docs.nitrokey.com /software/nk-app2/keepassxc

KeePassXC - Nitrokey Documentation

4-5 minutes

These instructions describe how to protect and encrypt a KeePassXC password database with Nitrokey 3.

Note

- KeePassXC version 2.7.6 or newer is required.
- Nitrokey App 2 version 2.2.2 or newer is required.

First Step: Generate a HMAC Secret With the Nitrokey App 2¶

1. Open Nitrokey App 2
2. Select the Nitrokey 3
3. Select the `PASSWORDS` tab
4. Click on `ADD` to create a new credential
5. Select `HMAC` from the algorithm drop-down menu

   Note

   - The credential is automatically named in `HmacSlot2`.
   - No extra attributes can be saved for the HMAC credential.
   - The HMAC secret must be *exactly 20 bytes* long and in *Base32* format. That is exactly 32 characters.
   - It is possible to save exactly one HMAC secret on a Nitrokey 3.

6. To generate a secret, there is a button in the field on the right-hand. It is also possible to enter your own secret, as long as it is compliant.

   Warning

   The database can no longer be unlocked if the Nitrokey 3 is lost or unavailable! Thus, you may want to set up a second Nitrokey 3 with the same HMAC secret as a backup device.

   Important

   The secret can **only** be seen before saving. If the KeePassXC database is to be used with another Nitrokey 3, the HMAC secret must be copied which is **only** possible **before saving** the credential.

7. Click on `SAVE` to save the credential

First Option: Protect an Existing KeePassXC Database With a Nitrokey 3¶

1. Open KeePassXC
2. Open the existing KeePassXC database that is to be protected with a Nitrokey 3.

3. Select `Database` -> `Database Security...` from the menu bar
4. Select `Security` on the left side
5. Click on the `Add additional protection...` button in the `Database Credentials` tab
6. Scroll down to `Challenge-Response` and click on `Add Challenge-Response`
7. Now if the Nitrokey 3 is plugged in and a HMAC was generated before, Nitrokey 3 should be displayed in the field.

   Click on `OK` to add the Nitrokey 3 to the existing KeePassXC database

Note

By default the Nitrokey 3 is used as a second factor in addition to the passphrase. To protect the database by the Nitrokey 3 exclusively, delete the passphrase by clicking the button `Remove Password`.

Tip

If the Nirokey 3 is not recognized, close KeePassXC completely. Then connect the Nitrokey 3 to your computer before restarting KeePassXC.

Second Option: Creating a KeePassXC Database, Protected by Nitrokey 3¶

1. Open KeePassXC
2. Select `Database` -> `New Database...` from the menu bar to create a new KeePassXC database.
3. Fill in the display name and an optional description for your new database and click on `Continue`
4. Further database encryption settings can now be configured here or the default settings can be retained. The settings can also be changed later in the database settings.

   Click on `Continue` to confirm the settings
5. **Database Credential**

   Here you can enter a password as a second factor to unlock the database. To connect the Nitrokey 3 (on which the HMAC secret was generated) to the new KeePassXC database, click on `Add additional protection...`
6. Scroll down to `Challenge-Response` and click on `Add Challenge-Response`
7. Now if the Nitrokey 3 is plugged in and a HMAC was generated before, Nitrokey 3 should be displayed in the field. Click on `Continue` to complete the creation of the new KeePassXC database.

Note

If the passphrase is left empty, the database will be protected by the Nitrokey 3 exclusively. If a passphrase is entered, the database will be protected by the passphrase **and** the Nitrokey 3.

Tip

If the Nitrokey 3 is not recognized, close KeePassXC completely. Then connect the Nitrokey 3 to your computer before restarting KeePassXC.

Troubleshooting for Linux¶

If the Nirokey 3 device is not recognised by KeePassXC on a Linux system:

- Provided that the udev rules have been set as described here.
- Provided that the `pcscd service` are has been started with:

```
sudo systemctl start pcscd.service
```

- Install the latest version of KeePassXC with flatpak:

```
flatpak install flathub org.keepassxc.KeePassXC
```

- Install `ccid` on Arch Linux based systems. See also: Arch wiki: Nitrokey.