

管理者コンソール > SSOでログイン >

# Ping Identity SAML Implementation

ヘルプセンターで表示:

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

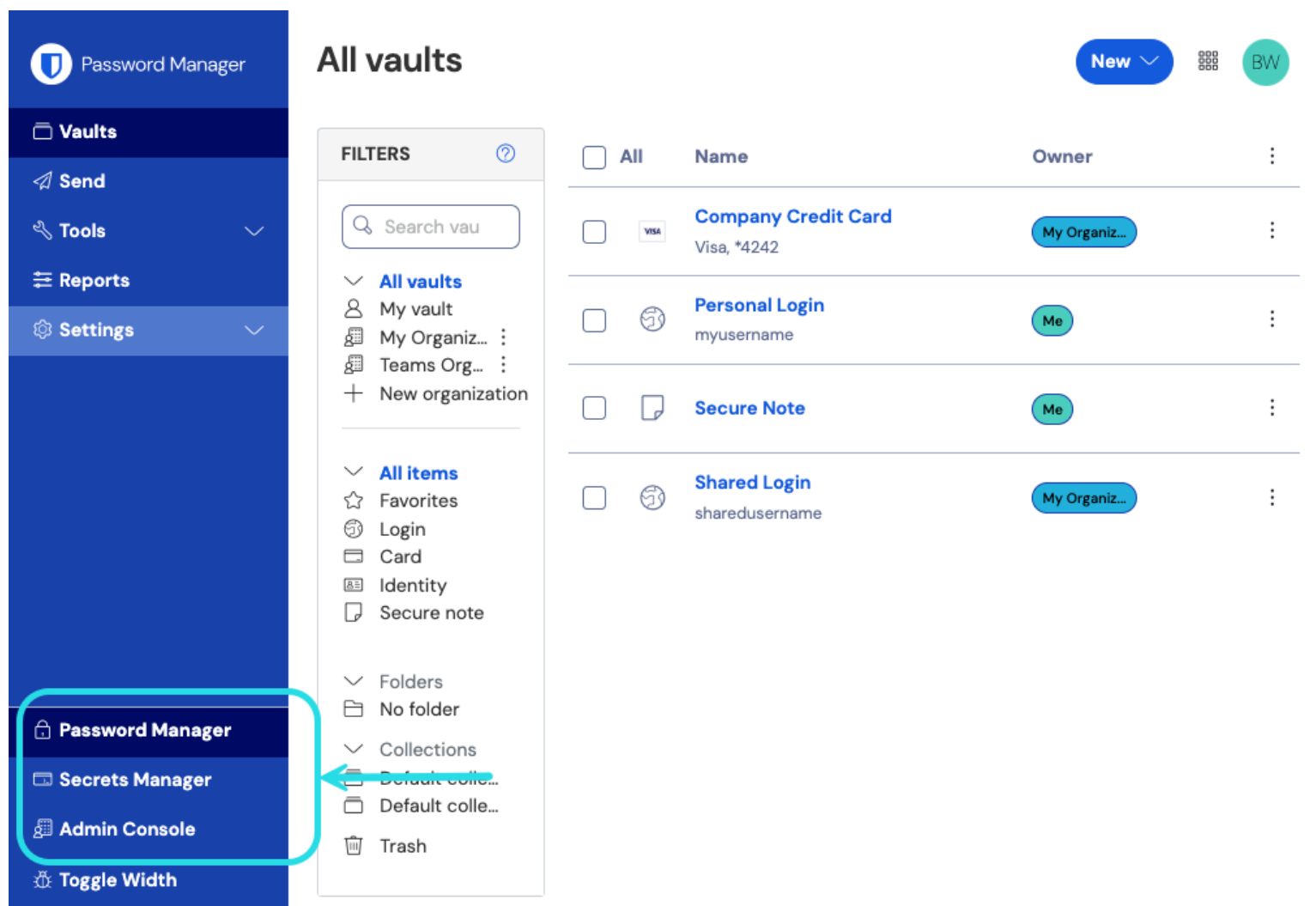
## Ping Identity SAML Implementation

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

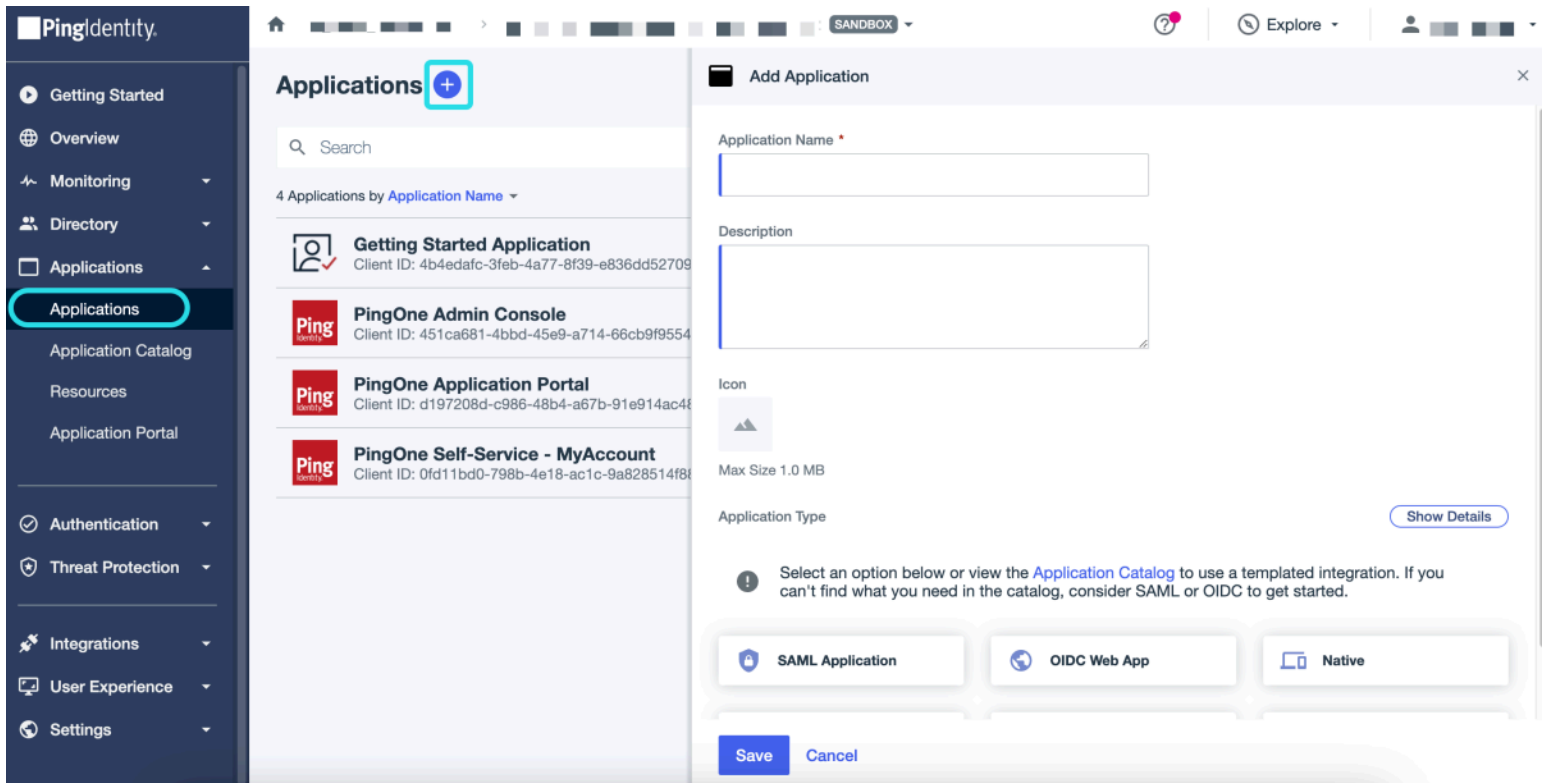
Log in to the Bitwarden web app and open the Admin Console using the product switcher:



製品-スイッチャー

Open your organization's **Settings** → **Single sign-on** 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 <b>Assertion Consumer Service (ACS) URL</b>.</p> <p>This automatically-generated value can be copied from the organization's <b>Settings</b> → <b>Single sign-on</b> screen and will vary based on your setup.</p> |
| Entity ID | <p>Set this field to the pre-generated <b>SP Entity ID</b>.</p> <p>This automatically-generated value can be copied from the organization's <b>Settings</b> → <b>Single sign-on</b> 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 <b>Subject Name ID Format</b> 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 <b>sha-256</b> from the dropdown.   |
| Expect signed assertions           | Whether Bitwarden expects SAML assertions to be signed. This setting should be <b>unchecked</b> .  |
| 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 <b>Entity ID</b> , retrieved from the Ping Identity Configuration screen.  |
| Binding Type                        | Set to <b>HTTP POST</b> or <b>Redirect</b> .   |
| Single Sign On Service URL          | Set this field to the Ping Identity application's <b>Single Sign-on Service</b> url, retrieved from the Ping Identity Configuration screen.  |
| Single Log Out URL                  | Login with SSO currently <b>does not</b> 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 <b>Configuration</b> tab and <b>Download Signing Certificate</b>.</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 <b>will cause certification validation to fail</b>.</p> |
| Outbound Signing Algorithm          | By default, Ping Identity will sign with RSA SHA-256. Select <b>sha-256</b> from the dropdown.   |
| Disable Outbound Logout Requests    | Login with SSO currently <b>does not</b> support SLO. This option is planned for future development.   |
| Want Authentication Requests Signed | Whether Ping Identity expects SAML requests to be signed.  |

### Note

X509証明書を完成させるとき、有効期限の日付をメモしてください。SSOエンドユーザーへのサービスの中断を防ぐために、証明書を更新する必要があります。証明書が期限切れになった場合でも、管理者と所有者のアカウントは常にメールアドレスとマスターパスワードでログインできます。

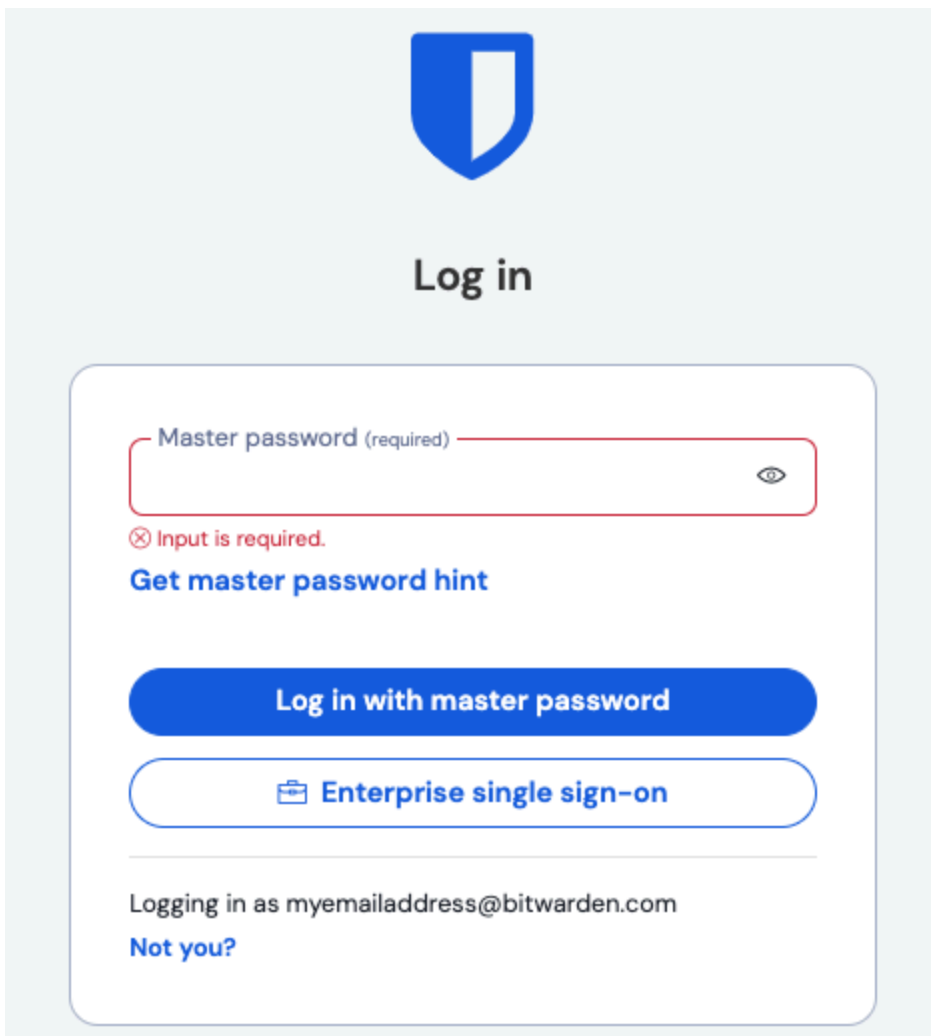
When you are done with the identity provider configuration, **Save** your work.

### Tip

シングルサインオン認証ポリシーを有効にすることで、ユーザーにSSOでログインすることを要求することができます。メモしてください、これは単一の組織ポリシーも同時に活性化する必要があります。もっと学ぶ

## Test the configuration

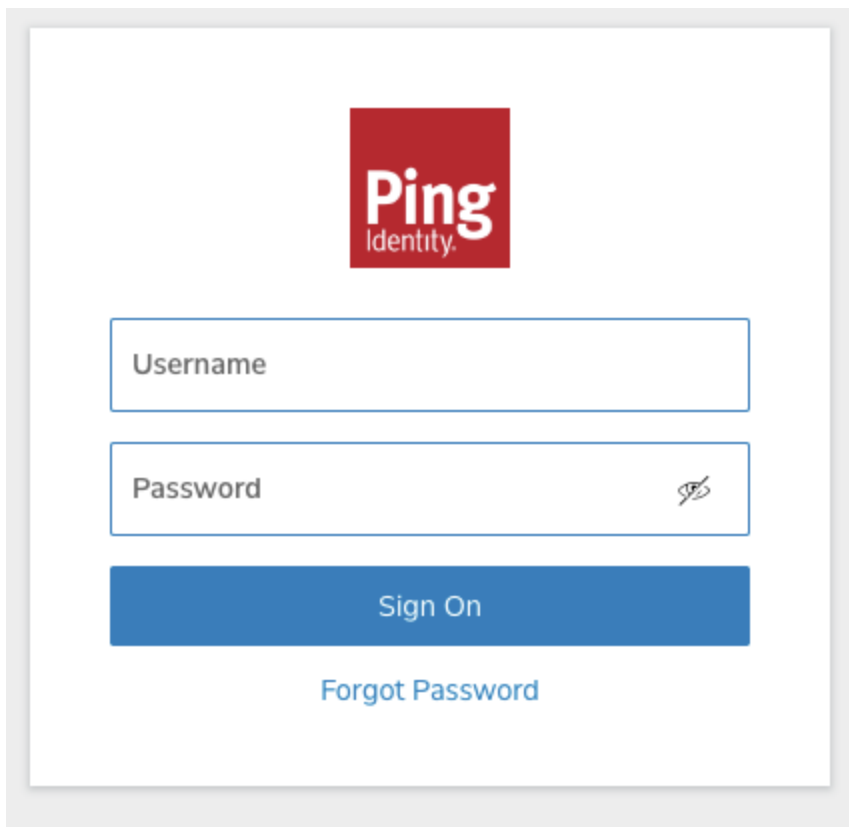
Once your configuration is complete, test it by navigating to <https://vault.bitwarden.com>, entering your email address, selecting **Continue**, and selecting the **Enterprise single sign-on** button:



The screenshot shows the Bitwarden login interface. At the top is the Bitwarden logo and the text "Log in". Below this is a form with a "Master password (required)" input field. The field is empty and has a red border, with a red "X" icon and the text "Input is required." below it. To the right of the input field is an eye icon. Below the input field is a link "Get master password hint". There are two buttons: a blue "Log in with master password" button and a white "Enterprise single sign-on" button with a briefcase icon. At the bottom of the form, it says "Logging in as myemailaddress@bitwarden.com" and a link "Not you?".

エンタープライズシングルサインオンとマスターパスワード

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は勝手なレスポンスをサポートしていませんので、あなたのIdPからログインを開始するとエラーが発生します。SSOログインフローはBitwardenから開始されなければなりません。

## Next steps

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