

Konfiguracja współpracy Comarch BPM z KSeF

Współpracę Comarch BPM z KSeF można skonfigurować zarówno w trybie jednospółkowym, jak i w trybie wielospółkowym.

Aby skonfigurować współpracę Comarch BPM z KSeF, należy:

- **dla trybu jednospółkowego:** na zakładce **Ustawienia** -> zakładka **Integracje**:

1. w ramach pola „Nip firmy” wprowadzić NIP firmy, dla której ma odbywać się współpraca z KSeF
2. w ramach pola „Token KSeF” wprowadzić token uwierzytelniający w KSeF.

W wersji 2026.0.1 zachowano możliwość ustawienia tokenu KSeF – zarówno poprzez wklejenie tokenu, jaki przez jego generowanie – analogicznie jak w dotychczasowych wersjach.

Uwaga

Używanie tokenów KSeF jako jednej z metod autoryzacyjnych z usługą KSeF będzie dostępne nie dłużej niż do 31.12.2026.

Uwaga

Jeśli autoryzacja przez token zakończy się niepowodzeniem, wówczas podczas próby importu dokumentów z KSeF zostanie wyświetlone okno z certyfikatami, w ramach którego należy wskazać właściwy certyfikat.

Uwaga

W wersji 2024.0.1 w pliku **Web.config** w folderze aplikacji serwerowej (dawnej web) dodano klucz `add key="KSeFWorkMode" value="Demo" />` – klucz umożliwia określenie, czy Firma testuje funkcjonalność wysyłania faktur do KSeF, czy korzysta z niej produkcyjnie.

Klucz może przybierać jedną z następujących wartości:

1.Demo – w przypadku wprowadzenia takiej wartości praca z systemem KSeF odbywa się w trybie Demo;

2.Production – **wartość domyślna od wersji 2026.0.0**; w przypadku wprowadzenia takiej wartości praca z systemem KSeF odbywa się w trybie Produkcyjnym, czyli wersji produkcyjnej systemu;

3.Test – w przypadku wprowadzenia takiej wartości praca z systemem KSeF odbywa się w trybie testowym.

Uwaga

W celu przetestowania współpracy z Comarch BPM na prawdziwych danych zalecamy korzystanie z trybu Demo.

W kwestii różnic pomiędzy powyższymi trybami zob. [Przełączanie trybu pracy z KSeF](#)

Uwaga

W wersji 2026.0.0 w pliku **Web.config** w folderze aplikacji serwerowej (dawnej web) wprowadzono nowy klucz **"KSeFProdVersion"**, który ma umożliwić zmianę wersji KSeF dla pracy w trybie produkcyjnym. Klucz może przyjmować jedną z następujących wartości:

- 1 – wartość domyślna w wersji 2026.0.0; możliwa jest praca w trybie produkcyjnym KSeF 1.0

- 2 – możliwa jest praca w trybie produkcyjnym KSeF 2.0

Praca w trybie produkcyjnym KSeF 2.0 będzie możliwa jedynie wtedy, gdy `<add key="KSeFWorkMode" value="Production" />` oraz `<add key="KSeFProdVersion" value="2" />` – ten tryb pracy będzie aktywny dopiero po uruchomieniu przez Ministerstwo Finansów środowiska produkcyjnego KSeF 2.0, tj. po 01.02.2026.

Klucz "KSeFProdVersion" nie wpływa na pracę w trybie „Test” oraz „Demo”.

Istnieje możliwość wygenerowania tokenu KSeF z poziomu Comarch BPM (dawniej DMS). W tym celu należy **kliknąć w link**

Wygeneruj token

[Wygeneruj token] znajdujący się obok pola „Token KSeF”, a następnie w oknie „Wybierz certyfikat” **wybrać odpowiedni certyfikat uwierzytelniający**.

Po wyborze certyfikatu **zostanie wygenerowany token KSeF**, który zostanie **automatycznie wprowadzony** w ramach pola „Token KSeF”.

Wprowadzone zmiany należy zapisać za pomocą przycisku

Zapisz

[Zapisz], dostępnego w ramach sekcji.

Uwaga

Aby wygenerować token konieczne jest zainstalowanie kwalifikowanego podpisu/pieczęci, za pomocą którego możliwe jest uwierzytelnienie się na stronach ministerstwa.

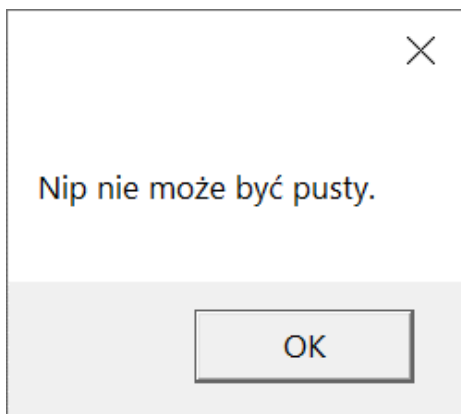
Aby wygenerować token uwierzytelniający, należy najpierw **uzupełnić pole „NIP Firmy”**.

Jeżeli użytkownik **nie uzupełni pola „NIP Firmy”** i naciśnie

link **Wygeneruj token**

[Wygeneruj token], wówczas zostanie

wyświetlony następujący komunikat.



Komunikat wyświetlany,
jeśli nie wpisano
numeru NIP w polu „NIP
Firmy”, ale naciśnięto
link „Wygeneruj token”

Wskazówka

Jeżeli operator pracuje w trybie Demo współpracy z KSeF 2.0,
wówczas może:

- wybrać odpowiedni certyfikat w ramach okna wyświetlanego
po kliknięciu w przycisk **Wygeneruj token** [Wygeneruj
token]. Wówczas w polu „Token KSeF” zostanie wprowadzony
token. Wprowadzone zmiany powinny zostać zapisane.

lub

- przejść na stronę <https://ap-demo.ksef.mf.gov.pl/web>,
kliknąć w pole „Uwierzytelnij się w Krajowym Systemie e-
Faktur”, zaznaczyć oświadczenie i kliknąć „Przejdź
dalej”, a następnie zalogować się do aplikacji w wybrany
sposób (profilem zaufanym lub certyfikatem
kwalifikowanym). Później należy wybrać zakładkę

„Tokeny”, sekcję „Generuj token” – w polu „Nazwa tokena” wprowadzić przykładową nazwę tokena, poniżej zaznaczyć uprawnienia i kliknąć w pole „Generuj token”. Po odświeżeniu strony należy skopiować wyświetlany token, a potem wkleić go w polu „Token KSeF”. Wprowadzone zmiany powinny zostać zapisane.

Od wersji 2026.0.1 w ramach Comarch BPM umożliwiono uwierzytelnianie za pomocą certyfikatu KSeF otrzymanego poprzez MCU – z tego powodu wprowadzono następujące nowe pola:

- **Klucz prywatny certyfikatu KSeF** – w ramach tego pola po

kliknięciu w przycisk  **[Dodaj]** można dodać z dysku plik o rozszerzeniu .key – klucz, który uzyskano podczas wnioskowania o certyfikat KSeF. Dodany plik zostanie wyświetlony zgodnie ze swoją nazwą. Operator może go

zapisać na dysku, klikając w ikonę  **[Zapisz]** lub usunąć z aplikacji Comarch BPM, klikając w przycisk

kosza  **[Usuń]**. Dane klucza prywatnego są zaszyfrowane i przechowywane w bazie danych Comarch BPM;

- **Odcisk certyfikatu KSeF** – w tym polu operator może wybrać certyfikat KSeF, z którym jest powiązany klucz prywatny, który wybrano w polu „Klucz prywatny certyfikatu KSeF”. W tym celu należy kliknąć w link

[Wybierz certyfikat](#)

[Wybierz certyfikat], a następnie w ramach okna Eksploratora plików wybrać odpowiedni plik i nacisnąć przycisk „Otwórz”. Dodawany plik powinien być certyfikatem z rozszerzeniem .crt, który uzyskano poprzez wnioskowanie o certyfikat KSeF. Jeżeli operator

wybrał plik w poprawnym formacie, wówczas pole „Odcisk certyfikatu KSeF” zostanie automatycznie wypełnione danymi odcisku palca tego certyfikatu, a obok pola

zamiast linku [Wybierz certyfikat](#) **[Wybierz certyfikat]**

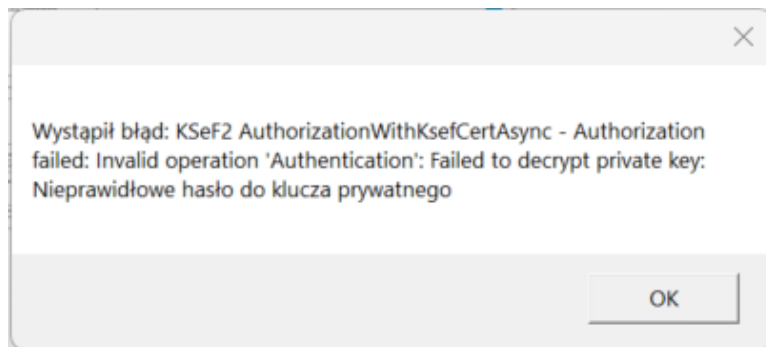
zostanie wyświetlony link [Usuń certyfikat](#) **[Usuń certyfikat]**. Dodany certyfikat jest przechowywany w formie zaszyfrowanej w bazie danych Comarch BPM. Ręczna edycja pola „Odcisk certyfikatu KSeF” nie jest możliwa.

- Jeśli operator kliknie w link [Usuń certyfikat](#) **[Usuń certyfikat]**, wówczas dane certyfikatu (odcisk odciska palca certyfikatu i certyfikat) zostaną usunięte zarówno z bazy Comarch BPM, jak i z pola „Odcisk certyfikatu KSeF”. Gdy certyfikat zostanie usunięty, link [Usuń certyfikat](#) **[Usuń certyfikat]**

zmieni się ponownie w link [Wybierz certyfikat](#) **[Wybierz certyfikat]** i będzie możliwe ponowne wybranie certyfikatu.

Uwaga

Aplikacja Comarch BPM nie weryfikuje zgodności dodanego certyfikatu z dodanym kluczem prywatnym. Jeśli operator wybrał certyfikat, z którym nie jest powiązany klucz prywatny wybrany w polu „Klucz prywatny certyfikatu KSeF”, wówczas przy próbie pobrania faktur z KSeF w punkcie ACd zostaje wyświetlony komunikat: „Wystąpił błąd: KSeF2 AuthorizationWithKsefCertAsync – Authorization failed: Invalid operation 'Authentication': Failed to decrypt private key: Nieprawidłowe hasło do klucza prywatnego”.



Komunikat wyświetlany przy próbie pobierania faktur z KSeF, gdy wybrany certyfikat nie jest powiązany z wybranym kluczem prywatnym

- **Hasło certyfikatu KSeF** – pole, w ramach którego należy wprowadzić hasło, które wprowadzono podczas wnioskowania o certyfikat KSeF. Wprowadzone hasło jest przechowywane w formie zaszyfrowanej w bazie danych Comarch BPM.

Comarch BPM 2026.0.1 Administrator

Ustawienia

AUTORYZACJA API SERWER POCZTOWY EMAIL DOMENA NARZĘDZIA API INTEGRACJE ANALIZA WYDAJNOŚCI LOGI SYSTEMOWE

Integracja z usługą KSeF

NIP firmy

Token KSeF Wygeneruj token

Klucz prywatny certyfikatu KSeF +

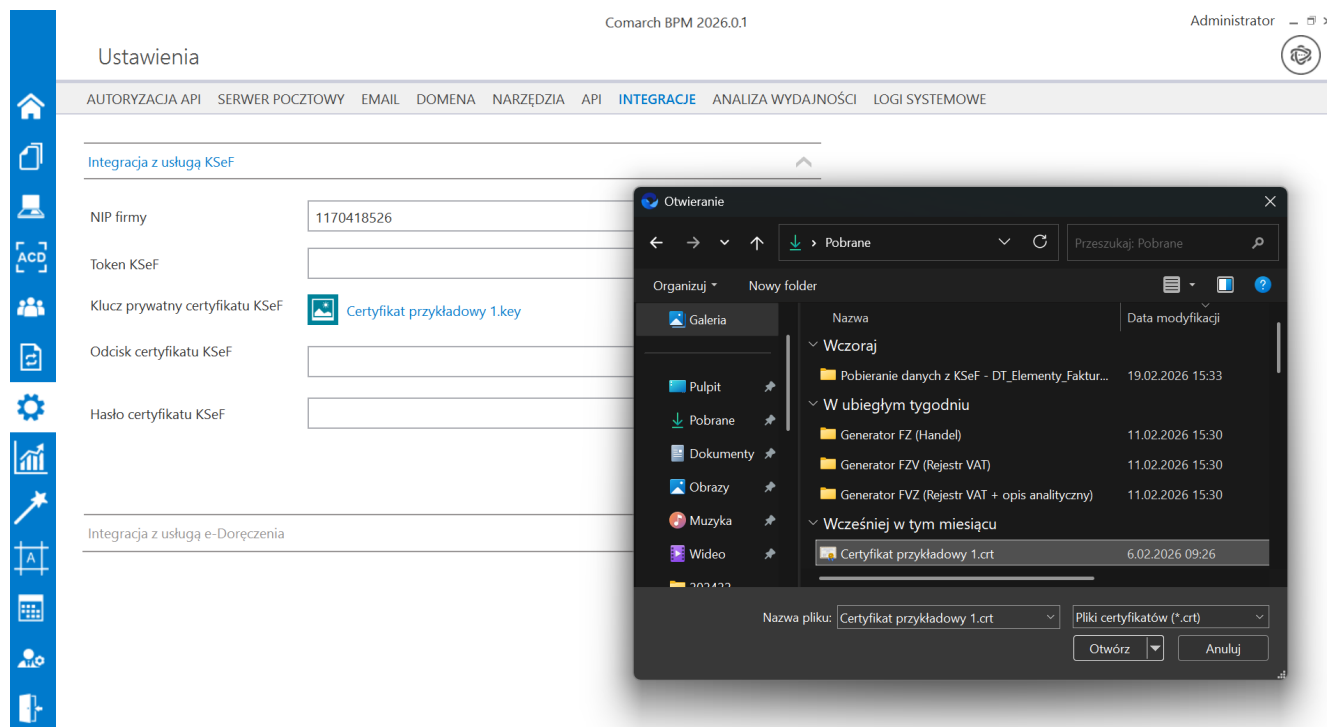
Odcisk certyfikatu KSeF Wybierz certyfikat

Hasło certyfikatu KSeF

Zapisz

Integracja z usługą e-Doręczenia

Sekcja „Integracja z usługą KSeF” na zakładce „Integracje” z nowymi polami – przed uzupełnieniem



Wybór certyfikatu po kliknięciu w link „Wybierz certyfikat” w ramach pola „Odcisk certyfikatu KSeF”

Comarch BPM 2026.0.1 Administrator

Ustawienia

AUTORYZACJA API SERWER POCZTOWY EMAIL DOMENA NARZĘDZIA API **INTEGRACJE** ANALIZA WYDAJNOŚCI LOGI SYSTEMOWE

Integracja z usługą KSeF

NIP firmy

Token KSeF [Wygeneruj token](#)

Klucz prywatny certyfikatu KSeF  [Certyfikat przykładowy 1.key](#)  

Odcisk certyfikatu KSeF [Usuń certyfikat](#)

Hasło certyfikatu KSeF

[Zapisz](#)

Integracja z usługą e-Doręczenia

Sekcja „Integracja z usługą KSeF” na zakładce „Integracje” z nowymi polami – po przykładowym uzupełnieniu

Comarch BPM 2026.0.1 Administrator

Ustawienia

AUTORYZACJA API SERWER POCZTOWY EMAIL DOMENA NARZĘDZIA API PRZECZYSKOWYWANIE PLIKÓW **INTEGRACJE** ANALIZA WYDAJNOŚCI LOGI SYSTEMOWE

Integracja z usługą KSeF

NIP firmy

Token KSeF [Wygeneruj token](#)

Klucz prywatny certyfikatu KSeF 

Odcisk certyfikatu KSeF [Wybierz certyfikat](#)

Hasło certyfikatu KSeF

[Zapisz](#)

Integracja z usługą e-Doręczenia

Zakładka „Integracje” – sekcja „Integracja z usługą KSeF”

Po ukończeniu konfiguracji należy przejść do konfiguracji punktu ACD współpracującego z KSeF (zob. [Definiowanie punktu konfiguracyjnego \(Import dokumentów zakupu z KSeF\)](#))

- **dla trybu wielospółkowego:** na zakładce **Ustawienia** -> zakładka **Połączenia z ERP** -> **ustawienia odpowiedniej spółki:**

1. w ramach pola „Nip firmy” należy wprowadzić NIP firmy, dla której ma odbywać się współpraca z KSeF
2. w ramach pola „Token KSeF” należy wprowadzić token uwierzytelniający w KSeF.

W wersji 2026.0.1 zachowano możliwość ustawienia tokenu KSeF – zarówno poprzez wklejenie tokenu, jaki przez jego generowanie – analogicznie jak w dotychczasowych wersjach.

Uwaga

Używanie tokenów KSeF jako jednej z metod autoryzacyjnych z usługą KSeF będzie dostępne nie dłużej niż do 31.12.2026.

Uwaga

Jeśli autoryzacja przez token zakończy się niepowodzeniem, wówczas podczas próby importu dokumentów z KSeF zostanie wyświetlone okno z certyfikatami, w ramach którego należy wskazać właściwy certyfikat.

Uwaga

W wersji 2024.0.1 w pliku **Web.config** w folderze aplikacji serwerowej (dawnej web) dodano klucz `add key="KSeFWorkMode" value="Demo" />` – klucz umożliwia określenie, czy Firma

testuje funkcjonalność wysyłania faktur do KSeF, czy korzysta z niej produkcyjnie.

Klucz może przybierać jedną z następujących wartości:

1.Demo – **wartość domyślna**; w przypadku wprowadzenia takiej wartości praca z systemem KSeF odbywa się w trybie Demo;

2.Production – w przypadku wprowadzenia takiej wartości praca z systemem KSeF odbywa się w trybie Produkcyjnym, czyli wersji produkcyjnej systemu;

3.Test – w przypadku wprowadzenia takiej wartości praca z systemem KSeF odbywa się w trybie testowym.

W kwestii różnic pomiędzy powyższymi trybami zob. [Przełączanie trybu pracy z KSeF](#)

Istnieje możliwość **wygenerowania tokenu KSeF z poziomu Comarch BPM (dawniej DMS)**. W tym celu należy **kliknąć w link**

Wygeneruj token

[Wygeneruj token] znajdujący się obok pola „Token KSeF”, a następnie w oknie „Wybierz certyfikat” **wybrać odpowiedni certyfikat uwierzytelniający**.

Po wyborze certyfikatu **zostanie wygenerowany token KSeF**, który zostanie **automatycznie wprowadzony** w ramach pola „Token KSeF”.

Wprowadzone zmiany należy zapisać za pomocą przycisku

Zapisz

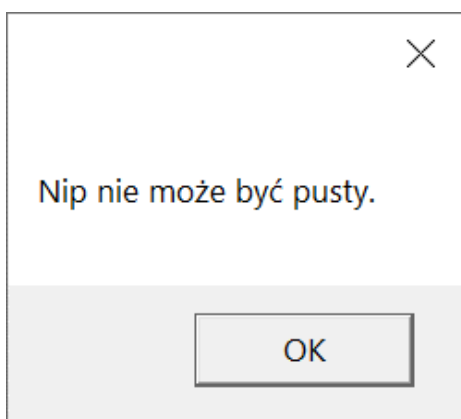
[Zapisz], dostępnego w ramach sekcji.

Uwaga

Aby wygenerować token konieczne jest zainstalowanie kwalifikowanego podpisu/pieczęci, za pomocą którego możliwe jest uwierzytelnienie się na stronach ministerstwa.

Aby wygenerować token uwierzytelniający, należy najpierw uzupełnić pole „NIP Firmy”.

Jeżeli użytkownik **nie uzupełni pola „NIP Firmy”** i naciśnie link [Wygeneruj token](#) **[Wygeneruj token]**, wówczas zostanie wyświetlony następujący komunikat.



Komunikat wyświetlany, jeśli nie wpisano numeru NIP w polu „NIP Firmy”, ale naciśnięto link „Wygeneruj token”

Od wersji 2026.0.1 w ramach Comarch BPM umożliwiono uwierzytelnianie za pomocą certyfikatu KSeF otrzymanego poprzez MCU – z tego powodu wprowadzono następujące nowe pola:

- **Klucz prywatny certyfikatu KSeF** – w ramach tego pola po



kliknięciu w przycisk **[Dodaj]** można dodać z dysku plik o rozszerzeniu .key – klucz, który uzyskano podczas wnioskowania o certyfikat KSeF. Dodany plik zostanie wyświetlony zgodnie ze swoją nazwą. Operator może go



zapisać na dysku, klikając w ikonę **[Zapisz]** lub usunąć z aplikacji Comarch BPM, klikając w przycisk



kosza **[Usuń]**. Dane klucza prywatnego są zaszyfrowane i przechowywane w bazie danych Comarch BPM;

- **Odcisk certyfikatu KSeF** – w tym polu operator może wybrać certyfikat KSeF, z którym jest powiązany klucz prywatny, który wybrano w polu „Klucz prywatny certyfikatu KSeF”. W tym celu należy kliknąć w link

[Wybierz certyfikat](#)

[Wybierz certyfikat], a następnie w ramach okna Eksploratora plików wybrać odpowiedni plik i nacisnąć przycisk „Otwórz”. Dodawany plik powinien być certyfikatem z rozszerzeniem .crt, który uzyskano poprzez wnioskowanie o certyfikat KSeF. Jeżeli operator wybrał plik w poprawnym formacie, wówczas pole „Odcisk certyfikatu KSeF” zostanie automatycznie wypełnione danymi odcisku palca tego certyfikatu, a obok pola

zamiast linku [Wybierz certyfikat](#) **[Wybierz certyfikat]**

zostanie wyświetlony link [Usuń certyfikat](#) **[Usuń certyfikat]**. Dodany certyfikat jest przechowywany w formie zaszyfrowanej w bazie danych Comarch BPM. Ręczna edycja pola „Odcisk certyfikatu KSeF” nie jest możliwa.

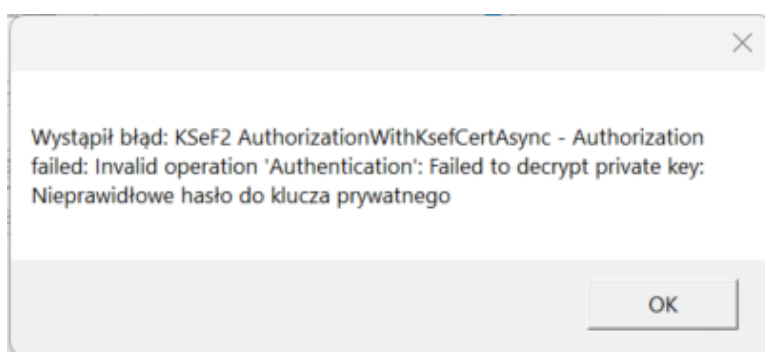
- Jeśli operator kliknie w link [Usuń certyfikat](#) **[Usuń certyfikat]**, wówczas dane certyfikatu (odcisk odciska palca certyfikatu i certyfikat) zostaną usunięte zarówno z bazy Comarch BPM, jak i z pola „Odcisk certyfikatu KSeF”. Gdy certyfikat zostanie

usunięty, link [Usuń certyfikat](#) **[Usuń certyfikat]**

zmieni się ponownie w link [Wybierz certyfikat](#) **[Wybierz certyfikat]** i będzie możliwe ponowne wybranie certyfikatu.

Uwaga

Aplikacja Comarch BPM nie weryfikuje zgodności dodanego certyfikatu z dodanym kluczem prywatnym. Jeśli operator wybrał certyfikat, z którym nie jest powiązany klucz prywatny wybrany w polu „Klucz prywatny certyfikatu KSeF“, wówczas przy próbie pobrania faktur z KSeF w punkcie ACd zostaje wyświetlony komunikat: „Wystąpił błąd: KSeF2 AuthorizationWithKsefCertAsync – Authorization failed: Invalid operation 'Authentication': Failed to decrypt private key: Nieprawidłowe hasło do klucza prywatnego“.



Komunikat wyświetlany przy próbie pobierania faktur z KSeF, gdy wybrany certyfikat nie jest powiązany z wybranym kluczem prywatnym

- **Hasło certyfikatu KSeF** – pole, w ramach którego należy wprowadzić hasło, które wprowadzono podczas wnioskowania o certyfikat KSeF. Wprowadzone hasło jest przechowywane w formie zaszyfrowanej w bazie danych Comarch BPM.

Po ukończeniu konfiguracji należy przejść do konfiguracji punktu ACD współpracującego z KSeF (zob. [Definiowanie punktu konfiguracyjnego \(Import dokumentów zakupu z KSeF\)](#))

Ustawienia

Comarch BPM 2026.0.1 [Domyślna spółka] Administrator

POŁĄCZENIA Z ERP SERWER POCTIOWY EMAIL NARZĘDZIA API PRZECHOWYWANIE PLIKÓW ANALIZA WYDAJNOŚCI LOGI SYSTEMOWE

(DS) Domyślna spółka

()

System ERP XL

Nazwa spółki Domyślna spółka

Spółka (skrót) DS

Baza firmowa Zmien

Klucz licencyjny

Nazwa bazy (nazwa firmy)

Wybierz wymiary z centrum ERP XL

Domyślny login operatora ERP

Hasło operatora ERP

Używaj domeny

Nazwa domeny

Grupa

NIP firmy 1170418526

Token KSeF Wygeneruj token

Klucz prywatny certyfikatu KSeF Certyfikat przykładowy 3.key

Odcisk certyfikatu KSeF 2934E978AA2282558E8083E8098AA8D406E6D22C Usuń certyfikat

Hasło certyfikatu KSeF

Adres skrzynki

Nazwa systemu wprowadzona w konfiguracji skrzynki e-Doręczenia

Klucz prywatny skrzynki e-Doręczenia

Ustawienia konfiguracyjne dla wszystkich spółek

Zakładka „Połączenia z ERP”, pola „Nip firmy” , „Token KSeF”, „Klucz prywatny certyfikatu KSeF”, „Odcisk certyfikatu KSeF”, „Hasło certyfikatu KSeF”

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](#)