2022

A VMsources Whitepaper

KeePass Secure Password Manager

JOHN BORHEK / VMSOURCES

Contents

Introduction

The reality is that as individuals and Organizations we have to create, apply and use and sometimes transmit a tremendous number of passwords.

Not only that, passwords must be stronger than ever in order to keep Threat Actors from brute-forcing their way onto your systems.

Current recommendations for just how strong vary, but at VMsources we recommend a minimum of 16 characters with mixed: upper, lower, numbers and special.

Why use KeePass? KeePass is widely regarded by security experts as the best and strongest password manager available.

"KeePass stands out among password managers for its superior security and customization." *- Forbes*[i]

KeePass has the following use advantages:

- Completely free OSI Certified open source
- Strongest database encryption possible: AES-256, ChaCha20 and Twofish
- Supports network installation[ii]
- Copy & Paste passwords without having to expose them
- Clipboard auto-delete
- Export individual passwords or groups of passwords for secure sharing by email

Sincerely,

John Borhek

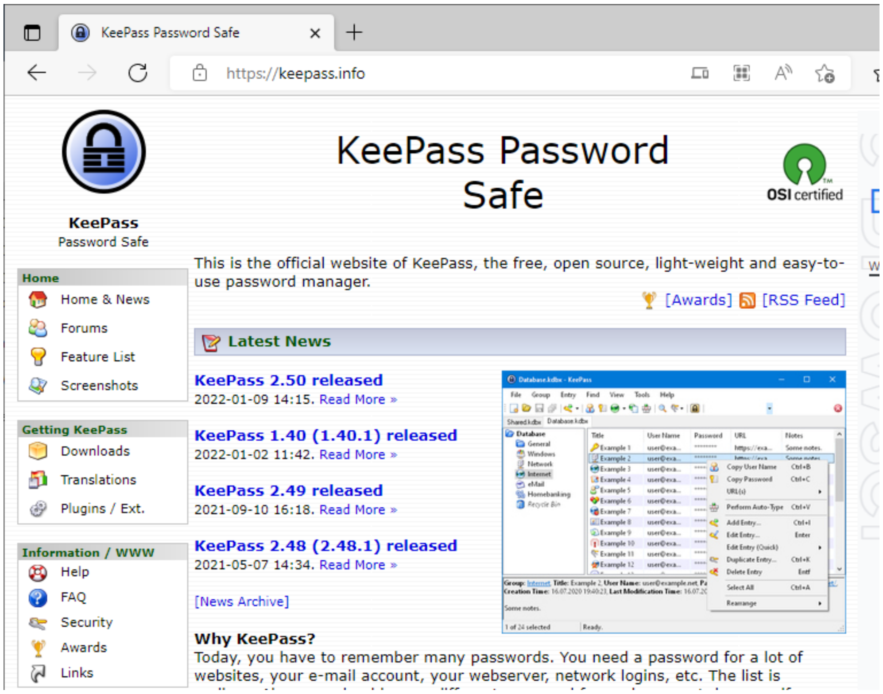
John Borhek,
Lead Solutions Architect

Email:	john@vmsources.com
Website:	https://vmsources.com
Mobile:	+1 928.606.0483
Office:	+1 215.764.6442 X1001

Getting and Installing KeePass

1. Link to: KeePass Password Safe

2. Download KeePass



KeePass Password Safe

This is the official website of KeePass, the free, open source, light-weight and easy-to-use password manager.

KeePass 2.50 released
2022-01-09 14:15. Read More »

KeePass 1.40 (1.40.1) released
2022-01-02 11:42. Read More »

KeePass 2.49 released
2021-09-10 16:18. Read More »

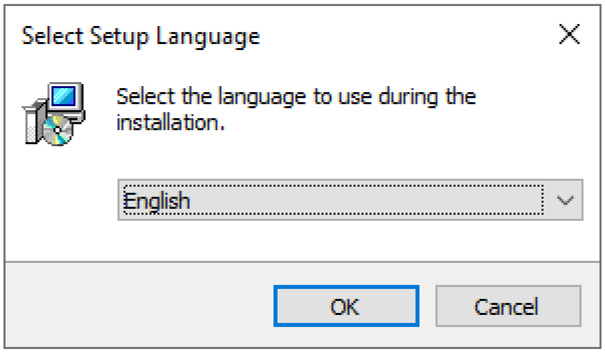
KeePass 2.48 (2.48.1) released
2021-05-07 14:34. Read More »

Why KeePass?
Today, you have to remember many passwords. You need a password for a lot of websites, your e-mail account, your webserver, network logins, etc. The list is

3.

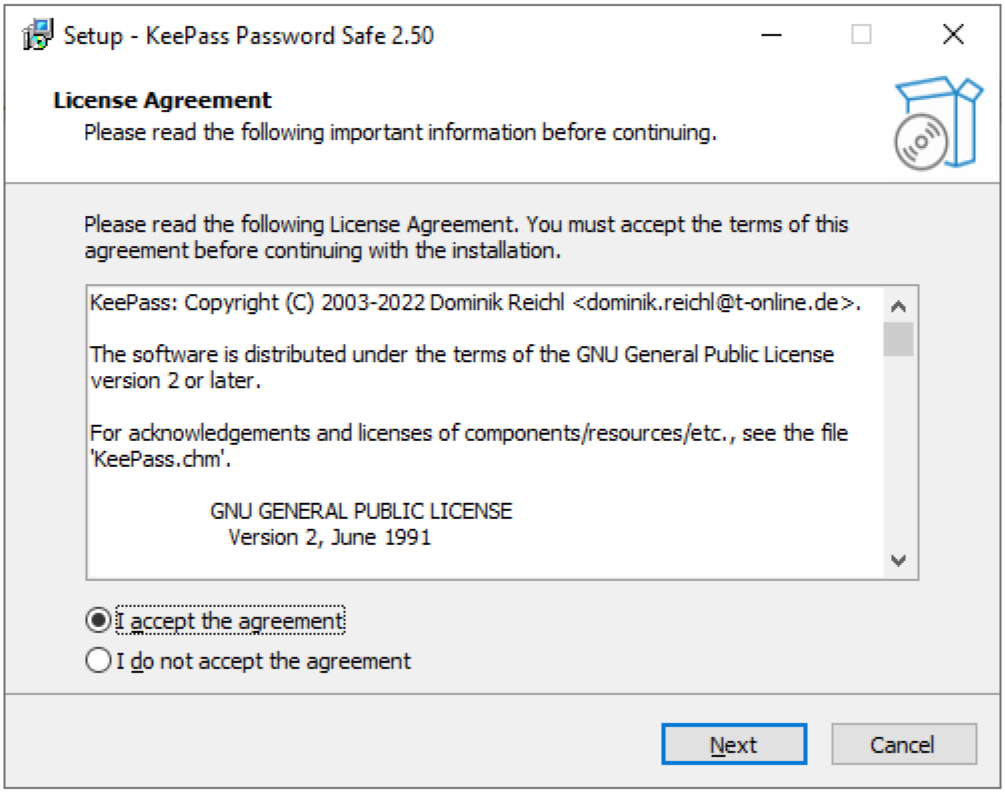
4. Install KeePass

a.



Select the language to use during the installation.

English


b.

Setup - KeePass Password Safe 2.50

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

KeePass: Copyright (C) 2003-2022 Dominik Reichl <dominik.reichl@t-online.de>.

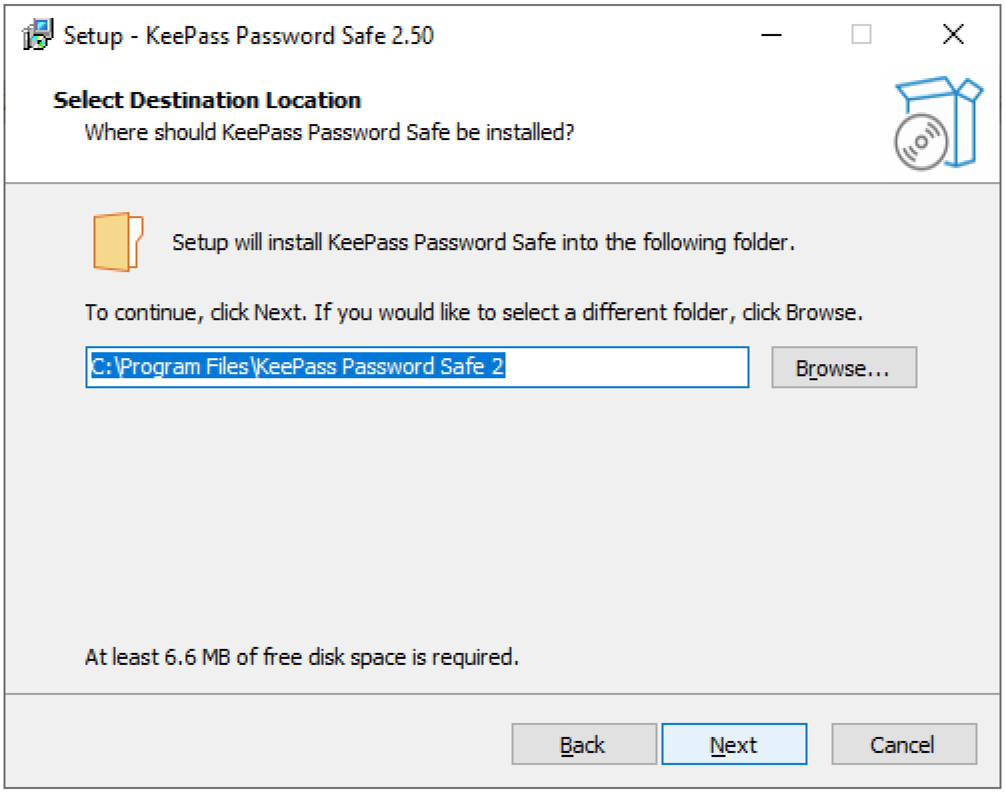
The software is distributed under the terms of the GNU General Public License version 2 or later.

For acknowledgements and licenses of components/resources/etc., see the file 'KeePass.chm'.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

● I accept the agreement

○ I do not accept the agreement


c.

Setup - KeePass Password Safe 2.50

Select Destination Location

Where should KeePass Password Safe be installed?

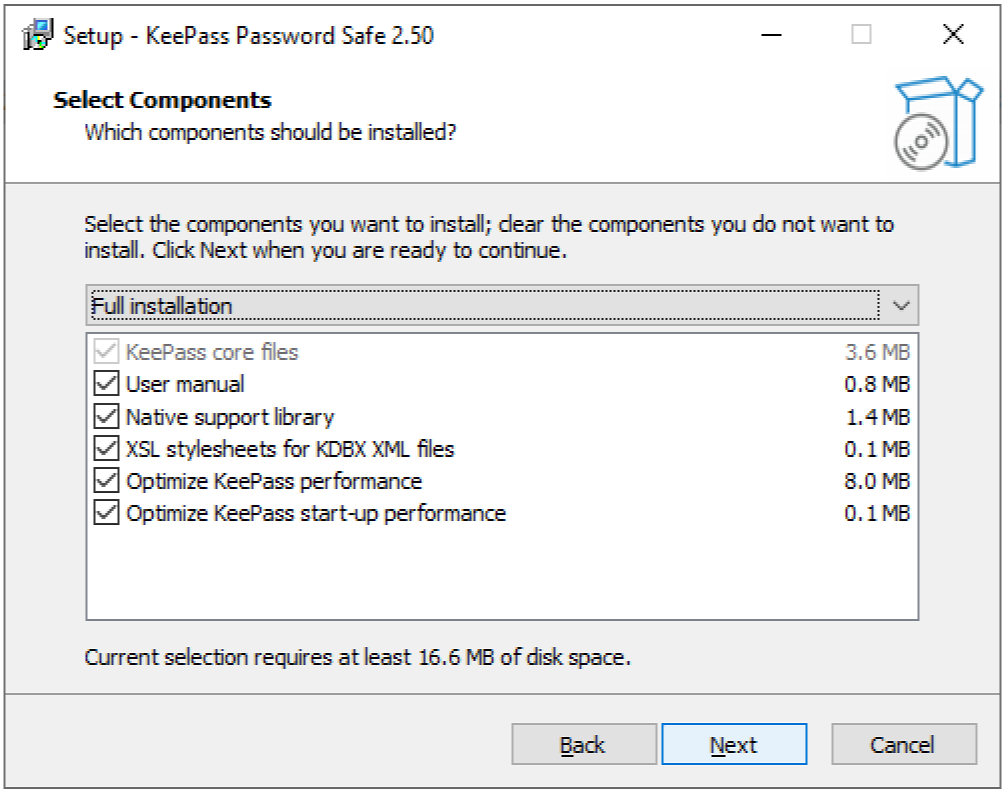
Setup will install KeePass Password Safe into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\KeePass Password Safe 2

At least 6.6 MB of free disk space is required.

d.



Setup - KeePass Password Safe 2.50

Select Components

Which components should be installed?

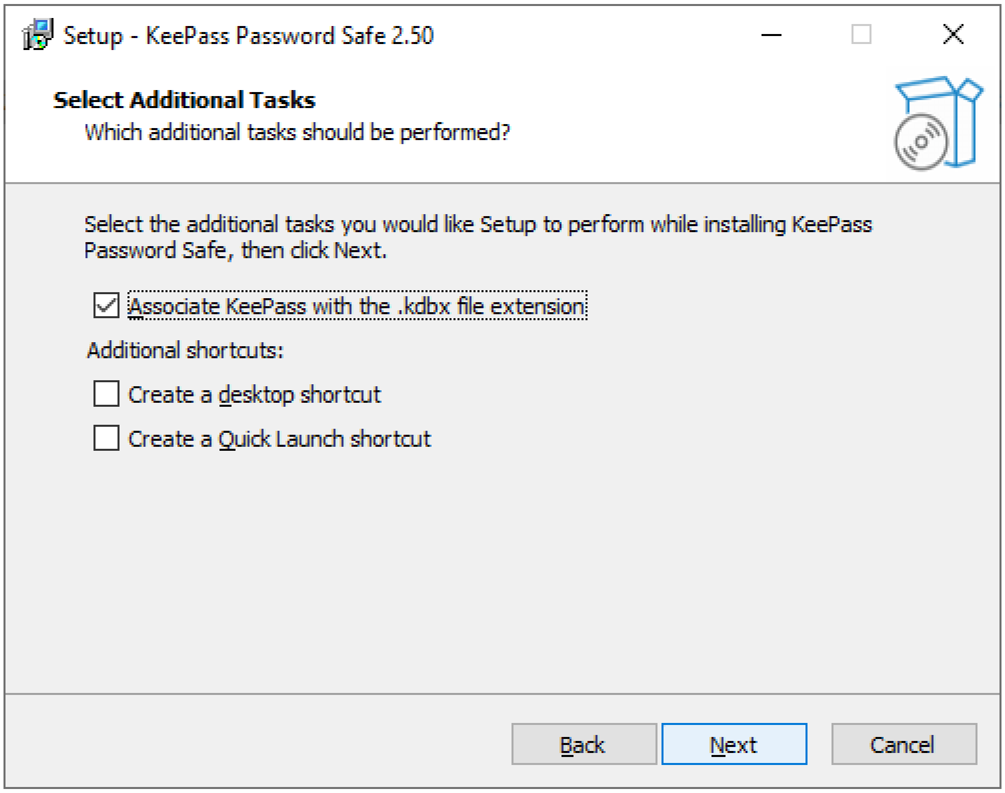
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

☑ KeePass core files	3.6 MB
☑ User manual	0.8 MB
☑ Native support library	1.4 MB
☑ XSL stylesheets for KDBX XML files	0.1 MB
☑ Optimize KeePass performance	8.0 MB
☑ Optimize KeePass start-up performance	0.1 MB

Current selection requires at least 16.6 MB of disk space.

e.



Setup - KeePass Password Safe 2.50

Select Additional Tasks

Which additional tasks should be performed?

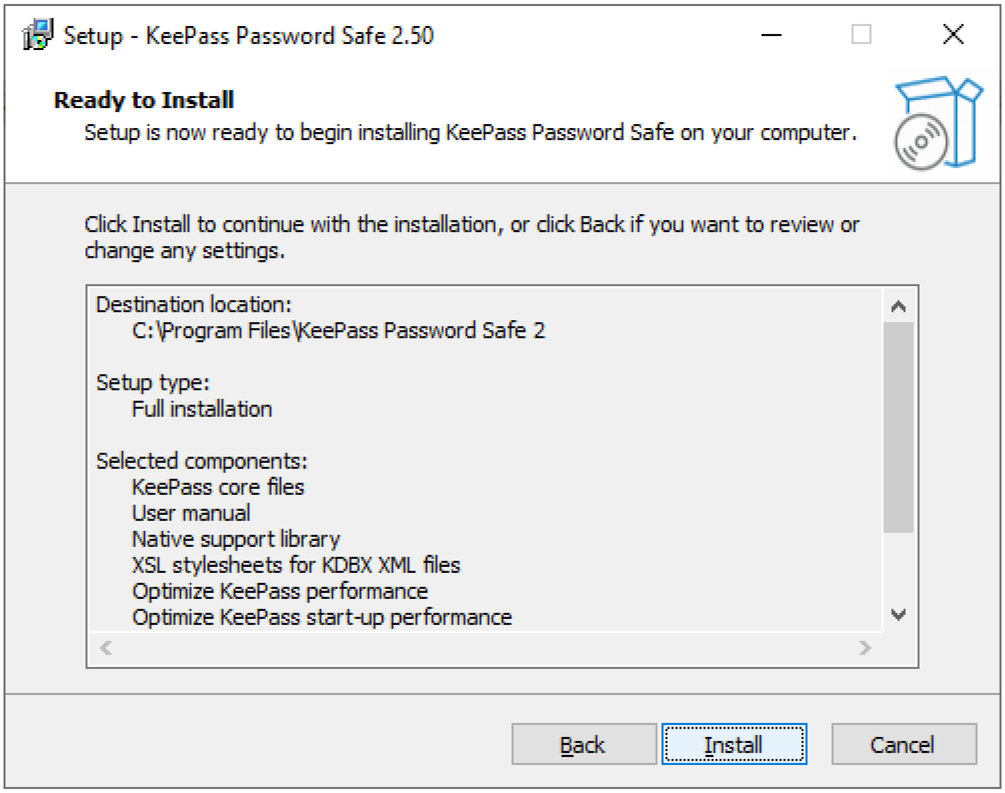
Select the additional tasks you would like Setup to perform while installing KeePass Password Safe, then click Next.

☑ Associate KeePass with the .kdbx file extension

Additional shortcuts:

☐ Create a desktop shortcut

☐ Create a Quick Launch shortcut

f. 

Ready to Install

Setup is now ready to begin installing KeePass Password Safe on your computer.

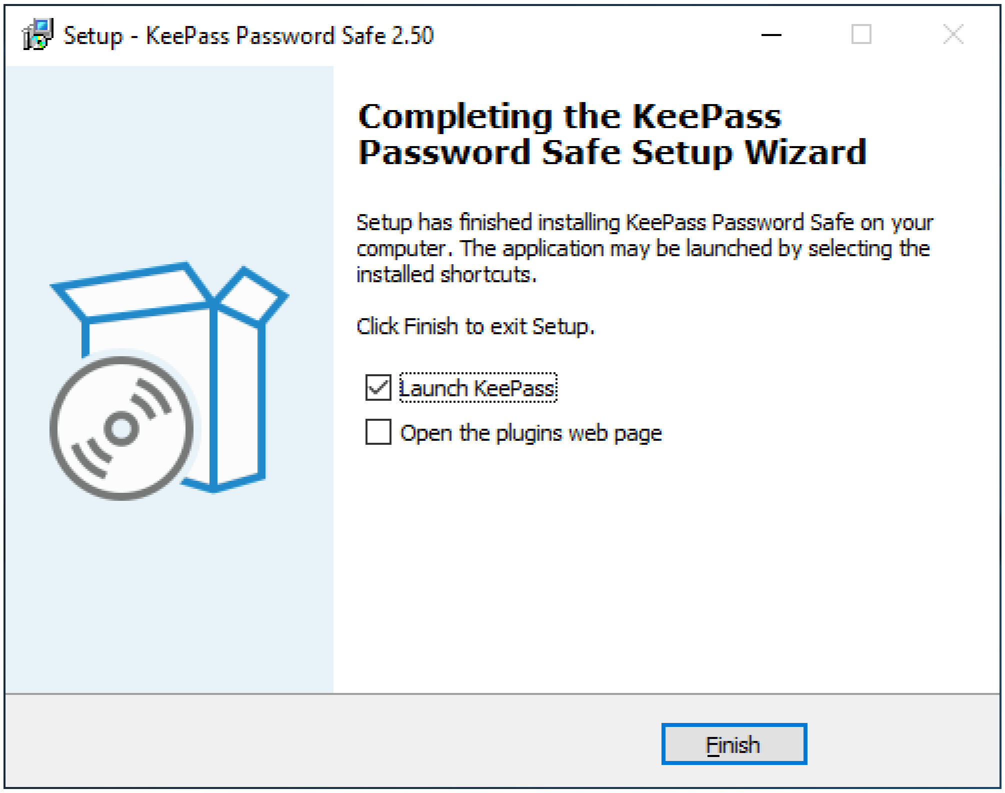
Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
      C:\Program Files\KeePass Password Safe 2

Setup type:
      Full installation

Selected components:
      KeePass core files
      User manual
      Native support library
      XSL stylesheets for KDBX XML files
      Optimize KeePass performance
      Optimize KeePass start-up performance
```

Configure KeePass

1. 

Setup - KeePass Password Safe 2.50

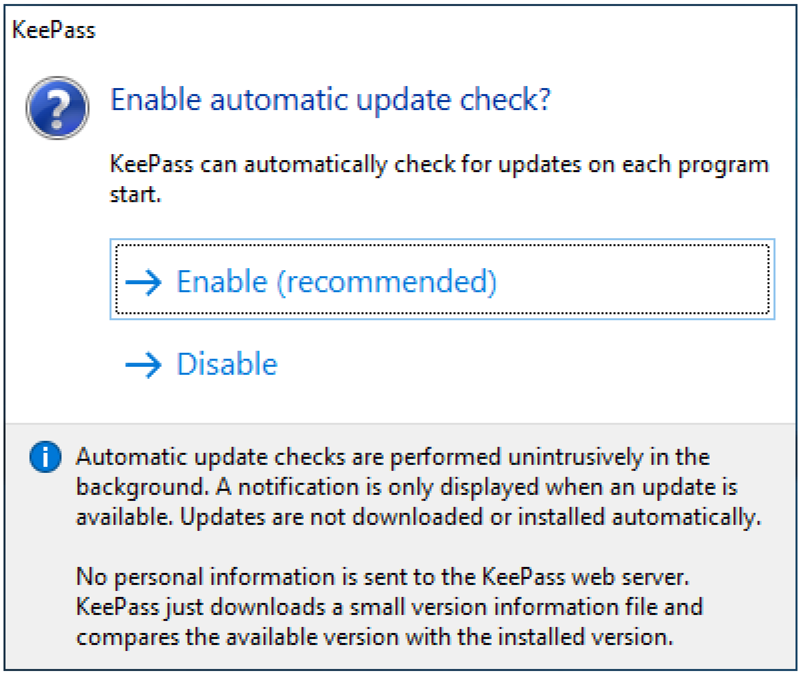
Completing the KeePass Password Safe Setup Wizard

Setup has finished installing KeePass Password Safe on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Launch KeePass

□ Open the plugins web page

a. 

KeePass

Enable automatic update check?

KeePass can automatically check for updates on each program start.

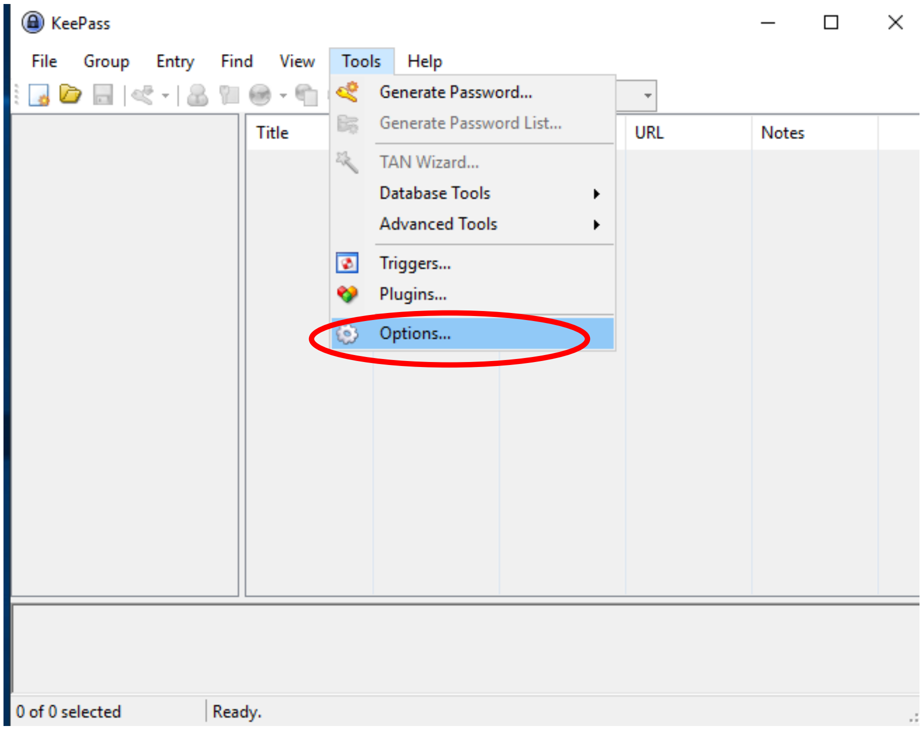
→ Enable (recommended)

→ Disable

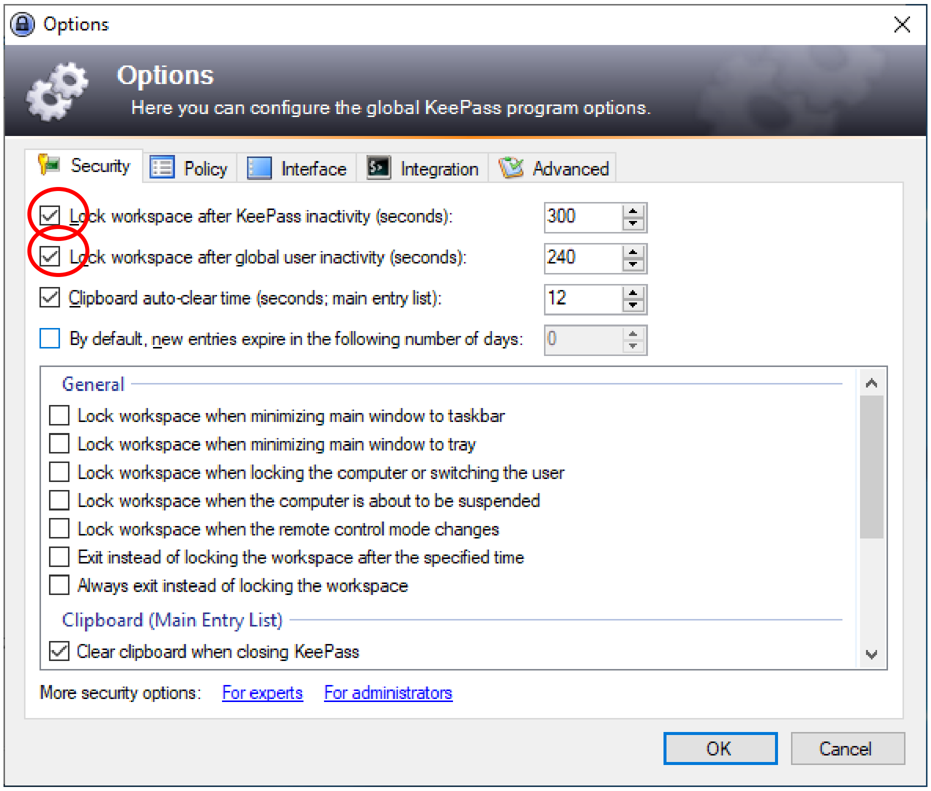
Automatic update checks are performed unintrusively in the background. A notification is only displayed when an update is available. Updates are not downloaded or installed automatically.

No personal information is sent to the KeePass web server. KeePass just downloads a small version information file and compares the available version with the installed version.

b. Before you get started, you are going to want to set some options



c. Two options which aren't enabled by default are the user inactivity timeout. Without enabling these, KeePass will remain open on a user's desktop indefinitely, basically defeating the whole purpose of the password manager process in the first place.



☑ Lock workspace after KeePass inactivity (seconds): 300

☑ Lock workspace after global user inactivity (seconds): 240

☑ Clipboard auto-clear time (seconds; main entry list): 12

☐ By default, new entries expire in the following number of days: 0

General

☐ Lock workspace when minimizing main window to taskbar

☐ Lock workspace when minimizing main window to tray

☐ Lock workspace when locking the computer or switching the user

☐ Lock workspace when the computer is about to be suspended

☐ Lock workspace when the remote control mode changes

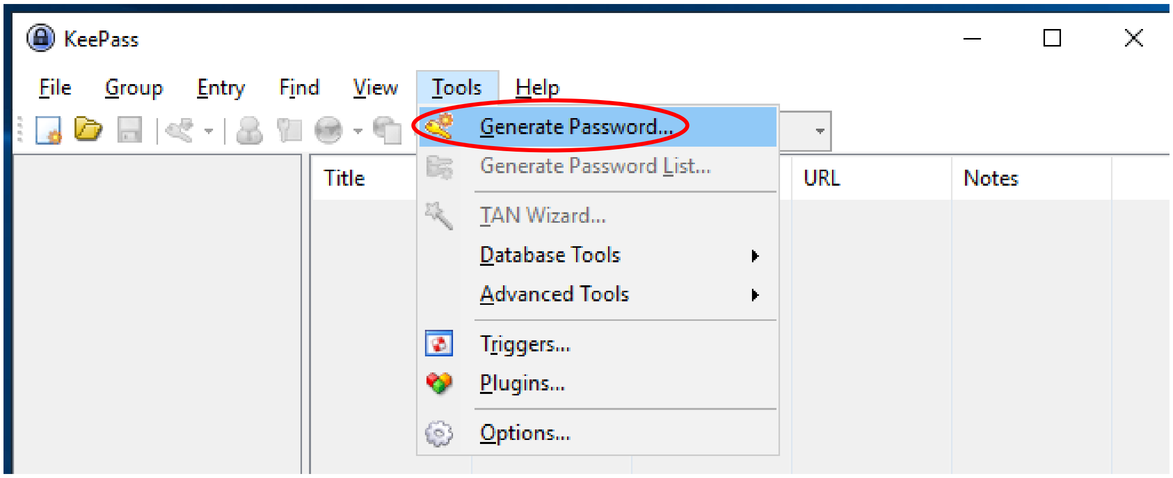
☐ Exit instead of locking the workspace after the specified time

☐ Always exit instead of locking the workspace

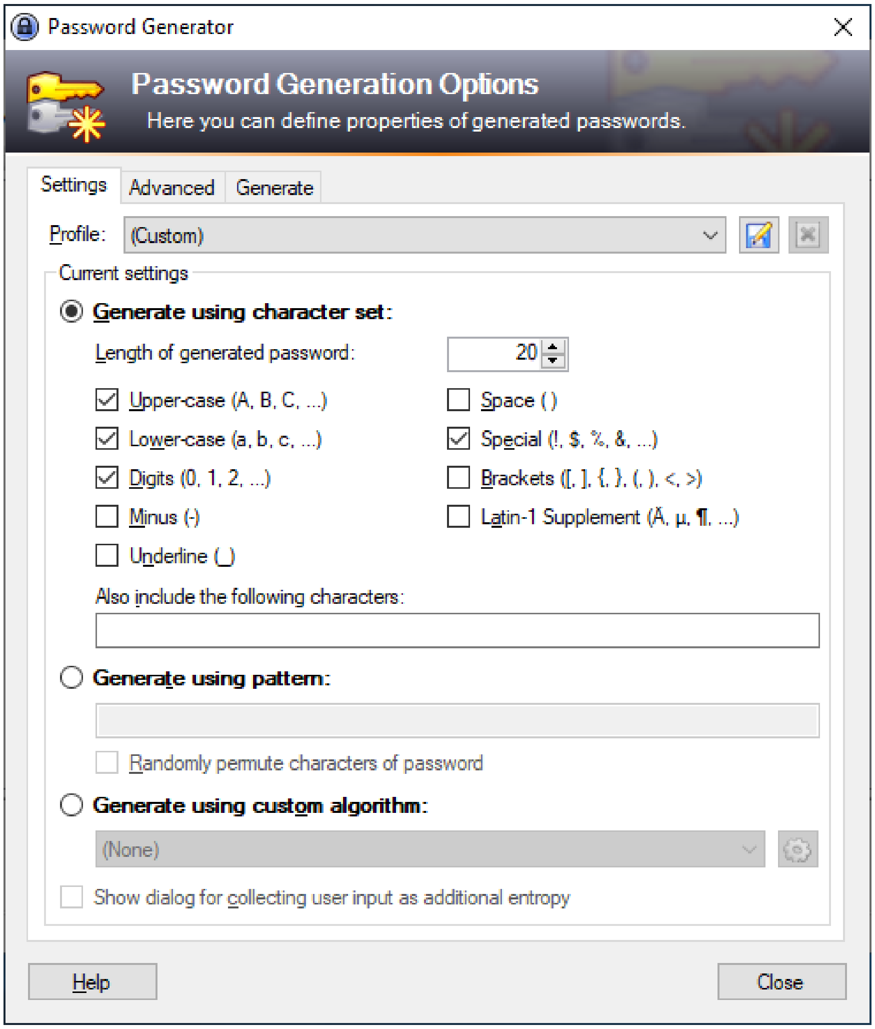
Clipboard (Main Entry List)

☑ Clear clipboard when closing KeePass

d. To set the password generation options, go to Generate Password



e. Set the options you require, we recommend a minimum 16 characters with mixed: upper, lower, numbers and special characters.


Password Generator

Password Generation Options

Here you can define properties of generated passwords.

Settings | Advanced | Generate

Profile: (Custom)

Current settings

● Generate using character set:

Length of generated password: 20

☑ Upper-case (A, B, C, ...)
☐ Space ( )
☑ Lower-case (a, b, c, ...)
☑ Special (!, $, %, &, ...)
☑ Digits (0, 1, 2, ...)
☐ Brackets ([,], {, }, (,), <, >)
☐ Minus (-)
☐ Latin-1 Supplement (Ä, µ, ¶, ...)
☐ Underline (_)

Also include the following characters:

○ Generate using pattern:

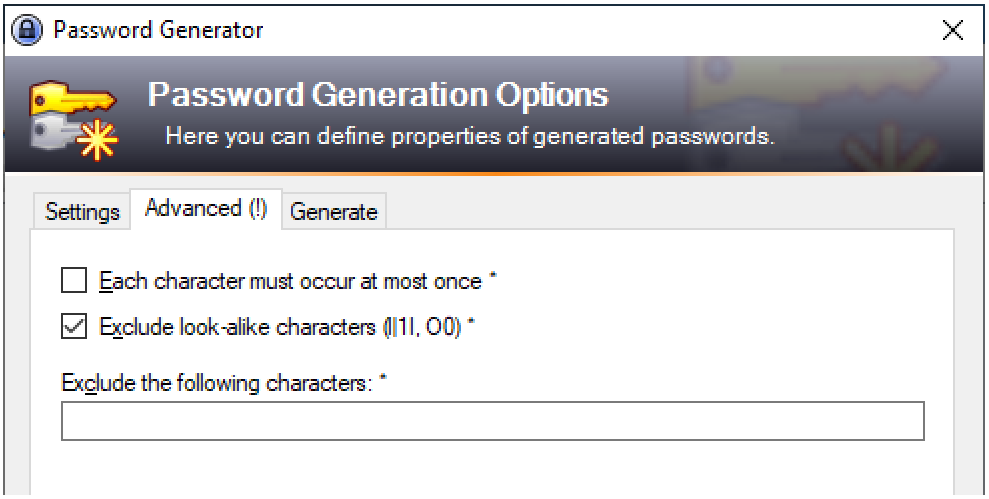
☐ Randomly permute characters of password

○ Generate using custom algorithm:

(None)

☐ Show dialog for collecting user input as additional entropy

f. You can prevent the use of look-alike characters; however this decreases the absolute strength of the password. In the event that a password needs to be entered by hand, however, being able to distinguish between the letter l and the number 1 and similar is absolutely necessary.



Password Generator

Password Generation Options

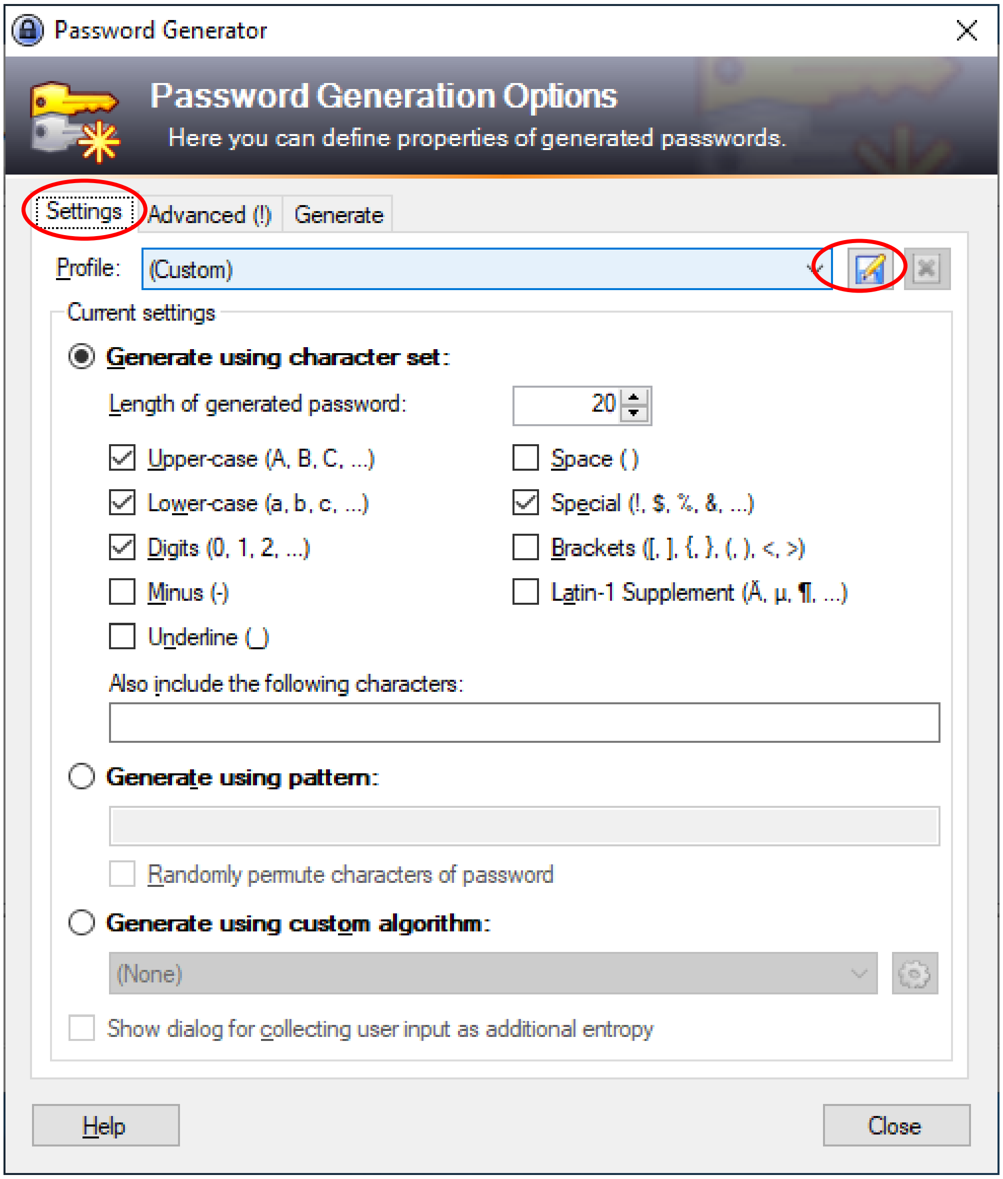
Here you can define properties of generated passwords.

☐ Each character must occur at most once *

☑ Exclude look-alike characters (l|1I, O0) *

Exclude the following characters: *

g. Once you have your default password policy configured, save that policy by going back to Settings and then click the disk icon



Password Generator

Password Generation Options

Here you can define properties of generated passwords.

Profile: (Custom)

Current settings

● **Generate using character set:**

Length of generated password: 20

☑ Upper-case (A, B, C, ...)
☐ Space ( )
☑ Lower-case (a, b, c, ...)
☑ Special (!, $, %, &, ...)
☑ Digits (0, 1, 2, ...)
☐ Brackets ([,], {, }, (,), <, >)
☐ Minus (-)
☐ Latin-1 Supplement (Ä, µ, ¶, ...)
☐ Underline (_)

Also include the following characters:

○ **Generate using pattern:**

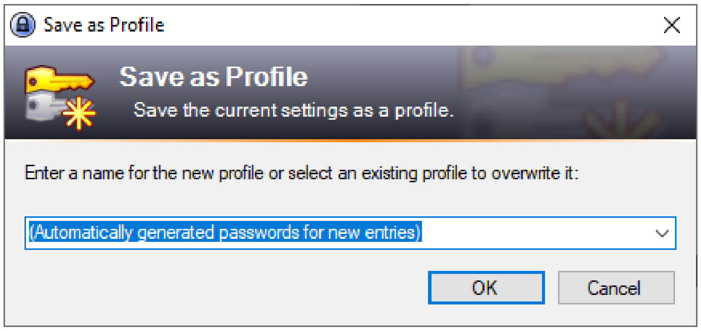
☐ Randomly permute characters of password

○ **Generate using custom algorithm:**

(None)

☐ Show dialog for collecting user input as additional entropy

h. If you would like this to be the default for automatically generated passwords, choose that in the dialog before saving



Save as Profile

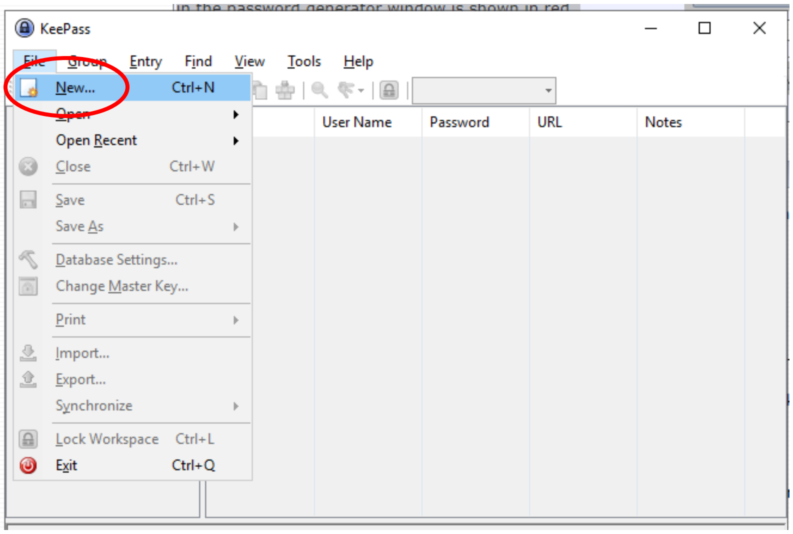
Save as Profile

Save the current settings as a profile.

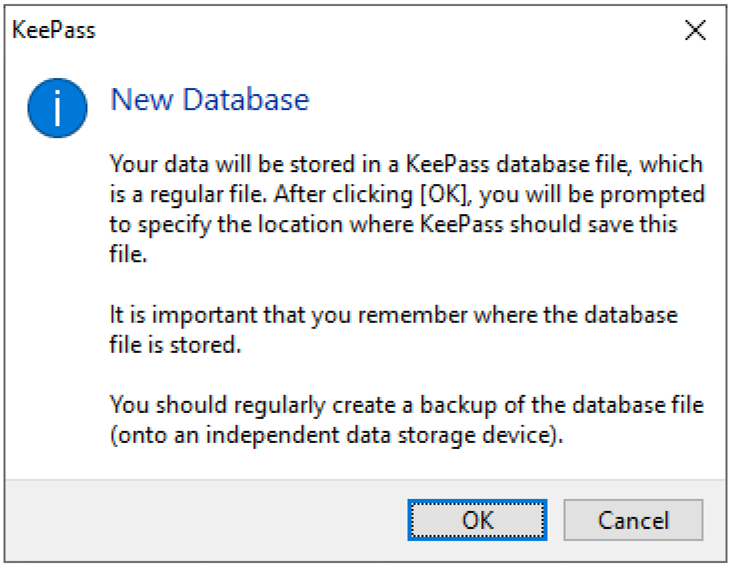
Enter a name for the new profile or select an existing profile to overwrite it:

(Automatically generated passwords for new entries)

Create your KeePass password vault



1.



KeePass

New Database

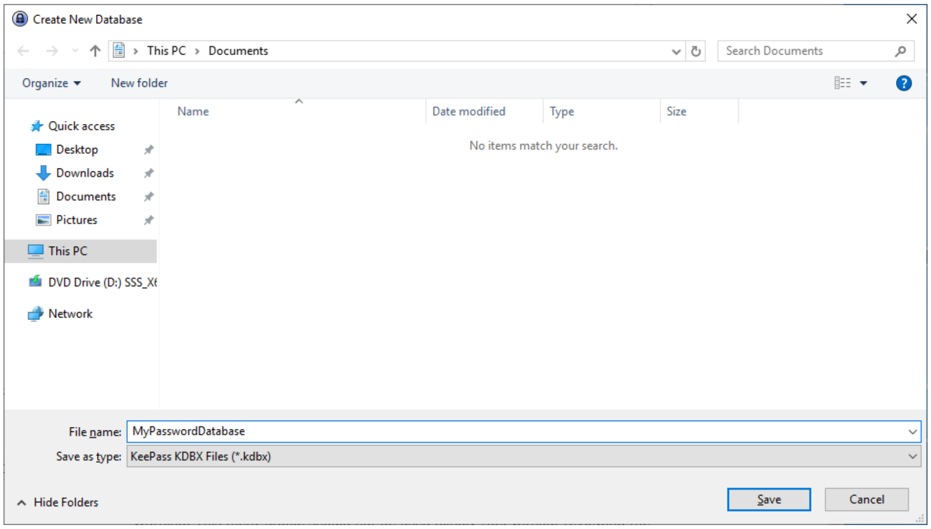
Your data will be stored in a KeePass database file, which is a regular file. After clicking [OK], you will be prompted to specify the location where KeePass should save this file.

It is important that you remember where the database file is stored.

You should regularly create a backup of the database file (onto an independent data storage device).

a.

b. Provide a file name for the *.kdbx database

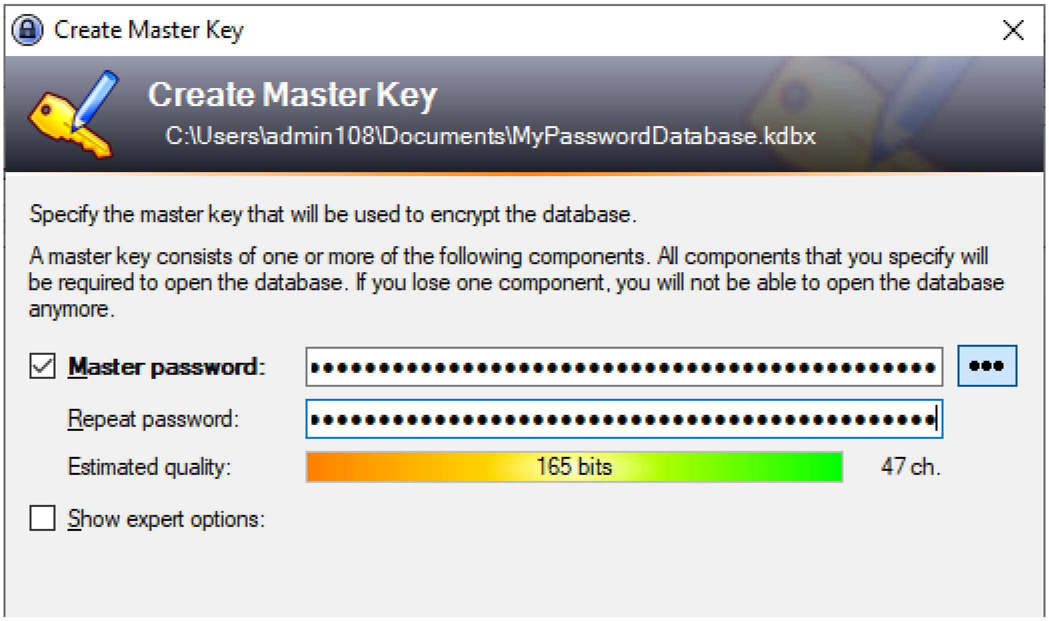


No items match your search.

File name: MyPasswordDatabase

Save as type: KeePass KDBX Files (*.kdbx)

c. Type in a master password or passphrase (that is used nowhere else). Make sure it is strong.



C:\Users\admin108\Documents\MyPasswordDatabase.kdbx

Specify the master key that will be used to encrypt the database.

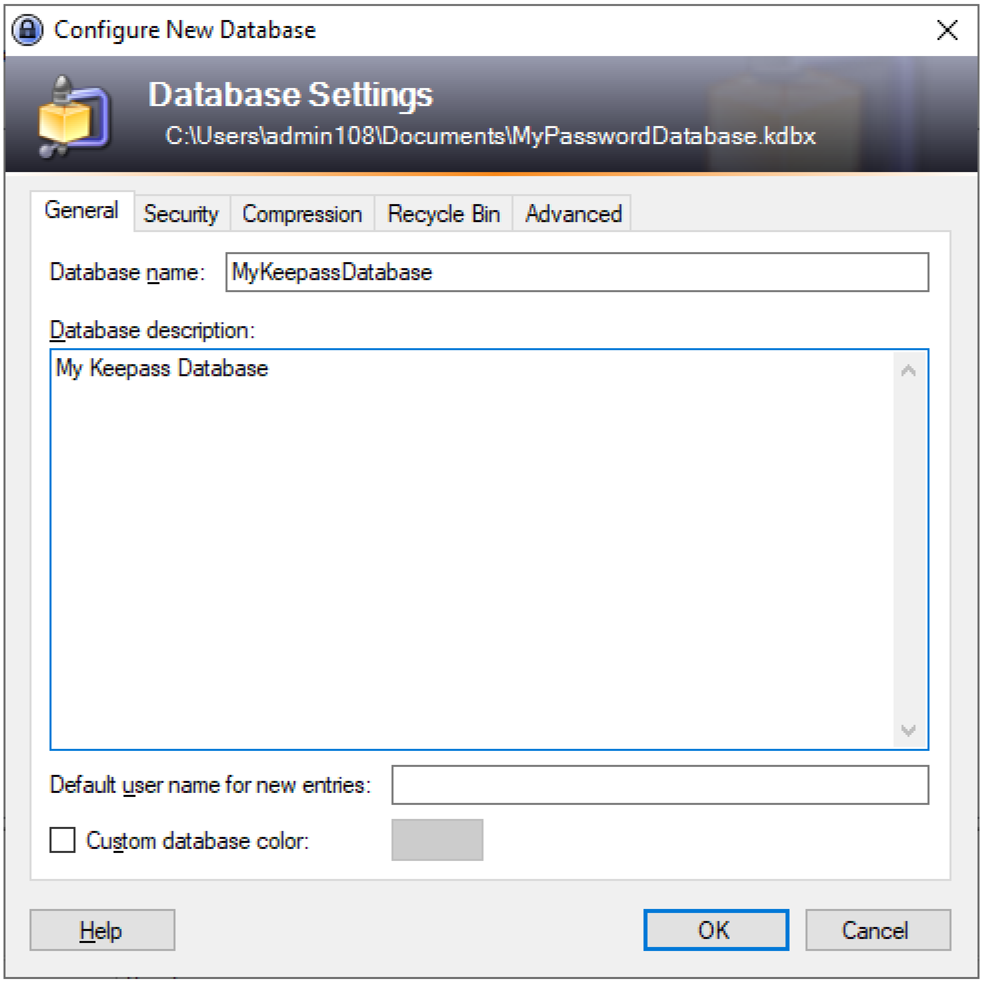
A master key consists of one or more of the following components. All components that you specify will be required to open the database. If you lose one component, you will not be able to open the database anymore.

☑ Master password: •••

Repeat password: •••

Estimated quality: 165 bits 47 ch.

□ Show expert options:



Database name: MyKeepassDatabase

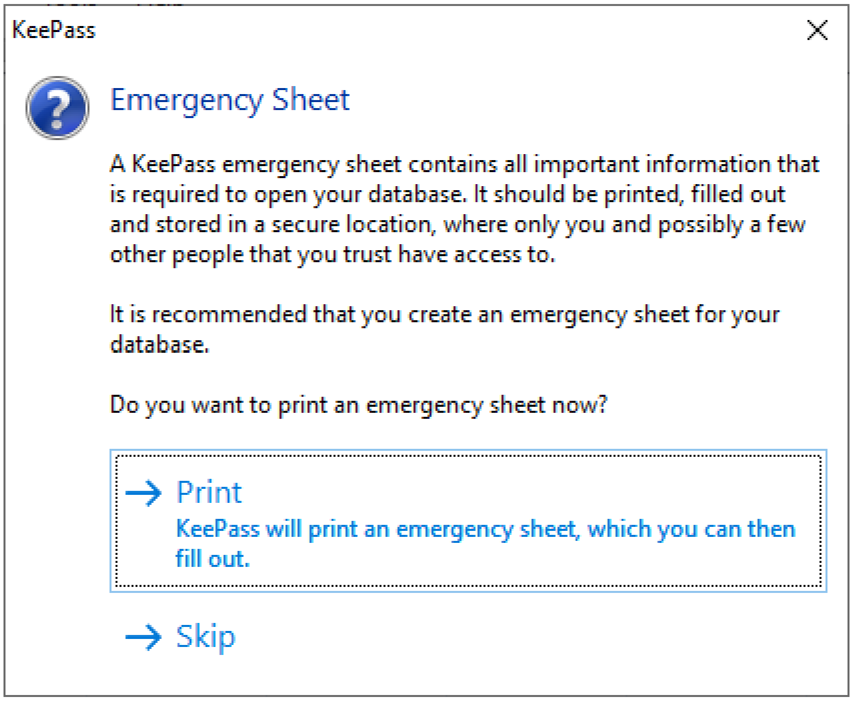
Database description:

My Keepass Database

Default user name for new entries:

☐ Custom database color:

d.



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.

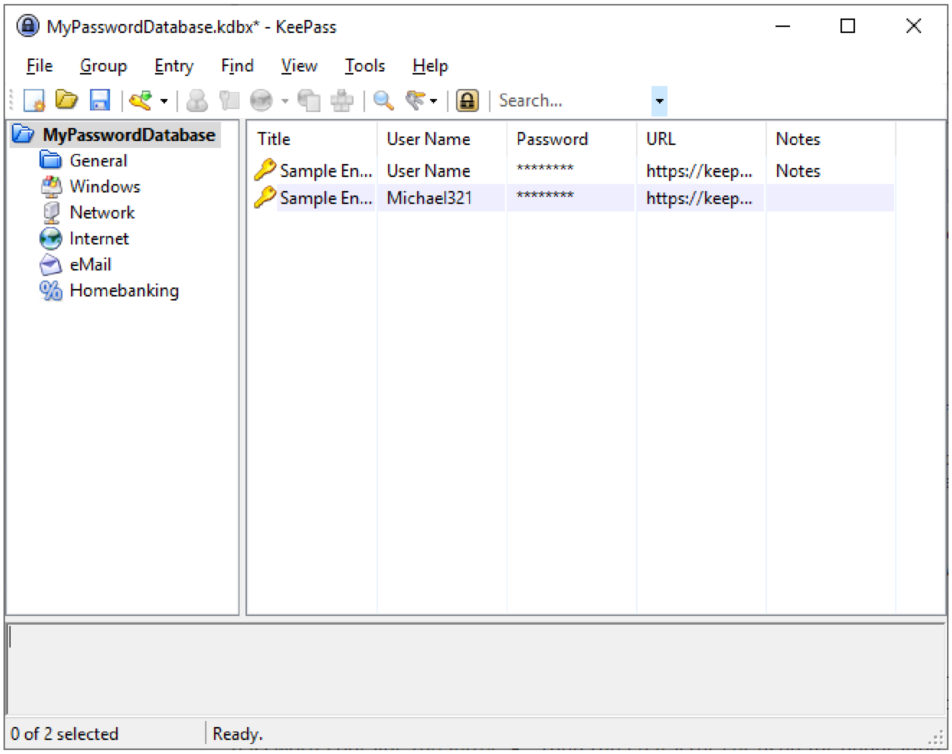
Do you want to print an emergency sheet now?

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

→ Skip

e.

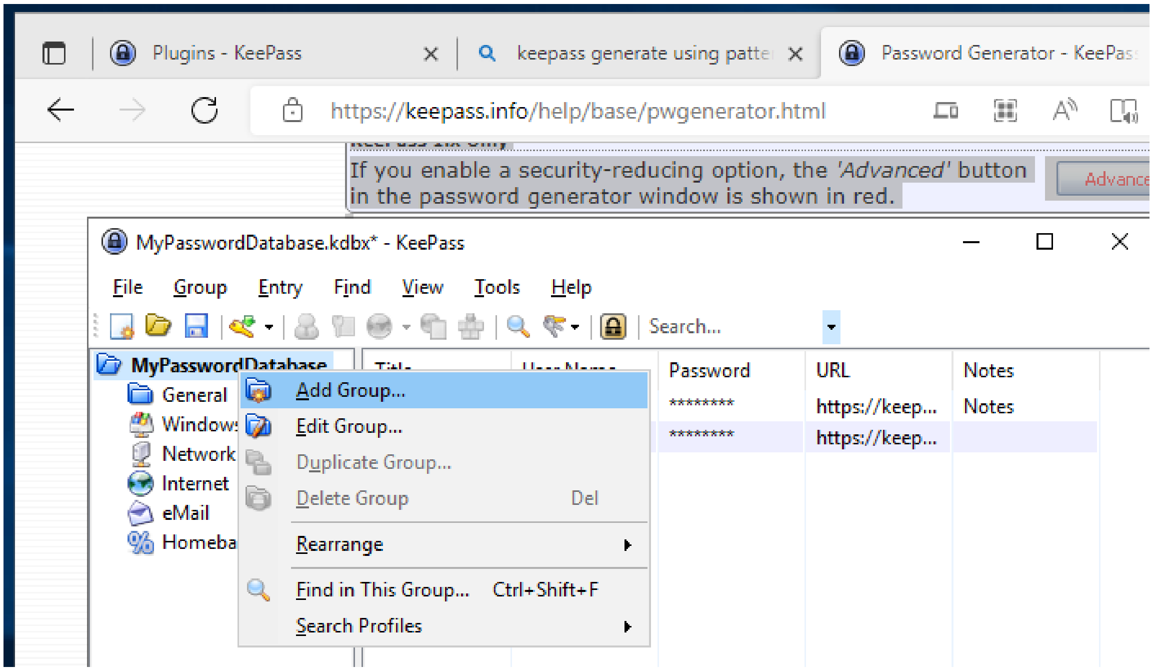
Create Groups and individual passwords in KeePass

1. 

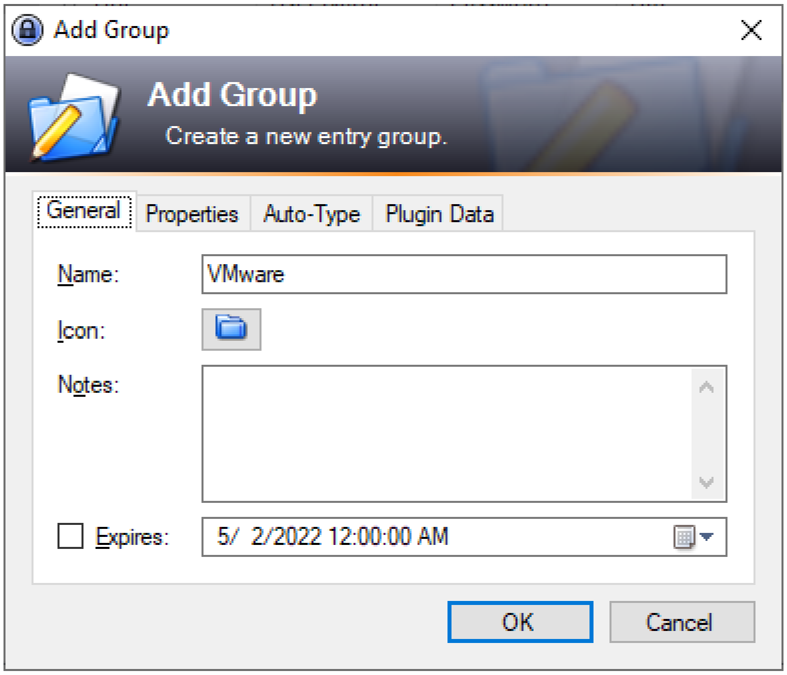
Title	User Name	Password	URL	Notes
Sample En...	User Name	********	https://keep...	Notes
Sample En...	Michael321	********	https://keep...	

0 of 2 selected Ready.

   a. Now create a new Group for entries



If you enable a security-reducing option, the *'Advanced'* button in the password generator window is shown in red.



Add Group

Create a new entry group.

General | Properties | Auto-Type | Plugin Data

Name: VMware

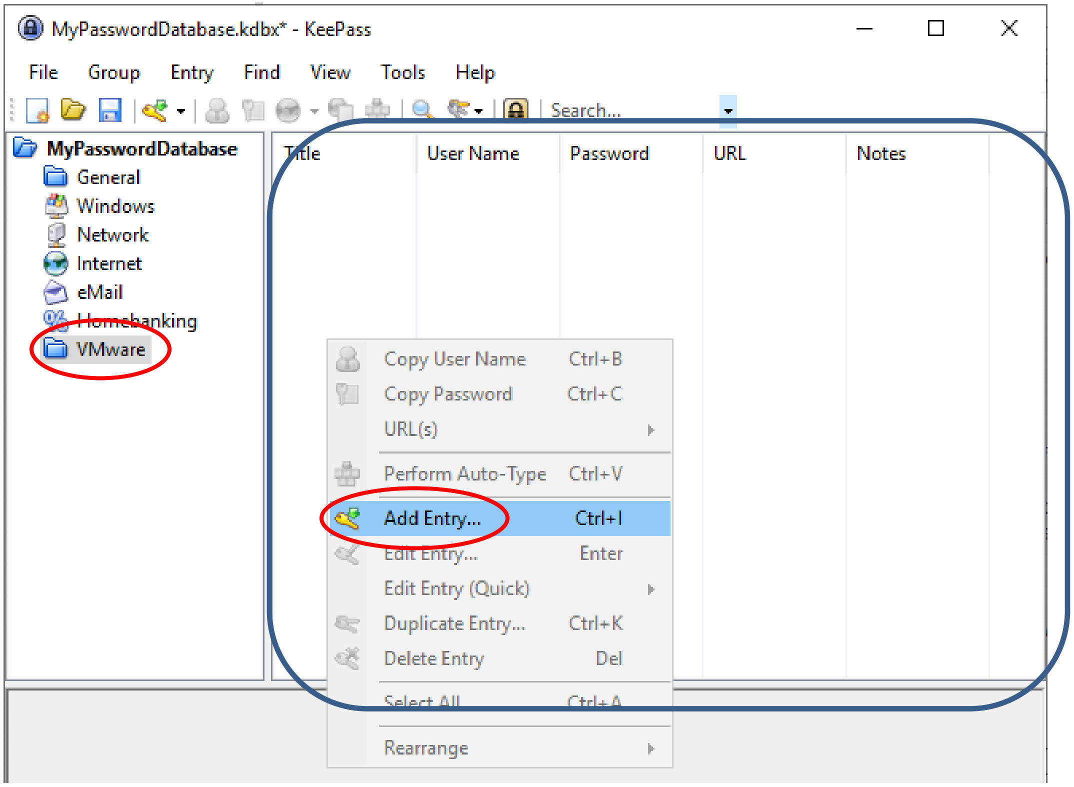
Icon:

Notes:

□ Expires: 5/ 2/2022 12:00:00 AM

b.

2. With the Group highlighted, right-click in the area on the right to start creating entries



MyPasswordDatabase.kdbx* - KeePass

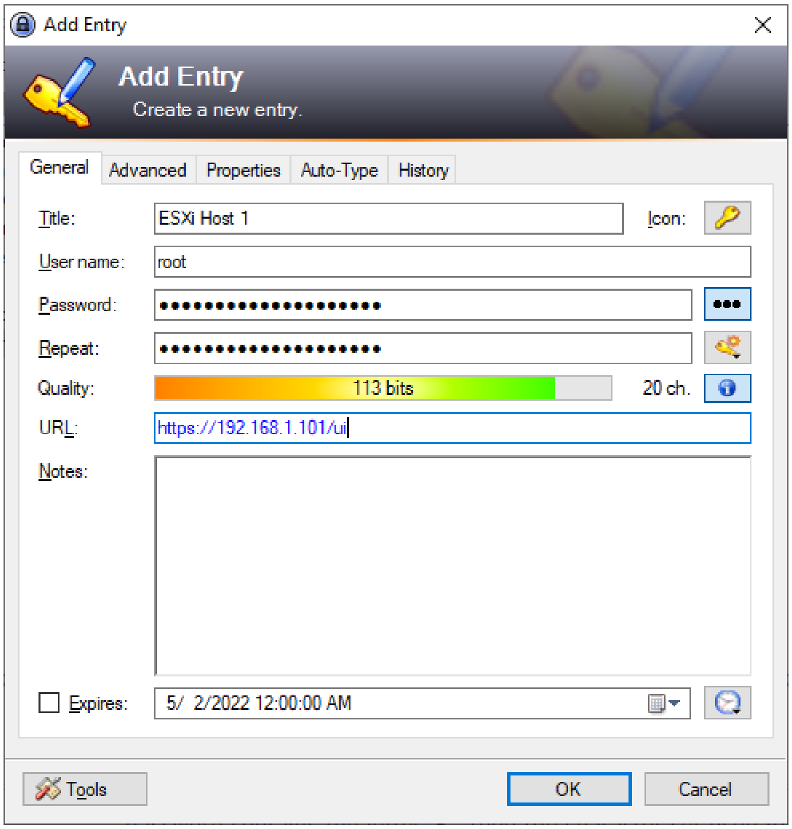
File Group Entry Find View Tools Help

Search...

MyPasswordDatabase
- General
- Windows
- Network
- Internet
- eMail
- Homebanking
- VMware

Title	User Name	Password	URL	Notes

a. The password is auto-generated following the rules you created earlier. You can specify: username, password, URL and other notes. All of the information is stored in the secure database.



Title: ESXi Host 1

User name: root

Password: ••••••••••••••••••••

Repeat: ••••••••••••••••••••

Quality: 113 bits 20 ch.

URL: https://192.168.1.101/ui

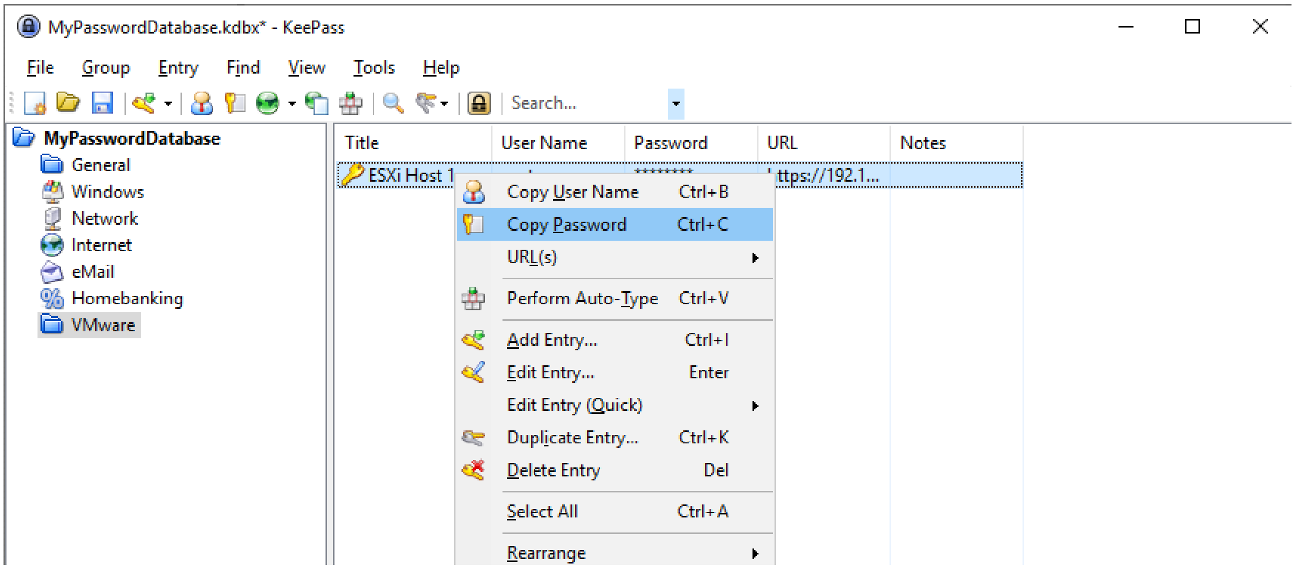
Notes:

□ Expires: 5/ 2/2022 12:00:00 AM

Using KeePass Passwords

One of the best things about KeePass is the ability to use/apply complex passwords without having to remember or even view the actual password. You simply right-click the entry and paste the password in the appropriate location.

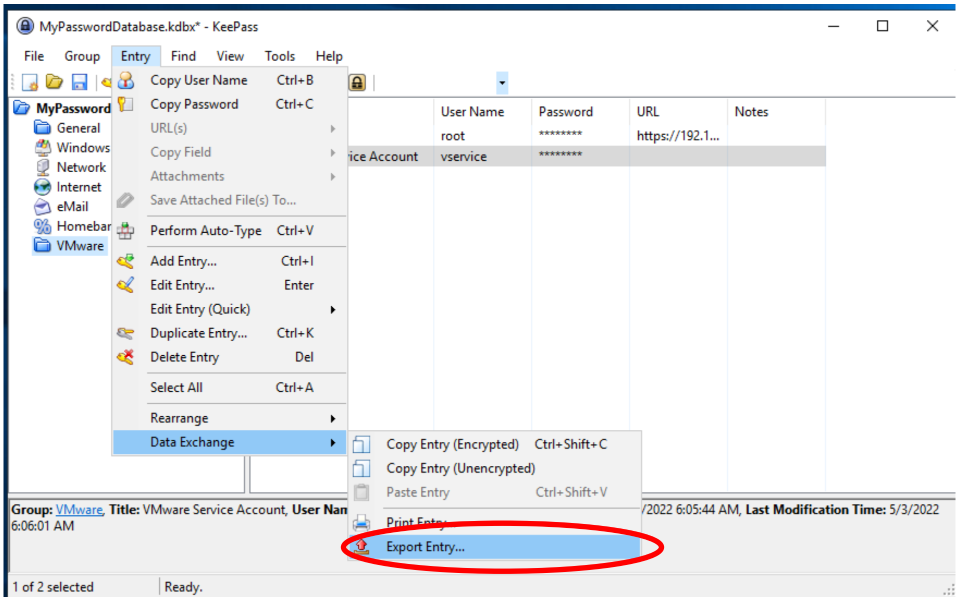
1. Right-click on the entry and copy user name or password



2. Paste the password into the application / platform / window of your choice

How to Export KeePass Passwords to transmit them securely

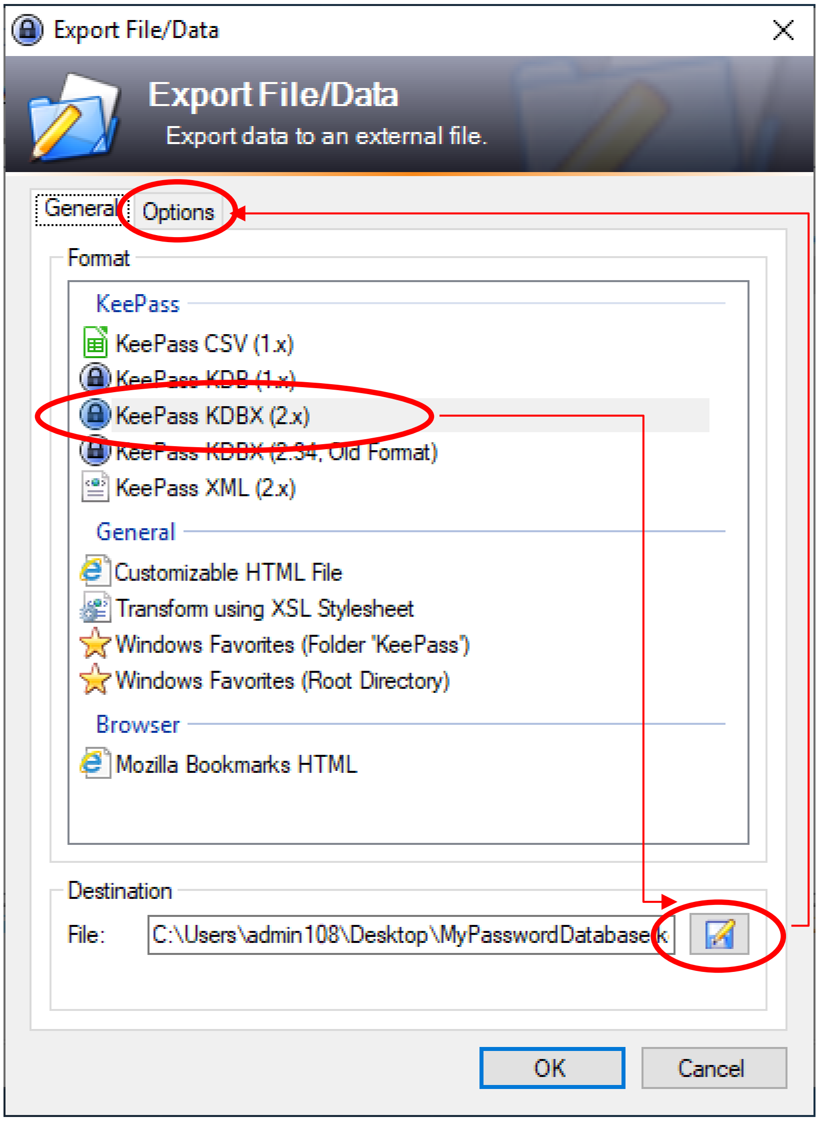
1. Choose the password or group of passwords which you want to send to someone like an MSP or remote employee and select Export Entry



	User Name	Password	URL	Notes
	root	********	https://192.1...	
ice Account	vservice	********		

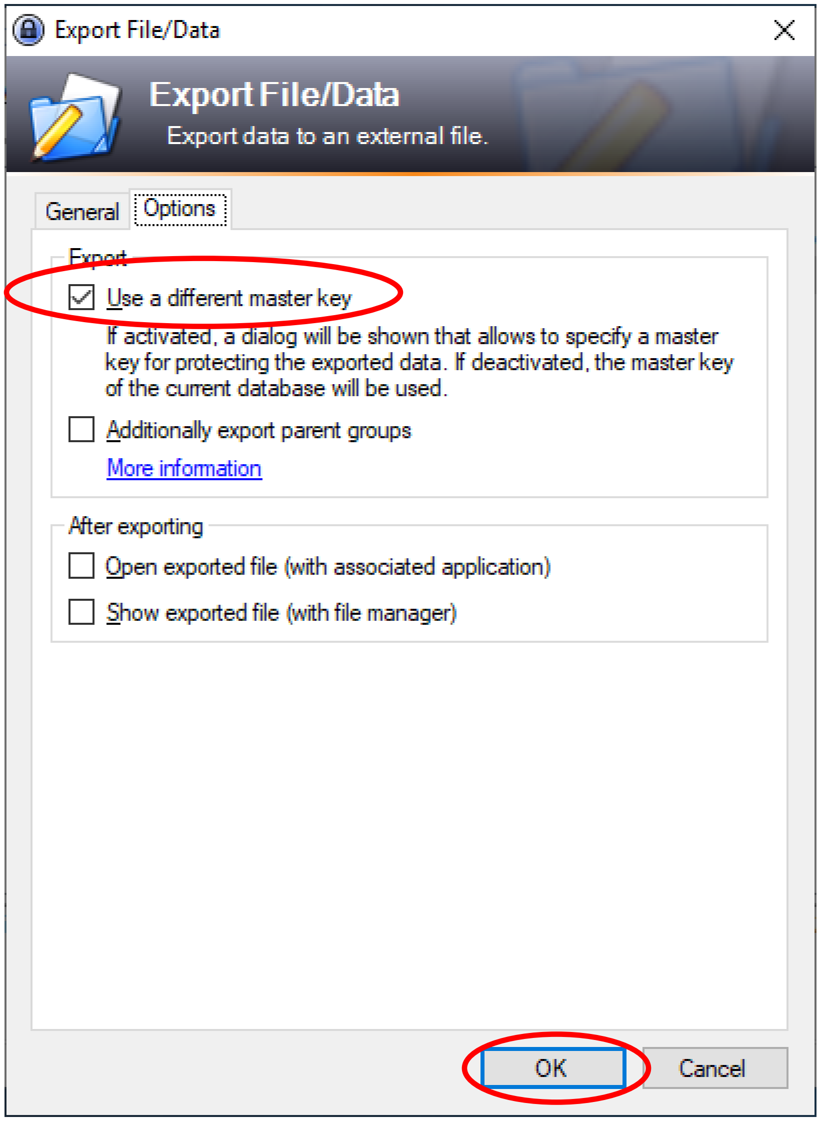
Group: VMware, **Title:** VMware Service Account, **User Nan** /2022 6:05:44 AM, **Last Modification Time:** 5/3/2022 6:06:01 AM

2. Select the most recent KDBX encrypted format, choose an export path, then choose Options



File: C:\Users\admin108\Desktop\MyPasswordDatabase.k

3. Now, under options, select: Use a different Master Key



Export File/Data

Export File/Data

Export data to an external file.

Export

☑ Use a different master key

If activated, a dialog will be shown that allows to specify a master key for protecting the exported data. If deactivated, the master key of the current database will be used.

□ Additionally export parent groups

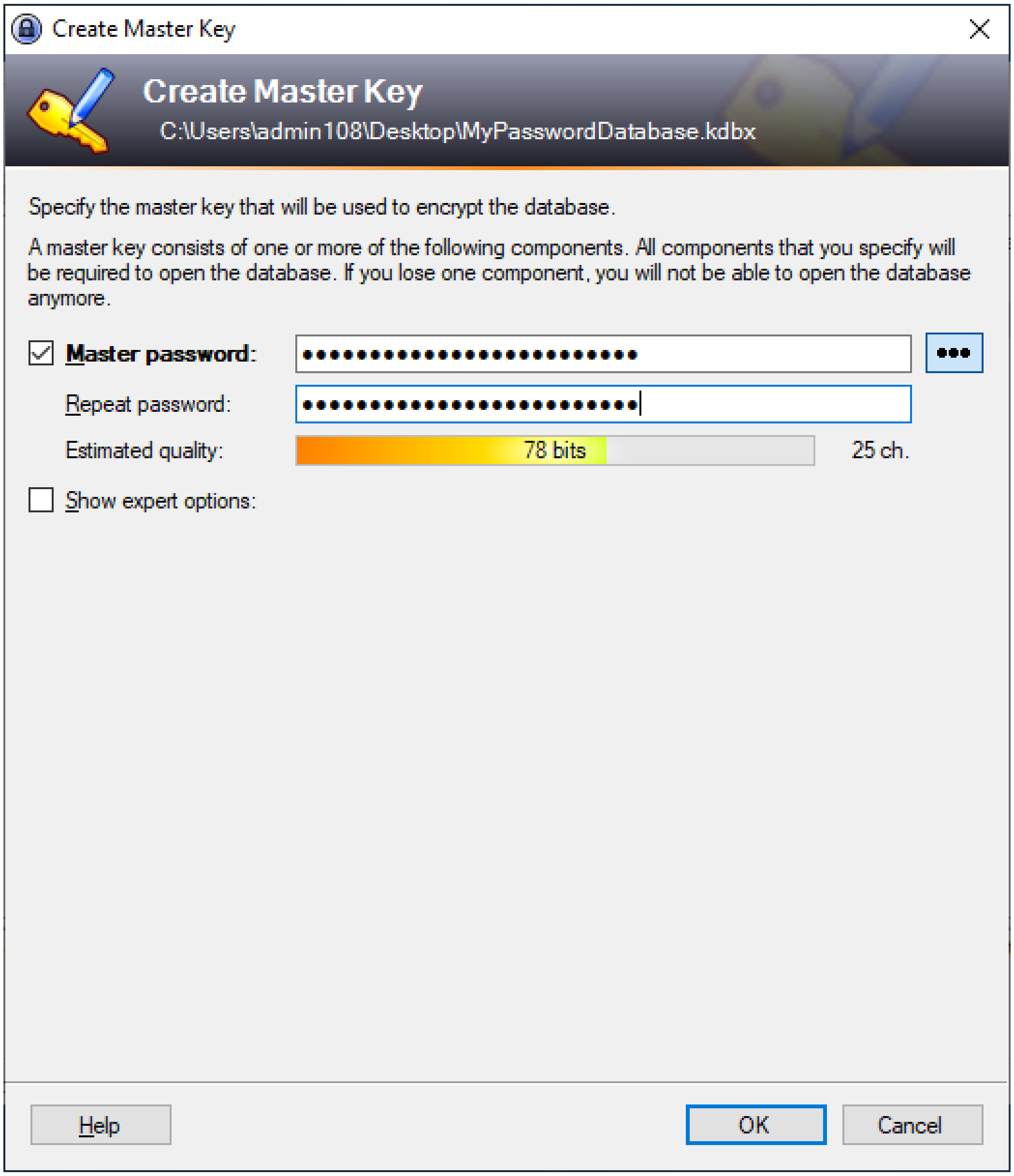
More information

After exporting

□ Open exported file (with associated application)

□ Show exported file (with file manager)

4. Specify a master key specifically for the MSP or remote user. We recommend a passphrase which is memorable and long enough to be secure



Create Master Key

C:\Users\admin108\Desktop\MyPasswordDatabase.kdbx

Specify the master key that will be used to encrypt the database.

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

☑ Master password: ••••••••••••••••••••••••

Repeat password: ••••••••••••••••••••••••

Estimated quality: 78 bits 25 ch.

□ Show expert options:

5. You can then safely email or transmit the KDBX to your remote user and communicate the Master password over the phone verbally (out-of-band)

Using patterns[iii]

KeePass can create passwords using patterns. A pattern is a string defining the layout of the new password. The following placeholders are supported:

Placeholder	Type	Character Set
a	Lower-Case Alphanumeric	abcdefghijklmnopqrstuvwxyz 0123456789
A	Mixed-Case Alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789
U	Upper-Case Alphanumeric	ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789
d	Digit	0123456789
h	Lower-Case Hex Character	0123456789 abcdef
H	Upper-Case Hex Character	0123456789 ABCDEF
l	Lower-Case Letter	abcdefghijklmnopqrstuvwxyz
L	Mixed-Case Letter	ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz
u	Upper-Case Letter	ABCDEFGHIJKLMNOPQRSTUVWXYZ
v	Lower-Case Vowel	aeiou
V	Mixed-Case Vowel	AEIOU aeiou
Z	Upper-Case Vowel	AEIOU
c	Lower-Case Consonant	bcdfghjklmnpqrstvwxyz
C	Mixed-Case Consonant	BCDFGHJKLMNPQRSTVWXYZ bcdfghjklmnpqrstvwxyz
z	Upper-Case Consonant	BCDFGHJKLMNPQRSTVWXYZ
p	Punctuation	,.;:
b	Bracket	()[]{}<>
s	Printable 7-Bit Special Character	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
S	Printable 7-Bit ASCII	A-Z, a-z, 0-9, !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

x	Latin-1 Supplement	Range [U+00A1, U+00FF] except U+00AD: ¡¢£¤¥¦§¨©ª«¬®¯ °±²³´µ¶·¸¹º»¼½¾¿ ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏ ÐÑÒÓÔÕÖ×ØÙÚÛÜÝÞß àáâãäåæçèéêëìíîï ðñòóôõö÷øùúûüýþÿ
\	Escape (Fixed Char)	Use following character as is.
{*n*}	Escape (Repeat)	Repeat the previous placeholder *n* times.
[...]	Custom Char Set	Define a custom character set.

The \ placeholder is special: it's an escape character. The next character that follows the \ is written directly into the generated password. If you want a \ in your password at a specific place, you have to write \\\\.

Using the **{*n*}** code you can define how many times the previous placeholder should occur. The **{ }** operator duplicates placeholders, not generated characters. Examples:
» d{4} is equivalent to dddd,
» dH{4}a is equivalent to dHHHHa and
» Hda{1}dH is equivalent to HdadH.

The **[...]** notation can be used to define a custom character set, from which the password generator will pick one character randomly. All characters between the '**[**' and '**]**' brackets follow the same rules as the placeholders above. The '**^**' character removes the next placeholders from the character set. Examples:
» [dp] generates exactly 1 random character out of the set digits + punctuation,
» [d\m\@^\3]{5} generates 5 characters out of the set "012456789m@",
» [u_][u_] generates 2 characters out of the set upper-case + '_'.

More examples:

ddddd
Generates for example: 41922, 12733, 43960, 07660, 12390, 74680, ...

\H\e\x\:\ HHHHHH
Generates for example: 'Hex: 13567A', 'Hex: A6B99D', 'Hex: 02243C', ...

Common password patterns:

Name	**Pattern**
Hex Key - 40-Bit	H{10}
Hex Key - 128-Bit	H{32}
Hex Key - 256-Bit	H{64}
MAC Address	HH\\-HH\\-HH\\-HH\\-HH\\-HH

[i] KeePass Review 2022 – Forbes Advisor

[ii] Enforced Configuration - KeePass

[iii] Password Generator - KeePass