



Setting up dual authentication (MFA) for iOS mobile devices

Jagiellonian University

IT Services Center

Information Systems Infrastructure Department

Document date: October 2024, Version:1.1

Authors:

Estera Ambroź (estera.ambroz@uj.edu.pl)

CONTACT INFORMATION

Centrum Informatyki, Dział Infrastruktury Systemów Informatycznych, ul. Reymonta 4, Kraków

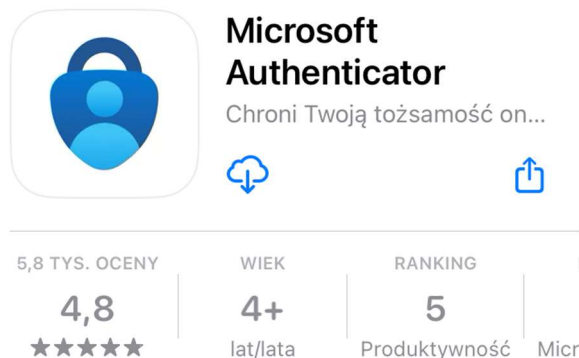
E-mail: ci@uj.edu.pl | **Web:** <https://it.uj.edu.pl>

Table of contents

Setting up dual authentication (MFA) for iOS mobile devices	1
Step 1 - Downloading the application to a mobile device	3
Step 2 - Enabling security on the JU account	5
Step 3 - Reporting the willingness to enable two-factor authentication	14
Step 4 - Login after enabling dual authentication	15
Additional steps required for certain devices and applications	18
iOS devices on which a JU account has previously been configured	18
OneDrive synchronisation client	24

STEP 1 - DOWNLOADING THE APPLICATION TO A MOBILE DEVICE

The first step to start setting up two-factor login (dual authentication) is to download the **Microsoft Authenticator** app from the App Store on your mobile device (smartphone or tablet).



Once the app has been downloaded and launched, a data privacy notice will be displayed, which must be approved by selecting *Accept*. On the next screen, select *Continue*. It is not necessary to consent to the app collecting additional data.



Firma Microsoft szanuje Twoją prywatność

Zbieramy wymagane dane diagnostyczne, aby zapewnić bezpieczeństwo i aktualizację aplikacji. Nie obejmuje to żadnych danych osobowych.

Akceptuj

[Oświadczenie o ochronie prywatności firmy Microsoft](#)



Pomóż nam ulepszyć aplikację Microsoft Authenticator

Zezwalając nam na zbieranie dodatkowych danych innych niż osobiste, możesz pomóc nam ulepszyć aplikację. Możesz włączyć lub wyłączyć tę funkcję w dowolnym momencie na stronie Ustawienia



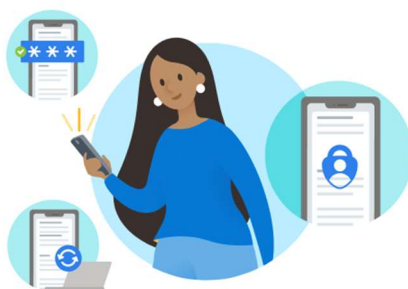
Ulepsz aplikację, udostępniając dane użycia aplikacji

Kontynuuj

[Oświadczenie o ochronie prywatności firmy Microsoft](#)

You will then be presented with another screen where it is possible to choose how to connect the application to your university account.

At this point, temporarily stop using application until you have enabled security settings on your account on the computer. This means that you temporarily do not select any of the following options.



Zabezpiecz swoje życie cyfrowe



Zaloguj się przy użyciu
konta Microsoft

W przypadku zalogowania się przy użyciu konta Microsoft, wszystkie zapisane hasła, adresy i inne informacje wypełniane automatycznie będą dostępne na tym urządzeniu.



Dodaj konto służbowe

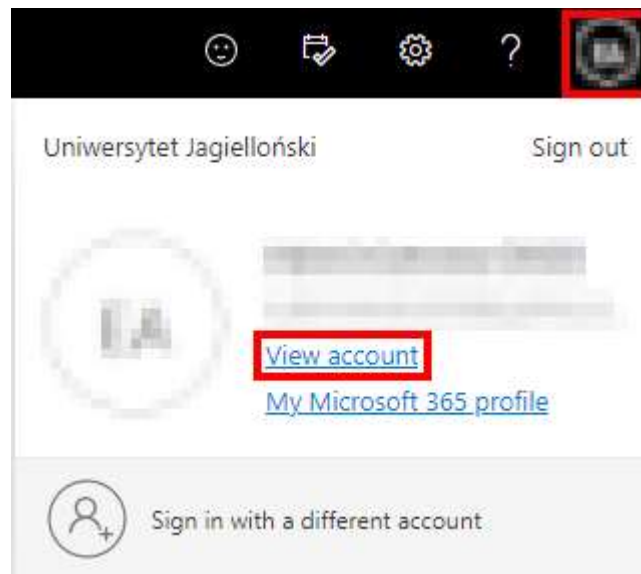


Zeskanuj kod QR

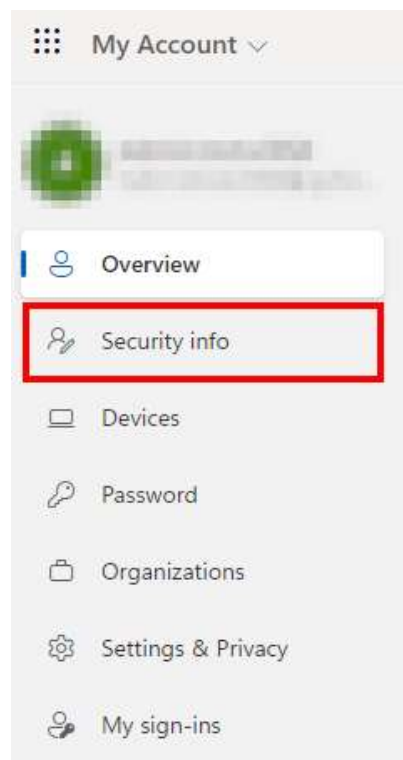
Przywróć z kopii zapasowej

STEP 2 - ENABLING SECURITY ON THE JU ACCOUNT

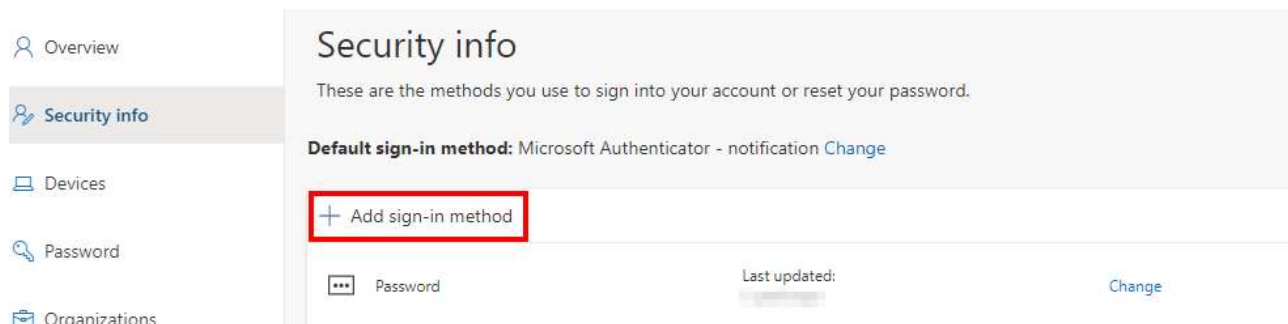
Using a computer, open a web browser and log in to *office.com* using your university login ID. Then click on the profile icon (with your initials or photo), which is located in the top right corner, and select *View Account*.



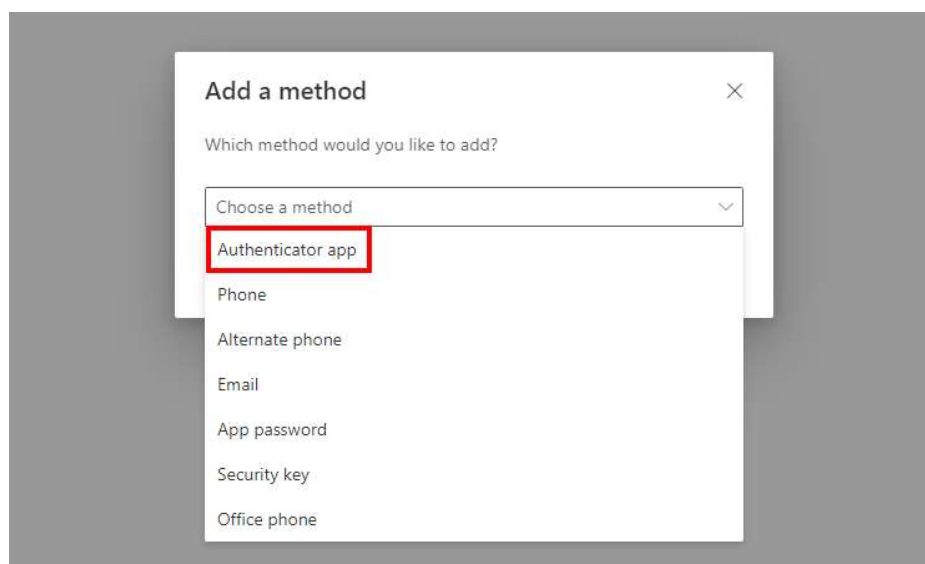
Then select *Security info* in the left-hand menu.



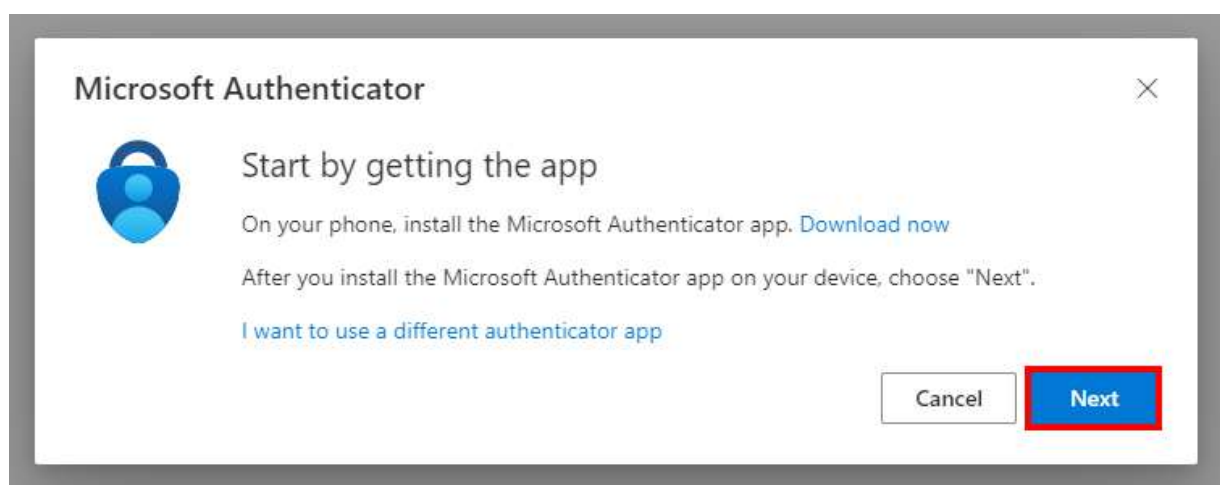
On the *Security info* page, select *Add sign-in method*.



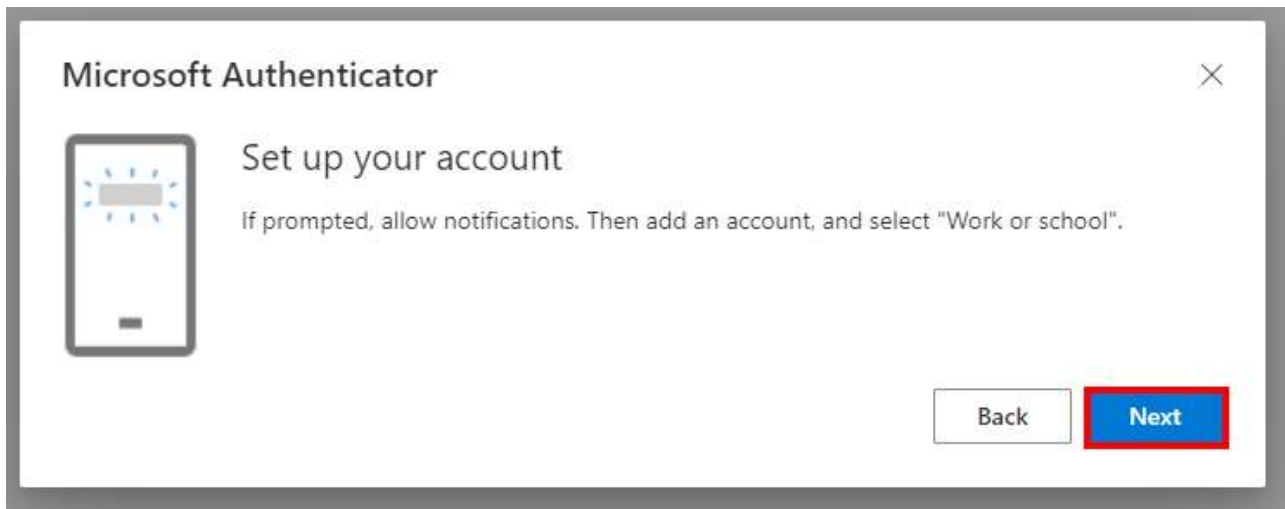
This opens a window where you can choose the second authentication method. Select Authenticator app and then click Add.



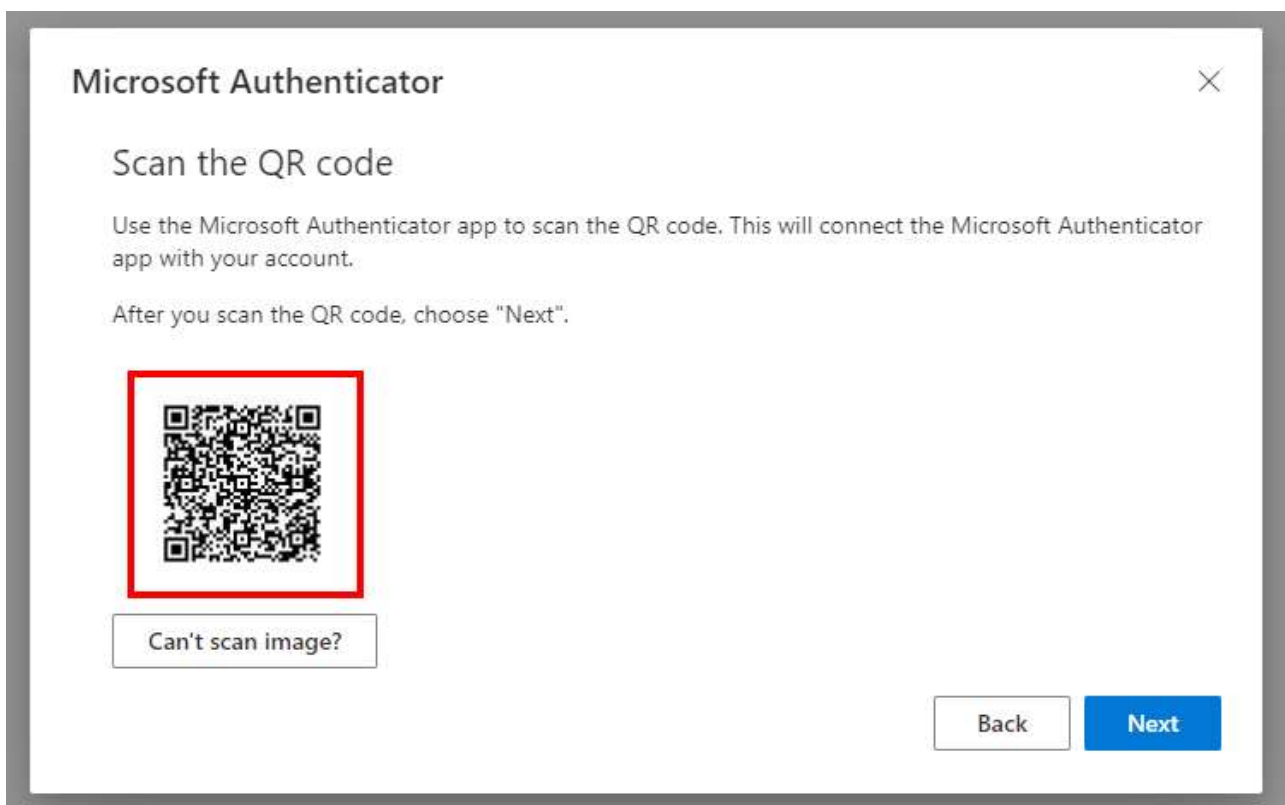
The system will then prompt you to download the application. By following these instructions, the application on the phone is already installed, so select *Next*.



In the next step, also select *Next*.



This will display QR code, which must be scanned using the Microsoft Authenticator app that was installed earlier.

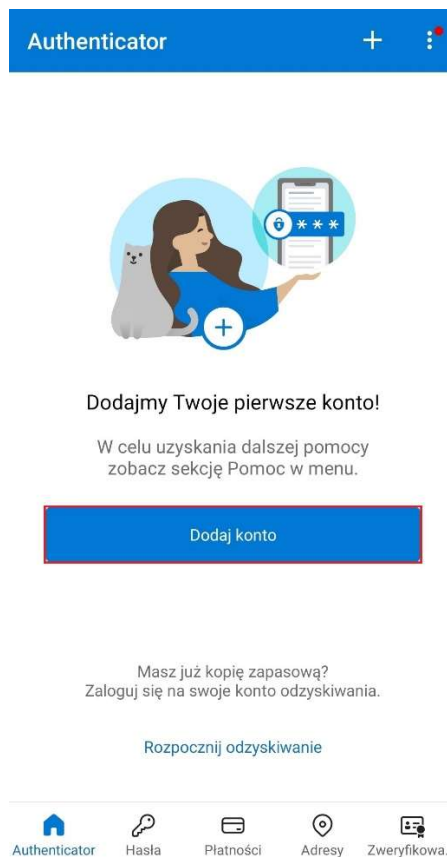


To do this, restart the Microsoft Authenticator app on the mobile device.

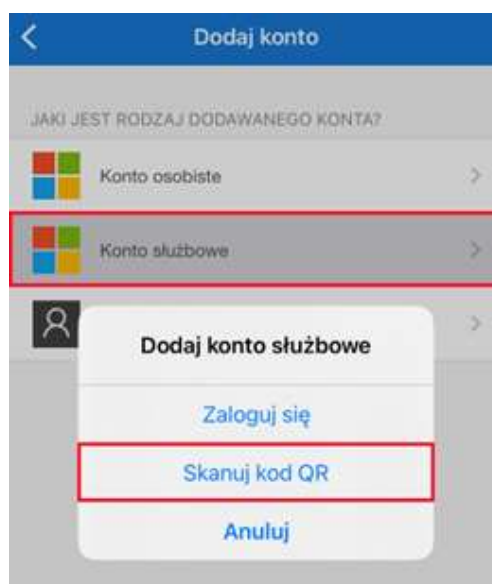
There are two possible scenarios for displaying the information on the user's mobile device.

1. Adding a new account view

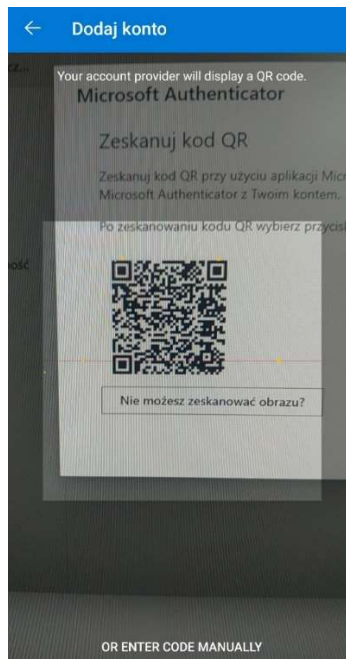
If the following view is displayed, select *Add account* or select the '+' icon.



Select *Business Account* from the list, which will bring up a window. In the window, select the *Scan QR code* option.

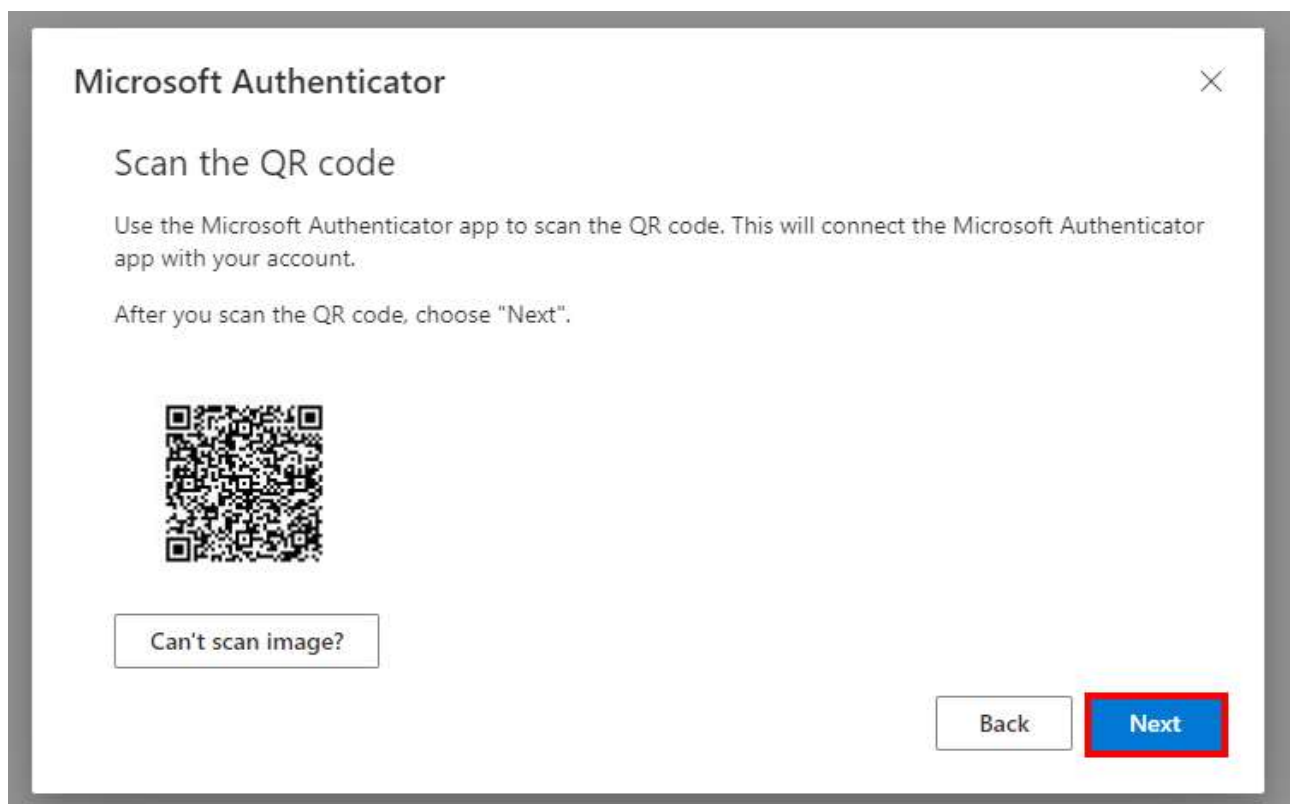


Then scan the QR code displayed on the computer screen in the app.

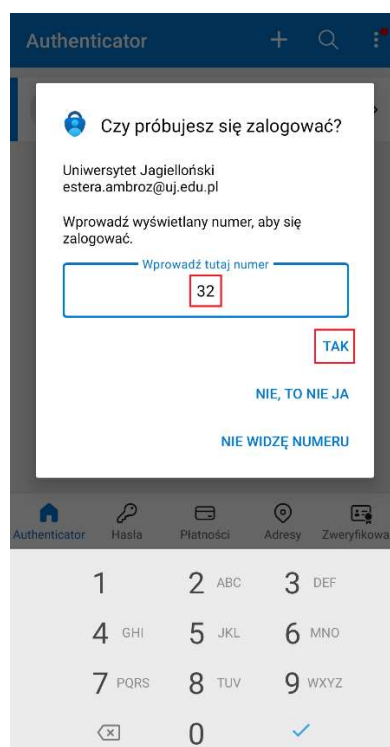


After scanning, the message *Application lock is enabled* appears. To better protect the Authenticator app, app lock is now enabled by default. To disable it, go to the app settings. This means that you will need to unlock the app each time before entering it in the same way you unlock your phone screen.

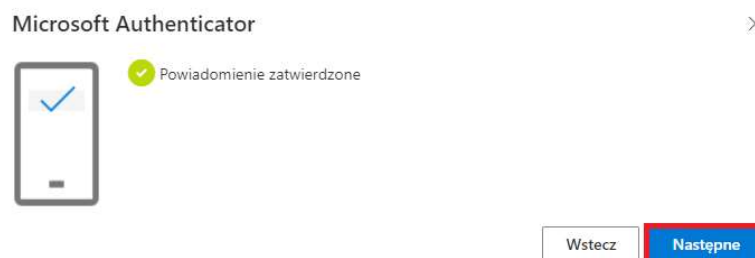
After scanning the QR code, return to the Security info tab previously opened in the web browser and select *Next*.



The browser will display a two-digit code that must be entered into the Microsoft Authenticator app on the mobile device.

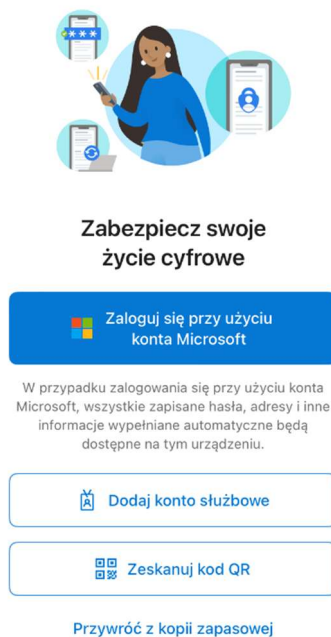


The final step is to select *Next* in the following prompt displayed in the browser. Once you complete the steps above, the method should be correctly configured.

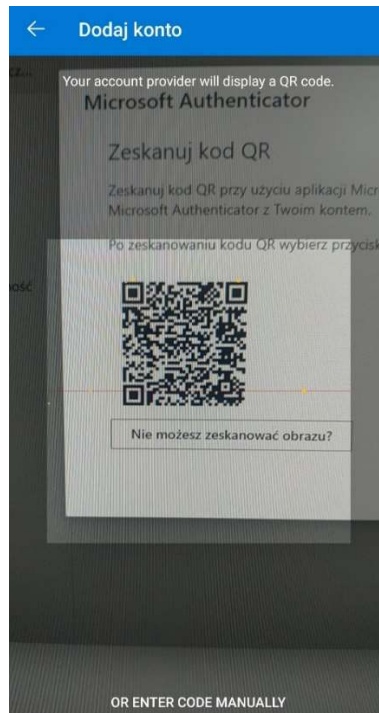


2. Action selection view

If the following view is displayed, select *Scan QR code*.

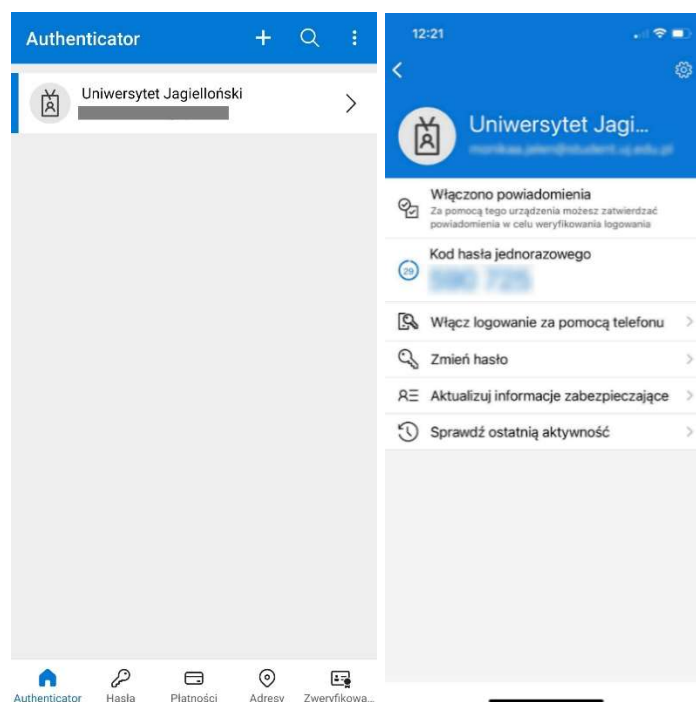


Then scan the QR code displayed on the computer screen in the app.

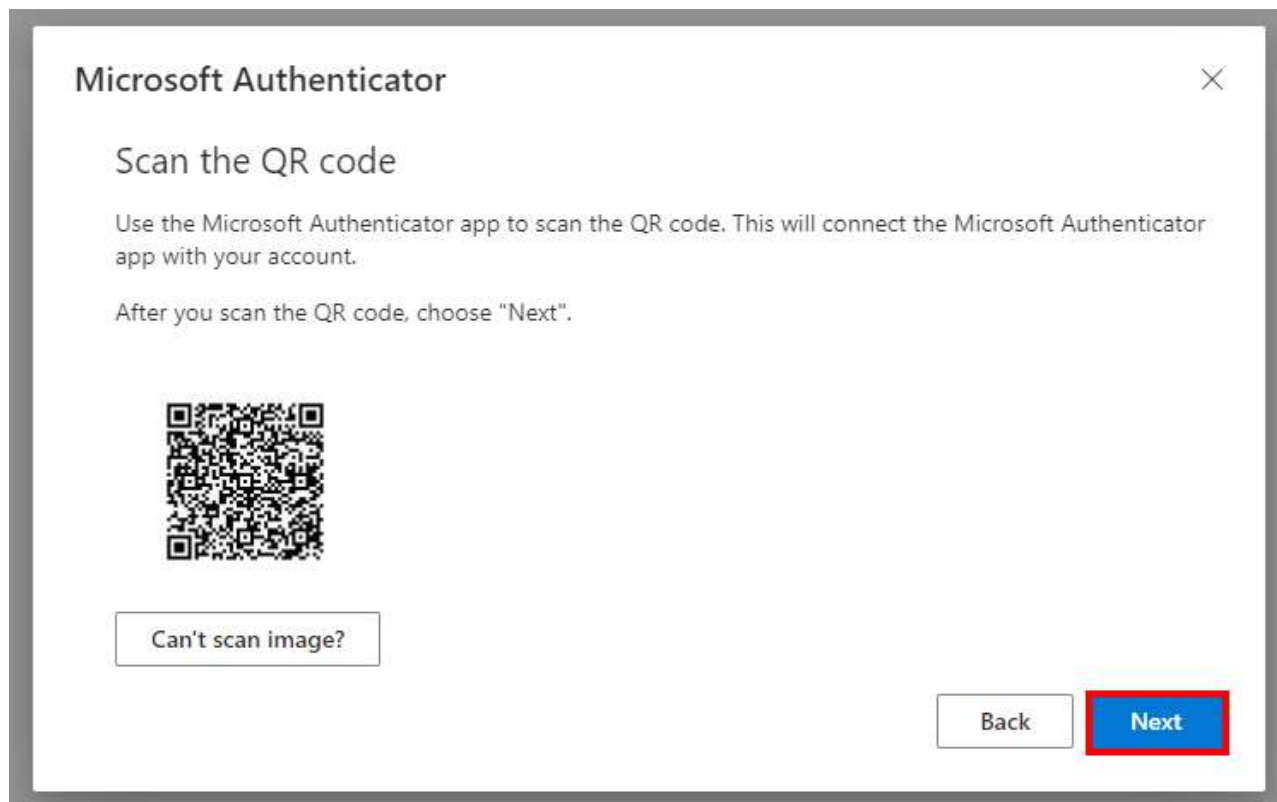


After scanning, the message *Application lock is enabled* appears. *To better protect the Authenticator app, app lock is now enabled by default. To disable it, go to the app settings.* This means that you will need to unlock the app each time before entering it in the same way you unlock your phone screen.

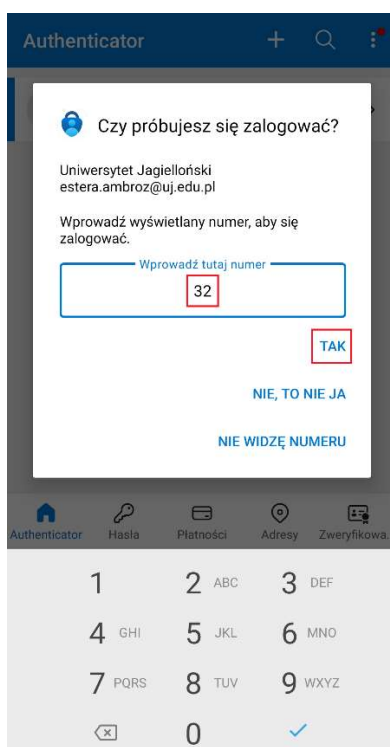
After scanning the QR code, your university account will appear in the mobile app.



After scanning the QR code, return to the Security info tab previously opened in the web browser and select *Next*.



The browser will display a two-digit code that must be entered into the Microsoft Authenticator app on the mobile device.



The next step is to select *Next* in the next message displayed in the browser.



The final step is to select the default login method in the *Security info* tab. Select *App based authentication - notification*.

The image shows two screenshots from a Microsoft account settings interface. The top screenshot is the 'Security info' page, which has a title 'Security info' and a subtitle 'These are the methods you use to sign into your account or reset your password.' Below this, a red box highlights the text 'Default sign-in method: Microsoft Authenticator - notification' followed by a blue 'Change' link. The bottom screenshot is a 'Change default method' dialog box. It has a title 'Change default method' and a close button (X) in the top right. The question 'Which method would you like to use to sign in?' is followed by a dropdown menu. A red box highlights the dropdown menu, which currently shows 'App based authentication - notification' with a downward arrow. Below the dropdown are two buttons: 'Back' and 'Confirm'. The 'Confirm' button is highlighted with a red box.

STEP 3 - REPORTING THE WILLINGNESS TO ENABLE TWO-FACTOR AUTHENTICATION

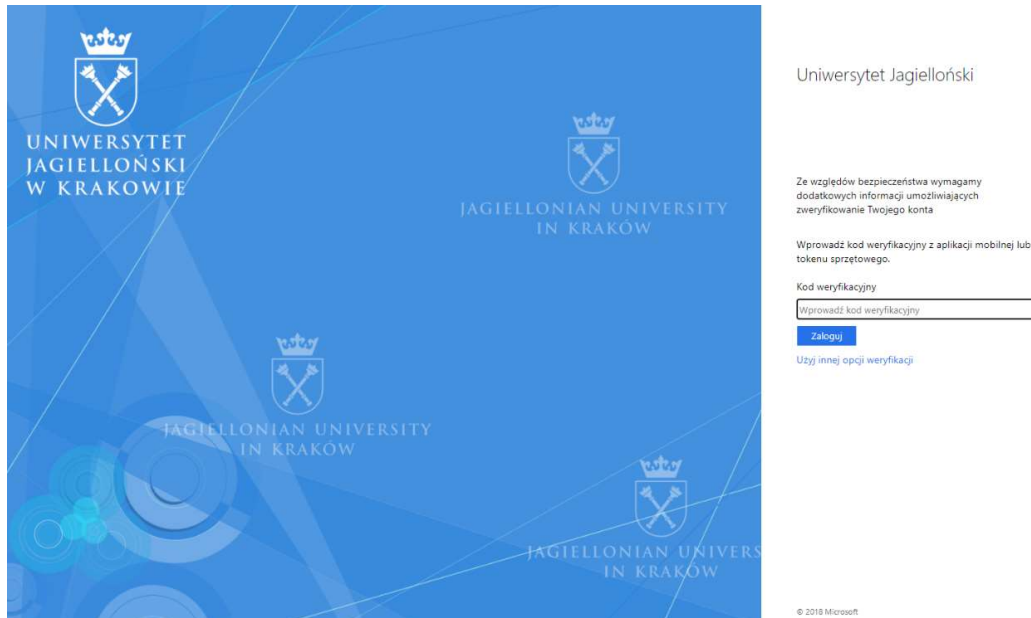
Once you have completed the steps above, you can declare your willingness to launch dual authentication early on your user account or wait until the designated date that was stated in the notification you received.

To request an early activation method, please contact IT Support at pomocit@uj.edu.pl.

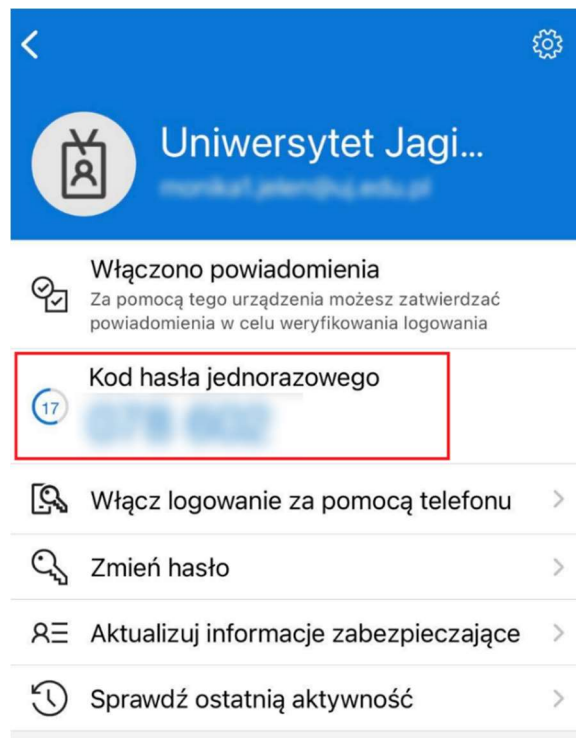
STEP 4 - LOGIN AFTER ENABLING DUAL AUTHENTICATION

Over the next few hours, applications on your computer or on other devices will prompt you to confirm your login with a second factor.

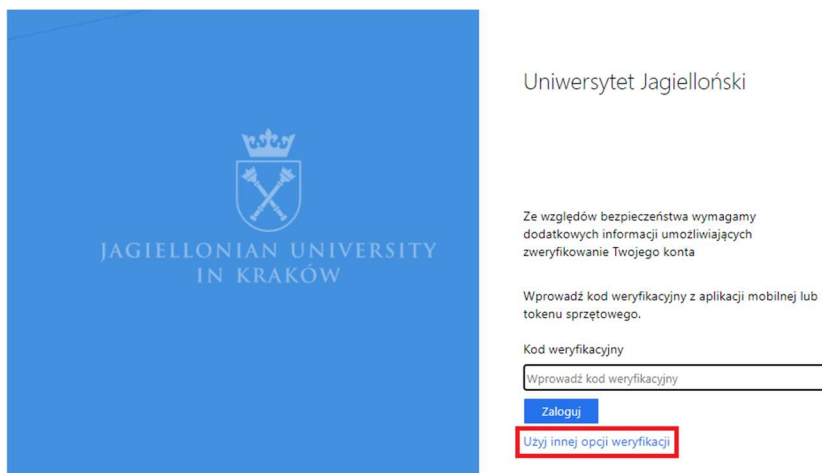
If you are logged in on your devices, you will be logged out and asked to log in again, and then to confirm your login in the Microsoft Authenticator app on your mobile device.



When the user is prompted to enter a verification code, they should launch the application on their phone (mobile device) and enter the code displayed.



It is also possible to change the verification option by selecting *Use another verification option*.



Uniwersytet Jagielloński

Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

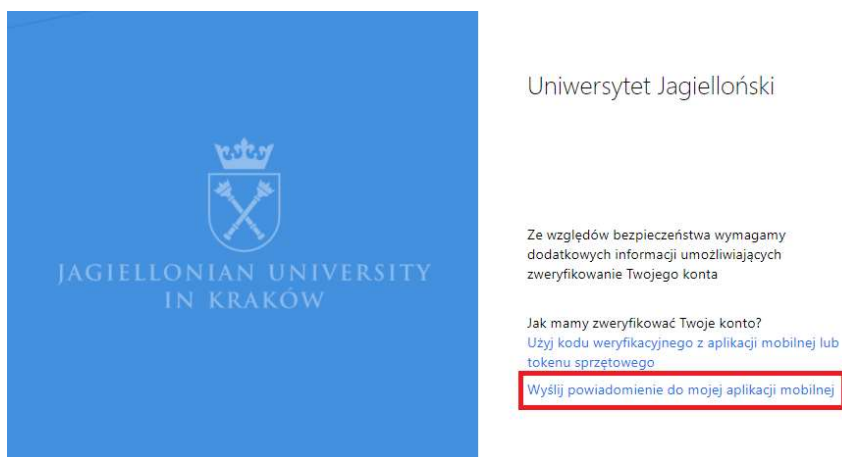
Wprowadź kod weryfikacyjny z aplikacji mobilnej lub tokenu sprzętowego.

Kod weryfikacyjny

Zaloguj

Użyj innej opcji weryfikacji

Then select *Send notifications to my mobile app*.



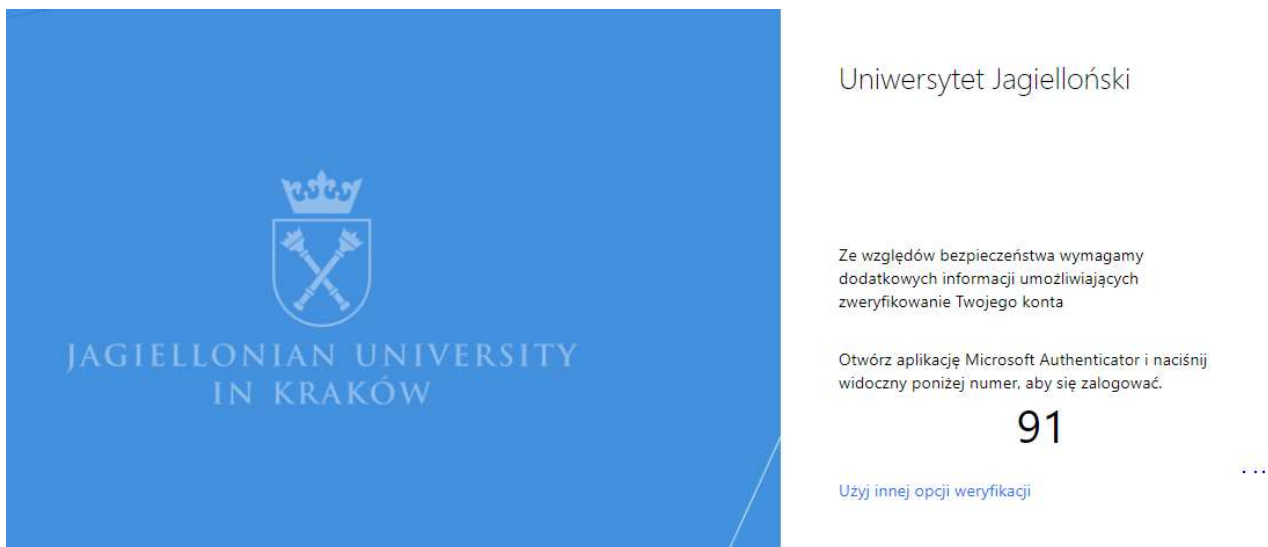
Uniwersytet Jagielloński

Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Jak mamy zweryfikować Twoje konto?
Użyj kodu weryfikacyjnego z aplikacji mobilnej lub tokenu sprzętowego

Wyślij powiadomienie do mojej aplikacji mobilnej

A number will then be displayed on the computer screen:



Uniwersytet Jagielloński

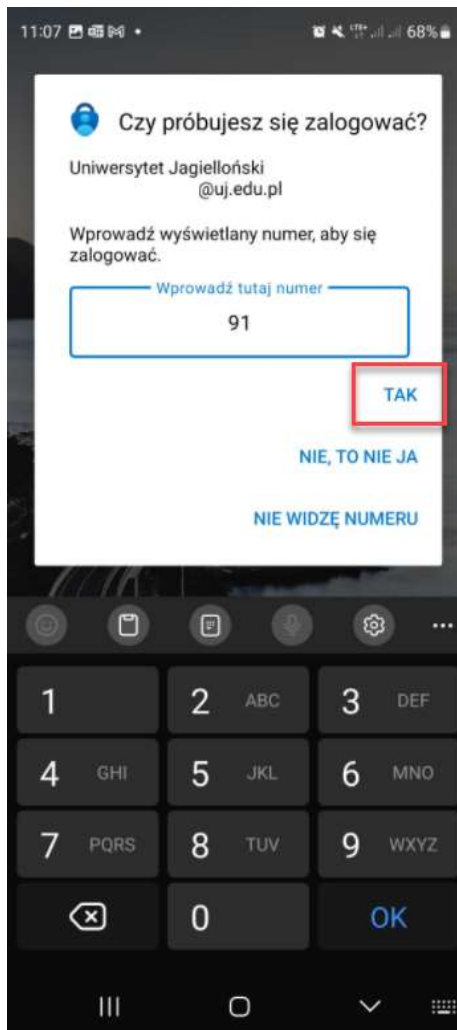
Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Otwórz aplikację Microsoft Authenticator i naciśnij widoczny poniżej numer, aby się zalogować.

91

Użyj innej opcji weryfikacji

A message will be displayed on your mobile device asking you to validate the login by entering the number displayed on the computer screen and clicking YES.



Once the number has been entered, the login must be confirmed with the pattern or screen lock code of the mobile device.

ADDITIONAL STEPS REQUIRED FOR CERTAIN DEVICES AND APPLICATIONS

For some devices and applications, an additional action will be required to ensure that dual authentication is fully configured and that data synchronisation on the device is not interrupted.

iOS devices on which a JU account has previously been configured

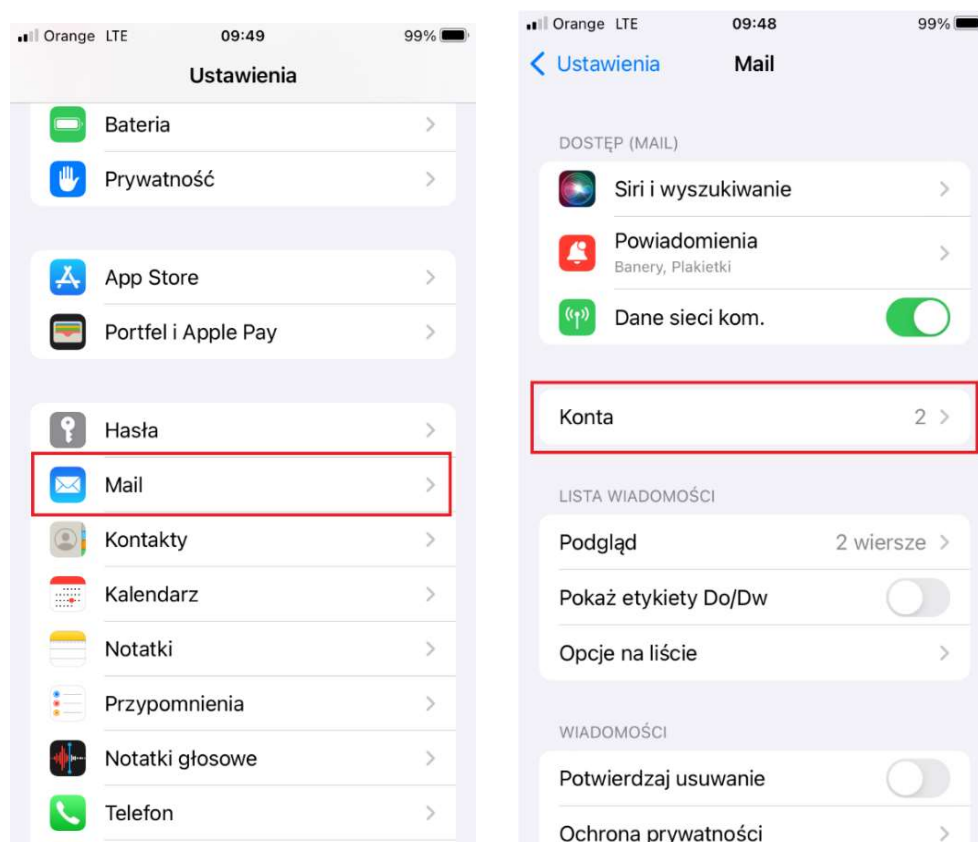
Devices running the iOS operating system (iPhone or iPad) do not prompt you to log back into your account after setting up dual authentication. It is necessary in this case to remove the JU account from the device and add it again.

To delete your JU account from your iOS device, please:

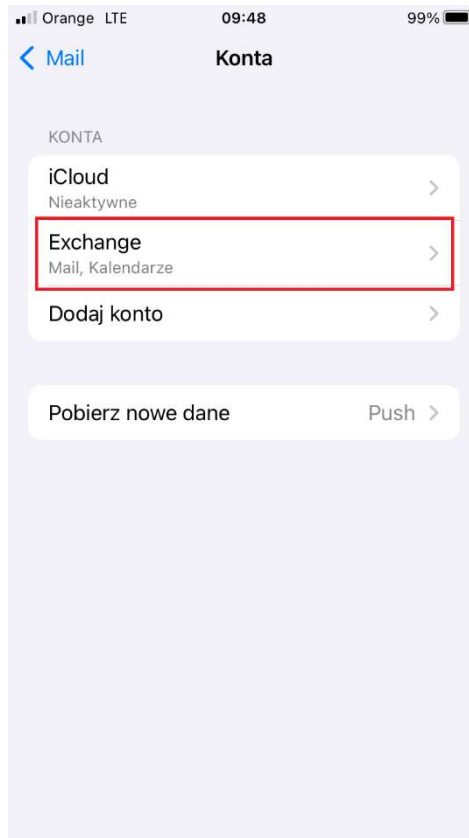
1. Open Device *Settings* with the icon:



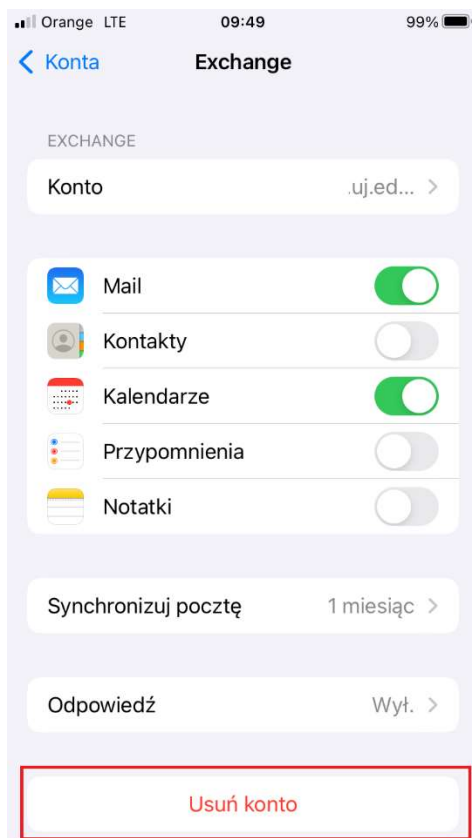
2. In Settings, go to *Passwords & Accounts* (for iOS 13.x or older) or to *Mail*, then *Accounts* (for iOS 14.x or later)



3. Select the JU account, named *Exchange* as standard:

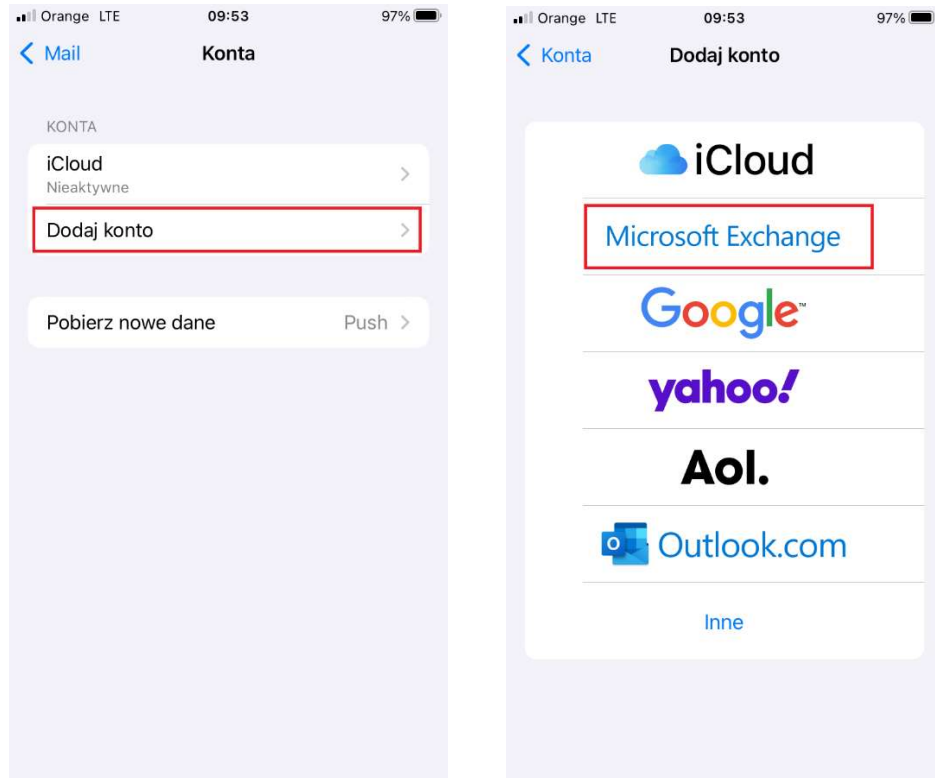


4. In the account view at the bottom of the page, click *Remove account* and confirm the removal operation:

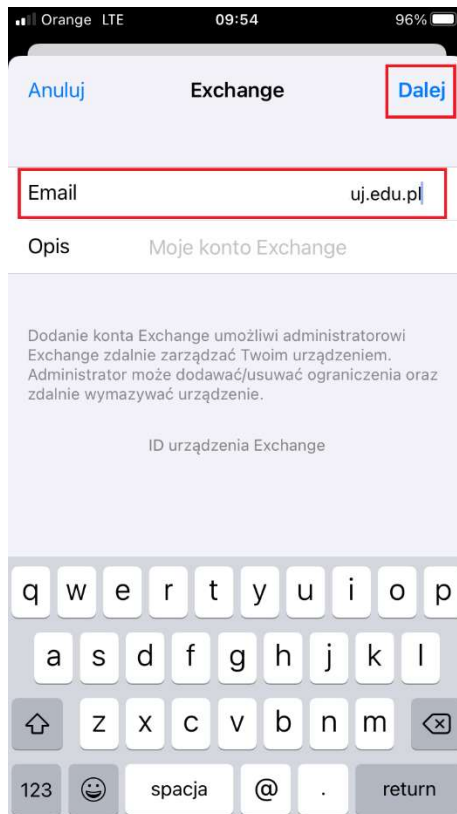


Once the JU account has been removed from the device, the *Accounts* view will be displayed, where the JU account will no longer be visible. At this point, you can add the account anew through the following steps:

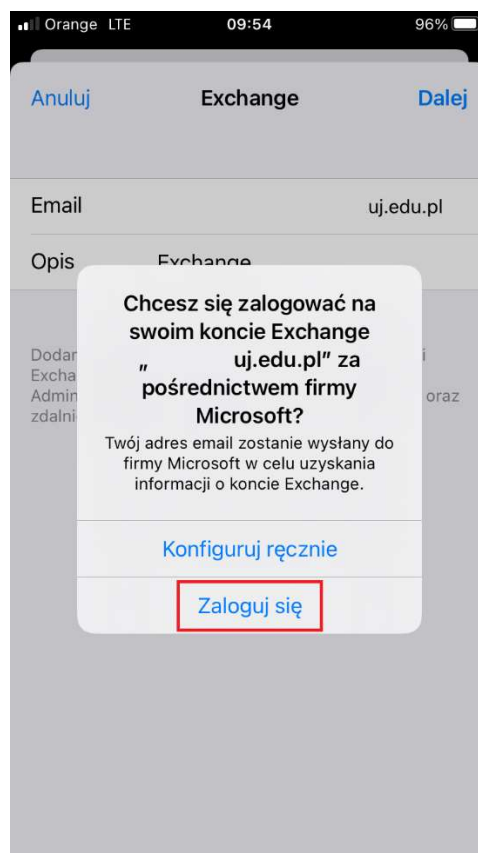
1. In the *Accounts* view, select *Add Account* and then *Microsoft Exchange*:



2. Enter an email address from the JU domain in the *Email* field and click *Next*:



3. In the *Do you want to log into your Exchange account* window, click *Log in*:



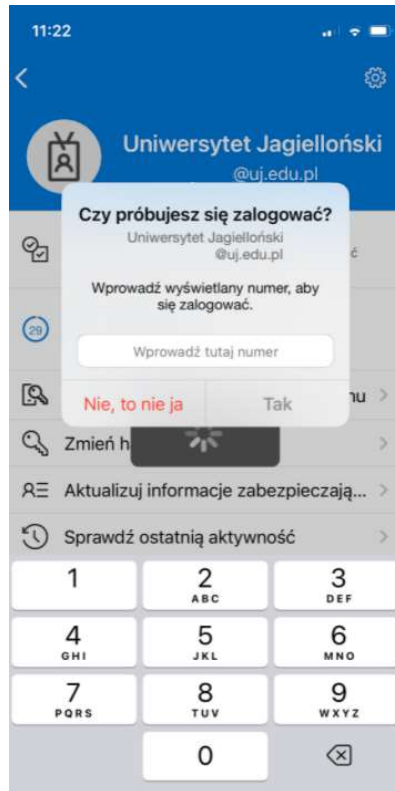
4. The JU login page will be displayed, where you will need to enter your password:



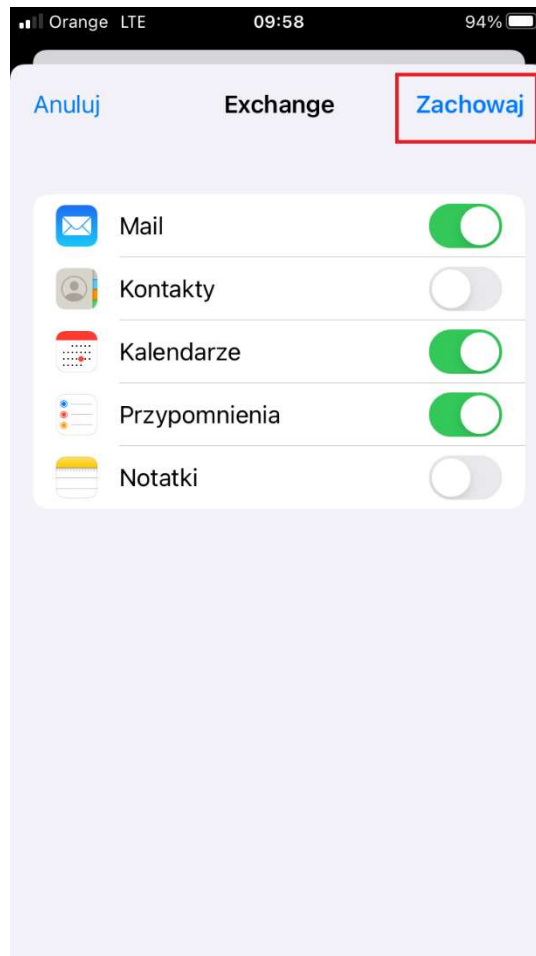
5. You will then be prompted to verify the login with a second factor with information on the number to be entered:



6. In the Microsoft Authenticator application, you will be prompted to approve the login along with a space to enter a number:



7. After confirming the login, select the applications to sync the data from the JU account to the device according to your preferences and click **Save**. After this action, the JU account is added to the device and the data is synchronised:



OneDrive synchronisation client

The OneDrive app you install on your computer to sync files with your cloud drive requires you to log back into the service after setting up dual authentication.

To do this, click on the OneDrive client icon on your computer's taskbar  and then click on the prompt asking you to log back in with your JU account.

In the Microsoft Authenticator app on your mobile device, you will be prompted to approve the login. After this approval, the OneDrive app will start syncing files to your computer again.