

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-ss-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。

📌 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

📌 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 (☰) を使用して管理者コンソールを開きます。

Filters:

- All vaults
 - My vault
 - My Organiz...
 - Teams Org...
 - New organization
- All items
 - Favorites
 - Login
 - Card
 - Identity
 - Secure note
- Folders
 - No folder
- Collections
 - Default colle...
 - Default colle...
- Trash

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

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。

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

Single sign-on

Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

Master password

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.

Type

SAML 2.0

SAML service provider configuration

Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID

[Masked SP entity ID]

SAML 2.0 metadata URL

[Masked SAML 2.0 metadata URL]

SAML 2.0設定

まだ作成していない場合は、あなたの組電にユニークな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値から組電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

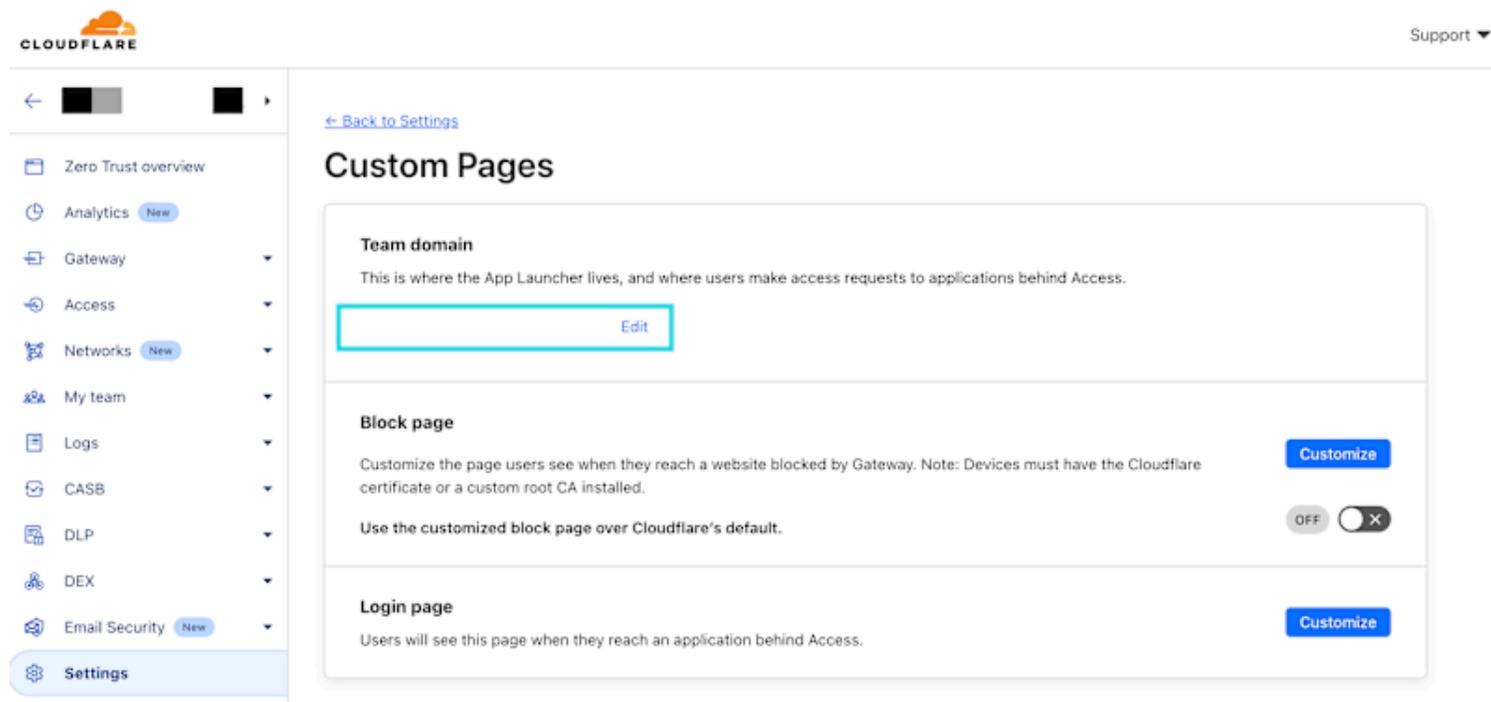
代替の**メンバー復号化オプション**があります。信頼できるデバイスでのSSOの使い方またはキーコネクタの使い方を学びましょう。

Cloudflare Zero Trustのログイン方法を作成します

Cloudflare Zero Trustログイン方法を作成するには：

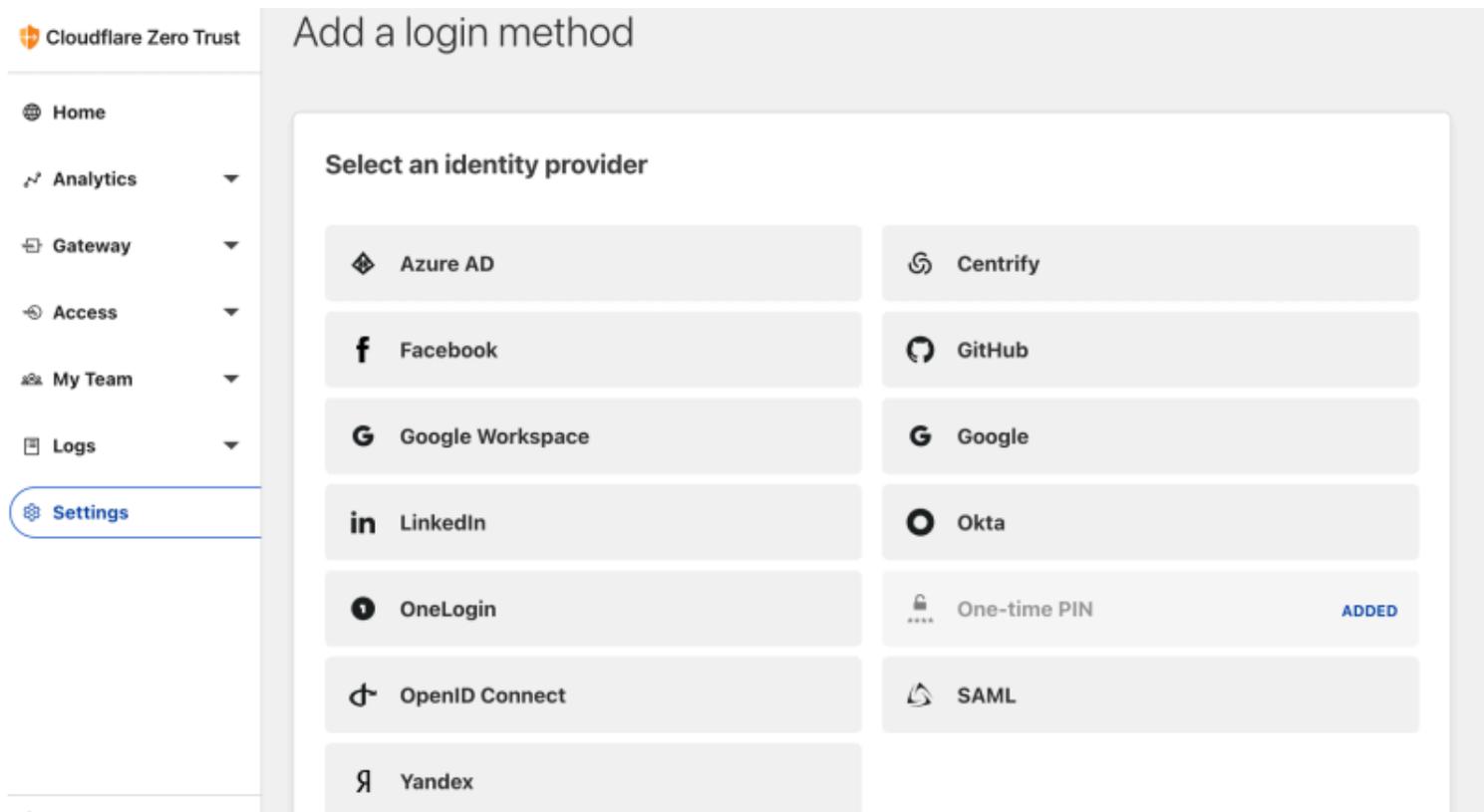
1. [Cloudflare Zero Trust](#)に移動してログインするか、アカウントを作成してください。

- あ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：



Team domain setting

- 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。
- 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 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。

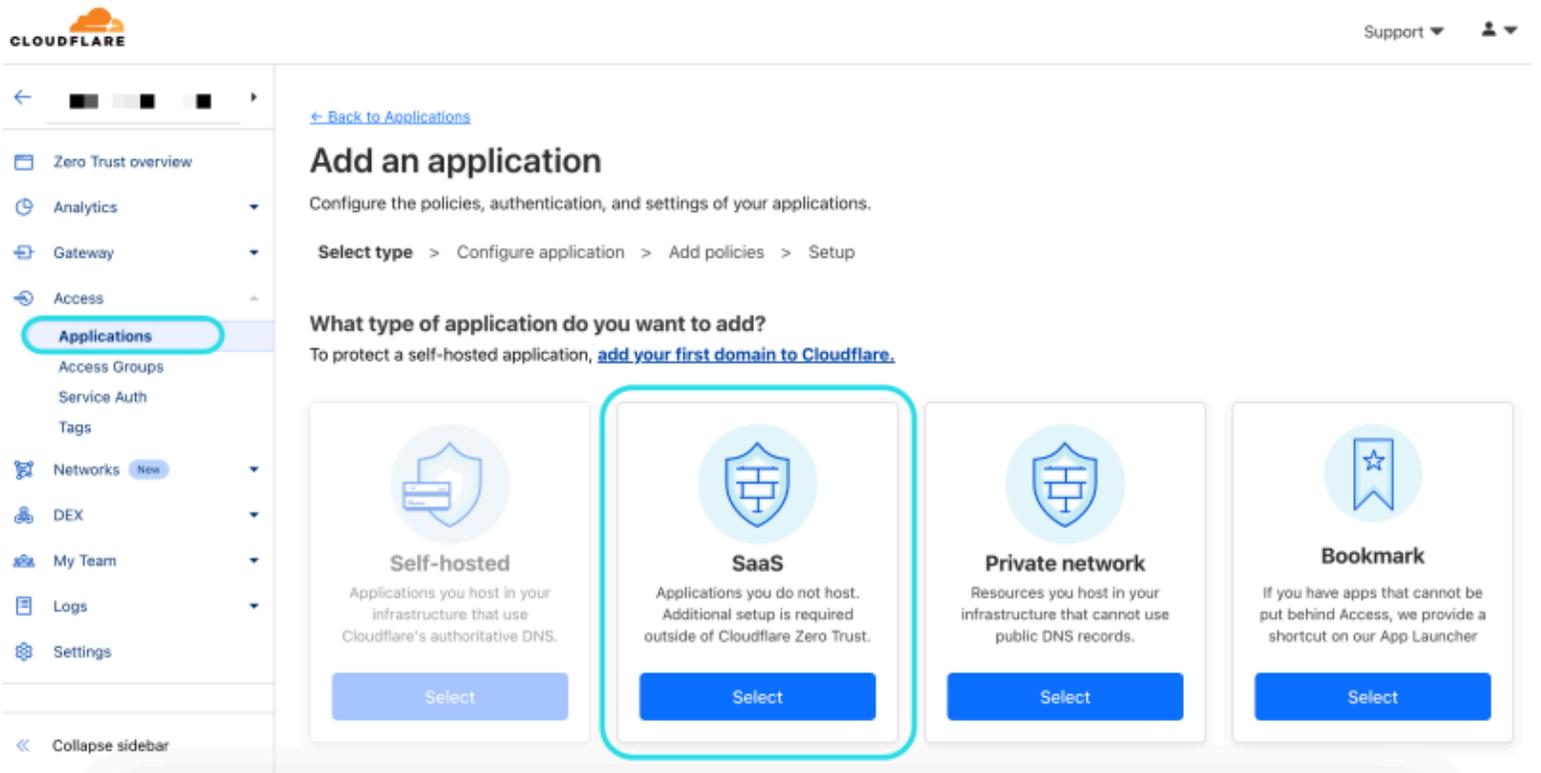
Note

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。



CFZT add an application

2. タイプSaaSを選択してください。

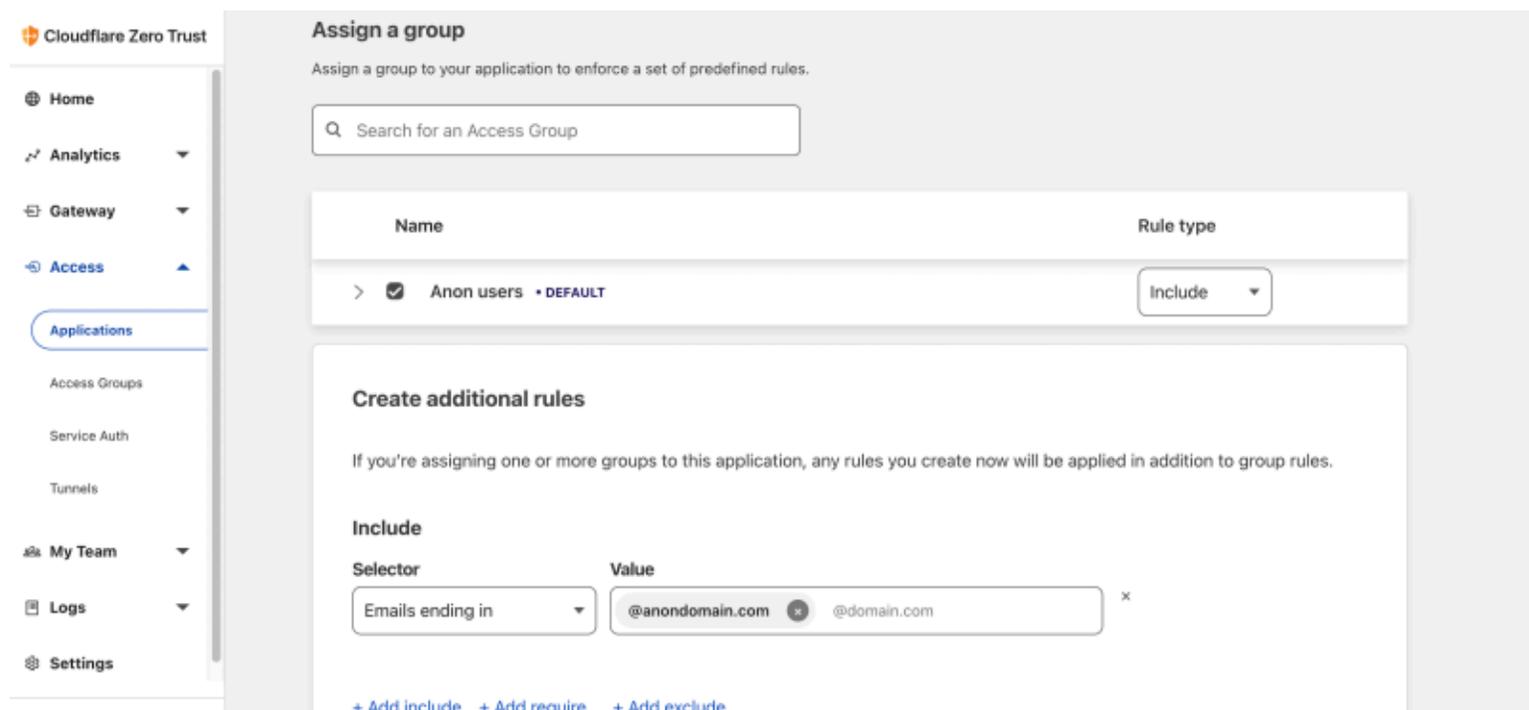
3. Bitwardenのウェブ保管庫で、あなたの組織を開き、**設定** → **シングルサインオン**画面に移動します。ウェブ保管庫からの情報を使用して、**アプリの設定**画面に情報を入力してください：

キー	説明
アプリ	Bitwarden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。

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。



CFZT app policy

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** → **App Launcher** → **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:

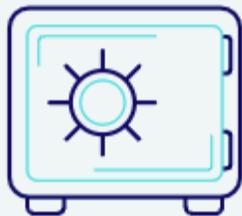
キー	説明
SSOエンドポイント	SSOエンドポイントは、あなたのSaaSアプリケーションがログインリクエストをSendする場所を指示します。 この値はBitwardenの シングルサインオンサービスURL フィールドに入力されます。
エンティティIDまたは発行者にアクセスする	アクセスエンティティIDまたは発行者は、あなたのSaaSアプリケーションの一意の識別子です。 この値はBitwardenの エンティティID フィールドに入力されます。
公開鍵	公開鍵は、あなたのIDを確認するために使用される公開証明書です。 この値はBitwardenの X509公開証明書 フィールドに入力されます。

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 to Bitwarden

Email address (required)

Remember email

Continue

or

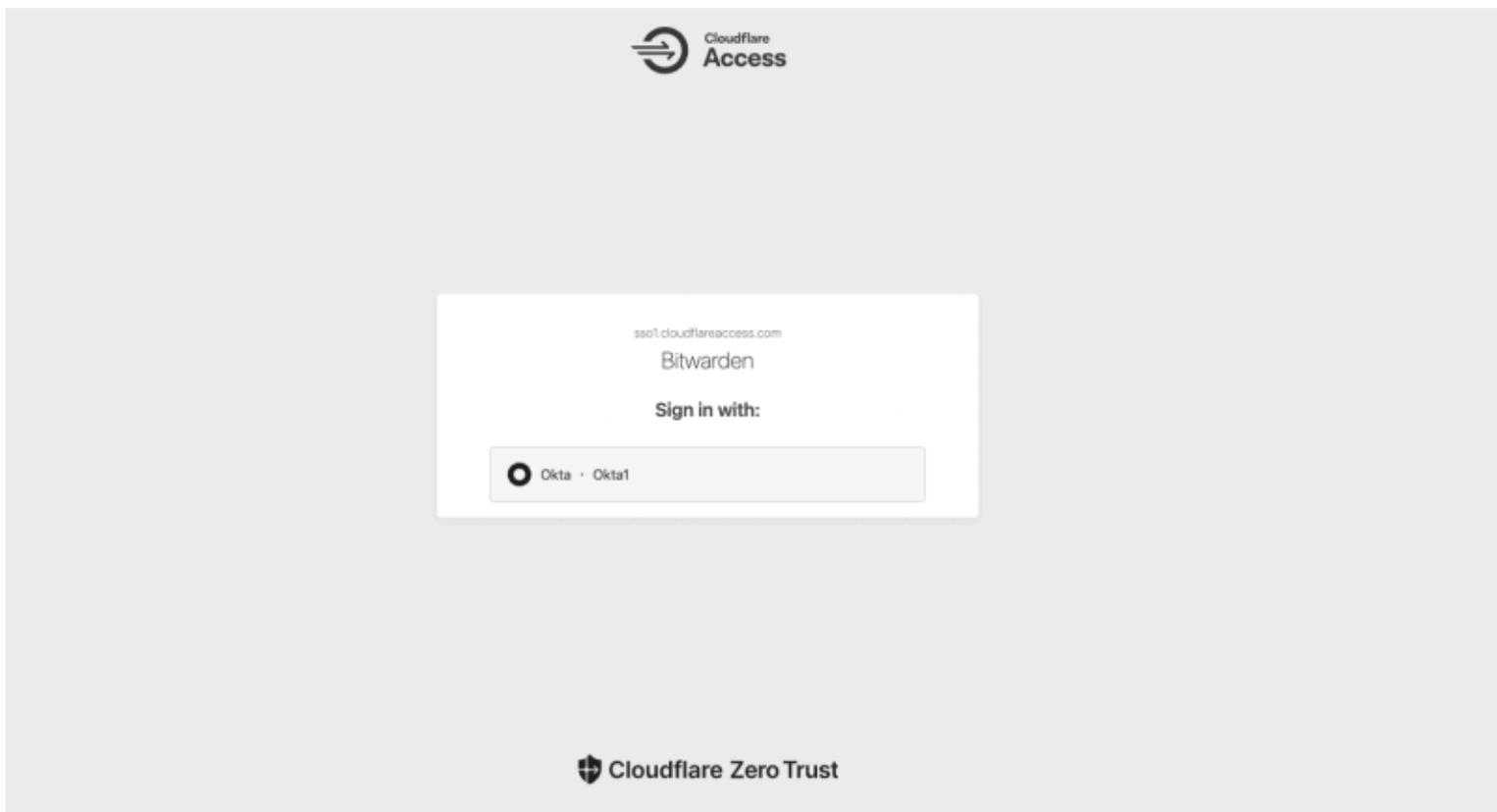
 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

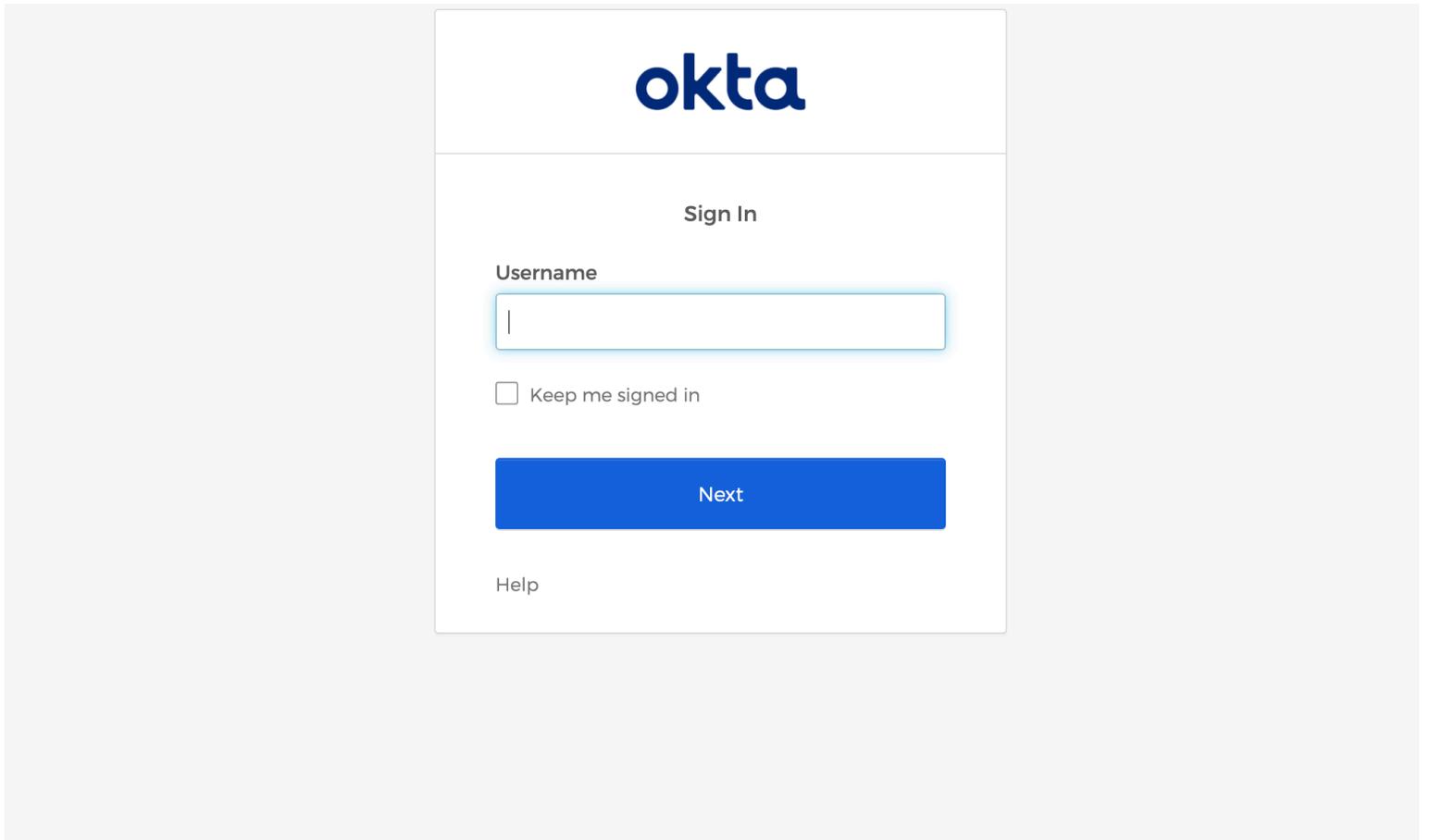
エンタープライズシングルサインオンとマスターパスワード

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 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！