CENTER FOR
SECURITY STUDIES
& CYBER DEFENSE

How To Use a Password Manager

Written By: AUCSSCD Student Intern

Who wants a secure password
Who wants to remember their secure password
imgflip.com

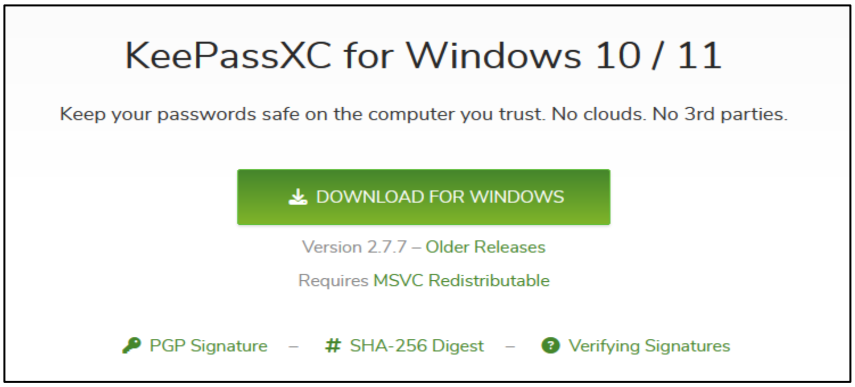
Nobody wants to remember strong passwords. As much as we all want to stay safe online it is just not easy to remember 7 different 20-character long passwords just to check your email address. This is what password managers are for.

- A password manager is a program that keeps all of your passwords encrypted by a single password.
- Certain password managers have extra features such as auto-filling inputs in websites, storing passwords on the cloud, and the ability to store files behind a single password as well.
- There are lots of good password managers out there but my personal recommendation is the KeePassXC password manager. I prefer KeePassXC because its autofills inputs on websites and has the ability to store things like images of passports. It also is a fully featured password manager that does not store passwords on the cloud, which is important to me because I like having control over who has access to my passwords. If you are curious about how to use KeePassXC, this guide will explain how.

1) Download

KeePass has versions that work on almost any platform or operating system, all of these can be found on the KeePassXC download page. This guide will assume that you are using Windows as that is the most common OS but know that Mac, and Linux users all should be able to use KeePassXC.

a) First click the download button

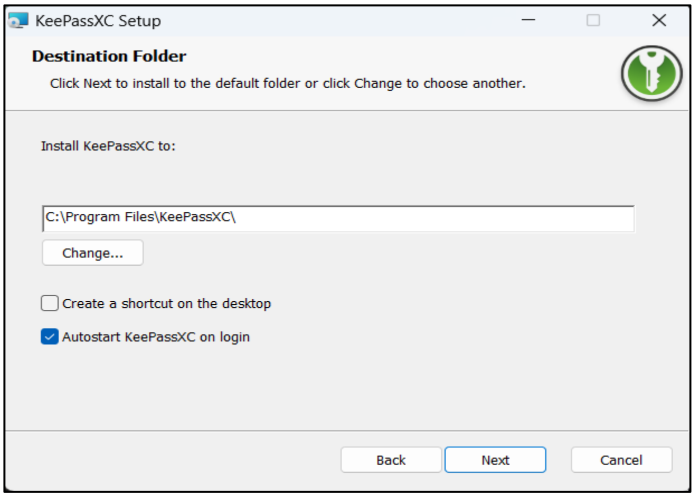


KeePassXC for Windows 10 / 11

Keep your passwords safe on the computer you trust. No clouds. No 3rd parties.

DOWNLOAD FOR WINDOWS
Version 2.7.7 – Older Releases
Requires MSVC Redistributable
PGP Signature – # SHA-256 Digest – Verifying Signatures

b) Accept the license agreement and then select a file location to store KeePass. If you don't know what to do with this the default option should be ok, you can also choose to enable AutoStart on login and create a desktop shortcut.



KeePassXC Setup

Destination Folder

Click Next to install to the default folder or click Change to choose another.

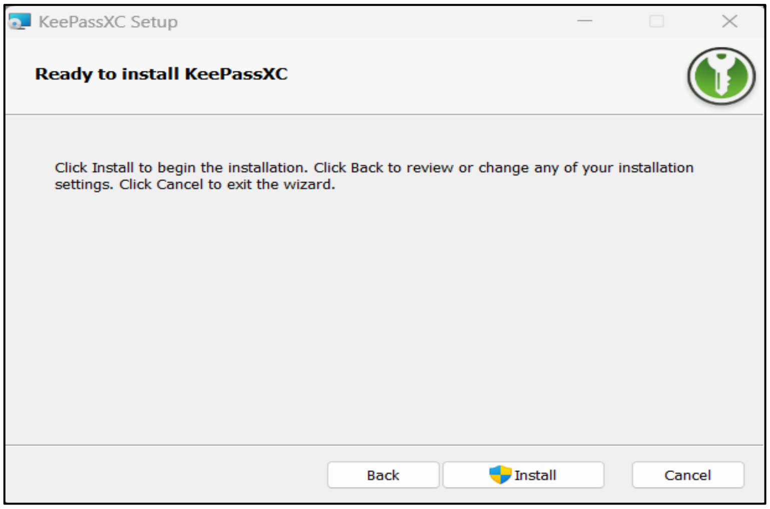
Install KeePassXC to:

C:\Program Files\KeePassXC\

☐ Create a shortcut on the desktop

☑ Autostart KeePassXC on login

c) The next section just confirms your installation so click install.

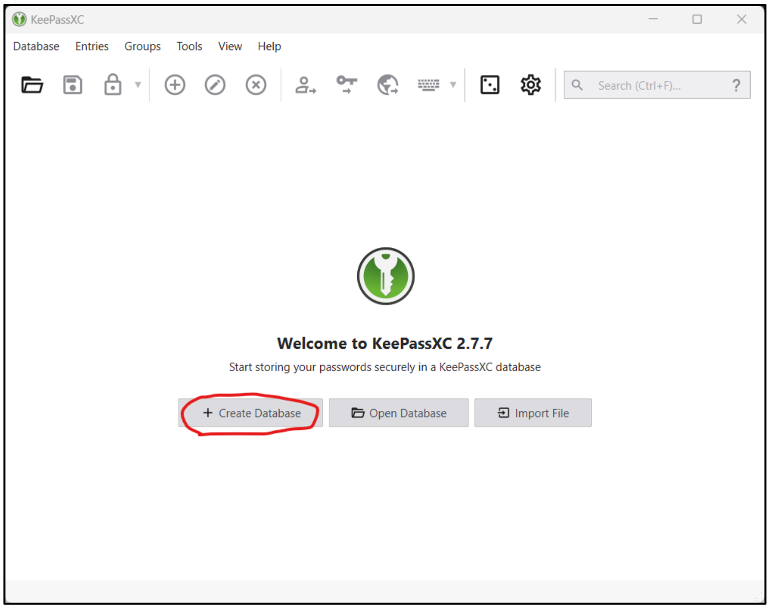


Ready to install KeePassXC

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

2) Create a Database

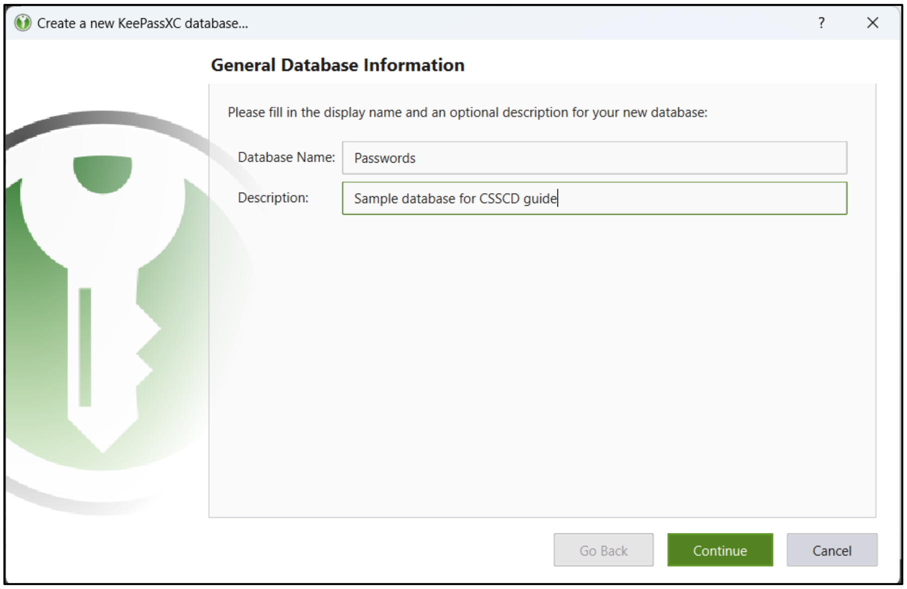
a) When launching KeePass for the first time you should see the following screen. The first step is to set up a database in order to store all of your passwords. To do so first, select this button to create a new database.



Welcome to KeePassXC 2.7.7

Start storing your passwords securely in a KeePassXC database

b) Doing so will prompt you to add a database name and a description.



Create a new KeePassXC database...

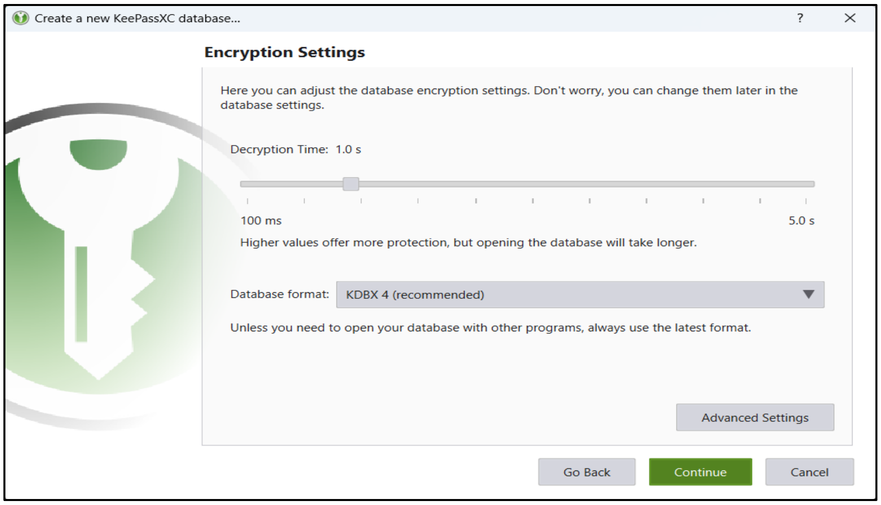
General Database Information

Please fill in the display name and an optional description for your new database:

Database Name: Passwords

Description: Sample database for CSSCD guide

c) The next section will give you more control over how the database is encrypted, most likely the default database format should be fine. You can also slide the decryption time slider to control how long it takes to decrypt your database once you put in the password, higher time is more secure but will be more annoying when decrypting.



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

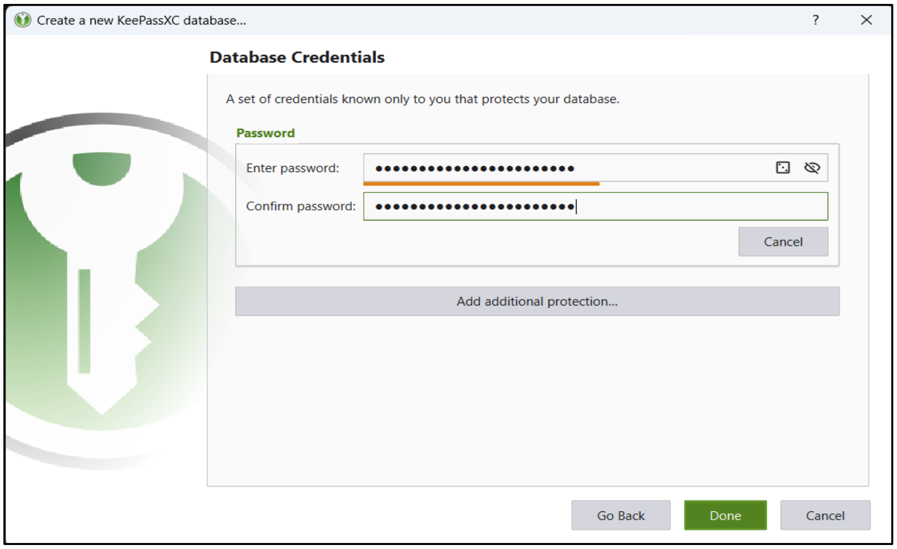
Higher values offer more protection, but opening the database will take longer.

Database format: KDBX 4 (recommended)

Unless you need to open your database with other programs, always use the latest format.

d) KeePass will then prompt you to create a Master Key for your new KeePass database. ***Please make sure that you can remember this password because if it is forgotten your passwords will be unrecoverable***

e) This is also where you can set up a key file if you wish by selecting show expert options but this guide will not go into this option.



Create a new KeePassXC database...

Database Credentials

A set of credentials known only to you that protects your database.

Password

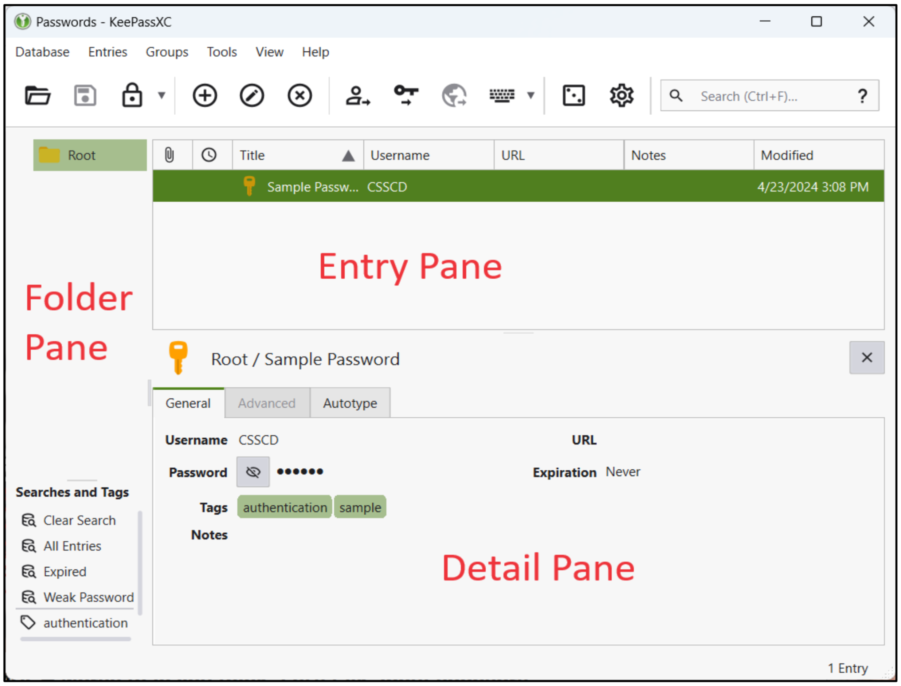
Enter password: ••••••••••••••••••••••

Confirm password: ••••••••••••••••••••••

f) The next section will ask you where you would like to save your database file. I would recommend creating a new folder for your database files so that you can easily find them and move them to other devices if necessary.

3) Add entries

a) Once your new database is created you will see a new UI, there are three main parts of this UI: The entry pane, the folder pane, and the details pane. I have added a sample entry into this database to show how each pane works. The folder pane is where you can add folders to organize your passwords, do this by right clicking in the folder pane and selecting “new group”. The entry pane shows each entry in the selected folder. The detail pane shows the details of the currently selected entry.



Title	Username	URL	Notes	Modified
Sample Passw...	CSSCD			4/23/2024 3:08 PM

Root / Sample Password

Username CSSCD

Password ••••••

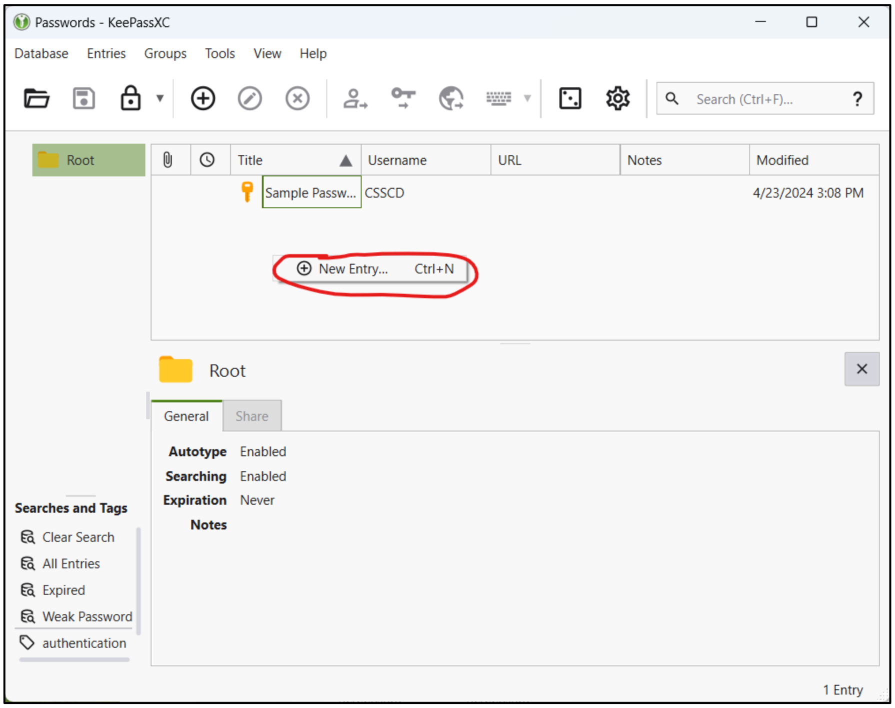
Tags authentication sample

Notes

URL

Expiration Never

b) Now let’s learn how to create our own entries, start by navigating to the folder you want to save the password in and right click anywhere in the password pane, from here you can select a new entry.



Title	Username	URL	Notes	Modified
Sample Passw...	CSSCD			4/23/2024 3:08 PM

Root

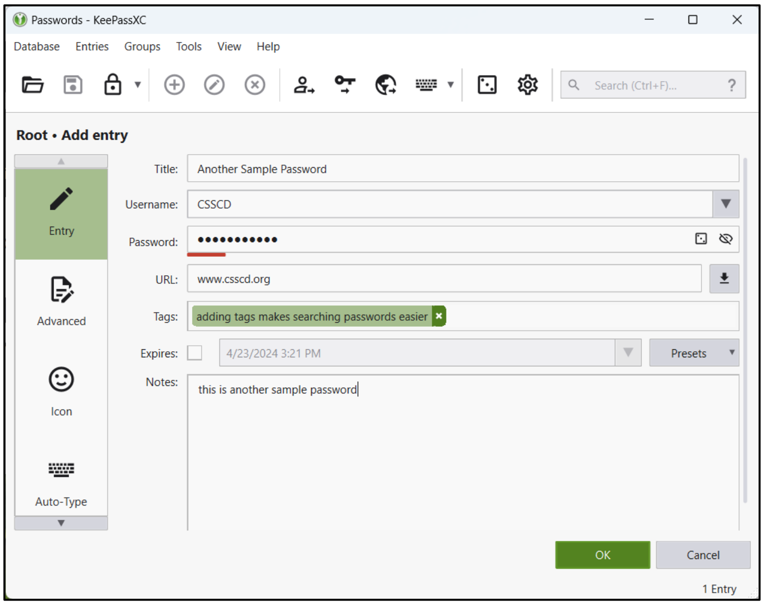
Autotype Enabled

Searching Enabled

Expiration Never

Notes

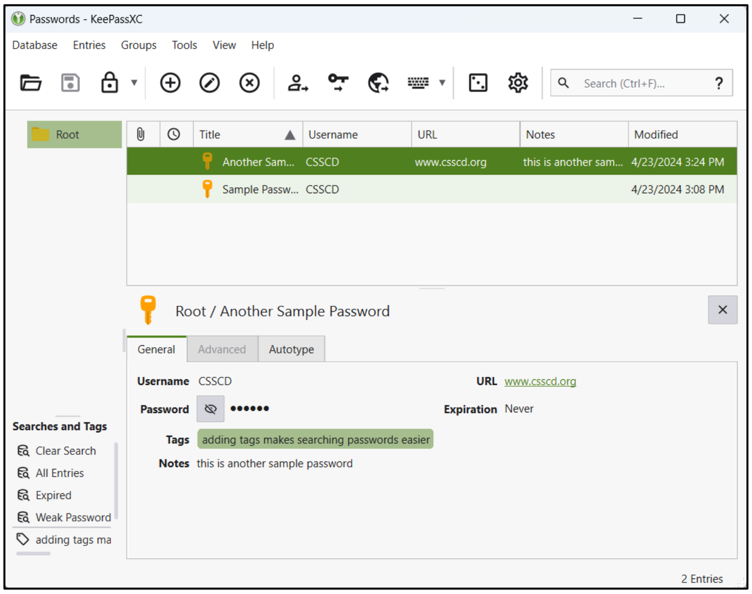
c) From here you can add attributes such as a title, username, url, notes, tags, and an expiration date. It will automatically generate a secure password for you but this can be overwritten if you choose, you can also use the dice icon to have it generate a new password for you.



Root • Add entry

Title:	Another Sample Password
Username:	CSSCD
Password:	•••••••••••
URL:	www.csscd.org
Tags:	adding tags makes searching passwords easier
Expires:	□ 4/23/2024 3:21 PM
Notes:	this is another sample password

d) Select OK when you finish and you should be able to see your new information in the password menu.



Title	Username	URL	Notes	Modified
Another Sam...	CSSCD	www.csscd.org	this is another sam...	4/23/2024 3:24 PM
Sample Passw...	CSSCD			4/23/2024 3:08 PM

Root / Another Sample Password

Username CSSCD URL www.csscd.org

Password •••••• Expiration Never

Tags adding tags makes searching passwords easier

Notes this is another sample password

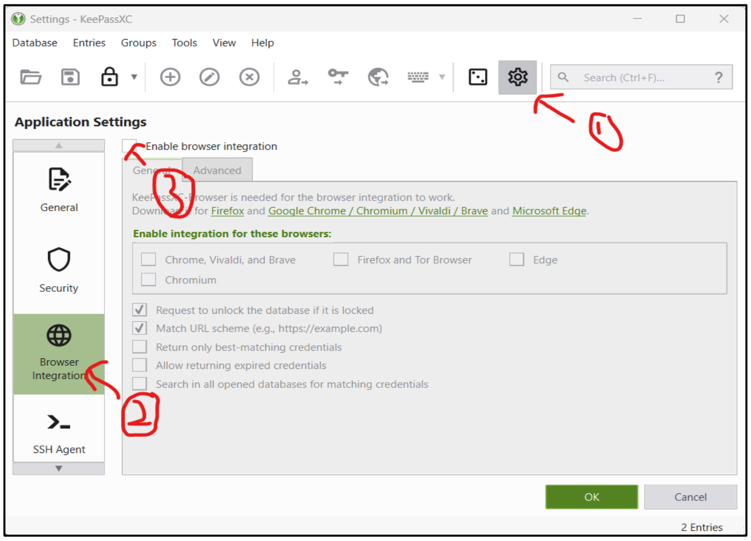
e) Bonus tip: by right clicking on a password entry you can select Copy Password and it will copy the password to your clipboard for 12 seconds giving you some time to paste it in wherever you need it.

4) Enable Auto-fill

One common feature to enable with any password manager is enabling it to integrate with your browser to auto-fill passwords on websites you visit. In order to use this feature, your password entries must include a URL field with the location you want to autofill the passwords but remember you can go back and add one now if you haven't already. It is also necessary that you keep your KeePass database open and unlocked when browsing for this feature to work, if needed KeePass can be configured to automatically start up when you log into your computer.

a) First you will need to get the KeePass browser extension for your chosen browser ([Firefox](), [Chrome](), [Edge]()). You will notice that once downloading the extension KeePass will not be able to sync to it just yet.

b) In order to integrate the browser plugin in KeePassXC, first click on the settings gear above your database, then click Browser Integration, and select the check box that says Enable Browser Integration



Application Settings

□ Enable browser integration

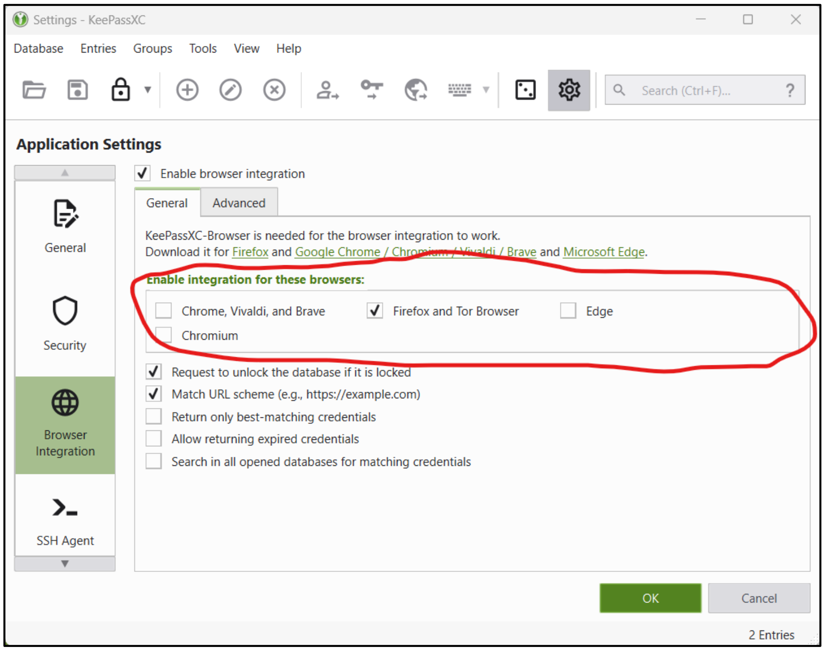
KeePassXC-Browser is needed for the browser integration to work.
Download it for Firefox and Google Chrome / Chromium / Vivaldi / Brave and Microsoft Edge.

Enable integration for these browsers:

□ Chrome, Vivaldi, and Brave □ Firefox and Tor Browser □ Edge
□ Chromium

☑ Request to unlock the database if it is locked
☑ Match URL scheme (e.g., https://example.com)
□ Return only best-matching credentials
□ Allow returning expired credentials
□ Search in all opened databases for matching credentials

c) Next select which browsers you will be integrating and select OK



Application Settings

☑ Enable browser integration

General | Advanced

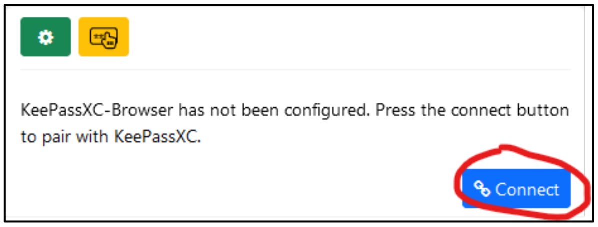
KeePassXC-Browser is needed for the browser integration to work.
Download it for Firefox and Google Chrome / Chromium / Vivaldi / Brave and Microsoft Edge.

Enable integration for these browsers:

☐ Chrome, Vivaldi, and Brave ☑ Firefox and Tor Browser ☐ Edge
☐ Chromium

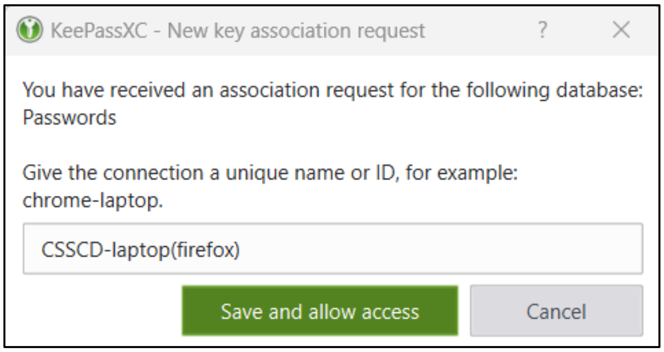
☑ Request to unlock the database if it is locked
☑ Match URL scheme (e.g., https://example.com)
☐ Return only best-matching credentials
☐ Allow returning expired credentials
☐ Search in all opened databases for matching credentials

d) Now in your browser you can click the extension and click reload. Now you will have the option to connect the extension to KeePassXC



KeePassXC-Browser has not been configured. Press the connect button to pair with KeePassXC.

e) Next you will need to add a unique identity for the browser you are setting up and select Save and allow access

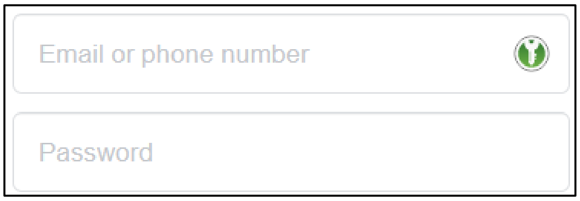


You have received an association request for the following database:
Passwords

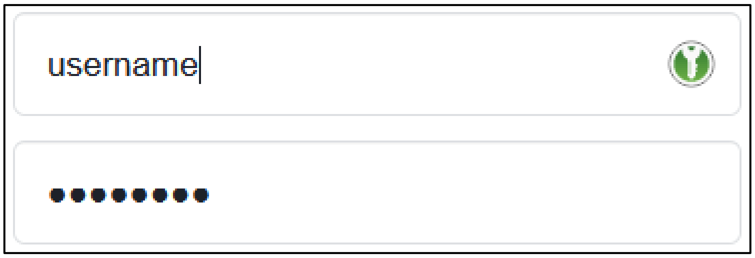
Give the connection a unique name or ID, for example:
chrome-laptop.

CSSCD-laptop(firefox)

f) Now as long as your database has a username and password associated with your URL this icon will appear in the login fields. (if the icon is grayed out you may need to check your KeePass application and allow the website to access the entry in the pop-up window)



g) Clicking the icon should immediately fill in the login fields with your information



username

••••••••