bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO

Configuración de OIDC

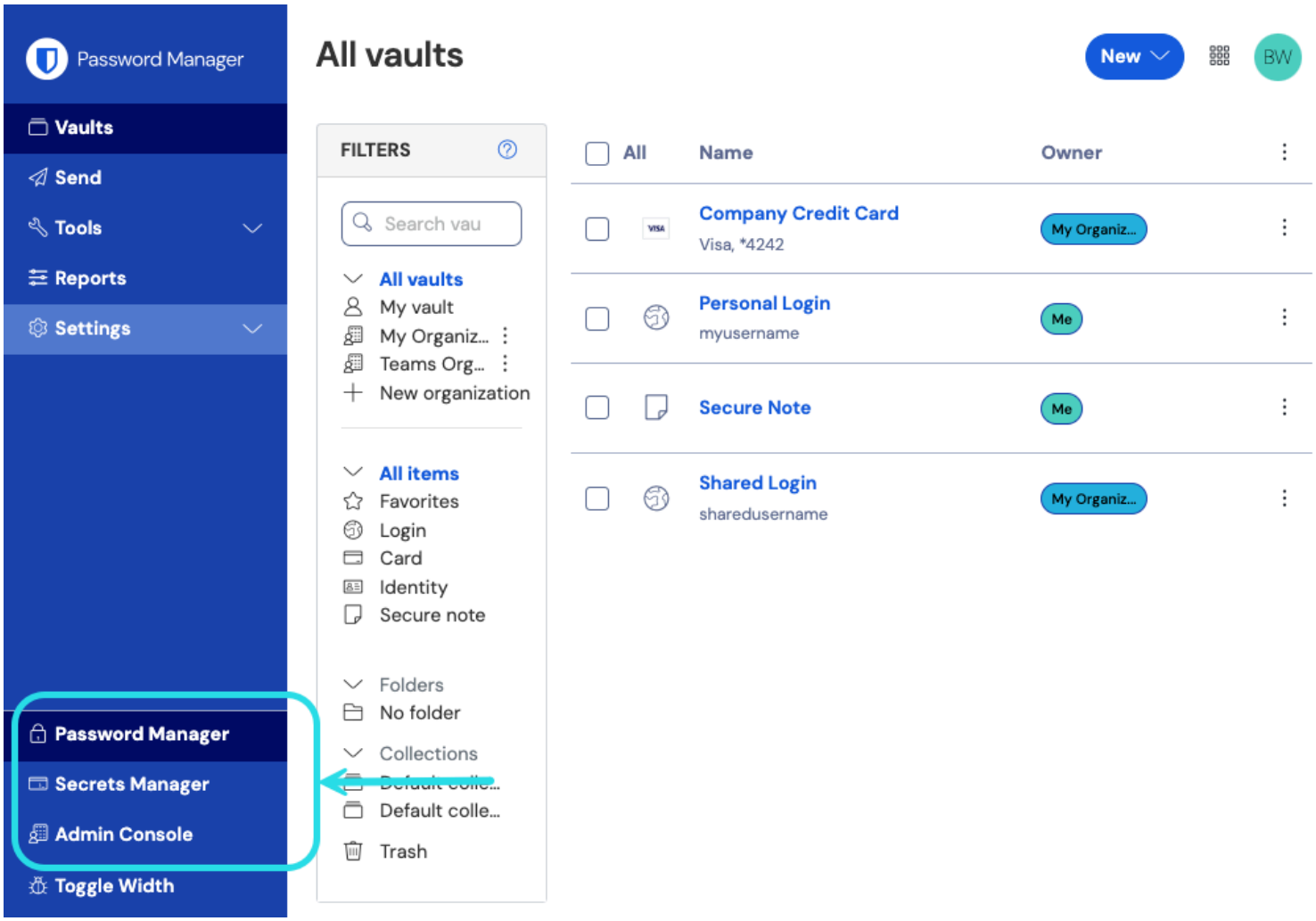
Ver en el centro de ayuda:
https://bitwarden.com/help/configure-sso-oidc/

Configuración de OIDC

Paso 1: Establecer un identificador SSO

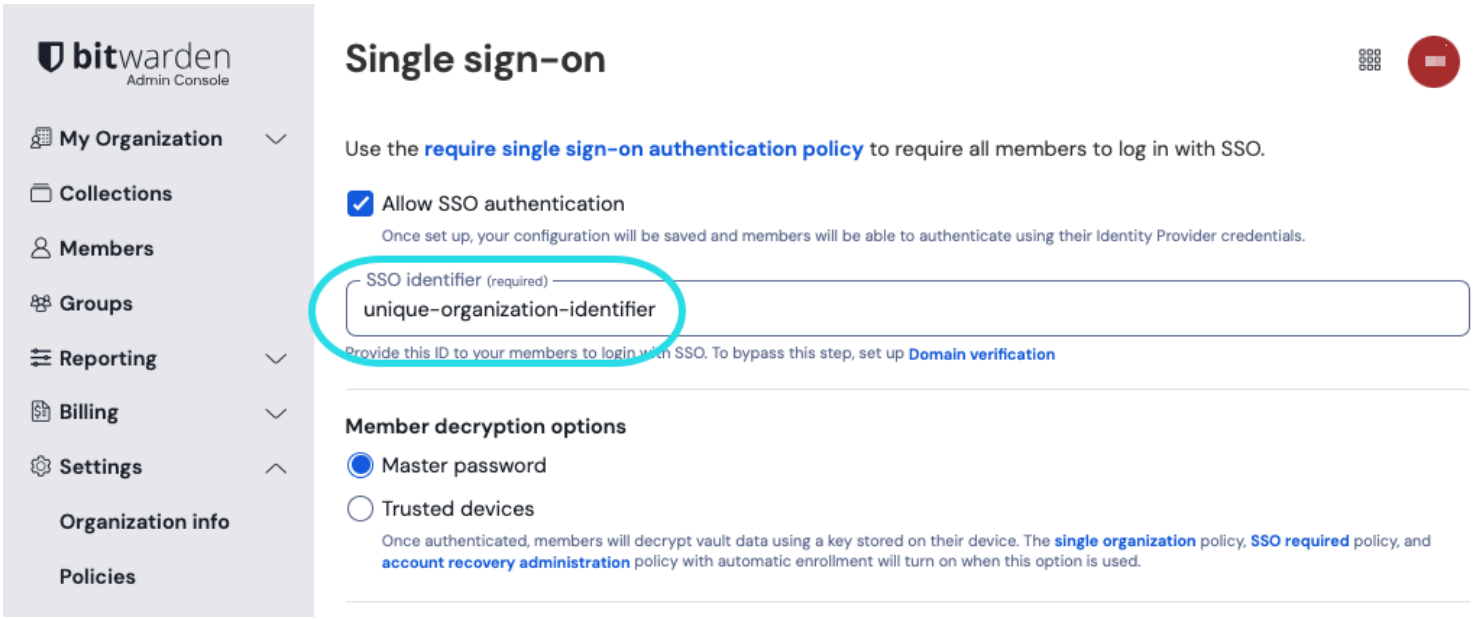
Los usuarios que autentican su identidad usando SSO deberán ingresar un **identificador SSO** que indica la organización (y por lo tanto, la integración SSO) contra la cual autenticarse. Para establecer un identificador SSO único:

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



Selector de producto

2. Navegue a **Ajustes** → **Inicio de sesión único**, e ingrese un **Identificador SSO** único para su organización:



Ingrese un identificador

3. Proceda a **Paso 2: Habilitar inicio de sesión con SSO**.

> **Tip**
> You will need to share this value with users once the configuration is ready to be used.

Paso 2: Habilitar el inicio de sesión con SSO

Una vez que tenga su identificador SSO, puede proceder a habilitar y configurar su integración. Para habilitar el inicio de sesión con SSO:

1. En la vista de **Ajustes** → **Inicio de sesión único**, marque la casilla de **Permitir autenticación SSO**:

Configuración de OIDC

2. Desde el menú desplegable de **Tipo**, selecciona la opción **OpenID Connect**. Si tienes la intención de usar SAML en su lugar, cambia a la guía de configuración de SAML.

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

Paso 3: Configuración

A partir de este punto, la implementación variará de proveedor a proveedor. Salta a una de nuestras **guías de implementación** específicas para obtener ayuda para completar el proceso de configuración:

Proveedor	Guía
Azul	Guía de Implementación de Azure

Proveedor	Guía
Okta	Guía de Implementación de Okta

Materiales de referencia de configuración

Las siguientes secciones definirán los campos disponibles durante la configuración del inicio de sesión único, independientemente del IdP con el que esté integrando. Los campos que deben configurarse estarán marcados (**requerido**).

> **Tip**
>
> **Unless you are comfortable with OpenID Connect**, we recommend using one of the above implementation guides instead of the following generic material.

Campo	Descripción
Ruta de devolución de llamada	(**Generado automáticamente**) La URL para la redirección automática de autenticación. 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 configurada, por ejemplo `https://your.domain.com/sso/oidc-signin`.
Ruta de devolución de llamada después de cerrar sesión	(**Generado automáticamente**) La URL para la redirección automática de cierre de sesión. Para los clientes alojados en la nube, esto es `https://sso.bitwarden.com/oidc-signedout` o `https://sso.bitwarden.eu/oidc-signedout`. Para instancias autoalojadas, esto está determinado por su URL de servidor configurada, por ejemplo `https://your.domain.com/sso/oidc-signedout`.
Autoridad	(**Requerido**) La URL de su servidor de autorización ("Autoridad"), contra el cual Bitwarden realizará la autenticación. Por ejemplo, `https://your.domain.okta.com/oauth2/default` o `https://login.microsoft.com//v2.0`.
ID de cliente	(**Obligatorio**) Un identificador para el cliente OIDC. Este valor es típicamente específico para una integración de aplicación IdP construida, por ejemplo, una registro de aplicación Azure o una aplicación web Okta.
Secreto del Cliente	(**Obligatorio**) El secreto del cliente utilizado junto con el ID del cliente para intercambiar por un token de acceso. Este valor es típicamente específico para una integración de aplicación IdP construida, por ejemplo, una registro de aplicación Azure o una Aplicación Web Okta.

Campo	Descripción
Dirección de Metadatos	(**Requerido si la Autoridad no es válida**) Una URL de metadatos donde Bitwarden puede acceder a los metadatos del servidor de autorización como un objeto JSON. Por ejemplo, `https://your.domain.okta.com/oauth2/default/.well-known/oauth-authorization-server`
Comportamiento de Redirección OIDC	(**Requerido**) Método utilizado por el IdP para responder a las solicitudes de autenticación de Bitwarden. Las opciones incluyen **Formulario POST** y **Redirección GET**.
Obtener reclamos del endpoint 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 los alcances personalizados para agregar a la solicitud (delimitados por comas).
Tipos de reclamaciones de identificación 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 clase Context 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	Defina el valor de la reclamación `acr` que Bitwarden espera y valida en la respuesta.

Atributos y reclamaciones de OIDC

Se requiere una **dirección de correo electrónico para la provisión de la cuenta**, que se puede pasar como cualquiera de los atributos o reclamaciones en la tabla a continuación.

También se recomienda encarecidamente un identificador de usuario único. Si está ausente, se utilizará el correo electrónico en su lugar para vincular al usuario.

Los atributos/reclamaciones se enumeran en orden de preferencia para la coincidencia, incluyendo alternativas donde sea aplicable:

Valor	Reclamación/Atributo	Reclamación/atributo de respaldo
ID Único	Configurado Reclamaciones de ID de Usuario Personalizado NameID (cuando no es transitorio) urn:oid:0.9.2342.19200300.100.1.1 Submarino IDU UPN EPPN	
Correo electrónico	Reclamaciones personalizadas de correo electrónico configurado Correo electrónico http://schemas.xmlsoap.org/ws/2005/05/identidad/claims/direcciondecorreo urn:oid:0.9.2342.19200300.100.1.3 Correo CorreoElectrónico	Nombre_de_usuario_preferido Urn:oid:0.9.2342.19200300.100.1.1 IDU
Nombre	Reclamaciones de Nombre Personalizado Configuradas Nombre http://schemas.xmlsoap.org/ws/2005/05/identidad/claims/nombre urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3 Nombre para Mostrar CN	Nombre + " " + Apellido (ver abajo)
Nombre	urn:oid:2.5.4.42 Nombre de pila Nombre de pila FN Nombre de pila Apodo	

Valor	Reclamación/Atributo	Reclamación/atributo de respaldo
Apellido	urn:oid:2.5.4.4 SN Apellido Apellido	