# KEEPASSX TOOL GUIDE

KeePassX Tool Guide  
Secure password management --------------------------

**Lesson to read:** [**Passwords**](umbrella://lesson/passwords)  
**Download Location:** <https://www.keepassx.org/downloads>  
**Computer requirements:** Windows 2000 or higher, Mac OS X 10.4-10.9  
**Version used in this guide:** KeePassX 0.4.3 (KeePassX is a cross-platform version of the Windows-only KeePass program.)  
**License:** Free and Open-Source Software (primarily GPLv2)  
**Other Reading:** <https://www.keepassx.org/forum/>  
**Level:** Beginner  
**Time required:** 5 minutes

**Using KeePassX will give you:**

? The ability to save all your passwords in one convenient and secure database  
? The ability to create and store many strong passwords without having to remember them

### 1.0 Things to consider with KeePassX

KeePassX is a password safe?a program you can use to store all your passwords for various websites and services. A password safe is a great tool because it allows you to use different difficult-to-guess passwords for all your services, without needing to remember them. Instead, you only need to remember one master password that allows you to decrypt a database of all your passwords. Password safes are convenient and allow you to organize all of your passwords in one location.

**It should be noted that using a password safe creates a single point of failure and establishes an obvious target for bad actors or adversaries. Research has suggested that many commonly used passwords safes have vulnerabilities, so use caution when determining whether or not this is the right tool for you.**

### 1.1 How KeePassX works

KeePassX works with files called password databases, which are exactly what they sound like?files that store a database of all your passwords. These databases are encrypted when they?re stored on your computer?s hard disk, so if your computer is off and someone steals it they won?t be able to read your passwords.

Password databases can be encrypted via three methods: using a master password, using a keyfile, or both. Let?s look at the pros and cons of each.

### 1.2 Using a master password

A master password acts like a key?in order to open the password database, you need the correct master password. Without it, nobody can see what?s inside the password database. There are a few things to keep in mind when using a master password to secure your password database.

? *This password will decrypt all of your passwords, so it needs to be strong!* That means it shouldn?t be something easy to guess, and it should also be long?the longer the better! Also, the longer it is, the less you need to worry about having special characters or capitals or numbers. A password that is only made up of six random words (in all lower case, with spaces in between) can be harder to break than a 12-character password made up of upper and lower case letters, numbers, and symbols.  
? *You need to be able to remember this password!* Since this one password will allow access to all your other passwords, you need to be able to make sure you can remember it without writing it down. This is another reason to use something like [Diceware](http://world.std.com/~reinhold/diceware.html)?you can use regular words that are easy to remember, instead of trying to remember unnatural combinations of symbols and capital letters.

### 1.3 Using a keyfile

Alternatively, you can use a keyfile to encrypt your password database. A keyfile acts the same way a password would?every time you want to decrypt your password database you will need to provide that keyfile to KeePassX. A keyfile should be stored on a USB drive or some other portable media, and only inserted into your computer when you want to open your password database. The benefit of this is that even if somebody gets access to your computer?s hard disk (and thus your password database) they still won?t be able to decrypt it without the keyfile stored in the external media. (Additionally, a keyfile can be much harder for an adversary to guess than a normal password.) The downside is that any time you want to access your password database, you?ll need to have that external media handy (and if you lose it or it gets damaged, then you won?t be able to open your password database).

Using a keyfile instead of a password is the closest thing to having an actual physical key to open your password database?all you need to do is insert your USB drive, select the keyfile, and presto! If you do choose to use a keyfile instead of a master password, though, make sure your USB drive is stored somewhere safe?*anyone who finds it will be able to open your password database*.

### 1.4 Using both

The most secure method for encrypting your password database is to use both a master password and a keyfile. This way, your ability to decrypt your password database depends on what you know (your master password) and what you have (your keyfile)?and any malicious entity who wants to get access to your passwords will need both. (With that said, keep in mind your threat model?for most home users who just want to store their passwords, a strong master password should be sufficient. But if you?re worried about protecting against state-level actors with access to huge computational resources, then the more security the better.)

Now that you understand how KeePassX works, let?s get started with actually using it!

### 2.0 Getting started with KeePassX

Once you?ve installed KeePassX from [here](https://www.keepassx.org/downloads), go ahead and launch it.

Once it?s started, select ?New Database? from the File menu.

A dialog will pop up which will ask you to enter a master password and/or use a keyfile. Select the appropriate checkbox(es) based on your choice.

Note that if you want to see the password you?re typing in (instead of obscuring it with dots) you can click the button with the ?eye? to the right.

Also note that you can use any existing file as a keyfile?an image of your cat for example, could be used as a keyfile. You?ll just need to make sure the file you choose never gets modified, because if its contents are changed then it will no longer work for decrypting your password database.

Also be aware that sometimes opening a file in another program can be enough to modify it; the best practice is to not open the file except to unlock KeePassX. (It is safe to move or rename the keyfile, though.)

Once you?ve successfully initialized your password database, you should save it by choosing ?Save Database? from the File menu. (Note that if you want, you can move the password database file later to wherever you like on your hard disk, or move it to other computers?you?ll still be able to open it using KeePassX and the password/keyfile you specified before.)

### 2.1 Organizing passwords

KeePassX allows you to organize passwords into ?Groups,? which are basically just folders. You can create, delete, or edit Groups or Subgroups by going to the ?Groups? menu in the menubar, or by right-clicking on a Group in the left-hand pane of the KeePassX window. Grouping passwords doesn?t affect any of the functionality of KeePassX?it?s just a handy organizational tool.

### 2.2 Storing/generating/editing passwords

To create a new password or store a password you already have, right-click on the Group in which you want to store the password, and choose ?Add New Entry? (you can also choose ?Entries > Add New Entry? from the menubar). For basic password usage, do the following:

? Enter a descriptive title you can use to recognize this password entry in the ?Title? field.  
? Enter the username associated with this password entry in the ?Username? field. (This can be blank if there is no username.)  
? Enter your password in the ?Password? field. If you?re creating a new password (i.e. if you?re signing up for a new website and you want to create a new, unique, random password) click the ?Gen? button to the right. This will pop up a password generator dialog, which you can use to generate a random password. There are several options in this dialog, including what sorts of characters to include and how long to make the password.  
\* Note that if you generate a random password, it?s not necessary that you remember (or even know!) what that password is! KeePassX stores it for you, and any time you need it you?ll be able to copy/paste it into the appropriate program. This is the whole point of a password safe?you can use different long random passwords for *each* website/service, without even knowing what the passwords are!  
\* Because of this, you should make the password as long as the service will allow and use as many different types of characters as possible.  
\* Once you?re satisfied with the options, click ?Generate? in the lower right to generate the password, and then click ?OK.? The generated random password will automatically be entered in the ?Password? and ?Repeat? fields for you. (If you?re not generating a random password, then you?ll need to enter your chosen password again in the ?Repeat? field.)  
? Finally, click ?OK?. Your password is now stored in your password database. To make sure the changes are saved, be sure to save the edited password database by going to ?File > Save Database.? (Alternatively, if you made a mistake, you can close and then re-open the database file and all changes will be lost.)

If you ever need to change/edit the stored password, you can just choose the Group it?s in and then double-click on its title in the right-hand pane, and the ?New Entry? dialog will pop up again.

### 2.3 Normal use

In order to use an entry in your password database, simply right-click on the entry and choose ?Copy Username to Clipboard? or ?Copy Password to Clipboard,? and then go to the window/website where you want to enter your username/password, and simply paste in the appropriate field. (Instead of right-clicking on the entry, you can also double-click on the username or password of the entry you want, and the username or password will be automatically copied to your clipboard.)

### 2.4 Advanced use

One of the most useful features of KeePassX is that it can automatically type in usernames and passwords for you into other programs when you press a special combination of keys on your keyboard. Note that although this feature is only available under Linux, other password safes like KeePass (on which KeePassX was based) support this feature on other operating systems, and it works similarly.

To enable this feature, do the following.

*1. Choose your global hotkey.* Choose ?Settings? from the ?Extras? menu, and then choose ?Advanced? in the pane on the left. Click inside the ?Global Auto-Type Shortcut? field, and then press the shortcut-key combination you wish to use. (For example, press and hold Ctrl, Alt, and Shift, and then hit ?p.? You can use any key combination you like, but you?ll want to make sure that it doesn?t conflict with hotkeys other applications use, so try to stay away from things like Ctrl+X or Alt+F4.) Once you?re satisfied, click ?OK.?

*2. Setup auto-type for a specific password.* Make sure that you have the window open where you?ll want to enter the password. Then go to KeePassX, find the entry for which you want to enable auto-type, and double-click on the entry?s title to open up the ?New Entry? dialog.

*3.* Click the ?Tools? button in the bottom left, and select ?Auto-Type: Select target window.? In the dialog that pops up, expand the drop-down box and choose the title of the window in which you want the username and password to be entered. Click OK, and then click OK again.

*Test it out!* Now in order to autotype your username and password, go to the window/website where you want KeePassX to autotype your username/password for you. Make sure your cursor is in the text box for your username, and then hit the combination of keys you chose above for the global hotkey. As long as KeePassX is open (even if it?s minimized or not focused) your username and password should automatically be entered.

Note that depending on how the website/window is set up, this feature may not work 100% correctly right off the bat. (It might enter the username but not the password, for example.) You can troubleshoot and customize this feature, though?for more information we recommend looking at the KeePass documentation [here](http://keepass.info/help/base/autotype.html). (Although there are some differences between KeePass and KeePassX, that page should be enough to guide you in the right direction.)

It is recommended that you use a key combination that is difficult to hit accidentally. You don't want to accidentally paste your bank account password into a Facebook post!

### 2.5 Other features

You can search your database by typing something in the search box (the text box in the toolbar of the main KeePassX window) and hitting enter.

You can also sort your entries by clicking on the column header in the main window.

You can also ?lock? KeePassX by choosing ?File > Lock Workspace,? so that you can leave KeePassX open, but have it ask for your master password (and/or keyfile) before you can access your password database again. You can also have KeePassX automatically lock itself after a certain period of inactivity. This can prevent someone from accessing your passwords if you step away from your computer. To enable this feature, choose ?Extras > Settings? from the menu and click on the security options. Then check the box that says ?Lock database after inactivity of {number} seconds.?

KeePassX can also store more than just usernames and passwords. For example, you can create entries to store important things like account numbers, or product keys, or serial numbers, or anything else. There?s no requirement that the data you put in the ?Password? field actually has to be a password. It can be anything you want?just input what you want to store in the ?Password? field instead of an actual password (and leave the ?Username? field blank if there?s no username) and KeePassX will safely and securely remember it for you.