bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de Okta SAML

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

Implementación de Okta SAML

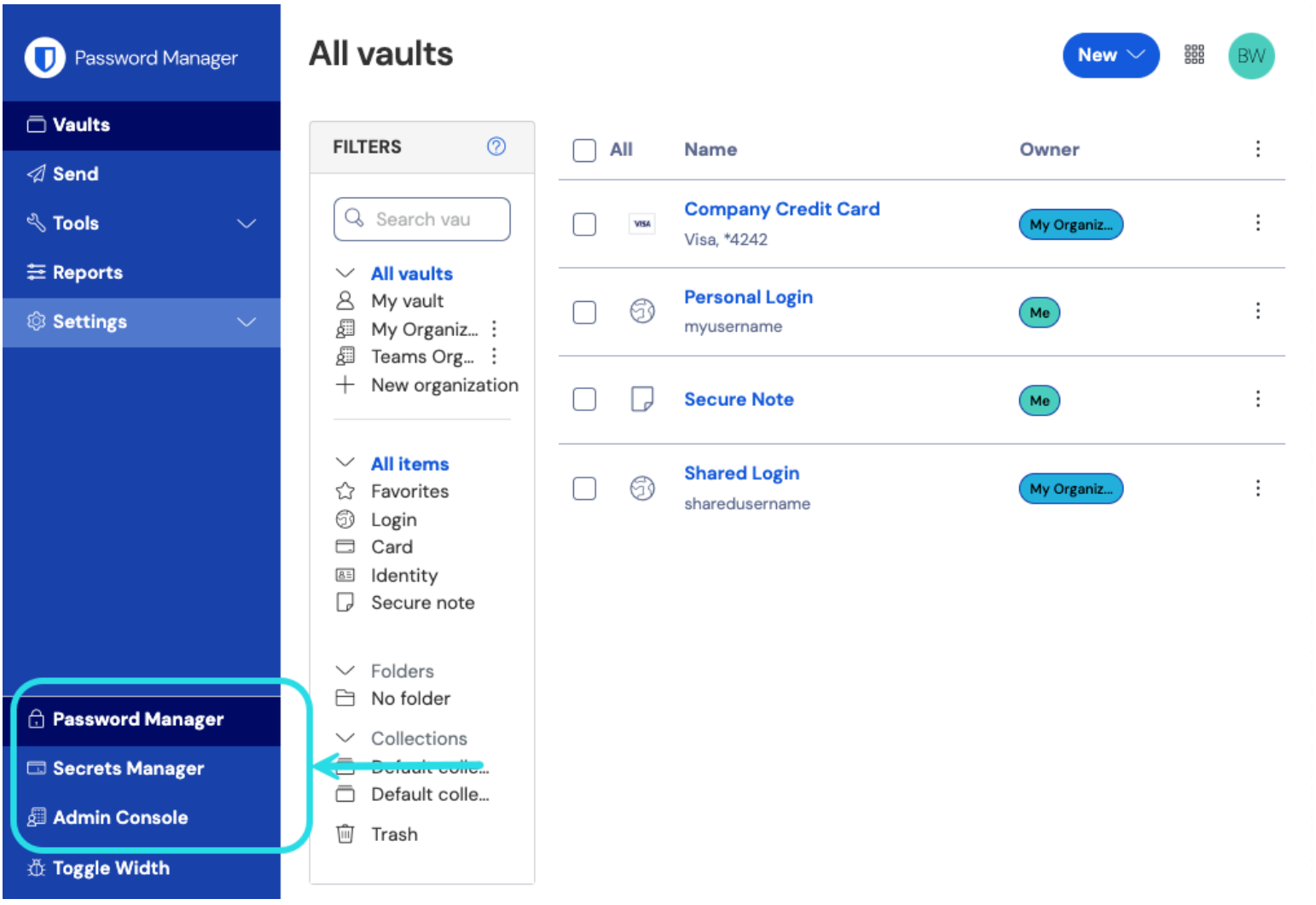
Este artículo contiene ayuda **específica de Okta** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte Configuración de SAML 2.0.

La configuración implica trabajar simultáneamente dentro de la aplicación web de Bitwarden y el Portal de Administrador de Okta. 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

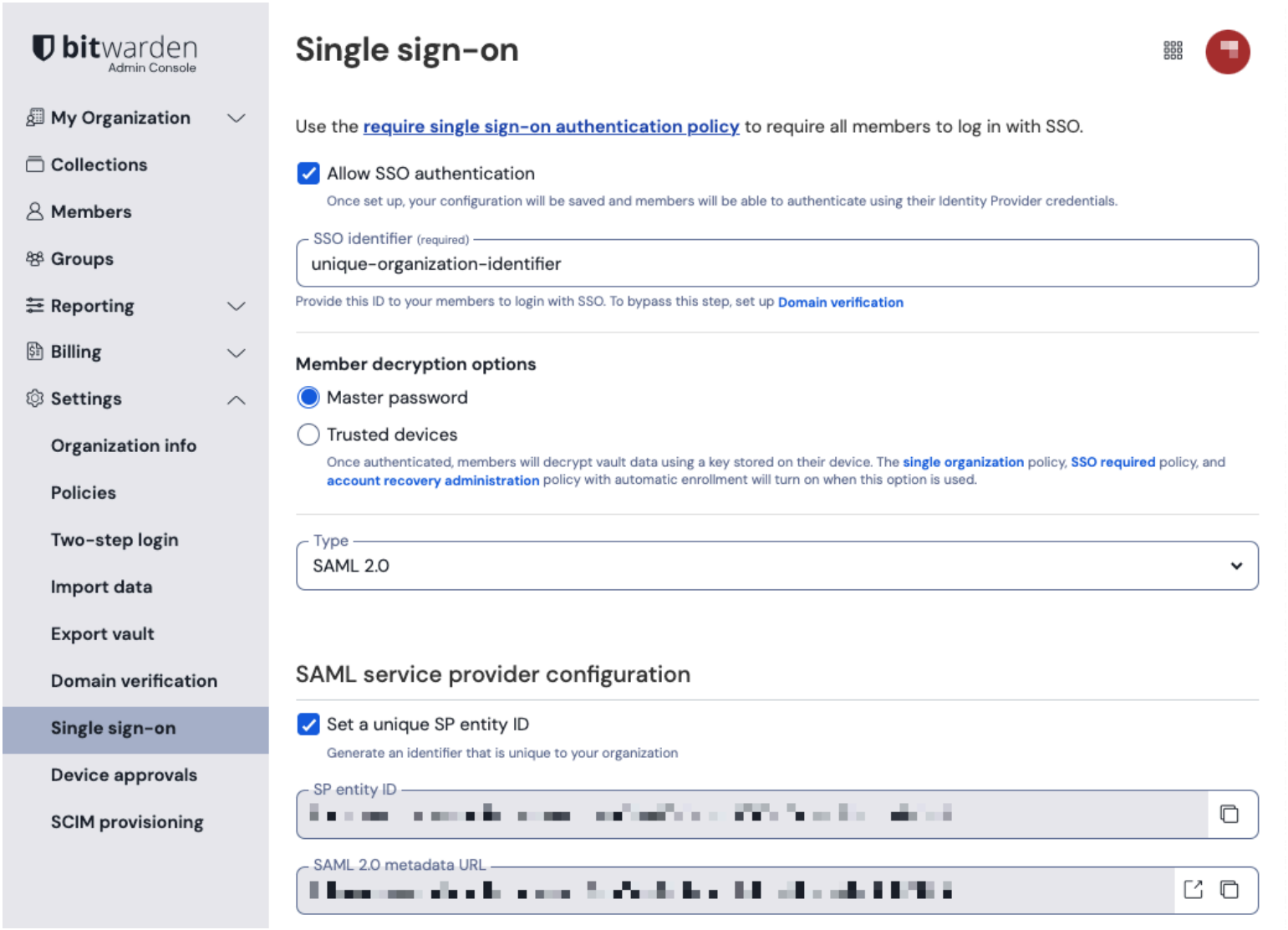
Abre SSO en la aplicación web

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

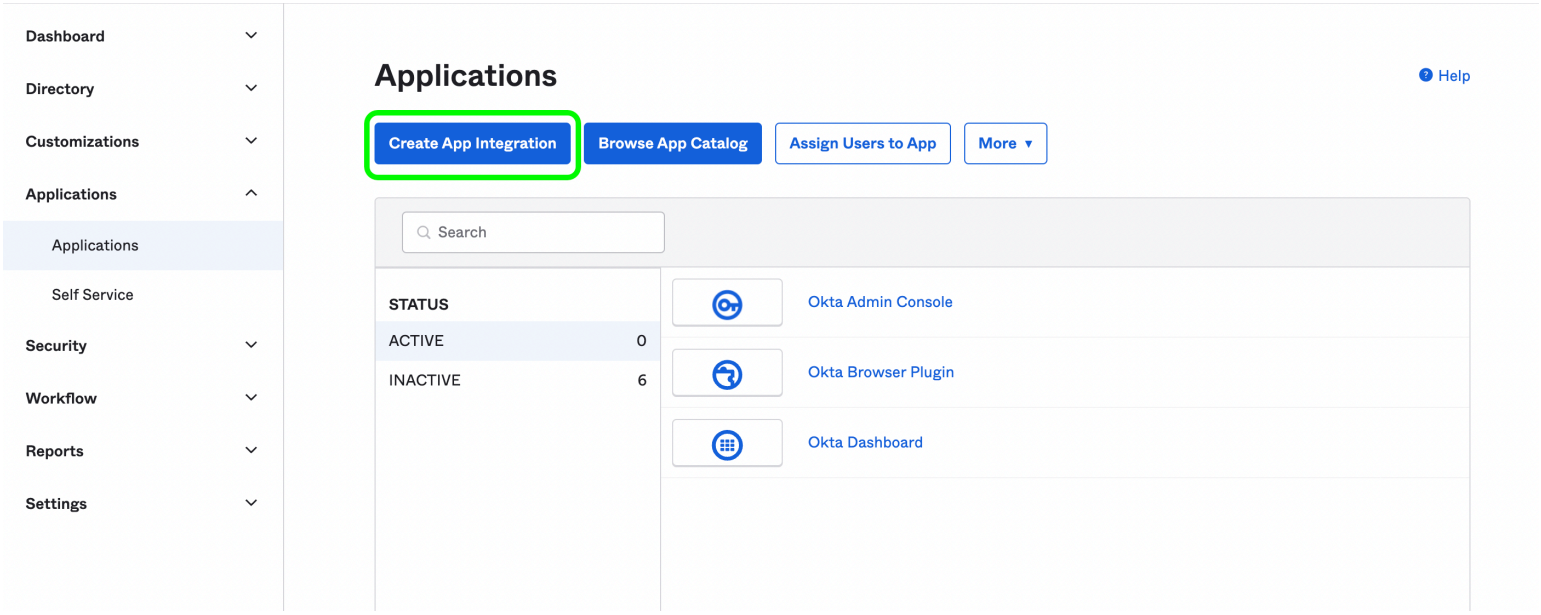
Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de **Tipo**. Mantén esta pantalla abierta para fácil referencia.

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 activada.

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

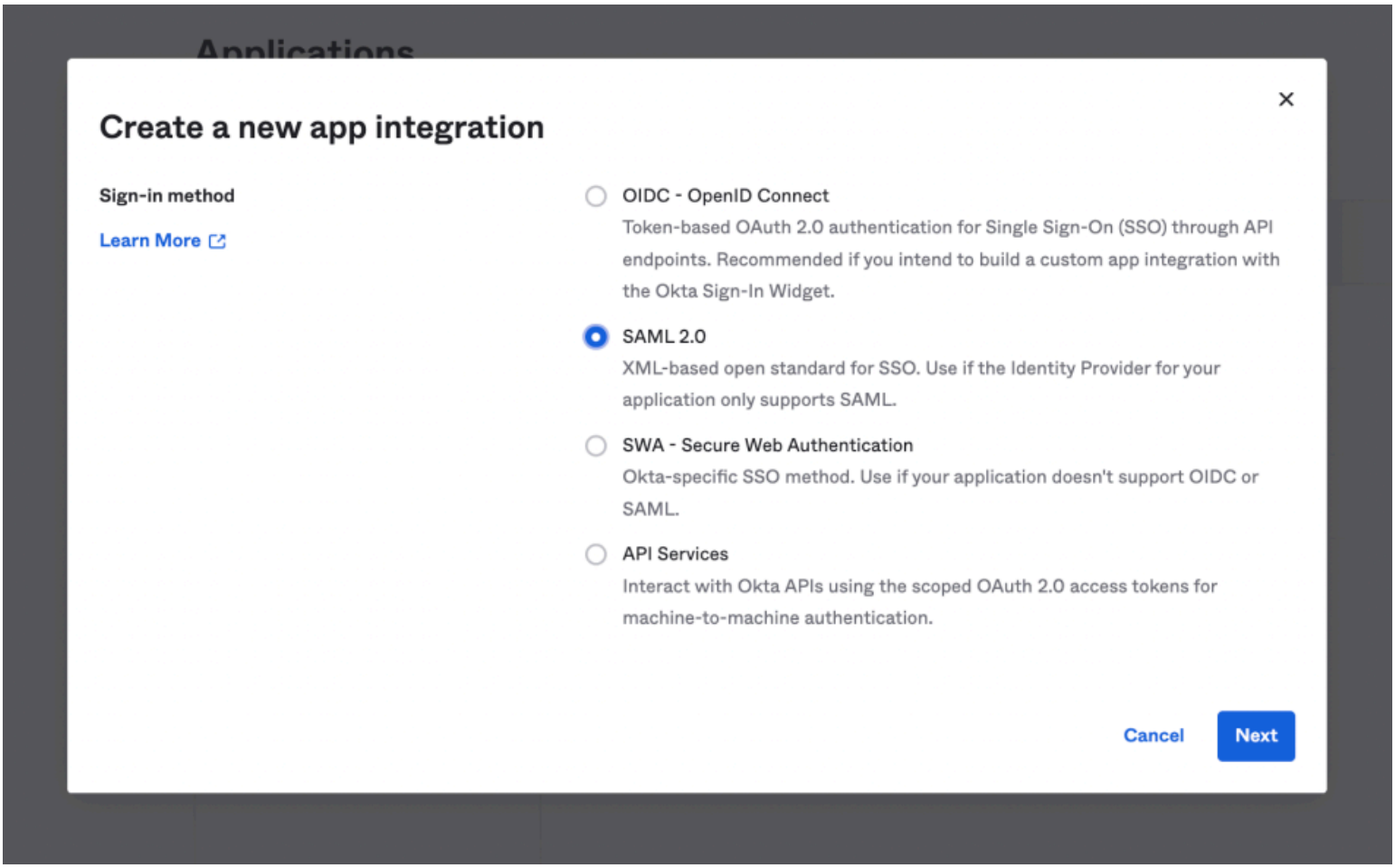
Crea una aplicación Okta

En el Portal de Administrador de Okta, selecciona **Aplicaciones → Aplicaciones** desde la navegación. En la pantalla de Aplicaciones, seleccione el botón **Crear Integración de Aplicación**:



Okta create app integration

En el cuadro de diálogo Crear una nueva integración de aplicación, seleccione el botón de opción **SAML 2.0**:



SAML 2.0 radio button

Seleccione el botón **Siguiente** para proceder a la configuración.

Ajustes generales

En la pantalla de **Ajustes Generales**, dale a la aplicación un nombre único, específico de Bitwarden y selecciona **Siguiente**.

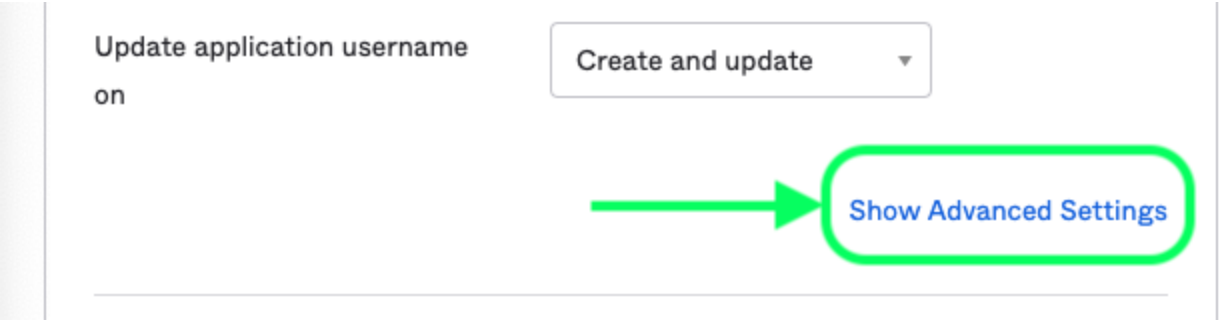
Configurar SAML

En la pantalla de **Configurar SAML**, configure los siguientes campos:

Campo	Descripción
URL de inicio de sesión único	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.
URI de la audiencia (ID de entidad SP)	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.
Formato de ID de nombre	Seleccione el formato SAML NameID para usar en las afirmaciones SAML. Por defecto, **No especificado**.
Nombre de usuario de la aplicación	Seleccione el atributo de Okta que los usuarios utilizarán para el inicio de sesión en Bitwarden.

Ajustes avanzados

Seleccione el enlace **Mostrar Ajustes Avanzados** y configure los siguientes campos:

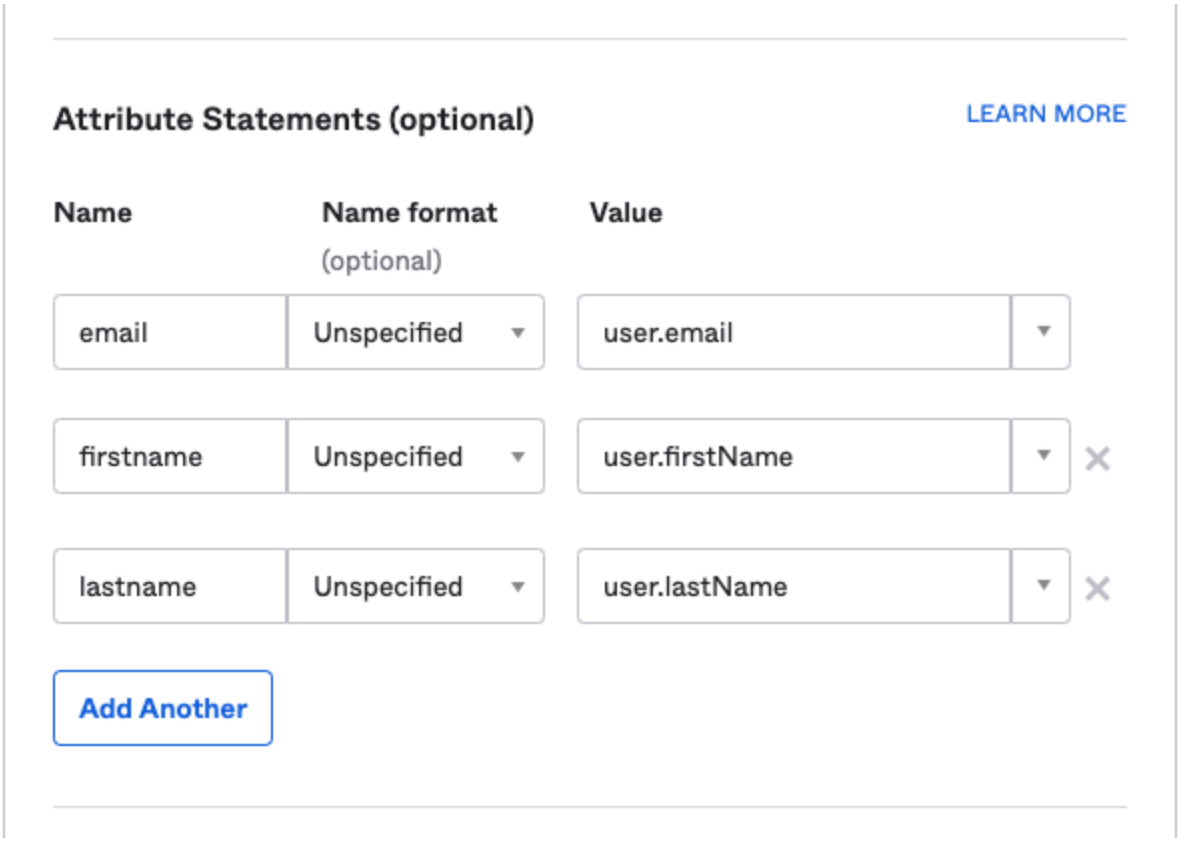


Advanced Settings

Campo	Descripción
Respuesta	Si la respuesta SAML está firmada por Okta.
Firma de Afirmación	Si la afirmación SAML está firmada por Okta.
Algoritmo de Firma	El algoritmo de firma utilizado para firmar la respuesta y/o afirmación, dependiendo de cuál esté configurado como **Firmado**. Por defecto, `rsa-sha256`.
Algoritmo de Digestión	El algoritmo de resumen utilizado para firmar la respuesta y/o afirmación, dependiendo de cuál esté configurado para **Firmado**. Este campo debe coincidir con el **Algoritmo de Firma** seleccionado.

Declaraciones de atributos

En la sección de **Declaraciones de Atributos**, construye las siguientes asignaciones de atributos SP → IdP:

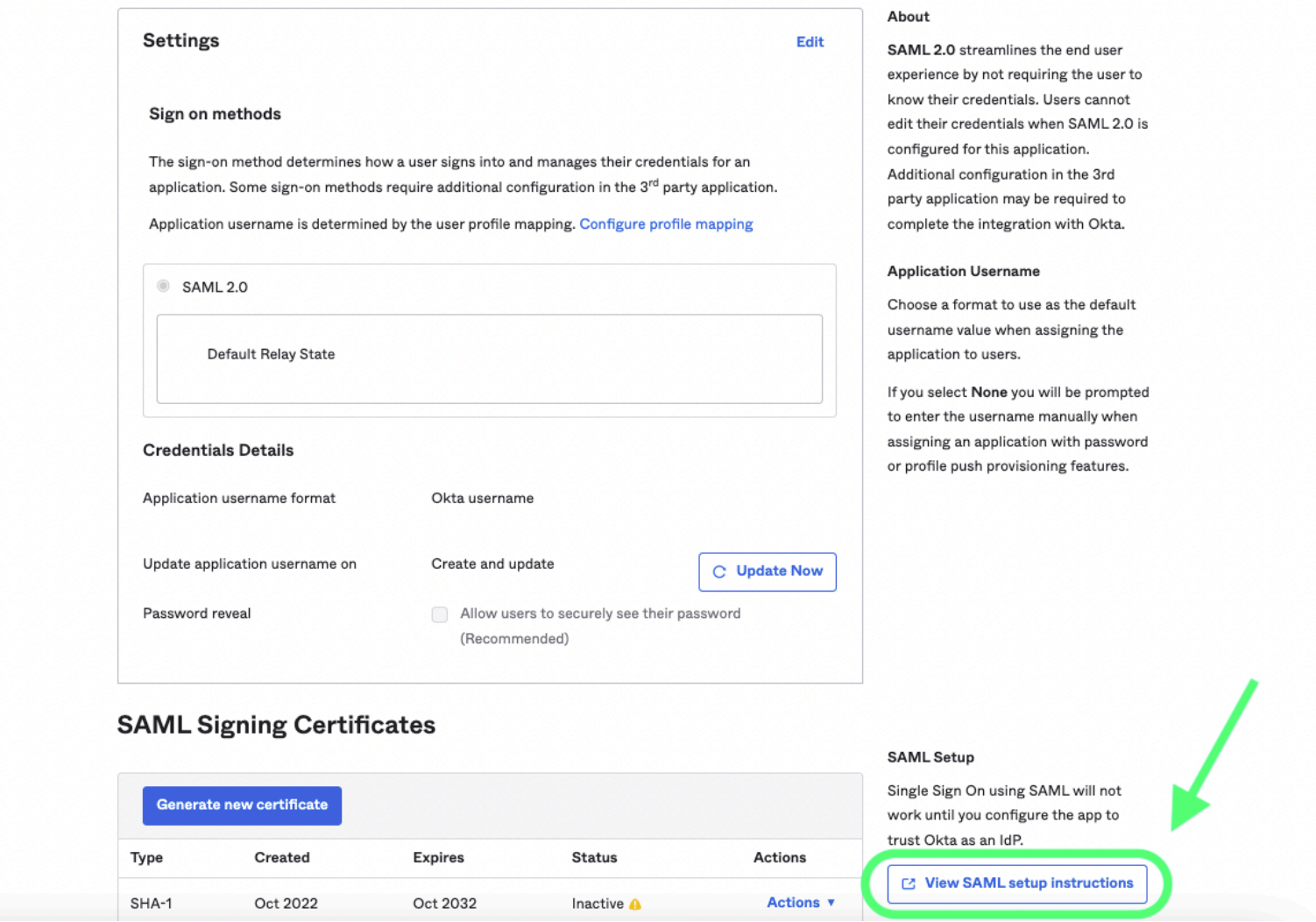


Attribute Statements

Una vez configurado, seleccione el botón **Siguiente** para proceder a la pantalla de **Comentarios** y seleccione **Finalizar**.

Obtener valores de IdP

Una vez que se ha creado su aplicación, seleccione la pestaña **Iniciar Sesión** para la aplicación y seleccione el botón **Ver Instrucciones de Configuración** ubicado en el lado derecho de la pantalla:



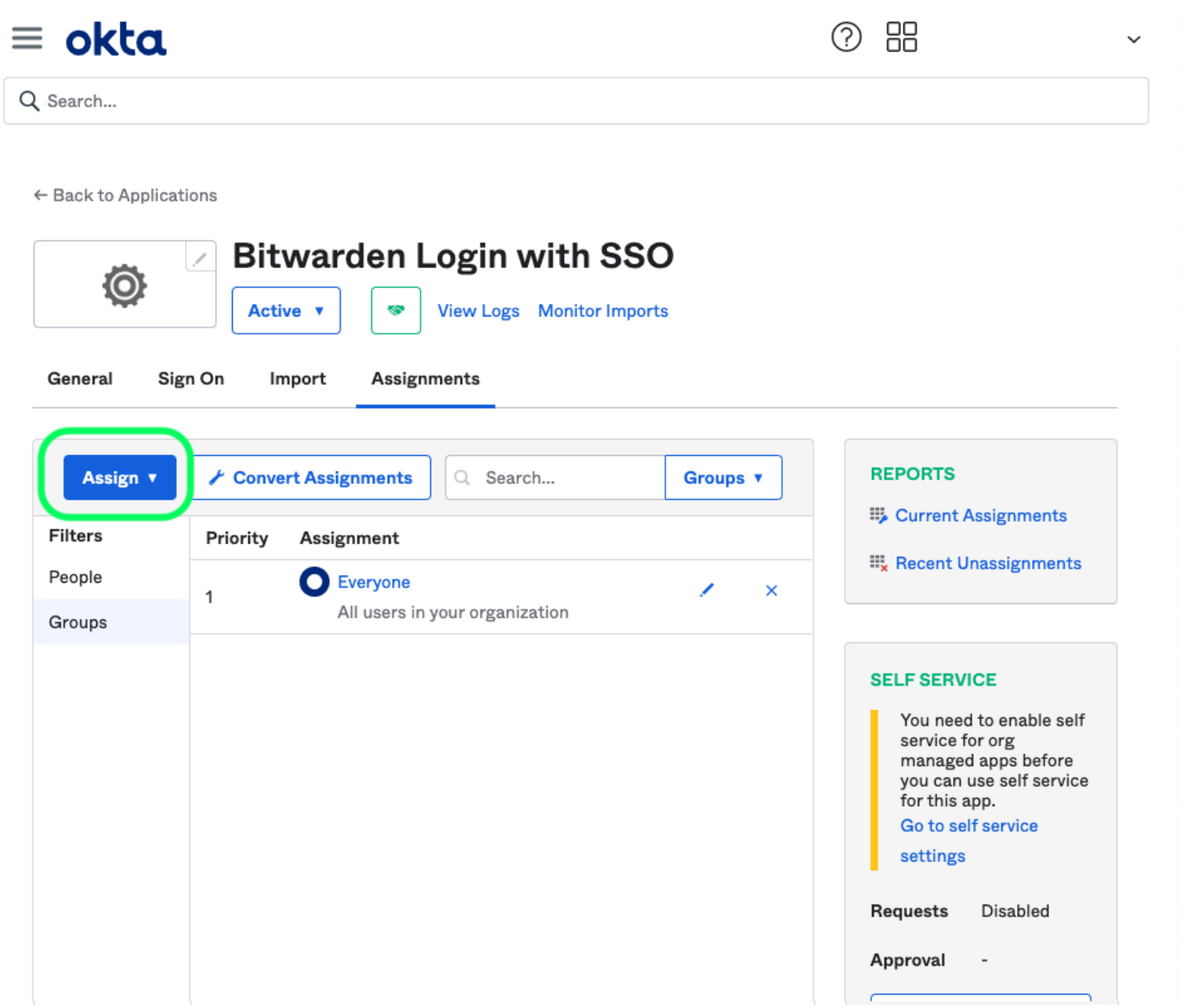
View SAML setup instructions

Deja esta página abierta para uso futuro, o copia la **URL de inicio de sesión único del proveedor de identidad** y el **emisor del proveedor de identidad** y descarga el **Certificado X.509**:

IdP Values

Tareas

Navega a la pestaña **Tareas** y selecciona el botón **Asignar**:



Assigning Groups

Puede asignar acceso a la aplicación de manera individual utilizando la opción **Asignar a Personas**, o en masa utilizando la opción **Asignar a Grupos**.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal de Administrador de Okta. Regresa a la aplicación web de Bitwarden para completar la configuración.

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.

Configuración del proveedor de servicios

Configure los siguientes campos de acuerdo a las opciones seleccionadas en el Portal de Administrador de Okta durante la creación de la aplicación:

Campo	Descripción
Formato de Identificación de Nombre	Establezca esto en cualquier formato de ID de nombre especificado en Okta, de lo contrario, deje **Sin especificar**.
Algoritmo de Firma de Salida	El algoritmo que Bitwarden utilizará para firmar solicitudes SAML.
Comportamiento de Firma	Si/cuando las solicitudes SAML serán firmadas.
Algoritmo de Firma de Entrada Mínima	Establezca esto en el Algoritmo de Firma especificado en Okta.
Quiero Afirmaciones Firmadas	Marca esta casilla si estableces el campo de Firma de Afirmación a **Firmado** en Okta.
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 dentro de la imagen de docker de inicio de sesión de Bitwarden con SSO.

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

Configuración del proveedor de Identidad

La configuración del proveedor de Identidad a menudo requerirá que vuelvas al Portal de Administrador de Okta para recuperar los valores de la aplicación:

Campo	Descripción
ID de la entidad	Ingrese su **Proveedor de Identidad Emisor**, recuperado de la pantalla de Ajustes de Inicio de Sesión de Okta seleccionando el botón de **Ver Instrucciones de Configuración**. Este campo distingue entre mayúsculas y minúsculas.
Tipo de Encuadernación	Establecer para **Redirigir**. Actualmente, Okta no admite HTTP POST.
URL del Servicio de Inicio de Sesión Único	Ingrese su **URL de inicio de sesión único del proveedor de Identidad**, obtenida de la pantalla de ajustes de inicio de sesión de Okta.
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 si lo deseas.

Certificado Público X509	Pega el certificado descargado, eliminando
	`-----INICIO CERTIFICADO-----`
	y
	`-----FIN DEL CERTIFICADO-----`
	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 de Firma seleccionado durante la configuración de la aplicación Okta. Si no cambió el Algoritmo de Firma, deje el predeterminado (`rsa-sha256`).
Permitir peticiones de cierre de sesión	El inicio de sesión con SSO actualmente **no** admite SLO.
Quiere Solicitudes de Autenticación Firmadas	Si Okta espera que las solicitudes SAML estén firmadas.

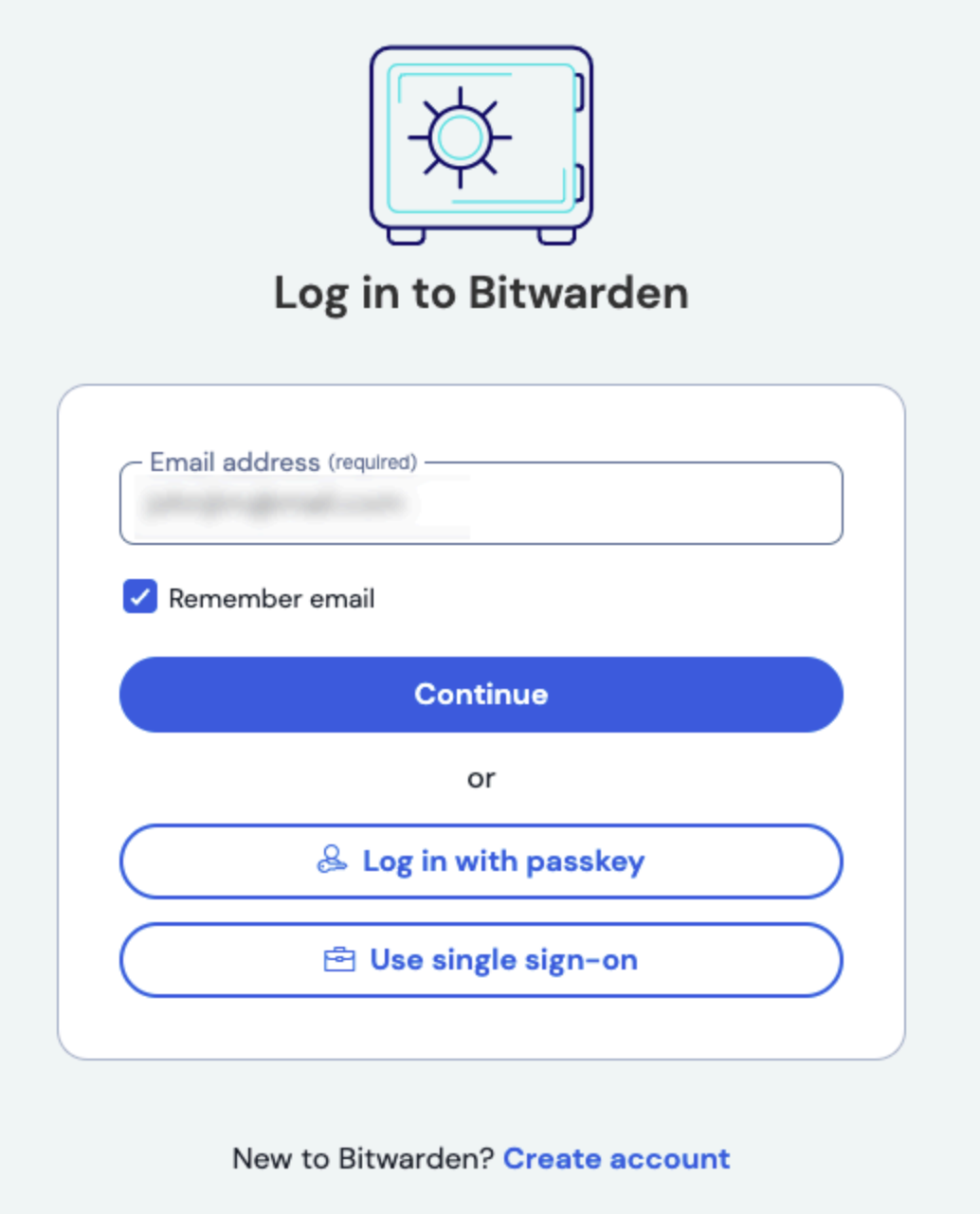
> **Note**
> Al completar el certificado X509, toma nota de la fecha de vencimiento. Los certificados tendrán que ser renovados para prevenir cualquier interrupción en el servicio a los usuarios finales de SSO. Si un certificado ha caducado, las cuentas de Administrador y Propietario siempre podrán iniciar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

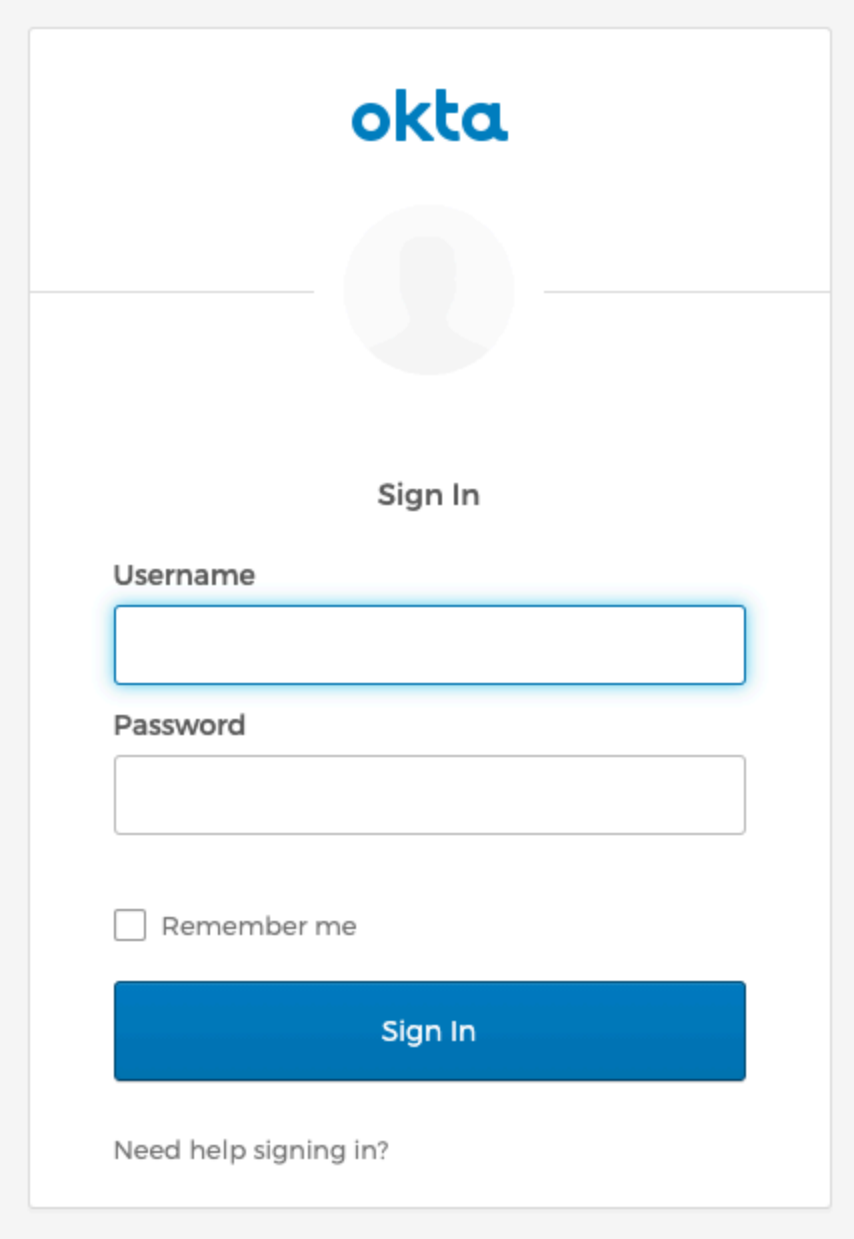
Prueba la configuración

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 de **Empresa de Inicio de Sesión Único**:



Inicio de sesión único empresarial y contraseña maestra

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



Log in with Okta

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

Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an Okta Bookmark App that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.
2. Click **Browse App Catalog**.
3. Search for **Bookmark App** and click **Add Integration**.
4. Add the following settings to the application:
    1. Give the application a name such as **Bitwarden Login**.
    2. In the **URL** field, provide the URL to your Bitwarden client such as `https://vault.bitwarden.com/#/login` or `your-self-hostedURL.com`.
5. Select **Done** and return to the applications dashboard and edit the newly created app.
6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained here.

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.