bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de Okta OIDC

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

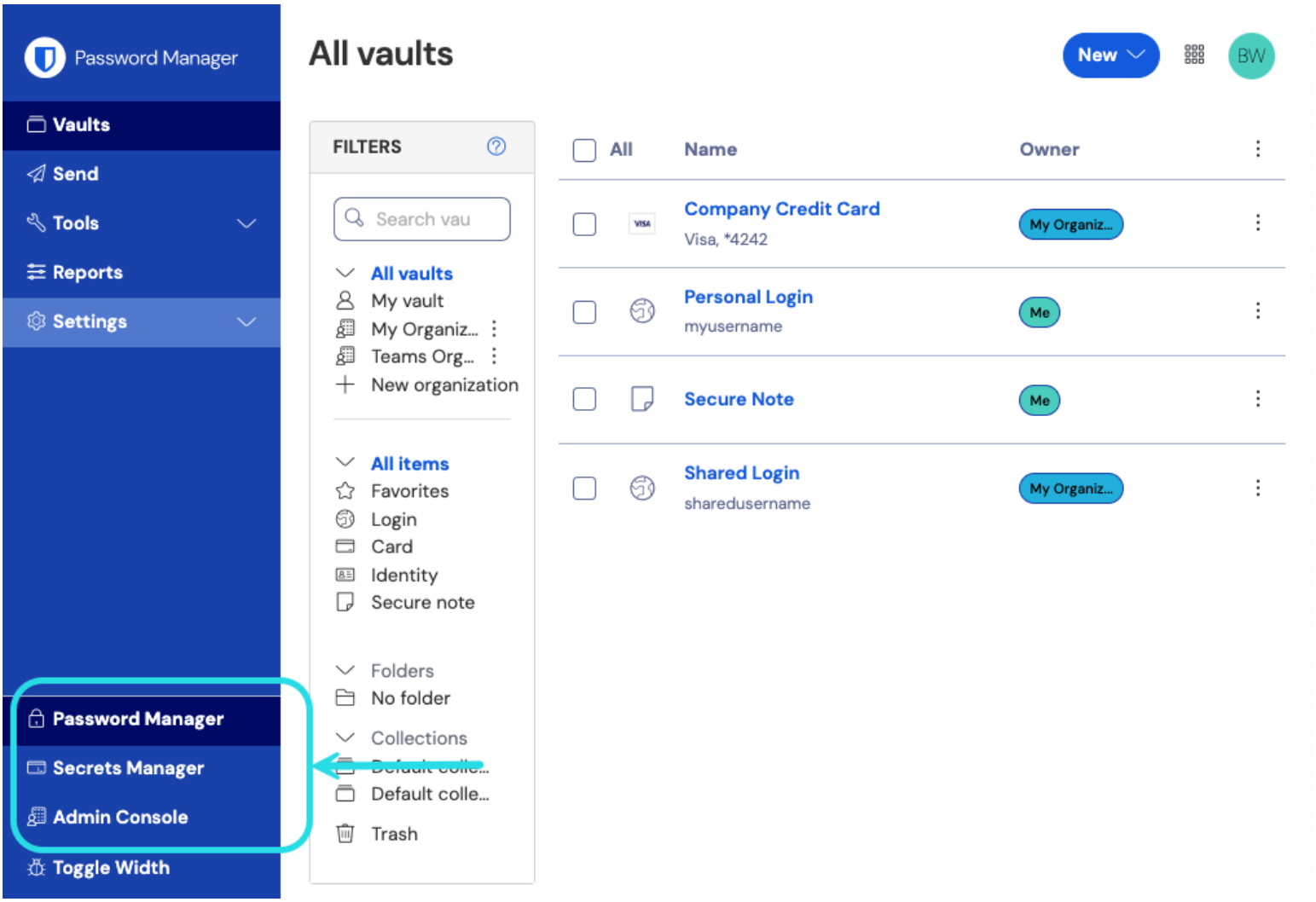
Implementación de Okta OIDC

Este artículo contiene ayuda **específica de Okta** para configurar el inicio de sesión con SSO a través de OpenID Connect (OIDC). Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP OIDC, o para configurar Okta a través de SAML 2.0, consulte Configuración OIDC o Implementación Okta SAML.

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.

Abre SSO en la caja fuerte web

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



Selector de producto

Seleccione **Ajustes → Inicio de sesión único** desde la navegación:

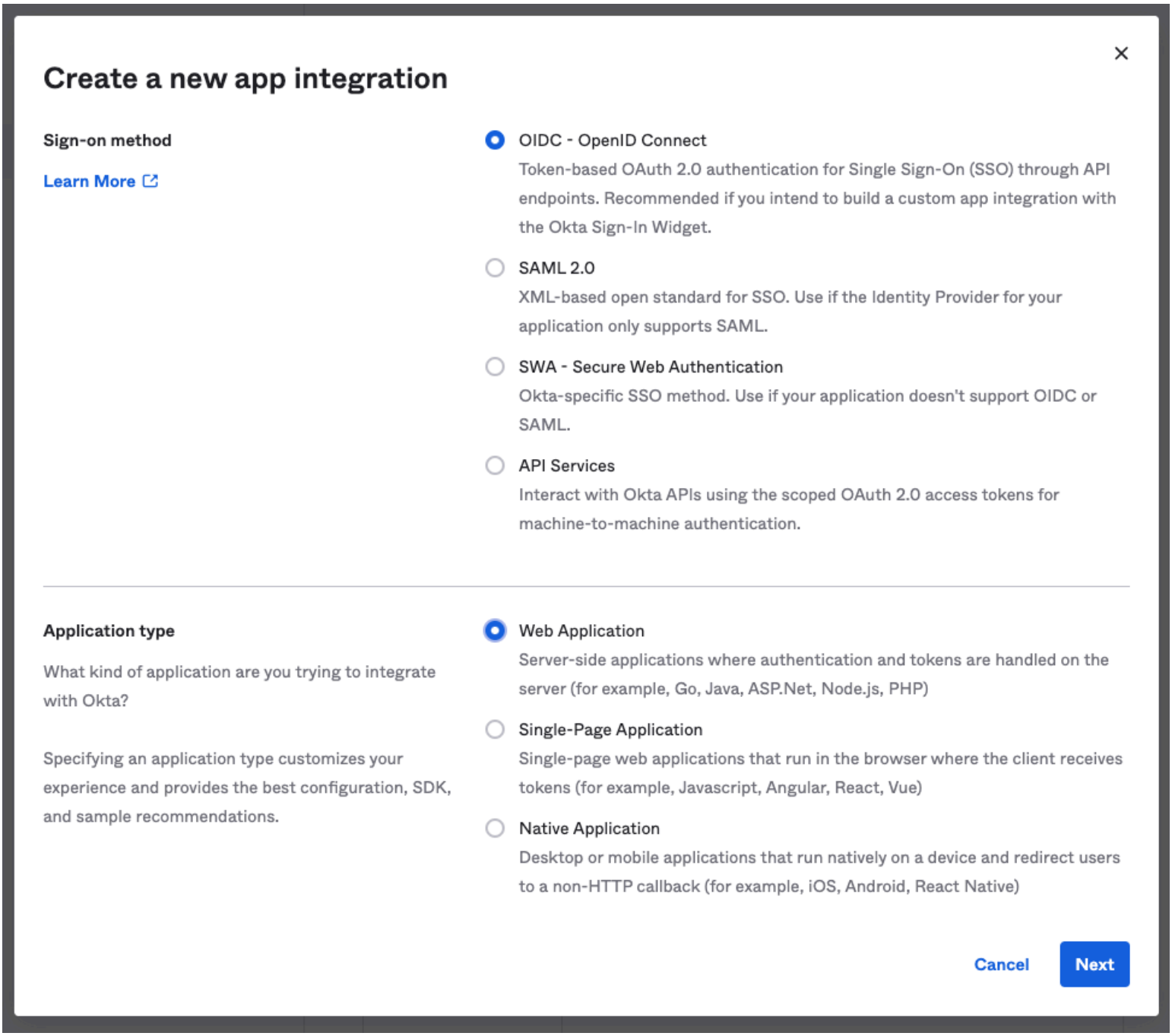
Configuración de OIDC

Si aún no lo has hecho, crea un **identificador SSO** único para tu organización. De lo contrario, no necesitas editar nada en esta pantalla todavía, pero mantenla abierta para una fácil referencia.

> **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**. Para el método de inicio de sesión, seleccione **OIDC - OpenID Connect**. Para el tipo de aplicación, seleccione **Aplicación Web**:



Create App Integration

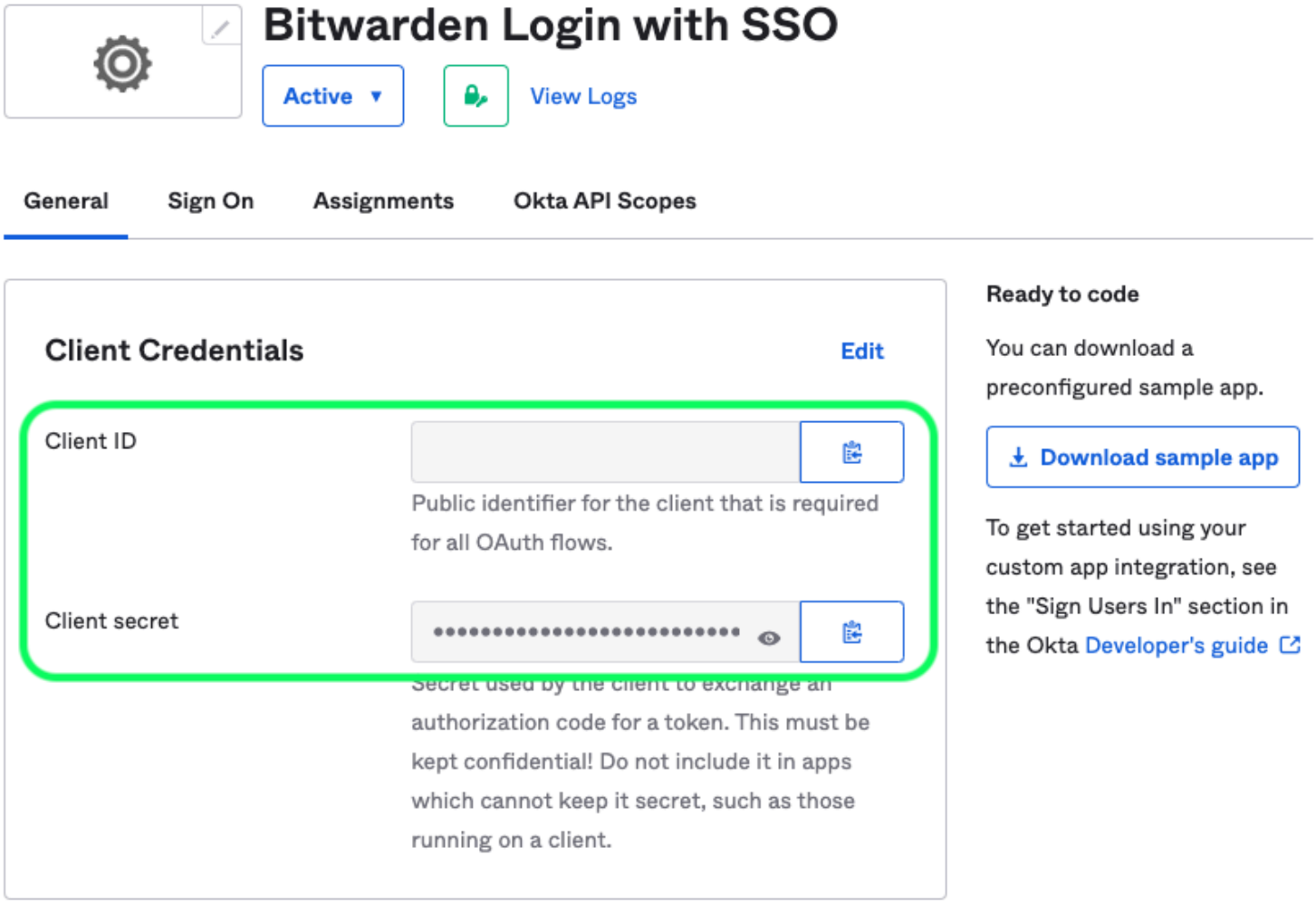
En la pantalla de **Integración de Nueva Aplicación Web**, configure los siguientes campos:

Campo	Descripción
Nombre de integración de la aplicación	Dale a la aplicación un nombre específico de Bitwarden.
Tipo de subvención	Habilita los siguientes tipos de concesión: - Cliente actuando en nombre de sí mismo → **Credenciales del Cliente** - Cliente actuando en nombre de un usuario → **Código de Autorización**
URI de redirección de inicio de sesión	Establezca este campo en su **Ruta de devolución de llamada**, que se puede obtener de la pantalla de configuración de SSO de Bitwarden. Para los clientes alojados en la nube, esto es `https://sso.bitwarden.com/oidc-signin` o `https://sso.bitwarden.eu/oidc-signin`. Para instancias autoalojadas, esto está determinado por su URL de servidor configurado, por ejemplo `https://your.domain.com/sso/oidc-signin`.
URI de redirección de cierre de sesión	Establezca este campo en su **Ruta de devolución de llamada cuando se cierra la sesión**, que se puede obtener de la pantalla de configuración de SSO de Bitwarden.
Tareas	Utilice este campo para designar si todos o solo grupos selectos podrán usar el inicio de sesión de Bitwarden con SSO.

Una vez configurado, seleccione el botón **Siguiente**.

Obtener credenciales de cliente

En la pantalla de la Aplicación, copiar el **ID del Cliente** y el **Secreto del Cliente** para la nueva aplicación Okta creada:

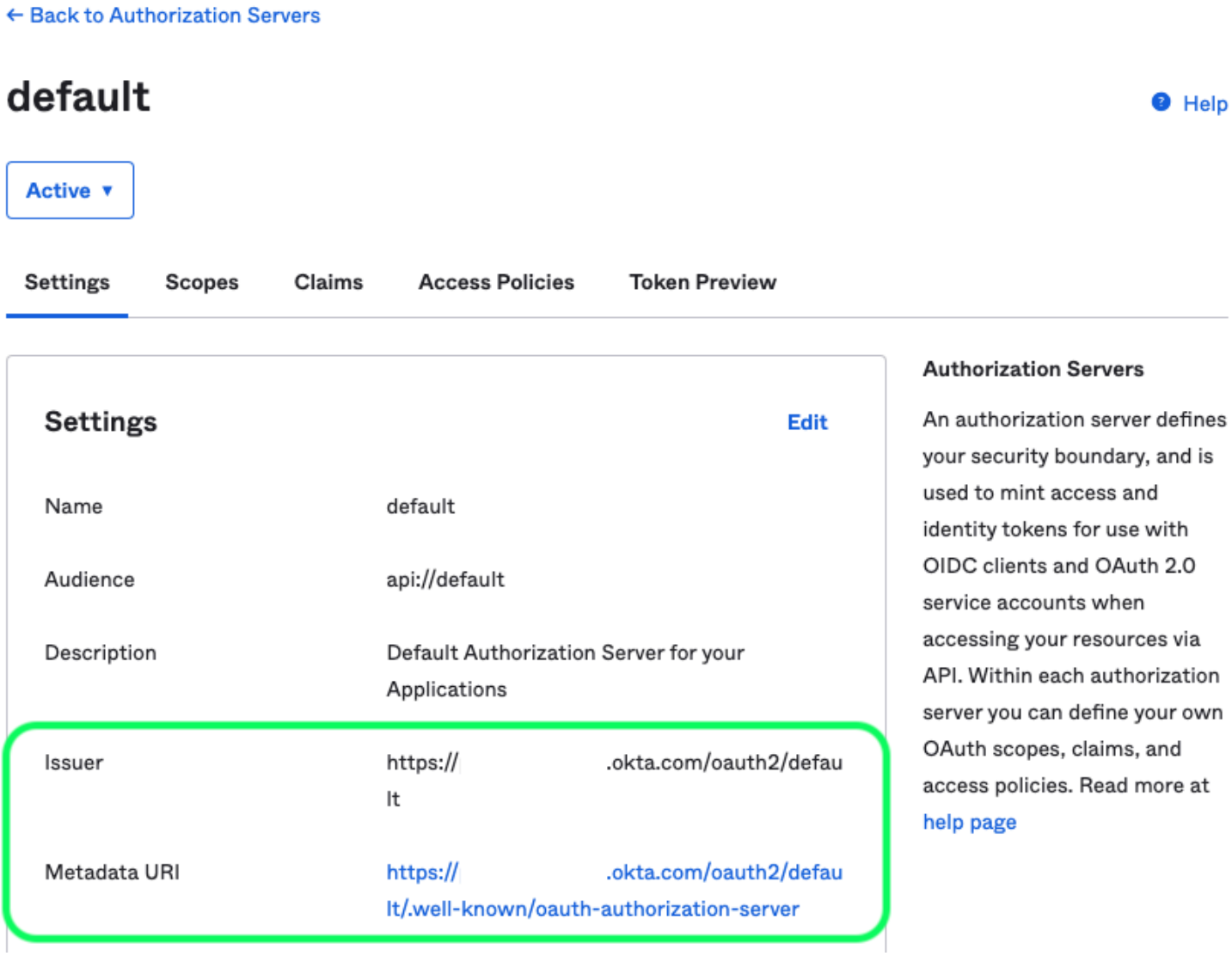


App Client Credentials

Necesitarás usar ambos valores durante un paso posterior.

Obtener información del servidor de autorización

Seleccione **Seguridad** → **API** desde la navegación. De la lista de **Servidores de Autorización**, selecciona el servidor que te gustaría usar para esta implementación. En la pestaña **Ajustes** para el servidor, copiar los valores de **Emisor** y **URI de Metadatos**:



Okta Authorization Server Settings

Necesitarás usar ambos valores durante el próximo paso.

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 configurar los siguientes campos:

Campo	Descripción
Autoridad	Ingrese el URI del emisor recuperado para su Servidor de Autorización.
ID de cliente	Ingrese el ID de Cliente recuperado para su aplicación Okta.

Campo	Descripción
Secreto del Cliente	Ingrese el secreto de Cliente recuperado para su aplicación Okta.
Dirección de Metadatos	Ingrese el URI de Metadatos recuperados para su Servidor de Autorización.
Comportamiento de Redirección OIDC	Seleccione **Redirigir GET**. Actualmente, Okta no admite Form POST.
Obtener Reclamaciones del Punto Final de Información del Usuario	Habilite esta opción si recibe errores de URL demasiado larga (HTTP 414), URLS truncadas y/o fallas durante el SSO.
Alcances Adicionales/Personalizados	Define los alcances personalizados para agregar a la solicitud (delimitados por comas).
Tipos de Reclamaciones de ID de Usuario Adicionales/Personalizadas	Defina las claves de tipo de reclamación personalizadas para la identificación del usuario (delimitadas por comas). Cuando se definen, se busca los tipos de reclamaciones personalizadas antes de recurrir a los tipos estándar.
Tipos de Reclamaciones de Correo Electrónico Adicionales/Personalizadas	Defina las claves de tipo de reclamación personalizadas para las direcciones de correo electrónico de los usuarios (delimitadas por comas). Cuando se definen, se busca los tipos de reclamaciones personalizadas antes de recurrir a los tipos estándar.
Tipos de Reclamaciones de Nombres Adicionales/Personalizados	Defina las claves de tipo de reclamación personalizadas para los nombres completos o nombres de visualización de los usuarios (delimitados por comas). Cuando se definen, se busca los tipos de reclamaciones personalizadas antes de recurrir a los tipos estándar.
Valores de referencia de la clase de contexto de autenticación solicitados	Defina los identificadores de referencia de la clase de contexto de autenticación (`acr_values`) (delimitados por espacios). Lista `acr_values` en orden de preferencia.

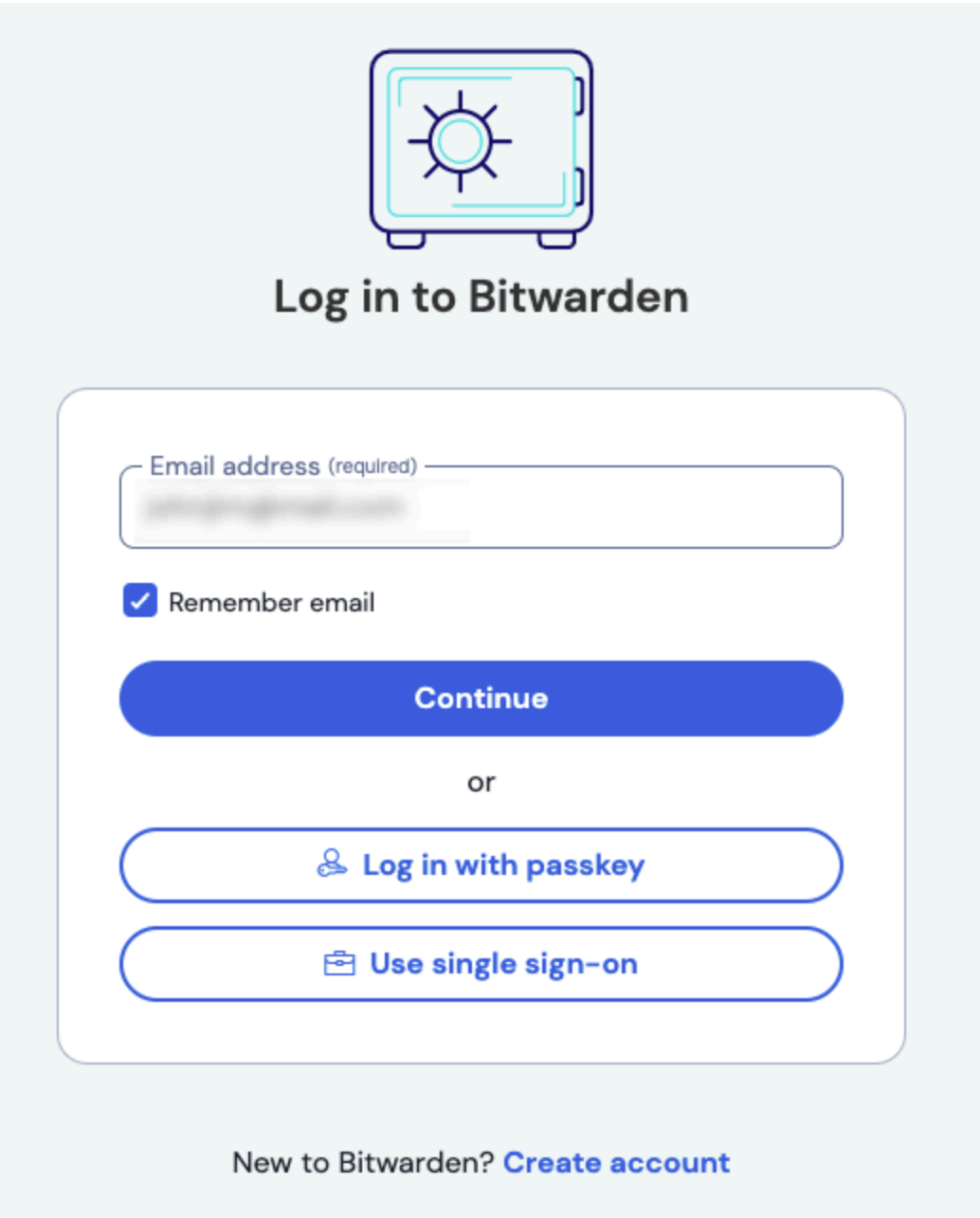
Campo	Descripción
Valor de reclamación "acr" esperado en respuesta	Define el valor de la reclamación `acr` que Bitwarden espera y valida en la respuesta.

Cuando hayas terminado de configurar estos campos, **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.

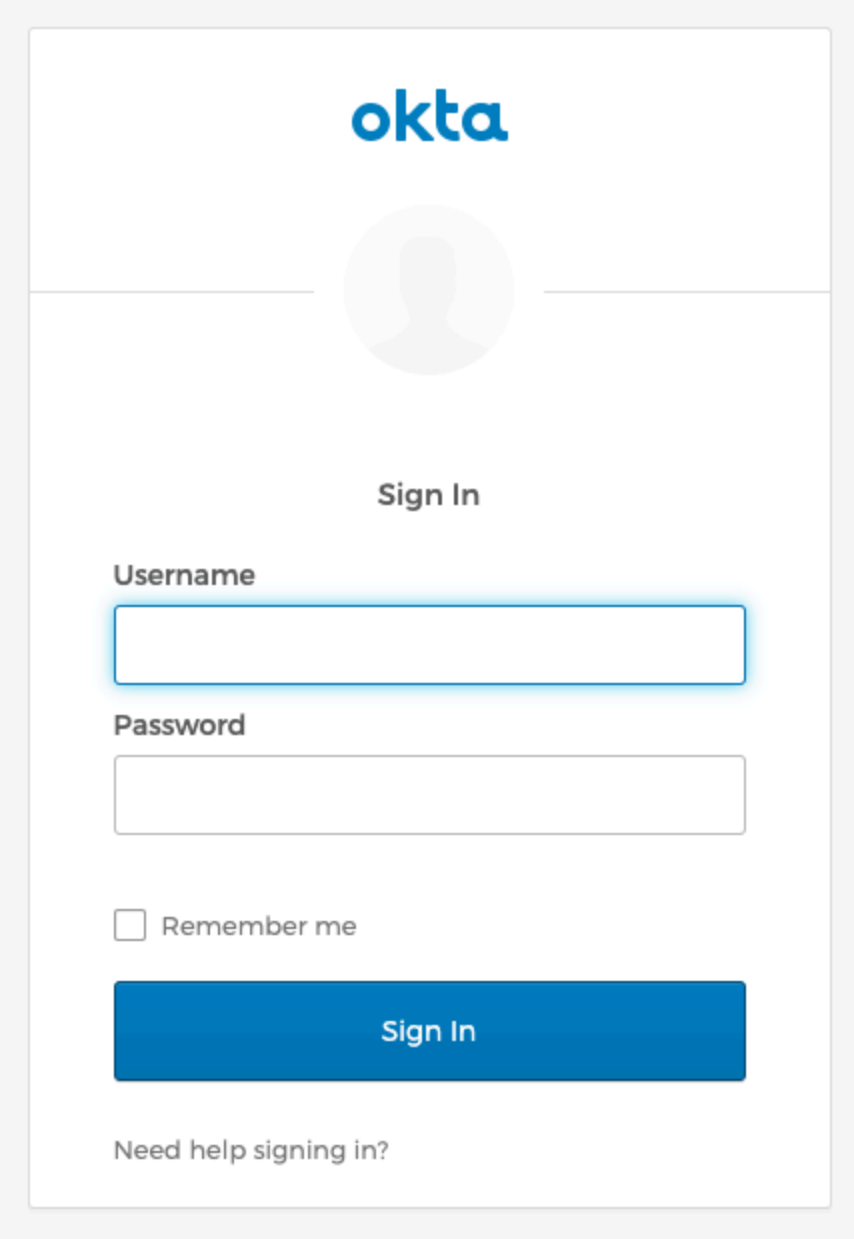
Prueba la configuración

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 **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 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.