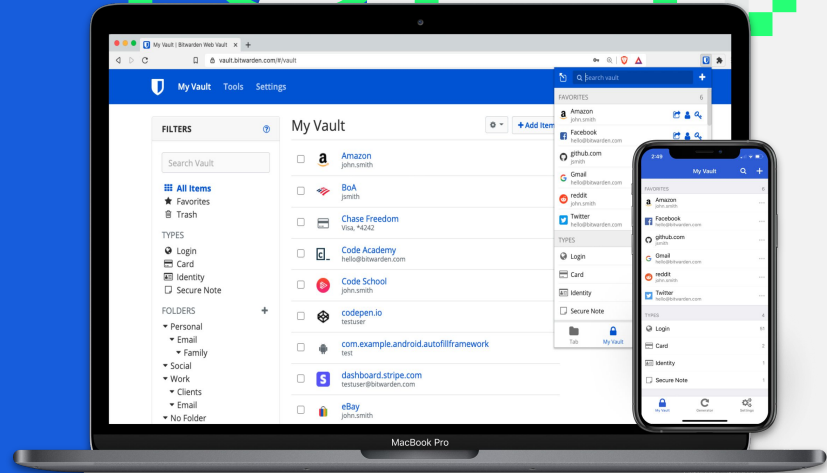




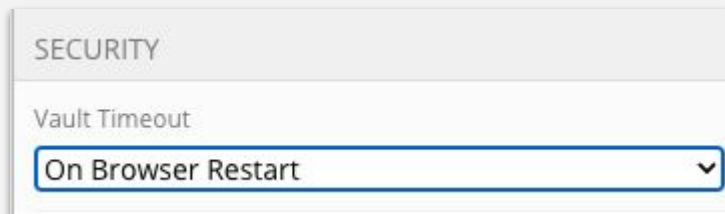
Vault Timeout Settings

Bitwarden Essential Series



Vault Timeout

- To keep your Bitwarden Vault secure, it will time out after a user-specified period of time.

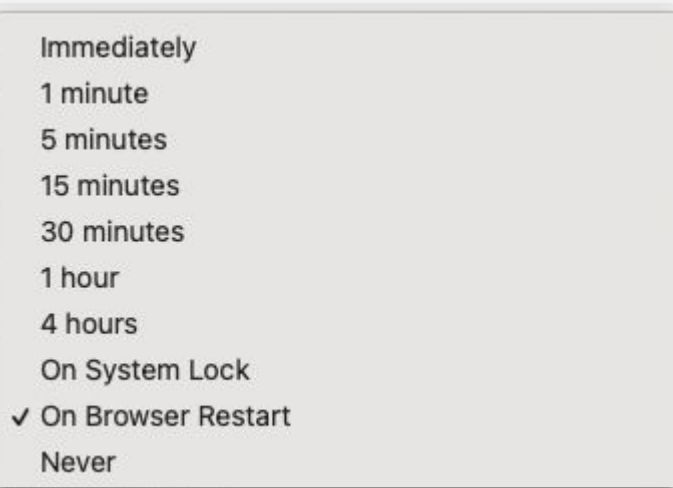


SECURITY

Vault Timeout

On Browser Restart

A screenshot of the Bitwarden Security settings panel. The 'SECURITY' section is highlighted. Underneath, the 'Vault Timeout' setting is shown as a dropdown menu. The current selection is 'On Browser Restart', which is highlighted with a blue border and a small downward arrow on the right side.



Immediately
1 minute
5 minutes
15 minutes
30 minutes
1 hour
4 hours
On System Lock
✓ On Browser Restart
Never

A screenshot of the Bitwarden Vault Timeout dropdown menu. The menu is open, showing a list of options. The 'On Browser Restart' option is selected, indicated by a checkmark to its left. The options are: Immediately, 1 minute, 5 minutes, 15 minutes, 30 minutes, 1 hour, 4 hours, On System Lock, ✓ On Browser Restart, and Never.

Vault Timeout: Maximum Duration

- Enabling the **Vault Timeout** policy will implement a maximum Vault Timeout duration for all members of your Organization.
- This policy applies the timeout restriction to all client applications (Mobile, Desktop, Browser Extension, etc.)

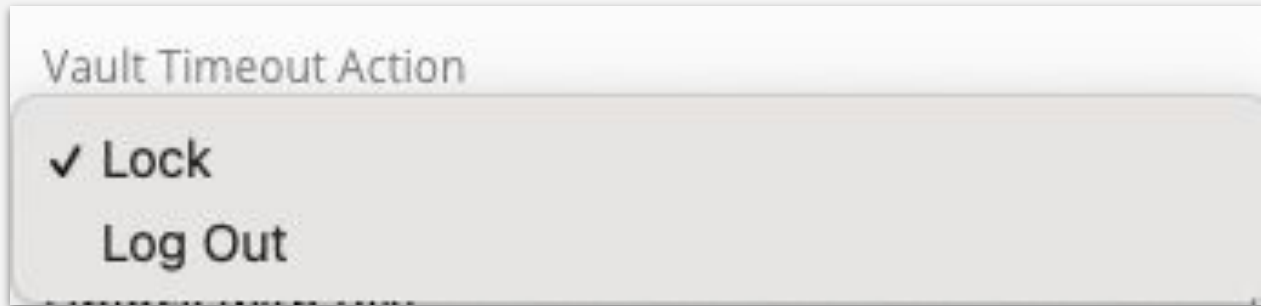
Note

The **Single Organization** policy must be enabled before activating this policy.

As a result, you must disable the **Vault Timeout** policy before you can disable the **Single Organization** policy.

Vault Timeout: Options

- Once the timeout has been reached, you can specify the behavior of your Vault.
- Options for **Lock** or **Log Out** are available.



Vault Timeout: Lock

- **Locking** your vault is the default Vault Timeout Action.
- **Locking** your vault allows you to access your data again by doing one of the following, depending on the client:
 - Entering your **Master Password** (available on all clients)
 - Entering a user-created **PIN** (available on all clients except CLI)
 - Authenticating via **Biometrics** (available with compatible hardware on Desktop, Browser, and Mobile)
- No internet connection is required to access a **Locked** vault.

Vault Timeout: Log Out

- **Log Out** offers additional protection for your vault.
- When the timeout period has occurred, the client application is logged out, removing the encrypted data from your device.
- When logging back into a vault that has **logged out** you will need to provide:
 - Your Bitwarden **Email** address
 - Your **Master Password**
 - Your **two-step login method** - unless you have selected *remember me* previously.
- Notes for logging in:
 - If you normally use **Login with SSO**, you will need to authenticate via SSO.
 - If you have previously selected *remember me* for a device, you will need to deauthorize sessions within your Web Vault to receive **two-step** prompts.

Web and Browser Extension Timeouts

- **Web Vault and Browser Extension** are dependent on your web browser.
 - **If you refresh your browser**, your Web Vault will lock.
Refreshing will not affect a Browser Extension
 - **If you close your browser tab**, you will be logged out of your Web Vault.
Closing a single tab will not affect a Browser Extension.
 - **If you close your browser**, you will be logged out of **both** your Web Vault and Browser Extension.

Tip

If you're using a Browser Extension, you can bypass this by enabling the **Unlock with PIN** option and unchecking the **Lock with master password on browser restart** checkbox.

Reference: Unlock Options per Client

Vault Timeout, Unlock, and Clear Clipboard Options

Settings	Choices	Desktop	Browser Extension	Web Vault	Mobile
Vault Timeout	Options by client app	✓	✓	✓	✓
Vault Timeout Action	Lock or Log Out	✓	✓	✓	✓
Unlock with PIN Code		✓	✓	✓	✓
Unlock with Biometrics	Options by device	✓	✓		✓
Settings > Options					
Clear Clipboard	10 sec to 5 min	✓	✓		✓

Visit [Bitwarden.com/help](https://bitwarden.com/help)
for more information

