Personal Password Manager in the Private Cloud

The Issue

- Passwords are either...

  - Too easy to guess

  - Too easy to bruteforce

- Or…

  - Too difficult to remember

Use a password manager

- Trusting someone else with your data

  - Synchronization by upload to remote server

- No synchronization of data

  - Stored on the local device

Hosting A Solution Yourself

- Private Cloud

- Not that expensive anymore

  - Small low-powered devices such as
    Raspberry Pi

- Complete control of data

What do we need?

(excerpt from the complete list of requirements)

- Distributed password database

- Multi-user support

  - Albeit solution should be aimed at individuals

- Password organization, in multiple levels

- Password sharing (for convenience)

- Passwords only ever appear in clear text client-side

- Auditing

- Two-factor authentication

And most importantly…

Something the user **wants** to use!

So… What already exists?

Reviewed Commercially Available Tools

- In-Browser Password Managers

- LastPass, and Similar Solutions

- KeePass, and Similar Solutions

- Rattic

- Encryptr

- Vault

- TeamPasswordManager

… But none fulfill the requirements in a satisfactory way!

Most are aimed at teams

Solution: Rattic DB

Good: Easy understand UI

Bad: Rattic is clearly aimed at teams. If the user wants to have passwords for him or herself, there needs to be a group with ONLY that user in, and those personal passwords then belong to that group.
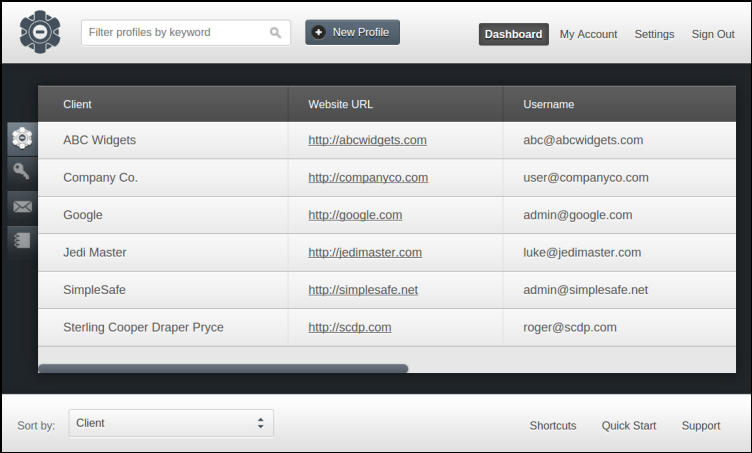
Most are aimed at teams
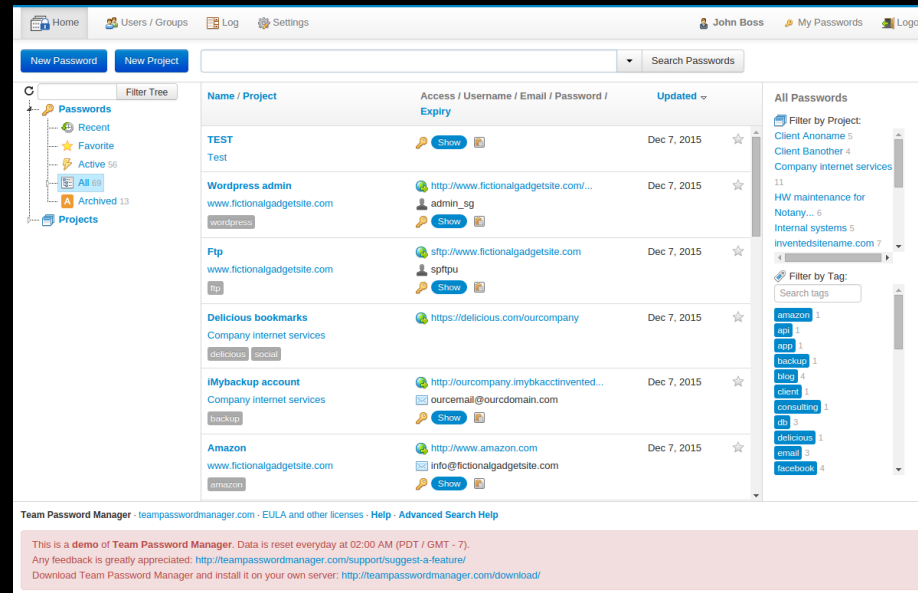
Solution: TeamPasswordManager

Good: Structuring is actually made logically, as a "tree"

Bad: Again, same thing as rattic: Teams. Passwords belong to teams instead of individual users.

Some have simply been discontinued since…

"…, we have made the tough decision to remove SimpleSafe for sale and cease to actively develop the product."

Solution: SimpleSafe

They have simply discontinued sale and development of the solution, during the master project.

Some lack organization
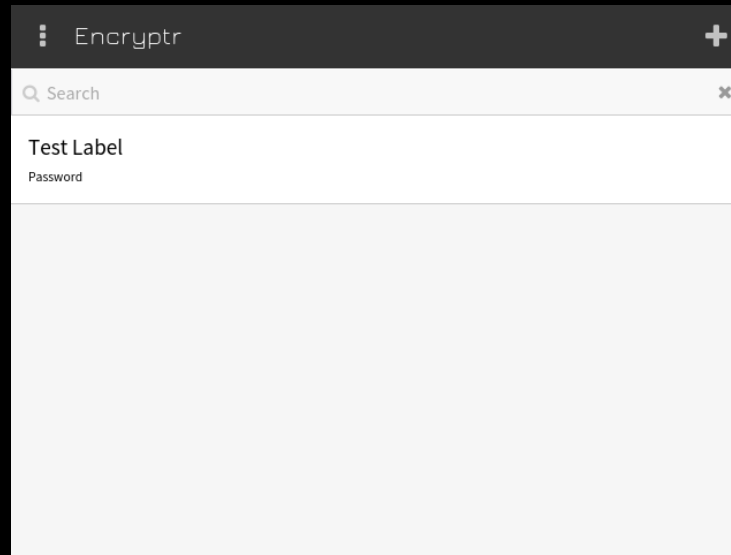
Solution: Encryptr

Good: Extremely sleek UI

Bad: NO organization what so ever. Passwords are stored in a single list.

Some invent their own organization
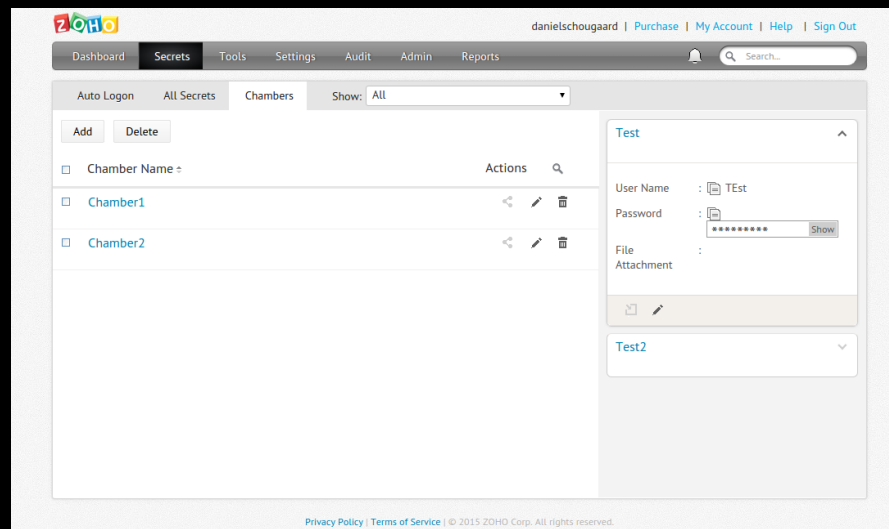
Solution: Vault

Bad: Chambers are not intuitive. Clunky, difficult.

Some doesn't even tell which platform it runs on
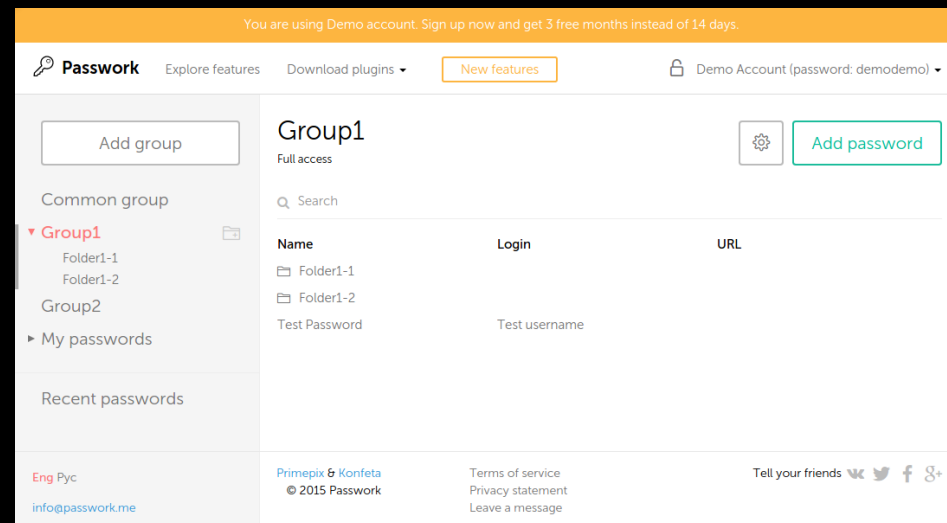
Solution: Passwork

Bad:
NO information regarding which platform it runs on

Their online demo was broken around half of the time
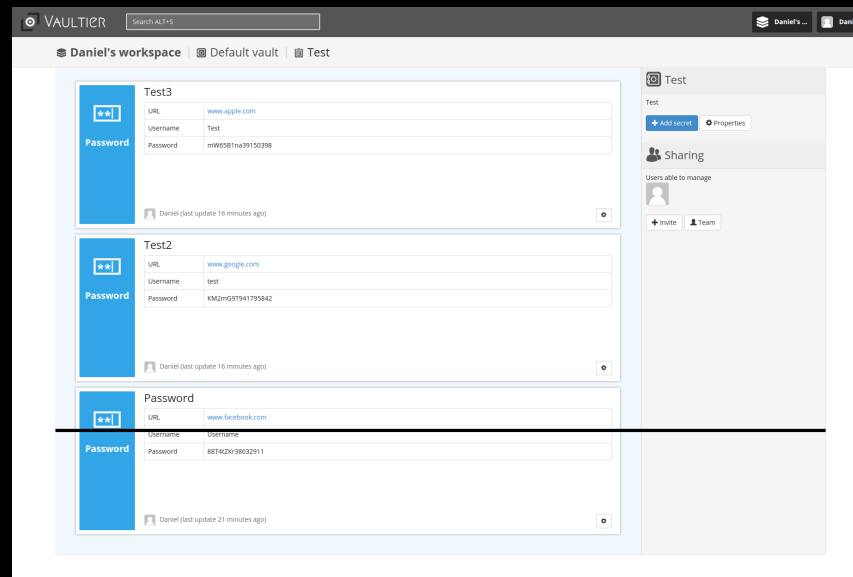
Solution: Vaultier.

The black line denotes where the buttom of a 1080p 24'' inch monitor is.

You can see 2-3 passwords at a time….. Imagine scrolling through just 10 passwords.

Some are WAY to complex
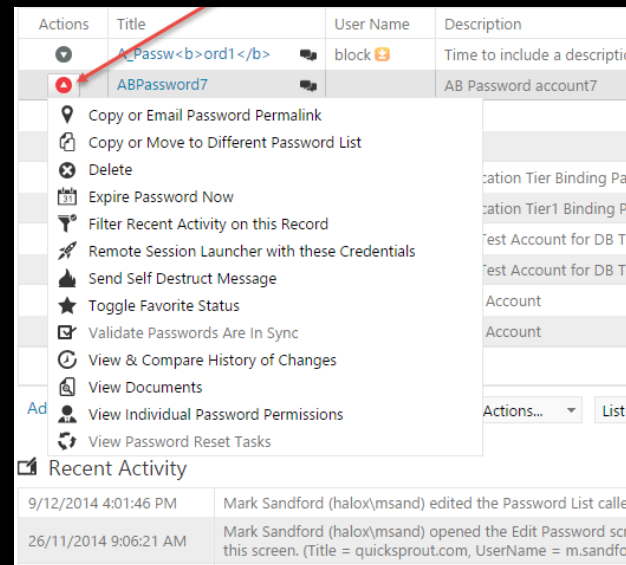
Solution: Passwordstate

Good: Probably a very good solution for enterprise uses.

Bad:
- FAR too complex for most scenarios involving a   private-cloud.
- Many enterprise features would simply end up not being used.
- Most users would be deterred from it, seeing that menu.

And some are just plain horrible

Solution: Simply Vault

Bad: If the implementation LOOKS sketchy, the user will THINK it is sketchy. And then the user simply wont be safe storing sensitive data in the soltion.

Reviewed Academic Solutions

- Tapas: Design, Implementation, and Usability Evaluation of a Password Manager

- Using CardSpace as a Password Manager & Implementing PassCard - a CardSpace-based Password Manager

- Stronger Password Authentication Using Browser Extensions

- Sesame: A Secure and Convenient Mobile Solution for Passwords

- All Your Browser-saved Passwords Could Belong to Us: A Security Analysis and a Cloud-based New Design

- Passpet: Convenient Password Management and Phishing Protection

- Cloud Based Manager Using Privacy-Preserved Biometrics

- A Password Manager that Doesn't Remember Passwords

- Password Management Using Doodles

- PALPAS -- PAssword Less PAssword Synchronization

- Cloud-based Storage-Free Browser-based Password Manager

- CredProxy

And the academics…?

Solution name (or paper name, if no name given)	Reason to dismissal
Tapas	Does not support multiple
CardSpace	Restricted to the Windows
PwDHash	Password derivation tool.
Sesame	Intended for smartphones, tablets, smart watches, and etc.
All your browser-saved	Relies on third party servers.
Passpet	Only works for website logins, in the browser.

And the academics…? Cont.

Solution name (or paper name, if no name given)	Reason to dismissal
Cloud password manager using privacy-preserved biometrics.	Not all devices has biometric inputs.
Versipass	Low amount of permutations and im-practical.
Doodles	Does not support multiple devices
PALPAS	Assumed dependency on third party servers and limited to native applications

And the academics…? Cont.

Solution name (or paper name, if no name given)	Reason to dismissal
Toward a secure and usable cloud-based password manager for web	Only works for website logins, in the browser.
CredProxy	Ambiguity in implementation details, no support for multiple

Summing up the academics

- None of them suggest a "full" solution

  - Either there is no multi-device support

  - Or..

  - They solve it by uploading it to a server the user does not control

- Highly platform dependant solutions

So unfortunately….

… None of them fit the bill

So… What then?

- We need something new

- Something better

- Something that actually fulfills the requirements