ADMINISTRATOR KONSOLE > MELDEN SIE SICH MIT SSO AN >

Cloudflare Zero Trust SSO-Implementierung

Ansicht im Hilfezentrum: https://bitwarden.com/help/cloudflare-zero-trust-sso-implementation/

Cloudflare Zero Trust SSO-Implementierung

Dieser Artikel enthält **Cloudflare Zero Trust-spezifische** Hilfe zur Konfiguration der Zugangsdaten mit SSO. Cloudflare Zero Trust ist eine cloudbasierte Identitäts- und Zugriffsverwaltungsplattform, die sich mit mehreren Identitätsanbietern (IdPs) integrieren kann. Sie können auch Gateways und Tunneling für den sicheren Zugang zur Plattform konfigurieren.

(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

Warum sollte man Cloudflare Zero Trust mit SSO verwenden?

Cloudflare Zero Trust ist eine cloud-basierte Proxy-Identitäts- und Zugriffsverwaltungsplattform, die sich mit mehreren Identitätsanbietern (IdPs) integrieren kann. Der Vorteil der Verwendung von Cloudflare Zero Trust zusätzlich zu Ihrem Standard-IdP besteht in seiner Fähigkeit, mehrere IdPs für die Zugangsdaten zu konfigurieren. Cloudflare Zero Trust kann SSO-Zugriff auf Bitwarden von mehreren getrennten Organisationen oder Benutzergruppen innerhalb einer Organisation bereitstellen.

Öffnen Sie SSO in der Web-App

(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.

Melden Sie sich bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktumschalter (58):

Password Manager	All vaults			New ~	BW
🗇 Vaults	FILTERS		Nama	Owner	:
🖉 Send			Name	Owner	•
\sim Tools \sim	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	:
æ Reports	✓ All vaults		Demonal Login		
🕸 Settings 🛛 🗸 🗸	B My Vault B My Organiz : B Toomo Org		myusername	Me	:
	+ New organization		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ③ Login □ Card □ Identity □ Secure note 		Shared Login sharedusername	My Organiz	÷
 Password Manager Secrets Manager Admin Operation 	 Folders No folder Collections Default colle 				
a Admin Console ∰ Toggle Width	前 Trash	Produktw	rechsler		

Öffnen Sie den **Einstellungen** → **Einmaliges Anmelden** Bildschirm Ihrer Organisation:

D bit warden	Single sign-on III III III III III III III IIII II
🖉 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.
磐 Groups	unique-organization-identifier
	 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	SAML 2.0
Import data	
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	C SP entity ID
SCIM provisioning	i a como a como de como contractiva e d'Arche e las calculas
	SAML 2.0 metadata URL

SAML 2.0 Konfiguration

Wenn Sie es noch nicht getan haben, erstellen Sie einen einzigartigen **SSO-Identifikator** für Ihre Organisation und wählen Sie **SAML** aus dem **Typ**-Dropdown aus. Lassen Sie diesen Bildschirm geöffnet, um leicht darauf zugreifen zu können.

Sie können die Option Legen Sie eine eindeutige SP-Entitäts-ID fest in diesem Stadium ausschalten, wenn Sie möchten. Wenn Sie dies tun, wird Ihre Organisations-ID aus Ihrem SP-Entity-ID-Wert entfernt. In fast allen Fällen wird jedoch empfohlen, diese Option aktiviert zu lassen.

⊘ Tip

Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit SSO auf vertrauenswürdigen Geräten oder mit Key Connector beginnen können.

Erstellen Sie eine Cloudflare Zero Trust Zugangsdaten Methode

Um eine Cloufdlare Zero Trust Zugangsdaten Methode zu erstellen:

1. Navigieren Sie zu Cloudflare Zero Trust und melden Sie sich an oder erstellen Sie ein Konto.

2. Konfigurieren Sie eine Domain, die als URL verwendet wird, auf die Ihre Benutzer zugreifen, um Ihre Anwendungen oder App Launcher zu nutzen, zum Beispiel https://my-business.cloudflareaccess.com/. Aus dem Cloudflare Zero Trust-Menü wählen Sie Einstellungen → Allgemein → Team-Domain:

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.	
÷	Access	-		
R	Networks New	-	Edit	
3 ⁰ 8	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. Beginnen Sie mit der Konfiguration der ersten Zugangsdaten-Methode, indem Sie zu **Einstellungen** → **Authentifizierung** → **Neu hinzufügen.** navigieren.
- 4. Wählen Sie die Zugangsdaten Methode aus, um sich mit Cloudflare Zero Trust zu verbinden. Wenn der IdP, den Sie verwenden, nicht in der IdP-Liste vorhanden ist, verwenden Sie die allgemeinen Optionen SAML oder OIDC. In diesem Artikel wird Okta als Beispiel verwendet:

🛟 Cloudflare Zero Trust	Add a login method		
Home			
Analytics 👻	Select an identity provider		
음 Gateway 🔻	Azure AD	ග Centrify	
⊸ Access 🔻	f Facebook	GitHub	
📽 My Team 🔻			
🗉 Logs 🛛 👻	G Google Workspace	G Google	
Settings	in LinkedIn	O Okta	
	OneLogin	G One-time PIN	ADDED
		🖒 SAML	
• · · ·	Я Yandex		

Cloudflare Zero Trust IdP list

5. Nachdem Sie Ihre gewählte IdP-Zugangsdaten-Methode ausgewählt haben, folgen Sie der von Cloudflare bereitgestellten Anleitung im Produkt zur Integration Ihres 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.

Erstellen Sie eine Cloudflare Zero Trust-Anwendung

Nachdem ein IdP konfiguriert wurde, müssen Sie eine Cloudflare Zero Trust-Anwendung für Bitwarden erstellen. In diesem Beispiel erstellen wir eine SAML-Anwendung :

1. Navigieren Sie zu **Zugang** → **Anwendungen** → **Eine Anwendung hinzufügen**.





÷		•	← 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	rou want to add? add your first domain to Cloudflare.		
	Service Auth					
	Tags					
ы М	Networks New	•		白	合	☆
ቆ	DEX	•		Ŧ	Ŧ	
<u>194</u>	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
\$	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. Wählen Sie den Typ **SaaS**.

3. Im Bitwarden Web-Tresor öffnen Sie Ihre Organisation und navigieren zu den **Einstellungen** → **Single Sign-On** Bildschirm. Verwenden Sie Informationen aus dem Web-Tresor, um Informationen auf dem **App konfigurieren**-Bildschirm auszufüllen:

Schlüssel	Beschreibung
Anwendung	Geben Sie <mark>Bitwarden</mark> ein.
Entitäts-ID	Kopieren Sie die SP-Entitäts-ID von der Bitwarden Single Sign-On-Seite in dieses Feld.
Assertion Consumer Service URL	Kopieren Sie die Assertion Consumer Service (ACS) URL von der Bitwarden Single Sign-On Seite in dieses Feld.
Namens-ID-Format	Wählen Sie E-Mail-Adresse aus dem Dropdown-Menü.

(i) Note

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

4. Scrollen Sie herunter zum Menü **Identitätsanbieter**. Wählen Sie die IdP(s), die Sie im vorherigen Abschnitt konfiguriert haben, scrollen Sie zurück nach oben und wählen Sie **Weiter.**

5. Erstellen Sie als nächstes Zugriffsrichtlinien für den Benutzerzugriff auf die Anwendung. Füllen Sie die Felder **Richtlinienname**, **Aktion** und **Sitzungsdauer** für jede Richtlinie aus.

6. Sie können wählen, eine Gruppenrichtlinie zuzuweisen (**Zugriff** → **Gruppen**) oder explizite Benutzerrichtlinienregeln (wie E-Mail-Adressen, "E-Mail-Adressen enden mit", "Land" oder "jeder"). Im folgenden Beispiel wurde die Gruppe "Anon Users" in die Richtlinien aufgenommen. Eine zusätzliche Regel wurde ebenfalls hinzugefügt, um E-Mails einzuschließen, die in der ausgewählten Domain enden:

💠 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. Sobald die Zugriffsrichtlinien konfiguriert wurden, scrollen Sie nach oben und wählen Sie Weiter.

8. Während Sie sich auf dem **Einrichtungs** Bildschirm befinden, kopieren Sie die folgenden Werte und geben Sie sie in die entsprechenden Felder auf der Bitwarden **Single Sign-On** Seite ein:

Schlüssel	Beschreibung
SSO-Endpunkt	Der SSO-Endpunkt gibt an, wohin Ihre SaaS-Anwendung Zugangsdaten Anfragen senden wird. Dieser Wert wird in das Feld Single Sign On Service URL in Bitwarden eingegeben.
Zugriff auf Entitäts-ID oder Aussteller	Die Zugriffs-Entitäts-ID oder der Aussteller ist die eindeutige Kennung Ihrer SaaS- Anwendung. Dieser Wert wird in das Feld Entity ID auf Bitwarden eingegeben.
Öffentlicher Schlüssel	Der öffentliche Schlüssel ist das öffentliche Zugriffszertifikat, das verwendet wird, um Ihre Identität zu überprüfen. Dieser Wert wird in das Feld X509 Öffentliches Zertifikat bei Bitwarden eingegeben.

9. Nachdem die Werte in Bitwarden eingegeben wurden, wählen Sie **Speichern** auf dem Bitwarden Single Sign-On Bildschirm und wählen Sie **Fertig** auf der Cloudflare-Seite, um die Anwendung zu speichern.

10. Um ein Lesezeichen für den Bitwarden Zugangsdaten mit SSO-Bildschirm zu erstellen, wählen Sie **Eine Anwendung hinzufügen** → **Lesezeichen**. Überprüfen Sie, ob das Lesezeichen im **App-Starter** sichtbar ist.

Testen Sie die Konfiguration

Sobald Ihre Konfiguration abgeschlossen ist, testen Sie diese, indem Sie zu https://vault.bitwarden.com navigieren, Ihre E-Mail-Adresse eingeben, Weiter auswählen und die Schaltfläche Enterprise Single Sign-On auswählen.



	Log in	
- Master	r password (required)	
	required	
⊗ Input is Get ma:	ster password hint	
8 Input is Get ma	ster password hint Log in with master password	
S Input is Get mas	ster password hint Log in with master password Enterprise single sign-on	

Unternehmens Single Sign On und Master-Passwort

Geben Sie den konfigurierten Organisationsbezeichner ein und wählen Sie **Anmelden**. Wenn Ihre Implementierung erfolgreich konfiguriert ist, werden Sie zu einem Cloudflare Access-Bildschirm weitergeleitet, auf dem Sie den IdP auswählen können, mit dem Sie sich mit Ihren Zugangsdaten anmelden können:



Nach der Auswahl Ihres IdP werden Sie zur Zugangsdaten-Seite Ihres IdP weitergeleitet. Geben Sie die Informationen ein, die verwendet werden, um sich über Ihren IdP anzumelden:

okta	
Sign In	
Username	
Keep me signed in	
Next	
Help	

CFZT IdP login

Nachdem Sie sich mit Ihren IdP-Anmeldeinformationen authentifiziert haben, geben Sie Ihr Bitwarden Master-Passwort ein, um Ihren Tresor zu entschlüsseln!