



Kaakkois-Suomen  
ammattikorkeakoulu

# MULTI-FACTOR AUTHENTICATION (MFA) INSTRUCTIONS

South-Eastern Finland  
University of Applied Sciences

<b>Title of the guidelines</b>	MULTI-FACTOR AUTHENTICATION (MFA) INSTRUCTIONS		
<b>Person in charge</b>	ICT Services		
<b>Effective from</b>	xx.xx.xxxx	<b>Decision</b>	xxxxx
<b>Updated</b>	01 December 2023	<b>Updated by</b>	Sirpa Kemppainen
<b>Updated</b>		<b>Decision</b>	
<b>Updated</b>		<b>Decision</b>	



Kaakkois-Suomen  
ammattikorkeakoulu

## TABLE OF CONTENT

<b>1</b>	<b>WHAT IS MULTI-FACTOR AUTHENTICATION?</b>	<b>1</b>
<b>2</b>	<b>WHY IS MULTI-FACTOR AUTHENTICATION IMPORTANT?</b>	<b>1</b>
<b>3</b>	<b>SETTING UP MULTI-FACTOR AUTHENTICATION WITH A TEXT MESSAGE OR PHONE CALL</b>	<b>2</b>
<b>4</b>	<b>USING MULTI-FACTOR AUTHENTICATION WITH A TEXT MESSAGE OR PHONE CALL</b>	<b>5</b>
<b>5</b>	<b>SETTING UP THE AUTHENTICATOR APP</b>	<b>5</b>
<b>6</b>	<b>YOUR SECURITY INFORMATION</b>	<b>10</b>



## 1 What is multi-factor authentication?

Multi-factor authentication is a secure login method where users are required to verify their identity using another method in addition to a password. This method may be

- an authentication from a mobile application (e.g., Microsoft Authenticator)
- a four to eight-digit code sent by text message to be entered on the site requesting it
- a phone call

In multi-factor authentication, you can verify your identity using a personal mobile device, usually a mobile phone. The phone number must be registered for multi-factor authentication so that you can use the text message or phone call authentication. (National Cyber Security Centre Finland 2023.)

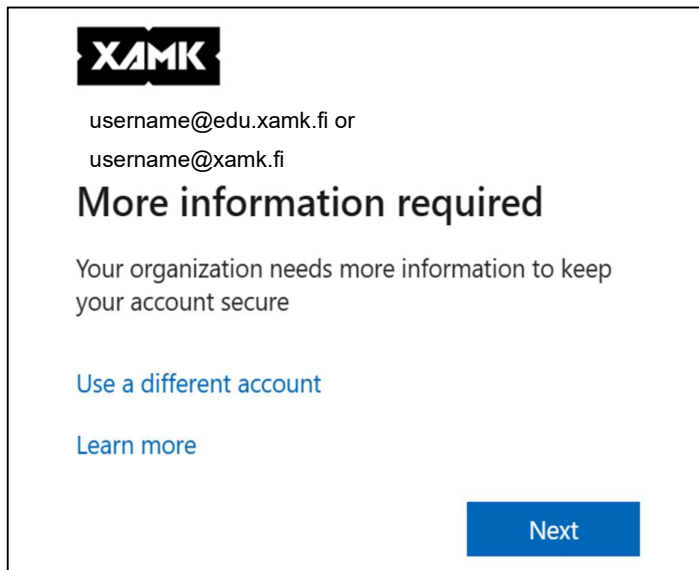
## 2 Why is multi-factor authentication important?

In multi-factor authentication, the user's identity is verified using two or more identification methods. This means that if, for example, someone else has gotten hold of the user's password, they cannot log in without the second phase, i.e., accepting the login on a mobile application. The owner of the account will receive a notification of the login attempt and can either reject or confirm the login. (National Cyber Security Centre Finland 2023.)

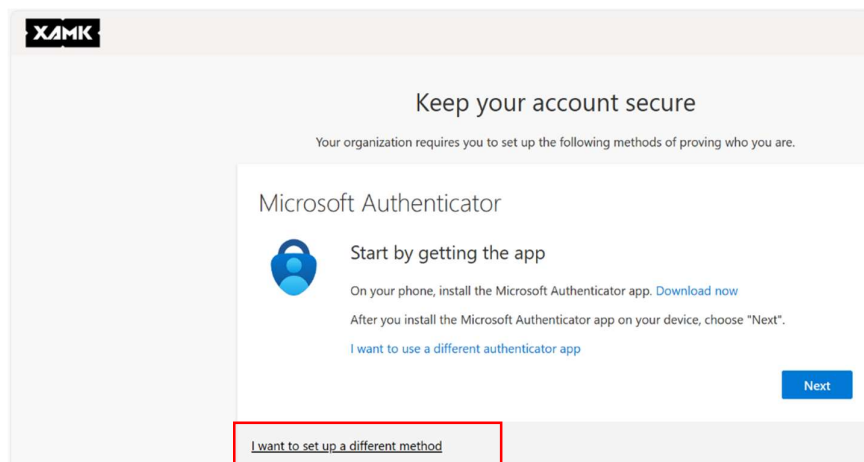


### 3 Setting up multi-factor authentication with a text message or phone call

After you first log in to a service that requires multi-factor authentication, you will receive a notification 'More information required' which will assist you in setting up the multi-factor authentication.

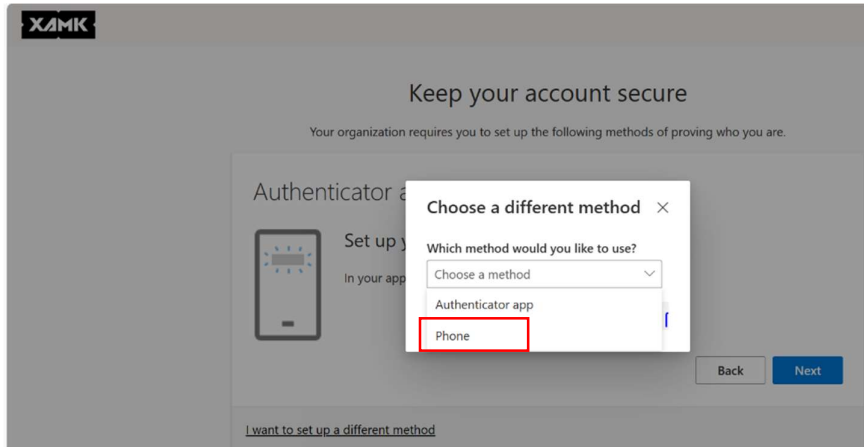


Next, decide which authentication method you wish to use. You will first be offered the Microsoft Authenticator application. If you wish to start using the application right away, download it from the application store on your phone and follow the instructions on your screen to set up the application. You can find instructions for setting up Microsoft Authenticator later on in this document. If you wish to use authentication by text message, choose '**I want to set up a different method**' at the bottom of the window.

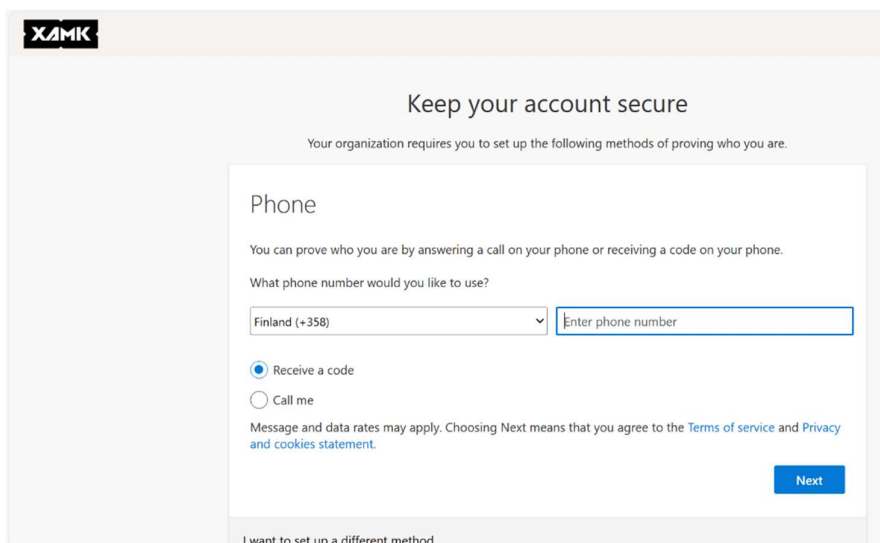




If you want to verify your identity by receiving a code via a text message, choose 'Phone'. After this, click 'Confirm'.



Select the country code of your phone subscription. In this case, it is Finland (+358). In the adjacent field, enter your phone number without the first zero. Select whether you want to receive a text message with a verification code or a phone call. Your selection will be the default login method for you in multi-factor authentication.



When you click 'Next', you will receive a text message on your phone with a six-digit code which you need to enter on the next screen.



The screenshot shows a web interface for account security. At the top left is the XAMK logo. The main heading is "Keep your account secure". Below it, a sub-heading reads "Your organization requires you to set up the following methods of proving who you are." The central content area is titled "Phone" and contains the text: "We just sent a 6 digit code to +358 [redacted]. Enter the code below." There is an input field labeled "Enter code" with a blue "Resend code" link below it. At the bottom right of the form are "Back" and "Next" buttons. At the bottom left of the form is a link: "I want to set up a different method".

Enter the code you received.

If you did not receive a code, click 'Back' and check whether the phone number you entered was correct. If you chose 'Call me', you will receive a phone call from Microsoft in English. You can verify your identity by answering the call and pressing the hashtag (#) sign on your phone.

The screenshot shows the same web interface as the previous one, but now displaying a success message. The heading "Keep your account secure" and sub-heading "Your organization requires you to set up the following methods of proving who you are." are still present. The central content area is titled "Success!" and contains the text: "Great job! You have successfully set up your security info. Choose 'Done' to continue signing in." Below this, it says "Default sign-in method:" followed by a phone icon and the word "Phone" next to a greyed-out input field. A blue "Done" button is located at the bottom right of the form.

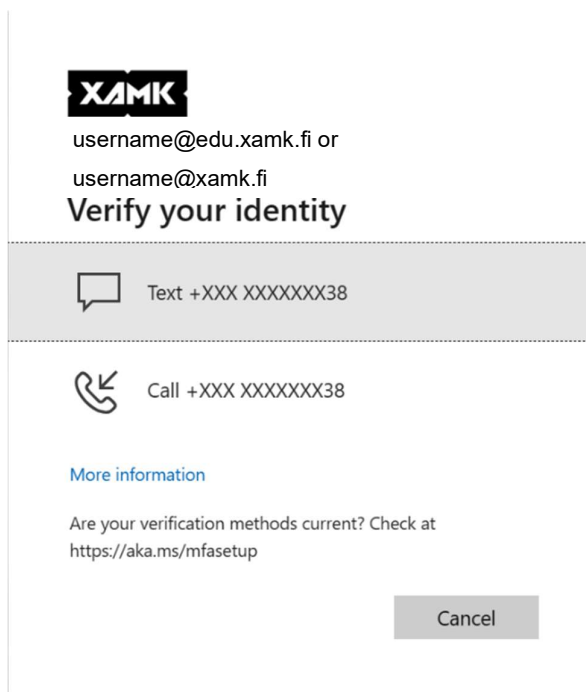
After this, you will receive a notification of a successful setup. Click 'Done'.



#### 4 Using multi-factor authentication with a text message or phone call

After logging in to a service that requires multi-factor authentication, you will receive a notification asking you to 'Verify your identity'.

Choose how you wish to verify your identity, either 'Text' or 'Call'. If you choose Text, you will receive a text message on your phone with a code that you have to enter on the next screen ('Enter code') and click 'Verify'. If you choose Call, you will receive a phone call in English from Microsoft. Answer the call and press the hashtag (#) symbol, after which you can log in to the service.

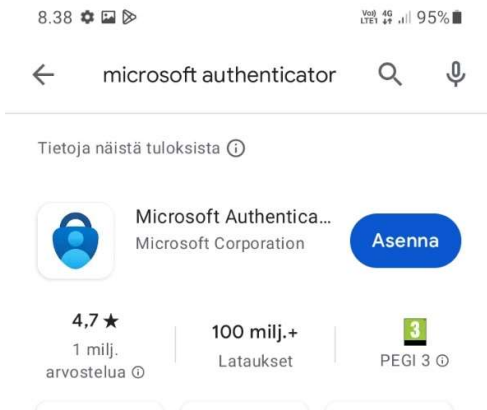


#### 5 SETTING UP THE AUTHENTICATOR APP

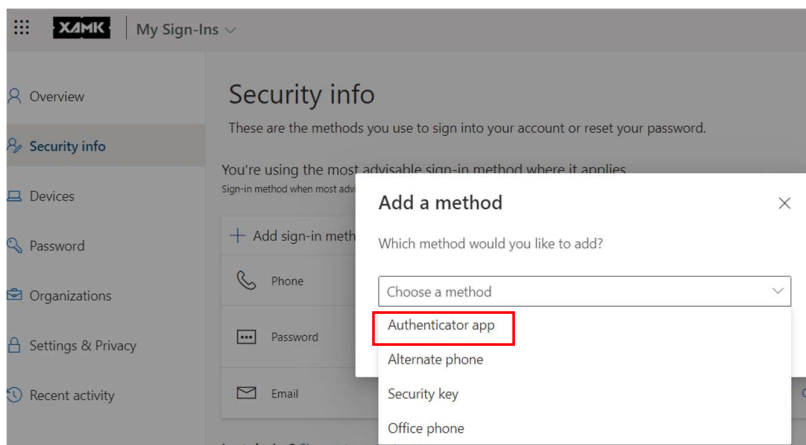
You can also use Microsoft Authenticator or Google Authenticator to verify your identity. You need to have a smart phone that supports the application and QR code scanning to be able to use Authenticator. When setting up Authenticator, you will need a phone and another device (computer) from which you can scan the QR code with your phone.

These instructions are only for Microsoft Authenticator.

Find Microsoft Authenticator on your phone's application store and install it.



Once the installation is done, open the application and approve the conditions and permissions it requests. After this, open the following address on your computer: <https://mysignins.microsoft.com/security-info>. A security info page will open. Click 'Add sign-in method', choose 'Authenticator app' from the drop-down menu, and click 'Add'.







If you have already downloaded Microsoft Authenticator on your phone, click 'Next' on your computer. Otherwise, download and install Authenticator from the application store on your phone before clicking 'Next' on your computer. If you use a different authenticator application, choose 'I want to use a different authenticator app' and follow the instructions.

### Microsoft Authenticator



#### Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

Cancel

Next

Leave on the 'Set up your account' screen on your computer and take your phone.

### Microsoft Authenticator

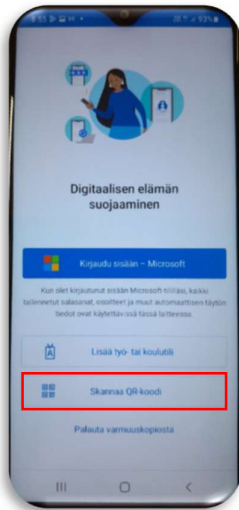


#### Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Back

Next



Open the Authenticator application on your phone, select 'Scan a QR code' and allow the application to access your camera. On the 'Set up your account' screen on your computer, click 'Next' and then, use your phone's camera to scan the QR code that appears on the computer screen.

Once the QR code is scanned, you will receive the first Authenticator notification on your phone.

An 'Approve sign in request' window will appear on your computer screen with a code. Enter the code on the notification that appeared on your phone. Open the notification on your phone, enter the code from your computer, and confirm the code by pressing 'Yes'.



### Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

83

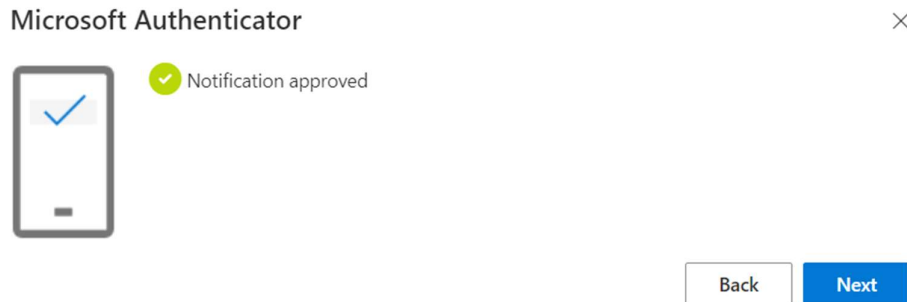
No numbers in your app? Make sure to upgrade to the latest version.

[I can't use my Microsoft Authenticator app right now](#)

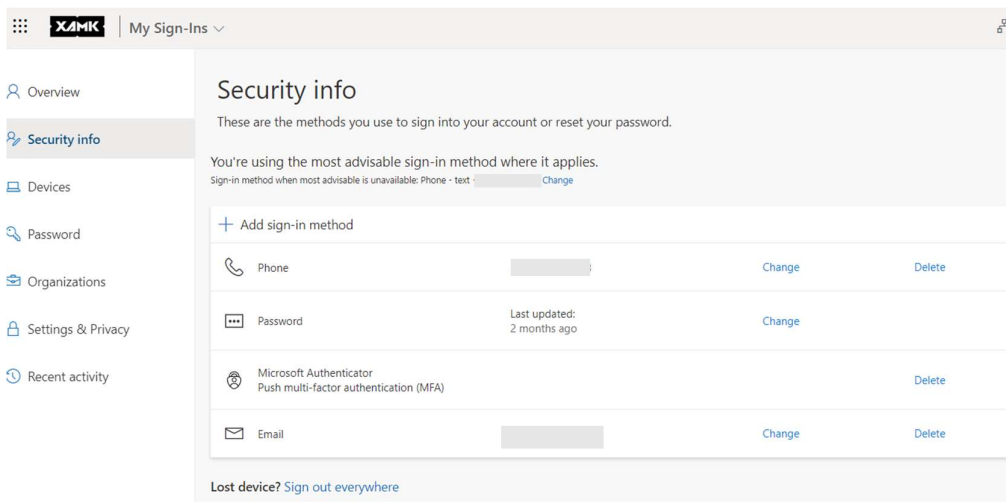
[More information](#)



The window on your computer will notify you of a successful authentication. Click 'Next'.



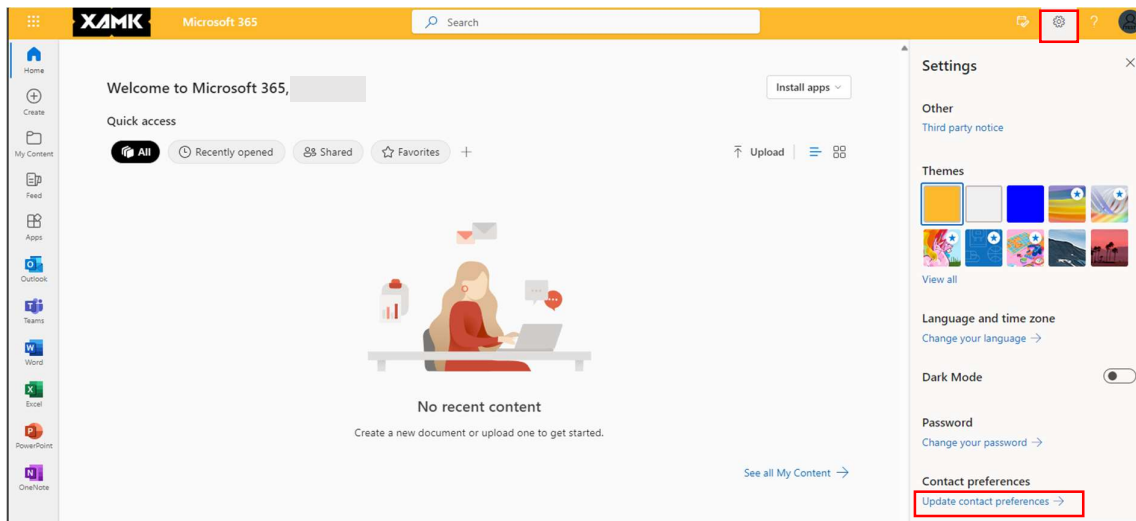
You will return to your 'Security info' page on the M365 portal where you can see your login methods.



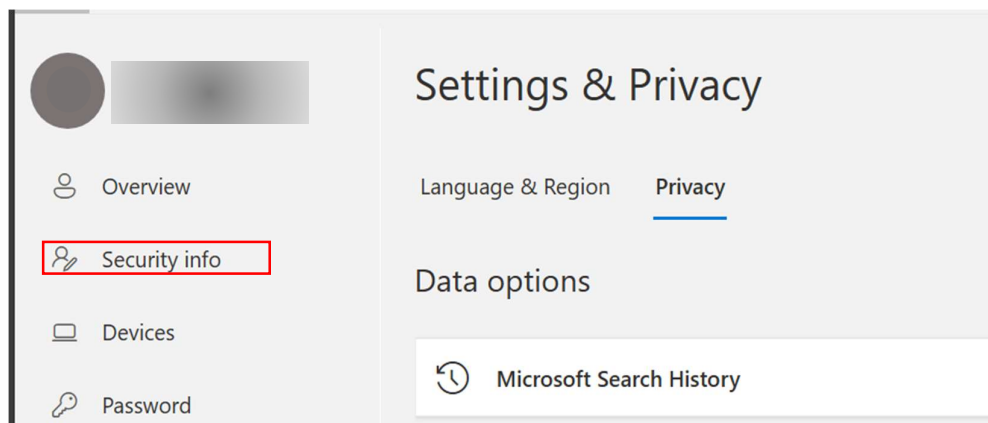


## 6 Your security information

You can access your security info directly at <https://mysignins.microsoft.com/security-info> or via the M365 portal (portal.office.com) by clicking 'Settings' (the gear icon) and then 'Update contact preferences'.



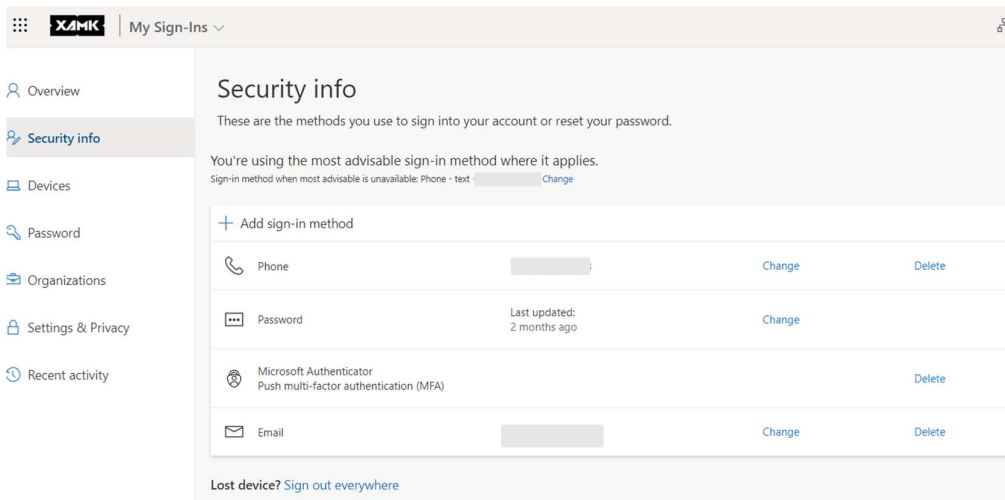
On the next page, click 'Security info' on the left-hand side. You will then receive a verification code or notification on your phone. Complete the verification to access the next page.





Here you can see your login methods.

By adding login methods, you can choose several different authentication methods. We recommend having at least two different authentication methods, e.g., an alternate phone number or email address in case your phone is broken.



## REFERENCES

National Cyber Security Centre Finland. Monivaiheinen tunnistautuminen suojaa käyttäjätilejasi. WWW document. Updated on 6 March 2023. Available at: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi>. [Accessed 1 December 2023].

Date	Revised chapters /pages	Description
XX.XX.XXXX		