Using Login with SSO

Using Login with SSO

As an end-user of Bitwarden, you may need to have an organization SSO identifier before you can login using SSO.

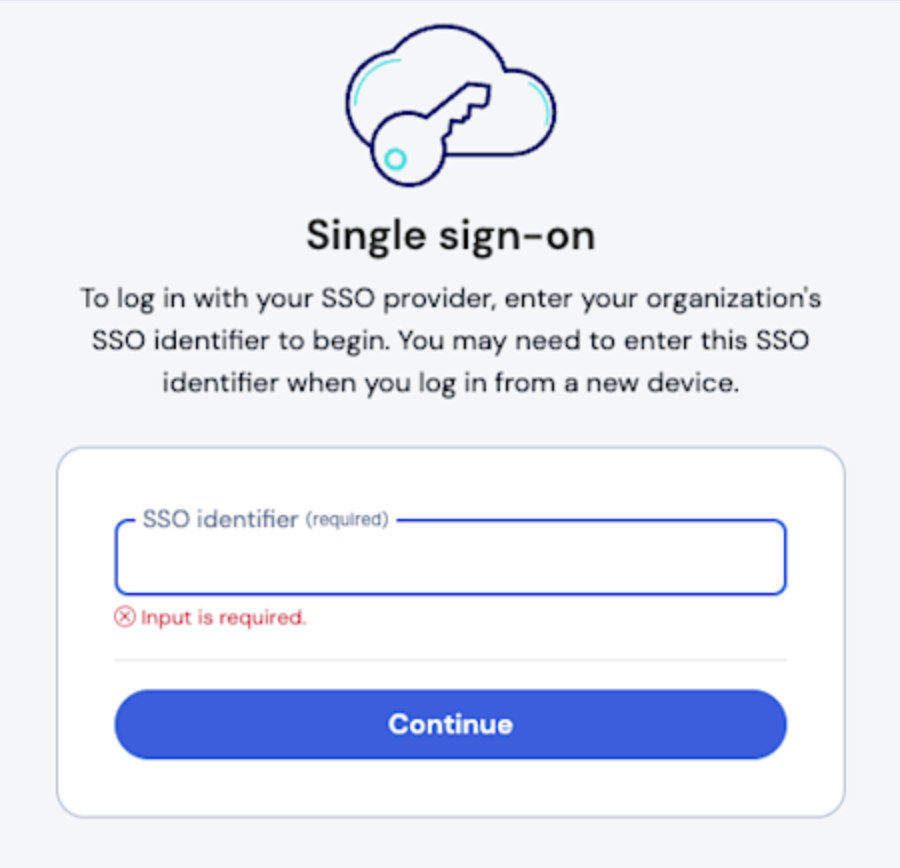
> **Tip**
>
> Depending on how your organization is set up, you may also need to link your account to SSO. This is typically required if you **already have a Bitwarden account that's a member of an organization** or if **your organization does not require you to use SSO**.

Get your organization identifier

Every Bitwarden organization has a unique identifier specifically for login with SSO. You will need this value to login, so ask your manager or Bitwarden administrator to retrieve it for you.

ⓘ Note

Enterprise customers can verify domain ownership (e.g., `mycompany.com`) for their organization. If your login email matches your organization's verified domain (e.g., `mycompany.com`), you won't need to enter in the SSO identifier when using login in with SSO.



Bypass SSO identifier

To learn more about domain verification, see here.

Join an organization using SSO

The steps required to join an organization using SSO will be slightly different depending on whether you have received an email invitation and whether you already have a Bitwarden account associated with the email address you want to join Bitwarden with:

⇒I have been invited

If you have an email invitation to join the organization in your inbox, follow one of these procedures depending on whether you already have a Bitwarden account with that email address:

I already have a Bitwarden account

If the invitation is sent to an email that is already linked to a Bitwarden account and matches the email address supplied by the IdP, follow these steps to join the organization:

1. Click the **Join Organization** button in the email invitation.
2. On the Bitwarden invitation page, select **Log in.** Enter your email address, then master password, and select **Log in** once more.
3. Once you have successfully logged in, a green banner will appear at the top of the page, indicating that your organization invitation has been accepted. An organization admin will need to confirm you to the organization before you can proceed.
4. Once you're confirmed, you'll be able to access the organization by logging in to Bitwarden again, this time using the **Enterprise single sign-on** option.

I don't have a Bitwarden account

If the invitation is sent to an email that isn't already linked to a Bitwarden account, follow these steps:

1. Click the **Join Organization Now** button in the email invitation.
    1. If your organization **does not** have the **Require SSO Authentication** policy enabled, you will be prompted to create a new Bitwarden account prior to logging in with your IdP.
    2. If **Require SSO Authentication** is **enabled**, proceed to step 2.
2. On the screen that opens following the link, select **Log in**. Your organization's **SSO identifier** will be pre-filled on this screen (if your email matches an organization's verified domain, you will bypass this step)**.**
3. Log in to your IdP. Once you do, you'll be redirected to a page where you can create a master password for your new account.
4. Create a master password for the account. An organization admin will need to confirm you to the organization before you can proceed. You may be required to log in using your master password before an admin can confirm you.
5. Once you're confirmed, you'll be able to access the organization by logging in to Bitwarden using the **Enterprise single sign-on** option, or with your master password.

If you receive the error message `<email> has been invited to the organization, please accept invitation.` while attempting to log in, there's already a Bitwarden account associated with this email. Please follow the **I already have a Bitwarden account** instructions above.

⇒I haven't been invited

If you don't have an email invitation to join the organization in your inbox, follow one of these procedures depending on whether you already have a Bitwarden account with that email address:

I already have a Bitwarden account

You won't be able to join an organization using SSO with this account. Contact your organization admin to request an invitation.

I don't have a Bitwarden account

If you are joining an organization without an invite and no pre-existing Bitwarden account, follow these instructions:

1. Enter your email on the Bitwarden login page. On the following page, select the **Enterprise single sign-on** button.
2. Enter your **SSO Identifier** and select **Log in** (if your email matches an organization's verified domain, you will bypass this step).
3. Log in to your IdP. Once you do, you'll be redirected to a page where you can create a master password for your new account.
4. Create a master password for the account. An organization admin will need to confirm you to the organization before you can proceed.
5. Once you're confirmed, you'll be able to access the organization by logging in to Bitwarden using the **Enterprise single sign-on** option.

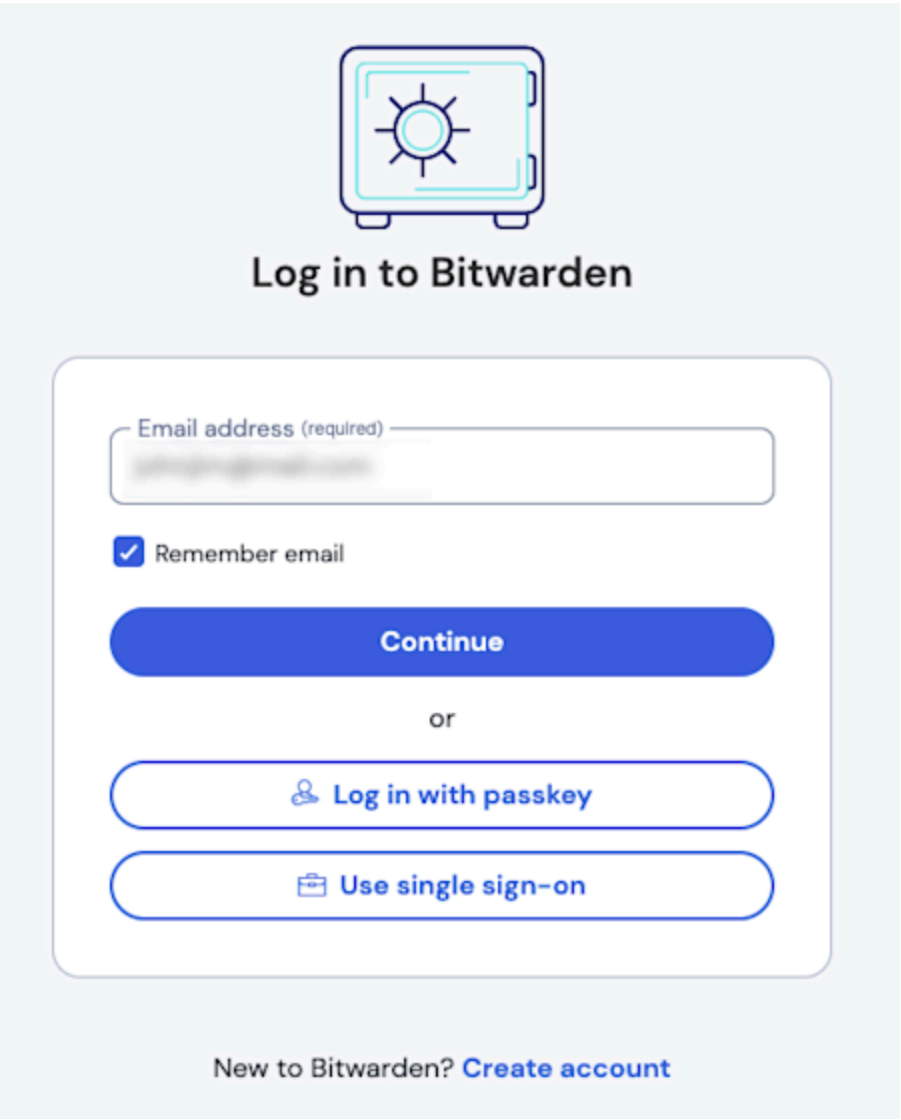
Login using SSO

The steps required to login using SSO will be slightly different depending on whether your organization is using master passwords for decryption or another supported member decryption option. These instructions are written for the web app (vault.bitwarden.com, vault.bitwarden.eu, or a self-hosted web app), however the steps are viable for most Bitwarden clients:

⇒Login with SSO & master password

To login using SSO and your master password:

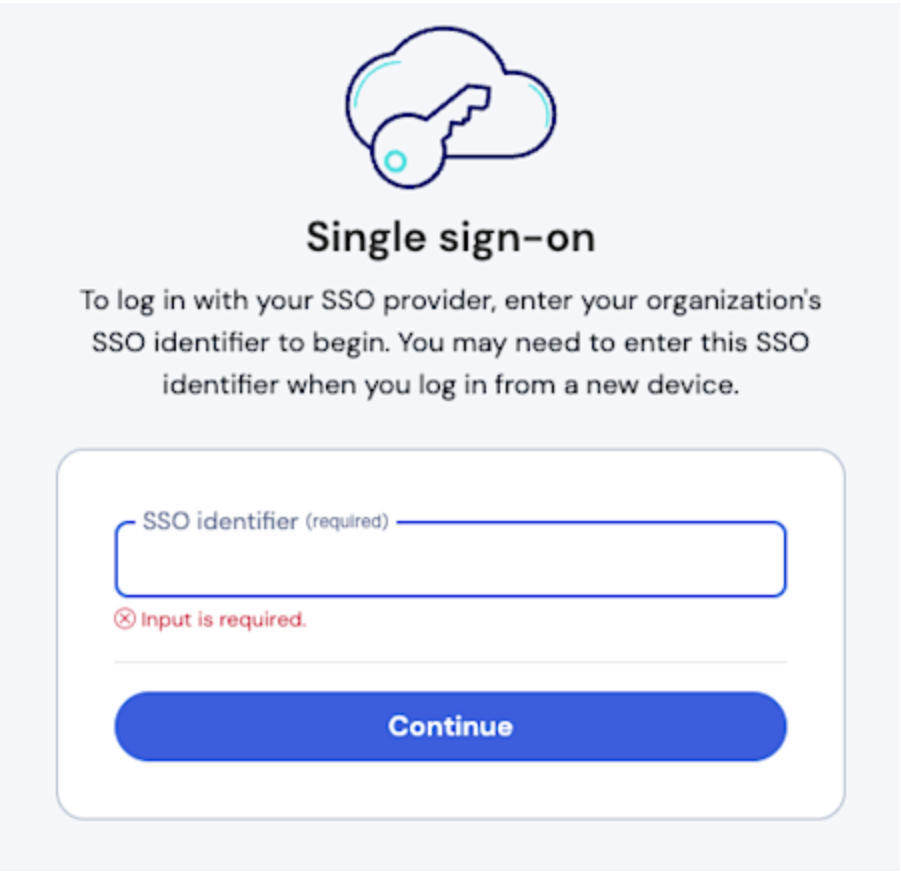
1. Open the Bitwarden app, enter your email address, and select the **Use single sign-on** button. If you don't have a Bitwarden account email yet, you may enter your company email.



Enter your email address

2. Enter your **SSO identifier** and select **Log in**:

> **Tip**
> Not everyone will need to complete this step, your organization may have configured set your log in procedure to not require it! If you don't see this screen, proceed to the next step in these instructions.



SSO identifier screen

> **Tip**
>
> If you did have to complete this SSO identifier step, we recommend bookmarking this page with your organization identifier included as a query string so that you don't have to enter it each time, for example `https://vault.bitwarden.com/#/sso?identifier=my-organization's-identifier` or `https://your.domain.com/#/sso?identifier=my-organization's-identifier`.

3. Now you'll be redirected to your IdP (for example, Microsoft Azure, Duo, OneLogin, and so on). Enter your SSO credentials to log in as usual.

4. Once you've authenticated using SSO, you will be prompted to either **enter your master password** to decrypt your vault **create a master password** if your account is new.

> **Note**
>
> **Why is my master password still required?**
>
> All vault data, including credentials shared by your organization, is kept by Bitwarden **only** in its encrypted form. This means that in order to use any of those credentials, **you** need a way to decrypt that data. We can't.
>
> Your master password is the source of that decryption key. Even though you are authenticating (proving your identity) to Bitwarden using SSO, you still need to use a decryption key (your master password) to unscramble vault data.

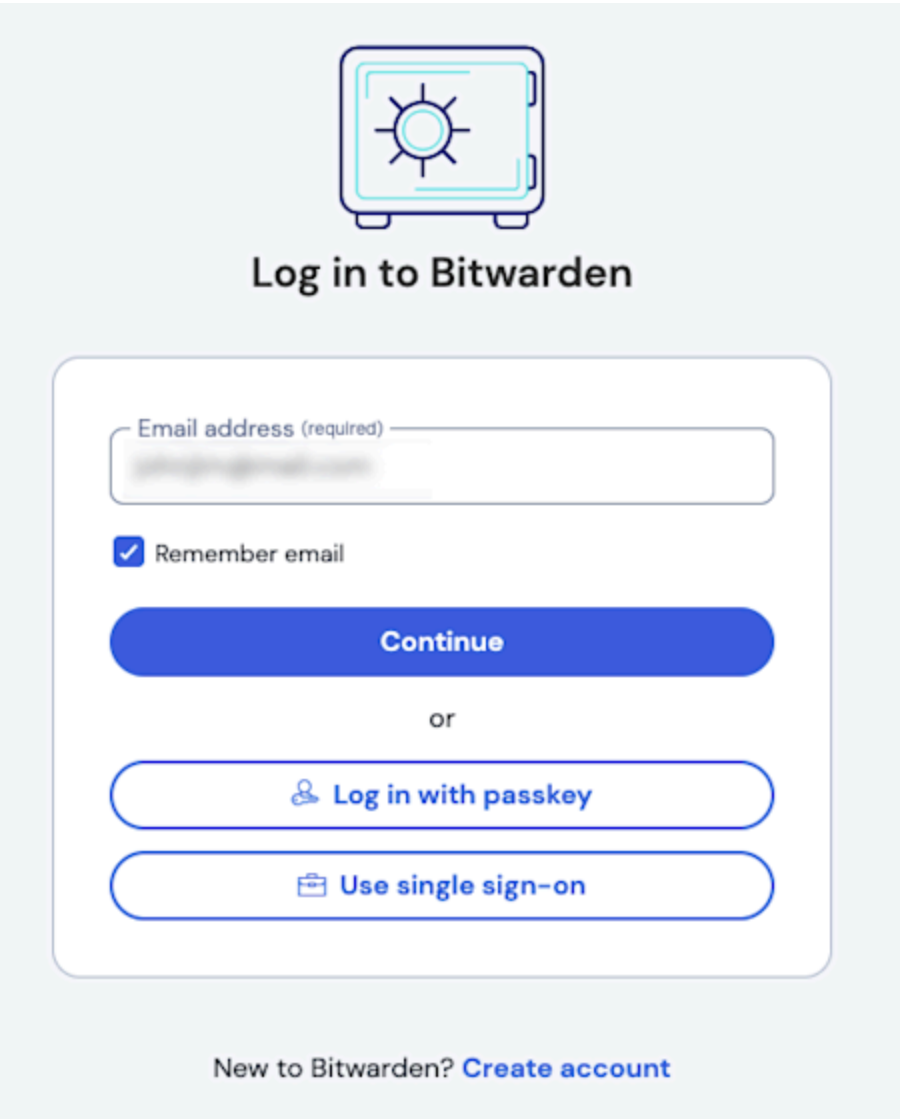
5. If you are using two-step login, authenticate using your secondary device.

> **Warning**
>
> Two-step login via email is not recommended if you are using **login with SSO**, as using multiple methods will cause errors. Consider setting up two-step login via a free authenticator instead.

⇒Login with SSO & trusted devices

To login using SSO and your master password:

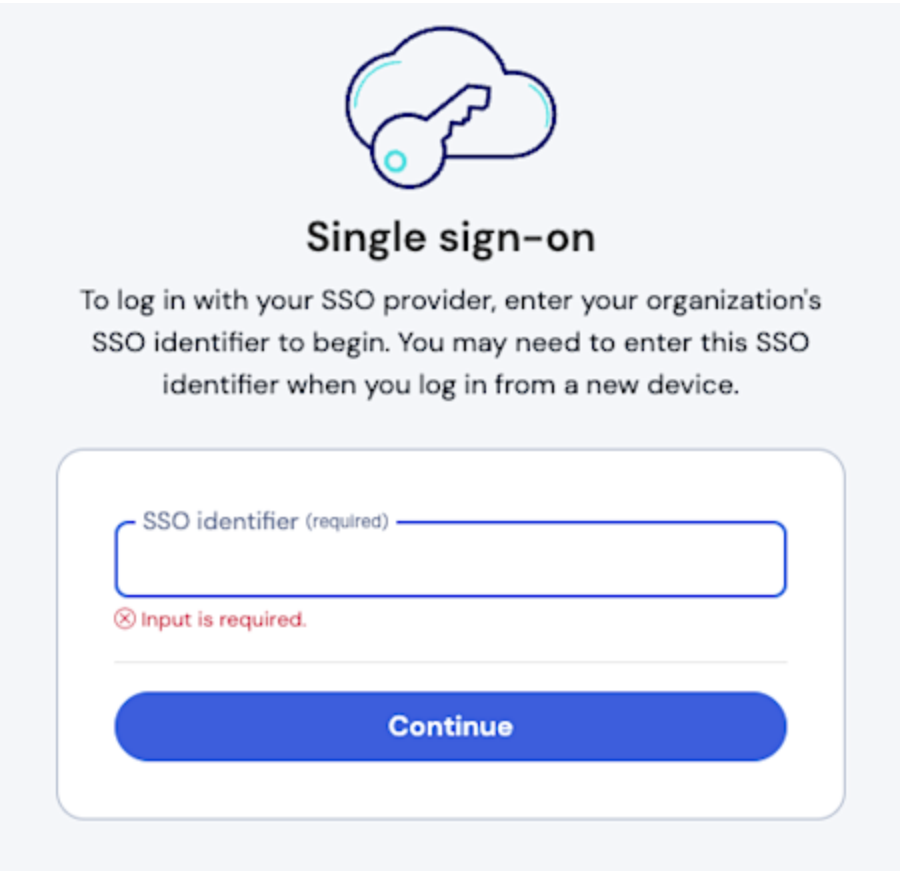
1. Open the Bitwarden app, enter your email address, and select the **Use single sign-on** button. If you don't have a Bitwarden account email yet, you may enter your company email.



Enter your email address

2. Enter your **SSO identifier** and select **Log in**:

> **Tip**
> Not everyone will need to complete this step, your organization may have configured set your log in procedure to not require it! If you don't see this screen, proceed to the next step in these instructions.

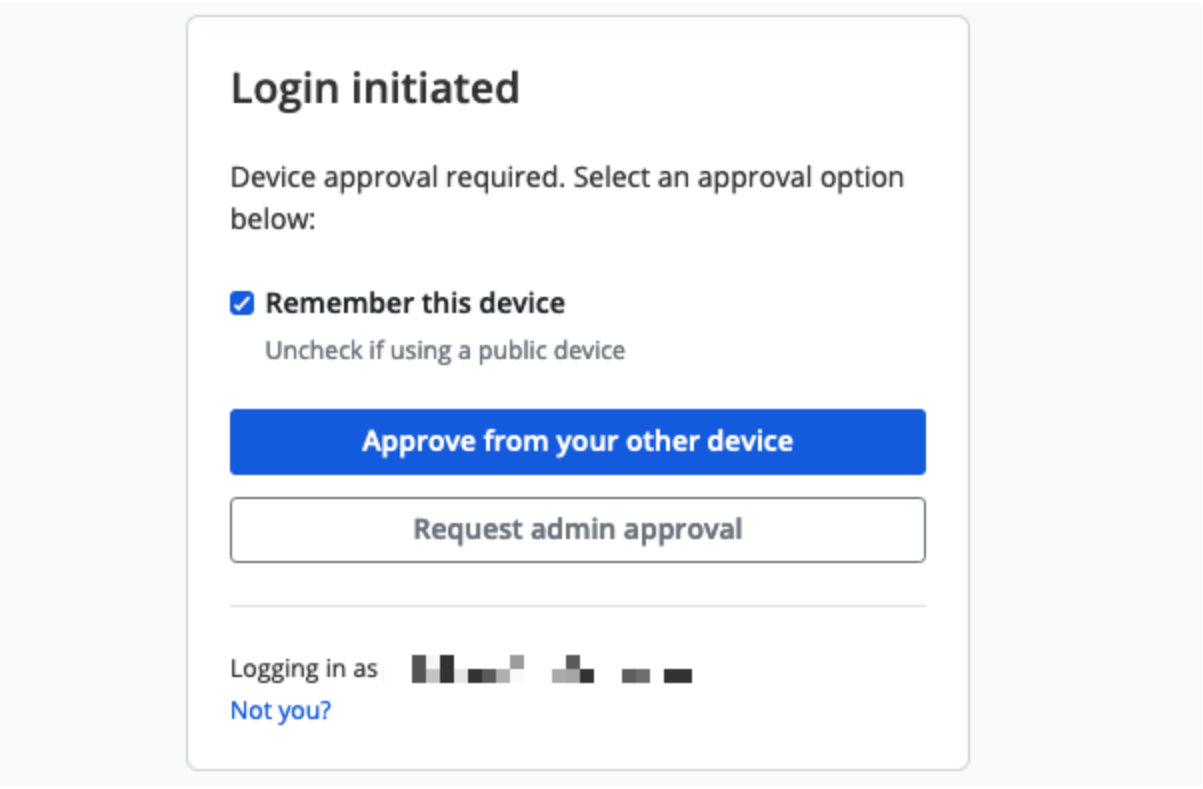


SSO identifier screen

> **Tip**
>
> If you did have to complete this SSO identifier step, we recommend bookmarking this page with your organization identifier included as a query string so that you don't have to enter it each time, for example `https://vault.bitwarden.com/#/sso?identifier=my-organization's-identifier` or `https://your.domain.com/#/sso?identifier=my-organization's-identifier`.

3. Now you'll be redirected to your IdP (for example, Microsoft Azure, Duo, OneLogin, and so on). Enter your SSO credentials to log in as usual.

4. Once you've authenticated using SSO, you'll be prompted to choose an option for establishing trust with the device you're logging in on (learn more about your options):



Options for establishing trust

> **Tip**
> If it's your first time logging in, you'll instead be allowed to designate this app as a trusted device instead of being required to use one of the above methods.

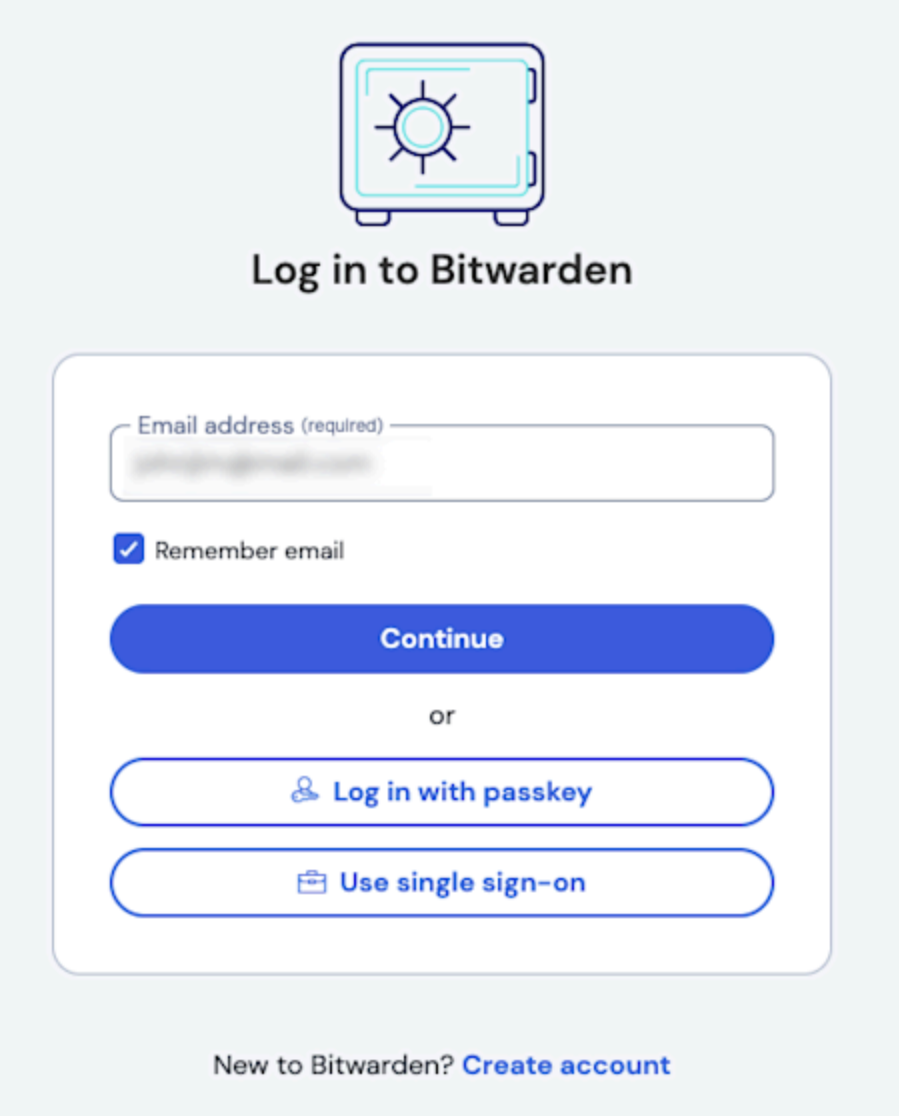
5. If you are using two-step login, authenticate using your secondary device.

> **⚠ Warning**
> Two-step login via email is not recommended if you are using **login with SSO**, as using multiple methods will cause errors. Consider setting up two-step login via a free authenticator instead.

⇒Login with SSO & Key Connector

To login using SSO and Key Connector:

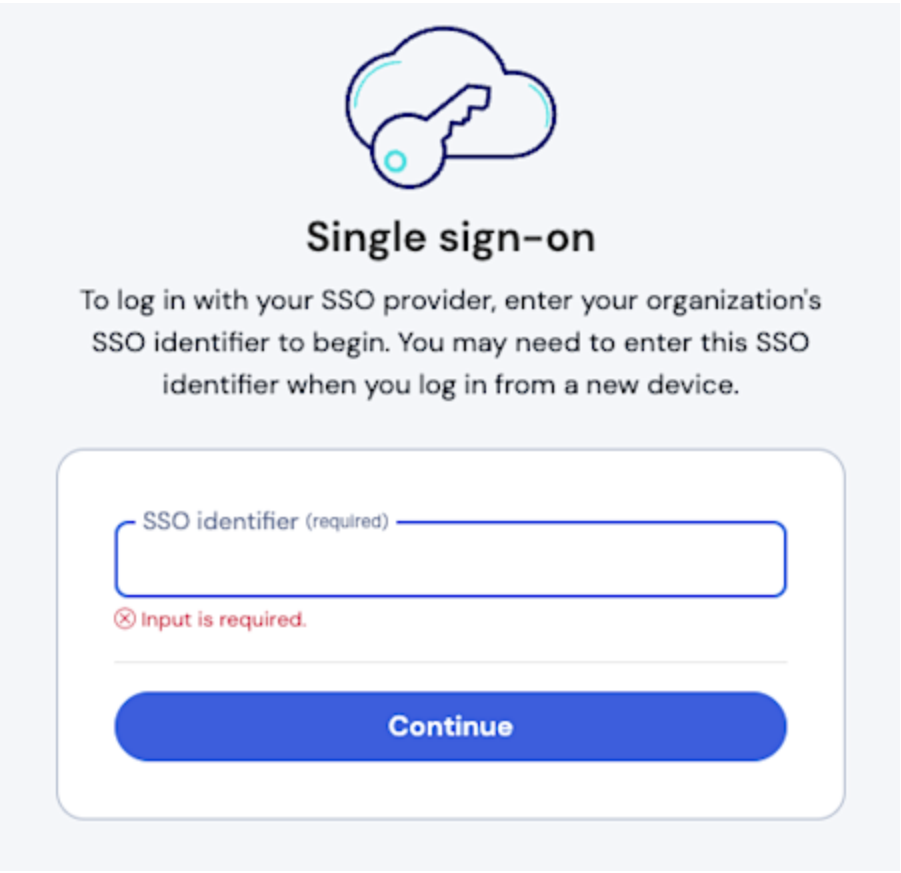
1. Open the Bitwarden app, enter your email address, and select the **Use single sign-on** button. If you don't have a Bitwarden account email yet, you may enter your company email.



Enter your email address

2. Enter your **SSO identifier** and select **Log in**:

> **Tip**
> Not everyone will need to complete this step, your organization may have configured set your log in procedure to not require it! If you don't see this screen, proceed to the next step in these instructions.



SSO identifier screen

> **Tip**
>
> We recommend bookmarking this page with your organization identifier includes as a query string so that you don't have to enter it each time, for example `https://vault.bitwarden.com/#/sso?identifier=YOUR-ORG-ID` or `https://your.domain.com/#/sso?identifier=YOUR-ORG-ID`.

3. Now you'll be redirected to your IdP (for example, Microsoft Azure, Duo, OneLogin, and so on). Enter your SSO credentials to log in as usual.

4. Depending on your account status, you might be required to enter or create a master password the first time you login with SSO and Key Connector. Doing so will remove the master password from your account.

> **Tip**
>
> We encourage you to read this and this to fully understand what it means to remove a master password from your account. You can instead elect to **leave the organization** instead, however this will remove access to both organization-owned vault items and collections and to single sign-on.

5. If you are using two-step login, authenticate using your secondary device.

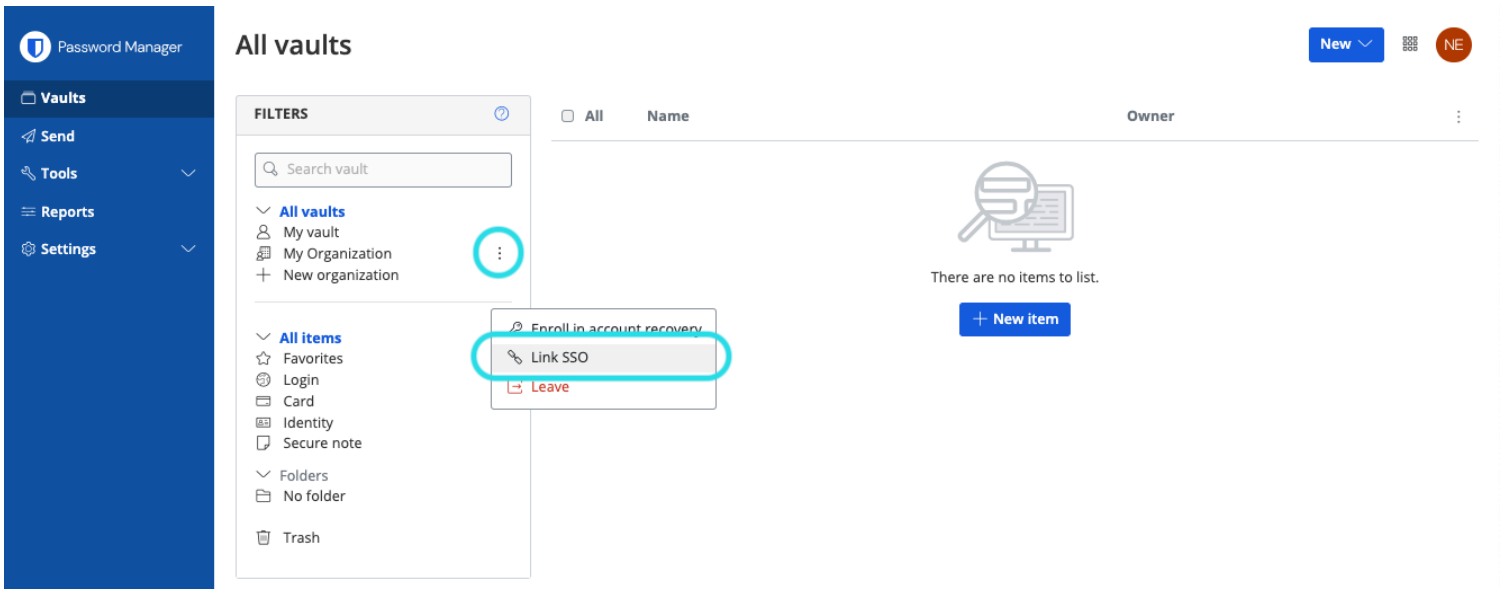
> **⚠ Warning**
>
> Two-step login via email is not recommended if you are using **login with SSO**, as using multiple methods will cause errors. Consider setting up two-step login via a free authenticator instead.

Link your account

You should only need to link your account to SSO if you already have a Bitwarden account that's a member of the organization or if your organization does not require you to use SSO:

1. Open the web app, and select the ⋮ **Options** menu next to your organization.

2. From the dropdown menu, select **Link SSO**.



Link SSO

Once linked, you should be able to login using SSO as documented above.

> **ⓘ Note**
>
> Once you're linked, you can **Unlink SSO** from the same menu. This is generally most useful when your email address changes in your IdP (e.g. Google, Azure) or in Bitwarden and SSO stops working as a result, or in situations when an IdP identity is linked to the wrong Bitwarden account and the existing link must be broken before a correct one can be made.