bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de Microsoft Entra ID OIDC

Ver en el centro de ayuda:
https://bitwarden.com/help/oidc-microsoft-entra-id/

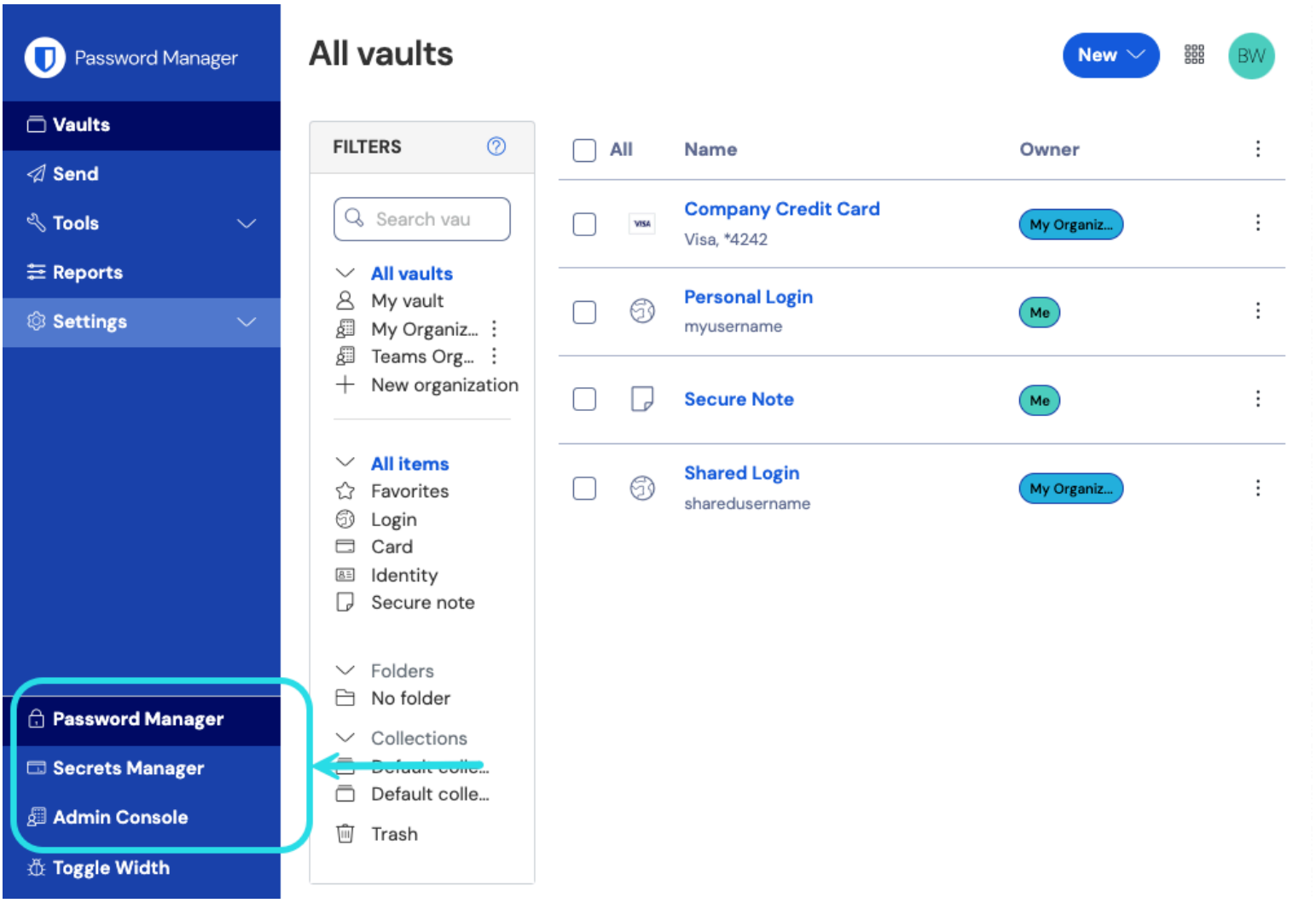
Implementación de Microsoft Entra ID OIDC

Este artículo contiene ayuda **específica de Azure** 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 Microsoft Entra ID a través de SAML 2.0, consulte Configuración OIDC o Implementación de Microsoft Entra ID SAML.

La configuración implica trabajar simultáneamente dentro de la aplicación web de Bitwarden y el Portal de Azure. 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 usando el cambiador de producto (⊞):



Selector de producto

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

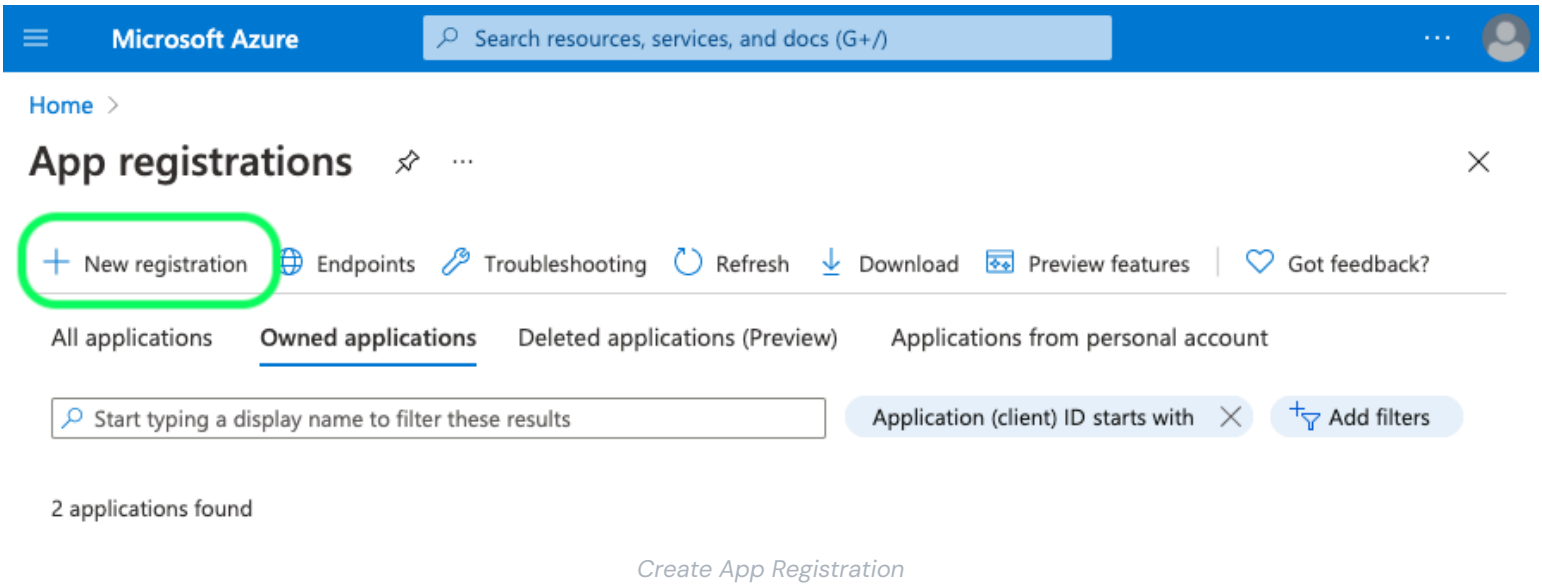
Configuración de OIDC

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

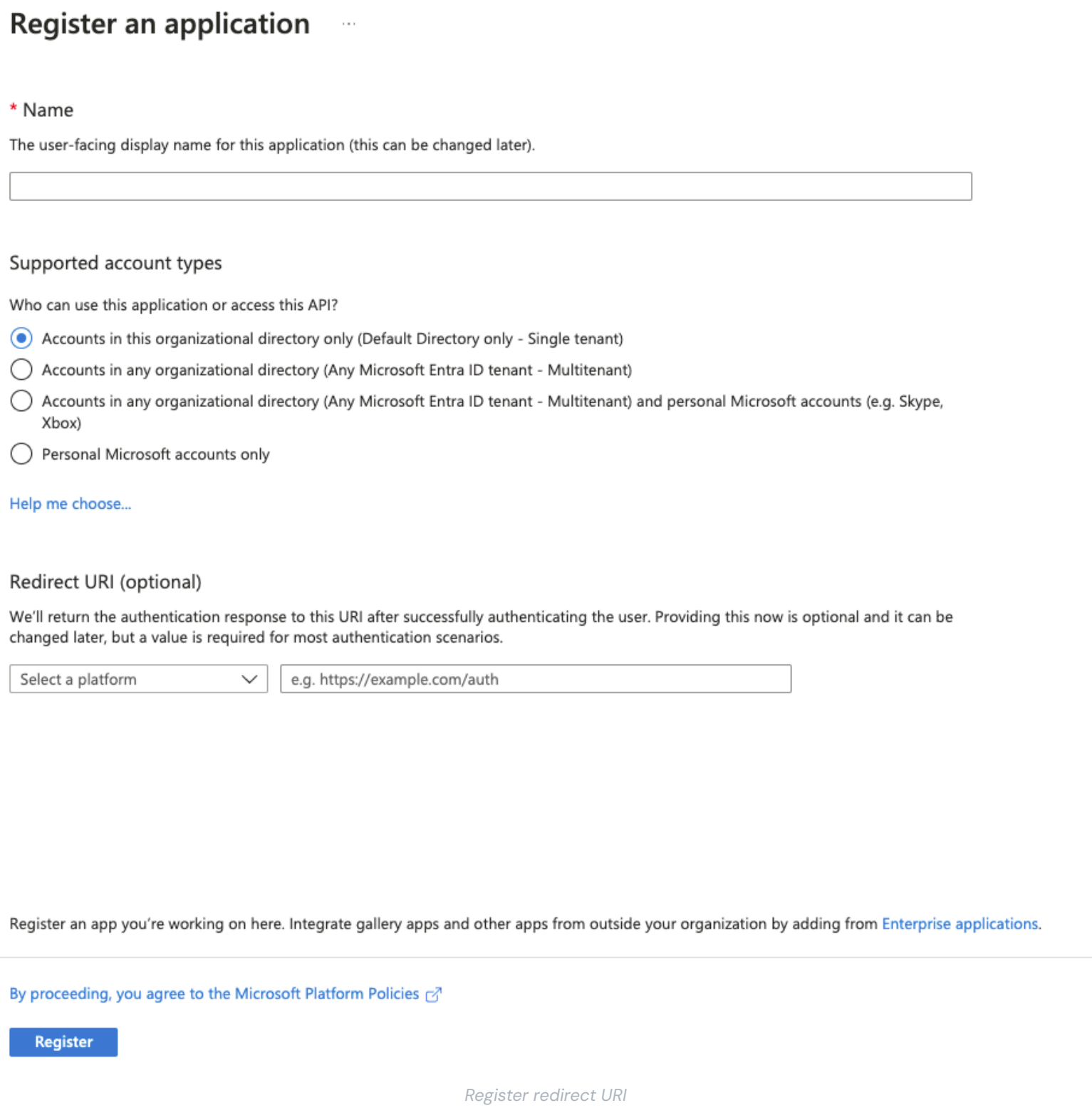
> **Tip**
>
> Hay opciones alternativas de **descifrado de miembro**. Aprenda cómo comenzar a usar SSO con dispositivos de confianza o Conector de clave.

Crea un registro de aplicación

En el Portal de Azure, navega a **Microsoft Entra ID** y selecciona **Registro de aplicaciones.** Para crear un nuevo registro de aplicación, selecciona el botón **Nuevo registro**:



Lo siento, no proporcionaste ningún campo para completar. Por favor, proporciona los campos que necesitas que complete.



Register redirect URI

1. En la pantalla de **Registrar una aplicación**, dale a tu aplicación un nombre específico de Bitwarden y especifica qué cuentas deberían poder usar la aplicación. Esta selección determinará qué usuarios pueden usar el inicio de sesión de Bitwarden con SSO.

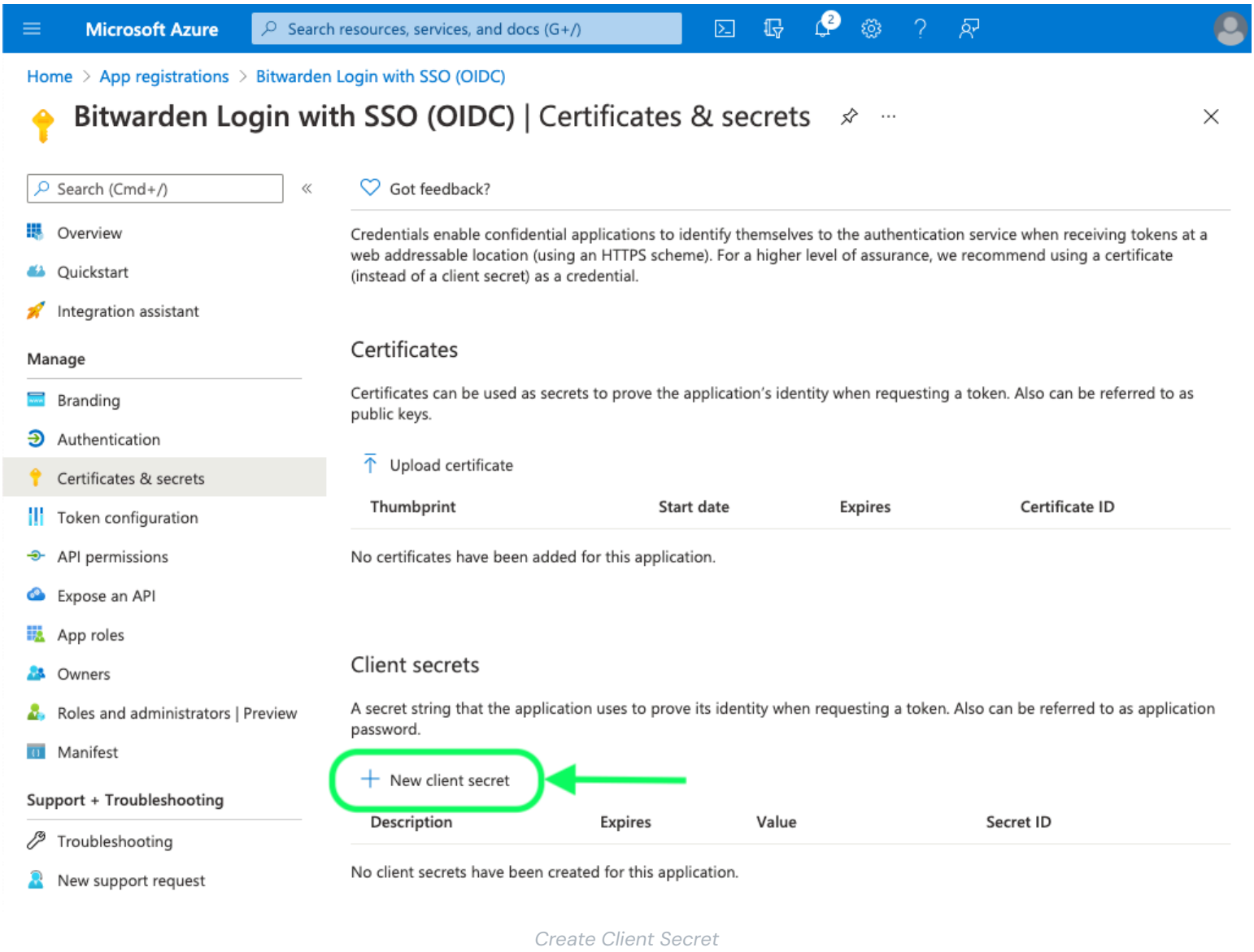
2. Seleccione **Autenticación** de la navegación y seleccione el botón **Agregar una plataforma**.

3. Seleccione la opción **Web** en la pantalla de Configurar plataformas e ingrese su **Ruta de devolución de llamada** en el campo de entrada de URI de redirección.

> **Note**
>
> Callback Path can be retrieved from the Bitwarden SSO Configuration screen. For cloud-hosted customers, this is `https://sso.bitwarden.com/oidc-signin` or `https://sso.bitwarden.eu/oidc-signin`. For self-hosted instances, this is determined by your configured server URL, for example `https://your.domain.com/sso/oidc-signin`.

Crea un secreto de cliente

Seleccione **Certificados y secretos** de la navegación, y seleccione el botón de **Nuevo secreto de cliente**:



Dale al certificado un nombre específico de Bitwarden y elige un marco de tiempo de vencimiento.

Crear consentimiento de administrador

Seleccione **permisos de API** y haga clic en ✓ **Conceder permiso de administrador para el Directorio predeterminado**. El único permiso necesario se agrega por defecto, Microsoft Graph > User.Read.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal de Azure. Regresa a la aplicación web de Bitwarden para configurar los siguientes campos:

Campo	Descripción
Autoridad	Ingrese `https://login.microsoft.com//v2.0`, donde `TENANT_ID` es el valor de **ID de Directorio (inquilino)** recuperado de la pantalla de resumen del registro de la aplicación.
ID de cliente	Ingrese el **ID de la aplicación (cliente)** del registro de la aplicación, que se puede obtener de la pantalla de resumen.
Secreto del Cliente	Ingrese el **Valor Secreto** del secreto de cliente creado.
Dirección de Metadatos	Para las implementaciones de Azure según lo documentado, puedes dejar este campo en blanco.
Comportamiento de Redirección OIDC	Seleccione **Formulario POST** o **Redirección GET**.
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 fallos durante el SSO.
Alcances Adicionales/Personalizados	Define ámbitos 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.

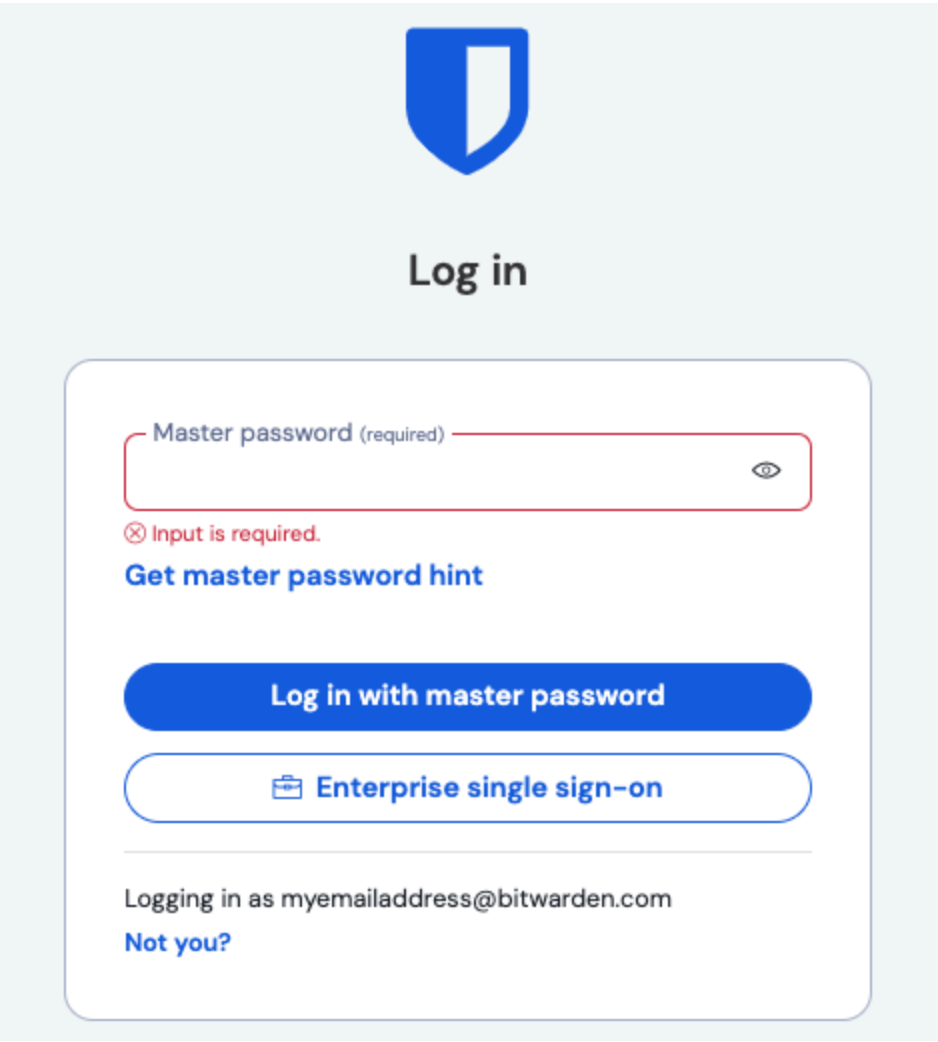
Campo	Descripción
Tipos de Reclamaciones de Correo Electrónico Adicionales/Personalizadas	Defina las claves de tipo de reclamación personalizadas para las direcciones de correo electrónico de los usuarios (delimitadas por comas). Cuando se definen, se busca los tipos de reclamaciones personalizadas antes 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 estándares.
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.
Valor de reclamación "acr" esperado en respuesta	Define el valor de 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.

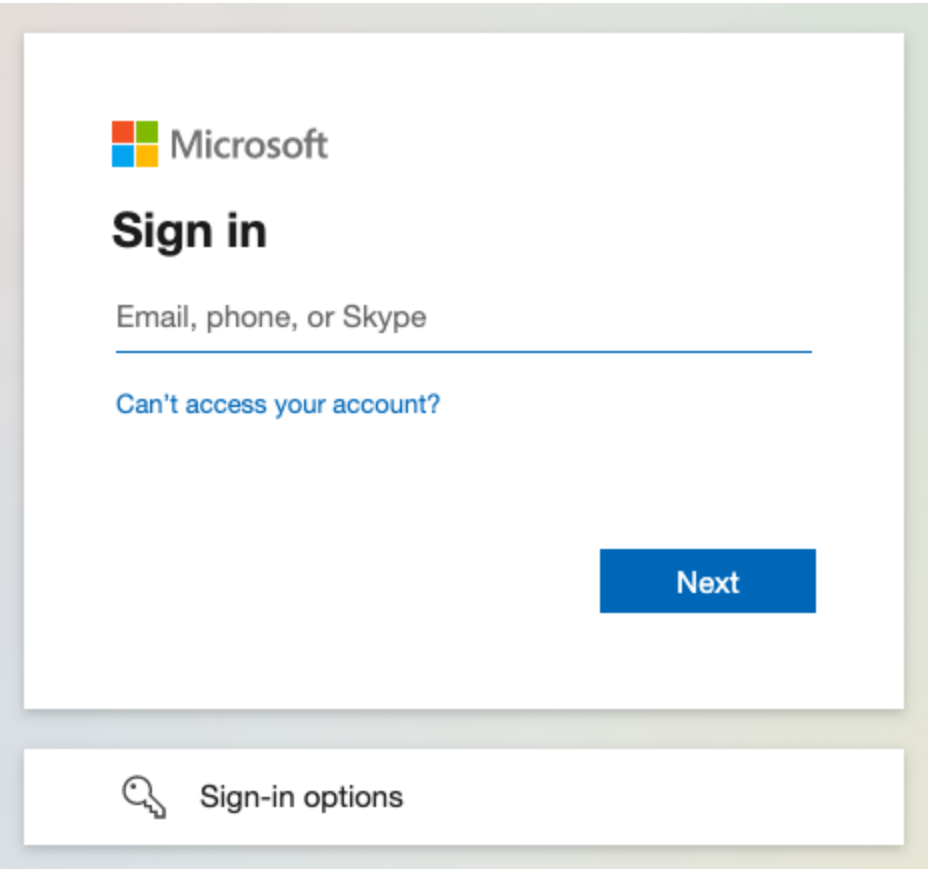
Prueba la configuración

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 con éxito, será redirigido a la pantalla de inicio de sesión de Microsoft:



Azure login screen

¡Después de autenticarte con tus credenciales de Azure, 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.

Próximos pasos

1. Eduque a los miembros de su organización sobre cómo usar el inicio de sesión con SSO.