bitwarden | Help Center Article

SÄKERHET

Vanliga frågor om säkerhet

View in the help center:
https://bitwarden.com/help/security-faqs/

Vanliga frågor om säkerhet

Den här artikeln innehåller vanliga frågor (FAQ) om säkerhet.

F: Varför ska jag lita på Bitwarden med mina lösenord?

S: Du kan lita på oss av några anledningar:

1. Bitwarden är programvara **med öppen källkod**. All vår källkod finns på GitHub och är gratis för alla att granska. Tusentals mjukvaruutvecklare följer Bitwardens källkodsprojekt (och det borde du också!).
2. Bitwarden **granskas av välrenommerade tredjepartssäkerhetsföretag** såväl som oberoende säkerhetsforskare.
3. Bitwarden lagrar **inte dina lösenord**. Bitwarden lagrar krypterade versioner av dina lösenord som bara du kan låsa upp. Din känsliga information krypteras lokalt på din personliga enhet innan den någonsin skickas till våra molnservrar.
4. **Bitwarden har ett rykte.** Bitwarden används av miljontals individer och företag. Om vi gjorde något tveksamt eller riskabelt, skulle vi gå i konkurs!

Litar du fortfarande inte på oss? Du behöver inte. Öppen källkod är vackert. Du kan enkelt vara värd för hela Bitwarden-stacken själv. Du kontrollerar din data. Läs mer här.

F: Vad händer om Bitwarden blir hackad?

S: Bitwarden vidtar extrema åtgärder för att säkerställa att dess webbplatser, applikationer och molnservrar är säkra. Bitwarden använder Microsoft Azure-hanterade tjänster för att hantera serverinfrastruktur och säkerhet, snarare än att göra det direkt.

Om Bitwarden av någon anledning skulle bli hackad och din data avslöjades, är din information fortfarande skyddad på grund av stark kryptering och envägssaltade hashåtgärder som vidtagits på dina valvdata och huvudlösenord.

F: Kan Bitwarden se mina lösenord?

A: Nej.

Din data är helt krypterad och/eller hashad innan den någonsin lämnar **din** lokala enhet, så ingen från Bitwarden-teamet kan någonsin se, läsa eller bakåtkonstruera för att komma till din riktiga data. Bitwarden-servrar lagrar endast krypterad och hashad data. För mer information om hur dina data krypteras, se Kryptering.

F: Är mitt Bitwarden-huvudlösenord lagrat lokalt?

A: Nej.

Vi sparar inte huvudlösenordet lokalt eller i minnet. Din krypteringsnyckel (som härrör från huvudlösenordet) sparas endast i minnet medan appen är upplåst, vilket krävs för att dekryptera data i ditt valv. När valvet är låst rensas denna data från minnet.

Vi laddar också om programmets återgivningsprocess efter 10 sekunders inaktivitet på låsskärmen för att säkerställa att alla hanterade minnesadresser som ännu inte har samlats in som skräp rensas. Vi gör vårt bästa för att se till att all data som kan finnas i minnet för att applikationen ska fungera bara lagras i minnet så länge du behöver den och att minnet rensas upp när applikationen är låst. Vi anser att applikationens krypterade data är helt säker medan applikationen är i låst tillstånd.

F: Vad gör jag om jag inte känner igen en ny enhet som loggar in på Bitwarden?

S: Om IP-adressen för en ny enhet inte matchar några kända IP-adresser (hemnätverk, arbetsnätverk, mobilnät och så vidare), ändra ditt huvudlösenord och se till att tvåstegsinloggning är aktiverat för ditt konto. Du bör också avauktorisera sessioner från sidan

Kontoinställningar i ditt webbvalv för att tvinga utloggning på alla enheter. Om du tror att dina valvobjekt kan äventyras bör du ändra dina lösenord.

F: Vad är Bitwarden kompatibel med? Vilka certifieringar har du?

S: Bitwarden är kompatibel med följande policyer:

- **GDPR.** Läs mer här.
- **CCPA.** Läs mer här.
- **HIPAA.** Läs mer här.
- **SOC 2 Typ 2.** Läs mer här.
- **SOC 3.** Läs mer här.

För mer information, besök vår sida för säkerhet och efterlevnad.

F: Hur uppfyller Bitwarden europeiska efterlevnadskrav?

S: Bitwarden är GDPR-kompatibel och använder godkända mekanismer för informationsöverföring inklusive EU Standard Contractual Clauses (SCCs) i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 godkänd av Europeiska kommissionens genomförandebeslut (EU) 2021/914 av den 4 juni 2021, som för närvarande anges på https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. För affärs- och företagskunder kan Bitwarden verkställa Bitwardens dataskyddsavtal.

Bitwardens molnservrar finns för närvarande på Microsoft Azure i USA och EU. Idag betjänar Bitwarden miljontals användare, inklusive myndigheter och företagskunder i hela Europa och världen, med denna infrastruktur.

För kunder som behöver full kontroll över datauppehållstillstånd kan Bitwarden alternativt hostas privat på din egen infrastruktur.

All valvdata som lagras i Bitwarden, oavsett om den är i molnet eller är egenvärd, är krypterad från ände till ände och inte tillgänglig för någon förutom Bitwarden-användaren. Med denna end-to-end, noll kunskapskrypteringsarkitektur kan inte ens Bitwarden komma åt dina data.

För en fullständig lista över Bitwardens säkerhets- och efterlevnadscertifieringar, besök https://bitwarden.com/compliance/.

F: Vilka tredjepartstjänster, bibliotek eller identifierare används i mitt Bitwarden-konto?

S: I mobilapparna används Firebase Cloud Messaging (ofta misstas för en tracker) endast för push-meddelanden relaterade till synkronisering och utför absolut inga spårningsfunktioner. Microsoft Visual Studio App Center används för kraschrapportering på en rad mobila enheter. I webbvalvet används Stripe- och PayPal-skript för betalningshantering endast på betalningssidor.

För de som föredrar att utesluta all kommunikation från tredje part tas Firebase och Microsoft Visual Studio App Center bort helt från F-Droid-bygget. Om du stänger av push-meddelanden på en Bitwarden-server som är självvärd kommer du dessutom att inaktivera användningen av push-reläservern.

Bitwarden Android-applikationen inkluderar också möjligheten att inaktivera kraschrapportering under Inställningar.

Bitwarden tar användarsäkerhet och integritet på allvar. Bitwarden upprätthåller säker end-to-end-kryptering med noll kunskap om din krypteringsnyckel. Som ett företag fokuserat på öppen källkod inbjuder vi alla att granska våra biblioteksimplementeringar när som helst på GitHub.

F: Hur kräver jag tvåstegsinloggning för min Bitwarden-organisation?

S: Använd en företagspolicy som ingår i ett Enterprise-organisationsabonnemang. Du kan också aktivera Duo MFA-integration för att genomdriva 2FA/MFA för din organisation. För mer information, se Tvåstegsinloggning via Duo.

F: Vilka är certifikatalternativen för en självvärd instans av Bitwarden?

S: Se Certifikatalternativ för en fullständig lista och instruktioner.

F: Hur ändras Bitwardens veterinärkod?

S: Förtroende för säkerheten i våra system är ytterst viktigt för Bitwarden. Alla föreslagna kodändringar granskas av en eller flera icke-författare i teamet innan de kan slås samman till någon kodbas. All kod går igenom flera test- och QA-miljöer innan produktion. Bitwarden har implementerat en SOC2-rapport för att granska och validera våra interna rutiner. Som nämnts i rapporten är vårt team föremål för rigorösa bakgrundskontroller och noggranna intervjuprocesser. Bitwarden, som är en produkt med öppen källkod, välkomnar också peer-review av vår kod när som helst. Teamet på Bitwarden strävar efter att göra allt vi kan för att hålla våra användare bekväma och hålla deras data säker.

F: Hur länge cachelagrar Bitwarden sessionsinformation?

A: Bra fråga! Svaret beror på den specifika informationen och klientapplikationen:

- Offlinevalvsessioner upphör att gälla efter 30 dagar.
  - **Förutom** för mobila klientapplikationer, som upphör att gälla efter 90 dagar.
- Tvåstegsinloggning **Remember** Me-valen kommer att upphöra efter 30 dagar.
- Directory Connector sync cache kommer att rensas efter 30 dagar.
- Organisationsinbjudningar upphör att gälla efter 5 dagar. Kunder med egen värd kan konfigurera detta med en miljövariabel.

F: Hur validerar jag kontrollsumman för en Bitwarden-app?

S: Kontrollsummor kan för närvarande valideras för lösenordshanterarens stationära appar, Android-mobilappar och CLI-klienter:

⇒Desktop

1. From https://github.com/bitwarden/clients/releases/, download the package for the latest release of the desktop app (for example, `Bitwarden-Installer-2024.8.2.exe`).
2. From the same page, download the `sha256-checksums.txt` file for that release and open it with a text editor.
3. Using `CertUtil` or `sha256sum`, generate a SHA-256 hash of the downloaded package, for example:

   ```
   Bash

   sha256sum Bitwarden-2024.8.2-universal.dmg
   ```

   This command will print a hash value to the console.
4. Compare the printed hash value to the value listed in `sha256-checksums.txt` for your downloaded package.

⇒Android

1. From https://github.com/bitwarden/android/releases/, download the package for the latest release of the Android app (for example, `com.x8bit.bitwarden.apk`).

2. From the same page, download the corresponding `{package}-sha256.txt` file and open it with a text editor.

3. Using `CertUtil` or `sha256sum`, generate a SHA-256 hash of the downloaded package, for example:

   ```bash
   sha256sum com.x8bit.bitwarden.apk
   ```

   This command will print a hash value to the console.

4. Compare the printed hash value to the value listed in `{package}-sha256.txt` for your downloaded package.

⇒CLI

1. From https://github.com/bitwarden/clients/releases/, download the package for the latest release of the CLI (for example, `bw-linux-2024.8.2.zip`).

2. From the same page, download the corresponding SHA-256 `.txt` file, in this example `bw-linux-sha256-2024.8.2.txt`, and open it with a text editor.

3. Using `CertUtil` or `sha256sum`, generate a SHA-256 hash of the downloaded `.zip`, for example:

   ```bash
   sha256sum bw-linux-2024.8.2.zip
   ```

   This command will print a hash value to the console.

4. Compare the printed hash value to the value listed in the SHA-256 `.txt` file for your downloaded package.

F: Hur gör jag ett säkerhetsavslöjande eller rapporterar till Bitwarden?

S: Bitwarden anser att det är avgörande att arbeta med säkerhetsforskare över hela världen för att hålla våra användare säkra. Om du tror att du har hittat ett säkerhetsproblem i vår produkt eller tjänst rekommenderar vi att du skickar en rapport via vårt HackerOne-program. Vi välkomnar att arbeta med dig för att lösa problemet snabbt. Läs mer om vår avslöjandepolicy.

F: Hur kan jag skydda mitt Bitwarden-konto från brute-force-attacker?

S: En brute-force attack är när en illvillig aktör cyklar igenom en kombination av svaga och korta lösenord i ett försök att få tillgång till ditt konto. Bitwarden erbjuder några sätt du kan skydda dig mot dessa potentiella attacker:

- Ha ett långt och unikt huvudlösenord. Bitwarden kräver minst 12 tecken för att öka kontosäkerheten.
- Ställ in 2FA på alla Bitwarden-konton för att lägga till ett extra lager av säkerhet.
- Bitwarden kommer att kräva CAPTCHA-verifiering efter 9 misslyckade inloggningsförsök från en okänd enhet.

Frågor om specifika klientappar

F: Vilken data använder Bitwarden från klientapplikationer?

S: Bitwarden använder administrativa data för att tillhandahålla Bitwarden-tjänsten till dig. Som framgår av vissa appsekretessrapporter tillhandahåller användare följande information om kontoskapande:

- Ditt namn (valfritt).
- Din e-postadress (används för e-postverifiering, kontoadministration och kommunikation mellan dig och Bitwarden).

Dessutom tilldelas en **Bitwarden-genererad** enhetsspecifik GUID (ibland kallad ett enhets-ID) till din enhet. Denna GUID används för att varna dig när en ny enhet loggar in i ditt valv.

F: Kan du förklara elektronappens säkerhet?

S: En ofta delad artikel föreslår ett fel med elektronappar, men den refererade attacken kräver att en användare har en kompromitterad maskin, vilket naturligtvis skulle tillåta en illvillig angripare att äventyra data på den maskinen. Så länge du inte har någon anledning att tro att enheten du använder har äventyrats är din data säker.

F: Hur säkrar Bitwarden webbläsartillägg?

S: Tillägg är säkra att använda om de har utvecklats på rätt sätt. På grund av hur webbläsartillägg fungerar finns det alltid en chans att ett fel uppstår. Vi är extremt försiktiga och försiktiga när vi utvecklar våra tillägg och tillägg, vi håller ögonen och öronen ute för allt som händer i branschen och vi genomför säkerhetsrevisioner för att hålla många ögon på allt.

F: Vad frågar webbläsartillägget om tillåtelse för?

S: Vid installationen kommer webbläsartillägget att be om tillåtelse att få åtkomst till ditt urklipp för att kunna använda den schemalagda urklippsrensfunktionen (åtkomlig i menyn **Alternativ**).

När den här **valfria funktionen** är aktiverad kommer urklippsrensning att ta bort alla Bitwarden-inlägg som gjorts av eller fyllts i ett konfigurerbart intervall. Åtkomst till urklipp tillåter Bitwarden att göra detta utan att ta bort ett urklippsobjekt som inte är associerat från Bitwarden-applikationen genom att kontrollera det senast kopierade objektet mot det senast kopierade objektet från ditt valv. Observera att den här funktionen är **avstängd som standard**.

F: Vilka appbehörigheter begärs av mobilappen?

S: Bitwarden Android- och iOS-appar kan be om följande behörigheter medan du använder appen:

Tillstånd	Resonera
Tillåta Bitwarden att ta bilder och spela in video?	För att skanna QR-koder för tvåstegsinloggning eller Bitwarden-autentisering.
Tillåta Bitwarden att komma åt foton och media på din enhet?	Skapa bilagor eller skickar från en fil som är sparad på din enhet.

Ytterligare grundläggande behörigheter som krävs av Bitwarden listas i Google Play Butik.

F: Varför behöver webbläsartillägget nativeMessaging-behörighet?

S: Version 1.48.0 av webbläsartillägget möjliggör biometrisk upplåsning för webbläsartillägg.

Denna behörighet, även känd som `nativeMessaging`, är säker att acceptera och tillåter webbläsartillägget att kommunicera med Bitwarden-skrivbordsappen, som krävs för att aktivera upplåsning med biometri.

Observera att när din webbläsare uppdateras till den här versionen kan du bli ombedd att acceptera en ny behörighet som heter "kommunicera med samarbetande inbyggda applikationer" (i Chromium-baserade webbläsare), eller "utbyta meddelanden med andra program än Firefox." Om du inte accepterar denna behörighet förblir tillägget inaktiverat.

F: Är Bitwarden FIPS-kompatibel?

S: Bitwarden använder FIPS 140-kompatibla bibliotek och kryptografi, och de flesta FIPS 140-installationer av Bitwarden utnyttjar alternativet för självvärd för att göra utvärderingar (till exempel Cyber Maturity Model Certification) enklare. Bitwarden-plattformen har inte utfört några FIPS-certifieringar för närvarande. Förfrågningar är välkomna via kontaktsidan.

F: Kan jag begränsa åtkomsten till Bitwarden till vissa enheter?

S: Med självvärd kan du använda anpassade brandväggs- och NGINX-konfigurationer samt VPN/VLAN-åtkomstkontroll för att bestämma enhetstyper och/eller nätverkslageråtkomst för din Bitwarden-instans. Du kan också använda andra verktyg som certifikat på enhetsnivå för att kontrollera specifik enhetsåtkomst till Bitwarden-instansen också.

F: Har Bitwarden en bärbar applikation?

A: Ja! Bitwarden-skrivbordsappen är tillgänglig för Windows som en bärbar `.exe` som kan laddas ner här. Den bärbara appen lämpar sig väl för **alltid offline-miljöer** eller scenarier där automatisk uppdatering av appen inte är önskvärd. Den bärbara appen kommer inte **att uppdatera sig själv**.

F: Kommer åtkomstalternativen för webbplatsen att störa webbläsartillägget Bitwarden?

S: Webbplatsåtkomstinställningar för Bitwardens webbläsartillägg måste ställas in på **På alla webbplatser**, eller på **På specifika webbplatser** med Bitwarden-servern tillagd i listan, för att webbläsartillägget ska fungera korrekt. **Att ställa in webbplatsåtkomst till** Vid klick begränsar Bitwardens möjlighet att hämta data från Bitwarden-servern, vilket i grunden krävs för att spara eller uppdatera referenser.