bitwarden | Help Center Article

ADMIN CONSOLE › LOGIN WITH SSO ›

OneLogin SAML Implementation

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

OneLogin SAML Implementation

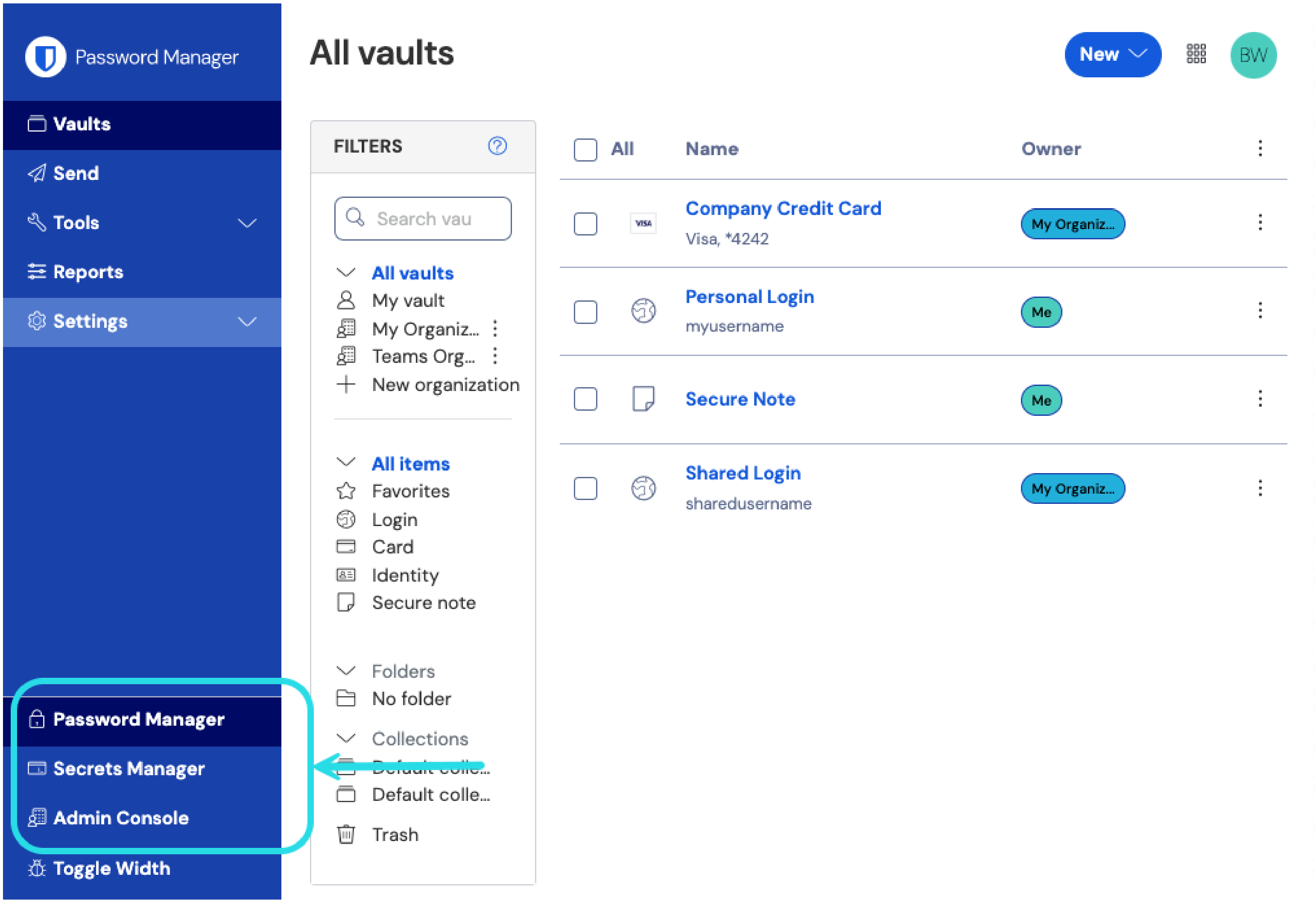
This article contains **OneLogin-specific** help for configuring login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to SAML 2.0 Configuration.

Configuration involves working simultaneously within the Bitwarden web app and the OneLogin Portal. 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

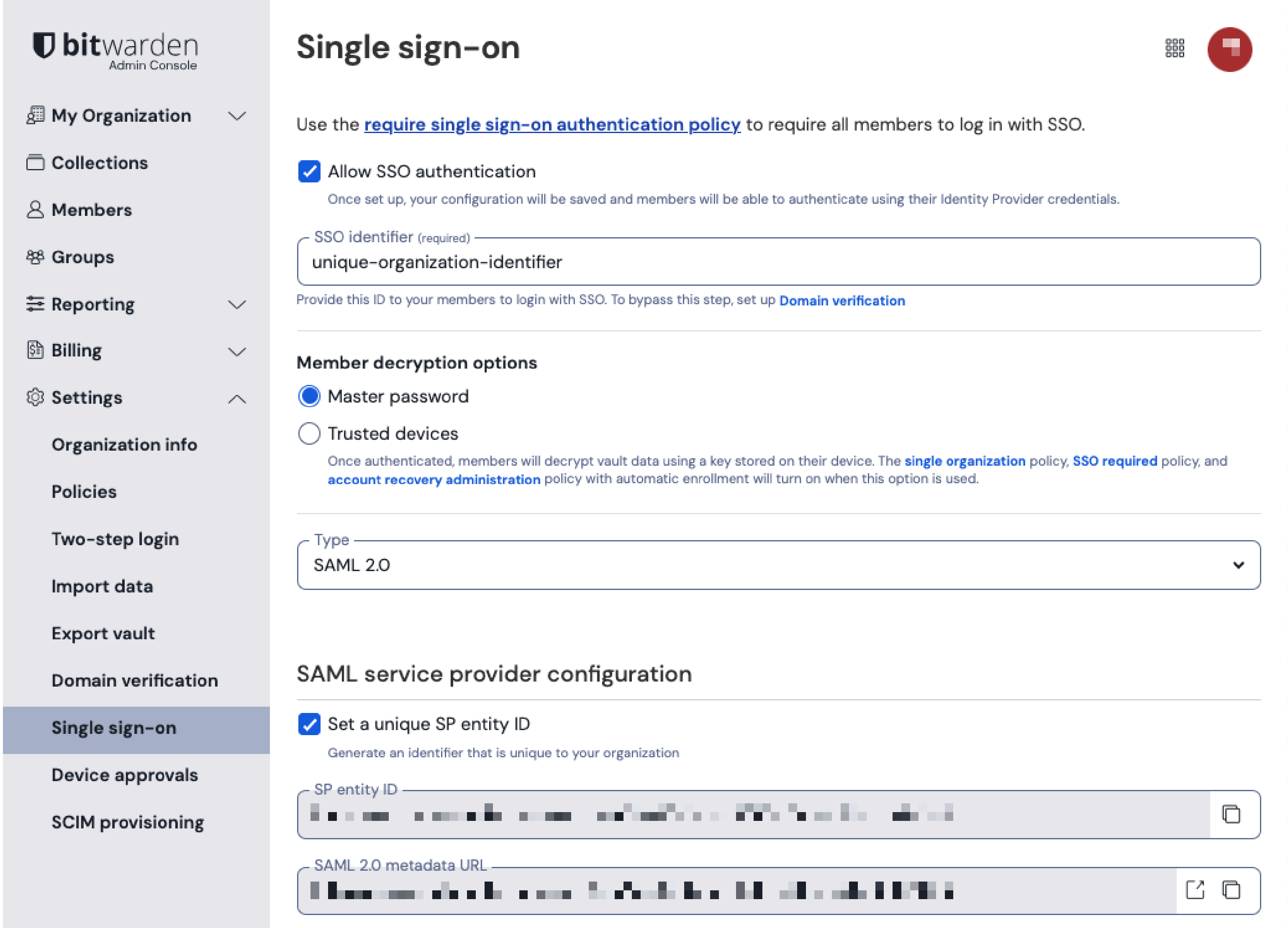
Open SSO in the web app

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:



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

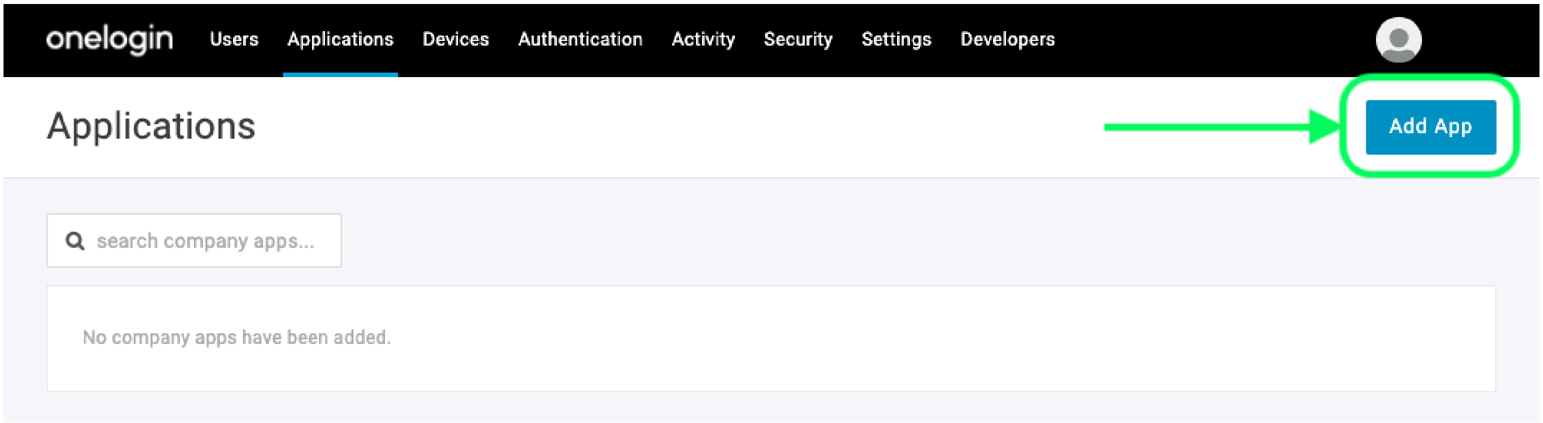
If you haven't already, create a unique **SSO identifier** for your organization and select **SAML** from the the **Type** dropdown. Keep this screen open for easy reference.

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.

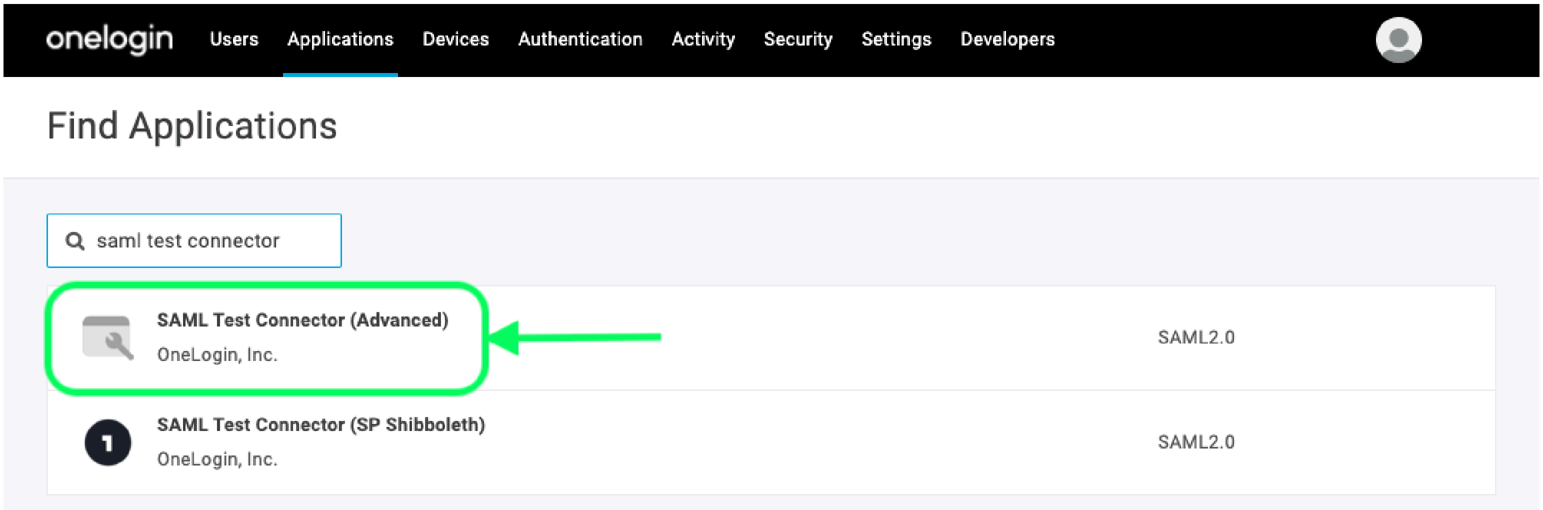
Create a OneLogin app

In the OneLogin Portal, navigate to the the **Applications** screen and select the **Add App** button:



Add an Application

In the search bar, type `saml test connector` and select the **SAML Test Connector (Advanced)** app:

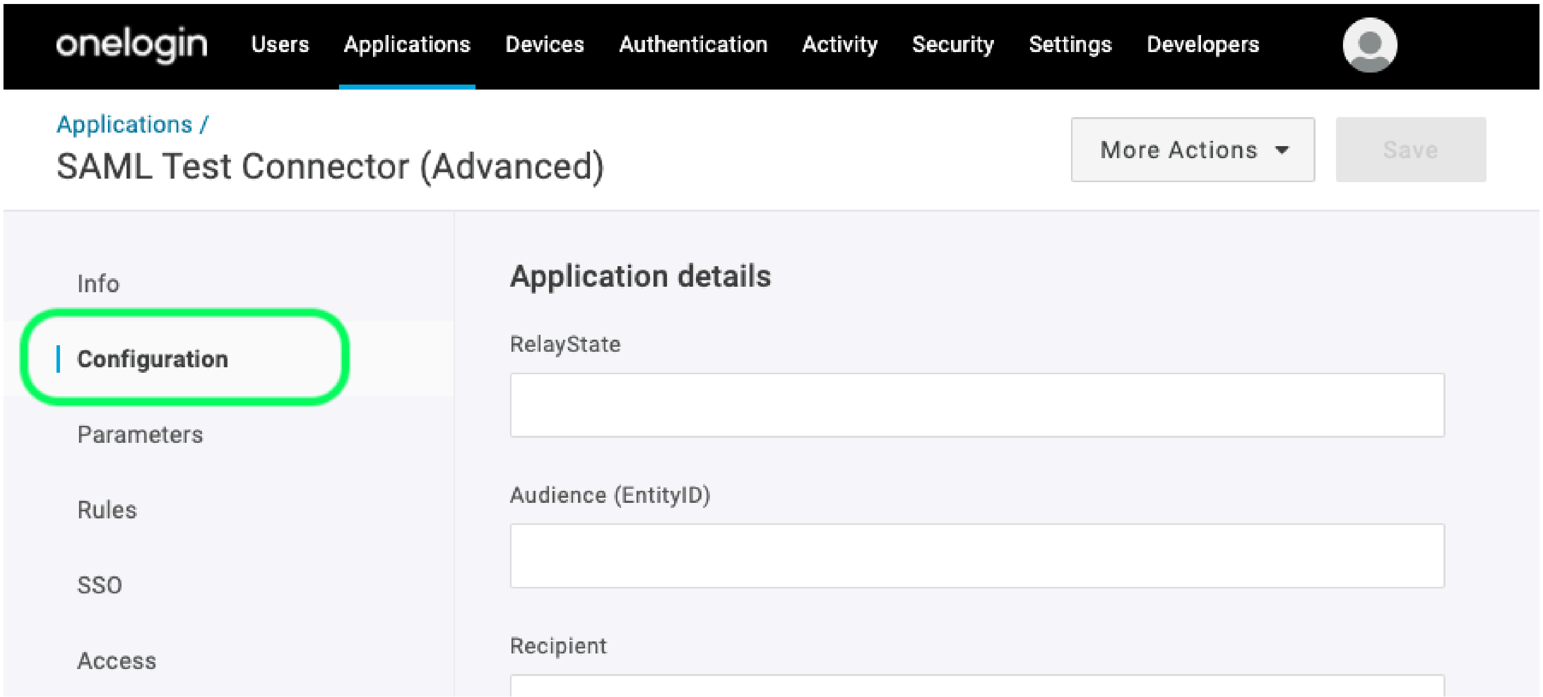


SAML Test Connector App

Give your application a Bitwarden-specific **Display Name** and select the **Save** button.

Configuration

Select **Configuration** from the left-hand navigation and configure the following information, some of which you will need to retrieve from the Single Sign-On screen:



App Configuration

Application Setting	Description
Audience (EntityID)	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.
Recipient	Set this field to the same pre-generated **SP Entity ID** used for the **Audience (Entity ID)** setting.
ACS (Consumer) URL Validator	Despite being marked **Required** by OneLogin, you don't actually need to enter information into this field to integrate with Bitwarden. Skip to the next field, **ACS (Consumer) URL**.
ACS (Consumer) 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.
SAML initiator	Select **Service Provider**. Login with SSO does not currently support IdP-initiated SAML assertions.

Application Setting	Description
SAML nameID Format	Set this field to the SAML NameID Format you want to use for SAML assertions.
SAML signature element	By default, OneLogin will sign the SAML Response. You can set this to **Assertion** or **Both**

Select the **Save** button to finish your configuration settings.

Parameters

Select **Parameters** from the left-hand navigation and use the + **Add** icon to create the following custom parameters:

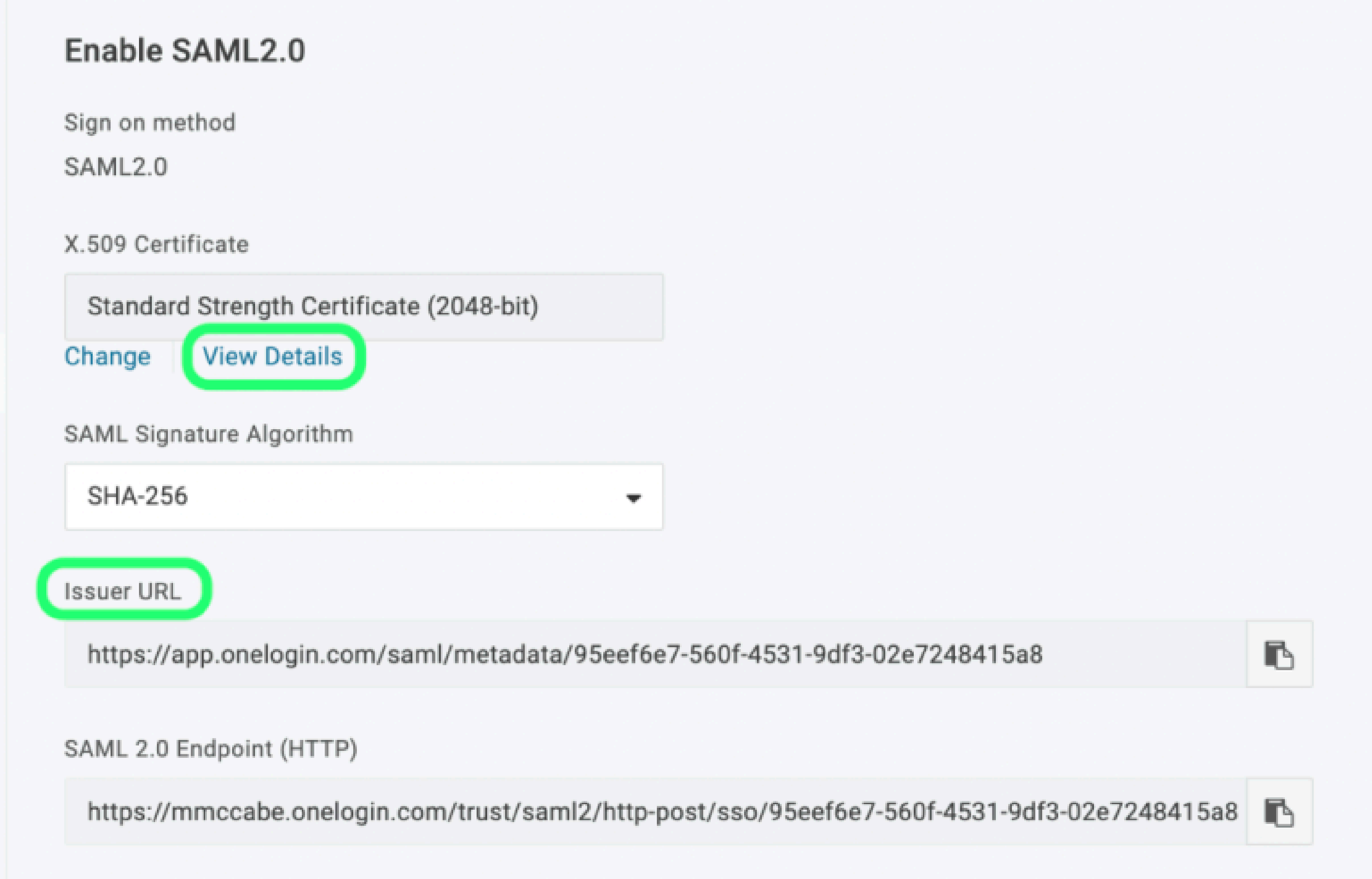
Field Name	Value
email	Email
firstname	First Name
lastname	Last Name

Select the **Save** button to finish your custom parameters.

SSO

Select **SSO** from the left-hand navigation and complete the following:

1. Select the **View Details** link under your X.509 Certificate:



Enable SAML2.0

Sign on method

SAML2.0

X.509 Certificate

Standard Strength Certificate (2048-bit)

Change | View Details

SAML Signature Algorithm

SHA-256

Issuer URL

https://app.onelogin.com/saml/metadata/95eef6e7-560f-4531-9df3-02e7248415a8

SAML 2.0 Endpoint (HTTP)

https://mmccabe.onelogin.com/trust/saml2/http-post/sso/95eef6e7-560f-4531-9df3-02e7248415a8

View your Cert

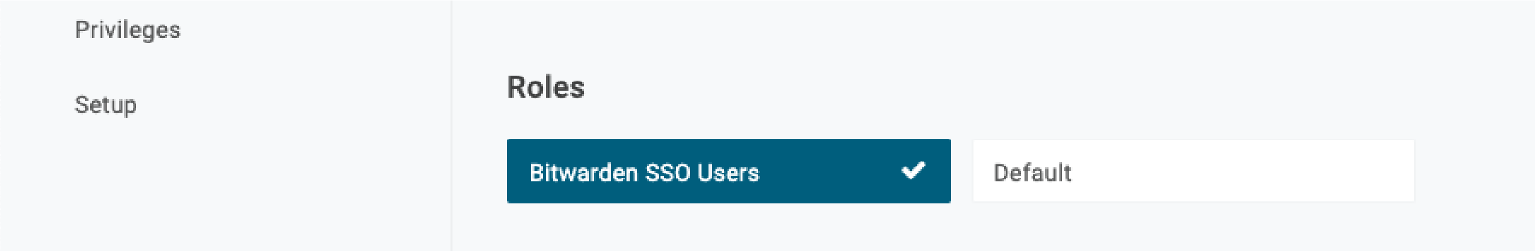
On the Certificate screen, download or copy your X.509 PEM Certificate, as you will need to use it later. Once copied, return to the main SSO screen.

2. Set your **SAML Signature Algorithm**.

3. Take note of your **Issuer URL** and **SAML 2.0 Endpoint (HTTP)**. You will need to use these values shortly.

Access

Select **Access** from the left-hand navigation. In the **Roles** section, assign application access to all the roles you would like to be able to use Bitwarden. Most implementations create a Bitwarden-specific role and instead opt to assign based on a catch-all (for example, **Default**) or based on pre-existing roles.



Roles

Bitwarden SSO Users ✓

Default

Role Assignment

Back to the web app

At this point, you have configured everything you need within the context of the OneLogin 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 according to the choices selected in the OneLogin Portal during app creation:

Field	Description
Name ID Format	Set this field to whatever you selected for the OneLogin **SAML nameID Format** field during app configuration.
Outbound Signing Algorithm	Algorithm used to sign SAML requests, by default `sha-256`.
Signing Behavior	Whether/when SAML requests will be signed. By default, OneLogin will not require requests to be signed.
Minimum Incoming Signing Algorithm	Set this field to whatever you selected for the **SAML Signature Algorithm** during app configuration
Want Assertions Signed	Check this box if you set the **SAML signature element** in OneLogin to **Assertion** or **Both** during app configuration.
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 OneLogin Portal to retrieve application values:

Field	Description
Entity ID	Enter your OneLogin **Issuer URL**, which can be retrieved from the OneLogin app SSO screen. This field is case sensitive.
Binding Type	Set to **HTTP Post** (as indicated in the SAML 2.0 Endpoint (HTTP)).
Single Sign On Service URL	Enter your OneLogin **SAML 2.0 Endpoint (HTTP)**, which can be retrieved from the OneLogin app SSO screen.
Single Log Out Service URL	Login with SSO currently **does not** support SLO. This option is planned for future development, however you may pre-configure it if you wish.

X509 Public Certificate	Paste the retrieved X.509 Certificate, removing
	`-----BEGIN CERTIFICATE-----`
	and
	`-----END CERTIFICATE-----`
	The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters **will cause certification validation to fail**.

Outbound Signing Algorithm	Select the SAML Signature Algorithm selected in the OneLogin SSO configuration section.
Disable Outbound Logout Requests	Login with SSO currently **does not** support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether OneLogin 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.

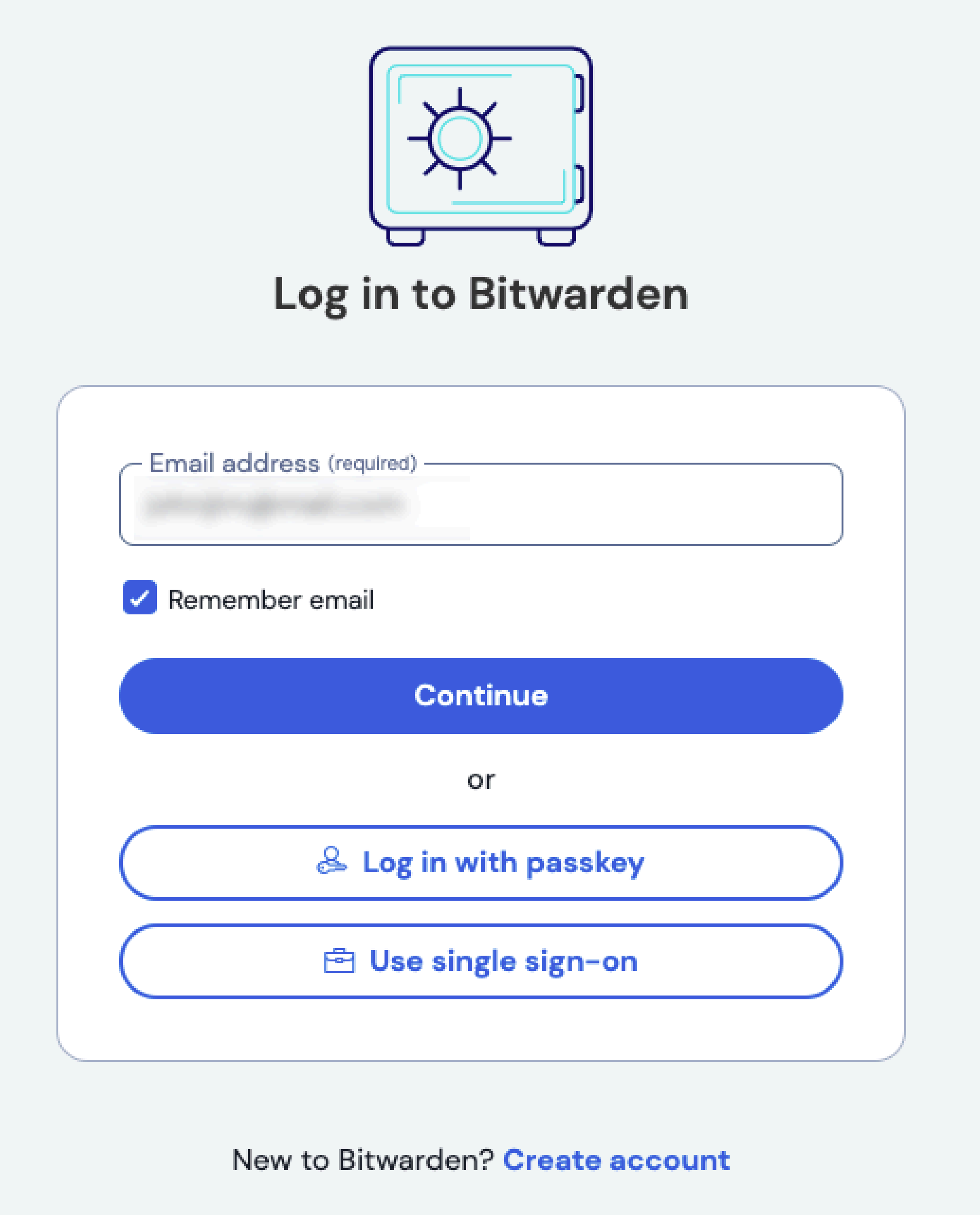
When you are done with the identity provider configuration, **Save** your work.

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:

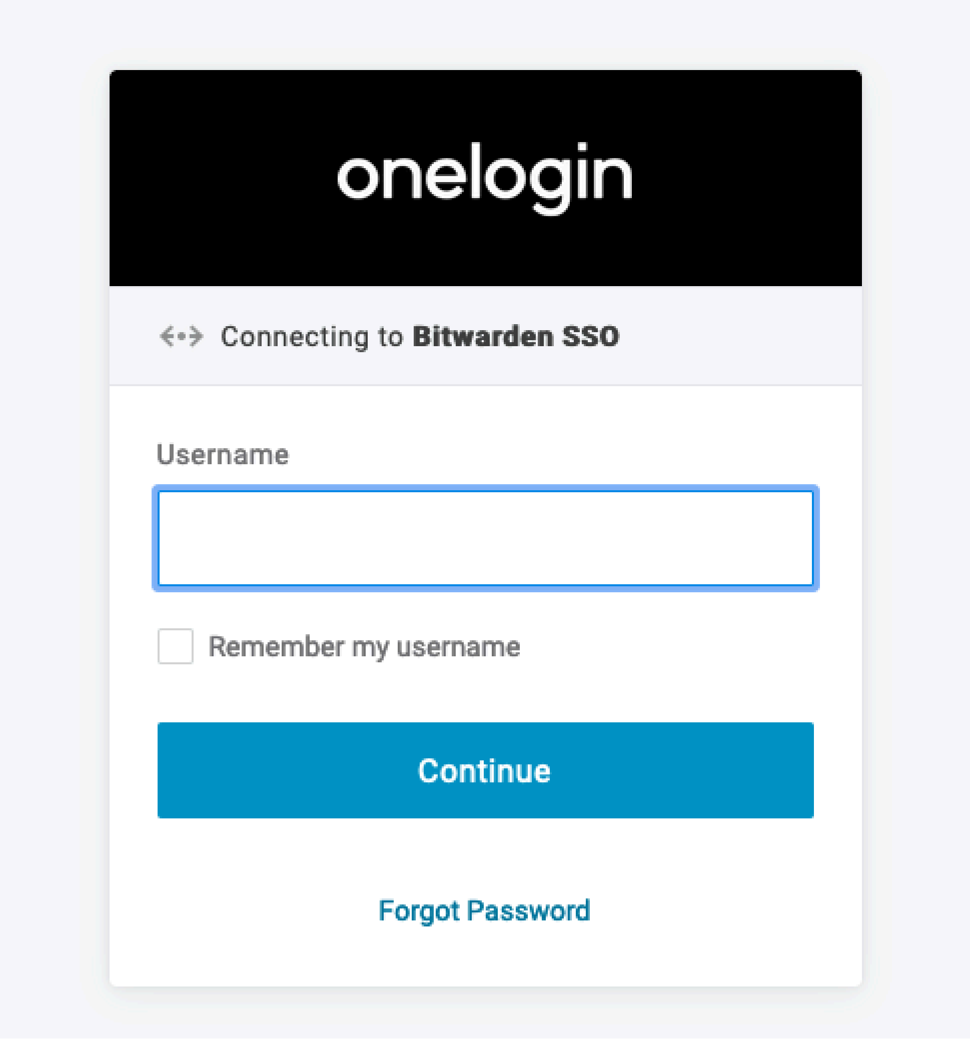


Email address (required): [redacted]

☑ Remember email

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 OneLogin login screen:



onelogin

Connecting to **Bitwarden SSO**

Username

□ Remember my username

OneLogin Login

After you authenticate with your OneLogin 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.