

# OKTA SSO externe verificatie configureren voor geavanceerde phishing-bescherming

## 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 Advanced Phishing Protection.

## Voorwaarden

Beheerderstoegang tot Cisco Advanced Phishing Protection Portal.

Beheerderstoegang tot Okta idP.

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

## Achtergrondinformatie

- Cisco Advanced Phishing Protection maakt het mogelijk om SSO-aanmelding in te schakelen voor beheerders die SAML gebruiken.
- OKTA is een identiteitsmanager die authenticatie- en autorisatieservices biedt voor uw toepassingen.
- Cisco Advanced Phishing Protection kan worden ingesteld als een toepassing die is verbonden met OKTA voor verificatie en autorisatie.
- SAML is een op XML gebaseerd open standaard dataformaat dat beheerders in staat stelt om naadloos toegang te krijgen tot een gedefinieerde set toepassingen nadat ze in een van die toepassingen zijn getekend.
- Voor meer informatie over SAML kunt u de volgende link gebruiken: [SAML General Information](#)

## Vereisten

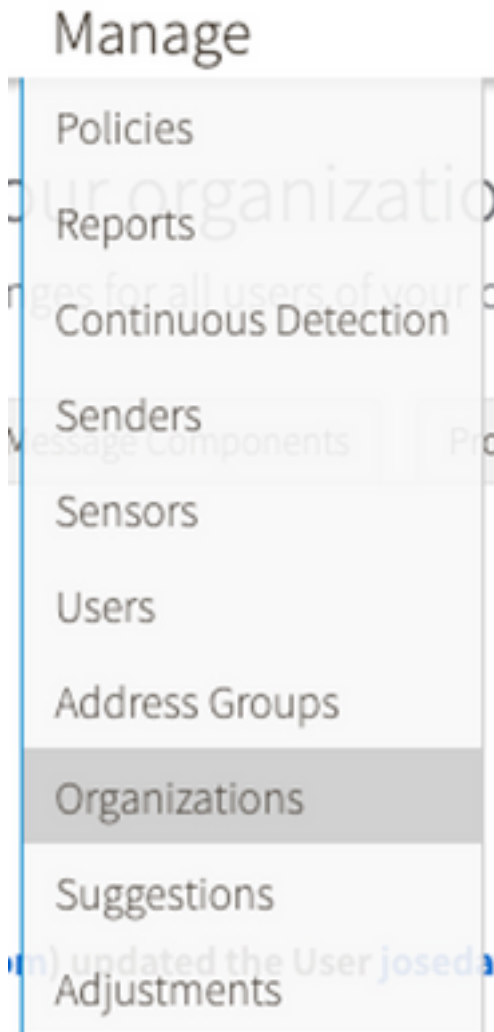
- Cisco Advanced Phishing Protection-portal.

- OKTA-beheerdersaccount.

## Configureren

Onder Cisco Advanced Phishing Protection Portal:

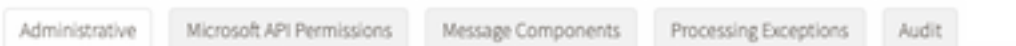
1. Log in op uw organisatieportal en selecteer vervolgens **Beheer > Organisaties**, zoals in de afbeelding:



2. Selecteer de naam van uw organisatie, **Bewerk organisatie**, zoals in de afbeelding:

### Edit Organization

Alter the settings for this organization.



3. Blader in het tabblad **Administratie** naar **Gebruikersaccountinstellingen** en selecteer **Inschakelen** onder SSO, zoals in de afbeelding:

## 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. Het volgende venster geeft u de informatie die moet worden ingevoerd onder de OKTA SSO-configuratie. Plakt de volgende informatie naar een blocnote en gebruik deze om OKTA-instellingen te configureren:

-Entiteits-ID: apcc.cisco.com

- Assertion Consumer Service: deze gegevens zijn toegesneden op uw organisatie.

Selecteer het genoemde formaat **e-mail** om een e-mailadres voor login te gebruiken, dat in het beeld wordt getoond:

## 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):
  - ✓ urn:csa:names:to:SAML\_1.1:named-format:unspecified
  - ✓ urn:csa:names:to:SAML\_1.1:named-format:emailAddress
  - ✓ urn:csa:names:to:SAML\_2.0:named-format:persistent

5. Minimaliseer momenteel de configuratie van Cisco Advanced Phishing Protection, aangezien u de toepassing eerst in OKTA moet instellen voordat u naar de volgende stappen gaat.

Onder Okta.

1. Navigeren naar het portaal Toepassingen en selecteer **App-integratie maken**, zoals in de afbeelding:

## Applications

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

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

## 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. Voer de App naam **Advanced Phishing Protection in** en selecteer **Volgende**, zoals in de afbeelding:

1 General Settings

App name: Cisco Advanced Phishing Protection

App logo (optional): [Gear icon]

App visibility:  Do not display application icon to users

Cancel Next

4. Vul onder de SAML-instellingen de gaten in, zoals in de afbeelding:

- Enkele aanmelding bij URL: Dit is de Assertion Consumer Service die is verkregen van Cisco Advanced Phishing Protection.
- URL ontvanger: Dit is de entiteit-ID die is verkregen van Cisco Advanced Phishing Protection.
- Formaat naam-ID: Niet opgegeven.
- Gebruikersnaam voor de toepassing: E-mail, die de gebruiker vraagt om zijn e-mailadres in te voeren in het verificatieproces.
- Gebruikersnaam voor toepassing bijwerken op: Maak en 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](#)

Blader omlaag naar **Toewijzingsverklaringen groep (optioneel)**, zoals in de afbeelding:

Voer de volgende attribootverklaring in:

- Name: groep
- Naamformaat: Niet gespecificeerd.
- filteren: "Gelijk" en "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](#)

Selecteer Volgende.

5. Wanneer u wordt gevraagd om Okta te helpen begrijpen hoe u deze toepassing hebt geconfigureerd, dient u de toepasselijke reden voor de huidige omgeving in te voeren, zoals wordt getoond in 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

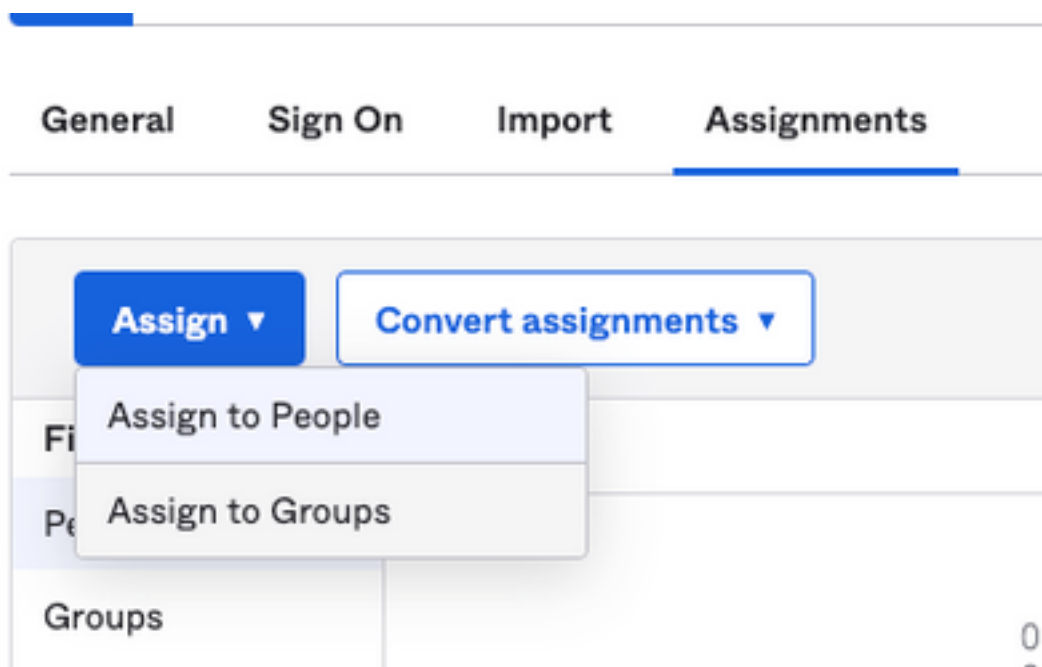
I'm a software vendor. I'd like to integrate my app with Okta

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

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

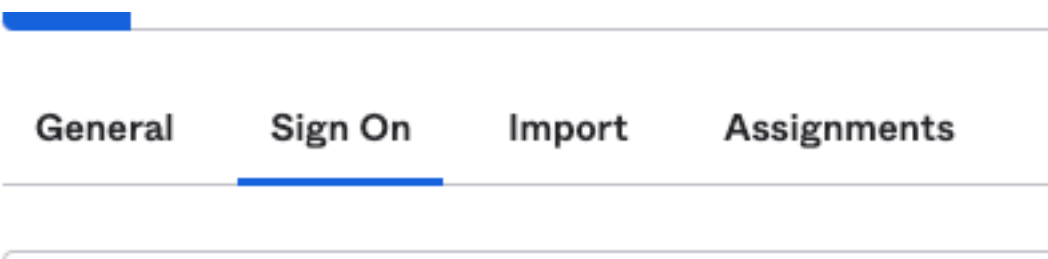
Selecteer **Voltoeien** om door te gaan naar de volgende stap.

6. Selecteer het tabblad **Toewijzingen** en selecteer vervolgens **Toewijzen > Toewijzen aan groepen**, zoals in de afbeelding:



7. Selecteer de OKTA-groep, de groep met de geautoriseerde gebruikers voor toegang tot de omgeving

8. Selecteer **Sign On**, zoals in de afbeelding:



9. Blader naar beneden en naar rechts, en voer de optie **SAML-installatie-instructies bekijken in**, zoals wordt aangegeven 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](#)

9. Sla de volgende informatie die nodig is om de Cisco Advanced Phishing Protection-portal te openen, zoals in het afbeelding:

- Identity Provider Single Sing-On URL.
- Identificeer de provider van de provider (niet vereist voor Cisco Advanced Phishing Protection , maar verplicht voor andere toepassingen).
- X.509-certificaat.

### 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/4nFOMA8OC5qGS1b3OQEBCwIAMIQVWQswCQYEDVQOOeAVUudTWBEG
```

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

[Download certificate](#)

10. Nadat u de OKTA-configuratie hebt voltooid, kunt u teruggaan naar Cisco Advanced Phishing Protection


### Onder Cisco Advanced Phishing Protection Portal:

1. Voer de volgende informatie in via het Name identifier Format:

- SAML 2.0 Endpoint (HTTP-omleiding): De Identify Provider Single Sign-On URL geleverd door Okta.
- Openbaar certificaat: Voer het X.509-certificaat in dat door Okta is verstrekt.

2. Selecteer **Test Settings** om te controleren of de configuratie correct is

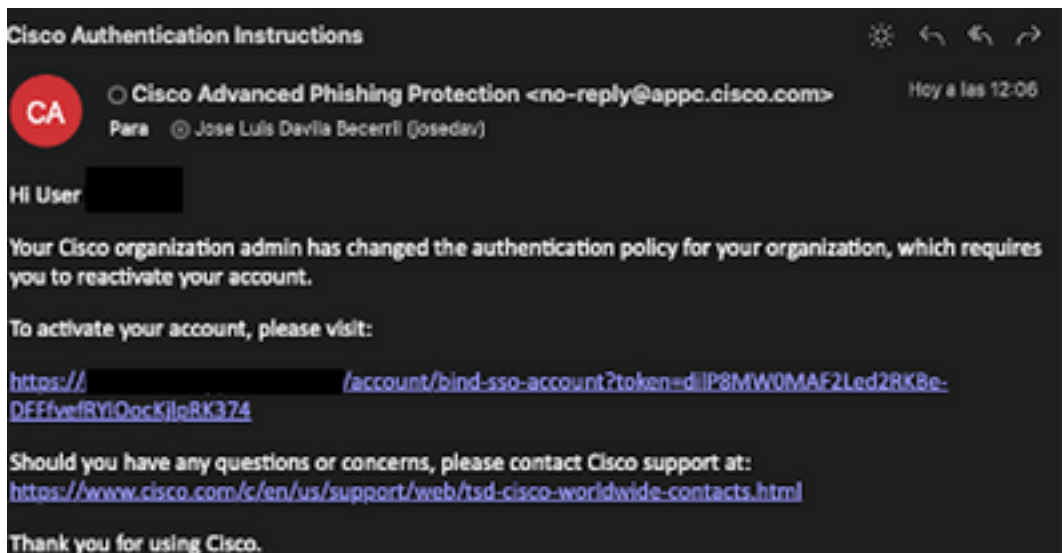
Als er geen fouten in de configuratie zijn, ziet u een succesvolle ingang van de Test en kunt nu uw instellingen opslaan, zoals in de afbeelding:



3. Instellingen opslaan

## Verifiëren

1. Bestaande beheerders die geen SSO gebruiken, worden via e-mail op de hoogte gesteld dat het verificatiebeleid voor de organisatie wordt gewijzigd en de beheerders worden gevraagd hun account te activeren via een externe link, zoals in de afbeelding:



2. Zodra de account is geactiveerd, voer je je e-mailadres in en leidt het je naar de inlogwebsite van OKTA voor inloggen, zoals in de afbeelding:



# Log In to Advanced Phishing Protection

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

Your Email:

Next

# okta

## Sign In

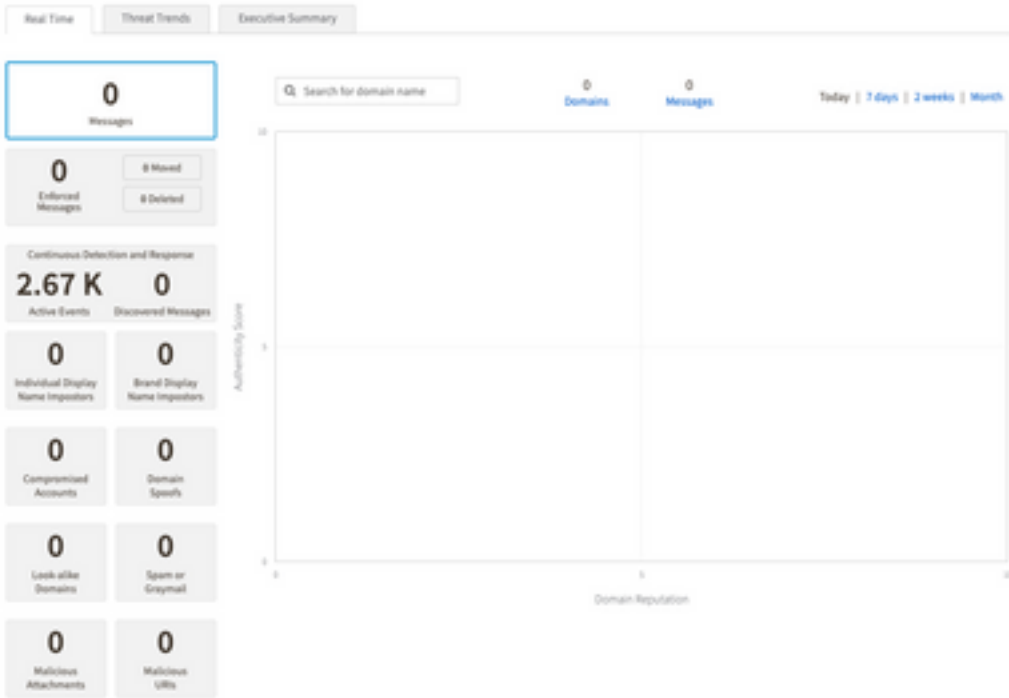
Username

Keep me signed in

Next

[Help](#)

3. Log na voltooiing van het OKTA-inlogproces in het Cisco Advanced Phishing Protection-portal, zoals in de afbeelding:



## Gerelateerde informatie

[Cisco Advanced Phishing Protection - productinformatie](#)

[Cisco Advanced Phishing Protection - Eindgebruikershandleiding](#)

[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.