

Konfiguracja uwierzytelniania dwuskładnikowego (2FA) w serwisie pocztowym pocztapro.cyfronet.pl

Aby zwiększyć bezpieczeństwo swojego konta pocztowego, możesz włączyć uwierzytelnianie dwuskładnikowe (2FA). Poniżej znajdziesz instrukcję krok po kroku jak włączyć dodatkowe zabezpieczenie swojego konta w serwisie pocztowym pocztapro.cyfronet.pl zarówno przy użyciu aplikacji mobilnej typu „authenticator” jak i przy pomocy dodatkowego adresu e-mail.

Spis treści

1.	Instalacja aplikacji mobilnej do uwierzytelniania dwuskładnikowego	2
1.1.	Wybór aplikacji mobilnej do uwierzytelniania dwuskładnikowego (2FA)	2
1.2.	Instalacja aplikacji mobilnej na smartfonie	2
2.	Włączenie uwierzytelniania dwuskładnikowego poprzez aplikację mobilną w serwisie pocztowym pocztapro.cyfronet.pl	3
2.1.	Konfiguracja ustawień.....	3
2.2.	Pierwsze uruchomienie oraz konfiguracja ogólna na przykładzie popularnych aplikacji mobilnych do uwierzytelniania dwuskładnikowego	5
3.	Włączenie uwierzytelniania dwuskładnikowego poprzez dodatkowy adres e-mail w serwisie pocztowym pocztapro.cyfronet.pl	14
3.1.	Konfiguracja ustawień.....	14
3.2.	Codzienne korzystanie z 2FA poprzez aplikację mobilną (podstawowy scenariusz) ...	17
3.3.	Codzienne korzystanie z 2FA poprzez dodatkowy adres e-mail (podstawowy scenariusz)	18
3.4.	Sytuacje awaryjne	19

1. Instalacja aplikacji mobilnej do uwierzytelniania dwuskładnikowego

1.1. Wybór aplikacji mobilnej do uwierzytelniania dwuskładnikowego (2FA)

Aby móc korzystać z uwierzytelniania dwuskładnikowego (2FA) w serwisie pocztowym pocztapro.cyfronet.pl, niezbędna jest instalacja aplikacji mobilnej typu „authenticator”, która będzie generować jednorazowe kody uwierzytelniające. Najczęściej używane aplikacje mobilne to:

- Microsoft Authenticator
- Google Authenticator

1.2. Instalacja aplikacji mobilnej na smartfonie

Otwórz sklep z aplikacjami na swoim smartfonie. W zależności od używanego systemu są to aplikacje:

- ✓ Google Play (dla Androida)
- ✓ App Store (dla iPhone)

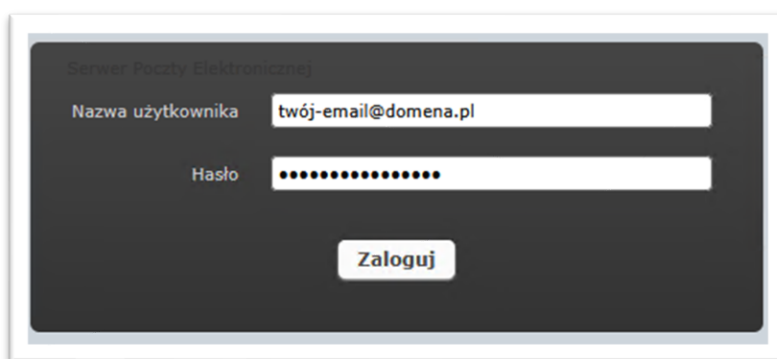
Następnie:

- Wyszukaj aplikację mobilną typu 2FA w sklepie z aplikacjami, wpisując np. Microsoft Authenticator.
- Kliknij „Zainstaluj” i poczekaj na zakończenie instalacji.
- Po zakończeniu instalacji uruchom aplikację – możesz zostać poproszony o skonfigurowanie zabezpieczeń (np. kod PIN lub biometryka) przy pierwszym uruchomieniu.

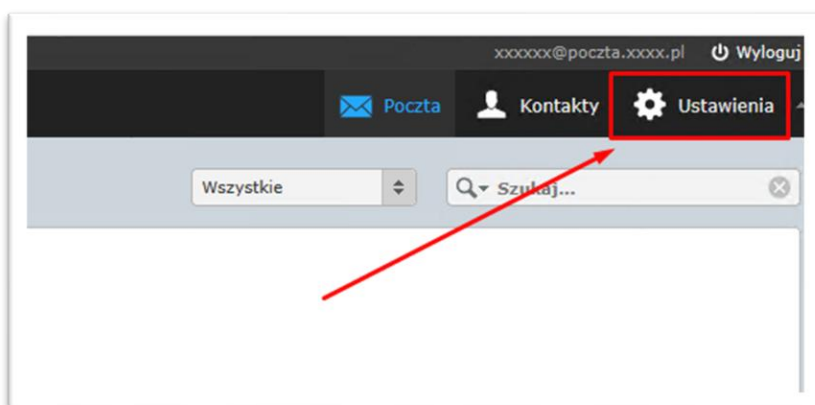
2. Włączenie uwierzytelniania dwuskładnikowego poprzez aplikację mobilną w serwisie pocztowym pocztapro.cyfronet.pl

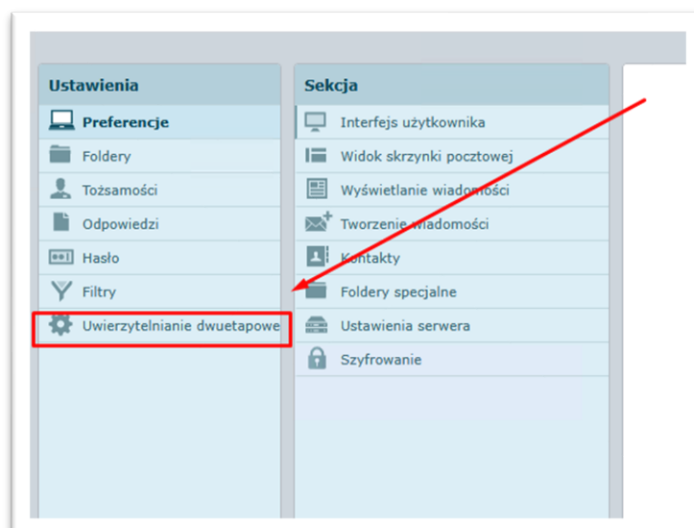
2.1. Konfiguracja ustawień

Po zalogowaniu się do serwisu pocztowego przez przeglądarkę, kliknij „Ustawienia”, a następnie wybierz zakładkę „Uwierzytelnianie dwuetapowe”.



Ustawienia znajdują się w prawym górnym rogu przeglądarki:





Następnie na ekranie urządzenia powinien pojawić się następujący wybór:

Włącz uwierzytelnianie dwuetapowe

Uwierzytelnianie dwuetapowe chroni Twoje konto przed nieautoryzowanym dostępem. Wybierz metodę weryfikacji, której chcesz używać i kliknij Włącz aby rozpocząć proces konfiguracji.



Aplikacja mobilna

Używaj aplikacji mobilnej, żeby generować kody weryfikacyjne.

Włącz



Email

Używaj wiadomości e-mail w celu uzyskania kodów weryfikacyjnych.

Włącz

W dalszej części instrukcji opisana zostanie również procedura dla opcji „Email”.

Wybieramy opcję Aplikacja Mobilna, klikamy „Włącz”. Potwierdzamy hasło do konta i klikamy przycisk „Kontynuuj”.

Potwierdź hasło

Aby zmienić ustawienia lub wyświetlić poufne informacje, musisz potwierdzić hasło do konta.

.....

Kontynuuj **Anuluj**

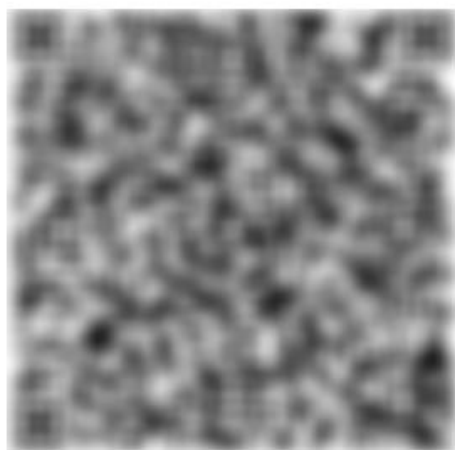
Następnie przechodzimy do konfiguracji uwierzytelniania poprzez aplikację mobilną. Na naszym ekranie pojawi się krótka instrukcja oraz kod QR, który będziemy skanować przez aplikację 2FA, którą już pobraliśmy.



Konfiguracja uwierzytelniania poprzez aplikację mobilną

W [App Store](#) lub [Google Play](#) poszukaj "TOTP authenticator" i zainstaluj jedną z najwyżej wyświetlonych darmowych aplikacji, takich jak: 2FA Authenticator, Microsoft Authenticator, Google Authenticator.

Skonfiguruj aplikację skanując kod QR lub wprowadzając ręcznie kod konfiguracji.



REFKEASROXUI37IR5M375VUW

Następna

Anuluj

Przejdźmy więc do aplikacji. Omówimy konfigurację zarówno dla aplikacji Microsoft Authenticator jak i Google Authenticator.

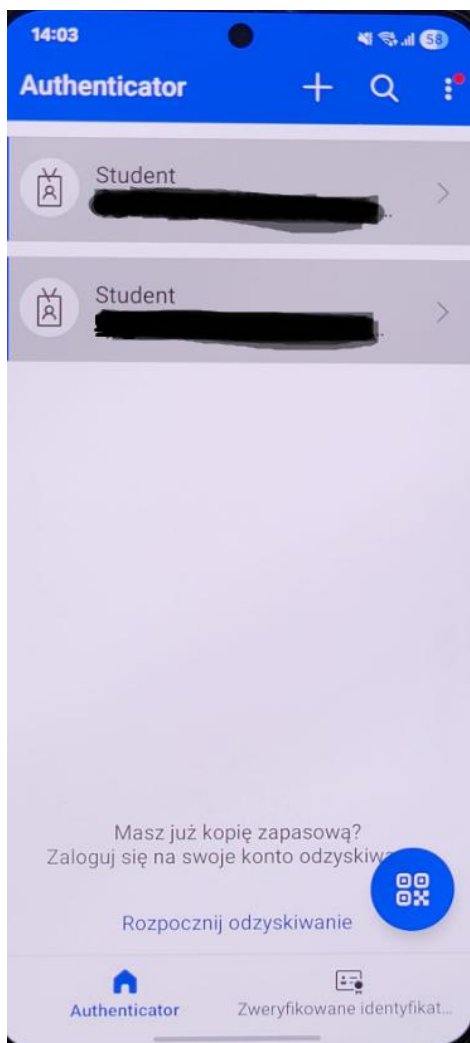
2.2. Pierwsze uruchomienie oraz konfiguracja ogólna na przykładzie popularnych aplikacji mobilnych do uwierzytelniania dwuskładnikowego

2.2.3. Microsoft Authenticator

Otwórz aplikację Microsoft Authenticator na swoim smartfonie.

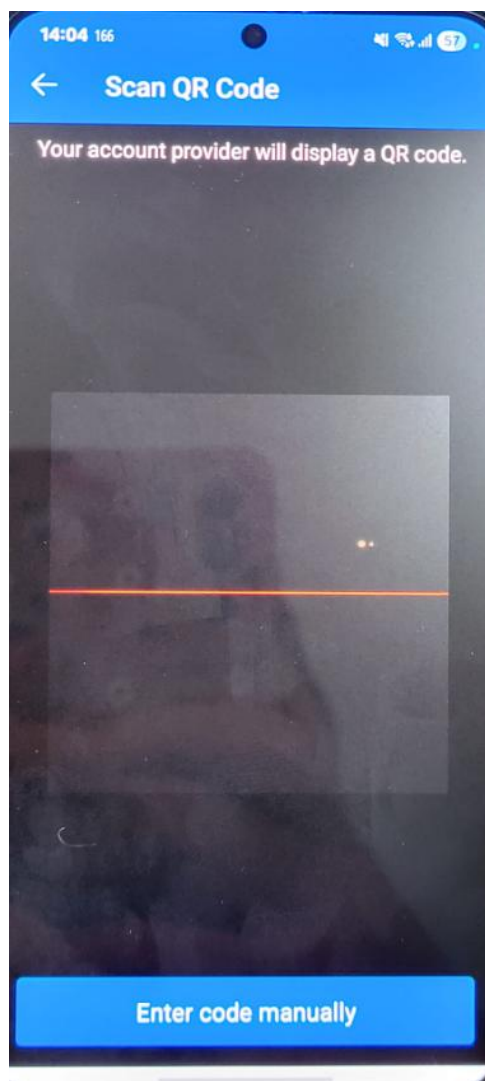
Jeśli uruchamiasz ją po raz pierwszy, przejdź przez wstępną konfigurację – ustaw zabezpieczenia dostępu do aplikacji (np. PIN, odcisk palca, rozpoznawanie twarzy).

Gdy znajdziesz się w głównym widoku aplikacji, kliknij ikonę „+” (zwykle w górnej części ekranu), aby dodać nowe konto. Może być to również ikona kodu QR, najczęściej występująca w prawym dolnym rogu aplikacji.

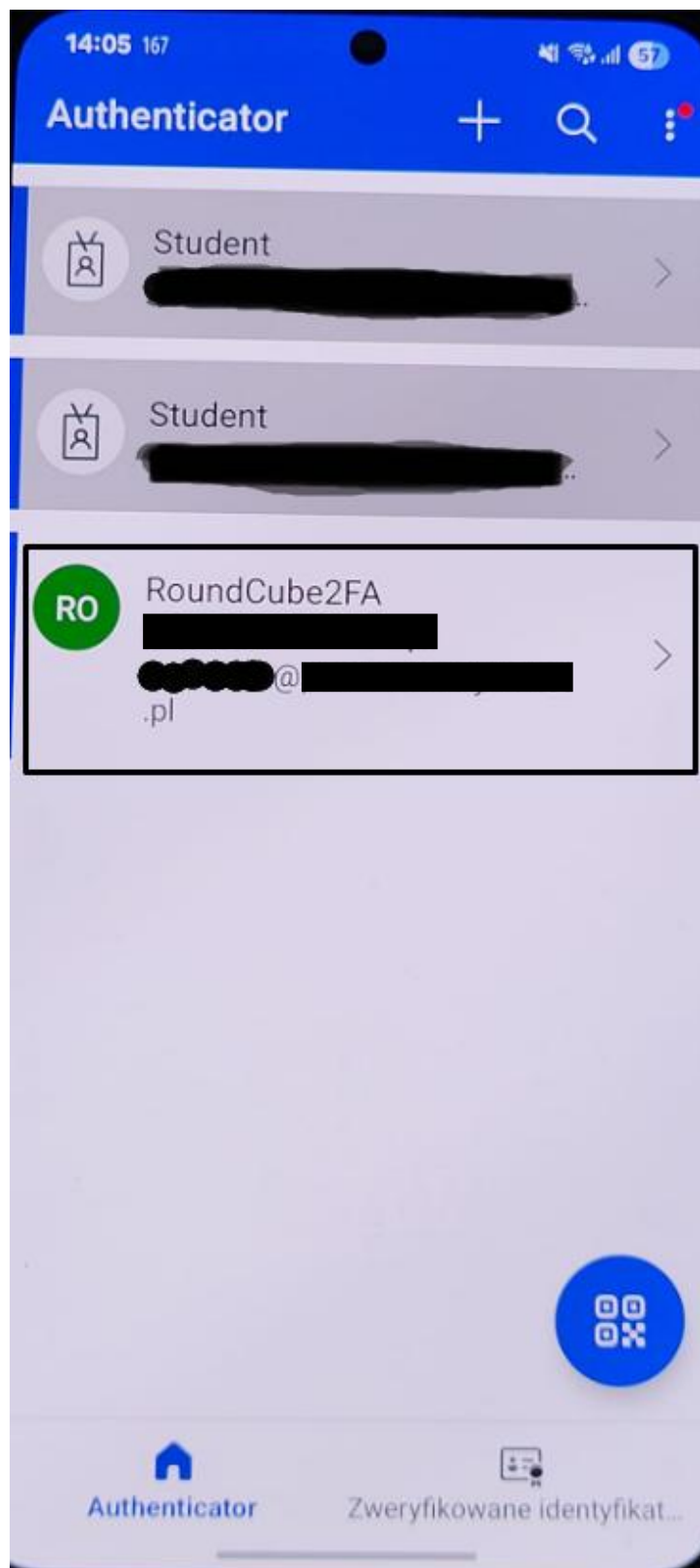


Jeśli aplikacja poprosi o dostęp do aparatu – zezwól na to, aby możliwe było zeskanowanie kodu.

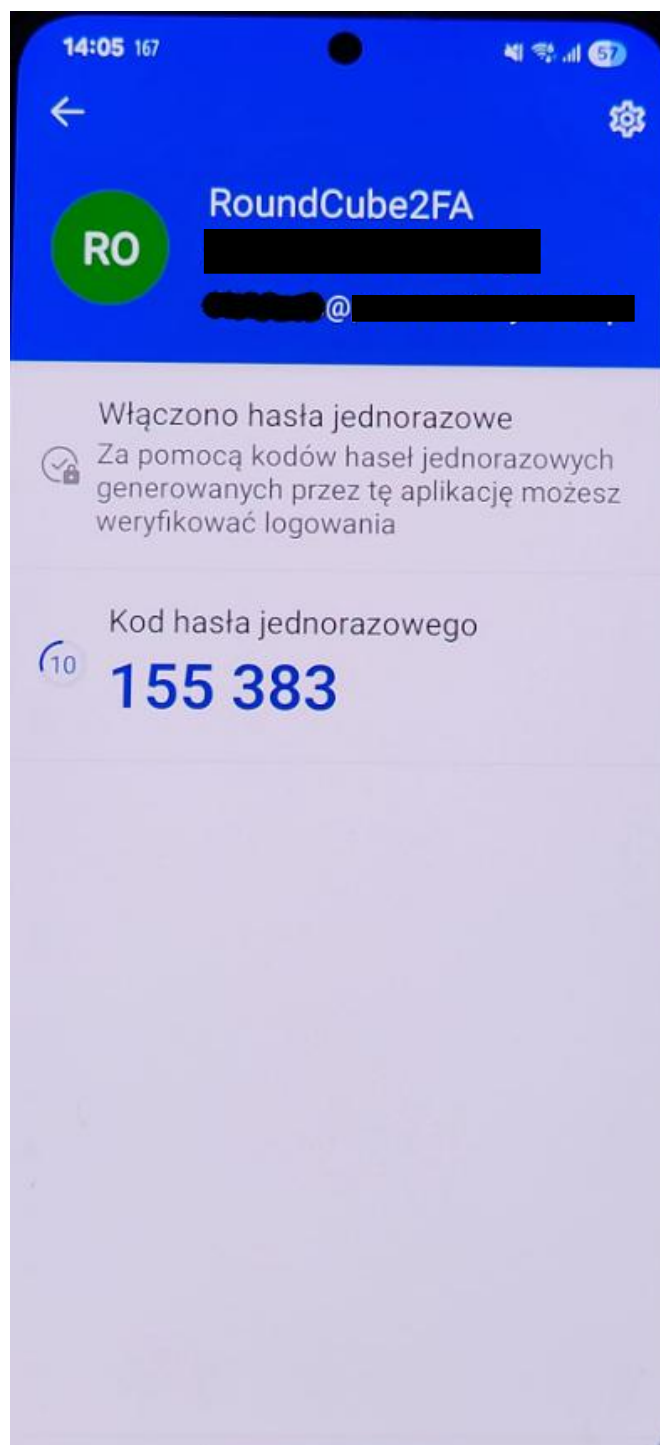
Skieruj aparat telefonu na kod QR wyświetlony na ekranie komputera – aplikacja automatycznie doda konfigurację.



Sprawdź nazwę dodawanego konta oraz dane

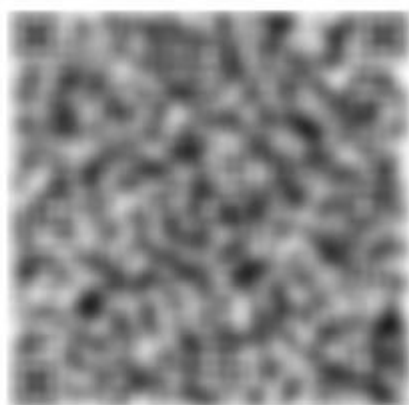


Po wejściu w dodany serwis/usługę na ekranie smartfona pojawi się sześciocyfrowy kod – jest to Twój kod jednorazowy.



Wróćmy teraz do naszego serwisu pocztowego. Kliknijmy w przycisk „Następna”:

ację skanując kod QR lub wprowadzając ręcznie kod konfiguracji.



REFKEASROXUI37IR5M375VUW



Następna

Anuluj

W tym miejscu zostaniemy poproszeni o przepisanie kodu z aplikacji celem weryfikacji oraz sfinalizowania procesu dodawania dwuskładnikowego uwierzytelniania poprzez aplikację mobilną.



Konfiguracja uwierzytelniania poprzez aplikację mobilną

Podaj kod weryfikacyjny wygenerowany przez Twoją aplikację.

Zakończ

Anuluj

Wpisujemy kod oraz klikamy „Zakończ”.

Od teraz nasze konto posiada już aktywne uwierzytelnianie dwuskładnikowe.

Poniżej możemy zauważyć następującą sekcję:



Kody zapasowe (10)

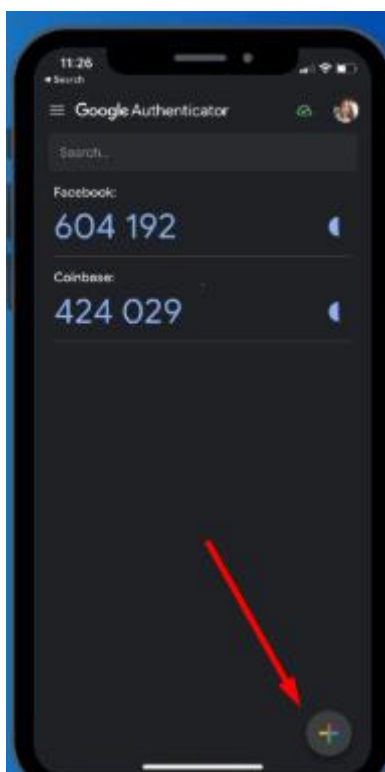
Kody zapasowe mogą być użyte zamiast standardowych kodów weryfikacyjnych w sytuacjach awaryjnych. Skopiuj je i przechowaj w bezpiecznym miejscu. Każdy z kodów zapasowych może być użyty tylko raz.

[Pokaż kody zapasowe](#) [Wygeneruj nowe kody zapasowe](#)

Są to tzw. kody zapasowe, czyli jednorazowe hasła/klucze, dzięki którym możemy uzyskać dostęp do konta w sytuacji gdy utracimy urządzenie do dwuskładnikowej weryfikacji (np. telefon). Warto zapisać kilka kodów na przyszłość, by w sytuacji awaryjnej nie utracić dostępu do swojego konta.

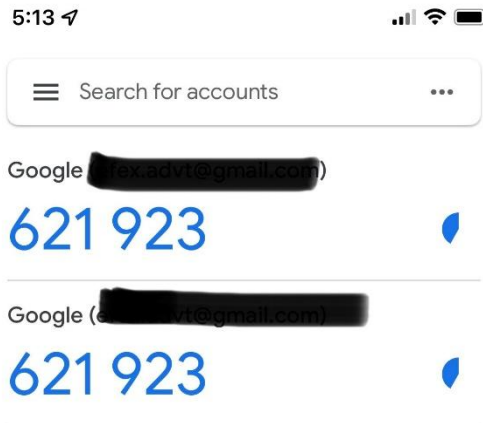
2.2.4. Google Authenticator

Analogicznie jak w przypadku aplikacji Microsoft Authenticator, w prawym dolnym rogu wybieramy opcję dodania nowej usługi:



Następnie wybieramy „Scan a QR code” lub „Skanuj kod QR” i skanujemy smartfonem kod QR z ekranu komputera





Po zeskanowaniu kodu, usługa zostanie dodana do listy i możemy korzystać już z generowanych kodów. Wróćmy teraz z powrotem do serwisu pocztowego.



Konfiguracja uwierzytelniania poprzez aplikację mobilną

Podaj kod weryfikacyjny wygenerowany przez Twoją aplikację.

Zakończ

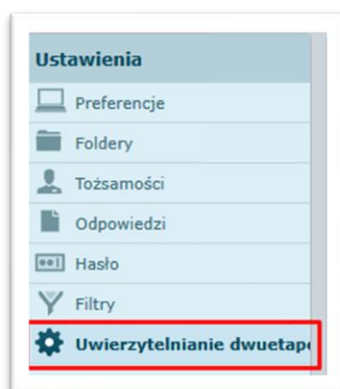
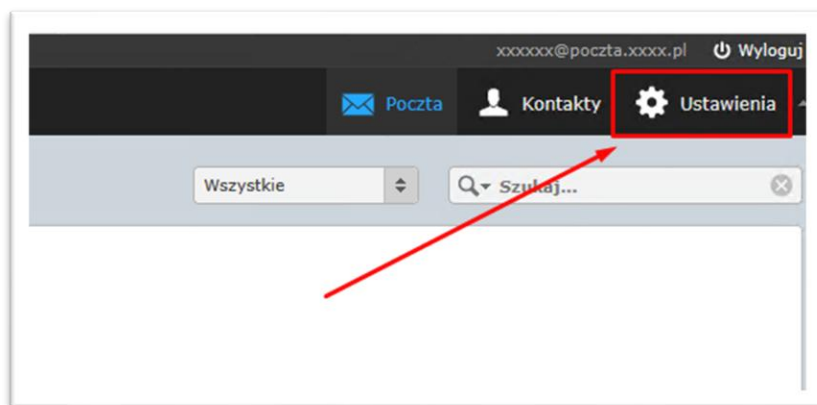
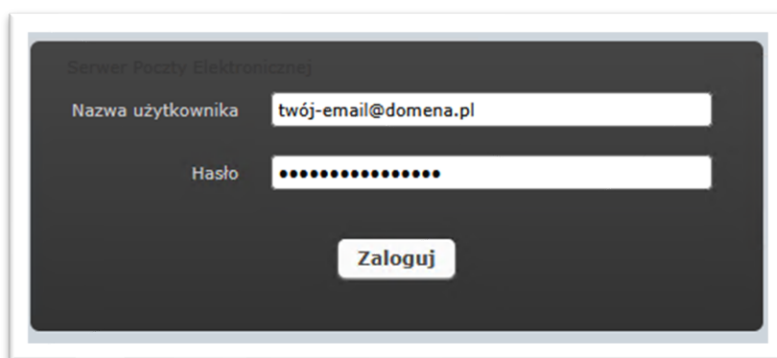
Anuluj

Analogicznie jak w przypadku poprzedniej aplikacji - wpisujemy kod z aplikacji mobilnej oraz klikamy „Zakończ”.

3. Włączenie uwierzytelniania dwuskładnikowego poprzez dodatkowy adres e-mail w serwisie pocztowym pocztapro.cyfronet.pl

3.1. Konfiguracja ustawień

Po zalogowaniu się do serwisu pocztowego przez przeglądarkę, kliknij „Ustawienia”, a następnie wybierz zakładkę „Uwierzytelnianie dwuetapowe”.



Następnie na ekranie urządzenia powinien pojawić się następujący wybór:

Włącz uwierzytelnianie dwuetapowe

Uwierzytelnianie dwuetapowe chroni Twoje konto przed nieautoryzowanym dostępem. Wybierz metodę weryfikacji, której chcesz używać i kliknij Włącz aby rozpocząć proces konfiguracji.

Aplikacja mobilna
Używaj aplikacji mobilnej, żeby generować kody weryfikacyjne.

Email
Używaj wiadomości e-mail w celu uzyskania kodów weryfikacyjnych.

Włącz

Włącz

Wybieramy opcję Email, klikamy „Włącz”. Potwierdzamy hasło do konta i klikamy przycisk „Kontynuuj”.

Potwierdź hasło

Aby zmienić ustawienia lub wyświetlić poufne informacje, musisz potwierdzić hasło do konta.

.....

Kontynuuj Anuluj

Następnie przechodzimy do konfiguracji uwierzytelniania poprzez E-mail.

Konfiguracja uwierzytelniania poprzez e-mail

Podaj adres e-mail, na który program będzie wysyłać kody weryfikacyjne.

.....

Następna Anuluj

Zgodnie z poleceniem wyświetlanym na ekranie podajemy adres e-mail, na który program będzie wysyłać kody weryfikacyjne. Następnie klikamy w przycisk „Następna”.

Konfiguracja uwierzytelniania poprzez e-mail

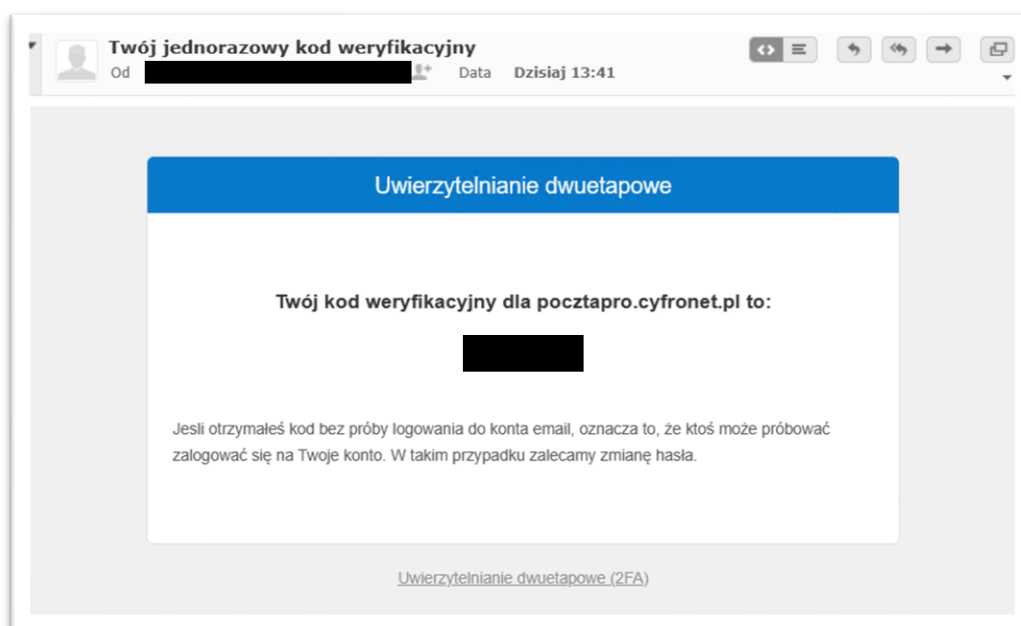
Wprowadź kod weryfikujący, który został wysłany na Twój adres e-mail.

.....

Zakończ Anuluj

Zgodnie z informacją wyświetlaną na ekranie, jesteśmy zobligowani do podania kodu weryfikującego jaki został przesłany na podany przez nas adres e-mail.

Oto przykładowa wiadomość z kodem weryfikującym:



Zgodnie z poleceniem, przepisujemy kod z e-maila do pola, a następnie klikamy „Zakończ”.



Konfiguracja uwierzytelniania poprzez e-mail

Wprowadź kod weryfikujący, który został wysłany na Twój adres e-mail.

Zakończ

Anuluj

Jeżeli podany kod jest prawidłowy użytkownik powinien otrzymać następujący komunikat, który potwierdza, że proces dodawania uwierzytelniania dwuetapowego został przeprowadzony pomyślnie:

 Uwierzytelnianie dwuetapowe jest włączone.

Wyłącz

Aktywne metody uwierzytelnianie dwuetapowego



Email (Domyślna)

Kody weryfikacyjne będą wysyłane na: [redacted]*****.pl.

[Usuń metodę](#)



Kody zapasowe (10)

Kody zapasowe mogą być użyte zamiast standardowych kodów weryfikacyjnych w sytuacjach awaryjnych. Skopiuj je i przechowaj w bezpiecznym miejscu. Każdy z kodów zapasowych może być użyty tylko raz.

[Pokaż kody zapasowe](#)

[Wygeneruj nowe kody zapasowe](#)

Dodaj metodę zapasową



Aplikacja mobilna

Używaj aplikacji mobilnej, żeby generować kody weryfikacyjne.

Włącz

W tym momencie konto użytkownika jest już chronione przy pomocy uwierzytelniania dwuskładnikowego opartego o dodatkowy kod 6-cyfrowy przesyłany na podany przez użytkownika adres e-mail.

3.2. Codzienne korzystanie z 2FA poprzez aplikację mobilną (podstawowy scenariusz)

Podczas każdej próby logowania do systemu z aktywnym 2FA (aplikacja mobilna):

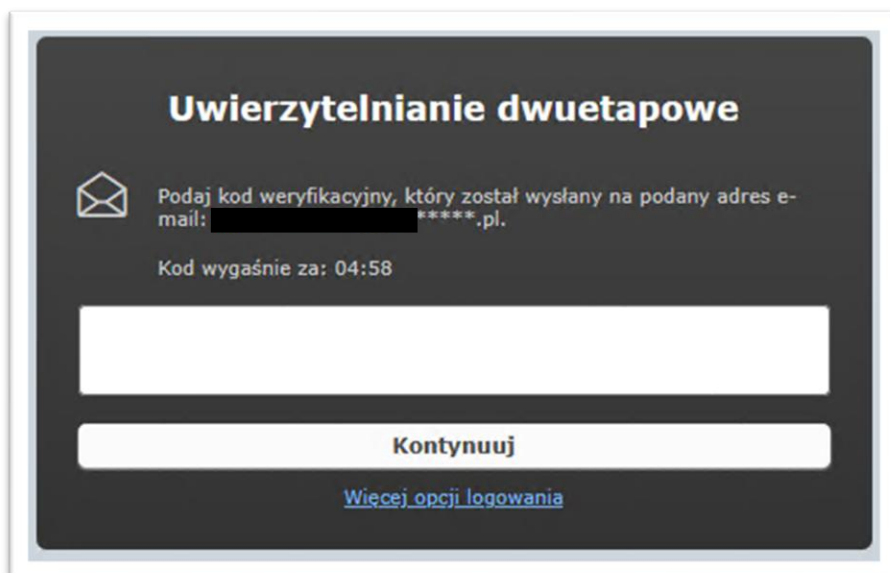
- Otwórz serwis pocztowy pocztapro.cyfronet.pl
- Wpisz swój adres e-mail (login) oraz hasło i kliknij „Zaloguj”
- Otrzymasz komunikat z prośbą o podanie 6-cyfrowego kodu z aplikacji mobilnej
- Odblokuj telefon.
- Uruchom aplikację typu 2FA np. Authenticator.
- Odszukaj odpowiednią konfigurację (nazwa systemu/konta/serwisu).
- Przepisz aktualny 6-cyfrowy kod z aplikacji do formularza logowania w przeglądarce.
- Naciśnij przycisk „Kontynuuj”

UWAGA: Kod jest ważny tylko przez krótki czas, dlatego wpisz go jak najszybciej po jego wygenerowaniu. Nigdy nie udostępniaj kodu osobom trzecim!

3.3. Codzienne korzystanie z 2FA poprzez dodatkowy adres e-mail (podstawowy scenariusz)

Podczas każdej próby logowania do systemu z aktywnym 2FA (dod. e-mail):

- Otwórz serwis pocztowy pocztapro.cyfronet.pl
- Wpisz swój adres e-mail (login) oraz hasło i kliknij „Zaloguj”
- Otrzymasz następujący komunikat:



Uwierzytelnianie dwuetapowe

Podaj kod weryfikacyjny, który został wysłany na podany adres e-mail: [redacted]****.pl.

Kod wygaśnie za: 04:58

[Redacted input field]

Kontynuuj

[Więcej opcji logowania](#)

- Otwórz skrzynkę pocztową (poprzez serwis www lub klienta pocztowego np. Thunderbird) obsługującą dodatkowy adres e-mail podany do konfiguracji uwierzytelniania dwuskładnikowego
- Przepisz 6-cyfrowy kod z otrzymanej wiadomości e-mail do pola logowania na serwisie pocztapro.cyfronet.pl
- Naciśnij przycisk „Kontynuuj”

UWAGA: Kod jest ważny tylko przez określony czas (5 minut), dlatego wpisz go jak najszybciej po jego otrzymaniu. Nigdy nie udostępniaj kodu osobom trzecim!

3.4. Sytuacje awaryjne

W razie utraty dostępu do aplikacji uwierzytelniającej (np. zgubiony lub zresetowany telefon), możliwe są różne scenariusze awaryjne:

Wskazówki bezpieczeństwa:

- Zapisz kody awaryjne w bezpiecznym miejscu (np. zaszyfrowanym pliku) i zawsze pamiętaj gdzie możesz je odnaleźć.
- Nie udostępniaj ich innym osobom.
- Nie instaluj aplikacji typu „authenticator” na współdzielonych urządzeniach.
- Jeśli zmienisz telefon – pamiętaj, by przenieść konfigurację aplikacji uwierzytelniającej przed zresetowaniem starego urządzenia.

UWAGA: Kody generują się automatycznie po wejściu w aplikację mobilną. Częstym i obserwowanym zjawiskiem jest również sytuacja, w której użytkownik wpisuje kod z aplikacji, który wygaśnie za kilka sekund. Może to prowadzić do komunikatów typu „Nieprawidłowy kod uwierzytelniający”. Proszę zwrócić uwagę, że nie liczy się czas w którym przepisujemy kod z urządzenia uwierzytelniającego, lecz faktycznie kiedy go wyślemy np. poprzez formularz logowania.

PORADA: Aby uniknąć potencjalnego wysyłania wygaśniętego już kodu z aplikacji, zaleca się aby wpisywać wyłącznie kody o dłuższym czasie ważności np. od 20 sekund i więcej. Pozwoli to uniknąć tego typu sytuacji.