

ADMIN CONSOLE > LOGGA IN MED SSO >

# ADFS SAML Implementation

View in the help center:

<https://bitwarden.com/help/saml-adfs/>

## ADFS SAML Implementation

This article contains **Active Directory Federation Services (AD FS)**-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 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.

### Tip

**Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

[Download sample](#)

## Open SSO in the web app

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

The screenshot shows the Bitwarden web app interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. At the bottom of the sidebar is the product switcher, which includes Password Manager, Secrets Manager, Admin Console, and Toggle Width. The Admin Console option is highlighted with a red circle and a red arrow. The main content area is titled 'All vaults' and features a 'New' button, a grid icon, and a 'BW' profile icon. Below this is a table of vaults with columns for 'All', 'Name', and 'Owner'. The table lists several vaults: Company Credit Card (owner: My Organiz...), Personal Login (owner: Me), Secure Note (owner: Me), and Shared Login (owner: My Organiz...). A 'FILTERS' panel is open on the left, showing search and filter options.

<input type="checkbox"/> All	Name	Owner	
<input type="checkbox"/>	<b>Company Credit Card</b> Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>	<b>Personal Login</b> myusername	Me	⋮
<input type="checkbox"/>	<b>Secure Note</b>	Me	⋮
<input type="checkbox"/>	<b>Shared Login</b> sharedusername	My Organiz...	⋮

Product switcher



1. On the Welcome screen, select **Claims Aware**.
2. On the Select Data Source screen, select **Enter data about the relying party manually**.
3. On the Specify Display Name screen, enter a Bitwarden-specific display name.
4. On the Configure URL screen, select **Enable support for SAML 2.0 WebSSO protocol**.
  - In the **Relying party SAML 2.0 SSO service URL** input, enter the 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.
5. On the **Choose Access Control Policy** screen, select the policy that meets your security standards.
6. On the **Configure Identifiers** screen, add the SP Entity ID as a relying party trust identifier. This automatically-generated value can be copied from the organization's **Settings** → **Single sign-on** screen and will vary based on your setup.
7. On the **Choose Access Control Policy** screen, select the desired policy (by default, **Permit Everyone**).
8. On the **Ready to Add Trust** screen, review your selections.

## Advanced options

Once the relying party trust is created, you can further configure its settings by selecting **Relying Party Trusts** from the left-hand file navigator and selecting the correct display name.

## Hash algorithm

To change the **Secure hash algorithm** (by default, SHA-256), navigate to the **Advanced** tab:

The screenshot shows the AD FS console interface. On the left, the 'Relying Party Trusts' folder is highlighted with a green circle. The main pane displays a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

A dialog box titled 'Bitwarden ADFS Test Properties' is open, showing the 'Encryption' tab. The 'Secure hash algorithm' dropdown is set to 'SHA-256'.

Set a Secure Hash Algorithm

## Endpoint binding

To change the endpoint **Binding** (by default, POST), navigate to the **Endpoints** tab and select the configured ACS URL:

The screenshot shows the AD FS console interface. On the left is a tree view with 'Relying Party Trusts' selected. The main pane shows a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

The 'Bitwarden ADFS Test Properties' dialog box is open, showing the 'Endpoints' tab. It contains a table of endpoints:

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://sso.bitwarden.com/sa...	0	POST	Yes	

The 'Edit Endpoint' dialog box is also open, with the 'Binding' dropdown menu highlighted in green. The 'Binding' is set to 'POST'. Other fields include 'Endpoint type' (SAML Assertion Consumer), 'Index' (0), 'Trusted URL' (https://sso.bitwarden.com/saml2/3e5d0), and 'Response URL'.

Edit Endpoint

## Edit claim issuance rules

Construct claim issuance rules to ensure that the appropriate claims, including **Name ID**, are passed to Bitwarden. The following tabs illustrate a sample ruleset:

⇒ Rule 1

AD FS

File Action View Window Help

AD FS

- Service
  - Attribute Stores
  - Authentication Methods
  - Certificates
  - Claim Descriptions
  - Device Registration
  - Endpoints
  - Scope Descriptions
  - Web Application Proxy
  - Access Control Policies
  - Relying Party Trusts**
  - Claims Provider Trusts
  - Application Groups

**Relying Party Trusts**

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

Edit Claim Issuance Policy for Bitwarden ADFS Test

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

Edit Rule - Bitwarden

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
	Display-Name	Name
	Given-Name	Given Name
	Surname	Surname
*		

View Rule Language... OK Cancel

ADFS Rule 1

## ⇒Rule 2

The screenshot shows the AD FS console interface. On the left, a tree view shows the 'Relying Party Trusts' folder selected. The main pane displays a table of Relying Party Trusts:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

An 'Edit Claim Issuance Policy for Bitwarden ADFS Test' dialog is open, showing a table of Issuance Transform Rules:

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

The 'Edit Rule - UPN' dialog is also open, showing configuration options:

- Claim rule name: UPN
- Rule template: Send LDAP Attributes as Claims
- Attribute store: Active Directory
- Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	UPN
*		

Buttons at the bottom include 'View Rule Language...', 'OK', and 'Cancel'.

ADFS Rule 2

### ⇒Rule 3

The screenshot shows the AD FS console with the 'Relying Party Trusts' tab selected. A table lists the trust configuration:

Display Name	Enabled	Type	Identifier	Access Control Policy
Bitwarden ADFS Test	Yes	WS-T...	https://sso.bitwarden.com/saml2	Permit everyone

An 'Edit Claim Issuance Policy for Bitwarden ADFS Test' dialog is open, showing a table of 'Issuance Transform Rules':

Order	Rule Name	Issued Claims
1	Bitwarden	E-Mail Address, Name, Giv...
2	UPN	UPN
3	Transform Name ID	Name ID

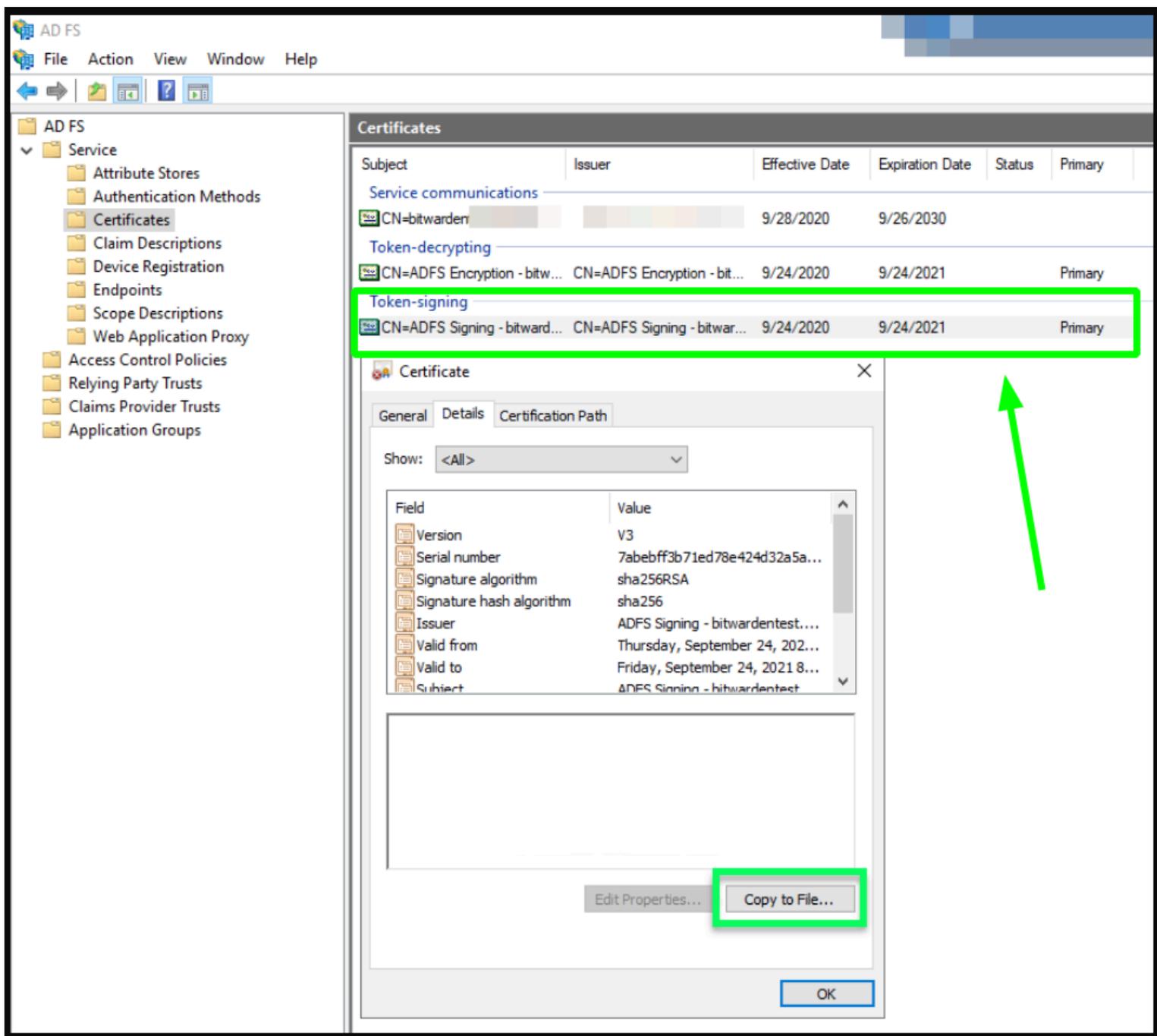
The 'Edit Rule - Transform Name ID' dialog is also open, showing configuration options:

- Claim rule name: Transform Name ID
- Rule template: Transform an Incoming Claim
- Incoming claim type: UPN
- Incoming name ID format: Unspecified
- Outgoing claim type: Name ID
- Outgoing name ID format: Persistent Identifier
- Selected option:  Pass through all claim values

ADFS Rule 3

### Get certificate

In the left-hand file navigator, select **AD FS** → **Service** → **Certificates** to open the list of certificates. Select the **Token-signing** certificate, navigate to its **Details** tab, and select the **Copy to File...** button to export the Base-64 encoded token signing certificate:

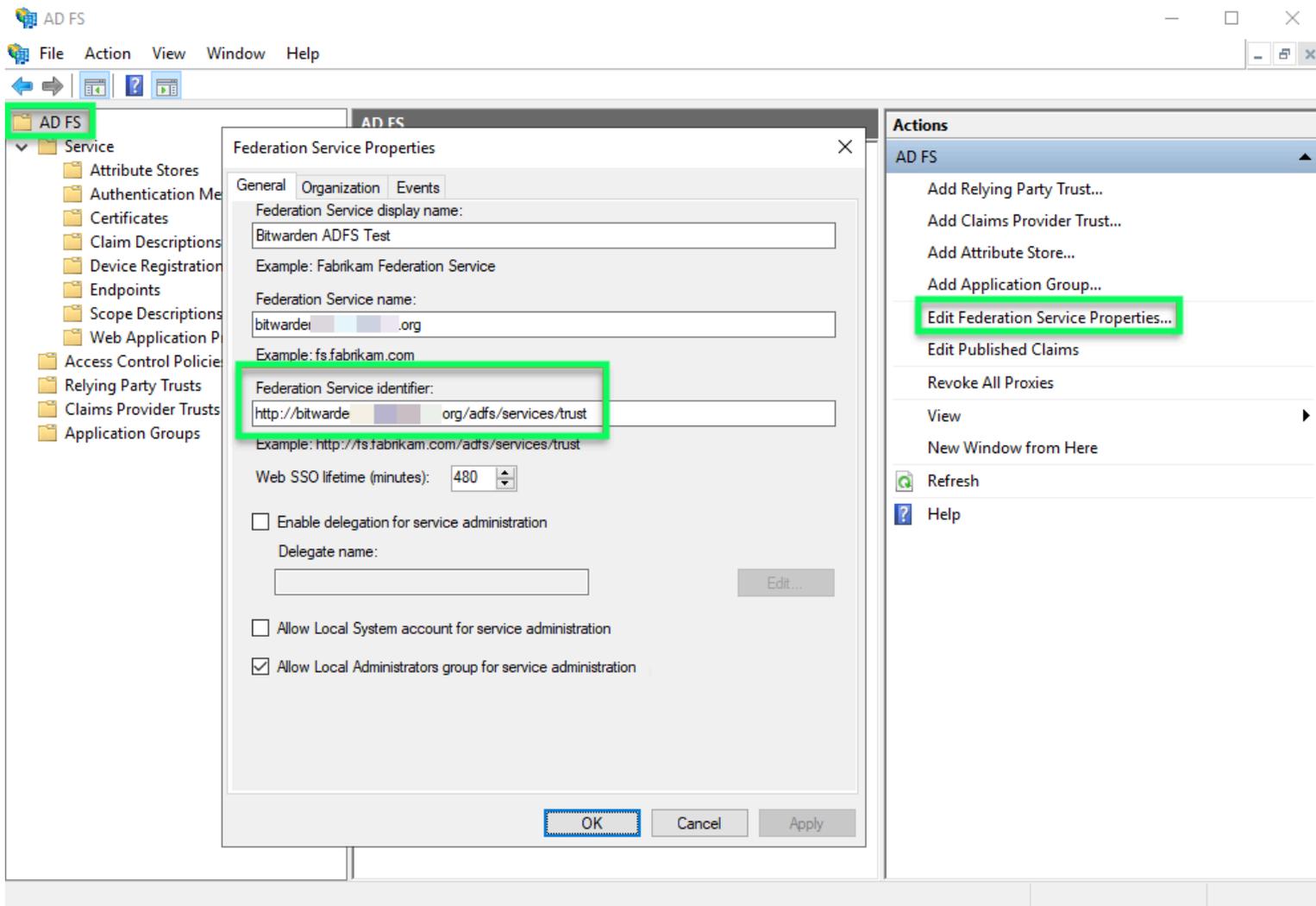


Get token-signing Certificate

You will need this certificate during a later step.

### Get federation service identifier

In the left-hand file navigator, select **AD FS** and from the right-hand options menu select **Edit Federation Service Properties**. In the Federation Service Properties window, copy the **Federation Service Identifier**:



Get Federation Service Identifier

You will need this identifier [during a later step](#).

## 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 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

In the service provider configuration section, configure the following fields:

Field	Description
Name ID Format	Select the <b>Outgoing Name ID Format</b> selected when constructing <a href="#">claims issuance rules</a> (see <b>Rule 3</b> ).
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, AD FS will sign with SHA-256. Select <b>SHA-256</b> from the dropdown unless you have <a href="#">configured AD FS to use different algorithm</a> .
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 within 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 AD FS Server Manager to retrieve values:

Field	Description
Entity ID	Enter the retrieved <a href="#">Federation Service Identifier</a> . Please note, this <b>may not use HTTPS</b> . This field is case sensitive.
Binding Type	By default, AD FS will use HTTP POST endpoint binding. Select <b>HTTP POST</b> unless you have <a href="#">configured AD FS to use a different method</a> .

Field	Description
Single Sign On Service URL	Enter the SSO Service Endpoint. This value can be constructed in the <b>Service</b> → <b>Endpoints</b> tab in AD FS Manager. The endpoint URL is listed as <b>URL Path for SAML2.0/WS-Federation</b> and is usually something like <a href="https://your-domain/adfs/ls">https://your-domain/adfs/ls</a> . You can obtain the exact value from the configuration key for SingleSignOnService in the <a href="#">FederationMetadata.xml</a> document.
X509 Public Certificate	<p>Paste the downloaded certificate, removing</p> <p>-----BEGIN CERTIFICATE-----</p> <p>and</p> <p>-----END CERTIFICATE-----</p> <p>The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters <b>will cause certification to fail</b>.</p>
Outbound Signing Algorithm	By default, AD FS will sign with SHA-256. Select <b>SHA-256</b> from the dropdown unless you have <a href="#">configured AD FS to use different algorithm</a> .
Disable Outbound Logout Requests	Login with SSO currently <b>does not</b> support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether AD FS 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.

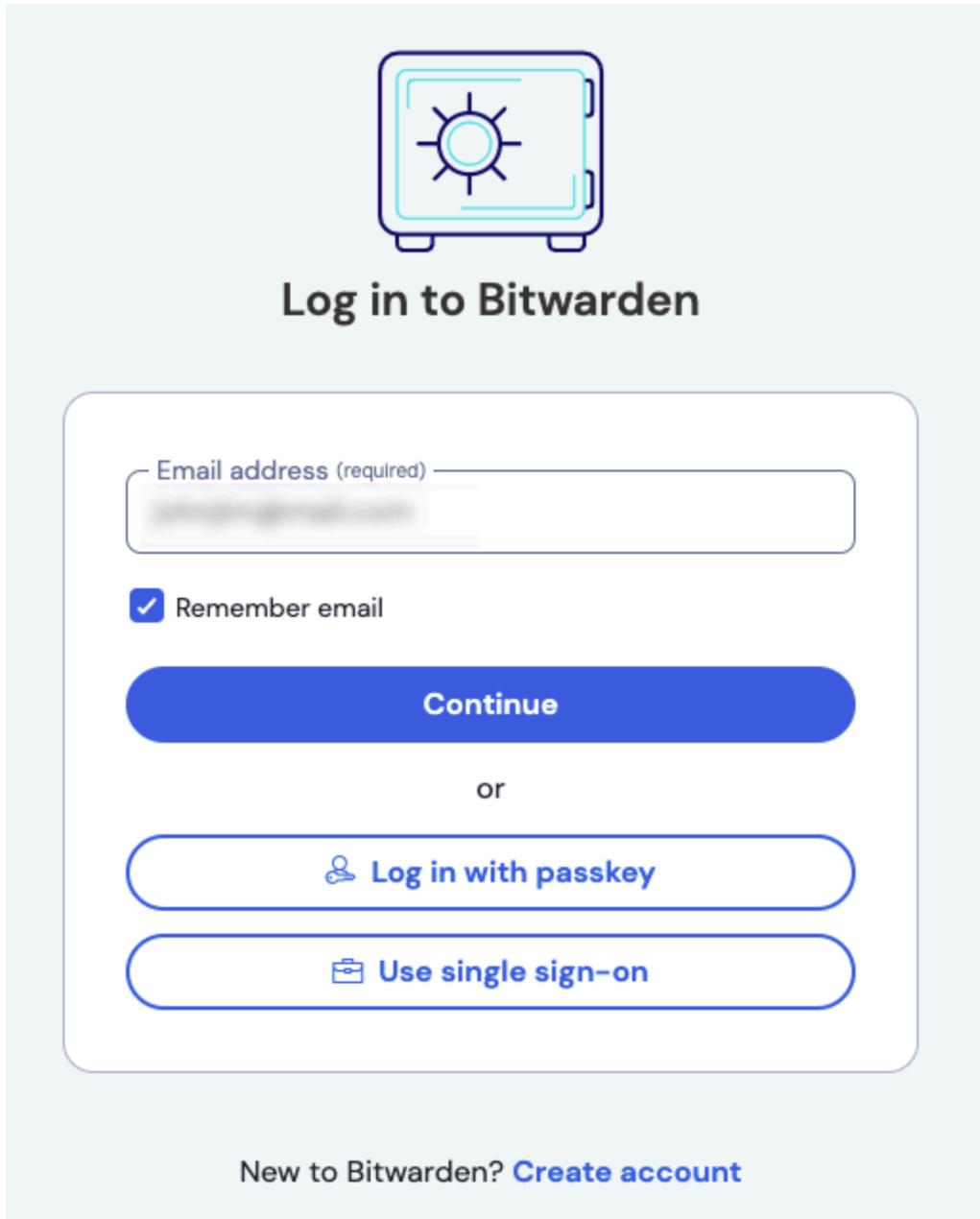
When you are done with the identity provider configuration, **Save** your work.

**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 options screen

Enter the [configured organization identifier](#) and select **Log In**. If your implementation is successfully configured, you will 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.