ADMIN CONSOLE  $\rightarrow$  LOGIN WITH SSO  $\rightarrow$ 

# 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:

D Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS ②		Name	Owner	
🖉 Send			Name	Owner	:
🖏 Tools 🛛 🗸 🗸	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
<b>፰</b> Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	A My vault B My Organiz	0 3	myusername	Me	:
	<ul> <li>Teams Org i</li> <li>+ New organization</li> </ul>		Secure Note	Me	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>③ Login</li> <li>□ Card</li> <li>Identity</li> <li>↓ Secure note</li> </ul>	0 0	Shared Login sharedusername	My Organiz	÷
🔒 Password Manager	<ul> <li>✓ Folders</li> <li>➡ No folder</li> <li>✓ Collections</li> </ul>				
🗔 Secrets Manager	-Defacit colle				
🗿 Admin Console	<ul> <li>□ Default colle</li> <li>□ Trash</li> </ul>				
🖞 Toggle Width					
		_ /			

Product switcher

Open your organization's Settings → Single sign-on screen:

<b>D bit</b> warden	Single sign-on III III III III III III III III III I
🕮 My Organization	✓ Use the <u>require single sign-on authentication policy</u> to require all members to log in with SSO.
	Allow SSO authentication
A Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.
뿅 Groups	SSO identifier (required)
➡ Reporting	<ul> <li>Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification</li> </ul>
St Billing	Member decryption options
Settings	Master password
Organization info	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.
Policies	account recovery auministration policy with acconacte enformment will turn on when this option is used.
Two-step login	SAML 2.0
Import data	SAIML 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	Generate an identifier that is unique to your organization
SCIM provisioning	
	SAML 2.0 metadata URL
	I have not a first that the first of the fir

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:

#### Secure and trusted open source password manager for business

of jumpcloud	SSO ©	ê Product Tour	r Pricing 🎝	Alerts P What's New	© Support i≣ Checklist MM
C Discover Cerstantion Home USER MANAGEMENT  Q Users USER AUTHENTICATION  C RADIUS  D Password Manager  C RADIUS  D Password Manager  C Device Groups  Device Groups  Device Groups  Device Groups  D Policy Management Corp		jumpcloud.	G i i i i i i i i i i i i i i i i i i i		
Commands		Add your first application			
Software Management	Single	Sign-On and Identity Management Application Integrat	tions		
INTEGRATIONS  Applications  Active Directory  Cloud Directories  Directories  Directories	Set up ar	f manage single sign-on or create an identity management integr import, update, and export users on a regular basis. Get Started	ration to		
HR Directories     HR Directories     Live Chat     Settings     Account     Collapse Menu		Pro Tip: You can connect nearly any HR Directory or Identity Provider to easily import new users into JumpCloud!			
	Create B	twarden app Jumpcloud			

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

🔾 bitwarden 🛛 🙁		
1 item		
Name 🔺	Supported Fun	ctionality
<b>D bit</b> warden	Bitwarden	configure

#### **∂** Tip

If you are more comfortable with SAML, or want more control over things like NamelD 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	
	-	r this application after activation. Click here to see the Knowledge Base article with details for configuring this appli
Service Provider Me		
Upload Metadata	adata: 0	
IdP Entity ID: 0	•	
JumpCloud		
SP Entity ID:		
https://sso.bitwarde	1.com/sami2/	
ACS URL: 0		
https://sso.bitwarde	n.com/sami2/YOUR_ORG_ID/Acs/	1
SP Certificate:		
Upload SP Certifie	ate	
IDP URL:		
https://sso.jumpo	loud.com/saml2/ bitwarden	
Attributes		
Attributes		intication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary

Jumpcloud SSO configuration

Field	Description
ldP Entity ID	Set this field to a unique, Bitwarden-specific value, for example, <a href="https://www.bitwardensso_yourcompany">bitwardensso_yourcompany</a> .
SP Entity ID	Set this field to the pre-generated <b>SP Entity ID</b> . 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.
ACS URL	Set this field to the pre-generated <b>Assertion Consumer Service (ACS) URL</b> . 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.

#### 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 NamelD	Specify the JumpCloud attribute that will be sent in SAML responses as the NameID.
SAMLSubject NamelD 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.

Field	Description
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.bitw arden.eu/#/sso. For self-hosted instances, this is determined by your configured server URL, for example https://your.domain.com/#/sso.

#### Attributes

In the **Single Sign-On Configuration**  $\rightarrow$  **Attributes** section, construct the following SP  $\rightarrow$  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: 0

Service Provider Attribute Name	JumpCloud Attribute Name	
email	email	T
uid		_
ula	username	v
firstname	firstname	T
lastname	lastname	~
add attribute		
	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**:

n jumpcloud	SSO		🗘 Alerts 🖽 Resources 💿	Support	_
A Home NEW ✓ USER MANAGEMENT Q Users	Featured Applic	<b>D bit</b> warden	Details User Groups		×
A     User Groups       USER AUTHENTICATION       B     LDAP       C     RADIUS	SI Supported functionality SSO JIT Identity Man	Bitwarden  IDP Certificate Valid	<ul> <li>General Info</li> <li>*Display Label:</li> <li>Bitwarden Login with SSO</li> </ul>		
<ul> <li>BSO</li> <li>DEVICE MANAGEMENT</li> <li>Devices</li> <li>Device Groups</li> <li>Configurations (Policies)</li> </ul>	+ Q Search	Regenerate certificate Download certificate Upload new certificate	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). Display Option:	A	

#### Download Certificate

#### Bind user groups

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

•1	jumpcloud	Us	er Gro	oups 🛈			\$ Alerts	Resources	③ Supp	ort (	FS
G	Home NEW										
								ex	pand go	: it	
R	Users										
• #R	User Groups		Q	Search					2 groups	delete	}
			Туре	Group 🔺							
6	LDAP			All Users						>	
C	RADIUS		0	Group of Users							
8	SSO		•	Bitwarden SSO Group of Users						>	
Ÿ.	Devices										
֎	Device Groups										

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:

			Users Device Gro SO user group is bound	oups <u>Applications</u> to the following application	RADIUS Directories	×
	0	Search Status	Name	Display Label 🔺	Supported Functionali	ity
	•	0	<b>U bit</b> warden	Bitwarden Login with S	SSO	
Bitwarden SSO						

**Bind App Access** 

#### **⊘** Tip

Alternatively, you can bind access to user groups directly from the SSO  $\rightarrow$  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 <b>Unspecified</b> .
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests.

Field	Description
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 <b>Sign Assertion</b> 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 <b>IdP Entity ID</b> , which can be retrieved from the JumpCloud Single Sign-On Configuration screen. This field is case sensitive.
Binding Type	Set to <b>Redirect</b> .
Single Sign On Service URL	Enter your JumpCloud <b>IdP URL</b> , which can be retrieved from the JumpCloud Single Sign-On Configuration screen.
Single Log Out Service URL	Login with SSO currently <b>does not</b> support SLO. This option is planned for future development.
X509 Public Certificate	Paste the retrieved certificate, removing
	BEGIN CERTIFICATE

Field	Description
	and
	END CERTIFICATE
	The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters <b>will cause certification validation to fail</b> .
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 <b>does not</b> support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether JumpCloud expects SAML requests to be signed.
(i) 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
Maste	r password (required)
⊗ Input is	required. ster password hint
	Log in with master password
$\square$	🖶 Enterprise single sign-on
Logging i	n as myemailaddress@bitwarden.com

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

User Email Address

#### Password

Password

SSO Login

#### Reset User Password

JumpCloud Login

After you authenticate with your JumpCloud credentials, enter your Bitwarden master password to decrypt your vault!

#### (i) 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.