bitwarden | Help Center Article

MY ACCOUNT > LOG IN & UNLOCK

Log in with Device

View in the help center:
https://bitwarden.com/help/log-in-with-device/

Log in with Device

Although most people log into their Bitwarden vault with a master password, there is a more convenient method of doing so called passwordless authentication. Using **Log in with device**, any time you log into Bitwarden on one device, you can opt to use another logged-in web app, mobile app, or desktop app to approve those authentication requests instead of typing your master password.

Log in with device can be initiated on the web app, browser extension, desktop app, and mobile app. Requests issued by these apps can be approved on the web app, mobile app and desktop app.

Learn about our zero-knowledge encryption implementation.

Prepare to log in with a device

To set up logging in with a device:

- Log in normally to the initiating app (web vault, browser extension, desktop, or mobile app) at least once so that Bitwarden can recognize your device.

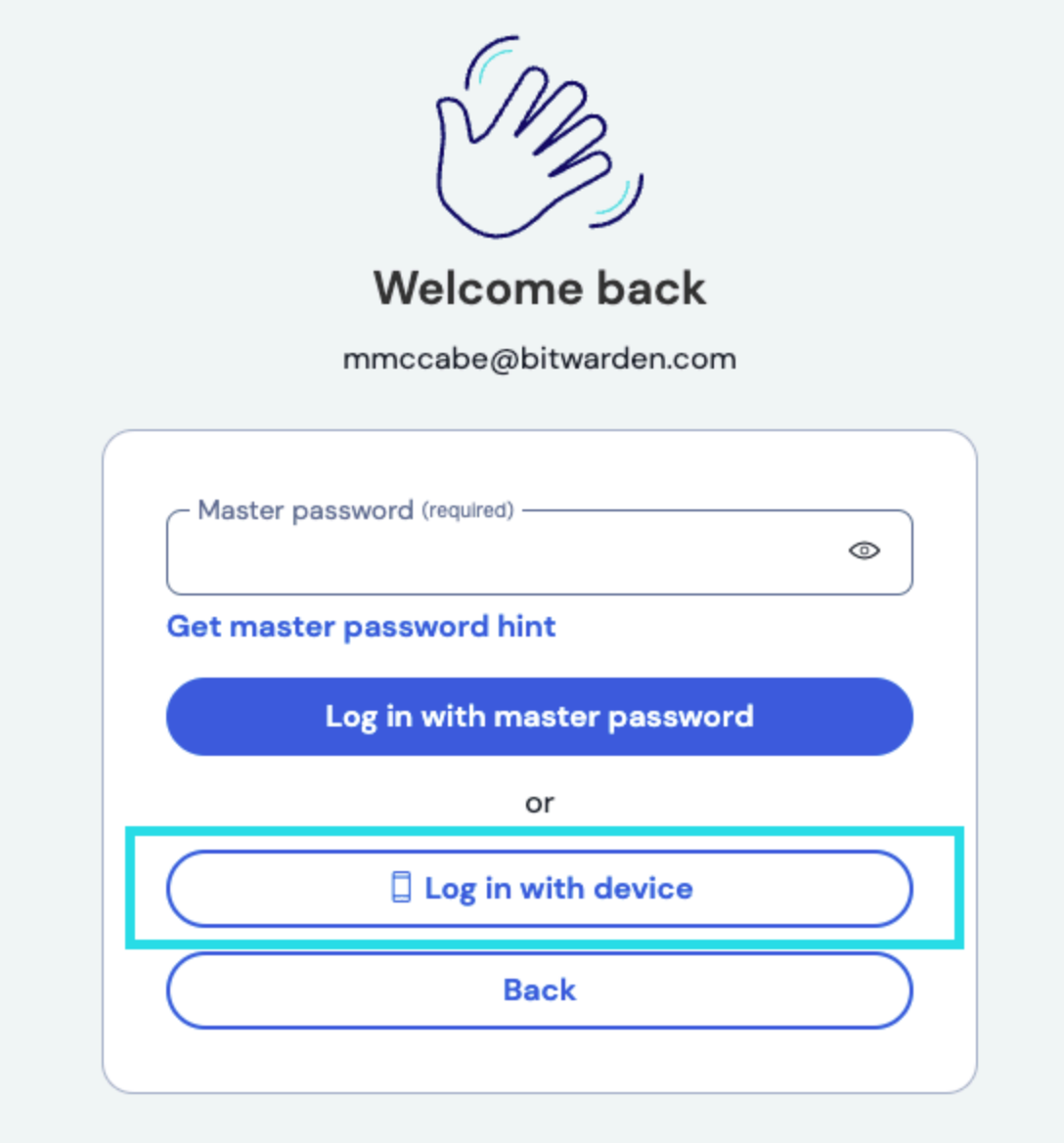
> **Note**
>
> Using Incognito mode or Private Browsing prevents Bitwarden from registering your browser, so you won't be able to log in with a device in a private browser window.

- Have a recognized account on an approving app (web vault, mobile or desktop app). Recognizing an account requires you to have successfully logged on to that device at any time.

> **Note**
>
> If, as a member of an Enterprise organization, you are subject to the require SSO policy, you won't be able to use the **Log in with device** option. You'll need to use SSO to log in instead.

Logging in with a device

On the login screen of the initiating app, enter your email address and select **Continue**. Then, select the **Log in with device** option:



Log in with a device

Using **Log in with device** will send authentication requests to any web vault, mobile or desktop apps that you're currently logged-in to for approval.

⇒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

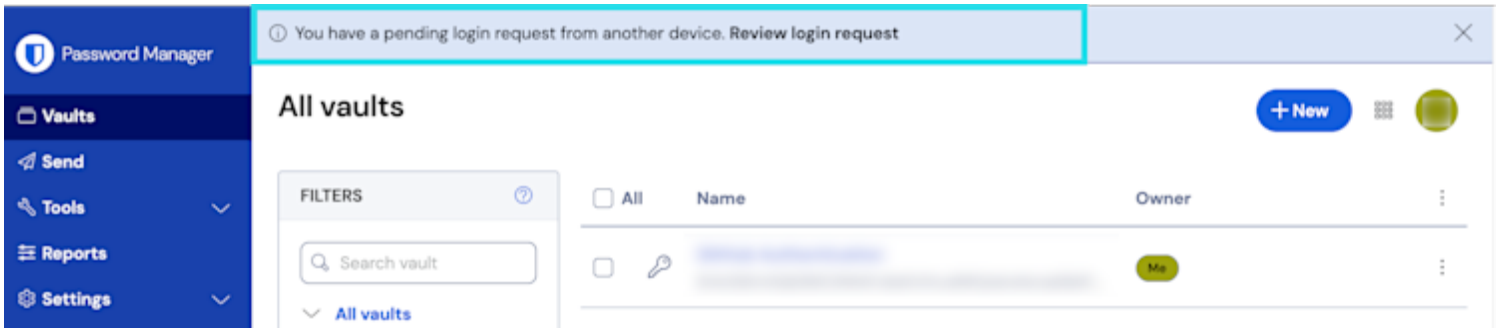
⇒Web app

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

1. Log in to the web app.

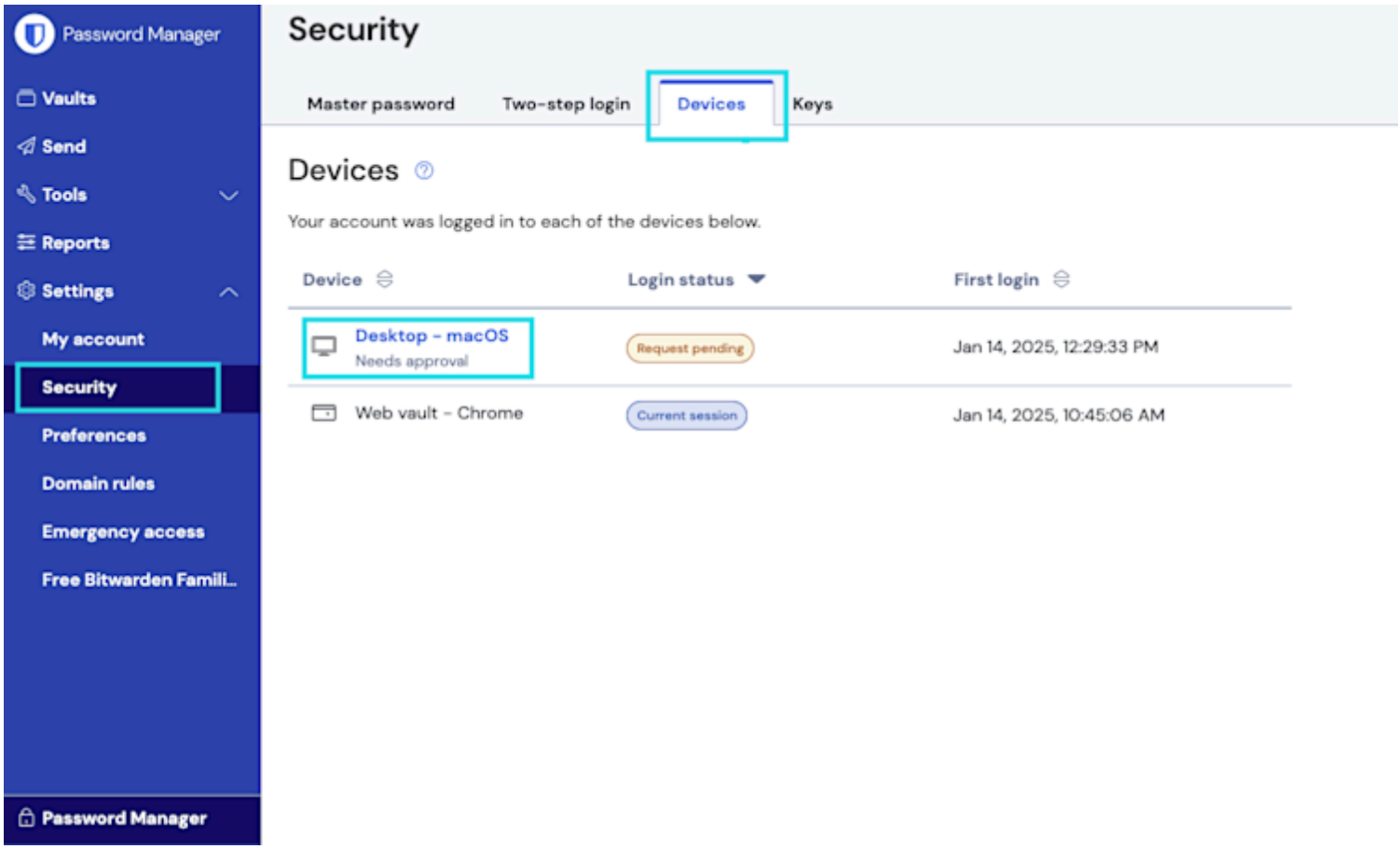
> **ⓘ Note**
>
> When requesting approval for a login for the browser extension, the extension window must remain open until the process is completed. Bitwarden recommends:
>
> - **For Chrome and chromium browsers**: Open the web app in a separate browser window, this will allow the extension to remain 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**, or select the link on the banner notification:



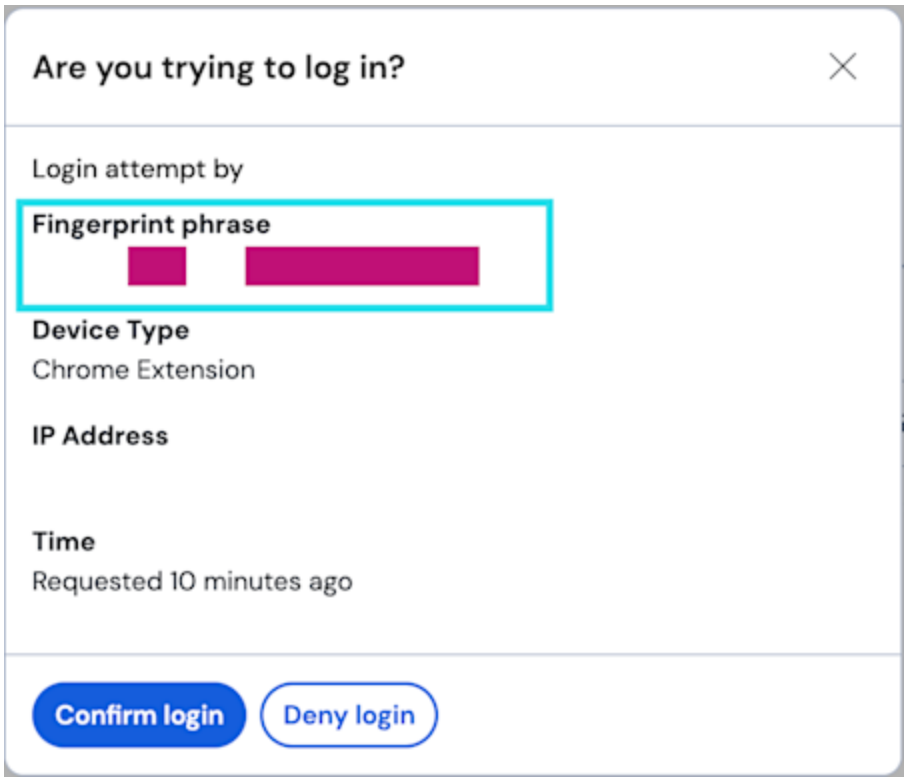
Login with Device Notification

3. Locate and select the active device request:



Web app approve device login

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

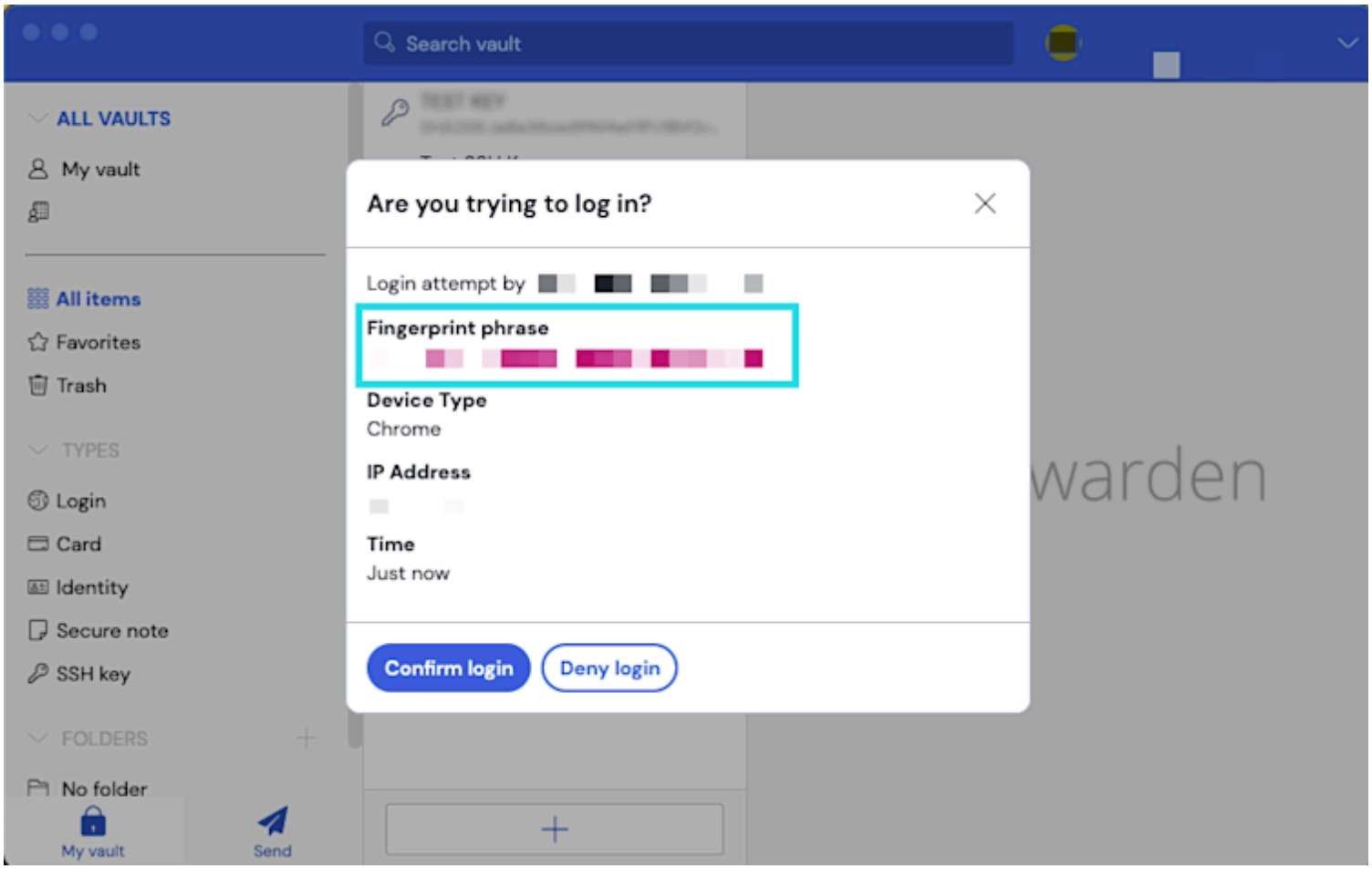


Confirm fingerprint web app

⇒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**.

Note that this is a unique fingerprint that isn't the same as your account fingerprint phrase.

Requests expire after 15 minutes if they aren't approved or denied. If you are not receiving login requests, try refreshing the web app, or manually syncing your vault from the mobile app.

> **Note**
>
> If you use the **Login with device** option, you'll still need to use any currently active two-step login method.

How it works

When logging in with a device is initiated:

1. The initiating client POSTs a request, which includes the account email address, a unique auth-request public key[a], and an access code, to an Authentication Request table in the Bitwarden database.

2. Registered devices, meaning mobile or desktop apps that are logged in and have a device-specific GUID stored in the Bitwarden database, are provided the request.

3. When the request is approved, the approving client encrypts the account's master key and master password hash using the auth-request public key enclosed in the request.

4. The approving client then PUTs the encrypted master key and encrypted master password hash to the Authentication Request record and marks the request fulfilled.

5. The initiating client GETs the encrypted master key and encrypted master password hash.

6. The initiating client then **locally** decrypts the master key and master password hash using the auth-request private key.

7. The initiating client then uses the access code and fulfilled authentication request to authenticate the user with the Bitwarden Identity service.

[α] - Auth-request public and private keys are uniquely generated for each passwordless login request and only exist for as long as the request does. Requests expire and are purged from the database every 15 minutes if they aren't approved or denied.