

First-time 2FA Setup via a Smart Phone

Preliminary Actions

You need to install an *app* on your Smart Phone 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 Software apps such as [FreeOTP](#) (download links below), but you are free to choose any apps that implement the open OTP standards.



Other mobile apps known to work with our system are *google authenticator* and *andOTP*. However, any app implementing the open TOTP standard will do.



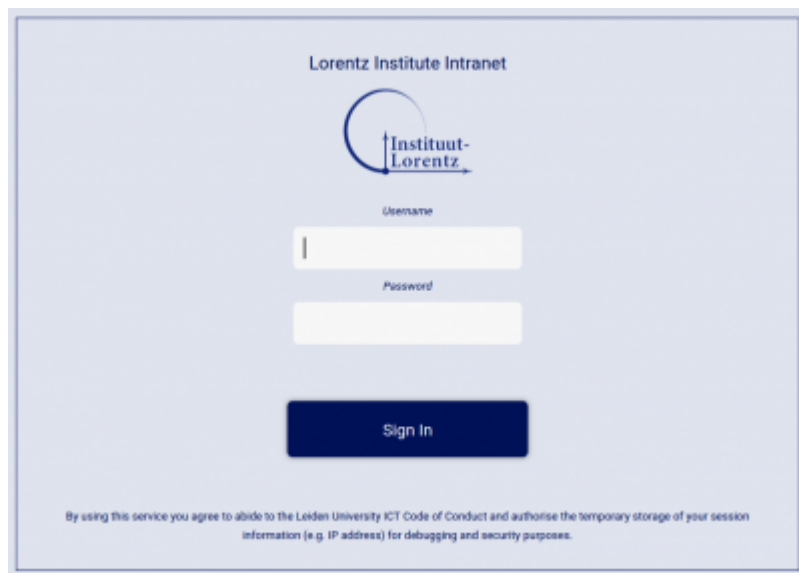
Leiden University suggests the use of the [NetIQ Advanced Authentication App](#) for 2FA. Should you want to install this proprietary software, you should know that the [QR codes generated by this app differ](#) from those generated by Free TOTP apps and can lead to 2FA problems if you scan a NetIQ-generated QR code with a Free app.

Setup

Step 1

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

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

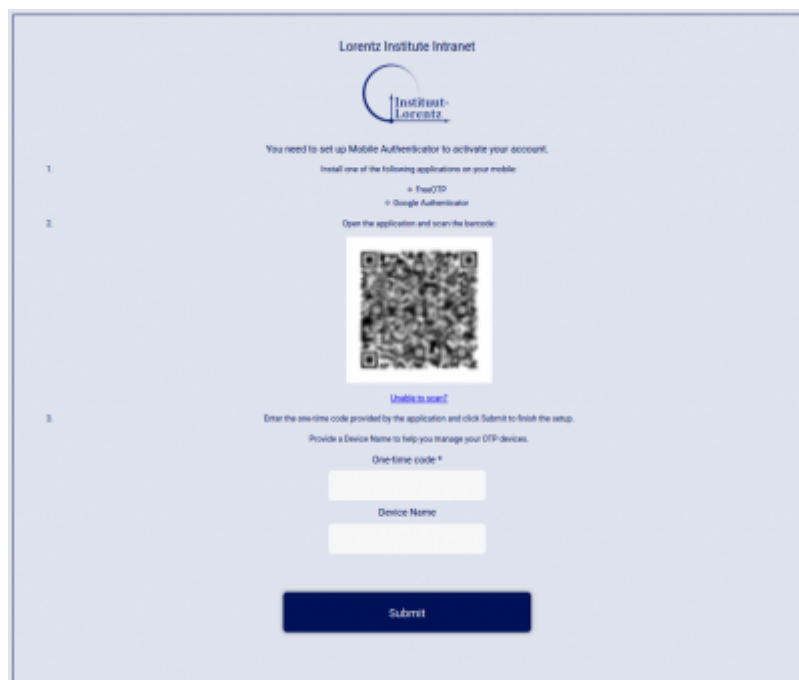


The image shows the login page of the Lorentz Institute Intranet. At the top, it says "Lorentz Institute Intranet" and features the "Instituut-Lorentz" logo. Below the logo are two input fields: "Username" and "Password". A dark blue "Sign In" button is positioned below the password field. At the bottom, there is a small disclaimer: "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 (a.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 to be scanned via your OTP mobile app (Figure 2). The QR code contains your shared **secret key** and other useful information regarding the OTP algorithm used by the IL authentication infrastructure.



The image shows the TOTP Setup Page. It starts with the "Lorentz Institute Intranet" header and logo. The main text says: "You need to set up Mobile Authenticator to activate your account." Below this, it lists two steps: 1. "Install one of the following applications on your mobile:" with options "FreeOTP" and "Google Authenticator". 2. "Open the application and scan the barcode:" followed by a QR code. Below the QR code is a link "Unable to scan?". Step 3 says: "Enter the one-time code provided by the application and click Submit to finish the setup." Below this, it says "Provide a Device Name to help you manage your OTP devices." and has two input fields: "One-time code *" and "Device Name". A dark blue "Submit" button is at the bottom.

Figure 2: TOTP Setup Page (QR code deliberately blurred)

Step 3

Open your OTP app and scan the QR code. Your secret key will now be stored on your phone and a new entry called **Lorentz Institute Intranet** with its corresponding TOTP will be created in your app (Figure 3). Insert this TOTP in the *One-time code* form input and, if you wish, a label in the form input

called *Device Name*. This label is meant to help you keep track with which device the **secret key** has been shared. Click on *Submit*.

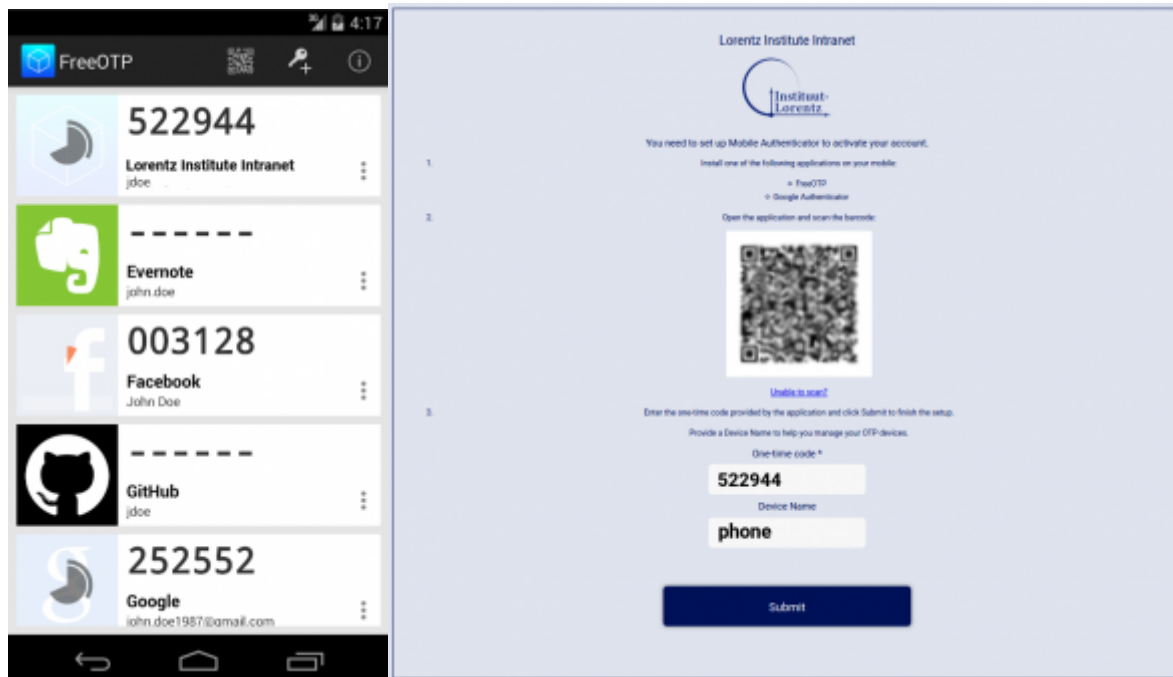


Figure 3: FreeOTP entry for **Lorentz Institute Intranet** and its corresponding TOTP. Upon expiration, a new TOTP will be automatically generated (left). 2FA Setup page with TOTP and label inserted (right).

Step 4

If Step 3 succeeds (errors might occur if there is too much lag time, i.e. the OTP expired), the system will send you an email to your private (not @lorentz) e-mail address with [precise instructions](#) on how to verify your identity. If your identity cannot be validated, you will not be granted access to the system.

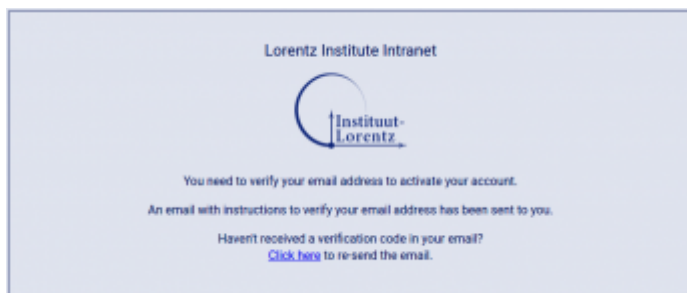


Figure 4: Verify your private email address.

Step 5

Verify your identity by visiting your private email inbox. You should have received an email from the Lorentz Institute Identity Provider ¹⁾. Open that email and copy (for instance using on most platforms Control-C or right-mouse click copy) the secret code in the body of the message. Visit <https://www.lorentz.leidenuniv.nl/idp/> and paste (on most platforms Control-P or right-mouse click paste) the secret code in the white text area. Click on 'Submit'. Your identity is now verified.

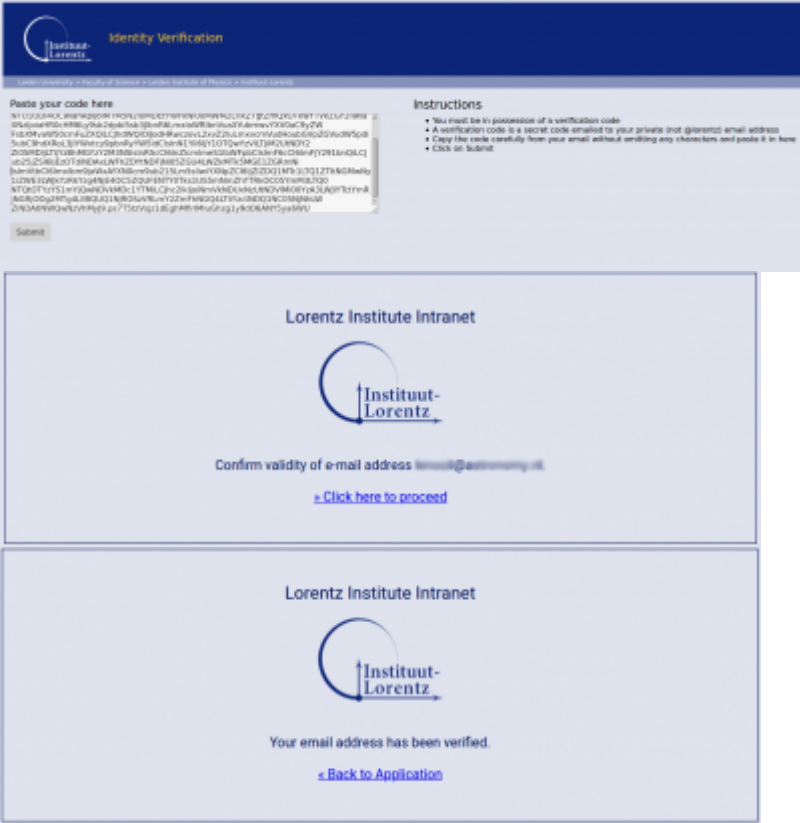


Figure 5: Screenshot of e-mail verification process.

Step 6

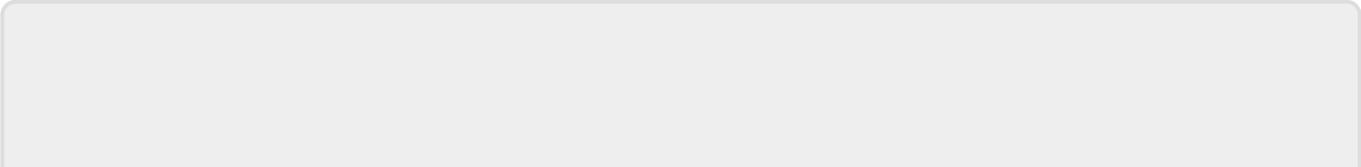
Click on *Back to application* to redirect your browser to the Lorentz Institute SSO web application from which you started the whole process or close the browser. Your setup is complete.

Problems and Solutions

I cannot setup 2FA/access the system	Make sure we have your private email address on record
I lost my smartphone/PC with my OTP secret	Notify support@lorentz.leidenuniv.nl Change your IL credentials
How do I disable 2FA?	2FA is mandatory on all SSO web services and to access our SSH server
My TOTP is incorrect	Make sure your phone's (PC's) clock is synchronised to the SSH server time and you scanned/copied all TOTP settings correctly
My OTP secret is compromised	Notify support@lorentz.leidenuniv.nl Change your IL credentials

1)

Details of this email are not disclosed here to prevent phishing.



From:

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

Permanent link:

https://helpdesk.physics.leidenuniv.nl/wiki/doku.php?id=institute_lorentz:2fa-smartphone&rev=1617289003

Last update: **2021/04/01 14:56**

