KONTOEINSTELLUNGEN > ANMELDEN & ENTSPERREN

Mit PIN-Code entsperren

Mit PIN-Code entsperren

Sie können einen PIN-Code als Methode zum Entsperren Ihres Tresors festlegen. PINs können nur verwendet werden, um Ihren Tresor zu entsperren, 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.

Mit PIN entsperren ist keine passwortlose Methode, um auf Ihr Bitwarden-Konto zuzugreifen. Wenn Sie sich über den Unterschied nicht sicher sind, sehen Sie Verständnis für entsperren vs. anmelden.

> **Note**
>
> Nach **fünf** fehlgeschlagenen PIN-Versuchen wird die App automatisch von Ihrem Konto abmelden.

Entsperren mit PIN aktivieren

Entsperren mit PIN kann für die Bitwarden Browser-Erweiterung, mobile App und Desktop-App aktiviert werden:

> **Warning**
>
> Die Verwendung einer PIN kann das Verschlüsselungsniveau schwächen, das die lokale Tresor-Datenbank Ihrer Anwendung schützt. Wenn Sie sich über Angriffsvektoren Sorgen machen, die eine Kompromittierung der lokalen Daten Ihres Geräts beinhalten, sollten Sie vielleicht den Komfort der Verwendung einer PIN überdenken.

⇒Browser-Erweiterungen

Um die Entsperrung mit PIN für Ihre Browser-Erweiterung zu aktivieren:

1. Öffnen Sie den **Einstellungen** Tab.
2. Öffnen Sie den Abschnitt Kontosicherheit und markieren Sie das Kontrollkästchen **Mit PIN entsperren**.
3. Geben Sie den gewünschten PIN-Code in das Eingabefeld ein. Ihre PIN kann eine beliebige Kombination von Zeichen sein (a-z, 0-9, $, #, usw.).

   > **Tip**
   >
   > Wenn Sie Ihr Gerät teilen, ist es wichtig, eine starke PIN zu erstellen, indem Sie leicht erratbare Ziffern wie das Geburtsdatum vermeiden oder eine PIN verwenden, die mehr als vier Ziffern hat.

4. Die vorausgewählte Option **Bei Browser-Neustart mit Master-Passwort sperren** erfordert, dass Sie Ihr Master-Passwort anstelle der PIN eingeben, wenn Ihr Browser neu startet. Wenn Sie die Möglichkeit haben möchten, mit einer PIN zu entsperren, auch wenn der Browser neu startet, deaktivieren Sie die Option.

   > **Note**
   >
   > Wenn Sie die Option **Beim Neustart mit Master-Passwort sperren** deaktivieren, kann die Bitwarden-Anwendung möglicherweise sensible Daten nicht vollständig aus dem Anwendungsspeicher löschen, wenn sie in einen gesperrten Zustand übergeht. Wenn Sie sich Sorgen um den lokalen Speicher Ihres Geräts machen, sollten Sie die Option **Bei Neustart mit Master-Passwort sperren** eingeschaltet lassen.

Einmal eingestellt, können Sie Ihre PIN ändern, indem Sie das Entsperren mit PIN deaktivieren und wieder aktivieren.

Wenn Sie sich von Ihrer Browser-Erweiterung **abmelden**, werden Ihre Einstellungen für das Entsperren mit PIN gelöscht und Sie müssen das Entsperren mit PIN erneut aktivieren.

⇒Handy

Um die Entsperrung mit PIN für Ihre mobile App zu aktivieren:

1. Öffnen Sie den **Einstellungen** Tab.
2. Scrollen Sie nach unten zum Sicherheitsbereich und tippen Sie auf die Option **Mit PIN-Code entsperren**.
3. Geben Sie den gewünschten PIN-Code in das Eingabefeld ein. Ihre PIN kann eine beliebige Kombination von Zahlen (0-9) sein.

   > **Tip**
   > Wenn Sie Ihr Gerät teilen, ist es wichtig, eine starke PIN zu erstellen, indem Sie leicht erratbare Ziffern wie das Geburtsdatum vermeiden oder eine PIN verwenden, die mehr als vier Ziffern hat.

4. Ein Dialogfeld wird angezeigt, in dem Sie gefragt werden, ob Sie beim Neustart der Anwendung das Entsperren mit Ihrem Master-Passwort verlangen möchten. Tippen Sie auf **Ja**, um Ihr Master-Passwort anstelle der PIN zu benötigen, wenn die App neu startet. Tippen Sie auf **Nein**, um die Möglichkeit zu haben, die App beim Neustart mit der PIN zu entsperren.

Einmal eingestellt, können Sie Ihre PIN ändern, indem Sie Entsperrt mit PIN deaktivieren und wieder aktivieren.

Wenn Sie sich von Ihrer mobilen App **abmelden**, werden Ihre Einstellungen für das Entsperren mit PIN gelöscht und Sie müssen das Entsperren mit PIN erneut aktivieren.

⇒PC

Mit PIN entsperren wird separat für jedes Konto eingestellt, das in der Desktop-App angemeldet ist. Um die Entsperrung mit PIN zu ermöglichen:

1. Öffnen Sie Ihre **Einstellungen** (unter Windows, **Datei** → **Einstellungen**) (unter macOS, **Bitwarden** → **Einstellungen**).
2. Scrollen Sie nach unten zum Abschnitt Sicherheit und markieren Sie das Kontrollkästchen **Mit PIN entsperren**.
3. Geben Sie den gewünschten PIN-Code in das Eingabefeld ein. Ihre PIN kann eine beliebige Kombination von Zeichen sein (a-z, 0-9, $, #, usw.).

   > **Tip**
   > Wenn Sie Ihr Gerät teilen, ist es wichtig, eine starke PIN zu erstellen, indem Sie leicht erratbare Ziffern wie das Geburtsdatum vermeiden oder eine PIN verwenden, die mehr als vier Ziffern hat.

4. Die vorausgewählte Option **Bei Neustart mit Master-Passwort sperren** erfordert, dass Sie Ihr Master-Passwort anstelle der PIN eingeben, wenn die App neu startet. Wenn Sie die Möglichkeit haben möchten, die App beim Neustart mit einer PIN zu entsperren, deaktivieren Sie diese Option.

> **Note**
>
> Wenn Sie die Option **Beim Neustart mit Master-Passwort sperren** deaktivieren, kann die Bitwarden-Anwendung möglicherweise sensible Daten nicht vollständig aus dem Anwendungsspeicher löschen, wenn sie in einen gesperrten Zustand übergeht. Wenn Sie sich Sorgen um den lokalen Speicher Ihres Geräts machen, sollten Sie die Option **Bei Neustart mit Master-Passwort sperren** eingeschaltet lassen.

Einmal eingestellt, können Sie Ihre PIN ändern, indem Sie das Entsperren mit PIN deaktivieren und wieder aktivieren.

Wenn Sie sich von Ihrer Desktop-App **abmelden**, werden Ihre Einstellungen für das Entsperren mit PIN gelöscht und Sie müssen das Entsperren mit PIN erneut aktivieren.

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 auf dem Server in ihrer verschlüsselten Form.

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.
>
> **Sperren** 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).