Password Manager CLI: User Manual

Contents

Master Password & Initialization

When you launch the Password Manager:

- The application will prompt for a vault name.
- If a vault with the given name exists, the user will be prompted to enter the vault's master password to enter.
- If no vault with the given name exists, the application will prompt the vault creation sequence immediately.
- The user will be asked to create a master password and confirm it.

If at any point the user wishes to exit the initialization sequence (doesn't want to create a vault under the given name, doesn't want to enter the existing vault, etc.), a keyboard interrupt (for example, Ctrl+C) will abort the application.

Vault Layout

- Password Manager's default vault storage path:

    <your home directory>/.passman/vaults/

- Inside of each of the vaults resides the vault's metadata (*vault.meta*), action log (*audit.log*) recording important events, and the vault's contents (*vault.bin*).
- The *.passman* directory and its contents can be accessed only by the home directory user and the root user, ensuring that your credentials are stored safely and tamper-free.

Inactivity Timer

If the user performs no input for 60 seconds:

- All secrets are wiped
- Application exits with logout message

Usage Guide

After unlocking, you will see:

```
Password Manager CLI - Menu:


1) List credentials

2) Add credential (+New)

3) Update credential

4) Delete credential

5) Reveal credential (logs action)

6) Copy credential

7) Quit

8) Delete current vault


Scroll up to see previous operation results.

>
```

Each startup will result in a log entry in the passman default log file. The input field expects to receive the number corresponding to the option you want to trigger. Each option is described below.

1) List credentials

Shows all saved credential labels:

```
Stored credentials:

  - gmail

  - github

  - mybank
```

2) Add credential (+New)

Prompts for:

- Label
- Username
- Password
- Notes (optional)

The password manager will encrypt the new credential using the master key, store it in the vault and log the event securely.

3) Update credential

Prompts for:

- Credential label
- Old password (verifies access)
- New password

The tool will load and decrypt the entry, verify the old password, update fields, and re-encrypt and overwrite the entry.

4) Delete credential

Prompts for:

- Label
- Confirmation via master password

If the password is correct, the entries are securely deleted from the vault.

5) Reveal credential (logs action)

Prompts for the credential label.

Then:

- Decrypts that entry
- Prints username, password and any corresponding notes

Use in private environments only.

6) Copy credential

Your password is copied to the OS clipboard for 15 seconds. After the timer expires, the clipboard is cleared.

Password Manager will warn you if Windows Clipboard History is enabled (risk of persistence).

7) Quit

Securely wipes master key, any decrypted data and session metadata – then exits.

8) Delete current vault

A destructive operation requiring:

- The user to type "DELETE" exactly
- The user to enter master password again

If confirmed, all encrypted entries are securely erased, vault.meta is wiped, audit.log is wiped, session keys are wiped – then exits.

Audit Logging

Password Manager logs:

- Add, update, delete actions
- Failed attempts
- Password reveals
- Clipboard copies
- Any security violations

Log entries include:

- Timestamp
- Event type
- Outcome
- Context fields

Audit logs contain only metadata. Secrets are never logged.

Backup and Restore

To back up your vault:

```
cp -r <your home directory>/.passman/vaults/<vault folder> <backup location>
```

To restore:

```
cp -r <backup> <your home directory>/.passman/vaults/
```

Troubleshooting

"Master password incorrect"

Ensure you are using the exact password used during initialization.

"Cannot read entry"

Entry file may be corrupted; check audit log.

"Clipboard clear didn't work"

Some Linux clipboard managers retain history. Windows "Clipboard History" keeps persistent snapshots.

"App logs me out too quickly"

The timeout is currently fixed at **60 seconds**. You can change the constant in the source code if needed.