Instrukcja konfiguracji uwierzytelniania wieloczynnikowego

Stan Nowy Jork rozpoczął stosowanie uwierzytelniania 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.

Niniejszy dokument ma na celu pomóc klientom w skonfigurowaniu uwierzytelniania wieloczynnikowego na ich koncie w serwisie NY.gov.

INDEKS

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”.

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

- Na swoim smartfonie pobierz aplikację Google Authenticator. Instrukcje dotyczące pobierania aplikacji znajdują się poniżej.
- Na ekranie komputera kliknij opcję **Setup/Konfiguracja** w obszarze Google Authenticator, aby rozpocząć proces konfiguracji.
- Wybierz iPhone lub Android w zależności od urządzenia.
    - Zostaniesz poinstruowany, aby pobrać aplikację Google Authenticator ze sklepu Google Play (Android) lub App Store (iPhone). Jeśli jeszcze tego nie zrobiłeś, powinieneś pobrać tę aplikację już teraz. Instrukcje dotyczące pobierania aplikacji znajdują się poniżej.

  PORADA: Jeśli masz tablet Apple, wybierz iPhone.
- Kliknij przycisk **Next/Dalej.**
- **Wykorzystaj następujące wskazówki dotyczące pobierania aplikacji Google Authenticator na urządzenie z systemem Android (Google Play) lub urządzenie Apple (App Store).**
- Na swoim smartfonie lub tablecie przejdź do Google Play (Android) lub App Store (urządzenie Apple). Upewnij się, że na Twoim smartfonie lub tablecie działa najnowsza wersja systemu operacyjnego (OS).
- W sklepie Google Play (Android) lub App Store (urządzenie Apple) wyszukaj aplikację Google Authenticator.
- Wybierz aplikację Google Authenticator.
- Pobierz i zainstaluj aplikację.
- Po zainstalowaniu aplikacji Google Authenticator na smartfonie lub tablecie, przejdź do aplikacji na swoim urządzeniu i otwórz ją. *(UWAGA: Aplikacja może wyglądać nieco inaczej w zależności od wersji telefonu)*
- **Wykorzystaj następujące wskazówki dotyczące korzystania z aplikacji Google Authenticator na swoim smartfonie lub tablecie.**
- Po wybraniu na ekranie komputera urządzenia Apple lub urządzenia z systemem Android, na ekranie komputera pojawi się okno dialogowe z kodem Quick Response (QR). Kod QR zostanie wyświetlony jako kwadrat wypełniony czarnymi kropkami.

- Jeśli nie możesz zeskanować kodu QR na swój smartfon lub tablet, kliknij opcję **Can't Scan?/Nie możesz zeskanować?** pod kodem QR na ekranie komputera.

- Jeśli jesteś w stanie zeskanować kod QR na swoim smartfonie lub tablecie, przejdź do aplikacji Google Authenticator i otwórz ją, jeśli nie jest jeszcze otwarta.
- Kliknij przycisk **Get Started/Rozpocznij.**
- Będziesz miał możliwość **zeskanowania kodu QR** lub **wprowadzenia klucza konfiguracji.** Wybierz jedną z tych opcji.

  PORADA: Jeśli nie możesz zeskanować kodu, wybierz opcję **Enter a setup key/Wprowadź klucz konfiguracji.** Poniżej znajdziesz wskazówki dotyczące wprowadzania klucza konfiguracji.
- Jeżeli masz telefon z systemem Android, aplikacja zapyta o zgodę na korzystanie z aparatu. Kliknij przycisk „While Using the App/Podczas używania aplikacji".
- Jeżeli masz urządzenie Apple, zobaczysz komunikat, że *aplikacja „Authenticator" chciałaby uzyskać dostęp do aparatu.* Kliknij OK.
- Po wydaniu zgody na korzystanie z aparatu, na ekranie Twojego smartfona pojawi się teraz pusty ekran z kwadratem w środku.
- Skieruj aparat smartfona lub tabletu na kod QR, który znajduje się na ekranie komputera, tak aby kod QR na ekranie komputera pojawił się w zielonym polu na ekranie smartfona. Aplikacja automatycznie zeskanuje kod do telefonu lub tabletu.
- **Skorzystaj z poniższych wskazówek, jeśli w aplikacji wybrano opcję Wprowadź klucz konfiguracji zamiast Skanuj kod QR.**
- 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.
- W aplikacji Google Authenticator zobaczysz ekran służący do wprowadzenia danych konta. Na ekranie należy podać następujące informacje:
  - Nazwę Twojego konta NY.gov w polu „Account name/Nazwa konta".
  - Twój tajny klucz w polu „Your Key/Twój klucz".
  - Wybierz „Time-Based" z rozwijanej listy Type of Key/Rodzaj klucza.
- Kliknij przycisk **Add/Dodaj.**
- **Użyj poniższych wskazówek, aby wprowadzić kod z aplikacji Google Authenticator do komputera.**
- Po pomyślnym zeskanowaniu przez aplikację kodu QR lub pomyślnym wprowadzeniu tajnego klucza do aplikacji, aplikacja wyświetli ekran z nazwą użytkownika i sześciocyfrowym kodem. Jest to kod, który wpiszesz na komputerze w kolejnych krokach. Kod ten będzie się zmieniał co 30 sekund.

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

  PORADA: Zaleca się skonfigurowanie więcej niż jednej metody uwierzytelniania wieloczynnikowego.
- 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 wygasła.
- Rozwiązanie: Klient musi zalogować się ponownie.

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

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

- Komunikat o błędzie: Nie można zeskanować kodu kreskowego.
- Rozwiązanie:
  - 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 wiadoność e-mail na adres użyty przy tworzeniu konta.
- Upewnić się, że urządzenie klienta „zezwoliło” na dostęp do aparatu.

Powrót do strony głównej

Konfiguracja uwierzytelniania wieloczynnikowego Okta Verify

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

- Na swoim smartfonie pobierz aplikację Okta Verify. Instrukcje dotyczące pobierania aplikacji znajdują się poniżej.
- Na ekranie komputera kliknij opcję **Setup/Konfiguracja** w obszarze Okta Verify, aby rozpocząć proces konfiguracji.
- Wybierz iPhone lub Android w zależności od urządzenia.
    - Zostaniesz poinstruowany, aby pobrać aplikację Okta Verify ze sklepu Google Play (Android) lub App Store (iPhone). Jeśli jeszcze tego nie zrobiłeś, powinieneś pobrać tę aplikację już teraz. Instrukcje dotyczące pobierania aplikacji znajdują się poniżej.

  PORADA: Jeśli masz tablet Apple, wybierz iPhone.
- Kliknij przycisk **Next/Dalej.**
- **Wykorzystaj następujące wskazówki dotyczące pobierania aplikacji Okta Verify na urządzenie z systemem Android (Google Play) lub urządzenie Apple (App Store).**
- Na swoim smartfonie lub tablecie przejdź do Google Play (Android) lub App Store (urządzenie Apple). Upewnij się, że na Twoim smartfonie lub tablecie działa najnowsza wersja systemu operacyjnego (OS).
- W sklepie Google Play lub App Store wyszukaj aplikację Okta Verify.
- Wybierz aplikację mobilną Okta Verify.
- Pobierz i zainstaluj aplikację.
- Po zainstalowaniu aplikacji Okta Verify na smartfonie lub tablecie, przejdź do aplikacji na swoim urządzeniu i otwórz ją.
- **Wykorzystaj następujące wskazówki, aby otworzyć aplikację Okta Verify na swoim smartfonie lub tablecie.**

- Na ekranie komputera pojawi się teraz okno dialogowe z kodem Quick Response (QR). Kod QR zostanie wyświetlony jako kwadrat wypełniony czarnymi kropkami.
    - Jeśli nie możesz zeskanować kodu QR, kliknij opcję **Can't Scan?/Nie możesz zeskanować?** pod kodem QR na ekranie komputera. Poniżej znajdują się wskazówki jak skonfigurować Okta Verify po kliknięciu Can't Scan.

- Jeśli możesz zeskanować kod QR, przejdź do aplikacji Okta Verify na swoim urządzeniu i otwórz ją.
- Kliknij przycisk **Get Started/Rozpocznij.**
- Kliknij przycisk **Next/Dalej.**
- Kliknij przycisk **Add Account/Dodaj konto.**
- Kliknij **Other/Inny.**
- Będziesz miał możliwość **zeskanowania kodu QR** lub **wprowadzenia klucza ręcznie.** Wybierz jedną z tych opcji.
    - Jeśli wybierzesz opcję **Wprowadź klucz ręcznie**, musisz wykonać poniższe czynności dla opcji weryfikuj ręcznie bez powiadomienia push z poniższej listy rozwijanej Can't Scan.
- **Wykorzystaj poniżesz wskazówki dotyczące używania aplikacji Okta Verify do skanowania kodu QR.**
- Jeżeli masz urządzenie z systemem Android, aplikacja zapyta o zgodę na korzystanie z aparatu. Kliknij OK.
- Jeżeli masz urządzenie Apple, zobaczysz komunikat, że *„Okta Verify" chciałby uzyskać dostęp do aparatu.* Kliknij OK.
- Skieruj aparat smartfona lub tabletu na kod QR, który znajduje się na ekranie komputera. Aplikacja automatycznie zeskanuje kod do telefonu lub tabletu.
- Na monitorze komputera pojawi się ekran rejestracji z wyskakującym okienkiem z kodem QR.
- W aplikacji Okta Verify kliknij opcję **Add Account/Dodaj konto.**
- Skieruj aparat smartfona lub tabletu na kod QR, który znajduje się na monitorze komputera.
- Po zeskanowaniu kodu QR w aplikacji pojawi się nowy ekran z pytaniem o zezwolenie na powiadomienia push. Wybierz opcję **Allow/Zezwól** lub **Skip/Pomiń.**
- Po pomyślnym zeskanowaniu kodu QR do smartfona, na ekranie komputera pojawi się informacja o pomyślnym zeskanowaniu kodu.
- **Wykorzystaj poniższe wskazówki, aby skonfigurować Okta Verify przez e-mail lub SMS po kliknięciu na Can't Scan.**

- Po kliknięciu opcji **Can't Scan/Nie można skanować** na ekranie komputera zobaczysz ekran z napisem Setup Okta Verify/Konfiguracja Okta Verify. Na tym ekranie znajduje się lista rozwijana, która oferuje następujące opcje: Wyślij link aktywacyjny za pośrednictwem poczty elektronicznej, Wyślij link aktywacyjny za pośrednictwem wiadomości SMS oraz Skonfiguruj ręcznie bez powiadomienia push.

  PORADA: Poniżej przedstawiono wskazówki dotyczące konfiguracji ręcznej bez powiadomienia push.

- Kliknij **Send activation link via email/Wyślij link aktywacyjny za pośrednictwem poczty elektronicznej** lub **Send activation link via SMS/Wyślij link aktywacyjny za pośrednictwem wiadomości SMS**. Otrzymasz link.

  PORADA: W link **należy** kliknąć ze smartfona lub tabletu.

- Aby uzyskać dostęp do linku, na smartfonie lub tablecie przejdź do swojej aplikacji do obsługi poczty elektronicznej lub wiadomości tekstowych. Otwórz wiadomość e-mail lub SMS, którą otrzymałeś. Kliknij link w wiadomości.
- Link przekieruje Cię na stronę Okta Verify.
- Kliknij przycisk **Get Started/Rozpocznij.**
- Twój smartfon połączy się z witryną Okta Verify i zweryfikuje link. Na ekranie komputera pojawi się informacja o pomyślnym zeskanowaniu kodu.
- **Wykorzystaj poniższe wskazówki, aby skonfigurować Okta Verify ręcznie bez powiadomienia push po kliknięciu na listę rozwijaną Can't Scan.**
- Po kliknięciu opcji **Can't Scan/Nie można skanować** na ekranie komputera zobaczysz ekran z napisem Setup Okta Verify/Konfiguracja Okta Verify. Na tym ekranie znajduje się lista rozwijana, która oferuje następujące opcje: Wyślij link aktywacyjny za pośrednictwem poczty elektronicznej, Wyślij link aktywacyjny za pośrednictwem wiadomości SMS oraz Skonfiguruj ręcznie bez powiadomienia push.
- Wybierz opcję: Zweryfikuj ręcznie bez powiadomienia push.
- Zostaniesz przeniesiony do ekranu, który zawiera tajny kod.
- Otwórz aplikację Okta Verify.
- Kliknij przycisk **Get Started/Rozpocznij.**
- Kliknij przycisk **Next/Dalej.**
- Kliknij przycisk **Add Account/Dodaj konto.**
- Kliknij **Other/Inny.**
- Wybierz Enter Key Manually/Wprowadź klucz ręcznie.
- Wpisz kod z ekranu komputera na ekran swojego smartfona. Na smartfonie wpisz nazwę konta (stworzoną przez Ciebie) oraz kod wyświetlany na ekranie Twojego komputera.
- Kliknij przycisk **Add Account/Dodaj konto.**

- Po zweryfikowaniu kodu, na ekranie komputera pojawi się informacja o pomyślnym zeskanowaniu kodu.

- Kliknij **Done/Gotowe**.
- **Wykorzystaj poniższe wskazówki po pomyślnym zeskanowaniu kodu QR lub ręcznej weryfikacji kodu za pomocą aplikacji.**
- Po zeskanowaniu kodu QR, aplikacja zmieni ekran na ekran z sześciocyfrowym kodem. Kod ten będzie się zmieniał co 30 sekund.

- Po pomyślnym skonfigurowaniu aplikacji Okta Verify na ekranie komputera pojawi się ekran rejestracji, na którym można skonfigurować kolejną metodę uwierzytelniania wieloczynnikowego. Na ekranie pojawi się teraz informacja, że Okta Verify znajduje się pod nagłówkiem zarejestrowanych czynników.
- 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 wygasła.
- Rozwiązanie: Klient musi zalogować się ponownie.

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

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

- Komunikat o błędzie: Nie można zeskanować kodu kreskowego.
- Rozwiązanie
  - 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 wiadoność e-mail na adres użyty przy tworzeniu konta.

- Upewnić się, że urządzenie klienta „zezwoliło” na dostęp do aparatu.

Powrót do strony głównej

Weryfikacja za pomocą SMS

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

- Kliknij Setup/Konfiguruj przy SMS Authentication/Uwierzytelnianie SMS.
- Zostaniesz poproszony o wprowadzenie numeru telefonu.

  PORADA: Ten numer telefonu musi umożliwiać odbieranie wiadomości tekstowych.
- Po wpisaniu numeru telefonu kliknij **Send code/Wyślij kod.**
- Otrzymasz wiadomość tekstową z kodem. Wprowadź ten kod w polu Enter Code/Wpisz kod.
- Naciśnij przycisk **Verify/Weryfikuj.**
- Zostaniesz przekierowany z powrotem do ekranu rejestracji uwierzytelniania wieloczynnikowego. Zwróć uwagę, że uwierzytelnianie SMS znajduje się teraz pod nagłówkiem Enrolled factors/Zarejestrowane czynniki.
- Zaleca się skonfigurowanie więcej niż jednej metody uwierzytelniania wieloczynnikowego.
- Po skonfigurowaniu wszystkich żądanych metod uwierzytelniania wieloczynnikowego kliknij przycisk **Finish/Zakończ.**

Powrót do strony głównej

Uwierzytelnianie za pomocą połączeń głosowych

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

- Kliknij Setup/Konfiguracja w obszarze Uwierzytelnianie połączeń głosowych.
- Zostaniesz poproszony o wprowadzenie numeru telefonu.
- Po wpisaniu numeru telefonu kliknij **Call/Zadzwoń.**
- Otrzymasz telefon. Gdy odbierzesz połączenie, nagrany głos odczyta pięciocyfrowy numer.

  PORADA: Numer zostanie powtórzony tylko raz. Przygotuj długopis i kartkę, aby zapisać numer.
- Wprowadź ten kod w polu Enter Code/Wpisz kod.

- Naciśnij przycisk **Verify/Weryfikuj.**
- Zostaniesz przekierowany z powrotem do ekranu rejestracji uwierzytelniania wieloczynnikowego. Zwróć uwagę, że uwierzytelnianie za pomocą połączeń głosowych znajduje się teraz pod nagłówkiem Enrolled factors/Zarejestrowane czynniki.
- Zaleca się skonfigurowanie więcej niż jednej metody uwierzytelniania wieloczynnikowego.
- Po skonfigurowaniu wszystkich żądanych metod uwierzytelniania wieloczynnikowego kliknij przycisk Finish/Zakończ.

Powrót do strony głównej