bitwarden | Help Center Article

MITT KONTO > LOGGA IN OCH LÅS UPP >

Lås upp med Biometrics

View in the help center:
https://bitwarden.com/help/biometrics/

Lås upp med Biometrics

Bitwarden kan konfigureras för att acceptera biometri som en metod för att låsa upp ditt valv.

Biometri kan **endast användas för att låsa upp** ditt valv, du kommer fortfarande att behöva använda ditt huvudlösenord eller logga in med enheten, och alla aktiverade tvåstegsinloggningsmetoder när du **loggar in**. Lås upp med Biometrics är inte en funktion utformad för att vara en lösenordslös inloggning, om du inte är säker på skillnaden, se Förstå upplåsning vs. logga in.

> **Tip**
>
> Biometric features are part of the built-in security in your device and/or operating system. Bitwarden leverages native APIs to perform this validation, and therefore **Bitwarden does not receive any biometrics information** from the device.

Aktivera upplåsning med biometri

Lås upp med biometri kan aktiveras för Bitwarden på mobil-, dator- och webbläsartillägg:

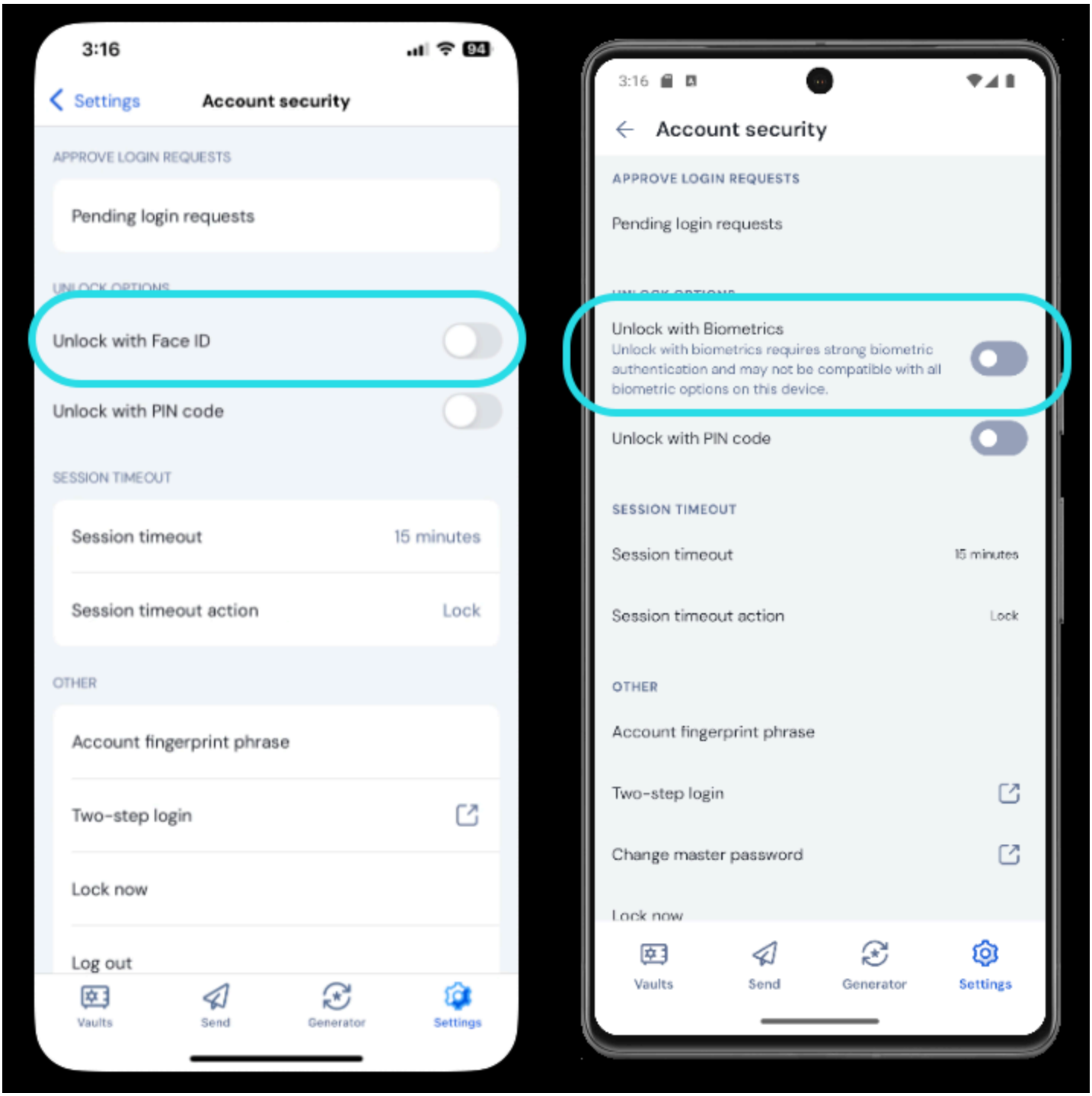
⇒Mobile

Enable for mobile

Unlock with biometrics is supported for Android (Google Play or FDroid) via fingerprint unlock or face unlock, and for iOS via Touch ID and Face ID.

To enable unlock with biometrics for your mobile device:

1. In your device's native settings (e.g. the iOS **Settings** app), make sure your biometric method is turned on.
2. In your Bitwarden app, open the **Settings** tab.
3. Open the Account security section and tap the biometrics option you want to enable. What's available on this screen is determined by your device's hardware capabilities and what you have enabled (**step one**), for example:



Biometric unlock on mobile

Tapping the option will prompt you to input your biometric (for example, face or thumb-print). The toggle will fill in when unlock with biometrics is successfully enabled.

Disabled pending master password verification

If you get a message reporting that biometric unlock is disabled for auto-fill pending verification of your master password:

1. Temporarily turn off auto-fill in Bitwarden.

2. Re-enable biometrics in Bitwarden.

3. Turn auto-fill back on in Bitwarden.

⇒Desktop

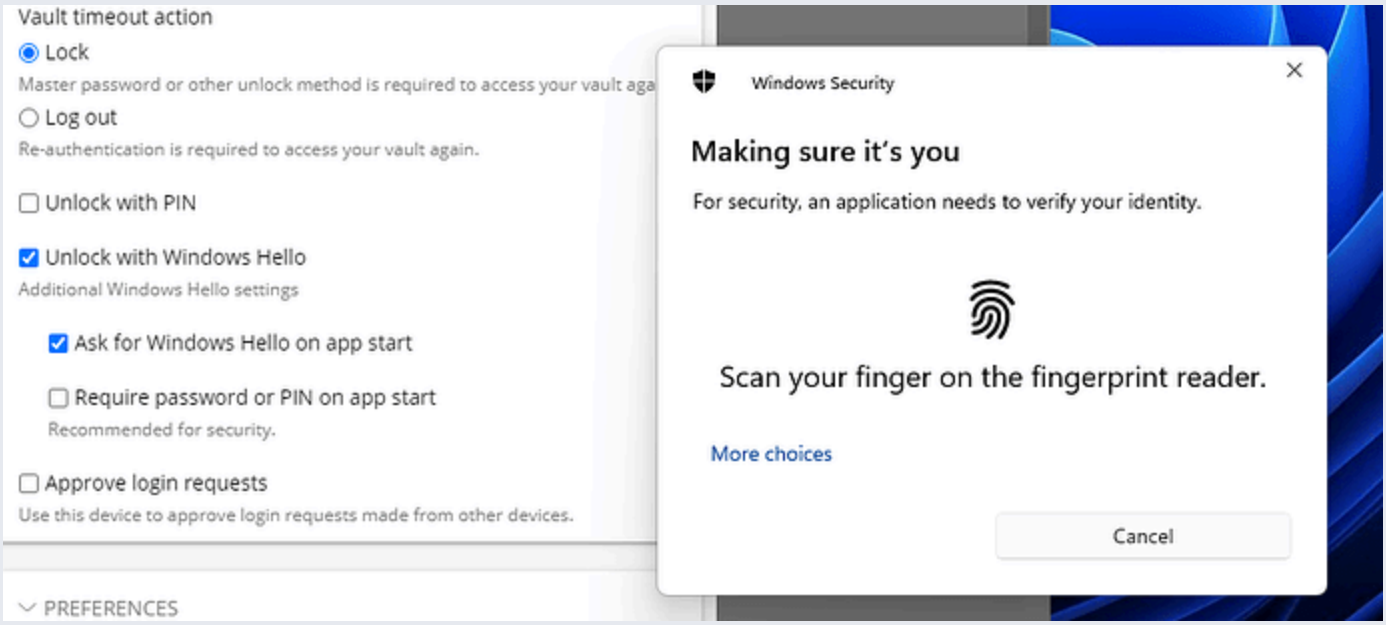
Enable for desktop

Unlock with biometrics is supported for Windows via Windows Hello using PIN, Facial Recognition, or other hardware that meets Windows Hello biometric requirements and for macOS via Touch ID and for Linux with system authentication.

Unlock with biometrics is set separately for each account logged in to the desktop app. To enable unlock with biometrics:

1. In your device's native settings (for example, the macOS ⚙ **System Preferences** app), make sure your biometric method is turned on.

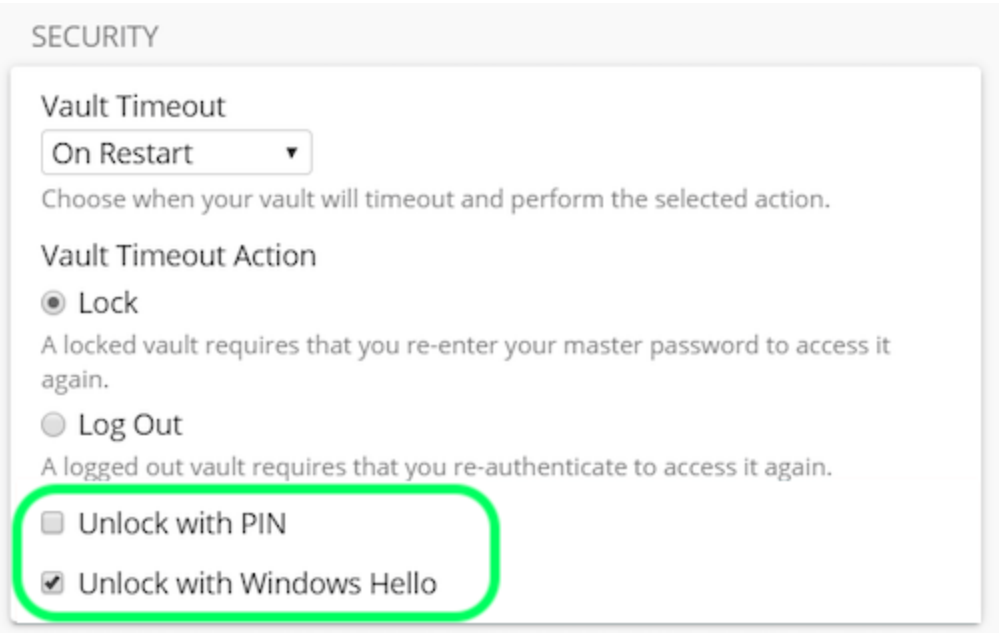
> **Tip**
>
> Windows users may need to install the Microsoft Visual C++ Redistributable before Windows Hello can be turned on in desktop preferences. Note that, the first time you activate Windows Hello on your machine, a required "Making sure it's you" prompt may appear in the background or timeout if not confirmed:



Windows Hello prompt

2. In your Bitwarden app, open your Settings (on Windows or Linux, **File → Settings**) (on macOS, **Bitwarden → Settings**).

3. In the security section, select the biometric option you want to enable. What's available on this screen is determined by your device's hardware capabilities and what you've turned on (**step 1**). On Linux, this will always be **Unlock with system authentication**. Example:

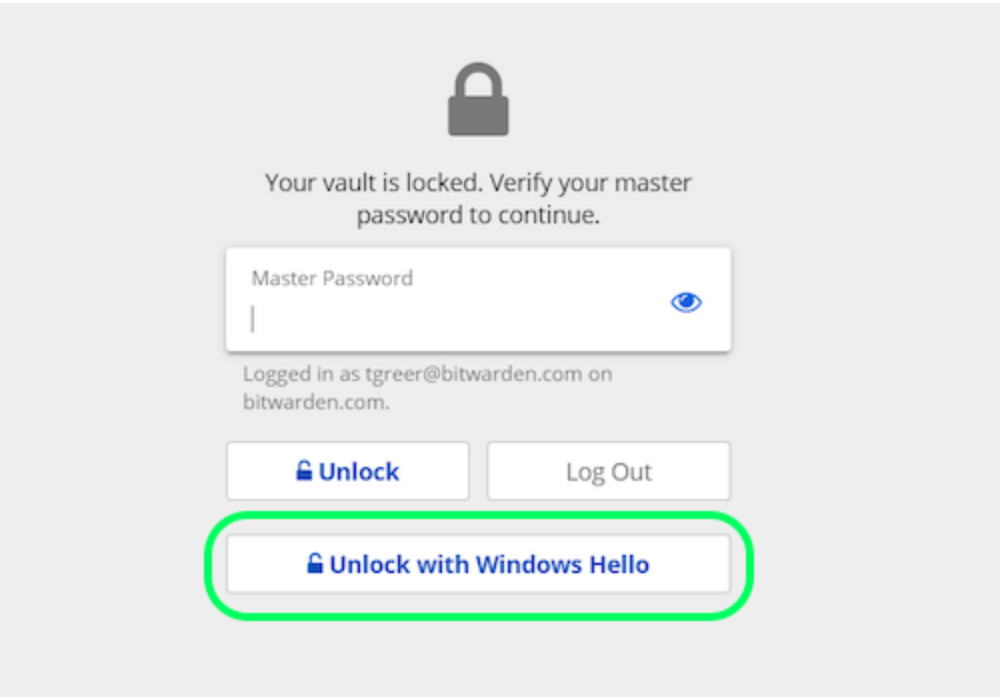


Unlock with Windows Hello

4. Optionally, select either the **Require password (or PIN) on app start** or **Ask for biometric on app start** option to set how your desktop app will behave when you start the the app.

> **Tip**
>
> If you're using Windows, Bitwarden recommends using the **Require password (or PIN) on first login after start** in order to maximize security.

If you select neither option, you can simply select the **Unlock with biometric** button on the login screen to prompt for your biometric option:



Unlock with Windows Hello

⇒Browser extension

About Biometrics in browser extensions

Unlock with biometrics is supported for extensions through an integration with the Bitwarden desktop app. In practical terms, this means:

1. **For all browser extensions**, you will need to enable unlock with biometrics in desktop before proceeding. **For all except Safari**, the Bitwarden desktop app must be logged in and running in order to use unlock with biometrics for a browser extension.

2. Browser extensions support the same biometrics options as desktop; for Windows via Windows Hello using PIN, Facial Recognition, or other hardware that meets Windows Hello biometric requirements, for macOS via Touch ID, and for Linux (Chromium-based browsers only) with system authentication.

Two things to bear in mind before enabling the integration are **Permissions** and **Supportability**, documented below:

Permissions

To facilitate this integration, browser extensions **except Safari** will ask you to accept a new permission for Bitwarden to `communicate with cooperating native applications`. This permission is safe, but **optional**, and will enable the integration that is required to enable unlock with biometrics.

Declining this permission will allow you to use the browser extension as normal, without unlock with biometrics functionality.

Supportability

Unlock with biometrics is supported for extensions on **Chromium-based** browsers (Chrome, Edge, Opera, Brave, and more), Firefox 87+, and Safari 14+. Unlock with biometrics is **currently not supported for**:

- Firefox ESR (Firefox v87+ will work).

- Microsoft App Store desktop apps (a side-loaded Windows desktop app, available at bitwarden.com/download will work fine).

- Side-loaded MacOS desktop apps (an App Store desktop app will work fine).

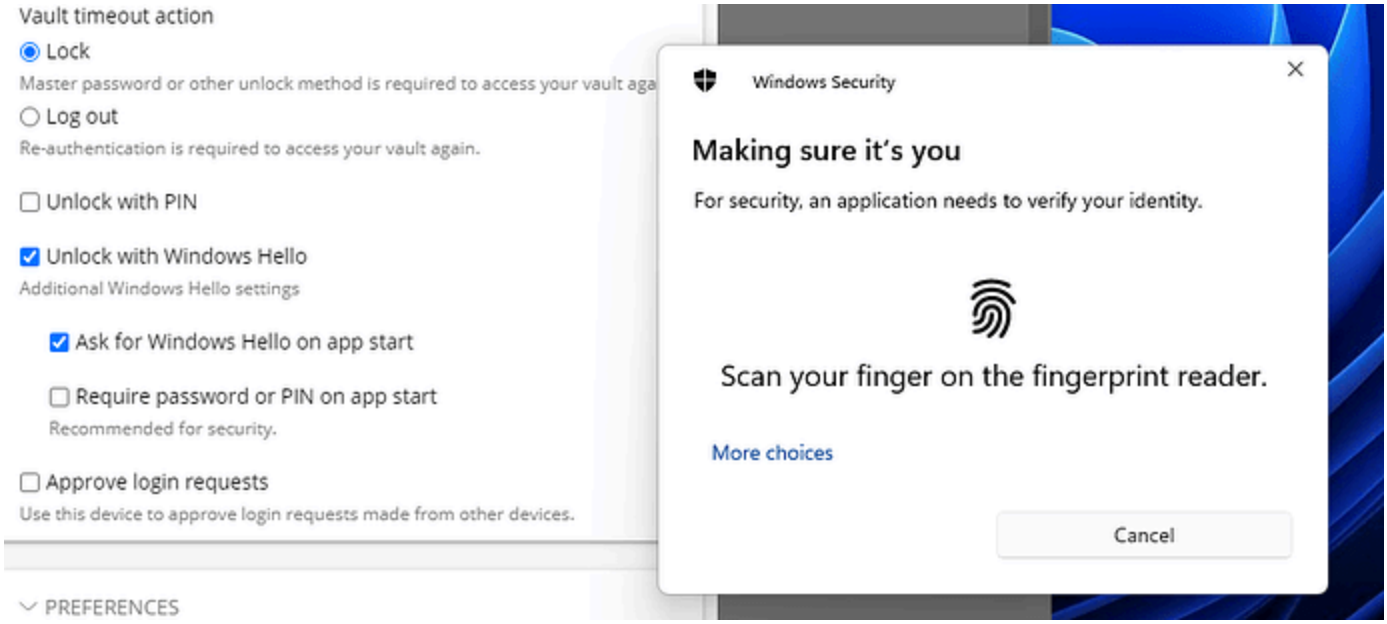
Enable for browser extensions

To enable unlock with biometrics for your browser extension:

Tip

Biometrics (Windows Hello or Touch ID) must be enabled in your desktop app before proceeding. If you don't see the Windows Hello option in your desktop app, you may need to install the Microsoft Visual C++ Redistributable. Additionally, **if you are using Safari**, you can skip straight to **step 4**.

Note that, the first time you activate Windows Hello on your machine, a required "Making sure it's you" prompt may appear in the background or timeout if not confirmed:



Windows Hello prompt

1. In your Bitwarden desktop app, navigate to settings (on Windows, **File → Settings**) (on macOS, **Bitwarden → Settings**).

2. Scroll down to the options section, and check the **Allow browser integration** box.

Note

On macOS, you may encounter an error if your username directory (e.g. `/Users/your_username/Library/...`) is longer than 104 characters. If you encounter this. error, shorten your username (e.g. `your_username`).

Note

Optionally, check the **Require verification for browser integration** option to require a unique fingerprint verification step when you activate the integration.

3. In your Browser, navigate to the extensions manager (e.g. `chrome://extensions` or `brave://extensions`), open Bitwarden, and toggle the **Allow access to file URLs** option.

   Not all browsers will require this to be toggled on, so feel free to skip this step and circle back to it only if the remaining procedure doesn't work.

4. In your browser extension, open the ⚙ **Settings** tab.

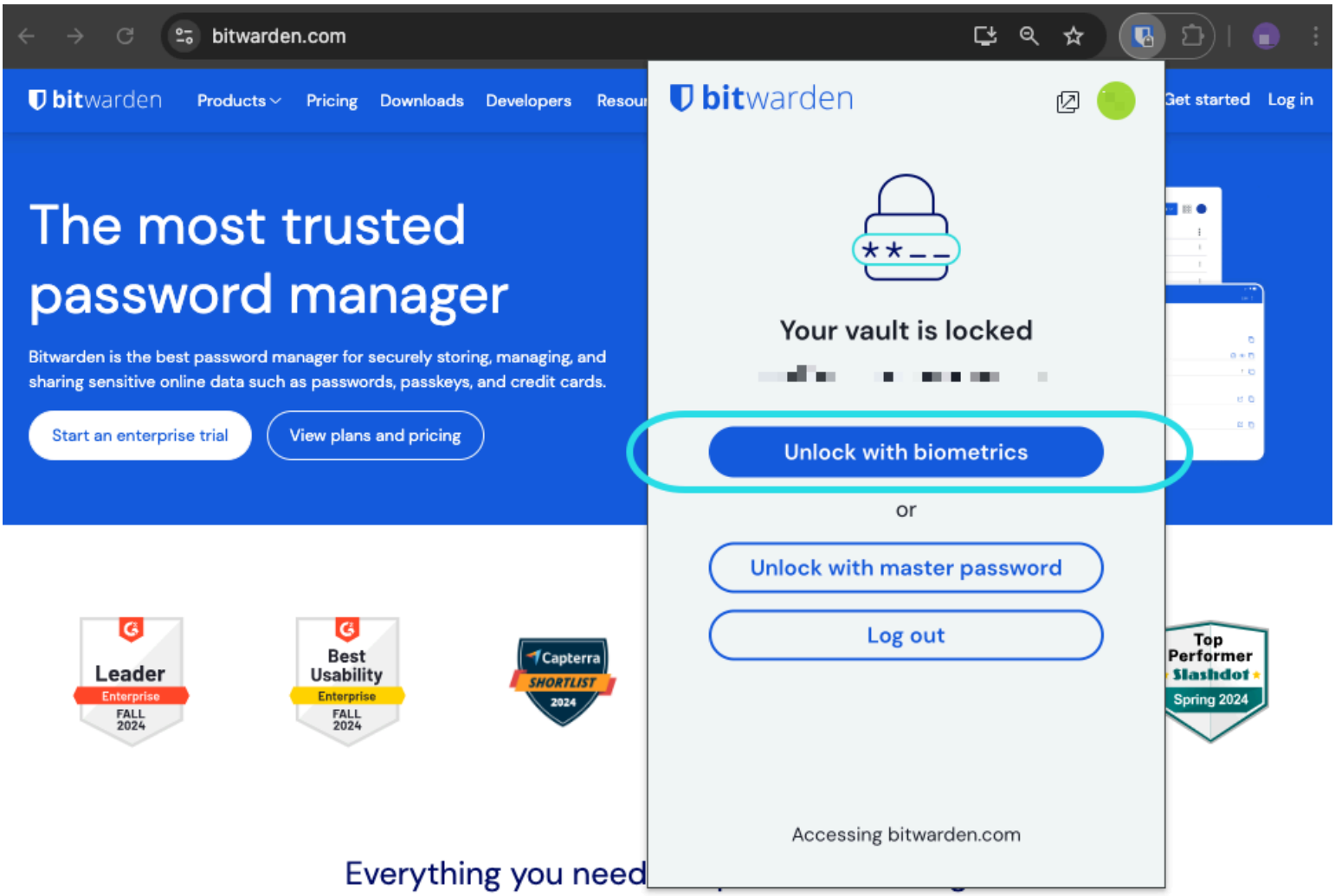
5. Select **Account security** and check the **Unlock with biometrics** box.

   > **Tip**
   >
   > You may be prompted at this stage to allow Bitwarden to `communicate with cooperating native applications`. This permission is safe, but **optional** and solely enables the browser extension to communicate with desktop as described above.

   You will be prompted by your desktop app to input your biometric. Doing so will complete the initial setup procedure. If you have opted to require verification (**step two**), you will need to approve a fingerprint validation check.

6. If you want the browser extension to automatically prompt for your biometric input when launched, make sure the **Prompt for biometrics on launch** option is on.

The browser extension will automatically prompt for your biometric when you open it. If you turn the prompt option off (**step six**), use the **Unlock with biometrics** button on the Unlock screen:



Browser extension unlock with biometrics

> **Tip**
> The Bitwarden desktop app must be logged in and running in order to use unlock with biometrics for a browser extension.

Disabled pending master password verification

If you get a message reporting that biometric unlock is disabled for auto-fill pending verification of your master password:

1. Temporarily turn off auto-fill in Bitwarden.
2. Re-enable biometrics in Bitwarden.
3. Turn auto-fill back on in Bitwarden.

Förstå upplåsning vs. logga in

För att förstå varför upplåsning och inloggning inte är samma sak är det viktigt att komma ihåg att Bitwarden aldrig lagrar okrypterad data på sina servrar. **När ditt valv varken är upplåst eller inloggat**, finns dina valvdata bara på servern i sin krypterade form.

Loggar in

Att logga in på Bitwarden hämtar krypterad valvdata och dekrypterar valvdata lokalt på din enhet. I praktiken betyder det två saker:

1. Om du loggar in måste du alltid använda ditt huvudlösenord eller logga in med enheten för att få tillgång till kontokrypteringsnyckeln som kommer att behövas för att dekryptera valvdata.

   Detta steg är också där alla aktiverade tvåstegsinloggningsmetoder kommer att krävas.

2. Inloggning kräver alltid att du är ansluten till internet (eller, om du är självvärd, ansluten till servern) för att ladda ner det krypterade valvet till disken, som sedan kommer att dekrypteras i din enhets minne.

Låser upp

Upplåsning kan endast göras när du redan är inloggad. Detta betyder, enligt avsnittet ovan, har din enhet **krypterad** valvdata lagrad på disken. I praktiken betyder det två saker:

1. Du behöver inte specifikt ditt huvudlösenord. Medan ditt huvudlösenord kan användas för att låsa upp ditt valv, så kan andra metoder som PIN-koder och biometri.

   > **Note**
   >
   > When you setup a PIN or biometrics, a new encryption key derived from the PIN or biometric factor is used to encrypt the account encryption key, which you will have access to by virtue of being logged in, and stored on disk[a].
   >
   > **Unlocking** your vault causes the PIN or biometric key to decrypt the account encryption key in memory. The decrypted account encryption key is then used to decrypt all vault data in memory.
   >
   > **Locking** your vault causes all decrypted vault data, including the decrypted account encryption key, to be deleted.
   >
   > [a] – If you use the **Lock with master password on restart** option, this key is only stored in memory rather than on disk.

2. Du behöver inte vara ansluten till internet (eller, om du är självvärd, ansluten till servern).