



**UNIVERZA V LJUBLJANI**  
**University of Ljubljana**

# User Guide for setting up MFA

Date: 11. 9. 2023

Document status: final

<b>1. INTRODUCTION .....</b>	<b>3</b>
<b>2. TERMINOLOGY.....</b>	<b>3</b>
<b>3. SETTING UP MULTI-STAGE VALIDATION .....</b>	<b>4</b>
3.1. Adding security mechanisms to a user profile .....	4
3.2. Setting up the "Authenticator" method on your smartphone .....	7
3.3. Setting up the "mobile phone" method .....	12
3.4. Setting the "security key" method .....	15
3.5. Changing the default authentication method .....	19
3.6. Action in the event of loss or theft of a device .....	20
<b>4. USEFUL LINKS .....</b>	<b>21</b>

# 1. Introduction

In today's digital world, security is crucial for businesses and their data. The steady rise in cyber-attacks and identity theft poses a serious threat to organizations of all sizes. In this situation, it is essential to ensure effective security measures to protect sensitive information such as business data, customer financial data, intellectual property and other important data.

One of the key methods to enhance security is the use of multi-factor authentication (MFA). MFA is a security mechanism that requires more than one factor of identity verification when accessing accounts and systems. While traditional authentication methods, such as using only passwords, are becoming less reliable, MFA provides businesses with additional protection against attacks and unauthorized access.

# 2. Terminology

To make it easier to understand the content of the document, let's define the terms that will be used in the following chapters.

The concept of	Explanation
Authentication	In computing, authentication or authentication is the process by which a server makes sure that a user is really who they say they are. The most common authentication method is to enter a username and password during the sign-in process to a particular IT system.
Authentication device	The device we will use to authenticate your login. This is most often a mobile smartphone, but can also be USB sticks (e.g. Gemalto).
Authentication app	An app installed on your smartphone to confirm a new login.
Authentication method (enrolment method)	The authentication method is the authentication security mechanism that will be used to authenticate new logins to your profile. Typically, these methods are: <ul style="list-style-type: none"><li>• Confirming the registration by obtaining a random number by SMS to a mobile phone</li><li>• confirmation of registration by calling and confirming the registration on the mobile phone</li><li>• confirmation of registration by calling and confirming registration on a company phone</li></ul> login validation by approval sent to a pre-established authentication app on a mobile smartphone
Multi-factor authentication (abbreviation MFA)	Multi-factor authentication is an additional security mechanism to give your profiles a higher level of security. MFA is an acronym in the Microsoft world but is also known more widely as 2FA (two-factor authentication).
PIN number	A four- or multi-digit number that can serve as a security mechanism as an alternative to a password.

### 3. Setting up multi-stage validation

The following section shows how to set up MFA for a service user account. In the presented example, we used a mobile smartphone with Android operating system and a PC to add security mechanisms. If you do not have a mobile smartphone, you can use a regular mobile phone (SMS, call) or a landline phone or a security key.

Once you have set up MFA with at least one of the security mechanisms, please inform the computer center that manages the user accounts to activate MFA authentication on your user profile.

#### 3.1. Adding security mechanisms to a user profile

Open the [Office.com](https://office.com) website in the web browser of your choice and log in with your profile (user/student account):

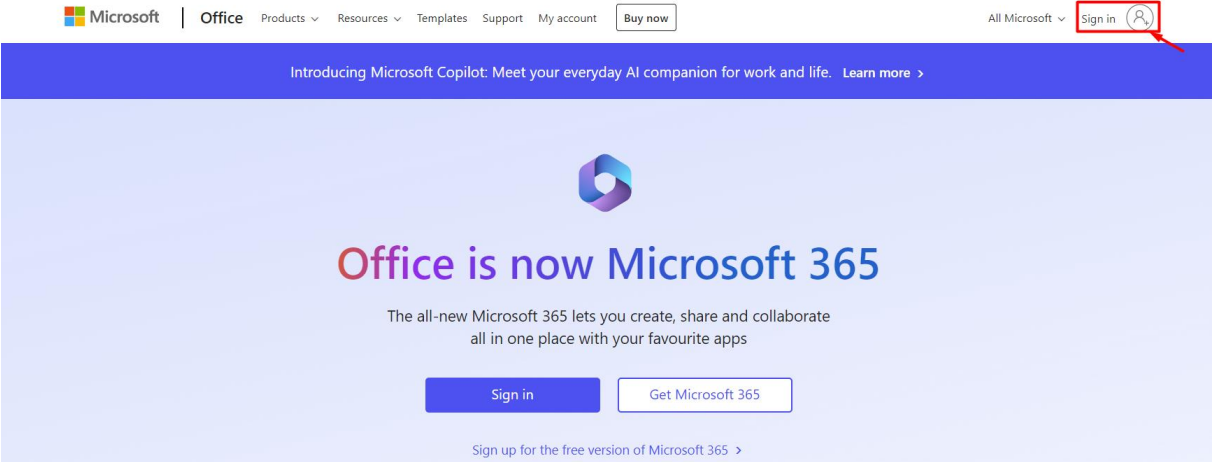


Figure 1: logging in to office.com

The website redirects you to the login screen, enter your username and select *Next*.

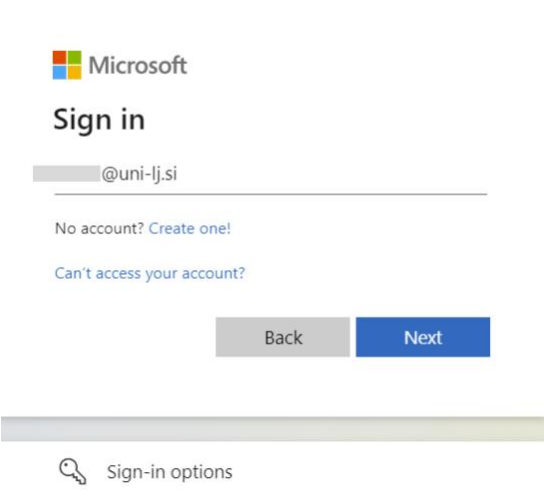


Figure 2: Login window.

After a successful login, you are now on the website, where you select *Options* and then *Update contact preferences*.

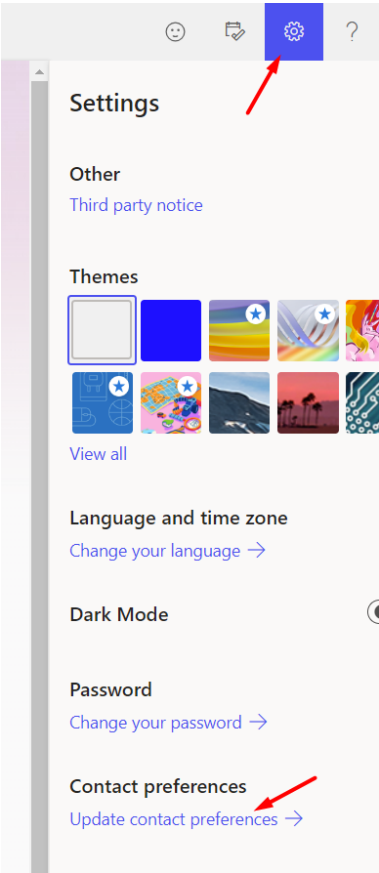


Figure 4: Updating your profile.

We are then redirected to the My Accounts page (in case it doesn't redirect us: <https://myaccount.microsoft.com/settingsandprivacy/privacy> ) and select *Security info*:

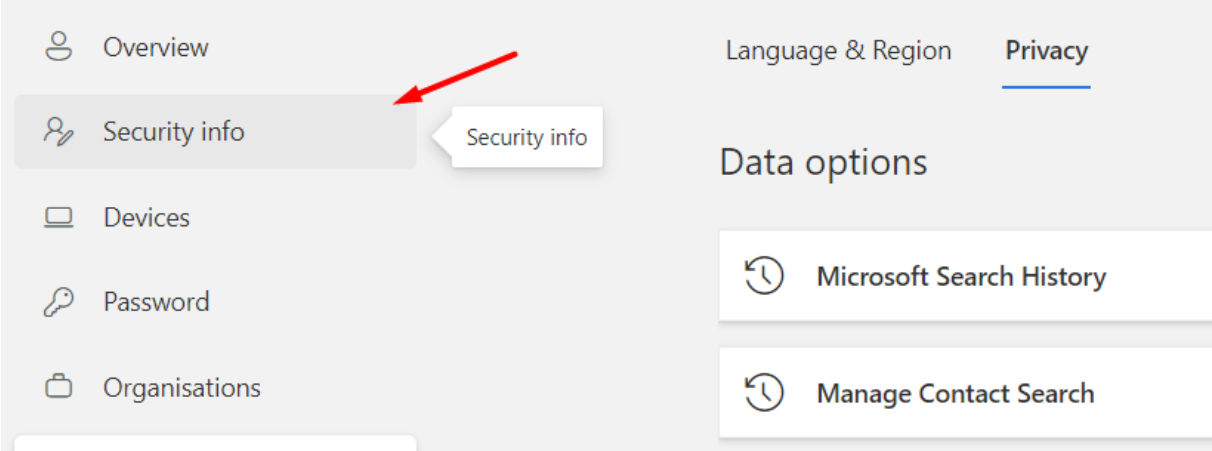


Figure 5: Security information section

Select *Add sign-in method*:

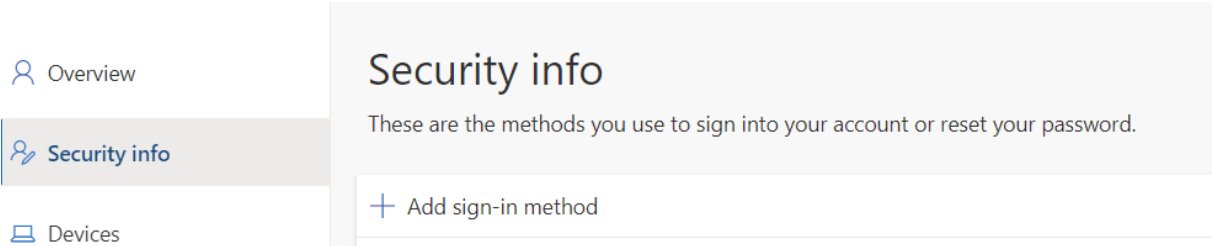


Figure 6: Adding an authentication method.

You can choose between several ways to enroll:

<i>Authenticator app</i>	Works on Android, iOS smartphone	<b>Recommended mode</b>
<i>Phone</i>	Code by SMS or call	Recommended as <b>alternative mode</b> or instead of smart phone.
<i>Replacement phone</i>	Code by SMS or call	Alternate in case of inability to use a personal phone
<i>Office phone</i>	Call	Alternate in case of inability to use a personal phone
<i>Security key</i>	USB key, biometric authentication	The security key must be inserted in the device at the time of enrolment.

**TIP:** we recommend setting at least two modes. In case one of the modes fails, you have other modes available. For example, the Autotimer app + phone (SMS) to a mobile number + back-up phone (call to a business number).  
If you don't use the Authenticator app, set up e.g. SMS/call to mobile + call to work phone.

### 3.2. Setting up the "Authenticator" method on your smartphone

After selecting *Add sign-in method* on the computer, we are presented with all the possible authentication methods that we can select. If we want to edit the authentication using the Authenticator application, we select the *Authenticator app option*:

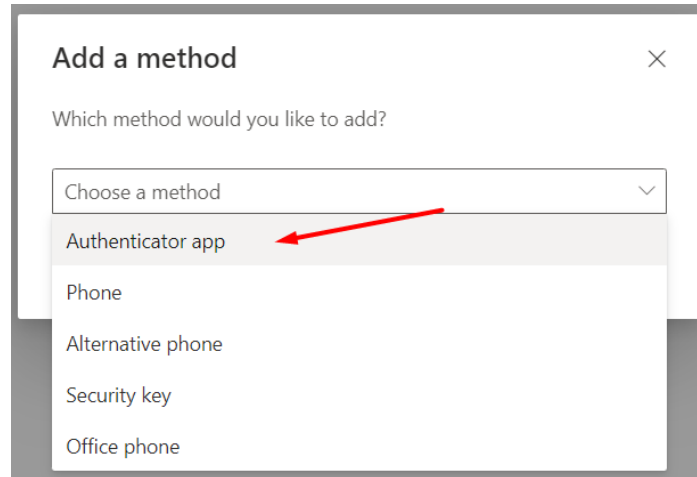


Figure 7: Selection of Application Authenticator

And continue with *Add*:

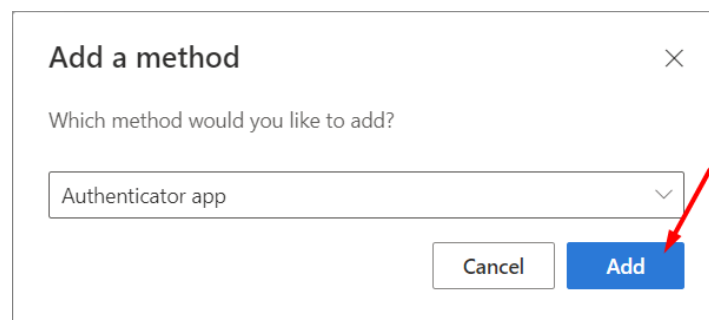


Figure 8: Add authentication method.

At this point, the following window appears:

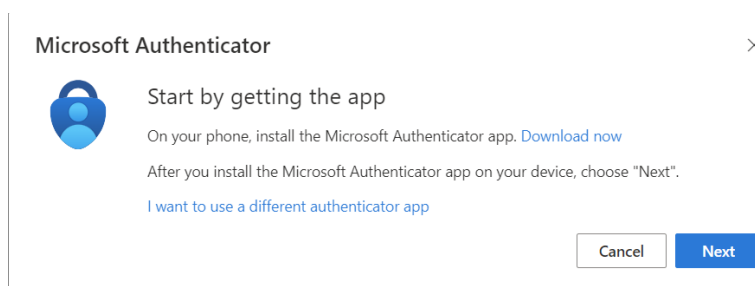


Figure 9: Window.

Leave the window open on your computer and take your **smart mobile phone**, open the *Google Play* store and search for and install the Microsoft Authenticator app.

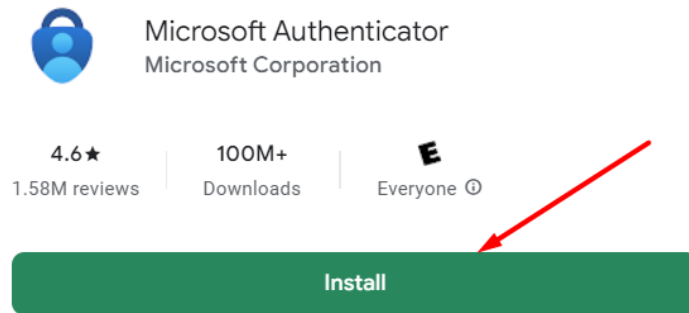


Figure 10: Microsoft Authenticator app.

Once the app has been successfully installed, we open the app and accept the privacy terms:

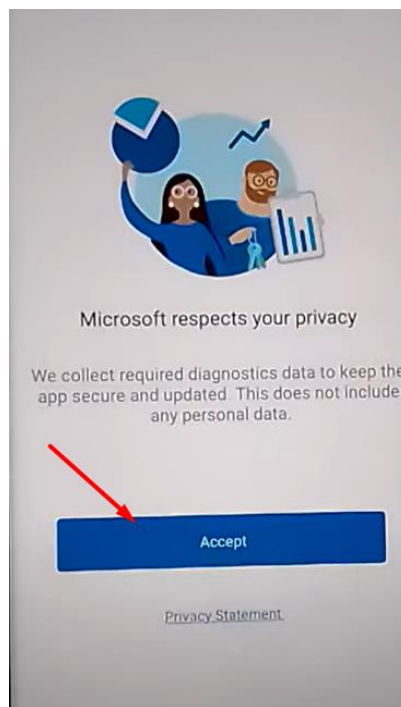


Figure 11: We accept the privacy terms.



Leave unticked and select *Next*:

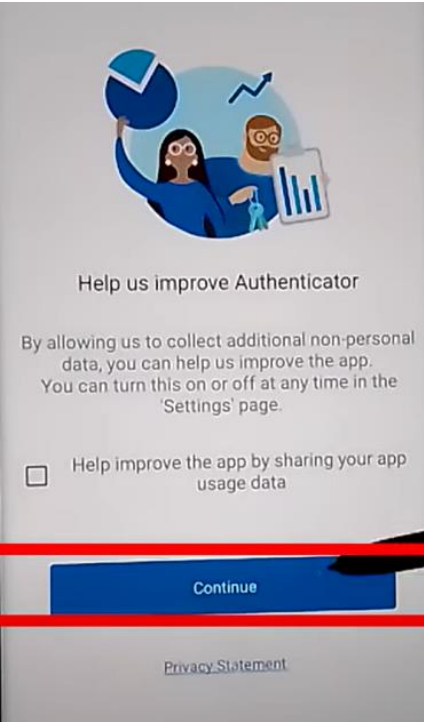


Figure 12: leave unticked and continue.

Select *Scan a QR code*:



Figure 13: QR code scanning step.

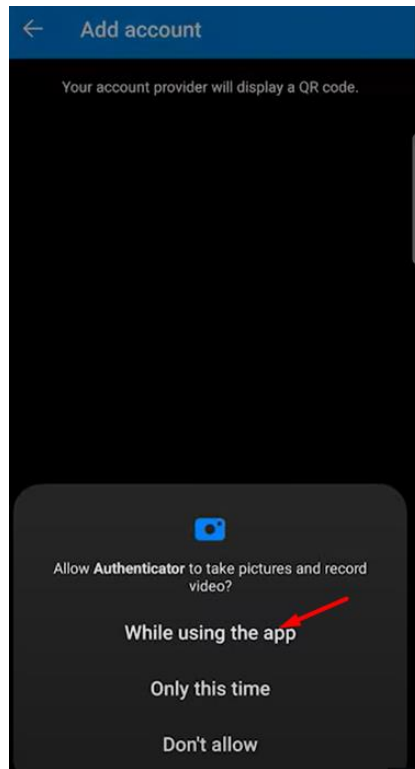


Figure 14: Enable permissions on the mobile phone.

Go **back to your computer to the still open window**, select *Next* and the QR code appears on the monitor. This QR code is **scanned with a smartphone**.

The QR code appears on the monitor. This QR code can be **optically read with a smartphone**. When you scan it on your computer, select *Next*, **and on your smartphone, OK**.

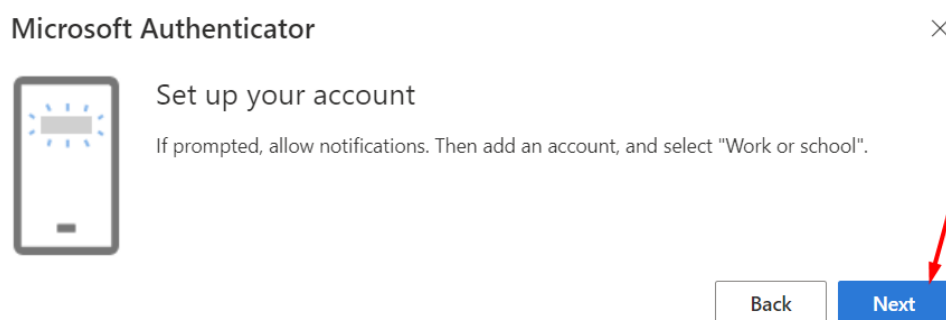


Figure 15: Click next.

A number appears on the **computer**, which is entered into the application on the **smart mobile phone**:

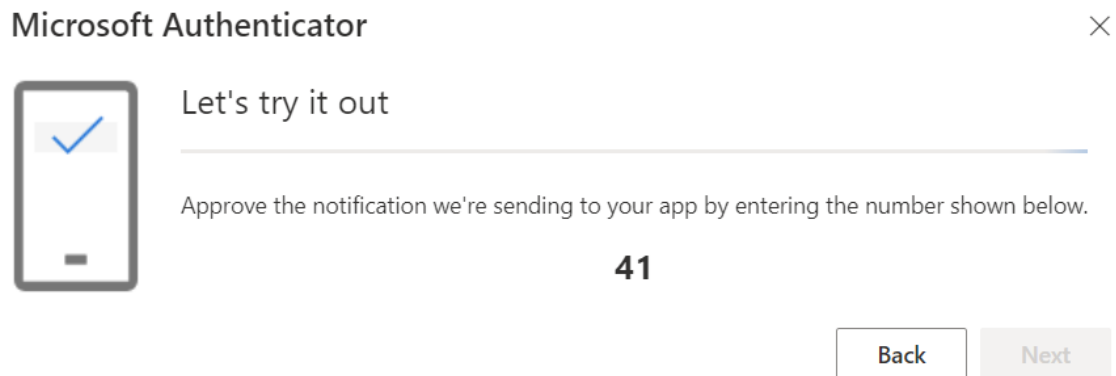


Figure 16: Time-limited enrolment number on a mobile smartphone.

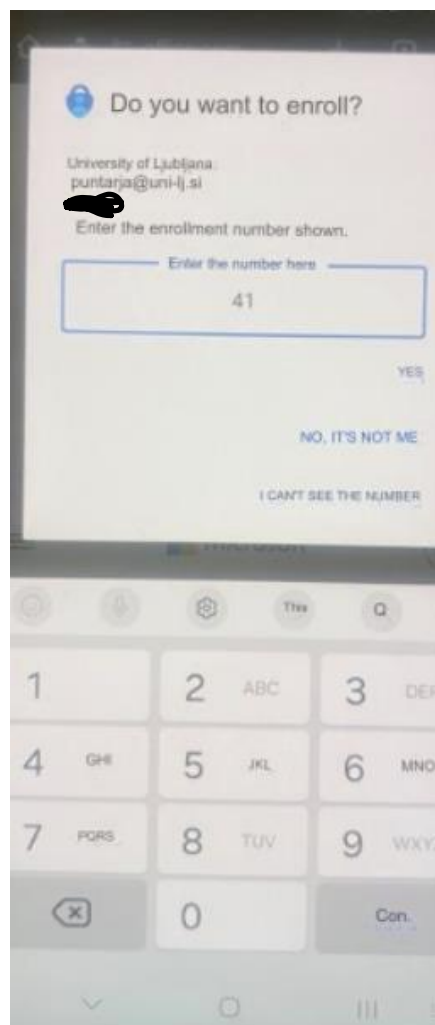


Figure 17: Entering a number from your computer and confirming your registration by selecting.

If we have set up a smartphone lock, we need to authorize enrolment using one of the pre-configured security methods.

Figure 18: Approval of enrolment.

If we have done everything correctly, we are notified of the success on the computer:

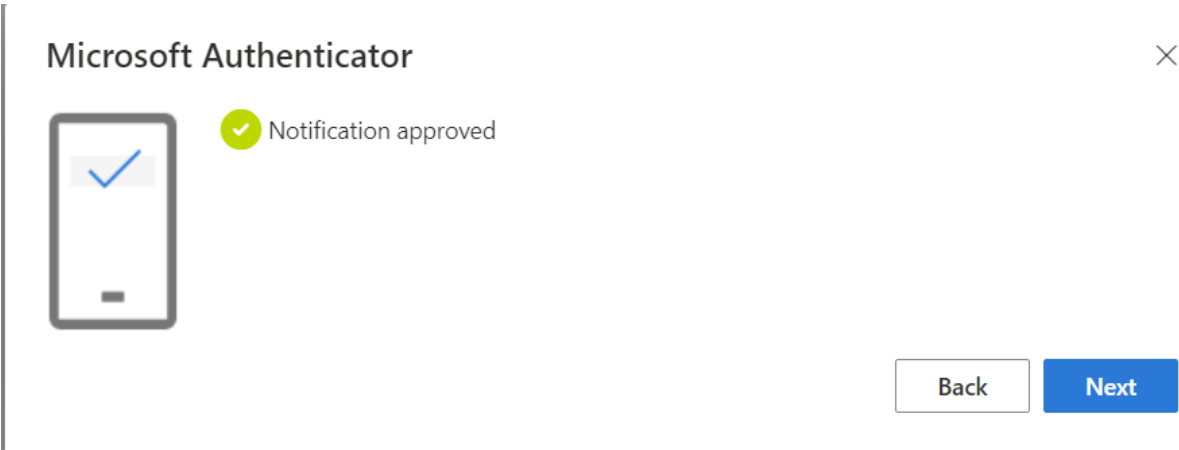


Figure 19: Authentication method successfully added.

This is how we added the authentication method using the Authenticator application. If you want to add SMS or some other method, you can continue reading the instructions.

### 3.3. Setting up the "mobile phone" method

You are on (<https://myaccount.microsoft.com/settingsandprivacy/privacy>) and select *Add entry mode*:

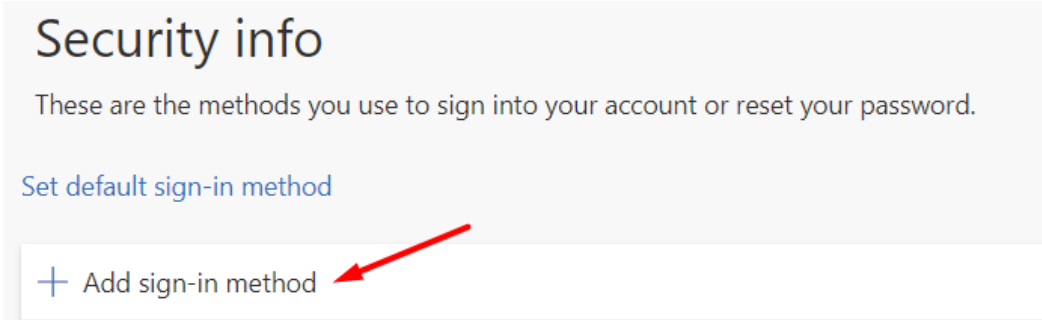


Figure 20: add an entry mode.

## Select *Phone*:

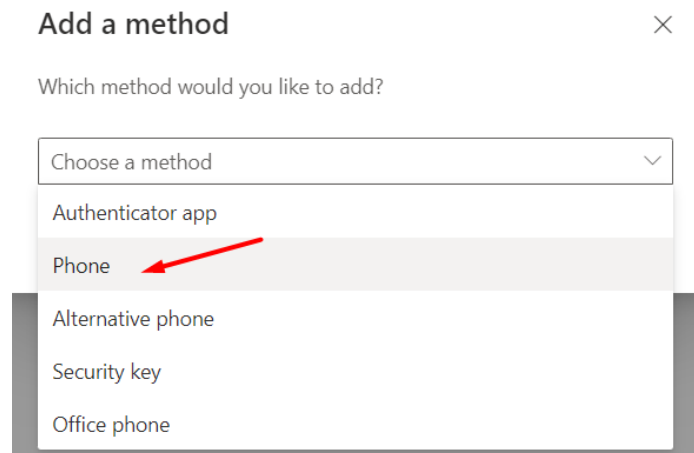


Figure 21: Phone selection.

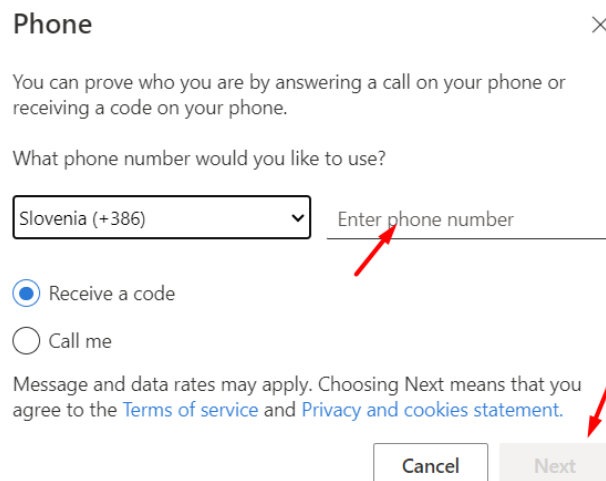


Figure 22: Enter your number and select Next.

Take your mobile phone, wait for the SMS message to arrive and type the 6-digit, time-limited number into the window on your computer:

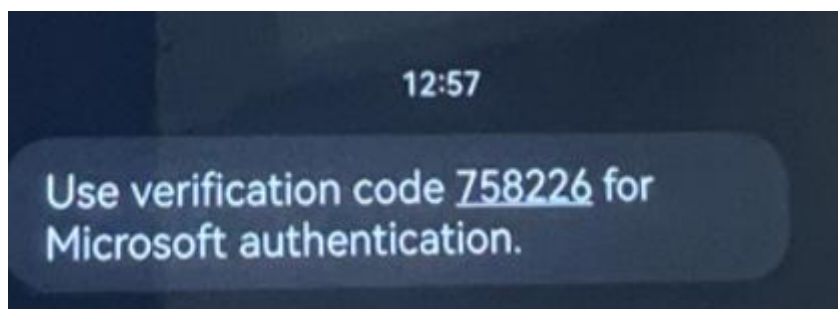


Figure 23: 6-digit, time-limited number received.

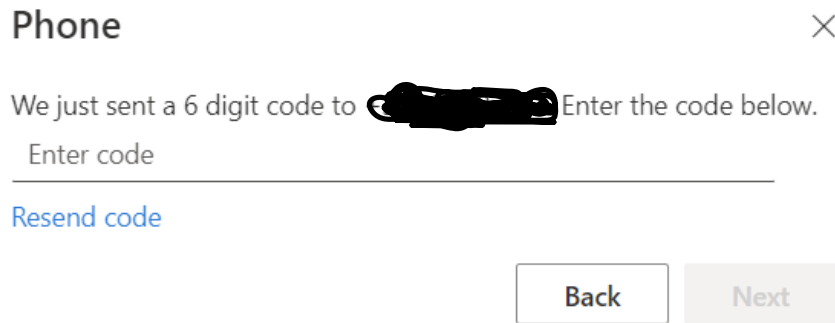


Figure 24: Entering a number in the displayed window on the computer.

If the correct 6-digit code is entered, we get a confirmation that the added authentication method was successful:

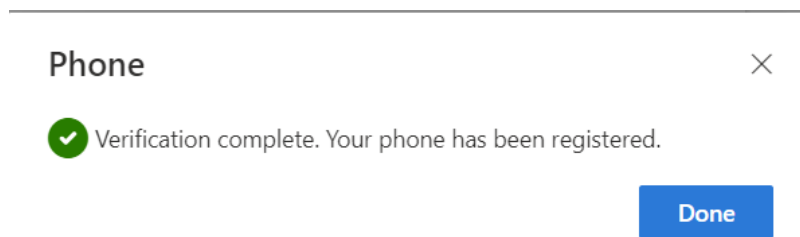


Figure 25: Authentication method successfully added.

You can also set up *Substitute phone*, *Business phone in the same way*. On the latter, only a call is available. Enter your service number, leave the *internal number* field blank.

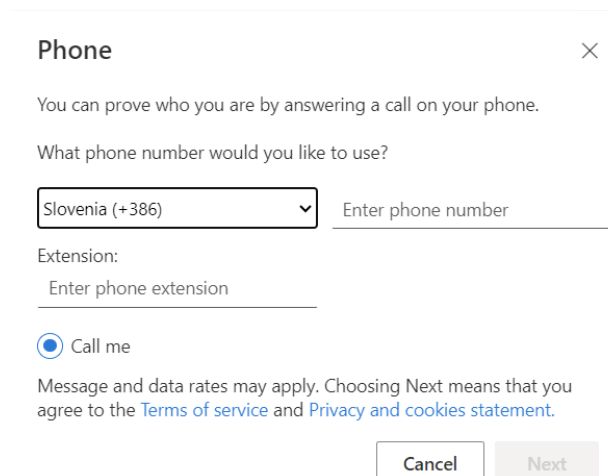


Figure 26: Entering a number for the Office phone.

### 3.4. Setting the "security key" method

For this method, you will need a security key that complies with the FIDO2 standard. Contact your ICT Service for a key. **Pre-set your** authentication mode with your phone or *Authenticator* app!

Pojdite na <https://myaccount.microsoft.com/settingsandprivacy/privacy> and select *Add entry mode*:

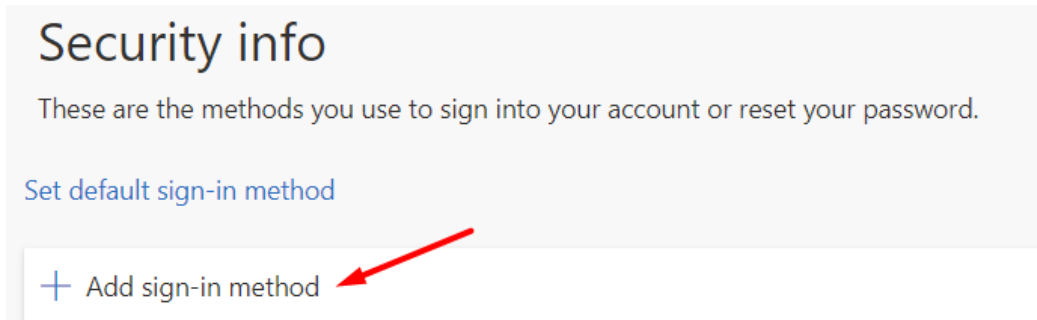


Figure 27: add an entry mode.

Select the *Security key*:

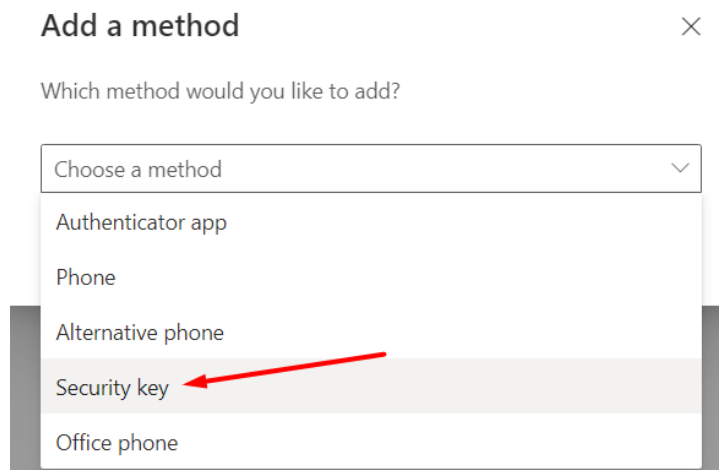


Figure 28: Security key selection.

Confirm the selection *Security key*.

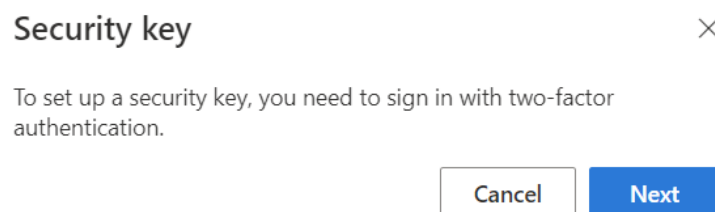


Figure 29: Security key selection.

Select "USB device" as the key type.



Figure 30: Choosing a key type - USB.

If a QR code appears in the next step, select "Use another device" and in the next step select "Use Windows Hello or external security key" (Figure 32).

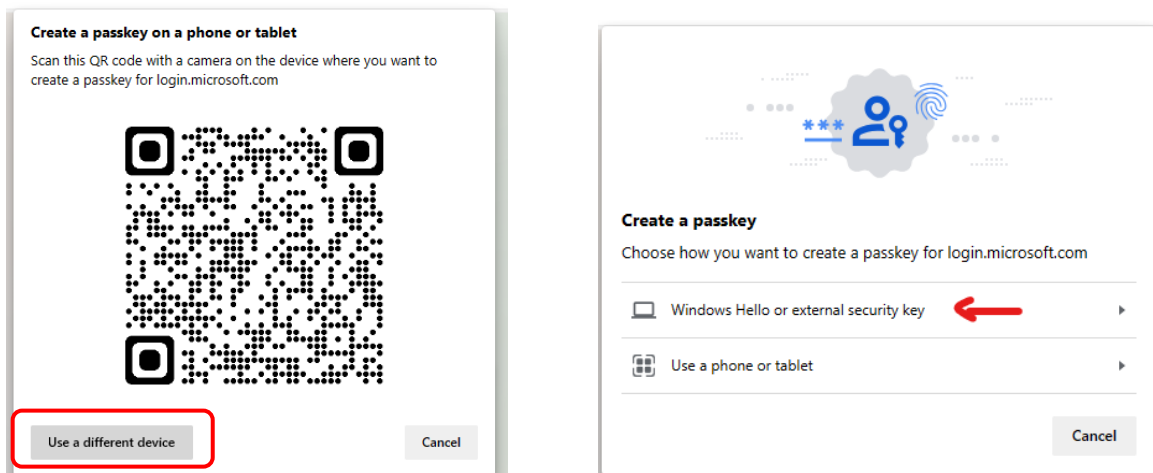


Figure 31: Choosing the right device.



Continue by clicking Next.

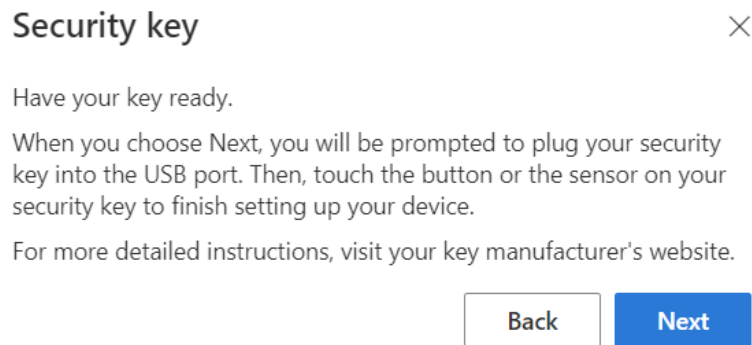


Figure 32: Confirmation to continue installation.

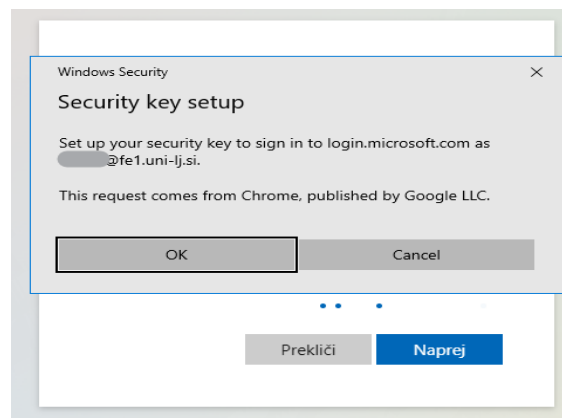


Figure 33: Binding a login with a key to a user profile.

Have your security key ready and insert it into the USB slot when you send the message.

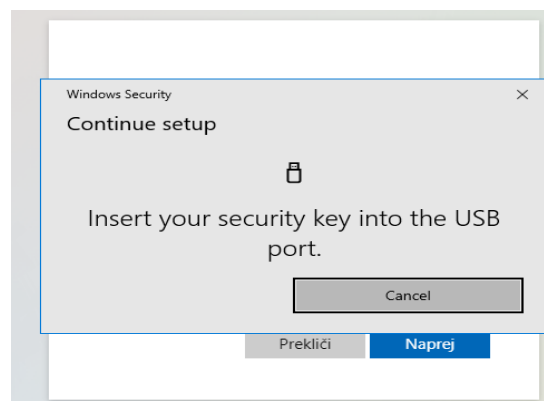


Figure 34: Inserting the dongle into the USB slot.

The first time you use the key, you will be prompted to **set your** PIN code and biometric fingerprint.

You will be prompted to enter your PIN and fingerprint on subsequent uses.

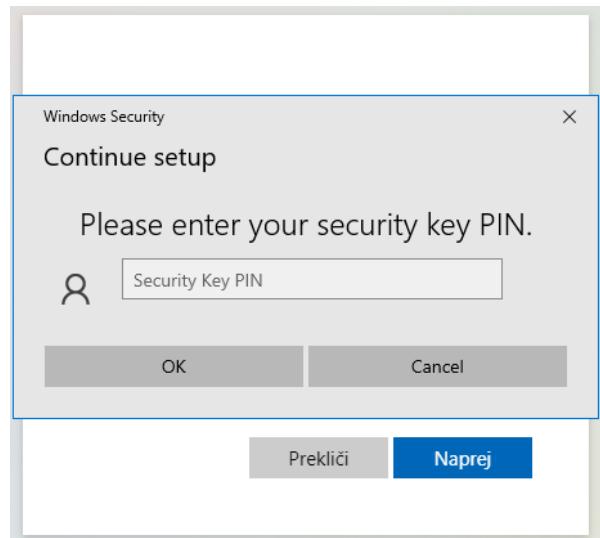


Figure 35: PIN setting (first activation only) or PIN entry.

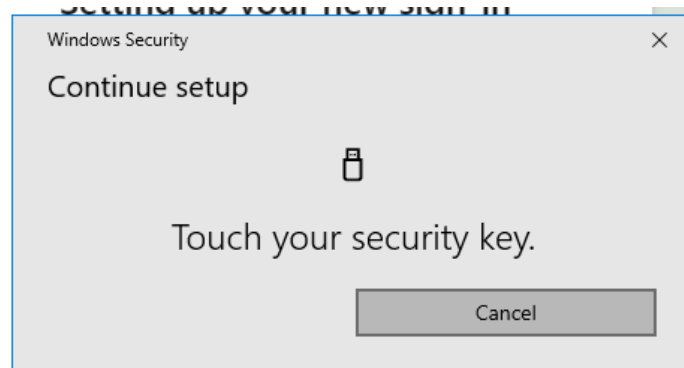


Figure 36: Fingerprint confirmation.

In the final step, you just need to name your key and the process is complete.

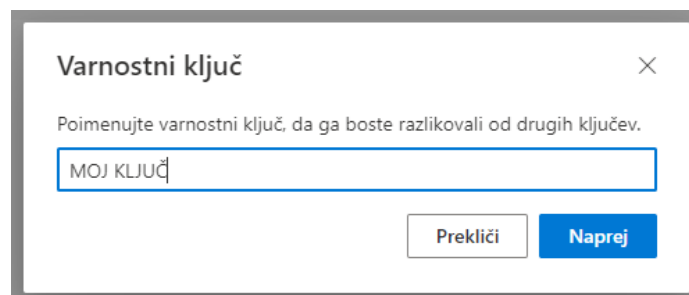


Figure 37: Naming the key.

### 3.5.Changing the default authentication method

The authentication methods we have set up for our profile can be seen on the website(<https://mysignins.microsoft.com/security-info> )where you can **change the default** entry mode. The default mode will be used as the first offered, i.e. preferred, validation method. **In any case, we can always choose between the other methods we have previously set up each time we log in.**

The default authentication method is set as follows:

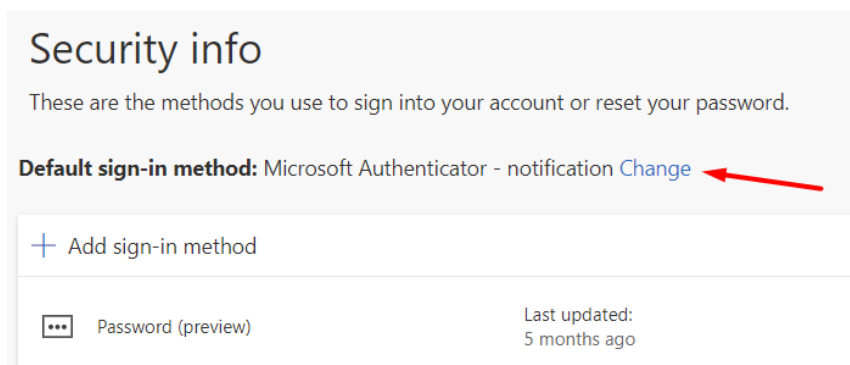


Figure 38: Default enrolment mode.

Select a mode from the drop-down menu:

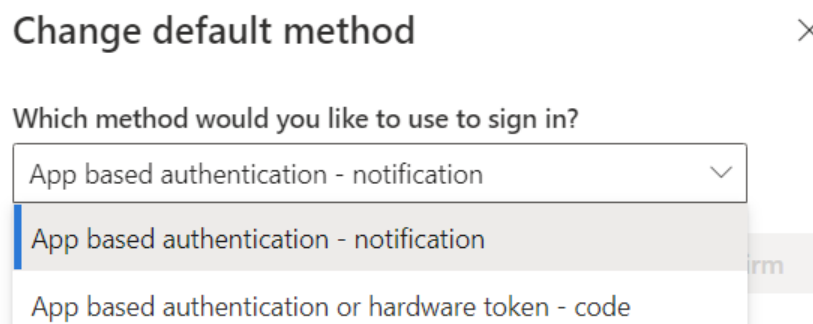
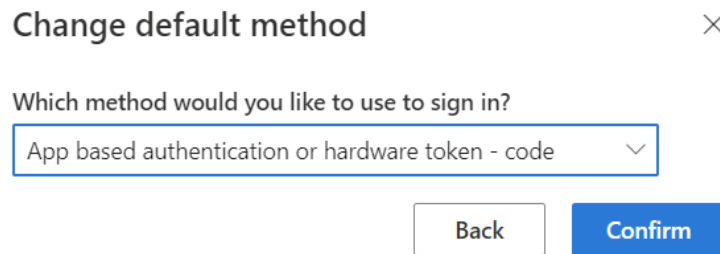


Figure 39: Mode selection.

And confirm the choice:



The screenshot shows a dialog box titled "Change default method" with a close button (X) in the top right corner. Below the title is the question "Which method would you like to use to sign in?". A dropdown menu is open, showing the selected option "App based authentication or hardware token - code". At the bottom of the dialog, there are two buttons: "Back" and "Confirm".

Figure 40: Authentication method validation.

At this point, please inform the Member's ICT Service that you have added authentication methods and would like to use MFA. Once the ICT Service has advised that MFA has been activated, it will now be requested in logins with your user account<sup>1</sup>.

### 3.6. Action in the event of loss or theft of a device

If the device you use for enrolment - MFA has been lost or stolen, please click on "Logout from all sites" to log out of devices and contact the IT Service of your faculty. If you are a student contact [helpdesk@uni-lj.si](mailto:helpdesk@uni-lj.si)

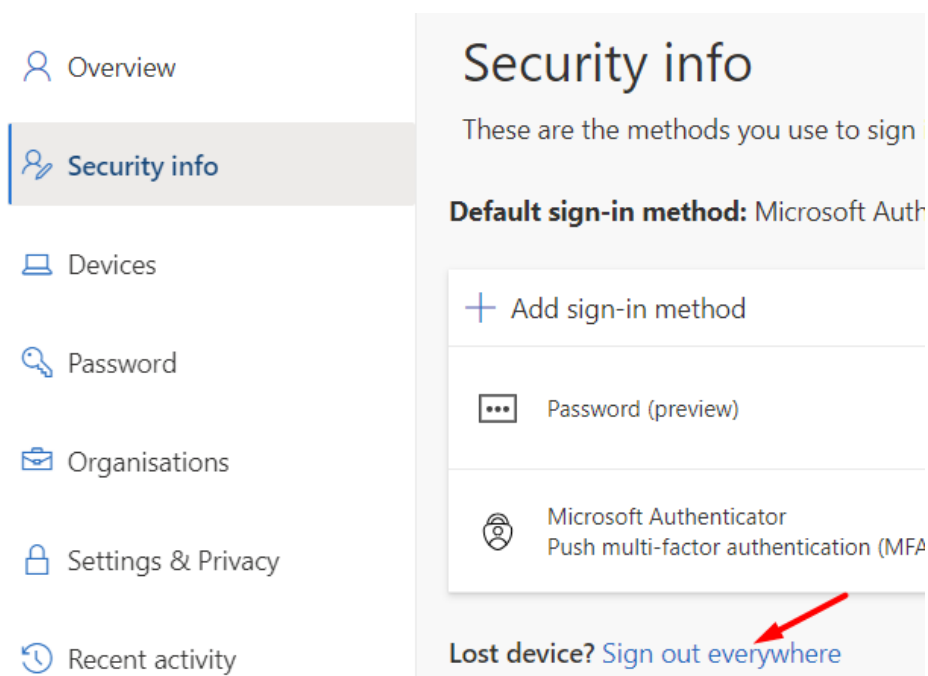


Figure 41: Sign out incase device is lost.

<sup>1</sup> Some applications and services at UL do not currently require MFA.

## 4. Useful links

1. Video instructions on how to set up an MFA:  
<https://www.youtube.com/watch?v=VwEd-vhmVzI>
2. Safety information: <https://mysignins.microsoft.com/security-info>
3. Microsoft 365 home page: <https://office.com/>