

Configuration de l'authentification externe OKTA SSO pour Advanced Phishing Protection

Contenu

[Introduction](#)

[Conditions préalables](#)

[Informations générales](#)

[Conditions requises](#)

[Configuration](#)

[Vérification](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification externe OKTA SSO pour la connexion à Cisco Advanced Phishing Protection.

Conditions préalables

Accès administrateur au portail Cisco Advanced Phishing Protection.

Accès administrateur à Okta idP.

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

Informations générales

- Cisco Advanced Phishing Protection permet d'activer la connexion SSO pour les administrateurs utilisant SAML.
- OKTA est un gestionnaire d'identité qui fournit des services d'authentification et d'autorisation à vos applications.
- Cisco Advanced Phishing Protection 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 s'être connectés à l'une de ces applications.
- Pour en savoir plus sur le langage SAML, cliquez sur le lien suivant : [SAML General Information](#)

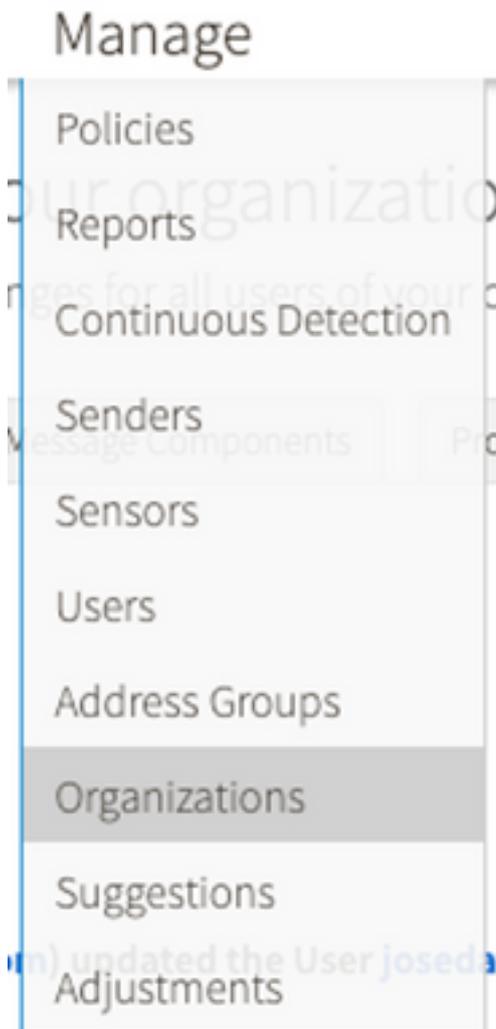
Conditions requises

- Portail Cisco Advanced Phishing Protection.
- Compte administrateur OKTA.

Configuration

Sous Cisco Advanced Phishing Protection Portal :

1. Connectez-vous au portail de votre organisation, puis sélectionnez **Manage > Organizations**, comme indiqué dans l'image :



2. Sélectionnez le nom de votre organisation, **Modifier l'organisation**, comme indiqué dans l'image :

Edit Organization

Alter the settings for this organization.



3. Dans l'onglet **Administrative**, faites défiler jusqu'à **User Account Settings** et sélectionnez **Enable** sous SSO, comme illustré dans l'image :

User Account Settings

Single Sign-On:

If Single Sign-On is enabled for the users in an organization, some of the following settings may be overridden by the Identity Provider used for authentication. Refer to the documentation for the Identity Provider for specific settings regarding failed login attempts and password policy.

4. La fenêtre suivante fournit les informations à saisir dans la configuration OKTA SSO. Collez les informations suivantes sur un bloc-notes, utilisez-les pour configurer les paramètres OKTA :

- ID d'entité : apcc.cisco.com
- Assertion Consumer Service : ces données sont adaptées à votre entreprise.

Sélectionnez le format **e-mail** nommé pour utiliser une adresse e-mail pour la connexion, comme indiqué dans l'image :

Single Sign-On Configuration

Follow the steps below to configure Cisco APP to use your organization's Single Sign-On solution. Upon completion, all users in your organization will receive an email with instructions to complete account setup to use Single Sign-On to authenticate with Cisco APP.

You may need the following parameters configured on your Identity Provider:

- Entity ID: apcc.cisco.com
- Assertion Consumer Service (ACS):
- Name Identifier Format: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

5. Réduisez la configuration de Cisco Advanced Phishing Protection à ce stade, car vous devez d'abord définir l'application dans OKTA avant de passer aux étapes suivantes.

Sous Okta.

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

Applications

[Create App Integration](#) [Browse App Catalog](#) [Assign Users to App](#) [More ▾](#)

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

Create a new app integration

X

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. Entrez le nom de l'application **Advanced Phishing Protection** et sélectionnez **Next**, comme indiqué dans l'image :

1 General Settings

App name

App logo (optional)

App visibility Do not display application icon to users

Cancel

4. Sous les paramètres SAML, remplissez les vides, comme indiqué dans l'image :

- URL de connexion unique : Il s'agit du service client d'assertion obtenu auprès de Cisco Advanced Phishing Protection.

- URL du destinataire : Il s'agit de l'ID d'entité obtenu auprès de Cisco Advanced Phishing Protection.

- Format d'ID de nom : conservez-la comme non spécifiée.

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

- Mettre à jour le nom d'utilisateur : 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 Statement (facultatif)**, comme indiqué dans l'image :

Entrez l'instruction d'attribut suivante :

- Name : groupe
- Format du nom : Non spécifié.
- Filtre : "Est égal à" et "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"/>

[Add Another](#)

Sélectionnez Suivant.

5. Lorsque vous êtes invité à aider Okta à comprendre comment vous avez configuré cette application, veuillez entrer 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

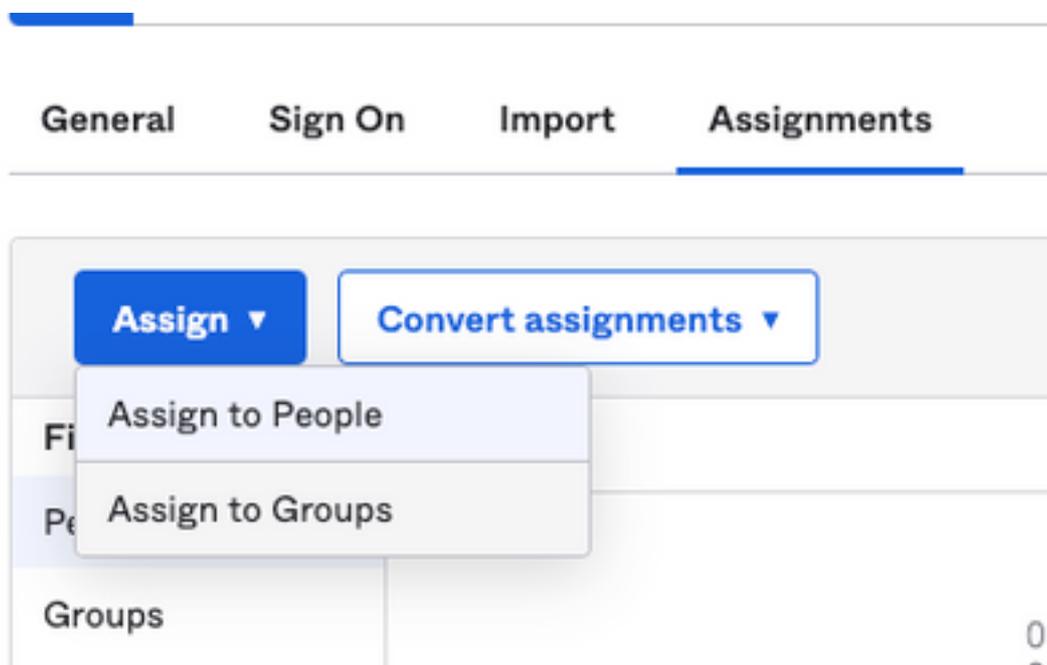
I'm a software vendor. I'd like to integrate my app with Okta

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

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

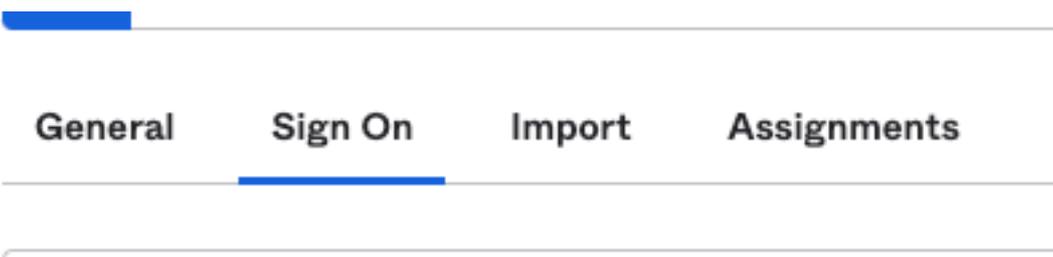
Sélectionnez **Terminer** pour passer à l'étape suivante.

6. Sélectionnez l'onglet **Affectations**, puis sélectionnez **Affecter** > **Affecter à des groupes**, comme indiqué dans l'image :



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 indiqué dans l'image :



9. Faites défiler vers le bas et dans le coin droit, entrez l'option **View SAML setup instructions**, comme indiqué dans 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](#)

9. Enregistrez sur un bloc-notes les informations suivantes, qui sont nécessaires pour accéder au portail Cisco Advanced Phishing Protection, comme illustré dans l'image :

- URL de connexion unique du fournisseur d'identité.
- Identifiez l'émetteur du fournisseur (non requis pour Cisco Advanced Phishing Protection, mais obligatoire pour les autres applications).
- Certificat X.509.

The following is needed to configure Advanced Phishing Protection

1 Identity Provider Single Sign-On URL:

https:// /eak2j1xb1n0qg9Rk0697/sso/saml

2 Identity Provider issuer:

http://www.okta.com/

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDqjOCAPkqAwIBAgIIGATN/4nF0MA8OC5qGS1b3OQEBCwIAAMTGVWQswCQEDVQQOEwAVUudTRBEG
```

```
-----END CERTIFICATE-----
```

[Download certificate](#)

10. Une fois la configuration OKTA terminée, vous pouvez revenir à Cisco Advanced Phishing Protection

Sous Cisco Advanced Phishing Protection Portal :

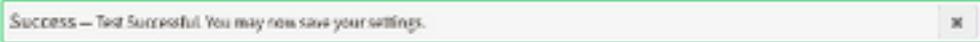
1. Avec le format d'identificateur de nom, entrez les informations suivantes :

- Point de terminaison SAML 2.0 (redirection HTTP) : L'URL d'authentification unique du fournisseur d'identité fournie par Okta.

- Certificat public : Saisissez le certificat X.509 fourni par Okta.

2. Sélectionnez **Test Settings** pour vérifier que la configuration est correcte

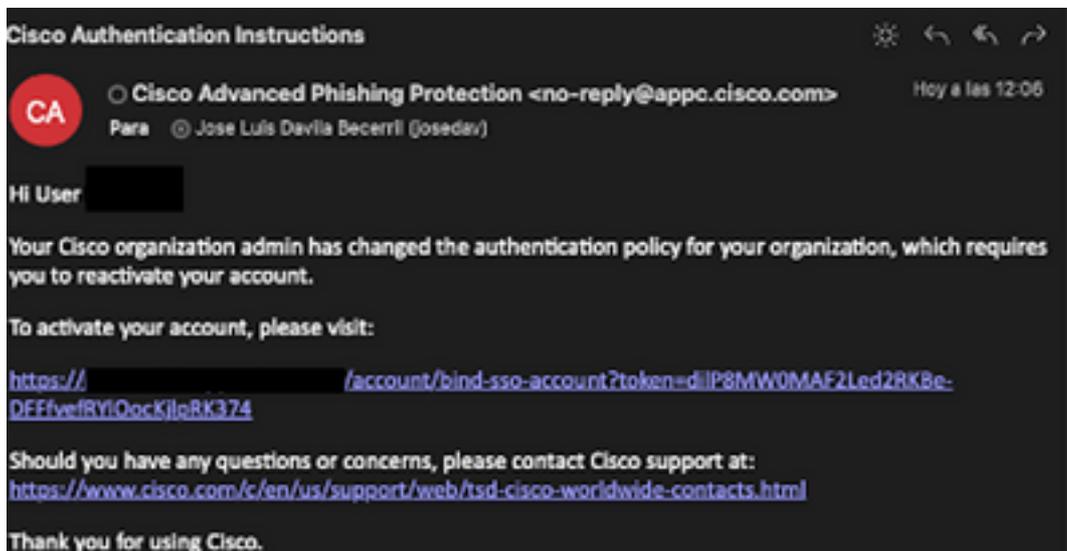
En l'absence d'erreur dans la configuration, une entrée Test Successful s'affiche et vous pouvez maintenant enregistrer vos paramètres, comme indiqué dans l'image :



3. Enregistrez les paramètres

Vérification

1. Pour les administrateurs existants n'utilisant pas SSO, ils sont avertis par e-mail que la stratégie d'authentification est modifiée pour l'organisation et les administrateurs sont invités à activer leur compte à l'aide d'un lien externe, comme indiqué dans l'image :



2. Une fois le compte activé, entrez votre adresse e-mail, puis il vous redirige vers le site Web de connexion OKTA pour la connexion, comme indiqué dans l'image :

Log In to Advanced Phishing Protection

Not a member? [Sign up here](#)

Your Email:

[Next](#)

okta

Sign In

Username

Keep me signed in

[Next](#)

[Help](#)

3. Une fois le processus de connexion OKTA terminé, connectez-vous au portail Cisco Advanced Phishing Protection, comme illustré dans l'image :

Real Time Threat Trends Executive Summary

0 Messages

0 Eulcered Messages
0 Deleted

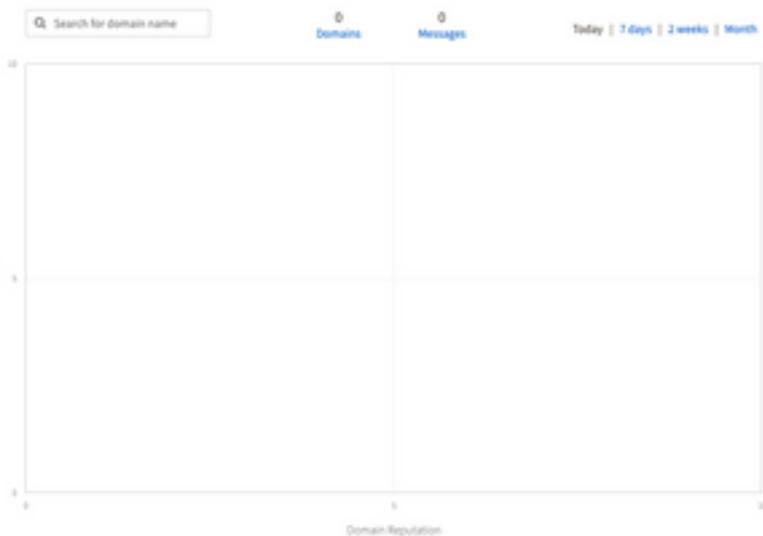
Continuous Detection and Response
2.67 K Active Events
0 Discovered Messages

0 Individual Display Name Impostors
0 Brand Display Name Impostors

0 Compromised Accounts
0 Domain Spoofs

0 Look alike Domains
0 Spam or Graymail

0 Malicious Attachments
0 Malicious URLs



Informations connexes

[Cisco Advanced Phishing Protection - Informations sur le produit](#)

[Cisco Advanced Phishing Protection - Guide de l'utilisateur final](#)

[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.