

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**.



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 to set it up (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 screenshots of the Lorentz Institute Intranet TOTP Setup Page. Both screenshots show the same interface with the Lorentz Institute logo at the top. The text reads: "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 says "Open the application and scan the barcode." The top screenshot shows a blurred QR code. Step 3 says "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." It has input fields for "One-time code *" and "Device Name", and a "Submit" button. The bottom screenshot shows step 4 with a blurred configuration key: "KEY: 843K 0B4D-0000 1JPC 00000000 04TY". It also has a "Scan barcode?" link and step 3 instructions. Step 4 says "Use the following configuration values if the application allows setting them: Type: Time-based, Algorithm: SHA1, Digits: 5, Interval: 30." It then has the same "One-time code *" and "Device Name" input fields and a "Submit" button.

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`.

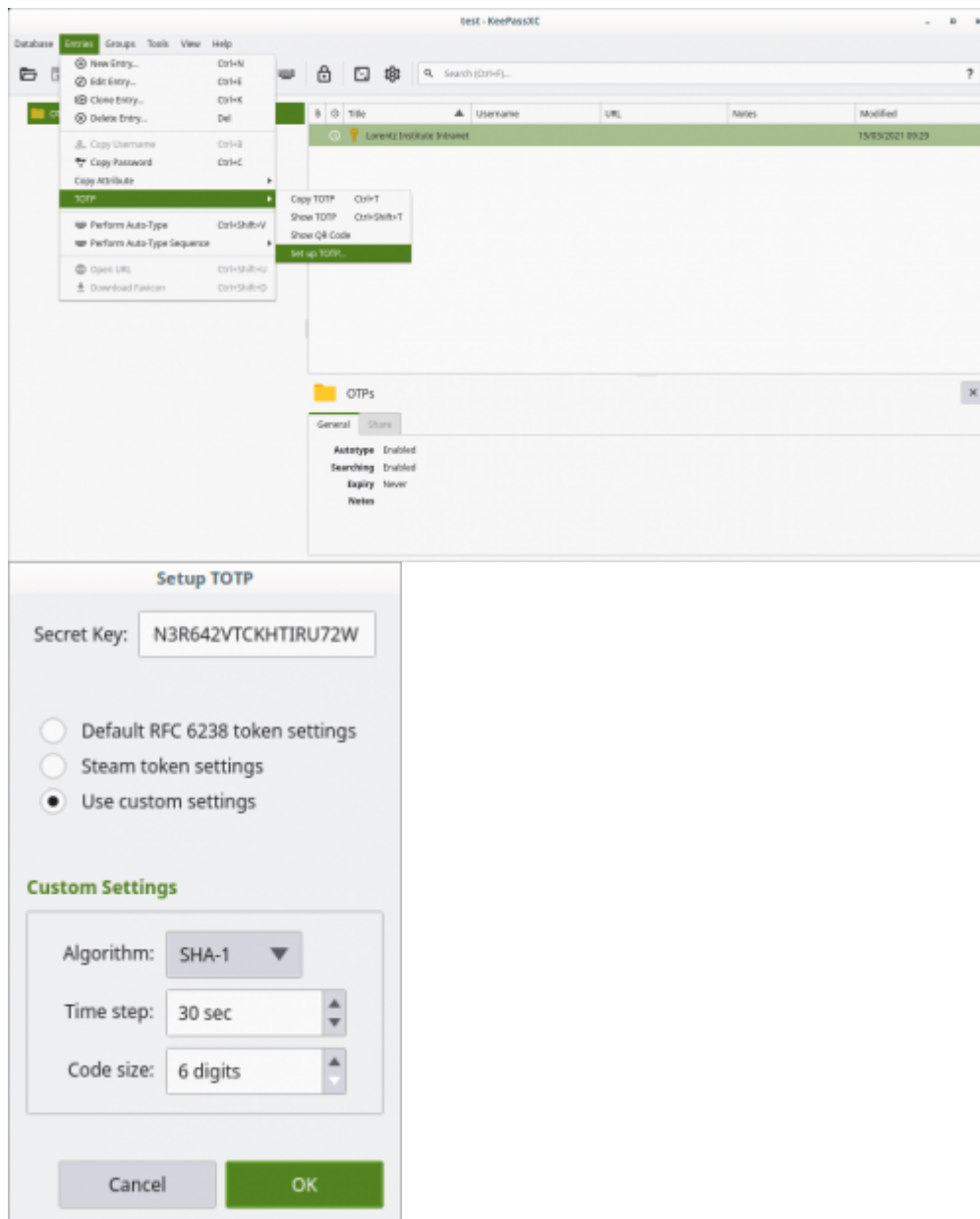
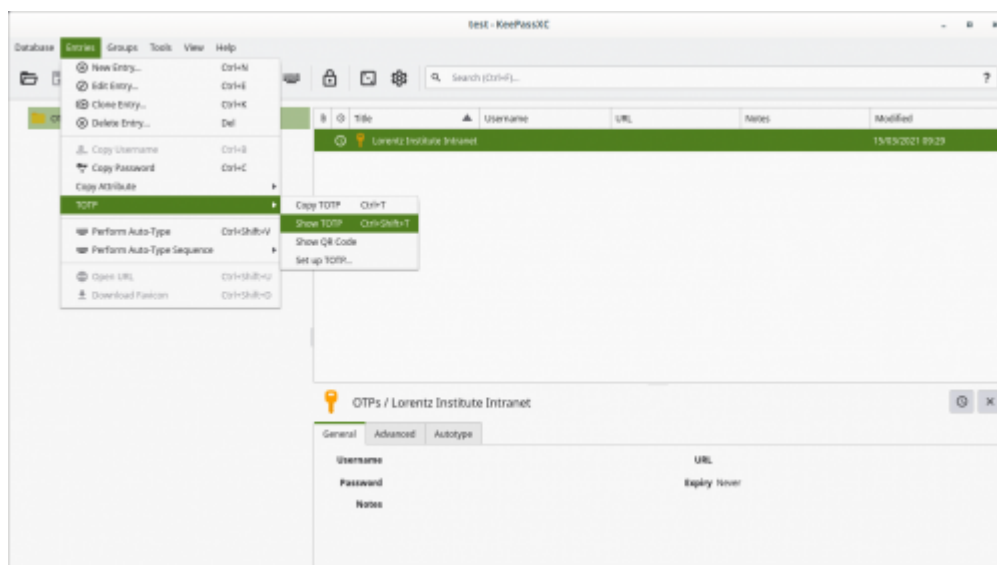


Figure 3: TOTP Setup with KeePassXC. Use the TOTP settings described in Step 2.

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



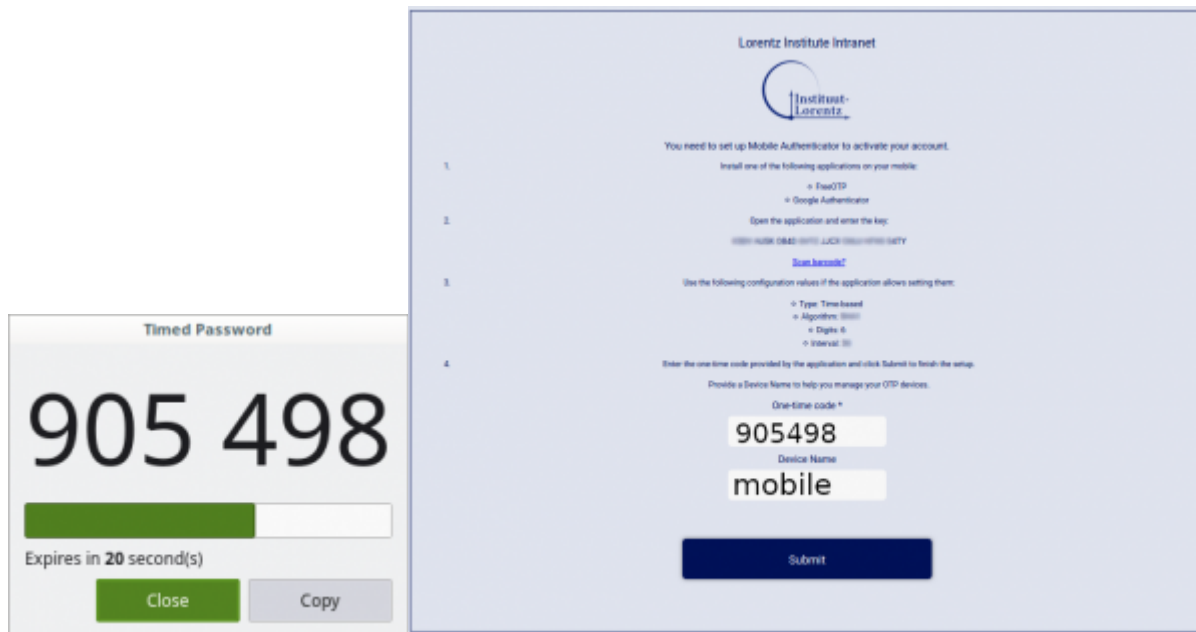


Figure 4: TOTP generation KeePassXC and final 2FA setup on the Lorentz Institute Identity Provider

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

Permanent link:
https://helpdesk.lorentz.leidenuniv.nl/wiki/doku.php?id=institute_lorentz:2fa-pc&rev=1615799013

Last update: **2021/03/15 09:03**

