

Roger Access Control System

VISO Web

Instrukcja obsługi

Wersja software: 2.0.4 lub nowsza

Wersja dokumentu: Rev. H

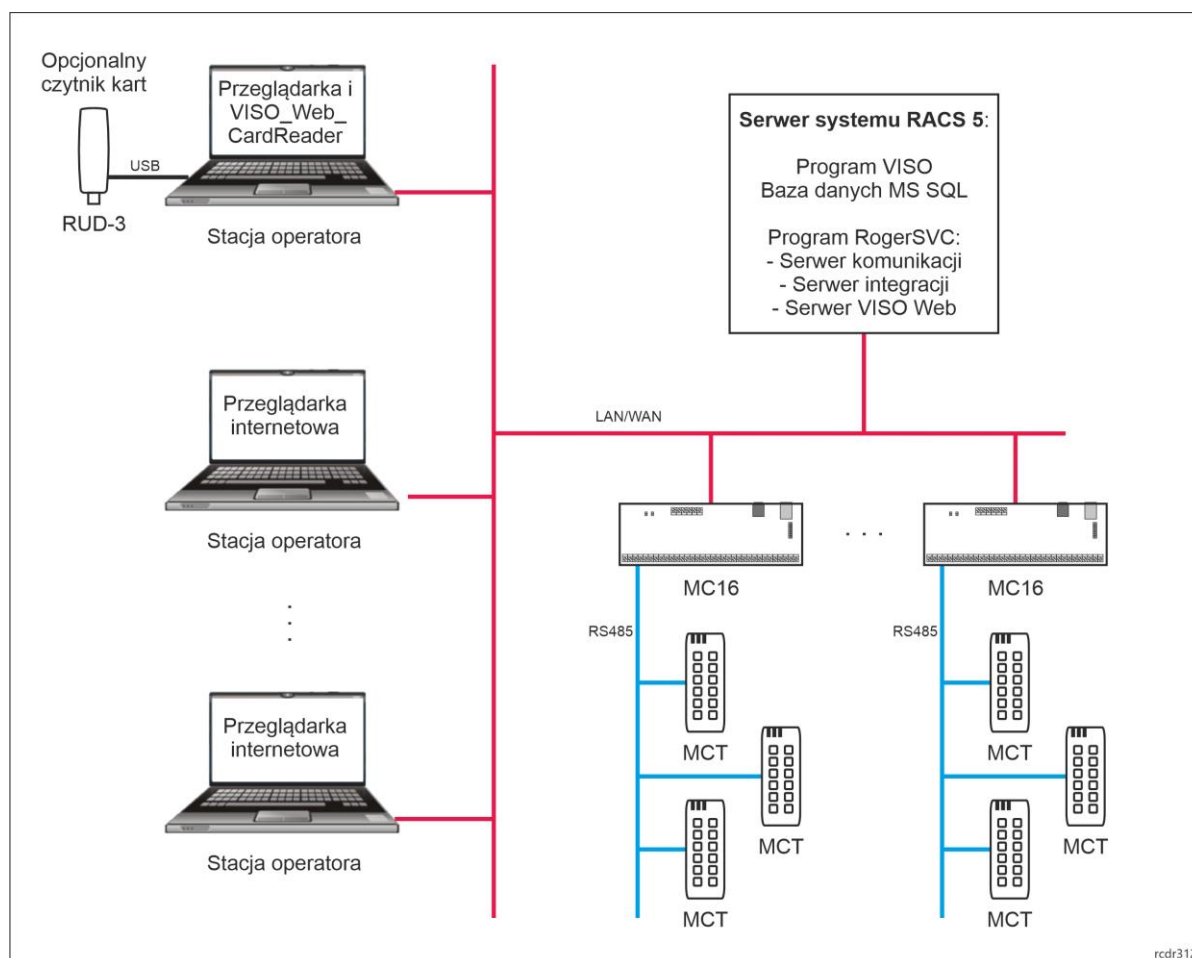
1. OPIS

Serwer VISO Web umożliwia zarządzanie i monitorowanie w systemie RACS 5 za pomocą przeglądarki internetowej. W takim scenariuszu pracy oprogramowanie VISO w wersji desktopowej jest niezbędne do skonfigurowania systemu w zakresie logiki funkcjonalnej tj. Przejść, Terminali dostępu, Linii wejściowych i wyjściowych, Uprawnień, Operatorów, itd. ale nie jest konieczne do codziennego zarządzania systemem. VISO Web umożliwia:

- Zarządzanie Grupami użytkowników, Osobami i Identyfikatorami
- Monitorowanie zdarzeń
- Przeglądanie historii zdarzeń
- Monitorowanie Przejść
- Monitorowanie Stref obecności
- Monitorowanie Węzłów automatyki
- Monitorowanie Stref alarmowych
- Wywoływanie Komend globalnych w systemie
- Przeglądanie i generowanie Raportów obecności



Uwaga: W przypadku VISO 1.4.2 lub nowszego, VISO Web może być stosowane także w ramach VISO ST a nie tylko licencjonowanego VISO EX.

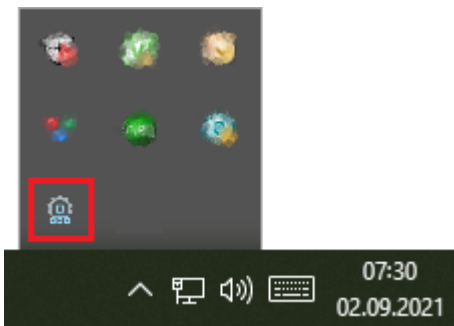
2. KONFIGURACJA SYSTEMU RACS 5



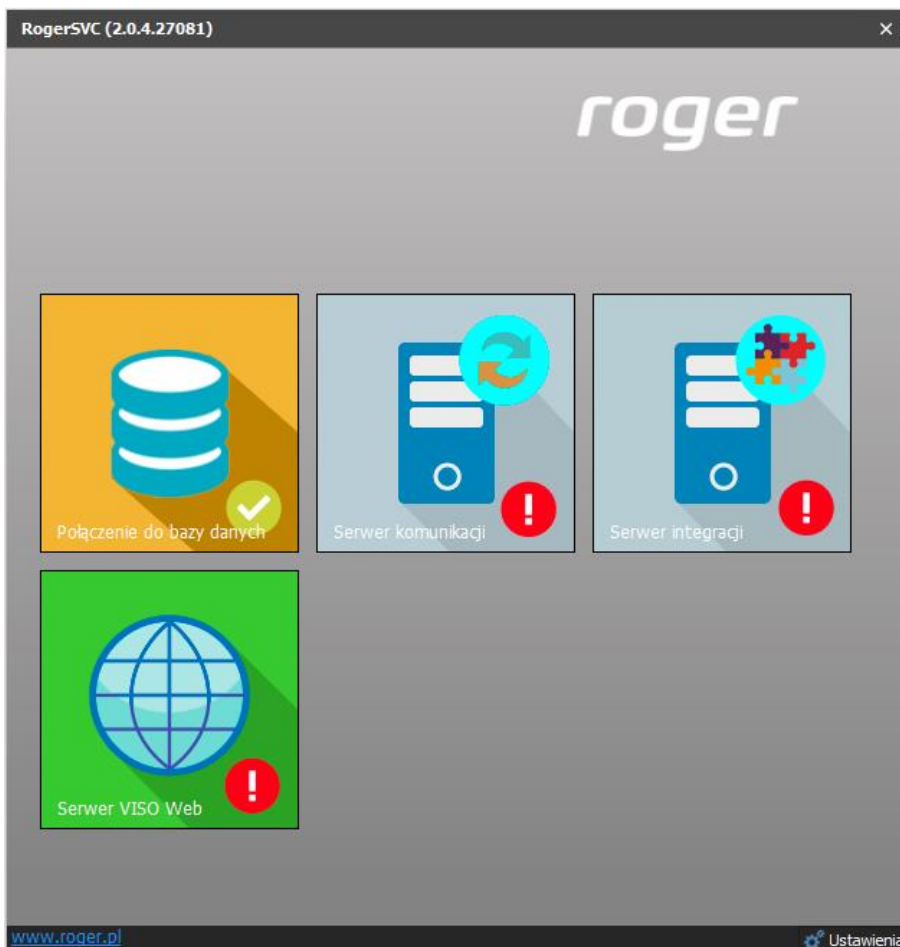
Rys. 1 Przykładowy ogólny schemat połączeń w systemie RACS 5 z wykorzystaniem VISO Web

W ramach wstępnej konfiguracji systemu RACS:

- Zainstaluj oprogramowanie VISO zgodnie z notą aplikacyjną AN006 tworząc serwerową bazę danych zgodnie z notą aplikacyjną AN017.
- Zainstaluj oprogramowanie RogerSVC zaznaczając nie tylko Serwer komunikacji ale również Serwer integracji i Serwer VISO Web. Jeżeli serwery mają działać na różnych komputerach to zainstaluj program RogerSVC oddzielnie na każdej maszynie wybierając odpowiednie serwery.
- Uruchom program RogerSVC wybierając *Start->ROGER->RogerSVC* w systemie Windows.
- W zasobniku kliknij ikonę  programu RogerSVC ( w starszych wersjach).



- W oknie RogerSVC wybierz kafelek *Połączenie do bazy danych* i wybierając *Konfiguracja* wskaż wcześniej utworzoną bazę danych systemu RACS 5. Wróć do okna głównego.




- W oknie RogerSVC wybierz kafelek *Serwer komunikacji*, kliknij polecenie *Konfiguracja* a następnie wprowadź adres IP komputera na którym działa serwer np. 192.168.11.13 i zdefiniuj port do komunikacji z serwerem (domyślnie 8890).

- Wybierz *Uruchom* i wróć do okna głównego. Serwer będzie działać w tle zawsze gdy uruchomiony jest komputer, także po zamknięciu okna programu RogerSVC.
- W oknie RogerSVC wybierz kafelek *Serwer integracji*, Wybierz *Uruchom* i wróć do okna głównego. Serwer będzie działać w tle zawsze gdy uruchomiony jest komputer, także po zamknięciu okna programu RogerSVC.
- Uruchom program VISO i skonfiguruj system RACS 5 w zakresie Przejść, Punktów identyfikacji, Uprawnień, Użytkowników itd. zgodnie z notą aplikacyjną AN006.
- Dodatkowo zdefiniuj Operatora(-ów) programu VISO definiując ich dane do logowania oraz Role. Login i hasło Operatora jest niezbędne do tego by osoba korzystająca z dostępu przez przeglądarkę internetową mogła zalogować się do systemu RACS 5. . Więcej informacji na temat Operatorów i Ról podano w notce aplikacyjnej AN040.
- W razie potrzeby na serwerze RACS 5 z programem RogerSVC uruchom Zaporę systemu Windows z zabezpieczeniami zaawansowanymi i dodaj nową zezwalającą regułę przychodzącą dla protokołu TCP i portu Serwera integracji (domyślnie 8892) oraz nową zezwalającą regułę przychodzącą dla protokołu TCP i portu Serwera VISO Web (domyślnie 8080)


3. URUCHOMIENIE ŚRODOWISKA VISO WEB

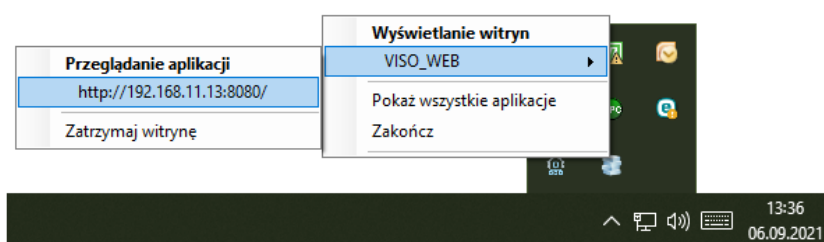
Metoda 1 - Konfiguracja Serwera VISO Web z poziomu Roger SVC

- Zainstaluj na serwerze oprogramowanie Internet Information Services (IIS) 10 Express ze strony firmy Microsoft np. z poniższego linku:
- <https://www.microsoft.com/pl-pl/download/details.aspx?id=48264>
- Uruchom RogerSVC i kliknij jego ikonę  w zasobniku Windows. Następnie wybierz kafelek *Serwer VISO Web* i następnie zdefiniuj adres IP oraz port pod którym będzie funkcjonował serwer w sieci (np. 192.168.11.13:8080). Te ustawienia będą stosowane na stacjach Operatorów do połączenia się z systemem RACS 5 przez przeglądarkę internetową. Jeżeli Serwer integracji działa na tym samym komputerze to można pozostawić jego domyślny adres IP i port czyli 127.0.0.1:8892.
- Wybierz *Uruchom* i wróć do okna głównego. Serwer będzie działać w tle zawsze gdy uruchomiony jest komputer, także po zamknięciu okna programu RogerSVC.

Uwaga: W przypadku próby uruchomienia Serwera VISO Web za pomocą programu RogerSVC poprzez zdalny pulpit mogą wystąpić problemy z uprawnieniami operatora Windows. W takim przypadku uruchom program Roger.Racs.WebAppService.exe ręcznie z uprawnieniami administratora w folderze RogerSVC (domyślna ścieżka C:\Program Files (x86)\Roger\RogerSVC).

Uwaga: W przypadku restartu serwera RACS 5, Serwis aplikacji VISO Web może wystartować wcześniej niż IIS. Nie będzie on wtedy działał dopóki nie zrestartuje się go ręcznie w programie RogerSVC. Aby trwale rozwiązać ten problem można w systemie Windows przejść do *Zarządzania komputerem*, wybrać *Usługi i aplikacje*, następnie *Usługi* i we właściwościach *RACSWebAppService* ustawić *Typ uruchomienia* na *Automatycznie (opóźnione uruchamianie)*.

- Po uruchomieniu Serwera VISO Web uruchomiony zostanie IIS Express, którego ikona  będzie widoczna w zasobniku systemu Windows. Kliknij tą ikonę prawym przyciskiem myszy.



Rys. 2 Oprogramowanie IIS

- Po kliknięciu adresu w polu *Przeglądanie aplikacji* uruchomi się przeglądarka internetowa z oknem umożliwiającym zalogowanie się do systemu RACS 5. Można również uruchomić samemu przeglądarkę i wpisać adres IP oraz port Serwera VISO Web. W podanym przykładzie byłoby to adres 192.168.11.13:8080. Pierwsze uruchomienie może zająć nawet do 1 minuty.
- W wyświetlonym oknie podaj login i hasło wcześniej utworzonego Operatora programu VISO lub użyj loginu Admin i zdefiniowanego dla niego hasła.

Problem z uprawnieniami

Jeżeli po zainstalowaniu IIS Express i uruchomieniu Serwera VISO Web nie pojawia się ikona IIS Express w zasobniku Windows to może to oznaczać, że uprawnienia użytkownika serwera do uruchomienia IIS Express w ramach określonej części obszaru nazw URL protokołu HTTP są za niskie. Należy wtedy z poziomu konsoli cmd, uruchomionej z uprawnieniami administratora, wykonać komendę dodania rezerwacji adresu URL dla grupy użytkowników (lub użytkownika):

```
netsh http add urlacl url=http://AdresStrony:Port/ user=Wszyscy
```

np. netsh http add urlacl url=http://192.168.11.13:8080/ user=Wszyscy

Do ewentualnego usunięcia rezerwacji adresu URL można wykorzystać komendę:

```
netsh http delete urlacl url=http://AdresStrony:Port/
```

np. netsh http delete urlacl url=http://192.168.11.13:8080/

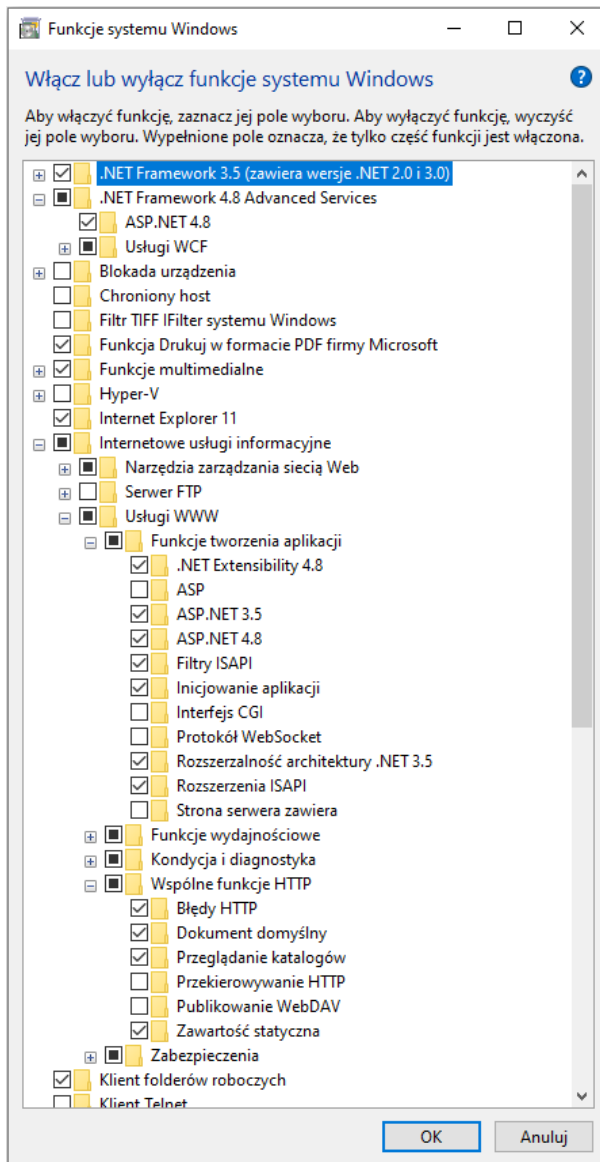
Problem z połączeniem

W przypadku problemów z połączeniem na poziomie przeglądarki internetowej może być konieczne nadanie uprawnień użytkownikowi Windows do zapisu w lokalizacji C:\ProgramData\WebAppService. W tym celu kliknij folder WebAppService prawym przyciskiem myszki, wybierz *Właściwości*, następnie zakładkę *Zabezpieczenia* i nadaj uprawnienia do zapisu.

Metoda 2: Konfiguracja i zarządzanie usługą IIS z poziomu systemu Windows 10

Aktywacja funkcji systemu Windows

Środowisko IIS dostępne jest w systemach operacyjnych Windows. W celu jego aktywacji w Panelu sterowania Windows wybierz polecenie *Programy i funkcje* i następnie *Włącz lub wyłącz funkcje systemu Windows*. W otwartym oknie zaznacz opcje jak na rys.3. Może istnieć konieczność aktualizacji niektórych składników w oparciu o funkcjonalności Windows Update. Wymagania te należy zaakceptować (pobierane i instalowane są automatycznie przez system Windows).



Rys. 3 Minimalny zestaw funkcji Windows 10 do obsługi IIS

W celu dokończenia konfiguracji środowiska serwera IIS należy zarejestrować technologie ASP.NET. W zależności od wersji systemu Windows można zastosować poniższe komendy:

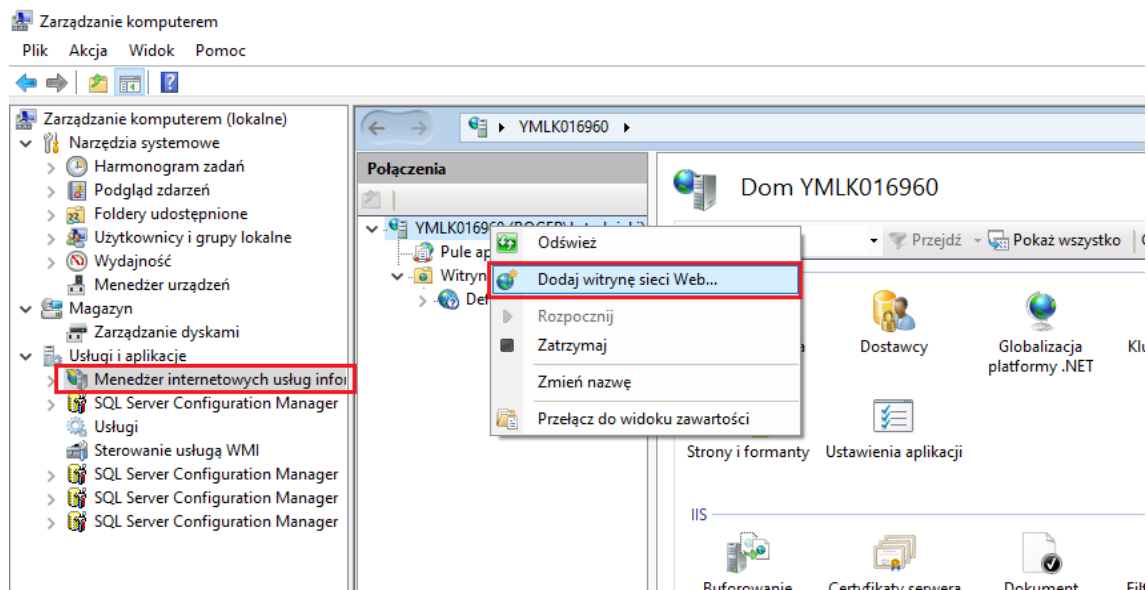
Dla systemów 32bit:

```
%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -ir
```

Dla systemów 64bit:

```
%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -ir
```

Po zainstalowaniu środowiska, dalsza konfiguracja jest możliwa po uruchomieniu *Zarządzania komputerem*, wybraniu opcji *Usługi i aplikacje* i następnie *Menedżera internetowych usług informacyjnych (IIS)*.

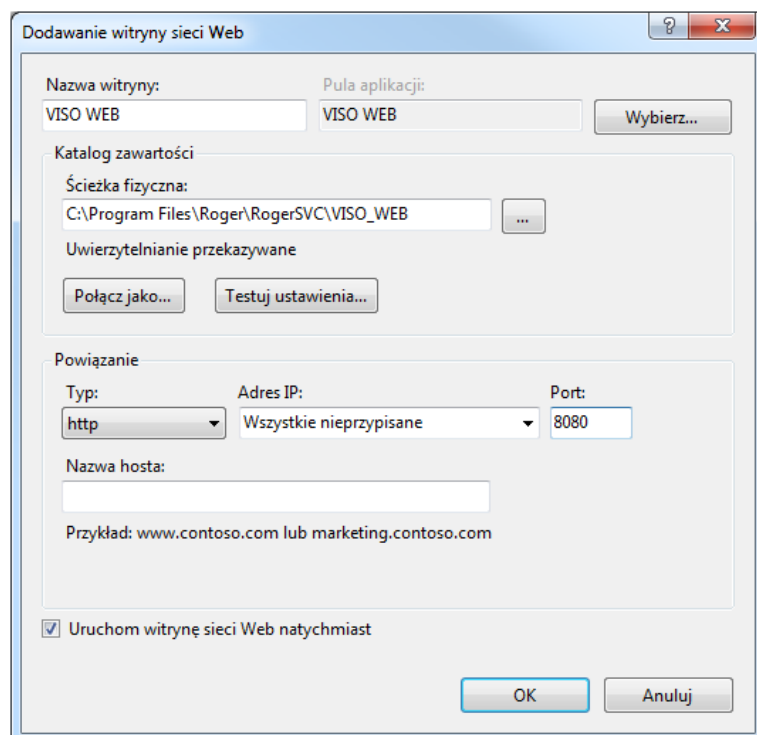


Rys. 4 Widok Menedżera internetowych usług informacyjnych (IIS)

Dodanie witryny sieci Web

Podczas dodawania witryny sieci Web należy uzupełnić parametry zgodnie z posiadaną konfiguracją. Przykładowa konfiguracja:

- *Nazwa witryny: VISO WEB*
- *Ścieżka fizyczna: C:\Program Files\ROGER\RogerSVC\VISO_WEB (w przypadku systemów starszych niż RACS 5 v2: C:\Program Files (x86)\ROGER\RogerSVC\VISO_WEB).*
- *Port: 8080*



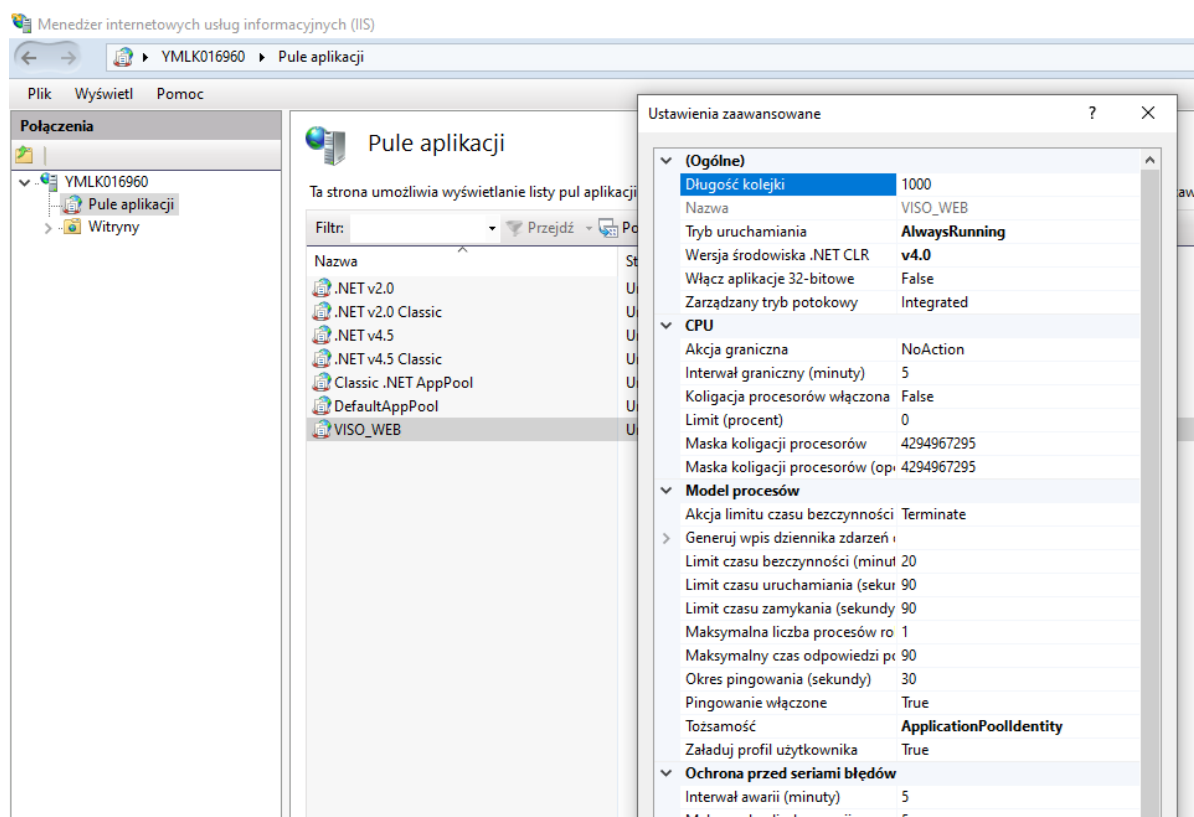
Rys. 5 Okno dodawania witryny VISO WEB

Konfiguracja puli aplikacji

Po utworzeniu witryny VISO Web aplikacja tworzona jest automatycznie. W celu dostosowania jej do wymagań VISO Web należy wprowadzić następujące parametry:

- *Wersja środowiska .NET CLR: v.4.0*
- *Tryb uruchamiania: AlwaysRunning*
- *Włącz aplikacje 32-bitowe: False (True w przypadku systemów starszych niż RACS 5 v2)*
- *Tożsamość: ApplicationPoolIdentity*

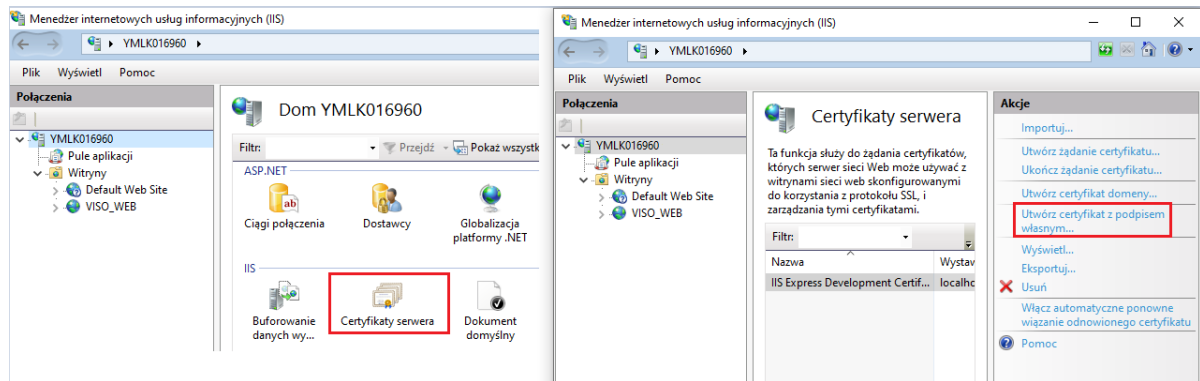
Pozostałe wartości nie wymagają zmian i mogą przyjmować wartości domyślne. W przypadku parametru *Tożsamość* można zmienić ustawienia na *Konto niestandardowe*. Przy takiej konfiguracji należy się upewnić, że wybrany operator ma wystarczające uprawnienia do zarządzania usługą IIS oraz dostęp do katalogu C:\Program Files\ROGER\RogerSVC\VISO_WEB a w przypadku systemów starszych niż RACS 5 v2 do katalogu C:\Program Files (x86)\ROGER\RogerSVC\VISO_WEB



Rys. 6 Ustawienia zaawansowane aplikacji VISO Web

Komunikacja zabezpieczona (HTTPS)

Komunikacja pomiędzy Serwerem VISO Web a przeglądarką jest realizowana za pomocą typowego protokołu HTTP. Możliwe jest jednak zabezpieczenie tej komunikacji poprzez jej szyfrowanie zgodnie z protokołem HTTPS. W tym celu konieczne jest zastosowanie odpowiednich certyfikatów. Jedną z możliwych metod polega na zdefiniowaniu certyfikatu serwera IIS jak poniżej gdzie po dwukrotnym kliknięciu ikony *Certyfikaty serwera* możliwe jest zdefiniowanie certyfikatu z podpisem własnym.



Rys. 7 Certyfikat serwera IIS z podpisem własnym

Komunikacja w sieci WAN

System RACS 5 może być obsługiwany przez przeglądarkę internetową nie tylko w sieci LAN czy VPN ale również w sieci WAN. Taką komunikację można uzyskać np. poprzez tunelowanie, które oferuje serwis ngrok.com. W tym celu:

- Utwórz konto w serwisie ngrok.com w zalecanej wersji PRO.
- Po zalogowaniu do konta wybierz *Endpoints->Domains* i zdefiniuj unikalną nazwę domeny dla VISO np. *viso.eu.ngrok.io*.
- Wybierz *Getting started->Your Authtoken* i odczytaj wartość tokena do późniejszego wykorzystania np. *1xIXCEfDzu5adBQ4yi8CrW2zQuT_2jSk7e3DFjo3fk6Zfwf61*.
- Pobierz program ngrok.exe i zapisz na komputerze z zainstalowanym Serwerem VISO Web (np. 192.168.11.13) w przykładowej lokalizacji *C:\NGROK* i następnie utwórz w tej lokalizacji tekstowy plik konfiguracyjny *ngrok.yml* o przykładowej zawartości:

```
authtoken: 1xIXCEfDzu5adBQ4yi8CrW2zQuT_2jSk7e3DFjo3fk6Zfwf61
```

```
region: eu
```

```
tunnels:
```

```
demo:
```

```
proto: http
```

```
addr: 192.168.11.13:8080
```

```
hostname: viso.eu.ngrok.io
```

```
bind-tls: true
```

- Uruchom tunelowanie przykładową komendą z linii poleceń cmd Windows:

```
ngrok start demo -config C:\ngrok\ngrok.yml
```

Ewentualnie dodaj również uruchamianie tunelowania w autostarcie systemu Windows tak by uruchamiało się ono automatycznie podczas uruchamiania komputera.

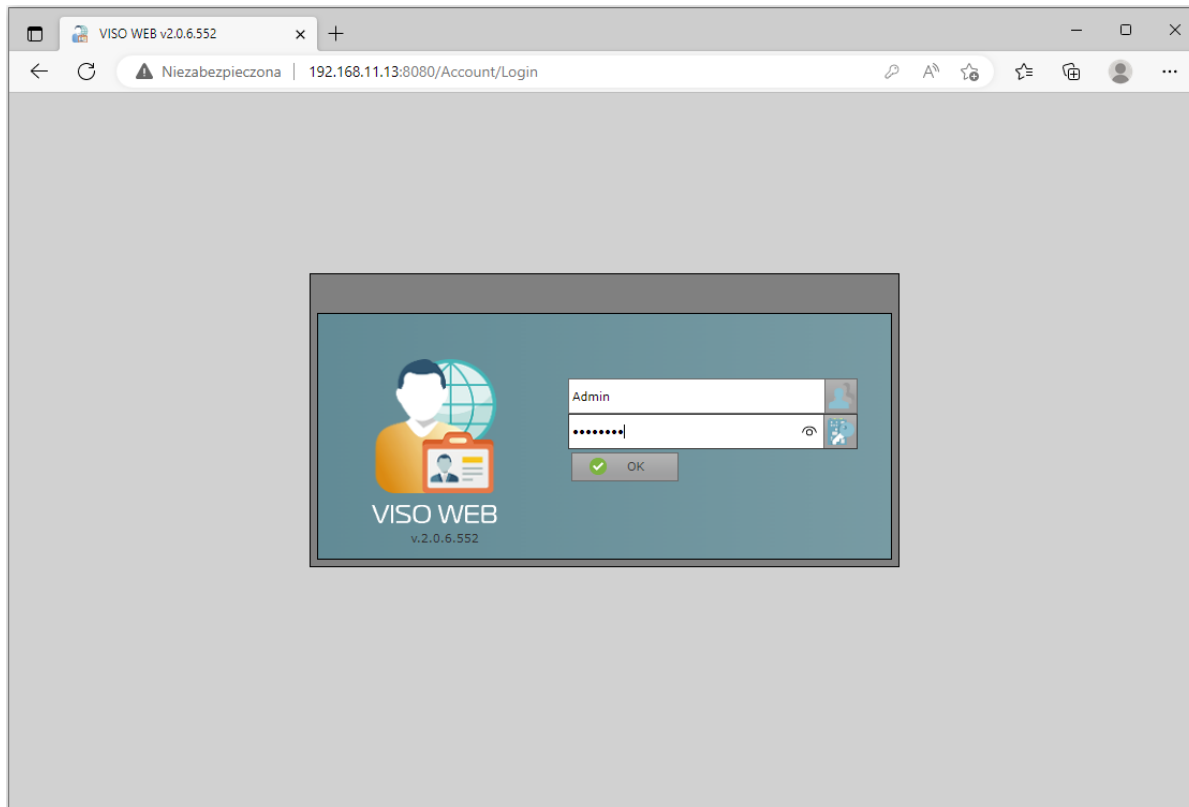
- Po uruchomieniu tunelowania wpisz w przeglądarce *viso.eu.ngrok.io* by następnie zalogować się do systemu RACS 5.

Uwaga: Więcej informacji na temat opisanego tunelowania podano w dokumentacji serwisu ngrok.

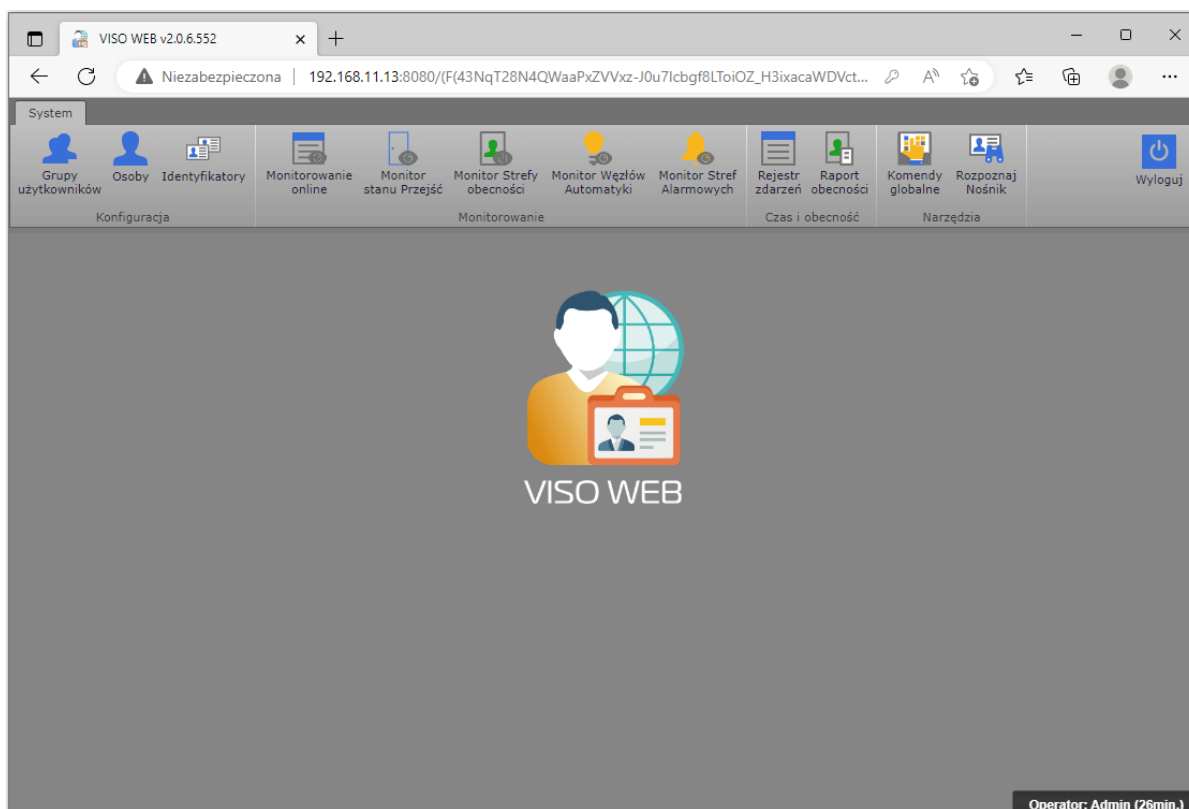
Uwaga: Podana w przykładzie opcja *bind-tls:true* ogranicza tunelowanie do szyfrowanego protokołu HTTPS.

4. URUCHOMIENIE I OBSŁUGA APLIKACJI VISO WEB

Bez względu na sposób uruchomienia IIS, aplikacja VISO Web dostępna jest dla wszystkich komputerów będących w sieci serwera RACS 5 i jej uruchomienie jest realizowane z poziomu przeglądarki internetowej. Aby uzyskać dostęp do aplikacji w przeglądarce należy wpisać adres strony VISO Web oraz port (np. 192.168.11.13:8080). Logowanie do VISO Web wymaga podania loginu i hasła operatora zdefiniowanego w programie VISO.



Rys. 8 Okno logowania



Rys. 9 Okno główne

Uwaga: Jeżeli aplikacja VISO Web jest uruchamiana na tym samym komputerze co VISO Web Serwer to użytkownik Windows musi mieć prawa do zapisu w folderach:

```
...\\RogerSVC\VISO_WEB\App_Data\UploadTemp
...\\RogerSVC\VISO_WEB\Content\Images\Temp
...\\RogerSVC\VISO_WEB
```

Uwaga: Jeżeli w momencie nawiązywania połączenia wyświetla się błąd 'HTTP Error 503. The service is unavailable' to w systemie Windows wybierz *Start*, następnie *Uruchom* i wpisz poniższą komendę:

```
"%systemroot%\system32\inetsrv\AppCmd.exe" set config -
section:system.webServer/globalModules
/[name='SPNativeRequestModule'].preCondition:integratedMode,bitness64
```

Definiowanie użytkownika

W odróżnieniu od programu VISO, aplikacja VISO Web nie daje możliwości definiowania Uprawnień (praw dostępu) ale pozwala stosować i przypisywać Uprawnienia z listy utworzonej wcześniej za pomocą programu VISO.

Metoda 1:

- W oknie głównym wybierz *Identyfikatory*, następnie przycisk *Dodaj*, wprowadź nazwę i zatwierdź by utworzyć Identyfikator. Jako nazwę można podać imię i nazwisko użytkownika, który będzie stosował ten Identyfikator.
- W dolnej części ekranu wybierz zakładkę *Nośniki* i następnie *Dodaj* by dodać do Identyfikatora kartę i/lub PIN. W nowo otwartym oknie wybierz typ a następnie wprowadź numer karty lub kod PIN i zatwierdź przyciskiem *OK*. Jeżeli do stacji operatora do portu USB podłączony jest czytnik serii RUD (np. RUD-3) i w tle uruchomiony jest program VISO Web CardReader to zamiast wpisywania numeru karty można go automatycznie odczytać wybierając przycisk *Odczytaj z czytnika*. Domyślna lokalizacja programu VISO Web CardReader to C:\Program Files (x86)\Roger\RogerSVC\VISO_WEB\CardReader.

- W dolnej części ekranu wybierz zakładkę *Uprawnienia* i/lub *Grupy Uprawnień* i za pomocą przycisku *Przypisz* wskaż, które z Uprawnień utworzonych wcześniej za pomocą programu VISO będą przypisane temu Identyfikatorowi.

Metoda 2:

- Zdefiniuj listę Identyfikatorów z przypisanymi Nośnika za pomocą programu VISO lub VISO Web.
- W oknie głównym wybierz *Grupy użytkowników* i zdefiniuj grupy za pomocą przycisku *Dodaj*. Każdej grupie w dolnej części ekranu poprzez zakładkę *Uprawnienia* przypisz wcześniej utworzone za pomocą programu VISO Uprawnienia.
- W oknie głównym wybierz *Osoby* i za pomocą przycisku *Dodaj* zdefiniuj użytkownika przypisując go do wybranej Grupy użytkowników.
- W dolnej części ekranu wybierz zakładkę *Identyfikatory* i przypisz Identyfikator(-y) z przypisanymi wcześniej Nośnikami (kartami/PIN-ami).

Monitorowanie online

Monitorowanie online w VISO Web działa analogicznie do monitorowania online w programie VISO i umożliwia wyświetlanie na bieżąco zdarzeń w momencie ich wystąpienie w systemie.

Monitor stanu Przejść

Monitor stanu Przejść w VISO Web działa analogicznie do Monitora stanu Przejść w programie VISO i umożliwia uzyskiwanie na bieżąco informacji na temat stanu otwarcia oraz trybu przejść na liście.

Dodatkowo możliwe jest również wydawanie komend dla wybranego Przejścia za pomocą przycisku *Komenda zdalna*. W ramach komendy dostępne są funkcje zmiany Trybu Drzwi, zdalnego otwarcia Przejścia, kasowania alarmów Przejścia, itp. Użycie Komendy zdalnej wymaga Uprawnienia przypisanego do operatora programu VISO. Aby Operator mógł zdalnie sterować Przejściem to musi być przypisany do Osoby posiadającej Identyfikator z Uprawnieniem do funkcji [121]...[136]. Takie powiązanie Osoby z Operatorem jest realizowane w programie VISO we właściwościach Osoby w zakładce *Zdalne zarządzanie* w polu *Operator*. Najprostszą metodą nadania wszystkich możliwych Uprawnień Operatorowi jest przypisanie go do Osoby z Identyfikatorem, który ma załączoną opcję *Wyjątek Master*. Domyślnie operator Admin nie jest przypisany do żadnej Osoby. Więcej informacji na temat Operatorów podano w nocie aplikacyjnej AN040.

Monitor Strefy obecności

Monitor Strefy Obecności działa analogicznie do Monitora Strefy Obecności w programie VISO i umożliwia monitorowanie na bieżąco którzy użytkownicy aktualnie znajdują się w wybranej Strefie obecności a którzy są po za nią. Strefy obecności definiuje się za pomocą programu VISO. Dodatkowo w przypadku VISO v1.6.6 i starszych monitor wymaga uruchomienia procesu monitorowania Stref Obecności w programie VISO po wybraniu w menu górnym polecenia *Narzędzia* i następnie ikony *Procesy Serwera Komunikacji*.

Monitor Węzłów Automatyki

Monitor Węzłów Automatyki działa analogicznie do Monitora Węzłów Automatyki w programie VISO i umożliwia uzyskiwanie na bieżąco informacji na temat stanu Węzłów Automatyki w systemie.

Możliwe jest również wydawanie komend dla wybranego węzła za pomocą przycisku *Komenda zdalna*. W ramach komendy dostępne są funkcje załączania, wyłączania i przełączenia węzła z różnymi opcjami czasowymi. Użycie Komendy zdalnej wymaga Uprawnienia przypisanego do Operatora programu VISO. Aby Operator mógł zdalnie sterować węzłami to musi być przypisany do Osoby posiadającej Identyfikator z Uprawnieniem do funkcji [145]...[168]. Takie powiązanie Osoby z Operatorem jest realizowane w programie VISO we właściwościach Osoby w zakładce *Zdalne zarządzanie* w polu *Operator*. Najprostszą metodą nadania wszystkich możliwych Uprawnień Operatorowi jest przypisanie go do Osoby z Identyfikatorem, który ma załączoną opcję *Wyjątek Master*. Domyślnie operator Admin nie jest przypisany do żadnej Osoby. Więcej informacji na temat Operatorów podano w nocie aplikacyjnej AN040.

Monitor Stref Alarmowych

Monitor Stref Alarmowych działa analogicznie do Monitora Stref Alarmowych w programie VISO i umożliwia uzyskiwanie na bieżąco informacji na temat stanu Stref Alarmowych.

Możliwe jest również wydawanie komend dla wybranej Strefy Alarmowej za pomocą przycisku *Komenda zdalna*. W ramach komendy dostępne są funkcje uzbrajania, rozbrajania i przezbrajania strefy. Użycie Komendy zdalnej wymaga Uprawnienia przypisanego do Operatora programu VISO. Aby Operator mógł zdalnie sterować Strefami Alarmowymi to musi być przypisany do Osoby posiadającej Identyfikator z Uprawnieniem do funkcji [104]...[109] i/lub [222]...[223]. Takie powiązanie Osoby z Operatorem jest realizowane w programie VISO we właściwościach Osoby w zakładce *Zdalne zarządzanie* w polu *Operator*. Najprostszą metodą nadania wszystkich możliwych Uprawnień Operatorowi jest przypisanie go do Osoby z Identyfikatorem, który ma załączoną opcję *Wyjątek Master*. Domyślnie operator Admin nie jest przypisany do żadnej Osoby. Więcej informacji na temat Operatorów podano w nocie aplikacyjnej AN040.

Rejestr zdarzeń

Rejestr zdarzeń w VISO Web działa analogicznie do rejestru zdarzeń w programie VISO i umożliwia przeglądanie zdarzeń zarejestrowanych w systemie z zastosowaniem definiowalnego filtru.

Raport obecności

Raport obecności w VISO Web działa analogicznie do tego co oferuje program VISO i wymaga zdefiniowania Strefy obecności za pomocą programu VISO.

Możliwe jest generowanie raportu obecności zawierającego czasy wejścia oraz wyjścia ze strefy jak też całkowity czas przebywania danej Osoby w strefie. Operator generujący raport dla danej Osoby lub Osób musi być prawidłowy powiązany z nimi tak jak to opisano w nocie aplikacyjnej AN016. Raport można eksportować w formacie PDF i XLS.

Komendy globalne

Komendy globalne definiuje się na poziomie programu VISO i można je wywoływać na poziomie programu VISO Web. Komendy globalne podobnie jak opisane powyżej Komendy zdalne wymagają powiązania operatora programu VISO z użytkownikiem posiadającym Uprawnienie do funkcji realizowanych przez Komendę globalną i umożliwiają one wykonanie wielu funkcji w wielu miejscach systemu jednocześnie. Komenda globalna może być wywołana na żądanie operatora systemu np. do awaryjnego otwarcia wszystkich przejść w systemie. Komendy globalne są realizowane przez Serwer komunikacji systemu. Więcej informacji na temat Komend Globalnych podano w nocie aplikacyjnej AN048.

Rozpoznaj Nośnik

Funkcjonalność działa tak jak w przypadku programu VISO i pozwala zidentyfikować użytkownika systemu na podstawie odczytu karty.

Kontakt:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Faks: +48 55 272 0133
Pomoc tech.: +48 55 267 0126
Pomoc tech. (GSM): +48 664 294 087
E-mail: pomoc.techniczna@roger.pl
Web: www.roger.pl