ADMIN CONSOLE > LOGGA IN MED SSO >

JumpCloud SAML Implementation

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

JumpCloud SAML Implementation

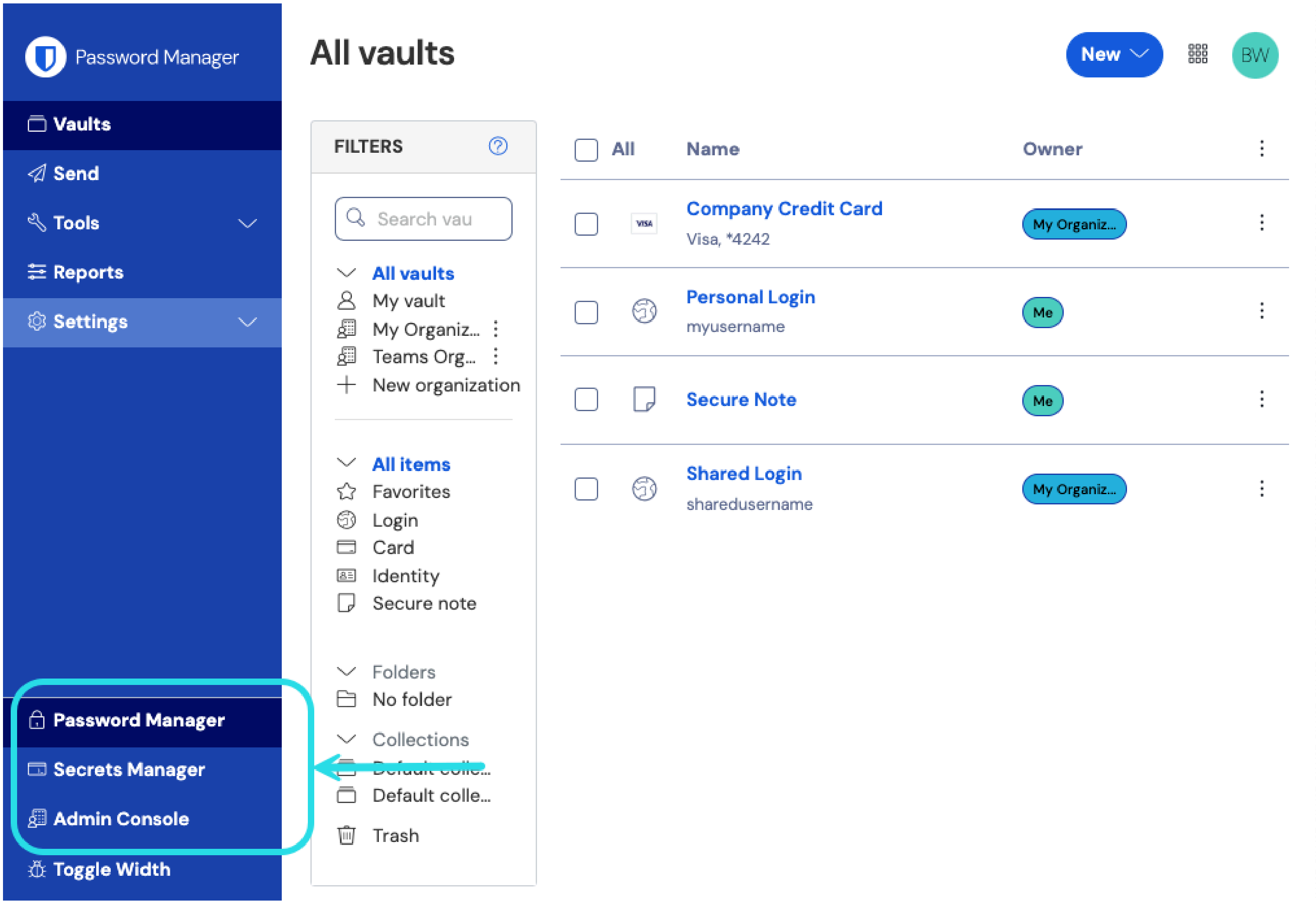
This article contains **JumpCloud-specific** help for configuring login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to SAML 2.0 Configuration.

Configuration involves working simultaneously within the Bitwarden web app and the JumpCloud 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

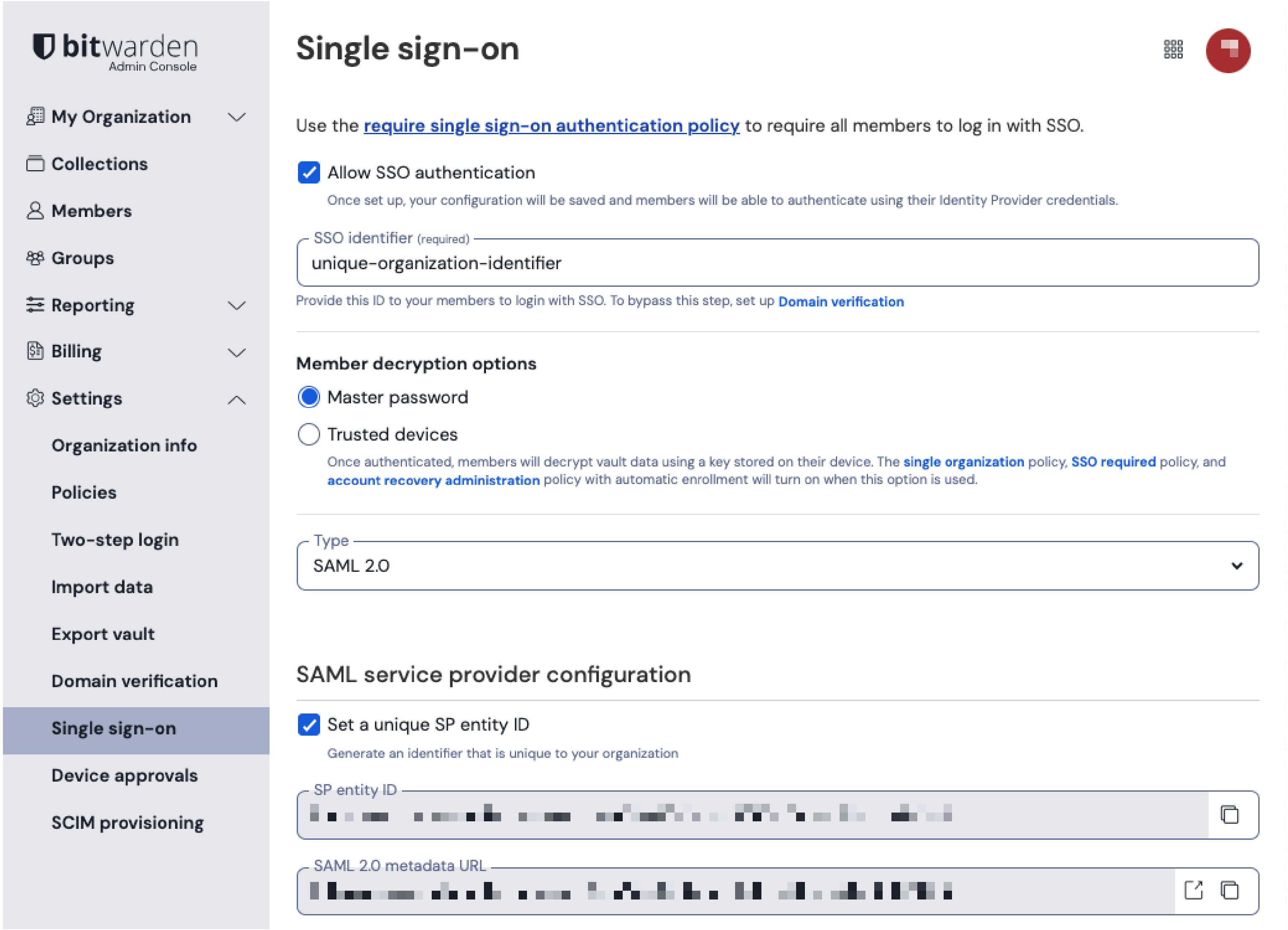
Log in to the Bitwarden web app and open the Admin Console using the product switcher:



All	Name	Owner
□	Company Credit Card Visa, *4242	My Organiz...
□	Personal Login myusername	Me
□	Secure Note	Me
□	Shared Login sharedusername	My Organiz...

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

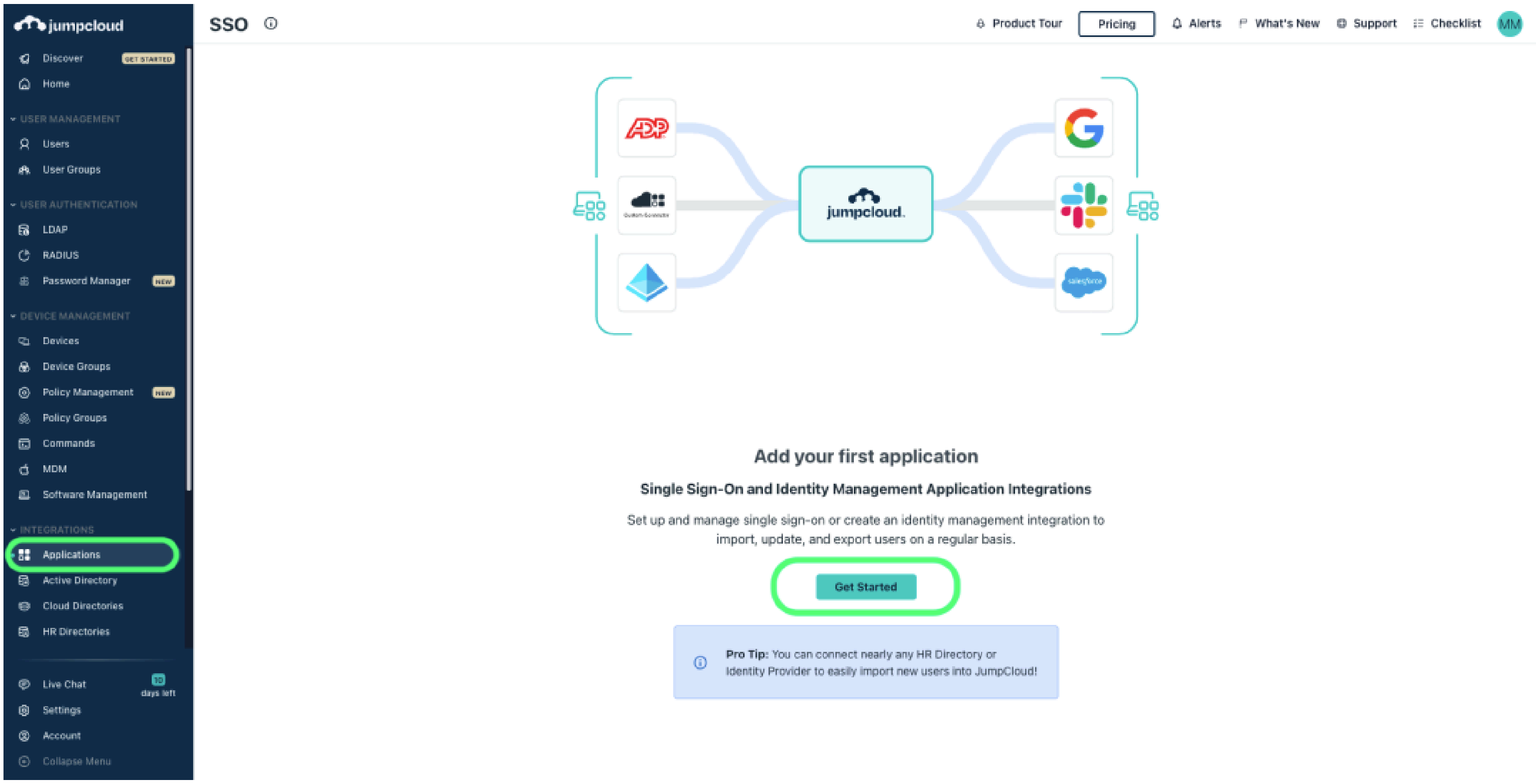
If you haven't already, create a unique **SSO identifier** for your organization and select **SAML** from the the **Type** dropdown. Keep this screen open for easy reference.

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 JumpCloud SAML application

In the JumpCloud Portal, select **Applications** from the menu and select the **Get Started** button:



Add your first application

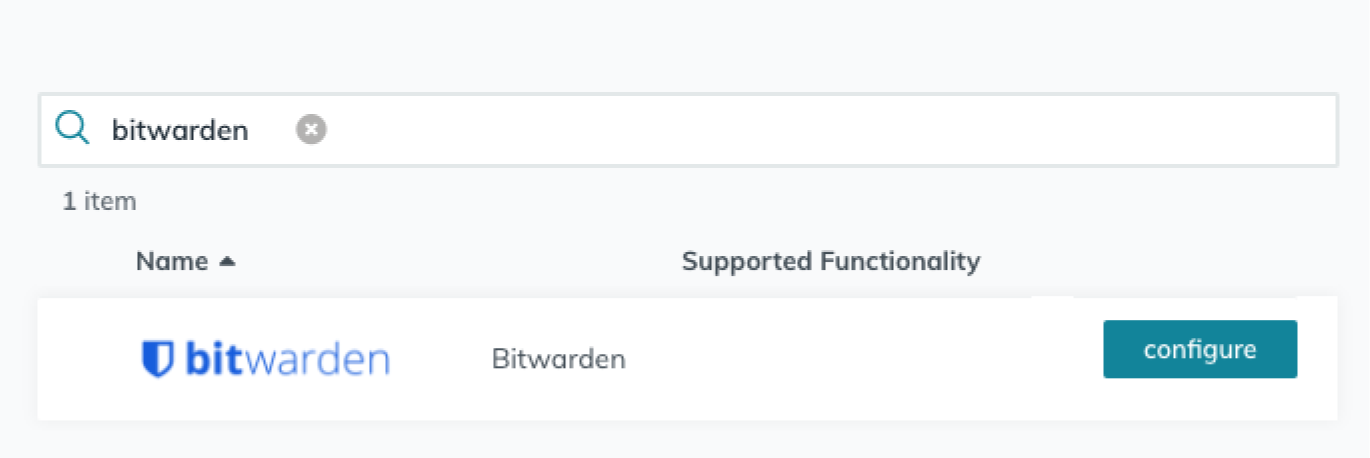
Single Sign-On and Identity Management Application Integrations

Set up and manage single sign-on or create an identity management integration to import, update, and export users on a regular basis.

Pro Tip: You can connect nearly any HR Directory or Identity Provider to easily import new users into JumpCloud!

Create Bitwarden app Jumpcloud

Enter `Bitwarden` in the search box and select the **configure** button:



Configure Bitwarden

> **Tip**
>
> If you are more comfortable with SAML, or want more control over things like NameID Format and Signing Algorithms, create a **Custom SAML Application** instead.

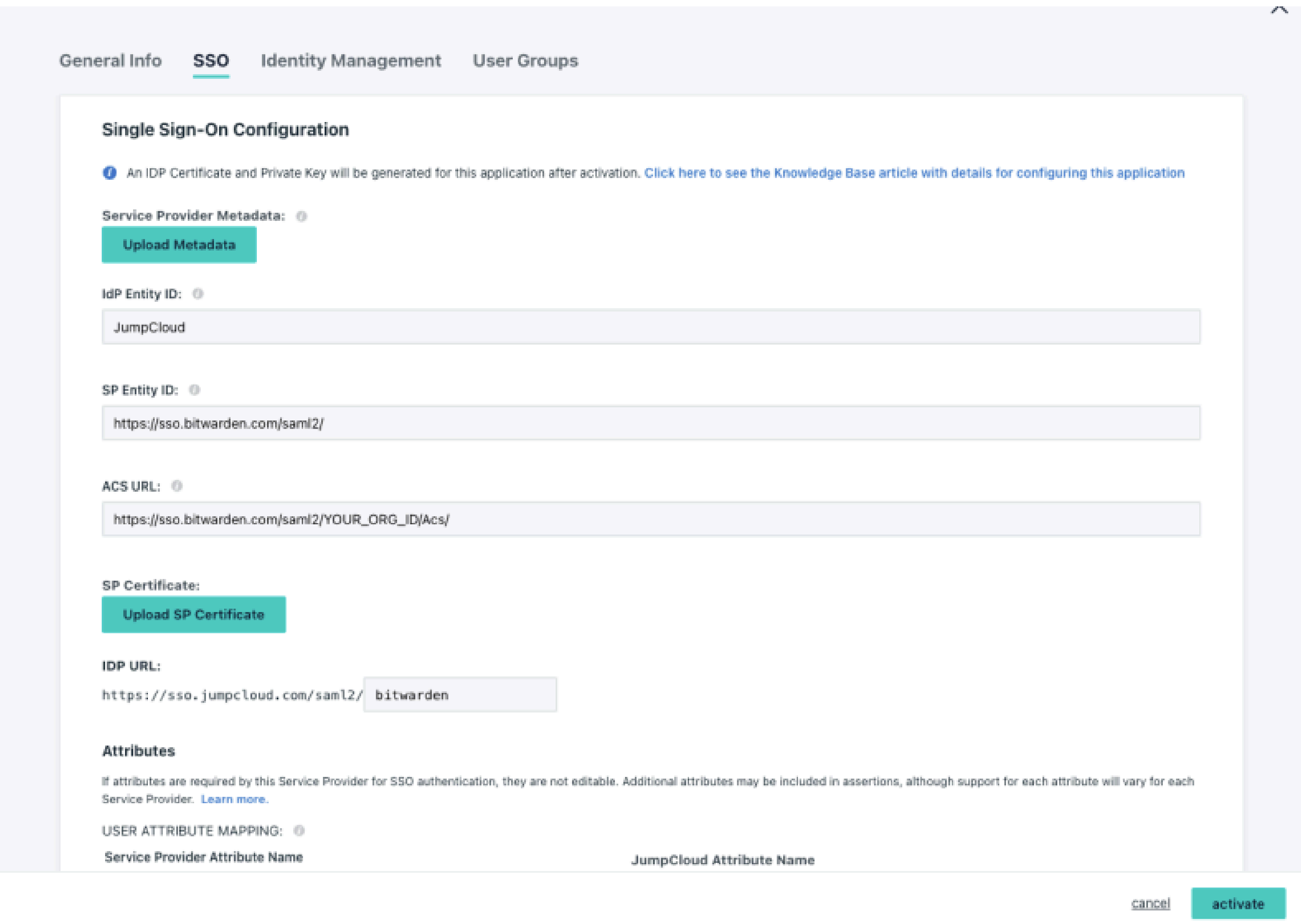
General info

In the **General Info** section, configure the following information:

Field	Description
Display Label	Give the Application a Bitwarden-specific name.

Single sign-on configuration

In the **Single Sign-On Configuration** section, configure the following information:



Single Sign-On Configuration

An IDP Certificate and Private Key will be generated for this application after activation. Click here to see the Knowledge Base article with details for configuring this application

Service Provider Metadata:

IdP Entity ID: JumpCloud

SP Entity ID: https://sso.bitwarden.com/saml2/

ACS URL: https://sso.bitwarden.com/saml2/YOUR_ORG_ID/Acs/

SP Certificate:

IDP URL: https://sso.jumpcloud.com/saml2/ bitwarden

Attributes

If attributes are required by this Service Provider for SSO authentication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary for each Service Provider. Learn more.

USER ATTRIBUTE MAPPING:

Service Provider Attribute Name	JumpCloud Attribute Name

Jumpcloud SSO configuration

Field	Description
IdP Entity ID	Set this field to a unique, Bitwarden-specific value, for example, `bitwardensso_yourcompany`.
SP 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.
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.

Custom SAML app only

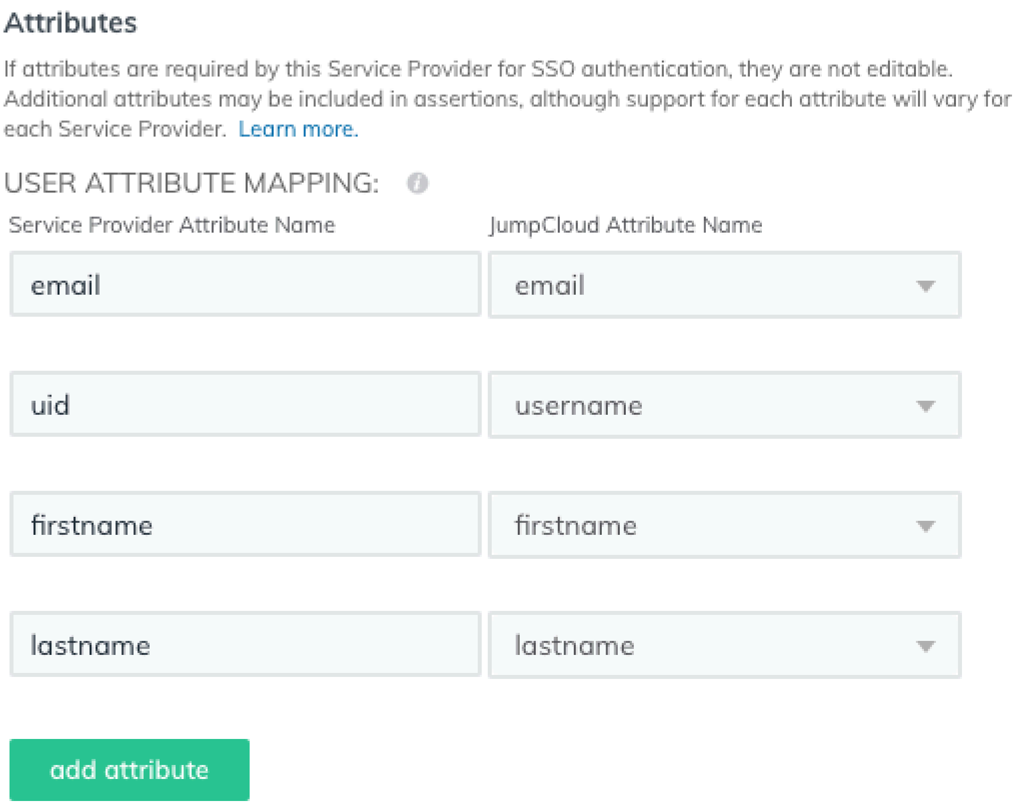
If you created a Custom SAML Application, you will also need to configure the following **Single Sign-On Configuration** fields:

Field	Description
SAMLSubject NameID	Specify the JumpCloud attribute that will be sent in SAML responses as the NameID.
SAMLSubject NameID Format	Specify the format of the NameID sent in SAML responses.
Signature Algoritm	Select the algorithm to use to sign SAML assertions or reponses.
Sign Assertion	By default, JumpCloud will sign the SAML response. Check this box the sign the SAML assertion.
Login URL	Specify the URL from which your users will login to Bitwarden via SSO. 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

Field	Description
	example `https://your.domain.com/#/sso`.

Attributes

In the **Single Sign-On Configuration → Attributes** section, construct the following SP → IdP attribute mappings. If you selected the Bitwarden Application in JumpCloud, these should already be constructed:



Attributes

If attributes are required by this Service Provider for SSO authentication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary for each Service Provider. Learn more.

USER ATTRIBUTE MAPPING:

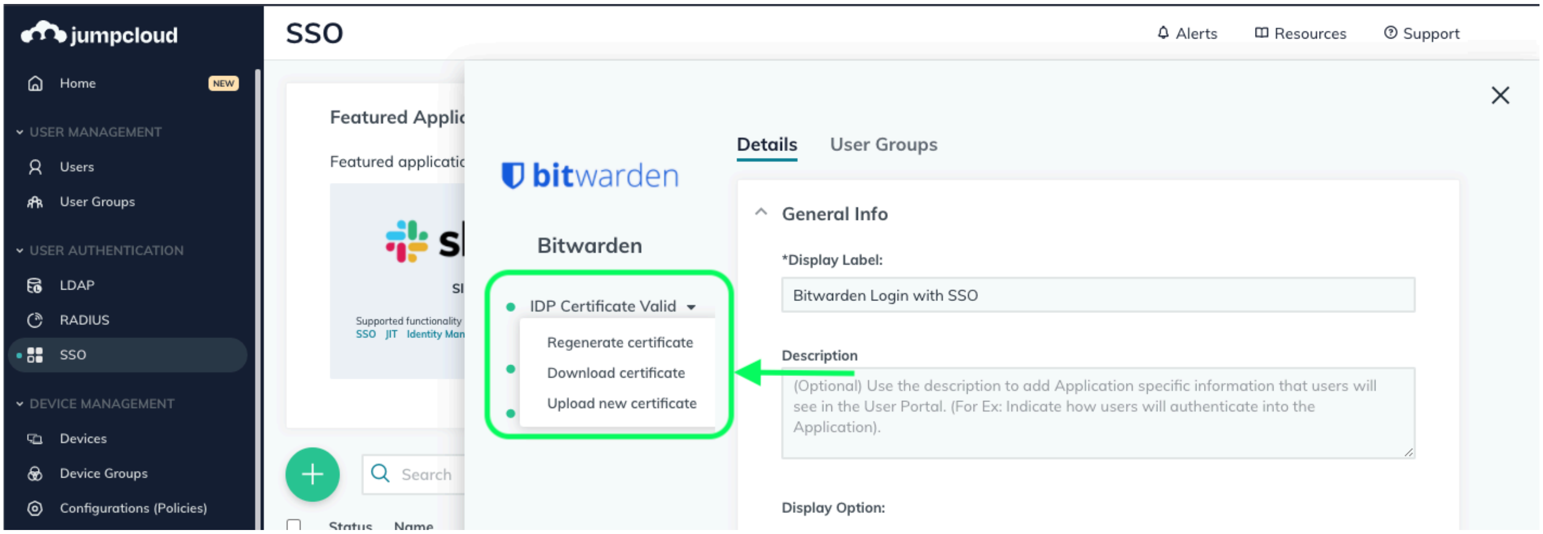
Service Provider Attribute Name	JumpCloud Attribute Name
email	email
uid	username
firstname	firstname
lastname	lastname

Attribute Mapping

Once you are finished, select the **activate** button.

Download the certificate

Once the application is activated, use the **SSO** menu option again to open the created Bitwarden application. Select the **IDP Certificate** dropdown and **Download certificate**:



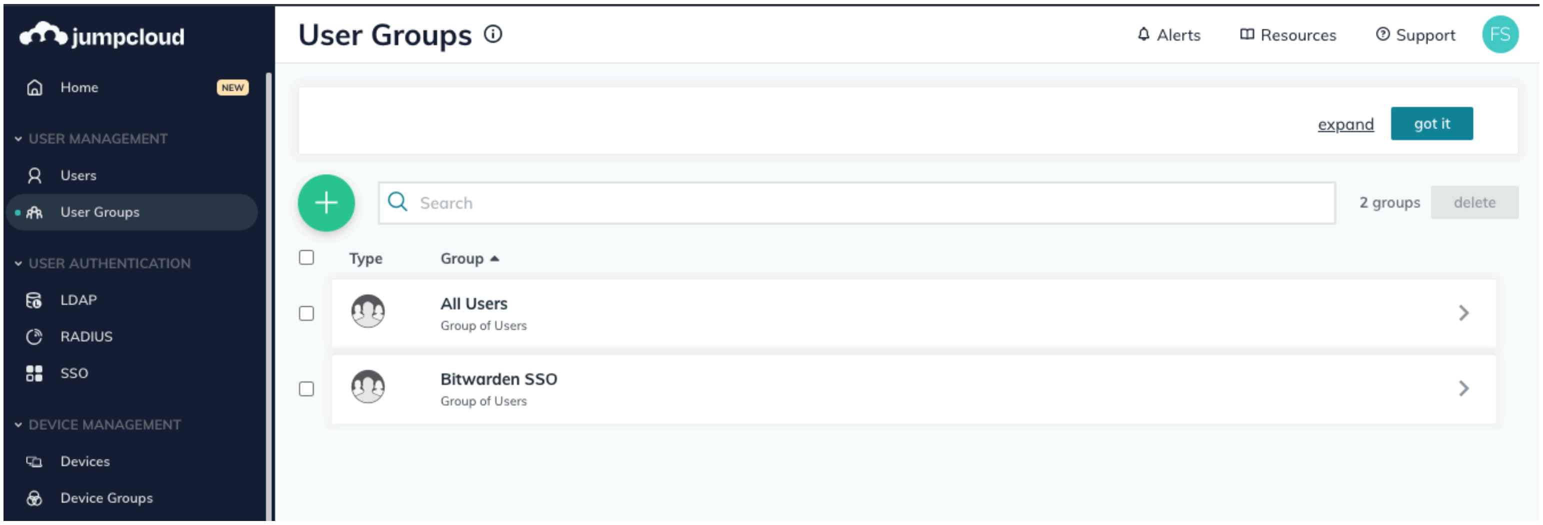
*Display Label: Bitwarden Login with SSO

Description: (Optional) Use the description to add Application specific information that users will see in the User Portal. (For Ex: Indicate how users will authenticate into the Application).

Download Certificate

Bind user groups

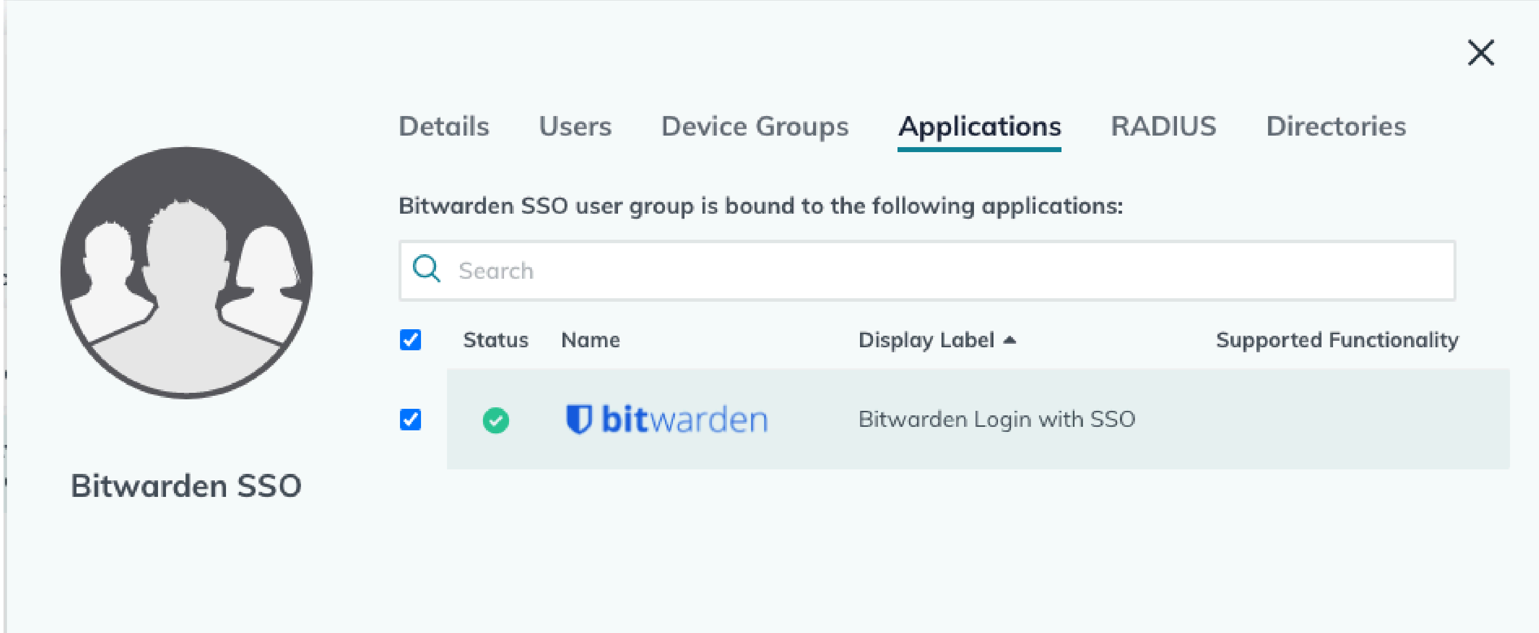
In the JumpCloud Portal, select **User Groups** from the menu:



Type	Group
□	All Users Group of Users
□	Bitwarden SSO Group of Users

User Groups

Either create a Bitwarden-specific user group, or open the All Users default user group. In either case, select the **Applications** tab and enable access to the created Bitwarden SSO application for that user group:



Bitwarden SSO user group is bound to the following applications:

☑	Status	Name	Display Label	Supported Functionality
☑	✓	bitwarden	Bitwarden Login with SSO	

Bind App Access

Tip

Alternatively, you can bind access to user groups directly from the **SSO → Bitwarden Application** screen.

Back to the web app

At this point, you have configured everything you need within the context of the JumpCloud Portal. Return to the Bitwarden web vault 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 JumpCloud Portal during app creation:

Field	Description
Name ID Format	If you created a Custom SAML Application, set this to whatever the specified SAMLSubject NameID Format is. Otherwise, leave **Unspecified**.

Field	Description
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests.
Signing Behavior	Whether/when SAML requests will be signed. By default, JumpCloud will not require requests to be signed.
Minimum Incoming Signing Algorithm	If you created a Custom SAML Application, set this to whichever Signature Algorithm you selected. Otherwise, leave as `rsa-sha256`.
Want Assertions Signed	If you created a Custom SAML Application, check this box if you set the **Sign Assertion** option in JumpCloud. Otherwise, leave 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 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 JumpCloud Portal to retrieve application values:

Field	Description
Entity ID	Enter your JumpCloud **IdP Entity ID**, which can be retrieved from the JumpCloud Single Sign-On Configuration screen. This field is case sensitive.
Binding Type	Set to **Redirect**.
Single Sign On Service URL	Enter your JumpCloud **IdP URL**, which can be retrieved from the JumpCloud Single Sign-On Configuration screen.

Field	Description
Single Log Out Service URL	Login with SSO currently **does not** support SLO. This option is planned for future development.

X509 Public Certificate	Paste the retrieved 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	If you created a Custom SAML Application, set this to whichever Signature Algorithm you selected. Otherwise, leave as `rsa-sha256`.
Disable Outbound Logout Requests	Login with SSO currently **does not** support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether JumpCloud 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.

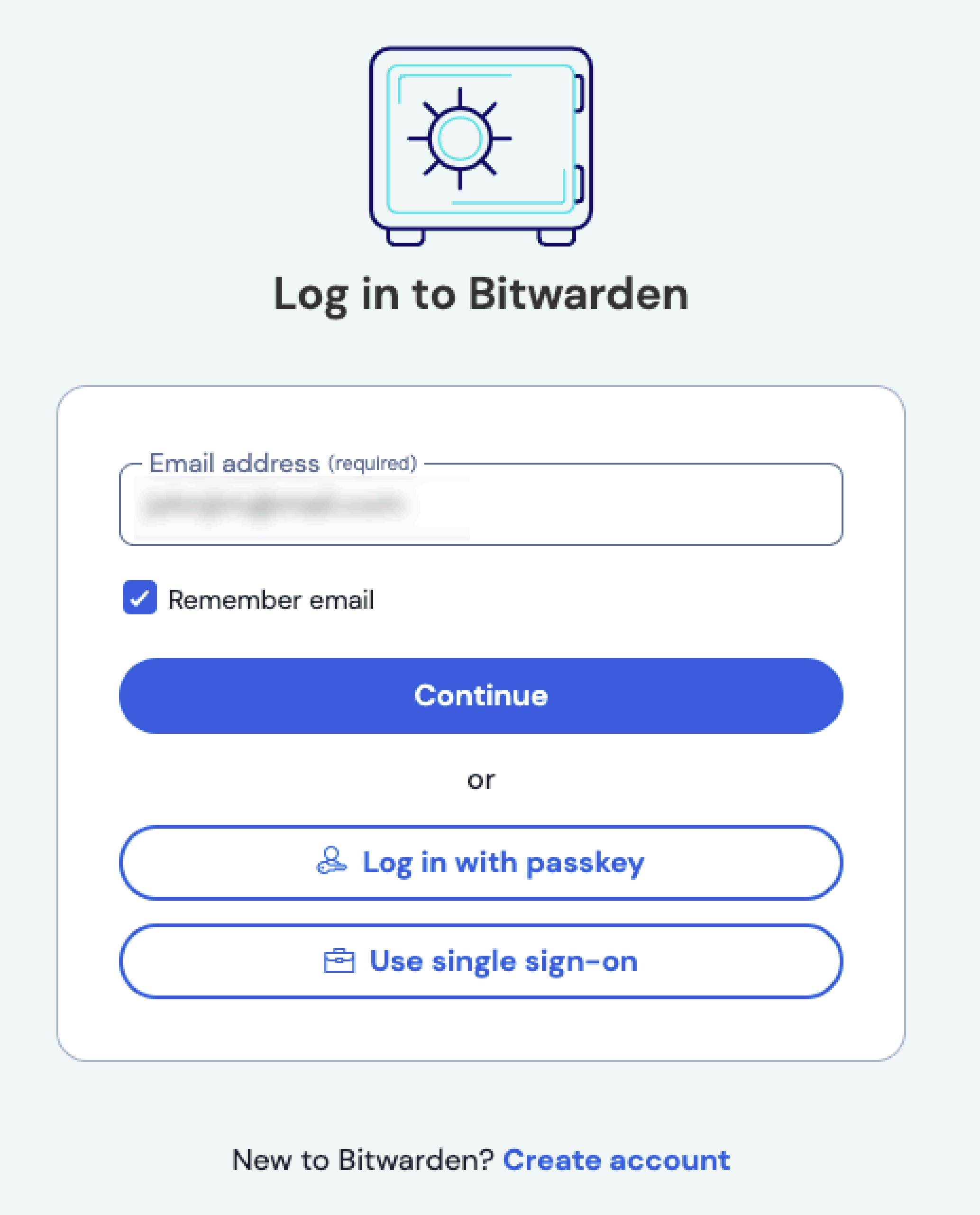
When you are done with the identity provider configuration, **Save** your work.

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:



Log in to Bitwarden

Email address (required)

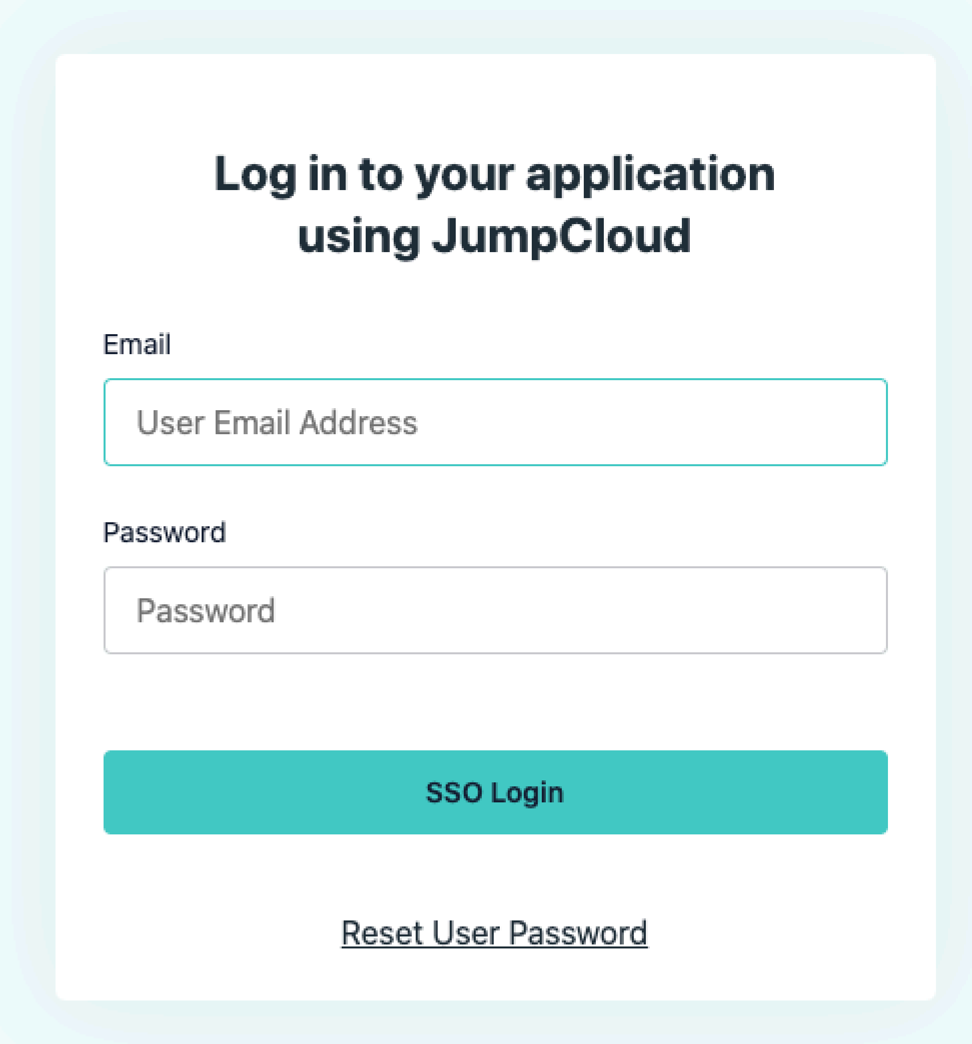
[redacted]

☑ Remember email

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 JumpCloud login screen:



Log in to your application using JumpCloud

Email

Password

JumpCloud Login

After you authenticate with your JumpCloud 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.