

R o g e r A c c e s s C o n t r o l S y s t e m 5 v 2

Application note no. 018

Document version: Rev. A

XProtect (Milestone) integration

Note: This document refers to RACS 5 v2.0.4 or higher

Introduction

Two scenarios of operation are available for integration of RACS 5 access control system and XProtect video management system. In the first scenario it is assumed that the main monitoring software is VISO which can use resources of XProtect system. In such case VISO enables video and photo downloading from Milestone system in association with events registered in RACS 5 system and it enables to view live video from cameras in dedicated window and on interactive map. In the second scenario it is assumed that XProtect is the main monitoring software and after installation of Roger plug-in it can recognize and react for events registered in RACS 5 system. Moreover it can be used to start remote commands affecting RACS 5 system (e.g. remote door opening). Both scenarios can be applied at the same time and both VISO and XProtect can be used simultaneously or interchangeably to monitor premises. The integration was developed with XProtect 2019 R1 and it is compatible with newer versions.


The configuration in the first scenario does not differ significantly from the solution offered by Roger for other supported CCTV providers (HIK Vision, Dahua, ONVIF, etc.) and it is explained in AN007 application note. This note is focused on the second scenario.

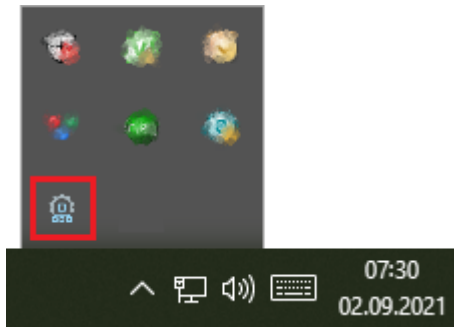
Preliminary configuration of RACS 5

In order to conduct preliminary configuration of RACS 5:

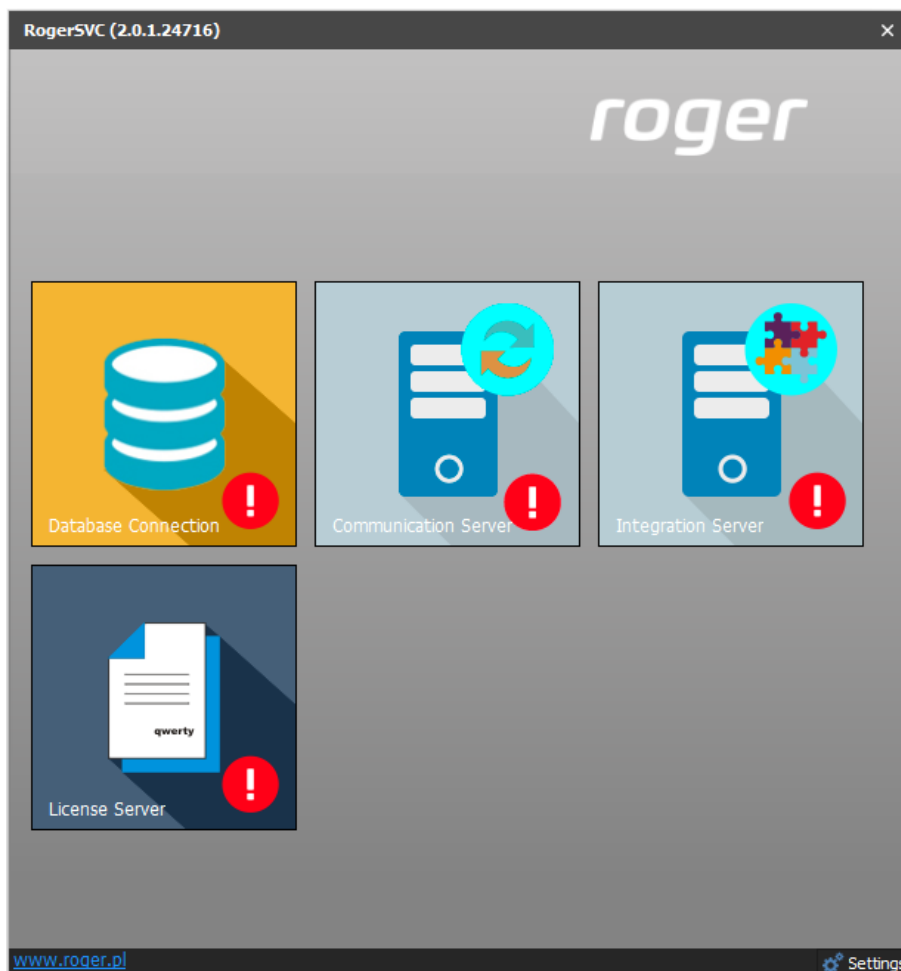
- Install VISO software and create database according to AN006 application note.
- Install RogerSVC software and select not only Communication Server but also License Server and Integration Server. If servers are supposed to be operated on individual computers then install RogerSVC on each computer selecting required servers.

Note: If License Server and Integration Server are supposed to be operated on individual computers then during installation of Integration Server, the License Server must be deselected. Only in such case it will be possible to indicate external License Server when Integration Server is configured.

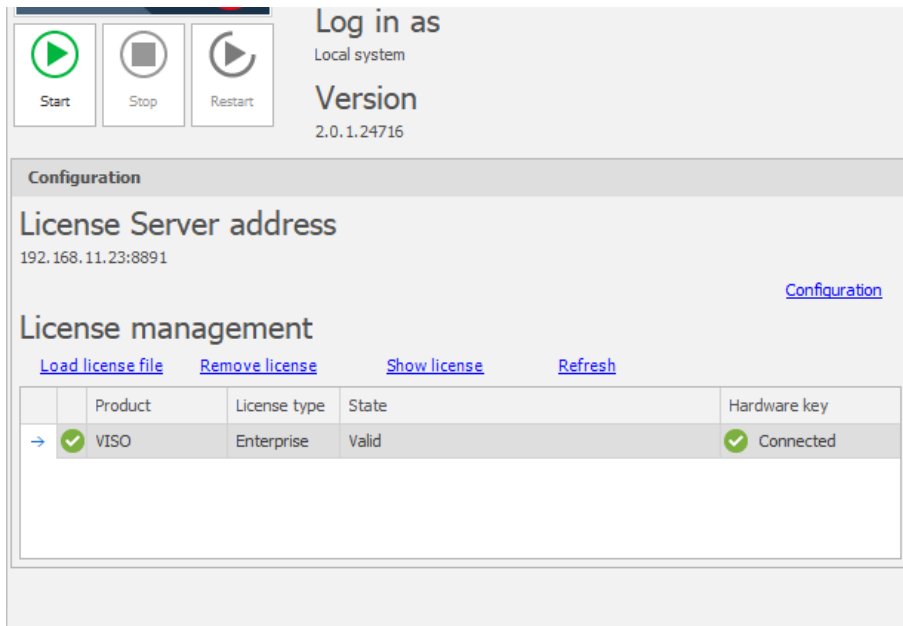
- When RogerSVC is launched then its icon is displayed in Windows tray. Click the icon . The RogerSVC icon in tray can also be launched from Windows menu *Start-> Roger-> RogerSVC*.



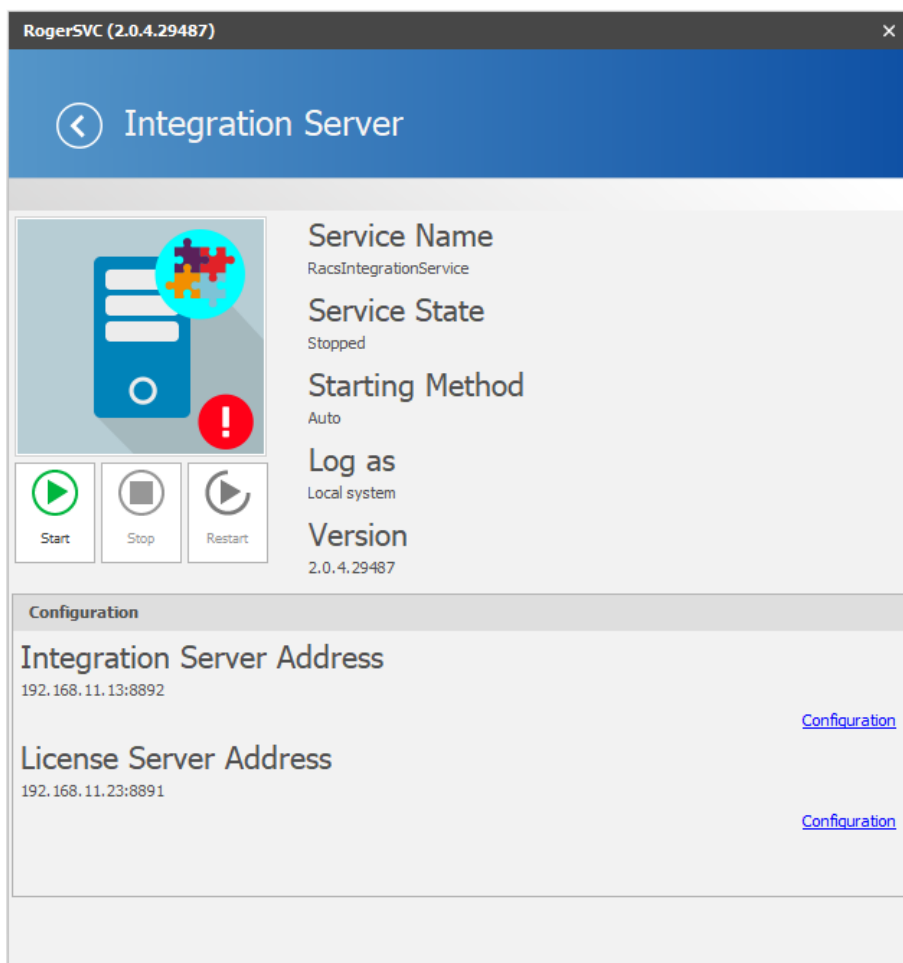
- In the RogerSVC window select *Database Connection* tile and then *Configuration* to indicate previously created RACS 5 database. Return to the main window.



- In the RogerSVC window select *Communication Server*, click *Configuration*, enter IP address of the computer with the server installed e.g. 192.168.11.13 and define port (8890 by default).
- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.
- Connect RUD-6-LKY hardware key to USB port of computer with License Server installed.
- In the RogerSVC window select *License Server* tile, click *Configuration*, enter IP address of the computer with the server installed e.g. 192.168.11.13 and define port (8891 by default).
- Select *Load license file* and indicate purchased license file for RUD-6-LKY hardware key.
- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.



- In the RogerSVC window select *Integration Server* tile, click *Configuration*, enter IP address of the computer with the server installed (e.g. 192.168.11.13) and define port (8892 by default).
- If contrary to previously presented configuration steps, the License Server is installed on a computer with exemplary 192.168.11.23 address while Integration Server is installed on computer with exemplary 192.168.11.13 address then it is possible to indicate external License Server for integration as below.



- Select *Start* and return to the main window. The server will be started and operated in the background whenever the computer is switched on even if RogerSVC window is closed.
- Start VISO software, in the top menu select *System*, then *Select License Server* and indicate previously defined License Server from RogerSVC software in order to start the VISO program in licensed version.

XProtect configuration

Install and start XProtect system according to manufacturer guidelines. Apart from typical license for XProtect software and CCTV devices the Milestone XProtect Access license must be purchased and activated to enable operation with RACS 5 system.

RACS 5 plug-in

XProtect system can communicate with RACS 5 system if equipped with adequate plug-in. In order to install the plug-in:

- Copy files from default folder C:\Program Files\ROGER\VISO\Plugins\Milestone to default folder C:\Program Files\Milestone\MIPPlugins\RogerAccessControlSystem.
- Start XProtect Management Client program.
- In the navigation tree right click *Access Control* and select *Create new...*
- In the opened window name the integration, select plug-in, enter IP addresses and ports of RACS 5 Integration Server and License Server, enter RACS 5 operator login and password (it is recommended to use VISO Administrator account) and select language version for plug-in objects displayed in XProtect Smart Client. Click *Next*.

Create Access Control System Integration



Create access control system integration

Name the access control system integration, select the integration plug-in and enter the connection details.

Name:	<input type="text" value="RACS 5 System"/>
Integration plug-in:	<input type="text" value="RACS 5.6.4.2"/>
Address of integration server:	<input type="text" value="192.168.10.24"/>
Port of integration server:	<input type="text" value="8892"/>
Address of license server:	<input type="text" value="192.168.10.24"/>
Port of license server:	<input type="text" value="8891"/>
Username:	<input type="text" value="Admin"/>
Password:	<input type="password"/>
Language:	<input type="text" value="English"/>

Next

Cancel

- In the next window the list of detected objects from RACS 5 system is displayed, including Access Doors and Access Points. Click *Next*.

Create Access Control System Integration



Connecting to the access control system...

Collecting configuration data...



Configuration successfully received from access control system.

Added:

Doors (4)

Units (8)

Servers (1)

Events (18)

Commands (4)

States (10)

Previous

Next

Cancel

- In the next window associate XProtect cameras with RACS 5 Access Points (readers). Click *Next* and then *Close* to finish the configuration.

Create Access Control System Integration



Associate cameras

Drag cameras to the access points for each door in the list. The associated cameras are used in the XProtect Smart Client when access control events related to one of the door's access points are triggered.

Doors:

All doors ▾

Name	Enabled	License		
K1_P2	<input checked="" type="checkbox"/>	Pending	<input checked="" type="checkbox"/>	
Access point: K1_P2_WE HIKVISION DS-2CD2432F-IW (192.168.10.73) - Camera 1 Drop camera here to associate it with the access point				
Access point: K1_P2_WY HikVisionGeneric (192.168.10.40) - Camera 1 Drop camera here to associate it with the access point				
K1_P3	<input checked="" type="checkbox"/>	Pending	<input type="checkbox"/>	
K1_P4	<input checked="" type="checkbox"/>	Pending	<input type="checkbox"/>	

Cameras:

- YMLE009133
 - Gościszewo
 - ONVIF 1.3MP (192.168.15.5) - Camera 1
 - Kowale
 - HIKVISION DS-2CD2432F-IW (192.168.10.73) - Camera 1
 - HikVisionGeneric (192.168.10.40) - Camera 1

Previous

Next

Cancel

Note: Every time the configuration of RACS 5 system is changed in regard of Access Doors and Access Points then it is necessary to start detection it in XProtect system by selection of *Access Control -> Your system -> General Settings -> Refresh Configuration*. Modifications of user list in RACS 5 do not require such refreshing and users are detected automatically by XProtect but sometimes with delay.

Note: The proper operation of XProtect software may require unblocking of 80 and 443 communication ports in Windows firewall. The full list of ports used by XProtect is available in Milestone manuals.

Application of integration

Detailed instructions on XProtect configuration are available in manuals offered by Milestone company. The information below is supposed to explain available functionalities and give some hints on proper configuration of RACS 5 system.

Events and users

Selected events from RACS 5 system (table 1) after their registration are sent to XProtect via RACS 5 Integration Server and plug-in. Additionally two events for monitoring of communication between RACS 5 and XProtect are available.

Registered events can be viewed in *Access Control* window of XProtect Smart Client software and if they are related to Access Points or Access Doors then video from associated camera(s) can be played. Additionally, events can be filtered in regard of their association with particular users (cardholders).

The screenshot shows the Milestone XProtect Smart Client interface. The 'Access Control' tab is selected. On the left, there is a list of events with columns for Time, Event, Source, and Cardholder. The event list includes entries for 'Access Granted' and 'Door Access Granted' for various users like Casillas Ahriman, Childers Adrienne, and Garland Masha. On the right, a video feed from a camera is displayed, showing a person in a warehouse setting. Below the video, details for a specific event are shown, including the time (13.08.2019 12:53:23), source (K1_P2_WE), and cardholder (Casillas Ahriman).

Table 1. RACS 5 events		
No	Name	Description
302	Unlocked Door Mode	Registered when access is granted at Access Door with Conditional Unlocked Mode resulting in Unlocked Mode.

321	Door Forced Alarm	Registered when Access Door opening is detected by input with the function [130]: <i>Door Contact Toggle</i> despite of not granting access at the door by the system.
322	Door Open Too Long Alarm	Registered when based on input with the function [130]: <i>Door Contact Toggle</i> it is detected that Access Door is opened longer than it is allowed by the parameter <i>Door Open Too Long Time</i> .
601	Door Access Granted	Registered when access is granted for input function [151] or [152].
602	Door Access Denied	Registered when access is denied for input function [151] or [152].
619	Access Point Bell	Registered when input function [159] is used.
629	Access Granted	Registered when access is granted for input function [151], [152], [175] or [176].
630	Access Denied	Registered when access is denied for input function [151], [152], [175] or [176].
637	Normal Door Mode	Registered when Normal Door Mode is switched on by input function [126], [136] or Schedule. Normal Door Mode is default one.
639	Locked Door Mode	Registered when Locked Door Mode is switched on by input function [124] or Schedule.
641	Unlocked Door Mode	Registered when Unlocked Door Mode is switched on by input function [125], [136] or Schedule.
643	Conditional Unlocked Door Mode	Registered when Conditional Unlocked Door Mode is switched on by input function [127] or Schedule.
645	Door Open	Registered when Access Door opening is detected by activation of input with the function [130]: <i>Door Contact Toggle</i> .
647	Door Closed	Registered when Access Door closing is detected by deactivation of input with the function [130]: <i>Door Contact Toggle</i> .
760	Tamper Violated	Registered when Tamper alarm is detected by activation of input with the function [133]: <i>Tamper Toggle</i> .
761	Tamper Restored	Registered when Tamper alarm is finished by deactivation of input with the function [133]: <i>Tamper Toggle</i> .
	Server connected	Registered when communication between XProtect and RACS 5 is established.
	Server connection lost	Registered when communication between XProtect and RACS 5 is lost.

Note: Emergency unlocking and locking i.e. input functions [121], [122] and [123] are not supported in the integration.

Access Door states and alarms

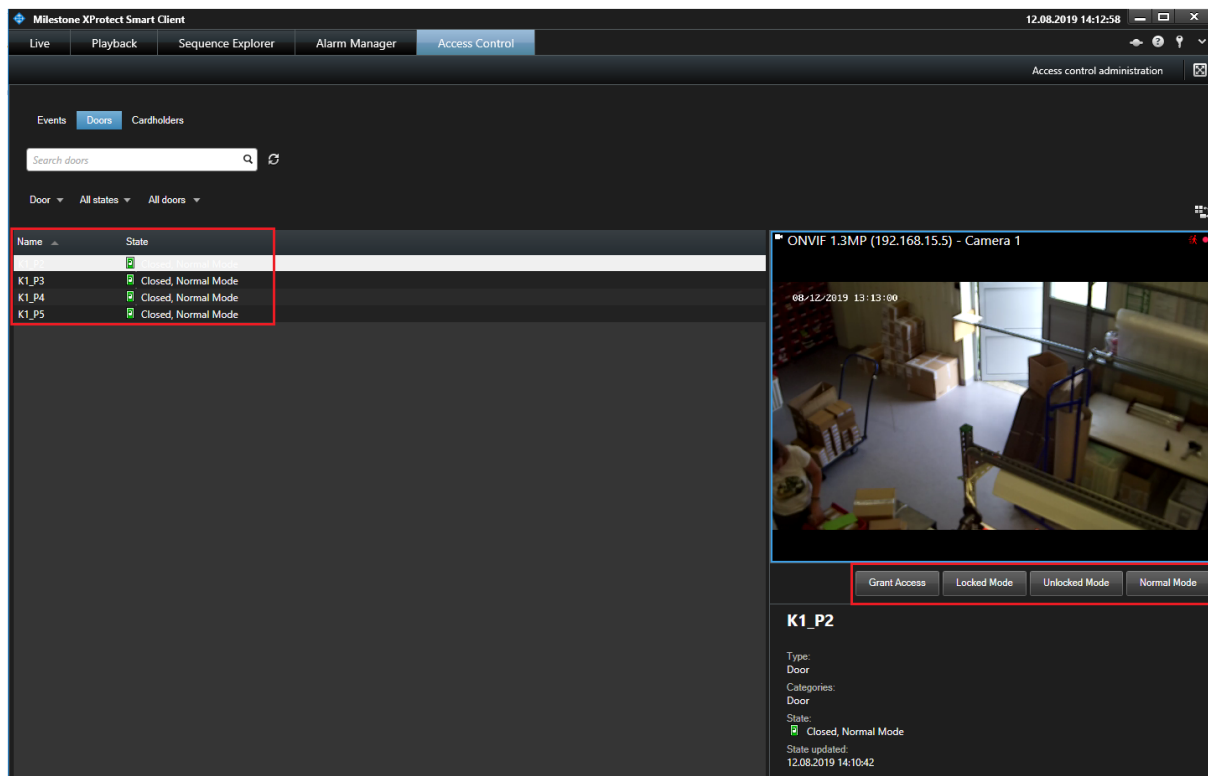
Detected RACS 5 Access Doors can be monitored and remotely controlled in XProtect Smart Client program. Following states are recognized in XProtect:

- Open
- Closed
- Normal Mode
- Unlocked Mode
- Locked Mode

Following RACS 5 remote commands are available in XProtect Smart Client:

- Grant Access
- Locked Mode

- Unlocked Mode
- Normal Mode



RACS 5 operator can use remote commands if there is proper association of such operator's account with RACS 5 user and the user is assigned with adequate Authorisations in the system. When remote command is started in XProtect Smart Client (e.g. Grant Access) then RACS 5 account (Administrator with Admin login) which was applied during plug-in configuration is used for authentication. The RACS 5 Administrator account requires configuration in regard of remote commands as by default it is not allowed to start such commands. In order to assign full rights to RACS 5 operator:

- Start user enrolment selecting *Wizards* tab in the top menu of VISO and then *Add Person Online*
- When Access Credential is defined within the wizard, select *Exemptions* tab and enable *Master exemption*. Access Credential with this exemption gives the user full rights to all functions in the system. If the exemption is not selected but in the next step Authorisations are assigned then user and further associated operator will be allowed to use only functions resulting from these Authorisations.
- When user is created with the wizard, select *Configuration* tab in the top menu of VISO and then *Access User Persons* icon.
- In the opened window select previously created person, click *Edit*, select *Remote management* tab and associate the user with operator (Administrator). Additionally select Access Credential with Master exemption.

More information on Operators in RACS 5 system is given in AN040 application note.

Edit Access User Person

General

ID: 15
 Name: MASTER
 First Name:
 Last Name:
 Group: (none)

Contact Information | Additional Options | Remote management | Private Data Protection | Description | Custom Fields

Operator: Administrator
 Default Credential: Access Credential_13_MASTER
 Supervisor: None

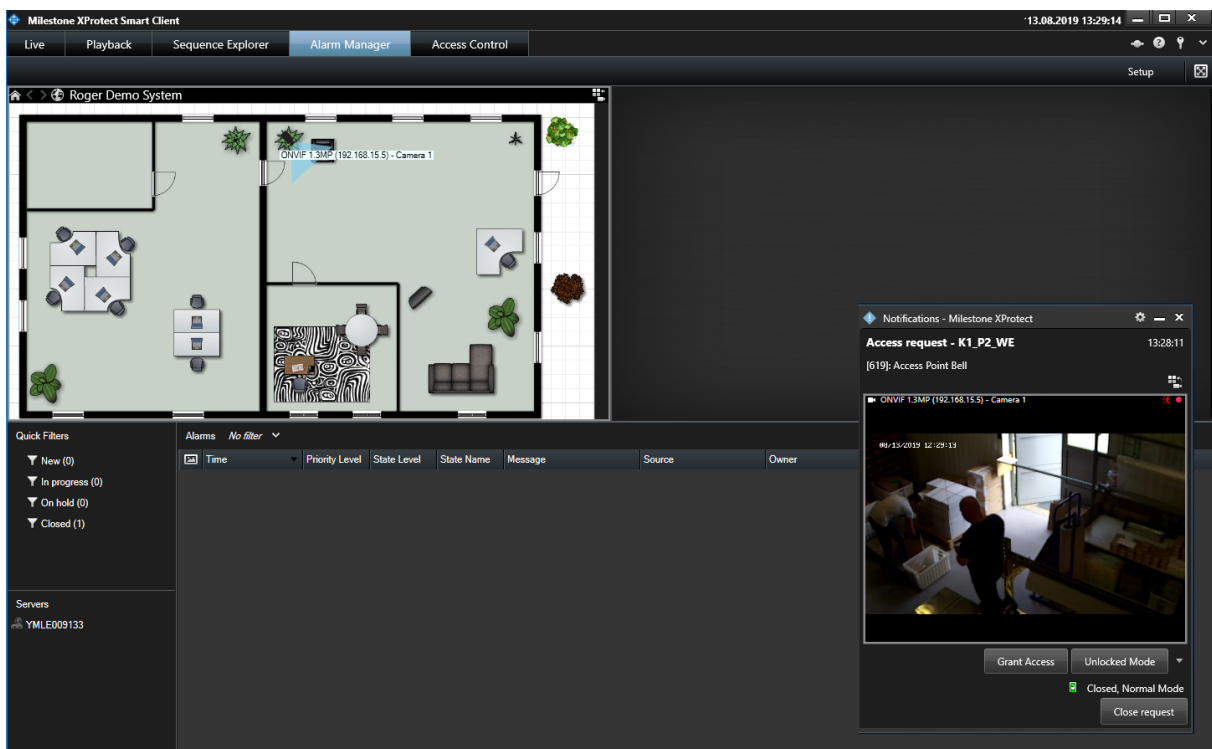
OK Cancel

Access request

When event [619] is registered in RACS 5 system for function [159]: *Access Point Bell* or event [630]: *Access denied* is registered then Access Request window automatically pops up in XProtect Smart Client and it includes video from camera which is associated with the Access Point when one of mentioned events is registered. The window can also include buttons which can be used to control door (e.g. open remotely).

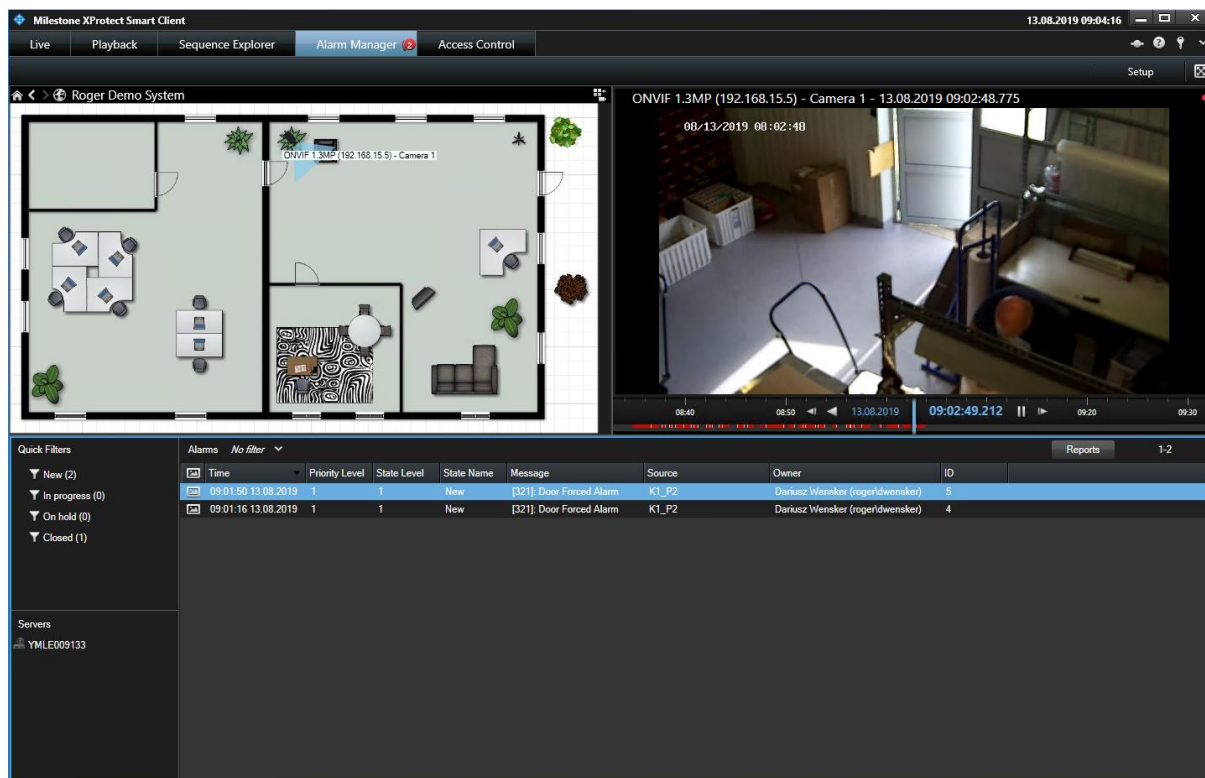
XProtect system reacts to [619] and [630] events and displays Access Request window because both events are assigned to *Access Request* category. Default event categories can be changed in XProtect Management Client selecting *Access Control* -> *Your system* -> *Access Control Events*.

The commands which are available in Access Request window can be defined by operator in XProtect Management Client selecting *Access Control*-> *Created system* -> *Access Request Notifications*. Additionally it is necessary to define new or modify default notification rule in XProtect Management Client selecting *Rules and Events* -> *Rules*.



Alarms

RACS 5 events can generate alarms in XProtect system. Alarms are defined in XProtect Management Client selecting *Alarms* in the navigation tree. When alarm is raised then it can be displayed in *Alarm Manager* tab of XProtect Smart Client program. Alarms can be associated with maps and cameras of XProtect system. Operator can interact with alarms (acknowledge, set on hold, close, edit, etc.)



The screenshot displays the Milestone XProtect Smart Client interface. The top menu bar includes 'Live', 'Playback', 'Sequence Explorer', 'Alarm Manager' (selected), and 'Access Control'. The main area is divided into three sections: a map view on the left showing a floor plan with camera locations, a video feed on the right showing a camera view, and a table of alarms at the bottom.

Map View: Shows a floor plan with camera locations. The camera is labeled 'ONVIF 1.3MP (192.168.15.5) - Camera 1'.

Video Feed: Shows a camera view of a room. The camera is labeled 'ONVIF 1.3MP (192.168.15.5) - Camera 1'. The timestamp is '08/13/2019 08:02:48'.

Alarms Table:

Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
09:01:50 13.08.2019	1	1	New	[321]: Door Forced Alarm	K1_P2	Dariusz Wonsker (roger@dwonsker)	5
09:01:16 13.08.2019	1	1	New	[321]: Door Forced Alarm	K1_P2	Dariusz Wonsker (roger@dwonsker)	4

Contact:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Fax: +48 55 272 0133
Tech. support: +48 55 267 0126
E-mail: support@roger.pl
Web: www.roger.pl