

University MFA Made Easier

This document explains how you can set up the University MFA (NetIQ) system to use your **FreeOTP** or **GoogleAuthenticator** app as the generator of secure codes. In this way, you will be able to use the same app for logging in to the institute and university services. This setup has to be done through the university account services and will enable so-called TOTP authentication. Follow the steps below to set up UL MFA for TOTP.

[Note on acronyms](#)

Steps to Enable TOTP

Access UL Account Services



You need to login to the university account services at <https://account.services.universiteitleiden.nl>. Use your ULCN account credentials for this.

This is followed by any MFA authentication that you may have chosen in the past.

Select the MFA Option



On the Account Services page you will find near the bottom left of the page a tile denoting Multi-Factor Authentication. Select this tile by clicking on it to go to the setup of MFA additional options. You do need to login again using your ULCN credentials...

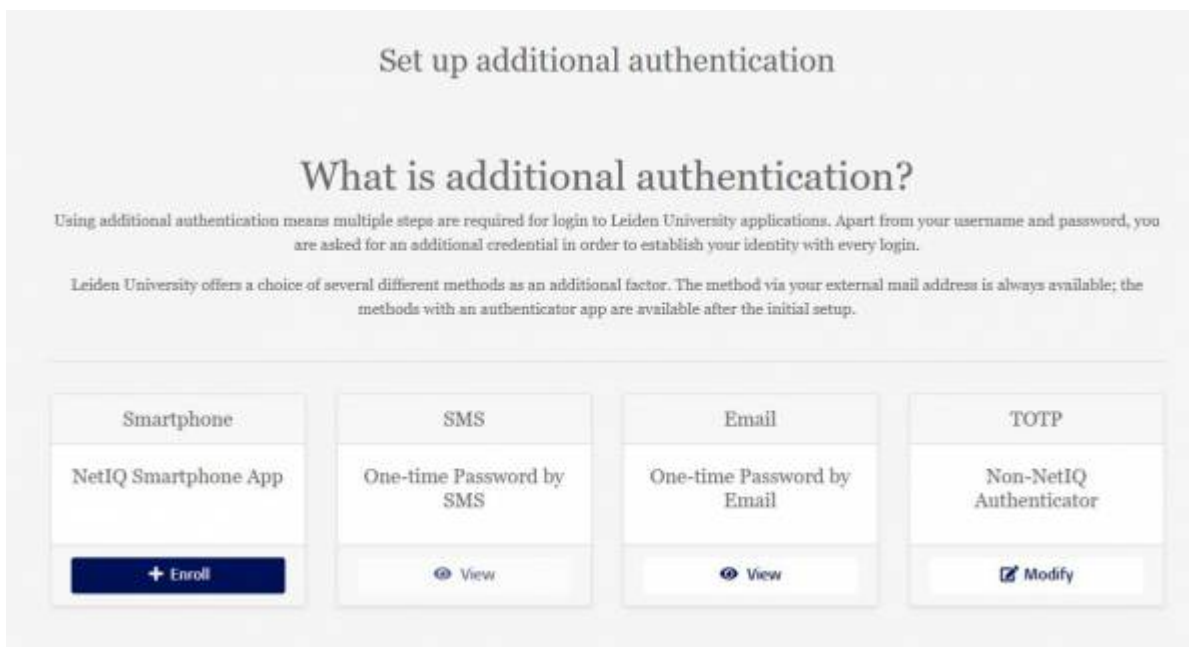
MFA selection page



After entering your ULCN credentials you again need to choose the MFA type to allow you to continue logging in. In this case

not all options are visible as the test account has not enrolled NetIQ, so you only see the three remaining options, by email or by SMS should always be there. Choose an option and provide the associated security code.

Chose MFA option

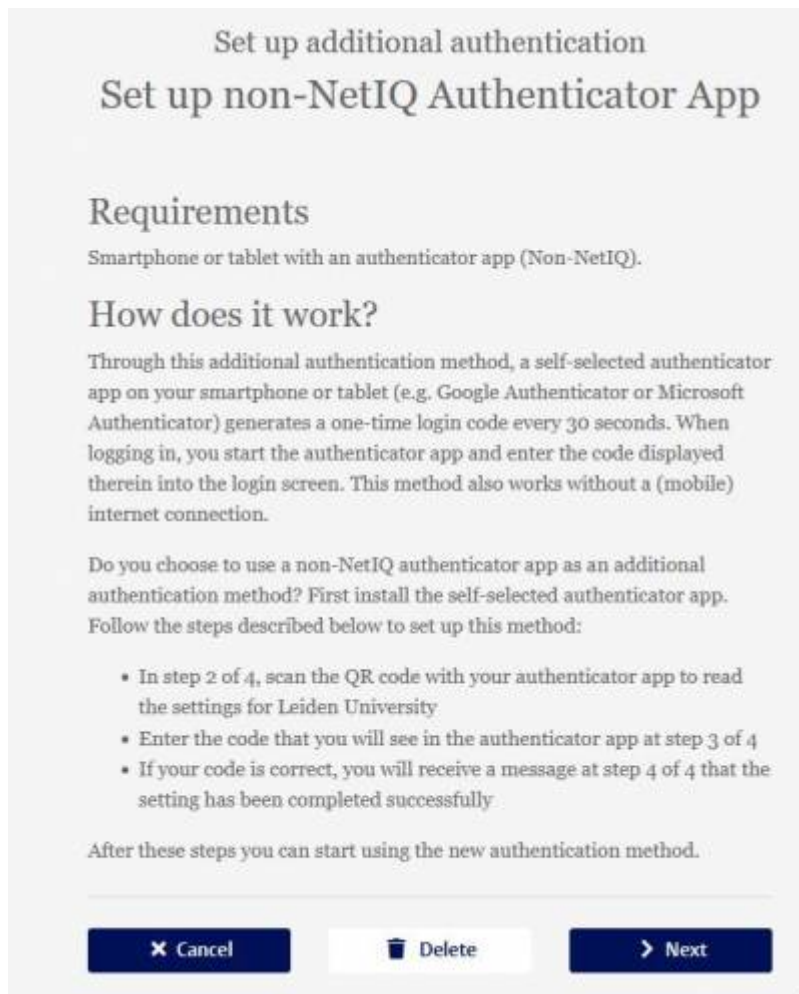


After that you will end up on the NetIQ selection page. That page shows all the options you may choose for authentication. In this example you see that NetIQ is not

previously selected. In your case the blue button may be a 'Modify' button, as is visible under the TOTP block on the right in this example.

In case you have the 'Install' button below the TOTP block, you may click that to set up a non-NetIQ authenticator app. You will be directed to a new page:

Set TOTP authentication



The screenshot shows a web interface for setting up additional authentication. The title is 'Set up additional authentication' followed by 'Set up non-NetIQ Authenticator App'. Under 'Requirements', it states 'Smartphone or tablet with an authenticator app (Non-NetIQ)'. The 'How does it work?' section explains that a self-selected authenticator app generates a one-time login code every 30 seconds. It then asks if the user wants to use a non-NetIQ authenticator app as an additional method, instructing them to install the app and follow the steps. A bulleted list details the steps: scanning a QR code, entering the code, and receiving a confirmation message. At the bottom, it says 'After these steps you can start using the new authentication method.' and provides three buttons: 'Cancel', 'Delete', and 'Next'.

Set up additional authentication

Set up non-NetIQ Authenticator App

Requirements

Smartphone or tablet with an authenticator app (Non-NetIQ).

How does it work?

Through this additional authentication method, a self-selected authenticator app on your smartphone or tablet (e.g. Google Authenticator or Microsoft Authenticator) generates a one-time login code every 30 seconds. When logging in, you start the authenticator app and enter the code displayed therein into the login screen. This method also works without a (mobile) internet connection.

Do you choose to use a non-NetIQ authenticator app as an additional authentication method? First install the self-selected authenticator app. Follow the steps described below to set up this method:

- In step 2 of 4, scan the QR code with your authenticator app to read the settings for Leiden University
- Enter the code that you will see in the authenticator app at step 3 of 4
- If your code is correct, you will receive a message at step 4 of 4 that the setting has been completed successfully

After these steps you can start using the new authentication method.

This is the first step/page of four to enable the TOTP function. In your case you might not see the 'Delete' button and can directly continue to 'Next'.

The bottom paragraph explains to you in detail the next steps. Follow those steps and you will end up with TOTP as a viable authentication method. If you are shown the QRCode, take your phone's app (FreeOTP or Google Authenticator) and scan the code.

Once all this is done you can use your preferred TOTP application (FreeOTP or Google Authenticator) as the MFA step in any of the university web applications.

From now on you can use the same app for Sterrewacht 2FA and University MFA.

Configure FreeOTP

In order for you to quickly see which entry in FreeOTP belongs to which system, you can insert an icon to each block in FreeOTP. First you need to download the icons we have prepared for you:

1. Sterrewacht 
2. University 
3. Institute Lorentz 

Then in FreeOTP you click the three dots on the right and choose option: 'Edit'. Click on the icon (on the left) and now you go to the place where you saved the icon on your phone. Select the file and it will be permanently display on the left side of the Authentication block.

Note: For those that have recently scanned the QRCode for the Observatory, your Authenticator block should already use the strw.png icon.



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

Permanent link:
https://helpdesk.lorentz.leidenuniv.nl/wiki/doku.php?id=univ:mfa_easier&rev=1642079668

Last update: **2022/01/13 13:14**

