

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 (<https://keepassxc.org> GUI) or,
- oathtool (<https://www.nongnu.org/oath-toolkit/> GNU/Linux cmd line) or,
- OTP Manager (<https://apps.apple.com/us/app/otp-manager/id928941247> MacOS)
- WinOTP or OTP manager for Windows

or any softwares that implements OTP standards.

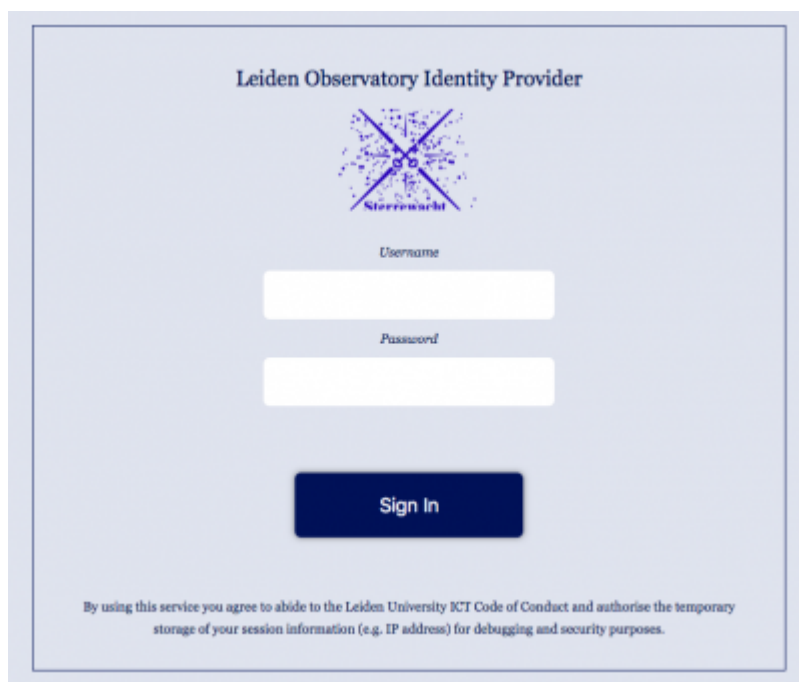


Figure 1: 2FA Login screen (Click image to enlarge).

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.



Leiden Observatory Identity Provider

You need to set up Mobile Authenticator to activate your account.

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.

[Unable to scan?](#)

Provide a Device Name to help you manage your OTP device.

(Six digit) One-time passcode *

Device Name

Submit

Figure 2: 2FA setup secret key form QR code version (Click image to enlarge).

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?](#)

Leiden Observatory Identity Provider

You need to set up Mobile Authentication to activate your account.

1. Install one of the following applications on your mobile:
 - FIDO2
 - Google Authenticator
2. Open the application and enter the key:

PR0WUMBS3QJRM0NRY0RIE04EN09XDCT1U

[Scan barcode?](#)
3. Use the following configuration values if the application allows setting them:
 - FIDO2 (FIDO2)
 - Algorithm: SHA1
 - Issuer: Leiden
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 3: 2FA setup secret key form clear text version (Click image to enlarge).

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.physics.leidenuniv.nl/wiki/> - **Computer Documentation Wiki**

Permanent link:
<https://helpdesk.physics.leidenuniv.nl/wiki/doku.php?id=services:2fa:computer&rev=1615399769>

Last update: **2021/03/10 18:09**

