Setting up two-factor authentication on student's web interface

A so-called two-factor identification service was introduced in order to increase the security of access to student's interface of Neptun study system of the University of Debrecen.

Two-factor authenticator identification means that after entering Login name and Password, a 6-digit code generated by an Authenticator (authentication application) must also be entered at each login.

Steps to set up two-factor authentication:

1. Download Authenticator (authentication application) to smartphone/computer

↓

2. Registration, setting up two-factor authentication

↓

3. Using Authenticator (authentication application) (enter code each time you log in)

1. Download Authenticator (authentication application)

Install one of the Authenticators recommended below on your smartphone/computer.

For smartphone:

Google Authenticator:

- Android: https://play.google.com/store/search?q=google+authenticator&c=apps&hl=hu
- iOS: https://apps.apple.com/hu/app/google-authenticator/id388497605

Microsoft Authenticator:

- Android: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=hu
- iOS: https://apps.apple.com/hu/app/microsoft-authenticator/id983156458?l=hu

For computer:

FortiToken:

- Windows: https://apps.microsoft.com/store/detail/fortitoken-windows/9P0TDH1J7WFZ?hl=en-us&gl=us
- macOS: https://apps.apple.com/us/app/fortitoken-mobile/id500007723

Step Two:

- https://steptwo.app/ An application available only for macOS, in which the two-factor key can be registered in a similar way to FortiToken.

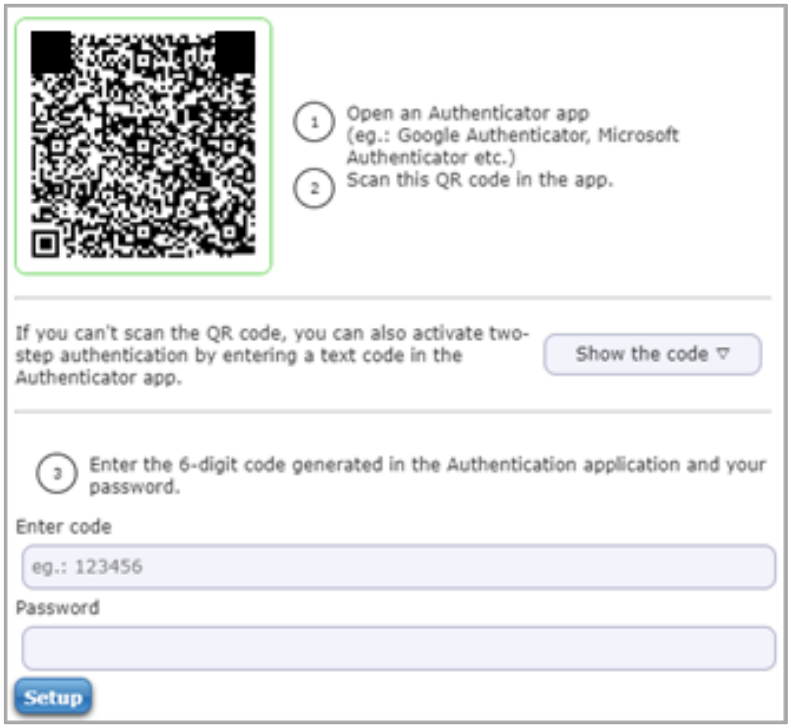
Installation and use of the listed applications is free!

2. Registration, setting up two-factor authentication

2.1. Setting up two-factor authentication in Neptun

According to point 1, it is necessary to install one of the recommended authenticators.

When log in Neptun, after entering your Login name and Password, the following two-factor authentication registration window appears on the student's login page:



Two-factor registration after login

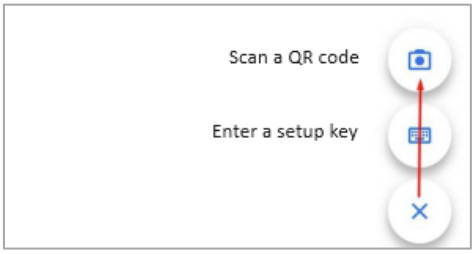
The displayed QR code must be scanned with the Authenticator (Authentication application) chosen and downloaded to smartphone, thereby registering the key in the Authenticator. Instead of scanning the QR code, by clicking the "**Show the code**" button, a copyable QR code will appear in the field, which can be copied into the Authenticator downloaded to computer. *(We can log in Neptun on any number of devices if we use Authenticator installed on smartphone, so it is advisable to choose instead of Authenticator installed on computer, where the copyable QR code needs to be saved/preserved and copied to the Authenticator installed on the computers.)* The Authenticator then generates a 6-digit code every half minute. After successful registration, enter the **current** 6-digit code in the "**Enter code**" field. In the "**Password**" field enter your **login password** to finalize it.

This registration needs to be done once. Every time you enter Neptun, after entering your Login name and Password, you must also enter the **current** 6-digit code received in the Authenticator! The authentication application can be closed after entering the code, it does not need to run continuously.

2.2 Using authenticators, setting up two-factor authentication

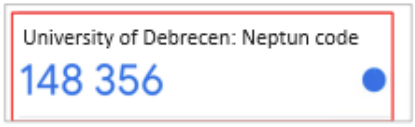
On smartphone using Google Authenticator:

After we have successfully installed the application on our smartphone, open it, then click on the + sign at the bottom right and select the "Scan QR code" option.



Create key

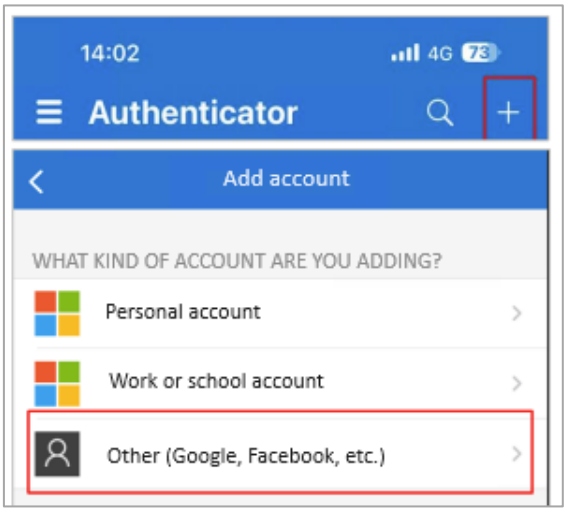
Code generation starts immediately after scanning the QR code. The name of the key will be "University of Debrecen" and the user's Neptun code.



Key name and generated code

On smartphone using Microsoft Authenticator:

Open the application, then click on the + sign on the right side and select the option "Other (Google, Facebook, etc.)" from the options that appear.



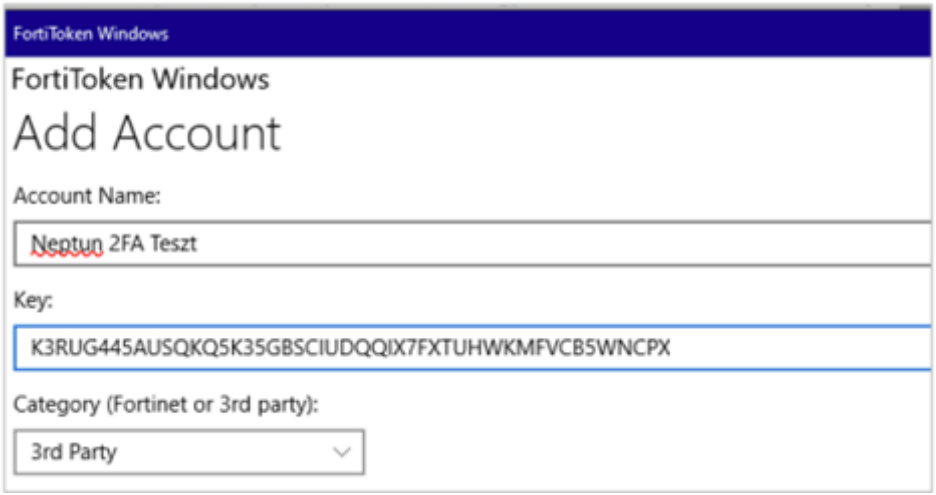
Create key

Code generation starts immediately after scanning the QR code. The name of the key will be "University of Debrecen" and the user's Neptun code.

Key name and generated code

On computer using FortiToken:

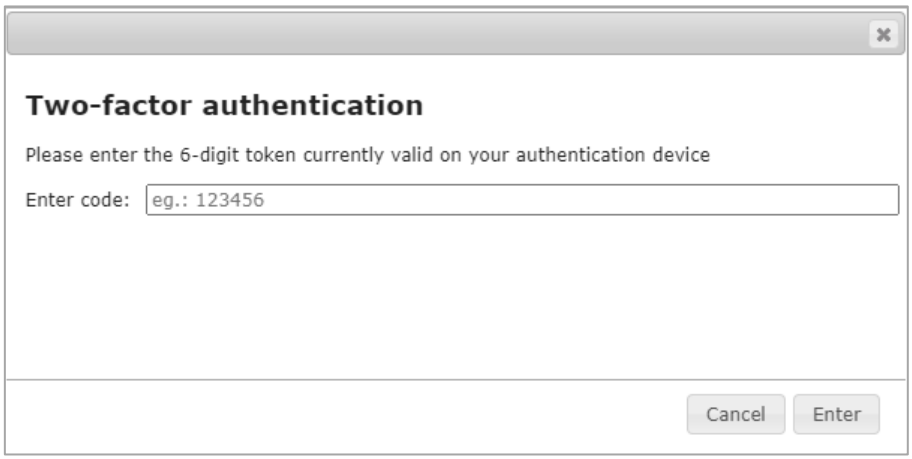
After download, you need to open the **FortiToken** application. The setting can be started by clicking the "+ Add" button in the lower right part of the interface. The "Account Name" field can be filled freely, this will be the name of the key. In the "Key" field, we must enter the copyable QR code that appears in the Neptun registration window when we click the "Show code" button. In the "Category (Fortinet or 3rd party)" field, select "3rd Party". After that, click on the "✓ Done" button in the lower right part of the interface.



Filling in data

3. Using the Authenticator (authentication application) (enter code each time you log in)

After the two-factor authentication has been successfully set, each time you log in, after entering your Login name and Password, the "Two-factor authentication" pop-up window will appear on the student's web login interface, in which the **current** 6-digit code generated in the previously successfully registered Authenticator must be entered.
To enter, click the "Enter" button.



Enter code

4. Other information, technical conditions, help

Terms of the two-factor authentication service:

- **Google Authenticator** is available for iOS version 13.0 or higher, Android version 4.4 or higher. **Microsoft Authenticator** is available on iOS version 11.0 or higher, Android version 6.0 or higher. **FortiToken** is available on Windows 10 version 14393.0 or higher, macOS 11.0 or higher.
- Internet connection on the device running the Neptun Study System. Internet connection is also required to install the chosen Authenticating application, but it is not required for key registration and 6-digit code generation.
- Smartphone (Android or iOS device) or computer
- Availability of an authentication application on the device chosen in point 1
- Student authorization in the DE Neptun system

What you need to pay attention when using two-factor authentication:

- When buying a new device, if the applications are not transferred to the new device, it is necessary to delete the two-factor authentication and then register it again on the new device. Delete authentication must be requested at the following email address: neptun@unideb.hu
- When registering again, the previous account must be deleted in the Authenticator.
- Enter the generated code correctly! If you make a typo, you will not be able to enter.
- We can log in Neptun on any number of devices if we use Authenticator installed on smartphone, so it is advisable to choose instead of Authenticator installed on computer, where the copyable QR code needs to be saved/preserved and copied to the Authenticator installed on the computers.
- Users who have access to several Neptun services (teacher's, student's, client administrator's) will have access to all interfaces with the code generated when registering through one interface. Authentication registration only needs to be done once.
- After unsuccessful registration, if the window containing the QR code has already been closed, but the corresponding account has already been created in our chosen authenticator application, then before re-registration the previously created code account must be deleted in the application, because it will no longer be valid and usable.

Technical assistance:

If you need technical assistance with two-factor authentication, please report the problem in detail, attach screenshot and indicate your **Neptun code** to the following e-mail address: neptun@unideb.hu