



mMedica

# Migracja do PostgreSQL 17

## Spis treści

---

1.	Migracja na systemach operacyjnych Windows.....	4
2.	Alternatywna metoda migracji (odtworzenie kopii zapasowej wykonanej na PostgreSQL 13) .....	10
3.	Migracja na systemach operacyjnych z rodziny Linux .....	11
4.	Aktualizacja stacji roboczych mMedica w sieci.....	17

---

## Wstęp

W niniejszej instrukcji przedstawiono najważniejsze informacje dotyczące wdrożenia nowego silnika bazy danych PostgreSQL w wersji 17. **Migrację można przeprowadzić dla mMedica w wersji 11.9.0 (w tej samej wersji powinny być także moduły eRejestracja oraz eArchiwum, jeśli zostały zainstalowane). W przypadku niższych wersji, przed rozpoczęciem migracji należy najpierw wykonać aktualizację do wersji 11.9.0 uwzględniając w niej wszystkie stacje robocze.**

Ponadto konieczne jest zapewnienie wolnej przestrzeni na dysku twardym, co najmniej na poziomie 150% wielkości folderu z bazą danych PostgreSQL 13. Migrację bazy danych najlepiej przeprowadzić za pomocą dedykowanego programu **mMigrator.exe**. W przypadku wystąpienia problemu (np. na starszych systemach operacyjnych, niewspieranych przez Microsoft) istnieje możliwość skorzystania z alternatywnej formy migracji opisanej w rozdziale 2.

Razem z PostgreSQL 17 wprowadzamy dodatkowe zabezpieczenie połączeń do bazy poprzez zastosowanie certyfikatów i mechanizmu SSL. Szerszy opis tej funkcjonalności został zawarty w dalszej części tej instrukcji.

W przypadku instalacji rozproszonych, w których eRejestracja i eArchiwum znajdują się na osobnych serwerach z Windows migrację wykonuje się w sposób analogiczny do migracji mMedica. W domyślnej ścieżce każdy serwer PostgreSQL otrzymuje unikalny zestaw certyfikatów SSL. Certyfikaty SSL dla PostgreSQL 17 wykorzystywane są jedynie w komunikacji mMedica <-> baza mMedica, eArchiwum <-> baza eArchiwum, eRejestracja <-> baza eRejestracja. Moduły dodatkowe łączące się do bazy mMedica (np. mMWS, Konektor.eRejestracja, MIUD, Xpress Scan) muszą być skonfigurowane z certyfikatami wygenerowanymi dla PostgreSQL 17 z bazą mMedica.

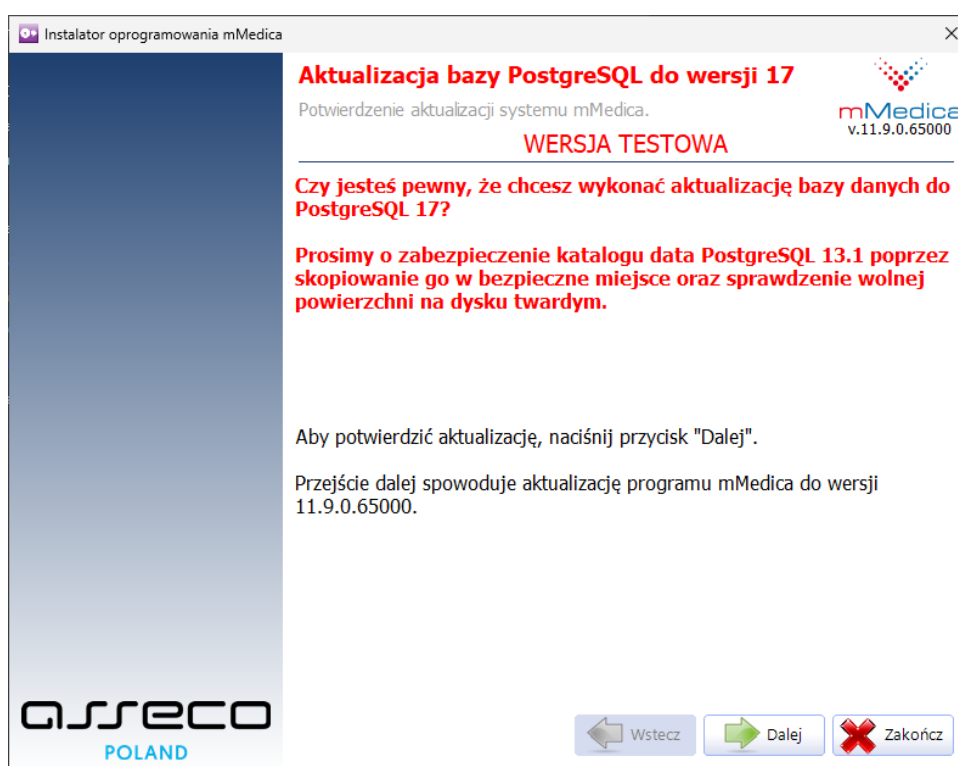
Ilustracje i zrzuty ekranu zamieszczone w niniejszej publikacji mają charakter instruktażowy i mogą odbiegać od rzeczywistego wyglądu ekranów.

## 1. Migracja na systemach operacyjnych Windows

mMigrator.exe umożliwia przeprowadzenie migracji danych z PostgreSQL 13 do PostgreSQL 17 w trybie specjalnej aktualizacji mMedica do wersji **11.9.0.65000**. **Migracja jest możliwa wyłącznie z mMedica w wersji 11.9.0 (moduły eArchiwum i eRejestracja również powinny być w tej wersji)**. Ponadto mMigrator.exe może zostać uruchomiony tylko w miejscu instalacji bazy PostgreSQL (tzn. na instalacji jednostanowiskowej lub na serwerze).

Przed przystąpieniem do migracji zalecamy zaktualizować oraz zrestartować system operacyjny Windows, a następnie **zabezpieczyć katalog data należący do PostgreSQL 13 poprzez skopiowanie go w bezpieczne miejsce** (przy wyłączonej usłudze postgresmm-13.1). Ponadto należy sprawdzić dostępność wolnej powierzchni na dysku oraz zalecamy wyłączyć oprogramowanie antywirusowe. W domyślnej konfiguracji migrator przeprowadza kopiowanie danych do katalogu .../PostgreSQL/17/data. Migrator przenosi wszystkie bazy mMedica, w tym bazy modułu eRejestracja oraz eArchiwum.

Po uruchomieniu programu mMigrator.exe **jako administrator** pojawi się okno powitalne.



Czas migracji zależy od wielkości zgromadzonych danych oraz wydajności komputera i może wynosić od kilku minut do nawet kilku godzin (sumarycznie nie powinien być dłuższy niż czas wykonania i odtworzenia wszystkich kopii zapasowych na klastrze). **W trakcie migracji dostęp do programu mMedica będzie niemożliwy.**

Po wyborze przycisku „Dalej” należy podać login i hasło do serwera PostgreSQL zgodne z rolą PostgreSQL **oraz kontem mMedica**. Użytkownik musi mieć uprawnienia wymagane do przeprowadzania aktualizacji systemu mMedica (takie same jak przy zwykłej aktualizacji).



W kolejnym kroku konieczne jest zaakceptowanie przypomnienia o konieczności zabezpieczenia danych.



Po złożeniu oświadczenia i wybraniu przycisku „Dalej” pojawi się okno konfiguracji SSL dla PostgreSQL 17. W procesie migracji zalecamy wybrać opcję „Wygeneruj certyfikaty za pośrednictwem serwera Asseco Poland z okresem ważności 5 lat” oraz „Udostępnij certyfikaty klienta za pośrednictwem serwera Asseco Poland przez 90 dni”. Po wybraniu opcji „Wygeneruj certyfikaty za pośrednictwem serwera Asseco Poland z okresem ważności 5 lat” migrator utworzy unikalny dla danej instalacji PostgreSQL zestaw certyfikatów SSL w formacie PEM zawierający takie pliki jak:

client.crt – publiczny certyfikat klienta

client.key – klucz prywatny klienta

root.crt – certyfikat CA

root.key – klucz prywatny CA

server.crt – publiczny certyfikat serwera

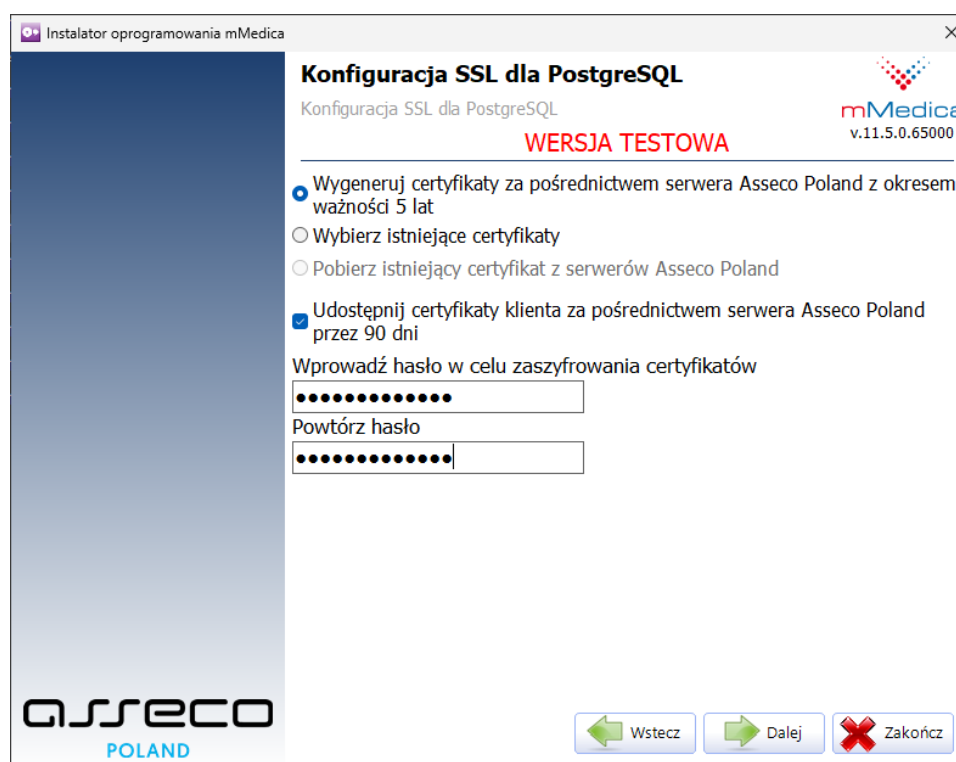
server.key – klucze prywatny serwera

Wszystkie certyfikaty będą zapisane pod ścieżką .../PostgreSQL/17/certs/

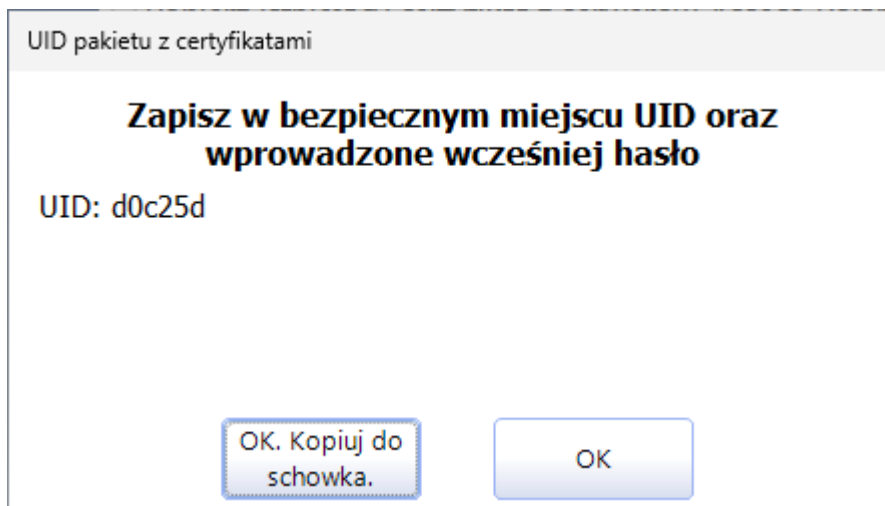
Ważność certyfikatów wygenerowanych przez Asseco wynosi 5 lat a ich aktualizacja jest planowana najwcześniej przy następnej migracji bazy danych po roku 2029.

Opcja „Udostępnij certyfikaty klienta za pośrednictwem serwera Asseco Poland przez 90 dni” umożliwia prostą konfigurację certyfikatów klienta na stacjach roboczych, która została opisana w rozdziale 4 tej instrukcji.

Certyfikaty będą przesyłane poprzez https. Hasło do archiwum z certyfikatami będzie tworzone przez użytkownika i musi mieć co najmniej 12 znaków. Serwer przechowujący certyfikaty nie będzie miał dostępu do hasła i nie będzie go używał.



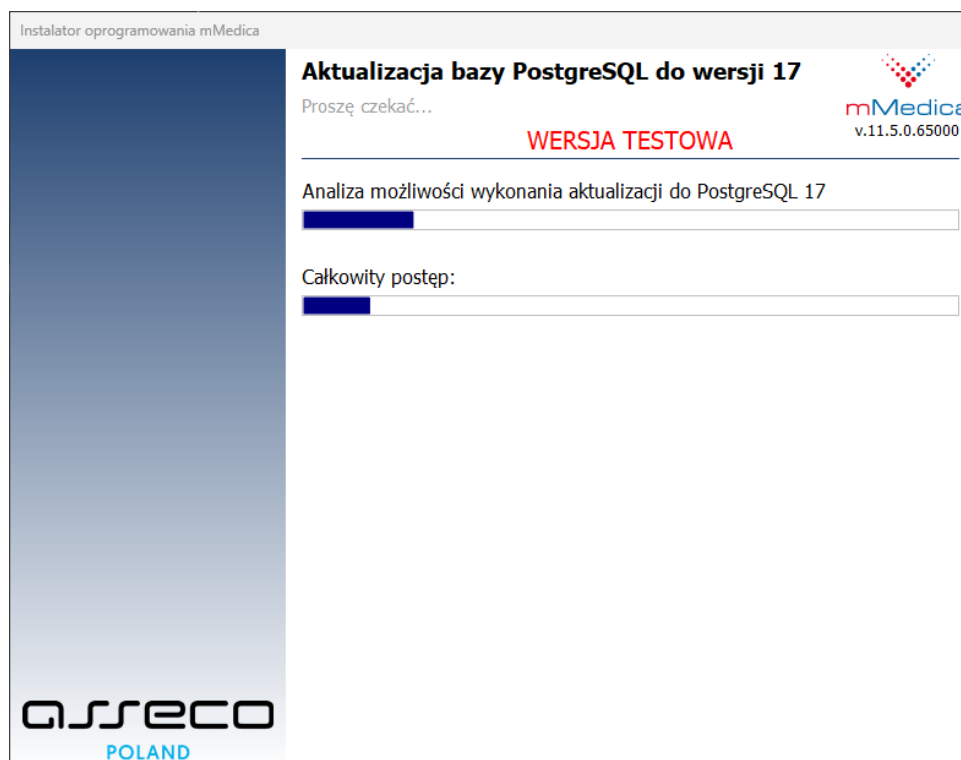
Po wyborze zalecanych ustawień oraz kliknięciu w przycisku „Dalej” pojawi się unikalny UID, który razem z hasłem należy zapamiętać. Będą one mogły być w przyszłości wykorzystane do zestawienia połączenia z PostgreSQL 17 po SSL na wszystkich stacjach roboczych opisanego w rozdziale 4 instrukcji.



### Uwaga!

Podane hasło oraz wygenerowane UID nie będą nigdzie zapisane a jego utrata może skutkować koniecznością ponownego udostępnienia certyfikatów za pośrednictwem trybu serwisowego instalatora i opcji „Konfiguracja SSL dla PostgreSQL” -> „Wybierz istniejące certyfikaty” -> „Udostępnij certyfikaty klienta za pośrednictwem serwera Asseco Poland przez 90 dni”. Z tej samej ścieżki można także skorzystać po wygaśnięciu udostępniania po upływie 90 dni.

Wybranie przycisku „OK” rozpocznie proces migracji danych.



W trakcie migracji OS Windows może poprosić o zezwolenie na dostęp PostgreSQL przez zaporę. Dla instalacji sieciowych należy zapewnić dostęp przez zaporę programowi postgres.exe. Zalecamy aby dostęp ten był ustawiony wyłączenie dla adresów IP z sieci lokalnej.

↑ > Panel sterowania > System i zabezpieczenia > Zapora Windows Defender > Dozwolone aplikacje

### Zezwalaj aplikacjom na komunikowanie się przez Zaporę Windows Defender

Aby dodać, zmienić lub usunąć dozwolone aplikacje i porty, kliknij pozycję **Zmień ustawienia**.

Jakie ryzyko wiąże się z zezwoleniem na komunikację aplikacji?

Zmień ustawie

Dozwolone aplikacje i funkcje:

Nazwa	Prywatne	Publiczne
<input checked="" type="checkbox"/> PostgreSQL Server	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Edytowanie aplikacji

Możesz zezwolić na komunikowanie się z tą aplikacją z dowolnego komputera, w tym z komputerów w Internecie lub w sieci.

Nazwa:

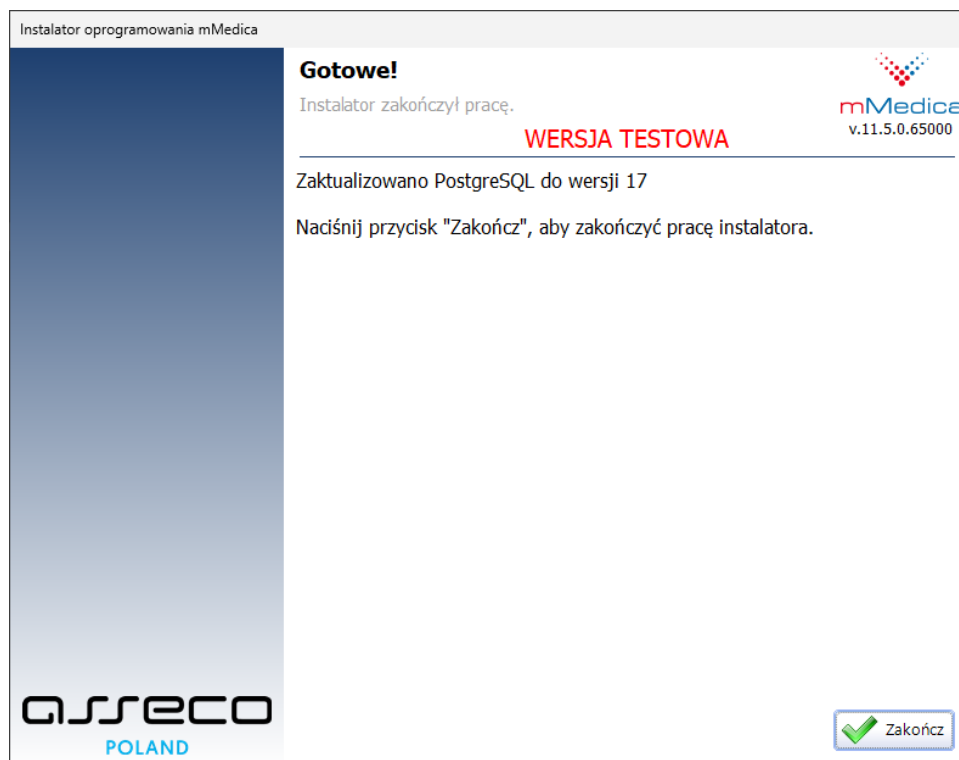
Ścieżka:

[Jakie ryzyko wiąże się z odblokowaniem aplikacji?](#)

Możesz wybrać, do których typów sieci dodać tę aplikację.

Zezwalaj na dostęp innej aplikacji

Jeśli migrator nie zgłosił błędu, oznacza to, że migracja się powiodła i można zakończyć pracę tej aplikacji. W przeciwnym wypadku migrator przywróci wersję mMedica sprzed migracji.



W przypadku wystąpienia błędu:

1. [...] could not open log file "pg\_upgrade\_internal.log": Permission denied:  
lub  
[...] You must have read and write access in the current directory
  - należy sprawdzić czy migrator został uruchomiony z konta o uprawnieniach administracyjnych oraz czy został uruchomiony z konta lokalnego (a nie domenowego)
  - należy rozpakować migrator np. za pomocą aplikacji 7-zip, ustawić pełne uprawnienia do tego katalogu dla wszystkich użytkowników, uruchomić go bezpośrednio z katalogu za pomocą pliku mmSetup.exe jako administrator
2. [...] "pg\_upgrade\_server.log" -D "C:/Program Files (x86)/PostgreSQL/13.1/data" -o "-p 50432 -b -c synchronous\_commit=off -c fsync=off -c full\_page\_writes=off -c vacuum\_defer\_cleanup\_age=0" start
  - Failure, exiting :
  - należy sprawdzić poleceniem netsh interface ipv4 show excludedportrange protocol=tcp czy port 50432 nie jest zajęty
  - można skorzystać z alternatywnego sposobu migracji opisanego w rozdziale 2.

W przypadku, gdy baza danych była replikowana konieczne będzie powtórzenie całego procesu utworzenia repliki zgodnie z instrukcją replikacji.

Po migracji należy wykonać aktualizację mMedica do wersji wyższej niż wersja migratora. Zaktualizować należy także mModuły (eRejestrację, eArchiwum i inne) oraz moduły firm partnerskich (MIUD, XPRESS SCAN, Wsparcie Zarządzania).

W mMedica istnieje mechanizm automatycznej aktualizacji stacji roboczych, który został opisany w rozdziale 4 tej instrukcji. Istnieje także możliwość aktualizacji stacji roboczych za pomocą instalatora mMedica w wersji **11.9.5** lub wyższej.

Instalatory są dostępne do pobrania w Centrum Zarządzania Licencjami pod adresem: <https://mmedica-licencje.asseco.pl/Download.aspx>

## 2. Alternatywna metoda migracji (odtworzenie kopii zapasowej wykonanej na PostgreSQL 13)

---

Nowa wersja mmBackup.exe (dla PostgreSQL 17) umożliwia odtworzenie w PostgreSQL 13 z kopii zapasowej wykonanej na wersji 11.9.0. Po odtworzeniu bazy w wersji 11.9.0 na komputerze z PostgreSQL 17 konieczne jest zaktualizowanie kont użytkowników za pomocą opcji napraw instalatora mMedica. W przeciwnym wypadku mogą wystąpić błędy autoryzacji podczas logowania się do mMedica.

Mechanizm ten może zostać wykorzystany jako alternatywna metoda przenoszenia danych do PostgreSQL 17 w którym **nie stosuje** się aplikacji mMigrator.exe.

- 1) Wyłączamy usługę mmService
- 2) Wykonujemy kopię zapasową baz mMedica w wersji 11.9.0
- 3) Odinstalowujemy mMedica
- 4) Instalujemy mMedica w wersji 11.9.5 z PostgreSQL 17
- 5) Odtwarzamy kopię zapasowe wykonane w wersji 11.9.0
- 6) **Uruchamiamy instalator w wersji 11.9.5 i wybieramy opcję NAPRAW**

Po instalacji zaktualizować należy także mModuły (eRejestrację, eArchiwum i inne) oraz moduły firm partnerskich (MIUD, XPRESS SCAN, Wsparcie Zarządzania).

W przypadku, gdy baza danych była replikowana konieczne będzie powtórzenie całego procesu utworzenia repliki zgodnie z instrukcją replikacji.

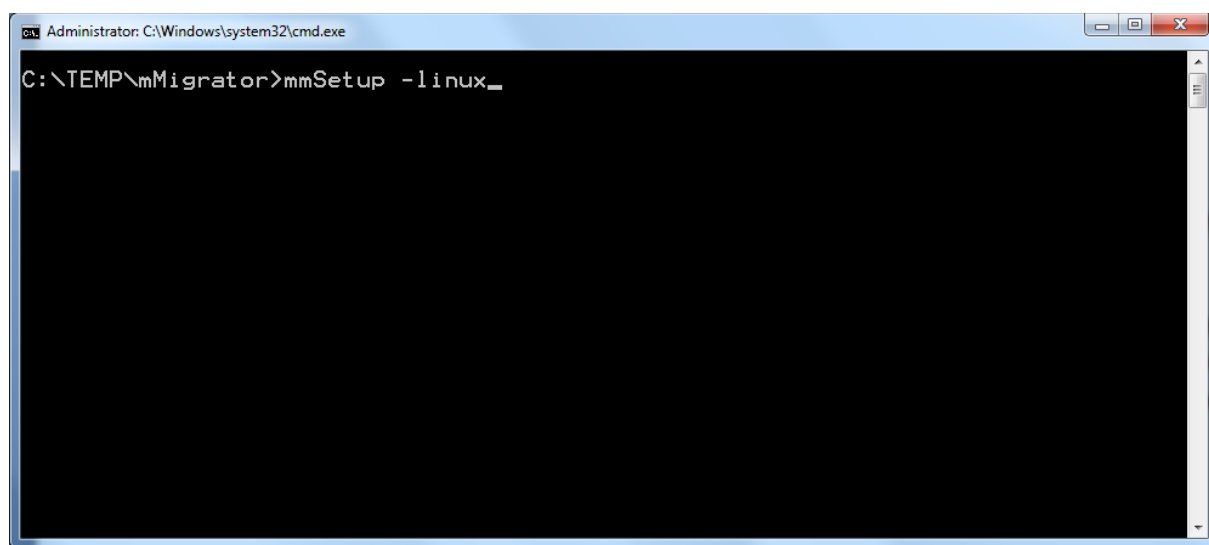
### 3. Migracja na systemach operacyjnych z rodziny Linux

mMigrator.exe wspiera proces migracji baz danych PostgreSQL 13 do PostgreSQL 17 na systemach operacyjnych z rodziny Linux. mMigrator.exe działa także z bazami danych modułu eRejestracja oraz eArchiwum.

W celu rozpoczęcia migracji, należy zaktualizować system do wersji **11.9.0** dowolną stacją roboczą w sieci posiadającą połączenie z PostgreSQL w wersji **13.5** (<http://mmedica-download.asseco.pl/inst/inne/PostgreSQL-13.5-Linux.tar>).

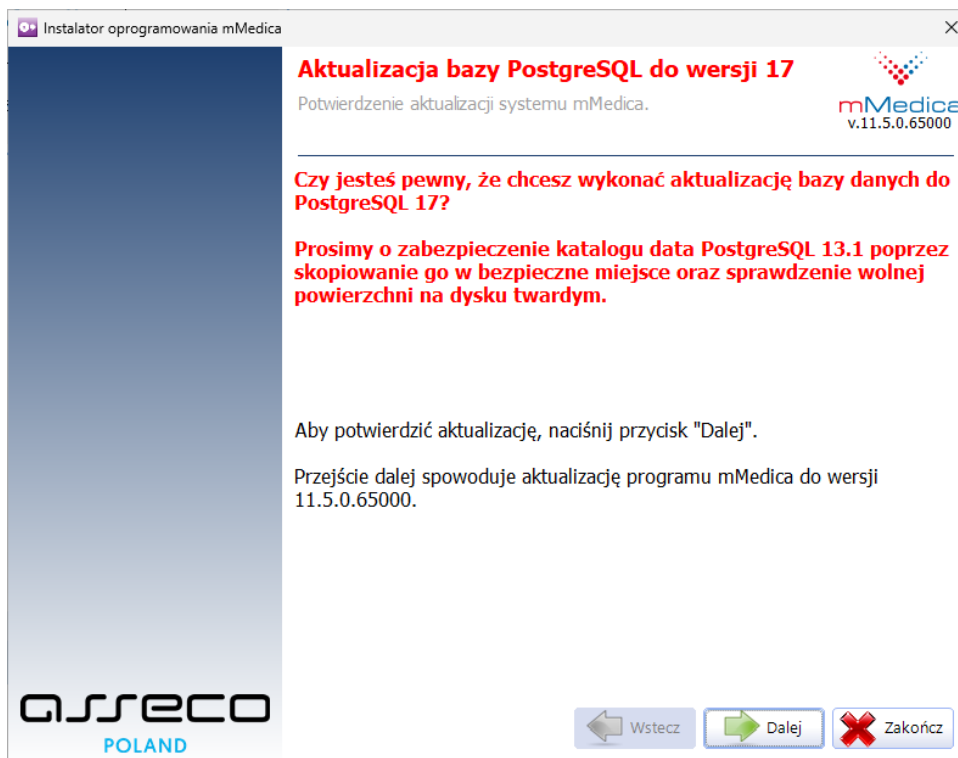
Certyfikaty SSL, można wygenerować za pomocą instalatora mMedica w wersji 11.9.5 lub wyższej za pomocą pliku mmSetup.exe wywołanego z parametrem **-certs**.

Po przygotowaniu certyfikatów należy rozpakować na tej samej stacji roboczej archiwum mMigrator.exe np. przy użyciu programu 7zip. W następnej kolejności należy wywołać mmSetup.exe z parametrem **-linux**.



W razie potrzeby istnieje możliwość wskazania alternatywnego do podanego podczas instalacji hosta i numeru portu za pośrednictwem parametrów **-h** oraz **-p** (np. **-h 192.168.100.100**).

Po wykonaniu polecenia **mmSetup.exe -linux** pojawi się okno powitalne migratora.



Po wyborze przycisku „Dalej” należy podać login i hasło do serwera PostgreSQL zgodne z rolą PostgreSQL oraz użytkownikami w bazach danych. Użytkownik musi mieć uprawnienia wymagane do przeprowadzania aktualizacji.



W celu rozpoczęcia procesu migracji należy wybrać przycisk „Krok1: weryfikacja spójności danych w PostgreSQL 13”.



Jeśli instalator nie wykryje błędów można przystąpić do kolejnego etapu w którym należy na OS Linux.

- wyłączyć PostgreSQL 13
- przeprowadzić instalację PostgreSQL 17 analogicznie z poniższym przykładem na OS Linux z uwzględnieniem konfiguracji postgresql.conf oraz pg\_hba.conf (**PostgreSQL zgodny z mMedica wymaga podmiiany wybranych plików**)
- Następnie należy uruchomić program pg\_upgrade wskazując w parametrach odpowiednie ścieżki do starego i nowego PostgreSQL oraz certyfikatów SSL
- po wykonaniu pg\_upgrade należy uruchomić PostgreSQL 17 a następnie wykonać w instalatorze „Krok 2: aktualizacja danych w PostgreSQL 17”

Minimalna wersja Ubuntu na którym działa PostgreSQL 17 od mMedica to **16.04**

Przykładowa migracja na OS Ubuntu w wersji 24.04 dla PostgreSQL 13 zainstalowanego w ścieżce /usr/local/pgsql/ i skonfigurowaną usługą o nazwie postgresql.

Przed przystąpieniem do prac należy wykonać kopię zapasową bazy danych i zapisać ją w bezpiecznym miejscu.

Poniższe polecenia najlepiej jest wykonać po wykonaniu w migratorze „Krok 1: weryfikacja spójności danych w PostgreSQL 13”

```
#zatrzymanie postgresql 13
```

```
sudo apt update
```

```
sudo mv /usr/local/pgsql/ /usr/local/pgsql13/
```

```
wget https://ftp.postgresql.org/pub/source/v17.0/postgresql-17.0.tar.gz
```

```
tar xvfz postgresql-17.0.tar.gz
```

```
cd postgresql-17.0/
sudo apt install -y build-essential libreadline-dev zlib1g-dev flex bison libxml2-dev libxslt1-dev libssl-dev libpam0g-
dev libedit-dev tcl-dev uuid-dev
sudo ./configure --prefix=/usr/local/pgsql/ --without-icu --with-openssl --without-readline
sudo make
sudo make install
sudo mkdir /usr/local/pgsql/data
sudo chown -R twoja_nazwa_uzytkownika /usr/local/pgsql/data
```

#następnie należy podmienić pliki PostgreSQL 17 na pliki znajdujące się w archiwum PostgreSQL-17.0-Linux.tar

**#initdb musi być wykonany dla locale pl\_PL.CP1250**

```
/usr/local/pgsql/bin/initdb -D /usr/local/pgsql/data
```

#przed przystąpieniem do pg\_upgrade należy utworzyć katalog na certyfikaty

```
sudo mkdir /usr/local/pgsql/certs
```

```
sudo chown -R twoja_nazwa_uzytkownika /usr/local/pgsql/certs
```

#należy wgrać do niego certyfikaty SSL (można je wygenerować za pomocą instalatora mMedica uruchomionego z parametrem - mmSetup.exe -certs)

#należy odpowiednio skonfigurować postgresql.conf w zakresie parametru listen\_addresses oraz parametrów dot. SSL:

```
ssl = on
```

```
ssl_ca_file = '/usr/local/pgsql/certs/root.crt'
```

```
ssl_cert_file = '/usr/local/pgsql/certs/server.crt'
```

```
ssl_key_file = '/usr/local/pgsql/certs/server.key'
```

#uprawnienia do certyfikatów SSL

```
cd /usr/local/pgsql/certs
```

```
chmod 700 .
```

```
chmod 400 *.key
```

```
chmod 400 *.crt
```

#polecenie pg\_upgrade należy wykonać z poziomu katalogu home użytkownika

```
cd /home/dwoja_nazwa_uzytkownika
```

```
sudo -u twoja_nazwa_uzytkownika /usr/local/pgsql/bin/pg_upgrade -b /usr/local/pgsql13/bin -d
/usr/local/pgsql13/data -B /usr/local/pgsql/bin -D /usr/local/pgsql/data -U postgres -v -L
/usr/local/pgsql/certs/client.crt -E /usr/local/pgsql/certs/client.key -M /usr/local/pgsql/certs/root.crt
```

Prawidłowo wykonany pg\_upgrade kończy się komunikatem:

**Upgrade Complete**

Optimizer statistics ...

W przypadku błędu, może być konieczne ponowne zainicjowanie klastra bazy danych PostgreSQL 17 za pomocą initdb i odpowiednie powtórzenie poleceń.

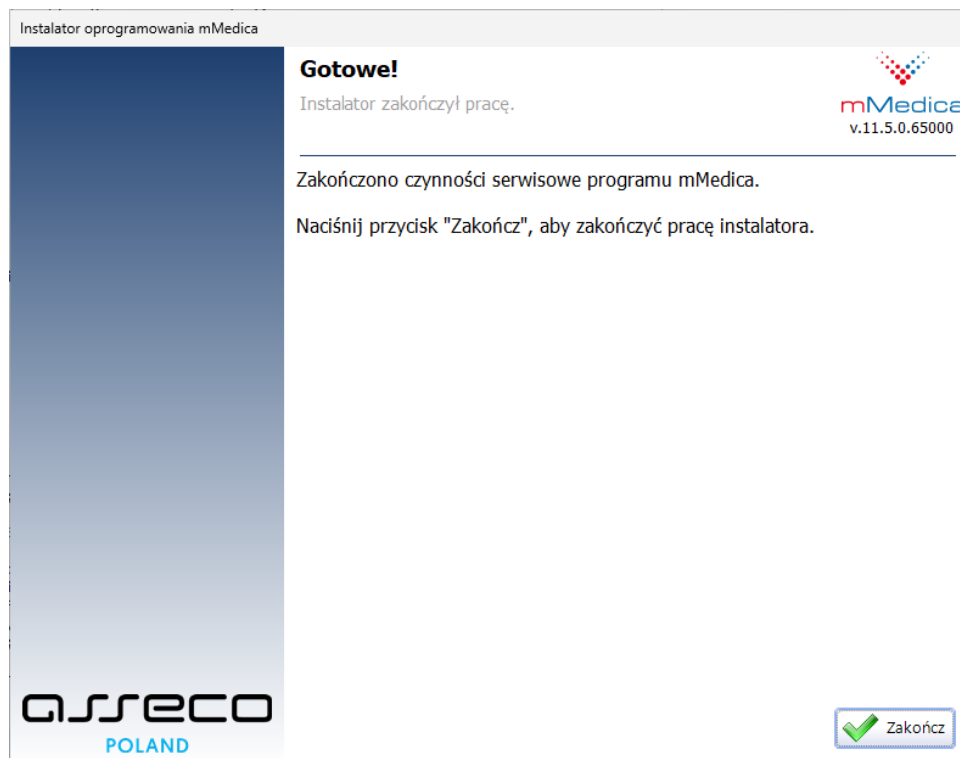
Następnie należy skonfigurować pg\_hba.conf dodając wpis umożliwiający połączenia z sieci lokalnej jak np.

```
# TYPE DATABASE USER ADDRESS METHOD
# IPv4 local connections:
hostssl all all 127.0.0.1/32 md5 clientcert=verify-ca
hostssl all all 192.168.0.0/16 md5 clientcert=verify-ca

# IPv6 local connections:
hostssl all all ::1/128 md5 clientcert=verify-ca
# Allow replication connections from localhost, by a user with the
# replication privilege.
hostssl replication all 127.0.0.1/32 md5 clientcert=verify-ca
hostssl replication all ::1/128 md5 clientcert=verify-ca
```

**W ostatnim kroku należy uruchomić PostgreSQL 17 oraz zaktualizować dane w bazach za pomocą przycisku „Krok 2: aktualizacja danych w PostgreSQL 17”.**

Jeśli migrator nie zgłosił błędu, oznacza to, że migracja się powiodła i można zakończyć pracę tej aplikacji.



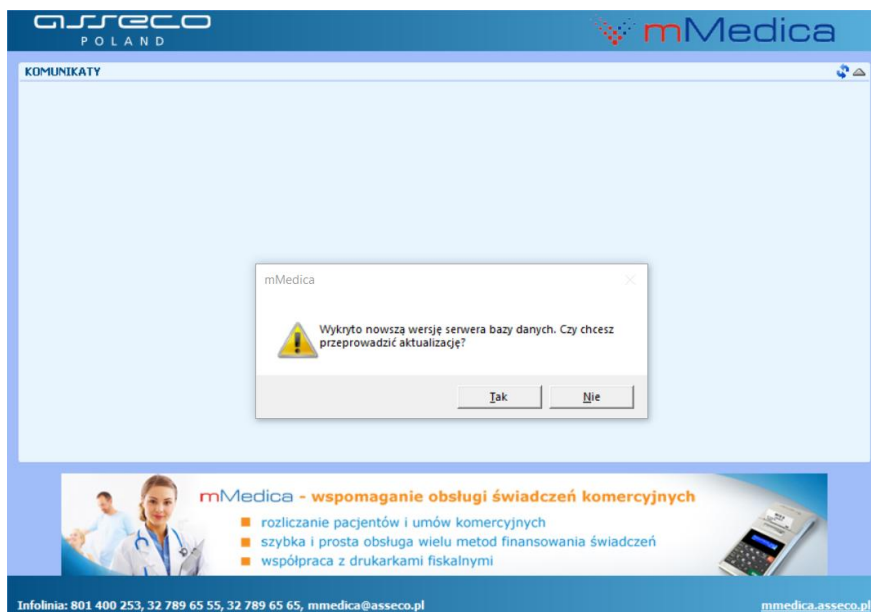
Po migracji należy wykonać aktualizację mMedica do wersji wyższej niż wersja migratora. Zaktualizować należy także mModuły (eRejestrację, eArchiwum i inne) oraz moduły firm partnerskich (MIUD, XPRESS SCAN, Wsparcie Zarządzania).

W przypadku, gdy baza danych była replikowana konieczne będzie powtórzenie całego procesu utworzenia repliki zgodnie z instrukcją replikacji.

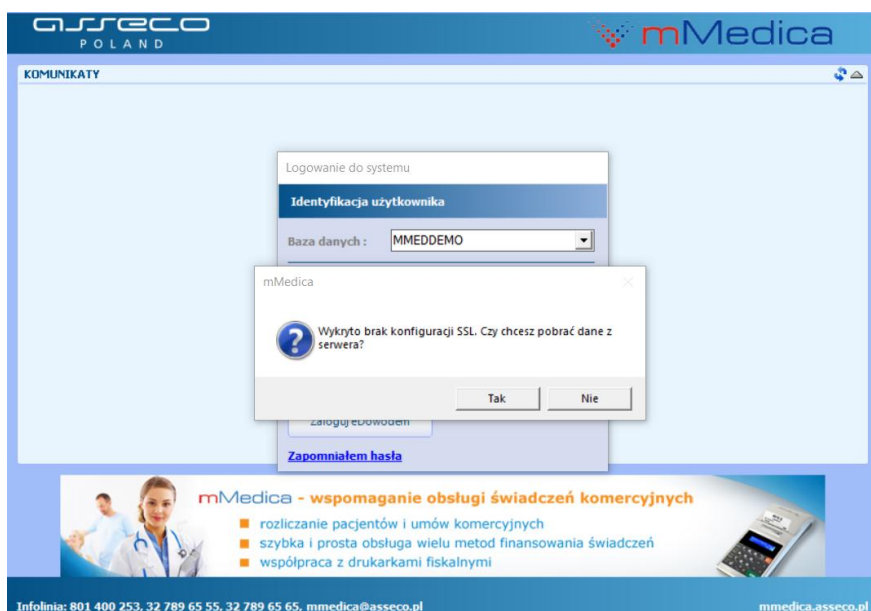
## 4. Aktualizacja stacji roboczych mMedica w sieci

Po zrealizowaniu migracji na serwerze należy zaktualizować wszystkie stacje robocze, które łączą się do bazy PostgreSQL. W tym celu można wykorzystać instalator mMedica w wersji wyższej niż wersja migratora.

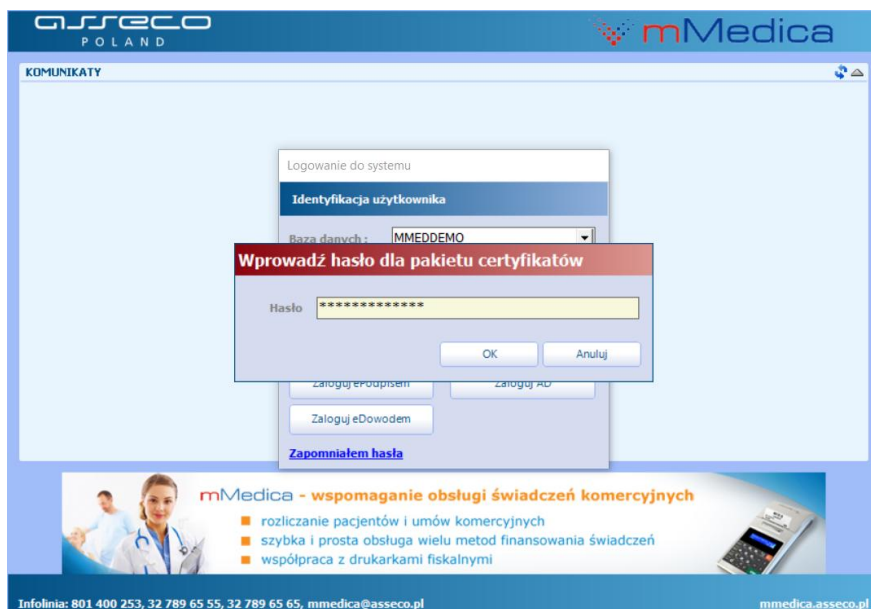
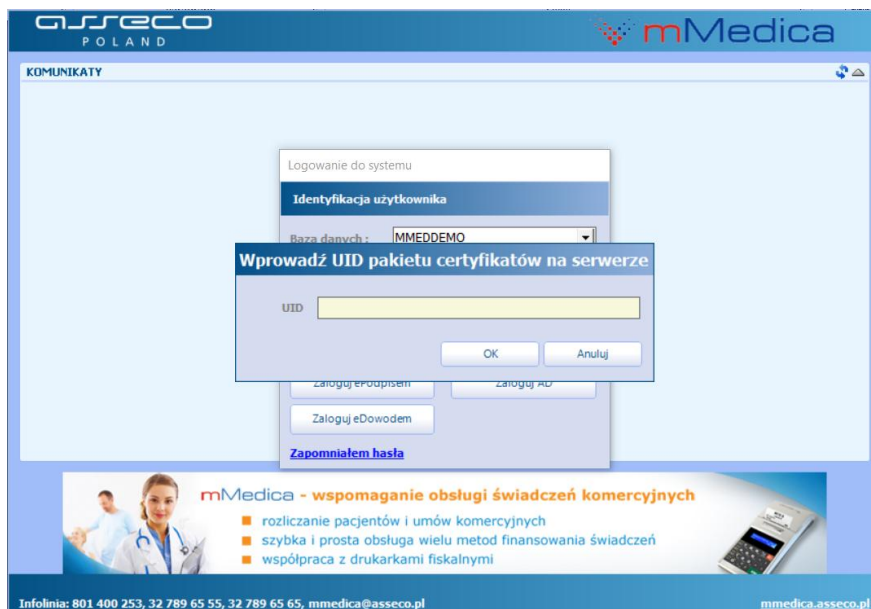
Alternatywnie można zastosować mechanizm automatycznej aktualizacji z wykorzystaniem serwerów Asseco na których znajduje się mMedica.exe zgodna z PostgreSQL 17. W takiej sytuacji przy pierwszej próbie logowania do PostgreSQL 17 na wersji starszej niż **11.9.5**, użytkownik otrzyma komunikat informujący o tym, że próbuje się połączyć do nowej bazy danych. Aby aktualizacja i konfiguracja SSL przebiegła bez błędów związanych z uprawnieniami mMedica musi być uruchomiona za pomocą opcji "Uruchom jako administrator".



Po akceptacji procesu aktualizacji mMedica pobierze wymagane pliki do zestawienia połączenia z PostgreSQL 17 i wykryje brak certyfikatów SSL klienta.



W następnym kroku będzie można podać kod UID wraz z hasłem w celu pobrania certyfikatów SSL i zainstalowania.



Po pobraniu certyfikatów i poprawnym logowaniu nastąpi aktualizacja (jeśli w współdzielonym folderze sieciowym będzie nowsza wersja mMedica.exe to zostanie pobrana i zastąpiona wersją mMedica.exe z serwerów Asseco Poland).

Certyfikaty SSL (client.crt, client.key oraz root.crt) wymagane do połączenia się mMedica z bazą danych zapisywane są domyślnie w ścieżce:

C:\Program Files (x86)\ASSECO\mMedica\certs\