

First Time Access

With a Personal Computer

If you do not have a Smart Phone, or if you do not want to use a Smart Phone, you can use alternative programs to provide the passcode needed for 2FA. A few of these programs are:

- KeepassXC (keepassxc.org GUI) or,
- oathtool ([oath-toolkit](https://github.com/jkolarik/oathtool) GNU/Linux cmd line) or,
- OTP Manager ([id928941247](https://github.com/leidenuniv/otpmanager) MacOS)

or any softwares that implement OTP standards.

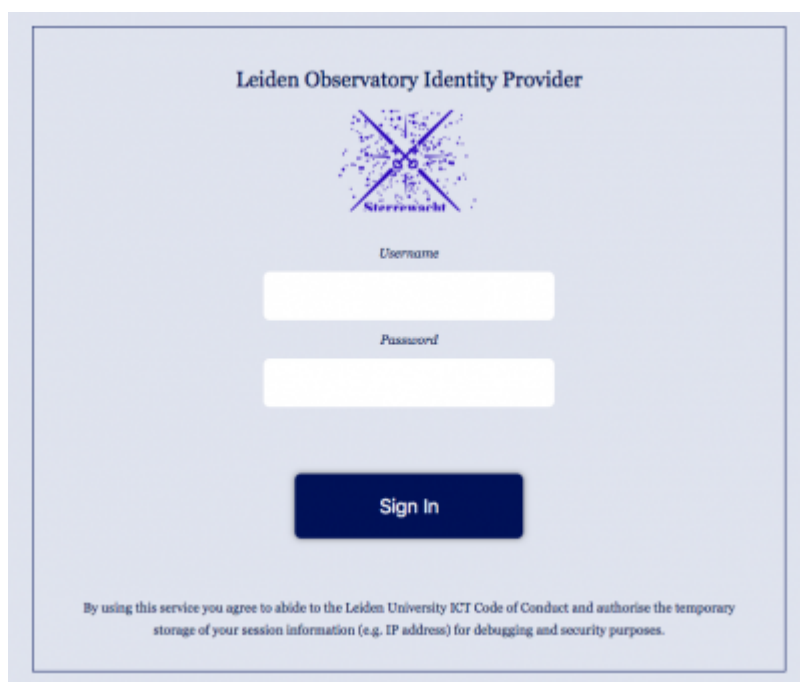


Figure 1: 2FA Login screen (Click image to enlarge).

So after installing one or more of the above programs you can proceed to go to a web page that helps you setup 2FA. This page is located in our [Self Service area](#). When you access that page you are redirected to the new Observatory Identity Provider and presented with a login window.



The screenshot shows a web page titled "Leiden Observatory Identity Provider". It features a logo at the top center. Below the logo, the text reads: "You need to set up Mobile Authenticator to activate your account." The page is divided into three numbered steps:

1. Install one of the following applications on your mobile:
 - a FreeOTP
 - o Google Authenticator
2. Open the application and scan the barcode:
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 device.

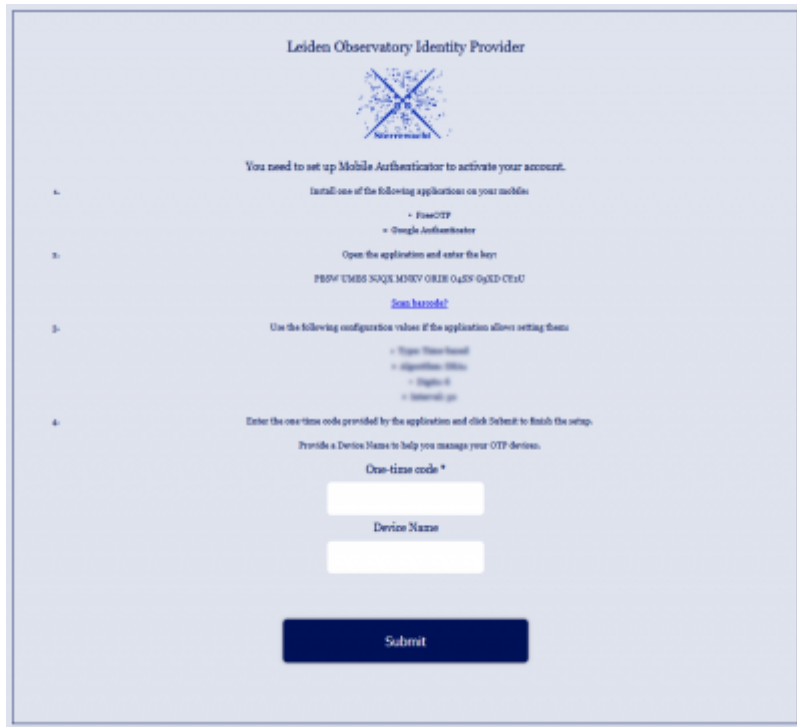
(Six digit) One-time passcode *

Device Name

Submit

<caption>2FA setup secret key form
(Click image to enlarge).</caption>

After entering your account credentials you are presented a QR code on the next page. Your computer programs are not equipped to scan QR codes, so you need to 'see' the secret key. For this you click the link [Unable to scan?](#)



The screenshot shows a web interface for the Leiden Observatory Identity Provider. At the top, it says "Leiden Observatory Identity Provider" with a logo. Below that, it states "You need to set up Mobile Authentication to activate your account." and lists four steps: 1. Install one of the following applications on your mobile (with links to FIDO2TP and Google Authenticator). 2. Open the application and enter the key (with a QR code and a "Scan barcode" link). 3. Use the following configuration values if the application allows setting them (with links to Google, Microsoft, and Apple). 4. Enter the one-time code provided by the application and click Submit to finish the setup. Below step 4, there are input fields for "One-time code *" and "Device Name", and a "Submit" button.

After clicking the link you will be presented a window that shows you the secret key in clear text. Copy this key and save it in a place where your program can use it. Then run this program to obtain a passcode (a six digit number). Transfer this passcode to the form. Note that the passcodes have a lifespan of 30 seconds, so you might need to regenerate a new passcode if the 30 sec. timeslot has passed.

Since you are now setting up 2FA for the first time, you may also type in a name for the device from which you are getting the passcodes. It is merely a tag for later use. Having filled in all required fields, you continue to **Submit** the next form.

Now follow the steps from section [Remaining Setup](#)

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

Permanent link:
<https://helpdesk.lorentz.leidenuniv.nl/wiki/doku.php?id=services:2fa:computer&rev=1615114529>

Last update: **2021/03/07 10:55**

