

User Guide

Disclaimer and Restrictions

The material in this publication is for information only and is subject to change without notice. This material does not constitute a commitment on the part of the development team. Every effort has been made to ensure the accuracy of this manual. However, the information in this document is subject to change without notice. We give no warranty with respect to this documentation and disclaim any implied warranties of merchantability and fitness for a particular purpose. We shall not be liable for any errors or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein.

Contact Us

We are committed to continually improve KeePassXC through customer experience and your feedback is important to us.

Please send us your feedback or comments to team@keepassxc.org.

To report issues, visit: https://github.com/keepassxreboot/keepassxc.

Thank You, Team KeePassXC

Table of Contents

Chapter 1: Introduction	5
Chapter 2: Installing KeePassXC	6
2.1 Downloading KeePassXC	6
2.1.1 Microsoft Windows	7
2.1.2 Linux	8
2.1.3 macOS	9
2.2 Installing KeePassXC	
2.3 Creating Your First Database	
2.4 Opening Existing Database	
Chapter 3: Entry Management	20
3.1 Adding an Entry	
3.1.1 Advanced Entry Settings	
3.1.2 Assigning Icons to Entries	
3.1.3 Configuring Auto-Type Feature	
3.2 Viewing Properties	
3.3 Managing History	
3.4 Editing an Entry	
3.5 Cloning an Entry	
3.6 Deleting an Entry	
Chapter 4: Database Management	
4.1 Importing External Databases	
4.1.1 Importing KeePass 1 Database	
4.1.2 Importing CSV File	
4.2 Advanced Database Settings	
4.2.1 General Settings	
4.2.2 Security Settings	
4.3 Storing Database File	50
4.4 Backing up Database File	51
4.5 Sharing Database File	51
Chapter 5: KeePassXC-Browser Extension	52
5.1 KeePass-Browser Extension	
5.1.1 Downloading KeePassXC-Browser Extension	

Table of Contents

5.1.2 Configuring KeePassXC-Browser	54
5.2 Populating Database Entries to Websites	56
Chapter 6: Search Operations	58
6.1 Modifiers	58
6.2 Wild Card Characters and Logical Operators	58
6.3 Sample Search Queries	59
Chapter 7: Password Generator	60
7.1 Generating Passwords	60
7.2 Generating Passphrases	61

Chapter 1: Introduction

KeePassXC is a modern open-source password manager. It is used to store and manage information such as URLs, usernames, passwords, and so on for various accounts on your web applications. KeePassXC stores the passwords in an encrypted format and provides secure access to all the your information with the help of a master password.

KeePassXC is helpful for people with extremely high demands of secure personal data management. It saves many different information, such as user names, passwords, URLs, attachments, and comments in one single database. For a better management, user-defined titles and icons can be specified for different entries in KeePassXC. In addition, the entries are sorted in customizable groups. The integrated search function allows to search in a single group or the complete database.

KeePassXC also provides a secure, customizable, fast, and easy-to-use password generator utility. This utility is very helpful to those who generate passwords frequently.

Chapter 2: Installing KeePassXC

This chapter covers the following topics:

- Downloading KeePassXC
- Installing KeePassXC
- Creating Your First Database
- Opening Existing Database

2.1 Downloading KeePassXC

KeePassXC is available for download for the following operating systems and platforms:

- Linux Official Cross-Distribution Packages
 - Applmage
 - Snap Package
- Linux Distribution-Specific Packages
 - Ubuntu
 - Debian
 - Arch Linux
 - Gentoo
 - Fedora
 - CentOS
 - OpenSUSE
- macOC
 - DMG Installer
 - Homebrew Cask
- Microsoft Windows
 - 64-bit Portable and MSI Installer
 - 32-bit Portable and MSI Installer

To download the KeePassXC installer for the desired platform, visit https://keepassxc.org/ download. **NOTE:** KeePassXC is open-source software and may be available on other websites that are unaffiliated with Team KeePassXC. We recommend obtaining this software from https://keepassxc.org only if you are in doubt.

Before installing KeePassXC, it is recommended that you verify that your downloaded installer matches the signature, which is published alongside the release package. By verifying the signatures of KeePassXC releases, you can verify the authenticity and integrity of the downloaded installation file. This guarantees that the file you downloaded was originally created by the KeePassXC Team and its contents have not been tampered with.

To know more about the steps to verify the authenticity and integrity of your downloaded package, visit https://keepassxc.org/verifying-signatures.

2.1.1 Microsoft Windows

The Windows MSI installer is signed by a secure certificate owned by DroidMonkey Apps, LLC. If you do not see this dialog when installing the application, click **DENY** and download the installed again from https://keepassxc.org.

^{User Account Control} Do you want to allow this app to make changes to your device?	×
KeePassXC Verified publisher: DroidMonkey Apps, LLC File origin: Hard drive on this computer Show more details Yes No	

2.1.2 Linux

You can easily download the KeePassXC installer for Linux. When you search for KeePassXC, multiple options are displayed as shown in the following screen:



The Snap and Flatpak options are *Sandboxed* applications (more secure). The Native option is installed with the operating system files.

2.1.3 macOS

With the Mac App Store built into macOS, getting the KeePassXC app is easy. To download the KeePassXC app on macOS, use the click and drag option as shown in the following screen:



2.2 Installing KeePassXC

Installing KeePassXC is a simple process and you can install KeePassXC on different operating systems by using the native installers.

Installation steps on different operating systems are similar except the initial few steps.

To install KeePassXC, perform the following steps:

 Start installing your KeePassXC application by using the installer your downloaded for your operating system. In case of Microsoft Windows, double-click on the KeePassXC-Y.Y-WinZZ.msi file. Here, Y.Y.Y represents the version of the software and ZZ represents the 32-bit/64-bit version of the Microsoft Windows operating system.



2. Click **Next** and follow the simple instructions on the **KeepPassXC Setup Wizard** to complete the installation.

2.3 Creating Your First Database

To start using KeePassXC, you need to first create a database that will store the password and other details.

To create a database, perform the following steps:

1. Open your KeePassXC application. The following screen appears:

€ KeePassXC	—	\times
<u>D</u> atabase E <u>n</u> tries <u>G</u> roups <u>T</u> ools <u>H</u> elp		
🕐 🎴 🔚 🖑 ể 🦓 🕼 🗓 🥙 🏰 🎯 🔒 🥕 🕋 Search (Ctrl+F)		0
Welcome to KeePassXC 2.4.0-beta1		
Create new database		
Open existing database		
Import from KeePass 1 Import from CSV		
Recent databases		

2. Click the **Create new database** button. The General Database Information screen appears.

I Create a new KeePassXC database	?	×
General Database Information		
Please fill in the display name and an optional description for your new database:		
Database Name: Passwords		
Description:		
Go Back Continue	Cancel	

- 3. Enter a name for your database in the **Database Name** field. If you do not enter a name in this field on this screen, you will be prompted to provide a name when you finish creating the database.
- 4. (Optional) Enter desired details in the **Description** field.
- 5. Click **Continue**. The Encryption Settings screen appears.

👀 Create a new KeePassXC database		? ×
	Encryption Settings	
	Here you can adjust the database encryption settings. Don't worry, you can change them later in the database settings.	
	Decryption Time: 1.0 s	
		1
		5 s
	Higher values offer more protection, but opening the database will take longer. Database format: KDBX 4.0 (recommended)	
	This is only important if you need to use your database with other programs. Advanced S	
	Go Back Continue	Cancel

- 6. Drag the **Decryption Time** slider based on your encryption strength of your database. Setting the **Decryption Time** slider at a higher values means that the database will have higher level of protection but the time taken by the database to open will increase.
- 7. Select the **Database format** from the following options available in the drop-down list.
 - KDBX 4.0 (recommended)
 - KDBX 3.1
- 8. Optional. Click the **Advanced Settings** to provide additional encryption settings for your database. The following screen appears:

Create a new KeePassXC database						?	×
	Encryption Settings						
	Here you can adjust the da	tabase encryption settings. Don't wo	rry, you	ı can change them later in the d	latabase settings.		
	Encryption Algorithm:	AES: 256-bit				\sim	
	Key Derivation Function:	Argon2 (KDBX 4 – recommended)				\sim	
	Transform rounds:	1	•	Benchmark 1-second delay			
	Memory Usage:	128 MiB	•				
	Parallelism:	4 thread(s)	▲ ▼				
					Simple Se	ettings	
				Go Back Co	ntinue	Cancel	

- a. Select the level of encryption algorithm from the **Encryption Algorithm** drop-down list. The following are the encryption algorithm options:
 - AES 256-bit
 - Twofish 256-bit
 - ChaCha20: 256-bit
- b. Select the Key Derivation Function. The following are the options:
 - Argon2 (KDBX 4 recommended)
 - AES-KDF (KDBX 4)
 - AES-KDF (KDBX 3.1)
- c. Enter a number in the **Transform rounds** field. Click the **Benchmark 1-second delay** button to set the recommended value.

- **WARNING:** Be careful when setting parameters for Argon2 because this algorithm is designed to take a long time on powerful hardware. Lower values are safe and it is recommended to set the benchmark to 1-second delay.
 - d. Set the appropriate value in the **Memory Usage** field.
 - e. Set the appropriate value in the **Parallelism** field.
 - 9. Click the **Continue** button. The Database Master Key screen appears:

👀 Create a new KeePassXC database		?	\times
	Database Master Key		
	A master key known only to you protects your database. Password Enter password: Confirm password: Cance Add additional protection	el	
	Go Back Done	Cancel	

- 10. Enter a strong password for your database on this screen.
- **NOTE:** Keep this password for your database safe. Either memorize it or note it down somewhere. Losing the database password might result in permanent locking of your database and you will not be able to retrieve information stored in the database.

11. Click the **Add additional protection** button. The following screen appears where you can provide enhanced protection for your database.

🛈 Create a new KeePassXC database		? ×
	Database Master Key	
	A master key known only to you protects your database. Password Enter password: Confirm password: Cancel Key File	
	You can add a key file containing random bytes for additional security. You must keep it secret and never lose it or you will be locked out!	
	Add Key File	
	YubiKey Challenge-Response If you own a <u>YubiKey</u> , you can use it for additional security. The YubiKey requires one of its slots to be programmed as <u>HMAC-SHA1 Challenge-Response</u>	<u>e</u> .
	Go Back Done C	ancel

12. Click the Add Key File button. The following screen appears:

👀 Create a new KeePassXC database	?	у X
	Database Master Key	
	A master key known only to you protects your database. Password Enter password: Confirm password: Cancel]
	Key File Browse Generate Cancel	
	YubiKey Challenge-Response If you own a <u>YubiKey</u> , you can use it for additional security. The YubiKey requires one of its slots to be programmed as <u>HMAC-SHA1 Challenge-Response</u>	
	Go Back Done Ca	ncel

- 13. Click the **Browse** button to locate and select a random file from your computer that you want to designate as your key file. Or, click the **Generate** button to create a key file with random data. The key file you generate is saved on your preferred location with a .**key** extension.
- **NOTE:** A key file is a master password in a file. Key files are typically stronger than master passwords, because the key file can be a lot more complicated. You can use a key file instead of a password in addition to a password. A key file can be any file you choose with random data. Do not modify the key file; else it will disable you from opening your database. To use a different key file, you can change the master key and use a new or a different key file. Always create backups of your key file on a different computer/disc or on your preferred storage space such as Google Drive or Microsoft OneDrive.
 - 14. Click **Done**. You are prompted to select a location to save your database file and complete creating a your database with basic settings. The database file is saved on to your computer with the default .kdbx extension.

2.4 Opening Existing Database

To open an existing database, perform the following steps:

1. Open your KeePassXC application. The following screen appears:

€ KeePassXC	—	×
<u>D</u> atabase E <u>n</u> tries <u>G</u> roups <u>T</u> ools <u>H</u> elp		
🕐 🎴 🔚 < < 🐇 🗓 🥙 🏰 🌍 🔒 🥕 🥟 Search (Ctrl+F)		0
Welcome to KeePassXC 2.4.0-beta1		
Open existing database		
Import from KeePass 1 Import from CSV		
Recent databases		

2. Click the **Open existing database** button.

3. Navigate to the location of the your database on your computer and open the database file. The following screen appears:

🚺 a.kdbx [Lo	ocked] - Ke	eePassXC										_		×
	Entries	Groups	Tools	Help										
🦻 💾		\ll	Ľ		i) () 🏟		1 Si	8	Search (Ctrl-	+F)			0
_ .														
Enter mas	ster key													
C:/a.kdbx														
De concerde														0
Password:		•												$\widehat{\circledast}$
Key File:												N	Brows	e
Challenge	Response:												Refres	h
												ОК	Cance	el l

- 4. Enter the password for your database.
- 5. Browse for the Key file if you have chosen it as an additional authentication factor while creating the database. See "Creating Your First Database" on page 11.

🛈 a.kdbx - KeePassXC				_		×
<u>D</u> atabase E <u>n</u> tries <u>G</u> roups <u>T</u> ools <u>H</u> elp						
P 🔒 🗟 🖑 🖓	i) Ø 🏦	🖗 🔒 🎤	😹 Search	(Ctrl+F)		0
Root	Title	Username	Password	URL	Notes	
	🔑 Standard Charte	johnsmith	•••••	www.standardcharter		
	<					>
	🔑 / Standard C	hartered				8
	General Attributes	Attachments Notes	Autotype			
	Username johnsi	mith				
	Password	•••••				
	URL <u>www.</u>	standardchartered.com				
	Expiration Never					

6. Click **OK**. The database opens and the following screen is displayed:

Chapter 3: Entry Management

This chapter covers the following topics:

- Adding an Entry
- Editing an Entry
- Deleting an Entry

3.1 Adding an Entry

All the details such as user names, passwords, URLs, attachments, comments, so on are stored in the database in individual entries. You can create as many entries as you want in the database.

To add an entry, perform the following step:

1. Navigate to Entries > New Entry (Or, press Ctrl+N). The following screen appears:

Passwor	ds - KeePassXC	_		\times
<u>D</u> atabase E	E <u>n</u> tries <u>G</u> roups	<u>T</u> ools <u>H</u> elp		
9 🖴 🔒	& & & &	🗐 🖗 🏶 🔒 🎤 🛛 🕷 Search		
Root > A	dd entry			
<u>^</u>	Title:	American Exress		
	Username:	johnsmith		
Entry	Password:	•••••		(
G	Repeat:	•••••		۲
10	URL:	https://www.americanexpress.com		
Advanced	Expires	20-03-2019 05:03	Presets	•
00	✓ Notes			
lcon				
Auto- Type				
1				
Properties				
		ОК	Cance	1

- 2. Enter a desired name of the entry, user name, password, repeat password, and notes on this screen.
- 3. Select **Expires** check-box to set the expiry date for the password. You can manually enter the date and time or click the **Presets** button to select a expiry date and time for your password.
- 4. Click OK.

3.1.1 Advanced Entry Settings

A lot of applications and web sites now require to provide additional information when you create accounts. The additional information is used to block hackers if any suspicious activity is detected. In addition, the additional information you provide is used to retrieve passwords if you forget them.

NOTE: Prefix the attribute name with **KPH:** if you want add attributes for use in the browser extension.

To add an entry, perform the following step:

- 1. Navigate to Entries > New Entry.
- 2. Select **Advanced** from the menu on the left. The following screen appears:

0 Passwords -	KeePassXC			_		\times
	es <u>G</u> roups <u>T</u> ools <u>H</u> el					
P 🔒 🔒 < «	x « I I I	🐨 🔒 🥜	🕷 Search			
Root > Add	entry					
<u> </u>	Additional attributes					
F ata (First Car	Toyota			Add	
Entry					Remove	
1 and a second s					Edit Name	
Advanced				[Protect	
					Reveal	
Icon	Attachments					
		Name	Size		Add	
Auto-					Remove	
Туре					Open Save	
					J	
Properties	Foreground Color:	Background Color	:			
▼						
				ОК	Can	cel

- 3. Under the **Additional attributes** section, click the **Add** button to add the attribute name and the associated value in the text boxes.
- 4. Select the **Protected** check-box if you want to hide the value associated with the attribute.

- 5. Under the **Attachments** section, click the **Add** button to store any file in the KeePassXC application.
- **NOTE:** When you try to open the attached file later and if the internal viewer/editor cannot handle (for example, a PDF file), KeePassXC extracts the attachment to a temporary file and opens it using the default application associated with this file type. After finishing viewing/editing, the you can choose between importing or discarding the changes that you made to the temporary file. KeePassXC securely deletes the temporary file (including overwriting it).

Passwords -					_		\times
	ies <u>G</u> roups <u>T</u> ools <u>I</u>						
	« « 🕹 🗊 🕘 🛔	🖤 🔒 🎤	🕷 Search				
Root > Add	entry						
<u> </u>	-						
	Additional attributes						
	First Car	[PROTECTED] Press re	veal to view or edit		А	.dd	
Entry					Dar	nove	
(C.					Ren	nove	
1°					Edit	Name	
Advanced					F	Protect	
					Re	veal	
00							
Icon	Attachments						
		Name	,	ize		Add	
						Remove	
Auto-	Document.rtf		330.00 B			Open	
Туре						Save	
Properties	Foreground Color	: Background	Color:				
Toperties							
					ОК	Cano	el

- 6. Click the **Foreground Color** check-box and the color button adjacent to it to select the text color for your entries.
- 7. Click and the **Background Color** check-box and the color button adjacent to it to select the background color for your entries.

🛈 Passwords - KeePas	sXC		- 🗆 X
<u>D</u> atabase E <u>n</u> tries <u>G</u> ro			1
P 🔒 🔒 🗟 🗸 🖑	🚺 Select Color	×	
Root > Add entry			Add Remove Edit Name I Protect
Icon Attach Auto- Type Properties	Add to Custom Colors	Hu <u>e</u> : 0 ♥ Red: 0 ♥ Sat: 0 ♥ Green: 0 ♥ Val: 0 ♥ Bl <u>u</u> e: 0 ♥ HTML: #000000 OK Cancel	Reveal Add Remove Open Save

8. Clear the check-boxes to set the default text color as black and background color as white.

3.1.2 Assigning Icons to Entries

You select various icons to be displayed along with your entries for identification purpose. KeePassXC comes with a set of default icons that you can use or you can use your own custom icons.

To add an icon to an entry, perform the following step:

1. Navigate to **Entries > New Entry > Icon**. The following screen appears:

Database Entries Grou	. –	<u>H</u> elp		Ø			Ω	1.6	r									
Root > Add entry	L L	i 4.) (1)	Ø,		8	0	1 6	-									
						Ŧ		1	<i>V</i>		8	Search	n (Ctrl+F))				0
-	<u>U</u> se default ic	on																
	/ 😒	Δ	2		8	%	2	@	3	Ø	0	P	\$	a		@	\odot	^
Entry	9	0	ß		<u>;</u>	\$ }	Ø		_		% ≡	5>	ė	••		Z	8	
	\$	4	\otimes		1	Ø		0	×	?	٦	ò	D	6	•		V	
June 1	/ 🔤	\checkmark	Ħ	8	~	6	숬	٥	/	Ò	W	\$	×.	2				~
	Use custo <u>m</u> io	on																
Advanced																		
00																		
lcon																		
▼			Add	custom	icon							C)elete cu	stom ico	า			
														Г	OK		Cance	2

- 2. Select the **Use default icon** check-box and then select a desired icon that you want to appear with your entry.
- 3. Or, select the **Use custom icon** check-box and then click the **Add custom icon** button to choose an icon from your computer.

NOTE: To delete the custom icon, select the item to be deleted and click the **Delete custom icon** button.

4. Click **OK**.

3.1.3 Configuring Auto-Type Feature

Auto-Type feature lets you automatically populate the data from your entries in the database to the corresponding websites or applications.

You can configure the Auto-Type feature to either function at global level or entry level.

- Configuring Global Auto-Type Feature
- Configure Auto-Type Sequences for Entries

3.1.3.1 Configuring Global Auto-Type Feature

Users can define global auto-type hotkeys that start the auto-type process:

To configure the Auto-Type feature, perform the following steps:

1. Open the KeePassXC application on your desktop and navigate to **Tools** > **Settings** > **Auto-Type**. The following screen appears.

👀 Settings - KeePassXC					_		×
	froups Tools Help						
		i) Ø 🔹 📦	Search	n (Ctrl+F)			0
Application Settings							
A	Basic Settings Auto-Ty)e					^
General		windows for global Auto-Type windows for global Auto-Type ming Auto-Type					
Scherdi	Global Auto-Type shortcut						
	Auto-Type start delay	500 ms				-	
v	Auto-Type typing delay	25 ms					
Security							
Browser Integration							Ŷ
			[ОК	Cancel	App	ý

- 2. Select the **Use entry title to match windows for global Auto-Type** check-box to start the auto-type process when entry title matches windows title.
- 3. Select the **Use entry URL to match windows for global Auto-Type** check-box to start the auto-type process when URL in the matches the URL in the browser window.

- 4. Select the **Always ask before performing Auto-Type check-box** to start the auto-type process when entry URL matches the URL in the windows.
- 5. In the **Global Auto-Type shortcut** field, press the key combination that you want to use to start the auto-type process.
- 6. In the **Auto-Type start delay** field, set the delay time in milliseconds before the auto-type process starts.
- 7. In the **Auto-Type typing delay** field, set the delay time in milliseconds before the auto-type process starts

3.1.3.2 Performing the Global-Level Auto-Type Operation

The global Auto-Type keyboard shortcut is used when you have focus on the window you want to auto-type into. To make use of global-level Auto-Type feature, it must be correctly configured. See "Configuring Global Auto-Type Feature" on page 26.

Pressing the shortcut keys searches the database for entries that match the window title. Multiple matches may be returned, which need to be selected by the user as shown in the following screen:

🚯 Auto-Type - Kee	PassXC			?	×
Select entry to Auto-	Type:				
Group	Title	Username	Sequence		
🝺 NewDatabase	🝐 Test 2	user	{USERNAME}{TAB}PASSWORD}EN	ITER}	
🔯 NewDatabase	Sample Entry 3	New User	{PASSWORD}{ENTER}		
🔯 NewDatabase	🔑 LinkedIn		{USERNAME}{TAB}PASSWORD}EN	ITER}	
þearch					
			[Cance	el l

3.1.3.3 Configure Auto-Type Sequences for Entries

The Auto-Type functionality in KeePassXC allows you to define a sequence of automatic keypresses. The simulated key-presses can be sent to any other currently open window of your choice (web browser windows, login dialogs boxes, and so on). By default, the auto-type sequence is {USERNAME}{TAB}{PASSWORD}{ENTER}. This means that it first types the **user name** of the selected entry, then presses the **Tab** key, then types the **password** of the entry and finally presses the **Enter** key.

NOTE: You do not need to install the KeePassXC-Browser plug-in to use the Auto-Type feature.

To enable Auto-Type for your entries, perform the following step:

1. Navigate to **Entries** > **New Entry**.

2. Select **Auto-Type** from the menu on the left. The following screen appears:

👀 Password	s - KeePassXC	- 🗆 X
<u>D</u> atabase E <u>n</u>	<u>tries G</u> roups <u>T</u> ools <u>H</u> elp	
9	ኛ ≪ ≪ & ⊕ Ø ☆ ♥ 🔒 ≁	🕷 Search
Root > Am	nerican Express > Edit entry	
<u> </u>	Enable Auto-Type for this entry	
	○ Inherit default Auto-Type sequence from the group	
Entry	• Use custom Auto-Type sequence:	
C.	{USERNAME}{TAB}{PASSWORD}{ENTER}	
10	Window Associations	
Advanced	American Express IN Log in Credit Cards, Re	Window title:
20 0		n Credit Cards, Rewards, Offers - Google Chrome
00		Use a specific sequence for this association:
lcon		{USERNAME}{TAB}{PASSWORD}{ENTER}
-		
Auto-		
Туре		
<i>€∕</i>	+ -	
		OK Cancel Apply

- 3. Select the Enable Auto-Type for this entry check-box.
- 4. You have an option to either inherit the Auto-Type sequence from the group-level or create custom sequence.
 - Select the **Inherit default Auto-Type sequence from the group** option if you have enabled and defined the Auto-Type sequence at the group-level.
 - Or, Select the Use custom Auto-Type sequence to define the sequence based on the inputs required for your desktop or web applications and in the text field, enter the desired sequence. For more information on the typing codes, see https://keepass.info/ help/base/placeholders.html.
- 5. Under the **Window Associations** section, click the + button and select any open window or application with which you want to associate the Auto-Type sequence. This is the window or application where the details of the entries will be sent when you perform the Auto-Type operation.

NOTE: You can use wild-card characters in the window title. For example, notepad*.

3.1.3.4 Performing the Entry-Level Auto-Type Operation

For this operation, the KeePassXC window is minimized and the Auto-Type action occurs in the previously selected window. Performing entry Auto-Type from the context menu or pressing Ctrl+Shift+V Auto-Types the currently selected entry into the last used window.

To make use of entry-level Auto-Type feature, it must be correctly configured. See "Configure Auto-Type Sequences for Entries" on page 27.

NOTE: Be careful when using this as it could select a wrong window. For example, a chat window.

To perform the Auto-Type operation, perform the following steps:

1. Select and right-click the entry that you have associated with a window or an application.



2. Click Perform Auto-Type.

The details from the entry get populated in the fields of the previously selected window or the application.

3.2 Viewing Properties

KeePassXC lets you view the basic properties such as date and time of creation, modification, and when last accessed.

To view the properties, navigate to **Entries** > **New Entry** > **Properties**. The following screen appears:

Password	ls - KeePas	ssXC						_		×
<u>D</u> atabase E <u>r</u>	ntries <u>G</u> ro	oups <u>T</u> ools <u>H</u> elp								
P 🔒 🔒 🖉	< ≪ ≪) 🔒 🎤	🕷 Search						
Root > An	nerican	Express > Edit	entry							
	Created:	20 Mar 2019 05:11	:22							
	Modified:	26 Mar 2019 16:40):39							
Entry	Accessed:	26 Mar 2019 16:40):39							
G	Uuid:	c2fc578c12df4210	da7bca0582390aa6							
10	Plugin D	ata								
Advanced		Кеу			Value				Remov	/e
900										
00										
Icon										
Auto-										
Туре										
Properties										
History										
						[OK	Cancel	Ар	bly

3.3 Managing History

KeePassXC maintains the history of changes you make to your entries. Each time you change an entry, KeePassXC automatically creates a backup copy of the current, non-modified entry before saving the new values. You can view the changes you made previously, restore, and delete the history of changes you made.

To manage the history associated with an entry, perform the following steps:

👀 Passwords - KeePassXC				_	
Database Entries Groups	Tools Help				
P 🚔 🔚 🗳 🍳	< < 🔊 👘 🖉	🏶 🔒 🎤	Search	(Ctrl+F)	0
Root	Title			Username	Passwore
	American Express	💐 New entry	Ctrl+N	johnsmith	•••••
		🔾 Edit entry	Ctrl+E		
		🖙 Clone entry	Ctrl+K		
	<	Delete entry	Del		>
		Copy username	Ctrl+B		8
	General Attributes Attachme	Copy password	Ctrl+C		
	Username johnsmith	Copy attribute			
		TOTP	•		
	Password 🝙 •••••	Open URL	Ctrl+Shift+U		
	URL http://www.americ	Perform Auto-Type	Ctrl+Shift+V		
	Expiration Never				

1. Select the entry for which you want to manage history.

2. Right-click on the entry for which you want to manage history and click **Edit entry** from the menu. The following screen appears:

Password	s - KeePassXC				—		×
<u>D</u> atabase E <u>n</u>							
9 🕒 🔒 🍕	2 < < 4	🗓 🕗 🏦 🖨 🔒 🥕	rch				
Root > Am	nerican Exp	ress > Edit entry					
	Title:	American Express					
Entry	Username:	johnsmith					
Entry	Password:	•••••					۲
	Repeat:	•••••					۲
Advanced	URL:	https://www.americanexpress.com					
	Expires	20-03-2019 05:11			\sim	Presets	5 -
000	✓ Notes						
lcon							
-1							
Auto-							
Туре							
12							
Properties							
1-41							
History							
				OK Ca	ancel	Appl	y

3. Click the **History** button in the menu bar on the left. The following screen appears:

🛈 Password	s - KeePassXC						_		\times
	atabase E <u>n</u> tries <u>G</u> roups <u>I</u> ools <u>H</u> elp P 🗃 🔜 🔍 🔍 🍣 🗊 🖉 🏦 💭 🖕			🛞 Search					
Root > An	nerican Express	> Edit entry							
	Last modified	Title	Username	URL					
Entry	26-03-2019 16:52	American Express	johnsmith	https://w	ww.americanexpress.	com			
ß									
Advanced									
00									
lcon									
Auto-									
Туре									
1									
Properties									
History									
	Show	,	Restore		Delete	9	Delete	e all	
						ОК	Cancel	Ap	ply

- 4. You can perform the following operations:
 - Show: Click the **Show** button to view details from the older entry.
 - Restore: Click the **Restore** button to reinstate the entry details from the older entry.
 - Delete: Click the **Delete** button to delete <need input here>.
 - Delete all: Click this button to delete the entire history.

3.4 Editing an Entry

To edit the details in an entry, perform the following steps:

- 1. Select the entry you want to edit.
- 2. Right-click and select **Edit entry** from the menu. The following screen appears:

					_		×
<u>D</u> atabase E <u>n</u>	tries <u>G</u> roups	<u>T</u> ools <u>H</u> elp					
9 📔 🔒 🖾	2 « « ا	i) 🕗 🛔 🖨 🔒 🎤 🛛	<i>8</i>	Search			
Root > Am	nerican Exp	ress > Edit entry					
<u> </u>	Title:	American Express					
	Username:	johnsmith					
Entry	Password:	••••					
la s	Repeat:	••••					۲
10	URL:	https://www.americanexpress	s.com				
Advanced	Expires	20-03-2019 05:11			~	Presets	•
00	✓ Notes						
Icon							
Auto-							
Туре							
1							
Properties							
		1		ОК	Cancel	Apply	,

- 3. Make the desired changes. For more information, see Adding an Entry.
- 4. Click Save.

3.5 Cloning an Entry

Creating a clone of an entry provides you a ready-to-use template for creating new entries with similar details of a master entry.

To create a clone of an existing entry, perform the following steps:

1. Right-click on the entry for which you want to create a clone as shown in the following figure.

👀 Passwords - KeePassXC					_		×
<u>D</u> atabase <u>En</u> tries <u>G</u> roups	ools <u>H</u> elp						
🕑 🔛 🔚 < 🗸	🥰 🔊 🗊 🥙 🎂 🛢	a fi	ŝ	Search (Ctrl+F)			0
Poot	Title			Username		F	asswor
Koot	American Express American Express General Attributes Attachments Notes Username johnsmith Password URL http://www.americanexpress.com Expiration Never	A B & B	New entry Edit entry Clone entry Delete entry Copy username Copy assword Copy attribute TOTP Open URL Perform <u>A</u> uto-Type	Ctrl+N Ctrl+K Del Ctrl+B Ctrl+C , Ctrl+C , Ctrl+Shift+U Ctrl+Shift+V			**************************************

The Clone Options window appears.



- Select the **Append** '- **Clone**' to title check-box to create a new entry with the word Clone as the suffix to the name of the new entry.
- Select the **Replace username and password with references** check-box to create the new entry where the username and the password fields contain the references to the username and password to the master entry.
- Select the **Copy history** checkbox to copy the history of the master entry to the clone.

3.6 Deleting an Entry

To delete an entry, perform the following steps:

- 1. Select the entry you want to delete and press the **Delete** button on your keyboard.
- 2. You are prompted to move the entry to Recycle Bin.
- **NOTE:** The entry is not deleted immediately. The entry moves to the Recycle Bin, which does not exist in KeePassXC by default. It is created dynamically when you delete an entry for the first time.
 - 3. To permanently delete the entry, navigate to the Recycle Bin, select the entry you want to delete and press the **Delete** button on your keyboard.
Chapter 4: Database Management

This chapter covers the following topics:

- Importing External Databases
- Advanced Database Settings
- Backing up Database File
- Sharing Database File

4.1 Importing External Databases

KeePassXC allows your to import external databases from the following options:

- KeePass 1 Database
- Comma-Separated Values (CSV) file

4.1.1 Importing KeePass 1 Database

KeePass 1 database is an older format of the database created using legacy version of KeePass. KeePassXC lets your import this older format of the database and you can seamlessly start using this database in your new KeePassXC application.

To import a KeePass 1 database file in KeePassXC, perform the following steps:

1. Open your KeePassXC application. The following screen appears:

KeePassXC		_	×
<u>D</u> atabase E <u>n</u> tries <u>G</u> rou			
🌔 🔚 🔚	🕐 ≪ 🍇 🗓 🥘 🏰 😨 🔒 🥕 🌾 Search (Ctrl+F)		0
	Welcome to KeePassXC 2.4.0-beta1		
	Create new database		
	Open existing database		
	Import from KeePass 1 Import from CSV		
	Recent databases		

2. Click the **Import from KeePass 1** button.

3. Navigate to the location of the your legacy KeePass 1 database file (.kdb) on your computer and open the file. You are prompted for the password and the Key file for your .kdb file.

👀 Database.kdb [Locked]	- KeePassXC —		
	roups <u>T</u> ools <u>H</u> elp		
	🕈 🔍 🖑 🏝 🗓 🥙 🏰 😰 🔒 🥕 🍙 Search (Ctrl+F)	0	
Import KeePass1 da	Itabase		
C:/Database.kdb			
Password:	•	۲	
Key File:	×	Browse	
Challenge Response:		Refresh	
	ОК	Cancel	
	- AU	Cancer	

- 4. Enter the password for your old .kdb file and click **OK**. You are prompted for provide a name for the new database format that KeePassXC recognizes.
- 5. Provide a name for the new database format, select a folder on your computer to save the file, and click **Save**.

The data from the .kdb file gets imported and converted to the new format, which is compatible with KeePassXC. You can now start using the new database file (.kdbx) in KeePassXC.

4.1.2 Importing CSV File

If you have been saving your URLs, usernames, passwords, and so on in a CSV file, you can migrate all that information from the CSV file to KeePassXC and start using KeePassXC to maintain your data.

To open the CSV file, perform the following steps:

1. Open your KeePassXC application. The following screen appears:

Database Entries Groups Tools Help Image: Additional stress of the stress	4	0
Image: Search (Ctrl+F) Image: Search (Ctrl+F)	4	0
Welcome to KeePassXC 2.4.0-beta1		
Create new database		
Open existing database		
Import from KeePass 1 Import from CSV		
Recent databases		

2. Click the **Import from CSV** button.

3. Navigate to the location of the your CSV file on your computer and open the file. The General Database Information screen appears.

🚯 Create a new KeePassXC database	?	×
General Database Information		
Please fill in the display name and an optional description for your new database: Database Name: Presswords Description:		
Go Back Continue	Cancel	

- 4. Enter a name in the **Database Name** field. If you do not enter a name in this field on this screen, you will be prompted to provide a name when you are done creating the database.
- 5. (Optional) Enter desired details in the **Description** field.
- 6. Click **Continue**. The Encryption Settings screen appears.

👀 Create a new KeePassXC database		? ×
	Encryption Settings	
	Here you can adjust the database encryption settings. Don't worry, you can change them later in the database settings.	
	Decryption Time: 1.0 s	
		1
	100 ms	5 s
	Higher values offer more protection, but opening the database will take longer. Database format: KDBX 4.0 (recommended)	~
	This is only important if you need to use your database with other programs.	ettings
	Go Back Continue	Cancel

- 7. Drag the **Decryption Time** slide based on your encryption strength of your database. Setting the Decryption Time slider at a higher values means that the database will have higher level of protection but the time taken for the database to open will increase.
- 8. Select the **Database format** from the following options available in drop-down list.
 - KDBX 4.0 (recommended)
 - KDBX 3.1
- 9. Optional. Click the **Advanced Settings** to provide additional settings for your database.

10. Click the **Continue** button. The Database Master Key screen appears:

👀 Create a new KeePassXC database		?	\times
	Database Master Key		
	A master key known only to you protects your database.		
	Password		
	Enter password:	6	
	Confirm password:		
	Car	ncel	
	Add additional protection		
	Go Back Done	Cancel	

- 11. Enter a strong password for your database on this screen.
- **NOTE:** Keep this password for your database safe. Either memorize it or note it down somewhere. Losing the database password might result in permanent locking of your database and you will not be able to information stored in the database.

12. Click **Done**. You are prompted to select a location to save your database file.

abase Entries Groups Tools Help				
? 🕒 🗐 🖑 🖉 🌾 🕼 🗐 🖗 🕯	ی 🔒 🔒	Searce	ch (Ctrl+F)	
nport CSV fields				
👀 Save database as		×		
\leftarrow \rightarrow \checkmark \uparrow \checkmark \rightarrow This PC \rightarrow LENOVO (D:) \checkmark \eth	Search LENOVO (D:)	Q		
Organize - New folder		🕜 l by	п	~
V S This PC Name	Date modified	_{Typ} vith	#	~
> 🧊 3D Objects 🔋 Applications	19-10-2014 09:25	File	Consider '\' an escape	e character
> Desktop	19-10-2014 09:25	File		
> 🗎 Documents				
> Downloads Music				
> Pictures V <		>		
File name: Passwords		~		
Save as type: KeePass 2 Database (*.kdbx)		~		
			Last Modified	Created
▲ Hide Folders	Save Cano	cel		
3 scraig scraig school491				
4 ccraig ccraig school491			ОК	Cancel
5 zcraig zcraig school491			0.	

13. Close the **Save database as** window. The Import CSV fields screen appears.

Pa.								
	sswords [New Datab	oase]* - KeePassXC						>
atak	ase Entries G	Groups Tools	Help					
9	🕒 🔒 🍕		6] () ()	🏥 🖤 🔒	and the	Sear	rch (Ctrl+F)	6
assw	ords.kdbx [Locked]	Passwords [New	w Database]* 🗵					
[mj	port CSV fields	1						
	PKMSampleImport.cs							
	oyte(s), 7 row(s), 3 co acoding	lumn(s)						
CI	-							
	Codec	UTF-8		~		Text is qualified by	н	~
Fie	lds are separated by	,		~	C	Comments start with	#	~
	First record has field i	names Nu	umber of headers line to	o discard 0 🜲			Consider '\' an escape	e character
	olumn layout			1 12				
	olumn layout Group column 1	~		UR	L Not present in C	CSV file 🗸		
	-	× ×		UR Note				
Co	Group column 1			Note		CSV file ~		
Ca	Group column 1 Title column 2	~		Note Last Modifie	Not present in C	CSV file ~		
Co	Group column 1 Title column 2 Isername column 3	~		Note Last Modifie	es Not present in C	CSV file ~		
Co	Group column 1 Title column 2 Isername column 3 Password Not presen	~	Username	Note Last Modifie	es Not present in C	CSV file ~	Last Modified	Created
Co	Group column 1 Title column 2 Isername column 3 Password Not presen	 ✓ t in CSV file ✓ 	Username PassKeyPassword	Note Last Modifie Create	 Not present in 0 Not present in 0 Not present in 0 	CSV file v CSV file v CSV file v	Last Modified	Created
Cc U F Pr	Group column 1 Title column 2 Isername column 3 Password Not presen eview Group	 ✓ t in CSV file ✓ 		Note Last Modifie Create	 Not present in 0 Not present in 0 Not present in 0 	CSV file v CSV file v CSV file v	Last Modified	Created
Ccc U F Pr 1 2	Group column 1 Title column 2 Isername column 3 Password Not presen eview Group SchoolwiresUser	 ✓ ✓ Title PassKeyUserNa 	PassKeyPassword	Note Last Modifie Create	 Not present in 0 Not present in 0 Not present in 0 	CSV file v CSV file v CSV file v	Last Modified	Created
Cc U Pr 1 2 3	Group column 1 Title column 2 Isername column 3 Password Not presen eview Group SchoolwiresUser vcraig	 t in CSV file Title PassKeyUserNa vcraig 	PassKeyPassword school491	Note Last Modifie Create	 Not present in 0 Not present in 0 Not present in 0 	CSV file v CSV file v CSV file v	Last Modified	

- 14. Choose the appropriate settings and change the column associations to match the database file with your CSV file.
- 15. Click **OK**. The **Save database as** window appears.
- 16. Provide a name for your new database file and click **Save**.

Your CSV file gets imported to KeePassXC and the data is converted to the KeePassXC format for further usage and maintenance. The new database file is saved on to your computer with the default .kdbx extension.

4.2 Advanced Database Settings

This section describes the advanced database settings.

4.2.1 General Settings

At any point of time, you can change the settings for your database that you created earlier.

To make changes to the general settings, perform the following steps:

1. Navigate to **Database > Database settings**. The following screen appears:

🛈 Passwords - KeePassX	ic la	_		×
Database Entries	<u>G</u> roups <u>T</u> ools <u>H</u> elp			
🌔 🔚 🔄	😤 🔍 🖑 🏭 🗓 🥙 🏰 🌍 🔒 🥕 🧥 Search (Ctrl+F)			0
A	Database Meta Data			
	Database name: Passwords			
und and a second	Database description:			
<i>I</i> 🔿	Default username:			
General	History Settings			
	Max. history items: 10			
	Max. history size: 6 MIB			
	✓ Use recycle bin			
	Additional Database Settings			
Security	✓ Enable compression (recommended)			
	C Enable compression (recommended)			
•••				
KeeShare				
•				
Advanced Settings		ОК	Car	icel

- 2. Click the **General** button in the menu bar in the left page and make the following changes as desired:
 - **Database name**: This is the default identifier for your database. You can change this name as desired.
 - Database description: Provide some meaningful description for your database.
 - **Default username**: Provide a default username for all the new entries that you create in a database.

- **Max. history items**: This is the maximum number of history items that are stored for each entry. When you set this to 0, history is not saved. Set this value to a low value to prevent the database from getting too large.
- **Max. history size**: When the history of an entry gets above this size, it is truncated. For example, this happens when entries have large attachments. Set this value small to prevent the database from getting too large.
- **Use recycle bin**: Select this check-box if you want the entries to move to the recycle bin when you delete them. The entries are not deleted immediately. The entries moves to the Recycle Bin, which does not exist in KeePassXC by default. It is created dynamically when you delete an entry for the first time.
- **Enable compression**: KeePassXC databases can be compressed before being encrypted. Compression reduces the size of the database, but also slows down the database saving/loading process a bit. It is not recommended to save databases without compression.

4.2.2 Security Settings

KeePassXC provides you with options such as master key and encryption that provide enhanced security to your databases.

The following sections describe the steps to configure enhanced security options for your databases.

4.2.2.1 Master Key Settings

You can set the password, key file, and YubiKey Challenge-Response to your database for enhanced security.

To do so, perform the following steps:

1. Navigate to **Database > Database settings** and then click on the **Security** button in the menu on the left. The following screen appears:

👀 Passwords - KeePassXC	:	-		×
<u>D</u> atabase E <u>n</u> tries <u>G</u>	roups <u>T</u> ools <u>H</u> elp			
9 💾 🔒 🍕	🕈 🔍 🖑 🏭 🗓 🥙 🏰 😰 🔒 🥕 👔 Search (Ctrl+F)			0
A	Master Key Encryption Settings			
	Password			
10	Password set, click to change or remove			
General	Change Password Remove Password			
	Add additional protection			
Security				
101				
KeeShare				
Advanced Settings		OK	Car	icel

- 2. Click the **Change Password** button to set a new password for your database.
- 3. Click the **Remove Password** button if you want to remove the password as the security setting of your database.

4. Click the Add additional protection button. The following screen appears:

🚺 Passwords - KeePassXC	:	—		\times
<u>D</u> atabase E <u>n</u> tries <u>G</u>	roups <u>T</u> ools <u>H</u> elp			
🕑 🔛 🖶 🝕	🕈 🔍 🖑 🎒 🗐 🔮 🏪 🌍 🔒 🥕 🛞 Search (Ctrl+F)			0
<u> </u>	Master Key Encryption Settings			
R.	Password			
10	Password set, click to change or remove			
General	Change Password Remove Password			
	Key File			
	You can add a key file containing random bytes for additional security.			
0	You must keep it secret and never lose it or you will be locked out!			
	Add Key File			
Security	Aud key file			
Security	YubiKey Challenge-Response			
	If you own a <u>YubiKey</u> , you can use it for additional security.			
	The YubiKey requires one of its slots to be programmed as <u>HMAC-SHA1 Challenge-Response</u> .			
	Add YubiKey Challenge-Response			
KeeShare				
Reeshare				
Advanced Settings		ОК	Car	ncel

5. Add security settings such as **Key File** and **YubiKey Challenge-Response**.

4.2.2.2 Encryption Settings

KeePassXC supports the highly secure Advanced Encryption Standard (AES), the Twofish, and ChaCha2.0 as the algorithms to encrypt its databases. KeePassXC encrypts complete databases and not just the password fields. For example, in addition to your passwords, your user names, notes, and so on are encrypted.

KeePassXC provides a protection against dictionary and guessing attacks. Such attacks cannot be prevented, but it can be made difficult for the attackers to crack the vulnerabilities. For this, the key *K* derived from the user's composite master key is transformed using a key derivation function with a random salt. This prevents a pre-computation of keys and adds a work factor that the user can make as large as desired to increase the computational effort of a dictionary or guessing attack.

The following key derivation functions are supported:

• **AES-KDF (KDBX 4 and KDBX 3.1)**: This key derivation function is based on iterating AES. Users can change the number of iterations. The more iterations, the harder are dictionary and guessing attacks, but also database loading/saving takes more time

(linearly). KDBX 3.1 only supports AES-KDF; any other key derivation function, like for instance Argon2, requires KDBX 4.

• Argon2 (KDBX 4 - recommended): KDBX 4, the Argon2 key derivation function can be used for transforming the composite master key (as protection against dictionary attacks). The main advantage of Argon2 over AES-KDF is that it provides a better resistance against GPU/ASIC attacks (due to being a memory-hard function). The number of iterations scales linearly with the required time. By increasing the memory parameter, GPU/ASIC attacks become harder (and the required time increases). The parallelism parameter can be used to specify how many threads should be used.

To chose and configure the encryption algorithms and key derivation functions perform the following steps:

👀 Passwords - KeePassX	c	_		\times
<u>D</u> atabase E <u>n</u> tries	<u>G</u> roups <u>T</u> ools <u>H</u> elp			
9 🔒 🔒 <	😵 🕰 🖏 🗓 🥘 🏪 😨 🔒 🥕 🚳 Search (Ctrl+F)			0
A	Database Meta Data			
	Database name: Passwords			
and the second s	Database description:			
I O	Default username:			
General	History Settings			
	Max. history items: 10			
	Max. history size: 6 MiB			
	✓ Use recycle bin			
Security	Additional Database Settings			
	Enable compression (recommended)			
•••				
KeeShare				
-				
•				
Advanced Settings		ОК	Can	icel

1. Navigate to **Database > Database settings**. The following screen appears:

2. Click the **Security** button in the menu on the left and then click the **Encryption Settings** tab. The following screen appears:

🛈 Passwords - KeePassX	c	_	
<u>D</u> atabase E <u>n</u> tries <u>O</u>	aroups Tools Help		
9 🔒 🔒 🍳	💱 🔍 🖑 🏭 🗐 🥙 🏰 🐨 🔒 🥕 👔 Search (Ctrl+F)		0
<u> </u>	Master Key Encryption Settings		
	Decryption Time: 1.0 s		
General	100 ms	1 1	۱ 5 s
0	Higher values offer more protection, but opening the database will take longer.		
Security	Database format: KDBX 4.0 (recommended) This is only important if you need to use your database with other programs.		~
•••			
KeeShare			
Advanced Settings		ОК	Cancel

- 3. Click and Drag the Decryption Time slider to set the time taken to decrypt the database. Higher values offer more protection but opening the database will take longer.
- 4. Select the Database format for your database. The options available are:
 - KDBX 4.0 (recommended)
 - KDBX 3.1

4.3 Storing Database File

The database file that you create might contain highly sensitive data and must be stored in a very secure way. You must make sure that the database is always protected with a strong and long password. The database file that is protected with a strong and long password is secure and encrypted while stored on your computer or cloud storage service.

Make sure that the database file is stored in a folder that is secure. Make sure that you or someone else does not accidentally delete the database file. Deletion of the database file results in a lot of inconvenience because you will need to manually retrieve the lost information for your various web applications. You must not share your database file with anyone unless absolutely necessary.

4.4 Backing up Database File

It is a good practice to create copies of your database file and store the copies of your database on different computer, smart phone, or cloud storage space such a Google Drive or Microsoft OneDrive.

Creating backups for your database give you a peace of mind should you lose one copy of your database. You can quickly retrieve the copy of your database and start using it.

4.5 Sharing Database File

If there is a need to share the database file with anyone, make sure that it is protected with a strong password. It is recommended that you also protect your database file with a Key file as well.

NOTE: Do not share the database file, password, and the Key File in a single communication. Send them separately through different messages.

KeePassXC

Chapter 5: KeePassXC-Browser Extension

This chapter covers the following topics:

- KeePass-Browser Extension
- Populating Database Entries to Websites

5.1 KeePass-Browser Extension

The KeePassXC-Browser extension is a software plug-in for your web browser that you can use to automatically pull your data from KeePassXC and populate them directly into the fields of your web-based application. It is a very useful plug-in that enhances your productivity by saving time. You do not need to manually copy the data from your KeePassXC database and paste them in the fields in the websites.

The KeePassXC-Browser extension is available on the following web browsers:

- Google Chrome
- Mozilla Firefox

5.1.1 Downloading KeePassXC-Browser Extension

You can download the KeePassXC-Browser extension from your web browser. In this section, the step to download the KeePassXC-Browser extension for Google Chrome are described.

To download the KeePassXC-Browser extension, perform the following steps:

1. Open **Google Chrome** and go to https://chrome.google.com/webstore/category/ extensions.

2. In the **Search** the store field, type **KeePassXC-Browser** and press **Enter**. The following screen appears.



3. From the search results, click on the Add to Chrome button. The following screen appears:

Add "KeePassXC-Brows	er"?
lt can:	
Read and change all your data on t	he websites you visit
Display notifications	
Modify data you copy and paste	
Communicate with cooperating nat	tive applications
	Add extension Cancel

4. Click the **Add extension** button from the pop-up window.

The KeePassXC-Browser extension gets added to Google Chrome.

5.1.2 Configuring KeePassXC-Browser

To start using KeePassXC-Browser, you must configure it so that it can communicate with the KeePassXC application on your desktop.

To configure KeePassXC-Browser, perform the following steps:

1. Open the KeePassXC application on your desktop and navigate to **Tools** > **Settings**. The following screen appears:



KeePassXC

2. Click the **Browser Integration** option on the left-hand side. The following screen appears:

🛈 Settings - KeePassXC		_		\times
Database Entries	Groups <u>T</u> ools <u>H</u> elp			
	😤 🔍 🖑 🏭 📋 🥘 🏰 😨 🔒 🥕 🧥 Search (Ctrl+F)			0
Application Settings				
	C Enable KeepassXC browser integration			
<u>f</u> a	General Advanced			
10	KeePassXC-Browser is needed for the browser integration to work. Download it for Firefox and Google Chrome / Chromium / Vivaldi.			
General	Enable integration for these browsers:			
	Chrome and Vivaldi			
	Chromium			
U 🔍	\checkmark Reguest to unlock the database if it is locked			
Security	✓ Match URL scheme (e.g., https://)			
	Return only best-matching credentials			
	• Sort <u>m</u> atching credentials by title			
۲	○ Sort matching credentials by <u>u</u> sername			
Browser Integration				
J. J				
•				
	OK	Cancel	Арј	ply

- 3. Under the **Enable integrations for these browsers** section, select the browsers for which you have downloaded the KeePassXC-Browser plug-in and click **OK**.
- 4. Open your browser for which you have downloaded the KeePassXC-Browser plug-in.
- 5. Click the **KeePassXC-Browser** plug-in icon in your browser (see figure). A pop-up window appears as shown in the following screen:



6. Click the **Connect** button in the pop-up window to complete integrating the KeePassXC-Browser plug-in with your KeePassXC desktop application. 7. If you connect the KeePassXC-Browser for the first time, you are prompted to enter a unique name to identify the connection. Enter a unique name in the field and click the **Save and allow access** button.



5.2 Populating Database Entries to Websites

The KeePassXC-Browser plug-in lets you automatically populate the entries from your KeePassXC database into the fields on the websites. To do so, perform the following steps:

- 1. Open your KeePassXC desktop application.
- 2. Open your web browser and open your website for which you have stored the URL, user name and password in the KeePassXC database.

The KeePassXC-Browser plug-in icon in your browser window automatically turns green when you open your KeePassXC desktop application. The green icon indicates that the KeePassXC desktop application is connected and communicating with the KeePassXC-Browser plug-in. The grey icon indicates that the KeePassXC desktop application is not connected with the KeePassXC-Browser plug-in.



3. If the KeePassXC desktop application is not connected with the KeePassXC-Browser plugin, click the grey KeePassXC-Browser plug-in icon in your web browser and click **Reload** from the pop-up window as shown in the following screen.



4. Open the URL for which you want to auto-populate the field values stores in your database. The **KeePassXC-Browser Confirm Access** window appears.

W KeePassXC-Browser Confirm Access	?	×
www.americanexpress.com has requested access to passwords for the following item(s). Please select whether you want to allow access.		
americanexpress - JohnSmith		
Remember this decision		
Allow	De	ny

- 5. Select the entry from the window and click **Allow**.
- 6. In your website, click inside your USER ID field, and select your username, which automatically gets extracted from your KeePassXC database. The username and the password automatically get populated in the respective fields.



Chapter 6: Search Operations

KeePassXC provides an enhanced and granular search features the enables you to search for specific entries in the databases using the different modifiers, wild card characters, and logical operators.

6.1 Modifiers

The following table lists the modifiers, which can be used in combination of one another:

Modifier	Description
-	Exclude this term from results.
+	Match this term exactly.
*	Term is handled as a regular expression.

You can use the modifier with the following fields:

- Title
- Username
- Password
- URL
- Notes
- Attribute
- Attachment

6.2 Wild Card Characters and Logical Operators

The search terms can contain the following wild card characters or logical operators in absence of regular expressions:

Wild Card Characters	Description
*	Match anything.
?	Match one character.

KeePassXC

Table 2: Wild Card Characters and	Logical Operators
-----------------------------------	-------------------

Wild Card Characters	Description
I	Logical OR.

6.3 Sample Search Queries

The following tables lists a few samples search queries for your reference:

Table 3: Sample Search Queries

Query	Description
user:johnsmith url:www.americanexpress.com	Searches the Username field for johnsmith and the URL field for www.americanexpress.com.
user:john smith	Searches the Username field for john OR smith.
+user:johnsmith -url:www.google.com *notes:"secret note \d"	Search the username field for exactly johnsmith, the URL must not contain www.google.com, and notes contains secret note [digit].

Chapter 7: Password Generator

This password generator helps you to generate random strong passwords and paraphase that you can use for your applications and websites you visit.

7.1 Generating Passwords

To generate random passwords, specify the characters to be used in your choice of password (for example, upper-case letters, digits, special characters, and so on) and KeePassXC will randomly pick characters out of the set.

To generate the random password using Password Generator, perform the following steps:

- 1. Open KeePassXC.
- 2. Navigate to Tools > Password Generator. The following screen appears:

€ KeePassXC	- 🗆	\times
<u>D</u> atabase E <u>n</u> tries <u>G</u> roups <u>T</u> ools <u>H</u> elp		
🕐 🔛 🔒 💐 🖧 🌾 🏝 🗓 🥙 🏰 👘 🔒 🥕 🕋 Search (Ctrl+F)		0
Password: r98&9f.N<\')E		
		6
Password Quality: Good	Entropy: 85.41 bit	
Password Passphrase		
	13	
Length:	13 🛟	ite
Length:		ite
Length:	Regenera	ite
Length:	Advanced Copy	ite
Length:	Advanced Copy	ite
Length:	Advanced Copy	ite
Length: Character Types A-Z a-z 0-9 /* ExtendedASCII	Advanced Copy	ite

- 3. Select the length of the desired password by dragging the Length slider.
- 4. Select the character-sets that you want to include in your password.
- 5. Click the **Advanced** button to specific advanced conditions for your desired password.
- 6. Click the **Regenerate** button to generate new random password.

7. Click the **Copy** button to copy the password to the clipboard. You can then paste your password in your entry in KeePassXC and your other applications.

7.2 Generating Passphrases

A passphrase is a sequence of words or other text used to control access to your applications and data. A passphrase is similar to a password in usage, but is generally longer for added security.

To generate the random passphrase using Password Generator, perform the following steps:

- 1. Open KeePassXC.
- 2. Navigate to **Tools > Password Generator**. The following screen appears:

🕡 KeePassXC	_		×
Database Entries Groups Tools Help			
🕐 🔛 🔒 💐 🖧 🌾 🏭 🗓 🥙 🏤 😰 🔒 🥕 🔝 Search (Ctrl+F)			0
Password: r9B&9f.N<\')E			(6)
Password Quality: Good	Entropy: 8	35.41 bit	
Password Passphrase	13		
Character Types	dvanced	Regener Copy Close	

3. Click the **Passphrase** tab. The following screen appears:

€ KeePassXC		_	
<u>D</u> atabase E <u>n</u> tries <u>G</u> roups <u>T</u> ools <u>H</u> elp			
[9 🕒 🔒 < << << 🕹 🗓 🥑 🚣 🔵 🌽 🥕	Search (Ctrl+F)		9
Password: frostedstatutedesignatecozy			6
Password Quality: Weak		Entropy:	51.70 bit
Password Passphrase			
Word Count:		¥ 🛟	
Word Separator:			Deservements
			Regenerate Copy
			Close
			Close

- 4. Select the number of words you want to be included in your passphrase by dragging the **Word Count** slider.
- 5. In the **Word Separator** field, enter a character, words, number or space that you want to use a separator between the words in your passphrase.
- 6. Click the **Regenerate** button to generate new random passphrase.
- 7. Click the **Copy** button to copy the passphrase to the clipboard. You can then paste your passphrase in your entry in KeePassXC and your other applications.