

ADMIN CONSOLE > LOGIN WITH SSO >

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.

[Download Sample](#)

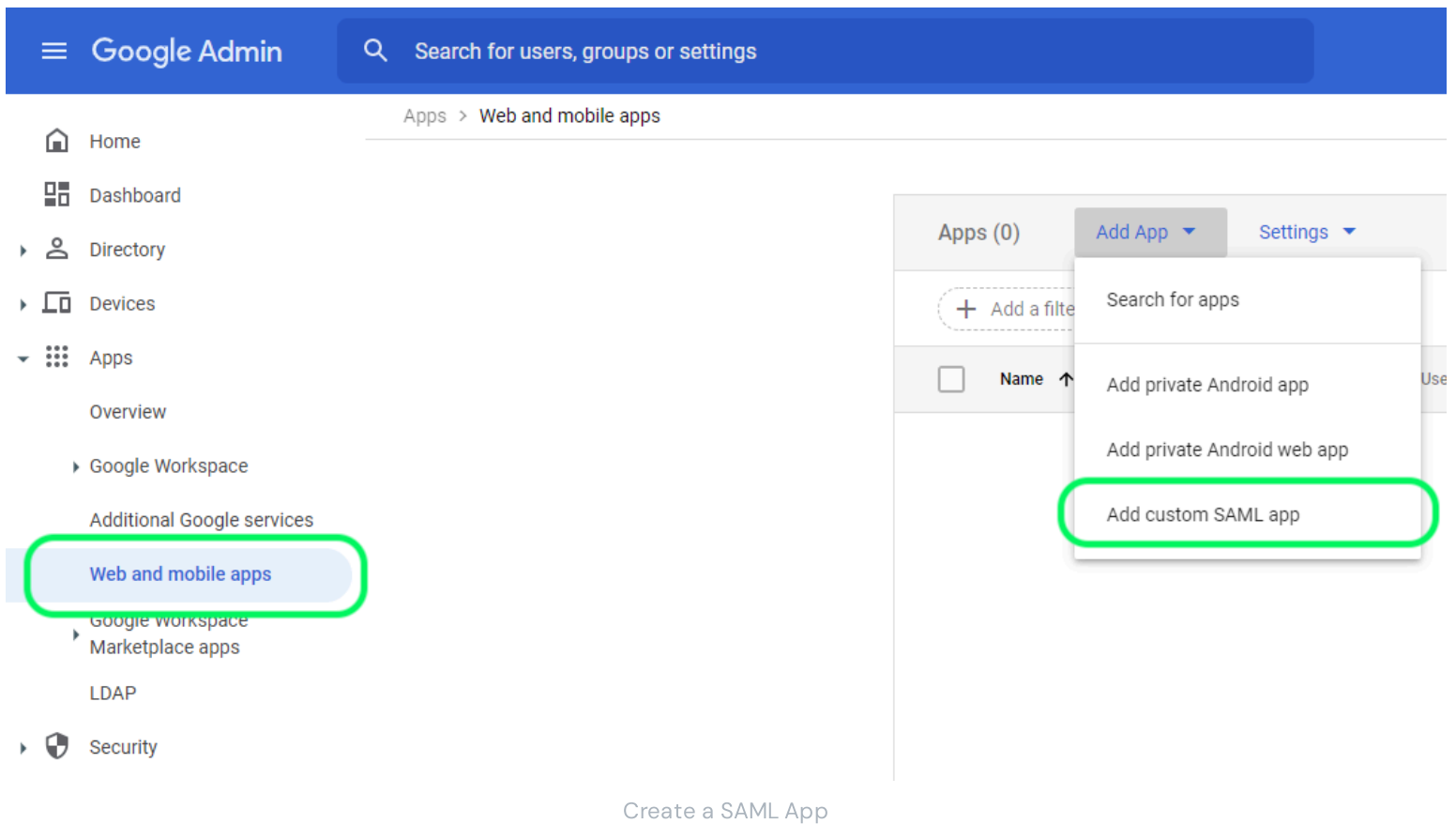
Open SSO in the web app

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

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Product switcher

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



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 custom SAML app

- 1 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 more](#)

Option 1: Download IdP metadata

DOWNLOAD METADATA

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

https://accounts.google.com/



Entity ID

https://accounts.google.com/



Certificate

Google_

Expires



-----BEGIN CERTIFICATE-----

SHA-256 fingerprint



BACK

CANCEL

CONTINUE

IdP Details

Select **Continue** when you are finished.

Service provider details

On the Service provider details 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>
Start URL	<p>Optionally, set this field to the login URL from which users will access Bitwarden.</p> <p>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://your.domain.com/#/sso.</p>
Signed response	<p>Check this box if you want Workspace to sign SAML responses. If not checked, Workspace will sign only the SAML assertion.</p>
Name ID format	<p>Set this field to Persistent.</p>
Name ID	<p>Select the Workspace user attribute to populate NameID.</p>

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:

The screenshot shows the configuration for a SAML app named 'Bitwarden Login with SSO'. In the 'User access' section, the status is 'OFF for everyone'. Below it, the 'Service provider details' section is visible, showing the Certificate as 'Google_2026-5-9-112241_SAML2_0 (Expires May 9, 2026)', the ACS URL, and the Entity ID as '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 , removing -----BEGIN CERTIFICATE----- and

Field	Description
	<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, 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.

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

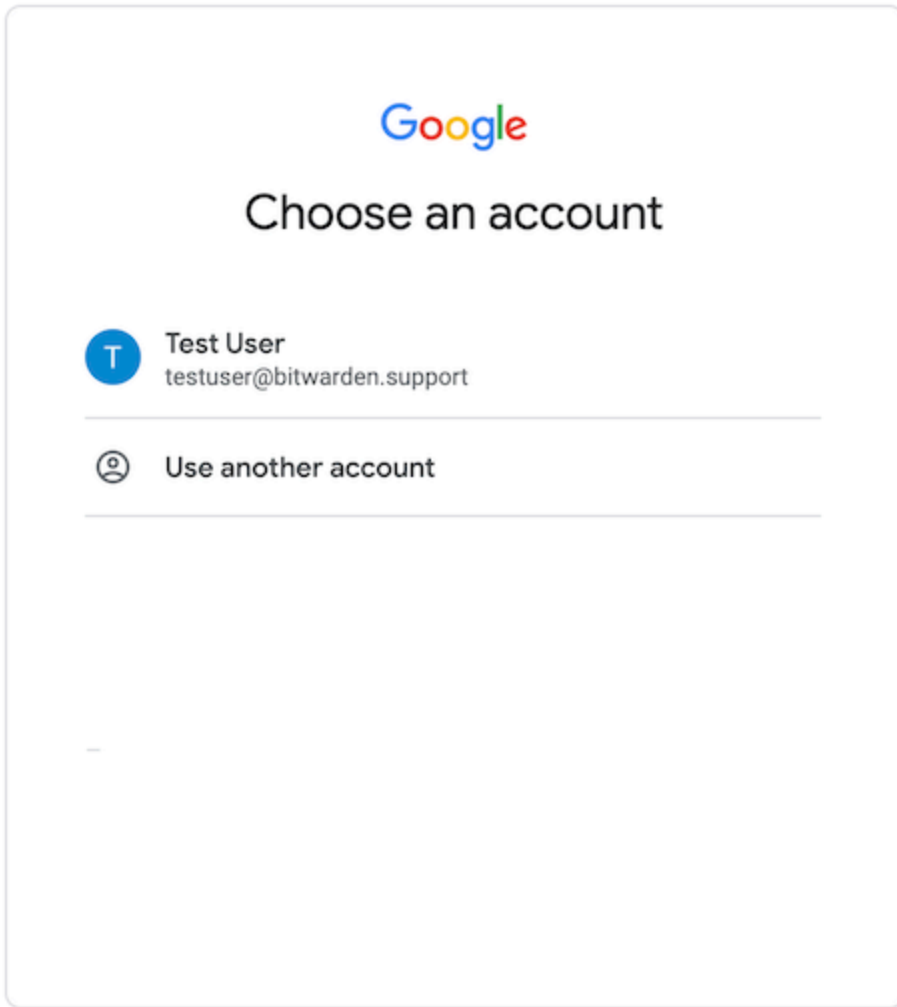
 Log in with passkey

 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 Google Workspace login screen:



Login

After you authenticate with your Workspace 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.