管理者コンソール > SSOでログイン >

CloudflareゼロトラストSSO実 装

ヘルプセンターで表示: https://bitwarden.com/help/cloudflare-zero-trust-sso-implementation/

CloudflareゼロトラストSSO実装

この記事には、SSOでのログインを設定するための**Cloudflare Zero Trust特有の**ヘルプが含まれています。Cloudflare Zero Trustは、 複数のIDプロバイダ(IdPs)と統合できるクラウドベースのIDおよびアクセス管理プラットフォームです。また、 プラットフォームへの安全なアクセスのためにゲートウェイとトンネリングを設定することもできます。

(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

なぜSSOを使用してCloudflare Zero Trustを使用するのですか?

Cloudflare Zero Trustは、複数のIDプロバイダ(IdPs)と統合できるクラウドベースのプロキシIDおよびアクセス管理プラットフォームです。 標準のIdPに加えてCloudflare Zero Trustを使用する利点は、ログインのための複数のIdPを設定する能力です。Cloudflare Zero Trustは、 複数の別々の組織からBitwardenへのSSOアクセスを提供することができます。また、組織内のユーザーセットに対しても提供できます。

ウェブアプリでSSOを開く

(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.

Bitwardenウェブアプリにログインし、製品スイッチャー(鼺)を使用して管理者コンソールを開きます。

D Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS		Nama	Owner	
🖉 Send			Name	Owner	:
\sim Tools \sim	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
 ≢ Reports	✓ All vaults		Personal Login		
Settings	 ∠ My vault ∅ My Organiz : ∅ Toomo Org 		myusername	Me	:
	 Hearns Org : + New organization 		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ④ Login □ Card □ Identity □ Secure note 		Shared Login sharedusername	My Organiz	÷
 Password Manager Secrets Manager ℬ Admin Console Ճ Toggle Width 	 ✓ Folders ➢ No folder ✓ Collections ➢ Default colle ➢ Default colle ☆ Trash 				
		製品-スイ	ッチャー		

あなたの組織の設定 → シングルサインオン画面を開きます。

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.
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
③ 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 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	Generate an identifier that is unique to your organization
SCIM provisioning	i e com la comunicación de la co
	SAML 2.0 metadata URL

SAML 2.0 設定

まだ作成していない場合は、あなたの組电にユニークなSSO識別子を作成し、タイプのドロップダウンからSAMLを選択してください。 この画面を開いたままにして、簡単に参照できるようにしてください。

この段階で、必要に応じて**ユニークなSPエンティティIDを設定する**オプションをオフにすることができます。これを行うと、 あなたのSPエンティティID値から組电IDが削除されますが、ほとんどの場合、このオプションをオンにしておくことをお勧めします。

🖓 Tip

代替のメンバー復号化オプションがあります。信頼できるデバイスでのSSOの使い方またはキーコネクターの使い方を学びましょう。

Cloudflare Zero Trustのログイン方法を作成します

Cloufdlare Zero Trustログイン方法を作成するには:

1. Cloudflare Zero Trustに移動してログインするか、アカウントを作成してください。

 aなたのアプリケーションにアクセスするためにユーザーが使用するURL、 またはアプリランチャーとして機能するドメインを設定します。例えば、https://my-business.cloudflareaccess.com/ のようなものです。Cloudflare Zero Trustメニューから、設定→一般→チームドメインを選択します:

CLC			Support 🔻
÷	-	← Back to Settings	
	Zero Trust overview	Custom Pages	
G	Analytics New		
Ð	Gateway	Team domain This is where the App Laurcher lives, and where users make access requests to applications behind Access	
÷	Access		
ø	Networks New	Edit	
2 ⁰ 8	My team		
Ξ	Logs	Block page Oustomize the page users see when they reach a website blocked by Gateway. Note: Devices must have the Cloutifiare 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. 最初のログイン方法を設定するには、設定→認証→新規追加に移動してください。
- 4. Cloudflare Zero Trustに接続するためのログイン方法を選択してください。あなたが使用しているIdPがIdPリストに存在しない場合は、 SAMLまたはOIDCの一般的なオプションを使用してください。この記事では、Oktaを例に使用します:

🛟 Cloudflare Zero Trust	Add a login method	
Home		
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	Cone-time PIN ADDED
		SAML
•	Я Yandex	

Cloudflare Zero Trust IdP list

5. 選択したIdPログイン方法を選択した後、Cloudflareが提供する製品内ガイドに従って、IdPを統合してください。

(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.

Cloudflare Zero Trustアプリケーションを作成します

IdPが設定された後、BitwardenのためのCloudflare Zero Trustアプリケーションを作成する必要があります。**この例では、SAML** アプリケーションを作成します。

1. **アクセス → アプリケーション → アプリケーションを追加**へ移動します。





÷		•	← 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		
Ŷ	Access Applications	*	What type of application do y To protect a self-hosted application, a	rou want to add? add your first domain to Cloudflare.		
	Access Groups Service Auth					
	Tags					
Ħ	Networks New	•		会	会	\$
æ	DEX	•		L.	(H)	
<u>898</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. タイプ**SaaS**を選択してください。

3. Bitwardenのウェブ保管庫で、あなたの組織を開き、設定 → シングルサインオン画面に移動します。ウェブ保管庫からの情報を使用して、 アプリの設定画面に情報を入力してください:

*-	説明
アプリ	<mark>Bitwarden</mark> に入ります。
エンティティID	Bitwardenシングルサインオンページから SPエンティティID をコピーして、 このフィールドに貼り付けてください。
アサーション消費者サービスURL	Bitwardenシングルサインオンページから アサーションコンシューマーサービス(ACS) URL をコピーして、このフィールドに貼り付けてください。
名前ID形式	ドロップダウンメニューから メールアドレス を選択してください。

(i) Note

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

4. **IDプロバイダー**メニューまでスクロールダウンしてください。前のセクションで設定したIdPを選択し、トップに戻って、 次へを選択してください。

5. 次に、ユーザーがアプリケーションにアクセスするためのアクセスポリシーを作成します。各ポリシーに対して、**ポリシー名**、**アクション**、 および**セッションの期間**のフィールドを完成させてください。

6. グループポリシーを割り当てることを選択できます(**アクセス→ グループ**)または明示的なユーザーポリシールール(メールアドレス、 「メールアドレスが以下で終わる」、「国」、または「全員」など)を選択できます。次の例では、グループ「Anon Users」 がポリシーに含まれています。選択したドメインで終わるメールアドレスも含めるという追加のルールが設けられました。

🛟 Cloudflare Zero	Trust	Assign a group		
Home		Assign a group to your application to enforce a set of predefined rules.		
2 Analytics	•	Q Search for an Access Group		
⊕ Gateway	•	Name Rule type		
Access	•	> Anon users • DEFAULT		
Applications				
Access Groups	- 1	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	- 1	Include		
ങ്ക 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. アクセスポリシーが設定されたら、トップまでスクロールして、次へを選択します。

8. セットアップ画面にいる間、以下の値をコピーして、それぞれのフィールドにBitwardenのシングルサインオンページに入力します:

+-	説明
SSOエンドポイント	SSOエンドポイントは、 あなたのSaaSアプリケーションがログインリクエストをSendする場所を指示します。 この値はBitwardenの シングルサインオンサービスURL フィールドに入力されます。
エンティティIDまたは発行者にアクセスする	アクセスエンティティIDまたは発行者は、 あなたのSaaSアプリケーションの一意の識別子です。 この値はBitwardenの エンティティID フィールドに入力されます。
公開鍵	公開鍵は、あなたのIDを確認するために使用される公開証明書です。 この値はBitwardenの X509公開証明書 フィールドに入力されます。

9. 値がBitwardenに入力された後、Bitwarden Single Sign-On画面で保存を選択し、 Cloudflareページで完了を選択してアプリケーションを保存します。

10. SSO画面へのBitwardenログインのブックマークを作成するには、アプリケーションを追加する→ ブックマークを選択します。 アプリランチャーでブックマークが表示されていることを確認してください。

設定をテストする

設定が完了したら、https://vault.bitwarden.comに移動し、メールアドレスを入力し、**続ける**を選択し、 エンタープライズシングルサインオンボタンを選択してテストしてください。



	Log in	
Maste ⊗ Input i	er password (required)	>
Get ma	aster password hint Log in with master password	
\sub	🖻 Enterprise single sign-on	\sum
Logging Not you	in as myemailaddress@bitwarden.com ?	

エンタープライズシングルサインオンとマスターパスワード

設定された組織識別子を入力し、**ログイン**を選択してください。あなたの実装が正常に設定されている場合、Cloudflare Accessの画面にリダイレクトされます。そこで、ログインするIdPを選択できます。

Cloudflare Access	
ssol cloudflareaccess.com Bitwarden Sign in with:	
Cloudflare Zero Trust	

Cloudflare IdP selection

あなたのIdPを選択した後、あなたのIdPのログインページにリダイレクトされます。 あなたのIdPを通じてログインするために使用される情報を入力してください:

CFZT IdP login

あなたのIdP資格情報で認証した後、Bitwardenのマスターパスワードを入力して保管庫を復号化してください!