South-Eastern Finland
University of Applied Sciences

MULTIFACTOR AUTHENTICATION (MFA) GUIDE

South-Eastern Finland
University of Applied Sciences

Guide title	Multifactor authentication (MFA)		
Responsible unit	IT Services		
Effective date		**Decision**	
Updated	04.11.2026	**Updated by**	IT Services
Updated		**Decision**	
Updated		**Decision**	

South-Eastern Finland
University of Applied Sciences

TABLE OF CONTENTS

1 WHAT IS MULTIFACTOR AUTHENTICATION AND WHY IS IT IMPORTANT? 3

2 INSTALL MICROSOFT AUTHENTICATOR FROM YOUR PHONE'S APP STORE 4

3 SET UP AUTHENTICATOR USING A PHONE 5

4 SET UP AUTHENTICATOR USING A COMPUTER AND A PHONE 8

5 SECURITY INFO 12

6 RECONFIGURING MFA 13

South-Eastern Finland
University of Applied Sciences

1 What is multifactor authentication and why is it important?

Multifactor authentication (MFA) means that a user's identity is verified using at least two different authentication factors, such as a password and the Microsoft Authenticator app installed on a phone. For example, if someone else obtains your password, they still cannot sign in to your account without the second step, which is approval through the mobile app. The account owner is therefore notified of the sign-in attempt and can either reject or approve it.

In addition to a password, the second authentication factor can be

- authentication requested by a mobile app, such as Microsoft Authenticator
- a 4–8-digit code received by text message and entered on the website requesting it (text message verification will be discontinued in February 2027)
- a biometric identifier, such as a fingerprint or facial recognition
- an external authentication device

In multifactor authentication, verification is performed using a personal mobile device, usually a mobile phone. Text message or phone call verification requires the phone number to be registered with the service that requires multifactor authentication. (Traficom, Finnish Transport and Communications Agency, 2026).

This guide explains how to set up multifactor authentication (MFA) for signing in to Xamk services. We recommend using the Authenticator mobile app and connecting your Xamk account to it. This guide uses Microsoft Authenticator as the authentication app.

You can set up the Authenticator app using only your phone or by using a computer and a phone together. Both methods are described in this guide.

Do not approve an Authenticator sign-in request that you did not initiate. If you receive an unexpected sign-in request, reject it.

The images in this guide are examples. The views may vary depending on your device and language settings.

South-Eastern Finland
University of Applied Sciences

2 Install Microsoft Authenticator from your phone's app store

When you sign in for the first time to a service that requires authentication, such as lux.xamk.fi, you must set up Authenticator either using your phone or using a computer and a phone together.

Install the Authenticator app from your phone's app store. If Authenticator is already installed on your phone, you can use it and proceed to the next section.

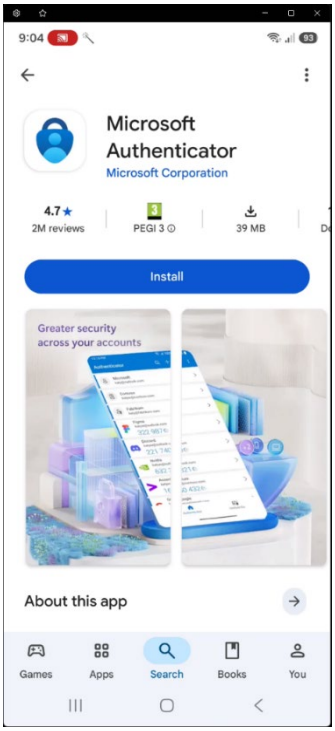
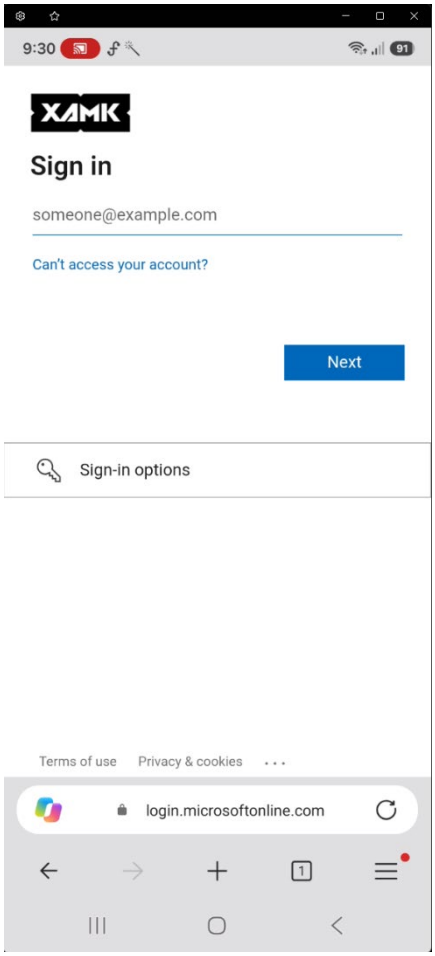


Figure 1. Searching for the app in the app store

1. Open the app store on your phone
2. Search for Microsoft Authenticator
3. When you find the app, tap Install

3 Set up Authenticator using a phone



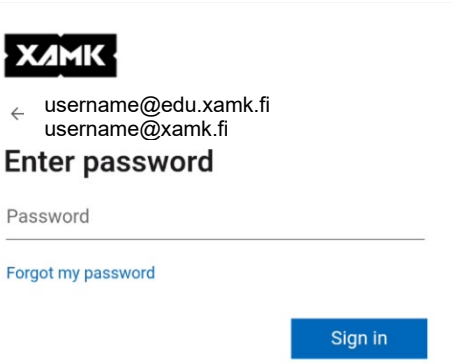


Figure 2. Sign in and Enter password views on a phone

1. On your phone, open a browser and go to an address that requires authentication, such as lux.xamk.fi or portal.office.com
2. The Xamk sign-in window opens and the address changes to login.microsoftonline.com
3. Enter your username in its full format (students: username@edu.xamk.fi, staff: username@xamk.fi)
4. Select Next
5. Enter the password you created for your username
6. Select Sign in

South-Eastern Finland
University of Applied Sciences

7. You will see the message “Let’s keep your account secure”. Tap Next.

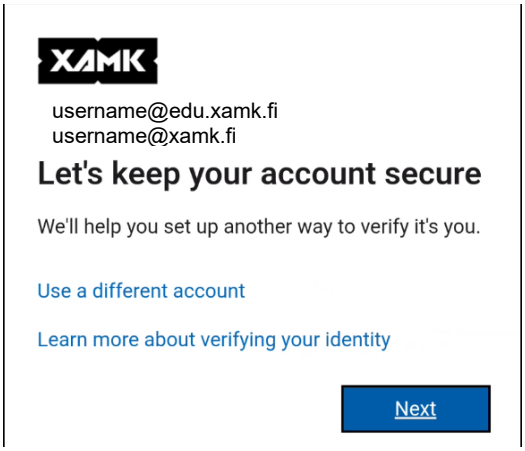


Figure 3. Let’s keep your account secure view

8. You are asked to install the Microsoft Authenticator app on your phone.

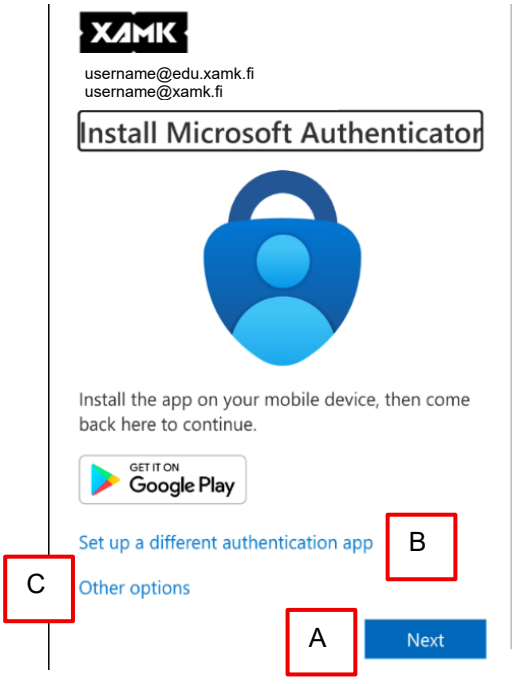


Figure 4. Install the Microsoft Authenticator app

A. Once you have installed the Microsoft Authenticator app on your phone, select Next.
B. If you want to use another authentication app, select Set up a different authentication app and follow the on-screen setup instructions.
C. Under Other options, you can view the other sign-in verification methods available at Xamk.

Note: Phone number verification will be discontinued in February 2027.

9. You will receive a notification about pairing Authenticator with your account.

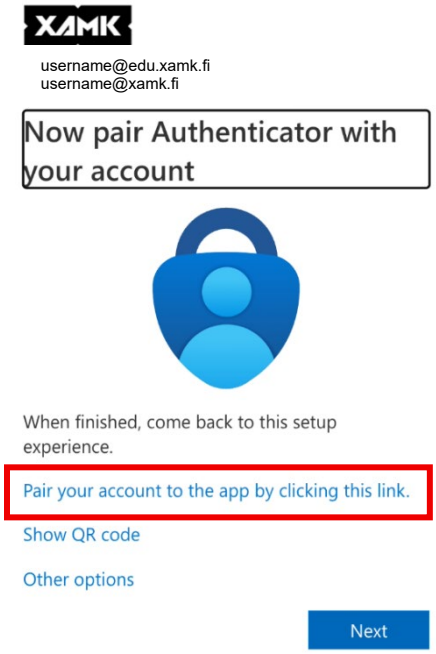


Figure 5. Connect your account to the app

Connect your account to Authenticator by selecting "Pair your account to the app by clicking this link".

Note: The view that opens depends on the browser used on your phone.

Edge: The notification shown below opens and asks you to open Authenticator (Figure 6).

Chrome: The Authenticator app opens directly. Continue to step 10 of the guide.

When using the Edge browser, the notification below opens. Select Open.

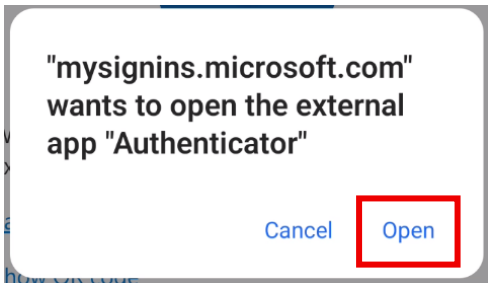


Figure 6. Open the Authenticator app

10. The Authenticator app opens on your phone. Approve the permissions displayed on the screen.
    1. Approve the collection of diagnostic data by selecting Continue.

       Note: Choose whether you want to share app usage data.
    2. Allow Microsoft Authenticator to receive notifications in your phone settings.
    3. Select Done.

Your Xamk account is now shown in Authenticator.

4 Set up Authenticator using a computer and a phone

1. On your computer, go to lux.xamk.fi
2. The Xamk username and password fields open.

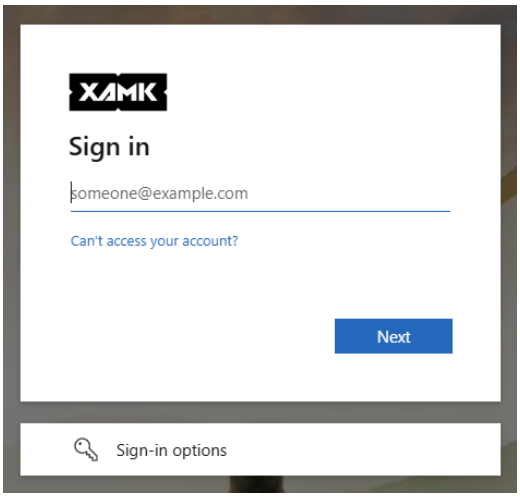


Figure 7. Sign-in window on a computer

Enter your username in its full format and select Next.

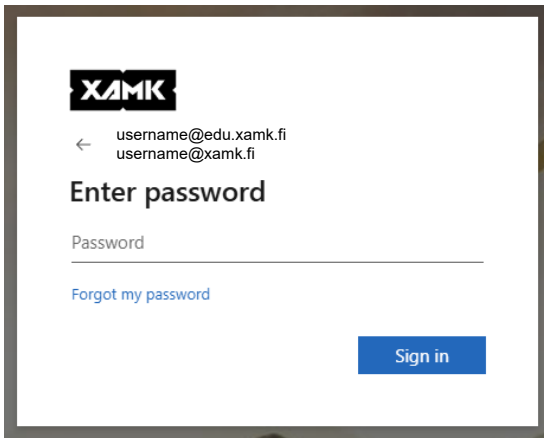


Figure 8. Password entry window on a computer

Enter your password and click Sign in.

3. You will see the message “Let’s keep your account secure”. Click Next.

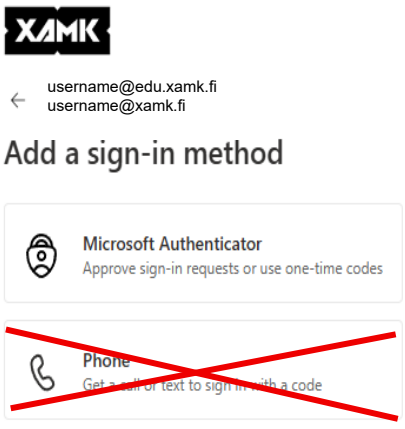


Figure 9. Let’s keep your account secure view

4. Select Microsoft Authenticator as the authentication method by clicking Next.



If you want to use an app other than Microsoft Authenticator, select Set up a different authentication app and follow the on-screen instructions.



Under Other options, you can view the other authentication methods available at Xamk.
NOTE: Phone number verification will be discontinued February 2024.

Figure 10. Install the app on your phone view

After selecting the authentication method you want to use, select Next. Authenticator setup will then begin.

5. A message about adding the account to the app on your phone appears on your computer screen. Now switch to your phone.

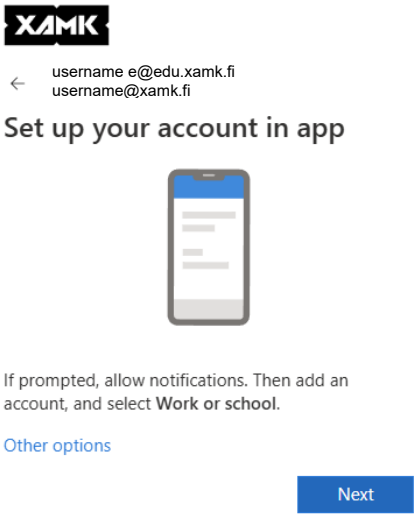


Figure 11. Adding the account to the app

6. Open the Authenticator app on your phone and make the selections below.
   - If you are setting up Microsoft Authenticator for the first time, your phone may ask permission to let Authenticator run in the background or to disable battery optimization for the app. Approve the request.
   - If you have already used Authenticator, tap the plus button at the top to add your account to the Authenticator app.
   - Tap “Add work or school account”.
   - At this stage, select Next on your computer to display a QR code.
   - On your phone, select Scan a QR code and allow camera access by choosing “While using the app”.
   - Scan the QR code displayed on your computer screen.
   - In the QR code view on your computer, select Next when the button becomes available. Your Xamk account now appears in the Authenticator app on your phone.

7. The first verification number then appears on your computer. Open the notification received in your phone's notification center, approve the sign-in by entering the number shown on the computer, and select Yes.

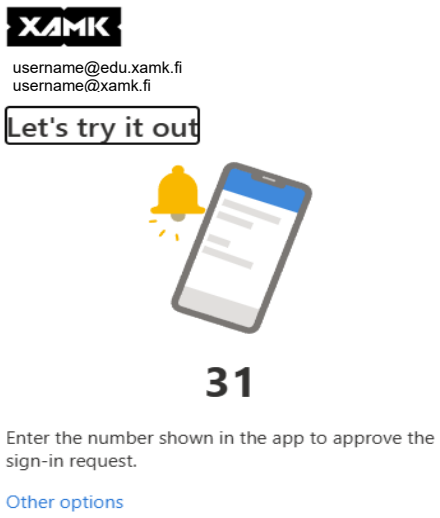


Figure 12. First verification number on the computer screen

8. After approving the sign-in request, the window shown opens. Click Done. You have now enabled Authenticator for sign-in verification.



Figure 13. Account added to Authenticator

5 Security info

Your Security info page may open on your computer. It shows which authentication methods you currently use and also allows you to manage your security information.

Direct address for Security info: https://mysignins.microsoft.com/security-info

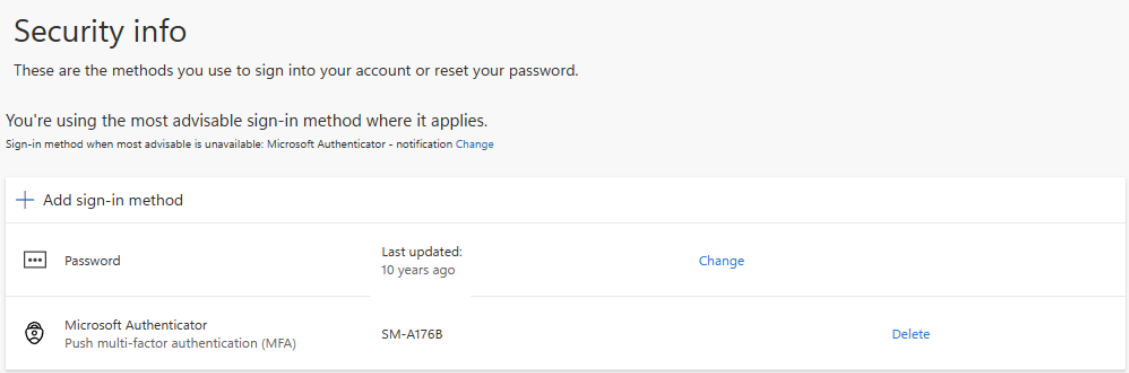


Figure 14. Security info

South-Eastern Finland
University of Applied Sciences

6 Reconfiguring MFA

If your phone is broken or has been replaced, or if you do not receive verification requests from Authenticator, you can set up a new MFA method in our identity verification service.

1. Go to id.xamk.fi
2. Scroll down and select Set up a new MFA method
3. Verify your identity using Finnish online banking credentials or a mobile certificate. If you do not have Finnish online banking credentials or a mobile certificate, please submit an ICT support request in Xinfo.
4. After identification, the Remove MFA methods view opens. Select Remove MFA methods.

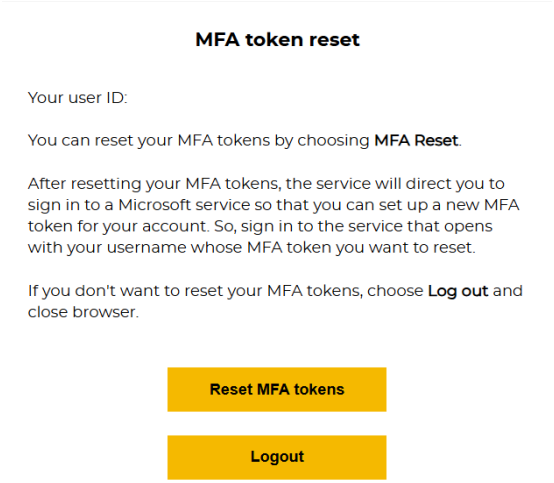


Figure 15. Removing MFA methods

5. Confirm the removal of the MFA methods from your account by selecting OK in the notification at the top of the browser.

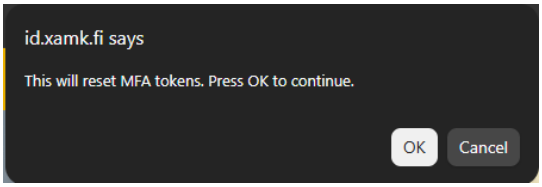


Figure 16. Confirming removal in the browser

6. Set up Authenticator again.

If you have problems with MFA, go to xinfo.xamk.fi, sign in using single sign-on (an MFA method is not required), and submit a service request to IT Support.

South-Eastern Finland
University of Applied Sciences

SOURCES

Traficom, Finnish Transport and Communications Agency. Multifactor authentication protects your user accounts. Web document. Updated 9 July 2026. Available at: https://www.traficom.fi/en/everyday-information-security/multi-factor-authentication-protects-your-user-accounts [Accessed 4.11.2026].