

管理者コンソール > SSOでログイン

OIDC設定

ヘルプセンターで表示:

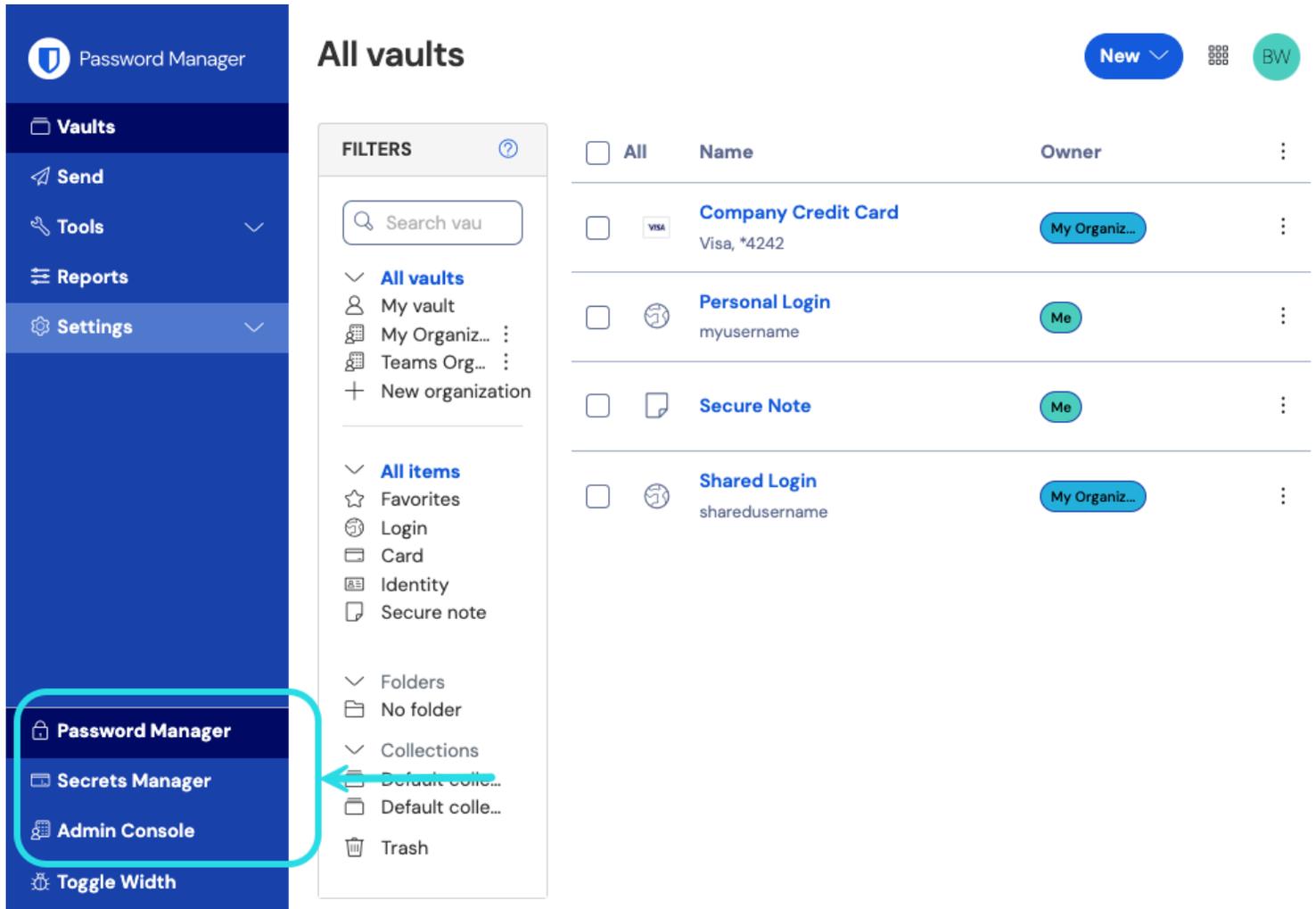
<https://bitwarden.com/help/configure-sso-oidc/>

OIDC設定

ステップ1：SSO識別子を設定する

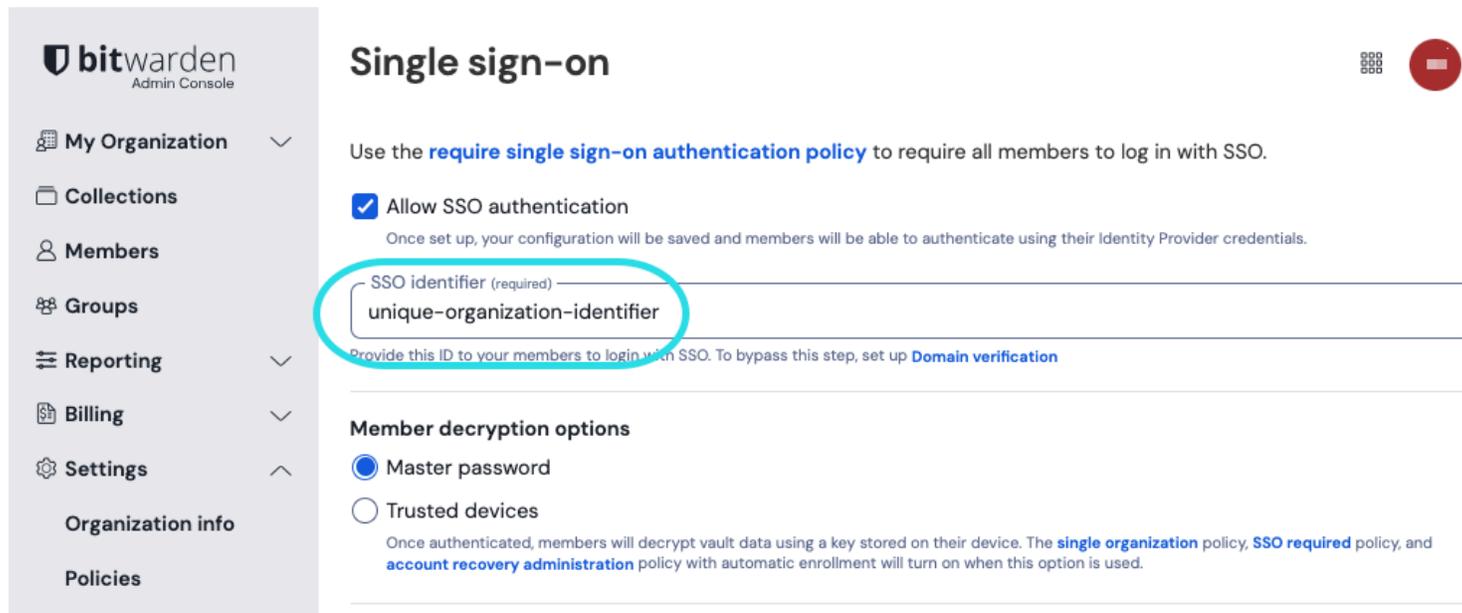
SSOを使用してIDを認証するユーザーは、認証に対抗する組織（したがって、SSO統合）を示す**SSO識別子**を入力する必要があります。ユニークなSSO識別子を設定するには：

1. Bitwardenの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。



製品-スイッチャー

2. 設定 → シングルサインオンに移動し、あなたの組織のためのユニークな**SSO識別子**を入力してください：



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)

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.

識別子を入力してください

3. ステップ2 : SSOでのログインを有効にするに進んでください。



Tip

You will need to share this value with users once the configuration is ready to be used.

ステップ2 : SSOでのログインを有効にする

あなたのSSO識別子を取得したら、あなたの統合を有効化し設定を進めることができます。SSOでのログインを有効にするには :

1. 設定 → シングルサインオン 表示で、SSO認証を許可する チェックボックスを確認してください。

bitwarden Admin Console

- 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
OpenID Connect

OpenID connect configuration

Callback path
[Redacted]

Signed out callback path
[Redacted]

OIDC設定

2. タイプのドロップダウンメニューから、**OpenID Connect**のオプションを選択してください。もし代わりにSAMLを使用するつもりなら、[SAML設定ガイド](#)に切り替えてください。



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。

ステップ3：設定

この時点から、実装はプロバイダーごとに異なります。設定プロセスの完了に役立つ、特定の[実装ガイド](#)の一つにジャンプしてください：

プロバイダー

ガイド

アズール

[Azure 実装ガイド](#)

オクタ

[Okta 実装ガイド](#)

設定参考資料

次のセクションでは、どのIdPと統合しているかに関係なく、シングルサインオン設定中に利用可能なフィールドを定義します。設定が必要なフィールドは、(必須)とマークされます。



Tip

Unless you are comfortable with OpenID Connect, we recommend using one of the [above implementation guides](#) instead of the following generic material.

フィールド	説明
コールバックパス	(自動生成) 認証自動リダイレクト用のURL。クラウドホストのお客様の場合、これは https://sso.bitwarden.com/oidc-signin または https://sso.bitwarden.eu/oidc-signin です。自己ホスト型のインスタンスの場合、これはあなたの設定されたサーバーURLによって決定されます。例えば、 https://your.domain.com/sso/oidc-signin などです。
サインアウトコールバックパス	(自動生成) サインアウト自動リダイレクトのURL。クラウドホストのお客様の場合、これは https://sso.bitwarden.com/oidc-signedout または https://sso.bitwarden.eu/oidc-signedout です。自己ホスト型のインスタンスの場合、これはあなたの設定されたサーバーURLによって決定されます。例えば、 https://your.domain.com/sso/oidc-signedout などです。
権限	(必須) あなたの認証サーバー ("Authority") のURL。Bitwardenはこれに対して認証を行います。例えば、 https://your.domain.okta.com/oauth2/default または https://login.microsoft.com/v2.0 。
クライアントID	(必須) OIDCクライアントの識別子。この値は通常、構築されたIdPアプリの統合に特化しています。例えば、 Azureアプリの登録 や Oktaウェブアプリ などです。
クライアントシークレット	(必須) クライアントIDと共に使用され、アクセストークンと交換するためのクライアントシークレット。この値は通常、構築されたIdPアプリの統合に特化しています。例えば、 Azureアプリの登録 や Okta Webアプリ などです。
メタデータアドレス	(権限が無効な場合に必要) BitwardenがJSONオブジェクトとして認証サーバーのメタデータにアクセスできるメタデータURL。例えば、 https://your.domain.okta.com/oauth2/default/.well-known/oauth-authorization-server
OIDCリダイレクトの挙動	(必須) IdPがBitwardenからの認証要求に応答するための方法。オプションには、 フォーム POST と リダイレクト GET が含まれます。

フィールド	説明
ユーザー情報エンドポイントから請求を取得する	このオプションを有効にすると、URLが長すぎるエラー（HTTP 414）、URLが切り捨てられる、および/またはSSO中に失敗が発生した場合に対応します。
追加/カスタムスコープ	リクエストに追加するカスタムスコープを定義します（カンマ区切り）。
追加/カスタムユーザーIDクレームタイプ	ユーザー識別のためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームタイプは、標準タイプに戻る前に検索されます。
追加/カスタムメールアドレス請求タイプ	ユーザーのメールアドレス用のカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。
追加/カスタム名前請求タイプ	ユーザーのフルネームまたは表示名のためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。
要求された認証コンテキストクラスの参照値	認証コンテキストクラス参照識別子（ <code>acr_values</code> ）（スペース区切り）を定義してください。 <code>acr_values</code> を優先順位でリストアップしてください。
応答で期待される "acr" 請求値	Bitwardenがレスポンスで期待し、検証する <code>acr</code> クレーム値を定義してください。

OIDC属性 & クレーム

アカウントの提供にはメールアドレスが必要です。これは、以下の表の属性またはクレームのいずれかとして渡すことができます。

ユニークなユーザー識別子も非常に推奨されます。もし不在の場合、ユーザーをリンクするためにメールアドレスが代わりに使用されます。

属性/請求は、適用可能な場合にはフォールバックを含めて、一致のための優先順位でリストされています。

値	請求/属性	フォールバッククレーム/属性
ユニークID	設定済みカスタムユーザーIDクレーム 非一時的な場合のNameID urn:oid:0.9.2342.19200300.100.1.1 サブ UID UPN EPPN	

値	請求/属性	フォールバッククレーム/属性
Eメール	カスタムメールアドレスのクレームを設定しました Eメール http://schemas.xmlsoap.org/ws/2005/05/ID/claims/emailaddress urn:oid:0.9.2342.19200300.100.1.3 メール メールアドレス	希望のユーザーネーム Urn:oid:0.9.2342.19200300.100.1.1 UID
お名前	設定されたカスタム名前クレーム お名前 http://schemas.xmlsoap.org/ws/2005/05/ID/claims/name urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3 表示名 CN	名前 + " " + 姓 (下記参照)
名	urn:oid:2.5.4.42 名前 ファーストネーム FN F名 ニックネーム	
姓	urn:oid:2.5.4.4 SN 苗字 苗字	