

管理者コンソール > SSOでログイン >

Ping Identity OIDC Implementation

ヘルプセンターで表示:

<https://bitwarden.com/help/ping-identity-oidc-implementation/>

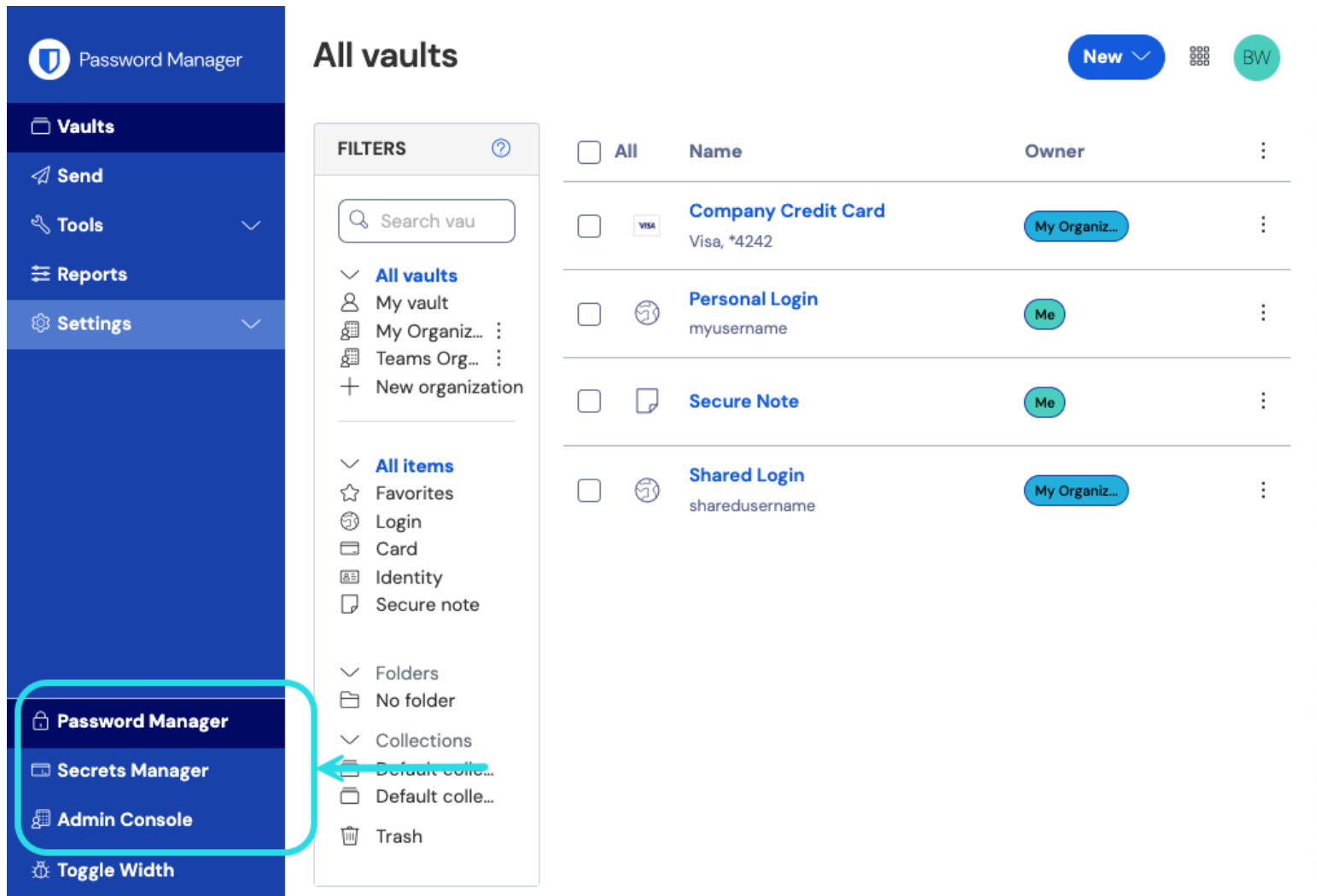
Ping Identity OIDC Implementation

This article contains Ping Identity specific help for configuring Login with SSO via OpenID Connect (OIDC). For help configuring Login with SSO for another OIDC IdP, or for configuring Ping Identity via SAML 2.0, see [OIDC Configuration](#) or [Ping Identity SAML implementation](#).

Configuration involves working simultaneously within the Bitwarden web app and the Ping Identity Administrator Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

Open SSO in the web vault

Log in to the Bitwarden [web app](#) and open the Admin Console using the product switcher:



製品-スイッチャー

Select **Settings** → **Single sign-on** from the navigation:

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

If you haven't already, create a unique **SSO identifier** for your organization. Otherwise, you don't need to edit anything on this screen yet, but keep it open for easy reference.



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。

Create OIDC app

In the Ping Identity Administrator Portal, select **Applications** and the ⊕ icon at the top of the screen to open the **Add Application** screen:

Add Application



Application Name *

Bitwarden SSO

Description

Icon



Max Size 1.0 MB

Application Type

Show Details



Select an option below or view the [Application Catalog](#) to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.



SAML Application



OIDC Web App



Native



Single-Page



Worker



Device Authorization

Save

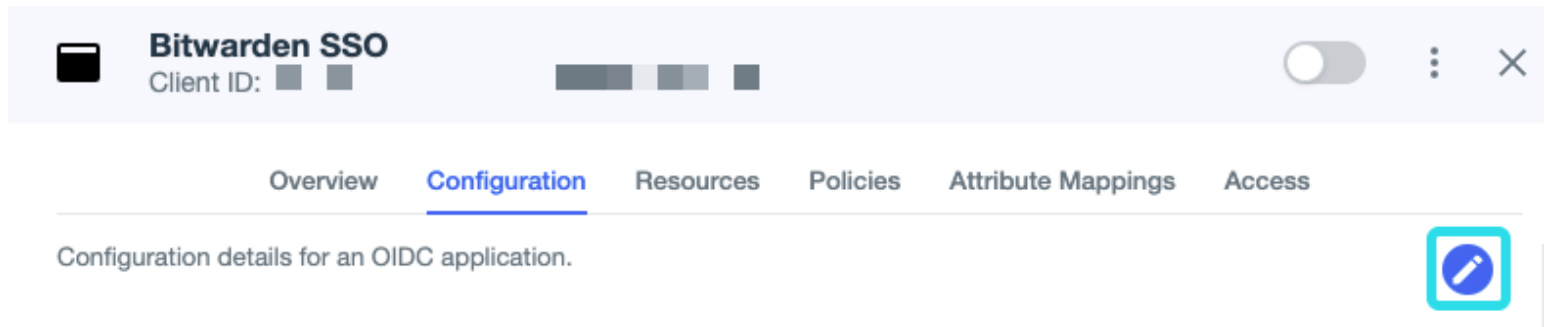
Cancel

*Ping Identity OIDC App***Add application**

1. Enter a Bitwarden Specific name in the **Application Name** field. Optionally, add desired description details as needed.
2. Select the **OIDC Web App** option and select **Save** once you have finished.

Configure application

On the Application screen, select the **Configuration** tab and then the edit button located on the top right hand of the screen.

*Ping OIDC Configuration Edit*

In the edit screen, fill in the following values retrieved from the Bitwarden Single sign-on screen:

Ping Identity Field	Description
Redirect URIs	Copy and paste the Callback path value retrieved from the Bitwarden Single sign-on page.
Signoff URLs	Copy and Paste the Signed out callback path value retrieved from the Bitwarden Single sign-on page.

Once this step has been completed, select **Save** and return to the **Configuration** tab on the Ping Identity Application screen. No other values on this screen require editing.

Resources

On the Resources tab of the Ping Identity Application screen, select the **edit** icon and enable the following allowed scopes:

- email
- openid

Back to the web app

At this point, you have configured everything you need within the context of Ping Identity. Return to the Bitwarden web app to configure the following fields:

Field	Description
Authority	Enter <code>https://auth.pingone.eu/<TENANT_ID></code> , where <code>TENANT_ID</code> is the Environment ID on Ping Identity.
Client ID	Enter the App's Client ID retrieved from the Application's Configuration tab.
Client Secret	Enter the Secret Value of the created client secret. Select Generate New Secret on the application's Configuration tab.
Metadata Address	For Ping Identity implementations as documented, you can leave this field blank.
OIDC Redirect Behavior	Select either Form POST or Redirect GET .
Get Claims From User Info Endpoint	Enable this option if you receive URL too long errors (HTTP 414), trusted URLs, and/or failures during SSO.
Additional/Custom Scopes	Define custom scopes to be added to the request (comma-delimited).
Additional/Custom Email Claim Types	Define custom claim type keys for users' email addresses (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Additional/Custom Name Claim Types	Define custom claim type keys for users' full names or display names (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Requested Authentication Context Class Reference values	Define Authentication Context Class Reference identifiers (<code>acr_values</code>) (space-delimited). List <code>acr_values</code> in preference-order.
Expected "acr" Claim Value in Response	Define the <code>acr</code> Claim Value for Bitwarden to expect and validate in the response.

When you are done configuring these fields, **Save** your work.

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

Test the configuration

Once your configuration is complete, test it by navigating to <https://vault.bitwarden.com>, entering your email address, selecting **Continue**, and selecting the **Enterprise single sign-on** button:

Master password (required)

⊗ Input is required.

[Get master password hint](#)

Log in with master password

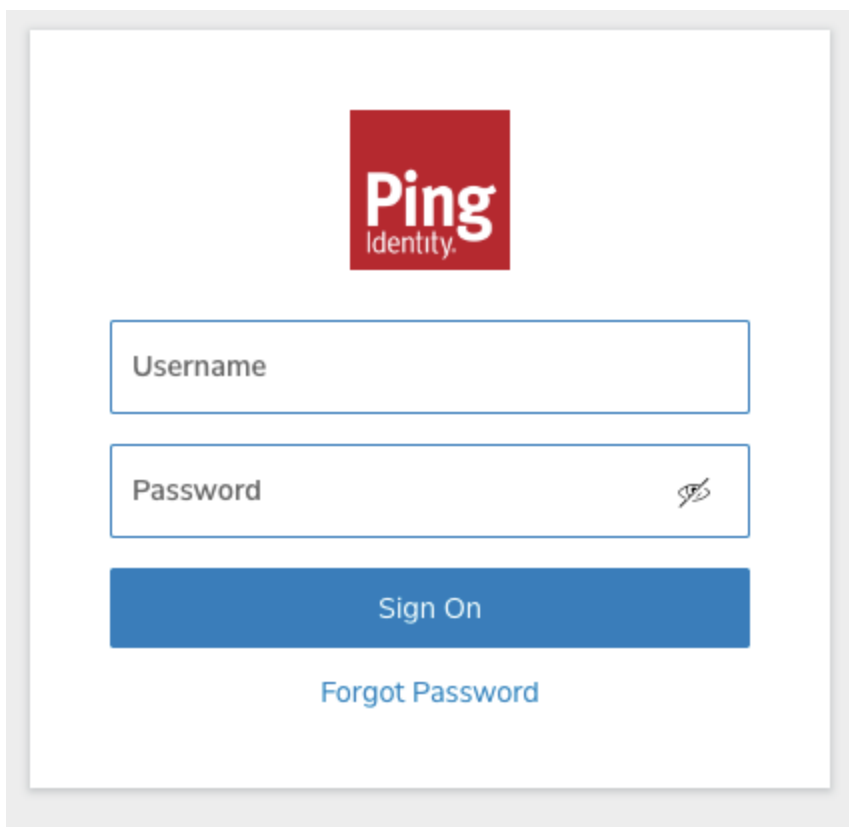
Enterprise single sign-on

Logging in as myemailaddress@bitwarden.com

[Not you?](#)

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

Enter the configured organization identifier and select **Log In**. If your implementation is successfully configured, you will be redirected to the Ping Identity login screen:



Ping Identity SSO

After you authenticate with your Ping credentials, enter your Bitwarden master password to decrypt your vault!

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。

Next steps

- Educate your organization members on how to [use login with SSO](#).