

管理者コンソール > SSOでログイン > 実装ガイド

# Microsoft Entra ID OIDC 実装

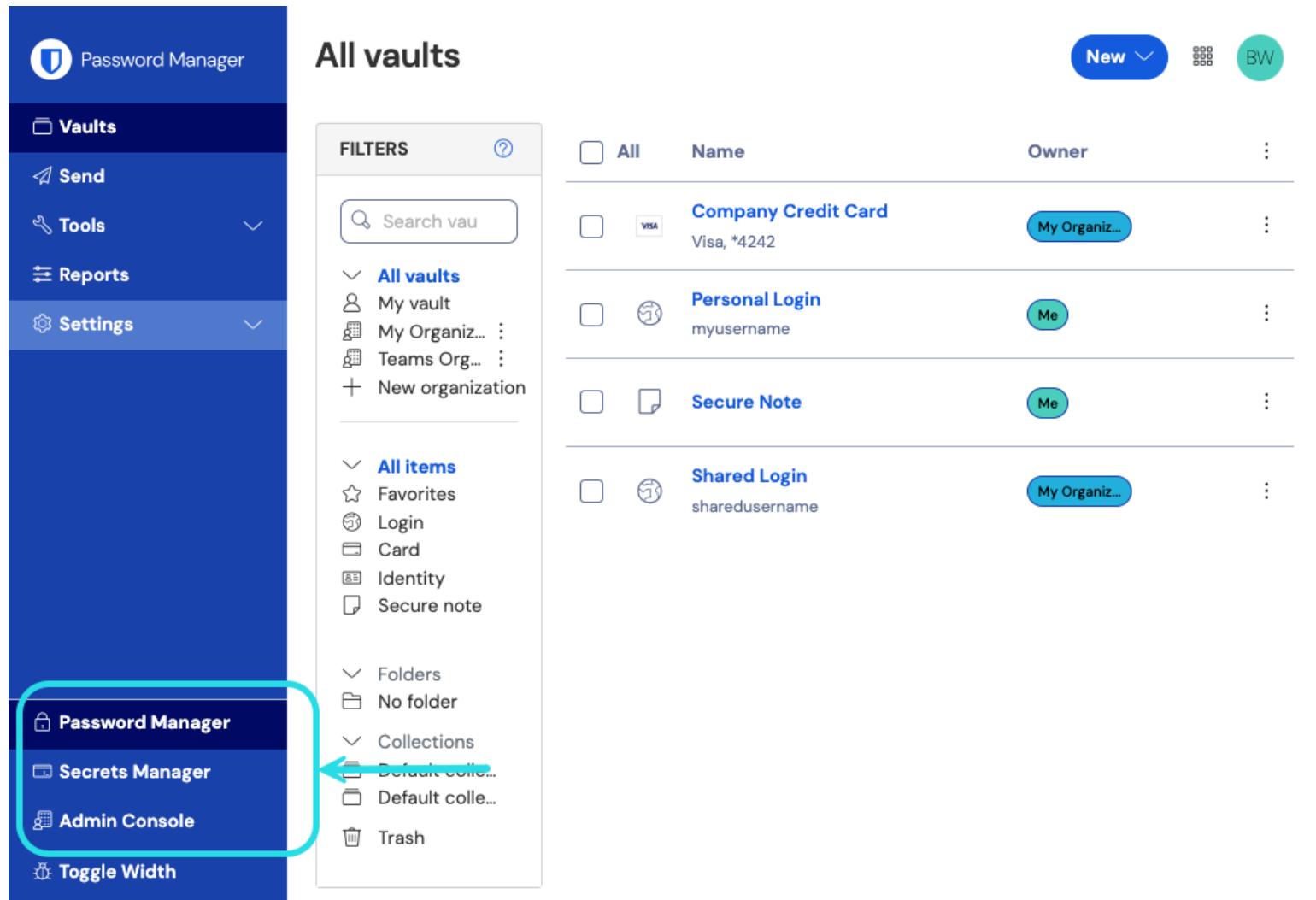
## Microsoft Entra ID OIDC 実装

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。



The screenshot shows the Bitwarden web application interface. On the left, there is a sidebar with a 'Password Manager' section highlighted by a red box. Below this, there are links for 'Secrets Manager' and 'Admin Console'. The main area is titled 'All vaults' and contains a list of vaults. A red arrow points to the 'Default collection' under the 'Collections' section in the left sidebar.

| Filters          | Name                | Owner         |
|------------------|---------------------|---------------|
| All vaults       | Company Credit Card | My Organiz... |
| My vault         | Personal Login      | Me            |
| My Organiz...    | Secure Note         | Me            |
| Teams Org...     | Shared Login        | My Organiz... |
| New organization |                     |               |

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。

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

Signed out callback path

## 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:

 Microsoft Azure

Home >

## App registrations

 New registration

 Endpoints

 Troubleshooting

 Refresh

 Download

 Preview features

 Got feedback?

All applications Owned applications Deleted applications (Preview) Applications from personal account

Application (client) ID starts with   Add filters

2 applications found

Create App Registration

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 an application ...

### \* Name

The user-facing display name for this application (this can be changed later).

### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

▼

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#) ↗

Register

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：

Home > App registrations > Bitwarden Login with SSO (OIDC)

### Bitwarden Login with SSO (OIDC) | Certificates & secrets

Search (Cmd+/) << Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
  - Branding
  - Authentication
  - Certificates & secrets**
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators | Preview
  - Manifest
- Support + Troubleshooting
  - Troubleshooting
  - New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

#### Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

| Thumbprint                                            | Start date | Expires | Certificate ID |
|-------------------------------------------------------|------------|---------|----------------|
| No certificates have been added for this application. |            |         |                |

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

| Description                                               | Expires | Value | Secret ID |
|-----------------------------------------------------------|---------|-------|-----------|
| No client secrets have been created for this application. |         |       |           |

Create Client Secret

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                       | <a href="https://login.microsoft.com/v2.0">https://login.microsoft.com/v2.0</a> にアクセスしてください。ここで、 <b>TENANT_ID</b> はアプリ登録の概要画面から取得した <b>ディレクトリ（テナント）ID</b> の値です。 |
| クライアントID                 | アプリ登録の <b>アプリケーション（クライアント）ID</b> 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             | <b>シークレットバリュー</b> を入力してください。 <a href="#">作成されたクライアントシークレット</a> 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ないでください。                                                                                                                     |
| OIDCリダイレクトの挙動            | <b>フォーム POST</b> または <b>リダイレクト GET</b> 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（ <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。                                                 |

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。





## Log in to Bitwarden

Email address (required)

☒ Remember email

Continue

or

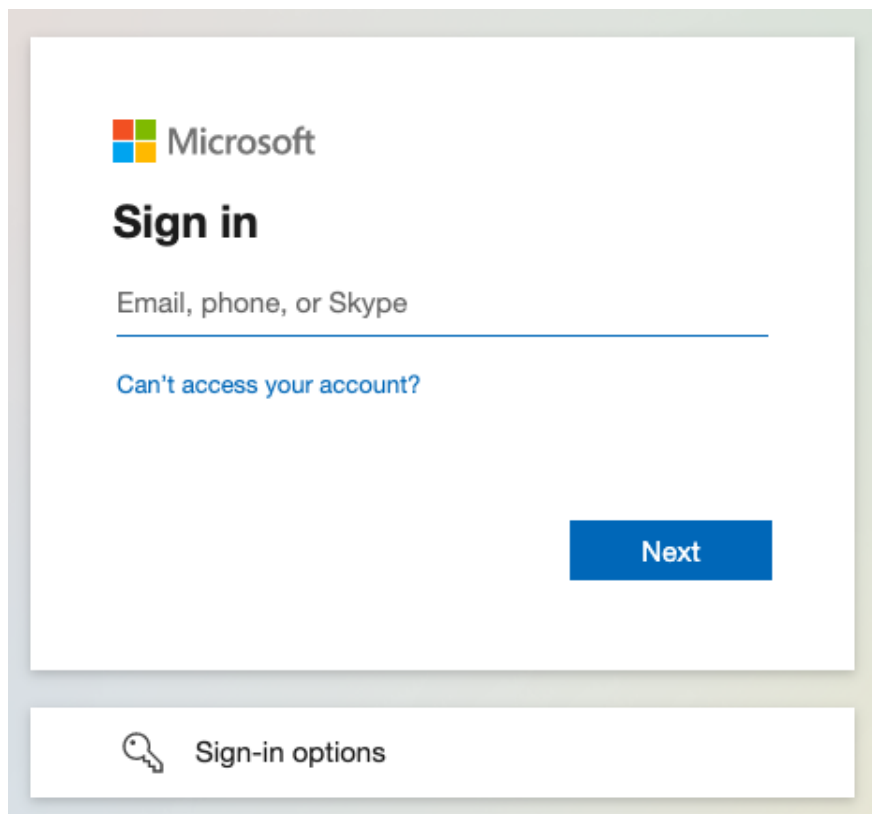
 Log in with paskey

 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、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！

#### ① Note

Bitwardenは勝手なレスポンスをサポートしていないので、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。