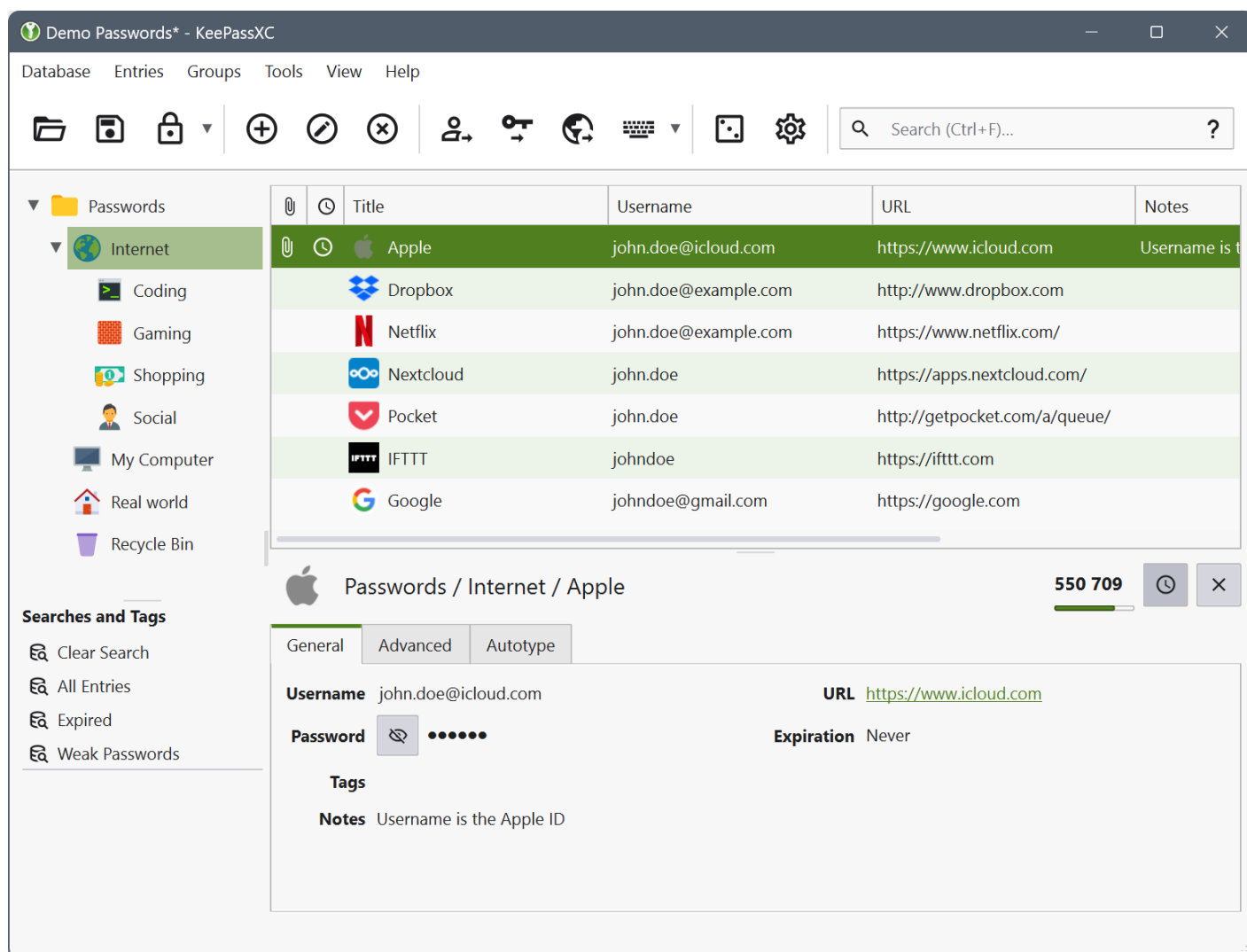
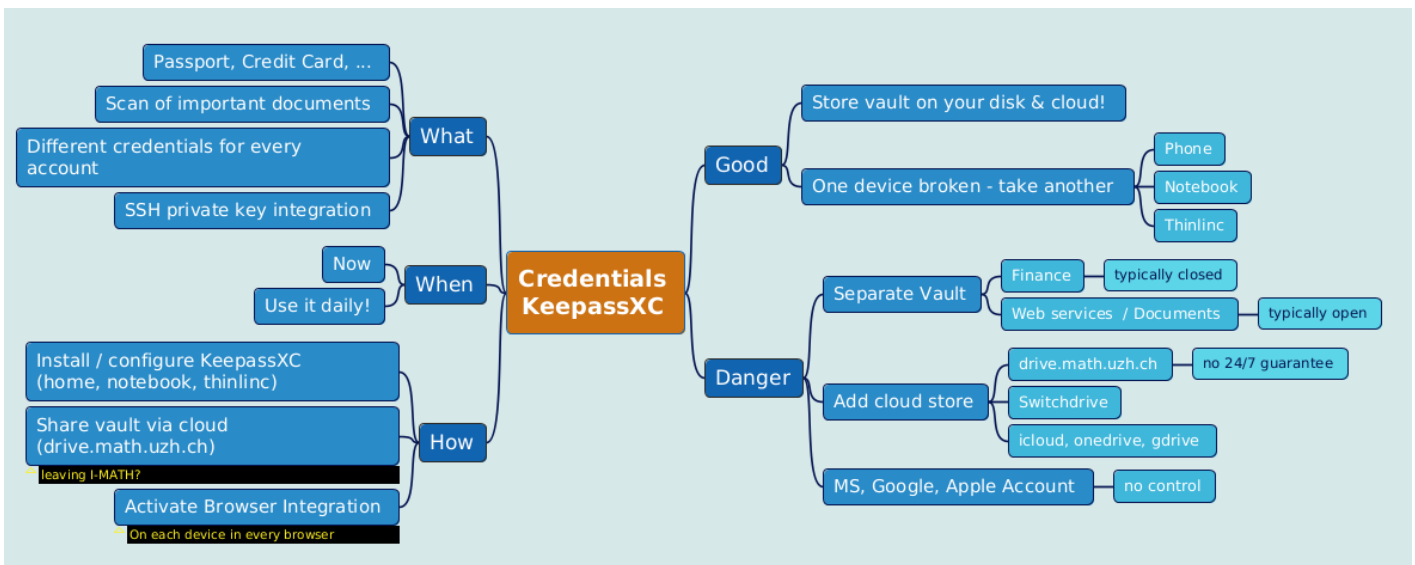


KeePassXC

- [Download](#)
- [Basics](#)
- [Background information](#)

An easy-to-use, cross-platform password manager with browser integration, strong encryption, zero cloud breach risk, and open-source transparency. You remain in full control of your data, because the vault is just a file. Do whatever you want with it. It is strongly encrypted, allowing you to sync it via the cloud provider of your choice. Because the format is open source, you will never lose access to your identities due to corporate mishaps, vendor lock-in, or a company shutting down.





Features

- Makes using secure passwords very very easy. The days of saving your password in an apple notes or docx file are OVER!
- Different passwords for different accounts - one get's hacked, no problem, others still save!
- Awesome browser integration! Even on mobile! Disabling your browser's password saving feature is a big security increase, as browser have a large attack surface.
- First class MFA/2FA and passkey integration, including mobile. Logging in with 2FA has never been faster.
- Open, post-quantum resistant file format.
- Apps for Android (KeepassDX) and iOS (Keepassium) - sync your vault file over all your devices with the cloud you already use.
- No single device dependency. Your passwords are wherever you sync them to (including your TOTP tokens!)
- No vendor-lock-in, no proprietary formats being discontinued in ten years, no trust issues whatsoever.

For Teams / Orgs:

- Security levels can be split into multiple vaults / files.
- This allows easy credential sharing between hierarchichal work groups.

Install

- MacOS/Windows/Linux - KeePassXC: <https://keepassxc.org/>.
 - For Windows please observe the requirement for [MSVC Redistributable](#) to be installed

- Android: [KeepassDX at Google Play Store](#)
- iOS - [Keepassium at Apple Appstore](#)

What it does

- KeePassXC creates/opens/edits and saves password-vaults as a single, AES-256 or Twofish-256 encrypted .kdbx-file
- You can store your various usernames/passwords/URLs and also attachments like pictures or other important / private documents.
- Encryption happens via a key which is derived from a master password that you can change at any time. Additional authentication factors are also possible. (But a strong master password of >12 mixed characters is usually enough.)
- Remember the master password well. In practice, you enter it everyday (depending on your settings), so complete loss of access is very unlikely.
- All features: <http://www.keepassx.org/features/>

Creating a Password Vault

- Click on "File" --> "New Database..."
- You will be prompted to set a master key. Input your master password (the master password for all your other stored passwords). Then click "OK"
- Repeat your master password. click "OK".
- Chose a group. (Standard choices are Internet of eMail. You can also create your own groups).
- Click on "Entries" --> "Add New Entry..."
- Input the information you need
 - Title: a short description of the entry
 - Username: your username
 - URL: on what homepage do you need the password (more urls can be added in the side tab *Browser Integration*)
 - Password: your password - you can also let KPXC generate one for you. Do not go overboard with this, 24 latin characters, numbers and 'common' special chars are enough. Though unlikely, you should still be able to enter the password with a normal keyboard. (So avoid accented characters etc).
 - Comment: a longer description of the entry. Make good use of this, it's very useful, because you might forget that a certain online service only required you to enter your email and no password. Note it down, so you won't be confused in 6 months when you see an empty password field.
- Click on "File" --> "Save Database"
- Chose a location and a name for your password database. click "OK"

Sync Your Vault: Sovereignty Over Convenience

Password management truly shines when your credentials are available on all the devices you need them on. To achieve this, you must sync your `.kdbx` database file across these devices. *The security of this process depends entirely on where you store that file.*

The Recommended Path: Sovereign Cloud Storage

For maximum data sovereignty, use trusted, non-US infrastructure. We recommend:

- I-MATH / DM3L Drive: drive.math.uzh.ch
- Switch Drive: drive.switch.ch (Swiss Education Cloud)

Why Avoid US-Based Giants? (Google, Dropbox, Apple, Microsoft)

While your `.kdbx` file is strongly encrypted, metadata and access patterns are not. Relying on US-based providers introduces critical risks:

1. Legal Surveillance: Since the Snowden revelations, it is confirmed that US intelligence agencies (like the NSA) have legal pathways to compel US companies to hand over user data. Often, the company is not even allowed to tell you that they handed over your data.
2. High-Value Targets: These massive platforms are the primary targets for state-level actors and sophisticated hackers, increasing the likelihood of a breach.
3. Data Sovereignty: Storing confidential data on servers subject to the US CLOUD Act means you effectively lose control over who can access your data, regardless of your encryption.

Rule of Thumb: Never store confidential data on infrastructure hosted by or subject to US jurisdiction.

The Trade-Off: To Cloud or Not to Cloud?

Pros of Cloud Sync

- Ubiquitous Access: Your entire identity is available on every device instantly.
- Implicit Redundancy: The cloud acts as an automatic, off-site backup, protecting against local hardware failure.

Cons of Cloud Sync

- Expanded Attack Surface: Your encrypted vault exists on multiple endpoints. If *any* single device is compromised, the vault is exposed.
- Provider Risk: If the cloud provider is breached or legally compelled to hand over data, attackers obtain your encrypted vault file. While they cannot read it without your master password, they possess the target indefinitely for offline brute-force attacks.

Verdict: Syncing is essential for usability, but only if you retain control over the infrastructure. Choose a sovereign provider to ensure that even if the server is accessed, your data remains under your legal and technical protection.

Sync Strategy: Nextcloud

Configuration: Store your vault at e.g. `Nextcloud/Passwords/Passwords.kdbx`. Install the [Nextcloud client](#) on your devices and open the database directly from the synced local folder with KeePassXC.

How it works:

- Automatic Synchronization: The Nextcloud client keeps the `.kdbx` file updated across all devices. KeePassXC monitors the file for external changes and reloads automatically.
- Conflict Resolution: If multiple devices modify the vault simultaneously, KeePassXC automatically merges the changes upon saving, preventing data loss or version conflicts.
- Team Usage: Multiple users can share the same file via a shared Nextcloud folder. Concurrent edits are merged seamlessly, eliminating the need for manual file exchanges or locking mechanisms.

This approach ensures a single, up-to-date vault across your infrastructure while maintaining full control over the storage location.

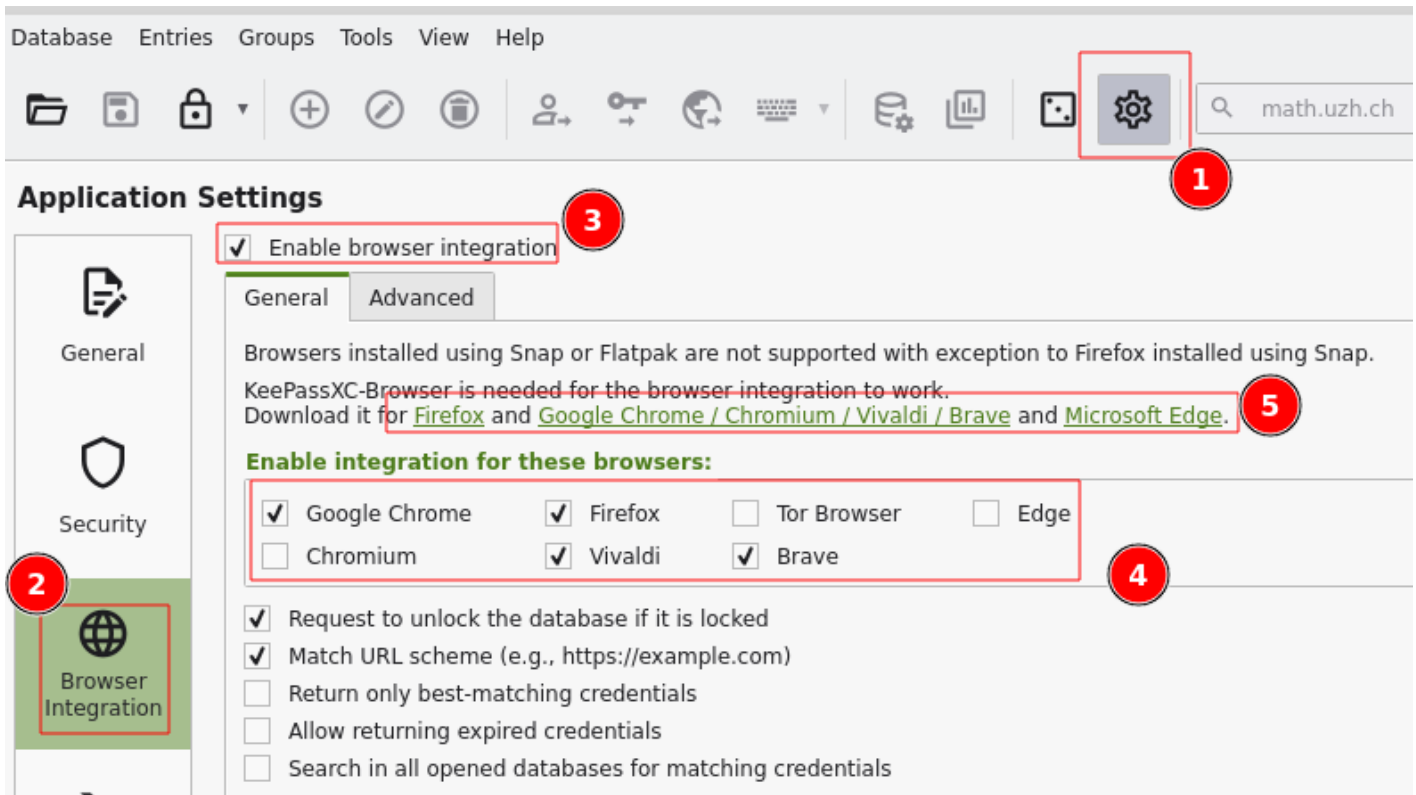
Browser integration / MFA Setup / Passkeys

- KeePassXC can be used from within a browser (Chrome, Chromium, Firefox, Vivaldi, Brave, ...)
- Browser connection to KeePassXC is nice: different browsers offer the same accounts/credentials - and if synced via cloud also on different computers.
- TOTP service (one time token)
- Passkeys
- Again, think on this: There is only one source of truth (=one KeePassXC vault), in all browsers you have all your credentials available.

Finally:

- **no more MS-Authenticator app needed**
- **no more single device dependency** (Phone at home, ...)
- **login to any MFA protected website without a mobile phone** - Biggest advantage: your second token are controlled by you, not any provider.
- **still secure** - the second factor is now your KeePassXC.

Settings



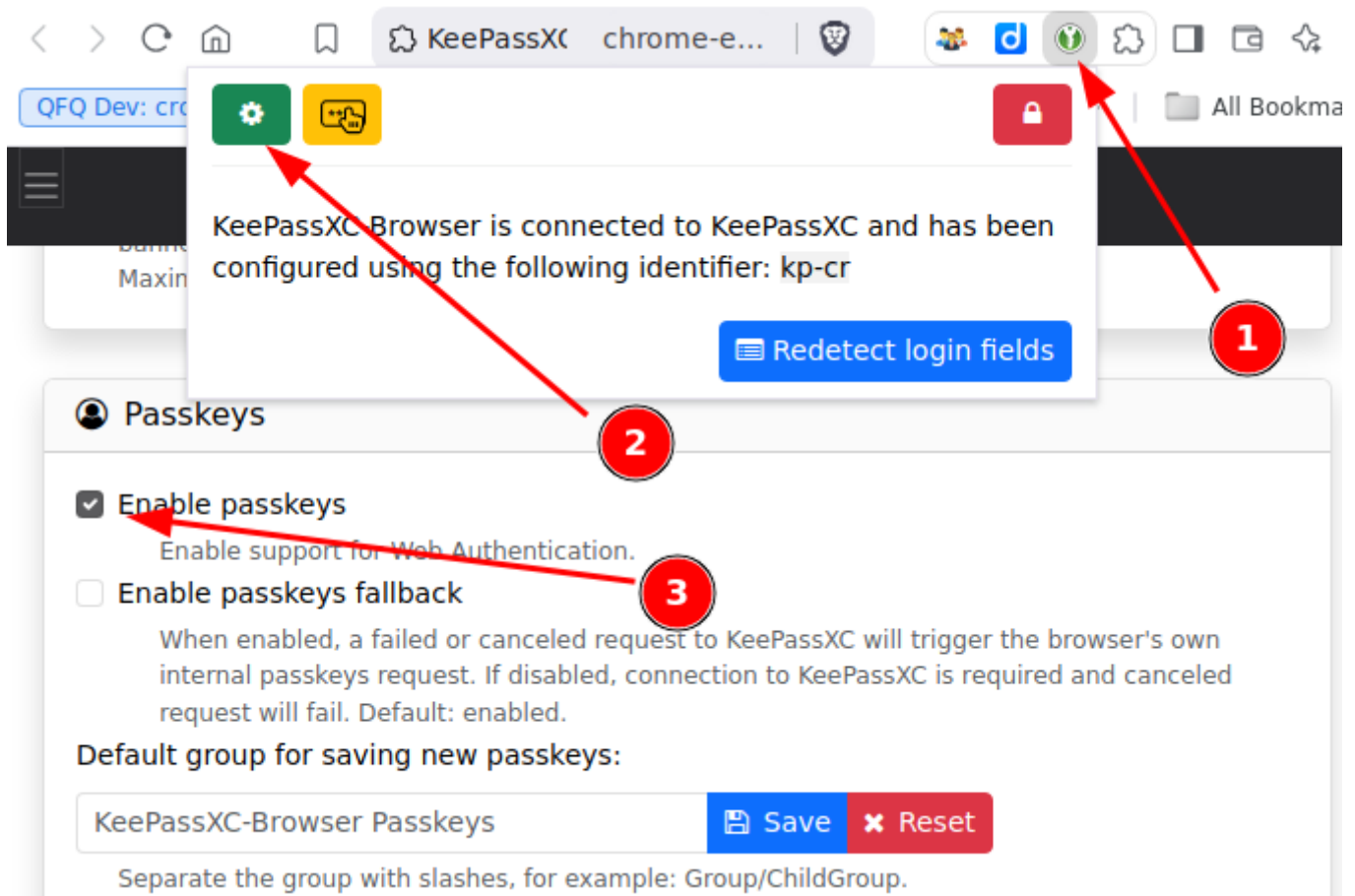
- Settings > Browser Integration > Enable integration ...: Chrome, Firefox, ...

Browser Plugin

- Install the corresponding browser plugin (links to app store: check above the settings dialog '5')

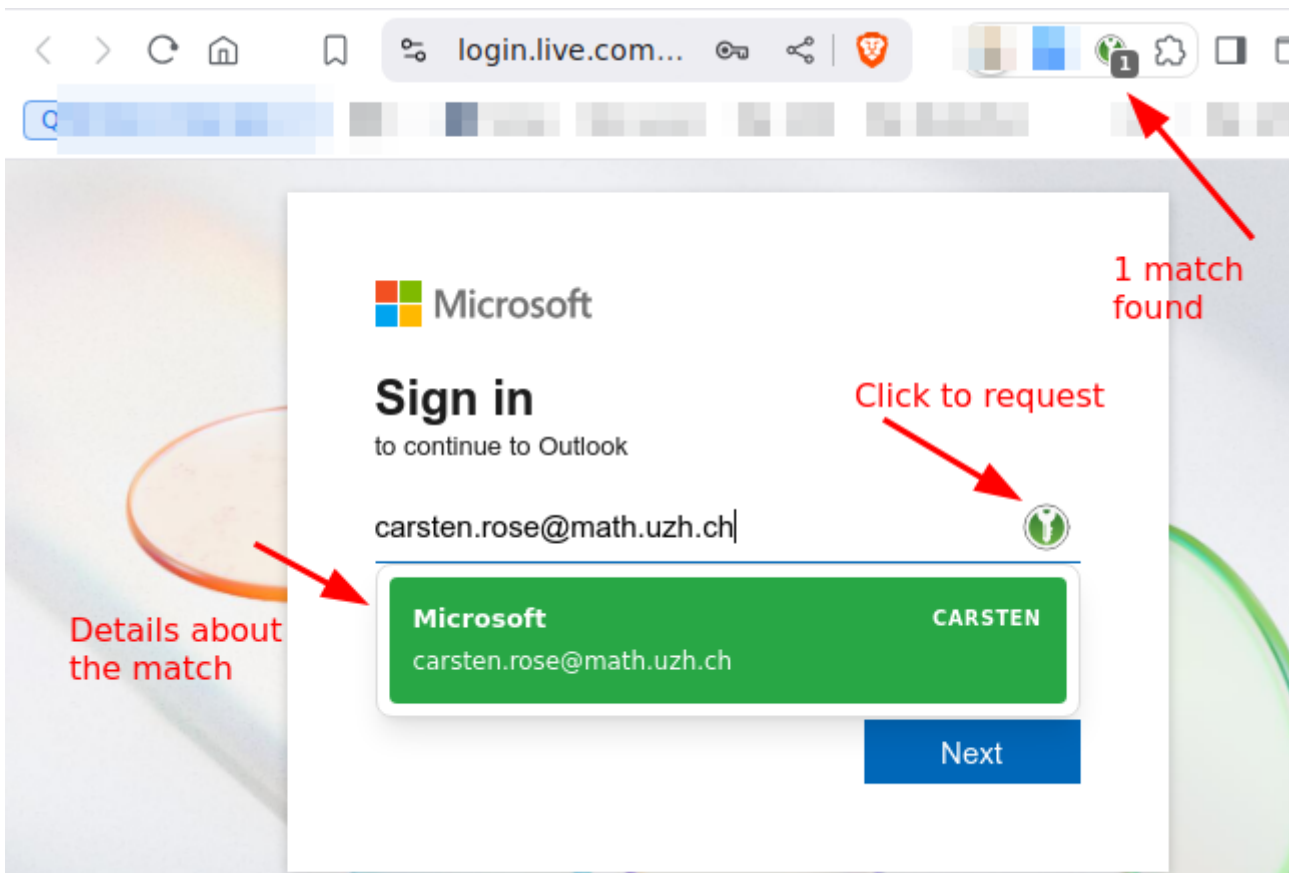
Option: Passkeys

- Passkeys have to explicitly enabled in the browser plugin:



Regular Username / Password

- Take care that the KeePassXC icon on the top right is 'green' = connection to vault is active.
- Open the login page in the browser.

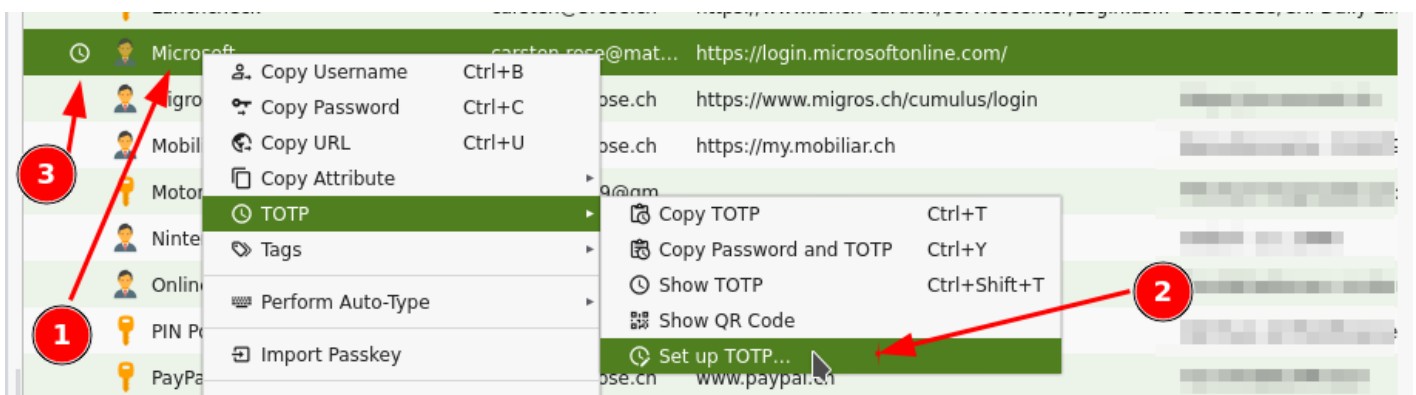


- Click on the small green kp icon.
- Choose the account.

MFA

TOTP

- To use TOTP with Microsoft Office 365 login: Add another (than MS-Authenticator-) app, as second factor [How To](#)



- Add [TOTP](#) functionality to individual accounts: Account > right mouse click > TOTP > Setup TOTP

- On a MFA-TOTP secured login website, just login as usual with KeePassXC, on the next page, where the one time token is requested, click again on the green symbol.

Hint:

- On the `TOTP setup` you have to provide the 'shared secret'.
- The shared secret is provided by the website which hosts the login, typically where the MFA can be configured.
 - Either in plaintext like 'ABCD EFGH 1234 IJKL 5678 MNOP QRST UV89'.
 - As a QR code to scan.
 - Here sometimes it's a URL or a `fido` string.
 - If it is not in plaintext in the URL, hopefully the assigned app (=keepassdx) opens.
 - Option: be creative - scan the QR, look at the url (or send the URL via 'share' to yourself): you should see the shared secret as an argument in the URL.

Passkey

- [Passkey / webauthn](#) are offered as an additional way to use MFA.
- Passkeys are significantly more secure than MFA via a) email code or b) One Time Token, c) Authenticator App, cause they use pairing between store and the application.
- But: Some websites work better than others. E.g. eduid.ch is ok, gitlab is ok but with popup, Microsoft is broken for Linux/Chrome/KeePassXC, ...
- The pairing is also a disadvantage: you need different keys for each store. Sure, KeePassXC acts like 'one store'.
- Logging to a passkey secured application only works with a running passkey device / software.
 - In contrast: TOTP is fine if you get the code from your Mobile/Keepass App and type it in a browser on a computer.
- Using passkeys is recommended, but only after you got experience with KeePassXC and the corresponding browser plugin.

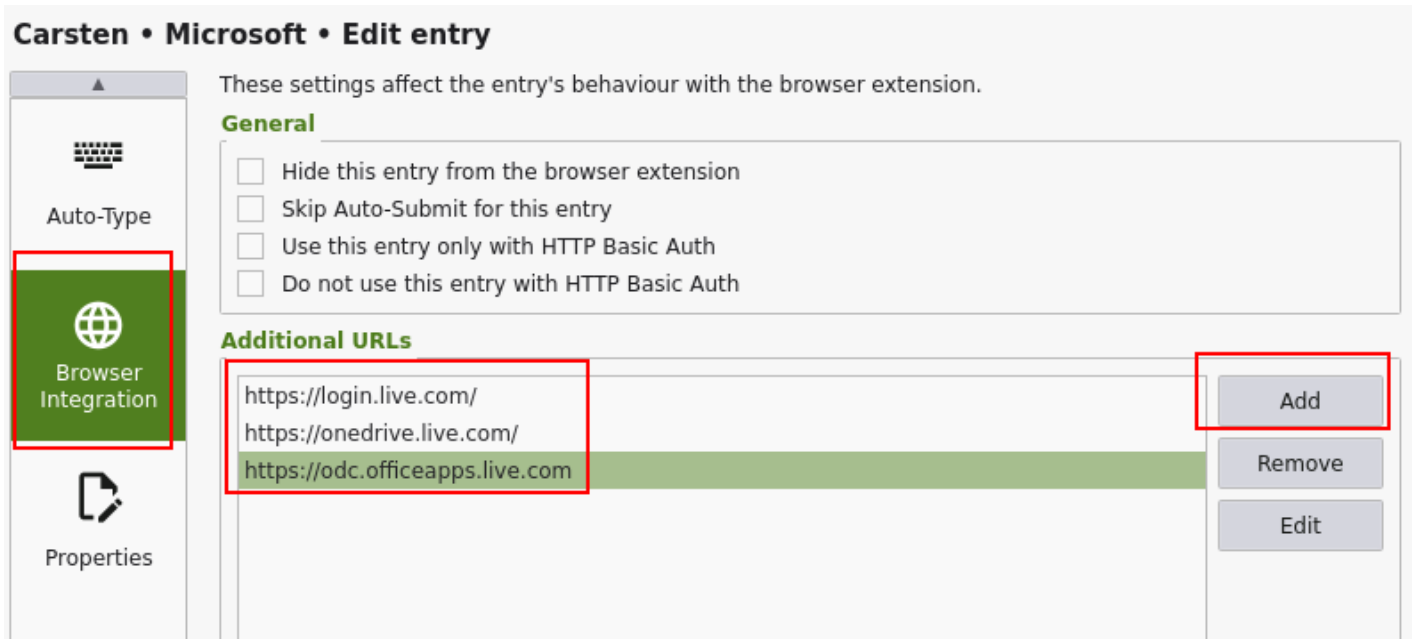
Recovery Keys

- Some services offer recovery keys.
- Copy the keys in corresponding account record in KeePassXC.
- If you used a key (it's burnt now), remove it from the list (if there was only one key, update it with the new one).

Same account / different URLs

- Some services, e.g. Microsoft (<https://login.live.com/>, <https://login.microsoftonline.com/>, <https://onedrive.live.com/>, <https://odc.officeapps.live.com/>), use a million different URLs to login. No problem.

- Don't make new KPXC entries, just add the additional urls to the *Additional URLs* section in the *Browser Integration* tab in the main Entry (e.g. your "Microsoft" entry)



- This is very **powerful** - add as many URLs you like to the same account record - the helps to keep your vault clean!

```
https://odc.officeapps.live.com
https://onedrive.live.com/
https://login.live.com/
```

Problems

Brave: No connection

If connection to KeePassXC fails after (re)starting Brave:

- In KeePassXC open `Settings > Browser Integration > Enable integration for there browsers: Off & On`

Brave: Plugin spinning wheel turns all the time, no connection

Option 1

- Quit Brave.
- Optional: Check that there are no leftover processes.
- Check if keepassx gets a connection.

- No? **Repeat** the quit/restart at least **4 times** - answer question like 'Restore pages' or 'Profile broken' (than quit). ... *makes no sense, right? Try it!*

Option 2

- Open the keepassx plugin options page.
- Change a setting.
- Close the tab.
- Open the keepassx plugin options page again.
- Is the setting still the one you choosed before?
- No: exit Brave (check that all processes are closed).
- Repeat the test - up to 3 times!!!

Option 3

- In Brave: **Remove extension keepassxc plugin.**
- Quit Brave.
- **Check that really all brave processes are quit:** `ps -ef | grep brave | grep $USER`
- **Clean tempfiles:** `\rm -R /tmp/.cache-$USER/BraveSoftware`
- Start Brave again.
- Install Brave plugin `keepassxc`.
- Optional: Import Brave plugin `keepassxc` settings (export them earlier when all is fine).

Option 4

- Close all Browser: Chrome, Brave, Firefox, Teams [PWA], Spotify [PWA]
- Close KeepassXC
- `for II in keepassxc-proxy keepassxc brave firefox chrome; do pkill $II; pkill -9 $II; done`
- ☐ **Start** and **quit** brave
- Start KeepassXC
- Start brave.
 - If necessary, remove keepassxc plugin and reinstall.
 - Connect to KeepassXC

Android: KeePassDX

- [Setup](#) the cloud service (e.g. Nextcloud).
- Install Nextcloud: <https://play.google.com/store/apps/details?id=com.nextcloud.client>
 - On the file `Passwords > Passwords.kdbx` set via *three dot menu* > **synchronize**
- Install: <https://www.keepassdx.com/>
 - Open KeePassDX
 - Choose `open existing database` and select `Nextcloud > Passwords > Passwords.kdbx`

- To unlock KeePassDX via fingerprint, check

<https://github.com/Kunzisoft/KeePassDX/wiki/Device-Unlocking>

- To use the Android virtual keyboard to fill in a password on a website, activate in Android

Settings > Password, Passkeys, ... > Preferred Service: KeePassDX

12:44

90%

← **Passwörter, Passkeys &...** 🔍 ⓘ

Wähle den Dienst aus, in dem Anmeldedaten und Autofill-Vorschläge gespeichert werden sollen („Bevorzugter Dienst“). Wenn auch andere Dienste Vorschläge liefern sollen, kannst du sie unter „Weitere Dienste“ aktivieren.

Bevorzugter Dienst



KeePassDX

Passkeys, Anbieter für das automatische Ausfüllen von Anmeldedaten

Ändern

Öffnen

Weitere Dienste



Microsoft Authenticator



Google

Google Passwortmanager, Google Pay, Google Wallet



Browser integration

- Chrome based browser: Settings > Autofill-Services > Autofill with other Services
- Firefox: Not necessary

TOTP

- Android Autofill should be assigned to KeePassDX (see above)
- Google Chrome based browser: select Autofill: System Services
- Open webpage with login page: after a short moment, you'll see in the virtual keyboard all matching entries. Select the corresponding.
 - Hint: not all websites offers autofill integration for TOTP - e.g. <https://login.microsoftonline.com/> regular has problems (depending on time and moon phase).
 - Alternative: Switch keyboard to 'Magic Keyboard' - <https://txtechnician.com/blog/tech-tips-2/how-to-use-keepassdx-magic-keyboard-for->

iOS: KeePassium

- Install Nextcloud: <https://apps.apple.com/us/app/nextcloud/id1125420102>
- Install: <https://keepassium.com/>
- Activate to be used as source:



Automatisch ausfüllen & Passwörter

Passwörter und Passkeys automatisch ausfüllen



Passwörter, Passkeys und BestätigungsCodes werden bei der Anmeldung in Apps und auf Websites automatisch vorgeschlagen.

QUELLE:



Passwörter

Passkeys, Passwörter und Codes



KeePassium

Passkeys, Passwörter und Codes



Authenticator

Passkeys



BESTÄTIGUNGSCODES

Nach Nutzung löschen



Lösche BestätigungsCodes nach der Nutzung automatisch aus „Nachrichten“ und Mail.

Codes konfigurieren in



Passwörter 

Passwörter wird verwendet, um Links zum Einrichten von BestätigungsCodes und QR-Codes zu öffnen.

Revision #14

Created 2026-06-30 10:54:52 CEST by admino

Updated 2026-07-03 12:31:12 CEST by Jonas Valentin Rose