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.

Jownload 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 (ﷺ):

Password Manager	All vaults			New 🗸	BW
Vaults			Name	0	
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	:
፰ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	A My Vault	0 6	myusername	Me	:
	 Earns Org : + New organization 		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ⑦ Login □ Card Identity □ Secure note 	0 0	Shared Login sharedusername	My Organiz	÷
 Password Manager Secrets Manager Admin Console 	 ✓ Folders ➢ No folder ✓ Collections ➢ Default colle ➢ Default colle ☑ Trash 				
🖞 Toggle Width					

Selector de producto

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

Secure and trusted open source password manager for business

D bit warden	Single sign-on 🖩 🖬
B My Organization	Use the <u>require single sign-on authentication policy</u> to require all members to log in with SSO.
	Allow SSO authentication
A Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.
뿅 Groups	SSO identifier (required) unique-organization-identifier
⇒ Reporting	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
Billing	Member decryption options
Settings	Master password
Organization info	○ Trusted devices
Policies	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.
Two-step login	C Type
Import data	SAML 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	Generate an identifier that is unique to your organization
SCIM provisioning	
	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.

Crea 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	
Applicati	ions								Add App
Q search co	mpany ap	ops							
No company	apps hav	e been added.							

Add an Application

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



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:

onelogin Users	Applications	Devices	Authentication	Activity	Security	Settings	Developers	
Applications / SAML Test Conne	ector (Adv	anced)	1			M	ore Actions 🔻	Save
Info Configuration Parameters Rules SSO		Applica RelaySta Audience	ation details te e (EntityID)					
Access		Recipien	t					
			App Confi	guration				
Ajuste de Aplicación Audiencia (EntityID)	Descripci Establezc Este valor sesión ún	ón a este car generadc i co de la o	mpo en el ID de 9 automáticame 1 ganización y va	Entidad Sl nte se pue riará segú	9 pre-gene de copiar n su confi _é	erado. desde la p guración.	oantalla de Ajuste	es → Inicio de
Destinatario	Establezc Audiencia	a este car a (ID de En	mpo con el misn I tidad) .	no ID de E i	ntidad SP	ore-genera	ado utilizado para	a el ajuste de
Validador de URL de ACS (Consumidor)	A pesar d informaci (Consumi	e estar ma ón en este dor) .	arcado como Re e campo para int	querido p egrarte co	or OneLog on Bitward	in, en realic en. Salta al	dad no necesitas siguiente campo	ingresar p, URL de ACS
URL (Consumidor) ACS	Establezc Este valor sesión ún	a este car generado i co de la o	mpo en la URL d automáticame rganización y va	el Servicio nte se pue riará segú	o de Consu ede copiar n su config	imo de As o desde la p guración.	erciones (ACS) p pantalla de Ajuste	re-generada. es → Inicio de

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

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	ß
SAML 2.0 Endpoint (HTTP)	
https://mmccabe.onelogin.com/trust/saml2/http-post/sso/95eef6e7-560f-4531-9df3-02e7248415a8	ß

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	Roles			
	Bitwarden SSO Users	✓	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 Formato de nombrelD SAML de OneLogin durante la configuración de la aplicación.
Algoritmo de Firma de Salida	Algoritmo utilizado para firmar solicitudes SAML, por defecto <mark>sha - 256</mark> .
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 Algoritmo de Firma SAML durante la configuración de la aplicación
Quiero Firmas en las Afirmaciones	Marca esta casilla si estableces el elemento de firma SAML en OneLogin a Afirmación o Ambos durante la configuración de la aplicación.
Validar Certificados	Marque esta casilla cuando utilice certificados confiables y válidos de su ldP 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	Ingrese su URL del emisor de OneLogin, que se puede obtener de la pantalla de SSO de la aplicación OneLogin. Este campo distingue entre mayúsculas y minúsculas.
Tipo de Encuadernación	Establecer a HTTP Post (como se indica en el Endpoint SAML 2.0 (HTTP)).
URL del Servicio de Inicio de Sesión Único	Ingrese su Punto final de SAML 2.0 (HTTP) de OneLogin , que se puede obtener de la pantalla de SSO de la aplicación OneLogin.
URL del Servicio de Cierre de Sesión Único	El inicio de 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 X.509 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	Seleccione el Algoritmo de Firma SAML seleccionado en la sección de configuración de OneLogin SSO.
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 OneLogin espera que las solicitudes SAML estén firmadas.

(i) 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**:

Log in to Bitwarden
Email address (required) Remember email
Continue
or
& Log in with passkey
🖻 Use single sign-on
New to Bitwarden? Create account

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	
<∘> Co	nnecting to Bitwarden SSO	
Usernar	ne	
Rem	ember my username	
	Continue	
	Forgot Password	

OneLogin Login

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

(i) 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.