KONTOEINSTELLUNGEN > ANMELDEN & ENTSPERREN

Mit Passkeys Beta anmelden

Mit Passkeys Beta anmelden

> **Note**
> Mit Passkeys anmelden ist derzeit in der Beta.

Passkeys können verwendet werden, um sich bei Bitwarden anzumelden, als Alternative zur Verwendung Ihres Master-Passworts und Ihrer E-Mail-Adresse. Passwörter, die zum Anmelden bei Bitwarden verwendet werden, erfordern eine Benutzerverifizierung, was bedeutet, dass Sie etwas wie einen biometrischen Faktor oder einen Sicherheitsschlüssel verwenden müssen, um erfolgreich Zugang zu Ihrem Passwort zu erhalten.

Die Anmeldung mit einem Passschlüssel umgeht die Bitwarden-Zwei-Schritt-Anmeldung, jedoch können nur PRF-fähige Browser- und Passschlüssel-Kombinationen verwendet werden, um die Anmeldung mit Passschlüsseln für die Tresor-Entschlüsselung einzurichten. Passwörter, die PRF nicht verwenden, erfordern, dass Sie Ihr Master-Passwort eingeben, nachdem Sie sich angemeldet haben, um Ihren Tresor zu entschlüsseln.

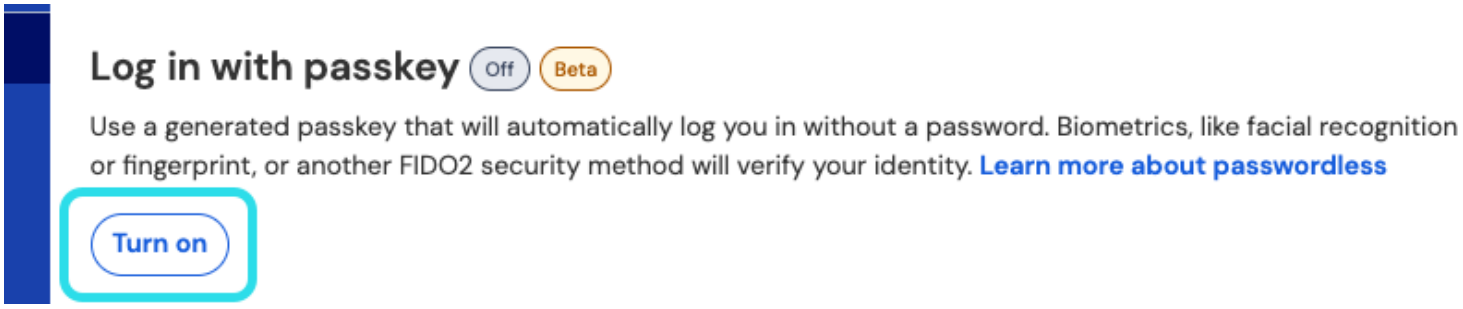
Passkeys können derzeit verwendet werden, um sich bei der Bitwarden-Web-App anzumelden, und die Unterstützung für andere Client-Anwendungen ist für eine zukünftige Veröffentlichung geplant.

> **Note**
> Die Anmeldung mit Passkeys kann nicht von Mitgliedern einer Organisation verwendet werden, die die Richtlinie Erfordert Einzelanmeldungs-Authentifizierung, SSO mit vertrauenswürdigen Geräten oder Key Connector verwendet.

Erstellen Sie einen Passschlüssel

Sie können sich jederzeit mit bis zu 5 Passwörtern anmelden. Um einen Passschlüssel zu erstellen, den Sie verwenden können, um sich bei Bitwarden anzumelden:

1. In der Web-App wählen Sie **Einstellungen** → **Mein Konto** aus der Navigation:
2. Vom Menü Einstellungen aus wählen Sie die **Sicherheits** Seite und den **Master-Passwort** Tab.
3. Im Abschnitt Anmelden mit Passwort, wählen Sie **Einschalten** oder, wenn Sie bereits ein Passwort eingerichtet haben, **Neues Passwort**. Sie werden aufgefordert, Ihr Master-Passwort einzugeben:



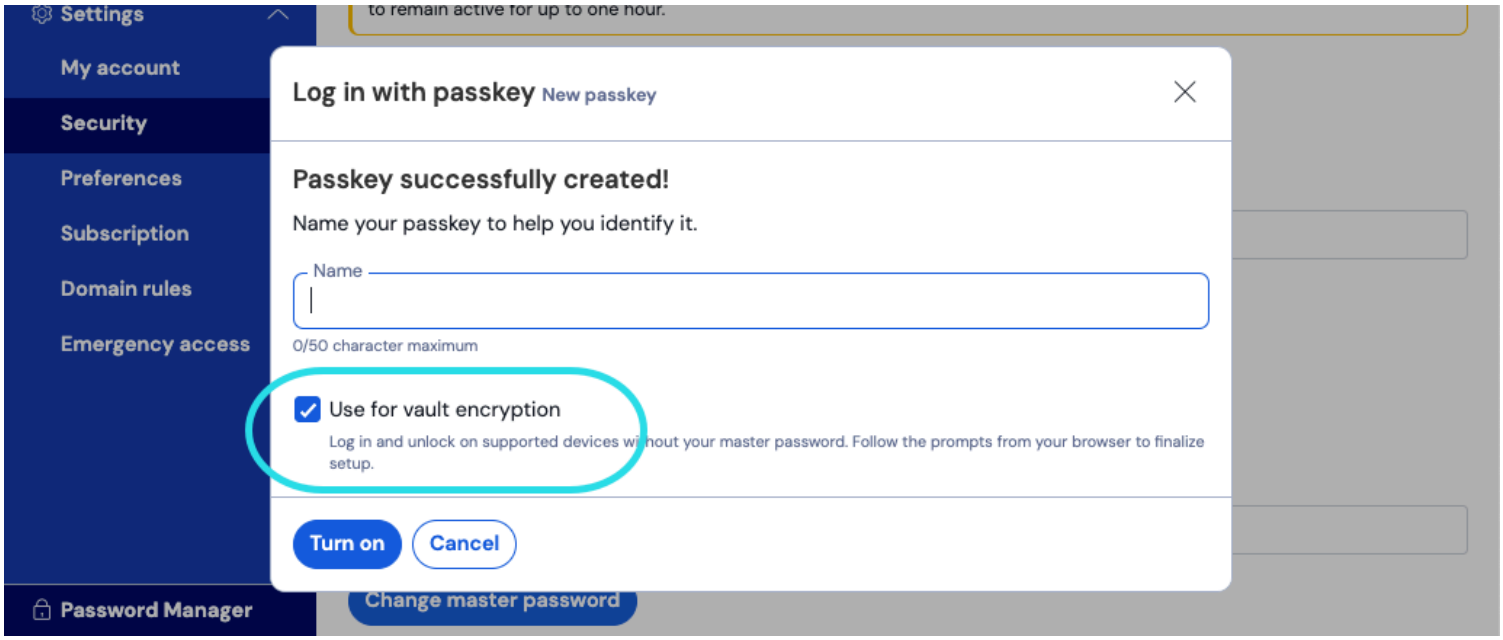
Aktivieren Sie die Anmeldung mit Zugangsdaten

4. Folgen Sie den Aufforderungen Ihres Browsers, um einen FIDO2-Passschlüssel zu erstellen. Sie können die Benutzerverifizierung mit einem Faktor wie einer Biometrie abschließen oder indem Sie eine PIN erstellen.

   Während dieses Verfahrens müssen Sie möglicherweise einen Standard-Authentifizierer abbrechen, den Ihr Browser verwenden möchte, zum Beispiel wenn Sie einen Hardware-Sicherheitsschlüssel auf einem macOS-Gerät verwenden möchten, das Touch ID priorisiert.

5. Geben Sie Ihrem Passwort einen **Namen**.

6. Wenn Sie Ihren Passkey nicht für die Tresor-Verschlüsselung und -Entschlüsselung verwenden möchten, deaktivieren Sie das Kontrollkästchen **Für Tresor-Verschlüsselung verwenden**:



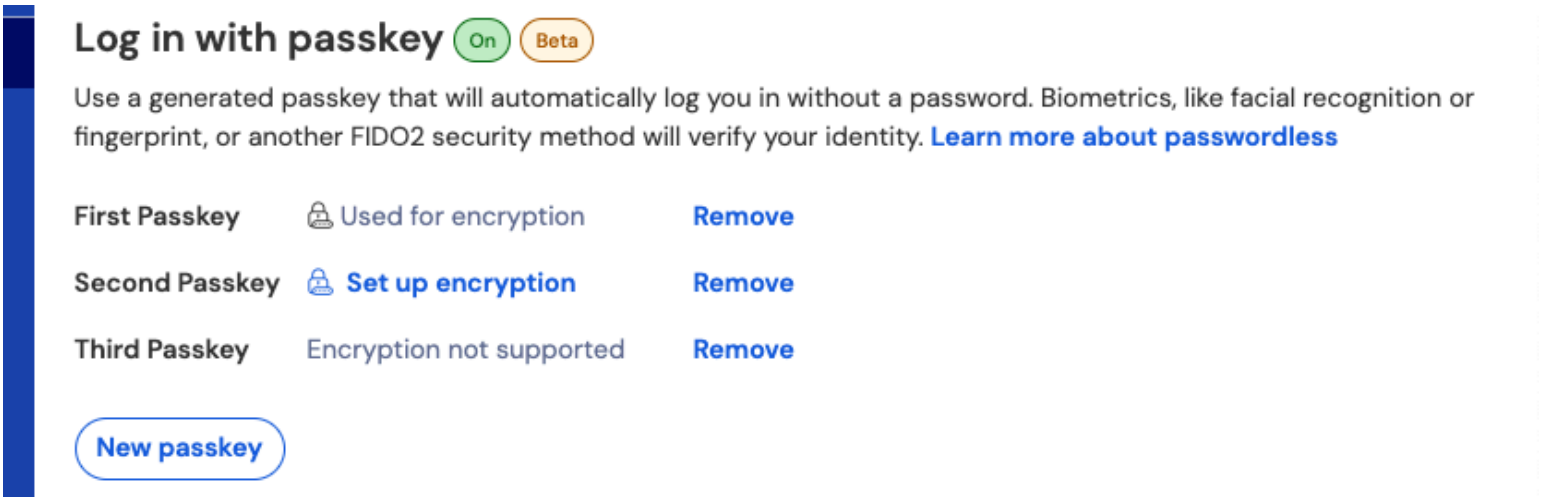
Verwenden Sie den Passschlüssel für die Tresor-Verschlüsselung

   Diese Option wird nur angezeigt, wenn Ihr Passkey und Ihr Browser PRF-fähig sind. Mehr erfahren.

7. Wählen Sie **Einschalten**.

Verschlüsselung einrichten

Sowohl Ihr Passwort als auch Ihr Browser müssen PRF-fähig sein, um die Verwendung des Passworts für die Verschlüsselung und Entschlüsselung des Tresors zu unterstützen. Ihre Passkey-Liste zeigt an, ob jeder Passkey für die Verschlüsselung verwendet wird, unterstützt aber nicht aktiviert ist, oder nicht unterstützt wird:



Passwortliste

Wenn Sie das Kontrollkästchen **Für Tresor-Verschlüsselung verwenden** bei der ersten Einrichtung des Passschlüssels nicht aktiviert haben, oder wenn zum Beispiel der Browser, den Sie zu diesem Zeitpunkt verwendet haben, nicht PRF-fähig war, navigieren Sie zu diesem Menü und wählen Sie die Schaltfläche **Verschlüsselung einrichten**.

Einen Passkey entfernen

Sie können einen vorhandenen Passkey aus Bitwarden entfernen, indem Sie die **Entfernen**-Schaltfläche auf demselben Bildschirm verwenden. Das Entfernen eines Passschlüssels aus Bitwarden wird den in Ihrem FIDO2-Authentifizierer gespeicherten privaten Schlüssel nicht löschen, aber Sie können ihn nicht mehr verwenden, um sich bei Bitwarden anzumelden.

Melden Sie sich mit Ihrem Passwort an

Sobald Ihr Passschlüssel erstellt wurde, können Sie ihn verwenden, um sich bei der Bitwarden-Web-App anzumelden:

1. Auf dem Bitwarden Zugangsdaten-Bildschirm, wählen Sie **Mit Passwort anmelden** dort, wo Sie normalerweise Ihre E-Mail-Adresse eingeben würden.

2. Folgen Sie den Aufforderungen Ihres Browsers, um den Passschlüssel zu lesen, dies wird Sie bei Bitwarden authentifizieren.

3. Wenn Ihr Passwort für die Tresor-Verschlüsselung eingerichtet ist, sind Sie fertig! Andernfalls geben Sie Ihr Master-Passwort ein und wählen Sie **Entsperren** um Ihre Tresor-Daten zu entschlüsseln.

Wie es funktioniert

Die folgende Beschreibung erklärt die Mechanik des Anmeldens mit Passwörtern. Welcher Tab für Sie relevant ist, hängt davon ab, ob Ihr Passkeys mit Verschlüsselung eingerichtet wurde.

⇒Passwörter mit aktivierter Verschlüsselung

Erstellen Sie einen Passschlüssel

Wenn ein Passschlüssel zum Anmelden bei Bitwarden registriert ist:

- Ein **öffentlicher und privater Schlüsselpaar-Passkey** wird vom Authentifikator über die WebAuth-API generiert. Dieses Schlüsselpaar ist per Definition das, was Ihren Passschlüssel ausmacht.

- Ein **PRF-Symmetrischer-Schlüssel** wird vom Authentifikator über die PRF-Erweiterung der WebAuthn-API generiert. Dieser Schlüssel wird aus einem **internen Geheimnis** abgeleitet, das einzigartig für Ihren Passschlüssel ist, und einem von Bitwarden bereitgestellten **Salt**.

- Ein **PRF öffentliches und privates Schlüsselpaar** wird vom Bitwarden-Client generiert. Der PRF-öffentlicher-Schlüssel verschlüsselt Ihren **Konto-Verschlüsselungsschlüssel**, auf den Ihr Client Zugriff hat, indem er angemeldet und entsperrt ist, und der resultierende **PRF-verschlüsselte-Konto-Verschlüsselungsschlüssel** wird an den Server gesendet.

- Der **PRF-Privatschlüssel** wird mit dem **PRF-Symmetrischen Schlüssel** verschlüsselt (siehe Schritt 2) und der resultierende **PRF-verschlüsselte Privatschlüssel** wird an den Server gesendet.

- Ihr Client sendet Daten an Bitwarden-Server, um einen neuen Passkey-Credential-Datensatz für Ihr Konto zu erstellen. Wenn Ihr Passwort bei der Unterstützung für die Verschlüsselung und Entschlüsselung des Tresors registriert ist, enthält dieser Datensatz:
  - Der Passwort-Name
  - Der öffentliche Passwort-Schlüssel
  - Der PRF-öffentlicher-Schlüssel
  - Der PRF-verschlüsselte Konto-Verschlüsselungsschlüssel
  - Der PRF-verschlüsselte private Schlüssel

Ihr privater Passkey, der zur Durchführung der Authentifizierung erforderlich ist, verlässt den Client nur in einem verschlüsselten Format.

Melden Sie sich mit Ihrem Passwort an

Wenn ein Passwort verwendet wird, um sich anzumelden und insbesondere Ihre Tresor-Daten zu entschlüsseln:

- Mit der WebAuthn API öffentlichen Schlüsselkryptographie wird Ihre Authentifizierungsanforderung behauptet und bestätigt.

- Ihr **PRF-verschlüsselter Konto-Verschlüsselungsschlüssel** und **PRF-verschlüsselter privater Schlüssel** werden vom Server an Ihren Client gesendet.

- Unter Verwendung des gleichen von Bitwarden bereitgestellten **salz** und des für Ihren Schlüssel einzigartigen **internen geheimnisses** wird der **prf-symmetrische-schlüssel** lokal neu erstellt.

- Der **PRF-Symmetrischer Schlüssel** wird verwendet, um Ihren **PRF-verschlüsselten privaten Schlüssel** zu entschlüsseln, was zu Ihrem **PRF-privaten Schlüssel** führt.

- Der **PRF-Privatschlüssel** wird verwendet, um Ihren **PRF-verschlüsselten Konto-Verschlüsselungsschlüssel** zu entschlüsseln, was zu Ihrem **Konto-Verschlüsselungsschlüssel** führt. Ihr Konto-Verschlüsselungsschlüssel wird verwendet, um Ihre Tresor-Daten zu entschlüsseln.

⇒Passwörter-mit-deaktivierter-verschlüsselung

Erstellen Sie einen Passschlüssel

Wenn ein Passschlüssel zur Anmeldung bei Bitwarden registriert ist:

1. Ein **öffentlicher und privater Schlüsselpaar-Passkey** wird erstellt. Dieses Schlüsselpaar ist per Definition das, was Ihren Passkey ausmacht.

2. Ihr Client sendet Daten an Bitwarden-Server, um einen neuen Passkey-Credential-Datensatz für Ihr Konto zu erstellen. Wenn Ihr Passwort nicht für die Verschlüsselung und Entschlüsselung des Tresors bei der Unterstützung registriert ist, enthält dieser Datensatz:
   - Der Name des Passschlüssels
   - Der öffentliche Schlüssel des Passworts

Der private Schlüssel Ihres Passworts, der zur Durchführung der Authentifizierung erforderlich ist, verlässt den Client nur in einem verschlüsselten Format.

Melden Sie sich mit Ihrem Passwort an

Wenn ein Passschlüssel verwendet wird, um sich anzumelden, wird Ihre Authentifizierungsanforderung mit der öffentlichen Schlüsselkryptographie der WebAuthn API bestätigt und bekräftigt. Sie werden dann aufgefordert, Ihren Tresor mit Ihrem Master-Passwort zu entschlüsseln.

Ihren Verschlüsselungsschlüssel erneuern

Erneuern Ihres Konto-Verschlüsselungsschlüssels wird die Verschlüsselungs- und Entschlüsselungsfunktion eines jeden Passwortschlüssels, der zur Verwendung für die Tresor-Verschlüsselung eingerichtet wurde, ungültig machen. Die Möglichkeit, dass dieser Passschlüssel für die Authentifizierung verwendet wird, wenn Sie sich bei Bitwarden **nicht** anmelden, wird nicht beeinträchtigt, wenn Sie Ihren Konto-Verschlüsselungsschlüssel erneuern.