Implementación de SSO de Confianza Cero de Cloudflare

Implementación de SSO de Confianza Cero de Cloudflare

Este artículo contiene ayuda específica de **Cloudflare Zero Trust** para configurar el inicio de sesión con SSO. Cloudflare Zero Trust es una plataforma de gestión de identidad y acceso basada en la nube que puede integrarse con múltiples proveedores de Identidad (IdPs). También puedes configurar pasarelas y túneles para un acceso seguro a la plataforma.

> **Note**
>
> Cloudflare Zero Trust can be configured with any IdP that operates using SAML 2.0 or OIDC SSO configurations. If you are not familiar with these configurations, refer to these articles:
>
> - SAML 2.0 Configuration
> - OIDC Configuration

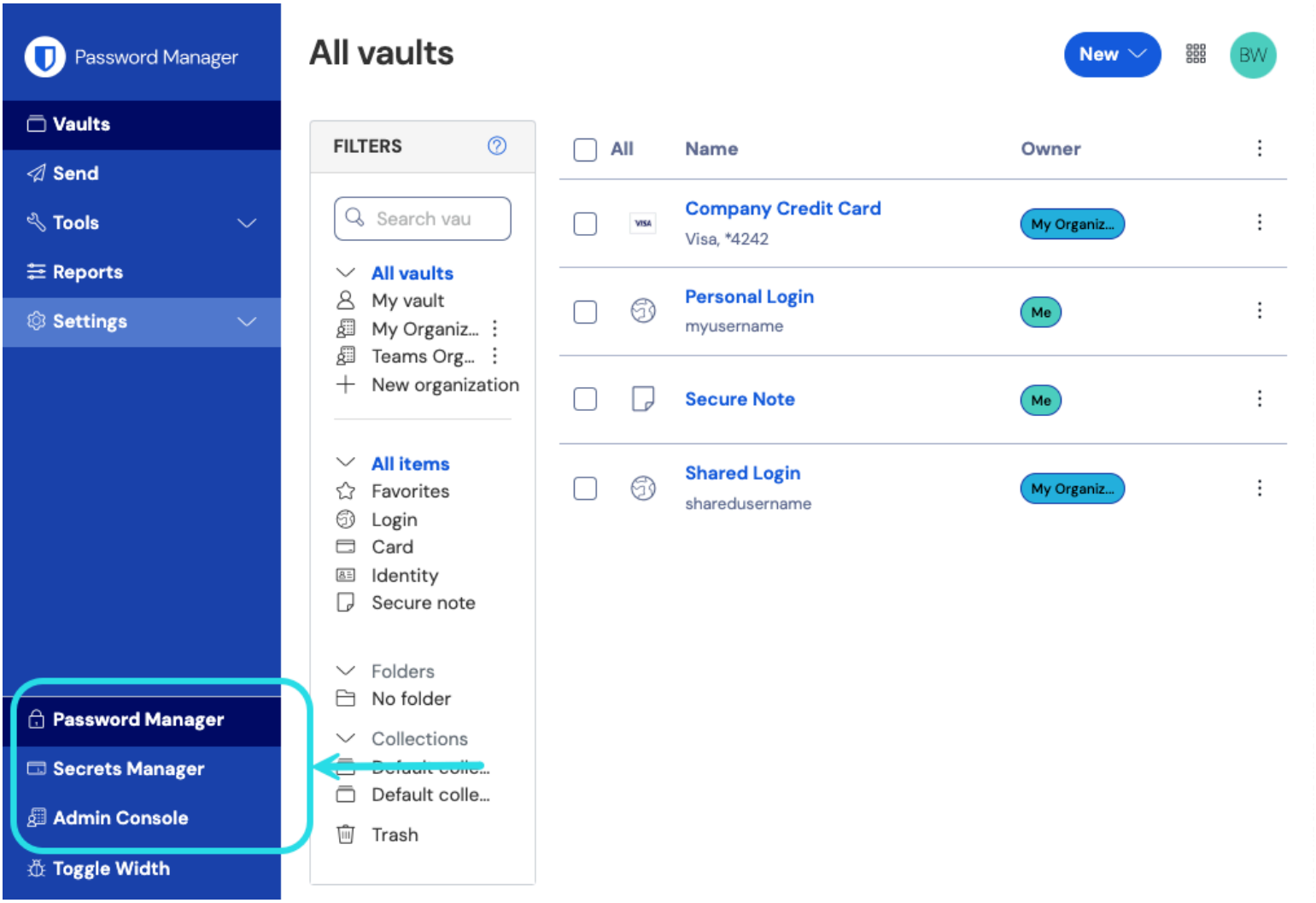
¿Por qué usar Cloudflare Zero Trust con SSO?

Cloudflare Zero Trust es una plataforma de gestión de identidad y acceso basada en la nube que puede integrarse con múltiples proveedores de Identidad (IdPs). La ventaja de usar Cloudflare Zero Trust además de su IdP estándar es su capacidad para configurar múltiples IdPs para el inicio de sesión. Cloudflare Zero Trust puede proporcionar acceso SSO a Bitwarden desde varias organizaciones separadas, o conjuntos de usuarios dentro de una organización.

Abre SSO en la aplicación web

> **Note**
>
> Cloudflare will only support SAML via the Access Application Gateway. This means that the **SAML 2.0** must be selected in the Bitwarden configuration. OIDC authentication can still be configured from the IdP and Cloudflare.

Inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el conmutador 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 una 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.

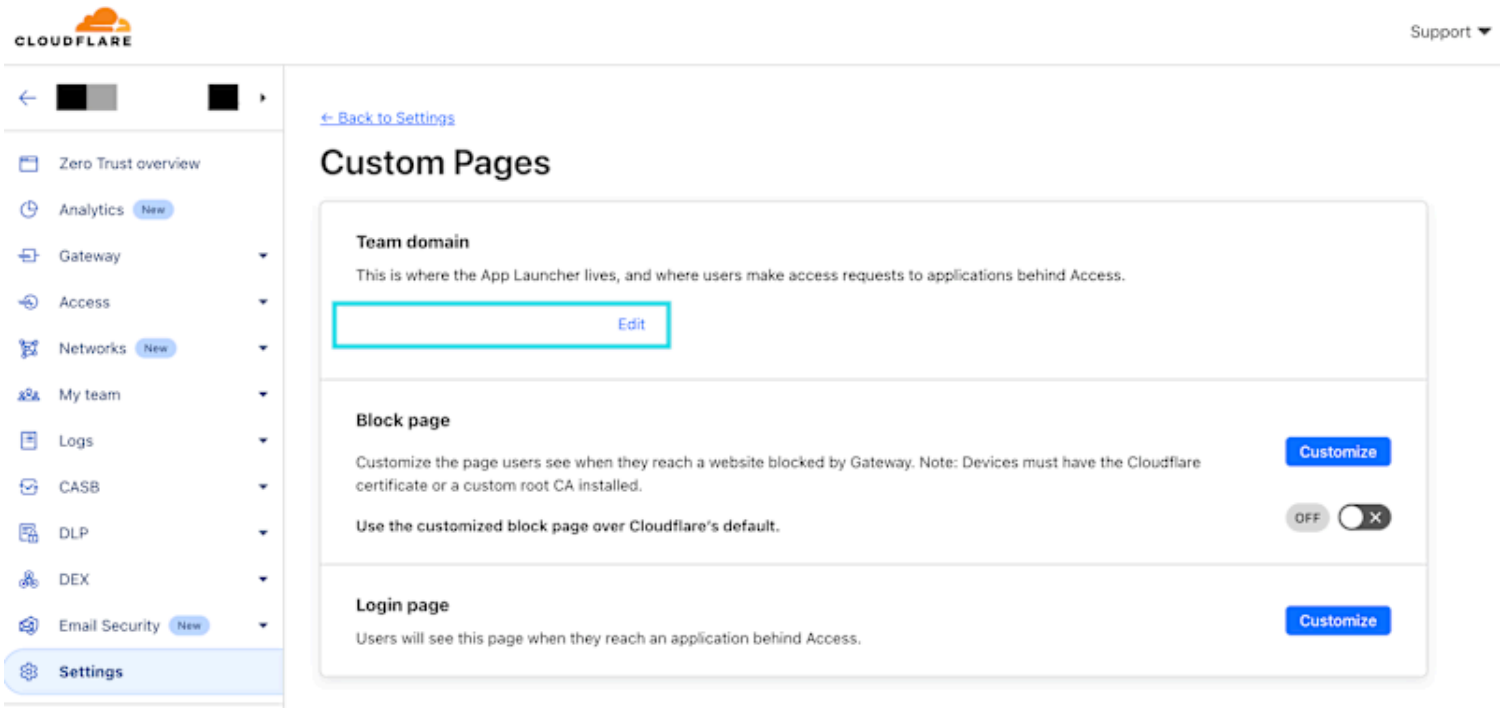
> **Tip**
>
> Hay opciones alternativas de **descifrado de miembro**. Aprenda cómo comenzar a usar SSO con dispositivos de confianza o Conector de clave.

Crea un método de inicio de sesión de confianza cero de Cloudflare

Para crear un método de inicio de sesión de Cloudfare Zero Trust:

1. Navega a Cloudflare Zero Trust e inicia sesión o crea una cuenta.

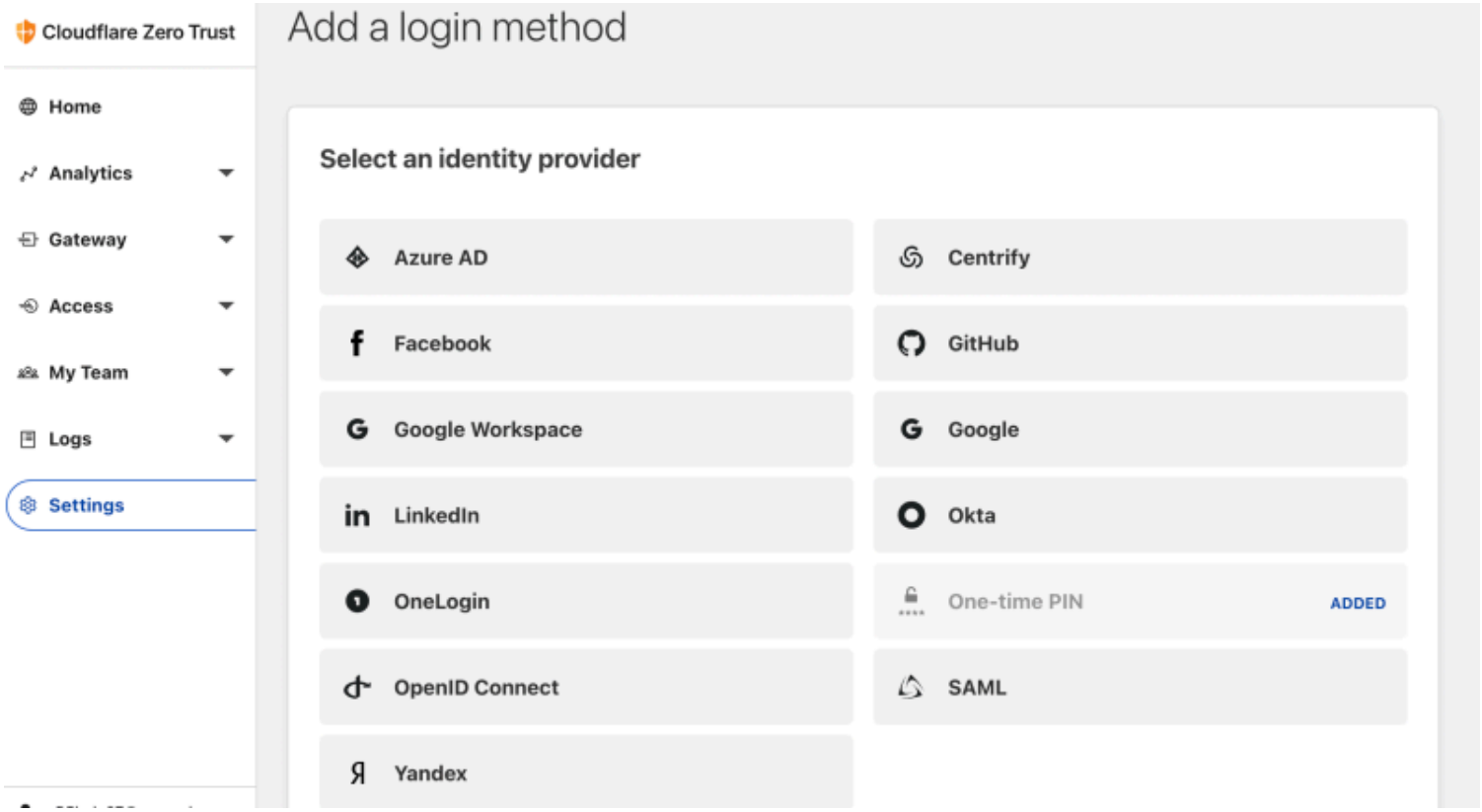
2. Configura un dominio, que actuará como la URL utilizada por tus usuarios para acceder a tus aplicaciones o **App Launcher**, por ejemplo `https://my-business.cloudflareaccess.com/`. Desde el menú de Cloudflare Zero Trust, selecciona **Ajustes** → **General** → **Dominio de Equipos**:



Team domain setting

3. Comienza a configurar el primer método de inicio de sesión navegando a **Ajustes** → **Autenticación** → **Agregar nuevo.**

4. Seleccione el método de inicio de sesión para conectarse a Cloudflare Zero Trust. Si el IdP que estás utilizando no está presente en la lista de IdP, utiliza las opciones genéricas de SAML o OIDC. En este artículo, Okta se utilizará como ejemplo:



Cloudflare Zero Trust IdP list

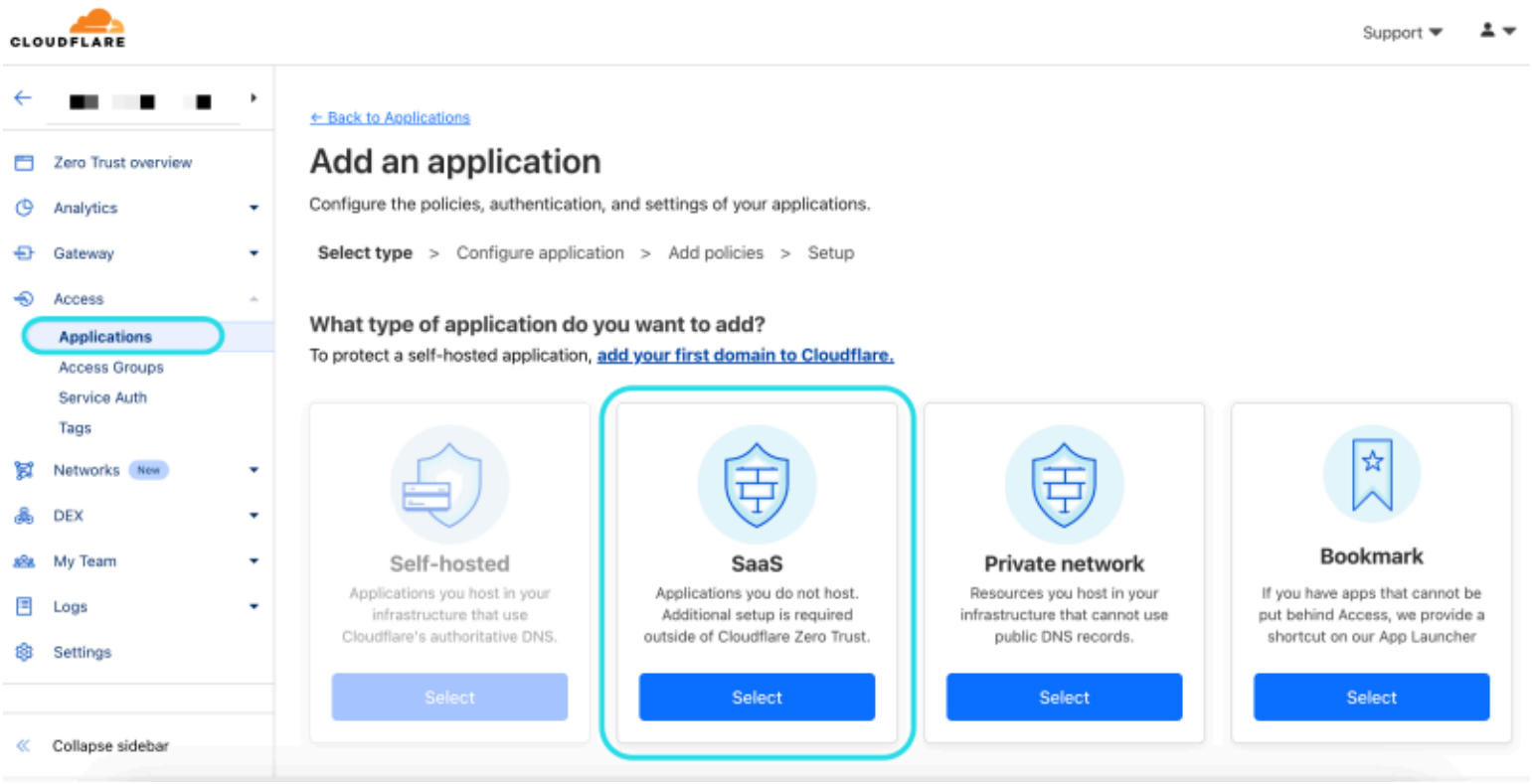
5. Después de seleccionar su método de inicio de sesión IdP elegido, siga la guía del producto proporcionada por Cloudflare para integrar su IdP.

> **Note**
>
> If the IdP you are using has a **support groups** feature, this option must be **disabled**. Bitwarden does not support group based claims, enabling this option will result in an XML element error on the Bitwarden end.

Crea una aplicación de Confianza Cero de Cloudflare

Después de que se haya configurado un IdP, tendrás que crear una aplicación de Confianza Cero de Cloudflare para Bitwarden. **En este ejemplo crearemos una aplicación SAML** :

1. Navega a **Acceso** → **Aplicaciones** → **Agregar una aplicación**.



CFZT add an application

2. Seleccione el tipo **SaaS**.

3. En la caja fuerte web de Bitwarden, abre tu organización y navega a la pantalla de **Ajustes** → **Inicio de Sesión Único**. Utilice la información de la caja fuerte web para completar la información en la pantalla **Configurar aplicación**:

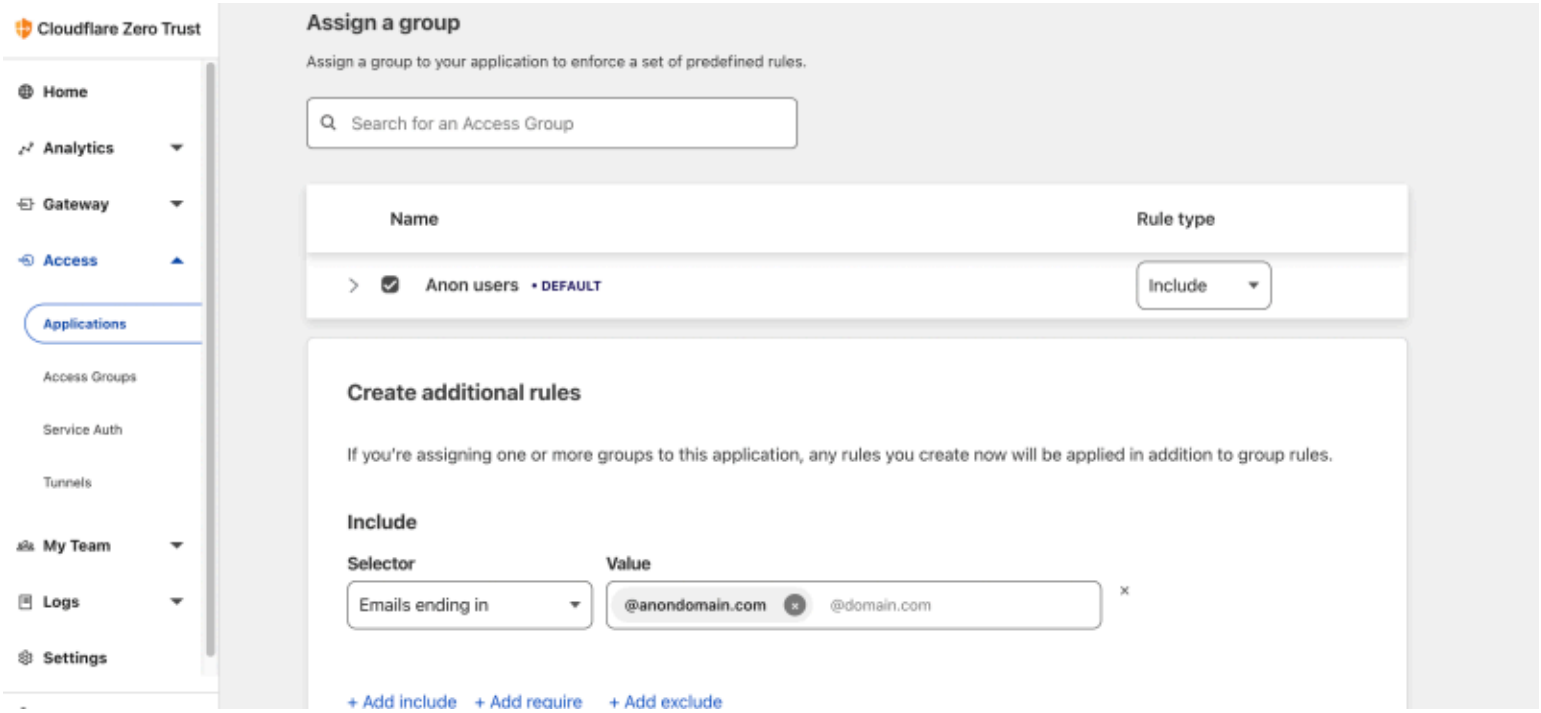
Clave	Descripción
Aplicación	Ingrese `Bitwarden`.
ID de la entidad	Copia el **ID de entidad SP** de la página de Bitwarden Single Sign-On en este campo.
URL del Servicio de Consumo de Afirmaciones	Copia la **URL del servicio de consumo de aserciones (ACS)** de la página de inicio de sesión única de Bitwarden en este campo.
Formato de Identificación de Nombre	Seleccione **Correo electrónico** del menú desplegable.

> **Note**
> For the generic OIDC configuration, the Auth URL, Token URL, and Certificate URL can be located with the well-known URL.

4. Desplázate hacia abajo hasta el menú de **Proveedores de Identidad**. Seleccione el o los IdP(s) que configuró en la sección anterior, desplácese de nuevo al principio y seleccione **Siguiente.**

5. A continuación, crea políticas de acceso para el acceso de los usuarios a la aplicación. Complete los campos de **Nombre de la política**, **Acción** y **Duración de la sesión** para cada política.

6. Puede elegir asignar una política de grupo (**Acceso** → **Grupos**) o reglas explícitas de políticas de usuario (como correos electrónicos, "correos electrónicos que terminan en", "país" o "todos"). En el siguiente ejemplo, el grupo "Anon Users" ha sido incluido en la política. Se ha agregado una regla adicional para incluir correos electrónicos que terminen en el dominio elegido:



CFZT app policy

> **Note**
> You can also apply user access through the **App Launcher** for access to the Bitwarden login with SSO shortcut. This can be managed by navigating to **Authentication** → **App Launcher** → **Manage**. The application policies in the above example can be duplicated or generated here.

7. Una vez que se hayan configurado las políticas de acceso, desplácese hasta la parte superior y seleccione **Siguiente**.

8. Mientras estás en la pantalla de **Configuración**, copia los siguientes valores e ingrésalos en sus respectivos campos en la página de **Inicio de Sesión Único** de Bitwarden:

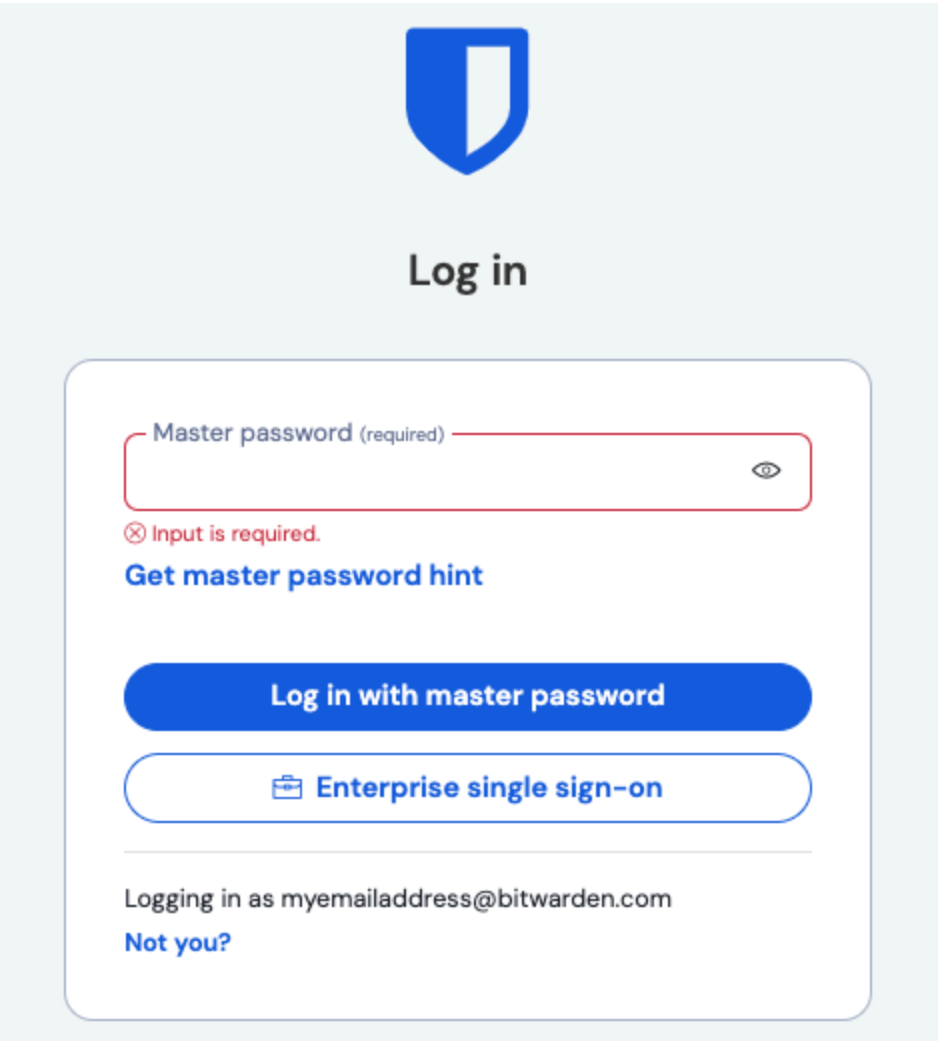
Clave	Descripción
Punto final de SSO	El punto final de SSO dirige a dónde su aplicación SaaS enviará las solicitudes de inicio de sesión. Este valor se ingresará en el campo **URL del Servicio de Inicio de Sesión Único** en Bitwarden.
Acceder a la entidad ID o emisor	La ID de Entidad de Acceso o Emisor es el identificador único de su aplicación SaaS. Este valor se ingresará en el campo **ID de Entidad** en Bitwarden.
Clave pública	La clave pública es el certificado de acceso público que se utilizará para verificar tu identidad. Este valor se ingresará en el campo **Certificado Público X509** en Bitwarden.

9. Después de que los valores hayan sido ingresados en Bitwarden, selecciona **Guardar** en la pantalla de Inicio de Sesión Único de Bitwarden y selecciona **Hecho** en la página de Cloudflare para guardar la aplicación.

10. Para crear un marcador para la pantalla de inicio de sesión de Bitwarden con SSO, selecciona **Agregar una aplicación** → **Marcador**. Verifica que el Marcador sea visible en el **Lanzador de Aplicaciones**.

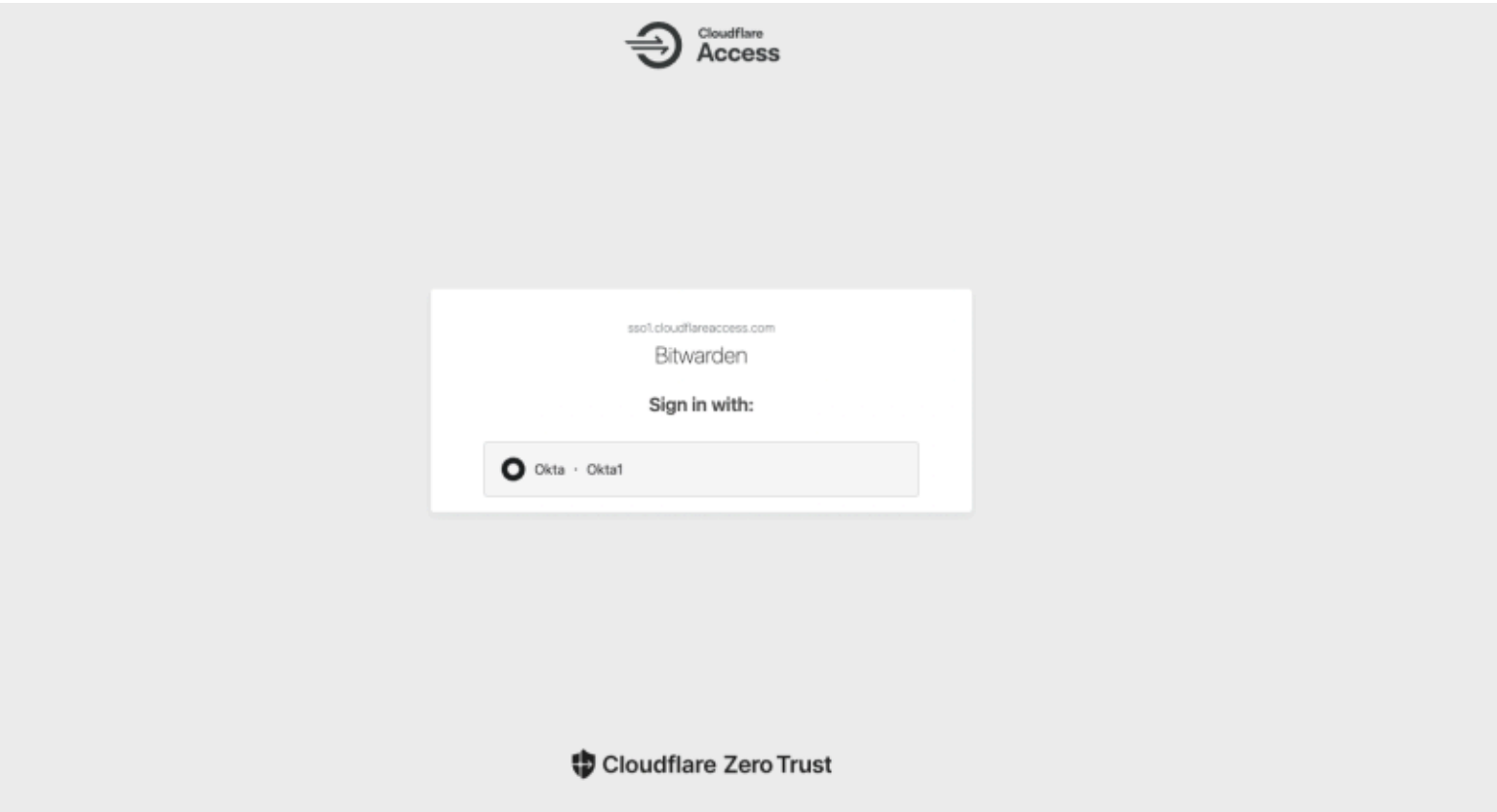
Prueba la configuración

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 **Inicio de sesión único de la Empresa** .



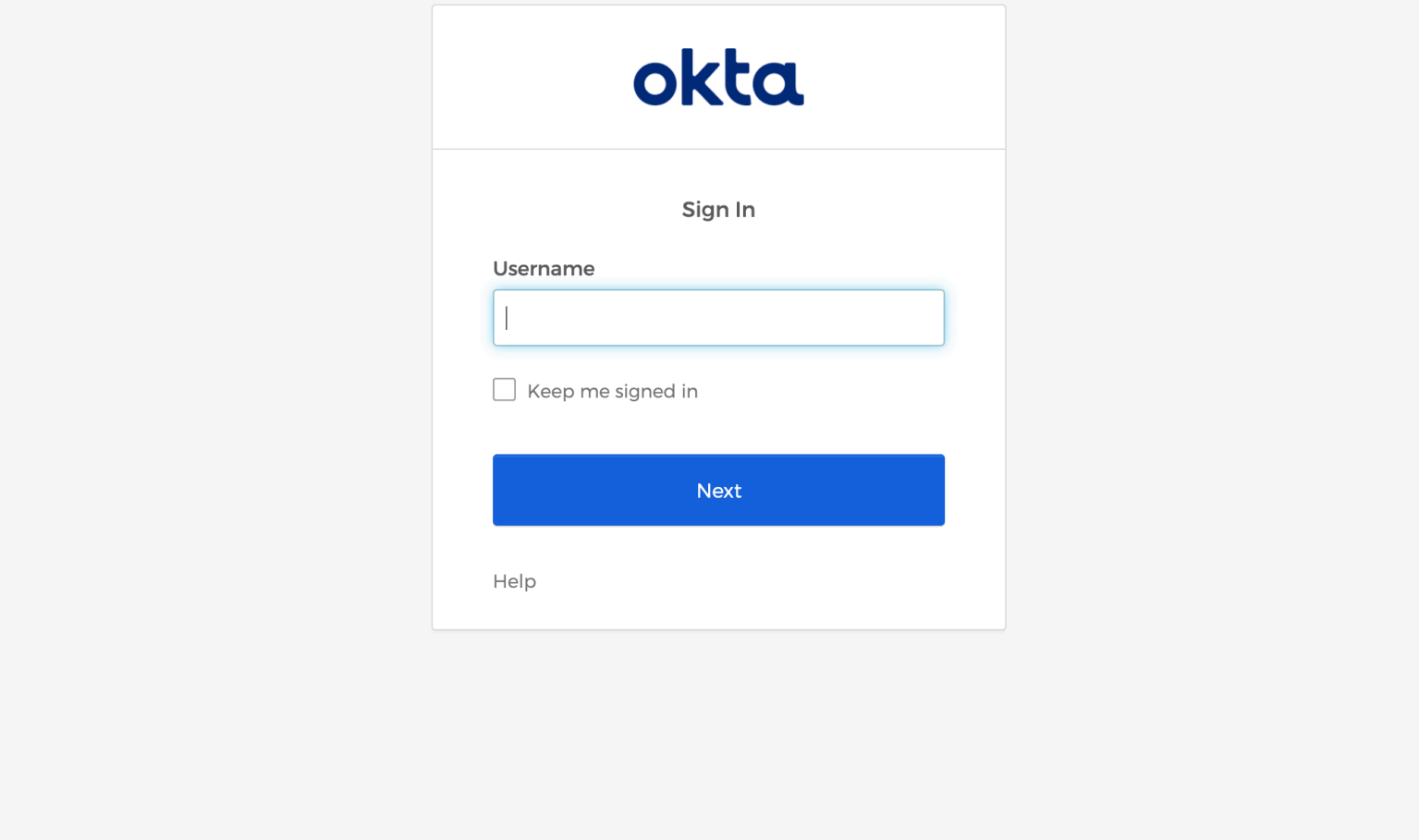
Inicio de sesión único empresarial y contraseña maestra

Ingrese el identificador de organización configurado y seleccione **Iniciar sesión**. Si su implementación está configurada correctamente, será redirigido a una pantalla de Cloudflare Access, donde puede seleccionar el IdP para iniciar sesión con:



Cloudflare IdP selection

Después de seleccionar tu IdP, serás dirigido a la página de inicio de sesión de tu IdP. Ingrese la información utilizada para el inicio de sesión a través de su IdP:



CFZT IdP login

¡Después de autenticarte con tus credenciales de IdP, ingresa tu contraseña maestra de Bitwarden para descifrar tu caja fuerte!