

ADMIN CONSOLE > LOGIN WITH SSO >

# ADFS OIDC Implementation

View in the help center:  
<https://bitwarden.com/help/adfs-oidc-implementation/>

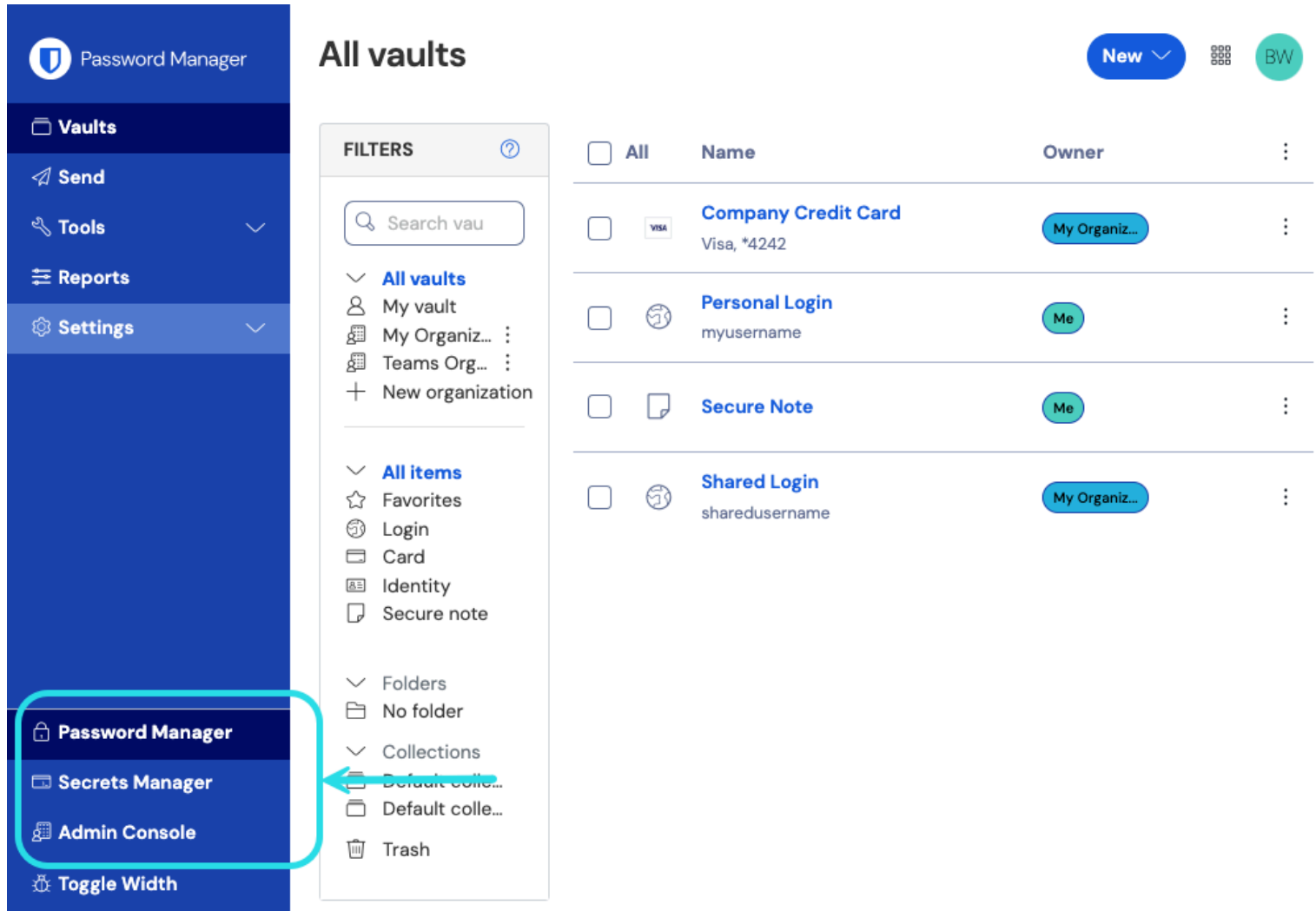
## ADFS OIDC Implementation

This article contains **Active Directory Federation Services (AD FS)–specific** help for configuring login with SSO via OpenID Connect (OIDC). For help configuring login with SSO for another OIDC IdP, or for configuring AD FS via SAML 2.0, see [OIDC Configuration](#) or [ADFS SAML Implementation](#).

Configuration involves working simultaneously within the Bitwarden web app and the AD FS Server Manager. 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:

- 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 application group

In Server Manager, navigate to **AD FS Management** and create a new application group:

1. In the console tree, select **Application Groups** and choose **Add Application Group** from the Actions list.
2. On the Welcome screen of the wizard, choose the **Server application accessing a web API** template.

### Add Application Group Wizard



#### Welcome

##### Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name:

Description:

Template:

##### Client-Server applications

- Native application accessing a web API
- Server application accessing a web API**
- Web browser accessing a web application

##### Standalone applications

- Native application
- Server application
- Web API

[More information...](#)

< Previous

Next >

Cancel

AD FS Add Application Group

3. On the Server application screen:

AD FS Server Application screen

- Give the server Application a **Name**.
- Take note of the **Client Identifier**. You will need this value in a subsequent step.
- Specify a **Redirect URI**. 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>.

4. On the Configure Application Credentials screen, take note of the **Client Secret**. You will need this value in a subsequent step.

5. On the Configure Web API screen:

**Add Application Group Wizard**

### Configure Web API

**Steps**

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API**
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

**Name:**  
BitwardenCloud - Web API

**Identifier:**  
Example: https://Contoso.com   
27a3f3ea-e4ba-4ed5-a203-3b1e6590cf0d   
**https://sso.bitwarden.com/**

**Description:**

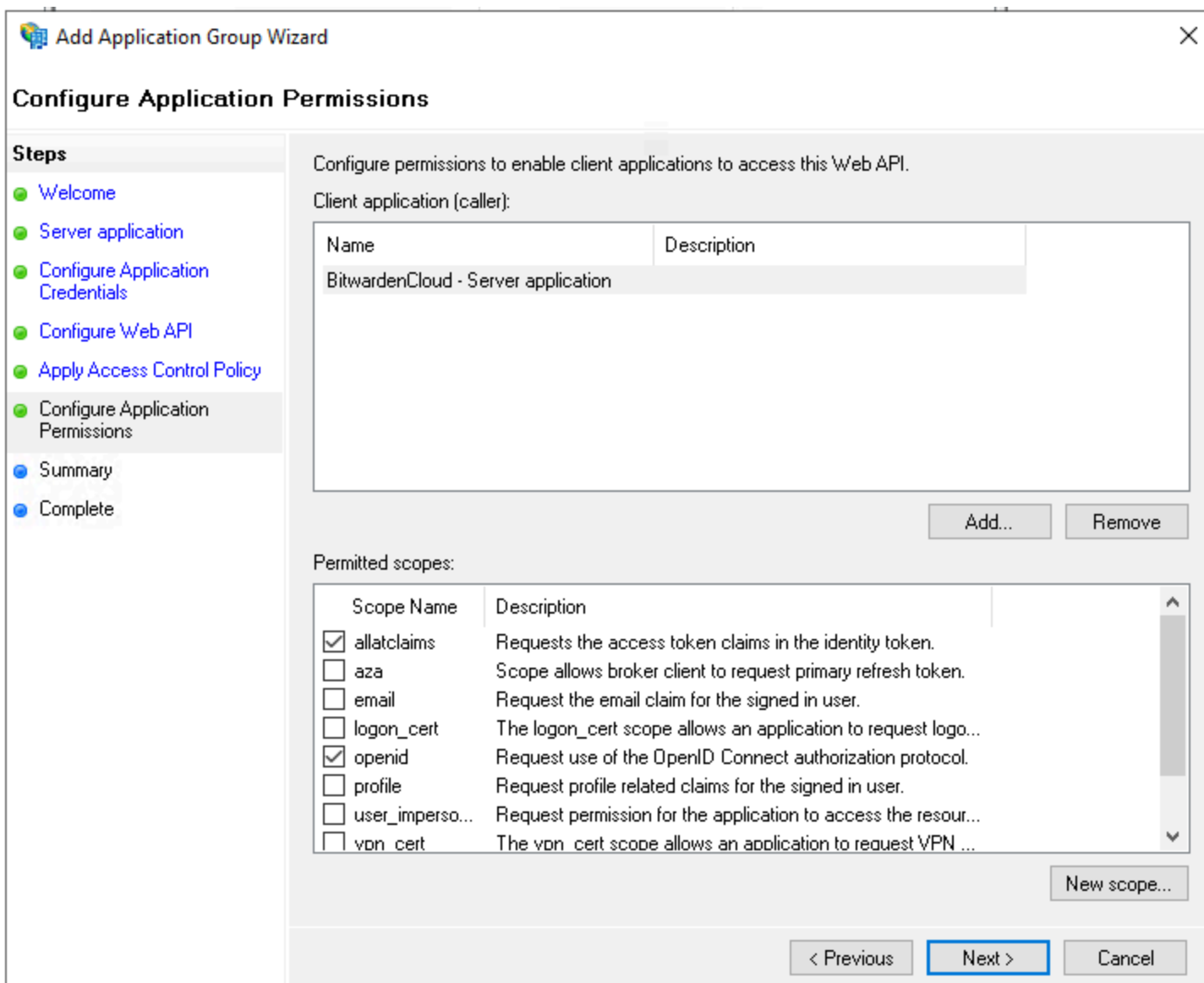
< Previous 

AD FS Configure Web API screen

- Give the Web API a **Name**.
- Add the **Client Identifier** and **Redirect URI** (see step 2B. & C.) to the Identifier list.

6. On the Apply Access Control Policy screen, set an appropriate Access Control Policy for the Application Group.

7. On the Configure application permissions screen, permit the scopes **allatclaims** and **openid**.



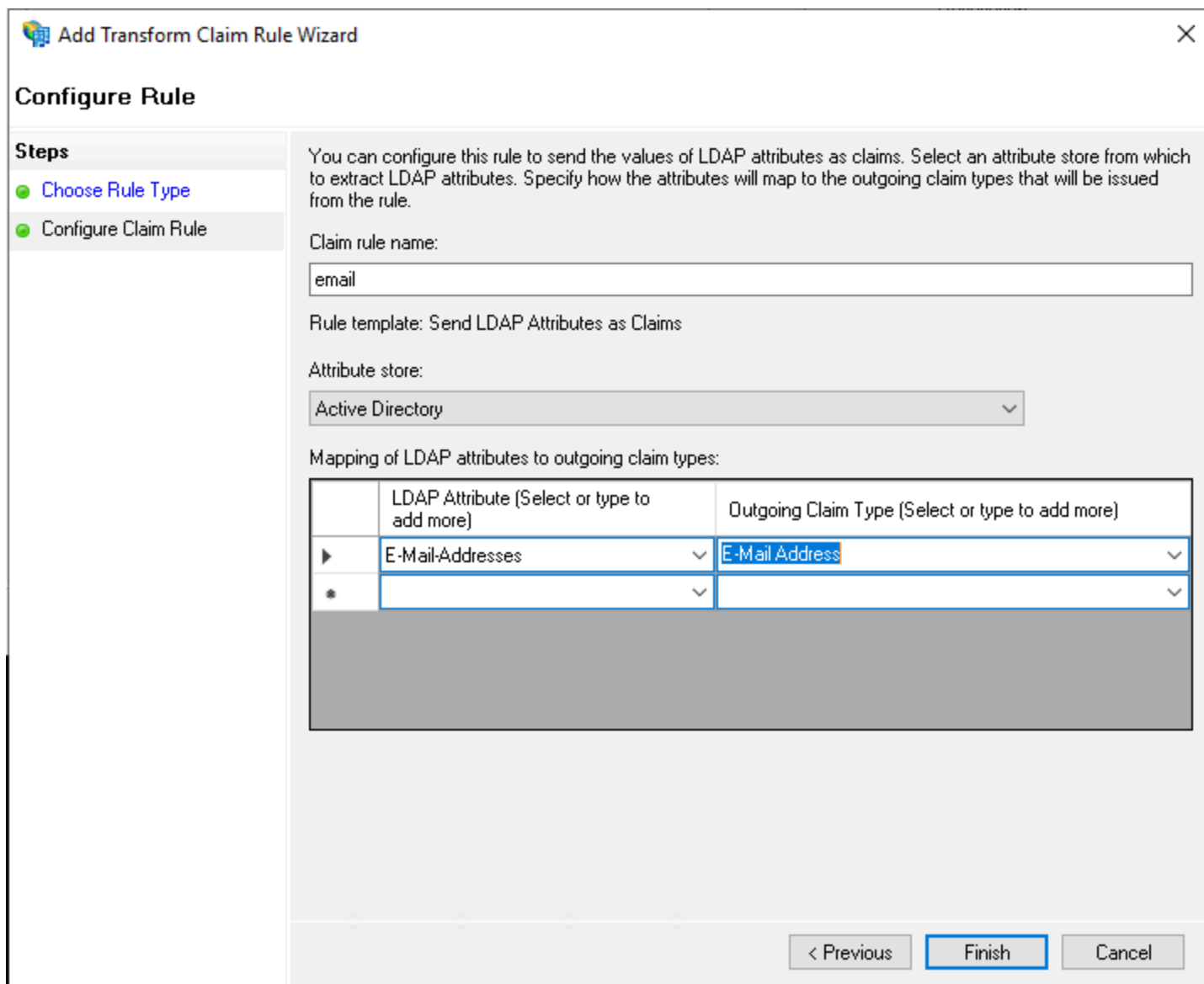
AD FS Configure Application Permissions screen

8. Finish the Add Application Group Wizard.

## Add a transform claim rule

In Server Manager, navigate to **AD FS Management** and edit the created application group:

1. In the console tree, select **Application Groups**.
2. In the Application Groups list, right-click the created application group and select **Properties**.
3. In the Applications section, choose the Web API and select **Edit...**
4. Navigate to the **Issuance Transform Rules** tab and select the **Add Rule...** button.
5. On the Choose Rule Type screen, select **Send LDAP Attributes as Claims**.
6. On the Configure Claim Rule screen:



AD FS Configure Claim Rule screen

- Give the rule a **Claim rule name**.
- From the LDAP Attribute dropdown, select **E-Mail-Addresses**.
- From the Outgoing Claim Type dropdown, select **E-Mail Address**.

7. Select **Finish**.

### Back to the web app

At this point, you have configured everything you need within the context of the AD FS Server Manager. Return to the Bitwarden web app to configure the following fields:



| Field  | Description  |
|--|--|
| Authority  | Enter the hostname of your AD FS Server with <code>/adfs</code> appended, for example <code>https://ads.mybusiness.com/adfs</code> .   |
| Client ID  | Enter the <code>retrieved Client ID</code> .   |
| Client Secret  | Enter the <code>retrieved Client Secret</code> .   |
| Metadata Address   | Enter the specified <b>Authority</b> value with <code>/.well-known/openid-configuration</code> appended, for example <code>https://ads.mybusiness.com/adfs/.well-known/openid-configuration</code> . |
| OIDC Redirect Behavior                                   | Select <b>Redirect GET</b> .   |
| 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.  |
| Custom Scopes  | Define custom scopes to be added to the request (comma-delimited).   |
| Customer 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.                                    |
| 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.                                 |
| 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 References values | Define Authentication Context Class Reference identifiers ( <code>acr_values</code> ) (space-delimited). List <code>acr_values</code> in preference-order.   |

| Field                                  | Description   |
|--|---|
| Expected "acr" Claim Value In Response | Define the <b>acr</b> Claim Value for Bitwarden to expect and validate in the response. |

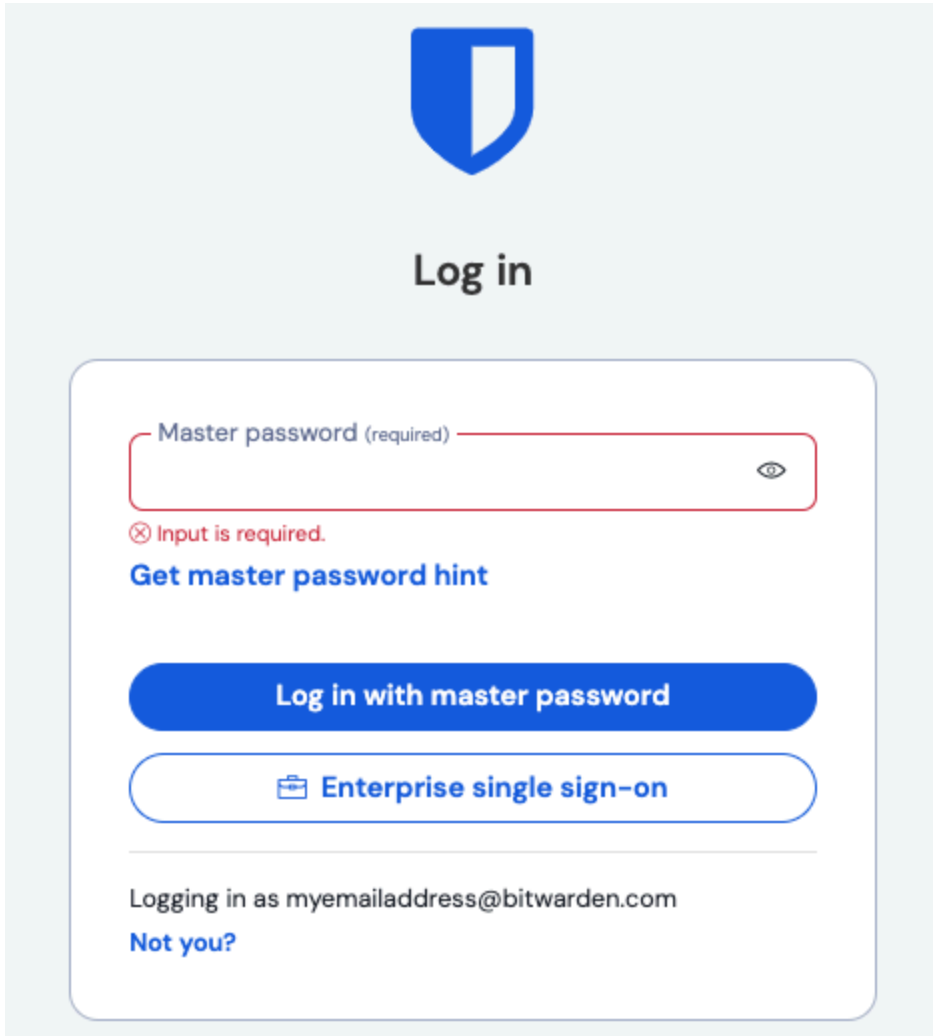
When you are done configuring these fields, **Save** your work.

**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.](#)

### 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:



Log in options screen

Enter the [configured Organization ID](#) and select **Log In**. If your implementation is successfully configured, you'll be redirected to the AD FS SSO login screen. After you authenticate with your AD FS 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.