# Configuración de Okta SAML SSO para SMA End User Quarantine

## Contenido


Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configuración

- Configuración del proveedor de servicios (SP) en el dispositivo SMA
- Configuración de la aplicación SAML en Okta
- Configure el proveedor de identidad (IdP) en el dispositivo SMA
- Asignar usuarios a la aplicación Okta
- Configuración de MFA en Okta (opcional)
- Verificar inicio de sesión SAML


## Introducción

Este documento describe cómo configurar Okta como el proveedor de identidad SAML 2.0 para el acceso de cuarentena de usuario final de SMA de Cisco Secure Email.

## Prerequisites

- Producto: Dispositivo de gestión de seguridad Cisco Secure Email Security Management Appliance (SMA)
- Función: SSO de SAML para cuarentena de usuario final (EUQ)
- Proveedor de identidad: Okta (SAML 2.0)
- Se aplica a: Implementaciones de SMA que proporcionan acceso a EUQ en plataformas virtuales o de hardware. Reemplace los nombres de host y los puertos de ejemplo por los valores de su entorno.
- Contexto de versión: Este procedimiento se aplica a las versiones de SMA que admiten SAML para EUQ. Compruebe los campos y las opciones de menú disponibles en la versión instalada.

---

Nota: Este documento se centra en la configuración SAML de SMA EUQ. Sólo se hace referencia a ESA para la generación de certificados cuando SMA no puede generar un certificado autofirmado.

---

### Requirements

Antes de empezar, compruebe que dispone de:

- Acceso administrativo a la interfaz web de SMA.
- Permisos administrativos en Okta para crear aplicaciones SAML 2.0 y asignar usuarios o grupos.
- Certificado y clave privada para la configuración del proveedor de servicios SMA. Un certificado autofirmado es aceptable para la prueba.
- Un nombre de dominio completo (FQDN) de EUQ SMA accesible y un puerto al que los usuarios finales pueden acceder desde sus navegadores.
- Los valores de URL de aserción SAML SMA e ID de entidad SP (de Administración del sistema > SAML después de crear la entrada SP).
- Cuentas de usuario de Okta asignadas a la aplicación Okta.
- Usuarios sincronizados con el directorio, si la implementación utiliza la integración de directorios.

---

Nota: Okta es un proveedor de identidad externo. Este documento proporciona una configuración de ejemplo para referencia del cliente.

---

### Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

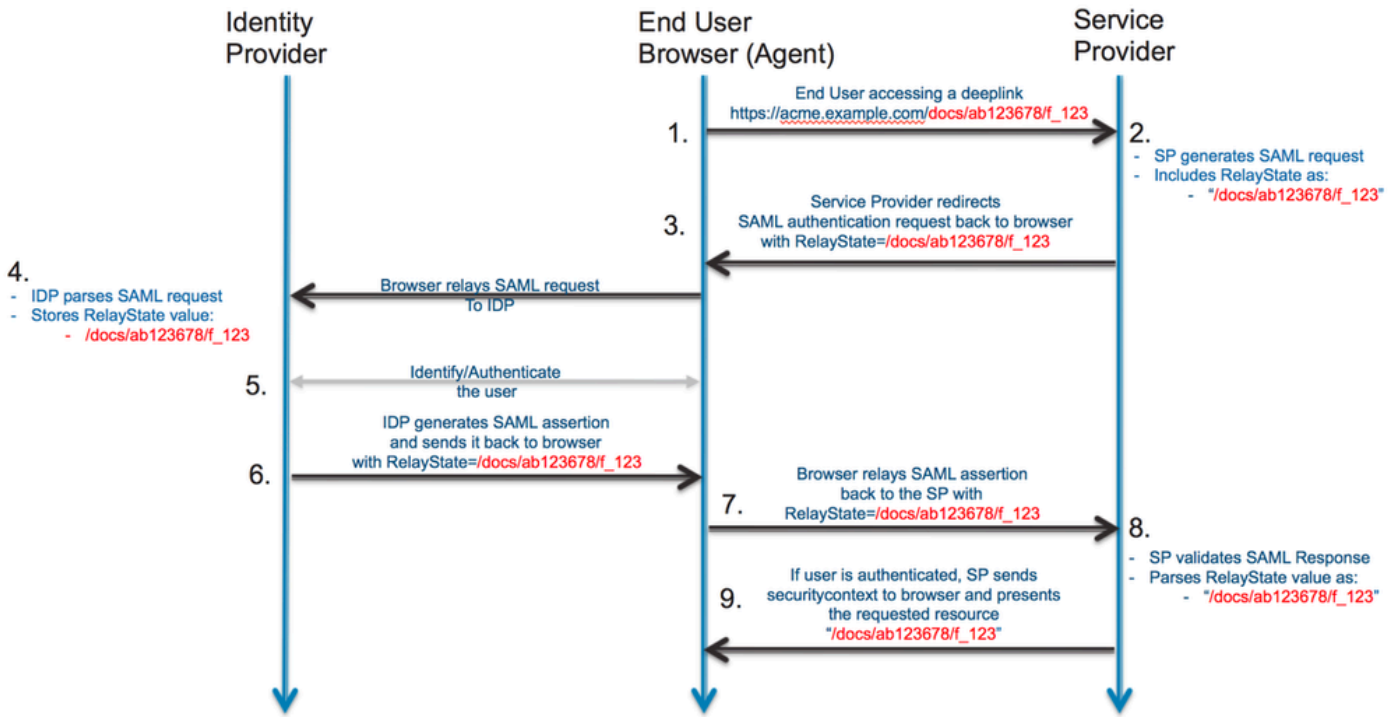
## Antecedentes

El objetivo es configurar el inicio de sesión único (SSO) para el portal de cuarentena de spam de modo que los usuarios sean redirigidos a Okta para autenticarse, completar la autenticación multifactor (MFA) si está habilitada en Okta y, a continuación, volver al portal de EUQ SMA. Este documento solo se aplica a SMA. Cisco Secure Email Gateway, anteriormente conocido como Dispositivo de seguridad de correo electrónico (ESA), sólo se utiliza para la generación de certificados cuando SMA no puede generar un certificado autofirmado.

Problema: Los usuarios deben autenticarse en el portal de cuarentena de spam SMA con Okta mediante SSO SAML y MFA opcional.

Resolución: Configure SMA como proveedor de servicios, configure una aplicación SAML en Okta, importe la configuración de Okta IdP en SMA, asigne usuarios en Okta y verifique el acceso.

Flujo SAML:




# Configuración

## Configuración del proveedor de servicios (SP) en el dispositivo SMA

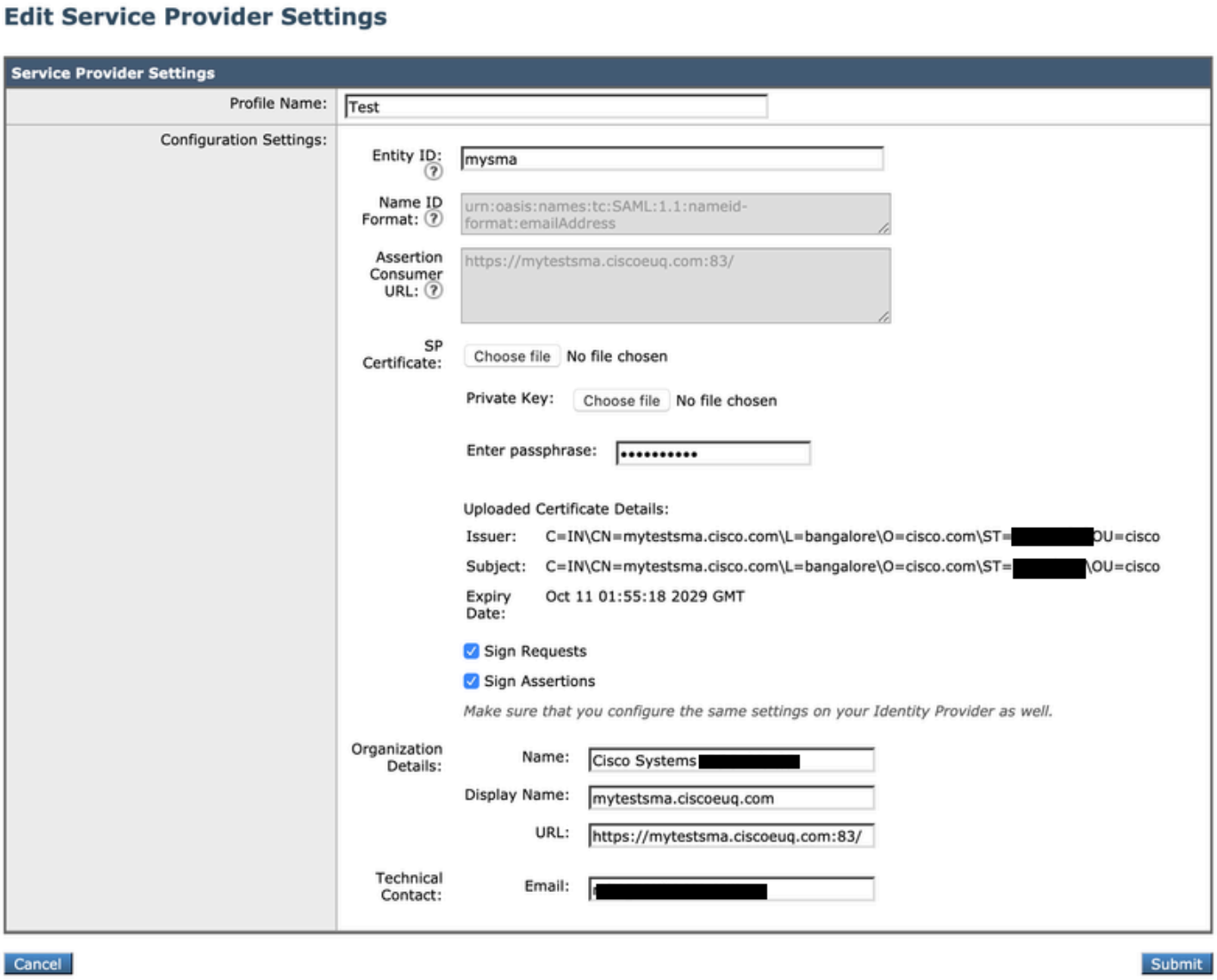
Para configurar el SMA como proveedor de servicios SAML para el acceso a la EUQ, siga estos pasos:

1. Inicie sesión en la interfaz web de SMA.
2. Vaya a Administración del sistema > SAML.
3. Seleccione Add Service Provider.
4. En Service Provider Entity ID, introduzca el entity ID que también puede configurar en Okta.
5. Verifique que Name ID Format y Assertion Consumer Service (ACS) URL se rellenen para la interfaz de EUQ.
6. En SP Certificate, cargue un certificado para firmar las solicitudes SAML.

---

Nota: SMA no puede generar un certificado autofirmado. También puede generar un certificado en un ESA y exportarlo para su uso en el SMA.

---

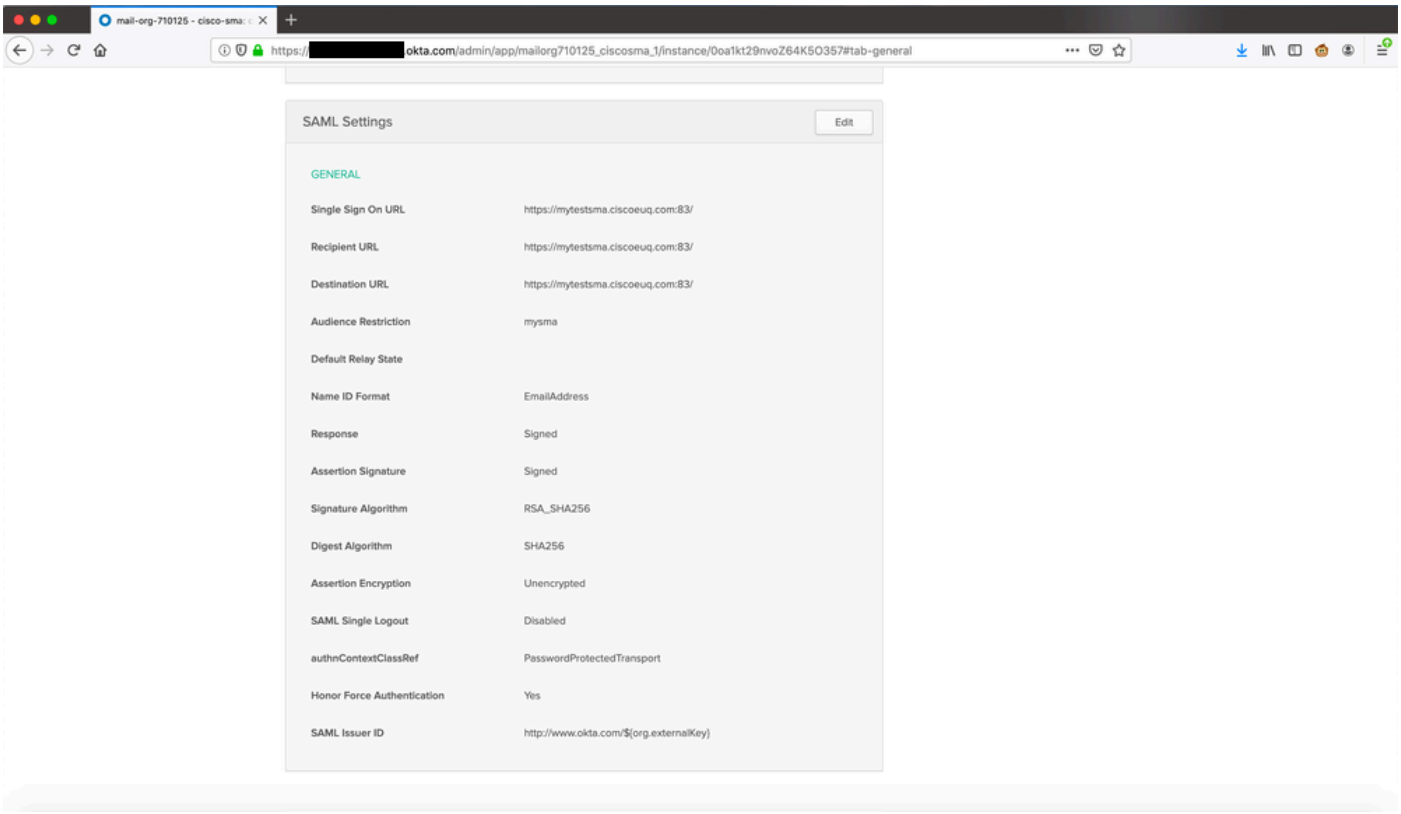



Configuración del proveedor de servicios en la GUI

## Configuración de la aplicación SAML en Okta

Para crear una aplicación SAML 2.0 en Okta para el acceso a EUQ SMA, siga estos pasos:

1. Inicie sesión en Okta como administrador.
2. Navegue hasta Aplicaciones > Aplicaciones, luego seleccione Crear integración de aplicaciones.
3. Seleccione SAML 2.0 y, a continuación, Next.
4. Introduzca un nombre de aplicación, por ejemplo, EUQ SMA, y seleccione Siguiente.
5. En Single Sign-on URL, ingrese la URL ACS de SMA de la configuración del proveedor de servicios de SMA.
6. En Audience URI (SP Entity ID), introduzca el mismo entity ID configurado en el SMA.
7. Para Name ID format, seleccione EmailAddress.
8. En Application username, seleccione el formato de nombre de usuario Okta adecuado para la implementación.
9. Complete el asistente, abra la nueva aplicación y copie el archivo IdP metadata XML o la metadata URL.

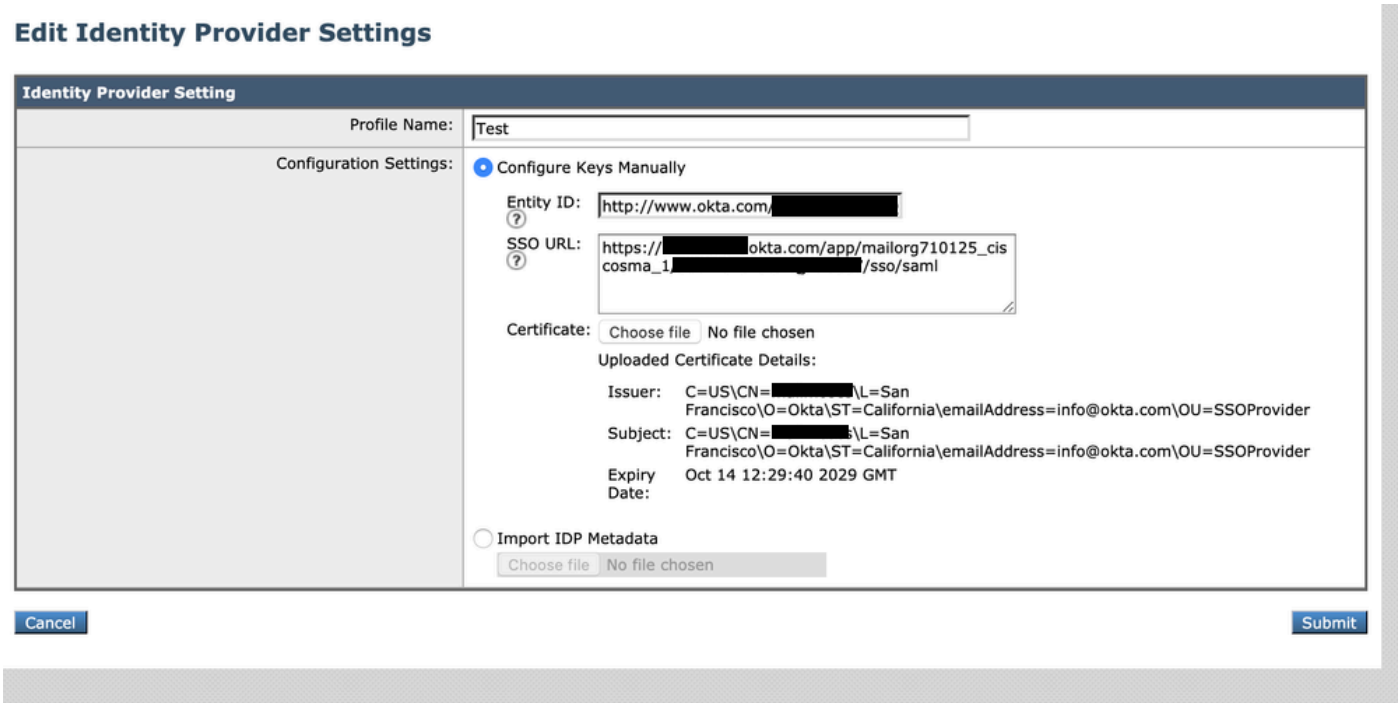



Ver portal Okta

## Configure el proveedor de identidad (IdP) en el dispositivo SMA

Para configurar Okta como proveedor de identidad (IdP) en el SMA, siga estos pasos:

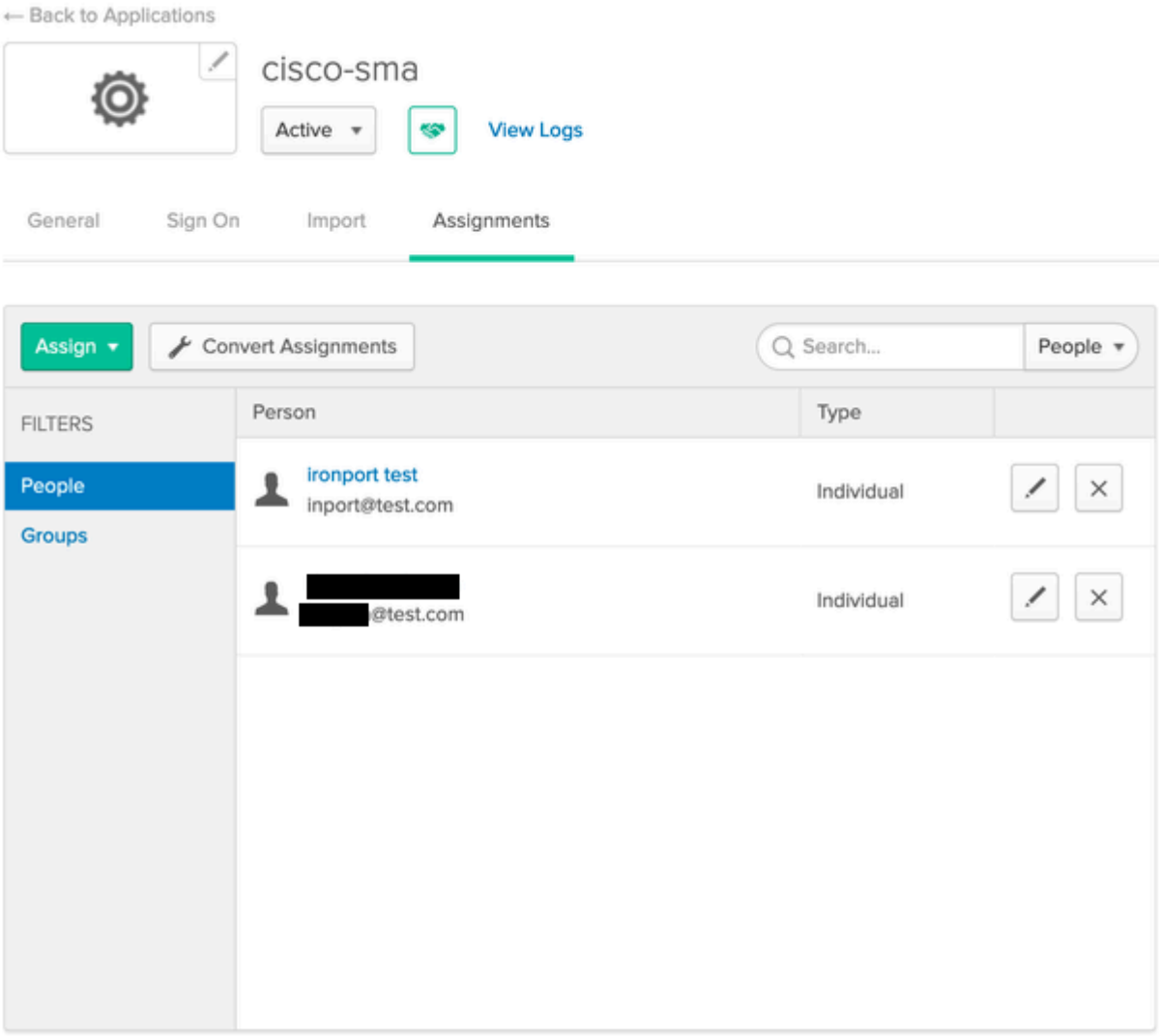
1. Inicie sesión en la interfaz web de SMA.
2. Vaya a Administración del sistema > SAML.
3. En Identity Provider Settings, importe los metadatos Okta IdP de la sección anterior o introduzca los valores manualmente.



## Asignar usuarios a la aplicación Okta

Para permitir que los usuarios se autentiquen en la EUQ SMA a través de Okta, asigne usuarios o grupos a la aplicación Okta:

1. En Okta, abra la aplicación que ha creado.
2. Navegue hasta Asignaciones > Personas, luego seleccione Asignar.
3. Seleccione Assign junto a cada usuario y, a continuación, seleccione Done.




Asignación de usuarios en Okta Portal

---

Nota: Puede asignar usuarios manualmente, sincronizar usuarios desde Active Directory o utilizar otra integración de directorios que admita Okta.

---

## Configuración de MFA en Okta (opcional)

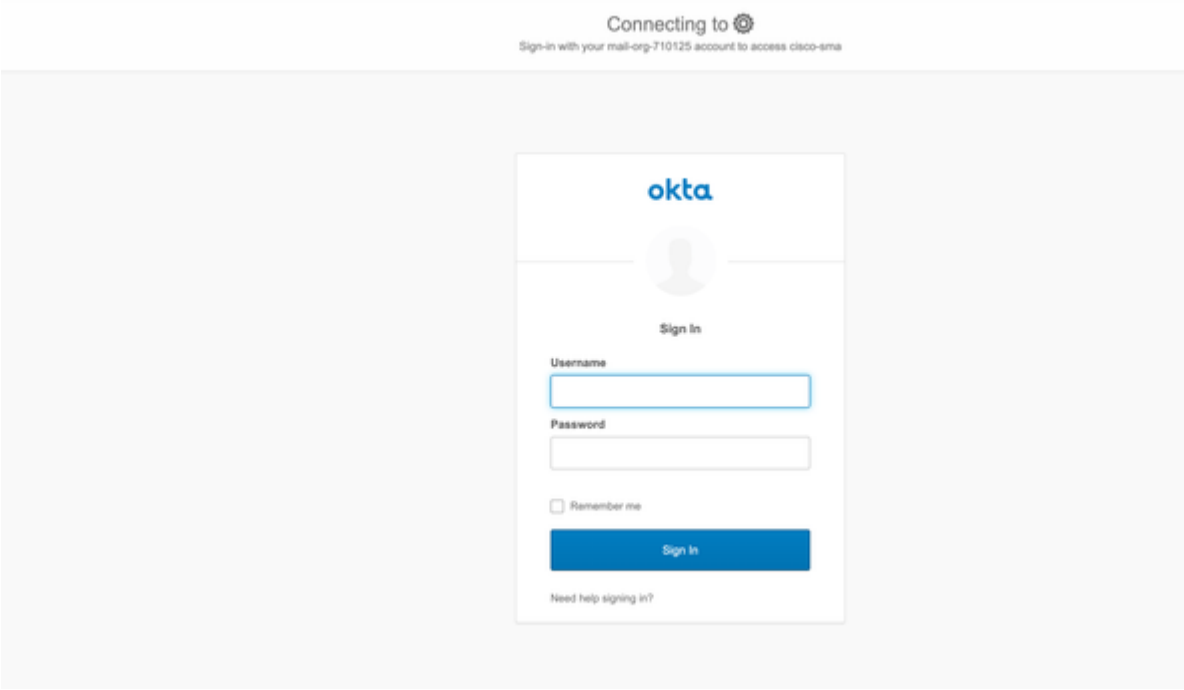
Si desea autenticación multifactor (MFA) para el acceso a EUQ, configure las políticas MFA en Okta para la aplicación:

1. En Okta Admin, navegue hasta Security > Authentication.
2. Configure los factores requeridos, por ejemplo, Okta Verify, Google Authenticator o SMS, y aplique la política a la aplicación SMA EUQ.

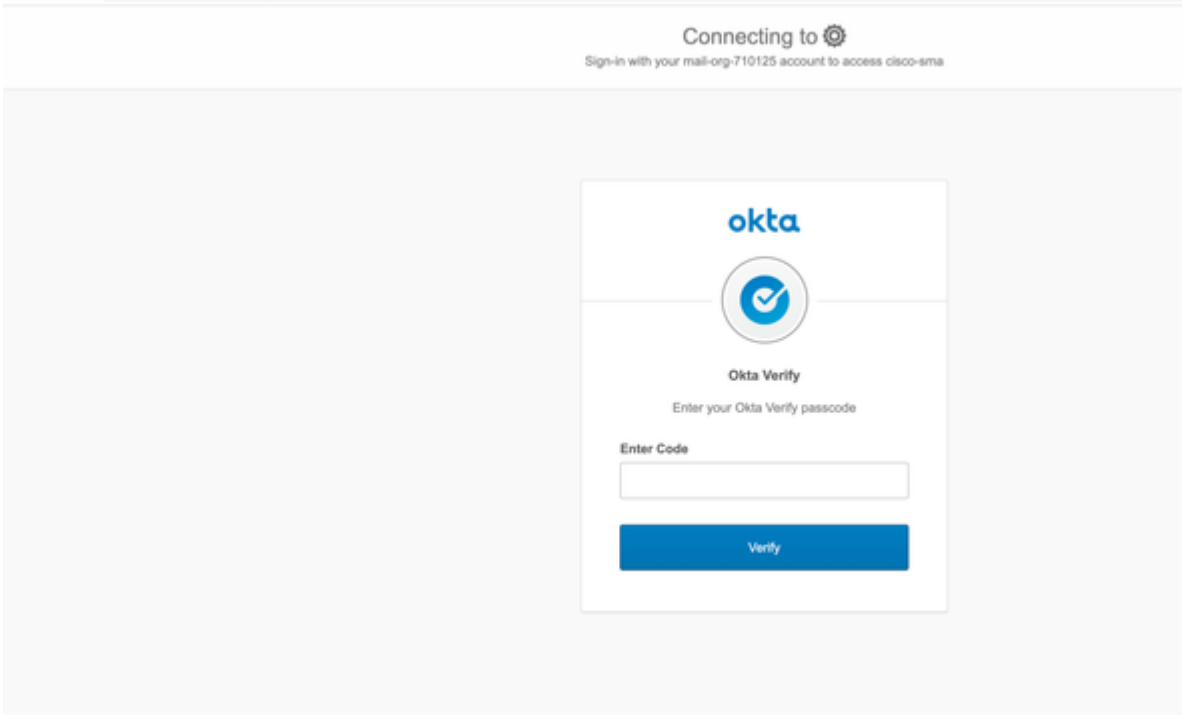
## Verificar inicio de sesión SAML

Resultado esperado: Para verificar la configuración, siga estos pasos:

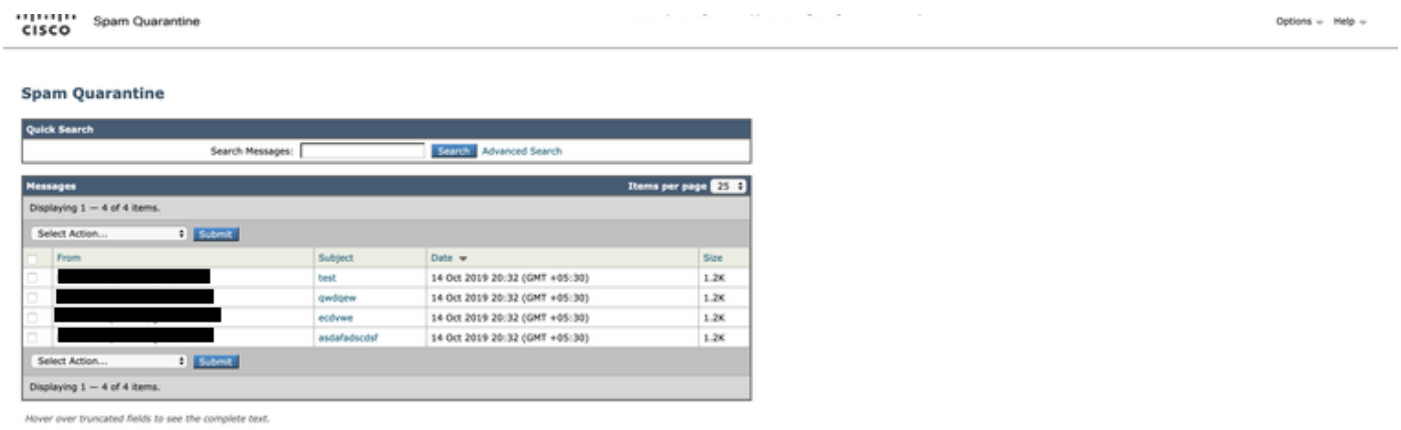
1. Vaya a la URL de EUQ SMA, por ejemplo, https://<sma-fqdn>:<port>/.
2. Confirme que el navegador redirige a Okta para la autenticación.
3. Si MFA está habilitado, complete el desafío MFA.
4. Confirme que se le redirige de nuevo al portal de cuarentena de spam de SMA y que puede acceder a las funciones de cuarentena.




Inicio de sesión con Okta




Introduzca el código para Okta Verify




Vista de Spam Quarantine después de iniciar sesión con 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).