Registration on AFM Portal

Manual (English)

Publication date: 09 November 2026 (version 3.0)
Classification: AFM – Public

The Dutch Authority for the Financial Markets

The Dutch Authority for the Financial Markets (AFM) is committed to promoting fair and transparent financial markets.

As an independent market conduct authority, we contribute to a sustainable financial system and prosperity in the Netherlands.

Table of Contents

1. Registering and viewing an account 4
    1.1 Registering an account 4
    1.2 Viewing an account 6
    1.3 Forgotten password 6
    1.4 Multi Factor Authentication (MFA) 6
        1.4.1 First time log in 7
        1.4.2 Log in using authenticator code 8
        1.4.3 Resetting Multi-Factor Authentication 8
        1.4.4 Important: Back up your security token 10

2. Linking the account to your company 10

3. Authorisations and environments 13
    3.1 Managing employees 14
    3.2 Viewing authorisations 17

1. Registering and viewing an account

The AFM Portal has an authorisation structure and a permissions structure. The authorisation structure determines which user can grant other users access to certain data. The permissions structure divides the data in the Portal into different environments for different purposes. This manual provides an explanation of these changes as they relate to creating an account for the AFM Portal and assigning the authorisations.

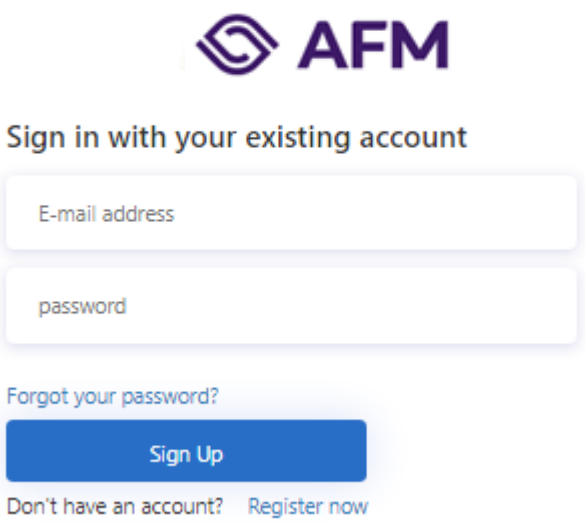
The AFM Portal is available in both Dutch and English: you can set the preferred language in each screen (at the top right). This manual is also available in Dutch.

Please also refer to the frequently asked questions about the AFM Portal on the AFM website.

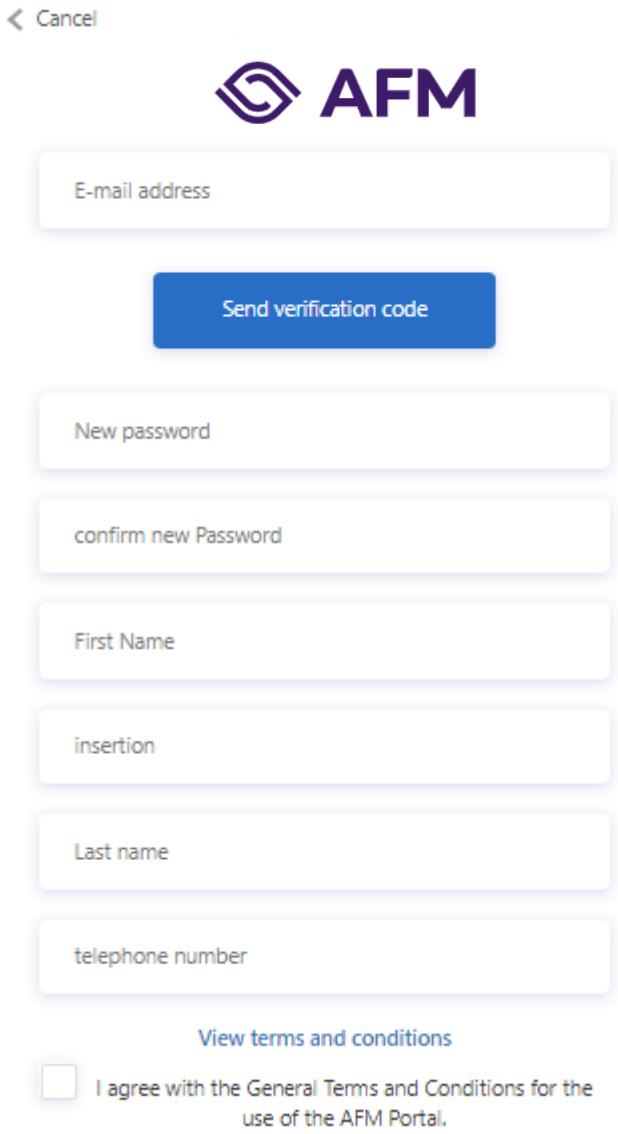
1.1 Registering an account

Go to https://Portaal.AFM.nl.

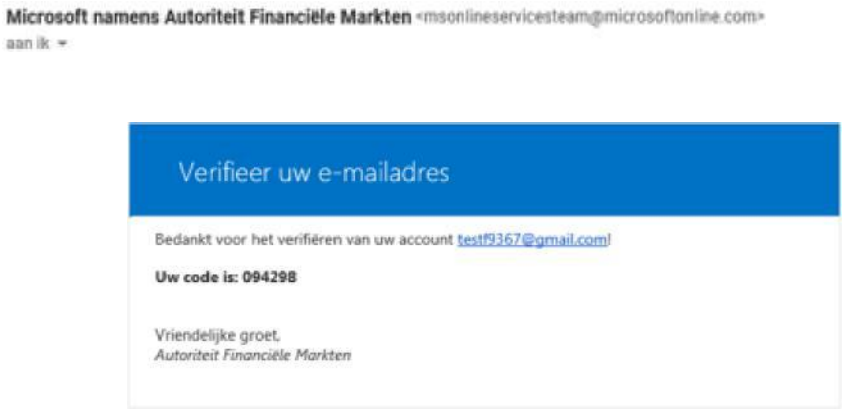
Click ‘Register now’ to register an account.



Enter your email address and click ‘Send verification code’. Please note that this must be a personal business email address, not your company's general email address.



The following email message will be sent to the person who registered. This is an email message from ‘Microsoft on behalf of the Dutch Authority for the Financial Markets’.



Enter the code you received in the ‘verification code’ field on the Portal and click verify code.

Fill in a new password and confirm. New passwords must meet the following requirements.

The password must have a length between 8 and 64 characters.
The password must contain at least 3 of the following characters:
- a lower-case letter
- an upper-case letter
- a numeric character
- a symbol (@ # $ % ^ & * - _ + = [ ] { } | : ' , ? / ` ~ " ( ) ; .)

Also fill in the following fields:

- First name
- Last name
- Prefix
- Telephone number

Read the General Terms and Conditions and tick to agree.

Then click on ‘Create’.

1.2 Viewing an account

After logging in, you can view your data via the ‘View data’ option, which appears as a drop-down menu next to your login name in the top right-hand corner of the screen.

1.3 Forgotten password

If you have forgotten your password, you can request a new one by clicking the ‘forgotten password’ option. If you cannot remember your username, simply request a new account. Your account will not be blocked if you enter incorrect passwords.

1.4 Multi Factor Authentication (MFA)

The AFM uses Multi-Factor Authentication (MFA). This means that when logging in—besides your username and password—you must also enter additional information: a 6-digit code generated by an app on your phone, tablet, or PC.

To use MFA, you need an authenticator app on your phone, tablet, or PC. The instructions below refer to the Microsoft Authenticator app. You can also use other authenticator apps (e.g., Google's). A minimum requirement is that the authenticator app generates 6-digit codes.

The reason AFM uses MFA is security. Research shows that data is much better protected when an additional layer of authentication is used.

1.4.1 Logging in for the first time

The first step is to link Multi-Factor Authentication (MFA) to your AFM account. If this has not yet been done, you will see the following screen the first time you enter your username and password:



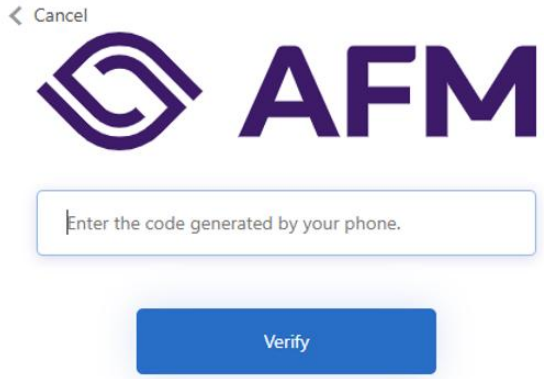
To use MFA, you need an authenticator app on your phone, tablet, or PC.

- **Don’t have an authenticator app yet?** Follow the provided link to the Google Play Store or Apple Store shown on the screen to download the Microsoft app.
- **Have you installed your preferred authenticator app?** You can then link a so-called token (similar to a certificate) to your account by scanning the QR code displayed on the screen.
- **Next, enter the code generated by the app**, and you’ll be securely logged into the AFM Portal (see section 1.4.2 for more details).

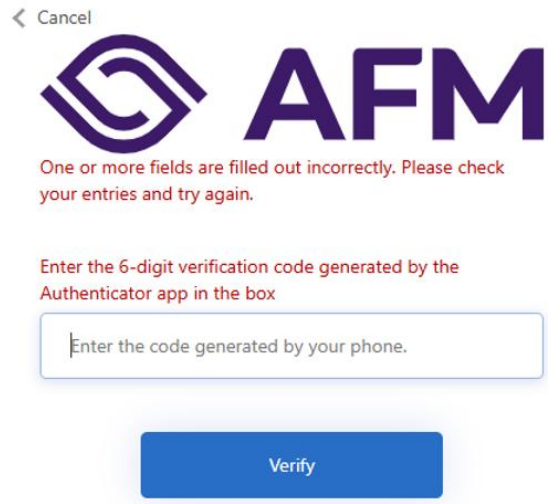
Note: The instructions above refer to the Microsoft Authenticator app. You may also use other **free** authenticator apps (e.g., Google’s). A minimum requirement is that the app generates 6-digit codes. **Important:** Always back up your token—see section 1.4.4.

1.4.2 Logging in with the authenticator code

After entering your username (email address) and password, you will see the screen below where you can enter the MFA code generated by your authenticator app.



If you accidentally entered the wrong code, you will see the following screen.

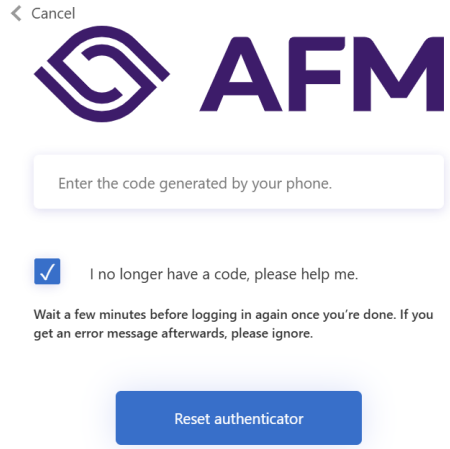


Enter the newly generated code here to log in to the portal.

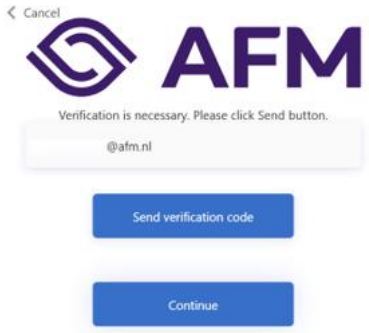
1.4.3 Resetting Multi-Factor Authentication

It is possible to reset your Multi-Factor Authentication. This may be necessary, for example, if you have a new phone and want to reregister the Authenticator app.

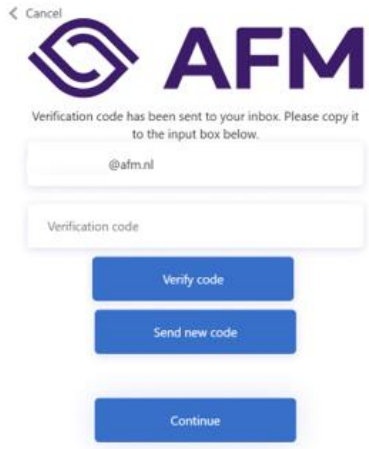
If you check the box “I no longer have a code, please help me.”, you will be able to re-register the Authenticator app on your phone.



A verification code will be sent to the email address known to the AFM.



You must enter the code sent to your email address in the input field below (named “Verification code”).



After clicking the Verify code button, your MFA will be reset. When you then click the Continue button, the screen below will appear and you can re-register the Authenticator app on your phone.



In some cases, you may receive an error message that can be ignored, as it does not affect the reset process. MFA will still be reset in the background, and after a few minutes you will be able to log in again. You will then see the screen shown in paragraph 1.4.1 (First-time login).

1.4.4 Important: Back up your security token

Are you planning to use a different device for MFA authentication? For example, if you get a new phone or lose your current one? Be aware that the security tokens from the app you downloaded when scanning the QR code are unique to your device (the token is linked to the device).

That's why it's important to use any backup option available in your chosen authenticator app. The app will then create a backup of the security tokens on your device. This backup is not automatic (and there's no automatic recovery), so you need to do it manually.

Switching to a new device? If you've created a backup in the app, you can import the tokens to your new device. After the import, you'll receive an authentication email from the provider of the authenticator app. You can then continue using the same MFA token.

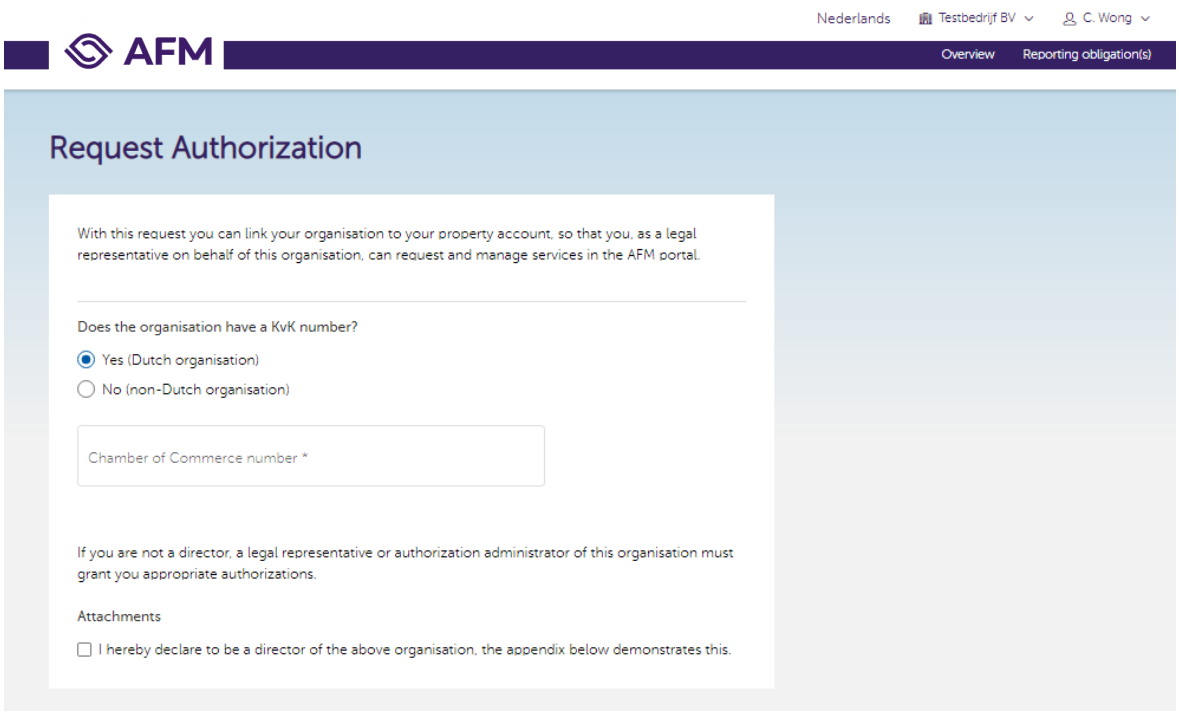
2. Linking the account to your company

Before a company director (a company director is referred to as 'legal representative' in the Portal) can start using the AFM's services, they must first activate the 'Link company' service. If you are not a director, a statutory representative or authorisation manager of this company must grant you the appropriate authorisations. This will be explained further in Chapter 3.

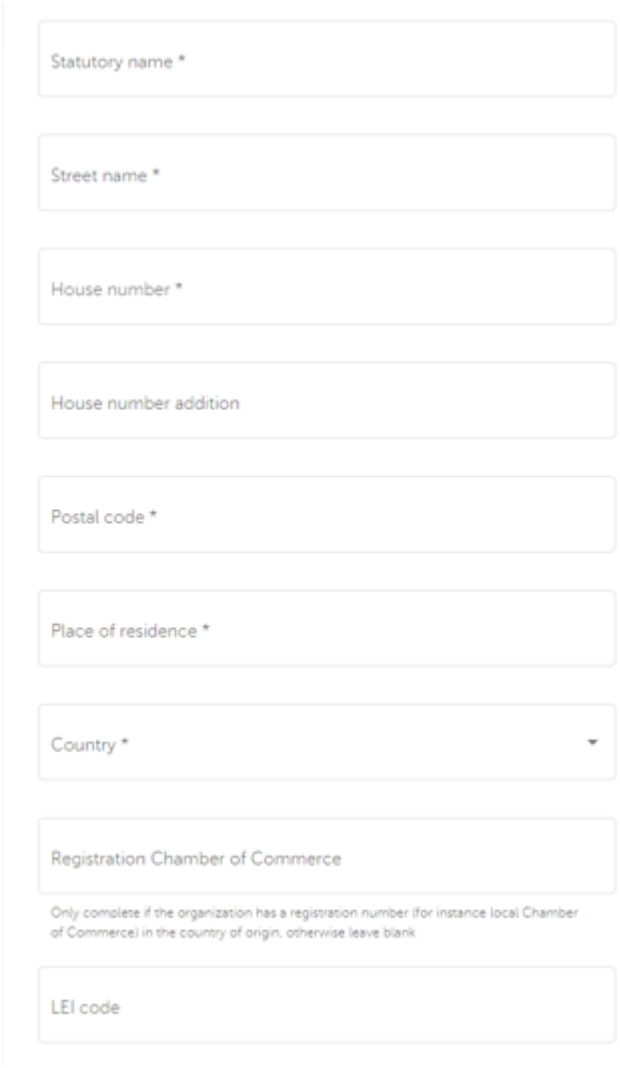
Make sure you have the following documents at hand before you activate this service:

- An extract from the Chamber of Commerce

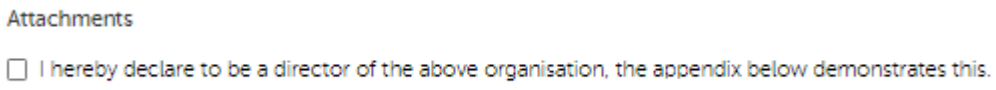
Activate the service 'Authorise company'.



Enter a Chamber of Commerce registration number. If you do not have a Chamber of Commerce registration number because your company is not a Dutch company or is not (or no longer) registered with the Chamber of Commerce, choose the option ‘No’ and fill in these fields.



Place a tick in the box next to the declaration that you are director of the specified company. Then add the requested attachment (extract from the Chamber of Commerce).



Click ‘Submit’

You will receive confirmation once your application has been processed.

3. Authorisations and components

Connecting or disconnecting a new user (who is not a statutory representative) to a company should from now on be done in the AFM Portal by a statutory representative of the company. The statutory representative (or an authorisation manager designated by the statutory representative) then determines which authorisations and permissions a new user will receive in terms of having access to the company's data (via a component) in the AFM Portal.

The authorisation structure in the AFM Portal has different levels of authorisation:

- **Statutory representative:** who has access to all data and authorisation to grant or deny others access to data. In principle, this is always a director of the company.
  A replacement statutory representative cannot be added by another legal representative. In addition, a role as statutory representative cannot be added.
- **Authorisation manager**: who is appointed by the statutory representative to grant or deny others access to data. An authorisation manager cannot change any of the statutory representative's authorisations or permissions.
- **Employee:** who has access to data as designated by the statutory representative or authorisation manager.

The AFM Portal contains the following sections, which can be accessed by a legal representative or authorization manager:

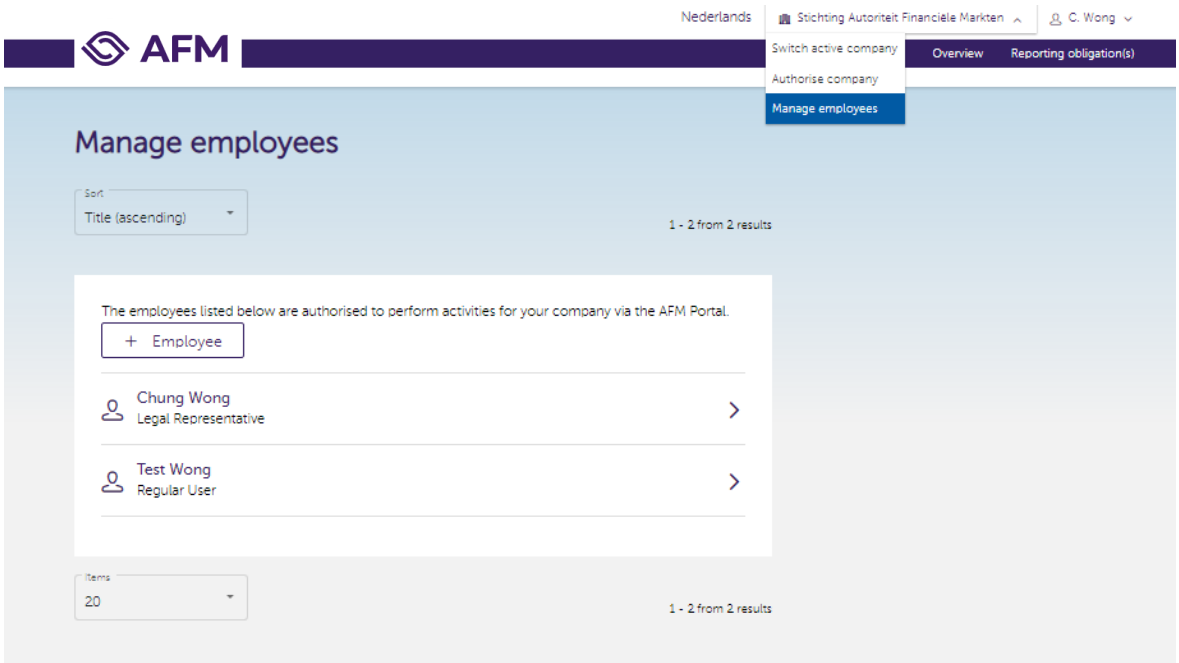
- **Asset Management:** Oversight of the Asset Management and Investment Market
- **Capital market notifications:** Oversight of Capital Markets
- **DORA Notification:** Serious ICT-related incidents and (new) agreements with ICT service providers can be reported. There is also an option to voluntarily report cyber threats.
- **Quality of Audit & Reporting:** Oversight of accountants.
- **Manage Authorisations:** For viewing and managing the authorizations and user rights within your company’s AFM Portal. This environment provides insight into the authorization structure for authorized users.
- **Market access and registration changes:** For registering or deregistering (partial) licenses, registrations, and assessable individuals.
- **Notification disclosure of inside information (article 17 MAR)**: This section is used to report inside information.
- **Reporting:** This section is for submitting reports and completing questionnaires.
- **STOR Notification:** To report a reasonable suspicion of market abuse.
- **TLPT:** Submission of threat-led penetration test (TLPT) reports.
- **Statutory Audit:** Data requests.

The above is summarised in a table below

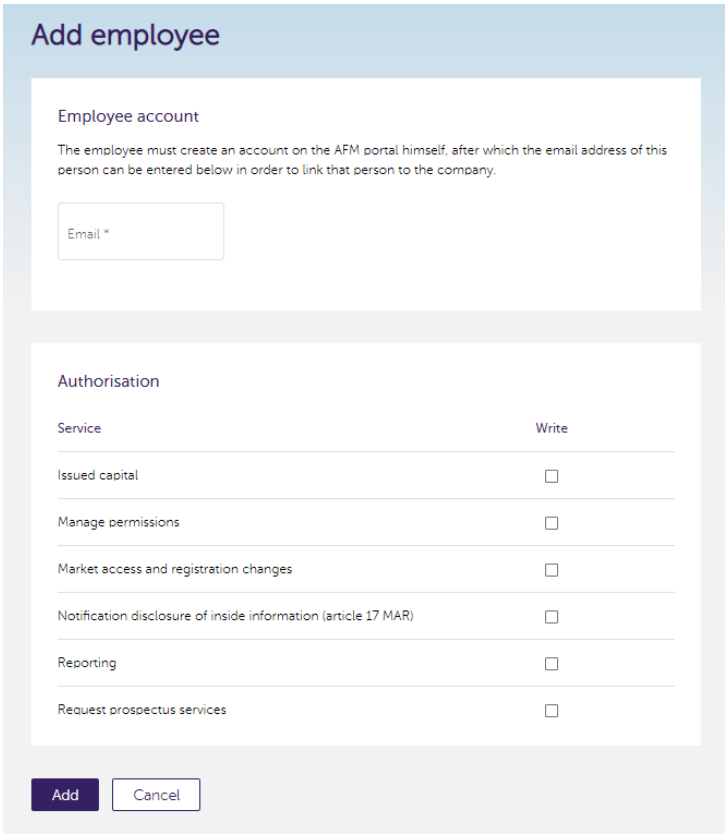
Authorisations and components		Authorisations		
		Statutory representative	Employee	Authorisations manager
Components	Manage authorisations	yes	no	yes
	Asset Management	yes	optional	optional
	Capital market notifications	yes	optional	optional
	DORA Notification	yes	optional	optional
	Market access and registration changes	yes	optional	optional
	Notification disclosure of inside information (article 17 MAR)	yes	optional	optional
	Reporting	yes	optional	optional
	STOR Notification	yes	optional	optional
	TLTP	yes	optional	optional
	Statutory Audit	yes	optional	optional

3.1 Managing employees

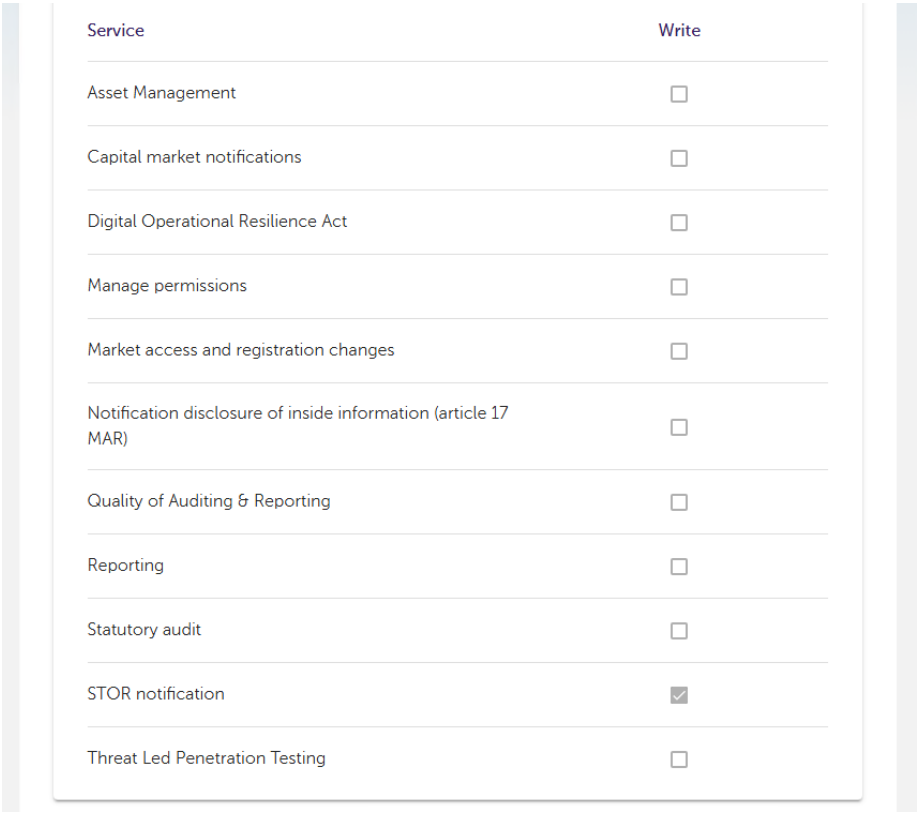
Log in as a statutory representative or authorisation manager and go to the 'Manage employees' option.



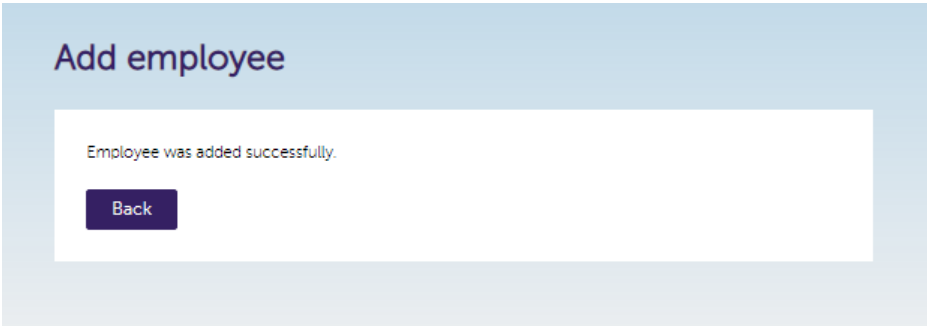
The '+ Employee' option allows you to add a new user to your company. The user must, however, be registered in the AFM Portal (see Chapter 1). To add the new user, fill in their email address.


Add employee
Employee account
The employee must create an account on the AFM portal himself, after which the email address of this person can be entered below in order to link that person to the company.
Email *
Authorisation
Service
Write
Issued capital
Manage permissions
Market access and registration changes
Notification disclosure of inside information (article 17 MAR)
Reporting
Request prospectus services
Add
Cancel

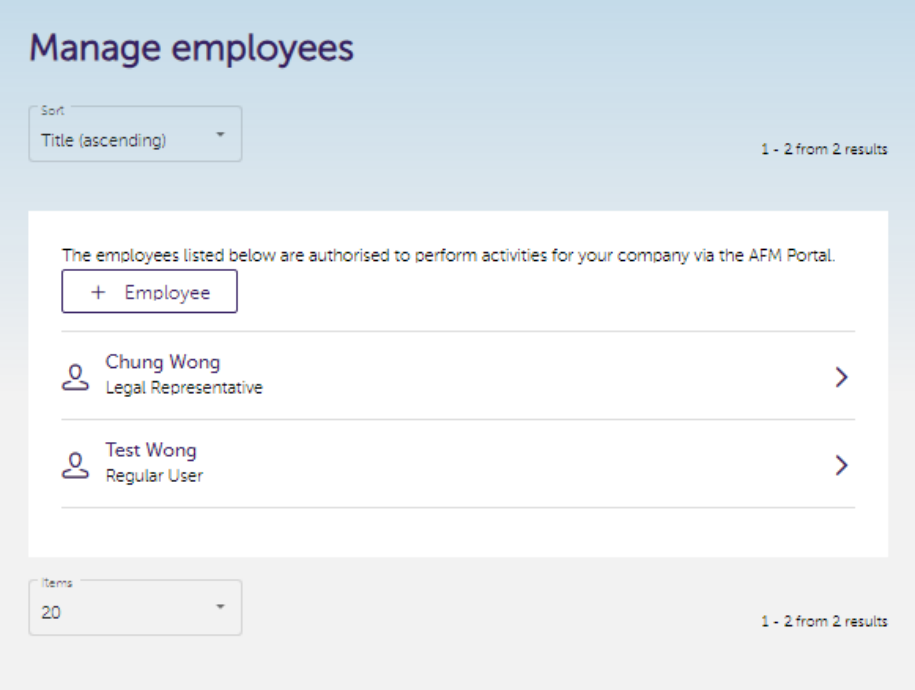
Then indicate which permissions the new user needs by ticking them off:



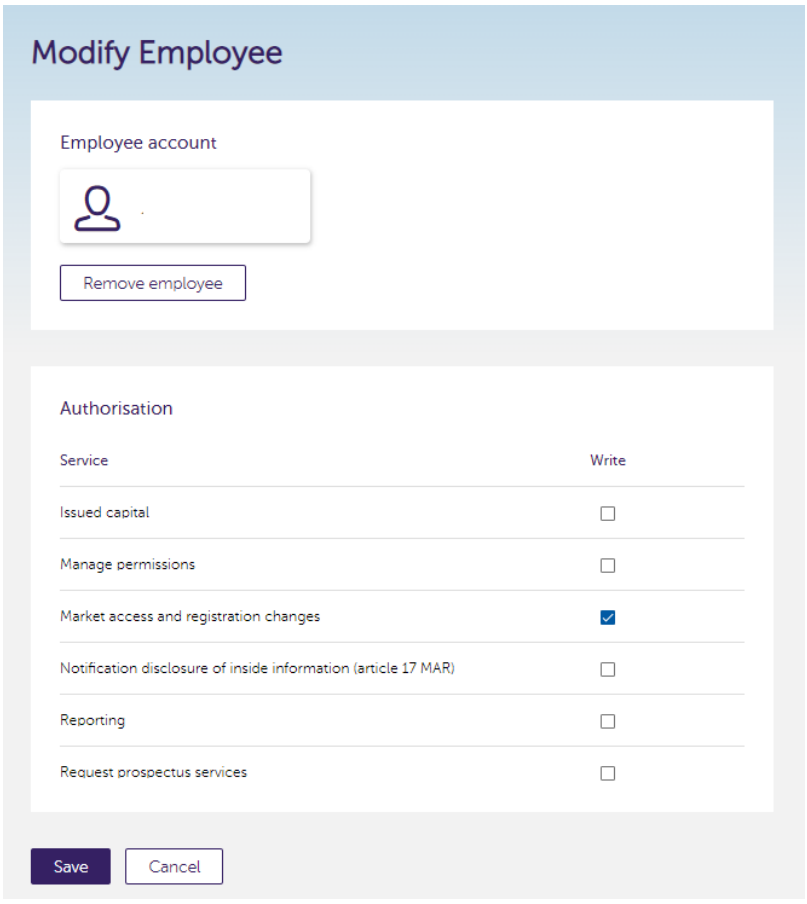
Click ‘Add’. This screen will then appear.



Click on ‘Back’ to go to the overview of ‘Manage employees’. The new user is now also on the list.

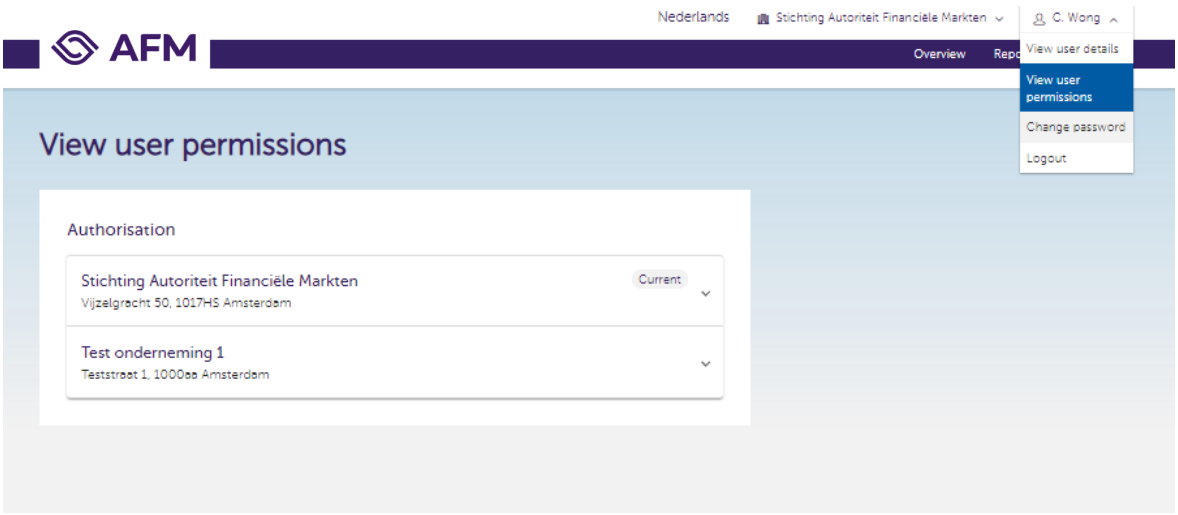


You can also change existing users in this overview. Click on the relevant user and you can make changes via this screen. You can delete the user or change the permissions. After making the changes, click on ‘Save’.



3.2 Viewing authorisations

Via ‘View user permissions’ you get an overview of the companies to which your account is linked.



You can open each company separately to see what permissions you have.

View user permissions

Authorisation

Miller Beheer B.V.
Raadhuisstraat 52, 4944VJ Raamsdonk

Current

Service	Write
Asset Management	☐
Capital market notifications	☐
Digital Operational Resilience Act	☐
Manage permissions	☐
Market access and registration changes	☐
Notification disclosure of inside information (article 17 MAR)	☐
Quality of Auditing & Reporting	☐
Reporting	☐
Statutory audit	☐
STOR notification	☑
Threat Led Penetration Testing	☐

Mitch Test BV 2
Vijzelgracht 50, 1017HS Amsterdam

Testbedrijf BV
teststraat 1, 1000aa Amsterdam

The Dutch Authority for the Financial Markets
T +31 20 797 2000 | F +31 20 797
3800 P.O. Box 11723 | 1001 GS
Amsterdam www.afm.nl

The text in this publication has been prepared with care and is informative in nature. No rights may be derived from it. Changes to legislation and regulations at national and international level may mean that the text is no longer up to date when you read it. The Dutch Authority for the Financial Markets (AFM) is not responsible or liable for the consequences – such as losses incurred or a drop in profits – of any action taken in connection with this text.