Table of contents

1. 2 FACTOR AUTHENTICATION

Current developments in cybercrime are forcing us to improve the security of our systems and web applications, and thus the protection of privacy-sensitive information.

We have been faced with a difficult choice, but eventually came to the conclusion that the disadvantages of 2 factor authentication do not outweigh the advantages. We would like to inform you that from Monday, April 4, 2022, you will only be able to log into Nmbrs with 2 factor authentication.

A 2 factor authentication is an additional 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.

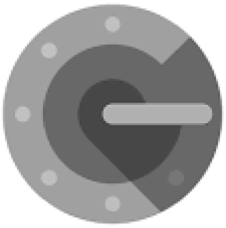
Note: although the 2 factor authentication ensures that an additional layer of security is added, the combination of a strong password and 2 factor authentication is particularly important. Make sure that your password contains at least 15 characters. Include uppercase and lowercase letters, numbers 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.

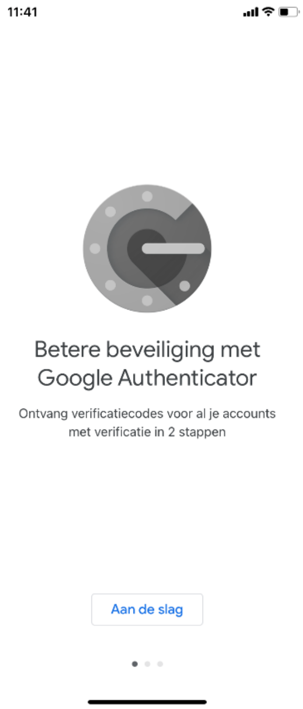
Tip: Make sure you are connected to a Wifi network prior to downloading the app, to avoid any Internet connection fees.

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:

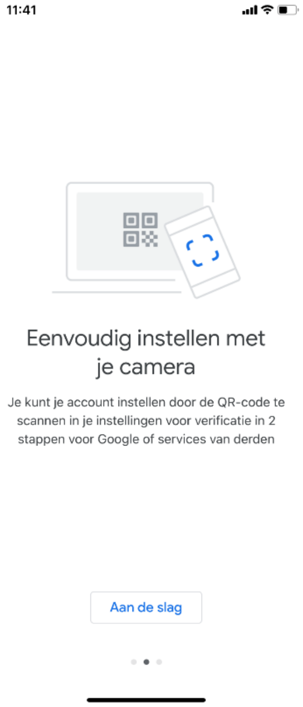


11:41

Betere beveiliging met Google Authenticator

Ontvang verificatiecodes voor al je accounts met verificatie in 2 stappen

Aan de slag

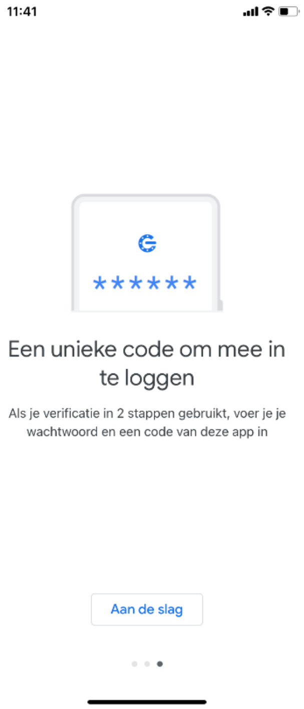


11:41

Eenvoudig instellen met je camera

Je kunt je account instellen door de QR-code te scannen in je instellingen voor verificatie in 2 stappen voor Google of services van derden

Aan de slag

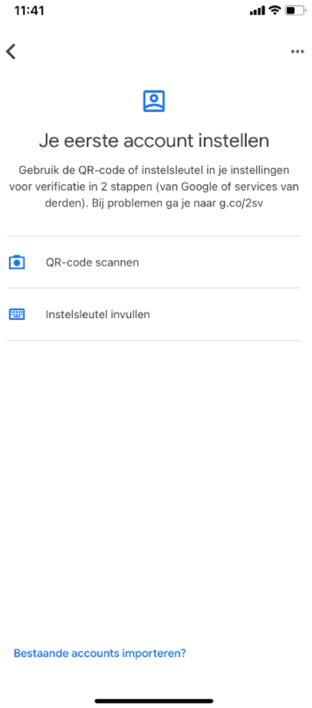


11:41

Een unieke code om mee in te loggen

Als je verificatie in 2 stappen gebruikt, voer je je wachtwoord en een code van deze app in

Aan de slag



11:41

Je eerste account instellen

Gebruik de QR-code of instelsleutel in je instellingen voor verificatie in 2 stappen (van Google of services van derden). Bij problemen ga je naar g.co/2sv

QR-code scannen

Instelsleutel invullen

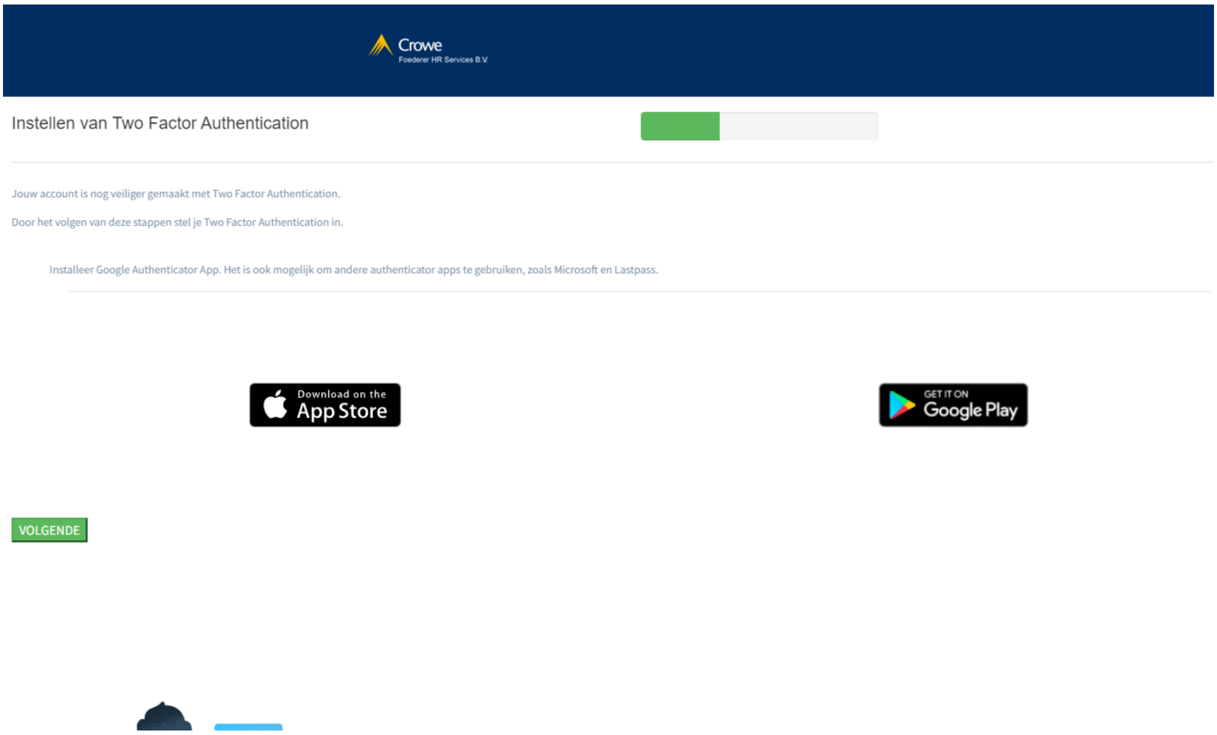
Bestaande accounts importeren?

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.

If you are logging into Nmbrs for the first time, you will see the following screen. You will be given the option to download an authentication app if you do not already have one.



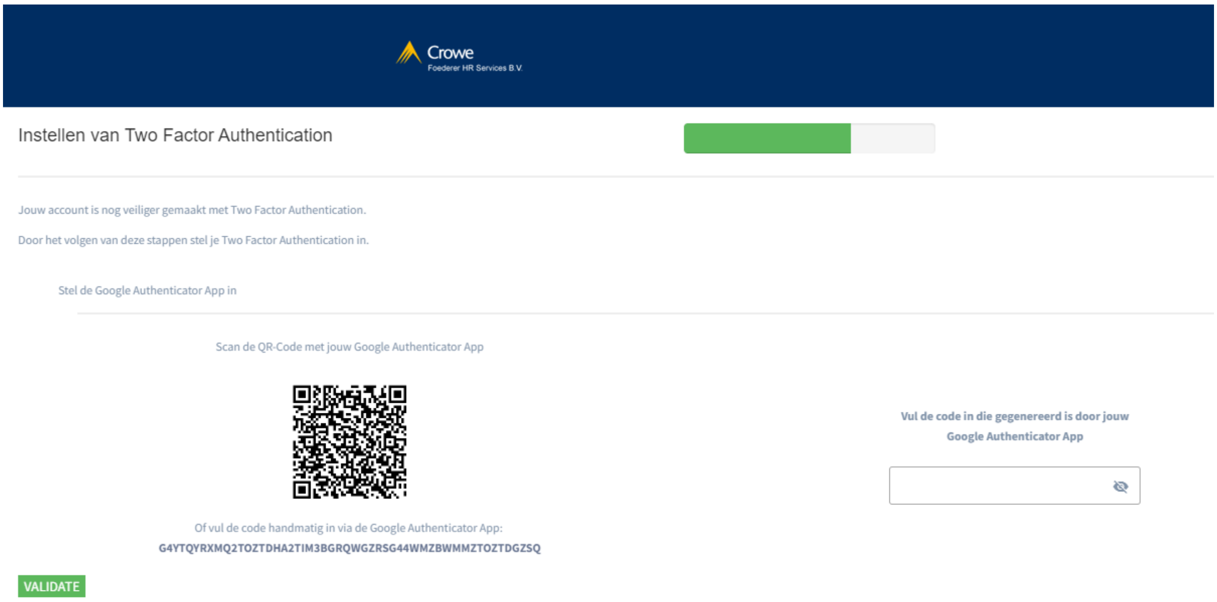
Instellen van Two Factor Authentication

Jouw account is nog veiliger gemaakt met Two Factor Authentication.

Door het volgen van deze stappen stel je Two Factor Authentication in.

Installeer Google Authenticator App. Het is ook mogelijk om andere authenticator apps te gebruiken, zoals Microsoft en Lastpass.

You will see the screen below. On it, at the bottom left of the page is the QR code that you can scan and below it is the code that you can enter manually if you choose to set an 'Institution Key'.



Instellen van Two Factor Authentication

Jouw account is nog veiliger gemaakt met Two Factor Authentication.

Door het volgen van deze stappen stel je Two Factor Authentication in.

Stel de Google Authenticator App in

Scan de QR-Code met jouw Google Authenticator App

Of vul de code handmatig in via de Google Authenticator App:
G4YTQYRXMQ2TOZTDHA2TIM3BGRQWGZRSG44WMZBWMMZTOZTDGZSQ

Vul de code in die gegenereerd is door jouw Google Authenticator App

Step 3
Once the QR code is on your screen, hold the phone in front of the screen such that the QR code fits within the red lines on your screen. Once the QR code is scanned, you will see a 6-digit code on your screen.

Then click on 'Done' or 'Validate'.

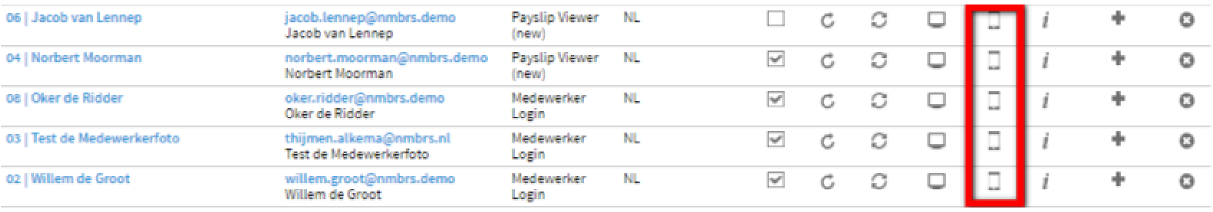
You do not need to write down the code generated now, as the code changes every 30 seconds. If you press the code, you copy this code. This makes it easy to use in other apps, by simply 'pasting'.
If you are using the web browser, you will need to enter the six-digit code manually.

2.2 DAILY USE

When you boot up and start the Nmbrs application, you will need to enter your username, password and a code generated by the Google Authenticator. Once you have entered this, you will be redirected to the Nmbrs online environment.

2.3 RESET AUTHENTICATOR APP IN NMBRS

When a user no longer has access to the Authenticator app, a 'reset' can be applied at the login for which it was set up. The user can then link the app to his user again. To do this, click on the phone icon at the user.



06 | Jacob van Lennep	jacob.lennep@nmbrs.demo Jacob van Lennep	Payslip Viewer (new)	NL	☐	↻	⟳	▭	📱	i	✚	⊗
04 | Norbert Moorman	norbert.moorman@nmbrs.demo Norbert Moorman	Payslip Viewer (new)	NL	☑	↻	⟳	▭	📱	i	✚	⊗
08 | Oker de Ridder	oker.ridder@nmbrs.demo Oker de Ridder	Medewerker Login	NL	☑	↻	⟳	▭	📱	i	✚	⊗
03 | Test de Medewerkerfoto	thijmen.alkema@nmbrs.nl Test de Medewerkerfoto	Medewerker Login	NL	☑	↻	⟳	▭	📱	i	✚	⊗
02 | Willem de Groot	willem.groot@nmbrs.demo Willem de Groot	Medewerker Login	NL	☑	↻	⟳	▭	📱	i	✚	⊗

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.