

Configurar SSO OKTA para quarentena de spam de usuário final

Contents

[Introduction](#)

[Prerequisites](#)

[Informações de Apoio](#)

[Componentes](#)

[Configurar](#)

[Verificar](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o SSO OKTA para fazer login na Quarentena de spam do usuário final do Security Management Appliance.

Prerequisites

- Acesso de administrador ao Cisco Security Management Appliance.
- Acesso de administrador ao OKTA.
- Certificados SSL X.509 com assinatura automática ou CA (opcional) no formato PKCS #12 ou PEM (fornecido pelo OKTA).

Informações de Apoio

O Cisco Security Management Appliance permite o login SSO para usuários finais que usam a Quarentena de spam do usuário final e se integra ao OKTA, que é um gerenciador de identidades que fornece serviços de autenticação e autorização para seus aplicativos. A Quarentena de spam do usuário final da Cisco pode ser definida como um aplicativo que está conectado ao OKTA para autenticação e autorização, e usa SAML, um formato de dados padrão aberto baseado em XML que permite aos administradores acessar um conjunto definido de aplicativos sem interrupções após o login em um desses aplicativos.

Para saber mais sobre SAML, consulte: [Informações Gerais de SAML](#)

Componentes

- Conta de administrador de nuvem do Cisco Security Management Appliance.
- Conta de administrador OKTA.

The information in this document was created from the devices in a specific lab environment. Todos os dispositivos usados neste documento foram iniciados com uma configuração limpa (padrão). se a rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando.

Configurar

Sob Okta.

1. Navegue até o portal Aplicativos e escolha **Create App Integration**, conforme mostrado na imagem:

Applications

Create App Integration

Browse App Catalog

Assign Users to App

More ▾

2. Escolha **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. Informe o nome do Aplicativo **SMA EUQ** e escolher **Next**, conforme mostrado na imagem:

1 General Settings

App name

SMA EUQ

App logo (optional)



App visibility

Do not display application icon to users

Cancel

Next

4. Nos termos do SAML settings, preencha as lacunas, conforme mostrado na imagem:

- URL de logon único: este é o Serviço de Consumidor de Asserção obtido da interface EUQ do SMA.

- URI da Audiência (ID da Entidade SP): é a ID da Entidade obtida da ID da Entidade EUQ do SMA.

- Formato de ID do nome: mantenha-o 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 ⓘ
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: group

- Formato do nome: Unspecified

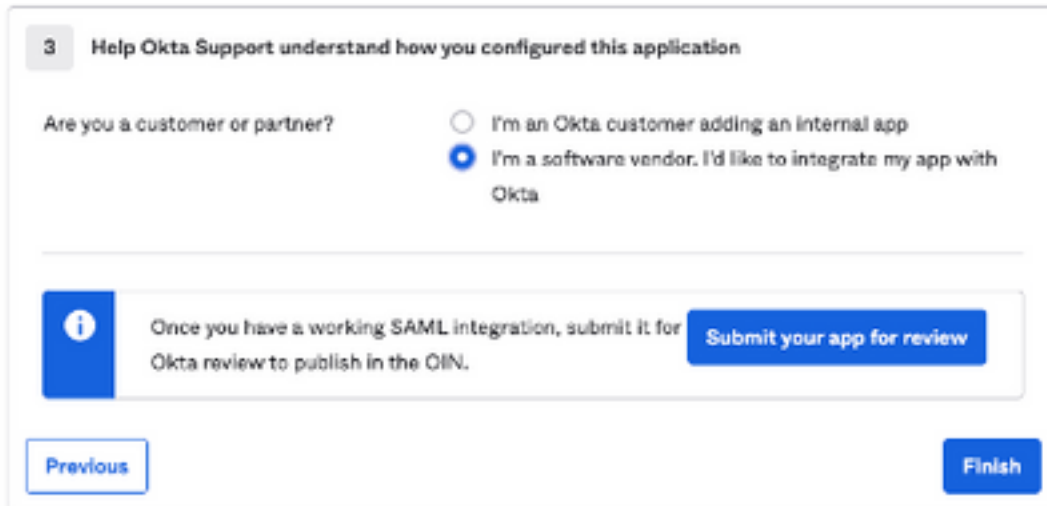
-Filtro: Equals e OKTA

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"/>

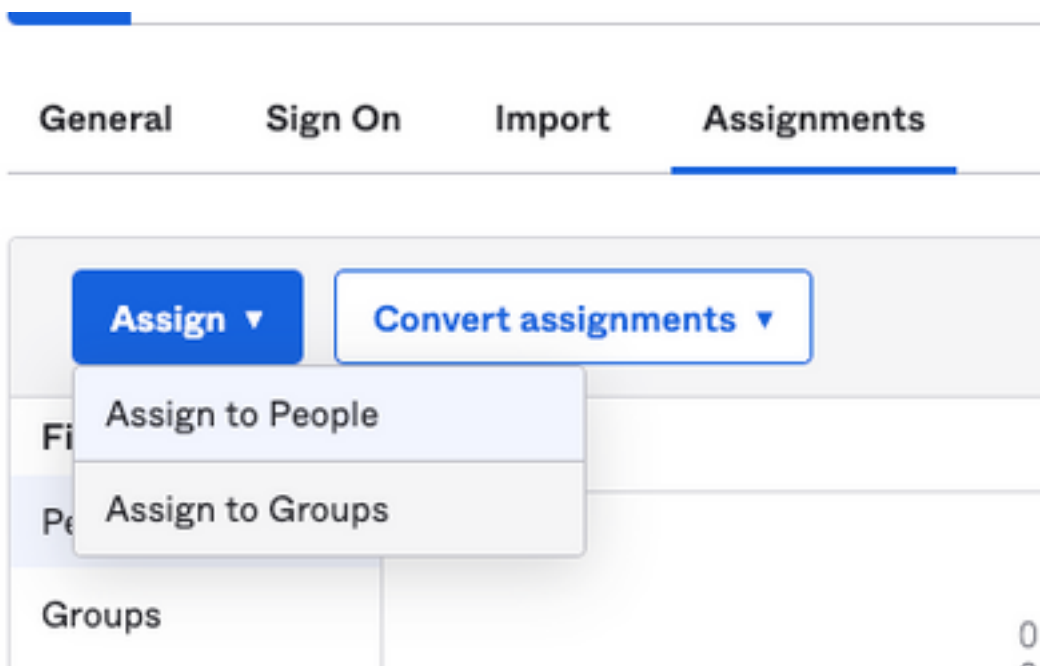
Selecionar Next .

5. Quando solicitado a Help Okta to understand how you configured this application, insira o motivo aplicável para o ambiente atual, como mostrado na imagem:



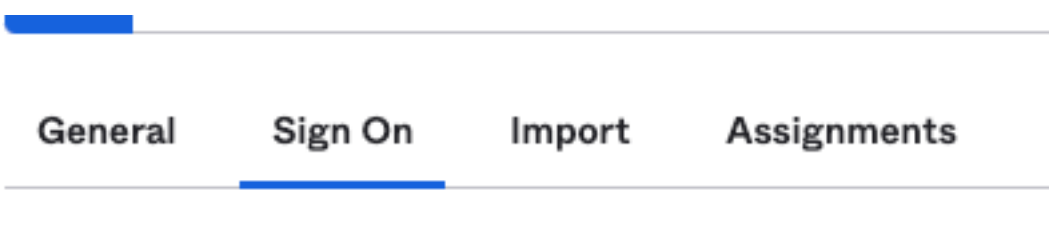
Escolher Finish para prosseguir para a próxima etapa.

6. Escolha Assignments e selecione Assign > Assign to Groups, conforme mostrado na imagem:



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

8. Escolha Sign On , conforme mostrado na imagem:



9. Role para baixo e, para o canto direito, escolha o botão 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](#)

10. Salve essas informações em um bloco de notas, é necessário colocá-las no Cisco Security Management Appliance Configuração SAML, como mostrado na imagem:

- URL de Logon Único do Provedor de Identidade
- Emissor do provedor de identidade
- Certificado X.509

The following is needed to configure CRES

1 Identity Provider Single Sign-On URL:

https://

2 Identity Provider Issuer:

http://www.okta.com/

3 X.509 Certificate:

-----BEGIN CERTIFICATE-----

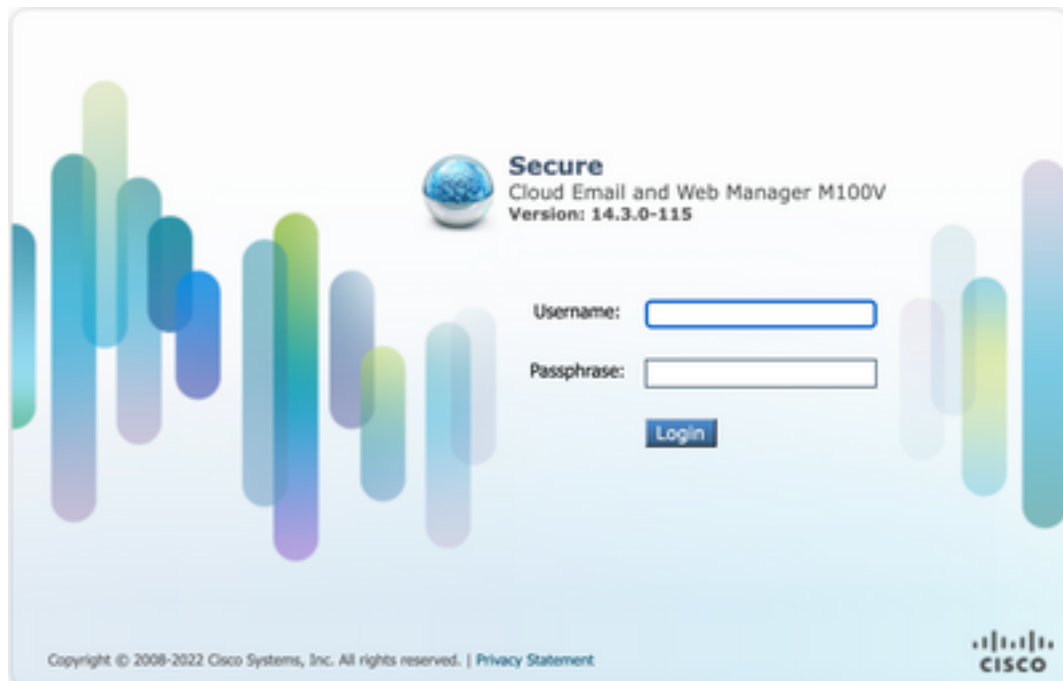
-----END CERTIFICATE-----

[Download certificate](#)

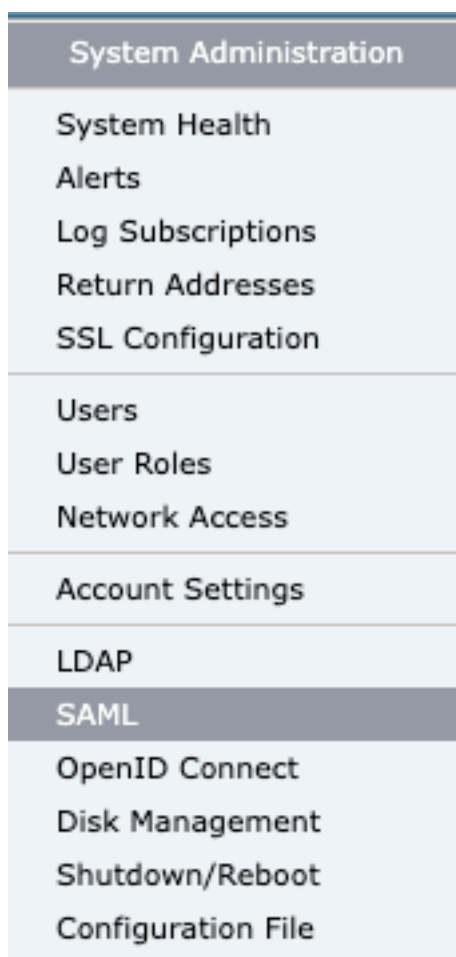
11. Depois de concluir a configuração do OKTA, você pode voltar para o Cisco Security Management Appliance.

No Cisco Security Management Appliance:

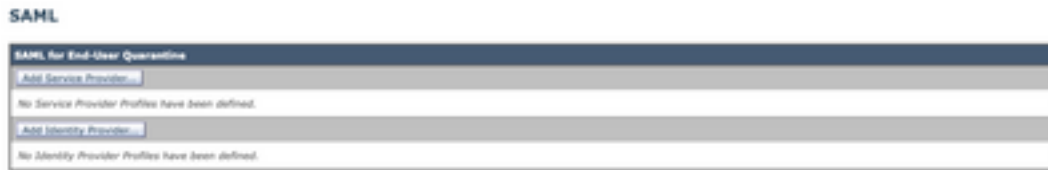
1. Faça login no Cisco Security Management Appliance como um administrador de nuvem, conforme mostrado na imagem:



2. No System Administration, escolha o SAML , como mostrado na imagem:



3. Uma nova janela é aberta para configurar o SAML. Sob SAML for End-User Quarantine, clicar Add Service Provider ,conforme mostrado na imagem:



4. Nos termos do Profile Name , insira um Nome de perfil para o perfil do provedor de serviços, conforme mostrado na imagem:

Profile Name:

5. Para Entity ID , insira um nome globalmente exclusivo para o provedor de serviços (nesse caso, seu equipamento). O formato do ID da entidade do provedor de serviços é geralmente um URI, como mostrado na imagem:

Entity ID:

6. Para Name ID Format , esse campo não é configurável. Você precisa desse valor ao configurar o provedor de identidade, como mostrado na imagem:

Name ID Format:

7. Para Assertion Consumer URL, insira a URL para a qual o provedor de identidade envia a asserção SAML depois que a autenticação tiver sido concluída com êxito. Neste caso, este é o URL para a quarentena de spam.

Assertion Consumer URL:

8. Para SP Certificate , carregue o certificado e a chave ou carregue o arquivo de #12 PKCS. Após o upload, o Uploaded Certificate Details é exibido, como mostrado na imagem:

Uploaded Certificate Details:

Issuer: (:1-
(\O=Cisco\ST=CDMX\OU=ESA TAC

Subject: (:1-
(\O=Cisco\ST=CDMX\OU=ESA TAC

Expiry Date: ! GMT

9. Para Sign Requests and Sign Assertions , marque ambas as caixas de seleção se desejar assinar as solicitações e Asserções SAML. Se você selecionar essas opções, certifique-se de definir as mesmas configurações no OKTA, como mostrado na imagem:

Sign Requests

Sign Assertions

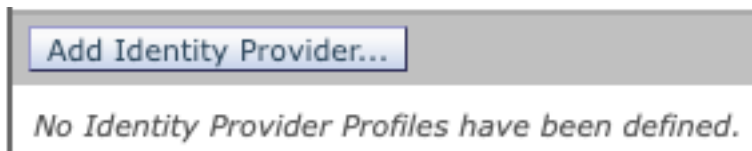
Make sure that you configure the same settings on your Identity Provider as well.

10. Para Organization Details, insira os detalhes de sua organização, como mostrado na imagem:

Organization Details:	Name:	<input type="text" value="EUQ SAML APP"/>
	Display Name:	<input type="text" value="https://-euq1.iphmx.com/"/>
	URL:	<input type="text" value="https://-euq1.iphmx.com/"/>
Technical Contact:	Email:	<input type="text" value="useradmin@domainhere.com"/>

11. Submit e Commit alterações antes de continuar a configurar Identity Provider Settings .

12. Nos termos do SAML , clique em Add Identity Provider, conforme mostrado na imagem:



13. Ao abrigo do Profile Name: digite um nome para o perfil do provedor de identidade, como mostrado na imagem:

Profile Name:	<input type="text" value="iDP Profile"/>
---------------	--

14. Selecione Configure Keys Manually e insira essas informações, conforme mostrado na imagem:

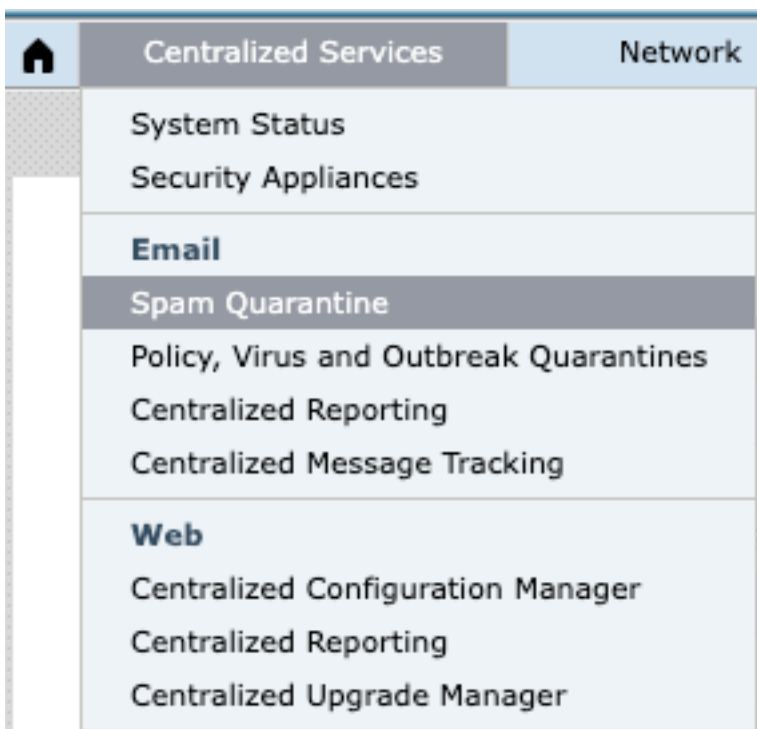
- ID da entidade: o ID da entidade do provedor de identidade é usado para identificar exclusivamente o provedor de identidade. Ele é obtido das configurações OKTA nas etapas anteriores.
- URL do SSO: o URL para o qual o SP deve enviar solicitações SAML Auth. Ele é obtido das configurações OKTA nas etapas anteriores.
- Certificado: o certificado fornecido pelo OKTA.

The image shows the "Configuration Settings" section with the "Configure Keys Manually" option selected. The form contains the following fields:

- Entity ID:
- SSO URL:
- Certificate: Sin archivos seleccionados
- Uploaded Certificate Details:
- Issuer:
- Subject:
- Expiry Date:

15. Submit e Commit as alterações para continuar com a ativação de login SAML.

16. Ao abrigo do Centralized Services > Email , clique em Spam Quarantine, conforme mostrado na imagem:



17. Ao abrigo do Spam Quarantine -> Spam Quarantine Settings , clique em Edit Settings , as shown in the image:



18. Role para baixo até End-User Quarantine Access > End-User Authentication , selecione SAML 2.0 , conforme mostrado na imagem:



19. Submit e Commit alterações para habilitar a Autenticação SAML para End User Spam Quarantine .

Verificar

1. Em qualquer navegador da Web, insira o URL da Quarentena de spam do usuário final de sua empresa, como mostrado na imagem:



2. Uma nova janela é aberta para continuar com a autenticação OKTA. Entre com as credenciais OKTA, como mostrado na imagem:



Sign In

Username

Keep me signed in

Next

Help

3. Se a Autenticação for bem-sucedida, o End User Spam Quarantine abre o conteúdo da Quarentena de spam para o usuário que entra, como mostrado na imagem:



Agora, o usuário final pode acessar a Quarentena de spam do usuário final com credenciais OKTA. .

Informações Relacionadas

[Guias do Usuário Final do Cisco Secure Email e Web Manager](#)

[Suporte a 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.