Configurar SSO SAML do Okta para quarentena de usuário final do SMA

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Configuração
  - Configurar o provedor de serviços (SP) no dispositivo SMA
  - Configurar o aplicativo SAML no Okta
  - Configurar o provedor de identidade (IdP) no dispositivo SMA
  - Atribuir usuários ao aplicativo Okta
  - Configurar MFA no Okta (opcional)
  - Verificar login SAML

Introdução

Este documento descreve como configurar o Okta como o provedor de identidade SAML 2.0 para o acesso à quarentena do usuário final do Cisco Secure Email SMA.

Pré-requisitos

- Produto: Cisco Secure Email Security Management Appliance (SMA)
- Recurso: SAML SSO para EUQ (Quarentena de usuário final)
- Provedor de identidade: Okta (SAML 2.0)
- Aplicável a: Implantações de SMA que fornecem acesso EUQ em plataformas virtuais ou de hardware. Substitua nomes de host e portas de exemplo por valores do seu ambiente.
- Contexto da versão: Este procedimento se aplica às versões do SMA que suportam SAML para EUQ. Verifique os campos disponíveis e as opções de menu na versão instalada.

Note: Este documento se concentra na configuração SMA EUQ SAML. O ESA é referenciado somente para geração de certificado quando o SMA não pode gerar um certificado autoassinado.

Requisitos

Antes de começar, verifique se você tem:

- Acesso administrativo à interface da Web do SMA.
- Permissões administrativas no Okta para criar aplicativos SAML 2.0 e atribuir usuários ou grupos.
- Um certificado e uma chave privada para a configuração do provedor de serviços do SMA. Um certificado autoassinado é aceitável para teste.
- Um FQDN (nome de domínio totalmente qualificado) EUQ SMA acessível e uma porta que os usuários finais podem acessar de seus navegadores.
- A URL de Asserção SAML do SMA e os valores de ID da entidade SP (em Administração do sistema > SAML depois que você cria a entrada SP).
- Contas de usuário no Okta que são atribuídas ao aplicativo Okta.
- Usuários sincronizados com o diretório, se a distribuição usar integração com o diretório.

Note: Okta é um provedor de identidade terceirizado. Este documento fornece uma configuração de exemplo para referência do cliente.

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

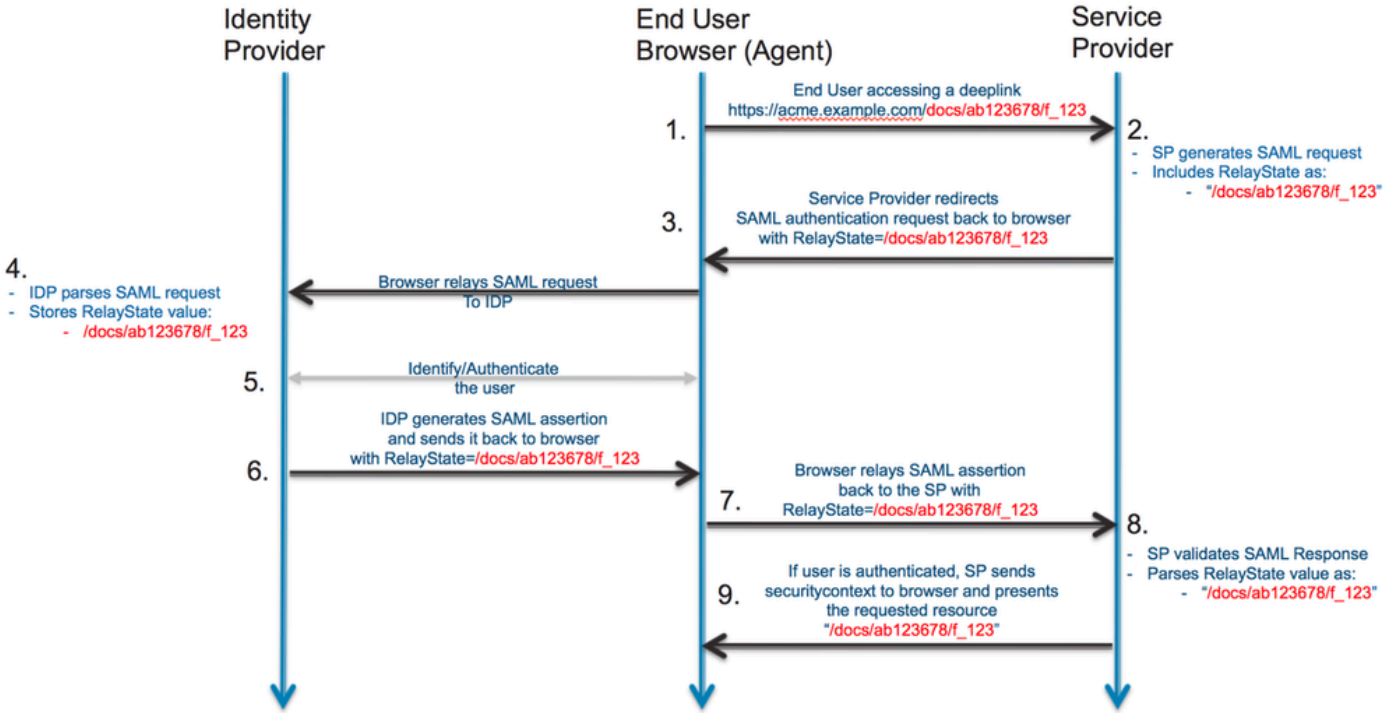
Informações de Apoio

O objetivo é configurar o logon único (SSO) para o portal de quarentena de spam, de modo que os usuários sejam redirecionados para o Okta para autenticar, completar a autenticação multifator (MFA) se estiver habilitada no Okta e, em seguida, retornar ao portal EUQ do SMA. Este documento se aplica somente ao SMA. O Cisco Secure Email Gateway, anteriormente conhecido como Email Security Appliance (ESA), é mencionado somente para a geração de certificado quando o SMA não pode gerar um certificado autoassinado.

Problema: Os usuários devem se autenticar no portal de quarentena de spam do SMA com o Okta usando o SAML SSO e o MFA opcional.

Resolução: Configure o SMA como o provedor de serviços, configure um aplicativo SAML no Okta, importe as configurações do IdP do Okta para o SMA, atribua usuários no Okta e verifique o acesso.

Fluxo SAML:



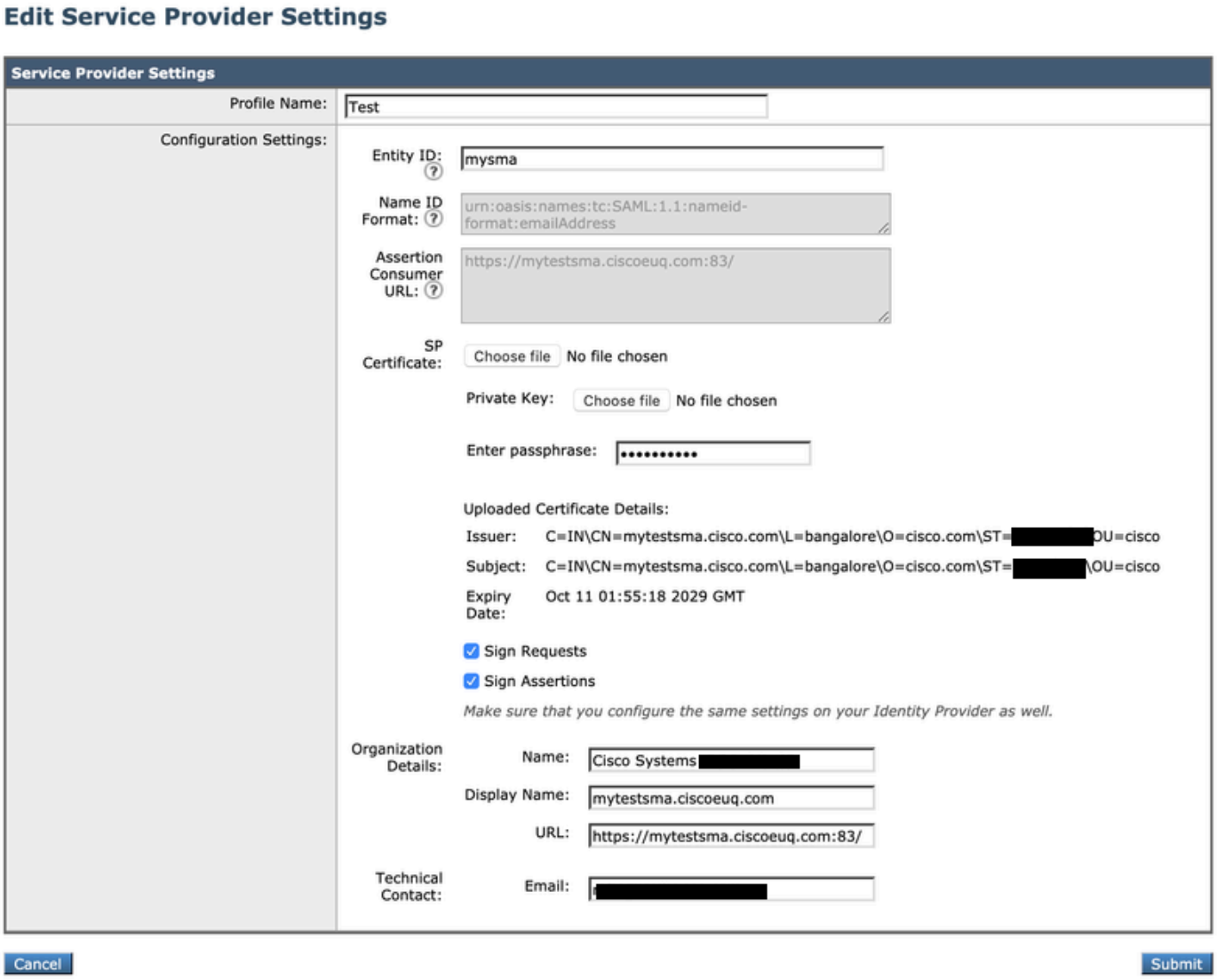
Configuração

Configurar o provedor de serviços (SP) no dispositivo SMA

Para configurar o SMA como um provedor de serviços SAML para acesso EUQ, siga estas etapas:

1. Faça login na interface da Web do SMA .
2. Navegue até Administração do sistema > SAML.
3. Selecione Adicionar provedor de serviços.
4. Em ID de entidade do provedor de serviços, insira a ID da entidade que você também pode configurar no Okta.
5. Verifique se Name ID Format e a URL do Assertion Consumer Service (ACS) estão preenchidos para a interface EUQ.
6. Em Certificado SP, carregue um certificado para assinar solicitações SAML.

Note: O SMA não pode gerar um certificado autoassinado. Você também pode gerar um certificado em um ESA e exportá-lo para uso no SMA.

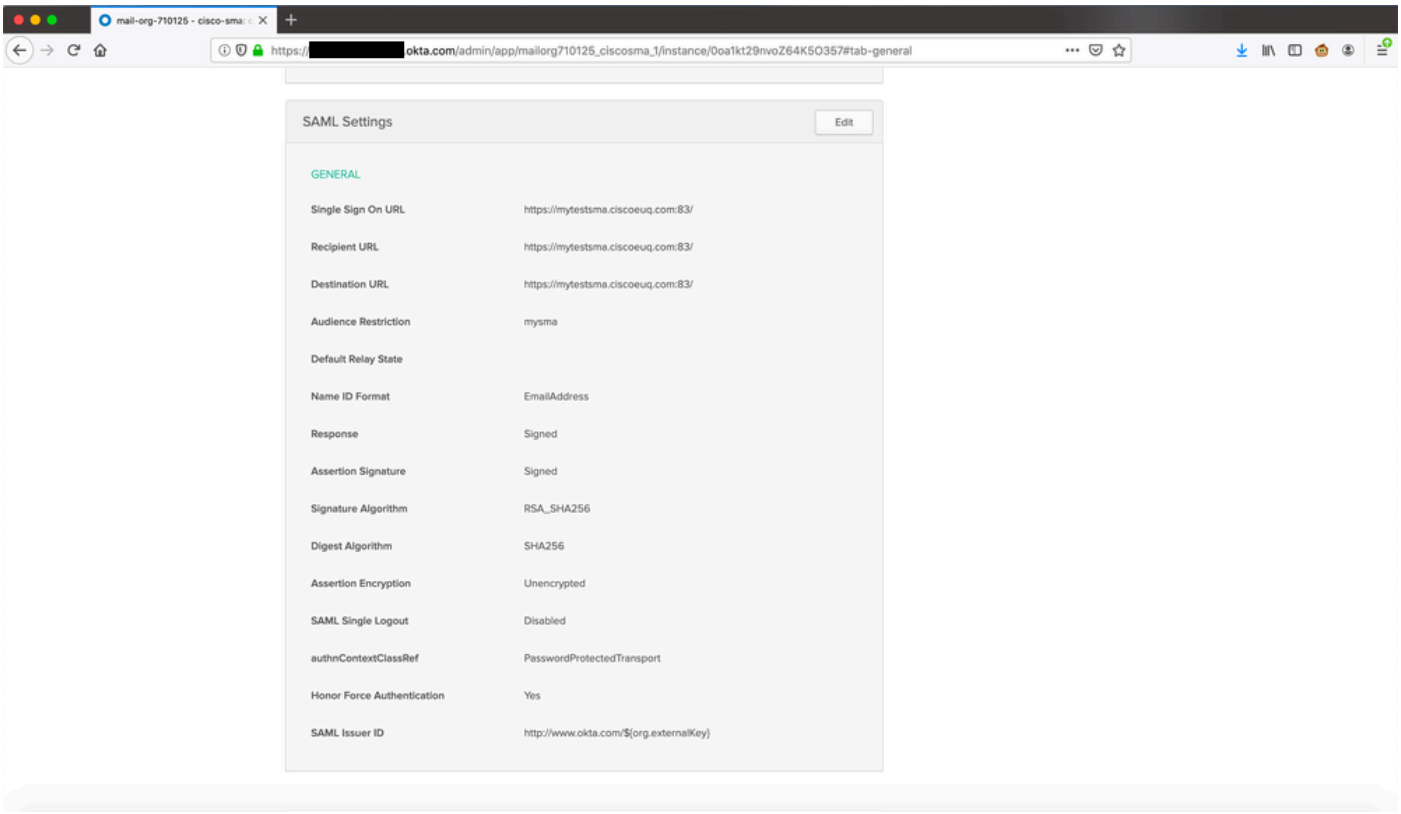


Configuração do provedor de serviços na GUI

Configurar o aplicativo SAML no Okta

Para criar um aplicativo SAML 2.0 no Okta para acesso EUQ SMA, siga estes passos:

1. Faça login no Okta como um administrador.
2. Navegue até Applications > Applications e selecione Create App Integration.
3. Selecione SAML 2.0 e, em seguida, selecione Next.
4. Insira um nome de aplicativo, por exemplo, SMA EUQ, e selecione Avançar.
5. Em URL de logon único, insira o URL do ACS do SMA nas configurações do provedor de serviços do SMA.
6. Em Audience URI (ID da entidade SP), insira a mesma ID da entidade configurada no SMA.
7. Para o formato de ID do nome, selecione EmailAddress.
8. Para Application username, selecione o formato de nome de usuário do Okta apropriado para sua implantação.
9. Conclua o assistente, abra o novo aplicativo e copie o arquivo de metadados IdP XML ou o URL dos metadados.

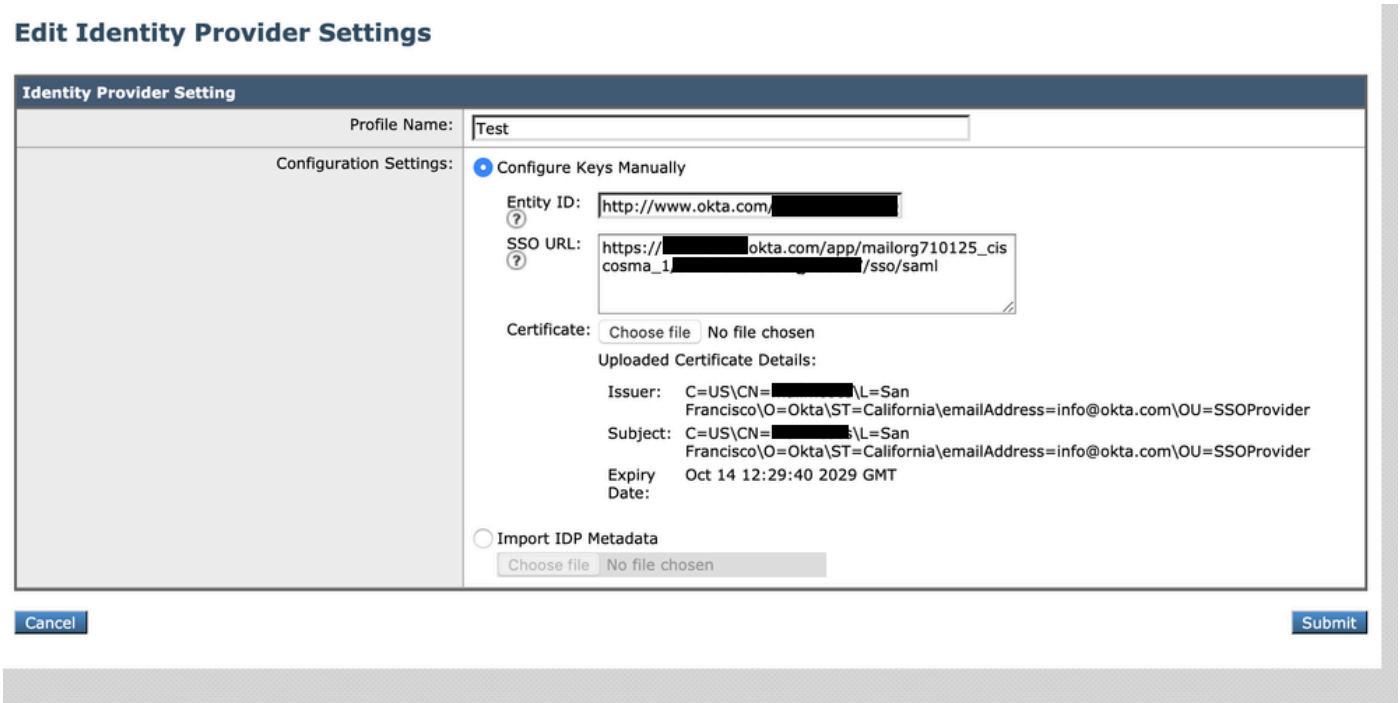


Exibir Portal do Okta

Configurar o provedor de identidade (IdP) no dispositivo SMA

Para configurar o Okta como o provedor de identidade (IdP) no SMA, siga estes passos:

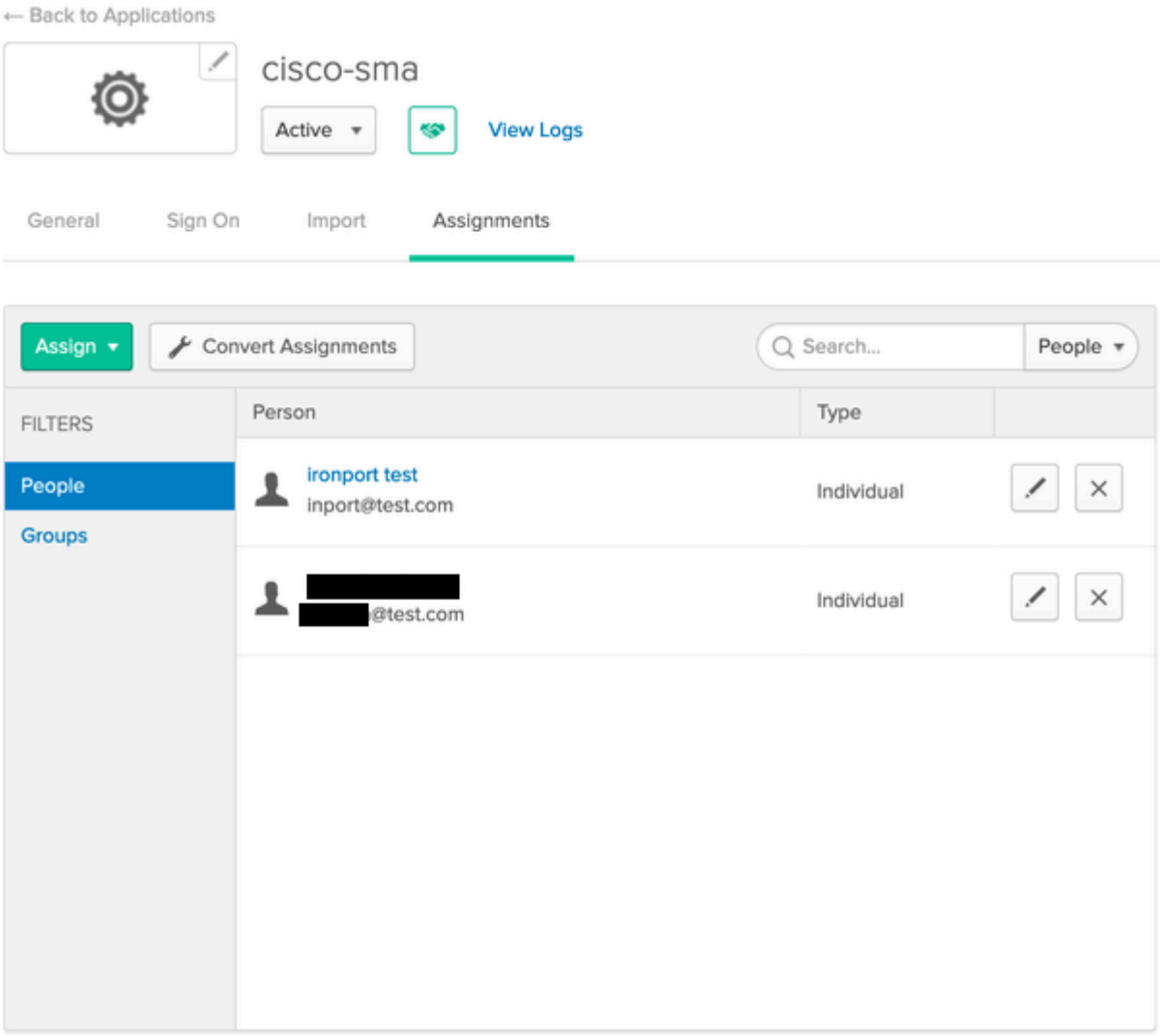
1. Faça login na interface da Web do SMA .
2. Navegue até Administração do sistema > SAML.
3. Em Identity Provider Settings, importe os metadados do Okta IdP da seção anterior ou insira os valores manualmente.



Atribuir usuários ao aplicativo Okta

Para permitir que os usuários se autentiquem no EUQ do SMA através do Okta, atribua usuários ou grupos ao aplicativo Okta:

1. No Okta, abra o aplicativo que você criou.
2. Navegue até Atribuições > Pessoas e selecione Atribuir.
3. Selecione Atribuir ao lado de cada usuário e, em seguida, selecione Concluído.



Atribuindo usuários no portal do Okta

Note: Você pode atribuir usuários manualmente, sincronizar usuários do Ative Diretory ou usar outra integração de diretório suportada pelo Okta.

Configurar MFA no Okta (opcional)

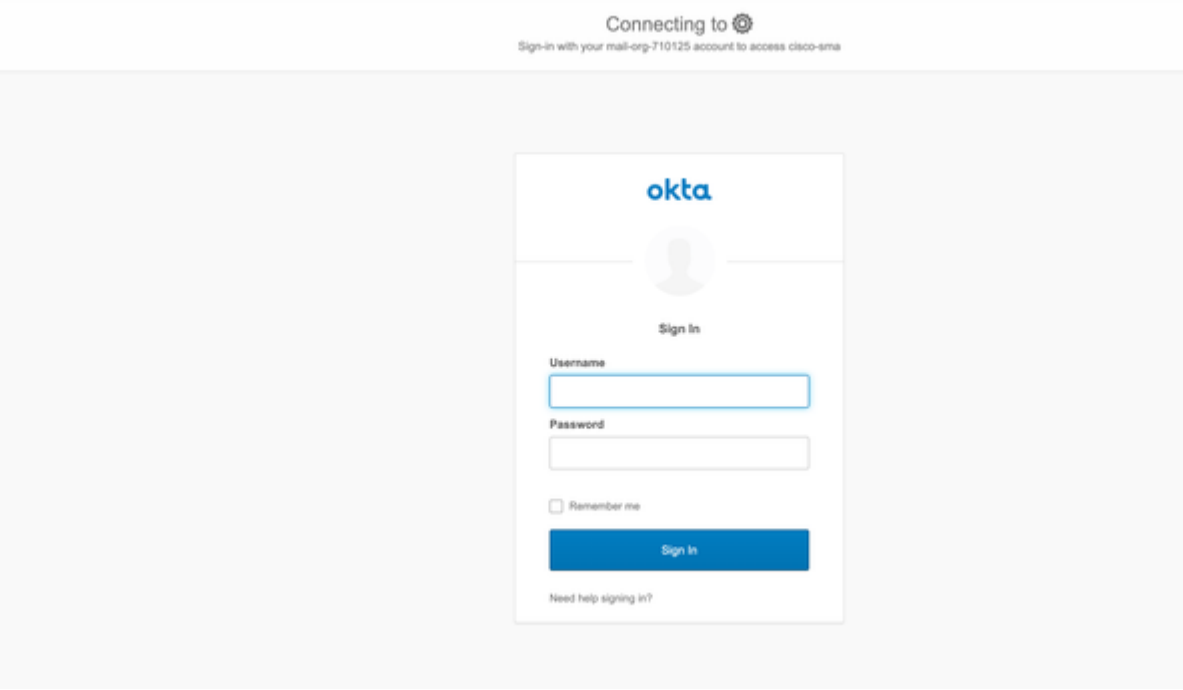
Se você quiser a autenticação multifator (MFA) para acesso EUQ, configure as políticas MFA no Okta para o aplicativo:

1. No Okta Admin, navegue para Segurança > Autenticação.
2. Configure os fatores obrigatórios, por exemplo, Okta Verify, Google Authenticator ou SMS, e aplique a política ao aplicativo EUQ do SMA.

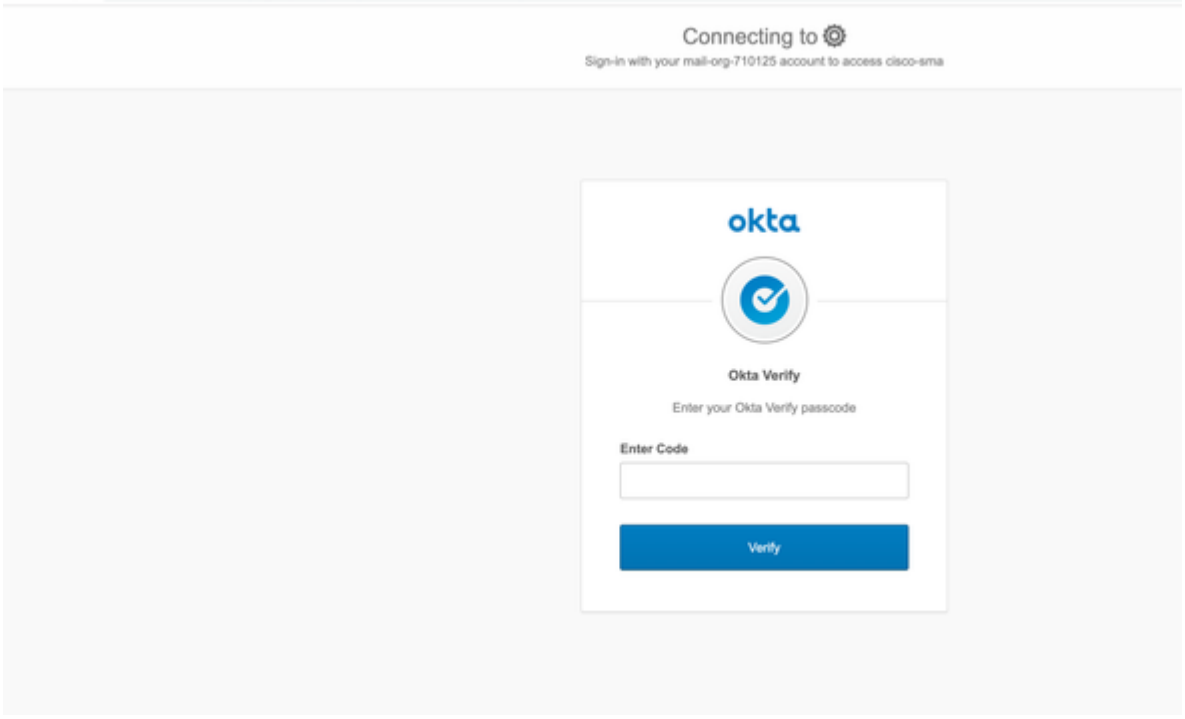
Verificar login SAML

Resultado esperado: Para verificar a configuração, execute estas etapas:

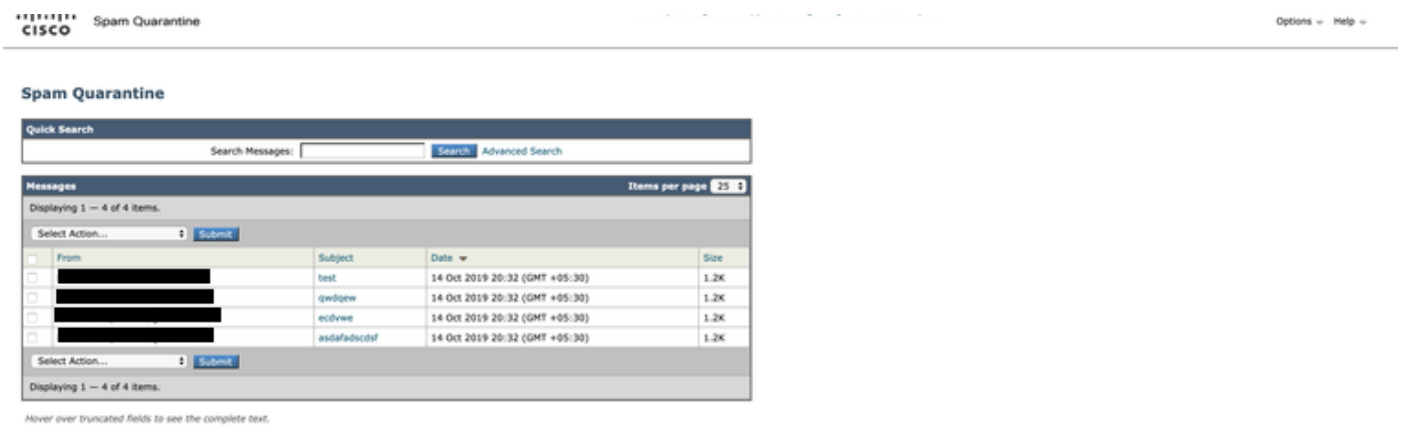
1. Navegue até a URL EUQ do SMA, por exemplo, https://<sma-fqdn>:<port>/.
2. Confirme se o navegador redireciona para o Okta para autenticação.
3. Se o MFA estiver habilitado, conclua o desafio MFA.
4. Confirme se você foi redirecionado de volta ao portal de quarentena de spam do SMA e se pode acessar as funções de quarentena.



Fazendo login usando o Okta



Inserir código para verificação do Okta



Visualização da quarentena de spam após fazer login no 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.