bitwarden | Help Center Article

ADMIN CONSOLE > LOGIN WITH SSO >

ADFS SAML Implementation

View in the help center:
https://bitwarden.com/help/saml-adfs/

ADFS SAML Implementation

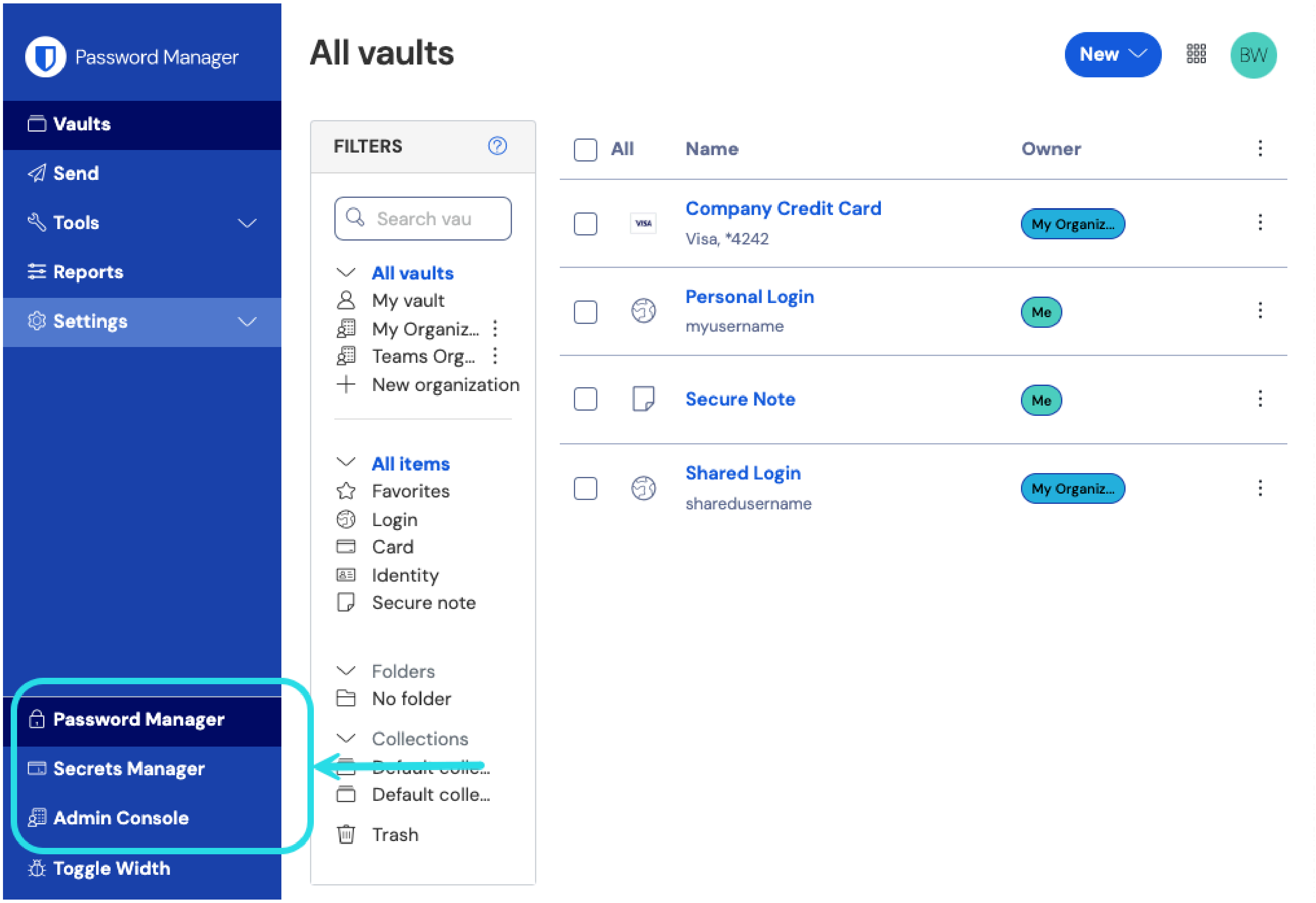
This article contains **Active Directory Federation Services (AD FS)-specific** help for configuring login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to SAML 2.0 Configuration.

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

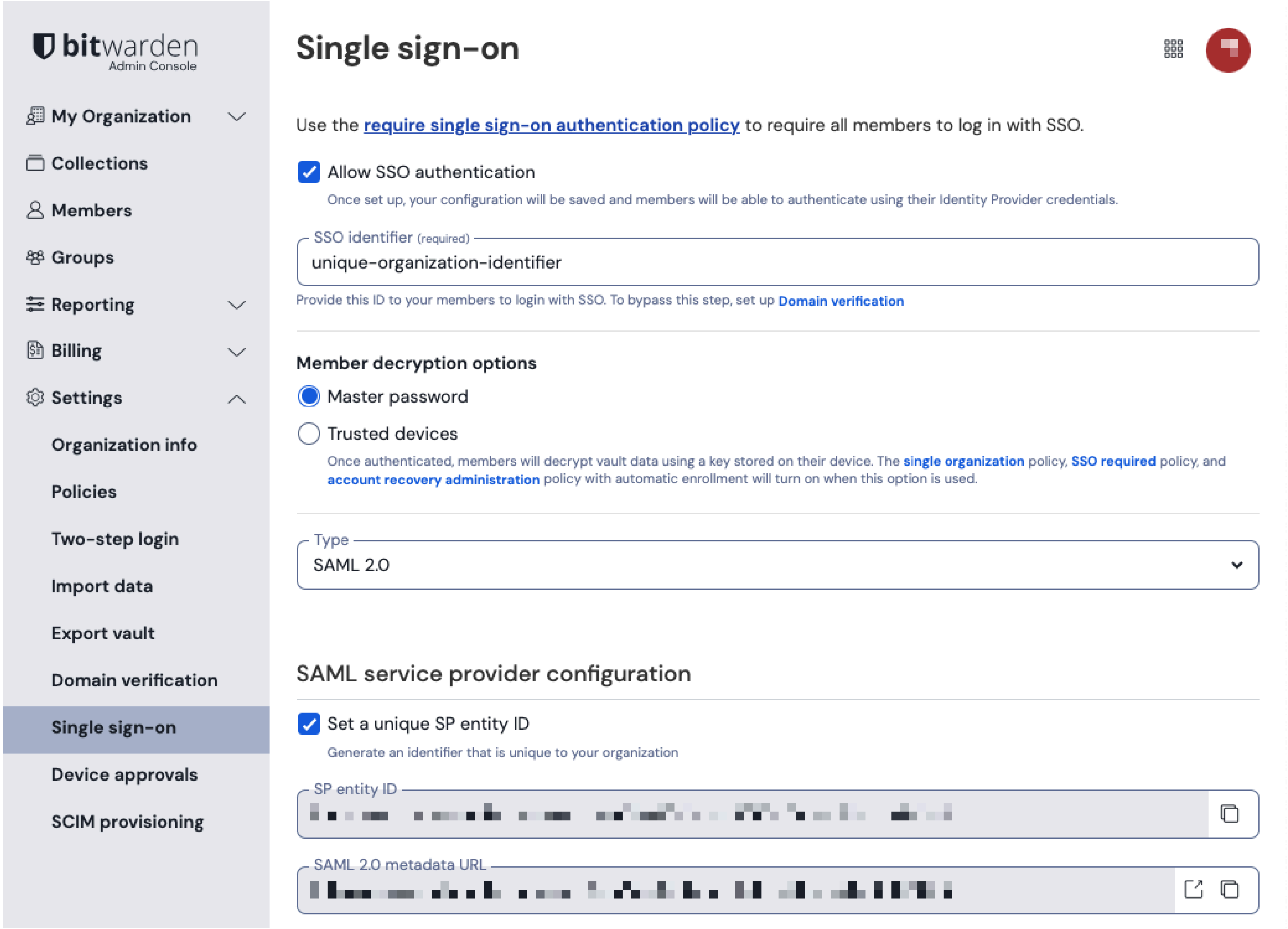
Open SSO in the web app

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



Product switcher

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



bitwarden Admin Console

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): 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: [redacted]

SAML 2.0 metadata URL: [redacted]

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**).

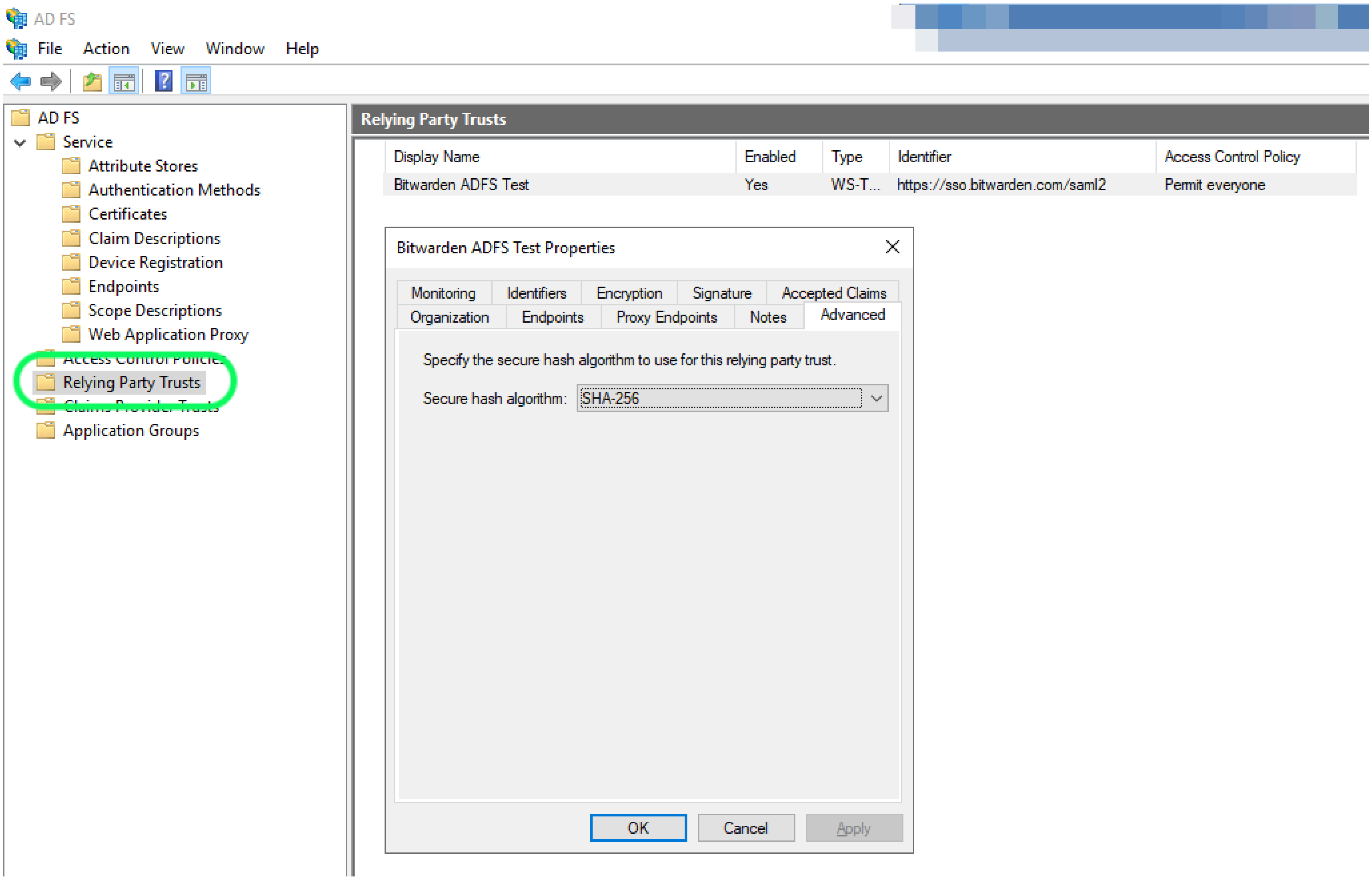
8. On the **Ready to Add Trust** screen, review your selections.

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:



[redacted]

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

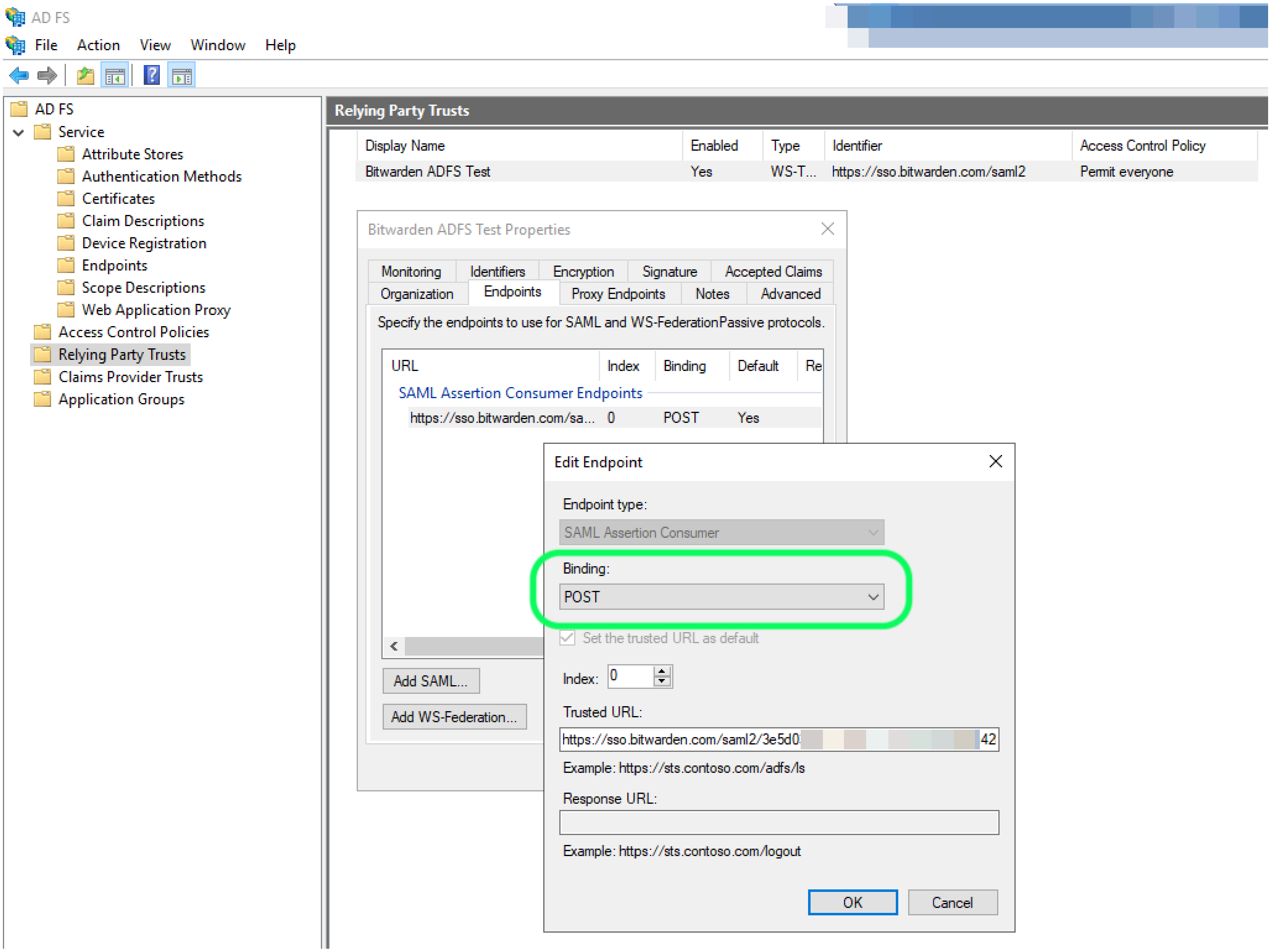
Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: 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:



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

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

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

Edit Endpoint

Endpoint type: SAML Assertion Consumer

Binding: POST

☑ Set the trusted URL as default

Index: 0

Trusted URL: https://sso.bitwarden.com/saml2/3e5d0[redacted]42

Example: https://sts.contoso.com/adfs/ls

Response URL:

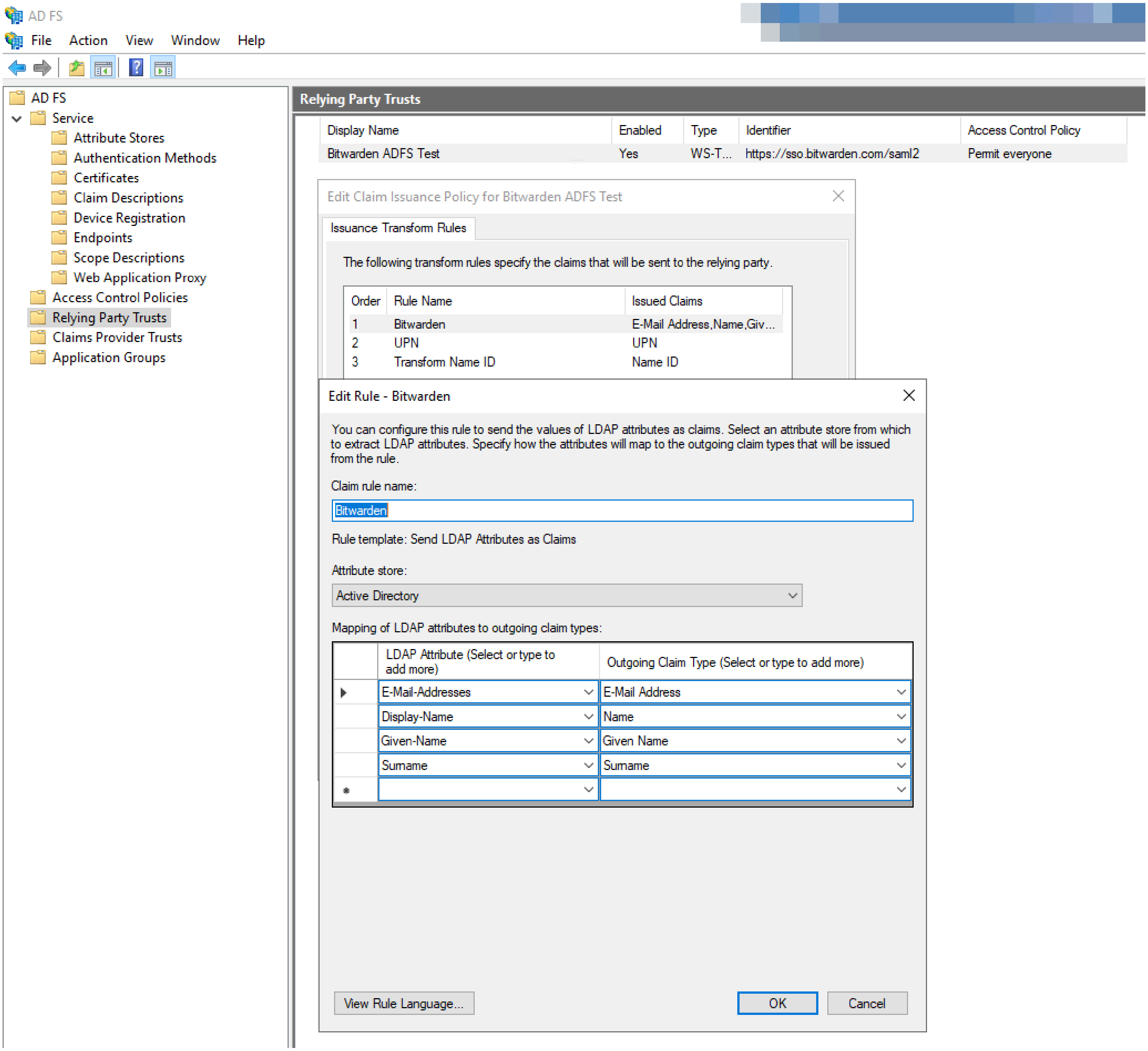
Example: https://sts.contoso.com/logout

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



[redacted]

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:

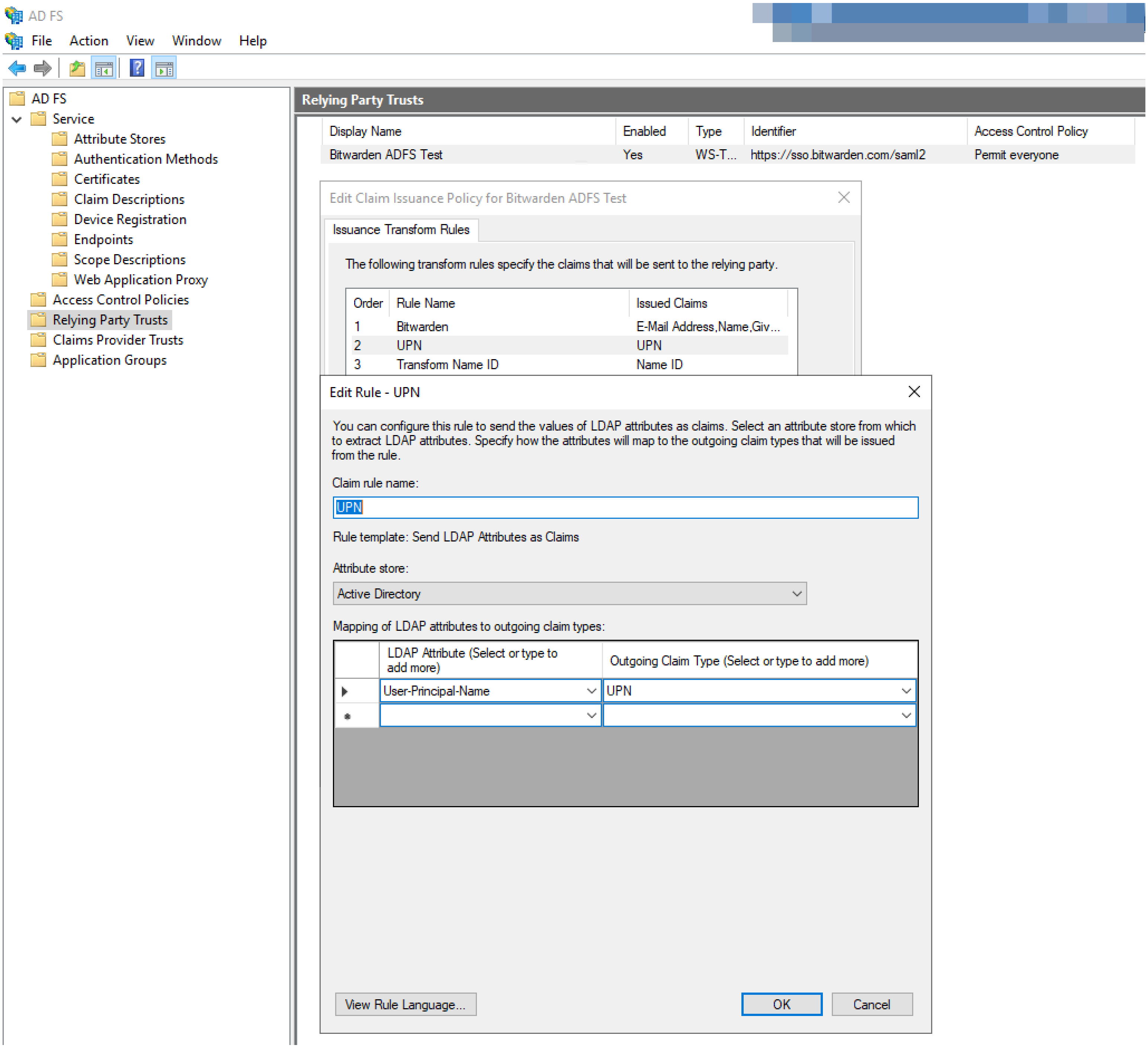
Active Directory

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

ADFS Rule 1

⇒Rule 2



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

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

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

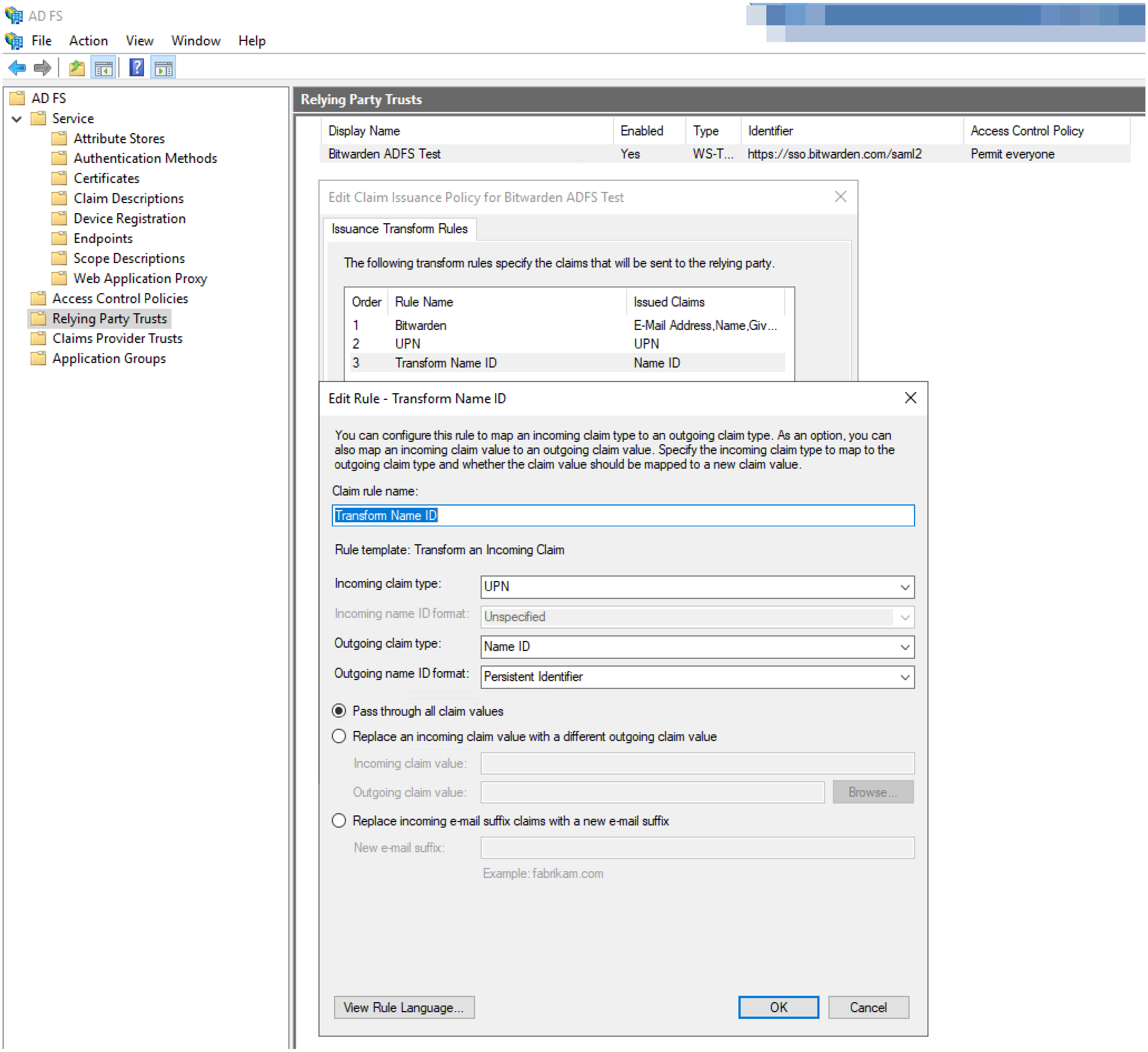
Attribute store: Active Directory

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

ADFS Rule 2

⇒Rule 3



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

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

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: 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

● 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

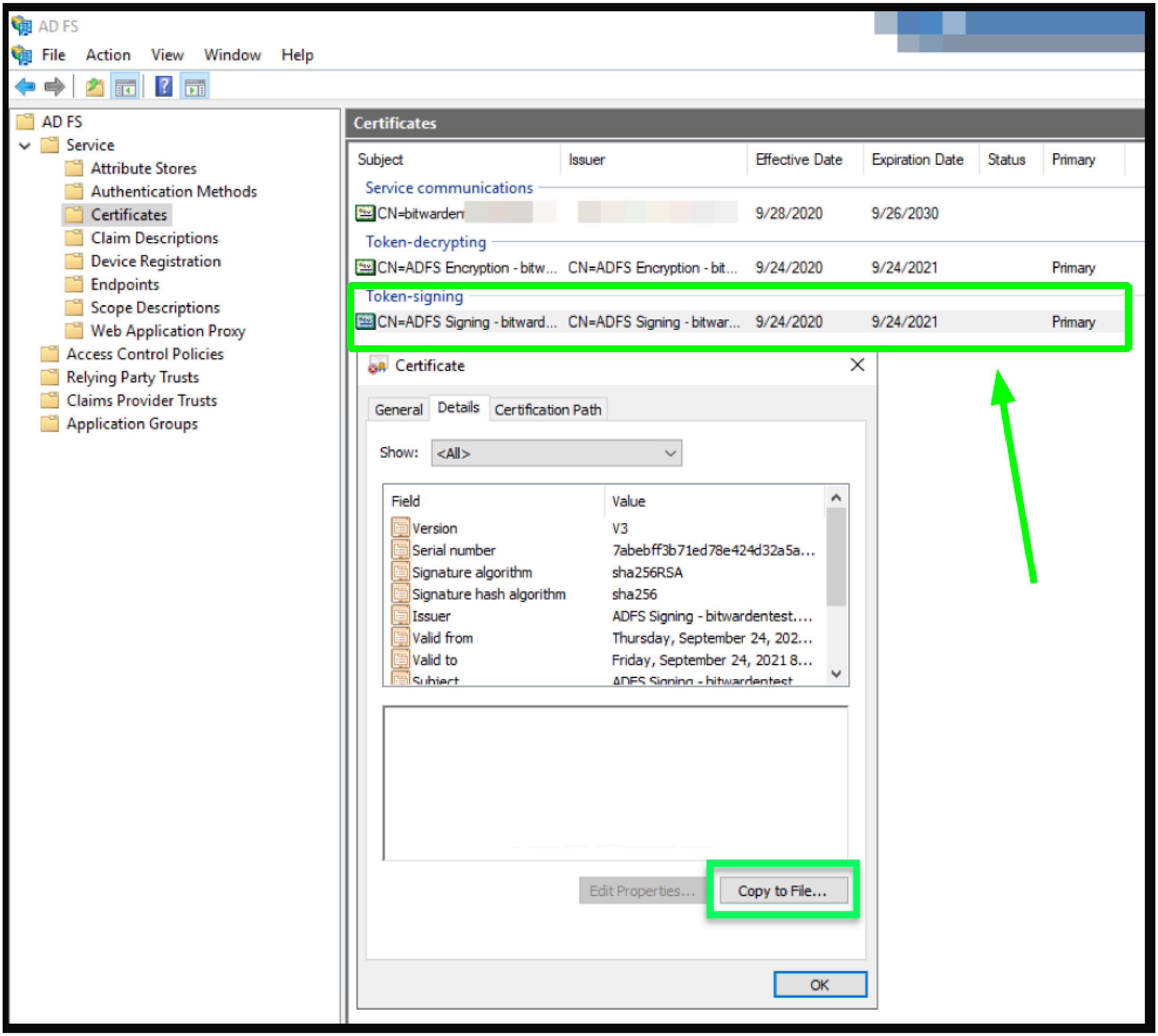
New e-mail suffix:

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:



Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=bitwarden[redacted]	[redacted]	9/28/2020	9/26/2030		
Token-decrypting					
CN=ADFS Encryption - bitw...	CN=ADFS Encryption - bit...	9/24/2020	9/24/2021		Primary
Token-signing					
CN=ADFS Signing - bitward...	CN=ADFS Signing - bitwar...	9/24/2020	9/24/2021		Primary

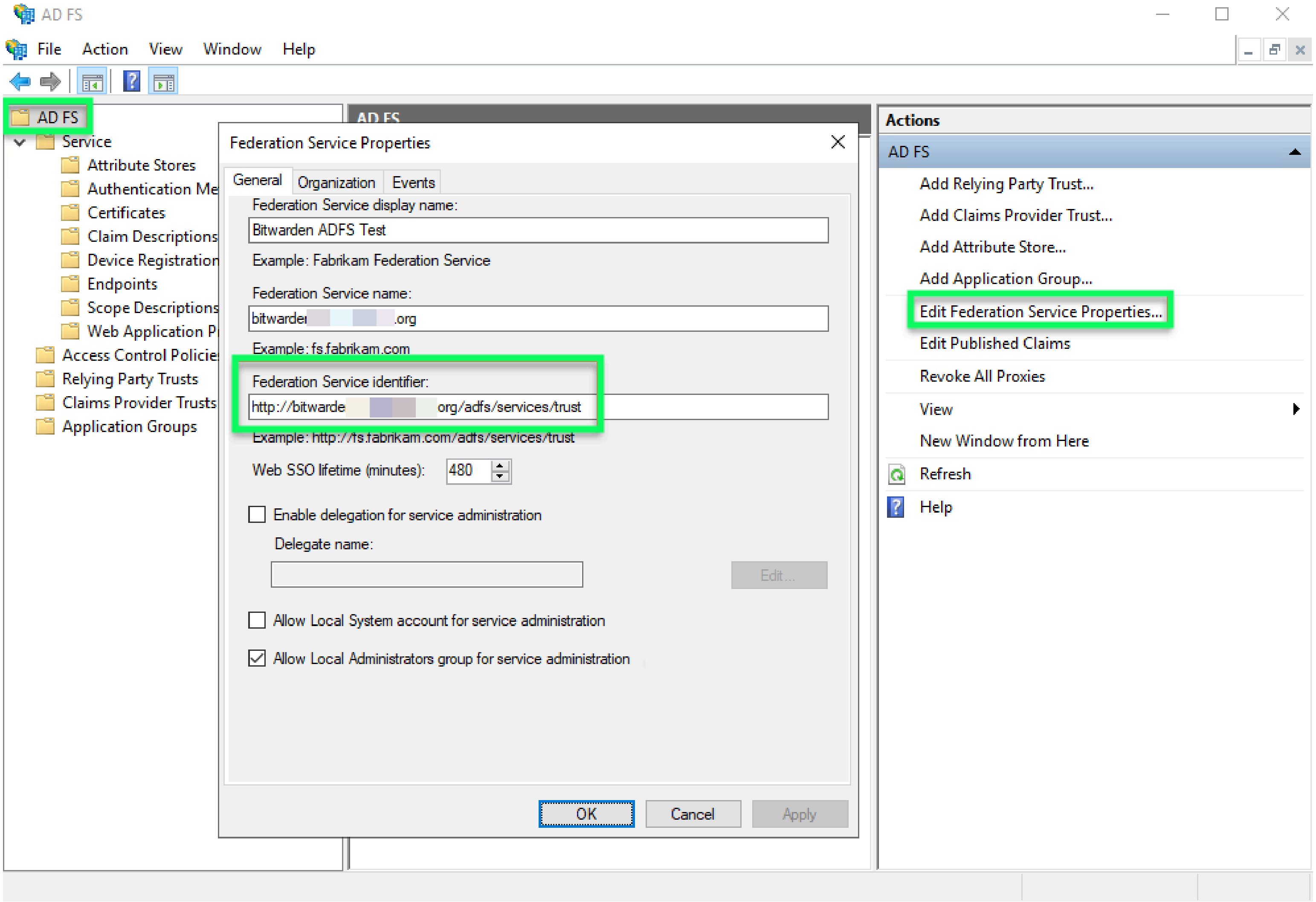
Field	Value
Version	V3
Serial number	7abebff3b71ed78e424d32a5a...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - bitwardentest....
Valid from	Thursday, September 24, 202...
Valid to	Friday, September 24, 2021 8...
Subject	ADFS Signing - bitwardentest

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**:



Federation Service Properties

Federation Service display name: Bitwarden ADFS Test

Example: Fabrikam Federation Service

Federation Service name: bitwarde[redacted].org

Example: fs.fabrikam.com

Federation Service identifier: http://bitwarde[redacted]org/adfs/services/trust

Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime (minutes): 480

☐ Enable delegation for service administration

Delegate name:

☐ Allow Local System account for service administration

☑ Allow Local Administrators group for service administration

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 with 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 `https://your-domain/adfs/ls`. You can obtain the exact value from the configuration key for SingleSignOnServce in the `FederationMetadata.xml` 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.

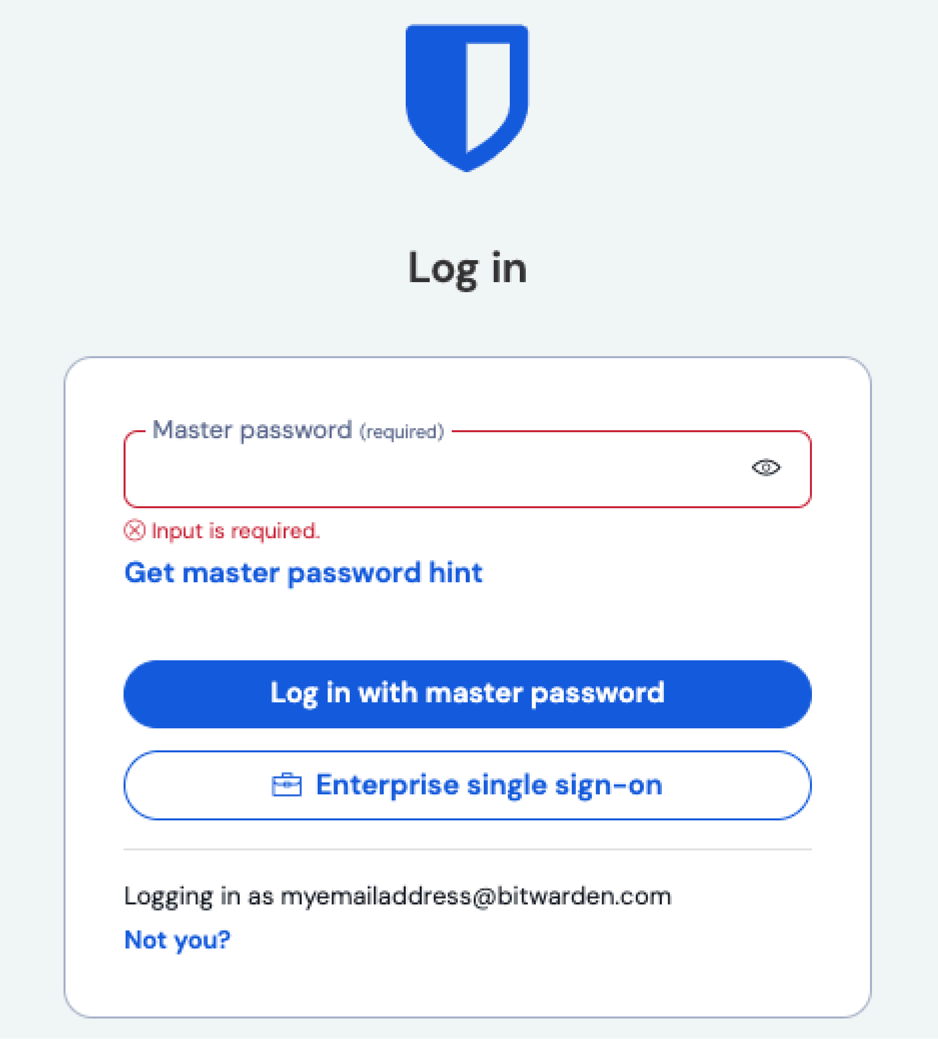
When you are done with the identity provider configuration, **Save** your work.

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, selecting **Continue**, and selecting the **Enterprise Single-On** button:



Log in

Master password (required)

Input is required.

Logging in as myemailaddress@bitwarden.com

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.