bitwarden | Help Center Article

ADMIN CONSOLE > LOGIN WITH SSO >

Add a Trusted Device

View in the help center:
https://bitwarden.com/help/add-a-trusted-device/

Add a Trusted Device

When you become a member of an organization, the device you log in with for the first time will automatically be registered as a trusted device. Once this occurs, all you'll need to do to log in to Bitwarden and decrypt your vault data is complete your company's established single sign-on flow.

> **Tip**
>
> Devices will be trusted by default when you log in on them. It is highly recommended that you uncheck the **Remember this device** option when logging in on a public or shared device.

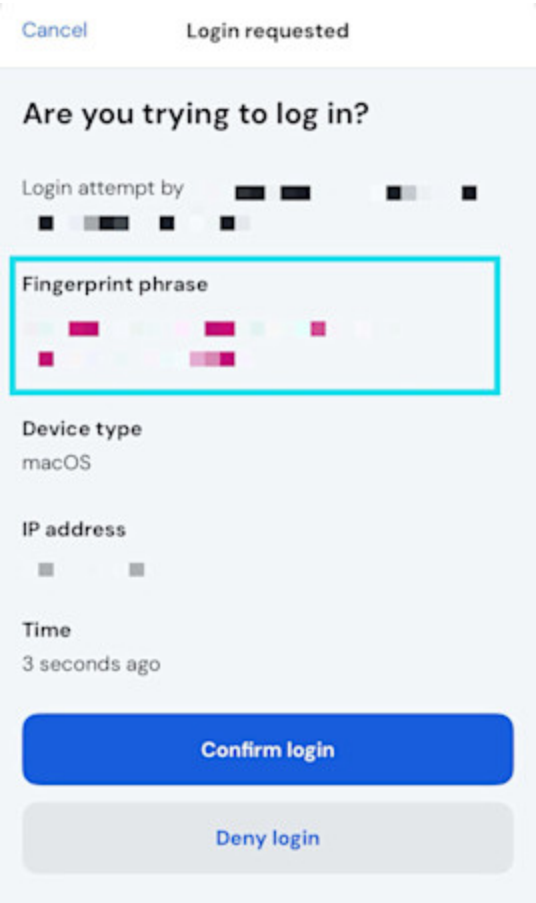
When you log into a new device however, you'll need to approve, or trust, that device. There are a few methods for doing so:

- **Approve from another device**: If you have another Bitwarden Password Manager web vault, mobile app or desktop app you're currently logged in to, you can approve the new device from there. On mobile, ensure first that the the Approve login requests option is enabled.

  ### ⇒Mobile app

  To approve a request with the mobile app once you have initiated **Log in with device**:

  1. Log in to the mobile app.
  2. Navigate to **Settings** → **Account security** → **Pending login requests**.
  3. Locate and select the active device request.
  4. Verify the fingerprint phrase and select **Confirm login**.



Mobile device approval

⇒Web app

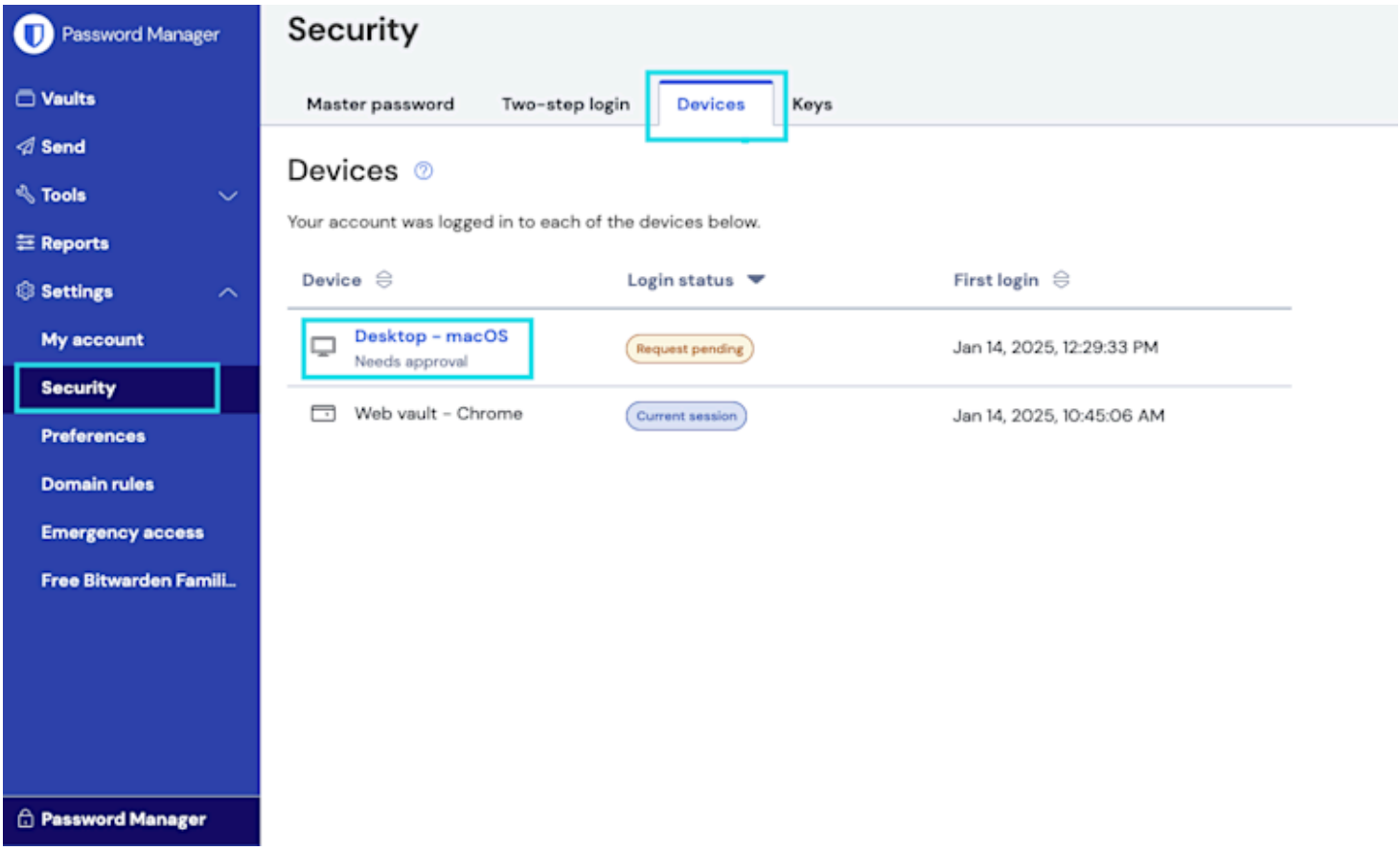
To approve a request with the web app once you have initiated **Log in with device**:

1. Log in to the web app.

> **ⓘ Note**
>
> When requesting approval for a login for the browser extension, the extension window must remain open until the process is completed. Bitwarden recommends:
>
> - **For Chrome and chromium browsers**: Open the web app in a separate browser window, this will allow the extension to remain open in the original window.
> - **For Safari**: Open the web app in a separate browser window, this will allow the extension to remain open in the original window.
> - **For Firefox**: Open the extension in the sidebar, this will allow it to persist while you open the web app.
>
> This will be improved in a future release.

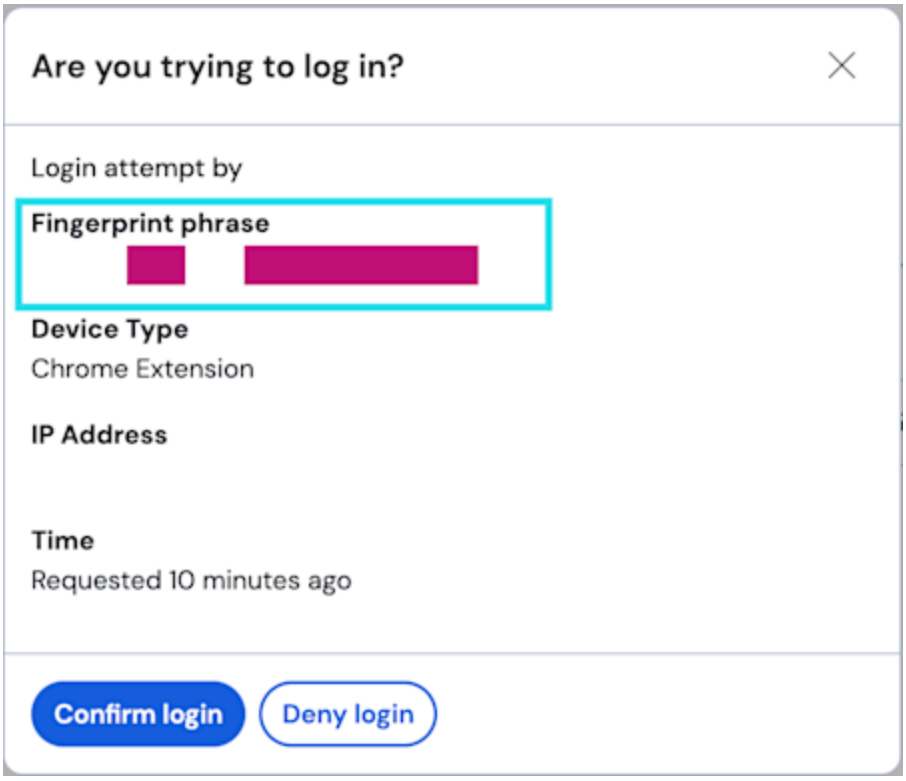
2. Navigate to **Settings** → **Security** → **Devices**.

3. Locate and select the active device request:



Web app approve device login

4. Verify the fingerprint phrase and select **Confirm login**.

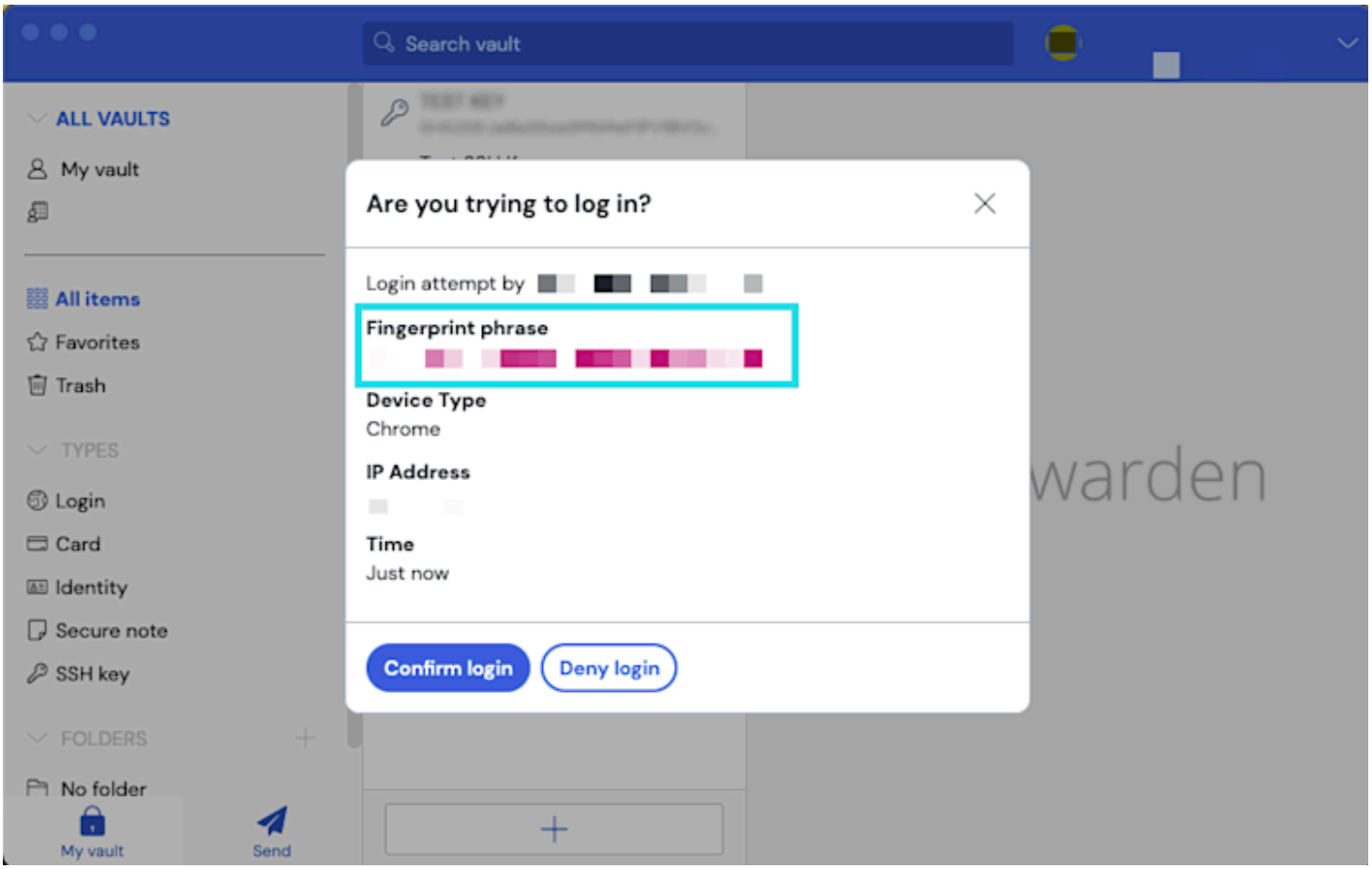


Confirm fingerprint web app

⇒Desktop app

To approve a request with the desktop app once you have initiated **Log in with device**:

1. Log in to the desktop app.
2. An authentication request will be sent to your desktop app:

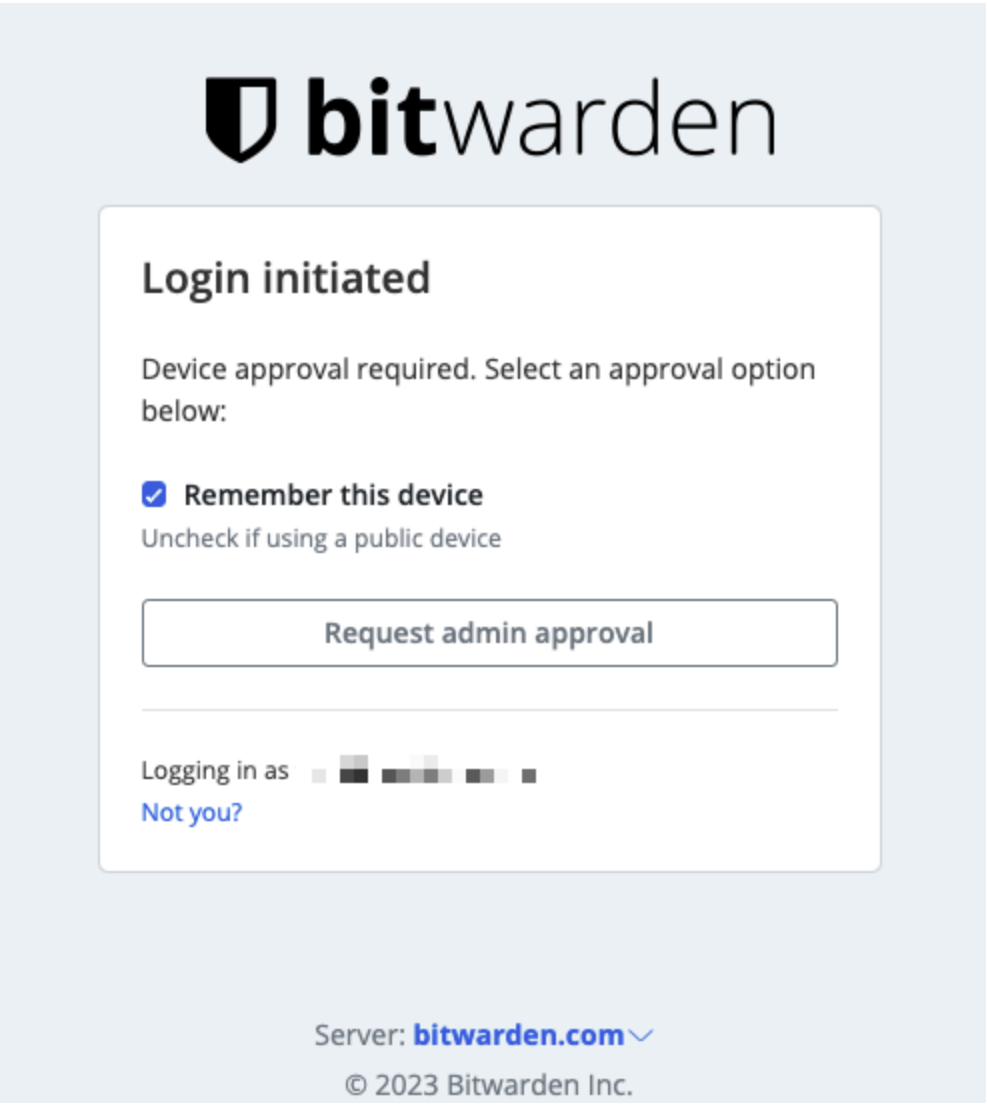


Approve device desktop

3. Verify the fingerprint phrase and select **Confirm login**.

> **Tip**
>
> We recommend trusting a mobile or desktop app first and immediately turning on the Approve login requests option. This will allow you to use the **Approve from another device** option to add subsequent devices.

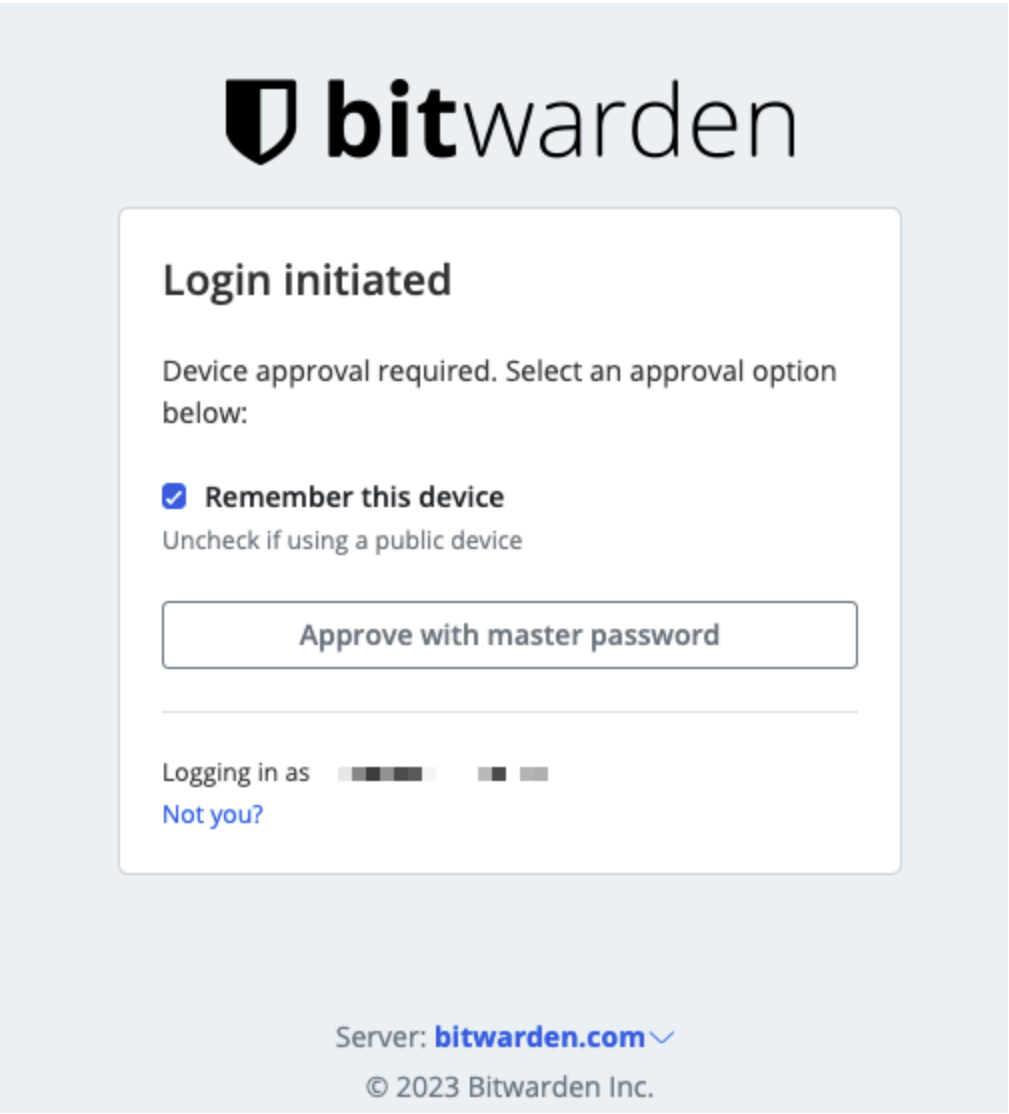
- **Request admin approval**: You can send a device approval request to admins and owners within your organization for approval. You **must** be enrolled in account recovery to request admin approval, though you may have been automatically enrolled when you joined the organization. In many cases, this will be the only option available to you (learn more).



Request admin approval

> **Note**
> If you use this option, you'll get an email informing you to continue logging in on the new device. You must take action by logging in to the new device within 12 hours, or the approval will expire.

- **Approve with master password**: If you are an admin or owner, or joined your organization before SSO with trusted devices was implemented, and therefore still have a master password associated with your account, you can enter it to approve the device.



Approve with master password

Once the new device becomes trusted, all you'll need to do to log in to Bitwarden and decrypt your vault data is complete your company's established single sign-on flow.

Adding your first trusted device

The initial client used to access Bitwarden for users who were invited with Just in Time (JIT) provisioning using login with SSO will become their first trusted device. If the initial client accessed is the Bitwarden desktop or mobile app, this device can be used to approve additional devices.

For the desktop or mobile app to become the first trusted device, the user should not use the organization invite link. Instead, open the mobile or desktop app and select the **Enterprise single sign-on** option to begin the JIT process.

Remove a trusted device

Devices will remain trusted until:

- The application or extension is uninstalled.

- The web browser's memory is cleared (web app only).
- The user's encryption key is rotated.

> **Note**
> Only users who have a master password can rotate their account encryption key. Learn more.