bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML en Keycloak

Ver en el centro de ayuda:
https://bitwarden.com/help/saml-keycloak/

Implementación de SAML en Keycloak

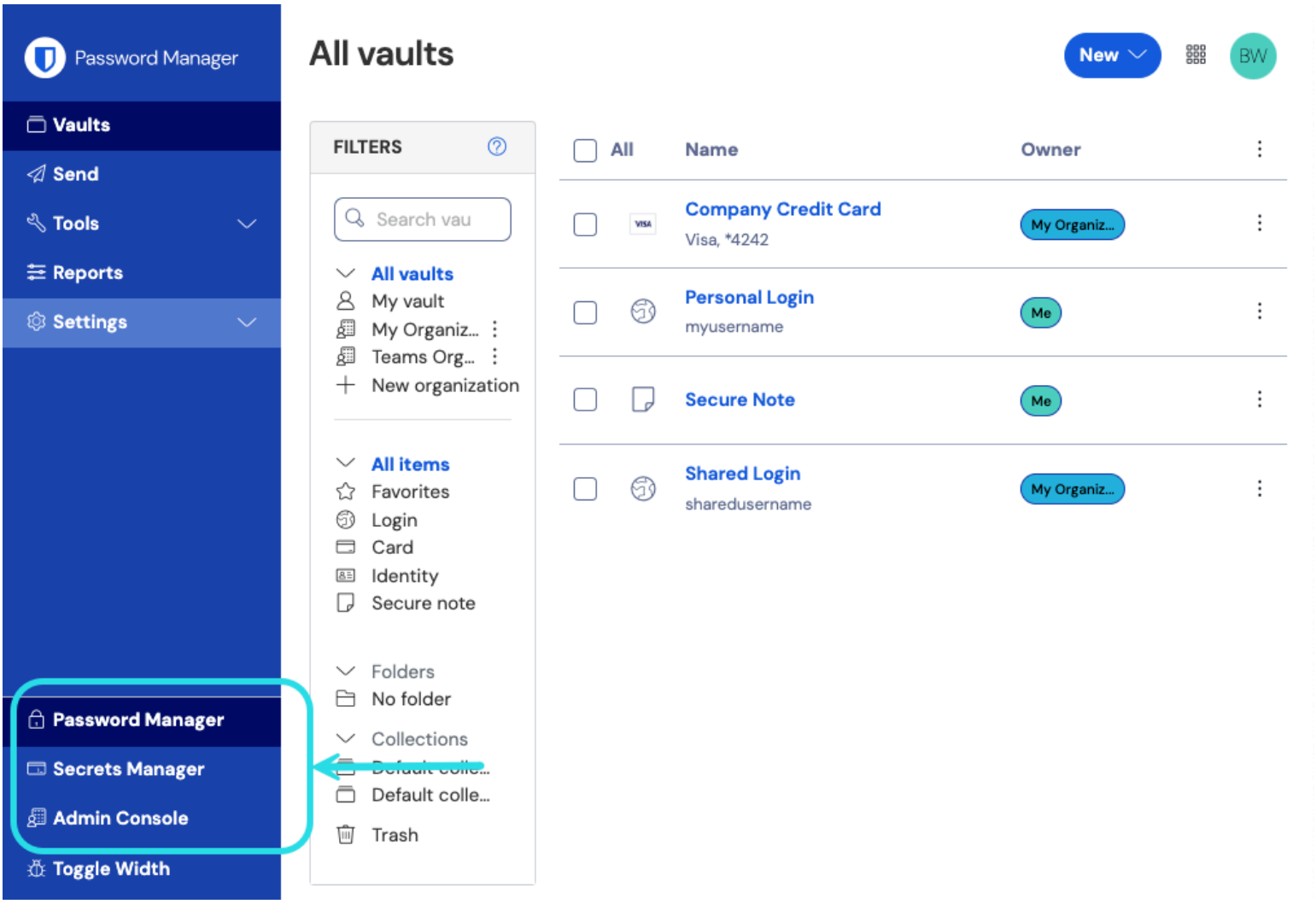
Este artículo contiene ayuda **específica de Keycloak** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte Configuración de SAML 2.0.

La configuración implica trabajar simultáneamente con la aplicación web de Bitwarden y el Portal de Keycloak. A medida que avanza, recomendamos tener ambos fácilmente disponibles y completar los pasos en el orden en que están documentados.

> **Tip**
>
> **Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.
>
> Download Sample

Abre SSO en la aplicación web

Inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el conmutador de producto (▦):



Selector de producto

Abra la pantalla de **Ajustes → Inicio de sesión único** de su organización:

Configuración de SAML 2.0

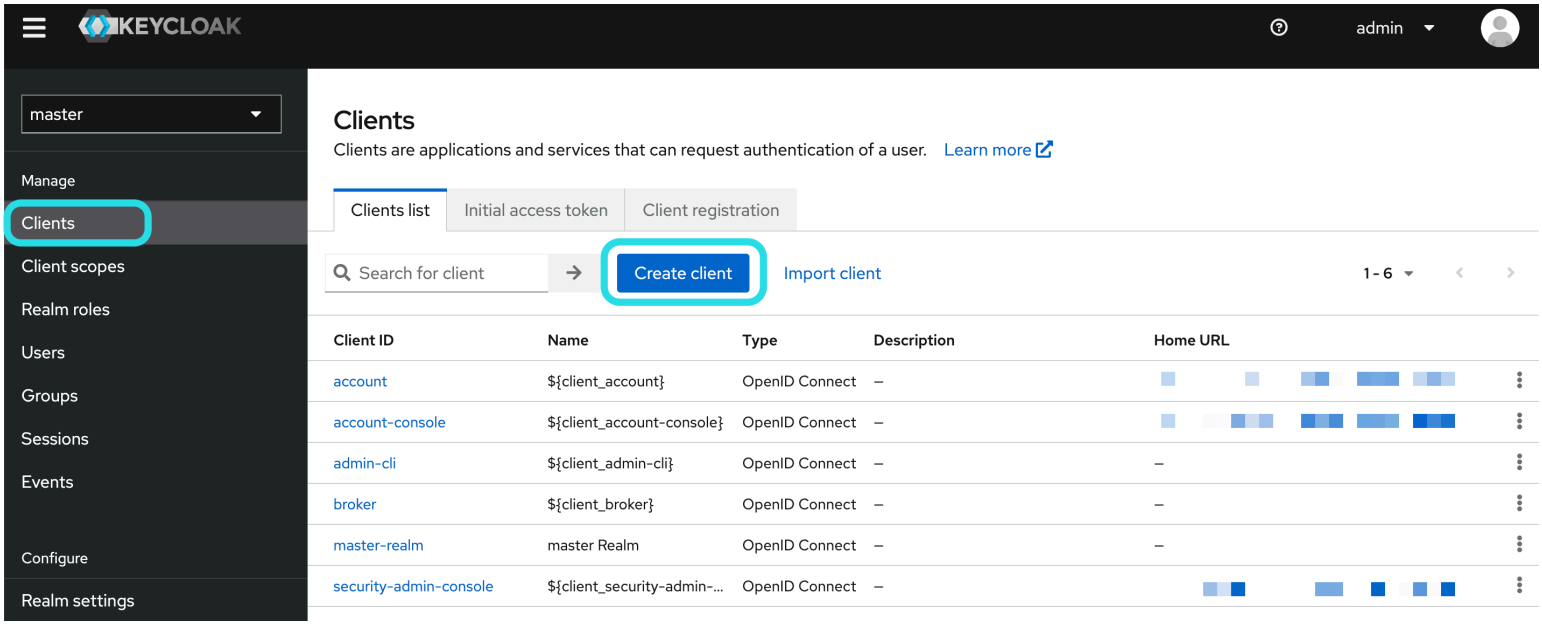
Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de **Tipo**. Mantén esta pantalla abierta para una fácil referencia.

Puedes desactivar la opción **Establecer una ID de entidad SP única** en esta etapa si lo deseas. Hacerlo eliminará su ID de organización de su valor de ID de entidad SP, sin embargo, en casi todos los casos, se recomienda dejar esta opción activa.

> **Tip**
>
> Hay opciones alternativas de **descifrado de miembro**. Aprenda cómo comenzar a usar SSO con dispositivos de confianza o Conector de clave.

Configuración de Keycloak

Inicie sesión en Keycloak y seleccione **Clientes → Crear Cliente**.



Create a Client

En la pantalla de Crear cliente, complete los siguientes campos:

Campo	Descripción
Tipo de cliente	Selecciona SAML.
ID de cliente	Establezca este campo en el **ID de Entidad SP** pre-generado. Este valor generado automáticamente se puede copiar desde la pantalla de **Ajustes → Inicio de sesión único** de la organización y variará según su configuración.
Nombre	Ingrese un nombre de su elección para el cliente Keycloak.

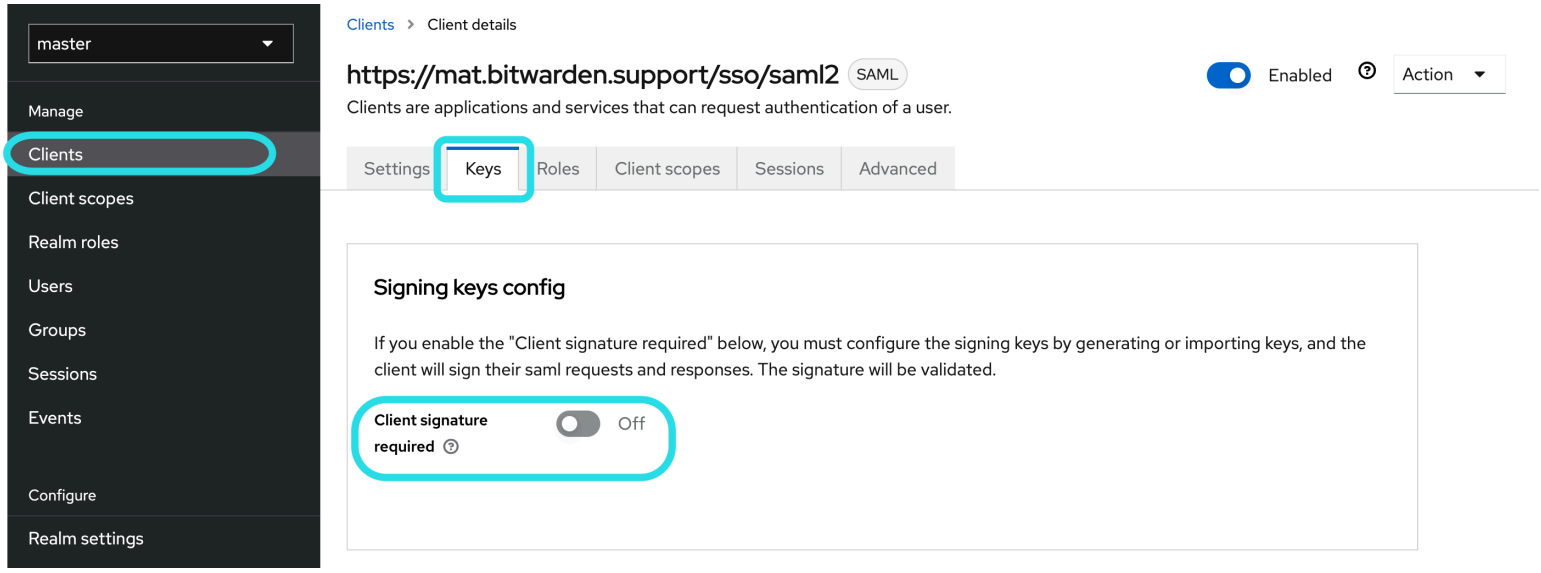
Una vez que haya completado los campos requeridos en la página de **Ajustes Generales**, haga clic en **Siguiente**.

En la pantalla de **ajustes de inicio de sesión**, complete el siguiente campo:

Campo	Descripción
URI de redireccionamiento válidos	Establezca este campo en la **URL del Servicio de Consumo de Aserciones (ACS)** pre-generada. Este valor generado automáticamente se puede copiar desde la pantalla de **Ajustes → Inicio de sesión único** de la organización y variará según su configuración.

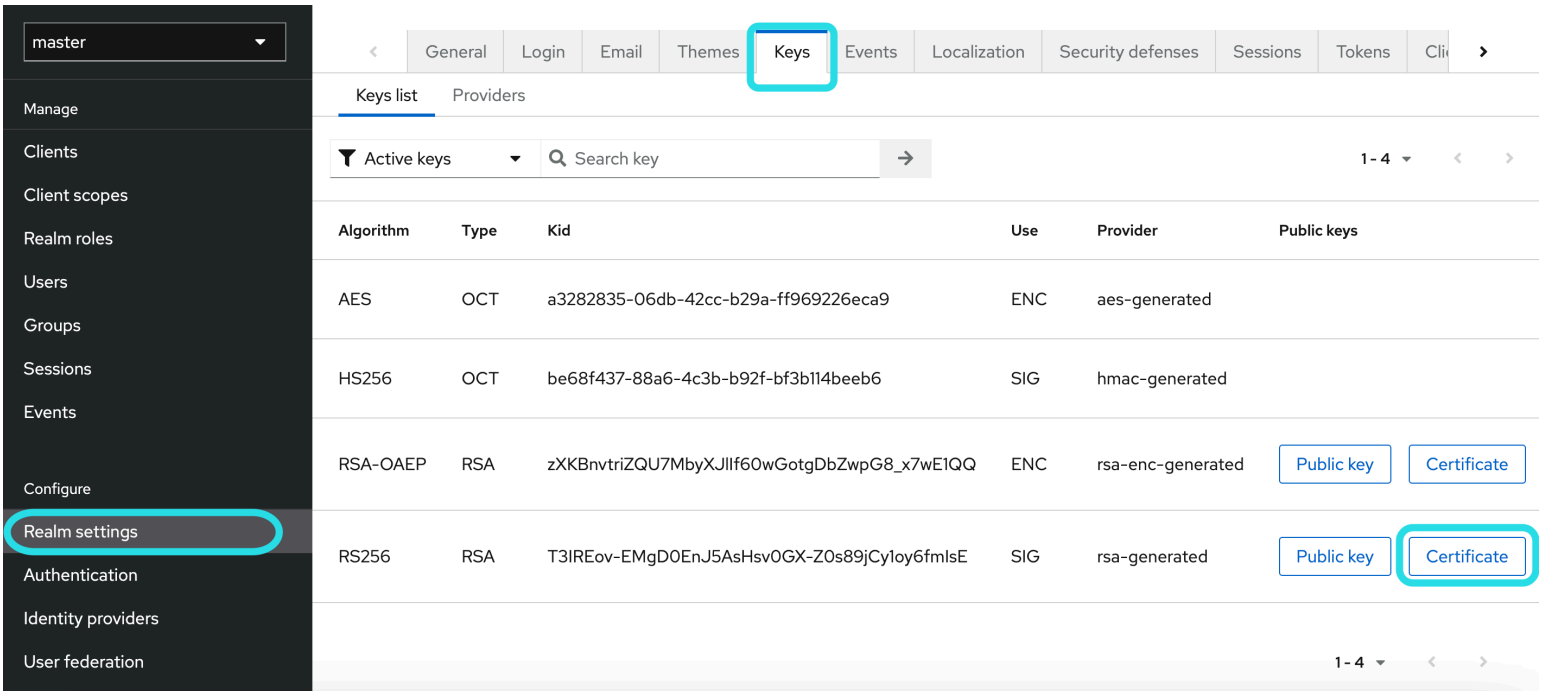
Selecciona **Guardar**.

Seleccione la pestaña de Keys y cambie la opción **Se requiere firma del cliente** a **Desactivado**.



Keycloak Keys Config

Por último, en la navegación principal de Keycloak, selecciona **Ajustes de Realm** y luego la **pestaña de Llaves**. Ubique el Certificado **RS256** y seleccione **Certificado**.



Keycloak RS256 Certificate

Se requerirá el valor del certificado para la siguiente sección.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal Keycloak. Regresa a la aplicación web de Bitwarden y selecciona **Ajustes → Inicio de sesión único** desde la navegación.

La pantalla de inicio de sesión único separa la configuración en dos secciones:

- **La configuración del proveedor de servicios SAML** determinará el formato de las solicitudes SAML.
- **La configuración del proveedor de identidad SAML** determinará el formato que se esperará de las respuestas SAML.

Complete los siguientes campos en la sección de **configuración del proveedor de servicio SAML**:

Campo	Descripción
Formato de ID de nombre	Seleccione **Correo electrónico**.
Algoritmo de Firma de Salida	El algoritmo que Bitwarden utilizará para firmar solicitudes SAML.

Campo	Descripción
Comportamiento de Firma	Si/cuando las solicitudes SAML serán firmadas.
Algoritmo de Firma de Entrada Mínima	Seleccione el algoritmo que el cliente Keycloak está configurado para usar para firmar documentos o afirmaciones SAML.
Quiero Firmas en las Afirmaciones	Si Bitwarden espera que las afirmaciones SAML estén firmadas. Si está activado, asegúrate de configurar el cliente de Keycloak para firmar afirmaciones.
Validar Certificados	Marque esta casilla cuando utilice certificados confiables y válidos de su IdP a través de una CA de confianza. Los certificados autofirmados pueden fallar a menos que se configuren cadenas de confianza adecuadas con la imagen de docker de inicio de sesión de Bitwarden con SSO.

Complete los siguientes campos en la sección de **configuración del proveedor de identidad SAML**:

Campo	Descripción
ID de la entidad	Ingrese la URL del reino de Keycloak en el que se creó el cliente, por ejemplo `https:///reinos/`. Este campo distingue entre mayúsculas y minúsculas.
Tipo de enlace	Selecciona **Redirigir**.
URL del servicio de inicio de sesión único	Ingrese su URL de procesamiento maestro SAML, por ejemplo `https:///reinos//protocolo/saml`.
URL del Servicio de Cierre de Sesión Único	El inicio de sesión con SSO actualmente **no** admite SLO. Esta opción está planeada para un desarrollo futuro, sin embargo, puedes preconfigurarla con tu **URL de cierre de sesión** si lo deseas.

Campo	Descripción
Certificado público X509	Ingrese el **certificado RS256** que se copió en el paso anterior. El valor del certificado es sensible a mayúsculas y minúsculas, espacios extra, retornos de carro y otros caracteres extraneous **harán que la validación del certificado falle**.
Algoritmo de Firma de Salida	Seleccione el algoritmo que el cliente Keycloak está configurado para usar para firmar documentos o afirmaciones SAML.
Deshabilitar Solicitudes de Cierre de Sesión Salientes	El inicio de sesión con SSO actualmente **no** admite SLO. Esta opción está planeada para un desarrollo futuro.
Quiere Solicitudes de Autenticación Firmadas	Si Keycloak espera que las solicitudes SAML estén firmadas.

> **Note**
> Al completar el certificado X509, toma nota de la fecha de vencimiento. Los certificados tendrán que ser renovados para prevenir cualquier interrupción en el servicio a los usuarios finales de SSO. Si un certificado ha caducado, las cuentas de Administrador y Propietario siempre podrán iniciar sesión con la dirección de correo electrónico y la contraseña maestra.

Cuando hayas terminado con la configuración del proveedor de identidad, **Guarda** tu trabajo.

> **Tip**
> Puede requerir que los usuarios inicien sesión con SSO activando la política de autenticación de inicio de sesión único. Por favor, tome nota, esto también requerirá la activación de la política de organización única. Más información.

Ajustes adicionales de Keycloak

En la **pestaña Configuración** del cliente Keycloak, hay opciones de configuración adicionales disponibles:

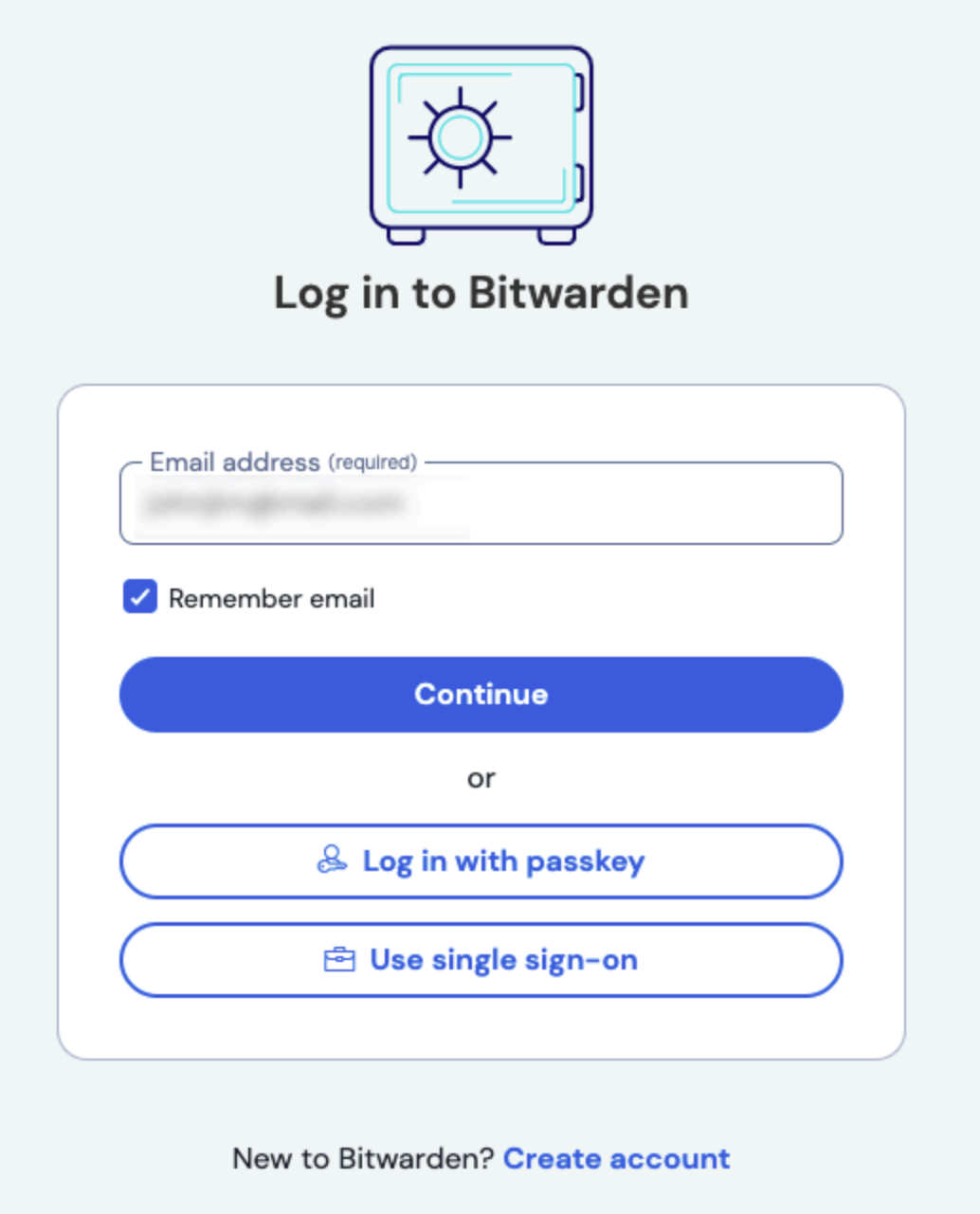
Campo	Descripción
Firmar Documentos	Especifique si los documentos SAML deben ser firmados por el reino Keycloak.
Firmar Declaraciones	Especifique si las afirmaciones de SAML deben ser firmadas por el reino de Keycloak.

Campo	Descripción
Algoritmo de Firma	Si **Afirmaciones de Signo** está habilitado, selecciona con qué algoritmo firmar (`sha-256` por defecto).
Formato de Identificación de Nombre	Seleccione el formato de ID de nombre que Keycloak utilizará en las respuestas SAML.

Una vez que hayas completado el foro, selecciona **Guardar**.

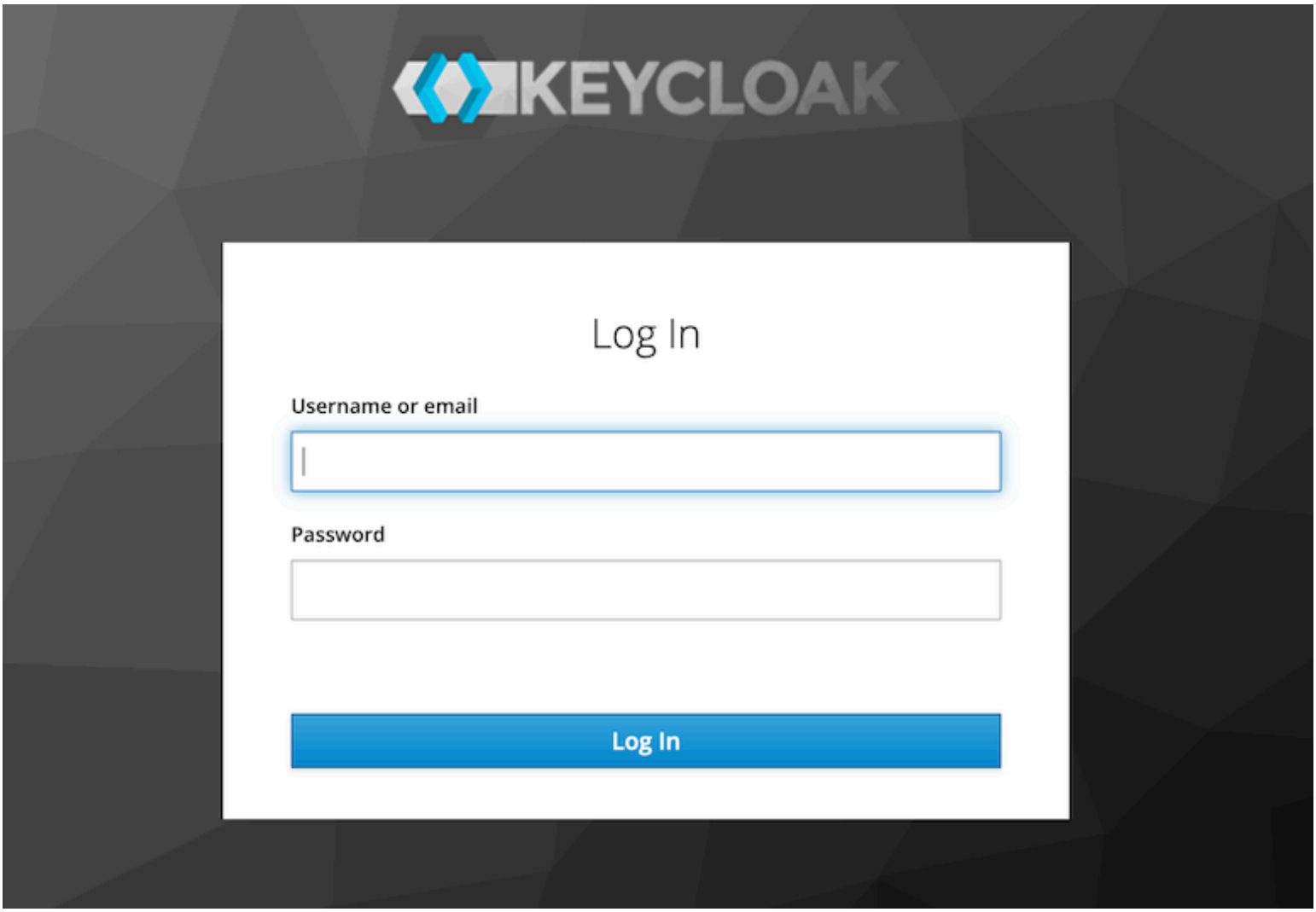
Prueba la configuración

Una vez que tu configuración esté completa, pruébala navegando a https://vault.bitwarden.com, ingresando tu dirección de correo electrónico, seleccionando **Continuar**, y seleccionando el botón **Empresa Único-Inicio**:



Inicio de sesión único empresarial y contraseña maestra

Ingrese el identificador de organización configurado y seleccione **Iniciar sesión**. Si su implementación está configurada con éxito, será redirigido a la pantalla de inicio de sesión de Keycloak:



Keycloak Login Screen

¡Después de autenticarte con tus credenciales de Keycloak, ingresa tu contraseña maestra de Bitwarden para descifrar tu caja fuerte!

> **Note**
> Bitwarden no admite respuestas no solicitadas, por lo que iniciar el inicio de sesión desde su IdP resultará en un error. El flujo de inicio de sesión de SSO debe iniciarse desde Bitwarden.