

KONTOEINSTELLUNGEN > ANMELDEN & ENTSPERREN

Mit biometrischen Daten entsperren

Ansicht im Hilfezentrum:
<https://bitwarden.com/help/biometrics/>

Mit biometrischen Daten entsperren

Bitwarden kann so konfiguriert werden, dass Biometrie als Methode zum Entsperren Ihres Tresors akzeptiert wird.

Biometrie kann **nur zum Entsperren** Ihres Tresors verwendet werden, Sie müssen immer noch Ihr Master-Passwort verwenden oder sich mit dem Gerät anmelden, und jede aktivierte [Zwei-Schritt-Anmelde-Methode](#), wenn Sie sich **anmelden**. Entsperren mit Biometrie ist keine Funktion, die als passwortloses Anmelden konzipiert wurde. Wenn Sie den Unterschied nicht kennen, sehen Sie [Verstehen von entsperren vs. anmelden](#).

Tip

Biometrische Funktionen sind Teil der integrierten Sicherheit in Ihrem Gerät und/oder Betriebssystem. Bitwarden nutzt native APIs, um diese Validierung durchzuführen, und daher **erhält Bitwarden keine Biometrie-Informationen** vom Gerät.

Biometrie zum Entsperren aktivieren

Entsperren mit Biometrie kann für Bitwarden auf Mobilgeräten, Desktop und Browser-Erweiterungen aktiviert werden:

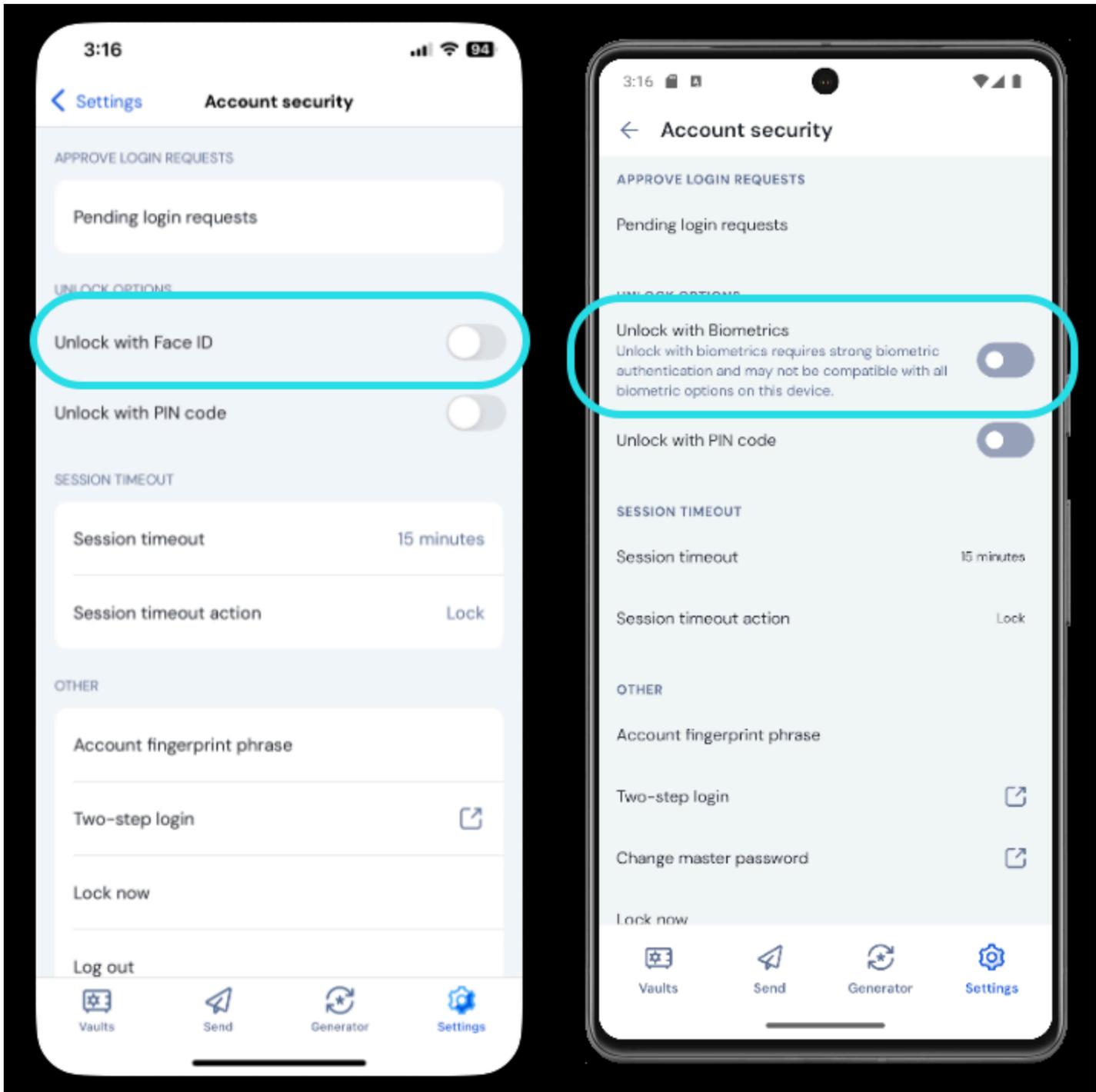
⇒ Handy

Auf dem Handy aktivieren

Die Entsperrung mit Biometrie wird für Android (Google Play oder FDroid) über [Fingerabdruck-Entsperrung](#) oder [Gesichtserkennung](#) und für iOS über [Touch ID](#) und [Face ID](#) unterstützt.

So aktivieren Sie die Entsperrung mit Biometrie für Ihr Mobilgerät:

1. Vergewissern Sie sich in den Einstellungen Ihres Geräts (z. B. in der  **Einstellungs**-App bei iOS), dass Ihre biometrische Methode aktiviert ist.
2. Öffnen Sie in Ihrer Bitwarden-App die Registerkarte  **Einstellungen**.
3. Scrollen Sie nach unten zum Abschnitt "Sicherheit" und tippen Sie auf die biometrische Option, die Sie aktivieren möchten. Was auf diesem Bildschirm verfügbar ist, hängt von den Hardware-Funktionen Ihres Geräts ab und davon, was Sie beispielsweise aktiviert haben – siehe (**Schritt eins**):



Face ID auf iOS aktivieren

Wenn Sie auf die Option tippen, werden Sie aufgefordert, Ihr biometrisches Merkmal (z. B. Gesicht oder Daumenabdruck) zu erfassen. Eine grüne Statusanzeige "Aktiviert" (siehe Abbildung oben) zeigt an, dass die Entsperrung mit biometrischen Daten erfolgreich aktiviert wurde.

Deaktiviert bis zur Überprüfung des Master-Passworts

Wenn Sie eine Meldung erhalten, dass die biometrische Entsperrung für das automatische Ausfüllen bis zur Überprüfung Ihres Master-Passworts deaktiviert ist:

1. Deaktivieren Sie vorübergehend das automatische Ausfüllen in Bitwarden.
2. Aktivieren Sie die Verwendung biometrischer Daten in Bitwarden erneut.
3. Schalten Sie Autofill in Bitwarden wieder ein.

⇒PC

Auf dem PC aktivieren

Das Entsperren mit Biometrie wird für Windows über [Windows Hello](#) mit PIN, Gesichtserkennung oder anderer Hardware, welche die [biometrischen Anforderungen von Windows Hello](#) erfüllt, und für macOS über [Touch ID](#) unterstützt.

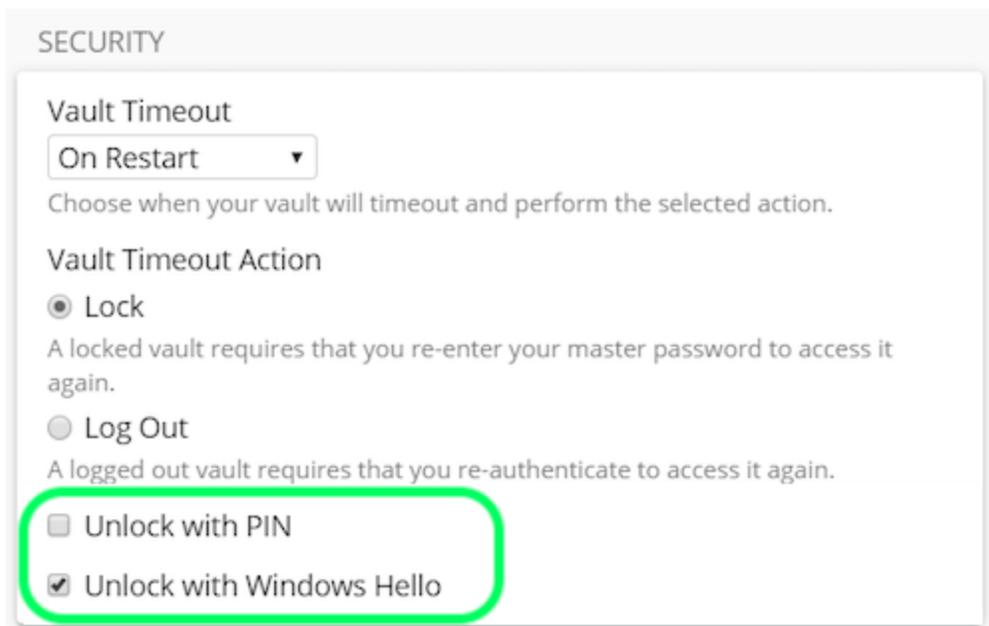
Die Entsperrung mit biometrischen Merkmalen wird [für jedes in der PC-Anwendung angemeldete Konto separat eingestellt](#). So aktivieren Sie die Entsperrung mit biometrischen Daten:

1. Stellen Sie in den systemeigenen Einstellungen Ihres Geräts (z. B. in den **Systemeinstellungen** von macOS) sicher, dass Ihre biometrische Methode aktiviert ist.

💡 Tip

Windows-Benutzer müssen möglicherweise [Microsoft Visual C++ Redistributable](#) installieren, bevor Windows Hello in den PC-Einstellungen aktiviert werden kann.

2. Öffnen Sie in Ihrer Bitwarden-App Ihre Einstellungen (unter Windows: **Datei** → **Einstellungen**; unter macOS: **Bitwarden** → **Einstellungen**).
3. Scrollen Sie nach unten zum Abschnitt Sicherheit und wählen Sie die biometrische Option, die Sie aktivieren möchten. Was auf diesem Bildschirm verfügbar ist, hängt von den Hardware-Fähigkeiten Ihres Geräts ab und davon, was Sie zum Beispiel aktiviert haben (siehe **Schritt eins**):



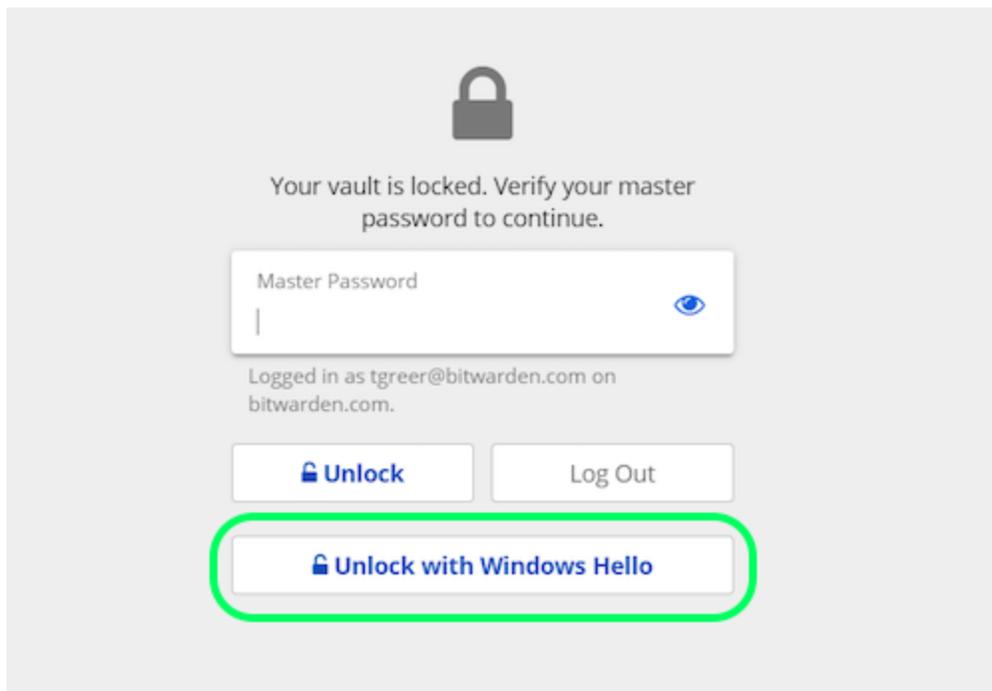
Entsperren mit Windows Hello

4. Optional können Sie entweder die Option **Passwort (oder PIN) beim Start der App anfordern** oder **Fragen Sie nach Biometrie beim Start der App** auswählen, um festzulegen, wie Ihre Desktop-App sich verhält, wenn Sie die App starten.

💡 Tip

Wenn Sie Windows verwenden, empfiehlt Bitwarden die Verwendung von **Passwort (oder PIN) bei erstem Login nach dem Start erforderlich**, um die Sicherheit zu maximieren.

Unabhängig von der Auswahl der automatischen **Eingabeaufforderung** wird auf dem **Entsperrungsbildschirm** eine neue Schaltfläche zum Entsperren des Tresors angezeigt:



Entsperren mit Windows Hello

⇒ Browser-Erweiterungen

Über Biometrie in Browser-Erweiterungen

Das Entsperren mit Biometrie wird für Browser-Erweiterungen durch eine Integration mit der Bitwarden PC-Anwendung unterstützt. In der Praxis bedeutet dies:

1. **Für alle Browser-Erweiterungen** müssen Sie die Entspernung mit Biometrie auf dem PC aktivieren, bevor Sie fortfahren. **Für alle Browser außer Safari** muss die Bitwarden PC-Anwendung eingeloggt sein und laufen, um das Entsperren mit Biometrie für eine Browser-Erweiterung zu nutzen.
2. Browser-Erweiterungen unterstützen die gleichen biometrischen Optionen wie der PC: für Windows über [Windows Hello](#) mit PIN, Gesichtserkennung oder *andere Hardware, welche die biometrischen Anforderungen von Windows Hello erfüllt*, und für macOS über [Touch ID](#).

Zwei Dinge sind zu beachten, bevor Sie die Integration aktivieren: **Berechtigungen** und **Unterstützung** (siehe unten):

Berechtigungen

Um diese Integration zu ermöglichen, werden Browser-Erweiterungen **außer Safari** Sie bitten, eine neue Berechtigung zu akzeptieren, damit Bitwarden **mit kooperierenden nativen Anwendungen kommunizieren** kann. Diese Erlaubnis ist sicher, aber **optional**, und ermöglicht die Integration, die erforderlich ist, um das Entsperren mit Biometrie zu ermöglichen.

Wenn Sie diese Berechtigung ablehnen, können Sie die Browser-Erweiterung wie gewohnt verwenden, ohne die Funktion zum Entsperren mit biometrischen Merkmalen.

Unterstützung

Das Entsperren mit biometrischen Daten wird bei Erweiterungen für **Chromium-basierten Browsern** (Chrome, Edge, Opera, Brave und andere), Firefox 87 und höher sowie Safari 14 und höher unterstützt. Freischalten mit Biometrie wird **derzeit nicht unterstützt** für:

- Firefox ESR (Firefox 87 und höher funktioniert).
- Microsoft App Store PC-Anwendungen (eine quergeladene Desktop-Anwendung für Windows, verfügbar unter bitwarden.com/download, funktioniert problemlos).
- Quergeladene Desktop-Anwendungen für MacOS (eine App Store Desktop-Anwendung funktioniert problemlos).

Biometrie aktivieren für Browser-Erweiterungen

So aktivieren Sie das Entsperren mit biometrischen Daten für Ihre Browser-Erweiterung:

💡 Tip

Biometrie (Windows Hello oder Touch ID) muss in Ihrer Desktop-App aktiviert sein, bevor Sie fortfahren. Wenn Sie die Option Windows Hello in Ihrer Desktop-App nicht sehen, müssen Sie möglicherweise den [Microsoft Visual C++ Redistributable](#) installieren. Zusätzlich können Sie, **wenn Sie Safari verwenden**, direkt zu **Schritt 4** springen.

1. Navigieren Sie in Ihrer Bitwarden PC-Anwendung zu den Einstellungen (unter Windows; **Datei** → **Einstellungen**; unter macOS: **Bitwarden** → **Einstellungen**).
2. Scrollen Sie nach unten zum Abschnitt Optionen und aktivieren Sie das Kontrollkästchen **Browserintegration zulassen**.

📘 Note

Aktivieren Sie optional die Option **Verifizierung für Browser-Integration verlangen**, um einen einmaligen Fingerabdruck-Verifizierungsschritt zu verlangen, wenn Sie die Integration aktivieren.

3. Navigieren Sie in Ihrem Browser zum Erweiterungsmanager (z. B. <chrome://extensions> oder <brave://extensions>), öffnen Sie Bitwarden und aktivieren Sie die Option **Zugriff auf Datei-URLs zulassen**.
Nicht alle Browser benötigen, dass dies eingeschaltet wird, also fühlen Sie sich frei, diesen Schritt zu überspringen und nur dann darauf zurückzukommen, wenn das restliche Verfahren nicht funktioniert.
4. Öffnen Sie in Ihrer Browsererweiterung die Registerkarte  **Einstellungen**.
5. Scrollen Sie nach unten zum Abschnitt Sicherheit und aktivieren Sie das Kontrollkästchen **Mit Biometrie entsperren**.

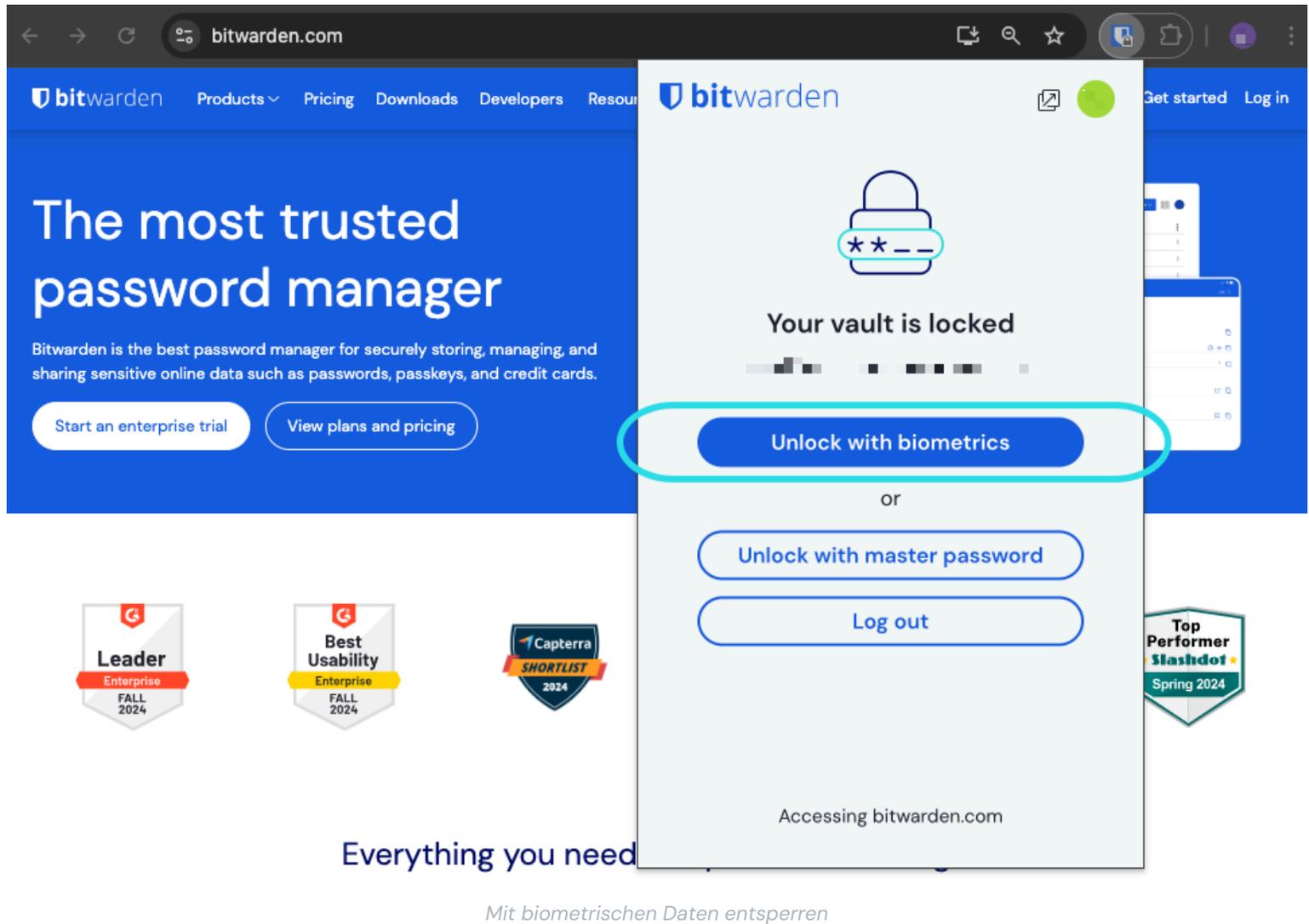
💡 Tip

Möglicherweise werden Sie zu diesem Zeitpunkt aufgefordert, **Bitwarden die Kommunikation mit kooperierenden nativen Anwendungen zu gestatten**. Diese Erlaubnis ist sicher, aber **optional** und ermöglicht lediglich der Browsererweiterung, wie oben beschrieben mit dem Desktop zu kommunizieren.

Sie werden von Ihrer PC-Anwendung aufgefordert, Ihr biometrisches Merkmal zu erfassen. Damit ist der Einrichtungsvorgang abgeschlossen. Wenn Sie sich dafür entschieden haben, eine Verifizierung zu verlangen (**Schritt zwei**), müssen Sie einer Überprüfung der Fingerabdrücke zustimmen.

6. Wenn Sie möchten, dass die Browser-Erweiterung beim Start automatisch zur Eingabe Ihrer biometrischen Daten auffordert, stellen Sie sicher, dass die Option **Beim Start nach biometrischen Daten fragen** aktiviert ist.

Die Browser-Erweiterung fragt automatisch nach Ihren biometrischen Daten, wenn Sie sie öffnen. Wenn Sie die entsprechende Option deaktivieren (**Schritt sechs**), verwenden Sie die Schaltfläche **Mit biometrischen Daten entsperren** auf dem Bildschirm Entsperren:



💡 Tip

Ihre Desktop-App muss angemeldet, aber nicht entsperret sein, um eine Browser-Erweiterung mit biometrischen Merkmalen zu entsperren.

Deaktiviert bis zur Überprüfung des Master-Passworts

Wenn Sie eine Meldung erhalten, dass die biometrische Entspernung für das automatische Ausfüllen bis zur Überprüfung Ihres Master-Passworts deaktiviert ist:

1. Deaktivieren Sie vorübergehend das automatische Ausfüllen in Bitwarden.
2. Aktivieren Sie die Verwendung biometrischer Daten in Bitwarden erneut.
3. Schalten Sie Autofill in Bitwarden wieder ein.

Verständnis entsperren vs. anmelden

Um zu verstehen, warum entsperren und anmelden nicht dasselbe sind, ist es wichtig zu bedenken, dass Bitwarden **niemals unverschlüsselte Daten** auf seinen Servern speichert. **Wenn Ihr Tresor weder entsperrt noch angemeldet ist**, existieren Ihre Tresor-Daten nur in ihrer **verschlüsselten Form** auf dem Server.

Anmelden

Anmelden bei Bitwarden ruft die verschlüsselten Tresor-Daten ab und entschlüsselt die Tresor-Daten lokal auf Ihrem Gerät. In der Praxis bedeutet das zwei Dinge:

1. Die Anmeldung erfordert immer die Verwendung Ihres Master-Passworts oder **Anmeldung mit Gerät**, um Zugang zum **Konto-Verschlüsselungsschlüssel** zu erhalten, der zum Entschlüsseln der Tresor-Daten benötigt wird.

In dieser Phase werden auch **alle aktivierten zweistufigen Zugangsdaten-Methoden** benötigt.

2. Die Anmeldung erfordert immer eine Internetverbindung (oder, wenn Sie selbst hosten, eine Verbindung zum Server), um den verschlüsselten Tresor auf die Festplatte herunterzuladen, der anschließend im Speicher Ihres Geräts entschlüsselt wird.

Entsperren

Entsperren kann nur durchgeführt werden, wenn Sie bereits angemeldet sind. Das bedeutet, laut dem oben genannten Abschnitt, dass Ihr Gerät **verschlüsselte** Tresor-Daten auf der Festplatte gespeichert hat. In der Praxis bedeutet das zwei Dinge:

1. Sie benötigen nicht speziell Ihr Master-Passwort. Während Ihr Master-Passwort *verwendet werden kann*, um Ihren Tresor zu entsperren, können dies auch andere Methoden wie PIN-Codes und Biometrie.

Note

Wenn Sie eine PIN oder Biometrie einrichten, wird ein neuer, von der PIN oder dem biometrischen Faktor abgeleiteter Verschlüsselungsschlüssel verwendet, um den **Konto-Verschlüsselungsschlüssel** zu verschlüsseln, auf den Sie Zugriff haben, weil Sie angemeldet sind, und der auf der Festplatte gespeichert wird^a.

Entsperren Ihres Tresors führt dazu, dass der PIN oder der biometrische Schlüssel den Verschlüsselungsschlüssel des Kontos im Speicher entschlüsselt. Der entschlüsselte Verschlüsselungsschlüssel des Kontos wird dann verwendet, um alle Tresor-Daten im Speicher zu entschlüsseln.

Sperrn Ihres Tresors führt dazu, dass alle entschlüsselten Tresor-Daten, einschließlich des entschlüsselten Konto-Verschlüsselungsschlüssels, gelöscht werden.

^a - Wenn Sie die Option **Beim Neustart mit Master-Passwort sperren** verwenden, wird dieser Schlüssel nur im Speicher und nicht auf der Festplatte gespeichert.

2. Sie müssen nicht mit dem Internet verbunden sein (oder, wenn Sie selbst hosten, mit dem Server verbunden sein).