Table of contents

1. 2 FACTOR AUTHENTICATION

Due to the current developments regarding cybercrime, we are forced to improve the security of our systems and web applications, and thus the protection of privacy-sensitive information. To achieve this, we need your cooperation!

2 factor authentication is an extra layer of security designed to ensure that you are the only person who can access your account, even if someone knows your password.

1.1 HOW 2 FACTOR AUTHENTICATION WORKS

As described above, 2 factor authentication ensures that only you have access to your account. When you log in, you will be asked for your username, password, and a six-digit verification code.

The six-digit verification code is generated by an authentication app. This code is valid for 30 seconds before a new code is generated. This significantly reduces the chances of malicious people accessing your account.

There are several authentication apps available for download for IOS and Android users. The most well-known are: Google Authenticator and Microsoft Authenticator.

The downloadable authentication apps are free and fully Dutch. They are also available in other languages.

Note: although the 2 factor authentication ensures that an additional layer of security is added, the combination of a strong password and 2 factor authentication is particularly important. Make sure that your password contains at least 15 characters. Include uppercase and lowercase letters, numbers and symbols in your password to make it difficult for malicious people to figure out your password.

2. GOOGLE AUTHENTICATOR

As mentioned, there are several authentication apps available. To get you started, in this guide we explain how to install Google Authenticator step-by-step. You can also choose to download another authentication app.

The Google Authenticator is a free app that you can install on your smartphone or tablet and generates a six-digit code. NB you cannot install this app on your PC.

After logging into a website or app that requires 2 factor authentication, you can enter the code from the Google Authenticator.
In your case, after logging in with your username and password, Nmbrs will ask for the additional code via your web browser. Here you enter the six-digit verification code generated by the Google Authenticator. How you receive this six-digit verification code, we explain below.

2.1 INSTALLATION GOOGLE AUTHENTICATOR

To use Google Authenticator, you need at least Android version 4.4 or an iPhone 3G.

Tip: Make sure you are connected to a Wifi network prior to downloading the app, to avoid any Internet connection fees.

Step 1
Download the Google Authenticator app on your smartphone or tablet. It is available for Android in the Google Play Store and for IOS users in the App Store.

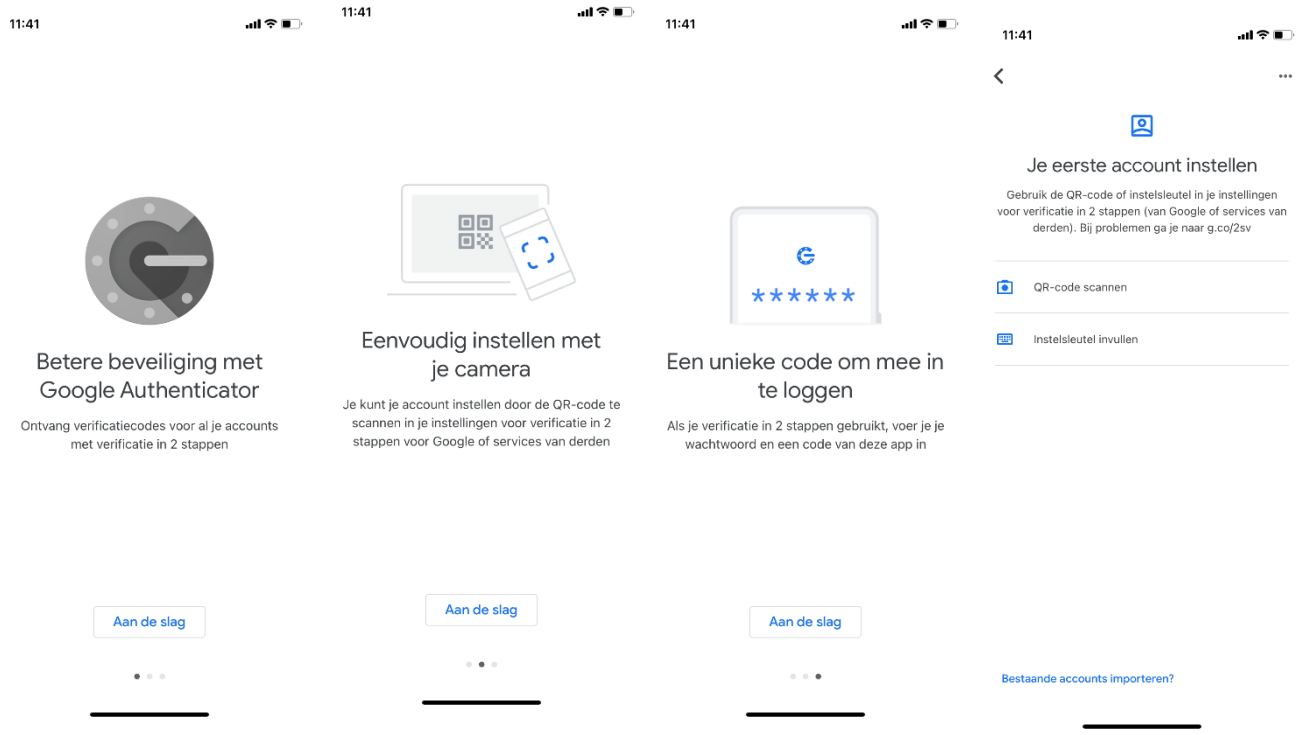
Once you have downloaded the Google Authenticator app, click on the Google Authenticator app icon on your smartphone or tablet to launch the app.

Step 2
When you use the Google Authenticator app for the first time, click 'Get started'. You will then click on 'Scan QR Code'. See images below:

If you do not already have an app on your tablet or phone that allows you to scan a QR code, you may now be asked if you would like to download and install such an app now.

There are several QR code scanners available in the PlayStore or Apple Store and all with the same purpose. So it doesn't matter which one you download.

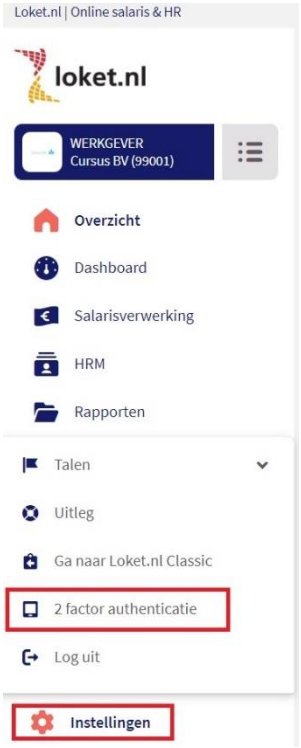
Your tablet or smartphone may ask you to give Google Authenticator access (authorize) to your camera, for scanning a QR code.



3 2 Factor authentication in Loket.nl

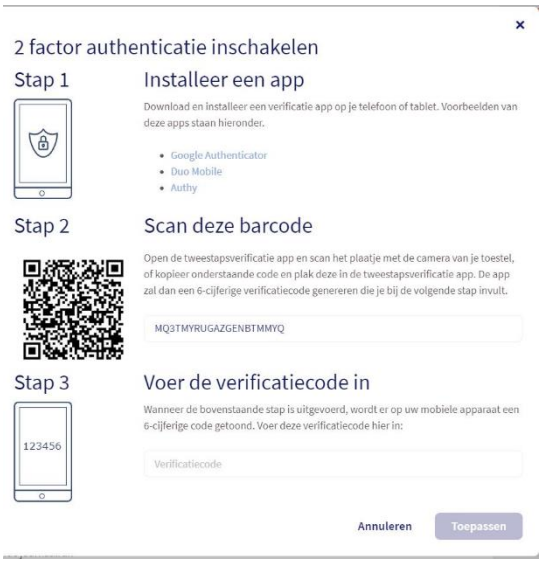
3.1 2 factor authentication for employers

3.1.1 Activation in Loket.nl



All Loket.nl users have the option to activate the extra security for logging in. The new menu option '2 factor authentication' appears at the bottom left via the 'Settings' button.
See left image.

Do you choose this menu option? Then the following screen appears, see image on the right:



Go through the procedure once and 2 factor authentication is activated for you. You will receive a notification in the top right corner of your screen.

3.1.2 Logging into Loket.nl

Once you have logged in and entered your username and password, this screen appears, see right:

Enter the code that you can find in the app installed on your mobile device. The code generated in the app is valid for a limited time.

3.1.3 Remember this device 30 days

If you check the option 'Remember this device for 30 days' the browser of the device you are logging into will remember the login for 30 days so you do not have to enter the verification code each time. Please note that this feature only works on the device you are currently working on.

3.1.4 Deactivating 2 factor authenticator in Loket.nl

Do you no longer want to use the 2 factor authentication option? Click on the 'settings' button in the left-hand corner and click on '2 factor authentication. The screen below appears. Enter the code generated by the app and click on the save button.

Given the developments written in the introduction of this document, we do not recommend disabling 2 factor authentication.

3.2 Are you unable to log in anymore?

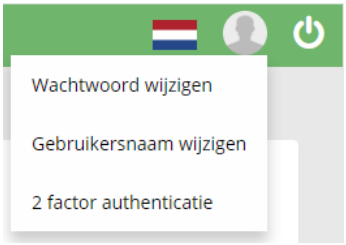
Please contact us at hrs@crowefoederer.nl.

3.2 2 factor authentication for employees (Employee counter)

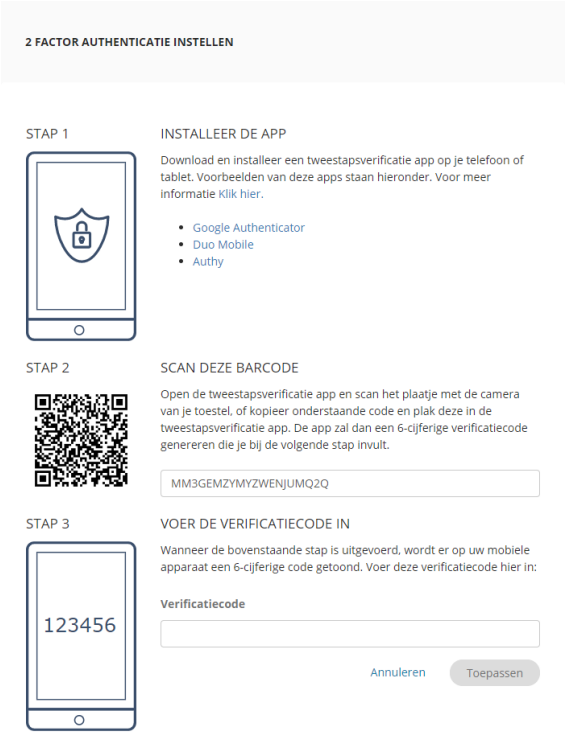
In the Employee counter it is possible to log in via 2 factor authentication for extra security of your access. In addition to entering your username and password, you will need your cell phone or tablet to perform the additional security step when logging in.

3.2.1 Activation in the Employee Desk

All users of the Werknemerloket will be given the option to activate the additional security for logging in. In the top right corner under the icon of a person (silhouette) the new menu option 'Two factor authentication' appears.



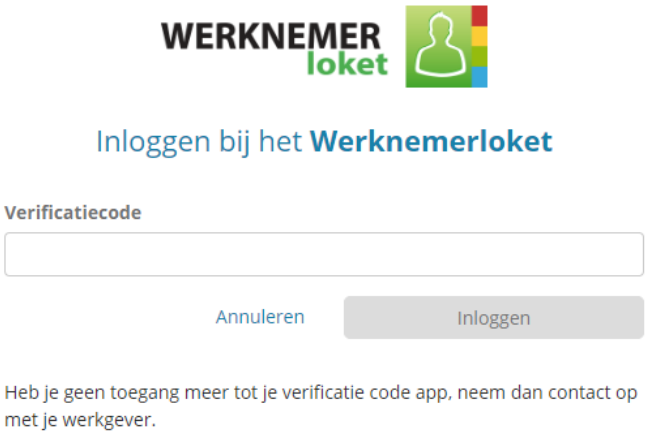
If you choose this menu option, the following roadmap will appear:



Go through this procedure once and 2 factor authentication is activated for you.

3.2.2 Werknemerloket login

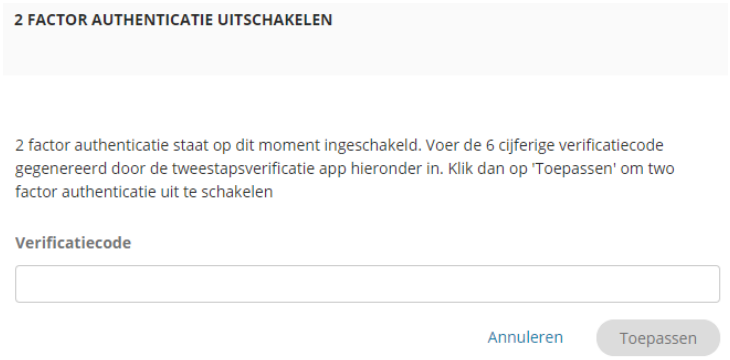
Once you log in and have entered your username and password, the screen below will appear:



Enter the code found in the Google authenticator. Please note that the code generated in the app is valid for a limited time.

3.2.3 Deactivation in the Werknemerloket

Do you no longer want to use the 2 factor authentication option? Click on the silhouette at the top right and then click on '2 factor authentication'. The following screen will appear.



Enter the code generated by Google authenticator
generated code and click 'apply'.

3.2.4 Can't log in anymore?

For whatever reason, you cannot log in anymore with your verification code? Please contact your employer who can turn off the verification so that you can perform the above actions again.

The employer can set the field 'Two-step verification' to 'No' in Loket.nl where he also provides access to the Werknemerloket. Please note: this is only possible when logging in directly to Loket; this is not possible via an SSO link.

As an employee, you can now log in with just your username and password. In the Werknemerloket it is possible to activate the 2 factor authentication again.

F.A.Q.

What does 2 factor authentication mean?
2 factor authentication refers to a security method used to protect accounts and systems from unauthorized access. Users are required to authenticate themselves with a code generated by the authentication app.

2 factor authentication can be used to strengthen the security of a phone, an online account or even a door. It works by requiring two types of information from the user: The first is a password or PIN, and the second is a fingerprint or one-time code sent to your phone.

What is a 2 factor authenticator?
With the 2 factor authenticator, a one-time code is generated to prove a user's identity when they try to access an online account or system. The code is sent via text message to a phone number or email associated with the user. You can only access an account when the 2 factor authentication is entered correctly.

Can a 2 factor authenticator be hacked?
While it is possible to hack 2 factor authenticator, the chance is very small and 2 factor authentication is definitely the best way to keep accounts and systems safe.

One way that 2 factor authentication can be hacked is through the SMS method. This is a method where a one-time code is sent to a user's phone number.

There are stories of hackers tricking cell phone providers into transferring someone else's phone number to their own phone. The hackers contact the providers posing as customers and ask for a new SIM card with the victim's number. They then have access to any authentication code associated with that phone number.

However, this is a rare occurrence. The very small risk of being hacked does not outweigh the benefits of 2 factor authentication. This is and will continue to be a very strong tool in the fight against cyber attacks and identity fraud.

I am switching devices soon. How do I transfer the Google Authenticator?
If you are switching smartphones, please disable pairing via the app before removing it. The authenticator app is tied with your device. On your new smartphone, reinstall the Google Authenticator app and link your account.

I have a problem with the Google Authenticator App and it is not listed here. Where can I find an answer to my question?
If there is an issue with the Google Authenticator App that is not covered above, we recommend you check Google's support site. They may have addressed your question in one of many articles: support.google.com.