

First-time 2FA Setup via a Personal Computer

Preliminary Actions

You need to install a *program* on your personal computer which will

- store the **secret key** that the IL authentication system will share with you
- calculate TOTP passcodes using the **secret key** as a seed

We advise Free Softwares such as [KeePassXC](#) (multiplatform with GUI) or the [OATH Toolkit](#) (GNU/Linux terminal), but you are free to choose any programs that implement the open OTP standards.

Setup

Step 1

Navigate to any of the Lorentz Institute SSO web applications, such [Account Services](#), [Remote Workspace](#), etc.

You will be redirected automatically to the Lorentz Institute Identity Provider login page as in **Figure 1**.

The screenshot shows a login form titled "Lorentz Institute Intranet". It features a logo with the text "Instituut-Lorentz". Below the logo are two input fields: "Username" and "Password", both with placeholder text. A large blue "Sign In" button is at the bottom. At the bottom of the page, there is a small legal notice: "By using this service you agree to abide to the Leiden University ICT Code of Conduct and authorise the temporary storage of your session information (e.g. IP address) for debugging and security purposes."

Figure 1: Identity Provider login page

Step 2

Enter your IL credentials to sign in. Upon successful login, you will be redirected to a page containing a QR code. Click on “Unable to Scan?” to display your shared **secret key** and the other parameters to input in your OTP program (Figure 2).

Note the secret key, the algorithm, the number of digits, and the time interval. You will need them in Step 3.

The figure consists of two vertically stacked screenshots of a web page titled "Lorentz Institute Intranet".

Screenshot 1 (Top):

- Step 1: You need to set up Mobile Authenticator to activate your account.
Install one of the following applications on your mobile:
 - + FreeOTP
 - + Google Authenticator
- Step 2: Open the application and scan the barcode:
[QR code]
- Step 3: Enter the one-time code provided by the application and click Submit to finish the setup.
Provide a Device Name to help you manage your OTP devices.
One-time code *
Device Name
Submit

Screenshot 2 (Bottom):

- Step 1: You need to set up Mobile Authenticator to activate your account.
Install one of the following applications on your mobile:
 - + FreeOTP
 - + Google Authenticator
- Step 2: Open the application and enter the key:
0000-0000-0000-0000-0000-0000-0000-0000
Scan barcode?
- Step 3: Use the following configuration values if the application allows setting them:
 - o Type: Time-based
 - o Algorithm: SHA256
 - o Digits: 6
 - o Interval: 30
- Step 4: Enter the one-time code provided by the application and click Submit to finish the setup.
Provide a Device Name to help you manage your OTP devices.
One-time code *
Device Name
Submit

Figure 2: TOTP Setup Page (QR code and other sensitive information deliberately blurred)

Step 3

Open KeePassXC (installed on all IL workstations), create a new passwords database if you do not want to use an existing one and click on *Entries* → *TOTP* → *Set Up TOTP*. Insert your private key, algorithm, time interval and number of digits from Step 2 and confirm by clicking on 'OK'.

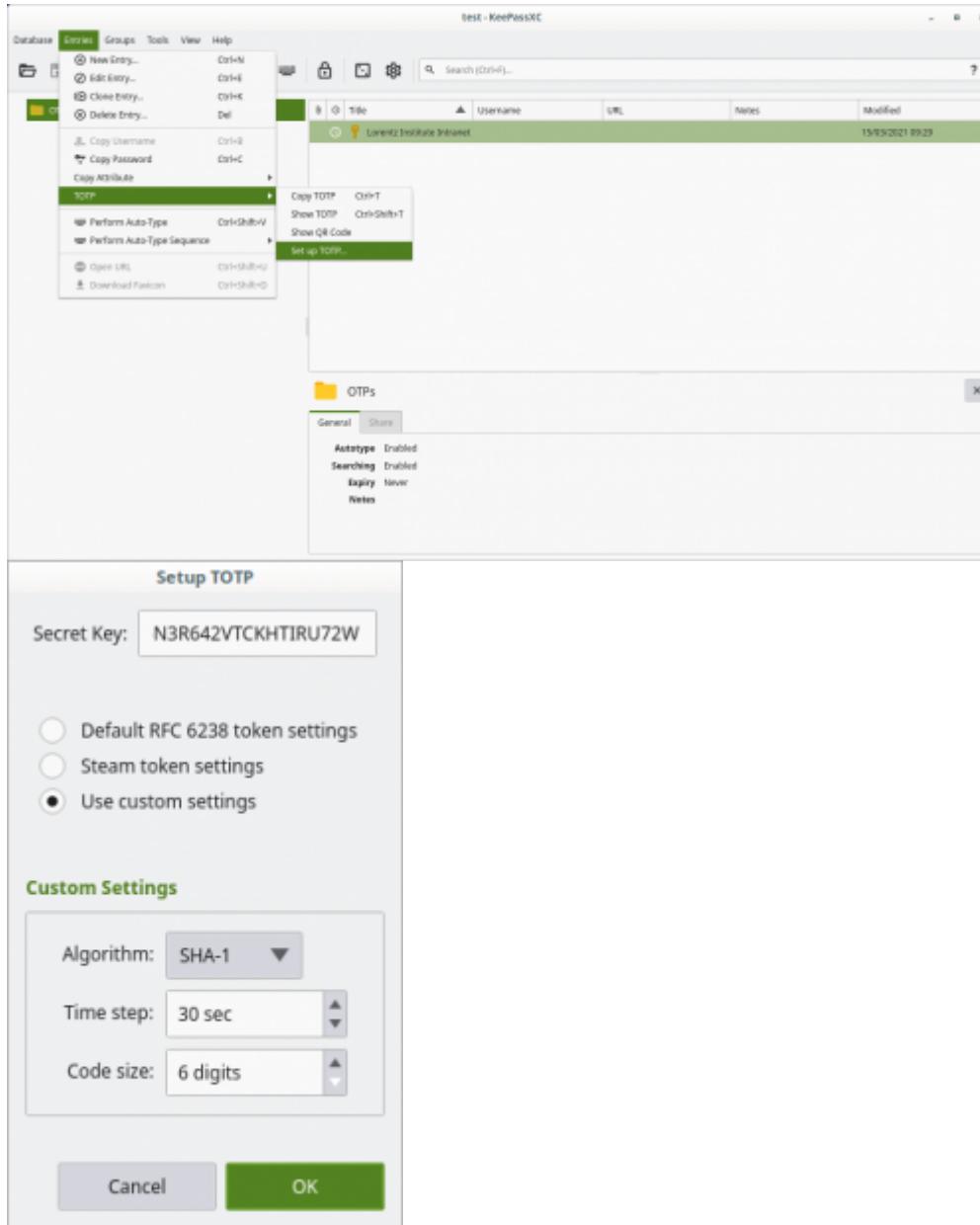
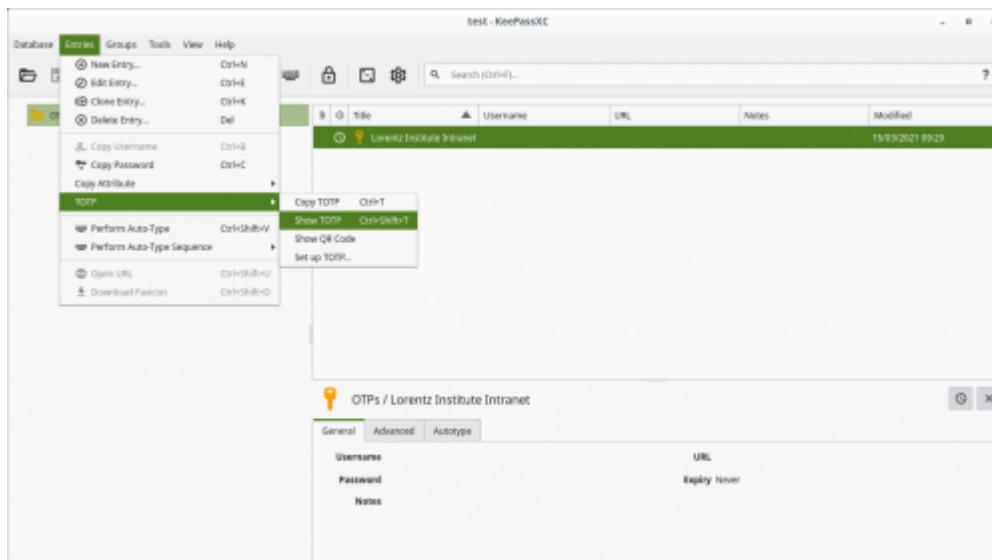


Figure 3: TOTP Setup with KeePassXC. Use the TOTP settings described in Step 2.

Generate a OTP by clicking on *Entries* → *TOTP* → *Show TOTP* and paste it to



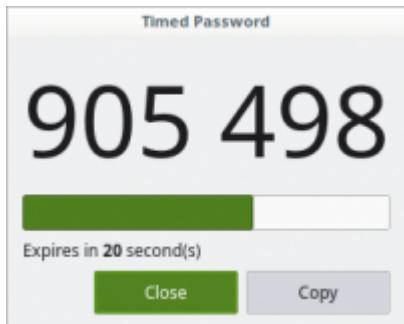


Figure 4: TOTP generation KeePassXC and final 2FA setup on the Lorentz Institute Identity Provider

From:
<https://helpdesk.physics.leidenuniv.nl/wiki/> - Computer Documentation Wiki

Permanent link:
https://helpdesk.physics.leidenuniv.nl/wiki/doku.php?id=institute_lorentz:2fa-pc&rev=1615798442

Last update: **2021/03/15 08:54**

