(Approx. 1,781 words)

Password Managers: What They Are and How to Use One

By Mike Morris, President / Editor, Front Range PC Users Group, Fort Collins, CO

Originally published in ***k-Byte***, the newsletter of the Front Range PC Users Group
www.frpcug.org

Introduction

A password manager application is ". . . software that helps a user organize passwords. . . . The software typically has a local database or a file that holds the encrypted password data for secure logon onto computers, networks, web sites and application data files . . . ." (Wikipedia) (http://bit.ly/PhVjkz).

Before you ask "why bother," think for a moment about how many web sites you connect to that require a password. Do you use the same (or very similar) password for most or all of those web sites? If you are like the overwhelming majority of computer users, the answer to that question is likely to be "yes."

You should, very definitely, NOT do that!

All of the computer security experts (and there are a lot of them these days) warn us not to use the same password for all accounts. For example:

> "The message of password reuse security is one that Hord Tipton, executive director of the International Information System Security Certification Consortium (ISC2), echoes. (www.ics2.org)
>
> "Diversifying your passwords for each account is essential to protecting all of your online information," Tipton said. "Once a password has been stolen, hackers often attempt to access multiple accounts, compounding the potential damage.""
>
> Source: Yahoo Email Is Breached: Lessons Learned (http://bit.ly/1h5jSZi)

See also Password Security, Protection, and Management (http://1.usa.gov/1fYSklG)

With respect to Mr. Tipton, "diversifying your passwords" is much easier said than done . . . unless you use a password manager.

There are a number of these applications (for example, see this http://bit.ly/PhT1Sg), but one, KeePass, is a ". . . free, open source, cross-platform and light-weight password management utility for Microsoft Windows, with unofficial ports for Linux, Mac OS X, iOS and Android . . . ." Wikipedia (http://bit.ly/1k8zUV3).

In fact, if you need a lot of passwords (I counted over 70 web sites that I use that need a password), it is almost impossible to keep track of them. But even if you have just a few (10 or a dozen), a password manager can be extremely helpful, and provide **an extra measure of security for you**.

How do password managers provide this extra security?

With KeePass the extra security is provided through these features:

1. All your passwords are stored in one database.
2. The database is locked with one master key or a key file, so you only have to remember one single master password (OK, you also need to remember the password to your computer, so that's 2 passwords you have to remember).
3. The database(s) is (are) encrypted using (one of) the best and most secure encryption algorithms currently known (AES).
4. KeePass can generate strong random passwords for you.

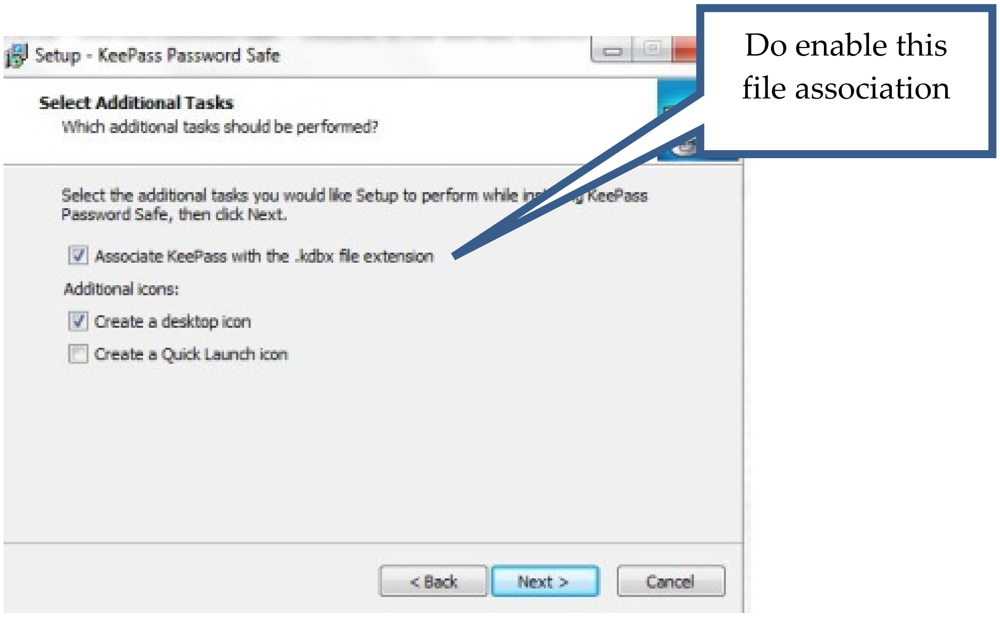
   Source: KeePass Password Safe (http://bit.ly/IzB7qC)

Since KeePass is open source, you get this extra security for free.

If all of those features sound a little "techie," don't worry, KeePass is actually easy to use. Therefore, KeePass (v. 2.20) will be used to demonstrate how you use a password manager application. As with all good things, it takes a little effort to enter the data--at least, it does if you need as many passwords as I do.

Installation

You can download the current version (which, as of 02/04/2014, for Windows, is 2.25) from the KeePass web site, http://keepass.info/. The installation follows the usual Windows sequence. However there is one window in the sequence worth a comment:



Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing KeePass Password Safe, then click Next.

☑ Associate KeePass with the .kdbx file extension

Additional icons:

☑ Create a desktop icon

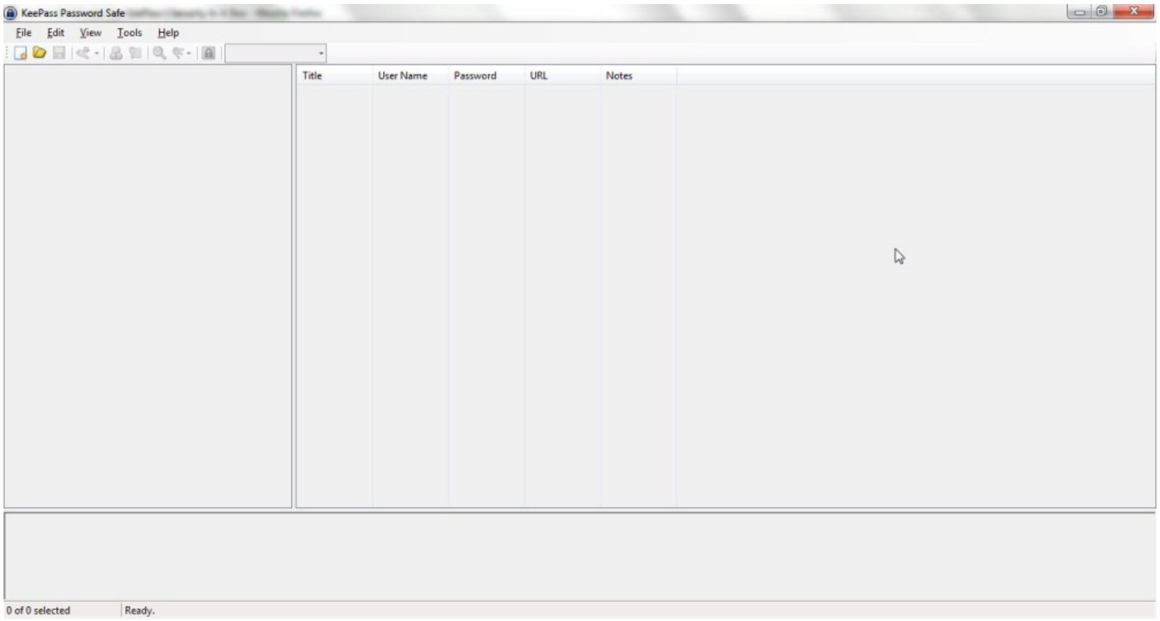
□ Create a Quick Launch icon

Do enable this file association

This step may not be necessary at this point, but establishing that file association at the beginning probably reduces the risk of future problems.

Set Up

Once the installation is complete, at the first launch you will see the KeePass main screen:

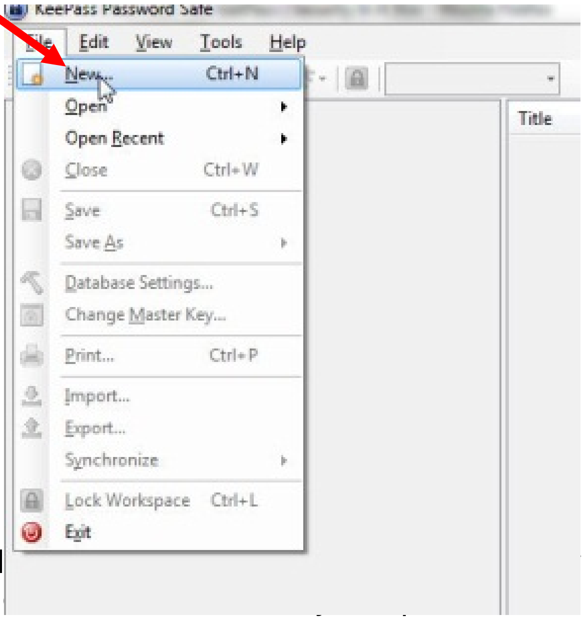


At this point, you have two primary set up tasks:

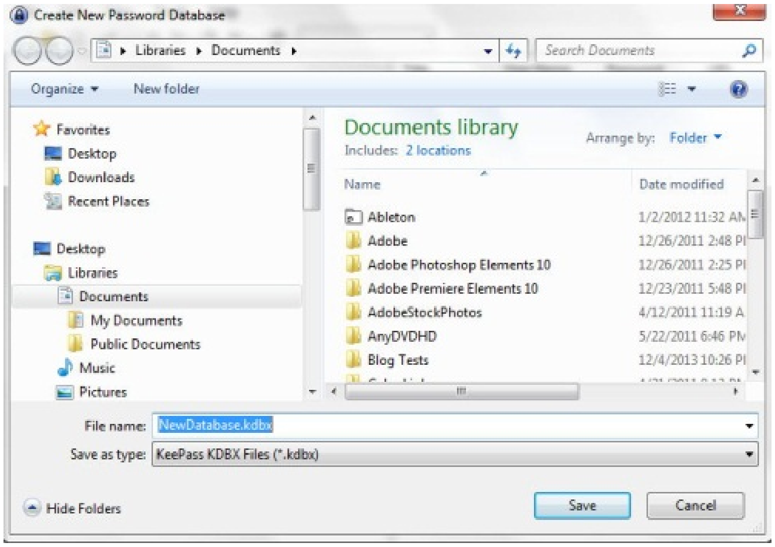
1. Create a database
2. Enter data into the database

You create a database with these steps:

Click on File, then on New:



You will be asked (in the usual ant to save the program. Here is an example



Name	Date modified
Ableton	1/2/2012 11:32 AM
Adobe	12/26/2011 2:48 PI
Adobe Photoshop Elements 10	12/26/2011 2:25 PI
Adobe Premiere Elements 10	12/23/2011 5:48 PI
AdobeStockPhotos	4/12/2011 11:19 A
AnyDVDHD	5/22/2011 6:46 PM
Blog Tests	12/4/2013 10:26 PI

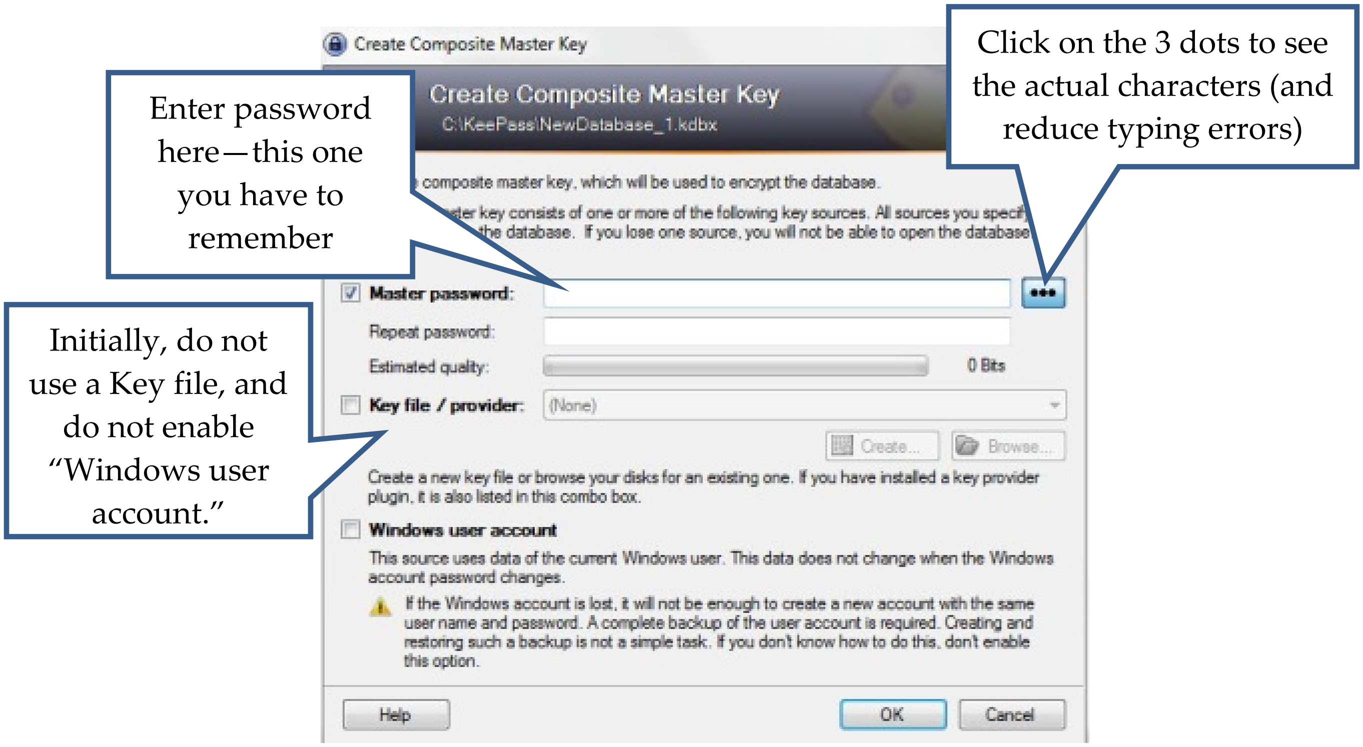
File name: NewDatabase.kdbx

Save as type: KeePass KDBX Files (*.kdbx)

The default Save location for Windows 7 is, of course, Documents. Remember, you can choose to save the database anywhere on your computer. I set up a separate folder called KeePass in the root directory of my hard drive and saved the database there (just my preference).

Note also that a default "File name" is entered. I modified that name, in the expectation (as yet unproven), that I will eventually need multiple databases. I chose NewDatabase_1.

With the location and file name selected, click on Save. You will see:



Create Composite Master Key

Create Composite Master Key
C:\KeePass\NewDatabase_1.kdbx

composite master key, which will be used to encrypt the database.

ster key consists of one or more of the following key sources. All sources you specif the database. If you lose one source, you will not be able to open the database

☑ Master password:

Repeat password:

Estimated quality: 0 Bits

☐ Key file / provider: (None)

Create a new key file or browse your disks for an existing one. If you have installed a key provider plugin, it is also listed in this combo box.

☐ Windows user account

This source uses data of the current Windows user. This data does not change when the Windows account password changes.

If the Windows account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the user account is required. Creating and restoring such a backup is not a simple task. If you don't know how to do this, don't enable this option.

Enter password here—this one you have to remember

Click on the 3 dots to see the actual characters (and reduce typing errors)

Initially, do not use a Key file, and do not enable “Windows user account.”

You enter a Master Password into this window. It needs to be a "strong" password, but it also needs to be something you can remember. A “strong” password is:

> “A password that is hard to detect both by humans and by the computer. Two things make a password stronger: (1) a larger number of characters, and (2) mixing numeric digits, upper and lower case letters and special characters ($, #, etc.).”

Source: PC Magazine (http://bit.ly/1h5lq5l)

This password you may want to write down (yes, using the old fashioned pencil and paper); and although this should be obvious, don't identify it on that piece of paper. You may also want to keep it with you.

From the KeePass Help file (Composite Master Key):

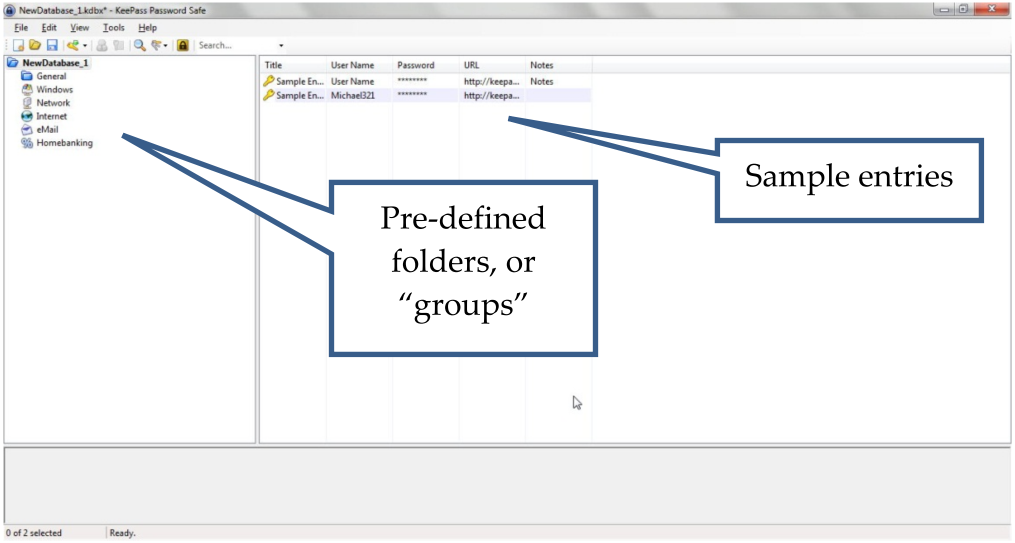
> "If you forget this master password, all your other passwords in the database are lost, too. There isn't any backdoor or a key which can open all databases. There is no way of recovering your passwords."

A more detailed discussion of passwords vs. key files is available from the Composite Master Key section of the KeePass Help file.

If creating a strong password that you can remember seems contradictory, enter:

> how to create strong passwords that you can remember into your favorite search engine. You will find many articles with suggestions.

After you enter your password, click on the OK button at the bottom right of the Create Composite Master Key window. You will see something similar to this (I will talk about the Database Settings window that is part of the database creation process later—the default values are acceptable):


NewDatabase_1.kdbx* - KeePass Password Safe
File Edit View Tools Help
Search...
NewDatabase_1
General
Windows
Network
Internet
eMail
Homebanking

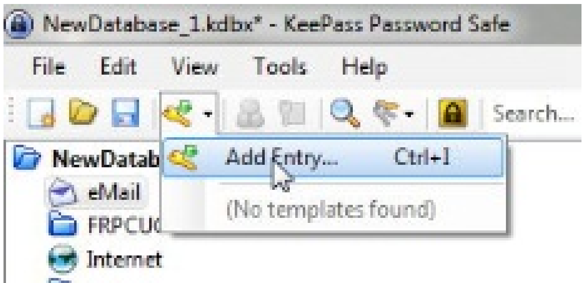
Title	User Name	Password	URL	Notes
Sample En...	User Name	********	http://keepa...	Notes
Sample En...	Michael321	********	http://keepa...	

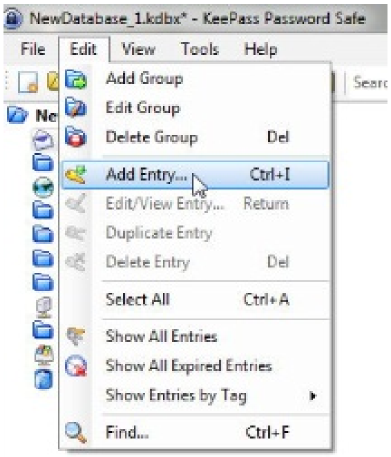
0 of 2 selected | Ready.

Sample entries

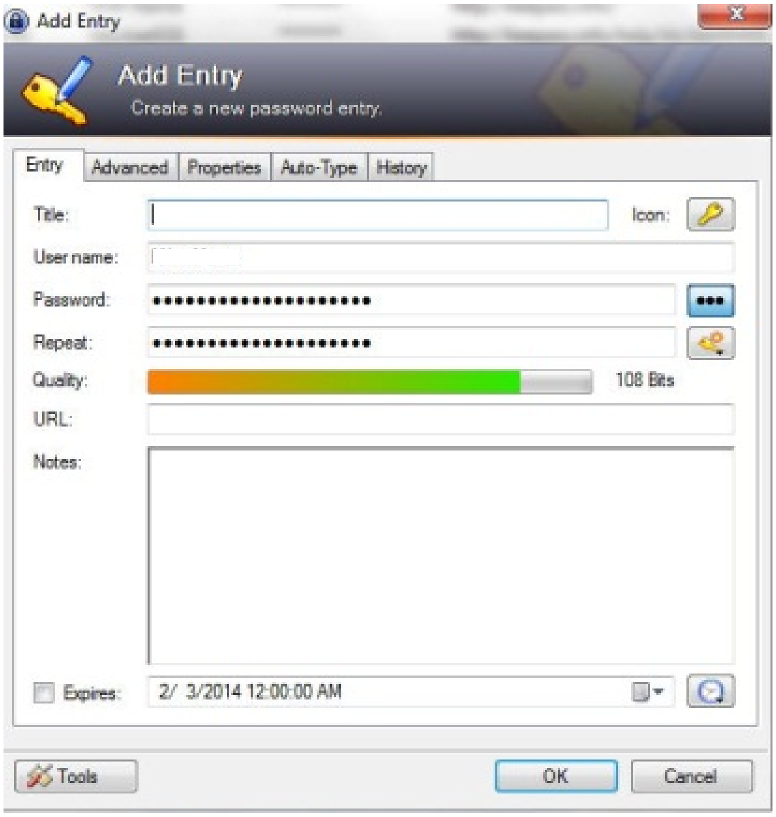
Pre-defined folders, or "groups"

You can add groups, and/or modify their order. However, you are, at this point, ready to enter data. You use the "Add Entry" window for this task. It is available from the Edit menu and from the Toolbar:





When the Add Entry window is displayed, it will already contain an automatically generated strong password:



Password: ••••••••••••••••••••

Repeat: ••••••••••••••••••••

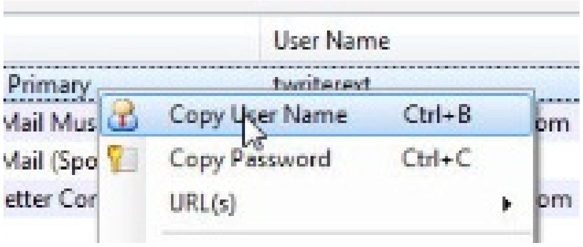
Quality: 108 Bits

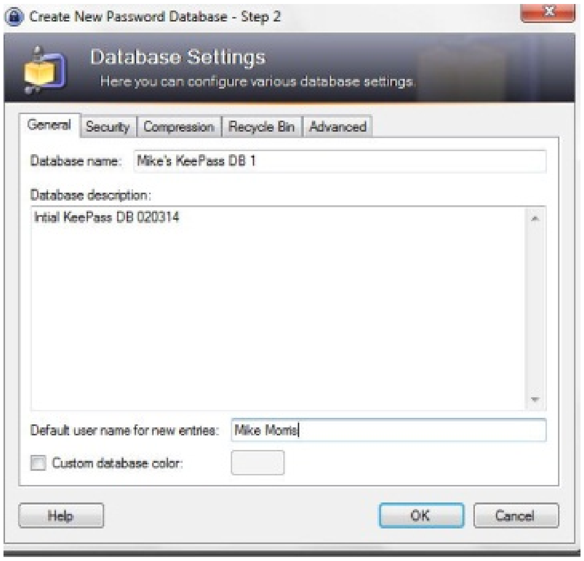
□ Expires: 2/ 3/2014 12:00:00 AM

Your user name will also be included. The only field required, other than the password, is the URL of the web site for which you want to use this password.

By the way, that Notes field is a handy place to record the answers to all those security questions you are asked when you register at any web site.
You add as many entries as you need passwords. If you choose to organize them into groups, click on the group name in the left panel before you click on Add Entry.

I want to depart momentarily from this sequence and return to the Create New Password Database steps. You will see a Database Settings window during this set up (you can also access Settings from the File menu after the database is created). All of those settings can be left at their default values. However, you may want to enter a description. For example:




Create New Password Database - Step 2
Database Settings
Here you can configure various database settings.
General
Security
Compression
Recycle Bin
Advanced
Help
OK
Cancel

Database name: Mike's KeePass DB 1

Database description: Intial KeePass DB 020314

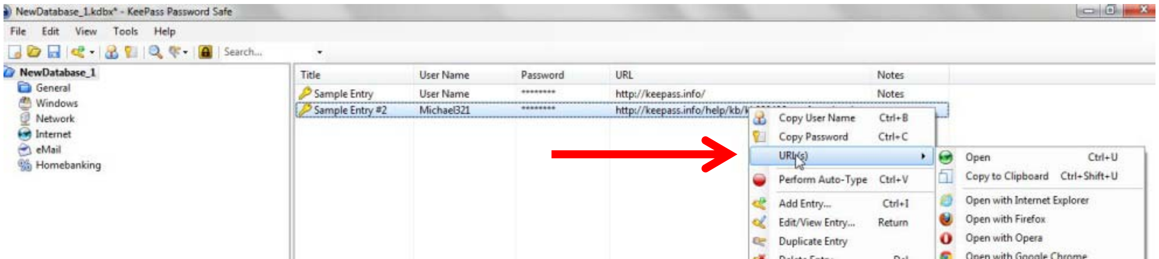
Default user name for new entries: Mike Morris

□ Custom database color:

How to Use the Password

Here are the steps for using the password:

1. Connect to the log in window of the web site of interest. You can also connect to the web site from KeePass. Right click on the entry for that web site and then click on URL. If you have more than one browser installed (as I do), you can choose which one to use from the list that is displayed:



Title	User Name	Password	URL	Notes
Sample Entry	User Name	********	http://keepass.info/	Notes
Sample Entry #2	Michael321	********	http://keepass.info/help/kb/k	

2. Once you are connected to the web site's log in window, in KeePass, right click on the entry for that web site and then click on "Copy User Name":

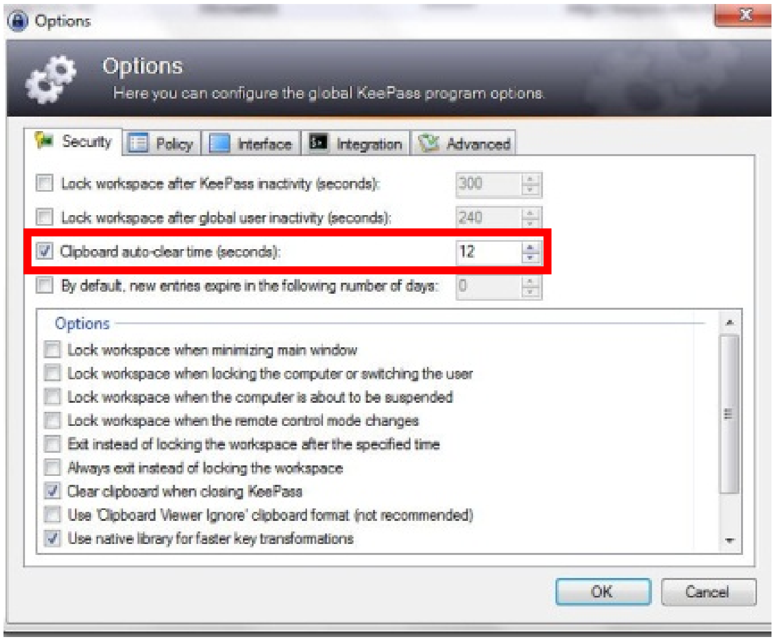
   Return to web site log in screen and paste the user name into the appropriate field (you could, of course, just type that in).

3. In KeePass, right click (again) on the entry for that web site and this time click on "Copy Password."

   Return to web site log in screen and paste the password into the appropriate field.

4. Click on the log in or sign in button for the web site.

There is one important note regarding these steps. You have only a limited (but adjustable) time to paste the user name or password after you copy it. KeePass will clear the Clipboard after some number of seconds for security reasons. That time is set in the Security tab of the Tools/Options menu item:



Options

Here you can configure the global KeePass program options.

□ Lock workspace after KeePass inactivity (seconds): 300

□ Lock workspace after global user inactivity (seconds): 240

☑ Clipboard auto-clear time (seconds): 12

□ By default, new entries expire in the following number of days: 0

Options

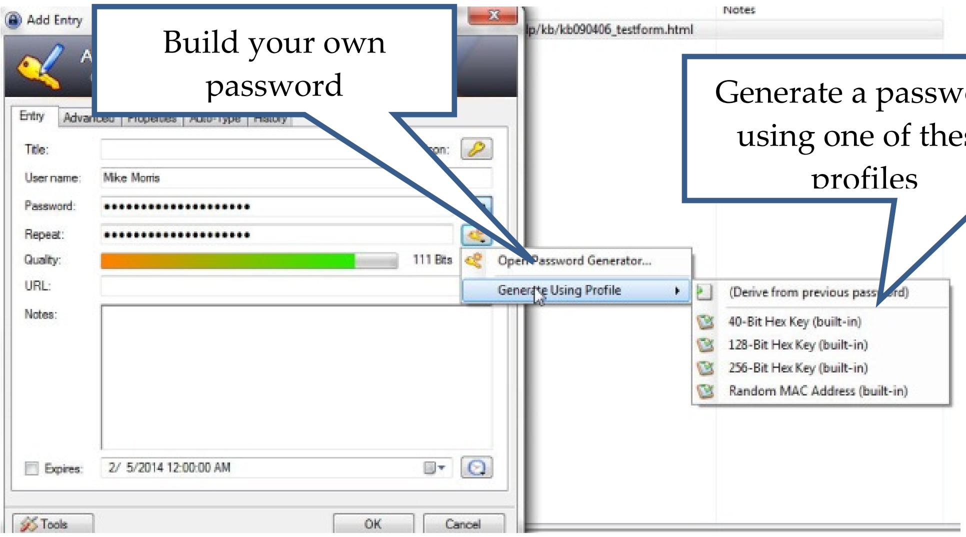
□ Lock workspace when minimizing main window
□ Lock workspace when locking the computer or switching the user
□ Lock workspace when the computer is about to be suspended
□ Lock workspace when the remote control mode changes
□ Exit instead of locking the workspace after the specified time
□ Always exit instead of locking the workspace
☑ Clear clipboard when closing KeePass
□ Use 'Clipboard Viewer Ignore' clipboard format (not recommended)
☑ Use native library for faster key transformations

Note that in the image above, that time is set to 12 seconds.

Extras

So far, these instructions cover just the basics. There are many extras, three of which are worth mentioning, although not discussed here in detail (see the KeePass Help file).

1. Generate your own passwords: If you are not satisfied with the automatically generated passwords, you can create your own. Click on the icon under the 3 dots and you will see:



Build your own password

Generate a password using one of these profiles

Title:

User name: Mike Morris

Password: ••••••••••••••••••••

Repeat: ••••••••••••••••••••

Quality: 111 Bits

URL:

Notes:

□ Expires: 2/ 5/2014 12:00:00 AM

Add Entry
Entry
Advanced
Properties
Auto-Type
History
Open Password Generator...
Generate Using Profile
(Derive from previous password)
40-Bit Hex Key (built-in)
128-Bit Hex Key (built-in)
256-Bit Hex Key (built-in)
Random MAC Address (built-in)
Tools
OK
Cancel
Notes
lp/kb/kb090406_testform.html

2. Mobility: There is a “portable” version (http://keepass.info/download.html) that you can install on a flash drive that will allow you to use KeePass on any other computer (with some restrictions—see the KeePass Help file) “without creating any new registry keys and it doesn't create any configuration files in your Windows or application data directory of your user profile.”

3. Plugins: There are a large number of plugins available (http://keepass.info/plugins.html), including one called KeeForm that will "(open) websites and fill in the login data automatically, for Internet Explorer and Firefox." Before you install any plugin, be sure to read the Plugins for KeePass 2.x (http://bit.ly/PhVjkz) information.

Acknowledgements

Thanks to Front Range PC Users Group member Bert Broekstra for his help with learning this program.

Thanks to Front Range PC Users Group member Herb Cantor for finding the “Yahoo Email is Breached . . .” article and for sending the link to me.