mMedica

Moduł Archiwum – instalacja i konfiguracja

Spis treści

1. WSTĘP 6

2. ARCHITEKTURA ORAZ WYMAGANIA 8

2.1. MIGRACJA Z WERSJI .NET CORE 3.1 DO .NET 6.0 8

2.2. PUBLIKOWANIE ARCHIWUM 9

2.3. WYMAGANIA SPRZĘTOWE ORAZ PROGRAMOWE 9

2.4. ZASADA DZIAŁANIA ASP .NET CORE Z SERWERAMI WWW 10

2.4.1. Hosting w procesie 10

2.4.2. Hosting poza procesem 10

2.5. MIAM – PODSTAWOWE INFORMACJE 11

2.6. KOMPONENT MMDAB 11

3. INSTALACJA DLA WINDOWS 12

3.1. INSTALACJA W SYSTEMACH WINDOWS 12

3.2. WYMAGANIA 12

3.3. INSTALACJA SERWERA IIS 13

3.4. INSTALACJA ASP .NET CORE WRAZ Z MODUŁEM IIS 17

3.5. INSTALACJA IIS PO INSTALACJI ASP .NET CORE 19

3.6. KB2533623 DLA WINDOWS 8.1, WINDOWS SERVER 2012 R2 20

3.7. KB3118401 DLA WINDOWS 8.1 21

3.8. INSTALACJA ZA POMOCĄ INSTALATORA 22

3.9. INSTALACJA DODATKOWYCH MODUŁÓW/KOMPONENTÓW 28

3.10. INSTALACJA MANUALNA 29

3.11. KONFIGURACJA NAZWY APLIKACJI 38

3.12. WERYFIKACJA INSTALACJI 39

3.13. DODATKOWA KONFIGURACJA IIS 41

3.13.1. Konfiguracja typów MIME w IIS 41

3.13.2. Konfiguracja certyfikatu SSL 42

3.13.3. Konfiguracja uwierzytelniania certyfikatem TLS 44

3.13.4. Zaawansowana konfiguracja witryn 50

3.13.5. Zaawansowana konfiguracja aplikacji 52

3.14. DOINSTALOWANIE KOMPONENTÓW 54

3.15. RESTARTOWANIE I ZATRZYMYWANIE KOMPONENTÓW 55

3.16. AKTUALIZACJA MODUŁU 56

4. INSTALACJA W DYSTRYBUCJACH LINUX 57

4.1. WYMAGANIA 57

4.2. INSTALACJA 57

4.3. INSTALACJA BAZY DANYCH ARCHIWUM 58

4.4. INSTALACJA WYMAGANEGO OPROGRAMOWANIA 58
4.5. KONFIGURACJA SERWERA ORAZ INSTALACJA MODUŁU 59
4.6. KONFIGURACJA NAZWY APLIKACJI 61
4.7. KONFIGURACJA ADRESU APLIKACJI 62
4.8. WERYFIKACJA INSTALACJI 62
4.9. KONFIGURACJA DODATKOWA APACHE 65
4.9.1. Konfiguracja typów MIME 65
4.9.2. Konfiguracja certyfikatu SSL 65
4.9.3. Konfiguracja uwierzytelniania certyfikatem TLS 66
4.9.4. Zaawansowana konfiguracja witryn 70
4.10. DOINSTALOWANIE KOMPONENTÓW 71
4.11. KONFIGURACJA WIELU ARCHIWUM LUB MMDAB NA JEDNYM SERWERZE 71
4.12. RESTARTOWANIE I ZATRZYMYWANIE KOMPONENTÓW 72
4.13. AKTUALIZACJA MODUŁU 72
4.14. POMOC 73

5. KONFIGURACJA APLIKACJI 74

5.1. KONFIGURACJA POŁĄCZENIA Z BAZAMI DANYCH 74
5.2. ZABEZPIECZENIE PRZED UŻYCIEM IFRAME 74
5.3. KONFIGURACJA NAZWY ORAZ ADRESU APLIKACJI 75
5.4. PRZEKIEROWANIE NAGŁÓWKÓW Z PROXY 75
5.5. URUCHAMIANIE WIELU MODUŁÓW WEWNĘTRZNYCH TEGO SAMEGO TYPU PRZEZ MMDAB 76
5.6. KONFIGURACJA MAKSYMALNEGO ROZMIARU ŻĄDANIA 77

6. ZARZĄDZANIE ORAZ KOPIE ZAPASOWE BAZ DANYCH 78

6.1. KOPIE BAZY DANYCH 78
6.1.1. Wykonywanie kopii bazy danych 78
6.1.2. Odtwarzanie bazy danych 78
6.1.3. Operacje na zdalnym serwerze PostgreSQL 79
6.1.4. Uproszczenie wykonywania kopii 79

7. BEZPIECZEŃSTWO MODUŁU 81

7.1. INFRASTRUKTURA 81
7.1.1. Zewnętrzny hosting lub VPS 81
7.1.2. Protokół SSL 81
7.1.3. VPN 82
7.2. OPROGRAMOWANIE 82
7.2.1. Konta użytkowników 82
7.2.2. Oprogramowanie antywirusowe 82
7.2.3. Firewall 82

7.2.4. Nieużywane protokoły TCP IP oraz protokoły serwera WWW ... 83
7.3. KONFIGURACJA MODUŁU ... 84
7.4. ZABEZPIECZENIA MODUŁU ... 84
7.4.1. Token bezpieczeństwa ... 84
7.4.2. Blokowanie adresów IP oraz kont ... 84
7.4.3. Inne ... 84
7.5. FILTROWANIE KOMUNIKACJI Z WYBRANYMI ADRESAMI IP ... 85
7.6. INTEGRACJA Z MODUŁEM EKOPIA+ ... 86
7.7. POZOSTAŁE ZALECENIA ... 86

8. KONFIGURACJA ARCHIWUM ... 87

8.1. PIERWSZE URUCHOMIENIE ... 87
8.1.1. Konfiguracja programu mMedica ... 89
8.2. ZMIANA HASŁA ... 90
8.3. STATUS APLIKACJI ... 91
8.4. DZIENNIK SYSTEMOWY ... 91
8.4.1. Zakładka „Portal" oraz „API" ... 93
8.5. LICENCJE ... 94
8.6. UŻYTKOWNICY ... 96
8.6.1. Lista użytkowników ... 96
8.6.2. Historia logowań ... 98
8.7. REJESTR ZABLOKOWANYCH IP ... 98
8.7.1. Portal ... 98
8.7.2. API mMedica ... 99
8.8. POBRANE DOKUMENTY ... 99
8.9. USUNIĘTE DOKUMENTY ... 100
8.10. HISTORIA ZMIAN WIDOCZNOŚCI DOKUMENTÓW ... 101
8.11. KONFIGURACJA ... 101
8.12. KOPIE ZAPASOWE BAZY DANYCH ... 105
8.12.1. Historia kopii zapasowych ... 105
8.12.2. Automatyczna kopia zapasowa ... 105
8.12.3. Zabezpieczenia kopii zapasowej ... 107
8.13. AUTORYZOWANE PODMIOTY W HUB IM ... 107
8.14. STATYSTYKI ... 108

9. KOMUNIKACJA ORAZ SYNCHRONIZACJA DANYCH Z MMEDICA ... 109

9.1. KOMUNIKACJA Z MMEDICA DO ARCHIWUM ... 109
9.2. KOMUNIKACJA Z MODUŁU EREJESTRACJA DO ARCHIWUM ... 109
9.3. KOMUNIKACJA Z MMEDICA DO SYSTEMU INFORMACJE MEDYCZNE ... 109
9.4. KOMUNIKACJA Z SYSTEMU INFORMACJE MEDYCZNE DO ARCHIWUM ... 110

9.5. Komunikacja z systemu Informacje Medyczne do bazy danych mMedica 111
9.6. Diagnostyka komunikacji 111

10. POBIERANIE DANYCH DIAGNOSTYCZNYCH 112

11. ROZWIĄZANIA CZĘSTYCH PROBLEMÓW 112

11.1. Nieprawidłowe hasło usług sieciowych (token) 112
11.2. Zapomniane hasło do konta administratora 112
11.3. Brak licencji na moduł w MIAM 112
11.4. Nieprawidłowe ustawienia Portalu – odtwórz. kopii bazy danych Archiwum 113
11.5. Biała strona komponentu po instalacji przez instalator na IIS 113
11.6. Błąd 403.4 na localhost lub na adresie komponentu na IIS 113
11.7. Błąd 500.21 w IIS 113
11.8. Błąd 502.5 w IIS 113
11.9. Polecenie dotnet nie jest rozpoznawalne – Linux 114
11.10. Status serwisu Main process exited – Linux 114
11.11. Brak portu w statusie usługi – Linux 114
11.12. Strona jest widoczna wyłącznie z komputera lokalnego 115
11.13. Przekroczenie czasu realizacji operacji na bazie danych (timeout) 115
11.14. Brak pliku api-ms-win-crt-runtime-l1-1-0 – Windows 115
11.15. Błąd „Unspecified certificate from client” w mMedica 115

1. Wstęp

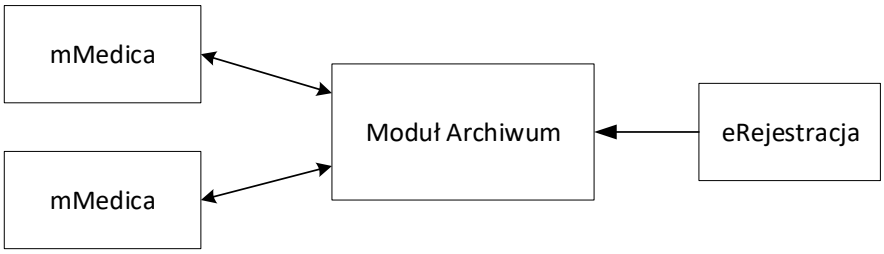
Niniejsza instrukcja opisuje architekturę, proces instalacji oraz konfiguracji modułu Archiwum (nazwa licencyjna eArchiwum). Dokument dostarcza również informacji dotyczących bezpieczeństwa.

Uwaga: Moduł eArchiwum i moduł Integracji z eRepozytorium w Chmurze nie mogą być uruchomione jednocześnie dla tej samej instalacji.

Moduł Archiwum jest systemem odpowiedzialnym za gromadzenia dokumentów medycznych. Dokumenty są przechowywane w dedykowanej bazie danych w formie dokumentów HL7 CDA.

Program mMedica integrując się z modułem Archiwum może w nim składować dokumenty medyczne, wyszukiwać, pobierać oraz usuwać dokumenty. Scentralizowany magazyn dokumentów pozwala na wygodne i bezpieczne zarządzanie danymi. Moduł Archiwum zapisuje historie operacji związane z usuwaniem oraz pobieraniem dokumentów. Dokumenty w Archiwum przechowywane są z dokładnością do numeru REGON jednostki medycznej, co oznacza, że wiele jednostek o różnych lub tych samych numerach REGON mogą być skomunikowane z jednym modułem Archiwum. Jednak jednostki mają dostęp wyłącznie do dokumentów przypisanych do swojego numeru REGON.

W przypadku posiadania modułu eRejestracja+ udostępnione przez personel w mMedica dokumenty medyczne pacjentów mogą być wyszukiwane, wyświetlane oraz pobierane przez użytkowników z poziomu Portalu eRejestracja.



Rysunek 1: Integracja programu mMedica, aplikacji eRejestracja i modułu Archiwum

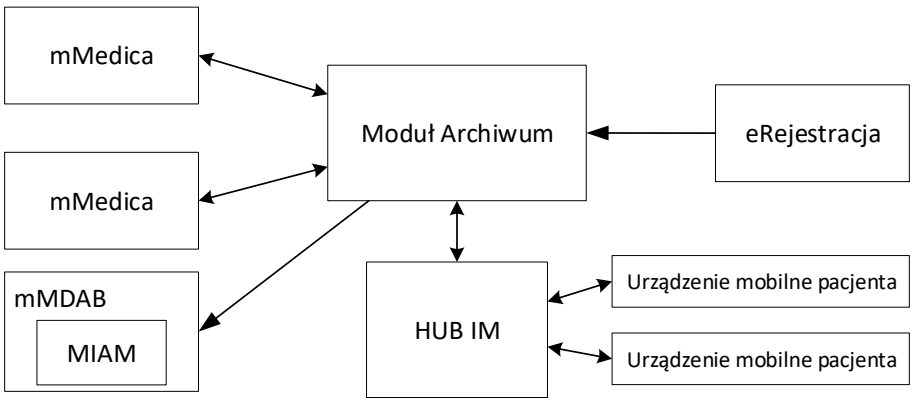
Dodatkowo moduł Archiwum może zostać opcjonalnie zintegrowany z systemem Informacje Medyczne (wymaga to stałego i publicznego adresu IP komputera, na którym zostanie dokonana instalacja), który umożliwia pacjentom dostęp do swoich dokumentów medycznych za pomocą urządzeń mobilnych opartych o system Android lub iOS poprzez aplikację Asseco Informacje Medyczne. Pacjent jest zatwierdzany w systemie Informacje Medyczne w procesie autoryzacji urządzenia mobilnego, jednak do zakończenia tego procesu ko-

nieczne jest wygenerowanie numeru PIN z poziomu aplikacji mMedica lub eRejestracja. Przed wygenerowaniu numeru PIN powinna zostać dokonana procedura wysłania do HUB IM zgody użytkownika na komunikacje z daną jednostką medyczną. Zgoda ta może zostać również wycofana, co również skutkuje wysłaniem informacji do HUB IM. Personel z poziomu aplikacji mMedica decyduje, czy udostępnić wybrany dokument medyczny. Pacjent może przeglądać udostępnione dokumenty oraz je pobierać. Ponadto pacjent może również utworzyć własny dokument medyczny, np. na podstawie zdjęcia (jako załącznik w formacie PDF) lub skorzystać z dokumentu dostarczonego z innej jednostki medycznej i wysłać do placówki. Taki dokument jest oznaczony w programie mMedica jako dokument pacjenta i może być włączony do dokumentacji medycznej. W przypadku, w którym pacjent utraci zautoryzowane do komunikacji z HUB IM urządzenie mobilne może zwrócić się do placówki z prośba o awaryjne wyrejestrowanie z HUB IM. Ruch dokumentów pomiędzy jednostką medyczną a urządzaniami mobilnymi odbywa się za pośrednictwem HUB IM. Komunikacja jest zabezpieczona przez klucze prywatne i publiczne pomiędzy systemami końcowymi (aplikacja mobilna oraz Archiwum), dlatego też HUB IM jako pośrednik nie jest w stanie odczytać ani zmodyfikować istotnych danych. Integracja z systemem Informacje Medyczne wymaga, aby z poziomu programu mMedica została dokonana procedura autoryzacji podmiotu w HUB IM. Możliwe jest również wycofanie autoryzacji do komunikacji z HUB IM.

Integracja z systemem Informacje Medyczne wymaga zakupu licencji na Moduł Integracji Aplikacji Mobilnych.

Integracja Archiwum z systemem Informacje Medyczne pozwala również na:

- wysyłanie powiadomień z programu mMedica do aplikacji mobilnej Informacje Medyczne na urządzeniach mobilnych pacjenta (wymaga dodatkowo licencji na moduł mPowiadomienia),
- sprawdzanie w aplikacji mobilnej Informacje Medyczne stanu kolejki do gabinetów, gdzie pacjent jest zarejestrowany (wymaga dodatkowo licencji na moduły System Kolejkowy oraz mPowiadomienia).



Rysunek 2: Integracja programu mMedica, aplikacji eRejestracja, systemu Informacje Medyczne i modułu Archiwum

2. Architektura oraz wymagania

Moduł Archiwum to jedna aplikacja, która składa się z obszarów:

- Portal – aplikacja webowa, do której mogą się logować administratorzy,
- mMedica API – interfejs do integracji z programem mMedica oraz eRejestracja,
- XDS API – interfejs wymiany dokumentów za pomocą standardu IHE XDS.b,
- Powiadomienia API – interfejs obsługi powiadomień Informacje Medyczne dla HUB IM,
- Kolejki API – interfejs obsługi kolejek dla systemu IM.

Dodatkowo z Modułem Archiwum mogą zostać zainstalowane:

- MIAM – usługa sieciowa pośrednicząca w dostępnie do bazy danych mMedica.
- mMDAB – usługa sieciowa, która zarządza i uruchamia inne usługi sieciowe pośredniczące w dostępie do bazy danych mMedica np. MIAM.

Portal jest stroną internetową dla administratorów do konfiguracji i monitorowania modułu. Z kolei API dla programu mMedica/eRejestracja oraz dla XDS pośredniczą w wymianie informacji pomiędzy bazą danych Archiwum i kolejno bazą danych mMedica (za pośrednictwem mMedica) oraz urządzeniem mobilnym z oprogramowaniem Informacje Medyczne.

mMDAB oraz MIAM są elementami, które pozwalają na komunikacje z aplikacji Archiwum do bazy danych mMedica. mMDAB oraz MIAM są elementami opcjonalnymi - oznacza to, że nie muszą być one instalowane, jeśli nie są wykorzystywane funkcjonalności, które są przez nie oferowane.

Aplikacje Archiwum, mMDAB oraz MIAM są uruchamiane za pomocą platformy .NET Core firmy Microsoft na wspieranych systemach operacyjnych Microsoft Windows oraz wybranych dystrybucjach systemów opartych o jądro Linux.

2.1. Migracja z wersji .NET Core 3.1 do .NET 6.0

Migracja do .NET 6.0 wymaga od użytkownika zainstalowania nowej wersji środowiska uruchomieniowego ASP .NET Core 6.0. W przypadku instalacji mModułów pod IIS, należy zainstalować wersję Bundle-Hosting\WindowsHosting - odnośnik. W trybie aktualizacji instalator mModułów jest w stanie sam pobrać i zainstalować nową wersję ASP .NET Core 6.0, jeśli taka nie została wcześniej zainstalowana. Proces instalacji oraz aktualizacji odbywa się w bardzo zbliżony sposób do poprzednich wersji. Odpowiednie kroki zostały opisane w działach *3. Instalacja dla Windows* oraz *4.* Instalacja w dystrybucjach Linux.

Uwaga: Przed wykonaniem procesu migracji, należy bezwzględnie wykonać kopię bazy danych modułu Archiwum.

Uwaga: Istnieje możliwość posiadania jednocześnie zainstalowanego środowiska uruchomieniowego .NET Core 3.1 oraz .NET 6.0.

2.2. Publikowanie Archiwum

Archiwum należy w uproszczeniu traktować jako stronę internetową, co oznacza, że podlega ona takim samym zasadom udostępniania w sieci Internet za pomocą serwerów WWW. Serwer WWW to oprogramowanie pozwalające opublikować stronę internetową w taki sposób, aby mogła ona być widoczna dla przeglądarek internetowych, które są zainstalowane na innych komputerach. Serwer WWW może być zainstalowany zarówno na komputerze użytkowym (np. wykorzystującym oprogramowanie mMedica), jak i specjalnie do tego dedykowanym. Wymogiem, aby moduł Archiwum był widoczny w sieci Internet, jest posiadanie publicznego (najlepiej stałego) adresu IP. Jednym z rozwiązań jest skorzystanie z usług hostingowych lub wirtualnych prywatnych serwerów (VPS), czyli zazwyczaj odpłatnych usług, w których firma zewnętrzna umieszcza w swoich zasobach strony internetowe oraz usługi sieciowe.

Archiwum może mieć adres domenowy, czyli przyjazną do zapamiętania nazwę, po wpisaniu której zostanie wyświetlone. Adres domenowy może zostać wykupiony (często w pakiecie z usługą hostingową) poprzez zewnętrzny podmiot. Bez wykorzystywania adresu domenowego, dostęp do komponentów możliwy jest przez adres IP komputera, na którym zostały zainstalowane komponenty modułu. Aby móc korzystać z bezpiecznego, szyfrowanego połączenia internetowego (HTTPS) należy dokonać zakupu certyfikatu SSL u zaufanego dostawcy.

2.3. Wymagania sprzętowe oraz programowe

Nie jest możliwe precyzyjne określenie wymagań sprzętowych modułu Archiwum. Wynika to m.in. z obciążenia ruchem, ilości zgromadzanych danych oraz innych usług zainstalowanych na komputerze.

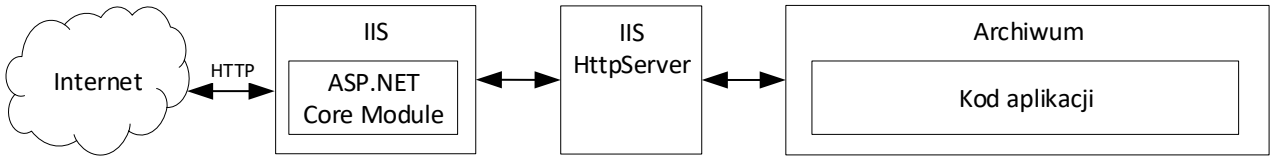
Wymagania programowe są zależne od systemu operacyjnego, z tego powodu zostały one umieszczone w rozdziałach instalacji dla każdego z systemów operacyjnych.

2.4. Zasada działania ASP .NET Core z serwerami WWW

W zależności od użytego systemu operacyjnego oraz komponentu (Archiwum lub mMDAB z MIAM) aplikacje mogą działać z jednym z dwóch trybów.

2.4.1. Hosting w procesie

Tryb ten dotyczy jedynie systemów Windows oraz serwera Internet Information Services (w skrócie IIS). W trybie tym Archiwum uruchamiane jest w wewnątrz procesu IIS. Wyeliminowanie komunikacji poprzez serwer proxy pozwala na zapewnienie większej wydajności.

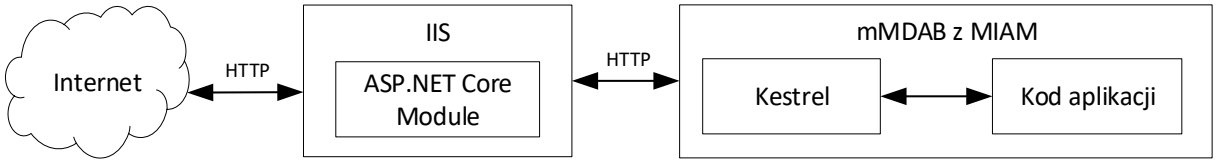


Rysunek 3: Hosting w procesie

2.4.2. Hosting poza procesem

Pliki każdego z komponentów (Archiwum, mMDAB z MIAM) zawierają wbudowany serwer WWW o nazwie Kestrel, którego zadaniem jest uruchamianie komponentów oraz pośredniczenie w ruchu pomiędzy nimi a właściwym serwerem WWW. Kestrel w domyślnej konfiguracji nasłuchuje wyłącznie ruchu sieciowego w obrębie lokalnego komputera. Ze względu bezpieczeństwa oraz znaczących ograniczeń, Kestrel nie powinien mieć upublicznionego połączenia do sieci Internet bez właściwego serwera WWW.

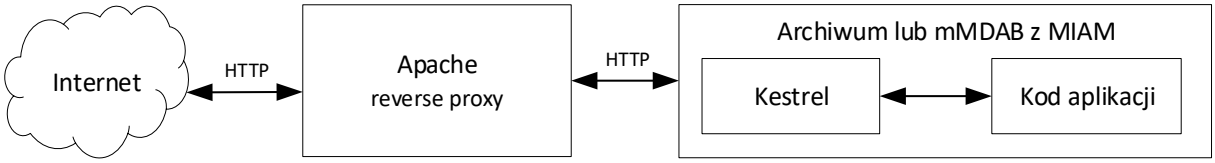
W przypadku instalacji dla systemów rodziny Windows, zalecanym serwerem jest Internet Information Services (w skrócie IIS), a uogólniony schemat z Kestrel został przedstawiony na *Rysunek 4*Rysunek 3.



Rysunek 4: Kestrel - połączenie z IIS

Domyślnie jedynie komponent mMDAB uruchamiany jest w tym trybie na systemach Windows.

Dla dystrybucji Linux zalecanym serwerem WWW jest Apache. Połączenie Apache z Kestrel zostało opisane na *Rysunek 5*.



Rysunek 5: Kestrel - połączenie z Apache

2.5. MIAM – podstawowe informacje

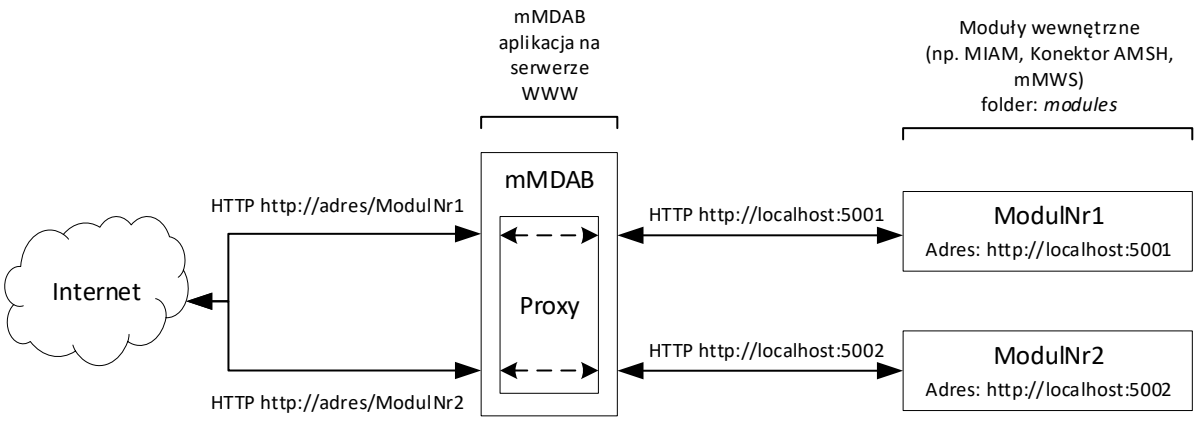
MIAM został wprowadzony od wersji 6.3.0 i umożliwia on komunikacje z aplikacji Archiwum do bazy danych mMedica. MIAM jest komponentem mMDAB, który został opisany w następnym podrozdziale.

Komponent MIAM jest zbliżony pod względem instalacji oraz konfiguracji do mMWS. W instrukcji znajdują się informacje dotyczące działania i sposobu konfiguracji mMDAB, jednak te kroki mogą zostać pominięte dla instalacji, które posiadają już instalację mMDAB. MIAM może zostać zainstalowany na istniejącej instalacji mMDAB (np. z mMWS), lecz istnieje możliwość osobnej instalacji mMDAB dedykowanej dla MIAM. Adres do aplikacji MIAM musi zostać skonfigurowany w aplikacji Archiwum (patrz: *8.11. Konfiguracja).*

Nie ma konieczności instalacji aplikacji MIAM w przypadku niekorzystania z funkcjonalności, które MIAM oferuje. Funkcjonalności, które wymagają użycia MIAM zostały wymienione w rozdziale *9.5. Komunikacja z systemu Informacje Medyczne do bazy danych mMedica*.

2.6. Komponent mMDAB

Komponent ma za zadanie ułatwić dodawanie nowych usług sieciowych (modułów wewnętrznych), które komunikują się z bazą danych mMedica. Aplikacja uruchamia podczas startu wewnętrzne moduły znajdujące się w jej strukturze katalogów (katalog *modules*) takie jak np. MIAM, Konektor AMSH, czy mMWS. Moduły wewnętrzne są uruchamiane tak, że akceptują wyłącznie ruch sieciowy wewnątrz komputera. mMDAB jest pośrednikiem w komunikacji do modułów wewnętrznych, tzn. przekierowuje do nich zgodnie z zasadą, że komunikacja na adres http://adres.szyny/PrzykladowyModul jest przekierowana do modułu wewnętrznego o nazwie PrzykladowyModul.



Rysunek 6: Zasada działania mMDAB

Konsekwencją takiego rozwiązania jest to, że skonfigurowany w aplikacji serwera WWW musi być wyłącznie mMDAB, a nie wszystkie moduły wewnętrzne.

3. Instalacja dla Windows

3.1. Instalacja w systemach Windows

Uwaga: Opisany proces instalacji jest zbliżony do instalacji modułu eRejestracja.

Proces instalacji modułów Archiwum w systemach Microsoft Windows może zostać wykonany za pomocą dedykowanego instalatora, który zainstaluje bazę danych oraz aplikację (wraz z ich uruchomieniem) na serwerze WWW Menedżer internetowych usług sieciowych (IIS). Możliwa jest również manualna instalacja oraz konfiguracja modułu z wykorzystaniem plików Archiwum. W takim przypadku instalator modułu jest wykorzystywany wyłącznie do instalacji bazy danych.

Instalator mMedica Moduły nie tylko instaluje moduł, ale również dokonuje procesu aktualizacji plików oraz bazy danych modułu. Aktualizacja dotyczy wyłącznie komponentów, które zostały zainstalowane za pomocą instalatora.

3.2. Wymagania

Uwaga: Wymagania dotyczące uruchomienia modułu Archiwum są zbieżne z modułem eRejestracja. Oznacza to, że jeżeli na serwerze zainstalowano moduł eRejestracja spełnia on również wymagana dotyczące Archiwum i nie wymaga on instalacji dodatkowego oprogramowania.

Przed przystąpieniem do instalacji modułów mMedica należy sprawdzić, czy zostały zainstalowane następujące elementy:

- System operacyjny (32 lub 64-bitowy): Windows 8.1, Windows Server 2012 R2, Windows 10, Windows Server 2016, Windows Server 2019, Windows 11, Windows Server 2022 (więcej informacji: https://docs.microsoft.com/pl-pl/dotnet/core/install/windows?tabs=net60).
- VC ++ Redistributable.
- Universal C Runtime w najnowszej dostępnej wersji (więcej informacji: https://support.microsoft.com/pl-pl/help/2999226/update-for-universal-c-runtime-in-windows).
- Serwer WWW: Menedżer internetowych usług sieciowych (w skrócie IIS, angielska nazwa: Internet Information Services) w wersji 7 lub wyższej.
- ASP .NET Core Runtime w wersji 6.0 wraz z modułem dla IIS (patrz: *3.4. Instalacja ASP .NET Core wraz z modułem* IIS).

Uwaga: System operacyjny wraz z jego składnikami powinien być zaktualizowany do najnowszej dostępnej wersji, np. za pomocą funkcjonalności automatycznych aktualizacji.

Uwaga: Funkcjonalności związane z Informacje Medyczne wymagają, aby komputery, na którym zostanie zainstalowane Archiwum miał publiczny i stały adres IP.

3.3. Instalacja serwera IIS

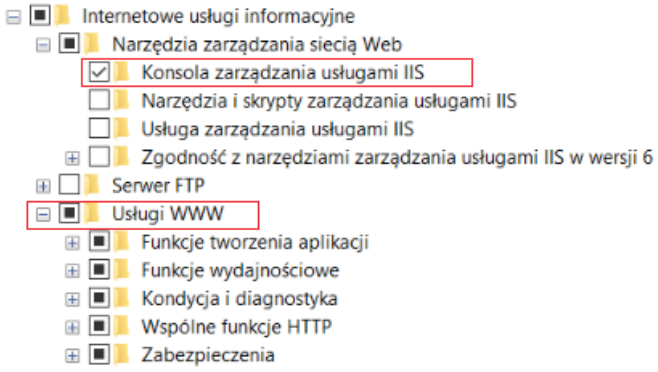
Uwaga: Komponenty serwera IIS wymagane do instalacji Archiwum są zbieżne z wymaganymi do urchomienia modułu eRejestracja. W przypadku, w którym na serwerze zainstalowany jest moduł eRejestracja instalację serwera IIS należy pominąć.

Niezbędnym krokiem jest przeprowadzenie instalacji serwera WWW. Proces instalacji został opisany poniżej:

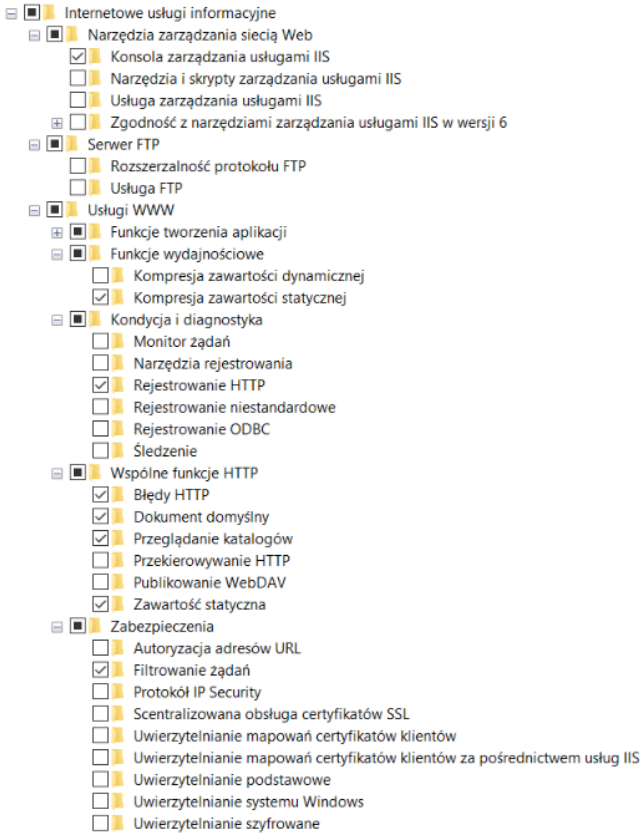
1. Uruchomić okno „Włącz lub wyłącz funkcje systemu Windows” - można to zrobić na dwa sposoby:
    a) Menu Start\Panel sterowania\Programy i funkcje, z menu po lewej wybrać „Włącz lub wyłącz funkcje systemu Windows”,

b) Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „optionalfeatures” i zatwierdzić klawiszem Enter.

2. Rozwinąć drzewo funkcji punktu „Internetowe usługi informacyjne”, a następnie zaznaczyć oznaczone kolorem czerwonym zgodnie z rysunkiem poniżej (patrz *Rysunek 7*):



Rysunek 7: Wymagane komponenty IIS



Rysunek 8: Wymagane komponenty IIS - szczegóły

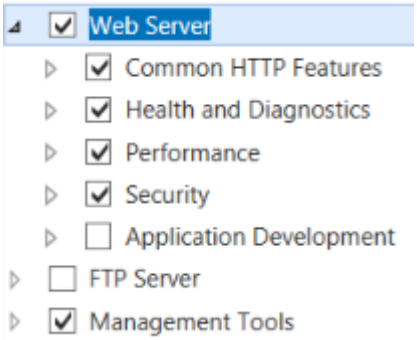
Należy zatwierdzić okno. Jeżeli wyświetlony zostanie komunikat o konieczności ponownego uruchomienia komputera, należy to wykonać.

Niektóre systemy serwerowe mogą mieć nieco odmienny interfejs włączania funkcji systemu Windows. Po uruchomieniu opcji „Włącz lub wyłącz funkcje systemu Windows” może pojawić się „Kreator dodawania ról i funkcji” (można to również uruchomić z poziomu „Menedżera serwera” – „Dodaj role i funkcje”). Następnie:

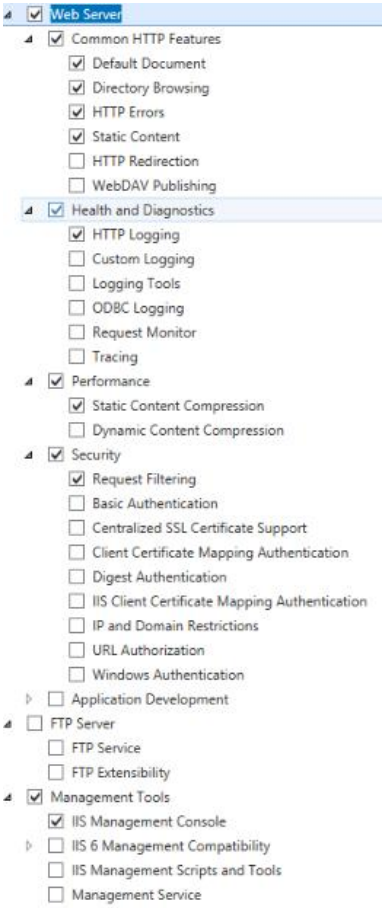
a) po lewej stronie wybrać „Wybieranie serwera”, gdzie należy upewnić się, że został zaznaczony właściwy serwer,

b) po lewej stronie wybrać „Role serwera” i na liście zaznaczyć „Web Server (IIS)”, zatwierdzić okno potwierdzenia,

c) z menu po lewej wybrać „Usługi ról” i zaznaczyć odpowiadające pozycje zgodnie z rysunkami poniżej (patrz *Rysunek 9*):



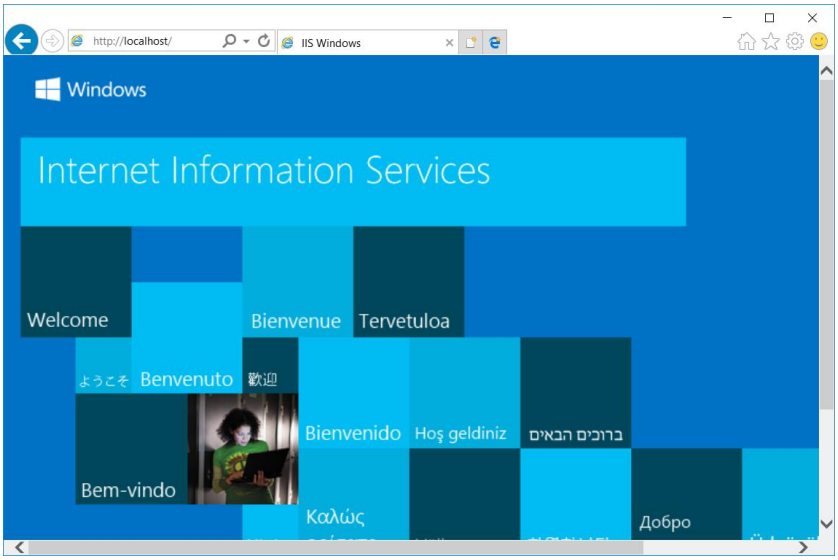
Rysunek 9: Komponenty IIS - Windows Server



Rysunek 10: Wymagane komponenty IIS - Windows Server - szczegóły

d) wybrać ponownie „Potwierdzenie” po lewej stronie (lub nacisnąć przycisk „Dalej >”), a następnie zainstalować komponenty wybierając przycisk „Zainstaluj”.

3. Zweryfikować czy po wpisaniu „http://localhost” w adres przeglądarki internetowej wyświetli się strona powitalna.



Rysunek 11: Przykładowa strona powitalna IIS

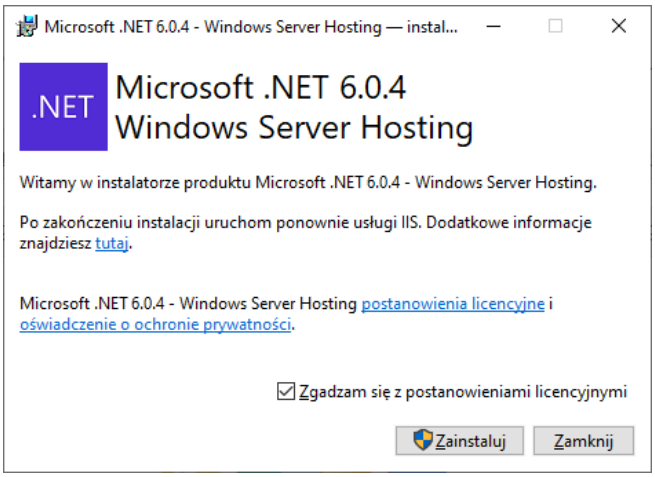
3.4. Instalacja ASP .NET Core wraz z modułem IIS

Uwaga: Wymagana wersja .NET Core jest taka sama jak dla modułu eRejestracja. W przypadku, w którym na serwerze zainstalowany jest moduł eRejestracja instalację pakietu ASP .NET Core należy pominąć.

Uwaga: Po zainstalowaniu środowiska uruchomieniowego ASP .NET Core 6.0 na administratora spada obowiązek aktualizacji tego oprogramowania. Najnowsza wersja środowiska uruchomieniowego ASP .NET Core 6.0 wraz z modułem IIS znajduje na stronie Microsoft: https://dotnet.microsoft.com/en-us/download/dotnet/6.0 (należy wybrać pakiet Hosting Bundle z sekcji ASP.NET Core Runtime w wersji 6.0.X, gdzie X oznacza dowolną podwersję systemu 6.0).

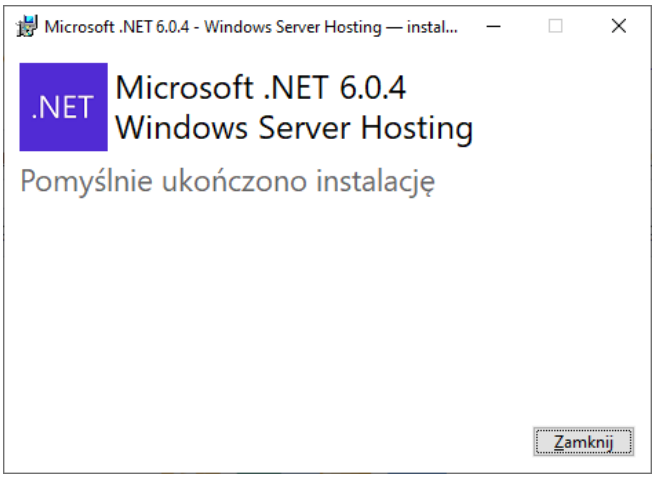
Do działania programu eRejestracja wymagana jest platforma ASP .NET Core w wersji 6.0 wraz modułem IIS o nazwie AspNetCoreModuleV2. Całość jest dostępna w pakiecie instalacyjnym:
https://mmedica-download.asseco.pl/inst/mModuly/dotnet-hosting-win.exe
Proces instalacji pakietu wygląda następująco:

1. Uruchomić pobrany plik z uprawnieniami administratora.
2. Zaznaczyć pole związane z akceptacją licencji i warunków („Zgadzam się…”). Warunki licencji są dostępne po naciśnięciu niebieskich odnośników. Nacisnąć przycisk „Zainstaluj”.



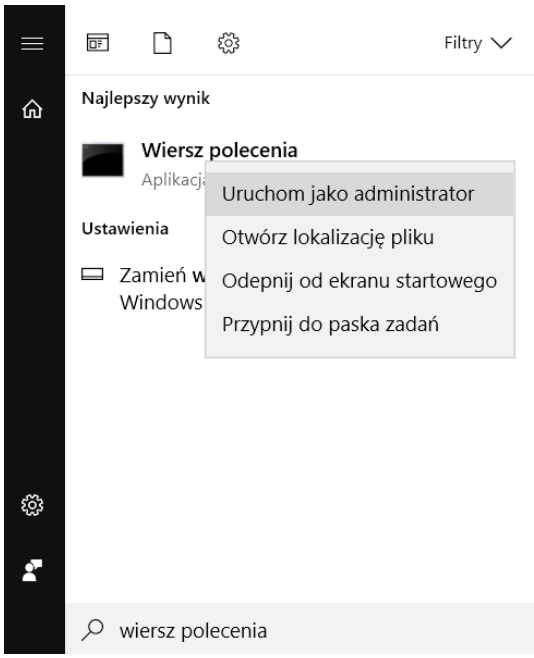
Rysunek 12: Instalacja .NET Core - nacisnąć przycisk „Install”.

3. Po instalacji wybrać przycisk „Zamknij”.



Rysunek 13: Instalacja .NET Core - potwierdzenie instalacji

4. W celu uruchomienia modułu dla IIS należy zrestartować serwer IIS (co spowoduje chwilowe zatrzymanie udostępniania witryn). Restart serwera IIS można wykonać poprzez ponowne uruchomienie systemu operacyjnego lub wykonanie poniższych kroków:
   a) uruchomić Wiersz polecenia w trybie administratora,



Rysunek 14: Uruchomienie Wiersz polecenia w trybie administratora - Windows 10

   b) zatrzymać usługę IIS wpisując poniże polecenie i zatwierdzając klawiszem Enter,

```
net stop was /y
```

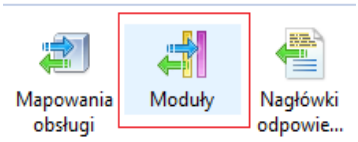
   c) uruchomić usługę IIS wpisując poniże polecenie i zatwierdzając klawiszem Enter,

```
net start w3svc
```

   d) dokonać weryfikacji instalacji modułu IIS uruchamiając panel zarządzania IIS w jeden z poniższych sposobów:

- Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr” i zatwierdzić klawiszem Enter,
- Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).

e) w oknie środkowym odnaleźć opcję „Moduły”,



Rysunek 15: IIS - moduły

f) jeśli na liście znajduje się pozycja o nazwie „AspNetCoreModuleV2” oznacza to, że moduł dedykowany dla .NET Core został zainstalowany pomyślnie.

Rysunek 16: Moduł IIS - weryfikacja

Uwaga: .NET może być zainstalowany równolegle z .NET Framework.

3.5. Instalacja IIS po instalacji ASP .NET Core

W przypadku, w którym w pierwszej kolejności został zainstalowany ASP .NET Core, a następnie IIS, należy doinstalować moduł AspNetCoreModuleV2 oraz zarejestrować jego obsługę w IIS. Proces instalacji wygląda następująco:

1. Uruchomić ponownie instalator ASP.NET Core z Windows Hosting (patrz: *3.4. Instalacja ASP .NET Core wraz z modułem* IIS). W przypadku, gdy w systemie zainstalowana jest nowsza ASP.NET Core z Windows Hosting, należy posłużyć się instalatorem w nowszej wersji.
2. Wybrać w instalatorze opcję: „Repair”.
3. Uruchomić panel zarządzania IIS na jeden z poniższych sposobów:
   a) Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr” i zatwierdzić klawiszem Enter,
   b) Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
4. W oknie środkowym odnaleźć opcję „Moduły”:

Rysunek 17: IIS - moduły

5. Jeśli na liście znajduje się pozycja o nazwie „AspNetCoreModuleV2” oznacza to, że moduł dedykowany dla .NET Core został zainstalowany pomyślnie. W przeciwnym razie trzeba przejść do kolejnych kroków.

AspNetCoreModuleV2	%ProgramFiles%\IIS\Asp.Net ...	Macierzysty	Lokalne

Rysunek 18: Sprawdzanie modułu dla .NET Core w IIS

6. W oknie „Moduły” z menu „Akcje” po lewej stronie należy wybrać „Konfiguruj moduły macierzyste…”.
7. Jeśli na liście w nowym oknie jest dostępny moduł „AspNetCoreModuleV2”, należy go oznaczyć. Jeśli moduł na liście nie występuje, należy wybrać przycisk „Zarejestruj”, a następnie uzupełnić:
   a) Nazwa: AspNetCoreModuleV2
   b) Ścieżka: %SystemRoot%\system32\inetsrv\aspnetcore.dll

   Zatwierdzić okno przyciskiem „OK”, a następnie oznaczyć go na liście dostępnych modułów.
8. Wybrać przycisk „OK”, zatwierdzając wybór modułu.
9. Wykonać restart serwera IIS, można go wykonać poprzez ponowne uruchomienie systemu operacyjnego lub wykonanie poniższych kroków:
   a) uruchomić Wiersz polecenia w trybie administratora,
   b) zatrzymać usługę IIS wpisując poniże polecenie i zatwierdzając klawiszem Enter,

```
net stop was /y
```

   c) uruchomić usługę IIS wpisując poniższe polecenie i zatwierdzając klawiszem Enter.

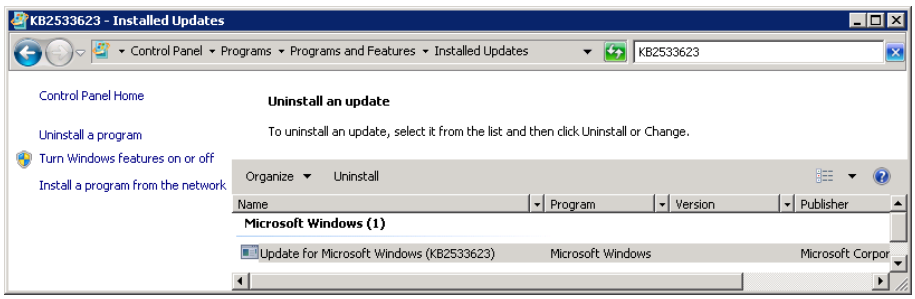
```
net start w3svc
```

3.6. KB2533623 dla Windows 8.1, Windows Server 2012 R2

Systemy operacyjne Windows 8.1, Windows Server 2012 R2 wymagają instalacji pakietu KB2533623 dostarczanego przez firmę Microsoft. W przypadku włączonych automatycznych aktualizacji systemu paczka powinna zostać automatycznie zainstalowana. Istnieje możliwość weryfikacji, czy podany pakiet został zainstalowany w następujący sposób:

1. Otworzyć Panel Sterowania.

2. Wybrać opcję „Programy i funkcje”.
3. Wybrać z menu po lewej stronie „Wyświetl zainstalowane aktualizacje”.
4. Wpisać w górnym pasku wyszukiwania „KB2533623”.
5. Jeśli na liście znajduje się wpis informujący o aktualizacji (patrz: *Rysunek 19*) oznacza to, że pakiet został już zainstalowany.



Rysunek 19: Weryfikacja instalacji KB2533623

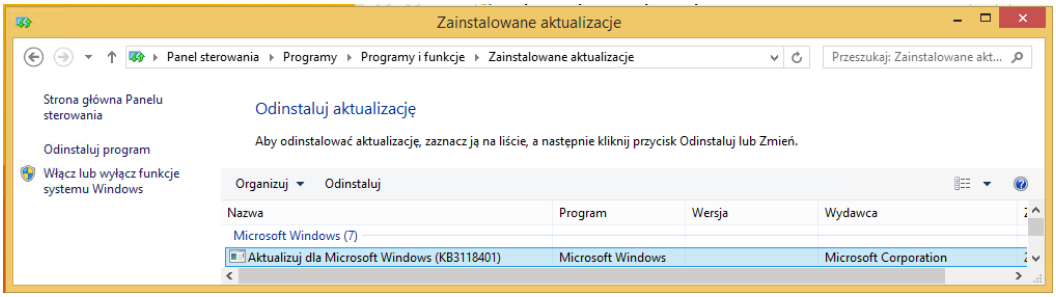
Składnik może zostać również zostać pobrany ze strony: https://support.microsoft.com/en-us/help/2533623/microsoft-security-advisory-insecure-library-loading-could-allow-remot.

3.7. KB3118401 dla Windows 8.1

System operacyjny Windows 8.1 wymaga instalacji pakietu KB3118401 dostarczanego przez firmę Microsoft. W przypadku włączonych automatycznych aktualizacji systemu paczka powinna zostać automatycznie zainstalowana. Istnieje możliwość weryfikacji, czy podany pakiet został zainstalowany w następujący sposób:

1. Otworzyć Panel Sterowania.
2. Wybrać opcję „Programy i funkcje”.
3. Wybrać z menu po lewej stronie „Wyświetl zainstalowane aktualizacje”.
4. Wpisać w górnym pasku wyszukiwania „KB3118401”.

Jeśli na liście znajduje się wpis informujący o aktualizacji (patrz: *Rysunek 20*) oznacza to, że pakiet został już zainstalowany.



Rysunek 20 Weryfikacja instalacji KB3118401

Składnik może zostać również pobrany ze strony: https://www.microsoft.com/en-ph/download/details.aspx?id=51106.

3.8. Instalacja za pomocą instalatora

Przedstawiony w tym rozdziale proces instalacji uwzględnia najprostszy przypadek, w którym aplikacja Archiwum oraz baza danych mają się znajdować na tym samym komputerze.

Pełen proces instalacji można przedstawić za pomocą następujących podpunktów:

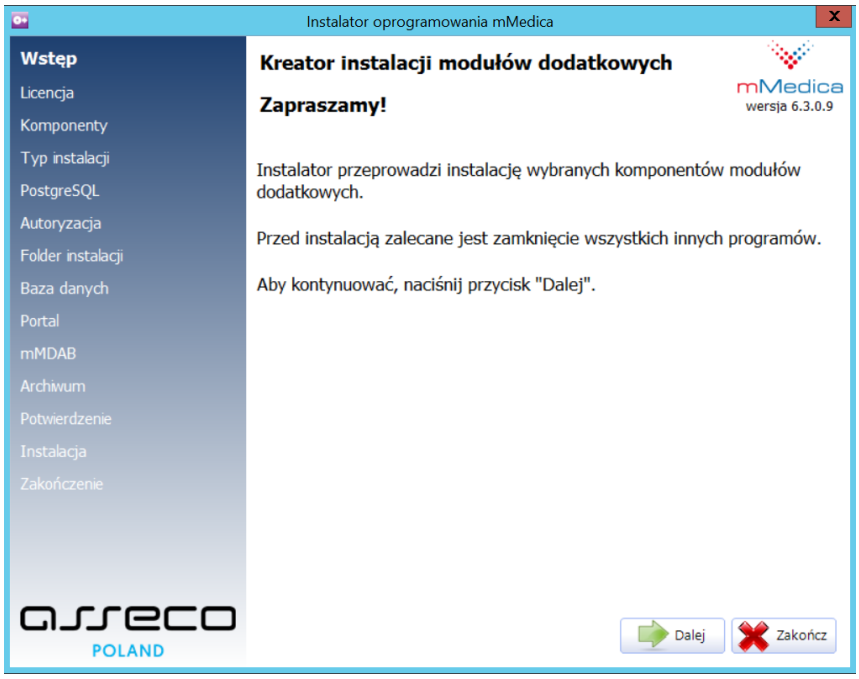
1. Instalacja niezbędnego oprogramowania związanego z wymaganiami.
2. Instalacja serwera WWW (*3.3. Instalacja serwera IIS*).
3. Instalacja ASP .NET Core (*3.4. Instalacja ASP .NET Core wraz z modułem* IIS).
4. Instalacja modułu przez instalator (baza danych oraz komponenty).
5. Weryfikacja instalacji.
6. Dodatkowa konfiguracja serwera WWW.
7. Weryfikacja instalacji (*3.12. Weryfikacja instalacji*).
8. Dodatkowa konfiguracja serwera WWW (*3.13. Dodatkowa konfiguracja IIS*).

Uwaga: Instalator może zainstalować wyłącznie jeden komponent danego typu. W przypadku chęci zainstalowania większej liczby komponentów należy posłużyć się informacjami zawartymi w *3.14. Doinstalowanie komponentów* lub posłużyć się instrukcją instalacji manualnej (patrz: *3.10. Instalacja manualna*).

Uwaga: Instalator modułów mMedica zawiera zarówno oprogramowanie do modułu Archiwum jak i modułu eRejestracja. W przypadku, w którym mają zostać zainstalowane oba moduły należy podczas procesu instalacji zaznaczyć wybrane komponenty modułu eRejestracja zgodnie z jej instrukcją instalacji oraz konfiguracji.

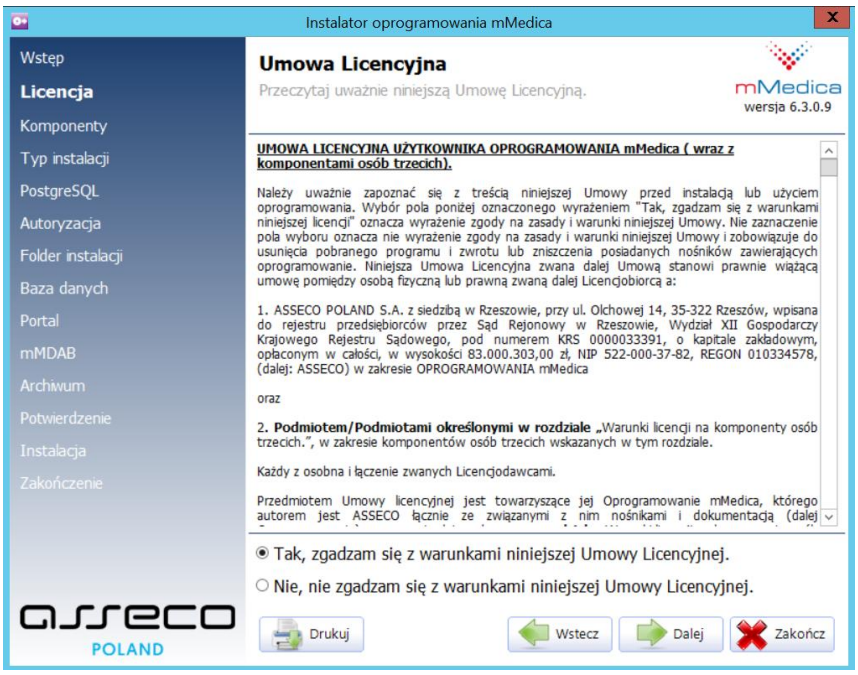
Proces instalacji:

1. Uruchomić plik instalatora modułów mMedica, który wyświetli formatkę powitalną. Przycisk strzałki w prawo pozwala przejść dalej (dotyczy to wszystkich kroków instalacji).



Rysunek 21: Formatka powitalna instalatora modułu

2. Zapoznać się z Umową Licencyjną. Aby ją zaakceptować należy zaznaczyć „Tak, zgadzam się z warunkami niniejszej Umowy Licencyjnej”.



Rysunek 22: Akceptacja umowy licencyjnej w instalatorze

3. Wybrać komponenty, które mają zostać zainstalowane.

Rysunek 23: Wybór komponentów do instalacji

4. W oknie wyboru można wybrać Moduł MIAM, który jest komponentem mMDAB.

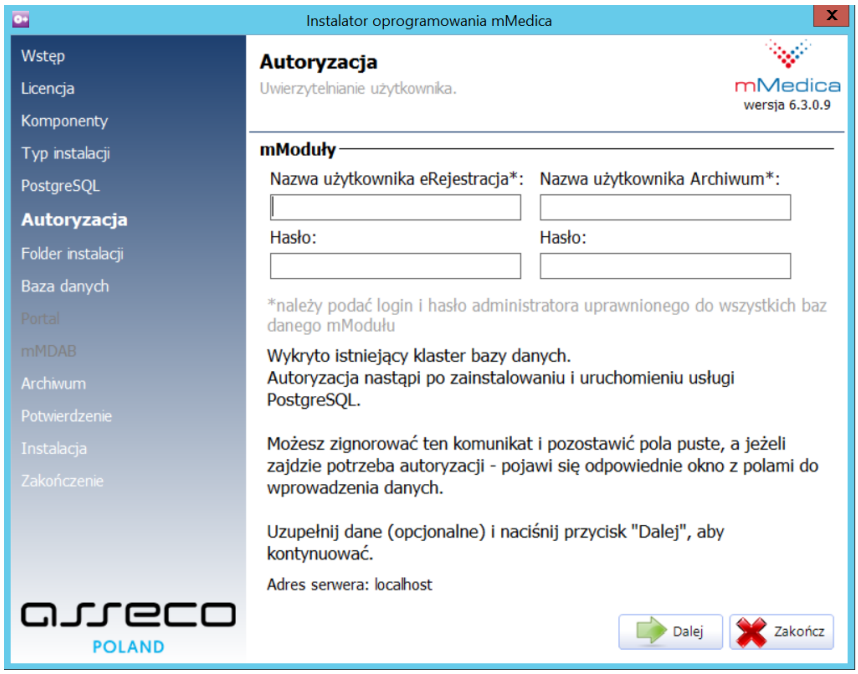
Rysunek 24: Wybór komponentów do instalacji

5. Zaznaczyć typ instalacji bazy danych (lokalna lub zdalna instalacja). Dla celów instruktażowych instalacja zostanie wykonana lokalnie. W przypadku zdalnej instalacji należy podać adres IP lub nazwę serwera oraz port komputera, na którym jest zainstalowany serwer bazy danych PostgreSQL. W takim

przypadku serwer PostgreSQL musi być tak skonfigurowany, aby zezwalać na komunikację z zewnątrz oraz sam port musi być odblokowany do komunikacji przychodzącej w oprogramowaniu typu firewall.

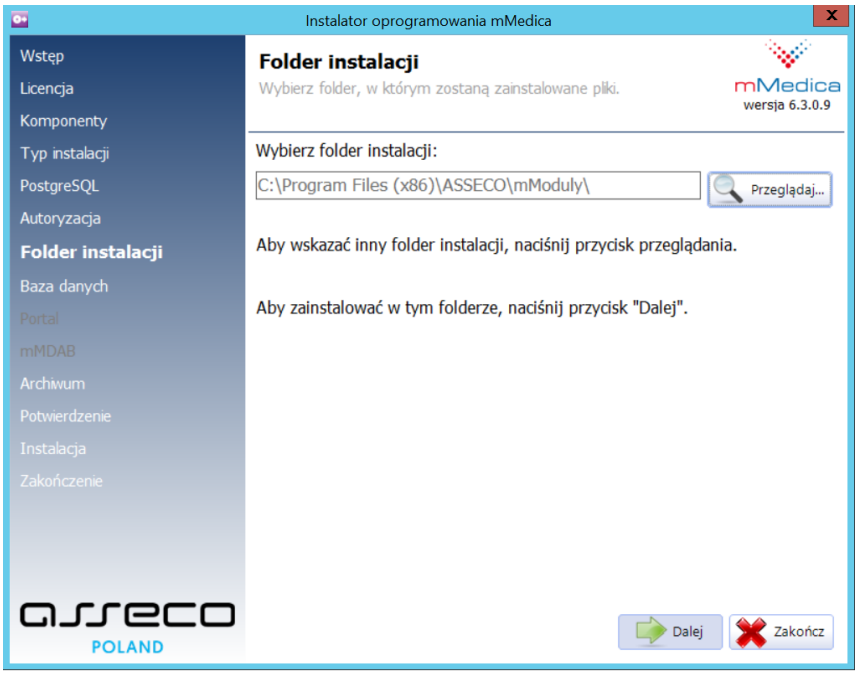
Rysunek 25: Wybór typu instalacji modułu

6. Opcjonalnie dokonać uwierzytelnienia do baz danych mModułów. Jeśli na komputerze nie są zainstalowane żadne bazy modułów eRejestracja lub Archiwum należy ten krok pominąć wybierając przycisk „Dalej”.



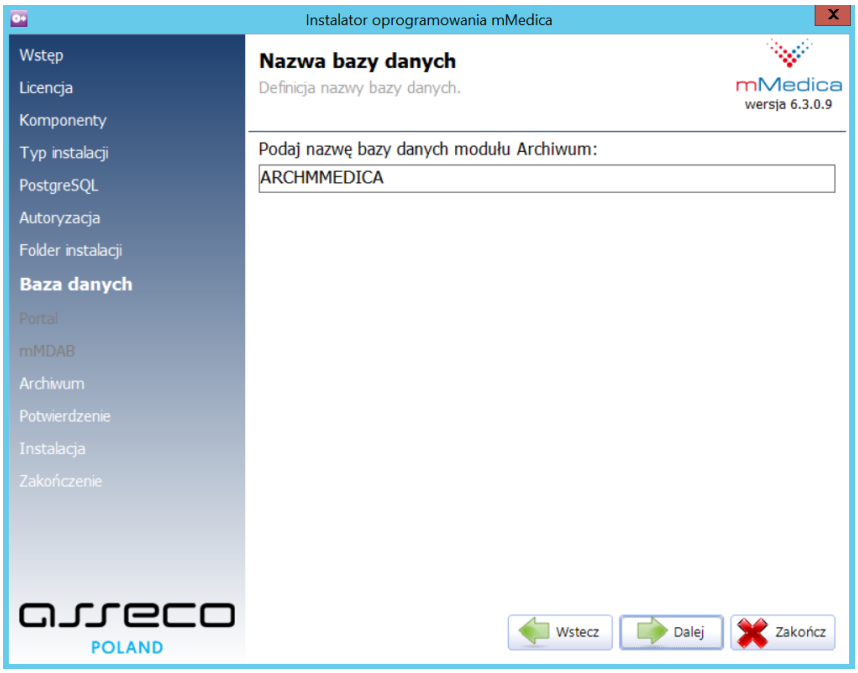
Rysunek 26: Opcjonalna autoryzacja dostępu do bazy danych

7. Wybrać folder, gdzie ma zostać zainstalowane zaznaczone oprogramowanie.



Rysunek 27: Wybór miejsca instalacji komponentów

8. Podać nazwę bazy danych Archiwum.



Rysunek 28: Wybór nazwy bazy danych Archiwum

9. W oknie konfiguracji mMDAB (dla komponentu MIAM) należy skonfigurować połączenie do bazy danych mMedica. Dodatkowo istnieje możliwość konfiguracji czy moduł ma wykorzystywać SSL, jaką nazwę ma mieć pula aplikacji oraz katalog wirtualny w IIS (więcej informacji znajduje się w *7.1.2. Protokół SSL*).

Rysunek 29: Konfiguracja mMDAB dla komponentu MIAM

Uwaga: SSL można również uruchomić po instalacji komponentów. Zaznaczenie wykorzystywania SSL bez importu i skonfigurowania certyfikatu na serwerze IIS spowoduje wyświetlenie białej strony w przeglądarce internetowej.

Uwaga: Możliwa jest zmiana adresu IP oraz nazwy bazy danych po instalacji komponentu. Więcej informacji w rozdziale *5.1. Konfiguracja połączenia z bazami danych.*

10. Na formatce konfiguracji Archiwum możemy wybrać, czy moduł ma wykorzystywać SSL, jaką nazwę ma mieć pulę aplikacji oraz katalog wirtualny w IIS (więcej informacji znajduje się w *7.1.2. Protokół SSL*).

Rysunek 30: Konfiguracja instalacji Portalu

11. Zatwierdzić instalację oraz poczekać na jej zakończenie.

Rysunek 31: Potwierdzenie instalacji moduł

3.9. Instalacja dodatkowych modułów/komponentów

W przypadku wcześniejszej instalacji tylko wybranych modułów/komponentów możliwe jest doinstalowanie pozostałych przy pomocy instalatora.

1. W tym celu należy uruchomić plik instalatora modułów mMedica, który zostanie uruchomiony w trybie serwisowym. Wybrać opcję Zarządzaj modułami dodatkowymi.

Rysunek 32: Tryb serwisowy instalatora

2. Wybrać komponenty, które mają zostać zainstalowane. W tym kroku można również doinstalować moduł eRejestracja oraz MIAM.

Rysunek 33: Wybór instalowanych komponentów

3. W dalszy krokach należy postępować podobnie jak jest to opisane w dziale *3.8. Instalacja za pomocą instalatora.*

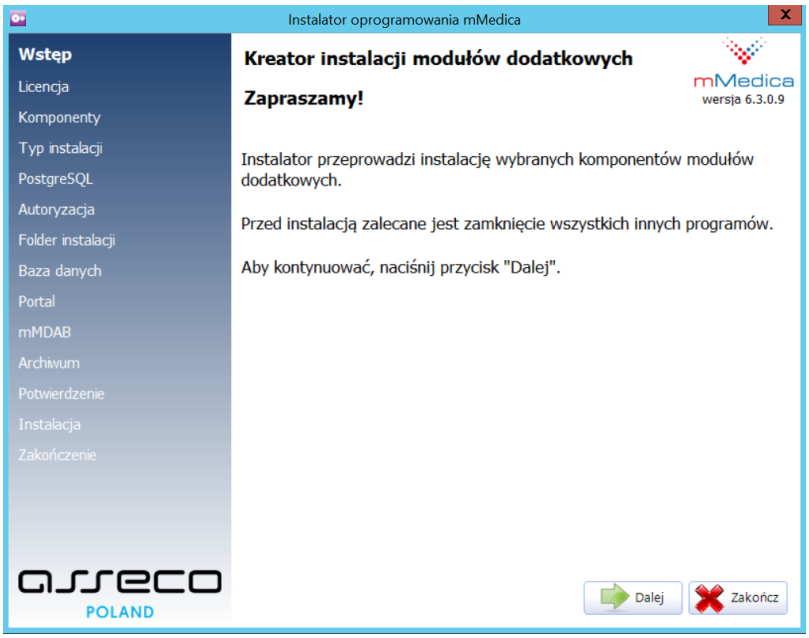
3.10. Instalacja manualna

Instalacja manualna to proces, który można sprowadzić do następujących kroków:

1. Instalacja niezbędnego oprogramowania związanego z wymaganiami.
2. Instalacja serwera WWW (*3.3. Instalacja serwera IIS*).
3. Instalacja ASP .NET Core (*3.4. Instalacja ASP .NET Core wraz z modułem* IIS).
4. Instalacja bazy danych przez instalator (poniższy proces instalacji).
5. Konfiguracja podstawowa serwera WWW (poniższy proces instalacji).
6. Skopiowanie plików poszczególnych komponentów (poniższy proces instalacji).
7. Konfiguracja połączenia z bazami danych dla komponentów (Uwaga: proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja - *5.1. Konfiguracja połączenia z bazami danych*).
8. Konfiguracja nazw aplikacji (*3.11. Konfiguracja nazwy aplikacji*).
9. Weryfikacja instalacji (*3.12. Weryfikacja instalacji*).
10. Dodatkowa konfiguracja serwera WWW (*3.13. Dodatkowa konfiguracja IIS*).

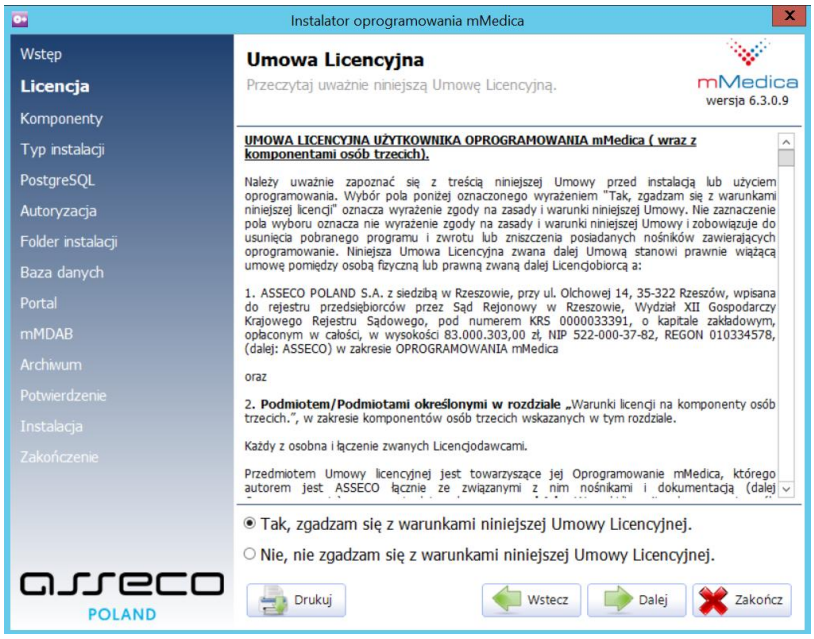
Proces instalacji:

1. Uruchomić plik instalatora modułów mMedica, który wyświetli formatkę powitalną. Przycisk strzałki w prawo pozwala przejść dalej (dotyczy to wszystkich kroków instalacji).



Rysunek 34: Formatka powitalna instalatora modułu

2. Zapoznać się z Umową Licencyjną. Aby ją zaakceptować należy zaznaczyć „Tak, zgadzam się z warunkami niniejszej Umowy Licencyjnej”.



Rysunek 35: Akceptacja umowy licencyjnej w instalatorze

3. Wybrać wyłącznie komponent „Baza danych".

Rysunek 36: Wybór komponentu Bazy danych do instalacji

4. Zaznaczyć typ instalacji bazy danych (lokalna lub zdalna instalacja). Dla celów instruktażowych instalacja zostanie wykonana lokalnie. W przypadku zdalnej instalacji należy podać adres IP lub nazwę serwera oraz port komputera, na którym jest zainstalowany serwer bazy danych PostgreSQL. W takim

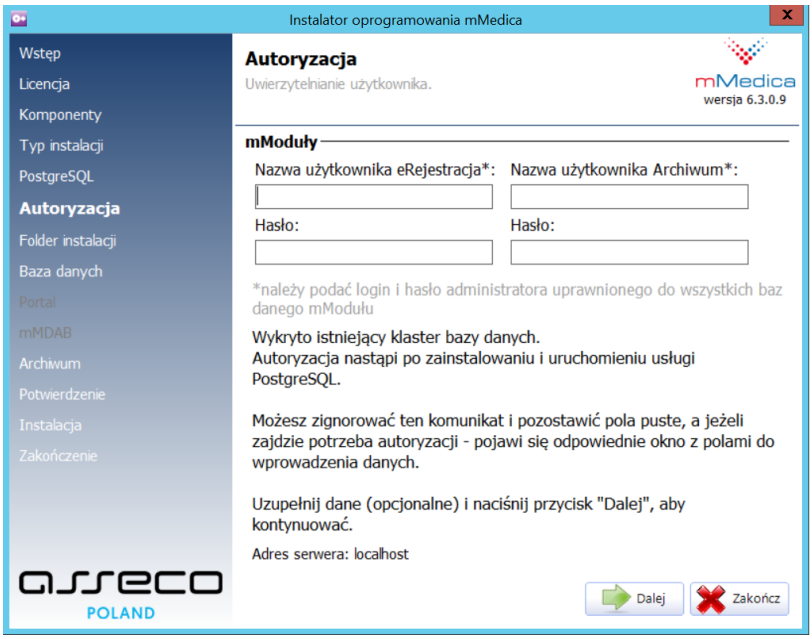
przypadku serwer PostgreSQL musi być tak skonfigurowany, aby zezwalać na komunikację z zewnątrz oraz sam port musi być odblokowany do komunikacji przychodzącej w oprogramowaniu typu firewall.

Rysunek 37: Wybór typu instalacji modułu

5. Wybrać miejsce instalacji oprogramowania bazy danych oraz miejsce składowania plików danych.

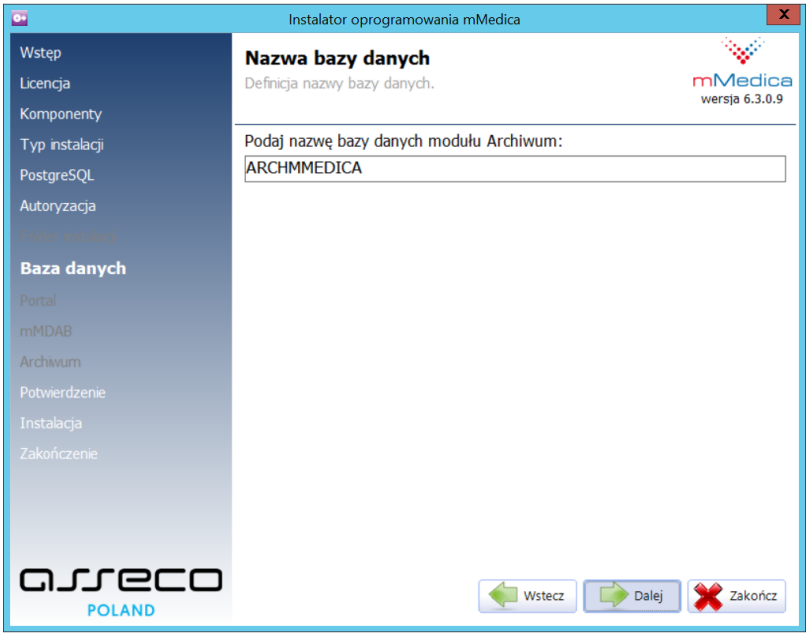
Rysunek 38: Konfiguracja instalacji serwera bazy danych

6. Opcjonalnie wpisać poświadczenia do bazy danych.



Rysunek 39: Opcjonalna autoryzacja dostępu do bazy danych

7. Podać nazwę bazy danych Archiwum.

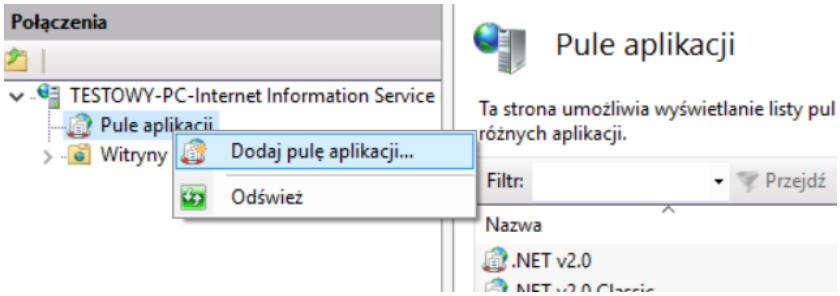


Rysunek 40: Wybór nazwy bazy danych Archiwum

8. Zatwierdzić instalację oraz poczekać na jej zakończenie.

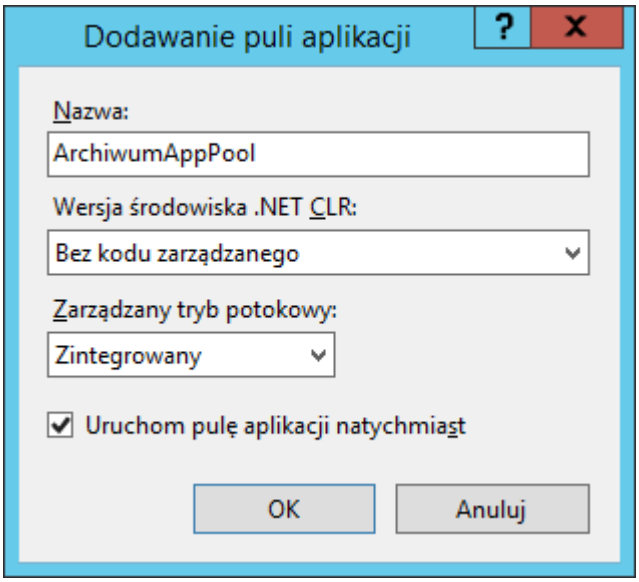
Rysunek 41: Potwierdzenie instalacji modułu

9. Uruchomić Menedżer internetowych usług informacyjnych IIS (Internet Information Service Manager). Poniżej zamieszczono sposoby uruchomienia:
   a) Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr” i zatwierdzić klawiszem Enter,
   b) Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
10. Rozwinąć po lewej stronie drzewko „Połączenia” na nazwie komputera, następnie kliknąć prawym przyciskiem myszy na ikonę podpisaną „Pule aplikacji” i wybrać opcję „Dodaj pulę aplikacji…”.



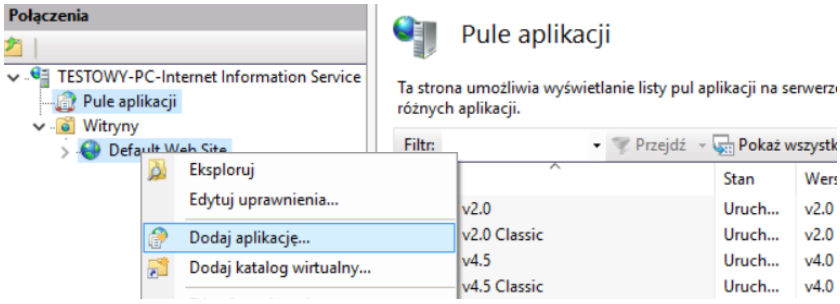
Rysunek 42: Tworzenie nowej puli aplikacji w programie IIS

11. Po wybraniu powyższej opcji powinno pojawić się okno, które należy uzupełnić jak poniżej. Nazwa puli aplikacji może być dowolna.



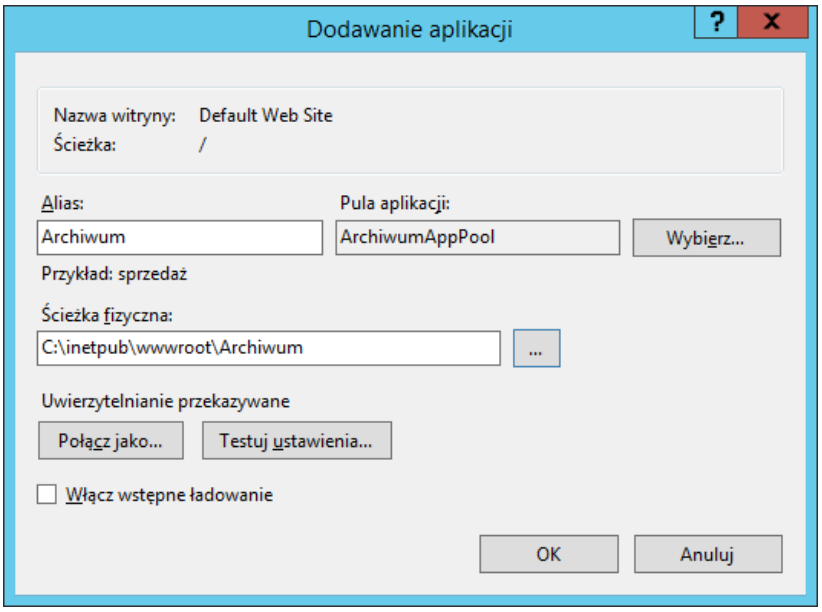
Rysunek 43: Tworzenie nowej puli aplikacji – ustawienia

12. Na liście puli aplikacji kliknąć prawym przyciskiem myszy na utworzoną pulę dla Archiwum, a następnie z menu kontekstowego wybrać opcję „Ustawienia zaawansowane…". W oknie ustawień odszukać pozycję „Załaduj profil użytkownika" (grupa „Model procesów") i upewnić, się, że ma ustawioną wartość na „True" Jeśli opcja ustawiona jest na „False" należy ja przestawić i zapisać ustawienia.
13. Kliknąć prawym przyciskiem myszy na „Default Web Site" i wybrać opcję „Dodaj aplikację…".



Rysunek 44: Dodawanie nowej aplikacji

14. Uzupełnić okno według zrzutu przedstawionego poniżej. Przy wybieraniu dowolnej fizycznej ścieżki do folderu, do którego w późniejszym etapie zostaną skopiowane pliki komponentu, można posłużyć się przyciskiem „…". Pliki komponentu można skopiować do wybranego folderu po dodaniu aplikacji. Za pomocą przycisku „Wybierz…" należy wybrać zdefiniowaną wcześniej pulę aplikacji.

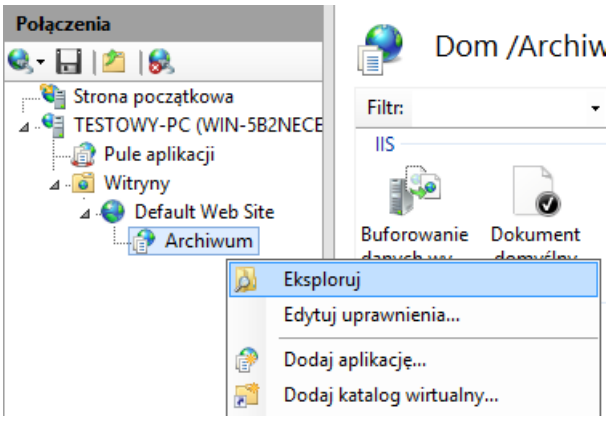


Rysunek 45: Dodawanie nowej aplikacji

15. Kroki z tworzeniem puli aplikacji oraz aplikacji należy powtórzyć dla mMDAB.
16. Pobrać pliki komponentów – odnośnik. Skopiować z dostarczonego archiwum pliki (ścieżki dla przykładu z zrzutu powyżej):

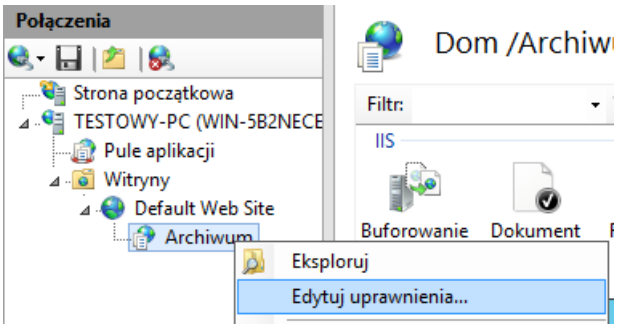
- Archiwum do: *C:\inetpub\wwwroot\Archiwum*
- mMDAB do: *C:\inetpub\wwwroot\mMDAB*
- MIAM do: C*:\inetpub\wwwroot\mMDAB\modules\MIAM*

Dla ułatwienia odszukania właściwego katalogu możliwe jest użycie opcji „Eksploruj”. Pojawia się ona do wyboru po naciśnięciu prawego przycisku myszy na dowolną aplikację (np. Portal) w oknie „Połączenia”.



Rysunek 46: Otworzenie katalogu aplikacji

17. Zaleca się umieszczanie plików komponentów w ścieżce C:\inetpub\wwwroot\, gdyż jest to folder przeznaczony do przechowywania plików IIS. Jeśli pliki komponentów zostały skopiowane do innego katalogu, możliwe jest wyświetlenie w oknie przeglądarki błędu 502.5 w procesie weryfikacji instalacji. W takim przypadku wymagane jest dodatkowe nadanie uprawnień, które zezwolą puli aplikacji na odczyt plików z danej ścieżki. Proces nadawania:
    a) Przejść do ścieżki pliku lub folderu komponentu. Następnie kliknąć prawym przyciskiem myszy na plik lub folder i wybrać z menu kontekstowego „Właściwości". Można również posłużyć się opcją „Edytuj uprawnienia…" dostępną w menu kontekstowym po wybraniu odpowiedniej aplikacji w IIS (patrz: *Rysunek 47: Edycja uprawnień do katalogu w IIS*).



Rysunek 47: Edycja uprawnień do katalogu w IIS

    b) Przejść do górnej zakładki „Zabezpieczenia".
    c) Wybrać przycisk „Edytuj".
    d) W oknie nadawania uprawnień wybrać przycisk „Dodaj".
    e) W dolnym polu tekstowym wpisać nazwę IIS APPPOOL\[Nazwa puli aplikacji], czyli dla przykładu: „IIS APPPOOL\ArchiwumAppPool" (dla katalogu Archiwum należy wybrać pulę aplikacji utworzona dla Archiwum, z kolei dla katalogu mMDAB pulę utworzoną dla mMDAB).
    f) Następnie kliknąć opcję sprawdzania nazwy „Sprawdź nazwy" oraz zatwierdzić przyciskiem „OK". Jeśli nazwa została odnaleziona, zostanie podkreślona.
    g) Zaznaczyć dodanego użytkownika (podaną wcześniej nazwę) kliknięciem myszy. W dolnym polu nadać użytkownikowi uprawnienia: „Odczyt i wykonywanie", „Wyświetlenie zawartości folderu", „Odczyt". Zatwierdzić zmianę przyciskiem OK.
18. Nadać uprawnienia do zapisu dla plików:
    a) Dla puli Archiwum:
        - [Ścieżka do Archiwum]\application.log
          dla przykładowej instalacji: *C:\inetpub\wwwroot\Archiwum*\application.log

b) Dla puli mMDAB:

- pliku: [Ścieżka do mMDAB]\application.log

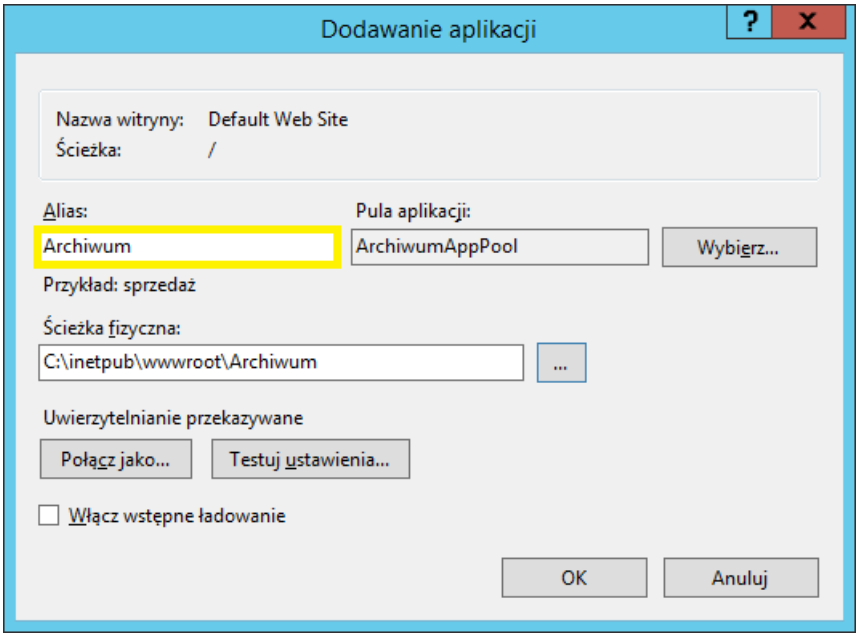
  dla przykładowej instalacji: C:\inetpub\wwwroot\mMDAB\application.log
- pliku: [Ścieżka do mMDAB]\modules\MIAM\application.log

  dla przykładowej instalacji: C:\inetpub\wwwroot\mMDAB\modules\MIAM\application.log

3.11. Konfiguracja nazwy aplikacji

Uwaga: Konfiguracja nazw aplikacji odbywa się identycznie jak w module eRejestracja.

Jeśli Archiwum nie mają swojego własnego adresu domenowego, to w pliku appsettings.json znajdującym się w katalogu każdej z aplikacji, należy wprowadzić nazwę aplikacji. Nazwa ta nie jest dowolna. Należy wprowadzić dokładnie tę samą nazwę, która zostanie wykorzystana do konfiguracji serwera IIS. Nazwa ta znajduje się w zaznaczonych miejscach:



Rysunek 48: Identyfikacja nazwy aplikacji

Nazwę tą należy umieścić w sekcji ApplicationName, dla przykładowej konfiguracji:

```
"ApplicationName": "Archiwum"
```

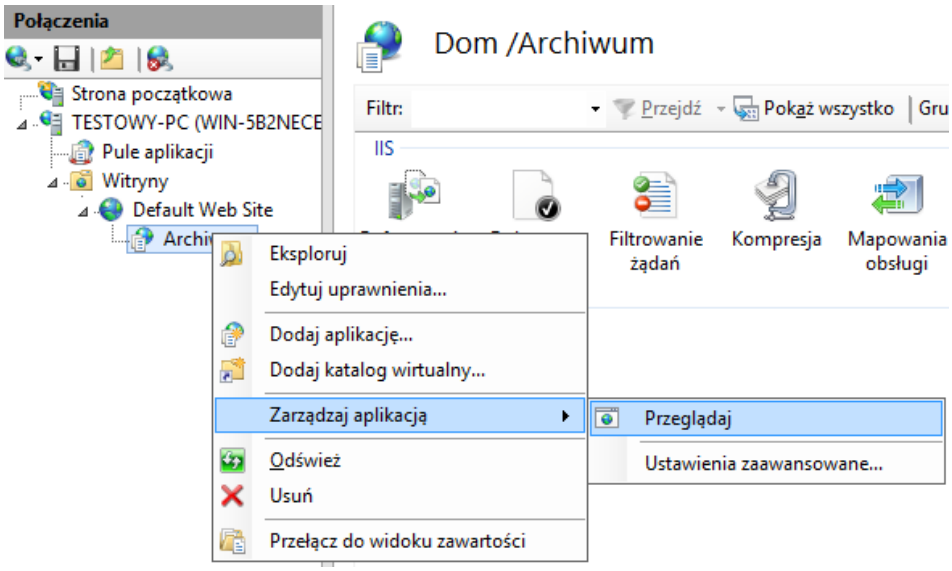
W przypadku instalacji mMDAB należy ten krok również wykonać dla mMDAB.

Nazwy powinny być unikalne w ramach jednego serwera WWW.

3.12. Weryfikacja instalacji

Po instalacji przez instalator jak i instalacji manualnej należy zweryfikować, czy instalacja została przeprowadzona poprawnie. Proces weryfikacji wygląda następująco:

1. Uruchomić Menedżer internetowych usług informacyjnych IIS (Internet Information Service Manager). Poniżej zamieszczono sposoby uruchomienia:
   a. Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr" i zatwierdzić klawiszem Enter,
   b. Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
2. Rozwinąć drzewo połączeń tak, aby widoczna była aplikacja, którą należy zweryfikować. Klikając prawym przyciskiem myszy na wybraną aplikację należy wybrać Zarządzaj aplikacją\Przeglądaj, co spowoduje uruchomienie aplikacji w przeglądarce internetowej.



Rysunek 49: Podgląd aplikacji z poziomu IIS

3. Weryfikacja usługi sieciowej Archiwum odbywa się poprzez wejście na stronę statusową usługi. Dla konfiguracji przykładowej adres wygląda następująco http://localhost/Archiwum. Wyświetlona zostanie strona statusowa dla aplikacji Archiwum z możliwością zalogowania się. Strona statusowa pozwala zweryfikować czy połączenie z bazą danych jest prawidłowe. Rezultat poprawnego działania Archiwum wygląda następująco:

mMedica Archiwum

ZALOGUJ SIĘ

Status aplikacji mMedica Archiwum

Status	Ok
Wersja aplikacji	5.15.0
Wersja bazy danych	5.15.0
Połączenie z bazą danych Archiwum	Tak
Kompatybilność wersji	Tak
Data z serwera aplikacji	20.09.2018 12:22:53
Data z serwera bazy danych Archiwum	20.09.2018 12:22:54

Rysunek 50: Weryfikacja działania aplikacji Archiwum

4. Weryfikacja usługi sieciowej mMDAB odbywa się poprzez wejście na stronę statusową usługi. Adres usługi dla przykładowej konfiguracji to: http://localhost/mMDAB. Wyświetlona zostanie strona statusowa z informacjami o dołączonych modułach takich jak MIAM.

Strona diagnostyczna mMedica DAB

Połączenie z bazą mMedica	Połączono

Link do pomocy swagger

Dołączone moduły				
Nazwa modułu	Wersja	Adres statusu	Port modułu	Udostępniony swagger
MIAM	6.3.0	/MIAM	5002	Tak

Rysunek 51: Weryfikacja działania modułu mMDAB

Błąd 500.21 oznacza problem z modułem .NET Core dla IIS – rozwiązanie zostało poruszone w rozdziale *11.7. Błąd 500.21 w IIS*.

Z kolei w przypadku, w którym rozmyślnie wybrano wymaganie SSL i zostanie wyświetlona zostanie biała strona lub błąd 403.4, należy skonfigurować SSL zgodnie z *3.13.2. Konfiguracja certyfikatu SSL*. Jeżeli wymaganie SSL zostało zaznaczone błędnie, jest możliwość jego wyłączenia zgodnie z podrozdziałem *11.5. Biała strona komponentu po instalacji przez instalator na IIS*.

5. Weryfikacja usługi sieciowej MIAM odbywa się poprzez wejście na stronę usługi, która kończy się frazą „MIAM”. Adres aplikacji MIAM dla przykładowej konfiguracji to: http://localhost/mMDAB/MIAM. Wyświetlona zostanie strona statusowa MIAM. Poprzez stronę statusową można zweryfikować, czy nawiązane zostało połączenie z bazą mMedica. Rezultat poprawnej komunikacji wygląda następująco:

Strona diagnostyczna MIAM

Status	OK
Wersja MIAM	6.3.0
Wersja mMedica	6.3.0
Połączenia z bazą danych mMedica	Tak
Baza mMedica w stanie aktualizacji	Nie
Licencja na moduł MIAM	Tak
Licencja na moduły	
Kompatybilność wersji	Tak
Uwagi dotyczące kompatybilności	OK
Data z serwera aplikacji	2019-09-25 11:22:41
Data z serwera bazy danych mMedica	2019-09-25 11:22:41

Rysunek 52: Weryfikacja MIAM

W przypadku problemów zostanie wyświetlony komunikat o błędzie. Możliwe problemy:

- nieprawidłowy adres serwera bazy danych, port lub nieprawidłowa nazwa bazy danych mMedica,
- brak komunikacji z serwerem bazy danych (zapora ogniowa lub konfiguracja serwera PostgreSQL).
- baza danych mMedica w stanie aktualizacji.

Uwaga: Najczęściej pojawiające się problemy zostały opisane w rozdziale *11. Rozwiązania częstych problemów.*

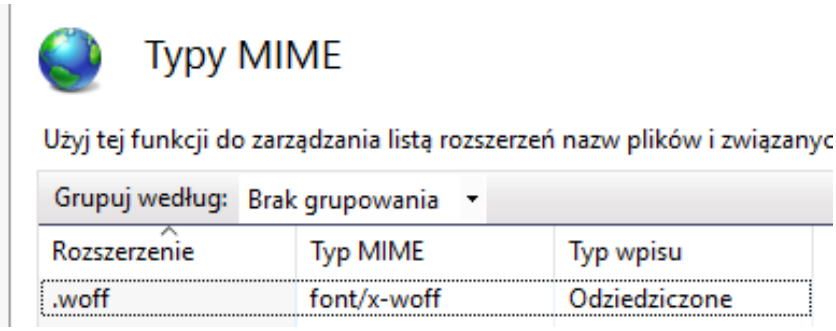
3.13. Dodatkowa konfiguracja IIS

3.13.1. Konfiguracja typów MIME w IIS

W przypadku instalacji manualnej należy dodać odpowiednie typy MIME do IIS. W pierwszym kroku należy zweryfikować czy poniżej podane typy nie zostały już wcześniej zdefiniowane:

Rozszerzenie	Typ MIME
.woff	font/x-woff
.woff2	application/font-x-woff2
.ttf	application/x-font-ttf

Można to zweryfikować klikając lewym przyciskiem myszy na wybraną witrynę (domyślnie „Default Web Site”), a następnie w oknie po lewej stronie wybrać ikonę z podpisem „Typy MIME”. Należy zwrócić uwagę, by zaznaczyć opcję widoku na „Widok funkcji” (na dole formatki). W typach MIME powinna wyświetlić się następująca pozycja (na przykładzie typu o rozszerzeniu .woff):



Rysunek 53: Podgląd typów MIME

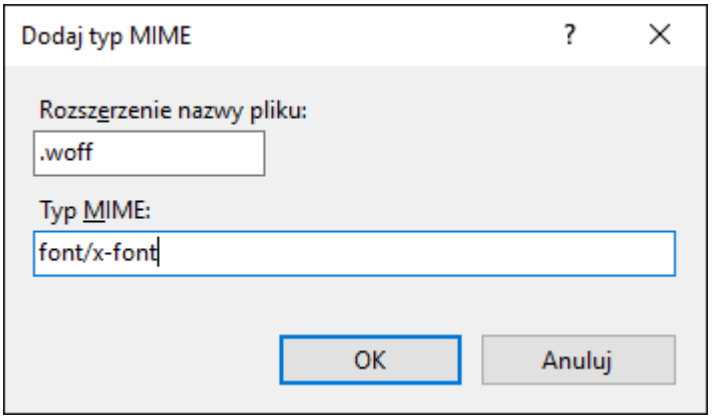
Należy również sprawdzić, czy wpis rejestrujący typ MIME nie znajduje się również w pliku C:\inetpub\wwwroot\web.config (o ile istnieje) w poniższej formie:

```
<mimeMap fileExtension="[rozszerzenie]" mimeType="[Typ MIME]" />
```

Przykład dla rozszerzenia .woff:

```
<mimeMap fileExtension=".woff" mimeType="font/x-woff" />
```

Sprawdzenia należy dokonać dla każdego podanego wyżej typu MIME. Jeśli dany plik nie istnieje, należy go dodać za pomocą opcji „Dodaj…” znajdującej się po prawej stronie listy Akcje, a następnie uzupełnić ją według poniższego wzoru:

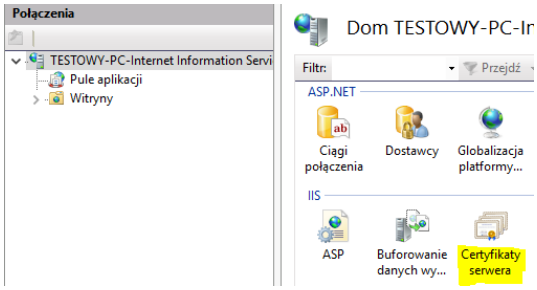


Rysunek 54: Tworzenie nowego typu MIME

3.13.2. Konfiguracja certyfikatu SSL

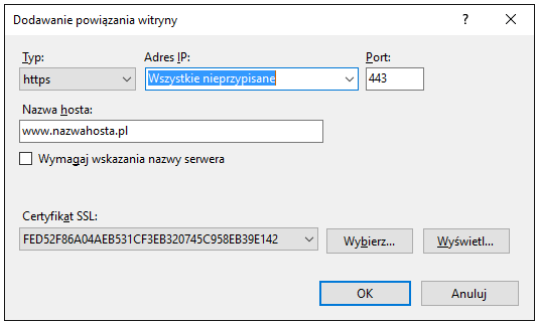
Konfiguracja certyfikatu SSL wygląda następująco:

1. Zainstalować otrzymany certyfikat w systemie operacyjnym zgodnie z instrukcją dostarczoną przez dystrybutora.
2. Otworzyć Menedżer internetowych usług sieciowych (IIS).
3. Wybrać z głównego okna opcję „Certyfikaty serwera”.



Rysunek 55: Dodawanie certyfikatów SSL

4. W otwartym oknie wybrać z menu po prawej stronie „Ukończ żądanie certyfikatu...”.
5. Wybrać certyfikat za pomocą przycisku „…”, nadać nazwę (do celów administracyjnych może być dowolna) oraz wybrać opcję „Osobisty” (dla pojedynczych certyfikatów SSL) lub „Usługa hosta sieci Web” dla certyfikatów z wykorzystaniem SNI). Zatwierdzić okno.
6. W menu po lewej stronie należy kliknąć prawym przyciskiem myszy na wybraną witrynę (domyślnie „Default Web Site”) i wybrać z menu kontekstowego opcję „Edytuj powiązania…”.
7. W otwartym oknie należy wybrać opcję „Dodaj…”.
8. Wybrać typ jako „https”, port zostawić na 443, ustawić odpowiedni adres domenowy w „Nazwa hosta” oraz wybrać certyfikat SSL z listy rozwijanej. Zatwierdzić okno.
9. Opcjonalnie można również usunąć powiązanie dla protokołu http na porcie 80.



Rysunek 56: Konfiguracja certyfikatu SSL dla witryny

10. Istnieje również możliwość wymuszenia korzystania z protokołu https poprzez zaznaczenie wybranej witryny (wybór z panelu środkowego „Ustawienia protokołu SSL”, w którym należy zaznaczyć opcję „Wymagaj protokołu SSL”).

3.13.3. Konfiguracja uwierzytelniania certyfikatem TLS

Uwaga: Konfiguracja uwierzytelnieniem certyfikatem jest dodatkowa (opcjonalna) i wymaga podstawowej wiedzy z zakresu konfiguracji serwera WWW.

Konfiguracja polega na wgraniu do aplikacji mMedica certyfikatu, który będzie wykorzystywany do komunikacji z Archiwum. Aplikacja Archiwum musi zostać skonfigurowana do przyjmowania komunikacji HTTPS oraz akceptowania przesyłanego przez mMedica certyfikatu. W takim przypadku Archiwum może dodatkowo uwierzytelniać ruch pochodzący z mMedica (oraz pośrednio z Portalu eRejestracja), a komunikacja po HTTPS pozwala na szyfrowanie ruchu. Do konfiguracji można wykorzystać certyfikaty wydane przez zaufanego dostawcę lub własnoręcznie wygenerowane. Warunkiem koniecznym jest, aby klucz publiczny miał możliwość użycia jako uwierzytelnienie klienta oraz serwera.

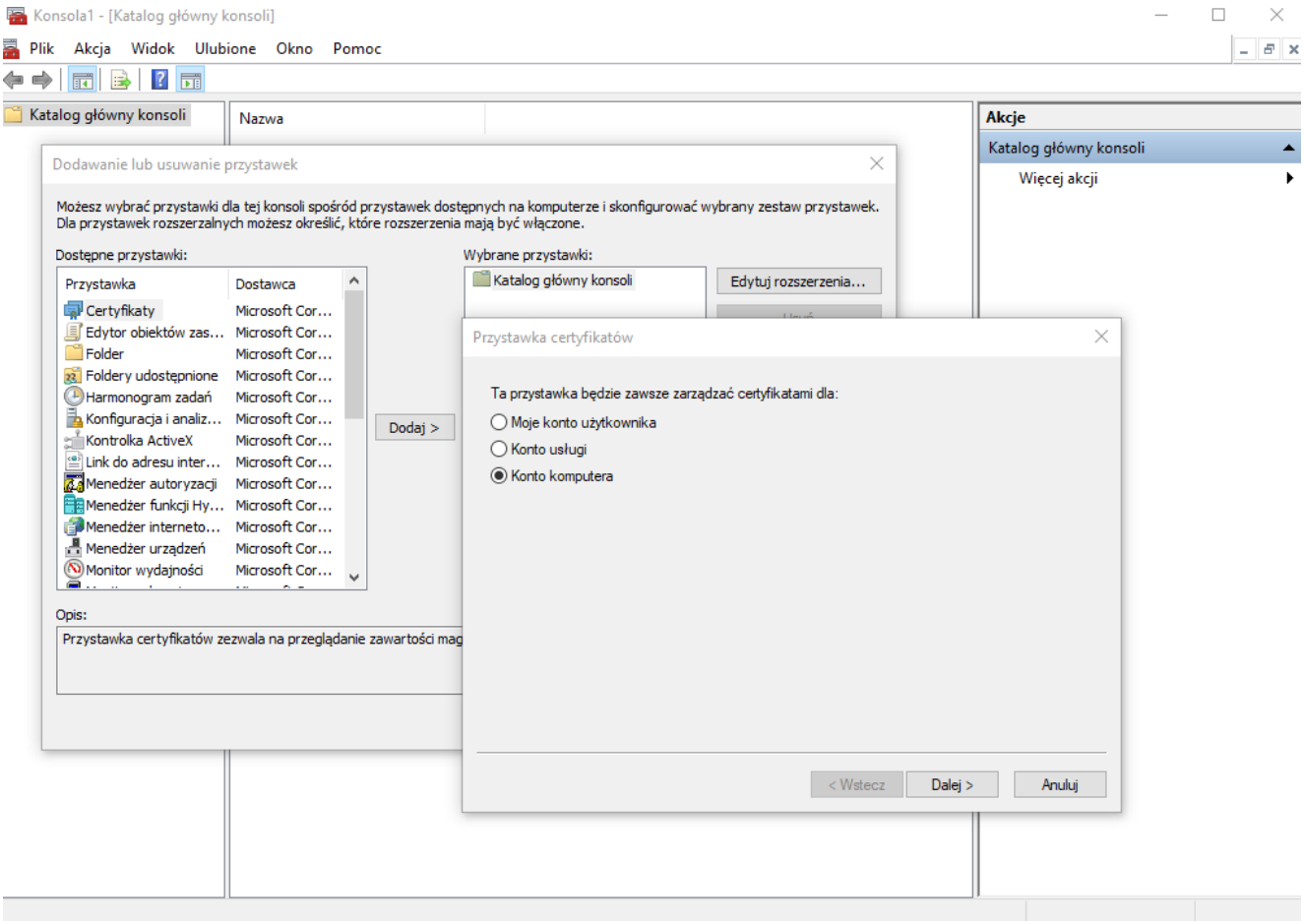
W celu skonfigurowania dodatkowego uwierzytelniania komunikacji za pomocą certyfikatu TLS dla Archiwum należy wykonać następujące kroki:

1. Dodanie certyfikatów (kluczy publicznych/klucza publicznego oraz klucza prywatnego) do magazynu certyfikatów.
2. Konfiguracja IIS.
3. Konfiguracja Archiwum.
4. Konfiguracja mMedica.

Uwaga: W przypadku posiadania wielu aplikacji w jednej witrynie w IIS razem z aplikacją Archiwum zaleca się przeniesienie Archiwum do osobnej witryny.

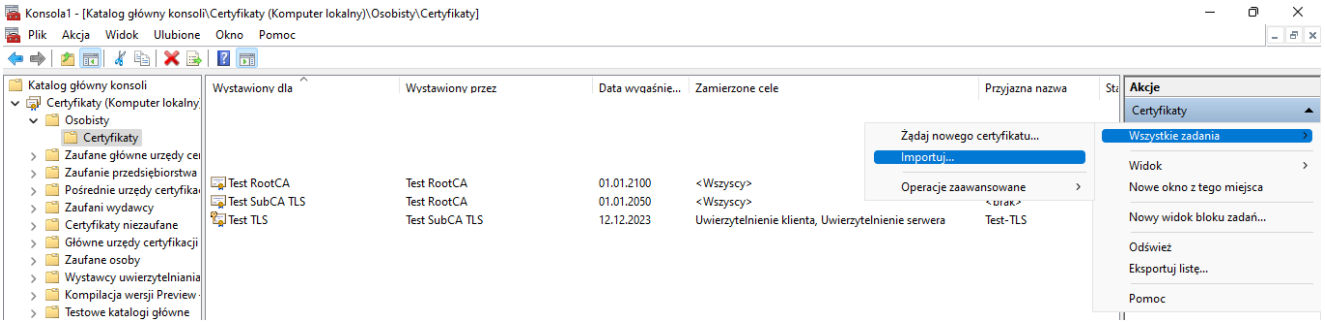
3.13.3.1. Dodawanie certyfikatu do magazynu certyfikatów

Do prawidłowej komunikacji należy pozyskać certyfikat do komunikacji po TLS wraz z certyfikatami nadrzędnymi, a następnie skonfigurować je w systemie operacyjnym. W celu skonfigurowania certyfikatu TLS wykorzystywanym do komunikacji oraz certyfikatów nadrzędnych wykorzystywanych podczas weryfikacji certyfikatu klienta TLS, należy w wierszu poleceń wprowadzić komendę „MMC” i wcisnąć na klawiaturze klawisz „Enter”. Operacja wymaga praw administratora. Po chwili powinno zostać otwarte okno. W oknie w menu „Plik” wybrać opcję „Dodaj/Usuń przystawkę…”. Wybrać przystawkę „Certyfikaty” i ją dodać. Przy dodawaniu przystawki należy wybrać opcję „Konto komputera”, a następnie opcję „Komputer lokalny”.



Rysunek 57: Dodawanie certyfikatów do komunikacji TLS

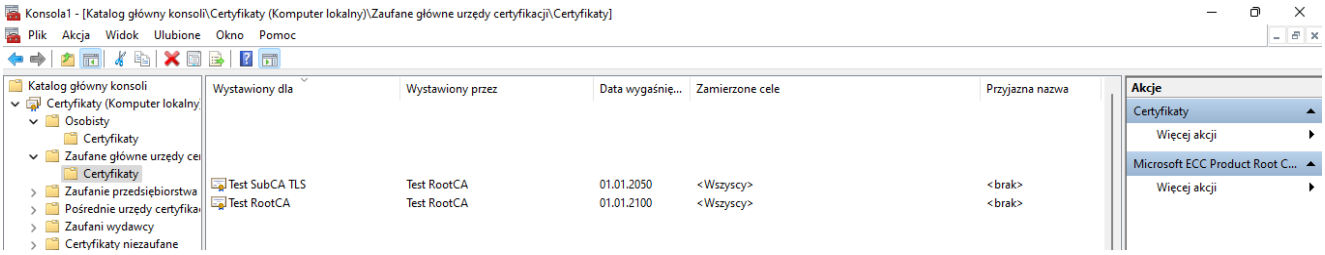
Po dodaniu przystawki kliknąć przycisk „Ok”. Rozwinąć katalog Certyfikaty i otworzyć katalog „Osobiste” > „Certyfikaty”. Po otwarciu katalogu wybrać z prawej strony opcję „Więcej akcji” > „Wszystkie zadania” > „Importuj”.



Rysunek 58: Importowanie certyfikatów

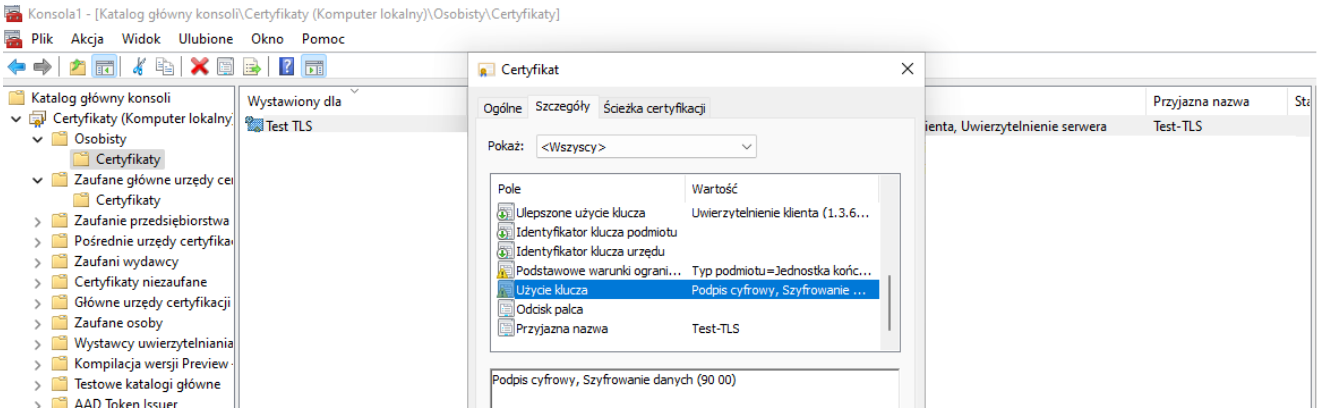
Należy zaimportować certyfikaty do komunikacji TLS, który należy umieścić w magazynie „Osobiste”. W przypadku, w którym plik z certyfikatem TLS nie zawiera certyfikatów nadrzędnych należy je wgrać osobno, w podobny sposób jak miało to miejsce w przypadku certyfikatu TLS. Certyfikaty nadrzędne należy umieścić w katalogu „Zaufane główne urzędy certyfikacji” > „Certyfikaty”.

Uwaga: W przypadku braku widoczności certyfikatu należy w oknie wybierania zmienić zakres wyświetlanych rozszerzeń plików.



Rysunek 59: Przeniesienie certyfikatów nadrzędnych

Należy uważać, aby certyfikat do komunikacji TLS posiadał właściwości użycia klucza: „Podpis cyfrowy, Szyfrowanie danych”. Można to sprawdzić klikając dwukrotnie w certyfikat TLS i przechodząc do zakładki „Szczegóły”.



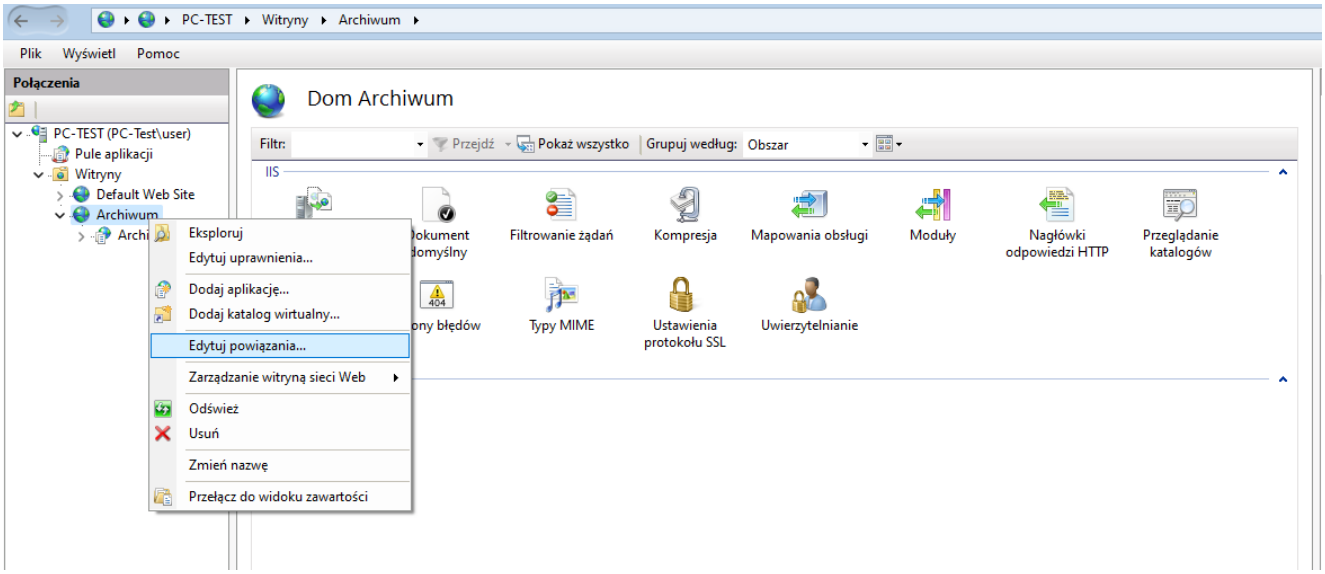
Rysunek 60: Weryfikacja właściwości certyfikatu

3.13.3.2. Konfiguracja IIS

Proces konfiguracji już zainstalowanego modułu Archiwum:

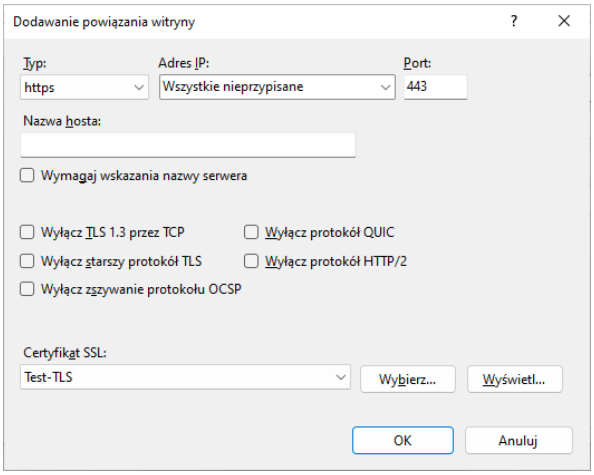
1. Uruchomić Menedżerze internetowych usług informacyjnych IIS (Internet Information Service Manager). Poniżej zamieszczono sposoby uruchomienia:
   a) Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr” i zatwierdzić klawiszem Enter,
   b) Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
2. Rozwinąć po lewej stronie drzewko „Połączenia” na nazwie komputera, a następnie rozwinąć „Witryny”.

3. Kliknąć prawym przyciskiem myszy na witrynę, w której znajduje się Archiwum i wybrać opcję „Edytuj powiązania”.



Rysunek 61: Edytowanie powiązania

4. W oknie wybrać opcję dodawania powiązania i następnie skonfigurować powiązanie typu „HTTPS”. Konieczne jest podanie certyfikatu SSL, należy tu wskazać certyfikat do komunikacji po TLS. Nie jest wymagane ustawianie aplikacji na porcie 443. Można wybrać dowolny niewykorzystany port.

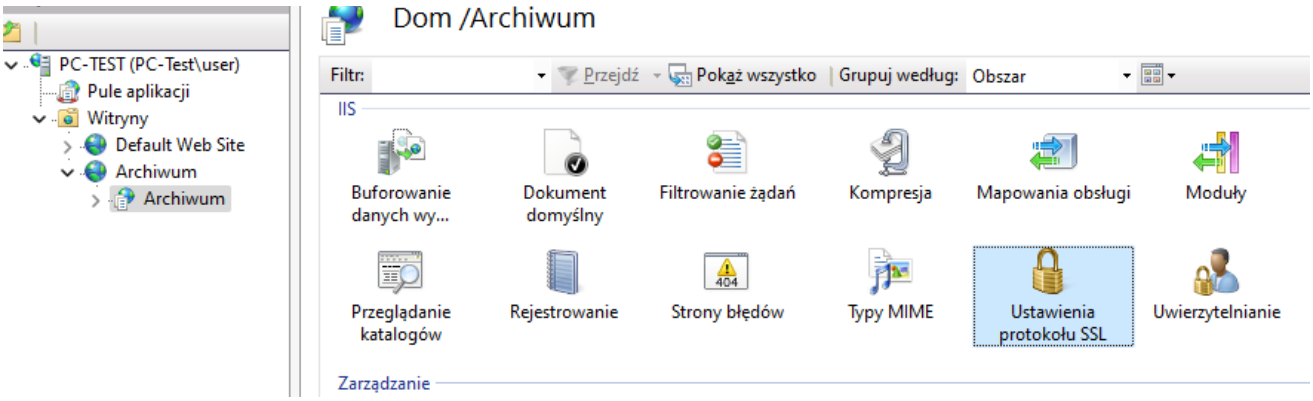


Rysunek 62: Konfiguracja powiązania typu "HTTPS"

Uwaga: Jeżeli certyfikat TLS nie jest widoczny w liście rozwijanej to możliwe, że konieczny jest restart komputera lub samego serwera IIS (z poziomu konsoli „cmd” uruchomionej w trybie administratora należy wpisać komendę „IISRESET”).

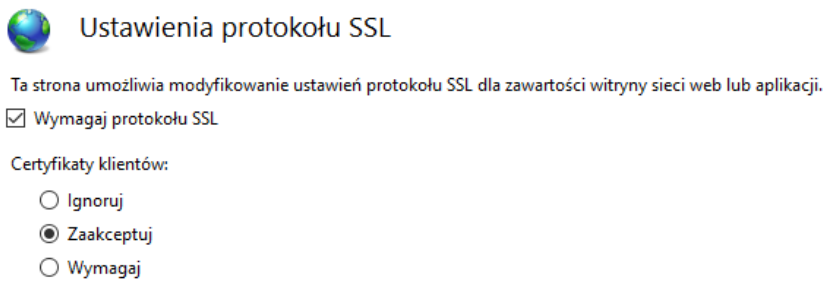
Uwaga: Zaleca się usunięcie wszelkich powiązań typu „HTTP”.

5. Wejść do aplikacji Archiwum z poziomu drzewa „Połączenia”.
6. Kliknąć dwukrotnie myszką w opcję „Ustawienia protokołu SSL”.



Rysunek 63: Przejście do konfiguracji SSL Archiwum

7. Zaznaczyć opcję „Wymagaj protokołu SSL”, natomiast w sekcji „Certyfikaty klientów” ustawić opcję „Zaakceptuj”. W celu prawidłowego działania szyfrowania komunikacji TLS z aplikacją Archiwum dopuszczalne są dwie formy konfiguracji:
   a) Zaakceptuj – pozwala na dostęp do części portalowej Archiwum bez przekazywania certyfikatu TLS. Dostęp do API dla mMedica oraz eRejestracji będzie wymagać przesłania certyfikatu TLS.
   b) Wymagaj – spowoduje, że aby dostać się do portalu aplikacji Archiwum konieczne będzie przekazanie certyfikatu TLS przez przeglądarkę. Dostęp do API dla mMedica oraz eRejestracji będzie wymagać przesłania certyfikatu TLS. Jeśli skonfigurowany certyfikat nie został wydany przez zaufanego dostawcę lub nie został wydany na domenę Archiwum wtedy należy się spodziewać ostrzeżenia w przeglądarce internetowej z informacją o nieprawidłowym certyfikacie.



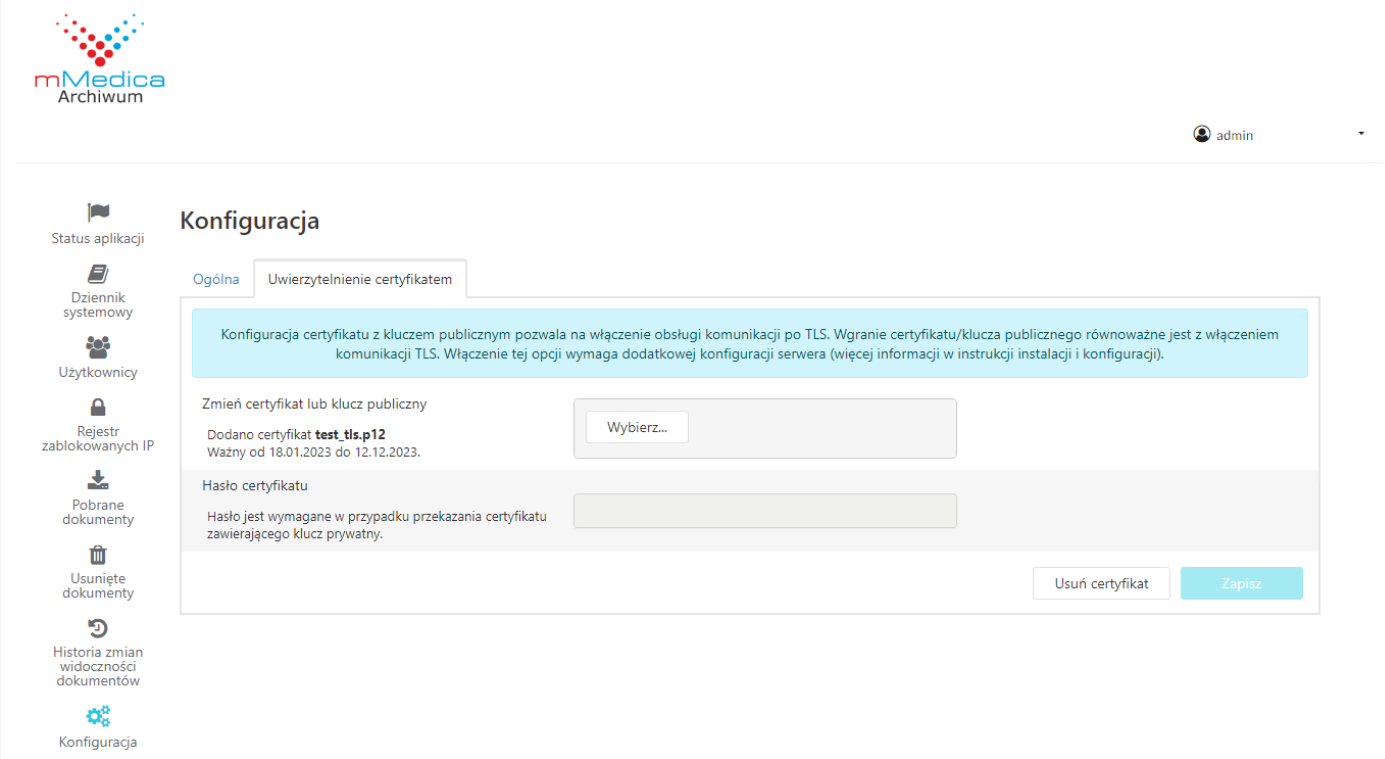
Rysunek 64: Parametry ustawienia protokołu SSL

8. Zapisać zmiany konfiguracji klikając z prawej strony okna opcję „Zastosuj”.

3.13.3.3. Konfiguracja Archiwum oraz mMedica

W celu dokończenia konfiguracji komunikacji TLS po stronie Archiwum konieczne jest wgranie certyfikatu TLS do Archiwum poprzez Portal Archiwum.

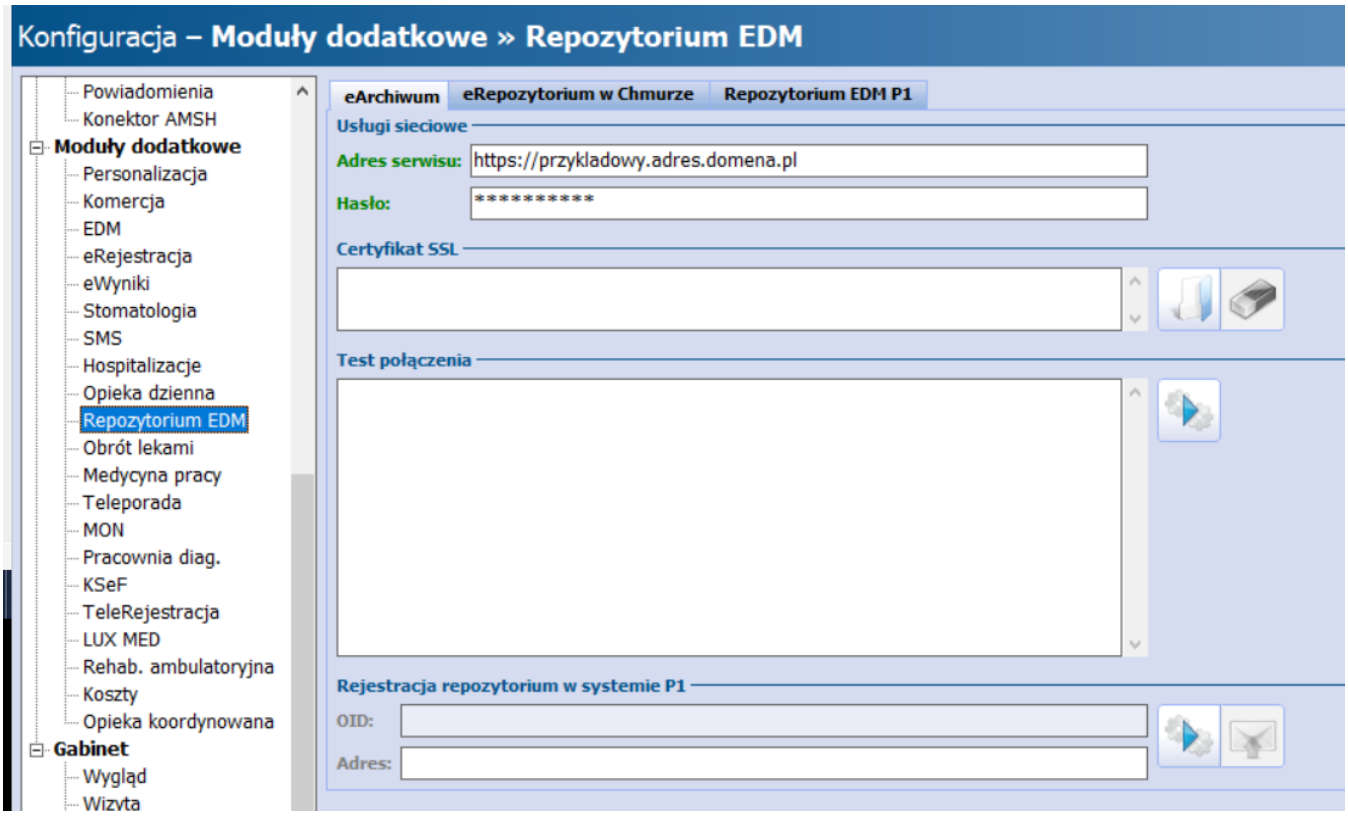
1. Zalogować się na administratora w Portalu Archiwum.
2. Przejść do zakładki „Konfiguracja” > „Uwierzytelnianie certyfikatem”.
3. Kliknąć przycisk „Wybierz” i wskazać plik certyfikatu TLS.
4. Podać hasło do certyfikatu.
5. Zapisać zmiany.
6. Po zapisaniu zmian formatka powinna prezentować się jak na poniższym zrzucie ekranu.



Rysunek 65: Konfiguracja komunikacji TLS w Archiwum

7. W celu przetestowania działania komunikacji TLS, należy zalogować się na administratora do aplikacji mMedica, a następnie przejść do formatki „Moduły dodatkowe”\„Repozytorium EDM”, a następnie przejść na zakładkę „eArchiwum”.
8. Należy podać adres Archiwum znajdującym się na protokole https://....
9. Podać prawidłowe hasło usług sieciowych, które również zostało zdefiniowane w Portalu Archiwum.
10. Wgrać certyfikat do komunikacji TLS w polu „Certyfikat SSL”.
11. Wykonać test połączenia z Archiwum.

Uwaga: eRejestracja automatycznie pobiera konfiguracje połączenia do Archiwum z bazy danych mMedica (również ustawienie certyfikatu) w przypadku integracji modułu eRejestracja+ z Archiwum. Oznacza to, że nie ma konieczności dodatkowej konfiguracji modułu eRejestracja po prawidłowej konfiguracji połączenia z mMedica do Archiwum.



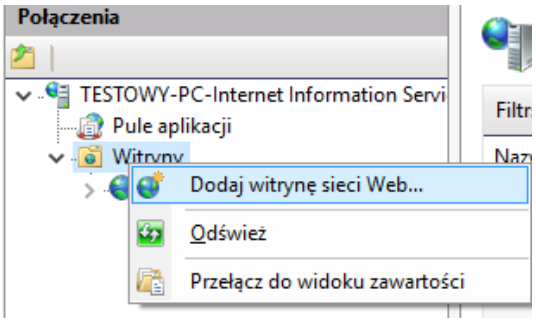
Rysunek 66: Konfiguracja połączenia do Archiwum w mMedica

3.13.4. Zaawansowana konfiguracja witryn

Numery portów komunikacji oraz wybór certyfikatu definiuje się na poziomie witryn IIS. W skład witryn wchodzą aplikacje, które dziedziczą ustawienia z witryny. Może zajść konieczność dodania nowej witryny (np. komponenty mogą pracować na innych portach lub pod innym certyfikatem). W tym rozdziale została opisana procedura dodawania nowej witryny oraz edycja powiązań witryn.

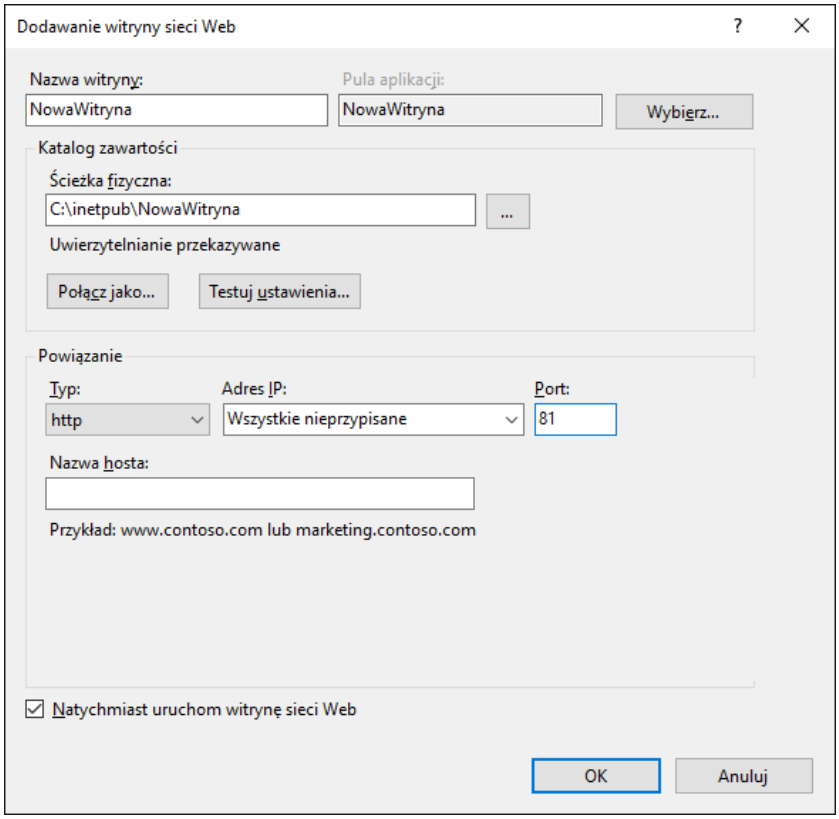
Dodawanie nowej witryny:

1. Uruchomić manager IIS.
2. Dodać nową pulę aplikacji.
3. Kliknąć prawym przyciskiem myszy na „Witryny” i wybrać „Dodaj witrynę sieci Web…”.



Rysunek 67: Dodawanie nowej witryny

4. W otwartym oknie nadać dowolną nazwę witryny. Za pomocą „Wybierz” wybrać stworzoną pulę aplikacji. Następnie przez przycisk „…” podać ścieżkę fizyczną do folderu, w którym znajdą się pliki aplikacji. Ostatnim etapem jest konfiguracja powiązania, która została opisana w dalszej części podrozdziału.



Rysunek 68: Okno dodawania nowej witryny

5. Do nowej witryny można dodawać nowe aplikacje oraz komponenty modułu tak jak zostało to opisane w oraz *3.14 Doinstalowanie komponentów*).

Edycja powiązań (zmiana: portu, nazwy hosta, certyfikatu, powiązania IP):

1. Uruchomić manager IIS.
2. Na wybranej witrynie kliknąć prawym przyciskiem „Edytuj powiązania…”.

3. W oknie zaznaczyć istniejące powiązanie (domyślnie http na porcie 80) i wybrać przycisk „Edytuj…” lub przycisk „Dodaj…”.
4. W oknie „Edytowanie powiązań witryny” można zdefiniować typ, nazwę hosta oraz port. Dodatkowo istnieje możliwość przypisania konkretnego adresu IP, z którego będzie dostępna witryna (opcja „Wszystkie nieprzypisane” oznacza dostępność dla wszystkich dostępnych adresów IP).

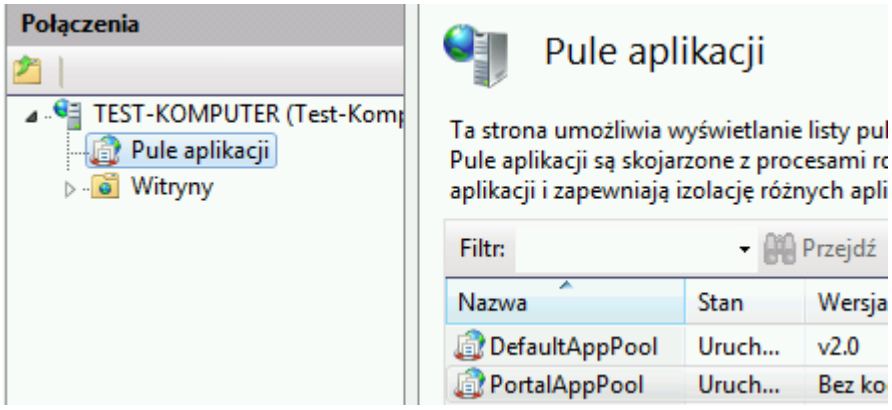
Uwaga: Każda z witryn, która nie posiada przypisanego adresu domenowego musi mieć unikalne numery portów.

Uwaga: W przypadku wykorzystywania innych portów niż 80 (dla http) oraz 443 (dla https) należy posługiwać się adresem zawierającym port np. http://localhost:81 (dla portu 81).

3.13.5. Zaawansowana konfiguracja aplikacji

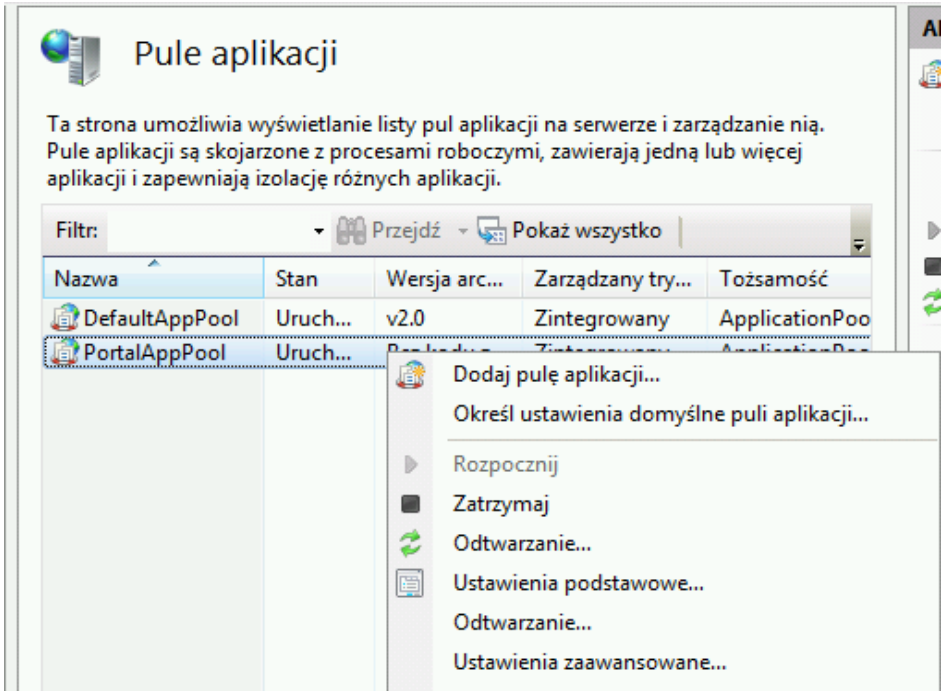
W celu wydłużenia czasu usypiania aplikacji w środowisku IIS należy uruchomić Menedżer internetowych usług informacyjnych.

Rozwinąć po lewej stronie drzewko „Połączenia” na nazwie komputera i wybrać opcję „Pule aplikacji”.



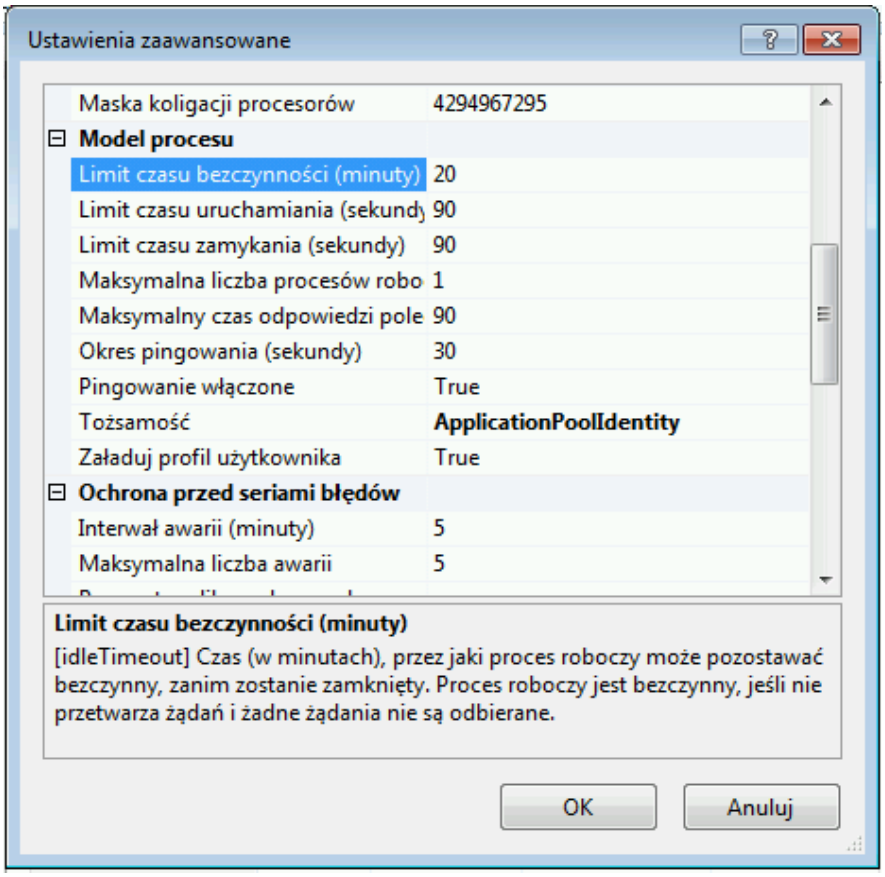
Rysunek 69: Drzewko "Połączenia" w aplikacji IIS Manager

Po wybraniu powyższej opcji po prawej stronie pojawi się okno do zarządzania pulami aplikacji. Z listy dostępnych pul należy wybrać interesującą nas pulę, kliknąć na nią prawym przyciskiem myszy i wybrać opcję „Ustawienia zaawansowane…”.



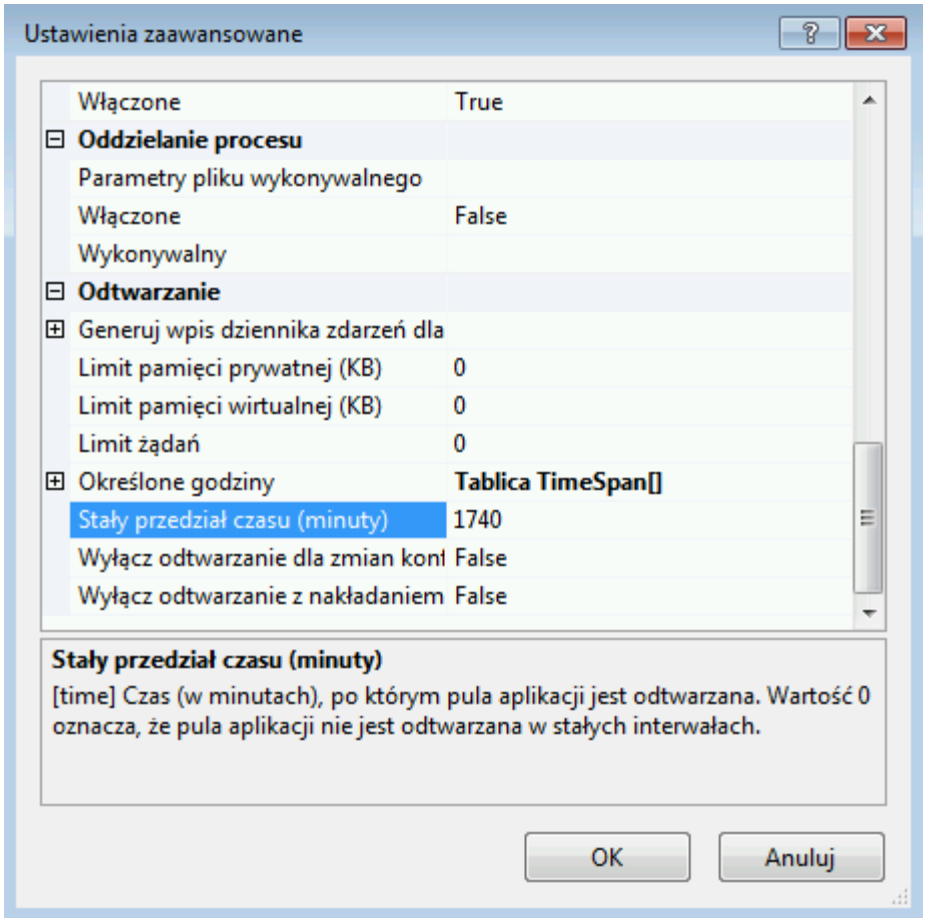
Rysunek 70: Okno zarządzania pulami aplikacji

Po wybraniu opcji pojawi się okno konfiguracji.



Rysunek 71: Okno konfiguracji - "Ustawienia zaawansowane": Limit czasu bezczynności (minuty)

Modyfikowanie wartości w polu „Limit czasu bezczynności (minuty)” pozwala na wydłużenie/skrócenie czasu, po którym aplikacja przejdzie w stan uśpienia. Ustawienie wartości 0 pozwala na skonfigurowania aplikacji tak, aby nie była ona usypiana.



Rysunek 72: Okno konfiguracji - "Ustawienia zaawansowane": Stały przedział czasu (minuty)

Kolejnym parametrem jest „Stały przedział czasu (minuty)”. Pozwala on na określenie czasu, po jakim pula aplikacji powinna ulec zrestartowaniu. Parametr ten również można ustawić na wartość 0. Spowoduje to, że pula aplikacji nie będzie restartowana. Nie jest to zalecane ze względu na zużywanie pamięci przez aplikację, gdyż w przypadku wykorzystania zbyt dużej ilości zasobów może dojść do błędów.

3.14. Doinstalowanie komponentów

Zarówno dla instalacji z pełnym wykorzystaniem instalatora, jak i w przypadku instalacji manualnej, możliwe jest doinstalowanie dodatkowych instalacji Archiwum. Jeśli konieczne jest zainstalowanie nowego komponentu (który nie jest zainstalowany), to można to zrobić z instalatora zgodnie z opisem w rozdziale *3.9.*

Instalacja dodatkowych modułów/komponentów. W przypadku instalacji manualnej należy zapoznać się z rozdziałem *3.10. Instalacja manualna.* Proces dodawania nowego komponentu wygląda następująco:

1. Dodać nową witrynę, jeżeli jest to konieczne (*3.13.3. Zaawansowana konfiguracja witryn*).
2. Dodać nową pulę aplikacji dla nowej aplikacji.
3. Dodać nową aplikację wybierając utworzoną pulę aplikacji oraz ścieżkę fizyczną do folderu, który będzie przechowywać pliki komponentu.
4. Dodać bazę danych za pomocą instalatora. W przypadku pierwszego użycia instalatora należy dodać bazę danych tak jak zostało to opisane w rozdziale *3.10. Instalacja manualna***.** W przypadku, w którym użyto już wcześniej instalatora do instalacji bazy danych lub dowolnego komponentu, należy przeprowadzić proces dodawania nowej bazy zgodnie z rozdziałem *6. Zarządzanie oraz kopie zapasowe baz danych*.
5. Skopiować do folderu z punktu 2. pliki komponentu – odnośnik lub wykonać kopię plików komponentu zainstalowanych przez instalator.
6. Skonfigurować połączenie z bazą danych dla Archiwum lub mMDAB (Uwaga: proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja - *5.1. Konfiguracja połączenia z bazami danych*).
7. Skonfigurować nazwy aplikacji (*3.11. Konfiguracja nazwy aplikacji*).
8. Zweryfikować instalację (*3.12.* Weryfikacja instalacji).

3.15. Restartowanie i zatrzymywanie komponentów

Komponenty zawierają wewnętrzną pamięć podręczną i może istnieć potrzeba jej wyczyszczenia za pomocą zrestartowania komponentu. Takim przypadkiem, w którym należy zrestartować komponent jest odtworzenie kopii zapasowej bazy danych.

Możliwe jest pełne zrestartowanie komponentu na dwa sposoby:

1. Zatrzymać pracę usługi IIS. Opcja jest dostępna w IIS z menu „Akcje” (Zarządzanie serwerem) z poziomu przycisk „Zatrzymaj”. Ponowne uruchomienie serwera IIS możliwe jest również z poziomu menu „Akcje” wybierając przycisk „Rozpocznij”.
2. Zatrzymanie witryny w IIS, w której znajdują się komponenty do zatrzymania. Z poziomu IIS rozwinąć po prawej stronie z okna „Połączenia” katalog „Witryny” i zaznaczyć wybraną witrynę. Następnie z menu po prawej stronie (o nazwie „Zarządzanie witryną sieci Web”) należy wybrać przycisk „Zatrzymaj”. Aby ponownie uruchomić witryny należy wybrać opcję „Rozpocznij”.

3.16. Aktualizacja modułu

W przypadku instalacji za pomocą instalatora w celu aktualizacji należy uruchomić najnowszy instalator modułów mMedica. Instalator wykryje istniejącą instalację Archiwum i zaktualizuje pliki, które zostały wcześniej utworzone przez instalator. Instalator równocześnie zaktualizuje wszystkie zainstalowane komponenty mModułów.

W przypadku instalacji manualnej należy podmienić wszystkie pliki komponentów oraz przenieść ustawienia z wcześniej skonfigurowanych plików appsettings.json do nowych. Nie zaleca się podmiany plików na wcześniej skonfigurowane, gdyż struktura pliku konfiguracyjnego może ulegać zmianie.

Dla każdego z powyższych sposobów instalacji instalator aktualizuje wszystkie dostępne na serwerze bazy danych Archiwum oraz (jeśli istnieją) bazy danych modułu eRejestracja. Zaleca się tworzenie kopii bazy danych przed wykonaniem aktualizacji modułu.

Proces aktualizacji powinien być wykonywany na zatrzymanych komponentach modułów mMedica w IIS (całym serwerze lub witrynie, w której znajdują się instalacje). Po aktualizacji należy uruchomić ponownie komponent na serwerze WWW. W przypadku aktualizacji przez instalator proces zatrzymywania i uruchamiania serwera jest dokonywany przez instalator. Z kolei w przypadku instalacji manualnej należy posłużyć się opisem znajdujących się w rozdziale *3.15. Restartowanie i zatrzymywanie komponentów*.

4. Instalacja w dystrybucjach Linux

4.1. Wymagania

Uwaga: Wymagania dotyczące uruchomienia modułu Archiwum są zbieżne z modułem eRejestracja. Oznacza to, że jeśli na serwerze zainstalowano moduł eRejestracja spełnia on również wymagana dotyczące Archiwum i nie wymaga on instalacji dodatkowego oprogramowania.

Instalacja modułu Archiwum możliwa jest na dystrybucji Linux, jeżeli jest możliwa instalacja poniższego oprogramowania:

- serwer WWW Apache2,
- libunwind8,
- ASP .NET Core 6.0 (więcej informacji: https://docs.microsoft.com/pl-pl/dotnet/core/install/linux).

Uwaga: Funkcjonalności związane z aplikacją Informacje Medyczne wymagają, aby komputery, na których zostanie zainstalowane Archiwum miały publiczny i stały adres IP.

4.2. Instalacja

Proces instalacji dla przypadku instalacji wszystkich komponentów oraz serwera bazy danych na jednym komputerze można opisać za pomocą następujących kroków:

1. Instalacja i przygotowanie bazy danych (*4.3. Instalacja bazy danych Archiwum*).
2. Instalacja niezbędnego oprogramowania (*4.4. Instalacja wymaganego oprogramowania*).
3. Skopiowanie plików komponentów (*4.5. Konfiguracja serwera oraz instalacja modułu*).
4. Konfiguracja serwera Apache (*4.5. Konfiguracja serwera oraz instalacja modułu*).
5. Konfiguracja nazw aplikacji (*4.6. Konfiguracja nazwy aplikacji*).
6. Konfiguracja adresów aplikacji (*4.7. Konfiguracja adresu aplikacji*).
7. Konfiguracji połączenia z bazami danych dla komponentów (Uwaga: proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja - *5.1. Konfiguracja połączenia z bazami danych*).
8. Weryfikacja instalacji (*4.8. Weryfikacja instalacji*).
9. Konfiguracja dodatkowa serwera WWW (*4.9. Konfiguracja dodatkowa Apache*).

4.3. Instalacja bazy danych Archiwum

Pierwszym etapem jest zainstalowanie serwera bazy danych PostgreSQL zgodnie z instrukcją: https://mmedica.asseco.pl/assets/Dokumentacja/mM-Instalacja-programu-mMedica.pdf (identycznie jak w przypadku oprogramowania mMedica). Drugim etapem jest zainstalowanie bazy danych poprzez uruchomienie instalatora mModuły z poziomu stacji roboczej z systemem Windows.

4.4. Instalacja wymaganego oprogramowania

UWAGA: Do przeprowadzenia procesu instalacji wymagana jest podstawowa znajomość systemów operacyjnych opartych o jądro Linux.

Poniżej przedstawiono procedurę instalacji wymaganego przez moduł oprogramowania na przykładzie Ubuntu Server 20.04 z poziomu konsoli:

1. Pobranie listy pakietów z repozytorium:

```
sudo apt-get update
```

2. Instalacja serwera WWW Apache:

```
sudo apt-get install apache2
```

3. Instalacja pakietu libcurl4-openssl-dev:

```
sudo apt-get install libcurl4-openssl-dev
```

4. Instalacja pakietu libunwind8:

```
sudo apt-get install libunwind8
```

5. Instalacja ASP .NET Core 6.0:

   a) Rejestracja produktu Microsoft:

```
wget https://packages.microsoft.com/config/ubuntu/20.04/packages-microsoft-
prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
rm packages-microsoft-prod.deb
```

UWAGA: Podczas realizacji tych komend najlepiej znajdować się w katalogu domowym, tak aby posiadać pełne uprawnienia do katalogów.
Na stronie https://docs.microsoft.com/pl-pl/dotnet/core/install/linux w poszczególnych działach, znajdują się instrukcje dla innych popularnych wersji systemu.

   b) Aktualizacja listy pakietów z repozytorium:

```
sudo apt-get update
```

c) Instalacja pakietu apt-transport-https:

```
sudo apt-get install apt-transport-https
```

d) Aktualizacja listy pakietów z repozytorium:

```
sudo apt-get update
```

e) Instalacja pakietu ASP .NET Core:

```
sudo apt-get install aspnetcore-runtime-6.0
```

UWAGA: Do prawidłowego działania modułu wymagana jest instalacja aspnetcore-runtime w wersji 6.0. Alternatywnie możliwa jest instalacja dotnet-sdk w wersji 6.0.

Proces instalacji dla innych dystrybucji Linux został opisany pod adresem: https://docs.microsoft.com/pl-pl/dotnet/core/install/ w poszczególnych działach.

4.5. Konfiguracja serwera oraz instalacja modułu

W niniejszym rozdziale omówiono najprostszą konfigurację serwera Apache. Procedura wygląda następująco:

1. Do katalogu /var/www (domyślny katalog stron dla Apache) należy przekopiować katalogi ze źródłami Archiwum oraz mMDAB. Zwartość katalogu MIAM musi zostać umieszczona w katalogu /var/www/mMDAB/modules/MIAM.
2. Należy przeprowadzić wstępną konfigurację opisaną w punktach *4.6. Konfiguracja nazwy aplikacji* oraz *4.7. Konfiguracja adresu aplikacji*.
3. Jeżeli w katalogu /var/www znajduje się plik index.html, należy go usunąć lub przenieść w inne miejsce.
4. Skonfigurować plik witryny /etc/apache2/sites-available/default (lub 000-default.conf) lub plik z konfiguracją SSL:

```
<VirtualHost *:80>
      ServerName localhost
      ProxyPreserveHost On
      ProxyPass /Archiwum http://localhost:5003/
      ProxyPassReverse /Archiwum http://localhost:5003/
      ProxyPass /mMDAB http://localhost:5001/
      ProxyPassReverse /mMDAB http://localhost:5001/
</VirtualHost>
```

- ServerName – nazwa lub adres serwera,
- ProxyPass oraz ProxyPassReverse zapewniają dwukierunkową komunikację. Pierwszym elementem jest adres routingu (jest on bezpośrednio powiązany z Konfiguracja nazwy aplikacji).

Drugi element to adres aplikacji, na który przekierowany ma zostać ruch (parametr powiązany z Konfiguracja adresu aplikacji).

Powyższy plik konfiguracyjny (dla protokołu http) definiuje wykorzystanie domyślnego portu 80 do komunikacji oraz wskazuje aplikacje na jakie przekierowywany ma być ruch. Apache pełni tu rolę serwera pośredniczącego, dlatego konieczne jest zezwolenie serwerowi na tego typu operacje:

```
sudo a2enmod ssl
sudo a2enmod proxy
sudo a2enmod proxy_balancer
sudo a2enmod proxy_http
sudo a2enmod headers
```

Apache domyślnie przekierowuje oryginalny adres IP żądania do aplikacji. Automatyczne przekierowanie protokołu z (http lub https) możliwe jest po dodaniu do pliku konfiguracji witryny wpisu:

```
RequestHeader set "X-Forwarded-Proto" expr=%{REQUEST_SCHEME}
```

5. Skonfigurować połączenie komponentów z bazami danych według opisu (Uwaga: proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja - *5.1. Konfiguracja połączenia z bazami danych*).
6. Zrestartować serwer Apache:

```
sudo service apache2 restart
```

7. Utworzyć skrypty uruchomieniowe:
   a) plik Archiwum.sh o zawartości:

```
#!/bin/sh
cd /var/www/Archiwum
dotnet ./Archiwum.dll
```

   b) plik mMDAB.sh o zawartości:

```
#!/bin/sh
cd /var/www/mMDAB
dotnet ./mMedica.mMDAB.dll
```

   c) Nadać plikom uprawnienia do wykonywania:

```
sudo chmod +x Archiwum.sh mMDAB.sh
```

8. Dodać aplikację do serwisu:
   a) Utworzyć plik mMedica.Archiwum.service w katalogu /etc/systemd/system o zawartości:

```
[Unit]
Description = mMedica Archiwum
[Service]
ExecStart=/var/www/Archiwum.sh
WorkingDirectory=/var/www/Archiwum
Restart=always
RestartSec=10
SyslogIdentifier=mMedica-Archiwum
```

```
User=user
Environment=ASPNETCORE_ENVIRONMENT=Production

[Install]
WantedBy=Multi-user.target
```

b) Utworzyć plik mMedica.mMDAB.service w katalogu /etc/systemd/system o zawartości:

```
[Unit]
Description = mMedica mMDAB
[Service]
ExecStart=/var/www/mMDAB.sh
WorkingDirectory=/var/www/mMDAB
Restart=always
RestartSec=10
SyslogIdentifier=mMedica-mMDAB
User=user
Environment=ASPNETCORE_ENVIRONMENT=Production

[Install]
WantedBy=Multi-user.target
```

W pole User należy wprowadzić nazwę istniejącego w systemie użytkownika, na którym uruchomiony zostanie serwis (nie zaleca się stosowanie użytkownika root).

c) Udostępnić serwisy:

```
sudo systemctl enable mMedica.Archiwum.service
sudo systemctl enable mMedica.mMDAB.service
```

d) Uruchomić serwisy:

```
sudo systemctl start mMedica.Archiwum.service
sudo systemctl start mMedica.mMDAB.service
```

9. Nadać uprawnienia do plików i folderów:

a) Nadać uprawnienia do zapisu pliku application.log w Archiwum:

```
sudo chmod +w /var/www/Archiwum/application.log
```

b) Nadać uprawnienia do zapisu plików application.log w mMDAB i MIAM:

```
sudo chmod +w /var/www/mMDAB/application.log
sudo chmod +w /var/www/mMDAB/modules/MIAM/application.log
```

c) Nadać uprawnienia do modyfikowania pliku modules.xml dla mMDAB:

```
sudo chmod 666 /var/www/mMDAB/modules.xml
```

4.6. Konfiguracja nazwy aplikacji

Jeśli Archiwum lub\i MDAB nie posiadają własnego adresu domenowego, to w pliku appsettings.json znajdującym się w katalogu każdej z aplikacji należy wprowadzić nazwę aplikacji. Nazwa ta nie jest dowolna.

Należy wprowadzić dokładnie tę samą nazwę, która zostanie wykorzystana do konfiguracji serwera apache. Nazwa ta znajduje się w zaznaczonych miejscach:

```
<VirtualHost *:80>
      ServerName localhost
      ProxyPreserveHost On
      ProxyPass /Archiwum http://localhost:5003/
      ProxyPassReverse /Archiwum http://localhost:5003/
      ProxyPass /mMDAB http://localhost:5001/
      ProxyPassReverse /mMDAB http://localhost:5001/
</VirtualHost>
```

Nazwę tą należy umieścić w sekcji ApplicationName:

a) w pliku konfiguracyjnym w Archiwum (dla przykładowej konfiguracji):

```
"ApplicationName": "Archiwum"
```

b) w pliku konfiguracyjnym w mMDAB (dla przykładowej konfiguracji):

```
"ApplicationName": "mMDAB"
```

Nazwy powinny być unikalne w ramach jednego serwera www.

4.7. Konfiguracja adresu aplikacji

Poprzez konfigurację sekcji ApplicationUrl w pliku appsettings.json zmieniać można adres pod jakim widoczna będzie aplikacja. Adres dla przykładowej konfiguracji:

```
"ApplicationUrl": "http://localhost:5003"
```

Port powinien być unikalny w ramach całego serwera.

4.8. Weryfikacja instalacji

W przypadku wykorzystywania systemu bez środowiska graficznego pomocne jest skorzystanie z drugiego komputera w celu wyświetlenia zawartości komponentów w przeglądarce internetowej (należy wtedy pamiętać o wpisaniu odpowiedniego adresu IP zamiast localhost).

1. Weryfikacja usługi sieciowej Archiwum odbywa się poprzez wejście na stronę usługi, dla konfiguracji przykładowej adres wygląda następująco http://localhost/Archiwum. Wyświetlona zostanie strona statusowa dla aplikacji Archiwum z możliwością zalogowania się. Strona statusowa pozwala zweryfikować czy połączenie z bazą danych jest prawidłowe. Rezultat poprawnego działania Archiwum wygląda następująco:

mMedica Archiwum

ZALOGUJ SIĘ

Status aplikacji mMedica Archiwum

Status	Ok
Wersja aplikacji	5.15.0
Wersja bazy danych	5.15.0
Połączenie z bazą danych Archiwum	Tak
Kompatybilność wersji	Tak
Data z serwera aplikacji	20.09.2018 12:22:53
Data z serwera bazy danych Archiwum	20.09.2018 12:22:54

Rysunek 73: Weryfikacja działania aplikacji Archiwum

2. Weryfikacja usługi sieciowej mMDAB odbywa się poprzez wejście na stronę statusową usługi. Adres usługi dla przykładowej konfiguracji to: http://localhost/mMDAB. Wyświetlona zostanie strona statusowa z informacjami o dołączonych modułach takich jak MIAM.

Strona diagnostyczna mMedica DAB

Połączenie z bazą mMedica	Połączono

Link do pomocy swagger

Dołączone moduły				
Nazwa modułu	Wersja	Adres statusu	Port modułu	Udostępniony swagger
MIAM	6.3.0	/MIAM	5002	Tak

Rysunek 74: Weryfikacja działania modułu mMDAB

3. Weryfikacja usługi sieciowej MIAM odbywa się poprzez wejście na stronę usługi, która kończy się frazą „MIAM”. Adres aplikacji MIAM dla przykładowej konfiguracji to: http://localhost/mMDAB/MIAM. Wyświetlona zostanie strona statusowa MIAM. Poprzez stronę statusową można zweryfikować, czy nawiązane zostało połączenie z bazą mMedica. Rezultat poprawnej komunikacji wygląda następująco:

Strona diagnostyczna MIAM

Status	OK
Wersja MIAM	6.3.0
Wersja mMedica	6.3.0
Połączenia z bazą danych mMedica	Tak
Baza mMedica w stanie aktualizacji	Nie
Licencja na moduł MIAM	Tak
Licencja na moduły	
Kompatybilność wersji	Tak
Uwagi dotyczące kompatybilności	OK
Data z serwera aplikacji	2019-09-25 11:22:41
Data z serwera bazy danych mMedica	2019-09-25 11:22:41

Rysunek 75: Weryfikacja MIAM

W przypadku problemów zostanie wyświetlony komunikat o błędzie. Możliwe problemy:

- nieprawidłowy adres serwera bazy danych, port lub nieprawidłowa nazwa bazy danych mMedica,
- brak komunikacji z serwerem bazy danych (zapora ogniowa lub konfiguracja serwera PostgreSQL).
- baza danych mMedica w stanie aktualizacji.

Jeśli strona Archiwum lub mMDAB się nie otwiera, należy sprawdzić czy usługa Apache działa:

```
service apache2 status
```

W wyniku powinien zostać wyświetlony status jako „active (running)”. Jeżeli usługa nie jest uruchomiona należy ją uruchomić:

```
sudo service apache2 start
```

Jeżeli strona nadal się nie wyświetla, a status Apache jest poprawny, należy sprawdzić status serwisu:

- Dla Archiwum:

```
sudo systemctl status mMedica.Archiwum.service
```

- Dla mMDAB:

```
sudo systemctl status mMedica.mMDAB.service
```

W wyniku powinien zostać wyświetlony status jako „active (running)”. Jeżeli usługi nie są uruchomione, należy je uruchomić i ponownie sprawdzić ich status. W przypadku, gdy status się nie zmieni,

należy sprawdzić czy pliki konfiguracyjne zawierają dobre dane, pliki skryptowe oraz konfiguracje serwisów zawierają odpowiednią treść.

Uwaga: Najczęściej pojawiające się problemy zostały opisane w rozdziale *11. Rozwiązania częstych problemów*.

4.9. Konfiguracja dodatkowa Apache

4.9.1. Konfiguracja typów MIME

Należy dodać do Apache obsługę następujących typy plików MIME (MIME type):

- typ: application/x-font-woff (o rozszerzeniu woff)
- typ: application/x-font-woff2 (o rozszerzeniu woff2)
- typ: application/x-font-ttf (o rozszerzeniu ttf)

W tym celu należy otworzyć plik zawierający konfigurację typów MIME mime.types, który w zależności od dystrybucji znajduje się najczęściej pod ścieżką: /etc/mime.types lub /usr/local/etc/httpd/conf/mime.types. Następnie sprawdzić czy w pliku znajdują się powyższe wpisy, a w przypadku ich braku należy je dodać. Konwencja dodawania wpisów jest następująca:

typ rozszerzenie rozszerzenie rozszerzenie

Przykładowe wpisy:

application/x-font-woff woff

application/x-font-woff2 woff2

Po edycji pliku należy go zapisać, a także zrestartować usługę Apache:

```
sudo service apache2 restart
```

4.9.2. Konfiguracja certyfikatu SSL

Proces konfiguracji certyfikatu SSL wygląda następująco:

1. Uruchomić moduł „ssl” dla Apache (zazwyczaj jest on już uruchomiony):

   ```
   sudo a2enmod ssl
   ```

2. Uruchomić moduł „headers” dla Apache:

   ```
   sudo a2enmod headers
   ```

3. Skopiować pliki zawierające:

- certyfikat serwera (crt),
- certyfikat pośredni (crt),
- klucz prywatny (key)

do katalogu, z którego serwer Apache będzie dokonywał ich odczytu, np.: /etc/ssl/certs/.

4. Otworzyć istniejący plik konfiguracyjny witryny (domyślnie default-ssl.conf) lub dodać nowy, a następnie dodać (modyfikując ścieżki do plików z punktu 2.) elementy oznaczone kolorem zielonym:

```
<VirtualHost *:443>
     ServerName localhost
     ProxyPreserveHost On
     ProxyPass /Archiwum http://localhost:5003/
     ProxyPassReverse /Archiwum http://localhost:5003/
     ProxyPass /mMDAB http://localhost:5001/
     ProxyPassReverse /mMDAB http://localhost:5001/


   SSLEngine on
   Header edit Set-Cookie ^(.*)$ $1;Secure
   SSLProtocol +TLSv1.2
   SSLCertificateFile /etc/ssl/certs/certyfikat_serwera.crt
   SSLCertificateKeyFile /etc/ssl/private/klucz_prywatny.key
   SSLCertificateChainFile /etc/ssl/certs/certyfikat_posredni.crt
  . . .
```

Uwaga: Należy zwrócić uwagę na numer portu. Domyślnie SSL wykorzystuje port 443.

Akceptowane protokoły są definiowane w „SSLProtocol”. Alternatywnie można zezwolić na wszystkie protokoły:

```
SSLProtocol all
```

5. Zrestartować serwer Apache:

```
sudo service apache2 restart
```

6. Na stronie http://httpd.apache.org/docs/current/mod/mod_ssl.html znajdują się wskazówki dotyczącej zaawansowanej konfiguracji SSL.

4.9.3. Konfiguracja uwierzytelniania certyfikatem TLS

Uwaga: Konfiguracja uwierzytelnieniem certyfikatem jest dodatkowa (opcjonalna) i wymaga podstawowej wiedzy z zakresu konfiguracji serwera WWW.

Konfiguracja polega na wgraniu do aplikacji mMedica certyfikatu, który będzie wykorzystywany do komunikacji z Archiwum. Aplikacja Archiwum musi zostać skonfigurowana do przyjmowania komunikacji HTTPS oraz akceptowania przesyłanego przez mMedica certyfikatu. W takim przypadku Archiwum może dodatkowo uwierzytelniać ruch pochodzący z mMedica (oraz pośrednio z Portalu eRejestracja), a komunikacja po HTTPS pozwala na szyfrowanie ruchu. Do konfiguracji można wykorzystać certyfikaty wydane przez zaufanego dostawcę lub własnoręcznie wygenerowane. Warunkiem koniecznym jest, aby klucz publiczny miał możliwość użycia jako uwierzytelnienie klienta oraz serwera.

W celu skonfigurowania dodatkowego uwierzytelniania komunikacji za pomocą certyfikatu TLS dla Archiwum wymagane jest rozbudowanie konfiguracji serwera np. Apache.

4.9.3.1. Dodawanie certyfikatu

Do działania komunikacji TLS wymagane jest dodanie certyfikatu TLS. W tym dziale zostanie opisany sposób przygotowania certyfikatów, które w kolejnym kroku zostaną wykorzystane w konfiguracji serwera.

1. Posiadany certyfikat TLS należy umieścić np. w katalogu „/etc/ssl/certs/nazwa_certyfikatu”.
2. Jeżeli posiadany jest pojedynczy plik certyfikatu np. o rozszerzeniu „.p12” zawierający również certyfikaty nadrzędne należy je rozdzielić na osobne pliki.

Uwaga: Serwer Apache nie przyjmuje certyfikatów o rozszerzeniu „.p12” i konieczne jest przekonwertowanie pliku na format „pem”. Proces konwertowania rozszerzenia zostanie opisany poniżej.

3. W celu wydzielenia certyfikatu do komunikacji TLS należy użyć komendy:

```
sudo openssl pkcs12 -in nazwa_certyfikatu.p12 -out nazwa_certyfikatu_tls.pem -nodes -
clcerts
```

4. W celu wydzielenia łańcucha certyfikatów nadrzędnych można użyć komendy:

```
sudo openssl pkcs12 -in nazwa_certyfikatu.p12 -out nazwa_certyfikatu_chain_tls.crt -
nokey -cacerts
```

4.9.3.2. Konfiguracja serwera

W niniejszym rozdziale opisana zostanie konfiguracja, w której Archiwum zostanie uruchomiony na osobnym porcie.

1. W celu skonfigurowania komunikacji TLS należy utworzyć nowy plik konfiguracyjny apache.

```
sudo nano /etc/apache2/sites-available/Archiwum.conf
```

2. Skonfigurować utworzony plik /etc/apache2/sites-aviable/Archiwum.conf

```
<VirtualHost *:443>
ServerName localhost
   ProxyPreserveHost On
   ProxyPass / http://localhost:5003/
   ProxyPassReverse / http://localhost:5003/

  SSLEngine on

  Header edit Set-Cookie ^(.*)$ $1;Secure

  SSLProtocol +TLSv1.2

  SSLCertificateFile /etc/ssl/certs/nazwa_certyfikatu_tls.pem


  RequestHeader set X-Forwarded-Proto https


  SSLCACertificateFile /etc/ssl/certs/nazwa_certyfikatu_chain_tls.crt

  SSLOptions +ExportCertData

  SSLVerifyClient optional

  SSLVerifyDepth 3

  RequestHeader set SSL_CLIENT_CERT "%{SSL_CLIENT_CERT}e"

  . . .
```

Uwaga: Używany port musi być unikatowy w ramach serwera.

Powyższy plik konfiguracyjny (dla protokołu https) definiuje wykorzystanie domyślnego portu 443 do komunikacji oraz wskazuje aplikacje na jakie przekierowywany ma być ruch. Konfiguracja ta pozwala na przesłanie przez klienta certyfikatu TLS.

Parametr SSLVerifyClient pozwala na sterowanie zachowaniem, czy certyfikat przesłany w żądaniu do Archiwum jest wymagany i w jakim stopniu:

a) Ustawienie „optional” – pozwala na dostęp do części portalowej Archiwum bez przekazywania certyfikatu TLS. Dostęp do API dla mMedica oraz eRejestracji będzie wymagać przesłania certyfikatu TLS.

b) Ustawienie „require” – spowoduje, że aby dostać się do portalu aplikacji Archiwum konieczne będzie przekazanie certyfikatu TLS przez przeglądarkę. Dostęp do API dla mMedica oraz eRejestracji będzie wymagać przesłania certyfikatu TLS. Jeśli skonfigurowany certyfikat nie został wydany przez zaufanego dostawcę lub nie został wydany na domenę Archiwum wtedy należy się spodziewać ostrzeżenia w przeglądarce internetowej z informacją o nieprawidłowym certyfikacie.

Parametr SSLVerifyDepth uzależniony jest od liczby certyfikatów nadrzędnych w łańcuchu certyfikacji tzn. w pliku nazwa_certyfikatu_chain_tls.crt.

- Jeżeli łańcuch zawiera tylko certyfikat nadrzędny parametr powinien mieć wartość: 2.
- Jeżeli łańcuch certyfikacji zawiera certyfikat główny oraz certyfikat pośredni to parametr powinien mieć wartość: 3.
- Jeżeli łańcuch certyfikacji zawiera certyfikat główny oraz dwa certyfikat pośrednie to parametr powinien mieć wartość: 4.
- Itd.

Apache pełni tu rolę serwera pośredniczącego, dlatego konieczne jest zezwolenie serwerowi na tego typu operacje:

```
sudo a2enmod ssl
sudo a2enmod proxy
sudo a2enmod proxy_balancer
sudo a2enmod proxy_http
sudo a2enmod headers
```

W przypadku wykorzystania innego portu niż 443 konieczne jest dodanie portu do listy portów nasłuchiwanych w pliku /etc/apache2/ports.conf.

3. Udostępnić nowo utworzoną witrynę komendą:

```
sudo a2ensite Archiwum.conf
```

4. Zrestartować serwer Apache:

```
sudo service apach2 restart
```

W przypadku problemów z uruchomieniem apache ze względu na długość klucza certyfikatu konieczna jest zmiana domyślnej konfiguracji SSL. Powód błędnego uruchamiania usługi apache można sprawdzić poprzez wylistowanie pliku błędów komendą:

```
cat /var/log/apache2/error.log
```

Jeżeli w pliku na końcu znajduje się podobny wpis „SSL Library Error: error:140AB18F:SSL routines:SSL_CTX_use_certificate:ee key too small” oznacza to, że konieczna jest edycja pliku /etc/ssl/openssl.cnf. Dopisując wskazane fragmenty na początku oraz na końcu pliku.

```
# This definition stops the following lines choking if HOME isn't
# defined.
HOME                    = .

# Extra OBJECT IDENTIFIER info:
#oid_file               = $ENV::HOME/.oid
oid_section             = new_oids
#Poczatek
```

```
#System default
openssl_conf = default_conf
. . .
#Koniec
[ default_conf ]
ssl_conf = ssl_sect
[ssl_sect]
system_default = system_default_sect

[system_default_sect]
MinProtocol = TLSv1.2
CipherString = DEFAULT:@SECLEVEL=1
```

4.9.3.3. Konfiguracja Archiwum oraz mMedica

Konfiguracja Archiwum została opisana w dziale *3.13.3.3. Konfiguracja Archiwum oraz mMedica.*

4.9.4. Zaawansowana konfiguracja witryn

Możliwe jest dodawanie nowych witryn do usługi Apache. Na poziomie witryny konfigurowany jest m.in. port komunikacji, adres domenowy, alias, certyfikat SSL, zakres IP z jakiego jest widoczna witryna. Możliwe jest działanie wielu witryn na tym samym porcie komunikacji. Pojedyncza witryna jest definiowana w pliku o rozszerzeniach „conf" w ścieżce /etc/apache2/sites-available/.

Przykładowa zawartość dla pliku s1.conf:

```
<VirtualHost *:80>
  ServerName www.ar.domena.pl
  ServerAlias ar.domena.pl
  ProxyPreserveHost On
  ProxyPass /Archiwum http://localhost:5003/
  ProxyPassReverse /Archiwum http://localhost:5003/
</VirtualHost>
```

Powyższa konfiguracja posiada przypisany adres domenowy www.ar.domena.pl oraz alias.

Przykładowa zawartość plik s2.conf:

```
<VirtualHost 10.10.10.2:1099>
  ServerName 10.10.10.2
  <Location /Archwium>
    Deny from all
    Allow from 10.10.10.1/24
    ProxyPass http://localhost:5003/
    ProxyPassReverse http://localhost:5003/
  </Location>
</VirtualHost>
```

W pliku s2.conf witryna jest przypisana do adresu 10.10.10.2 i tylko pod takim będzie widoczna. Z kolei „Allow from” pozwala zdefiniować zakres adresów IP, z których jest widoczna strona. Domyślnie ma on wartość „all” oznaczającą brak ograniczeń.

Po utworzeniu pliku z konfiguracją witryny w ścieżce /etc/apache2/sites-available/, należy wykonać polecenie:

```
sudo a2ensite NAZWA_PLIKU_KONFIGURACJI.conf
```

Przykład:

```
sudo a2ensite s1.conf
```

Następnie należy przeładować konfigurację usługi Apache:

```
sudo service apache2 reload
```

4.10. Doinstalowanie komponentów

Instalacja nowych komponentów polega na:

1. Skopiowaniu nowych plików komponentu do pożądanej ścieżki.
2. Dodaniu bazy danych za pomocą instalatora. W przypadku pierwszego użycia instalatora należy dodać bazę danych zgodnie z *4.3. Instalacja bazy danych Archiwum*. W przypadku, w którym użyto już wcześniej instalatora do instalacji bazy danych lub dowolnego komponentu, należy przeprowadzić proces dodawania nowej bazy zgodnie z punktem *5.1. Konfiguracja połączenia z bazami danych*.
3. Skonfigurowaniu połączenia do bazy danych.
4. Skonfigurowaniu nazw aplikacji (*4.6. Konfiguracja nazwy aplikacji*).
5. Skonfigurowaniu adresów aplikacji (*4.7. Konfiguracja adresu aplikacji*).
6. Konfiguracji serwera oraz instalacji modułu (*4.5. Konfiguracja serwera oraz instalacja modułu*).
7. Weryfikacji instalacji (*4.8. Weryfikacja instalacji*).
8. Konfiguracji dodatkowej serwera WWW (*4.9. Konfiguracja dodatkowa Apache*).

4.11. Konfiguracja wielu Archiwum lub mMDAB na jednym serwerze

W przypadku, kiedy na jednym serwerze Apache udostępniony jest więcej niż jeden moduł Archiwum lub mMDAB, należy poczynić dodatkowe kroki konfiguracyjne. Utworzyć dla każdego z komponentów osobny katalog, w którym znajdować się będą pliki aplikacji. Wymagana jest zmiana portu, na którym dana aplikacja będzie udostępniona, dlatego należy w pliku appsettings.json każdej aplikacji zmienić adres aplikacji.

Uwaga: Ważne, aby każda z instancji Archiwum oraz mMDAB miała unikalny atrybut „ApplicationUrl” oraz „ApplicationName” w ramach jednego serwera www.

Konieczne jest ponowne dokonanie kroków opisanych w punkcie *4.5. Konfiguracja serwera oraz instalacja modułu*.

4.12. Restartowanie i zatrzymywanie komponentów

Komponenty zawierają wewnętrzną pamięć podręczną i może istnieć potrzeba jej wyczyszczenia za pomocą zrestartowania komponentu. Takim przypadkiem, w którym należy zrestartować komponent jest odtworzenie kopii zapasowej bazy danych. Możliwe jest zrestartowanie komponentów w następujący sposób:

1. Przykład dla Archiwum:
   a) Wyłączyć usługę Archiwum w serwisach:

```
sudo systemctl stop mMedica.Archiwum.service
```

   b) Uruchomić usługę ponownie po odczekaniu około 1 min. wykorzystując polecenie:

```
sudo systemctl start mMedica.Archiwum.service
```

2. Przykład dla mMDAB:
   a) Wyłączyć usługę mMDAB w serwisach:

```
sudo systemctl stop mMedica.mMDAB.service
```

   b) Uruchomić usługę ponownie po odczekaniu około 1 min. wykorzystując polecenie:

```
sudo systemctl start mMedica.mMDAB.service
```

4.13. Aktualizacja modułu

Należy podmienić wszystkie pliki komponentu oraz przenieść ustawienia z wcześniej skonfigurowanego pliku appsettings.json do nowych. Nie zaleca się podmiany plików na wcześniej skonfigurowane, gdyż struktura pliku konfiguracyjnego może ulegać zmianie.

Dla każdego z powyższych sposobów instalacji instalator aktualizuje wszystkie dostępne na serwerze bazy danych Archiwum oraz (jeśli występują) bazy modułu eRejestracja. Zaleca się tworzenie kopii bazy danych przed wykonaniem aktualizacji modułu.

Proces aktualizacji powinien być wykonywany na zatrzymanych komponentach modułów w dystrybucjach Linux. Po aktualizacji należy uruchomić ponownie komponent w systemie. Do aktualizacji komponentów należy posłużyć się opisem znajdujących się w rozdziale *4.12. Restartowanie i zatrzymywanie komponentów.*

4.14. Pomoc

W razie problemów można skorzystać z pomocy pod następującymi adresami internetowymi:

1. http://httpd.apache.org/docs/
2. http://httpd.apache.org/docs/current/mod/mod_ssl.html
3. https://docs.microsoft.com/en-us/dotnet/core/linux-prerequisites?tabs=netcore1x
4. https://docs.microsoft.com/en-us/aspnet/core/publishing/apache-proxy

5. Konfiguracja aplikacji

Uwaga: Proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja.

5.1. Konfiguracja połączenia z bazami danych

W przypadku instalacji manualnej w systemach operacyjnych Microsoft Windows, dystrybucjach systemów opartych o jądro Linux oraz w przypadku doinstalowania komponentów konieczna jest konfiguracja połączenia z bazami danych w komponentach. Możliwa jest również edycja parametrów połączeń, które zostały utworzone przez instalator. Każdy z komponentów posiada plik appsettings.json, w którym znajdują się parametry połączenia z bazą danych (adres serwera bazy danych, port oraz nazwa bazy danych).
Konfiguracja połączenia z bazą danych wygląda następująco:

1. Otworzyć plik appsettings.json z prawami administratora do edycji.
2. Wyszukać fragment (identyczny lub podobny) dla:

```
"ConnectionString": "Server=localhost,5432;Database=ARCHMMEDICA;"
```

3. Zmienić według wzoru: „Server=localhost,5432;Database=NAZWA_BAZY" – baza danych o nazwie NAZWA_BAZY znajduje się na komputerze, na którym działa komponent (localhost) na porcie 5432. W przypadku innej nazwy bazy danych należy zmienić właściwość „Database" na odpowiednią. Dla innego adresu, na którym znajduje się baza, należy zmienić parametr Server.

Zapisać plik i zrestartować komponent zgodnie z *3.15. Restartowanie i zatrzymywanie komponentów* (Windows) lub *4.12. Restartowanie i zatrzymywanie komponentów* (Linux).

5.2. Zabezpieczenie przed użyciem IFRAME

Atak na strony internetowe typu clickjacking polega na przechwyceniu kliknięć nieświadomego użytkownika na spreparowanej stronie internetowej, a następnie wykonanie określonych operacji na innej stronie internetowej, uwierzytelniając ją danymi użytkownika. Metoda wykorzystuje element języka HTML o nazwie IFRAME (ramka) poprzez zagnieżdżenia na stronie spreparowanej zawartości strony, do której mają zostać przekierowane akcje. W celu zabezpieczenia się przez atakiem tego typu, należy w pliku appsettings.json (znajdującym się w katalogu Archiwum) umieścić następujący jeden z poniższych wpisów:

a) Portal Archiwum może być wyświetlany w IFRAME tylko jeżeli pochodzi z tego samego miejsca, co strona zagnieżdżająca:

```
"AllowShowPortalInIframe": true,
```

```
"AllowShowPortalInIframeOnlyFromURL": ""
```

b) Żadna strona nie może wyświetlać strony Archiwum w ramce:

```
"AllowShowPortalInIframe": false,
"AllowShowPortalInIframeOnlyFromURL": ""
```

c) Strona Archiwum może być wyświetlana w ramce jeżeli strona zagnieżdżająca pochodzi z podanego adresu:

```
"AllowShowPortalInIframe": true,
"AllowShowPortalInIframeOnlyFromURL": "ADRES"
```

UWAGA: Przykładowy plik appsettings.json zawiera konfigurację typu DENY.

5.3. Konfiguracja nazwy oraz adresu aplikacji

Konfiguracja ta została opisana osobno dla systemu Windows (w rozdziale *3.11 Konfiguracja nazwy aplikacji*) oraz Linux (w rozdziałach *4.6 Konfiguracja nazwy aplikacji* oraz *4.7 Konfiguracja adresu aplikacji*).

5.4. Przekierowanie nagłówków z proxy

W przypadku, w którym komponent Archiwum lub mMDAB zainstalowany jest na IIS (system rodziny Windows) dostępny jest poprzez proxy lub reverse-proxy, należy odpowiednio skonfigurować plik appsettings.json. Uruchomienie obsługi proxy polega na edycji sekcji w pliku appsettings.json danego komponentu poprzez zmianę wartości klucza *ProxyWindowsEnable*:

Ustawienie domyślne (proxy wyłączone):

```
"ProxyWindowsEnable": false
```

Włączona obsługa proxy:

```
"ProxyWindowsEnable": true
```

Mechanizm automatycznie obsługuje proxy, które jest uruchomione na tym samym systemie co komponent (adres lokalny). Jeśli proxy znajduje się pod innym adresem niż adres lokalny, należy jego adres IP wpisać w kluczu *ProxyIPs* (w przypadku wielu proxy należy wpisać adresy po średniku), przykład:

```
"ProxyIPs": "192.168.137.1;192.168.137.2;192.168.137.3"
```

Na środowisku opartym o jądro Linux ruch do komponentów przekierowywany z Apache do odpowiednich usług komponentów. Jednak Archiwum oraz mMDAB automatycznie obsługują odpowiednie nagłówki z proxy dla Linux. Podobnie jak w przypadku komponentów zainstalowanych w systemie Windows, o ile proxy

jest na adresie lokalnym, nie wymaga on dodatkowej konfiguracji. W innym przypadku konfiguracja odbywa się na takich samych zasadach jak dla instalacji pod Windows (edycja klucza *ProxyIPs*).

Do prawidłowego działania mechanizmu przekazywania nagłówków http z proxy konieczne jest, aby proxy obsługiwało nagłówek HTTP X-Forwarded-For, w którym przekazywany jest oryginalny adres IP pochodzący z żądania.

Brak odpowiedniej konfiguracji proxy będzie skutkowało odczytem nieprawidłowych adresów IP z żądań, co z kolei może spowodować nieprawidłowe działanie mechanizmu blokad IP podczas logowania w Portalu oraz mechanizmie blokad dostępowych do komponentów.

5.5. Uruchamianie wielu modułów wewnętrznych tego samego typu przez mMDAB

Komponent mMDAB daje możliwość uruchamiania wielu modułów wewnętrznych tego samego typu, tzn. możliwe jest uruchomienie np. trzech modułów MIAM. W celu uruchomienia wielu modułów wewnętrznych przez mMDAB konieczne jest umieszczanie kolejnych jego instancji w osobnych folderach o nazwach według następującego wzorca: typModułu_dodatkowaNazwa. Jeżeli chodzi o typ modułu to musi być on dokładnie taki sam jak rodzaj modułu, który będzie uruchamiany np. MIAM. Dodatkowa nazwa pozwala identyfikować moduł wewnętrzny, przykładem może być nazwa Test. Ważne jest to, aby typ modułu odseparować od nazwy dodatkowej separatorem jakim jest „_”. Jest to konieczne w celu prawidłowego działania aplikacji. Dodatkowym obostrzeniem jest, aby nazwa folderu nie zawierała żadnego dodatkowego znaku specjalnego poza pojedynczym znakiem separującym wspomnianym wcześniej. Każdy z modułów MIAM powinien zostać skonfigurowany poprzez plik appsettings.json znajdującym się w folderze każdego modułu w celu poprawnego łączenia się z bazą danych mMedica.

Przykładowa konfiguracja dla modułów wewnętrznych typu MIAM:

1. Utworzyć wewnątrz katalogu „modules” komponentu MIAM dwa foldery o nazwie MIAM_Test oraz MIAM_Test2.
2. Umieścić pliki aplikacji MIAM wewnątrz tych folderów.
3. Uruchomić aplikację zgodnie z wersją wykorzystywanego systemu Windows (*3.15. Restartowanie i zatrzymywanie komponentów* (Windows) oraz *4.12. Restartowanie i zatrzymywanie komponentów* (Linux).

Po uruchomieniu moduły będą dostępne pod adresami http://adresmMDAB/MIAM_Test oraz http://adresmMDAB/MIAM_Test2

5.6. Konfiguracja maksymalnego rozmiaru żądania

Moduł Archiwum umożliwia konfiguracje maksymalnego rozmiaru żądania przesyłanego do aplikacji. Konfiguracji dokonuje się poprzez dopisanie do pliku appsettings.json sekcji MaxContentLength. Nowa sekcja od poprzednich musi być oddzielona przecinkiem.

Ustawienie domyślne to 30 MB:

```
"MaxContentLength": 31457380
```

Maksymalna dopuszczalna wartość konfiguracji wynosi 1GB

```
"MaxContentLength": 1073741824
```

W celu wyznaczenia wartości wystarczy przemnożyć oczekiwaną wartość w MB przez odpowiednie wagi.
Dla przykładu: w celu wyznaczenia wartości dla 60 MB wystarczy pomnożyć 60 x 1024 x 1024 = 62 914 560.

6. Zarządzanie oraz kopie zapasowe baz danych

Uwaga: Proces zarządzania bazami danych jest taki sam jak w przypadku modułu eRejestracja.

6.1. Kopie bazy danych

Wykonywanie kopii baz danych eRejestracji oraz Archiwum jak i ich odtwarzanie możliwe jest za pomocą aplikacji mMBackup.exe, która jest częścią składową oprogramowania mMedica. Podobnie jak w przypadku wykonywania kopii bazy danych mMedica, stan bazy danych jest zapisywany do pliku o rozszerzeniu ZIP, który w nazwie zawiera informacje o dacie, godzinie i nazwie bazy danych.

6.1.1. Wykonywanie kopii bazy danych

Aby wykonać kopię bazy należy z poziomu wiersza poleceń systemu Windows (Menu Start\Uruchom – skrót: klawisz Windows + r, następnie wpisać „cmd” i zatwierdzić) wpisać:

```
„[Ścieżka do mMedica]\mmBackup.exe” [Nazwa bazy danych Archiwum] backup
```

Przykład wykonywania kopii dla domyślnej ścieżki instalacji i bazy danych o nazwie „ARCHMMEDICA”:

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ARCHMMEDICA backup
```

Następnie w oknie podać miejsce zapisu kopii bazy danych oraz nazwę użytkownika z uprawnieniami administratora w Portalu (domyślnie „admin”), hasło oraz nacisnąć przycisk „Start”.

6.1.2. Odtwarzanie bazy danych

Odtworzenie kopii bazy danych wygląda w bardzo zbliżony sposób. Również z poziomu wiersza poleceń należy wpisać:

```
„[Ścieżka do mMedica]\mmBackup.exe” [Baza danych Archiwum] restore
```

Przykład odtwarzania kopii dla domyślnej ścieżki instalacji i bazy danych o nazwie „ARCHMMEDICA”:

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ARCHMMEDICA restore
```

W oknie należy wybrać ścieżkę do pliku kopii bazy danych i nacisnąć przycisk „Start” (nie jest wymagane ponowne podawanie nazwy użytkownika oraz hasła). W oknie odzyskiwania danych można również zmienić adres serwera bazy danych oraz odczytać wersję bazy danych. Kopia bazy danych może zostać odtworzona pod inną nazwą niż pierwotna.

6.1.3. Operacje na zdalnym serwerze PostgreSQL

Wykonywanie kopii lub odtwarzanie bazy danych na zdalnym serwerze PostgreSQL wymaga dodatkowej konfiguracji. W tym celu należy:

1. Otworzyć do edycji plik DBXCONNECTIONS.INI znajdujący się w katalogu programu mMedica.
2. Dodać lub zmienić wpisy według poniższego wzoru:

```
[ARCHMMEDICA_LNX]
DriverName=PostgreSQL
Database=10.3.4.138:5432/ARCHMMEDICA
```

   „[ARCHMMEDICA_LNX]" oznacza alias jaki będzie podawany w poleceniu mMBackup.exe.

   W „Database" określa się kolejno adres IP oraz port nasłuchu serwera PostgreSQL, a po ukośniku nazwę bazy danych modułu.

3. Zapisać plik.
4. Wykonać polecenie wykonania lub odtworzenia kopii, dla powyższego przykładu:
   a. Wykonanie kopii bazy danych „ARCHMMEDICA_LNX":

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ARCHMMEDICA_LNX
backup
```

   b. Odtworzenie kopii bazy danych „ARCHMMEDICA_LNX":

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ARCHMMEDICA_LNX re-
store
```

Istnieje również możliwość utworzenia nowej bazy danych na podstawie istniejącej kopii (odtworzenie bazy pod inną nazwą) na zdalnym serwerze. Aby dokonać takiej operacji należy:

1. Wykonać polecenie odtwarzania kopii bazy danych „ARCHMMEDICA_LNX:

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ARCHMMEDICA2_LNX restore
```

   „ARCHMMEDICA2_LNX" będzie nazwą dla nowej bazy danych.

2. W oknie programu mMBackup w polu serwer należy podać adres IP zdalnego serwera PostgreSQL.

Uwaga: Serwer PostgreSQL musi zezwalać na zdalną komunikację, a oprogramowanie typu firewall musi zezwalać na komunikacje na wybranym porcie.

6.1.4. Uproszczenie wykonywania kopii

Możliwe jest również utworzenie skrótu do mMBackup.exe, który będzie wykonywał kopię lub odzyskiwanie bazy danych. W tym celu należy wejść do katalogu domyślnej instalacji oprogramowania mMedica

(domyślnie: C:\Program Files\Asseco\mMedica lub C:\Pliki programów (x86)\Asseco\mMedica), zaznaczyć prawym przyciskiem myszy plik mMBackup.exe i wybrać pozycję „Utwórz skrót”, a następnie umieścić go w żądanym miejscu. Następnie kliknąć prawym przyciskiem myszy na skrót, wybrać opcję „Właściwości” i zmodyfikować pole „Element docelowy” tak, aby zawierało ono polecenie „backup” lub „restore” dla wybranej bazy danych:

```
"c:\Program Files (x86)\ASSECO\mMedica\mmBackup.exe" ARCHMMEDICA restore
```

7. Bezpieczeństwo modułu

Uwaga: Proces zarządzania bazami danych jest taki sam jak w przypadku modułu eRejestracja.

Rozdział opisuje jedynie najczęściej stosowane praktyki zapewnienia bezpieczeństwa informacji. Ostateczna decyzja dotycząca wprowadzenia zabezpieczeń należy do administratora. Ponadto obowiązkiem administratora jest aktualizacja zabezpieczeń zgodnie z powstającymi nowymi standardami bezpieczeństwa oraz zmianami w obowiązującym prawie.

7.1. Infrastruktura

7.1.1. Zewnętrzny hosting lub VPS

Moduł Archiwum może być instalowany zarówno we własnej infrastrukturze jak i za pośrednictwem usług firm zewnętrznych (hosting lub VPS). VPS, czyli wirtualny, prywatny serwer dający więcej możliwości konfiguracyjnych. Pozwala on na zarządzanie takie jak na zwykłym komputerze. Rekomenduje się, aby moduł Archiwum (szczególnie w przypadku jednostanowiskowej infrastruktury) nie był zainstalowany na komputerze przeznaczonym do zadań użytkowych, np. pracy biurowej. Minimalizuje to ryzyko związane z ingerencją złośliwego oprogramowania, spadkiem wydajności komputera czy połączeniem sieciowym.

7.1.2. Protokół SSL

Wysoce zalecane jest stosowanie protokołu SSL, który zapewnia szyfrowanie transmitowanych danych. Dzięki temu, jeśli przesyłane dane zostaną przechwycone, nie zostaną odczytane ani zmodyfikowane. Dla pełnego bezpieczeństwa protokół powinien zostać użyty dla wszystkich elementów modułu Archiwum.

Protokół będzie spełniał swoją rolę wyłącznie, gdy wszędzie będą używane adresy internetowe wykorzystujące ten protokół. Z tego powodu nie zaleca się ustawienia podwójnego protokołu dostępu HTTP oraz HTTPS na serwerach WWW. Sposób konfiguracji SSL powinien zostać dostarczony przez dostawcę certyfikatu.

W przypadku zastosowania protokołu SSL dla Archiwum, użytkownicy będą informowani przez przeglądarkę internetową o istnieniu bezpiecznego połączenia ze stroną, co pozwala użytkownikowi na wykrycie przypadku phishingu, czyli podmiany strony na łudząco podobną, służącą do wyłudzenia danych osobowych lub autoryzacyjnych. Dodatkowo protokołu SSL szyfruje transmisję dla interfejsów przeznaczonych dla aplikacji mMedica oraz Informacje Medyczne.

7.1.3. VPN

W przypadku, w którym architektura modułu Archiwum, aplikacji mMedica oraz baz danych jest rozproszona, warto rozważyć zastosowanie tunelu VPN pomiędzy poszczególnymi elementami. Zastosowanie VPN pozwala na utworzenie prywatnej, wirtualnej sieci o ograniczonym dostępnie.

7.2. Oprogramowanie

7.2.1. Konta użytkowników

Komputer, na którym zainstalowany jest moduł Archiwum, powinien posiadać aktualny system operacyjny oraz aktualne oprogramowanie wspierające bezpieczeństwo (np. oprogramowanie antywirusowe).

Dostęp do systemu operacyjnego powinien być zabezpieczony hasłem poprzez indywidualne konto dla każdego użytkownika systemu. Ponadto hasło powinno podlegać przymusowej zmianie co ściśle określony interwał czasu.

Należy również rozważnie konfigurować oraz korzystać z usług zdalnych połączeń do komputera (usługi typu RDP). W celu zwiększenia stopnia bezpieczeństwa poleca się stosowanie szyfrowanych nośników do przechowywania baz danych Archiwum.

7.2.2. Oprogramowanie antywirusowe

Dodatkowo zaleca się stosowanie ochrony antywirusowej wraz z aktualną bazą definicji szkodliwego oprogramowania. Ochrona antywirusowa powinna mieć skonfigurowane okresowe skanowanie systemu oraz włączoną ochronę w czasie rzeczywistym.

7.2.3. Firewall

Kolejnym ważnym aspektem jest instalacja i konfiguracja zapory ogniowej (firewall). Zapora powinna zezwalać wyłącznie na ruch usług, które są świadomie uruchomione na komputerze. W przypadku modułu Archiwum wymaga się odblokowania portu HTTP (80) lub/oraz HTTPS (443), lub innych w zależności od konfiguracji serwera WWW, portu do serwera bazy danych (jeżeli jest to wymagane, domyślnie 5432), a także portu do komunikacji z serwerem poczty wychodzącej.

Przy konfiguracji zapory ogniowej rekomenduje się stosowanie podejścia, w którym punktem wyjścia jest blokada komunikacji, a następnie świadome dodawanie pojedynczych reguł zezwalających dla komunikacje dla usług, aplikacji oraz na numerach portów. Takie podejście jest zalecane wyłącznie osobom posiadającym

wiedzę techniczną, gdyż istnieje ryzyko zablokowania komunikacji, która jest wymagana do prawidłowego i bezpiecznego działania systemu operacyjnego oraz zainstalowanych aplikacji, czy usług.

7.2.4. Nieużywane protokoły TCP IP oraz protokoły serwera WWW

Zaleca się wyłącznie na serwerze obsługi protokołów TCP, której nie są używane (np. IPv6). Brak takich działań może skutkować negatywnie m.in. w przypadku, w którym administrator zapomni o odpowiednim skonfigurowaniu zapory ogniowej dla nieużywanego protokołu lub w aplikacji serwera WWW (IIS, Apache).
Instrukcja wyłączenia IPv6 dla Windows:

1. Przejść do „Panelu Sterowania".
2. Uruchomić „Centrum sieci i udostępniania".
3. Wybrać „Zmień ustawienia karty sieciowej".
4. Kliknąć prawym przyciskiem myszy i wybrać z menu kontekstowej „Właściwości" po kolei na każda z aktywnych kart (fizyczne oraz wirtualne), które komunikują się z siecią.
5. Odznaczyć w oknie „Internet Protocol Version 6 (TCP/IPv6)".
6. Zapisać zmiany.

Serwery WWW (IIS, Apache) również powinny zostać skonfigurowane tak, aby udostępniać wyłącznie aktywne protokoły komunikacji (np.: http, https, ftp) i to wyłącznie na aktywnych protokołach TCP (IPv4, IPv6).
Instrukcja wyłączania protokołów dla IIS:

1. Uruchomić IIS.
2. W menu „Połączenia" prawym przyciskiem myszy uruchomić menu kontekstowe witryny, której ustawienia należy zmienić (np. Default Web Site).
3. Z menu kontekstowego wybrać opcję „Edytuj powiązania…".
4. W oknie powiązań zostaną wyświetlone wszystkie uruchomione protokoły komunikacji aplikacji (typy) oraz przypisane adresy IP (symbol * oznacza wszystkie adresy), które wynikają z aktywnych protokołów TCP.
5. Za pomocą opcji „Edytuj…" można zmienić już istniejące w tabeli wpisy. Wpisy można również dodać lub usunąć za pomoc przycisków kolejno „Dodaj…" oraz „Usuń".
6. Po wprowadzeniu zmian okno „Powiązania witryny" można zamknąć za pomocą przycisku „Zamknij".

7.3. Konfiguracja modułu

Po zainstalowaniu modułu zaleca się zmianę hasła domyślnego dla administratora Archiwum. Dodatkowo należy pamiętać o zmianie hasła usług sieciowych, które zapewnia bezpieczną komunikacje z programem mMedica.

Dobrą praktyką jest utworzenie dodatkowego konta administratora, które umożliwi dostęp do Portalu Archiwum w przypadku zablokowania lub utracenia hasła do konta domyślnego.

W konfiguracji wielostanowiskowej zaleca się wprowadzenie ograniczenia na adresy IP, które mogą łączyć się z serwerem bazy danych. W katalogu „data" w ścieżce instalacji bazy danych znajduje się plik pg_hba.conf, który pozwala na podanie zakresu adresów IP lub konkretnego adresu IP (dotyczy to również adresów VPN). Pełną specyfikację konfiguracji dostępu do bazy danych można odnaleźć na stronie producenta bazy danych PostgreSQL.

7.4. Zabezpieczenia modułu

7.4.1. Token bezpieczeństwa

Komunikacja pomiędzy poszczególnymi modułem Archiwum a aplikacją jest autoryzowana przy udziale hasła usług sieciowych, na podstawie którego powstaje token bezpieczeństwa. Nie jest więc możliwe połączenie Archiwum z mMedica bez wspólnego hasła usług sieciowych.

7.4.2. Blokowanie adresów IP oraz kont

Portal Archiwum zawiera mechanizm blokowania adresów IP komputerów, z których dochodzi do wielokrotnej nieudanej próby logowania na nieistniejącego użytkownika. W przypadku, w którym dochodzi do nagminnej próby nieprawidłowego logowania na istniejące konto następuje jego blokada. Administrator ma możliwość usunięcia adresu IP oraz odblokowania użytkownika. Powyższe funkcjonalności mają za zadanie ograniczać możliwość logowania do Portalu za pomocą używania metod siłowych (brute force).

7.4.3. Inne

Archiwum posiada mechanizm zbierania informacji o błędach oraz o ewentualnych próbach włamań do dziennika systemowego umieszczonego w Portalu. Dziennik systemowy umożliwia administratorowi eksport wpisów z dziennika systemowego do zaszyfrowanego pliku, który może zostać wysłany do analizy Serwisu mMedica.

Dostęp do bazy danych Archiwum jest zabezpieczony przed możliwością bezpośredniej (z pominięciem oprogramowania mMedica) ingerencji w bazę danych.

7.5. Filtrowanie komunikacji z wybranymi adresami IP

Dla każdego z komponentów możliwe jest poprzez plik konfiguracyjny appsettings.json ustawienie filtrowania komunikacji z wybranymi adresami IP. Dostępne są dwa tryby pracy:

- W pierwszym dostęp do zasobów strony jest odmawiany wszystkim użytkownikom o wskazanych adresach.
- W drugim dostęp do zasobów jest udostępniony jedynie użytkownikom o wskazanym adresie IP.

Proces konfiguracji filtrowania komunikacji z wybranymi adresami IP wygląda następująco:

1. Otworzyć plik appsettings.json z prawami administratora do edycji.
2. Wyszukać fragmenty (identyczne lub podobne) lub utworzyć następujące sekcje:

```
"IpFilteringOptionPortal": 0,
"SetOfIpAddressesPortal": "192.168.137.1;192.168.137.10-192.168.20"

"IpFilteringOptionAPI": 0,
"SetOfIpAddressesAPI": "192.168.137.1;192.168.137.10-192.168.20"

"IpFilteringOptionXDS": 0,
"SetOfIpAddressesXDS": "192.168.137.1;192.168.137.10-192.168.20"
```

Obszary filtrowania ruchu:

- „SetOfIpAddressesPortal” – dostęp do części portalowej aplikacji,
- „SetOfIpAddressesAPI” – dostęp do interfejsu wymiany informacji dla mMedica oraz eRejestracja.
- „SetOfIpAddressesXDS” – dostęp wymiany dokumentów dla interfejsu XDS (Informacje Medyczne).

Opis parametrów:

"IpFilteringOption…": 0 – parametr ten można ustawić na trzy sposoby. Ustawiając jego wartość na 0 wyłączone zostanie filtrowanie komunikacji. Wartość 1 spowoduje blokowanie komunikacji z adresami zdefiniowanymi w sekcji "*SetOfIpAddresses…*”. Z kolei ustawienie na wartość 2 pozwoli na dostęp do zasobów jedynie użytkownikom o wskazanych w sekcji "*SetOfIpAddresses…*” adresach IP.

"SetOfIpAddresses…": "192.168.137.1;192.168.137.10-192.168.20" – w sekcji tej podaje się adresy IP, które mają być brane pod uwagę. Adresy można podawać na dwa sposoby:

- Jako pojedyncze adresy 192.168.137.1,

- Jako pule adresów 192.168.137.10-192.168.20. Pule adresów należy odczytywać jako zakres adresów, np. pula 192.168.137.10-192.168.20 oznacza adresy 192.168.137.10, 192.168.137.11, 192.168.137.12 … aż do 192.168.137.20.

Kolejne pojedyncze adresy bądź pule adresów należy rozdzielać separatorem „;”.

3. Zrestartować moduł. W zależności od systemu odpowiednio Windows (*3.15 Restartowanie i zatrzymywanie komponentów*) lub Linux (*4.12 Restartowanie i zatrzymywanie komponentów*).

7.6. Integracja z modułem eKopia+

eArchiwum posiada integracje z modułem eKopia+ w zakresie wsparcia do dodatkowego szyfrowania kopii zapasowych bazy danych eArchiwum przez hasło nadal przez administratora.

7.7. Pozostałe zalecenia

Wszystkie używane hasła (np. do kont administracyjnych oraz usług sieciowych) powinny być silne, tj. rekomenduje się użycie haseł, które zawierają zarówno małe, jak i wielkie litery, cyfry oraz znaki specjalne. Hasło nie powinno również zawierać fraz słownikowych (np. imiona) i fraz związanych bezpośrednio z rodzajem prowadzanej działalności (np. nazwa świadczeniodawcy). Minimalna wymagana długość haseł:

a) hasło do konta: 12 znaków (dla kont administracyjnych zalecana jest minimalna długość 16 znaków),
b) hasło usług sieciowych: 20 znaków.

Lista osób mających dostęp do infrastruktury oraz użytkowników administracyjnych Archiwum powinna być ściśle określona, a konta dostępowe powinny być indywidualne.

Osoba odpowiedzialna za infrastrukturę i oprogramowanie powinna okresowo wykonywać sprawdzenia wydajności komputerów, zużycie łącza internetowego oraz przeprowadzać wykonywanie kopii bazy danych Archiwum. Kopie bazy danych Archiwum nie powinny być składowane na komputerze, na którym zainstalowany jest serwer bazy danych. Rekomenduje się stosowanie szyfrowanych nośników do przechowywania kopii baz danych. Stanowczo odradza się trzymanie kopii baz danych w katalogach serwerów WWW.

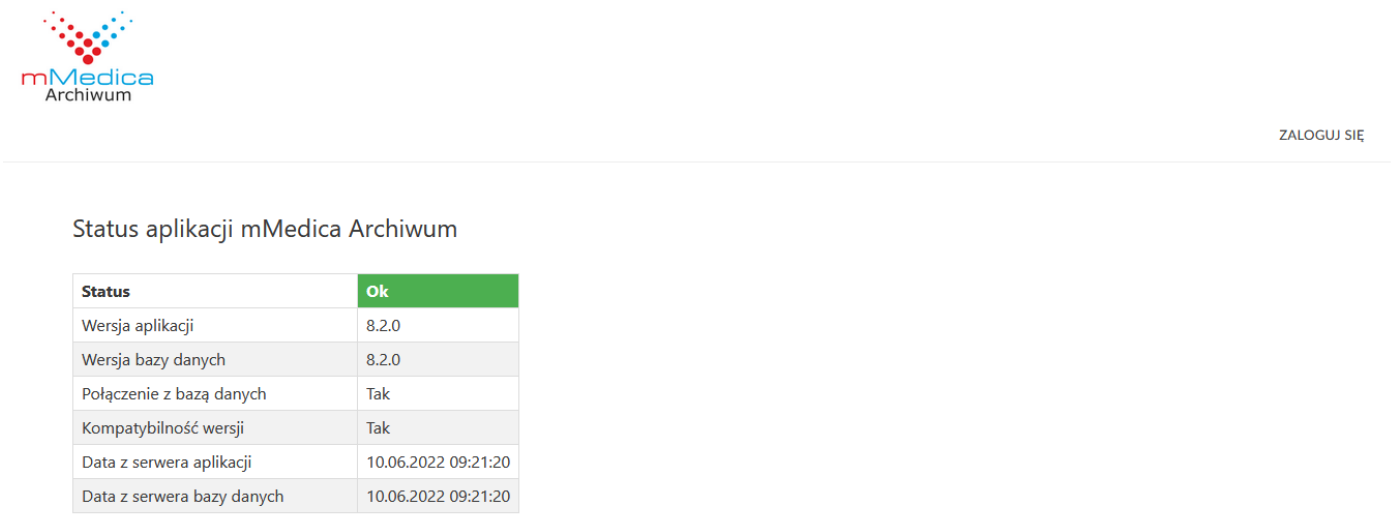
Wszelkie sytuacje, które mogą świadczyć o ingerencji osób nieupoważnionych w infrastrukturę (np. do serwera WWW) wymagają natychmiastowej reakcji. W takim przypadku należy niezwłocznie zmienić hasła dostępowe i (jeżeli to możliwe) dokonać rozłączenia połączonych użytkowników.

8. Konfiguracja Archiwum

8.1. Pierwsze uruchomienie

Uwaga: Należy się upewnić czy systemy operacyjne, na których jest zainstalowany moduł Archiwum oraz serwery baz danych mają ustawioną tą samą strefę czasową i możliwie maksymalnie zbliżoną datę oraz czas.

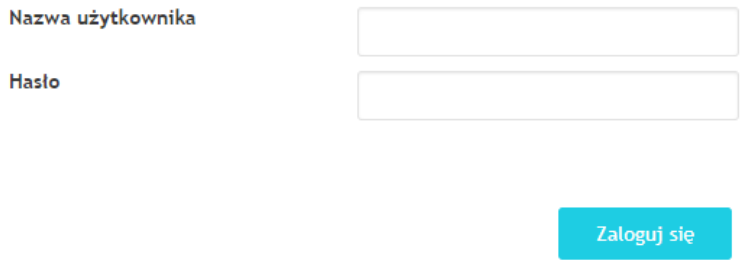
Po otworzeniu Portalu Archiwum w przeglądarce internetowej powinna zostać wyświetlona strona statusowa z możliwością zalogowania się podobnie jak na rysunku poniżej:



Rysunek 76: Strona główna Portalu Archiwum

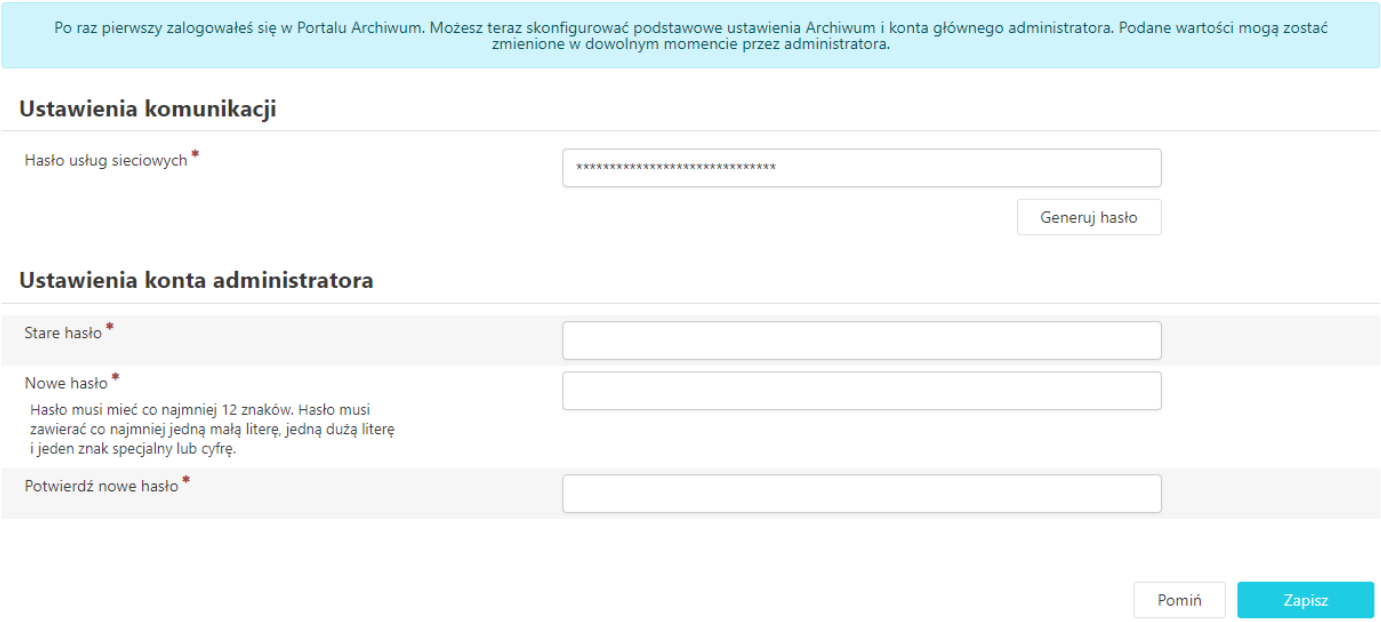
Po wybraniu z prawego, górnego rogu opcji „Zaloguj się” pojawi się formularz logowania. Domyślne dane logowania dla administratora są następujące:

- nazwa użytkownika: admin
- hasło: test2018



Rysunek 77: Formularz logowania do Portalu Archiwum

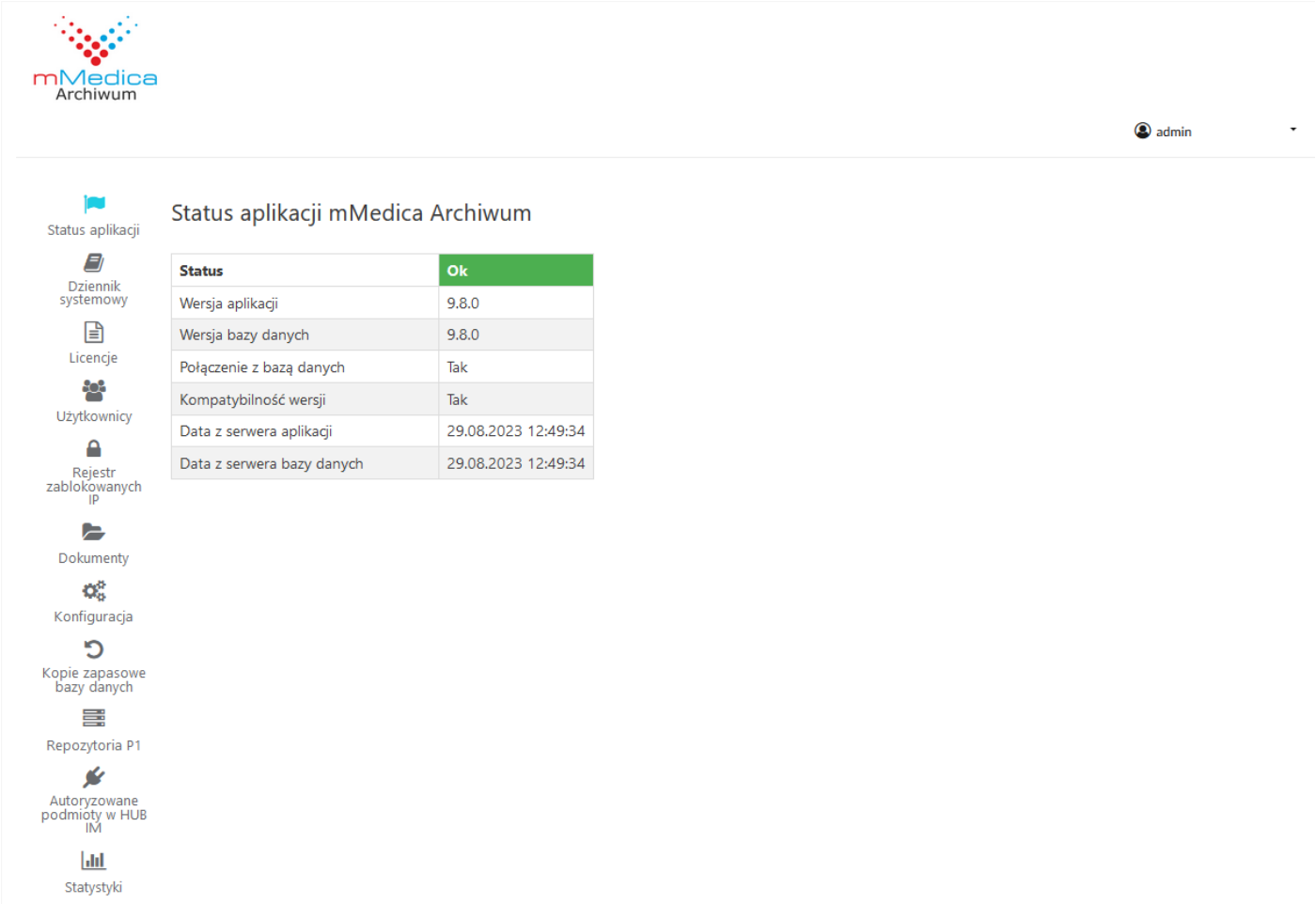
Proces logowania nastąpi po wpisaniu danych logowania w odpowiednich polach oraz naciśnięciu przycisku „Zaloguj się”. Po dokonaniu tej czynności administrator zostanie zalogowany i przeniesiony na stronę konfiguracji wstępnej modułu. Na stronie konfiguracji można ustawić własne hasło usług sieciowych lub wygenerować przyciskiem „Generuj hasło”. Dodatkowo konfiguracja pozwala na zmianę hasła do konta administratora. Przycisk „Zapisz” zapisuje wprowadzone ustawienia. Konfigurację wstępną można pominąć przyciskiem „Pomiń”, a ustawienia wprowadzić później.



Rysunek 78: Konfiguracja wstępna modułu Archiwum

Uwaga: Należy zwrócić dużą uwagę na wpisywane hasło usług sieciowych, gdyż będzie ono wymagane podczas konfigurowania programu mMedica. Jeśli instalacja zawiera moduł eRejestracja, ze względów bezpieczeństwa należy nadać hasło usług sieciowych Archiwum inne niż dla modułu eRejestracja.

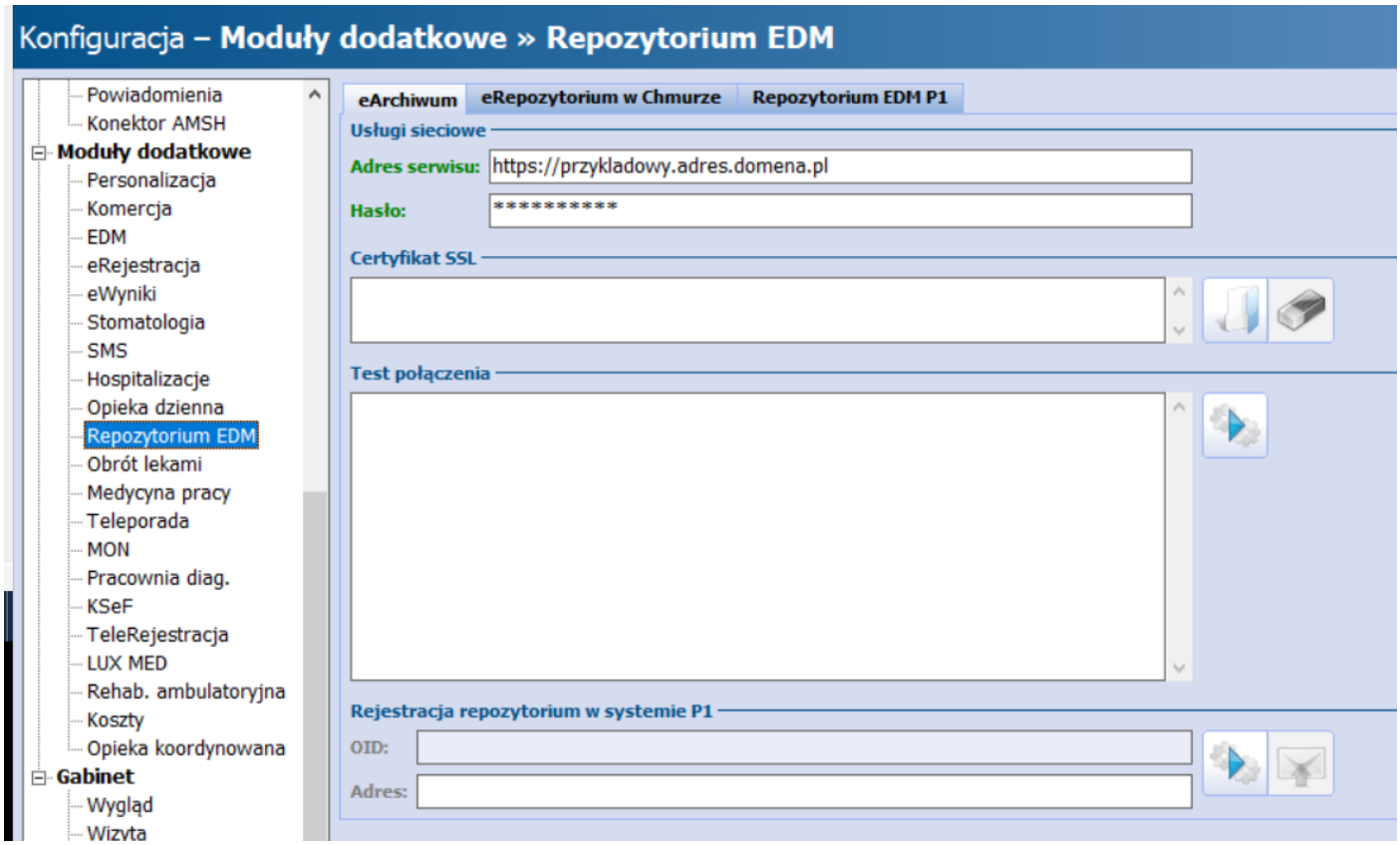
Po pominięciu lub zapisaniu konfiguracji użytkownik zostaje przeniesiony na stronę główną portalu, która jest również stroną statusową nieco różniącą się od tej dla niezalogowanego użytkownika i wygląda następująco:



Rysunek 79: Strona główna Portalu Archiwum po zalogowaniu

8.1.1. Konfiguracja programu mMedica

W programie mMedica należy skonfigurować parametry połączenia z Archiwum. W Zarządzanie/Konfiguracja/Konfigurator (w kontekście systemu) należy po lewej stronie z sekcji „Moduły dodatkowe”\ „Repozytorium EDM”, a następnie przejść na zakładkę „eArchiwum”.



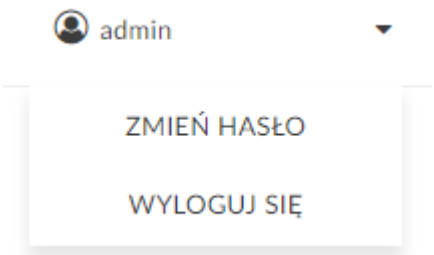
Rysunek 80: Konfiguracja modułu Archiwum w programie mMedica

W sekcji „Usługi sieciowe” w polu „Adres serwisu” należy podać adres usługi Archiwum. Jeśli Archiwum ma być wykorzystywane do komunikacji z systemem Informacje Medyczne, to wpisany adres musi być publiczny. W pole „Hasło” należy wpisać tą samą wartość co w haśle usług sieciowych Portalu Archiwum. W celu weryfikacji połączenia można posłużyć się przyciskiem testu połączenia. Integracja modułu Archiwum oraz programu mMedica z systemem Informacje Medyczne została opisana w instrukcji dotyczącej programu mMedica.

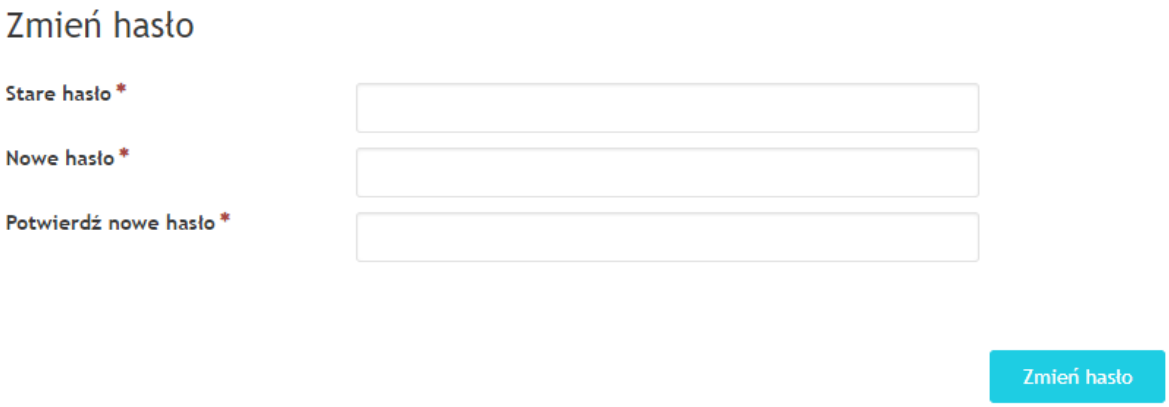
Sekcja „certyfikat SSL” jest opcjonalna do uzupełnienia i została opisana w osobnych rozdziałach związanych z konfiguracją uwierzytelnieniem certyfikatem, patrz: *3.13.3. Konfiguracja uwierzytelniania certyfikatem TLS* (Windows) oraz *4.9.3. Konfiguracja uwierzytelniania certyfikatem TLS (Linux)*

8.2. Zmiana hasła

W celu zmiany hasła należy zalogować się na konto, a następnie wejść w menu Zmień hasło i wypełnić formularz. Jeśli dane zostaną uzupełnione poprawnie, po naciśnięciu przycisku „Zmień hasło” wyświetli się komunikat potwierdzający dokonanie zmiany. Od tej pory administrator może logować się za pomocą zmienionego hasła.



Rysunek 81: Menu rozwijane administratora w Archiwum



Rysunek 82: Formularz zmiany hasła w Archiwum

8.3. Status aplikacji

Formatka ta pozwala na zweryfikowanie czy połączenie z bazą danych Archiwum jest prawidłowe. Ze strony można pozyskać takie informacje jak: wersja aplikacji, wersja bazy danych, informację o tym czy aplikacja jest kompatybilna z bazą, datę i czas z serwera aplikacji oraz serwera bazy danych Archiwum. Wygląd strony przedstawiony jest na zrzucie ekranu (patrz: *Rysunek 79: Strona główna Portalu Archiwum po zalogowaniu*).

8.4. Dziennik systemowy

Weryfikacja dziennika systemowego następuje poprzez wybranie z menu (umieszczonego po lewej stronie) opcji „Dziennik systemowy”. Dziennik systemowy dzieli się na trzy zakładki, z których każda odpowiedzialna jest za wyświetlanie informacji o zdarzeniach z innej części aplikacji. Pierwsza z nich pozwala na przeglądanie informacji o zdarzeniach związanych z działaniem Portalu Archiwum. Druga z nich odpowiada za część aplikacji związanej z interfejsem obsługi dokumentów. Z kolei, trzecia zawiera informacje o komunikatach ATNA związanych z procesem wymiany dokumentów za pośrednictwem systemu P1 (informacji w instrukcji modułu RepozytoriumP1).

Dziennik systemowy

Portal API Logi P1 ATNA

Szczegóły | Eksport wybranego wpisu | Eksport

Data	Błąd	Informacja
28.09.2021 10:00:07	**Logowanie użytkownika**	Błąd testowy

Strona 1 z 1 | 10 na stronę | Wyświetlanie elementów 1 - 1 z 1

Dziennik systemowy

Portal API Logi P1 ATNA

Szczegóły | Eksport wybranego wpisu | Eksport

Data	Błąd	Informacja
21.09.2021 13:29:42	**Tworzenie i rejestracja repozytorium w P1**	Wystąpił błąd podczas rejestracji repozytorium w systemie P1
21.09.2021 10:51:15	**Aktualiacja adresu repozytorium w P1**	Brak repozytorium '2.16.840.1.113883.3.4424.7.24..... ' w bazie danych
21.09.2021 10:50:23	**Aktualiacja adresu repozytorium w P1**	Brak repozytorium '2.16.840.1.113883.3.4424.7.24..... ' w bazie danych
21.09.2021 10:49:19	**Szyfrowana komunikacja**	Nastąpił problem podczas odszyfrowywania wiadomości żądania: nieprawidłowy podpis wiadomości.

Strona 1 z 1 | 10 na stronę | Wyświetlanie elementów 1 - 4 z 4

Dziennik systemowy

Portal API Logi P1 ATNA

Szczegóły

Data wysyłki	Wysłano do P1	REGON	Id dokumentu	Pacjent	Rodzaj dokumentu
17.09.2021 10:31:44	✔	00000000000000	10842	00000000000 (PESEL)	Informacja dla lekarza kierującego/POZ (08.90)
17.09.2021 10:31:40	✖	00000000000000	10814	00000000000 (PESEL)	Wyniki badań diagnostycznych (06.00)
17.09.2021 10:31:22	✔	00000000000000	10842	00000000000 (PESEL)	Informacja dla lekarza kierującego/POZ (08.90)
17.09.2021 10:31:04	✔	00000000000000	10842	00000000000 (PESEL)	Informacja dla lekarza kierującego/POZ (08.90)
17.09.2021 10:26:58	✔	00000000000000	10842	00000000000 (PESEL)	Informacja dla lekarza kierującego/POZ (08.90)

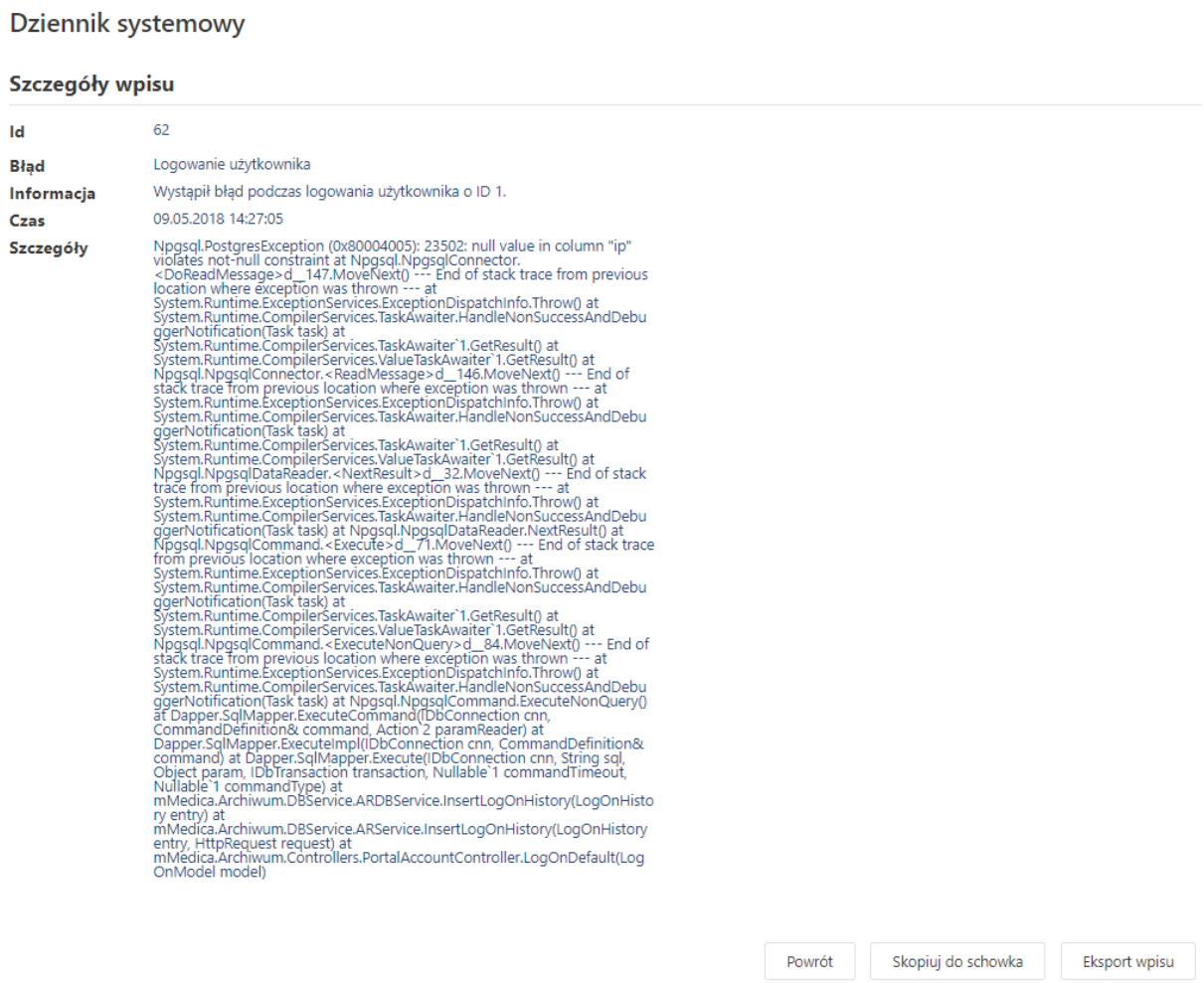
Strona 1 z 2120 | 5 na stronę | Wyświetlanie elementów 1 - 5 z 10596

Rysunek 83: Dziennik systemowy Archiwum

Kolumny wpisów dziennika systemowego mogą być sortowane poprzez naciśnięcie na ich nazwę oraz filtrowane za pomocą przycisku filtra ( ) .

8.4.1. Zakładka „Portal” oraz „API”

Dziennik zawiera informacje o czasie wystąpienia zdarzenia, nazwie zdarzenia oraz zawiera jego opis. Dodatkowo w przypadku, gdy znane są szczegóły błędu można je wyświetlić poprzez zaznaczenie wpisu i naciśnięciu przycisku „Szczegóły”. Wywoła to przekierowanie na formatkę wyświetlającą dokładne informacje o zdarzeniu. W przypadku, w którym przycisk szczegółów pozostaje nieaktywny, oznacza to brak informacji dodatkowych dotyczących zaznaczonego wpisu.

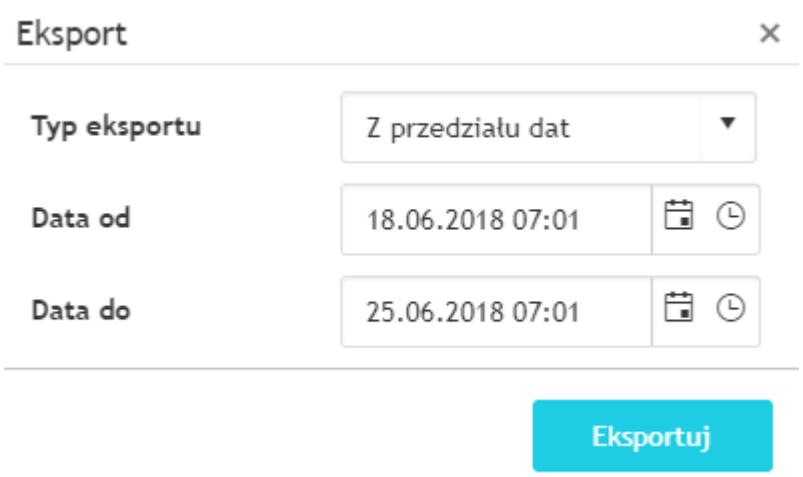


Rysunek 84: Szczegóły zdarzenia Archiwum

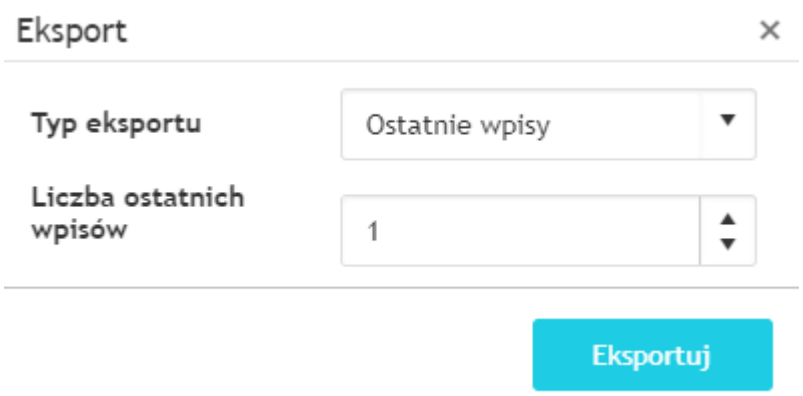
Przycisk „Skopiuj do schowka” kopiuje wszystkie zawarte w szczególe wpisu dane. Dzięki temu możliwe jest wklejenie danych informacji do edytora tekstowego. Można zrobić to za pomocą kliknięcia prawego przycisku myszy i wybrania opcji „Wklej” lub za pomocą skrótów klawiszowych Ctrl + v.

Eksport wpisów z dziennika systemowego pozwala na zapis poszczególnych wpisów do pliku *.csv. Przycisk „Eksport” otwiera okno zawierające opcje eksportu. Rozwijana lista „Rodzaj eksportu” umożliwia eksport wpisów na podstawie wybranego przedziału dat, ostatnich wpisów (wymaga podania liczby ostatnich wpi-

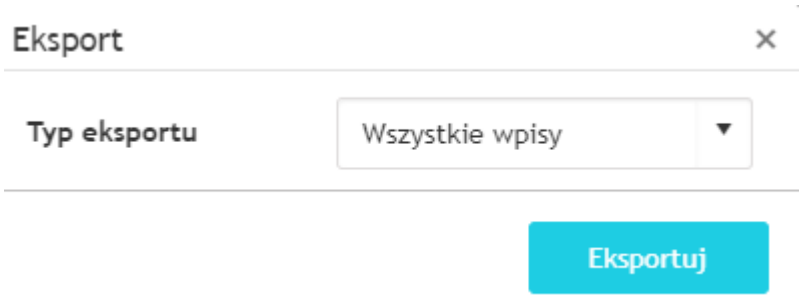
sów do eksportu) lub wszystkich wpisów dziennika systemowego. Przycisk „Eksport wybranego wpisu” pozwala na zapis pojedynczego, zaznaczonego na liście wpisu. Jest on dostępny również z poziomu szczegółowych informacji wpisu.



Rysunek 85: Eksport wpisów dziennika systemowego Archiwum z wybranego okresu.



Rysunek 86: Eksport wpisów dziennika systemowego Archiwum dla ostatnich wpisów

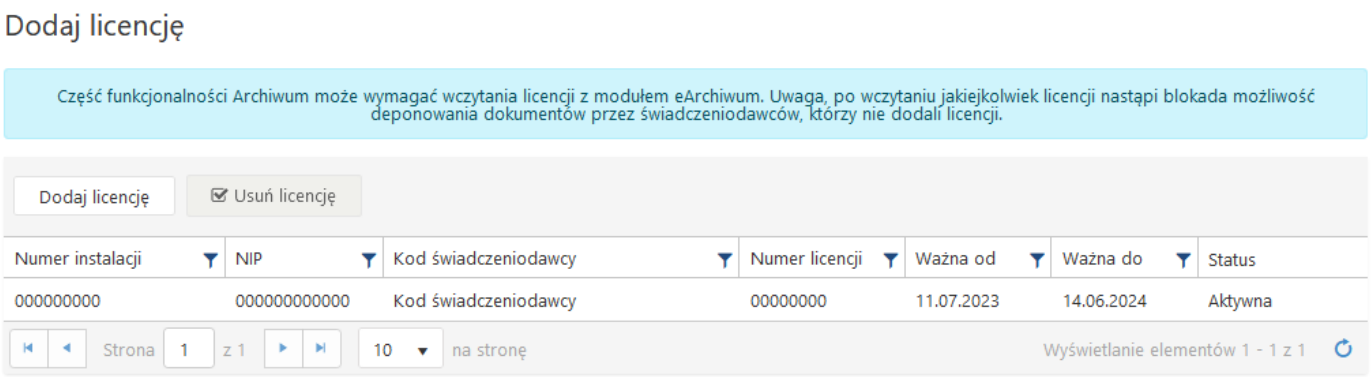


Rysunek 87: Eksport wszystkich wpisów z dziennika systemowego Archiwum

8.5. Licencje

eArchiwum umożliwia wgranie licencji mMedica z modułem eArchiwum co pozwala aktywować dodatkowe funkcje w aplikacji.

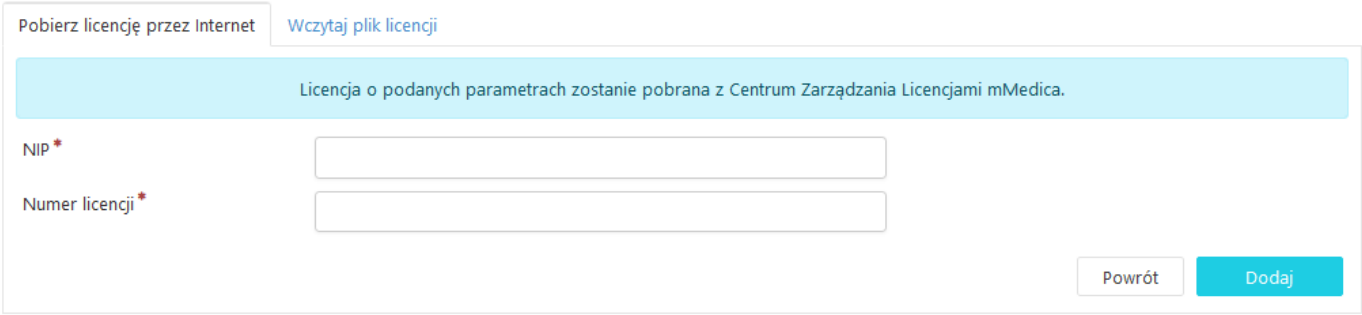
Uwaga: Po wczytaniu jakiejkolwiek licencji nastąpi blokada możliwość deponowania dokumentów przez świadczeniodawców, którzy nie dodali licencji. Funkcjonalność wgrywania licencji jest opcjonalna i konieczna tylko do aktywowania wymienionych w rozdziale dodatkowych funkcjonalności. Innymi słowy brak wczytania licencji nie powoduje zablokowania podstawowych funkcji aplikacji jak deponowanie, pobieranie dokumentów, integracja z systemem P1, IM, czy modułem eRejestracja+.



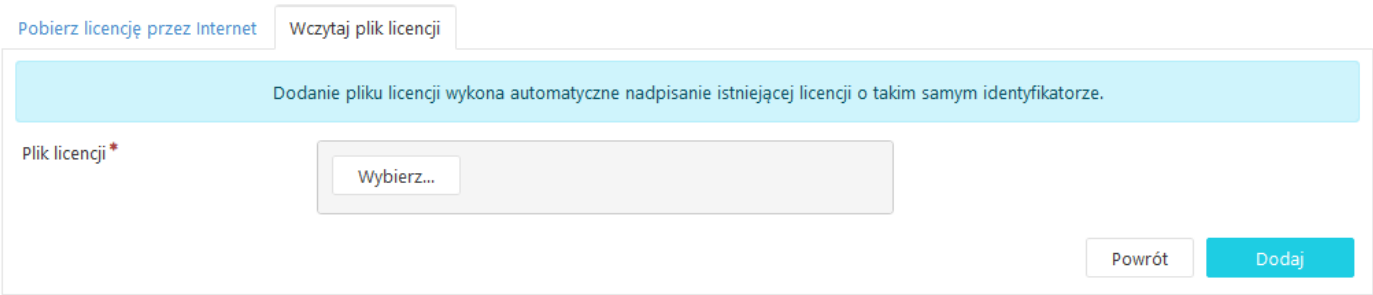
Rysunek 88: Lista licencji w Portalu Archiwum

Wgranie licencji możliwe jest wybraniu przycisku „Dodaj licencję” a następnie przez wybranie jednej z dwóch dostępnych metod:

- pobranie pliku licencji na podstawie NIP i nr licencji z Centrum Zarządzania Licencjami mMedica,
- wgranie pliku licencji.



Rysunek 89: Pobieranie licencji z Centrum Zarządzania Licencjami mMedica



Rysunek 90: Wczytanie pliku z licencją

Lista dodanych licencji wyświetla dane z licencji takie jak:

- numer instalacji,
- NIP,
- kod świadczeniodawcy,
- numer licencji,
- data ważności licencji od
- data ważności licencji do
- Status, np.: aktywna, karencja, wygasła.

Lista wczytanych licencji pozwala również na usunięcie licencji po jej zaznaczeniu i wybraniu przycisku „Usuń licencję”.

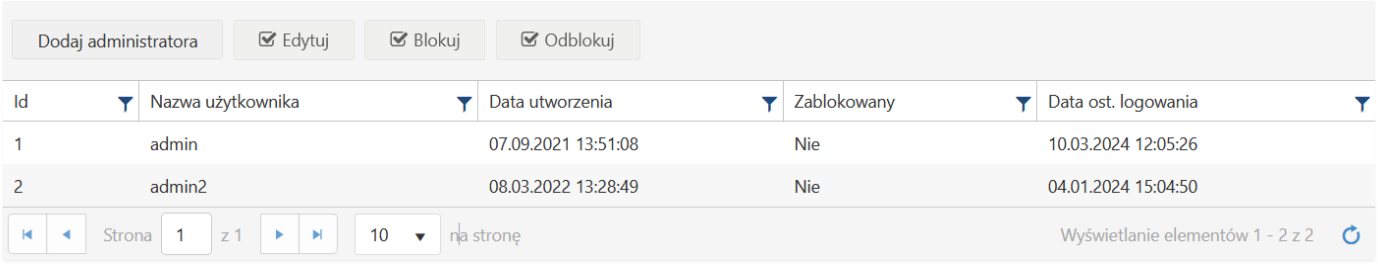
Lista funkcjonalności możliwa po wgraniu licencji:

- Licencja z modułem dodatkowym eKopia+ umożliwia skonfigurowanie dodatkowego hasła zabezpieczającego kopie bazy danych eArchiwum.

8.6. Użytkownicy

8.6.1. Lista użytkowników

Lista użytkowników dostępna jest po wybraniu opcji „Użytkownicy” z lewego menu. Na stronie tej znajduje się lista z użytkownikami Portalu Archiwum. Wszyscy użytkownicy w tym systemie posiadają uprawnienia administratorskie.

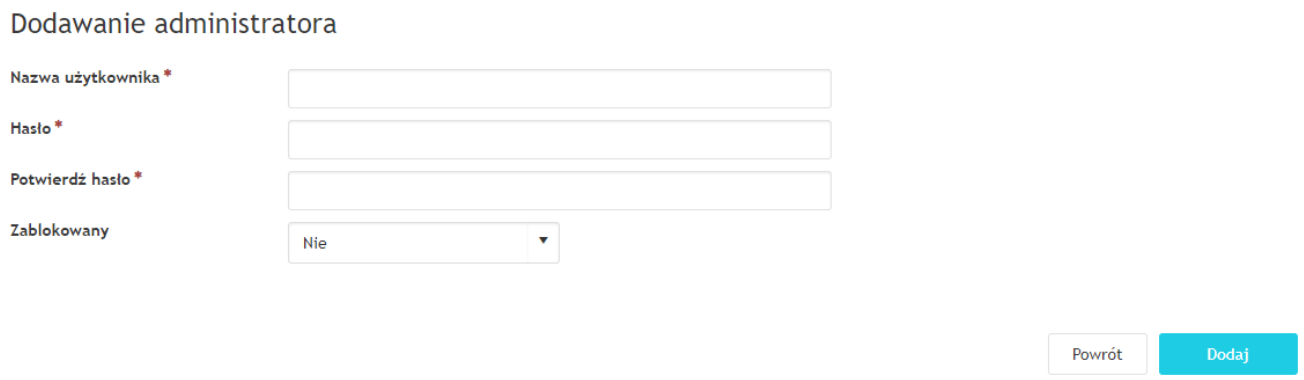


Rysunek 91: Lista użytkowników Portalu Archiwum

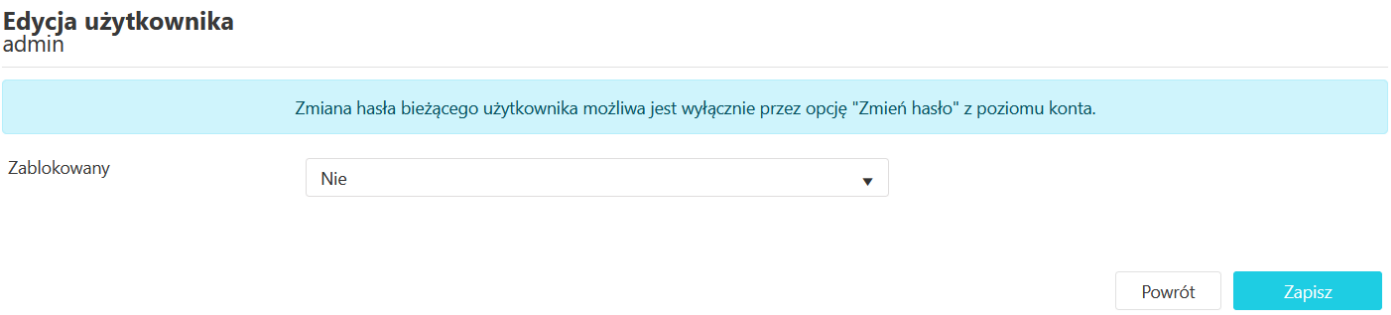
Z listy można pozyskać informację między innymi o tym czy konto jest zablokowane oraz kiedy nastąpiło ostatnie logowanie na konto.

W górnym, poziomym menu aplikacji znajdują się przyciski pozwalające zarządzać kontem użytkownika. Służą one do zmiany statusu użytkownika. Poniżej opisano działanie każdego z nich:

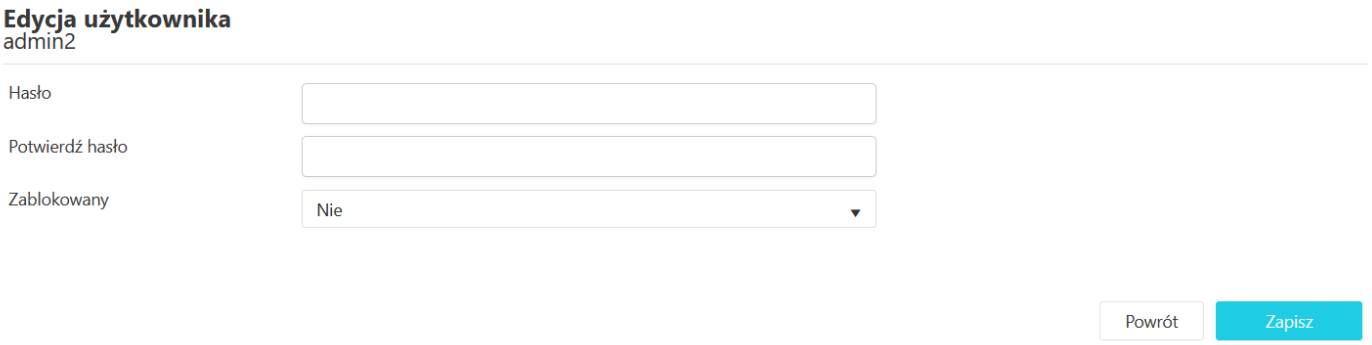
- Dodaj administratora,
- Edytuj – aktywny po zaznaczeniu użytkownika,
- Zablokuj – aktywny po zaznaczeniu niezablokowanego użytkownika,
- Odblokuj – aktywny po zaznaczeniu zablokowanego użytkownika,



Rysunek 92: Dodawanie administratora Portalu Archiwum



Rysunek 93: Edycja konta bieżącego użytkownika



Rysunek 94: Edycja konta użytkownika innego niż bieżący zalogowany

8.6.2. Historia logowań

Drugą dostępną zakładką jest „Historia logowań” zawierająca archiwum logowań użytkowników. Przy każdej próbie logowania widnieje data, informacja czy logowanie było pomyślne, adres IP, z którego się logowano oraz User Agent, czyli przeglądarka, której użyto.

Użytkownicy

Lista | Historia logowania

Usuń wpisy starsze niż 30 dni

Data logowania	Nazwa użytkownika	Poprawne	Adres IP	Nazwa hosta	Useragent
23.01.2019 08:32:58	admin	Tak	::1		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
21.01.2019 09:47:38	admin	Tak	::1		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
21.01.2019 09:47:27	admin	Nie	::1		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
07.01.2019 09:24:01	admin	Tak	::1		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
07.12.2018 13:37:17	admin	Tak	::1		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36

Strona 1 z 12 | 5 na stronę | Wyświetlanie elementów 1 - 5 z 60

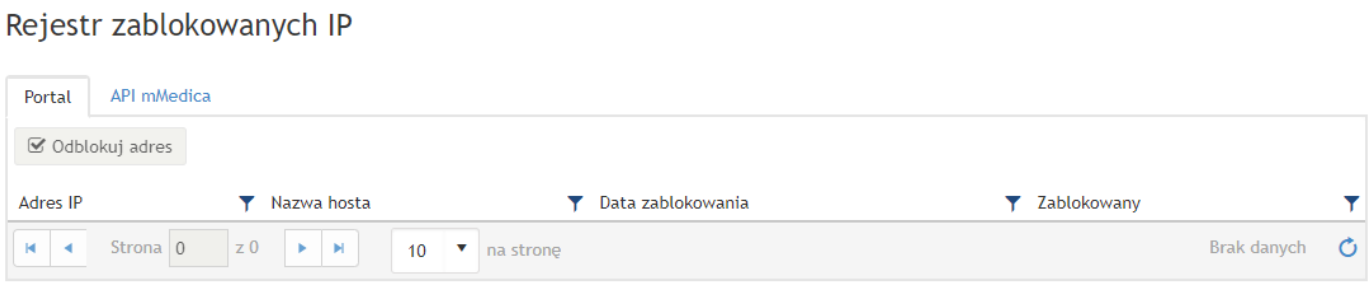
Rysunek 95: Historia logowań użytkowników Archiwum

8.7. Rejestr zablokowanych IP

Lista zablokowanych adresów IP ukazuje się po wybraniu w konfiguracji opcji „Rejestr zablokowanych adresów IP”. Rejestr podzielony jest na dwie zakładki: Portal oraz API mMedica.

8.7.1. Portal

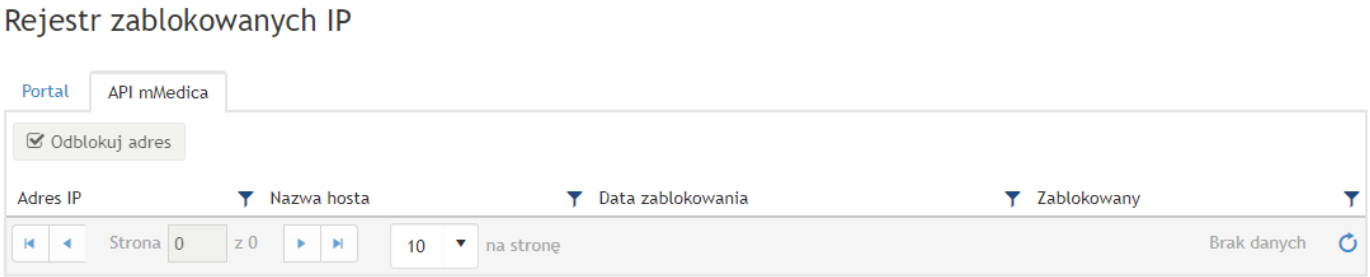
W zakładce portal dostępna jest list adresów IP, które zostały zablokowane ze względu na przekroczenie liczby niepoprawnych logowań do Portalu. Od tego momentu użytkownicy o podanym adresie IP nie będą mogli się zalogować do Archiwum. Adres IP można odblokować poprzez zaznaczenie adresu na liście i kliknięciu przycisku „Odblokuj adres IP”.



Rysunek 96: Lista zablokowanych adresów IP - Portal

8.7.2. API mMedica

W zakładce API mMedica dostępna jest lista zablokowanych adresów IP, ze względu na przekroczenie liczby dozwolonych prób uwierzytelnienia z niepoprawnym tokenem bezpieczeństwa w API mMedica. Od tego momentu użytkownicy o podanym adresie IP nie będą mogli się zalogować do Archiwum. Adres IP można odblokować poprzez zaznaczenie adresu na liście i kliknięciu przycisku „Odblokuj adres IP".



Rysunek 97: Lista zablokowanych adresów IP - API mMedica

8.8. Pobrane dokumenty

Pobrane dokumenty przedstawiają listę dokumentów, które zostały pobrane za pomocą aplikacji Informacje Medyczne, mMedica lub eRejestracja. Domyślnie wyświetlane pozycje są wyświetlane w kolejności od najnowszej daty pobrania do najstarszej daty pobrania. Dla pozycji „pobrany z programu mMedica" wyświetlany jest również personel, który dokonał tej operacji. Z tabeli można odczytać również numer REGON podmiotu, Id dokumentu, Identyfikator pacjenta oraz rodzaj pobranego dokumentu. Lista pozwala na bezpowrotne usunięcie wpisów starszych niż 30 dni za pomocą przycisku „Usuń wpisy starsze niż 30 dni".

Pobrane dokumenty

Usuń wpisy starsze niż 30 dni | Szczegóły logu P1 ATNA

Data pobrania	REGON	Id dok.	Rodzaj pobrania	Przez	Pacjent	Rodzaj dokumentu
06.10.2021 14:04:22	0000000000000	29774	mMedica	Imię Nazwisko	00000000000 (PESEL)	Informacja dla lekarza kierującego/POZ (08.90)
06.10.2021 08:00:29	0000000000000	29771	mMedica	Imię Nazwisko	00000000000 (PESEL)	Informacja dla lekarza kierującego/POZ (08.90)
30.09.2021 12:09:36	0000000000000	11703	P1	Podmiot leczniczy: 000000000001 Osoba (medical doctor): 0000000 (NPWZ) Cel: Ratowanie życia	00000000000 (PESEL)	Informacja dla lekarza kierującego/POZ (08.90)
30.09.2021 12:06:53	0000000000000	29621	P1	Podmiot leczniczy: 000000000001 Osoba (medical doctor): 0000000 (NPWZ) Cel: Ratowanie życia	00000000000 (PESEL)	Karta informacyjna z leczenia szpitalnego (00.20)

Strona 1 z 2199 | 5 na stronę | Wyświetlanie elementów 1 - 5 z 10995

Rysunek 98: Lista pobranych dokumentów w Portalu Archiwum

8.9. Usunięte dokumenty

Usunięte dokumenty wyświetlają dokumenty, które zostały usunięte z poziomu aplikacji mMedica z Archiwum. Domyślnie pozycje wyświetlane są w kolejności od najnowszej daty usunięcia dokumentu do najstarszej daty usunięcia dokumentu. Lista zawiera informacje o numerze REGON, Id dokumentu, sposobie usunięcia wpisu, pacjencie przypisanym do dokumentu oraz o wartości skrótu dokumentu (w formie SHA1), miejscu utworzenia dokumentu, i rodzaju dokumentu. Nad listą umieszczony jest przycisk, który pozwala bezpowrotnie usunąć pozycje starsze niż 30 dni.

Usunięte dokumenty

Usuń wpisy starsze niż 30 dni

Data usunięcia	REGON	Id dok.	Przez	Pacjent	Informacje
09.06.2021 13:37:20	00000000000000	11296	Imię Nazwisko	00000000000 (PESEL)	Skrót: 915e3c8ce3d8a631debd51539427de8628bd1a8e Utworzony przez: mMedica Rodzaj: Prośba o objęcie opieką (02.12)
09.06.2021 13:37:20	00000000000000	11285	Imię Nazwisko	00000000000 (PESEL)	Skrót: 1a0493d330a32e3acf78910bd2d45f64e630c1ca Utworzony przez: mMedica Rodzaj: Prośba o objęcie opieką (02.12)

Strona 1 z 29 | 5 na stronę | Wyświetlanie elementów 1 - 5 z 142

Rysunek 99: Lista usuniętych dokumentów w Portalu Archiwum

8.10. Historia zmian widoczności dokumentów

Historia zmian widoczności dokumentów przedstawia rejestr zmian widoczności dokumentów do pobrania przez pacjenta z poziomu aplikacji mMedica. Domyślnie historia wyświetlana jest w kolejności od najnowszej daty wprowadzenia modyfikacji widoczności do najstarszej daty wprowadzenia modyfikacji widoczności. Lista zawiera informacje o REGONie podmiotu, Id dokumentu, personelu zmieniającym widoczność, pacjencie przypisanym do dokumentu oraz rodzaju dokumentu. Wykaz pozwala na trwałe usunięcie wpisów starszych niż 30 dni.

Historia zmian widoczności dokumentów

Usuń wpisy starsze niż 30 dni

Data zmiany	REGON	Id dok.	Przez	Pacjent	Rodzaj dokumentu
06.10.2021 15:04:51	00000000000000	29779	Automat Systemowy	00000000000 (PESEL)	Skierowanie na badanie lub leczenie (02.10)
06.10.2021 14:39:49	00000000000000	29778	Imię Nazwisko	00000000000 (PESEL)	Informacja dla lekarza kierującego/POZ (08.90)
06.10.2021 14:39:48	00000000000000	29777	Imię Nazwisko	00000000000 (PESEL)	Wyniki badań diagnostycznych (06.00)

Strona 2 z 2456 5 na stronę Wyświetlanie elementów 6 - 10 z 12277

Rysunek 100: Historia zmian widoczności dokumentów w Portalu Archiwum

8.11. Konfiguracja

Podstrona „Konfiguracja” pozwala na edytowanie podstawowych ustawień modułu Archiwum. Lista parametrów:

Bezpieczeństwo:

- Hasło usług sieciowych – hasło, które pozwala na bezpieczną komunikacje z mMedica. Wprowadzone hasło musi być takie samo jak w programie mMedica. Obok pola na wpisanie hasła znajduje się przycisk „Pokaż hasło”. Po jego kliknięciu zakropkowane hasło stanie się widoczne, a obok niego pojawi się przycisk „Ukryj hasło”, umożliwiający ponowne zakropkowanie hasła.
- Czas wygaśnięcia tokena bezpieczeństwa [s] – okres ważności hasła wygenerowanego z programu mMedica podczas komunikacji do Archiwum.
- Adres usługi MIAM – adres usługi powiadomień MIAM. W przypadku braku posiadania komponentu MIAM parametr konfiguracyjny powinien być pusty.
- Blokowanie adresów IP w API mMedica – opcja blokowania adresów IP, z których dokonano zbyt dużej liczby błędnych logowań w API mMedica.

- Liczba dopuszczalnych błędnych prób logowania w API mMedica – liczba dopuszczalnych błędnych prób logowania w API mMedica, po przekroczeniu której nastąpi zablokowanie adresu IP, z którego dokonywano błędnych logowań w API mMedica.
- Domyślna ścieżka wykonywania kopii bazy danych – w polu należy wpisać istniejącą (poprawną) ścieżkę, w której będą zapisywane kopie bazy danych wykonywane z poziomu aplikacji (patrz rozdział *8.12 Kopie zapasowe bazy danych*).

Repozytorium w P1:

- Czas wygaśnięcia operacji z P1 [s] – maksymalny dopuszczalny czas operacji z systemem P1 (timeout) wyrażony w sekundach.
- Walidacja konfiguracji aplikacji Repozytorium P1 – opcja jest odpowiedzialna za weryfikację konfiguracji RepozytoriumP1 przez aplikację Archiwum podczas: rejestracji repozytorium w P1, zmiany adresu repozytorium w P1 oraz aktualizacji certyfikatów dla Repozytorium P1.
- Czas wygaśnięcia operacji z serwerem synchronizacji czasu [s] – maksymalny dopuszczalny czas operacji z serwerem synchronizacji czasu (timeout) wyrażony w sekundach.

Dokumenty:

- Wymagany REGON w żądaniach – pozwala na filtrowanie żądań dotyczących dokumentów (w obszarach dedykowanych mMedica oraz eRejestracja) na podstawie wpisanego REGON9 lub REGON14. Jeśli żądanie pochodzące np. z mMedica przedstawia się innym REGONem to zostanie ono odrzucone. Brak wpisanej wartości (ustawienie domyślne) oznacza brak filtrowania żądań.
- Okres widoczności dokumentów dla pacjenta [h] – domyślny czas wyrażony w godzinach widoczności dokumentów do pobrania przez pacjenta.
- Udostępniaj pacjentowi tylko dokumenty podpisane elektronicznie – opcja umożliwia zablokowanie udostępniania pacjentom elektronicznych dokumentów medycznych, które nie zostały podpisane elektronicznie przez lekarza.

Informacja Medyczne:

- Blokuj duplikaty dokumentów dodanych przez Informacje Medyczne – ustawienie blokuje możliwość dodania tych samych dokumentów przez pacjenta.
- Maksymalny rozmiar dokumentu dodanego przez Informacje Medyczne [kB] – maksymalny rozmiar dokumentu dodanego przez pacjenta z aplikacji Informacje Medyczne. Rozmiar definiowany jest w kilobajtach. Ustawienie wartości 0 wyłącza weryfikację rozmiaru dokumentów.

- Liczba dni, po których niepobrane przez personel dokumenty własne użytkownika zostaną usunięte – liczba dni, po których niepobrane przez personel dokumenty własne użytkownika zostaną automatycznie usunięte. Ustawienie wartości na 0 oznacza, że dane będą przechowywane do momentu pobrania ich przez personel.
- Maksymalna liczba wysłanych dokumentów własnych użytkownika na dobę – maksymalna liczba dokumentów własnych, które użytkownik może wysłać w ciągu doby. Pozostawienie pustego pola oznacza, że nie istnieje ograniczenie co do liczby przesłanych plików. Wartość 0 oznacza, że użytkownik nie może przesyłać dokumentów.

Konfiguracja

Bezpieczeństwo

Hasło usług sieciowych *	••••••••••••••••••••••••••••••... Pokaż hasło
Czas wygaśnięcia tokena bezpieczeństwa [s] *	30
Adres usługi MIAM	
Blokowanie adresów IP w API mMedica	☑
Liczba dopuszczalnych błędnych prób logowania w API mMedica *	10
Domyślna ścieżka wykonywania kopii bazy danych	

Repozytorium w P1

Czas wygaśnięcia operacji z P1 [s] *	30
Czas wygaśnięcia operacji z serwerem synchronizacji czasu [s] *	5
Walidacja konfiguracji aplikacji Repozytorium P1	☑

Dokumenty

Wymagany REGON w żądaniach	
Okres widoczności dokumentów dla pacjenta [h] *	48
Udostępniaj pacjentowi tylko dokumenty podpisane elektronicznie	☐

Informacje Medyczne

Blokuj duplikaty dokumentów dodanych przez Informacje Medyczne	☑
Maksymalny rozmiar dokumentu dodanego przez Informacje Medyczne [kB] * Wartość 0 oznacza wyłączoną weryfikację rozmiaru.	0
Liczba dni, po których niepobrane przez personel dokumenty własne użytkownika zostaną usunięte * Ustawienie wartości na 0 oznacza, że dane będą przechowywane do momentu pobrania ich przez personel.	0
Maksymalna liczba wysłanych dokumentów własnych użytkownika na dobę Pozostawienie pustego pola oznacza, że nie istnieje ograniczenie co do liczby przesłanych plików. Wartość 0 oznacza, że użytkownik nie może przesłać dokumentów.	

Zapisz

Rysunek 101: Konfiguracja Archiwum

8.12. Kopie zapasowe bazy danych

8.12.1. Historia kopii zapasowych

Historia kopii zapasowych zawiera tabelę utworzonych wcześniej automatycznych kopii zapasowych. Tabela zawiera:

- status,
- datę utworzenia automatycznej kopii zapasowej,
- nazwę pliku,
- numer wersji programu,
- nazwę użytkownika, który dodał automatyczną kopię zapasową
- informację czy kopia została zaplanowana, czy utworzona ręcznie.
- informację, czy kopia została wykonana z załącznikami (plikami dokumentów).

Kopie zapasowe bazy danych

Historia kopii zapasowych | Automatyczna kopia zapasowa | Zabezpieczenia kopii zapasowej

Status	Data utworzenia	Nazwa pliku	Wersja	Użytkownik	Zaplanowano	Z załącznikami
	26.07.2023 15:23:37	2023-07-26-1523-ARCHMMEDICA(b).zip	9.7.0	admin		
	12.05.2023 14:24:44	8.back	9.4.0	admin		
	12.05.2023 14:21:30	7.back	9.4.0	admin		
	12.05.2023 14:21:30	7.back	9.4.0	admin		
	12.05.2023 14:19:39	test6.back	9.4.0	admin		
	12.05.2023 14:19:39	test6.back	9.4.0	admin		
	12.05.2023 14:18:11	test5.back	9.4.0	admin		
	12.05.2023 14:18:11	test5.back	9.4.0	admin		
	12.05.2023 14:16:45	test4.back	9.4.0	admin		
	12.05.2023 14:16:45	test4.back	9.4.0	admin		

Strona 1 z 3 10 na stronę Wyświetlanie elementów 1 - 10 z 25

Rysunek 102: Historia kopii zapasowych

8.12.2. Automatyczna kopia zapasowa

Zakładka ta umożliwia zaplanowanie przez administratora wykonywania się automatycznych kopii zapasowych. Aby zaplanować automatyczną kopię, należy wypełnić pola:

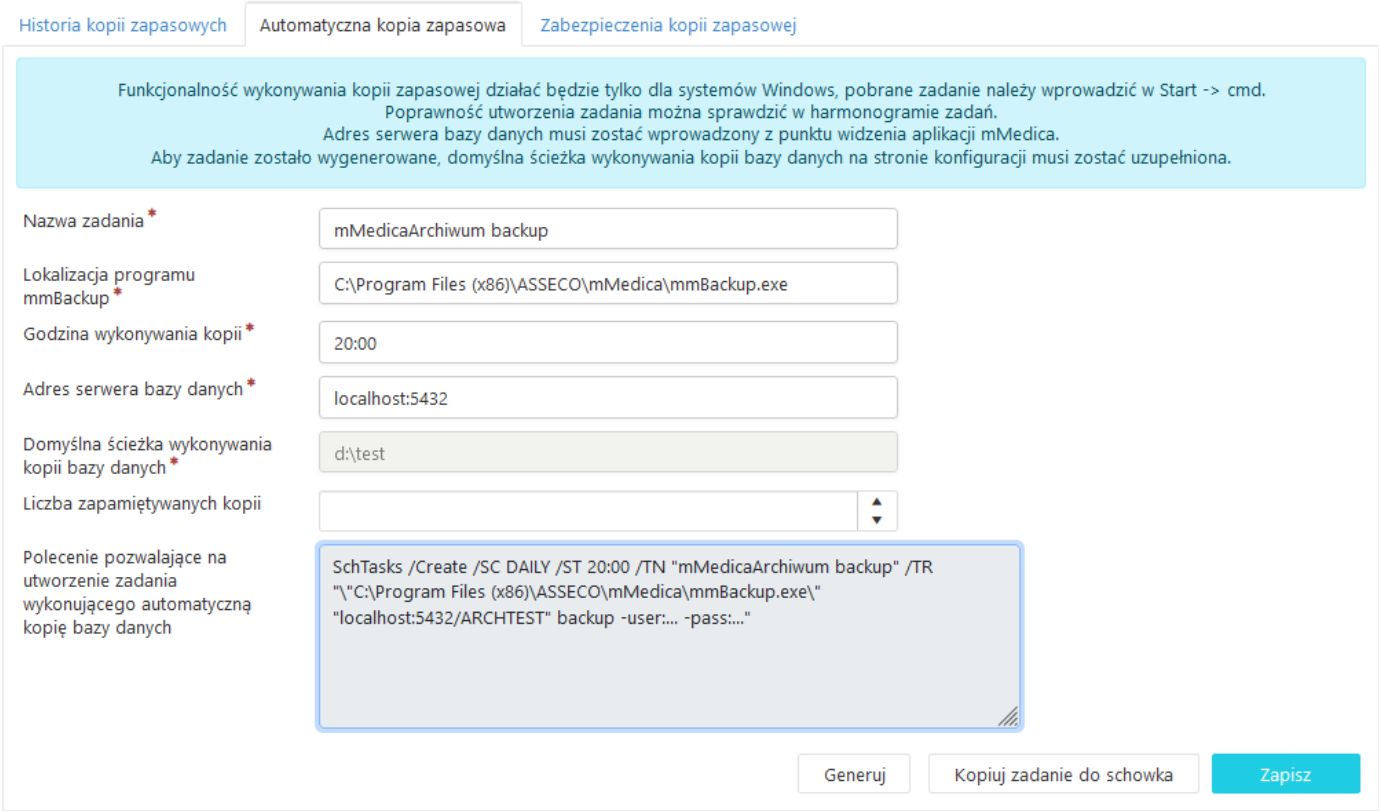
- Nazwa zadania,
- Lokalizacja programu mmBackup (należy wpisać pełną ścieżkę dostępu do pliku mmBackup.exe),

- Godzina wykonywania kopii (należy wpisać godzinę, o której codziennie będzie wykonywać się kopia zapasowa),
- Liczba zapamiętanych kopii bazy danych,
- Adres serwera bazy danych.

Pole „Domyślna ścieżka wykonywania kopii bazy danych” uzupełniona jest wartością zapisaną w zakładce Konfiguracja w polu „Domyślna ścieżka wykonywania kopii bazy danych” i tylko tam możliwa jest jej edycja.

Po uzupełnieniu pól należy kliknąć przycisk „Generuj”, który utworzy odpowiednie polecenie (w polu „Polecenie pozwalające na utworzenie zadania wykonującego automatyczną kopię bazy danych”). Dane polecenie należy skopiować ręcznie lub poprzez kliknięcie przycisku „Kopiuj zadanie do schowka”. Następnie należy otworzyć na komputerze wiersz poleceń i wkleić do niego skopiowane polecenie, oraz zatwierdzić je naciskając klawisz „Enter”.

Konfigurację można również zapisać co może być przydatne przy ewentualnej zmianie parametrów zadania w przyszłości.



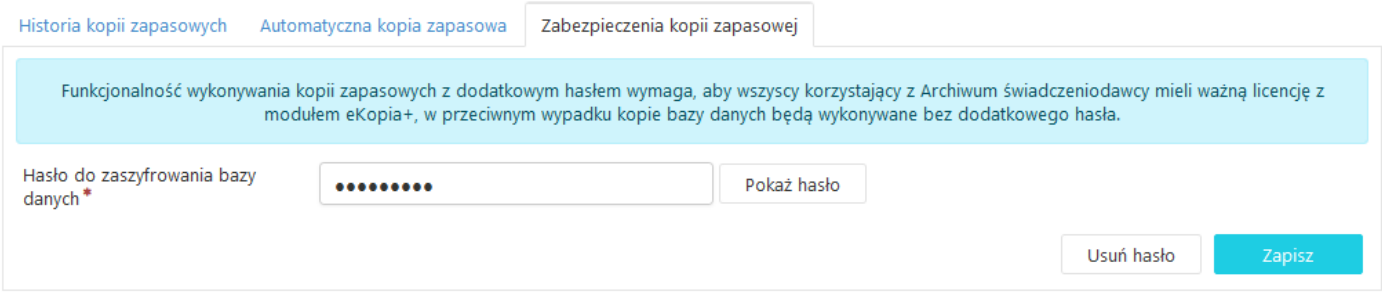
Rysunek 103: Automatyczna kopia zapasowa

Uwaga: Za każdym razem, gdy zmieni się hasło użytkownika generującego automatyczną kopię zapasową, należy wygenerować na nowo wszystkie utworzone zadania wykonujące automatyczne kopie bazy danych.

8.12.3. Zabezpieczenia kopii zapasowej

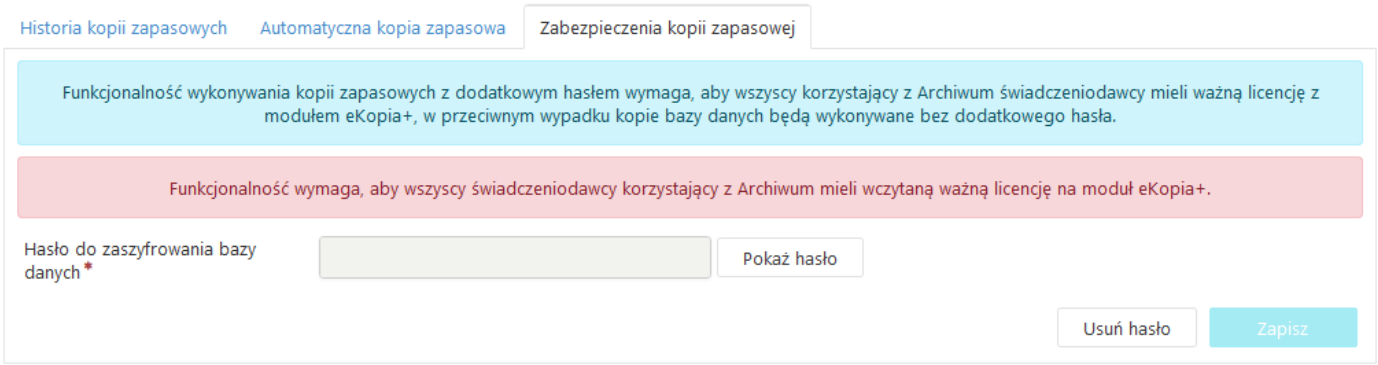
Uwaga: Funkcjonalność wymaga zaczytania licencji z modułem eKopia+ w eArchiwum.

Formatka zabezpieczenia kopii zapasowej pozwala na zdefiniowanie dodatkowego hasła zabezpieczającego kopie bazy danych eArchiwum. Funkcjonalność wykonywania kopii zapasowych z dodatkowym hasłem wymaga, aby wszyscy korzystający z Archiwum świadczeniodawcy mieli ważną licencję z modułem eKopia+, w przeciwnym wypadku kopie bazy danych będą wykonywane bez dodatkowego hasła. Konfiguracje hasła można usunąć za pomocą przycisku „Usuń hasło”.



Rysunek 104: Ustawienie dodatkowego hasła zabezpieczającego kopie bazy danych

W przypadku ważnej braku licencji z modułem eKopia+ formatka przechodzi w stan uniemożliwiający nadanie hasła.



Rysunek 105: Zablokowana formatka do hasła zabezpieczającego kopie bazy danych

8.13. Autoryzowane podmioty w HUB IM

Lista autoryzowanych w HUB IM zawiera informacje użyte do rejestracji podmiotu m.in. ważność certyfikatu do komunikacji z Informacje Medyczne. Po jego wygaśnięciu należy z programu mMedica wycofać autoryzację i autoryzować ponownie podmiot w HUB IM.

Autoryzowane podmioty w HUB IM

REGON	NIP	Dane świadczeniodawcy	Adresy	Ważność certyfikatu
000000000	0000000000	Nazwa: Świadczeniodawca Numer instalacji: 000000 Identyfikator lokalizacji: 00000	Konektor: https://przykladowy.adres.domena/XDS Email: przykladowy.adres@domena	12.06.2020 10:13:43

Strona 1 z 1 10 na stronę Wyświetlanie elementów 1 - 1 z 1

Rysunek 106: Lista autoryzowanych podmiotów w HUB IM

8.14. Statystyki

Podstrona statystyk dostarcza informacji o rozmiarze bazy danych modułu Archiwum. Podstrona zawiera również tabelę, w której umieszczone są dane o liczbie pacjentów posiadających dokument, liczbie dokumentów oraz pobrań, dla każdego REGONu, dla którego został dodany co najmniej jeden dokument z mMedica lub Informacje Medyczne.

Statystyki

Szacunkowy rozmiar	Rozmiar
Bazy danych	518 MB
Załączników w bazie danych	433 MB

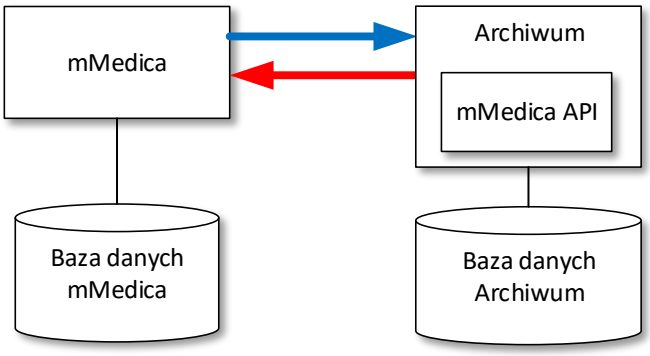
REGON	Liczba pacjentów	Liczba dokumentów			Liczba pobrań dokumentów			
		mMedica	Informacje Medyczne	Łącznie	mMedica	Informacje Medyczne	eRejestracja	Łącznie
00000000	3	9	12	21	15	37	0	52
00000001	10	45	26	71	2	191	27	220
00000002	6	36	6	42	7	70	93	170
00000003	11	46	28	74	61	196	402	659
00000004	5	14	9	23	9	31	0	40
Suma	**35**	**150**	**81**	**231**	**94**	**525**	**522**	**1141**

Rysunek 107: Wykaz statysty Archiwum

9. Komunikacja oraz synchronizacja danych z mMedica

9.1. Komunikacja z mMedica do Archiwum

Komunikacja z mMedica do Archiwum odbywa się przez dedykowany interfejs w aplikacji Archiwum.



Rysunek 108: Model komunikacji z mMedica do Archiwum (kolorem niebieskim oznaczono żądanie, z kolei czerwonym odpowiedź)

Przykłady komunikacji:

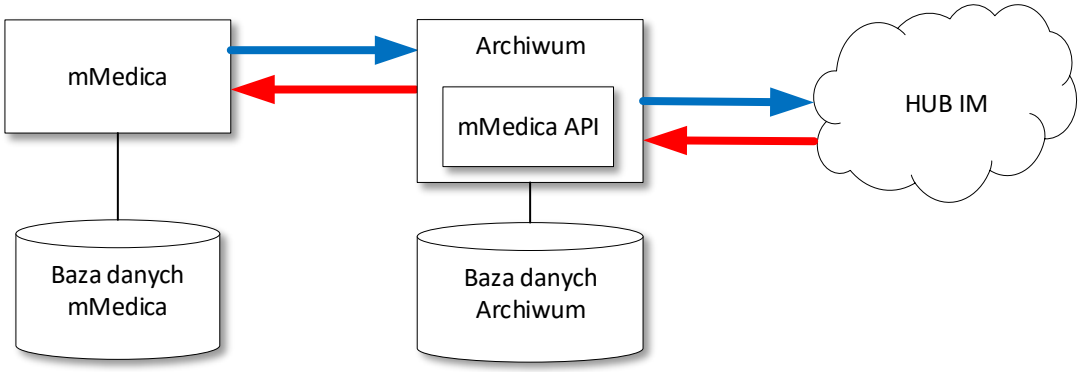
- dodanie dokumentu,
- wyszukiwanie dokumentów,
- pobieranie dokumentu,
- usuwanie dokumentu,
- zmiana widoczności dokumentu do pobrania przez pacjenta,

9.2. Komunikacja z modułu eRejestracja do Archiwum

Opis modelu komunikacji pomiędzy Archiwum a Modułem eRejestracja znajduje się w instrukcji instalacji i konfiguracji modułu eRejestracja.

9.3. Komunikacja z mMedica do systemu Informacje Medyczne

Komunikacja z programu mMedica do systemu Informacje Medyczne odbywa się za pośrednictwem Archiwum.



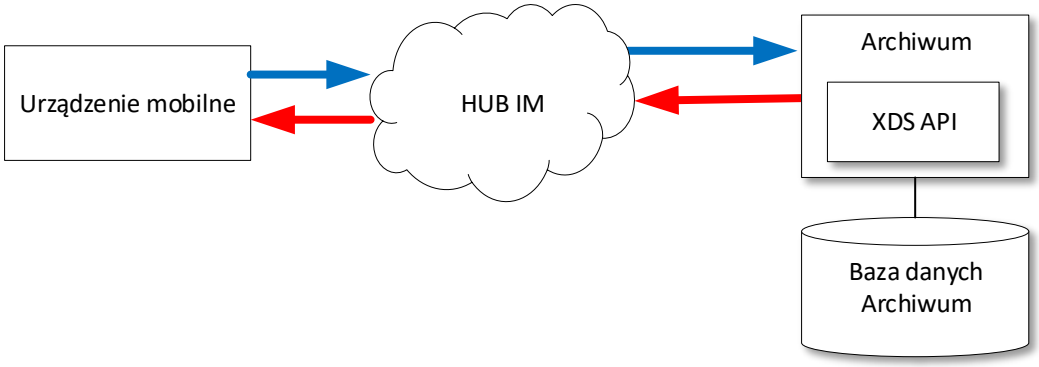
Rysunek 109: Model komunikacji z mMedica do systemu Informacje Medyczne (kolorem niebieskim oznaczono żądanie, z kolei czerwonym odpowiedź)

Przykłady komunikacji:

- autoryzacja zakładu w HUB IM,
- wycofanie autoryzacji zakładu z HUB IM,
- generacja numeru PIN dla użytkowników aplikacji mobilnej Asseco Informacje Medyczne,
- awaryjne usunięcie powiązania urządzenia mobilnego pacjenta z HUB IM,
- wyrażenie zgody na komunikacje pacjenta poprzez HUB IM z danym zakładem,
- wycofanie zgody na komunikacje pacjenta poprzez HUB IM z danym zakładem.

9.4. Komunikacja z systemu Informacje Medyczne do Archiwum

Komunikacja z systemu Informacje Medyczne do Archiwum odbywa się z inicjatywy urządzenia mobilnego z aplikacja mobilna Asseco Informacje Medyczne.



Rysunek 110: Model komunikacji z systemu Informacje Medyczne do Archiwum (kolorem niebieskim oznaczono żądanie, z kolei czerwonym odpowiedź)

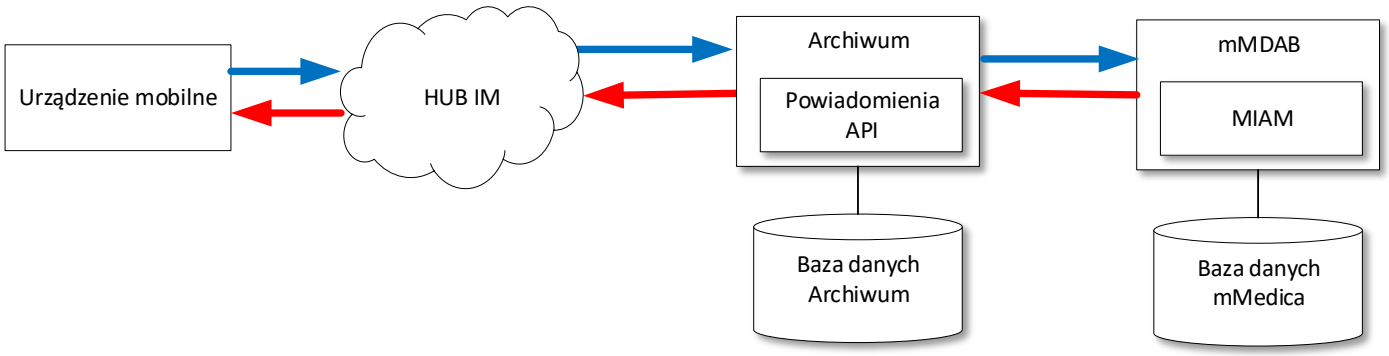
Przykłady komunikacji:

- dodanie dokumentu własnego pacjenta,
- wyszukiwanie dokumentów pacjenta,

- pobieranie dokumentu pacjenta.

9.5. Komunikacja z systemu Informacje Medyczne do bazy danych mMedica

Komunikacja z systemu Informacje Medyczne do bazy danych mMedica odbywa się z inicjatywy urządzenia mobilnego z aplikacja mobilna Asseco Informacje Medyczne. Rolę pośrednika w tej komunikacji odbywa Archiwum oraz MIAM. Komunikacja wymaga zainstalowanego i poprawnie skonfigurowanego komponentu MIAM (m.in. wprowadzeniu adresu MIAM w konfiguracji Archiwum, patrz: *8.11. Konfiguracja*).



Rysunek 111: Model komunikacji z systemu Informacje Medyczne do bazy danych mMedica (kolorem niebieskim oznaczono żądanie, z kolei czerwonym odpowiedź)

Przykłady komunikacji:

- potwierdzenie odczytania na urządzeniu mobilnym wysłanego powiadomienia (zmiana statusu powiadomienia na odczytany w bazie danych mMedica).
- pobieranie listy gabinetów, gdzie pacjenta ma zarejestrowany termin,
- pobieranie stanu kolejki dla gabinetu, gdzie pacjenta ma zarejestrowany termin,
- oznaczenie subskrypcji zmiany stanu kolejki, gdzie pacjenta ma zarejestrowany termin.

9.6. Diagnostyka komunikacji

Diagnostyka podstawowa problemów opiera się na pozyskiwaniu informacji ze strony statusowej modułu oraz Dziennika systemowego (opis w rozdziale *8.4 Dziennik systemowy*), w którym są zapisane informacje o błędach. Istnieje również możliwość diagnozy komunikacji programu mMedica do Archiwum poprzez przetestowanie połączenia w konfiguratorze modułu eArchiwum z poziomu programu mMedica.

10. Pobieranie danych diagnostycznych

Możliwe jest pobieranie danych diagnostycznych w formie XML lub JSON dotyczących działania komponentów mModułów. Zakres danych do pobrania jest tożsamy z danymi wyświetlanymi na stronach statusowych. Opis techniczny znajduje się w dokumencie pod odnośnikiem.

11. Rozwiązania częstych problemów

11.1. Nieprawidłowe hasło usług sieciowych (token)

Należy sprawdzić czy hasło usług sieciowych wpisanie w Konfiguracji Archiwum (*8.11. Konfiguracja*) jest takie samo jak hasło wpisane w programie mMedica w Konfiguratorze (*8.1.1.* Konfiguracja programu mMedica). Szczególną uwagę należy zwrócić na wielkość liter, białe oraz specjalne znaki. Należy także zweryfikować czy na wszystkich komputerach, na których zainstalowane jest Archiwum oraz bazy danych, jest ustawiona ta sama strefa czasowa. Jeżeli podczas komunikacji mMedica w kierunku Archiwum nadal występuje problem z nieprawidłowym hasłem usług sieciowych, może to oznaczać zbyt małą wartość w „Czas wygaśnięcia tokena bezpieczeństwa [s]” w Konfiguracji Archiwum.

11.2. Zapomniane hasło do konta administratora

W przypadku, w którym zapomniano hasła do konta jedynego administratora, należy zgłosić się do Serwisu mMedica w celu otrzymania procedury serwisowej nadającej nowe hasło. Jeżeli w Portalu jest więcej niż jeden aktywny administrator, można za pomocą jego konta w Rejestrze użytkowników zmienić hasło innemu administratorowi (opis w *8.6.1 Lista użytkowników*).

11.3. Brak licencji na moduł w MIAM

W przypadku gdy licencja na moduł MIAM została dodana w programie mMedica, a mimo to występuje problem, należy w pierwszej kolejności sprawdzić, czy komponent ten łączy się do poprawnej bazy danych mMedica (plik [MIAM]\appsettings.json). W sytuacji, w której licencja na MIAM została dodana po jego instalacji, możliwa jest sytuacja, w której MIAM zapamięta stan braku licencji. W takim wypadku najprościej jest zrestartować komponent mMDAB według informacji zawartych *3.15. Restartowanie i zatrzymywanie komponentów* (Windows) oraz *4.12. Restartowanie i zatrzymywanie komponentów* (Linux).

11.4. Nieprawidłowe ustawienia Portalu – odtwórz. kopii bazy danych Archiwum

W takim przypadku należy wykonać restart komponentów. Procedura restartowania została zawarta w *3.15. Restartowanie i zatrzymywanie komponentów* (Windows), *4.12. Restartowanie i zatrzymywanie komponentów* (Linux).

11.5. Biała strona komponentu po instalacji przez instalator na IIS

Powodem takiej sytuacji jest zaznaczenie w instalatorze dla komponentu wymagania korzystania z SSL bez konfiguracji certyfikatu w IIS. Jeżeli wymaganie SSL zostało zaznaczone rozmyślnie, należy skonfigurować SSL zgodnie z *3.13.2. Konfiguracja certyfikatu SSL*. W innym przypadku istnieje możliwość wyłączenia opcji. W tym celu należy uruchomić Menedżer internetowych usług informacyjnych, następnie wybrać witrynę, w której zostały zainstalowane aplikacje (domyślnie „Default Web Site”). Z panelu środkowego wybrać „Ustawienia protokołu SSL” i odznaczyć pole „Wymagaj protokołu SSL”. Następnie kliknąć prawym przyciskiem myszy na witrynę (domyślnie „Default Web Site”) i wybrać opcję „Edytuj powiązania…”. Jeżeli w oknie brak jest typu „http”, należy go dodać opcją „Dodaj…” z portem 80. Jeżeli na liście powiązań widnieje typ „https”, to można go usunąć zaznaczając wiersz i wybierając opcję „Usuń”. Dodatkowo należy zaznaczyć witrynę i w menu „Zarządzaj witryną sieci Web” wybrać opcję „Rozpocznij” (jeśli witryna jest zatrzymana). Istnieje również możliwość późniejszej konfiguracji SSL zgodnie z podrozdziałem *3.13.2. Konfiguracja certyfikatu SSL*.

11.6. Błąd 403.4 na localhost lub na adresie komponentu na IIS

Rozwiązanie problemu zostało opisane w podrozdziale *11.5. Biała strona komponentu po instalacji przez instalator na IIS.*

11.7. Błąd 500.21 w IIS

Powodem błędu jest brak zainstalowanego modułu AspNetCoreModuleV2 dla IIS. Konieczne jest zainstalowanie lub zainstalowanie ponowne pakietu ASP.NET Core Windows Hosting – rozdział *3.4. Instalacja ASP .NET Core wraz z modułem* IIS. Warto również zapoznać się z rozdziałem dotyczącym ponownej instalacji ASP.NET Core Windows Hosting (patrz: *3.5. Instalacja IIS po instalacji ASP .NET* Core).

11.8. Błąd 502.5 w IIS

Błąd najczęściej jest spowodowany brakiem zrestartowania usługi IIS po instalacji ASP.NET Core Windows Hosting (patrz: *3.4. Instalacja ASP .NET Core wraz z modułem* IIS lub *3.5. Instalacja IIS po instalacji ASP*

.NET Core). Problem może również być wynikiem braku instalacji pakietu KB2533623 dla systemów Windows 7 SP1 oraz Windows Server 2008 R2 SP1 (więcej informacji w rozdziale *3.6. KB2533623 dla Windows 8.1, Windows Server* 2012 R2). Innym powodem błędu może być brak uprawnień do odczytu folderu komponentu przez pulę aplikacji – punkt *17* z *3.10. Instalacja manualna*.

11.9. Polecenie dotnet nie jest rozpoznawalne – Linux

Do poprawnego uruchomienia aplikacji wymagana jest instalacja środowiska ASP .NET Core. Proces instalacji opisany został w punkcie *5* w rozdziale *4.4. Instalacja wymaganego oprogramowania*. Jeżeli po dodaniu certyfikatu Microsoft, podczas próby zaktualizowania listy pakietów pojawi się problem związany z brakiem możliwości zweryfikowania podpisu, to pobierany jest certyfikat dla nieodpowiedniej wersji systemu. Przykładowy certyfikat dla Linux Ubuntu 20.04:

```
wget https://packages.microsoft.com/config/ubuntu/20.04/packages-microsoft-
prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
```

Na stronie https://docs.microsoft.com/pl-pl/dotnet/core/install/linux znajdują się instrukcje dla innych popularnych wersji systemu.

11.10. Status serwisu Main process exited – Linux

Błąd ten może wynikać z wielu przyczyn:

a) Brak uprawnień wykonywania dla pliku z rozszerzeniem .sh. Należy je wtedy dodać poprzez polecenie:

```
sudo chmod +x nazwa_pliku.sh
```

b) W pliku */etc/systemd/system/[*nazwa_serwisu*].service* została umieszczona błędna ścieżka do pliku wykonywalnego. Należy ja poprawić zgodnie z punktem *8* w rozdziale *0. Proces instalacji dla innych dystrybucji* Linux został opisany pod adresem: https://docs.microsoft.com/pl-pl/dotnet/core/install/ w poszczególnych działach.

c) Konfiguracja serwera oraz instalacja modułu.

d) W pliku *nazwa_pliku.sh* umieszczona została błędna ścieżka do pliku wykonywalnego. Należy ja poprawić zgodnie z punktem *7* w rozdziale *0. Proces instalacji dla innych dystrybucji* Linux został opisany pod adresem: https://docs.microsoft.com/pl-pl/dotnet/core/install/ w poszczególnych działach.

e) Konfiguracja serwera oraz instalacja modułu.

11.11. Brak portu w statusie usługi – Linux

Jeśli podczas sprawdzania statusu serwisu poprzez polecenie:

```
sudo systemctl status nazwa_serwisu.service
```

pojawił się komunikat o uruchomieniu aplikacji, ale brak informacji o tym na jakim porcie aplikacja została wystawiona, to najprawdopodobniej jest to związane z błędną konfiguracją komponentów. Więcej informacji można uzyskać uruchamiając plik wykonywalny *nazwa_pliku.sh* ręcznie. Poprzez komendę:

```
./nazwa_pliku.sh
```

W razie potrzeby należy poprawić konfigurację w pliku appsettings.json komponentu zgodnie z instrukcją *5. Konfiguracja aplikacji*. Możliwe jest również, że błąd wynika z braku odpowiedniego pakietu. Jeżeli podczas ręcznego uruchomienie wyświetlony zostanie komunikat o błędzie związanym z libunwind, należy go zainstalować zgodnie z punktem *3* w rozdziale *4.4. Instalacja wymaganego oprogramowania*.

11.12. Strona jest widoczna wyłącznie z komputera lokalnego

Należy sprawdzić, czy strona została właściwie powiązana z adresem, a także czy zapora ogniowa akceptuje ruch przychodzący na porcie działania usługi WWW.

11.13. Przekroczenie czasu realizacji operacji na bazie danych (timeout)

Możliwa jest edycja maksymalnego czasu wykonywania operacji na bazie danych dla każdego komponentu. W tym celu należy wpisać „CommandTimeout=WARTOSC” w pliku appsettings.config komponentu (sekcja „ConnectionString”). WARTOSC jest podawana w sekundach. Przykład dla 250 sekund i bazy danych Archiwum:

```
"ConnectionString": "Server=localhost,5432;Database=ARCHMMEDICA;CommandTimeout=250;"
```

11.14. Brak pliku api-ms-win-crt-runtime-l1-1-0 – Windows

W przypadku błędu informującego o braku pliku api-ms-win-crt-runtime-l1-1-0 podczas uruchomienia Archiwum należy zainstalować lub zaktualizować pakiet „Universal C Runtime in Windows”. Więcej informacji na stronie: https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows.

11.15. Błąd „Unspecified certificate from client” w mMedica

Jeśli w mMedica podczas komunikacji do eArchiwum (np. w teście połączenia) pojawia się błąd, w którego treści znajduje się fraza „Unspecified certificate from client” to oznacza, że niepoprawnie została skonfigurowana witryna zawierającą aplikację eArchiwum. Powodem błędu jest ustawienie protokołu SSL dla witryny na opcjonalne lub obligatoryjne przesyłanie certyfikatu klienta.

Konfiguracja w IIS:

a) Przejść w IIS do witryny z aplikacją eArchiwum.
b) Wybrać ze środkowego okna „Ustawienie protokołu SSL”.
c) Zmienić ustawienie „Certyfikaty klientów” na „Ignoruj”.
d) Zaleca się restart witryny.

Konfiguracja w apache:

a) Uruchomić w trybie edycji plik konfiguracyjny witryny eArchiwum.
b) Usunąć opcję „SSLVerifyClient” lub ustawić ją na „none”.
c) Zapisać plik konfiguracyjny witryny.
d) Przeładować konfiguracje apache lub wykonać jego restart.