

ADMIN CONSOLE > LOGGA IN MED SSO >

Microsoft Entra ID SAML Implementation

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

Microsoft Entra ID SAML Implementation

This article contains **Azure-specific** help for configuring Login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to [SAML 2.0 Configuration](#).

Configuration involves working simultaneously with 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.

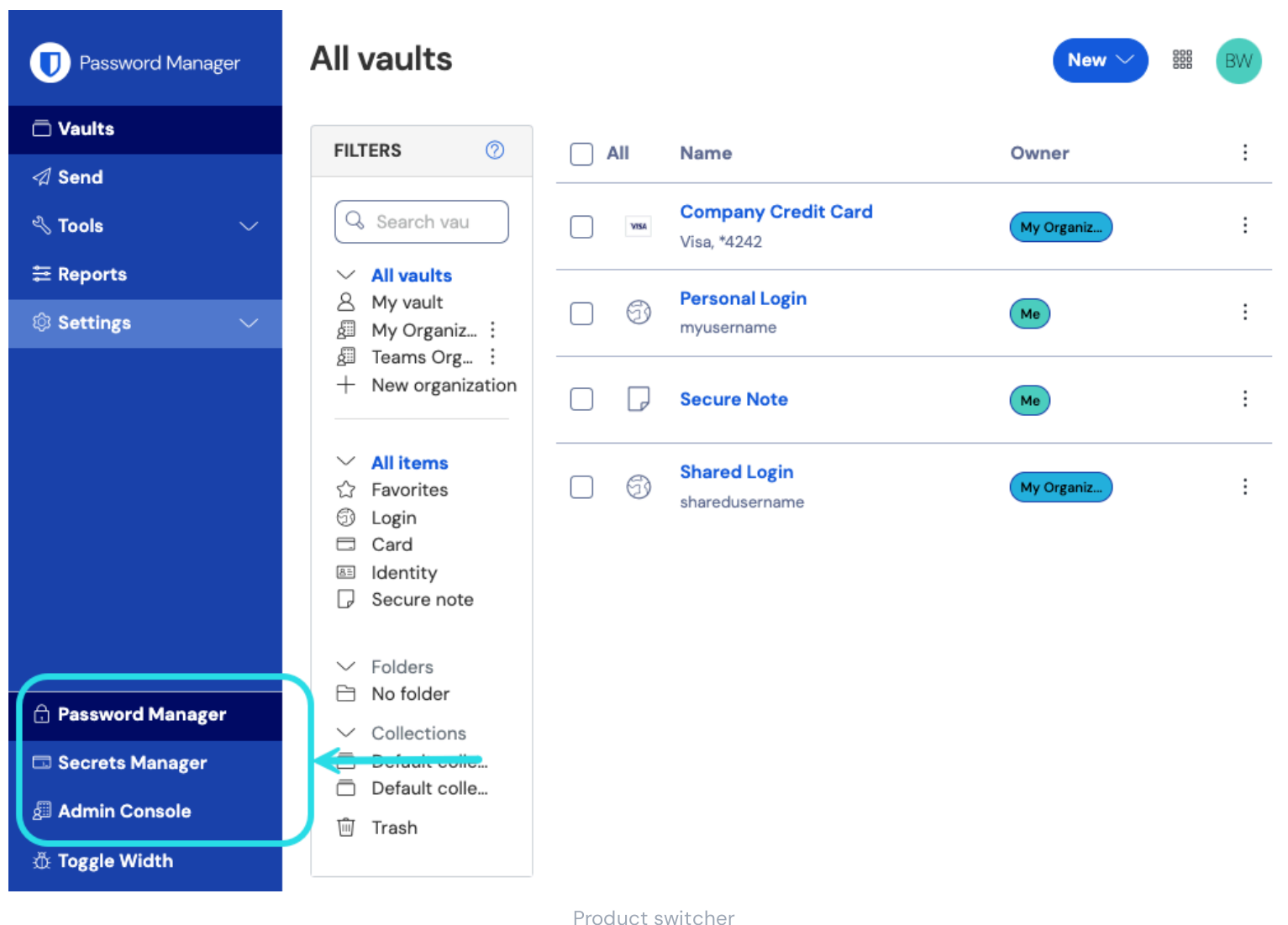


Already an expert? Skip the instructions in this article and download the quick configuration guide to setup SSO and SCIM with Entra ID.

[Quick reference guide](#)

Open SSO in the web app

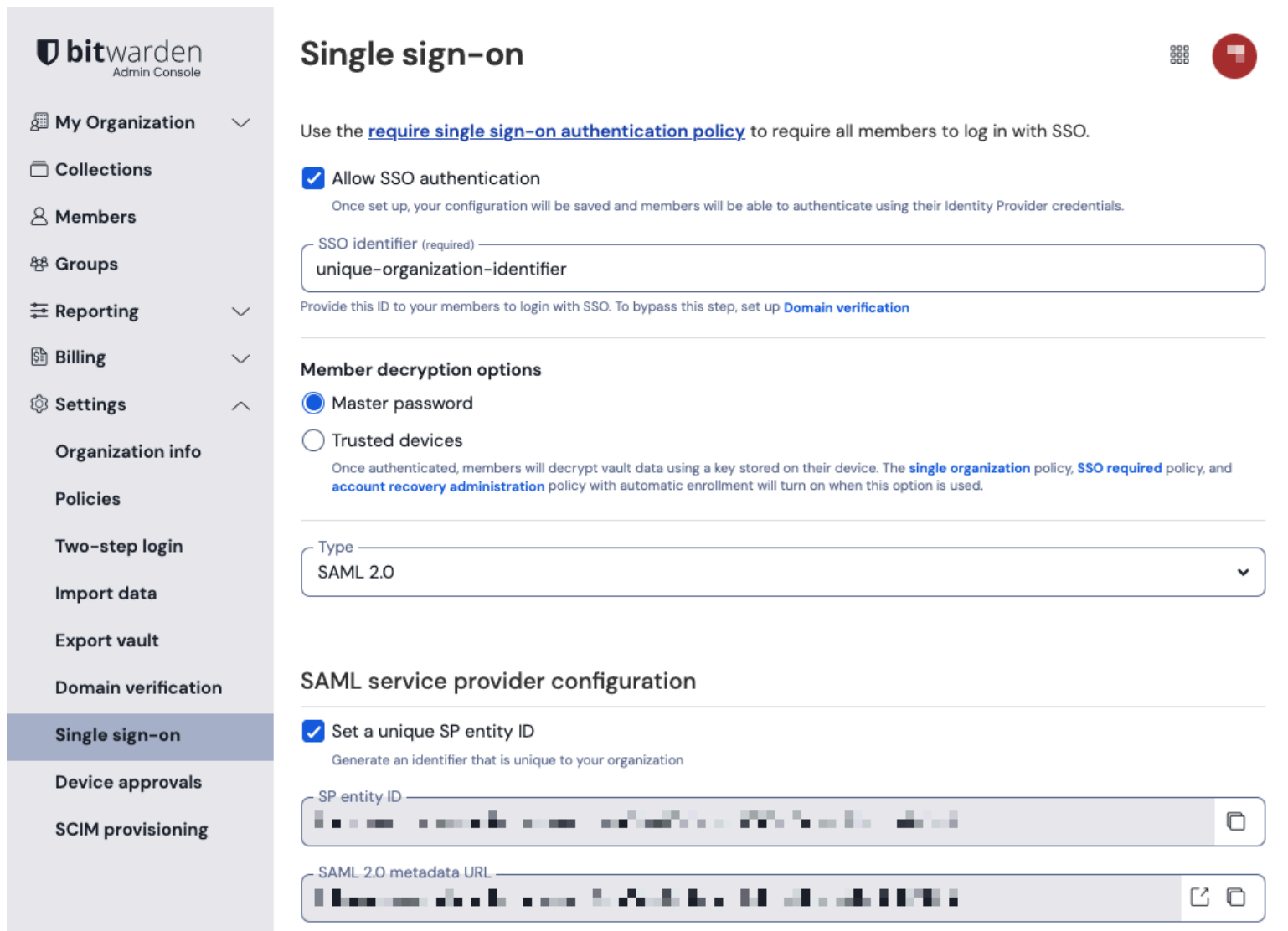
Log in to the Bitwarden web app and open the Admin Console using the product switcher:



The screenshot displays the Bitwarden web app interface. On the left is a dark blue sidebar with a 'Password Manager' header and a menu containing 'Vaults', 'Send', 'Tools', 'Reports', 'Settings', 'Password Manager', 'Secrets Manager', 'Admin Console', and 'Toggle Width'. The 'Admin Console' option is highlighted with a red box and a red arrow. The main content area is titled 'All vaults' and features a 'FILTERS' sidebar with a search bar and categories like 'All vaults', 'All items', 'Folders', 'Collections', and 'Trash'. The main list shows vaults such as 'Company Credit Card', 'Personal Login', 'Secure Note', and 'Shared Login'. In the top right corner, there is a 'New' button, a grid icon, and a circular 'Product switcher' button labeled 'BW'.

Product switcher

Open your organization's **Settings** → **Single sign-on** screen:



The screenshot shows the Bitwarden Admin Console interface. On the left is a navigation sidebar with options: My Organization, Collections, Members, Groups, Reporting, Billing, Settings, Organization info, Policies, Two-step login, Import data, Export vault, Domain verification, **Single sign-on** (selected), Device approvals, and SCIM provisioning. The main content area is titled 'Single sign-on' and includes a QR code icon and a user profile icon. The instructions state: 'Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.' There is a checked checkbox for 'Allow SSO authentication' with a note: 'Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.' Below this is a text field for 'SSO identifier (required)' containing 'unique-organization-identifier'. A note says: 'Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)'. The 'Member decryption options' section has two radio buttons: 'Master password' (selected) and 'Trusted devices'. A note explains: '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.' There is a dropdown menu for 'Type' set to 'SAML 2.0'. The 'SAML service provider configuration' section has a checked checkbox for 'Set a unique SP entity ID' with a note: 'Generate an identifier that is unique to your organization'. Below this are two text fields: 'SP entity ID' and 'SAML 2.0 metadata URL', both containing masked values and having copy icons.

SAML 2.0 configuration

If you haven't already, create a unique **SSO identifier** for your organization and select **SAML** from the the **Type** dropdown. Keep this screen open for easy reference.

You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.



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

Create an enterprise application

In the Azure Portal, navigate to **Microsoft Entra ID** and select **Enterprise applications** from the navigation menu:

[Home](#) >

Default Directory | Overview

Microsoft Entra ID

[+ Add](#) [Manage tenants](#) [What's new](#) [Preview features](#) [Got feedback?](#)

Overview Monitoring Properties Recommendations Tutorials

Basic information

Name		Users
Tenant ID		Groups
Primary domain		Applications
License		Devices

Alerts



Microsoft Entra Connect v1 Retirement

All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect v2.x.

[Learn more](#)



Azure AD is now Microsoft Entra ID

Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.

[Learn more](#)

Enterprise applications

Select the **+ New application** button:

[Home](#) > [Enterprise applications](#)

Enterprise applications | All applications

Default Directory - Microsoft Entra ID

Overview

Overview
[Diagnose and solve problems](#)

Manage

[+ New application](#)

[Refresh](#)

[Download \(Export\)](#)

[Preview info](#)

[Columns](#)

[Preview features](#)

[Got feedback?](#)

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Application type == **Enterprise Applications**

Application ID starts with

[Add filters](#)

Create new application

On the Browse Microsoft Entra ID Gallery screen, select the **+ Create your own application** button:

[Home](#) > [Default Directory](#) | [Enterprise applications](#) > [Enterprise applications](#) | [All applications](#)

Browse Microsoft Entra ID Gallery

[+ Create your own application](#)

[Got feedback?](#)

The Microsoft Entra ID App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra ID Gallery for other organizations to discover and use, you can file a request using the process described in [this article](#).

Single Sign-on : **All**

User Account Management : **All**

Categories : **All**

Create your own application

On the Create your own application screen, give the application a unique, Bitwarden-specific name and select the (Non-gallery) option. Once you are finished, click the **Create** button.

Enable single sign-on

From the Application Overview screen, select **Single sign-on** from the navigation:



On the Single Sign-On screen, select **SAML**.

SAML setup

Basic SAML configuration

Select the **Edit** button and configure the following fields:

Field	Description
Identifier (Entity ID)	Set this field to the pre-generated SP Entity ID. This automatically-generated value can be copied from the organization's Settings → Single sign-on screen and will vary based on your setup.
Reply URL (Assertion Consumer Service URL)	Set this field to the pre-generated Assertion Consumer Service (ACS) URL. This automatically-generated value can be copied from the organization's Settings → Single sign-on screen and will vary based on your setup.
Sign on URL	Set this field to the login URL from which users will access Bitwarden. For cloud-hosted customers, this is https://vault.bitwarden.com/#/sso or https://vault.bitwarden.eu/#/sso. For self-hosted instances, this is determined by you configured server URL, for example https://your-domain.com/#/sso.

User attributes & claims

The default claims constructed by Azure will work with login with SSO, however you can optionally use this section to configure the NameID format used by Azure in SAML responses.

Select the **Edit** button and select the **Unique User Identifier (Name ID)** entry to edit the NameID claim:

Attributes & Claims

[+ Add new claim](#)
[+ Add a group claim](#)
[☰ Columns](#)
[🗨 Got feedback?](#)

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

▼ Advanced settings

Unique User Identifier

Options include Default, Email Address, Persistent, Unspecified, and Windows qualified domain name. For more information, refer to [Microsoft Azure documentation](#).

SAML signing certificate

Download the Base64 Certificate for use [during a later step](#).

Set up your application

Copy or take note of the **Login URL** and **Microsoft Entra ID Identifier** in this section for use [during a later step](#):

4

Set up BW-Login-SSO

You'll need to configure the application to link with Microsoft Entra ID.

Login URL

Microsoft Entra ID Identifier

Logout URL

Azure URLs

Note

If you receive any key errors when logging in via SSO, try copying the X509 certificate information from the Federation Metadata XML file instead.

Users and groups

Select **Users and groups** from the navigation:

Microsoft Azure

Search resources, services, and docs (G+/)

Home

Default Directory

Enterprise applications

Bitwarden Login with SSO

Bitwarden Login with SSO

Enterprise Application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

<<

+ Add user/group

Edit

Remove

Update Credentials

Columns

Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
No application assignments found		

Assign users or groups

Select the **Add user/group** button to assign access to the login with SSO application on a user or group-level.

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 complete configuration.

The Single sign-on screen separates configuration into two sections:

- **SAML service provider configuration** will determine the format of SAML requests.
- **SAML identity provider configuration** will determine the format to expect for SAML responses.

Service provider configuration

Configure the following fields:

Field	Description
Name ID Format	By default, Azure will use email address. If you changed this setting , select the corresponding value. Otherwise, set this field to Unspecified or Email Address .
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests.
Signing Behavior	Whether/when SAML requests will be signed.
Minimum Incoming Signing Algorithm	By default, Azure will sign with RSA SHA-256. Select rsa-sha256 from the dropdown.
Want Assertions Signed	Whether Bitwarden expects SAML assertions to be signed.
Validate Certificates	Check this box when using trusted and valid certificates from your IdP through a trusted CA. Self-signed certificates may fail unless proper trust chains are configured with the Bitwarden login with SSO docker image.

When you are done with the service provider configuration, **Save** your work.

Identity provider configuration

Identity provider configuration will often require you to refer back to the Azure Portal to retrieve application values:

Field	Description
Entity ID	Enter your Microsoft Entra ID Identifier , retrieved from the Azure Portal's Set up your application section. This field is case sensitive.
Binding Type	Set to HTTP POST or Redirect .
Single Sign On Service URL	Enter your Login URL , retrieved from the Azure Portal's Set up your application section.
Single Log Out Service URL	Login with SSO currently does not support SLO. This option is planned for future development, however you may preconfigure it with your Logout URL if you wish.
X509 Public Certificate	Paste the downloaded certificate, removing -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters will cause certificate validation to fail.
Outbound Signing Algorithm	By default, Azure will sign with RSA SHA-256. Select rsa-sha256 from the dropdown.
Disable Outbound Logout Requests	Login with SSO currently does not support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether Azure expects SAML requests to be signed.

Note

When completing the X509 certificate, take note of the expiration date. Certificates will have to be renewed in order to prevent any disruptions in service to SSO end users. If a certificate has expired, Admin and Owner accounts will always be able to log in with email address and master password.

When you are done with the identity provider configuration, **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](#).

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

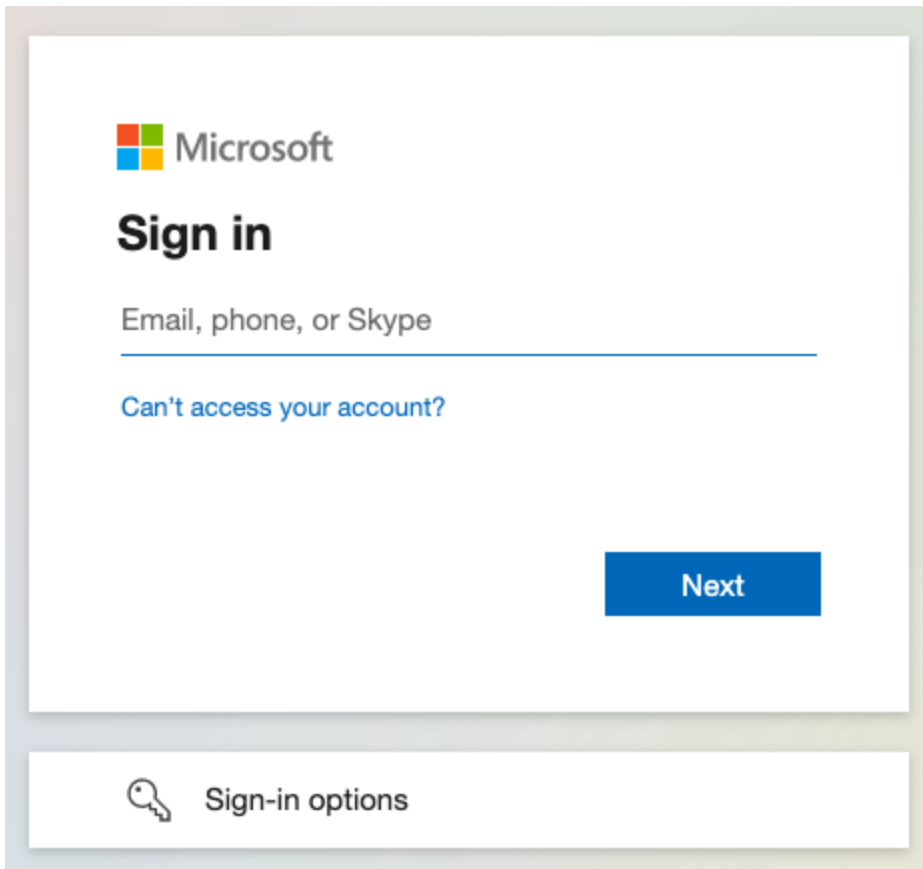
 Log in with passkey

 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. Entra ID SAML administrators can setup an Enterprise application for users to be directed to the Bitwarden SSO login page:

1. Disable the existing Bitwarden button in the **All Applications** page by navigating to the current Bitwarden enterprise Application, selecting **Properties**, and setting the **Visible to users** option to **No**.
2. Create a new app registration by navigating to **Enterprise applications** and selecting **New application**.
3. Select **Create your own application**.
4. Provide a name for the application such as **Bitwarden**, then select **Integrate any other application you don't find in the gallery (Non-gallery)**. Once you have finished, select **Create**.
5. Once the app has been created, navigate to **Single sign-on** located on the navigation menu. Select **Linked**.
6. Add the following settings to the application:
 1. Set the **Sign on URL** to your Bitwarden client login page, such as <https://vault.bitwarden.com/#/sso>. Then, select **Save**.
 2. You may change the logo for end-user recognition in **Properties**. You can retrieve the Bitwarden logo [here](#).

Once this process has been completed, assigned users will have a Bitwarden application that will link them directly to the Bitwarden web vault SSO login page.