

Instrukcja konfiguracji MFA - dla dotychczasowych użytkowników kont w domenie UEW

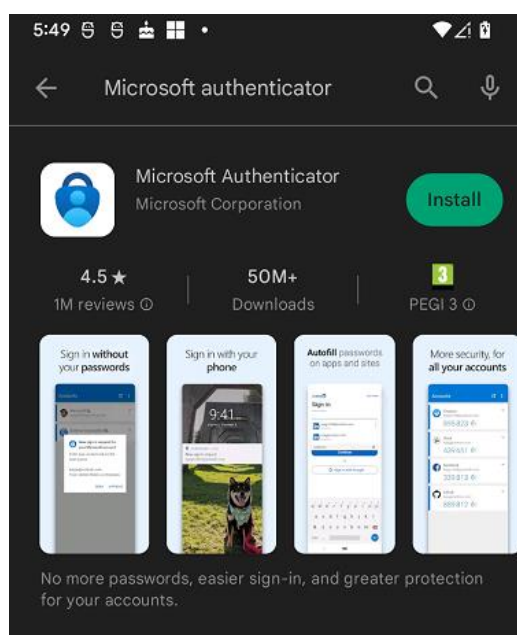
Krok 1: Włączenie MFA z poziomu konta

1. Zaloguj się na <https://myaccount.microsoft.com>
2. Przejdź do sekcji **Security info (Informacje zabezpieczeń)**
3. Kliknij **Add method (Dodaj metodę logowania)** > z rozwiniętej listy wybierz Microsoft Authenticator
4. Postępuj zgodnie z instrukcjami na ekranie.

Krok 2: Pobierz aplikację

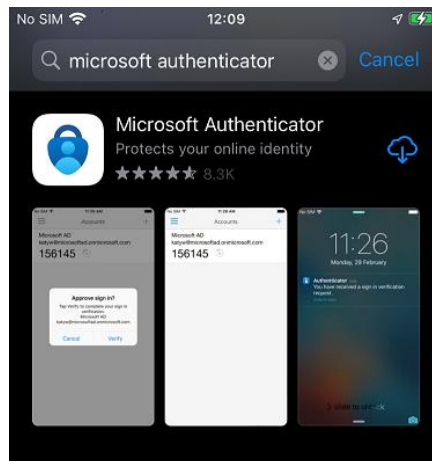
Android:

Na służbowym lub prywatnym urządzeniu mobilnym należy pobrać aplikację ze sklepu Google Play, wpisując "Microsoft Authenticator".

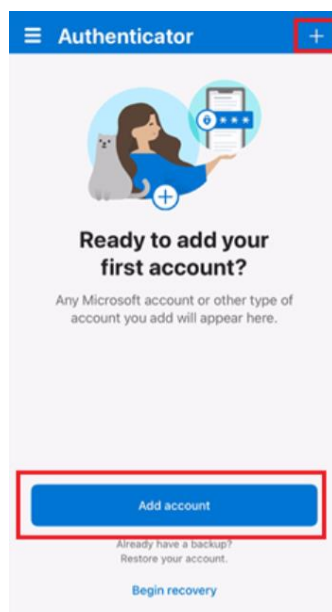


iOS oraz iPadOS:

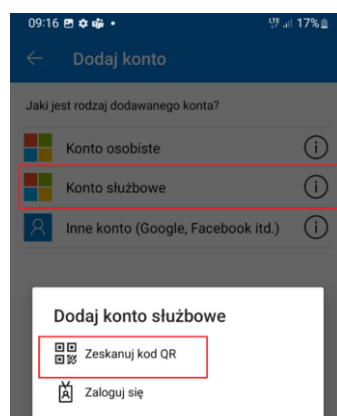
Na służbowym lub prywatnym urządzeniu mobilnym aplikację Microsoft Authenticator należy pobrać z Apple App Store.



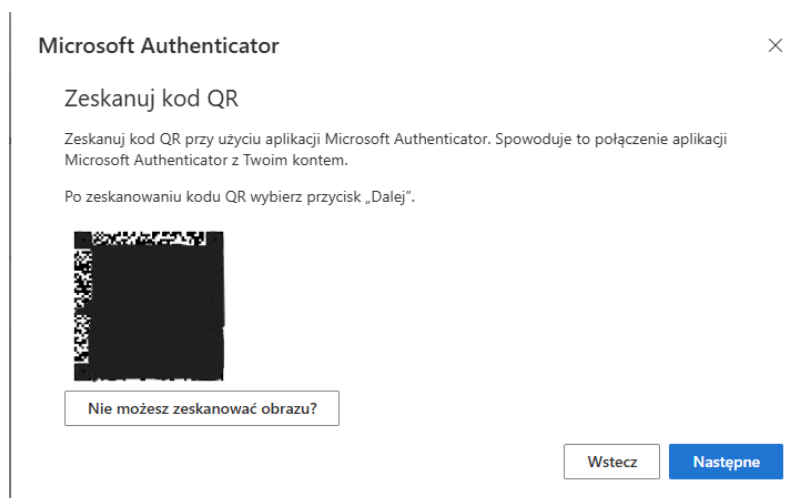
Po instalacji aplikacji otwórz ją na urządzeniu mobilnym i kliknij ikonę „+” → **Dodaj konto**.



Wybierz **Konto służbowe** → **Skanuj kod QR**.



Teraz wróć do komputera i zeskanuj wyświetlony kod urządzeniem mobilnym z aplikacją Microsoft Authenticator i kliknij „**Następne**”.



W przeglądarce zostanie wyświetlony dwucyfrowy kod, który należy wprowadzić w aplikacji Microsoft Authenticator na urządzeniu mobilnym.

Krok 3: Test logowania z MFA

1. Wyloguj się z konta służbowego UEW.
2. Zaloguj się ponownie — po wpisaniu hasła powinien pojawić się kod dwucyfrowy, który należy przepisać do aplikacji.
3. Potwierdź tożsamość aplikacją.

Krok 4: Dodatkowe rekomendacje

-  Skonfiguruj kopię zapasową MFA (np. drugi numer telefonu). Instrukcja: Dodanie numeru telefonu jako dodatkowego składnika logowania do konta MS365
-  W przypadku utraty dostępu, kradzieży urządzenia MFA lub udostępnienia go osobom nieuprawnionym, należy zgłosić ten przypadek do Działu Wsparcia IT oraz mailowo na skrzynkę incydent@ue.wroc.pl, zgodnie z Regulaminem stosowania uwierzytelnienia wieloskładnikowego MFA w UEW.