

Identity & Access Management (IAM)

Multi-Factor Authentication

SSO – login.tudelft.nl



Manual

Single Sign On and 2 Factor Authentication



Version control:

Person	Date	Version
M. Soehawan	01-09-2022	v0.1
O. Oduncu	07-11-2022	v0.4

Table of contents

- 1 Login 4
 - 1.1 NetID..... 4
- 2 Strong Authentication 6
 - 2.1 SMS code 6
 - 2.2 Authenticator App..... 7
 - 2.2.1 Smart device registration..... 7
 - 2.2.2 Sign On 12
 - 2.3 Backup and Restore..... 13


1 Login

For all services at the TU Delft that require login, you will need a NetID account. This NetID is a personal account, which is linked to your registration at the TU Delft.

1.1 NetID

You can login with your NetID and password at TU Delft services provided via Single Sign On (SSO). When trying to logon to a TU Delft service such as Brightspace or the Intranet, you will see the following login page "login.tudelft.nl":

English | [Nederlands](#)



Please login to access login-protected services

Username

Password

Login

Close your webbrowser to quit the login-protected services
A browser has the login ticket in memory. As long as the ticket is not expired and the browser is not closed, the login ticket is still valid and can be used by anyone who has access to your browser. So close your browser to quit the protected services, especially if you're logged in on a public spot.

[Forgot your password?](#)
[Experiencing trouble with your login? Contact one of the Service Desks.](#)

It is important to activate your NetID first on "password.tudelft.nl". Your NetID will be activated and ready to use after you have set an initial password.

Unable to logon?

Go to "password.tudelft.nl" to change your current password or use the "forgot my password" option.

Please Sign in

Self Service Password Reset

NetID / Username

Current Password

Sign in

🔒 [Activate NetID/Forgot my password?](#)

2 Strong Authentication

Stringer security measures are applied to services provided by the TU Delft when you are logging in via SSO. This includes services such as EduVPN and or other TOPdesk for example.

2.1 SMS code

After logging in with your NetID and password, a stronger authentication method will be applied in some cases. In the next screen you are asked to enter an SMS code.

During your initial registration for at the TU Delft, a mobile will be registered as it is required for two factor authentication with the provided NetID.

English | [Nederlands](#)



Two factor authentication

This application requires an SMS code that has been sent to your mobile phone number as registered at e-service.tudelft.nl.

For more information and assistance, contact your Service Desk.

Time left to enter your SMS code: 9 Min. 54 sec.

SMS code

[Send code again](#)

[Ok](#)

Close your webbrowser to quit the login-protected services

A browser has the login ticket in memory. As long as the ticket is not expired and the browser is not closed, the login ticket is still valid and can be used by anyone who has access to your browser. So close your browser to quit the protected services, especially if you're logged in on a public spot.

Not receiving SMS codes?

Please go to "e-service.tudelft.nl" and check your NetID profile on which mobile number your account is using. Add or modify your mobile number as needed.


Note: mobile numbers can only be changed if you are present at the TU Delft Campus. In all other cases you will have to contact the Service Desk to have it adjusted for you. Identification for this is required.

2.2 Authenticator App

Sending SMS messages is unfortunately not always reliable, in some cases it is not delivered or delayed exponentially. For this there is we are providing a more secure and reliable alternative when a second factor of authentication (2FA) is required.

On the SMS code input screen, you will see a message to use a different method of 2FA other than SMS:

Two factor authentication



Stronger 2-factor authentication method recommended

Currently you are using SMS for 2-factor authentication. A more secure, reliable and faster alternative is to use an Authenticator app on your mobile phone. Set up an Authenticator app (e.g. Microsoft Authenticator) now, to ensure a secure 2FA code will be available in the app anytime and anywhere.

[Set up Authenticator app*](#)

*The login process for the protected service will be interrupted.

When you press “Set up authenticator app”, the registration process will be started.


You are advised to use the Microsoft Authenticator App:

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

2.2.1 Smart-device registration

Before the registration of a smartphone or tablet, you will first have to authenticate with an SMS code. You may receive a second SMS message if you are registering a 'smart-device' for the first time:

English | [Nederlands](#)



Two factor authentication

This application requires an SMS code that has been sent to your mobile phone number as registered at e-service.tudelft.nl.

For more information and assistance, contact your Service Desk.

Time left to enter your SMS code: 9 Min. 54 sec.

SMS code

[Send code again](#) [Ok](#)

Close your webbrowser to quit the login-protected services

A browser has the login ticket in memory. As long as the ticket is not expired and the browser is not closed, the login ticket is still valid and can be used by anyone who has access to your browser. So close your browser to quit the protected services, especially if you're logged in on a public spot.

In the next screen you will see your current authentication method, where you will have to press the “Change your 2-factor verification method” button:



2-Factor verification method


Your current 2-Factor verification method **sms**

Change your 2-factor verification method

After installing the [Microsoft Authenticator App](#), you can add your smart device to your profile in the next screen:

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

Choose your preferred method for 2-factor authentication




Authenticator app


Using an Authenticator app is the most secure, reliable and fast 2-factor authentication method available, and is therefore highly recommended.

With this option a one-time code will be generated in the registered Authenticator app. The advised app to use is the Microsoft Authenticator app* that is available on iOS and Android

* Other Authenticator apps that support TOTP can be used as well, but will not be supported.

 **Need help to register the Authenticator app?**
Read [here](#) how to register and use the Microsoft Authenticator app.

Add



SMS

With this option a one-time code will be sent in a textmessage to the mobile phone number that is registered in e-service.

SMS is the least secure form of two-factor authentication. Therefore it is highly recommended to activate another available option (like the usage of an Authenticator app).

Active

Ok

You will be presented the following screen by pressing “Add”:

Step 1

In order to activate 2FA, it is needed to add an account to the Microsoft Authenticator app (or other authenticator app that you prefer). Please scan the QR-code you find here below, with the authenticator app. You can find the instructions [here](#).



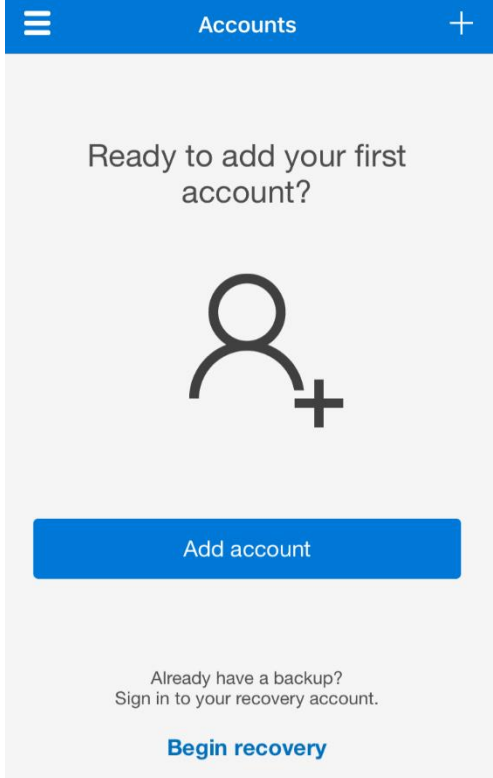
A new entry will be added in your authenticator showing: 'login-test.tudelft.nl (msoehawan)'

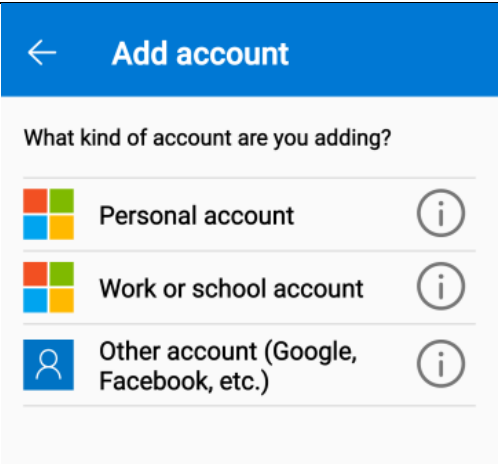
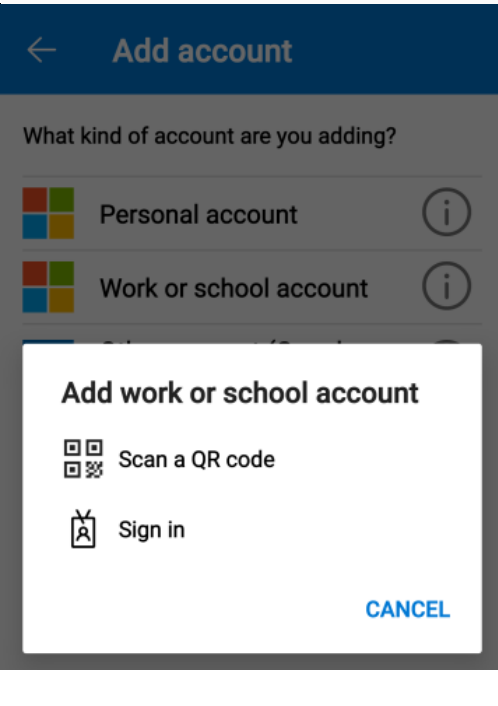
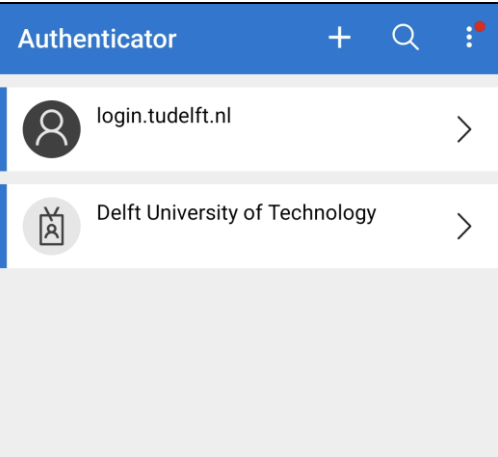
Step 2

Enter the code from the authenticator

Confirm

Cancel

Step 1	Open the Microsoft Authenticator app and select '+' Add account to add a new connection	
---------------	---	---

Stap 2	Choose “ <i>Other account (Google, Facebook, etc.)</i> ” from the overview	
Stap 3	Scan the displayed QR code	
Stap 4	Select “login.tudelft.nl” and use the presented code for confirming the smart-device registration process.	

With a correct code input, your smart-device registration should be successful followed by the following confirmation:

Authenticator Activation

Activated

Congratulations! (Improved) 2FA has been activated for your NetID. Where an application requires strong authentication, you will now be asked to fill in the code as generated by the authenticator app.

Ok

The registration process should now be successfully completed. Close this browser or session to resume with your login.

Important: Do not forget to enable the “Cloud Backup” feature available in the settings of the Microsoft Authenticator App! This allows you to perform a recovery of your connections should you loose or change your current device.

Please follow these extended instructions for enabling backup features in the Microsoft Authenticator App:
<https://support.microsoft.com/en-us/account-billing/back-up-and-recover-account-credentials-in-the-authenticator-app-bb939936-7a8d-4e88-bc43-49bc1a700a40>

2.2.2 Authentication

After the succesfull registration of your smart-device you will be prompted the following two factor authentication screen when login in via SSO:

English | [Nederlands](#)

Authenticator

Two factor authentication

This application requires a one time password from your authentication app.
For more information and assistance, contact your Service Desk.

Time left to enter your code: 9 Min. 51 sec.

Code

Ok

The SMS option is now setup as your failover method and as of now you will always have to enter the code from an Authenticator App.

Open the Microsoft Authenticator App, and select the “**login.tudelft.nl**” profile to see your 2FA code.

It is likely you have registered multiple profiles in your Microsoft Authenticator App. Make sure to use the correct profile distinguishable by it's name.

Note: the authentication code changes every 30 seconds!

2.3 Backup and Restore

If for whatever reason you no longer have access to your smart device, you can restore access using one of these methods:

1. (re)install and open the Microsoft authenticator App
2. login with your personal or work Microsoft account within the App.
- 3.

If the steps above did not provide any solution, you should then contact of the Servicepoints according to your faculty so that may delete your 2FA profile.

By doing this, the next time you login you will prompted to register a new smart-device again.

Important: By deleting the 2FA profile, the authentication process will revert to the default SMS method. If for some reason you are not receiving any SMS codes, check your mobile number in e-service.tudelft.nl or contact the Servicepoint from your faculty to change it for you. Identification will be required when requesting this via the Servicepoints.