bitwarden | Hilfezentrum Artikel

SICHERHEIT

# Verschlüsselung

Ansicht im Hilfezentrum:
https://bitwarden.com/help/what-encryption-is-used/

## Verschlüsselung

Bitwarden verwendet AES-CBC 256-Bit-Verschlüsselung für Ihre Tresor-Daten und PBKDF2 SHA-256 oder Argon2 zur Ableitung Ihres Verschlüsselungsschlüssels.

Bitwarden verschlüsselt und/oder hasht Ihre Daten **immer** auf Ihrem lokalen Gerät, bevor etwas zur Speicherung an Cloud-Server gesendet wird. **Bitwarden-Server werden nur zur Speicherung verschlüsselter Daten verwendet.** Für weitere Informationen, siehe Speicher.

Die Daten im Tresor können nur mit dem Schlüssel entschlüsselt werden, der von Ihrem Master-Passwort abgeleitet wurde. Bitwarden ist eine Verschlüsselungslösung mit Nullwissen, was bedeutet, dass Sie die einzige Partei sind, die Zugang zu Ihrem Schlüssel hat und in der Lage ist, Ihre Tresor Daten zu entschlüsseln.

> **Tip**
>
> Wenn Sie mehr darüber erfahren möchten, wie diese Verschlüsselungsschlüssel verwendet werden, um Ihren Tresor zu schützen, können Sie auch unser Sicherheits-Whitepaper einsehen.

### AES-CBC

AES -CBC (Cipher Block Chaining) , das zur Verschlüsselung von Tresordaten verwendet wird, ist ein Standard in der Kryptographie und wird von der US-Regierung und anderen Regierungsbehörden auf der ganzen Welt zum Schutz streng geheimer Daten verwendet. Mit einer ordnungsgemäßen Implementierung und einem starken Verschlüsselungsschlüssel (Ihr Master-Passwort) gilt AES als unknackbar.

### PBKDF2

PBKDF2 SHA-256 wird verwendet, um den Verschlüsselungsschlüssel aus Ihrem Master-Passwort abzuleiten, jedoch können Sie Argon2 als Alternative wählen. Bitwarden salzt und hasht Ihr Master-Passwort mit Ihrer E-Mail-Adresse **lokal**, bevor es an unsere Server übertragen wird. Sobald ein Bitwarden-Server das gehashte Passwort erhält, wird es erneut mit einem kryptographisch sicheren zufälligen Wert gesalzen, erneut gehasht und in unserer Datenbank gespeichert.

Die standardmäßig verwendete Iterationsanzahl mit PBKDF2 beträgt 600.001 Iterationen auf dem Client (die Iterationsanzahl auf der Client-Seite kann in Ihren Kontoeinstellungen konfiguriert werden) und dann zusätzliche 100.000 Iterationen, wenn sie auf unseren Servern gespeichert wird (insgesamt standardmäßig 700.001 Iterationen). Der Schlüssel der Organisation wird über RSA-2048 geteilt.

> **Tip**
>
> Die Anzahl der standardmäßig von Bitwarden verwendeten Iterationen wurde im Februar 2023 erhöht. Konten, die nach dieser Zeit erstellt wurden, verwenden 600.001, jedoch sollten Sie die Iterationsanzahl erhöhen, wenn Sie Ihr Konto vor diesem Zeitpunkt erstellt haben. Anweisungen dazu finden Sie im folgenden Abschnitt.

Die verwendeten Hash-Funktionen sind Einweg-Hashes, was bedeutet, dass sie von niemandem bei Bitwarden **rückgängig gemacht werden können**, um Ihr Master-Passwort zu enthüllen. Selbst wenn Bitwarden gehackt werden würde, gäbe es keine Methode, mit der Ihr Master-Passwort erhalten werden könnte.

### Ändern der KDF-Iterationen

Bitwarden verwendet eine sichere Standardeinstellung, wie oben erwähnt, jedoch können Sie die Iterationsanzahl im **Einstellungen → Sicherheit → Schlüssel** Menü des Web-Tresors ändern.

Das Ändern der Iterationsanzahl kann dabei helfen, Ihr Master-Passwort vor einem Brute-Force-Angriff durch einen Angreifer zu schützen, sollte jedoch nicht als Ersatz für die Verwendung eines starken Master-Passworts von Anfang an betrachtet werden. Die

Änderung der Iterationszahl wird den geschützten symmetrischen Schlüssel neu verschlüsseln und den Authentifizierungshash aktualisieren, ähnlich wie eine normale Änderung des Master-Passworts, aber der symmetrische Verschlüsselungsschlüssel wird nicht erneuert, sodass die Daten im Tresor nicht neu verschlüsselt werden. Siehe hier für Informationen zur erneuten Verschlüsselung Ihrer Daten.

Wenn Sie Ihre KDF-Iterationen zu hoch einstellen, könnte dies zu schlechter Leistung führen, wenn Sie sich bei Bitwarden anmelden (und entsperren) auf Geräten mit langsameren CPUs. Wir empfehlen, dass Sie den Wert in Schritten von 100.000 erhöhen und dann alle Ihre Geräte testen.

Wenn Sie die Iterationsanzahl ändern, werden Sie von allen Clients abgemeldet. Obwohl das Risiko, das bei der Erneuerung Ihres Verschlüsselungsschlüssels besteht, beim Ändern der KDF-Iterationsanzahl nicht vorhanden ist, empfehlen wir dennoch, Ihren Tresor zu exportieren, bevor Sie dies tun.

## Argon2id

Argon2, der Gewinner des Passwort-Hashing-Wettbewerbs 2015, steht als Alternative zu PBKDF2 zur Verfügung (mehr erfahren). Es gibt drei Versionen des Algorithmus und Bitwarden hat Argon2id implementiert wie von OWASP empfohlen. Argon2id ist eine Hybridversion anderer Versionen und verwendet eine Kombination aus datenabhängigen und datenunabhängigen Speicherzugriffen, was ihm einen Teil der Widerstandsfähigkeit von Argon2i gegen Seitenkanal-Cache-Timing-Angriffe und einen Großteil der Widerstandsfähigkeit von Argon2d gegen GPU-Cracking-Angriffe verleiht (Quelle).

Standardmäßig ist Bitwarden so eingestellt, dass es 64 MiB Speicher zuweist, 3 Mal darüber iteriert und dies über 4 Threads verteilt. Diese Standardwerte liegen über den aktuellen OWASP-Empfehlungen, aber hier sind einige Tipps, sollten Sie sich entscheiden, Ihre Einstellungen zu ändern:

- Eine Erhöhung der **KDF-Iterationen** wird die Laufzeit linear erhöhen.
- Die Menge an **KDF-Parallelität**, die Sie verwenden können, hängt von der CPU Ihres Computers ab. Im Allgemeinen, Max. Parallelismus = Anzahl der Kerne x 2.

> **Note**
>
> Benutzer von Argon2id mit einem KDF-Speicherwert höher als 48 MB erhalten jedes Mal eine Warnmeldung, wenn die iOS-Autofill-Funktion gestartet wird oder ein neuer Send über das Share-Menü erstellt wird. Um diese Nachricht zu vermeiden, passen Sie die Argon2id Einstellungen an oder aktivieren Sie Entsperren mit Biometrie.

## Aufgerufene Kryptobibliotheken

**Bitwarden schreibt keinen kryptografischen Code.** Bitwarden verwendet nur Krypto aus beliebten und renommierten Krypto-Bibliotheken, die von Kryptographie-Experten geschrieben und gepflegt werden. Die folgenden Krypto-Bibliotheken werden verwendet:

- JavaScript (Web-Tresor, Browser-Erweiterung, Desktop und CLI)
  - Web-Krypto
  - Node.js Krypto
  - Schmiede
- C# (Mobil)
  - CommonCrypto (iOS, Apple)

- Javax.Crypto (Android, Oracle)
- BouncyCastle (Android)