

INSTRUKCJA PIERWSZEJ KONFIGURACJI MFA

Spis treści

Cel dokumentu	3
Dostępne metody uwierzytelniania	3
Konfiguracja metody uwierzytelniania przy użyciu aplikacji Microsoft Authenticator.....	3
Konfiguracja metody uwierzytelniania przy użyciu aplikacji Google Authenticator.....	5

Cel dokumentu

Celem dokumentu jest poinstruowanie użytkownika w jaki sposób skonfigurować uwierzytelnianie dwuetapowe.

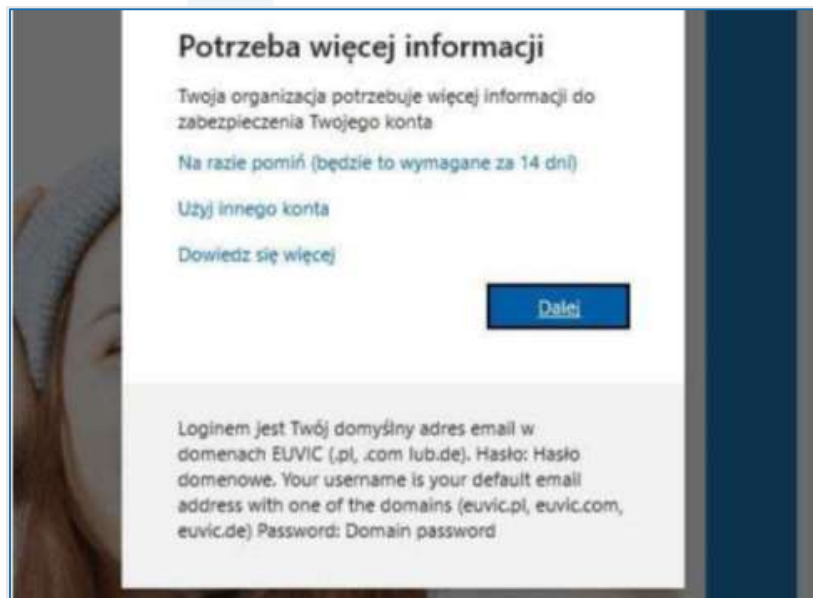
Dostępne metody uwierzytelniania

Obecnie w organizacji Euvic jedyną metodą weryfikacji logowania dwuetapowego jest potwierdzenie logowania za pomocą dedykowanej aplikacji. Zalecamy do korzystania z aplikacji Microsoft Authenticator lub Google Authenticator dla których przygotowaliśmy tą instrukcję.

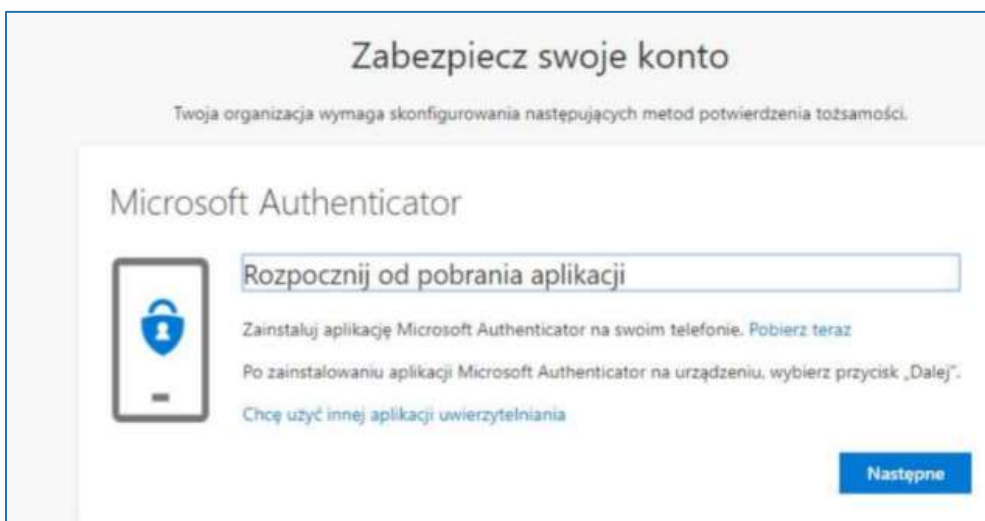
Konfiguracja metody uwierzytelniania przy użyciu aplikacji

Microsoft Authenticator

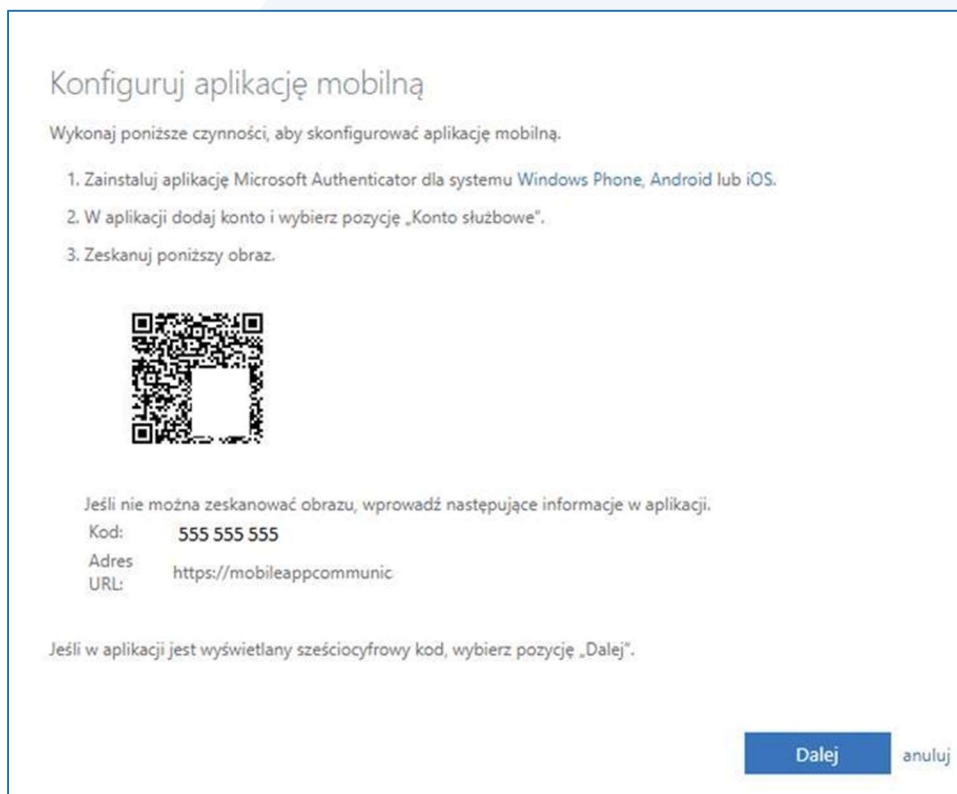
1. Podczas próby pierwszego logowania do konta lub po restarcie ustawień MFA wyświetli się następujący komunikat. Należy wybrać przycisk „Dalej” w przypadku chęci konfiguracji uwierzytelniania przy użyciu aplikacji.



2. Po wybraniu opcji „Dalej” zostanie wyświetlony komunikat informujący o możliwości skonfigurowania metody uwierzytelniania za pomocą aplikacji Microsoft Authenticator lub innej aplikacji uwierzytelniania (np. Google Authenticator).

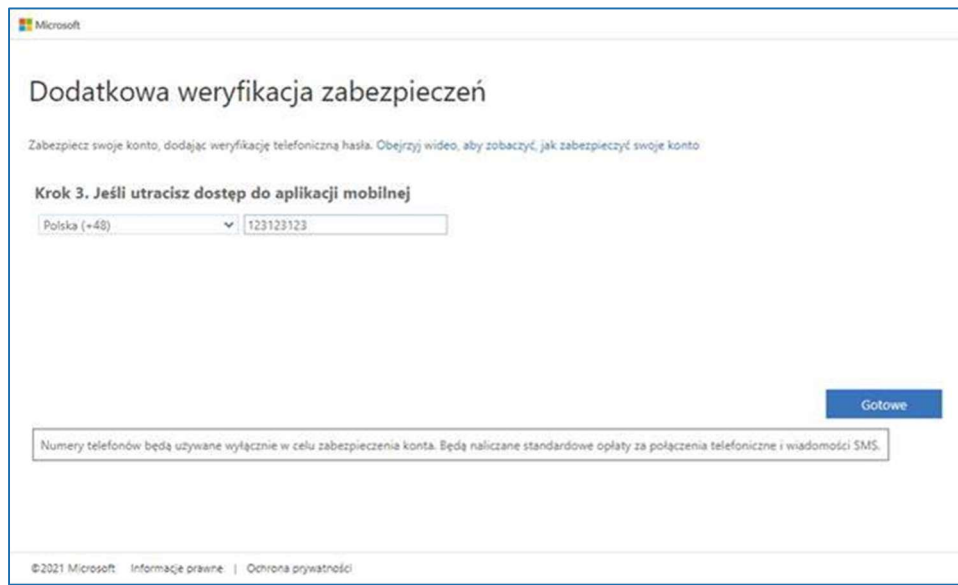


3. Należy wybrać przycisk „Następne”. Zostanie wyświetlony następujący ekran:



4. Należy pobrać i zainstalować aplikację Microsoft Authenticator na urządzeniu mobilnym
5. W aplikacji należy dodać konto i wybrać pozycję „Konto służbowe”
6. Aparatem urządzenia mobilnego należy zeskanować kod QR wyświetlony na ekranie w punkcie 4. Alternatywną opcją jest przepisanie kodu wyświetlonego pod kodem QR.

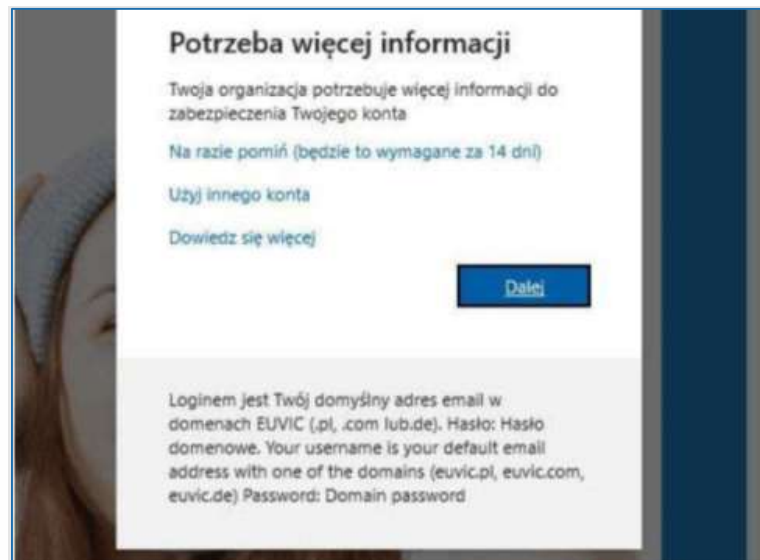
- Wyświetlenie się na telefonie 6-cyfrowego kodu oznacza powodzenie dodania konta do aplikacji. Należy wybrać przycisk „Dalej” na ekranie z kodem QR.
- W przeglądarce zostanie wyświetlony następujący ekran. Należy podać swój numer telefonu, aby było możliwe zweryfikowanie tożsamości w przypadku utraty dostępu do aplikacji mobilnej. Następnie należy wybrać przycisk „Gotowe”.



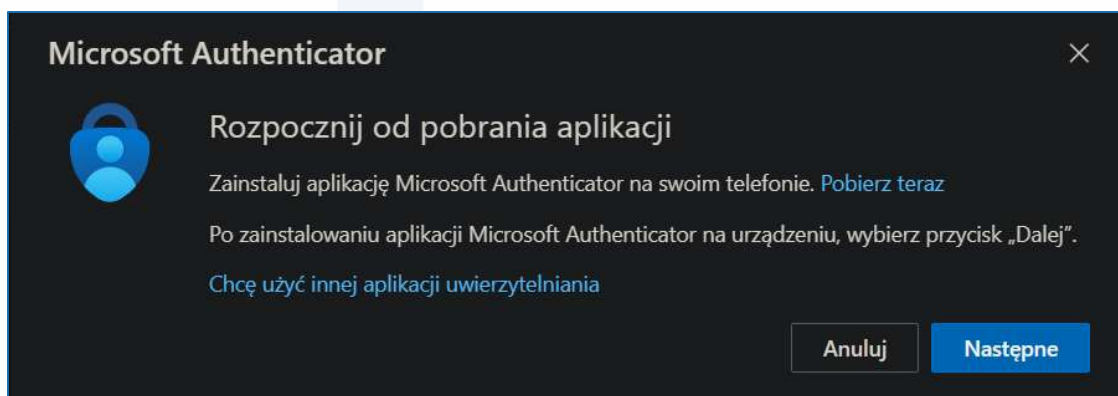
- Po kliknięciu 'Gotowe' konfiguracja jest zakończona i pojawi się podsumowanie skonfigurowanych parametrów.
Okno przeglądarki może zostać zamknięte.

Konfiguracja metody uwierzytelnienia przy użyciu aplikacji Google Authenticator

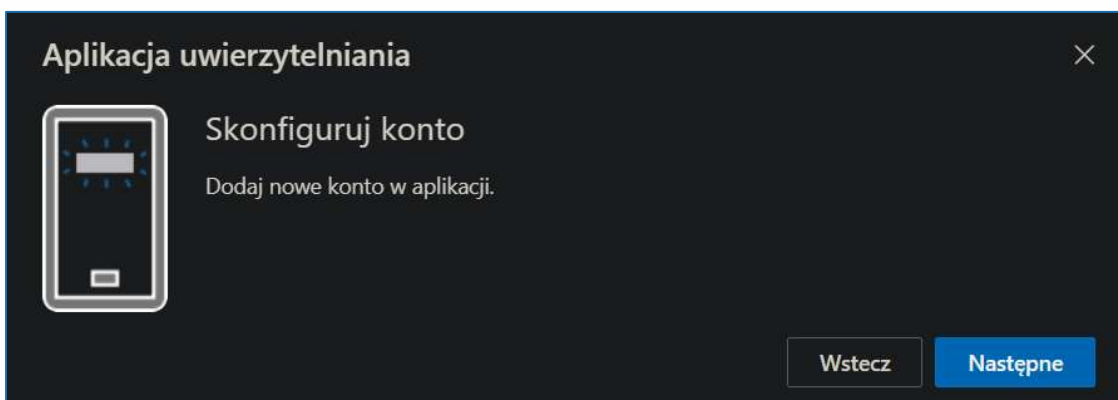
- Podczas próby pierwszego logowania do konta lub po restarcie ustawień MFA wyświetli się następujący komunikat. Należy wybrać przycisk „Dalej” w przypadku chęci konfiguracji uwierzytelniania przy użyciu aplikacji.



2. Po wybraniu opcji „Dalej” zostanie wyświetlony komunikat informujący o możliwości skonfigurowania metody uwierzytelniania za pomocą aplikacji Microsoft Authenticator lub innej aplikacji uwierzytelniania (np. Google Authenticator). Należy wybrać przycisk „Chcę użyć innej aplikacji uwierzytelniania”.

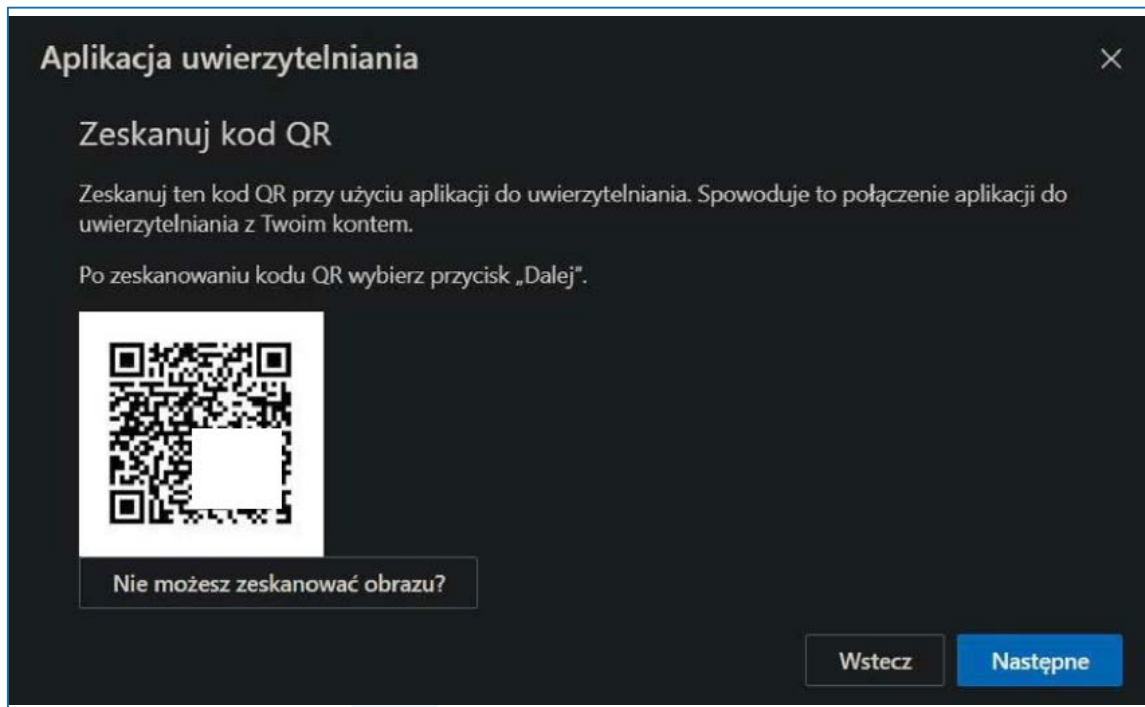


3. Zostanie wyświetlone następujące okno. Należy wybrać przycisk „Następne”



IT Works

4. Zostanie wyświetlone następujące okno



5. Należy pobrać i zainstalować aplikację Google Authenticator na urządzeniu mobilnym
6. **W aplikacji nie należy się logować kontem służbowym**, należy wybrać opcję „Używaj bez logowania”
7. Zostanie wyświetlone okno z przyciskami „Dodaj kod” oraz „Zaloguj się”. Należy kliknąć do „Dodaj kod” a następnie „Zeskanuj kod QR”
8. Zostanie uruchomiona kamera w telefonie, którą należy zeskanować kod z ekranu (zrzut ekranu w pkt 4.)
9. Po zeskanowaniu kodu należy kliknąć „Następne”
10. Na telefonie zostanie wyświetlony 6-cyfrowy kod, który należy przepisać do nowego okna, które zostało wyświetlone na komputerze.
11. Okno przeglądarki może zostać zamknięte.