CONSOLE ADMIN > IDENTIFIEZ-VOUS AVEC SSO >

Mise en œuvre du SSO Zero Trust de Cloudflare

Afficher dans le centre d'aide: https://bitwarden.com/help/cloudflare-zero-trust-sso-implementation/

Mise en œuvre du SSO Zero Trust de Cloudflare

Cet article contient de l'aide spécifique à **Cloudflare Zero Trust** pour configurer l'identifiant avec SSO. Cloudflare Zero Trust est une plateforme de gestion d'identité et d'accès basée sur le cloud qui peut s'intégrer à plusieurs fournisseurs d'identité (IdPs). Vous pouvez également configurer des passerelles et du tunneling pour un accès sécurisé à la plateforme.

(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

Pourquoi utiliser Cloudflare Zero Trust avec SSO?

Cloudflare Zero Trust est une plateforme de gestion d'identité et d'accès proxy basée sur le cloud qui peut s'intégrer à plusieurs fournisseurs d'identité (IdPs). L'avantage d'utiliser Cloudflare Zero Trust en plus de votre IdP standard est sa capacité à configurer plusieurs IdP pour l'identifiant. Cloudflare Zero Trust peut fournir un accès SSO à Bitwarden depuis plusieurs organisations distinctes, ou ensembles d'utilisateurs au sein d'une organisation.

Ouvrez SSO dans l'application 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.

Connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit (ﷺ):

D Password Manager	All vaults			New ~	BW
🗇 Vaults			Nome	Owner	
🖉 Send			Name	Owner	•
$ m \ll$ Tools $~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	÷
≅ Reports	✓ All vaults		Personal Login		
Settings	My Vault	0 3	myusername	Me	:
	 ℬ Teams Org : + New organization 		Secure Note	Me	:
	 ✓ All items ☆ Favorites ⑦ Login □ Card Identity □ Secure note 	0 Ø	Shared Login sharedusername	My Organiz	÷
 Password Manager Secrets Manager Admin Console Toggle Width 	 ✓ Folders ➢ No folder ✓ Collections ➢ Default colle ➢ Default colle ☆ Trash 				

commutateur-de-produit

Ouvrez l'écran **Paramètres** \rightarrow **Connexion unique** de votre organisation :

D bit warden	Single sign-on III III III III III III III III III I
🕮 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	unique-organization-identifier
➡ Reporting	 Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
St Billing	Member decryption options
Settings	Master password
Organization info	Trusted devices Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, and policy trademark required policy with automatic application will turn on when this option is used.
Policies	account recovery auministration policy with accomatic emoliment will turn on when this option is used.
Two-step login	Type
Import data	SAIML 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	SP entity ID
SCIM provisioning	i a com a comunicación de la comunicación d
	SAML 2.0 metadata URL

Configuration SAML 2.0

Si vous ne l'avez pas déjà fait, créez un **identifiant SSO** unique pour votre organisation et sélectionnez **SAML** dans le menu déroulant **Saisir** . Gardez cet écran ouvert pour une référence facile.

Vous pouvez désactiver l'option **Définir un ID d'entité SP unique** à ce stade si vous le souhaitez. En faisant cela, votre ID d'organisation sera supprimé de la valeur de votre ID d'entité SP, cependant dans presque tous les cas, il est recommandé de laisser cette option activée.

∏ Tip

Il existe des options alternatives de **décryptage des membres**. Apprenez comment commencer à utiliser SSO avec des appareils de confiance ou Key Connector.

Créez une méthode d'identifiant Zero Trust de Cloudflare

Pour créer une méthode d'identifiant Zero Trust Cloufdlare :

1. Naviguez vers Cloudflare Zero Trust et connectez-vous ou créez un compte.

 Configurez un domaine, qui servira d'URL utilisée par vos utilisateurs pour accéder à vos applications ou à votre Lanceur d'Applications, par exemple https://my-business.cloudflareaccess.com/. Dans le menu Cloudflare Zero Trust, sélectionnez Paramètres → Général → Domaine d'équipe:

CLO		St	upport 🔻
÷		← Back to Settings	
	Zero Trust overview	Custom Pages	
G	Analytics New		
Ð	Gateway	Team domain This is where the Ann Launcher lives, and where users make access requests to applications behind Access	
÷	Access		
×	Networks New	- Edit	
8 ⁹ 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	•	
Ŵ	Email Security New	Users will see this page when they reach an application behind Access.	
\$	Settings		

Team domain setting

3. Commencez à configurer la première méthode d'identifiant en naviguant vers **Paramètres** → **Authentification** → **Ajouter nouveau.**

4. Sélectionnez la méthode d'identifiant pour vous connecter à Cloudflare Zero Trust. Si l'IdP que vous utilisez n'est pas présent sur la liste des IdP, utilisez les options génériques SAML ou OIDC. Dans cet article, Okta sera utilisé comme exemple :

🛟 Cloudflare Zero Trust	Add a login method	
Home		
Analytics ▼	Select an identity provider	
	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
		SAML
•	Я Yandex	

Cloudflare Zero Trust IdP list

5. Après avoir sélectionné votre méthode d'identifiant IdP choisie, suivez le guide produit fourni par Cloudflare pour intégrer votre 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.

Créez une application Cloudflare Zero Trust

Après avoir configuré un IdP, vous devrez créer une application Cloudflare Zero Trust pour Bitwarden. Dans cet exemple, nous allons créer une application SAML:

1. Naviguez vers Accès → Applications → Ajouter une application.





÷		•	+ 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 applicati	on > Add policies > Setup		
*) (Access Applications Access Groups	*	What type of application do y To protect a self-hosted application, a	ou want to add? Idd your first domain to Cloudflare.		
	Service Auth					
	Tags					
۶,	Networks New	•		合	会	*
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
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. Sélectionnez le type SaaS.

3. Dans le coffre web de Bitwarden, ouvrez votre organisation et naviguez vers l'écran **Paramètres** → **Connexion unique**. Utilisez les informations du coffre web pour remplir les informations sur l'écran **Configurer l'application** :

Clé	Description
Application	Entrez Bitwarden.
ID de l'entité	Copiez le ID de l'entité SP de la page Bitwarden Single Sign-On dans ce champ.
URL du service de consommation d'assertion	Copiez l' URL du service de consommation d'assertion (ACS) de la page Bitwarden Single Sign-On dans ce champ.
Format d'identifiant de nom	Sélectionnez Courriel dans le menu déroulant.

(i) Note

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

 Faites défiler jusqu'au menu Fournisseurs d'Identité. Sélectionnez le(s) IdP que vous avez configuré(s) dans la section précédente, faites défiler vers le haut et sélectionnez Suivant.

5. Ensuite, créez des politiques de sécurité pour l'accès des utilisateurs à l'application. Complétez les champs **Nom de la politique**, **Action**, et **Durée de la session** pour chaque politique de sécurité.

6. Vous pouvez choisir d'attribuer une stratégie de groupe (**Accès** → **Groupes**) ou des règles de stratégie utilisateur explicites (telles que les e-mails, « e-mails se terminant par », « pays » ou « tout le monde »). Dans l'exemple suivant, le groupe "Anon Users" a été inclus dans la politique de sécurité. Une règle supplémentaire a également été ajoutée pour inclure les courriels se terminant dans le domaine choisi :

🐤 Cloudflare Zerc	Trust	Assign a group
⊕ Home		Assign a group to your application to enforce a set or prederined rules.
Analytics	-	Q. Search for an Access Group
- Gateway	•	Name Rule type
• Access	•	Anon users • DEFAULT
Applications		
Access Groups	- 1	Create additional rules
Service Auth		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	- 1	
ा My Team	-	Include Selector Value
🗏 Logs	•	Emails ending in 🔹 Ranondomain.com 💿 @domain.com
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. Une fois les politiques de sécurité configurées, faites défiler jusqu'en haut et sélectionnez Suivant.

8. Sur l'écran de **Configuration**, copiez les valeurs suivantes et saisissez-les dans leurs champs respectifs sur la page **Single Sign-On** de Bitwarden :

Clé	Description
Point de terminaison SSO	Le point de terminaison SSO indique où votre application SaaS va envoyer les demandes d'identifiant. Cette valeur sera entrée dans le champ URL du Service de Connexion Unique dans Bitwarden.
Accéder à l'ID de l'entité ou à l'émetteur	L'ID de l'entité d'accès ou l'émetteur est l'identifiant unique de votre application SaaS. Cette valeur sera entrée dans le champ ID de l'entité sur Bitwarden.
Clé publique	La clé publique est le certificat d'accès public qui sera utilisé pour vérifier votre identité. Cette valeur sera entrée dans le champ Certificat Public X509 sur Bitwarden.

9. Après avoir entré les valeurs dans Bitwarden, sélectionnez **Enregistrer** sur l'écran Bitwarden Single Sign-On et sélectionnez **Terminé** sur la page Cloudflare pour enregistrer l'application.

10. Pour créer un signet vers l'écran d'identifiant Bitwarden avec SSO, sélectionnez **Ajouter une application** → **Signet**. Vérifiez que le Signet est visible dans le **Lanceur d'application**.

Testez la configuration

Une fois votre configuration terminée, testez-la en vous rendant sur https://vault.bitwarden.com, en entrant votre adresse de courriel, en sélectionnant **Continuer** et en sélectionnant le bouton **Connexion unique de l'Entreprise**.



	Log in
- Maste	r password (required)
⊗ Input is Get ma	s required. Ister password hint
	Log in with master password
	Log in with master password

Connexion unique d'entreprise et mot de passe principal

Entrez l'identifiant de l'organisation configurée et sélectionnez **Se connecter**. Si votre mise en œuvre est correctement configurée, vous serez redirigé vers un écran d'accès Cloudflare, où vous pouvez sélectionner l'IdP pour vous connecter avec l'identifiant :



Après avoir sélectionné votre IdP, vous serez dirigé vers la page d'identifiant de votre IdP. Entrez les informations utilisées pour vous connecter via votre IdP :

Sign In Username Keep me signed in Help
Username I Image: Second se
Keep me signed in Next Help
Next Help
Help

CFZT IdP login

Après vous être authentifié avec vos identifiants IdP, entrez votre mot de passe principal Bitwarden pour déchiffrer votre coffre !