

SECURITY

Account Encryption Key

View in the help center:
<https://bitwarden.com/help/account-encryption-key/>

Account Encryption Key

Each unique Bitwarden account has an encryption key which is used to encrypt all vault data.

Rotate your encryption key

Warning

Rotating your encryption key is a potentially dangerous operation. Please read this section thoroughly to understand the full ramifications of doing so.

Rotating your account's encryption key generates a new encryption key that is used to re-encrypt all vault data. You should consider rotating your encryption key if your account has been compromised in such a way that someone has obtained your encryption key.

Before rotating

Before rotating, you should take the following actions to protect against potential data loss or corruption.

Re-create any account backup exports

If you are using Account backup [encrypted exports](#) to store long-term secure backups, you should immediately re-create the encrypted export of your vault data using the new encryption key.

Account backup encrypted exports use your encryption key to encrypt **and decrypt** your vault data, meaning that a rotated encryption key will not be able to decrypt an export created with the "stale" (prior-to-rotation) key.

Log out of client applications

Before you rotate an encryption key, we recommend you log out of any logged-in sessions on Bitwarden client applications (desktop app, browser extension, mobile app, and so on). Logging out of client applications in this way will prevent sessions from using the "stale" (prior-to-rotation) encryption key. After doing so, logging back in as normal will use the new encryption key.

Making changes in a session with a "stale" encryption key will cause data corruption that will make your data unrecoverable.

Warning

We recommend creating a vault backup prior to rotating your account encryption key. To learn more about vault exports and what items are included, see [Export Vault Data](#).

How to rotate your encryption key

To rotate your account encryption key:

1. In the web app, navigate to **Settings** → **Security** → **Master password**:

The screenshot shows the Bitwarden web interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, My account, Security (highlighted), Preferences, Domain rules, Emergency access, and Free Bitwarden Famili... At the top right of the main content area, there is a 'Security' header, a grid icon, and a 'BW' profile icon. Below the header are three tabs: 'Master password' (selected), 'Two-step login', and 'Keys'. The main heading is 'Change master password'. A yellow warning box states: 'Warning: Proceeding will log you out of your current session, requiring you to log back in. Active sessions on other devices may continue to remain active for up to one hour.' Below this are three input fields: 'Current master password', 'New master password', and 'Confirm new master password'. A note reads: 'Important: Your master password cannot be recovered if you forget it! 12 character minimum'. There are two checkboxes: 'Check known data breaches for this password' (checked) and 'Also rotate my account's encryption key' (unchecked). Below these is a 'New master password hint (optional)' input field. A blue 'Change master password' button is at the bottom. At the very bottom, there is a 'Log in with passkey' section with 'Off' and 'Beta' buttons.

Master password settings

2. Enter your **Current master password** and create/confirm a **New master password**.

Tip

If you don't want to change your master password and only rotate your account encryption key, you can enter your current master password in the **New** fields to prevent it from changing.

3. Check the **Also rotate my account's encryption key** checkbox and accept the dialog.

4. Select the **Change master password** button.