Software description

SUPERVISORY SOFTWARE

NMS ACCESS CONTROL

Version 3.0.XX Update: 03-07-2020

AAT SYSTEMY BEZPIECZEŃSTWA Sp. z o.o.
431 Pulawska St, 02-801 Warsaw, phone: +48 22 546 05 46, fax: +48 22 546 05 01
www.aat.pl

What for and for whom this manual is intended.

This manual is intended for installers and people who want to read the NMS ACCESS CONTROL program in detail. It describes all the windows and functions of the program according to the menu lay-out.

A description of the steps related to the installation process of the program and the programming of the system in the recommended order is contained in the *NMS ACCESS CONTROL – Installation and operation manual.*

The development of the NMS ACCESS CONTROL program is planned with new advanced access control functions and further functionalities related to the video surveillance system (VSS), which will be successively appearing in successive versions.

TABLE OF CONTENTS

TABLE OF CONTENTS

Section 1 Introduction

1.1 Basic information

The NMS ACCESS CONTROL is a new supervisor software that is designed for small and medium-sized access control systems. It works with the KDH-KS3012-IP, KDH-KS3024-IP and KDH-KS2000-IP-ELV standard controllers. Due to the client-server structure, it is possible to operate the system from multiple workstations (2 stations under a free license, additional after the purchase of expansion licenses). The system is simple to install and has an operator friendly graphical interface. In the current version, it is a program designed primarily to support access control systems, but it contains some elements of VSS and an extensive visualization of system elements state.

The operator interface allows:

- defining system parameters (permissions for operators, licenses, backup)
- configuration of parameters of physical system components (controllers, doors, readers)
- defining logical elements (schedules, access levels, cards)
- define scenarios that automatically react to events in the system
- monitoring the status of the "on-line" system using the icons of system elements located on the site maps (with hierarchical structure), on the synoptic array and through the messages displayed on the event stack
- displaying user pictures after using the card
- displaying of cameras located in controlled passages automatically after an event or by clicking on the icon
- access control to floors through the reader located in the elevator cabin (with the option to unlock all or selected floors by the operator or schedule; * option available soon)
- access control to locker cabinets - up to 69 with one set of controller, modules and reader
- generating filtered event reports (automatically or on demand) and save in CSV or HTML format (with print to PDF option)

The NMS ACCESS CONTROL software also offers a number of features described in detail further that allow to meet the requirements often posed by the system administrator, such as: access after using 2, 3 or 4 cards, the first unlock of the controlled passage using the so-called "first card" with special privileges, access after operator confirmation, man trap and anti-passback within the controller. The program will be gradually expanded with new features.

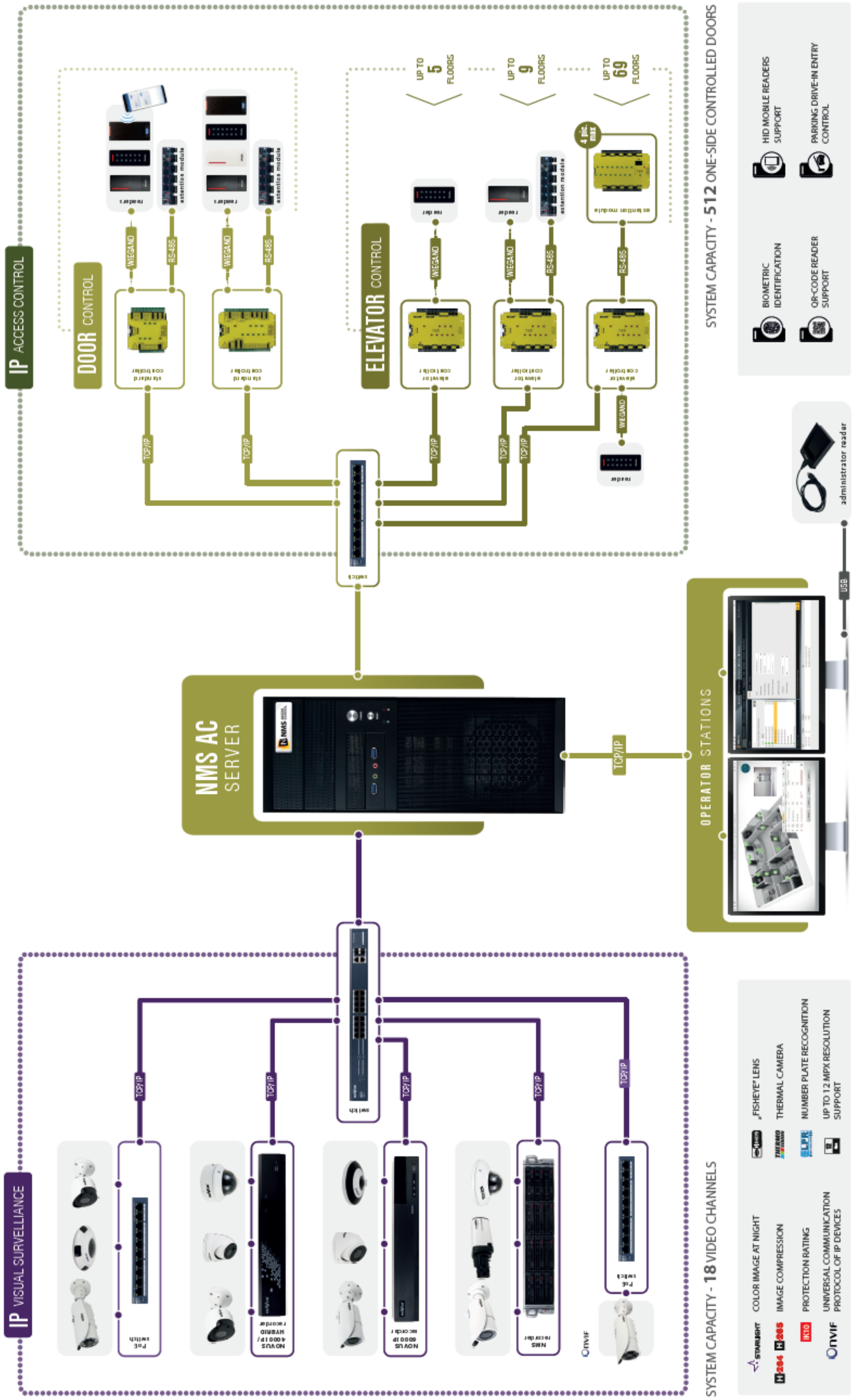
The list of key functions and parameters of the system is presented in the attached table and the structure of the system is shown in the enclosed scheme. Controllers with IP ports communicate with the server service over Ethernet. In the current version of the program, the system can support up to 128 controllers (8 under the free license, additional after the purchase of expansion licenses), so with 4-door controllers - 512 single-sided controlled doors or 256 double-sided. The capacity of card users is 20 000 cards.

The basic license version is available free of charge for download from the website www.nmsac.aat.pl in the download section or you can obtain it by contacting the AC Department and the description of the licenses tab is located in ‘System settings’ chapter of this manual. Paid licenses extending the capacity of the system can be found in the price list in the NMS ACCESS CONTROL section.

1.2 NMS ACCESS CONTROL functions and parameters

Parameter or function name	Parameter or function value
PC operating system	Windows 10 Pro
Database	Microsoft SQL
‘On-line’ monitoring	YES
NOVUS NVR and IP cameras integration	YES
Elevator control (up to 69 floors)	YES
Panels with system elements icons	YES
User photos displaying	YES
Access related functions	
- user identification mode	Card, PIN, card or PIN, card + PIN
- local anti-passback	YES
- global anti-passback	YES
- „first opening card”	YES
- supervisor mode	YES
- multiple access (2 - 4)	YES
- latch mode	YES
- schedule based with first opening card or automatic unlocking	YES
Alarm functions	
- threaten code	YES
Users import from file	YES
Controllers	KDH-KS3012-IP, KDH-KS3024-IP. KDH-KS3000-IP-ELV
KaDe controller’s memory capacity	
- card memory	20 000
- event memory	50 000
Communication	
Built in IP ports	- Ethernet network
Readers and cards	
- card format	26-40 bit Wiegand format compatible
- card type	any reader compatible technology
Access related parameters	
- access levels quantity	200
- schedules quantity	200
- holidays quantity	80 (32 days)
Reports	Filtered, save in CSV, HTML (PDF) format

1.3 System block diagram



1.4 PC minimal requirements

The minimum requirements listed below should be considered as absolute minimum and intended for small systems. It is not possible to specify exactly what parameters the computer should have for a given number of devices. Therefore, the given parameters in terms of processors or RAM should be treated as indicative.

- Operating system: Windows 10 Pro,
- Intel Pentium Gold G5400 processor, 8GB RAM, PCI Express 16x graphic card with 1 GB memory and DirectX 9.0 support
- Network card 10/100 MB, HDD 500 MB (for system without video devices)

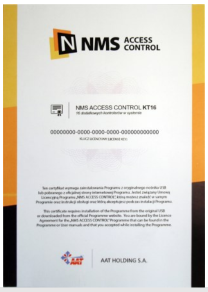
The .NET Framework V 4.7 and MS SQL Server installation is required for the correct operation of the system. If they are not in the system, they will be automatically installed before the installation of the application because they are in the installation file.

For larger systems that include devices for the access control system and the video surveillance system in quantities close to the maximum capacity of the system we recommend the computer station from our offer. It has sufficient parameters to handle the size of the system.

ATTENTION! Controllers should be connected to separated physical network (switch, network card etc.) or separated VLAN.

1.5 Maximal system capacity (after adding extension licenses)

* Due to limited functionality of integrated VSS in current version of NMS ACCESS CONTROL we do not offer paid extension options for video. They will be available in succeeding versions.



NMS ACCESS CONTROL

NMS ACCESS CONTROL **KT16**
16 dodatkowych kontrolerów w systemie

00000000-0000-0000-0000-000000000000
KLUCZ LICENCYJNY (LICENSE KEY)

Ten certyfikat wymaga zainstalowania Programu z oryginalnego nośnika USB lub pobranego z oficjalnej strony internetowej Programu. Jesteś związany Umową Licencyjną Programu „NMS ACCESS CONTROL", którą możesz znaleźć w samym Programie oraz instrukcji obsługi oraz którą akceptujesz podczas instalacji Programu.

This certificate requires installation of the Programme from the original USB or downloaded from the official Programme website. You are bound by the Licence Agreement for the „NMS ACCESS CONTROL" Programme that can be found in the Programme or User manuals and that you accepted while installing the Programme.

AAT HOLDING S.A.

Licenses	Free	Max.
Client stations licenses	2	10
Controllers licenses	8	128
Number of controlled doors:		
- Single-sided (KS-3024)	32	512
- Double-sided (KS-3024)	16	256
NOVUS video channels licenses	16	
ONVIF video channels licenses	1	
RTSP video channels licenses	1	*
Video channels summary license		64
Panels licenses	4	64
Scenarios licenses	4	64

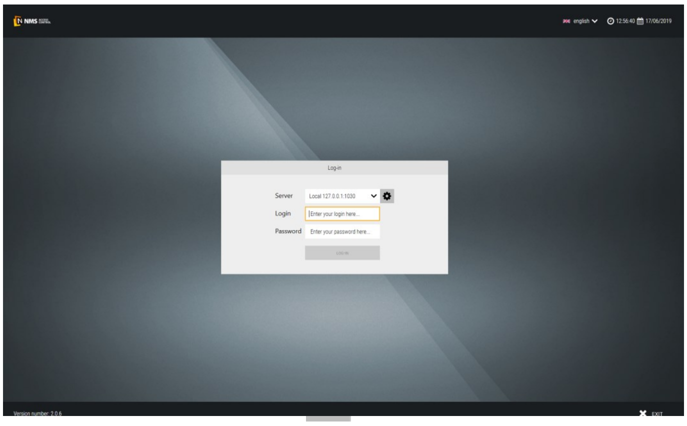
Paid licenses
Client stations licenses
NMS ACCESS CONTROL KL1
Controllers licenses
NMS ACCESS CONTROL KT4
NMS ACCESS CONTROL KT8
NMS ACCESS CONTROL KT16
NMS ACCESS CONTROL KT32
Panels licenses
NMS ACCESS CONTROL PN4
NMS ACCESS CONTROL PN8
NMS ACCESS CONTROL PN16
NMS ACCESS CONTROL PN32
Scenarios licenses
NMS ACCESS CONTROL SC4
NMS ACCESS CONTROL SC8
NMS ACCESS CONTROL SC16
NMS ACCESS CONTROL SC32

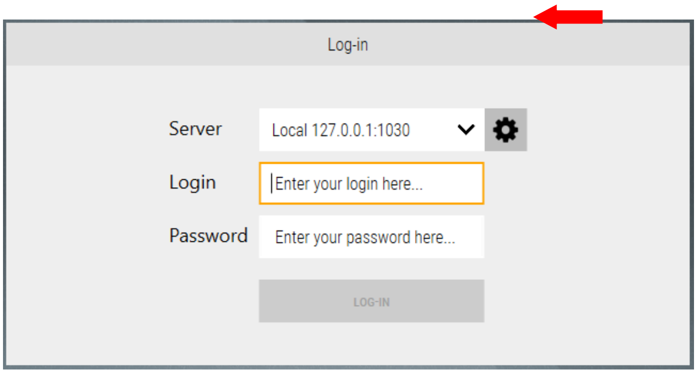
1.6 Software starting

After NMS AC installation icon shown below appears on the desktop by default and NMS ACCESS CONTROL group is crated in Windows start menu. You can run the software using them.

Starting the program results in the logon screen. There is a login window in its central part . In the ***Server*** section , you can select NMS ACCESS CONTROL server that you want to connect to. The installed NMS AC client application allows you to connect to one any server. The server application runs as a service and starts by default when Windows starts. This allows you to connect to and log in from any client station within the network. The server service connects to the system SQL database. The icon next to the check box selected in the following drawing opens the ***server list***. Enter the operator's login details in the ***login*** and ***password*** fields . The default operator's Login is **root**, but the password is **pass**. To prevent unauthorized access to the system, we recommend that you change this password during setup. This step will be described later in this manual. The ***exit*** button in the bottom right corner closes the program.

ATTENTION! Controllers should be connected to separated physical network (switch, network card etc.) or separated VLAN.





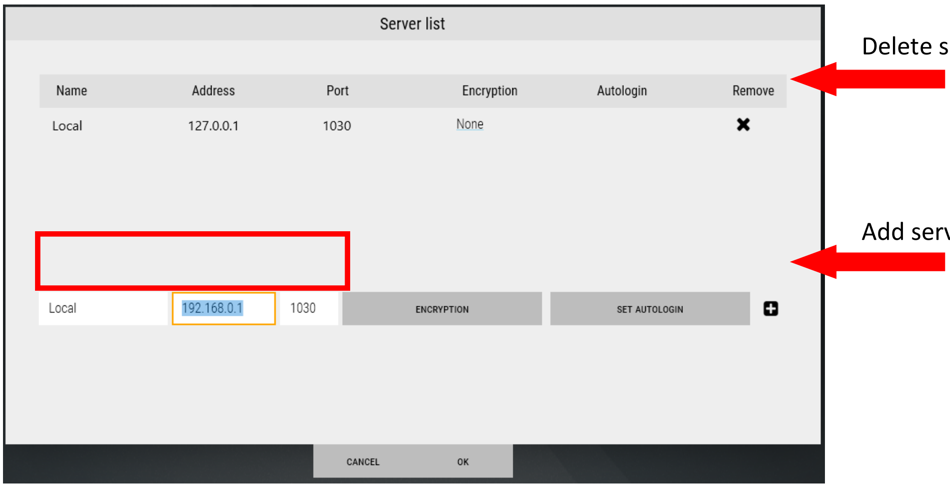
Log-in

Server: Local 127.0.0.1:1030

Login: Enter your login here...

Password: Enter your password here...

The server list window allows you to add, remove and configure NMS ACCESS CONTROL servers which you can connect an operator station to. The server settings that can be performed in this window are: name, IP address, port, type of communication encryption, autologin and alarms and messages sounds.



Server list

Name	Address	Port	Encryption	Autologin	Remove
Local	127.0.0.1	1030	None		✖

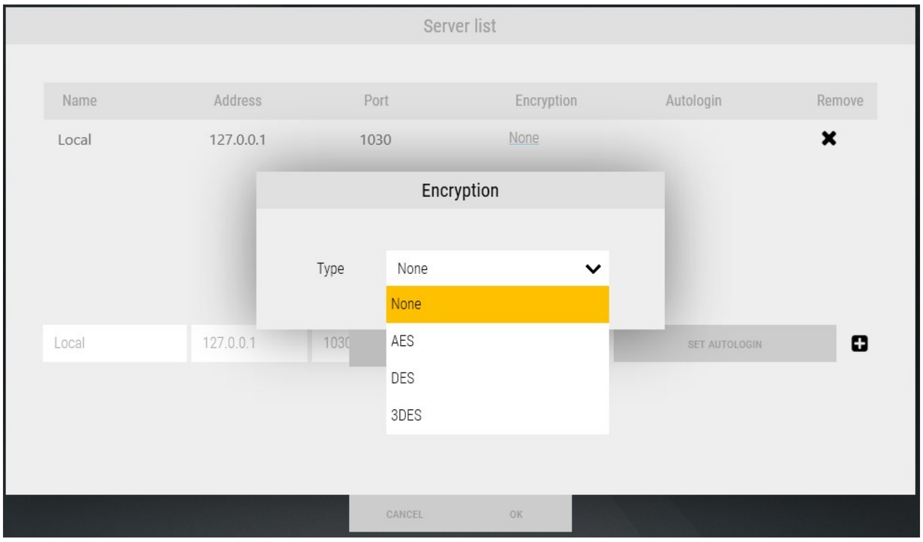
Local | 192.168.0.1 | 1030

Delete server

Add server

When you select a server on the list, its network parameters are configured in the fields marked in the previous drawing.

When you click the ***Encryption*** button in the dialog box that appears, you can select from a list of several available encryption types between server and client applications. ***None*** means that there will be no encryption.



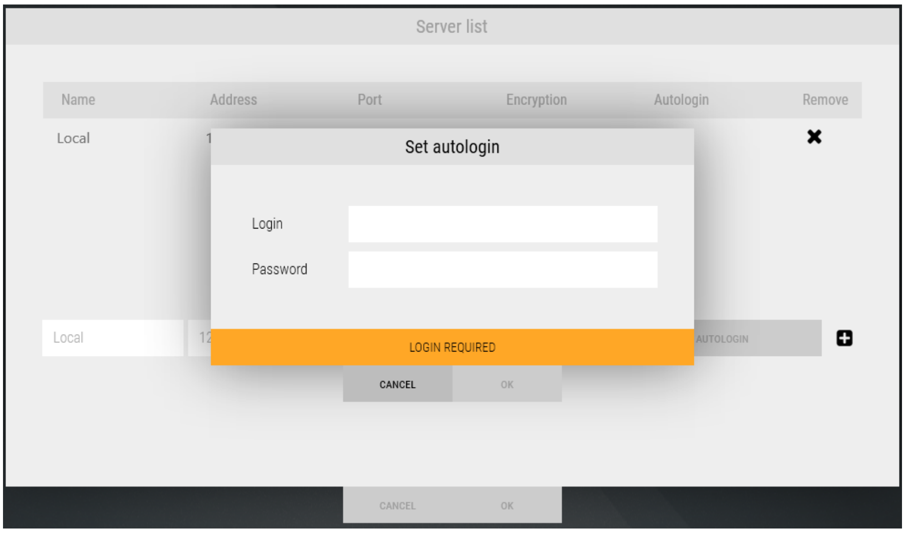
Server list

Name	Address	Port	Encryption	Autologin	Remove
Local	127.0.0.1	1030	None		✖

Encryption

Type: None

After clicking on the ***Autologin*** button there is possibility to set automatic operator login directly after software start.



Server list

Name	Address	Port	Encryption	Autologin	Remove
Local	1				✖

Set autologin

Login:

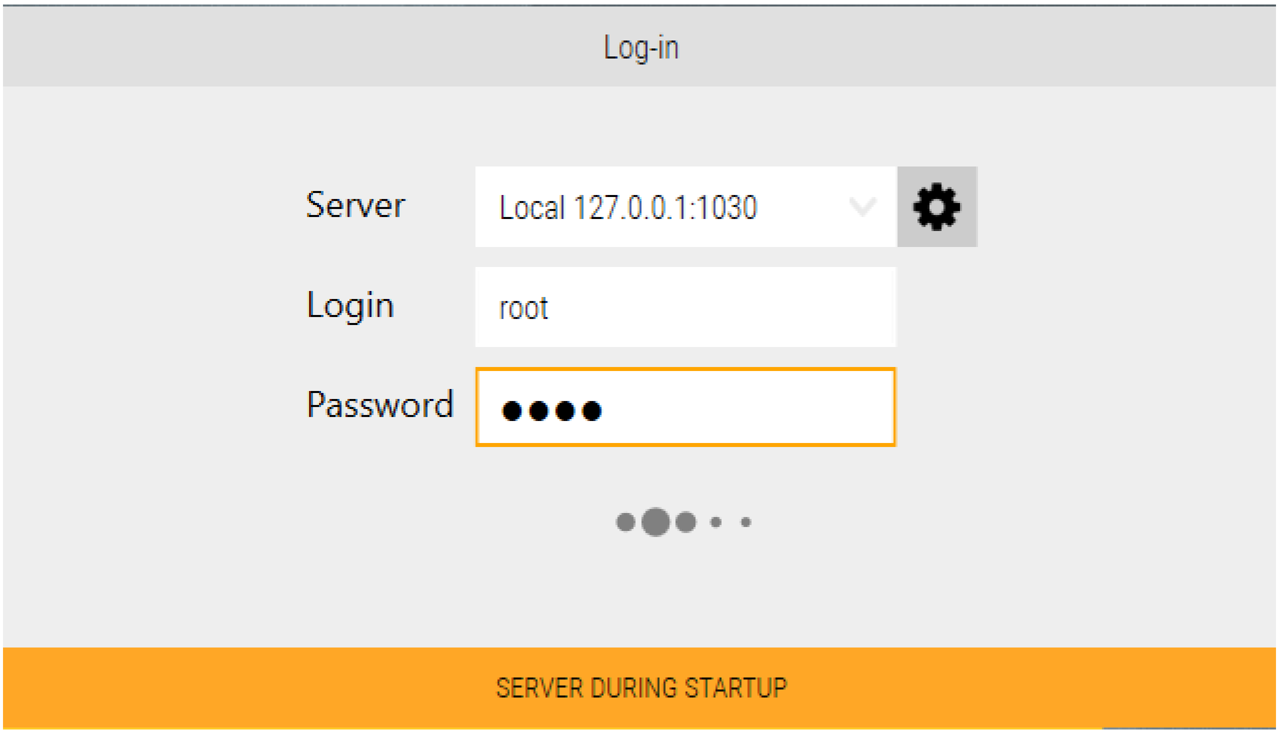
Password:

From ***Alert sound*** and ***Message sound*** drop-down lists event sound can be selected .

You must approve any of the options you have entered or selected by clicking ***OK***. Clicking ***Cancel*** discards changes to the settings.

After you enter the correct login information, the ***Quick Start*** window appears as in the drawing on the next page.

After you type the login and password and click ***Log-in*** button, *Server starting* information may appear at the bottom of the window. This means that you must wait because the server service starts (for example, after re-boot).



Log-in

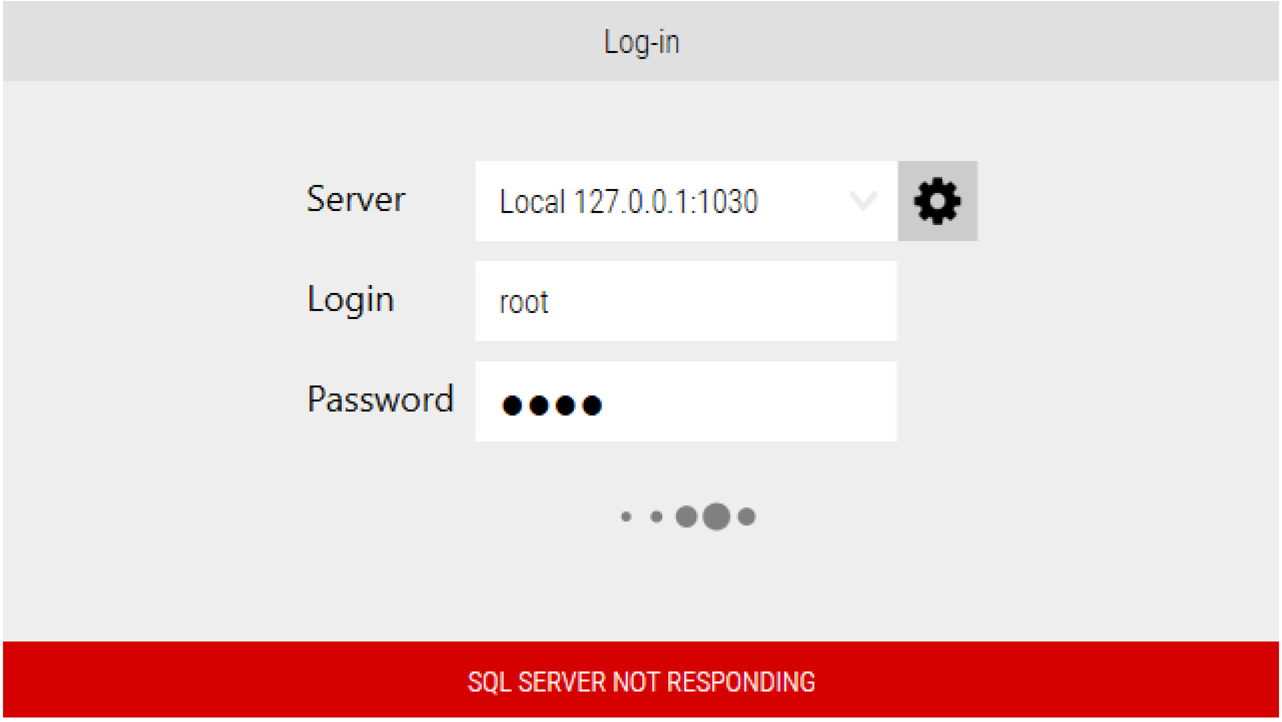
Server: Local 127.0.0.1:1030

Login: root

Password: ●●●●

SERVER DURING STARTUP

In the same situation, the lower part of the window may display a message that the *Server is not responding.* This means that the server service was stopped for some reason. You must then run the service manually using the Task/Service Manager window in Windows.



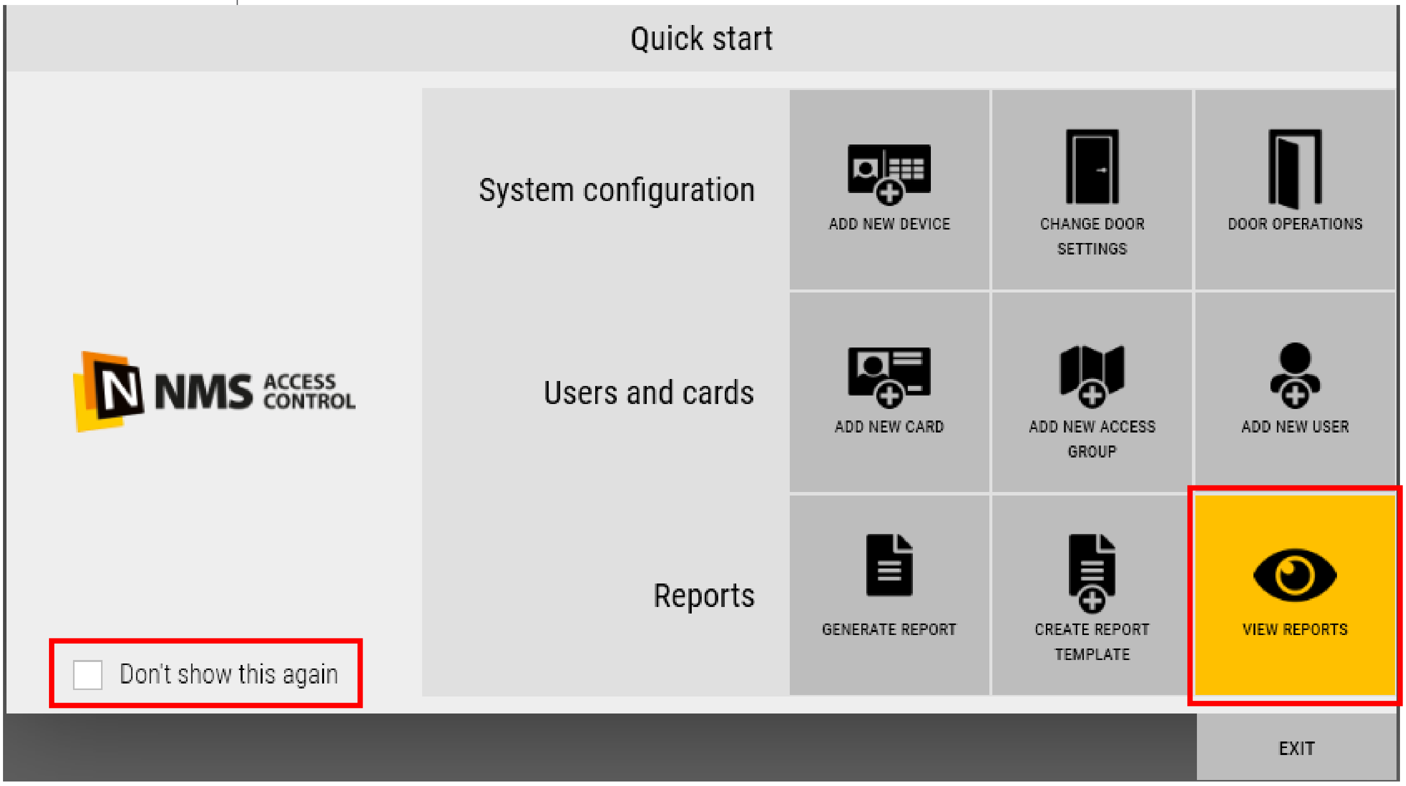
Log-in

Server: Local 127.0.0.1:1030

Login: root

Password: ●●●●

SQL SERVER NOT RESPONDING



The ***Quick Start*** window contains nine shortcut icons for the most commonly used system options from three thematic groups:

1. ***System Configuration***

- ***Add new device*** - opens the *Add AC or VSS device* window
- ***Change door settings*** - quickly opens the Door Settings Details tab in the controllers added to the system
- ***Door Operations*** - quickly opens operations that can be performed on the doors added to the system tab

2. ***Users and Cards***

- ***Add new Card*** - opens the window for adding cards to the system
- ***Add new Access group*** - quickly opens the *Access Group* tab and adds a new access group
- ***Add new User*** - quickly opens the *Users* tab and adds a new user

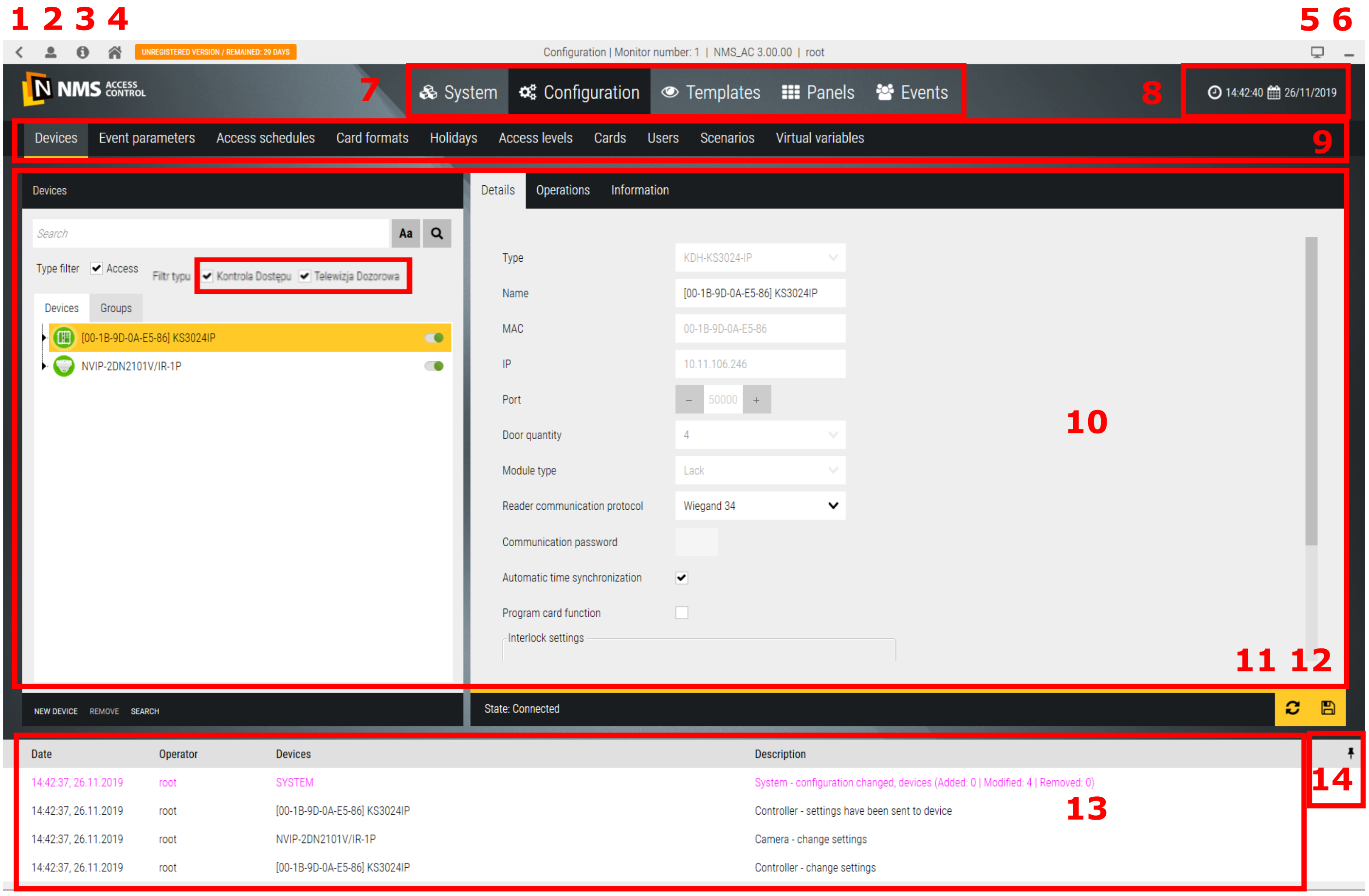
3. ***Reports***

- ***Generate report*** - opens a window for generating an automatic report
- ***Create a report template*** - opens the *List of events* tab in the *Events* section
- ***View reports*** - opens *Files on server* tab in the *Events* section

If you select ***Don't show this again*** checkbox shown in the image above, the ***Quick Start*** window is not automatically displayed when you run NMS AC. The ***Exit*** button closes the ***Quick Start*** window.

1.7 Operator screen and navigation in the program window

Operator screen is graphic user interface allowing interaction with NMS AC system. Its view is shown in the picture below.



Type	KDH-KS3024-IP
Name	[00-1B-9D-0A-E5-86] KS3024IP
MAC	00-1B-9D-0A-E5-86
IP	10.11.106.246
Port	50000
Door quantity	4
Module type	Lack
Reader communication protocol	Wiegand 34
Communication password	
Automatic time synchronization	☑
Program card function	☐

Date	Operator	Devices	Description
14:42:37, 26.11.2019	root	SYSTEM	System - configuration changed, devices (Added: 0 | Modified: 4 | Removed: 0)
14:42:37, 26.11.2019	root	[00-1B-9D-0A-E5-86] KS3024IP	Controller - settings have been sent to device
14:42:37, 26.11.2019	root	NVIP-2DN2101V/IR-1P	Camera - change settings
14:42:37, 26.11.2019	root	[00-1B-9D-0A-E5-86] KS3024IP	Controller - change settings

1. ***Back*** button - revers to the previously visited screen.

2. ***Logout*** button - logs out the current operator and opens the login screen.

3. ***About application*** button - opens information window about the installed software version.

4. ***Quick Start*** button - opens the *Quick Start* window.

5. ***Monitor selection*** button on which you want to display the operator screen.

6. ***Minimize*** button - minimizes the NMS AC window.

7. Section selection bar - click on the corresponding section allows you to configure or preview the options.

8. Current server time and date.

9. Tabs bar - allows you to navigate through the tabs of the selected section.

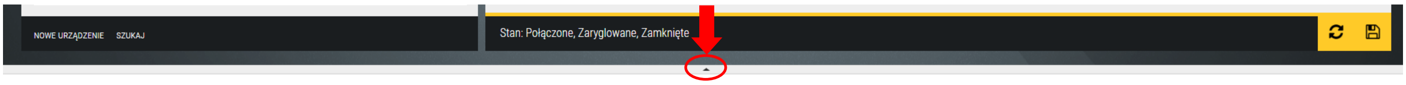
10. Workspace.

11. ***Refresh*** button - refreshes the displayed data.

12. ***Save*** button - saves changes made in the system configuration.

13. ***System Log*** window - this window displays logs about changes in system configuration and other events in the system.

14. ***Pin*** button - allows you to change the display of the log window. It can be permanently visible in the screen area or as a collapsible beam at the bottom, thus increasing the Work field 10. When you click on this button you can collapse the beam. To expand it , click on:



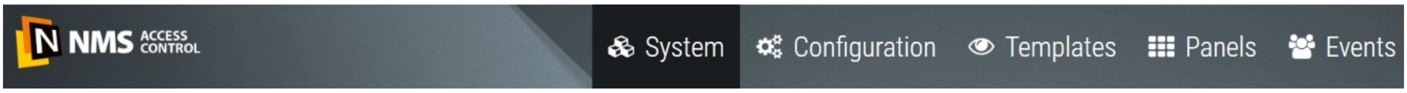
Stan: Połączone, Zaryglowane, Zamknięte

The beam is displayed automatically when new events are appearing in this window, and collapses when clicked in area 10.

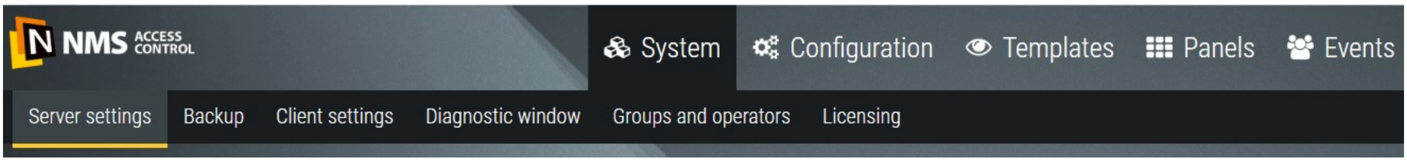
1.8 Program menu

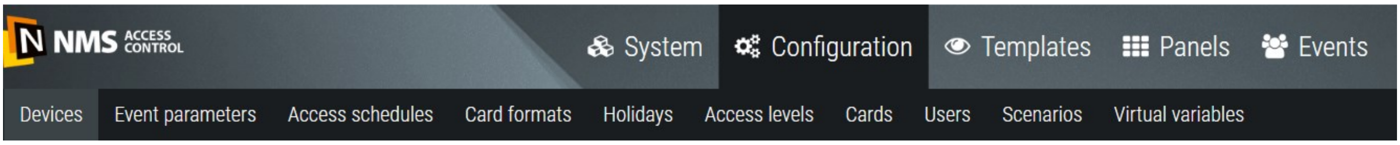
Program menu contains two bars.

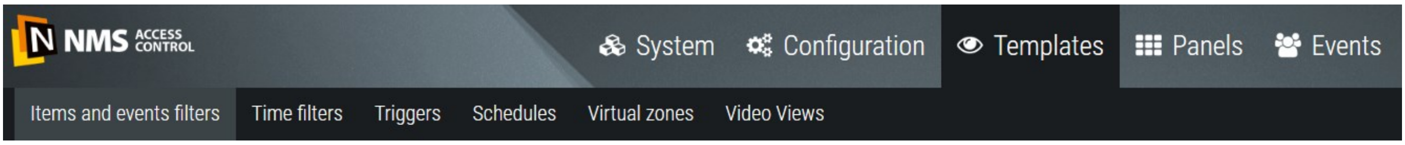
Main bar:

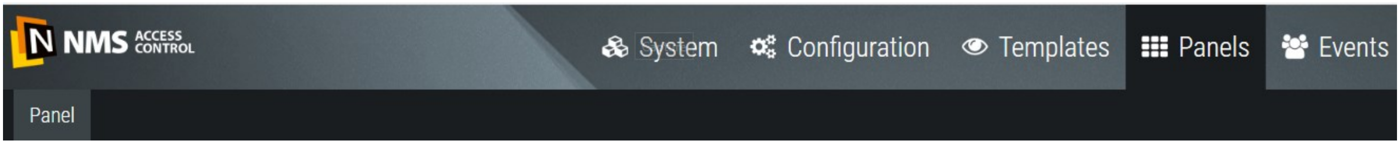


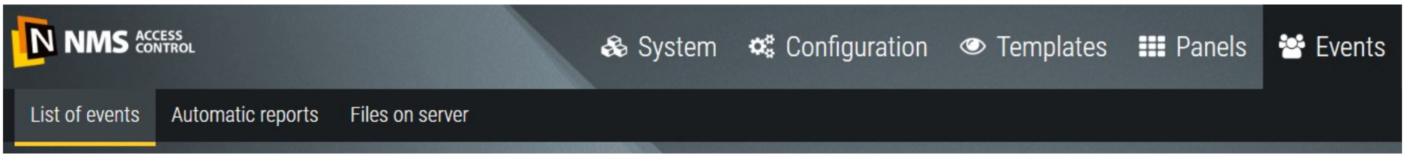
It has 5 tabs. Each contains following positions.



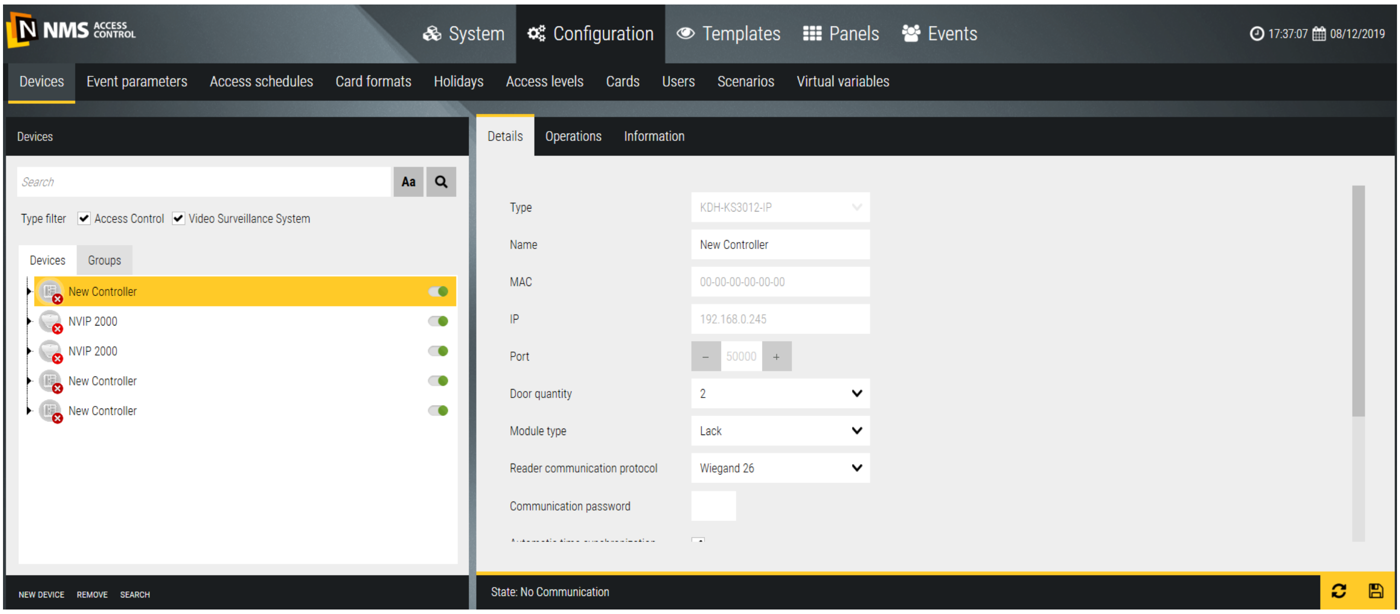








Each tab on the second bar contains further tabs below and two windows: left wit elements list and right with settings of position selected in the left window. For example in *Configuration / Devices* window it looks as following:



Type filter ☑ Access Control ☑ Video Surveillance System

- New Controller
- NVIP 2000
- NVIP 2000
- New Controller
- New Controller

Type	KDH-KS3012-IP
Name	New Controller
MAC	00-00-00-00-00-00
IP	192.168.0.245
Port	– 50000 +
Door quantity	2
Module type	Lack
Reader communication protocol	Wiegand 26
Communication password	

State: No Communication

1.9 Program window icons

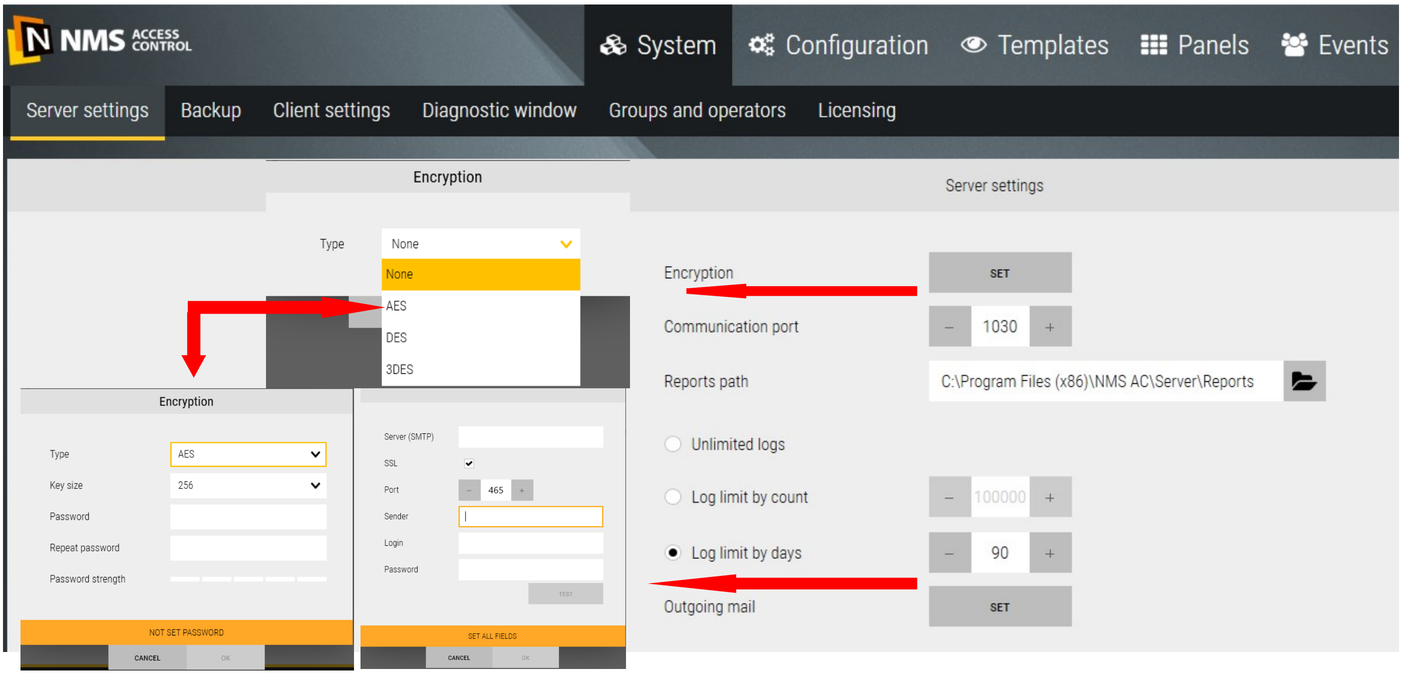
In program windows following icons occur:

Icon symbol	Description	Localization
<	Back	Top bar
👤	Log-out	Top bar
ℹ	About	Top bar
🏠	Quick start	Top bar
🖥	Choose monitor	Top bar
—	Minimize	Top bar
✏	Panel edition	Top bar
⚙	Back to configuration	Top bar
🔍	Search	-
👁	Go to panel	-
📅	Date	-
🕒	Time	-
📌	Attach console	-
CSV	CSV report	Events
HTML	HTML report	Events
A	Automatic report	Events
✓✓	Delete alarms	-
🔔	Alarm	-
🔄	Refresh	Configuration
💾	Save	Configuration
Aa	Capitalization	-
⚠	Warning/Error	-

Section 2 System

In *System* tab you can set server parameters, backup or restore system, set operator language, add new operators with privileges according to program and expand licenses.

2.1 Server settings



Encryption: Type: None (None, AES, DES, 3DES)

Encryption: Type: AES; Key size: 256; Password; Repeat password; Password strength

Server (SMTP); SSL ☑; Port: 465; Sender; Login; Password

Encryption: SET

Communication port: 1030

Reports path: C:\Program Files (x86)\NMS AC\Server\Reports

○ Unlimited logs

○ Log limit by count: 100000

● Log limit by days: 90

Outgoing mail: SET

Encryption - after clicking on *Set* button you can choose encryption mode between server and operator station. You can choose from among three the most common types: AES, DES, 3DES or none. After selecting encryption and key size you have to set the password which will be used in communication between server and operator station, which will connect to it. If you set encryption here, you have to set the same parameters in login window (*Server list - Encryption*) on all operator stations connected to this server.

Communication port - in LAN default value 1030 is recommended.

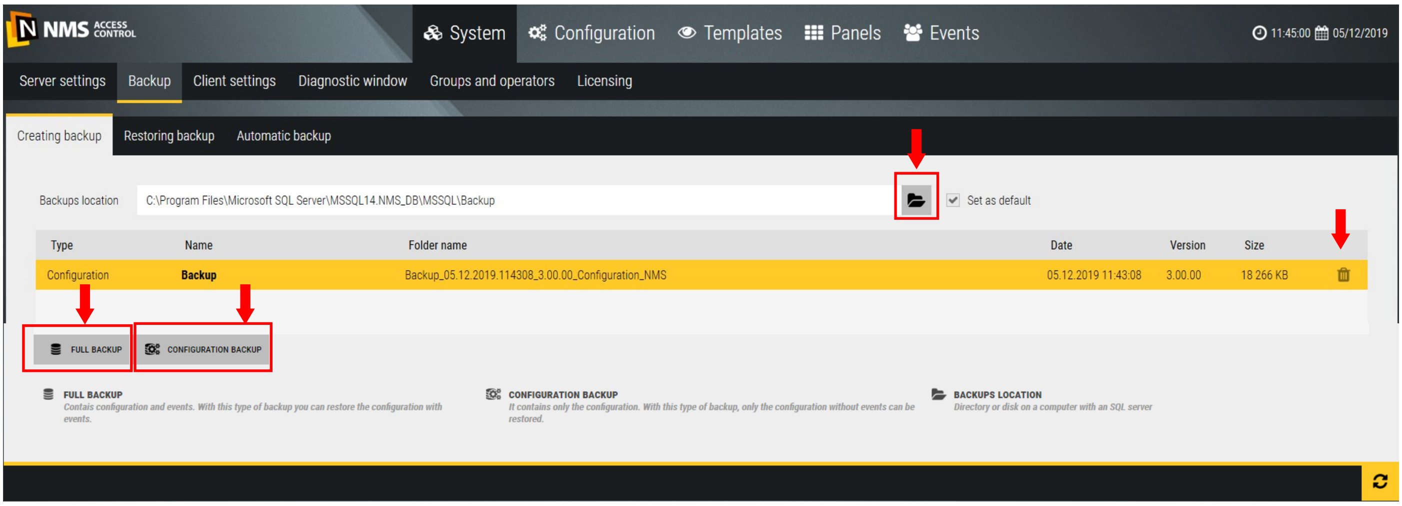
Reports path - default path to directory which reports are saved in. Click directory icon to change.

Log limit - one of three logs stored in database limit options to choose: unlimited logs, log limit by count or log limit by days.

Outgoing mail - fill fields according to mail server and user (e-mail, username and password) settings.

2.2 Backup

In this tab you can create or restore system backup.



Backups location: C:\Program Files\Microsoft SQL Server\MSSQL14.NMS_DB\MSSQL\Backup ☑ Set as default

Type	Name	Folder name	Date	Version	Size
Configuration	**Backup**	Backup_05.12.2019.114308_3.00.00_Configuration_NMS	05.12.2019 11:43:08	3.00.00	18 266 KB

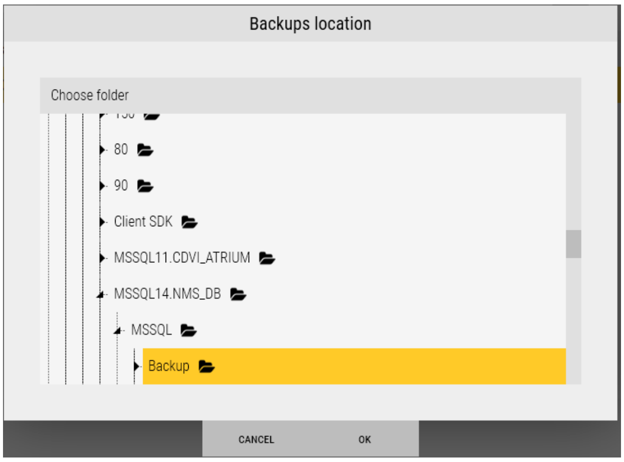
FULL BACKUP
Contais configuration and events. With this type of backup you can restore the configuration with events.

CONFIGURATION BACKUP
It contains only the configuration. With this type of backup, only the configuration without events can be restored.

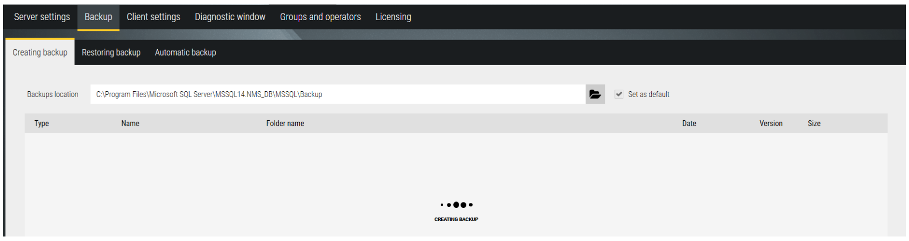
BACKUPS LOCATION
Directory or disk on a computer with an SQL server

Creating backup

On the top of the window system backup localization is displayed. You can change default path by clicking on directory icon.



You can select directory on current disk, pendrive or other computer mapped disk and select it as default localization. You can create full backup or configuration backup only by clicking one of the buttons on the bottom of the window. Backup name's beginning can be changed. Default name contains generation date and time tag and backup type.

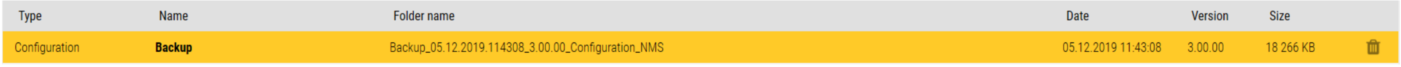


Backups location: C:\Program Files\Microsoft SQL Server\MSSQL14.NMS_DB\MSSQL\Backup

☑ Set as default

Type	Name	Folder name	Date	Version	Size

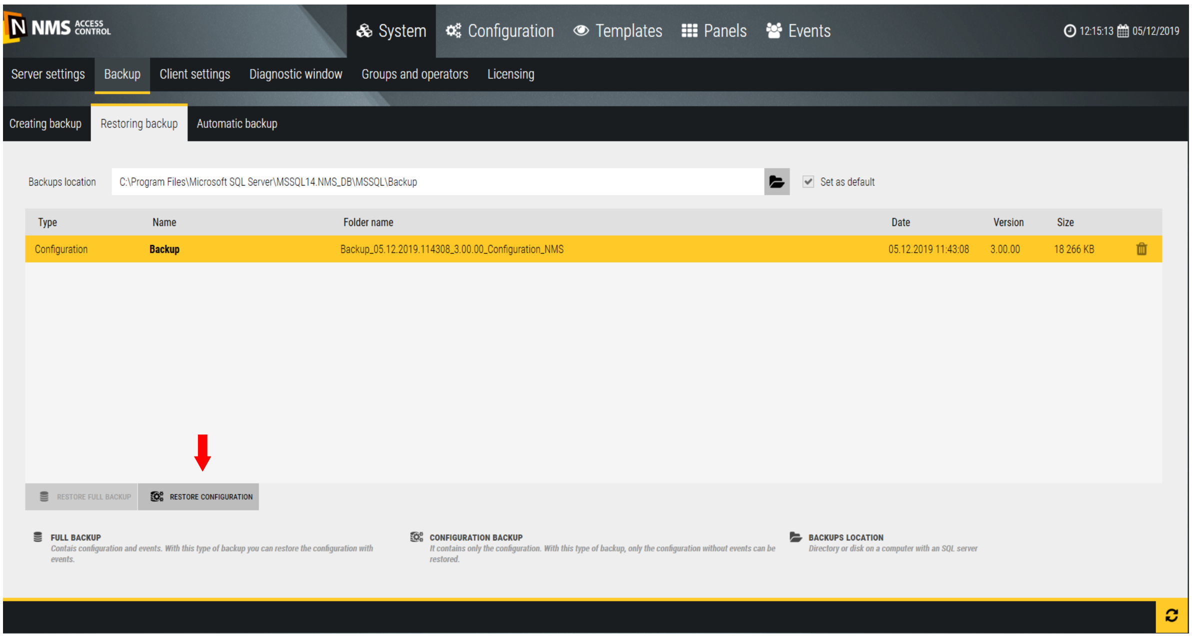
After backup creation it appears on the list. After pointing selected backup with cursor recycle bin icon appears on the right - you can delete backup by clicking it.



Type	Name	Folder name	Date	Version	Size	
Configuration	**Backup**	Backup_05.12.2019.114308_3.00.00_Configuration_NMS	05.12.2019 11:43:08	3.00.00	18 266 KB	🗑

Restoring backup

Window which you can restore backup from looks similar as creating backup window. To restore system backup you have to select directory which backups are stored in, select one and click *Restore backup* button on the bottom of the window.



Backups location: C:\Program Files\Microsoft SQL Server\MSSQL14.NMS_DB\MSSQL\Backup

☑ Set as default

Type	Name	Folder name	Date	Version	Size	
Configuration	**Backup**	Backup_05.12.2019.114308_3.00.00_Configuration_NMS	05.12.2019 11:43:08	3.00.00	18 266 KB	🗑

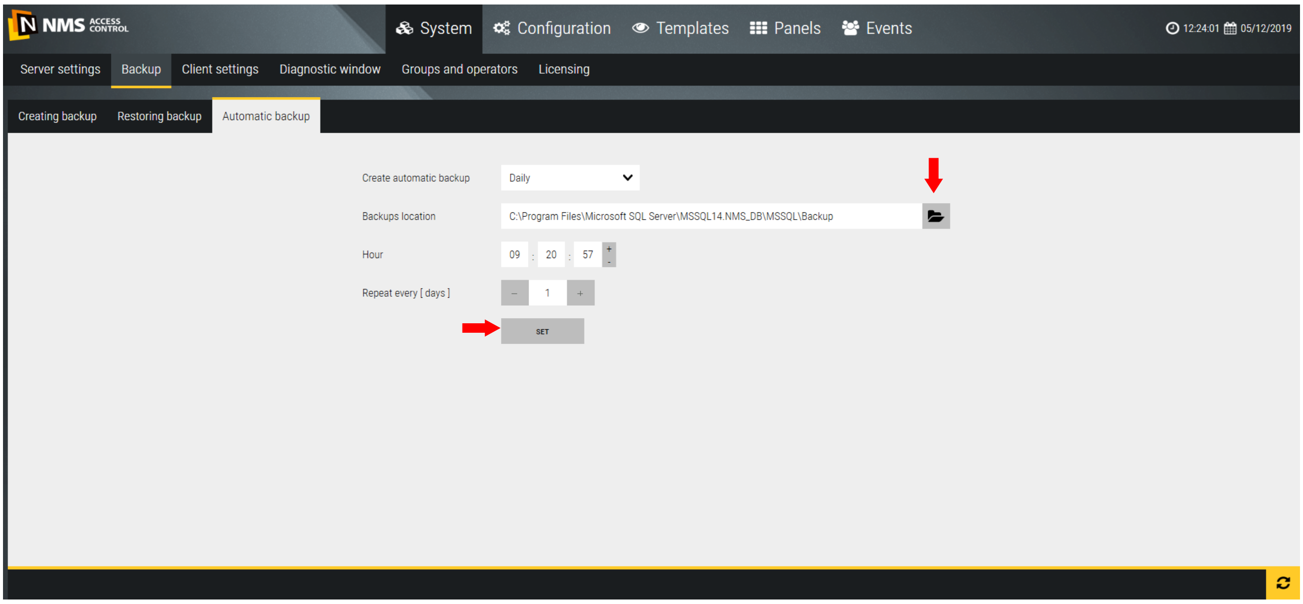
FULL BACKUP
Contais configuration and events. With this type of backup you can restore the configuration with events.

CONFIGURATION BACKUP
It contains only the configuration. With this type of backup, only the configuration without events can be restored.

BACKUPS LOCATION
Directory or disk on a computer with an SQL server

Automatic backup

A window in which you can set the parameters of an automatic backup.
The automatic backup can be created and saved daily, weekly or monthly.
Click SET after settings backup parameters.

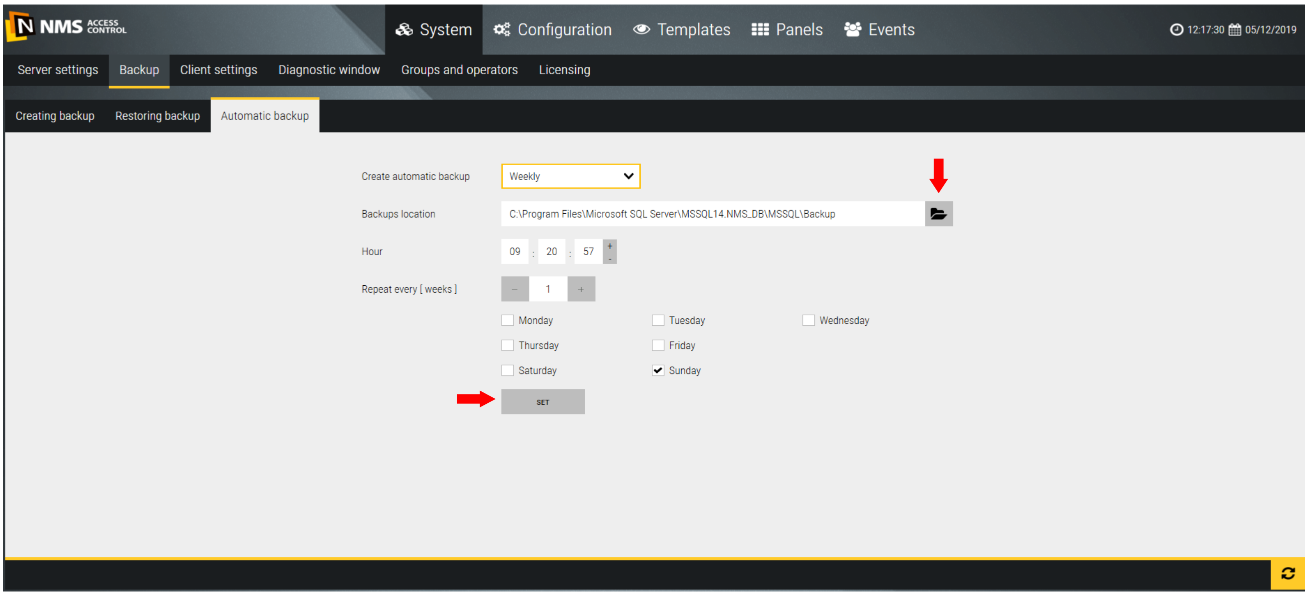


Create automatic backup: Daily

Backups location: C:\Program Files\Microsoft SQL Server\MSSQL14.NMS_DB\MSSQL\Backup

Hour: 09 : 20 : 57

Repeat every [days]: 1



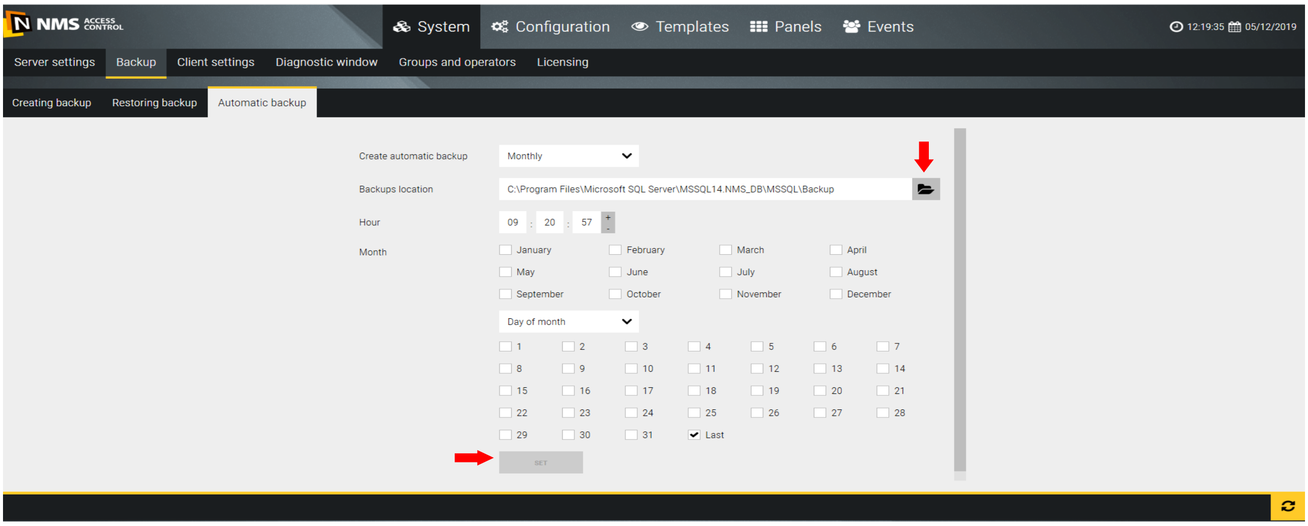
Create automatic backup: Weekly

Backups location: C:\Program Files\Microsoft SQL Server\MSSQL14.NMS_DB\MSSQL\Backup

Hour: 09 : 20 : 57

Repeat every [weeks]: 1

☐ Monday ☐ Tuesday ☐ Wednesday
☐ Thursday ☐ Friday
☐ Saturday ☑ Sunday



Create automatic backup: Monthly

Backups location: C:\Program Files\Microsoft SQL Server\MSSQL14.NMS_DB\MSSQL\Backup

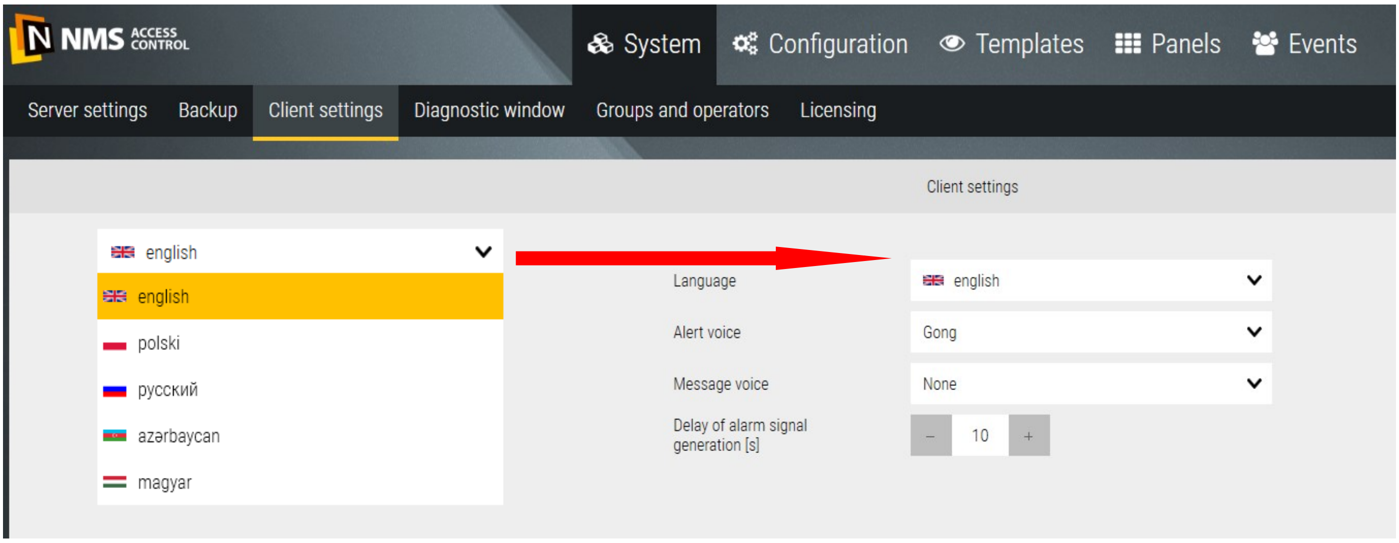
Hour: 09 : 20 : 57

Month:
☐ January ☐ February ☐ March ☐ April
☐ May ☐ June ☐ July ☐ August
☐ September ☐ October ☐ November ☐ December

Day of month
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14
☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21
☐ 22 ☐ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27 ☐ 28
☐ 29 ☐ 30 ☐ 31 ☑ Last

2.3 Client settings (operator station)

In this tab you can set program language for operator. You can currently choose from among four languages: English, Polish, Russian, Azeri and Hungarian. Other options are designed to alarm signalization settings.

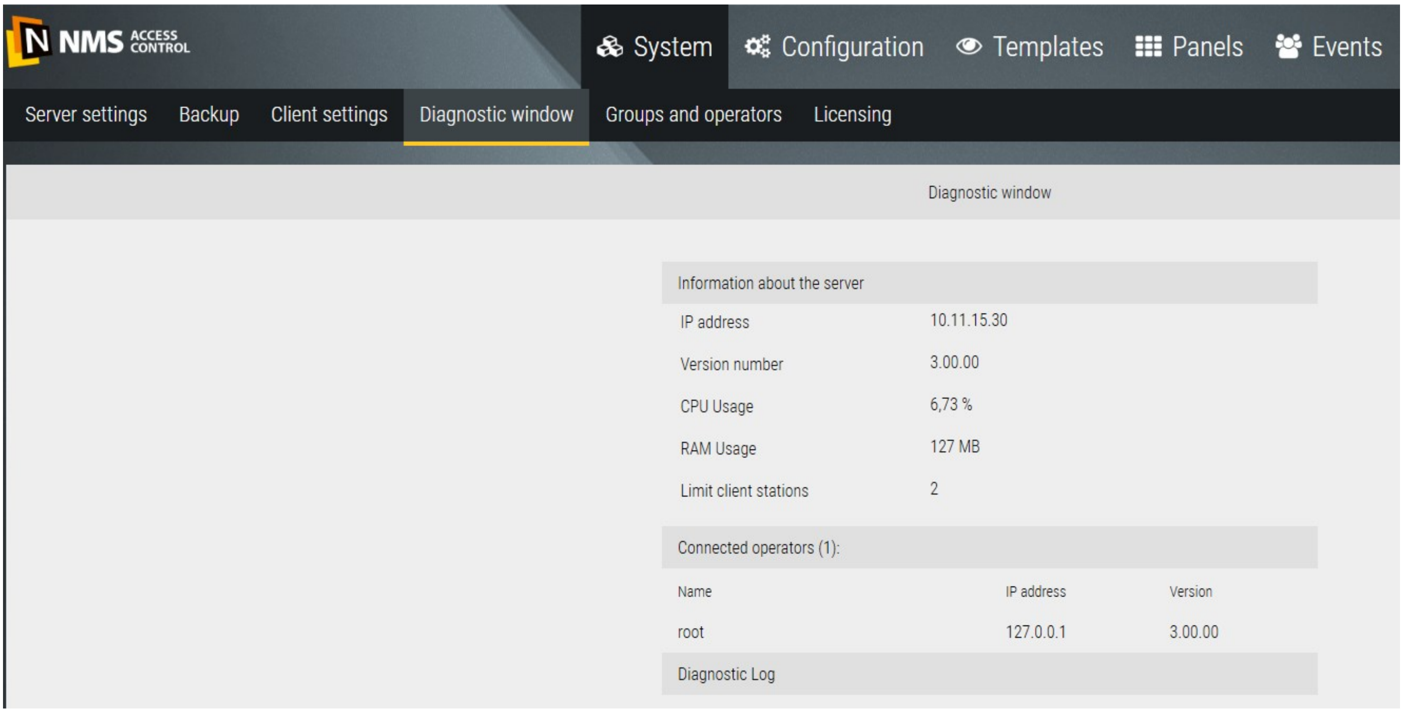


Client settings

Language	english
Alert voice	Gong
Message voice	None
Delay of alarm signal generation [s]	– 10 +

2.4 Diagnostic window

In this window you can see information about server address, program version, CPU and RAM usage, quantity of available operator stations according to owned license and connected operators list.



Diagnostic window

Information about the server

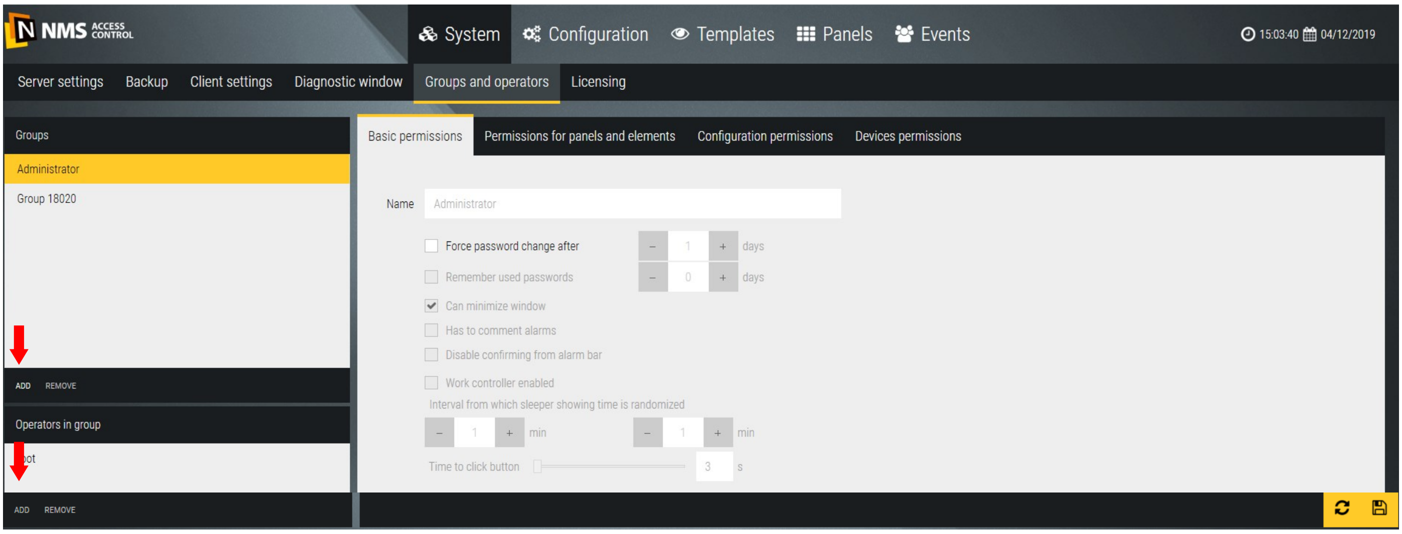
IP address	10.11.15.30
Version number	3.00.00
CPU Usage	6,73 %
RAM Usage	127 MB
Limit client stations	2

Connected operators (1):

Name	IP address	Version
root	127.0.0.1	3.00.00

Diagnostic Log

2.5 Groups and operators



Groups: Administrator, Group 18020

Operators in group: root

Name: Administrator

☐ Force password change after – 1 + days

☐ Remember used passwords – 0 + days

☑ Can minimize window

☐ Has to comment alarms

☐ Disable confirming from alarm bar

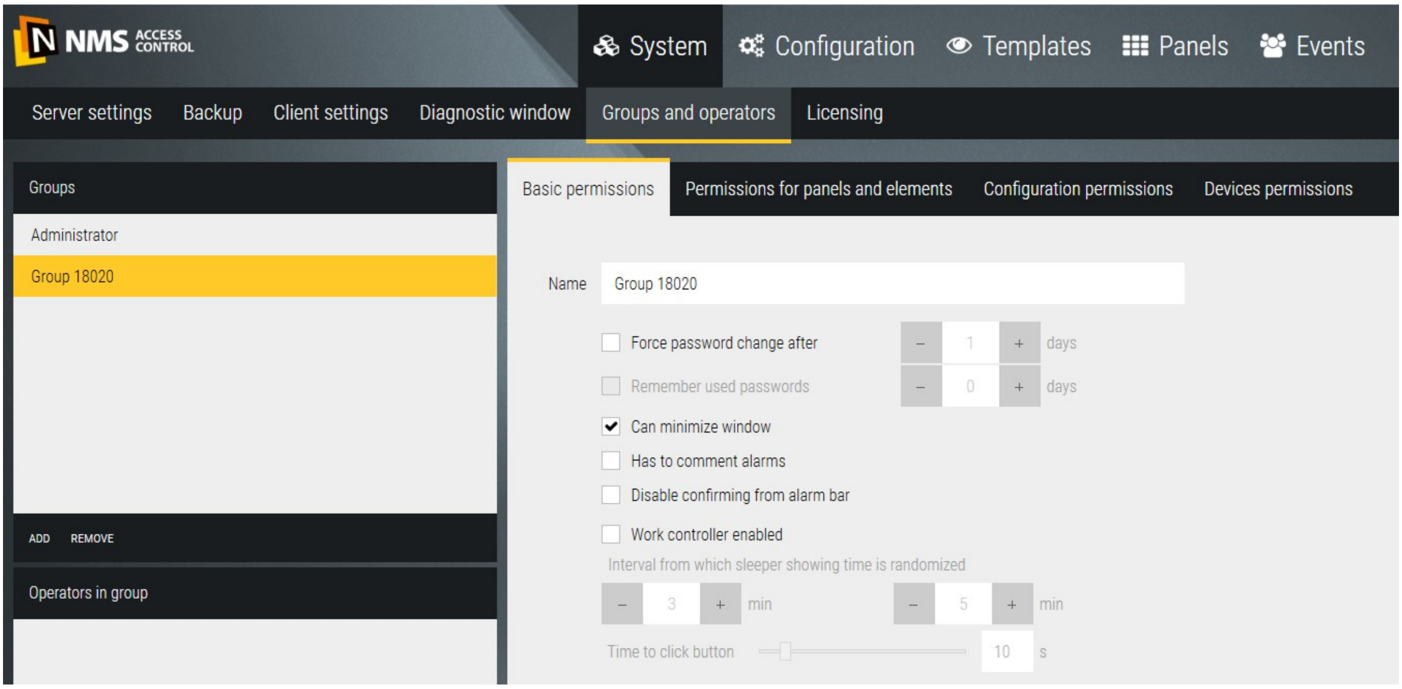
☐ Work controller enabled

Interval from which sleeper showing time is randomized – 1 + min – 1 + min

Time to click button 3 s

By default, one group of operators named *Administrator* with full program and system permissions is defined. By clicking on the *Add* button in the upper left window, we can add additional groups with restricted permissions. When you select a group in the top window, you can add operators. By default, a single *root* operator with full privileges is defined in *Administrator* group. The permissions are defined for the group (not for individual operators), for a new group of operators set in subsequent tabs.

Basic permissions



Groups: Administrator, Group 18020

Name: Group 18020

☐ Force password change after – 1 + days

☐ Remember used passwords – 0 + days

☑ Can minimize window

☐ Has to comment alarms

☐ Disable confirming from alarm bar

☐ Work controller enabled

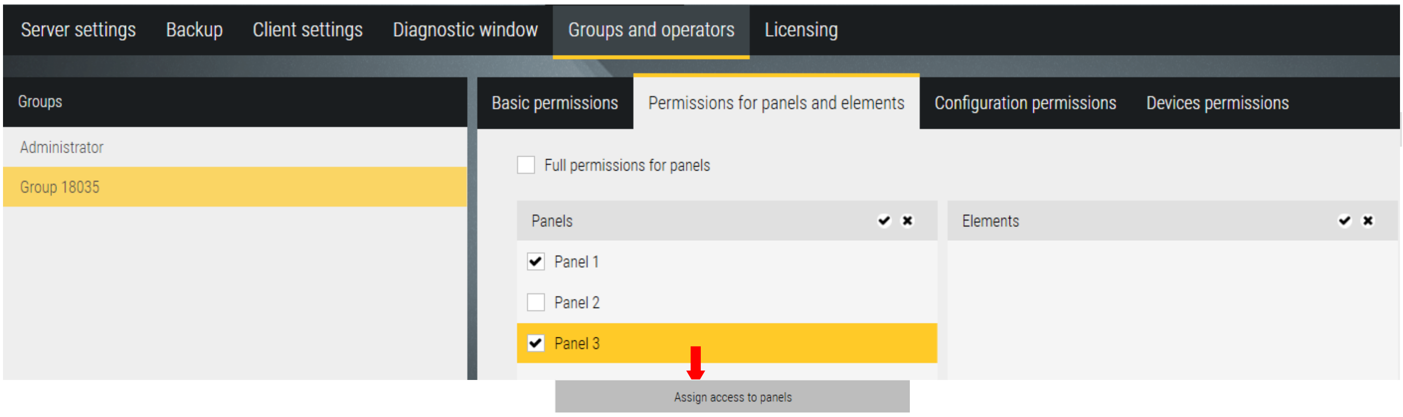
Interval from which sleeper showing time is randomized – 3 + min – 5 + min

Time to click button 10 s

The *Basic permissions* tab contains a number of checkboxes that you must select to assign the selected options.

The *__Work controller__* function controls the security personnel of the facility monitoring the system at the operator stations at random intervals. When active it requires confirmation in the displayed window and it is logged.

Permissions for panels and elements

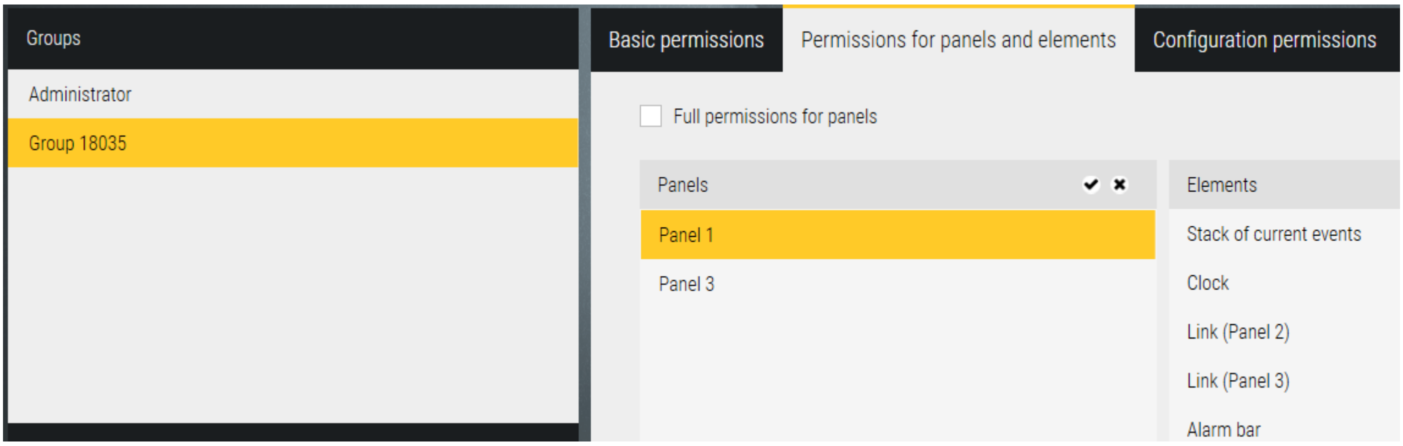


□ Full permissions for panels

☑ Panel 1
□ Panel 2
☑ Panel 3

Clicking on the button at the bottom of the window in the first column displays a list of available panels - select those which operators in this group have access to and *OK*.

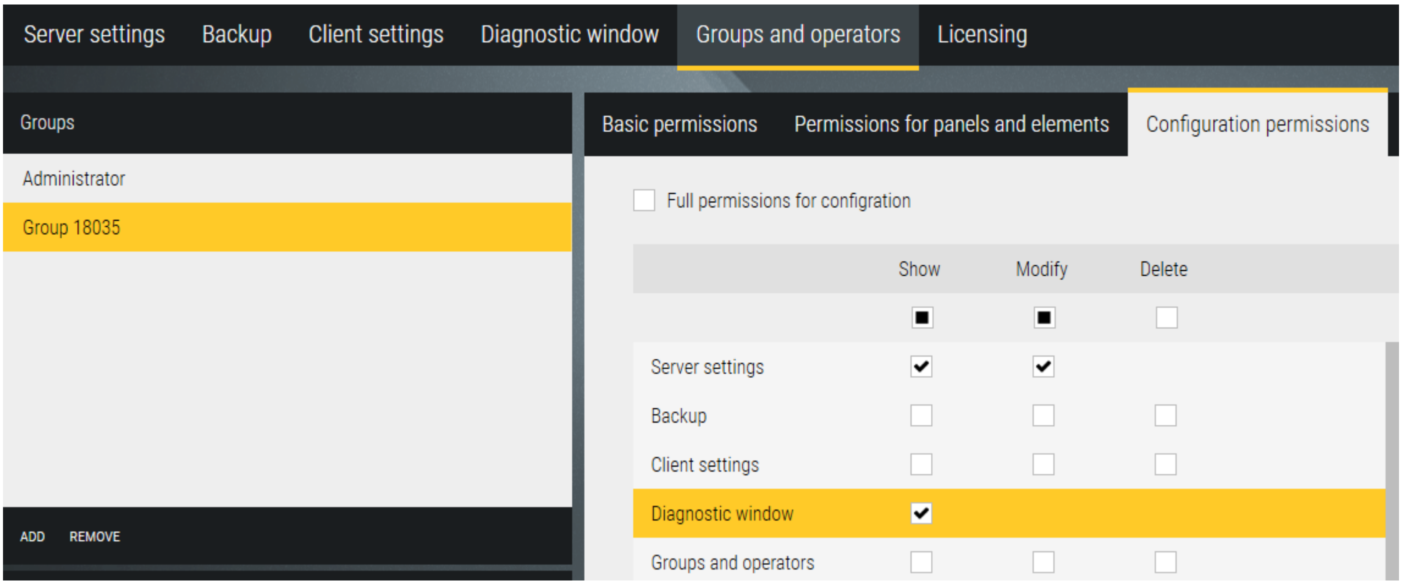
The second column (*elements)* displays a list of embedded items in the panel. When you select item in this list in the third column (*status*), you can choose to hide this item in the panel.



□ Full permissions for panels

Panels	Elements
Panel 1	Stack of current events
Panel 3	Clock
	Link (Panel 2)
	Link (Panel 3)
	Alarm bar

Configuration permissions

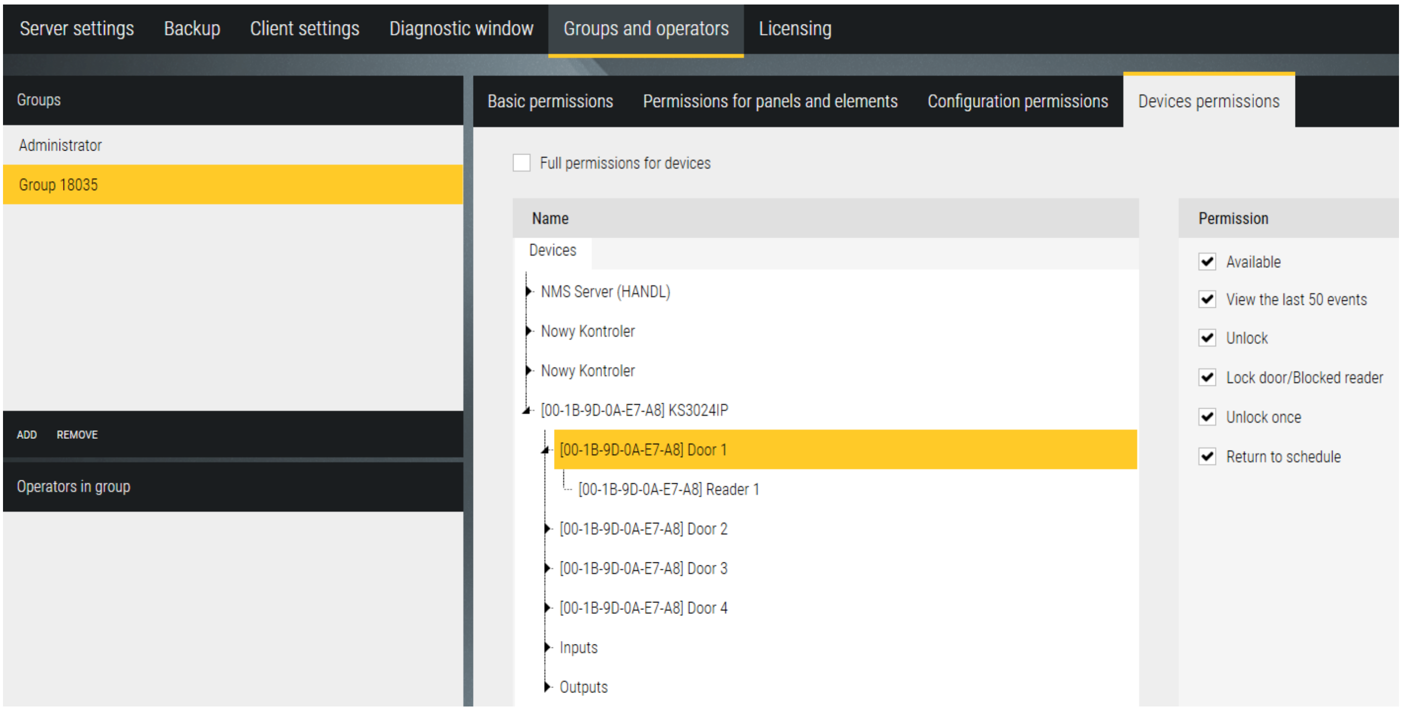


□ Full permissions for configration

	Show	Modify	Delete
	■	■	□
Server settings	☑	☑	
Backup	□	□	□
Client settings	□	□	□
Diagnostic window	☑		
Groups and operators	□	□	□

In this tab you need to set which items from the program menu will be accessed by operators in this group. The Administrator has full access in terms of read, modify, and delete. For the *Security* group, only the selected menu items with the *Read* attribute are usually chosen.

Device permissions



Administrator

Group 18035

□ Full permissions for devices

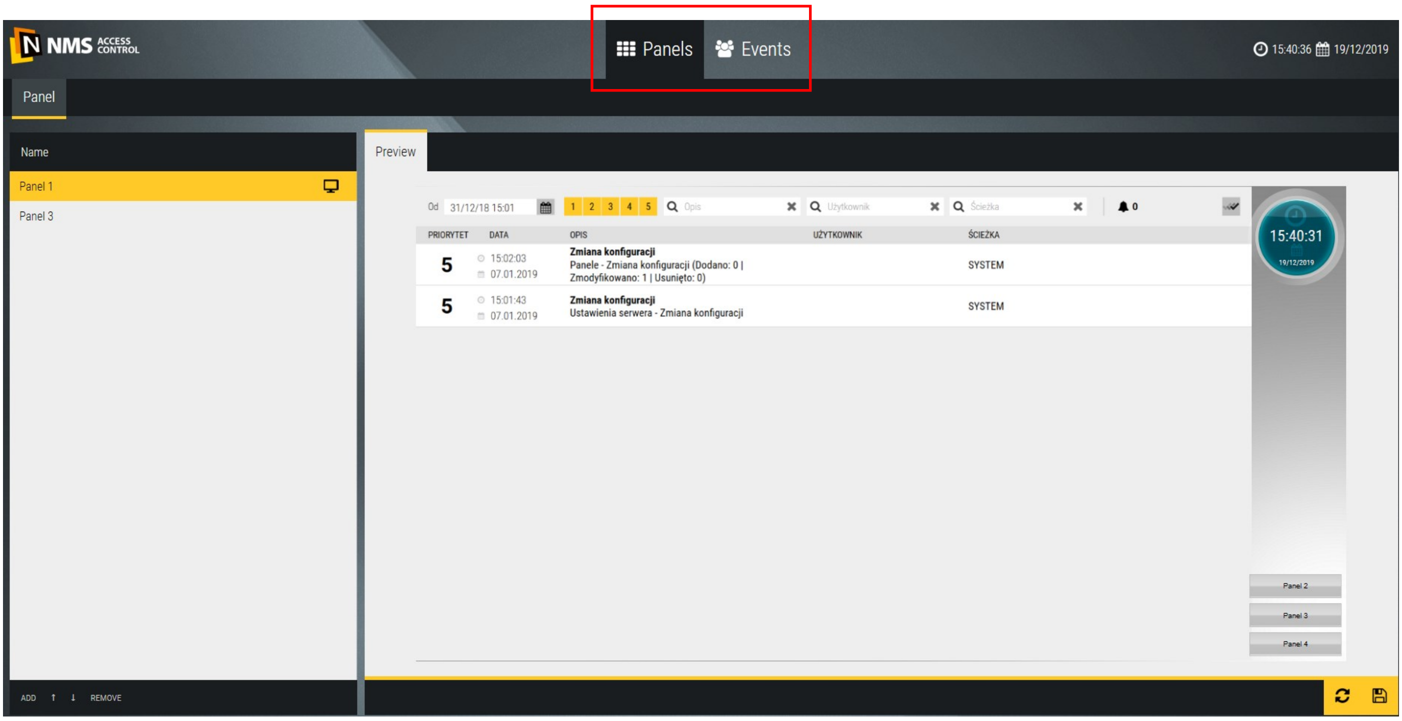
Name
Devices
NMS Server (HANDL)
Nowy Kontroler
Nowy Kontroler
[00-1B-9D-0A-E7-A8] KS3024IP
[00-1B-9D-0A-E7-A8] Door 1
[00-1B-9D-0A-E7-A8] Reader 1
[00-1B-9D-0A-E7-A8] Door 2
[00-1B-9D-0A-E7-A8] Door 3
[00-1B-9D-0A-E7-A8] Door 4
Inputs
Outputs

Permission

- ☑ Available
- ☑ View the last 50 events
- ☑ Unlock
- ☑ Lock door/Blocked reader
- ☑ Unlock once
- ☑ Return to schedule

In this tab you need to set which system devices will be accessed by operators in this group in terms of performing specific operations on them. The Administrator has full access to all operations. For the *Security* group, only the selected items related to basic operations, e.g. *Unlocking/Locking the door* are left.

Example of program window view after operator from *Security* group with limited privileges login.



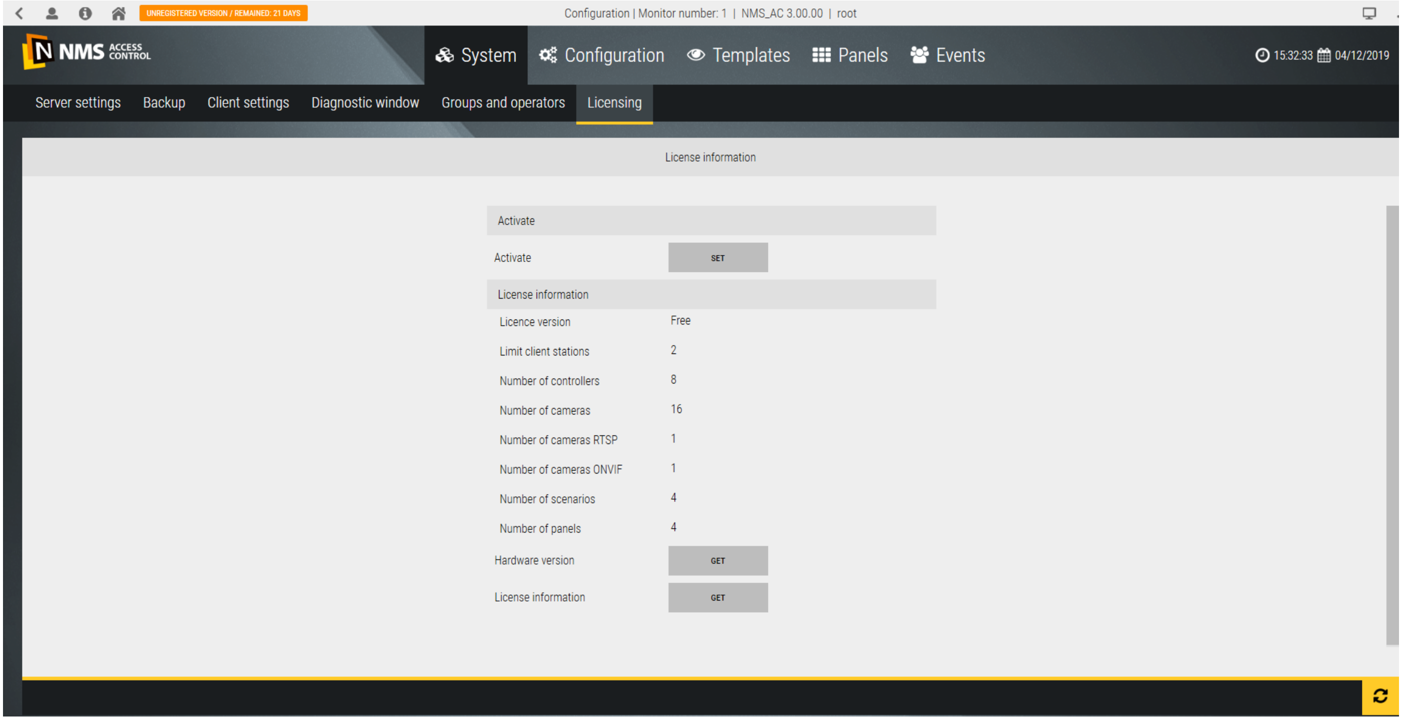
Panel 1

Panel 3

Od 31/12/18 15:01 | 1 2 3 4 5 | Opis | Użytkownik | Ścieżka | 0

PRIORYTET	DATA	OPIS	UŻYTKOWNIK	ŚCIEŻKA
5	15:02:03 07.01.2019	**Zmiana konfiguracji** Panele - Zmiana konfiguracji (Dodano: 0 | Zmodyfikowano: 1 | Usunięto: 0)		SYSTEM
5	15:01:43 07.01.2019	**Zmiana konfiguracji** Ustawienia serwera - Zmiana konfiguracji		SYSTEM

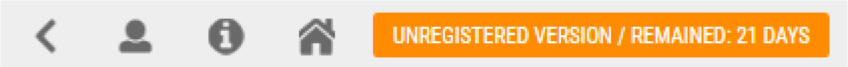
8.3 Licensing



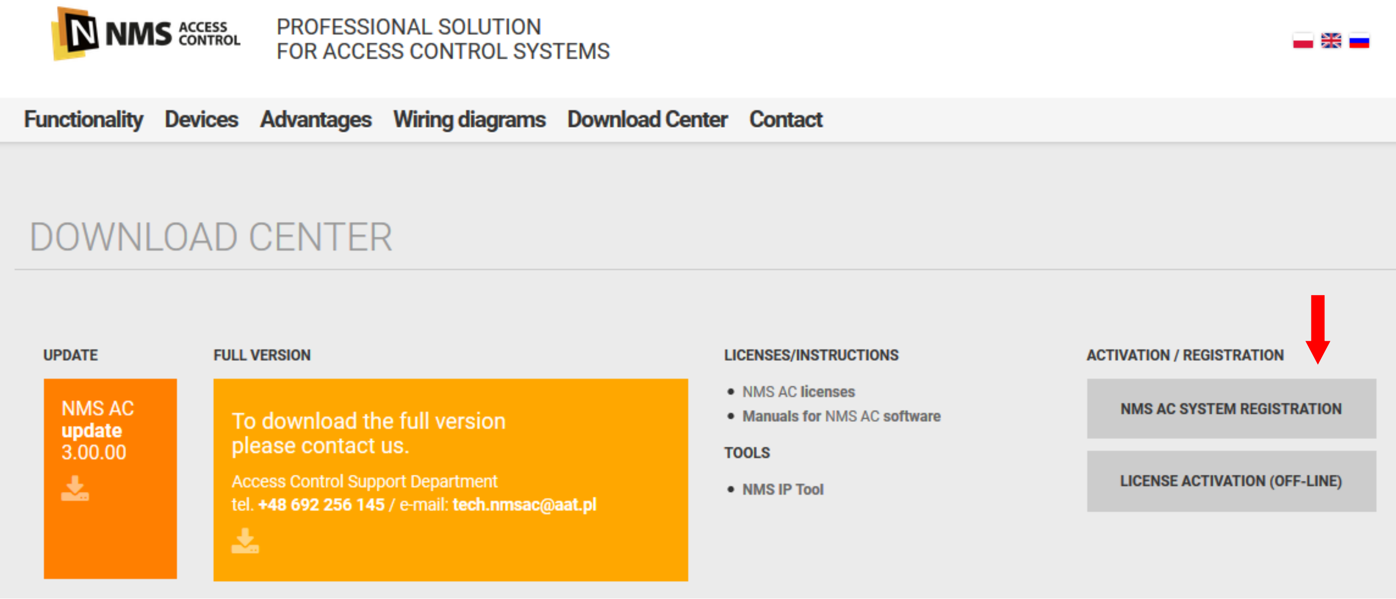
License information	
Licence version	Free
Limit client stations	2
Number of controllers	8
Number of cameras	16
Number of cameras RTSP	1
Number of cameras ONVIF	1
Number of scenarios	4
Number of panels	4
Hardware version	GET
License information	GET

In this tab you can register a free license and activate new licenses to expand the capacity and functionality of the system. By default, the values for the free license are displayed. Purchased new licenses can be added online when the computer running NMS ACCESS CONTROL is connected to the Internet or off-line when there is no such connection. Licenses are based on strings and do not require hardware keys.

The NMS ACCESS CONTROL software installed works in a limited time period up to 30 days from the date of installation. This indicates the message displayed in the orange box in the upper left corner of the screen.



It is fully functional, but to work after 30 days it should be registered at this time on the site: www.nmsac.aat.pl in the *Download center/NMS AC System Registration.*

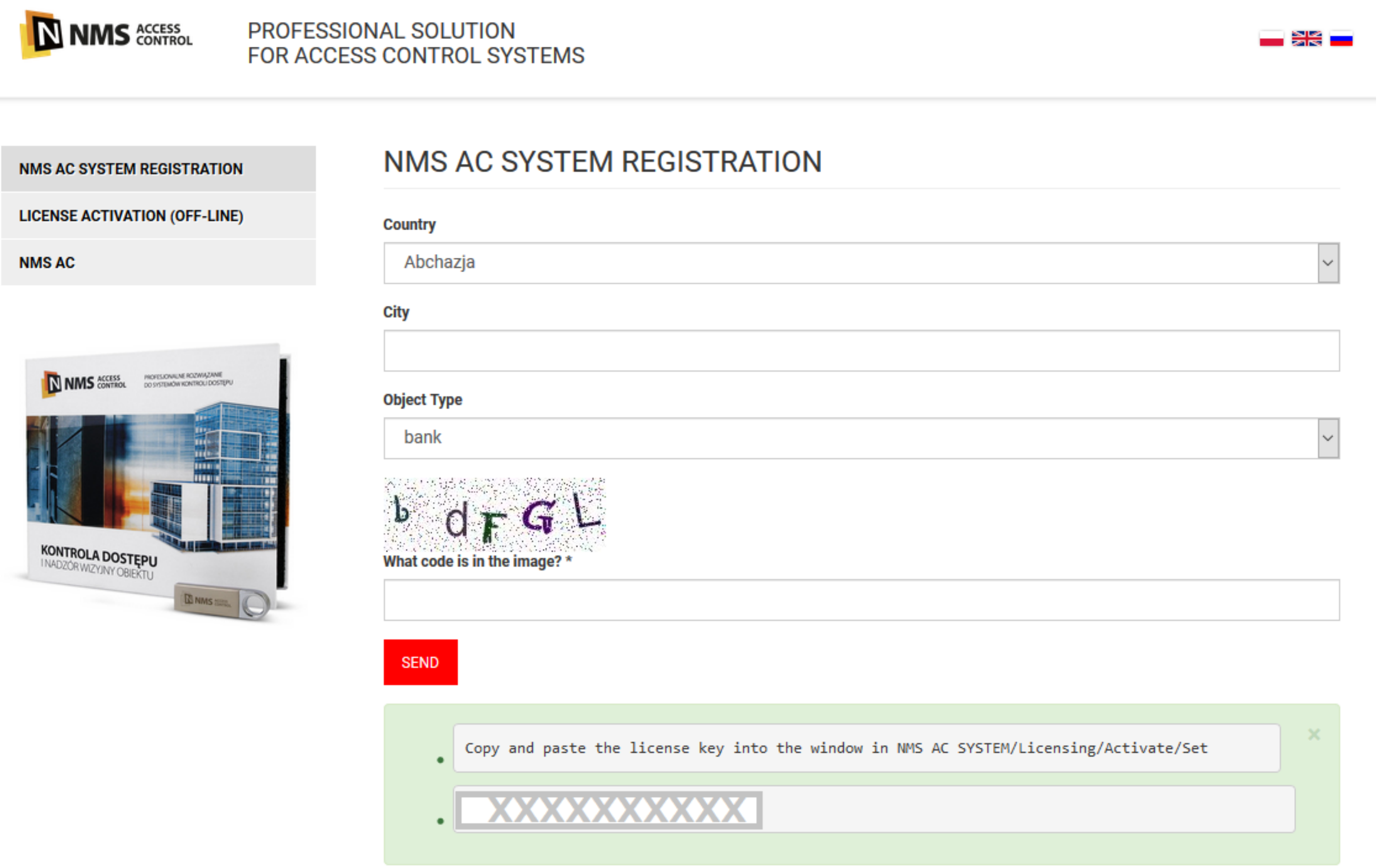


To download the full version please contact us.

Access Control Support Department
tel. +48 692 256 145 / e-mail: tech.nmsac@aat.pl

System registration in ON-LINE mode (NMS AC server is connected to the Internet)

Clicking on the REGISTER button will display a window as below:



NMS AC SYSTEM REGISTRATION

Country: Abchazja

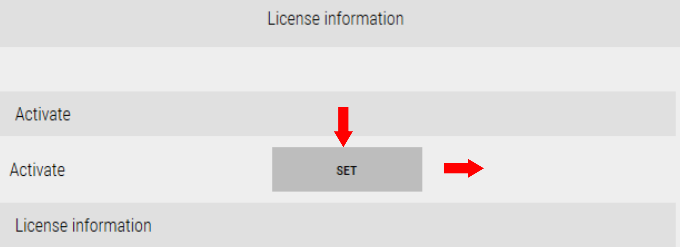
City:

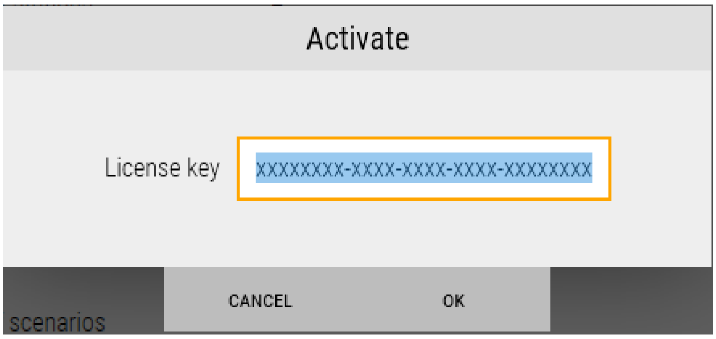
Object Type: bank

What code is in the image? *

- Copy and paste the license key into the window in NMS AC SYSTEM/Licensing/Activate/Set
- XXXXXXXXXXX

Fill in the fields for the installation location of the system: country (from drop down list), city and object type.
After entering the code from the image and clicking *OK* at the bottom the system registration code will be displayed, which should be copied and pasted into the box *SET* according to the info above: SYSTEM tab/Licensing/Activate/Set.



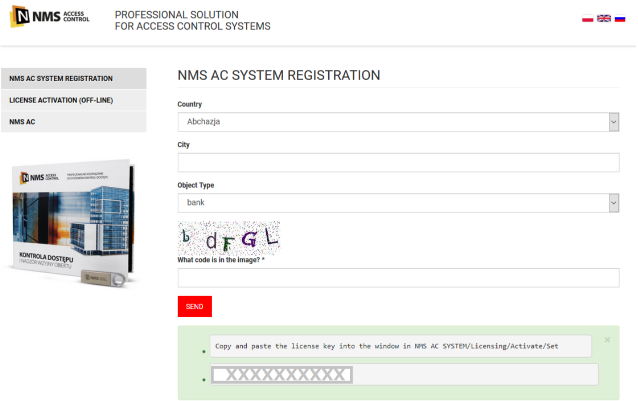


License key: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX

The program will reboot and after logging orange bar at the top of the window disappears. From that point on, the system will run indefinitely.

System registration in OFF-LINE mode (NMS AC server is not connected to the Internet)

In this case, the system registration process must be performed on a separate computer with Internet access.
Open the page www.nmsac.aat.pl in the *Download Center/Registration.*
Clicking on the REGISTER button will display a window as below:


PROFESSIONAL SOLUTION
FOR ACCESS CONTROL SYSTEMS
NMS AC SYSTEM REGISTRATION
LICENSE ACTIVATION (OFF-LINE)
NMS AC
KONTROLA DOSTĘPU
I NADZÓR WIZYJNY OBIEKTU
SEND

NMS AC SYSTEM REGISTRATION

Country: Abchazja

City:

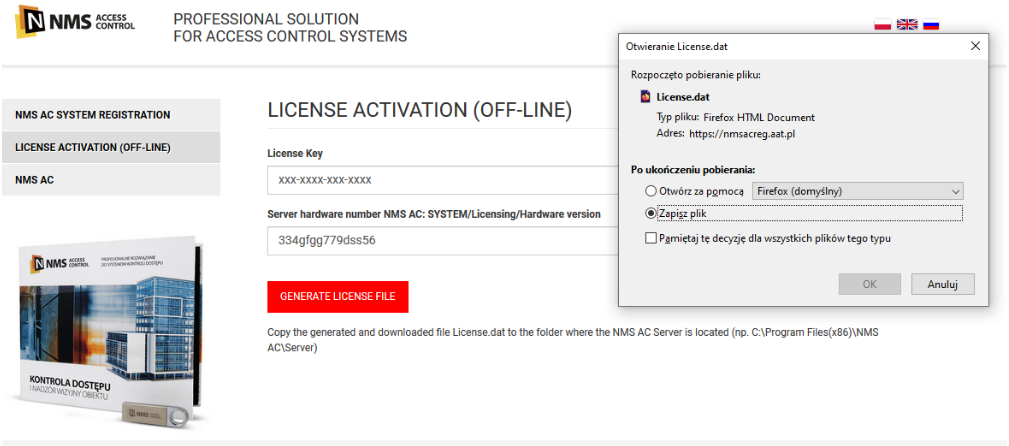
Object Type: bank

What code is in the image? *

Copy and paste the license key into the window in NMS AC SYSTEM/Licensing/Activate/Set

XXXXXXXXXX

Fill in the fields for the installation location of the system: country (from drop down list), city and object type. After entering the code from the image and clicking OK at the bottom will display the system registration code, which should be copied and go to the window www.nmsac.aat.pl/*Download Center/ACTIVATION OFF-LINE.*



LICENSE ACTIVATION (OFF-LINE)

License Key: XXX-XXXX-XXX-XXXX

Server hardware number NMS AC: SYSTEM/Licensing/Hardware version: 334gfgg779dss56

Copy the generated and downloaded file License.dat to the folder where the NMS AC Server is located (np. C:\Program Files(x86)\NMS AC\Server)

Otwieranie License.dat

Rozpoczęto pobieranie pliku:

License.dat

Typ pliku: Firefox HTML Document

Adres: https://nmsacreg.aat.pl

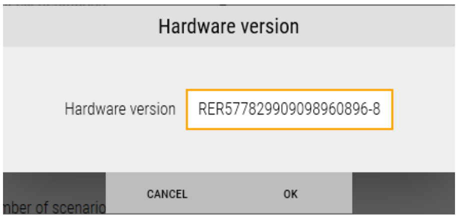
Po ukończeniu pobierania:

○ Otwórz za pomocą Firefox (domyślny)

● Zapisz plik

□ Pamiętaj tę decyzję dla wszystkich plików tego typu

Paste the key copied from *REGISTRATION* window into first field and *Hardware version* from SYSTEM/ Licensing/Hardware version **on NMS AC server.**

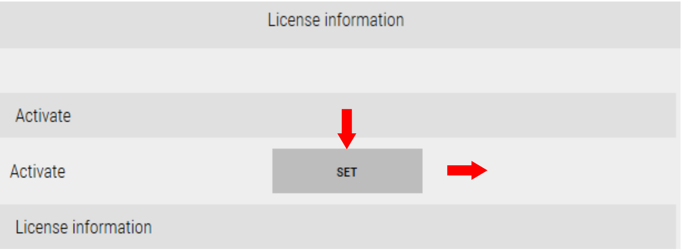


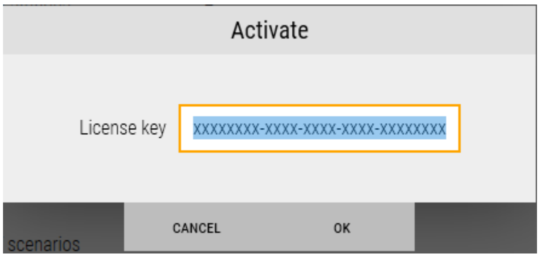
Hardware version: RER5778299090989608968

After clicking *Generate license file* button a License.dat file will be downloaded to the disk.

You must copy License.dat file to *C:\Program Files (x86)\NMS AC\Server* directory **on NMS AC serwer**.

Paste license key copied from REGISTRATION window to *Activate* window on **NMS AC Server**.



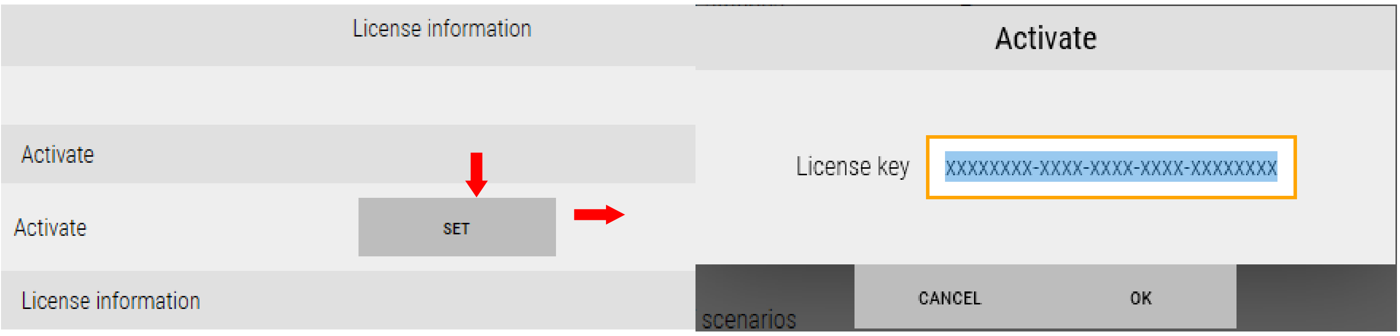


License key: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX

The program will reboot and after logging orange bar at the top of the window disappears. From that point on, the system will run indefinitely.

Paid licenses activation in ON-LINE mode (NMS AC server connected to the Internet)

After obtaining paid license key you need to copy it and paste i *Set* field: SYSTEM tab/Licensing/Activate/Set on NMS AC Server.


License information

Activate

Activate SET

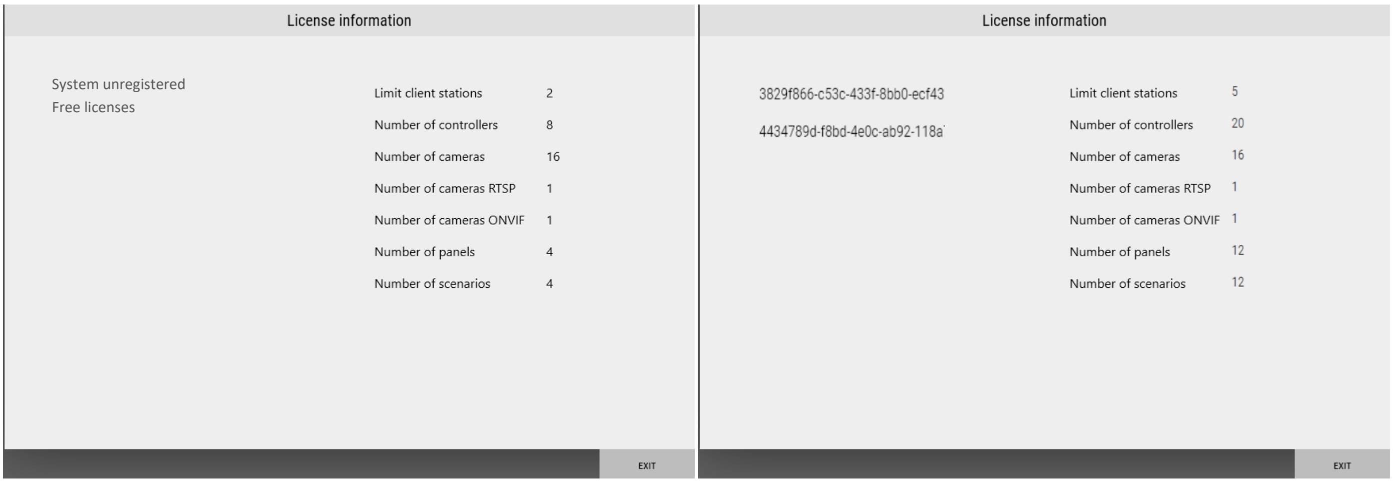
License information

Activate

License key XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX

scenarios CANCEL OK

Software will restart. In *Licenses* tab summary components quantity will be displayed which you can add to the system. After clicking on License GUID information - Get button you can verify owned licenses (after clicking on the key).


License information

System unregistered
Free licenses

Limit client stations	2
Number of controllers	8
Number of cameras	16
Number of cameras RTSP	1
Number of cameras ONVIF	1
Number of panels	4
Number of scenarios	4

EXIT

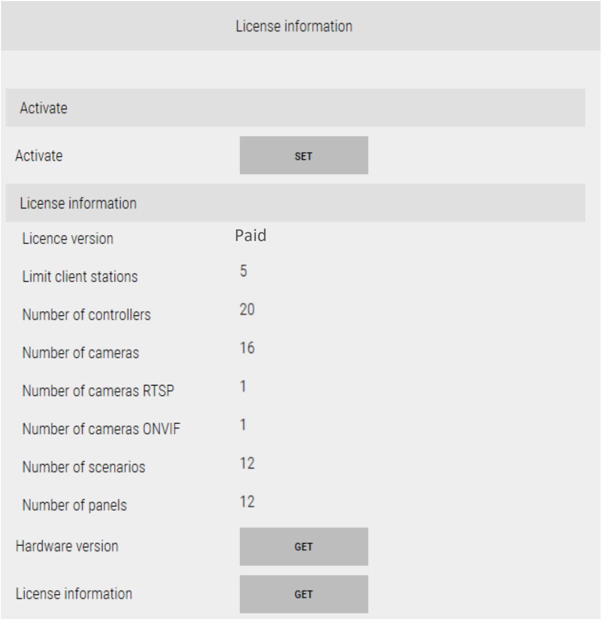
License information

3829f866-c53c-433f-8bb0-ecf43
4434789d-f8bd-4e0c-ab92-118a'

Limit client stations	5
Number of controllers	20
Number of cameras	16
Number of cameras RTSP	1
Number of cameras ONVIF	1
Number of panels	12
Number of scenarios	12

EXIT

In main window of Licensing tab summary quantities are displayed.


License information

Activate

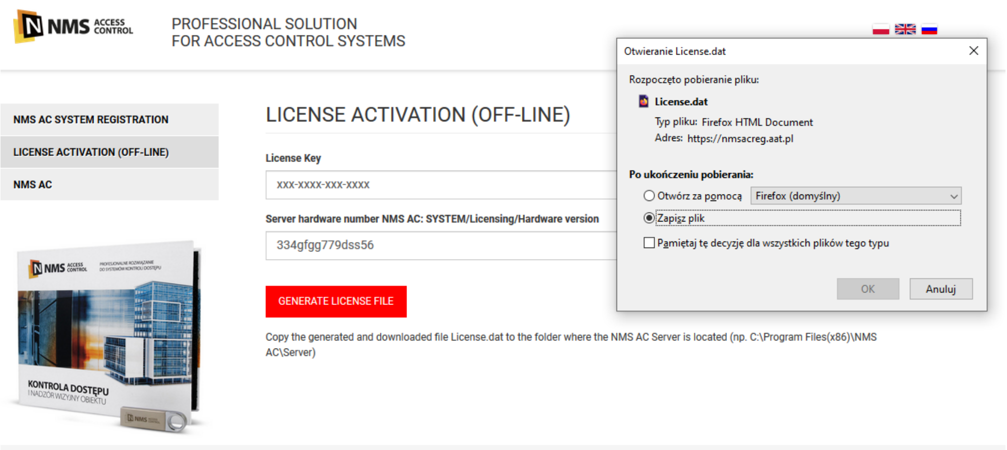
Activate SET

License information

Licence version	Paid
Limit client stations	5
Number of controllers	20
Number of cameras	16
Number of cameras RTSP	1
Number of cameras ONVIF	1
Number of scenarios	12
Number of panels	12
Hardware version	GET
License information	GET

Paid licenses activation in OFF-LINE mode (NMS AC server has no connection to the Internet)

In this case, the system registration process must be performed on a separate computer with Internet access.
Open the page www.nmsac.aat.pl in the *Download Center/OFF-LINE ACTIVATION.*
Clicking on the *OFF-LINE ACTIVATION* button will display a window as below:


NMS ACCESS CONTROL
PROFESSIONAL SOLUTION
FOR ACCESS CONTROL SYSTEMS
NMS AC SYSTEM REGISTRATION
LICENSE ACTIVATION (OFF-LINE)
NMS AC
GENERATE LICENSE FILE
OK
Anuluj

LICENSE ACTIVATION (OFF-LINE)

License Key: XXX-XXXX-XXX-XXXX

Server hardware number NMS AC: SYSTEM/Licensing/Hardware version: 334gfgg779dss56

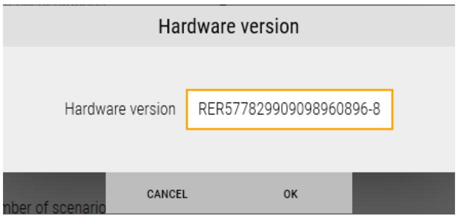
Copy the generated and downloaded file License.dat to the folder where the NMS AC Server is located (np. C:\Program Files(x86)\NMS AC\Server)

Otwieranie License.dat

Rozpoczęto pobieranie pliku:
License.dat
Typ pliku: Firefox HTML Document
Adres: https://nmsacreg.aat.pl

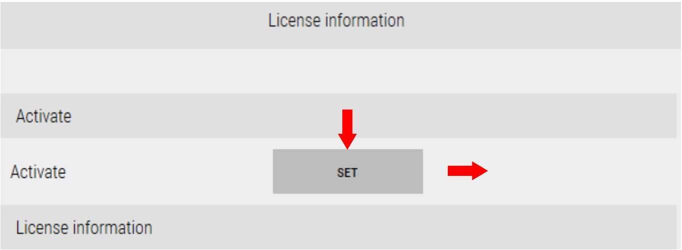
Po ukończeniu pobierania:
○ Otwórz za pomocą Firefox (domyślny)
● Zapisz plik
□ Pamiętaj tę decyzję dla wszystkich plików tego typu

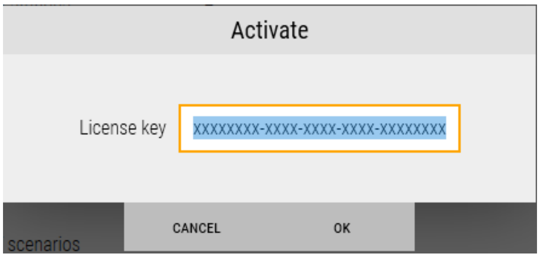
Paste or type purchased license into *License key* field, and *Hardware version* from SYSTEM/Licensing/ Hardware version **on NMS AC server** below.



Hardware version: RER577829909098960896-8

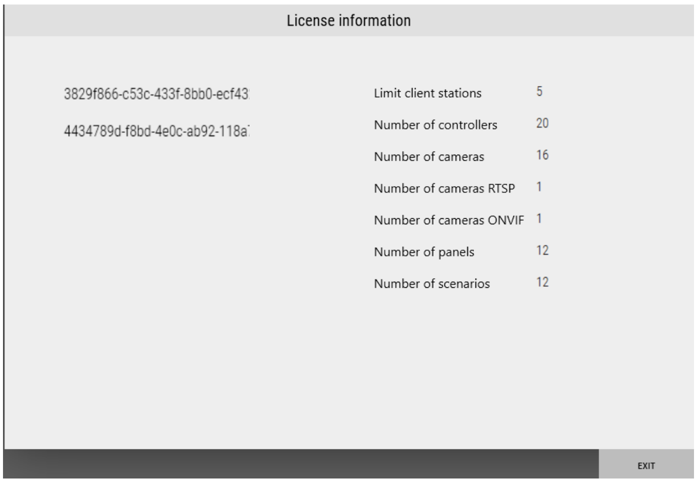
After clicking *Generate license file* button a License.dat file will be downloaded to the disk.
You must copy License.dat file to *C:\Program Files (x86)\NMS AC\Server* directory **on NMS AC serwer**.
Paste or type purchased license key to *Activate* window on **NMS AC Server**.



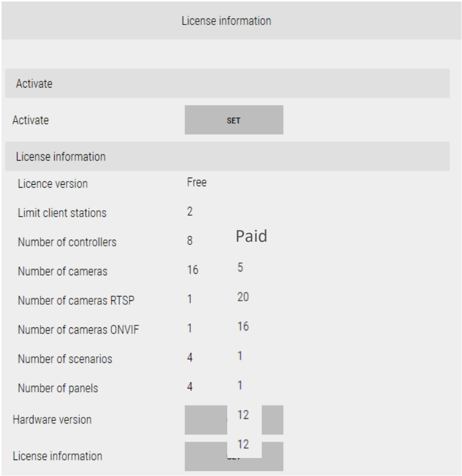


License key: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX

Software will restart. In Licenses tab summary components quantity will be displayed which you can add to the system. After clicking on License GUID information - Get button you can verify owned licenses (after clicking on the key). In main window of Licensing tab summary quantities are displayed.



3829f866-c53c-433f-8bb0-ecf43	Limit client stations	5
4434789d-f8bd-4e0c-ab92-118a	Number of controllers	20
	Number of cameras	16
	Number of cameras RTSP	1
	Number of cameras ONVIF	1
	Number of panels	12
	Number of scenarios	12



Licence version	Free	
Limit client stations	2	
Number of controllers	8	Paid
Number of cameras	16	5
Number of cameras RTSP	1	20
Number of cameras ONVIF	1	16
Number of scenarios	4	1
Number of panels	4	1
Hardware version		12
License information		12

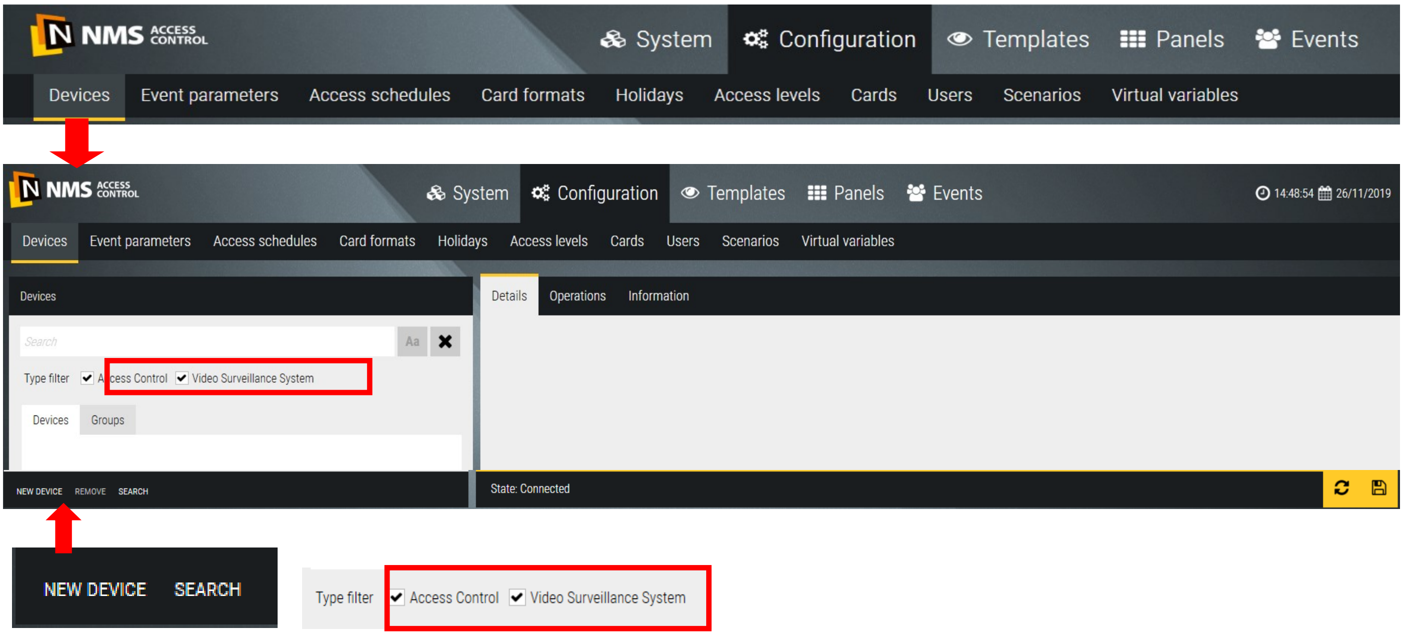
Section 3 System configuration

This chapter will discuss the subject of NMS ACCESS CONTROL system configuration . These are the actions performed by the system installer. *Configuration* tab is used to do this. It includes a number of windows to add devices to your system, schedules, access levels, cards and users. You can also use this tab to define scenarios and virtual variables.

3.1 Devices - Access Control - Controllers

The configuration process begins with the *Device* tab.

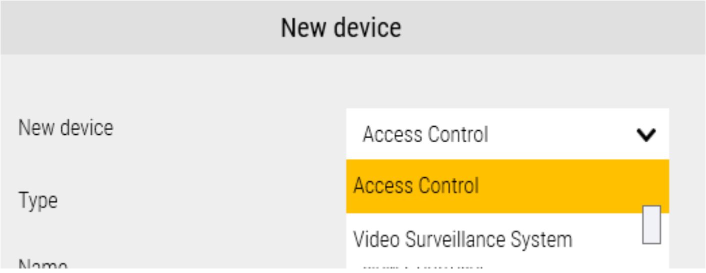
Type filter allows displaying devices list containing one or both device type - AC and VSS.



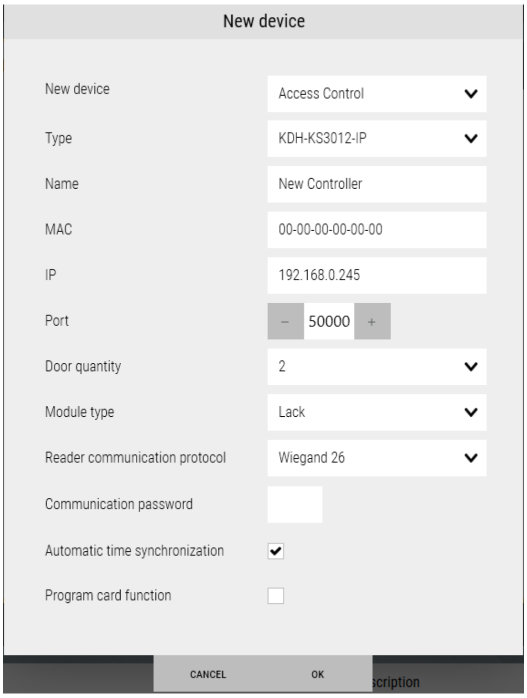
The system can be set up in off-line mode before connecting to the system on the facility, but much faster the configuration process goes in on-line mode when the devices are already installed, connected to power and Ethernet network. We can then use the search engine, which will display a list of available devices and address parameters after searching the network. This procedure will be described in the next step.

New device

This option allows you to add a new device in off-line mode, when you can not use the search engine. When you click on this button you will see a window like one below where you can select the type of device you want to add:



After selecting access control system device, a window will be displayed as below:



New device

New device	Access Control
Type	KDH-KS3012-IP
Name	New Controller
MAC	00-00-00-00-00-00
IP	192.168.0.245
Port	50000
Door quantity	2
Module type	Lack
Reader communication protocol	Wiegand 26
Communication password	
Automatic time synchronization	☑
Program card function	□

Type - the controller model can be selected from the drop-down list:

- KDH-KS3012-IP
- KDH-KS3024-IP
- KDH-KS2000-IP-ELV (in the next version will be replaced by KDH-KS3000-IP-ELV with new f/w)

Name - editable field to type the name of the controller

MAC - editable field to enter the MAC address of the controller (it is on the sticker on the device).

If you do not know this address at this stage, please leave the default.

After communicating with the device with the IP address as below, this field will be updated.

IP - editable field to type the static IP address of the controller

(Default 192.168.0.245 - should be changed to target)

Port - editable field to enter port number (it is recommended to leave the default value)

Number of doors - from the drop down list you can select 1, 2 or 4 doors depending on the controller model

Module type - from the drop-down list type can be selected depending on the controller model:

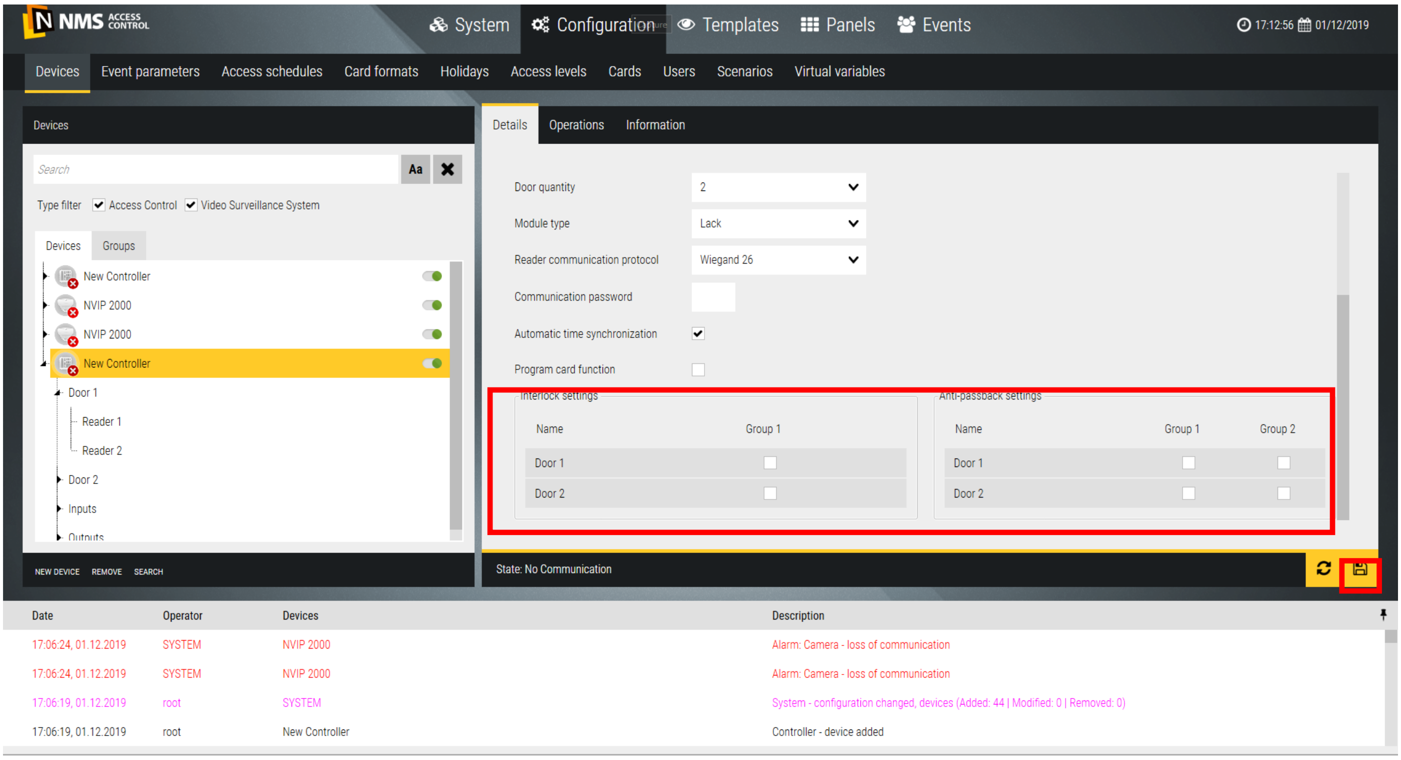
- KDH-MOD2000INOUT (for KDH-KS30XX-IP controllers)
- KDH-MOD2000-ELV (for KDH-KS2000-IP-ELV controller)
- KDH-MOD2016-ELV (for KDH-KS2000-ELV controller) - 1 to 4 modules

Wiegand format - from the drop-down list format can be selected depending on the reader and card model: 26, 32, 34, 37, 39 or custom

Communication Password - editable field for typing 4-digit communication password (0000-9999)

Program card function - option to select, allows to enable adding cards to the controller without communicating with the program (the description is in the instructions to the controller)

After you have made the settings, click ***OK***. The program will return to the main configuration window and the added device appears in the list in the left window.



Door quantity: 2

Module type: Lack

Reader communication protocol: Wiegand 26

Communication password:

Automatic time synchronization: ☑

Program card function: □

Interlock settings

Name	Group 1
Door 1	□
Door 2	□

Anti-passback settings

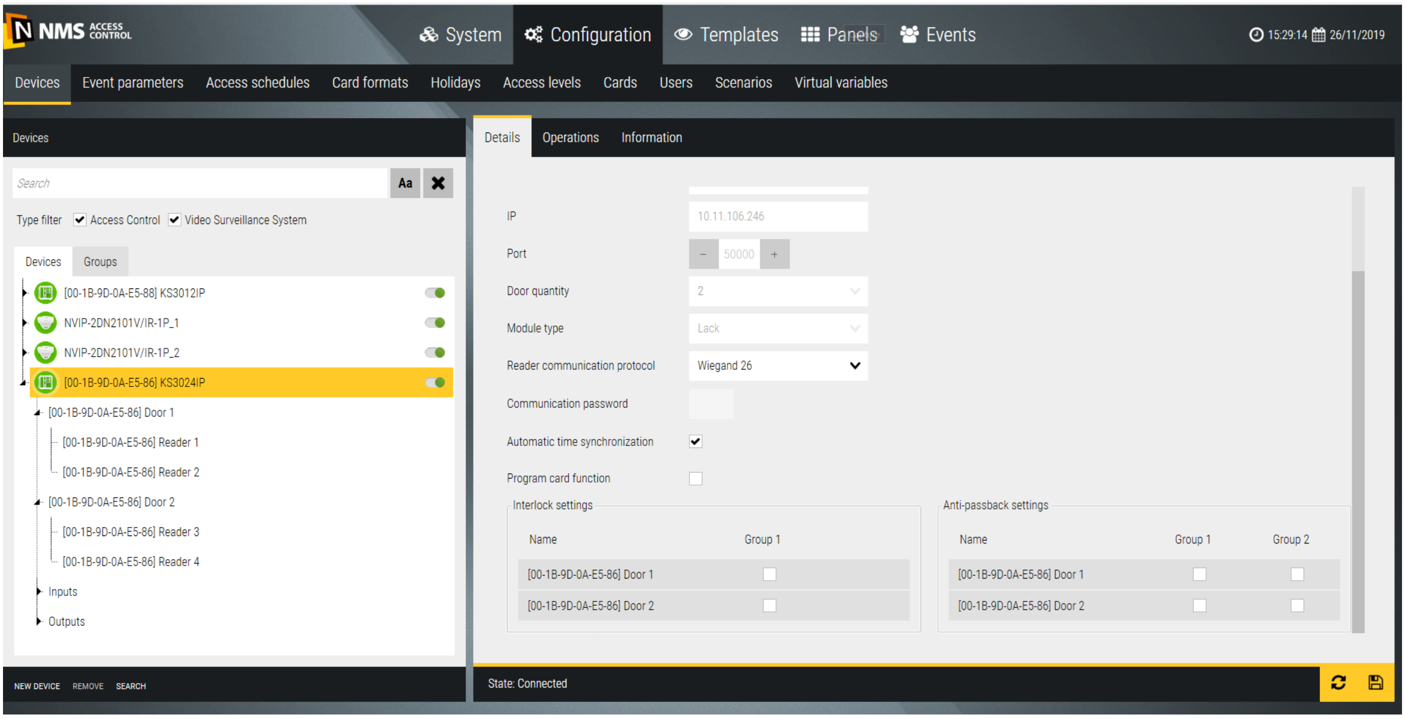
Name	Group 1	Group 2
Door 1	□	□
Door 2	□	□

State: No Communication

Date	Operator	Devices	Description
17:06:24, 01.12.2019	SYSTEM	NVIP 2000	Alarm: Camera - loss of communication
17:06:24, 01.12.2019	SYSTEM	NVIP 2000	Alarm: Camera - loss of communication
17:06:19, 01.12.2019	root	SYSTEM	System - configuration changed, devices (Added: 44 | Modified: 0 | Removed: 0)
17:06:19, 01.12.2019	root	New Controller	Controller - device added

For KDH-KS3012/24-IP controllers, additional fields appear in the lower right window to add controller doors and readers to one or two groups. This applies independently of the man-trap function (the reciprocal control of the state of the door leaf) and the anti-passback (control the order of reading the card on the entry and exit readers). These fields do not exist for the elevator controller.

Once all settings have been made, save them by clicking on the floppy disk icon in the bottom right corner. A series of messages about this operation appears in the System Log window, and the controller icons change to green. Save can be done once after adding more than one device.



IP: 10.11.106.246

Port: 50000

Door quantity: 2

Module type: Lack

Reader communication protocol: Wiegand 26

Communication password:

Automatic time synchronization: ☑

Program card function: □

Interlock settings

Name	Group 1
[00-1B-9D-0A-E5-86] Door 1	□
[00-1B-9D-0A-E5-86] Door 2	□

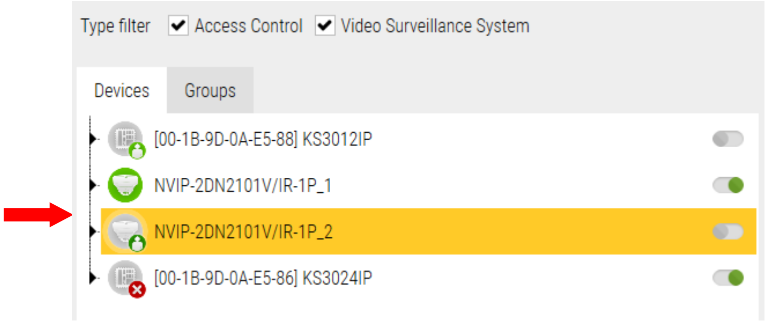
Anti-passback settings

Name	Group 1	Group 2
[00-1B-9D-0A-E5-86] Door 1	□	□
[00-1B-9D-0A-E5-86] Door 2	□	□

State: Connected

When you save the settings, the icon status can show one of three situations:

- No communication with the device - gray icon with red box (check address settings or network connection and power supply)
- Device disconnected by operator - grey icon with green box (disable monitoring by moving left slider to the right to edit settings or perform maintenance operations)
- Correct Communication - green icon

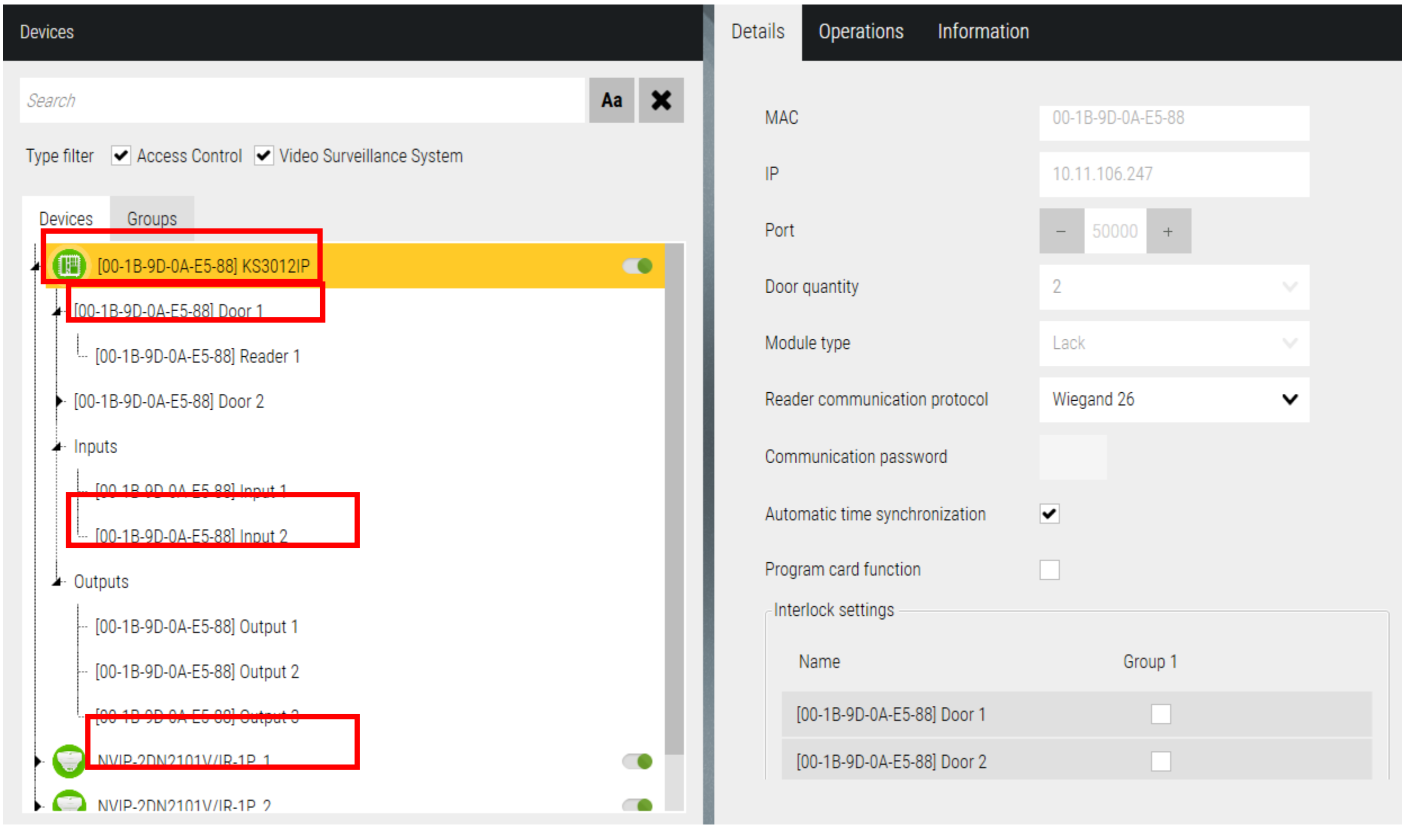


Type filter ☑ Access Control ☑ Video Surveillance System

Devices | Groups

- [00-1B-9D-0A-E5-88] KS3012IP
- NVIP-2DN2101V/IR-1P_1
- NVIP-2DN2101V/IR-1P_2
- [00-1B-9D-0A-E5-86] KS3024IP

You can expand controller icon by clicking the black triangle on the main tree line and display linked elements. You can edit element's settings by selecting it on the list.



Devices

Search | Aa | ✖

Type filter ☑ Access Control ☑ Video Surveillance System

Devices | Groups

- [00-1B-9D-0A-E5-88] KS3012IP
  - [00-1B-9D-0A-E5-88] Door 1
    - [00-1B-9D-0A-E5-88] Reader 1
  - [00-1B-9D-0A-E5-88] Door 2
  - Inputs
    - [00-1B-9D-0A-E5-88] Input 1
    - [00-1B-9D-0A-E5-88] Input 2
  - Outputs
    - [00-1B-9D-0A-E5-88] Output 1
    - [00-1B-9D-0A-E5-88] Output 2
    - [00-1B-9D-0A-E5-88] Output 3
- NVIP-2DN2101V/IR-1P_1
- NVIP-2DN2101V/IR-1P_2

Details | Operations | Information

MAC	00-1B-9D-0A-E5-88
IP	10.11.106.247
Port	− 50000 +
Door quantity	2
Module type	Lack
Reader communication protocol	Wiegand 26
Communication password	
Automatic time synchronization	☑
Program card function	□

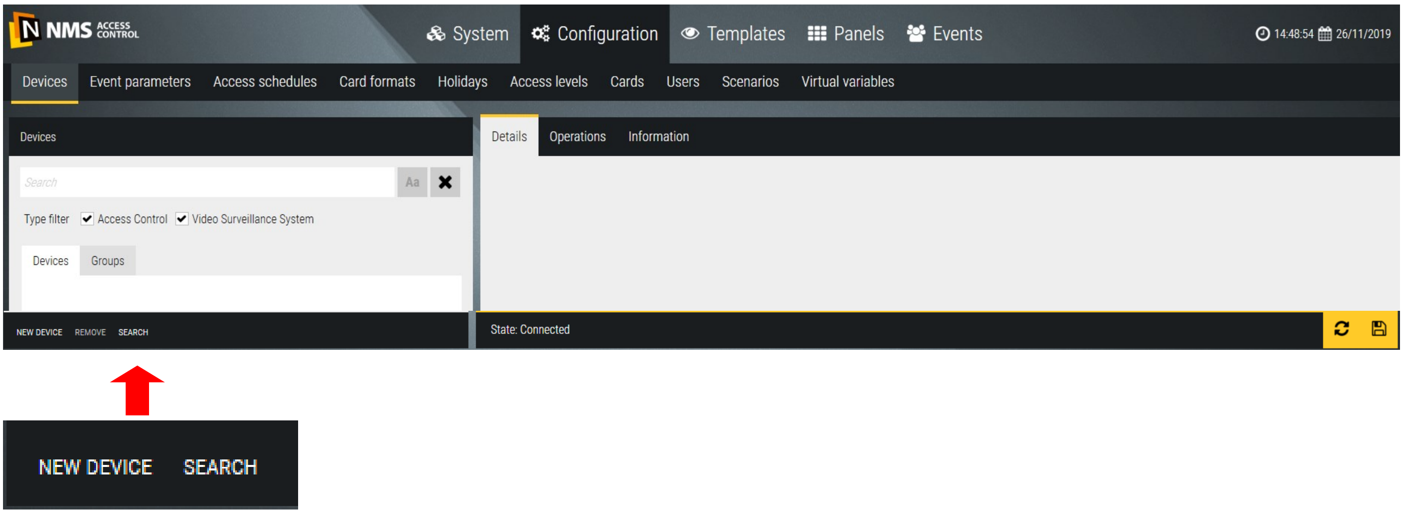
Interlock settings

Name	Group 1
[00-1B-9D-0A-E5-88] Door 1	□
[00-1B-9D-0A-E5-88] Door 2	□

This includes components such as doors, readers, inputs and control outputs. When you select an item, the right window displays its settings, which you can edit. The selected item is highlighted in yellow. After changing the settings, save them by clicking on the floppy disk in the lower right corner of the configuration window. To edit the controller settings, disconnect it by sliding the green slider to the left. When you are finished editing, move the slider to the right again and click on the ***Save*** icon.

The defined controller can be edited or deleted by selecting it on the list and clicking the ***Delete*** button in the lower left corner of the window. All system-wide components are deleted with the controller.

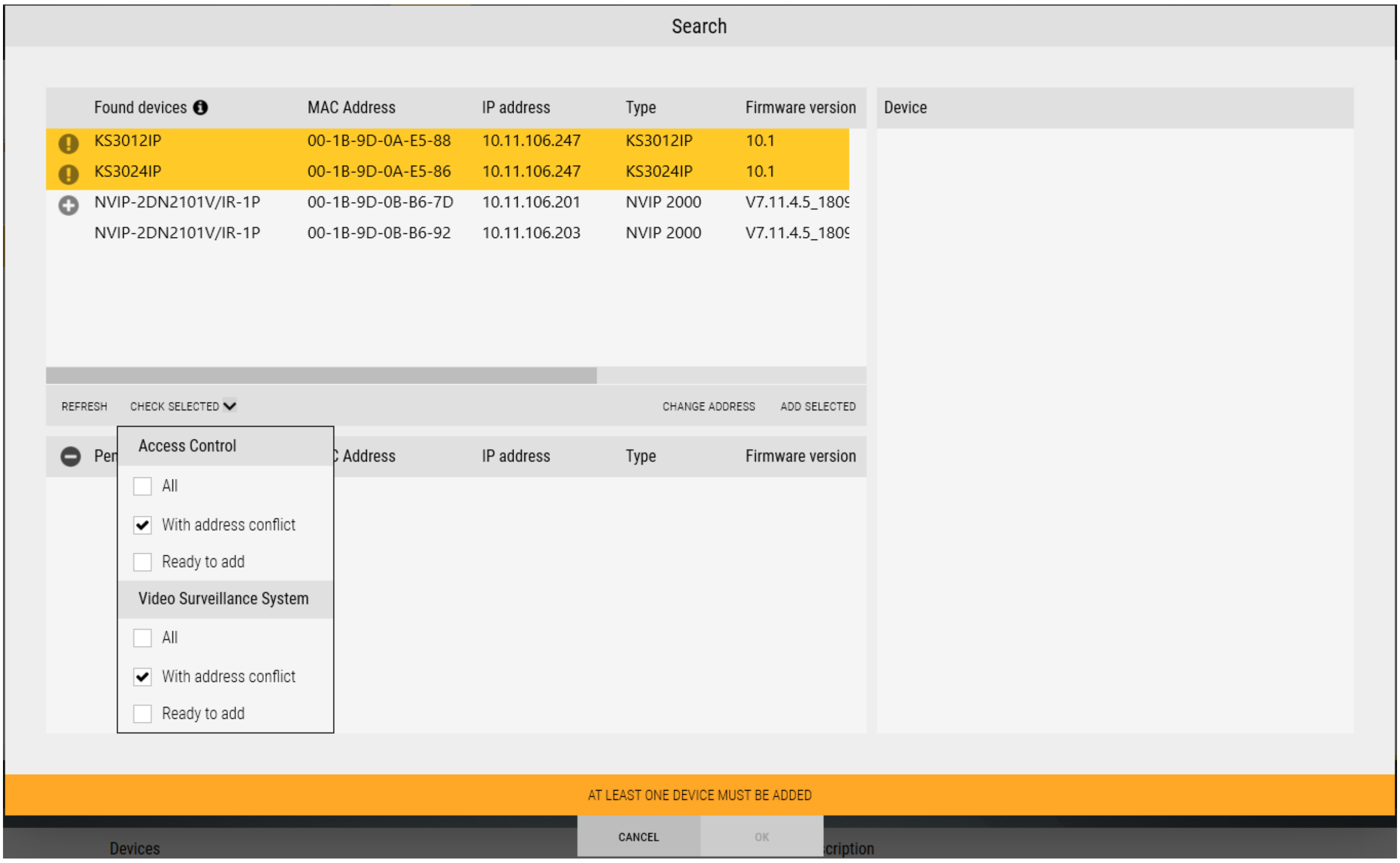
Search



Type filter ☑ Access Control ☑ Video Surveillance System

State: Connected

When controllers and VSS devices are installed in facility, connected to Ethernet and power, it is recommended to use the search engine to add them to your system base. This greatly accelerates this process. To run the search engine you need to click on the *Search* button at the bottom of the window as above. The program displays a window in which you will see a list of controllers vand VSS devices searched in the network.



	Found devices	MAC Address	IP address	Type	Firmware version
!	KS3012IP	00-1B-9D-0A-E5-88	10.11.106.247	KS3012IP	10.1
!	KS3024IP	00-1B-9D-0A-E5-86	10.11.106.247	KS3024IP	10.1
⊕	NVIP-2DN2101V/IR-1P	00-1B-9D-0B-B6-7D	10.11.106.201	NVIP 2000	V7.11.4.5_180ς
	NVIP-2DN2101V/IR-1P	00-1B-9D-0B-B6-92	10.11.106.203	NVIP 2000	V7.11.4.5_180ς

	Per	Address	IP address	Type	Firmware version

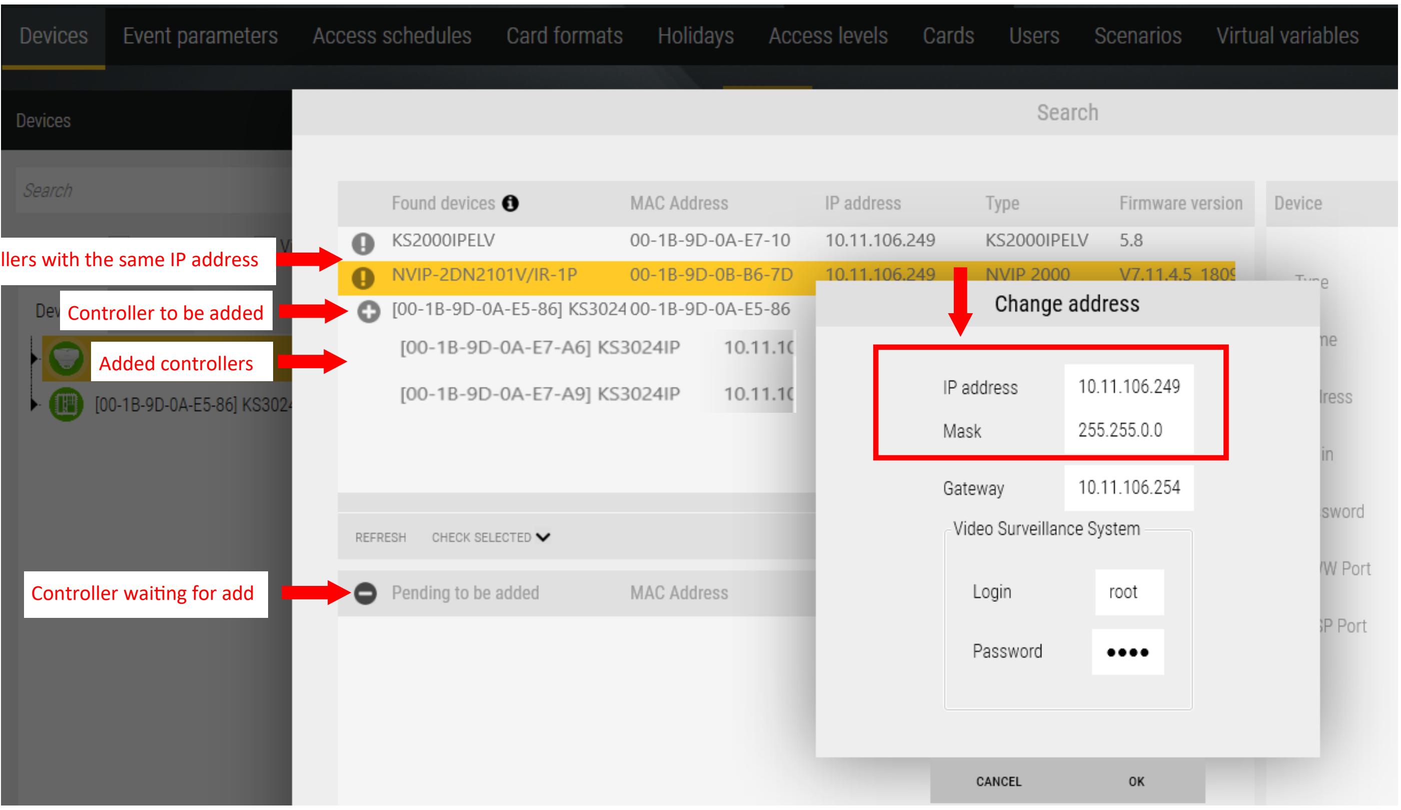
Access Control
- □ All
- ☑ With address conflict
- □ Ready to add

Video Surveillance System
- □ All
- ☑ With address conflict
- □ Ready to add

Controllers searched in the network are displayed in upper left side of the window with status icons:

- ! - controllers with the same IP address - displayed on the top of the list
- ⊕ - controllers possible to add to the system
- ⊖ - controllers transferred from upper window, waiting to add; you can transfer back to upper list
- - controllers searched, already added to the system - no status icon

Each new controller has the same default IP address - 192.168.0.245. This group of controllers is displayed at the beginning of the list with ❗ icon - you can select them all (using *Check selected* list) and group change their IP to addresses according to the target administrator assigned pool by clicking on the ***Change Address*** button. After entering the starting address, the end address of the scope will be generated automatically depending on the number of selected controllers with the same IP address. The icons will ⊕ change to and controllers can then be added to the bottom window by clicking on the icon.



Controllers with the same IP address

Controller to be added

Added controllers

Controller waiting for add

Found devices	MAC Address	IP address	Type	Firmware version
KS2000IPELV	00-1B-9D-0A-E7-10	10.11.106.249	KS2000IPELV	5.8
NVIP-2DN2101V/IR-1P	00-1B-9D-0B-B6-7D	10.11.106.249	NVIP 2000	V7.11.4.5_180
[00-1B-9D-0A-E5-86] KS3024	00-1B-9D-0A-E5-86			

[00-1B-9D-0A-E7-A6] KS3024IP 10.11.1

[00-1B-9D-0A-E7-A9] KS3024IP 10.11.1

[00-1B-9D-0A-E5-86] KS302

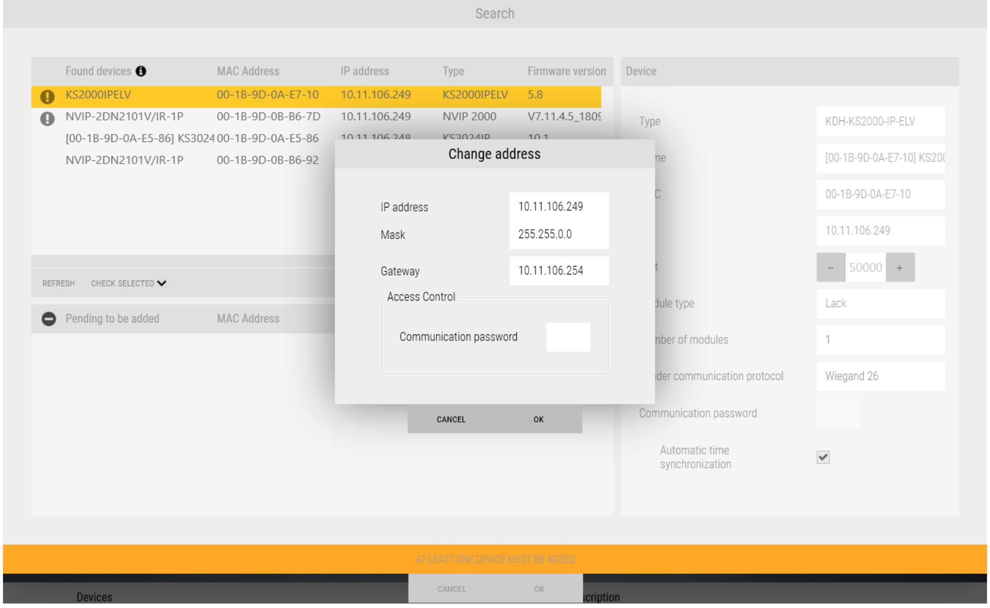
Pending to be added | MAC Address

Change address

IP address: 10.11.106.249
Mask: 255.255.0.0
Gateway: 10.11.106.254

Video Surveillance System
Login: root
Password: ••••

In case you want to change one controller address select it on the list in upper window and click *Change address* button.



Found devices	MAC Address	IP address	Type	Firmware version
KS2000IPELV	00-1B-9D-0A-E7-10	10.11.106.249	KS2000IPELV	5.8
NVIP-2DN2101V/IR-1P	00-1B-9D-0B-B6-7D	10.11.106.249	NVIP 2000	V7.11.4.5_180
[00-1B-9D-0A-E5-86] KS3024	00-1B-9D-0A-E5-86	10.11.106.248	KS3024IP	10.1
NVIP-2DN2101V/IR-1P	00-1B-9D-0B-B6-92			

Pending to be added | MAC Address

Change address

IP address: 10.11.106.249
Mask: 255.255.0.0
Gateway: 10.11.106.254

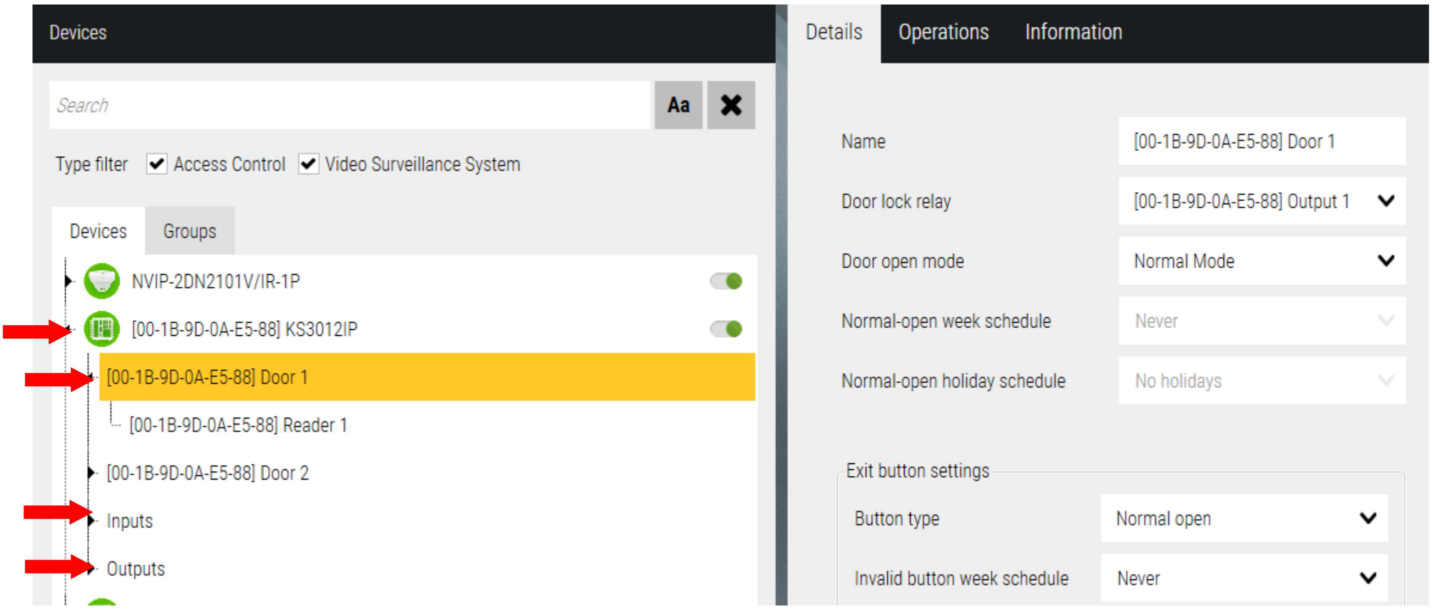
Access Control
Communication password:

Device
Type: KDH-KS2000-IP-ELV
ne: [00-1B-9D-0A-E7-10] KS20
C: 00-1B-9D-0A-E7-10
10.11.106.249
t: 50000
dule type: Lack
nber of modules: 1
der communication protocol: Wiegand 26
Communication password:
Automatic time synchronization: ☑

After address settings and adding all controllers to the list in bottom window click ***OK*** button. Added controllers appear in *Devices* window.

3.2 Devices - Access Control - Controller - Doors

In the process of adding controllers, the program automatically adds the cooperating elements in quantities dependent on the controller type. This includes doors, inputs, control outputs and expansion modules. These elements appear under each of the added controllers and can be viewed by clicking on the black triangles in each of the branches of the device tree.



Devices
Search
Aa
✖
Type filter
☑ Access Control
☑ Video Surveillance System
Devices
Groups
NVIP-2DN2101V/IR-1P
[00-1B-9D-0A-E5-88] KS3012IP
[00-1B-9D-0A-E5-88] Door 1
[00-1B-9D-0A-E5-88] Reader 1
[00-1B-9D-0A-E5-88] Door 2
Inputs
Outputs
Details
Operations
Information

Name: [00-1B-9D-0A-E5-88] Door 1

Door lock relay: [00-1B-9D-0A-E5-88] Output 1

Door open mode: Normal Mode

Normal-open week schedule: Never

Normal-open holiday schedule: No holidays

Exit button settings

Button type: Normal open

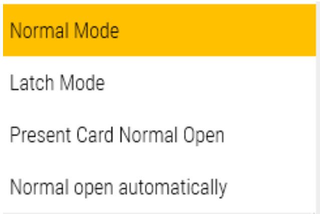
Invalid button week schedule: Never

Door settings

Name - editable field to type the name of the door instead of the default name.

Door lock relay - from the drop-down list you can select the control output (relay), which will control the lock, 1-2 relays or 1-4 are assigned by default and relay 3 or 5 is the relay to connect the alarm beacon.

Door Unlocking Mode - one of four modes to choose from:



Normal mode unlocks the door for the time set in the field below.

The latch mode unlocks and locks the door alternately after subsequent readings of the card.

Mode 3 and 4 require a schedule setting at the beginning of which the door is unlocked permanently after reading a valid card or automatically.

Normal-open week schedule - from the drop-down list you can select a schedule defined earlier, according to which the door will be unlocked permanently after reading a valid card or automatically depending on the option chosen above.

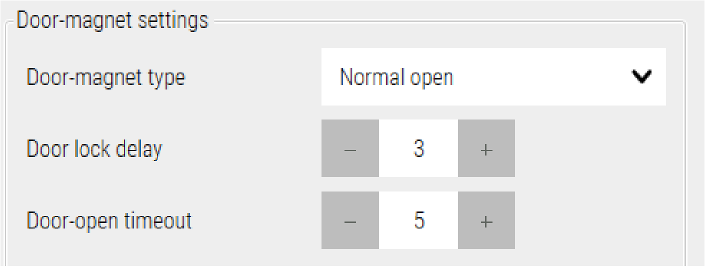
Normal-open holiday schedule - refers to the holidays, is the parent of normal-open week schedule and blocks its operation. If there is a holiday during the week, door will not be unlocked automatically.

Exit button settings

Button type - from the drop down list you can select NO or NC type - NC recommended.

Invalid button week schedule - from the drop-down list you can select a schedule defined earlier, during the period of its activity the door can not be unlocked by pressing the button.

Door-magnet settings



Door-magnet settings

Door-magnet type: Normal open

Door lock delay: 3

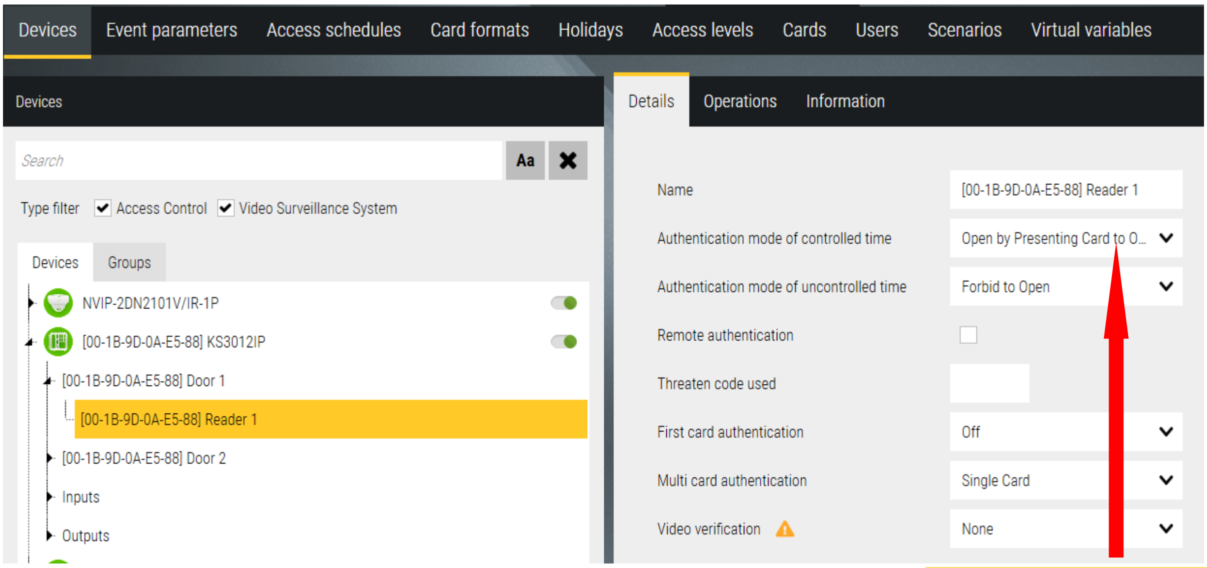
Door-open timeout: 5

Door-magnet type - from the drop-down list you can select NO or NC type

Door lock delay - editable field to enter the time (s) of unlocking the lock after reading a valid card or pressing the exit button. You can also set the time by clicking the - or + buttons. Maximum value - 50 s.

Door open timeout - editable field to enter the time (s) for closing the door leaf. After the time that is the sum of the door lock delay and door open timeout *Door - door open too long* alarm will be generated - by default 8 s (3 + 5). You can also set the time by clicking the - or + buttons. Maximum value - 50 s.

3.3 Devices - Access Control - Controller - Door - Readers



Type filter ☑ Access Control ☑ Video Surveillance System

Name: [00-1B-9D-0A-E5-88] Reader 1

Authentication mode of controlled time: Open by Presenting Card to O...

Authentication mode of uncontrolled time: Forbid to Open

Remote authentication: □

Threaten code used:

First card authentication: Off

Multi card authentication: Single Card

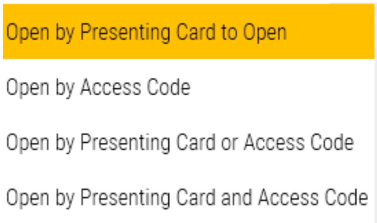
Video verification ⚠: None

Name - editable field to type the name of the reader in place of the default name.

Authentication mode of controlled time - from the drop-down list you can select:

Authentication mode of controlled time - you can select from the drop-down list:

(This mode applies to the off-hours period, weekends and public holidays)



Open by Presenting Card to Open

Open by Access Code

Open by Presenting Card or Access Code

Open by Presenting Card and Access Code

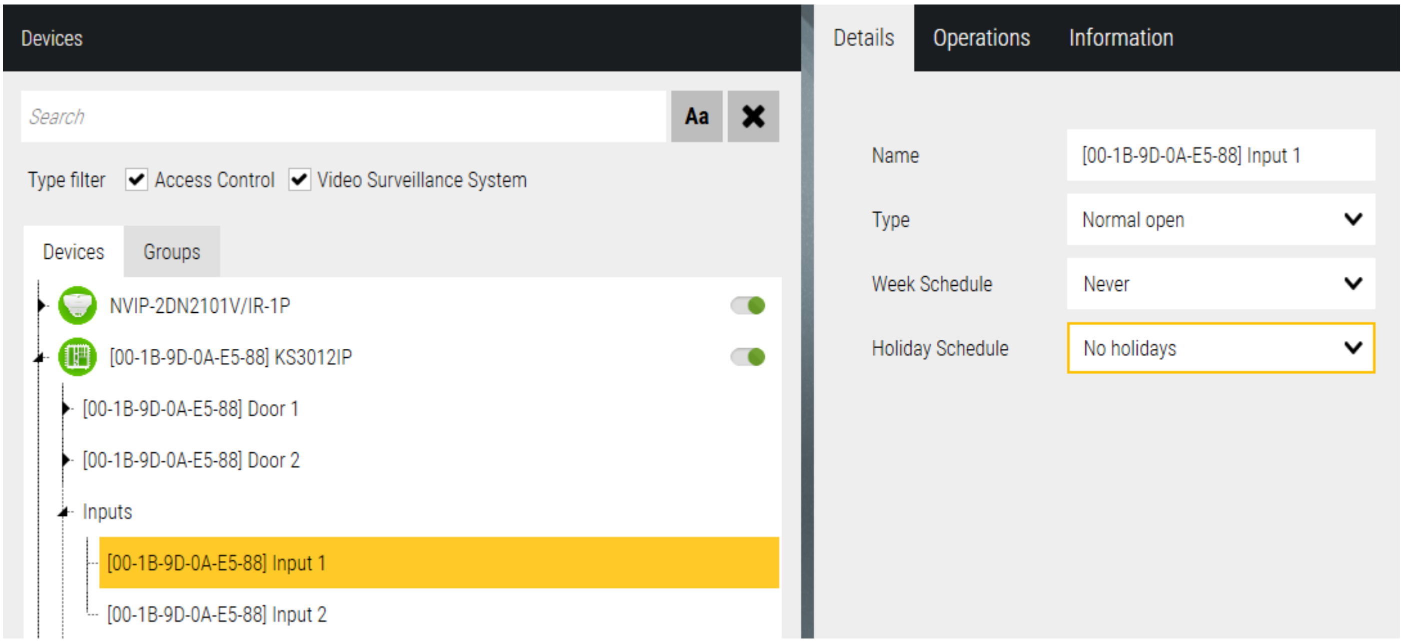
Remote authentication - when checked, access from this reader will require a valid card to be read and confirmation by the operator in a special pop-up window. Select this option only when the system is in online mode and the operator or security worker is present at the station.

Threaten code used - a field for entering the passcode to be used on the reader's keyboard in case of a forced entry. It generates a discrete alarm on the operator station.

First card authentication - access requires the use of a card in each day with the option set to Yes (this is the field in the users settings).

Multi card authentication - access requires the use of one to four valid cards to unlock. Special option for rooms requiring greater security (so-called "commission entry").

3.4 Devices - Access Control - Controller - Inputs


Devices
Search
Aa
✖
Type filter ☑ Access Control ☑ Video Surveillance System
Devices
Groups
NVIP-2DN2101V/IR-1P
[00-1B-9D-0A-E5-88] KS3012IP
[00-1B-9D-0A-E5-88] Door 1
[00-1B-9D-0A-E5-88] Door 2
Inputs
[00-1B-9D-0A-E5-88] Input 1
[00-1B-9D-0A-E5-88] Input 2
Details
Operations
Information

Name: [00-1B-9D-0A-E5-88] Input 1

Type: Normal open

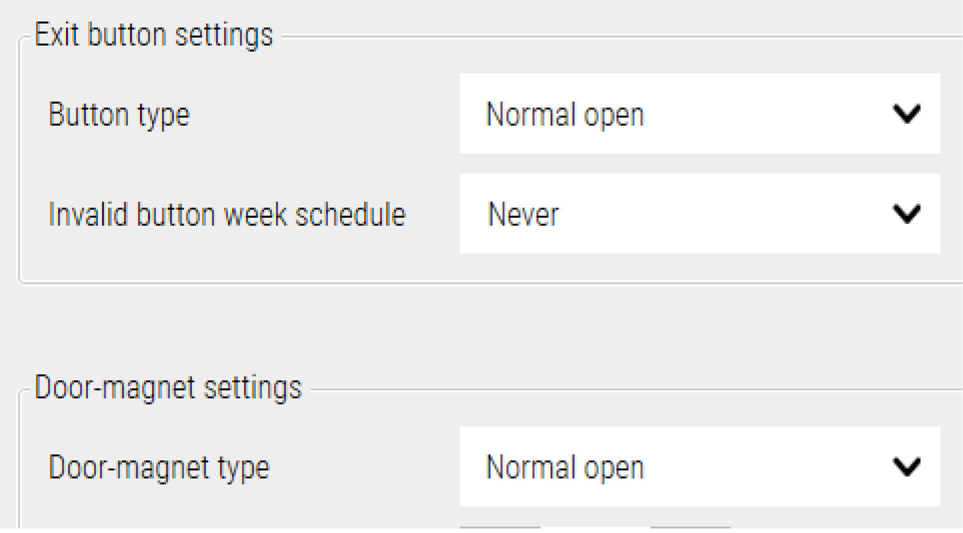
Week Schedule: Never

Holiday Schedule: No holidays

The input lines located on the controller allow you to connect and monitor various types of detectors.
To activate the monitoring mode, you need to set the week and holiday schedule. If monitoring is disabled, this input activation only results in a change in the state of the panel icon. Depending on the controller model, we have 2 or 4 input lines and 4 on the KDH-MOD2000INOUT expansion module.

Name - editable field to enter the name of the input line in place of the default name.
Type - from the drop-down list you can select NO or NC type - recommended NC.
Week schedule - in the drop-down list you can select a predefined schedule according to which the input will be monitored and then the alarms will be generated.
Holiday schedule - refers to holidays, is the parent of a weekly schedule and changes its effect if there is a holiday day during the week in which the input should have a different monitoring schedule.
Input lines on the extension module look similarly if implemented.

The settings for the input lines for the door sensors and exit buttons status are available in the Door configuration window.



Exit button settings

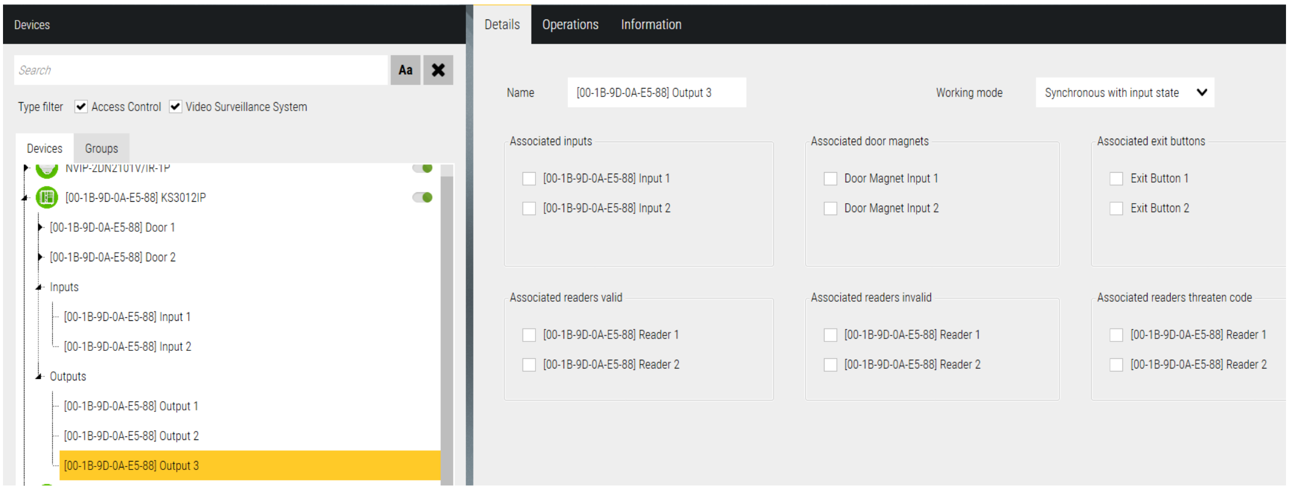
Button type: Normal open

Invalid button week schedule: Never

Door-magnet settings

Door-magnet type: Normal open

3.5 Devices - Access Control - Controller - Outputs



Devices

Search Aa ✖

Type filter ☑ Access Control ☑ Video Surveillance System

Devices Groups

NVIP-2DN2101V/IR-1P

[00-1B-9D-0A-E5-88] KS3012IP

[00-1B-9D-0A-E5-88] Door 1

[00-1B-9D-0A-E5-88] Door 2

Inputs

[00-1B-9D-0A-E5-88] Input 1

[00-1B-9D-0A-E5-88] Input 2

Outputs

[00-1B-9D-0A-E5-88] Output 1

[00-1B-9D-0A-E5-88] Output 2

[00-1B-9D-0A-E5-88] Output 3

Details Operations Information

Name [00-1B-9D-0A-E5-88] Output 3

Working mode Synchronous with input state

Associated inputs
□ [00-1B-9D-0A-E5-88] Input 1
□ [00-1B-9D-0A-E5-88] Input 2

Associated door magnets
□ Door Magnet Input 1
□ Door Magnet Input 2

Associated exit buttons
□ Exit Button 1
□ Exit Button 2

Associated readers valid
□ [00-1B-9D-0A-E5-88] Reader 1
□ [00-1B-9D-0A-E5-88] Reader 2

Associated readers invalid
□ [00-1B-9D-0A-E5-88] Reader 1
□ [00-1B-9D-0A-E5-88] Reader 2

Associated readers threaten code
□ [00-1B-9D-0A-E5-88] Reader 1
□ [00-1B-9D-0A-E5-88] Reader 2

Control outputs located on the controller allow you to connect and control various types of devices. In terms of functionality and settings, they are divided into two groups:

- Door outputs and control of the electric lock
- General purpose control outputs

The control outputs of the electric lock in the settings have only a name change and you can not put their icon on the panel because their state illustrates a padlock in the door icon.

The other outputs have settings as in the image above. You can assign them to the status of system items located on the same controller or selected events. Changing the status of the assigned item or occurrence of the selected event causes the relay switch.

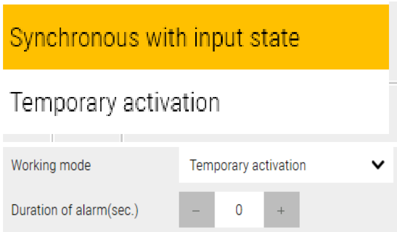
Depending on the controller model, there are 3 or 5 control outputs and 4 on the KDH-MOD2000INOUT expansion module.

Name - editable field to enter the name of the control output in place of the default name.

Working mode - from the drop down list you can select the operating mode:

Synchronously with input state - switches when the assigned input line enters or exits the alarm status

Temporary activation - switches to the time set in the field below



Synchronous with input state

Temporary activation

Working mode Temporary activation

Duration of alarm(sec.) – 0 +

You have the choice of:

- states of three elements: input lines, door magnets and exit button
- events regarding to access granted, denied and threaten code

The sync assignment becomes active when you select checkbox.

Sliders let you display the remaining check boxes.

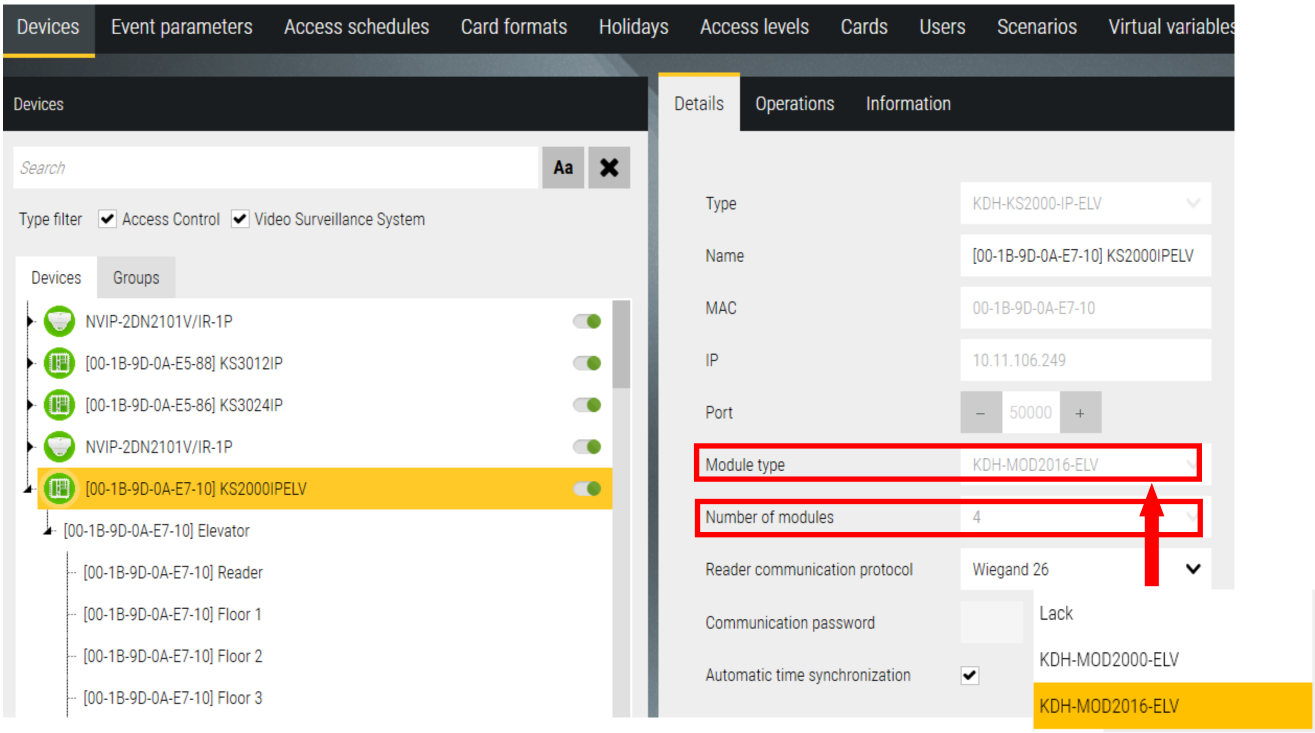
* Week Schedule - from the drop-down list you can select an earlier defined schedule according to which output will be automatically switched.

* Holiday Schedule - refers to the holidays, is the parent of week schedule and blocks its operation. If there is a holiday during the week, output will not be switched automatically.

(* will be implemented in the next version of the program)

Settings for control outputs on the expansion module are similar if implemented.

3.6 Devices - Access Control - Elevator controllers



Devices | Event parameters | Access schedules | Card formats | Holidays | Access levels | Cards | Users | Scenarios | Virtual variables

Devices

Search

Type filter ☑ Access Control ☑ Video Surveillance System

Devices | Groups

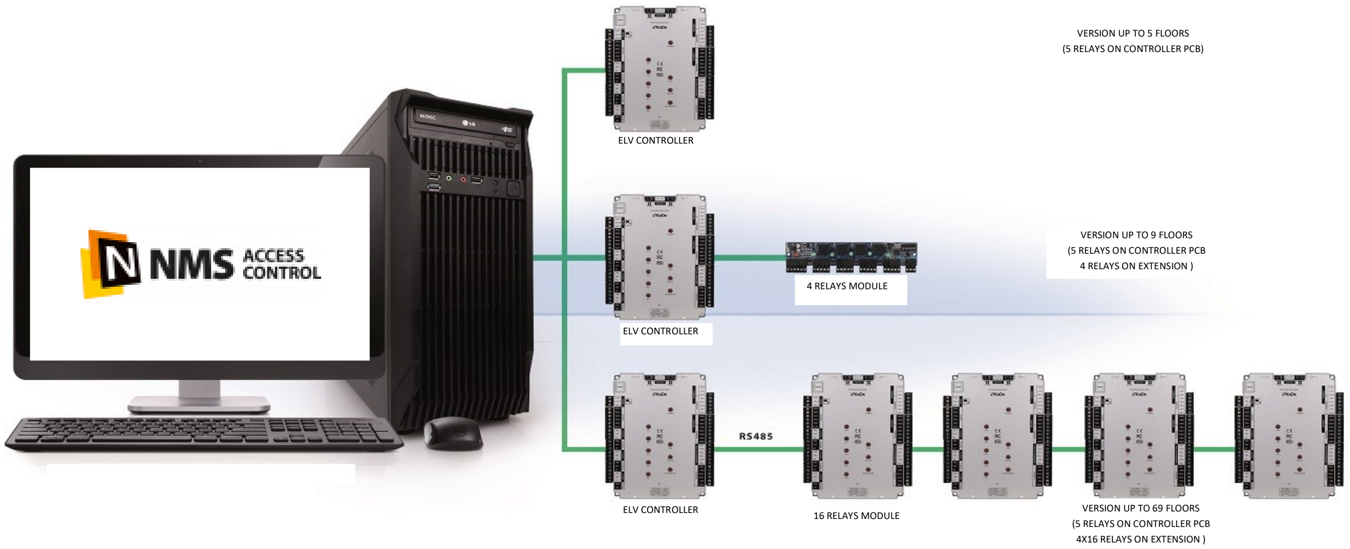
- NVIP-2DN2101V/IR-1P
- [00-1B-9D-0A-E5-88] KS3012IP
- [00-1B-9D-0A-E5-86] KS3024IP
- NVIP-2DN2101V/IR-1P
- [00-1B-9D-0A-E7-10] KS2000IPELV
  - [00-1B-9D-0A-E7-10] Elevator
    - [00-1B-9D-0A-E7-10] Reader
    - [00-1B-9D-0A-E7-10] Floor 1
    - [00-1B-9D-0A-E7-10] Floor 2
    - [00-1B-9D-0A-E7-10] Floor 3

Details | Operations | Information

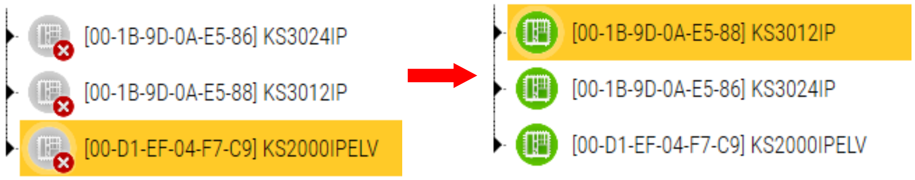
Type	KDH-KS2000-IP-ELV
Name	[00-1B-9D-0A-E7-10] KS2000IPELV
MAC	00-1B-9D-0A-E7-10
IP	10.11.106.249
Port	50000
Module type	KDH-MOD2016-ELV
Number of modules	4
Reader communication protocol	Wiegand 26
Communication password	
Automatic time synchronization	☑

Lack
KDH-MOD2000-ELV
KDH-MOD2016-ELV

To KDH-KS2000-IP-ELV you can add expansion modules also. There are two types of modules. Depending on floors quantity operated by elevator there are some combinations as following.



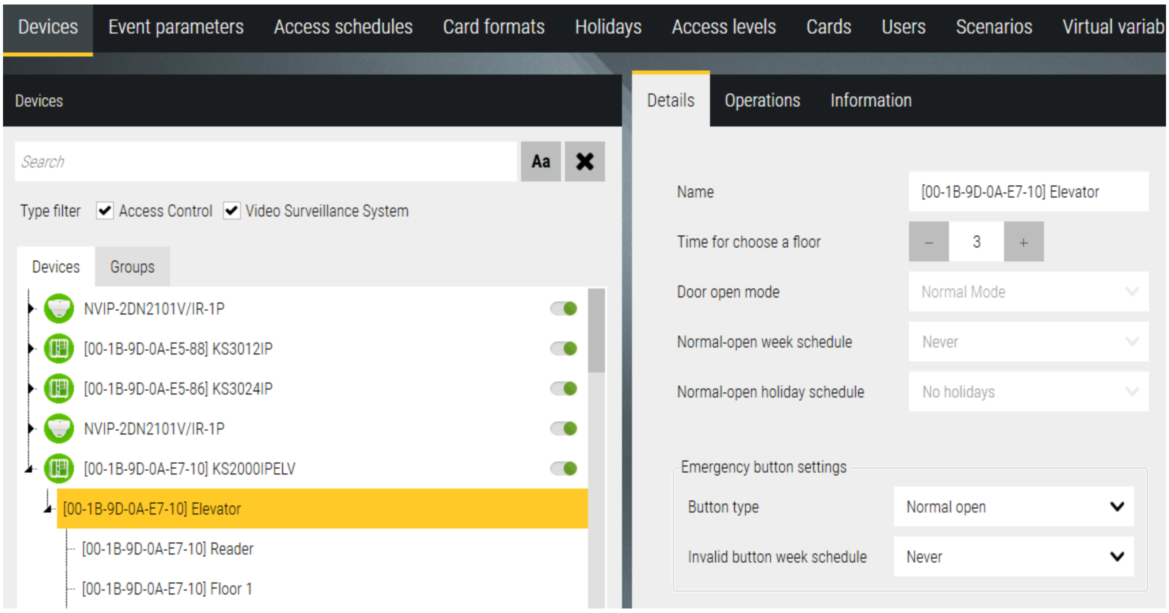
After you have completed all the settings for each controller (analogical to adding controllers in off-line mode), click on the floppy disk icon in the lower right corner of the *Configuration* window to save to the database. During this process, a series of messages informing the successful completion of the data save will appear in the System Log window. The controller icons will change to green, which shows the correct communication:



- [00-1B-9D-0A-E5-86] KS3024IP
- [00-1B-9D-0A-E5-88] KS3012IP
- [00-D1-EF-04-F7-C9] KS2000IPELV

- [00-1B-9D-0A-E5-88] KS3012IP
- [00-1B-9D-0A-E5-86] KS3024IP
- [00-D1-EF-04-F7-C9] KS2000IPELV

3.7 Devices - Access Control - Elevator controller - Elevator


Devices
Event parameters
Access schedules
Card formats
Holidays
Access levels
Cards
Users
Scenarios
Virtual variab
Devices
Search
Aa
Type filter ☑ Access Control ☑ Video Surveillance System
Devices
Groups
NVIP-2DN2101V/IR-1P
[00-1B-9D-0A-E5-88] KS3012IP
[00-1B-9D-0A-E5-86] KS3024IP
NVIP-2DN2101V/IR-1P
[00-1B-9D-0A-E7-10] KS2000IPELV
[00-1B-9D-0A-E7-10] Elevator
[00-1B-9D-0A-E7-10] Reader
[00-1B-9D-0A-E7-10] Floor 1
Details
Operations
Information

Name: [00-1B-9D-0A-E7-10] Elevator

Time for choose a floor: 3

Door open mode: Normal Mode

Normal-open week schedule: Never

Normal-open holiday schedule: No holidays

Emergency button settings

Button type: Normal open

Invalid button week schedule: Never

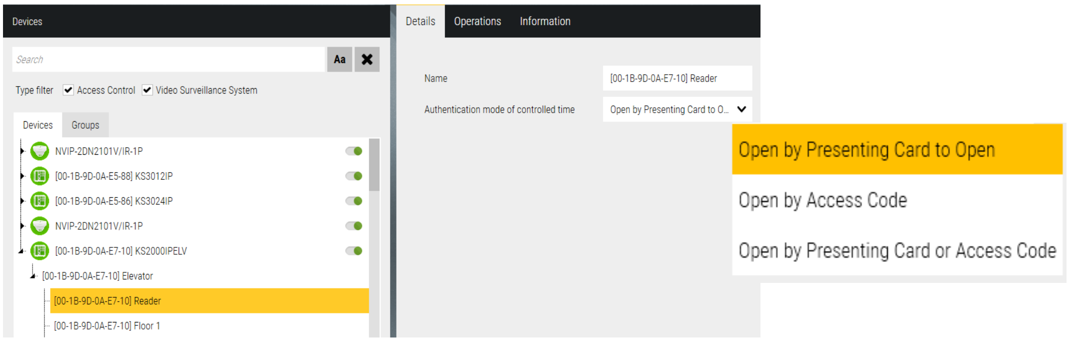
Name - editable field to type the name of the elevator in place of the default name.

Time for choose a floor - editable field to enter or set the time to select the floor after reading a valid card

Emergency button settings - used to unlock all floors permanently, so it should be a two-state button. Recommended model KDH-EXIT1030-P - with push-in plastic plate (as for emergency door unlocking).

- Button type - select NO or NC
- Invalid button week schedule - select from the drop-down list. During the period when the schedule is active the button will not work.

3.8 Devices - Access Control - Elevator controller - Elevator - Reader


Devices
Search
Aa
Type filter ☑ Access Control ☑ Video Surveillance System
Devices
Groups
NVIP-2DN2101V/IR-1P
[00-1B-9D-0A-E5-88] KS3012IP
[00-1B-9D-0A-E5-86] KS3024IP
NVIP-2DN2101V/IR-1P
[00-1B-9D-0A-E7-10] KS2000IPELV
[00-1B-9D-0A-E7-10] Elevator
[00-1B-9D-0A-E7-10] Reader
[00-1B-9D-0A-E7-10] Floor 1
Details
Operations
Information
Open by Presenting Card to Open
Open by Access Code
Open by Presenting Card or Access Code

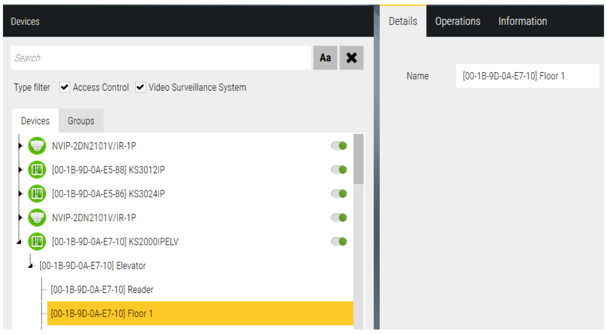
Name: [00-1B-9D-0A-E7-10] Reader

Authentication mode of controlled time: Open by Presenting Card to O...

Name - editable field to type the name of the reader in place of the default name.

3.9 Devices - Access Control - Elevator controller - Elevator - Reader - Floor

Name - editable field to type the name of the floor in place of the default name.


Devices
Search
Aa
Type filter ☑ Access Control ☑ Video Surveillance System
Devices
Groups
NVIP-2DN2101V/IR-1P
[00-1B-9D-0A-E5-88] KS3012IP
[00-1B-9D-0A-E5-86] KS3024IP
NVIP-2DN2101V/IR-1P
[00-1B-9D-0A-E7-10] KS2000IPELV
[00-1B-9D-0A-E7-10] Elevator
[00-1B-9D-0A-E7-10] Reader
[00-1B-9D-0A-E7-10] Floor 1
Details
Operations
Information

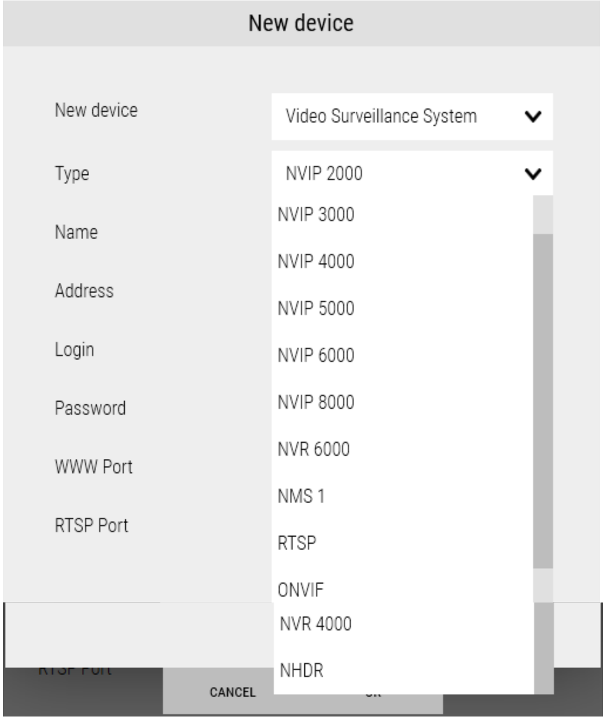
Name: [00-1B-9D-0A-E7-10] Floor 1

3.10 Devices - Video Surveillance System

In addition to the functions associated with access control, NMS ACCESS CONTROL also integrates the video surveillance system. At this stage, this functionality is limited to:

- displaying the live image from the selected camera by clicking on the icon on the panel
- automatic display of such an image after a specific event (e.g. door forced, card reading) as a result of the execution of a scenario

List of VSS devices that can be connected with NMS ACCESS CONTROL:



New device

New device: Video Surveillance System

Type: NVIP 2000

The main items in the list are NOVUS devices (DVR and IP Camera series), but it is also possible to integrate with RTSP and ONVIF compliant video stream devices. A free license allows you to connect:

NOVUS video channels	16
ONVIF video channels	1
RTSP video channels	1

In the current version of the software, you can only add VSS devices manually using the *New device - Video surveillance system* option*.* A window will be displayed as on the next page.

Type - first select the type of video device as on the list as above.

Name - editable field to type the name of the video device in place of the default name if you want. This field will be filled automatically when camera is connected.

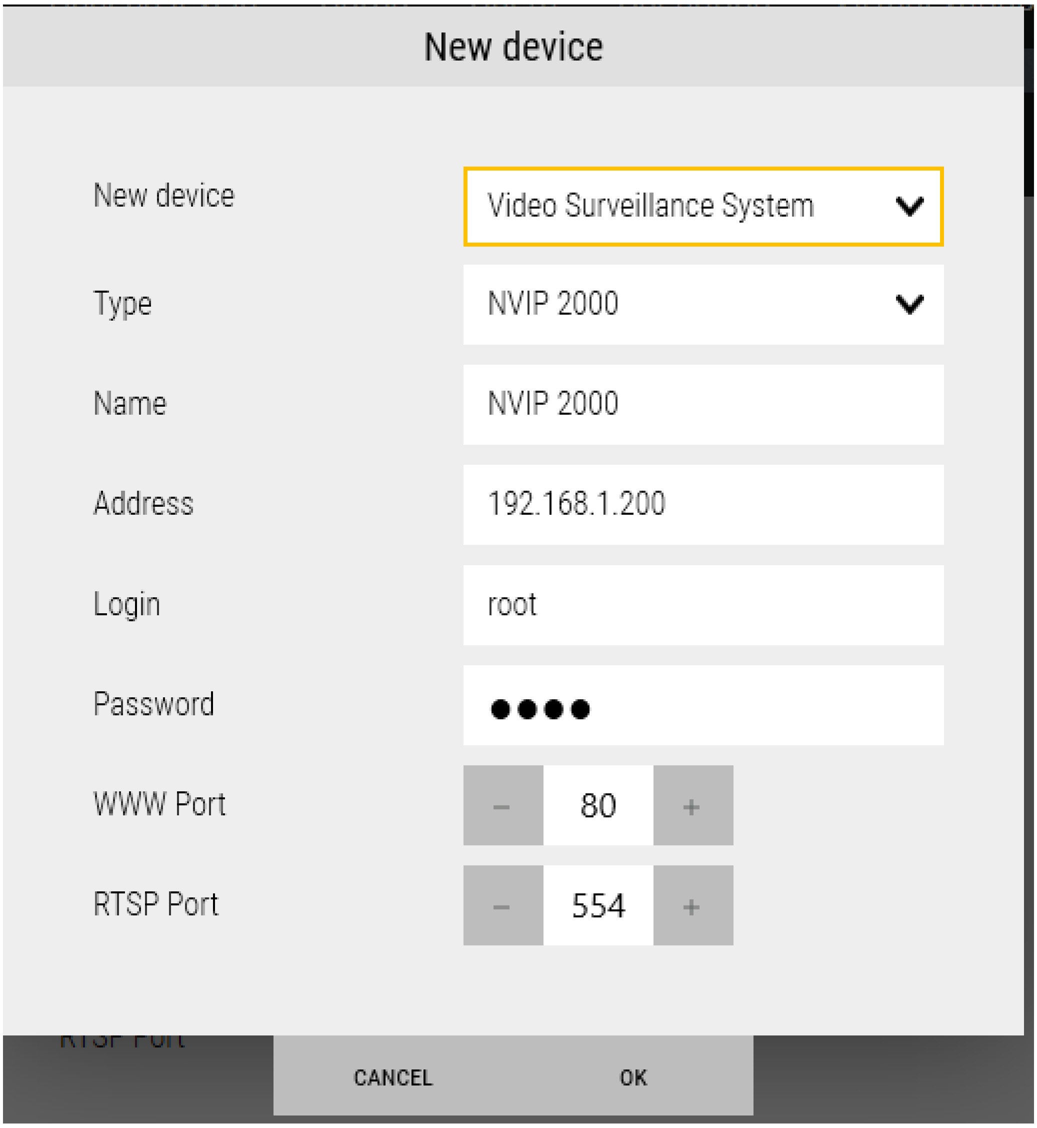
Description - editable field for description, e.g. location of the camera.

IP Address - field for entering IP address that matches the settings of the camera

WWW Port - field for entering the port number that matches the settings of the camera

RTSP Port - field for entering the port number that matches the settings of the video device

Data Port - field to type the port number that matches the settings on the video device



New device

New device: Video Surveillance System

Type: NVIP 2000

Name: NVIP 2000

Address: 192.168.1.200

Login: root

Password: ●●●●

WWW Port: 80

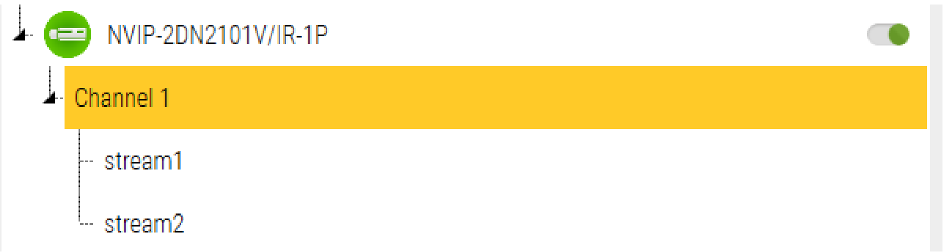
RTSP Port: 554

User - editable field to type a user name that matches the settings of the video device.

Password - editable field for typing a user password that matches the settings of the video device.

After setting the required parameters click on the ***OK*** button, and when returning to the *Device* window save by clicking on the floppy disk icon in the lower right corner of the configuration window. A series of messages informing you that the settings have been saved to the database will appear in the System Log window. Then, when connected to the device, the icon turns green.

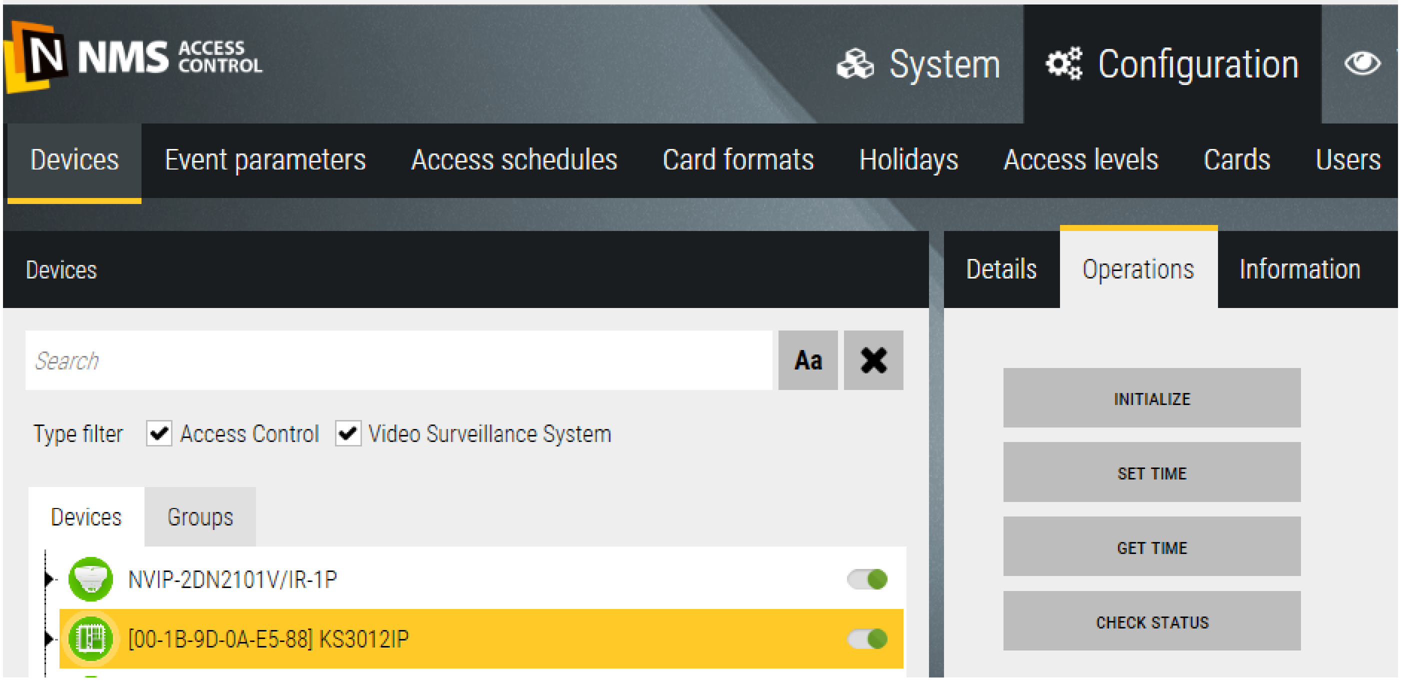
For panel operations, we use the Channel X position, which is displayed in the tree when expanded.



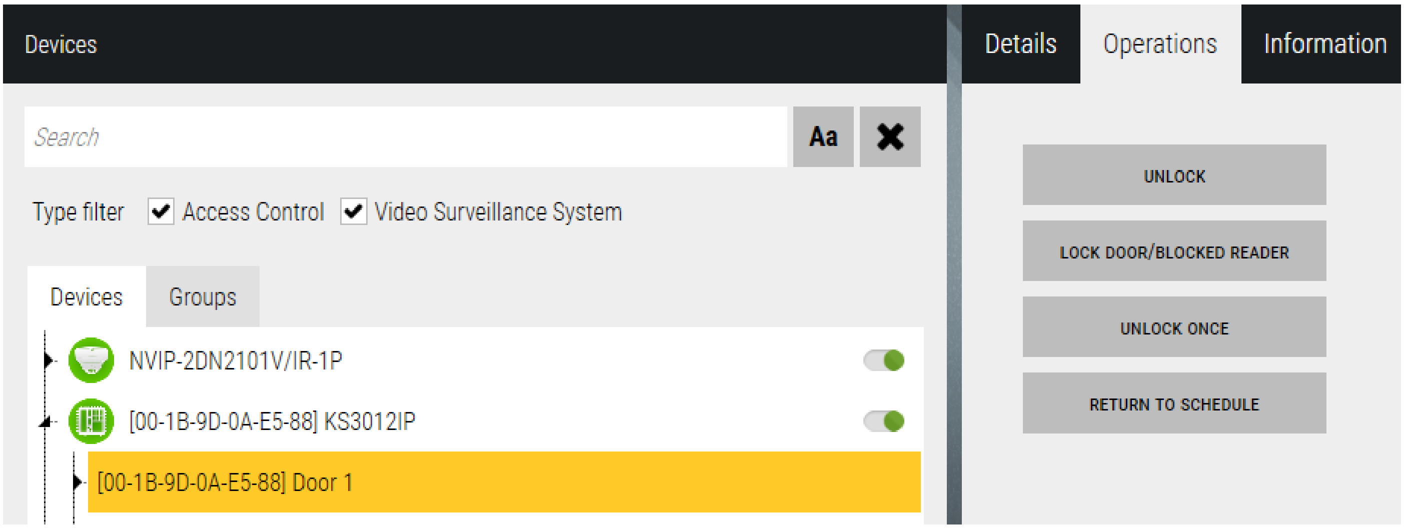
3.11 Devices - Operations

System items shown below have operators commands in Operations tab, which allow to perform certain operations as on the lists below.

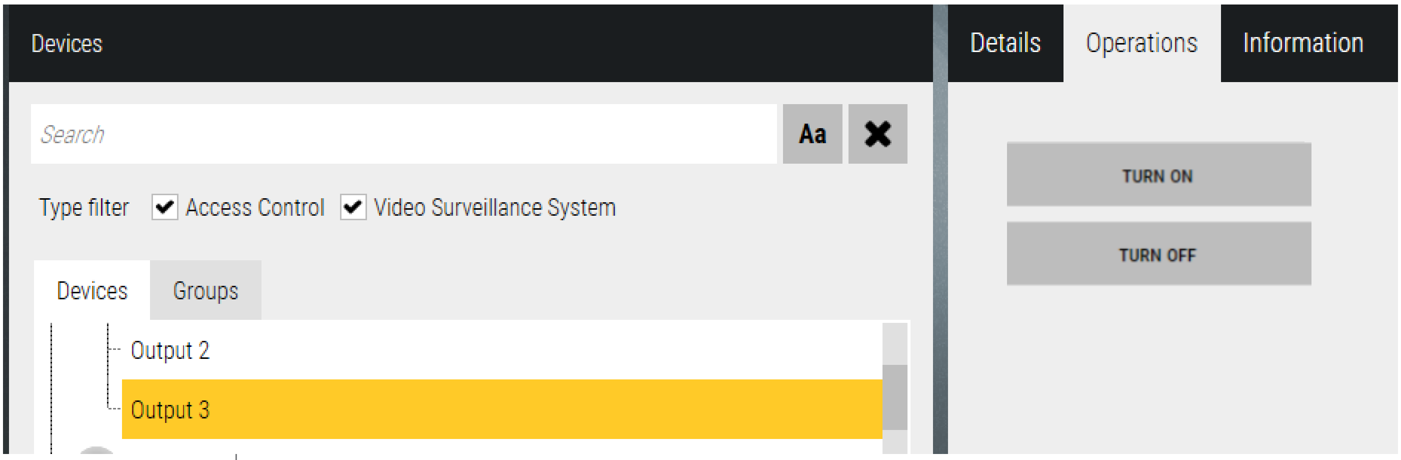
Controller



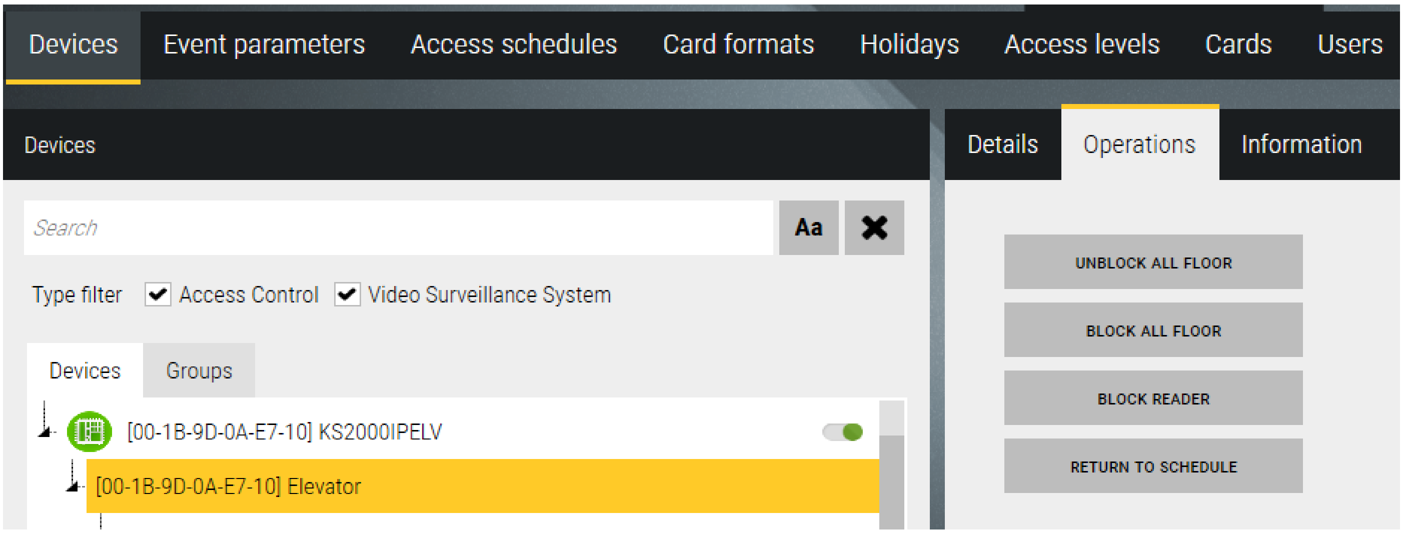
Door



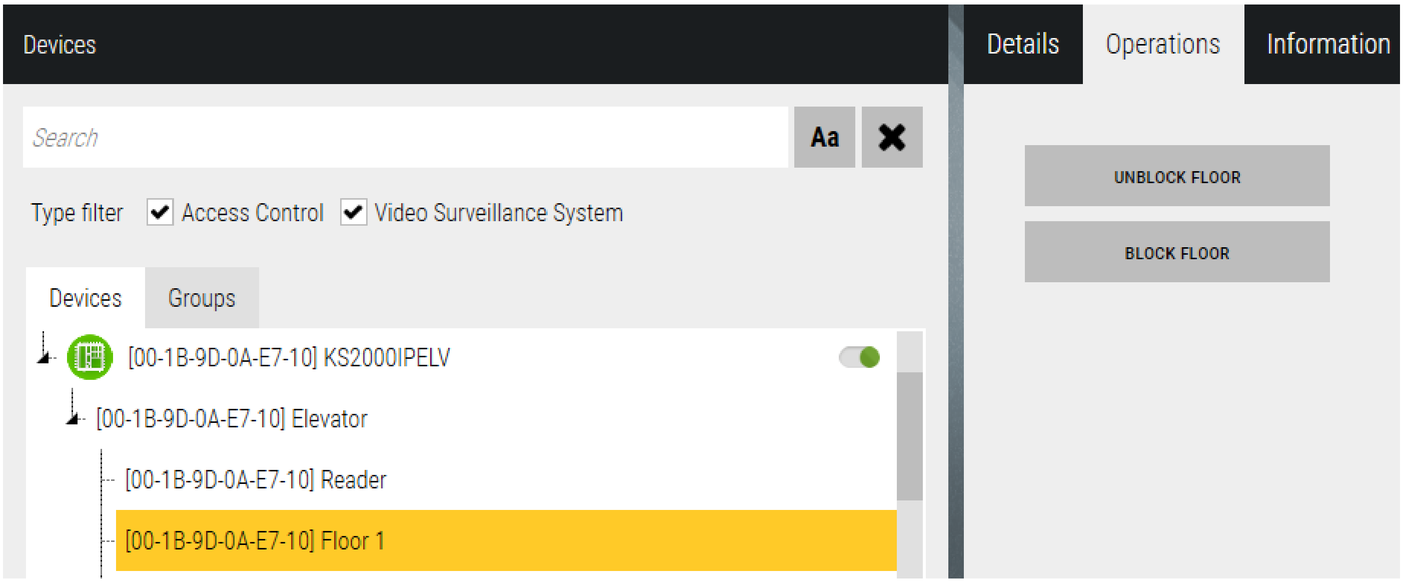
Output (not linked with lock only)



Elevator

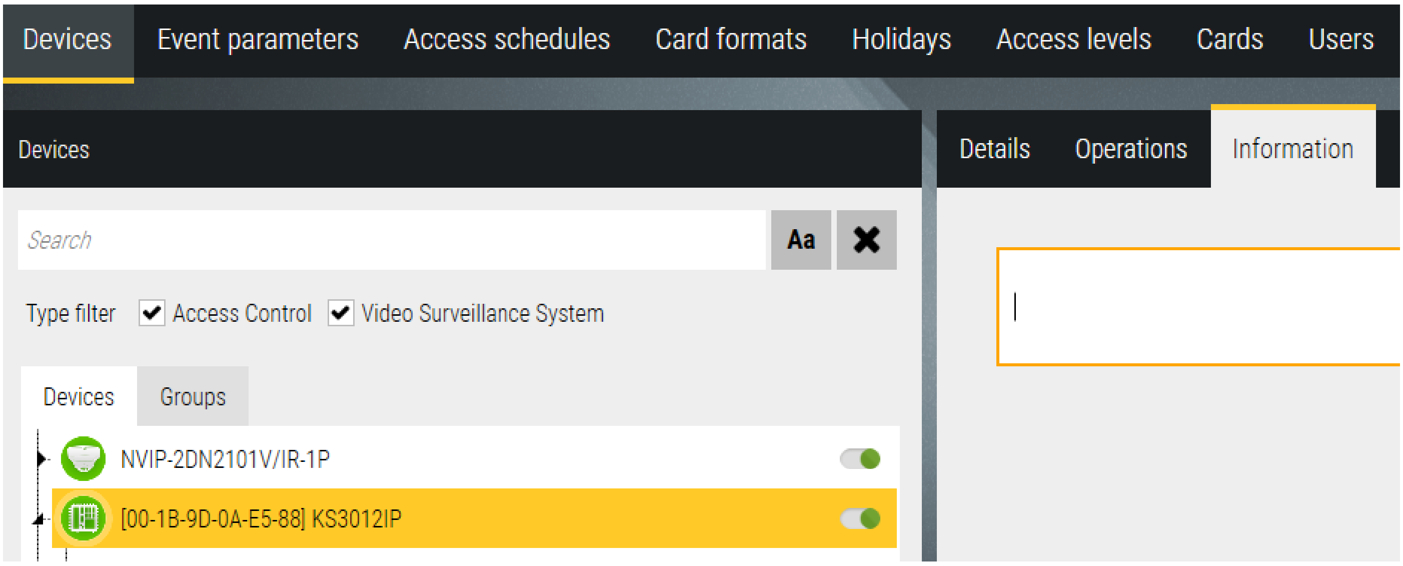


Floor


Devices
Details
Operations
Information
Search
Aa
Type filter
☑ Access Control
☑ Video Surveillance System
Devices
Groups
[00-1B-9D-0A-E7-10] KS2000IPELV
[00-1B-9D-0A-E7-10] Elevator
[00-1B-9D-0A-E7-10] Reader
[00-1B-9D-0A-E7-10] Floor 1
UNBLOCK FLOOR
BLOCK FLOOR

3.12 Devices - Information

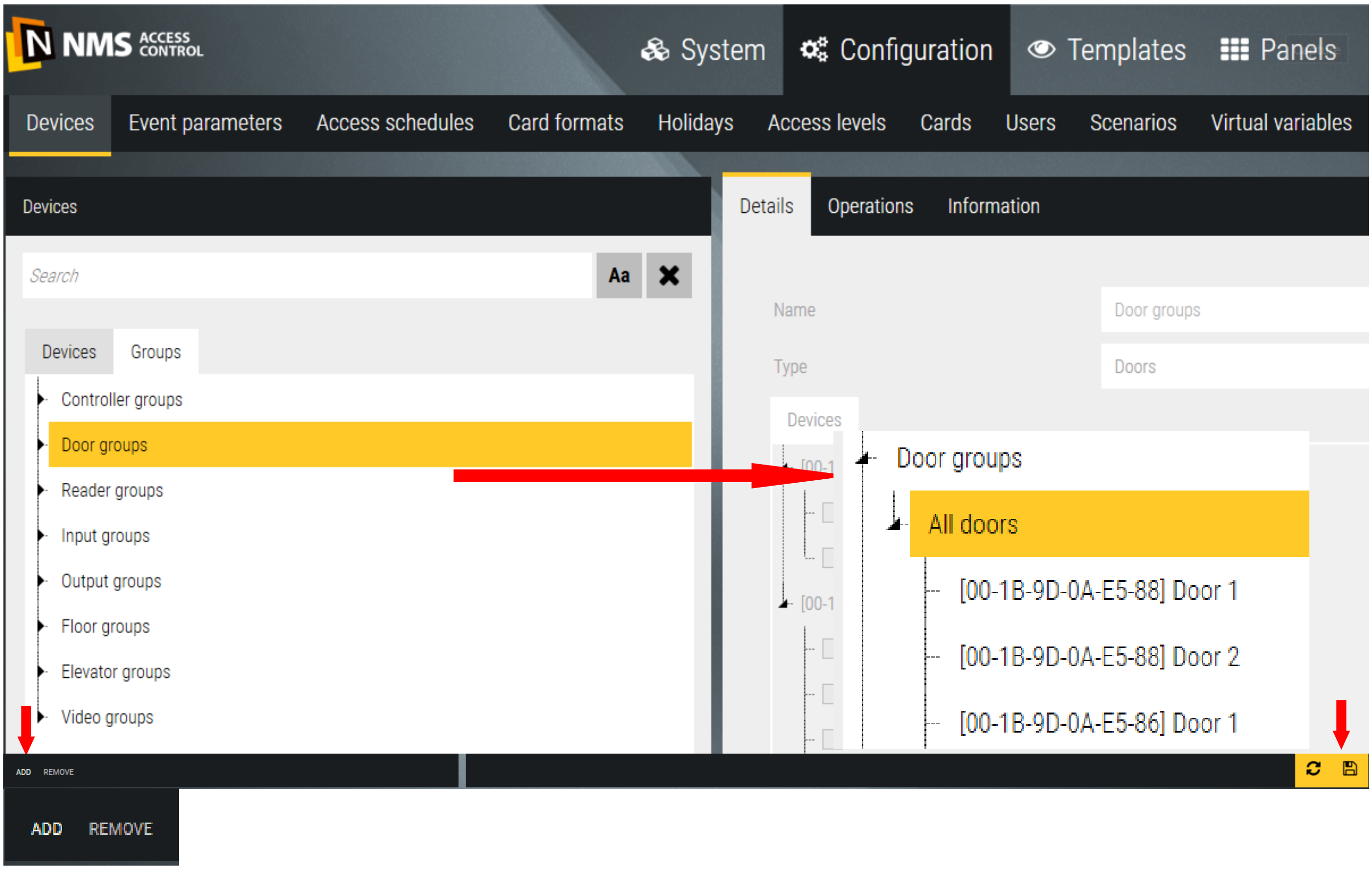
Every item has *Information* tab, which you can place optional information in.



3.13 Devices - Groups

Use the *Groups* tab to define groups of system elements. The list of default main groups is displayed in the left window. Each default group has a defined group that contains all the elements of that type (see *Door groups)* and is automatically updated when a new element of the type is added.

Groups are used to perform collective operations on elements of the system e.g. unlocking the door group, which greatly accelerates this process with a large number of doors. You can perform group operations from the black group icon context menu on the panel or by navigating to the *Operations* tab in this window.



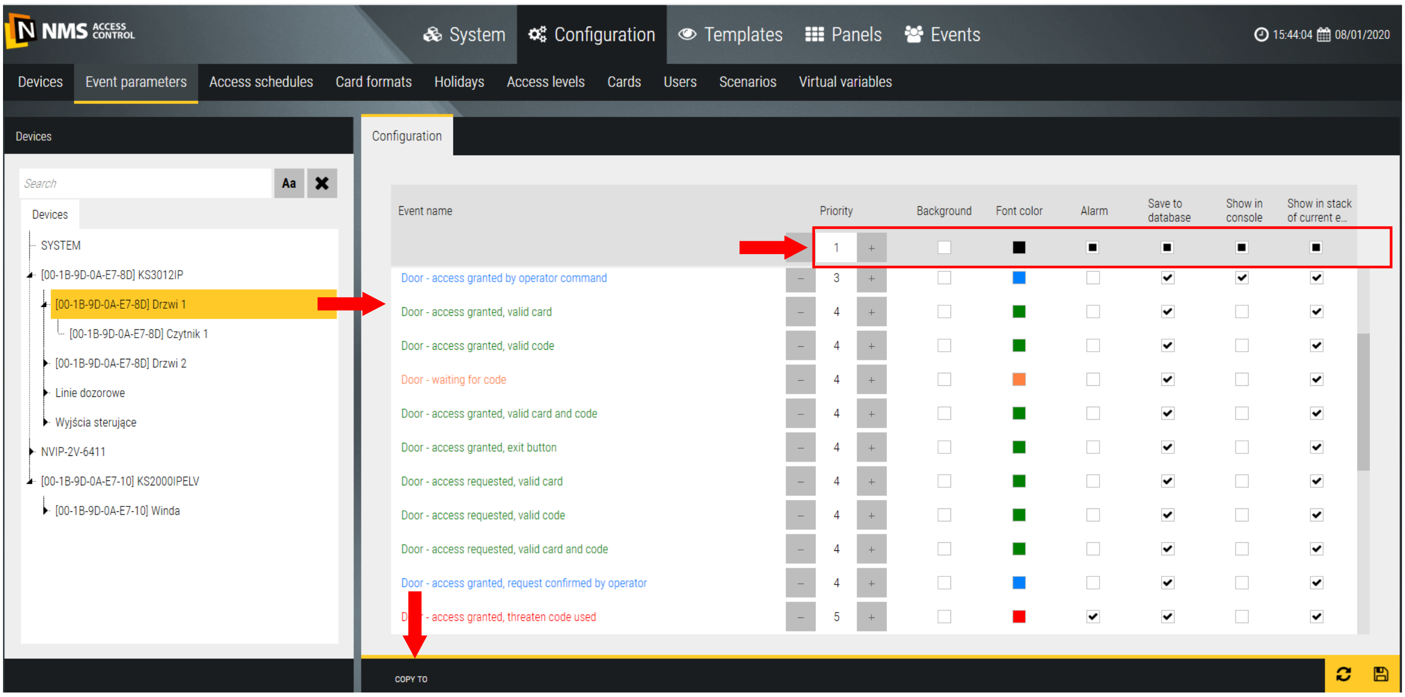
In addition to the default groups that contain all elements of a given type, you can define subgroups that contain only selected elements of that type. To do this, select the default group of the type and click *Add* at the bottom of the window. A new subgroup appears in the group tree, and a list of all elements of the type is displayed in the right window. Select the items that you want to add to the new group.

To add a new group in the main tree, no groups can be selected. If there is a selection (yellow bar) then click on it while holding down the CTRL button. A group added in the main tree can contain elements of different types. This can be used to create a system structure in multiple locations.

You can edit or delete a defined group by selecting it on the list and clicking the *Delete* button in the lower left corner of the window.

3.14 Event parameters

The *Event parameters* tab contains the default settings for selected message parameters associated with system elements. Each element of a given type (controller, door, etc.) has its own list of events.



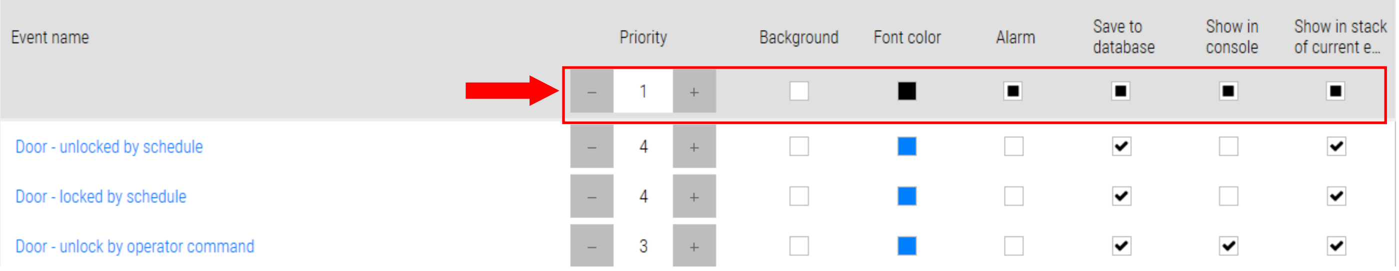
Event name	Priority	Background	Font color	Alarm	Save to database	Show in console	Show in stack of current e...
	1	□	■	■	■	■	■
Door - access granted by operator command	3	□	🟦	□	☑	☑	☑
Door - access granted, valid card	4	□	🟩	□	☑	□	☑
Door - access granted, valid code	4	□	🟩	□	☑	□	☑
Door - waiting for code	4	□	🟧	□	☑	□	☑
Door - access granted, valid card and code	4	□	🟩	□	☑	□	☑
Door - access granted, exit button	4	□	🟩	□	☑	□	☑
Door - access requested, valid card	4	□	🟩	□	☑	□	☑
Door - access requested, valid code	4	□	🟩	□	☑	□	☑
Door - access requested, valid card and code	4	□	🟩	□	☑	□	☑
Door - access granted, request confirmed by operator	4	□	🟦	□	☑	□	☑
D - access granted, threaten code used	5	□	🟥	☑	☑	□	☑

The parameter list includes the following items:

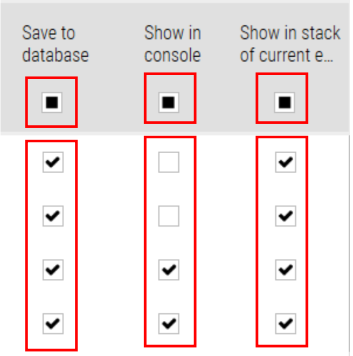
- Priority - from 1 to 5, allows additional filtering on the event stack. The default settings specify the event group, for example priority 4 is assigned to access-related events.
- Background - selectable from the color palette when clicked. Default setting - white for all events.
- Font color - to choose from the color palette when clicked. The default settings specify the event group, for example the green color is assigned to access granted-related events.
- Alarm - after selecting the message becomes an alarm message and is displayed on the alarm bar. It is displayed in red by default and requires confirmation by the operator. This includes, for example door forcing, input activation with monitoring enabled, loss of communication with the controller, etc. Each event can be marked as an alarm, but must then be handled by the operator.
- Write to database - decides whether the event will be written to the system database and will then be available by generating the report. Each event besides a descriptive part has a date and time stamp.
- Show in console - decides whether the event will be displayed in the console (lower window).
- Show in stack - decides whether the event will be displayed in the event stack on the panel.

Copy to - allow to copy events parameters settings to the others component (the same type)

The fields above the parameter columns allow you to select/deselect or select one color for all events in the list. They also indicate whether all items have the same or different settings in the list. A smaller black square in the field from this line indicates that there are different settings in the column below.

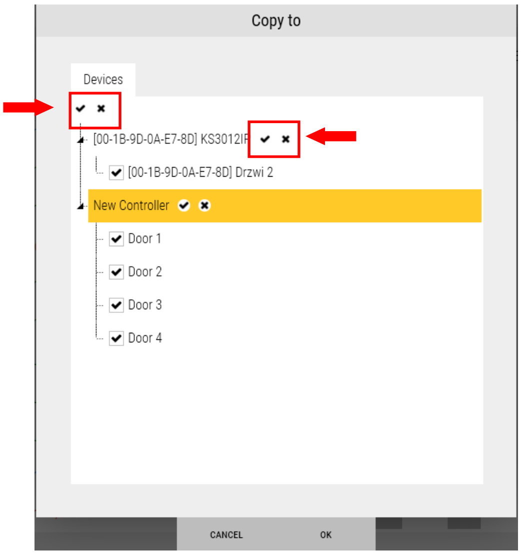


Event name	Priority	Background	Font color	Alarm	Save to database	Show in console	Show in stack of current e...
	– 1 +	□	■	■	■	■	■
Door - unlocked by schedule	– 4 +	□	🟦	□	☑	□	☑
Door - locked by schedule	– 4 +	□	🟦	□	☑	□	☑
Door - unlock by operator command	– 3 +	□	🟦	□	☑	☑	☑



Save to database	Show in console	Show in stack of current e...
■	■	■
☑	□	☑
☑	□	☑
☑	☑	☑
☑	☑	☑

New system elements added (controllers, doors, etc.) have automatically assigned the default settings of the event parameters. If you change the default parameter setting for the selected event, you can copy it for the other items of that type (e.g. door) by clicking on the *Copy* button at the bottom of the window. A window with a list of items of the type is displayed:



Copy to

Devices

✔ ✖

[00-1B-9D-0A-E7-8D] KS3012IP ✔ ✖

☑ [00-1B-9D-0A-E7-8D] Drzwi 2

New Controller ✔ ✖

☑ Door 1

☑ Door 2

☑ Door 3

☑ Door 4

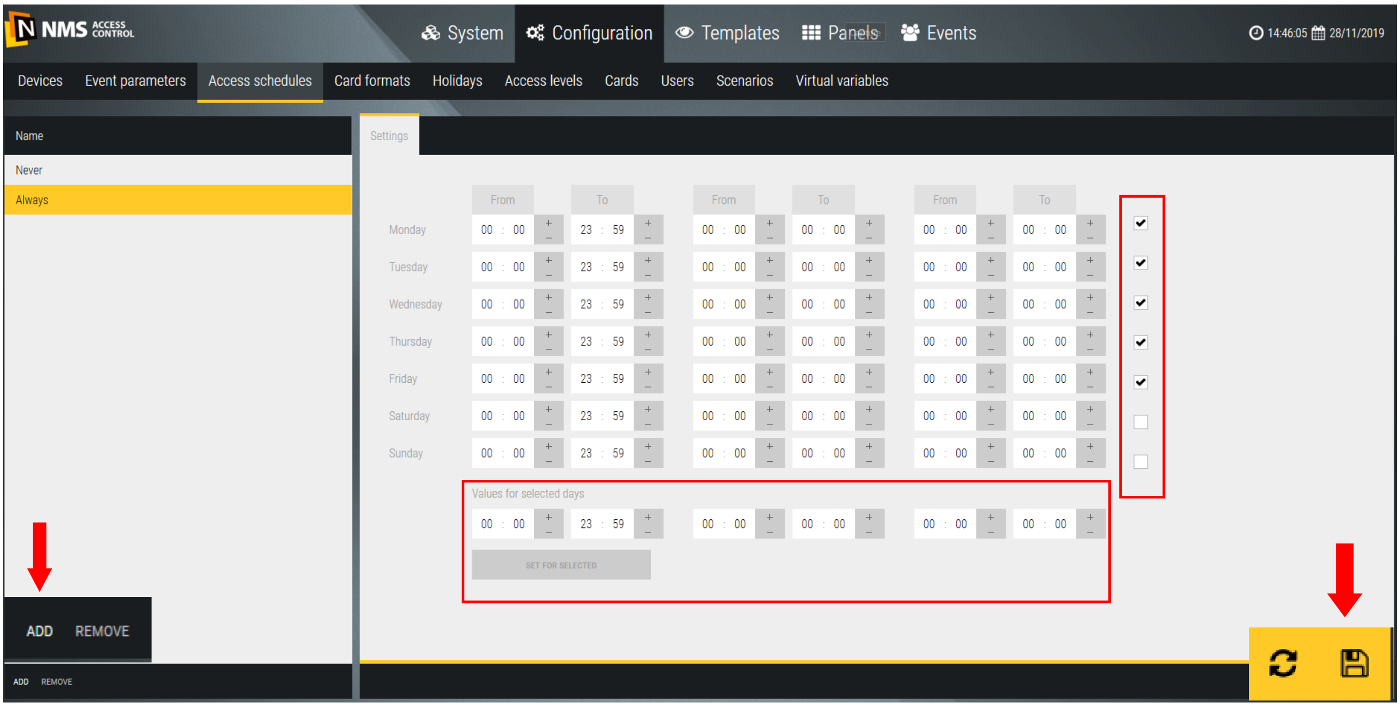
Using the checkboxes ✔ ✖ you can quickly select to deselect items in the entire list or parts of it.
The program also allows different settings for the same event for different elements of the same type e.g. doors.

You can edit the defined default parameters.

3.15 Access schedules

The *Access schedules* tab allows you to define the schedules for access levels, automatic door unlocking, monitoring of the inputs at specified intervals and switching on the control outputs* (* option available soon).

By default, two schedules are defined, *Never* and *Always,* which cannot be deleted or edited.



Name
Never
Always

	From	To	From	To	From	To	
Monday	00 : 00	23 : 59	00 : 00	00 : 00	00 : 00	00 : 00	☑
Tuesday	00 : 00	23 : 59	00 : 00	00 : 00	00 : 00	00 : 00	☑
Wednesday	00 : 00	23 : 59	00 : 00	00 : 00	00 : 00	00 : 00	☑
Thursday	00 : 00	23 : 59	00 : 00	00 : 00	00 : 00	00 : 00	☑
Friday	00 : 00	23 : 59	00 : 00	00 : 00	00 : 00	00 : 00	☑
Saturday	00 : 00	23 : 59	00 : 00	00 : 00	00 : 00	00 : 00	☐
Sunday	00 : 00	23 : 59	00 : 00	00 : 00	00 : 00	00 : 00	☐
Values for selected days	00 : 00	23 : 59	00 : 00	00 : 00	00 : 00	00 : 00	

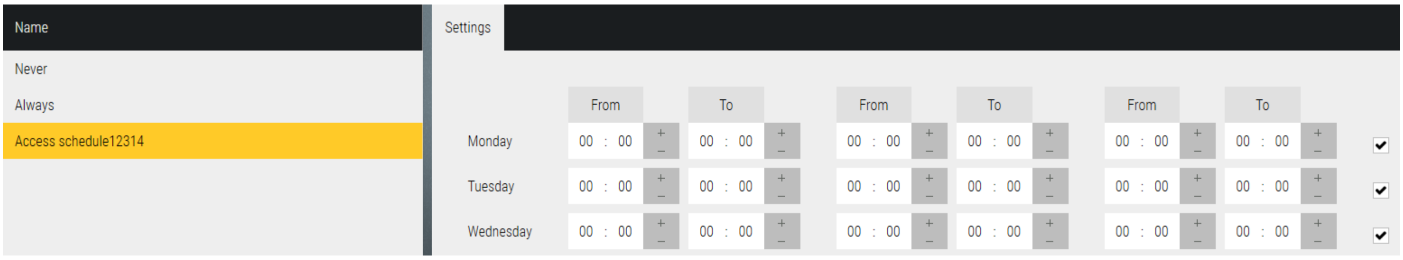
To add a new schedule, click on the *Add* button in the lower left corner of the screen. You can change the default name on the yellow box to your own.

Then, type the start and end time of the schedule activity for each day of the week. Two additional time columns allow you to define a schedule consisting of two or three time intervals in a day or passing through the midnight e.g. from 10 p.m. to 6 a.m. (22:00-23:59, 00:00-06:00).

If the schedule activity hours repeat for several days (e.g. Monday to Friday), you can select them in the right column and then enter the required settings in the bottom row. When you click the *Set for selected* button, the fields above in the selected rows are filled by the bottom row. This functionality greatly accelerates the definition of new schedules.

To edit the bottom row, select at least one day in the right column.

You can edit or delete a defined schedule by selecting it in the list and clicking the *Delete* button in the lower left corner of the window.

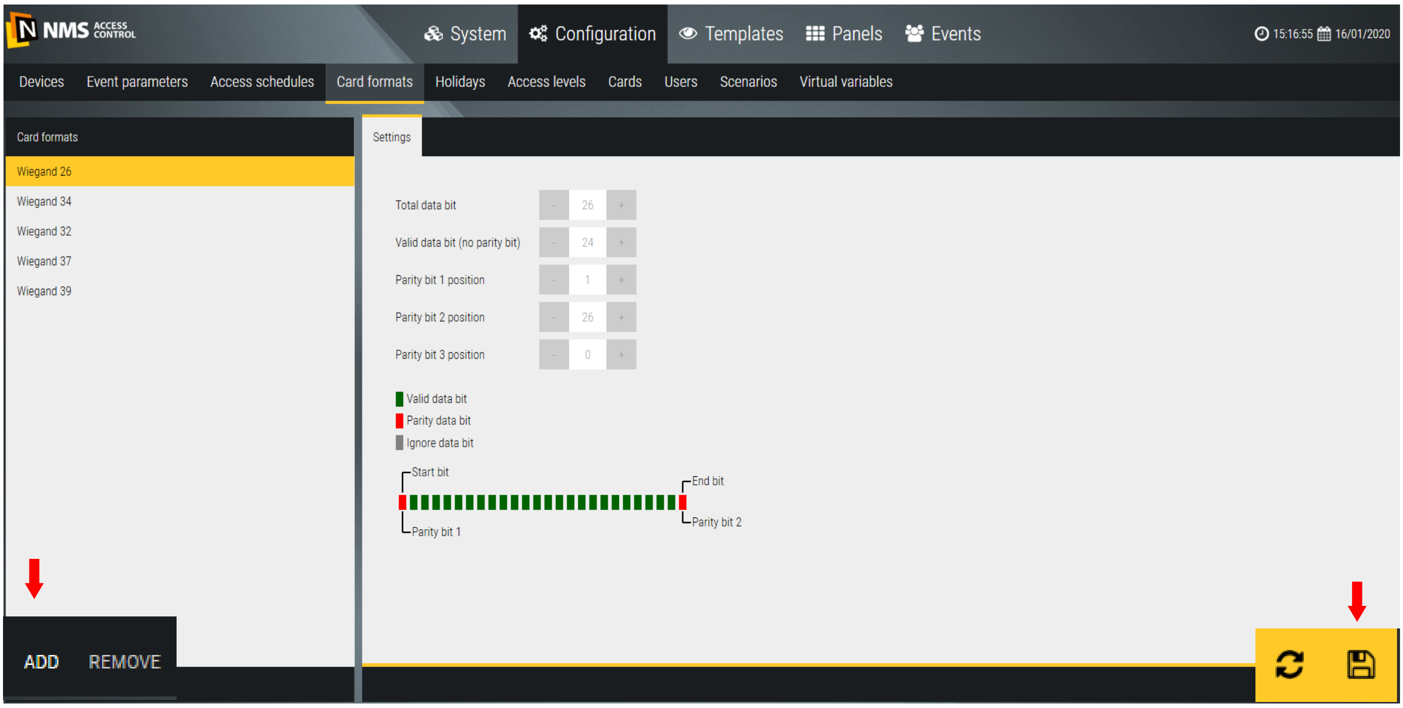


Name
Never
Always
Access schedule12314

	From	To	From	To	From	To	
Monday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	☑
Tuesday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	☑
Wednesday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	☑

3.16 Card formats

This tab allows you to define a new format for reading cards by the reader connected to the controller, when none of the existing ones in the list match. 30XX series controllers support Wiegand formats up to 40 bits. This number contains parity bits if used.



Total data bit - 26 +

Valid data bit (no parity bit) - 24 +

Parity bit 1 position - 1 +

Parity bit 2 position - 26 +

Parity bit 3 position - 0 +

🟩 Valid data bit
🟥 Parity data bit
▨ Ignore data bit

To add a new card format, click on the *Add* button - left bottom corner.

Name - an editable field in the left window to type the name of the new format in place of the default name.

Total data bits - a field for entering the number of data bits to be sent from the reader to the controller after reading the card.

Important data bits (no parity bits) - a field for entering the number of data bits in the string to be transmitted which contain the correct card number, usually the one printed on the card. Example often for the HID format Wiegand 26 The number printed on the card is 16 bit, and this value should be set in this field if you want the program to display the printed number.

The position of the 1st parity bit - usually at position 1 in the string and is called the startup bit. Its value (0 or 1) is calculated as a checksum of the following bit string. The number of bits as it is taken into account depends on the format and algorithm adopted. The controller should implement an algorithm to validate the transmission correctness by calculating the bit value from the received string (from pos. 2) and comparing it to the bit value on the pos. 1 in the received bit string from the reader.

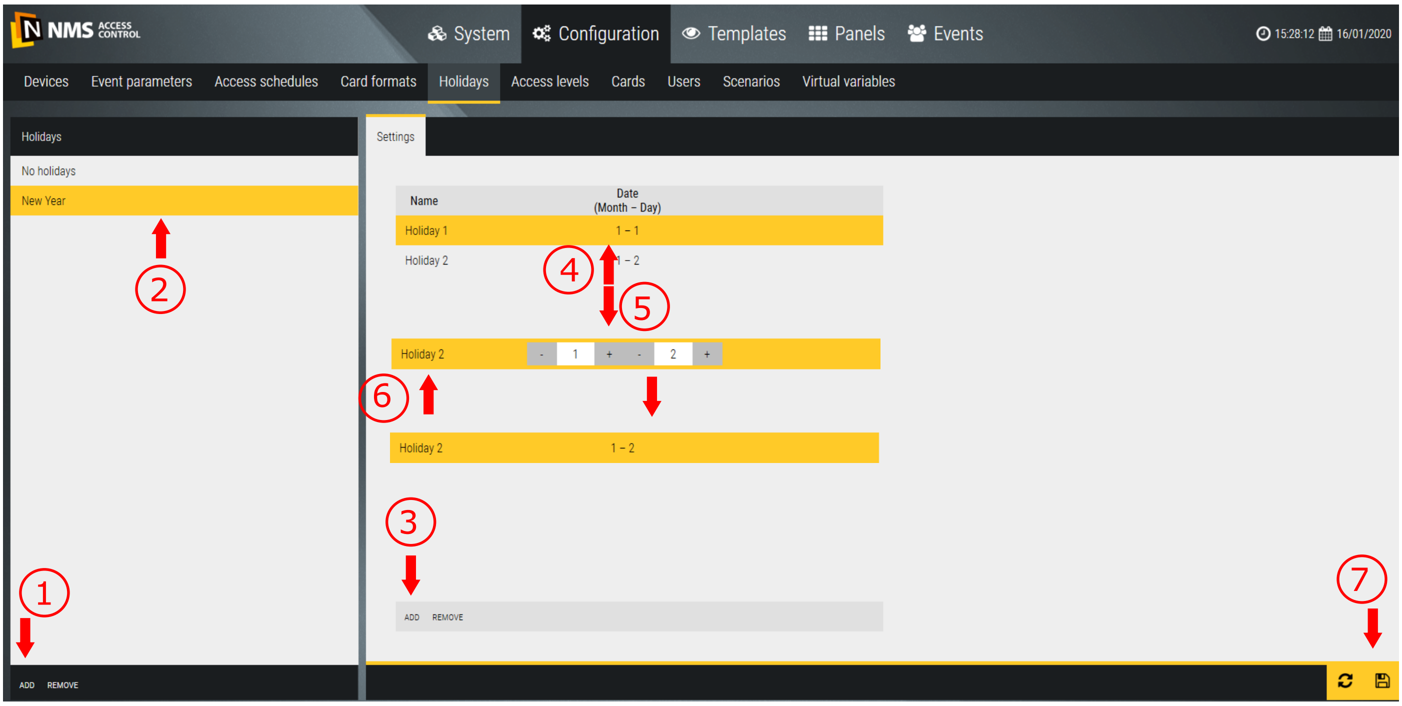
The position of the 2nd parity bit - usually at the last position in the string and is called the stop bit. Its value (0 or 1) is calculated as the checksum of the preceding bit string. Verification in the controller is similar to the start bit.

Bit 3 is rarely used. Parity and odd bits are used to control the correctness of the transmission between the reader and the controller.

The defined card formats are listed in the field in the controller settings - *Wiegand Format.*

Save settings with click the floppy disk icon in the lower-right corner.

3.17 Holidays



This tab allows you to define special holidays that fall on weekdays other than Saturday and Sunday. This allows you to change the system operation on such days to another mode. This is especially true for access levels and e.g. schedules that control the automatic unlocking of the door.

To add a new holiday day, click on the *Add* button - bottom left corner.

Name - editable field in the left window to type the name of the new holiday day in place of the default name.

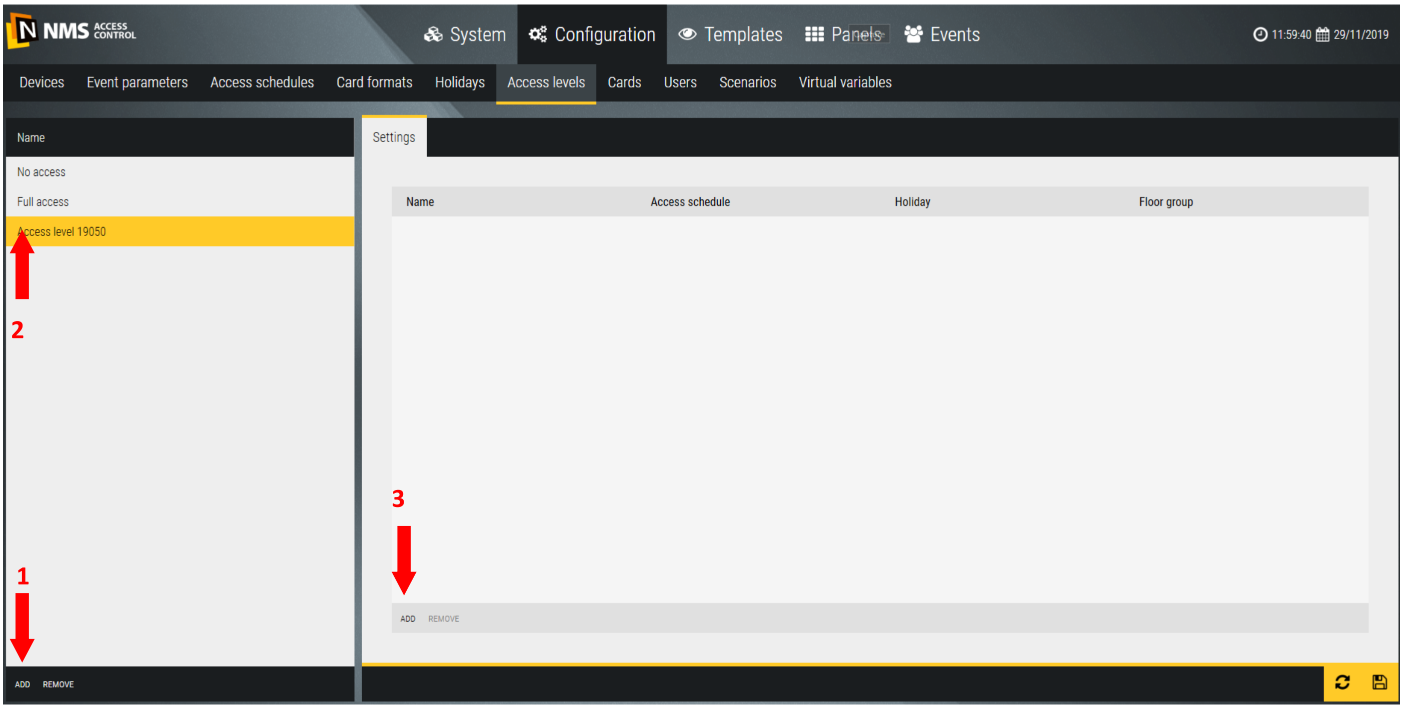
Settings - when new holiday period is added to the left window, in the right window you have to define days by the date you want to include this period. Each holiday period may cover more than one day, although it is usually one day.

When you click *Add* in the right window, a yellow bar with date 1-1 (represents 1st of January) appears.

To set the correct date for the holiday, click in the date field. Editable fields are displayed to set the month and day.

Save settings by clicking the floppy disk icon in the lower-right corner.

3.18 Access levels



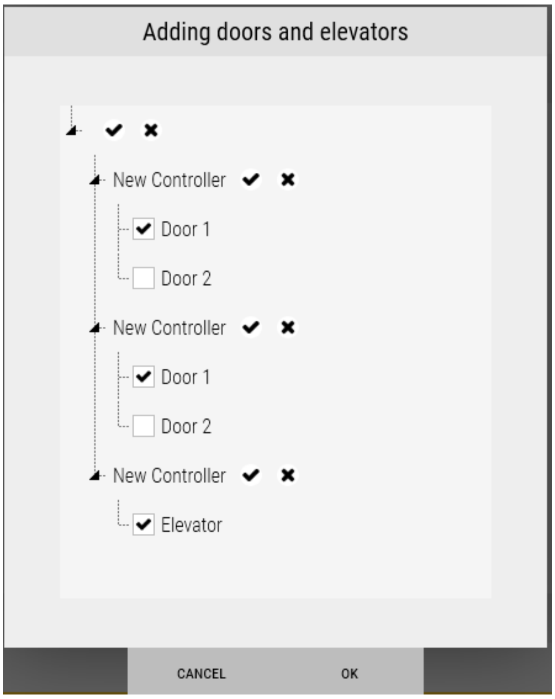
Use the *Access levels* tab to define access levels for card users. The access level is a set of permissions that determines which transitions and how long a user will have access.

By default, two access levels are defined: *No access* and *Full access that* can not be deleted or edited.

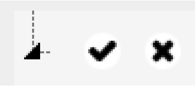
To add a new access level click on the *Add* button in the lower left corner of the screen. You can change the default name on the yellow box to your own.

Then click on the *Add* button in the right window.

A window with a list of all previously added doors and elevators will be displayed.

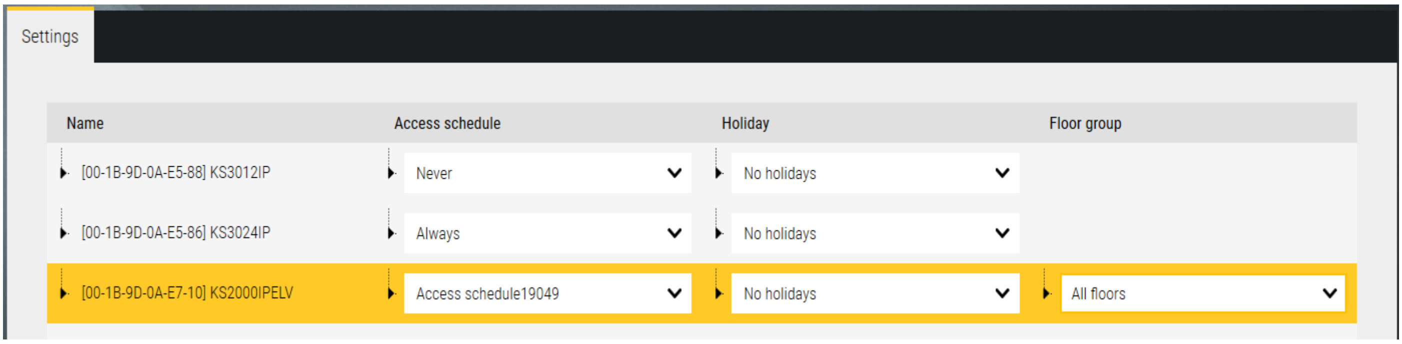


Select the doors and elevators (as readers in the cabin) to which the user will have access rights over a specified period of time and confirm with the OK button.



ChecCheckboxes as above allow you to quickly select and deselect all items.

In the right window appears a table as below, containing the selected doors and elevators in the previous window.



Name	Access schedule	Holiday	Floor group
[00-1B-9D-0A-E5-88] KS3012IP	Never	No holidays	
[00-1B-9D-0A-E5-86] KS3024IP	Always	No holidays	
[00-1B-9D-0A-E7-10] KS2000IPELV	Access schedule19049	No holidays	All floors

In the second column (*Access schedule)* in the drop down list, select the schedule according to the expected access permissions.

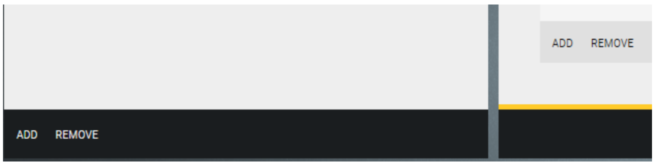
In the third column (*Holiday)* in the drop-down list, select the holiday schedule according to the expected access rights.

In the fourth column (*Group of floors)* in the drop down list, select a group of floors according to the expected access privileges.

Save the settings by clicking on the floppy disk icon in the lower right corner of the configuration window.

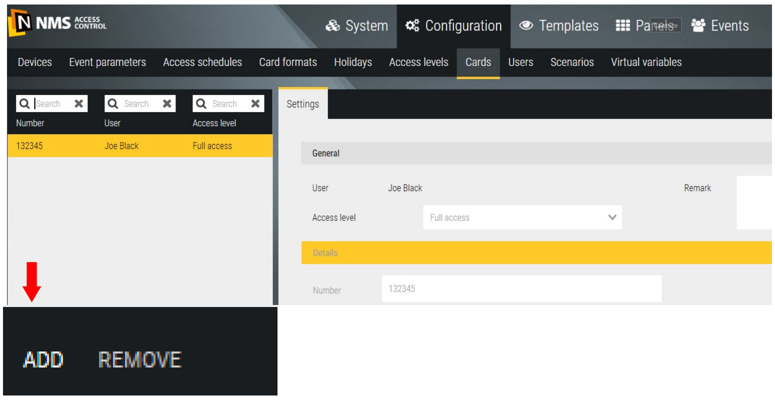
Access levels defined this way can be assigned to one or more users.

Delete button at the bottom of the left window is used to delete the entire access level, and in the right to erase one row of selected door or elevator.



3.19 Cards

This tab allows you to create a list of cards with numbers for later and faster assignment to users.



Number	User	Access level
132345	Joe Black	Full access

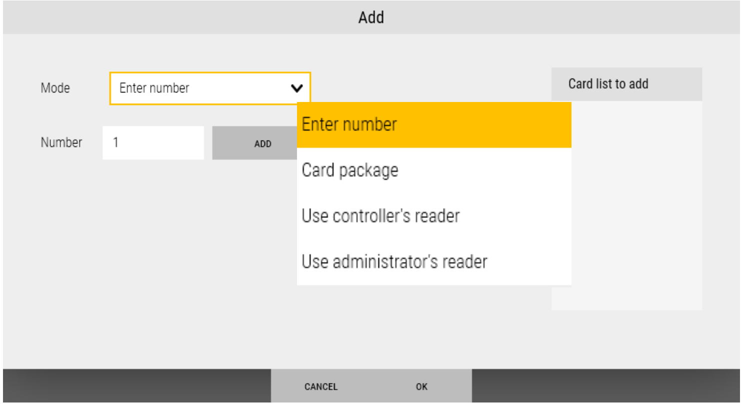
User: Joe Black

Remark:

Access level: Full access

Number: 132345

When you click on the *Add* button a window is displayed as below:

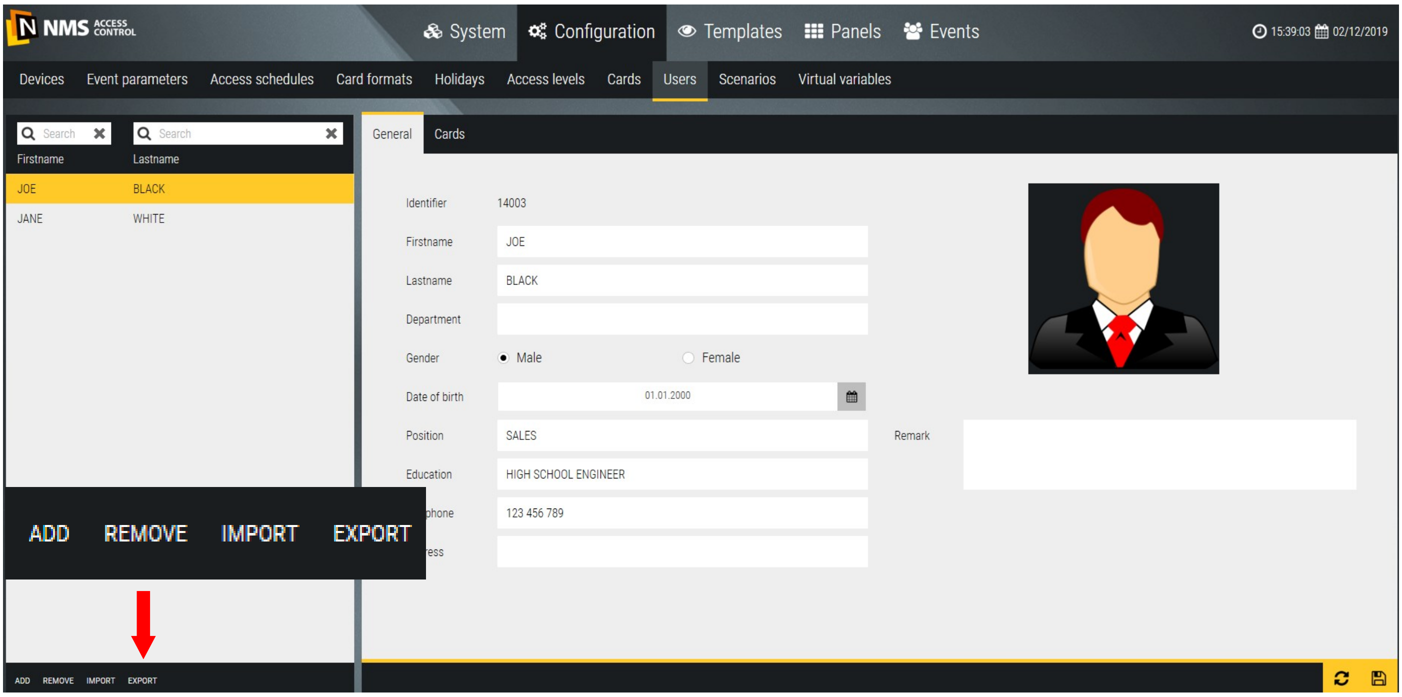


Mode: Enter number

Number: 1

The procedure for adding cards is described in section 4.4 - *Users/Cards.*

3.20 Users

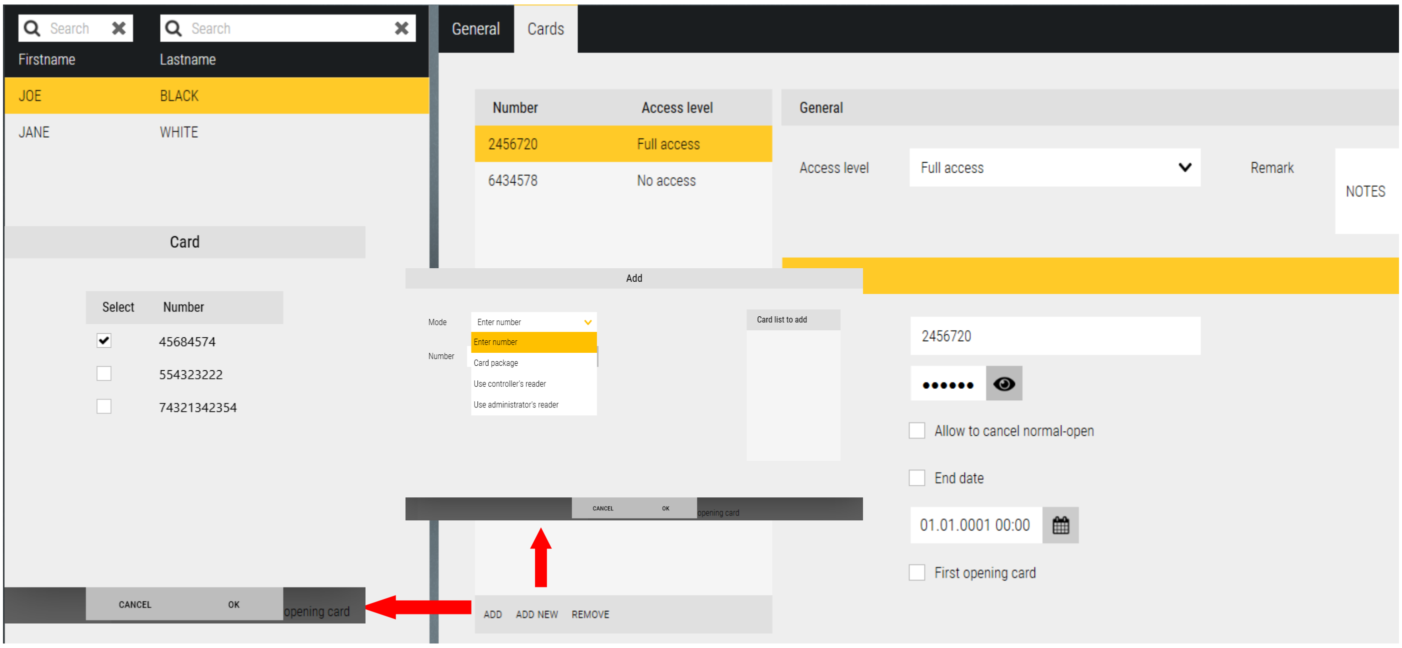


Firstname	Lastname
JOE	BLACK
JANE	WHITE

Identifier	14003
Firstname	JOE
Lastname	BLACK
Department	
Gender	● Male ○ Female
Date of birth	01.01.2000
Position	SALES
Education	HIGH SCHOOL ENGINEER
phone	123 456 789
ress	
Remark	

Users can be added manually or by importing data from a file. File **import procedure** significantly accelerates this process for a large quantity of cards. If the window is empty then click on the *Export* button. The exported file (*csv users*) contains two example rows. For new users, the ID column should be empty. The order of the columns in the imported file must be the same as the exported one. If after the first import we want to continue to work on such a file (i.e. change parameters of previously added users or add new ones), it is always necessary to export the current database first and work on such a file.

To add a user manually click on the *Add* button in the lower left corner of the window (to delete, select and click *Delete).* Then fill in the form fields in the right window. Except the name and last name fields, the remaining fields are not obligatory. You can also add a user photo from a file by clicking on the black box. The left window displays a list of added users. To assign a card number to a user, go to the *Cards* tab. The program will display the window as below:



Firstname	Lastname
JOE	BLACK
JANE	WHITE

Select	Number
☑	45684574
□	554323222
□	74321342354

Number	Access level
2456720	Full access
6434578	No access

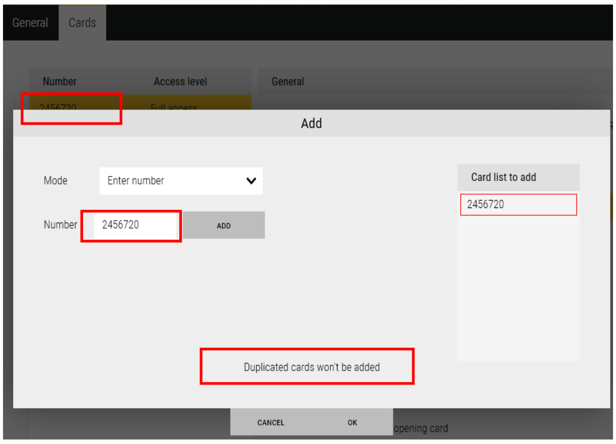
Access level	Full access
Remark	NOTES
	2456720
	••••••
□ Allow to cancel normal-open	
□ End date	01.01.0001 00:00
□ First opening card	

In the window on the previous page we have two ways to assign a new card to the user. User can have more than one card (max. 5).

After clicking on the *Add* button a window pops up as on the left side with a list of cards added earlier through the *Cards* tab. Select the card numbers that you want to assign to the user.

After clicking on the *Add new* button window pops up as on the right. In this window you can select one of four options to enter the card number into the list:

- Manually enter a number in the editable field (when we know the card number)
  The number entered is subject to verification if it already exists in the database, it is highlighted in red and cannot be added.

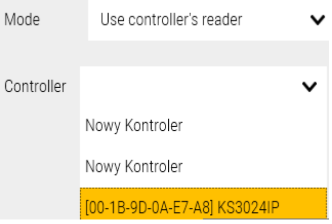


Mode: Enter number

Number: 2456720

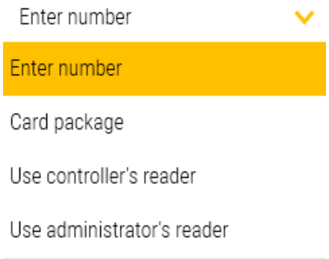
Card list to add: 2456720

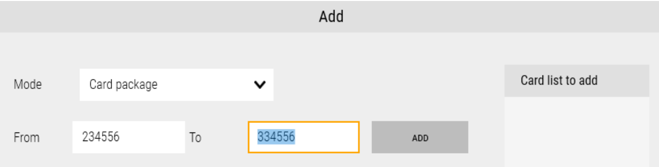
Duplicated cards won't be added



Mode: Use controller's reader

Controller

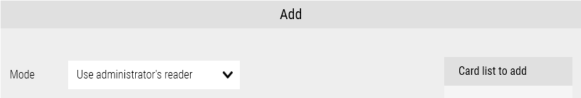




Mode: Card package

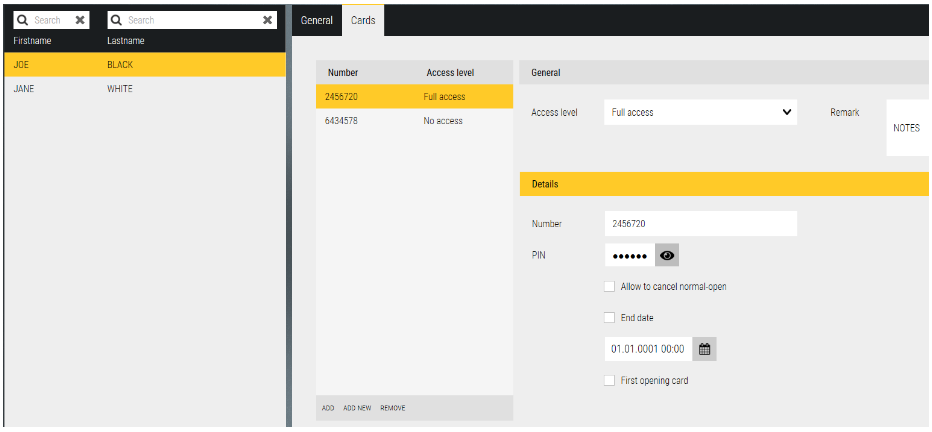
From: 234556 To: 334556

- Manually enter the first number from the card container (consecutive pack) and the final
- Reading the card on the controllers' reader
- By USB administrator reader



Mode: Use administrator's reader

After adding the card numbers to the list, return to the *Users/Cards* tab*,* which now looks like the following.



Firstname	Lastname
JOE	BLACK
JANE	WHITE

Number	Access level
2456720	Full access
6434578	No access

Access level: Full access

Number: 2456720

PIN: ••••••

□ Allow to cancel normal-open

□ End date

01.01.0001 00:00

□ First opening card

Each card has a separate menu on the right side of the window that appears when you select a card in the list. Deleting a card from this list does not remove it from the system. To remove it from, go to the *Cards* tab.

Access level - select from the drop-down list

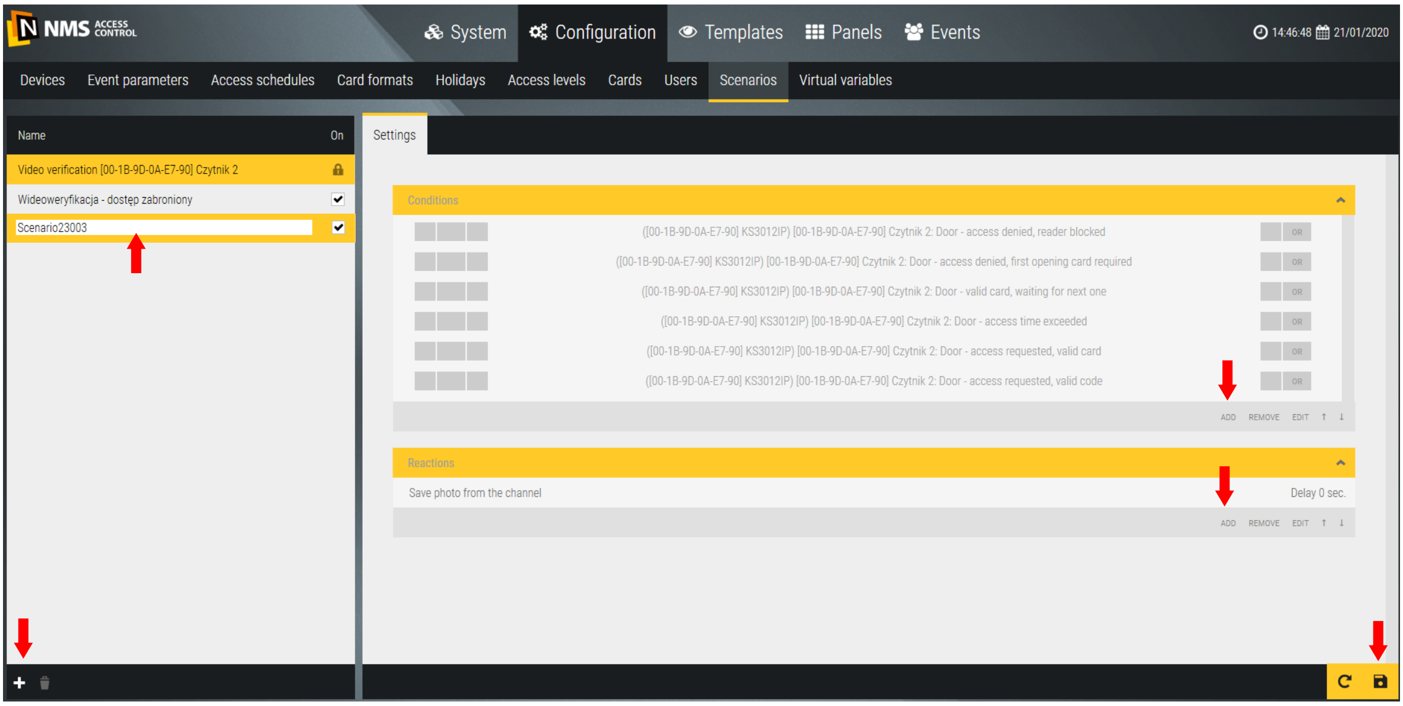
PIN - editable field to enter the passcode associated with this card (6 digits)

Allow to cancel normal-open - option for the user to lock the door opened by schedule after double reading this card. Return the door to the schedule by single reading this card.

End Date - when selected, set the required date, enter or select from the calendar

First opening card - the option required for the user when it has to be able to unlock access for other users without this permission. Active on readers with this option enabled.

3.20 Scenarios



Video verification [00-1B-9D-0A-E7-90] Czytnik 2

Wideoweryfikacja - dostęp zabroniony ☑

Scenario23003 ☑

Conditions

([00-1B-9D-0A-E7-90] KS3012IP) [00-1B-9D-0A-E7-90] Czytnik 2: Door - access denied, reader blocked OR

([00-1B-9D-0A-E7-90] KS3012IP) [00-1B-9D-0A-E7-90] Czytnik 2: Door - access denied, first opening card required OR

([00-1B-9D-0A-E7-90] KS3012IP) [00-1B-9D-0A-E7-90] Czytnik 2: Door - valid card, waiting for next one OR

([00-1B-9D-0A-E7-90] KS3012IP) [00-1B-9D-0A-E7-90] Czytnik 2: Door - access time exceeded OR

([00-1B-9D-0A-E7-90] KS3012IP) [00-1B-9D-0A-E7-90] Czytnik 2: Door - access requested, valid card OR

([00-1B-9D-0A-E7-90] KS3012IP) [00-1B-9D-0A-E7-90] Czytnik 2: Door - access requested, valid code OR

Reactions

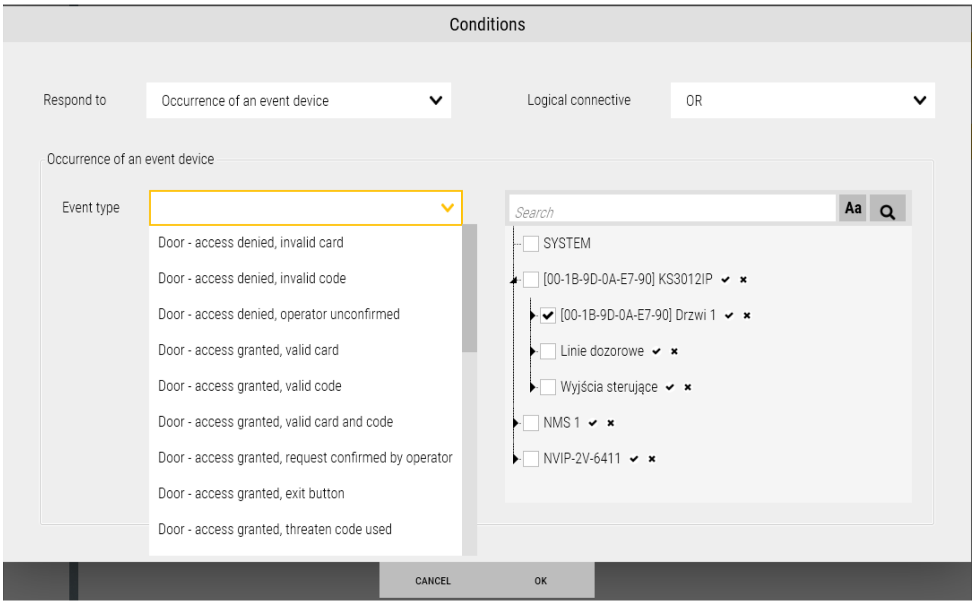
Save photo from the channel Delay 0 sec.

This tab allows you to define scenarios that can perform automatically selected processes e.g. generate an automatic event report, display the camera image after reading the card, etc. This option is very flexible and allows you to define many different actions and reactions.

To add a new scenario, click on the *Add* button - bottom left corner.

Name - editable field to type the name of the scenario in place of the default name.

Conditions - a window for selecting a condition that must occur to run the scenario. You can add more than one condition with a conjunction and/or.



Conditions

Respond to: Occurrence of an event device

Logical connective: OR

Occurrence of an event device

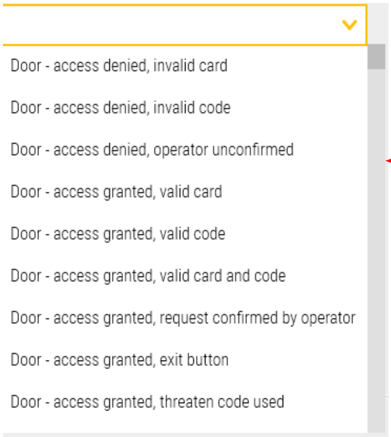
Event type:

- Door - access denied, invalid card
- Door - access denied, invalid code
- Door - access denied, operator unconfirmed
- Door - access granted, valid card
- Door - access granted, valid code
- Door - access granted, valid card and code
- Door - access granted, request confirmed by operator
- Door - access granted, exit button
- Door - access granted, threaten code used

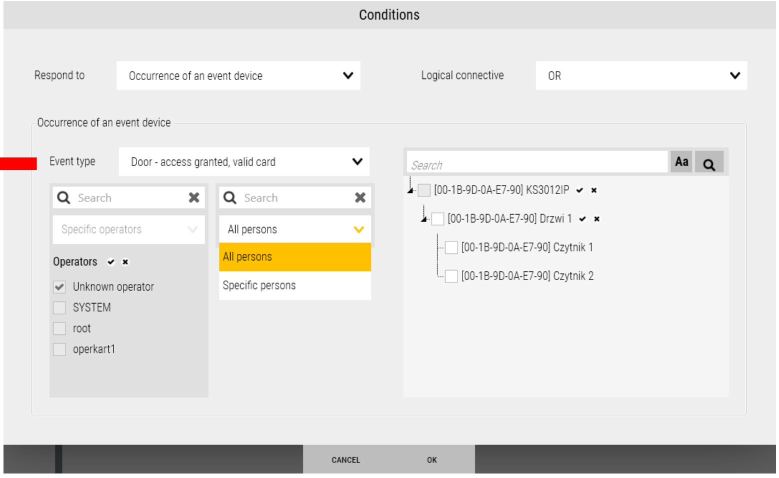
□ SYSTEM
□ [00-1B-9D-0A-E7-90] KS3012IP ✔ ✖
☑ [00-1B-9D-0A-E7-90] Drzwi 1 ✔ ✖
□ Linie dozorowe ✔ ✖
□ Wyjścia sterujące ✔ ✖
□ NMS 1 ✔ ✖
□ NVIP-2V-6411 ✔ ✖

When you click on the *Add* button in the *Conditions* section, expand *Respond to.* Depending on the selected item, different options will be displayed below.

When you click on the *Add* button in the *Conditions* section, expand *Respond to* list. Depending on the selected item, different options will be displayed below. For the most commonly used condition, *Occurrence of device event* you can see options like in the window below.



- Door - access denied, invalid card
- Door - access denied, invalid code
- Door - access denied, operator unconfirmed
- Door - access granted, valid card
- Door - access granted, valid code
- Door - access granted, valid card and code
- Door - access granted, request confirmed by operator
- Door - access granted, exit button
- Door - access granted, threaten code used



Conditions

Respond to: Occurrence of an event device

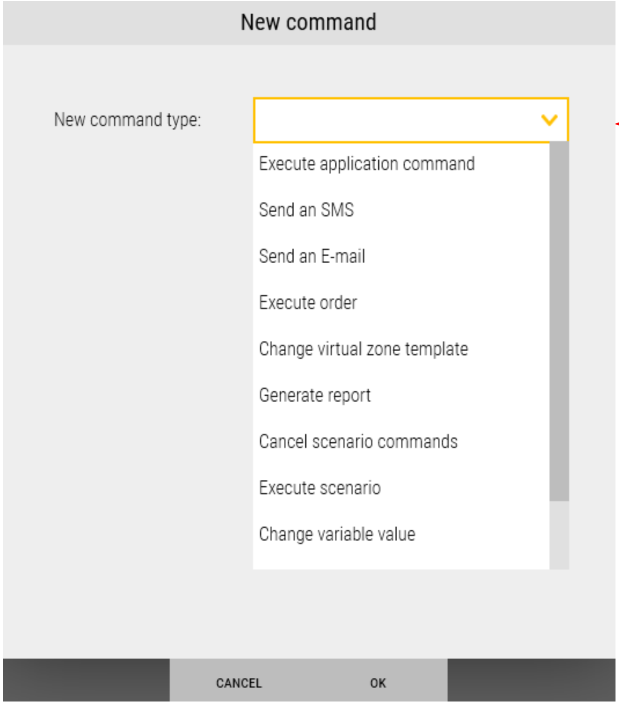
Logical connective: OR

Occurrence of an event device

Event type: Door - access granted, valid card

In this case, select the event, the user whose card reading on the selected to the right door has to initiate the scenario. This allows you to set the condition very precisely. It looks similarly for the other conditions in the list. Of course, you must define the selected elements of the system first to display the options below e.g. schedules, triggers or virtual variables.

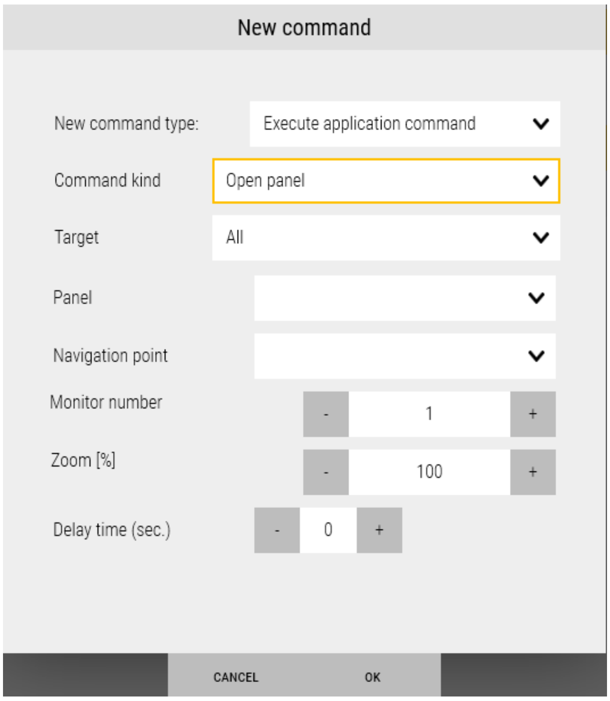
<u>Reactions</u> - a window for selecting reactions to conditions defined above.



New command

New command type:

- Execute application command
- Send an SMS
- Send an E-mail
- Execute order
- Change virtual zone template
- Generate report
- Cancel scenario commands
- Execute scenario
- Change variable value



New command

New command type: Execute application command

Command kind: Open panel

Target: All

Panel:

Navigation point:

Monitor number: 1

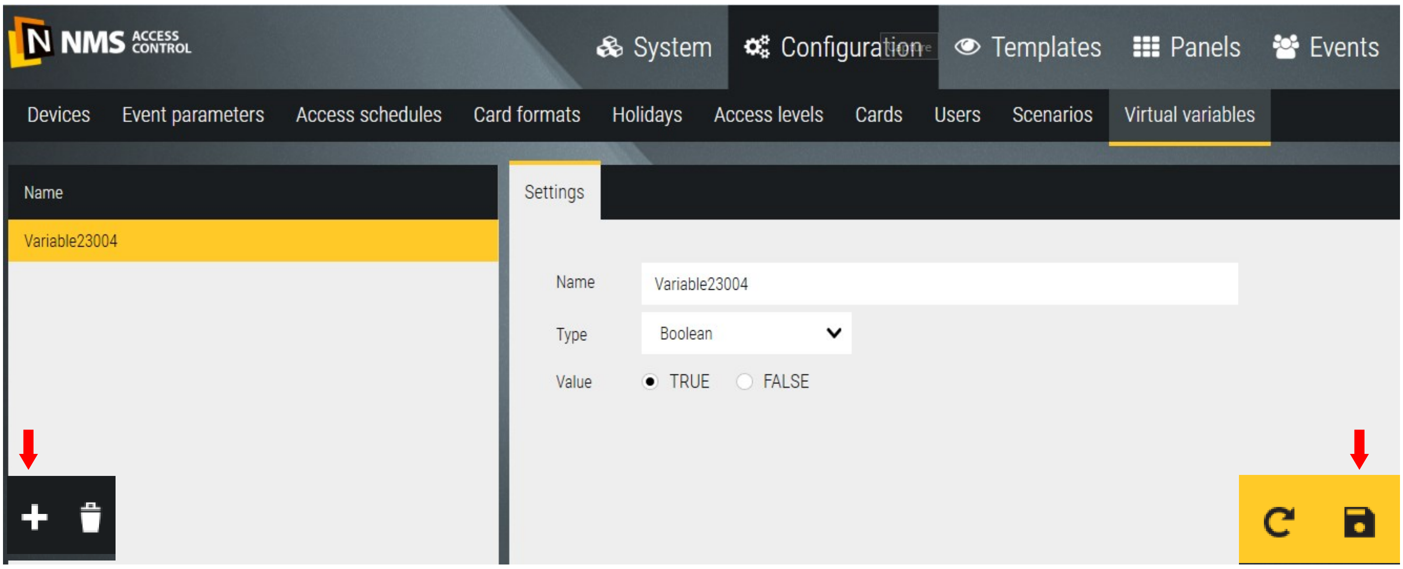
Zoom [%]: 100

Delay time (sec.): 0

In the response window *New command* set the parameters. The appearance of the window varies depending on the selected command.

Save settings by clicking the floppy disk icon in the lower-right corner.

3.21 Virtual Variables



Name
Variable23004

Name: Variable23004

Type: Boolean

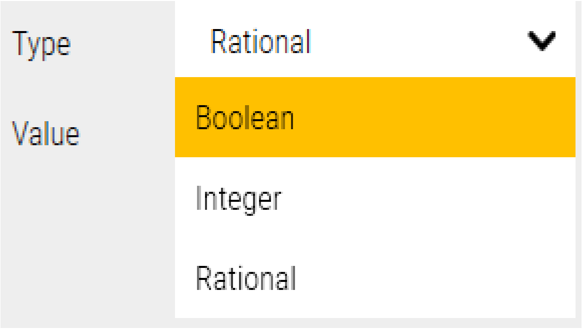
Value: ● TRUE ○ FALSE

This tab allows you to define virtual variables that are used to control selected functions, events and scenarios.

To add a new virtual variable, click on the *Add* button - left corner.

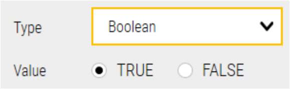
Name - editable field in the right window to type the name of the new variable in place of the default name.

Type - drop-down list of variable type selection:



Value:

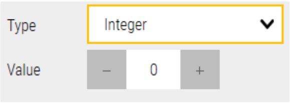
- *Boolean* - to selections one of the options: *true* or *false*



Type: Boolean

Value: ● TRUE ○ FALSE

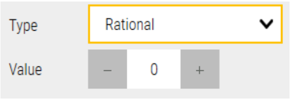
- *Integer number* - editable field to set the value



Type: Integer

Value: – 0 +

- *Rational number* - editable field to set the value



Type: Rational

Value: – 0 +

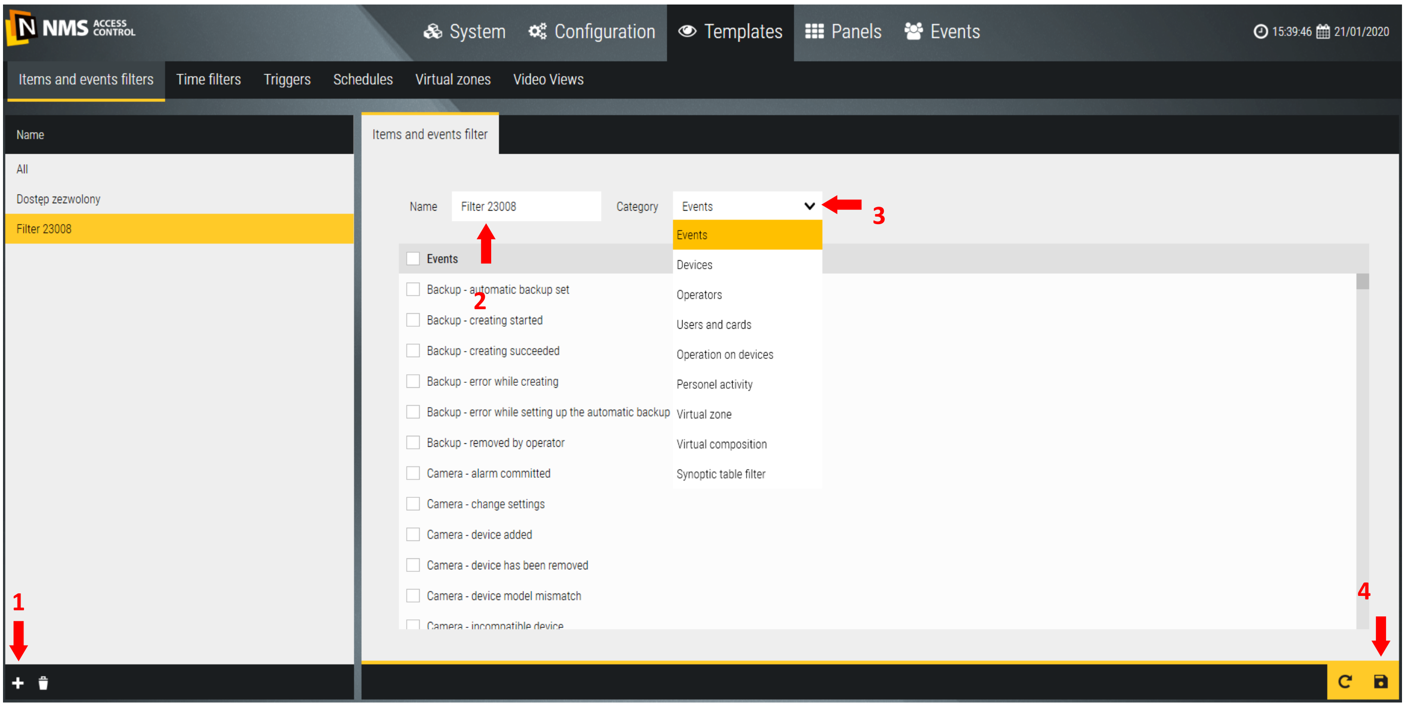
Save settings by clicking the floppy disk icon in the lower-right corner.

Section 4 Templates

In the *Templates* tab, you can define element and event filters, time filters, triggers, schedules and virtual zones. These are logical elements of the system used in various places of the program. For example, element and event filters are used in the process of generating event reports.

4.1 Element and event filters

Use this tab to define element and event filters for different categories.



Name

All

Dostęp zezwolony

Filter 23008

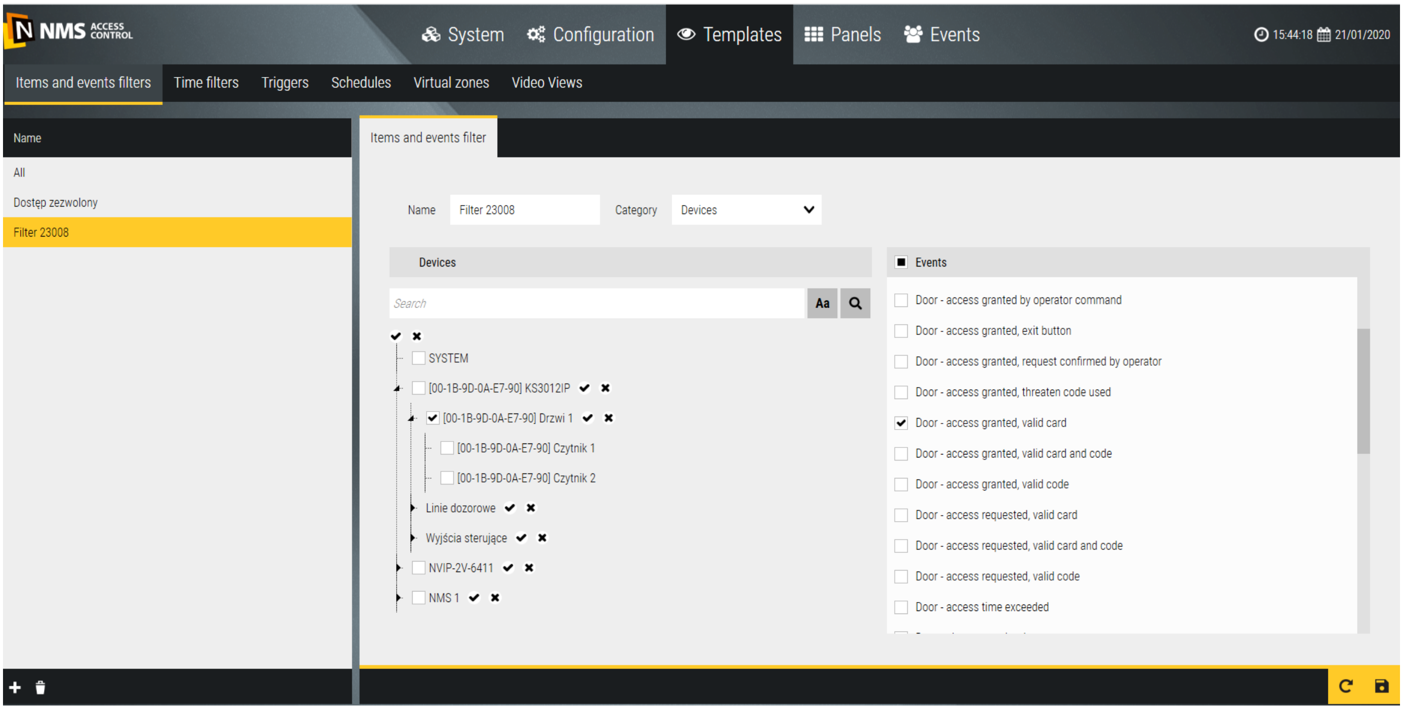
Name: Filter 23008 Category: Events

Categories: Events, Devices, Operators, Users and cards, Operation on devices, Personel activity, Virtual zone, Virtual composition, Synoptic table filter

□ Events

□ Backup - automatic backup set
□ Backup - creating started
□ Backup - creating succeeded
□ Backup - error while creating
□ Backup - error while setting up the automatic backup
□ Backup - removed by operator
□ Camera - alarm committed
□ Camera - change settings
□ Camera - device added
□ Camera - device has been removed
□ Camera - device model mismatch
□ Camera - incompatible device

When you click the *Add* button *(1)* , the editable *Name (2)* field and the *Category (3)* drop-down box are displayed in the right window. When you select a filter category, set its parameters. Here's an example when you select *Device* category. The right window displays the events that are selected in the middle column of elements.



Name

All

Dostęp zezwolony

Filter 23008

Name: Filter 23008 Category: Devices

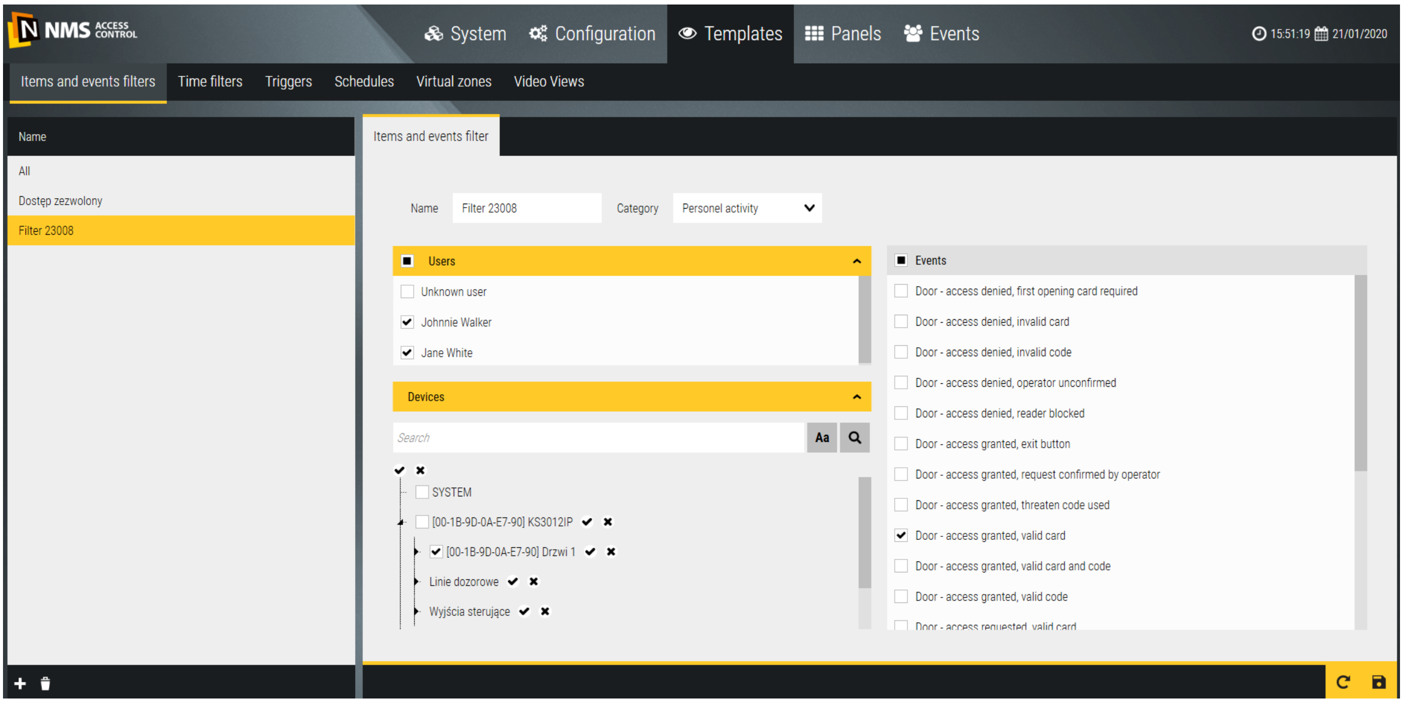
Devices

- □ SYSTEM
- □ [00-1B-9D-0A-E7-90] KS3012IP ✔ ✖
  - ☑ [00-1B-9D-0A-E7-90] Drzwi 1 ✔ ✖
    - □ [00-1B-9D-0A-E7-90] Czytnik 1
    - □ [00-1B-9D-0A-E7-90] Czytnik 2
  - Linie dozorowe ✔ ✖
  - Wyjścia sterujące ✔ ✖
- □ NVIP-2V-6411 ✔ ✖
- □ NMS 1 ✔ ✖

■ Events

□ Door - access granted by operator command
□ Door - access granted, exit button
□ Door - access granted, request confirmed by operator
□ Door - access granted, threaten code used
☑ Door - access granted, valid card
□ Door - access granted, valid card and code
□ Door - access granted, valid code
□ Door - access requested, valid card
□ Door - access requested, valid card and code
□ Door - access requested, valid code
□ Door - access time exceeded

Another example when you select the *Personal activity* category. The right window displays the events that are selected in the middle column of items. In this case, users of cards and doors/readers on which they used cards.



Name
- All
- Dostęp zezwolony
- Filter 23008

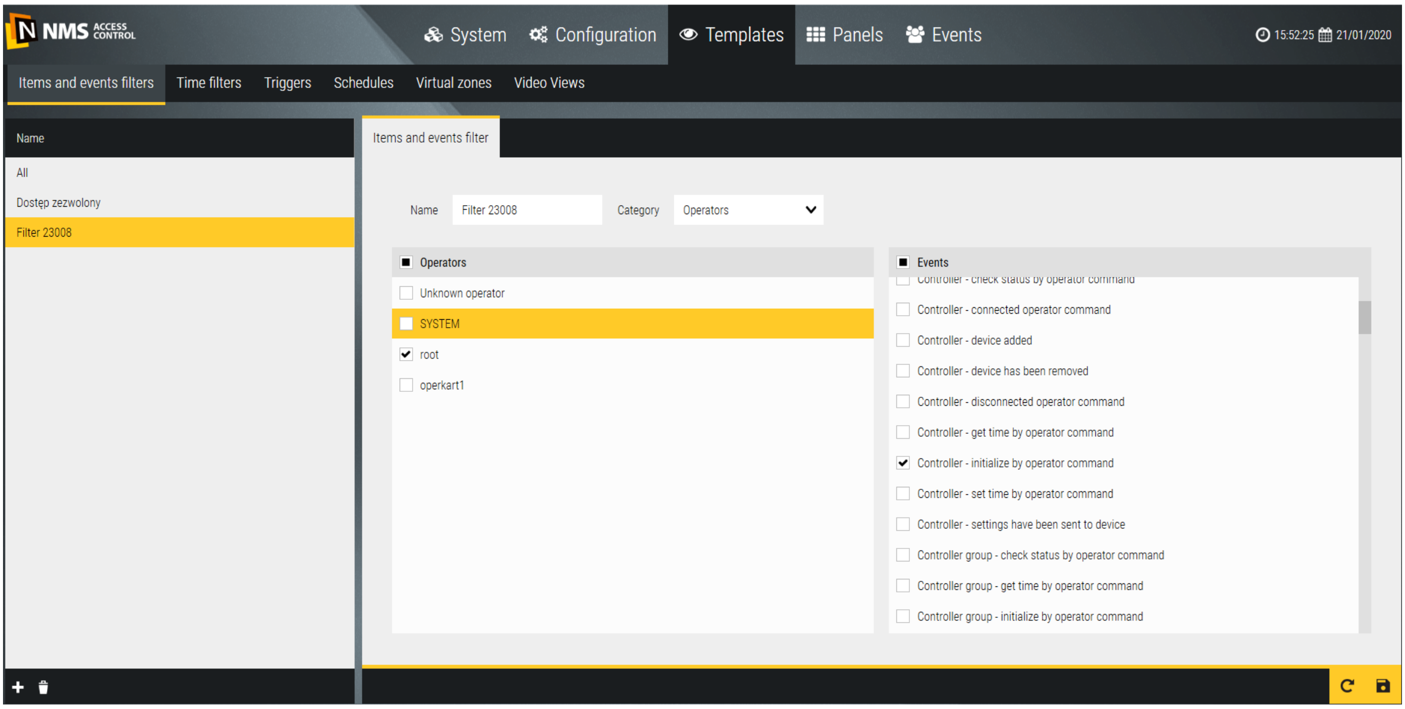
Name: Filter 23008 Category: Personel activity

Users
- □ Unknown user
- ☑ Johnnie Walker
- ☑ Jane White

Devices
- □ SYSTEM
- □ [00-1B-9D-0A-E7-90] KS3012IP ✓ ✖
- ☑ [00-1B-9D-0A-E7-90] Drzwi 1 ✓ ✖
- Linie dozorowe ✓ ✖
- Wyjścia sterujące ✓ ✖

Events
- □ Door - access denied, first opening card required
- □ Door - access denied, invalid card
- □ Door - access denied, invalid code
- □ Door - access denied, operator unconfirmed
- □ Door - access denied, reader blocked
- □ Door - access granted, exit button
- □ Door - access granted, request confirmed by operator
- □ Door - access granted, threaten code used
- ☑ Door - access granted, valid card
- □ Door - access granted, valid card and code
- □ Door - access granted, valid code
- □ Door - access requested, valid card

Another example after selecting the *Operators* category. The right window displays the events that are selected in the middle column of items. In this case, the operation according to operators.



Name
- All
- Dostęp zezwolony
- Filter 23008

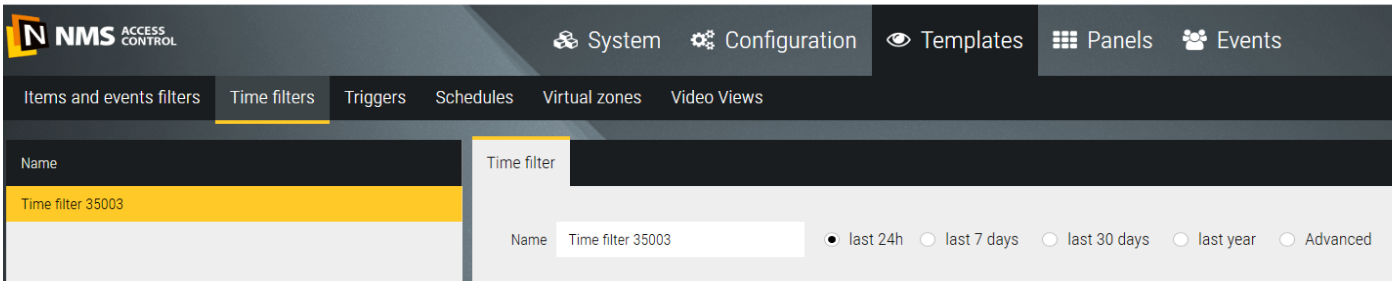
Name: Filter 23008 Category: Operators

Operators
- □ Unknown operator
- □ SYSTEM
- ☑ root
- □ operkart1

Events
- Controller - check status by operator command
- □ Controller - connected operator command
- □ Controller - device added
- □ Controller - device has been removed
- □ Controller - disconnected operator command
- □ Controller - get time by operator command
- ☑ Controller - initialize by operator command
- □ Controller - set time by operator command
- □ Controller - settings have been sent to device
- □ Controller group - check status by operator command
- □ Controller group - get time by operator command
- □ Controller group - initialize by operator command

4.2 Time filters

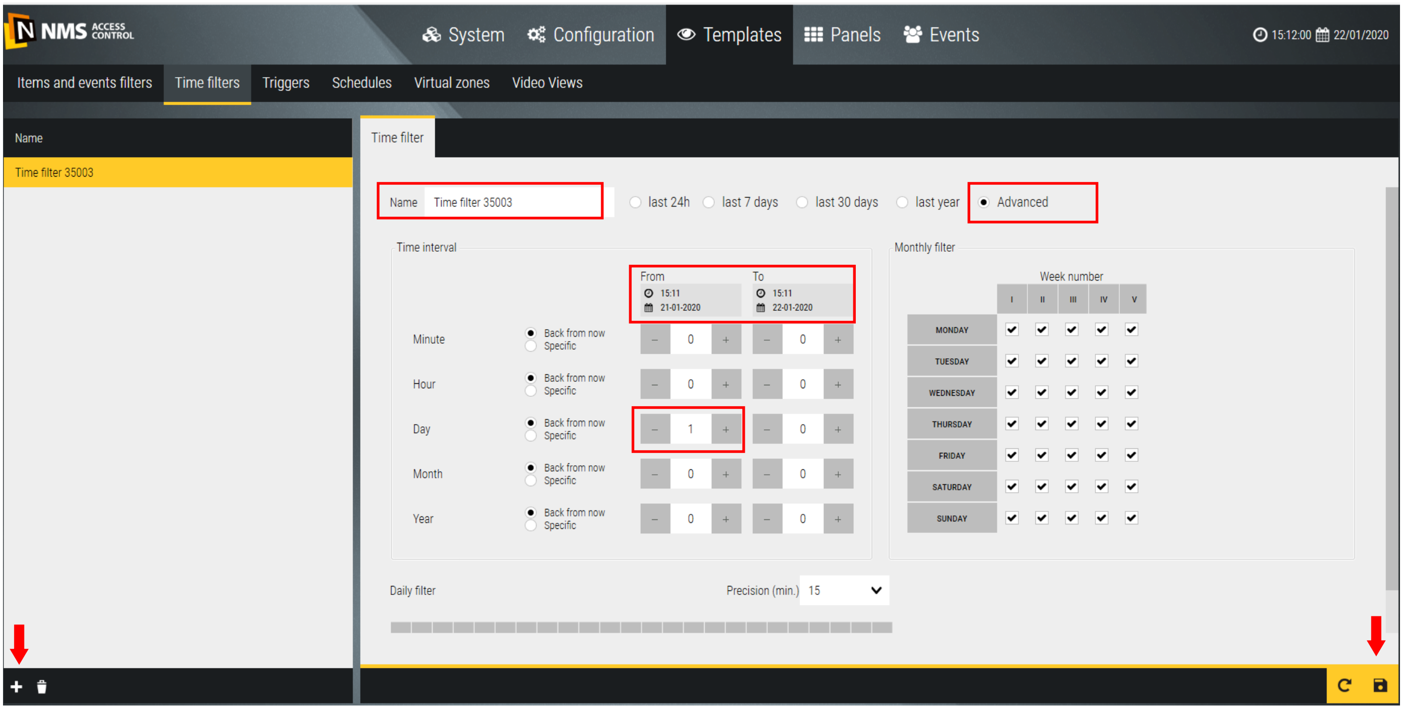
This tab allows you to define time filters that, like element and event filters, are used in the process of generating event reports. In a simple version, the filter may include the last day, last week, last month or last year. To add a new time filter, click on the *Add* button - bottom left corner.



Name
Time filter 35003

Name: Time filter 35003 ● last 24h ○ last 7 days ○ last 30 days ○ last year ○ Advanced

In the advanced version you have much more settings.



Name
Time filter 35003

Name: Time filter 35003 ○ last 24h ○ last 7 days ○ last 30 days ○ last year ● Advanced

Time interval

From: 15:11 21-01-2020 To: 15:11 22-01-2020

		From	To
Minute	● Back from now ○ Specific	0	0
Hour	● Back from now ○ Specific	0	0
Day	● Back from now ○ Specific	1	0
Month	● Back from now ○ Specific	0	0
Year	● Back from now ○ Specific	0	0

Monthly filter

Week number	I	II	III	IV	V
MONDAY	✓	✓	✓	✓	✓
TUESDAY	✓	✓	✓	✓	✓
WEDNESDAY	✓	✓	✓	✓	✓
THURSDAY	✓	✓	✓	✓	✓
FRIDAY	✓	✓	✓	✓	✓
SATURDAY	✓	✓	✓	✓	✓
SUNDAY	✓	✓	✓	✓	✓

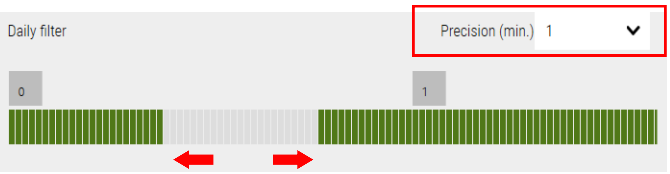
Daily filter Precision (min.) 15

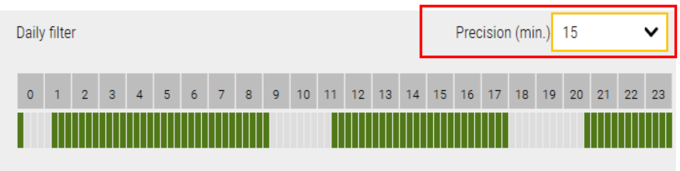
You can set the time intervals for each day of the week in different ways, with the specified accuracy in the day. In *From/To* fields current time interval setting is displayed.

Time interval - has two options: *Back from now* and *Specific.* By setting the appropriate values, you can select any time period from the past.

Monthly filter - includes the whole month, divided into weeks (I-V) and days of the week. Allows you to limit the time interval you set earlier to only certain days of the week. You can uncheck/select the entire row by clicking on the weekday name. Uncheck causes events that are not included in the report.

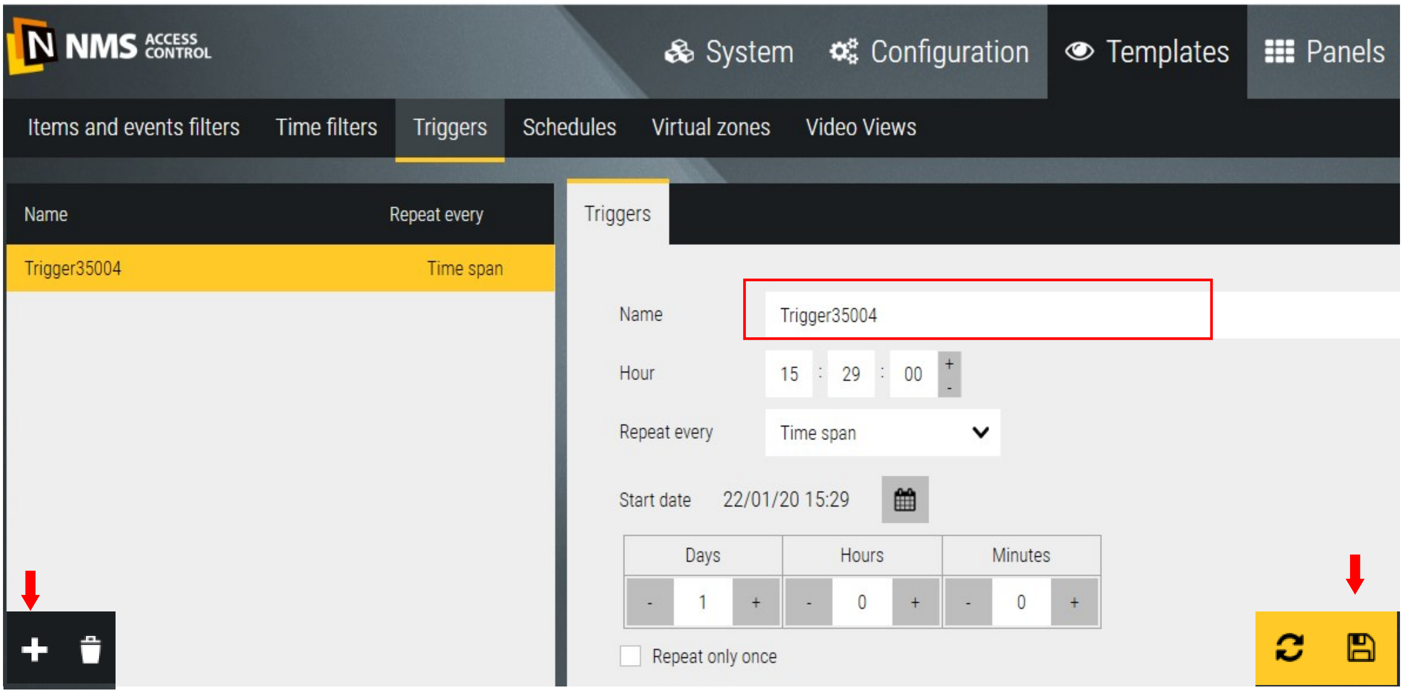
Daily filter - includes 24 hours and allows you to limit the preset time and days of the week to specific hours and minutes through the day with an accuracy of 1 or 15 minutes. The Daily filter is presented in graphical form - by default the whole day is active (green stripes). When you right-click and drag the bars, the color changes to gray, and the events in that compartment are not included in the report. The same operation with the left mouse button restores the green color.


Daily filter Precision (min.) 1


Daily filter Precision (min.) 15

4.3 Triggers

Use this tab to define triggers. Triggers are used, among other things, to run scenarios and to generate automated reports.



Name	Repeat every
Trigger35004	Time span

Name: Trigger35004

Hour: 15 : 29 : 00

Repeat every: Time span

Start date: 22/01/20 15:29

Days	Hours	Minutes
1	0	0

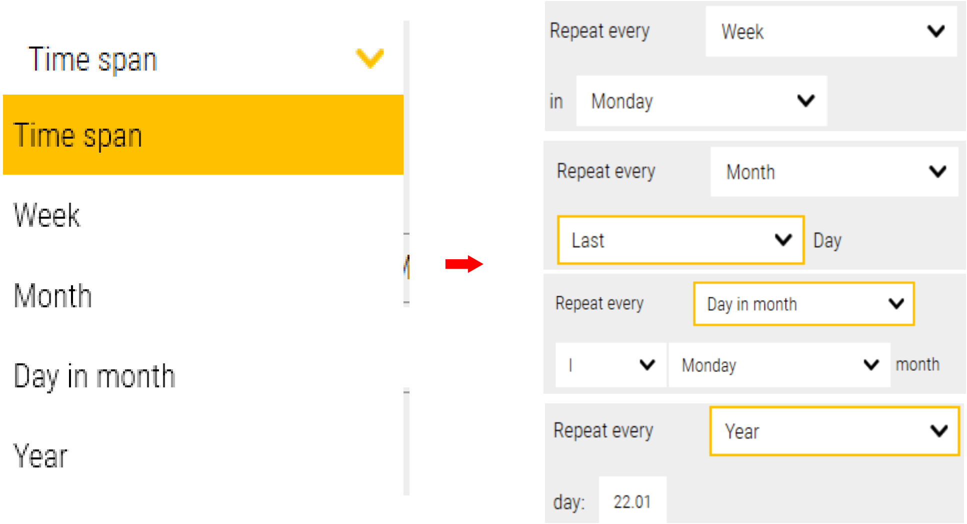
□ Repeat only once

To add a new trigger click on the *Add* button - left corner.

Name - editable field to type the name of the trigger in place of the default name.

Hour - the time at which the function controlled by this trigger will occur.

Repeat every - operation will be repeated with set frequency.



Repeat every: Week; in: Monday

Repeat every: Month; Last Day

Repeat every: Day in month; I Monday month

Repeat every: Year; day: 22.01

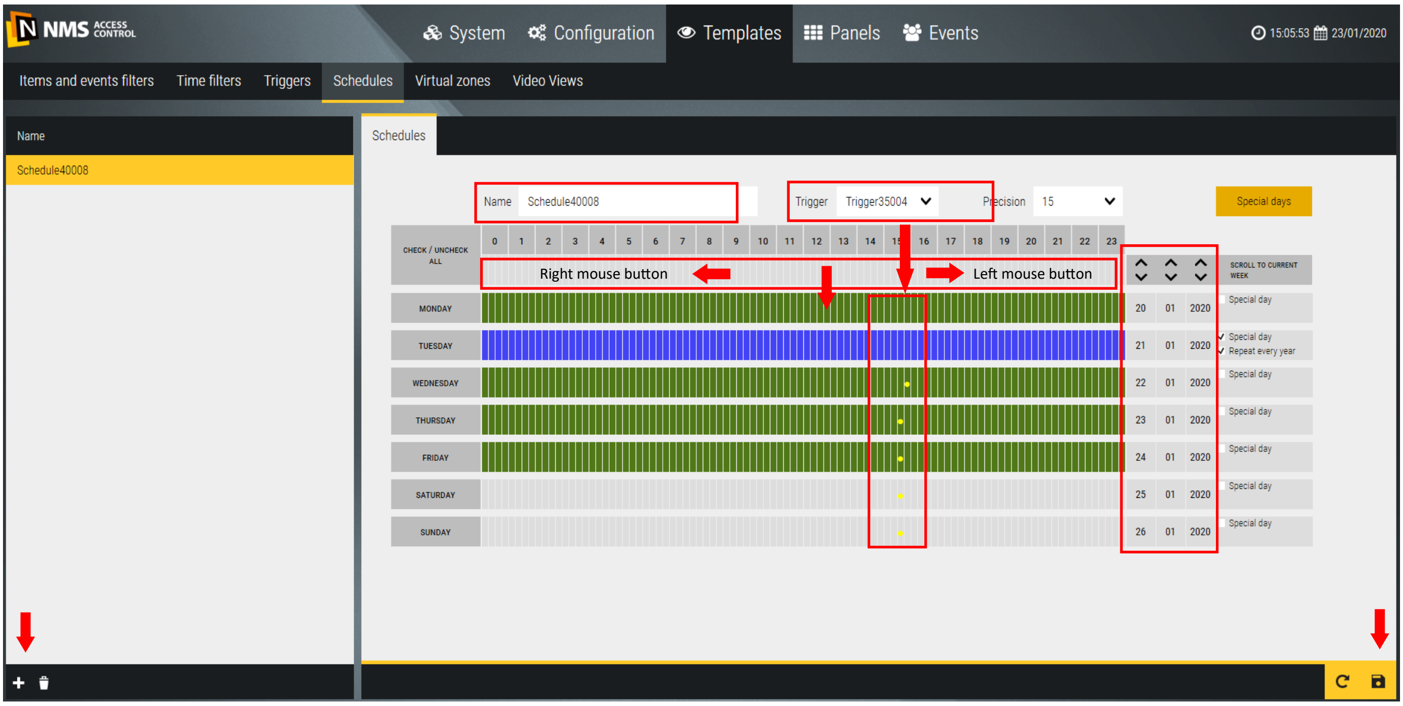
Start date - the date from which the operation will begin to repeat.

Repeat only once - if selected, the operation will be performed only once.

Save settings by clicking the floppy disk icon in the lower-right corner.

4.4 Schedules

This tab allows you to define schedules that are used in the process of defining scenarios.



Schedule40008

Name: Schedule40008 · Trigger: Trigger35004 · Precision: 15

20	01	2020	□ Special day
21	01	2020	✓ Special day ✓ Repeat every year
22	01	2020	□ Special day
23	01	2020	□ Special day
24	01	2020	□ Special day
25	01	2020	□ Special day
26	01	2020	□ Special day

To add a new schedule, click on the *Add* button - bottom left corner.

Name - editable field in the right window to type the schedule's name in place of the default name.

Trigger - a drop-down list that allows you to select a previously defined trigger that can also initiate a response during or outside the active schedule period (yellow dots on the graphic).

Accuracy - selectable one of two grid options to display time: 1 minute or 15 minutes. When you select 1 minute, a time scroll bar appears.

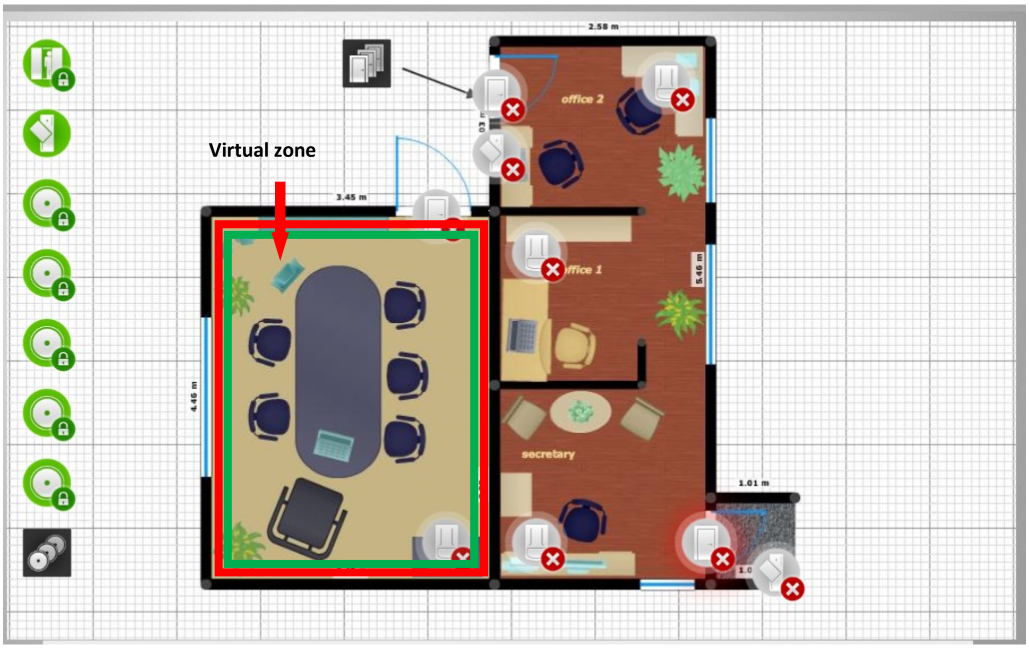
A field with red arrows allows you to quickly fill the fields of the days of the week below.
When you right-click and drag the bars, the color changes to gray (that is, the period in which the schedule is inactive). The same operation with the left mouse button changes to a green color (that is, the period in which the schedule is active).
You can quickly select/deselect all fields by clicking the right/left mouse button in the upper left corner.

Special days - allows you to set the schedule and trigger activity on special days. When you click on the *Special days* button, the following calendar is displayed, which allows you to set the date. This is done by scrolling in the columns of the day, month, year (by clicking on the top-down arrows). After you set the date on the corresponding weekday, click in the checkbox and select a *Special day* , then mark the time interval and/or select the trigger as described above. The selected schedule activity interval is displayed in navy blue. If a special day is repeated every year with the same date then select the checkbox below in that line.

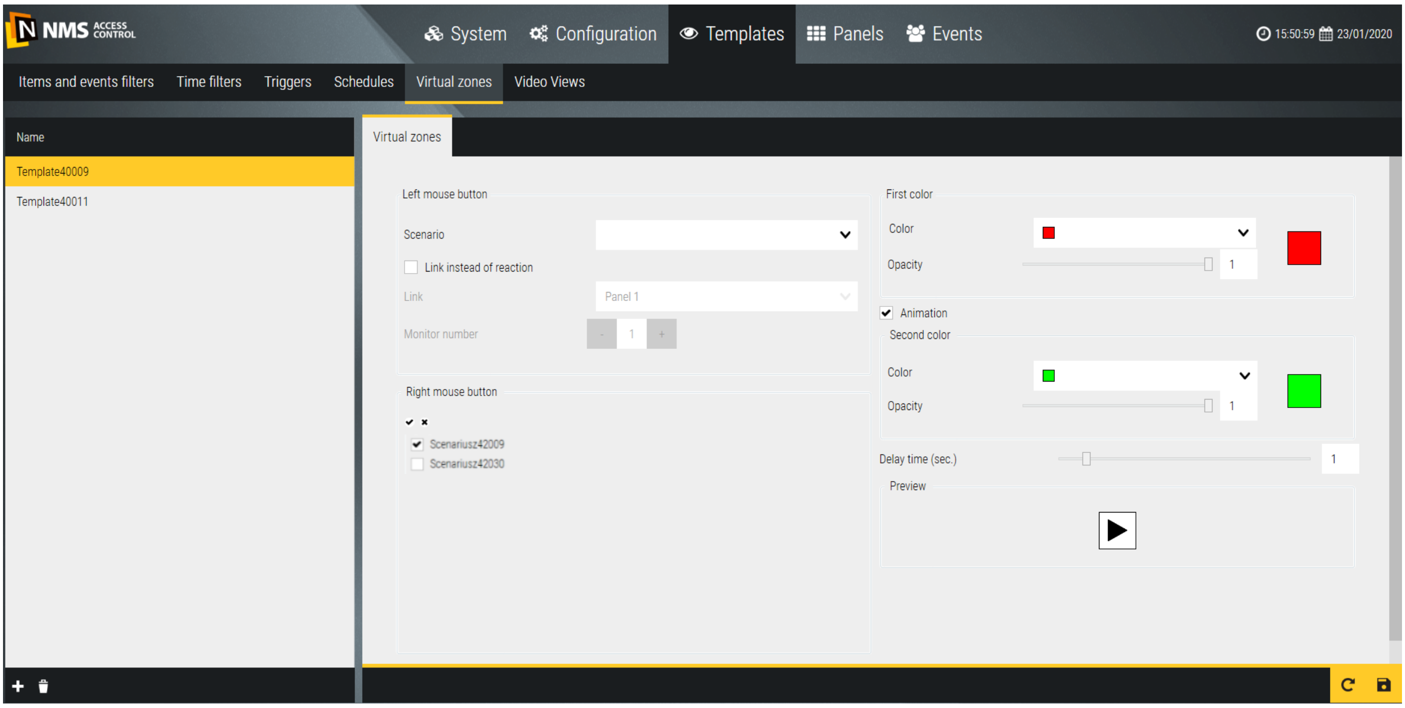
Save settings by clicking the floppy disk icon in the lower-right corner.

4.5 Virtual zones

This tab allows you to define the properties of zones, which can then be placed as objects on the panel.



A zone can have a scenario assigned or respond to right-click, animation and transparency level. In panel edition mode it’s recommended to place it on a separate layer.



Name

Template40009

Template40011

Virtual zones

Left mouse button

Scenario

□ Link instead of reaction

Link: Panel 1

Monitor number: - 1 +

Right mouse button

✓ ×

☑ Scenariusz42009

□ Scenariusz42030

First color

Color: 🟥

Opacity: 1

☑ Animation

Second color

Color: 🟩

Opacity: 1

Delay time (sec.): 1

Preview

▶

<u>Left mouse button</u> - sets the zone's response to a click in its area with the left mouse button. There are two options to choose from:

Execution of a scenario or a link to a selected panel. You can also select the monitor number on which you want to display the panel set in this link.

<u>Right mouse button</u> - sets the zone's response to a right-click in its area. We have a list of scenarios to choose from. You can select checkboxes for one or more of the scenarios that will be performed after this click.

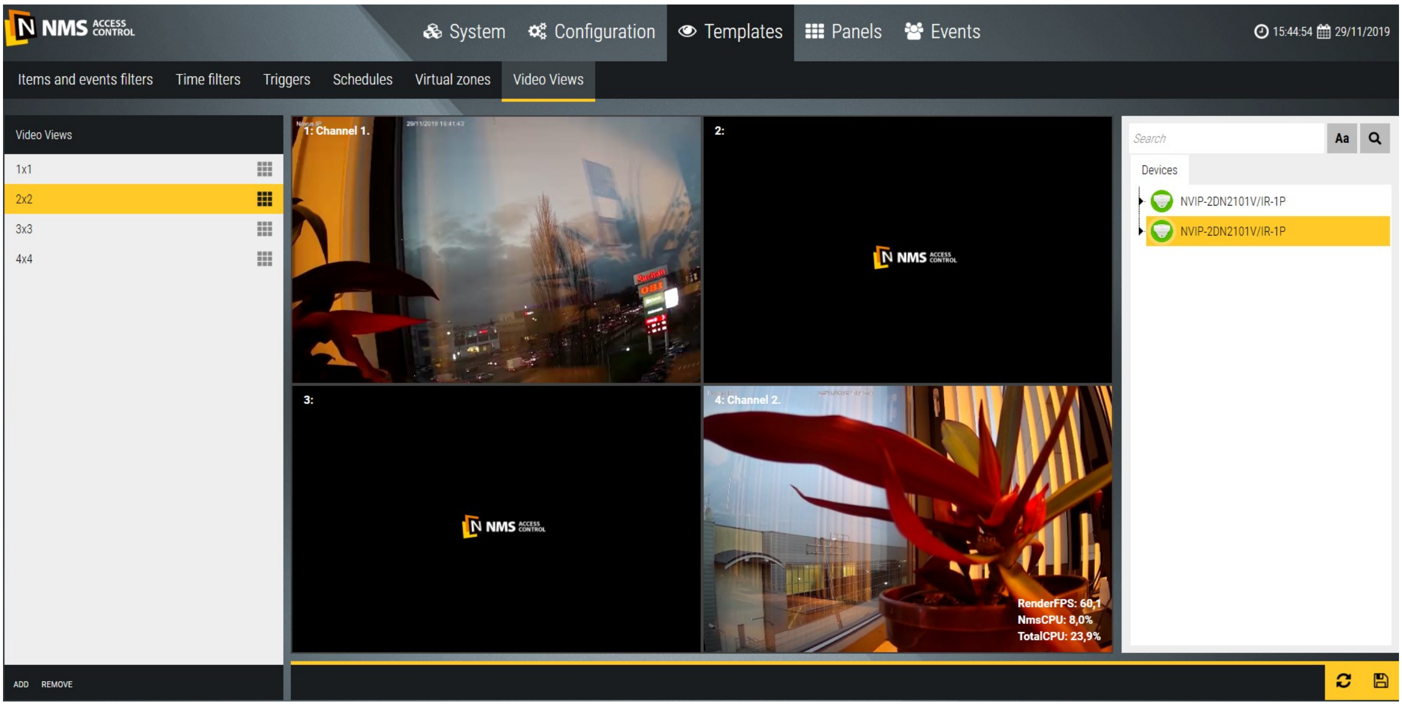
<u>Zone display on the panel</u> - select the default color, transparency, animation checkbox (the second color) and its speed.

The defined zone templates appear in the panel edit mode when virtual zone is placed.

Save settings by clicking the floppy disk icon in the lower-right corner.

4.6 Video views

In the *Video views* tab, you can define sets of video views that are used to visualize and monitor the state of the system and display video streams from the cameras placed in the object. The list of defined video views is displayed in the left window. By default, four panels with different division are defined. After clicking the *Add* button you can add a new view, rename it, assign a division by clicking on the icon ▦ in the view name field and the video stream by dragging it with the mouse from the list on the right in the selected view window. The video view can be displayed by clicking on its name in the left window.



Default views can be edited and changed according to your needs.

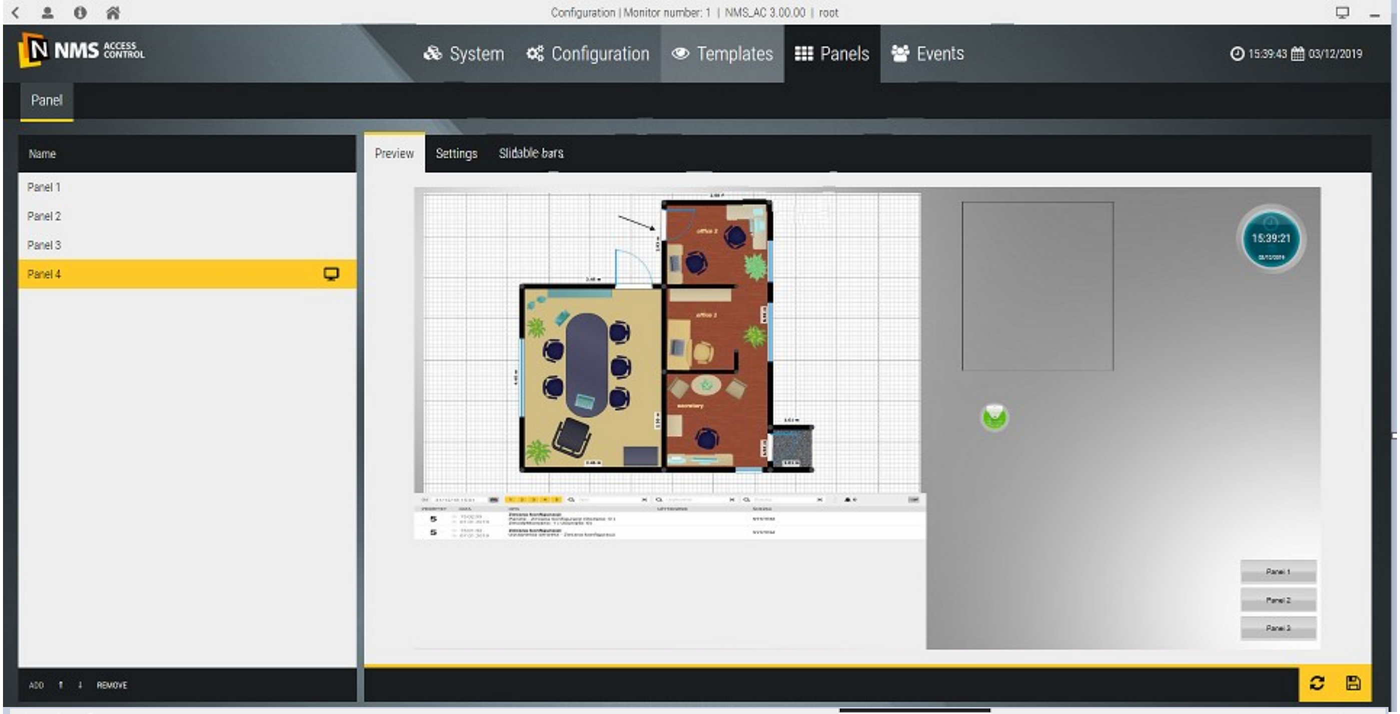
After you have defined the video views, click the *Save* button in the lower-right corner.

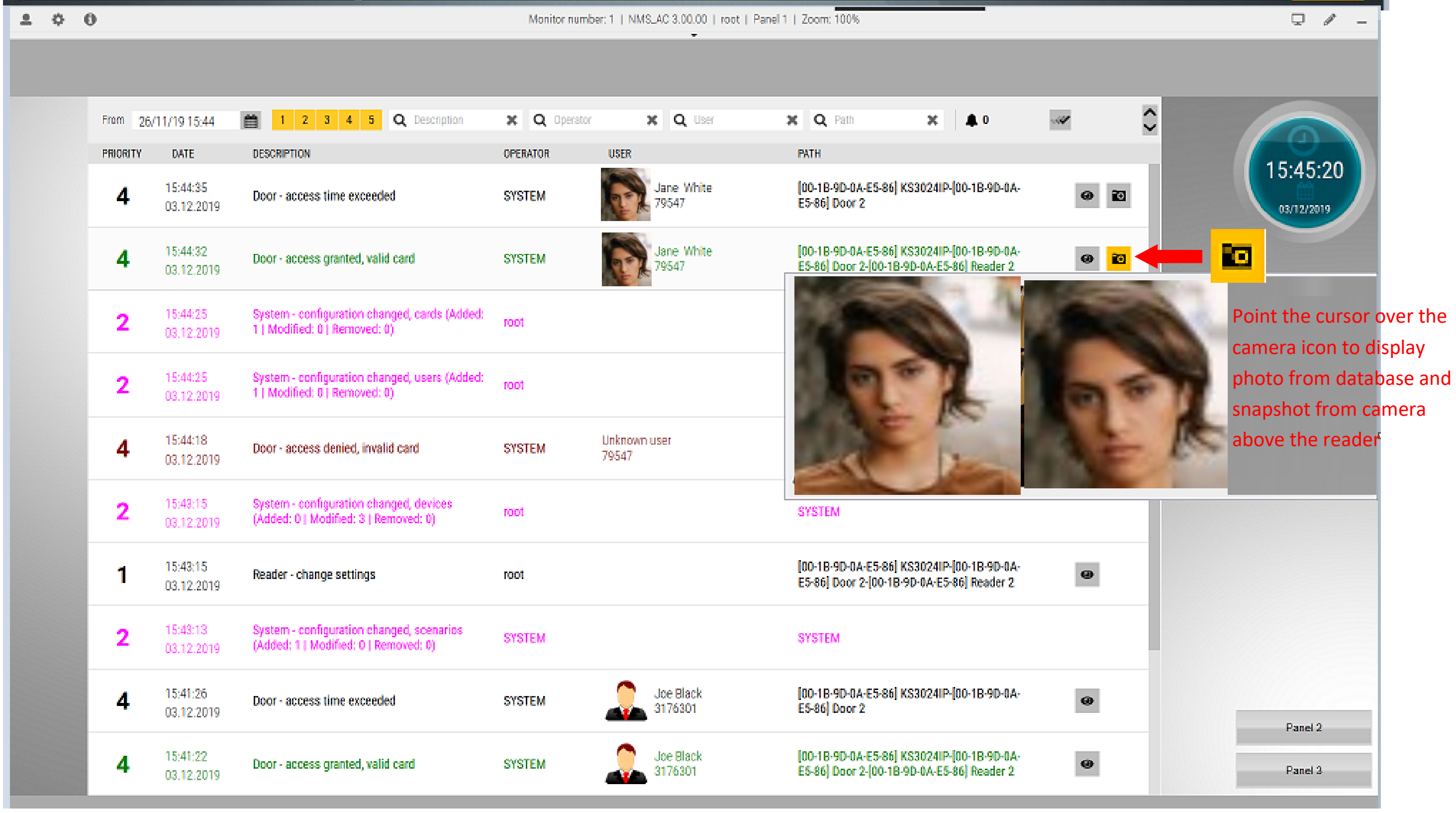
You can view the defined *Video views* on panels in video windows. Panel 3 defined by default includes this view window.

Section 5. Panels

In the *Panels* tab you can define the panels, which are used to visualize and monitor the status of various system elements and display events and other additional information. The list of defined panels is displayed in the left window and depends on your license. Under the free license, you can define four panels, two of which are the default. The panel can be displayed by clicking on its name in the left window.

The default *Panel 1* includes: event stack, clock, and button with link to *Panel 2*.



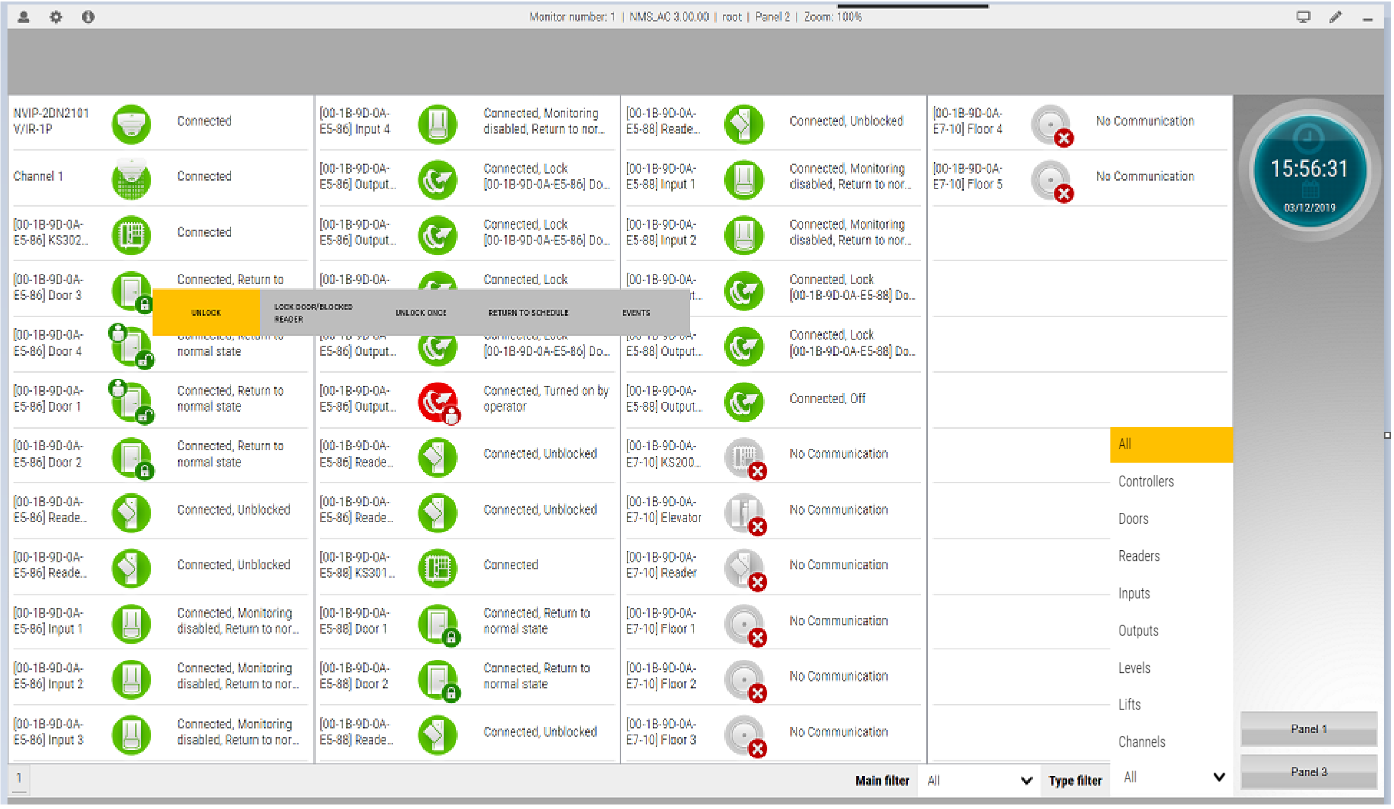


PRIORITY	DATE	DESCRIPTION	OPERATOR	USER	PATH
4	15:44:35 03.12.2019	Door - access time exceeded	SYSTEM	Jane White 79547	[00-1B-9D-0A-E5-86] KS3024IP-[00-1B-9D-0A-E5-86] Door 2
4	15:44:32 03.12.2019	Door - access granted, valid card	SYSTEM	Jane White 79547	[00-1B-9D-0A-E5-86] KS3024IP-[00-1B-9D-0A-E5-86] Door 2-[00-1B-9D-0A-E5-86] Reader 2
2	15:44:25 03.12.2019	System - configuration changed, cards (Added: 1 | Modified: 0 | Removed: 0)	root		
2	15:44:25 03.12.2019	System - configuration changed, users (Added: 1 | Modified: 0 | Removed: 0)	root		
4	15:44:18 03.12.2019	Door - access denied, invalid card	SYSTEM	Unknown user 79547	
2	15:43:15 03.12.2019	System - configuration changed, devices (Added: 0 | Modified: 3 | Removed: 0)	root		SYSTEM
1	15:43:15 03.12.2019	Reader - change settings	root		[00-1B-9D-0A-E5-86] KS3024IP-[00-1B-9D-0A-E5-86] Door 2-[00-1B-9D-0A-E5-86] Reader 2
2	15:43:13 03.12.2019	System - configuration changed, scenarios (Added: 1 | Modified: 0 | Removed: 0)	SYSTEM		SYSTEM
4	15:41:26 03.12.2019	Door - access time exceeded	SYSTEM	Joe Black 3176301	[00-1B-9D-0A-E5-86] KS3024IP-[00-1B-9D-0A-E5-86] Door 2
4	15:41:22 03.12.2019	Door - access granted, valid card	SYSTEM	Joe Black 3176301	[00-1B-9D-0A-E5-86] KS3024IP-[00-1B-9D-0A-E5-86] Door 2-[00-1B-9D-0A-E5-86] Reader 2

Point the cursor over the camera icon to display photo from database and snapshot from camera above the reader

⚙ Return to the *Configuration* tab, ✎ Enter the panel edit mode; below the alarm beam with the erase buttons. The *Event stack* displays events according to the default settings in the *Event Parameters* tab. You can filter them by typing a keyword in one of the fields with magnifier or by unchecking the selected yellow priority boxes.

The default *Panel 2* contains a synoptic table, a clock, and a buttons with a link to other panels.



Monitor number: 1 | NMS_AC 3.00.00 | root | Panel 2 | Zoom: 100%

NVIP-2DN2101 V/IR-1P	Connected	[00-1B-9D-0A-E5-86] Input 4	Connected, Monitoring disabled, Return to nor...	[00-1B-9D-0A-E5-88] Reade...	Connected, Unblocked	[00-1B-9D-0A-E7-10] Floor 4	No Communication
Channel 1	Connected	[00-1B-9D-0A-E5-86] Output...	Connected, Lock [00-1B-9D-0A-E5-86] Do...	[00-1B-9D-0A-E5-88] Input 1	Connected, Monitoring disabled, Return to nor...	[00-1B-9D-0A-E7-10] Floor 5	No Communication
[00-1B-9D-0A-E5-86] KS302...	Connected	[00-1B-9D-0A-E5-86] Output...	Connected, Lock [00-1B-9D-0A-E5-86] Do...	[00-1B-9D-0A-E5-88] Input 2	Connected, Monitoring disabled, Return to nor...		
[00-1B-9D-0A-E5-86] Door 3	Connected, Return to	[00-1B-9D-0A-	Connected, Lock	[00-1B-9D-0A- ...t...	Connected, Lock [00-1B-9D-0A-E5-88] Do...		
[00-1B-9D-0A-E5-86] Door 4	normal state	E5-86] Output...	[00-1B-9D-0A-E5-86] Do...	E5-88] Output...	Connected, Lock [00-1B-9D-0A-E5-88] Do...		
[00-1B-9D-0A-E5-86] Door 1	Connected, Return to normal state	[00-1B-9D-0A-E5-86] Output...	Connected, Turned on by operator	[00-1B-9D-0A-E5-88] Output...	Connected, Off		
[00-1B-9D-0A-E5-86] Door 2	Connected, Return to normal state	[00-1B-9D-0A-E5-86] Reade...	Connected, Unblocked	[00-1B-9D-0A-E7-10] KS200...	No Communication		
[00-1B-9D-0A-E5-86] Reade...	Connected, Unblocked	[00-1B-9D-0A-E5-86] Reade...	Connected, Unblocked	[00-1B-9D-0A-E7-10] Elevator	No Communication		
[00-1B-9D-0A-E5-86] Reade...	Connected, Unblocked	[00-1B-9D-0A-E5-88] KS301...	Connected	[00-1B-9D-0A-E7-10] Reader	No Communication		
[00-1B-9D-0A-E5-86] Input 1	Connected, Monitoring disabled, Return to nor...	[00-1B-9D-0A-E5-88] Door 1	Connected, Return to normal state	[00-1B-9D-0A-E7-10] Floor 1	No Communication		
[00-1B-9D-0A-E5-86] Input 2	Connected, Monitoring disabled, Return to nor...	[00-1B-9D-0A-E5-88] Door 2	Connected, Return to normal state	[00-1B-9D-0A-E7-10] Floor 2	No Communication		
[00-1B-9D-0A-E5-86] Input 3	Connected, Monitoring disabled, Return to nor...	[00-1B-9D-0A-E5-88] Reade...	Connected, Unblocked	[00-1B-9D-0A-E7-10] Floor 3	No Communication		

Main filter: All

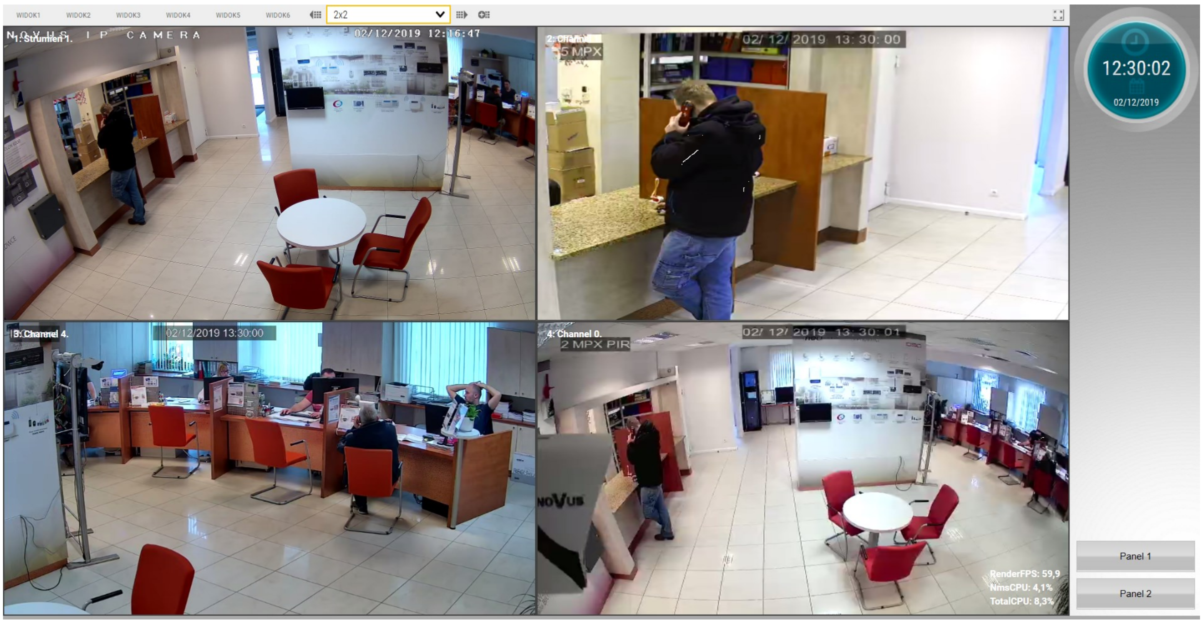
Type filter: All

Panel 2 contains a synoptic array, which automatically adds additional controllers together with the cooperating elements (doors, input lines, control outputs, elevators, floors) and surveillance television devices as icons representing their current status. The status of the icons is updated in real time (when communication with devices is correct). Icons have a context menu (left mouse button).

There are two filters in the lower right corner of the synoptic array to display only selected items:

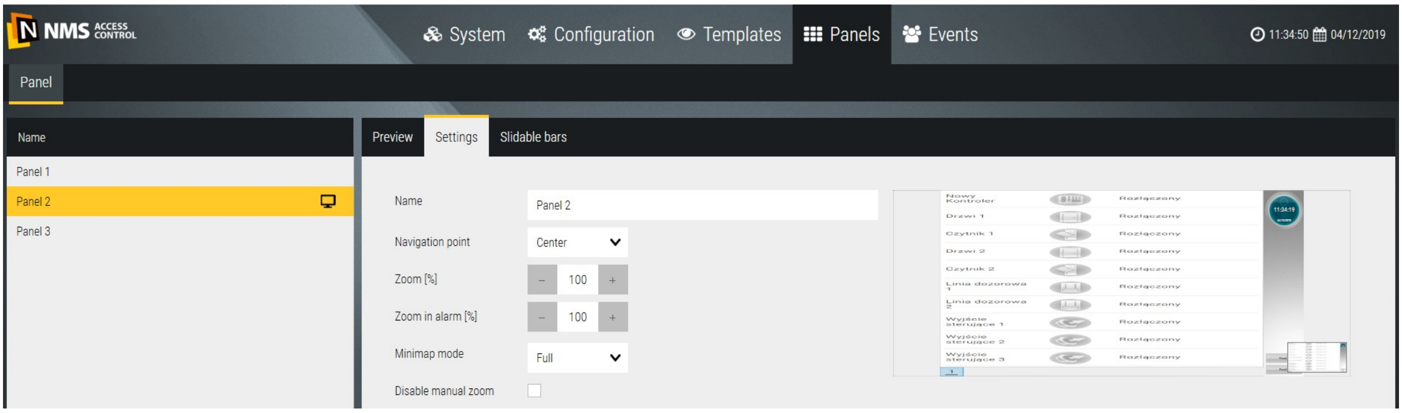
- *Main filter* - defined in the tab *Templates/Items and events filter*
- *Type filter* - allows to display elements of only one type from the currently available on the board.

To define a new panel, click on the *Add* button in the lower left corner of the *Panels* window .



The added panel appears in the list in the left window. A preview of the panel background is displayed in the right.

Settings tab



Name

Panel 1

Panel 2

Panel 3

Name: Panel 2

Navigation point: Center

Zoom [%]: − 100 +

Zoom in alarm [%]: − 100 +

Minimap mode: Full

Disable manual zoom □

Name - editable field to type the name of the panel

Navigation point - point on the panel to which the process relates, default *Center,* other items will appear in this list after defining additional navigation points on the panel

Zoom [%] - sets the zoom value on the panel

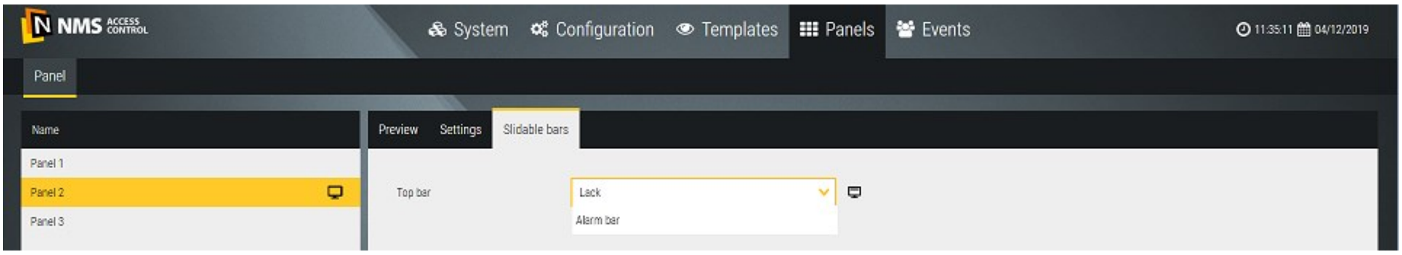
Zoom in alarm [%] - sets the zoom value for the alarm event on the panel

Disable manual zoom - allows you to turn off the zoom on the panel with the mouse wheel

Minimap mode - selectable from the drop-down list of map thumbnail display mode: full, background only, transparent or no minimap.

Set background - allows you to select the background of the panel from the specified folder from bmp, jpg, png file or default

Slidable bars tab



Name

Panel 1

Panel 2

Panel 3

Top bar: Lack

Alarm bar

Top bar - selectable from the drop-down list: alarm bar or none

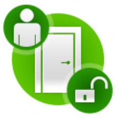
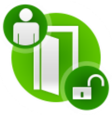
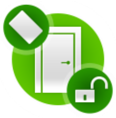
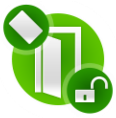
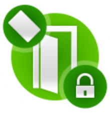
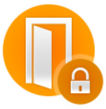
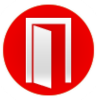
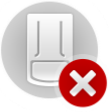
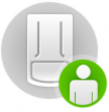
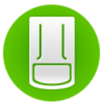
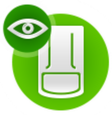
Once defined, save the settings for the new panel by clicking on the floppy disk icon in the bottom right corner.

By clicking on the panel name in the left window, you can enter the display mode and verify the settings.

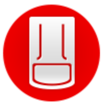
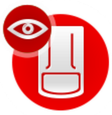
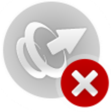
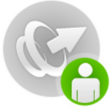
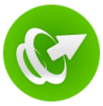
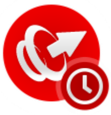
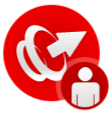
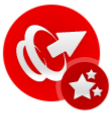
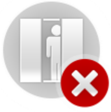
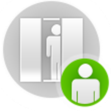
On NMS ACCESS CONTROL panels following icons can occur:

	Controllers	
	Controller - communication lost, restaring connection	
	Controller - communication lost, disconnected by operator	
	Controller - connected	
	Controller - connected, uploading settings	
	Controller - connected, downloading events	
	Doors	
	Door - communication lost, restaring connection	
	Door - communication lost, disconnected by operator	
	Door - connected, locked, closed	
	Door - connected, reader disabled by operator, closed	
	Door - coonected, unlocked by schedule, closed	
	Door - coonected, unlocked by schedule, open	

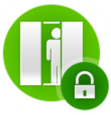
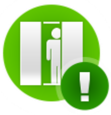
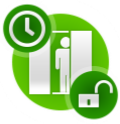
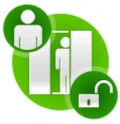
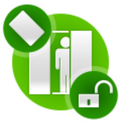
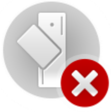
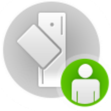
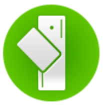
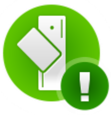
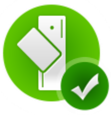
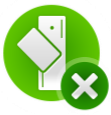
On NMS ACCESS CONTROL panels following icons can occur:

	Door - connected, unlocked by operator, closed	
	Door - connected, unlocked by operator, opened	
	Door - connected, unlocked on access granted, closed	
	Door - connected, unlocked on access granted, opened	
	Door - connected, locked after access granted, opened	
	Door – connected, opened too long	
	Door - connected, forced	
	Inputs	
	Input - communication lost, restaring connection	
	Input - communication lost, disconnected by operator	
	Input - connected, monitoring off	
	Input - connected, monitoring on	

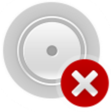
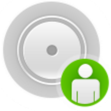
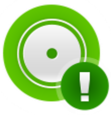
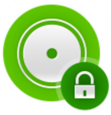
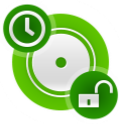
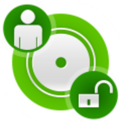
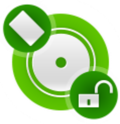
On NMS ACCESS CONTROL panels following icons can occur:

	Input - connected, monitoring off, active	
	Input - connected, monitoring on, alarm	
	Outputs	
	Output - communication lost, restaring connection	
	Output – communication lost, disconnected by operator	
	Output - connected, inactive	
	Output - connected, activated by schedule	
	Output - connected, activated by operator	
	Output - connected, activated by event	
	Elevators	
	Elevator - communication lost, restaring connection	
	Elevator - communication lost, disconnected by operator	

On NMS ACCESS CONTROL panels following icons can occur:

	Elevator - connected, all floors locked	
	Elevator - connected, reader disabled by opertator	
	Elevator - connected, selected floors unlocked by schedule	
	Elevator - connected, selected floors unlocked by operator	
	Elevator - connected, selected floors unlocked on access granted	
Readers		
	Reader - communication lost, restaring connection	
	Reader - communication lost, disconnected by operator	
	Reader - connected	
	Reader - connected, disabled by operator	
	Reader - connected, access granted	
	Reader - connected, access denied	

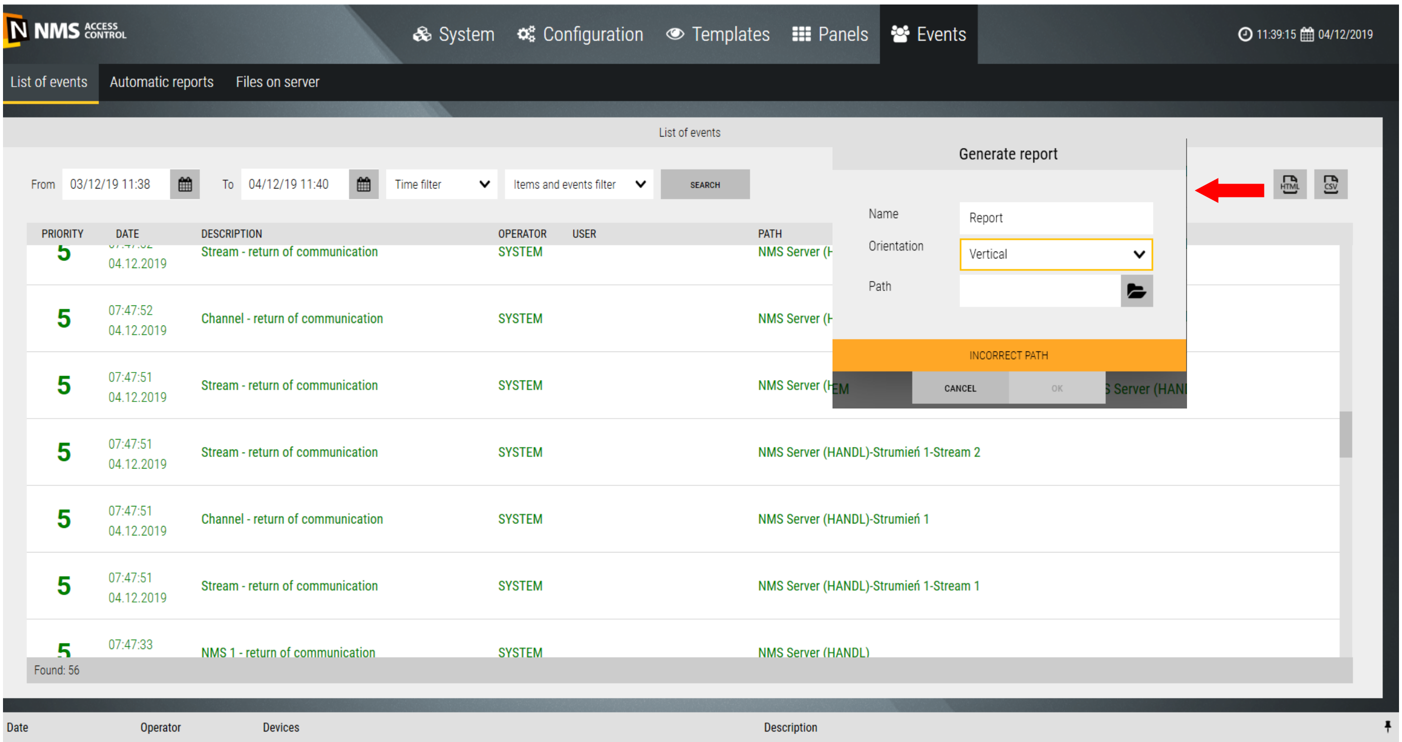
On NMS ACCESS CONTROL panels following icons can occur:

	Floors	
	Floor - communication lost, restaring connection	
	Floor - communication lost, disconnected by operator	
	Floor - connected, reader disabled by operator	
	Floor - connected, locked	
	Floor - connected, unlocked by schedule	
	Floor - connected, unlocked by operator	
	Floor - connected, unlocked on access granted	

Section 6 Events and reports

6.1 List of events

In the *Events* tab you can generate a filtered report. The generated report is displayed on the screen or can be saved as a file on disk (the buttons in the upper right corner of the window) in the format *. CSV or *. HTML (with PDF export capability).



From 03/12/19 11:38 To 04/12/19 11:40 Time filter Items and events filter

Generate report

Name: Report

Orientation: Vertical

Path:

INCORRECT PATH

PRIORITY	DATE	DESCRIPTION	OPERATOR	USER	PATH
5	07:47:52 04.12.2019	Stream - return of communication	SYSTEM		NMS Server (H
5	07:47:52 04.12.2019	Channel - return of communication	SYSTEM		NMS Server (H
5	07:47:51 04.12.2019	Stream - return of communication	SYSTEM		NMS Server (H
5	07:47:51 04.12.2019	Stream - return of communication	SYSTEM		NMS Server (HANDL)-Strumień 1-Stream 2
5	07:47:51 04.12.2019	Channel - return of communication	SYSTEM		NMS Server (HANDL)-Strumień 1
5	07:47:51 04.12.2019	Stream - return of communication	SYSTEM		NMS Server (HANDL)-Strumień 1-Stream 1
5	07:47:33	NMS 1 - return of communication	SYSTEM		NMS Server (HANDL)

Found: 56

Each report line contains a date and time, a description of the event and the association with the operator or card user and the physical element of the system affected by the event.

At the top of the window are the filter fields for date, time interval (default last 24 hours) and items and events. This makes it easier to analyze the events on the object.

After setting the filters, click on the *Search* button. A report appears in the window.

The lower-right corner of the window displays information about the number of events in the generated report. The maximal number of events is 10 000. If this value is exceeded by the filter settings, this information is displayed. You must change the filter settings.

7.2 Automatic reports

In the Automatic Reports tab you can set parameters of the new automatically generated report template according to the selected trigger. Generating automated reports is accomplished with scenarios. For ease a simple to use scenarios wizard has been implemented in this window. Similarly to manually generated reports, you have a set of filters here. Click *Add* and configure a new auto report template.

Name - editable field to type the name of the report template

Time filter - selectable from the drop-down list previously defined in the

Templates/Time Filters

Items and events filters - select from the drop-down list defined in the

Templates/Items and events filters

Trigger -selectable from the drop-down list previously defined in the

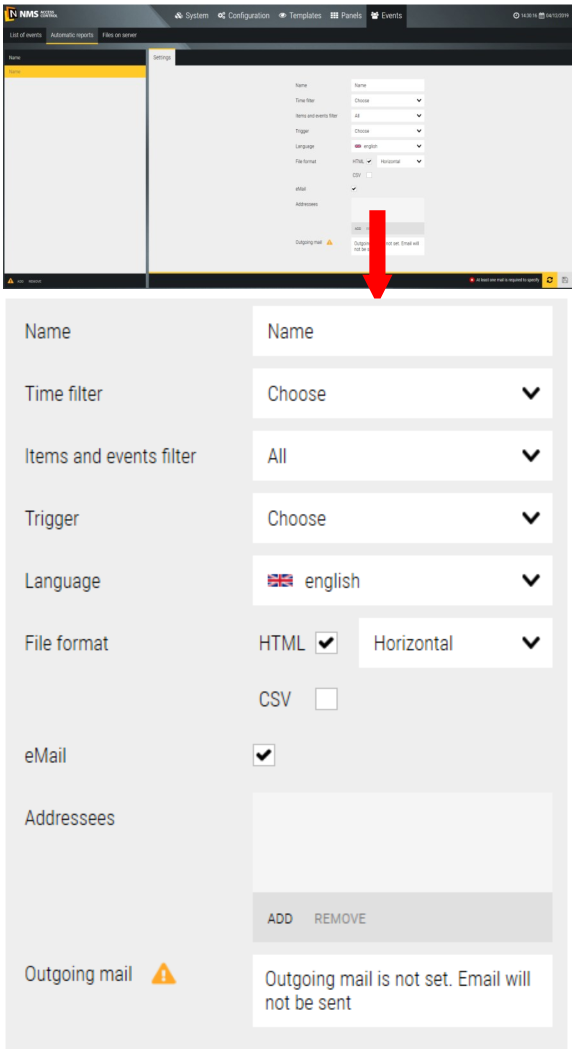
Templates/Triggers

Report - select one of the file formats: CSV or HTML

Orientation - select the horizontal or vertical orientation of the page to preview or print. Recommended horizontal orientation due to the number of columns in the report and long descriptions.

Language - selectable from the drop-down list: Polish, English, Russian, Azerbaijani. The next languages during the translation.

Email - the field selected if the report must be sent as email. When selected, the following fields are displayed to enter the recipients and subject of the email. To add a recipient, click on the *Add* button at the bottom of the window and enter the email address in the field that appears.



Name: Name

Time filter: Choose

Items and events filter: All

Trigger: Choose

Language: english

File format: HTML ☑ Horizontal

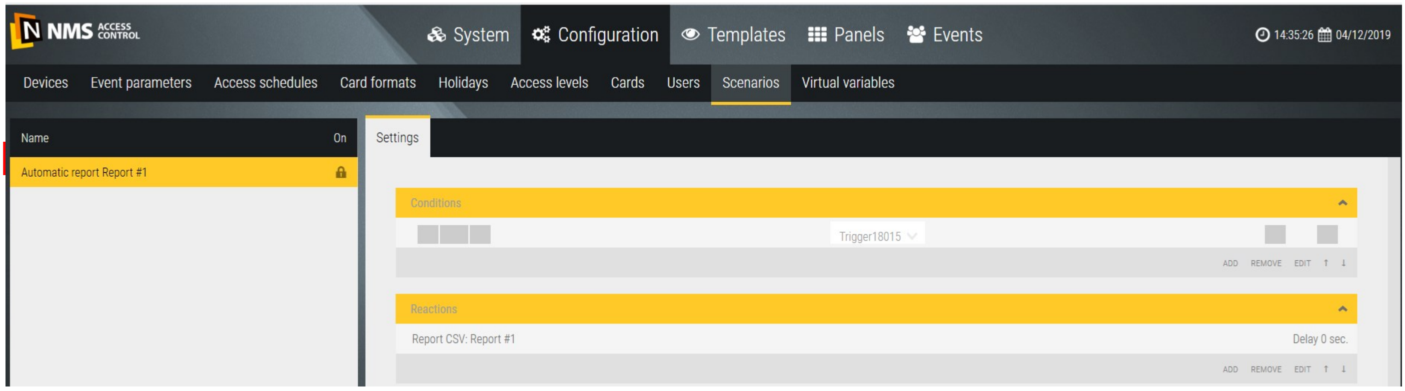
CSV □

eMail ☑

Addressees

ADD REMOVE

Outgoing mail ⚠ Outgoing mail is not set. Email will not be sent



Automatic report Report #1

Conditions

Trigger18015

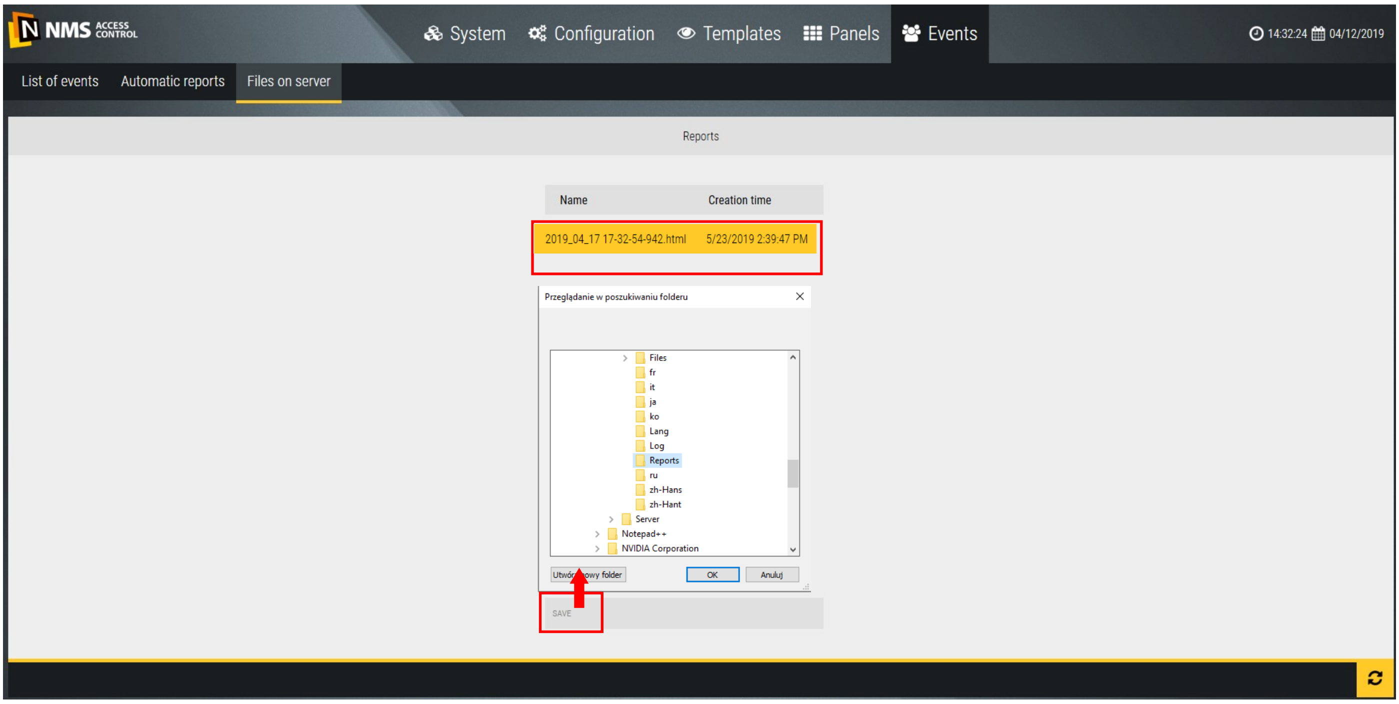
Reactions

Report CSV: Report #1 Delay 0 sec.

After making the settings and clicking *OK* you move to the *Configuration/Scenarios* window - in the left window is a list of defined templates of automatic reports.

7.3 Files on server

Reports generated automatically according to the template assigned trigger are saved in the report archive on the computer where the NMS AC Server service is installed. You can change this path in the *System* tab.



Name	Creation time
2019_04_17 17-32-54-942.html	5/23/2019 2:39:47 PM

At the client station that is connected to the server you can see a list of automatically generated reports as in the window below (tab *Files on the server*). When you select a report in the list, you can copy it to the client station to the specified folder.

6.4 Events occuring in NMS AC system

Controller – loss of communication
Controller – return of communication
Controller – initialize by operator command
Controller – disconnected by operator command
Controller – connected by operator command
Controller – check status by operator command (+ info about KT)
Controller – set time by operator command
Controller – get time by operator command (+ time info)
Controller – device has been removed
Controller – connection error
Controller – change settings
Controller – settings have been sent to device
Controller – alarm confirmed
Door – unlocked by schedule
Door – locked by schedule
Door – unlocked by operator command
Door – locked by operator command, blocked reader
Door – return to schedule by operator command
Door – access granted by operator command
Door – access granted, valid card
Door – Access granted, valid code
Door – waiting for code
Door – access granted, valid card and code
Door – access granted, exit button
Door – access requested, valid card
Door – access requested, valid code
Door – access requested, valid card and code
Door – access granted, request confirmed by operator
Door – access granted, threaten code used
Door – valid card, waiting for next one
Door – access time exceeded
Door – access denied, invalid card
Door – access denied, invalid code
Door – access denied, operator unconfirmed
Door – access denied, reader blocked
Door – access denied, first opening card required

Door – forced door
Door – door opened too long
Door – return to normal state
Door – change settings
Door – settings have been sent to device
Door – alarm confirmed
Input – in alarm state
Input – return to normal state
Input – violated input
Input – change settings
Input – settings have been sent to device
Input – alarm confirmed
Output – enabled by operator command
Output – disabled by operator command
Output – enabled by the event
Output – disabled by event
Output - change settings
Output – settings have been sent to device
Output – alarm confirmed
Elevator – selected floors unlocked by operator command
Elevator – selected floors locked by operator command
Elevator - restored to schedule by operator command
Elevator – selected floors unlocked on access granted
Elevator – access denied, invalid card
Elevator – all floors unlocked by emergency button
Elevator – change settings
Elevator – settings have been sent to device
Elevator – alarm confirmed
Reader – enabled by operator command
Reader – disabled by operator command
Reader – change settings
Reader – settings have been sent to device
Reader – alarm confirmed
Floor – unlocked by operator command
Floor – locked by operator command
Floor – unlocked on access granted
Floor – change settings
Floor – settings have been sent to device
Floor - alarm confirmed

THE LICENCE AGREEMENT
FOR THE "NMS ACCESS CONTROL" PROGRAMME

AAT SYSTEMY BEZPIECZEŃSTWA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
with a registered office in Warsaw
ul. Puławska 431, 02-801 Warsaw
The District Court for the Capital City of Warsaw, XIII Commercial Division, entry number KRS 0000838329,
Tax identification number NIP 9512500868, statistical number REGON: 385953687,
Value of the share capital: PLN 17 005,000.00 ("the Company")

This licence agreement is an agreement concluded between the user (hereinafter referred to as the User) and AAT SYSTEMY BEZPIECZEŃSTWA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, with a registered office in Warsaw, ul. Puławska 431, 02-801 Warsaw, entered in the Register of Entrepreneurs kept by the District Court for the Capital City of Warsaw, Thirteenth Commercial Division of the National Court Register, number of entry KRS 0000838329, tax identification number NIP 9512500868, statistical number REGON: 385953687, value of the share capital: PLN 17 005,000.00 (hereinafter referred to as the Producer) for the use of the NMS ACCESS CONTROL programme, subject to the terms and conditions specified below. The User acknowledges that the Agreement concerns all the possibilities of using the Programme, regardless of the place or method of its installation.

1. Definitions

1.1. "Copyrights and Related Rights" – each and all copyrights and related rights, including, in particular, copyrights, rights to patents, trademarks, as well as know-how and business secrets forming a part of incorporated in the Programme, constituting the property of the Producer. Copyrights and neighbouring rights are protected, in particular, by the Act of 4 February 1994 on Copyrights and Neighbouring Rights (Journal of Laws of 1994, no. 24, item 83, as amended). This Agreement shall not transfer any copyrights and neighbouring rights to the User and shall not grant him such rights. The User shall only have a possibility of using the Programme within the scope specified in the Agreement.

1.2. "Installer" - a third party performing in particular sales/deliveries and installation of the Programme at the User's. The installer shall be only granted the right to resell the Programme and install it at the User's, the Installer shall have no other rights indicated in the Agreement and concerning the User.

1.3. "Key" – distributed along with the Programme sequence of signs enabling activation of the Programme's licence, intended for use in the server where the Programme is installed. The key prevents, among others, free license transfer. Key loss or damage makes it impossible for the Programme to operate.

1.2. "The Agreement" – this licence agreement which the User concludes with the Producer for the purpose of obtaining a possibility of using the Programme.

1.3. "NMS ACCESS CONTROL" or "the Programme" – a computer programme developed by the Producer dedicated only for some devices, enabling, among others, integration to a limited extent of Access Control Systems (KD) CCTV systems (VSS), along with the function of receiving technical and alarm signals.

2. Licence and limitations

2.1. The Producer hereby grants a licence to the User, solely for the User's use, on a non-exclusive basis, without a right of transfer or sublicencing thereof to third parties, for downloading, installation and use of the Programme on a PC or a laptop, also using mobile devices and the Internet.

2.2. The Installer may mediate in sales of the Programme and perform its installation at the User's, which shall not be regarded as breach of the terms hereof.

2.3.The Agreement covers one server post and customer post of the User, and the number of devices connected and customers connected is limited by the efficiency of hardware used by the User and the kind of Key and/or Programme version.

2.4. Installation of the programme on the User server and customer posts on computers placed in facilities of the User is made by the Installer after the Producer or Installer gives the carriers with the Programme and the Key. Transferring the carriers does not mean the User acquiring proprietary copyrights to the Programme.

2.5. In order to enable implementation of the Agreement the Producer shall assign to the User ownership to carriers of the Programme as well the Key upon issuing them to the User.

2.6. The User has the right to make one back-up copy of the Programme.

2.7. The User may not, in any way, transfer for use, resell, transfer, distribute or in any way make the Programme or any part thereof available to third parties, and breach any rights referring to the Programme or any parts thereof.

2.8. The User shall not be authorized and undertakes not to undertake, not to cause and not to grant consent or authorization to any third party to conduct modification, create derivative elements, translations, de-compilations, disassembly or breaking the code of the Programme or any parts thereof or the Key.

2.9. The Producer reserves the exclusive right to modify, extend, update, translate, as well as repair the Programme at his own discretion.

2.10. The Producer is not obliged to inform the User about any modifications, extensions, updates, translations or next versions of the Programme.

2.11. The Producer is not obliged to provide the User with the next versions of the Programme, its extensions, updates and translations.

2.12. The User, supported by the Installer, may collect and install the modifications, extensions or Programme's updates made available by the Producer on their website or directly transferred to the User or the Installer.

3. Term of the Agreement

3.1. The Agreement shall be conclude by the acceptance of the terms and conditions hereof by the User during the Programme installation.

3.2. The Agreement is concluded for an unspecified period of time.

3.3 The Agreement shall be unrestricted territorially, the User has the right to use the Programme on the territory of Poland and any other country.

3.4. Either Party shall have the right to terminate the Agreement with due observance of the period of notice of one month, with legal effect for the Party as of the last day of the next calendar month. Expiration or termination of the Agreement shall have no effect on the responsibilities of the Parties resulting from Copyright and Related Rights and shall not waive the prohibition to breach in any way the integrity of the Programme, including its modification, creating derivative elements, translation, decompilation, disassembly, or breaking the Programme's code or its part or the Key.

3.5. The Producer shall have the right to terminate the Agreement without notice in the event of significant breach of its provisions by the User. A significant breach of the provisions of the Agreement is especially proprietary breach of copyright to the Programme granted to the Producer.

3.6. The User may, at any moment, terminate the Agreement without a notice period by uninstalling the Programme and removing it from memories of all PCs and portable computers, mobile devices, destroying backup copies.

3.7. Upon termination of the Agreement, all the User's rights to the Programme transferred hereunder shall expire.

Then the User shall be obliged to stop using the Programme and delete the Programme and the backup copy thereof from all media and devices.

3.8. The Producer shall not bear liability for any damages incurred in connection with termination of the Agreement.

4. Guarantees and liability of the Producer

4.1. The Producer guarantees that he has the legal capacity to conclude and perform the Agreement.

4.2. The Producer shall deliver the Programme as is, with no guarantees and shall not bear any liability for the consequences of using the Programme in the cases of improper operation of the computer system caused defects of the hardware, improper installation or configuration of the software and hardware, and in the events of occurrence of improper operation of the Programme.

4.4. The Producer shall not bear liability under any warranty or guarantee for the Programme. In the event that the aforementioned limitation of liability is not possible, such liability shall be limited to the greatest possible extent.

4.5. The Producer shall not bear liability for the method of use of the Programme by the User, and in particular for the use of the Programme in contradiction with the Agreement or instruction manual accompanying the Programme, e.g. at a computer station other than the one designated for that purpose, and for any damages connected therewith.

5. User's risk

5.1. The User guarantees that he has the legal capacity to conclude and perform the Agreement.

5.2.The User acknowledges and agrees that all the risk connected with the use of the Programme in the manner specified in the Agreement and in the instruction manual accompanying the Programme shall be borne by the User, to the greatest extent permitted by the provisions of law. Moreover, in the event that circumstances arise which prevent the operation of the Programme – unless a direct cause of such circumstances are the reasons attributable to the Programme – the User should immediately notify the Producer thereof, under the pain of exclusion of any liability of the Producer thereunder. The User acknowledges that installation of the Programme should be made by the Installer.

5.3. The Producer may control the manner of using the Programme by the User in terms of its compliance with the provisions of the Agreement and intended use of the Programme.

5.4. The Producer may additionally control whether there were any attempts to remove or evade technical protections of the Programme. Should the inspection disclose that the User has a computer programme used solely for removing protections, the Producer may claim destroying such a Programme.

5.5. If the Producer has legal interest in obtaining the User's statement that they use the Programme on the basis of the Agreement, they may request from the User to issue such a statement.

5.6. The name and logo of the Programme are subject to legal protection on the basis of relevant regulations. The User without prior written consent of the Producer is not entitled to record, multiply or distribute intangible goods referred to in the previous sentence, either in full or in part, by any means and in any form.

6. Settlement of disputes

6.1. The Parties undertake to settle any disputes which may arise in connection with the performance of the Agreement in an amicable manner.

6.2. In the event that the Parties are unable to settle a dispute resulting from the Agreement in an amicable manner, the Parties shall subject themselves to the Polish law as the law governing the settlement of any disputes, which shall be referred by them for settlement to a court having jurisdiction over the registered office of the Producer.

7. Copyrights and Neighbouring Rights

A breach of Copyrights and Neighbouring Rights of the Producer may entail civil and penal liability of the entity breaching such rights.

8. Remuneration

8.1. Under the Producer granting to the User license in accordance with the Agreement, the User has made one-time lump-sum license fee when purchasing the license to the Software.

8.2. The amount of remuneration indicated in passage 1 above includes also remuneration for transfer of ownership of the Programme carrier/carriers and the Key.

9. Final provisions

9.1. The Producer may transfer his rights to the Programme or its part to any third parties of his choice, without an obligation to notify the User thereof.

9.2. The User may not transfer his rights granted hereunder to any third parties without the consent of the Producer.

9.3. Any amendments to this Agreement shall require a written form, under a pain of nullity.

9.4. The Parties declare that they have read the text of the Agreement, that they understand it and that they are aware of the scope of their rights and obligations.

10. Partial Invalidity

If any provision of the Agreement is illegal or its purpose is the circumvention of law, it shall be invalid. The remaining provisions of the Agreement shall remain in full force and effect unless it follows from the circumstances that without those invalid provisions, the Agreement would not have been entered into. In such situation, the Parties agree to enter into negotiations in order to replace invalid provisions by provisions fulfilling possibly the most similar economic goal.

NMS ACCESS CONTROL