

ADMIN CONSOLE > LOGIN WITH SSO >

Microsoft Entra ID OIDC Implementation

View in the help center:

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

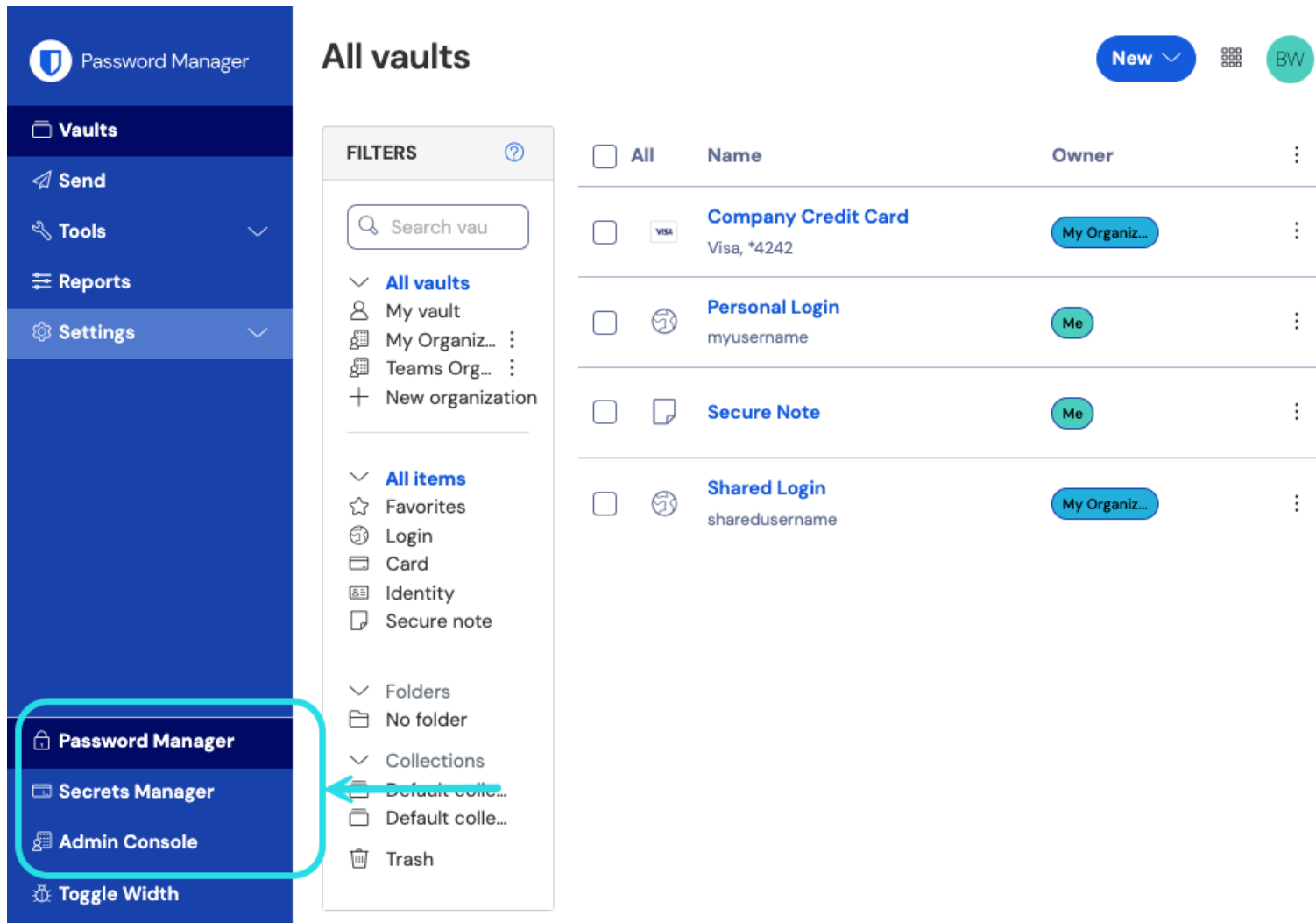
Microsoft Entra ID OIDC Implementation

This article contains **Azure-specific** help for configuring Login with SSO via OpenID Connect (OIDC). For help configuring Login with SSO for another OIDC IdP, or for configuring Microsoft Entra ID via SAML 2.0, see [OIDC Configuration](#) or [Microsoft Entra ID SAML Implementation](#).

Configuration involves working simultaneously within the Bitwarden web app and the Azure 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:



Product switcher

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 configuration

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.



There are alternative **Member decryption options**. Learn how to get started using [SSO with trusted devices](#) or [Key Connector](#).

Create an app registration

In the Azure Portal, navigate to **Microsoft Entra ID** and select **App registrations**. To create a new app registration, select the **New registration** button:

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](#)

Complete the following fields:

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.

Select a platform 	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. On the **Register an application** screen, give your app a Bitwarden-specific name and specify which accounts should be able to use the application. This selection will determine which users can use Bitwarden login with SSO.
2. Select **Authentication** from the navigation and select the **Add a platform** button.

3. Select the **Web** option on the Configure platforms screen and enter your **Callback Path** in the Redirect URIs input.

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>.

Create a client secret

Select **Certificates & secrets** from the navigation, and select the **New client secret** button:

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure' and a search bar. The breadcrumb trail is 'Home > App registrations > Bitwarden Login with SSO (OIDC)'. The main heading is 'Bitwarden Login with SSO (OIDC) | Certificates & secrets'. On the left, a navigation pane lists various management options, with 'Certificates & secrets' selected. The main content area is divided into two sections: 'Certificates' and 'Client secrets'. The 'Certificates' section includes a description, an 'Upload certificate' button, and a table with columns 'Thumbprint', 'Start date', 'Expires', and 'Certificate ID'. Below this, it states 'No certificates have been added for this application.' The 'Client secrets' section includes a description and a '+ New client secret' button, which is highlighted with a green circle and a green arrow pointing to it. Below this, it states 'No client secrets have been created for this application.' At the bottom of the page, there is a link that says 'Create Client Secret'.

Give the certificate a Bitwarden-specific name, and choose an expiration timeframe.

Create admin consent

Select **API permissions** and click ✓ **Grant admin consent for {your directory}**. The only permission needed is added by default, Microsoft Graph > User.Read.

Back to the web app

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

Field	Description
Authority	Enter <code>https://login.microsoftonline.com/<TENANT_ID>/v2.0</code> , where TENANT_ID is the Directory (tenant) ID value retrieved from the app registration's Overview screen.
Client ID	Enter the App registration's Application (client) ID , which can be retrieved from the Overview screen.
Client Secret	Enter the Secret Value of the created client secret .
Metadata Address	For Azure 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), truncated URLs, and/or failures during SSO.
Additional/Custom Scopes	Define custom scopes to be added to the request (comma-delimited).
Additional/Custom User ID Claim Types	Define custom claim type keys for user identification (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
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.

Field	Description
Requested Authentication Context Class Reference values	Define Authentication Context Class Reference identifiers (acr_values) (space-delimited). List acr_values in preference-order.
Expected "acr" Claim Value in Response	Define the acr Claim Value for Bitwarden to expect and validate in the response.

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

Tip

You can require users to log in with SSO by activating the single sign-on authentication policy. Please note, this will require activating the single organization policy as well. [Learn more.](#)

Additional custom claim types

If your SSO configuration requires custom claim types, additional steps are required in order for Microsoft Entra ID to recognize the non-standard claims.

1. On Microsoft Entra ID, add a custom claim type by navigating to **Enterprise applications** → **App registrations** → **Token configuration**.
2. Select **+ Add optional claim** and create a new optional claim with a selected value.

The screenshot shows the Microsoft Entra ID 'Token configuration' page. On the left is a navigation pane with 'Token configuration' selected. The main area shows 'Optional claims' with a table containing no results. A '+ Add optional claim' button is highlighted. A modal dialog titled 'Add optional claim' is open on the right. It shows 'Token type' set to 'ID' and a list of claims. The 'upn' claim is selected with a checkmark.

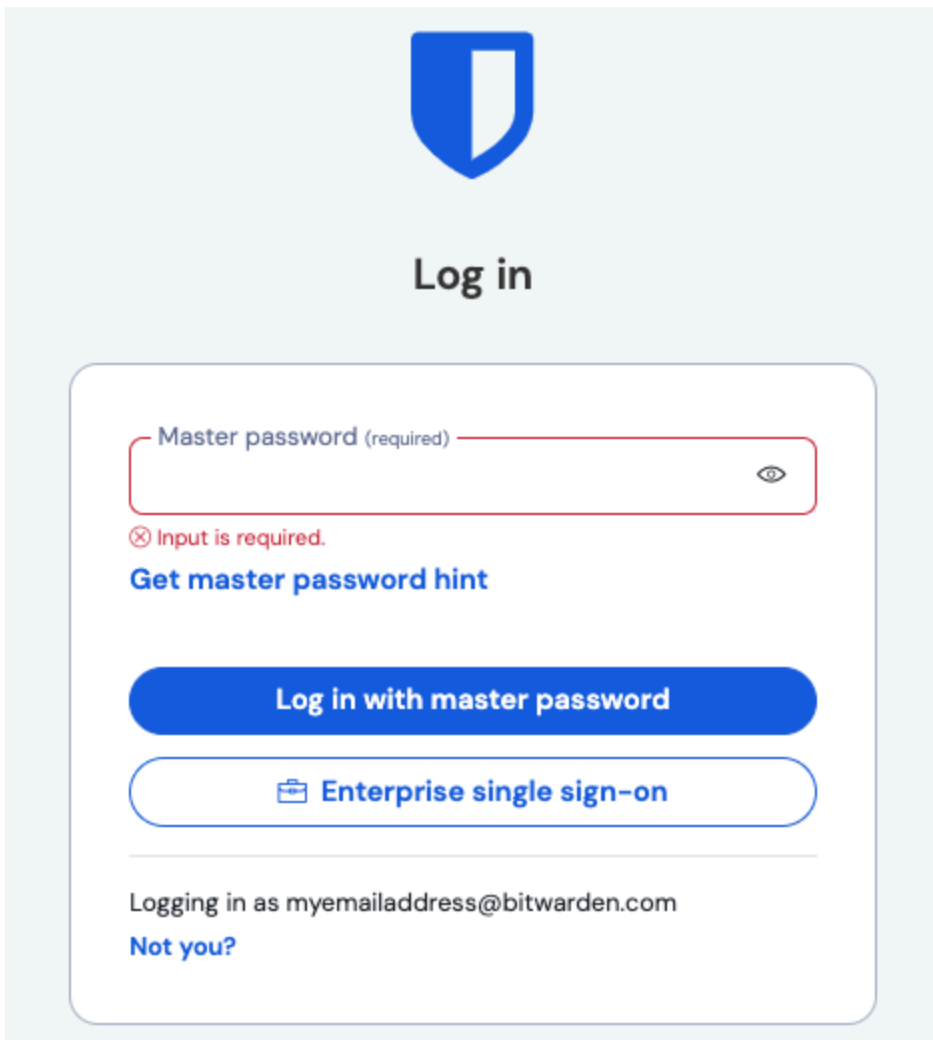
Claim	Description
<input type="checkbox"/> pwo_uri	A URL that the user can visit to change their password
<input type="checkbox"/> sid	Session ID, used for per-session user sign out
<input type="checkbox"/> tenant_ctry	Resource tenant's country/region
<input type="checkbox"/> tenant_region_scope	Region of the resource tenant
<input checked="" type="checkbox"/> upn	An identifier for the user that can be used with the user...
<input type="checkbox"/> verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
<input type="checkbox"/> verified_secondary_email	Sourced from the user's SecondaryAuthoritativeEmail
<input type="checkbox"/> vnet	VNET specifier information
<input type="checkbox"/> xms_cc	Whether the application can handle claims challenges
<input type="checkbox"/> xms_pdl	Preferred data location

Microsoft Entra ID custom claim

3. On the Bitwarden SSO configuration screen, enter the fully qualified path for a custom claim field in the corresponding **custom claim types** field. For example: <https://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn>.
4. Select **Save** once you have completed the configuration.

Test the configuration

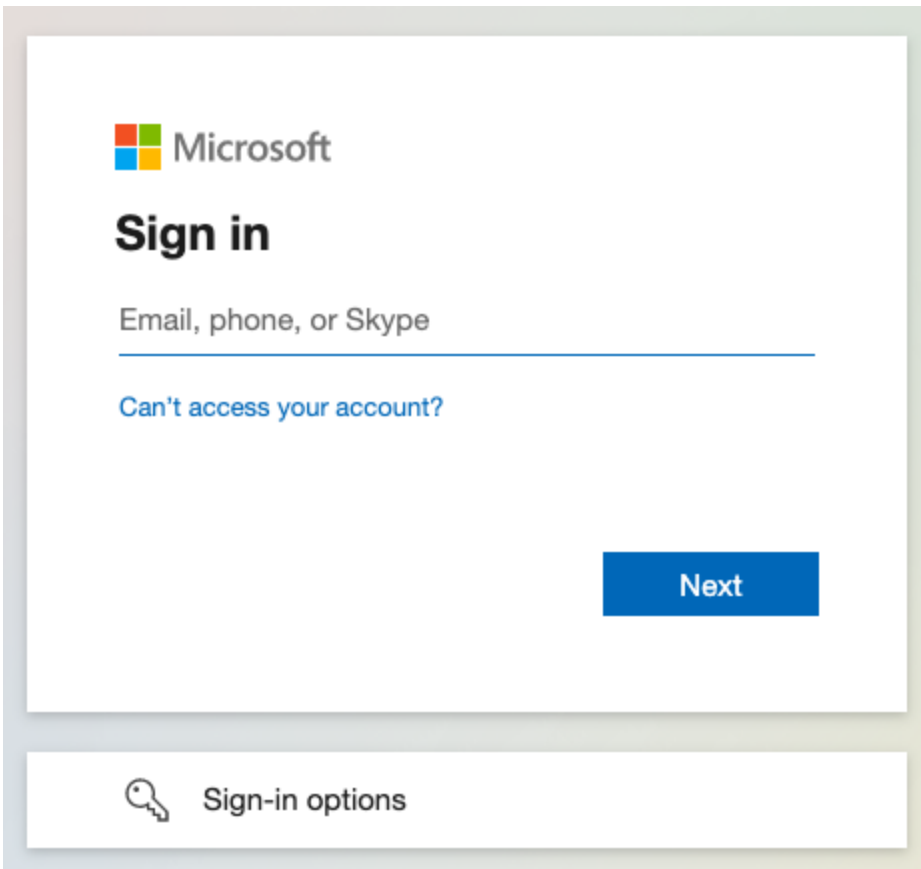
Once your configuration is complete, test it by navigating to <https://vault.bitwarden.com>, entering your email address, selecting **Continue**, and selecting the **Enterprise Single-On** button:



The screenshot shows the Bitwarden login interface. At the top is the Bitwarden logo and the text "Log in". Below this is a form with a "Master password (required)" input field. The input field is empty and has a red border, with a red error message "Input is required." below it. To the right of the input field is an eye icon. Below the input field is a link "Get master password hint". There are two buttons: "Log in with master password" and "Enterprise single sign-on". At the bottom, it says "Logging in as myemailaddress@bitwarden.com" and a link "Not you?".

Log in options screen

Enter the [configured organization identifier](#) and select **Log In**. If your implementation is successfully configured, you will be redirected to the Microsoft login screen:



Azure login screen

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

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.

Next steps

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