# YubiKey Multi-Factor Authentication

for Microsoft Services and TUD account (NetID)

TUDelft

# Manual

## YubiKey MFA-registration

.

**Version:**

| Persoon | Datum | Versie |
|---|---|---|
| A. Gorgees | 08-03-2024 | v0.1 |
| | | |
| | | |

# Table of contents

# 1 Introduction

We recommend using Microsoft Authenticator as your verification method, but you can also choose from other options, such as YubiKey. This manual describes how to install and use the Yubikey with the accompanying Yubico Authenticator app when logging in to Microsoft services and business applications such as TOPdesk and Basware Alusta.

**What do I need to configure YubiKey?**
- Yubico Authenticator app
- YubiKey (physical key)
You can order the Yubikey in the external webshop 'ARP webshop for employees' in Basware.

Unlike the Microsoft Authenticator, YubiKey adds an extra layer of security by using a physical key. This YubiKey must be connected to your device before you can use the Yubico Authenticator.

Follow this guide to use YubiKey as an MFA method for your Microsoft Work account and/or your TUD account (NetID).

# 2 Add YubiKey as MFA method

## 2.1 Install Yubico Authenticator app - Windows

**<u>Windows</u>**
Install the 🔲 Yubico Authenticator app, which is available in the Software Center. When you open the app, the following screen will appear asking you to connect your YubiKey to your device:
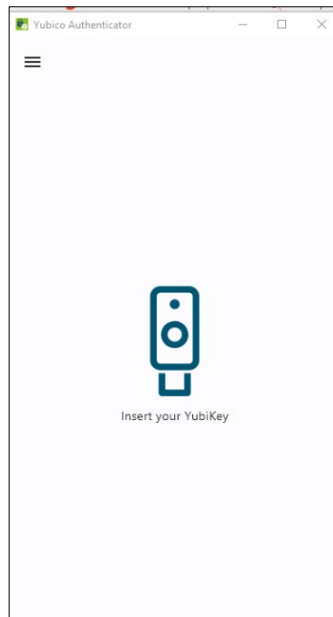


Connect your YubiKey (physical key) to your device. After it has been successfully connected, the 🔲 Yubico Authenticator app shows an empty screen: "**No accounts**".
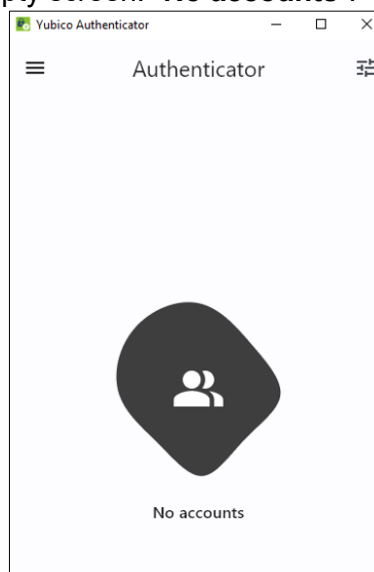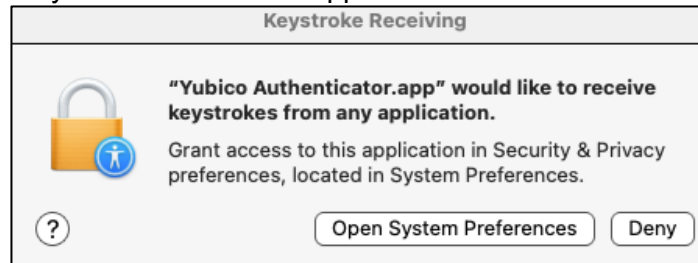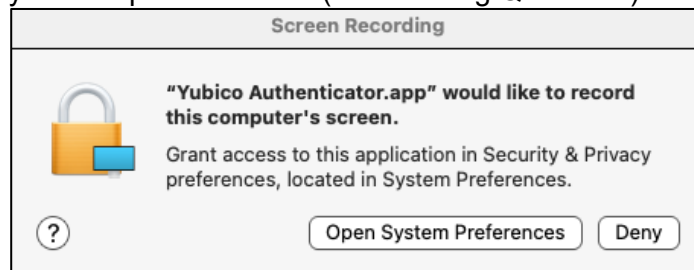
## 2.1 Install Yubico Authenticator app - macOS

**macOS**
Install the ⬛ Yubico Authenticator app, which is available in Self Service (or via https://software.tudelft.nl on your private device). Then connect the Yubikey to your device. Once installed, the ⬛ Yubico Authenticator requires the following:

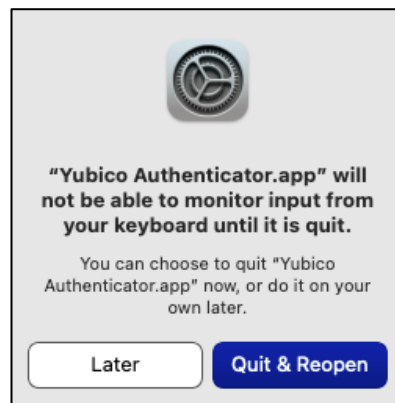- Permission to receive keystrokes from other applications:



- Permission to record your computer's screen (for scanning QR codes)



Open the "**System Preferences**" and make sure Yubico Authenticator is checked:



Finally, the message below will follow to apply the changes. Close the ⬛ Yubico Authenticator app and restart it with the button "**Quit & Reopen**":

## 2.2 Microsoft MFA registration

**Step 1a**: Go to https://aka.ms/mfasetup on a desktop computer or laptop and log in.
If you have not yet registered an MFA device (for example, new employees), continue with
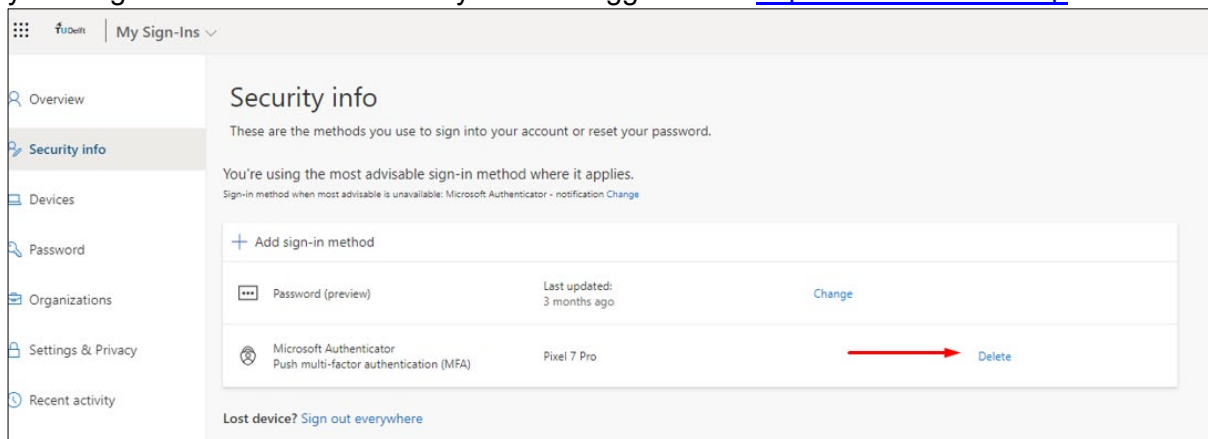**step 3.**

Within your Microsoft account it is possible to set up multiple MFA methods (e.g. Microsoft Authenticator +
YubiKey). Please note that the **default method** is Microsoft Authenticator. You will always see the Microsoft
Authenticator screen first when logging in (see image below). To then use your *other* MFA method, choose **"I
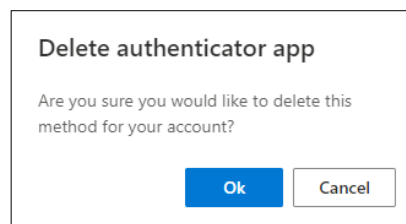cant use my Microsoft Authenticator app right now"**
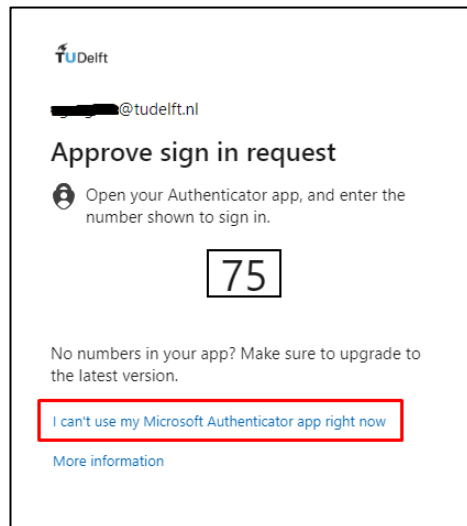


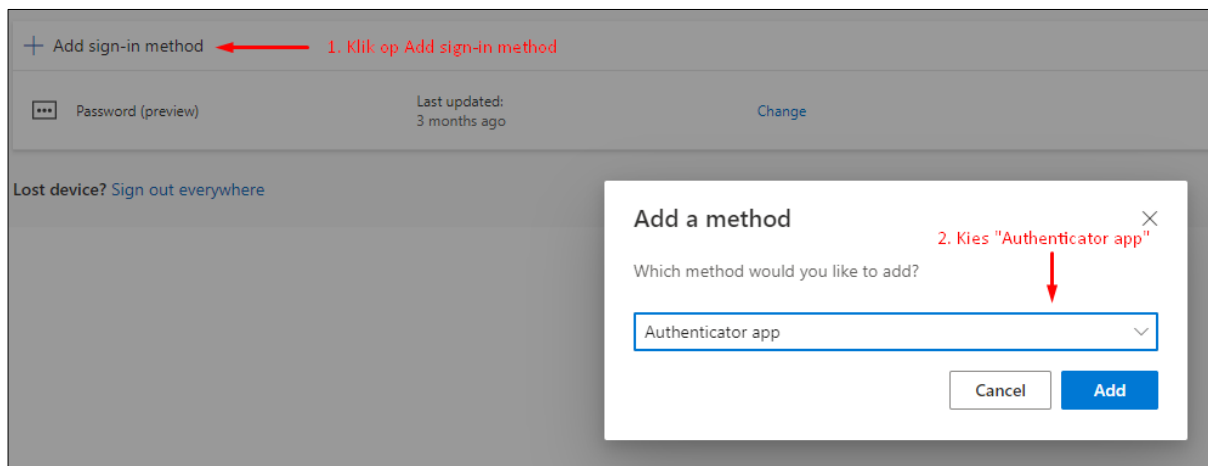Then choose the other method you configured:

If you only want to use the YubiKey as your MFA-method, remove the existing Microsoft Authenticator MFA method by clicking the "**Delete**" button after you have logged in via https://aka.ms/mfasetup:
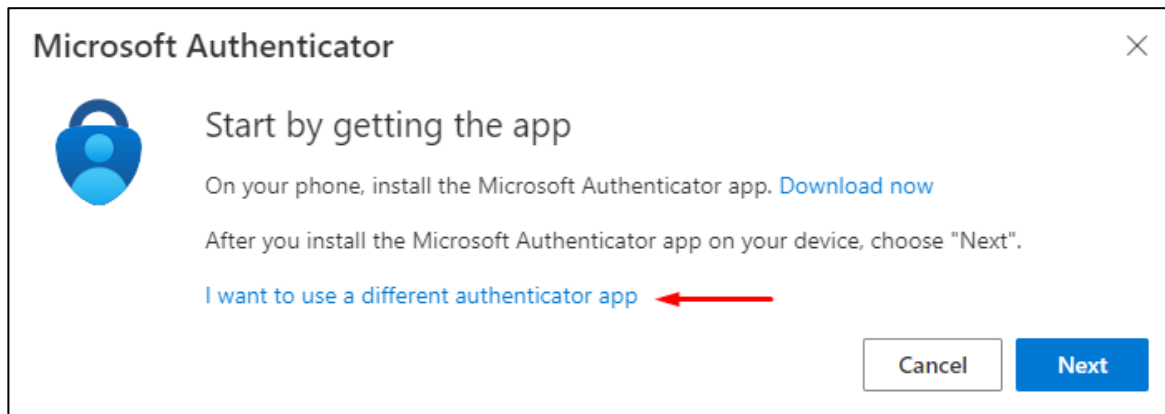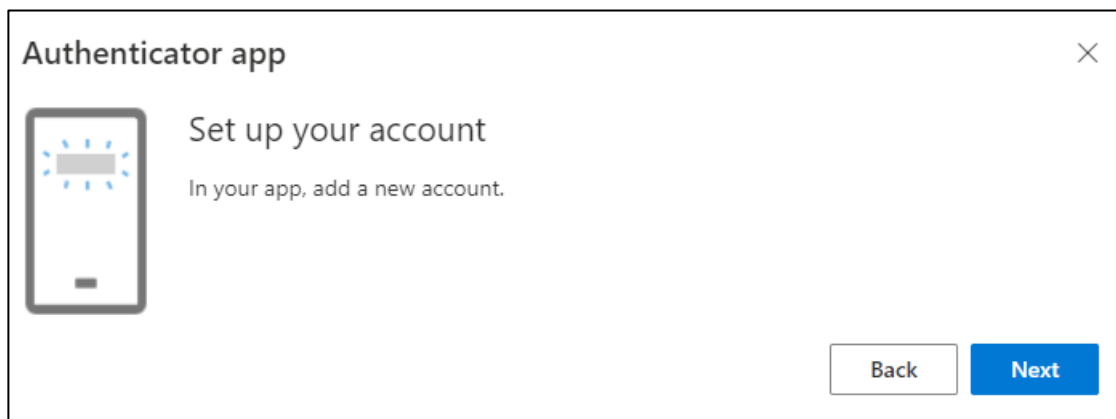


**1b**. Then click "**OK**":



**Step 2**. Click on **Add sign-in method**: choose Authenticator app and click on "**Add**"
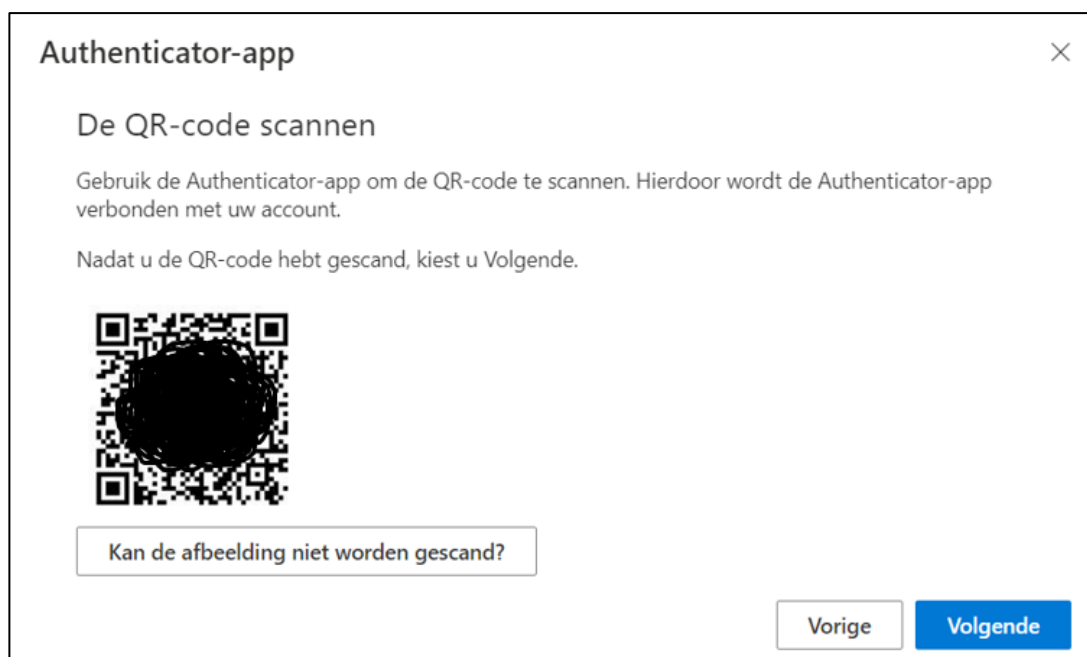
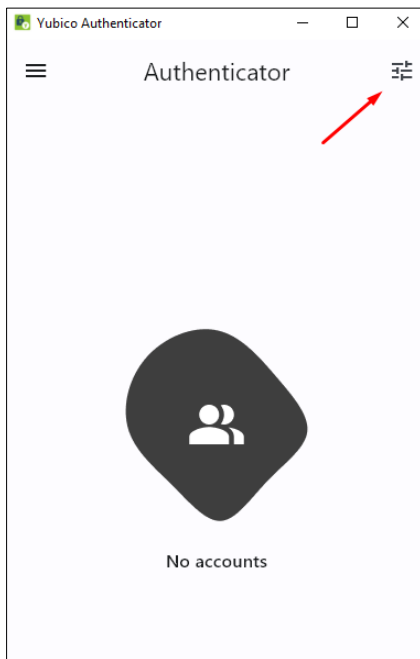**Step 3:** Click here on **"I want to use a different authentication app"**



**Step 4a:** The following screen will now be shown. Click "**Next**":
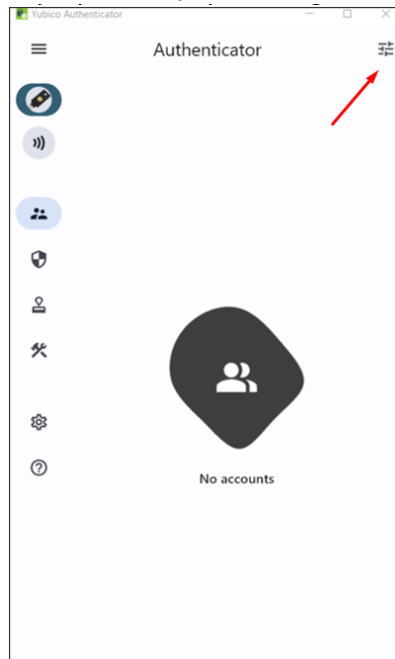


**4b.** A QR code is now shown.

**Step 5:** Now open the 🔲 Yubico Authenticator app on your desktop/laptop and click on the following button:
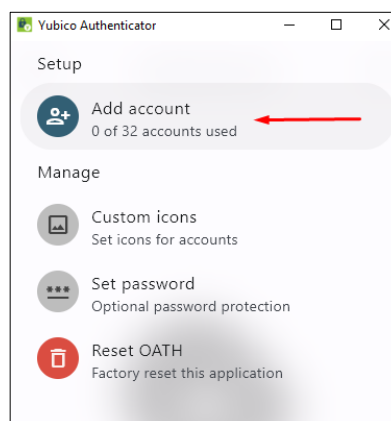


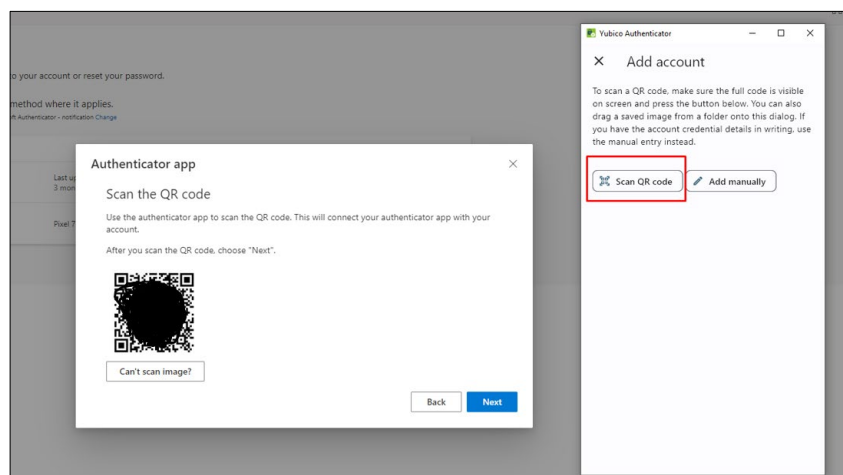*Windows 10*                    *Windows 11*                    *macOS*
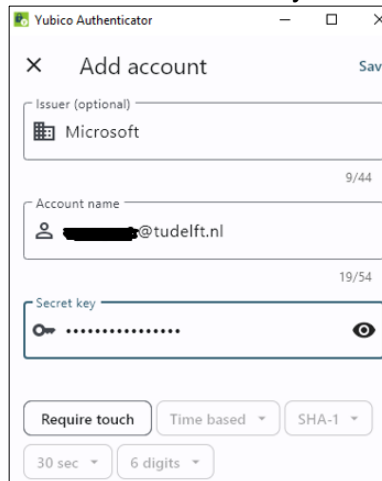
**Step 6:** Click on "**Add account**"



**Step 7:** The 🔲 Yubico Authenticator (right) now shows two options. Choose "Scan QR code" while your browser is open (left). In this way, the 🔲 Yubico Authenticator automatically takes over the data by scanning the QR code on your screen.
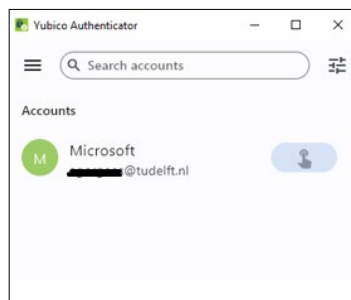
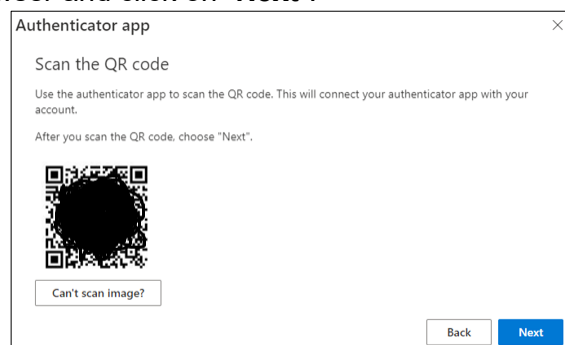If this is done successfully, the data will be filled in automatically:



If desired, you can choose in this screen that a "Touch" action is always required. This means that you must first physically touch the YubiKey on the "touch" part before a code is generated that you can use to log in. The rest of this manual is based on the "**Require touch**" option.

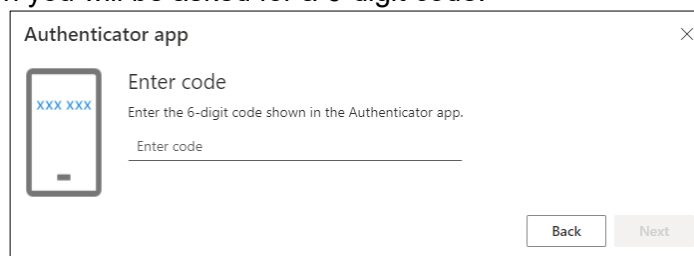Finally, click on "**Save**" at the top right.
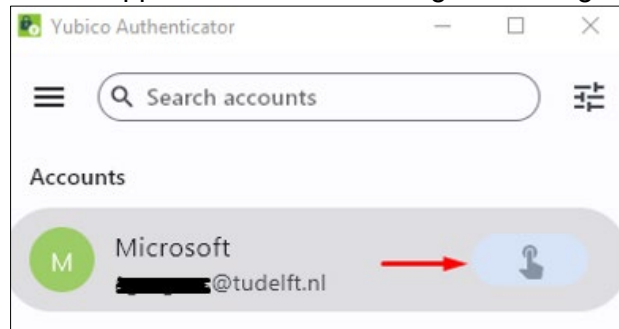Your Microsoft account is now added and visible in the Yubico Authenticator app:



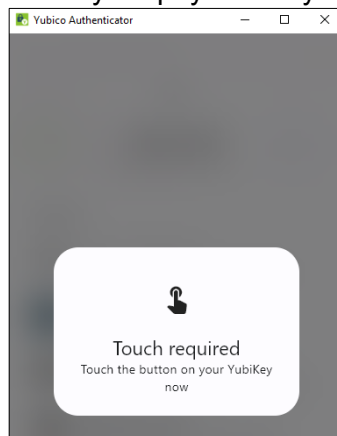**Step 8a:** Now go back to the browser and click on "**Next**":



**8b:** In this next screen you will be asked for a 6-digit code.

**8c**: Return to the 🟢 Yubico Authenticator app. Click on the following button to generate a 6-digit code:



**8d:** 🟢 Yubico Authenticator requires a "touch" on your physical key. Touch the "button" on your physical key.



**8e:** The 6-digit code was generated in the 🟢 Yubico Authenticator app (right). Click on "**Copy to clipboard**" and now paste this code into the browser (left). Then click **Next** in the browser:
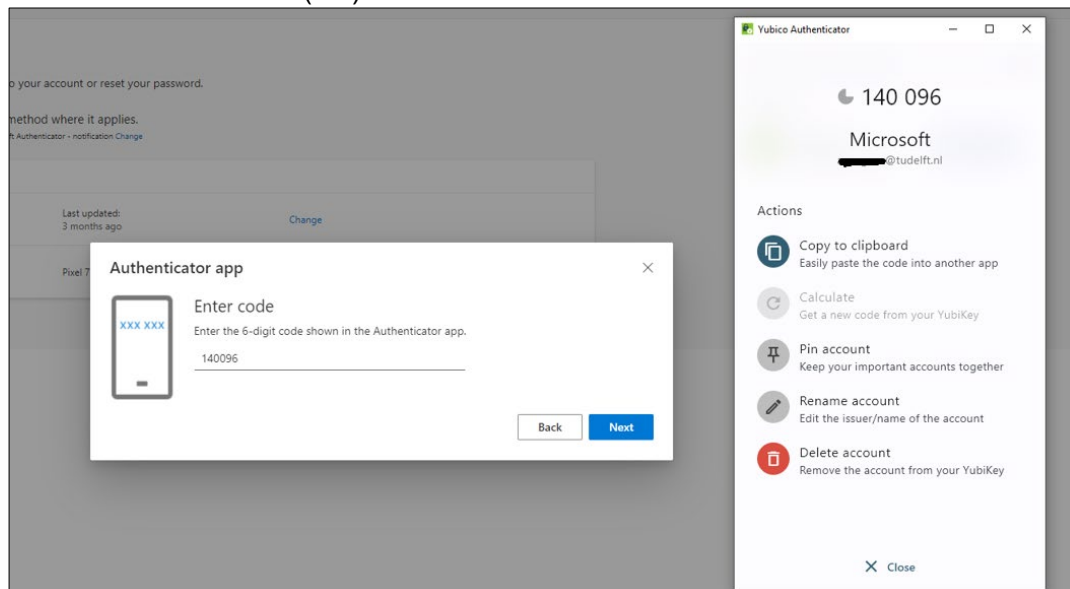
The connection is now made. If this is done successfully, a message will appear at the top right of your browser "**Authenticator app was successfully registered"**:
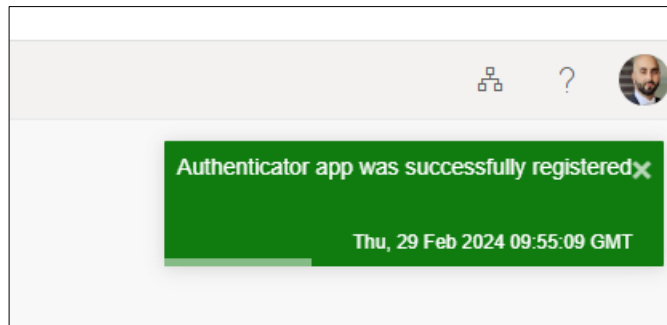


Success! Click on "**Done**"

YubiKey is now successfully configured as an authenticator. Every time you sign in to your Microsoft Work or School account, you'll be asked to enter a verification code from the ▣ Yubico Authenticator app.
**Please note:** the ▣ Yubico Authenticator app can only be used in combination with your physical key. You must therefore always connect this to your device to be able to use the functionalities of the app.

## 2.3 TUD account (NetID) MFA registration

You will have to log in with a NetID account to all TU Delft services that require a login. This NetID is a personal account that is linked to the registration of your commitment to TU Delft.
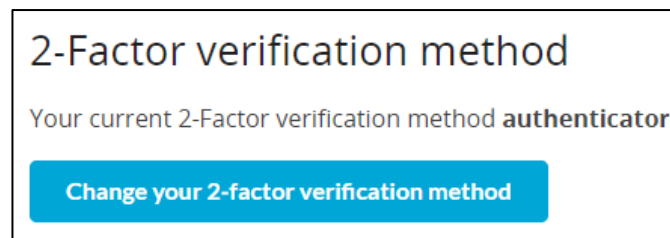
With your NetID and password you can log in to all services via the "Single Sign On - SSO" principle. When you register for a TU Delft service, such as BrightSpace or the intranet, you will see a login page of 'login.tudelft.nl':

An additional security measure will be applied to a number of services provided by TU Delft when registering via SSO. This includes services such as "eduVPN" for which it is important to apply a second factor of authentication (the full TUD MFA manual can be found here).

To configure **YubiKey** for your TUD account (NetID), follow the steps below.

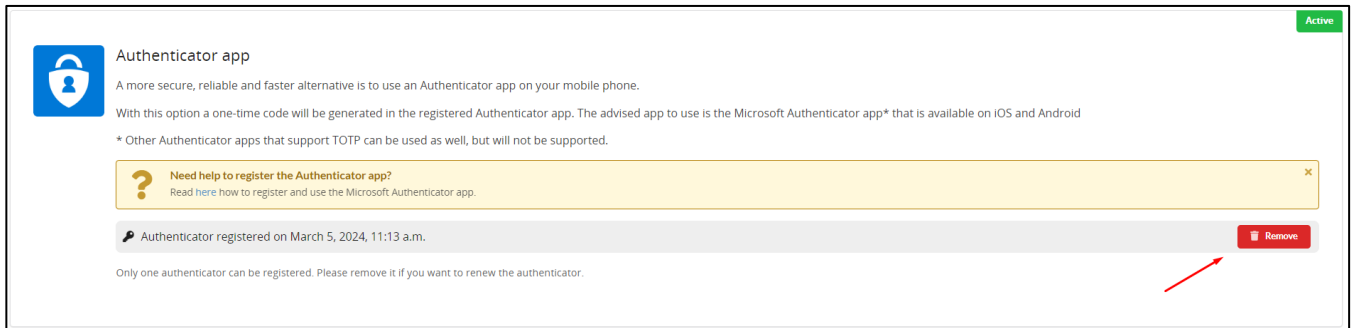**Step 1:** Go to https://login.tudelft.nl/mfa/. You will arrive at the following page:

 **Step 1a:** To change your MFA settings, click on "**Change current 2-factor verification method**"
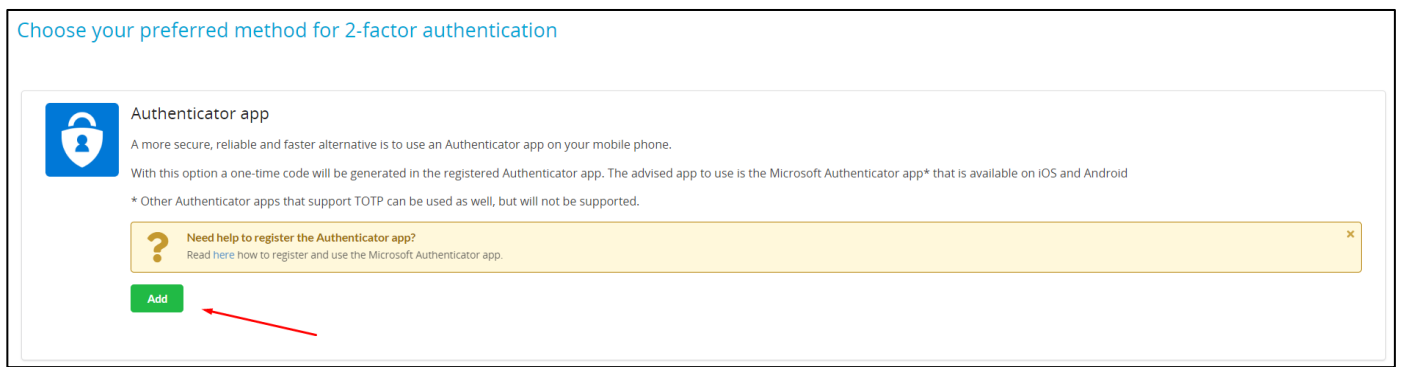
**Please note**: Only one authenticator can be registered. To use Yubikey as an authenticator, you must first delete the current registration.

**Step 2:** Remove your current authenticator by clicking the "**Remove**" button. Then confirm this Action by clicking "**Ok**".
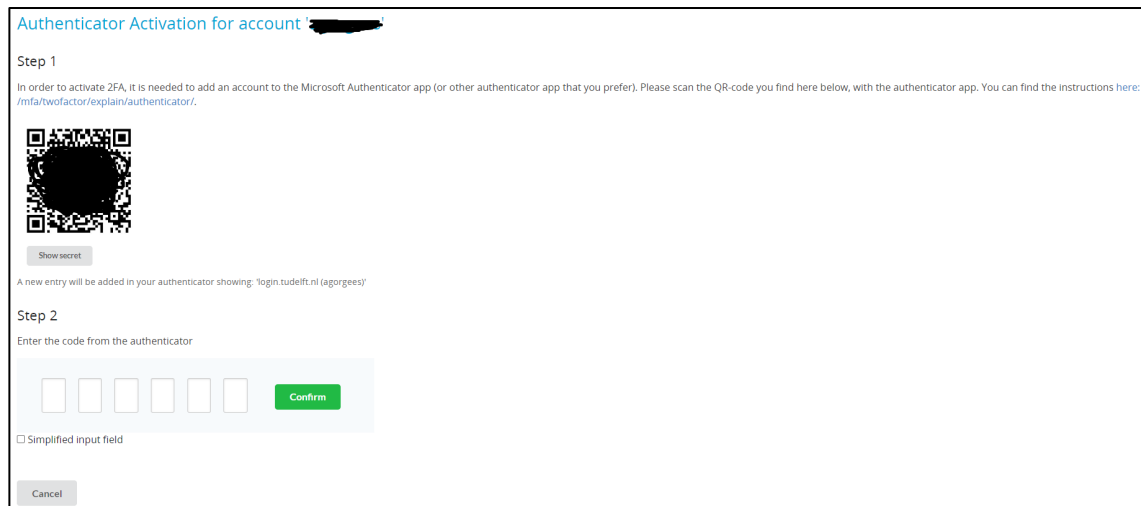


**Step 3:** Now click on the "**Add**" button:



**Step 4:** A QR code will be shown in your browser:

**Step 5:** Now open the 🟩 Yubico Authenticator app on your desktop/laptop and click on the following button:


*Windows 10*


*Windows 11*

**Step 6:** Click on "**Add account**"
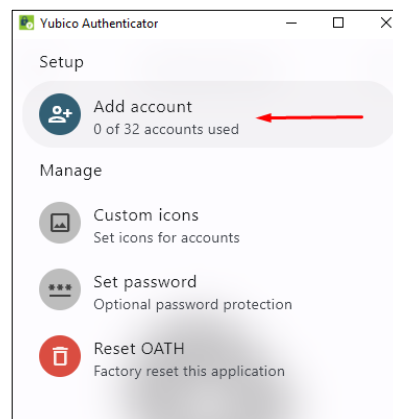
**Step 7:** The  Yubico Authenticator (right) toont nu twee opties. Choose "Scan QR code" while your browser is open (left). In this way, the  Yubico Authenticator automatically takes over the data by scanning the QR code on your screen.



**Step 7a:** If this is done successfully, the data will be filled in automatically:
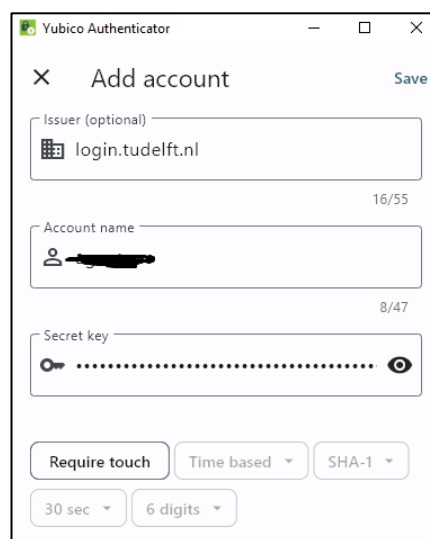
Finally, click on "**Save**" at the top right.
Your TUD account (NetID) has now been added and visible the ▣ Yubico Authenticator app:
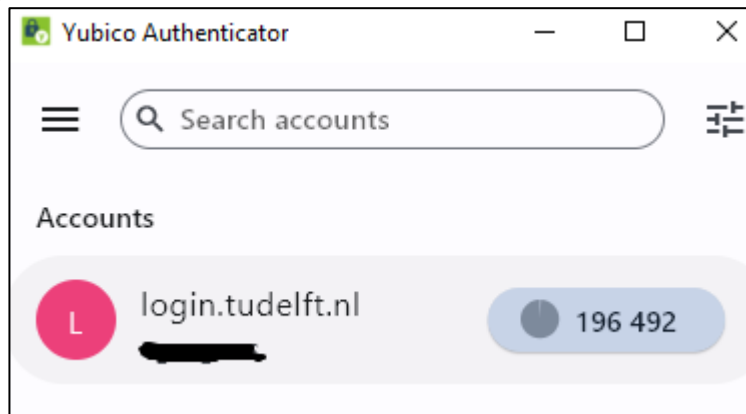


**Step 8:** Now copy the 6-digit code from the ▣ Yubico Authenticator app and paste it into the browser (*tip: to quickly copy the code from the authenticator; click on the 6-digit code and keep it pressed until a message appears "Code copied to clipboard"*):
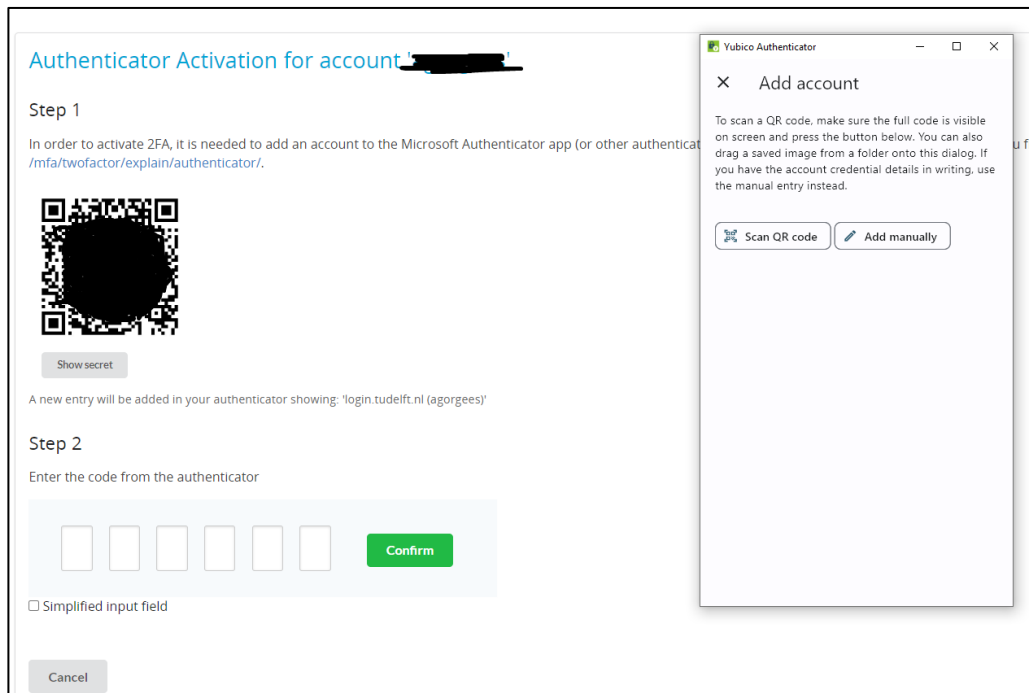


**Step 9:** Congratulations! 2FA is now activated for your NetID. If an application requires a strong form of authentication, you will now be asked for the code which you can find in the ▣ Yubico Authenticator app.

Finally, a confirmation email will follow. This is an automated security process to confirm that the 2FA has been changed.



# 3 Yubico Authenticator on smartphone (Android/iOS)

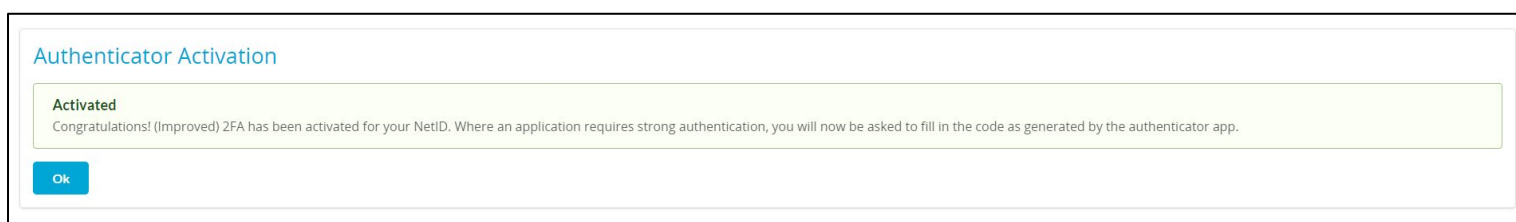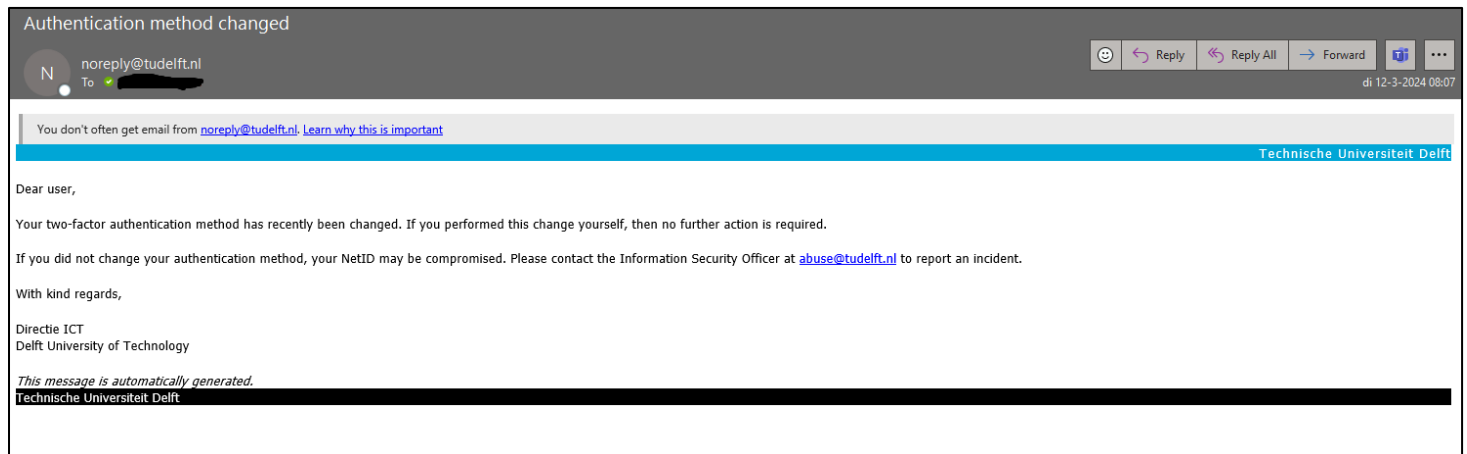The 🔑 Yubico Authenticator app can also be used on a smartphone (Android/iOS) provided it supports NFC. After the YubiKey has been successfully configured as an authenticator as described in the previous chapter, you can download the app from the Play Store/App Store. Then follow the next steps:
1. Open the 🔑 Yubico Authenticator app on your smartphone
2. Hold your physical YubiKey against the NFC reader of your smartphone (usually on the back of your smartphone)
3. Your account will automatically load in the app. You will immediately see a 6-digit code that you can use. This is valid for **30 seconds**
4. Once the timer expires, this code can no longer be used. To generate a new code, tap the expired code and choose "Calculate" (Get a new code from your YubiKey).

The data from your YubiKey accounts will not remain stored in the app. You must go through these steps every time to generate a code when using the smartphone app.

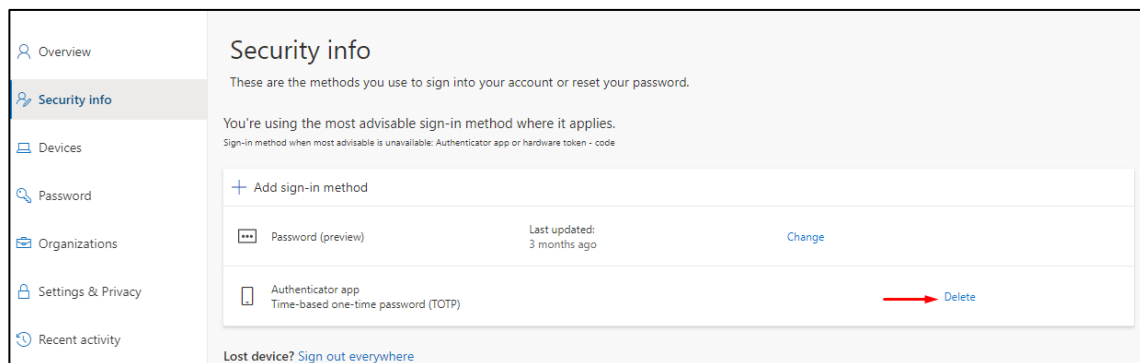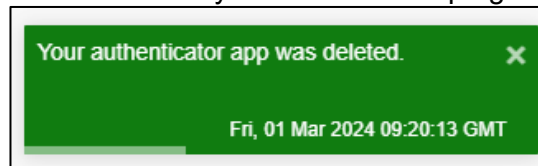# *4* Remove YubiKey as MFA-method

**Please note:** to prevent you from no longer having access to your account, you must always first remove the MFA method within your Microsoft or TUD account (NetID) before removing it within the 🔲 Yubico Authenticator.

**Step 1a. <u>For Microsoft account:</u>**
Go to https://aka.ms/mfasetup and log in. You will arrive at the screen below. Remove the existing YubiKey MFA method by clicking the "**Delete**" button:
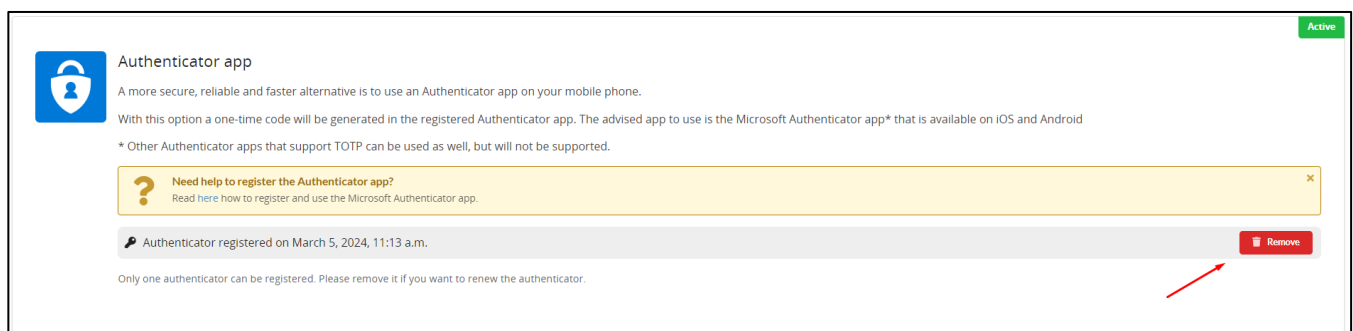


A notification will follow that it has been successfully deleted at the top right of the screen:



**Step 1b. <u>For TUD Account (NetID)</u>**
Ga naar https://login.tudelft.nl/mfa/ and log in. Click on the "**Remove**" button as shown below:
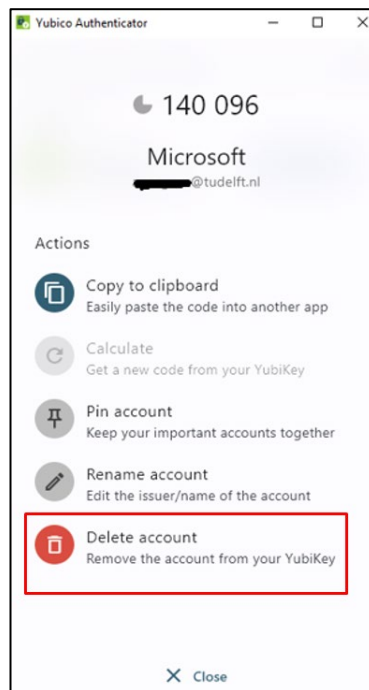


Then confirm this action by clicking "**Ok**".

**Step 2.** Now go to your ▦ Yubico Authenticator and click on this button (if requested, verify by touching the "button" on your YubiKey):
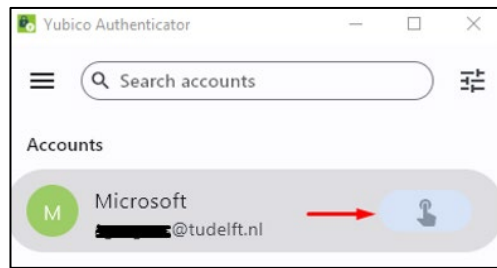


**Step 3a.** In the following screen, choose "**Delete account**":



**Step 3b.** To prevent you from no longer having access to your account, you will receive a warning that you must always first remove the MFA method within your account (Microsoft and/or TUD account) before removing it within the ▦ Yubico Authenticator. Click on "**Delete**".
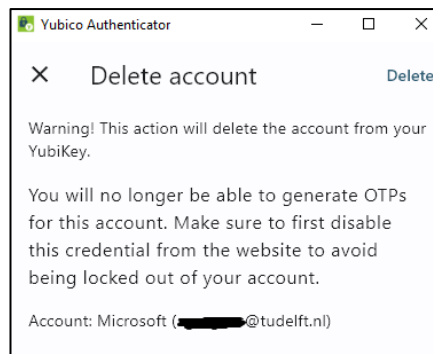


YubiKey has now been successfully removed as an MFA authentication method.

# *5*   Problems

## *5.1 Change MFA-method:*

**Microsoft MFA**
If you previously set up an MFA registration and want to change or transfer your MFA settings to another device. Then you can visit the Microsoft MFA environment self-service portal at: https://aka.ms/mfasetup


**TUD account MFA (NetID)**
To change your MFA registration for your TUD account, go to: https://login.tudelft.nl/mfa/.

## *5.2 Lost your YubiKey physical key*
If you have lost your YubiKey with your MFA profile(s) and you cannot use your mobile number to register a new device, you will need to contact your faculty service point to request an MFA change.

You are hereby requested to verify your identity and details with one of our colleagues. After it has been confirmed that you are the owner, one of our service point colleagues can help you further.