Microsoft Entra ID OIDC 実装

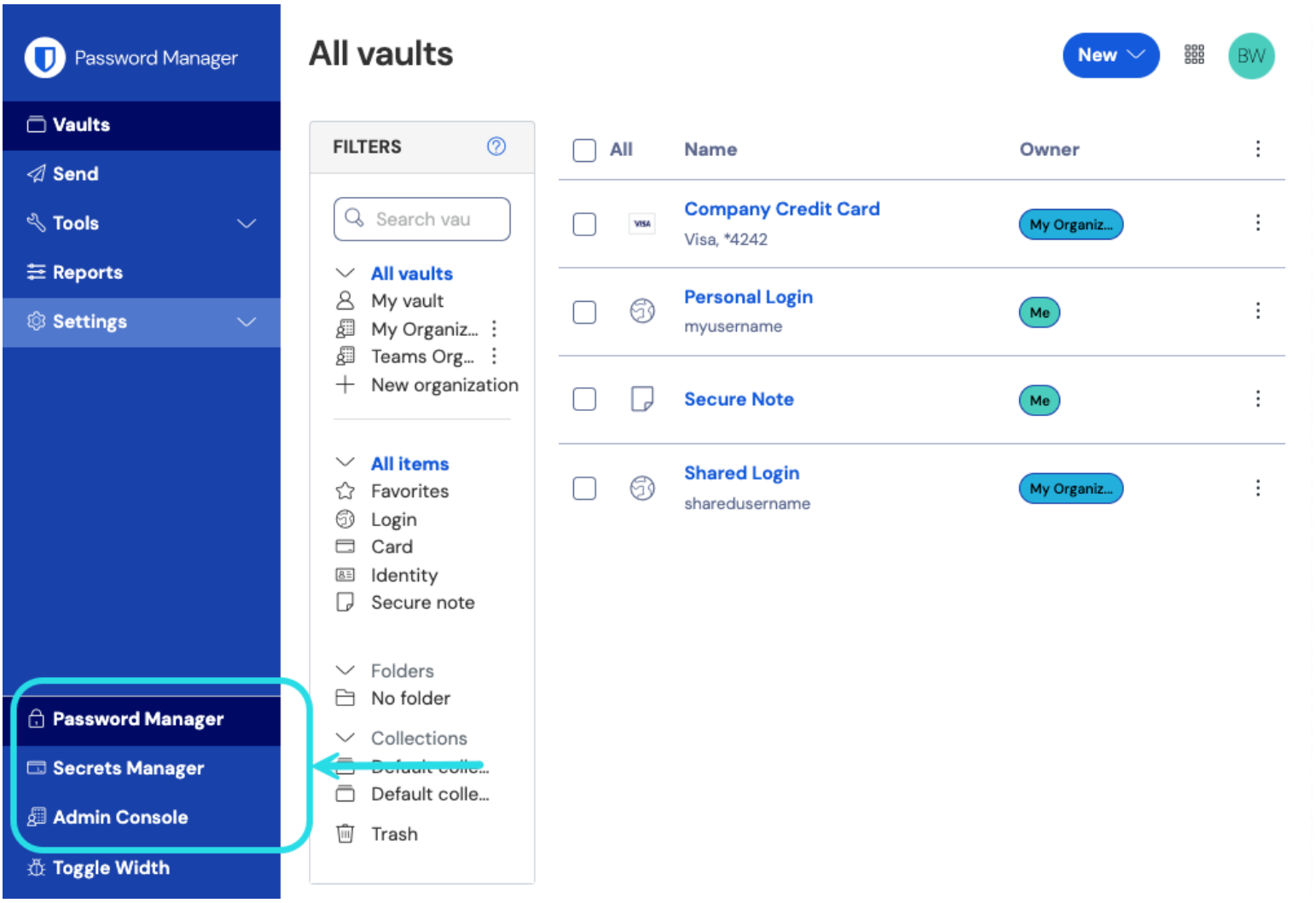
Microsoft Entra ID OIDC 実装

この記事には、OpenID Connect（OIDC）を介したSSOでのログインを設定するための**Azure特有の**ヘルプが含まれています。別のOIDC IdPのSSOでのログインの設定、またはMicrosoft Entra IDのSAML 2.0経由の設定についてのヘルプは、OIDC設定またはMicrosoft Entra ID SAML実装をご覧ください。

設定は、Bitwardenウェブアプリと Azure Portal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**を選択します。

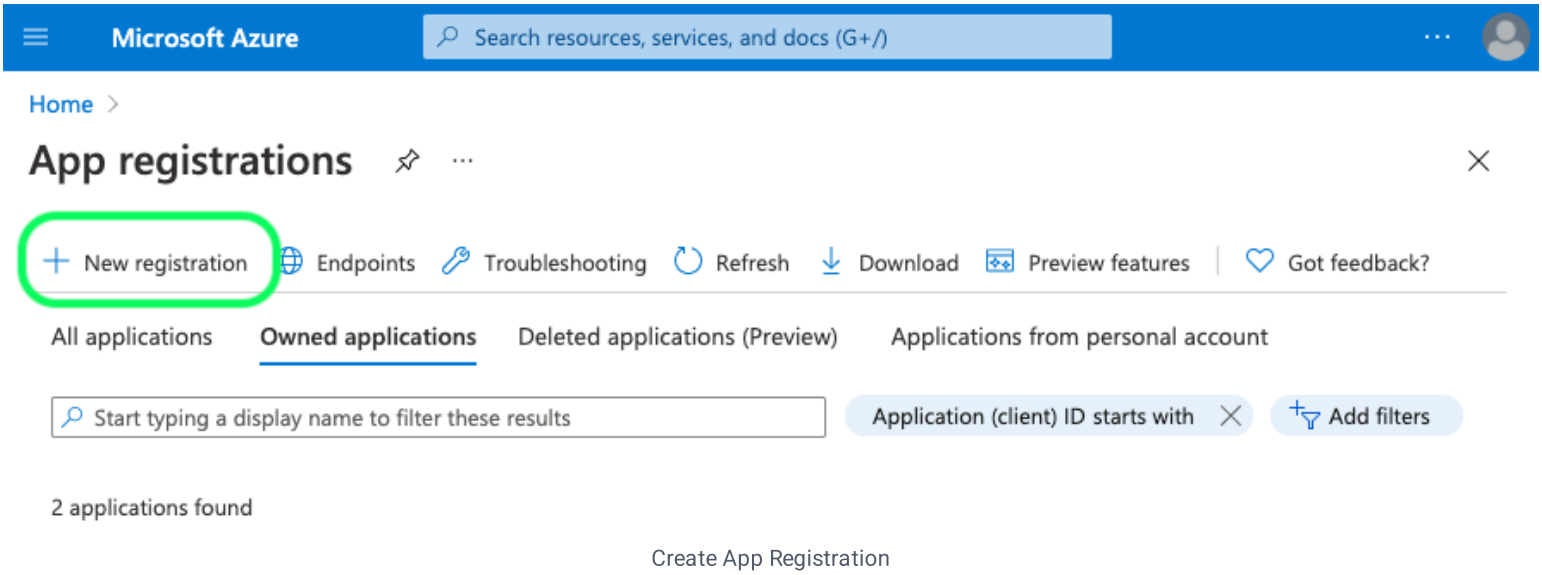
OIDC設定

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。それ以外の場合、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。

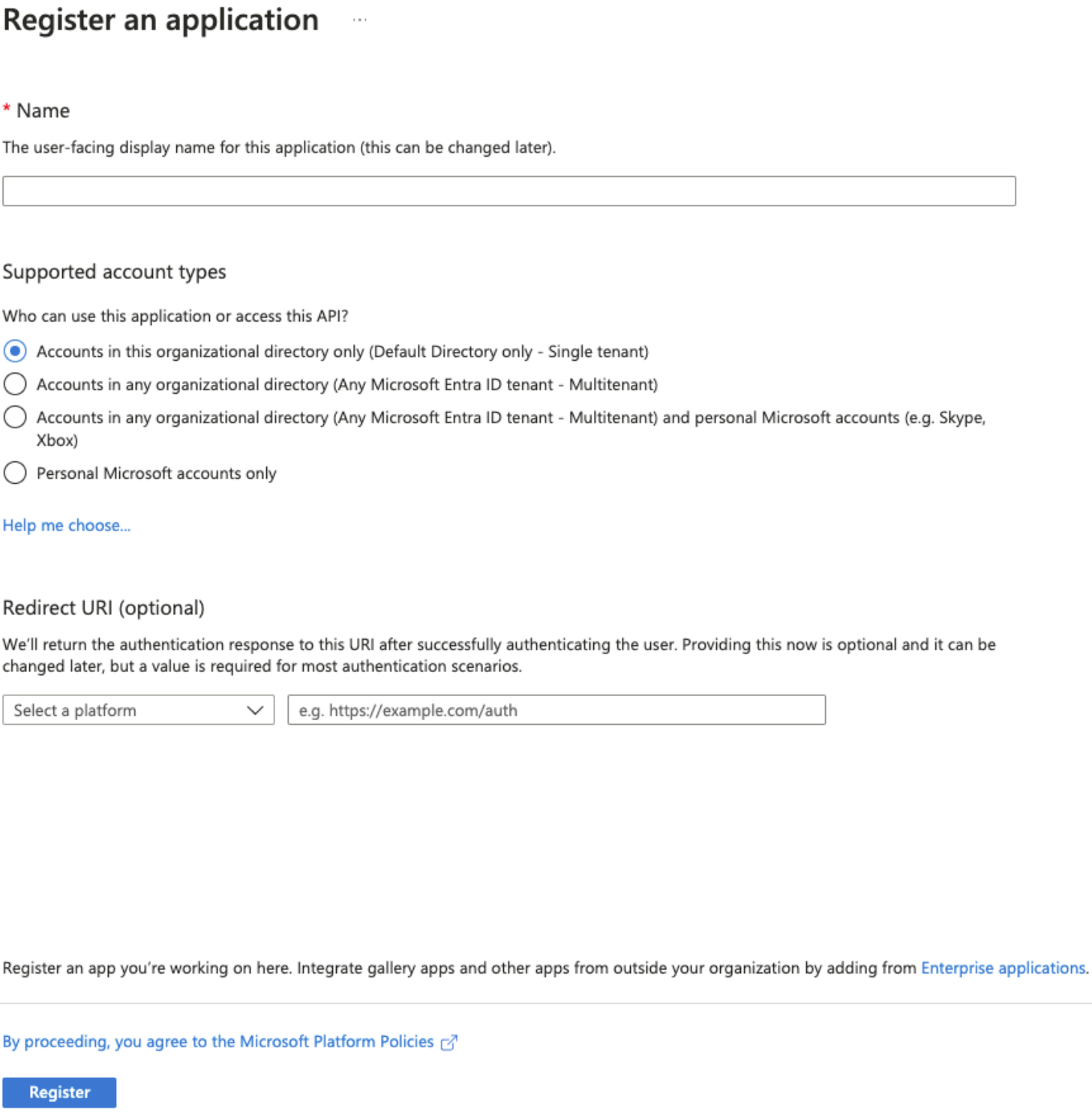
> **Tip**
> 代替の**メンバー復号化オプション**があります。信頼できるデバイスでのSSOの使い方またはキーコネクターの使い方を学びましょう。

アプリ登録を作成する

Azure Portalで、**Microsoft Entra ID**に移動し、**アプリの登録を選択します。**新しいアプリ登録を作成するには、**新規登録**ボタンを選択します:



申し訳ありませんが、翻訳するフィールドが指定されていません。具体的なフィールドを提供していただけますか？



Register redirect URI

1. **アプリケーションを登録する**画面で、あなたのアプリにBitwarden特有の名前を付け、
   どのアカウントがアプリケーションを使用できるかを指定してください。この選択は、
   どのユーザーがSSOを使用してBitwardenにログインできるかを決定します。

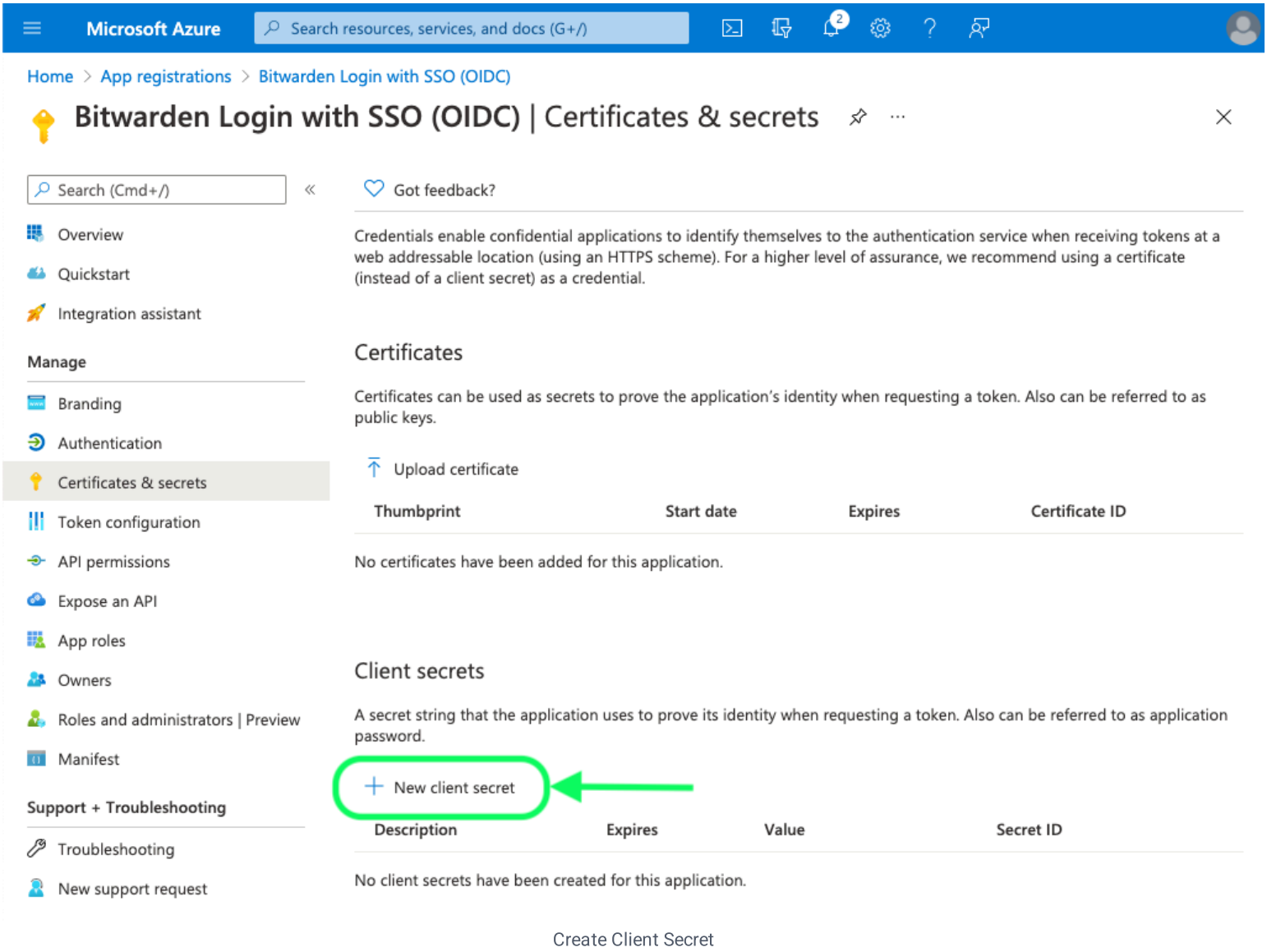
2. ナビゲーションから**認証**を選択し、**プラットフォームを追加**ボタンを選択してください。

3. 「プラットフォームの設定」画面で**Web**オプションを選択し、リダイレクトURI入力に**コールバックパス**を入力してください。

> **ⓘ Note**
>
> Callback Path can be retrieved from the Bitwarden SSO Configuration screen. For cloud-hosted customers, this is `https://sso.bitwarden.com/oidc-signin` or `https://sso.bitwarden.eu/oidc-signin`. For self-hosted instances, this is determined by your configured server URL, for example `https://your.domain.com/sso/oidc-signin`.

クライアントシークレットを作成します

ナビゲーションから**証明書とシークレット**を選択し、**新しいクライアントシークレット**ボタンを選択します：



証明書にBitwarden固有の名前を付け、有効期限の時間枠を選択してください。

管理者の同意を作成する

API 権限を選択し、✓ **デフォルトディレクトリの管理者同意を付与**をクリックします。必要な唯一の権限はデフォルトで追加され、Microsoft Graph > User.Readです。

ウェブアプリに戻る

この時点で、Azure Portal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	`https://login.microsoft.com//v2.0`にアクセスしてください。ここで、`TENANT_ID`はアプリ登録の概要画面から取得した**ディレクトリ（テナント）ID**の値です。
クライアントID	アプリ登録の**アプリケーション（クライアント）ID**を入力してください。これは概要画面から取得できます。
クライアントシークレット	**シークレットバリュー**を入力してください。作成されたクライアントシークレットの。
メタデータアドレス	文書化されたAzureの実装については、このフィールドを空白のままにしていただいて構いません。
OIDCリダイレクトの挙動	**フォーム POST** または**リダイレクト GET**を選択してください。
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、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。

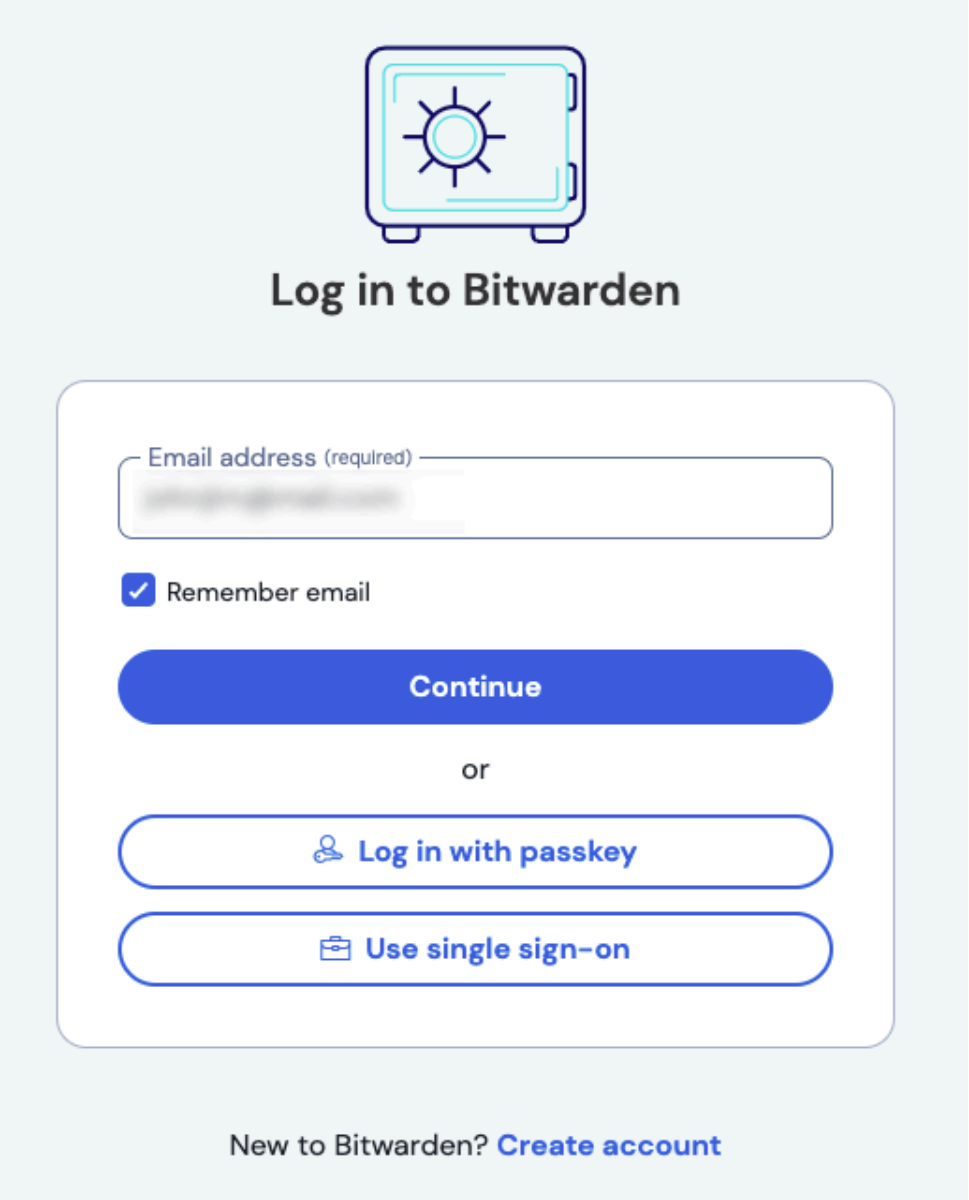
フィールド	説明
追加/カスタム名前クレームタイプ	ユーザーのフルネームまたは表示名のためのカスタムクレームタイプキーを定義します（カンマ区切り）。定義された場合、カスタムクレームのタイプは、標準のタイプに戻る前に検索されます。
要求された認証コンテキストクラス参照値	認証コンテキストクラス参照識別子（`acr_values`）（スペース区切り）を定義してください。`acr_values`を優先順位でリストアップしてください。
応答で期待される "acr" 請求値	Bitwardenがレスポンスで期待し、検証する`acr`クレーム値を定義してください。

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

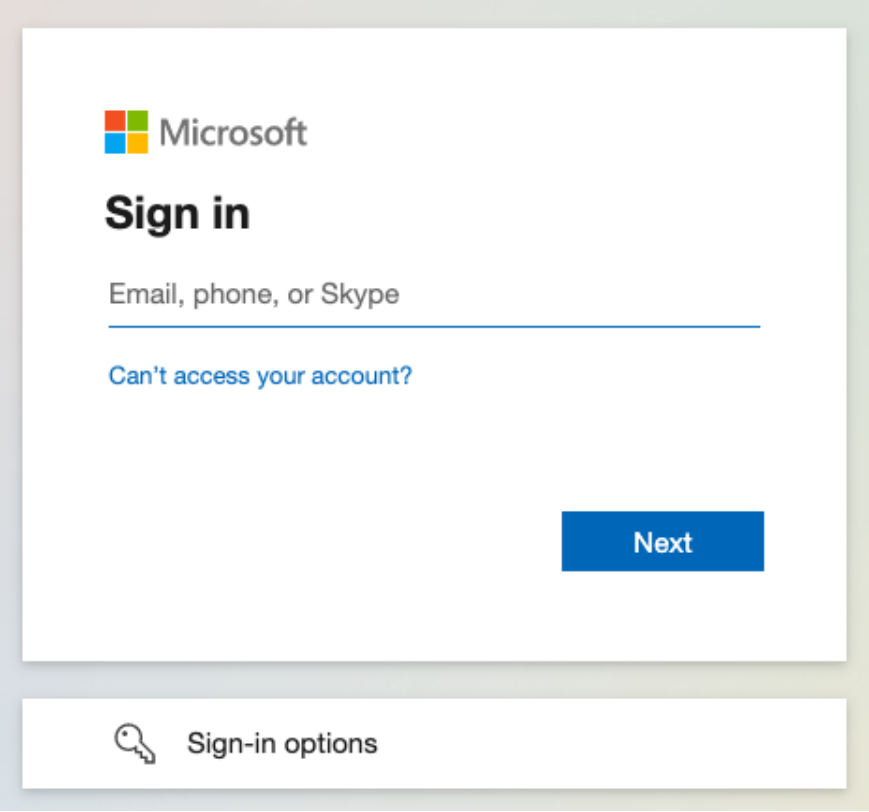
設定をテストする

設定が完了したら、https://vault.bitwarden.comに移動してテストを行います。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**ボタンを選択します。



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、Microsoftのログイン画面にリダイレクトされます。



Azure login screen

あなたのAzure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は勝手なレスポンスをサポートしていませんので、あなたのIdPからログインを開始するとエラーが発生します。
> SSOログインフローはBitwardenから開始されなければなりません。

次のステップ

1. あなたの組織のメンバーに、SSOを使用したログインの使い方を教えてください。