Configuración de OKTA SSO para Spam Quarantine de usuario final

Contenido

Introducción

Este documento describe cómo configurar OKTA SSO para iniciar sesión en la cuarentena de spam de usuario final del dispositivo de administración de seguridad.

Prerequisites

- Acceso de administrador al dispositivo de administración de seguridad de Cisco.
- Acceso de administrador a OKTA.
- Certificados SSL X.509 autofirmados o firmados por CA (opcional) en formato PKCS #12 o PEM (proporcionados por OKTA).

Antecedentes

Cisco Security Management Appliance permite el inicio de sesión SSO para los usuarios finales que utilizan Spam Quarantine para usuarios finales y se integra con OKTA, que es un gestor de identidades que proporciona servicios de autenticación y autorización a sus aplicaciones. Cisco End User Spam Quarantine se puede configurar como una aplicación conectada a OKTA para la autenticación y autorización, y utiliza SAML, un formato de datos estándar abierto basado en XML que permite a los administradores acceder a un conjunto definido de aplicaciones sin problemas después de iniciar sesión en una de esas aplicaciones.

Para obtener más información sobre SAML, consulte: [Información general sobre SAML](#)

Componentes

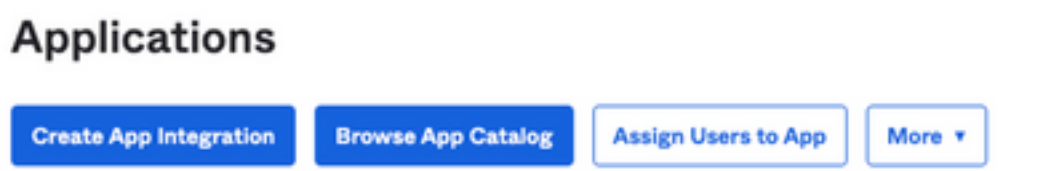
- Cuenta de administrador de nube de Cisco Security Management Appliance.
- Cuenta de administrador OKTA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos utilizados en este documento se iniciaron con una configuración desactivada (predeterminada). si la red está activa, asegúrese de comprender el impacto potencial de cualquier comando.

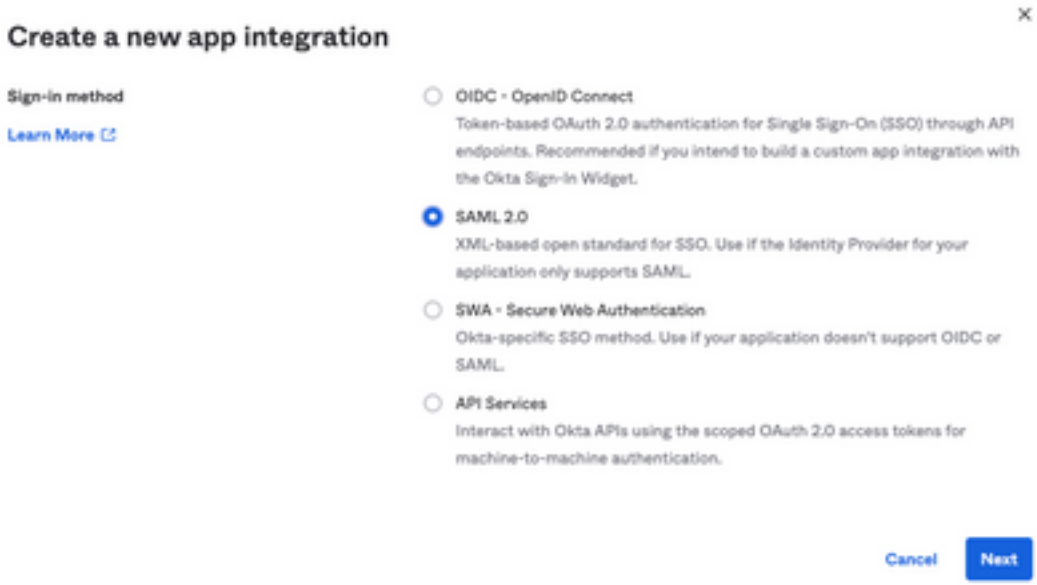
Configurar

Bajo Okta.

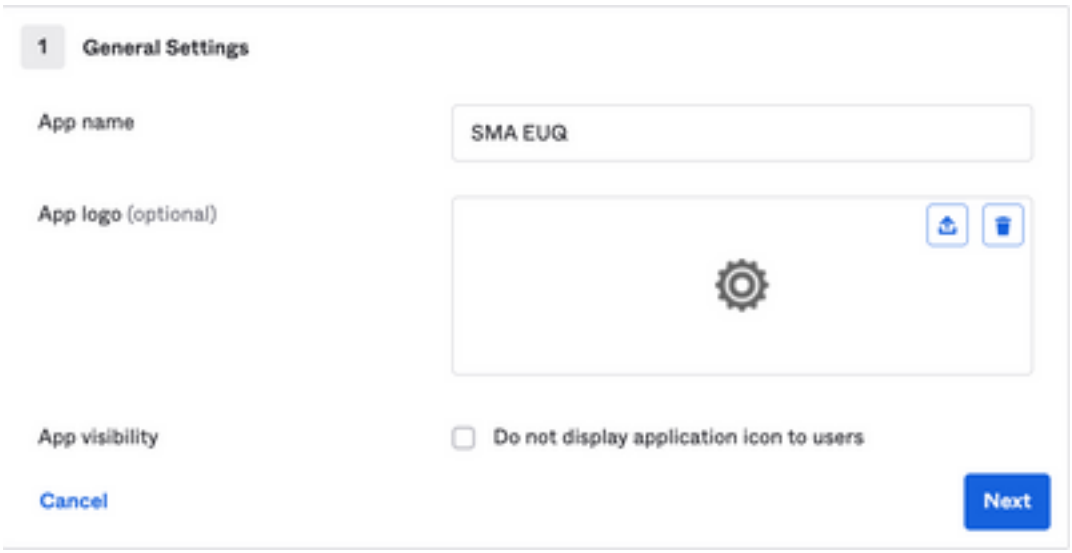
1. Acceda al portal de aplicaciones y seleccione Create App Integration , como se muestra en la imagen:



2. Seleccione SAML 2.0 como tipo de aplicación, como se muestra en la imagen:



3. Introduzca el nombre de la aplicación SMA EUQ y elija Next, como se muestra en la imagen:



4. En virtud del SAML settings, rellene los espacios, como se muestra en la imagen:

- URL de inicio de sesión único: se trata del servicio de consumidor de aserción obtenido de la

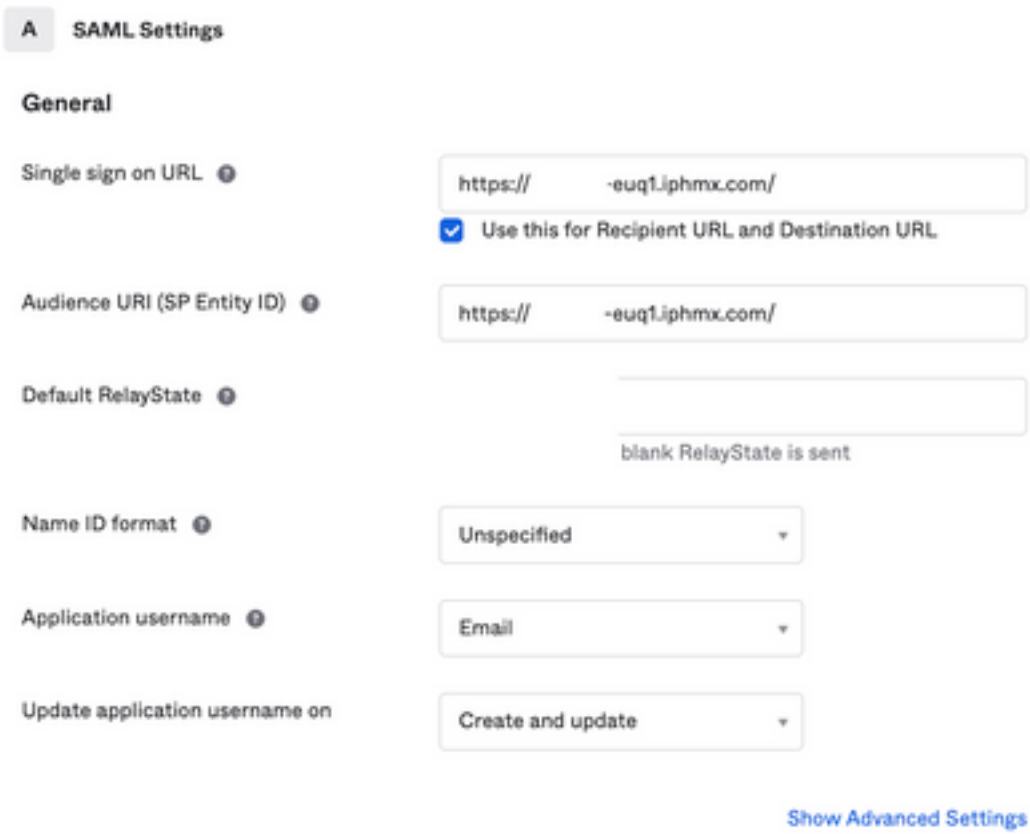
interfaz SMA EUQ.

- URI de público (ID de entidad SP): es la ID de entidad obtenida de la ID de entidad de EUQ SMA.

- Formato de ID de nombre: mantenerlo como Sin especificar.

- Nombre de usuario de la aplicación: correo electrónico que solicita al usuario que introduzca su dirección de correo electrónico en el proceso de autenticación.

- Actualizar nombre de usuario de aplicación en: Crear y actualizar.



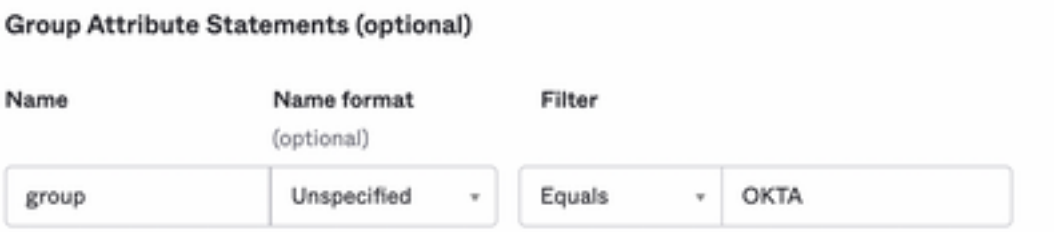
Desplácese hasta Group Attibute Statements (optional) , como se muestra en la imagen:

Introduzca la siguiente sentencia de atributo:

-Nombre: group

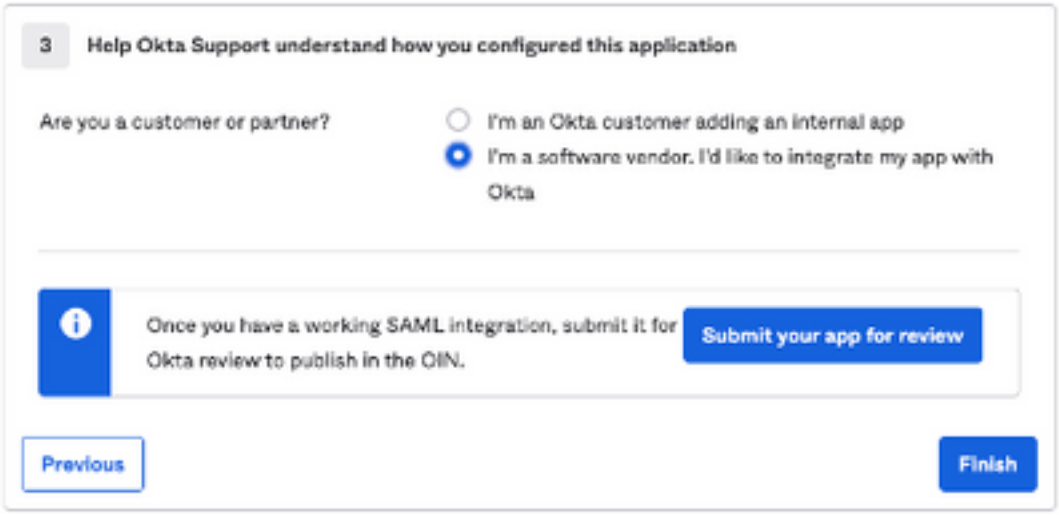
- Formato del nombre: Unspecified

- Filtro: Equals y OKTA



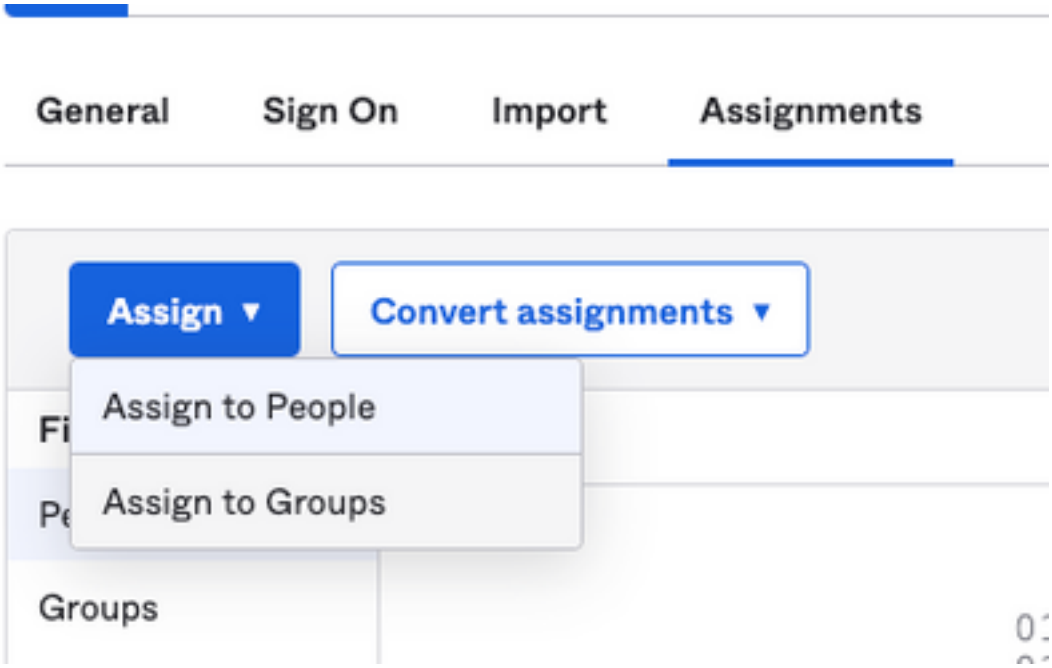
Seleccionar Next .

5. Cuando se le solicite Help Okta to understand how you configured this application, introduzca el motivo aplicable al entorno actual, como se muestra en la imagen:



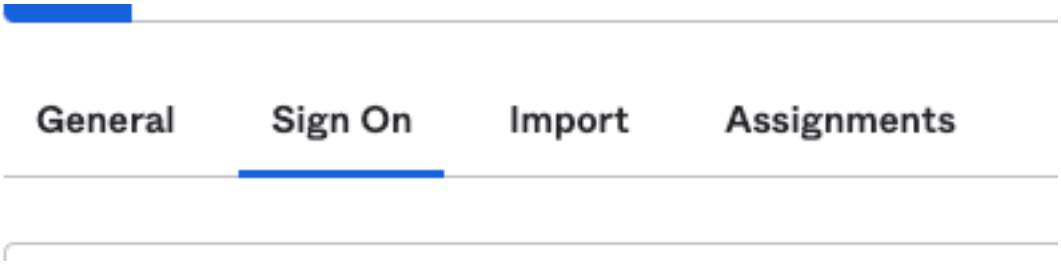
Elegir Finish para continuar con el paso siguiente.

6. Seleccione Assignments y, a continuación, seleccione Assign > Assign to Groups, como se muestra en la imagen:

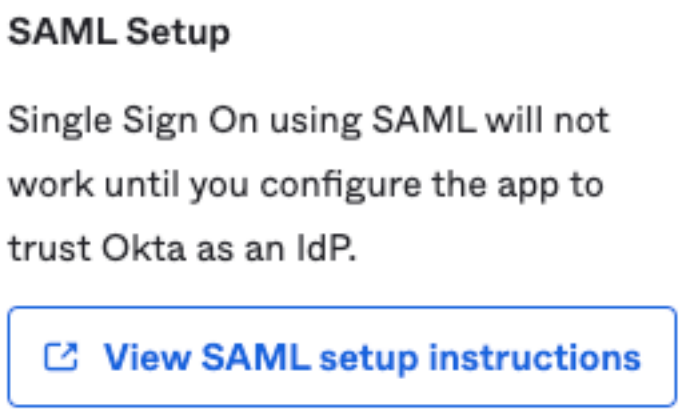


7. Seleccione el grupo OKTA, que es el grupo con los usuarios autorizados para acceder al entorno

8. Seleccione Sign On , como se muestra en la imagen:

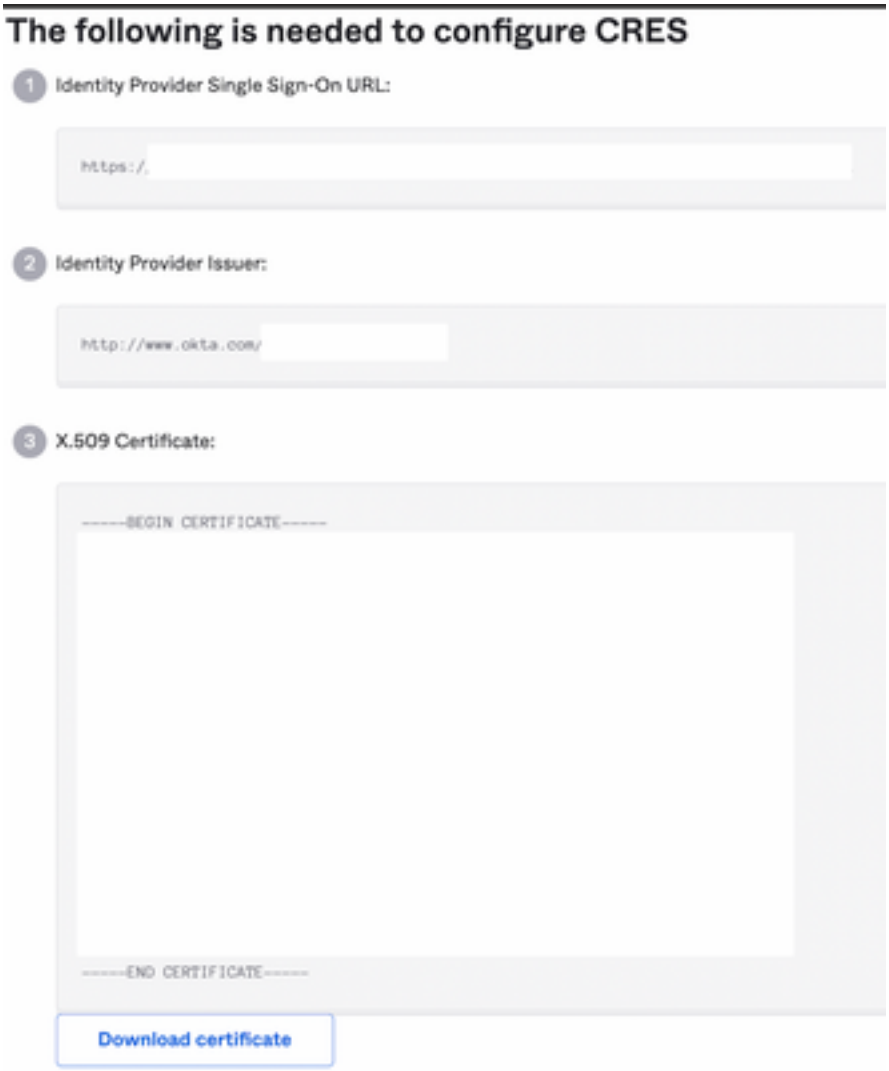


9. Desplácese hacia abajo y a la esquina derecha, seleccione el View SAML setup instructions , como se muestra en la imagen:



10. Guarde esta información en un bloc de notas, es necesario poner en el Cisco Security Management Appliance Configuración SAML, como se muestra en la imagen:

- URL de inicio de sesión único del proveedor de identidad
- Emisor del proveedor de identidad
- Certificado X.509

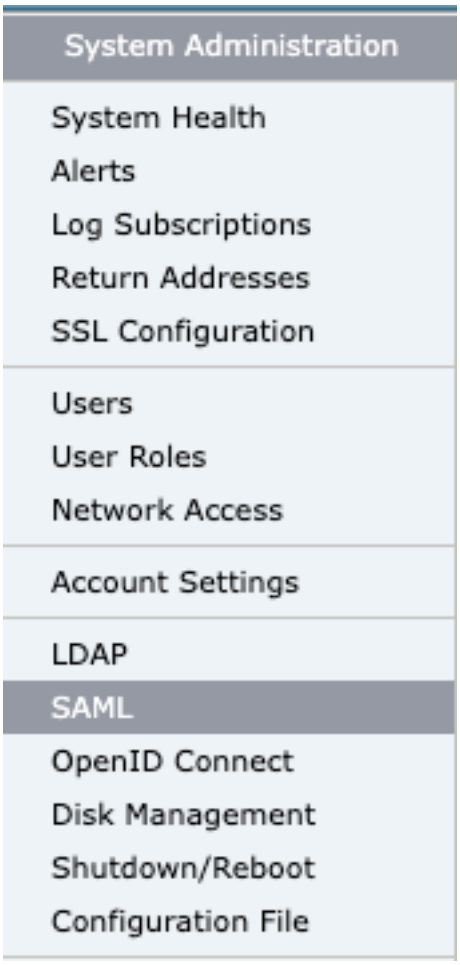


11. Una vez completada la configuración de OKTA, puede volver a Cisco Security Management Appliance.

En Cisco Security Management Appliance:

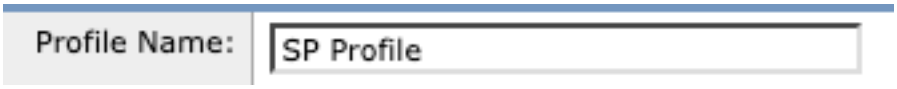
1. Inicie sesión en el dispositivo de administración de seguridad de Cisco como administrador de la nube, como se muestra en la imagen:

2. En el System Administration, seleccione la ficha SAML , como se muestra en la imagen:



3. Se abre una nueva ventana para configurar SAML. Debajo SAML for End-User Quarantine, clic Add Service Provider , como se muestra en la imagen:

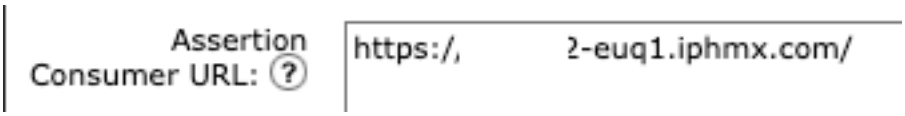
4. En Profile Name , introduzca un nombre de perfil para el perfil del proveedor de servicios, como se muestra en la imagen:



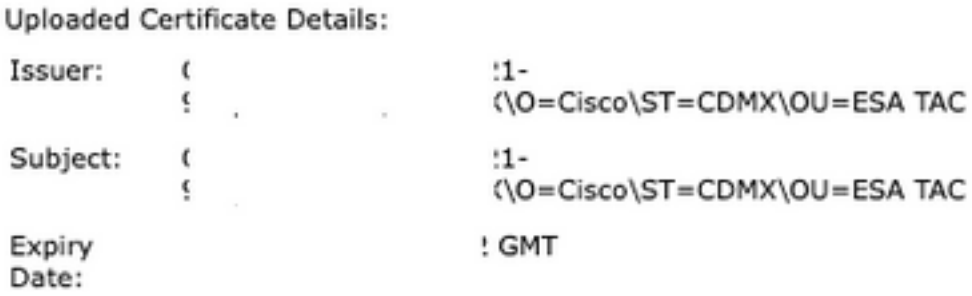
5. Para Entity ID , introduzca un nombre único global para el proveedor de servicios (en este caso, su dispositivo). El formato del ID de entidad del proveedor de servicios suele ser un URI, como se muestra en la imagen:

6. Para **Name ID Format** , este campo no se puede configurar. Necesita este valor al configurar el proveedor de identidad, como se muestra en la imagen:

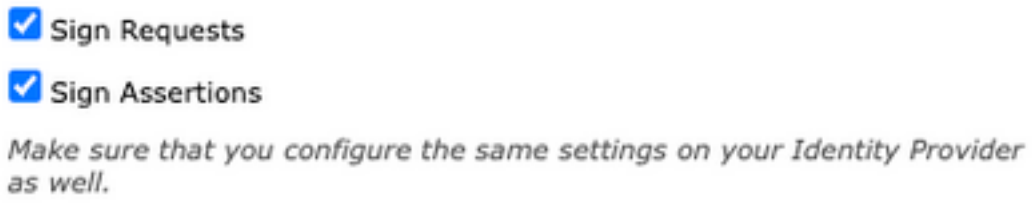
7. Para **Assertion Consumer URL**, introduzca la URL a la que el proveedor de identidad envía la afirmación SAML después de que la autenticación se haya completado correctamente. En este caso, esta es la URL a su cuarentena de spam.



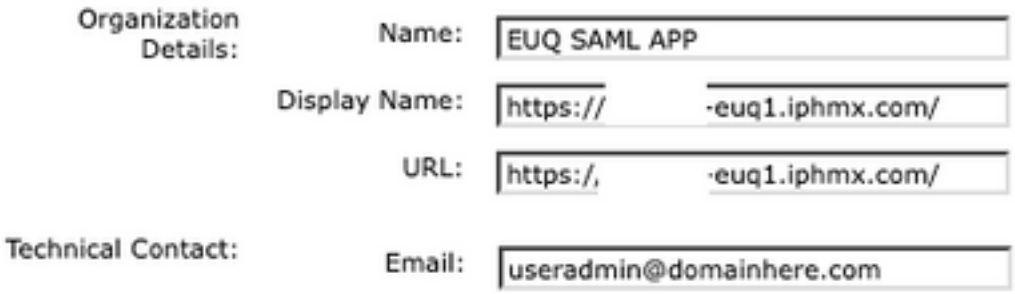
8. Para SP Certificate , cargue el certificado y la clave, o cargue el archivo PKCS #12. Una vez cargado, el Uploaded Certificate Details muestra, como se muestra en la imagen:



9. Para Sign Requests and Sign Assertions , marque ambas casillas de verificación si desea firmar las solicitudes SAML y las aserciones. Si selecciona verificar estas opciones, asegúrese de configurar los mismos ajustes en OKTA, como se muestra en la imagen:

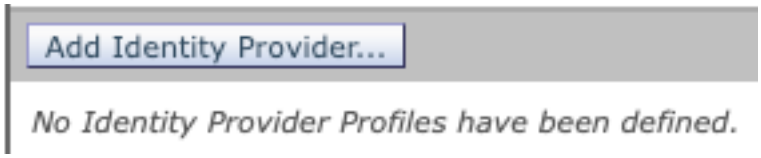


10. Para Organization Details, introduzca los detalles de su organización, como se muestra en la imagen:

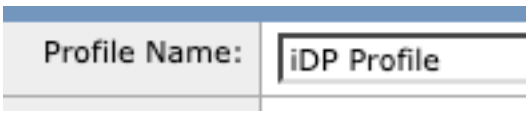


11. Submit y Commit cambios antes de continuar con la configuración Identity Provider Settings .

12. En SAML , haga clic en Add Identity Provider, como se muestra en la imagen:



13. En Profile Name: introduzca un nombre para el perfil del proveedor de identidad, como se muestra en la imagen:

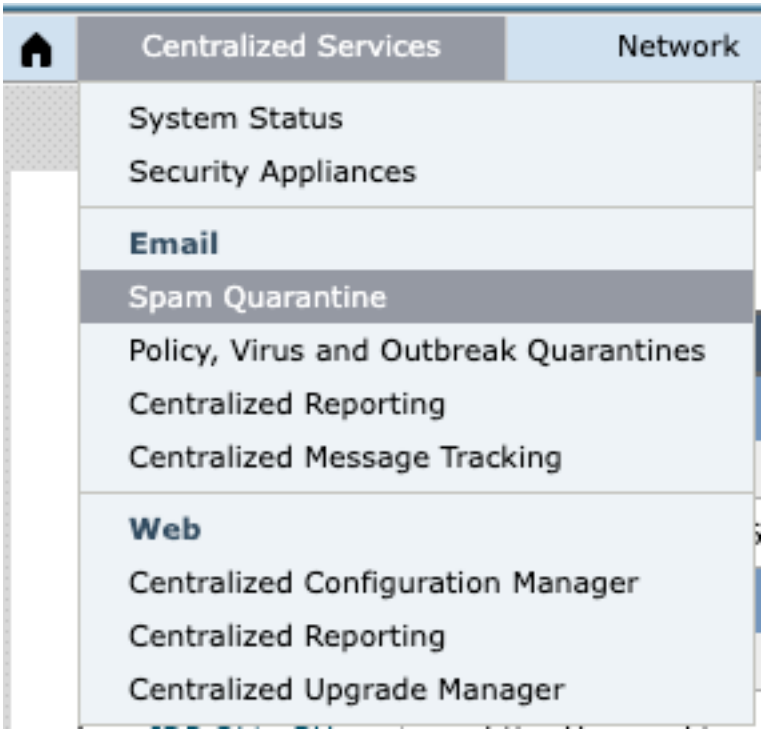


14. Seleccione Configure Keys Manually e introduzca esta información, como se muestra en la imagen:

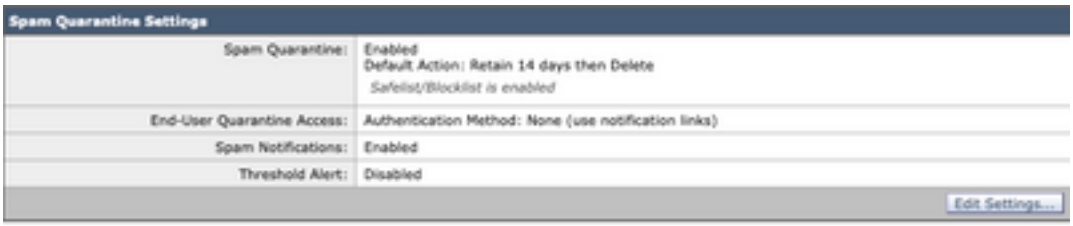
- Id. de entidad: el Id. de entidad del proveedor de identidad se utiliza para identificar de forma única al proveedor de identidad. Se obtiene de la configuración de OKTA en los pasos anteriores.
- SSO URL: URL a la que el SP debe enviar las solicitudes de autenticación SAML. Se obtiene de la configuración de OKTA en los pasos anteriores.
- Certificado: El certificado proporcionado por OKTA.

15. Submit y Commit los cambios para continuar con la activación de inicio de sesión SAML.

16. En Centralized Services > Email , haga clic en Spam Quarantine, como se muestra en la imagen:



17. En Spam Quarantine - > Spam Quarantine Settings , haga clic en Edit Settings , as shown in the image:



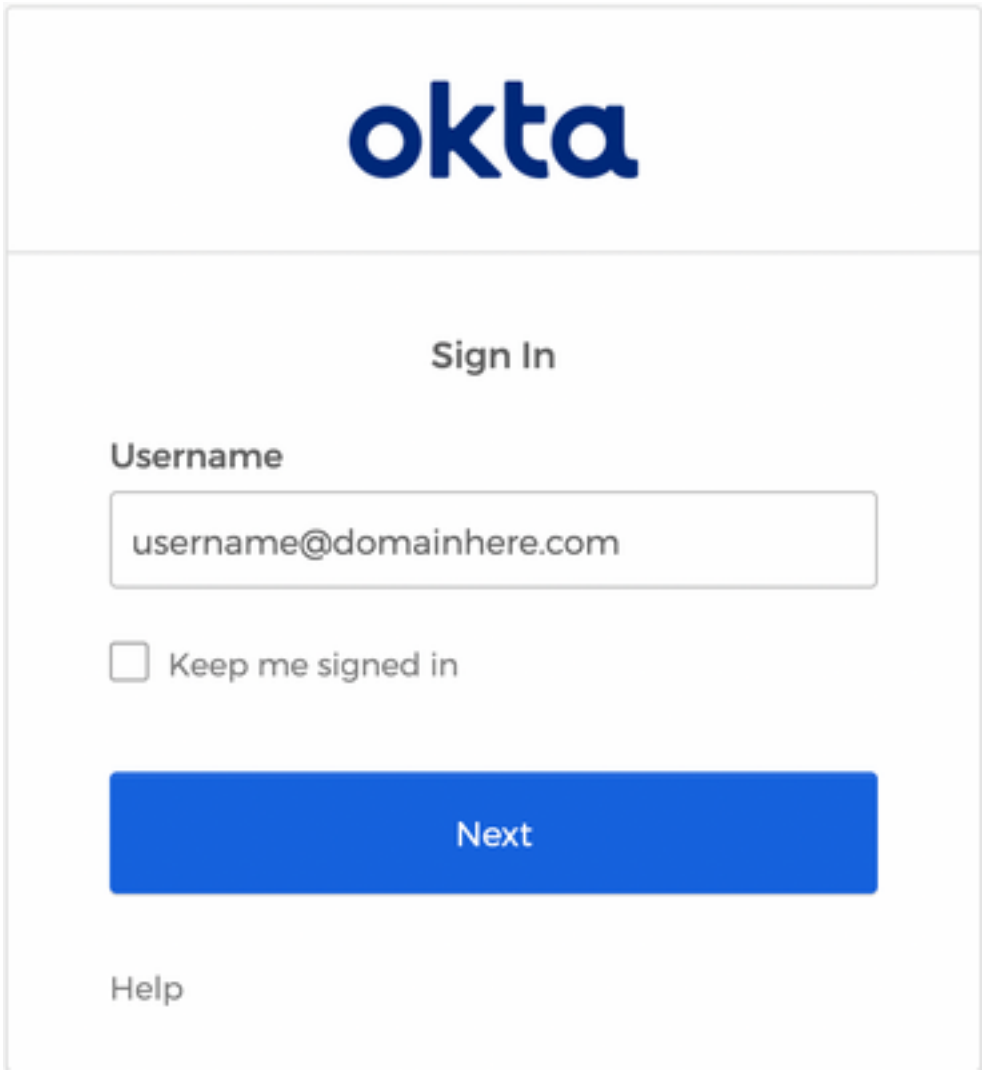
18. Desplácese hasta End-User Quarantine Access > End-User Authentication , seleccione SAML 2.0 , como se muestra en la imagen:

19. Submit y Commit cambios para habilitar la autenticación SAML para **End User Spam Quarantine** .

Verificación

1. En cualquier navegador web, introduzca la URL de la cuarentena de spam de usuario final de su empresa, como se muestra en la imagen:

2. Se abre una nueva ventana para continuar con la autenticación OKTA. Inicie sesión con las **credenciales de OKTA**, como se muestra en la imagen:



3. Si la autenticación se realiza correctamente, el End User Spam Quarantine abre el contenido de Spam Quarantine para el usuario que inicia sesión, como se muestra en la imagen:

Ahora el usuario final puede acceder a la cuarentena de spam de usuario final con credenciales OKTA. .

Información Relacionada

Guías de usuario final de Cisco Secure Email and Web Manager

Asistencia para 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).