

Procedure to be followed if the administrator enforces two-factor authentication - iOS

Jagiellonian University

IT Services Center

Information Systems Infrastructure Department

Document date: August 2024, Version:1.0

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

Procedure to be followed if the administrator enforces two-factor authentication - iOS	1
Step 1 - First login after enforcing dual authentication	3
Step 2 - Downloading the application to your mobile device	4
Step 3 - Enabling security on the UJ account	6
Step 4 - Login with dual authentication	16
Additional steps required for certain devices and applications	17
OneDrive synchronisation client	17

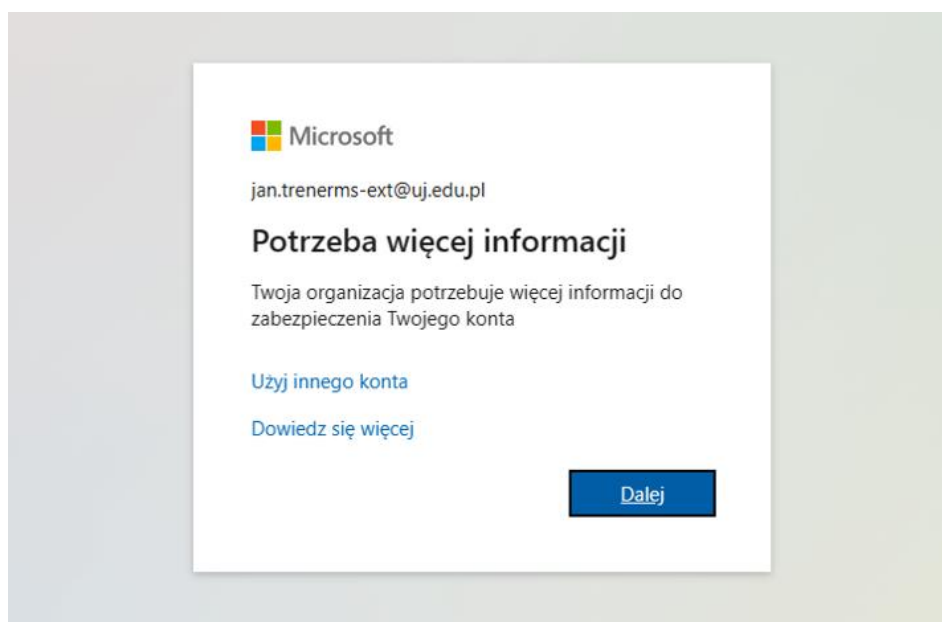
STEP 1 - FIRST LOGIN AFTER ENFORCING DUAL AUTHENTICATION

On the date indicated as the day on which two-factor login is enabled, the first login will require the user to perform additional steps.

When logging in for the first time with an account in the @uj.edu.pl domain (e.g. to the MS Teams application, Outlook, or the <https://portal.office.com> website, a message will be displayed *For security reasons, we require additional information to verify your account*. The user will then be redirected to a page where the process of adding a second authentication component will begin.



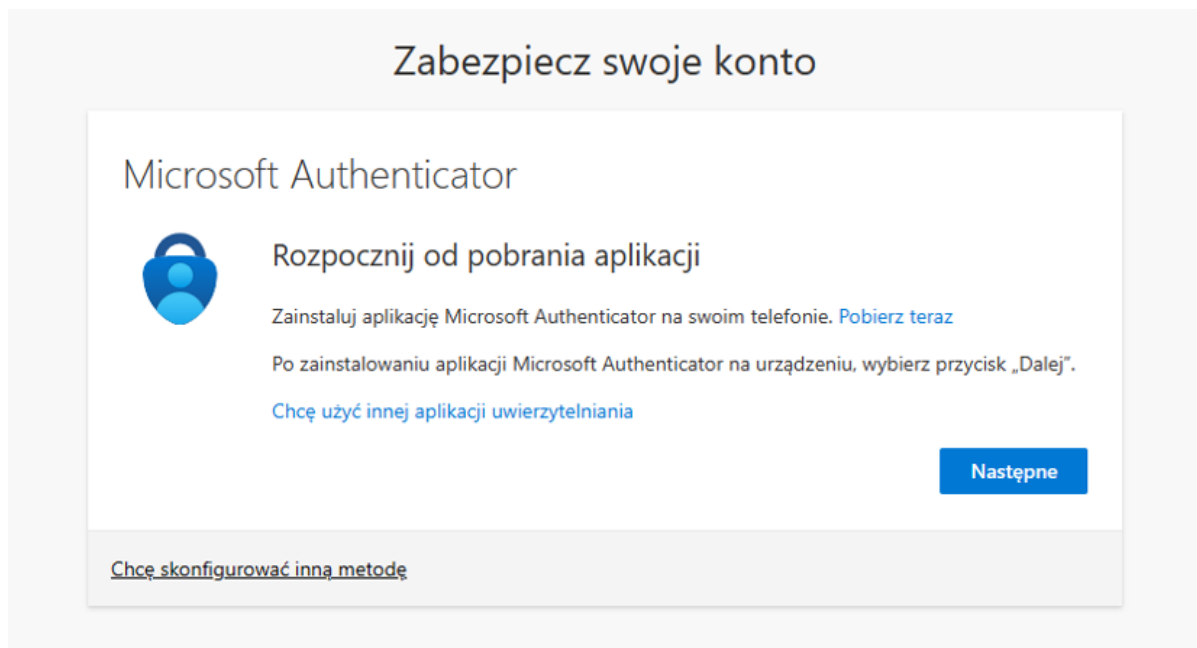
When the page with the message *More information is needed* is displayed, click *Next*.



The *Secure your account* window appears. The Microsoft Authenticator application is prompted as the default second authentication component.

Here you can change to a different authentication application *I want to use a different authentication application* or add an authentication method via a phone number *I want to configure a different method*.

If you choose an app, start by downloading it from the Google Play Store.



STEP 2 - DOWNLOADING THE APPLICATION TO YOUR MOBILE DEVICE

The first step to properly start setting up two-factor login (dual authentication) is to download the **Microsoft** app **Authenticator** 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 *I Agree*.



Twoja prywatność jest ważna

Zbieramy wymagane dane diagnostyczne, aby aplikacja była bezpieczna i aktualna. Nie obejmuje to Twojego nazwiska ani danych poufnych.

Gromadzimy też opcjonalne dane dotyczące użycia, aby poprawić środowisko aplikacji. W dowolnej chwili możesz zrezygnować z udostępniania opcjonalnych danych użycia, przechodząc do ustawień aplikacji.

Zgadzam się

[Zasady zachowania poufności informacji](#)

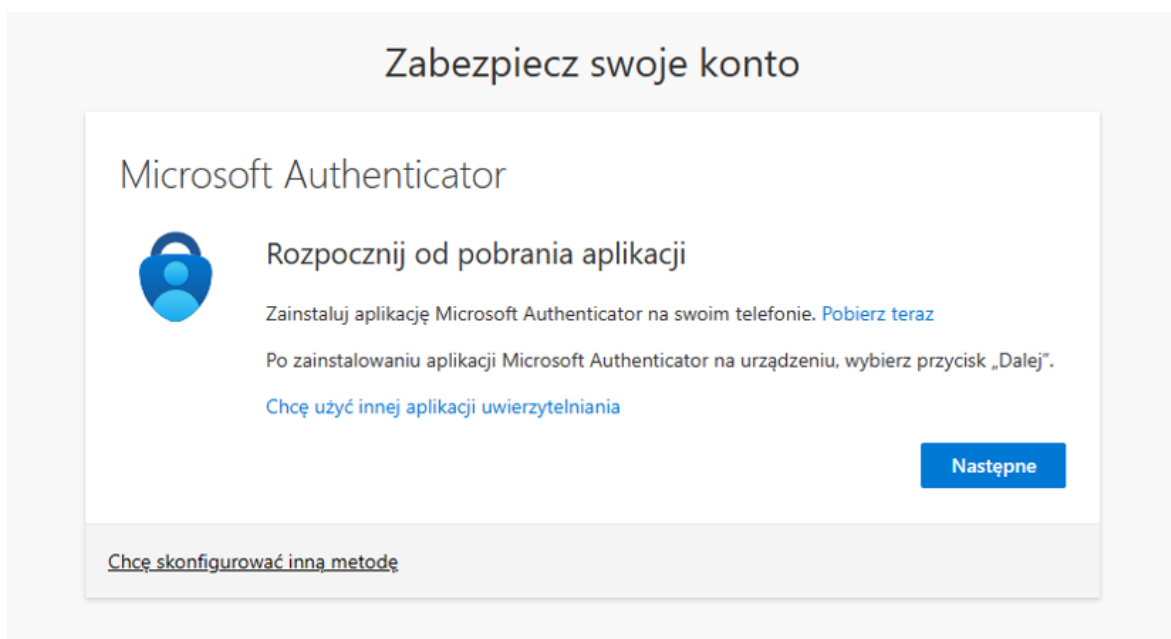
You will then be presented with another screen where it is possible to choose how to connect the application to your university account.

At this point, close the Microsoft Authenticator app on the mobile device and switch to the web browser window on the computer (from step 1)

STEP 3 - ENABLING SECURITY ON THE UJ ACCOUNT

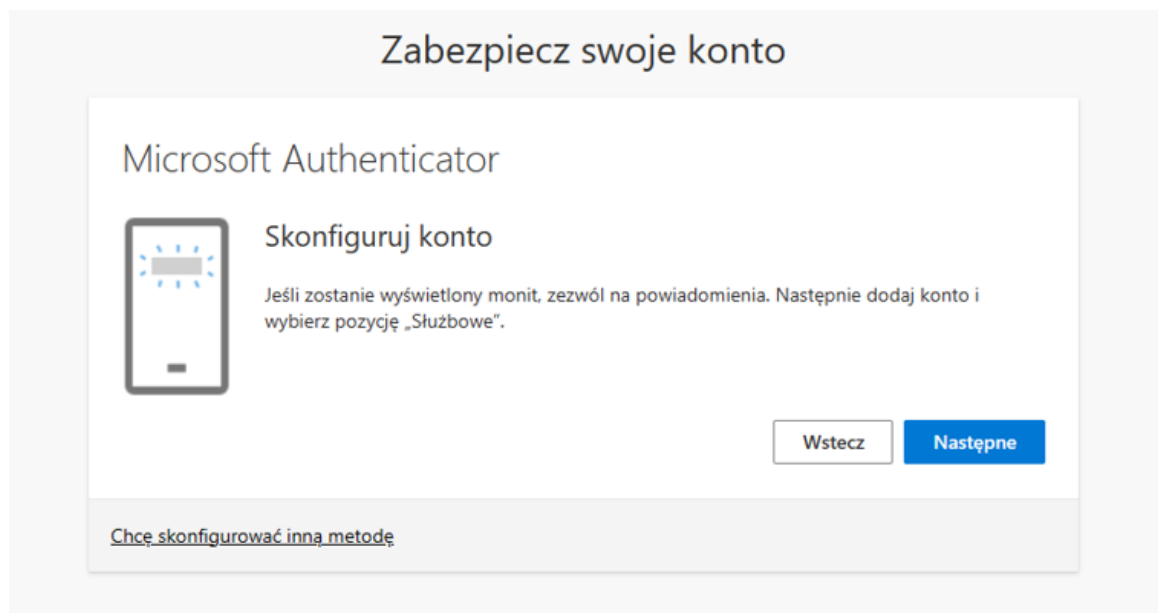
If the application download has been prolonged and the browser window has remained open for a long time, it is advisable to refresh it or close it and try again to log in at <https://www.office.com/>.

After downloading the application, we select the 'Next' button in the 'Secure your account' window.

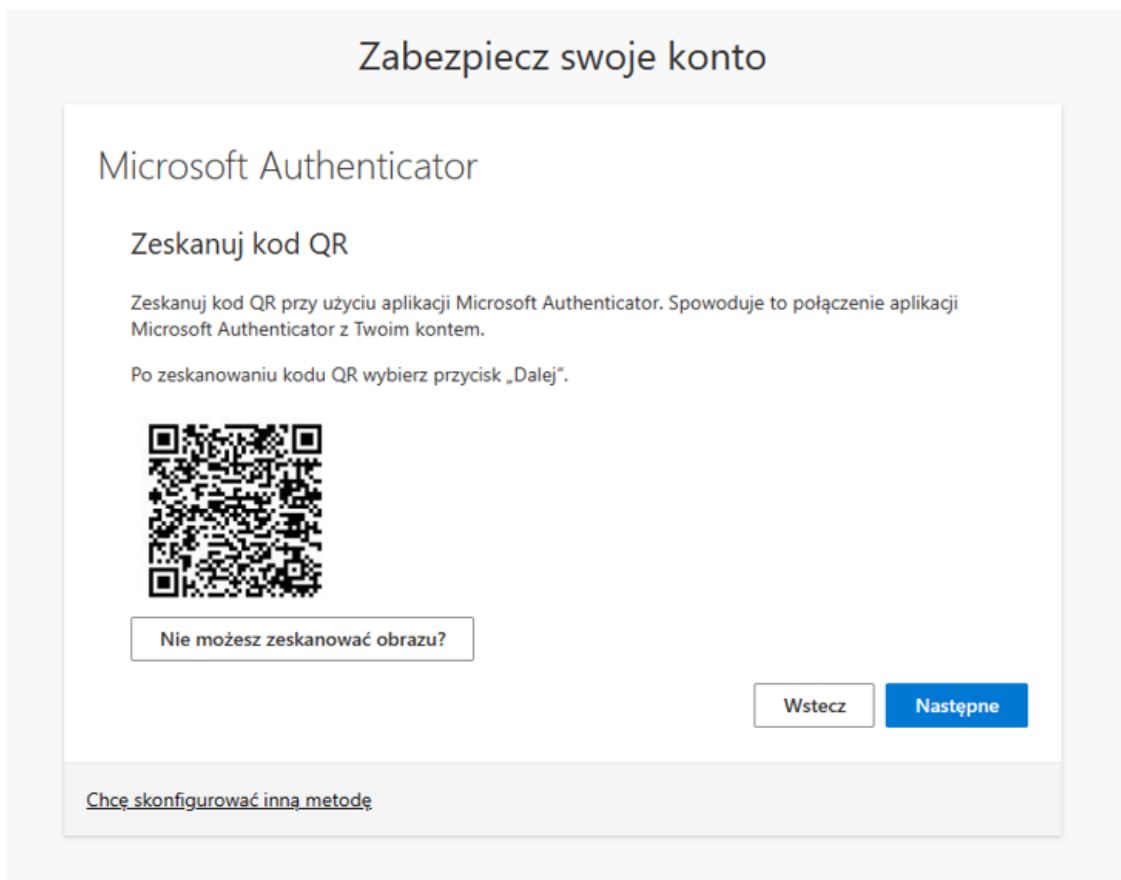


In the next step, also select *Next*.

It is also worth noting the information contained in the account configuration message. If you are prompted in the application on your phone you should allow notifications.



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

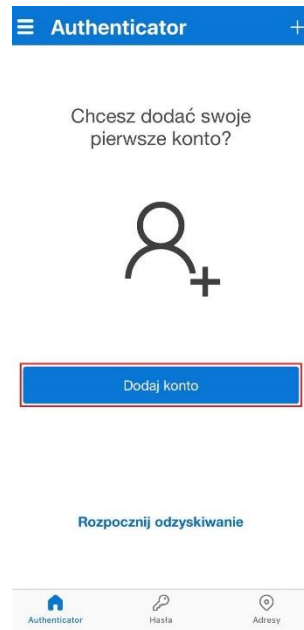


To do this, restart the Microsoft Authenticator app on the mobile device.

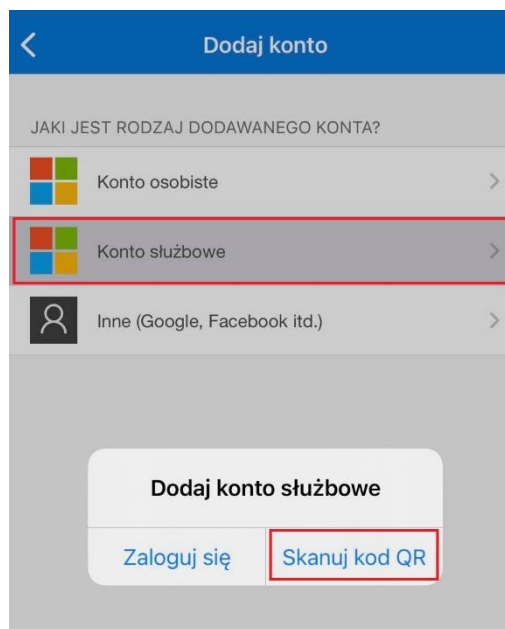
There are two possible scenarios for displaying the information on the user's mobile device.

Variant 1. View adding a new account

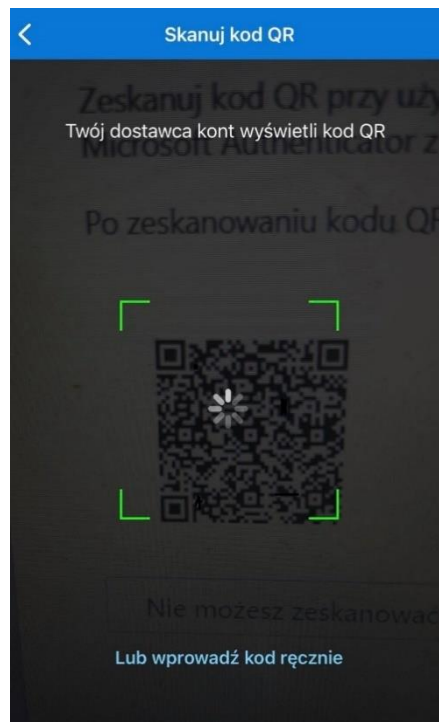
If the following view is displayed, select *Add Account* or select the "+" icon. If the view of the screen is different go to Option 2 described further on.



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

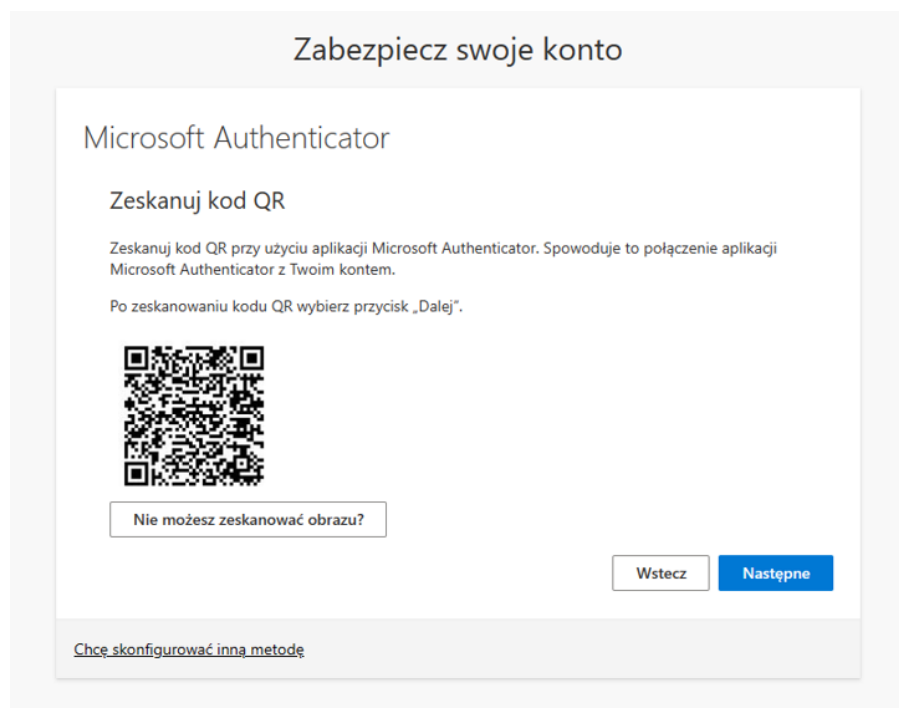


The QR code must be scanned with the phone using the Microsoft Authenticator app.



The message *App lock is enabled* may appear on your device. 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 *Secure Your Account* window previously opened in your web browser and select *Next*.



A two-digit code will be displayed, which must be entered in the app on the phone. Once you have entered the code in the app, select Yes and then confirm in the same way you unlock your phone.

Microsoft Authenticator



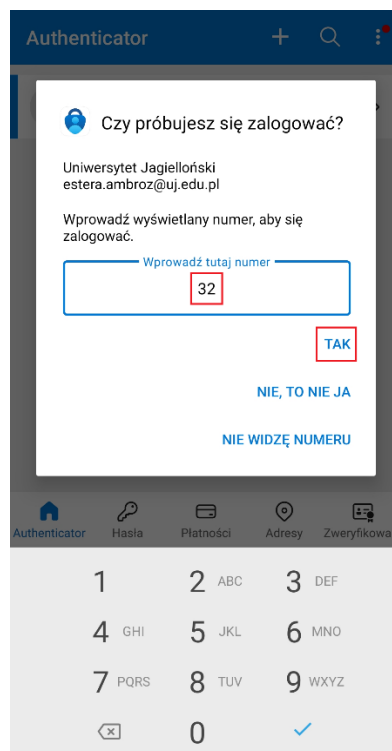
Spróbujmy

Zatwierdź powiadomienie, które wysyłamy do Twojej aplikacji, wprowadzając numer pokazany poniżej.

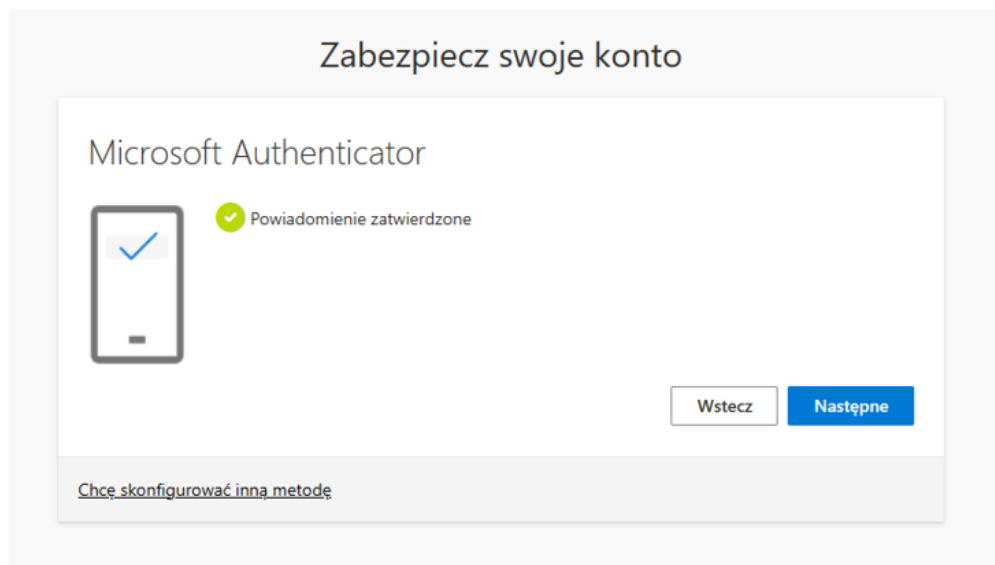
32

Wstecz

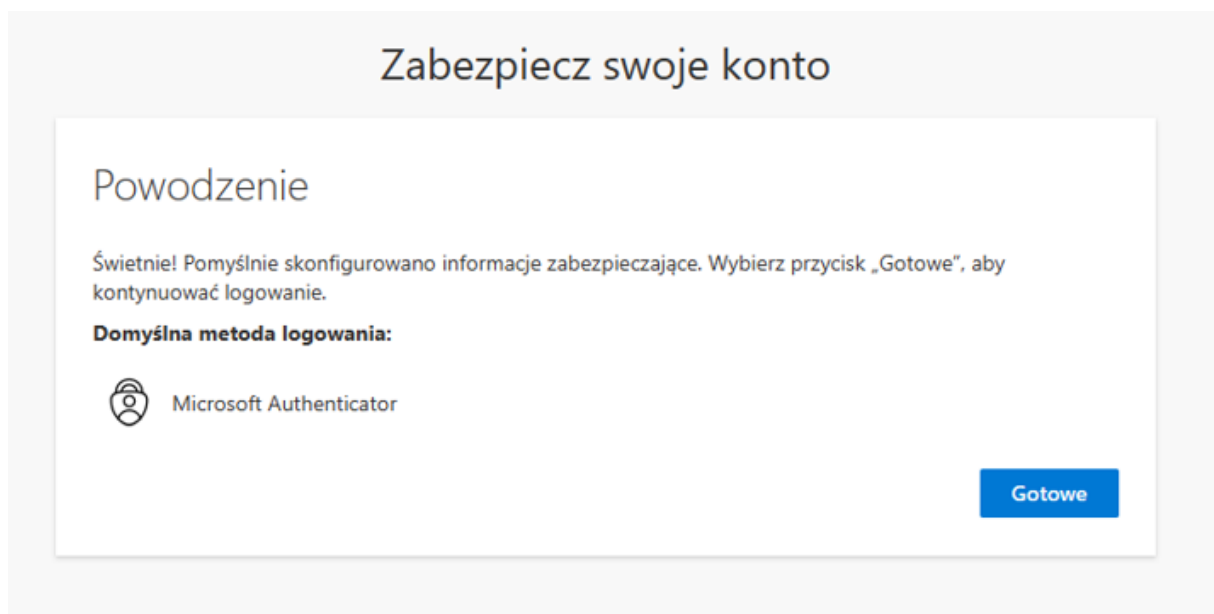
Następne



If everything goes correctly, we should receive a message that the notifications have been approved. In this window, click the "Next" button.

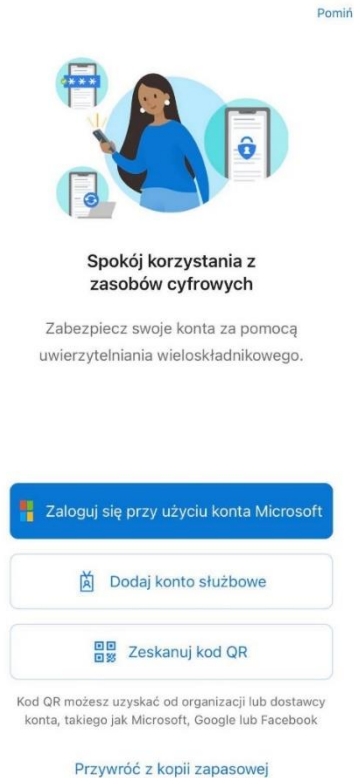


At this point, a message should appear stating that you have successfully added a login method to your account. When you select 'Done', the procedure for adding a second authentication component will be complete.

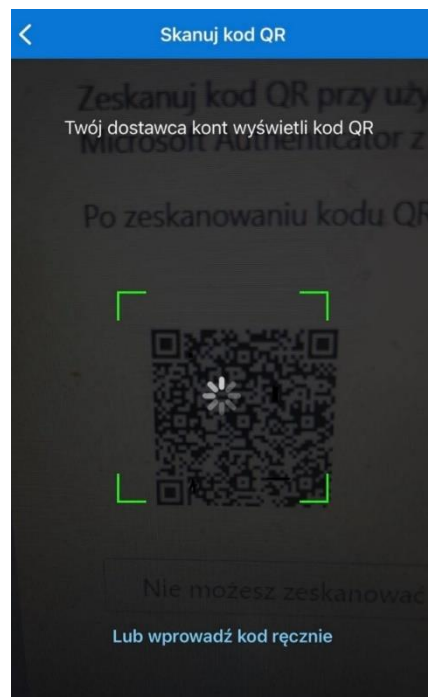


Option 2. Action selection view

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

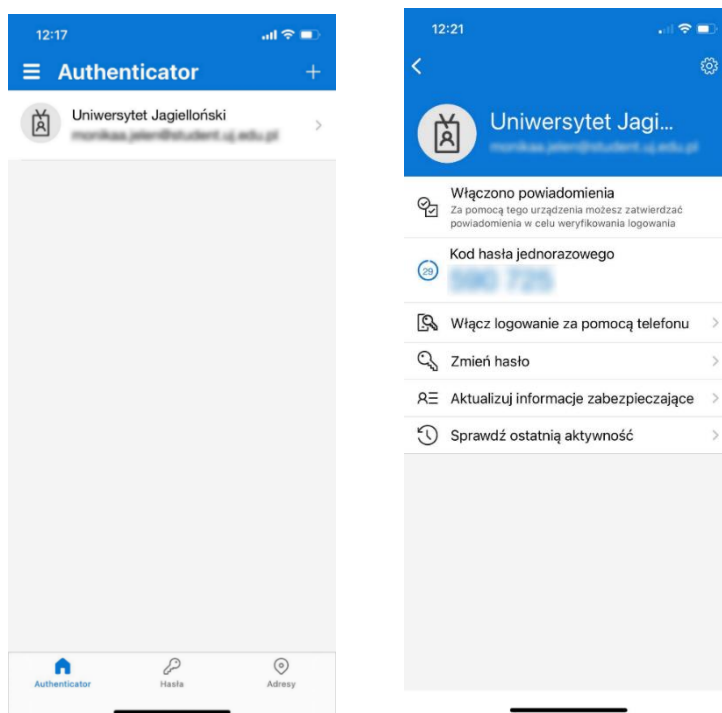


Then scan the QR code displayed on the computer screen in the app.

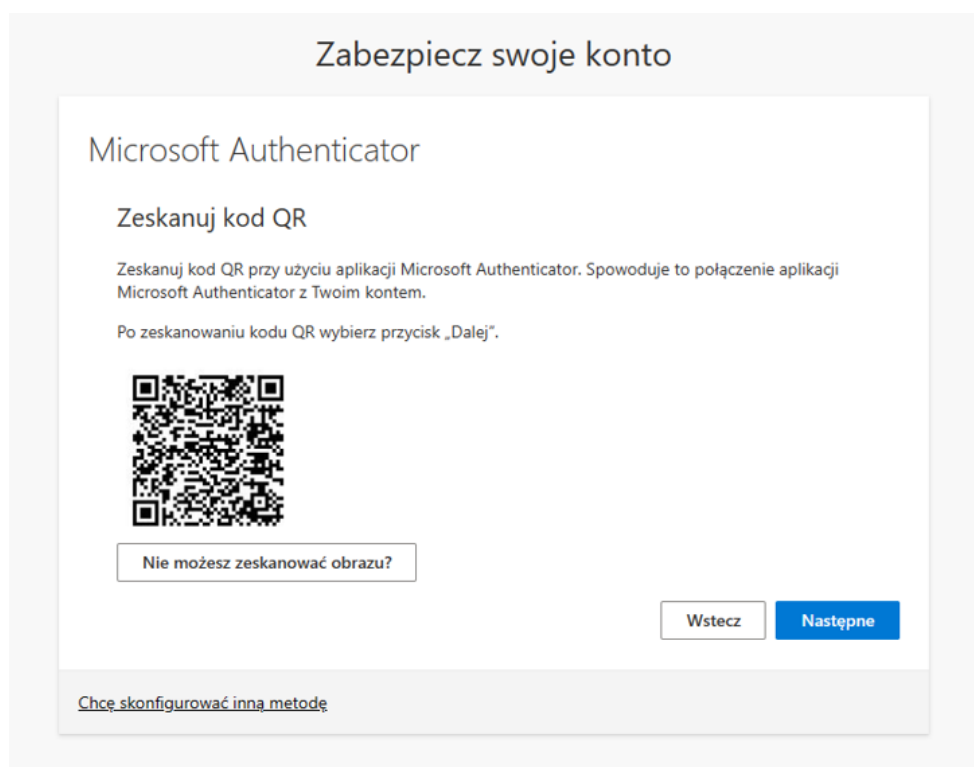


After scanning, the message *Application lock is enabled* appears. *To better protect the Authenticator app, app lock is now enabled by default. To disable it, go to the app settings.* This means that you will need to unlock the app every time before entering it in the same way you unlock your phone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

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



After scanning the QR code, return to the *Secure Your Account* window previously opened in your 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.

Microsoft Authenticator



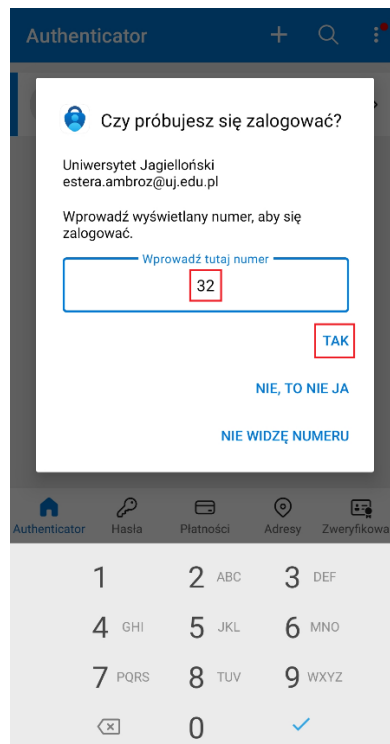
Spróbujmy

Zatwierdź powiadomienie, które wysyłamy do Twojej aplikacji, wprowadzając numer pokazany poniżej.

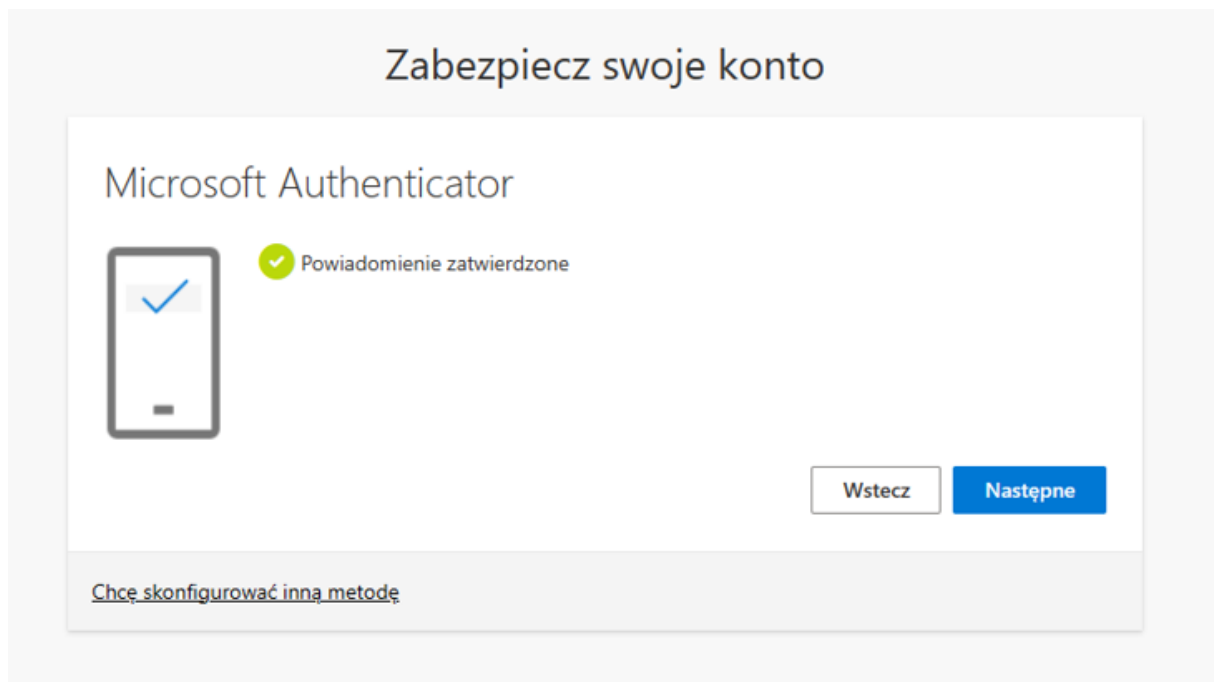
32

Wstecz

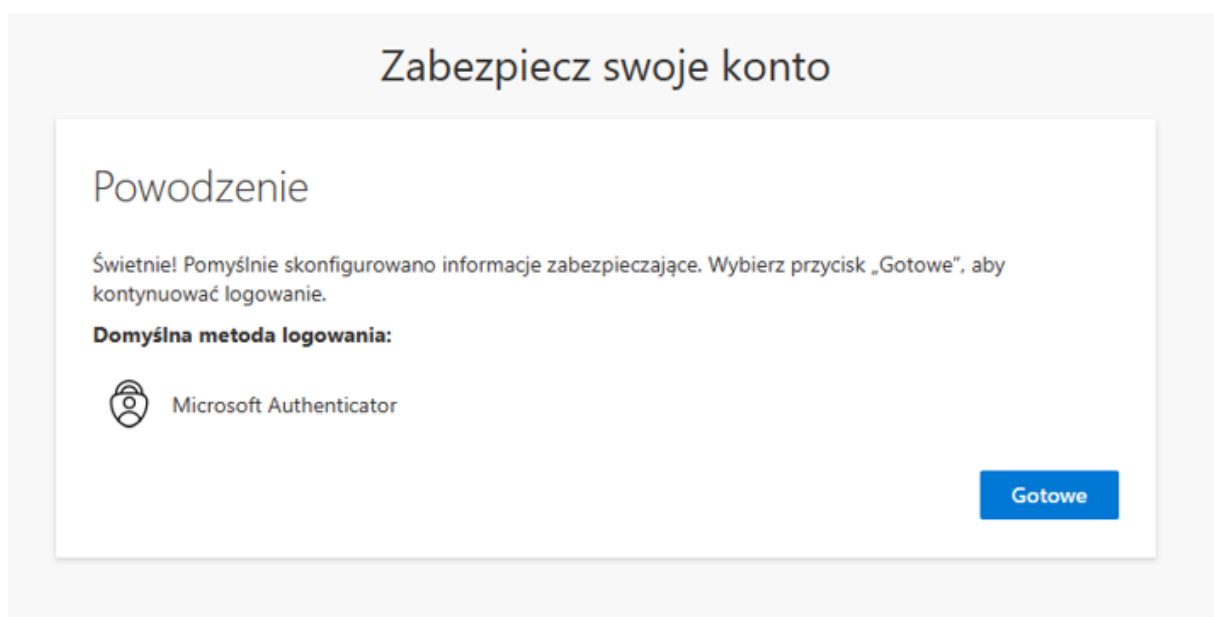
Następne



If everything goes correctly, we should receive a message that the notifications have been approved. In this window, click the "Next" button.

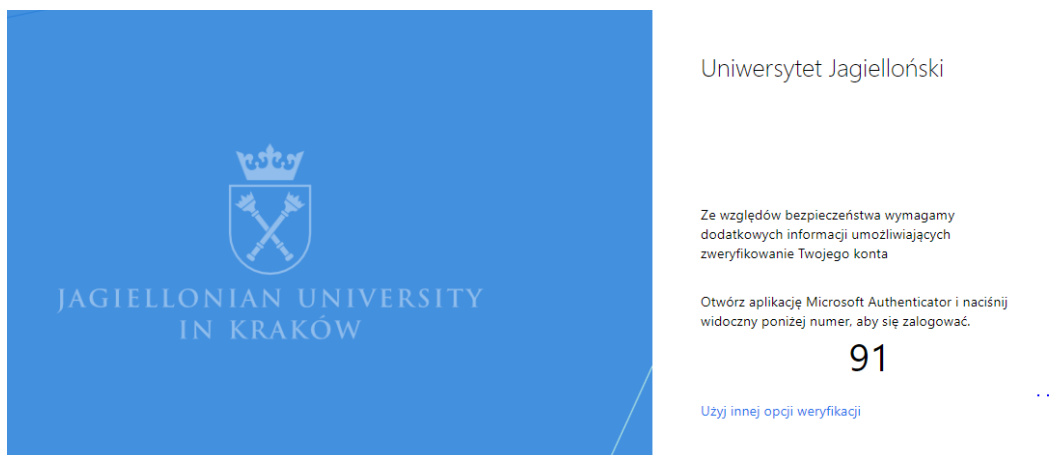


At this point, a message should appear stating that you have successfully added a login method to your account. When you select 'Done', the procedure for adding a second authentication component will be complete.

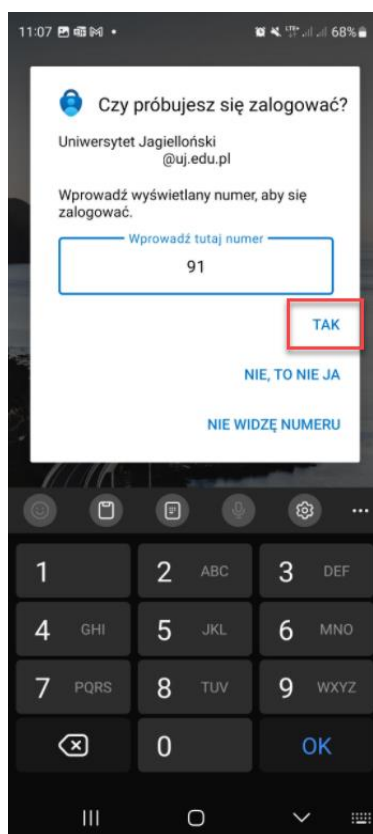


STEP 4 - LOGIN WITH DUAL AUTHENTICATION

For accounts covered by two-factor login, in addition to providing a login ID and password, it is necessary to confirm the login in the MS Authenticator application.



Once the correct login and password have been entered, a screen will appear presenting a two-digit numeric code. At the same time, a notification will appear on your mobile device with the MS Authenticator app, asking you to confirm your login in the app.



After entering a code identical to the one presented on the screen when logging in, click YES and confirm the log-in with the lock screen code/pattern or fingerprint.

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.

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 UJ 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.