

## 1. ADMINISTRACJA UWIERZYTELNIANIEM WIELOSKŁADNIKOWYM (MFA)

### 1.1. ZARZĄDZANIE UWIERZYTELNIANIEM WIELOSKŁADNIKOWYM

W Portalu Świadczeniodawcy Narodowego Funduszu Zdrowia istnieje możliwość stosowania uwierzytelniania wieloskładnikowego. Uwierzytelnianie wieloskładnikowe znacznie podnosi bezpieczeństwo – zabezpieczenie przed dostępem do portalu osób nieuprawnionych.

Stosowanie do identyfikacji samych identyfikatorów użytkownika i haseł, obecnie, stało się już niewystarczające ze względu na duże zagrożenie włamaniami do systemu a także metody stosowane przez hakerów.

Wdrożenie mechanizmu **uwierzytelniania wieloskładnikowego (MFA)** w Portalu Świadczeniodawcy ma kluczowe znaczenie dla zapewnienia bezpieczeństwa. Klasyczne hasła nie są już bezpieczne głównie dlatego, że:

- użytkownicy nadal używają słabych haseł,
- używają tych samych haseł w wielu portalach,
- strony nadal źle zabezpieczają hasła, co powoduje możliwość wycieku haseł.

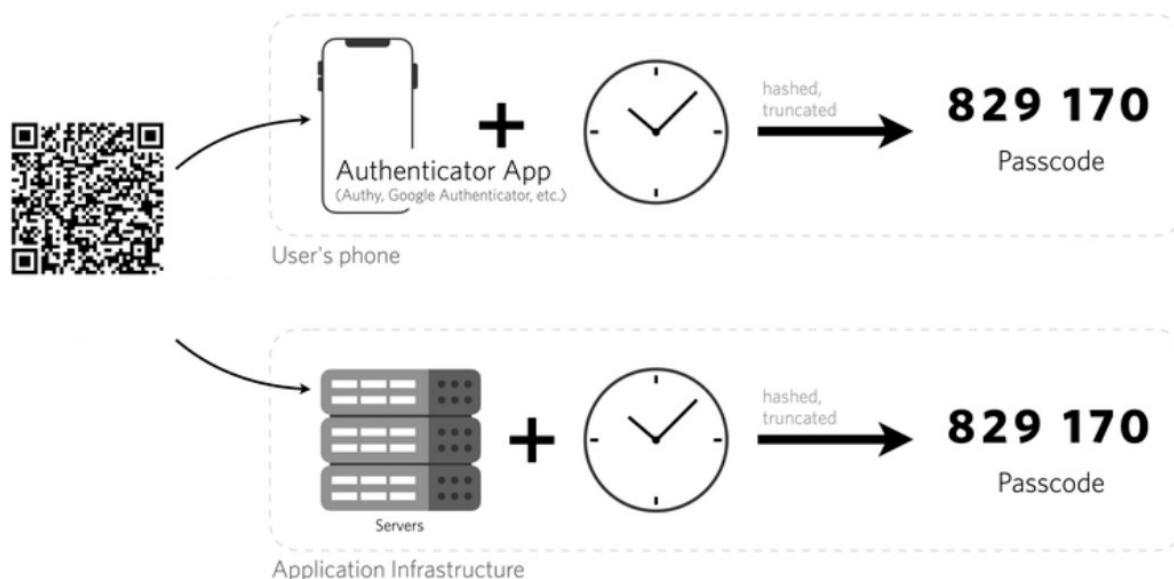
#### Czym jest uwierzytelnianie wieloskładnikowe?

Uwierzytelnianie wieloskładnikowe składa się z czegoś co użytkownik zna czyli np. hasła, kodu, PIN-u i dodatkowo czegoś co użytkownik ma czyli np. telefon, token sprzętowy, karta kodów. Mogą być również wykorzystywane indywidualne cechy użytkownika czyli odcisk palca, tęcza (może być wykorzystywana biometria).

MFA wymaga dwóch lub więcej składników do uwierzytelnienia. W systemie Narodowego Funduszu Zdrowia zastosowano uwierzytelnianie dwuskładnikowe czyli składające się z hasła (jak do tej pory) i z systemu jednorazowych kodów wysyłanych na urządzenie świadczeniodawcy np. na telefon komórkowy.

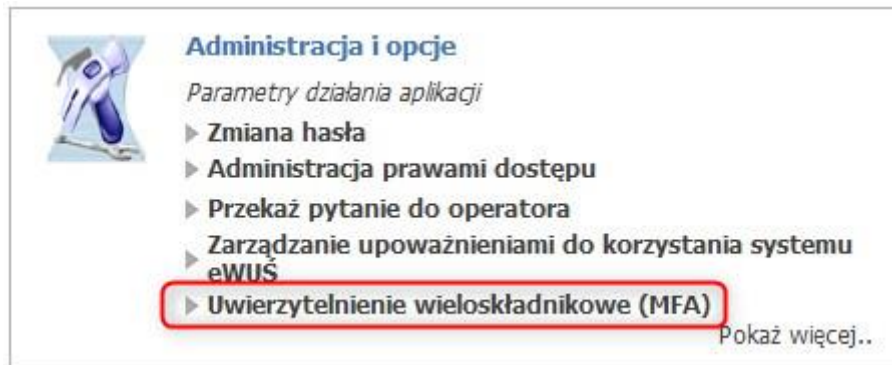
#### Tokeny TOTP

**TOTP** (Time-based One-Time Password), jest to mechanizm oparty na czasie. Od momentu wygenerowania hasła/kodu użytkownik ma określoną liczbę sekund na jego użycie, w przeciwnym wypadku straci ono ważność.



Operator Portalu Świadczeniodawcy ma możliwość zarządzania sposobem uwierzytelniania do portalu. Dostępność mechanizmu MFA w systemie Funduszu nie oznacza, że został on automatycznie włączony dla

wszystkich świadczeniodawców. Rozpoczęcie stosowania uwierzytelniania dwuskładnikowego wymaga włączenia go przez operatora świadczeniodawcy, korzystając z funkcji **Włącz** w funkcji konfiguracji MFA.



## Zarządzanie uwierzytelnieniem wieloskładnikowym

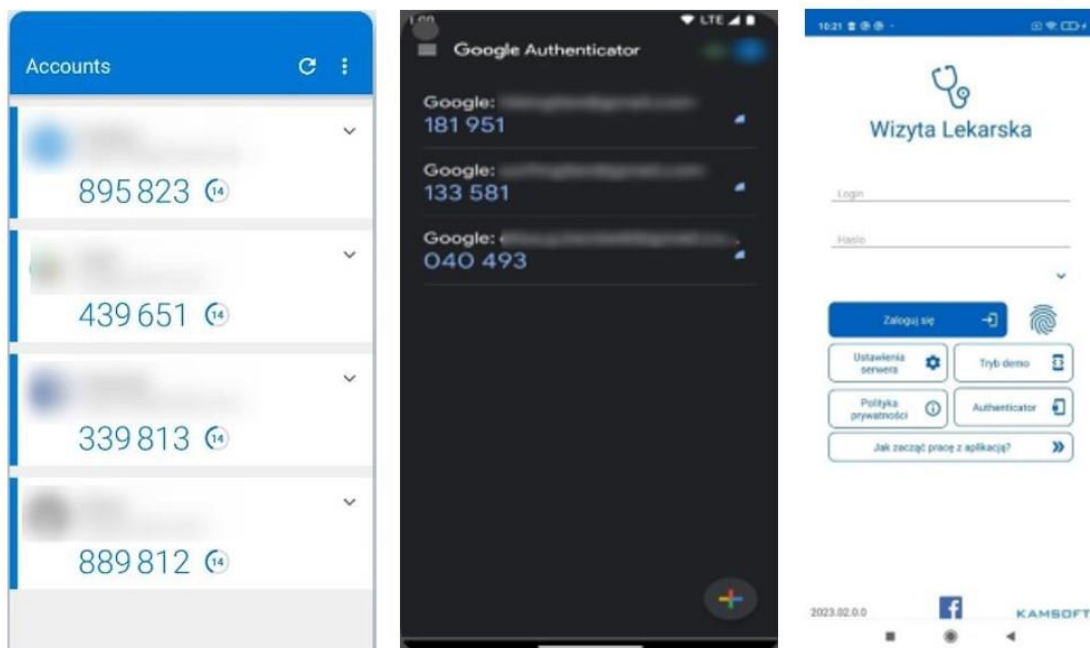
▶ Powrót   ▶ Pomoc

Kod świadczeniodawcy: [blurred]  
Nazwa świadczeniodawcy: [blurred]  
Użytkownik: [blurred]

Składnik	Informacja	Akcje
Konfiguracja uwierzytelnienia	Nieaktywny	<b>Włącz</b>
Kody odzyskiwania	Nieaktywny	

Operator Portalu Świadczeniodawcy może włączyć mechanizm MFA wykorzystujący tokeny TOTP.

Aby móc skorzystać z tego mechanizmu konieczne jest posiadanie na urządzeniu aplikacji, która obsługuje otwarty standard TOTP. Taką aplikacją jest np. Microsoft Authenticator, Google Authenticator, Wizyta lekarska firmy Kamssoft, ale liczba aplikacji generujących tokeny TOTP jest bardzo duża i są to zarówno produkty darmowe jak i komercyjne.




Rozpoczęcie korzystania z mechanizmu FMA wymaga jednorazowego wykonania czynności powiązania konta w portalu z aplikacją do uwierzytelniania.

Aby móc włączyć MFA wykorzystujący tokeny TOTP, użytkownik musi zeskanować w aplikacji, którą ma zainstalowaną np. na telefonie kod QR wyświetlony w portalu.

### Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



### Ręczne dodanie konta

Wprowadź poniższe informacje ręcznie w aplikacji do uwierzytelniania:

Nazwa konta:

Sekret:

### W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej

Kod hasła jednorazowego:

Zamiast zeskanowania kodu QR użytkownik może go przepisać ręcznie czyli na żądanie wyświetlić kod (sekret) i przepisać/skopiować do aplikacji używanej do uwierzytelniania. Wpisanie kodu ręcznie da ten sam efekt co zeskanowanie kodu QR. W aplikacji do uwierzytelniania zostanie wygenerowany kod potwierdzający.

## TOTP – Potwierdzanie konta

Twilio (Example Account)

765 286



Segment (Example Account)

003 457



Aby potwierdzić powiązanie aplikacji uwierzytelniającej z portalem należy wpisać 6-cyfrowy kod, generowany przez aplikację i użyć funkcji **Powiąz**. Nastąpi powiązanie uwierzytelnienia wieloskładnikowego.

**W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej**

Kod hasła jednorazowego:

Zweryfikowano pozytywnie

Powiąż

**Kody odzyskiwania**

Aby nie stracić dostępu do konta na wypadek utraty urządzenia z aplikacją uwierzytelniającą, wygenerowane zostały kody odzyskiwania jednorazowego użytku.  
Aby kontynuować, naciśnij przycisk **Drukuj** lub **Zapisz**. Wydruk/plik zachowaj w bezpiecznym miejscu.

Drukuj Zapisz

Od7bxut	
Zzrsgldf	
e073er5	
en6me6	
fxoqcjpv	

Kolejnym krokiem, wymaganym w procesie włączania MFA, jest wyświetlenie kodów odzyskiwania wraz z możliwością ich wydruku lub zapisania. Kody te pozwalają na awaryjne zalogowanie się wykorzystując MFA w przypadku utracenia urządzenia generującego tokeny TOTP lub wystąpienia problemu z użyciem aplikacji uwierzytelniającej. Są to kody jednorazowego użytku (raz wykorzystany kod staje się nieaktywny). Zaleca się te kody wydrukować, zapisać i schować w bezpieczne miejsce, nie ujawniać ich osobom niepowołanym.


Po wydrukowaniu/zapisaniu kodów operator zapisuje konfigurację za pomocą klawisza Zapisz konfigurację. Po poprawnym zapisaniu pokaże się informacja **Poprawnie zapisano konfigurację**.

## Włączanie MFA i powiązanie aplikacji do uwierzytelniania z portalem – wykaz czynności.

1. Aby włączyć MFA wykorzystujący tokeny TOTP operator musi skorzystać z linku **Włącz**.

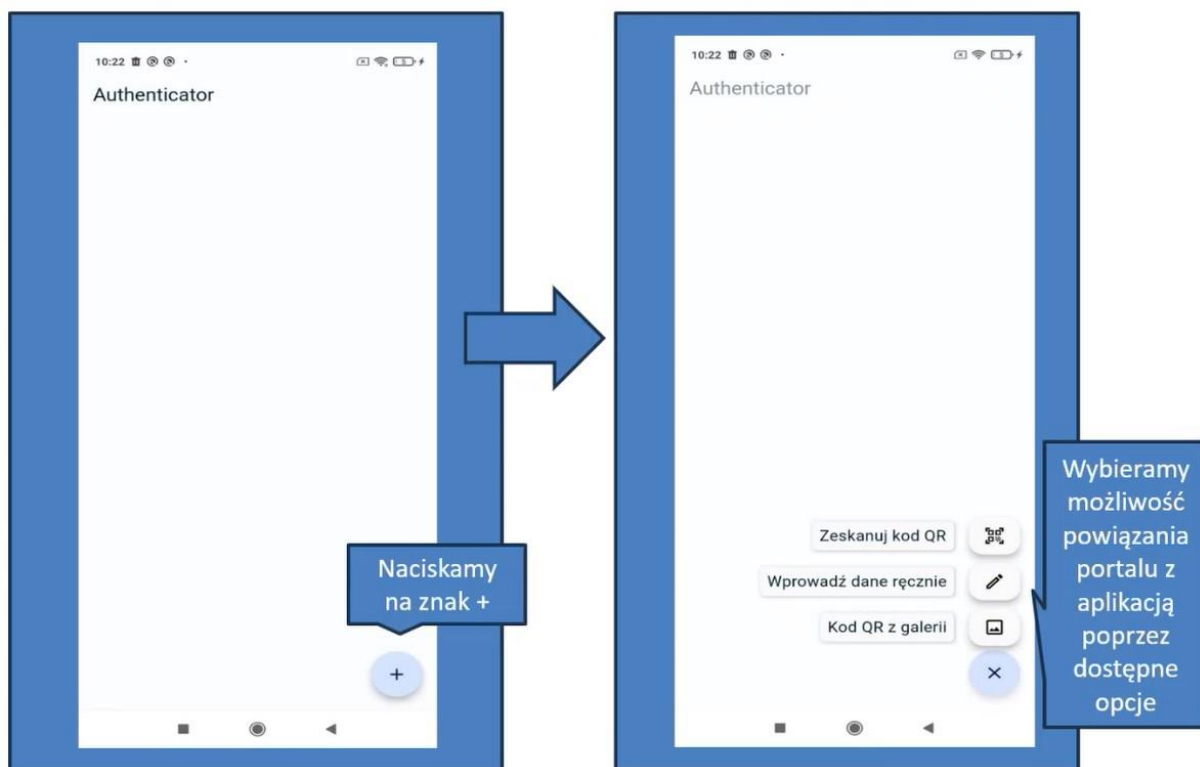
### Zarządzanie uwierzytelnieniem wieloskładnikowym

► Powrót ► Pomoc

 Kod świadczeniodawcy:  
Nazwa świadczeniodawcy:  
Użytkownik:

Składnik	Informacja	Akcje
Konfiguracja uwierzytelnienia	Nieaktywny	<b>Włącz</b>
Kody odzyskiwania	Nieaktywny	


2. Po otwarciu formatki w aplikacji do uwierzytelniania operator dodaje i skanuje kod QR na aplikacji zewnętrznej.




3. Zamiast zeskanowania można kliknąć w **Dodaj konto ręcznie**.

### Administracja uwierzytelniania wieloskładnikowego (MFA)

► Powrót ► Pomoc

 Kod świadczeniodawcy: [blurred]  
Nazwa świadczeniodawcy: [blurred]  
Użytkownik: [blurred]

**Skanowanie kodu QR**  
Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



**Dodaj konto ręcznie**

**W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej**  
Kod hasła jednorazowego:

4. Po udanym powiązaniu urządzenia, aplikacja jest gotowa do uwierzytelnienia wieloskładnikowego.



5. Operator przepisuje kod z aplikacji zewnętrznej do portalu i klika w **Powiąz**.

## Administracja uwierzytelniania wieloskładnikowego (MFA)

► Powrót ► Pomoc



Kod świadczeniodawcy: **01221**  
Nazwa świadczeniodawcy: **Niepubliczna przychodnia Jutrzenka**  
Użytkownik: **magda\_szkolenie**

### Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



### Ręczne dodanie konta

Wprowadź poniższe informacje ręcznie w aplikacji do uwierzytelniania:

**Nazwa konta:** Portal NFZ OW08:ws-01221-magda\_szkolenie  
**Sekret:** HOFERKIMKYG6DPGXZF2XOXKTP4HM42ZHMNUJD58ZYLRDRKBMUNRH30TEWTGMAXAOD

Ukryj

**W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej**

Kod hasła jednorazowego:

6. Po prawidłowym powiązaniu pokaże się informacja **Zweryfikowano pozytywnie** oraz lista kodów odzyskiwania.

Lista kodów odzyskiwania jest to lista 10 kodów, które można użyć w przypadku problemów z użyciem aplikacji uwierzytelniającej np. zgubienia lub uszkodzenia telefonu.

Kody należy zapisać lub wydrukować. Bez tej czynności program nie będzie mógł zakończyć konfiguracji.

**W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej**

Kod hasła jednorazowego:

**Zweryfikowano pozytywnie**

Powiąz

**Kody odzyskiwania**

Aby nie stracić dostępu do konta na wypadek utraty urządzenia z aplikacją uwierzytelniającą, wygenerowane zostały kody odzyskiwania jednorazowego użytku.  
Aby kontynuować, naciśnij przycisk **Drukuj** lub **Zapisz**. Wydruk/plk zachowaj w bezpiecznym miejscu.

Drukuj Zapisz

0d7lxut	
2zrsgld	
e073er5	
en6me6	
fxoqcjpw	

7. Po wydrukowaniu/zapisaniu kodów operator zapisuje konfigurację za pomocą klawisza **Zapisz konfigurację**. Po poprawnym zapisaniu pokaże się informacja **Poprawnie zapisano konfigurację**.

**W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej**

Kod hasła jednorazowego:

**Zweryfikowano pozytywnie**

Powiąz

**Kody odzyskiwania**

Aby nie stracić dostępu do konta na wypadek utraty urządzenia z aplikacją uwierzytelniającą, wygenerowane zostały kody odzyskiwania jednorazowego użytku.  
Aby kontynuować, naciśnij przycisk **Drukuj** lub **Zapisz**. Wydruk/plk zachowaj w bezpiecznym miejscu.

Drukuj Zapisz

0d7lxut1	
2zrsgldh	
e073er5v	
en6me6i	
fxoqcjpw	
h2h6jhh	
id5kpxuc	
ok6zsuht	
t0l13aexC	
vd5p72k	


Poprawnie zapisano konfigurację.

Wyjdź

Jeśli mechanizm logowania do portalu z wykorzystaniem mechanizmu MFA jest już aktywny to pojawiają się dodatkowe funkcje/linki.

## Zarządzanie uwierzytlenieniem wieloskładnikowym

▶ Powrót ▶ Pomoc

 Kod świadczeniodawcy:  
Nazwa świadczeniodawcy:  
Użytkownik:

Składnik	Informacja	Akcje
Konfiguracja uwierzytlenienia	Aktywny	Wyłącz Kod qr Nowa konfiguracja
Kody odzyskiwania	Aktywny	Podgląd Generuj nowe

### 1.2. WYŚWIETLENIE KODU QR


Wyświetlenie kodu QR może być przydatne w sytuacji, gdy operator chce używać więcej niż jednego telefonu do uwierzytelniania – generowania kodów jednorazowych. W takim przypadku, dla aplikacji zainstalowanej na kolejnym telefonie należy powtórzyć operacje powiązania aplikacji z kontem w Portalu. Należy ponownie wykonać skanowanie kodu QR lub wpisanie kodu ręcznie.

Operator może wyświetlić **Kod QR**.

Składnik	Informacja	Akcje
Konfiguracja uwierzytlenienia	Aktywny	Wyłącz Kod qr Nowa konfiguracja
Kody odzyskiwania	Aktywny	Podgląd Generuj nowe


## Administracja uwierzytelniania wieloskładnikowego (MFA)

▶ Powrót ▶ Pomoc

 Kod świadczeniodawcy:  
Nazwa świadczeniodawcy:  
Użytkownik:


### Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



Należy przepisać lub skopiować kod (sekret) do aplikacji generującej jednorazowe kody.



 Kod świadczeniodawcy:  
Nazwa świadczeniodawcy:  
Użytkownik:

### Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



### Ręczne dodanie konta

Wprowadź poniższe informacje ręcznie w aplikacji do uwierzytelniania:

Nazwa konta: Portal NFZ

Sekret: BWMH

Ukryj

## 1.2.1. KONFIGURACJA UWIERZYTELNIENIA WIELKOSKŁADNIKOWEGO (TOTP)

Aby potwierdzić zeskanowanie lub przepisanie kodu i przejść dalej należy wpisać token/kod 6 cyfrowy wygenerowany przez aplikację służącą do generowania tokenów TOTP a następnie kliknąć w **Powiąz**.

## Administracja uwierzytelniania wieloskładnikowego (MFA)

► Powrót ► Pomoc

 Kod świadczeniodawcy:  
Nazwa świadczeniodawcy:  
Użytkownik:

### Skanowanie kodu QR

Zeskanuj poniższy kod QR w aplikacji do uwierzytelniania.



Dodaj konto ręcznie

**W celu powiązania urządzenia do celów weryfikacyjnych proszę wygenerować kod w aplikacji zewnętrznej i wprowadzić w polu poniżej**

Kod hasła jednorazowego:

Powiąz

## 1.2.2. LISTA KODÓW ODZYSKIWANIA


**Kody odzyskiwania.**


Kody odzyskiwania służą do awaryjnego logowania w przypadku braku możliwości skorzystania z aplikacji do uwierzytelniania, niezbędnej do uwierzytelniania MFA (zgubienie lub uszkodzenie telefonu, przywrócenie urządzenia do stanu fabrycznego).

Są to kody jednorazowego użytku, które zaleca się wydrukować i schować w bezpieczne miejsce.

## Lista kodów odzyskiwania

► Powrót ► Pomoc


 Kod świadczeniodawcy:  
Nazwa świadczeniodawcy:  
Użytkownik:

 **Kody odzyskiwania**  
W celu wygenerowania nowych kodów odzyskiwania przejdź do panelu **Nowe kody odzyskiwania**

[Drukuj](#) [Zapisz](#)

Kod odzyskiwania	Użycie
2n7sa	Nie wykorzystany
33tpu	Nie wykorzystany
4wkst	Nie wykorzystany
5w9fk	Nie wykorzystany
ax25v	Nie wykorzystany
o82f7	Nie wykorzystany
s2hbg	Nie wykorzystany
sk418	Nie wykorzystany
snmjv	Nie wykorzystany
stv76	Nie wykorzystany

Aby wygenerować nowe kody odzyskiwania należy przejść do strony **Zarządzanie uwierzytelnieniem wielokładnikowym** i skorzystać z linku **Generuj nowe** lub posłużyć się linkiem **Nowe kody odzyskiwania**.

 **Kody odzyskiwania**  
W celu wygenerowania nowych kodów odzyskiwania przejdź do panelu **Nowe kody odzyskiwania**

[Drukuj](#) [Zapisz](#)

Kody, które zostały wykorzystane są oznaczone jako **Wykorzystane** oraz dodatkowo przekreślone.

## Lista kodów odzyskiwania

► Powrót ► Pomoc



Kod świadczeniodawcy:  
Nazwa świadczeniodawcy:  
Użytkownik:



### Kody odzyskiwania

W celu wygenerowania nowych kodów odzyskiwania przejdź do panelu **Nowe kody odzyskiwania**

Drukuj

Zapisz

Kod odzyskiwania	Użycie
1lsvyuwaynv	Nie wykorzystany
42avcqtuh3jc	Nie wykorzystany
6axze611uluv	Wykorzystany
7qjmnzd1rd9	Nie wykorzystany
9je7duvu6zei	Wykorzystany
acjq6dkz0pi	Nie wykorzystany
k9j9xby3d8l0	Nie wykorzystany
pr1zz3ecxej1	Nie wykorzystany
v5dod80r5os	Nie wykorzystany
zaw62t6nfst9	Nie wykorzystany

**Uwaga:** Jeżeli z jakiegoś powodu, kody odzyskiwania zostaną przez osobę nieuprawnioną przechwycone, należy jak najszybciej anulować kody poprzez wygenerowanie nowych, które je nadpiszą.

### 1.2.3. GENEROWANIE NOWYCH KODÓW ODZYSKIWANIA

Aby wygenerować nowe kody odzyskiwania należy skorzystać z linku **Generuj nowe** na stronie **Zarządzanie uwierzytelnieniem wieloskładnikowym**.

Składnik	Informacja	Akcje
Konfiguracja uwierzytelnienia	Aktywny	Wyłącz Kod qr Nowa konfiguracja
Kody odzyskiwania	Aktywny	Podgląd Generuj nowe

Operator zostanie poproszony o potwierdzenie tożsamości poprzez wpisanie hasła do Portalu Świadczeniodawcy.

### Potwierdź tożsamość do Portalu Świadczeniodawcy



Kod świadczeniodawcy:  
Użytkownik:



Hasło:

Hasło

Zaloguj


Po wpisaniu hasła otworzy się strona z wygenerowanymi kodami odzyskiwania.


Przycisk **Zapisz**, zapisuje kody odzyskiwania.

Przycisk **Drukuj** umożliwi wydrukowanie kodów odzyskiwania.

### Generowanie nowych kodów odzyskiwania

► Powrót ► Pomoc

 Kod świadczeniodawcy:  
Nazwa świadczeniodawcy:  
Użytkownik:

 **Kody odzyskiwania**

Aby nie stracić dostępu do konta na wypadek utraty urządzenia z aplikacją uwierzytelniającą, wygenerowane zostały kody odzyskiwania jednorazowego użytku.  
Aby kontynuować, naciśnij przycisk **Drukuj** lub **Zapisz**. Wydruk/plik zachowaj w bezpiecznym miejscu. Po zapisaniu/wydrukowaniu pojawi się przycisk **Zapisz konfigurację**, użyj go w celu zapisania nowych kodów.

[Drukuj](#) [Zapisz](#)

Kod odzyskiwania	Użycie
02hp6ini0	Niewykorzystany
1xwo1b1l	Niewykorzystany
48xilas5t	Niewykorzystany
bd2z9e	Niewykorzystany
eu1ms	Niewykorzystany
fdqjevcki	Niewykorzystany
gs86kzqh	Niewykorzystany
kfnt1e8	Niewykorzystany
x39fro9p	Niewykorzystany
xa0a4:	Niewykorzystany

Po zapisaniu lub wydrukowaniu kodów odzyskiwania należy zapisać konfigurację za pomocą przycisku **Zapisz konfigurację**.

Kod odzyskiwania	Użycie
1mcp3:	Niewykorzystany
1p6npy	Niewykorzystany
6p2bf8	Niewykorzystany
7du1ipe	Niewykorzystany
8s007c	Niewykorzystany
cx0xjp	Niewykorzystany
f5ycgq	Niewykorzystany
ieg8pq1	Niewykorzystany
rf9v84t	Niewykorzystany
riblrwfi	Niewykorzystany

[Zapisz konfigurację](#) [Wyjdź](#)