Brunel University KeePass v2 User Guidelines

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins

Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Luke Woolford	Initial Draft	30/10/2019
V 1.0	Andrew Clarke	Format with ISMS standard template	05/11/2019
V 1.1	Luke Woolford	Add screenshots	05/11/2019
V 1.2	Luke Woolford	OneDrive Database location (1.2)	13/11/2019

Document Approval

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 05 Nov 2019
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

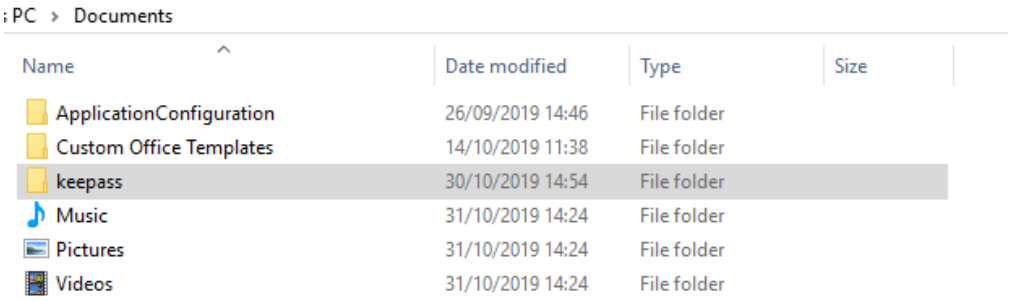
1.1 What is KeePass?

KeePass is a password safe software which stores all passwords, usernames and URLs for any websites or programs which require login credentials and authentication. Keeping this information in one software location means users are less likely to forget the vast amount of login credentials they may use within Brunel University.

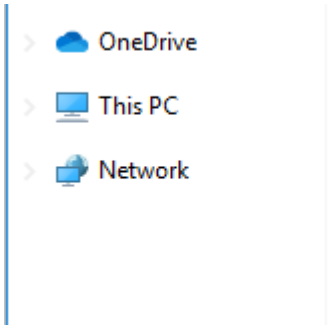
1.2 Where to place database folder

When the user starts the KeePass2 program for the first time they will be asked where they would like to place their Database folder, this will store all the information of the users password.
The default location for this folder would be the “Documents” folder within windows.

We highly recommend that the user relocate this folder within OneDrive so that they can access the database from different devices on campus and other locations (such as home).



To setup your database directory on your OneDrive, simply navigate to the “file” tab and go down to “Save As” then simply save the “database.kdbx” file within the OneDrive on your file explorer page.



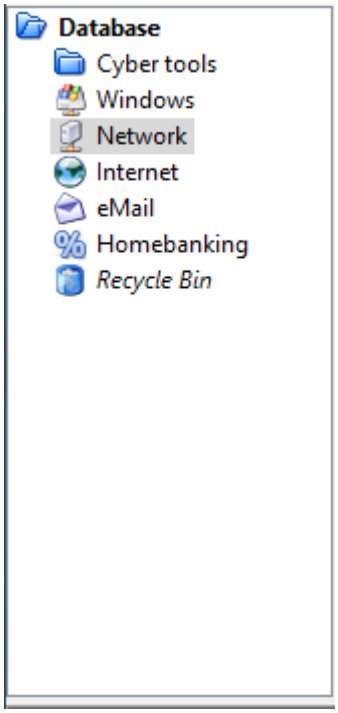
1.3 How to use KeePass

KeePass is extremely easy to use. First the user must create a master password which will allow them into their KeePass database.

This password is essential to retain access to all the passwords saved within the database. Never reveal this password to anyone and ensure that this password is never compromised.
Remember, the longer the password, the more secure it is. The recommendation is that this password is at least 12 characters long and uses one character from all four character sets

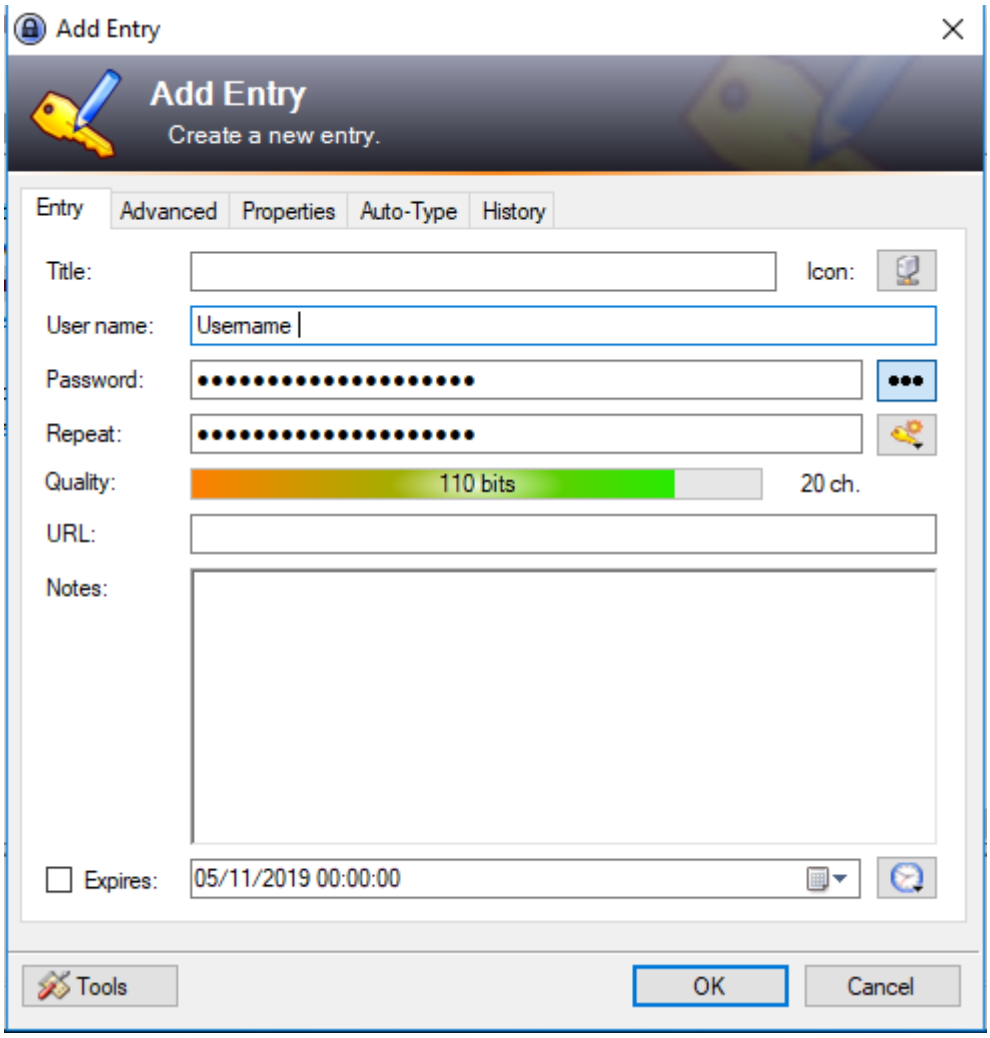
The database is located on the left hand side of the application and is broken down into customisable categories. For example the “eMail” tab may store all the passwords for email accounts you use on campus.

It will look something like this:



To add a password / account to the database the user must select a category in the database on the left side. Then right click the window to the right of the database and then left click “Add entry” which will open up the add entry prompt.
Once the user has navigated to this page they must enter a custom title for the entry so they can easily remember it, then they can proceed to enter the specific details for that login.

For example:



To view the password click the three dots to the left of the text box

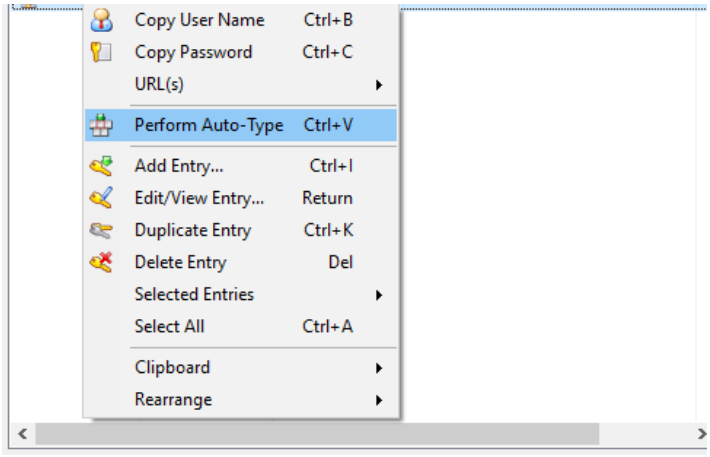
Once the user has entered their details they must copy and paste the URL which is related to that specific entry. Unless it is an application login then they can leave it blank.

Once that is completed, click the “Ok” button and navigate to “file” and “save” this will save any added entries or the user can alternatively press (Ctrl + S).

1.4 How To autofill passwords

Once the user has created an entry they can navigate using the web browser or open the program which they have made that entry for and have KeePass open at the same time. Then open KeePass with the required login screen in the background and right click the required entry then click “Perform auto type” the program would begin to fill in the details on the login screen.

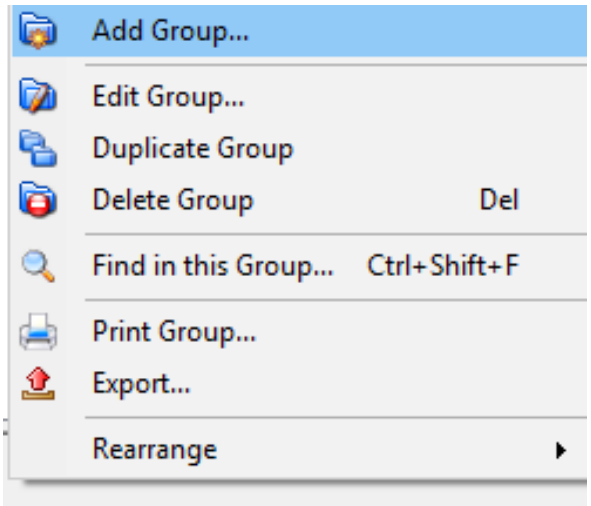
Alternatively the user can highlight the required entry and press (Ctrl + V).



1.5 How to add / edit a group

To add a group the user must simply right click the database window located on the left hand side of the application and click “Add group” then add a custom name in the group name text box.

Alternatively the user can edit one of the pre-set groups by right clicking on the group and clicking “Edit group” and then altering the text box.



1.6 How to lock your passwords within the application

To lock the application the user can click on the little lock icon on the top taskbar which will minimise the app and require the master password to open again. Alternatively the user can simply close down the app and next time they login it will prompt the password again.

Warning!

Users should not forget their master password, if they forget this password there is no way or getting back into the application or recovering the user's passwords. However DO NOT leave a password text file on your computer as then all your passwords will not be secure. It is recommended to save the master password on another device or write it down and store it safely somewhere (or better yet just remember it!)