

ADMIN CONSOLE > LOGGA IN MED 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.

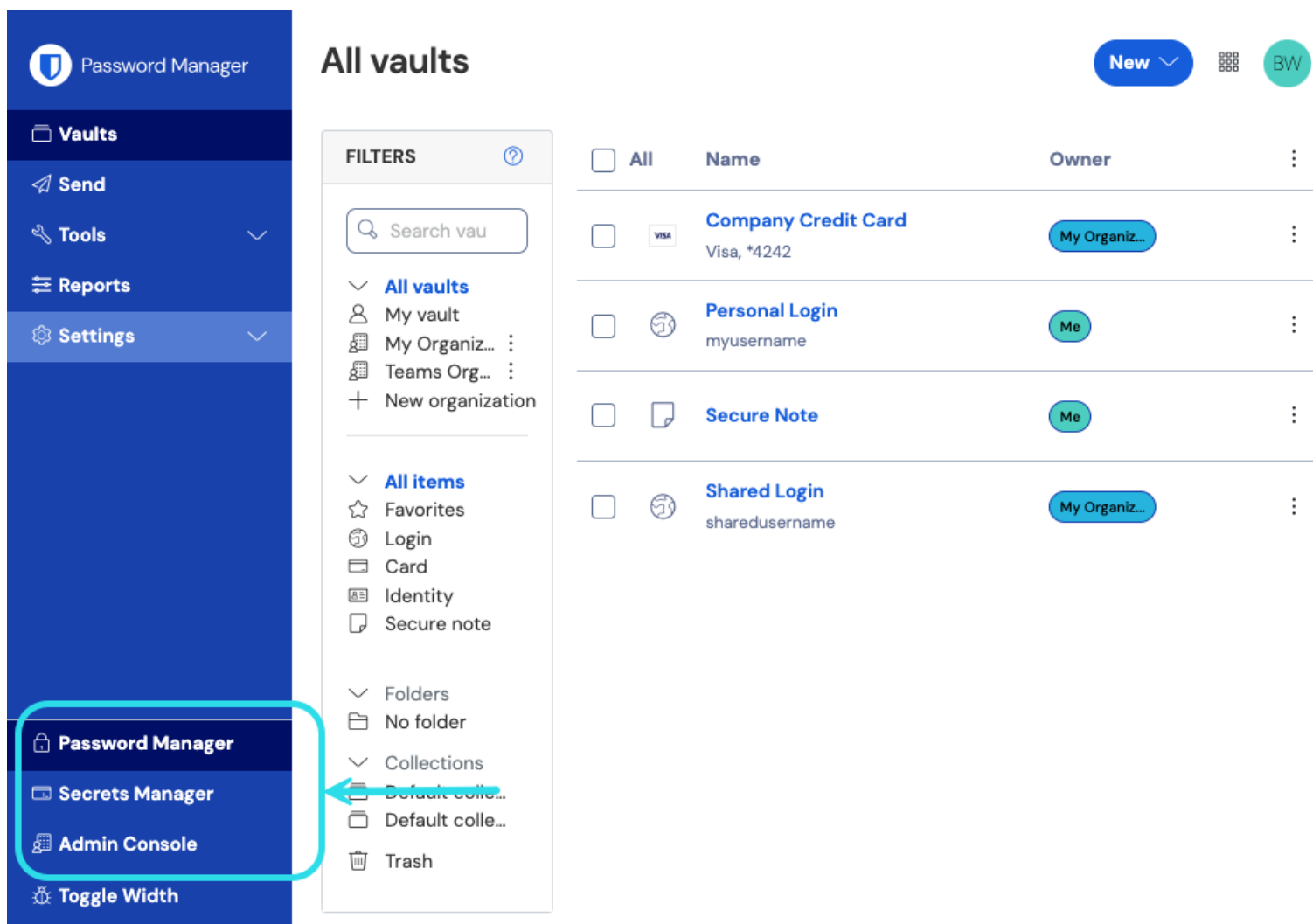


**Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

[Download Sample](#)

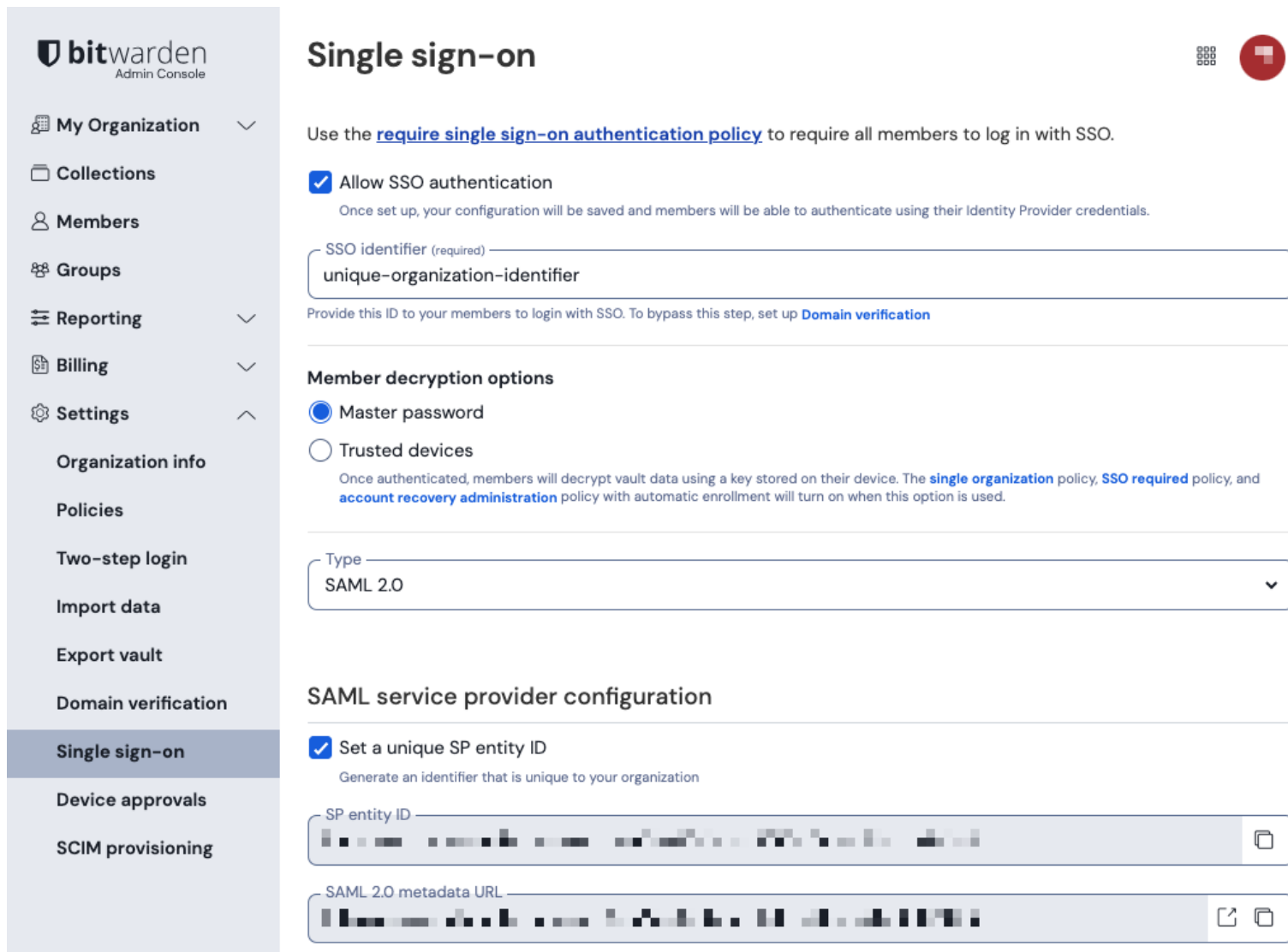
## Open SSO in the web app

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



Product switcher

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



The screenshot shows the Bitwarden Admin Console interface. On the left is a sidebar with navigation links: My Organization, Collections, Members, Groups, Reporting, Billing, Settings (expanded), Organization info, Policies, Two-step login, Import data, Export vault, Domain verification, Single sign-on (selected), Device approvals, and SCIM provisioning. The main content area is titled 'Single sign-on'. It includes a header with a QR code icon and a red arrow icon. The main text says: 'Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.' Below this is a checkbox 'Allow SSO authentication' which is checked. A note states: 'Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.' There is a text input field for 'SSO identifier (required)' with the value 'unique-organization-identifier'. A note below the field says: 'Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)'.

Below the SSO identifier field is a section titled 'Member decryption options'. It has two radio buttons: 'Master password' (selected) and 'Trusted devices'. A note below the radio buttons says: '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.'

Below the decryption options is a dropdown menu for 'Type' with the value 'SAML 2.0'.

Below the dropdown is a section titled 'SAML service provider configuration'. It has a checkbox 'Set a unique SP entity ID' which is checked. A note below the checkbox says: 'Generate an identifier that is unique to your organization'. There is a text input field for 'SP entity ID' with a generated value. There is a text input field for 'SAML 2.0 metadata URL' with a generated value.

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.

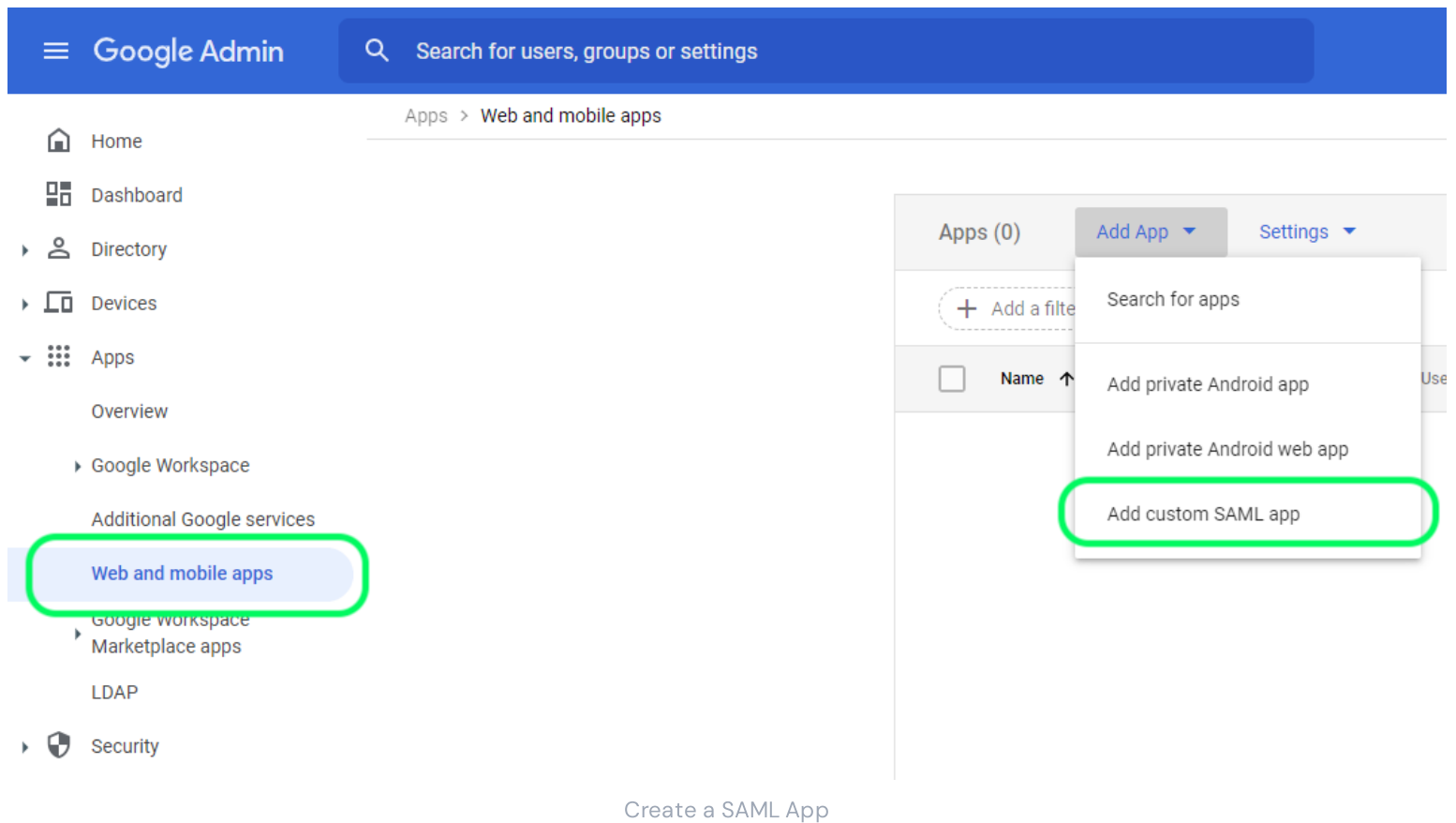
You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.



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**:



The screenshot shows the Google Admin console interface. On the left, the navigation menu includes 'Home', 'Dashboard', 'Directory', 'Devices', 'Apps', 'Overview', 'Google Workspace', 'Additional Google services', 'Web and mobile apps' (highlighted with a green circle), 'Google workspace', 'Marketplace apps', 'LDAP', and 'Security'. The main content area shows the breadcrumb 'Apps > Web and mobile apps'. On the right, the 'Apps (0)' section is visible, with an 'Add App' dropdown menu open. The dropdown menu options are 'Search for apps', 'Add private Android app', 'Add private Android web app', and 'Add custom SAML app' (highlighted with a green circle). Below the dropdown, a link 'Create a SAML App' is visible.

## 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

✓ 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 <b>Assertion Consumer Service (ACS) URL</b>.</p> <p>This automatically-generated value can be copied from the organization's <b>Settings → 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 → Single sign-on</b> 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 <a href="https://vault.bitwarden.com/#/sso">https://vault.bitwarden.com/#/sso</a> or <a href="https://vault.bitwarden.eu/#/sso">https://vault.bitwarden.eu/#/sso</a>. For self-hosted instances, this is determined by your <a href="#">configured server URL</a>, for example <a href="https://your.domain.com/#/sso">https://your.domain.com/#/sso</a>.</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 <b>Persistent</b>.</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:

SAML

 Bitwarden Login with SSO

TEST SAML LOGIN

DOWNLOAD METADATA

DELETE APP

User access

To make the managed app available to select users, choose a group or organizational unit. [Learn more](#)

[View details](#)

OFF for everyone

Service provider details

|                                                         |         |                                 |
|---------------------------------------------------------|---------|---------------------------------|
| Certificate                                             | ACS URL | Entity ID                       |
| Google_2026-5-9-112241_SAML2_0<br>(Expires May 9, 2026) |         | 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 <a href="#">selected in Workspace</a> . |
| Outbound Signing Algorithm | The algorithm Bitwarden will use to sign SAML requests.                      |

| Field                              | Description                                                                                                                                                                                                              |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Signing Behavior                   | Whether/when SAML requests will be signed.                                                                                                                                                                               |
| Minimum Incoming Signing Algorithm | By default, Google Workspace 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 Workspace Admin console to retrieve application values:

| Field                      | Description                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Entity ID                  | Set this field to Workspace's <b>Entity ID</b> , retrieved from the <a href="#">Google Identity Provider details section</a> or using the <b>Download Metadata</b> button. This field is case sensitive. |
| Binding Type               | Set to <b>HTTP POST</b> or <b>Redirect</b> .                                                                                                                                                             |
| Single Sign On Service URL | Set this field to Workspace's <b>SSO URL</b> , retrieved from the <a href="#">Google Identity Provider details section</a> or using the <b>Download Metadata</b> button.                                 |
| 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.                                                       |

| Field                               | Description                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X509 Public Certificate             | <p>Paste the <a href="#">retrieved certificate</a>, removing</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, Google Workspace 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 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

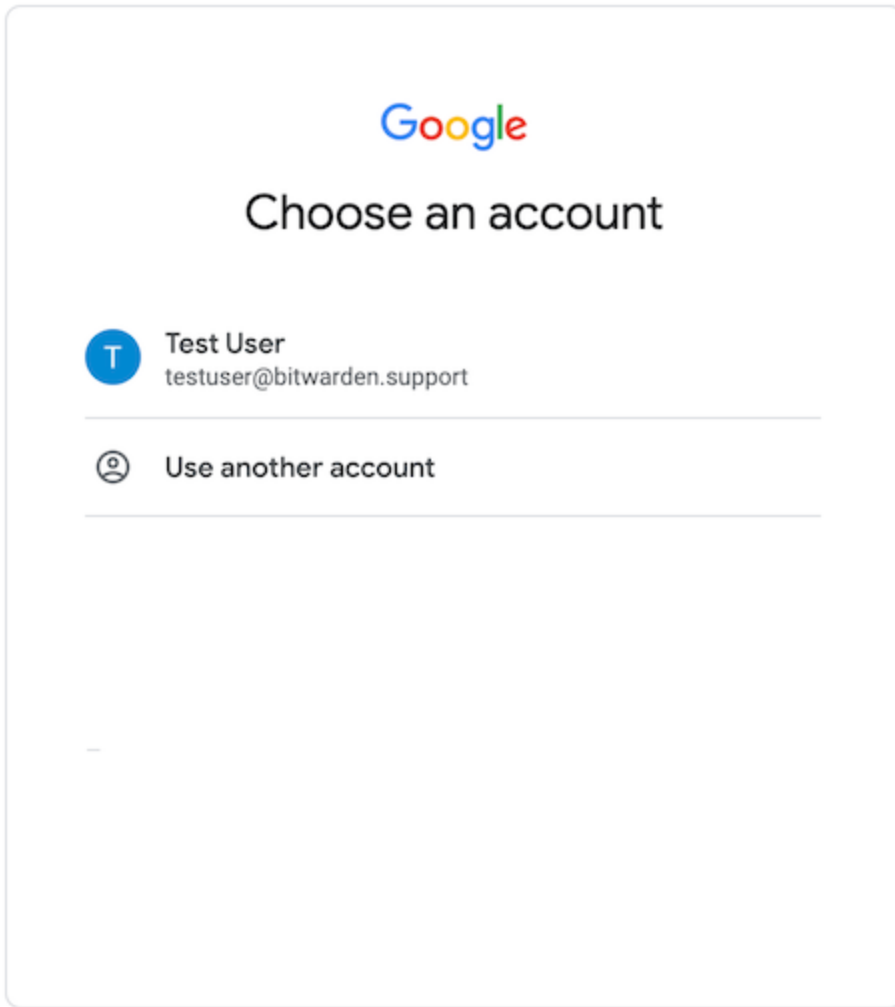
 Log in with passkey

 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.