

Skonfiguruj uwierzytelnianie dwuskładnikowe (2FA) z SALESmanago

Spis treści

<u>1. Czym jest 2FA i dlaczego jest kluczowe dla bezpieczeństwa?</u>	<u>2</u>
<u>2. Konfiguracja 2FA</u>	<u>3</u>
<u>Krok 1. Połącz swoje konto SALESmanago z aplikacją uwierzytelniającą</u>	<u>4</u>
<u>A. Instrukcje dla Google Authenticator</u>	<u>5</u>
<u>B. Instrukcje dla Microsoft Authenticator</u>	<u>8</u>
<u>Krok 2. Wygeneruj pierwszy kod dla swojego konta SALESmanago</u>	<u>12</u>
<u>Krok 3. Zaloguj się do swojego konta SALESmanago</u>	<u>13</u>
<u>3. Często zadawane pytania (FAQ)</u>	<u>15</u>

1. Czym jest 2FA i dlaczego jest kluczowe dla bezpieczeństwa?

Uwierzytelnianie dwuskładnikowe (2FA) to mechanizm bezpieczeństwa, w ramach którego użytkownik, aby uzyskać dostęp do swojego konta, musi przejść dwuetapowy proces weryfikacji:

- **Krok 1** to podanie standardowych danych logowania (login/adres e-mail i hasło).
- **Krok 2** to podanie szybko wygasającego kodu dostarczanego na urządzenie mobilne użytkownika.

2FA zapewnia dodatkową warstwę ochrony przed nieautoryzowanym dostępem do twoich danych i operacji.

W świecie, w którym cyberzagrożenia są coraz bardziej wyrafinowane, poleganie wyłącznie na hasłach nie jest już wystarczające. 2FA staje się niezbędnym rozwiązaniem dla firm, które chcą zapewnić maksymalne bezpieczeństwo swoich zasobów cyfrowych. Ten dwuetapowy proces nie tylko minimalizuje ryzyko związane z typowymi zagrożeniami, takimi jak kradzież hasła czy ataki phishingowe, ale także znacznie utrudnia włamanie się na konto metodami “siłowymi”.

Dzięki 2FA, nawet jeśli jeden czynnik uwierzytelniania (hasło) zostanie ujawniony, dodatkowa warstwa weryfikacji (kod dostarczany na urządzenie mobilne SMS-em lub za pośrednictwem aplikacji uwierzytelniającej) sprawia, że nieautoryzowany dostęp pozostaje dla atakującego dużym wyzwaniem.

Poprzez wdrożenie 2FA zwiększasz ogólne bezpieczeństwo swojego konta i chronisz poufne informacje przed ujawnieniem nieautoryzowanym stronom trzecim. Dzięki temu zapewniasz spokój ducha sobie, swojemu zespołowi i całej firmie.

2. Konfiguracja 2FA

Uwierzytelnianie dwuskładnikowe jest łatwe do skonfigurowania – wszystko, czego potrzebujesz, to twoje dane logowania do SALESmanago oraz twój smartfon.

Jeżeli administrator twojego konta SALESmanago aktywował dla ciebie uwierzytelnianie dwuskładnikowe, zobaczysz następujący komunikat z prośbą o skonfigurowanie drugiego kroku procesu uwierzytelniania:

Skonfiguruj uwierzytelnianie dwuskładnikowe (2FA)

1. Otwórz aplikację uwierzytelniającą i wprowadź kod alfanumeryczny lub zeskanuj kod QR

Możesz użyć dowolnej aplikacji uwierzytelniającej, na przykład Google Authenticator lub Microsoft Authenticator.

Wprowadź kod alfanumeryczny w aplikacji uwierzytelniającej

A327MNRY4EMJXDUA

Zeskanuj kod QR za pomocą aplikacji uwierzytelniającej



2. Zweryfikuj konfigurację

Kod weryfikacyjny

Anuluj

Aktywuj

Może się to zdarzyć podczas trwającej sesji SALESmanago lub przy następnej próbie zalogowania.

Komunikat zawiera instrukcje krok po kroku, które zostały opisane bardziej szczegółowo na kolejnych stronach tego dokumentu.

Krok 1. Połącz swoje konto SALESmanago z aplikacją uwierzytelniającą

Aby skonfigurować 2FA dla swojego konta, musisz pobrać aplikację uwierzytelniającą na swój smartfon i połączyć ją ze swoim kontem SALESmanago.

Aplikacja uwierzytelniająca to rodzaj oprogramowania, które umożliwia wdrożenie oraz korzystanie z uwierzytelniania dwuskładnikowego (2FA). Aplikacja generuje ograniczony czasowo, zwykle sześciocyfrowy kod, znany jako *Time-based One-Time Password* (ograniczone czasowo jednorazowe hasło; TOTP), który należy podać podczas procesu logowania obok standardowego hasła.

Twoja Organizacja prawdopodobnie określi, z jakiej aplikacji powinni korzystać jej pracownicy. Aplikacje uwierzytelniające zalecane przez SALESmanago to Google Authenticator oraz Microsoft Authenticator. Poniżej znajdziesz szczegółowy przewodnik dla obu tych aplikacji.

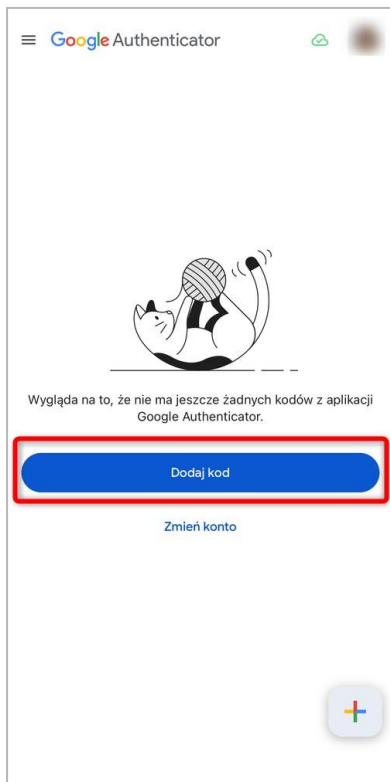
A. Instrukcje dla Google Authenticator

Na swoim smartfonie przejdź do sklepu [Apple Store](#) lub [Google Play Store](#) i pobierz aplikację Google Authenticator.

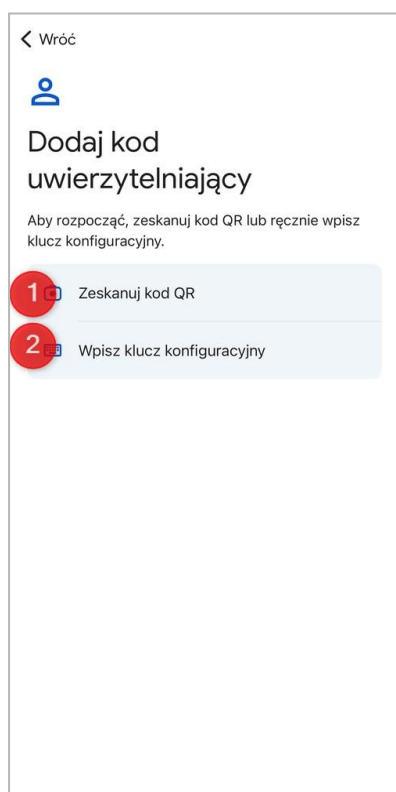
Otwórz aplikację i kliknij **Rozpocznij**. Zobaczysz następujący ekran:



W zależności od instrukcji wydanych przez twoją Organizację, kliknij **Zaloguj się [1]** i wybierz z listy konto Google Workspace, lub kliknij **Użyj aplikacji Authenticator bez logowania [2]**.



Jeżeli korzystasz z aplikacji po raz pierwszy, nie będziesz mieć na liście żadnych kodów. Kliknij **Dodaj kod**, aby połączyć Google Authenticator ze swoim kontem SALESmanago i rozpocząć generowanie kodów TOTP wymaganych przy logowaniu.



Możesz połączyć Google Authenticator ze swoim kontem SALESmanago na dwa sposoby:

- poprzez **zeskanowanie swojego indywidualnego kodu QR [1]** lub
- poprzez **wpisanie indywidualnego klucza konfiguracyjnego [2]**.

Zarówno kod QR, jak i klucz konfiguracyjny ("kod alfanumeryczny") są podane w komunikacie wyświetlanym na platformie SALESmanago, informującym o konieczności skonfigurowania 2FA (zob. strona 3 powyżej).

WAŻNE: Nigdy nie zachowuj kodu QR ani kodu alfanumerycznego w żadnej formie, w szczególności:

- nie rób zdjęć ani zrzutów ekranu,
- nie drukuj kodów,
- nie zapisuj kodu alfanumerycznego na kartce, w zeszycie, itp.,
- nie skanuj kodów za pomocą aplikacji innej niż aplikacja uwierzytelniająca.

Wszystkie wyżej wymienione działania uważane są za naruszenie bezpieczeństwa.

Niezależnie od wybranej metody (skanowanie/wpisanie kodu), aplikacja zwróci **kod weryfikacyjny**, który należy wprowadzić w SALESmanago. Aby ukończyć konfigurację, **przejdź do Kroku 2** (strona 12 poniżej).

B. Instrukcje dla Microsoft Authenticator

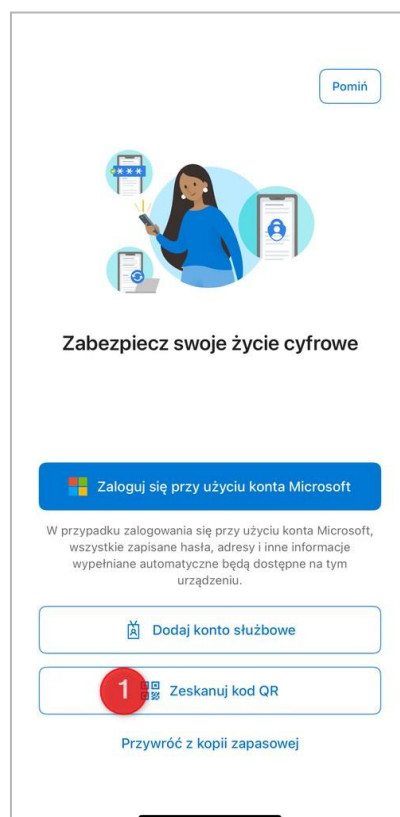
Na smartfonie przejdź do sklepu [Apple Store](#) lub [Google Play Store](#) i pobierz aplikację Microsoft Authenticator.

Otwórz aplikację i kliknij **Akceptuj**, aby potwierdzić warunki. Następnie upewnij się, że przełącznik pozwalający na udostępnianie danych użycia aplikacji jest wyłączony.



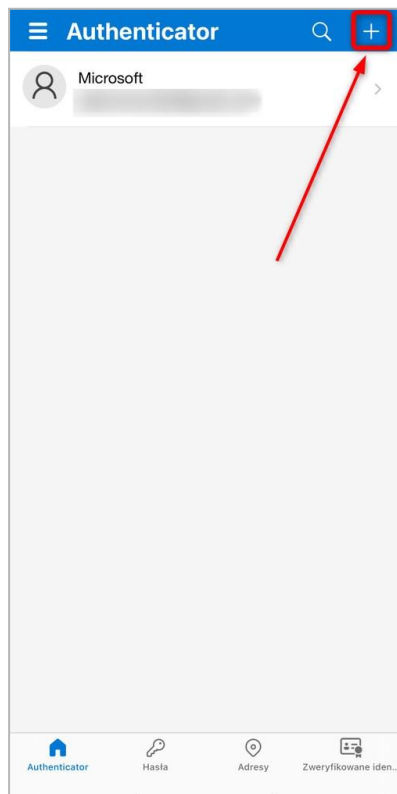
Kliknij **Kontynuuj**.

Następnie kliknij **Zeskanuj kod QR [1]**.

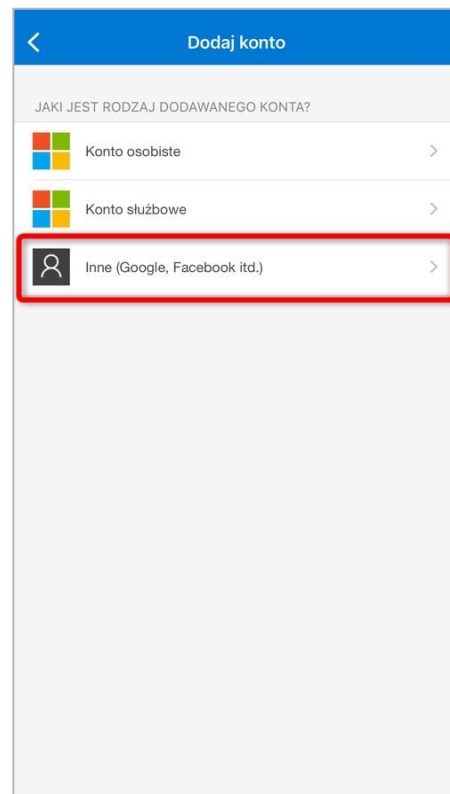


Zobaczysz komunikat pytający, czy zezwalasz aplikacji na robienie zdjęć i nagrywanie filmów. Kliknij **Pozwól**, aby móc zeskanować kod QR.

UWAGA: Jeżeli masz już inną usługę połączoną z Microsoft Authenticator, zobaczysz nieco inny ekran. W tym przypadku:



[1] Kliknij **ikonę plusa**, aby połączyć Microsoft Authenticator ze swoim kontem SALESmanago i rozpocząć generowanie kodów TOTP wymaganych przy logowaniu.



[2] Wybierz rodzaj konta: **Inne (Google, Facebook, itd.)**.

Na tym etapie zobaczysz następujący ekran:



Zeskanuj swój indywidualny kod QR [1] lub **ręcznie wprowadź swój indywidualny kod alfanumeryczny [2]**, aby połączyć Microsoft Authenticator ze swoim kontem SALESmanago.

Zarówno kod QR, jak i klucz konfiguracyjny (kod alfanumeryczny) są podane w komunikacie wyświetlanym na platformie SALESmanago, informującym o konieczności skonfigurowania 2FA (zob. strona 3 powyżej).

WAŻNE: Nigdy nie zachowuj kodu QR ani kodu alfanumerycznego w żadnej formie, w szczególności:

- nie rób zdjęć ani zrzutów ekranu,
- nie drukuj kodów,
- nie zapisuj kodu alfanumerycznego na kartce, w zeszycie, itp.,
- nie skanuj kodów za pomocą aplikacji innej niż aplikacja uwierzytelniająca.

Wszystkie wyżej wymienione działania uważane są za naruszenie bezpieczeństwa.

Niezależnie od wybranej metody, aplikacja zwróci **kod weryfikacyjny**, który należy podać w SALESmanago. Aby ukończyć konfigurację, **przejdź do Kroku 2** (strona 12 poniżej).

Krok 2. Wygeneruj pierwszy kod dla swojego konta SALESmanago

Na tym etapie potwierdź konfigurację przeprowadzoną w aplikacji uwierzytelniającej i dokończ tworzenie połączenia pomiędzy aplikacją a kontem SALESmanago.

Po zeskanowaniu kodu QR lub ręcznym podaniu kodu alfanumerycznego w aplikacji uwierzytelniającej, aplikacja zwróciła kod weryfikacyjny. Wprowadź ten kod na platformie SALESmanago, w następującym polu:

Skonfiguruj uwierzytelnianie dwuskładnikowe (2FA)

1. Otwórz aplikację uwierzytelniającą i wprowadź kod alfanumeryczny lub zeskanuj kod QR

Możesz użyć dowolnej aplikacji uwierzytelniającej, na przykład Google Authenticator lub Microsoft Authenticator.

Wprowadź kod alfanumeryczny w aplikacji uwierzytelniającej

A327MNR4EMJXDUA

Zeskanuj kod QR za pomocą aplikacji uwierzytelniającej



2. Zweryfikuj konfigurację

Kod weryfikacyjny

Anuluj

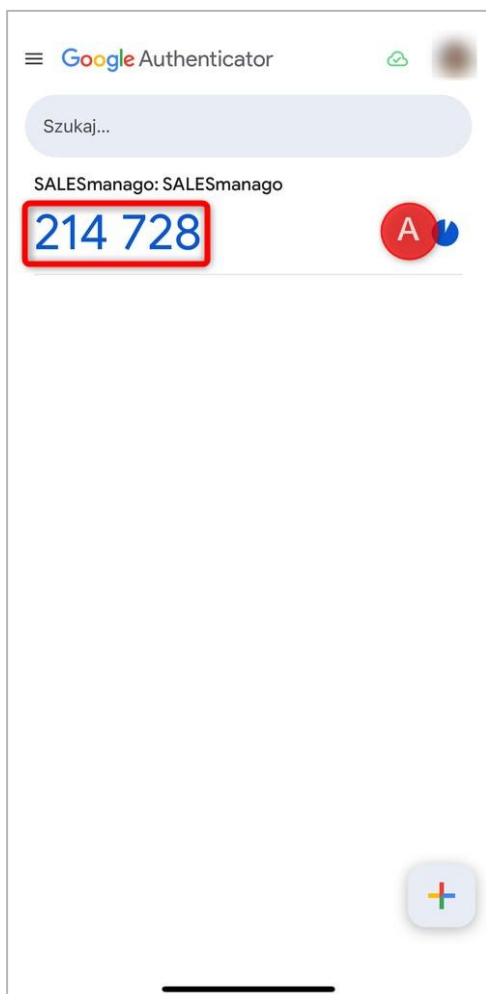
Aktywuj

Po wprowadzeniu kodu kliknij **Aktywuj**.

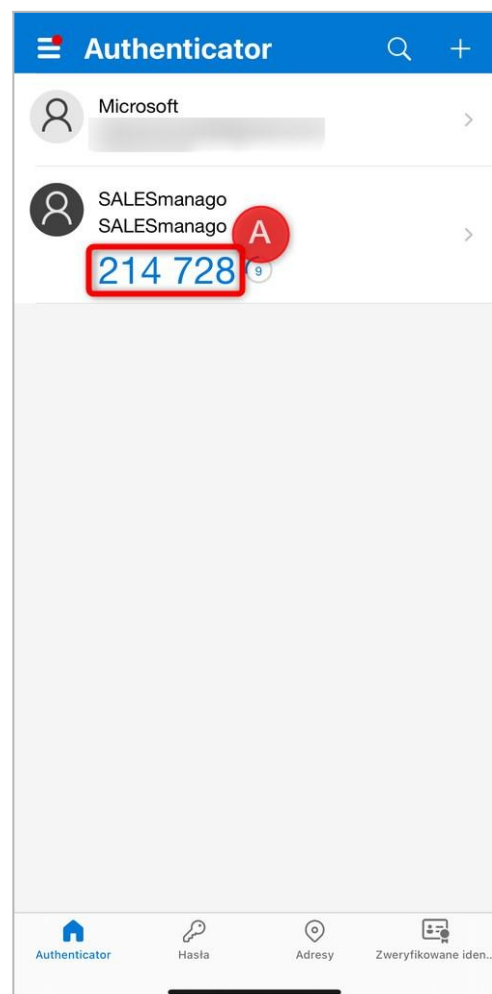
Twoje konto SALESmanago zostało pomyślnie połączone z aplikacją uwierzytelniającą. Teraz możesz **przejsć do procesu logowania** (zob. Krok 3 poniżej).

Krok 3. Zaloguj się do swojego konta SALESmanago

W wyniku konfiguracji przeprowadzonej w Krokach 1 i 2 powyżej, aplikacja uwierzytelniająca zacznie wyświetlać krótkotrwałe kody, tak jak pokazano na poniższych zrzutach ekranu.



Kod wyświetlany w Google Authenticator



Kod wyświetlany w Microsoft Authenticator

Zauważ, że obok kodu znajduje się ikona, która pokazuje, ile czasu pozostało do wygaśnięcia kodu [A]. Upewnij się, że podczas procesu logowania używasz aktualnie wyświetlanego kodu. Jeżeli widzisz, że kod pozostanie ważny jeszcze tylko przez kilka sekund, lepiej poczekaj na następny.

Przy logowaniu na swoje konto SALESmanago zobaczysz następujący ekran:

The screenshot shows the SALESmanago login interface. At the top is the SALESmanago logo. Below it, the title 'Weryfikacja dwuetapowa' (Two-step verification) is displayed. A message explains that the account is secured with 2FA and that a code must be entered to complete login. A text input field labeled 'Kod*' is marked with a red circle containing the number '1'. Below the input field is a large white button with a red circle containing the number '2' and the text 'Zaloguj się' (Login). At the bottom, there are five award badges: 'High Performer Enterprise WINTER 2022', 'Easiest Admin WINTER 2022', 'Users Love Us', 'High Performer Europe WINTER 2022', and 'Leader Europe WINTER 2022'. The version 'Wersja 16.15.0' is shown at the very bottom.

SALESmanago

Weryfikacja dwuetapowa

Twoje konto jest zabezpieczone za pomocą uwierzytelniania dwuskładnikowego (2FA). Aby dokończyć proces logowania, wprowadź kod uwierzytelniający.

1 Kod*

2 Zaloguj się

High Performer Enterprise WINTER 2022

Easiest Admin WINTER 2022

Users Love Us

High Performer Europe WINTER 2022

Leader Europe WINTER 2022

Wersja 16.15.0

Podaj aktualnie wyświetlany kod w polu [1] i kliknij **Zaloguj się** [2]. Gotowe!

Podanie kodu będzie wymagane przy każdym logowaniu do SALESmanago.

3. Często zadawane pytania (FAQ)

Co mam zrobić, jeśli zgubię swojego smartfona?

Skontaktuj się z administratorem konta SALESmanago w swojej Organizacji.

Czy mogę zrezygnować z 2FA na swoim koncie?

Decyzja o aktywowaniu bądź dezaktywowaniu 2FA (dla pojedynczych lub wszystkich użytkowników) jest podejmowana przez administratora konta SALESmanago w twojej Organizacji.

Czy mogę wyłączyć 2FA na swoim koncie?

2FA może zostać wyłączone jedynie przez administratora konta SALESmanago w twojej Organizacji.

Czy mogę używać aplikacji innych niż opisane powyżej?

Tak, jest to możliwe, jednak zdecydowanie zalecamy korzystanie z Google Authenticator lub Microsoft Authenticator.

Czy wszyscy członkowie zespołu muszą korzystać z tej samej aplikacji uwierzytelniającej?

To zależy od polityki twojej Organizacji. Jeżeli twoja Organizacja nie przekazała konkretnych instrukcji, zalecamy zainstalowanie Google Authenticator lub Microsoft Authenticator.

Czy aplikacja Authenticator działa w trybie offline?

Tak, nie jest potrzebne ani połączenie z internetem, ani połączenie GSM.

Czy mogę ponownie wyświetlić kod QR, aby skonfigurować 2FA na innym urządzeniu?

Nie, nie jest to możliwe. Aby ponownie skonfigurować 2FA na innym urządzeniu, skontaktuj się z administratorem konta SALESmanago w twojej Organizacji.

Jeżeli masz jakiegokolwiek pytania bądź wątpliwości dotyczące konfiguracji 2FA, skontaktuj się z nami pod adresem:

support@salesmanago.com
