bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML de Google

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

Implementación de SAML de Google

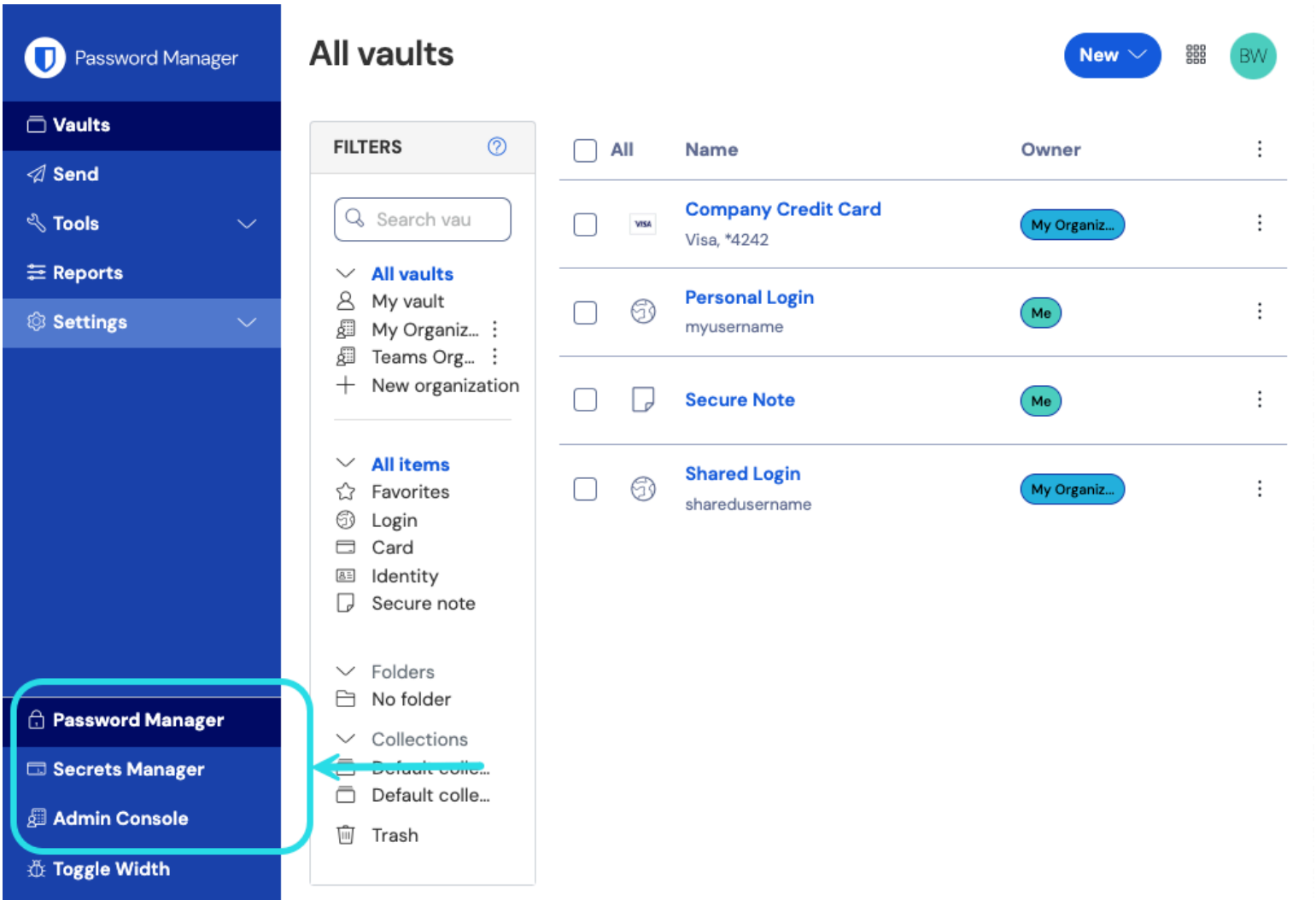
Este artículo contiene ayuda específica de **Google Workspace** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte Configuración de SAML 2.0.

La configuración implica trabajar simultáneamente con la aplicación web de Bitwarden y la consola de administrador de Google Workspace. 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

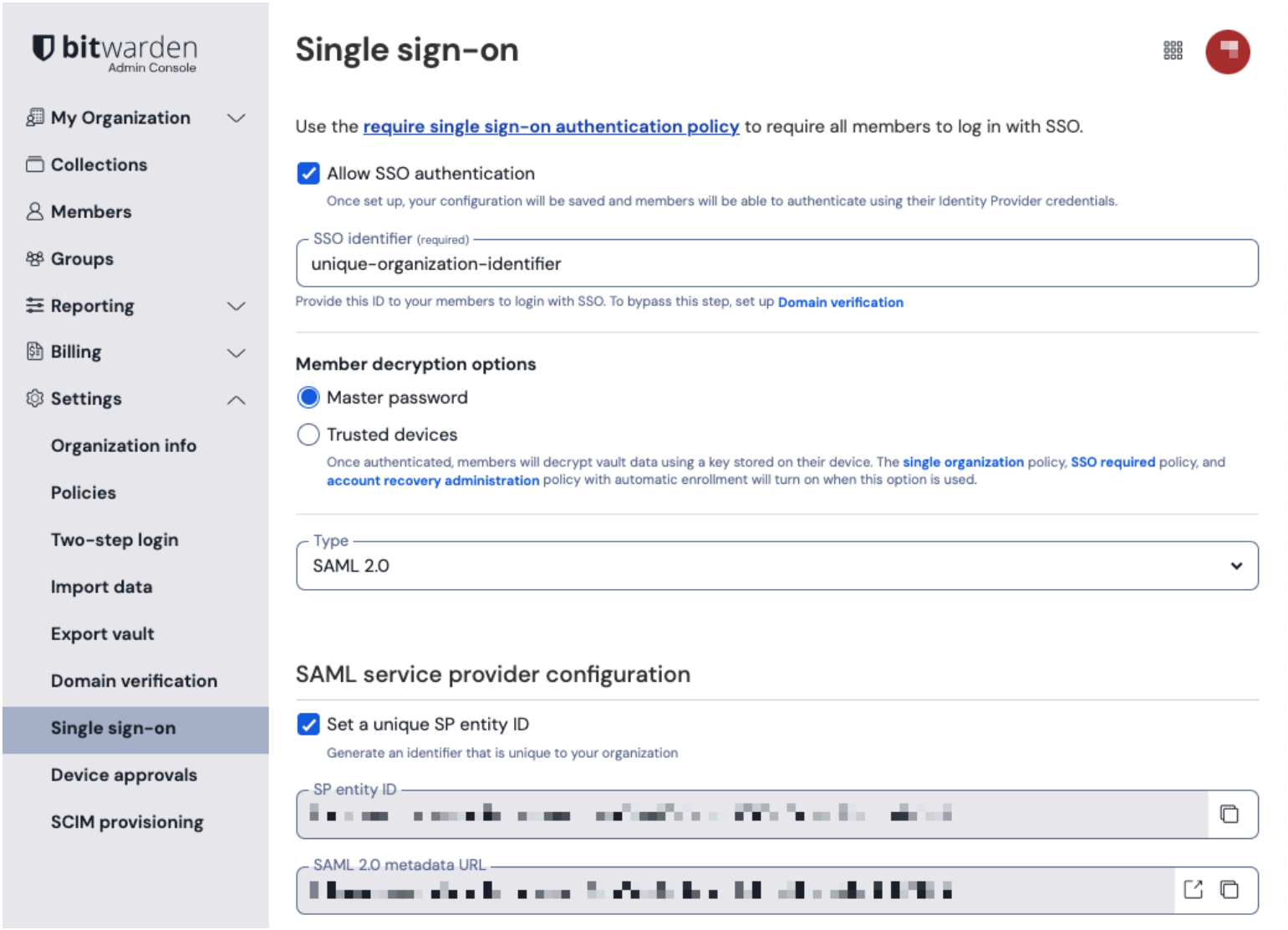
Abre SSO en la aplicación web

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



Selector de producto

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



Configuración de SAML 2.0

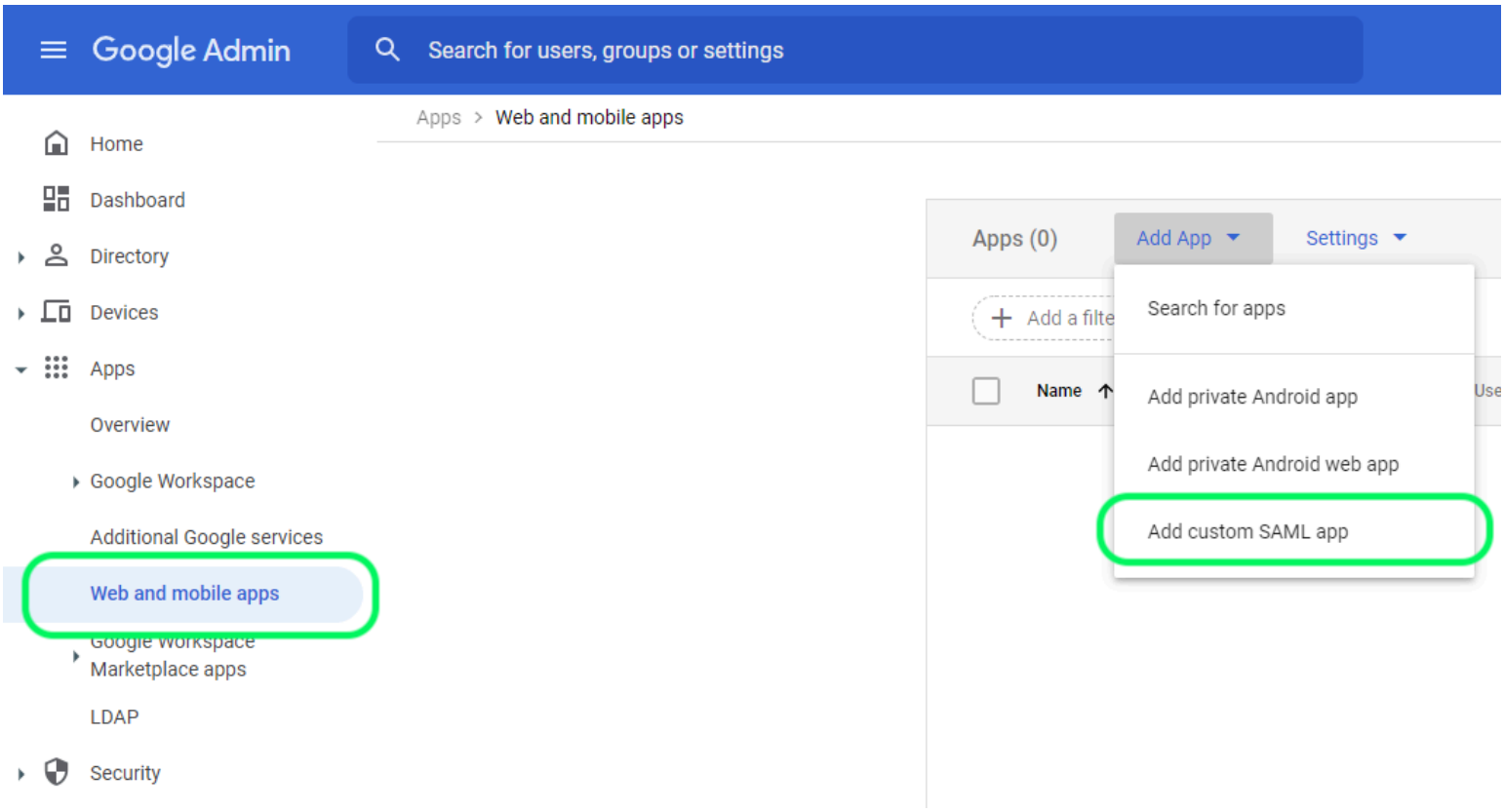
Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de **Tipo**. Mantén esta pantalla abierta para fácil referencia.

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 activa.

> **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 SAML

En la consola de administrador de Google Workspace, selecciona **Aplicaciones → Aplicaciones web y móviles** desde la navegación. En la pantalla de Web y aplicaciones móviles, selecciona **Agregar Aplicación → Agregar aplicación SAML personalizada**:



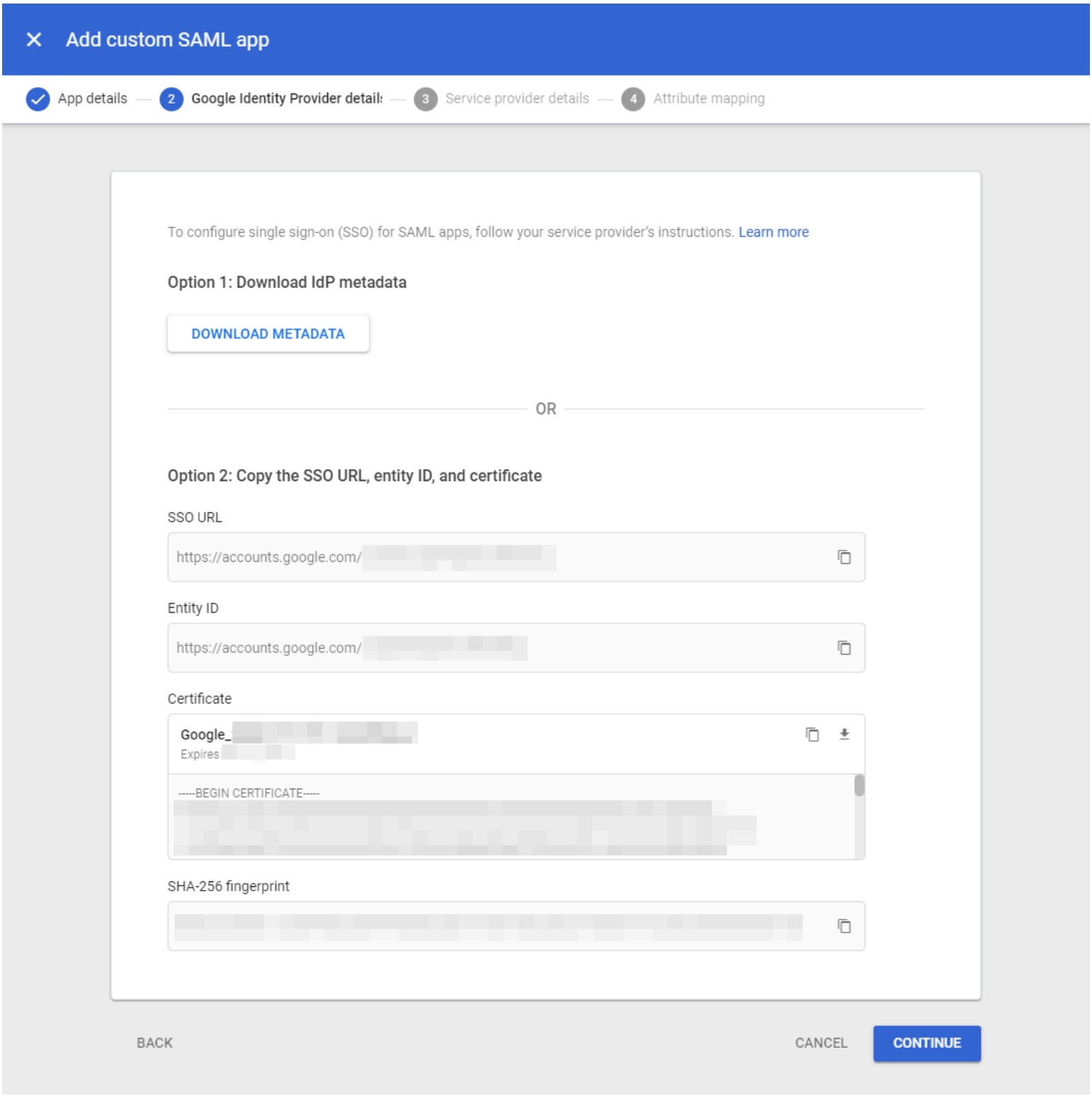
Create a SAML App

Detalles de la aplicación

En la pantalla de detalles de la aplicación, dale a la aplicación un nombre único específico de Bitwarden y selecciona el botón **Continuar**.

Detalles del proveedor de identidad de Google

En la pantalla de detalles del proveedor de identidad de Google, copia tu **URL de SSO**, **ID de entidad** y **Certificado** para usar en un paso posterior:



IdP Details

Seleccione **Continuar** cuando haya terminado.

Detalles del proveedor de servicios

En la pantalla de detalles del proveedor de servicios, configure los siguientes campos:

Campo	Descripción
URL de ACS	Establezca este campo en la **URL del Servicio de Consumo de Afirmaciones (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.
ID de la entidad	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.
Iniciar URL	Opcionalmente, establezca este campo con la URL de inicio de sesión desde la cual los usuarios accederán a Bitwarden. Para los clientes alojados en la nube, esto es `https://vault.bitwarden.com/#/sso` o `https://vault.bitwarden.eu/#/sso`. Para instancias autoalojadas, esto está determinado por su URL de servidor configurado, por ejemplo `https://your.domain.com/#/sso`.
Respuesta firmada	Marque esta casilla si desea que Workspace firme las respuestas SAML. Si no se verifica, Workspace solo firmará la afirmación SAML.
Formato de ID de nombre	Establece este campo a **Persistente**.
Identificación de nombre	Seleccione el atributo de usuario del Espacio de trabajo para llenar NameID.

Seleccione **Continuar** cuando haya terminado.

Mapeo de atributos

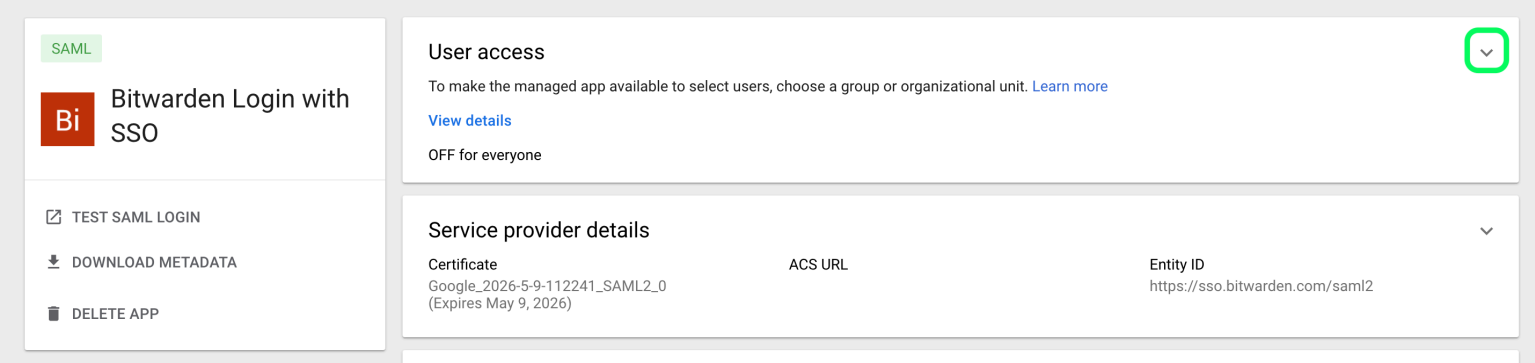
En la pantalla de mapeo de atributos, seleccione el botón **Agregar Mapeo** y construya el siguiente mapeo:

Atributos del Directorio de Google	Atributos de la aplicación
Correo electrónico principal	correo electrónico

Seleccione **Finalizar**.

Enciende la aplicación

Por defecto, las aplicaciones SAML de Workspace estarán **DESACTIVADAS para todos**. Abra la sección de acceso de usuario para la aplicación SAML y configure a **ON para todos** o para grupos específicos, dependiendo de sus necesidades:



User Access

Guarde sus cambios. Por favor, tome nota de que puede tardar hasta 24 horas para que una nueva aplicación de Workspace se propague a las sesiones existentes de los usuarios.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto de la consola de administrador de Google Workspace. 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 la consola del Administrador del Espacio de Trabajo durante la configuración:

Campo	Descripción
Formato de Identificación de Nombre	Establezca este campo en el formato de ID de nombre seleccionado en Workspace.
Algoritmo de Firma de Salida	El algoritmo que Bitwarden utilizará para firmar solicitudes SAML.

Campo	Descripción
Comportamiento de Firma	Si/cuando las solicitudes de SAML serán firmadas.
Algoritmo Mínimo de Firma Entrante	De forma predeterminada, Google Workspace firmará con RSA SHA-256. Selecciona `sha-256` del menú desplegable.
Esperar afirmaciones firmadas	Si Bitwarden espera que las afirmaciones SAML estén firmadas. Este ajuste debe estar **desmarcado**.
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 Bitwarden Inicio de sesión con SSO.

Cuando termines 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 vuelva a la consola del administrador de Workspace para recuperar los valores de la aplicación:

Campo	Descripción
ID de la entidad	Establezca este campo en el **ID de Entidad** del Espacio de trabajo, recuperado de la sección de detalles del Proveedor de Identidad de Google o utilizando el botón de **Descargar Metadatos**. Este campo distingue entre mayúsculas y minúsculas.
Tipo de Encuadernación	Establecer a **HTTP POST** o **Redireccionar**.
URL del Servicio de Inicio de Sesión Único	Establezca este campo en la **URL de SSO** del Espacio de trabajo, obtenida de la sección de detalles del Proveedor de Identidad de Google o utilizando el botón de **Descargar Metadatos**.
URL 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.

Campo	Descripción

Certificado Público X509	Pega el certificado recuperado, 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	Por defecto, Google Workspace firmará con RSA SHA-256. Selecciona `sha-256` del menú desplegable.
Deshabilitar Solicitudes de Cierre de Sesión Saliente	El inicio de sesión con SSO actualmente **no** admite SLO. Esta opción está planeada para un desarrollo futuro.
Quiere Solicitudes de Autenticación Firmadas	Si Google Workspace 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.

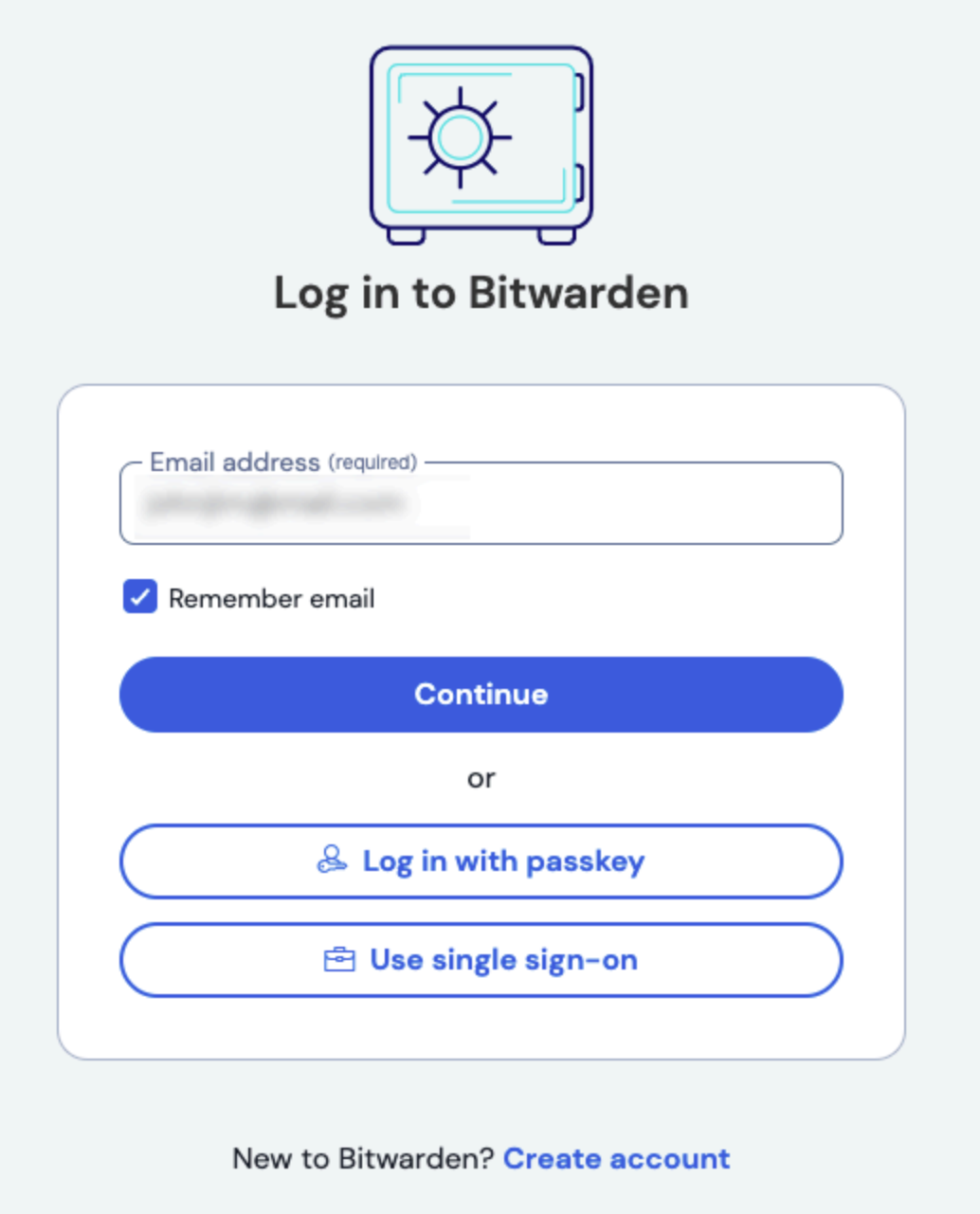
Cuando termines con la configuración del proveedor de identidad, **Guarda** tu trabajo.

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.

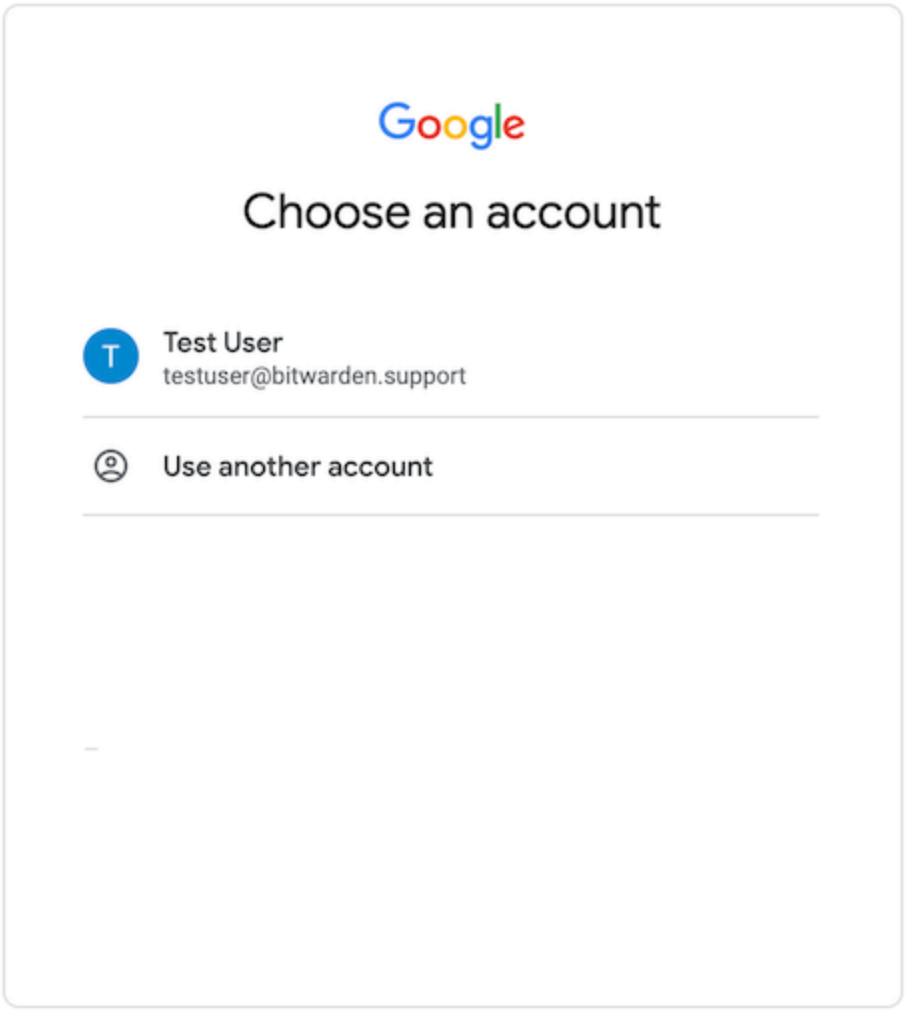
Prueba la configuración

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 **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 Google Workspace:



Login

¡Después de autenticarte con tus credenciales de Workspace, 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.