

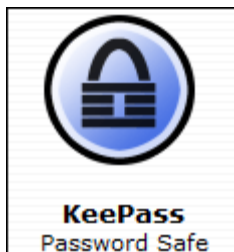
The Best Password Manager for Windows – Mac – Linux / Ubuntu – Smart Phones and more...

- http://technerdia.com/284_password-manager.html

When it comes to kick butt little tools, KeePass wins hands down!

This tool has changed how I use my computer, my browsers and even how I plan for vacations.

What is KeePass? Simply, it's a very secure password manager, that can group your passwords together for easy management. And it works on just about everything, Windows of all flavors, Smart Devices like the iPhone, Droids, BlackBerry's, and so on... Linux/Ubuntu, Mac OS X, I'm probably missing a few. It's light weight, simple to use, has a movable database... truly, it rocks.



Other than Google, every Password I have is no longer stored in my browser. I keep everything, from the web, ftp, shell, database and client

secure details in my KeePass.

- I only have one password to remember, and that's to KeePass.
- I use KeePass to generate long random passwords for me.
- No site, service or feature has the same password.

Downloading KeePass: <http://keepass.info/>

The options are the Classic Edition and Professional Edition. The Pro Edition requires MS .NET Framework.... I downloaded the [Classic Edition](#). Choose either, or go with the Classic if you're not sure which one to choose.

Installing KeePass

KeePass is portable, it doesn't make registry changes and runs without special libraries. You can place it on a USB drive and even run it on a public machine all without installing anything.

Setting up KeePass

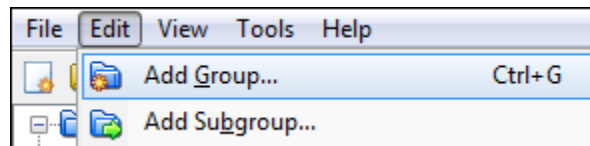
Once you run KeePass it will ask you to create a database and Composite Master Key, which I recommend doing for Security reasons. You have two things to remember here, your Master Password (so select a strong one) and the location to where you save the Database.kdb and pwsafe.key files.

- Be sure to backup your Database.kdb and pwsafe.key files once you've populated them with account details.
- Your pwsafe.key file may be hidden on your Computer depending on your OS and setup. You may need to unhide important files before you can copy the key file for a backup.

Running KeePass

Once you start KeePass, enter your Master Password and select your Key. The software can be a bit confusing at first, but a couple features cover most of your needs.

First is Groups, groups simply group your accounts/passwords together. I have groups for my clients (with sub-groups inside of it), affiliate programs, social networks, tools, forums, etc.



- **To create a group:** Click the Edit link at the top, then select Add Group



The next feature is Adding an Entry. On the main toolbar, it's the 4th icon. If you mouse over it, it says Add Entry. Clicking Add Entry brings up a window to enter the details. Everything here is self explanatory other than maybe the Password Generator.

- **To add an entry:** Click the 4th icon in the main menu (Add Entry) or access the Edit link at the top, then select Add Entry.

Every new entry gets a fresh new password, click the icon to the right of the Password box to expose the password, for copying or pasting in a new password.



If you want to generate a new password, click the Keys Icon to the right of the Repeat Password box. At the bottom of the window, click the Generate button to create a new password. It's instantly copied over to the entries password field.

Maintaining Entries

Each entry can be dragged into groups. So if the entry is created in the wrong spot, simply select and drag it to the proper location.

To View or Edit an Entry, right click on the Entry and select Edit/View Entry. Use this same menu to delete or duplicate an entry.

Creating Multiple Databases For Others To Access

Does your Computer get used by your spouse, kids or staff? Then no worries... In the main menu, click the New Icon (first icon). Set a new Master Key then your Password. Now everyone can have a unique way to access PassKeep to store passwords.

My spouse uses her own Master Key File while my kids just have a Password enter with no Key File to select. It's hard enough to get children to use this software, so cut out every step you can that may push them away from using it, every time!

- Backup your database and key file before doing this.

KeePass Settings

To access the Settings open the Tools Menu at the top, then click on Options. Setting up the software is really more about how you want to use it...

- **Security:** I have two fields unchecked, the 3rd (Lock wordpress) and the last (expire entries) - the others are all checked.
- **Interface (GUI):** The two key settings here for me are the Minimize and [x] close selections. I have both selected. Instead of the software closing, it goes to my system tray, when I open it - I have to enter my Master Password, just like I would if the software was fully closed.
- I didn't modify any other settings past these.... I do suggest you read through the other tabs & features to ensure the settings are set how you like.

Vacation Time



I always take a note pad and pen with me when I travel. Every time before traveling, I would write down the most important login details, passwords, and even url's. No worries, I used my own form of encryption to mask things.

Today though... I just grab a copy of KeePass, my Database and Key file and put them on a flash drive and I burn a CD to toss in with my suitcase as a backup. I also put the information in a zip file on my server, within a password protected directory.

No longer do I worry about losing my note pad, backup paper in my wallet or what actually happened the most, I forgot to write down a password to something important.... I'm very happy to say, those worries are now gone.

KeePass

It's here to stay... It's used daily, it's used by family members, it's even used on vacations. You should be using [KeePass](#) as well.

Proper security starts and ends with you!

**[Follow techNerdia on Google+](#) | [Follow Chris on Google+](#)
[Subscribe to techNerdia's RSS Feed](#)**

Copyright 2012 © [techNerdia](#) - All Rights Reserved
<http://techNerdia.com/>