bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML en Auth0

Ver en el centro de ayuda:
https://bitwarden.com/help/saml-auth0/

Implementación de SAML en Auth0

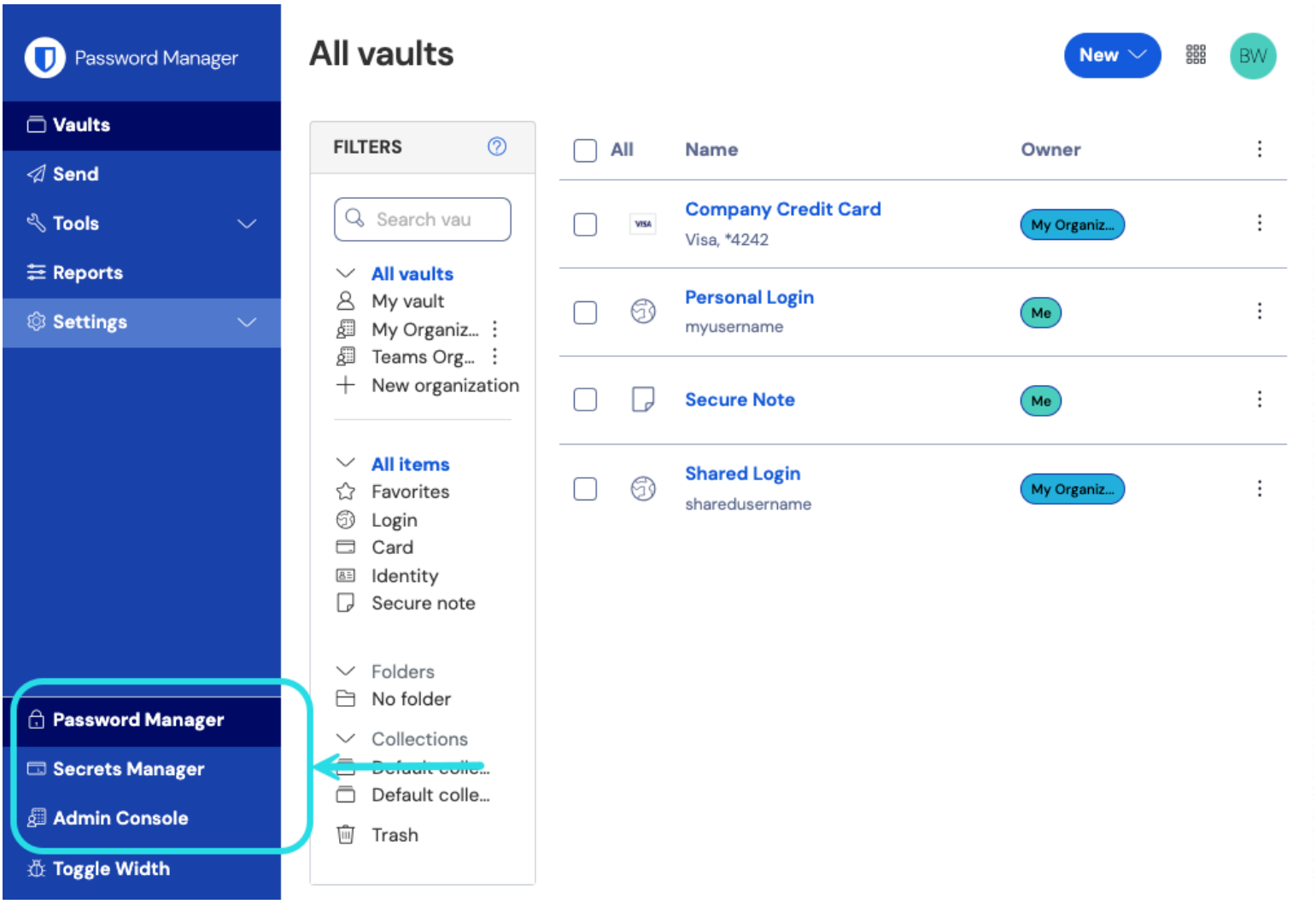
Este artículo contiene ayuda **específica de Auth0** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte Configuración de SAML 2.0.

La configuración implica trabajar simultáneamente dentro de la aplicación web de Bitwarden y el Portal de Auth0. 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 conmutador de producto (▦):



Selector de producto

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

Configuración de SAML 2.0

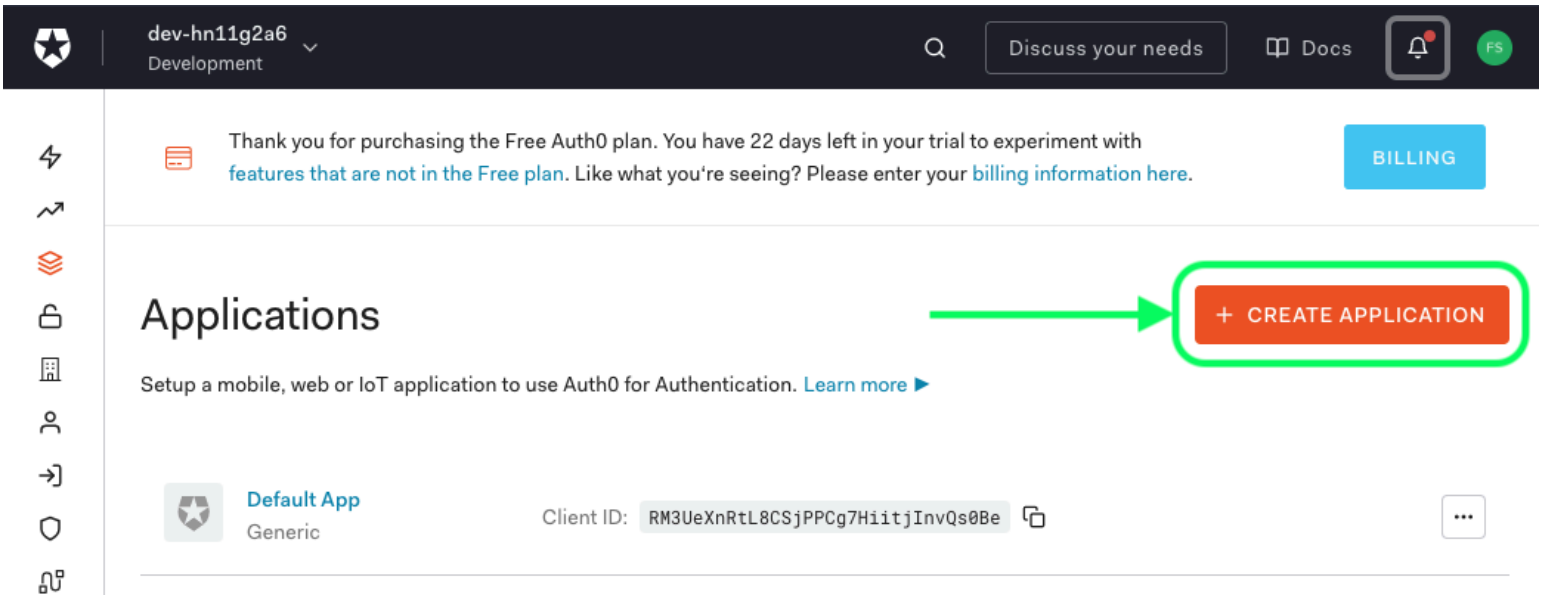
Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de **Tipo**. Mantén esta pantalla abierta para fácil referencia.

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.

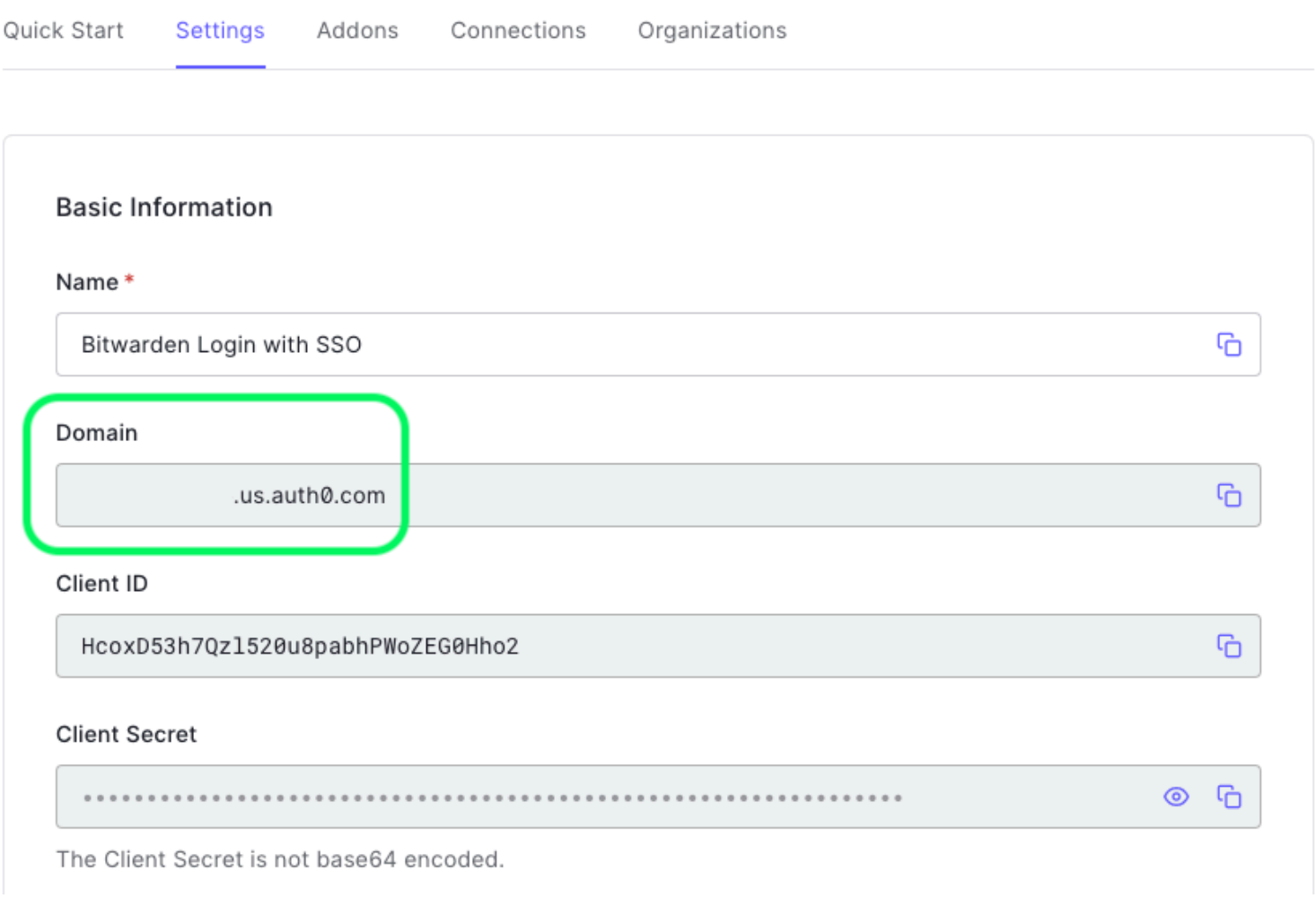
Crea una aplicación Auth0

En el Portal de Auth0, use el menú de Aplicaciones para crear una **Aplicación Web Regular**:



Auth0 Create Application

Haz clic en la pestaña **Ajustes** y configura la siguiente información, parte de la cual necesitarás recuperar de la pantalla de inicio de sesión único de Bitwarden:



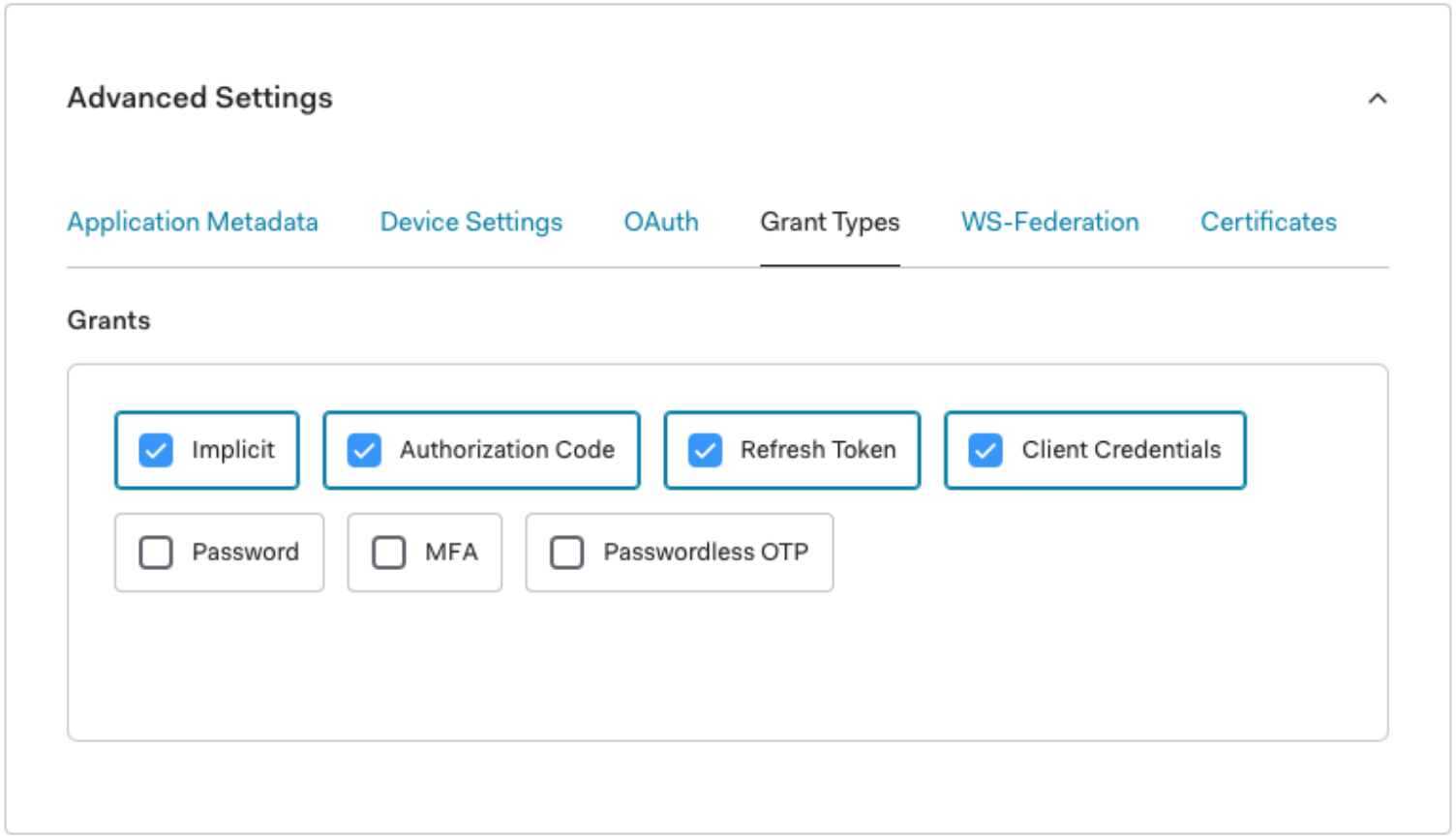
AuthO Settings

Ajuste de AuthO	Descripción
Nombre	Dale a la aplicación un nombre específico de Bitwarden.
Dominio	Toma nota de este valor. Lo necesitarás durante un paso posterior.
Tipo de Aplicación	Seleccione **Aplicación Web Regular**.
Método de Autenticación del Punto Final del Token	Seleccione **Post** (HTTP Post), que se mapeará a un atributo de **Tipo de Enlace** que configurará más tarde.

Ajuste de Auth0	Descripción
URI de inicio de sesión de la aplicación	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.
URLS de devolución de llamada permitidos	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.

Tipos de Subvenciones

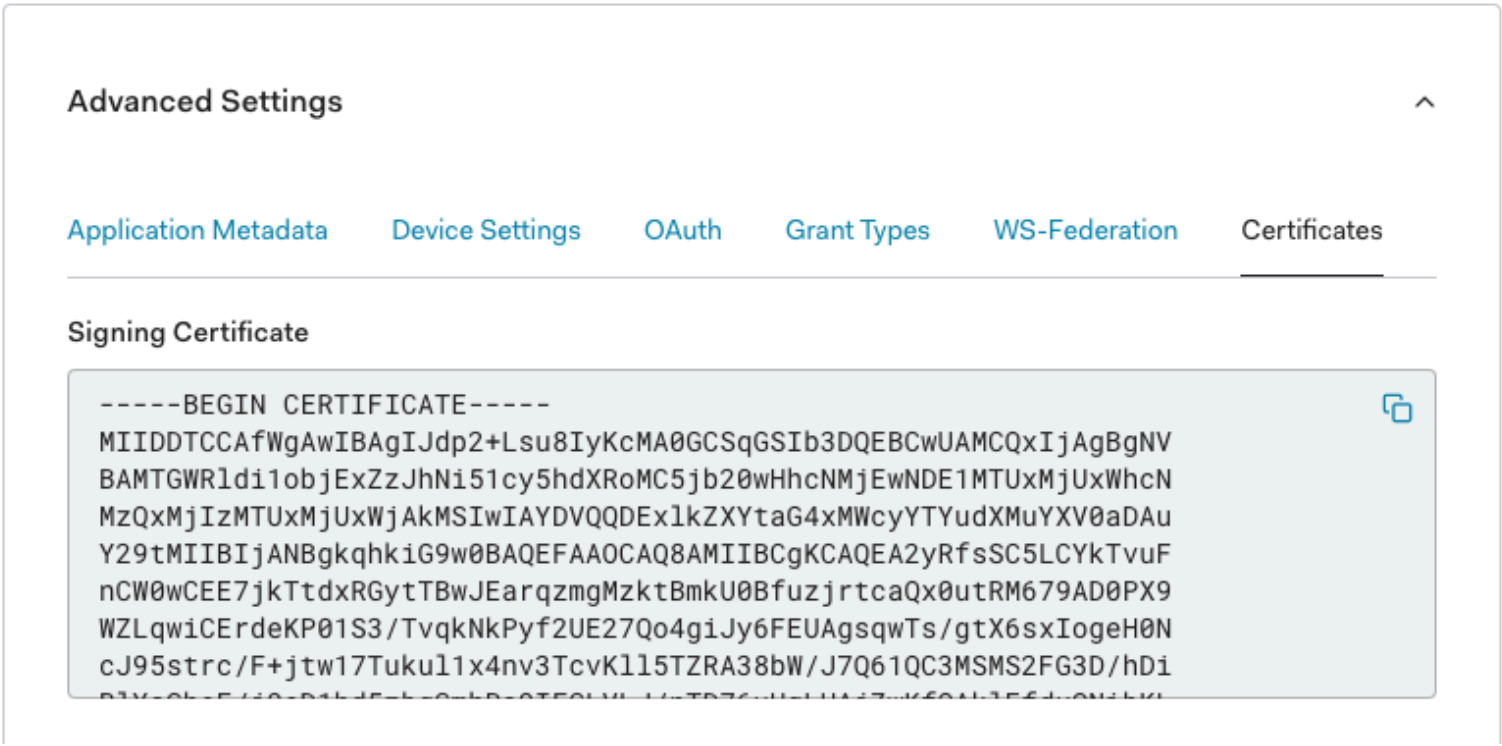
En la sección de **Ajustes Avanzados → Tipos de Concesión**, asegúrate de que los siguientes Tipos de Concesión estén seleccionados (pueden estar preseleccionados):



Application Grant Types

Certificados

En la sección de **Ajustes Avanzados → Certificados**, copia o descarga tu certificado de firma. No necesitarás hacer nada con eso por ahora, pero necesitarás referenciarlo más tarde.

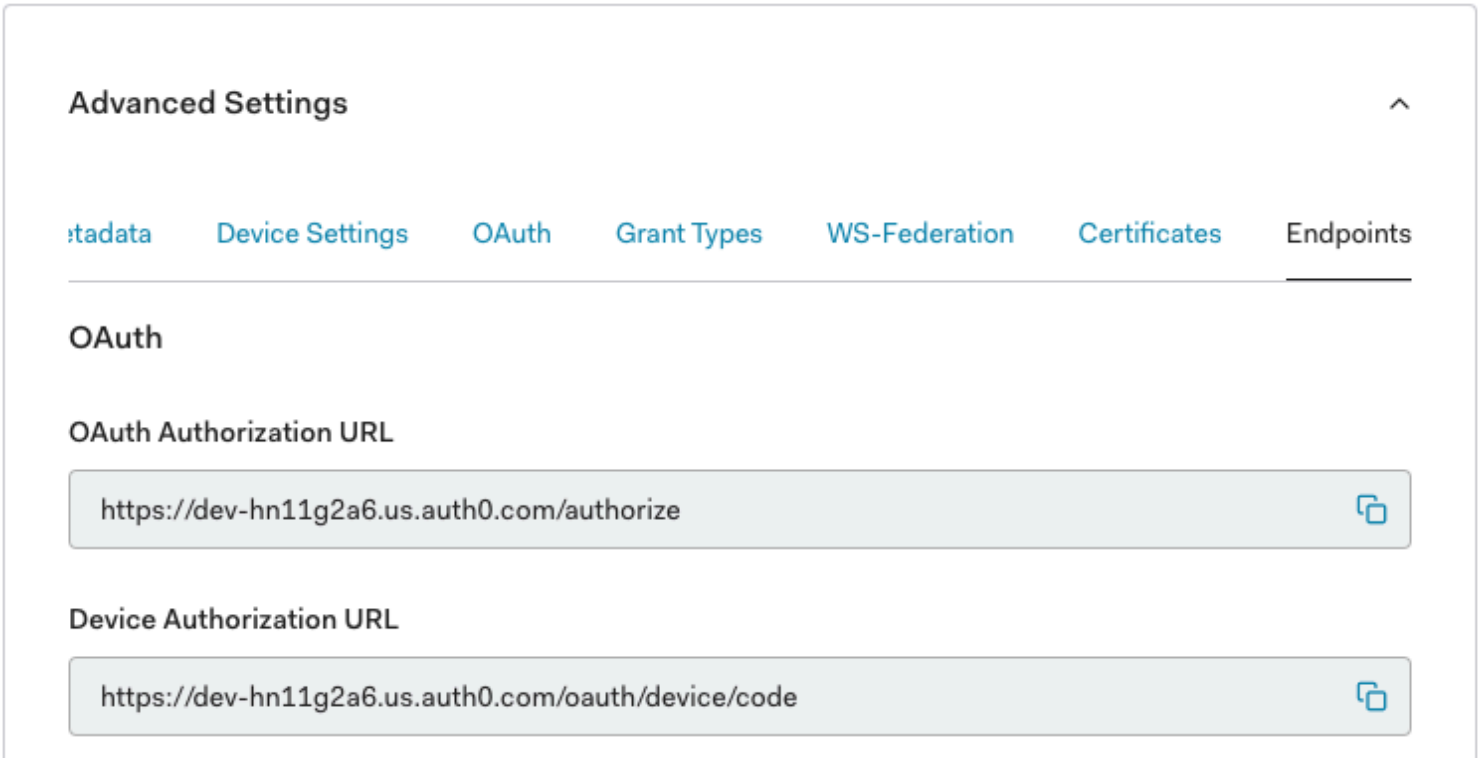


Auth0 Certificate

Puntos finales

No necesitas editar nada en la sección de **Ajustes Avanzados → Puntos finales**, pero necesitarás los puntos finales de SAML para referencia posterior.

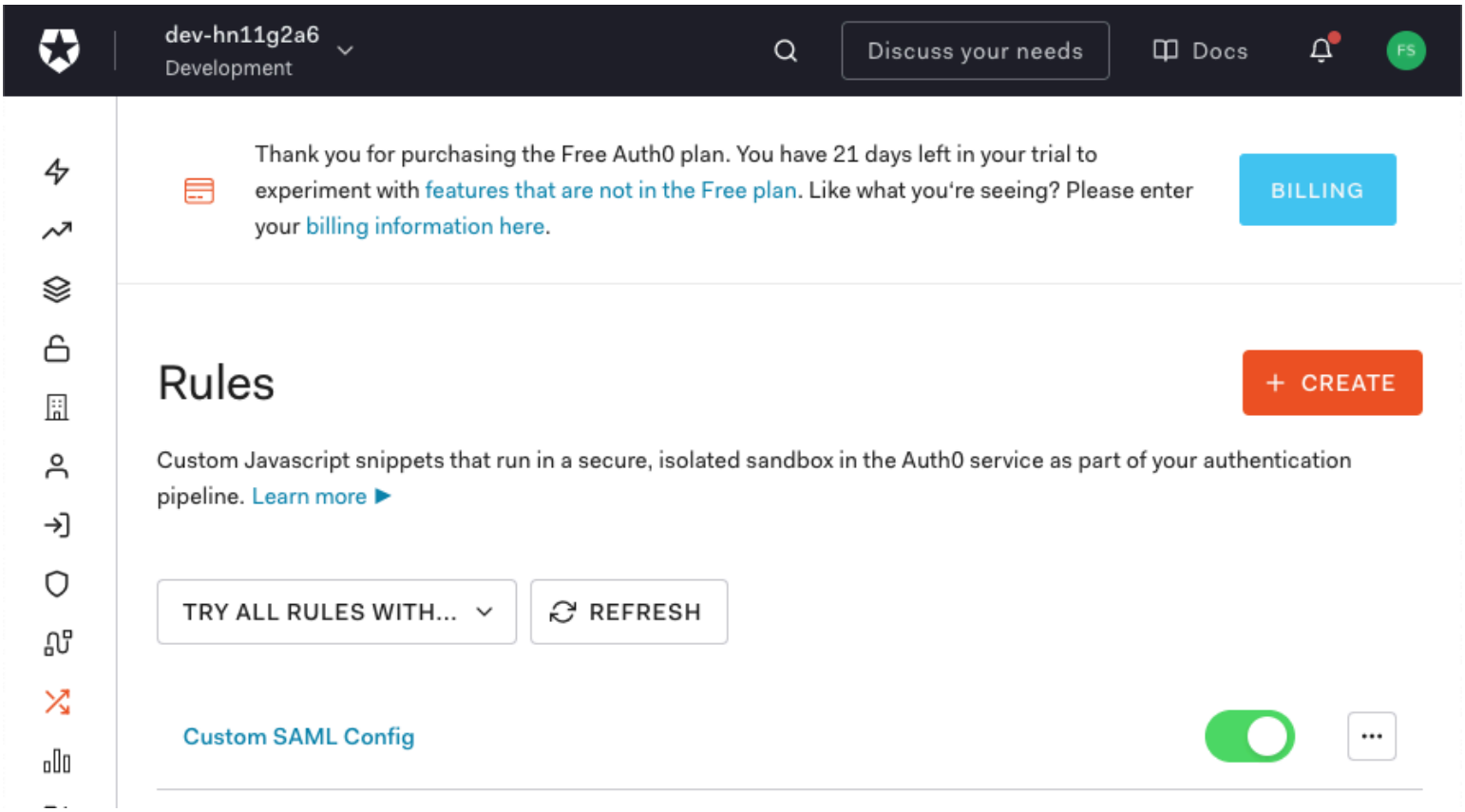
> **Tip**
>
> In smaller windows, the **Endpoints** tab can disappear behind the edge of the browser. If you're having trouble finding it, click the **Certificates** tab and hit the Right Arrow key (→).



Auth0 Endpoints

Configura las reglas de Auth0

Crea reglas para personalizar el comportamiento de la respuesta SAML de tu aplicación. Mientras que Auth0 proporciona un número de opciones, esta sección se centrará solo en aquellas que se corresponden específicamente con las opciones de Bitwarden. Para crear un conjunto de reglas de configuración SAML personalizado, use el menú **Tubería de Autenticación** → **Reglas** para + **Crear** Reglas:



Auth0 Rules

Puede configurar cualquiera de los siguientes:

Clave	Descripción
`algoritmoDeFirma`	Algoritmo que Auth0 utilizará para firmar la afirmación o respuesta SAML. Por defecto, se incluirá `rsa-sha1`, sin embargo, este valor debería ajustarse a `rsa-sha256`. Si cambias este valor, debes: -Establezca `digestAlgorithm` en `sha256`. -Establece (en Bitwarden) el **Algoritmo de Firma Entrante Mínimo** a `rsa-sha256`.
`algoritmoDigestión`	Algoritmo utilizado para calcular el resumen de la afirmación o respuesta de SAML. Por defecto, `sha-1`. El valor para `signatureAlgorithm`, también debe establecerse en `sha256.`
`Respuesta de firma`	Por defecto, Auth0 solo firmará la afirmación SAML. Establezca esto en `verdadero` para firmar la respuesta SAML en lugar de la afirmación.

Clave	Descripción
`formatoDeIdentificadorDeNombre`	Por defecto, `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`. Puedes establecer este valor a cualquier formato de NameID SAML. Si lo haces, cambia el campo SP **Formato de ID de Nombre** a la opción correspondiente (ver aquí).

Implementa estas reglas usando un **Script** como el que se muestra a continuación. Para obtener ayuda, consulte la Documentación de Auth0.

```bash
function (user, context, callback) {
    context.samlConfiguration.signatureAlgorithm = "rsa-sha256";
    context.samlConfiguration.digestAlgorithm = "sha256";
    context.samlConfiguration.signResponse = "true";
    context.samlConfiguration.nameIdentifierFormat = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
    context.samlConfiguration.binding = "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect";
    callback(null, user, context);
}
```

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal Auth0. 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

A menos que haya configurado reglas personalizadas, su configuración del proveedor de servicios ya estará completa. Si configuraste reglas personalizadas o quieres hacer más cambios en tu implementación, edita los campos relevantes:

Campo	Descripción
Formato de Identificación de Nombre	Formato de NameID para especificar en la solicitud SAML (`Política de NameID`). Para omitir, establezca en **No Configurado**.

Campo	Descripción
Algoritmo de Firma de Salida	Algoritmo utilizado para firmar solicitudes SAML, por defecto `rsa-sha256`.
Comportamiento de Firma	Si/cuando las solicitudes SAML de Bitwarden serán firmadas. Por defecto, Auth0 no requerirá que las solicitudes estén firmadas.
Algoritmo Mínimo de Firma Entrante	El algoritmo de firma mínimo que Bitwarden aceptará en las respuestas de SAML. Por defecto, Auth0 firmará con `rsa-sha1`. Seleccione `rsa-sha256` del menú desplegable a menos que haya configurado una regla de firma personalizada.
Quiero Afirmaciones Firmadas	Si Bitwarden quiere firmas de afirmaciones SAML. Por defecto, Auth0 firmará las afirmaciones SAML, así que marque esta casilla a menos que haya configurado una regla de firma personalizada.
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 dentro de 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 vuelvas al Portal de Auth0 para recuperar los valores de la aplicación:

Campo	Descripción
ID de la entidad	Ingrese el valor de **Dominio** de su aplicación Auth0 (ver aquí), precedido por `urn:`, por ejemplo `urn:bw-help.us.auth0.com`. Este campo distingue entre mayúsculas y minúsculas.
Tipo de Encuadernación	Seleccione **HTTP POST** para coincidir con el valor especificado en su aplicación Auth0 para el Método de Autenticación del Endpoint del Token.

Campo	Descripción
URL del Servicio de Inicio de Sesión Único	Ingrese la **URL del Protocolo SAML** (vea Puntos finales) de su aplicación Auth0. Por ejemplo, `https://bw-help.us.auth0.com/samlp/HcpxD63h7Qzl420u8qachPWoZEG0Hho2`.
URL del Servicio de Cierre de Sesión Único	Inicie sesión con SSO actualmente **no** admite SLO. Esta opción está planeada para desarrollo futuro, sin embargo, puedes preconfigurarla si lo deseas.

Certificado Público X509	Pega el certificado de firma 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, Auth0 firmará con `rsa-sha1`. Seleccione `rsa-sha256` a menos que haya configurado una regla de firma personalizada.
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 Auth0 espera que las solicitudes SAML estén firmadas.

Note

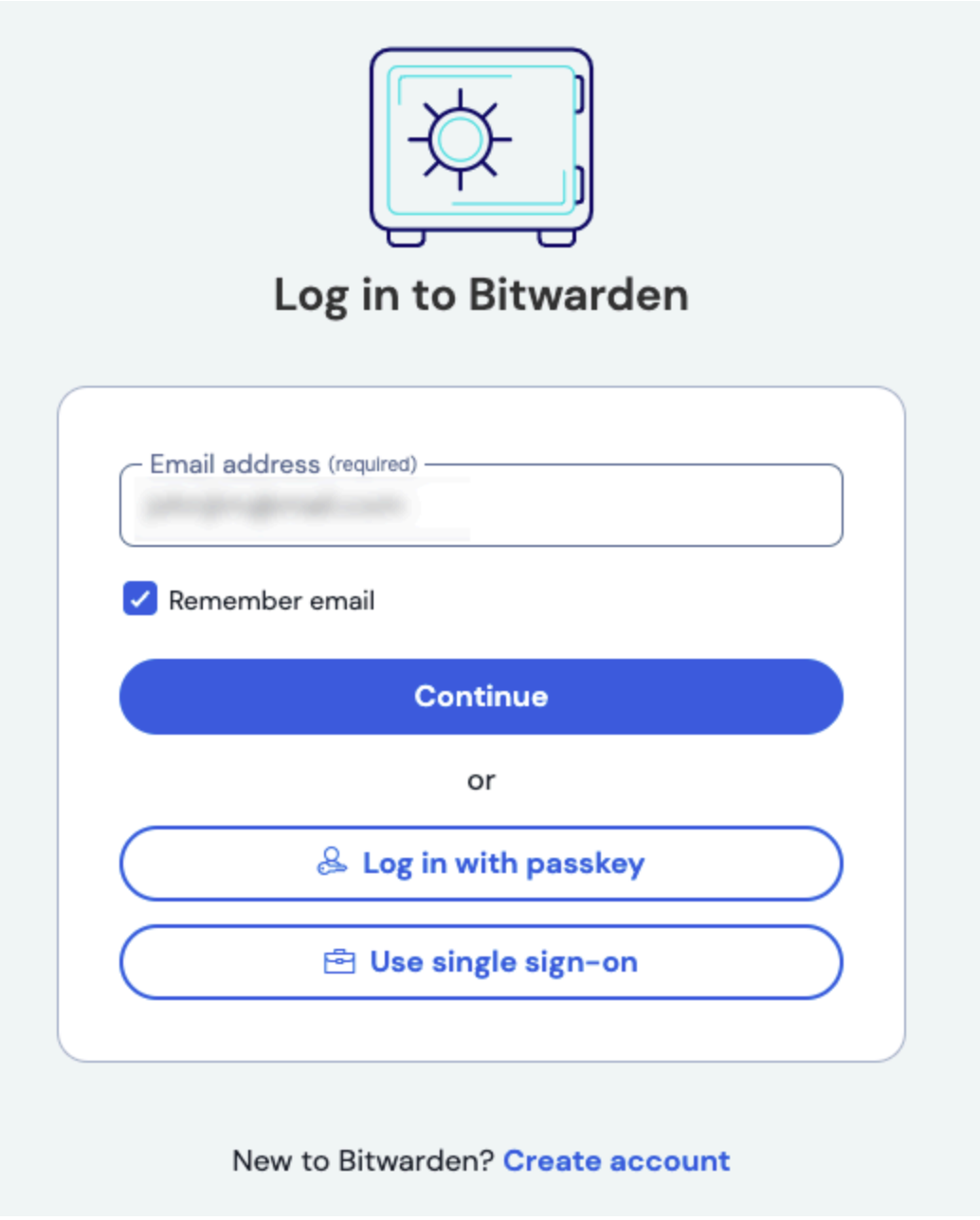
Al completar el certificado X509, toma nota de la fecha de vencimiento. Los certificados tendrán que ser renovados para prevenir cualquier interrupción en el servicio a los usuarios finales de SSO. Si un certificado ha caducado, las cuentas de Administrador y Propietario siempre podrán iniciar sesión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

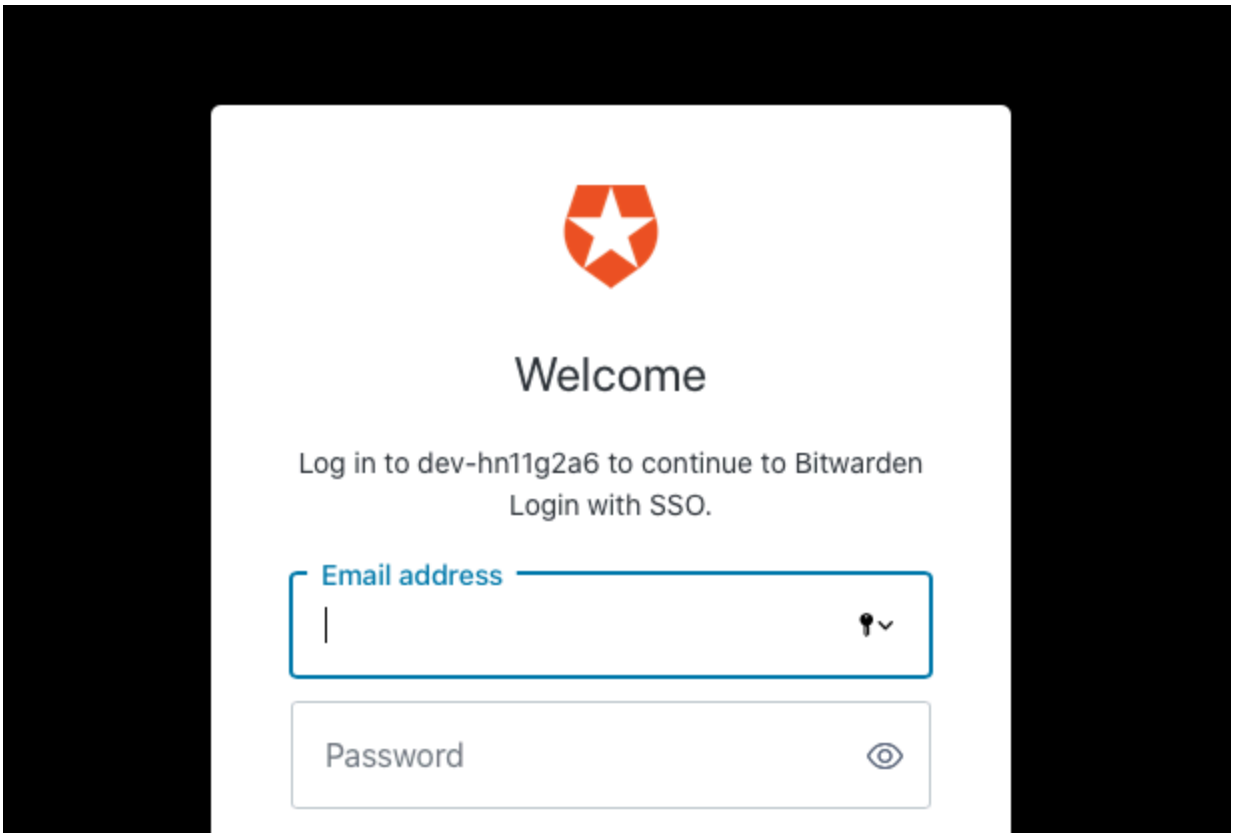
Prueba la configuración

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 Auth0:



Auth0 Login

¡Después de autenticarte con tus credenciales de Auth0, ingresa tu contraseña maestra de Bitwarden para desencriptar 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.