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 a different Bitwarden app you're logged in to to approve the authentication request instead of typing your master password.

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 app, browser extension, desktop, or mobile app) at least once so that Bitwarden can recognize your device.

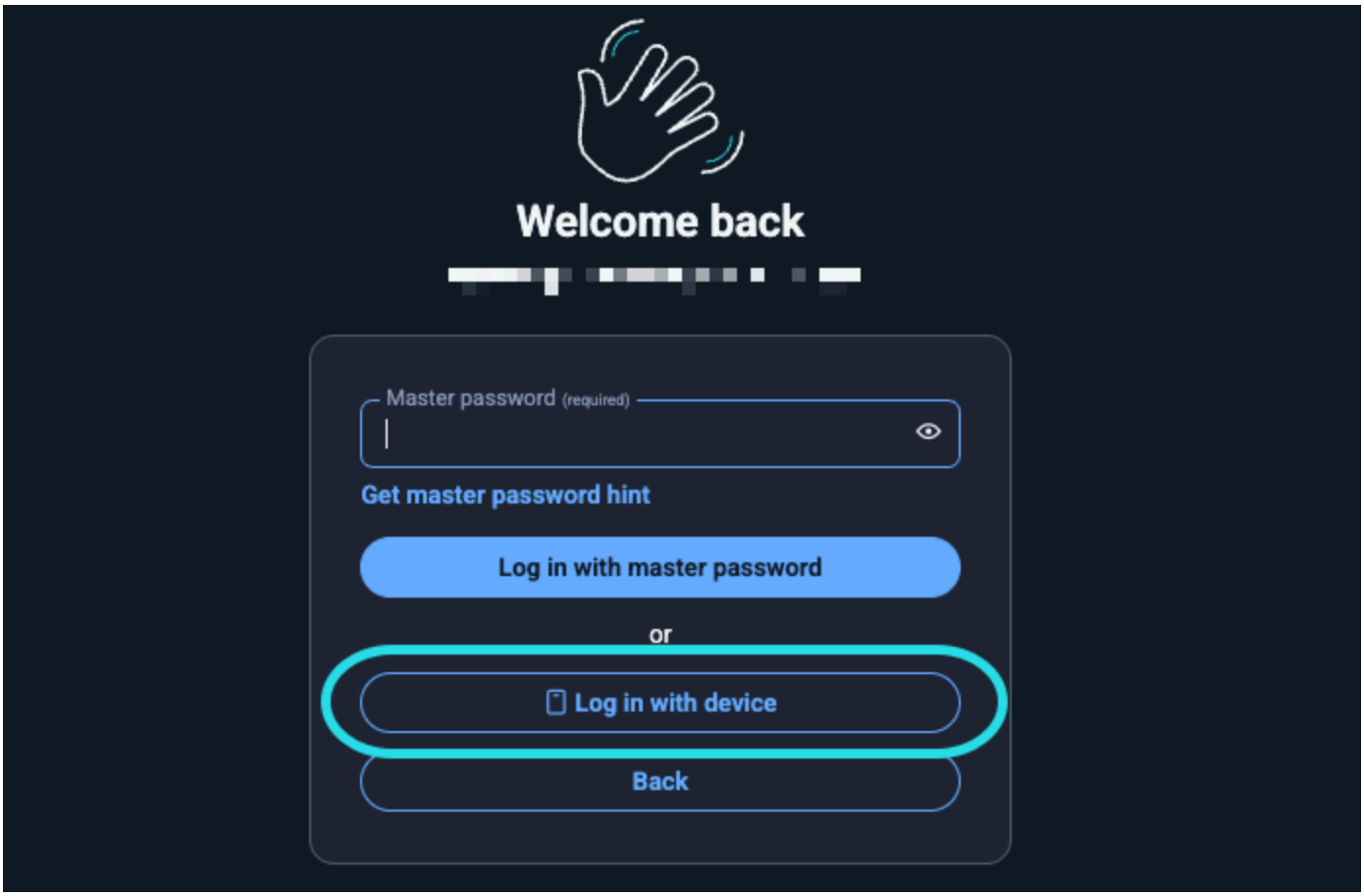
> **ⓘ Note**
>
> Using Incognito mode or Private Browsing prevents Bitwarden from registering your browser, so you won't be able to log in with a device in a private browser window.

- Have a recognized account on an approving app (web app, browser extension, 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.

Log 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

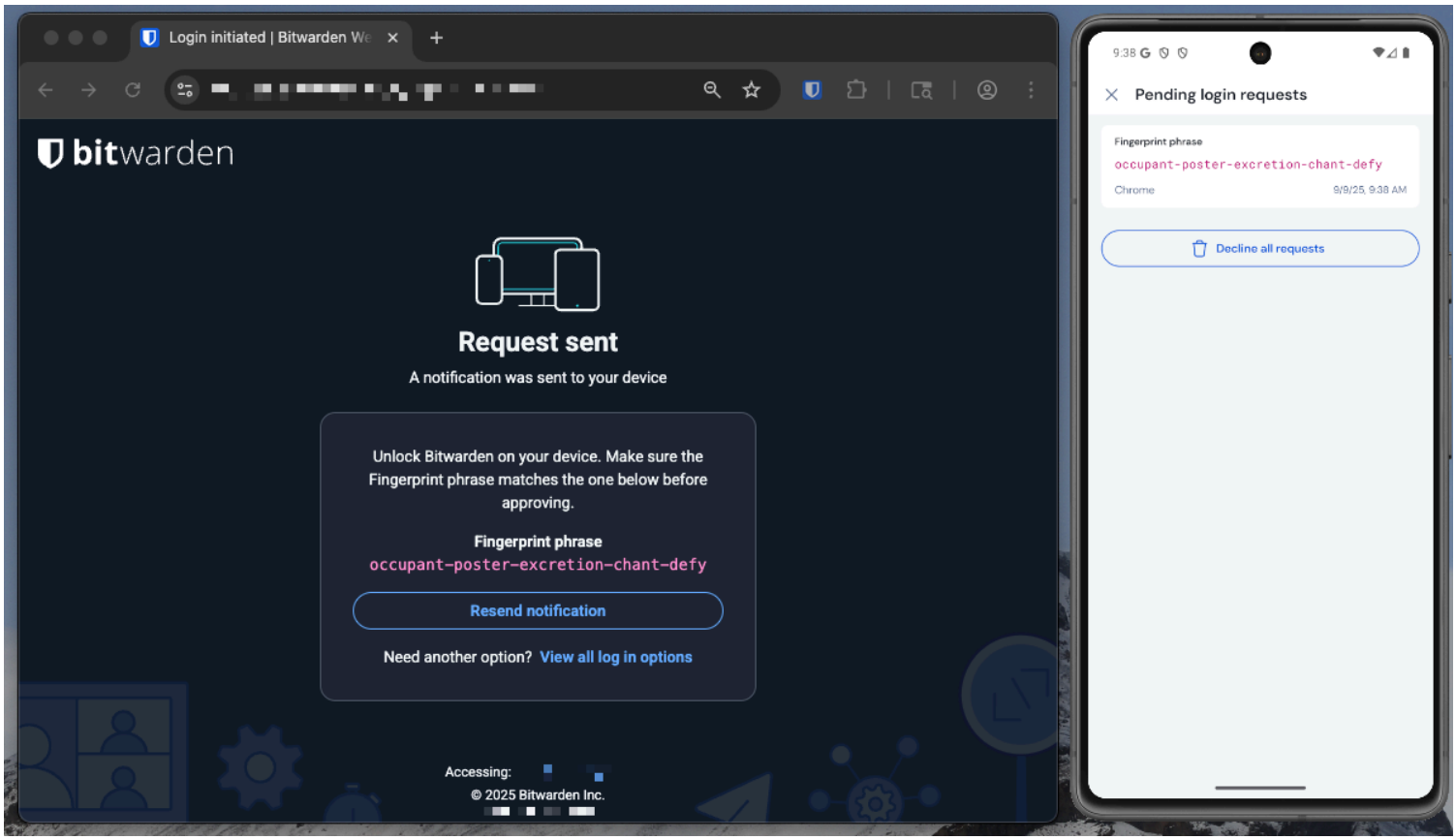
Approve a log in request

Using **Log in with device** will send authentication requests to any Bitwarden app that you're currently logged in to for approval:

⇒Mobile app

To approve a request with the mobile app:

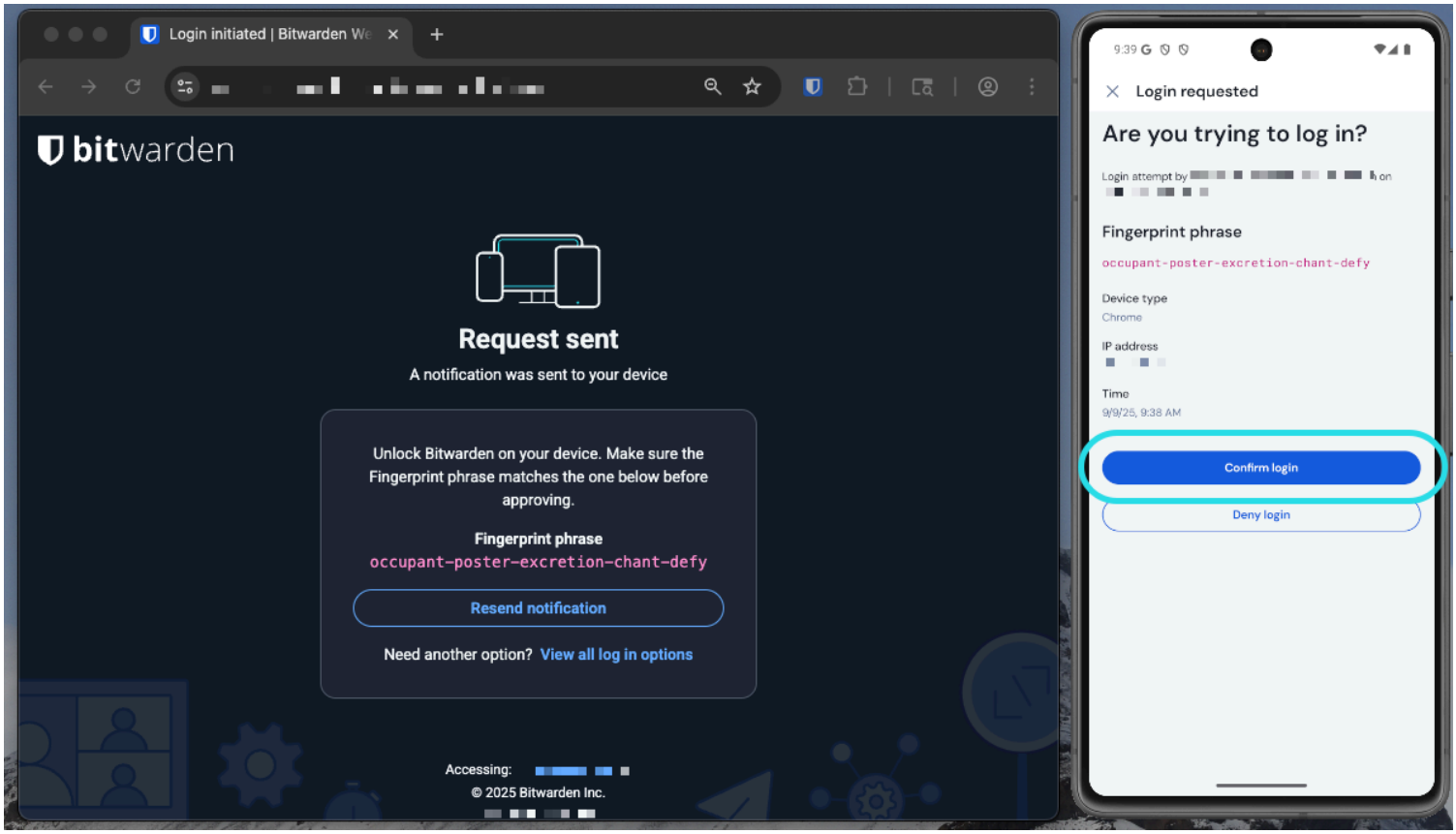
1. In the mobile app, navigate to **Settings** → **Account security** → **Pending login requests**:



Pending login requests on mobile

2. Locate and tap the pending device request.

3. Verify that fingerprint phrase matches and select **Confirm access**:

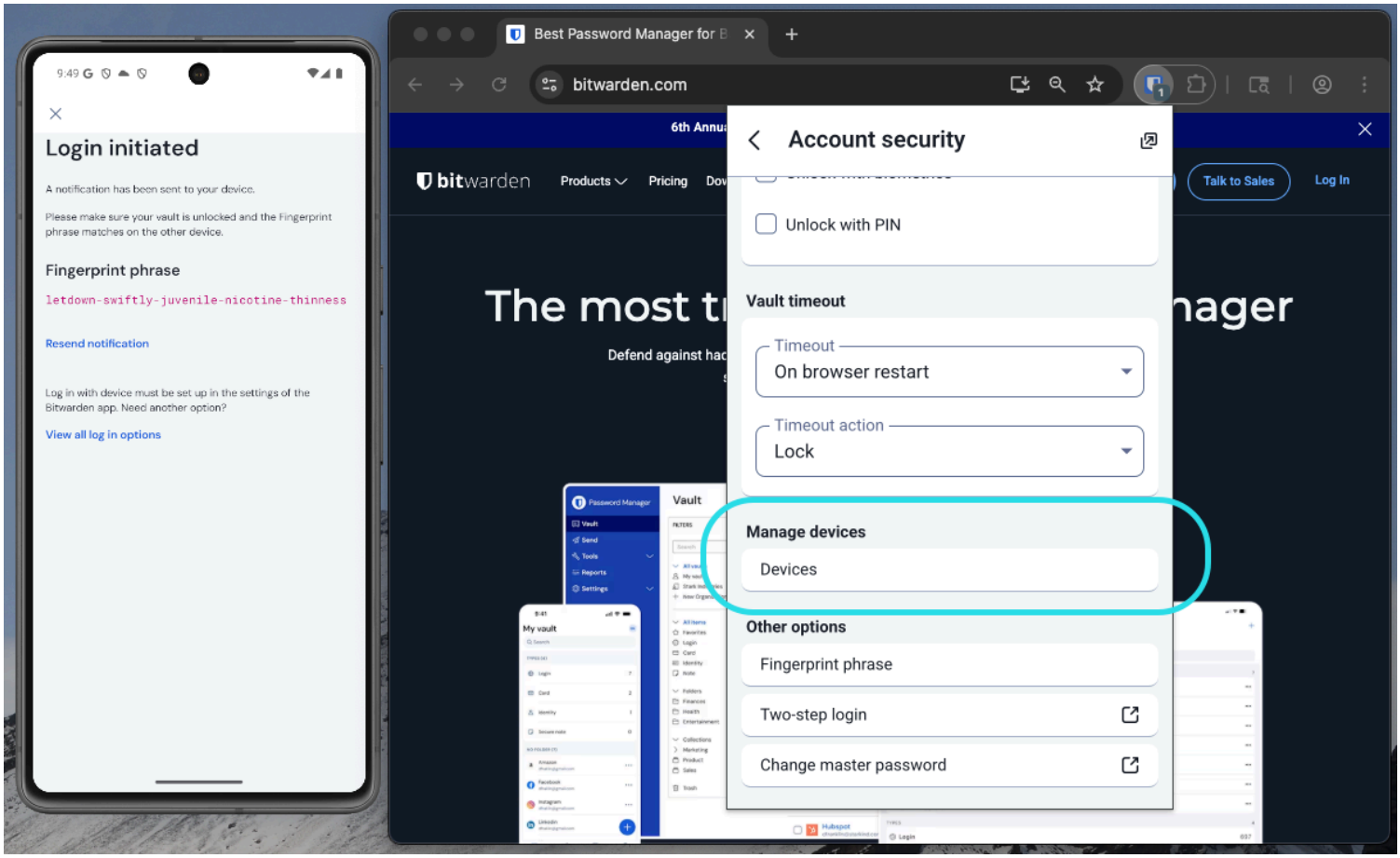


Approve a login on mobile

⇒Browser extension

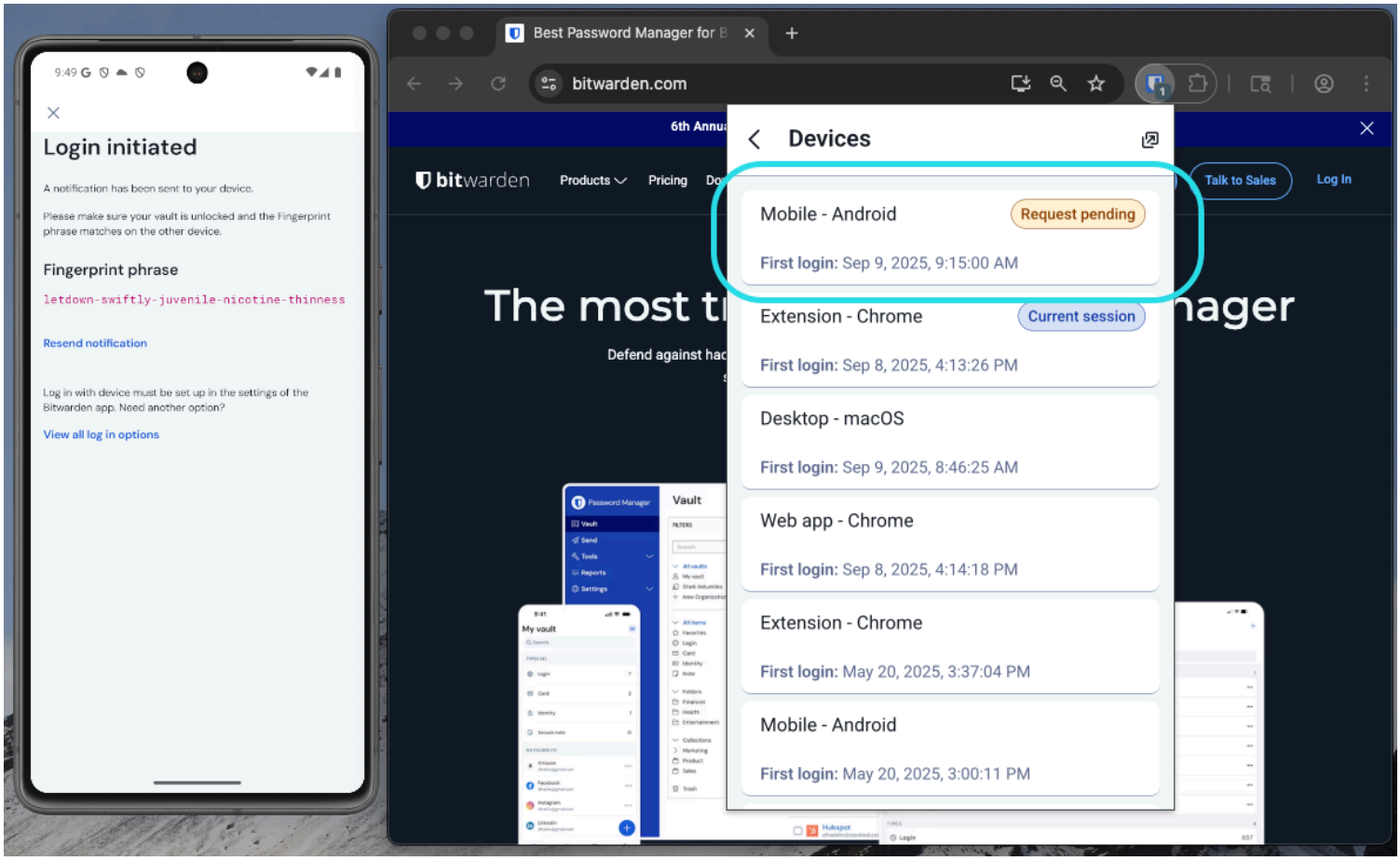
To approve a request with the browser extension:

1. In the browser extension, wait for a device approval request to be received or navigate to **Settings** → **Account security** → **Devices**:



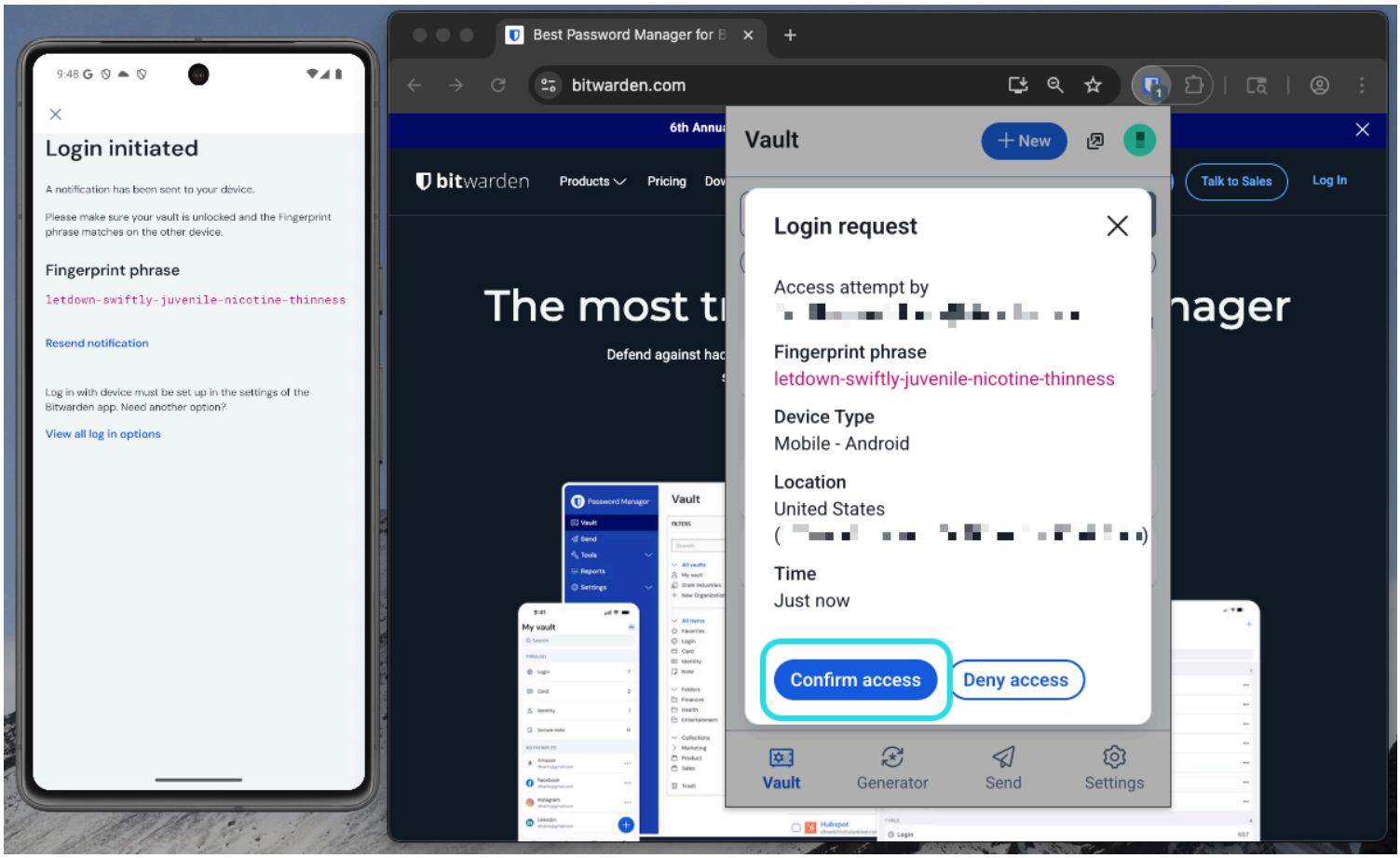
Devices view on browser extensions

2. In the **Devices** view, locate and select the pending device request:



Devices list on browser extensions

3. Verify that fingerprint phrase matches and select **Confirm access**:



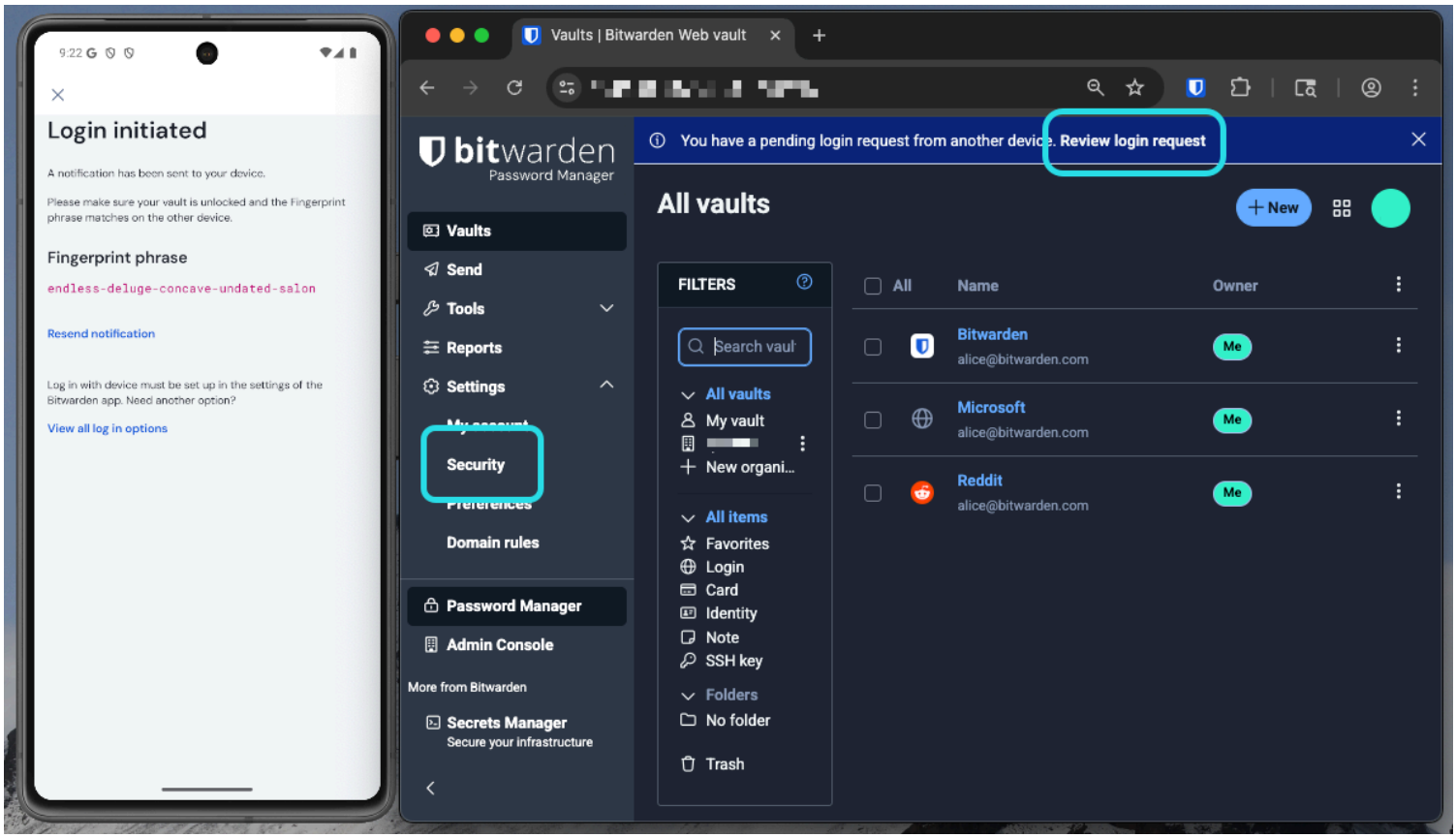
Approve a device on browser extensions

⇒Web app

To approve a request with the web app:

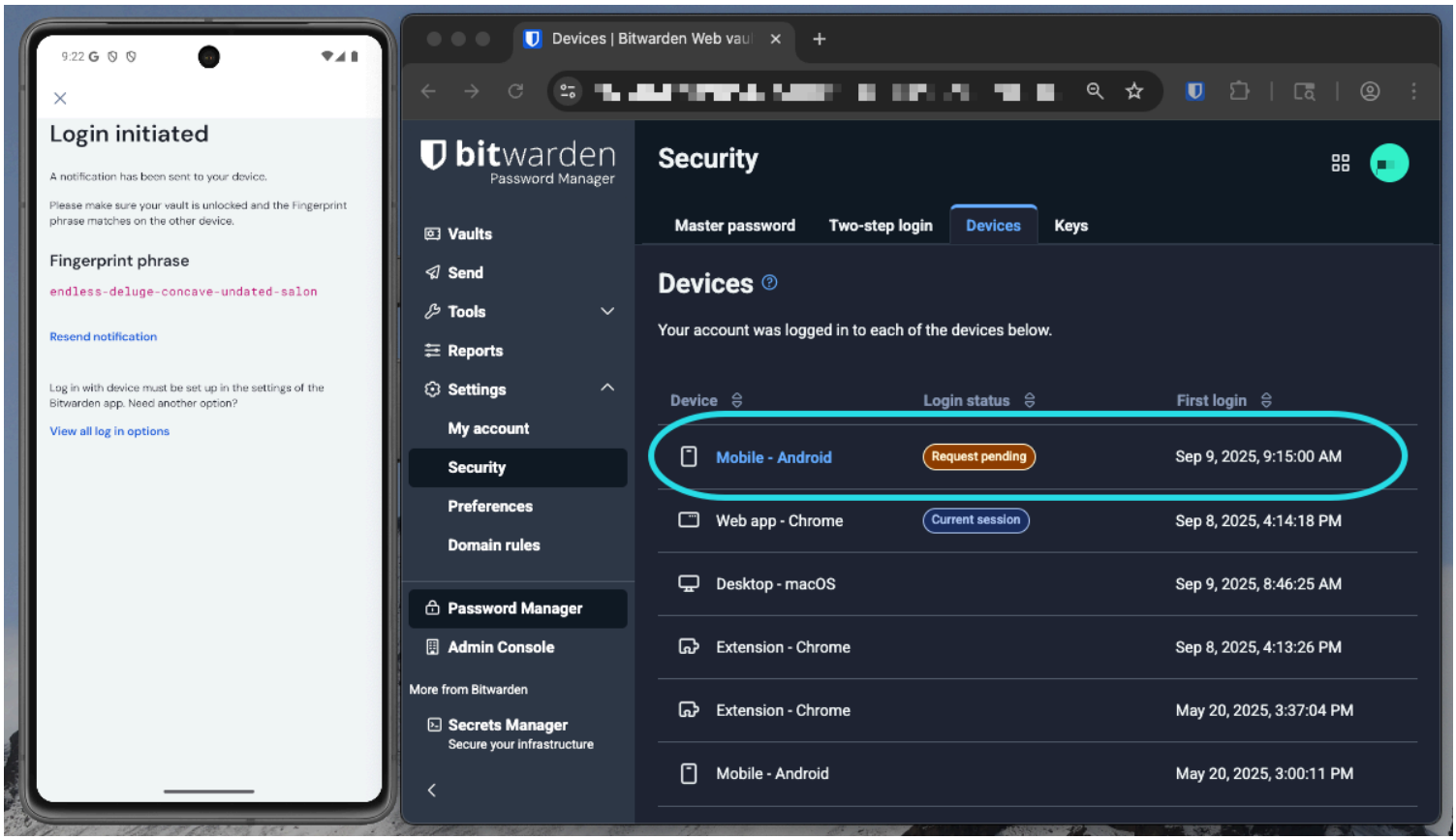
> **ⓘ Note**
>
> When requesting approval for a login of the browser extension, the extension will wait for up to two minutes for approval even if you click out of or minimize the extension window in order to approve the request using the web app.

1. In the web app, select the **Review login request** link in the banner notification or navigate to **Settings** → **Security** → **Devices**:



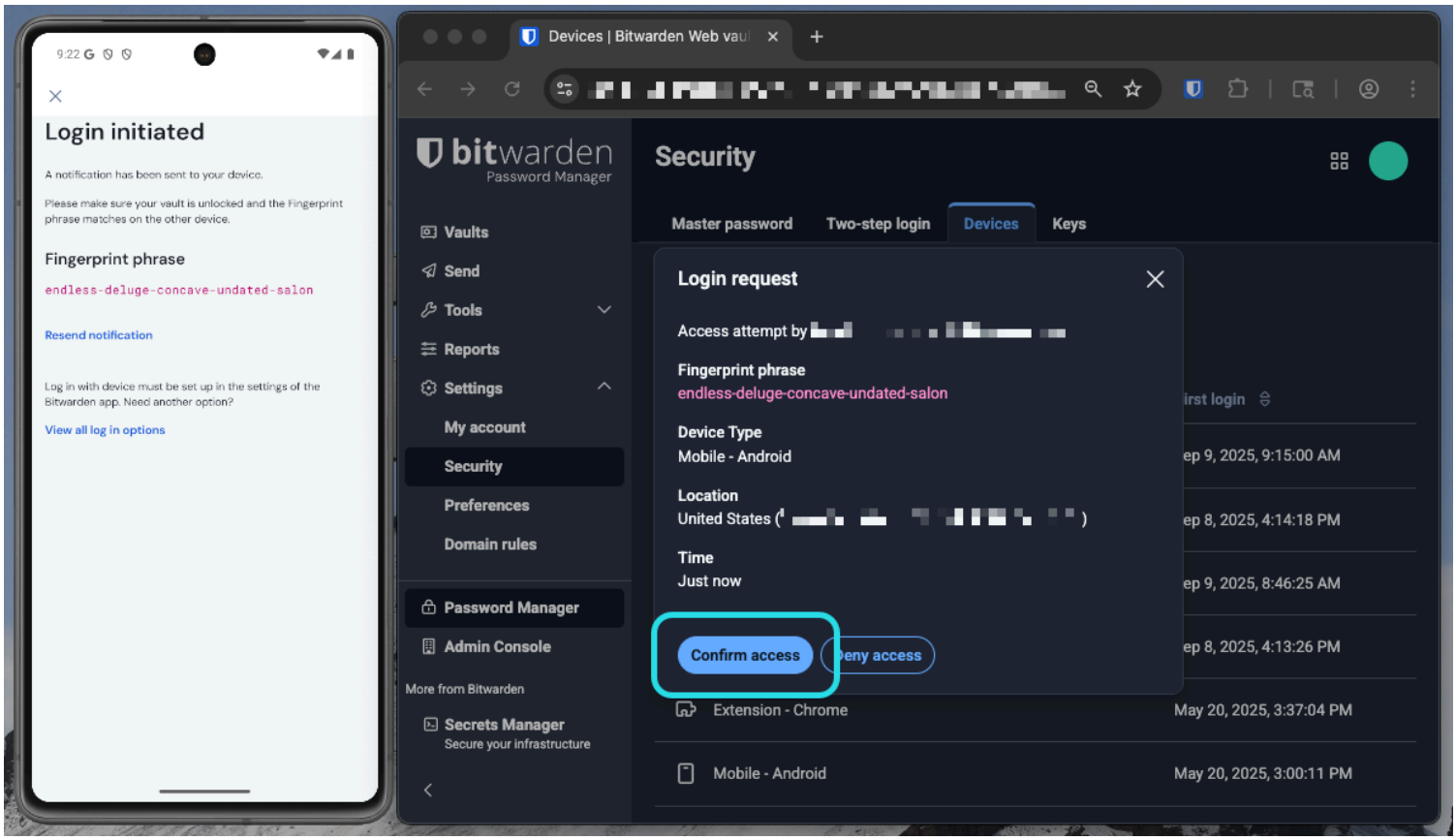
Approval request on web

2. On the **Devices** tab, locate and select the pending device request:



Device list on web app

3. Verify that fingerprint phrase matches and select **Confirm access**:

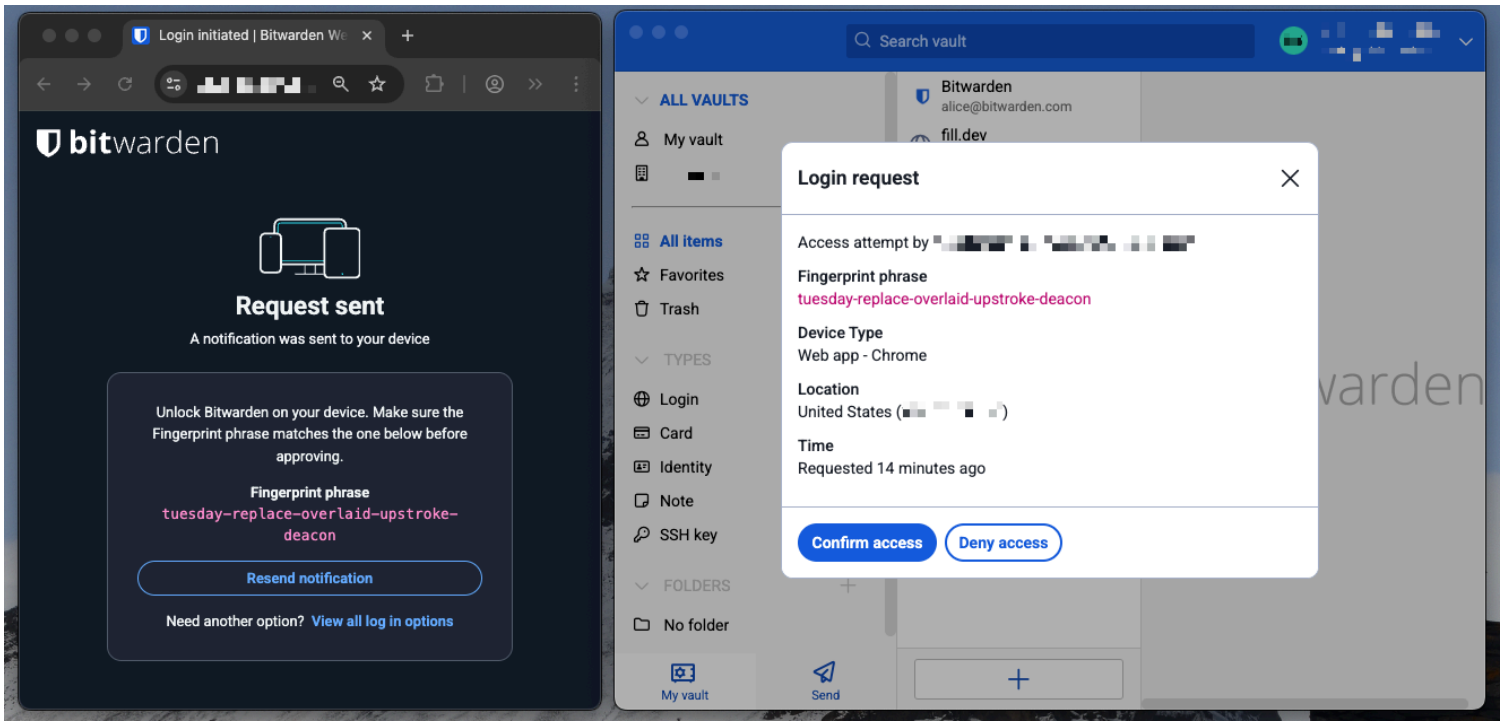


Confirm access with web app

⇒Desktop app

To approve a request with the desktop app:

1. In the desktop app, wait for a device approval request to be received:



Approve on desktop

2. Verify that fingerprint phrase matches and select **Confirm access**.

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 sends 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. Registered devices, meaning clients that are logged in and have a device-specific GUID stored in the Bitwarden database, are provided the request.

2. When the request is approved, the approving client encrypts the account's **User Encryption key** using the **Auth-request public key** enclosed in the request.

3. The approving client then sends the **User Encryption key** to the Authentication Request record and marks the request fulfilled.

4. The initiating client requests the encrypted **User Encryption key**.

5. The initiating client then **locally** decrypts the **User Encryption key** using the **Auth-request private key.**

6. The initiating client then uses the access code to authenticate the user with the Bitwarden Identity service.

7. The initiating client can then retrieve the user's vault data and use the **User Encryption key** to decrypt it.

[a] - **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 periodically if they aren't approved or denied.