Configurar Autenticação Externa de SSO OKTA para Proteção Avançada contra Phishing

Contents

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

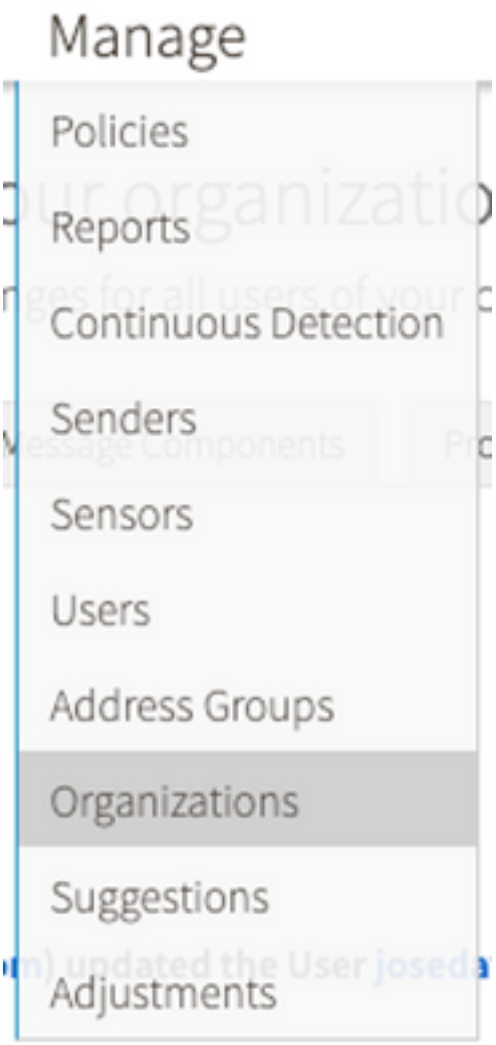
Requirements

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

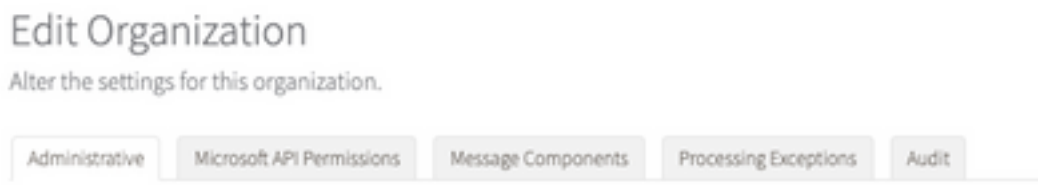
Configurar

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:



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

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.

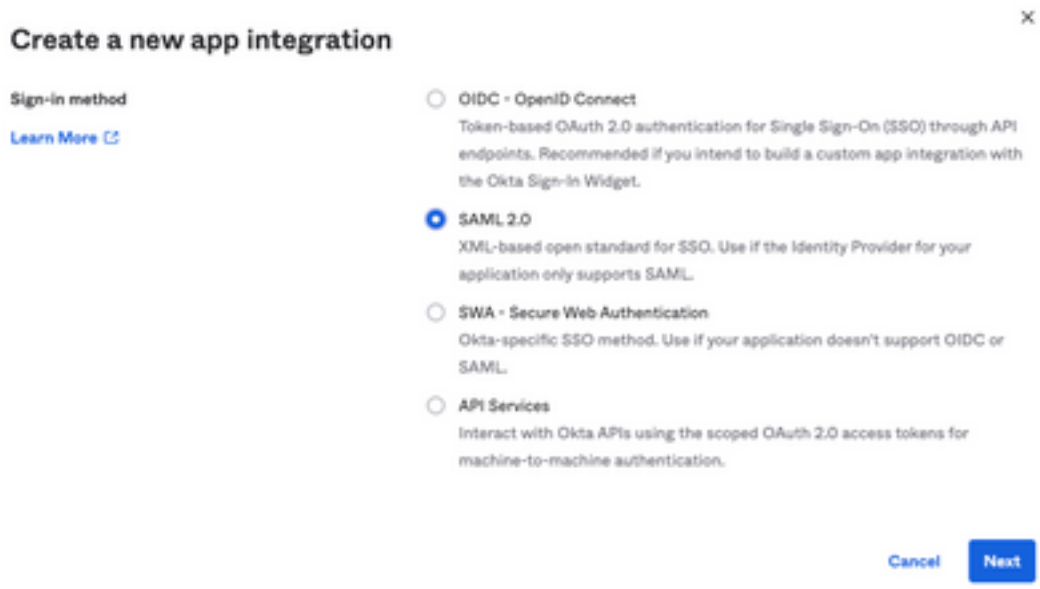
Selecione o formato nomeado **email** para usar um endereço de email para logon, mostrado na imagem:

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.

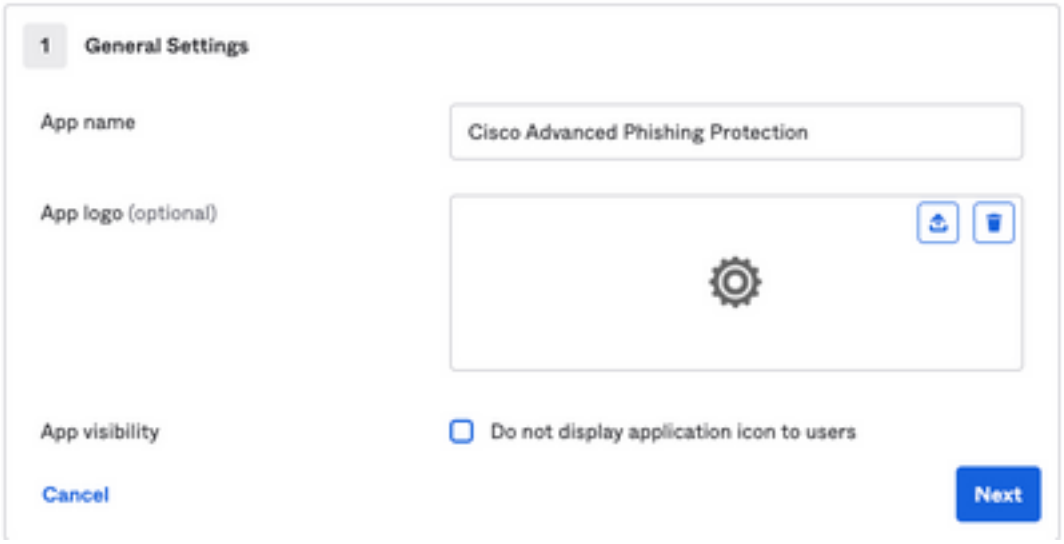
1. Navegue até o portal Aplicativos e selecione **Criar Integração de Aplicativos**, conforme mostrado na imagem:

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



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

imagem:



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

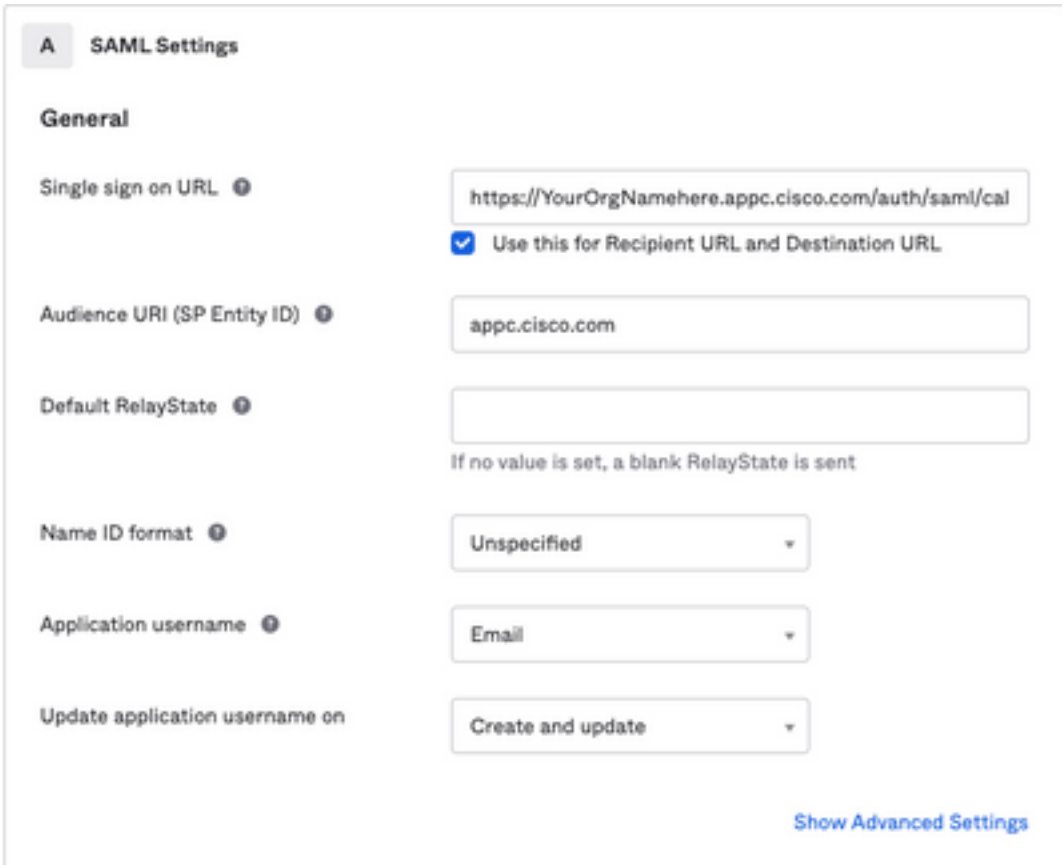
- URL de logon único: Este é o Assertion Consumer Service obtido da Cisco Advanced Phishing Protection.

- 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.



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

Insira a próxima instrução de atributo:

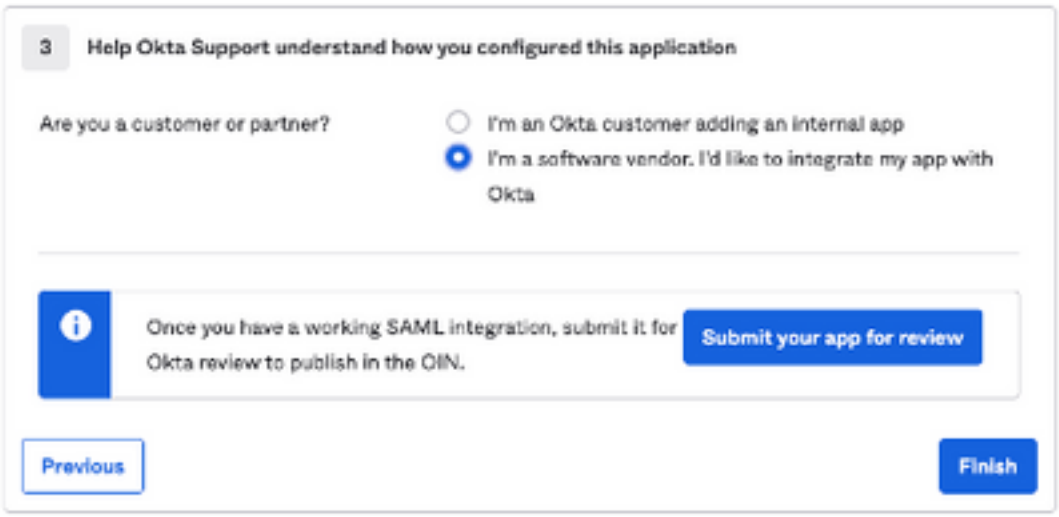
-Nome: grupo

- Formato do nome: Não especificado.

-Filtro: "Iguais" e "OKTA"

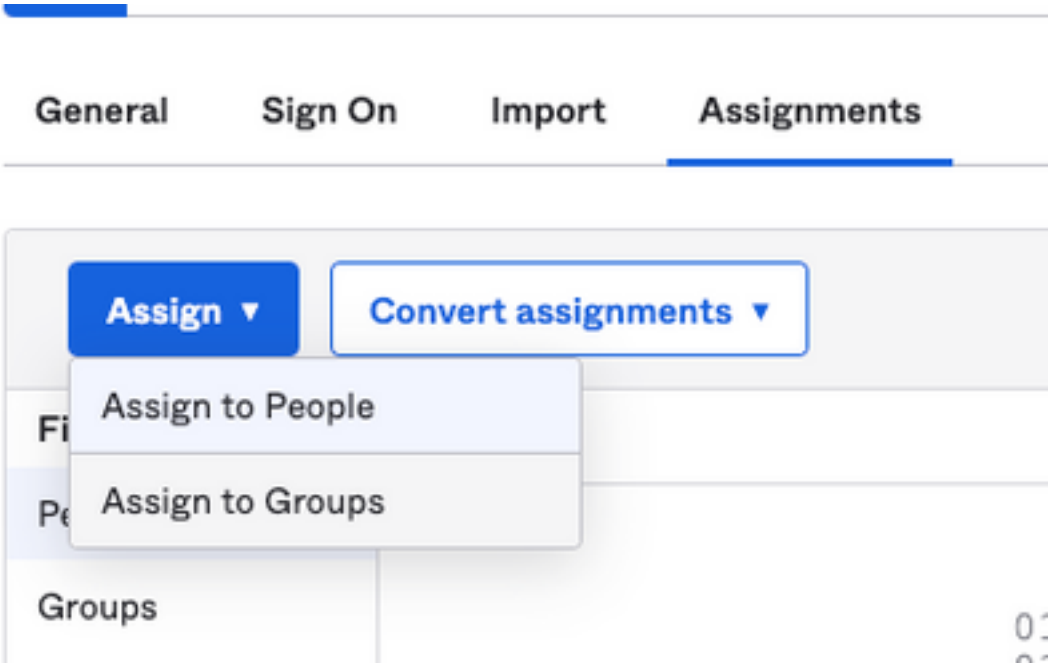
Selecione Avançar.

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:



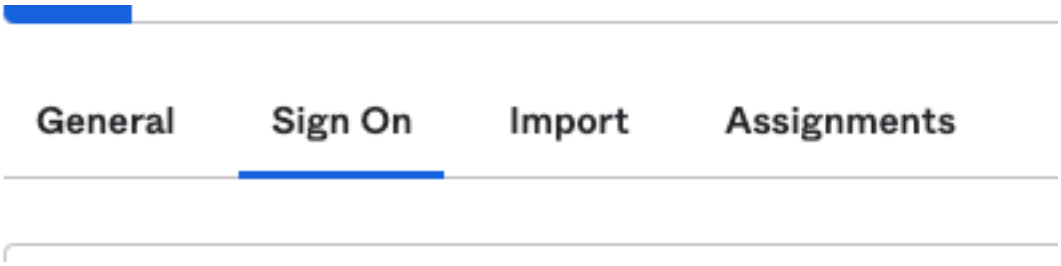
Selecione **Finish** para prosseguir para a próxima etapa.

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

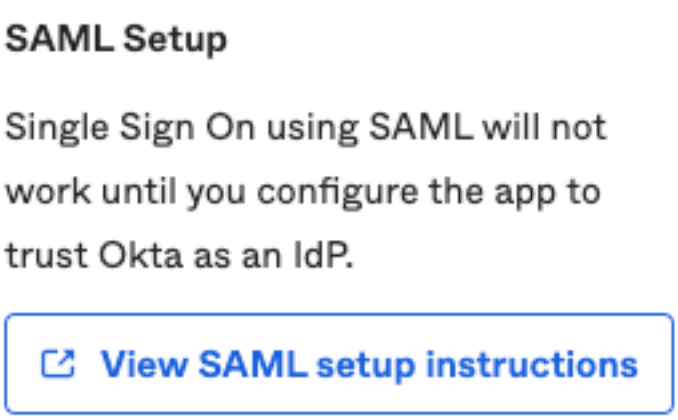


7. Selecione o grupo OKTA, que é o grupo com os usuários autorizados a acessar o ambiente

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:

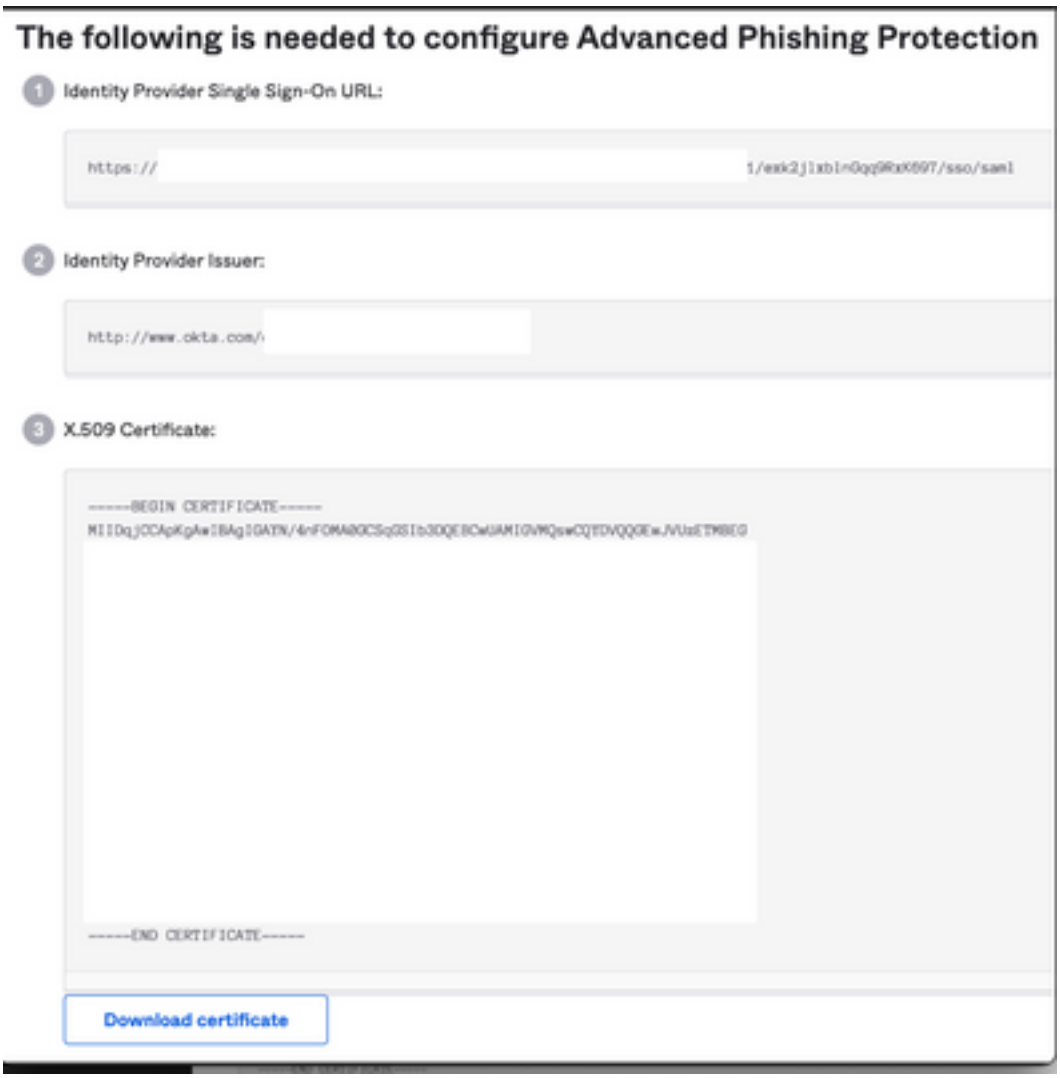


9. Salve em um bloco de notas as próximas informações, que são necessárias para colocar no portal Cisco Advanced Phishing Protection, conforme mostrado na imagem:

- 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.



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

No Cisco Advanced Phishing Protection Portal:

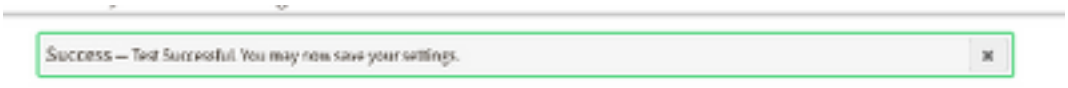
1. Com o Formato do identificador de Nome, especifique as próximas informações:

- 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

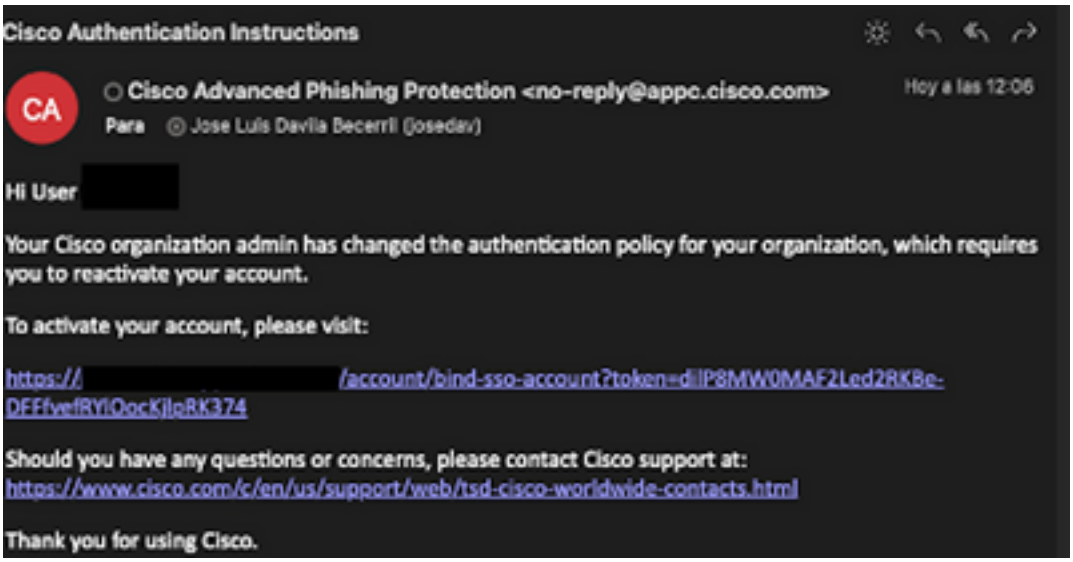
Se não houver erros na configuração, você verá uma entrada Test Successful e agora poderá salvar suas configurações, como mostrado na imagem:



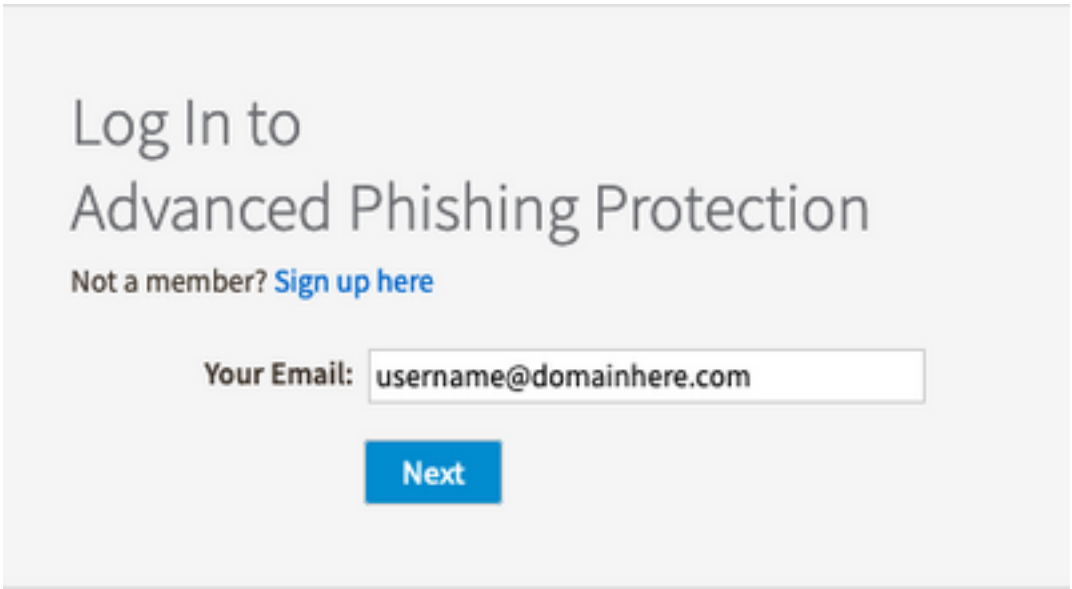
3. Salvar configurações

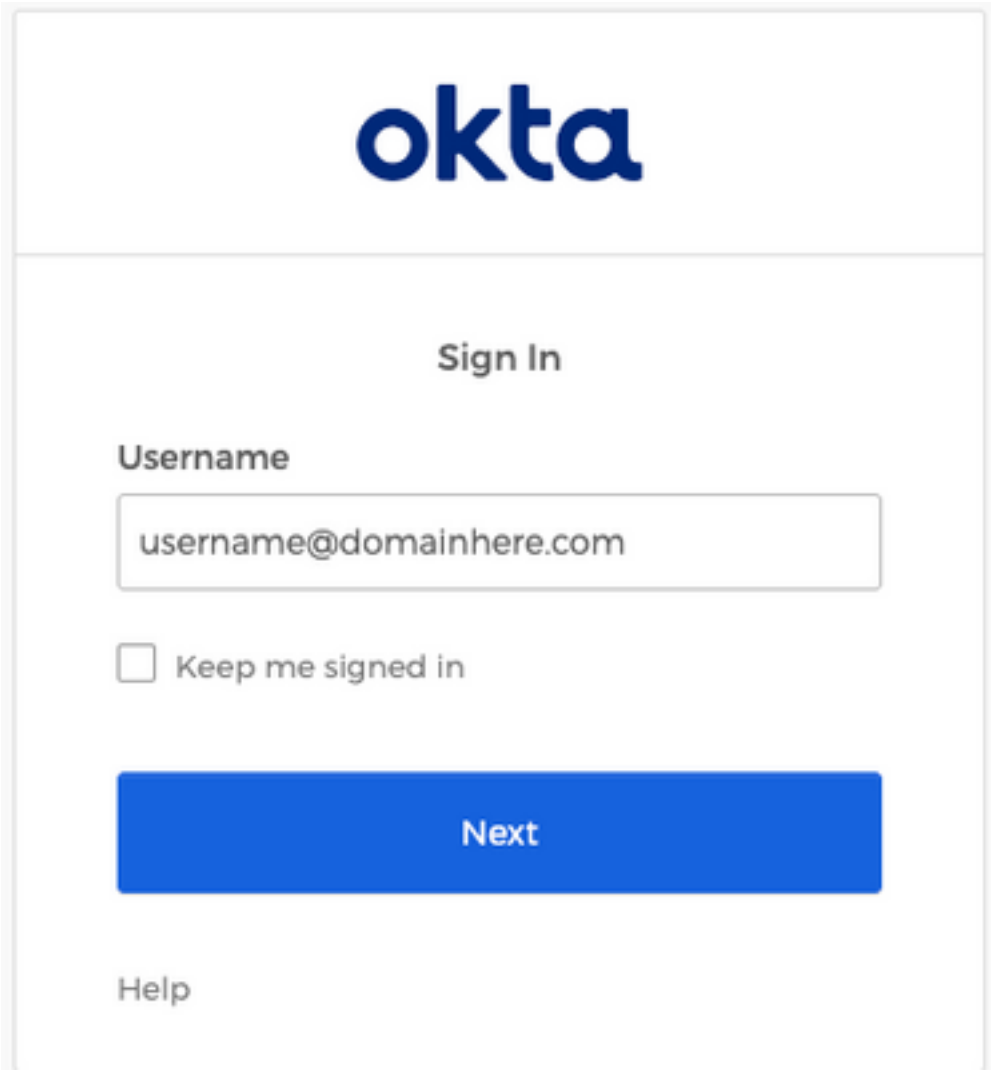
Verificar

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:

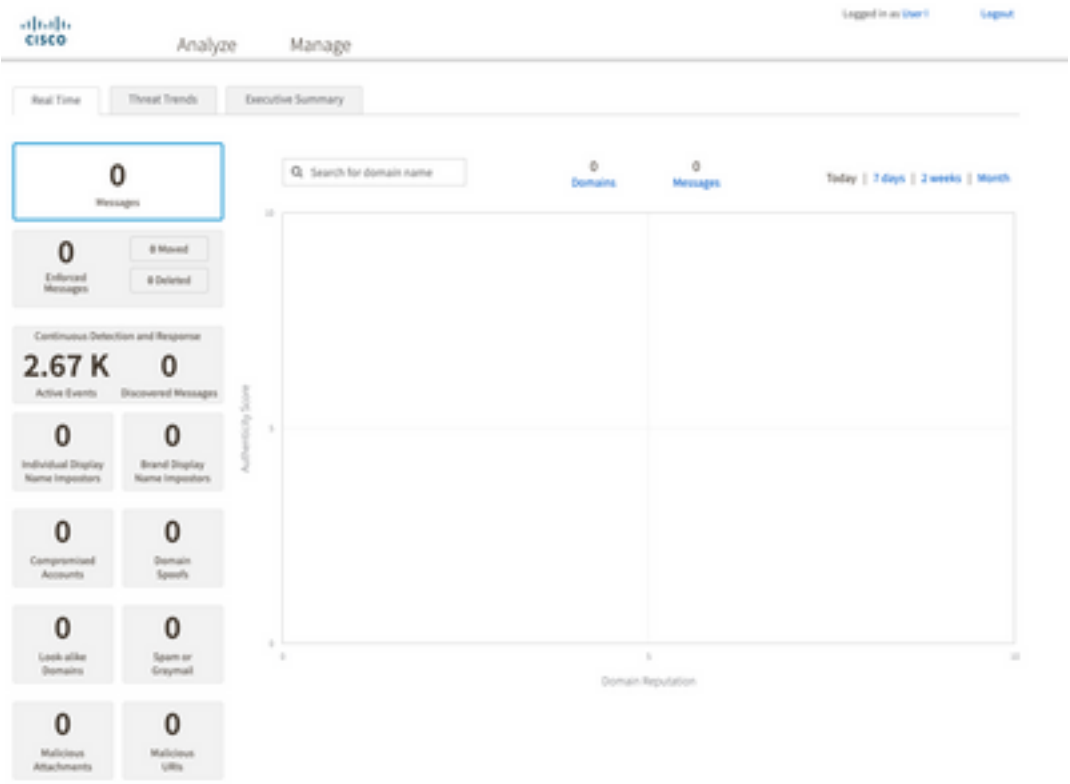


2. Uma vez que a conta é ativada, digite seu endereço de e-mail e, em seguida, ele o redireciona para o site de login OKTA para login, como mostrado na imagem:





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.