

Logowanie dwuskładnikowe (2FA) - APLIKACJA

Instrukcja konfiguracji logowania dwuetapowego (2FA) w usługach Microsoft z wykorzystaniem aplikacji Microsoft Authenticator (zalecana metoda).
Po włączeniu zabezpieczenia logowanie wymaga potwierdzenia w aplikacji mobilnej.

Przewidywany czas: 5-10 minut

Poziom trudności: średnia

Dostępność: publiczna

Ostatnia aktualizacja: 07.05.2026

Ta instrukcja opisuje konfigurację logowania dwuetapowego (2FA) z wykorzystaniem aplikacji Microsoft Authenticator.
Jeśli chcesz skorzystać z weryfikacji za pomocą telefonu (SMS lub połączenie), przejdź do instrukcji dotyczącej tej metody.

Instrukcja

- 1 Zaloguj się do konta Microsoft, wpisując login oraz hasło.



The screenshot shows a login interface for the University of Medicine in Białymstok. At the top left is the university's logo, a green tree inside a circle, with the text "UNIWERSYTET MEDYCZNY W BIAŁYMSTOKU" to its right. Below the logo is a back arrow and the email address "jerzy.romanowski@umb.edu.pl". The main heading is "Enter password". Below this is a password input field with ten black dots and a vertical cursor on the right. Underneath the password field is a link that says "Forgot my password". To the right of the password field is a blue rectangular button with the text "Sign in". At the bottom of the page, there is a grey footer bar with the text "Uniwersytet Medyczny w Białymstoku."

2 Dodatkowe zabezpieczenie konta

Po wprowadzeniu hasła pojawi się komunikat:

„Potrzeba więcej informacji”

z informacją, że organizacja wymaga dodatkowego zabezpieczenia konta.

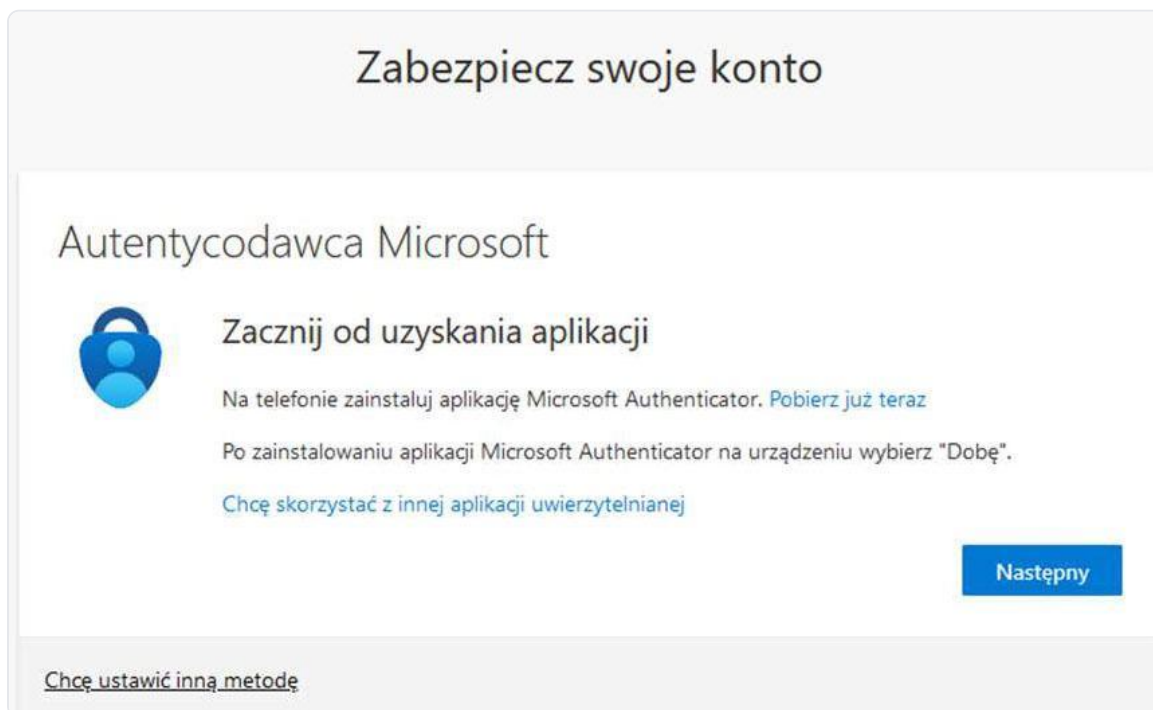
Aby kontynuować:

- kliknij przycisk **„Dalej”**,
- przejdź do kolejnego etapu konfiguracji zabezpieczeń.



3 Powinien pojawić się komunikat dotyczący zabezpieczenia konta.

Wybierz opcję „Pobierz już teraz”, aby rozpocząć konfigurację dodatkowego zabezpieczenia.



4 Instalacja aplikacji Microsoft Authenticator



Po przejściu dalej zostanie wyświetlona strona z dwoma kodami QR.



W zależności od systemu operacyjnego telefonu (Android lub iOS):

- zeskanuj odpowiedni kod QR przypisany do Twojego urządzenia **lub**
- otwórz na telefonie **Sklep Play** (Android) albo **App Store** (iOS) i wyszukaj aplikację **Microsoft Authenticator**, a następnie ją zainstaluj.

Get the app on your phone

Scan the QR code with your Android or IOS mobile device.



Google Play
[Get the app](#)



App Store
[Get the app](#)

Wyszukując aplikację ręcznie, upewnij się, że pobierasz właściwą aplikację Microsoft Authenticator (wydawca: Microsoft).

Zwróć uwagę na ikonę aplikacji przedstawioną poniżej.

5 Po uruchomieniu aplikacji wybierz opcję „Dodaj konto”.



Chcesz dodać swoje pierwsze konto?

W tym miejscu pojawi się dowolne konto Microsoft lub inny typ dodanego konta.

[Dodaj konto](#)

Masz już kopię zapasową?
Przywróć konto.

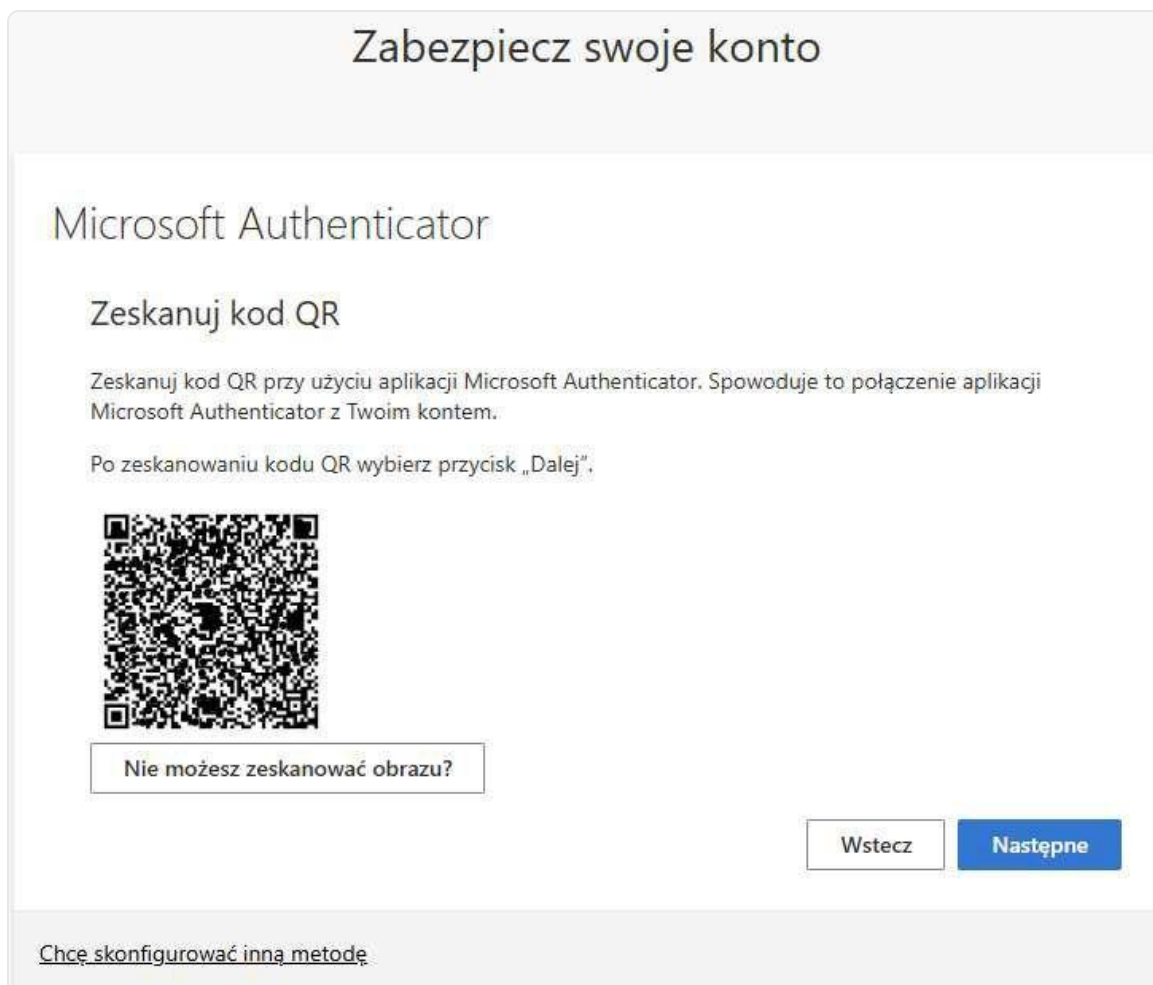
[Rozpocznij odzyskiwanie](#)

6 Dodanie konta służbowego w aplikacji

W aplikacji Microsoft Authenticator wybierz „**Dodaj konto służbowe**”.

7 W aplikacji Microsoft Authenticator wybierz opcję „Zeskanuj kod QR”.

Następnie skieruj aparat telefonu na kod QR wyświetlony na ekranie komputera i zeskanuj go.



8 Po zeskanowaniu kodu QR i przejściu dalej nastąpi próba weryfikacji.

Na ekranie komputera w przeglądarce zostanie wyświetlona liczba. Wprowadź tę samą liczbę w aplikacji Microsoft Authenticator na telefonie, aby potwierdzić logowanie.



Operację potwierdź, wybierając przycisk „Tak” w aplikacji.

Następnie na ekranie komputera kliknij „Następnie”, aby przejść do kolejnego kroku.

9 Po zatwierdzeniu hasła przyciskiem „Następnie” nasze konto jest zabezpieczone

