Password Manager: Using KeePassXC

v3 2022 Mar 28 Æpstein

1. Overview

Why have a password manager? The reason is to make it possible to have a different, unique password for every system that you use. These systems might be used for email, banking, shopping, medical or social media. If you use the same password for some or all of these systems, if someone were to discover this password, they could easily get access to information in all other systems that share this password. Therefore it is best to have a different password for each system.

In addition, a short password, like: 123456 is easy to remember, but it is also easy to "hack" or discover by someone else. A long and complicated password, such as: Jupitrs@70#RINGS is much safer for important systems (email, bank and medical accounts) as it has 16 alphanumeric & special characters, caps, misspelled words, etc.

A password manager is like a file that contains login names and passwords for all the various systems that you use. Instead of trying to remember the login names and passwords for all of your systems, all you will have to do is remember one strong *master* password to open your password manager file. Then you can see each system's login name and password.

This guide explains how to setup and use a solid and free password manager: KeePassXC.

2. Installation

KeePassXC can be downloaded from: https://keepassxc.org/download .
Macintosh users should choose MacOS and "DMG Installer (Intel) - Binary bundle (macOS 10.13+)" for most systems.
Windows users should choose Windows and "Installer (64-bit) - MSI installer" for most systems.
Follow the directions to install. You will need your Administrator password to do this.

3. Preparation

All your passwords in the KeePassXC password manager will be stored in a database. It is useful to have a name for your database, such as "Alex Passwords" or "Locker".

You will also need a Master password to unlock the database. Since you will use this every day, the Master password must be easy to remember yet long and not easily guessed or hacked.
IMPORTANT: If you forget your Master password, you will not be able to access your database of passwords!

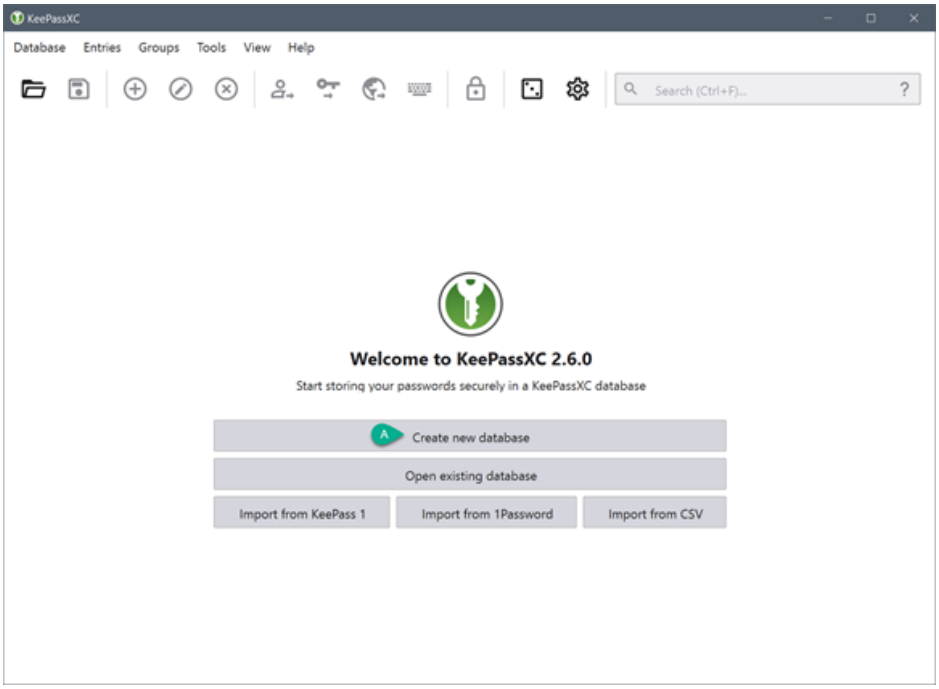
A secure Master password will include more than 15 characters, special characters and misspelled words, but avoid proper names and anything that can be associated with you (ie: your pet, job, address, etc). Here are some examples of secure passwords (*please don't use any of these yourself!*):

- ✓ futbol SPEEKS 2 me (i hope(
- ✓ $4501@92%=Happynice!
- ✓ Tintd 4tunes[MISTEAK]+
- ✓ [5] score and 9000 years IGO boldly ware

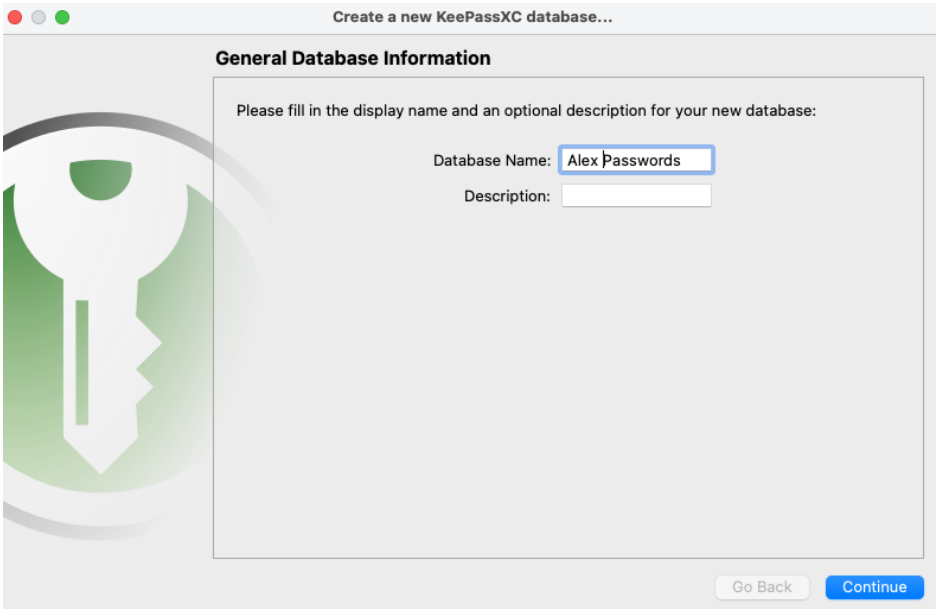
Create a secure password for yourself and practice until you can type your password from memory later in the day. If you must write your master password down, store it in a safe or a locked drawer.

4. Start a Password Database

Start up KeePassXC. Click on “Create new database” (A).

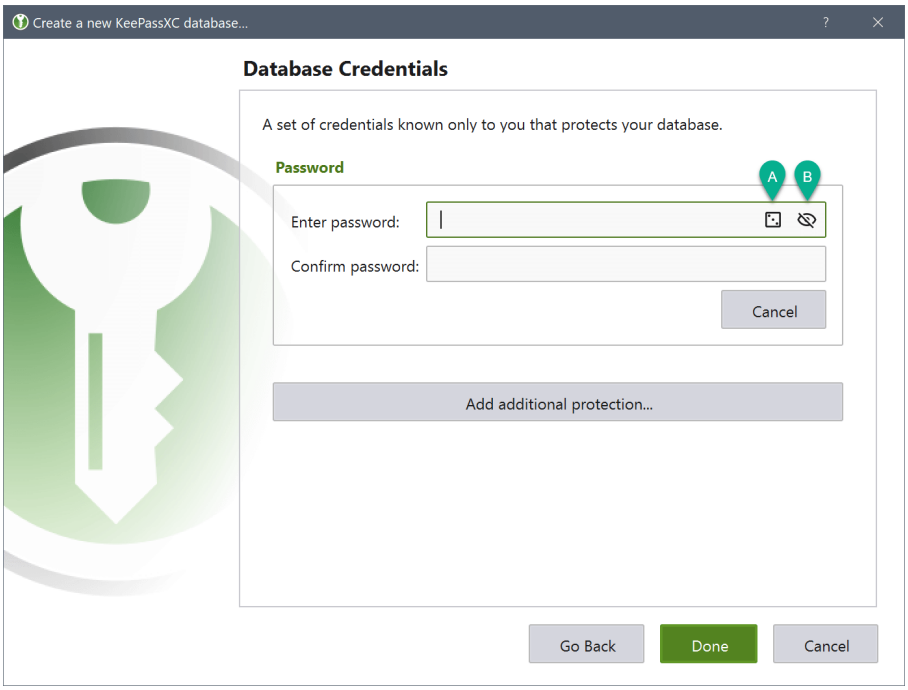


Fill in your Database Name, such as “Alex Passwords”. Then click Continue.

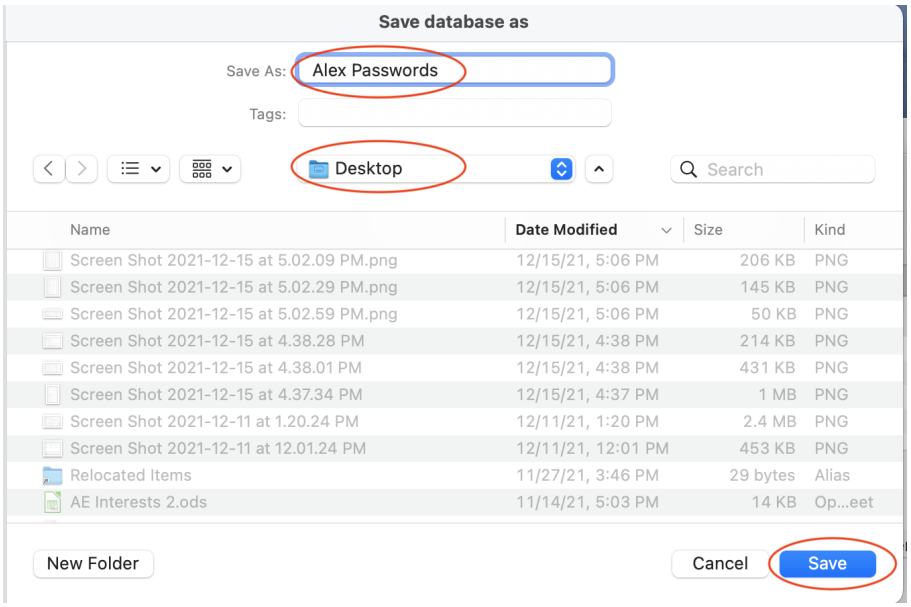


For Encryption Settings, just click Continue.

For Database Credentials, enter your new Master password that you committed to memory. Confirm by entering it again. Then click Done.



At this point you will see the Save database as screen. It will be helpful to use the same name as your database so you can easily find it. Also, ensure that the location you want to store it is someplace you can find. Then Save.

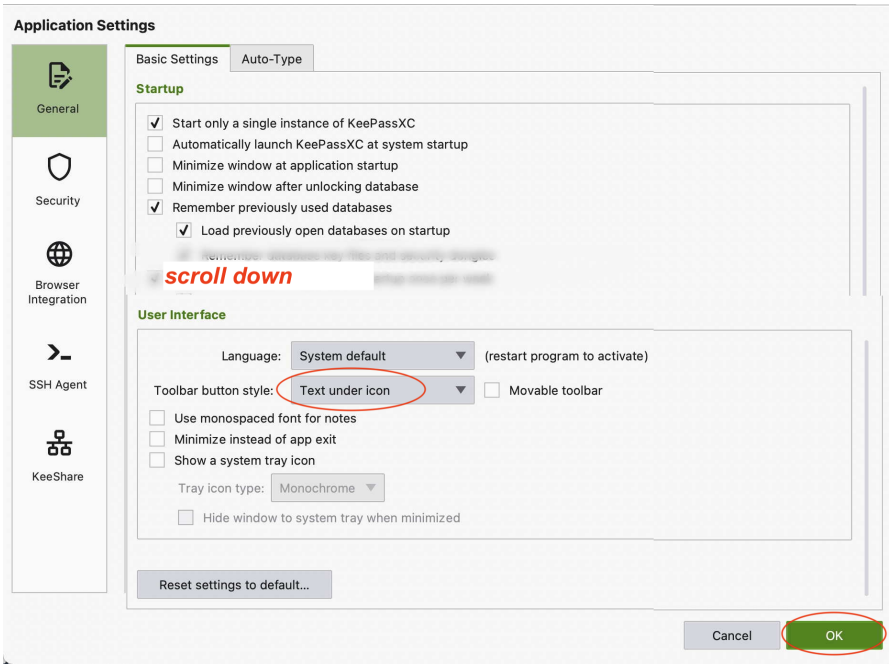


5. Configure Your Password Manager

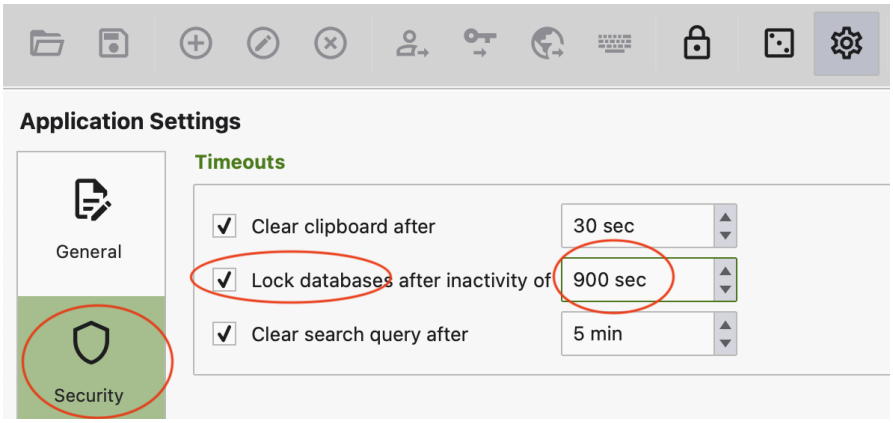
Take these steps to configure Your Password Manager so it is easy to use and to ensure your passwords will be kept safe:

- Click on the gear icon in the top right.

- In the General tab, Basic Settings, scroll down to the User Interface section. Change the Toolbar button style to Text under icon.



- In the Security tab, set “Lock databases after inactivity of” to some short but reasonable time. 900 sec is equivalent to 15 minutes. This ensures that if you step away from your computer without closing your password database, it will automatically close after 15 minutes of inactivity.

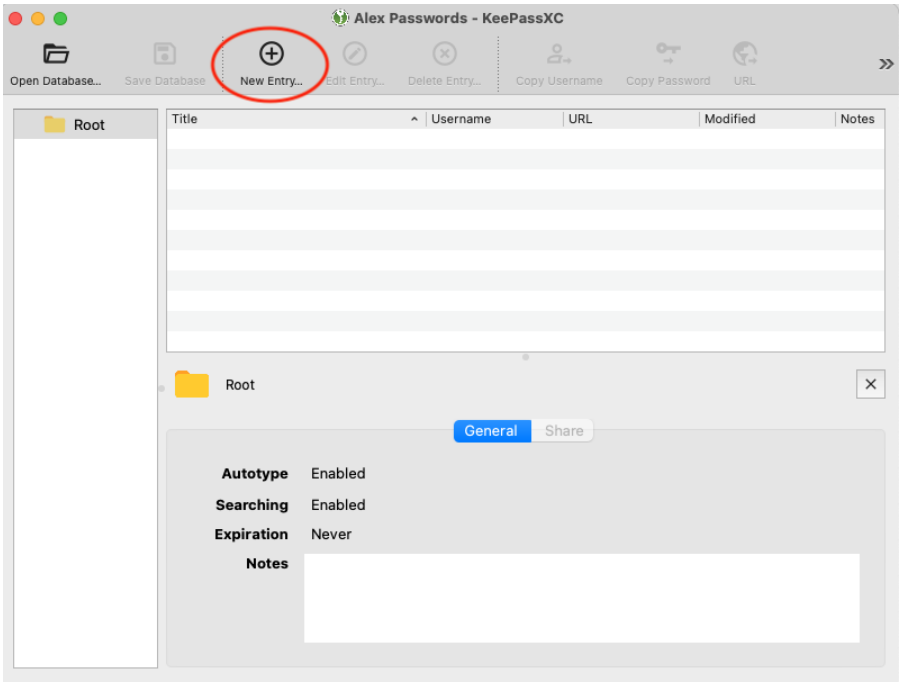


- Finally, click OK.

You might also want to change the appearance of KeePassXC by changing the Theme in the View menu at the top. Feel free to experiment with the different themes to find the one you like best.

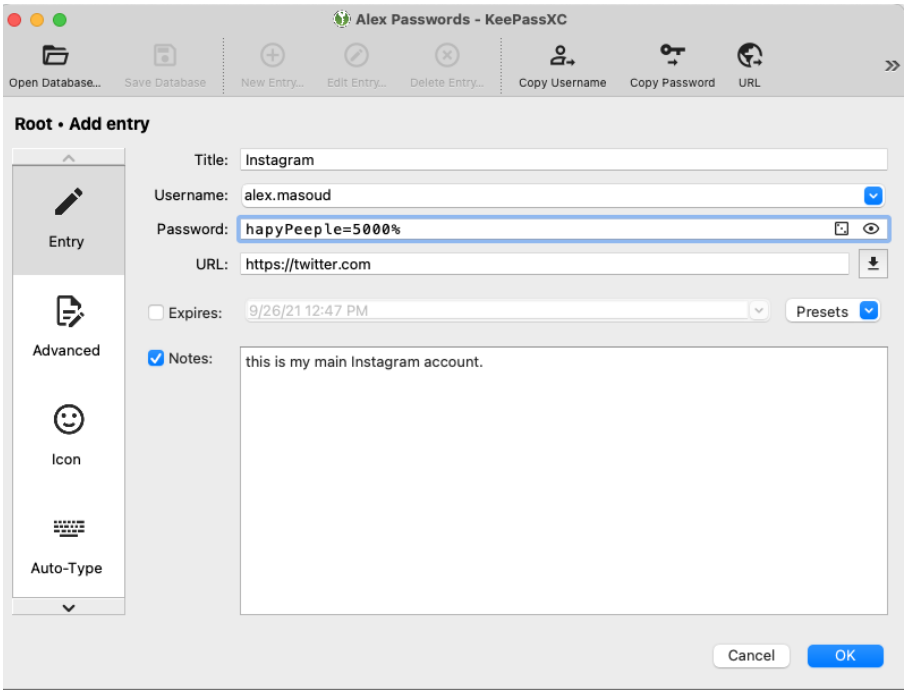
6. Add New Passwords to Your Database

Initially your database will have nothing in it. Click the New Entry button to create a password entry.



To add a password, follow these steps:

- Give it a title that describes what it is for.
- Enter the username to login to this site.
- Enter the password for this site.
- Add the URL to the login page. You can Cut and Paste this from the website so it includes the https:// .
- Add any (optional) description or other information in the Notes.
- Click OK.



Repeat this process for each of your accounts and passwords.

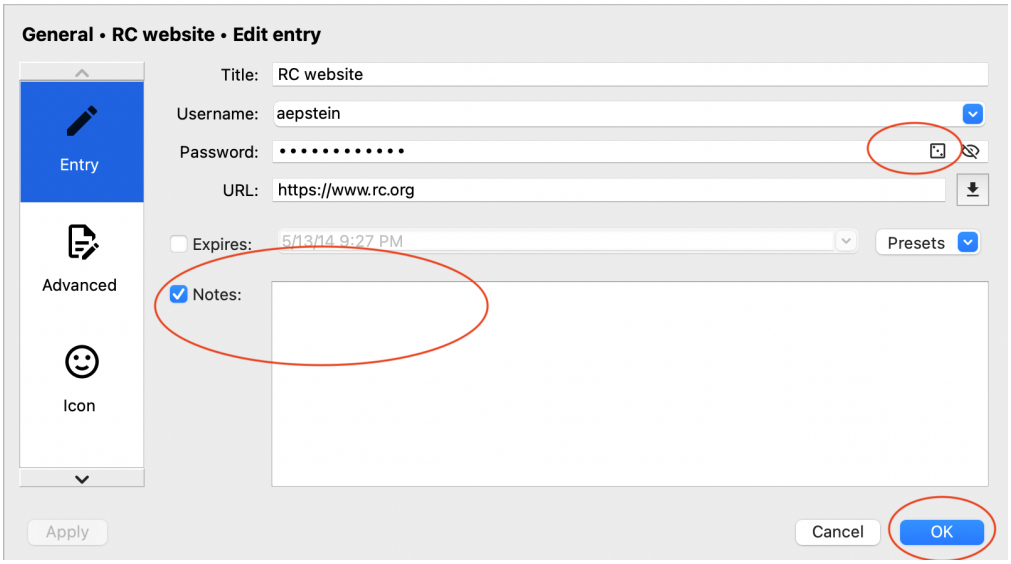
7. Using Your Stored Passwords

Once you have entered some of your passwords, use your passwords as follows:

- Open the password manager if it is not already open.
- Browse to the website login page whose password you have already saved.
- In KeePassXC, click once on the password you wish to use.
- At the top, click the Copy Username icon.
- Click back to the website login page and Paste into the username field.
- In KeePassXC again, click the Copy Password icon at the top.
- Click back to the website login page and Paste into the password field and click OK.
- You should now be logged into the website.

8. Change a Stored Password

To update a password you already stored, double-click on the title of that password in your list. This will allow you to change the username, password or URL. You can also add Notes that pertain to this entry.

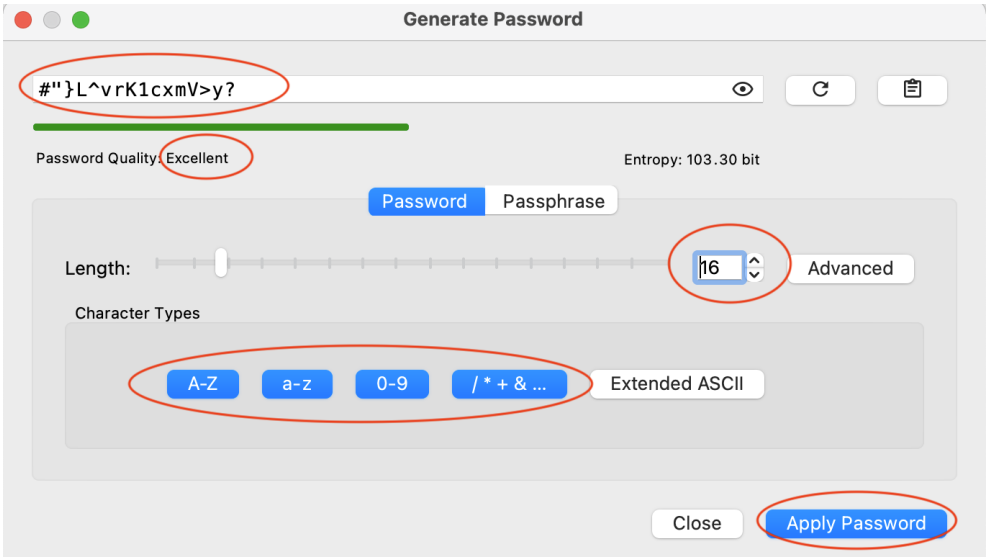


9. Automatically create a strong password

You can also ask KeePassXC to create a strong password for you. This is helpful when you are changing a password for a website. Click on the icon to the right of the Password line to open the Generate Password screen.

Here you can choose how long you want the password to be and the different types of characters to use, all of which affects the Password Quality. For websites where you will always use KeePassXC, you can generate a long and complex password since you won't need to remember it. You can also revise the generated password if you wish.

Click Apply Password when you are satisfied with the generated password. The icon to the extreme right of the Password line displays your password.



Back on the Edit Entry screen, click OK to make the change to the password entry. Click Cancel if you want to revert back to the original password.

10. Back Up Your Password Manager Database

Since your password file contains critical information you don't want to lose, be sure to regularly make a copy of the file on a thumb drive or another disk.

Remember: If you lose the file OR the Master password, you will not be able to recover your passwords. Guard both well!