

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML en AuthO

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

Implementación de SAML en AuthO

Este artículo contiene ayuda **específica de AuthO** 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 AuthO. 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 conmutador de producto (ﷺ):

Password Manager	All vaults			New >>	BW
🗇 Vaults			Nores	0	
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	:
æ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	My Vault	0 6	myusername	Me	:
	/ Teams Org : + New organization		Secure Note	Me	:
	 ✓ All items ☆ Favorites ④ Login □ Card Identity □ Secure note 		Shared Login sharedusername	My Organiz	:
Password Manager	 ✓ Folders ➡ No folder >✓ Collections 				
🗔 Secrets Manager	Default colle				
Admin Console	🔟 Trash				
🍈 Toggle Width					
		Coloctordo	a raduata		

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 🖩 🗐
🗐 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)
₽ 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 Policies	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.
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 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 AuthO

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

\mathbf{Q}	dev-hn11g2a6 Development Q Discuss your needs Docs Q	
4 ∼	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.	
\$		2
6	Applications	
i: n	Setup a mobile, web or IoT application to use Auth0 for Authentication. Learn more	/
2		
)		
0	Generic Client ID: RM3UeXnRtL8CSjPPCg7HiitjInvQs0Be	
ល		-
	AuthO 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:



U bitwarden

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):

Application Metadata	Device Settings	OAuth	Grant Types	WS-Federation	Certificates
Grants					
	Authorization Cod	de 🔽	Refresh Token	Client Creder	ntials
Password		Passwordle	ss 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.

Application Metadata	Device Settings	OAuth	Grant Types	WS-Federation	Certificates
Signing Certificate					
					_
BEGIN CERT	IFICATE	(aNA0000a	COTHODOEDO		C)
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldilobiF	IFICATE BAgIJdp2+Lsu8Iył x7zJhNi51cy5hdXF	CCMA0GCSq RoMC5ib20	GSIb3DQEBCwU	AMCQxIjAgBgNV 1MTUxMiUxWhcN	C)
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU	IFICATE BAgIJdp2+Lsu8Iyk xZzJhNi51cy5hdXk xWjAkMSIwIAYDVQ0	<pre>(cMA0GCSq RoMC5jb20 QDEx1kZXY</pre>	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu	Ċ
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU Y29tMIIBIjANBgk	IFICATE BAgIJdp2+Lsu8Iył xZzJhNi51cy5hdXf xWjAkMSIwIAYDVQ0 qhkiG9w0BAQEFAA0	KcMA0GCSq RoMC5jb20 QDExlkZXY OCAQ8AMII	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY BCgKCAQEA2yR	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu fsSC5LCYkTvuF	Ċ
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU Y29tMIIBIjANBgk nCW0wCEE7jkTtdx	IFICATE BAgIJdp2+Lsu8Iyk xZzJhNi51cy5hdXF xWjAkMSIwIAYDVQ0 qhkiG9w0BAQEFAA0 RGytTBwJEarqzmgM	(cMA0GCSq RoMC5jb20 QDEx1kZXY DCAQ8AMII 4ZktBmkU0	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY BCgKCAQEA2yR BfuzjrtcaQx0	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu fsSC5LCYkTvuF utRM679AD0PX9	Ċ
BEGIN CERT MIIDDTCCAfWgAwI BAMTGWRldi1objE MzQxMjIzMTUxMjU Y29tMIIBIjANBgko nCW0wCEE7jkTtdx WZLqwiCErdeKP01	IFICATE BAgIJdp2+Lsu8Iył xZzJhNi51cy5hdXf xWjAkMSIwIAYDVQ0 qhkiG9w0BAQEFAA0 RGytTBwJEarqzmgł S3/TvqkNkPyf2UE2	KcMA0GCSq RoMC5jb20 QDExlkZXY OCAQ8AMII MZktBmkU0 27Qo4giJy	GSIb3DQEBCwU wHhcNMjEwNDE taG4xMWcyYTY BCgKCAQEA2yR BfuzjrtcaQx0 6FEUAgsqwTs/	AMCQxIjAgBgNV 1MTUxMjUxWhcN udXMuYXV0aDAu fsSC5LCYkTvuF utRM679AD0PX9 gtX6sxIogeH0N	Ċ

AuthO 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 (\rightarrow).

tadata	Device Settings	OAuth	Grant Types	WS-Federation	Certificates	Endpoints
DAuth						
Auth A	uthorization URL					

AuthO Endpoints

Configura las reglas de AuthO

Crea reglas para personalizar el comportamiento de la respuesta SAML de tu aplicación. Mientras que AuthO 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:

Secure and trusted open source password manager for business

\$	dev-hn11g2a6 Development Q Discuss your needs ID Docs C IS
4> ∼ ⊗	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.
》 [] የ ት	Rules Custom Javascript snippets that run in a secure, isolated sandbox in the Auth0 service as part of your authentication pipeline. Learn more ►
ଠ ନ୍ୟ X	Custom SAML Config
- 00 	AuthO Rules

Puede configurar cualquiera de los siguientes:

Clave	Descripción
algoritmoDeFir ma	Algoritmo que AuthO utilizará para firmar la afirmación o respuesta SAML. Por defecto, se incluirá rsa-sha 1, 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.
algoritmoDiges tión	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 f irma	Por defecto, AuthO solo firmará la afirmación SAML. Establezca esto en verdadero para firmar la respuesta SAML en lugar de la afirmación.

Clave	Descripción
formatoDeIdent	Por defecto, <mark>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</mark> . Puedes establecer este
ificadorDeNomb	valor a cualquier formato de NamelD SAML. Si lo haces, cambia el campo SP Formato de ID de Nombre a
re	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 AuthO.

Bash
function (user, context, callback) {
context.samlConfiguration.signatureAlgorithm = "rsa-sha256";
<pre>context.samlConfiguration.digestAlgorithm = "sha256";</pre>
<pre>context.samlConfiguration.signResponse = "true";</pre>
<pre>context.samlConfiguration.nameIdentifierFormat = "urn:oasis:names:tc:SAML:1.1:nameid-format:ema</pre>
ilAddress"
<pre>context.samlConfiguration.binding = "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect";</pre>
callback(null, user, context);

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal AuthO. 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 NamelD 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 <mark>rsa-sha256</mark> .
Comportamiento de Firma	Si/cuando las solicitudes SAML de Bitwarden serán firmadas. Por defecto, AuthO 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, AuthO firmará con <mark>rsa-sha1</mark> . Seleccione <mark>rsa-sha256</mark> 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, AuthO 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 AuthO para recuperar los valores de la aplicación:

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

Secure and trusted open source password manager for business

Campo	Descripción
URL del Servicio de Inicio de Sesión Único	Ingrese la URL del Protocolo SAML (vea Puntos finales) de su aplicación AuthO. Por ejemplo, https://bw-help.us.auth0.com/samlp/HcpxD63h7Qzl420u8qachPWoZEG0H ho2.
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, AuthO 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 AuthO 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**:



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 AuthO:



AuthO Login

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