

Configuración de la Autenticación Externa SSO de OKTA para Protección Avanzada contra Phishing

Contenido

[Introducción](#)

[Prerequisites](#)

[Información general](#)

[Requirements](#)

[Configurar](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la Autenticación Externa SSO de OKTA para iniciar sesión en la Protección avanzada contra phishing de Cisco.

Prerequisites

Acceso de administrador al portal de protección frente a suplantación de identidad avanzada de Cisco.

Acceso de administrador a Okta idP.

Certificados SSL X.509 con firma automática o CA firmada (opcional) en formato PKCS #12 o PEM.

Información general

- Cisco Advanced Phishing Protection permite habilitar el inicio de sesión SSO para los administradores que utilizan SAML.
- OKTA es un gestor de identidades que proporciona servicios de autenticación y autorización a sus aplicaciones.
- La protección frente a suplantación de identidad avanzada de Cisco se puede establecer como una aplicación conectada a OKTA para la autenticación y autorización.
- SAML es un formato de datos estándar abierto basado en XML que permite a los administradores acceder a un conjunto definido de aplicaciones sin problemas después de iniciar sesión en una de esas aplicaciones.
- Para obtener más información sobre SAML, puede acceder al siguiente enlace: [Información general sobre SAML](#)

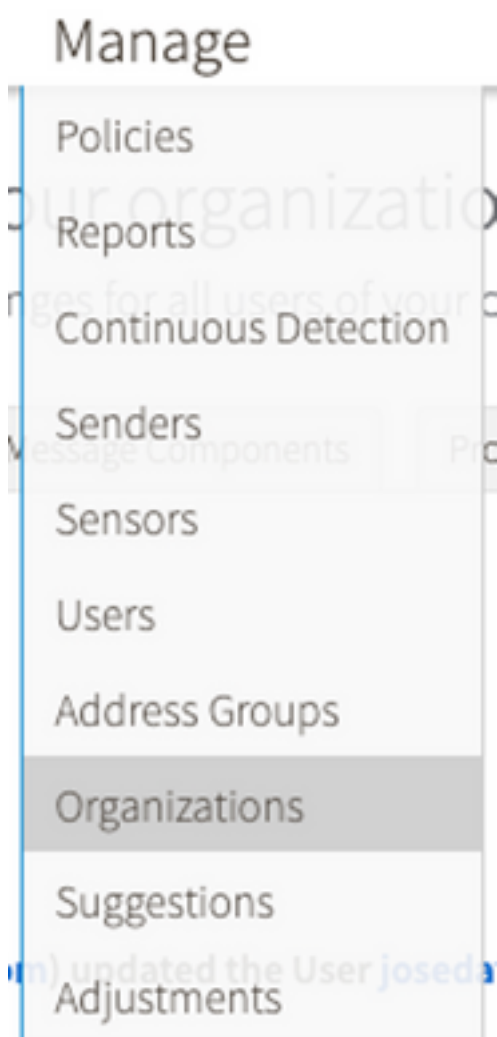
Requirements

- Portal de protección frente a phishing avanzada de Cisco.
- Cuenta de administrador OKTA.

Configurar

En el portal de protección frente a phishing avanzada de Cisco:

1. Inicie sesión en el portal de su organización y seleccione **Manage > Organizations**, como se muestra en la imagen:



2. Seleccione el nombre de la organización, **Editar Organización**, como se muestra en la imagen:

Edit Organization

Alter the settings for this organization.



3. En la pestaña **Administrative**, desplácese hacia abajo hasta **User Account Settings** y seleccione **Enable** bajo SSO, como se muestra en la imagen:

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 siguiente ventana proporciona la información que se debe introducir en la configuración de OKTA SSO. Pegue en un bloc de notas la siguiente información y utilícela para configurar los parámetros de OKTA:

- ID de entidad: apcc.cisco.com
- Servicio al consumidor de aserción: estos datos se adaptan a su organización.

Seleccione el formato de **correo electrónico** con nombre para utilizar una dirección de correo electrónico para el inicio de sesión, que se muestra en la imagen:

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:oasis:names:tc:SAML:1.1:nameid-format:unspecified
 - urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
 - urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

5. Minimice la configuración de Cisco Advanced Phishing Protection en este momento, ya que debe configurar primero la aplicación en OKTA antes de continuar con los siguientes pasos.

Bajo Okta.

1. Navegue hasta el portal de aplicaciones y seleccione **Create App Integration**, como se muestra en la imagen:

Applications

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

2. Seleccione **SAML 2.0** como tipo de aplicación, como se muestra en la imagen:

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. Introduzca el nombre de la aplicación **Advanced Phishing Protection** y seleccione **Next**, como se muestra en la imagen:

1 General Settings

App name

App logo (optional)

App visibility Do not display application icon to users

Cancel

4. En la configuración de SAML, rellene los espacios, como se muestra en la imagen:

- URL de inicio de sesión único: Este es el servicio de aserción al consumidor obtenido de la protección frente a phishing avanzada de Cisco.

- URL del destinatario: Se trata del ID de entidad obtenido de la protección frente a phishing avanzada de Cisco.

- Formato de ID de nombre: manténgalo como Sin especificar.

- Nombre de usuario de aplicación: Correo electrónico, que solicita al usuario que introduzca su dirección de correo electrónico en el proceso de autenticación.

- Actualizar nombre de usuario de aplicación en: Crear y actualizar.

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](#)

Desplácese hacia abajo hasta **Group Attribute Statement (opcional)**, como se muestra en la imagen:

Introduzca la siguiente sentencia de atributo:

- Nombre: grupo
- Formato del nombre: Sin especificar.
- Filtro: "Igual" y "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"/>

Seleccione Siguiente.

5. Cuando se le solicite que ayude a Okta a entender cómo configuró esta aplicación, introduzca el motivo aplicable al entorno actual, como se muestra en la imagen:

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

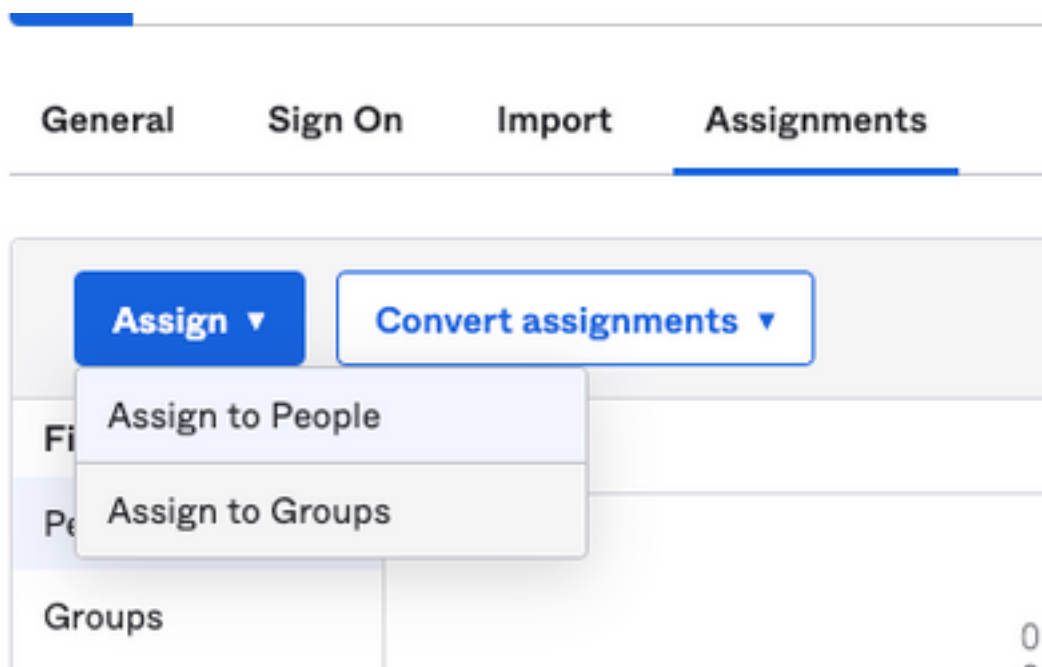
I'm a software vendor. I'd like to integrate my app with Okta

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

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

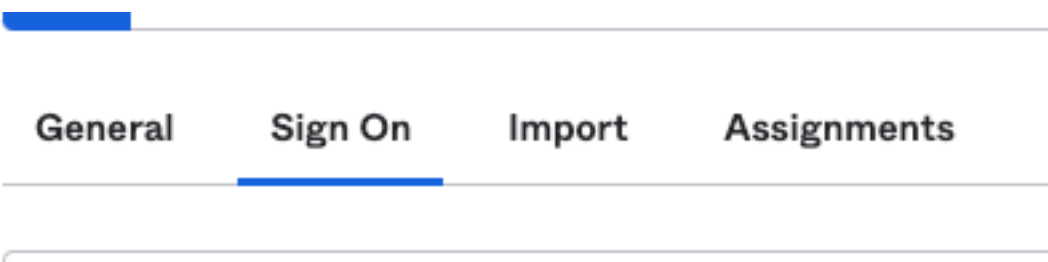
Seleccione **Finish** para continuar con el siguiente paso.

6. Seleccione la pestaña **Asignaciones** y luego seleccione **Asignar > Asignar a Grupos**, como se muestra en la imagen:



7. Seleccione el grupo OKTA, que es el grupo con los usuarios autorizados para acceder al entorno

8. Seleccione **Iniciar sesión**, como se muestra en la imagen:



9. Desplácese hacia abajo y a la esquina derecha, ingrese la opción **Ver instrucciones de configuración SAML**, como se muestra en la imagen:

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. Guarde en un bloc de notas la siguiente información necesaria para poner en el portal de protección frente a phishing avanzada de Cisco, como se muestra en la imagen:

- URL de inicio de sesión único del proveedor de identidad.
- Identifique al proveedor emisor (no es necesario para la protección frente a phishing avanzada de Cisco, pero es obligatorio para otras aplicaciones).
- Certificado 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-----  
MIIDqjOCAPkGw2BAg1GATN/4nF0MA80CSqDS1b3OQEBCwIATAI0VWQswCQjEDVQQOEwAVUzdTRBEG
```

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

[Download certificate](#)

10. Una vez completada la configuración de OKTA, puede volver a la protección frente a phishing avanzada de Cisco

En el portal de protección frente a phishing avanzada de Cisco:


1. Con el Formato del Identificador de Nombre, ingrese la siguiente información:

- Terminal SAML 2.0 (redirección HTTP): La URL de inicio de sesión único del proveedor de identidad proporcionada por Okta.

- Certificado público: Introduzca el certificado X.509 proporcionado por Okta.

2. Seleccione **Test Settings** para verificar que la configuración es correcta

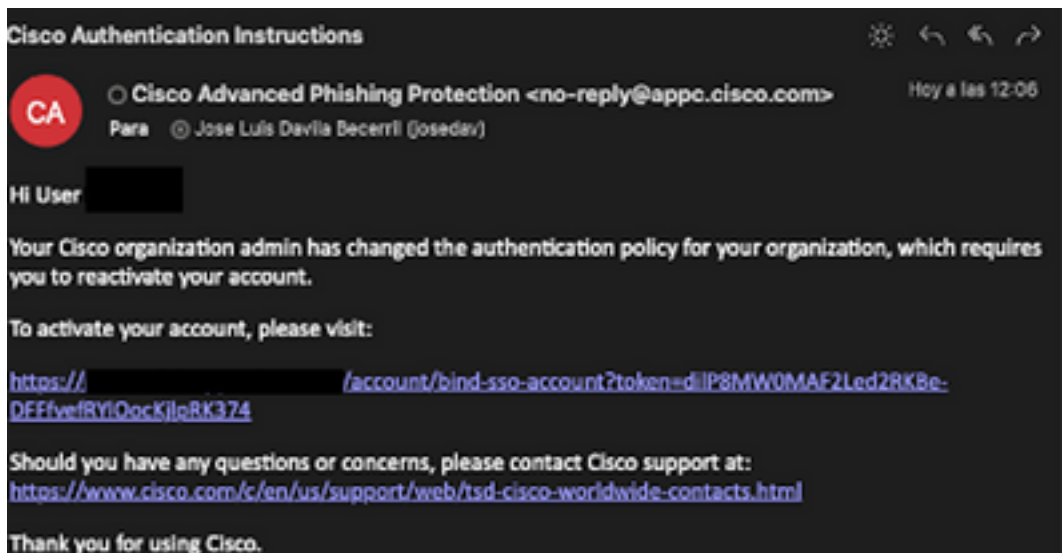
Si no hay errores en la configuración, verá una entrada Test Successful (Prueba correcta) y ahora podrá guardar los parámetros, como se muestra en la imagen:



3. Guardar configuración

Verificación

1. A los administradores existentes que no utilicen SSO se les notifica por correo electrónico que se ha modificado la política de autenticación de la organización y se les pide que activen su cuenta mediante un enlace externo, como se muestra en la imagen:



2. Una vez activada la cuenta, ingrese su dirección de correo electrónico y luego lo redirige al sitio web de inicio de sesión de OKTA para iniciar sesión, como se muestra en la imagen:

Log In to Advanced Phishing Protection

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

Your Email:

[Next](#)

okta

Sign In

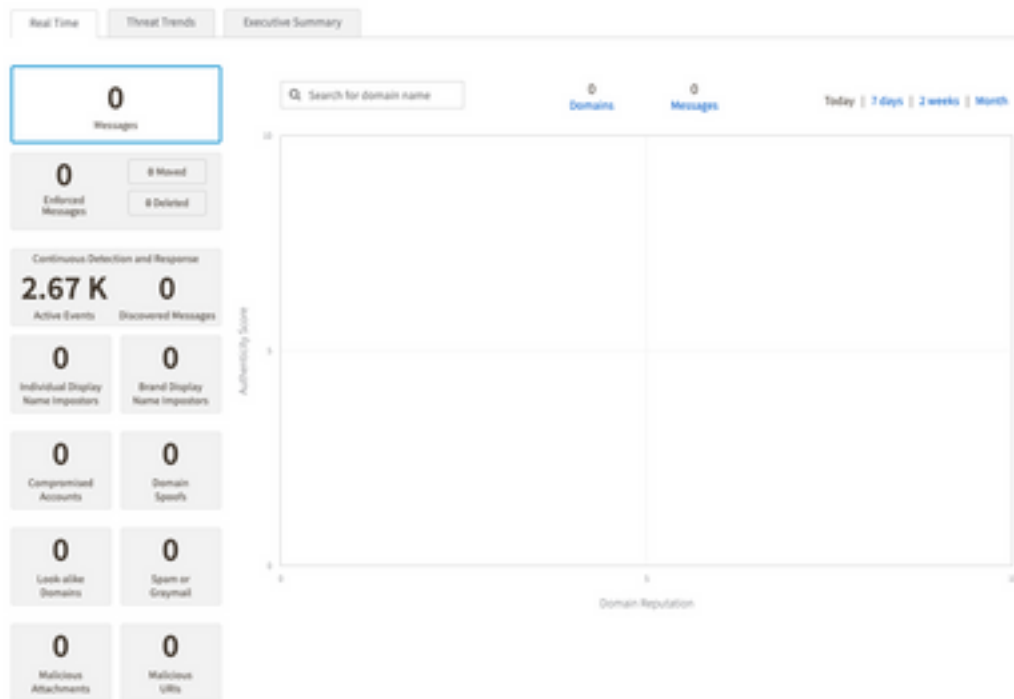
Username

Keep me signed in

[Next](#)

[Help](#)

3. Una vez finalizado el proceso de inicio de sesión de OKTA, inicie sesión en el portal Cisco Advanced Phishing Protection, como se muestra en la imagen:



Información Relacionada

[Protección frente a phishing avanzada de Cisco: información del producto](#)

[Protección frente a phishing avanzada de Cisco: guía del usuario final](#)

[Asistencia para OKTA](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).