CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SSO de Confianza Cero de Cloudflare

Ver en el centro de ayuda: https://bitwarden.com/help/cloudflare-zero-trust-sso-implementation/

Implementación de SSO de Confianza Cero de Cloudflare

Este artículo contiene ayuda específica de **Cloudflare Zero Trust** para configurar el inicio de sesión con SSO. Cloudflare Zero Trust es una plataforma de gestión de identidad y acceso basada en la nube que puede integrarse con múltiples proveedores de Identidad (IdPs). También puedes configurar pasarelas y túneles para un acceso seguro a la plataforma.

(i) Note

Cloudflare Zero Trust can be configured with any IdP that operates using SAML 2.0 or OIDC SSO configurations. If you are not familiar with these configurations, refer to these articles:

- SAML 2.0 Configuration
- OIDC Configuration

¿Por qué usar Cloudflare Zero Trust con SSO?

Cloudflare Zero Trust es una plataforma de gestión de identidad y acceso basada en la nube que puede integrarse con múltiples proveedores de Identidad (IdPs). La ventaja de usar Cloudflare Zero Trust además de su IdP estándar es su capacidad para configurar múltiples IdPs para el inicio de sesión. Cloudflare Zero Trust puede proporcionar acceso SSO a Bitwarden desde varias organizaciones separadas, o conjuntos de usuarios dentro de una organización.

Abre SSO en la aplicación web

(i) Note

Cloudflare will only support SAML via the Access Application Gateway. This means that the **SAML 2.0** must be selected in the Bitwarden configuration. OIDC authentication can still be configured from the IdP and Cloudflare.

Inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el conmutador de producto (2000):

D Password Manager	All vaults			New 💛	BW
🗇 Vaults	FILTERS		Nome	Owner	
🖉 Send			Name	Owner	:
$ m \ll$ Tools \sim	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	÷
≅ Reports	 ✓ All vaults ○ More with 		Personal Login		
🕸 Settings 🛛 🗸 🗸	My Vault	0 6	myusername	Ме	:
	giiii Teams Org : ┼ New organization		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ③ Login □ Card □ Identity □ Secure note 		Shared Login sharedusername	My Organiz	÷
Password Manager Secrets Manager	 Folders No folder Collections Befault colle 				
all Admin Console	🔟 Trash				
toggie width					

Selector de producto

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

D bit warden	Single sign-on III III III III IIII IIII IIII IIII
My Organization	✓ Use the <u>require single sign-on authentication policy</u> to require all members to log in with SSO.
	Allow SSO authentication
△ Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.
绺 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 SP entity ID
SCIM provisioning	i a come a come in come confectivity i the first side of the second
	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 un método de inicio de sesión de confianza cero de Cloudflare

Para crear un método de inicio de sesión de Cloudfare Zero Trust:

1. Navega a Cloudflare Zero Trust e inicia sesión o crea una cuenta.

2. Configura un dominio, que actuará como la URL utilizada por tus usuarios para acceder a tus aplicaciones o App Launcher, por ejemplo https://my-business.cloudflareaccess.com/. Desde el menú de Cloudflare Zero Trust, selecciona Ajustes → General → Dominio de Equipos:

CLC				Support 🔻
~			← Back to Settings	
	Zero Trust overview		Custom Pages	
G	Analytics New			
Ð	Gateway	•	Team domain This is where the App Launcher lives, and where users make access requests to applications behind Access.	
۲	Access	•		
R	Networks New	•	Edit	
328	My team	-		
Ξ	Logs	•	Block page Customize the page users see when they reach a website blocked by Gateway. Note: Devices must have the Cloudflare Customize	
9	CASB	•	certificate or a custom root CA installed.	
R	DLP	•	Use the customized block page over Cloudflare's default.	•
æ	DEX	•		
4	Email Security New	-	Login page Users will see this page when they reach an application behind Access. Customize	
۲	Settings			

Team domain setting

- 3. Comienza a configurar el primer método de inicio de sesión navegando a Ajustes → Autenticación → Agregar nuevo.
- 4. Seleccione el método de inicio de sesión para conectarse a Cloudflare Zero Trust. Si el IdP que estás utilizando no está presente en la lista de IdP, utiliza las opciones genéricas de SAML o OIDC. En este artículo, Okta se utilizará como ejemplo:

💠 Cloudflare Zer	o Trust	Add a login method	
Home			
パ Analytics	•	Select an identity provider	
- Gateway	•	Azure AD	ගි Centrify
⊸ Access	•	f Facebook	G GitHub
🕮 My Team	•		
🗏 Logs	•	G Google Workspace	G Google
Settings		in LinkedIn	O Okta
		OneLogin	One-time PIN ADDED
		d OpenID Connect	🖒 SAML
•		Я Yandex	

Cloudflare Zero Trust IdP list

5. Después de seleccionar su método de inicio de sesión IdP elegido, siga la guía del producto proporcionada por Cloudflare para integrar su IdP.

(i) Note

If the IdP you are using has a **support groups** feature, this option must be **disabled**. Bitwarden does not support group based claims, enabling this option will result in an XML element error on the Bitwarden end.

Crea una aplicación de Confianza Cero de Cloudflare

Después de que se haya configurado un IdP, tendrás que crear una aplicación de Confianza Cero de Cloudflare para Bitwarden. **En este** ejemplo crearemos una aplicación SAML :

1. Navega a Acceso \rightarrow Aplicaciones \rightarrow Agregar una aplicación.





÷		•	← Back to Applications			
	Zero Trust overview		Add an application			
G	Analytics	-	Configure the policies, authentication	, and settings of your applications.		
Ð	Gateway	•	Select type > Configure application	ion > Add policies > Setup		
* (Access Applications Access Groups	*	What type of application do y To protect a self-hosted application, a	ou want to add? add your first domain to Cloudflare.		
	Service Auth					
	Tags					
ы М	Networks New	•		白	白	\$
Å	DEX	•		Ŧ	Ŧ	
<u>18</u> 1	My Team	-	Self-hosted	SaaS	Private network	Bookmark
Ξ	Logs	-	Applications you host in your infrastructure that use	Applications you do not host. Additional setup is required	Resources you host in your infrastructure that cannot use	If you have apps that cannot be put behind Access, we provide a
۲	Settings		Cloudflare's authoritative DNS.	outside of Cloudflare Zero Trust.	public DNS records.	shortcut on our App Launcher
			Select	Select	Select	Select
«	Collapse sidebar					

CFZT add an application

2. Seleccione el tipo **SaaS**.

3. En la caja fuerte web de Bitwarden, abre tu organización y navega a la pantalla de **Ajustes** → **Inicio de Sesión Único**. Utilice la información de la caja fuerte web para completar la información en la pantalla **Configurar aplicación**:

Clave	Descripción
Aplicación	Ingrese Bitwarden.
ID de la entidad	Copia el ID de entidad SP de la página de Bitwarden Single Sign-On en este campo.
URL del Servicio de Consumo de Afirmaciones	Copia la URL del servicio de consumo de aserciones (ACS) de la página de inicio de sesión única de Bitwarden en este campo.
Formato de Identificación de Nombre	Seleccione Correo electrónico del menú desplegable.

(i) Note

For the generic OIDC configuration, the Auth URL, Token URL, and Certificate URL can be located with the well-known URL.

4. Desplázate hacia abajo hasta el menú de **Proveedores de Identidad**. Seleccione el o los IdP(s) que configuró en la sección anterior, desplácese de nuevo al principio y seleccione **Siguiente**.

5. A continuación, crea políticas de acceso para el acceso de los usuarios a la aplicación. Complete los campos de **Nombre de la política**, **Acción** y **Duración de la sesión** para cada política.

6. Puede elegir asignar una política de grupo (**Acceso** → **Grupos**) o reglas explícitas de políticas de usuario (como correos electrónicos, "correos electrónicos que terminan en", "país" o "todos"). En el siguiente ejemplo, el grupo "Anon Users" ha sido incluido en la política. Se ha agregado una regla adicional para incluir correos electrónicos que terminen en el dominio elegido:

💠 Cloudflare Zerc	Trust	Assign a group
Home		Assign a group to your application to enrorce a set of predenined rules.
ン Analytics	•	Search for an Access Group
⊕ Gateway	•	Name Rule type
- Access	•	> S Anon users • DEFAULT
Applications		
Access Groups		Create additional rules
Service Auth	- 1	If you're assigning one or more groups to this application, any rules you create now will be applied in addition to group rules.
Tunnels		Include
ाहे My Team	-	Selector Value
🗏 Logs	-	Emails ending in
Settings		
-		+ Add include + Add require + Add exclude
		CFZT app policy

(i) Note

You can also apply user access through the **App Launcher** for access to the Bitwarden login with SSO shortcut. This can be managed by navigating to **Authentication** \rightarrow **App Launcher** \rightarrow **Manage**. The application policies in the above example can be duplicated or generated here.

7. Una vez que se hayan configurado las políticas de acceso, desplácese hasta la parte superior y seleccione Siguiente.

8. Mientras estás en la pantalla de **Configuración**, copia los siguientes valores e ingrésalos en sus respectivos campos en la página de **Inicio de Sesión Único** de Bitwarden:

Clave	Descripción
Punto final de SSO	El punto final de SSO dirige a dónde su aplicación SaaS enviará las solicitudes de inicio de sesión. Este valor se ingresará en el campo URL del Servicio de Inicio de Sesión Único en Bitwarden.
Acceder a la entidad ID o emisor	La ID de Entidad de Acceso o Emisor es el identificador único de su aplicación SaaS. Este valor se ingresará en el campo ID de Entidad en Bitwarden.
Clave pública	La clave pública es el certificado de acceso público que se utilizará para verificar tu identidad. Este valor se ingresará en el campo Certificado Público X509 en Bitwarden.

9. Después de que los valores hayan sido ingresados en Bitwarden, selecciona **Guardar** en la pantalla de Inicio de Sesión Único de Bitwarden y selecciona **Hecho** en la página de Cloudflare para guardar la aplicación.

10. Para crear un marcador para la pantalla de inicio de sesión de Bitwarden con SSO, selecciona **Agregar una aplicación** \rightarrow **Marcador**. Verifica que el Marcador sea visible en el **Lanzador de Aplicaciones**.

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 de **Inicio de sesión único de la Empresa**.



	Log in	
- Maste	r password (required)	•
⊗ Input is Get ma	required. ster password hint	
	Log in with master password	
	🖻 Enterprise single sign-on	
Logging i Not you?	n as myemailaddress@bitwarden.com	

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 una pantalla de Cloudflare Access, donde puede seleccionar el IdP para iniciar sesión con:



Después de seleccionar tu IdP, serás dirigido a la página de inicio de sesión de tu IdP. Ingrese la información utilizada para el inicio de sesión a través de su IdP:

okta
Sign In
Username
Keep me signed in
Next
Help

CFZT IdP login

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