bitwarden | Hilfezentrum Artikel

KONTOEINSTELLUNGEN > 2FA >

Zwei-Schritt-Zugangsdaten über FIDO2 WebAuthn

Ansicht im Hilfezentrum:
https://bitwarden.com/help/setup-two-step-login-fido/

Zwei-Schritt-Zugangsdaten über FIDO2 WebAuthn

Zweistufige Zugangsdaten mit FIDO2 WebAuthn-Zertifikaten sind für alle Bitwarden-Benutzer kostenlos verfügbar.

Alle FIDO2 WebAuthn-zertifizierten Anmeldeinformationen können verwendet werden, einschließlich Sicherheitsschlüssel wie YubiKeys, SoloKeys und Nitrokeys, sowie native Biometrie-Optionen wie Windows Hello und Touch ID.

> **Tip**
>
> Neue U2F-nur Schlüssel **können nicht** zu einem Konto hinzugefügt werden. Bestehende FIDO U2F Sicherheitsschlüssel können jedoch weiterhin verwendet werden und werden als **(Migriert von FIDO)** im Zwei-Schritt-Zugangsdaten → FIDO2 WebAuthn verwalten Dialog gekennzeichnet.

FIDO2 WebAuthn ist mit den meisten Bitwarden-Anwendungen kompatibel. Wenn Sie eine Version verwenden möchten, die dies nicht unterstützt, stellen Sie sicher, dass Sie eine alternative Zwei-Schritt-Zugangsdaten-Methode aktivieren. Unterstützte Anwendungen beinhalten:

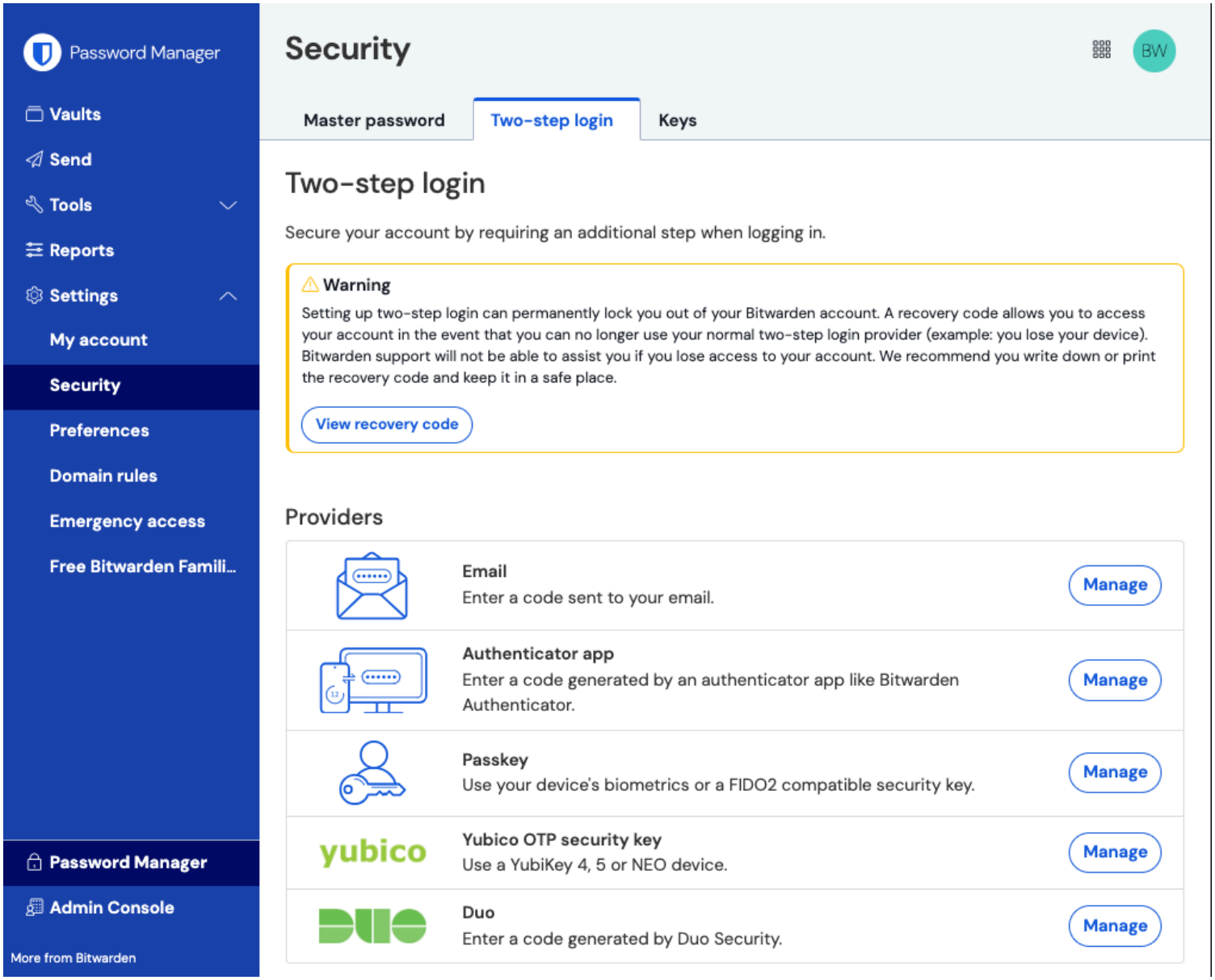
- **Web-Tresor** auf einem Gerät mit einem FIDO2-unterstützten Browser.
- **Browser-Erweiterungen** für einen FIDO2-unterstützten Browser.
- **Desktop-Apps** auf Windows 10 und höher.
- **Mobile-apps** für Android und iOS 13.3+ mit einem FIDO2-unterstützten Browser.

FIDO2-WebAuthn-Einrichtung

Um die Zwei-Schritt-Zugangsdaten mit FIDO2 WebAuthn zu aktivieren:

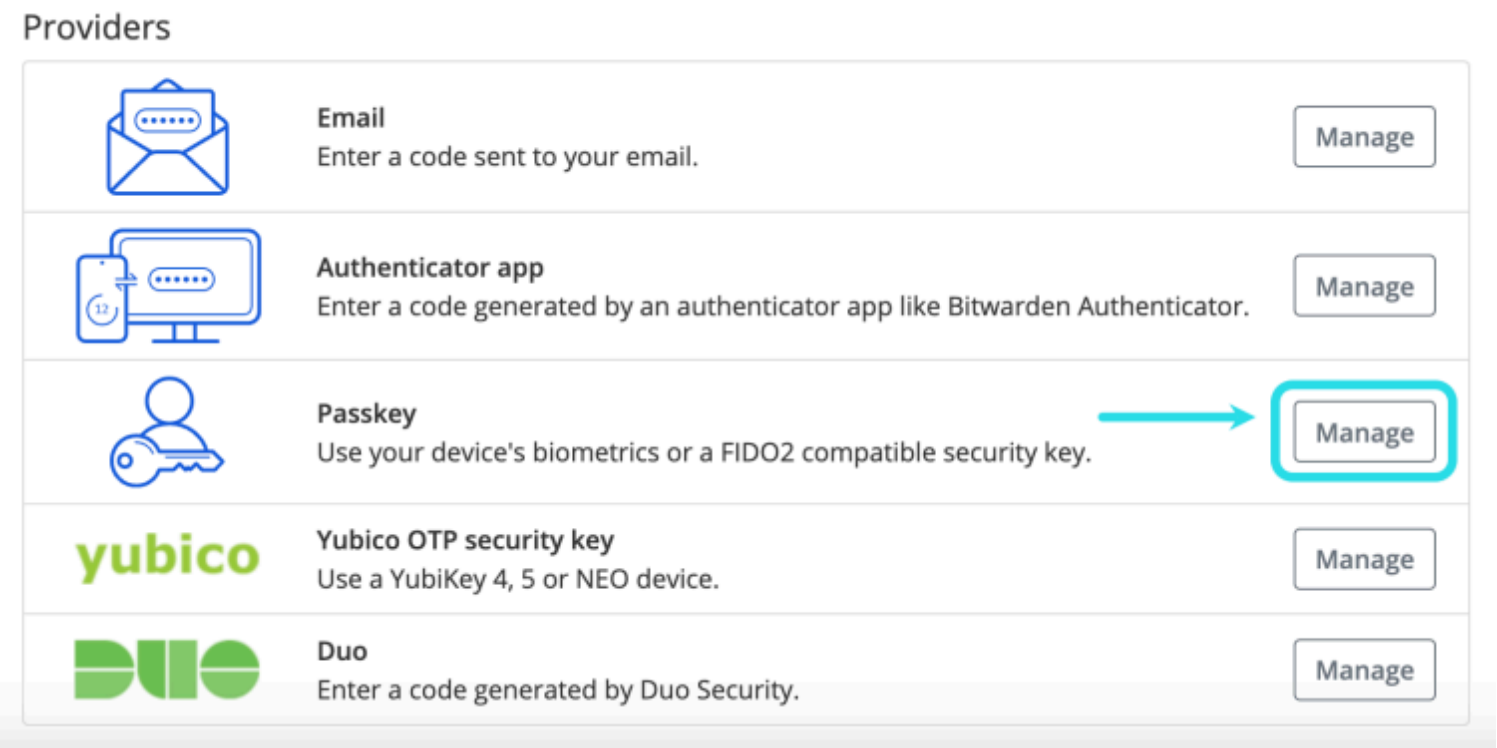
> **⚠ Warning**
>
> **Wenn Sie den Zugriff auf Ihr Gerät für die zweistufige Anmeldung verlieren, können Sie dauerhaft aus Ihrem Tresor ausgesperrt werden**, es sei denn, Sie notieren sich Ihren Wiederherstellungscode für die zweistufige Anmeldung und bewahren ihn an einem sicheren Ort auf oder haben eine alternative Methode für die zweistufige Anmeldung aktiviert und verfügbar.
>
> Rufen Sie Ihren Wiederherstellungscode sofort nach der Aktivierung einer beliebigen Methode auf dem Bildschirm für die **zweistufige Anmeldung** ab.

1. Melden Sie sich bei der Bitwarden-Web-App an.
2. Wählen Sie **Einstellungen** → **Sicherheit** → **Zwei-Schritt-Zugangsdaten** aus der Navigation:



Authentifizierungs-App verwalten

3. Finden Sie die Option **FIDO2 WebAuthn** und wählen Sie die Schaltfläche **Verwalten** aus.



Wählen Sie die Schaltfläche Verwalten

Sie werden aufgefordert, Ihr Master-Passwort einzugeben, um fortzufahren.

4. Geben Sie Ihrem Sicherheitsschlüssel einen freundlichen **Namen**.

5. Stecken Sie den Sicherheitsschlüssel in den USB-Anschluss Ihres Geräts und wählen Sie **Schlüssel Lesen**. Wenn Ihr Sicherheitsschlüssel einen Knopf hat, berühren Sie ihn.

> **ⓘ Note**
>
> Einige Geräte, einschließlich solcher mit Windows Hello oder macOS-Geräten, die Passkeys unterstützen, sind native FIDO2-Authentifizierer, die diese Optionen standardmäßig anbieten. Wenn Sie einen Sicherheitsschlüssel oder einen anderen Authentifizierer registrieren möchten, müssen Sie möglicherweise eine **Versuchen Sie es auf eine andere Weise**, **Andere Optionen** oder **Abbrechen** Schaltfläche auswählen, um Ihre anderen Optionen zu öffnen.

6. Wählen Sie **Speichern**. Eine grüne `Aktiviert` Nachricht zeigt an, dass die zweistufige Anmeldung mit FIDO2 WebAuthn erfolgreich aktiviert wurde und Ihr Schlüssel wird mit einem grünen Häkchen erscheinen (✓).

7. Wählen Sie die **Schließen** Schaltfläche und bestätigen Sie, dass die **FIDO2 WebAuthn** Option jetzt aktiviert ist, wie durch ein grünes Kontrollkästchen angezeigt (✓).

Wiederholen Sie diesen Vorgang, um bis zu 5 FIDO2 WebAuthn Sicherheitsschlüssel zu Ihrem Konto hinzuzufügen.

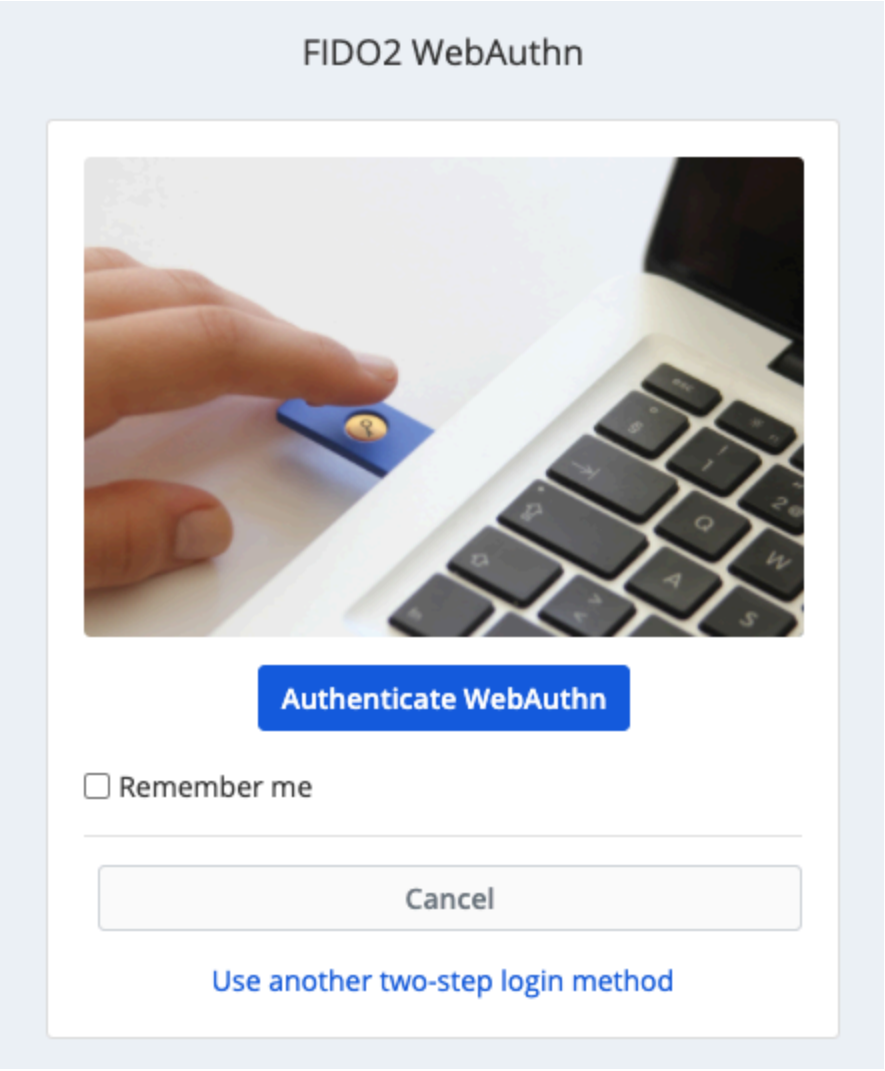
> **Note**
>
> Wir empfehlen Ihnen, die aktive Registerkarte des Web-Tresors geöffnet zu lassen, bevor Sie mit dem Testen der zweistufigen Anmeldung fortfahren, falls etwas falsch konfiguriert wurde. Sobald Sie sich vergewissert haben, dass es funktioniert, loggen Sie sich von all Ihren Bitwarden-Anwendungen aus, um jeweils die zweistufige Anmeldung zu verlangen. Sie werden dann automatisch ausgeloggt.

Verwenden Sie FIDO2 WebAuthn

Es wird angenommen, dass **FIDO2 WebAuthn** Ihre höchstpriorisierte-aktivierte-methode ist. Um auf Ihren Tresor mit einem FIDO2 WebAuthn Gerät zuzugreifen:

1. Melden Sie sich an Ihrem Bitwarden-Tresor an und geben Sie Ihre E-Mail-Adresse und Ihr Master-Passwort ein.

   Sie werden aufgefordert, Ihren Sicherheitsschlüssel in den USB-Anschluss Ihres Geräts einzustecken. Wenn es einen Knopf hat, berühre ihn.



FIDO2-Aufforderung

> **Tip**
>
> Aktivieren Sie das Kontrollkästchen **Angemeldet bleiben**, um Ihr Gerät für 30 Tage zu speichern. Wenn Ihr Gerät angemeldet bleibt, müssen Sie den zweistufigen Anmeldeschritt 30 Tage lang nicht mehr durchführen.

Sie müssen Ihre sekundäre Zwei-Schritt-Zugangsdaten-Einrichtung nicht abschließen, um Ihren Tresor zu **entsperren**, sobald Sie angemeldet sind. Für Hilfe bei der Konfiguration von abmelden vs. sperren Verhalten, siehe Tresor-Timeout-Optionen.

NFC-Fehlerbehebung

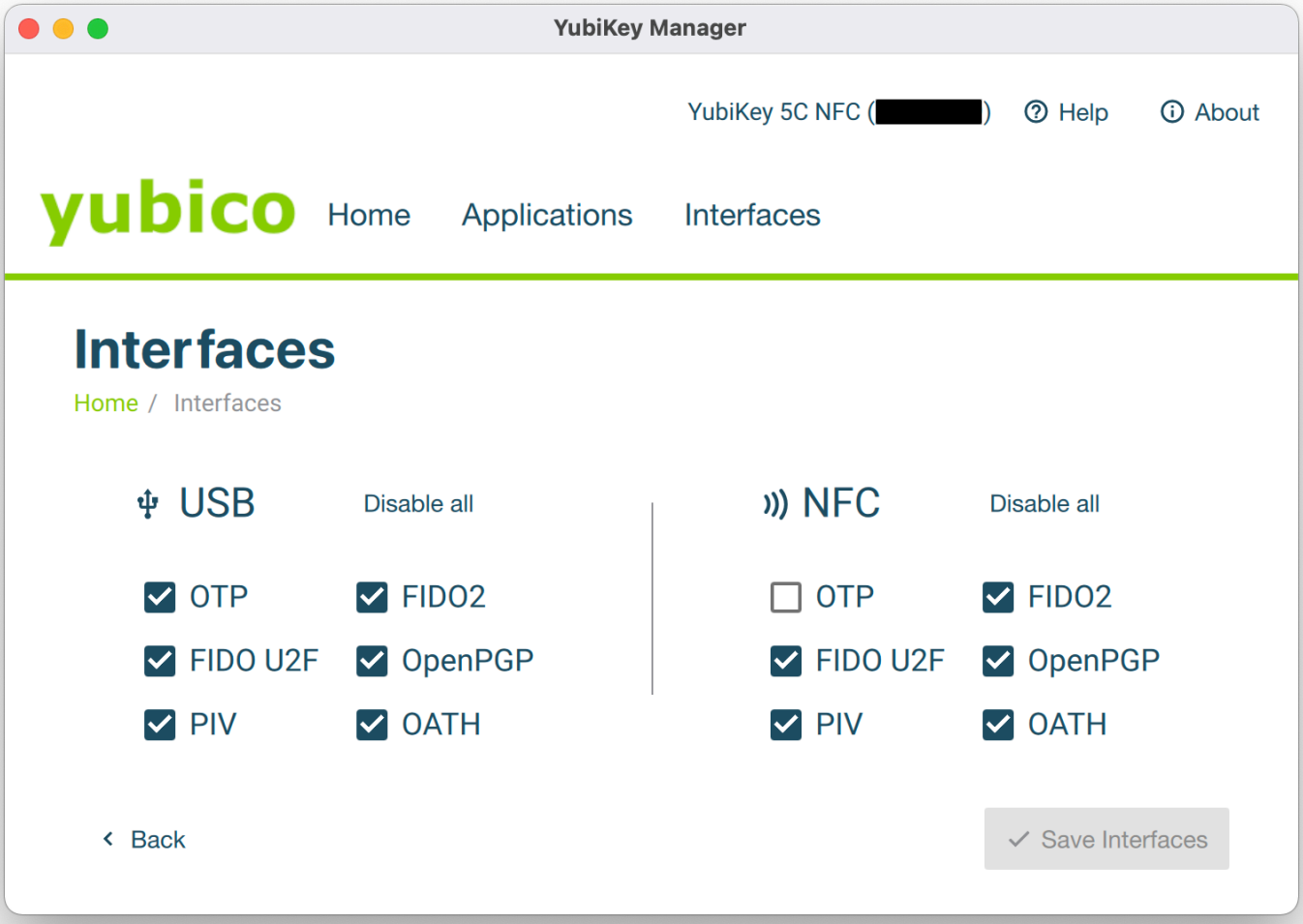
Wenn Sie einen FIDO2-Authentifikator mit NFC-Funktionalität wie einen YubiKey oder einen anderen Hardware-Sicherheitsschlüssel verwenden, müssen Sie möglicherweise üben, den NFC-Leser in Ihrem Gerät zu finden, da verschiedene Geräte NFC-Leser an unterschiedlichen physischen Standorten haben (zum Beispiel oben am Telefon vs. unten am Telefon oder vorne vs. hinten).

> **Tip**
>
> Hardware-Sicherheitsschlüssel haben in der Regel einen physischen Stecker, der in Fällen, in denen NFC schwierig ist, zuverlässiger funktioniert.

Fehlerbehebung-YubiKey-NFC

Auf mobilen Geräten kann es vorkommen, dass Ihr YubiKey zweimal hintereinander gelesen wird. Sie werden wissen, dass dies passiert ist, wenn der Browser Ihres Geräts die YubiKey OTP-Website öffnet (`https://demo/yubico.com/yk`) und wenn Ihr Gerät mehrmals vibriert, um mehrere NFC-Lesungen zu signalisieren.

Um dies zu lösen, verwenden Sie die Anwendung YubiKey Manager, um die **NFC** → **OTP** Schnittstelle für Ihren Schlüssel zu deaktivieren:



YubiKey-Verwalter

⚠ Warning

Das Deaktivieren von **NFC** → **OTP** verhindert, dass Sie Zwei-Schritt-Zugangsdaten über YubiKey (OTP) über NFC mit diesem Schlüssel verwenden können. In diesem Szenario wird OTP über USB wie erwartet funktionieren.