

Logowanie

Aplikację uruchamia się poprzez kliknięcie na plik **BPM.exe** (przed wersją 2025.2.0 **DMS.exe**)



– ikona **pliku uruchamiającego aplikację Comarch BPM (dawniej DMS)**

Aplikacja Comarch BPM (dawniej DMS) ma **domyślnie wprowadzonego użytkownika Administrator**, który ma dostęp do konfiguracji aplikacji.

Aby zalogować się po raz pierwszy do aplikacji Comarch BPM (dawniej DMS) w polu **Login** należy wpisać „**Administrator**”, natomiast pole **Hasło** należy zostawić **puste**. Od wersji 2025.1.0 w przypadku, gdy aplikację Comarch BPM (dawniej DMS) instalowano za pomocą instalatora, w polu „Hasło” należy wprowadzić hasło, które wprowadzono dla administratora podczas instalacji, w ramach okna „Klucze licencji i hasło Administratora”.

Następnie należy kliknąć ikonę  **[Zaloguj się]**, aby **przejsć do aplikacji desktop Comarch BPM (dawniej DMS)**.

Uwaga

Jeśli Administrator nie ma nadanego hasła podczas instalacji, wówczas po zalogowaniu się do aplikacji **należy ustawić hasło dla Administratora**.

Wskazówka

Jeżeli podczas logowania do nowoutworzonej bazy pojawia się komunikat: „**Nieprawidłowy login lub hasło**” zobacz [tutaj](#)

Wskazówka

Jeżeli podczas próby zalogowania się do Comarch BPM (dawniej DMS) i pojawia się komunikat: **Wystąpił błąd przy pobieraniu klucza licencji: 3** – zobacz [tutaj](#)

Uwaga

Od wersji 2023.0.0 aplikacja desktop Comarch BPM (dawniej DMS) i domyślnie otwiera się na stronie startowej (zob. [Strona startowa](#)). Użytkownik może zmienić to ustawienie w zakładce



[Panel użytkownika] tak, aby po zalogowaniu wyświetlana była lista dokumentów (zob. [Panel użytkownika](#)).

Strona startowa jest dostępna w każdej chwili w zakładce **[Strona startowa]**



W wersji 2024.3.0 wprowadzono funkcjonalność uwierzytelnienia dwustopniowego. Uwierzytelnienie dwustopniowe może być:

- Obowiązkowe – jeśli zostało włączone przez administratora dla wszystkich użytkowników (zob. [Narzędzia](#))
- Dobrowolne – jeśli zostało ustawione przez danego operatora z jego własnej woli (zob. [Konfiguracja](#))

Jeżeli administrator włączył obowiązkowe logowanie dwustopniowe dla wszystkich użytkowników, a dany operator nie ustawił wcześniej logowania dwustopniowego, wówczas musi je skonfigurować podczas kolejnego logowania – po wprowadzeniu loginu i hasła i kliknięciu „Zaloguj” zostaje otwarte okno „Włącz logowanie dwuetapowe”.

×

1. Pobierz aplikację Google Authenticator na urządzeniu mobilnym.
2. Zeskanuj kod QR lub przepisz kod do aplikacji Google Authenticator.
3. Zapisz klucz bezpieczeństwa na zewnętrznym nośniku. Dzięki temu będziesz mógł odzyskać dostęp do konta np. podczas utraty telefonu.
4. Wpisz kod weryfikacyjny z aplikacji Google Authenticator.



Klucz bezpieczeństwa W6SU XRIT 7G5S 5DO3

Wpisz kod weryfikacyjny z aplikacji Google Authenticator.

Zapisz

Anuluj

Okno „Włącz logowanie dwuetapowe” wyświetlone przy logowaniu do aplikacji desktop Comarch BPM (dawniej DMS) i w przypadku, jeśli administrator włączył wymuszenie logowania dwuetapowego, a dany operator nie miał go uruchomionego

Następnie operator musi kolejno wykonać następujące czynności:

1. Pobrać aplikację Google Authenticator na urządzeniu mobilnym
2. Otworzyć aplikację Google Authenticator

3. W aplikacji Google Authenticator kliknąć w przycisk „Dodaj kod”

4. Wybrać jedną z następujących możliwych ścieżek postępowania:

- kliknąć w opcję „Zeskanuj kod QR” w aplikacji Google Authenticator i zeskanować kod QR widoczny w oknie „Włącz logowanie dwuetapowe” w aplikacji Comarch BPM (dawniej DMS)

lub

- kliknąć w opcję „Wpisz klucz konfiguracyjny” w aplikacji Google Authenticator, a następnie w polu „Nazwa konta” wprowadzić nazwę, pod jaką będzie widoczne konto w aplikacji Google Authenticator, a w polu „Twój klucz bezpieczeństwa” wpisać 16-cyfrowy kod dostępny w ramach pola „Klucz bezpieczeństwa” w oknie „Włącz logowanie dwuetapowe” w Comarch BPM (dawniej DMS) i. Po wprowadzeniu wartości należy nacisnąć przycisk „Dodaj” w aplikacji Google Authenticator

5. Zapisać kod z pola „Klucz bezpieczeństwa” na nośniku zewnętrznym – umożliwi to dostęp do konta w przypadku utraty lub usterki urządzenia mobilnego

6. W polu „Wpisz kod weryfikacyjny z aplikacji Google Authenticator” dostępnym w oknie „Włącz logowanie dwuetapowe” w Comarch BPM (dawniej DMS) i wpisać 6-cyfrowy kod weryfikacyjny wyświetlany w aplikacji Google Authenticator, zanim upłynie jego ważność, oznaczona zanikającym niebieskim kołem (kod jest ważny 60 sekund) – jeśli dany kod wygasł, w Comarch BPM (dawniej DMS) i należy wpisać kolejny wygenerowany kod

7. Kliknąć przycisk

Zapisz

[Zapisz].

×

1. Pobierz aplikację Google Authenticator na urządzeniu mobilnym.
2. Zeskanuj kod QR lub przepisz kod do aplikacji Google Authenticator.
3. Zapisz klucz bezpieczeństwa na zewnętrznym nośniku. Dzięki temu będziesz mógł odzyskać dostęp do konta np. podczas utraty telefonu.
4. Wpisz kod weryfikacyjny z aplikacji Google Authenticator.



Klucz bezpieczeństwa W6SU XRIT 7G5S 5DO3

Wpisz kod weryfikacyjny z aplikacji Google Authenticator.

Zapisz

Anuluj

Okno „Włącz logowanie dwuetapowe” – wprowadzanie kodu w polu „Wpisz kod weryfikacyjny z aplikacji Google Authenticator”

Po kliknięciu przycisku

Zapisz

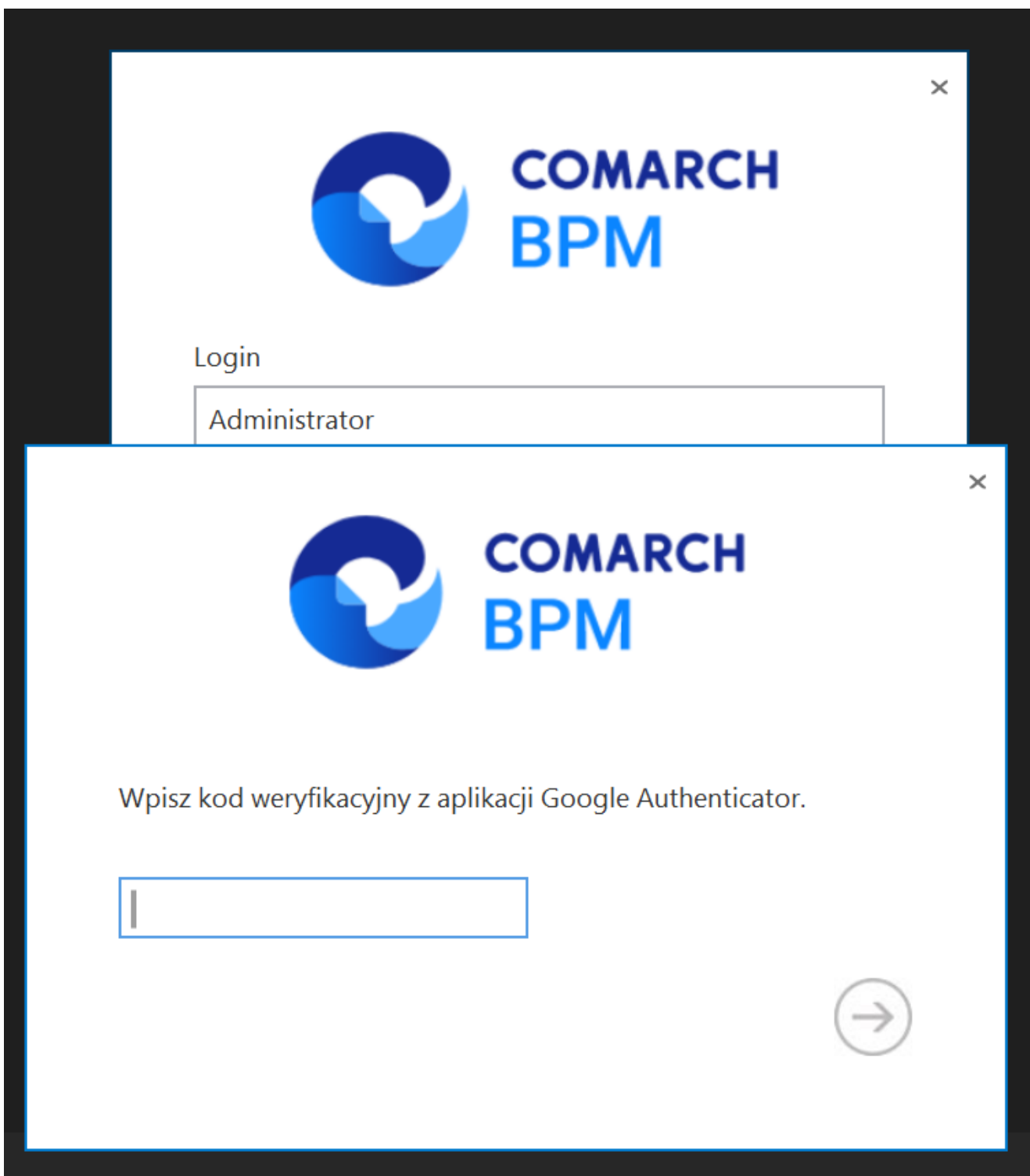
[Zapisz] operator

zostanie zalogowany do aplikacji desktop Comarch BPM (dawniej DMS).

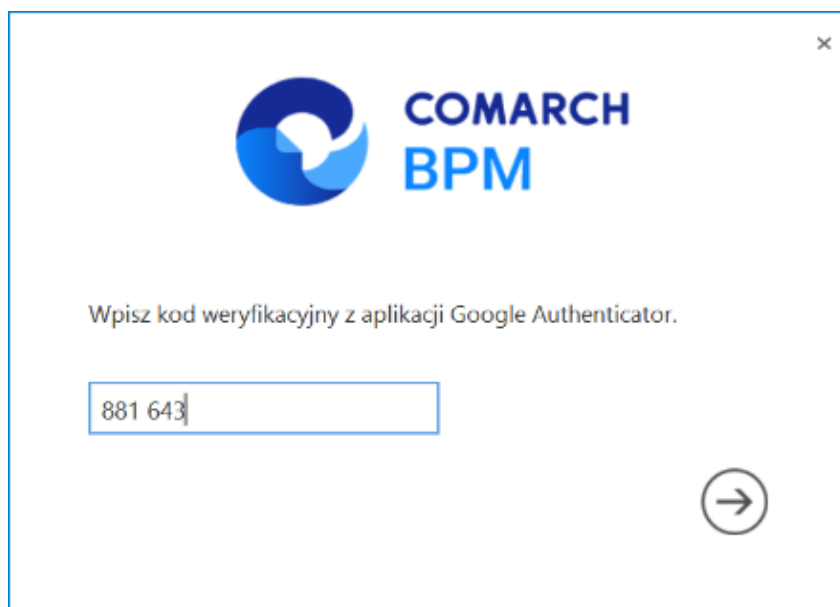
Jeżeli operator ma już włączoną weryfikację dwuetapową, wówczas przy kolejnym otwarciu okna logowania do aplikacji desktop i wprowadzeniu loginu i hasła, a następnie kliknięciu

w przycisk  **[Zaloguj się]** zostaje wyświetlone okno „Podaj kod z aplikacji”. W ramach tego okna należy wprowadzić 6-cyfrowy kod weryfikacyjny wyświetlany w aplikacji Google Authenticator (zanim upłynie jego ważność, oznaczona zanikającym niebieskim kołem (kod jest ważny 60 sekund) – jeśli dany kod wygasł, w oknie „Podaj kod z aplikacji” należy wpisać kolejny wygenerowany kod. Następnie operator powinien

kliknąć w przycisk  **[Zaloguj się]** dostępny w ramach okna „Podaj kod z aplikacji”.



Okno logowania do aplikacji stacjonarnej Comarch BPM (dawniej DMS) z oknem „Podaj kod z aplikacji”

The screenshot shows a web browser window with the COMARCH BPM logo at the top. Below the logo, there is a text prompt: "Wpisz kod weryfikacyjny z aplikacji Google Authenticator." Underneath this prompt is a text input field containing the code "881 643". To the right of the input field is a circular button with a right-pointing arrow. A small 'x' icon is visible in the top right corner of the window frame.

Okno „Podaj kod z aplikacji” – wprowadzanie kodu w polu „Wpisz kod weryfikacyjny z aplikacji Google Authenticator”

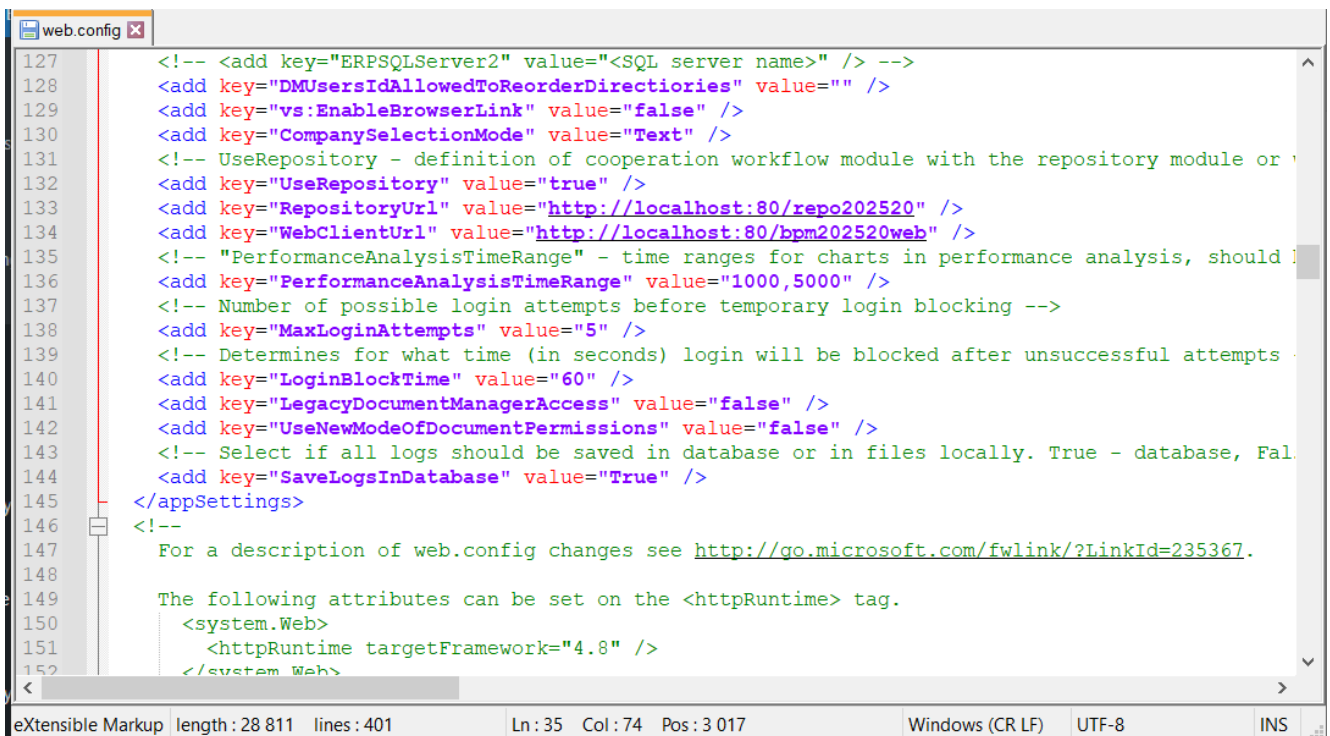
Po wprowadzeniu prawidłowego kodu weryfikacyjnego i naciśnięciu przycisku  [Zaloguj się] okno logowania i okno „Podaj kod z aplikacji” zostają zamknięte, a otwiera się aplikacja desktop Comarch BPM (dawniej DMS).

W wersji 2024.1.1 wprowadzono możliwość **zablokowania logowania** po określonej liczbie prób logowania na wybrany okres czasu.

W tym celu w pliku **Web.config** znajdującym się w katalogu z plikami aplikacji serwerowej (dawna web) wprowadzono dwa nowe klucze:

- `<add key='MaxLoginAttempts' value="5"/>` – w ramach tego klucza należy podać, jaka ma być maksymalna liczba prób logowania dla operatora zanim nastąpi zablokowanie logowania – domyślna wartość to 5
- `<add key='LoginBlockTime' value="60"/>` – w ramach tego klucza należy podać, po jakim czasie (liczonym

w sekundach) operator będzie mógł podjąć kolejną próbę logowania, po tym, jak logowanie zostało zablokowane – domyślna wartość to 60.



```
127 <!-- <add key="ERPSSQLServer2" value="<SQL server name>" /> -->
128 <add key="DMUsersIdAllowedToReorderDirectories" value="" />
129 <add key="vs:EnableBrowserLink" value="false" />
130 <add key="CompanySelectionMode" value="Text" />
131 <!-- UseRepository - definition of cooperation workflow module with the repository module or
132 <add key="UseRepository" value="true" />
133 <add key="RepositoryUrl" value="http://localhost:80/repo202520" />
134 <add key="WebClientUrl" value="http://localhost:80/bpm202520web" />
135 <!-- "PerformanceAnalysisTimeRange" - time ranges for charts in performance analysis, should
136 <add key="PerformanceAnalysisTimeRange" value="1000,5000" />
137 <!-- Number of possible login attempts before temporary login blocking -->
138 <add key="MaxLoginAttempts" value="5" />
139 <!-- Determines for what time (in seconds) login will be blocked after unsuccessful attempts
140 <add key="LoginBlockTime" value="60" />
141 <add key="LegacyDocumentManagerAccess" value="false" />
142 <add key="UseNewModeOfDocumentPermissions" value="false" />
143 <!-- Select if all logs should be saved in database or in files locally. True - database, Fal
144 <add key="SaveLogsInDatabase" value="True" />
145 </appSettings>
146 <!--
147 For a description of web.config changes see http://go.microsoft.com/fwlink/?LinkId=235367.
148
149 The following attributes can be set on the <httpRuntime> tag.
150 <system.Web>
151 <httpRuntime targetFramework="4.8" />
152 </system.Web>
```

Plik Web.config z nowymi kluczami MaxLoginAttempts i LoginBlockTime

Jeśli operator próbował zalogować się do aplikacji desktop Comarch BPM (dawniej DMS) za pomocą błędnego loginu i/lub hasła, a liczba prób przekroczyła wartość wprowadzoną w ramach klucza `<add key='MaxLoginAttempts' value="5"/>`, wówczas poniżej pola „Hasło” zostanie wyświetlona informacja *Wykryto zbyt wiele nieudanych prób logowania. Poczekaaj i spróbuj ponownie.*

W takim przypadku operator musi poczekać, aż upłynie czas określony w ramach klucza `<add key='LoginBlockTime' value="60"/>`, aby znów spróbować się **zalogować**.



**COMARCH
BPM**

Login

Hasło

Wykryto zbyt wiele nieudanych prób logowania. Poczekaj i spróbuj ponownie.

[Zmień język](#)[Zmień hasło](#)

☐ zapamiętaj logowanie



Okno logowania do aplikacji desktop Comarch BPM (dawniej DMS) w trybie jednofirmowym – jeśli operator próbował logować się za pomocą błędnych danych zbyt wiele razy

×



COMARCH
BPM

Spółka

Domyślna spółka

▼

Login

Administrrrator

Hasło

●●●●●●●●●●●●●●●●●●●●

Wykryto zbyt wiele nieudanych prób logowania. Poczekaj i spróbuj ponownie.

Zmień język

Zmień hasło

☐ zapamiętaj logowanie

→

Okno logowania do aplikacji desktop Comarch BPM (dawniej DMS) w trybie wielofirmowym – jeśli operator próbował logować się za pomocą błędnych danych zbyt wiele razy

Funkcjonalność logowania oferuje również opcję **zapamiętywania logowania**.

×

**COMARCH
BPM**

Login

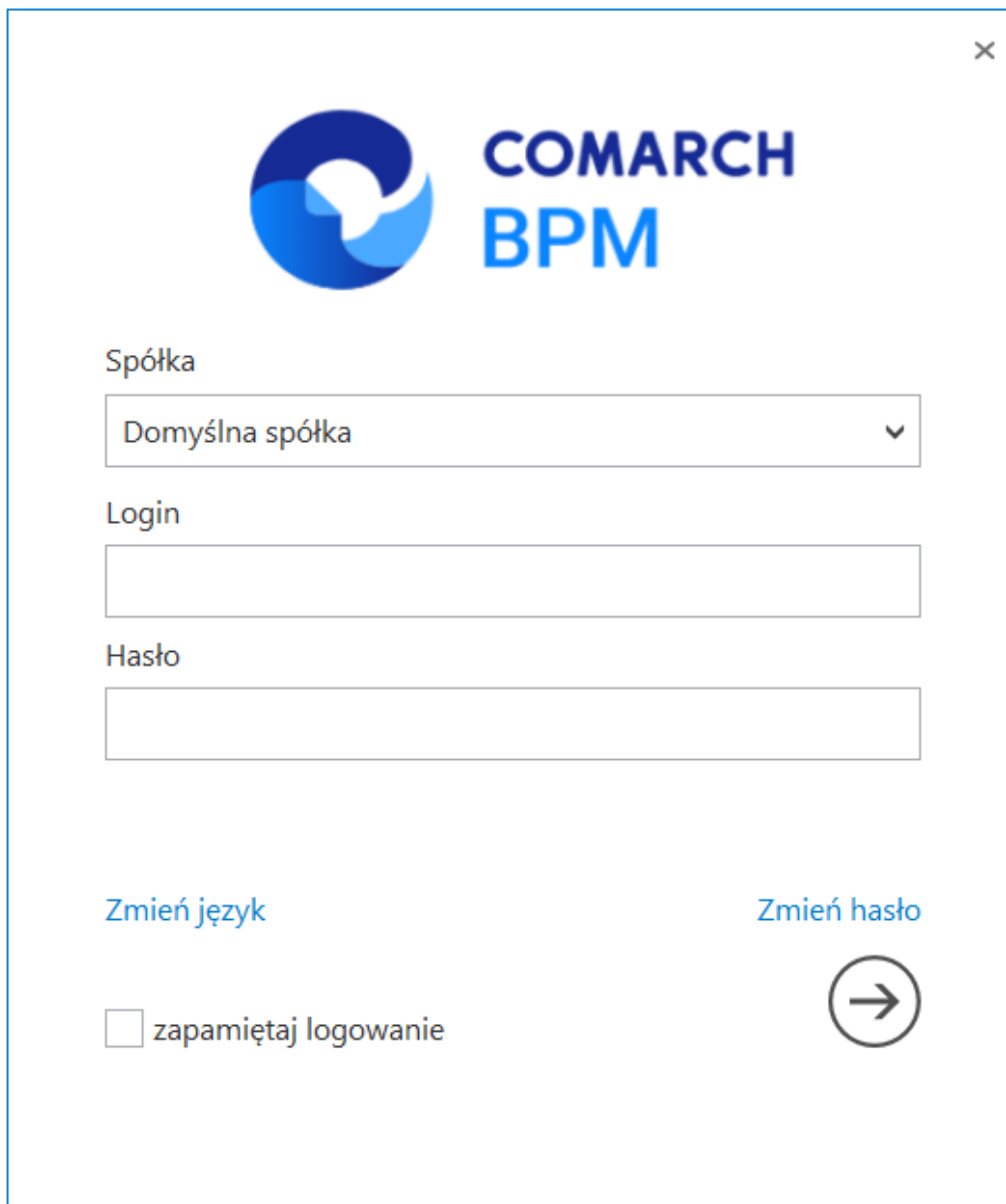
Hasło

[Zmień język](#)[Zmień hasło](#)

☐ zapamiętaj logowanie



Okno logowania do systemu



Okno logowania do systemu w trybie wielospółkowym

Parametr ☐ zapamiętaj logowanie [zapamiętaj logowanie] –
zaznaczenie parametru oznacza, że **operator jest zalogowany w**

Comarch BPM (dawniej DMS) do momentu użycia funkcji [Wyloguj się]. Gdy zalogowany operator zamknie okno Comarch

BPM (dawniej DMS) za pomocą przycisku , **ponowne uruchomienie aplikacji nie będzie wymagało wpisywania loginu i hasła, logowanie przebiegnie automatycznie.**



Link [Zmień język](#) **[Zmień hasło]** jest dostępny, jeśli:

- podczas instalacji aplikacji serwerowej (dawna web) Comarch BPM (dawniej DMS) za pomocą instalatora zaznaczono opcję „[Prezentuj zmianę języka na ekranie logowania](#)„

lub

- w pliku **Web.config** w ramach klucza „[ShowChangeLanguage](#)” wpisano wartość „**true**” (zob. przykładowo [Instalacja aplikacji serwerowej \(dawnej web\) w trybie ręcznym](#))

Po kliknięciu w link [Zmień język](#) **[Zmień hasło]** otwierana jest **lista, z której można wybrać jeden z 4 języków: polski, angielski, niemiecki albo francuski** – po zalogowaniu do Comarch BPM (dawniej DMS) **aplikacja będzie wyświetlana w wybranym języku**.

×

**COMARCH
BPM**

Spółka

Dom

Login

Hasło

Polski

Polski

English

Deutsch

Français

Zmień hasło



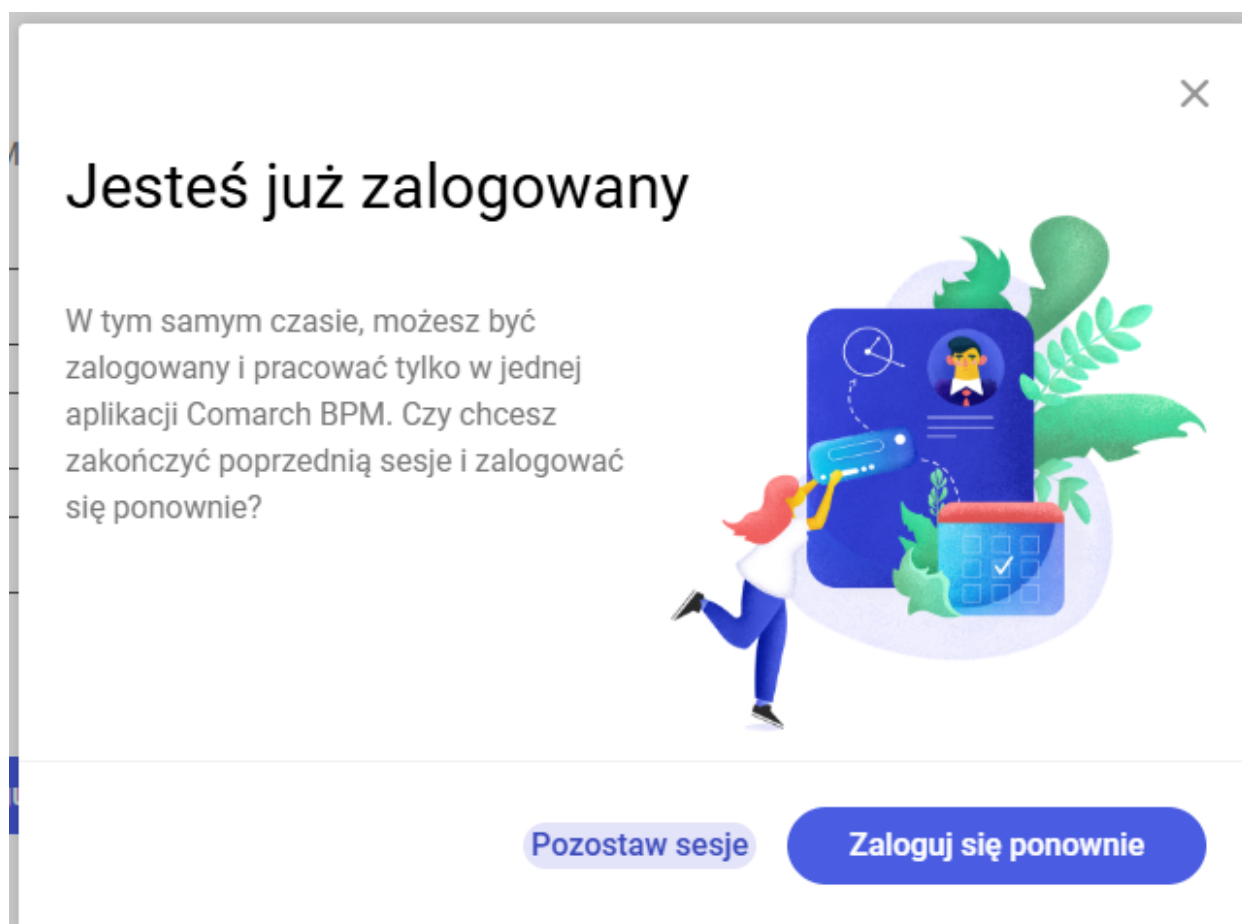
Wybór języka wyświetlania Comarch BPM (dawniej DMS)

W danym momencie operator może pracować tylko z jedną wersją (stacjonarną, WWW lub mobilną) aplikacji Comarch BPM (dawniej DMS).

Podczas logowania, aplikacja weryfikuje czy operator jest już

zalogowany do innej wersji aplikacji.

Jeżeli weryfikacja wykaże, że obecnie operator zalogowany jest do innej wersji, wyświetlony zostanie **komunikat** z pytaniem dotyczącym automatycznego wylogowania. **Zatwierdzenie komunikatu spowoduje wylogowanie operatora z dotychczasowej wersji aplikacji i umożliwi zalogowanie do nowej.**



Komunikat wyświetlany podczas logowania do aplikacji web

Rozpoczynasz pracę z Comarch BPM (dawniej DMS) i chcesz dowiedzieć się, jak korzystać z programu? A może masz już podstawową wiedzę o Comarch BPM (dawniej DMS) i chcesz dowiedzieć się więcej?

[Sprawdź Szkolenia Comarch BPM!](#)

[Powrót do początku artykułu](#)