Tampere University
Tampere University of Applied Sciences

Setting up TUNI multifactor authentication

Tampere University
Tampere University of Applied Sciences

Setting up TUNI multifactor authentication

Additional protection

Multifactor authentication provides additional protection when you sign-in to TUNI electronic services.

Againts theft

Multifactor authentication provides additional protection in situations where your password has been fallen into wrong hands.

Verification by mobile phone

TUNI sign-in is verified with an authentication application installed on your phone or with SMS message code.

Tampere University
Tampere University of Applied Sciences

Enabling TUNI multifactor authentication

INSTALL AUTHENTICATION APPLICATION

ADD AUTHENTICATION APPLICATION TO YOUR ACCOUNT

SET UP SMS-BASED AUTHENTICATION

Multifactor authentication is enabled in three steps.

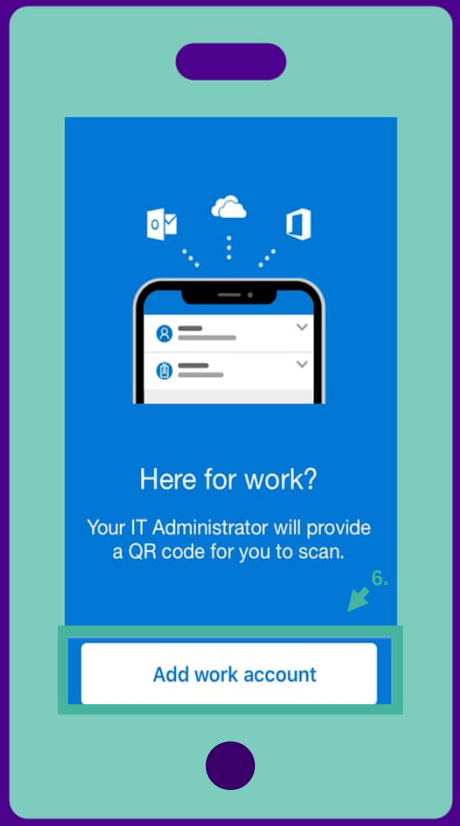
Tampere University
Tampere University of Applied Sciences

To be notified when enabling multifactor authentication

- **TUNI Staff´s** work computer must be on the TUNI-STAFF network or TUNI VPN has to be connected, if you're working off campus in order to enable multifactor authentication. When using your own personal device, you need to install eduVPN on your computer and turn it on. Read eduVPN instructions.
- **Students and visitors** (including those with the same access rights as staff) do not need a VPN connection to enable multifactor authentication
- If you have not already installed the Google or Apple account on your phone, you may install it with your own account or with a newly created account on your mobile phone.
- If the Microsoft Authenticator application asks for a lock code, please use the same lock code that you use to unlock the display of your phone.

Tampere University
Tampere University of Applied Sciences

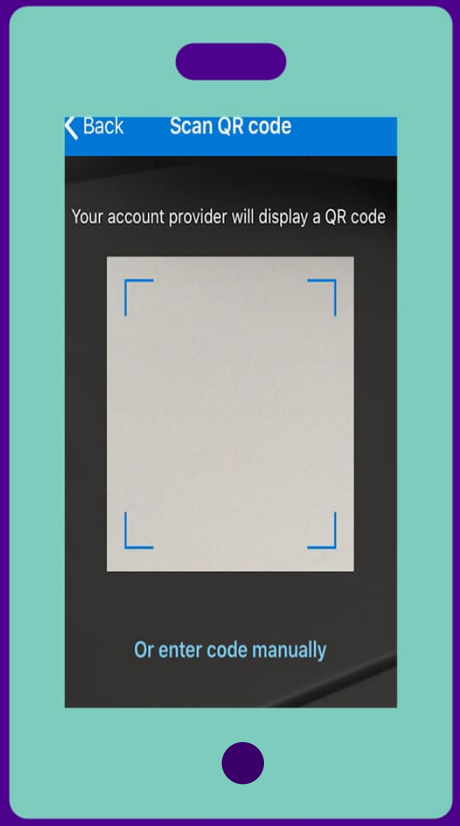
Phase 1: Install the Microsoft Authenticator app on your phone



1. Open an application store on your phone (e.g. Play Store or App Store) .
2. Search and install **Microsoft Authenticator** app on your phone.
3. Open Microsoft Authenticator app after the installation is completed.
4. The first time you log in, allow the collection of anonymised data when prompted to do so. You can turn off data collection later.
5. If prompted, select **Allow** to allow notifications.
6. Select **Add a new account** and then select **Work- or school account**

Tampere University
Tampere University of Applied Sciences

Phase 1: Install the Microsoft Authenticator app on your phone

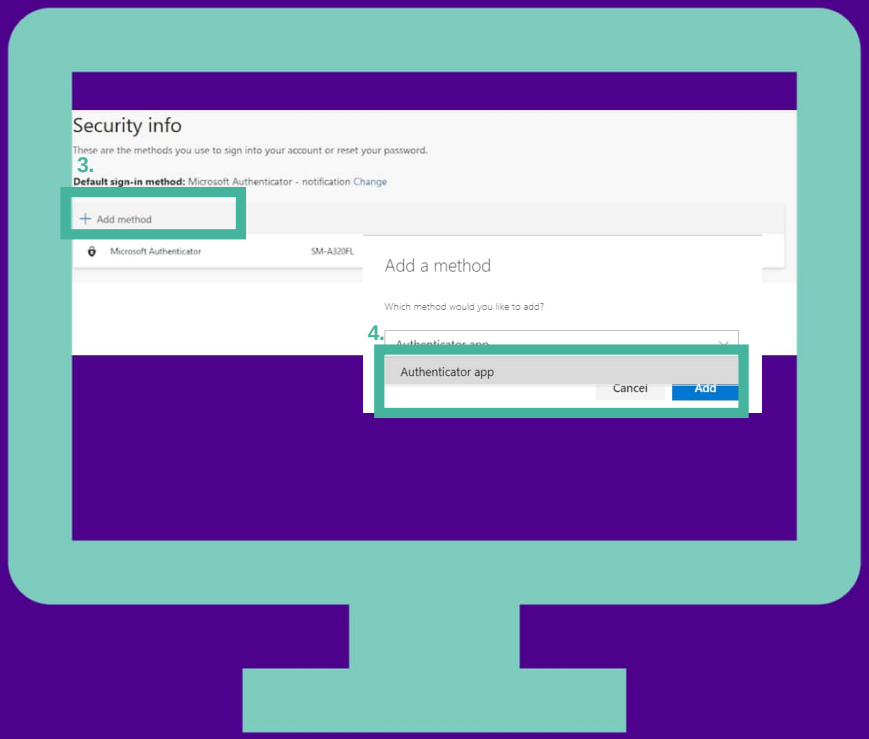


7. Select **Scan QR code**.
8. Allow the authenticator app access to your camera to take a picture of the QR code in the next phase.
9. The app waits for a QR code to add your TUNI account to the Microsoft Authenticator app on your phone.
10. Put your phone aside for a moment and go to phase 2.

NOTE! If the authentication application indicates that it is locked and asks you to enter the lock code, then use the same code that you use to unlock your phone screen/display.

Tampere University
Tampere University of Applied Sciences

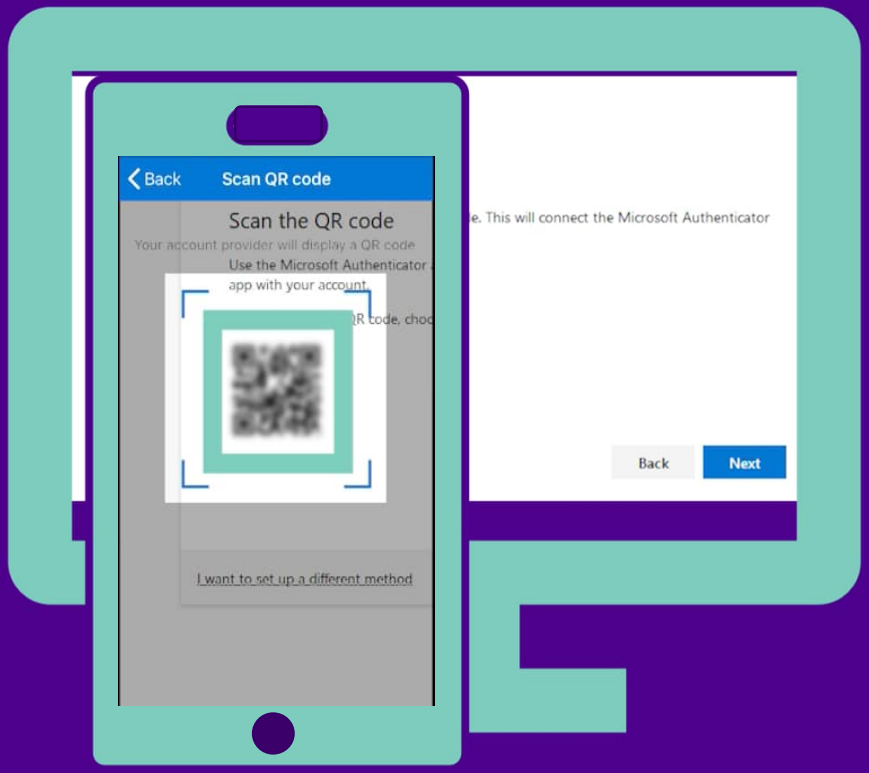
Phase 2: Add your TUNI account to the Microsoft Authenticator app



1. On your computer, if you already closed your browser, go again to the web address aka.ms/mfasetup.
2. Log in with your **TUNI email address** and **password**.
3. When your web browser asks whether the login will be saved, you can select **No**.
4. The browser displays a notification about the definition of additional details, select **Next**.
5. The browser displays information about the use of the Microsoft Authenticator app.
6. Click **Next**, and a QR code appears on screen.

Tampere University
Tampere University of Applied Sciences

Phase 2: Add your TUNI account to the Microsoft Authenticator app



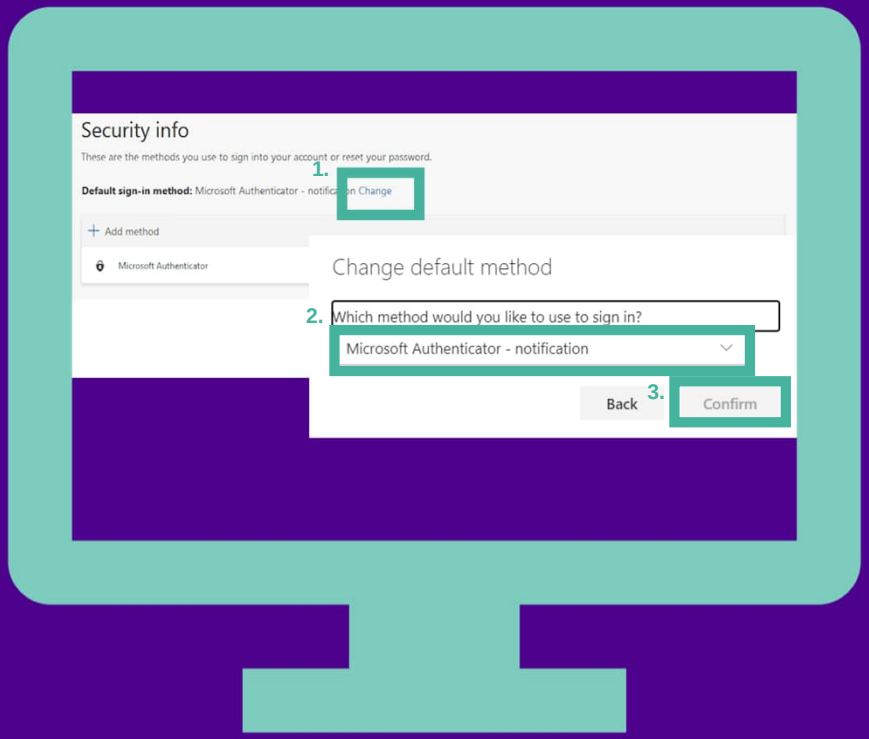
7. Take your phone and scan the provided QR code with the QR code reader of the Microsoft Authenticator app.

   If the authenticator application asks for a lock code, this is the lock code of the phone display.
8. After the Microsoft Authenticator app has scanned the QR code, click **Next** on the browser window of your computer.
9. The app will send a notification to your phone as a test which you shall **Approve.**
10. In the browser of your computer, click **Next.**
11. Then click **Done**.

If you are unable to capture the QR code, you can add it manually. Instructions in the handbook of IT services, see Frequently asked questions.

Tampere University
Tampere University of Applied Sciences

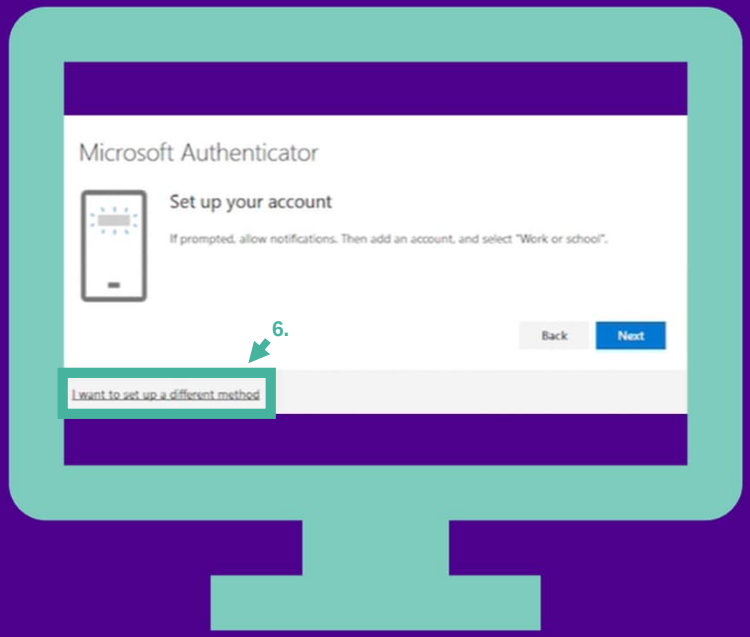
Phase 2: Add your TUNI account to the Microsoft Authenticator app



12. Your TUNI account has now been added to the Microsoft Authenticator app on your phone.
13. We also recommend that you enable SMS-based authentication as a secondary authentication method if, for example, you accidentally remove the authentication application from your phone. In your browser, leave the Security info page open and go to phase 3.

Tampere University
Tampere University of Applied Sciences

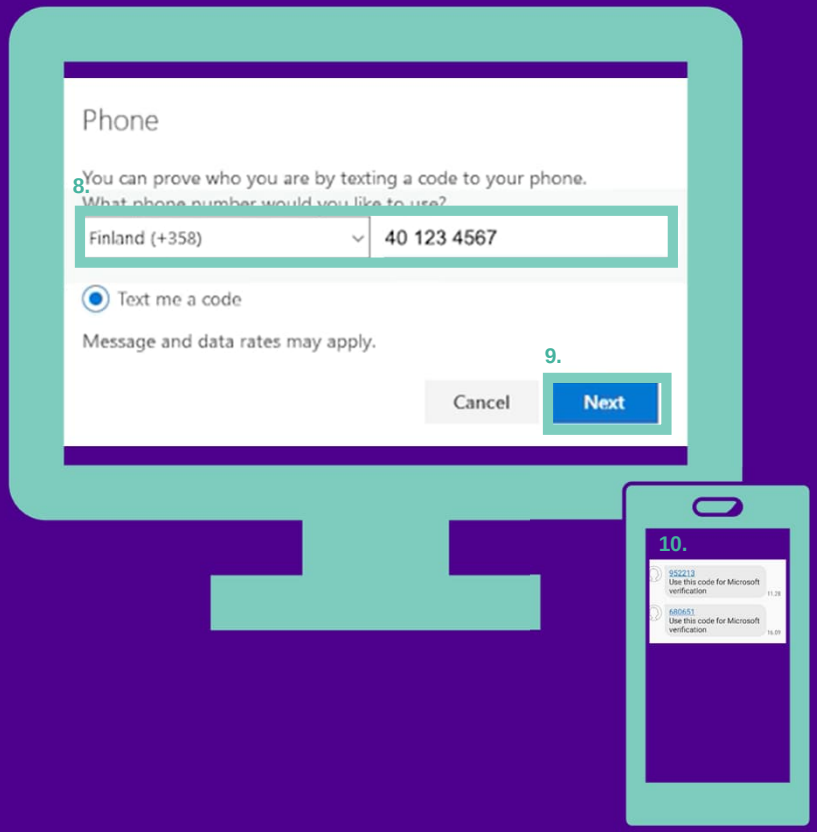
Phase 3: Set up SMS-based authentication method



1. Open your browser and go to the web address aka.ms/mfasetup
2. Log in with your **TUNI email address** and **password**.
3. If you have a smartphone and have already installed Authenticator, click **+ Add method** -button on Security info -page and skip to step 5.
4. If you do not have a smartphone and have not been able to install Authenticator, click the **I want to set up a different method** -link at the bottom of that box.
5. In the drop-down menu, select **Phone** and click **Confirm**.
6. In the drop-down menu, select country code and type the rest of your phone number in the provided field.

Tampere University
Tampere University of Applied Sciences

Phase 3: Set up SMS-based authentication method

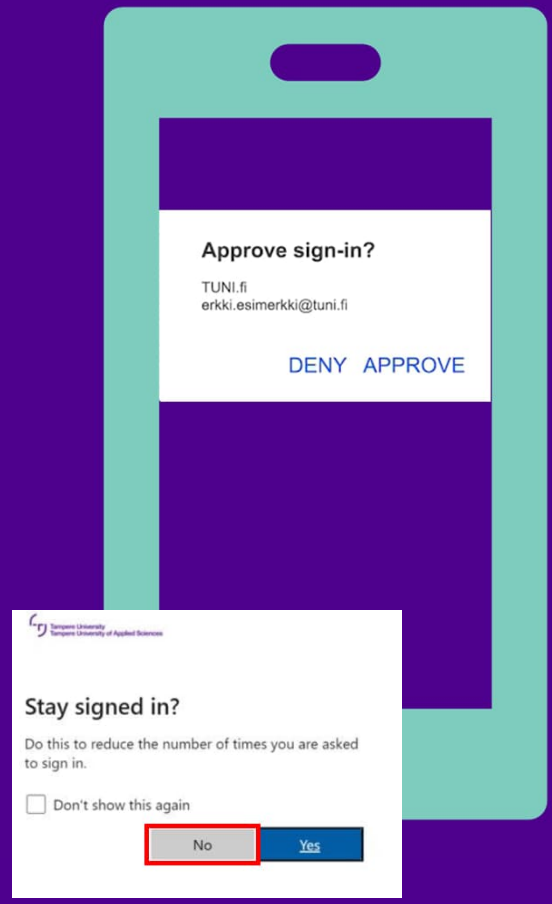


7. Click **Next**.
8. You will receive an SMS on your phone containing a numeric code of 6 digits. Enter this code in the field displayed in your web browser.
9. In the browser click **Done**.
10. Your TUNI account has now been connected to your phone number.

Tampere University
Tampere University of Applied Sciences

Signing into TUNI electronic service

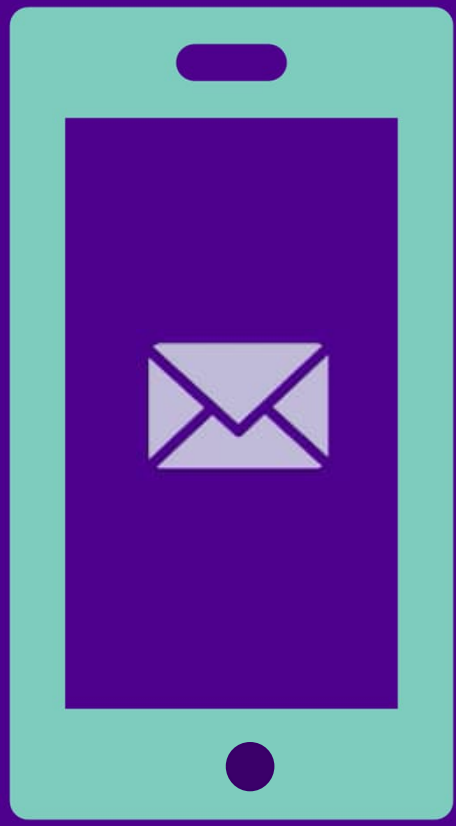
- You will initially receive frequent verification prompts either on the Microsoft Authenticator app you installed on your phone or as SMS depending which method you selected as the default sign-in method (in step 3). Number of verification prompts will decrease after a day or two.
- The next verification prompt will appear in about 2-3 months if you always use the same device or broser.
- Be careful! Do not accept a verification prompt on your phone if you receive a verification prompt and you are not signing into TUNI service yourself. Contact IT Helpdesk if the situations recurs.
- **When using something other than your personal device,** be sure to answer "No" to the question in the Stay signed in window, so that no one else can log in with your user account to your information and the TUNI electronic services you have used.



Tampere University
Tampere University of Applied Sciences

Supported email applications

- Please note that not all email applications are yet supporting the multifactor authentication or are not compatible with the used authentication technology.
- Due to the security reasons we can’t accept to use of TUNI emails and calendar with a non-supported application.
- List of supported email application is found in the handbook of IT services.



Tampere University
Tampere University of Applied Sciences

Good to know

Extra devices

You can also activate authenticator application for another devices, if you wish, such as your personal phone.

Add and remove authentication

If you change your phone, remember to install multifactor authentication on your new phone. Remember also to remove the authentication from your old phone before you hand it over.

This all and more can be done here aka.ms/mfasetup