

Instrukcja konfiguracji uwierzelniania wieloczynnikowego (MFA)

Stan Nowy Jork rozpoczął stosowanie uwierzelniania wieloczynnikowego (MFA) w niektórych swoich aplikacjach publicznych. MFA to sposób, który pomaga zapewnić bezpieczeństwo i ochronę Twojego konta. Wymaga to drugiego czynnika udowadniającego (poza samym hasłem), że jesteś tym, za kogo się podajesz. Jeśli korzystasz z aplikacji chronionej MFA, nawet jeśli ktoś odgadnie lub ukradnie Twoje hasło, nadal nie będzie mógł się zalogować bez Twojego drugiego czynnika. Podczas gdy hasło to coś, co znasz, drugi czynnik to coś, czym jesteś (zwykle odczytywane przez urządzenie biometryczne) lub coś, co masz.

Porada: Zaleca się skonfigurowanie więcej niż jednej metody uwierzelniania wieloczynnikowego.

Porada: Jeśli będziesz konfigurował metodę uwierzelniania wieloczynnikowego, która wykorzystuje aplikację na telefon (Okta Verify lub Google Authenticator), pobierz aplikację przed kliknięciem przycisku Setup/Konfiguruj na stronie przeglądarki „Set up multifactor authentication/Konfiguruj uwierzelnianie wieloczynnikowe”. Dwie metody uwierzelniania wieloczynnikowego, które wykorzystują aplikacje, to Okta Verify i Google Authenticator. Aby pobrać aplikację już teraz, [kliknij tutaj dla urządzeń z systemem Android](#), a [tutaj dla urządzeń Apple](#).

UWAGA: Wszystkie zrzuty ekranu pochodzą z monitora komputera, chyba że zostały zrobione za pomocą telefonu komórkowego.

Indeks

[Konfiguracja Google Authenticator Uwierzelnianie wieloetapowe](#)

[Pobieranie Google Authenticator dla urządzeń z systemem Android](#)

[Pobieranie Google Authenticator dla urządzeń Apple](#)

[Korzystanie z aplikacji](#)

[Wskazówki dotyczące wprowadzania klucza konfiguracji](#)

[Wskazówki dotyczące skanowania kodu QR](#)

[Potencjalne komunikaty o błędach](#)

Konfiguracja uwierzytelniania wieloczynnikowego przez Google Authenticator

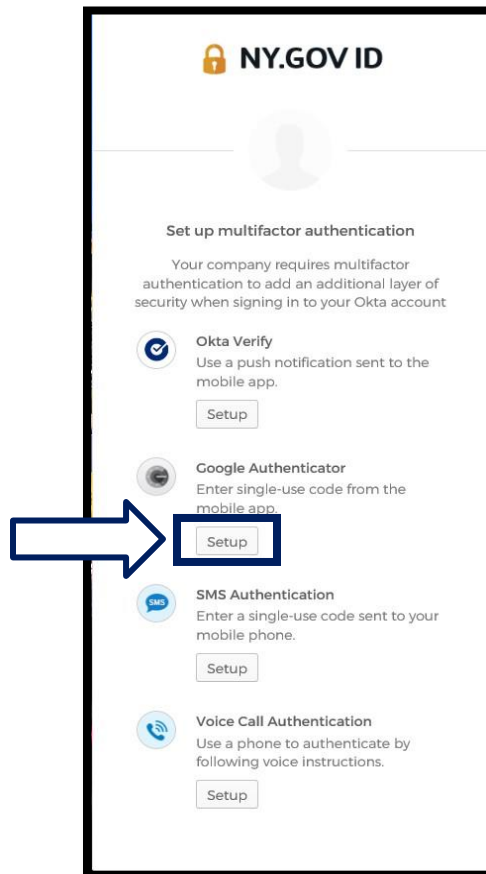
Jeśli nie jesteś jeszcze zapisany do MFA, zostaniesz poproszony o zapisanie się po zalogowaniu się do Labor Online Services i kliknięciu przycisku „Unemployment Services/Usługi dla osób bezrobotnych”.

The screenshot shows the user interface of the New York State Department of Labor's online services. The layout is as follows:

- Messages:** A notification box stating "You have no messages." with a "Go to My Inbox" button.
- Online Forms:** A section indicating "You have 0 pending forms" and listing available forms for filing: Unemployment Insurance Forms, Labor Standards Forms, and 15-day Child Performer Permit Application. It includes a "Go To My Online Forms" button.
- Most Recent Postings:** A yellow warning banner stating "Previewing jobs has been temporarily disabled. Please visit JobZone to view jobs" and a "Search More Jobs" button.
- Important Information:** A list of links including "You may not be eligible for benefits when outside the United States...", "Beware of text messages, email and phone scams", "Beware of companies charging...", "Verify receipt of benefits...", "Work Search Requirements", and "Resources for Families".
- Job Search:** A section with the text "Manage your career, organize your job search, and plan for the future with JobZone" and "Choose the Job Zone button for:" followed by a list: Job Search, Online Work Search Record, and Employability Scoring and other Job Search tools. It features a "JobZone" button.
- Unemployment Insurance:** A section with a "Services" list: File a Claim, Claim Weekly Benefits, View Payment History, Direct Deposit, View / Print 1099-Gs, and Change Tax Withholding. Below this is a "Tools" section with a "Work Search Record" button. A blue arrow points to the "Unemployment Services" button, which is highlighted with a blue box.

Na ekranie komputera pojawi się ekran z prośbą o skonfigurowanie uwierzytelniania wieloczynnikowego.

1. Na swoim smartfonie pobierz aplikację Google Authenticator.
2. Na ekranie komputera kliknij opcję Setup/Konfiguracja w obszarze Google Authenticator, aby rozpocząć proces konfiguracji.



3. Na monitorze komputera otworzy się nowy ekran. Wybierz iPhone lub Android w zależności od urządzenia. Jeśli masz tablet Apple, wybierz iPhone.

Jeśli masz urządzenie z systemem Android, zobaczysz:



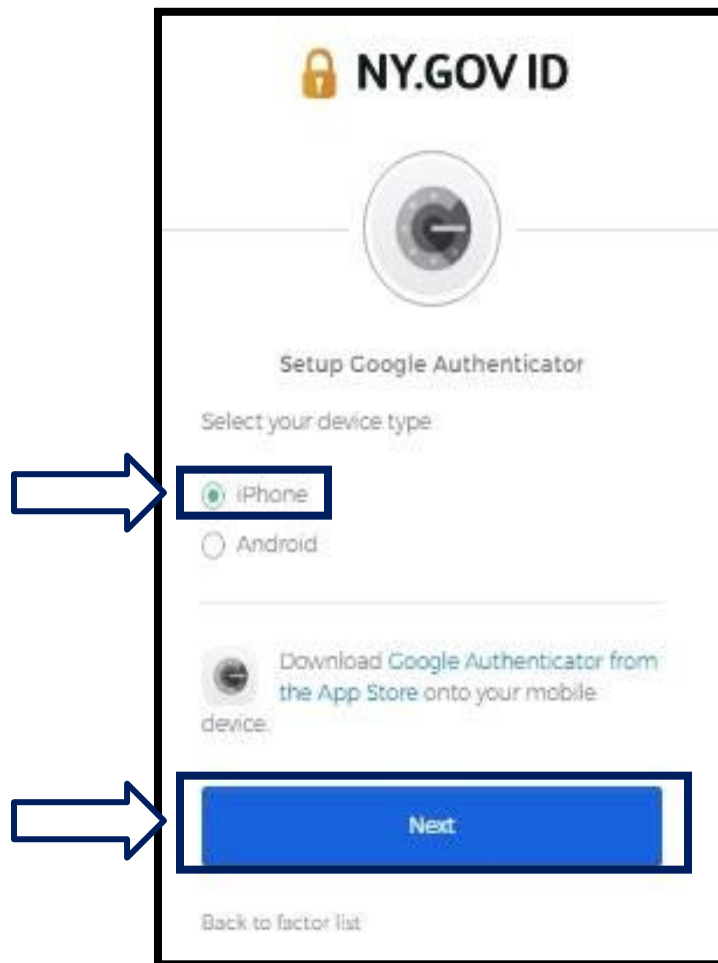
Zostaniesz poinstruowany, aby pobrać aplikację Google Authenticator ze sklepu Google Play. Jeśli jeszcze tego nie zrobiłeś, powinieneś pobrać tę aplikację już teraz.

[Kliknij tutaj, aby uzyskać wskazówki, jak pobrać aplikację Google Authenticator na urządzenie z systemem Android.](#)

4. Kliknij przycisk Next/Dalej.

[Kliknij tutaj, aby kontynuować.](#)

Jeśli masz urządzenie iPhone, zobaczysz:



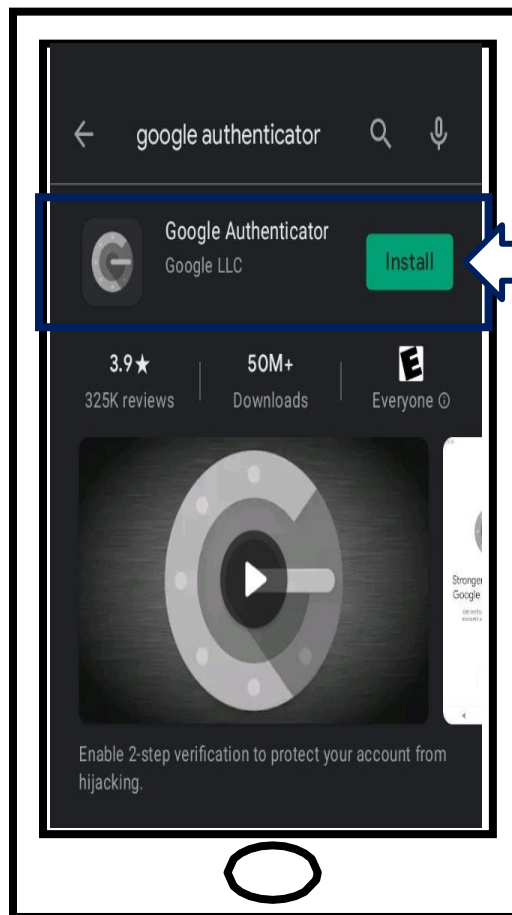
Zostaniesz poinstruowany, aby pobrać aplikację Google Authenticator ze sklepu App Store. Jeśli jeszcze tego nie zrobiłeś, powinieneś pobrać tę aplikację już teraz.

[Kliknij tutaj, aby uzyskać wskazówki, jak pobrać aplikację Google Authenticator na urządzenie Apple.](#)

5. Kliknij przycisk Next/Dalej.

Wskazówki dotyczące pobierania aplikacji Google Authenticator na urządzenie z systemem Android.

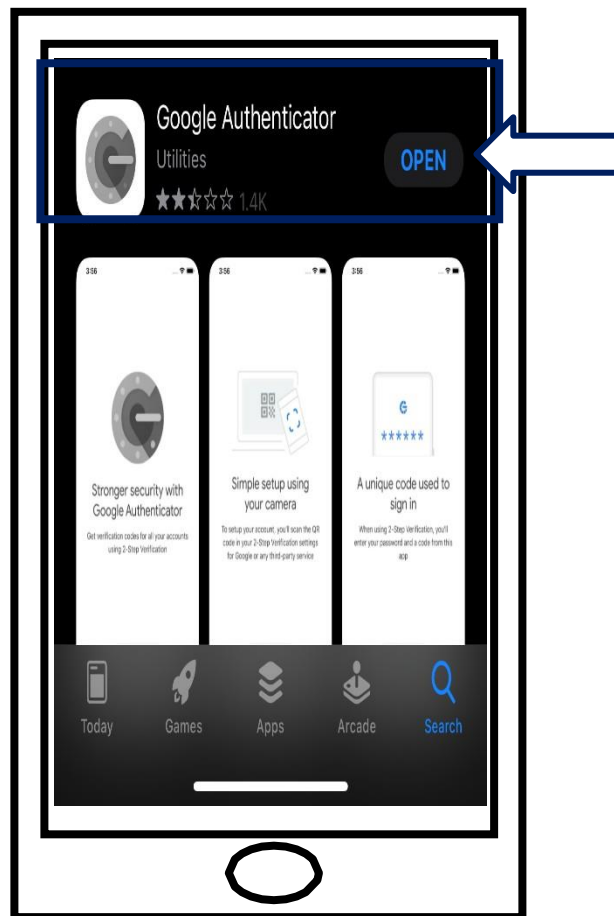
6. Na swoim smartfonie lub tablecie przejdź do Google Play. Upewnij się, że na Twoim smartfonie lub tablecie działa najnowsza wersja systemu operacyjnego (OS).
7. W sklepie Google Play wyszukaj aplikację Google Authenticator.
8. Po znalezieniu aplikacji, pobierz i zainstaluj ją na swoim smartfonie lub tablecie. *(UWAGA: Aplikacja może wyglądać nieco inaczej w zależności od wersji telefonu)*



[Kliknij tutaj, aby wrócić do strony głównej](#)

Wskazówki dotyczące pobierania aplikacji Google Authenticator na urządzenie Apple.

9. Na swoim smartfonie lub tablecie przejdź do App Store. Upewnij się, że na Twoim smartfonie lub tablecie działa najnowsza wersja systemu operacyjnego (OS).
10. W sklepie App Store wyszukaj aplikację Google Authenticator.
11. Wybierz aplikację mobilną Google Authenticator.
12. Pobierz i zainstaluj aplikację.



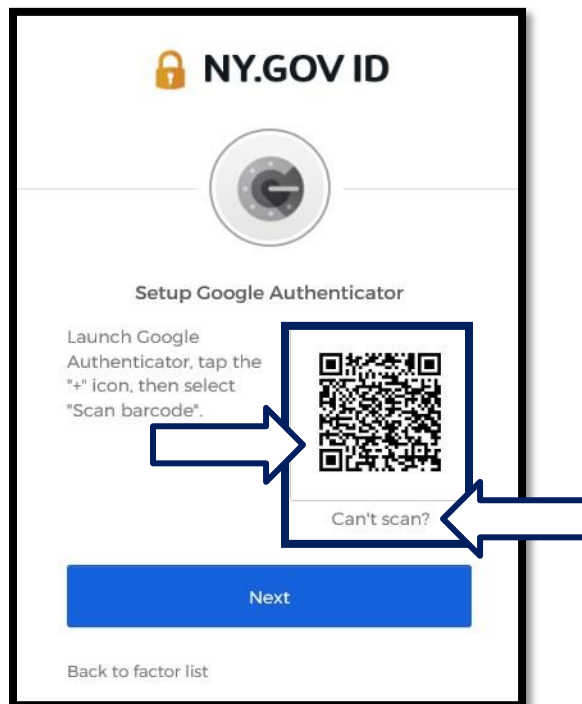
13. Po zainstalowaniu aplikacji Google Authenticator na smartfonie lub tablecie, przejdź do aplikacji na swoim urządzeniu i otwórz ją.

[Kliknij tutaj, aby wrócić do strony głównej](#)

Otwórz aplikację Google Authenticator na swoim smartfonie lub tablecie.

14. Na ekranie komputera pojawi się teraz okno dialogowe z kodem Quick Response (QR).

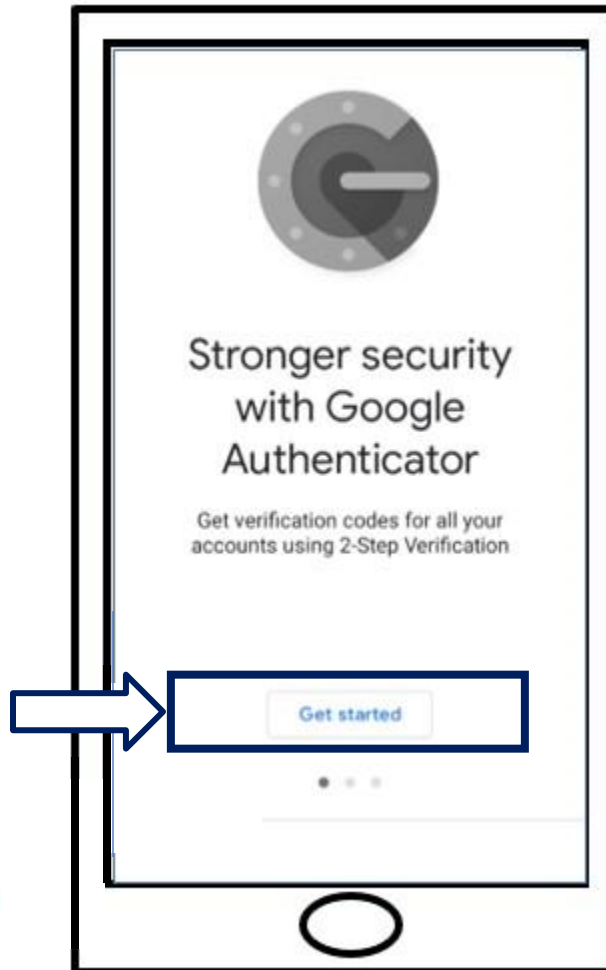
- Jeśli nie możesz zeskanować kodu QR, kliknij opcję **Can't Scan?/Nie możesz zeskanować?** pod kodem QR na ekranie komputera. [Kliknij tutaj, aby uzyskać instrukcje dotyczące opcji Can't Scan.](#)



15. Przejdź do swojej aplikacji Google Authenticator i otwórz ją.

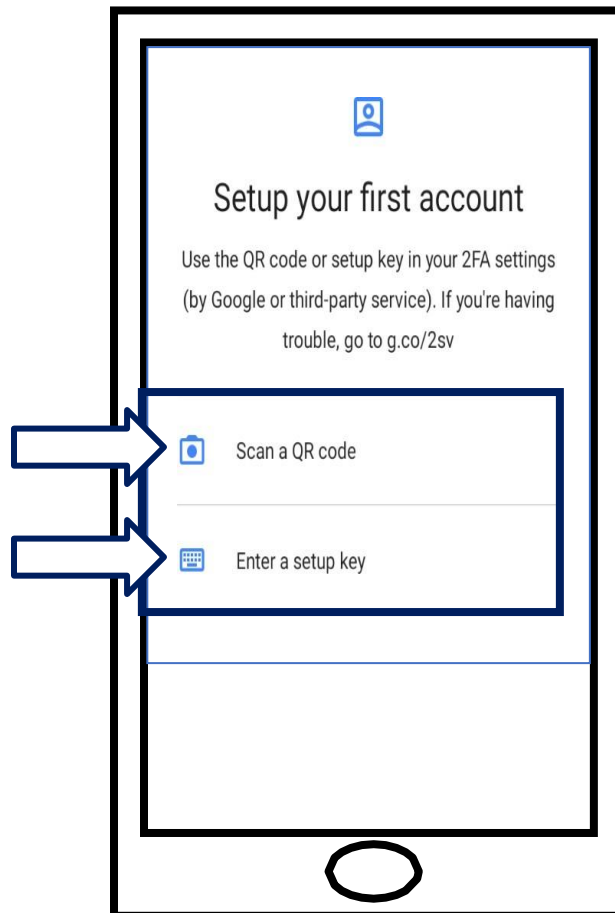
Korzystanie z aplikacji Google Authenticator

16. Na smartfonie zobaczysz ten ekran.



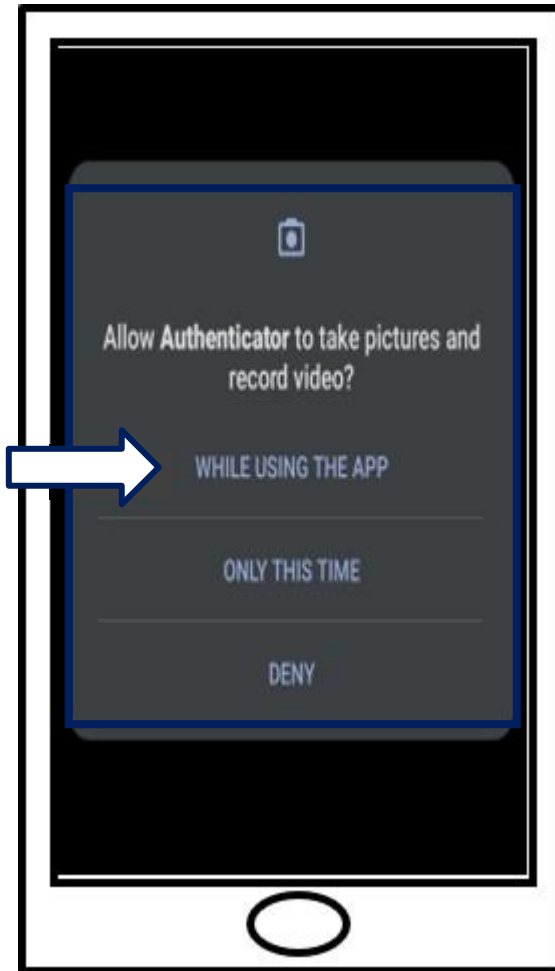
17. Kliknij przycisk **Get Started/Rozpocznij**.

18. Zostanie otwarty ten ekran. Będziesz miał możliwość **zeskanowania kodu QR** lub **wprowadzenia klucza konfiguracji**. Wybierz jedną z tych opcji.



Wskazówki dotyczące używania aplikacji Google Authenticator do skanowania kodu QR: Urządzenie z systemem Android

19. Aplikacja zapyta o zgodę na korzystanie z aparatu. Kliknij przycisk **While Using the App/Podczas używania aplikacji**.



20. Przejdź do [skanowania kodu QR](#).

Urządzenie Apple

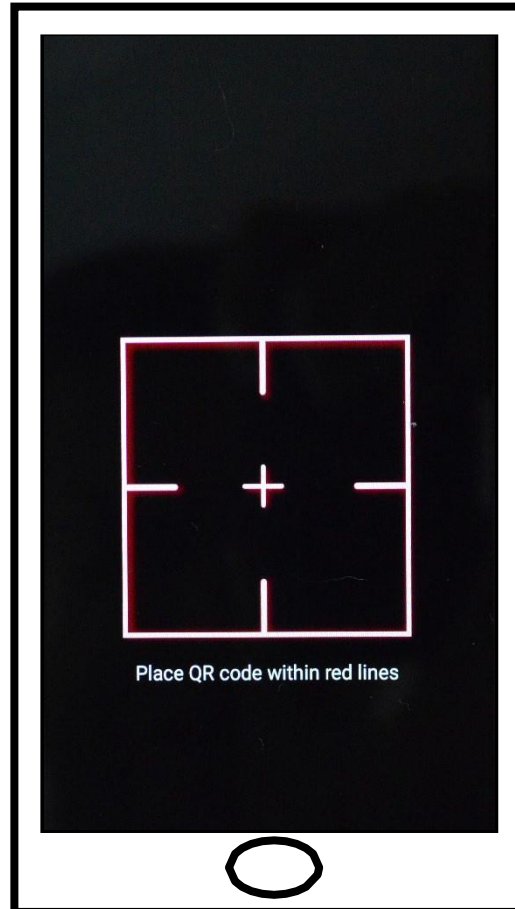
21. Zobaczysz komunikat, że aplikacja „Authenticator” chciałaby uzyskać dostęp do aparatu. Kliknij OK.



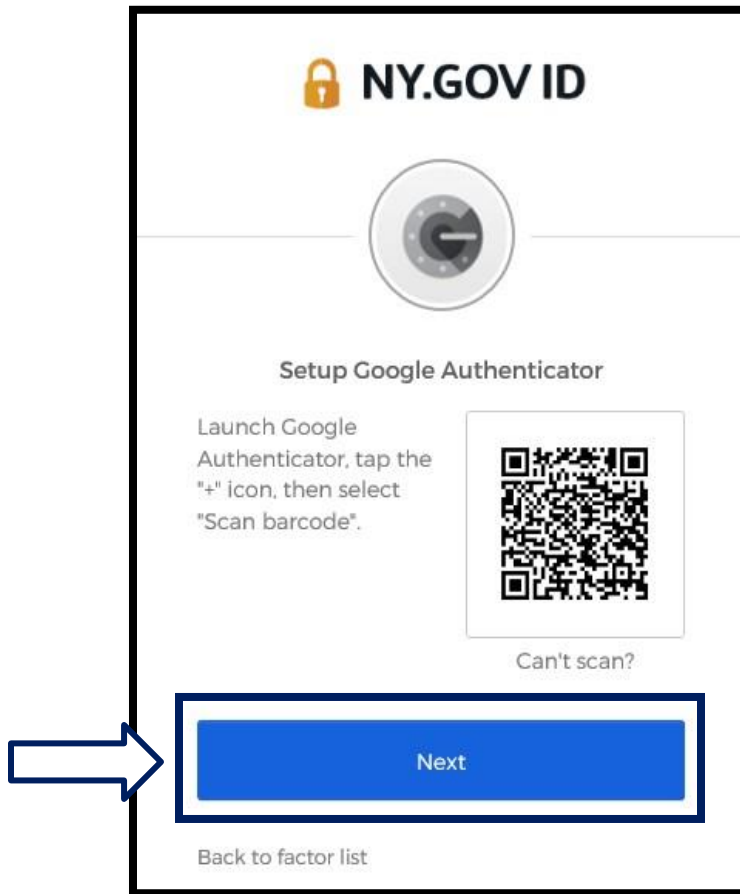
22. Przejdź do [skanowania kodu QR](#).

Zeskanuj kod QR

23. Na ekranie Twojego smartfona pojawi się teraz pusty ekran z kwadratem w środku.



24. Skieruj aparat smartfona lub tabletu na kod QR, który znajduje się na ekranie komputera (patrz poniższy obrazek), tak aby kod QR na ekranie komputera pojawił się w zielonym polu na ekranie smartfona. Aplikacja automatycznie zeskanuje kod do telefonu lub tabletu.



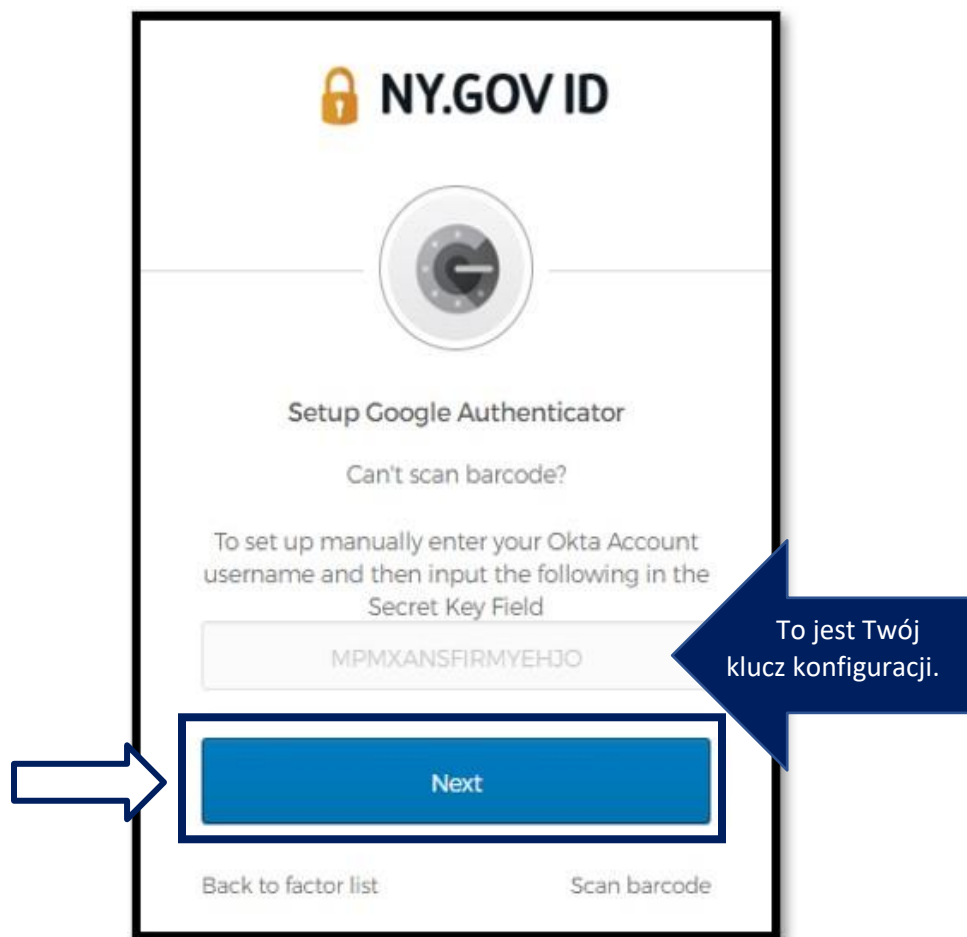
25. Przejdź do [wprowadzania kodu](#) krok po kroku.

Wskazówki dotyczące wprowadzania klucza konfiguracji (jeżeli nie możesz zeskanować kodu QR).

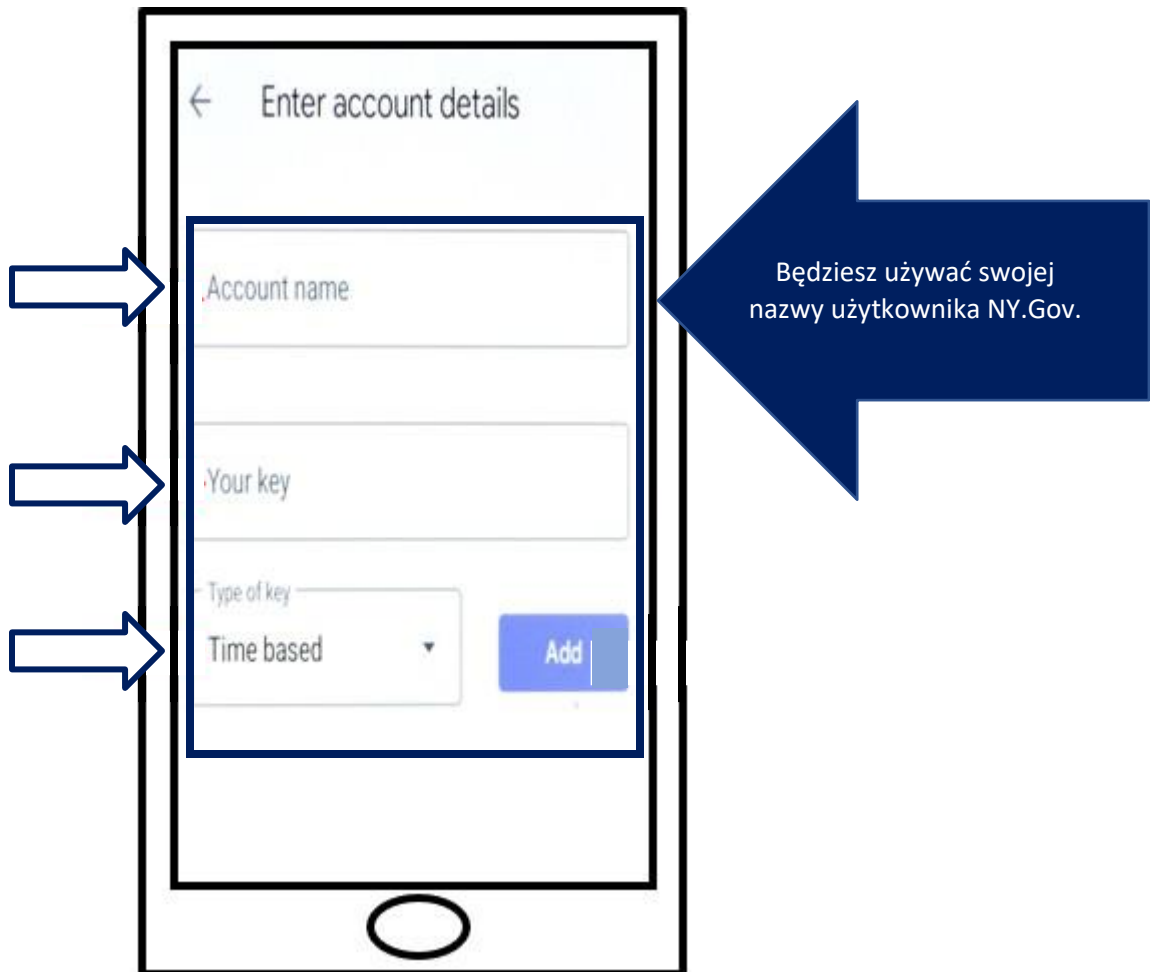
26. Jeśli nie możesz zeskanować kodu, w kroku 13 powyżej wybierz opcję **Enter a setup key/Wprowadź klucz konfiguracji**.

Porada: [Kliknij tutaj, aby poznać inne możliwe przyczyny tego błędu oraz sposób ich naprawienia.](#)

27. Na ekranie komputera pojawi się tajny klucz. Jest to kod, który wpiszesz w aplikacji Google Authenticator. Zostanie wyświetlony ekran zawierający instrukcje dotyczące wprowadzania klucza konfiguracji. **UWAGA:** Aby przejść do tego kroku, musisz najpierw skonfigurować metodę uwierzytelniania wieloczynnikowego Okta Verify.



28. W aplikacji Google Authenticator wprowadź nazwę swojego konta NY.gov, wprowadź swój tajny klucz, wybierz opcję Time based.



29. Kliknij przycisk **Add/Dodaj**.

30. Przejdź do [wprowadzania kodu](#) krok po kroku.

Wprowadzanie kodu

31. Gdy aplikacja pomyślnie zeskanuje kod QR, Twój smartfon wyświetli ekran z Twoją nazwą użytkownika i sześciocyfrowym kodem. Jest to kod, który wpiszesz na komputerze w kolejnych krokach. Kod ten będzie się zmieniał co 30 sekund.



32. Wpisz kod z aplikacji w pole Enter Code/Wpisz kod na monitorze komputera i kliknij **Verify/Zweryfikuj**.

NY.GOV ID

Setup Google Authenticator

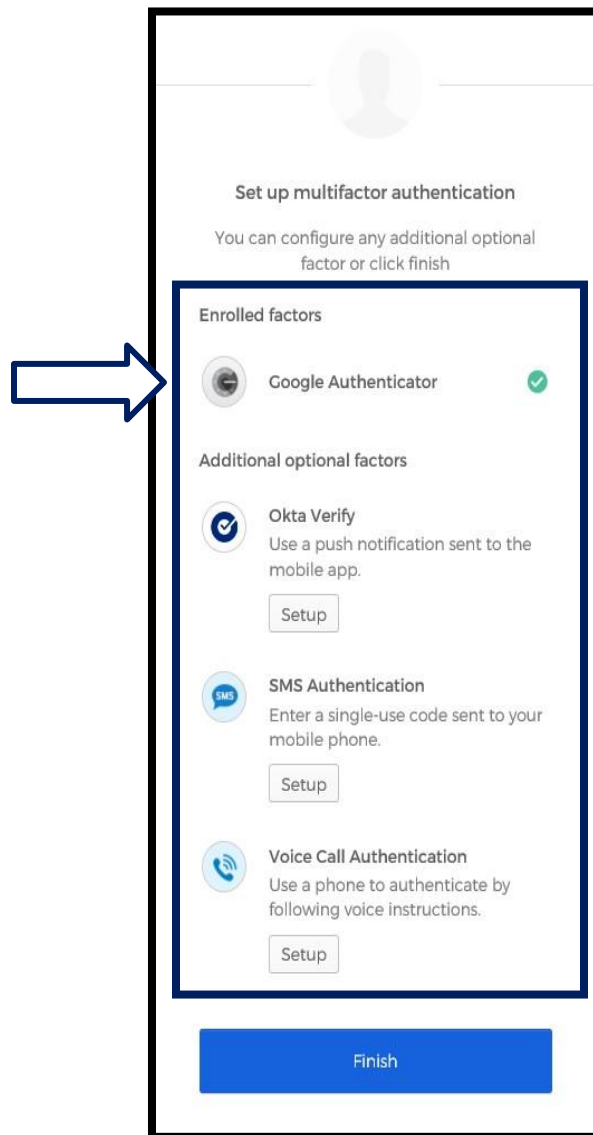
Enter code displayed from the application

Enter Code

Verify

[Back to factor list](#)

33. Zostaniesz przekierowany z powrotem do ekranu rejestracji, gdzie możesz skonfigurować inną metodę uwierzytelniania wieloczynnikowego. Zwróć uwagę, że Google Authenticator znajduje się teraz pod nagłówkiem Enrolled factors/Zarejestrowane czynniki. Zaleca się skonfigurowanie więcej niż jednej metody uwierzytelniania wieloczynnikowego.

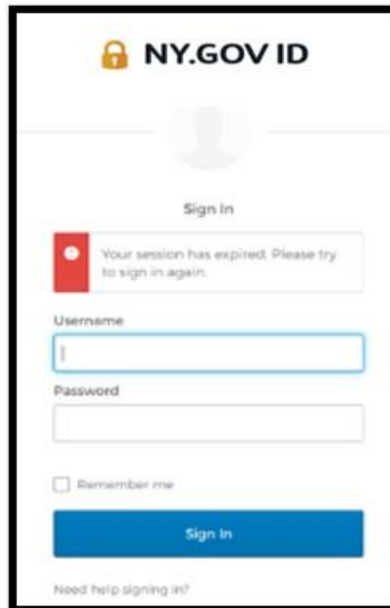


34. Po skonfigurowaniu wszystkich żądanych metod uwierzytelniania wieloczynnikowego kliknij przycisk Finish/Zakończ.

- Porada: Jeśli będziesz konfigurował metodę uwierzytelniania wieloczynnikowego, która wykorzystuje aplikację na telefon, pobierz aplikację przed kliknięciem przycisku Setup/Konfiguruj na stronie przeglądarki „Set up multifactor authentication/Konfiguruj uwierzytelnianie wieloczynnikowe”. Dwie metody uwierzytelniania wieloczynnikowego, które wykorzystują aplikacje, to Okta Verify i Google Authenticator.

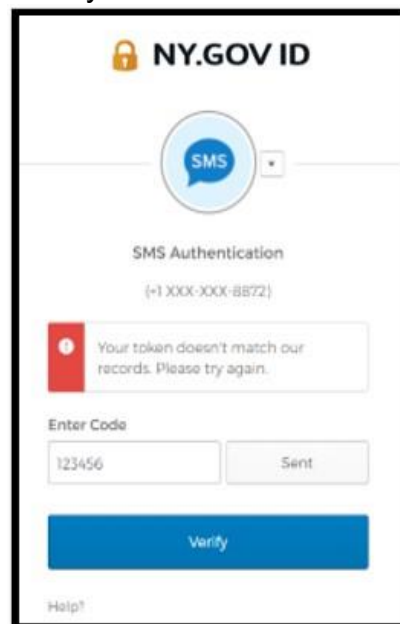
Potencjalne komunikaty o błędach i sposoby ich rozwiązywania.

- Komunikat o błędzie: Sesja wygaśa.
- Rozwiązanie: Klient musi zalogować się ponownie.



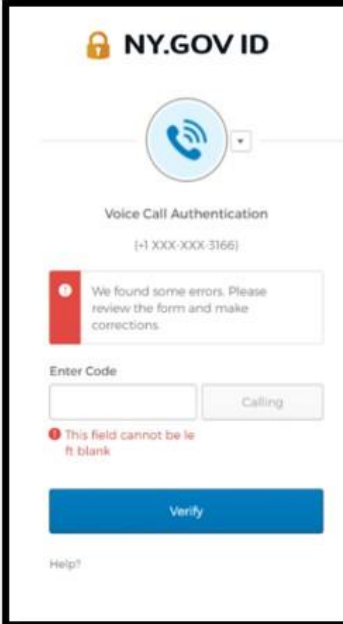
The screenshot shows the NY.GOV ID sign-in interface. At the top, there is a lock icon and the text "NY.GOV ID". Below this is a "Sign In" button. A red error message box states: "Your session has expired. Please try to sign in again." Below the error message are input fields for "Username" and "Password", a "Remember me" checkbox, and a blue "Sign In" button. At the bottom, there is a link that says "Need help signing in?"

- Komunikat o błędzie: Token nie pasuje.
- Rozwiązanie:
 1. Klient powinien sprawdzić poprawność.
 2. Klient powinien ponownie „wysłać” kod.



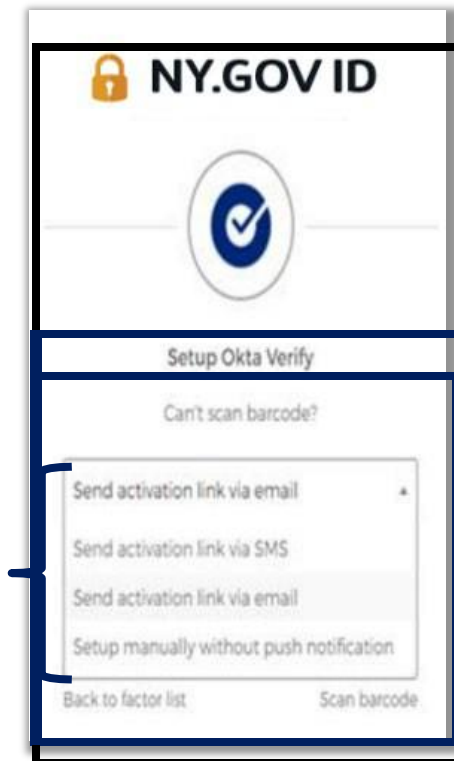
The screenshot shows the NY.GOV ID SMS Authentication interface. At the top, there is a lock icon and the text "NY.GOV ID". Below this is an "SMS" button. Below the button is the text "SMS Authentication" and a phone number "(+1 XXX-XXX-8872)". A red error message box states: "Your token doesn't match our records. Please try again." Below the error message is an "Enter Code" input field containing "123456" and a "Sent" button. Below these is a blue "Verify" button. At the bottom, there is a link that says "Help?"

- Komunikat o błędzie: Znaleziono błąd.
- Rozwiązanie: Klient musi wprowadzić kod.



The screenshot shows the NY.GOV ID Voice Call Authentication interface. At the top, there is a lock icon and the text "NY.GOV ID". Below this is a circular icon with a telephone handset and a dropdown arrow. The text "Voice Call Authentication" and the phone number "(+1 XXX-XXX-3166)" are displayed. A red error message box contains the text: "We found some errors. Please review the form and make corrections." Below the error message is a text input field labeled "Enter Code" and a "Calling" button. A red error message below the input field states: "This field cannot be left blank". At the bottom of the form is a blue "Verify" button and a "Help?" link.

- Komunikat o błędzie: Nie można zeskanować kodu kreskowego.
- Rozwiązanie:
 1. Wypróbuj podane metody alternatywne.
 - „Wyślij aktywację SMSem” - klient może wprowadzić numer telefonu.
 - „Konfiguracja ręczna bez push” - klient zobaczy kod tymczasowy.
 - „Wyślij aktywacyjną wiadomość e-mail” - do klienta zostanie wysłana wiadomość e-mail na adres użyty przy tworzeniu konta.



2. Upewnić się, że urządzenie klienta „zezwoiło” na dostęp do aparatu.
[\(kliknij tutaj, aby uzyskać instrukcje\)](#)

[Powrót do strony głównej](#)