KeePassXC 사용하기

KeePassXC는 모든 비밀번호를 한 장소에 저장할 수 있도록 다양한 환경에서 사용되는 패스워드 매니저(비밀번호 관리 프로그램)이다. 패스워드 매니저는 강력한 비밀번호를 생성하고 저장하는 도구로, 사용자는 많은 비밀번호를 외울 필요 없이 다양한 비밀번호를 여러 사이트 및 서비스에서 사용할 수 있다. 사용자는 모든 비밀번호를 저장한 암호화된 패스워드 매니저 데이터베이스에 접속하게 하는 마스터 비밀번호 하나만 암기하면 된다.

KeePassX, KeePass, KeePass2처럼 KeePassXC와 비슷한 이름의 프로그램이 많다. 이 프로그램 중 일부는 같은 코드에 기반하지만, 나머지는 동일한 데이터베이스 포맷을 사용할 뿐이다. 본 가이드라인은 KeePassXC가 다양한 환경에서 사용되며 다른 유사 프로그램보다 좀 더 활발하게 개발되기 때문에 KeePassXC를 추천한다.

패스워드 매니저는 단일한 공격지점을 만들게 되며 따라서 악의적인 공격자의 명백한 목표물이 될 수 있다. 연구에 의하면 일반적으로 사용되는 많은 패스워드 매니저에 취약점이 존재하기 때문에, 패스워드 매니저가 당신에게 적합한 도구인지 아닌지 판단이 필요하다.

다운로드 장소 : 윈도우/맥OS/리눅스: https://keepassxc.org/download
컴퓨터 사양: 윈도우 7이상, 맥OS 10.7 이상, 리눅스 (대부분의 리눅스 배포판)
본 가이드에서 사용된 버전: KeePassXC 2.2.0 (KeePassXC는 윈도우 전용 KeePass 프로그램의 범용 버전이다.)
라이센스 : FOSS (주로 GPLv2)
참고 기사 : https://github.com/keepassxreboot/keepassxc/wiki
수준 : 초급
소요 시간 : 설치하는 데 5분, 그 이후 평생 강력한 비밀번호 이용
최종 수정일 : 2018년 4월 30일

KeePassXC 작동 방법

KeePassXC는 모든 비밀번호 목록을 저장하는 파일인 비밀번호 데이터베이스와 함께 작동한다. 이 데이터베이스는 컴퓨터 하드 디스크에 저장될 때 암호화된다. 따라서 컴퓨터가 꺼져 있을때 누군가 훔쳐가도 비밀번호를 읽을 수 없다.

비밀번호 데이터베이스는 마스터 비밀번호를 사용하여 암호화될 수 있다. 마스터 비밀번호가 다른 모든 비밀번호를 보호하기 때문에, 마스터 비밀번호를 가능한 한 강력하게 만드는 것이 중요하다.

마스터 비밀번호 사용하기

마스터 비밀번호는 열쇠와 같다. 비밀번호 데이터베이스를 열기 위해서, 정확한 마스터 비밀번호가 필요하다. 마스터 비밀번호 없이는 비밀번호 데이터베이스에 무엇이 있는지 누구도 볼 수 없다. 마스터 비밀번호를 사용하여 비밀번호 데이터베이스를 보호하기 위해선 아래의 사항을 유의한다.

- 마스터 비밀번호는 모든 비밀번호의 암호를 풀기 때문에 강력해야 한다! 추측이 어렵고 길어야 한다. 마스터 비밀번호가 길수록 특수문자, 대문자 또는 숫자를 염려할 필요가 적어진다. 따라서 마스터 비밀번호를 패스프레이즈 (비밀번호 문장)으로 만든다. 패스프레이즈는 사용자는 기억하기 쉽지만 다른 사람들은 추측하기 어렵게 여러 단어를 조합한 것이다.

- 평범하고 임의적인 단어를 사용하여 강력한 마스터 패스프레이즈를 생성할 수 있다. 특수문자와 대문자를 아무렇게나 조합하는 것보다 기억하기 쉽다. 강력한 비밀번호 생성방법을 좀 더 알고 싶다면 비밀번호 가이드인 "강력한 비밀번호 생성하기"를 참고한다.

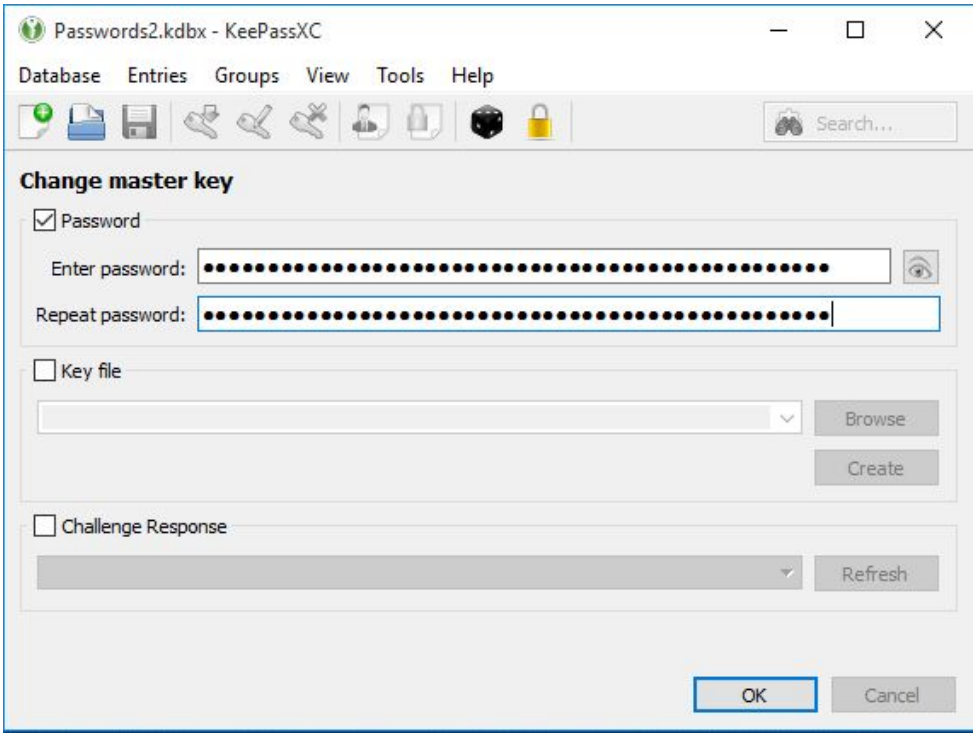
KeePassXC 시작하기

KeePassXC를 설치하여 시작한다. 데이터 베이스 메뉴를 클릭하여 "New Database(새 데이터베이스 만들기)"를 선택한다. 비밀번호 데이터베이스를 저장하라는 메시지가 뜬다. 이후 비밀번호 데이터베이스 파일을 하드디스크 또는 다른 컴퓨터로 옮길 수 있으며, KeePassXC와 마스터 비밀번호 또는 사전에 지정한 키파일(keyfile)을 사용하여 데이터베이스를 열수 있음을 명심하자.

키(key)파일이란 무엇인가? *마스터 비밀번호에 추가하여 키파일을 사용하게 되면 누군가 비밀번호 데이터베이스의 사본을 훔쳐도 암호를 푸는 것이 어려워진다. 기존의 파일을 키파일로 사용할 수 있다. 예를 들어 애완 고양이 사진을 키파일로 사용할 수 있다. 만약 키파일의 내용이 변경되면 비밀번호 데이터베이스의 암호를 푸는 키파일로 더 이상 사용할 수 없기 때문에 키파일로 선택한 파일이 수정되지 않도록 주의한다. 또한 다른 프로그램에서 키파일을 여는 것만으로도 그 파일을 수정할 수 있으므로 KeePassXC를 열 때 외에는 해당 파일을 열지 않는다. (키 파일을 옮기거나 이름을 바꾸는 것은 괜찮다.) 보통 강력한 마스터 비밀번호는 그 자체로 충분하지만, 마스터 비밀번호 외에 추가로 키파일을 사용하기로 한 경우, 이를 비밀번호 데이터베이스와는 다른 곳에 저장하도록 한다.*

이후 마스터 비밀번호를 입력하라는 명령과/또는 키파일을 사용하라는 메시지가 뜬다. 당신의 선택에 따라 적절한 체크박스를 선택한다.

입력중인 비밀번호를 (점으로 가리는 것 대신) 직접 확인하고 싶다면, 오른쪽의 눈(eye) 버튼을 클릭한다.



비밀번호 정리하기

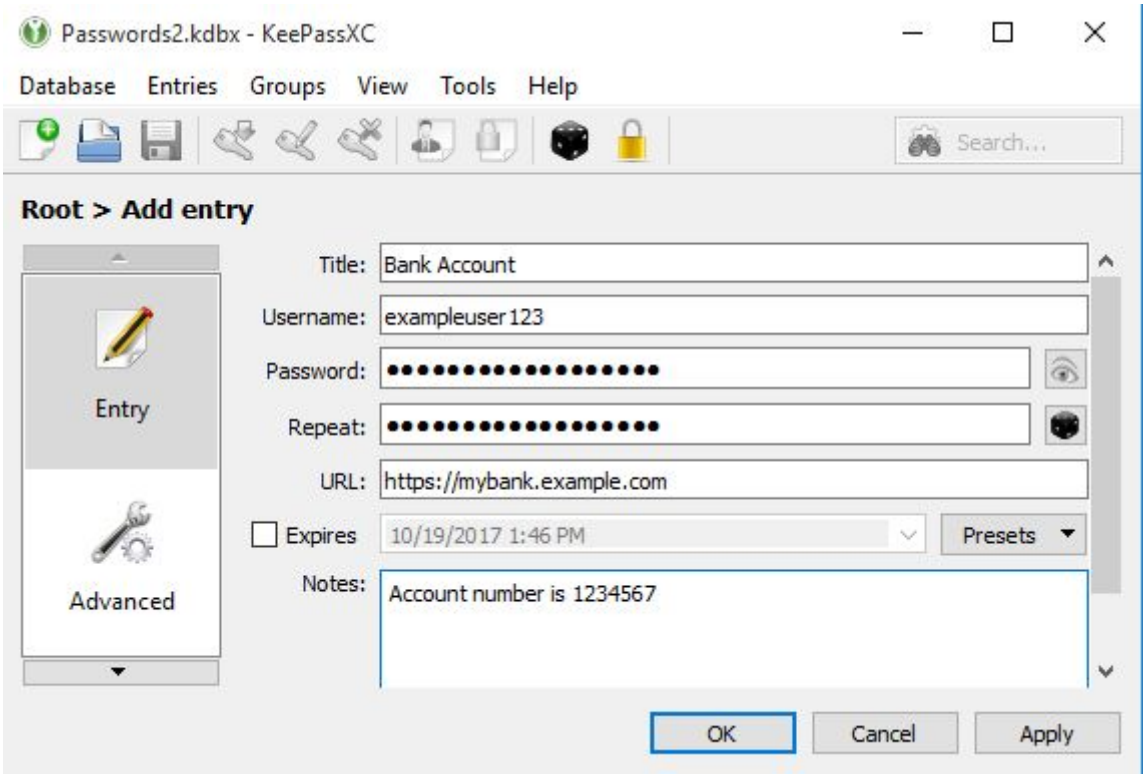
KeePassXC는 비밀번호를 폴더 형태인 “Groups”(그룹들)로 정리할 수 있도록 한다. 예를 들어 메뉴바의 "Groups” 메뉴로 가거나 또는 KeePassXC의 왼쪽창의 그룹에서 마우스 우클릭을 통해 그룹 또는 하위 그룹을 생성, 삭제, 편집할 수 있다. 비밀번호 그룹화는 KeePassXC의 기능에 어떠한 영향도 주지 않으며, 유용한 관리 도구이다.

비밀번호의 저장, 생성, 편집

새로운 비밀번호를 생성하거나, 이미 사용하고 있는 비밀번호를 저장하기 위해서는 원하는 그룹에서 마우스 우클릭을 해서 "Add New Entry (새 항목 추가)"를 선택한다. (혹은 메뉴바에서 "Entries > Add New Entry(항목 > 새 항목 추가)"를 선택한다.) 기본적인 비밀번호 이용법은 아래를 참고한다.

- "Title(제목)”칸에 비밀번호 항목을 구분할 수 있는 제목을 입력한다. 예를 들어, 비밀번호가 사용되는 웹사이트 또는 서비스명이 될 수 있다.
- "Username(사용자 이름)"칸에 비밀번호 항목과 관련된 사용자 이름(아이디)를 입력한다. (사용자 이름이 없는 경우 공란으로 남긴다.)
- "Password(비밀번호)"칸에 비밀번호를 입력한다. 새 비밀번호를 생성하거나 (또는 새 웹사이트에 가입하거나, 오랫동안 사용한 취약한 비밀번호를 새롭고 고유한 임의의 패스프레이즈로 바꿀 때도) 오른쪽의 주사위 아이콘을 클릭한다. 주사위 아이콘을 클릭하면 비밀번호 생성기(password generator)가 윈도우에 나타나는데, 임의적인 비밀번호를 생성할 때 사용해도 된다. 비밀번호에 들어갈 문자 종류와 길이를 포함한 여러 옵션을 선택한다.
    - 임의의 비밀번호를 생성할 경우, 그 비밀번호를 외울 필요가 없다는 점을 명심하자. (심지어 알 필요도 없다!) KeePassXC가 이를 저장하며, 필요할 때마다 적당한 프로그램에

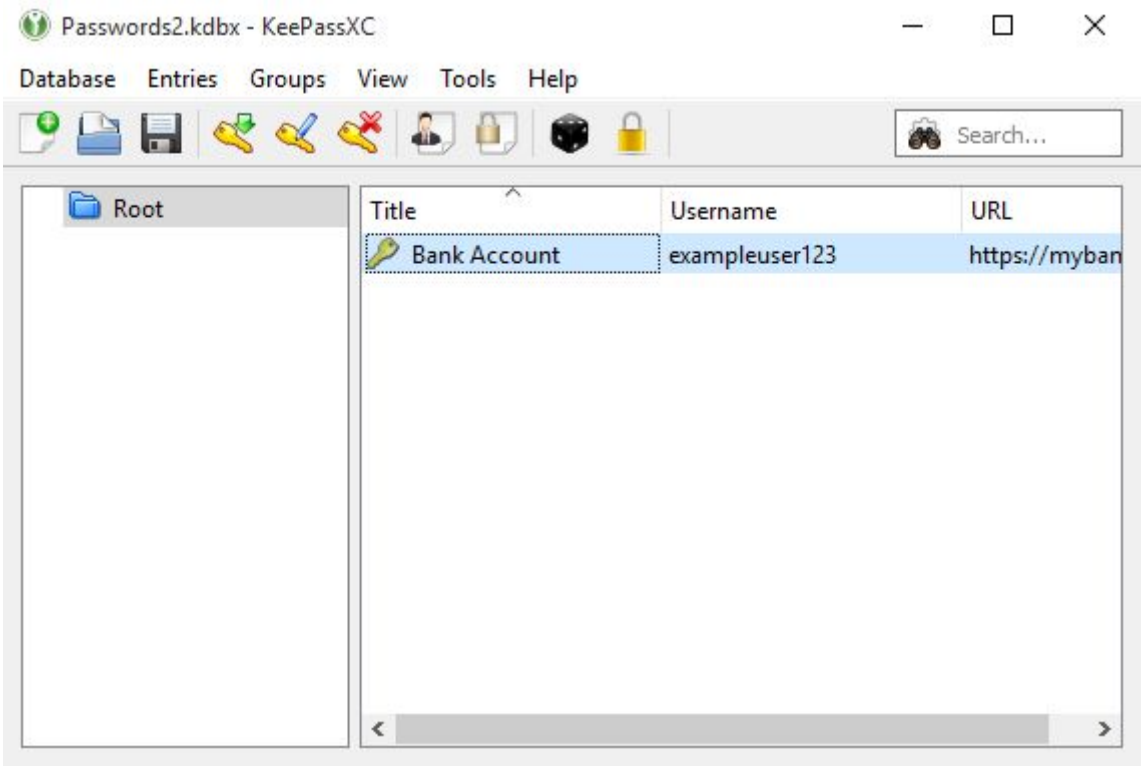
비밀번호를 복사/붙여넣기 할 수 있다. 이것이 패스워드 매니저(password manager)의 핵심이고, 웹사이트 또는 서비스마다 서로 다른 긴 임의의 비밀번호를 생성할 수 있으며, 그 비밀번호들이 무엇인지 알 필요가 없다!
    - 이 덕분에, 서비스에서 허용하는 가장 길고, 다양한 문자로 비밀번호를 구성해 만드는 것이 좋다.
    - 선택한 옵션에 만족한 경우, 오른쪽 아래 "Generate(생성)"를 클릭하여 비밀번호를 생성한다. 생성된 임의의 비밀번호는 자동적으로 "Password(비밀번호)"칸과 "Repeat(비밀번호 재입력/확인)"칸에 입력된다. 만약 KeePassXC 구버전을 사용하고 있는 경우, 임의의 비밀번호는 "Password"와 "Repeat"칸에 자동적으로 입력되지 않을 수 있으므로, "Apply(적용)"을 클릭한다. (임의의 비밀번호를 생성하지 않는 경우라면, 선택한 비밀번호를 입력하고 "Repeat"칸에 다시 입력해야 한다.) 마지막으로 "OK"를 클릭한다.
- 이제 비밀번호 데이터베이스에 비밀번호가 저장됐다. 변경사항을 저장하기 위해, "Database>Save Database (데이터베이스>데이터베이스 저장)"에 가서 변경사항을 저장한다.

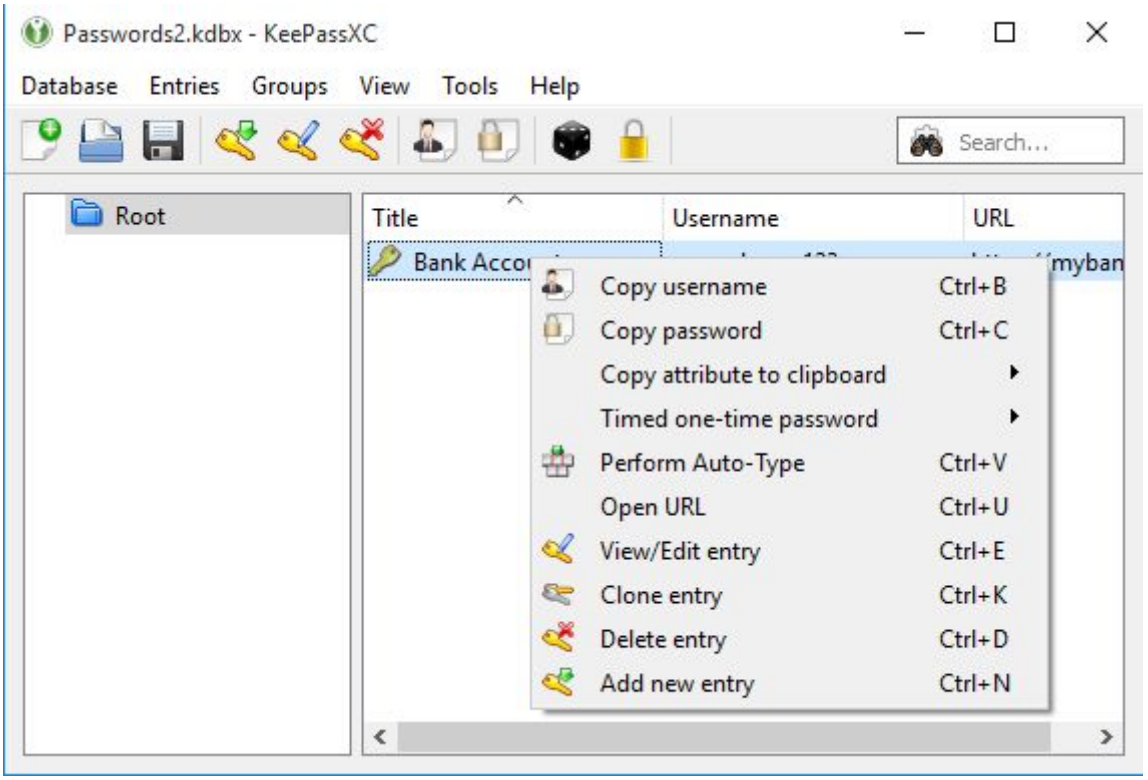


저장된 비밀번호를 변경/편집해야 하는 경우, 해당 그룹을 선택한 후 오른쪽 영역의 타이틀을 더블 클릭하면 "Edit Entry(항목 편집)"팝업창이 뜬다.

일반적인 사용

비밀번호 데이터베이스에 입력된 항목을 사용하기 위해서는, 해당 항목에서 마우스를 우클릭하여 "Copy username(사용자이름 복사)" 또는 "Copy password(비밀번호 복사)"를 선택한다. 사용자 이름/비밀번호를 입력하고자 하는 윈도우/웹사이트에 가서 적절한 칸에 붙여넣기 한다. (항목에서 우클릭을 하는 대신 항목에 입력된 아이디나 비밀번호를 더블 클릭해도 자동으로 클립보드에 복사된다.)





-

그 외 기능

KeePassXC의 다른 기능들은 아래와 같다.

- 검색창(메인 KeePassXC 윈도우창 툴바의 텍스트박스)을 사용하여 데이터베이스를 검색할 수 있다.
- 메인 창에서 열(column) 헤더를 클릭하여 입력된 항목을 분류할 수 있다.
- "Tools(도구) > Lock Database (데이터베이스 잠그기)"를 선택하여 KeePassXC를 잠가 보자("lock"). 이렇게 하면, KeePassXC를 실행된 상태로 놔두더라도 비밀번호 데이터베이스에 다시 접근할 때에 마스터 비밀번호 (그리고/또는 키파일)을 요구한다. 또한 일정 시간 이상 사용하지 않으면 KeePassXC가 자동으로 잠기게 할 수도 있다. 이렇게 하면 자리를 비웠거나 또는 컴퓨터를 분실한 경우에도 누군가가 비밀번호에 접근하는 것을 막을 수 있다. 맥OS에서 이 기능을 이용하기 위해서는, "Preferences(환경설정)> Settings(설정)"메뉴로 가 보안 옵션을 클릭한다. "Lock database after inactivity of [number] seconds (비활성화 시간이 [숫자]초 지나면 데이터베이스 잠그기" 박스를 클릭한다. 리눅스 또는 윈도우를 사용하는 경우, 메뉴의 "Tools>Settings(도구>설정)"를 클릭하여 보안 옵션을 선택하고, "비활성화 시간이 [숫자]초 지나면 데이터베이스 잠그기(Lock database after inactivity of [number] seconds)"를 클릭한다.

KeePassXC에는 아이디와 비밀번호 외에도 더 많은 것들을 저장할 수 있다. 예를 들어, 계좌 번호, 제품 키, 항공사 마일리지 정보 또는 일련번호 등처럼 중요한 정보에 대한 항목을 만들 수 있다. "비밀번호(Password)"칸에 들어가는 것이 반드시 비밀번호일 필요는 없다. 실제 비밀번호 대신 저장하고 싶은 데이터를 "비밀번호" 칸에 입력해 놓으면 (사용자이름(아이디)는 없기 때문에"사용자이름" 칸은 비워둔다) KeePassXC가 이를 안전하게 저장해 줄 것이다.

-

브라우저 확장 기능을 설치하는 방법

본 설명은 https://keepassxc.org/docs/keepassxc-browser-migration/를 참고하였다. (접속날짜: 2018.4.30)

브라우저 확장 기능은 웹 브라우저에 추가 기능을 설치하는 소프트웨어 요소이다. KeePassXC 브라우저 확장 기능은 웹 브라우저와 KeePassXC 응용 프로그램의 소통을 편리하게 한다. 또한 웹에 비밀번호를 빠르게 저장하거나 자동으로 입력할 수 있도록 한다.

2.3버전부터 KeePassXC는 KeePassXC-Browser로 불리는 새로운 브라우저 플러그인을 제공하며, 구글 크롬, 크로미움, 파이어폭스 및 비발디와 호환되며, 크롬 웹 스토어 또는 모질라 애드온 저장소에서 다운받을 수 있다.

새 애드온(부가 기능)은 구 KeePassHTTP 애드온(KeePassHttp-Connector, chromeIPass, PassIFox등)을 대체하며, 구버전 애드온에 대한 지원은 향후 KeePassXC 버전에서는 삭제될 것이다.

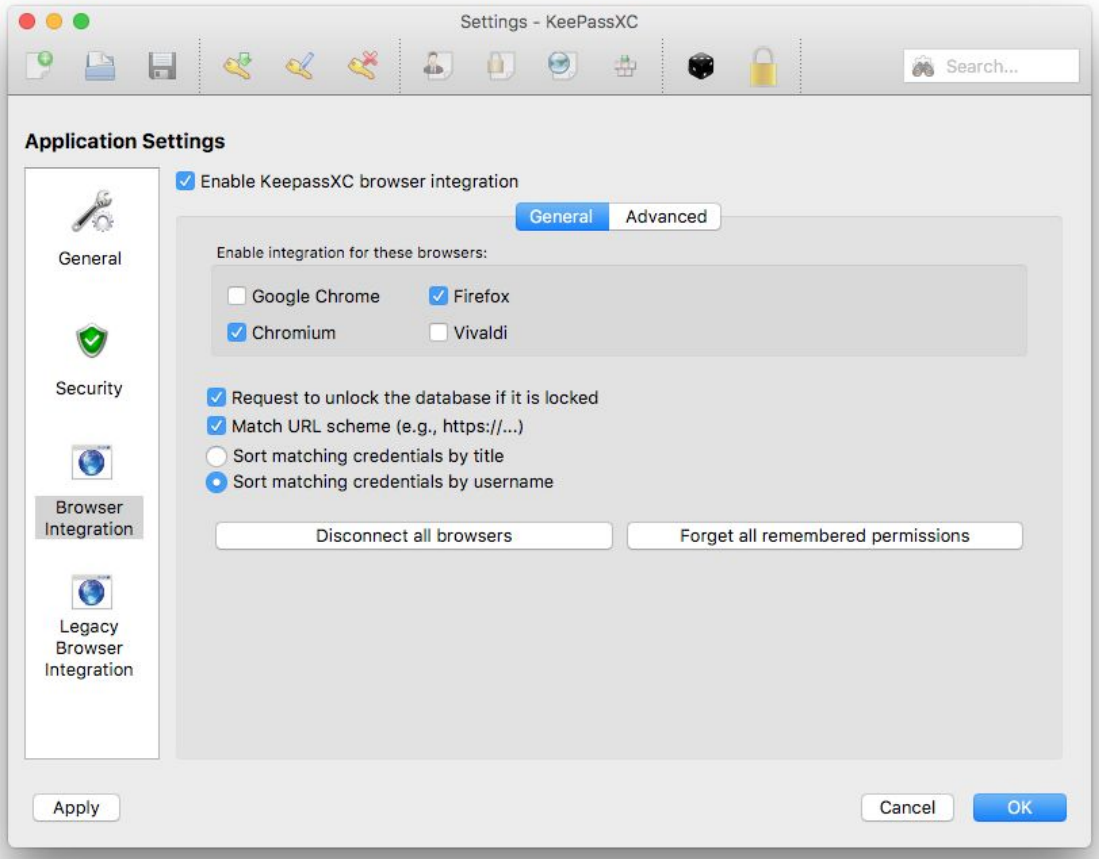
-

KeePassXC와 KeePassXC-브라우저 연결하기

KeePassXC-브라우저와 KeePassXC를 설치 한 뒤에는, 먼저 KeePassXC를 시작하고 기본설정에서 활성화 되지 않은 일부 설정을 조정해야한다.

1. 브라우저 통합 활성화

KeePassXC의 설정(Settings)으로 가서 "*Browser Integration / Enable KeePassXC Browser Integration(*브라우저 통합/ KeePassXC 브라우저 통합 활성화)"로 간다. 이 기능이 활성화 되지 않으면, 브라우저 확장 기능은 KeePassXC와 연동될 수 없다.



브라우저 통합이 활성화 되었다면, 구 KeePassHTTP 인터페이스는 "*Legacy Browser Integration / Enable KeePassHTTP server*"으로 가서 해제할 수 있다.

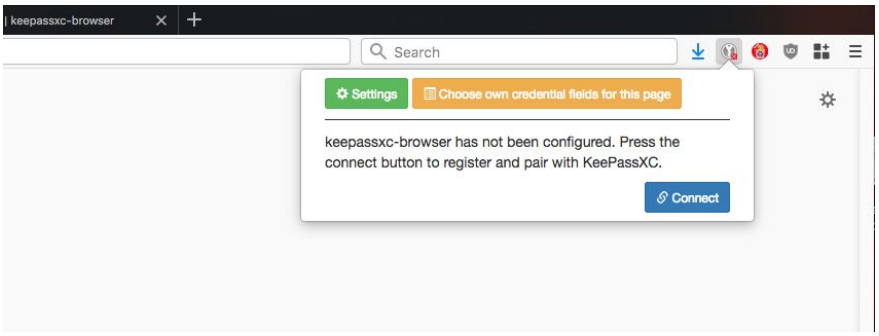
2. 브라우저 기능 활성화

브라우저에서 KeePassXC의 접속을 허용하기 위해, KeePassXC 프로그램 파일 위치를 찾을 수 있도록 설정해야 한다. 다행히도 KeePassXC는 이를 자동으로 수행할 수 있다. 사용자는 단지 KeePassXC를 사용하고자 하는 브라우저에서 "*Enable integration for these browsers*"라는 체크박스에 표시만 하면 된다.

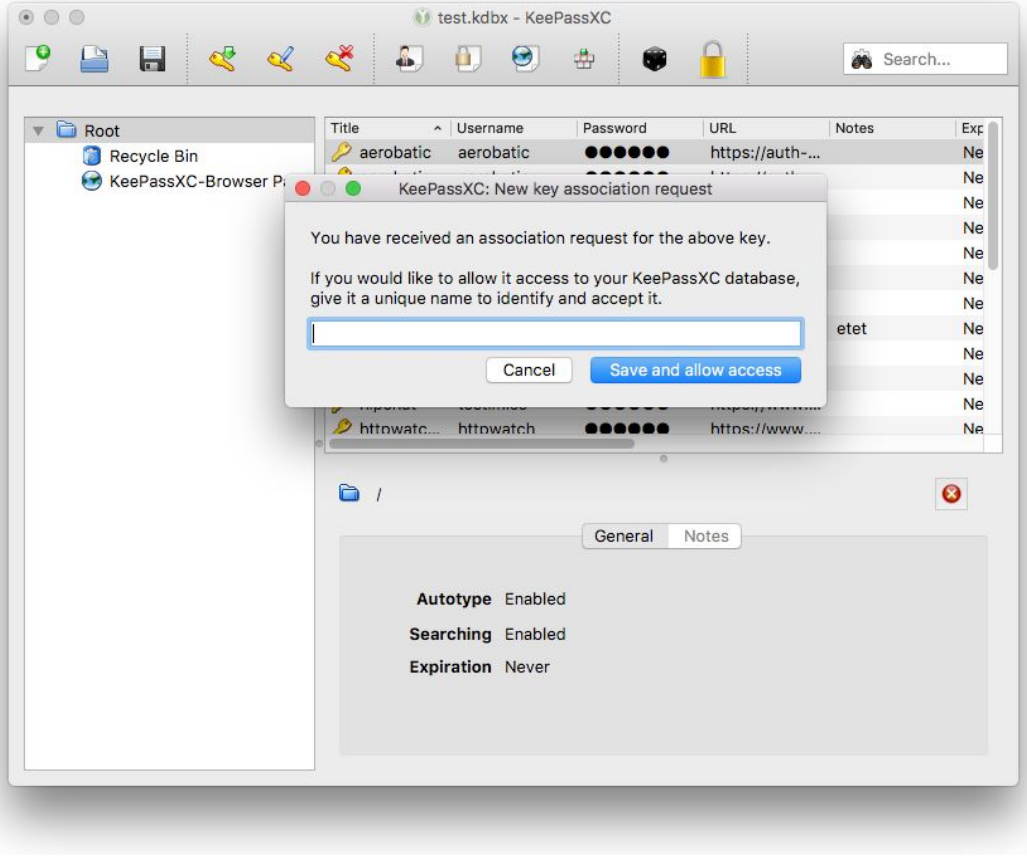
3. 데이터베이스에 연결하기

KeePassXC를 열어 데이터베이스의 잠금을 푼다 (데이터베이스가 잠겨있거나 KeePassXC 열려있지 않은 경우 다음 단계들이 실행되지 않기 때문에 중요하다).

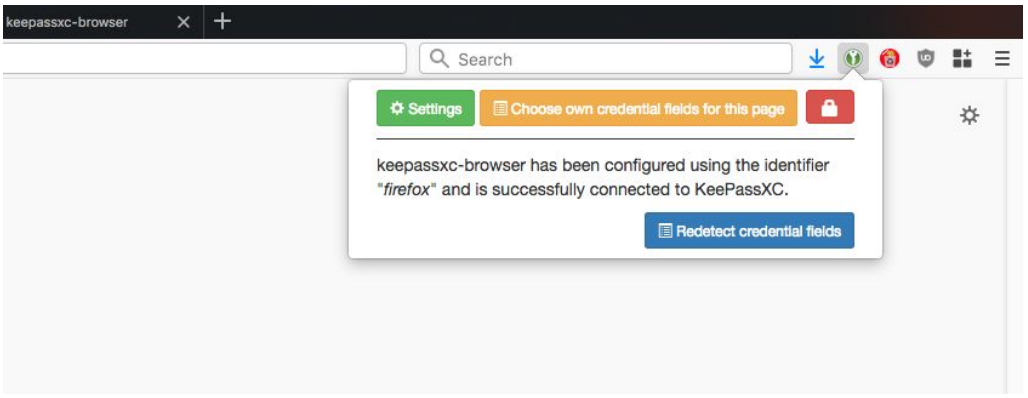
브라우저로 가서 주소창 옆에 있는 KeePassXC아이콘을 클릭한다. KeePassXC-브라우저가 구성되지 않았다는 팝업창이 뜬다 (다른 에러메시지가 뜨면 "*Refresh*(새로고침)"를 클릭한 뒤 몇 초 기다린다).



"*Connect*(연결)"버튼을 클릭한다. 브라우저 명칭을 입력하라는 창이 뜨며, 접근이 승인된다.



원하는 브라우저 명칭(가장 좋은 명칭은 어떤 브라우저인지 식별하는 명칭이다)을 입력하고 "*Save and allow access*(저장 및 접근 허용)"을 클릭하면, 사용자의 브라우저는 KeePassXC와 연결된다.



Autofill(자동 채우기)기능은 정보 보안에 나쁠 수 있다. 이 기능을 해제하기 위해서는, 설정에서 “Automatically fill-in single credentials entry(1회 인증 입력값으로 자동 채우기)” 와 “Activate autocomplete for username fields(사용자이름 자동 채우기 기능 활성화)”를 해제한다.

이제 KeePassXC 사용에 관한 설명이 모두 끝났다. 사용자는 웹에서 사용하는 모든 인증을 KeePassXC에 저장할 수 있다. 또한 사용자 이름(ID)/비밀번호를 자동으로 저장할 수 있다.

KeePassXC는 사용하기 편리하고, 강력한 기능을 가진 소프트웨어이다. KeePassXC에 대해 더 검색하여 KeePassXC가 제공하는 모든 유용한 기능을 배워보자.