bitwarden | ヘルプセンターの記事

管理者コンソール > SSOでログイン >

Okta OIDCの実装

ヘルプセンターで表示:
https://bitwarden.com/help/oidc-okta/

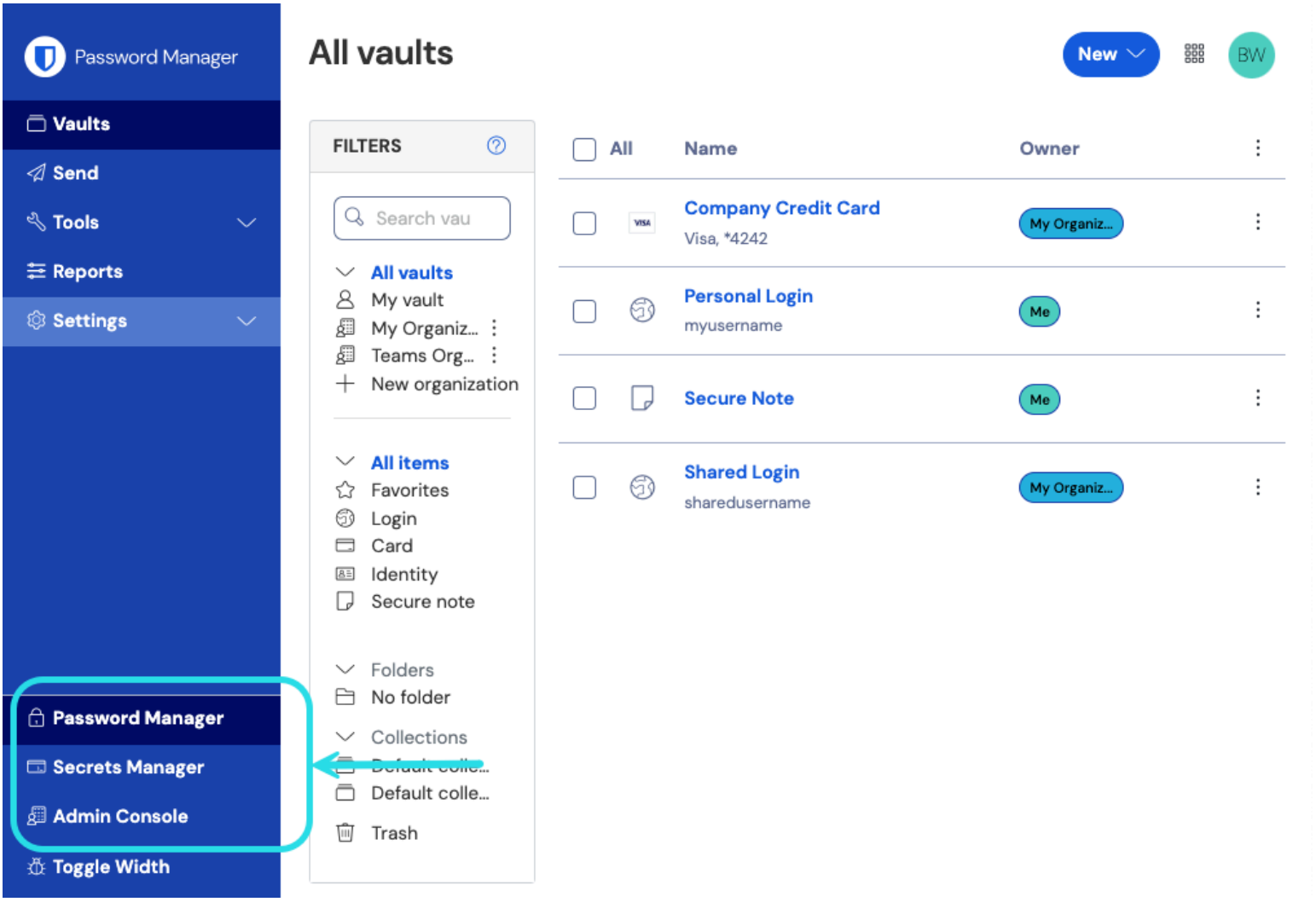
Okta OIDCの実装

この記事には、OpenID Connect（OIDC）を介したSSOでの**Okta特有の**ログインを設定するためのヘルプが含まれています。別のOIDC IdPでのSSOを使用したログインの設定、またはSAML 2.0を介したOktaの設定についてのヘルプは、OIDC設定またはOkta SAML実装を参照してください。

設定は、Bitwardenウェブアプリと Okta管理者ポータルの両方で同時に作業を行うことを含みます。進行するにあたり、両方をすぐに利用できる状態にして、記録されている順序で手順を完了することをお勧めします。

ウェブ保管庫でSSOを開く

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

ナビゲーションから**設定** → **シングルサインオン**を選択してください。

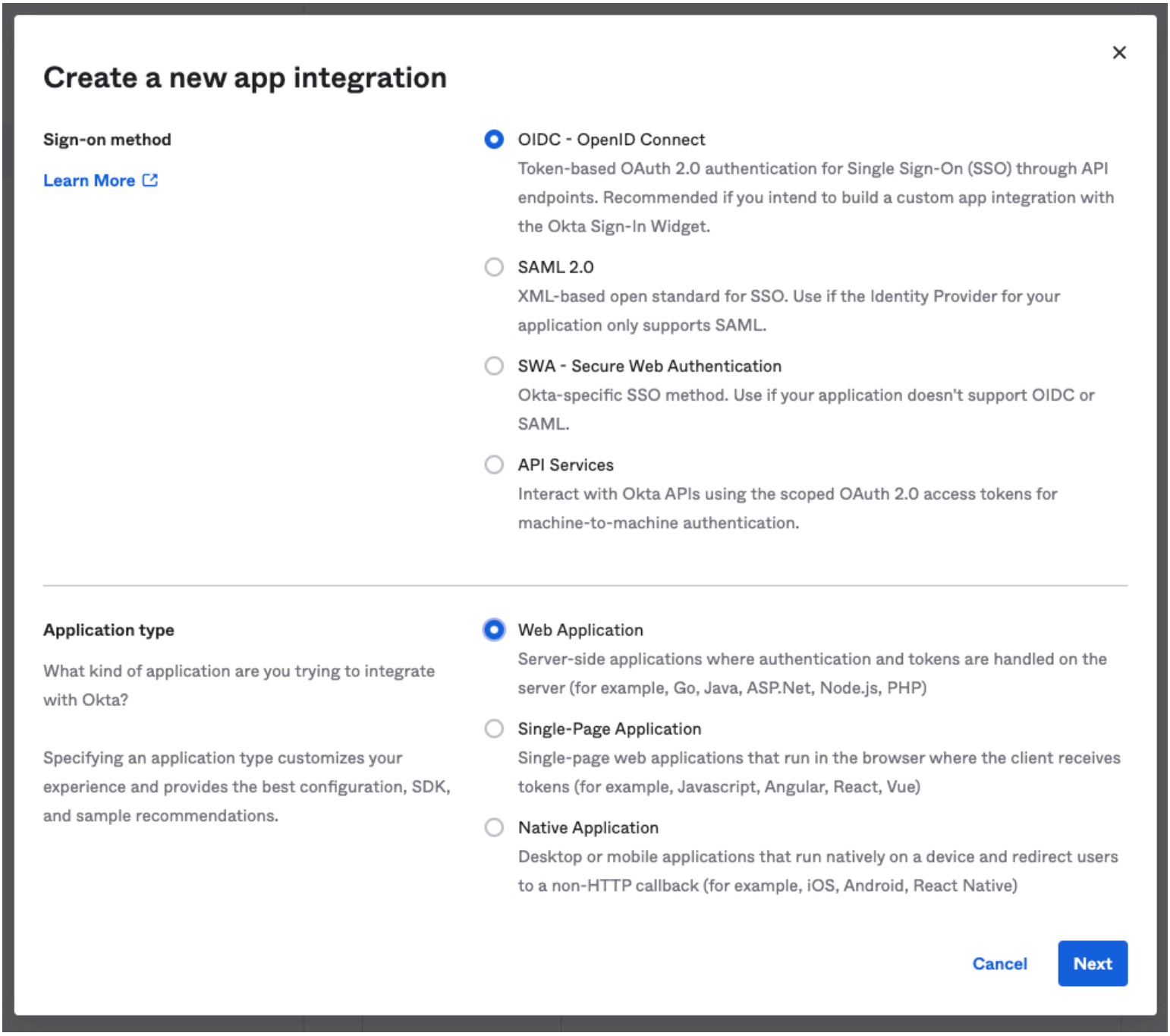
OIDC設定

まだ作成していない場合は、あなたの組織のためのユニークな**SSO識別子**を作成してください。それ以外では、この画面でまだ何も編集する必要はありませんが、簡単に参照できるように開いたままにしておいてください。

> **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。

Oktaアプリを作成する

Okta管理者ポータルで、**アプリケーション → アプリケーション**をナビゲーションから選択します。アプリケーション画面で、**アプリ統合を作成**ボタンを選択します。サインオン方法で、**OIDC - OpenID Connect**を選択してください。アプリケーションのタイプで、**ウェブアプリケーション**を選択してください。



Create App Integration

新しいWebアプリの統合画面で、以下のフィールドを設定します：

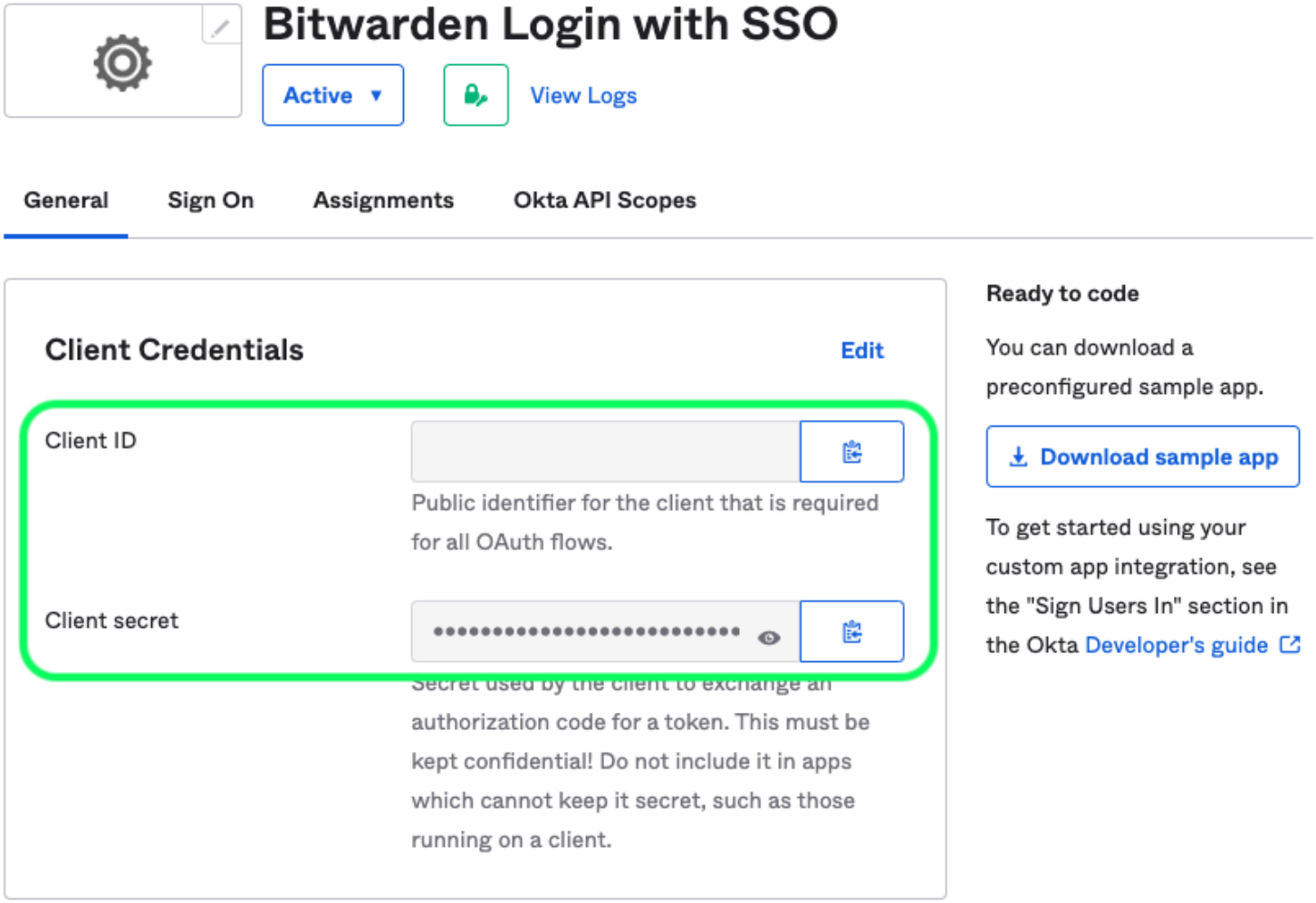
フィールド	説明
アプリ統合名	アプリにBitwarden専用の名前を付けてください。

フィールド	説明
グラントタイプ	以下の許可タイプを有効にしてください： - クライアントが自身を代表して行動 → **クライアント資格情報** - ユーザーを代表して行動するクライアント → **認証コード**
サインインリダイレクトURI	このフィールドをあなたの**コールバックパス**に設定してください。これはBitwarden SSO設定画面から取得できます。 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。
サインアウトリダイレクトURI	このフィールドをあなたの**サインアウトコールバックパス**に設定してください。これはBitwarden SSO設定画面から取得できます。
課題	このフィールドを使用して、すべてまたは選択したグループのみがBitwarden ログインをSSOで使用できるように指定します。

設定が完了したら、**次へ**ボタンを選択してください。

クライアントの資格情報を取得します

アプリケーション画面で、新しく作成されたOktaアプリの**クライアントID**と**クライアントシークレット**をコピーします：

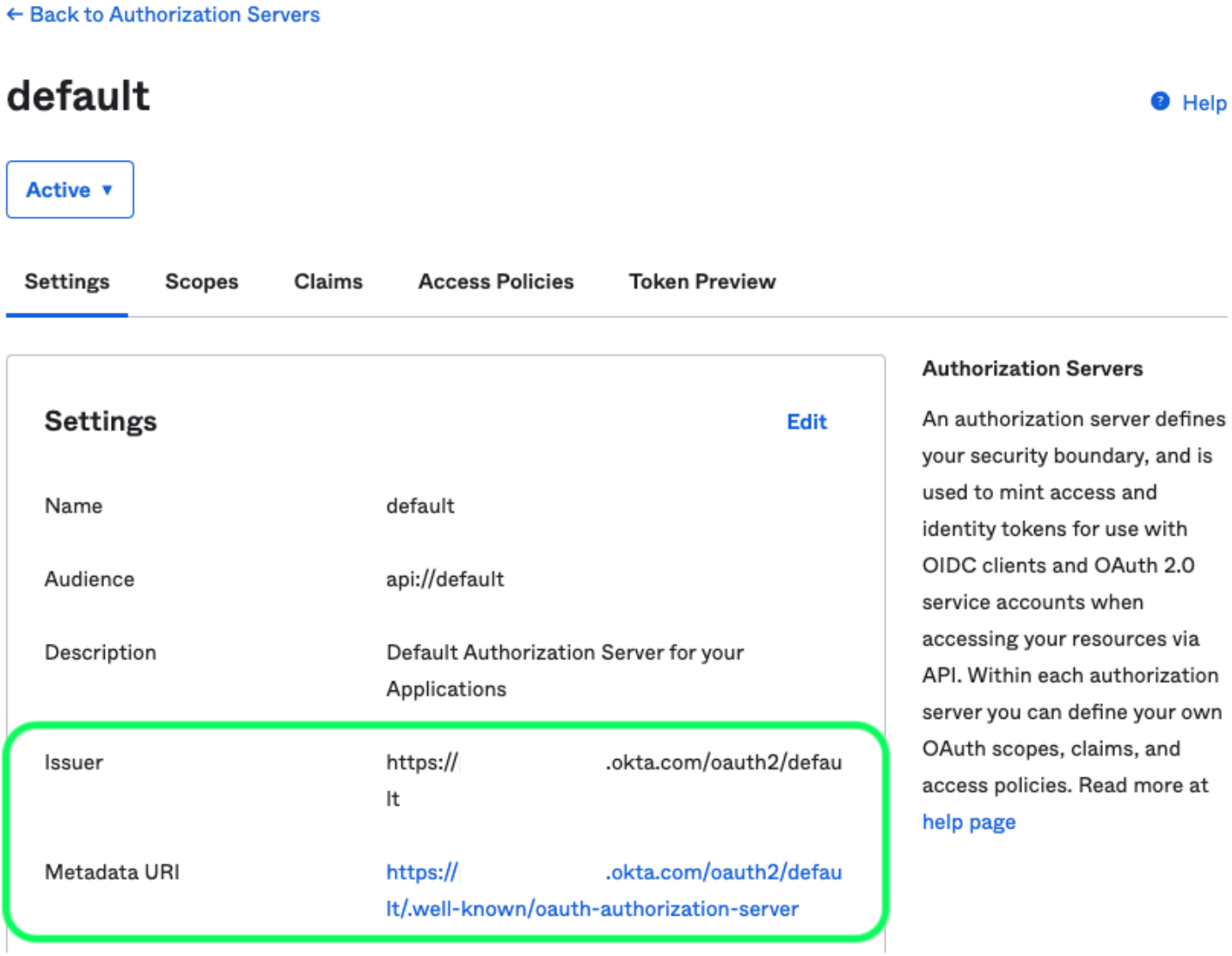


App Client Credentials

あなたは後のステップで両方の値を使用する必要があります。

認証サーバー情報を取得します

ナビゲーションから**セキュリティ** → **API**を選択します。**認証サーバー**のリストから、この実装に使用したいサーバーを選択してください。
サーバーの**設定**タブで、**Issuer**と**Metadata URI**の値をコピーします:



Okta Authorization Server Settings

次のステップで両方の値を使用する必要があります。

ウェブアプリに戻る

この時点で、Okta管理者ポータルのコンテキスト内で必要なすべてを設定しました。次のフィールドを設定するために、Bitwardenウェブアプリに戻ってください：

フィールド	説明
権限	あなたの認証サーバーのための取得した発行者URIを入力してください。
クライアントID	あなたのOktaアプリの取得したクライアントIDを入力してください。

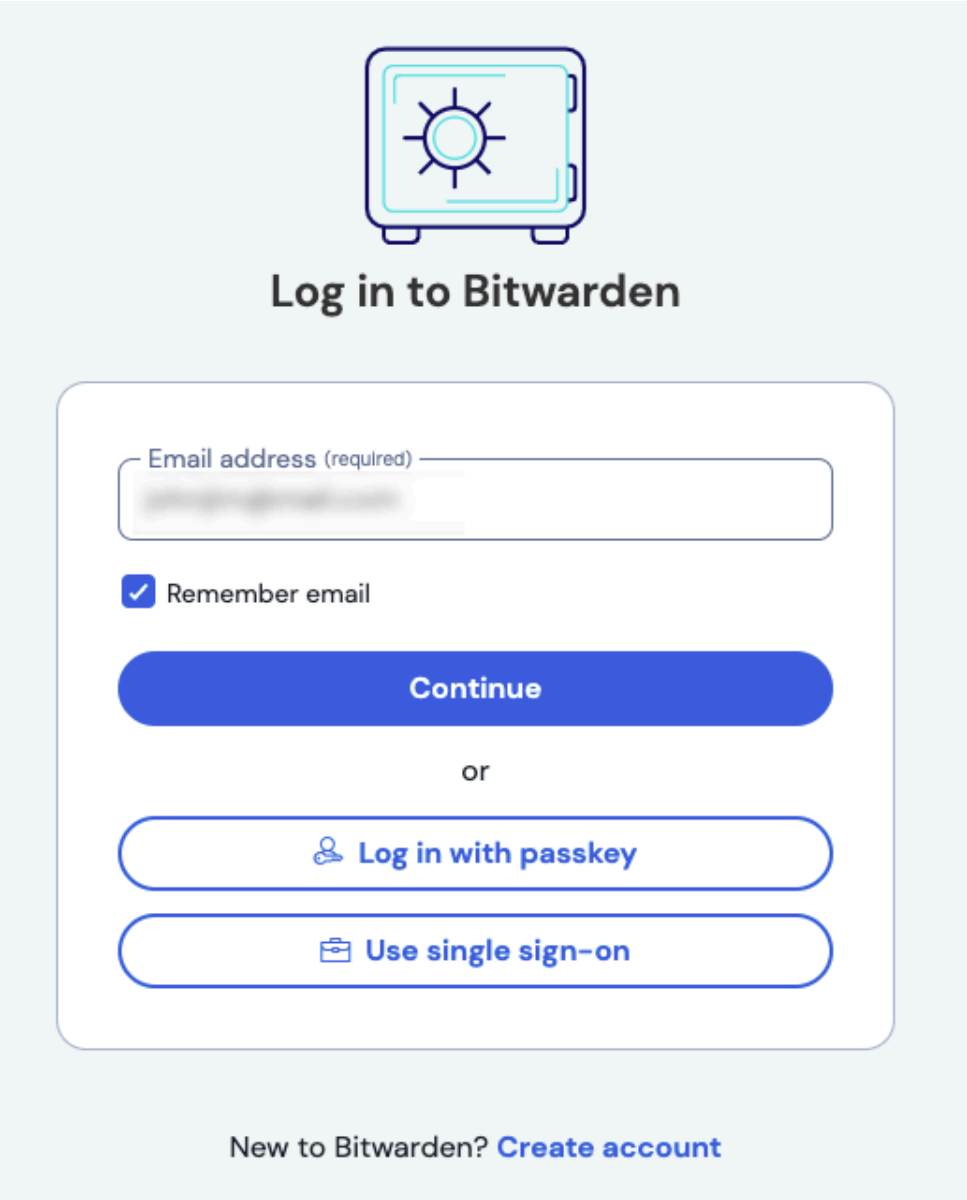
フィールド	説明
クライアントシークレット	あなたのOktaアプリの取得したクライアントシークレットを入力してください。
メタデータアドレス	あなたの認証サーバーのための取得したメタデータURIを入力してください。
OIDCリダイレクトの挙動	**リダイレクト GET**を選択します。現在、 OktaはフォームPOSTをサポートしていません。
ユーザー情報エンドポイントからクレームを取得する	このオプションを有効にすると、URLが長すぎるエラー（HTTP 414）、 切り捨てられたURL、および/またはSSO中の失敗が発生した場合に対応します。
追加/カスタムスコープ	リクエストに追加するカス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 メールアドレス クレーム タイプ	ユーザーのメールアドレス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/カスタム名前クレームタイプ	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参照値	認証コンテキストクラス参照識別子（`acr_values`）（スペース区切り） を定義してください。リスト`acr_values` を優先順位で並べてください。
応答で期待される "acr" 請求値	Bitwardenが応答で期待し、検証する`acr`クレーム値を定義してください。

これらのフィールドの設定が完了したら、**保存**してください。

> **Tip**
> シングルサインオン認証ポリシーを有効にすることで、ユーザーにSSOでログインすることを要求することができます。メモしてください、
> これは単一の組織ポリシーも同時に活性化する必要があります。もっと学ぶ

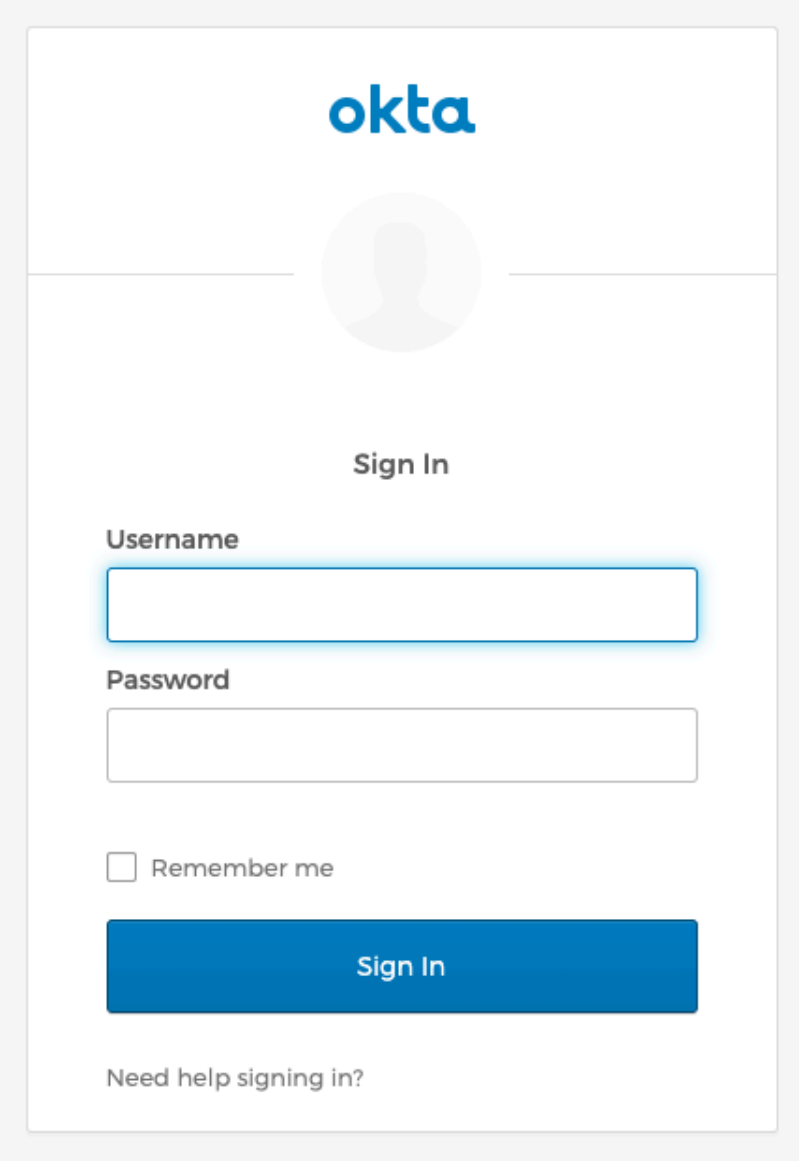
設定をテストする

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



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、Oktaのログイン画面にリダイレクトされます。



Log in with Okta

あなたのOktaの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！

ⓘ Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an Okta Bookmark App that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.
2. Click **Browse App Catalog**.
3. Search for **Bookmark App** and click **Add Integration**.
4. Add the following settings to the application:
    1. Give the application a name such as **Bitwarden Login**.
    2. In the **URL** field, provide the URL to your Bitwarden client such as `https://vault.bitwarden.com/#/login` or `your-self-hostedURL.com`.
5. Select **Done** and return to the applications dashboard and edit the newly created app.
6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained here.

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.