bitwarden | Help Center Article

SÄKERHET > ENCRYPTION

Kryptering

View in the help center:
https://bitwarden.com/help/what-encryption-is-used/

Kryptering

Bitwarden använder AES-CBC 256-bitars kryptering för dina valvdata och PBKDF2 SHA-256 eller Argon2 för att härleda din krypteringsnyckel.

Bitwarden krypterar och/eller hashar **alltid** dina data på din lokala enhet innan något skickas till molnservrar för lagring. **Bitwarden-servrar används endast för att lagra krypterad data.** För mer information, se Lagring.

All valvdata krypteras av Bitwarden innan den lagras någonstans. För att lära dig hur, se Bitwarden Security Whitepaper. Bitwarden är en krypteringslösning med noll kunskap, vilket innebär att du är den enda parten med tillgång till de nycklar som krävs för att dekryptera valvdata.

> **Tip**
>
> If you'd like to learn more about how these encryption keys are used to protect your vault, you can also check out our Security Whitepaper.

AES-CBC

AES-CBC (cipher block chaining), som används för att kryptera valvdata, är en standard inom kryptografi och används av den amerikanska regeringen och andra statliga myndigheter runt om i världen för att skydda topphemlig data. Med korrekt implementering och en stark krypteringsnyckel (ditt huvudlösenord) anses AES vara okrossbar.

PBKDF2

PBKDF2 SHA-256 används för att härleda krypteringsnyckeln från ditt huvudlösenord, men du kan välja Argon2 som ett alternativ. Bitwarden saltar och hashar ditt huvudlösenord med din e-postadress **lokalt** innan överföring till våra servrar. När en Bitwarden-server väl tar emot det hashade lösenordet, saltas det igen med ett kryptografiskt säkert slumpmässigt värde, hashas igen och lagras i vår databas.

Det förinställda antalet iterationer som används med PBKDF2 är 600 001 iterationer på klienten (antalet iterationer på klientsidan kan konfigureras från dina kontoinställningar), och sedan ytterligare 100 000 iterationer när de lagras på våra servrar (för totalt 700 001 iterationer som standard). Organisationsnyckeln delas via RSA-2048.

> **Tip**
>
> The number of default iterations used by Bitwarden was increased in February, 2023. Accounts created after that time will use 600,001, however if you created your account prior to then you should increase the iteration count. Instructions for doing so can be found in the following section.

De använda hashfunktionerna är envägshashar, vilket innebär att de inte **kan omvändas** av någon på Bitwarden för att avslöja ditt huvudlösenord. Även om Bitwarden skulle hackas, skulle det inte finnas någon metod för att få ditt huvudlösenord.

Ändra KDF-iterationer

Bitwarden använder en säker standard, som nämnts ovan, men du kan ändra antalet iterationer från menyn **Inställningar → Säkerhet → Nycklar** i webbvalvet.

Att ändra antalet iterationer kan hjälpa till att skydda ditt huvudlösenord från att bli brutalt tvingat av en angripare, men bör inte ses som ett substitut till att använda ett starkt huvudlösenord i första hand. Ändring av iterationsantalet kommer att kryptera om den skyddade symmetriska nyckeln och uppdatera autentiseringshashen, ungefär som en vanlig huvudlösenordsändring, men kommer inte

att rotera den symmetriska krypteringsnyckeln så att valvdata inte kommer att krypteras på nytt. Se här för information om omkryptering av dina data.

Om du ställer in dina KDF-iterationer för högt kan det resultera i dålig prestanda när du loggar in (och låser upp) Bitwarden på enheter med långsammare CPU:er. Vi rekommenderar att du ökar värdet i steg om 100 000 och sedan testar alla dina enheter.

När du ändrar antalet iterationer kommer du att loggas ut från alla klienter. Även om risken med att rotera din krypteringsnyckel inte existerar när du ändrar antalet KDF-iterationer, rekommenderar vi ändå att du exporterar ditt valv i förväg.

Argon2id

Argon2, vinnaren av 2015 års Password Hashing Competition, är tillgänglig som ett alternativ till PBKDF2 (läs mer). Det finns tre versioner av algoritmen, och Bitwarden har implementerat Argon2id som rekommenderas av OWASP. Argon2id är en hybrid av andra versioner, som använder en kombination av databeroende och dataoberoende minnesåtkomster, vilket ger den en del av Argon2is motstånd mot sidokanal-cache-timingsattacker och mycket av Argon2ds motstånd mot GPU-krackningsattacker (källa).

Som standard är Bitwarden inställd på att allokera 64 MiB minne, iterera över det 3 gånger och göra det över 4 trådar. Dessa standardvärden ligger över nuvarande OWASP-rekommendationer, men här är några tips om du väljer att ändra dina inställningar:

- Ökande **KDF-iterationer** kommer att öka körtiden linjärt.
- Mängden **KDF-parallellism** du kan använda beror på din maskins CPU. I allmänhet är Max. Parallellism = Num. av kärnor x 2.

> **Note**
> Argon2id users with a KDF memory value higher than 48 MB will receive a warning dialogue every time iOS autofill is initiated or a new Send is created through the Share sheet. To avoid this message, adjust Argon2id settings or enable unlock with biometrics.

Anropade kryptobibliotek

Bitwarden implementerar inga kryptografiska primitiver. Bitwarden använder endast kryptografiska primitiver från populära och välrenommerade kryptobibliotek som är skrivna och underhållna av kryptografiska experter. Följande kryptobibliotek används:

- JavaScript:
  - Webbkrypto
  - Node.js krypto
  - Smedja
  - Argon 2
- Rostlådor:
  - RustCrypto
  - curve25519-dalek
  - rost-slumpmässigt
  - prasslar