Roger Access Control System 5

Nota aplikacyjna nr 018

Wersja dokumentu: Rev. B

Integracja XProtect (Milestone)

Uwaga: Niniejszy dokument dotyczy RACS 5 v1.6.6 lub nowszy

Wprowadzenie

W ramach integracji systemu RACS 5 z platformą XProtect firmy Milestone do monitoringu wizyjnego dostępne są dwa scenariusze pracy. W pierwszym z nich zakłada się, że głównym oprogramowaniem do monitoringu obiektu jest VISO, które może korzystać z zasobów systemu XProtect. W takim układzie program VISO umożliwia pobieranie i wyświetlanie materiałów wideo i zdjęć z systemu Milestone w powiązaniu ze zdarzeniami zarejestrowanymi w systemie RACS 5 jak też udostępnia podgląd online z kamer systemu XProtect w dedykowanym oknie oraz na mapie. Drugi scenariusz pracy zakłada, że głównym oprogramowaniem do monitoringu obiektu jest XProtect, które po zainstalowaniu opracowanej przez firmę Roger wtyczki (plug-in) jest w stanie rozpoznawać i reagować na zdarzenia generowane w systemie RACS 5 jak też pozwala wydawać zdalne polecenia do systemu RACS 5 (np. otwarcie przejścia). Możliwe jest stosowanie obu scenariuszy pracy jednocześnie po to by naprzemiennie lub równoległe wykorzystywać programy VISO oraz XProtect do monitorowania obiektu. Integracja została opracowana z wykorzystaniem oprogramowania XProtect 2019 R1.

Konfiguracja i korzystanie z integracji w pierwszym scenariuszu nie odbiega od rozwiązania opracowanego przez firmę Roger dla innych producentów systemów CCTV (HIK Vision, Dahua, ONVIF, itd.) i można się z nim zapoznać w ramach noty AN007. Niniejsza nota opisuje z kolei drugi z wymienionych scenariuszy pracy.

Wstępna konfiguracja systemu RACS 5

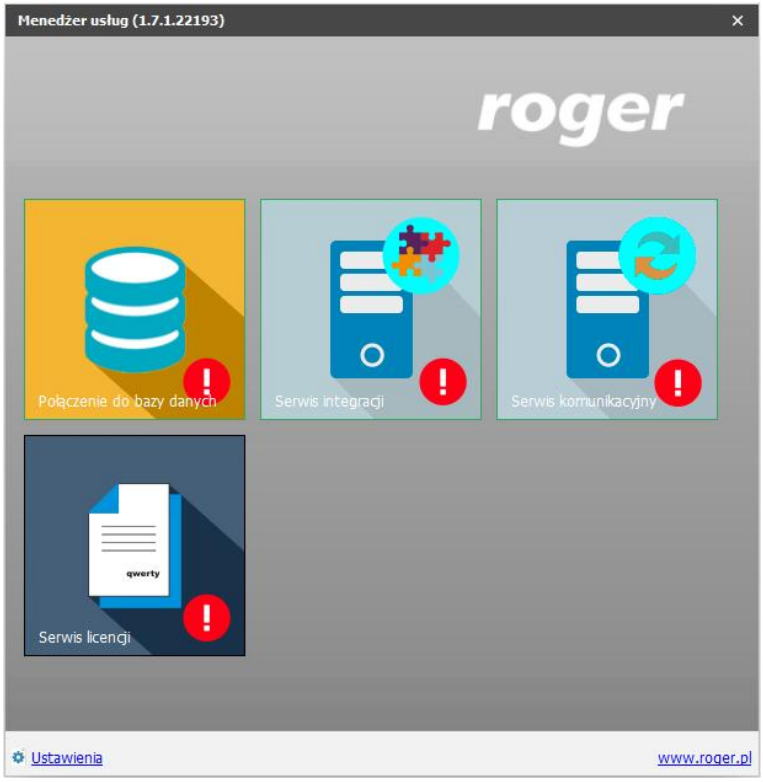
W ramach wstępnej konfiguracji systemu RACS:

- Zainstaluj oprogramowanie VISO tworząc plikową bazę danych zgodnie z notą aplikacyjną AN006 lub tworząc zalecaną serwerową bazę danych zgodnie z notą aplikacyjną AN017.
- Zainstaluj oprogramowanie RogerSVC zaznaczając nie tylko serwis komunikacyjny ale również serwis integracji i serwis licencji. Jeżeli serwisy mają działać na różnych serwerach to zainstaluj program RogerSVC oddzielnie na każdej maszynie wybierając odpowiednie serwisy. W systemie RACS 5 może funkcjonować maksymalnie jeden serwis komunikacji.

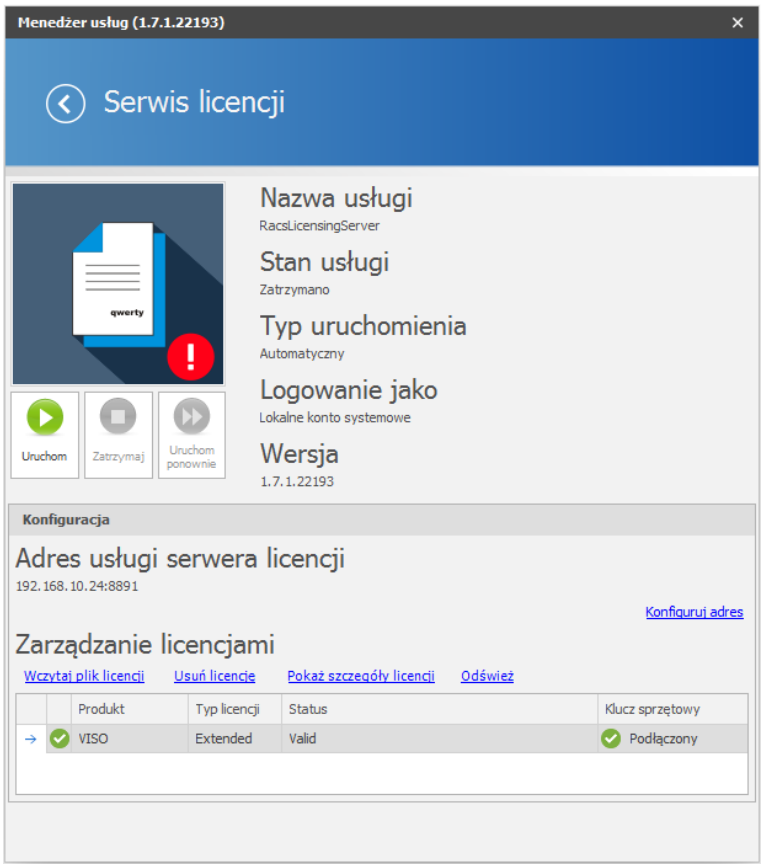
Uwaga: Jeżeli serwis licencji i serwis integracji mają funkcjonować na osobnych serwerach to podczas instalacji serwisu integracji w ramach oprogramowania RogerSVC koniecznie odznacz instalację serwisu licencji. Tylko w takim układzie podczas późniejszej konfiguracji serwisu integracji będzie możliwe wskazanie serwisu licencji działającego na innym serwerze.

- Uruchom Menedżer usług RACS 5 wybierając *Start->ROGER->RogerSVC* w systemie Windows.
- W zasobniku kliknij ikonę menedżera.

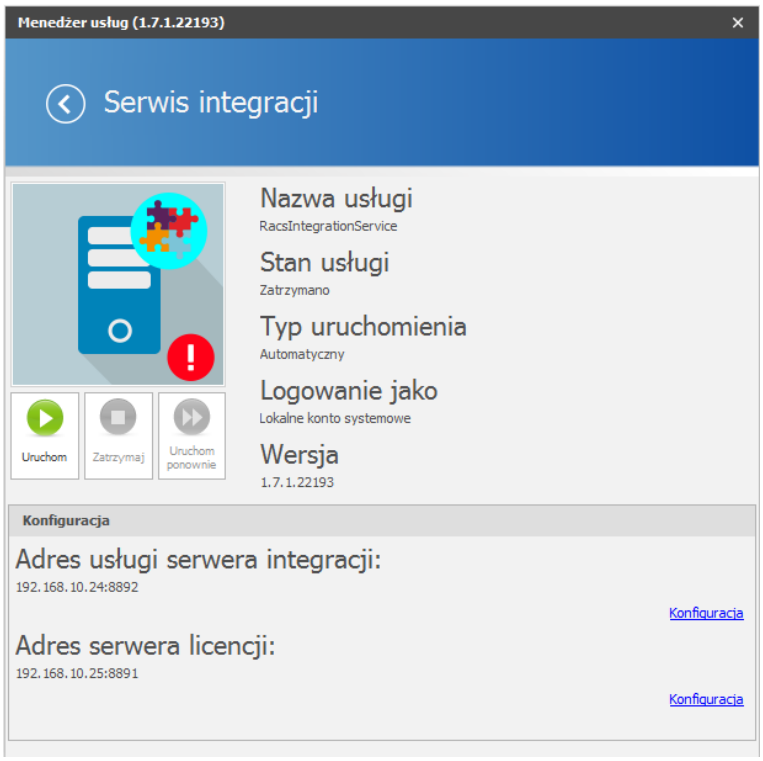
- W oknie Menedżera usług wybierz kafelek *Połączenie do bazy danych* i wybierając *Konfiguracja połączenia* wskaż wcześniej utworzoną bazę danych systemu RACS 5. Wróć do okna głównego.



- W oknie Menedżera usług wybierz kafelek *Serwis komunikacyjny* i wybierz *Uruchom*. Wróć do okna głównego.
- Podłącz klucz sprzętowy RUD-6-LKY do portu USB serwera z zainstalowanym serwisem licencji.
- W oknie Menedżera usług wybierz kafelek *Serwis licencji*, kliknij polecenie *Konfiguruj adres* a następnie wprowadź adres IP komputera na którym działa serwis (np. 192.168.10.24) i zdefiniuj port do komunikacji z serwisem (domyślnie 8891).
- Wybierz polecenie *Wczytaj plik licencji* i wskaż zakupiony plik licencji dla klucza sprzętowego RUD-6-LKY.
- Wybierz *Uruchom* i wróć do okna głównego. Serwis będzie działać w tle zawsze gdy uruchomiony jest komputer, także po zamknięciu Menedżera usług.



- W oknie Menedżera usług wybierz kafelek *Serwis integracji*, kliknij polecenie *Konfiguracja* a następnie wprowadź adres IP komputera na którym działa serwis (np. 192.168.10.24) i zdefiniuj port do komunikacji z serwisem (domyślnie 8892).
- Jeżeli inaczej niż wcześniej pokazano, serwis licencji nie został zainstalowany na tym samym serwerze co serwis integracji czyli serwerze z adresem 192.168.10.24 bo został zainstalowany na innym serwerze np. z adresem 192.168.10.25 to wtedy można wskazać ten serwis licencji dla serwera integracji jak w przykładzie poniżej.
- Wybierz *Uruchom* i wróć do okna głównego. Serwis będzie działać w tle zawsze gdy uruchomiony jest komputer, także po zamknięciu Menedżera usług.



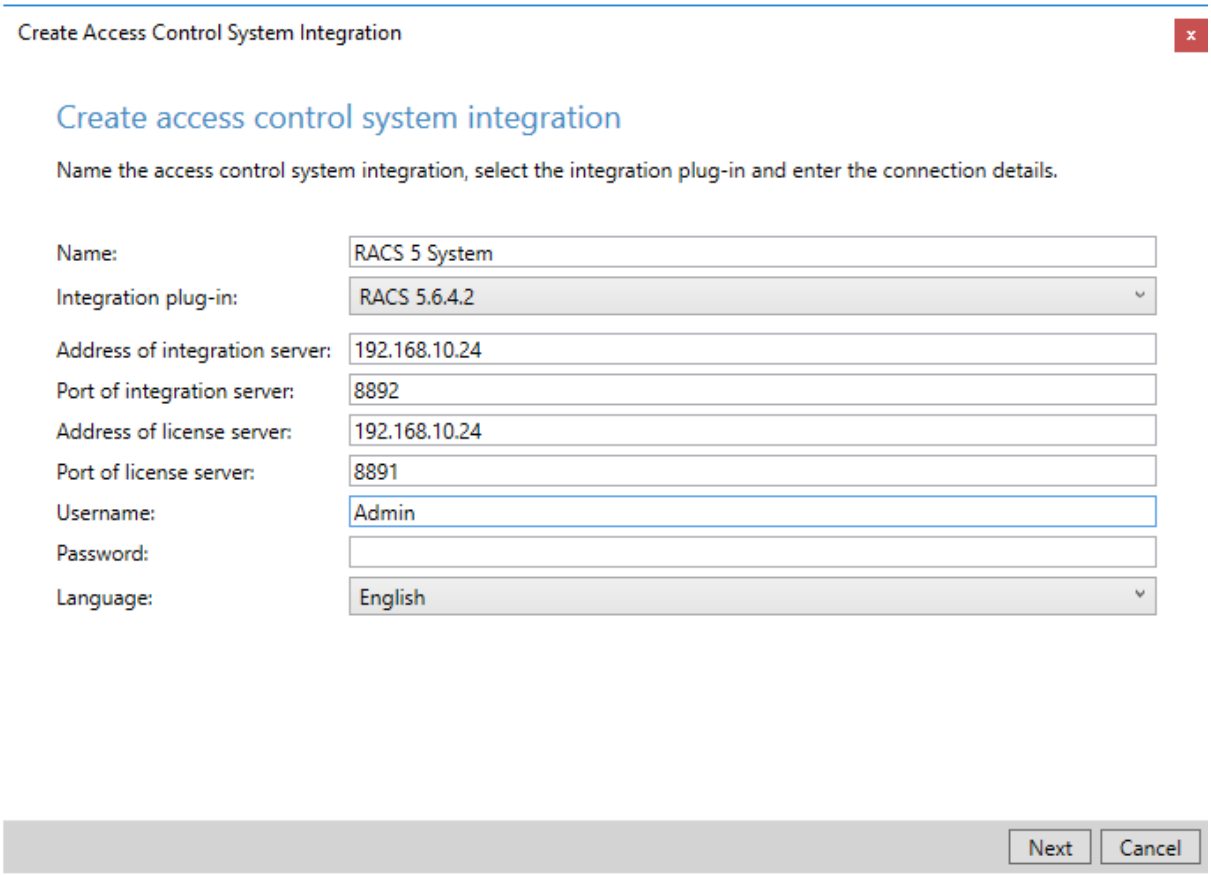
Konfiguracja XProtect

Zainstaluj i uruchom system XProtect zgodnie z instrukcjami producenta. Oprócz standardowej licencji na samo oprogramowanie XProtect oraz urządzenia CCTV dodatkowo konieczny jest zakup i aktywacja licencji Milestone XProtect Access umożliwiającej współpracę z systemem kontroli dostępu.

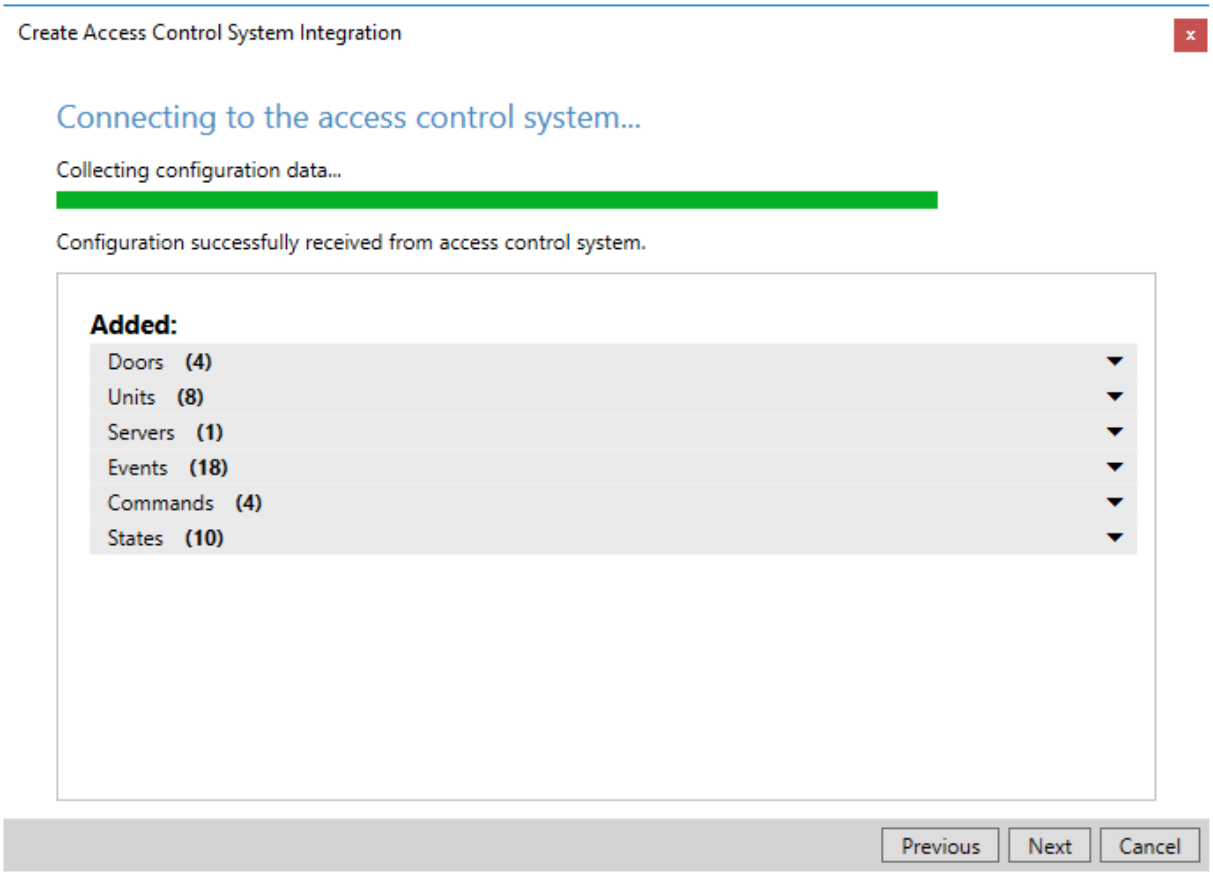
RACS 5 plug-in

System XProtect może komunikować się z systemem RACS 5 jeżeli zostanie wyposażony w odpowiednią wtyczkę (plug-in). Aby zainstalować wtyczkę:

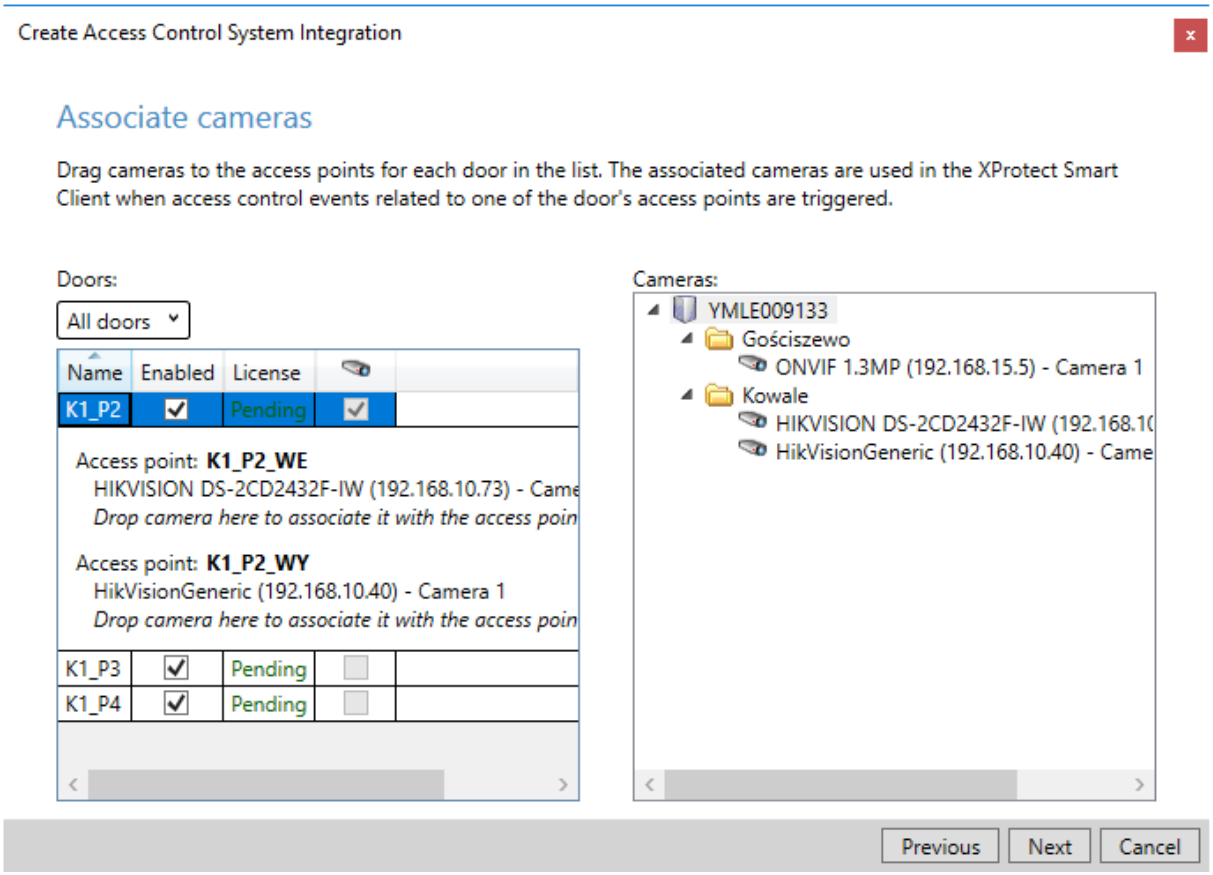
- Skopiuj pliki RogerAccessControlSystem.dll oraz acplugin.def z domyślnego folderu C:\Program Files (x86)\ROGER\VISO\Plugins\Milestone do domyślnego folderu C:\Program Files\Milestone\MIPPlugins\RogerAccessControlSystem.
- Uruchom program XProtect Management Client.
- W drzewku nawigacyjnym kliknij polecenie *Access Control* prawym przyciskiem myszki i wybierz *Create new…*
- W otwartym oknie nadaj nazwę, wskaż wtyczkę (plug-in), wprowadź wcześniej zdefiniowane ustawienia serwisów systemu RACS 5 i podaj login oraz hasło operatora systemu RACS 5. Zalecane jest wprowadzenie danych operatora Administrator w VISO. Dodatkowo można ustawić język dla elementów plug-inu stosowanych w programie XProtect Smart Client. Kliknij *Next*.



- W kolejnym oknie wyświetlona zostanie lista obiektów odczytanych z systemu RACS 5, w tym Przejścia oraz Punkty identyfikacji. Kliknij *Next*.



- W otwartym oknie powiąż kamery XProtect z Punktami identyfikacji (czytnikami) RACS 5. Kliknij *Next* i następnie *Close* by zakończyć konfigurację.



Uwaga: Za każdym razem gdy zmienione zostanie konfiguracja systemu RACS 5 w zakresie Przejść i Punktów identyfikacji to konieczne jest jej ręczne przeładowanie w systemie XProtect poprzez wybranie *Access Control -> Utworzony system -> General Settings -> Refresh Configuration*. Zmiany w zakresie użytkowników RACS 5 nie wymagają ręcznego przeładowywania i są rozpoznawane przez XProtect automatycznie z uwzględnieniem możliwych opóźnień.

Uwaga: Do prawidłowej obsługi oprogramowania XProtect może być konieczne odblokowanie portów 80 i 443 w zaporze Windows. Pełna lista portów wykorzystywanych przez XProtect jest dostępna w materiałach firmy Milestone.

Zastosowanie integracji

Szczegółowe informacje na temat konfiguracji systemu XProtect są dostępne w instrukcjach producenta. W poniższych podpunktach podano zakres możliwości oraz wskazówki co do ustawień po stronie systemu RACS 5.

Zdarzenia i użytkownicy

Wybrane zdarzenia systemu RACS 5 (tabela 1) po zarejestrowaniu są na bieżąco udostępniane poprzez serwis integracji i plug-in oprogramowaniu XProtect. Dodatkowo dostępne są zdarzenia sygnalizujące stan połączenia pomiędzy systemem XProtect a serwerem RACS 5.

Zarejestrowane zdarzenia mogą być przeglądane w zakładce *Access Control* oprogramowania XProtect Smart Client i jeżeli dotyczą one Punktów identyfikacji lub Przejść, do których przypisane są kamery to możliwe jest odtwarzanie dla nich zarejestrowanego materiału wideo. Dodatkowo zdarzenia mogą być filtrowane także pod względem ich powiązania z konkretnym użytkownikiem systemu RACS 5.

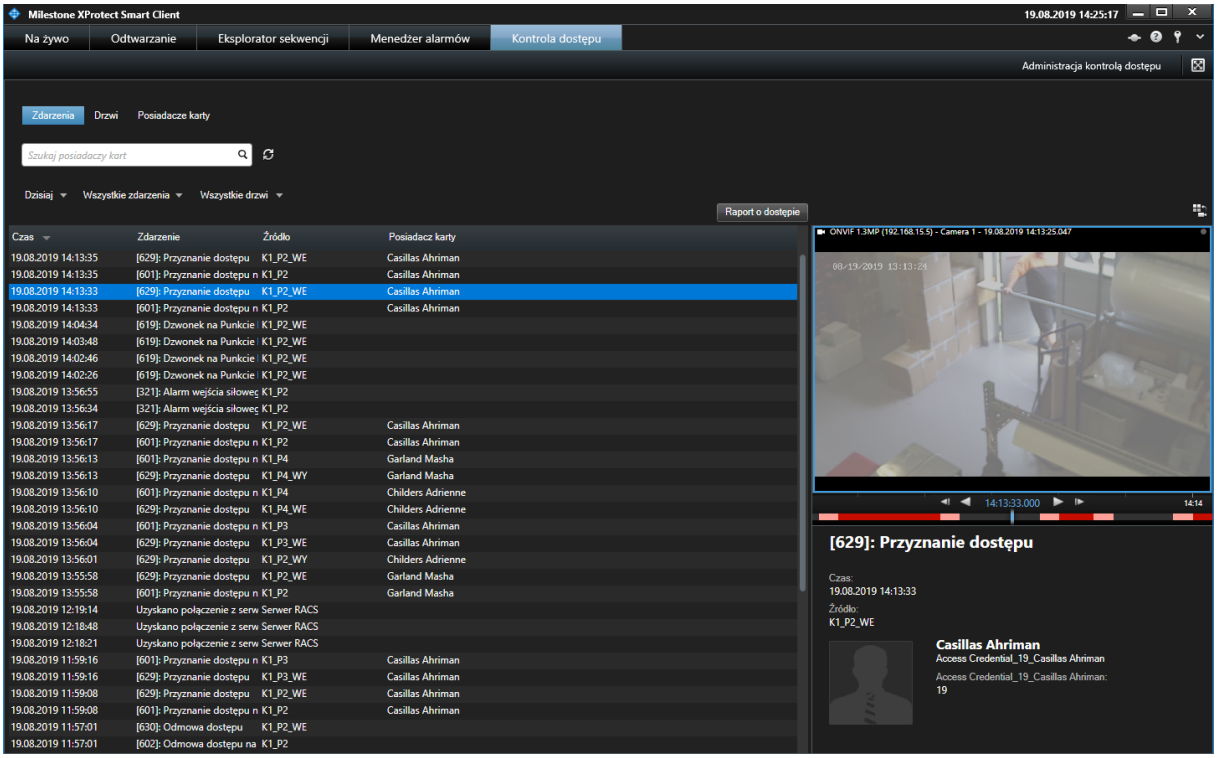


Tabela 1. Zdarzenia RACS 5		
Kod	Nazwa zdarzenia	Opis
302	Ustawienie Przejścia w Tryb odblokowane	Rejestrowane gdy na Przejściu z ustawionym Trybem drzwi Warunkowo odblokowane nastąpi przyznanie dostępu skutkującego przełączeniem Przejścia do trybu Odblokowane.
321	Alarm wejścia siłowego	Rejestrowane gdy wykryte zostanie otwarcie Przejścia na podstawie sygnału z linii wejściowej z funkcją *[130]: Czujnik otwarcia – klucz stały* pomimo tego że nie nastąpiło przyznanie dostępu ze strony systemu.
322	Alarm zbyt długo otwartych drzwi	Rejestrowane gdy na podstawie sygnału z linii wejściowej z funkcją funkcją *[130]: Czujnik otwarcia – klucz stały* wykryte zostanie że Przejście jest otwarte dłużej niż wskazuje na to parametr *Czas na zamknięcie*.
601	Przyznanie dostępu na Przejściu	Rejestrowane w momencie przyznania dostępu dla funkcji wejściowej *[151]* lub *[152]*.
602	Odmowa dostępu na Przejściu	Rejestrowane w momencie odmowy dostępu dla funkcji wejściowej *[151]* lub *[152]*.
619	Dzwonek na Punkcie identyfikacji	Rejestrowane w momencie użycia funkcji wejściowej *[159]*.
629	Przyznanie dostępu	Rejestrowane w momencie przyznania dostępu dla funkcji wejściowej *[151]*, *[152]*, *[175]* lub *[176]*.
630	Odmowa dostępu	Rejestrowane w momencie odmowy dostępu dla funkcji wejściowej *[151]*, *[152]*, *[175]* lub *[176]*.
637	Ustawienie Przejścia w Tryb normalny	Rejestrowane w momencie ustawienia Trybu drzwi Normalny za pomocą funkcji wejściowej *[126]*, *[136]* lub harmonogramem. Tryb drzwi Normalny jest domyślnym trybem drzwi.
639	Ustawienie Przejścia w Tryb zablokowane	Rejestrowane w momencie ustawienia Trybu drzwi Zablokowane za pomocą funkcji wejściowej *[124]* lub harmonogramem.

641	Ustawienie Przejścia w Tryb odblokowane	Rejestrowane w momencie ustawienia Trybu drzwi Odblokowane za pomocą funkcji wejściowej *[125], [136]* lub harmonogramem.
643	Ustawienie Przejścia w Tryb warunkowo odblokowane	Rejestrowane w momencie ustawienia Trybu drzwi Warunkowo Odblokowane za pomocą funkcji wejściowej *[127]* lub hamonogramem.
645	Otwarcie Przejścia	Rejestrowane w momencie otwarcia Przejścia czyli załączenia linii wejściowej z funkcją *[130]: Czujnik otwarcia – klucz stały.*
647	Zamknięcie Przejścia	Rejestrowane w momencie zamknięcia Przejścia czyli wyłączenia linii wejściowej z funkcją *[130]: Czujnik otwarcia – klucz stały.*
760	Załączenie stanu TAMPER	Rejestrowane w momencie wykrycia alarmu antysabotażowego czyli załączenia linii wejściowej z funkcją *[133]: TAMPER – klucz stały*.
761	Wyłączenie stanu TAMPER	Rejestrowane w momencie zakończenia alarmu antysabotażowego czyli wyłączenia linii wejściowej z funkcją *[133]: TAMPER – klucz stały*.
	Uzyskano połączenie z serwerem	Rejestrowane w momencie nawiązania połączenia pomiędzy systemem XProtect i serwerem integracji RACS 5.
	Utracono połączenie z serwerem	Rejestrowane w momencie utraty połączenia pomiędzy systemem XProtect i serwerem integracji RACS 5.

Uwaga: W integracji nie jest obsługiwane awaryjne odblokowywanie i zablokowywanie Przejść czyli funkcje wejściowe *[121]*, *[122]* i *[123]*.

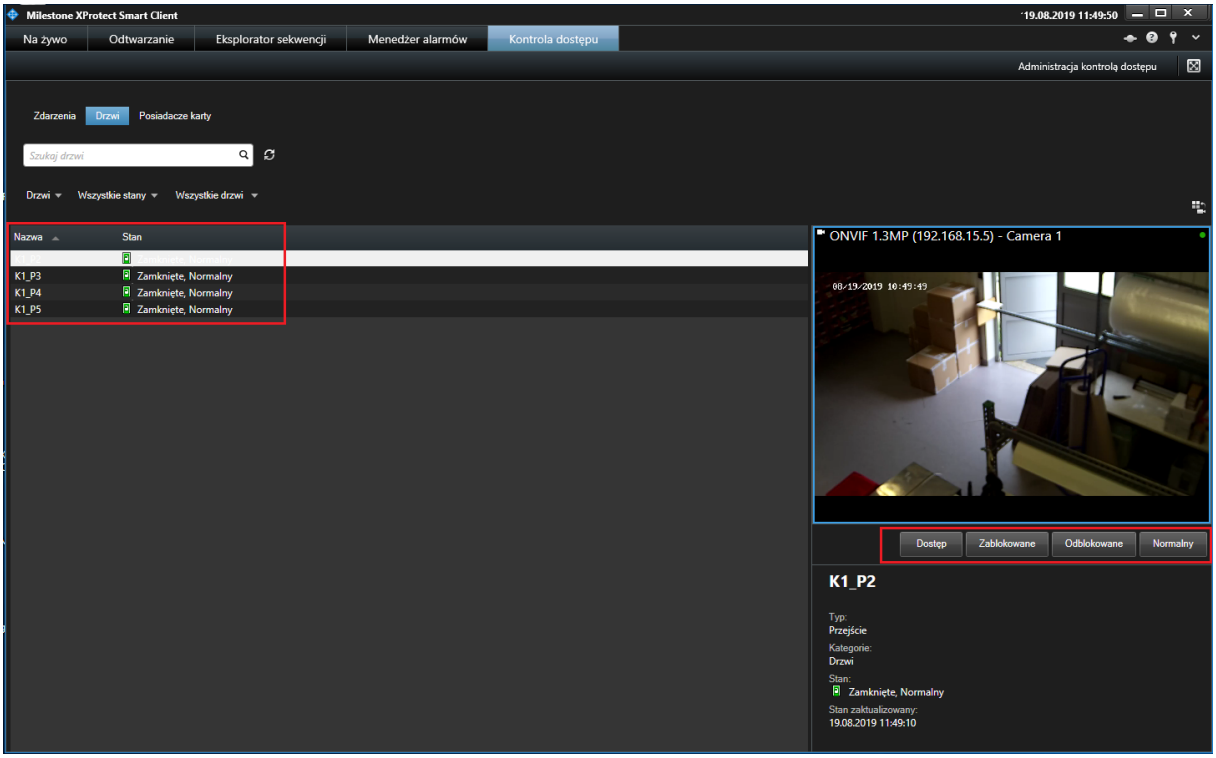
Stany i alarmy Przejść

Wykryte przejścia systemu RACS 5 mogą być monitorowane i zdalnie kontrolowane w programie XProtect Smart Client. Stany Przejść RACS 5 rozpoznawane i raportowane w systemie XProtect:

- Otwarte
- Zamknięte
- Normalny
- Odblokowane
- Zablokowane

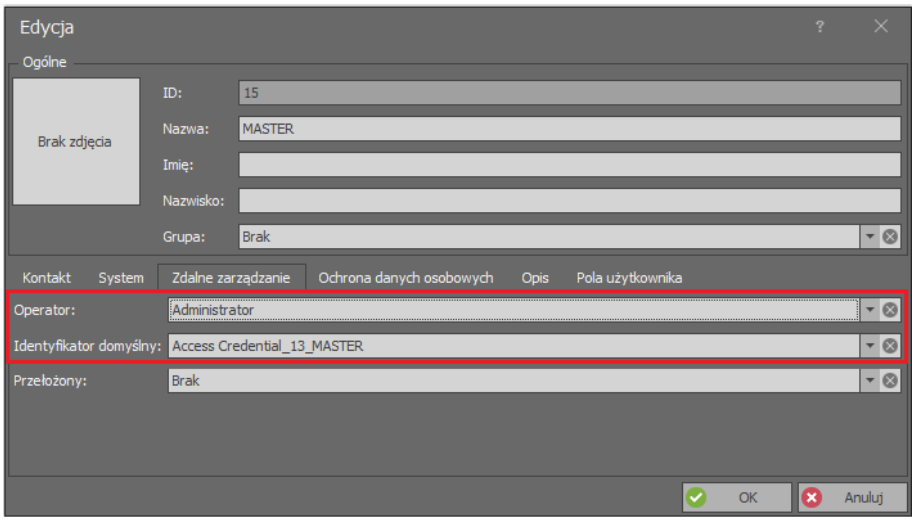
Zdalne polecenia obsługiwane z poziomu XProtect dla Przejść systemu RACS 5:

- Dostęp
- Zablokowane
- Odblokowane
- Normalny



Operator systemu RACS 5 może wydawać zdalne komendy jeżeli jego konto jest powiązane z użytkownikiem systemu RACS 5 posiadającym odpowiednie Uprawnienia. Gdy zdalna komenda jest wywołana w programie XProtect Smart Client (np. Dostęp) to do autoryzacji wykorzystywane jest konto operatora, które zostało podane podczas konfiguracji wtyczki (plug-in). Konto Administratora RACS 5 wymaga dodatkowej konfiguracji w zakresie komend zdalnych bo domyślnie nie daje możliwości ich wydawania. Aby przypisać operatorowi pełne uprawnienia w zakresie komend zdalnych:

- Rozpocznij definiowanie użytkownika wybierając zakładkę Kreatory w menu górnym programu VISO i następnie wybierz *Dodaj Osobę online*
- Gdy definiowany jest Identyfikator w ramach kreatora to wybierz zakładkę *Wyjątki* i zaznacz opcję *Wyjątek Master*. Identyfikator z takim wyjątkiem daje użytkownikowi pełne prawa do wszystkich funkcji w systemie. Jeżeli wyjątek nie zostanie zaznaczony ale w następnym kroku przypisane zostaną Uprawnienia to użytkownik i później powiązany z nim operator będą mogli stosować jedynie funkcje wynikające z tych Uprawnień.
- Gdy użytkownik zostanie utworzony za pomocą kreatora to w menu górnym programu VISO wybierz *Konfiguracja* i następnie ikonę *Osoby*.
- W otwartym oknie wybierz utworzonego użytkownika, wybierz *Edytuj*, zakładkę *Zdalne zarządzanie* i powiąż użytkownika z operatorem (Administratorem). Dodatkowo wskaż Identyfikator z wyjątkiem Master.

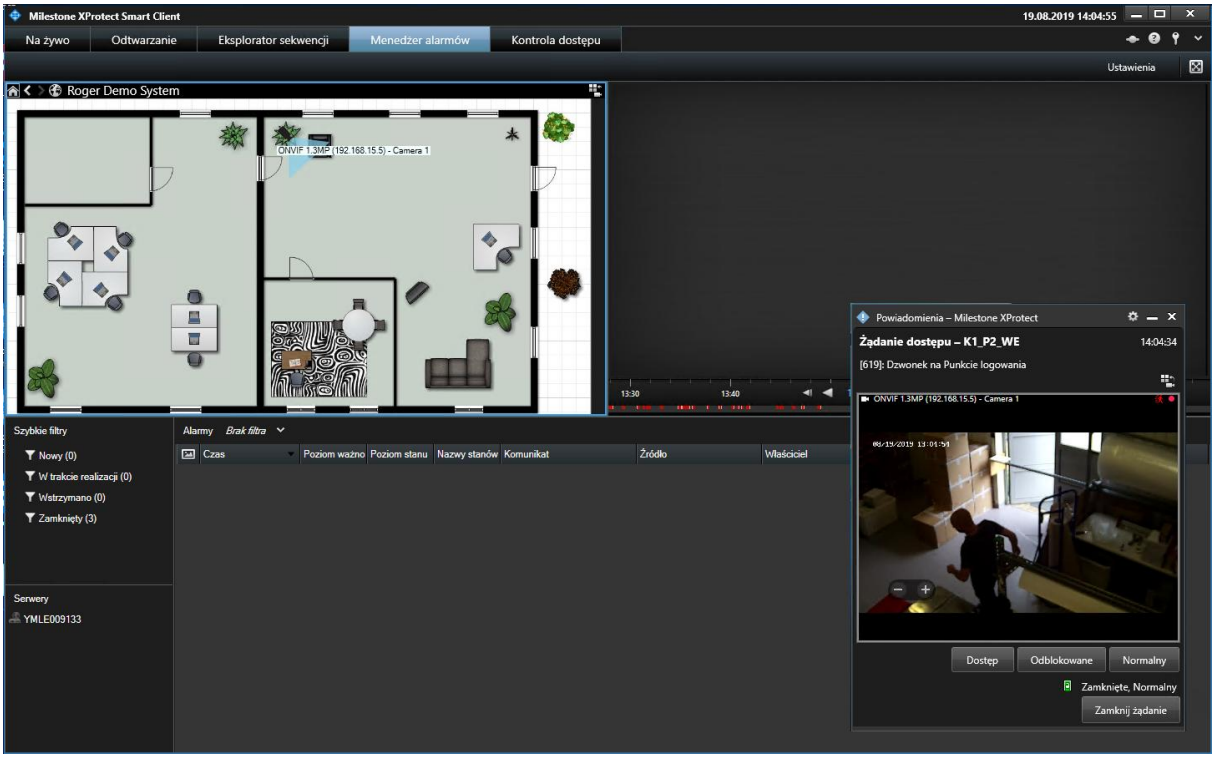


Żądanie dostępu

Wywołanie zdarzenia *[619]* w systemie RACS 5 za pomocą funkcji *[159]: Uruchom dzwonek na punkcie identyfikacji* albo zdarzenia *[630]: Odmowa dostępu* skutkuje automatycznym wywołaniem w programie XProtect Smart Client okienka Żądanie dostępu wyświetlającego obraz z kamery powiązanej z Punktem identyfikacji, na którym wywołane zostało zdarzenie. Operator systemu na podstawie takiego wywołanie może np. zdalnie otworzyć przejście.

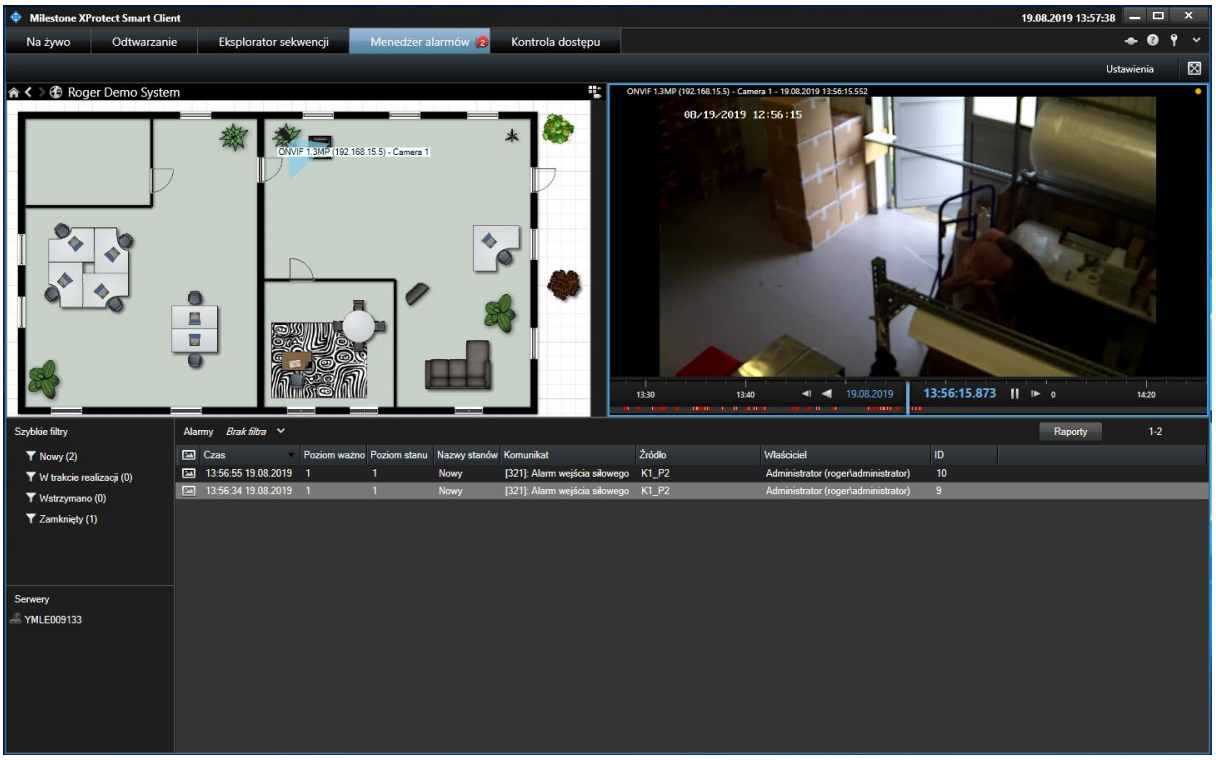
System XProtect reaguje na zdarzenia *[619]* oraz *[630]* wywołaniem okienka Żądanie dostępu, dlatego że domyślnie te zdarzenia mają przypisaną kategorię *Access Request*. Zmiany domyślnych kategorii można dokonać wybierając w programie XProtect Management Client polecenie *Access Control -> Utworzony system -> Access Control Events.*

Polecenie które będą dostępne w okienku Żądanie dostępu można zdefiniować samemu za pomocą XProtect Management Client wybierając *Access Control -> Utworzony system -> Access Request Notifications.* Dodatkowo konieczne jest zdefiniowanie nowej lub zmodyfikowanie domyślnej reguły wyświetlania powiadomień w XProtect Management Client wybierając *Rules and Events -> Rules*.



Alarmy

Dla zdarzeń RACS 5 mogą być generowane alarmy w systemie XProtect. Alarmy definiuje się poleceniem *Alarms* w drzewku programu XProtect Managment Client. Alarmy w momencie ich wystąpienia mogą być wyświetlane w zakładce *Alarm Manager* programu XProtect Smart Client i mogą one być powiązywane z kamerami i mapami systemu XProtect. Operator może reagować na alarmy (zatwierdzać, wstrzymywać, zamykać ,edytować, itp.).



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