Roger Access Control System 5v2

Nota aplikacyjna nr 021

Wersja dokumentu: Rev. B

Integracja Active Directory

Uwaga: Niniejszy dokument dotyczy RACS 5 v2.0.8 lub nowszy

Wprowadzenie

System RACS 5 umożliwia integrację z usługami katalogowymi do których zalicza się usługę Active Directory, czyli hierarchiczną bazą danych zawierającą informacje o użytkownikach, grupach użytkowników, komputerach, a także zasobach w sieciach firmowych z serwerami Windows firmy Microsoft. Usługa Active Directory pozwala administratorom sieci zarządzać całym zbiorem użytkowników w sieci, określać ich uprawnienia do zasobów sieciowych, a także konfigurować komputery, na których pracują.

Integracja systemu RACS 5 z usługą Active Directory (AD) umożliwia:

- Uwierzytelnianie operatora logującego się do programu VISO za pomocą AD
- Ręczną synchronizację listy użytkowników systemu RACS 5 z listą użytkowników AD
- Automatyczną synchronizację listy użytkowników systemu RACS 5 z listą użytkowników AD

Korzyści z synchronizacji polegają na tym, że lista użytkowników danej organizacji może być zarządzana z jednego miejsca (Active Directory) a jej zmiany mogą być uwzględniane w systemie kontroli dostępu RACS 5. Na podstawie nazwy jednostki organizacyjnej (OU) do której należy użytkownik tworzona jest Grupa użytkowników o odpowiadającej jej nazwie i użytkownik jest do niej przypisywany. Ponieważ Grupy użytkowników mogą mieć przypisywane Uprawnienia w programie VISO to przypisanie użytkownika do danej jednostki w AD po imporcie będzie jednocześnie skutkować nadaniem mu Uprawnień w systemie kontroli dostępu RACS 5.

Uwaga: Automatyczna synchronizacja w odróżnieniu od uwierzytelniania operatora oraz ręcznej synchronizacji wymaga wykupienia licencji.

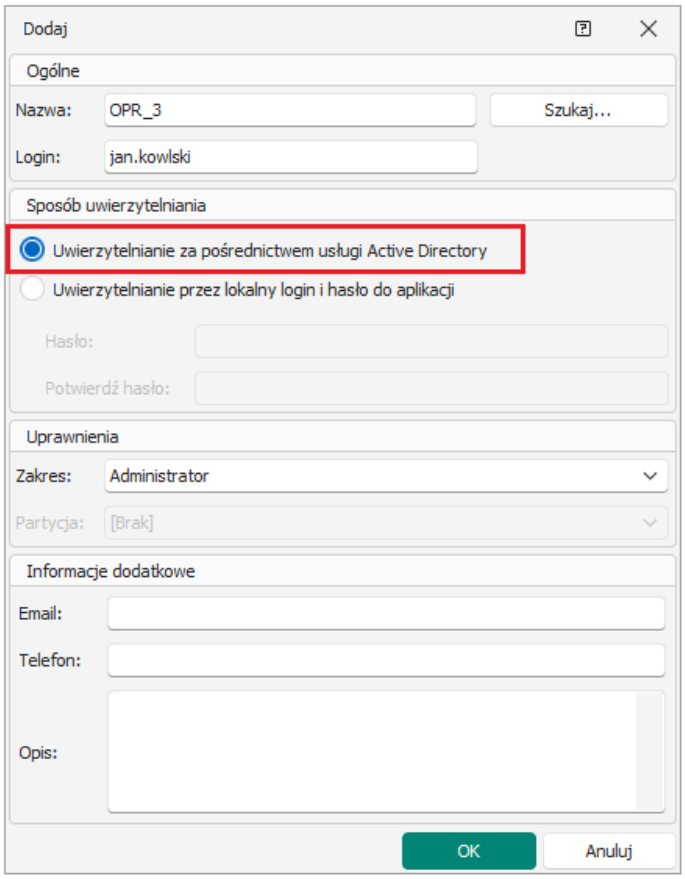
Uwierzytelnianie operatora

W systemie RACS 5, którego uruchomienie opisano w nocie aplikacyjnej AN006 automatycznie tworzony jest Operator ‘Admin’. Z kolei zgodnie z notą aplikacyjną AN040 istnieje możliwość definiowania wielu Operatorów programu VISO do zarządzania systemem kontroli dostępu RACS 5 jak też definiowanie ich uprawnień do poszczególnych obszarów programu VISO (np. zarządzanie użytkownikami, dostęp do monitorów i mapy, itp.)

Operator logując się do programu VISO musi podać swój login oraz hasło, które zostały zdefiniowane w bazie danych systemu RACS 5. Alternatywnie, do logowania się w programie VISO można wykorzystywać login i hasło, które zdefiniowano w domenie usługi Active Directory. Dzięki temu Operator nie musi dysponować oddzielnymi danymi do logowania i przede wszystkim można zarządzać hasłami z poziomu jednego systemu czyli Active Directory. Aby skonfigurować uwierzytelnianie za pomocą usługi Active Directory:

- Utwórz użytkownika w domenie Active Directory

- Uruchom program VISO i w menu górnym wybierz *Administracja* i następnie *Operatorzy*.
- W otwartym oknie wybierz *Dodaj* by zdefiniować nowego Operatora lub *Edytuj* by zmienić dane istniejącego Operatora.
- W kolejnym oknie w polu *Login* podaj login użytkownika utworzonego w Active Directory i wybierz *Uwierzytelnianie za pośrednictwem usługi Active Directory*.



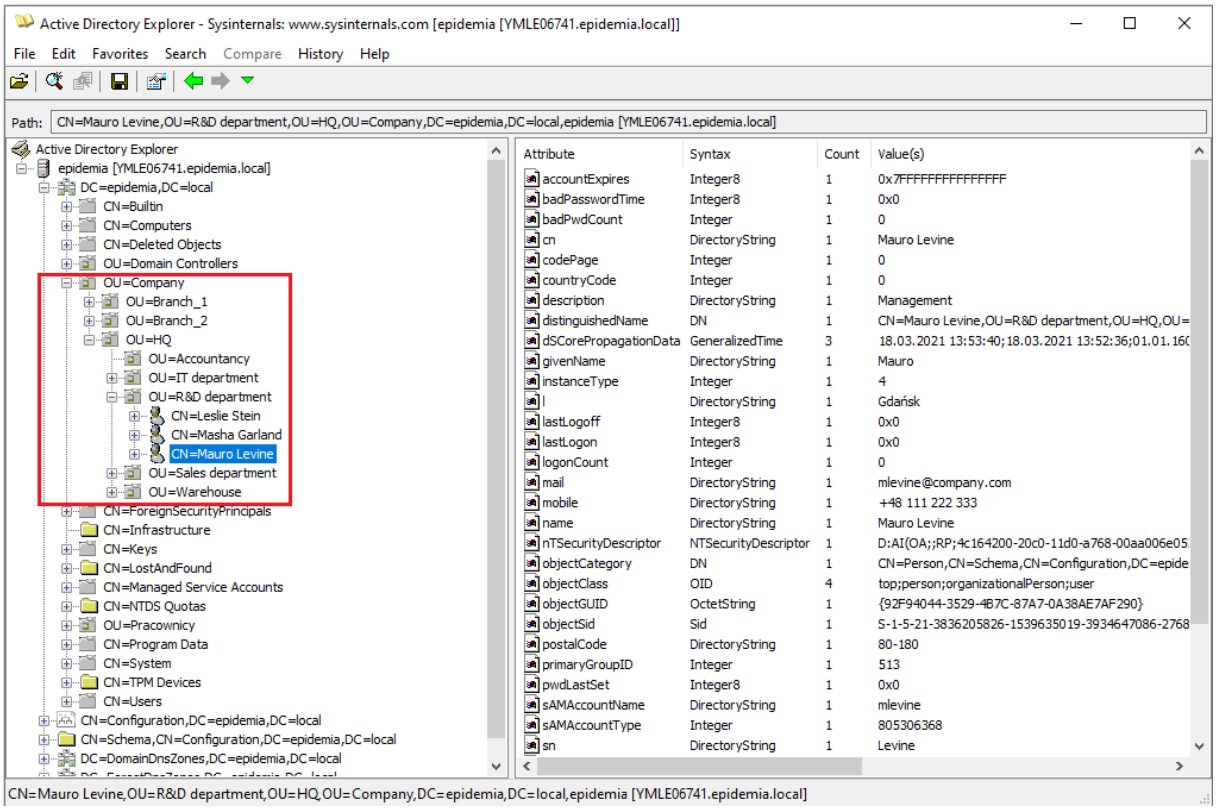
Ręczna synchronizacja użytkowników

Synchronizacja ręczna umożliwia pobranie listy użytkowników z usługi katalogowej (AD) na żądanie operatora programu VISO. Import dotyczy atrybutów AD podanych w *VISO->Narzędzia->Mapowanie atrybutów*. Możliwe jest definiowanie własnych mapowań tak jak opisano to kolejnych sekcjach noty.

Import użytkowników

Aby zaimportować użytkowników:

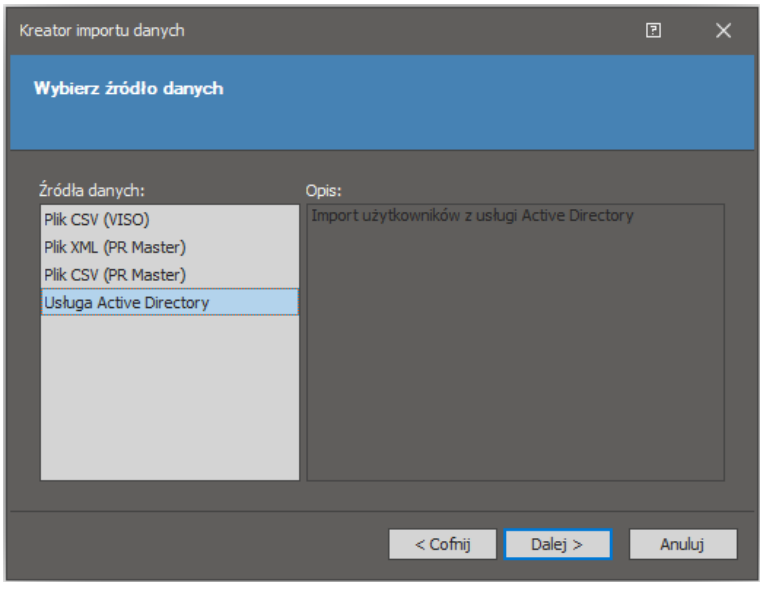
- Skonfiguruj system RACS 5 w zakresie Serwera komunikacji, bazy danych, kontrolerów, Przejść, Uprawnień, itd. zgodnie z notą aplikacyjną AN006.
- Utwórz użytkowników w domenie Active Directory w poszczególnych kontenerach typu jednostka organizacyjna (OU) jak w przykładzie poniżej. Później w trakcie importu będzie możliwe wskazanie jednostek, z których mają być pobierane dane.
- Zdefiniuj użytkownikom takie dane jak imię, nazwisko i opcjonalnie email, nr telefonu, adres, opis i inne.



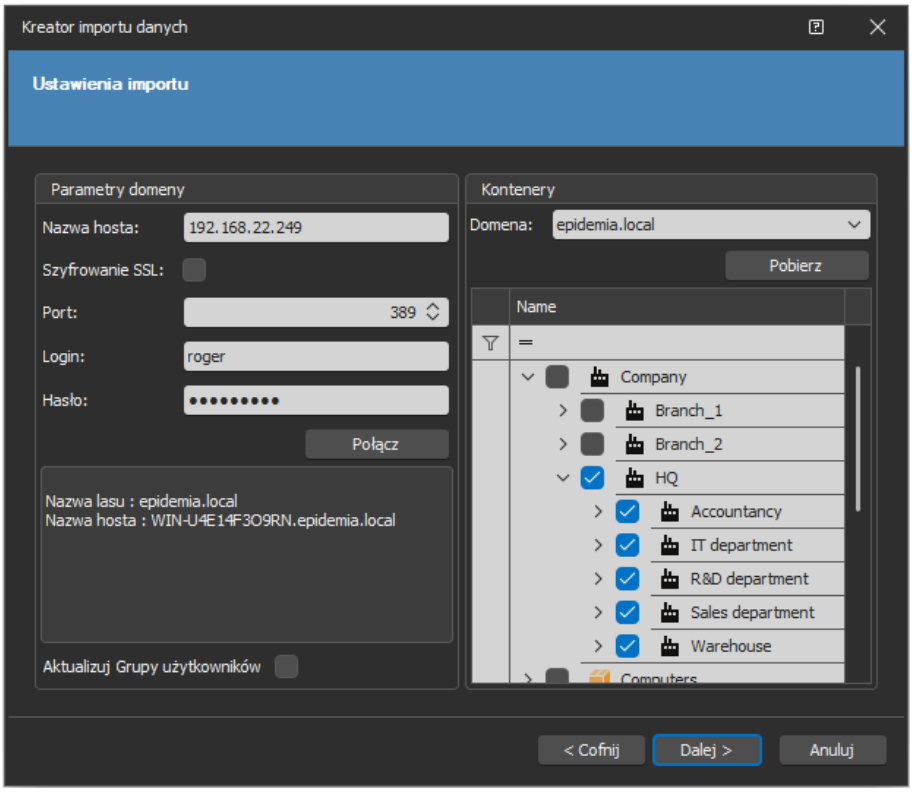
- Uruchom program VISO i w menu górnym wybierz *System* i następnie *Import…*

Uwaga: Komputer z zainstalowanym programem VISO musi być zalogowany do domeny Active Directory po to by mógł pobierać z niej dane. Szczegółowy zakres pobieranych danych zależy od nadanych uprawnień w AD.

- W otwartym oknie wybierz *Dalej*, następnie *Usługa Active Directory* i znowu *Dalej*.

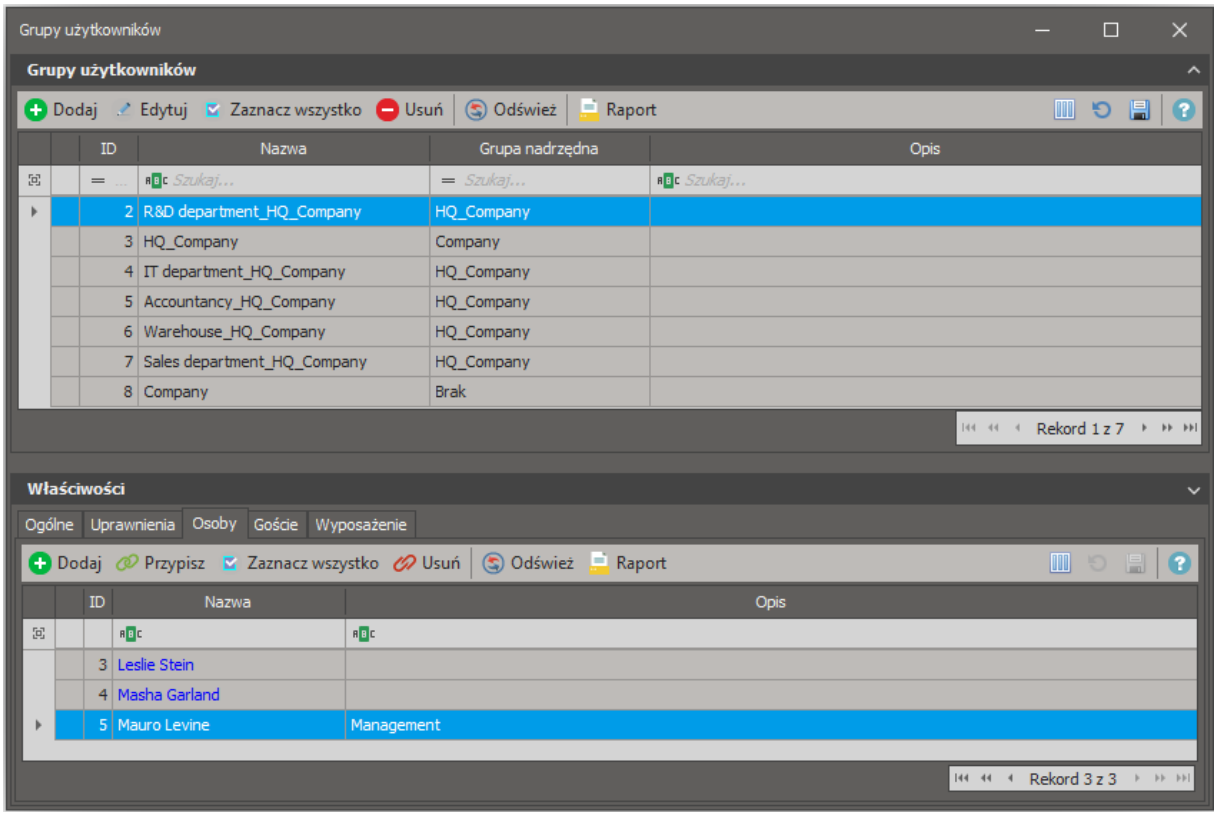


- W kolejnym oknie wprowadź parametry domeny, kliknij *Połącz*, wybierz domenę i następnie *Pobierz*. Na liście zaznacz z których kontenerów typu OU mają być zaimportowani użytkownicy. Jeżeli zaznaczona jest opcja *Aktualizuj Grupy użytkowników* to użytkownicy, którzy po wcześniejszym imporcie z AD zostali ręcznie przeniesieni w VISO do innych grup w ramach bieżącego importu zostaną z powrotem przeniesieni do grup wynikających z przyporządkowania w AD.

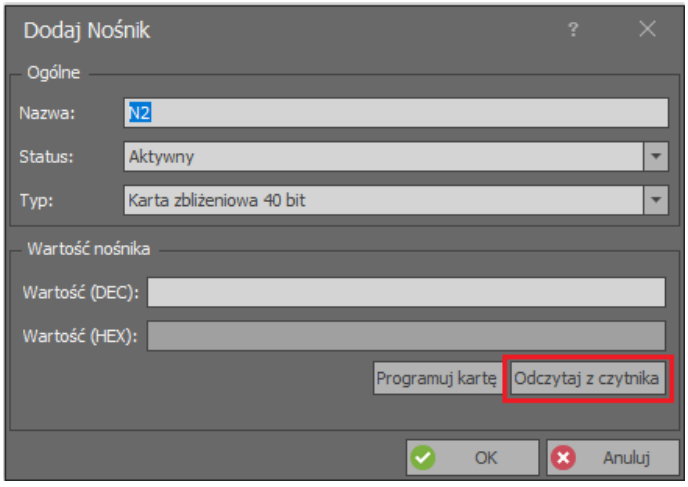


Uwaga: Użytkownicy zostaną pobrani tylko z tych jednostek, które zostaną zaznaczone i jedynie ci którzy są bezpośrednio przypisani w danych jednostkach. Przykładowo jeżeli zostanie zaznaczona jednostka *HQ* a nie zostanie zaznaczona jednostka *IT department* to pobrani zostaną jedynie użytkownicy utworzeni bezpośrednio w jednostce *HQ* i nie zostaną pobrani użytkownicy z jednostki podrzędnej *IT department* dopóki nie zostanie ona zaznaczona.

- W kolejnym oknach wybierz *Dalej* a w ostatnim oknie *Zakończ* by zaimportować użytkownik z AD. Przy imporcie pomijane są inne obiekty np. drukarki i pobierani są jedynie użytkownicy czyli obiekty z atrybutem sAMAccountType=805306368.
- W menu górnym programu VISO wybierz *Konfiguracja* i następnie *Grupy użytkowników*. Jeżeli nie istniały Grupy użytkowników w systemie RACS 5, które odpowiadałyby nazwom jednostek w AD to grupy zostaną automatycznie utworzone i użytkownicy zostaną do nich przypisani.
- W dolnej części ekranu wybierz zakładkę *Uprawnienia* i następnie przypisz wcześniej utworzone Uprawnienia do danej grupy. Wszystkie Osoby należące do tej grupy będą miały takie same Uprawnienia do poszczególnych Przejść i innych obiektów systemu RACS 5.
- Opcjonalnie wybierz zakładkę *Osoby*, kliknij nazwę danej Osobę i w otwartym oknie w zakładce *Uprawnienia* przypisz indywidualne Uprawnienia. W takim układzie Osoba będzie dysponować nie tylko Uprawnieniami wynikającymi z przynależności do grupy ale również swoimi indywidualnymi Uprawnieniami.

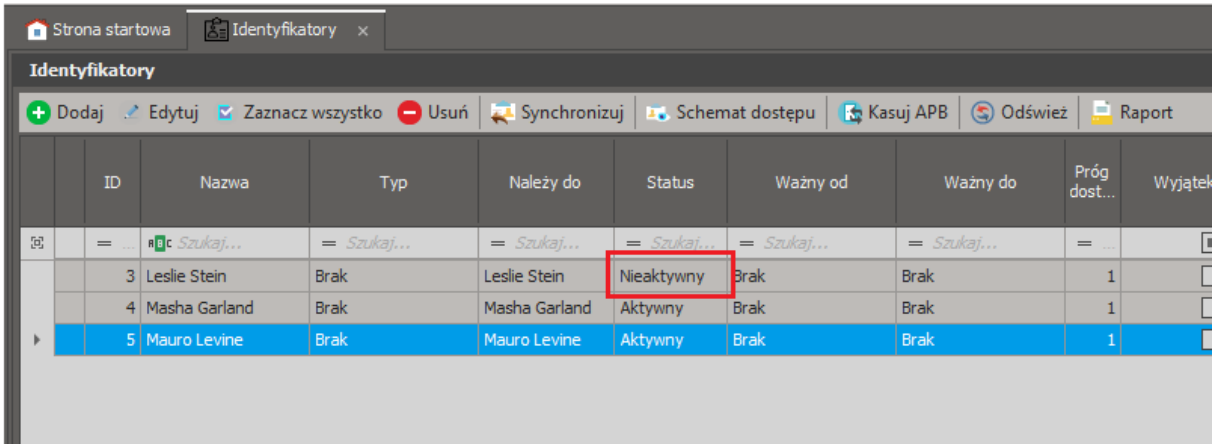


- W menu górnym programu VISO wybierz *Konfiguracja* i następnie *Identyfikatory*.
- Dla Identyfikatora danej Osoby w dolnej części ekranu wybierz zakładkę *Nośniki* i następnie *Dodaj* by zdefiniować kartę, kod PIN lub inny typ Nośnika, który będzie mógł być wykorzystywany do identyfikacji na czytnikach systemu RACS 5. Numer karty można odczytać na czytniku administratora typu RUD podłączonym do portu USB komputera lub dowolnym czytniku zainstalowanym w systemie.



Dezaktywacja i usuwanie użytkowników

Każdorazowy import użytkowników z AD będzie aktualizował ich dane w systemie RACS 5. Jeżeli konto użytkownika zostanie dezaktywowane w AD, to po imporcie Identyfikator tej Osoby będzie również nieaktywny w bazie danych systemu RACS 5. Jeżeli użytkownik zostanie usunięty w AD to po imporcie taka Osoba oraz jej Identyfikator zostaną również usunięte z bazy danych systemu RACS 5.



Synchronizacja z kontrolerami MC16

Po synchronizacji bazy danych systemu RACS 5 z kontrolerami dostępu MC16, użytkownicy z Identyfikatorami nieaktywnymi jak też usunięci użytkownicy tracą możliwość identyfikacji na czytnikach systemu RACS 5.

Taka synchronizacja w systemie RACS 5 może być wywoływana na żądanie poprzez kliknięcie prawym przyciskiem serwera komunikacji i następnie *Synchronizuj* w drzewku nawigacyjnym programu VISO lub może być wywoływana automatycznie poprzez harmonogram synchronizacji, który definiuje się poleceniem *Harmonogramy* w drzewku nawigacyjnym programu VISO i przypisuje się we właściwościach serwera komunikacji.

Automatyczna synchronizacja użytkowników

Synchronizacja automatyczna umożliwia pobieranie listy użytkowników z usługi katalogowej (AD) w tle, bez udziału operatora i zgodnie ze zdefiniowaną częstotliwością. Ta synchronizacja jest realizowana przez kontroler wirtualny z pakietu oprogramowania RogerSVC i wymaga licencji na poziomie oprogramowania VISO. Import dotyczy atrybutów AD podanych w *VISO->Narzędzia->Mapowanie atrybutów*. Możliwe jest definiowanie własnych mapowań tak jak opisano to kolejnych sekcjach noty.

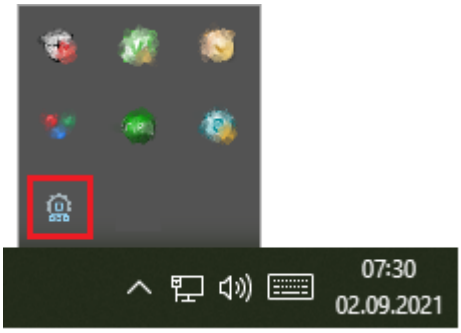
Wstępna konfiguracja systemu RACS 5

W ramach wstępnej konfiguracji systemu RACS:

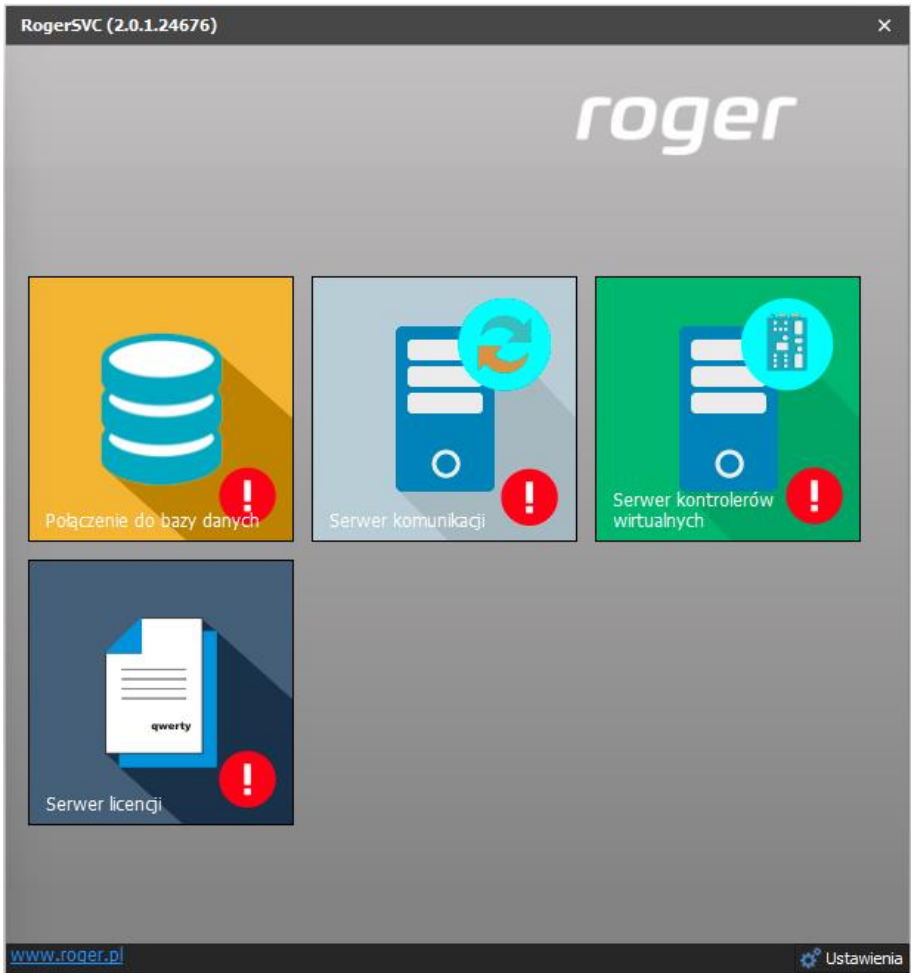
- Zainstaluj oprogramowanie VISO i utwórz bazę danych zgodnie z notą aplikacyjną AN006.
- Zainstaluj oprogramowanie RogerSVC zaznaczając nie tylko Serwer komunikacji ale również Serwer licencji i Serwer kontrolerów wirtualnych. Jeżeli serwery mają działać na różnych komputerach to zainstaluj program RogerSVC oddzielnie na każdej maszynie wybierając odpowiednie serwery.

Uwaga: Jeżeli Serwer licencji i Serwer kontrolerów wirtualnych mają funkcjonować na osobnych komputerach to podczas instalacji Serwera kontrolerów wirtualnych w ramach oprogramowania RogerSVC koniecznie odznacz instalację Serwera licencji. Tylko w takim układzie podczas późniejszej konfiguracji Serwera kontrolerów wirtualnych będzie możliwe wskazanie Serwera licencji działającego na innym komputerze.

- Jeżeli program RogerSVC jest uruchomiony to w zasobniku Windows kliknij jego ikonę  . Ikonę RogerSVC w zasobniku można wywołać również poprzez menu *Start-> Roger-> RogerSVC.*

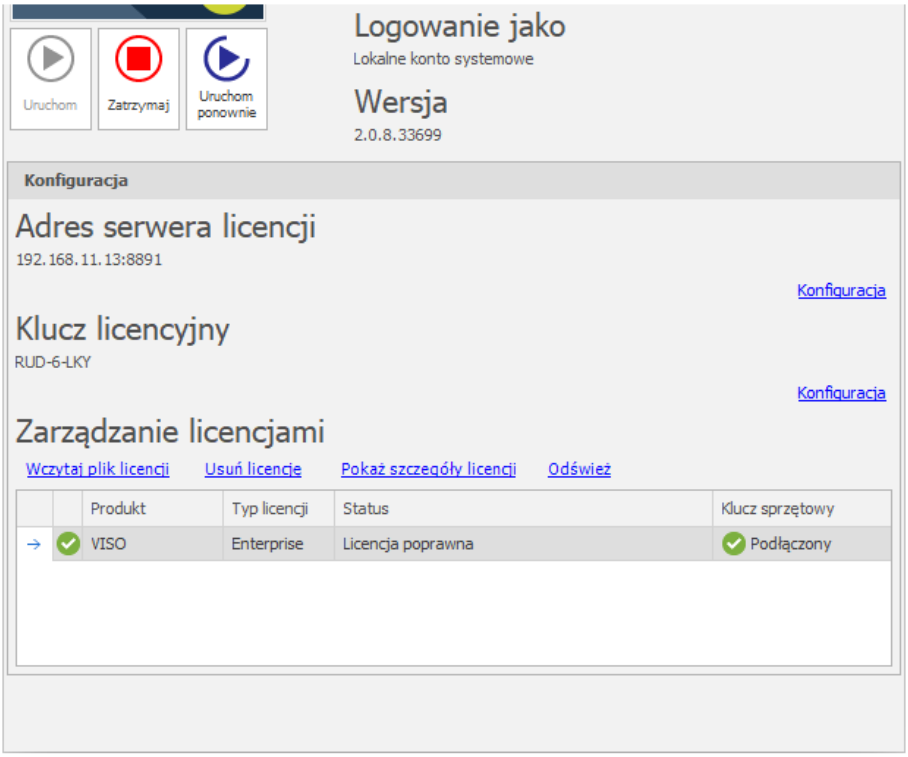


- W oknie RogerSVC wybierz kafelek *Połączenie do bazy danych* i wybierając *Konfiguracja* wskaż wcześniej utworzoną bazę danych systemu RACS 5. Wróć do okna głównego.

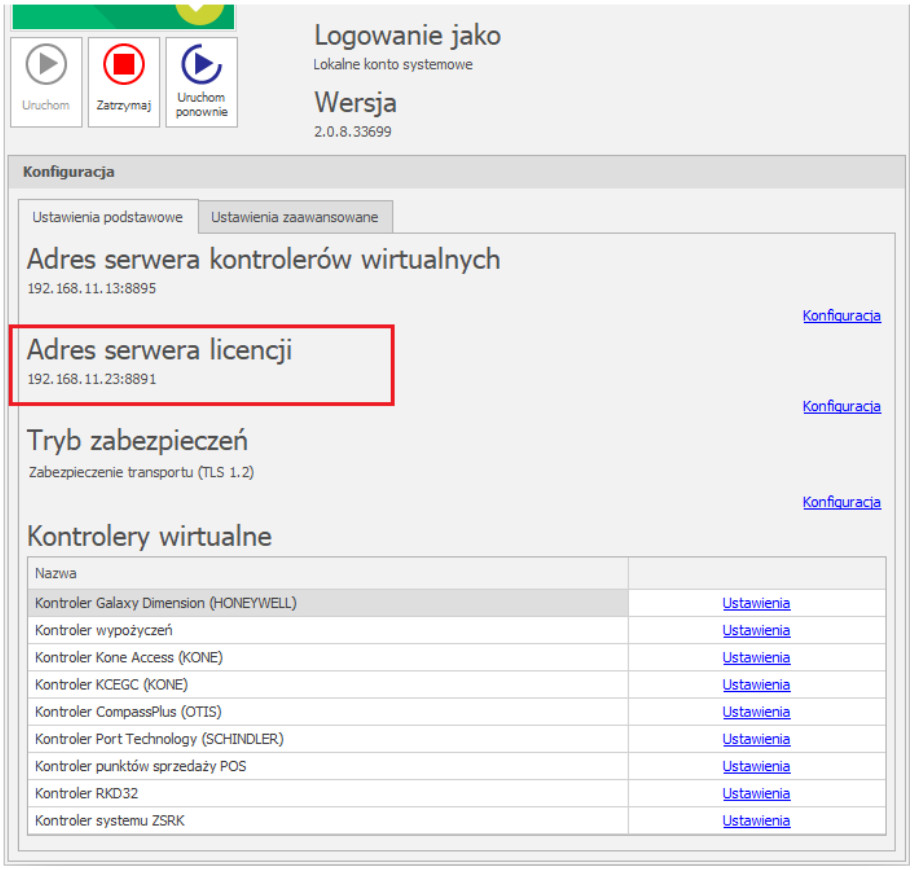


- W oknie RogerSVC wybierz kafelek *Serwer komunikacji,* kliknij polecenie *Konfiguracja* a następnie wprowadź adres IP komputera na którym działa serwer np. 192.168.11.13 i zdefiniuj port do komunikacji z serwerem (domyślnie 8890).
- Wybierz *Uruchom* i wróć do okna głównego. Serwer będzie działać w tle zawsze gdy uruchomiony jest komputer, także po zamknięciu okna programu RogerSVC.
- Podłącz klucz sprzętowy RUD-6-LKY do portu USB komputera z zainstalowanym Serwerem licencji lub klucz sprzętowy RLK-1 do sieci LAN wskazując jego adres IP w RogerSVC.
- W oknie RogerSVC wybierz kafelek *Serwer licencji*, 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 8891).
- Wybierz polecenie *Wczytaj plik licencji* i wskaż zakupiony plik licencji dla klucza sprzętowego.

- 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 kontrolerów wirtualnych*, 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 8895).
- Jeżeli inaczej niż wcześniej pokazano, Serwer licencji nie został zainstalowany na tym samym komputerze co Serwer kontrolerów wirtualnych czyli na komputerze z adresem 192.168.11.13 bo został zainstalowany na innym komputerze np. z adresem 192.168.11.23 to wtedy można wskazać ten Serwer licencji dla kontrolerów wirtualnych jak w przykładzie poniżej.

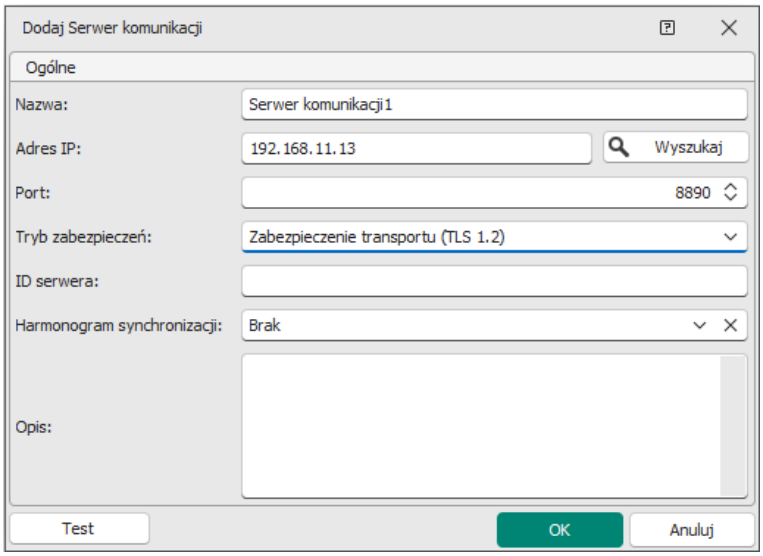


- Wybierz *Uruchom* i wróć do okna głównego. Serwer będzie działać w tle zawsze gdy uruchomiony jest komputer, także po zamknięciu okna programu RogerSVC.
- Uruchom program VISO, w menu górnym wybierz *System*, następnie *Wybierz serwer licencji* i wskaż na liście wcześniej zdefiniowany Serwer Licencji z pakietu oprogramowania RogerSVC aby uruchomić program w wersji licencjonowanej.

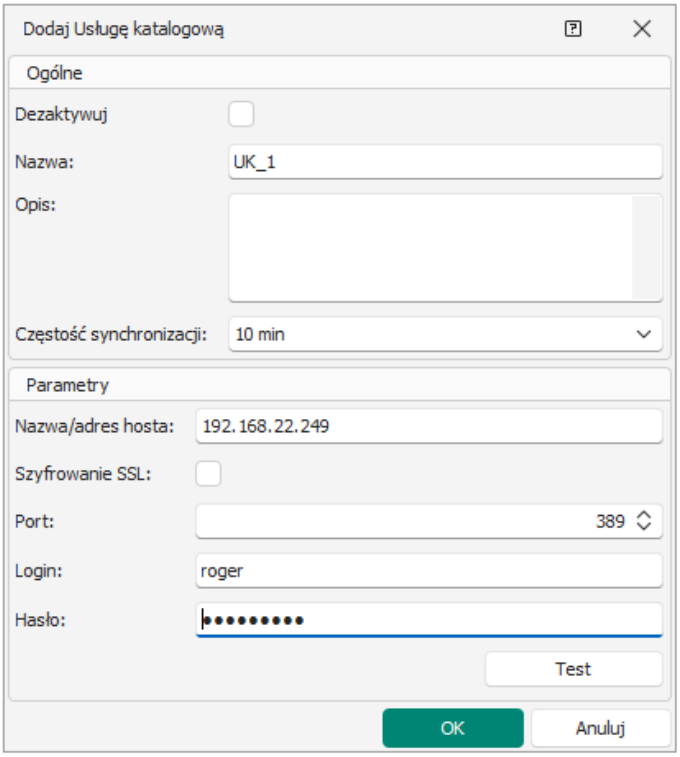
Konfiguracja połączenia i import użytkowników

Aby skonfigurować kontroler wirtualny:

- Jeżeli w programie VISO nie został jeszcze dodany Serwer komunikacji to w drzewku nawigacyjnym programu VISO kliknij prawym przyciskiem *Sieci* i następnie wybierz *Dodaj Serwer komunikacji*.
- W otwartym oknie wprowadź parametry Serwera komunikacji wcześniej skonfigurowane w programie RogerSVC i następnie zamknij okno przyciskiem *OK*. Zalecane jest stosowanie trybu TLS 1.2 do szyfrowania komunikacji.

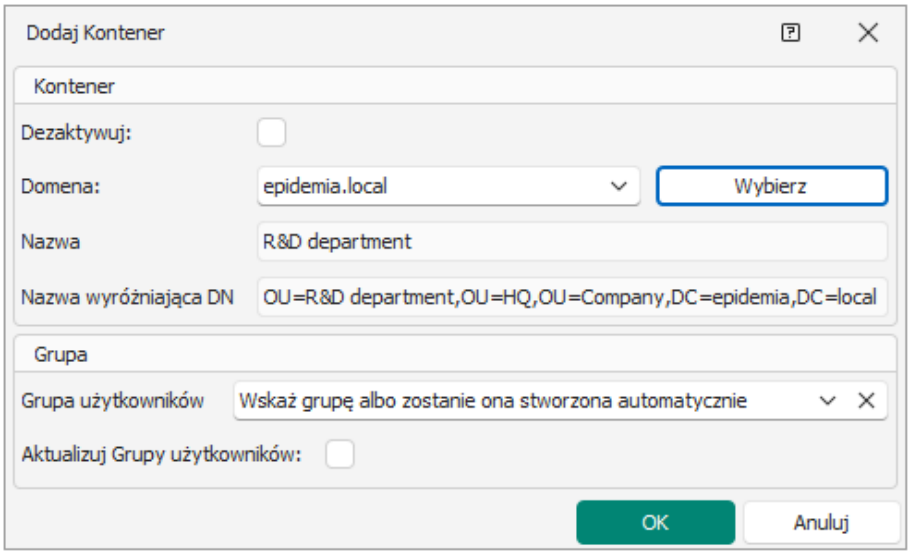


- W drzewku nawigacyjnym kliknij prawym przyciskiem myszki *Serwer kontrolerów wirtualnych* i następnie wybierz *Dodaj Serwer*. W otwartym oknie wprowadź parametry Serwera kontrolerów wirtualnych wcześniej skonfigurowane w programie RogerSVC i następnie kliknij przycisk *OK.* Zalecane jest stosowanie trybu TLS 1.2 do szyfrowania komunikacji.
- W drzewku nawigacyjnym kliknij prawym przyciskiem myszki dodany serwer i następnie wybierz *Dodaj Kontroler wirtualny*. W kategorii *Inne sytemy* wybierz *Kontroler usług katalogowych*. Jeżeli na liście wyboru nie widać kontrolera to najprawdopodobniej oznacza to problem z licencją na poziomie programu VISO lub RogerSVC. Zamknij okno przyciskiem OK.
- W drzewku nawigacyjnym programu VISO dwukrotnie kliknij *Kontroler usług katalogowych* i w otwartym oknie wybierz przycisk *Dodaj*.
- W otwartym oknie zdefiniuj parametry połączenia z usługą katalogową Active Directory. Częstość automatycznej synchronizacji użytkowników pomiędzy RACS 5 a AD można ustawić w zakresie od 1min do 24h. Zamknij okno przyciskiem *OK*.



- W dolnej części ekranu wybierz zakładkę *Kontenery* i następnie *Dodaj*.

- W otwartym oknie kliknij *Wybierz* by wskazać kontener typu jednostka organizacyjna (OU) w danej domenie. Jeżeli zostanie dodatkowo wskazana wcześniej utworzona Grupa użytkowników to użytkownicy importowani z Active Directory będą do niej przypisywani. Jeżeli nie zostanie wskazana grupa z listy to wtedy grupa o nazwie bazującej na wybranej nazwie jednostki organizacyjnej w Active Directory zostanie utworzona automatycznie i do niej będą przypisywani zaimportowani użytkownicy. Jeżeli zaznaczona jest opcja *Aktualizuj Grupy użytkowników* to użytkownicy, którzy po wcześniejszym imporcie z AD zostali ręcznie przeniesieni przez operatora w VISO do innych grup, w ramach kolejnych importów będą z powrotem przenoszeni do grup wynikających z przyporządkowania w AD. Zamknij okno przyciskiem *OK*.



- Zdefiniuj kolejne kontenery w ramach tej samej usługi i ewentualnie kolejne usługi ze swoimi kontenerami w innych domenach zgodnie z wymogami danej instalacji.
- W górnej części okna wybierz *Importuj* by ręcznie pobrać dane z Active Directory albo odczekaj aż kontroler samoczynnie pobierze dane zgodnie z ustawioną częstością (domyślnie co 10 minut). Przy imporcie pomijane są inne obiekty np. drukarki i pobierani są jedynie użytkownicy czyli obiekty z atrybutem sAMAccountType=805306368.
- Analogicznie jak w przypadku wcześniej opisanej synchronizacji ręcznej, przypisz Uprawnienia na poziomie Grup użytkowników i ewentualnie poszczególnych Osób jak też zdefiniuj Nośniki (np. karty) na poziomie Identyfikatorów poszczególnych Osób.

Uwaga: Stosowanie automatycznej synchronizacji oraz ręcznej synchronizacji z poziomu kreatora importu wywoływanego w menu górnym *System* programu VISO jest niewskazane i w szczególnych okolicznościach może wywoływać konflikty. Ręczną synchronizację w przypadku zdefiniowanej automatycznej synchronizacji można za to wywoływać przyciskiem *Importuj* w oknie usług katalogowych.

Dezaktywacja i usuwanie użytkowników

W przypadku synchronizacji automatycznej dezaktywacja/usuwanie użytkowników jest realizowane na tej samej zasadzie jak w przypadku wcześniej opisanej synchronizacji ręcznej. Użytkownicy usunięci w AD są usuwani w bazie danych systemu RACS 5 a użytkownicy dezaktywowani w AD są dezaktywowani w bazie danych systemu RACS 5.

Synchronizacja z kontrolerami MC16

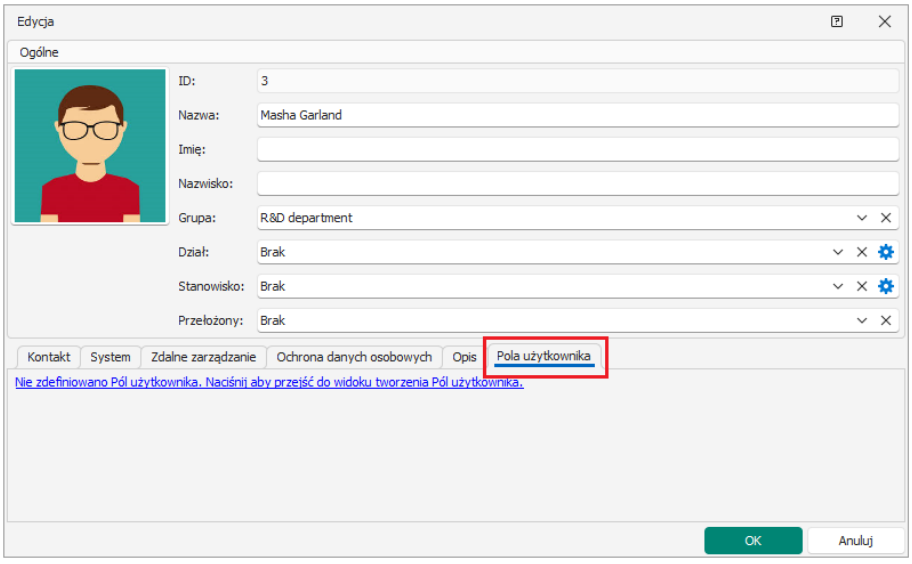
W przypadku synchronizacji automatycznej, synchronizacja z kontrolerami MC16 jest realizowana na tej samej zasadzie jak w przypadku wcześniej opisanej synchronizacji ręcznej. Kontrolery mogą być konfigurowane na żądanie lub automatycznie na bazie harmonogramu, który definiuje się po wybraniu *Harmonogramy* w drzewku nawigacyjnym programu VISO.

Mapowania atrybutów

W programie VISO można zdefiniować mapowania atrybutów, czyli określić które dane użytkowników z AD mają być importowane do VISO i gdzie mają być zapisywane. Mapowania konfiguruje się po wybraniu w menu górnym *Narzędzia-> Mapowania atrybutów*. Predefiniowane mapowania to:

- Nazwa (name)
- Imię (givenname)
- Nazwisko (sn)
- Opis (description)
- Adres email (mail)
- Telefon (telephonenumber)
- Adres (streetaddress)
- Miasto (l)
- Kod pocztowy (postalcode)
- Stanowisko (title)
- Dział (department)
- Przełożony (manager)
- Dezaktywacja Identyfikatora (useraccountcontrol)
- Ważność Identyfikatora (accountexpires)

Możliwe jest edytowanie tych mapowań jak też definiowanie własnych. Do mapowanie można wykorzystywać nie tylko wbudowane pola Osób dostępne w VISO takie jak np. imię czy nazwisko ale dodatkowo można zdefiniować własne wybierając w menu górnym *Narzędzia->Pola użytkownika* a następnie definiując mapowanie które będzie importować parametr użytkownika z AD do zdefiniowanego pola użytkownika. Pola użytkowników po ich zdefiniowaniu są widoczne w zakładce *Pola użytkownika*.



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