

keepass

- [Keepass](#)
 - [Keepass Download](#)
 - 1.xx or 2.xx
- [Dropbox](#)
 - [Dropbox download](#)
- [Installation](#)
- [Creating password database example](#)
- [Open password database](#)
- [Creating new entry](#)
- [Keepass on Android](#)
- [Keepass on iOS](#)

Keepass

Saving your passwords offline using keepass (<https://keepass.info/>). Why keepass? It is free and open source. It also have number of plugins (see <https://keepass.info/plugins.html>), that I do not use.

Keepass Download

OS	Name	Link
Windows	Keepass	https://keepass.info
Mac OS	MacPass	https://macpassapp.org/
iOS	MiniKeePass	https://itunes.apple.com/app/id451661808
Android	keepass2android	https://play.google.com/store/apps/details?id=keepass2android.keepass2android

More can be found at <https://keepass.info/download.html>

1.xx or 2.xx

1.xx have less features, but more 3-rd party clients (at least it was so several years ago).

Now I would use 2.xx (files with kbdx extension)

Dropbox

to sync password database between devices any cloud file sync service can be used. For example <https://www.dropbox.com/>

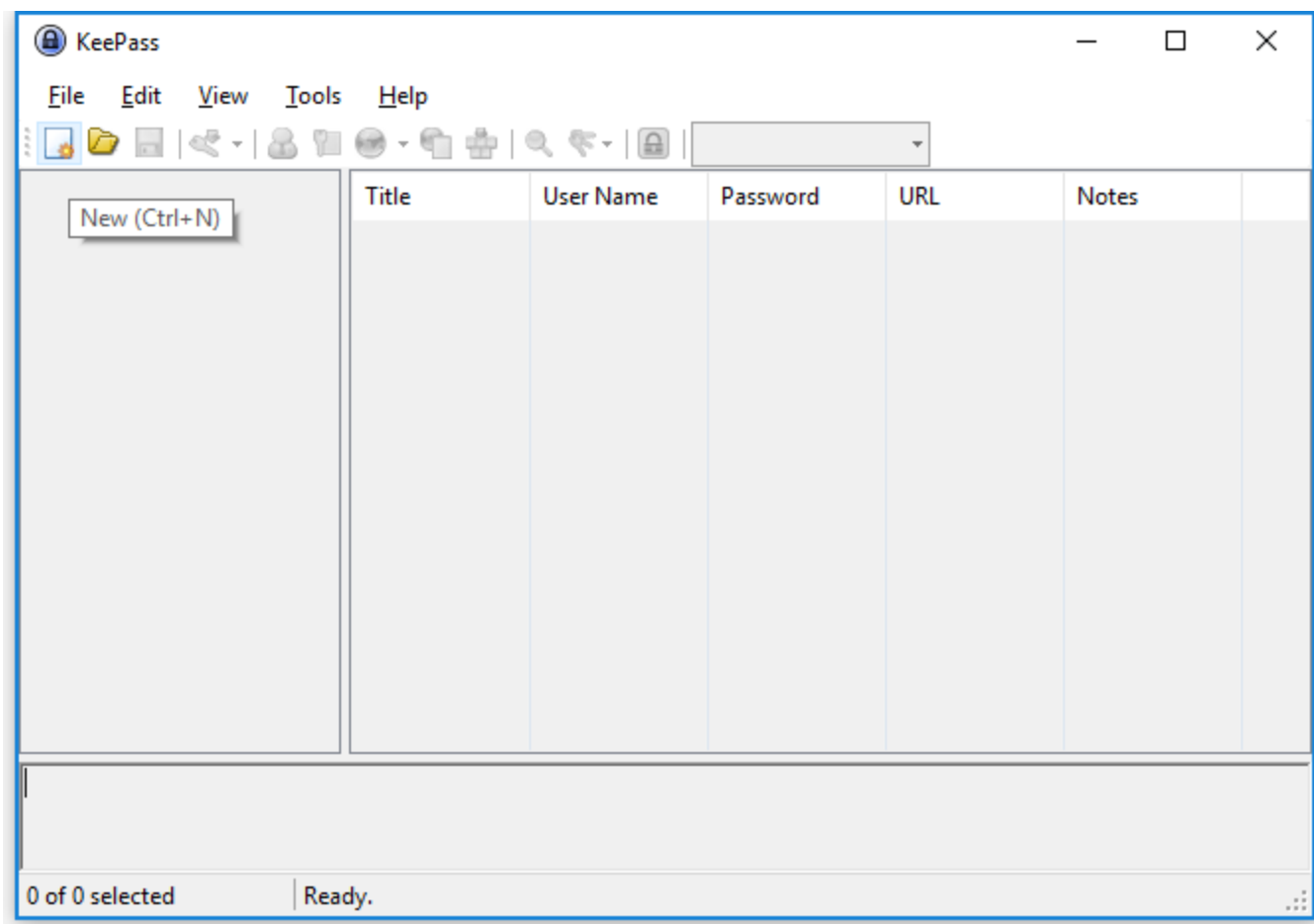
Dropbox download

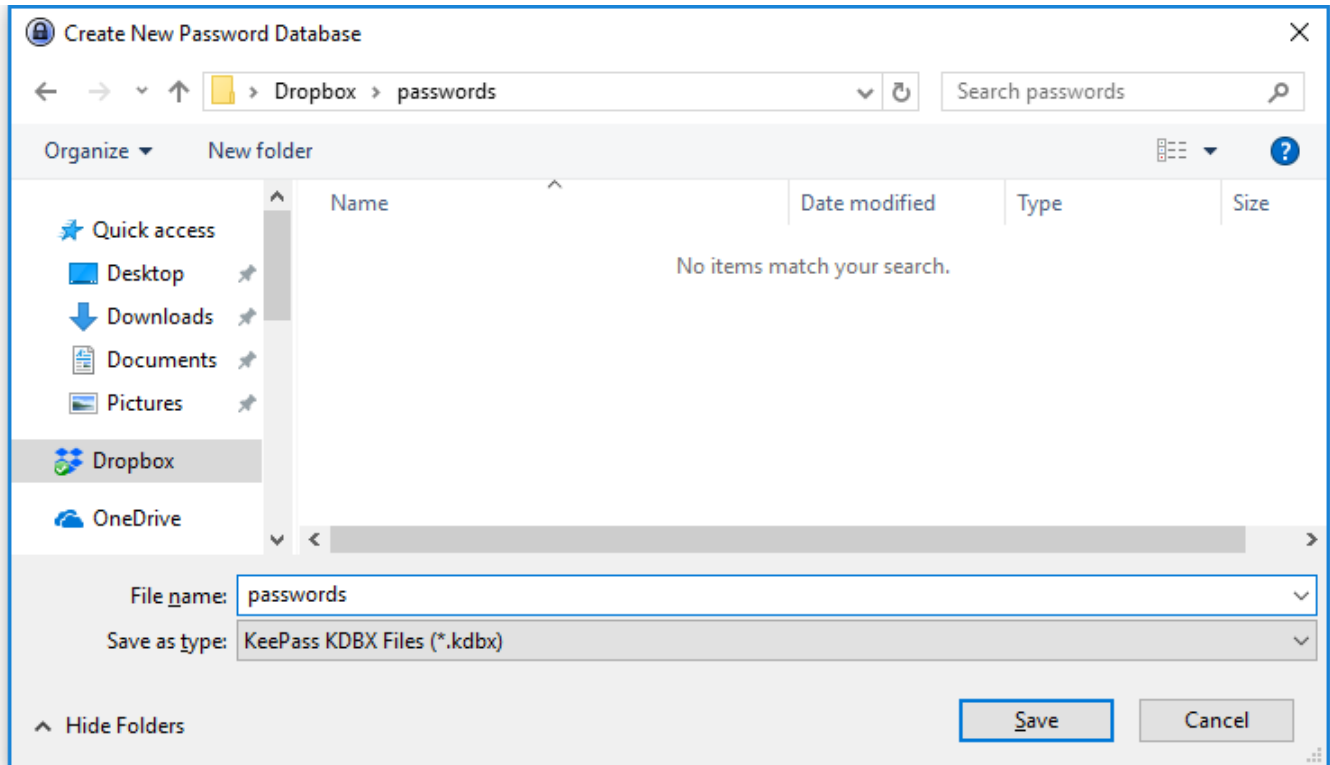
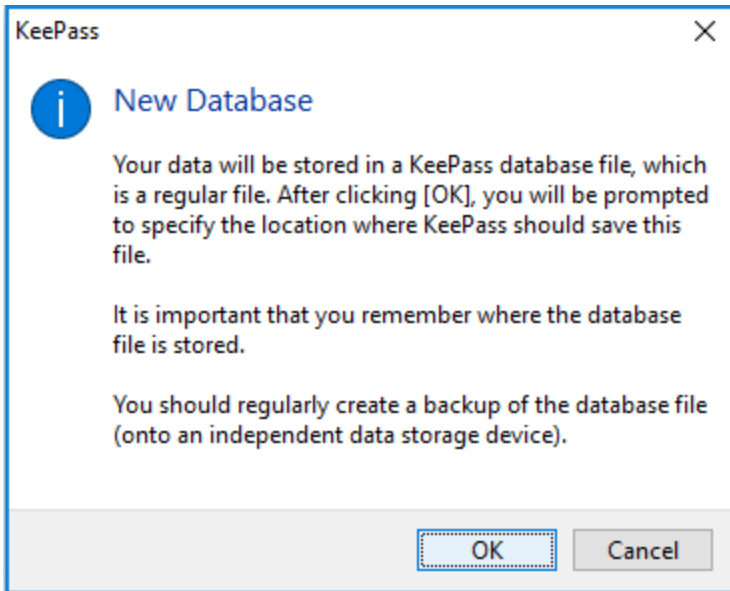
OS	Name	
Windows	Dropbox	https://www.dropbox.com/install
Mac OS	Dropbox	https://www.dropbox.com/install
iOS	Dropbox	https://itunes.apple.com/app/id327630330
Android	Dropbox	https://play.google.com/store/apps/details?id=com.dropbox.android

Installation

1. Setup Dropbox client on all devices
2. Setup keepass client an all devices
3. Create password database in Dropbox folder
4. Open password database on other device
5. Enjoy 😊

Creating password database example





Choose some Master password that is important to remember. On Screenshot is example with **\$tr0ngPass2018** (45bit)



Create Composite Master Key



Create Composite Master Key

C:\Files\OL\Dropbox\passwords\passwords.kdbx

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

A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database anymore.



Master password:

.....



Repeat password:

.....

Estimated quality:



45 bits

14 ch.



Show expert options:

Help

OK

Cancel

Create New Database - Step 3

Database Settings


Here you can configure various database settings.

General Security Compression Recycle Bin Advanced

Database name: Oleksandr Liutyi Passwords

Database description:
All my passwords for everything I have :)


Default user name for new entries: liutyi

☐ Custom database color: 

Help OK Cancel

Some optional fine tuning (slower open - better brute force attack protection, use compression, etc.)

Create New Database - Step 3



Database Settings

Here you can configure various database settings.

General

Security

Compression

Recycle Bin

Advanced

On this page you can configure file-level security settings.

Encryption

Database file encryption algorithm: AES/Rijndael (256-bit key, FIPS 197)

Key transformation

The composite master key is transformed using a key derivation function. This adds a work factor and makes dictionary and guessing attacks harder.

Key derivation function: AES-KDF

Iterations: 15460352

The more iterations, the harder are dictionary and guessing attacks, but also database loading/saving takes more time.

1 Second Delay


Test

Help

OK

Cancel

Create New Database - Step 3



Database Settings

Here you can configure various database settings.

General

Security

Compression

Recycle Bin

Advanced

Data compression reduces the size of the database.

Algorithm	Compression	Performance
<input type="radio"/> None	No compression	Moderate
<input checked="" type="radio"/> GZip	Moderate	Very good

Help

OK

Cancel



Create New Database - Step 3



Database Settings

Here you can configure various database settings.

General

Security

Compression

Recycle Bin

Advanced

☒ Use a recycle bin

If this option is enabled, KeePass moves entries/groups to the recycle bin group instead of deleting them. Deleting an entry/group from the recycle bin will permanently remove it.

Recycle bin group:

(Automatically create new)



Help

OK

Cancel

Create New Database - Step 3

Database Settings

Here you can configure various database settings.

General Security Compression Recycle Bin **Advanced**

Templates

Entry templates group:

(None)

Click the drop-down arrow of the 'Add Entry' toolbar button in the main window to create a new entry based on a template in the group above.

Automatic entry history maintenance

☒ Limit number of history items per entry: 10

☒ Limit history size per entry (MB): 6

Master key

☐ Recommend changing the master key (days): 182

☐ Force changing the master key (days): 365

☐ Force changing the master key the next time (once)

Help OK Cancel

KeePass

Emergency Sheet

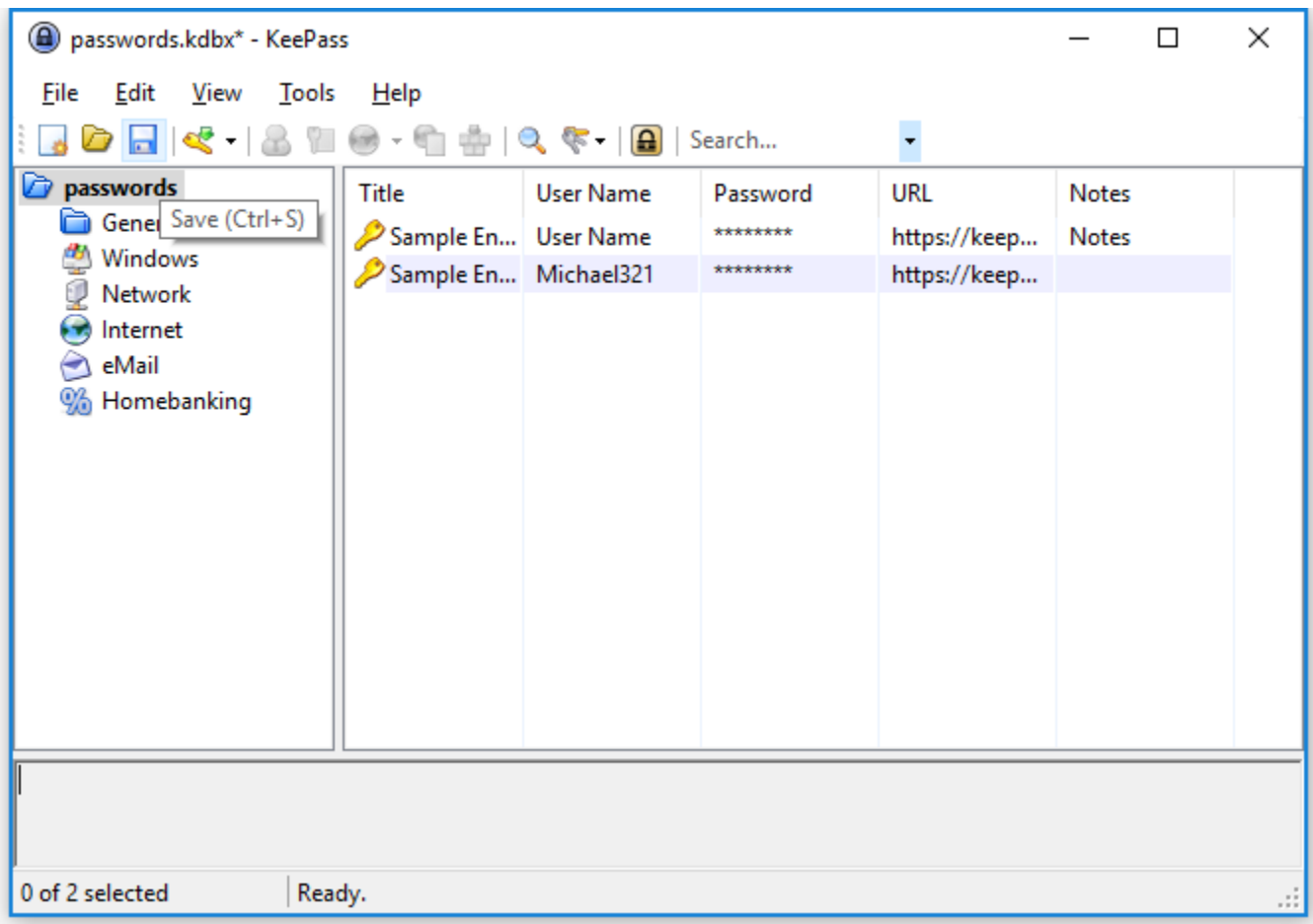
A KeePass emergency sheet contains all important information that is required to open your database. It should be printed, filled out and stored in a secure location, where only you and possibly a few other people that you trust have access to.

It is recommended that you create an emergency sheet for your database.

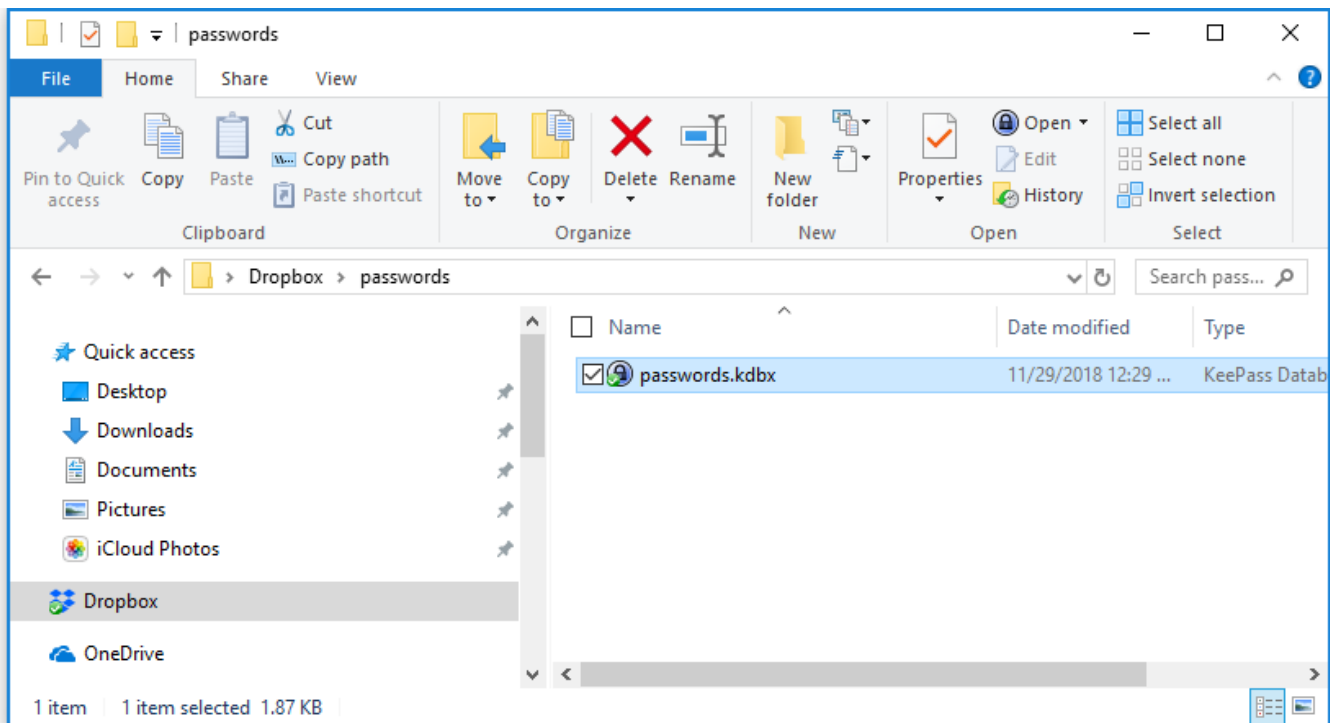
Do you want to print an emergency sheet now?

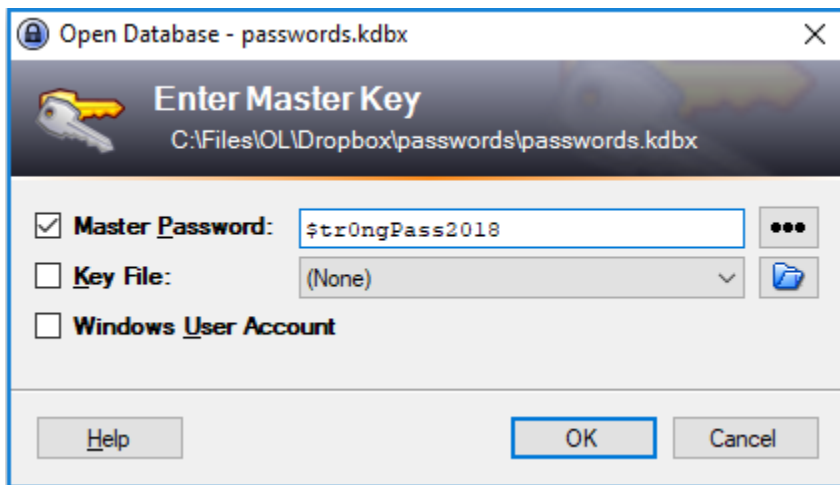
→ Print
KeePass will print an emergency sheet, which you can then fill out.

→ Skip



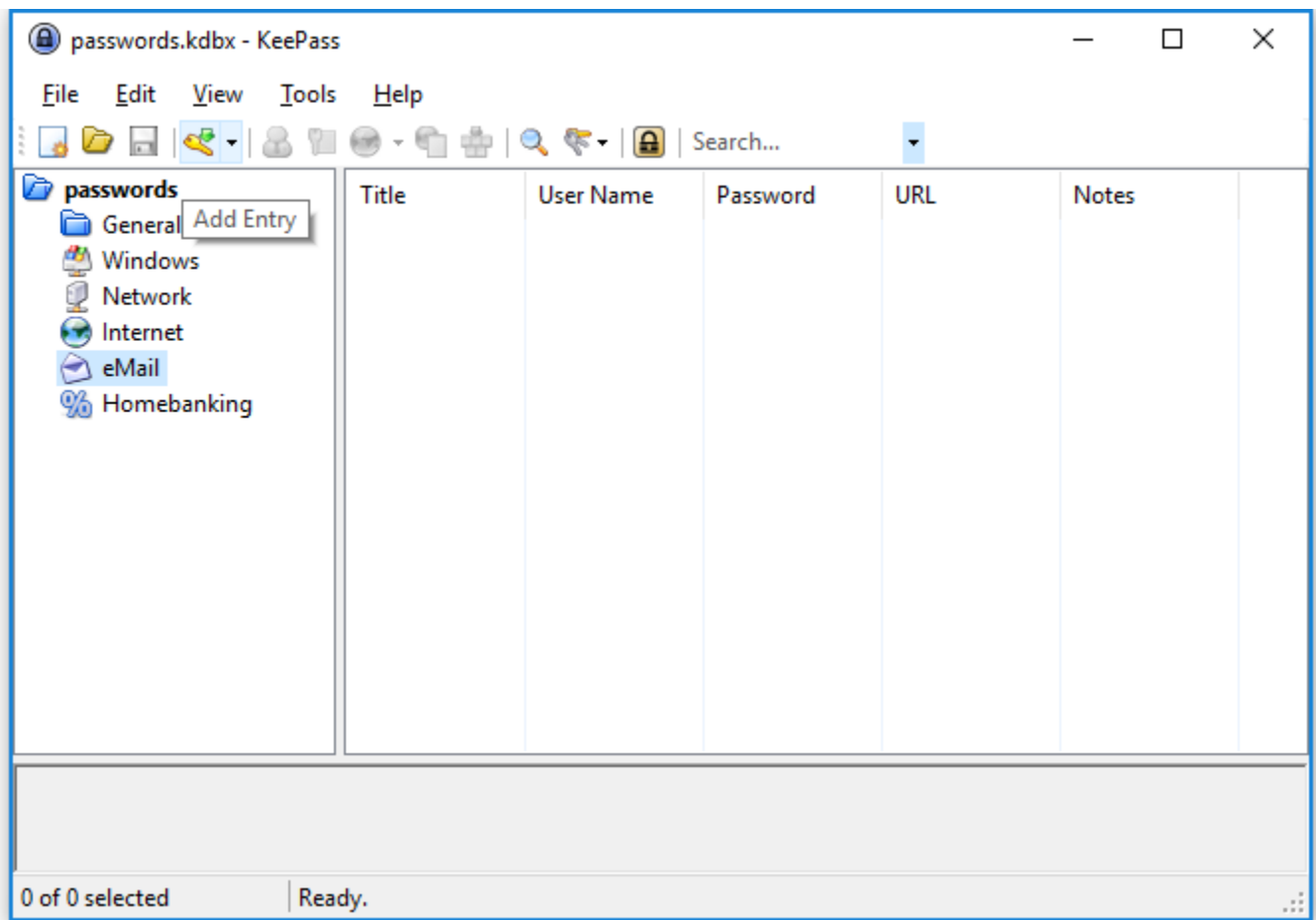
Open password database








Creating new entry

1. Choose folder
2. Press Add Entry
3. Input login, (generate or) input password, url, notes, icon (all optional).
4. Save database



 Add Entry





Add Entry

Create a new entry.

Entry

Advanced


Properties

Auto-Type

History


Title:

Icon:




User name:

Password:



Repeat:



Quality:

116 bits


20 ch.


URL:


Notes:

Not in use, was created ...

☐ Expires:

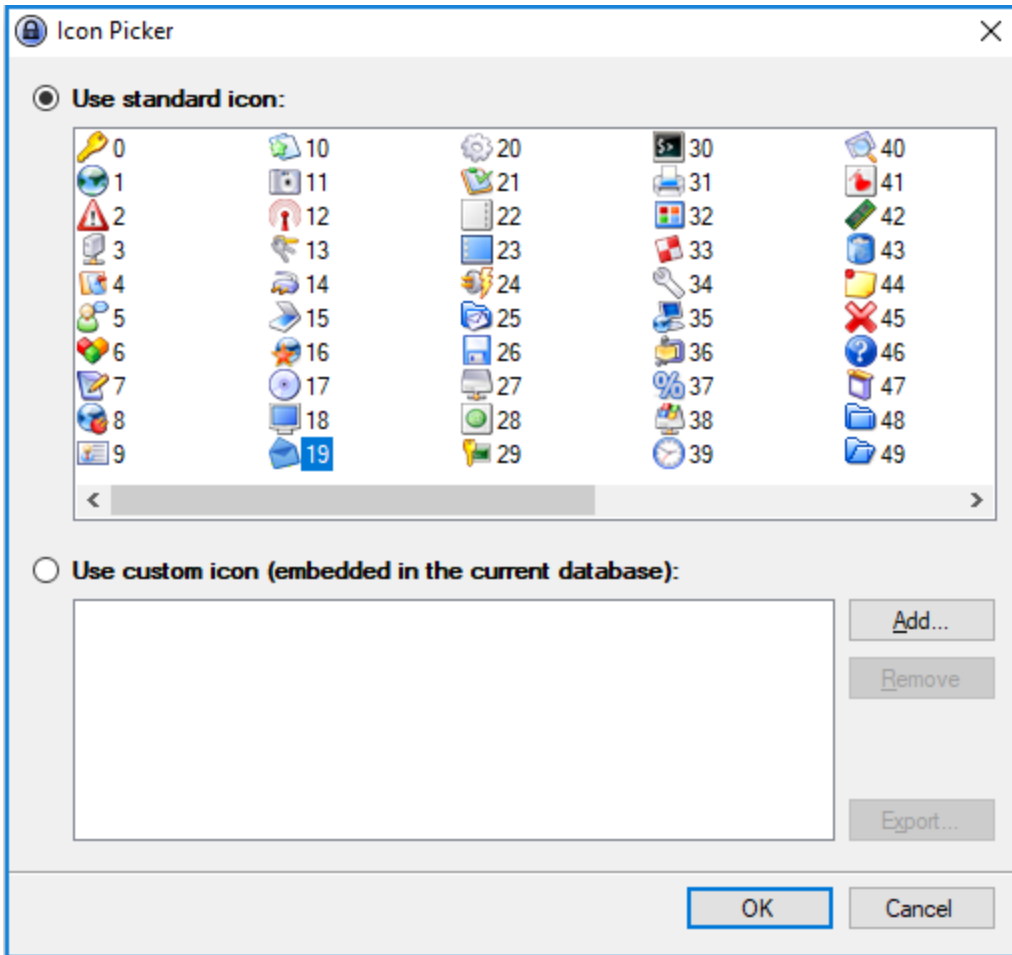






 Tools


OK

Cancel



 Password Generator







Password Generation Options

Here you can define properties of generated passwords.

Settings



Advanced

Preview

Profile: (Custom)  

Current settings

☒ **Generate using character set:**

Length of generated password: 12  

☒ Upper-case (A, B, C, ...)

☐ Space ()

☒ Lower-case (a, b, c, ...)

☐ Special (!, \$, %, &, ...)

☒ Digits (0, 1, 2, ...)

☐ Brackets ([,], {, }, (,), <, >)

☐ Minus (-)

☐ High ANSI characters


☒ Underline (_)

Also include the following characters:

☐ **Generate using pattern:**

☐ Randomly permute characters of password

☐ **Generate using custom algorithm:**

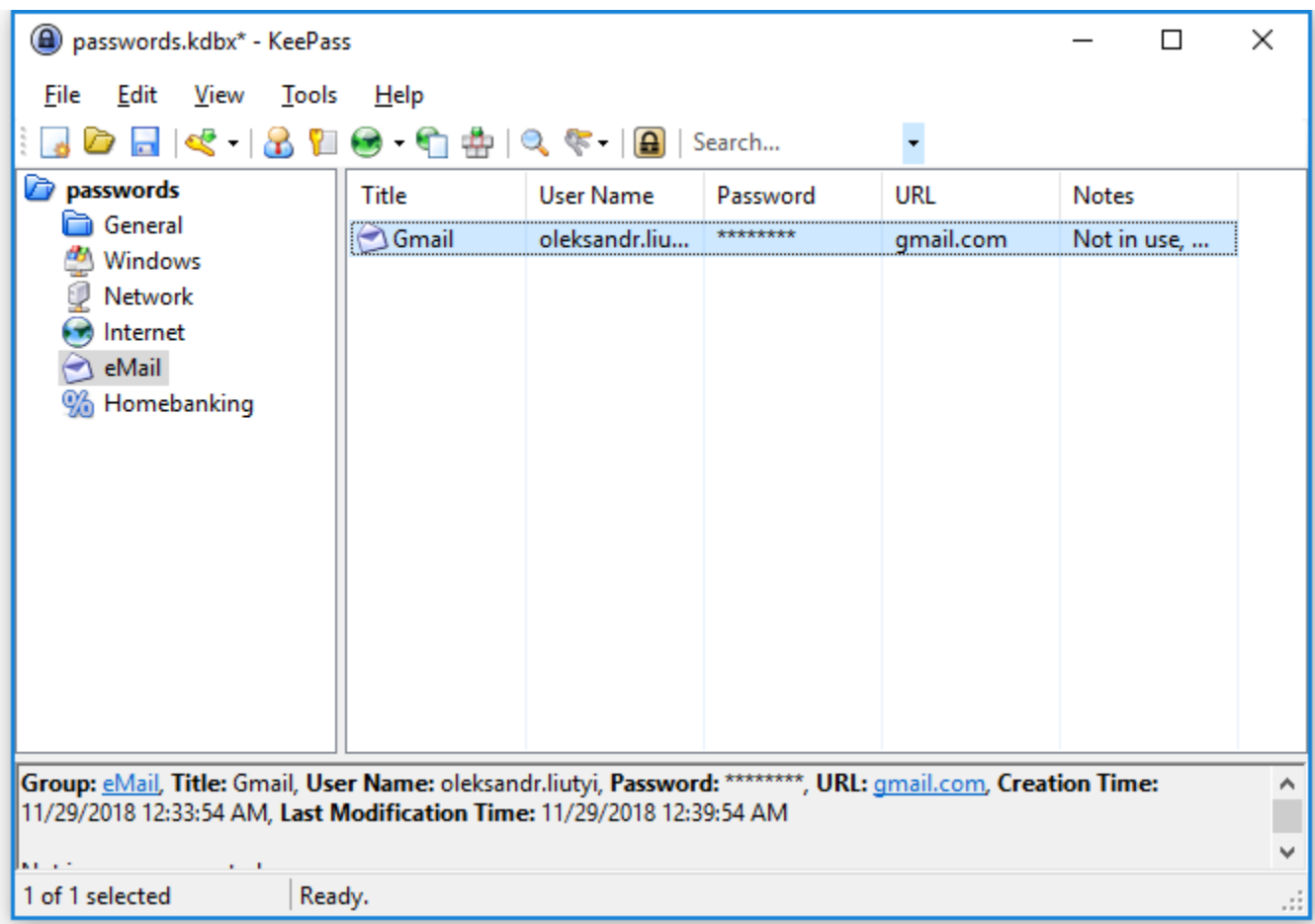
(None) 

☐ Collect additional entropy

Help

OK


Cancel



Keepass on Android

00:45

Google Play


 **Keepass2Android**
Password Safe
Phillipp Crocoll (Croco Apps)

Tools

INSTALL

4.6 ★
21K reviews

18 MB
Rated for 3+ ⓘ

 **Keepass2Android**


Keepass2Android is a password manager compatible with KeePass 2 (.kdbx) files

[Read more](#)

Rate this app

00:45

Select the storage type

 **Keepass2Android**

Open file...

Create new database...

System file picker

Dropbox

Dropbox (KP2A folder)

Google Drive

OneDrive

SFTP (SSH File Transfer)

FTP

HTTP (WebDav)


HTTPS (WebDav)

OwnCloud

Get from third-party app

00:46

Dropbox



Keepass2Android would like access to the files and folders in your Dropbox. [Learn more](#)


Allow
liutyi@gmail.com

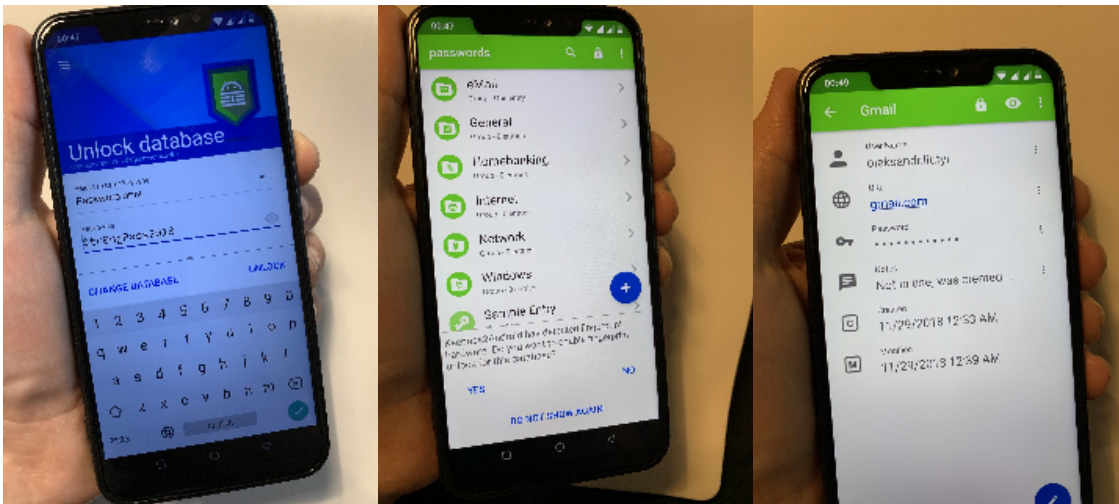
Use a different account

00:46

Choose file...

Root • passwords

 passwords.kdbx 2.11 KiB, 12:42 AM



Keepass on iOS

