

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 (🏠):

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card	My Organiz...	⋮
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Selector de producto

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

The screenshot shows the "Single sign-on" configuration page in the Bitwarden Admin Console. On the left is a sidebar with navigation options: My Organization, Collections, Members, Groups, Reporting, Billing, Settings, Organization info, Policies, Two-step login, Import data, Export vault, Domain verification, Single sign-on (active), Device approvals, and SCIM provisioning. The main content area has the title "Single sign-on" and a QR code icon. Below the title is a description: "Use the [require single sign-on authentication policy](#) to require all members to log in with SSO." There are two checked options: "Allow SSO authentication" (with a sub-note: "Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.") and "Member decryption options" (with sub-options: "Master password" selected and "Trusted devices" unselected, with a note: "Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used."). A text input field contains "unique-organization-identifier" under the label "SSO identifier (required)". Below it is a note: "Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)". A dropdown menu for "Type" is set to "SAML 2.0". The "SAML service provider configuration" section includes a checked option "Set a unique SP entity ID" (with sub-note: "Generate an identifier that is unique to your organization") and two masked input fields for "SP entity ID" and "SAML 2.0 metadata URL", each with a copy icon.

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](#).

Creando una aplicación Auth0

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

dev-hn11g2a6
Development

Thank you for purchasing the Free Auth0 plan. You have 22 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your [billing information here](#). BILLING

Applications

Setup a mobile, web or IoT application to use Auth0 for Authentication. [Learn more](#) ▶

Default App
Generic

Client ID: `RM3UeXnRtL8CSjPPCg7HiitjInvQs0Be`

[+ CREATE APPLICATION](#)

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:

Basic Information

Name *

Bitwarden Login with SSO



Domain

.us.auth0.com



Client ID

HcoxD53h7Qz1520u8pabHPWoZEG0Hho2



Client Secret

.....



The Client Secret is not base64 encoded.

Auth0 Settings

Ajuste de Auth0

Nombre

Descripción

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 AuthO	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):

Advanced Settings

Application Metadata Device Settings OAuth **Grant Types** WS-Federation Certificates

Grants

Implicit Authorization Code Refresh Token Client Credentials

Password MFA Passwordless OTP

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](#).

Advanced Settings ^

[Application Metadata](#) [Device Settings](#) [OAuth](#) [Grant Types](#) [WS-Federation](#) **[Certificates](#)**

Signing Certificate

```
-----BEGIN CERTIFICATE-----
MIIDDTCCAfwGAWIBAgIJdp2+Lsu8IyKcMA0GCSqGSIb3DQEBCwUAMCQxIjAgBgNV
BAMTGWRldi1objExZzJhNi51cy5hdXRoMC5jb20wHhcNMjEwNDE1MTUxMjUxWhcN
MzQxMjIzMTUxMjUxWjAkMSIwIAYDVQQDExlkZXYtaG4xMWcyYTYudXMUyXV0aDAu
Y29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2yRfsSC5LCYkTvuF
nCW0wCEE7jkTtdxRGytTBwJEarqzmgMzktBmkU0BfuzjrtcaQx0utRM679AD0PX9
WZLqwICErdeKP01S3/TvqkNkPyf2UE27Qo4giJy6FEUAgSqWts/gtX6sxIogeH0N
cJ95strc/F+jtw17Tukul1x4nv3TcvK115TZRA38bW/J7Q61QC3MSMS2FG3D/hDi
-----END CERTIFICATE-----
```



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 (→).

Advanced Settings ^

[Metadata](#) [Device Settings](#) [OAuth](#) [Grant Types](#) [WS-Federation](#) [Certificates](#) [Endpoints](#)

OAuth

OAuth Authorization URL

`https://dev-hn11g2a6.us.auth0.com/authorize`

Device Authorization URL

`https://dev-hn11g2a6.us.auth0.com/oauth/device/code`

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**:

dev-hn11g2a6
Development

Docs
F5

Thank you for purchasing the Free Auth0 plan. You have 21 days left in your trial to experiment with [features that are not in the Free plan](#). Like what you're seeing? Please enter your [billing information here](#). BILLING

Rules + CREATE

Custom Javascript snippets that run in a secure, isolated sandbox in the Auth0 service as part of your authentication pipeline. [Learn more](#) ▶

TRY ALL RULES WITH... ▼
REFRESH

Custom SAML Config

...

Auth0 Rules

Puede configurar cualquiera de los siguientes:

Clave	Descripción
algoritmoDeFirma	<p>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.</p> <p>Si cambias este valor, debes:</p> <ul style="list-style-type: none"> -Establezca digestAlgorithm en sha256. -Establece (en Bitwarden) el Algoritmo de Firma Entrante Mínimo a rsa-sha256.
algoritmoDigestión	<p>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.</p>
Respuesta de firma	<p>Por defecto, Auth0 solo firmará la afirmación SAML. Establezca esto en verdadero para firmar la respuesta SAML en lugar de la afirmación.</p>

Clave	Descripción
<code>formatoDeIdentificadorDeNombre</code>	Por defecto, <code>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</code> . 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, establece 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	<p>Pega el certificado de firma recuperado, eliminando</p> <p>-----INICIO CERTIFICADO-----</p> <p>y</p> <p>-----FIN DEL CERTIFICADO-----</p> <p>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.</p>
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.

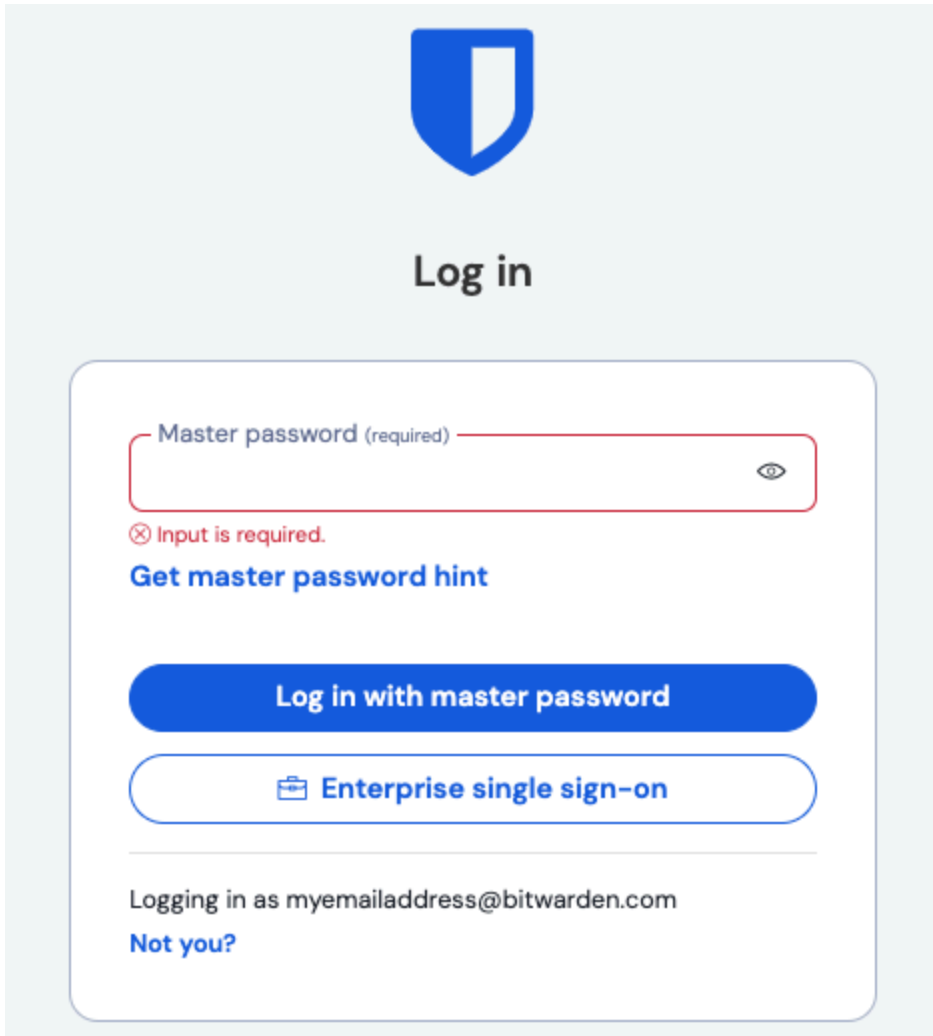
Cuando termines con la configuración del proveedor de identidad, **Guarda** tu trabajo.

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](#).

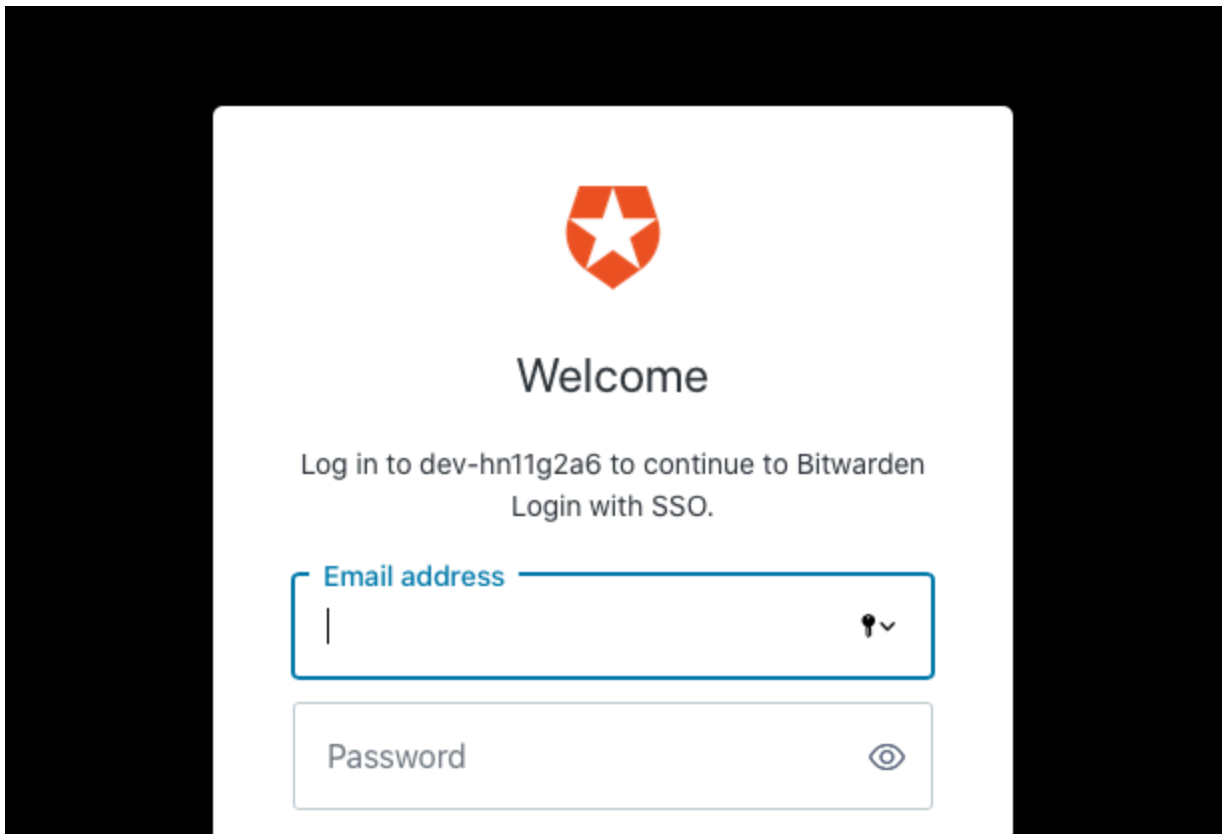
Prueba la configuración

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 descryptar 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.