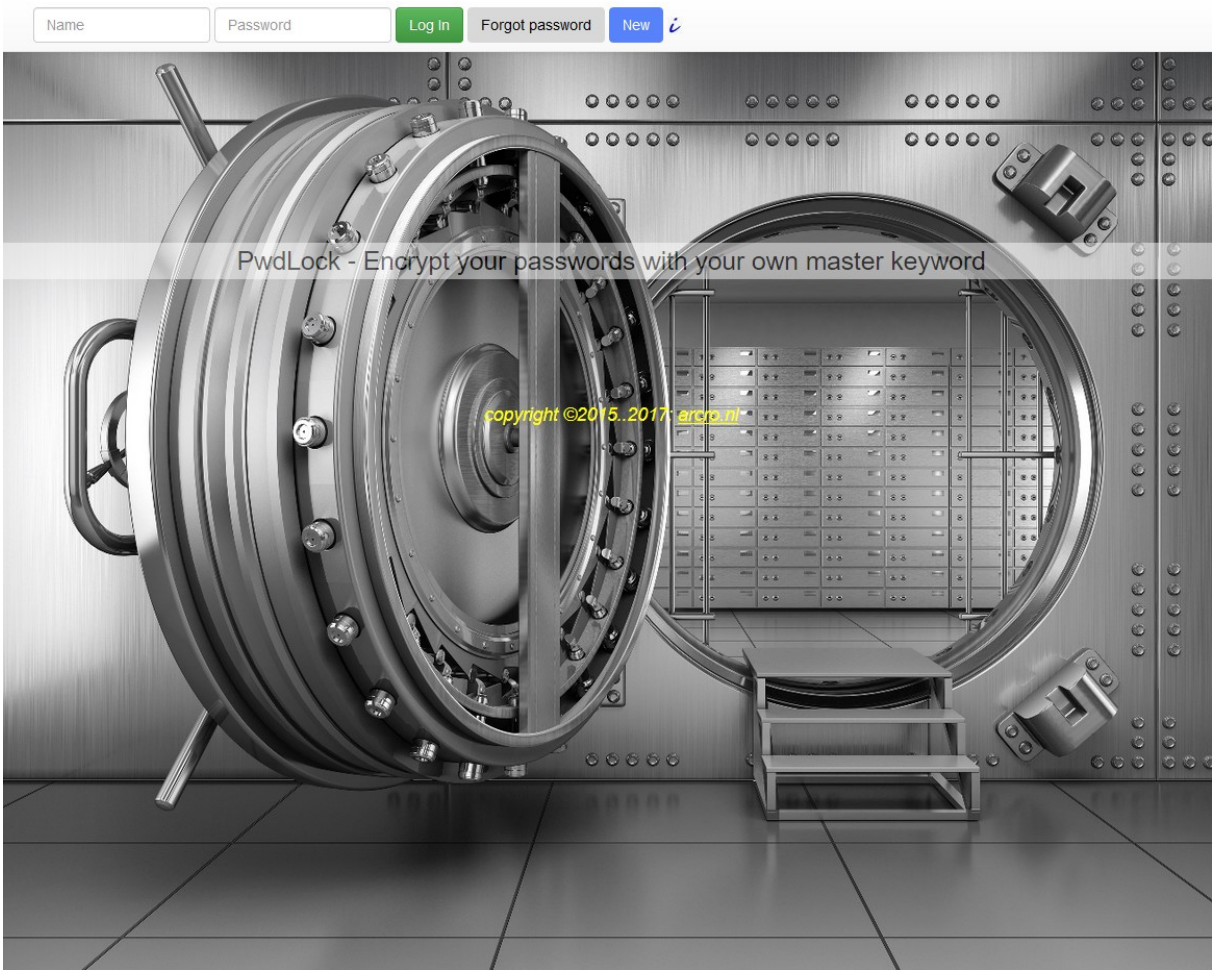
Manual for the password locker *pwdLock*



The password locker lets you store your precious passwords in the cloud, needing only two passwords to remember: your login password and a master keyword.

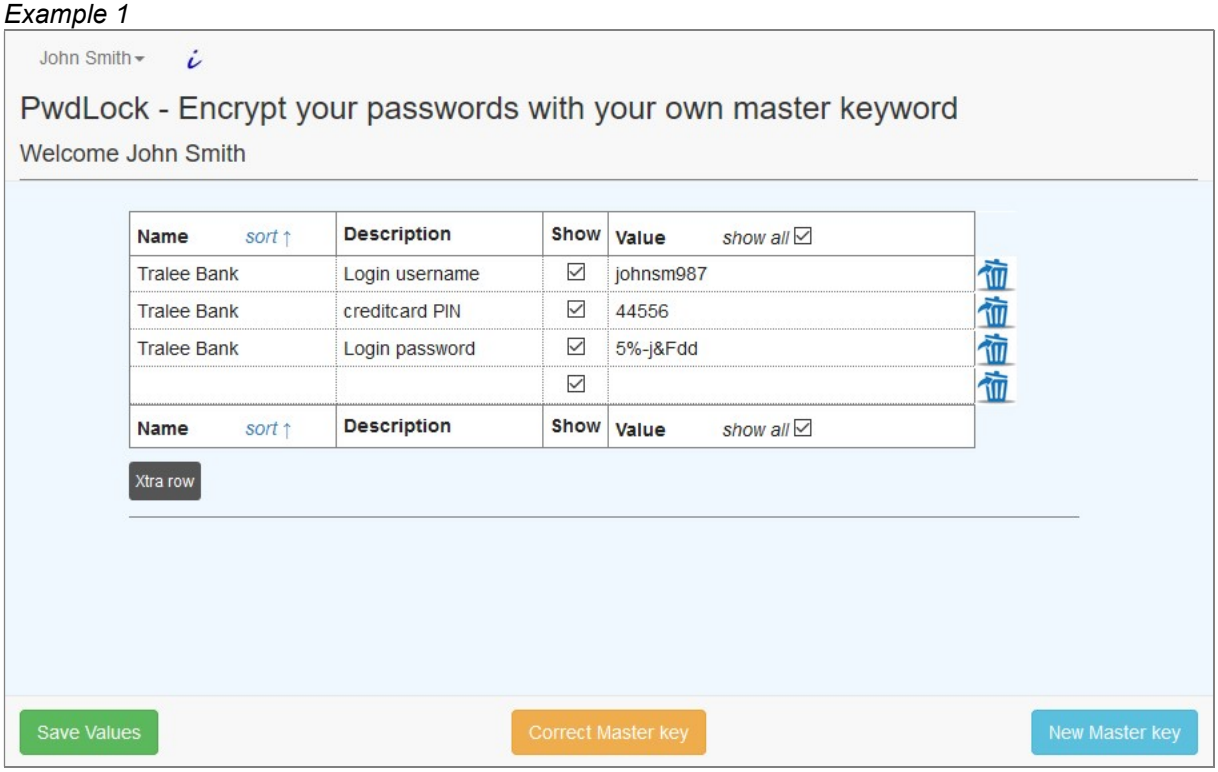
This has great advantages compared to a local storage:
- You can access your passwords everywhere with your smartphone, tablet or computer
- No need to make backups from locally stored data.

It is safe too: your passwords are encrypted with your master keyword and the master keyword is not stored (*never*) on your computer or elsewhere (the encryption takes place on your computer and not on the server where your encrypted passwords are saved).

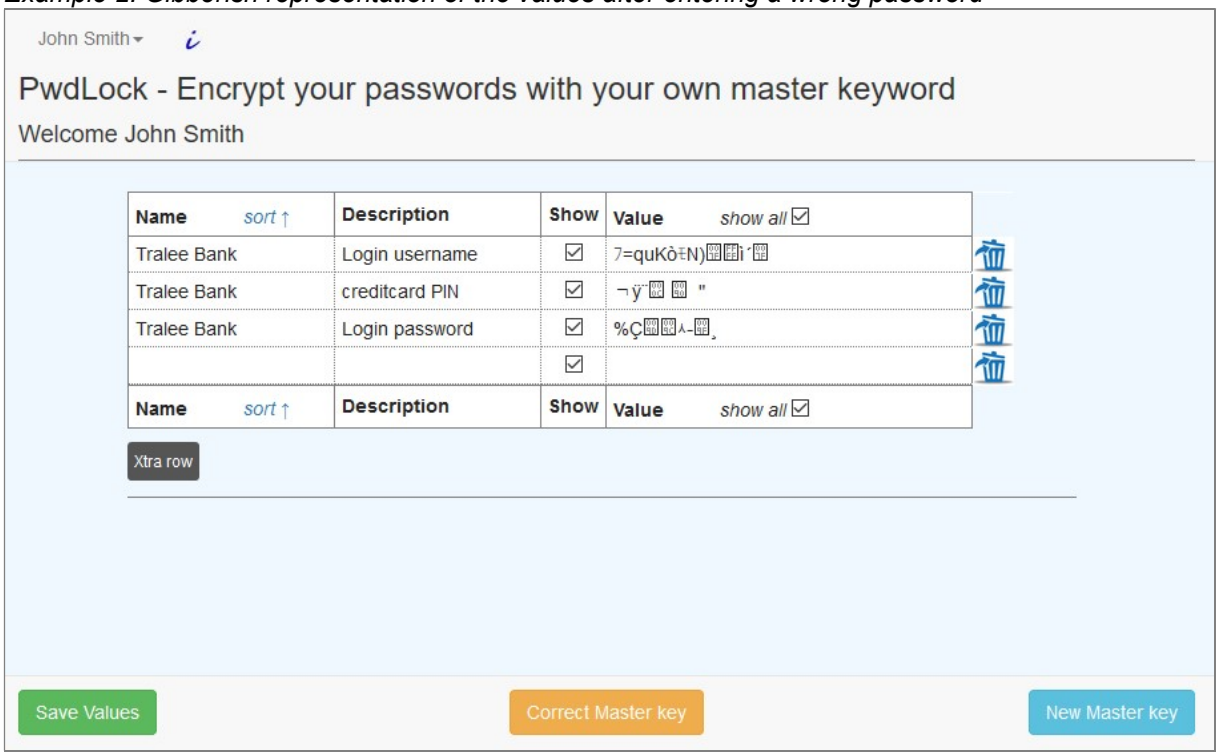
The complete manual has only 4 steps:
1. Log in with your username and password
2. Enter your Master keyword (the first time you use the program you think of a Master keyword yourself; it must contain at least 8 characters, with at least 1 uppercase, 1 lowercase letter and 1 digit.)
3. Fill in or edit the table (see example below); check the ‘show all’ box to see all the values and thus to ascertain you entered the right Master keyword! Instead you can check a ‘show’ box at an one or more lines to make only certain lines visible.
   if the values in the table only contain gibberish (like in example 2) you probably entered a wrong Master keyword.
   You can correct this by clicking the orange button ‘Correct Master key’.
4. Save the values and confirm it by entering your Login-password.

4a. You can change your Master keyword by clicking the blue button ‘*New Master Key*’

Example 1



Example 2: Gibberish representation of the values after entering a wrong password



Passwords can be **deleted** by clicking the wastebin-button at the right side of the line. The wastebin-button is then replaced by an undo-button, by which the deleted line can be retrieved.

You can **save your entered data** (names, descriptions and values) by clicking the green button '*Save values*'. Only the entries in the table are saved; deleted lines will be lost.

Note that when saving the values or changing the master keyword your login password is asked for authorization.

Terminate the program by clicking your name in the top left corner and choose Log Out

Change your login name and password by clicking your name in the top left corner and choose Change Login Data.

And this is how it works....

No, we are not going into technical details here, but for anyone interested in how it works, just click with your right mouse button on the screen and choose “View page source” or something similar, depending on your browser. And there it is, the full script (don’t forget to click on the two links in the last two lines of the script, that read:

```
<script type="text/javascript" src="js/pwdlock_main.js"></script>
<script type="text/javascript" src="js/tea.js"></script>
```

because that’s where the handling of the encrypting and sending to the server takes place).
The essence is that in your browser (and thus on your local computer) the encrypting takes place and is then forwarded to the server **without your Masterkey.** So there is no way of knowing on the server-side which encryption key was used. What’s more: even if someone obtained your login password, he or she cannot decipher the gibberish without having the Masterkey as well!