bitwarden | Help Center Article

SECURITY

Security FAQs

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

Security FAQs

This article contains frequently asked questions (FAQs) regarding security.

Q: Why should I trust Bitwarden with my passwords?

A: You can trust us for a few reasons:

1. Bitwarden is **open source** software. All of our source code is hosted on GitHub and is free for anyone to review. Thousands of software developers follow Bitwarden's source code projects (and you should too!).

2. Bitwarden is **by reputable third-party security firms** as well as independent security researchers.

3. Bitwarden **does not store your passwords**. Bitwarden stores encrypted versions of your passwords that only you can unlock. Your sensitive information is encrypted locally on your personal device before ever being sent to our cloud servers.

4. **Bitwarden has a reputation.** Bitwarden is used by millions of individuals and businesses. If we did anything questionable or risky, we would be out of business!

Still don't trust us? You don't have to. Open source is beautiful. You can easily host the entire Bitwarden stack yourself. You control your data. Learn more here.

Q: What happens if Bitwarden gets hacked?

A: Bitwarden takes extreme measures to ensure that its websites, applications, and cloud servers are secure. Bitwarden uses Microsoft Azure managed services to manage server infrastructure and security, rather than doing so directly.

If for some reason Bitwarden were to get hacked and your data was exposed, your information is still protected due to strong encryption and one-way salted hashing measures taken on your vault data and master password.

Q: Can Bitwarden see my passwords?

A: No.

Your data is fully encrypted and/or hashed before ever leaving **your** local device, so no one from the Bitwarden team can ever see, read, or reverse engineer to get to your real data. Bitwarden servers only store encrypted and hashed data. For more information about how your data is encrypted, see Encryption.

Q: Is my Bitwarden master password stored locally?

A: No.

We do not keep the master password stored locally or in memory. Your encryption key (derived from the master password) is kept in memory only while the app is unlocked, which is required to decrypt data in your vault. When the vault is locked, this data is purged from memory.

We also reload the application's renderer process after 10 seconds of inactivity on the lock screen to make sure any managed memory addresses which have not yet been garbage collected are purged. We do our best to ensure that any data that may be in memory for the application to function is only held in memory for as long as you need it and that memory is cleaned up whenever the application is locked. We consider the application's encrypted data to be completely safe while the application is in a locked state.

Q: What do I do if I don't recognize a new device logging into Bitwarden?

A: If the IP address of a new device doesn't match any known IP addresses (home network, work network, mobile network, and so on), change your master password and make sure two-step login is enabled for your account. You should also deauthorize sessions from the **Account settings** page of your web vault to force logout on all devices. If you think your vault items might be compromised, you should change your passwords.

Q: What is Bitwarden compliant with? What certifications do you have?

A: Bitwarden is compliant with the following policies:

- **GDPR.** Read more here.
- **CCPA.** Read more here.
- **HIPAA.** Read more here.
- **SOC 2 Type 2.** Read more here.
- **SOC 3.** Read more here.

For more information, please visit our Security and Compliance page.

Q: How does Bitwarden meet European compliance requirements?

A: Bitwarden is GDPR-compliant and uses approved information transfer mechanisms including EU Standard Contractual Clauses (SCCs) pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. For business and enterprise customers, Bitwarden can execute the Bitwarden Data Protection Agreement.

Bitwarden cloud servers are currently hosted on Microsoft Azure within the United States and the European Union. Today Bitwarden serves millions of users, including government and enterprise customers throughout Europe and the world, with this infrastructure.

For customers who need full control over data residency, Bitwarden can alternatively be privately hosted on your own infrastructure.

All vault data stored in Bitwarden, regardless if on the cloud or self-hosted, is end-to-end encrypted and not accessible by anyone except the Bitwarden user. With this end-to-end, zero knowledge encryption architecture even Bitwarden cannot access your data.

For a full list of Bitwarden security and compliance certifications, please visit https://bitwarden.com/compliance/.

Q: What third-party services, libraries or identifiers are used in my Bitwarden account?

A: In the mobile apps, Firebase Cloud Messaging (often mistaken for a tracker) is used only for push notifications related to sync and performs absolutely no tracking functions. Microsoft Visual Studio App Center is used for crash reporting on a range of mobile devices. In the web vault, Stripe and PayPal scripts are used for payment processing only on payment pages.

For those who prefer to exclude all 3rd party communication, Firebase and Microsoft Visual Studio App Center are removed completely from the F-Droid build. Additionally, turning off push notifications on a self-hosted Bitwarden server will disable using the push relay server.

The Bitwarden Android application also includes the ability to disable crash reporting under Settings.

Bitwarden takes user security and privacy seriously. Bitwarden maintains secure, end-to-end encryption with zero knowledge of your encryption key. As a company focused on open source, we invite anyone to review our library implementations at any time on GitHub.

Q: How do I require two-step login for my Bitwarden organization?

A: Use an enterprise policy, included with an Enterprise organization subscription. You can also enable Duo MFA integration to enforce 2FA/MFA for your organization. For more information, see Two-step Login via Duo.

Q: What are the certificate options for a self-hosted instance of Bitwarden?

A: See Certificate Options for a complete list and instructions.

Q: How does Bitwarden vet code changes?

A: Confidence in the security of our systems is of utmost important to Bitwarden. All proposed code changes are reviewed by one or more non-author members of the team before they can be merged into any codebase. All code goes through multiple test and QA environments prior to production. Bitwarden has implemented a SOC2 report to audit and validate our internal procedures. As mentioned in the report, our team is subject to rigorous background check and thorough interview processes. Bitwarden, being an open-source product, also welcomes peer-review of our code at any point. The team at Bitwarden strives to do everything we can to keep our users comfortable, and keeping their data secure.

Q: How long does Bitwarden cache session information?

A: Great question! The answer depends on the particular piece of information and client application:

- Offline vault sessions will expire after 30 days.
  - **Except** for mobile client applications, which will expire after 90 days.
- Two-step login **Remember Me** selections will expire after 30 days.
- Directory Connector sync cache will be cleared after 30 days.
- Organization invites will expire after 5 days. Self-hosted customers can configure this using an environment variable.

Q: How do I validate the checksum of a Bitwarden app?

A: Checksums can currently be validated for Password Manager desktop apps, Android mobile apps, and CLI clients:

⇒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.

Q: How do I make a security disclosure or report to Bitwarden?

A: Bitwarden believes that working with security researchers across the globe is crucial to keeping our users safe. If you believe you've found a security issue in our product or service, we encourage you to please submit a report through our HackerOne Program. We welcome working with you to resolve the issue promptly. Learn more about our disclosure policy.

Q: How can I protect my Bitwarden account from brute-force attacks?

A: A brute-force attack is when a malicious actor cycles through a combination of weak and short passwords in an attempt to gain access to your account. Bitwarden offers a few ways you can protect yourself from these potential attacks:

- Have a long and unique master password. Bitwarden requires a 12 character minimum to increase account security.
- Set up 2FA on all Bitwarden accounts to add an additional layer of security.
- Bitwarden will require CAPTCHA verification after 9 failed login attempts from an unknown device.

Questions regarding specific client apps

Q: What data does Bitwarden use from client applications?

A: Bitwarden uses administrative data to provide the Bitwarden service to you. As indicated by some **App Privacy** reports, users provide the following information on account creation:

- Your name (optional).
- Your email address (used for email verification, account administration, and communication between you and Bitwarden).

Additionally, a **Bitwarden-generated** device-specific GUID (sometimes referred to as a Device ID) is assigned to your device. This GUID is used to alert you when a new device logs into your vault.

Q: Can you explain electron app security?

A: An often shared article suggests a flaw with electron apps, however the referenced attack requires a user to have a compromised machine, which of course would allow a malicious attacker to compromise data on that machine. As long as you have no reason to believe the device you are using has been compromised, your data is safe.

Q: How does Bitwarden secure browser extensions?

A: Extensions are safe to use if they are developed correctly. Due to the nature of how browser extensions work there is always a chance for a bug to arise. We take extreme care and caution when we are developing our extensions and add-ons, we keep our eyes and ears out for anything going on in the industry, and we conduct security audits to keep many eyes on everything.

Q: What is the Browser extension asking permission for?

A: On installation, the browser extension will ask permission to access your clipboard in order to use the scheduled clipboard clear function (accessed in the **Options** menu).

When this **optional feature** is enabled, clipboard clear will clear any Bitwarden entries made by or filled on a configurable interval. Access to the clipboard allows Bitwarden to do this without removing a clipboard item not associated from the Bitwarden application by checking the last-copied item against the last-copied item from your vault. Please note, this feature is **off by default**.

Q: What app permissions are asked for by the mobile app?

A: Bitwarden Android and iOS apps may ask for the following permissions while you are using the app:

Permission	Reason
Allow Bitwarden to take pictures and record video?	To scan QR codes for two-step login or Bitwarden authenticator.
Allow Bitwarden to access photos and media on your device?	To create attachments or Sends from a file saved on your device.

Additional basic permissions required by Bitwarden are listed in the Google Play store.

Q: Why does the browser extension need nativeMessaging permission?

A: Version 1.48.0 of the browser extension enables biometric unlock for browser extensions.

This permission, also known as `nativeMessaging`, is safe to accept and allows the browser extension to communicate with the Bitwarden desktop app, which is required to enabled unlock with biometrics.

Note that when your browser updates to this version, you may be asked to accept a new permission called "communicate with cooperating native applications" (in Chromium-based browsers), or "exchange messages with programs other than Firefox." If you don't accept this permission, the extension will remain disabled.

Q: Is Bitwarden FIPS compliant?

A: Bitwarden uses FIPS 140 compliant libraries and cryptography, and most FIPS 140 installations of Bitwarden leverage the self-hosting option to make evaluations (for example, Cyber Maturity Model Certification) easier. The Bitwarden platform has not performed any FIPS certifications at this time. Inquiries are welcome via the contact us page.

Q: Can I restrict access to Bitwarden to certain devices?

A: Using self-hosting, you can use custom firewall and NGINX configurations as well as VPN/VLAN access control to determine the device types and/or network layer access for your Bitwarden instance. You may also use other tools such as device-level certificates to control specific device access to the Bitwarden instance as well.

Q: Does Bitwarden have a portable application?

A: Yes! The Bitwarden desktop app is available for Windows as a portable `.exe` that can be downloaded here. The portable app is well suited to **always-offline** environments or scenarios where automatic updating of the app is not desired. The portable app **will not update itself**.

Q: Will site access options interfere with the Bitwarden browser extension?

A: Site access settings for the Bitwarden browser extension must be set to **On all sites**, or to **On specific sites** with the Bitwarden server added to the list, in order for the browser extension to work properly. Setting site access to **On click** will restrict Bitwarden's ability to fetch data from the Bitwarden server, which is fundamentally required to save or update credentials.