

Configurar Autenticação Externa de SSO OKTA para Proteção Avançada contra Phishing

Contents

[Introduction](#)

[Prerequisites](#)

[Informações de fundo](#)

[Requirements](#)

[Configurar](#)

[Verificar](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar a Autenticação Externa OKTA SSO para fazer login no Cisco Advanced Phishing Protection.

Prerequisites

Acesso de administrador ao portal Cisco Advanced Phishing Protection.

Acesso de administrador ao Okta idP.

Certificados SSL X.509 com assinatura automática ou CA (opcional) no formato PKCS #12 ou PEM.

Informações de fundo

- O Cisco Advanced Phishing Protection permite ativar o login SSO para administradores que usam SAML.
- O OKTA é um gerenciador de identidades que fornece serviços de autenticação e autorização para seus aplicativos.
- O Cisco Advanced Phishing Protection pode ser definido como um aplicativo conectado ao OKTA para autenticação e autorização.
- O SAML é um formato de dados padrão aberto baseado em XML que permite que os administradores acessem um conjunto definido de aplicativos perfeitamente após entrarem em um desses aplicativos.
- Para saber mais sobre SAML, você pode acessar o próximo link: [SAML General Information](#)

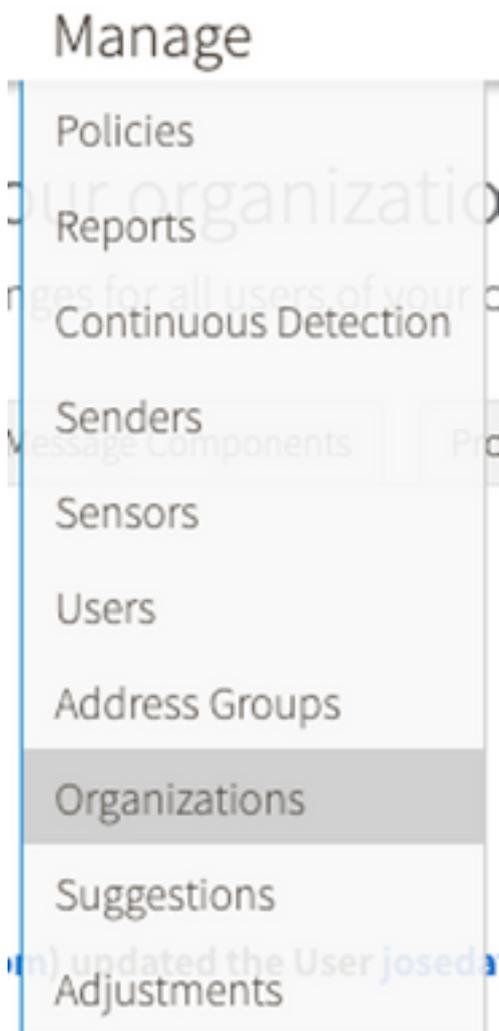
Requirements

- Portal Cisco Advanced Phishing Protection.
- Conta de administrador OKTA.

Configurar

No Cisco Advanced Phishing Protection Portal:

1. Faça login no portal da sua organização e selecione **Gerenciar > Organizações**, como mostrado na imagem:



2. Selecione o nome da sua Organização, **Editar Organização**, conforme mostrado na imagem:

Edit Organization

Alter the settings for this organization.



3. Na guia **Administrative**, role para baixo para **User Account Settings** e selecione **Enable** em SSO, como mostrado na imagem:

User Account Settings

Single Sign-On: Enable

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. A próxima janela fornece as informações a serem especificadas na configuração do SSO OKTA. Cole as seguintes informações em um bloco de notas e use-as para definir as configurações de OKTA:

- ID da entidade: apcc.cisco.com

- Serviço de Consumidor de Asserção: esses dados são personalizados de acordo com a sua organização.

Selecione o formato nomeado **email** para usar um endereço de email para logon, mostrado na imagem:

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:csas:names:tc:SAML:1.1:nameid-format:unspecified
- Name Identifier Format: urn:csas:names:tc:SAML:1.1:nameid-format:emailAddress
- urn:csas:names:tc:SAML:2.0:nameid-format:persistent

5. Minimize a configuração da Cisco Advanced Phishing Protection neste momento, pois você precisa definir primeiro o aplicativo no OKTA antes de passar para as próximas etapas.

Sob Okta.

1. Navegue até o portal Aplicativos e selecione **Criar Integração de Aplicativos**, conforme mostrado na imagem:

Applications



2. Selecione **SAML 2.0** como o tipo de aplicativo, conforme mostrado na imagem:

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. Insira o nome do aplicativo **Advanced Phishing Protection** e selecione **Next**, como mostrado na

imagem:

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. Nas configurações SAML, preencha as lacunas, conforme mostrado na imagem:

- URL de logon único: Este é o Assertion Consumer Service obtido da Cisco Advanced Phishing Protection.
- URL do destinatário: Essa é a ID da entidade obtida do Cisco Advanced Phishing Protection.
- Formato de ID do nome: mantê-lo como Não especificado.
- Nome de usuário do aplicativo: E-mail, que solicita que o usuário insira seu endereço de e-mail no processo de autenticação.
- Atualizar nome de usuário do aplicativo em: Criar e atualizar.

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](#)

Role para baixo até **Group Attribute Statements (optional)**, conforme mostrado na imagem:

Insira a próxima instrução de atributo:

- Nome: grupo
- Formato do nome: Não especificado.
- Filtro: "Iguais" e "OKTA"

Group Attribute Statements (optional)

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

[Add Another](#)

Selecione Avançar.

5. Quando solicitado a ajudar o Okta a entender como você configurou este aplicativo, insira o motivo aplicável para o ambiente atual, como mostrado na imagem:

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

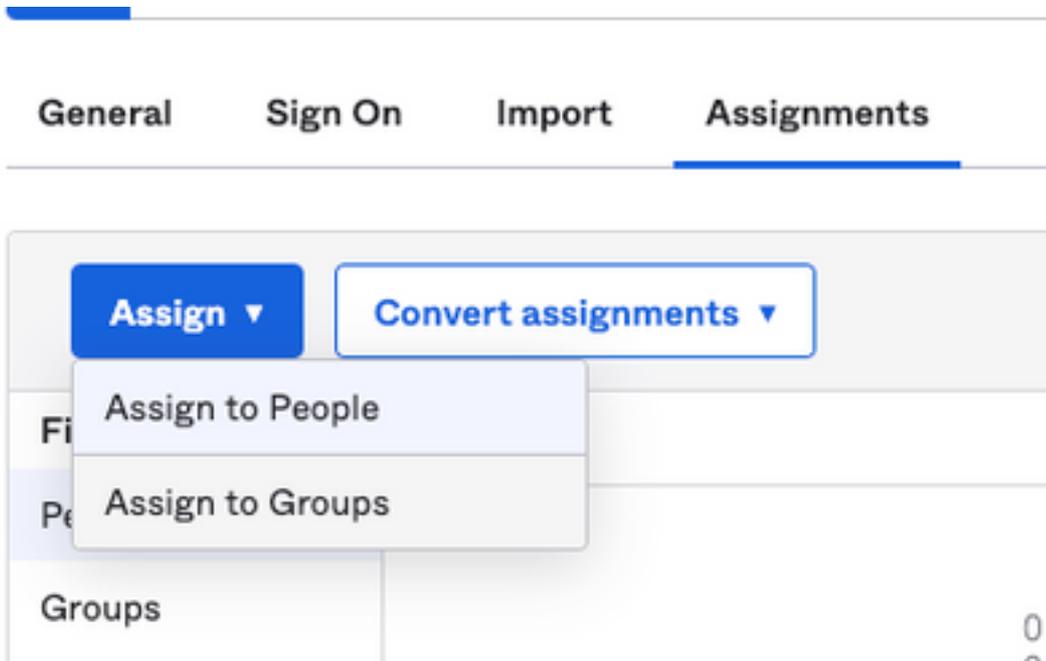
I'm a software vendor. I'd like to integrate my app with Okta

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

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

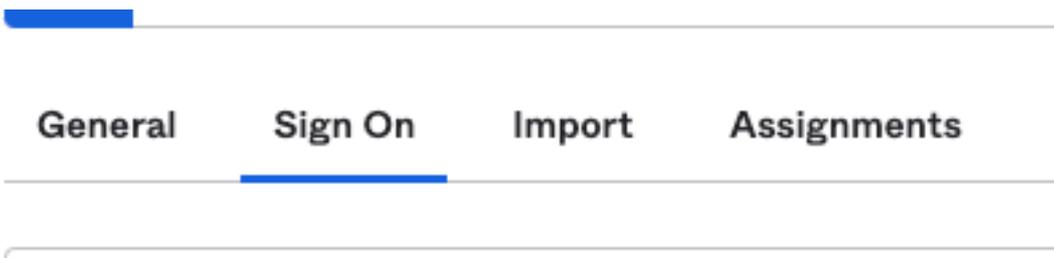
Selecione **Finish** para prosseguir para a próxima etapa.

6. Selecione a guia **Assignments** e, em seguida, selecione **Assign > Assign to Groups**, como mostrado na imagem:



7. Selecione o grupo OKTA, que é o grupo com os usuários autorizados a acessar o ambiente

8. Selecione **Sign On**, conforme mostrado na imagem:



9. Role para baixo e para o canto direito, insira a opção **View SAML setup instructions**, como mostrado na imagem:

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. Salve em um bloco de notas as próximas informações, que são necessárias para colocar no portal Cisco Advanced Phishing Protection, conforme mostrado na imagem:

- URL de logon único do provedor de identidade.

- Identifique o Emissor do Provedor (não é obrigatório para o Cisco Advanced Phishing Protection , mas para outros aplicativos).

- Certificado X.509.

The following is needed to configure Advanced Phishing Protection

- 1 Identity Provider Single Sign-On URL:**
https:// [redacted] /saml
- 2 Identity Provider Issuer:**
http://www.okta.com/
- 3 X.509 Certificate:**
-----BEGIN CERTIFICATE-----
MIIDqJOCAPkGw2BAg1GATN/4nFOMABOC5qGS1b3OQEBCwIAAM1OVWQswCQYEDVQOQeAVUzdTRBEG
-----END CERTIFICATE-----
[Download certificate](#)

10. Depois de concluir a configuração do OKTA, você pode voltar para Cisco Advanced Phishing Protection

No Cisco Advanced Phishing Protection Portal:

1. Com o Formato do identificador de Nome, especifique as próximas informações:

- Ponto de Extremidade SAML 2.0 (Redirecionamento HTTP): A URL de login único do provedor de identificação fornecida pelo Okta.

- Certificado público: Insira o Certificado X.509 fornecido pelo Okta.

2. Selecione **Test Settings** para verificar se a configuração está correta

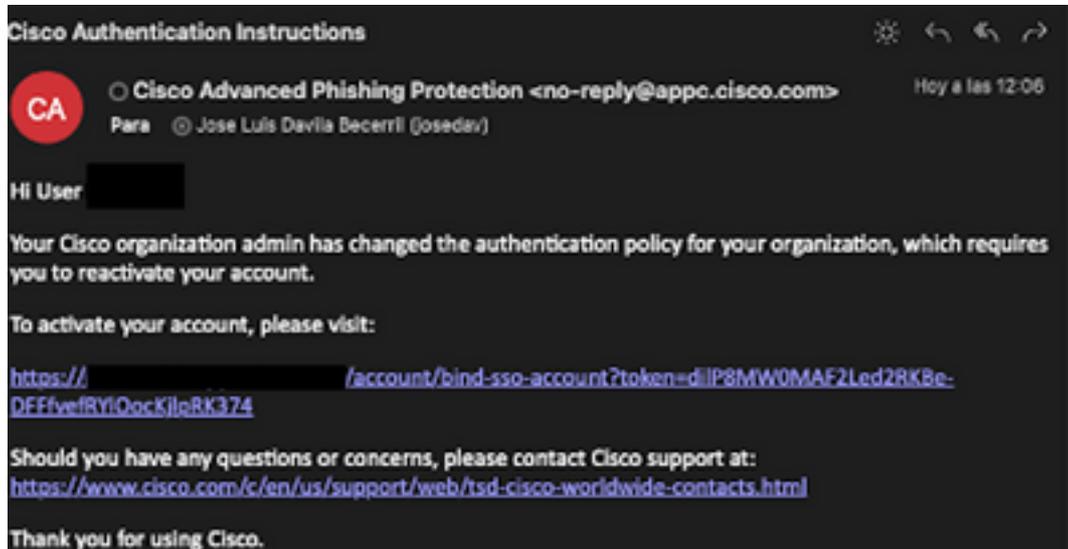
Se não houver erros na configuração, você verá uma entrada Test Successful e agora poderá salvar suas configurações, como mostrado na imagem:

Success — Test Successful You may now save your settings.

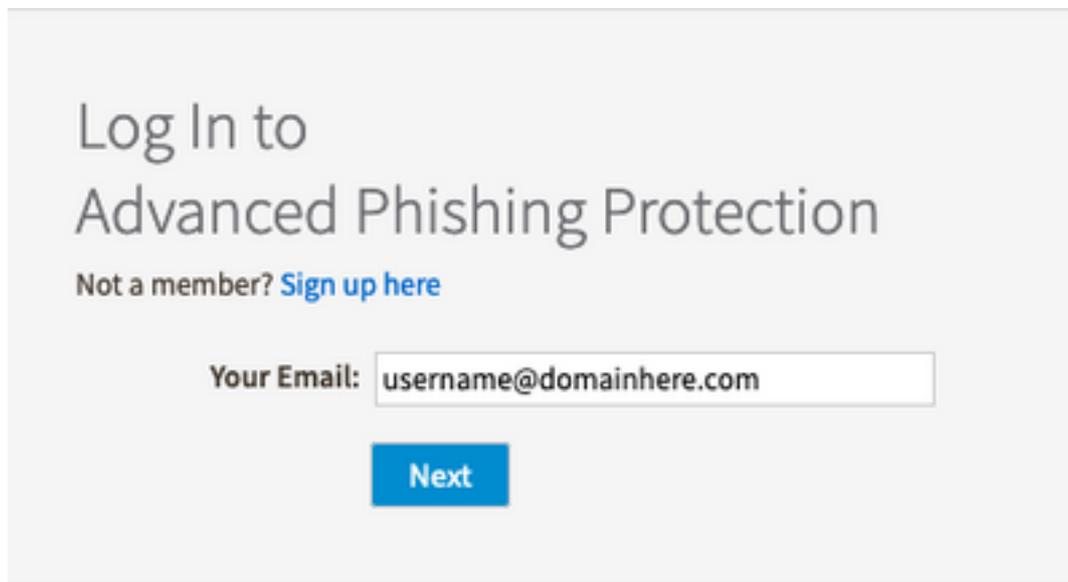
3. Salvar configurações

Verificar

1. Para qualquer administrador existente que não use o SSO, ele é notificado por e-mail de que a política de autenticação é alterada para a organização e os administradores são solicitados a ativar sua conta usando um link externo, como mostrado na imagem:



2. Uma vez que a conta é ativada, digite seu endereço de e-mail e, em seguida, ele o redireciona para o site de login OKTA para login, como mostrado na imagem:





Sign In

Username

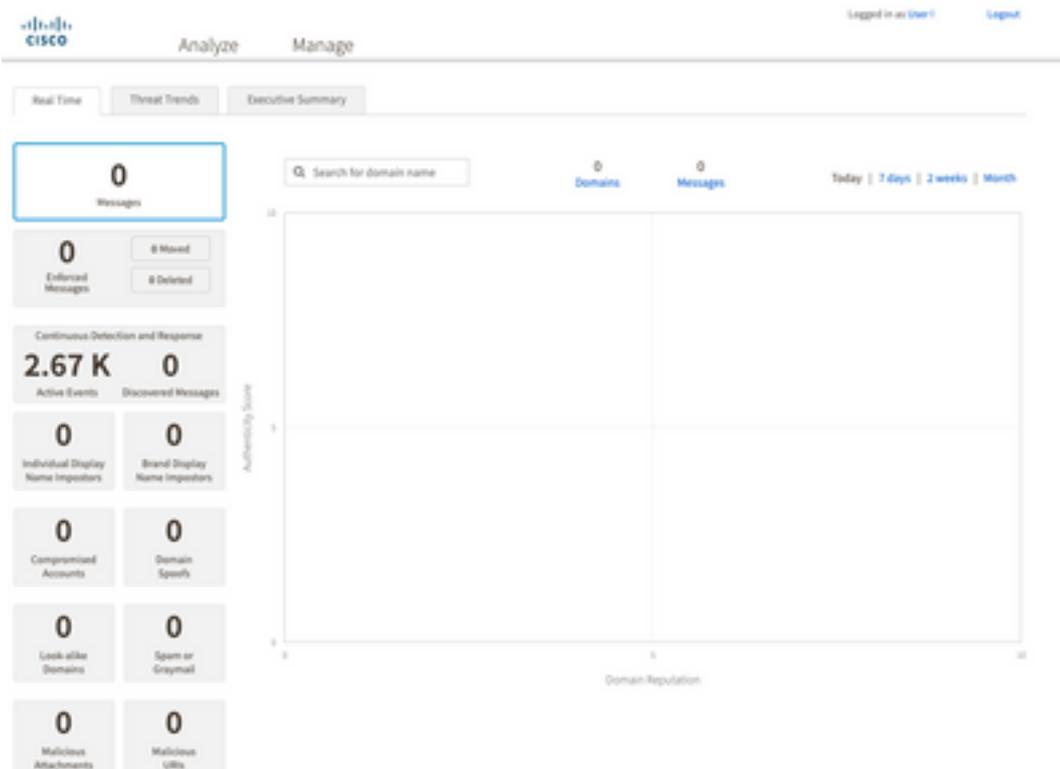
username@domainhere.com

Keep me signed in

Next

Help

3. Quando o processo de login do OKTA for concluído, faça login no portal Cisco Advanced Phishing Protection, como mostrado na imagem:



Informações Relacionadas

[Cisco Advanced Phishing Protection - Informações do produto](#)

[Cisco Advanced Phishing Protection - Guia do usuário final](#)

[Suporte OKTA](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.