

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

# Implementación de SAML de OneLogin

Ver en el centro de ayuda:  
<https://bitwarden.com/help/saml-onelogin/>

## Implementación de SAML de OneLogin

Este artículo contiene ayuda específica de **OneLogin** 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 OneLogin. 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 (🏠):

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

Selector de producto

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

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

## Single sign-on



Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

### Member decryption options

Master password

Trusted devices

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.

Type

SAML 2.0

### SAML service provider configuration

Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID

[Masked SP entity ID]

SAML 2.0 metadata URL

[Masked SAML 2.0 metadata URL]

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](#).

## Creación de una aplicación OneLogin

En el Portal de OneLogin, navegue a la pantalla de **Aplicaciones** y seleccione el botón de **Agregar App**:

onelogin Users Applications Devices Authentication Activity Security Settings Developers

## Applications

search company apps...

No company apps have been added.

*Add an Application*

En la barra de búsqueda, escribe **conector de prueba saml** y selecciona la aplicación **Conector de Prueba SAML (Avanzado)**:

onelogin Users Applications Devices Authentication Activity Security Settings Developers

## Find Applications

saml test connector

|  |  |         |
|--|--|---------|
|  | <b>SAML Test Connector (Advanced)</b><br>OneLogin, Inc.      | SAML2.0 |
|  | <b>SAML Test Connector (SP Shibboleth)</b><br>OneLogin, Inc. | SAML2.0 |

*SAML Test Connector App*

Dale a tu aplicación un **Nombre de Visualización** específico de Bitwarden y selecciona el botón de **Guardar**.

### Configuración

Seleccione **Configuración** de la navegación izquierda y configure la siguiente información, parte de la cual deberá recuperar de la pantalla de inicio de sesión único:



Info

Configuration

Parameters

Rules

SSO

Access

## Application details

RelayState

Audience (EntityID)

Recipient

App Configuration

## Ajuste de Aplicación

## Descripción

Audiencia (EntityID)

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.

Destinatario

Establezca este campo con el mismo **ID de Entidad SP** pre-generado utilizado para el ajuste de **Audiencia (ID de Entidad)**.

Validador de URL de ACS (Consumidor)

A pesar de estar marcado como **Requerido** por OneLogin, en realidad no necesitas ingresar información en este campo para integrarte con Bitwarden. Salta al siguiente campo, **URL de ACS (Consumidor)**.

URL (Consumidor) ACS

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.

| Ajuste de Aplicación     | Descripción  |
|--------------------------|--|
| Iniciador SAML           | Seleccione <b>Proveedor de Servicio</b> . El inicio de sesión con SSO actualmente no admite afirmaciones SAML iniciadas por IdP. |
| Formato de nombreID SAML | Establezca este campo en el <a href="#">Formato de NombreID SAML</a> que desea usar para las afirmaciones SAML.                  |
| Elemento de firma SAML   | Por defecto, OneLogin firmará la Respuesta SAML. Puedes configurar esto a <b>Afirmación</b> o <b>Ambos</b>                       |

Seleccione el botón **Guardar** para finalizar sus ajustes de configuración.

### Parámetros

Seleccione **Parámetros** del menú de navegación izquierdo y use el icono **+** **Agregar** para crear los siguientes parámetros personalizados:

| Nombre del Campo   | Valor              |
|--------------------|--------------------|
| correo electrónico | Correo electrónico |
| nombre de pila     | Nombre             |
| apellido           | Apellido           |

Seleccione el botón **Guardar** para finalizar sus parámetros personalizados.

### SSO

Seleccione **SSO** de la navegación izquierda y complete lo siguiente:

1. Seleccione el enlace **Ver Detalles** debajo de su Certificado X.509:

### Enable SAML2.0

Sign on method  
SAML2.0

X.509 Certificate

Standard Strength Certificate (2048-bit)

[Change](#) [View Details](#)

SAML Signature Algorithm

SHA-256

[Issuer URL](#)

<https://app.onelogin.com/saml/metadata/95eef6e7-560f-4531-9df3-02e7248415a8>

SAML 2.0 Endpoint (HTTP)

<https://mmccabe.onelogin.com/trust/saml2/http-post/sso/95eef6e7-560f-4531-9df3-02e7248415a8>

[View your Cert](#)

En la pantalla de Certificado, descargue o copie su Certificado PEM X.509, ya que necesitará [usarlo más tarde](#). Una vez copiado, regresa a la pantalla principal de SSO.

2. Establezca su **Algoritmo de Firma SAML**.

3. Toma nota de tu **URL del emisor** y **Punto final de SAML 2.0 (HTTP)**. Necesitarás [usar estos valores pronto](#).

### Acceso

Seleccione **Acceso** desde la navegación de la mano izquierda. En la sección de **Roles**, asigna el acceso a la aplicación a todos los roles que te gustaría que pudieran usar Bitwarden. La mayoría de las implementaciones crean un rol específico de Bitwarden y optan por asignar en base a un término general (por ejemplo, **Predeterminado**) o en base a roles preexistentes.

|            |                              |
|------------|------------------------------|
| Privileges |                              |
| Setup      | <b>Roles</b>                 |
|            | <b>Bitwarden SSO Users</b> ✓ |
|            | Default                      |

[Role Assignment](#)

## De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal OneLogin. 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 el Portal OneLogin [durante la creación de la aplicación](#):

| Campo                               | Descripción  |
|-------------------------------------|--|
| Formato de Identificación de Nombre | Establezca este campo a lo que seleccionó para el campo <b>Formato de nombreID SAML de OneLogin</b> <a href="#">durante la configuración de la aplicación</a> .  |
| Algoritmo de Firma de Salida        | Algoritmo utilizado para firmar solicitudes SAML, por defecto <b>sha-256</b> .   |
| Comportamiento de Firma             | Si/cuando las solicitudes SAML serán firmadas. Por defecto, OneLogin no requerirá que las solicitudes estén firmadas.  |
| Algoritmo Mínimo de Firma Entrante  | Establezca este campo a lo que seleccionó para el <b>Algoritmo de Firma SAML</b> <a href="#">durante la configuración de la aplicación</a>   |
| Quiero Firmas en las Afirmaciones   | Marca esta casilla si estableces el <b>elemento de firma SAML</b> en OneLogin a <b>Afirmación</b> o <b>Ambos</b> <a href="#">durante la configuración de la aplicación</a> .   |
| 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 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 OneLogin para recuperar los valores de la aplicación:

| Campo  | Descripción   |
|--|---|
| ID de la entidad                                       | Ingresa su <b>URL del emisor</b> de OneLogin, que se puede obtener de la <a href="#">pantalla de SSO de la aplicación OneLogin</a> . Este campo distingue entre mayúsculas y minúsculas.  |
| Tipo de Encuadernación                                 | Establecer a <b>HTTP Post</b> (como se indica en el Endpoint SAML 2.0 (HTTP)).  |
| URL del Servicio de Inicio de Sesión Único             | Ingresa su <b>Punto final de SAML 2.0 (HTTP) de OneLogin</b> , que se puede obtener de la <a href="#">pantalla de SSO de la aplicación OneLogin</a> .   |
| URL del Servicio de Cierre de Sesión Único             | El inicio de sesión con SSO actualmente <b>no</b> admite SLO. Esta opción está planeada para desarrollo futuro, sin embargo, puedes preconfigurarla si lo deseas.   |
| Certificado Público X509                               | Pega el <a href="#">Certificado X.509 recuperado</a> , eliminando<br>-----INICIO CERTIFICADO-----<br><br>Y<br><br>-----FIN DEL CERTIFICADO-----<br><br>El valor del certificado es sensible a mayúsculas y minúsculas, espacios extra, retornos de carro y otros caracteres extraneous <b>harán que la validación del certificado falle</b> . |
| Algoritmo de Firma de Salida                           | Seleccione el Algoritmo de Firma SAML seleccionado en la sección de configuración de <a href="#">OneLogin SSO</a> .   |
| Deshabilitar Solicitudes de Cierre de Sesión Salientes | El inicio de sesión con SSO actualmente <b>no</b> admite SLO. Esta opción está planeada para un desarrollo futuro.  |
| Quiere Solicitudes de Autenticación Firmadas           | Si OneLogin 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.

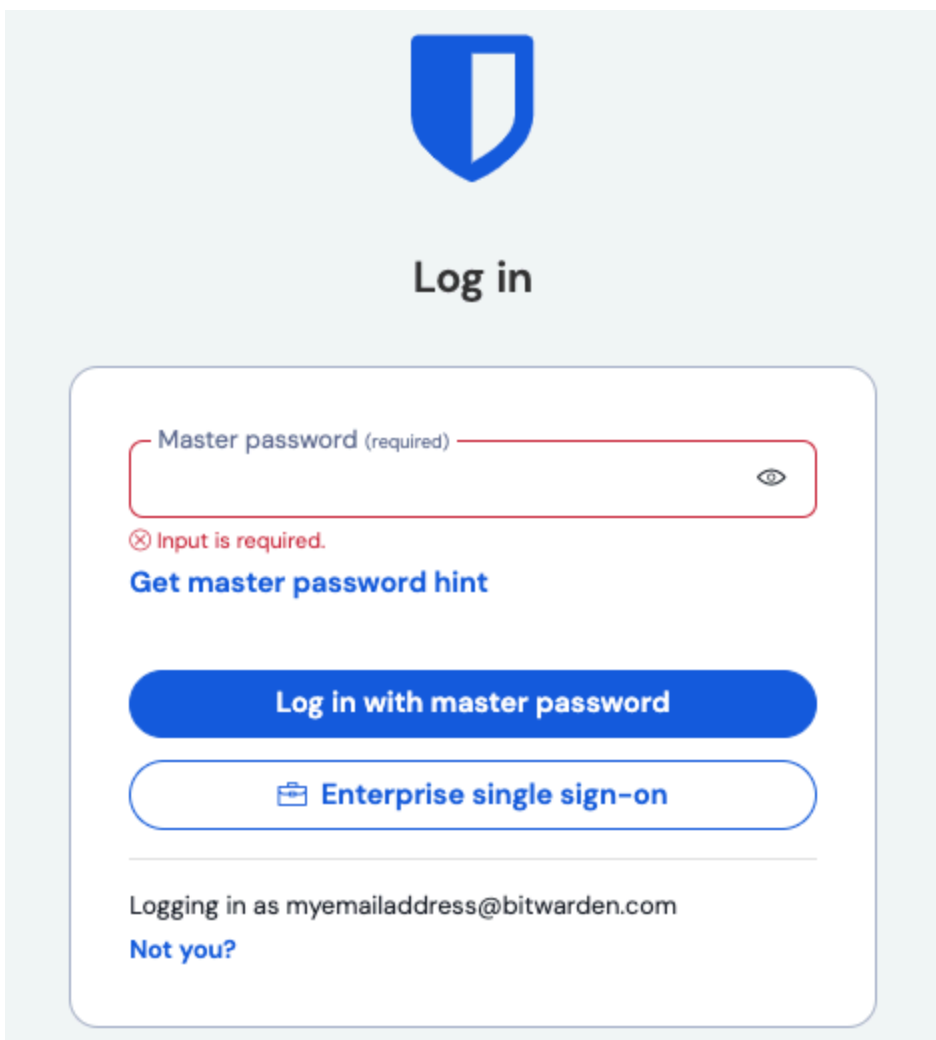
Cuando termines con la configuración del proveedor de identidad, **Guarda** tu trabajo.

**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.](#)

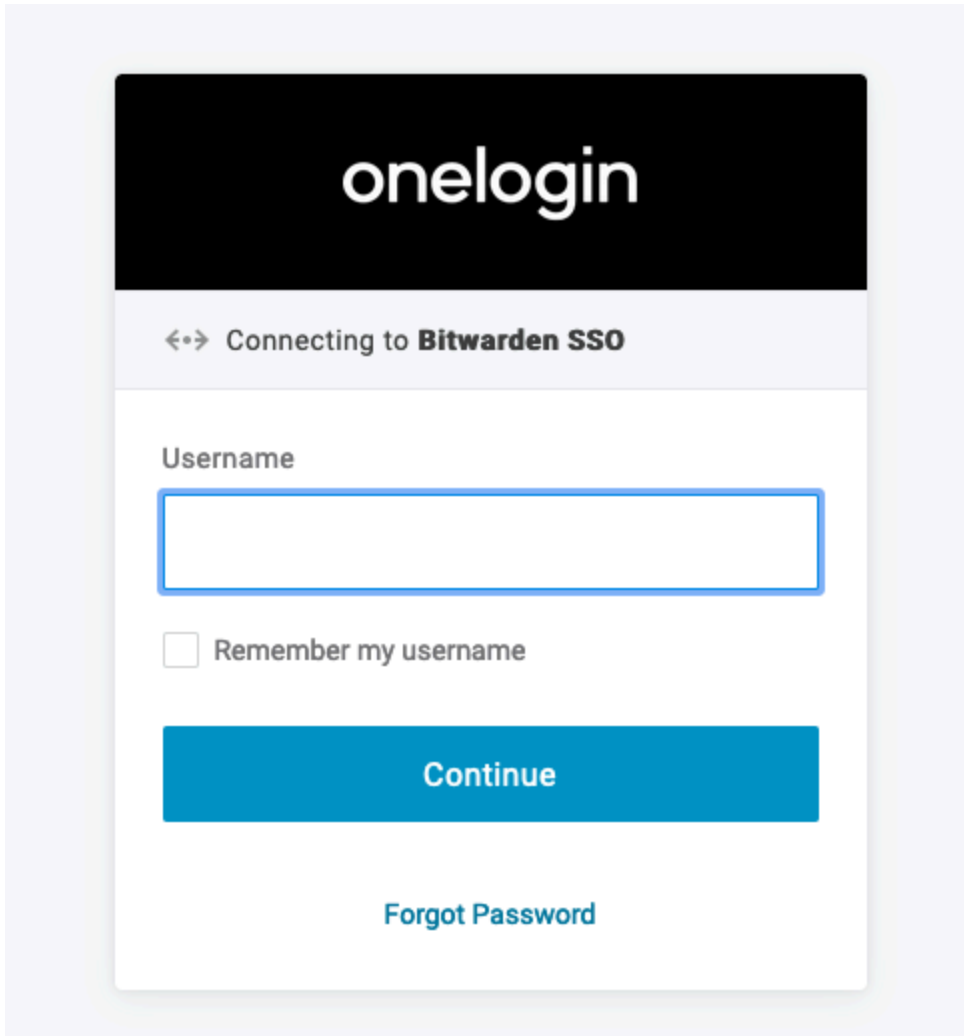
**Prueba la configuración**

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 correctamente, será redirigido a la pantalla de inicio de sesión de OneLogin:



*OneLogin Login*

¡Después de autenticarte con tus credenciales de OneLogin, 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.