KeePass Guide [EN]

Goal

KeePass is a password manager that has many advantages over other password managers:

- It’s self-hosted, the data always stays on your devices
- You can use it to keep track of your global security and of all the services you use
- You can use it to store PGP secret keys
- You can also store all kinds of other informations about your account
- You can also connect it to your browser to easily insert your password when needed
- Since the passwords will only show up if the URL is correct, it can also protect you against fishing attacks
- You can also use it for 2 factor authentication since it can generate OTP codes

Here we’ll see how to configure it to be as secure as possible while being synchronized on multiple devices using Syncthing.

Documentation

You can find further documentation about the tools we’ll use here on the following websites:

- KeePassXC User Guide
- Syncthing’s getting started guide

Installation

Since I want this tutorial to be cross-platform, I’ll not cover the installation, you can look on the resources below to know more…

- Installing KeepassXC (for all desktop devices)
- Installing KeepassDX (for all Android devices)
- Installing Synchting (for all devices to be synchronized)

Creating the database

1. Once you installed KeePassXC, you can create a new empty directory then open Keepass and create a new database in the empty directory.
2. When asked for a passphrase, use the built-in tool to generate a random, secure password and set the word length to 7.
3. Write down the passphrase and keep it safe.
4. You can then add new accounts in KeePass.
5. After a while of getting used to your passphrase, you might try to destroy the paper you wrote it on

Setting up the browser addon

1. Install the KeepassXC-Browser addon
2. In the settings of KeepassXC, enable browser integration for the browser you use
3. Go in the addon and click on “connect”, then choose a name for the browser.
4. Finally, when you go on a site that requires logging in, click on the keepass icon and click on “Allow” to allow keepass to auto-fill the details

Synchronizing with other devices

1. On device A, click on “Add a new device” then add the ID of device B
2. On device B, allow the connection to device A
3. Open Syncthing and add a new shared directory. Then select the directory containing the keepass database. Select device B in the settings to share it with.
4. Accept the transfer on device B and select where you want it to be saved. After a few minutes the two should be synced.
5. Open the database using Keepass

Setting biometrics on a phone for easier access

1. Open the synchronized keepass database in keepassDX, then open it with your passphrase
2. In KeepassDX’s settings, go in advanced unlocking and enable biometric unlocking so you can use your fingerprint instead of always typing your passphrase
3. Lock the database then type your passphrase, click on the fingerprint icon to enable it.

Using Keepass

- To create a basic entry, click on “+” then fill the info for the title, username, password and URL.
- You can also go in the “icon” section and download the icon of the website.
- You can also go in the “advanced” section to add your secret key as an attachment or add any additional data there
- To add a TOTP (2 factor auth), right click on the entry and choose “TOTP” then “Define a TOTP”. In there you can put your TOTP token.

> For TOTP, make sure the clocks on all your devices are perfectly synchronized otherwise it won’t work.

Analyze your global security

1. Press CTRL+MAJ+R to get the statistics
2. Then go in “Health Check” to locate security issues.
3. Go in HIBP and click on the analyze button, this will tell you if one of your password have been corrupted.

Revision #1
Created 2 August 2023 11:37:03 by SnowCode
Updated 2 August 2023 11:38:44 by SnowCode