

ADMIN CONSOLE > LOGGA IN MED SSO >

Microsoft Entra ID OIDC Implementation

View in the help center:
<https://bitwarden.com/help/oidc-microsoft-entra-id/>

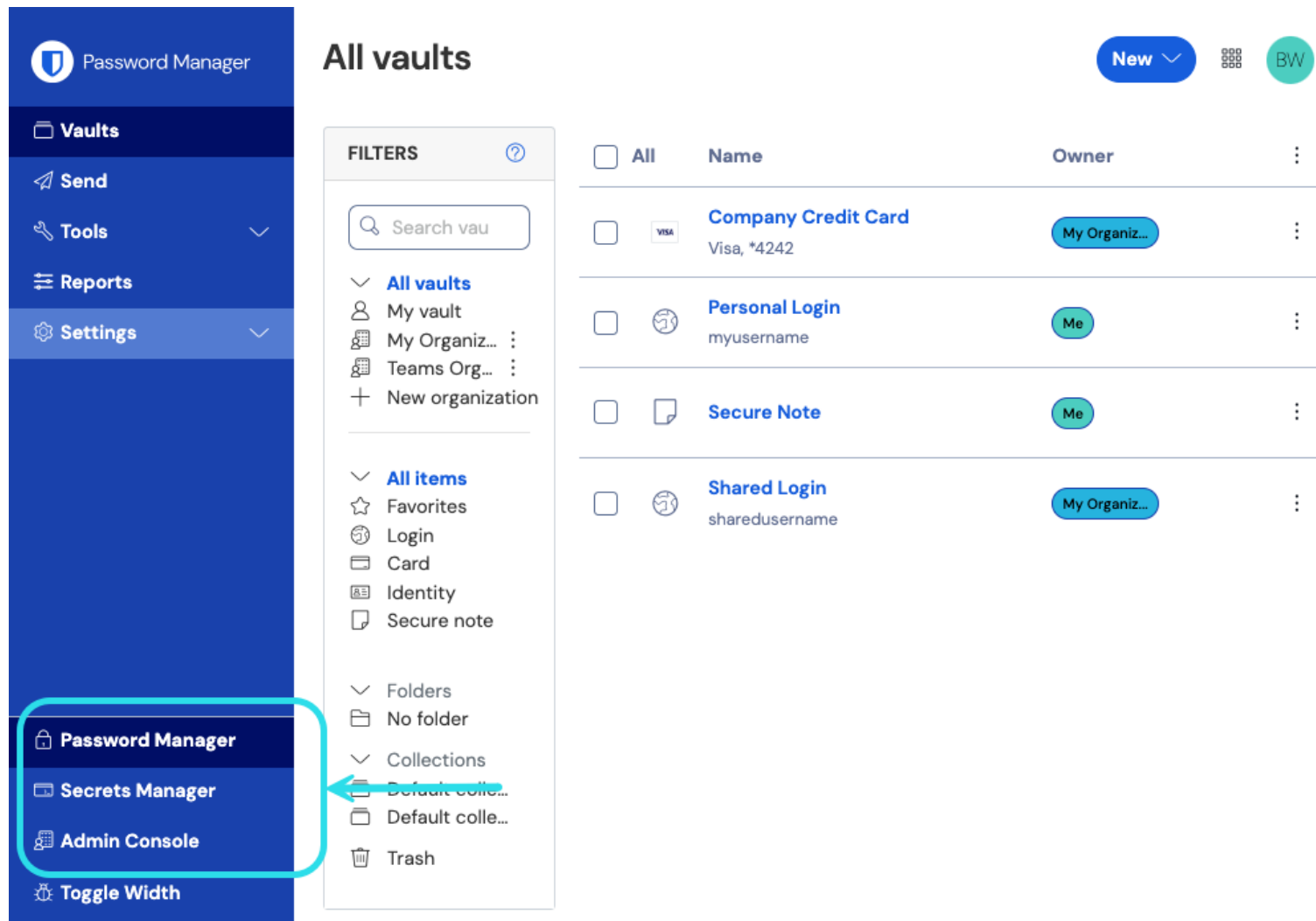
Microsoft Entra ID OIDC Implementation

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:



The screenshot displays the Bitwarden web app interface. On the left, a dark blue sidebar contains navigation options: 'Password Manager', 'Vaults', 'Send', 'Tools', 'Reports', and 'Settings'. The 'Settings' option is highlighted with a red box and a red arrow. The main area shows a list of vaults under the heading 'All vaults'. The list has columns for 'Name' and 'Owner'. The 'Product switcher' is visible in the top right corner.

	Name	Owner
☐	Company Credit Card Visa, *4242	My Organiz...
☐	Personal Login myusername	Me
☐	Secure Note	Me
☐	Shared Login sharedusername	My Organiz...

Product switcher

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

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.

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.

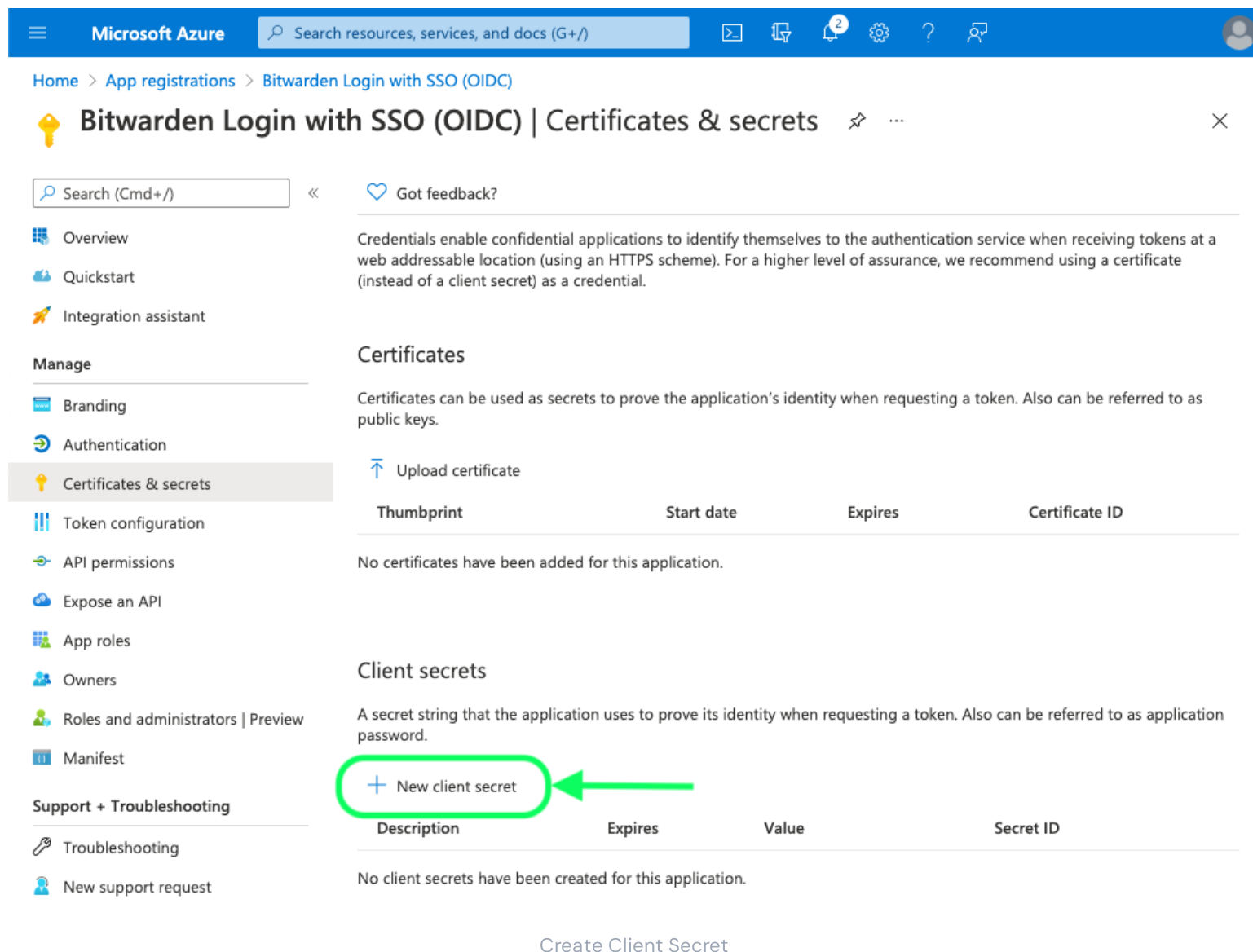
3. Select the **Web** option on the Configure platforms screen and enter your **Callback Path** in the Redirect URIs input.

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:



Microsoft Azure Search resources, services, and docs (G+)

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

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.

Field	Description
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 (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.

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens.

+ Add optional claim + Add groups claim

Claim ↑↓	Description
No results.	

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

* Token type

Access and ID tokens are used by applications for authentication. [Learn more](#)

- ☒ ID
☐ Access
☐ SAML

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

Add

Cancel

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 and selecting the **Use single sign-on** button:



Log in to Bitwarden

Email address (required)

☒ Remember email

Continue

or

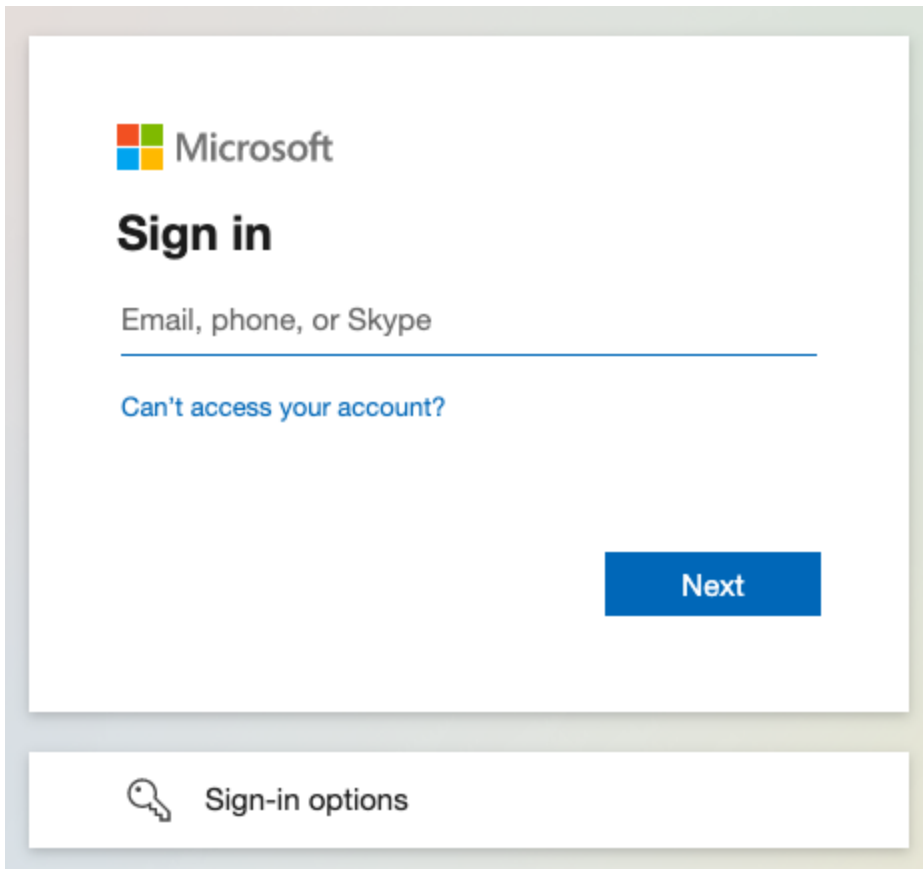
 Log in with passkey

 Use single sign-on

New to Bitwarden? [Create account](#)

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](#).