Multi Factor Authentication (English)

This manual helps you setting up Multi Factor Authentication.

-- When using UM IT services you agree to UM's Acceptable Use Policy. The complete text can be found on the website: https://www.maastrichtuniversity.nl/about-um/cybersecurity/security-policy-acceptable-use --

What do you need?

- A smartphone with the ability to install apps
- A UM account
- A computer with access to the internet

Introduction

Multi Factor Authentication (MFA) adds an extra layer of security to the login procedure. After typing in your UM account and password (something you know), a second authentication step follows via a separate device, e.g. a mobile phone.

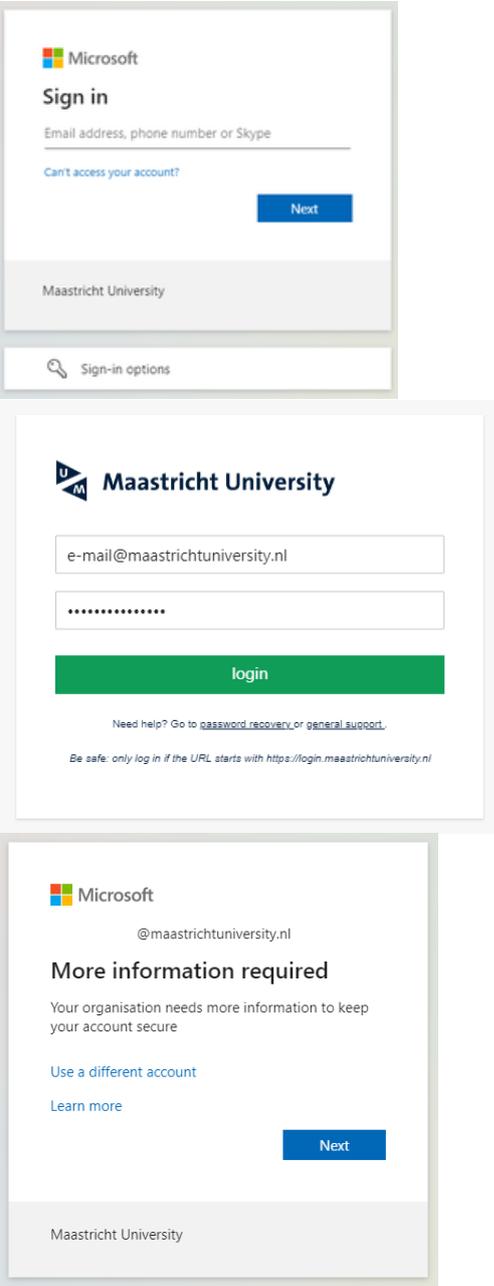MFA helps to protect your account and UM data and systems.

Note:

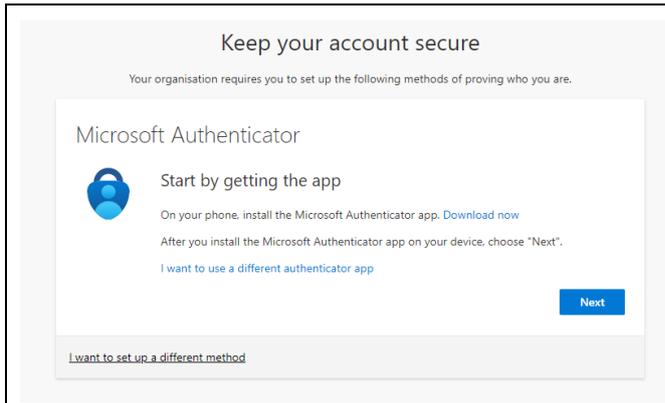This manual uses the Microsoft Authenticator App as the default.

If you do not want to use the app you can configure MFA on an alternative method, for example SMS or phone call.

In this case follow the steps below the paragraph '[MFA configuration based on other login method](#)'.

Important: Never approve an authentication request from Microsoft Authenticator if you have not been attempting to log into or access an application related to the UM from an already logged on workstation or browser. In such a case, this could be attempted abuse by someone with knowledge of your password or with access to one of your devices. If you notice an unexpected push notification you should change your UM password and report this to the ICTS service desk, or call +3143 388 5555 immediately.
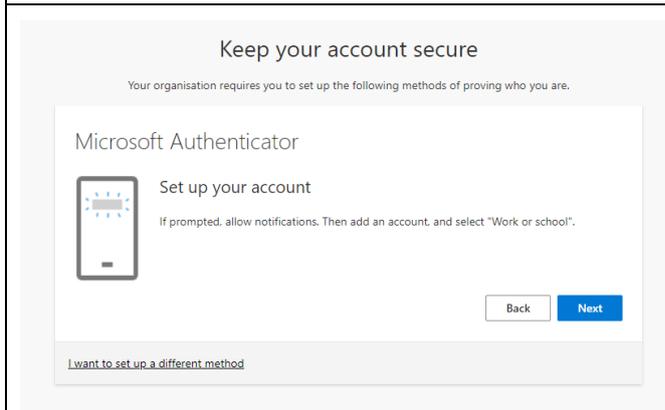
MFA configuration on MS Authenticator App:

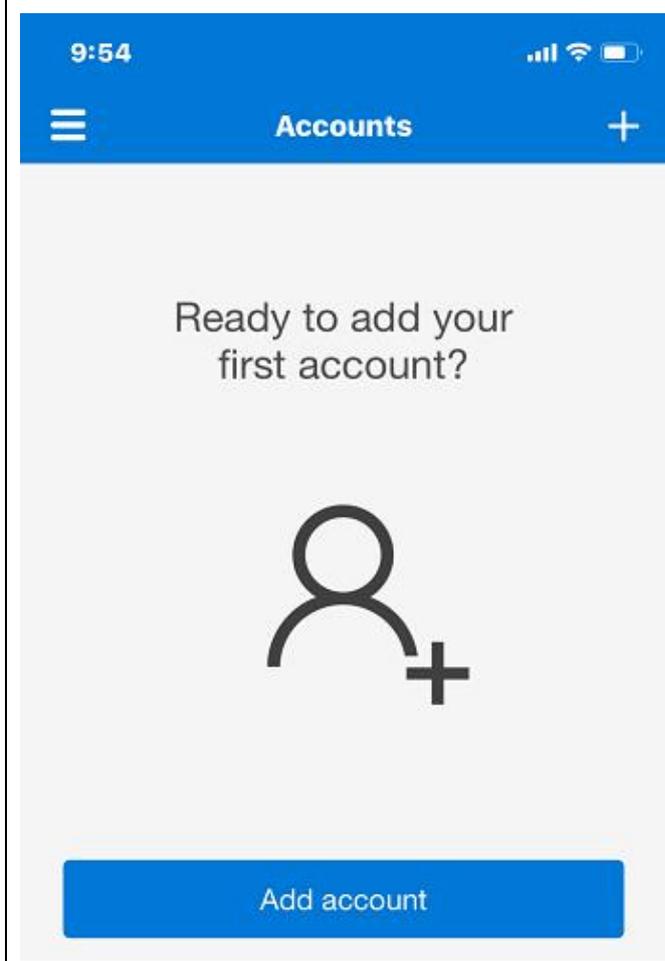| Screenshot	Information
	Step 1: **On your mobile device** visit the Apple app store or Google play store and install the Microsoft Authenticator app. Alternatively, visit aka.ms/authapp and download the Microsoft Authenticator app. Make sure you really install the Microsoft app. This app is free of charge. Do not uninstall the app.
	Step 2: **On your computer** visit the website https://aka.ms/mfasetup. Fill in your UM e-mail address and sign in with your e-mail address and password. Click on "Next".

|	
Keep your account secure Your organisation requires you to set up the following methods of proving who you are. Microsoft Authenticator **Start by getting the app** On your phone, install the Microsoft Authenticator app. Download now After you install the Microsoft Authenticator app on your device, choose "Next". I want to use a different authenticator app Next I want to set up a different method	**Step 3:** Click on "Next".
Keep your account secure Your organisation requires you to set up the following methods of proving who you are. Microsoft Authenticator **Set up your account** If prompted, allow notifications. Then add an account, and select "Work or school". Back Next I want to set up a different method	**Step 4:** Click on "Next". You will now see a screen with a QR code.
9:54 ☰ **Accounts** + Ready to add your first account? Add account	**Step 5:** Open the Microsoft Authenticator app **on your phone** and click on the "+" sign.
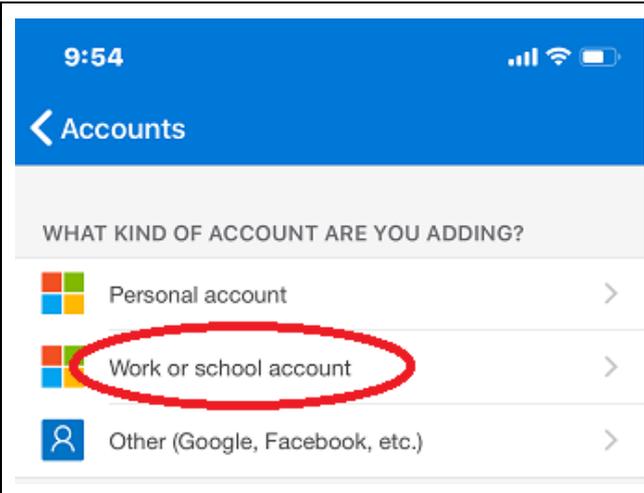
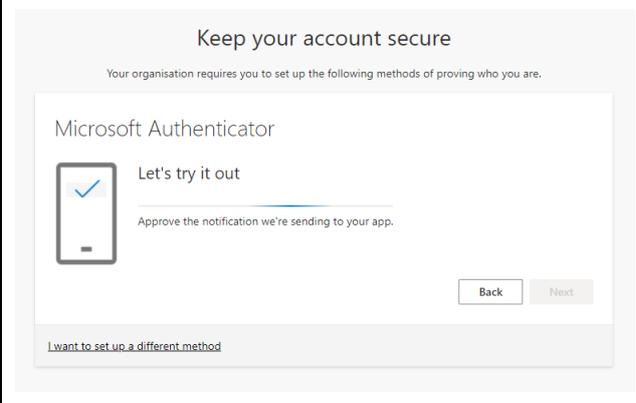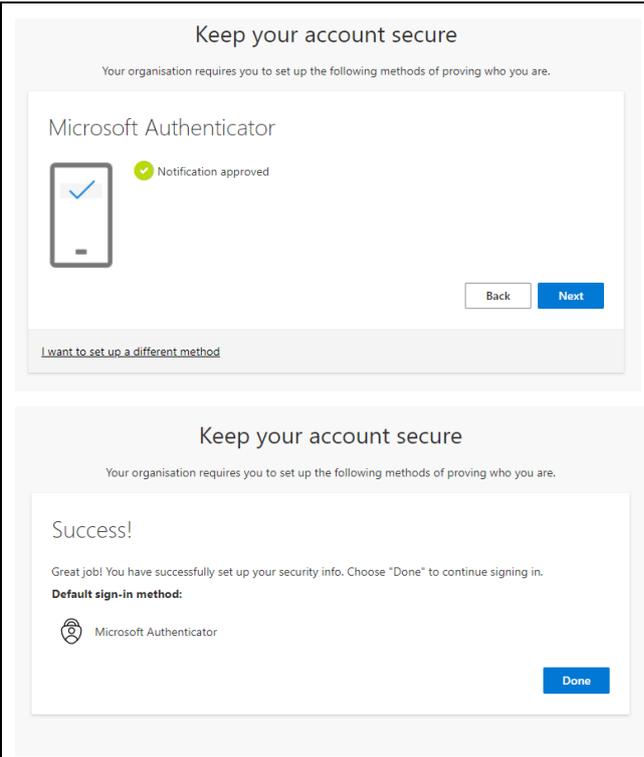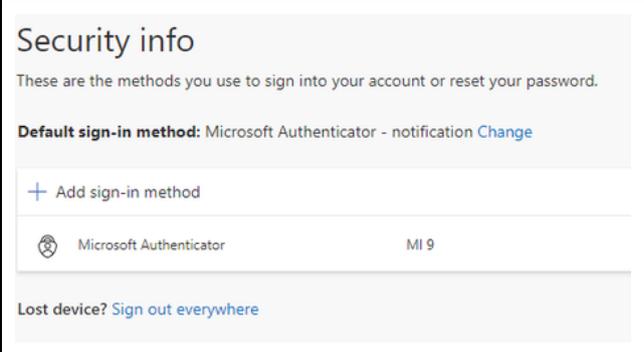|	
	Step 6: Choose "Work or school account".
	Step 7: Click on "Scan a QR code" Scan the QR code that is displayed **on your computer.**
	Step 8: After scanning the QR code **on your computer with your phone**, click on next.
	Step 9: A test notification will be sent to your phone. **On your mobile device** accept the test notification in the app by click on "Allow".
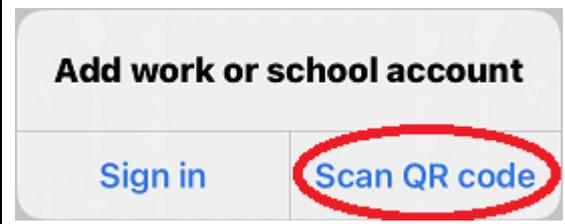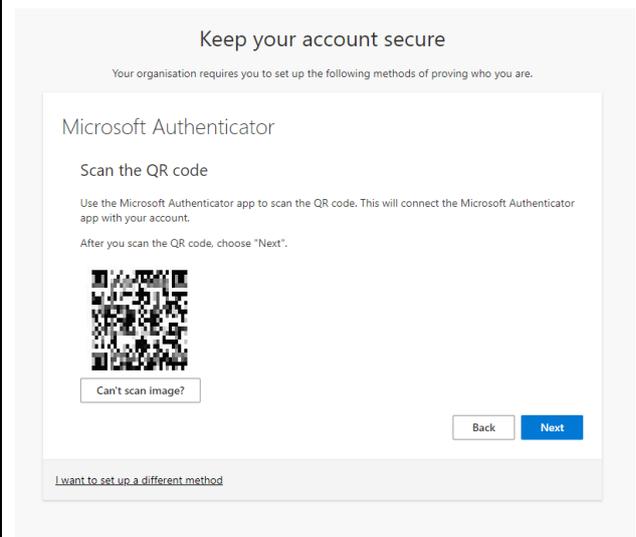
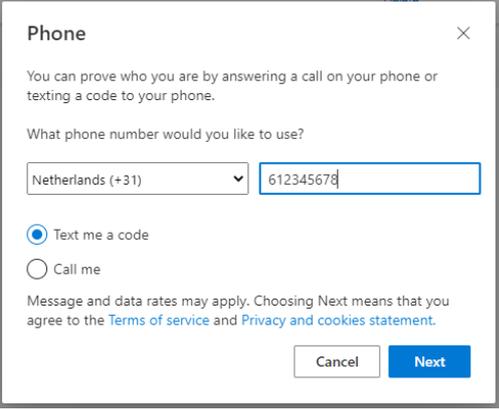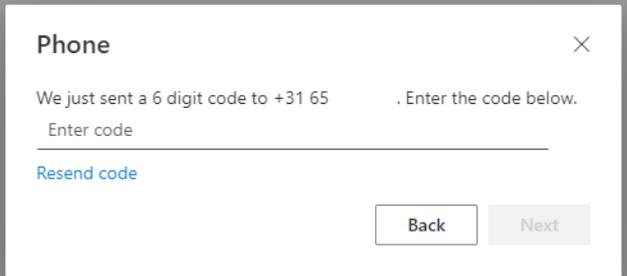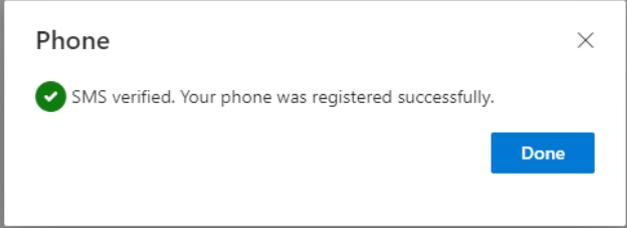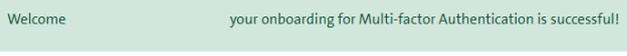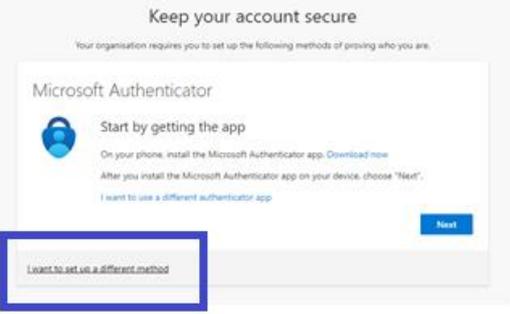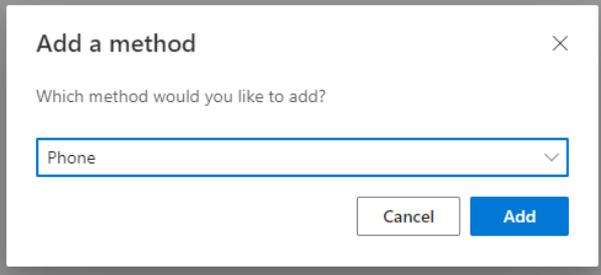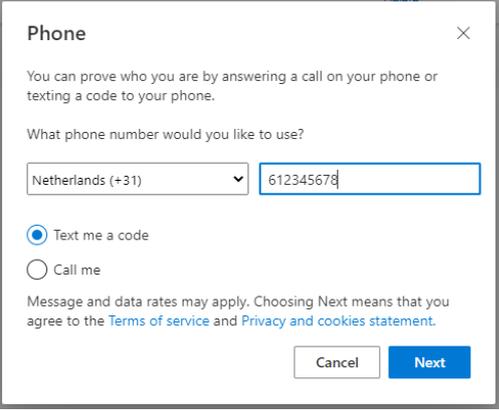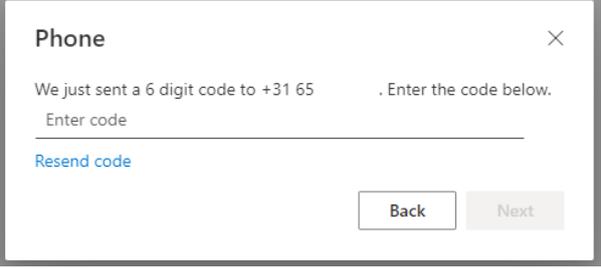|	
Keep your account secure Your organisation requires you to set up the following methods of proving who you are. Microsoft Authenticator ✓ Notification approved Back Next I want to set up a different method Keep your account secure Your organisation requires you to set up the following methods of proving who you are. Success! Great job! You have successfully set up your security info. Choose "Done" to continue signing in. **Default sign-in method:** Microsoft Authenticator Done	**Step 10:** Click on next. After that click on "Done". Important: It is **highly recommended** to setup an additional verification method. It is advised to use an alternative login method in case your default method is not available.
Security info These are the methods you use to sign into your account or reset your password. **Default sign-in method:** Microsoft Authenticator - notification Change + Add sign-in method Microsoft Authenticator MI 9 Lost device? Sign out everywhere	**Step 11:** You might need to sign in again via the website https://aka.ms/mfasetup. Click on "Add sign-in method".
Add a method ✕ Which method would you like to add? Phone ⌄ Cancel Add	**Step 12:** In the drop-down menu choose for "Phone" and click on "Add". You may also choose a different option in this list as your additional verification method.
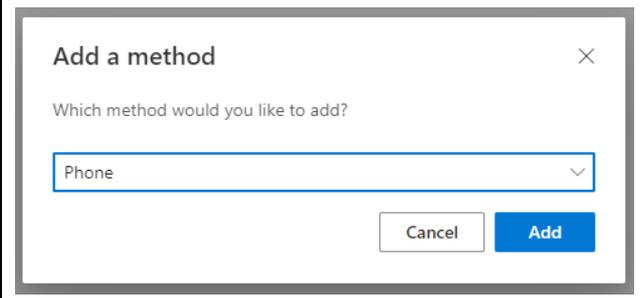
Phone ✕ You can prove who you are by answering a call on your phone or texting a code to your phone. What phone number would you like to use? Netherlands (+31) ▾ 612345678 ◉ Text me a code ○ Call me Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement. Cancel **Next**	**Step 13:** Choose your number's prefix and add the phone number. Choose for one of the two options: Text me a code: receive the code by text or Call me: you receive a phone call and you have to press "#" on your phone Click on "Next".
Phone ✕ We just sent a 6 digit code to +31 65 . Enter the code below. Enter code Resend code Back Next	**Step 14 (text me a code only):** Fill in the code that you have received by phone or SMS and click on "Next".
Phone ✕ ✅ SMS verified. Your phone was registered successfully. **Done**	**Step 15:** You have now successfully setup MFA with two verification methods. Click on "Done".
Welcome your onboarding for Multi-factor Authentication is successful!	You can check if MFA registration is done successfully at: https://checkmfa.maastrichtuniversity.nl

MFA configuration based on other login method:

Screenshot	Information
	Step 1: **On your computer** visit the website https://aka.ms/mfasetup. Fill in your e-mail address and sign in with your e-mail address and password. Click on "Next".

	Step 2: Click on the bottom left on "I want to setup a different method".
	Step 3: In the drop-down menu choose for "Phone" and click on "Add".
	Step 4: Choose your number's prefix and add the phone number. Choose whether you want to receive a call or a text. Click on "Next".
	Step 5: Text me a code: Fill in the code that you have received by SMS. Call me: Answer the phone, press # on your phone when you get the call. Click on "Next" on your computer
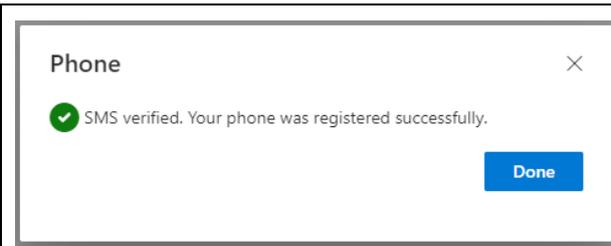
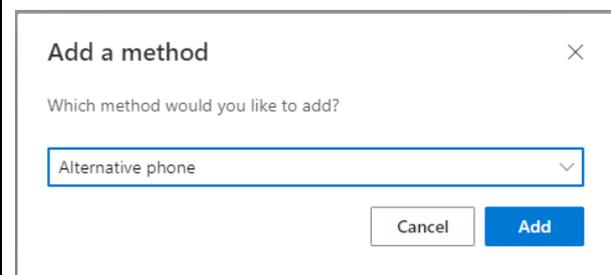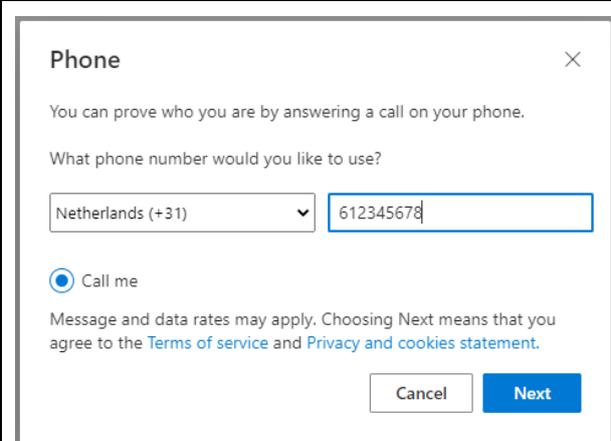|	
Phone ✕ ✅ SMS verified. Your phone was registered successfully. **Done**	**Step 6:** You have now successfully setup MFA with two verification methods. Click on "Done". Important: It is **highly recommended** to setup an additional verification method. It is advised to use an alternative login method in case your default method is not available. Keep following this guide to set this up.
Security info These are the methods you use to sign into your account or reset your password. **Default sign-in method:** Microsoft Authenticator - notification Change ╋ Add sign-in method Ⓜ Microsoft Authenticator MI 9 **Lost device?** Sign out everywhere	**Step 7:** You might need to sign in again via the website https://aka.ms/mfasetup. Click on "Add sign-in method".
Add a method ✕ Which method would you like to add? Alternative phone ⌄ Cancel **Add**	**Step 8:** Choose "Alternative phone" as the MFA sign-in method.
Phone ✕ You can prove who you are by answering a call on your phone. What phone number would you like to use? Netherlands (+31) ⌄ 612345678 🔘 Call me Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement. Cancel **Next**	**Step 9:** You have now successfully setup MFA with two verification methods. Click on "Done".
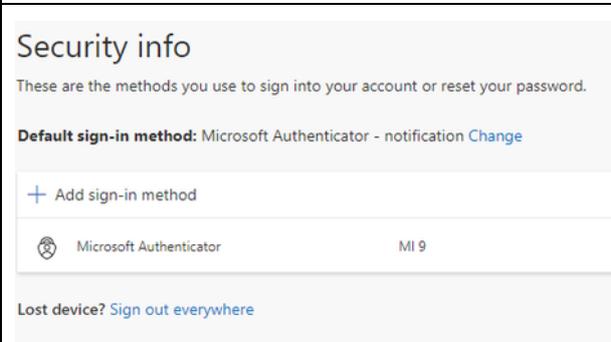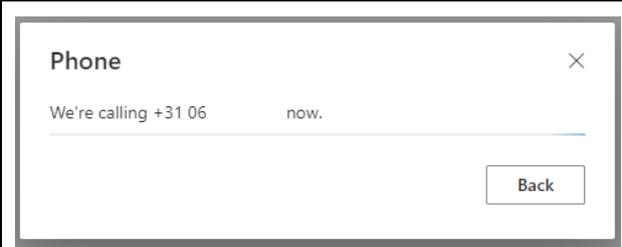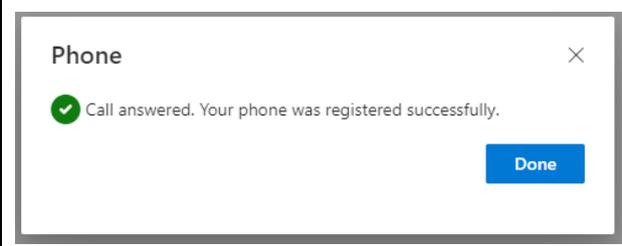
Phone ✕ We're calling +31 06 now. Back	**Step 10:** You will receive a phone call. Answer the phone and press # on your phone to verify the request.
Phone ✕ ✔ Call answered. Your phone was registered successfully. Done	**Step 11:** You have now successfully setup MFA with two verification methods. Click on "Done".
Welcome your onboarding for Multi-factor Authentication is successful!	You can check if MFA registration is done successfully at: https://checkmfa.maastrichtuniversity.nl