Frequently Asked Questions (FAQ) - UM Multi Factor Authentication (MFA). New version 14-12-2022

Question: *Why is Multi Factor Authentication necessary?*
Answer: Maastricht University uses many information systems within which sensitive (personal) data is processed. UM's security policy and the obligations for processing sensitive data within the General Data Protection Regulation (GDPR) require additional security measures.
To protect these systems and data, Maastricht University uses authentication in two steps: Multi Factor Authentication (MFA). Please visit https://www.maastrichtuniversity.nl/cyber-security for more information on UM's security policy.

Question: *Why is logging in with only my account and password insufficiently secure?*
Answer: Information systems may contain data to which others are not permitted access. This may include research data, examination results, or bank account numbers. Passwords may be retrieved with relative ease, for example when you:

- Are a victim of a virus infection or other malware;
- Use your UM password on other systems websites;
- Download software from the internet which contains malware;
- Accidentally activate incorrect links in a phishing email;
- Have provided your password to others.

MFA requires authentication in two steps. Not only a password (*something you know*) is required, but also a second verification such as a code in the authenticator app on your smartphone (*something you have*), to prove your identity.

Question: *Which applications require MFA?*
Answer: Initially on UM web applications (e.g. HR- and procurement system, Student Portal, Canvas), VPN and VDI (Virtual desktop for UM employees and students).

Question: *How do I register my account for MFA?*
Answer: Via https://aka.ms/mfasetup

Question: *How can I change my MFA settings?*
How can I add or remove a sign-in method?
Answer: Within the UM implementation we will use the Microsoft Authenticator app as the default method. If you can't or don't want to use the app, you can setup MFA with alternative methods such as an SMS or phone call to a work or private phone number. You can change this via https://aka.ms/mfasetup.
We highly recommend you to add an additional login method next to your default method. This way there is always a way to access your account in case something happens with your default method.
See also the extensive manual on the website https://www.maastrichtuniversity.nl/mfa for more information

Question: *I do not have an UM smartphone and I do not want to use the Microsoft Authenticator app. How can I log in with MFA? (employees)*

Answer: In this case you can configure alternative methods. This option allows you to receive an SMS code or phone call to your private phone number. These options are free of charge.
You can configure alternative methods via https://aka.ms/mfasetup. See more information on how to configure alternative methods in the extensive manual at the option 'MFA configuration based on other login method' on the website: https://maastrichtuniversity.nl/mfa.

=

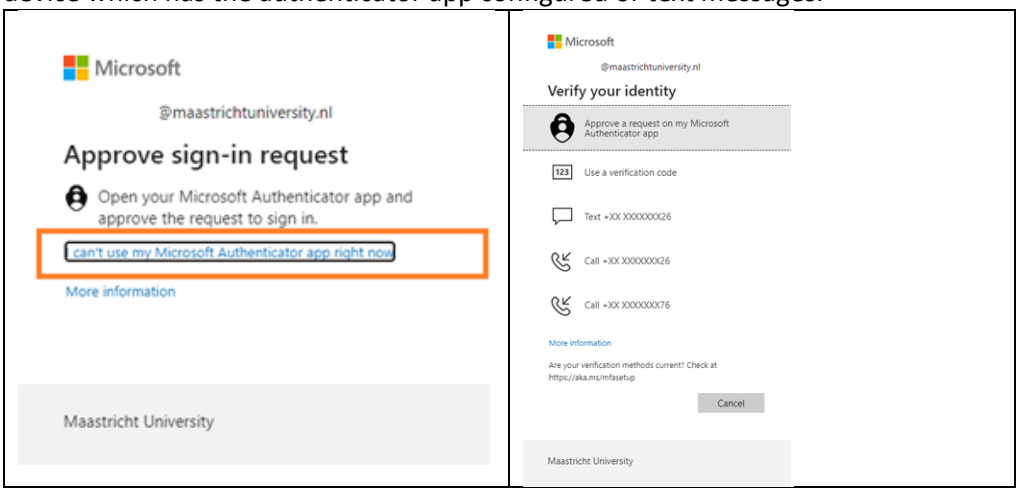
Question: *Do I have to login with MFA often?*

Answer: MFA login is requested for login to UM web services (e.g. Intranet, HR- and procurement system, Student Portal, Canvas), for VPN and for VDI (Virtual desktop for UM employees and students). UM web services work with Single Sign On (SSO) in your internet browser. This means that only a single login is required for using UM web services, including MFA, as long as your internet browser window is open. This browser-login remains active during your workday.

TIP:
Keep your Internet browser window open / active, to prevent regular MFA login requests for UM web applications.
Make sure to always lock your workstation when leaving your desk or workplace. After locking your workstation, your session will remain open /active.
Also check: Lock your screen, even if you leave your PC for a moment - About UM - Maastricht University

Question: *I (temporarily) don't have a smartphone available. What should I do?*

Answer: Use one of the alternative sign-in methods you can configure. This may be a phone call by Microsoft on an additional phone number (work or private), or an extra device which has the authenticator app configured or text messages.



NB: this pop-up screen is currently only available on UM web applications. It is not available on VPN nor on VDI.

Question: *I am unable to login and I don't have an extra sign-in method configured for my account. What should I do?*

Answer: Contact Servicedesk ICTS. We can provide you with a temporary access pass (TAP). Before we can provide you with a TAP you need to send us a picture or copy of a valid ID (such as a driver's license or passport) so we can verify we send the TAP

code to you and not someone else pretending to be you. **We highly recommend you to add an additional login method next to your default method**, to prevent this from happening.

Question: *What is a Temporary Access Pass (TAP)?*
Answer: If you are unable to login and do not have any other registered MFA sign-in methods, the TAP will be valid for 2 hours and enables you to add an extra sign-in method via https://aka.ms/mfasetup. The TAP also enables you to change your default sign-in method.

Question: *Apart from the Microsoft Authenticator app, is it also possible to receive text messages or phone calls for MFA?*
Answer: Yes, you can add an extra sign-in method via https://aka.ms/mfasetup

Question: *I have new / spare smartphone because my smartphone is old/broken/ stolen / lost. What should I do?*
Answer:

1. FIRST; reconfigure the authenticator app on your new / spare phone at https://aka.ms/mfasetup (select Add sign-in method) before disposing of the old phone.
2. SECOND; Remove your old/broken/stolen/lost phone via https://aka.ms/mfasetup.

Question: *I forgot my smartphone and cannot log in to MFA secured systems now. What should I do?*
Answer:

- Collect your smartphone, if possible.
- When using an MFA secured UM web application, use one of the extra verification options you configured by choosing '*Use a different verification option*'.
- Contact Servicedesk ICTS when trying to log in to VDI or VPN or in case you do not have an extra verification method configured.

Question: *I do not have an internet connection on my mobile telephone, will the app still work?*
Answer: An internet connection is required for app configuration
Once the app is configured, depending on your configuration you can also use the time-based, one-time passcode in the app offline.

Question: *Can I authorize someone else to log in on my behalf?*
Answer: No, this is never allowed. Passwords and MFA are for personal use only and cannot be transferred.

Question: *Why does the MFA app request access to the camera?*
Answer: The app only requires camera access to scan a code during installation / configuration.

Question: *Can I use a Yubikey as extra sign-in method?*
Answer: Yes you can with several Yubikeys in combination with a software authenticator. For more information: Using YubiKeys with Azure MFA OATH-TOTP – Yubico

Question: *Why does MFA work differently on UM web applications compared to VPN and VDI?*

Answer: Both VPN and VDI currently use a different underlying technology compared to UM web applications, which results in a somewhat different user experience.

Question: *Maastricht University uses MFA. Can I also use MFA for private purposes?*
Answer: MFA is already widely used by the Dutch government (DigiD) and banks (for secure online banking).

Question: *Is MFA required during digital exams?*
Answer: No.

Question: *I do not have an UM smartphone, I'd rather not use my private telephone for work and the advised alternative methods are not an option for me.. How can I log in with MFA? (employees)*
Answer: In this case you can contact your information manager. After your information manager approves this request it will be forwarded to ICTS and you will be informed on further actions as soon as possible. Such requests will be critically assessed because there are costs involved for other solutions.

Question: Is MFA also mandatory for resource/system accounts?
Answer: No, not at this time. If this changes you will get informed.

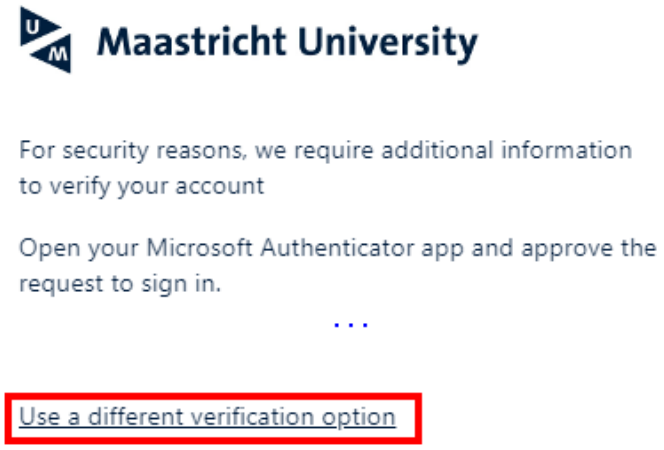
Question I already use MFA (or another online Microsoft service) for another organisation and now my UM MFA enrollment gets automatically forwarded to my already existing MFA registration or Microsoft service sign-in page.

Answer: You can resolve this by using an "incognito/inprivate"-tab in your browser. Instructions

Question: I deleted the app/I have a new phone and now I cannot login anymore.

Answer: I installed an alternative authentication method: You can click on "Use a different verification option" when trying to log in, you can then get a text (SMS) with a login code on your phone or receive a phone call (dependent on the option you configured).

You can add the app again to your authentication methods on by logging in with the text (SMS) function or Phone call. If you added your cell phone number as an alternative login method, you can click "Use a different verification option" during login and have an SMS sent to your phone or receive a phone call.



You can add the app again at https://aka.ms/mfasetup by logging in with an SMS code or phone call.

I did not install an alternative login method:
Send an e-mail to: servicedesk-icts@maastrichtuniversity.nl with your UM username and a copy of a valid ID document (not a UM card). When doing so, make sure your BSN number, passport photo and so-called Machine Readable Zone at the bottom of the document are made unreadable and apply text to the copy to indicate that the copy is for a one-time MFA reset. It is recommended to use the government's Copy ID app for this purpose.

We will then generate a TAP code for you which you can use to login on https://aka.ms/mfasetup and enables you to add a new authentication method.
Also add your phone number as a back-up option.