KeePass Password Safe: Password Manager

The recommended from Information Services at the University of Regina password manager is KeePass Password Safe.

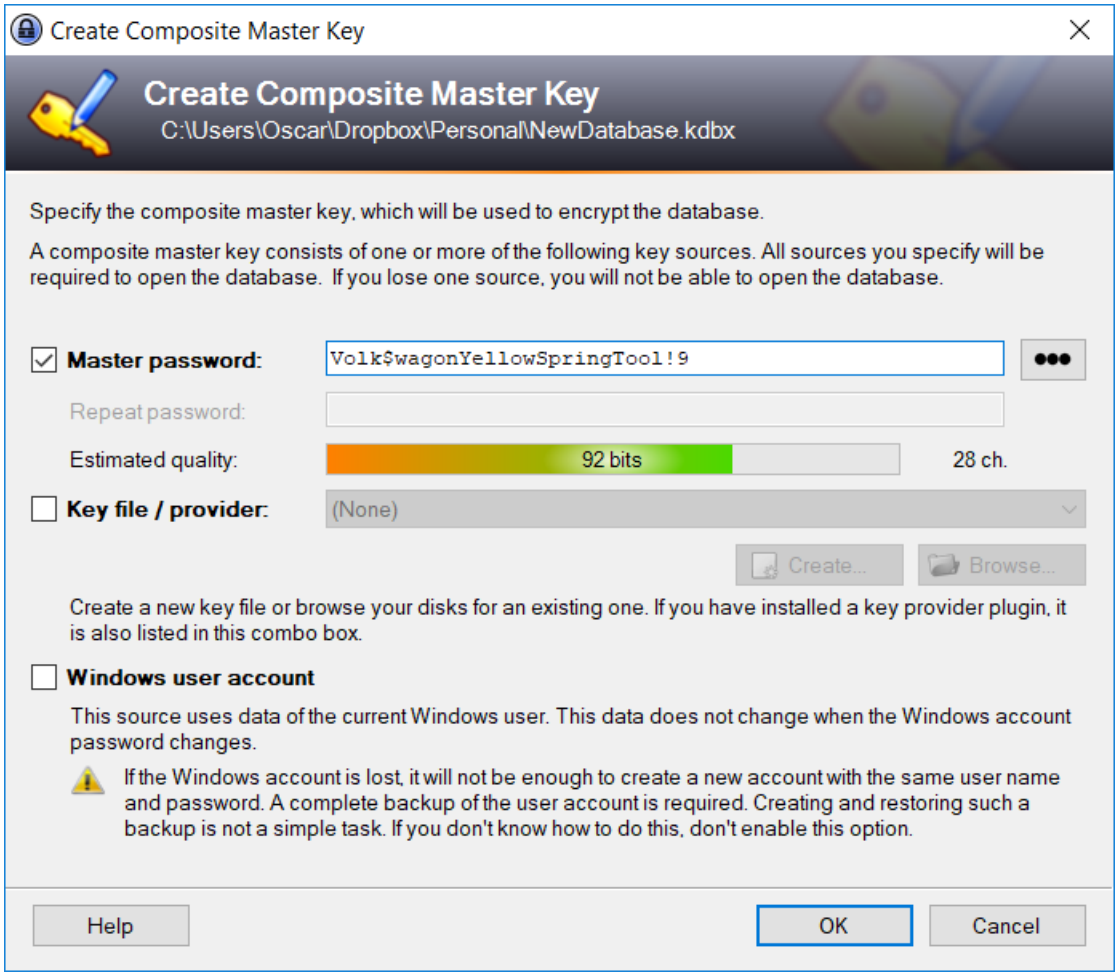
This documents is designed to assist with the creation and usage of a password database in KeePass Password Safe.

Installation instructions can be found at: https://www.uregina.ca/is/security/resources/resource-password-manager.html.

Create Password Database and Store Passwords:

After software installation, the first time you open the KeePass you'll need to create a new database by clicking on File>New.

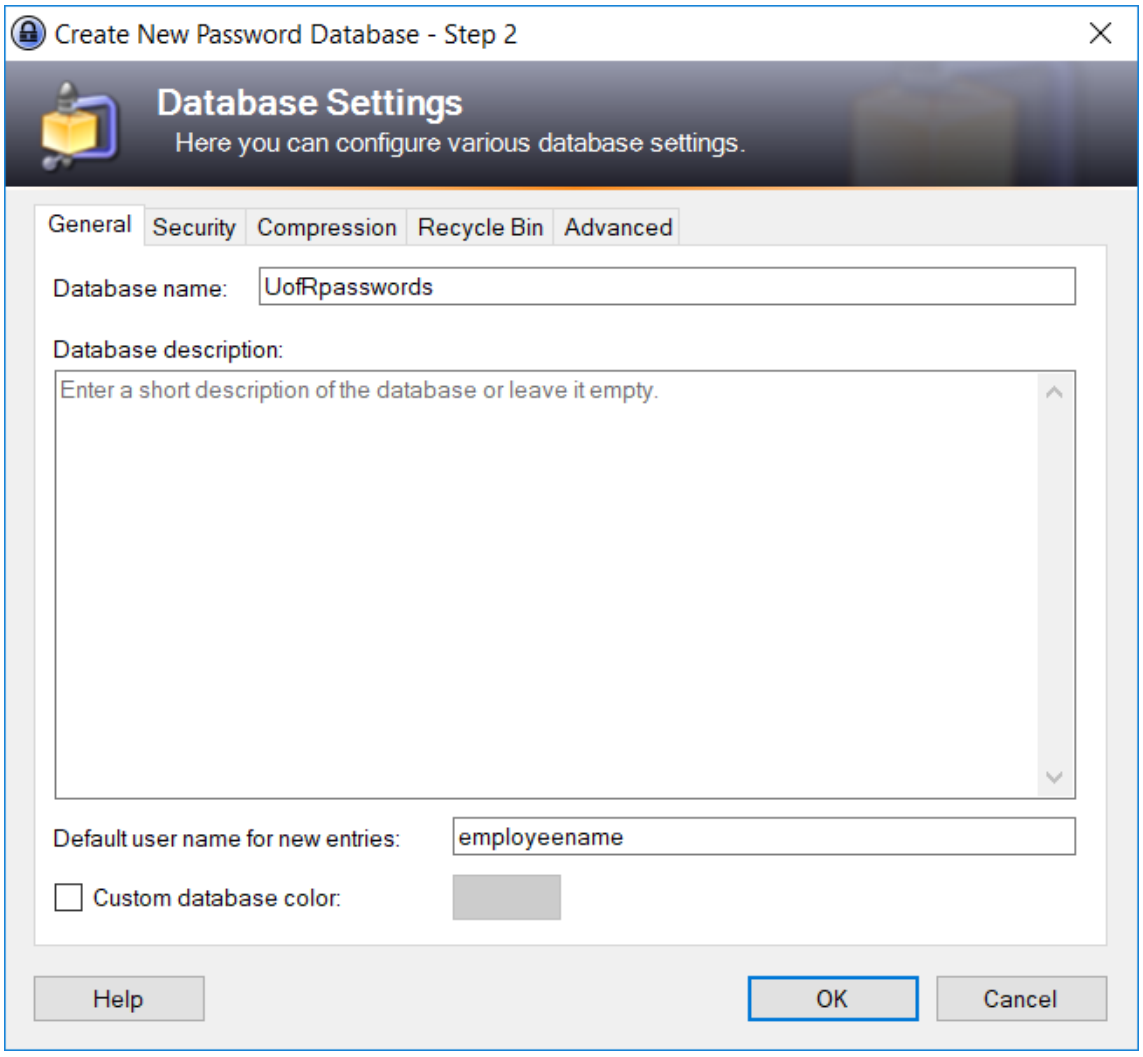
You'll be prompted to enter a Master Password which is the only password you will need to remember. Make sure and pick a strong password with several characters, symbols, and numbers. It can be an entire phrase, sentence, or whatever you want it to be with virtually any characters you want. Please use a long, secure master password, as all your other passwords are secured by this single master password.



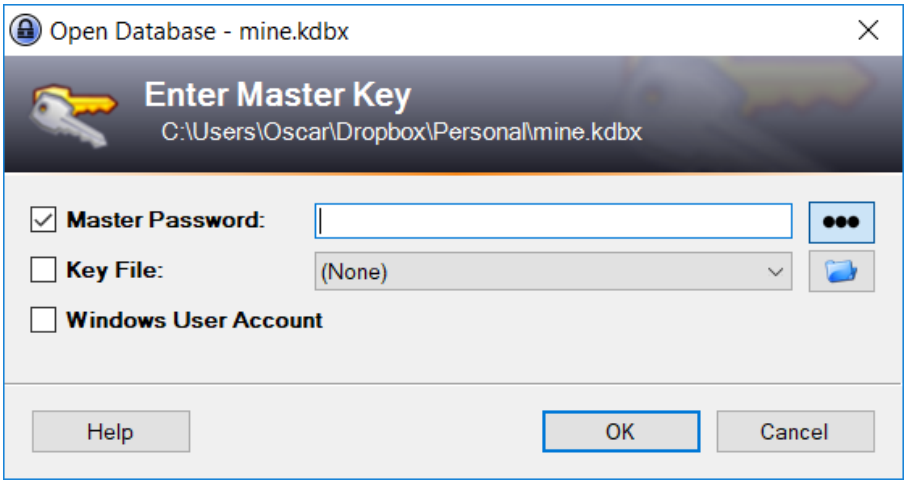
You can select a strong password if you follow the characteristics which are detailed in the University Password Guidelines at: https://www.uregina.ca/is/security/resources/resource-password.html.

You can also use a Key File which is a master password in a file. It's not recommended to use the Key file by itself but using a combination of both a Master password and Key file will greatly enhances the security of your password database as an attacker would have to know both your Master password and have access to your Key file. You will want to keep the Key file in a secret location other than your local hard drive and to have a secure backup of the file.

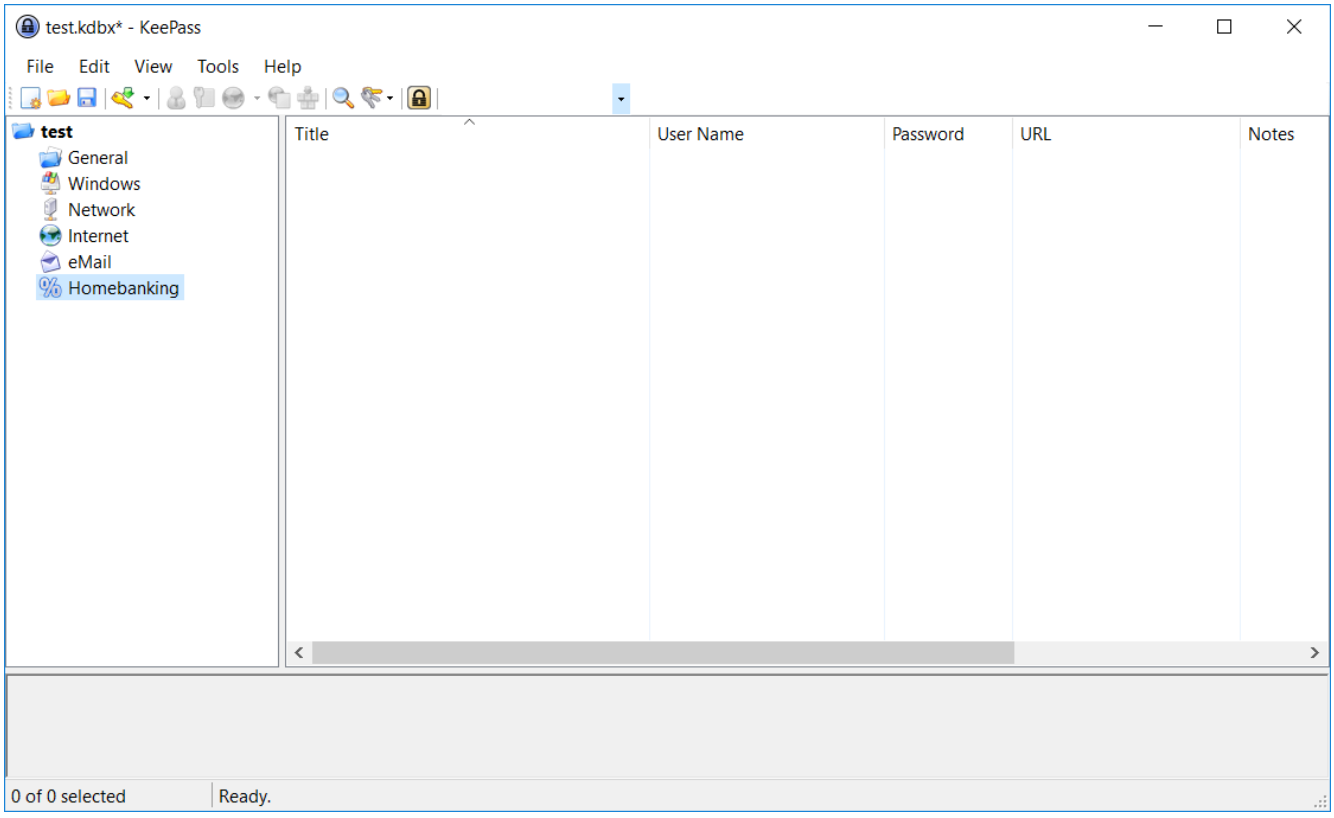
You'll next be prompted to adjust some database settings including name, description, and default name for all new key entries.



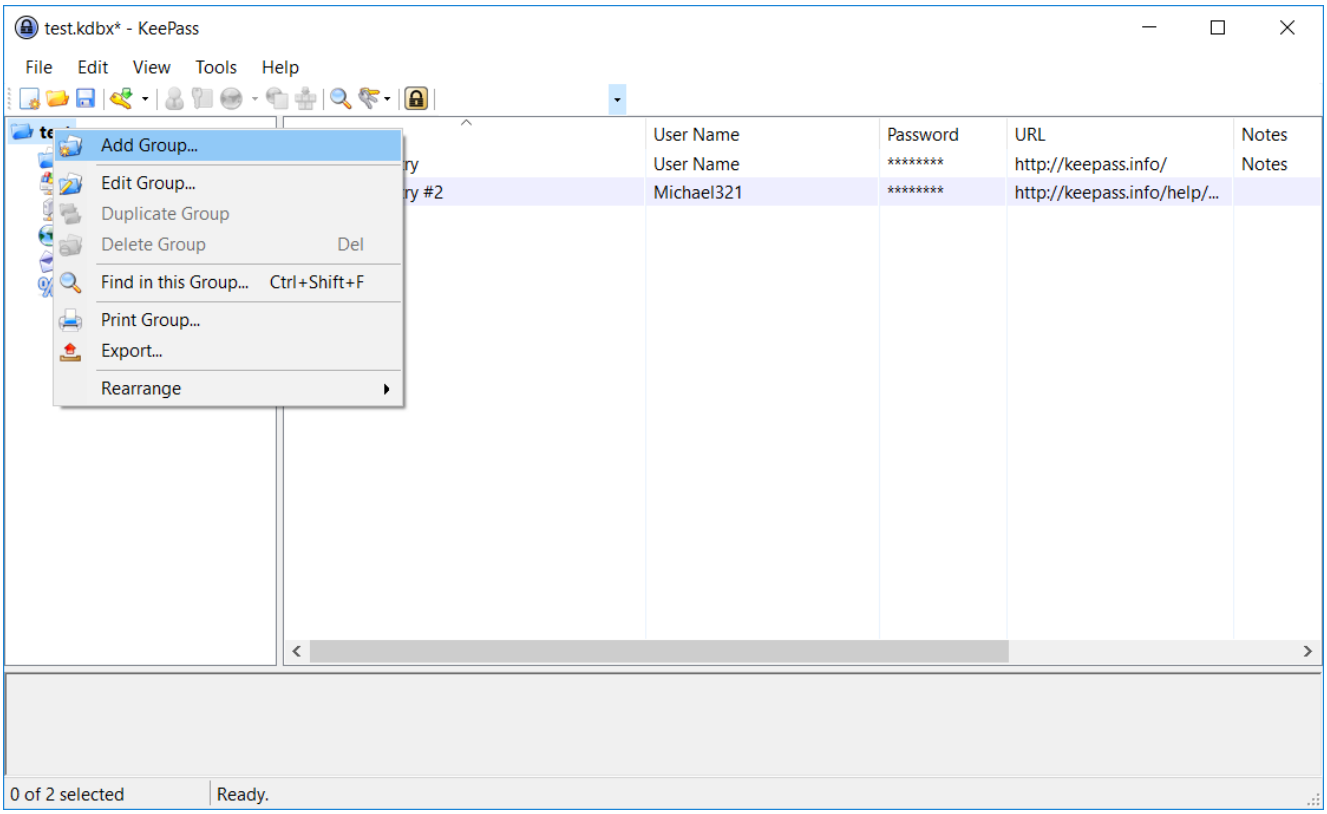
Once the database is saved, you'll be prompted to enter the Master password every time you open the program.



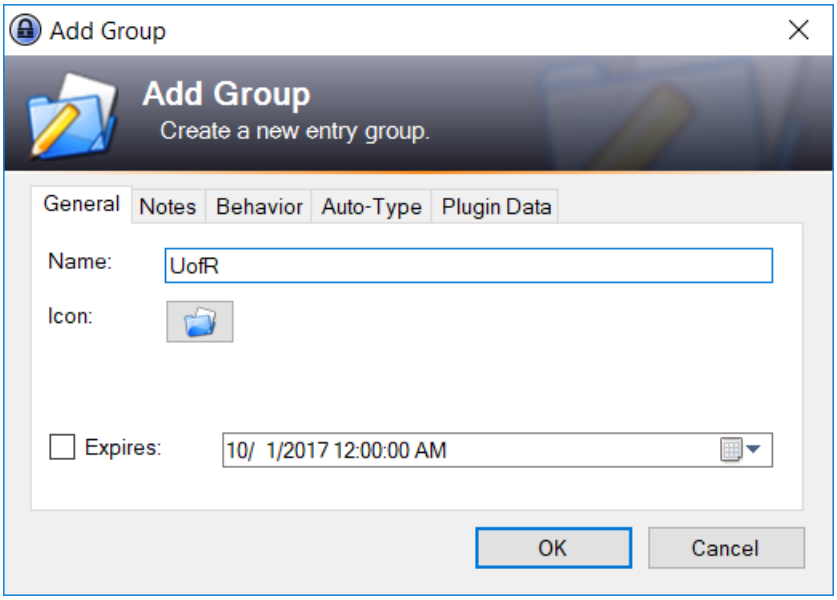
After opening the database, you'll be presented with the default view. The prebuilt groups can be deleted.



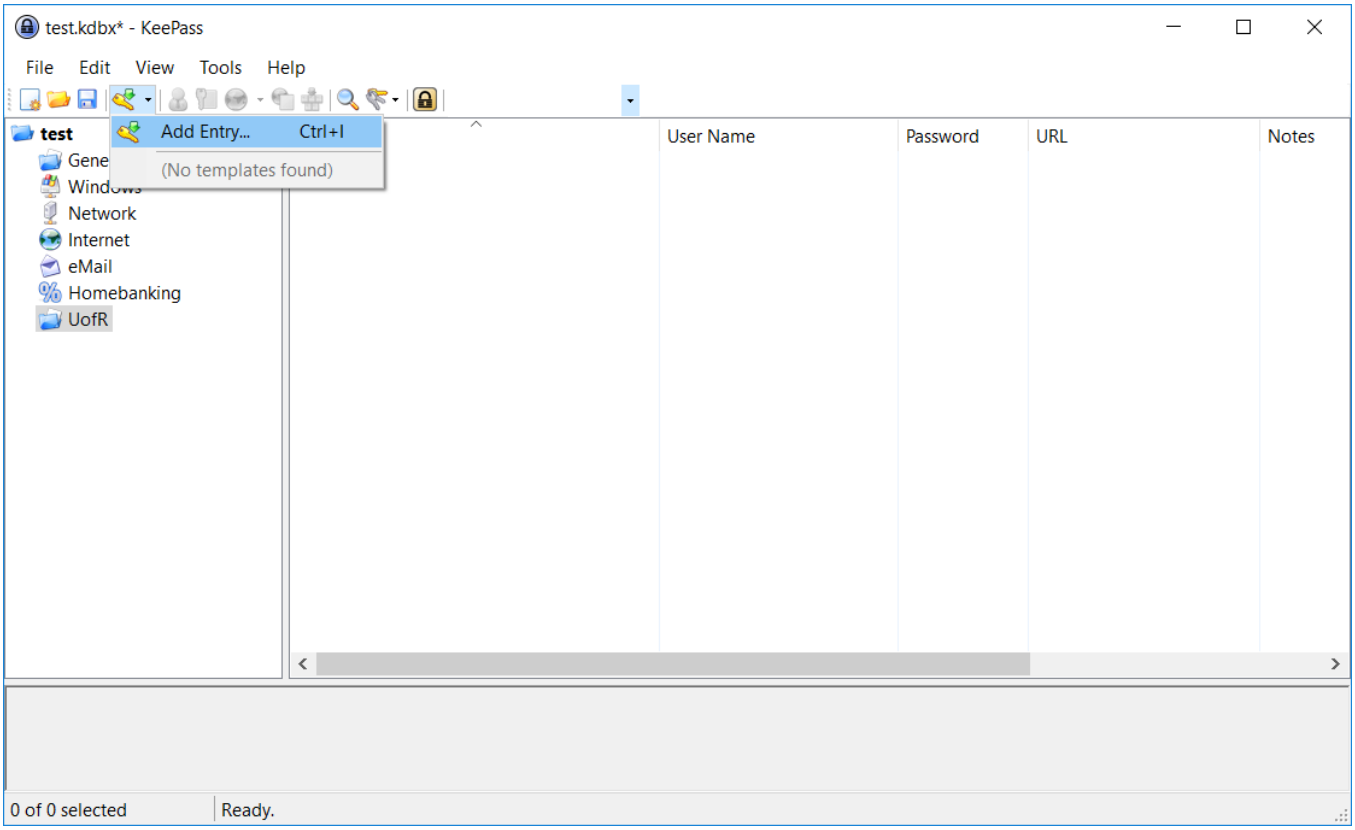
To create a new group choose Add a New Group from the database folder context menu.



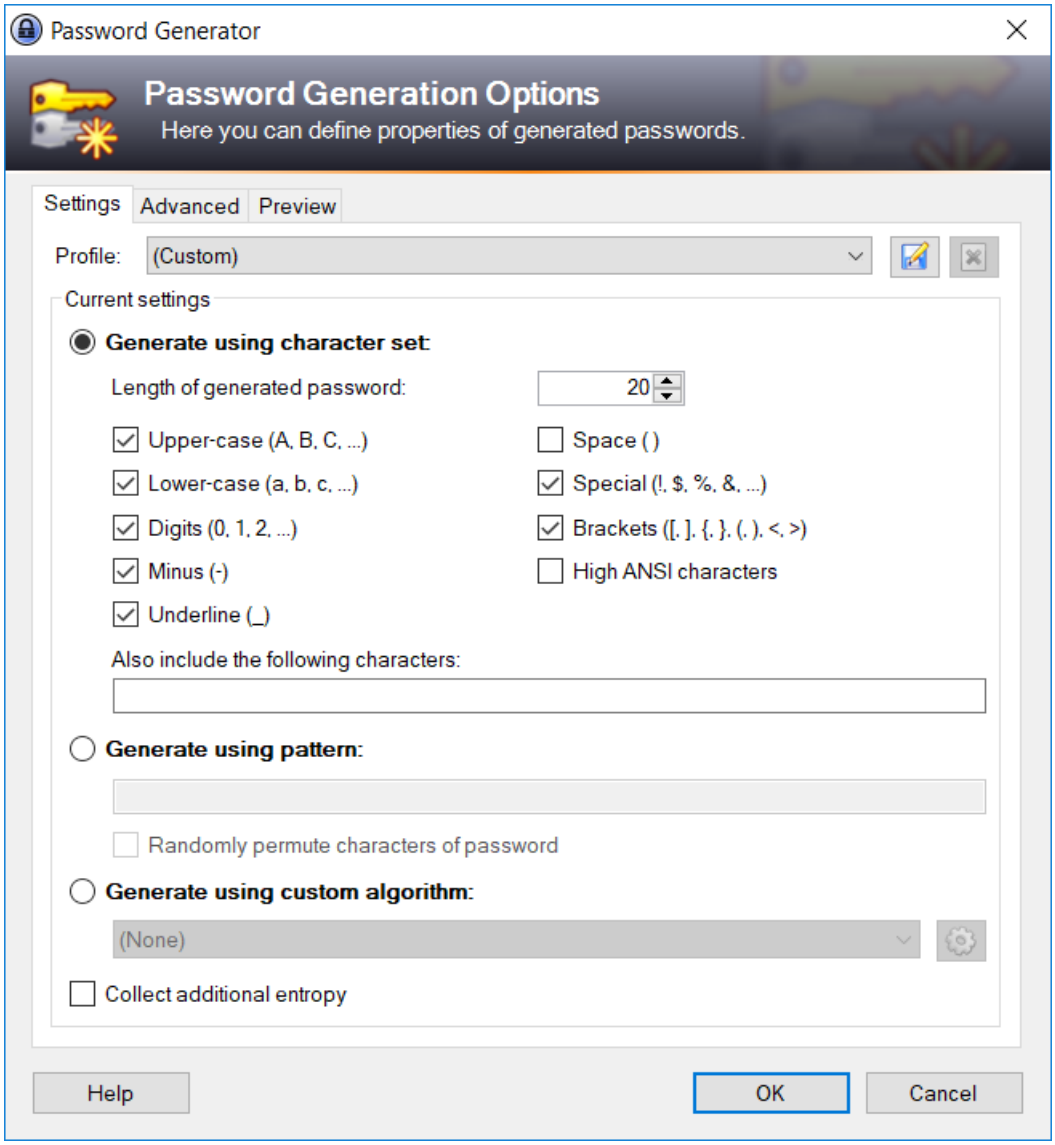
Enter the group properties including name, icon, and any notes.



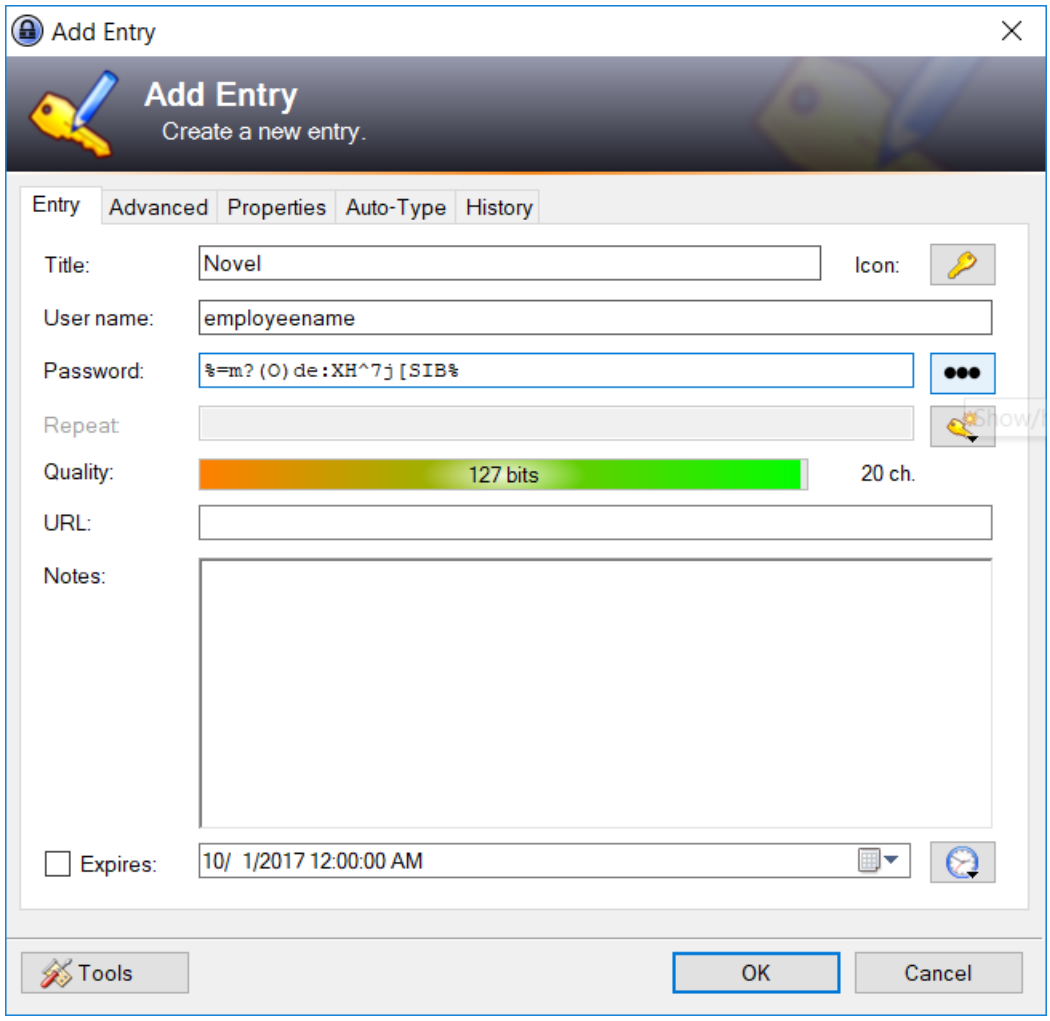
Now add the password entry you want to save in the group.



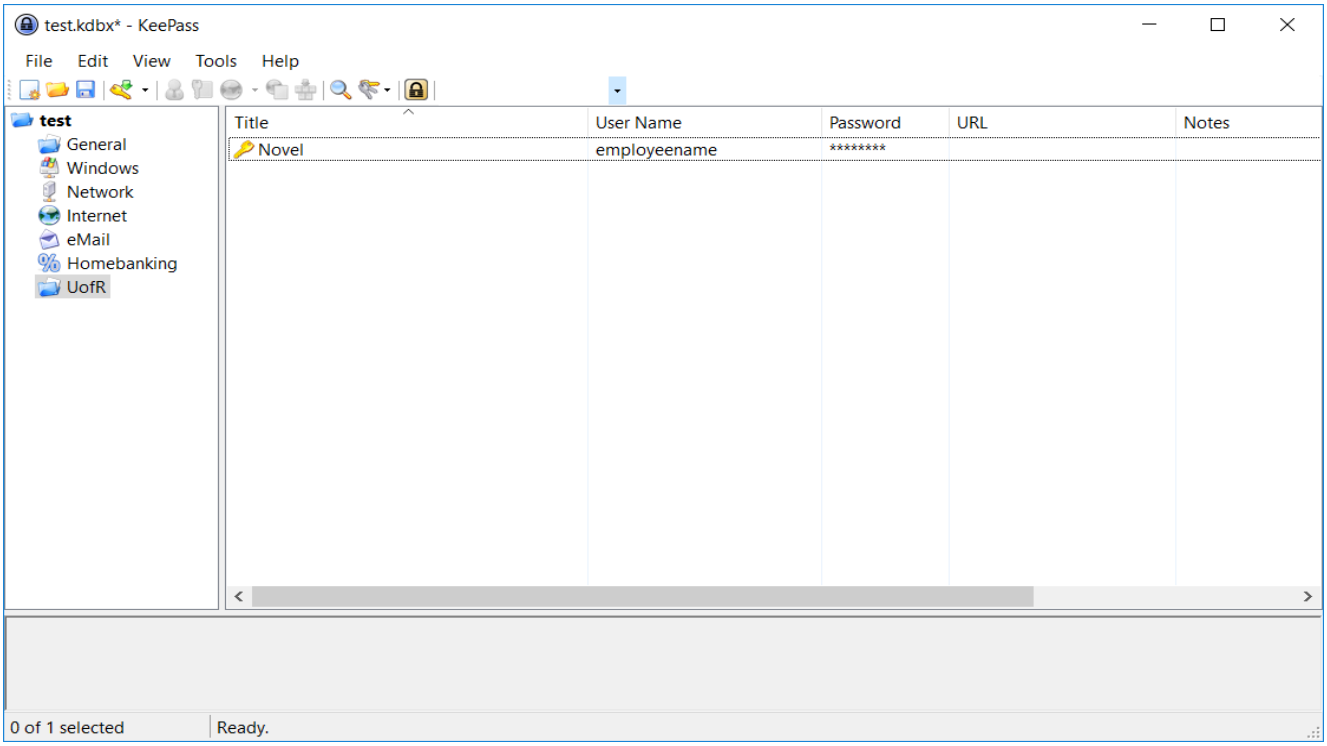
A note about the built-in password generator: the default options on the character sets being used should be changed to be as complex as possible. However, note that some software has limitations on what characters can be used. For example, there are limitations on University of Regina Banner passwords listed int eh password guideline webpage. Additionally, this should be configured to include all entries except spaces – many pieces of software won't accept spaces in passwords.



A dialog will pop up prompting to enter a title, user name that will use the password, a URL associated to where the password is used, and any notes you want to keep. Clicking on the ellipses button will show you the generated password.

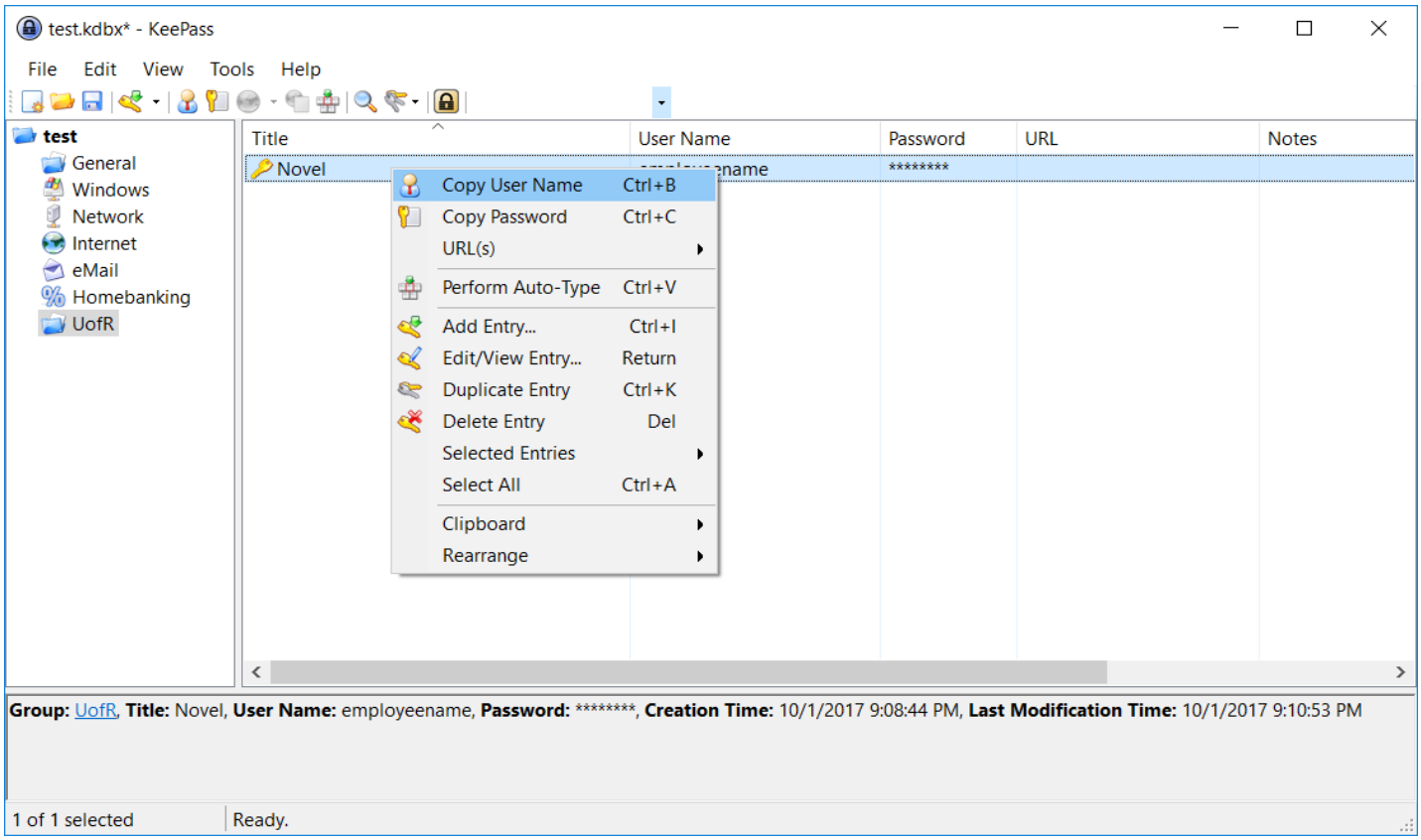


The new password key will now be displayed in the group folder.



Use Store Passwords:

To use the new key when prompted to enter a username and password into a software dialog box, just right click to bring up the keys context menu.



1. ctrl-alt-k opens your database.

2. ctrl-v when highlighting an entry changes to your browser and enters username + password, starting in the field that was active (i.e. you must've clicked in the 'username' box)

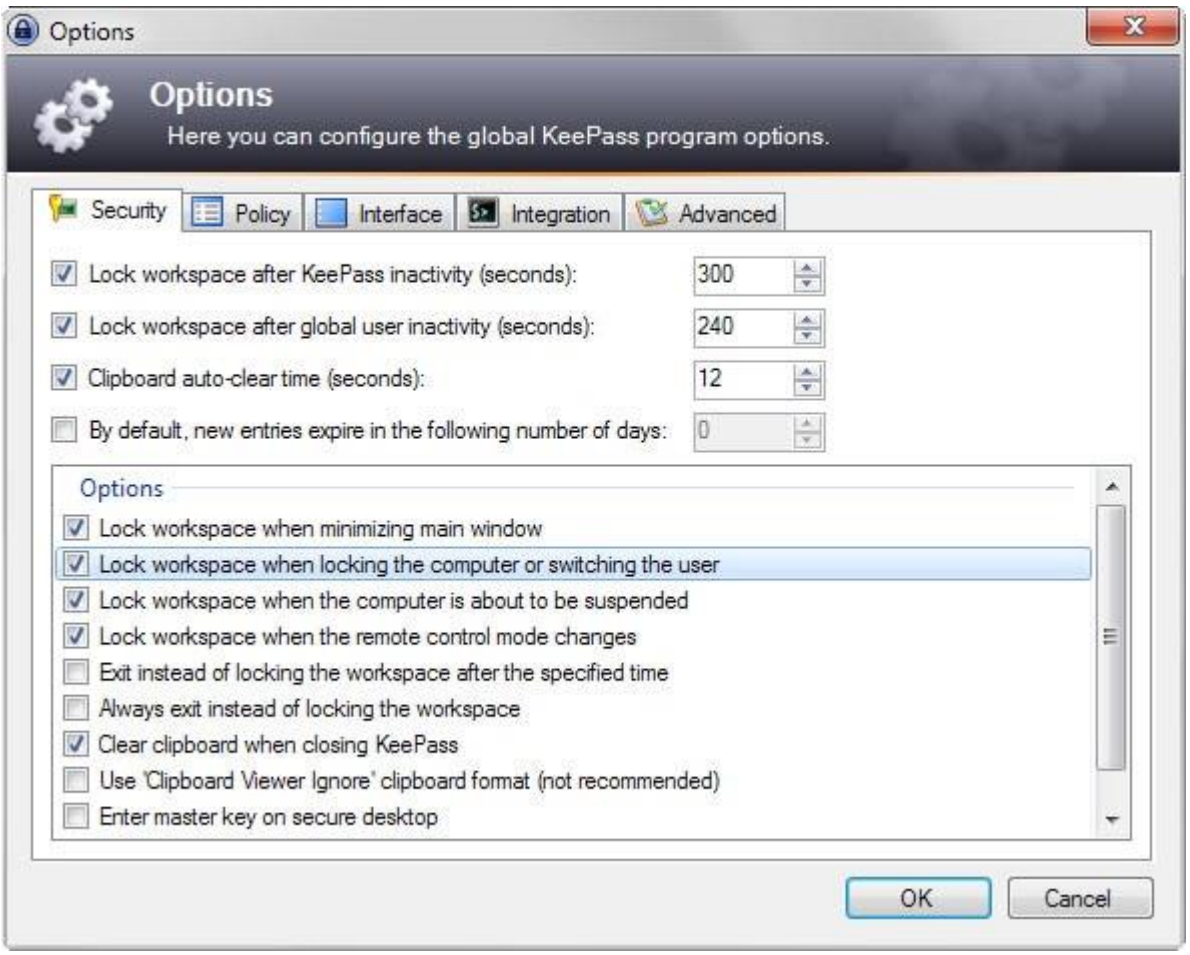
3. ctrl-c when highlighting an entry copies the password for you to paste into required field. Password is cleared from memory after 10 seconds

4. ctrl-f. Remember this, vital once you get quite a few passwords.

Locking KeePass Password Safe Workspace:

To ensure KeePass locks after a period of inactivity, ensure the following configuration is present:

1. Start KeePass and select Tools > Options from the menu.
2. Switch to the Security tab.
3. Ensure lock workspace after inactivity is set, lock workspace after global user inactivity is set, and clipboard auto-clear time is set to 300 seconds or less. Recommended settings are below.
4. Ensure the the following options are enabled:
    a. Lock workspace when locking computer or switching user
    b. Lock workspace when the computer is about to be suspended
    c. Lock workspace when remote control mode changes
    d. Clear clipboard when closing KeePass.



Additionally, ensure that the Lock button is pressed when KeePass is not in use. This secures your passwords if you step away from your computer.