

管理者コンソール > SSOでログイン >

Microsoft Entra ID OIDC 実装

ヘルプセンターで表示:

<https://bitwarden.com/help/oidc-microsoft-entra-id/>

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 (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, a dark blue sidebar contains navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. A red box highlights the 'Password Manager' and 'Secrets Manager' items, with a red arrow pointing to the 'Product Switcher' icon (a grid of squares) in the 'Collections' section. The main content area is titled 'All vaults' and features a 'New' button, a product switcher icon, and a 'BW' profile icon. Below this is a table of vaults with columns for selection, name, owner, and actions.

<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

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。

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)

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 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:

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せんか？

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.

<input type="text" value="Select a platform"/>	<input type="text" value="e.g. https://example.com/auth"/>
--	--

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：

The screenshot shows the Azure portal interface for 'Bitwarden Login with SSO (OIDC) | Certificates & secrets'. The left sidebar contains navigation options like Overview, Quickstart, Integration assistant, and Manage. The main content area is divided into 'Certificates' and 'Client secrets' sections. The 'Client secrets' section is currently empty, and a green circle and arrow highlight the '+ New client secret' button.

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

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

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	<p>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。</p>
クライアントID	<p>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。</p>
クライアントシークレット	<p>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。</p>
メタデータアドレス	<p>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ください。</p>
OIDCリダイレクトの挙動	<p>フォーム POST または リダイレクト GET を選択してください。</p>
ユーザー情報エンドポイントからクレームを取得する	<p>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。</p>
追加/カスタムスコープ	<p>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)。</p>
追加/カスタムユーザーIDクレームタイプ	<p>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。</p>
追加/カスタム メールアドレス クレーム タイプ	<p>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。</p>
追加/カスタム名前クレームタイプ	<p>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。</p>

フィールド	説明
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。

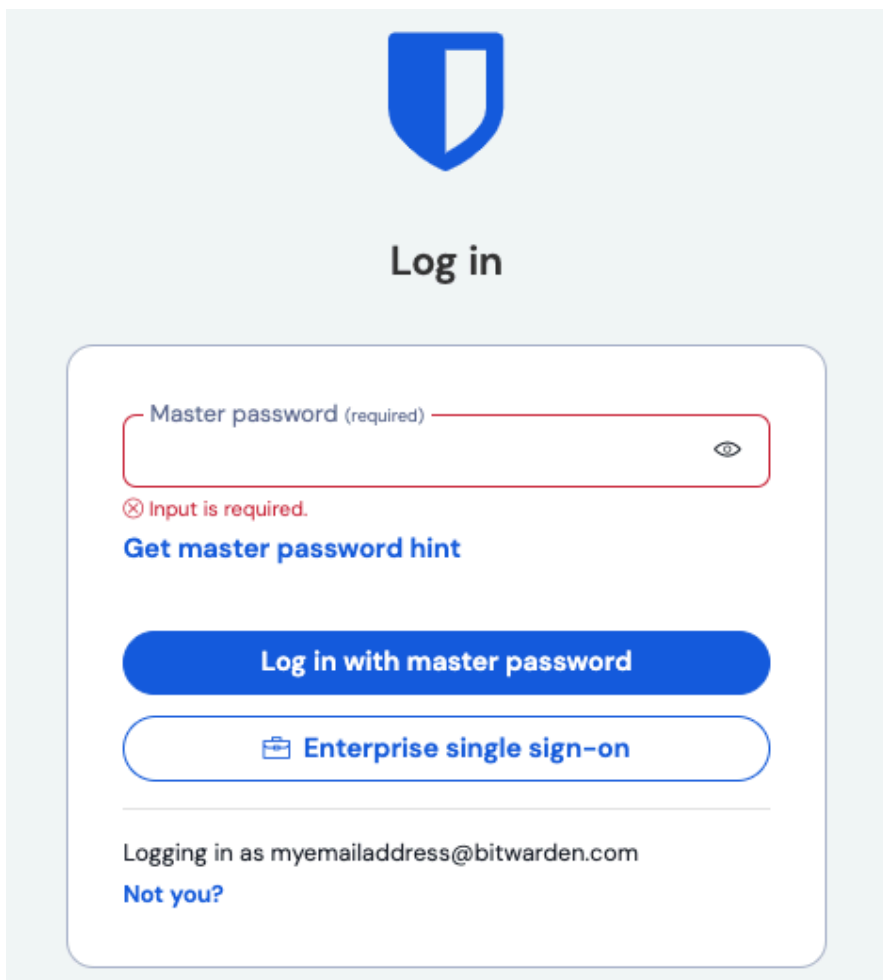
これらのフィールドの設定が完了したら、**保存**してください。

💡 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](#)

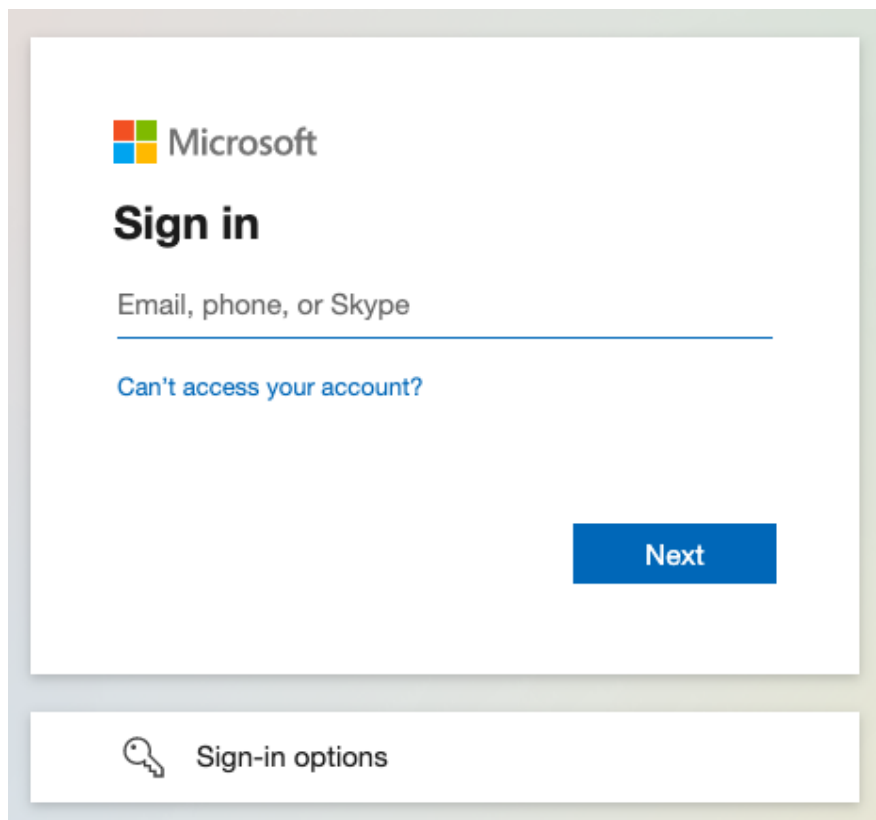
設定をテストする

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。



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は勝手の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。