

SECURITY

Storage

A decorative graphic consisting of numerous thin, light gray wavy lines that create a sense of motion and depth across the middle section of the page.

View in the help center:

<https://bitwarden.com/help/data-storage/>

Storage

This article describes where Bitwarden stores your vault data and administrative data.

Bitwarden **always** encrypts and/or hashes your data on your local device before anything is sent to cloud servers for storage. **Bitwarden servers are only used for storing encrypted data.** For more information, see [Encryption](#).

Some encrypted data, including a user's protected symmetric key and master password hash, are also transparently encrypted at rest by the application, meaning they're encrypted and decrypted again as they flow in and out of the Bitwarden database.

Bitwarden additionally uses Azure transparent data encryption (TDE) to protect against the threat of malicious offline activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest.

On Bitwarden servers

Bitwarden processes and stores all vault data securely in the [Microsoft Azure Cloud](#) in the [US](#) or [EU](#) using services that are managed by the team at Microsoft. Since Bitwarden only uses service offerings provided by Azure, there is no server infrastructure to manage and maintain. All uptime, scalability, security updates, and guarantees are backed by Microsoft and their cloud infrastructure. Review the [Microsoft Azure Compliance Offerings](#) documentation for more detail.

Bitwarden maintains point-in-time restore (PITR) policies for disaster recovery. The functionality leveraged by Bitwarden for this purpose **does not** involve creating or storing a BACPAC or otherwise moveable backup file, but instead allows for disaster recovery by reverse-processing transactional logs to make the database consistent with a selected point-in-time (see [Microsoft's documentation](#)). Bitwarden has configured a strict 7-day retention policy for PITR and a policy of no long-term retention. This functionality is for **disaster recovery purposes only**, users and organizations are responsible for creating and securely storing backups of their own vault data. Blob-stored data, specifically attachments and Send files, are not subject to PITR functionality and are irrecoverable once deleted from Bitwarden.

Don't trust Bitwarden servers? 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](#).

On your local machine

Data that is stored on your computer/device is encrypted and only decrypted when you unlock your vault. Decrypted data is stored **in memory** only and is **never written to persistent storage**. Encrypted data is stored in the following locations at rest:

Desktop app

- Windows
 - Standard installation: `%AppData%\Bitwarden`
 - Microsoft Store installation: `%LocalAppData%\Packages\8bitSolutionsLLC.bitwardendesktop_h4e712dmw3xyy\LocalCache\Roaming\Bitwarden`
 - Portable: `.\bitwarden-appdata`
- macOS
 - Standard installations: `~/Library/Application Support/Bitwarden`
 - Mac App Store: `~/Library/Containers/com.bitwarden.desktop/Data/Library/Application Support/Bitwarden`
- Linux
 - Standard installations: `~/.config/Bitwarden`

- Flatpak: `~/.var/app/com.bitwarden.desktop/`
- Snap: `~/snap/bitwarden/current/.config/Bitwarden`

💡 Tip

You can override the storage location for your Bitwarden desktop app data by setting the `BITWARDEN_APPDATA_DIR` environment variable to an absolute path.

Browser extension

- Windows
 - Chrome: `%LocalAppData%\Google\Chrome\User Data\Default\Local Extension Settings\nngceckbapebfimlniiiahkandclblb`
 - Edge: `%LocalAppData%\Microsoft\Edge\User Data\Default\Local Extension Settings\jbkfoedolllekgbhcboahfnbanhhlh`
 - Brave: `%LocalAppData%\BraveSoftware\Brave-browser\User Data\Default\Local Extension Settings\nngceckbapebfimlniiiahkandclblb`
 - Vivaldi: `%LocalAppData%\Vivaldi\User Data\Default\Local Extension Settings\nngceckbapebfimlniiiahkandclblb`

💡 Tip

In Chromium browsers, `Default` represents the name of a browser profile. If you've installed Bitwarden under a different profile, substitute that profile's name in the path.

- Firefox: `%AppData%\Mozilla\Firefox\Profiles\your_profile\storage\default\moz-extension+++[UUID]^userContextId=[integer]`
- Opera: `%AppData%\Opera Software\Opera Stable\Local Extension Settings\ccnckbpmacehanjmeomladnmlffdjgn`

• macOS

- Chrome: `~/Library/Application Support/Google/Chrome/Default/Local Extension Settings/nngceckbapebfimlniiiahkandclblb`
- Edge: `~/Library/Application Support/Microsoft Edge/Default/Local Extension Settings/jbkfoedolllekgbhcboahfnbanhhlh`

💡 Tip

In Chromium browsers, `Default` represents the name of a browser profile. If you've installed Bitwarden under a different profile, substitute that profile's name in the path.

- Firefox: `~/Library/Application Support/Firefox/Profiles/your_profile/storage/default/moz-extension+++[UUID]^userContextID=[integer]`
- Safari: `~/Library/Safari/Databases`

- Linux
 - Chrome: `~/.config/google-chrome/Default/Local Extension Settings/nngceckbapebfimlniiahkandclblb`
 - Edge: `~/.config/microsoft-edge/Default/Local Extension Settings/jbkfoedolllekgbhcboahfnbanhhlh`

💡 Tip

In Chromium browsers, `Default` represents the name of a browser profile. If you've installed Bitwarden under a different profile, substitute that profile's name in the path.

- Firefox: `~/.mozilla/firefox/your_profile/storage/default/moz-extension+++[UUID]^userContextID=[integer]`

📌 Note

To enhance security, Firefox uses universally unique identifiers (UUIDs) within extension storage folder names. In the address bar, navigate to `about:debugging#/runtime/this-firefox` to locate your Bitwarden extension UUID. Replace `[UUID]` with that value.

Firefox also allows users to customize where to store their profiles (and thus local Bitwarden extension data). The location specified above is the default.

Mobile

- iOS: app group for `group.com.8bit.bitwarden`
- Android: `/data/data/com.x8bit.bitwarden/`

Web

- Chrome: **☰ Menu → More Tools → Developer Tools**, then select the **Application → Local storage**.
- Safari: **Develop → Show Web Inspector → Storage → Local Storage**.
- Firefox: **☰ Menu → More tools → Web Developer Tools → Storage → Local Storage**.
- Edge: **⋮ Menu → More tools → Developer tools → Application → Local storage**.
- Opera:
 - Windows: **Menu → Developer → Developer Tools → Application → Local storage**.
 - MacOS: **Developer → Developer Tools → Application → Local storage**.

CLI

- Windows: `%AppData%\Bitwarden CLI`
- macOS: `~/Library/Application Support/Bitwarden CLI`
- Linux: `~/.config/Bitwarden CLI`

 **Tip**

You can override the storage location for your Bitwarden CLI app data by setting the `BITWARDENCLI_APPDATA_DIR` environment variable to an absolute path.