bitwarden | Help Center Article

ADMIN CONSOLE > LOGIN WITH SSO >

Duo SAML Implementation

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

Duo SAML Implementation

This article contains **Duo-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.

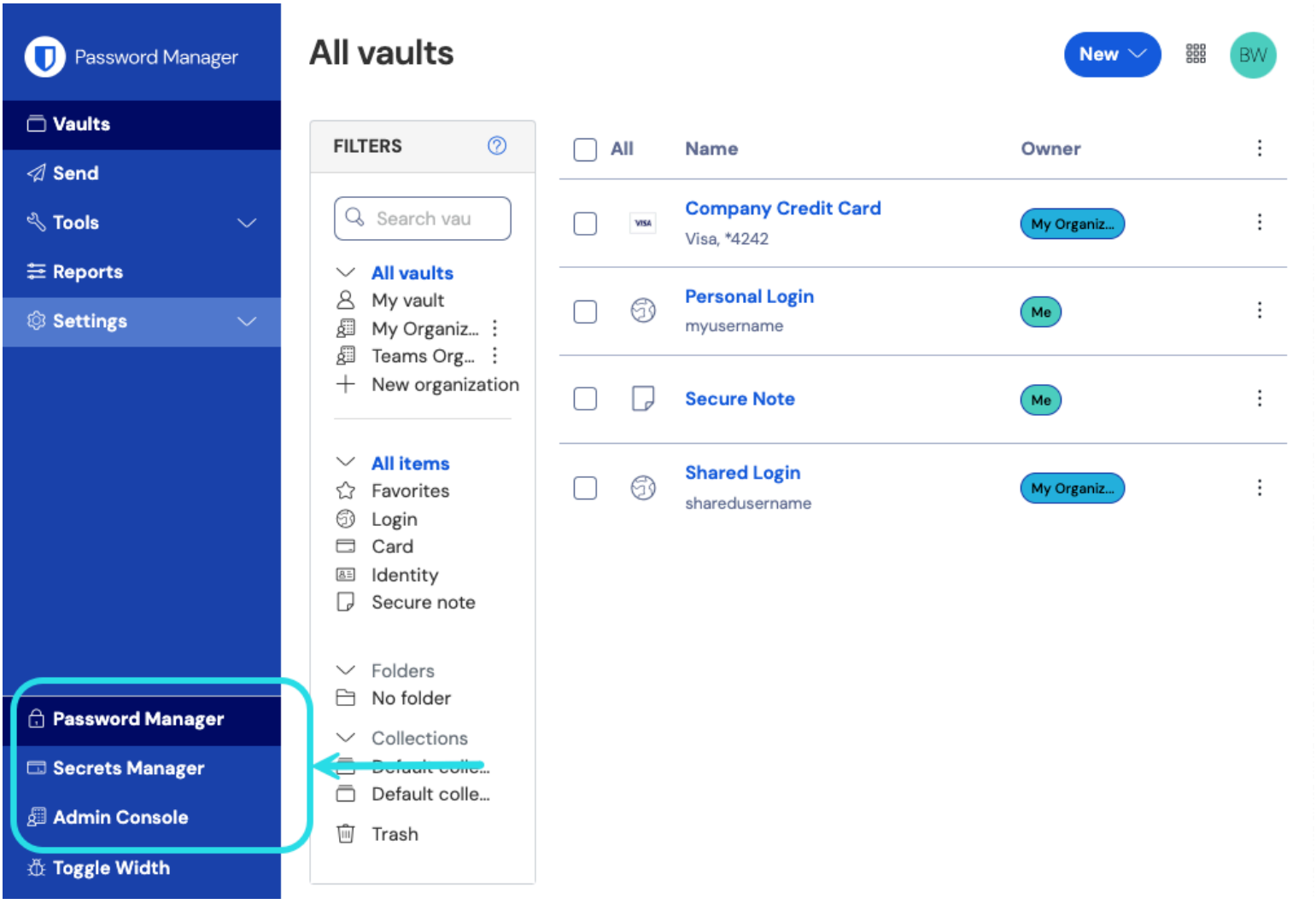
Configuration involves working simultaneously between the Bitwarden web app and the Duo Admin Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

> **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

> **Warning**
>
> This article assumes that you have already set up Duo with an Identity Provider. If you haven't, see Duo's documentation for details.

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:

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.

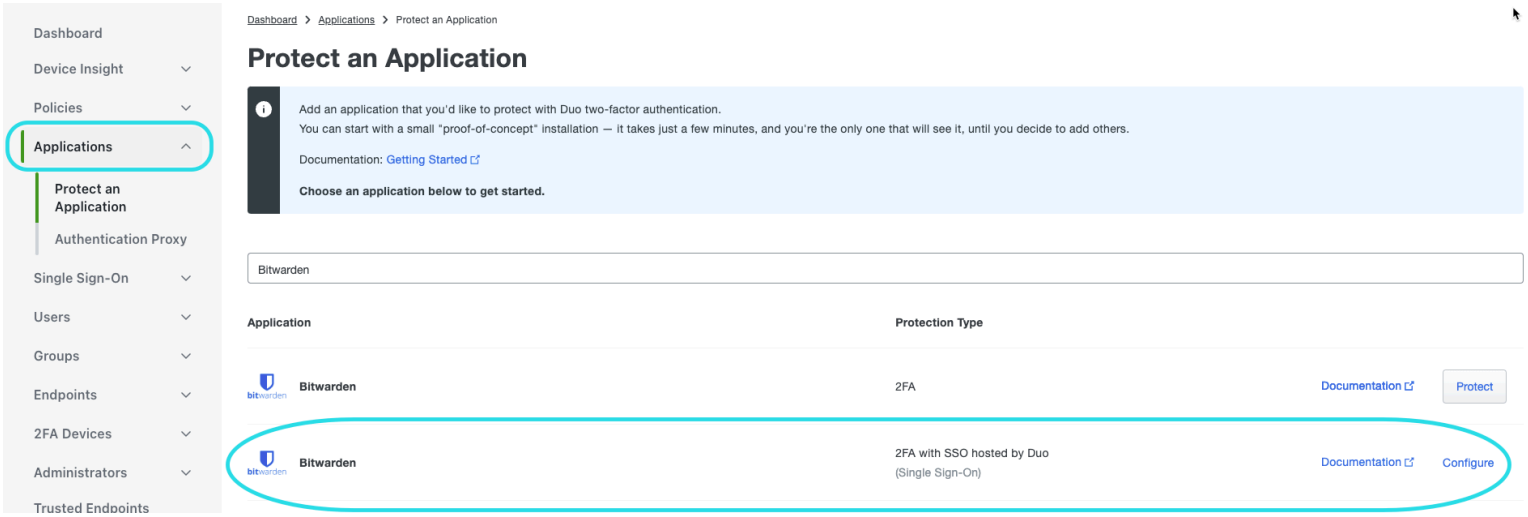
You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.

> **Tip**
>
> There are alternative **Member decryption options**. Learn how to get started using SSO with trusted devices or Key Connector.

Protect an application

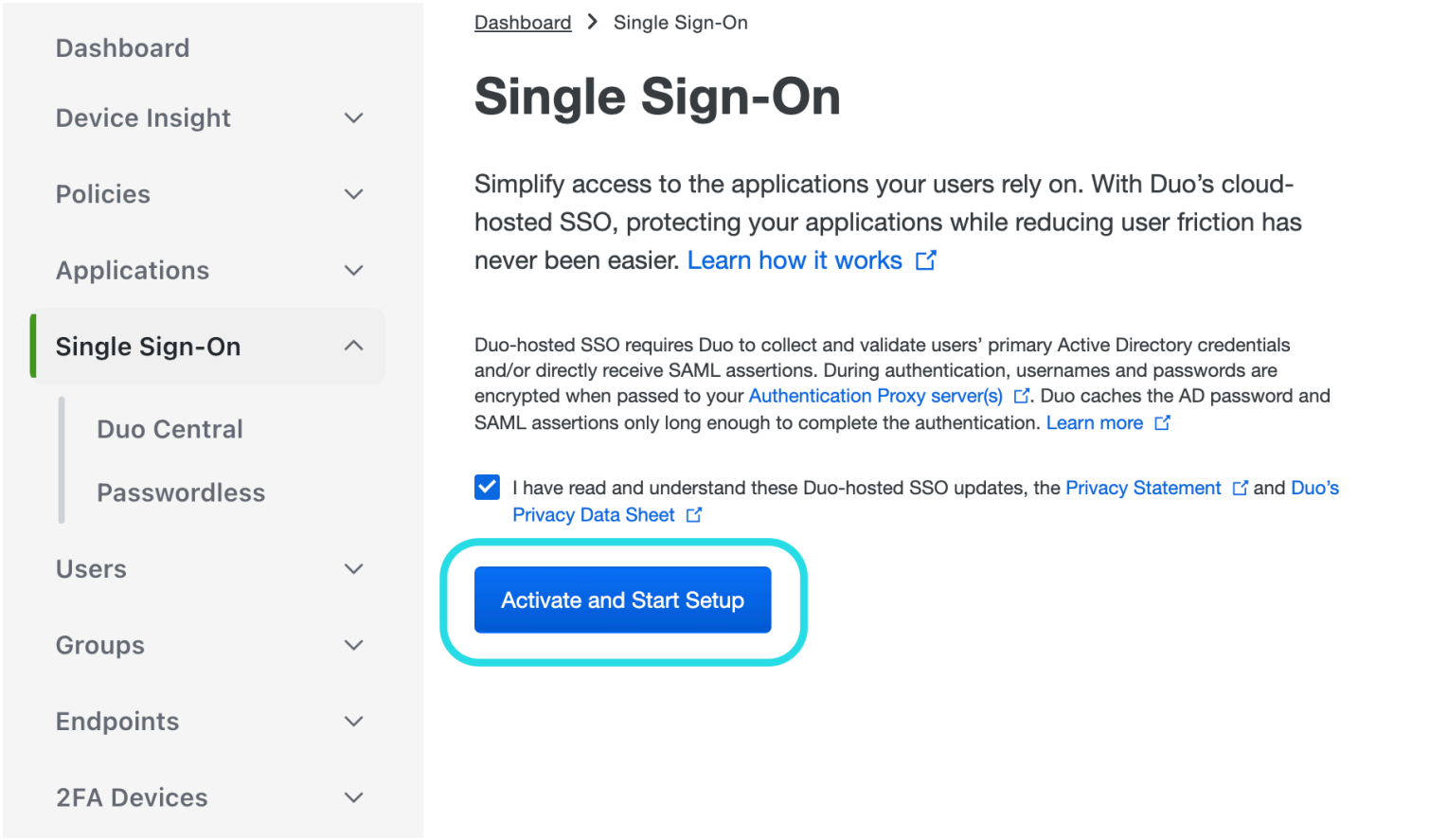
Before continuing, please refer to Duo's documentation to verify that Duo Single Sign-On has been configured with your SAML identity provider for authentication.

In the Duo Admin Portal, navigate to the **Applications** screen and select **Protect an Application**. Enter **Bitwarden** into the search bar and select **Configure** for the **Bitwarden 2FA with SSO hosted by Duo** application:



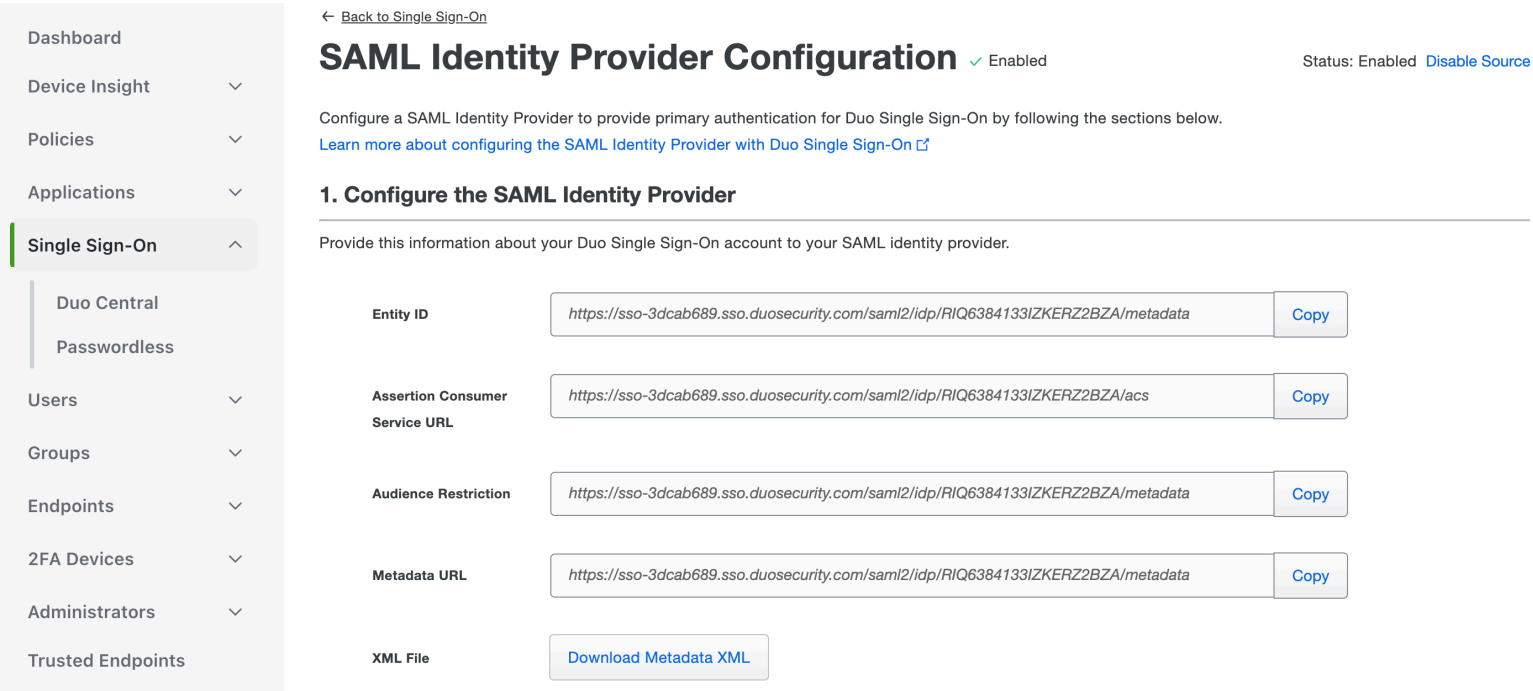
Duo Bitwarden Application

Select **Activate and Start Setup** for the newly created application:



Duo Activation and Setup

Complete the following steps and configurations on the Application configuration screen, some of which you will need to retrieve from the Bitwarden single sign-on screen:



DUO SAML Identity Provider Configuration

Metadata

You don't need to edit anything in the **Metadata** section, but you will need to use these values later:

URLs for Configuration

Downloads

Select the **Download certificate** button to download your X.509 Certificate, as you will need to use it later in the configuration.

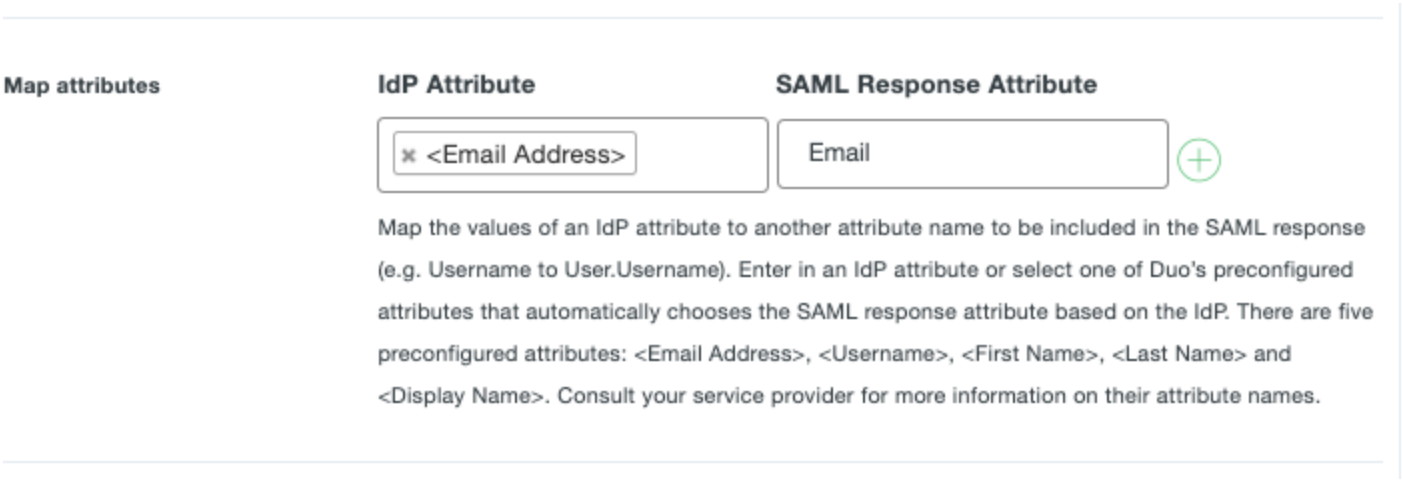
Service provider

Field	Description
Entity ID	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.

Field	Description
Assertion Consumer Service (ACS) 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.
Service Provider Login URL	Set this field to the login URL from which users will access Bitwarden. For cloud-hosted customers, this is `https://vault.bitwarden.com/#/sso` or `https://vault.bitwarden.eu/#/sso`. For self-hosted instances, this is determined by your configured server URL, for example `https://your.domain.com/#/sso`.

SAML response

Field	Description
NameID format	Set this field to the SAML NameID format for Duo to send in SAML responses.
NameID attribute	Set this field to the Duo attribute that will populate the NameID in responses.
Signature algorithm	Set this field to the encryption algorithm to use for SAML assertions and responses.
Signing options	Select whether to **Sign response**, **Sign assertion**, or both.
Map attributes	Use these fields to map IdP attributes to SAML response attributes. Regardless of which NameID attribute you configured, map the IdP `Email Address` attribute to `Email`, as in the following screenshot:



Required Attribute Mapping

Once you have finished configuring these fields, **Save** your changes.

Back to the web app

At this point, you have configured everything you need within the context of the Duo 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 Duo Admin Portal during application setup:

Field	Description
Name ID Format	NameID Format to use in the SAML request (`NameIDPolicy`). Set this field to the selected NameID format.
Outbound Signing Algorithm	Algorithm used to sign SAML requests, by default `rsa-sha256`.
Signing Behavior	Whether/when SAML requests will be signed. By default, Duo will not require requests to be signed.

Field	Description
Minimum Incoming Signing Algorithm	The minimum signing algorithm Bitwarden will accept in SAML responses. By default, Duo will sign with `rsa-sha256`, so choose that option from the dropdown unless you have selected a different option.
Want Assertions Signed	Whether Bitwarden wants SAML assertions signed. Check this box if you selected the .
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 Duo Admin Portal to retrieve application values:

Field	Description
Entity ID	Enter the **Entity ID** value of your Duo application, which can be retrieved from the Duo app Metadata section. This field is case sensitive.
Binding Type	Set this field to **HTTP Post**.
Single Sign On Service URL	Enter the **Single Sign-On URL** value of your Duo application, which can be retrieved from the Duo app Metadata section.
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 with the **Single Log-Out URL** value of your Duo application.
X509 Public Certificate	Paste the downloaded certificate, removing `-----BEGIN CERTIFICATE-----` and

Field	Description
	`-----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	Set this field to the selected SAML Response signature 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 Duo expects SAML requests to be signed.

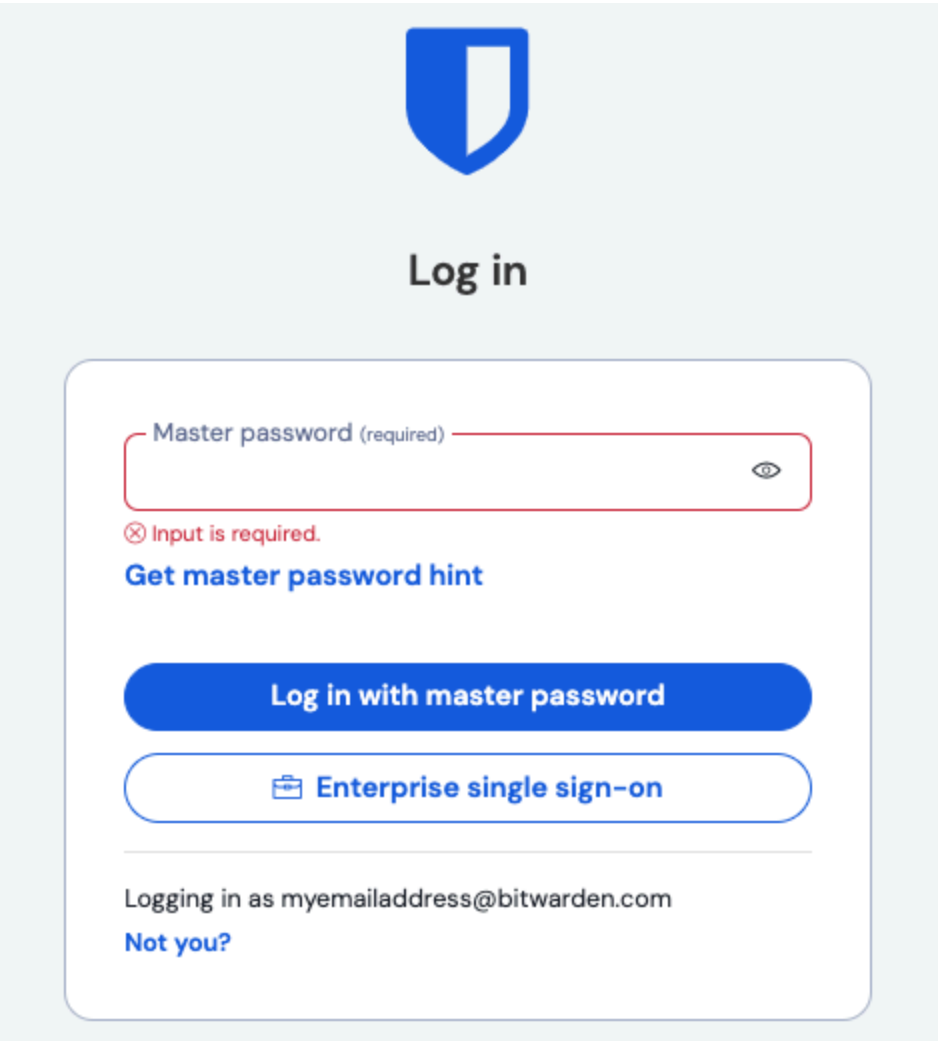
> **Note**
> When completing the X509 certificate, take note of the expiration date. Certificates will have to be renewed in order to prevent any disruptions in service to SSO end users. If a certificate has expired, Admin and Owner accounts will always be able to log in with email address and master 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 options screen

Enter the configured organization identifier and select **Log In**. If your implementation is successfully configured, you will be redirected to your source IdP's login screen.

After you authenticate with your IdP login and Duo Two-factor, 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.