

ADMIN CONSOLE > LOGGA IN MED SSO >

Ping Identity SAML Implementation

View in the help center:

<https://bitwarden.com/help/ping-identity-saml-implementation/>

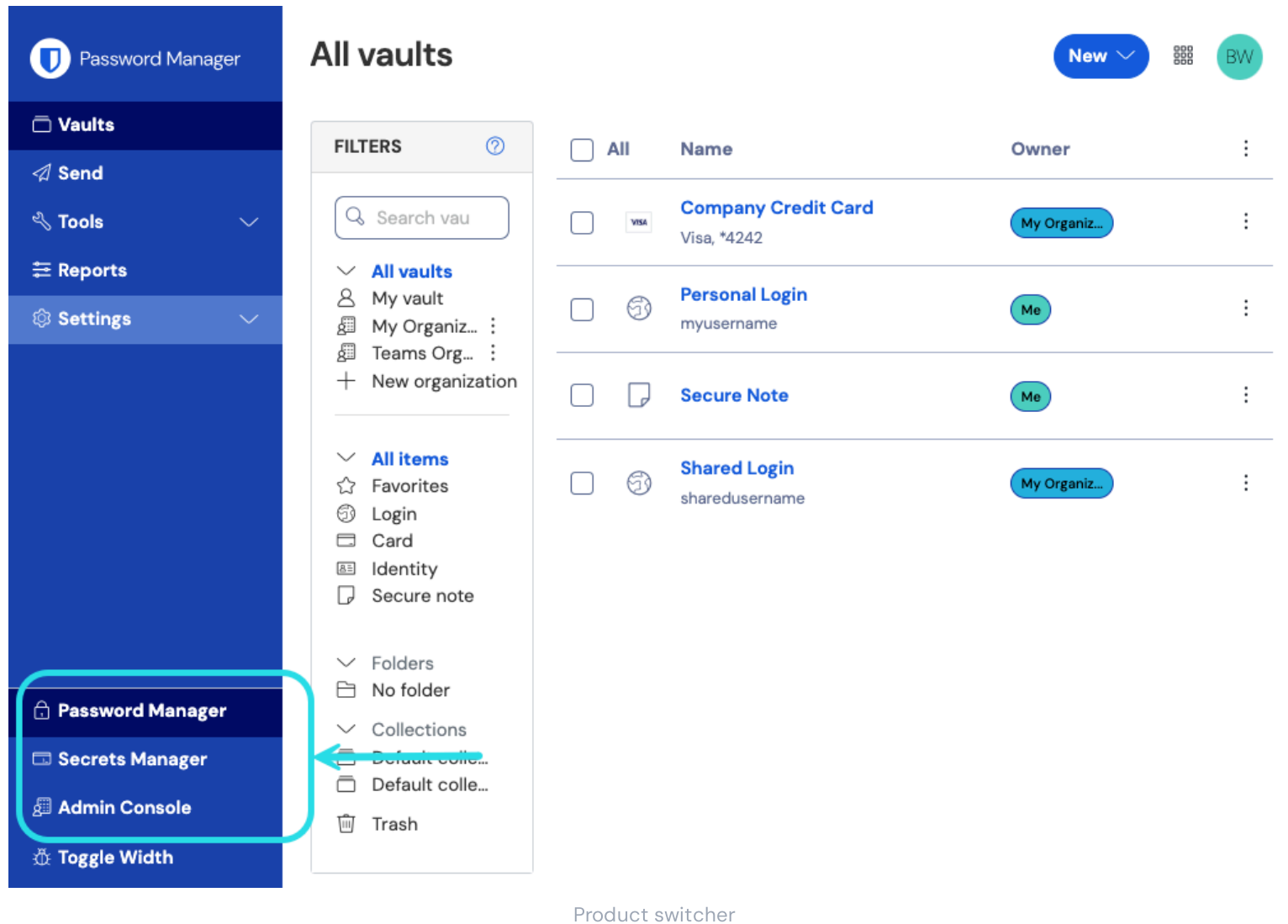
Ping Identity SAML Implementation

This article contains **Ping Identity-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 with the Bitwarden web app and the Ping Identity Administrator Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.


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:



- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

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

SAML 2.0 metadata URL

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.

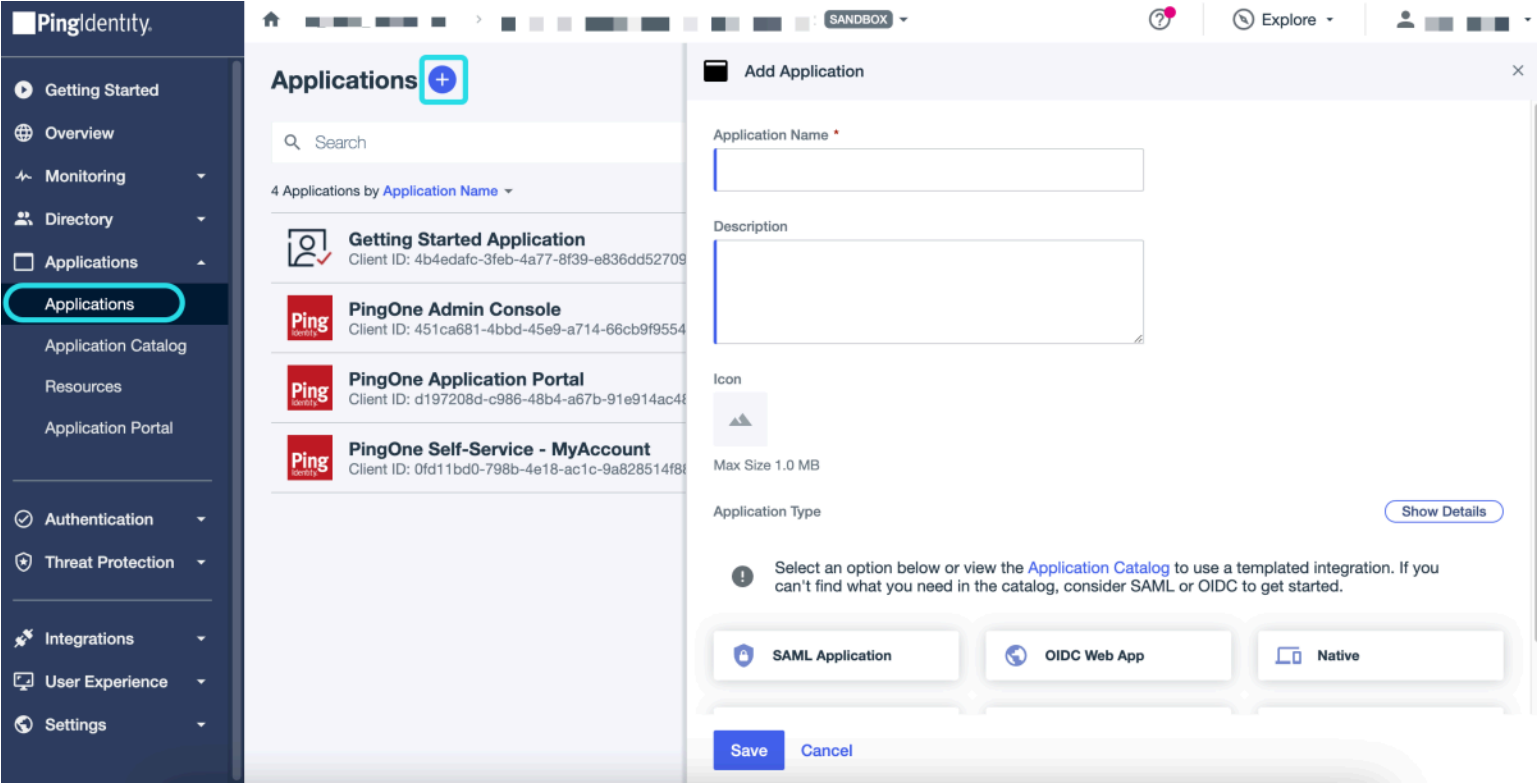
You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.



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

Create SAML app

In the Ping Identity Administrator Portal, select **Applications** and the  icon at the top of the screen to open the **Add Application** screen:



Ping Identity Add Application

- 1. Enter a Bitwarden Specific name in the **Application Name** field. Optionally add desired description details as needed.
- 2. Select the **SAML Application** option and then **Configure** once you have finished.
- 3. On the **SAML Configuration** screen select **Manually Enter**. Using the information on the Bitwarden single sign-on screen, configure the following fields:

Field	Description
ACS URL	<p>Set this field to the pre-generated Assertion Consumer Service (ACS) URL.</p> <p>This automatically-generated value can be copied from the organization's Settings → Single sign-on screen and will vary based on your setup.</p>
Entity ID	<p>Set this field to the pre-generated SP Entity ID.</p> <p>This automatically-generated value can be copied from the organization's Settings → Single sign-on screen and will vary based on your setup.</p>

Select **Save** to continue.

Back to the web app

At this point, you have configured everything you need within the context of the Ping Identity Administrator 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 information provided in the Ping Identity app **Configuration** screen:

Field	Description
Name ID Format	Set this field to the Subject Name ID Format specified in the Ping Identity app configuration.
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, Ping Identity will sign with RSA SHA-256. Select sha-256 from the dropdown.
Expect signed assertions	Whether Bitwarden expects SAML assertions to be signed. This setting should be unchecked .
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 with 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 Ping Identity Configuration screen to retrieve application values:

Field	Description
Entity ID	Set this field to the Ping Identity application's Entity ID , retrieved from the Ping Identity Configuration screen.
Binding Type	Set to HTTP POST or Redirect .
Single Sign On Service URL	Set this field to the Ping Identity application's Single Sign-on Service url, retrieved from the Ping Identity Configuration screen.
Single Log Out 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	<p>Paste the signing certificate retrieved from the application screen. Navigate to the Configuration tab and Download Signing Certificate.</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 will cause certification validation to fail.</p>
Outbound Signing Algorithm	By default, Ping Identity will sign with RSA SHA-256. Select sha-256 from the dropdown.
Disable Outbound Logout Requests	Login with SSO currently does not support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether Ping Identity 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 **Enterprise Single-On** button:



Log in to Bitwarden

Email address (required)

☒ Remember email

Continue

or

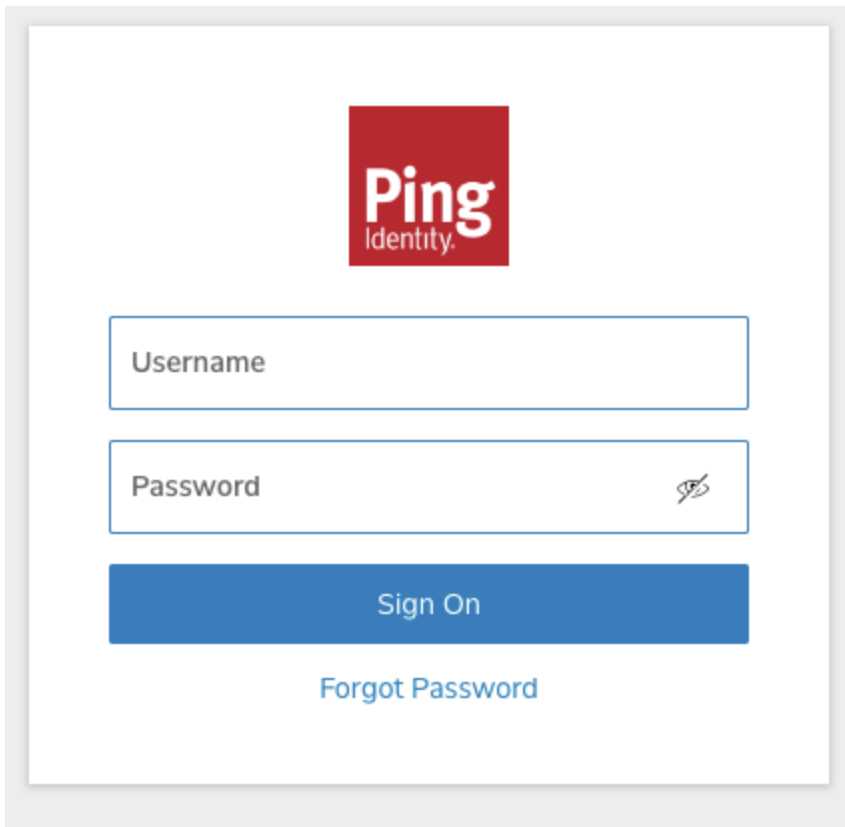
 Log in with passkey

 Use single sign-on

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 Ping Identity login screen:



Ping Identity SSO

After you authenticate with your Ping Identity 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.

Next steps

- Educate your organization members on how to [use login with SSO](#).