ADMIN CONSOLE \rightarrow LOGIN WITH SSO \rightarrow

Google SAML Implementation

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

Google SAML Implementation

This article contains **Google Workspace-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 Google Workspace Admin console. 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.

Jownload 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 🕜		Name	Owner	:
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	÷
≅ Reports	✓ All vaults		Personal Legin		
Settings	A My vault	0 9	Personal Login myusername	Me	:
	 Feams Org : + New organization 		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ⑦ Login □ Card Identity □ Secure note 		Shared Login sharedusername	My Organiz	:
🕆 Password Manager	 ✓ Folders ➡ No folder 				
Secrets Manager	Collections				
	Default colle				
🖉 Admin Console	🔟 Trash				
🍈 Toggle Width					
		Duralization	and the later of		

Product switcher

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

Secure and trusted open source password manager for business

D bit warden	Single sign-on 🖩 🗧
g My Organization $~~ \lor~~$	Use the require single sign-on authentication policy to require all members to log in with SSO.
Collections	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) unique-organization-identifier
$ agreen arrow = Reporting \qquad \lor$	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
😫 Billing 🗸 🗸	Member decryption options
\otimes Settings \land	Master password
Organization info Policies	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.
Two-step login	C Type
Import data	SAML 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 SP entity ID
SCIM provisioning	
	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.

∂ Tip

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

Create a SAML app

In the Google Workspace Admin console, select **Apps** → **Web and mobile apps** from the navigation. On the Web and mobile apps screen, select **Add App** → **Add custom SAML app**:

≡	Google Admin	Q Search for users, groups or settings
Ĺ) Home	Apps > Web and mobile apps
₽	Dashboard	
• 0	Directory	Apps (0) Add App 🔻 Settings 🔻
، ⊑	Devices	+ Add a filte Search for apps
• !!	Apps	□ Name ↑ Add private Android app Use
	Overview	
	 Google Workspace 	Add private Android web app
_	Additional Google services	Add custom SAML app
(Web and mobile apps	
	Marketplace apps	
	LDAP	
• 🕄	Security	
		Create a SAML App

App details

On the app details screen, give the application a unique Bitwarden-specific name and select the **Continue** button.

Google identity provider details

On the Google Identity Provider details screen, copy your SSO URL, Entity ID, and Certificate for use during a later step:

× Add custo	om SAML app		
🗸 App details —	2 Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping		
	To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn mor Option 1: Download IdP metadata	e	
	DOWNLOAD METADATA		
	OR		
	Option 2: Copy the SSO URL, entity ID, and certificate		
	SSO URL		
	https://accounts.google.com/	Ō	
	Entity ID		
	https://accounts.google.com/	ē	
	Certificate		
	Google_ Expires	Ē ±	
	BEGIN CERTIFICATE		
	SHA-256 fingerprint		
		Ō	
BA	ACK C	ANCEL	CONTINUE



Select **Continue** when you are finished.

Service provider details

On the Service provider details screen, configure the following fields:

Field	Description
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.
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.
Start URL	Optionally, 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://yo ur.domain.com/#/sso.
Signed response	Check this box if you want Workspace to sign SAML responses. If not checked, Workspace will sign only the SAML assertion.
Name ID format	Set this field to Persistent .
Name ID	Select the Workspace user attribute to populate NamelD.

Select **Continue** when you are finished.

Attribute mapping

On the Attribute mapping screen, select the **Add Mapping** button and construct the following mapping:

Google Directory attributes	App attributes
Primary email	email

Select Finish.

Turn on the app

By default, Workspace SAML apps will be **OFF for everyone**. Open the User access section for the SAML app and set to **ON for everyone** or for specific Groups, depending on your needs:

Bitwarden Login with SSO	User access To make the managed app available to selec View details OFF for everyone	t users, choose a group or organization	al unit. Learn more	Č
 TEST SAML LOGIN DOWNLOAD METADATA DELETE APP 	Service provider details Certificate Google_2026-5-9-112241_SAML2_0 (Expires May 9, 2026)	ACS URL	Entity ID https://sso.bitwarden.com/saml2	~

User Access

Save your changes. Please note that it can take up to 24 hours for a new Workspace app to propagate to users existing sessions.

Back to the web app

At this point, you have configured everything you need within the context of the Google Workspace Admin console. 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 Workspace Admin console during setup:

Field	Description
Name ID Format	Set this field to the Name ID format selected in Workspace.
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests.
Signing Behavior	Whether/when SAML requests will be signed.

Field	Description
Minimum Incoming Signing Algorithm	By default, Google Workspace 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 Workspace Admin console to retrieve application values:

Field	Description
Entity ID	Set this field to Workspace's Entity ID , retrieved from the Google Identity Provider details section or using the Download Metadata button. This field is case sensitive.
Binding Type	Set to HTTP POST or Redirect.
Single Sign On Service URL	Set this field to Workspace's SSO URL , retrieved from the Google Identity Provider details section or using the Download Metadata button.
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	Paste the retrieved certificate, removingBEGIN 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	By default, Google Workspace 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 Google Workspace 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.

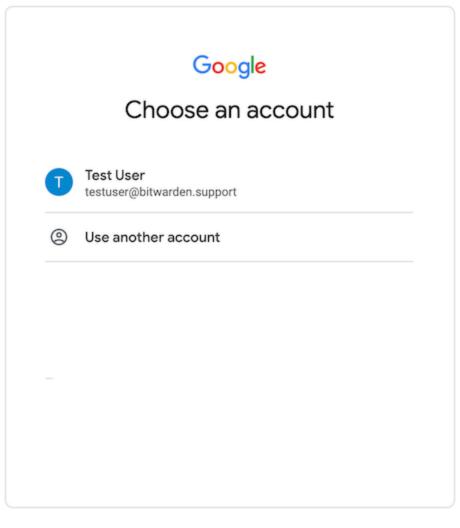
Test the configuration

Once your configuration is complete, test it by navigating to https://vault.bitwarden.com, entering your email address and selecting the **Enterprise Single-On** button:

	Log in to Bitwarden	
	Log III to bitwarden	
	address (required)	
	Continue	
	or	
\square	🐣 Log in with passkey	\supset
	🖻 Use single sign-on	5 J

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 Google Workspace login screen:



Login

After you authenticate with your Workspace 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.