Frequently Asked Questions (FAQ) - Multi Factor Authenticatie (MFA).

Versie	Toelichting	Datum
1.0	Start versie	Okt ’22
2.0.		14-12-‘22
3.0.	Number matching	14-02-‘23

Inhoud

Multi Factor Authenticatie (MFA) uitgebreid met number matching.

Vanaf **27 februari '23** activeert Microsoft '*number matching*' als nieuwe standaard voor gebruikers van de Microsoft Authenticator – notification inlogmethode. Wanneer je reageert op een MFA-melding met de Authenticator-app, krijg je een 2-cijferig nummer te zien of moet je de 6-cijferige eenmalige wachtwoordcode ophalen uit je Authenticator-app. Typ dat nummer in het bijbehorende venster om de goedkeuring te voltooien en het aanmeldingsproces voort te zetten.

Zie voor een uitgebreide toelichting a.u.b. ook de onderstaande informatie.

Waarom verandert dit?

Deze instelling wordt toegepast als extra veiligheidsmaatregel, om te voorkomen dat er per ongeluk goedkeuring wordt gegeven aan malafide inlogpogingen (als gevolg van MFA-moeheid van de gebruiker).

Wat betekent dit voor mij?

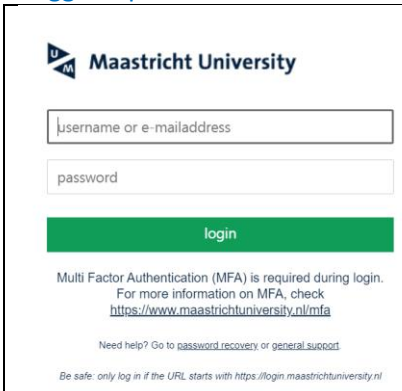
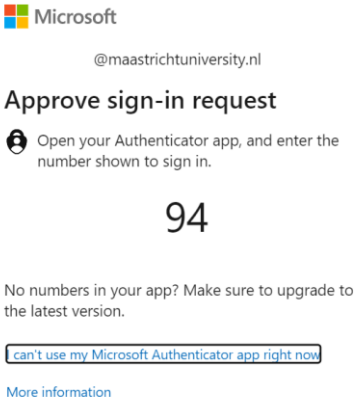
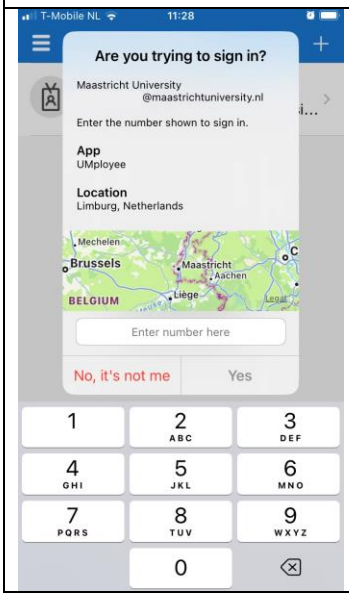
Wat er voor jou wijzigt is afhankelijk van de standaard MFA-inlogmethode die je ingesteld hebt.

- Op de website https://mysignins.microsoft.com/security-info zie je welke 'Default sign-in method' je ingesteld hebt voor jouw UM account.
- In de onderstaande tabel zie je of er iets voor jou verandert.

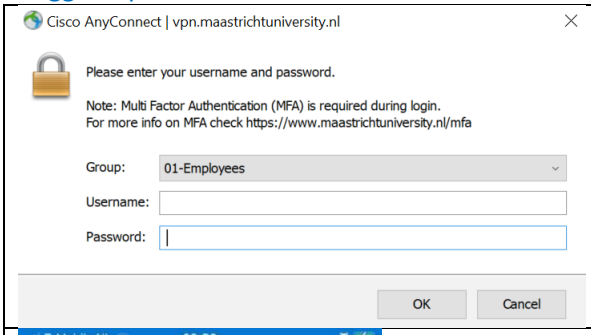
Door jou ingestelde standaard MFA methode.	Wat verandert er bij inloggen op UM webdiensten?	Wat verandert er bij inloggen op VPN of VDI?
Microsoft Authenticator – notification	Er dient een 2-cijferig nummer te worden ingevuld.	De 6-cijferige code die verschijnt in je app (of hardware token) dient te worden ingevuld.
Authenticator app or hardware token	Er verandert niets.	Er verandert niets.
Phone - text	Er verandert niets.	Er verandert niets.
Phone - call	Er verandert niets.	Er verandert niets.

- Zie onderstaande uitgebreide toelichting voor het login proces op UM webdiensten, VPN en VDI.

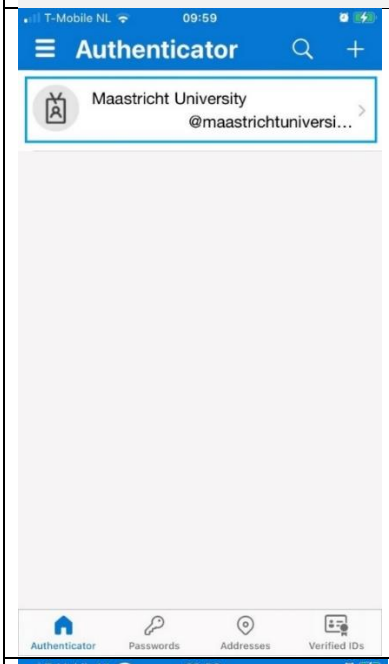
Inloggen op UM webdiensten:

	1. Log in met je UM-account en wachtwoord en klik 'login'.
	2. In je browser verschijnt een 2-cijferig nummer.
	3. In je Microsoft Authenticator App controleer je of de aangegeven applicatie en locatie correct zijn. Zo ja, vul je het 2-cijferige nummer uit stap 2 in en klik je op Yes om door te gaan.

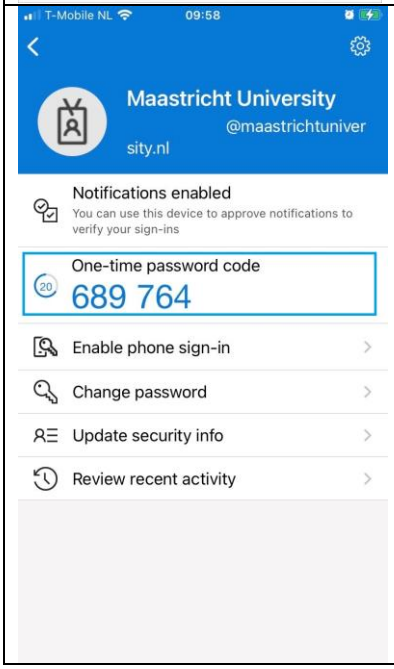
Inloggen op VPN:

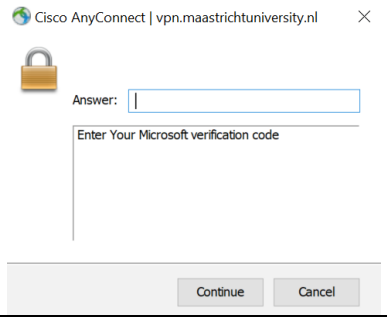


1. Log in met je UM-account en wachtwoord en klik ‘OK’.



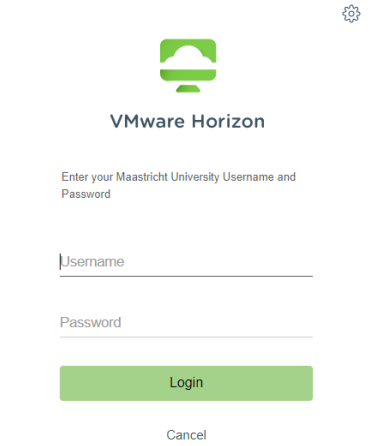
2. Klik in je Microsoft Authenticator App op je Maastricht University account.



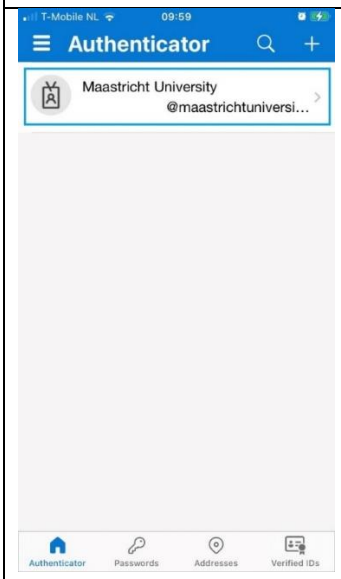


3. Type de 6-cijferige One-time password uit je MS Authenticator App (of je hardware token) in je VPN inlogvenster en klik ‘Continue’.

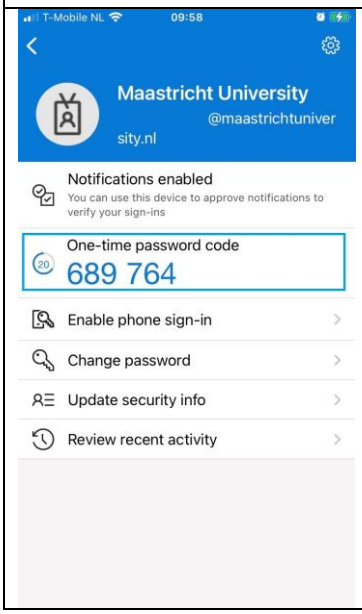
Inloggen op VDI:

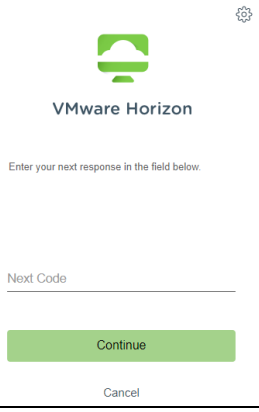


1. Log in met je UM-account en wachtwoord en klik ‘Login’.



2. Klik in je Microsoft Authenticator App, op je Maastricht University account.





3. Type de 6-cijferige One-time password uit je MS Authenticator App (of je hardware token) in je VDI inlogvenster en klik ‘Continue’.

Waarom Multi Factor Authenticatie?

De UM heeft veel informatiesystemen met vertrouwelijke gegevens, die in lijn met het hoge risico en de eisen in de Algemene Verordening Gegevensbescherming (AVG), om extra beveiligings-maatregelen vragen. Vandaar dat de UM-authenticatie in twee stappen gebruikt, Multi factor Authenticatie (MFA), om deze systemen en data extra te beveiligen.
Zie https://www.maastrichtuniversity.nl/cyber-security voor uitleg over UM-beleid hierover.

Waarom is inloggen met alleen mijn account en wachtwoord soms niet veilig genoeg?

Informatiesystemen kunnen gevoelige gegevens bevatten waar anderen geen toegang toe mogen hebben. Denk bijvoorbeeld aan onderzoeksdata, toetsresultaten of bankrekeningnummers. Een wachtwoord kan vrij makkelijk achterhaald worden door anderen. Bijvoorbeeld wanneer je:

- Slachtoffer bent van een virusinfectie of andere malware;
- Je UM-wachtwoord ook nog op een ander systeem of website gebruikt;
- De software die je downloadt van internet malware blijkt te bevatten;
- Per ongeluk verkeerde links activeert in een phishing-mail;
- Je wachtwoord een keer bekend hebt gemaakt aan een ander.

MFA vereist authenticatie in twee stappen. Niet alleen je wachtwoord is vereist (*iets dat jij weet*), maar ook een tweede verificatie zoals een code in de authenticator app op je smartphone (*iets dat jij hebt*), om jouw identiteit te bevestigen.

Op welke systemen wordt MFA geactiveerd?

In eerste instantie op UM web applicaties (zoals o.a. UM intranet, het HR- en inkoop systeem, Student Portal, Canvas), VPN en VDI (virtuele desktop voor medewerkers en studenten).

Ik heb geen smartphone van de UM en ik wil geen MS Authenticator app gebruiken (medewerkers).

In dat geval kun je gebruik maken van alternatieve MFA inlog methodes.
Dit betreft een optie om via SMS een code te ontvangen of om een telefoontje te ontvangen op je privé telefoon. Deze methodes zijn gratis.
Je kunt alternatieve MFA inlog methode instellen via https://aka.ms/mfasetup.
Op https://maastrichtuniversity.nl/nl/mfa staat in de uitgebreide MFA handleiding onder ''MFA configuratie op basis van andere inlog methode' hoe je dit kunt doen.

Moet ik vaak met MFA inloggen?

MFA inlog is nodig voor UM web applicaties (zoals o.a. UM intranet, het HR- en inkoop systeem, Student Portal, Canvas), VPN en VDI (virtuele desktop voor medewerkers en studenten).
UM web gebaseerde diensten werken met Single Sign On (SSO) in je internet browser. Vanwege Single Sign On (SSO) hoef je voor het gebruik van UM web gebaseerde diensten maar één keer in te loggen. Zolang je browser venster openblijft, blijft je MFA-toegang geldig voor alle UM web gebaseerde diensten. Zo'n browser-login blijft een hele werkdag geldig.

TIP:
Houd je internetbrowser venster open/ actief, om te voorkomen dat je elke keer bij gebruik van een UM web applicatie opnieuw met MFA moet inloggen. Maar zorg er wél altijd voor dat je bij het (tijdelijk) verlaten van je werkplek je scherm locked. Bij het locken blijft jouw werksessie open/ actief staan.
Zie ook : 'Lock' je scherm, ook als je je PC even achterlaat - Over de UM - Maastricht University

Hoe registreer ik mijn account voor het gebruik van MFA?

Via https://aka.ms/mfasetup
Zie ook de handleiding op de website https://www.maastrichtuniversity.nl/nl/mfa
Het is ook mogelijk om je UM-account toe te voegen aan een authenticator app die je mogelijk al hebt ingesteld voor een andere dienst.

Hoe pas ik mijn MFA-instellingen aan?

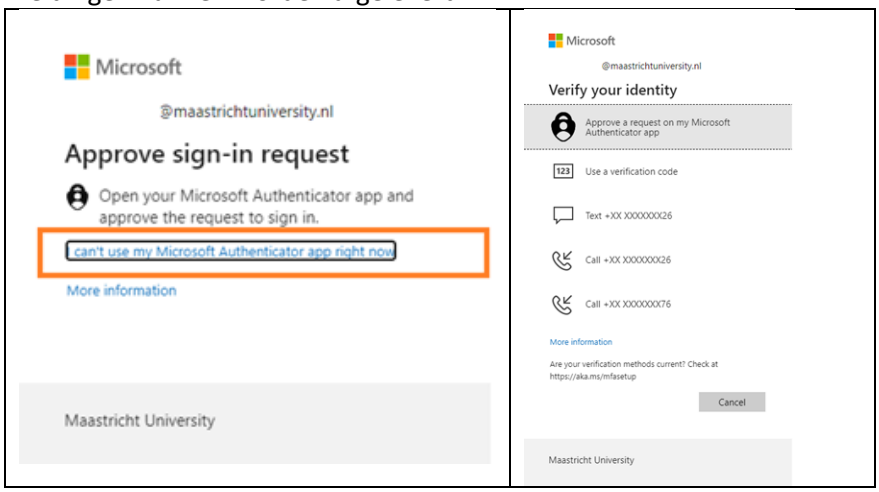
Hoe kan ik een inlogmethode toevoegen of verwijderen?

Binnen de UM implementatie wordt standaard uitgegaan van het gebruik van de Microsoft Authenticator App. Wanneer je geen gebruik kunt maken van de App, kun je MFA instellen op basis van een alternatieve login methode, zoals een SMS of telefoontje (Phone call) naar een werk- of privé telefoonnummer. Dit kun je aanpassen op https://aka.ms/mfasetup.
We raden het erg aan om een extra authenticatie methode toe te voegen naast je standaardmethode.

Dit zorgt ervoor dat er altijd een manier is om in te loggen in je account in het geval dat er iets is gebeurd met je standaardmethode.
Zie ook de uitgebreide handleiding op de website https://www.maastrichtuniversity.nl/nl/mfa

Ik heb (tijdelijk) geen smartphone met de MFA-app beschikbaar. Wat nu?

Maak gebruik van een van de alternatieve verificatie opties die je kunt configureren.
Dit kan zijn; een extra telefoonnummer (mobiel of werk- of privénummer), dat door Microsoft kan worden gebeld of een extra device, waarop een authenticator app is geconfigureerd of waarop sms meldingen kunnen worden afgeleverd.



N.B.: Bovenstaande keuze verschijnt vooralsnog alleen bij web-toegang. Niet bij VPN of VDI.

Ik heb geen alternatieve verificatie optie ingesteld en kan niet inloggen. Wat nu?

Neem contact op met ICTS Servicedesk zodat er een temporary access pass (TAP) aan je beschikbaar kan worden gesteld. Voordat we dit aan je kunnen geven moet je een kopie of foto van een geldig ID-bewijs (e.g. rijbewijs/paspoort) naar ons sturen zodat we kunnen verifiëren dat we de code daadwerkelijk naar jou sturen. **We raden het erg aan om een extra authenticatie methode toe te voegen naast je standaardmethode**, zodat je dit kan voorkomen.

Wat is een Temporary Access Pass (TAP)?

Dit is een tijdelijke code (2u geldig) waarmee je je authenticatie methodes kunt aanpassen en een nieuwe factor kunt registreren voor jouw account via https://aka.ms/mfasetup.

Is het, naast een app melding, ook mogelijk om SMS of telefoongesprekken in te stellen?

Ja, je kunt via https://aka.ms/mfasetup een extra methode toevoegen. Je kunt op deze website ook je standaardmethode aanpassen.

Wat te doen in geval van een nieuwe/ reserve/ defecte/ gestolen smartphone?

In dat geval moet de Microsoft Authenticator app opnieuw ingesteld worden.

1. Voeg EERST je nieuwe / reserve *smartphone* toe via https://aka.ms/mfasetup (selecteer Add sign-in method).
2. Verwijder DAARNA je oude/defecte/gestolen smartphone via https://aka.ms/mfasetup.

Ik heb mijn smartphone vergeten en kan niet inloggen. Wat nu?

- Haal je smartphone op (indien mogelijk).
- Selecteer bij gebruik van een UM-webapplicatie een van de andere verificatie opties die je hebt ingesteld door te kiezen voor '*Use a different verification option*'.
- Wanneer je probeert in te loggen op VDI of VPN of wanneer je nog geen tweede verificatie optie hebt ingesteld: neem contact op met de Servicedesk ICTS.

Ik heb geen wifi/internet op mijn smartphone. Kan ik de Authenticator app toch gebruiken?

Voor de installatie/activatie van de app heb je internet via wifi of mobiele data nodig.

Kan ik iemand machtigen om namens mij op MFA te mogen inloggen?

Nee, het is nooit toegestaan toegangscodes over te dragen. Wachtwoorden en MFA zijn persoonsgebonden.

Waarom wil de Microsoft Authenticator app toegang tot de camera?

De app heeft alleen tijdens de configuratie toegang nodig tot je camera, omdat je hiermee een code moet scannen tijdens de installatie.

Kan ik ook een Yubikey als alternatieve factor opvoeren?

Dat kan bij een aantal Yubikeys in combinatie met een software authenticator.
Zie ook: Using YubiKeys with Azure MFA OATH-TOTP – Yubico

Waarom werkt MFA anders bij web-applicaties dan bij VPN en VDI?

VPN en VDI gebruiken momenteel nog een andere achterliggende MFA configuratie waardoor met name het gebruik van een alternatieve methode via een pop-up scherm nu nog niet mogelijk is.

De UM werkt nu met MFA. Kan ik dat ook privé gebruiken?

MFA wordt al toegepast op veel app's zoals die van je bank of DigiD. Op veel privé internetdiensten, zoals die van Microsoft en Google kun je ook MFA instellen. We raden je aan om MFA altijd te activeren als die mogelijkheid geboden wordt. Je kunt de meeste MFA-app's voor meerdere diensten gebruiken, wel zo handig.

Wordt MFA ook geactiveerd tijdens digitale toetsing?

Nee.

Ik heb geen UM smartphone en wil geen privé telefoon gebruiken (medewerkers).

Wanner de overige geadviseerde alternatieve opties (SMS of telefoontje) voor jou ook niet mogelijk zijn kun je een verzoek sturen naar je informatiemanager. Na beoordeling door de informatiemanager wordt het doorgestuurd naar de Servicedesk ICTS , waarna je z.s.m. wordt

geïnformeerd over het vervolg. Deze aanvragen zullen kritisch worden beoordeeld aangezien er kosten worden verbonden aan andere oplossingen.

Is MFA ook verplicht voor resource/service-accounts?

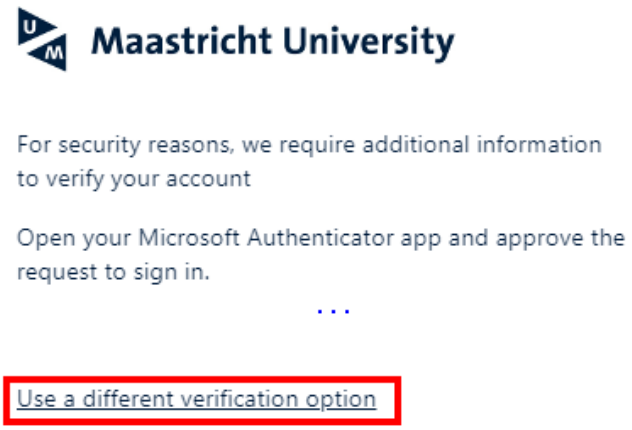
Op dit moment nog niet. Mocht dit veranderen dan word je daar nog over geïnformeerd.

Wanneer ik MFA wil configureren word ik steeds naar mijn andere MFA-registratie of Microsoft service login-pagina geleid.

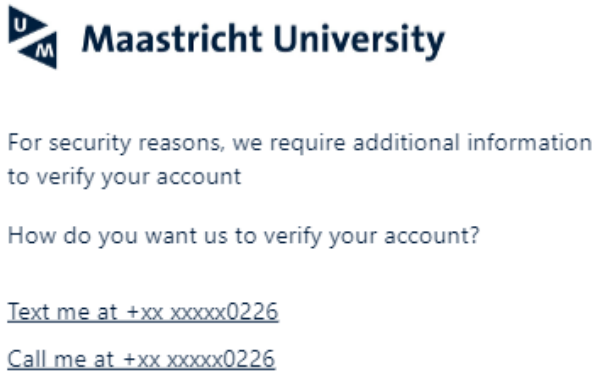
Mogelijk gebruik je al MFA (of een andere online Microsoft service) bij een andere organisatie.
Je kunt dit oplossen door een "incognito/inprivate"-tab in je browser te gebruiken.
Klik hier voor instructies

Ik heb de app van mijn telefoon verwijderd /ik heb een nieuwe telefoon en nu kan ik niet (meer) inloggen.

Wanneer je je gsm-nummer als alternatieve inlogmethode hebt toegevoegd kun je tijdens het inloggen klikken op “Use a different verification option” (Een andere verificatie optie gebruiken) en een SMS laten versturen naar je telefoon of een telefoontje ontvangen (afhankelijk van de door jou ingestelde opties).



Je kan de app opnieuw toevoegen op https://aka.ms/mfasetup door in te loggen met een SMS code of Phone call (ontvangen telefoontje). Zie onderstaand voorbeeld (weergave is afhankelijk van de ingestelde opties).



Ik heb geen alternatieve inlogmethode toegevoegd:

Stuur een email naar: servicedesk-icts@maastrichtuniversity.nl met je UM-gebruikersnaam en een kopie van een geldig ID-bewijs (geen UM-card). Zorg er daarbij voor dat je BSN-nummer, pasfoto en zogenaamde Machine Readable Zone aan de onderzijde van het document onleesbaar zijn gemaakt en breng op de kopie een tekst aan om aan te geven dat de kopie bestemd is voor een eenmalige MFA reset. Geadviseerd wordt om hiervoor de Kopie ID app van de overheid te gebruiken.
Wij maken dan een TAP code voor je aan die je kan gebruiken om in te loggen op https://aka.ms/mfasetup waarna je een nieuwe authenticatie methode kan toevoegen.
Voeg dan ook gelijk je telefoonnummer toe als back-up optie.