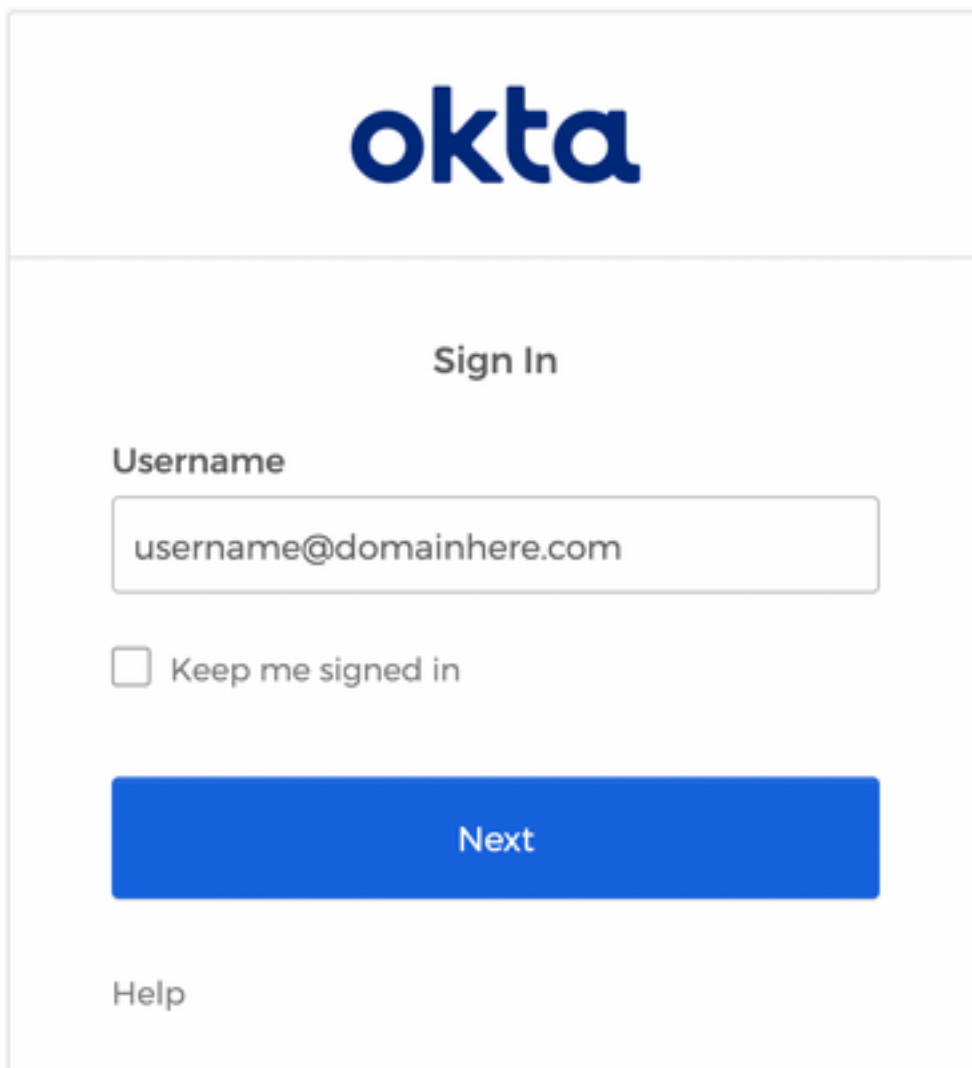
Username*

Log In

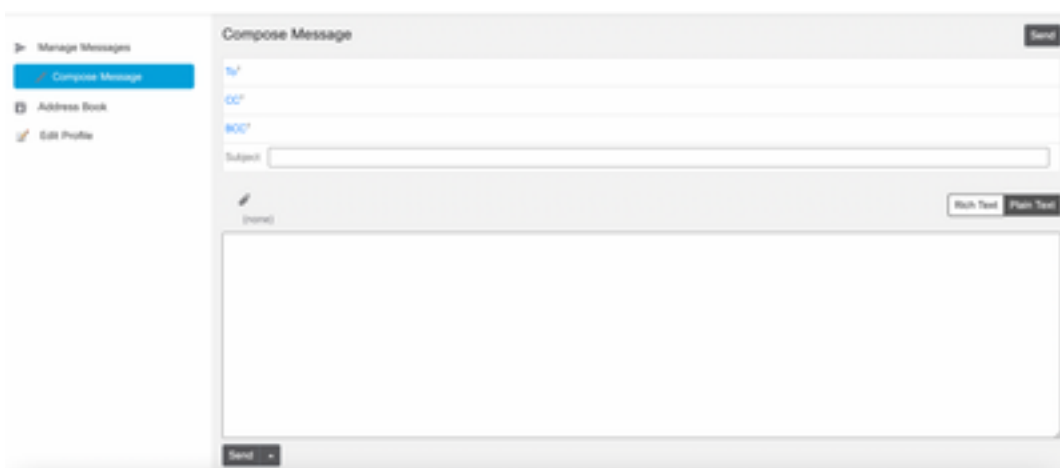
OR

 Sign in with Google

2. Une nouvelle fenêtre s'ouvre pour poursuivre l'authentification OKTA. Connectez-vous avec les **identifiants OKTA**, comme indiqué dans l'image :



3. Si l'authentification réussit, le service Secure Email Encryption Service ouvre le Compose Message , comme l'illustre l'image :



L'utilisateur final peut désormais accéder au portail Secure Email Encryption Service pour rédiger des e-mails sécurisés ou ouvrir de nouvelles enveloppes avec des identifiants OKTA.

Informations connexes

[Guide de l'administrateur de compte Cisco Secure Email Encryption Service 6.2](#)

[Guides d'utilisation de Cisco Secure Gateway](#)

[Assistance OKTA](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.