

Identity & Access Management (IAM)

Multi-Factor Authentication

SSO – login.tudelft.nl



Handleiding

Single Sign On en 2-Stapsverificatie



Versie beheer:

Persoon	Datum	Versie
M. Soehawan	01-09-2022	v0.1
O. Oduncu	26-10-2022	v0.2

Inhoudsopgave

1 Inloggen	4
1.1 NetID.....	4
2 Sterke authenticatie	5
2.1 SMS Code	5
2.2 Authenticator App.....	6
2.2.1 Smart-device registratie	6
2.2.2 Aanmelden	10
2.3 Back-up en herstel.....	11

1 Inloggen

Op alle diensten van de TU Delft waar een login voor benodigd is, zal je met een NetID account moeten aanmelden. Dit NetID is een persoonlijke account welke gekoppeld is aan de registratie van jou verbintenis met de TU Delft.

1.1 NetID

Met jou NetID en wachtwoord kan je op alle diensten aanmelden via het “Single Sign On - SSO” principe. Wanneer je op een TU Delft dienst aanmeld, zoals bijv. een BrightSpace of het intranet, krijg je een login pagina van ‘login.tudelft.nl’ te zien:

[English](#) | [Nederlands](#)



Meld u aan voor toegang tot beveiligde diensten

Gebrowsersnaam	<input type="text" value="uw NetID"/>
Wachtwoord	<input type="password" value="uw wachtwoord"/>

Inloggen

Sluit deze webbrowser om de met toegangscontrole beveiligde diensten te verlaten.

Een browser bewaart een login ticket in het geheugen. Zolang dit ticket nog niet is verlopen en de browser niet is gesloten, is dit ticket geldig en te gebruiken door iedereen die toegang heeft tot deze browser. Sluit deze browser dus om de beveiligde diensten te verlaten, zeker als je ingelogd bent op een publieke computer.

[Wachtwoord vergeten?](#)

[Problemen met inloggen? Neem dan contact op met een van de Servicepunten.](#)

Wanneer je voor de eerste keer met je NetID wil aanmelden, is het belangrijk om je NetID te activeren voor gebruik. Door een initiële wachtwoord in te stellen via “password.tudelft.nl” wordt jou NetID daarmee ook actief gesteld, en klaar om bijvoorbeeld aan te melden via SSO.

Lukt het niet om aan te melden? Dan kan je het wachtwoord van jou NetID ook via “password.tudelft.nl” aanpassen/herstellen.

2 Sterke authenticatie

Op een aantal diensten die de TU Delft levert zal er bij het aanmelden via SSO, een extra beveiligingsmaatregel toegepast worden. Hierbij valt te denken aan diensten zoals een EduVPN waarvoor het van belang is om een tweede factor authenticatie toe te passen.

2.1 SMS Code

Na het aanmelden met jou NetID en wachtwoord, zal er in sommige gevallen een sterkere authenticatie vorm toegepast worden. In het volgende scherm zal er dan gevraagd worden om een SMS code in te voeren.

Bij jou registratie voor bij de TU Delft is er een mobiele nummer vastgelegd voor o.a. mee aan te melden op een aantal TU Delft diensten.



Two factor authentication

Authenticator app instellen



Op dit moment gebruik je SMS voor 2-staps verificatie. Een veiliger, betrouwbaarder en sneller alternatief is het gebruik van een Authenticator app op je mobiele telefoon. Stel nu een Authenticator app (bijvoorbeeld Microsoft Authenticator) in, zodat een veilige 2-staps inlogcode altijd direct en overal beschikbaar is op je mobiele telefoon.

[Authenticator app instellen*](#)

*Het aanmeldproces voor de beveiligde dienst wordt onderbroken.

Tijd over om je SMS code in te voeren: 6 Min. 59 sec.

SMS code

[Code opnieuw verzenden](#)

[OK](#)

Sluit deze webbrowser om de met toegangscontrole beveiligde diensten te verlaten.

Een browser bewaart een login ticket in het geheugen. Zolang dit ticket nog niet is verlopen en de browser niet is gesloten, is dit ticket geldig en te gebruiken door iedereen die toegang heeft tot deze browser. Sluit deze browser dus om de beveiligde diensten te verlaten, zeker als je ingelogd bent op een publieke computer.

Heb je geen mobiele nummer opgegeven en of ontvang je geen SMS? Controleer dan jou NetID profiel op "e-service.tudelft.nl" om zo je mobiele nummer te controleren en aanpassen.

Let op: mobiele nummers kunnen alleen aangepast worden als je op de TU Delft Campus aanwezig bent. In alle overige gevallen zal je met de Servicepunten contact moeten opnemen om het voor jou te laten aanpassen. Legitimatie hiervoor is verplicht.

2.2 Authenticator App

Het versturen van een SMS bericht is helaas niet zo betrouwbaar, en komt zelfs in sommige gevallen niet aan. Hiervoor krijg je de mogelijkheid om een veiliger en betrouwbaar alternatief te gebruiken wanneer er een tweede factor aan authenticatie (2FA) benodigd is.

Op het SMS code invoer scherm zie je de melding om een andere vorm van 2FA te gebruiken dan SMS:



Wanneer je op “Authenticator app instellen” drukt, zal het ‘smartphone’ registratie proces gestart worden.

Advies is om de Microsoft Authenticator App te gebruiken:

<https://www.microsoft.com/nl-nl/security/mobile-authenticator-app>

2.2.1 Smart-device registratie

Voordat je een smartphone of tablet kan registreren, zal je eerst met de bij ons bekende mobiele nummer moeten verifiëren middels een SMS code. Het kan zijn dat je een tweede SMS bericht ontvangt als je voor het eerst een ‘smart-device’ wil registreren:

In het volgen scherm krijg je de huidige sterke authenticatie vorm te zien, en zal je daar op “Verander je 2-steps verificatie methode” knop moeten drukken:

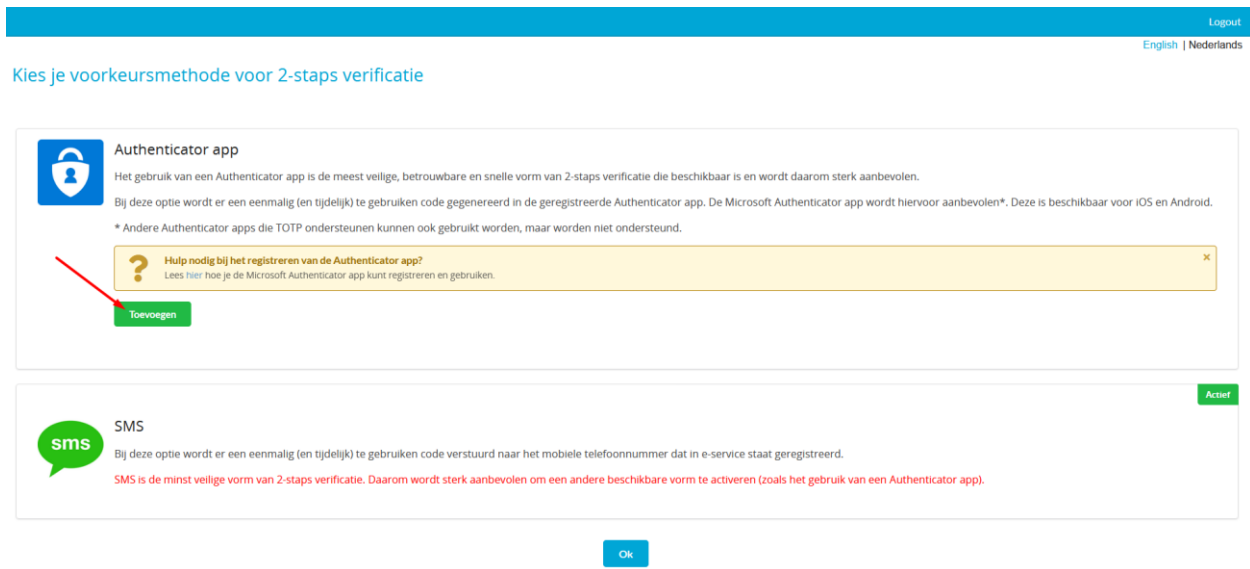


2-Steps verificatie methode

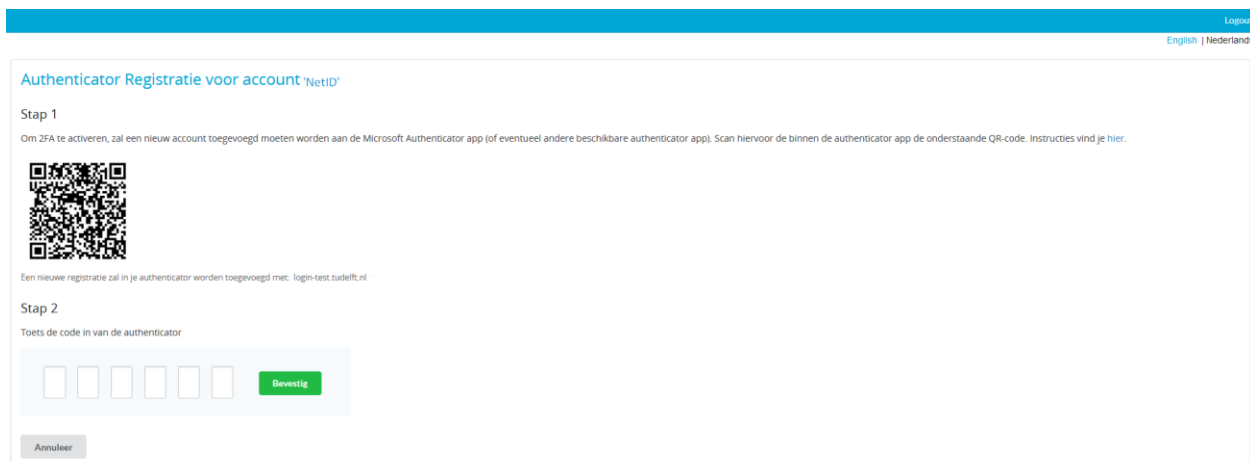
Je huidige 2-steps verificatie methode **authenticator**

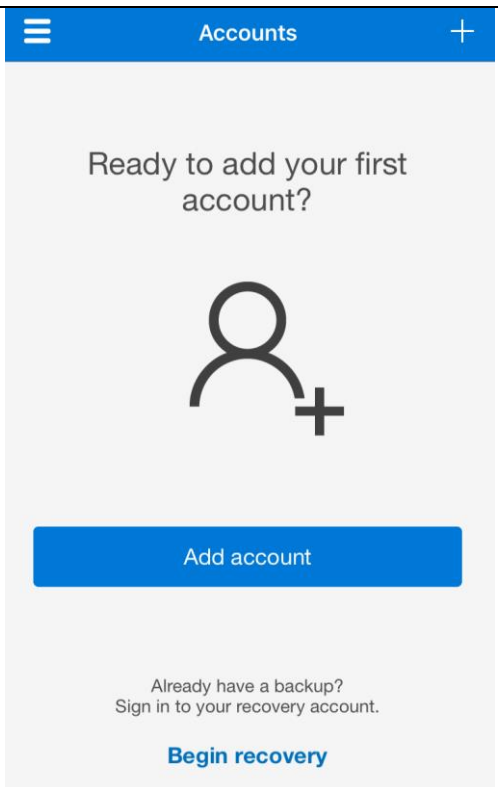
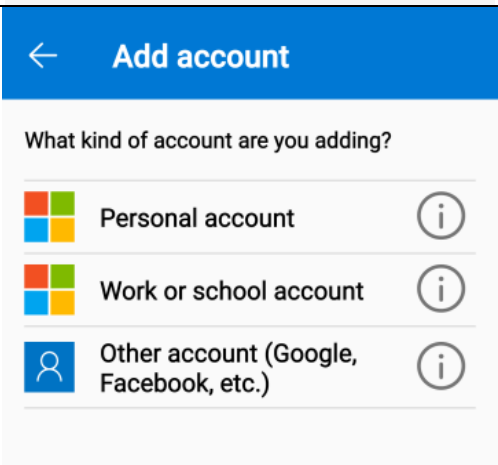
[Verander je 2-steps verificatie methode](#)

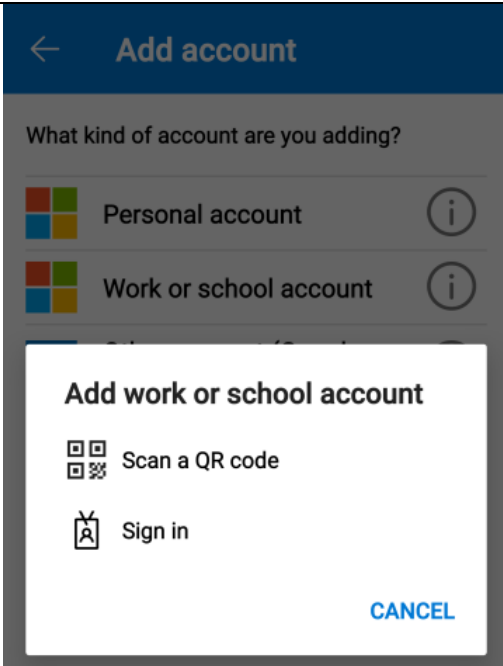
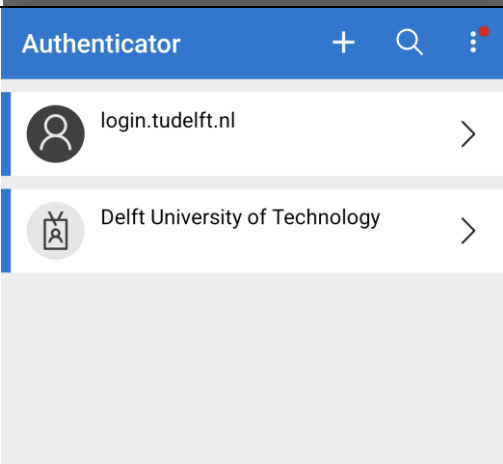
Nadat je de [Microsoft Authenticator App](#) hebt geïnstalleerd, kan je in de volgende scherm een smart-device toevoegen aan jou profiel:



Door op “toevoegen” te drukken zal het volgende scherm getoond worden:



<p>Stap 1</p>	<p>Open de Microsoft Authenticator app en klik op '+' Account toevoegen' om een nieuwe koppeling toe te voegen</p>	
<p>Stap 2</p>	<p>Kies in het overzicht voor 'Persoonlijk account' of voor 'Werk- of schoolaccount'</p>	

<p>Stap 3</p>	<p>Kies in de app voor 'Een QR-code scannen'</p>	
<p>Stap 4</p>	<p>Klik in de App “op login.tudelft.nl”, en geef de getoonde code op ter controle in dit scherm</p>	

Bij een correcte code is de koppeling gelukt, en zal je de volgende succes berichten pagina te zien krijgen:

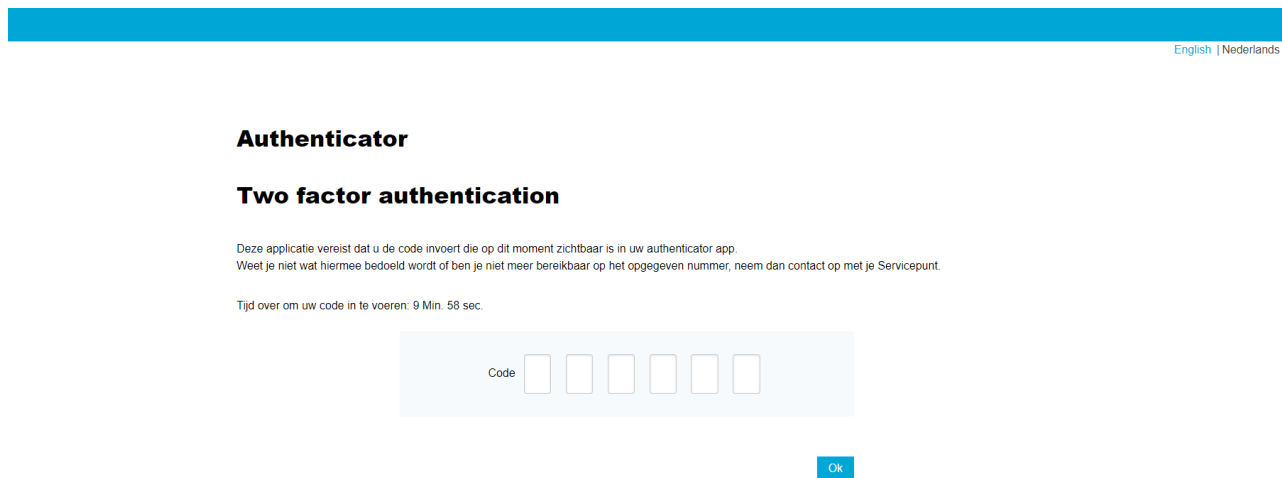


Hiermee is de registratie proces voltooid, en kan je deze sessie afsluiten om het aanmeld proces te hervatten.

Belangrijk: Vergeet niet om de “Cloud Back-up” functie in de Microsoft Authenticator App in te schakelen! Mocht je de smart-device of App kwijtraken, dan kan je de wachtwoordcodes alsnog herstellen door aan te melden met het gekoppelde Microsoft ‘herstel-account’ in de Microsoft Authenticator App.

2.2.2 Aanmelden

Na het succesvol registreren van jou smart-device zal je bij iedere TU Delft dienst waarvoor 2-staps verificatie voor vereist is, het volgende scherm te zien krijgen:



The screenshot shows a mobile application interface for two-factor authentication. At the top right, there is a language selector: "English | Nederlands". The main heading is "Authenticator", followed by the sub-heading "Two factor authentication". Below this, there is a small explanatory text: "Deze applicatie vereist dat u de code invoert die op dit moment zichtbaar is in uw authenticator app. Weet je niet wat hiermee bedoeld wordt of ben je niet meer bereikbaar op het opgegeven nummer, neem dan contact op met je Servicepunt." Underneath the text, a timer indicates "Tijd over om uw code in te voeren: 9 Min. 58 sec.". The central part of the screen features a light blue box with the label "Code" and six empty input fields for entering the authentication code. At the bottom right of this box, there is a blue "Ok" button.

Het SMS profiel is hiermee als back-up methode ingesteld, en zal je voortaan altijd met een Authenticator App de code moeten invoeren.

Open de Microsoft Authenticator App, klik op "**login.tudelft.nl**" om jou 2-staps verificatie code op te vragen.

Het kan zijn dat je meerdere profielen in de Microsoft Authenticator App hebt geristreerd staan, let daarom goed op de naam van het wachtwoordcode-profiel.

Let op: deze code verandert iedere 30 seconden!

2.3 Back-up en herstel

Mocht je het smart-device of app niet meer tot jou beschikking hebben, dan kan je die op de volgende twee manieren herstellen:

1. Log opnieuw in met jou Persoonlijke of werk Microsoft account in de Microsoft Authenticator App.
2. Als stap 1 niet lukt, neem dan contact op met de Servicepunten om jou 2-stapsverificatie profiel te verwijderen.

Hiermee zal je bij de volgende aanmeldpoging de Authenticator App registratie proces weer mogen starten.