

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.

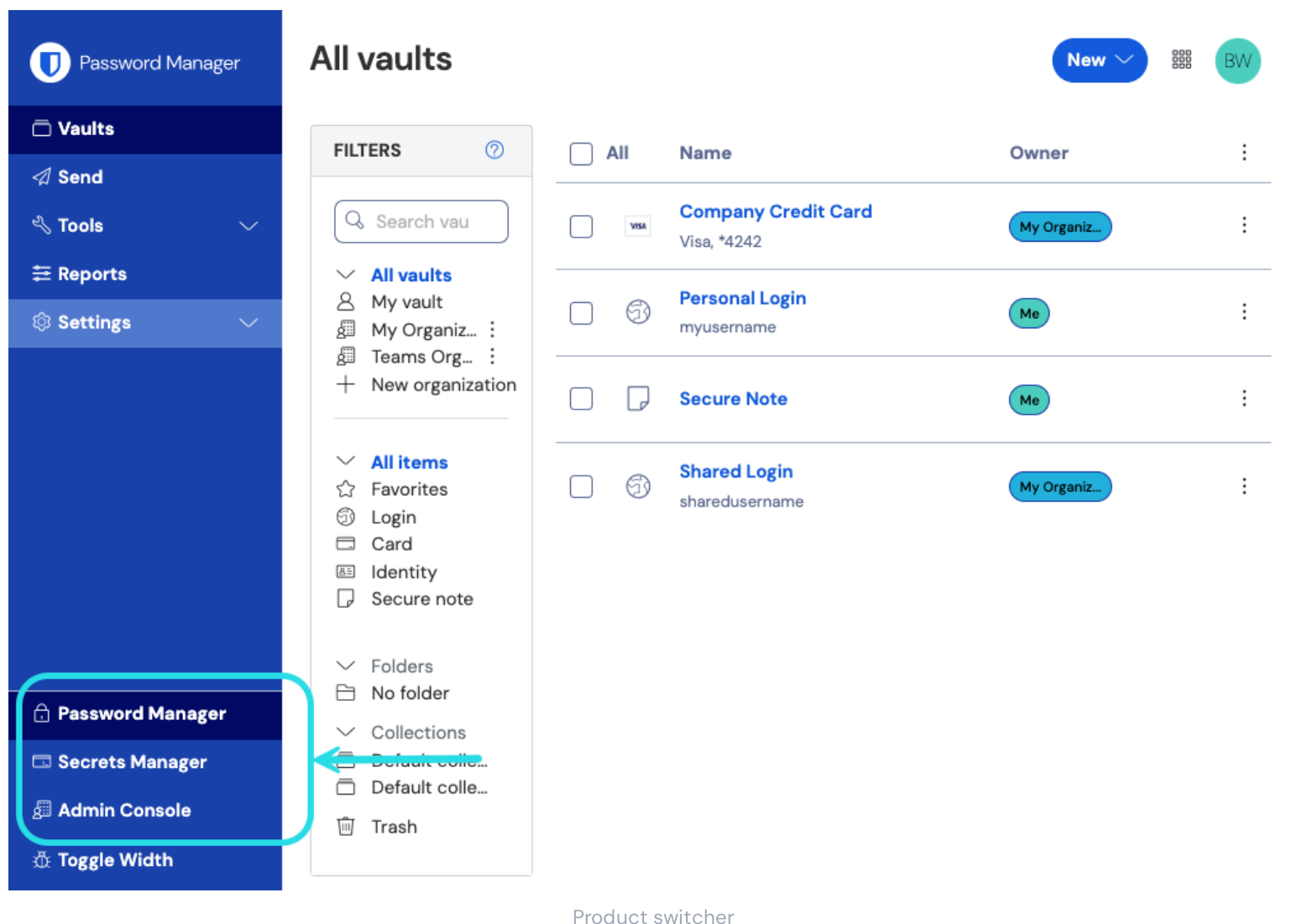


Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

[Download sample](#)

Open SSO in the web app

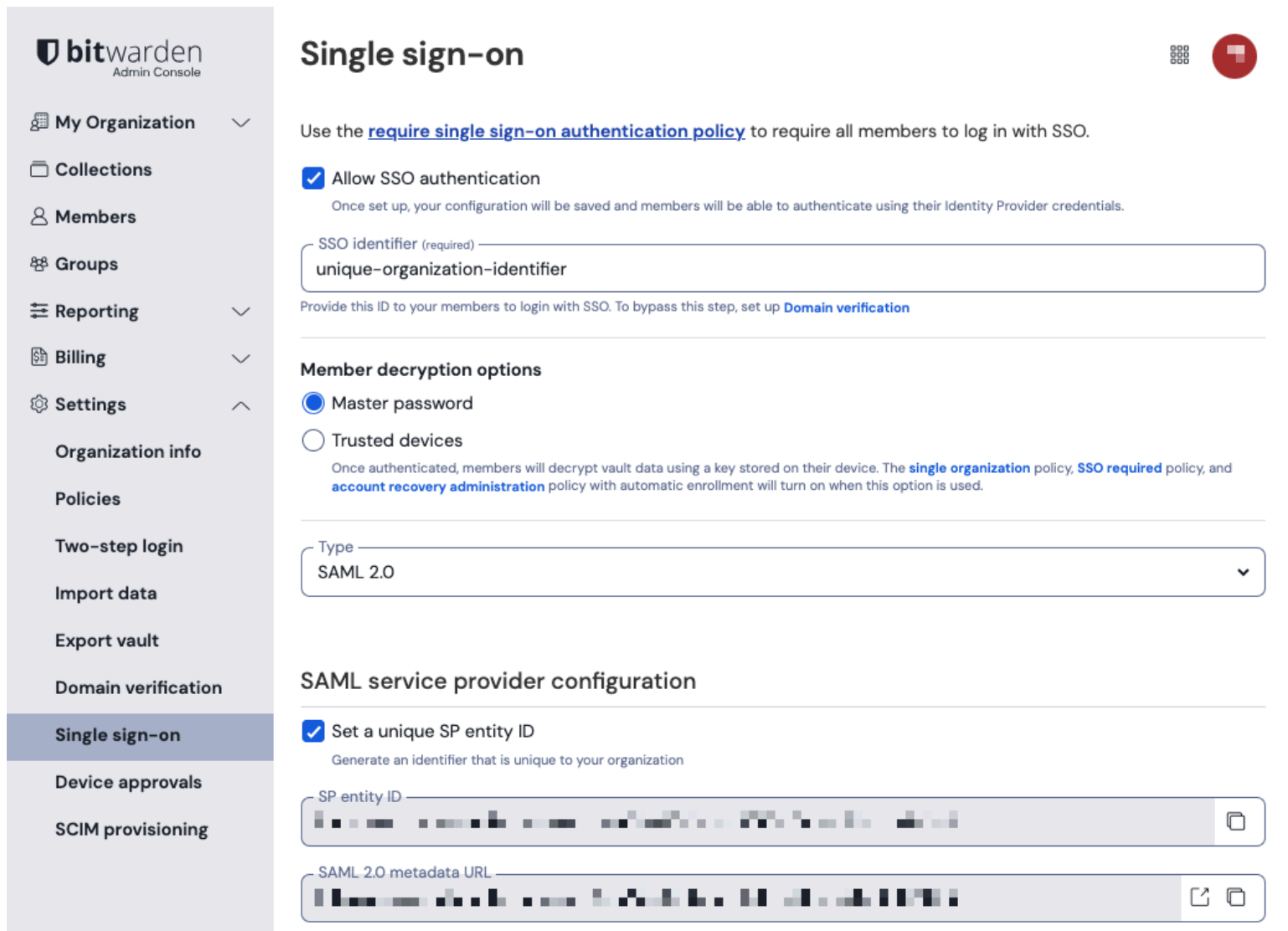
Log in to the Bitwarden web app and open the Admin Console using the product switcher:



The screenshot displays the Bitwarden web app interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. A red box highlights the bottom section of the sidebar, which includes Password Manager, Secrets Manager, Admin Console, and a Toggle Width button. A red arrow points from the Admin Console option to the 'All vaults' section of the main content area. The 'All vaults' section features a search bar and a list of filters. The main content area shows a table of vaults with columns for checkboxes, icons, names, owners, and more options. The vaults listed are: Company Credit Card (Visa, *4242), Personal Login (myusername), Secure Note, and Shared Login (sharedusername). The owner for the first three is 'Me' and for the last is 'My Organiz...'. In the top right corner, there is a 'New' button, a grid icon, and a circular product switcher with 'BW' inside.

Product switcher

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



The screenshot shows the Bitwarden Admin Console interface. On the left is a sidebar with navigation links: My Organization, Collections, Members, Groups, Reporting, Billing, Settings (expanded), 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 configuration steps are as follows:

- 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)**
unique-organization-identifier
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**
SAML 2.0
- SAML service provider configuration**
 - ☒ **Set a unique SP entity ID**
Generate an identifier that is unique to your organization
 - SP entity ID**
[Random alphanumeric string]
 - SAML 2.0 metadata URL**
[Random alphanumeric string]

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.



Tip

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

Create a relying party trust

In the AD FS Server Manager, select **Tools** → **AD FS Management** → **Action** → **Add Relying Party Trust**. In the wizard, make the following selections:

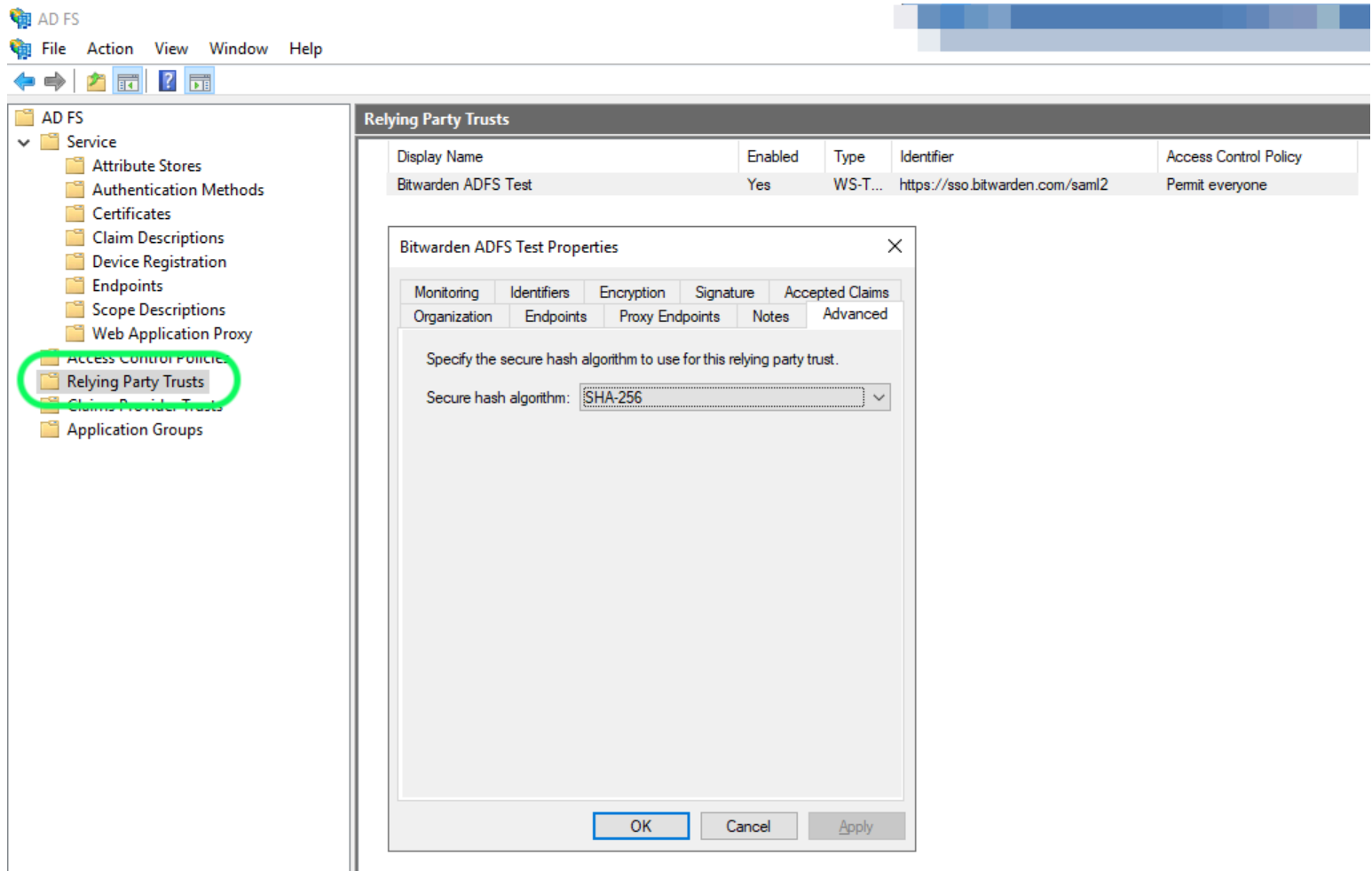
1. On the Welcome screen, select **Claims Aware**.
2. On the Select Data Source screen, select **Enter data about the relying party manually**.
3. On the Specify Display Name screen, enter a Bitwarden-specific display name.
4. On the Configure URL screen, select **Enable support for SAML 2.0 WebSSO protocol**.
 - 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 with the 'Relying Party Trusts' folder selected in the left-hand tree. The main pane displays a table of existing trusts, including 'Bitwarden ADFS Test'. A properties dialog for this trust is open, showing the 'Advanced' tab where the 'Secure hash algorithm' is set to 'SHA-256'.

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

Bitwarden ADFS Test Properties

Monitoring | Identifiers | Encryption | Signature | Accepted Claims

Organization | Endpoints | Proxy Endpoints | Notes | **Advanced**

Specify the secure hash algorithm to use for this relying party trust.

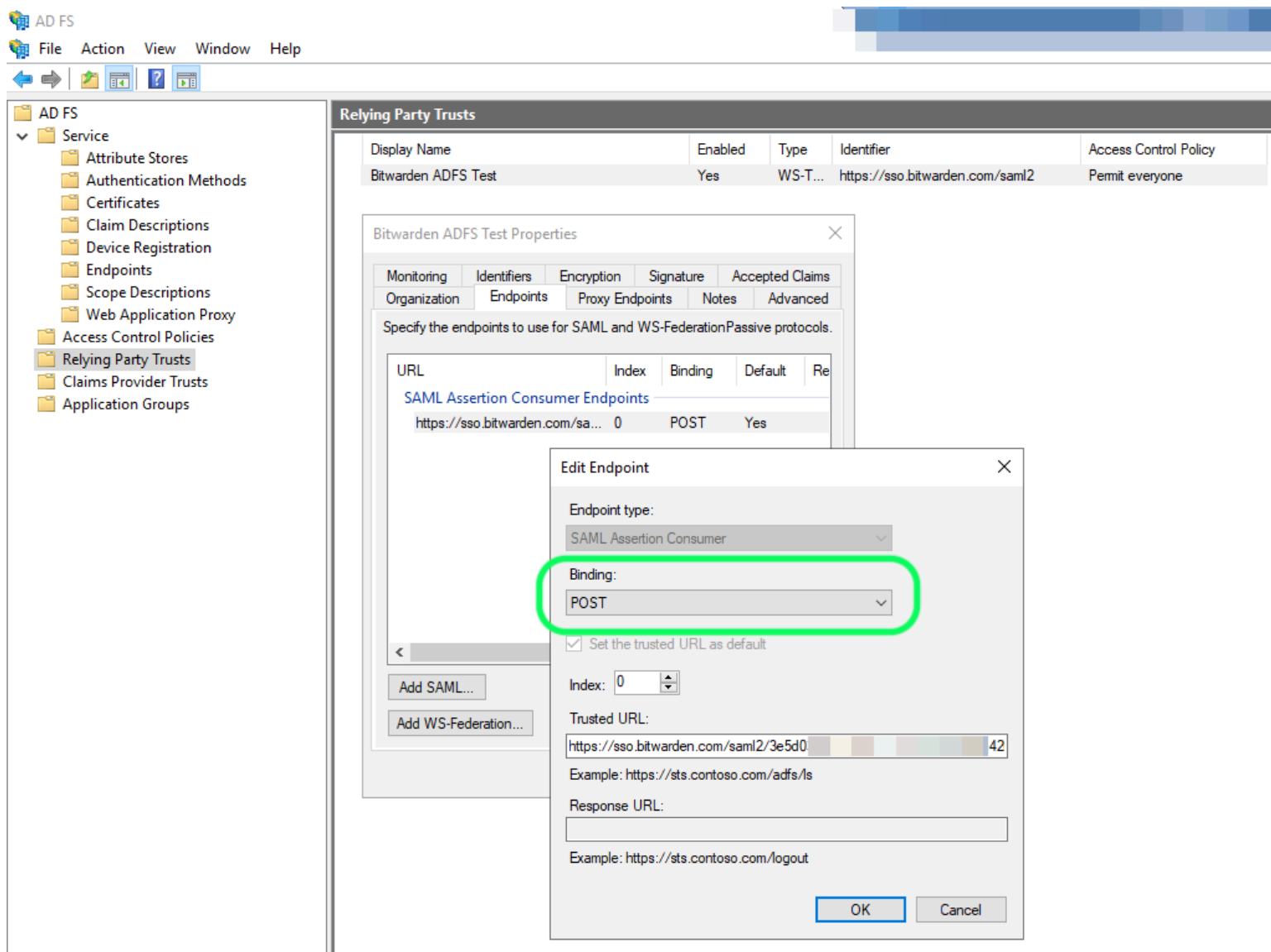
Secure hash algorithm:

OK Cancel Apply

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, the 'AD FS' tree view is expanded to 'Relying Party Trusts'. The main pane displays a table of 'Relying Party Trusts' with columns: Display Name, Enabled, Type, Identifier, and Access Control Policy. The table contains one entry: 'Bitwarden ADFS Test' with 'Enabled' set to 'Yes', 'Type' as 'WS-T...', 'Identifier' as 'https://sso.bitwarden.com/saml2', and 'Access Control Policy' as 'Permit everyone'.

The 'Bitwarden ADFS Test Properties' dialog box is open, showing the 'Endpoints' tab. It lists the endpoints for SAML and WS-FederationPassive protocols. The 'SAML Assertion Consumer Endpoints' are listed with a URL of 'https://sso.bitwarden.com/sa...', Index 0, Binding POST, and Default Yes.

The 'Edit Endpoint' dialog box is open, showing the 'Endpoint type' as 'SAML Assertion Consumer' and the 'Binding' as 'POST' (highlighted with a green circle). The 'Trusted URL' is 'https://sso.bitwarden.com/saml2/3e5d0' and the 'Response URL' is empty.

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:
Bitwarden

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)
▶	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

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 - UPN

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:
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
*		

View Rule Language...

OK Cancel

ADFS Rule 2

⇒Rule 3

The screenshot shows the AD FS console with the 'Relying Party Trusts' configuration for 'Bitwarden ADFS Test'. The 'Edit Claim Issuance Policy' dialog is open, showing a table of transform rules. The 'Edit Rule - Transform Name ID' dialog is also open, showing the configuration for the 'Transform Name ID' rule.

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 - Transform Name ID

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

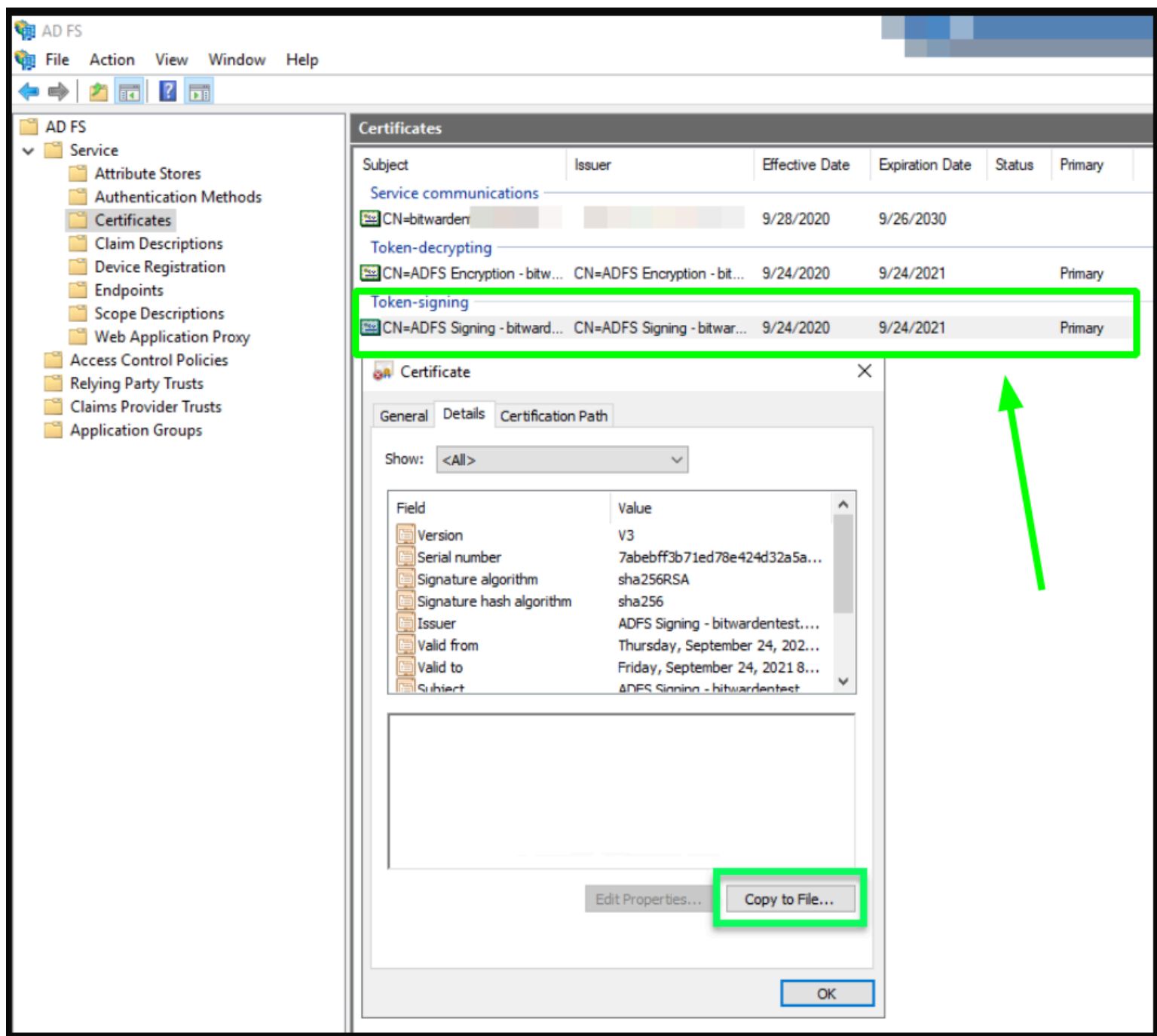
New e-mail suffix:

Example: fabrikam.com

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:

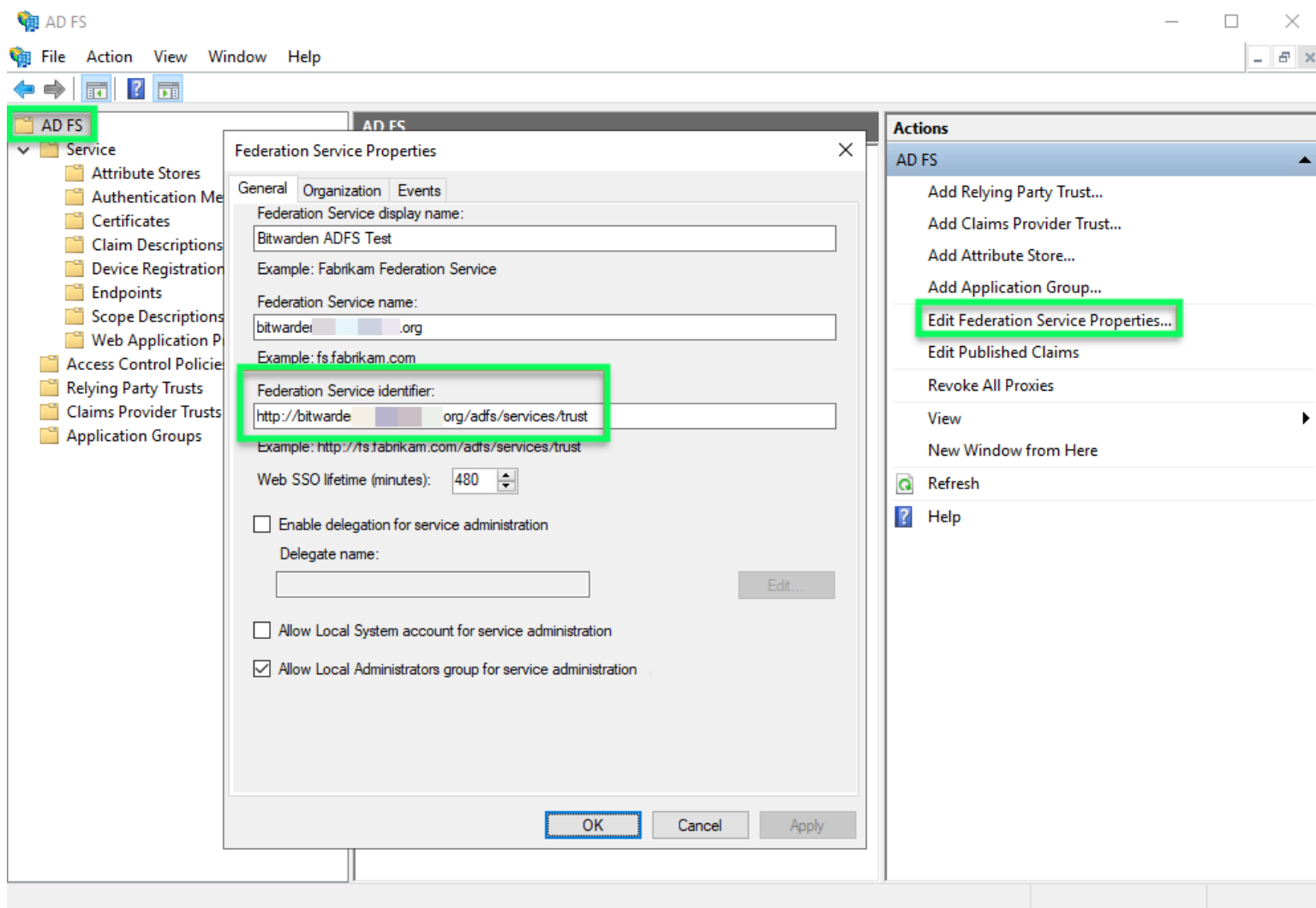


Get token-signing Certificate

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 Outgoing Name ID Format selected when constructing claims issuance rules (see Rule 3).
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 SHA-256 from the dropdown unless you have configured AD FS to use different algorithm .
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 Federation Service Identifier . Please note, this may not use HTTPS . This field is case sensitive.
Binding Type	By default, AD FS will use HTTP POST endpoint binding. Select HTTP POST unless you have configured AD FS to use a different method .

Field	Description
Single Sign On Service URL	Enter the SSO Service Endpoint. This value can be constructed in the Service → Endpoints tab in AD FS Manager. The endpoint URL is listed as URL Path for SAML2.0/WS-Federation and is usually something like <code>https://your-domain/adfs/ls</code> . You can obtain the exact value from the configuration key for SingleSignOnService in the <code>FederationMetadata.xml</code> document.
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 certification to fail.
Outbound Signing Algorithm	By default, AD FS will sign with SHA-256. Select SHA-256 from the dropdown unless you have configured AD FS to use different algorithm .
Disable Outbound Logout Requests	Login with SSO currently does not 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.

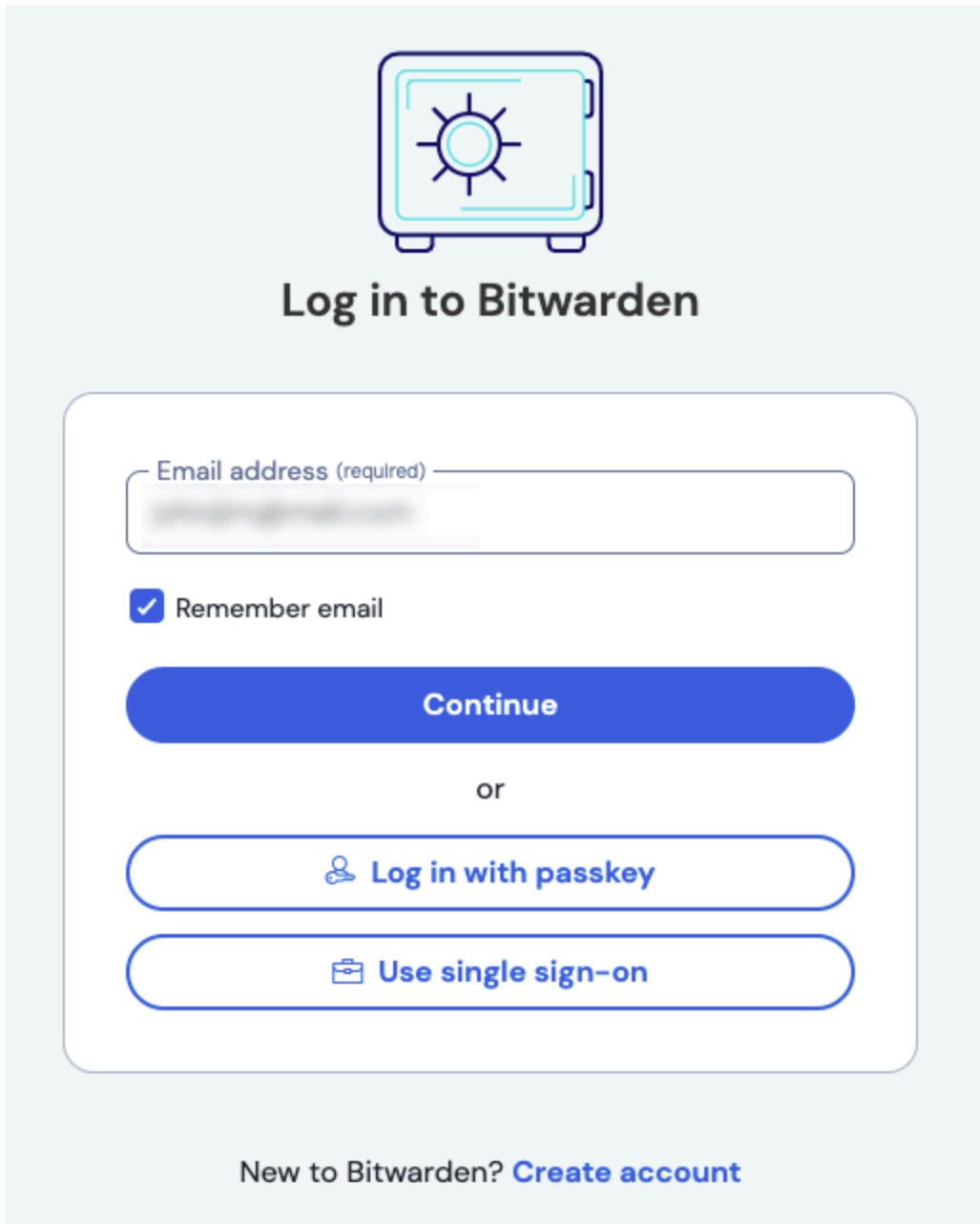
When you are done with the identity provider configuration, **Save** your work.

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:



The screenshot shows the Bitwarden login interface. At the top is a blue icon of a safe with a sun-like symbol inside. Below the icon is the text "Log in to Bitwarden". The main login area is a white rounded rectangle containing an "Email address (required)" input field with a blurred email address, a checked "Remember email" checkbox, a blue "Continue" button, and the word "or" in the center. Below "or" are two buttons: "Log in with passkey" with a person icon and "Use single sign-on" with a briefcase icon. At the bottom of the white area is the text "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 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.