

# Setup KeePassXC for Okta MFA on Linux

- 1) Ensure that your packages and repositories are up to date:

Debian based distributions (Ubuntu, Pop! OS etc.):

```
sudo apt update && sudo apt upgrade
```

Fedora:

```
sudo dnf update
```

- 2) Install the KeePassXC package:

Flatpack package:

```
flatpak remote-add --user --if-not-exists flathub https://flathub.org/repo/flathub.flatpakrepo
```

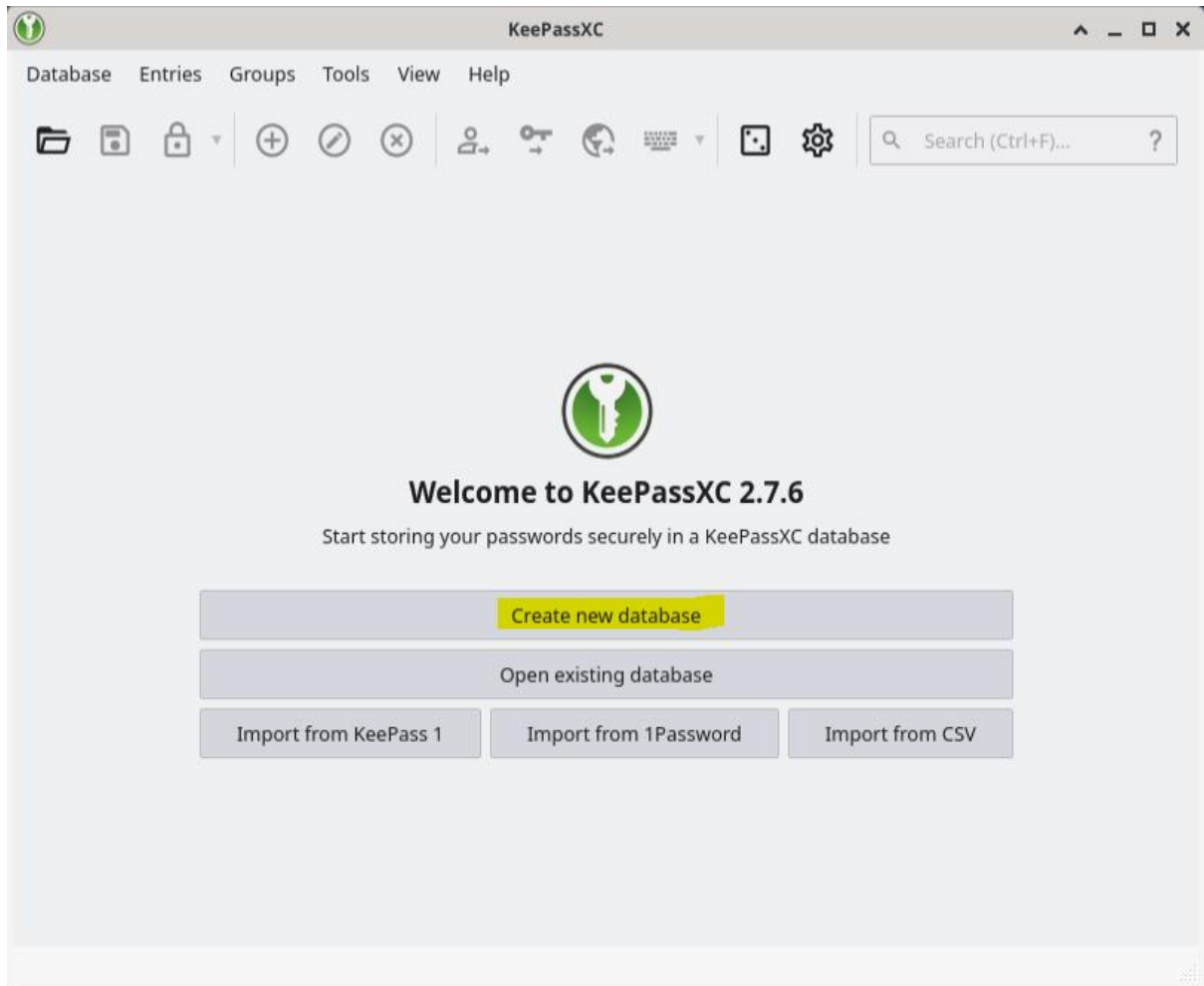
```
flatpak install --user flathub org.keepassxc.KeePassXC
```

Snap Package:

```
sudo snap install keepassxc
```

For distribution specific options, see <https://keepassxc.org/download/#>

3) Launch KeePassXC then select “Create new database”



4) Enter any name and description then click next

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

5) Click continue on the encryption settings screen

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

100 ms 5.0 s

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

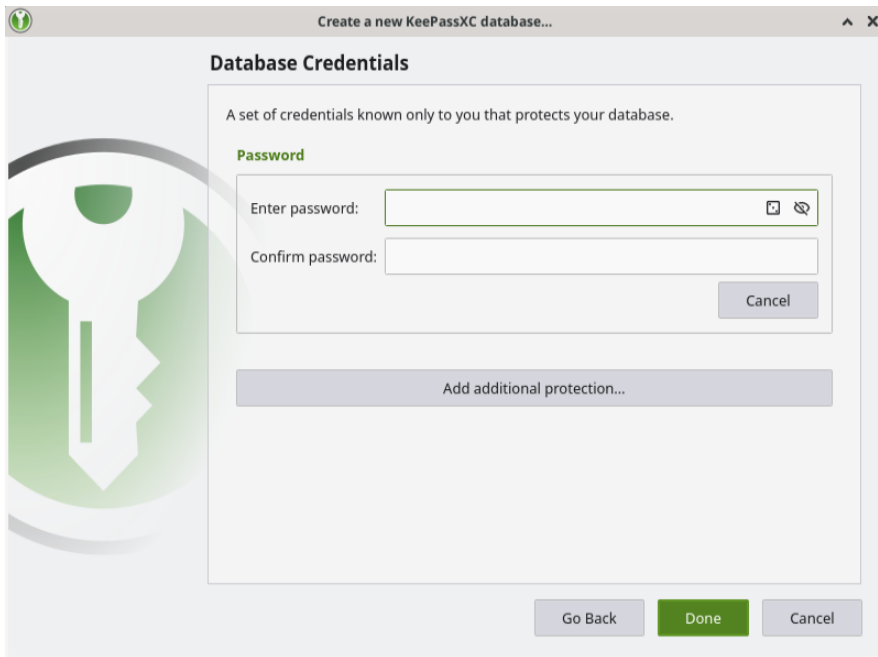
Database format: KDBX 4 (recommended)

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

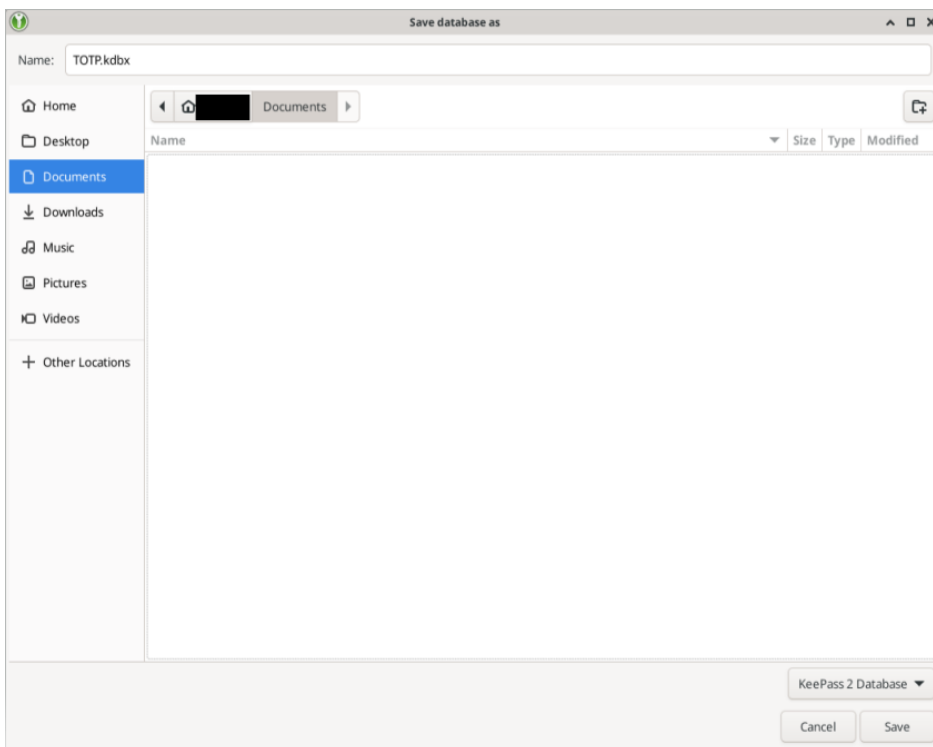
Advanced Settings

Go Back Continue Cancel

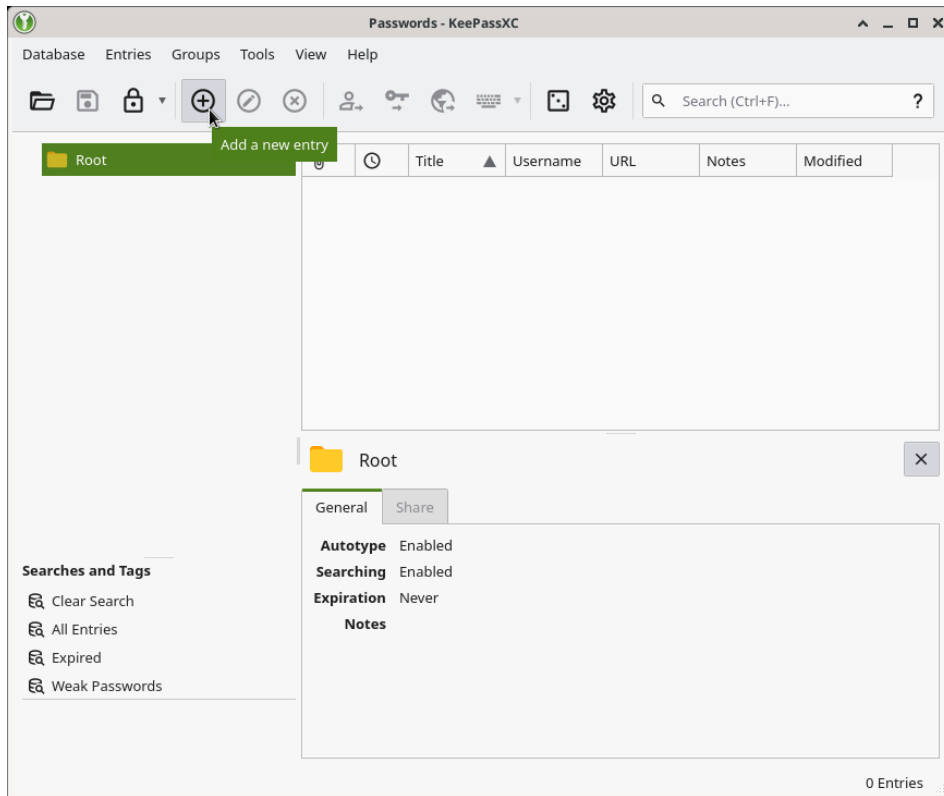
- 6) Enter a strong master password, this will be used to unlock the database for your MFA codes



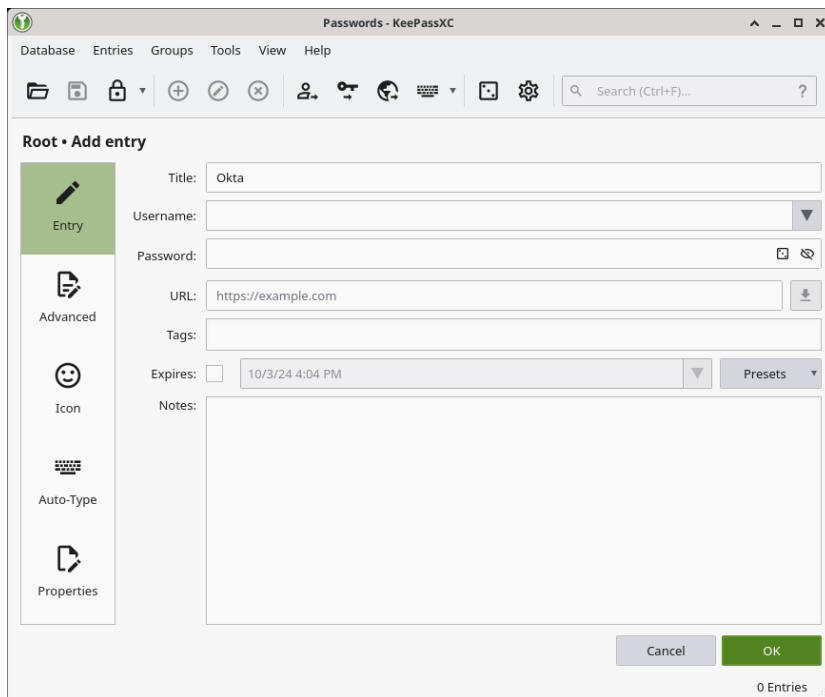
- 7) Choose where to save your database



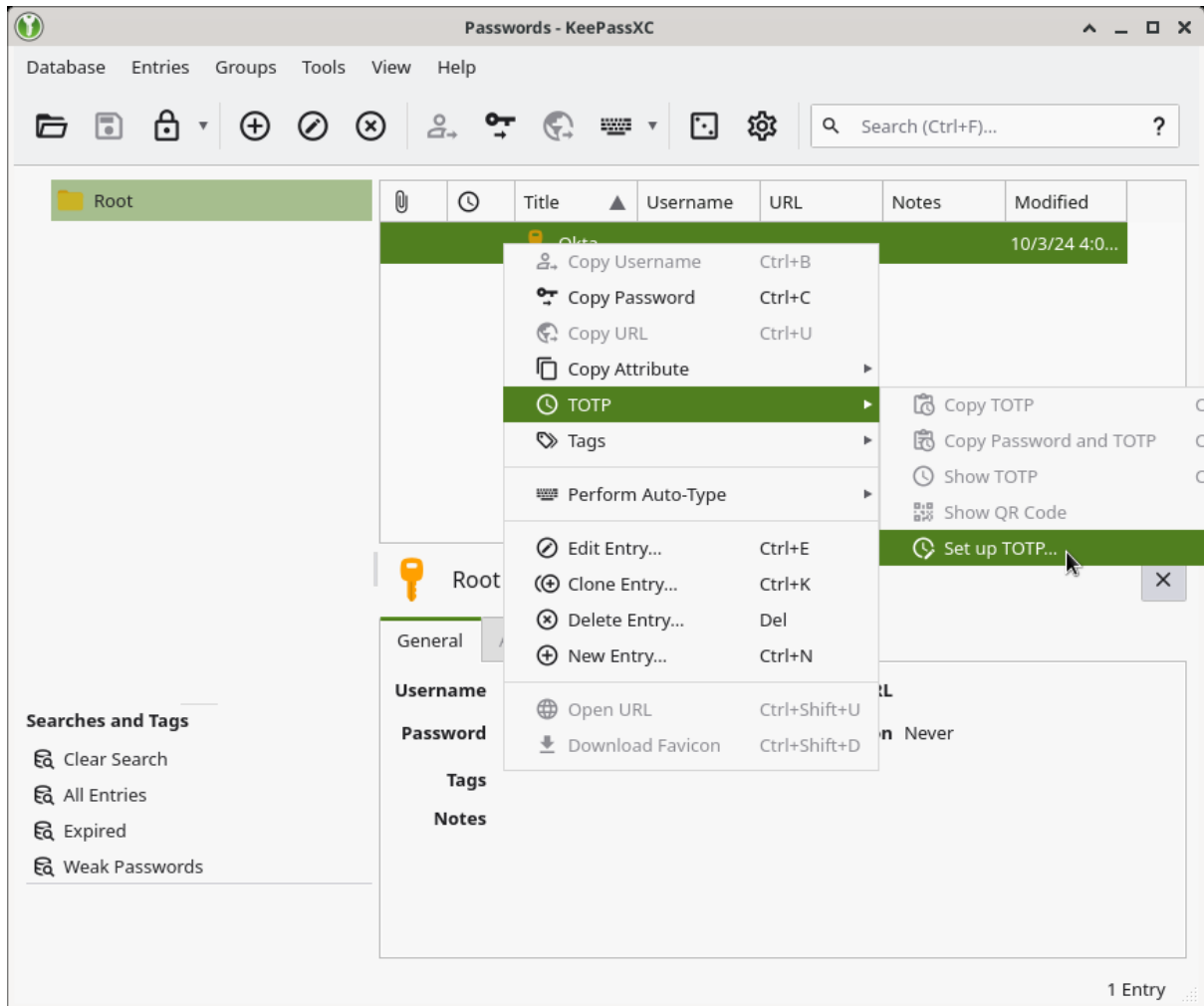
8) Once on the main screen, click the plus icon to add a new entry



9) Choose a name then click OK



10) Right click on the entry, choose TOTP then Set up TOTP...



11) Open your web browser, go to the [MFA setup page](#) and login with your student OneID and password

12) Choose google authenticator then select "Can't Scan?"



### Set up Google Authenticator

  @mqauth.uni.mq.edu.au

Scan barcode

Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".

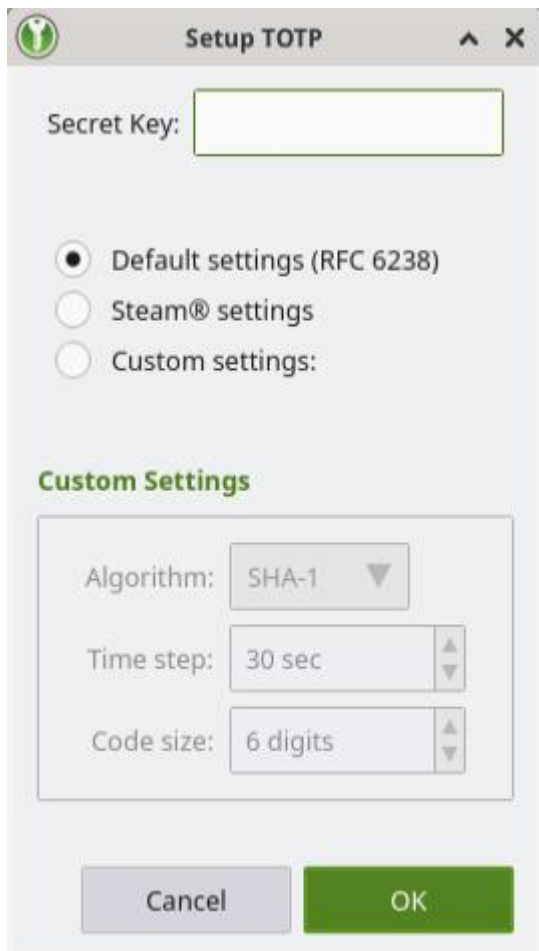


[Can't scan?](#)

[Next](#)

[Return to authenticator list](#)

13) Copy the 16 Character secret key into the Secret key field in KeePassXC then click OK

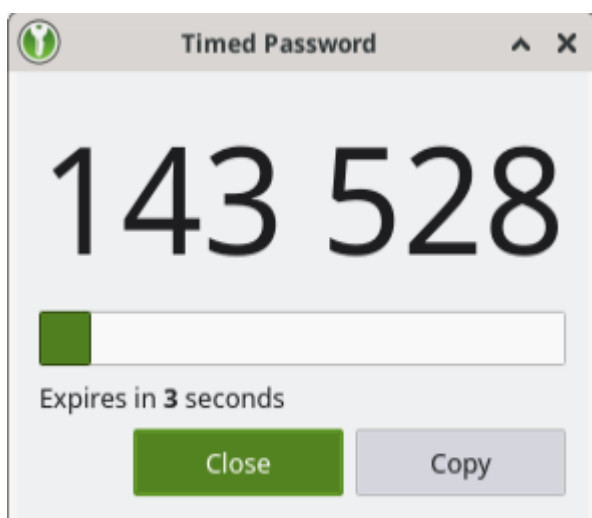
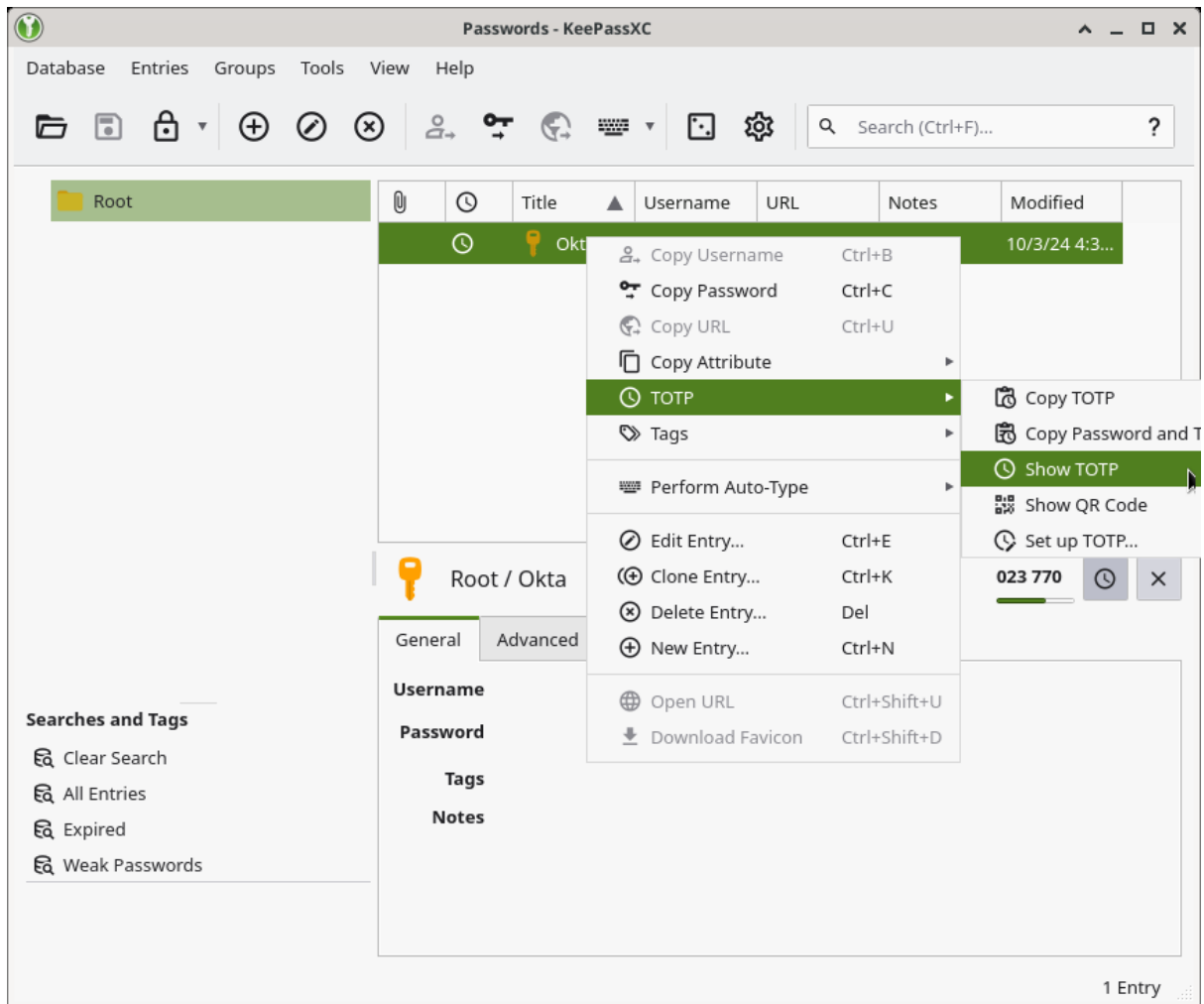


The image shows a dialog box titled "Setup TOTP" with a green icon in the top-left corner. The dialog has a title bar with a maximize button and a close button. The main content area contains a "Secret Key:" label followed by an empty text input field. Below this are three radio button options: "Default settings (RFC 6238)" (which is selected), "Steam® settings", and "Custom settings:". Under the "Custom Settings" section, there are three controls: "Algorithm:" with a dropdown menu showing "SHA-1", "Time step:" with a spinner box showing "30 sec", and "Code size:" with a spinner box showing "6 digits". At the bottom of the dialog are two buttons: "Cancel" and "OK".


14) After copying the code click next in the browser window.




15) You'll then need to enter your TOTP code. You can right click on the entry and either copy the TOTP code to the clipboard or show TOTP.



16) Enter this code into the setup window on your browser and click Verify



**MACQUARIE**  
University



**Set up Google Authenticator**

@ [REDACTED] @mqauth.uni.mq.edu.au

Enter code displayed from application

**Enter code**

[Verify](#)

[Return to authenticator list](#)

You have now setup KeePassXC for use with okta MFA. To log in again, simply repeat steps 15 & 16 when you are prompted to enter your code.

Note1: Every time you relaunch KeePassXC you will have to reenter the password you chose in step 6. Should you lose access to this database or forget your password you will have to request an MFA reset by contacting the help desk and verifying your identity.

Note2: KeePassXC also functions as a password manager. It is recommended that you keep your passwords and TOTP codes in a separate database if you will also be utilising password management features of this application.