bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML ID de Microsoft Entra

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

Implementación de SAML ID de Microsoft Entra

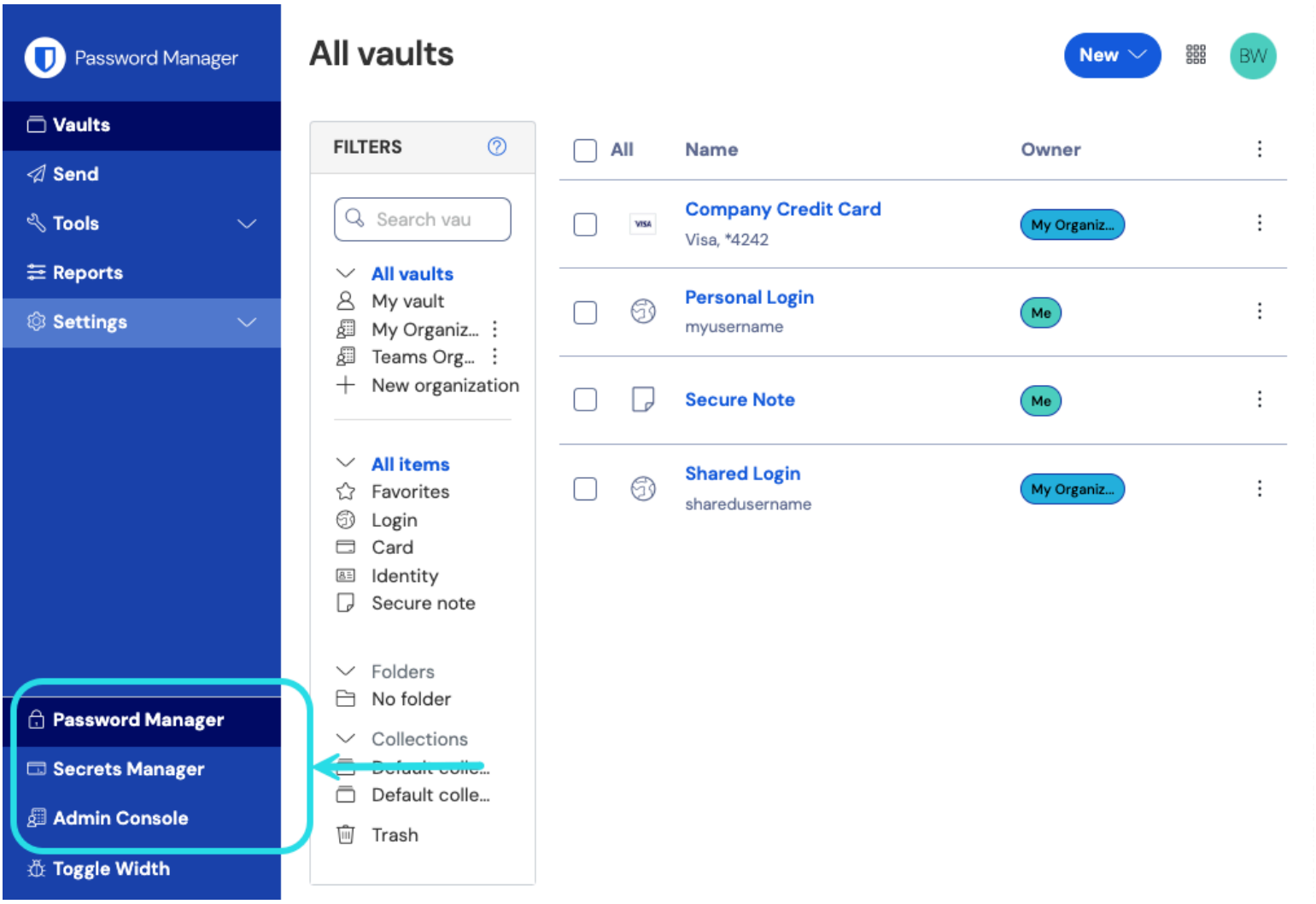
Este artículo contiene ayuda **específica de Azure** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte Configuración de SAML 2.0.

La configuración implica trabajar simultáneamente con la aplicación web de Bitwarden y el Portal de Azure. A medida que avanza, recomendamos tener ambos fácilmente disponibles y completar los pasos en el orden en que están documentados.

> **Tip**
>
> **¿Ya eres un experto en SSO?** Omite las instrucciones en este artículo y descarga capturas de pantalla de configuraciones de muestra para comparar con las tuyas.
>
> tipo: enlace de activo id: 7CKe4TX98FPF86eAimKgak

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

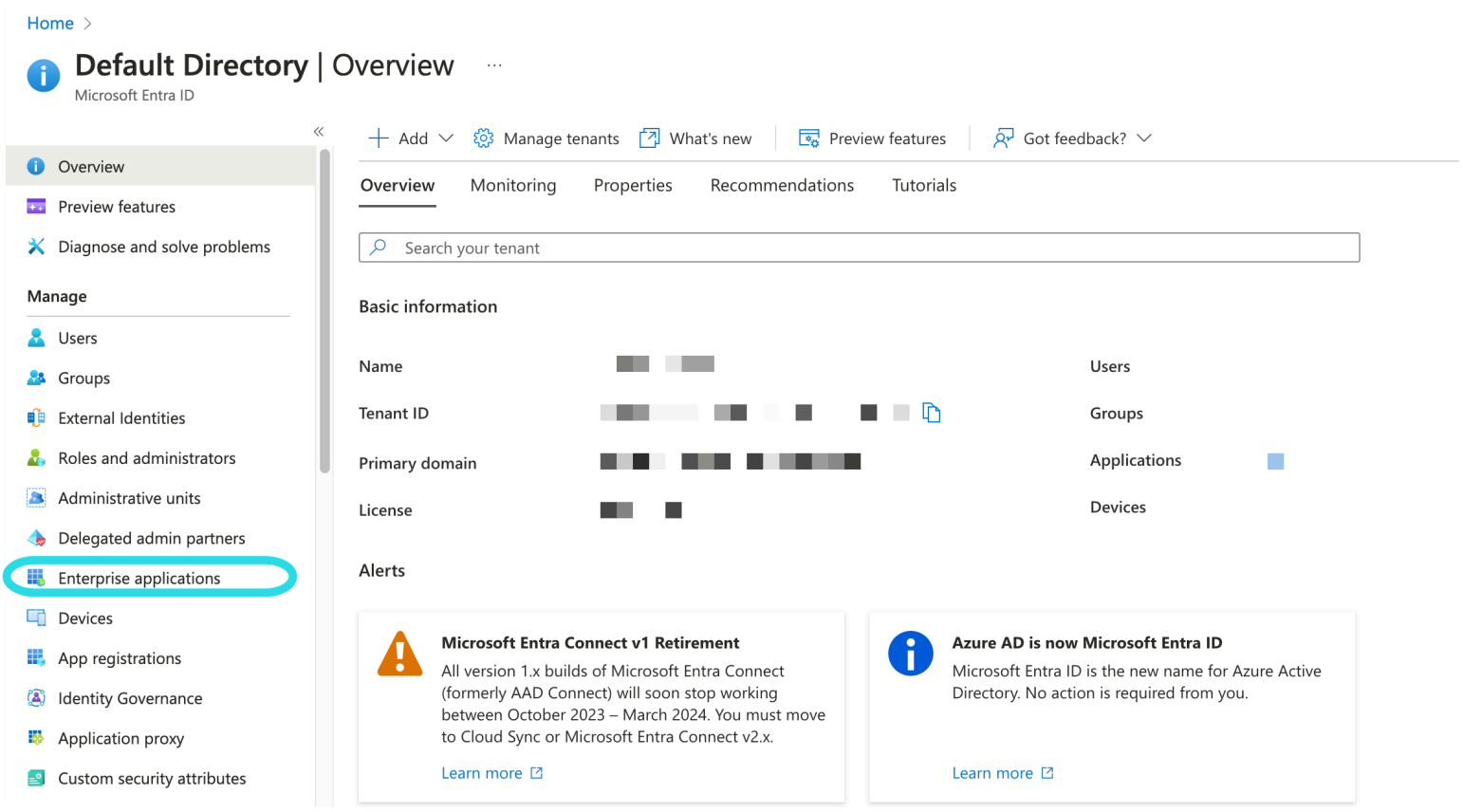
Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de **Tipo**. Mantén esta pantalla abierta para fácil referencia.

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.

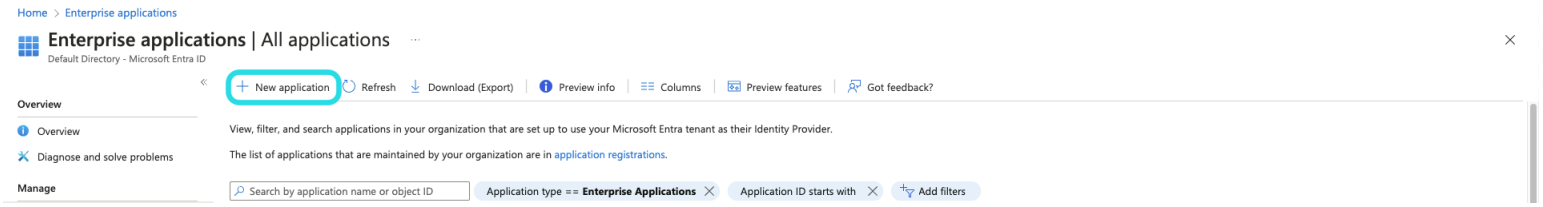
Crea una aplicación de empresa

En el Portal de Azure, navegue a **Microsoft Entra ID** y seleccione **Aplicaciones de Empresa** desde el menú de navegación:



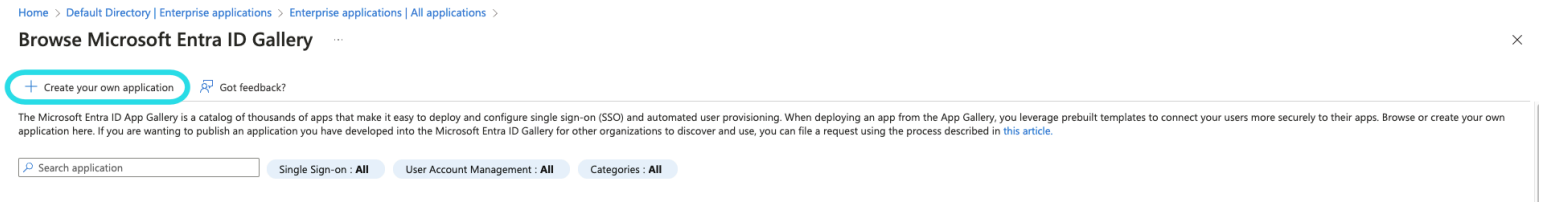
Enterprise applications

Seleccione el botón ＋ **Nueva aplicación**:



Create new application

En la pantalla de Galería de ID de Entra de Microsoft, selecciona el botón ＋ **Crea tu propia aplicación**:

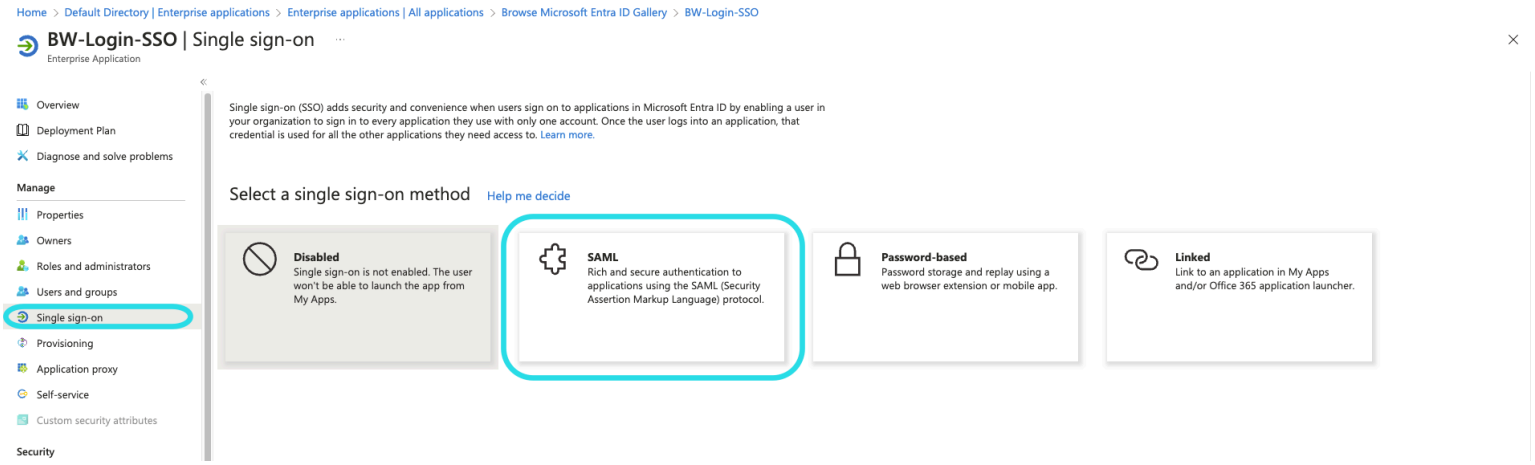


Create your own application

En la pantalla de Crear tu propia aplicación, dale a la aplicación un nombre único y específico de Bitwarden y selecciona la opción (No de galería). Una vez que hayas terminado, haz clic en el botón **Crear**.

Habilitar inicio de sesión único

Desde la pantalla de Resumen de la Aplicación, seleccione **Inicio de sesión único** desde la navegación:



Configure Single sign-on

En la pantalla de inicio de sesión único, seleccione **SAML**.

Configuración de SAML

Configuración básica de SAML

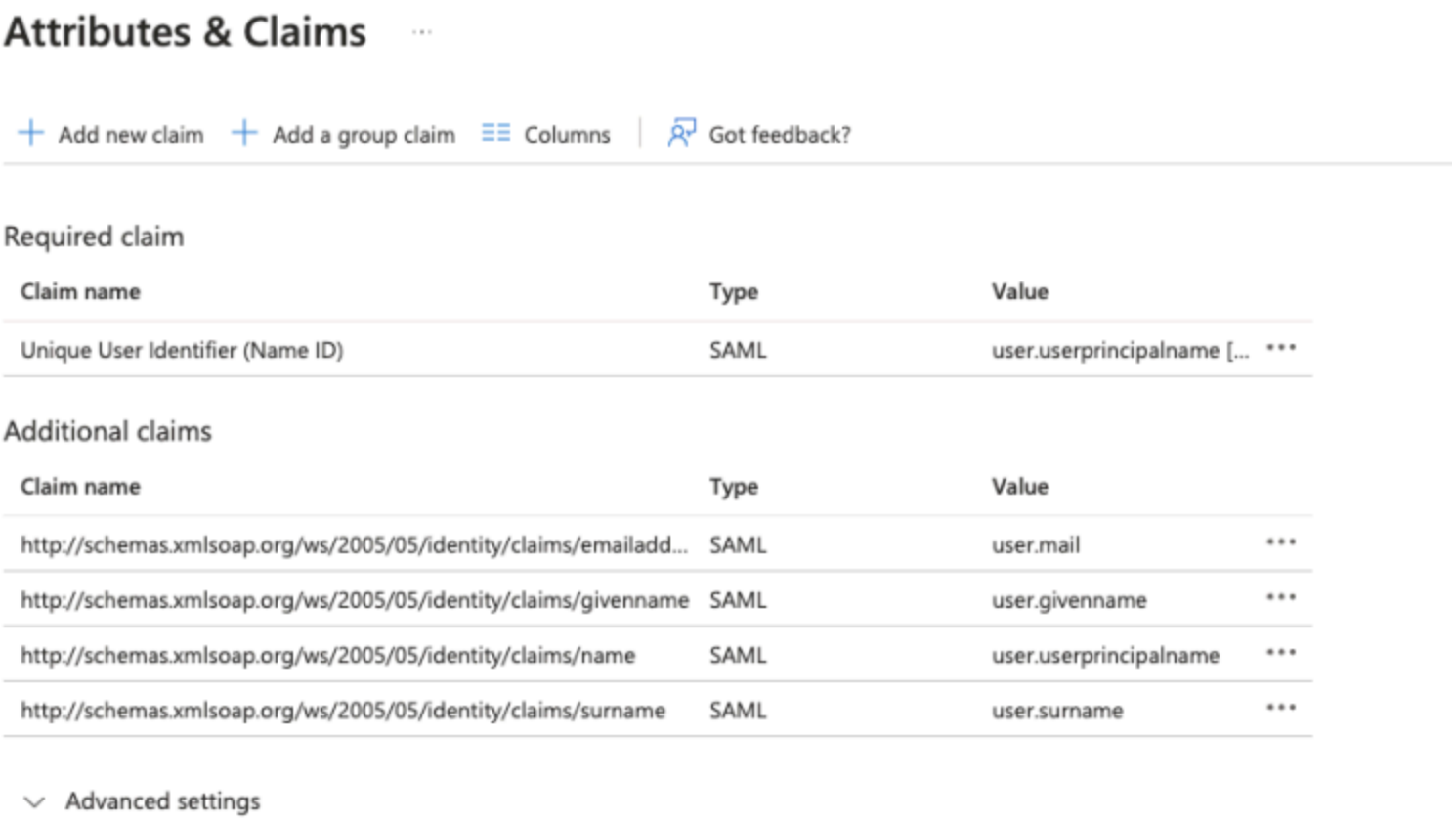
Seleccione el botón **Editar** y configure los siguientes campos:

Campo	Descripción
Identificador (ID de 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.
URL de respuesta (URL del Servicio de Consumo de Afirmaciones)	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.
Iniciar sesión en URL	Establezca este campo en 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 es determinado por usted URL del servidor configurado, por ejemplo `https://su-dominio.com/#/sso`.

Atributos y reclamaciones del usuario

Las reclamaciones predeterminadas construidas por Azure funcionarán con el inicio de sesión con SSO, sin embargo, opcionalmente puedes usar esta sección para configurar el formato NameID utilizado por Azure en las respuestas SAML.

Seleccione el botón **Editar** y seleccione la entrada **Identificador Único de Usuario (Nombre ID)** para editar la reclamación de NombreID:



Editar Reclamo de NombreID

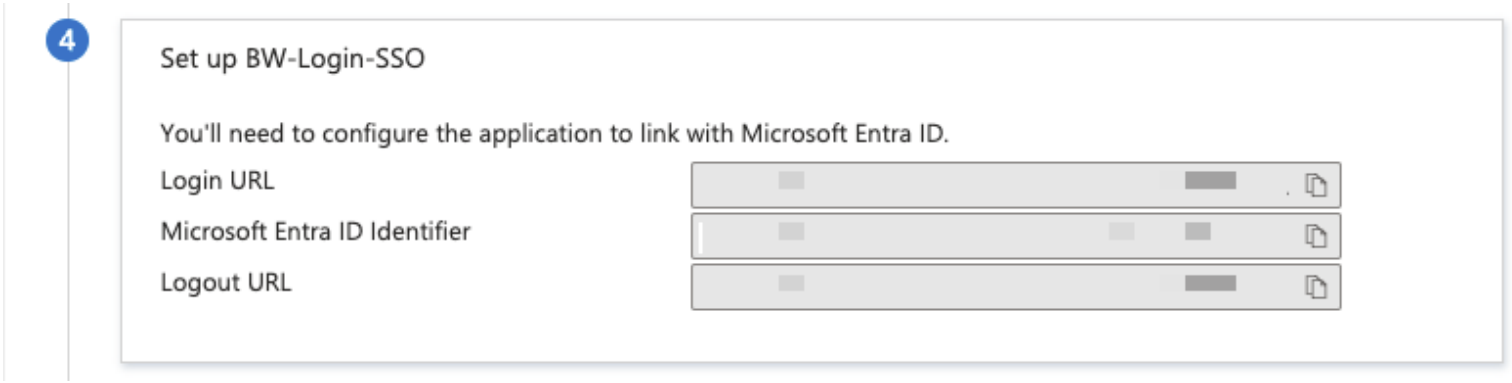
Las opciones incluyen Predeterminado, Dirección de correo electrónico, Persistente, No especificado y Nombre de dominio calificado de Windows. Para obtener más información, consulte la documentación de Microsoft Azure.

Certificado de firma SAML

Descarga el Certificado Base64 para usarlo durante un paso posterior.

Configura tu aplicación

Copia o toma nota de la **URL de inicio de sesión** y el **Identificador de Microsoft Entra ID** en esta sección para usar durante un paso posterior:

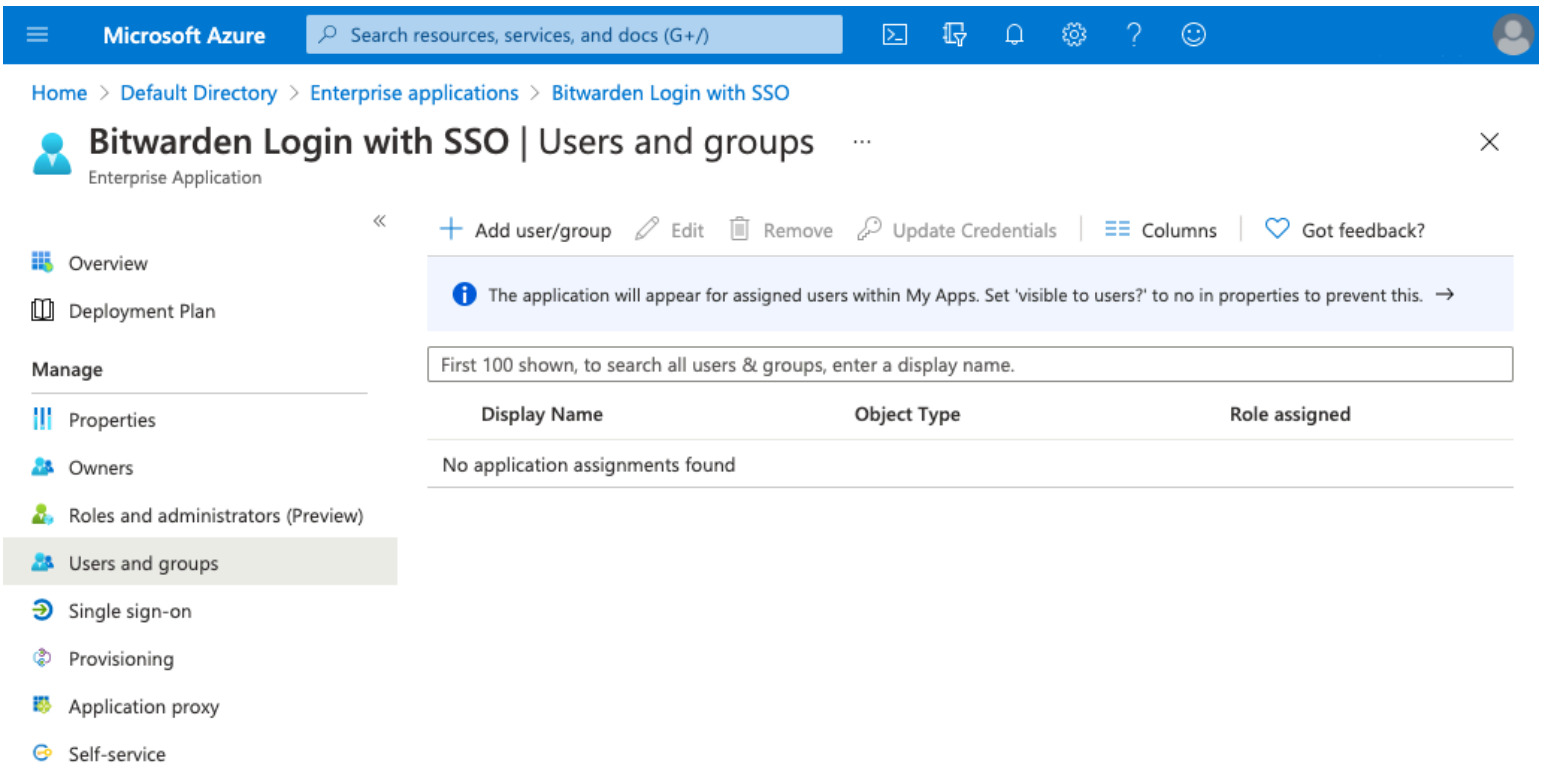


Azure URLs

> **Note**
> If you receive any key errors when logging in via SSO, try copying the X509 certificate information from the Federation Metadata XML file instead.

Usuarios y grupos

Seleccione **Usuarios y grupos** de la navegación:



Assign users or groups

Seleccione el botón **Agregar usuario/grupo** para asignar acceso al inicio de sesión con la aplicación SSO a nivel de usuario o grupo.

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 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:

Campo	Descripción
Formato de Identificación de Nombre	Por defecto, Azure utilizará la dirección de correo electrónico. Si cambió este ajuste, seleccione el valor correspondiente. De lo contrario, establezca este campo en **No especificado** o **Dirección de correo electrónico**.
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	Por defecto, Azure firmará con RSA SHA-256. Seleccione `rsa-sha256` del menú desplegable.
Quiero Afirmaciones Firmadas	Si Bitwarden espera que las afirmaciones SAML estén firmadas.
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 inicio de sesión de Bitwarden 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 vuelvas al Portal de Azure para recuperar los valores de la aplicación:

Campo	Descripción
ID de la entidad	Ingrese su **Identificador de Entra ID de Microsoft**, obtenido de la sección Configure su aplicación del Portal de Azure. Este campo distingue entre mayúsculas y minúsculas.
Tipo de Encuadernación	Establecer en **HTTP POST** o **Redirigir**.
URL del Servicio de Inicio de Sesión Único	Ingrese su **URL de inicio de sesión**, obtenida de la sección Configure su aplicación del Portal de Azure.
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 con tu **URL de cierre de sesión** si lo deseas.

Certificado Público X509	Pega el certificado descargado, eliminando
	`-----INICIO CERTIFICADO-----`
	y
	`-----FIN DEL CERTIFICADO-----`
	El valor del certificado distingue entre 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, Azure firmará con RSA SHA-256. Seleccione `rsa-sha256` del menú desplegable.
Deshabilitar Solicitudes de Cierre de Sesión Salientes	El inicio de sesión con SSO actualmente **no** admite SLO. Esta opción está planeada para un desarrollo futuro.
Quiere Solicitudes de Autenticación Firmadas	Si Azure espera que las solicitudes SAML estén firmadas.

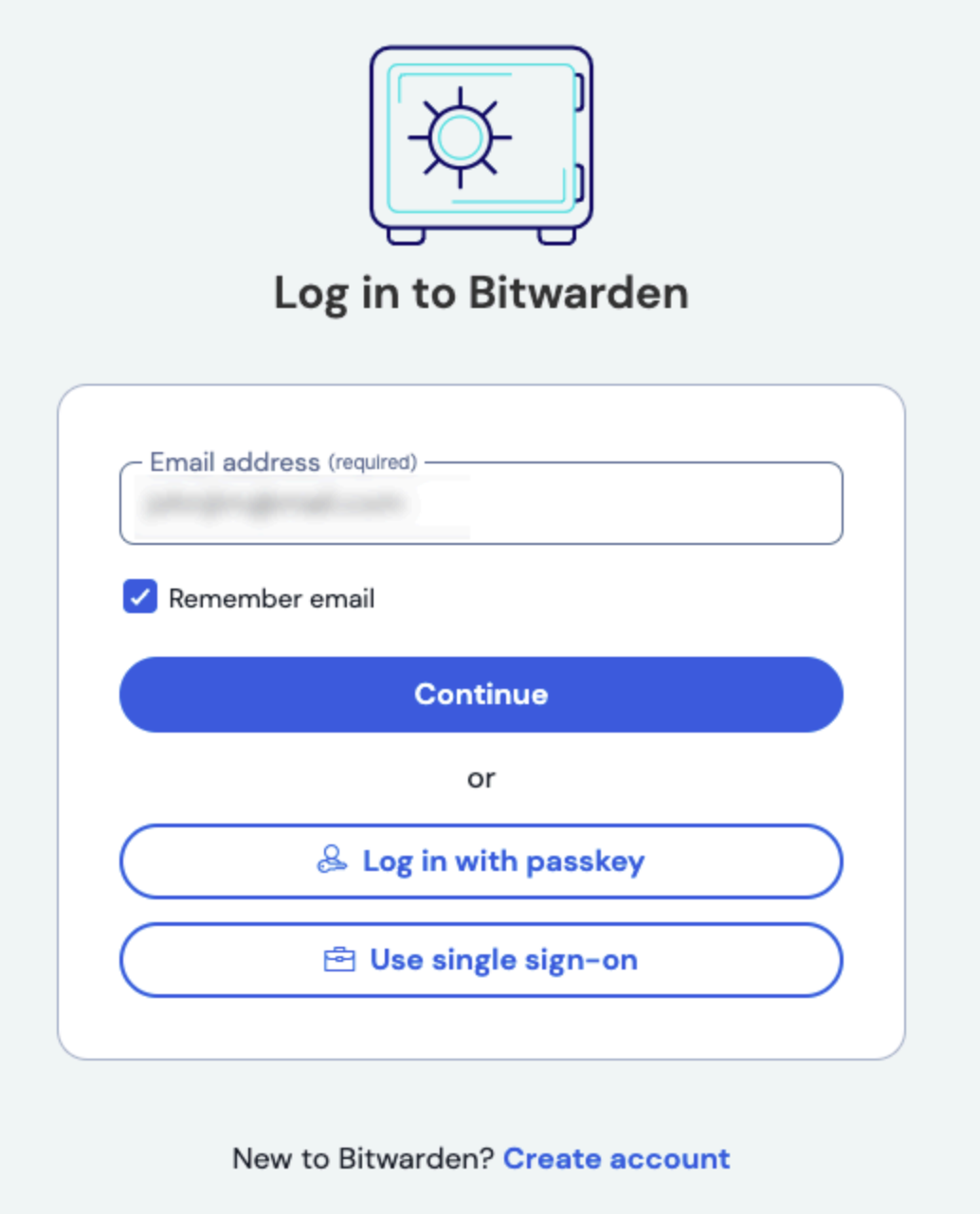
> **Note**
>
> Al completar el certificado X509, toma nota de la fecha de vencimiento. Los certificados tendrán que ser renovados para prevenir cualquier interrupción en el servicio a los usuarios finales de SSO. Si un certificado ha caducado, las cuentas de Administrador y Propietario siempre podrán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

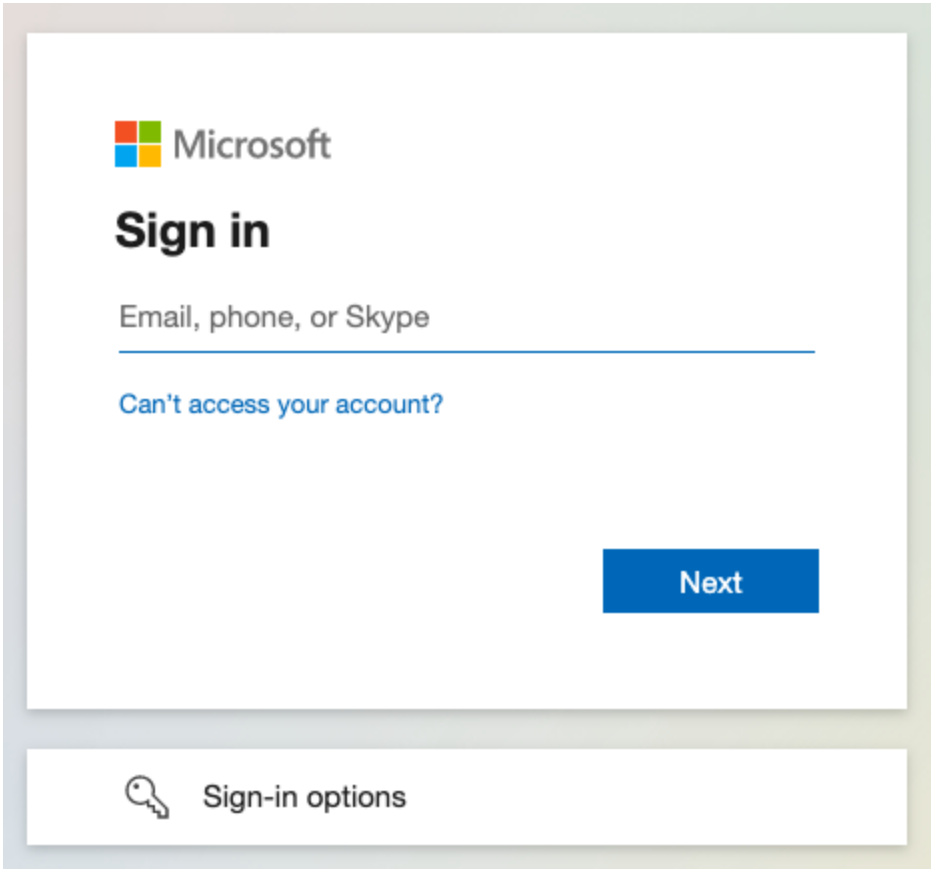
Prueba la configuración

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 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 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 SSO debe iniciarse desde Bitwarden. Los administradores de Azure SAML pueden configurar un Registro de Aplicación para que los usuarios sean dirigidos a la página de inicio de sesión de la caja fuerte web de Bitwarden.

1. Desactive el botón de Bitwarden existente en la página de **Todas las Aplicaciones** navegando a la aplicación actual de Bitwarden Empresa y seleccionando propiedades y establezca la opción **Visible para los usuarios** a **No**.

2. Crea el registro de la aplicación navegando a **Registros de Aplicaciones** y seleccionando **Nuevo Registro**.

3. Proporcione un nombre para la aplicación como **Bitwarden SSO**. No especifique una URL de redirección. Seleccione **Registrarse** para completar el foro.

4. Una vez que se ha creado la aplicación, navegue a **Marca & Propiedades** ubicado en el menú de navegación.

5. Agrega los siguientes ajustes a la aplicación:

    1. Sube un logotipo para el reconocimiento del usuario final. Puedes recuperar el logo de Bitwarden aquí.

    2. Establezca la **URL de la página de inicio** en su página de inicio de sesión del cliente Bitwarden, como `https://vault.bitwarden.com/#/login` o `su-propiaURLalojada.com`.

Una vez completado este proceso, los usuarios asignados tendrán una aplicación Bitwarden que los vinculará directamente a la página de inicio de sesión de la caja fuerte web de Bitwarden.