PERCo

PERCo-Web ACS Software

PERCo-WS

«Standard software package»

ADMINISTRATOR MANUAL

Software version: 1.3.0.16

CONTENT

1 Introduction

This *«Administrator Manual»* (hereinafter - Manual) is designed to provide information about technical capabilities, main technical characteristics, princip of operation and special aspects of tweakage of ***PERCo-Web*** access control system (hereinafter - system).

The manual is intended to use by administrators of the system, LAN administrators, hardware and software support division engineers.

The manual contains the description of terms, used in the system specification, the list of supported equipment, PC and Ethernet requirements for the system installation.

This manual should be used with *«User manual»* ***PERCo-Web*** system software.

> ***Important:***
> Service documentation for the equipment and software of ***PERCo-Web*** system is available in electronic format on ***PERCo*** website, at the following URL: www.perco.com, in **Support> Downloads** section.

Used abbreviations:

WKS – workstation;
DB – data base;
OD – operating device;
ACP – access control point;
RC – remote control;
PC – personal computer, notebook;
SW – software;
ACM – access control mode;
ACS – access control system;
DBMS – data base management system;
WTL – work time logging.

2 Purpose

PERCo-Web security system (hereinafter - system) is meant to be used in commercial facilities, institutions, banks, business-centers, medical, educational institutions. The system performs following tasks:

- Access control system automation at the facility territory, including:
  - Unauthorized access protection from unauthorized outsiders.
  - Assignment of access privileges of staff and visitors to administrative premises,
  - Arrangement of WKS for security staff members who are responsible for carrying out verification procedures of employees and visitors, including usage of video camera and biometric technologies.
- Improvement of the facility efficiency, including:
  - Employees Work Time Logging automation,
  - Automation of labor discipline violation control,
  - Arrangement of different specialization WKS for monitoring departments, staff, access control departments, accounts departments.

3 Main features

- Data transfer between WKS, DB and system equipment is executed over *Ethernet* network. It allows to use an existing IT-infrastructure of the facility during the system deployment.
- System server, DB server and all required elements are installed on one PC that is connected to the *Ethernet* network. No additional software installation required. Computer access is organized remotely via Web-interface of the system server.
- Permanent connection of controllers with server is not required. Access privileges data of cardholders is send to nonvolatile memory of every controller. Every event is registered in the controller's memory. After connection reactivation all events data is sent to system DB.
- It is possible to upgrade the firmware of the controller over the *Ethernet*.
- The system could be easily extended by adding additional controllers (ACP) and WKS with their integration in existed system.
- Adding WKS is a simple process of adding a new operator and giving him access permissions to sections and sub-sections of the system software.
- System software allows you to personalize WKS operator's privileges. Permissions are given to operators individually: for sections, sub-sections, equipment, premises, departments etc. However, WKS is connected to operator account, not to the certain PC.
- The system supports biometric technologies, manufactured by **Suprema** company. Fingerprint scanning, if needed, fills up the standard method of ID card verification and allows to improve system safety throughout facility territory and prevents the passage of employees by presenting another person's ID card.
- **Mifare** cards can be integrated into the system. This type of cards is widely-spread over the world and allows to organize access control and personal data protection on a high level.
- The system uses **NFC** (Near Field Communication for wireless data transmission) technology to emulate proximity cards. The passage and access are done by using a smartphone with **NFC** technology.

4 Configuration and system operation principal

The system consists of the following elements (see figure *«Structural configuration of PERCo-Web system»*):

System server

System software includes: server, videoserver, system DB and additional software. Every employee and visitor gets personal identificator that has unique number and this data is stored in the system DB. ID card and/or biometric data (fingerprints) act as identificator. Configuration and management is performed via the system server Web-interface.

ACP

ACPs are equipped with controllers, ID card readers, OD (turnstiles, locks, swing gates etc) and additional equipment (RC, Soundization, emergency escape device (*FireAlarm input*), card readers, IP-videocameras, biometric equipment etc). All ACPs are connected to each other and to the server PC over *Ethernet*.

Possible variants of operating ODs at ACPs:

- Manual operating – operator of the ACP uses RC.
- ACP operator uses PC and sets the OD direction for using one of the access control modes (ACM): *«Open», «Closed», «Consider»*. It allows, if needed, to organize free passage in chosen direction or completely block it. ACM *«Consider»* is used for passage by ID cards and/or fingerprints scanning.
- Automatic - ACP Considerler Considers passage by ID cards and/or fingerprints scanning. ACM *«Consider»* has to be used in the passage direction. Actions of the ID card owner at the ACP:
  - in case of ID card verification - present card to reader;
  - in case of fingerprints scanning verification – proceed with a fingerprint scanning procedure;
  - in case of ID card and fingerprints scanning verification – present a card to reader and proceed with a fingerprint scanning procedure.

  By virtue of analysis of card number and/or biometric data and owner's privileges, the controller decides whether to grant or deny access by sending relevant commands to OD. Every ID card presentation event and/or fingerprints scanning event is registered in the DB, indicating place and time of presentation/scanning. It allows the system to keep an eye on the card owner, check the residence time and moving around the facility.

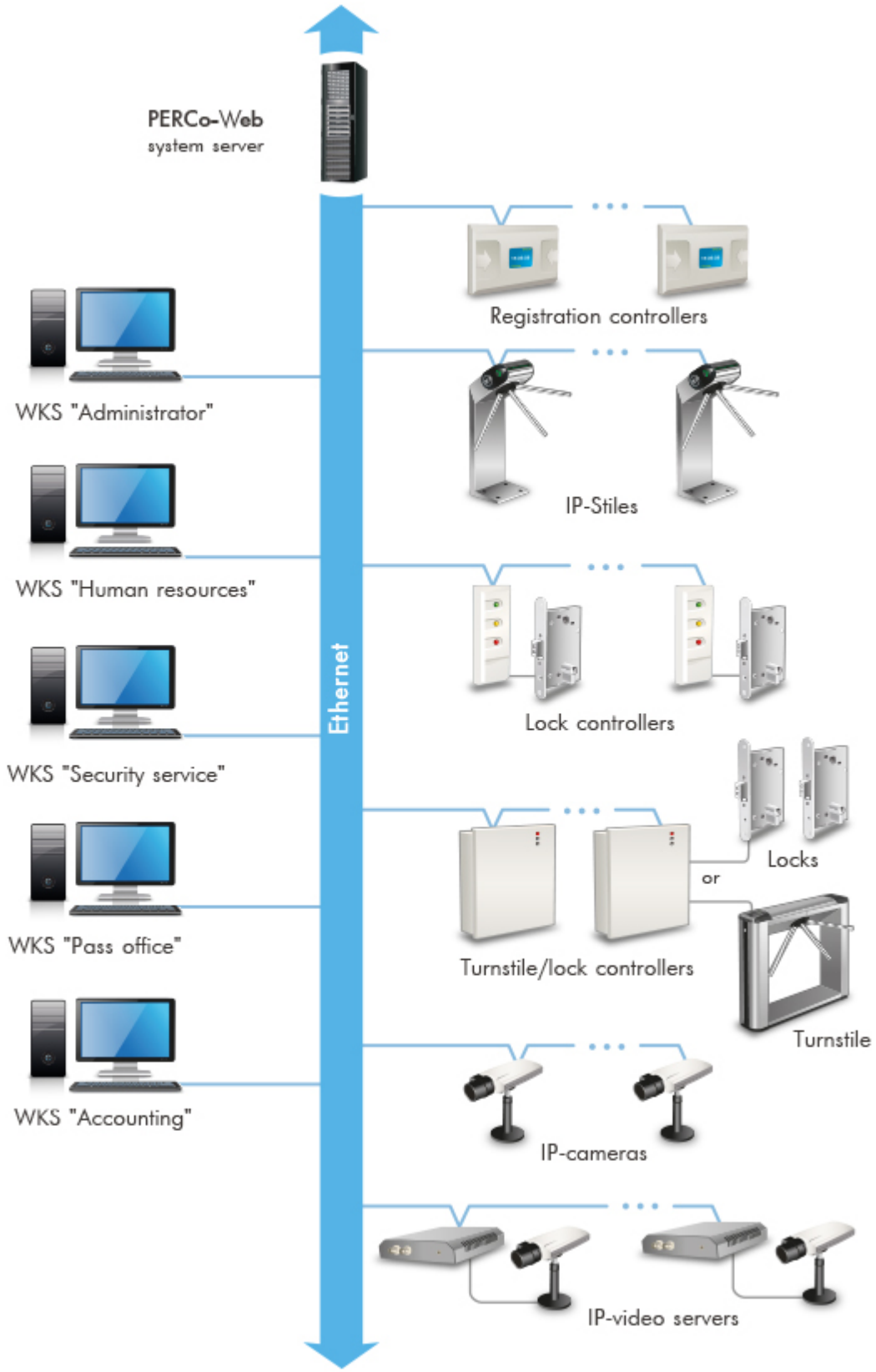
Verification procedure that is performed by ACP operator helps to improve the control of access at the facility. It is also possible to perform a verification procedure by means of IP-videocameras (IP-servers with videocameras), that are connected to the system. The system software includes a video server for this purpose.

WKS

WKS are organized on the remote PCs that are connected to the system server. WKS organization within the system involves giving access permissions to operators for using sections and sub-sections of the system

software. Operator is only able to use those sections and sub-sections that his account has permission for. Possible WKS organizations on the remote PCs:

- *«Administrator»* (section ***«Administration»***),
- *«Human resources»* (section ***«Staff»***),
- *«Security service»* (sections: ***«Access control», «Pass order», «Verification»***),
- *«Pass office»* (section ***«Pass office»***),
- *«Accounts department»* (section ***«Time & Attendance»***).



PERCo-Web system architecture

5 Supported hardware

Important:
Operating documentation for the system hardware is available in electronic format on ***PERCo*** website, URL: www.perco.com, section ***Support> Download***.

Door operating controllers

Doors are equipped with lock controllers that are used with electromechanical or electromagnetic locks. It is possible to use locks (strike plates) produced by ***PERCo*** or a third party manufacturer. ***PERCo*** produces the following door controllers:

CL05 helps to organize one ACP for the passage control in one direction. The controller is equipped with HID, EM-Marine card reader and LED display module.

CL05.1 Allows you to organize one ACP for the passage control in one direction. Two controllers of this type allow you to organize ACP for bidirectional passage control. Controller is equipped with build in *HID, EM-Marine* card reader and LED indication module.

CL05.2 Allows to organize one one-way entry point or one two-way entry point when using two of these controllers. The controller has a built-in HID, EM-Marine card reader and a LED indication block. CL05.2 version of the controller can now store up to 230 000 events in the registration log, it is possible to use unlimited amount of double-checking cards, the Web-interface has also been improved.

CT/L04 *«Controller for operating one two-sided door»* operation mode allows you to organize one ACP for the bi-directional passage control. *«Controller for operating two two-sided doors»* operation mode allows you to organize two ACPs for one direction passage control which correspondingly operates one or two ODs. Remote-mounted readers are connected to the controller over *RS-485* interface.

CT/L04.2 2 Allows to organize two two-way entry points or four one-way entry points in this case controlling two or four ODs correspondingly. Upon that, additional external readers are connected to controller via RS-485 interface.

CL201.x connects as a second level controller to ***CT/L04, CT/L04.2*** or to built-in IP STILE ***CT03, CT03.2*** controller over *RS-485* interface and allows to organize one ACP for the passage control in one direction. Controller is equipped with built-in *HID, EM-Marine* card reader and LED indication module. It is possible to connect up to 8 second level controllers simultaneously to the first level controller.

Important:
Connections of the second level ***CL201.x*** controllers to ***CT/L04.2, CT03.2*** controller must be done via Web-interface of the ***CT/L04.2, CT03.2*** controller. Configuration parameters of the connected controllers will become available via ***PERCo-Web*** interface.

Turnstile main controllers

Controllers are used for operating turnstiles or swing gates manufactured by ***PERCo*** or by a third party manufacturer. ***PERCo*** produces the following types of turnstile controllers:

CT/L04 *«Controller for operating a turnstile»* mode allows you to organize one ACP for bi-directional passage control. Built-in card readers or optional remote-mounted readers are connected to the controller over *RS-485* interface.

CT/L04.2 Allows to organize one two-way entry point. In this case, the built-in controllers of the turnstile, additional external readers or ODs (locks) are connected to the controller via RS-485 interface.

CT03, CT03.2 Built-in controller comes with IP STILE and allows you to organize one ACP for the bi-directional passage control.

Registry controller

CR01 LICON Controller is designed for organization the work time logging terminal and labor discipline control. It is equipped with two built-in *HID, EM-Marine* card readers and LCD display. The controller doesn't support OD operating.

CR01.2 LICON has two built in HID, EM-Marine card reader and LCD (display). The controller is used for organization the work time logging terminal and labor discipline control (The controller doesn't operate ODs). CR01.2 LICON version of the controller can now store up to 50 000 access cards, the Web-interface has been improved.

OD – Lock

- ***LB*** and ***LBP*** series of electromechanical locks with contact block;
- ***LC*** series of electromechanical locks;
- Third party electromechanical and electromagnetic locks.

OD – Turnstile

- Tripods series ***T*** and ***TTR***;
- Box tripods series ***TTD, TB*** *and* ***TBC***;
- Rotor turnstiles series ***RTD***;
- Turnstiles – ***ST*** series speed gates
- Third party turnstiles.

OD – Swing Gate

- Electromechanical semi-automatic swing gates series ***WHD***;
- Electromechanical automatic swing gates series ***WMD***;
- Third party swing gates.

Readers

It is possible to use *HID, EM-Marin* or *MIFARE* card readers. External readers are connected to controllers over *RS-485* interface. It is necessary to use ***AC02*** interface converter in order to connect readers with *Wiegand-26, 34, 37, 40, 42* interface.

As an external reader it is possible to use:

- ***IR, MR*** series readers that are equipped with LED indication;
- ***IRP01*** reader post with an LCD display.

USB connection is accomplished by ***IR05*** readers that are used for *HID, EM-Marin* cards and ***IR08, MR08*** used for *MIFARE* cards.

IP-Stiles

IP STILE is a set of equipment, more specifically OD, card readers and built-in controller that allows you to organize ACP for the bi-directional passage control. It is possible to install *HID, EM-Marin* or *MIFARE* card reader in IP STILE.

- ***KT02, KT08*** – IP STILE series is based on tripod turnstiles;
- ***KT05*** – IP STILE series is based on box tripod turnstiles;
- ***KTC01*** – IP STILE series is based on box tripod turnstiles with built-in card capture reader.

Control devices

H6/4 – wired remote control (RC) is designed for ODs autonomous control. With the help of RC, operator is able to issue command of unblocking the OD for a single pass, set free passage mode or to block OD. RC is equipped with LED and audible indication. RC is included in swing gates, turnstiles and IP STILE supply packages. Everything is manufactured by ***PERCo***.

Radio control device (RCD) – is designed for OD autonomous control. The supply package contains the receiver that is connected to OD and breloque-transmitters with range capability up to 40m. With the help of RCD, operator is able to issue commands of unblocking OD for a single pass, set free passage mode or to block OD.

AU01 – IR-remote control that is used to remote OD control. It allows operator to change ACM and passage direction, unblock OD for a single passage. It is possible to use IR-remote control with ***CT/L04*** and ***CT/L04.2*** controllers. ***AI01*** IR-receiver detects IR signal. IR-receiver must be connected to the controller over *RS-485*.

RC «Exit» button – is intended for manual operation of OD when organizing ACP for the passage control in one direction (example: exit door opening). It is possible to use any non-locking button with normally open «dry» contacts.

SUPREMA controllers

For the purpose of biometric technologies implementation in the ***PERCo-Web*** system, it is possible to install ***Suprema*** controllers for simultaneous usage with ***PERCo*** controllers. Usage of ***Suprema*** access controllers allows you to tighten access control at the facility.

- ***BioEntry Plus*** – biometric access controller that connects over Ethernet and uses TCP/IP protocol.
- ***BioEntry W2*** – biometric access controller in durable metal dust-and-moisture proof housing that connects over Ethernet and uses TCP/IP protocol.
- ***BioEntry P2*** – biometric access controller proof housing that connects over Ethernet and uses TCP/IP protocol.
- ***BioMini*** – series of desktop fingerprint readers that uses USB interface.

Important:
For integration biometric controllers should have inner software ("firmware") version not less than:
for controller BioEntry W2 – 1.1.1;
for controller BioEntry Plus (platform BioStar 2) – 2.3.1.

There are two ways of connection of the above mentioned controllers to the system:

- As a controller for a one-sided lock. In this case, the OD should be connected directly to the control output of the Suprema controller. System connection with the Suprema controller is established via Ethernet interface,
- As a fingerprint reader when operating one direction of a two-sided lock (turnstile). In this case the Suprema controller should be connected to ***CT/L04*** or ***CT/L04.2*** controller via Wiegand interface and by using ***AC02*** interface converter.

Additional equipment

Card capture readers:
- ***IC02, IC05*** card capture readers series;
- Third party card capture readers series.

AU05 – system time display. Connects to ***CT/L04, CT/L04.2*** and ***CT03, CT03.2*** controllers over *RS-485* interface.

PDS – passage detection sensor is designed to register unauthorized passage under barriers.

Alarm – sound alarm.

Videocameras

The system supports IP-videocameras and analog videocameras connected to the IP-videoservers.

Important:
The list of supported models of IP-videocameras can be found in **Camera templates** tab, subsection **«Administration»** of the «Verification» section.

6 Main technical characteristics

Interface standard	*Ethernet (IEEE 802.3)*
Data transmission rate Ethernet, Mb/s	10/100
Number of controllers of ACS	no more than 512
Passage intensity with zonality change, pass/seconds	
50000 cards controllers	no more than 50
10000 cards controllers	no more than 200
ID cards format	*HID*, *EM-Marin*, *Mifare*
ID cards total number, pcs.	Less than 100 000
visitors temporary cards among them:	Less than 50 000
Number of events per controller	Less than 140 000
Number of control zones	No more than 1024
Number of access criteria	
Time zone (up to 4 time intervals)	No more than 255
Week schedule	No more than 255
Daily flextime (within 30 days period)	No more than 255
Weekly access criteria flextime (within 54 weeks period)	No more than 255
Number of special status days, holidays (up to 8 types)	No more than 365

The amount of PERCo memory for storing log IDs and events

Controller	Configuration option	Cards number	Events number
CL201.1	Second level lock controller	up to 1 000	-
CR01 LICON	T&A controller	up to 5 000	up to 140 000
CL05.1	Lock controller	up to 50 000	up to 135 000
CT/L04	Controller for 1 double-sided door	up to 50 000	up to 135 000
	Controller for 1 one-sided doors with connection of up to 8 ***CL201*** lock controllers	up to 10 000	up to 135 000
	Controller for 2 one-sided doors with connection of up to 8 ***CL201*** lock controllers	up to 1000 for each lock	up to 135 000

Controller	Configuration option	Cards number	Events number
CT/L04, CT03	Turnstile controller	up to 50 000	up to 135 000
	Turnstile controller with connection of up to 8 ***CL201*** lock controllers	up to 10 000	up to 135 000
CT/L04	Vehicle checkpoint controller	up to 50 000	up to 135 000
	Vehicle checkpoint controller with connection of up to 8 ***CL201*** lock controllers	up to 10 000	up to 135 000
CR01.2 LICON	T&A controller	up to 50 000	up to 125 000
		up to 40 000	up to 280 000
		up to 30 000	up to 440 000
		up to 20 000	up to 600 000
		up to 10 000	up to 760 000
CL05.2	Lock controller	up to 50 000	up to 230 000
		up to 40 000	up to 390 000
		up to 30 000	up to 550 000
		up to 20 000	up to 710 000
		up to 10 000	up to 870 000
CT/L04.2	Multipurpose turnstile / lock controller	up to 50 000	up to 230 000
		up to 40 000	up to 390 000
		up to 30 000	up to 550 000
		up to 20 000	up to 710 000

Controller	Configuration option	Cards number	Events number
		up to 10 000	up to 870 000
CT03.2	IP-stile in-built controller	up to 50 000	up to 230 000
		up to 40 000	up to 390 000
		up to 30 000	up to 550 000
		up to 20 000	up to 710 000
		up to 10 000	up to 870 000

Important:

- Exceeding the passage intensity might cause errors of Antipass function.
- ***CL201.x*** second level controller events are stored in the first level memory of the controller.

Number of connections:

IP videocameras	No more than 512
IP videocameras per one videoserver	No more than 64
Software videoservers	No more than 8
Video capture frequency, frames/seconds	No more than 2
Number of verification points in one template	No more than 4
Number of verification templates	No more than 512

Important:

Every verification point can transmit signal from one camera.

7 Hardware and software requirements

System server hardware requirements

Minimal system requirements:

- CPU: *Intel Core i5* (not less than 3.2 GHz),
- RAM: 4 Gb,
- HDD: 10 Gb.
- Graphics card, monitor with screen resolution 1280x1024 px.
- Network: *Ethernet* (IEEE 802.3) 10-BaseT, 100-BaseTX.

System server software requirements

The system runs under licensed *Microsoft Windows OS*. It is possible to use 64-bit version of OS.

- It is recommended to use *OS Windows Server: 2008 R2, 2012 R2, 2016.*
- It is possible to use *OS Windows: 7, 8.1, 10.*

The system is operated via following web-browsers:

- *Microsoft IE* version 10 or higher;
- *Google Chrome* version 32 or higher;
- *Mozilla Firefox* version 32 or higher;
- *Opera* version 30 or higher;
- *Microsoft Edge.*

WKS Hardware requirements

PC has to satisfy the following minimal technical requirements:

- CPU:
  - Minimum: *Intel Celeron* (2 CPUs, frequency not less than 1.8 GHz),
  - Recommended: *Intel Core i3* (2 CPUs, frequency not less than 1.8 GHz).
- RAM:
  - Minimum: 2 Gb,
  - Recommended: 4 Gb.
- Graphics card, monitor with screen resolution 1280x1024 px.
- Network: *Ethernet* (IEEE 802.3) 10-BaseT, 100-BaseTX.

WKS software requirements

The system runs under licensed *Microsoft Windows OS* or *Apple Mac OS*. It is recommended to use OS: *Windows 7, 8.1, 10; MacOS X* or higher.

One of the following web-browsers is required for operating the system:

- *Microsoft IE* version 10 or higher;
- *Google Chrome* version 32 or higher;
- *Mozilla Firefox* version 32 or higher;
- *Opera* version 30 or higher;
- *Microsoft Edge*;
- *Apple Safari 9* or higher.

8 System setup

One of the system controllers is used as a *software license key*. Functioning as a *license key* doesn't affect a controller's main function. Controller that is used as a *license key* must be added to the system configuration in ***«License»*** subsection of the ***«Administration»*** section.

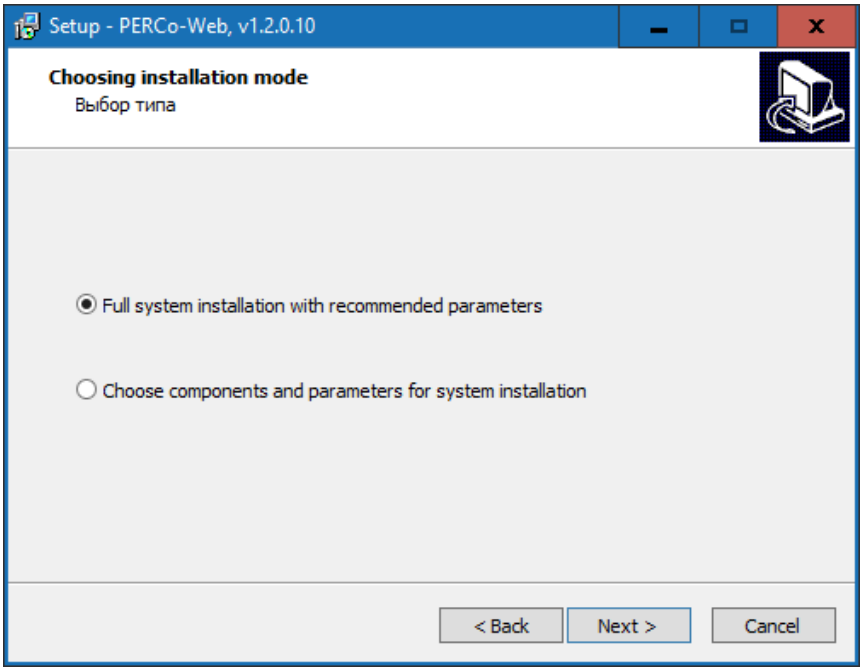
Important!

An additional configuration of the *Windows firewall* might be needed for correct operation of the system server.

Follow the described sequence of actions during the installation process:

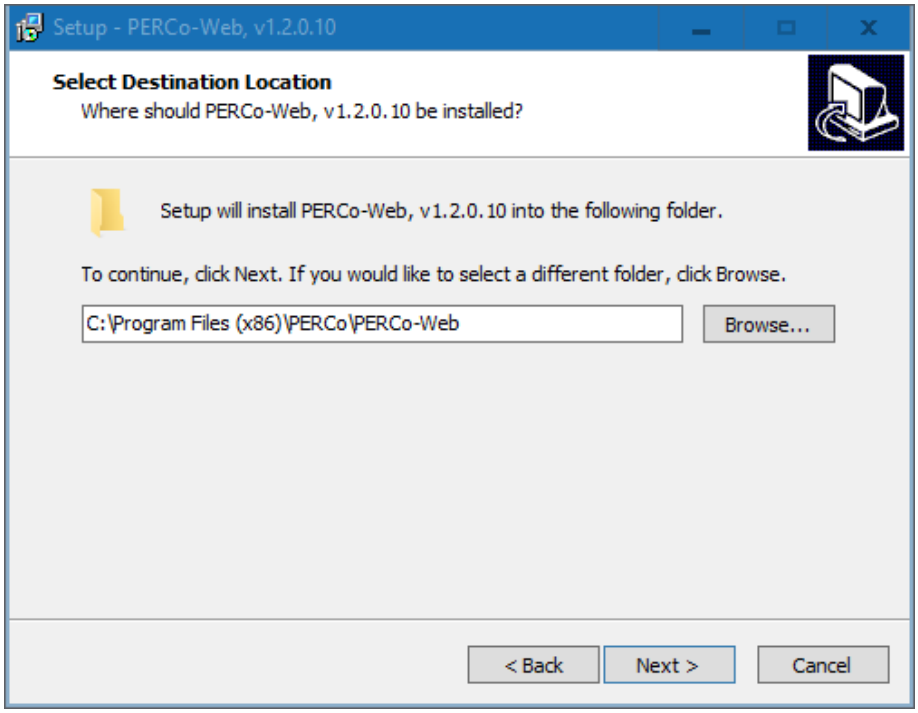
1. Launch `Setup.exe` installation file. Follow the instructions of setup wizard. The most recent version of *«PERCo-Web»* installation file is available at ***PERCo*** web-site, at the following URL www.perco.com in the **Support> Software** section.
2. Choose the type of installation. If you don't want to choose components and set the system network parameters, then proceed with **Full system installation with recommended parameters,** otherwise – **Choose components and parameters for system installation.** Click **Next**.

   Window overview:



3. Specify the installation folder. Click **Next**.

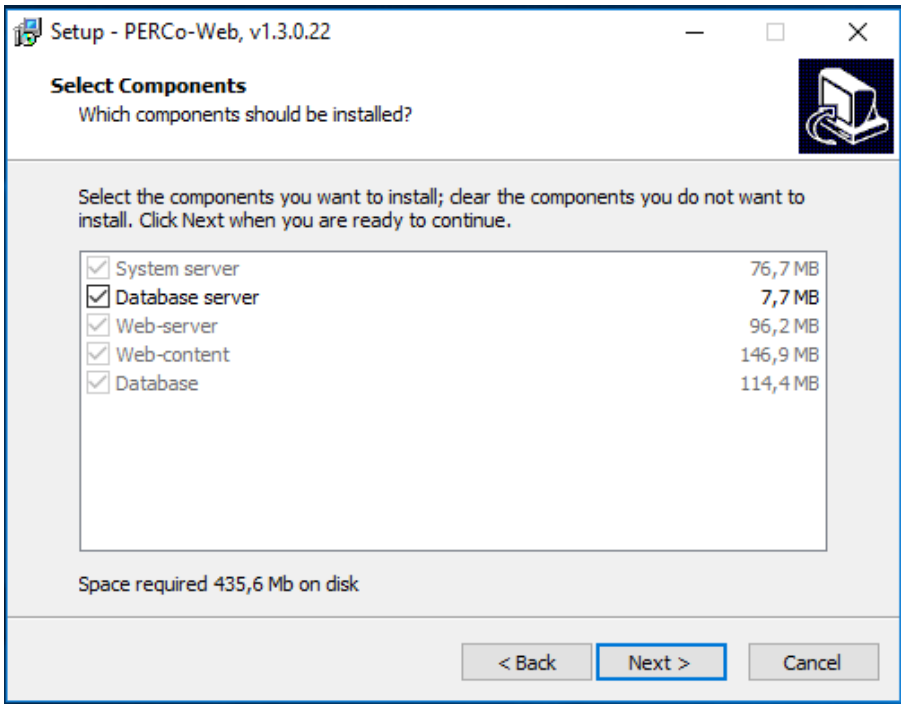
Window overview:



4. Use the checkboxes and choose system components which you would like to install. Click **Next**.

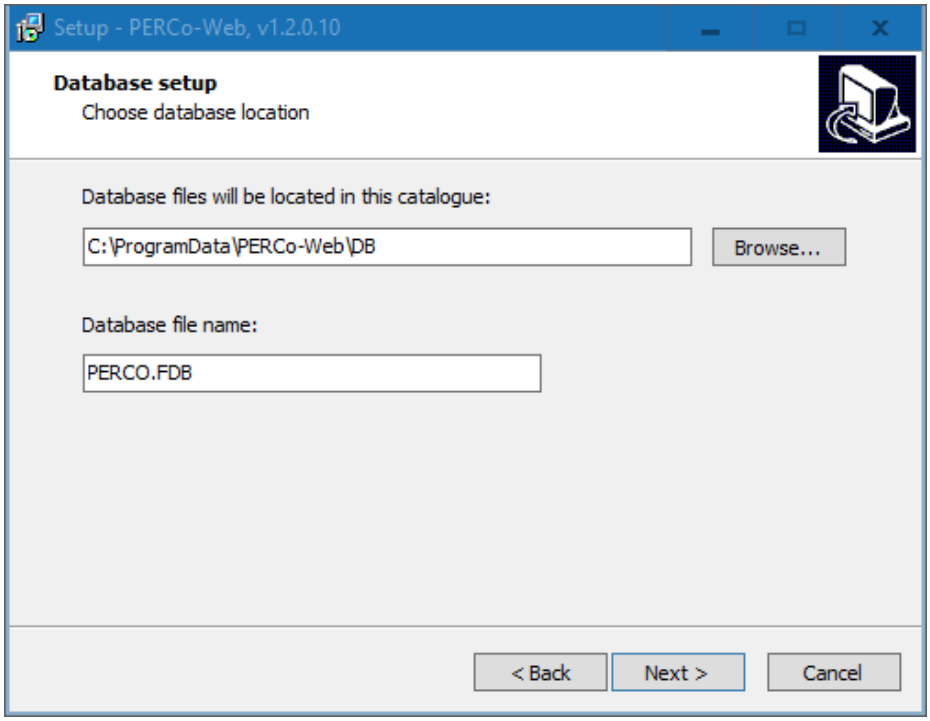
Important:
If **Database server** is checked, then SQL standard setup wizard of *Firebird* and *Firebird ODBC Driver* will be launched.

Window overview:

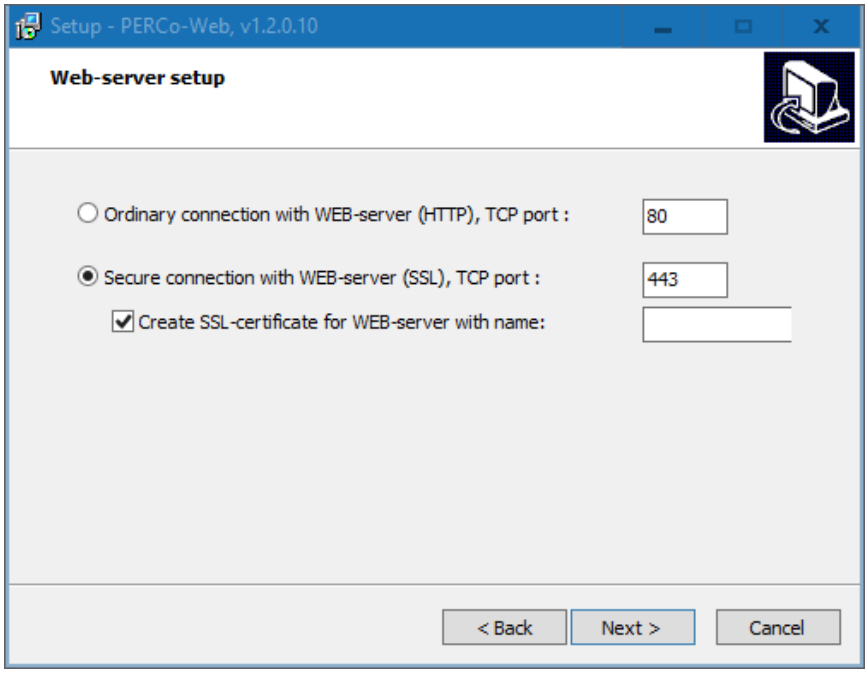


5. Specify the Database location folder. Click **Next**.

Window overview:

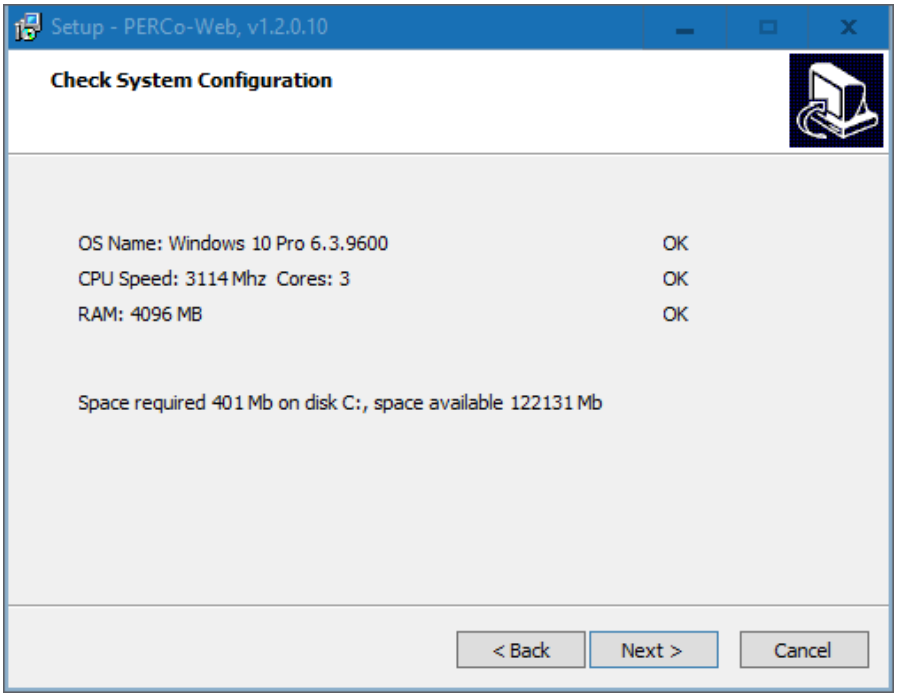


6. Configure network parameters of the server. Click **Next**.
Window overview:

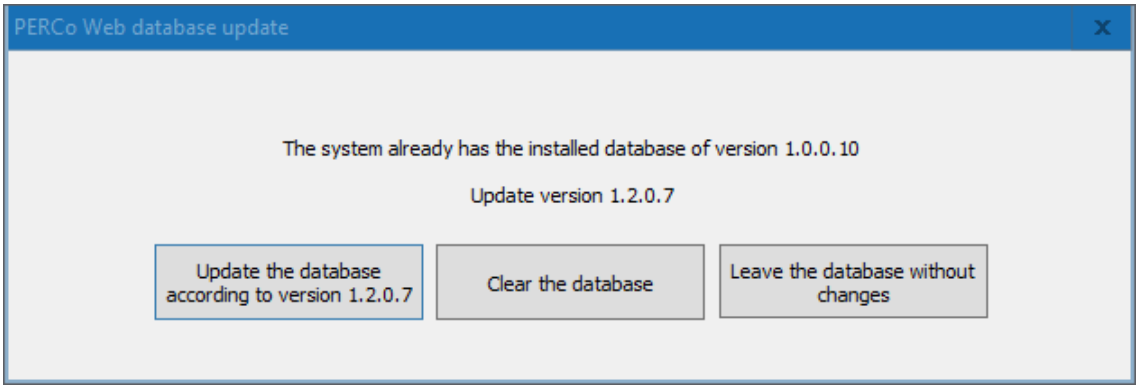


7. System configuration check will be performed. Click **Next** button when it's finished.

Window overview:



8. System installation will start. After completion a new DB will be automatically created in the specified directory. If the specified directory contains previously created DB, then the ***Database Upgrade*** window will appear:



9. In the appeared window push one of the following buttons:

- **Upgrade the database**
- **Clear the database**
- **Leave the database without changes**

10. Purchase software license if needed.

Important:
Use standard *MS Windows* «Add or remove programs» component for complete uninstallation of all system modules. To launch a component: go to **Start> Settings> Control Panel> Add or remove programs**. In the opened window select *«PERCoWeb»* and click **Remove** button.

9 License management

System software consists of ***«Standard software package»*** module and additional software enhancement modules. The software can be purchased both as a bundle of modules, and as a separate modules. Functioning of additional modules is possible only with the ***«Standard software package»***. The following modules are available for purchase:

- ***WS «Standard software package»*** – allows you to organize fully functioning ACS that provides all main safety functions, including: access control by time, zonality control (antipass), double check access.
- ***WM-01 «Working time logging»*** – allows you to register employees working time and generate labor discipline reports.
- ***WM-02 «Verification»*** – allows you to improve access control at the facility by ACP operator who performs the verification procedure.

From the first start, the software works in a 60 days trial mode for adaptation purposes and simplification of the purchase procedure. All software functionality capabilities are available.

Access to optional software modules will be denied after expiration of the trial period. If the license wasn't purchased, ***«Standard software package»*** will merge into free ***WB «Basic software package»*** with the following restrictions:

- ID cards amount will be limited to first 100 registered;
- Data entry and visitor's card issue options will be unavailable.

Upon that, all previously entered data will be stored in DB and will become available after you purchase ***«Standard software package»*** license.

One of the system controllers is used as a software license key. Functioning as a license key doesn't affect a controller's main function. Controller that is used as a license key must be added to the system configuration in ***«Configuration»*** subsection of the ***«Administration»*** section.

All licensed software modules will function for 30 days in case of connection loss between the key-controller and the system server. Access to all software sections will be blocked except for the ***«Administration»*** license code activation section, if the connection is not restored in the above mentioned period. All previously entered data is stored in the system DB and will become available after the connection is restored.

PERCo-Web software modules structure

Software module	Included sections
WB «Basic software package»	The number of cards is limited – up to ***100.*** Sections: ***«Staff»***, with subsections: • ***«Employees»***, • ***«Departaments»***, • ***«Positions»***; ***«Pass office»***, with subsections: • ***«Employees»***, • ***«Access templates»***; ***«Access control»***, with subsection: • ***«Device management»***; ***«Administration»***, with subsections: • ***«Configuration»***, • ***«System events»*** • ***«Tasks»***, • ***«Operators»***, • ***«Roles and permissions»***, • ***«Licenses»***
WS «Standard software package»	All sections included in **«Basic software package»**, and also added: sections ***«Pass order»***, in section ***«Staff»*** subsection is added: • ***«Additional data»***; in section ***«Pass office»*** added subsections: • ***«Visitors»***, • ***«Card design»***, • ***«Visitors report»***; in section ***«Access control»*** added subsections: • ***«Passage report»*** and • ***«Room access report»***
WM-01 «Working time logging»	All sections included in **«Basic software package»**, and also added: sections ***«Time & Attendance»***, with subsections: • ***«Worked time log»***, • ***«Supporting documents»***, • ***«Discipline report»***; in section ***«Staff»*** subsection is added: • ***«Work schedules»***; in section ***«Access control»*** subsection is added: • ***«Location»***

PERCo-Web software modules structure

Software module	Included sections
WM-02 «Verification»	All sections included in **«Basic software package»**, and also added: sections ***«Verification»***, with subsections: • ***«Verification»***, • ***«Verification configuration»***; in section ***«Access control»***, subsection is added: • ***«Verification log»***

Software purchase procedure

To purchase a license code:

1. Choose one of the previously purchased ***PERCo*** controllers that will be used as software electronic protection key.
2. Fill in the system software order form. The form is available at ***PERCo*** website, at the following URL www.perco.com, section ***Support> Software> PERCo-Web software> Licensing procedure of PERCo-Web or Catalogue> Access control system PERCo-Web> Software> SOFTWARE PERCo-Web> Licensing procedure of PERCo-Web SOFTWARE***. Put the following information in the form:
   - MAC-address of the chosen controller,
   - The list of required modules.
3. After receiving a license agreement that includes modules activation codes, it is necessary to type them in the ***«License»*** subsection of the ***«Administration»*** section.

10 PERCo-Web security system manager

Click on the desktop icon or on the task bar icon to open *«PERCo-Web security system manager»* (hereinafter – *«PERCo-Web Manager»*) window. *«PERCo-Web Manager»* window consists of two tabs:

Status tab is used to:

- start and stop the system server;
- display the list of controllers that are connected to the server.

Database tab is used for:

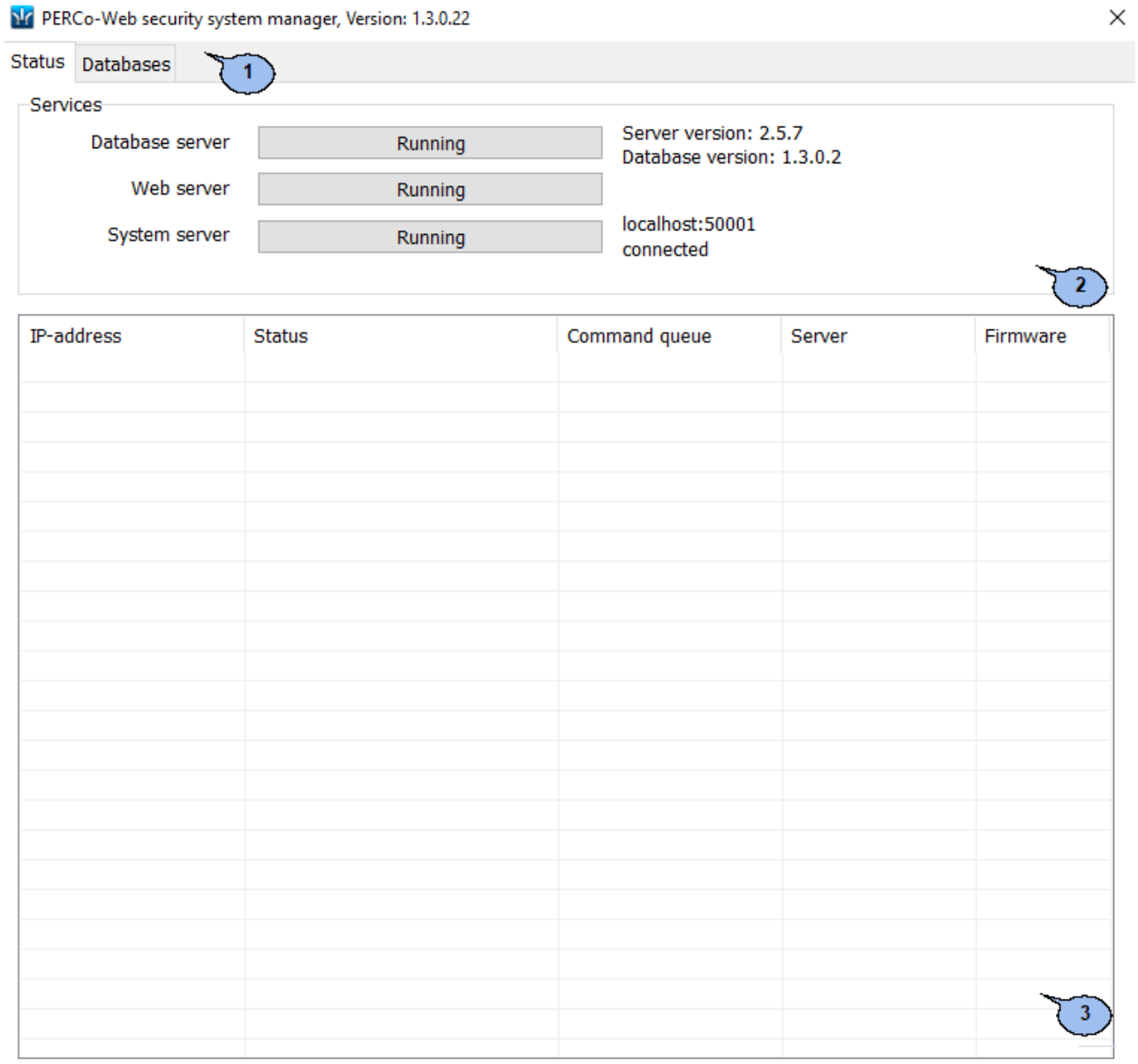
- specifying the path of DB files and DB backups;
- backup system DB;

  Important:
  The system can automatically backup the DB on schedule. Timetable can be created in the ***«Tasks»*** section of the ***«Administration»*** section.

- Restore DB from the backup file;
- Import DB from the earlier versions of DB files.

10.1 System servers management

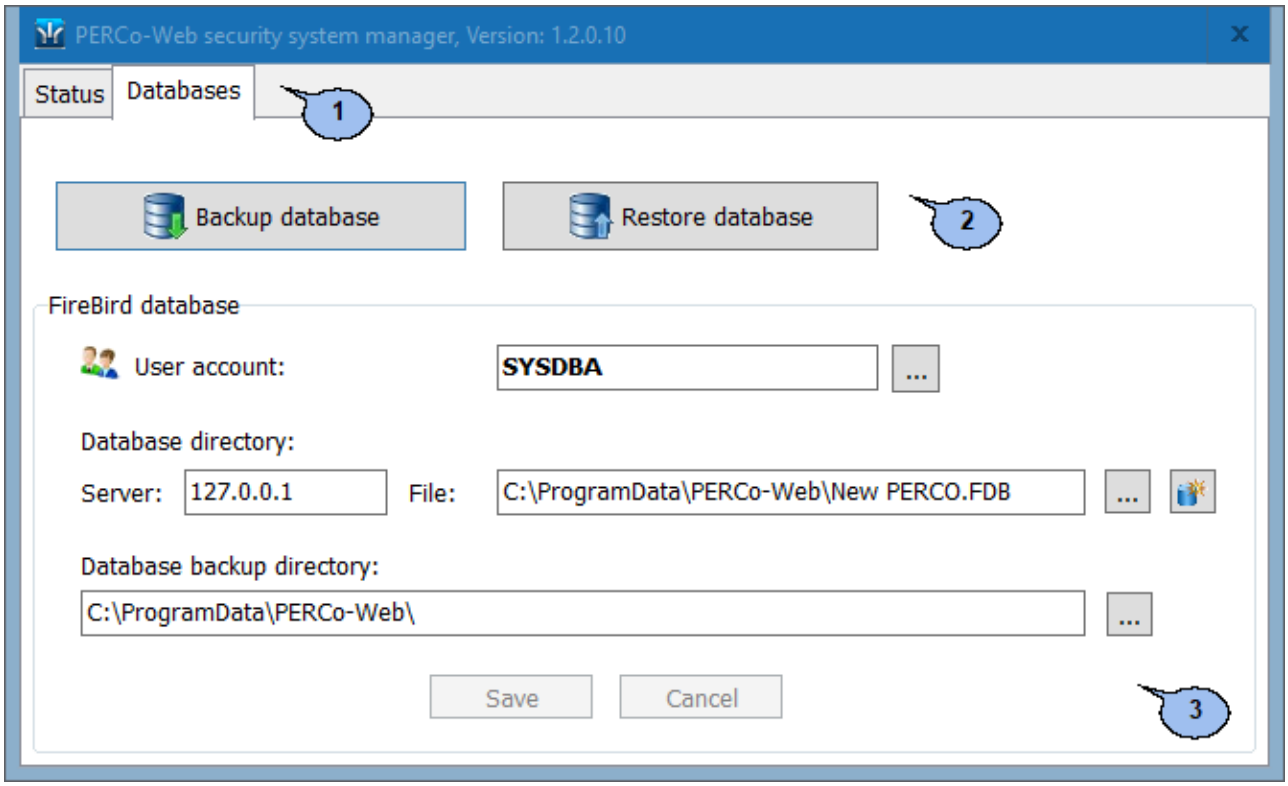
Start and stop of the system servers can be done at **Status** tab of the «*PERCo-Web Manager*» window. Tab overview:



1. Tab selection:
   - **Status**
   - **Databases**
2. The server start and stop buttons can be found on the **Services** panel.
3. Tab operation area includes the list of controllers that are connected to system server.

10.2 DB management

DB management can be performed on the **Database** tab of the *«PERCo-Web manager»* window. Tab overview:



1. Window tab selection:
   - **Status**
   - **Databases**
2. DB Control buttons:
   - **Backup database – use this button to create a database backup.**
   - **Restore database – use this button to restore DB from the previously created backup.**
3. **Fire Bird Database** panel consists of:

   User account: – click this button ... to create a new DB account or select from the previously created.

   Database location:

   Server: – PC IP-address field, where DBMS is installed.

   File: – click this button ... to open the explorer and specify the DB location folder.

   Create new Database – use this button to create a new DB in the specified directory.

   Database archives location: – use this button ... to open the explorer window and specify DB backup location.

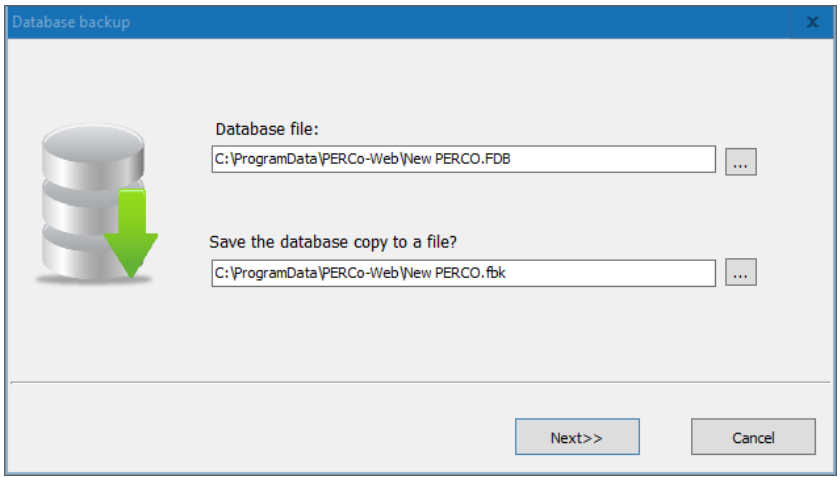
   Save – use this button to save changes.

   Cancel – use this button to cancel changes.

10.2.1 DB backup

To create a DB backup:

1. Launch *«PERCo-Web Manager»*.
2. Select the **Database** tab.
3. Click the **Database backup** button. A **Database backup** window will appear:



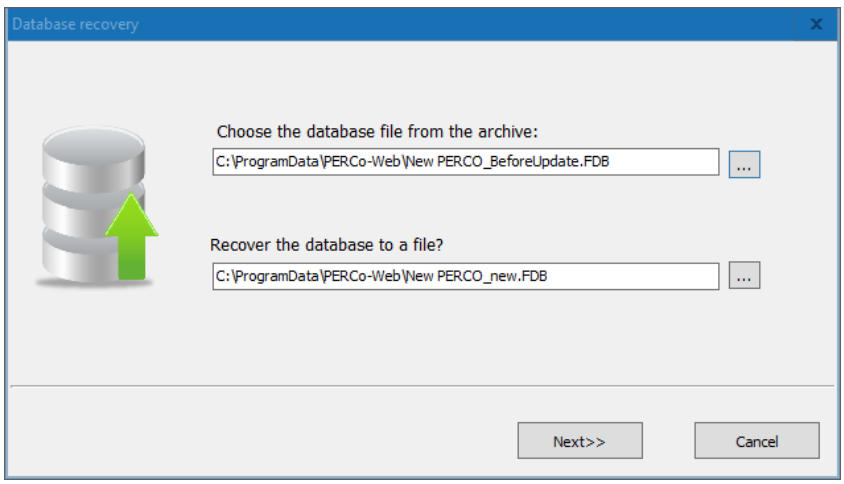
4. Click the button ... of the **Database file** field. In the appeared window specify the DB location folder.

5. Click the button ... of the field **Save the database copy to a file?** . In the appeared window specify the folder, where you would like to save the DB backup. Click **Next**.
6. The DB backup process will start. Click **OK** button after the process is finished. **Database backup** window will close.

10.2.2 Restoring DB from the backup file

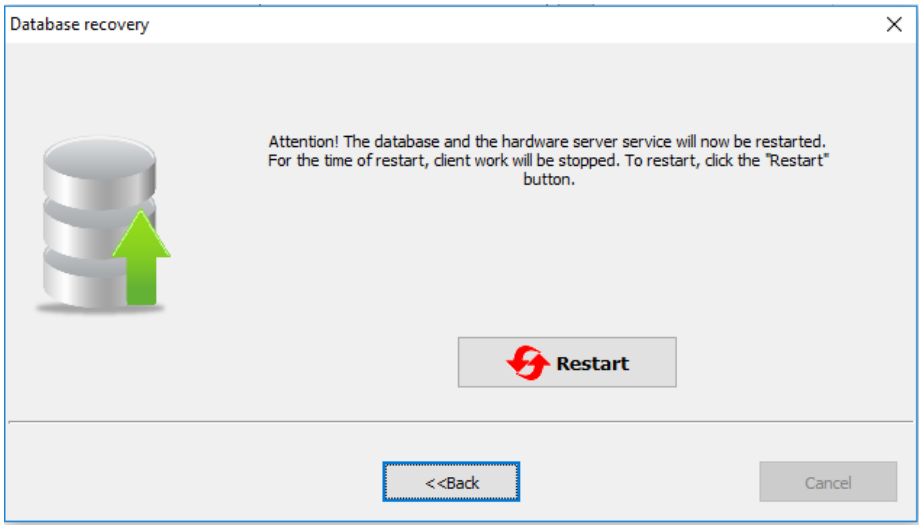
For DB backup creation:

1. Launch *«PERCo-Web manager»*.
2. Select the **Databases** tab.
3. Click **Restore database** button. A **Database recovery** window will appear:



4. Click the button ... of the **Select archived databases** field. In the appeared explorer window choose the DB backup location folder.

5. Click the button ... of the **Select the file to save DB to** field. In the appeared explorer window specify the folder where you would like to save the restored DB. Click **Next**.
6. DB restoration process will start. Click **Next** after the process is finished. A message with the server restart demand and **Restart** button will appear:



7. Click **Restart** button. Click **OK** button after the servers restart process is finished. **Database recovery** window will close. The system server will begin to operate with the restored DB.

11 Prior configuration

Follow the described procedure when performing prior system configuration:

1. Log in, using web-browser. Use the URL bar and type-in the IP-address of the PC where the system server is installed. It is necessary to set a password for the unmodified `admin` account when you first log in.

2. Go to the  ***«Administration»*** section by using the navigation panel.
   - Open ***«Configuration»*** subsection.
     - select the language and date display format;
     - create the list of premises;
     - perform a search and add controllers;
     - place controllers on the premises scheme.
   - Open ***«Roles and permissions»*** subsection, create the desired roles for operators and give permissions to them.
   - Open ***«Operators»*** subsection, create accounts for system operators, apply the previously created roles to them and set access permissions for the sections.

3. Go to the section  ***«Pass Office»*** by using the navigation panel. Open ***«Access templates»*** subsection.
   - Create access templates for employees and visitors. During the creation process you will set individual access permission and time access permissions for every premise.
   - If needed, edit the holidays calendar so the access to the premises will be limited or denied during this period.

4. Go to  ***«Staff»*** section by using the navigation panel.
   - Open ***«Positions»*** subsection and create the list of all company positions.
   - Open ***«Additional data»*** subsection and create fields for additional text and graphic input.
   - Open ***«Work schedules»*** subsection:
     - create time-tables for employees. Set the registered premises and labor discipline report parameters;
     - If needed, edit the holidays calendar (calendar is used for the report generation in ***«Time & Attendance» section***).
   - Open ***«Departments»*** subsection and create the list of business units of the facility. Determine the options for every department which will be automatically applied to its employees and visitors.

5. Go to the  ***«Pass Office»*** section using the navigation panel. Open ***«Card design»*** subsection and create design templates of ID cards for employees and visitors of the facility.

6. Go to the  «Staff» section by using the navigation panel. Open the «Employees» subsection and create the list of employees. For every employee:
   - Fill in the registration card (full name, department, position, Work schedules etc.).

- Add photo.
- Issue an ID card and set the access template.
- Print the card (sticker for ID card).

7. Go to the  ***«Administration»*** section by using the navigation panel. Open ***«Configuration»*** subsection and associate employees to the controllers, whose ID cards will be double checking.
8. Configure the control of personal access parameter functions.

12 Antipass and Global Antipass functions

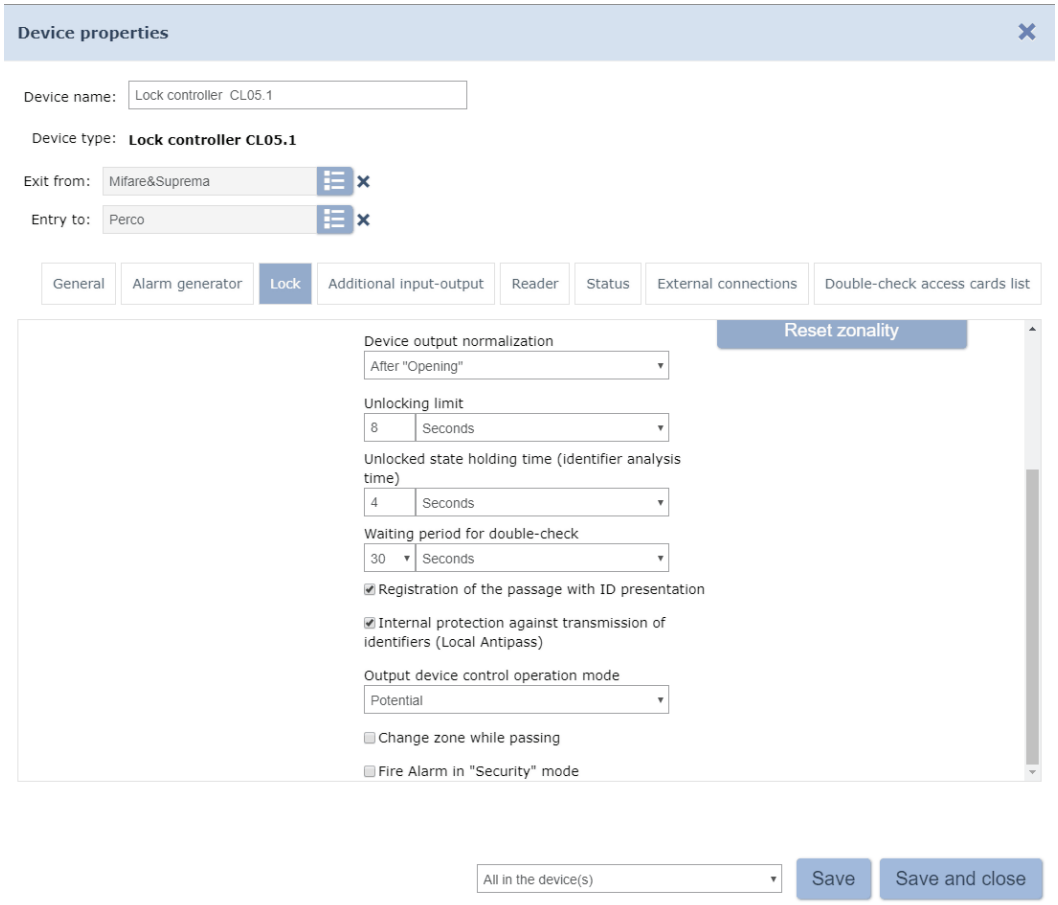
It is possible to switch on/off the control function of ID cards personal access parameters.

Antipass function

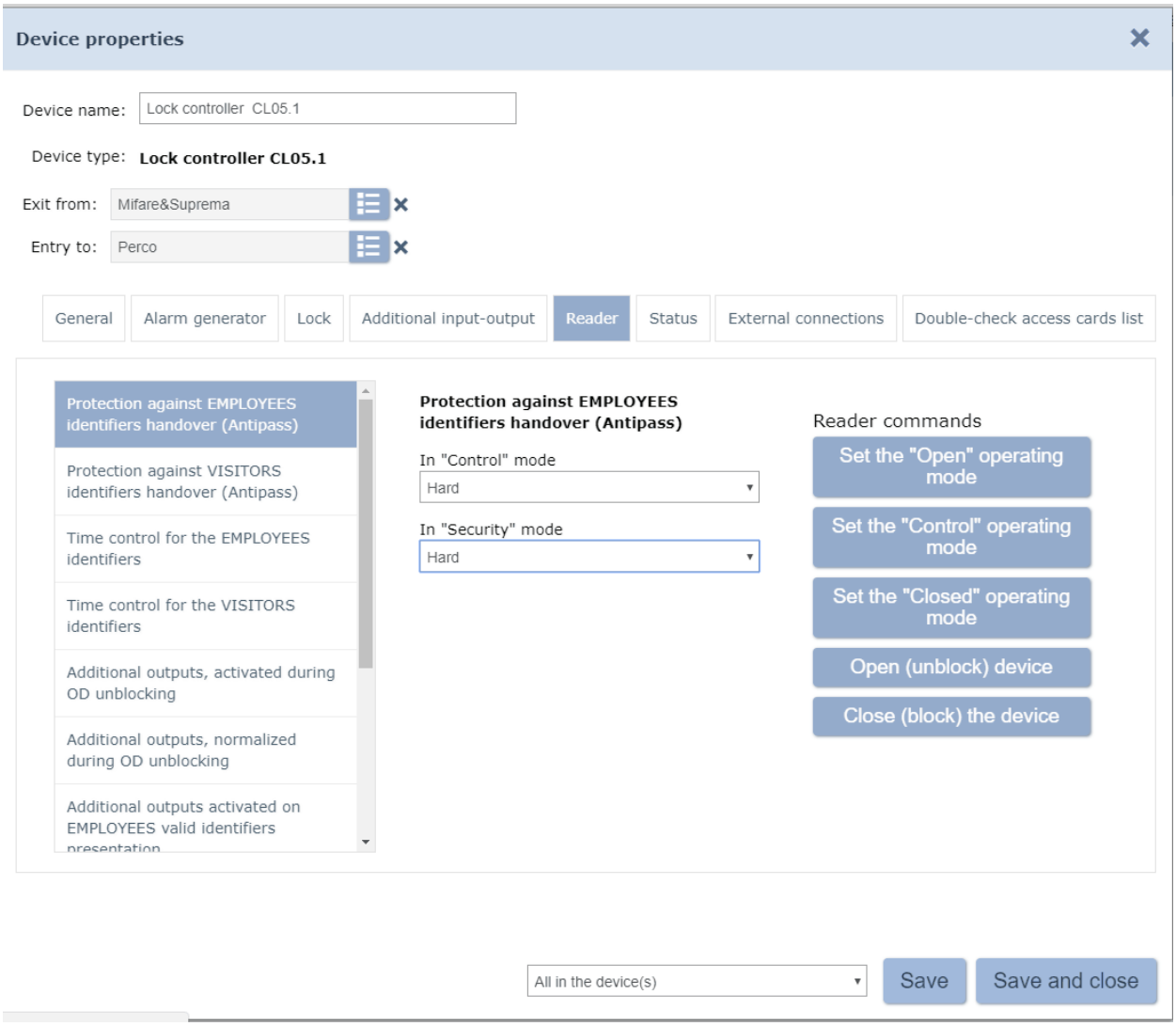
Important:
In order to use antipass function, the ID card access permissions template must contain the information about premises, where the controlling function has to be activated. Configuration of the template can be done in ***«Access template»*** subsection of the ***«Pass office»*** section.

To switch on/off the zonality control function:

1. Go to the  ***«Administration»*** section by using the navigation panel.
2. Open ***«Configuration»*** subsection.
3. Switch to the **Devices** tab.
4. Select the controller which will control zonality.
5. Push the button  **Edit** on the page toolbar. **Device properties** window will appear.
6. In the appeared window switch to **OD** (lock) tab. Window overview:



7. For switching on/off the zonality control function on the selected OD, use the checkbox of the **Internal protection against transmission of identifiers (Local Antipass)** option.
8. Switch to the **Reader** tab and configurate parameters of zonality control during the passage for the selected direction. Window overview:



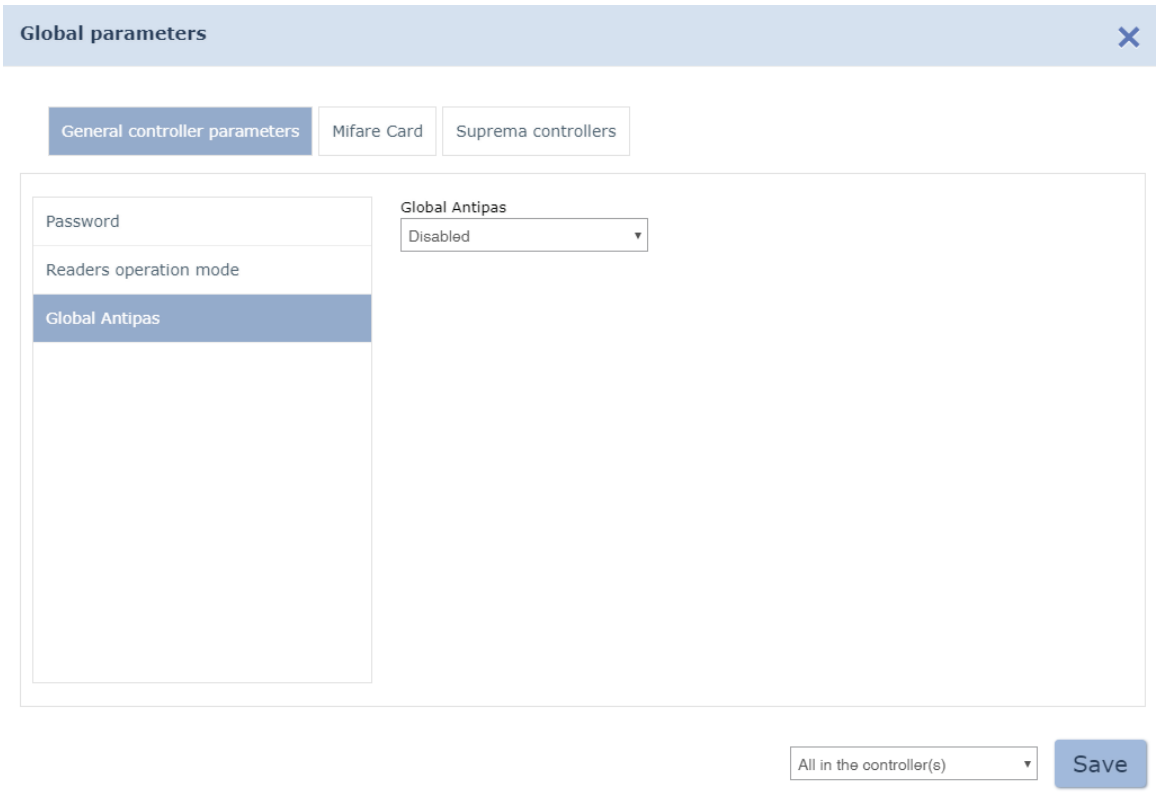
9. Set hard or light zonality control mode individually for employees and visitors.
10. Click **Save**. Controller options window will close, saved changes will be applied to the controller.

Global Antipass Function

For switching on/off the zonality control function:

1. Go to the  **«Administration»** by using the navigation panel.
2. Open **«Configuration»** subsection.

3. Switch to **Devices** tab.
4. Select the root element of the **Global parameters** list.
5. Click **Edit** button on the page toolbar. The window **Global parameters** will appear.
6. Click **Global antipass** button on the left side of the window. The working area will look like this:



7. For switching on/off the zonality global control, choose **On/Off** value from the **Global antipass** drop-down menu.
8. Click **Save**. The **Global parameters** window will close, all changed parameters will be applied to the controllers.

13 «Administration» section

This section is used for organizing WKS for employees who are responsible for configuration and administration of the system. This section helps to carry out the initial configuration of devices, add new operators and licence the system. This section helps to control the workflow of the system and creates reports on registered events.

13.1 «Configuration» subsection

The following tabs are available:

Rooms tab is used for creation the premises list.

Devices tab is used for:

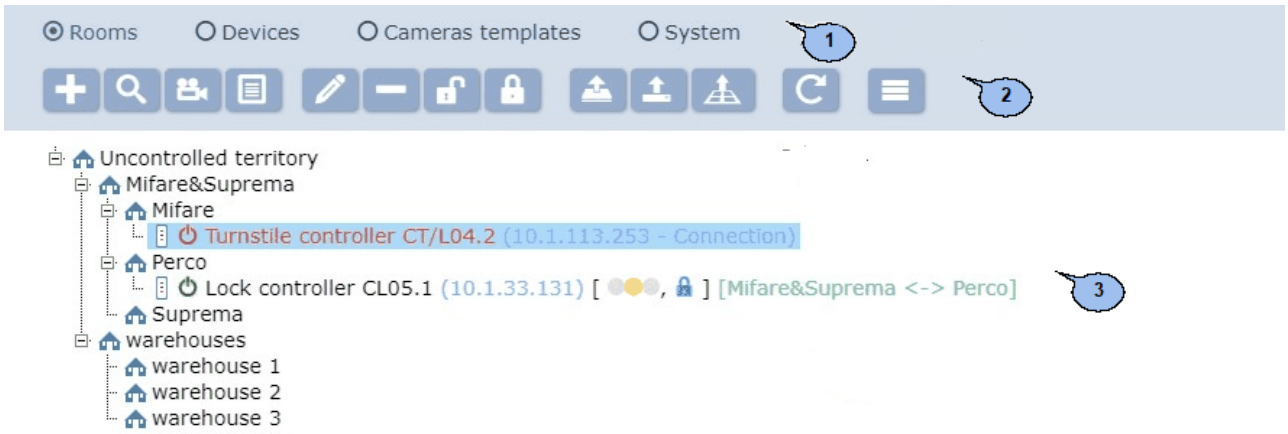
- searching of controllers in local network and adding them in system configuration;
- configurating controllers parameters and their resources;
- sending control commands;
- temporary exclusion of the controller;
- creation the Double-check access cards list.

Cameras templates tab is designed for interface language selection and date format configuration.

System is used for language of the interface selection.

13.1.1 «Rooms» tab

Page overview:



1. Tab selector:
   - **Rooms**
   - **Devices**
   - **Camera templates**
   - **System**
2. Page toolbar:

    **Add room** – click to add an enclosed premise to premise that is selected on the page working area.

 **Search devices** – click to search for controllers (that have not been previously added to system configuration) from the local network and locate them at the selected premise.

 **Add camera** – button allows connecting camera to a selected video server of page working area..

 **Install the device** – click to place controllers that have been previously added to system configuration at the selected premise.

 **Edit** – click to change the name of premise or configure parameters of the selected controller.

 **Delete room/ Disconnect device** – click to delete a premise that is selected on the page working area or remove controller from the premise.

 **Activate** – click to include previously disconnected or newly found controller to the system configuration.

 **Deactivate** – click this button to temporary exclude the controller that is selected on the page working area. In such case the name of the controller will become shadowed.

 **Send configuration changes to device** – click to send edited parameters to system controllers.

 **Send entire configuration to device** – click to send all parameters to system controllers.

 **Send readers security zones** – click to send information about reader location relative to security zones.

 **Refresh** – click to update system controller status information.

 **More – click to open command menu**:

-  **Table print** – click to print the list of premises and controllers that are located there.
-  **Export into XLS** – allows you to save the list of premises and controllers that are located there as *MS Office Excel* spreadsheet file with `.xls` extension.
-  **Export into CSV** – allows you to save the list of premises and controllers that are located there as *OpenOffice Calc* spreadsheet file with `.csv` extension.

3. The page working area contains a multi-level drop down list of premises and controllers that are located there. By default there is *«Uncontrolled area»* premise that can not be deleted.

Important:

Drag-and-drop premises for changing their location.

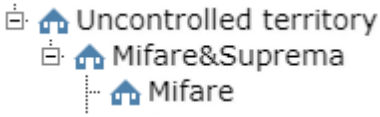
Creation of the Rooms list

To create a list of premises:

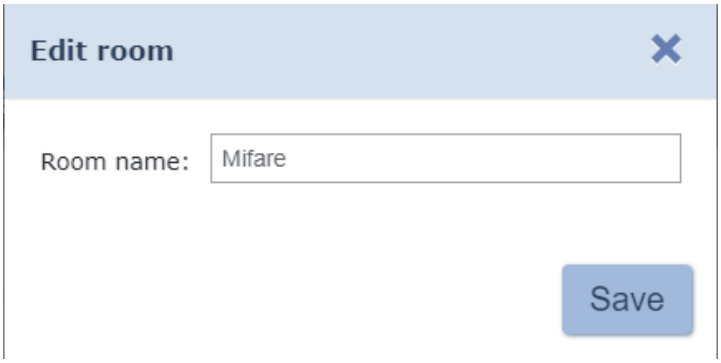
1. Go to  ***«Administration»***.
2. Open ***«Configuration»*** subsection.
3. Switch to **Rooms** tab.
4. Select *«Uncontrolled area»* premise.
5. Click **Add rooms**  button on the page toolbar. **Add room** window will appear:

6. Enter a name of new premise and click **Save**. The window will close, and the premise will be added to the page working area drop down list as an enclosed premise of *«Uncontrolled area»*:

7. To add an enclosed premise: select the premise where you want to add an enclosed premise and click **Add room**  . **Add room** window will appear.
8. In the appeared window enter a name of premise and click **Save**. The window will close and the premise will be added:



9. To change the name of the previously added premise: select it on the page working area and click **Edit**  button that is located on the page toolbar. **Edit room** window will appear:

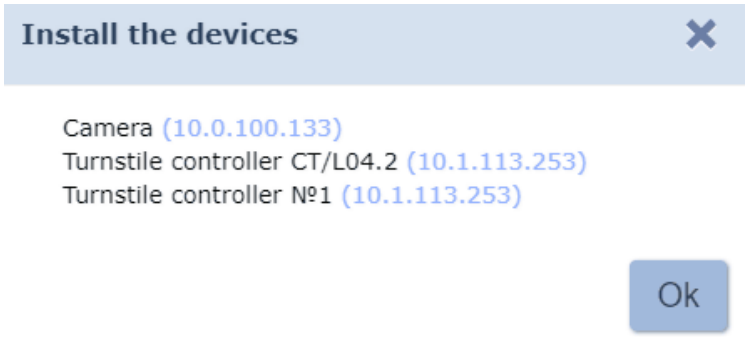


10. Edit data and click **Save**.
11. To delete the previously added premise: select it on the page working area and click **Remove the room /Detach controller** button that is located on the page toolbar. The confirmation window will appear. Click **OK**. The premise will be removed from the list.

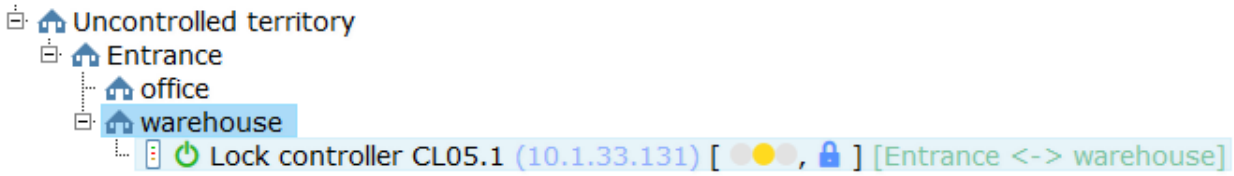
Placing controllers at premise

It is necessary to place system controllers at the premises. To place a controller:

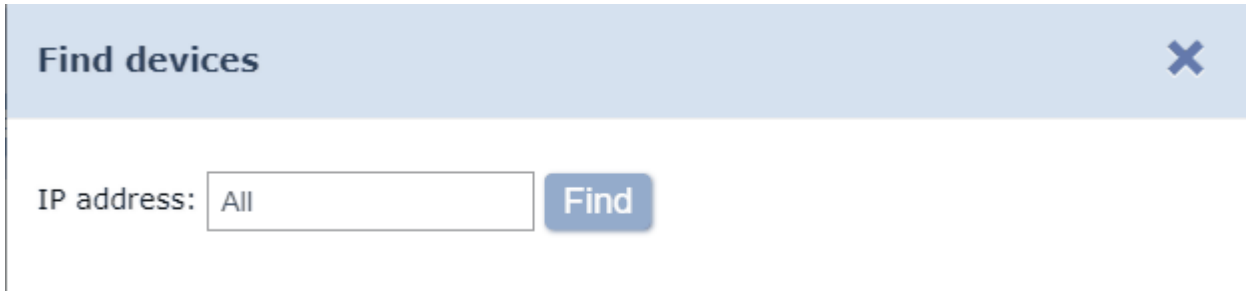
1. Select a premise and click **Install the device** button on the page working area. **Install the device** window will appear. This window contains the list of the previously added system controllers:



2. In the appeared window select a controller and click **Ок**. The controller will appear in the selected premise:



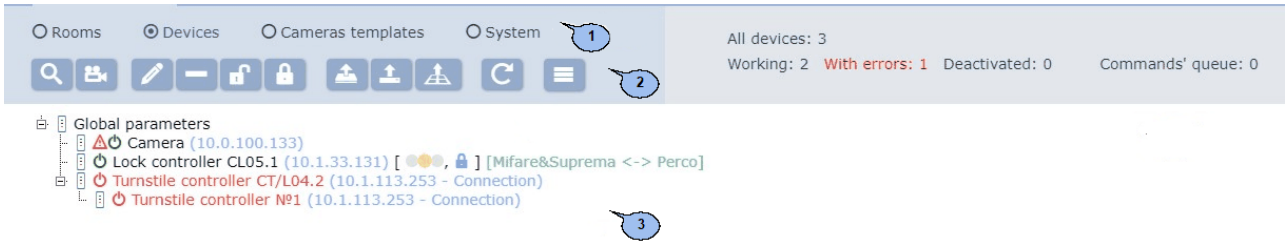
3. It is possible to place a controller at the premise which has not been added to system configuration. To do this: select a premise and click **Search device** button. **Find device** window will appear:



4. Enter IP-address of the desirable controller and click **Find**. Found controller will be placed at the premise and automatically added to system configuration.
5. Configure controller operation parameters if needed. To do this: select the controller on the page working area and click **Edit** button on the page toolbar. Edit desirable parameters in the appeared **Device properties** window and click **Save and close** button.
6. Controllers of ***CL05.1*** electromechanical locks that are opened when the voltage is supplied can be configured to work with additional controller when ACP is organized for controlling bi-directional passage. In order to apply zonality change at such ACP, it is necessary to check **Change zone while passing** parameter that corresponds to OD controller. This can be done in **Device properties** window.
7. To delete the previously added controller from the premise: select it on the page working area and click **Remove the room /Detach controller** on the page toolbar. Click **OK** button in the confirmation window. The premise will be deleted from the list.
8. Click **Send entire configuration to device** button that is located on the page toolbar.

13.1.2 «Devices» tab

Page overview:



1. Tab selector:
   - **Rooms**
   - **Devices**
   - **Camera templates**
   - **System**
2. Page toolbar:
   Search devices – click this button to search for controllers that have not been added to system configuration.

Edit – click this button to open **Device properties** window in order to change parameters of the selected controller. **Controllers general parameters** window will appear if you select *«Controllers gerenal parameters»* root element.

Add camera – button allows connecting camera to a selected video server of page working area.

Delete – click this button to delete the selected controller from the system configuration.

Activate – click to include a previously disconnected or newly found controller to the system configuration.

Deactivate – click this button to temporary exclude the controller that is selected on the page working area. In such a case the name of the controller will become shadowed.

Send configuration changes to device – click to send edited parameters to system controllers.

Send entire configuration to device – click to send all parameters to system controllers.

Send readers security zones – click to send information about reader location relative to security zones.

Refresh – click to update system controller status information.

More – click to open command menu:

- **Table print** – click to print the list of premises and controllers that are located there.
- **Export into XLS** – allows you to save the list of premises and controllers that are located there as *MS Office Excel* spreadsheet file with `.xls` extension.
- **Export into CSV** – allows you to save the list of premises and controllers that are located there as *OpenOffice Calc* spreadsheet file with `.csv` extension.
- **Select all (Ctrl+A)** – allows you to select all controllers.

3. System controllers status panel.

The page working area contains the list of controllers that have been added to system configuration. **Validity** sign indicates that edited parameters have not been sent to controller. The following signs are located on the right side of the controller and inform about applied ACM and OD status:

– ACM *«Open»*,
– ACM *«Control»*,
– ACM *«Closed»*,
– OD is blocked,
– OD is unblocked,
– OD break in.

Search for controllers

To proceed with automatic configuration:

1. Go to  ***«Administration»***.
2. Open ***«Configuration»*** subsection.
3. Switch to **Controllers** tab.
4. Click  **Search device** button on the page toolbar. **Find device** window will appear:

5. Enter IP-address of the controller if you want to find it by its **IP-Address** and click **Find**.
6. Click **Find** button if you would like to find all local controllers.
7. The list of found controllers will appear on the page working area after the procedure is finished:

8. Enter IP-address of desirable controller in the field that is located at the bottom of the window and click **Find**. Name of the controller will be marked yellow.
9. Select a controller (controllers) from the list which you want to add to system configuration. Click **Add**. Window will close and all selected controllers will appear on the page working area.
10. Activate the controller. To do this: select it on the page working area and click **Activate**  .
11. Configure parameters of the controller. To do this: select the controller or the its resourse on the page working area and click **Edit**  button on the toolbar. **Device properties** window will appear.
12. Change the name of the controller by using **Device name** field and edit the description if needed.
13. Specify (or, if needed, change) premises that will be controlled by this controller. Click **Select from list**  button on the right side of the **Exit from** field. Select the premise in the appeared **Rooms** window. Access to this premise will be controlled by the controller №1. Click **Ок**. Specify the premise that will be controlled by the controller №2 by using **Enter in** field.
14. In order to configure controller resources parameters: switch to tab that corresponds to desirable resource and edit the configuration. The list of available parameters depends on the type of controller and selected resourse.
15. Select parameters save method by using the **Device properties** drop down list and click **Save and close**. **Device properties** window will close.
16. Send configuration to controllers. To do this: click **Send configuration changes to device**  or **Send entire configuration to device**  buttons.

Add camera

Important:

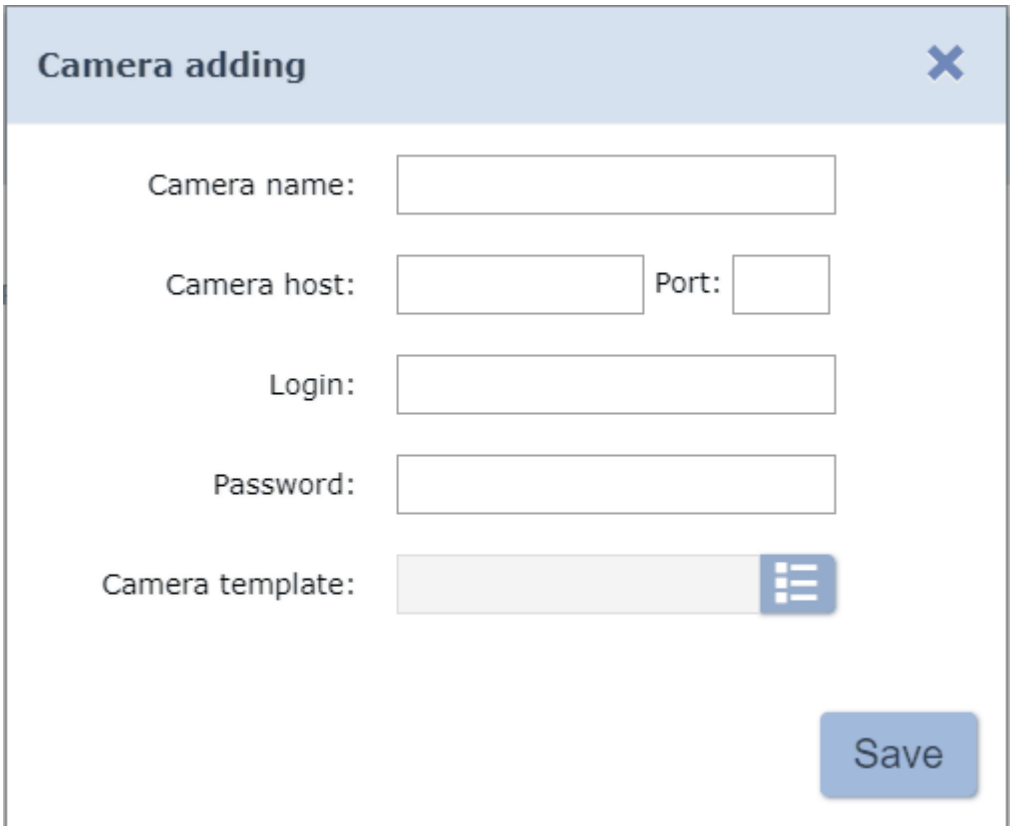
Create templates for the devices that you are going to connect prior to adding. The templates can be created on Camera templates tab of «Verification» subsection from the «Administration» section.

To add camera to the selected premise:

1. Go to  «***Administration***» section by using the navigation panel.
2. Open «***Configuration***» subsection.
3. Switch to **Rooms** tab or **Devices** tab.
4. Select the premise from the page working area where you would like to add camera.

Important:
Cameras that work with ONVIF protocol can be added by using the Search device button. Other types of cameras like mjpeg_over_http can be added by using Add camera button.

5. Click Add camera button on the page toolbar. **Camera adding** window will appear:



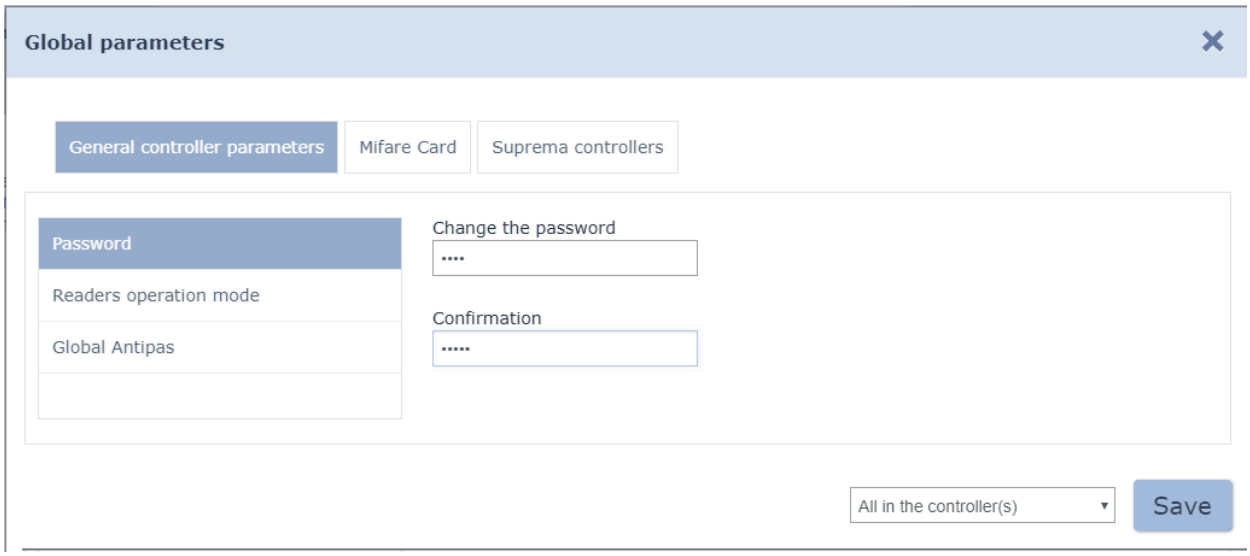
6. Enter the camera name and specify the camera template for it.
7. Configure other parameters of the camera. Click **Save** button. **Camera adding** window will close. The camera will be added to the page working area.

Controllers general configuration

To configure global parameters:

1. Go to  ***«Administration»***.
2. Open subsection ***«Configuration»*** subsection.
3. Switch to **Devices** tab.
4. Select a **Global parameters** root element.
5. Click **Edit**  button on the page toolbar.

The following parameters are presented on the tab:



1. **Password** – allows you to change the common password to all controllers.
2. **Readers operation mode** – allows you to change parameters of readers operational mode.
3. **Global antipass** – allows you to switch on or switch off the global zonality control parameter.

Select parameters save method by using a drop down list at the bottom of the window. Other parameters can be changed in **Mifare cards** tab and **Suprema controllers** tab. Click **Save** to finish.

Important:

In ***PERCo-Web*** security system it is possible to perform a passage by using smartphones with NFC technology. The feature is enabled by default.

- When using an Android smartphone that supports NFC technology, a unique identifier (IMSI) associated with the phone's SIM card is used as an employee (visitor) identifier (requires installation and launch of the **"PERCo. Access"** application, which can be downloaded from *Google Play*).
- When using an Apple smartphone that supports NFC technology, a unique identifier (Token) connected to a bank card is used as an employee (visitor) identifier (the Token of the currently used card will be read, when several Bank cards are connected).

The unique identifier is added to the system in the same way as other cards.

The following options are available on **Mifare Cards** tab:

1. **Select card types** – allows you to select cards that will be used in the ACS. The following types of cards are available for selection:
   - **Ultralight EV1 48 byte,**
   - **Ultralight EV1 128 byte,**
   - **Ultralight C 144 byte,**
   - **Classic ID 64 byte,**
   - **Classic 1KB,**
   - **Classic 4KB,**
   - **Plus 2KB,**
   - **Plus 4KB,**
   - **Plus SE 1KB,**
   - **DESFire Ev1.**
2. **Cards list** – displays the list of selected **Mifare cards**. It allows you to switch between cards and to configure their parameters.
3. **Card parameters** – contains the list of parameters that can be edited for the selected card type.

Important:
The list of available **Card parameters** and **Card management commands** can be changed depending on the selected card type.

4. **Commands of cards management** – contains the list of commands that are available for operation with cards and reader:

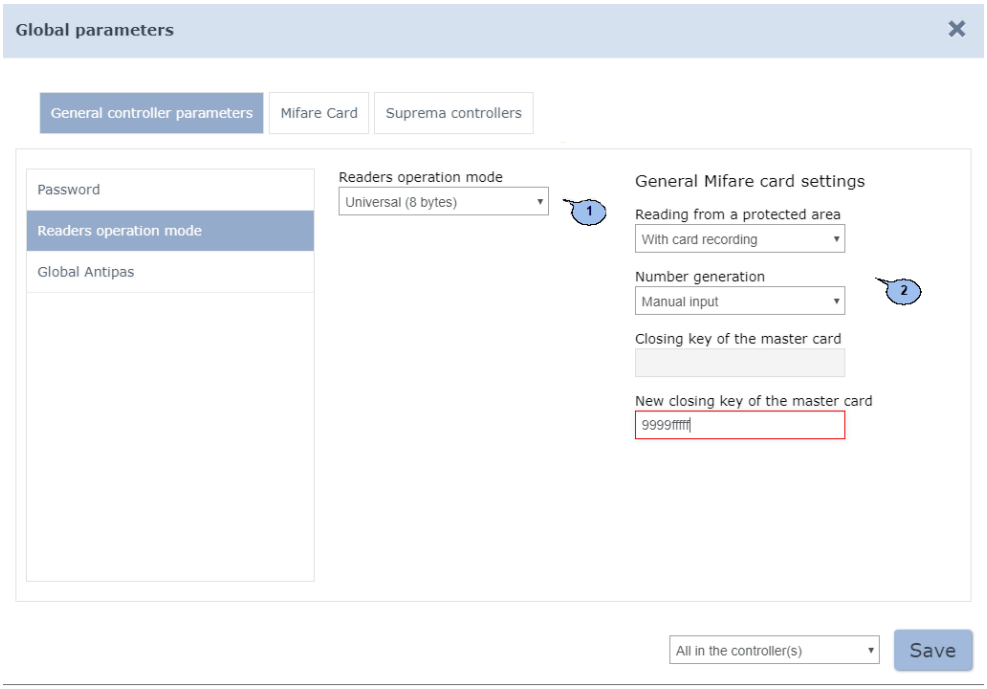
   - **Configuration record to the memory** – allows you to write configured parameters of the selected card type to the reader nonvolatile memory;
   - **Configuration record to the master card** – allows you to write configured parameters of the selected card type to master-card;

Important:
Mifare DESFire cards are used as master-cards. They can be also used as ordinary cards.

   - **Change key** – this command allows to write edited parameters for all Normal output types of cards (Ultralight, Classic, Plus, DESFire). Reader detects the card by command, defines its type and changes **card parameters** according to parameters that are applied for the reader and this type of cards;
   - **View card information** – displays the information about selected card. The following information will be displayed in the pop-up **Card information** window:
     - Card type – displays **Mifare** card type;
     - UID Series – displays series of the unique identificator;
     - UID Number – displays number of the unique identificator;
     - Card type – displays the card type: master-card, Normal output card;
     - Master-card current status – displays the current status of the master-card (for **Mifare DESFire** cards);
     - Security level – displays the current security level (for **Mifare Plus** cards).
   - **Improve security level SL** – this command improves SL (security level) for all types of **Mifare Plus** cards that have security level 1 and 2;
   - **Format** – is used for Normal output.

Important:
- Editing of the Mifare cards configuration can be done only by one user at a time;
- The operation of Mifare cards will be blocked at the moment of configuration («Configuration is in progress» warning box will appear when attempting to work with reader);
- Any change of Mifare cards configuration is stored in the system DB after successful save is done. After this, the configuration is automatically sent to all readers that are connected to ACS at the moment.

Readers operating mode allows to configure additional operating mode parameters of readers. Page overview:



1. **Readers operation mode** drop down menu allows to select Readers operation mode:
   - Universal (8 bytes);
   - Wiegand 26.
2. **General Mifare card settings -** allows you to select the following parameters:

   - **Protected area reading** – defines the mode of operation with Mifare card protected area:
     - Read – reading of Card UID;
     - With card recording – reading of card number from protected area and rewriting it by using applied algorithm of number generation.

   - **Number Generation** – defines method of card number generation that will be written on Mifare card protected area and that is used by ACS as identificator:
     - Manual input – card number must be entered manually when issued;
     - Random number – random card number will be generated automatically when issued;
     - In ascending order – card number will be generated by the program by using its internal algorithm.

   - **Master-card block key** – the current master-card block key is displayed in this field.

   - **New master-card block key** – this field allows to enter new master-card block key.

It is necessary to use cards with copy protection function in order to arrange the access control system and be sure in its safety. The following **MIFARE** cards can provide this**: Classic, Plus, DESFire.**

Important:

MIFARE Ultralight cards (except **MIFARE Ultralight C**) don't have copy protection and can be compared to traditional Proximity-cards.

MIFARE cards are brought from manufacturer without any protection. Reader will use only open UID of the card that can be easily copied.

Important!

Customer / owner of the facility should pay careful attention to cryptoprotection — he must not entrust the processes of card creation, card cryptoprotection write operations to card and readers supplier, ACS mounter or anybody alse. Access cards can be easily copied when a third party has cryptographic keys.

It is necessary that the owner of the ACS or his representative will come up with passwords and keys and write them to cards and readers. A master-card is used for readers programming. It contains all key information. After that operator can "Flash" readers using the master-card but will not have access to keys and passwords.

Different MIFARE chIP Stile main characteristics

Card type	MIFARE Ultralight	MIFARE Classic ID 64/1KB/ 4KB	MIFARE DESFire EV1 2K/4K/8K	MIFARE Plus S2K/4K	MIFARE Plus X 2K/4K
Cryptoalgorithm	No	CRYPTO1	DES & 3DES/AES	CRYPTO1/AES	CRYPTO1/AES
Length of serial number, byte	7	4/7	7	7	7
EEPROM, byte	64	1024/4096/4096	2048/4096/8192, flexible file structure	2048/4096	2048/4096
Number of write cycles	10 000	100 000	500 000	200 000	200 000
Structure	16 pages/ 4 byte	16 sect./ 64 byte, 32 sect./ 64 byte, 8 sect./ 256 byte	Defines by the software	32 sect./ 4 blocks, 8 sect./1 block	32 sect./ 4 blocks, 8 sect./1 block

Cryptosecurity that is build in **MIFARE Classic** chip is considered to be weak nowadays. **MIFARE Plus** series of cards is designed to provide hard level of security. It uses AES cryptography which is impossible to crack.

Important:

MIFARE Plus prox cards support 3 levels of security and can be upgraded from one level to another anytime:

Security level SL1. This level of **MIFARE Plus** cards provides 100% compatibility with **MIFARE Classic 1K (4K)** cards.

Security level SL2. AES authentification is obligatory. CRYPTO1 is used for data protection.

Security level SL3. Authentification, exchange of data, work with memory is done by using AES.

MIFARE DESFire EV1 cards have the highest protection level and flexible file structure of memory.

In order to protect **MIFARE Classic 1K (4K)** card it is enough to write identificator (for example, a number that is 3 bytes length and that is send over Wiegand-26) to one of the memory blocks and block access to it by using the crypto key. You can also configure reader in the way that it will read identificator from the specified memory block of **MIFARE Classic** card that is protected with the same crypto key.

If you want **MIFARE** cards to work in the security mode:

1. Take precautions in order to prevent loss of the key information.
2. For **MIFARE Plus** cards – select the security level which will be used by ACS: SL1, SL2 or SL3. Every security level has to be chosen depending on the facility specific character and its safety requirements. SL3 security level — is considered as the most secure.
3. Prepare readers. Every reader that is connected to the ACS controller must be programmed to read data from the same memory block and must use the same AES key as the **MIFARE** card. It is necessary to configure reader, write master-card and configure all ACS readers by using it.
4. Emission of **MIFARE** cards by using reader with USB **MR08** interface. It is a write operation of identificator to the selected **MIFARE** memory sector, operation of switching the security level (SL1, SL2 or SL3 for MIFARE Plus cards), operation of blocking of the selected memory sector with crypto key (AES or CRYPTO1). Such identificator will be connected to a certain employee and will be read in protected mode.

Algorithm of operation of **Mifare** protected memory area during user ID writing process which will be used by ACS as a card number. The example is based on operation with **Mifare Classic 4KB** card.

In order read data from protected area, it is necessary to:

Write configuration to reader. To do this: go to ***Administration > Configuration >*** **Devices** . Select **Global parameters** option and click  **Edit**. Switch to **Mifare cards** tab in the appeared **Global parameters** window.

1. Click **Select card type**  button on **Mifare cards** tab. In the appeared window check **Mifare Classic 4KB** card option and click **Ок**.
2. Specify the **Sector number**. It represents a part of memory that will be used as identificator storage and will be read from there when client uses ACS. The number is selected randomly.
3. Specify **Block number**. It represents a part of memory that will be used as identificator storage and will be read from there when the client uses ACS. The number is selected randomly.
4. Previously saved parameters will be displayed in **The old type of authentication key** and in **Old authentification key** fields.

Important:

It is important that parameter values **The old type of authentication key** and **Old authentification key** have the same type of authentification key and authentification key that are written on the card. Otherwise it will be impossible to re-write the card.

5. The current Master-card type of authentification key is displayed in **The type of authentication key** field. In other words it is the type of key which was used for card locking.
6. Enter new athentification key in the **Authentification key** field. This key will be used as a new identification key.
7. Click **Write cofiguration to memory** button to save new configuration.

Then it is necessary to write configuration from the controller to a master-card. To do this:

1. Put the card towards the controller and click **Write cofiguration to master-card**.

Important:

DESFire card is used in the ACS as a master-card. Normal output type of **DESFire** card can be used as an additional master-card. Rewriting of master-card to Normal output type is impossible! (i.e. – once **DESFire card** has been written as master-card it will keep being a master-card even after rewriting attempts.)

2. It is necessary to program all readers by using the master-card. To do this: put the card towards the reader – the stored card configuration will be automatically written to reader.

Now your ACS is ready for operation with configured parameters. The last thing to do is to program Normal output cards.

- If Normal output cards have been previously used then they have to be reprogrammed. To do this: put a card towards the reader and click **Change key** button from the **Mifare cards** tab working area. A new configuration will be written to the access card.
- If Normal output cards which you want to reprogram have not been used before, then it is necessary to personalize them, i.e. – to issue an identificator. This can be done in **Staff > Employees** section or in **Pass Office > Employees** section by using the  **Issue card** button.

It is necessary to specify desirable card parameters when you will configure reader. Parameters depend on the card type and the department:

- **Numbers of page, block, sector or application** – it is a place where the card number that is used by ACS will be stored.
- **Authentification keys and their types** – passwords and their types that give access to card.
- **Keys for changing security level (SL)** – passwords that allow you to change card configuration. Only **Mifare Plus** cards have it.
- **Access keys to card data** – additional passwords that allow you to get access to card data. Only **Mifare DESFire** cards have it.

Repeat the above mentioned operations if you would like to change configuration. Proceed from the point 1, whilst note that:

a. The previously added cards will work even new types of cards are added to the currently applied ACS configuration.
b. If any parameters (like numbers of pages/sectors/blocks, types or values of keys, SL security levels) are changed for the previously issued cards, then it is necessary to reprogram them by applying the new configuration.
c. Operational aspects of working with master-cards, password recommendations can be found in **MR08** control reader maintenance manual.

Every type of **Mifare** card (Ultralight, Classic, Plus, DESFire) has specific parameters that are available for editing or viewing.

Important:
"Old authentification key", **"The old type of authentication key"** fieds display the current configuration parameters that have been written to the reader earlier. If you want to write configuration parameters to reader: fill in **"The type of authentication key", "Authentification key"** fields and write configuration to reader.

Ultralight, Classic, Plus, DESFire subtabs allow you to configure parameters of cryptosecurity for types of cards that are selected in the **Mifare card types.** Click **Select types of cards** button to open this window. These parameters will be applied to user's Normal output cards during issuing and personalization by using the reader. These parameters will be sent to the configuration of readers which are located at the master-cards pass points.

Important:
Parameter permitted values are displayed in the drop down lists after you click the arrow from the field. It is possible to apply any active pararmeter (disabled are marked grey) to the configuration.

The **Cards list** displays subtabs that are designed for configuration of the parameters of the following card types:

- **Ultralight: EV1 48 bytes, EV1 128 bytes, C 144 bytes;**
- **Classic: ID64, 1KB, 4KB;**
- **Plus: 2KB, 4KB, SE1KB;**
- **DESFire.**

Subtabs of the various types of cards include the following parameters of cryptoprotection:

- **Page number, sector number, block number** – part of the card's memory where the ID is stored. This ID is used by the ACS.
- **Authentification key** – a password which blocks acces to card ID, displayed in Hex format.
- **Old parameters, Old authentification key** – these fields display the password of card ID and its characteristics which are used prior to the parameter reconfiguration (they could be found in the **Actual parameters, Actual authentification key** fields before the previous parameter configuration).
- **Actual parameters, Actual authentification key** – these fields display the password of card ID and its characteristics which will be

used after parameter reconfiguration (they will be displayed in **Old parameters, Old authentification key** after the next reconfiguration).

- For **Plus** cards, besides, there are parameters that define the security level (SL1, SL2, SL3).

Important!

These parameters provide the highest level of security (eg. For payment system cards). It is not recommended to use these parameters within basic ACS. Loss of these parameters values will result in reconfiguration of all cards that are already personified in the system.

Parameters of **Mifare Ultralight** cards.

- **Ultralight EV1 48 byte**
  - **Page** – card memory page number where the card number is stored. This number is used by ACS, permitted values: 4-15.
- **Ultralight EV1 128 byte**
  - **Page** – card memory page number where the card number is stored. This number is used by ACS, permitted values: 4-35.
- **Ultralight C 144 byte**
  - **Page** – card memory page number where the card number is stored. This number is used by ACS, permitted values: 4-39.
  - **Old authentification key** – displays old authentification key, length 6 bytes in *Hex* format;
  - **Authentification key** – key that is used for user athentification, length 6 bytes in *Hex* format.

Parameters of **Mifare Classic** cards.

- **Classic ID 64**
  - **Block number** – block number where the card number is stored. This number is used by ACS, permitted values: 1, 2;
  - **The old type of authentication key** – displays old type of authentification key, permitted values: A, B;
  - **Old authentification key** – displays old authentification key, length 6 bytes in *Hex* format;
  - **The type of authentication key** – Type of authentification key, permitted values: A, B;
  - **Authentification key** – key that is used for user authentification, length 6 bytes in *Hex* format.
- **Classic 1 KB**
  - **Sector number**– sector number where the card number is stored in the block, permitted values: 0-15;
  - **Block number**– block number, where the card number is stored, this number is used by ACS, permitted values:
    - 1, 2 – for sector number 0,
    - 0, 1, 2 – for sectors 1-15;

- **The old type of authentication key** – displays old type of authentification key, permitted values: A, B;
- **Old authentification key** – displays old authentification key, length 6 bytea in *Hex* format;
- **The type of authentication key** – Type of authentification key, permitted values: A, B;
- **Authentification key** – key that is used for user authentification, дlength 6 bytes in *Hex* format.

- **Classic 4 KB**
  - **Sector number**– sector number where the card number is stored in the block, permitted values: 0-39;
  - **Block number**– block number, where the card number is stored, this number is used by ACS, permitted values:
    - 1, 2 – for sector number 0,
    - 0, 1, 2 – for sectors 1-31,
    - 0-14 – for sectors 32-39;
  - **The old type of authentication key** – displays old type of authentification key, permitted values: A, B;
  - **Old authentification key** – displays old authentification key, length 6 bytes in *Hex* format;
  - **The type of authentication key** – Type of authentification key, permitted values: A, B;
  - **Authentification key** – key that is used for user authentification, length 6 bytes in *Hex* format.

Important:

- **Sector number**– number of the internal area of the card memory that contains several blocks for data.
- **Block number**– the smallest part of the card memory. Data blocks are available for reading/writing upon successful authorization.

Parameters of the **Mifare Plus** card**:**

- **Plus 2 KB**
  - **Sector number**– sector number where the card number is stored in the block, permitted values: 0-31.
  - **Block number**– block number, where the card number is stored, this number is used by ACS, permitted values:
    - 1, 2 – for sector number 0,
    - 0, 1, 2 – for sectors 1-31;
  - **The old type of authentication key** – displays old type of authentification key, permitted values: A, B;
  - **Old authentification key** – displays previously written authorization key, that is used in SL1 and SL2 card security level, length 6 bytes in *Hex* format;
  - **Old key for security level 3 in case of key type A** – displays authentification Key for security level 3 in case of key type A, length 16 bytes in Hex format;

- **Old key for SL3 security level and B key type** – displays authentification key for SL3 security level and A key type, length 16 bytes in Hex format;
- **The type of authentication key** – type of authentification key, permitted values: A, B;
- **Authentification key** – key that is used when the card works with SL1 and SL2 security levels, length 6 bytes in Hex format;
- **Key for security level 3 in case of key type A** – authentification key for SL3 security level and A key type, length 16 bytes in Hex format;
- **Key for SL3 security level and B key type** – authentification key for SL3 security level and B key type, length 16 bytes in Hex format;
- **Security level SL** – Security level of **Mifare Plus** cards, permitted values: 1-3;

Keys for changing the security level (SL):

- **Master key**– key, length 16 bytes in Hex format;
- **Configuration key** – key, length 16 bytes in Hex format;
- **Authentification key for SL1 security level**– AES key, length 16 bytes in Hex format;
- **Switch key to security level 2** – key, length 16 bytes in Hex format;
- **Switch key to security level 3** – key, length 16 bytes in Hex format.

Important:

Unlike authentification keys that can be changed when it is necessary, keys for changing security level (SL):

- **Master key,**
- **Configuration key,**
- **Authentification key for SL1 security level,**
- **Authentification key for SL2 security level,**
- **Switch key to security level 3**)

of **Mifare Plus** cards can be written only once and can not be changed!!!

- **Plus 4 KB**
  - **Sector number**– sector number where the card number is stored in the block, permitted values: 0-31;
  - **Block number**– block number, where the card number is stored, this number is used by ACS, permitted values:
    - 1, 2 – for sector number 0,
    - 0, 1, 2 – for sectors 1-31,
    - 0 - 14 – for sectors 32-39;
  - **The old type of authentication key** – displays old type of authentification key, permitted values: A, B;

- **Old authentification key** – displays previously written authentification key that is used for working with SL1 and SL2 security levels, length 6 bytes in Hex format;
- **Old key for security level 3 in case of key type A** – displays authentification key for SL3 security level and A key type, length 16 bytes in Hex format;
- **Old key for SL3 security level and B key type** – displays authentification key for SL3 security level and B key type, length 16 bytes in Hex format;
- **The type of authentication key** – type of authentification key, permitted values: A, B;
- **Authentification key** – authentification key that is used for working with SL1 and SL2 security levels, length 6 bytes in Hex format;
- **Key for security level 3 in case of key type A** – authentification key for SL3 security level and A key type, length 16 bytes in Hex format;
- **Key for SL3 security level and B key type** – authentification key for SL3 security level and B key type, length 16 byte in Hex format;
- **Security level SL** – **Mifare Plus** cards security level, permitted values: 1-3;

Keys for changing security level (SL):

- **Master key**– key, length 16 bytes in Hex format;
- **Configuration key** – key, length 16 byte in Hex format;
- **Authentification key for SL1 security level**– AES key, length 16 bytes in Hex format;
- **Switch key to security level 2** – key, length 16 bytes in Hex format;
- **Switch key to security level 3** – key, length 16 bytes in Hex format.

- **Plus SE 1 KB**
  - **Sector number**– the sector where the card number is stored in the block, permitted values: 0-15;
  - **Block number**– the block, where the card number is stored, this number is used by ACS, permitted values:
    - 1, 2 – for sector number 0,
    - 0, 1, 2 – for sectors 1-15;
  - **The old type of authentication key** – displays old type of authentification key, permitted values: A, B;
  - **Old authentification key** – displays previously written authentification key that is used for working with SL1 and SL2 security levels, length 6 bytes in Hex format;
  - **Old key for security level 3 in case of key type A** – displays authentification key for SL3 security level and A key type, length 16 bytes in Hex format;
  - **Old key for SL3 security level and B key type** – displays authentification key for SL3 security level and B key type, length 16 bytes in Hex format;

- **The type of authentication key** – Type of authentification key, permitted values: A, B;
- **Authentification key** – authentification key that is used when the card works with SL1 and SL2 security levels, length 6 bytes in Hex format;
- **Key for security level 3 in case of key type A** – authentification key for SL3 security level and A key type, length 16 bytes in Hex format;
- **Key for SL3 security level and B key type** – authentification key for SL3 security level and B key type, length 16 bytes in Hex format;
- **Security level SL** – Security level of **Mifare Plus** cards, permitted values: 1-3;

Keys for changing security level (SL):

- **Master key**– key, length 16 bytes in Hex format;
- **Configuration key** – key, length 16 bytes in Hex format;
- **Authentification key for SL1 security level**– AES key, length 16 bytes in Hex format;
- **Switch key to security level 2** – key, length 16 bytes in Hex format;
- **Switch key to security level 3** – key, length 16 bytes in Hex format.

Important:

- **Sector number**– part of the card internal memory area which contains several blocks for data storing.
- **Block number**– the smallest part of the card memory. Data blocks are available for reading/writing after successful key authorization.
- **SL (secure level)** – the security level, level of protection. **Mifare Plus** cards support 3 levels of protection:
  - **Security level 0, or the basic level. Mifare Plus** cards have this status prior to initial operation. The security level will be changed from SL0 to;
  - **Security level 1.** Having this level**, Mifare Plus** cards are fully compatible with **Mifare Classic 1K, Mifare Classic 4K** on this level. They can be used in one ACS;
  - **Security level 2. AES** cryptoalgorithm authentification is a must. **CRYPTO1** Cryptoalgorithm is used for data protection**;**
  - **Security level 3. AES** cryptoalgorithm is used for authentification, sharing and encryption of data**.**

Security level of **Mifare Plus** cards can be switched from the lowest to the safest at any time. Switching the safest level to the lowest level is not impossible!!!

Parameters of **Mifare DESFire** cards**:**

Important:
Unlike the rest types of cards, **Mifare DESFire** cards are used both as Normal output cards and as master-cards. Normal output **DESFire** cards can be programmed as additional master-card for the ACS. It is impossible to rewrite **DESFire** card from master-card status to generic status! (I.e. –once **DESFire** card is written as a master-card it will stay the same even after rewriting procedure.)

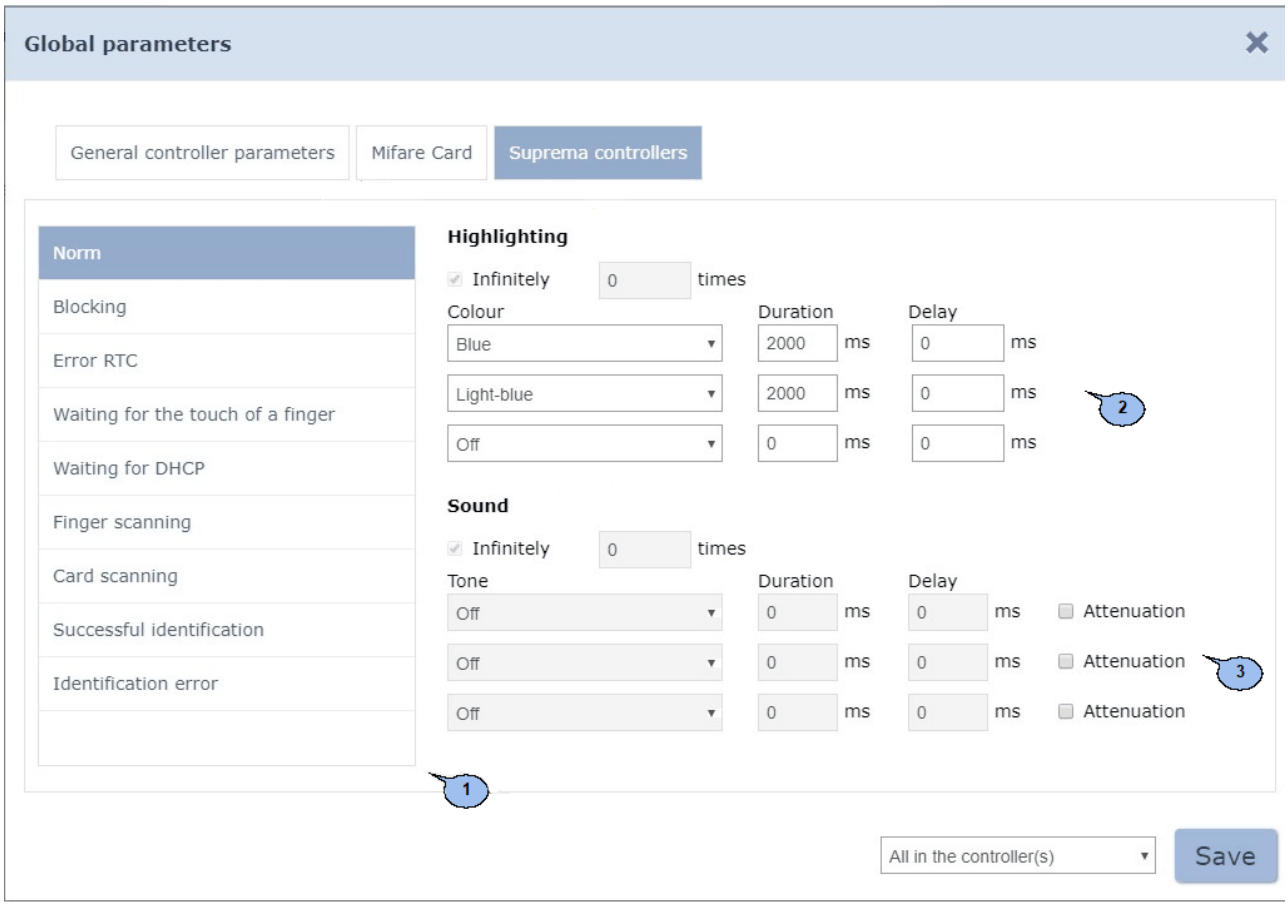
- **DESFire Ev1**
  - **Old application number** – displays old application number where the card number is stored. This number is used by ACS, length 3 bytes in Hex format;
  - **Old type of the card key** – displays old key type of the card, permitted values:
    - AES (AES 128 Key [16 Bytes]) – type of key which uses symmetrical algorithm of block encryption, length 16 bytes;
    - 2K3DES (2 Key Triple Des [16 Bytes]) – type of key which uses symmetrical algorithm of block encryption, uses triple encryption with two keys, length 16 bytes;
    - 3K3DES (3 Key Triple Des [24 Bytes]) – type of key which uses symmetrical algorithm of block encryption, uses triple encryption with three keys, length 24 bytes.
  - **Old key card** – displays old key, length depends on the key type:
    - AES – length 16 bytes in Hex format;
    - 2K3DES – length 16 bytes in Hex format;
    - 3K3DES – length 24 bytes in Hex format.
  - **Old type of the application key**– displays old key type of the application, variants:
    - AES (AES 128 Key [16 Bytes]) – type of key which uses symmetrical algorithm of block encryption, length 16 bytes;
    - 2K3DES (2 Key Triple Des [16 Bytes]) – type of key which uses symmetrical algorithm of block encryption, uses triple encryption with two keys, length 16 bytes;
    - 3K3DES (3 Key Triple Des [24 Bytes]) – type of key which uses symmetrical algorithm of block encryption, uses triple encryption with three keys, length 24 bytes.
  - **Old application key** – displays old application key, length depends on the key type:
    - AES – length 16 bytes in Hex format;
    - 2K3DES – length 16 bytes in Hex format;
    - 3K3DES – length 24 bytesin Hex format.

- **Application number**– application number, where the card number is stored. This number is used by ACS. Length 3 bytes in Hex format;
- **Type of the card key** – Type of key card, variants:
  - AES (AES 128 Key [16 Bytes]) – type of key which uses symmetrical algorithm of block encryption, length 16 bytes;
  - 2K3DES (2 Key Triple Des [16 Bytes]) – type of key which uses symmetrical algorithm of block encryption, uses triple encryption with two keys, length 16 bytes;
  - 3K3DES (3 Key Triple Des [24 Bytes]) – type of key which uses symmetrical algorithm of block encryption, uses triple encryption with three keys, length 24 bytes.
- **Card key** – key of the card, length depends on the key type:
  - AES – length 16 bytes in Hex format;
  - 2K3DES – length 16 bytes in Hex format;
  - 3K3DES – length 24 bytes in Hex format.
- **Type of application key** – Application key type, variants:
  - AES (AES 128 Key [16 Bytes]) – type of key which uses symmetrical algorithm of block encryption, length 16 bytes;
  - 2K3DES (2 Key Triple Des [16 Bytes]) – type of key which uses symmetrical algorithm of block encryption, uses triple encryption with two keys, length 16 bytes;
  - 3K3DES (3 Key Triple Des [24 Bytes]) – type of key which uses symmetrical algorithm of block encryption, uses triple encryption with three keys, length 24 bytes.
- **Application key** – application key, length depends on the key type:
  - AES – length 16 bytes in Hex format;
  - 2K3DES – length 16 bytes in Hex format;
  - 3K3DES – length 24 bytes in Hex format.

Important:

Application number – number of the file that is stored in the card internal memory and contains the written information.

Suprema controllers tab allows you to configure the color coding indication and aural signals of the controller for the following list of events:



1. **List of events** – displays the list of events which support the color coded indication configuring and assigning of the aural signals:

•Normal – the event occurs during the normal operation of the controller (operation mode **"Control"**);

•Block – the event occurs in case of controller blocking (operation mode **"Closed"**);

•RTC error(Real Time Clock) – the event occurs when controller internal time does not match with the local network time;

•Awaiting for finger scanning – the event occurs if **Access with card and fingerprint scan** mode has been selected;

•Waiting for DHCP(Dynamic Host Configuration Protocol) – the event occurs during awaiting of IP-address from DHCP-server;

•Fingerprint scanning – the event occurs when you add a fingerprint that acts as employee/visitor identificator (if the controller is selected as identificator receiver);

•Card scanning – the event occurs when you add access card that acts as employee/visitor identificator (if the controller is selected as identificator receiver);

•Successful identification – the event occurs in case of successful identification;

•Identification error – the event occurs in case of identification error.

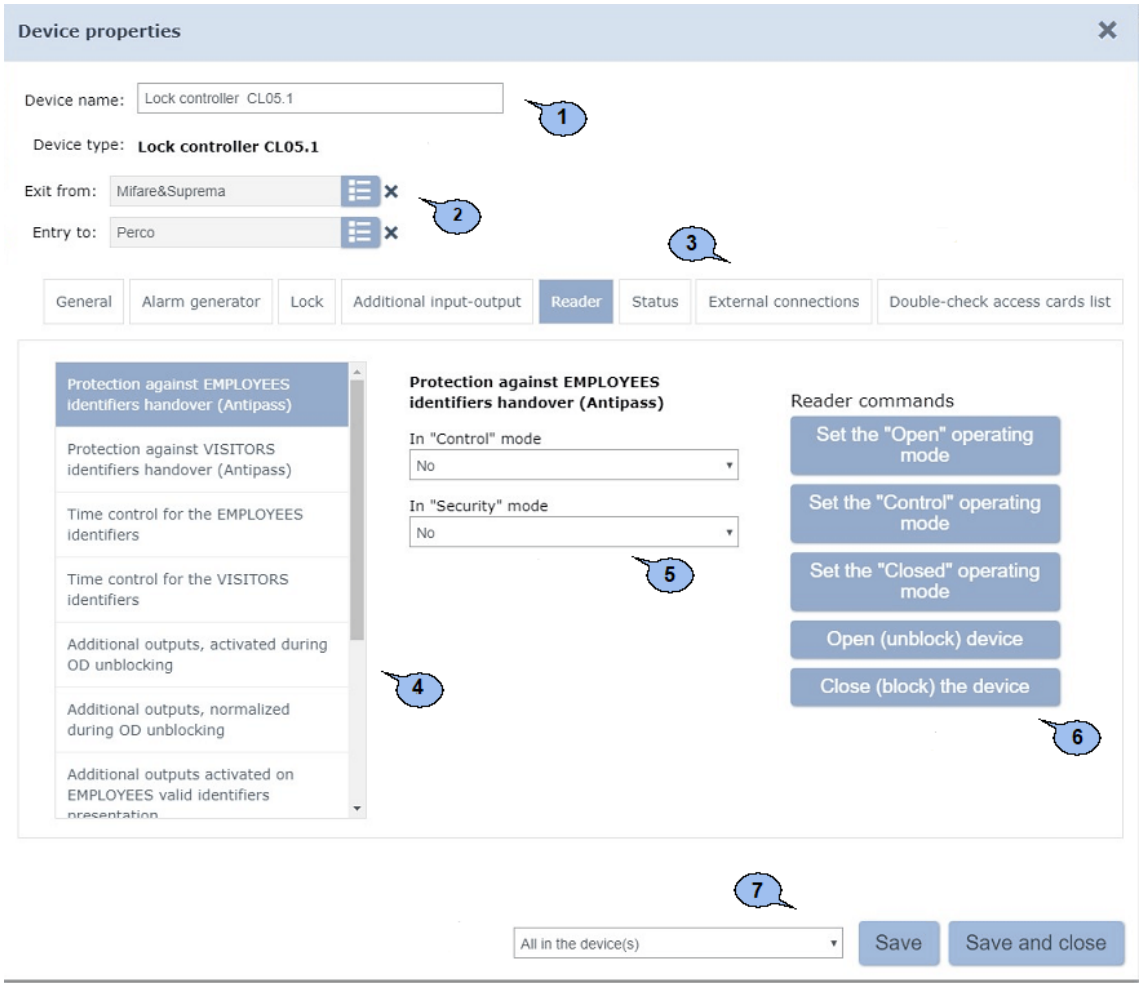
2. **Highlight** – displays color coded indication parameters of the controller for the the selected event from the list of events.

3. **Sound** – displays aural signals parameters of the controller for the selected event from the list of events.

To save press **Save** button, otherwise button. .

«Device properties» window

Device properties window overview:



1. **Device name**– controller name entry field.

2. Tools for pointing and changing of premises that work with controller.

Select from list – button on the right side of the **Exit from** field allows you to select a desirable premise. Access to this premise is provided by reader №1. Click **Reset** button to delete the previously selected premise from the field.

Select from list – button on the right side of the **Enter in** field allows you to select a desirable premise. Access to this premise is provided by reader №2. Click **Reset** button to delete the previously selected premise from the field.

3. Tab selector. The number of tabs can differ depending on the type of controller. The following tabs are available:
   - **For PERCo controllers**
     - **External connections**– this tab contains information about controller external connections;
     - **Alarm generator**;
     - **Additional inputs**;
     - **Additional outputs**;
     - **Auxillary output**;
     - **CL-05.1 lock**;
     - **OD** (Lock, Turnstile);
     - **General**;
     - **LICON properties and Lines**;
     - **Status** – this tab contains controller status information;
     - **Double-check access cards list**;
     - **Reader**.
   - **For Suprema controllers**
     - **General**;
     - **Lock**;
     - **Reader**.
   - **For camera**
     - **Camera;**
     - **About camera**
     - **Video.**
4. Parameters which are available for this resourse.
5. Possible values and variants of parameter configuration.
6. Control command buttons which are available for the selected resourse. ***«Device management»*** subsection of the ***«Access control»*** section can be used for quick operation.
7. **Save**, **Save and close** buttons, the drop down list of saved changes:
   - **To the database only** – parameters are saved only to system DB and must be send to controller(s) afterwards.
   - **All to the controller(s)** – all parameters are send to controller(s).
   - **Changed in controller(s)** – only changed parameters will be sent to controller(s).

Creation of double-check cards list

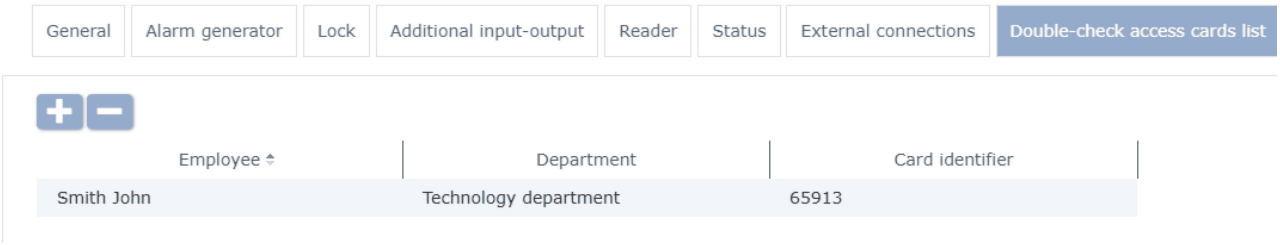
Important:

It is necessary to specify premises in the access template. Access to these premises will be granted by using the double-check function. Rooms must be configured using **...with double-check** access type. The template can be configured in the ***«Access template»*** subsection of the ***«Access control department»*** section.

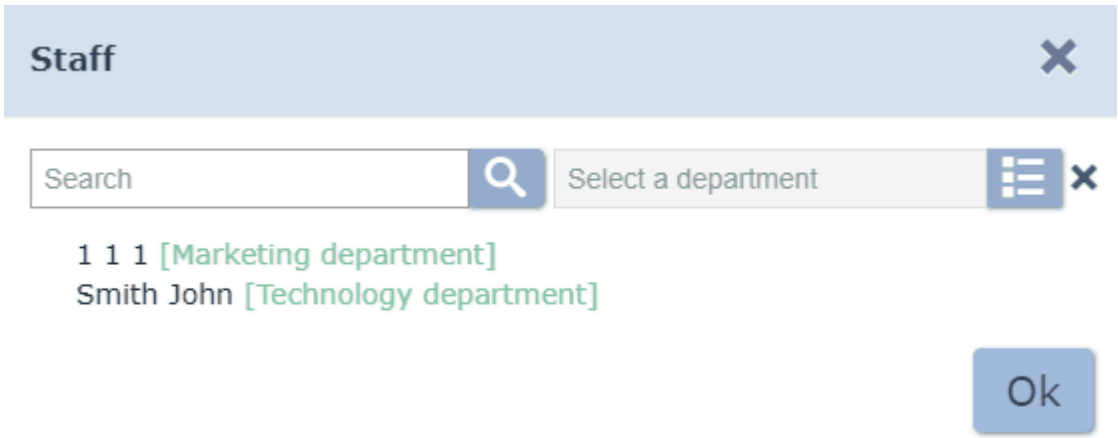
To create a Double-check access cards list:

1. Go to  ***«Administration»***.
2. Open ***«Configuration»*** subsection.
3. Switch to **Device** tab.
4. Select a controller on the page working area.

5. Click **Edit** on **Devices** panel. **Device properties** window will appear.
6. Switch to the **Double-check access cards list** tab. Page overview:



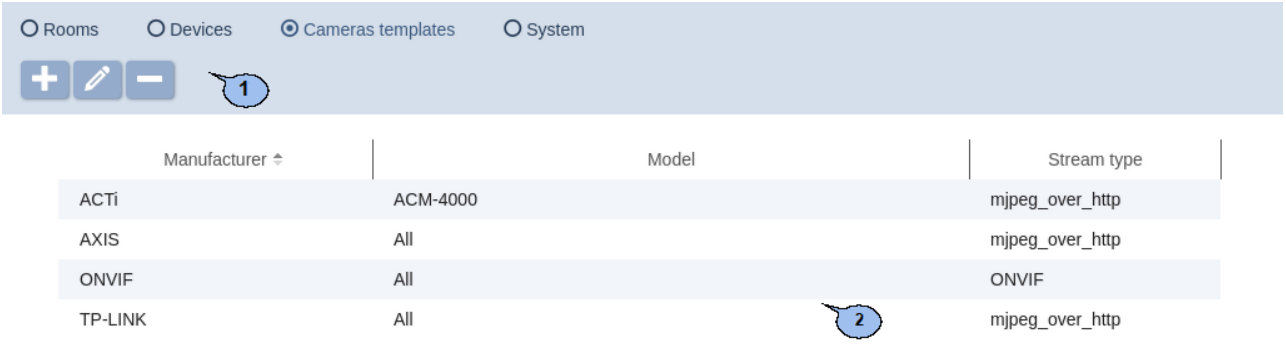
7. Click **Add** . **Staff** window will appear:



8. Select one or several employees by using **Search** and **Select Department** functions. Cards of the selected employees will become double-checking for the current controller.
9. Click **Ок**. **Employees** window will close and numbers of selected cards will be added to tab working area.
10. Select parameters saving method using the drop down list and click **Save**. **Device properties** window will close.

13.1.3 «Cameras templates» tab

Camera templates tab is designed for interface language selection and date format configuration. The tab also contains the software version information.
Page overview:



1. Panel toolbar contains:

   Add – Click to create a new camera template.

   Edit – click to edit a camera template that is selected on the page working area.

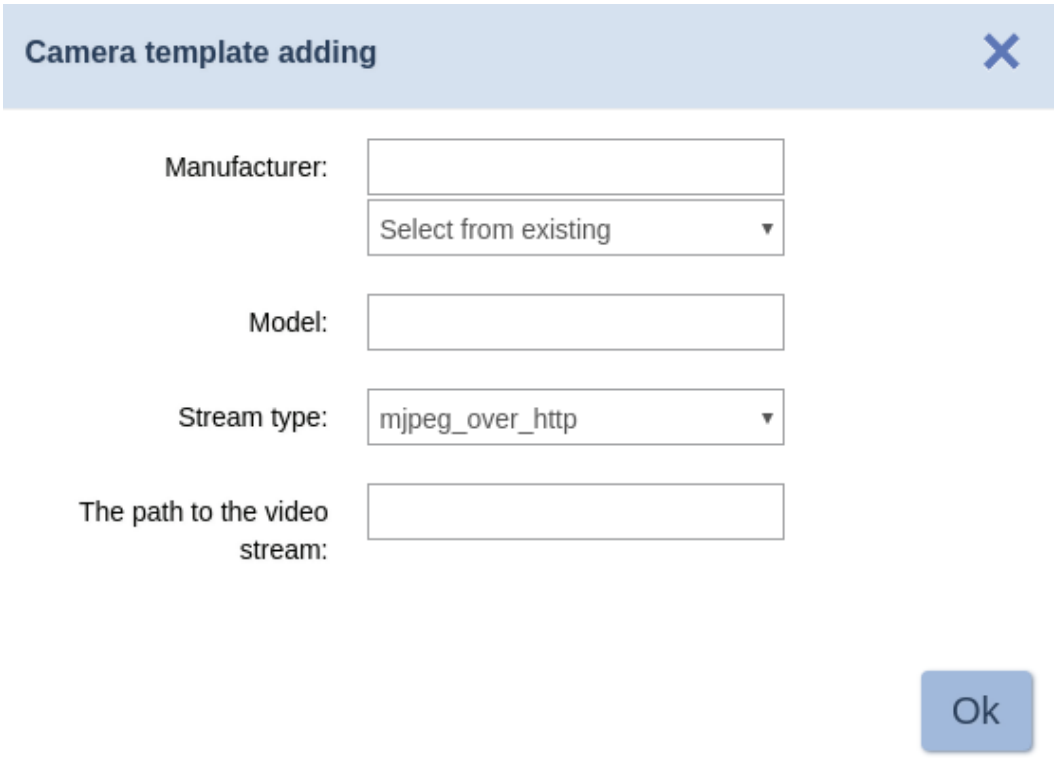
   Delete – click to delete a camera template that is selected on the page working area.

2. The page working area contains the list of created camera templates, manufacturer information, model and type of the stream.

Create camera template

To create a new camera template:

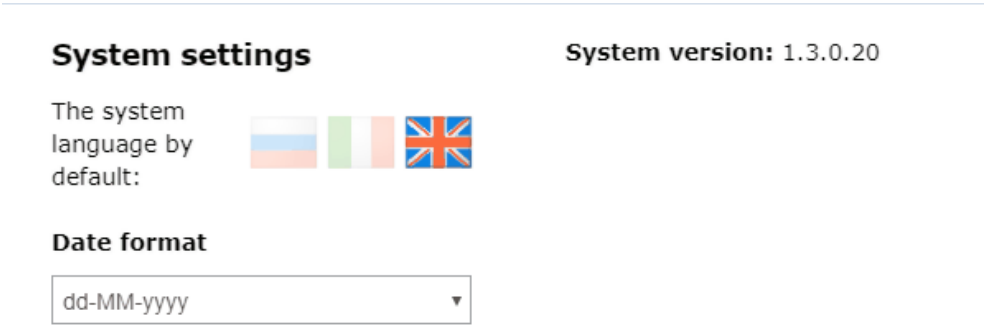
1. Go to ***«Administration»***.
2. Open ***«Configuration»*** subsection.
3. Switch to Camera templates tab.
4. Click Add button on the page toolbar. **Camera template adding** window will appear:



5. Configure parameters of the template in the appeared window. Click Ok button. **Camera template adding** window will close and new template will be added to the page working area.

13.1.4 «System» tab

System tab is used for interface language selection and date configuration. Software version information can be also found on this tab. Window overview:



13.2 «System events» subsection

Subsection is used for:

- creation of reports on events that have been registered by system devices and operators activity;
- real-time viewing of events that have been registered in the system.

Subsection page overview:

1. Subsection panel contains:

More – click to open command menu:

- **Export into XLS** – allows you to save the list of events as *MS Office Excel* spreadsheet file with *.xls* extension.
- **Export into CSV** – allows you to save the list of events as *OpenOffice Calc* spreadsheet file with *.csv* extension.
- **Reset filters** – click to Reset all applied filters (as well as the Departments).
- **Table display parameters**– allows you to call an additional window where you can select the columns that will be displayed on the page working area.

 **Advanced search** – click this button to configure filters for data that is displayed on the page working area.

 **Update data** – click to update data from the page working area in accordance to applied filters.

 – click to open calendar panel for date and time period that will be displayed on the page working area. Applied date and time are displayed near the correspondent button.

 **Apply –** click to create the list of events for the specified period.

Automatic update – registered events will be displayed in real-time mode when this option is checked.

Search – search input field. Click **Reset**  to clear the field.

2. The working area of the subsection contains registered events for the specified period.

Important:

- Functions of sorting by columns, changing width and changing column sequences are available on the page working area.
- The bottom area of the page contains data pages navigation tools.

3. Panel of Additional data contains information about event that is selected on the page working area.

13.3 «Tasks» subsection

Tab is designed for creation of events that are automatically executed by the system server. The following types of events are available:

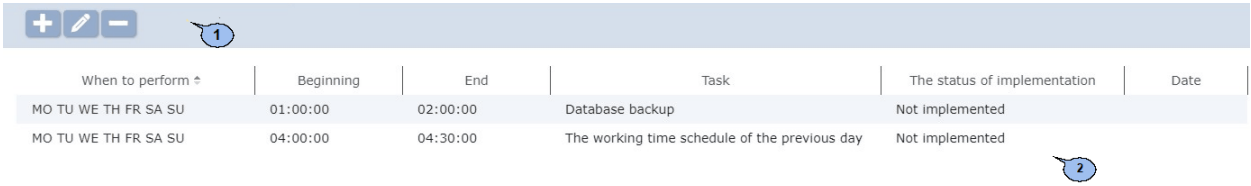
- *«Data base backup»* – it used for creating a DB backup. By default, the DB backup is stored in `C:\ProgramData\PERCo-Web` folder as a file with `.fbk` extension.
- *«Recording of working time for the previous day»* – is used for automatic calculation of worked time for the previous day. It allows you to speed up the output of reports in **«Time & Attendance»** section.

Important!

There are events of every type that are created in the subsection by default. It is possible to change the parameters of these events. Deleting of the event without adding a new one with the same type will lead to:

- DB backup deactivation,
- increase of the report camputation time.

Subsection page overview:



1. Page toolbar contains:

   Add – click to add a new task.

   Edit – click to edit parameters of the task that is selected on the page working area.

   Delete – click delete the task that is selected on the page working area.

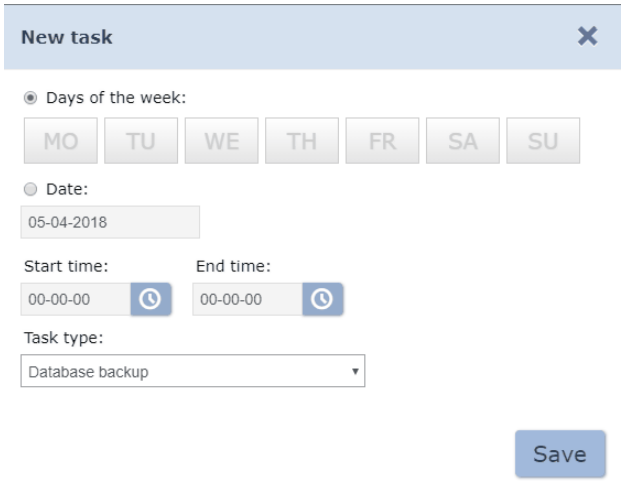
2. The tab working area contains the list of system server tasks. There are events of every type that are created in the subsection by default.

   Important:
   Functions of sorting by columns, changing width are available on the page working area.

13.3.1 Creation of a new task

To create a new system server task:

1. Go to ***«Administration»*** section.
2. Open ***«Tasks»*** subsection.
3. Click **Add** button on the page toolbar. **New task** window will appear:



4. Select the **Task type**:
   - **Data base backup**
   - **Recording of working time for the previous day**
5. Specify task run frequency by using the selector:
   - **Days of the week** – use this option if it necessary to run this task weekly. Specify days of the week when the task will be run.

- **Date** – use this option if it is necessary to run this task once. Specify the run date by using calendar.

Important:
It is recommended to specify the run period when there are minimum pass events registered and minimum operators that are connected to the server.

6. Specify the task run period within 24 hours by using **Start time** and **End time** entry fields.
7. Click **OK** after you've finished configuring. **Task** window will close. A new task will appear on the page working area.

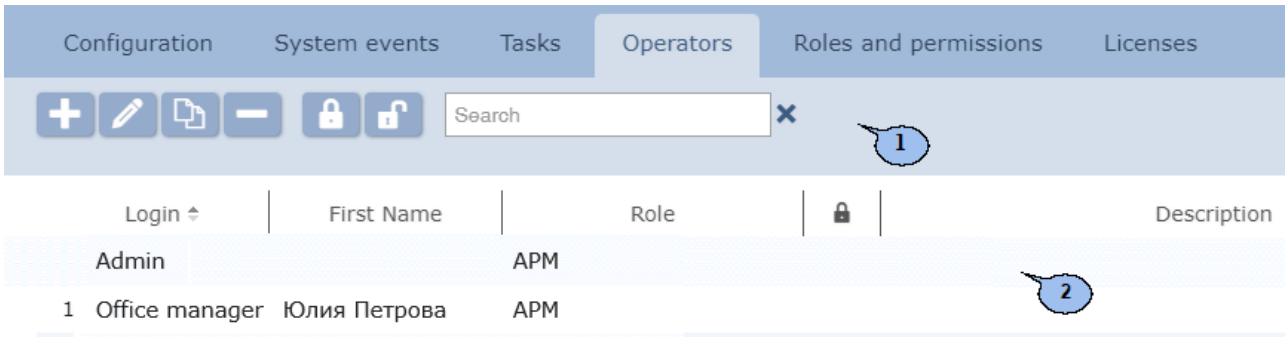
13.4 «Operators» subsection

Important:
Create roles of operators and give them permissions in ***«Roles and permissions»*** subsection of the ***«Administration»*** subsection before you start working with the section.

Subsection is used for:

- creating the list of operators, specifying their rights, roles and selecting sections that are available to them,
- temporary access blocking/ unblocking,
- data editing and deleting of the previously added operators.

Subsection page overview:



1. Page toolbar:

Add – click this button to add new operator.

Edit – click this button to change information of operator that is selected on the page working area.

Delete – click this button to delete the selected operator.

Block – click this button to temporary block access to operator that is selected on the page working area.

Unblock – click this button to unblock access to operator that is selected on the page working area.

Search – search input field. Click **Reset** to clear the field.

2. The page working area contains the list of operators. Sign indicates that system access for this operator is blocked.

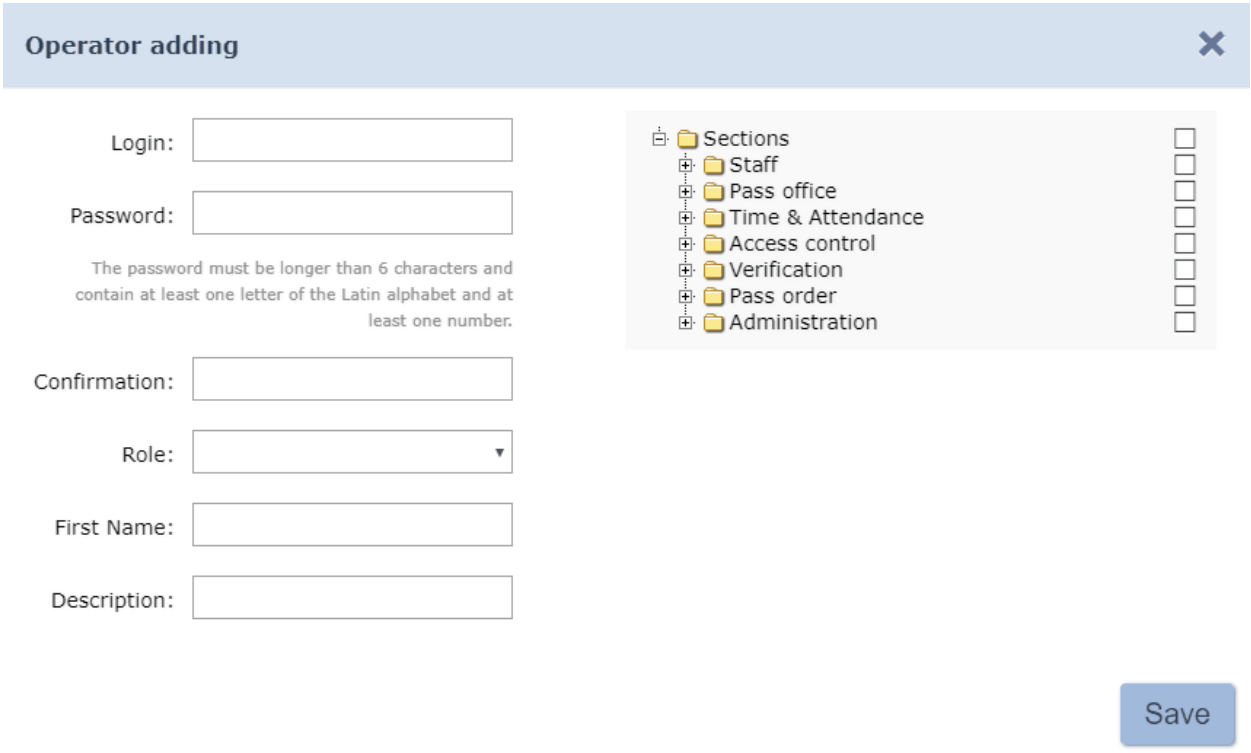
Important:
Functions of sorting by columns, changing width are available on the page working area.

13.4.1 Adding system operator

Important:
Create roles and give them privileges before you start working with this subsection. Visit **Roles and permissions** section of ***«Administration»*** section**.**

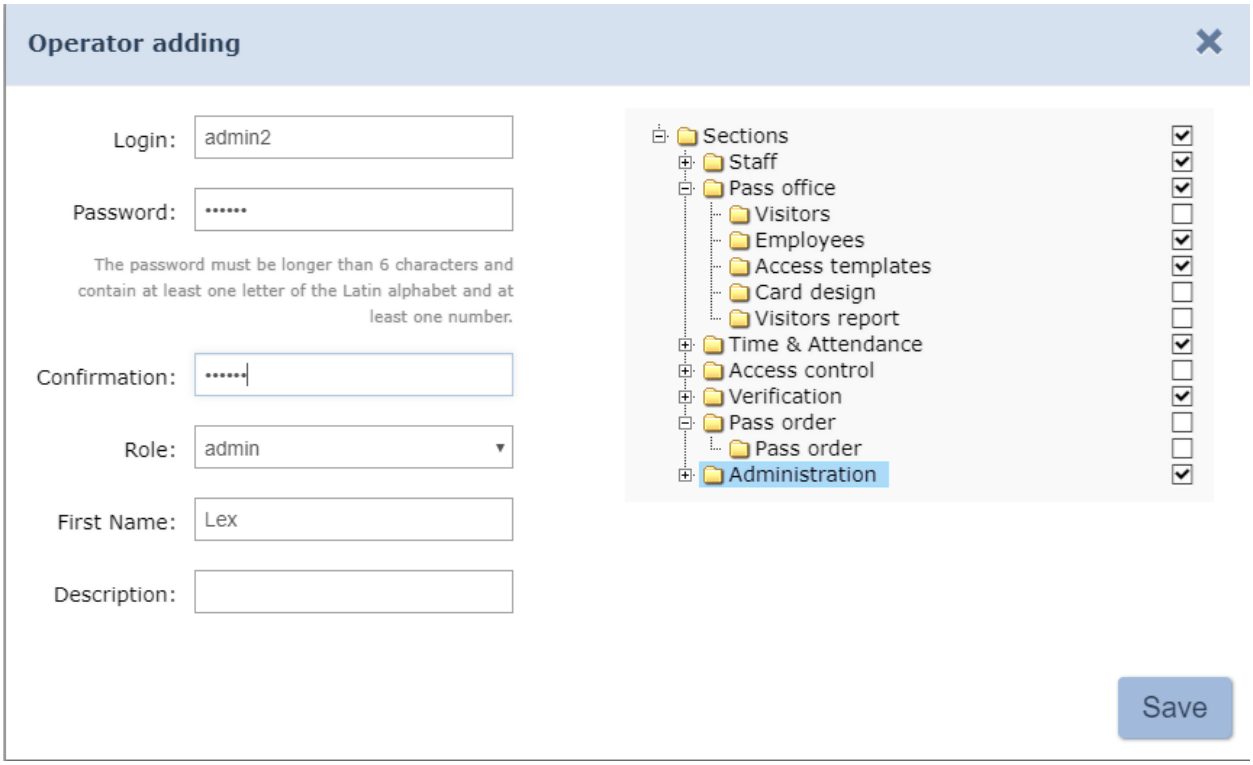
To add a new operator:

1. Go to ***«Administration»*** section.
2. Open ***«Operators»*** subsection.
3. Click **Add** button on the tab toolbar. **Operator adding** window will appear:



4. Specify login and password for operator by using the correspondent fields.
5. Specify the role of operator and his privileges by using **Role** drop down list. Roles of operators can be created in ***«Operator rights»*** section.
6. Specify the **Name** and the **Description** of the operator if needed.

Page overview:



7. Operator can use reader to check the card number and can use table fingerprint reader to undertake reading procedure. In order to allow operator to use these USB devices: check **Reader** and **Table fingerprint reader** options.
8. If operator will not use reader and/or fingerprint reader: select the controller with its readers which will be used for entering the card numbers and/or fingerprint reading. Click **Select from list** button that is located on the right side of the **Controller** field and/or **Fingerprint controller** field. Select desirable controller.
9. Check subsections and subsection tabs that will be available to operator by using **Access to sections** option.

Important!

- Operator gets full access permissions to system controllers if you grant him access to ***«Configuration»*** subsection of ***«Administration»*** section. In this case, operator will get access regardless privileges and role that is applied to him. This might lead to unauthorized access to the premises.
- Operator will be able to create new roles and change parameters of the previously created roles if he has access to **«Roles and permissions»** subsection, ***«Administration»*** section. This might lead to unauthorized editing of the roles access permissions.

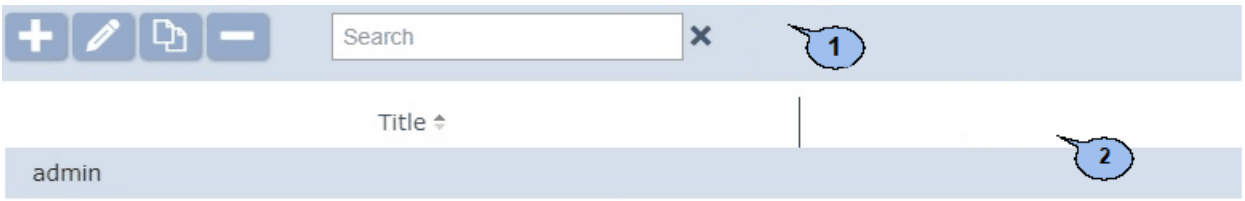
10. Click **Save**. **Operator adding** window will close. A new operator will be added to the list that is located on the page working area.

13.5 «Roles and permissions» subsection

Subsection is used for:

- creating roles and giving access permissions,
- editing and deleting of the previously created roles of operators.

Subsection page overview:



1. Page toolbar:

   Add – click this button to add new operator role.

   Edit – click this button to edit name, description and access permissions of the role that is selected on the page working area.

   Copy – click this button to add a new role that is based on the previously created.

   Delete – click this button to delete a role that is selected on the page working area.

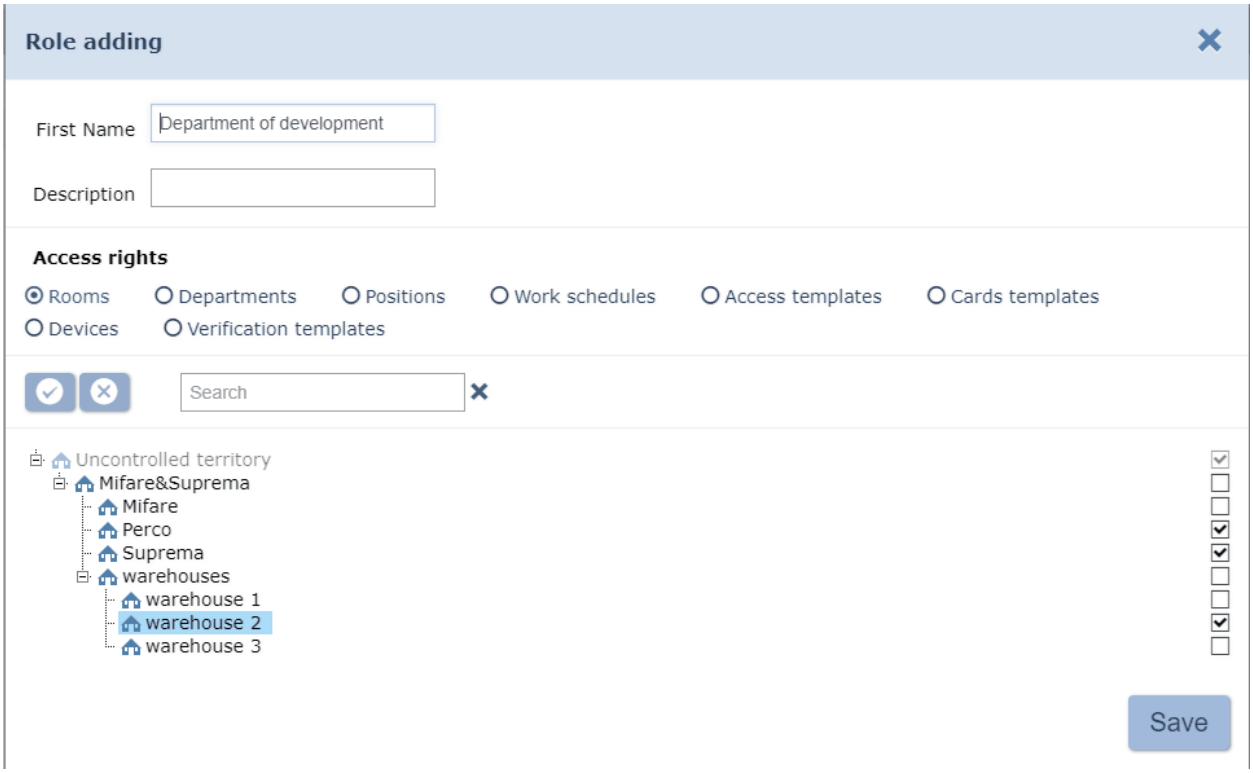
2. The page working area contains the list of the previously created roles.

   Important:
   Functions of sorting by columns, changing width are available on the page working area.

13.5.1 Role adding (access permissions)

To add a new role:

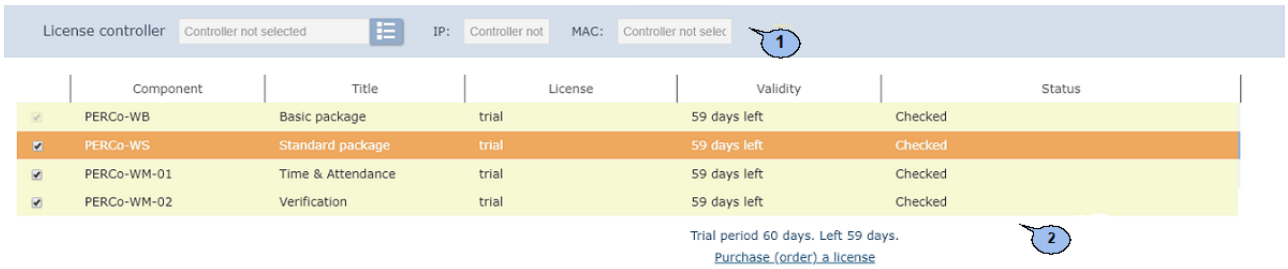
1. Go to ***«Administration»***.
2. Open **«Roles and permissions»** subsection.
3. Click **Add** button on the tab toolbar. **Role adding** window will appear:

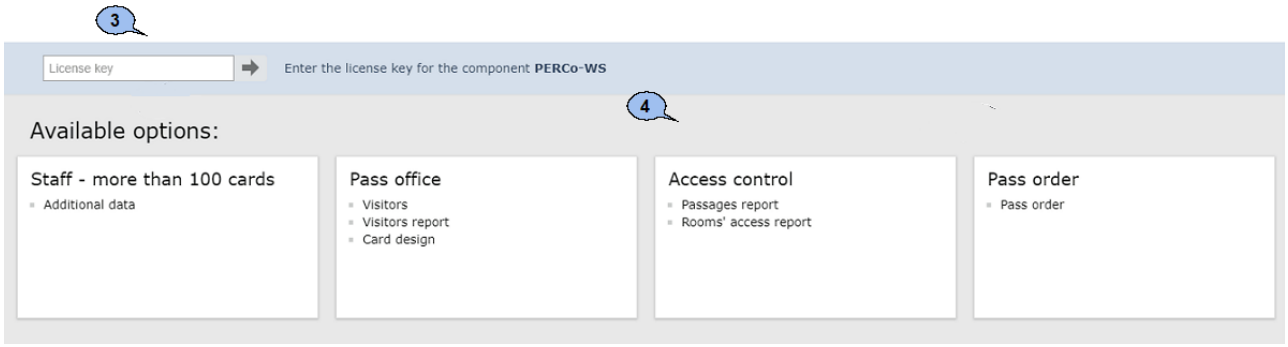


4. Specify the **Name** of the role and use the **Description** field if you want to enter additional information.
5. Give access permissions to the role. To do this: select the type of permissions by using the selector. Upon that, the list of such available objects will appear on the page working area. The following types of access permissions are available:
   - **Rooms**
   - **Departments**
   - **Positions**
   - **Work schedules**
   - **Access templates**
   - **Verification templates**
   - **Cards templates**
   - **Controllers**
   - **Devices**
   - **Verification templates**
6. Check those objects, which you would like to give operator privileges to. Use **Select all** and **Deselect** buttons if needed.
7. Select another type of objects and give access permissions to it.
8. Click **Save**. **Role adding** window will close. New role will be added to the list on the page working area.
9. To add new operator: open ***«Operators»*** subsection.

13.6 «Licenses» subsection

This subsection is designed for entering activation codes for the installed software modules. Subsection page overview:





1. **Licensed controller** panel contains a **Select controller** button. You can use this button to select a controller which will be used as electronic protection-key of the system software and field that displays IP and Mac addresses of the selected controller.
2. Tab working area contains the list of installed modules.

   Important:
   Functions of sorting by columns, changing width are available on the page working area.
3. **License key** – a field where you should enter activation code. The panel appears after you select one of the modules from the page working area.
4. **Available options** panel contains the list of system sections and subsections that are available for the selected module.

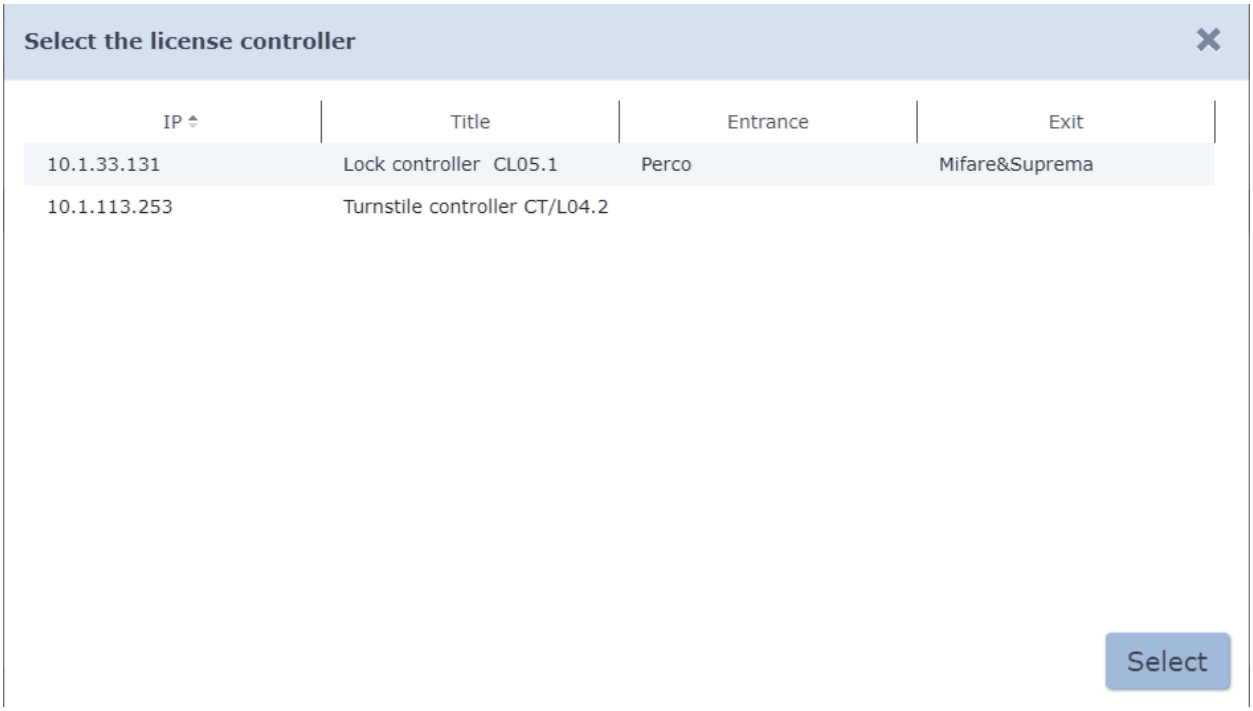
13.6.1 Entering the activation code

To enter the software activation code:

1. Go to ***«Administration»*** section.
2. Open ***«Licenses»*** subsection.

   Important:
   Controller that is used as electronic protection-key of the software must be added to the system configuration on the ***Devices*** tab from the ***«Configuration»*** subsection.

3. Click **Select controller** button on the **Licensed controller** panel. **Select the licensed controller** window will appear:



4. Select a controller in the appeared window that is used as a software electronic protection-key. Click **Select**.
5. **Select licensed controller** window will close. Name, IP and MAC addresses of the controller will appear on the **Licensed controller** panel.
6. Select the module name which you would like to activate.
7. Find activation code from the licence agreement and enter it in the **License key** field. The code must be entered without spaces. Click **Send** button that is located on the right side of the field.
8. The system server will check the entered activation code. A word *«activated»* will appear near **Licenses type** field if the activation procedure has been successfully completed.
9. A warning window will appear if the activation code has been entered incorrectly or this code doesn't correspond to the selected software module (controller) or in case of the faulty connection with the controller.

14 PERCo controller parameters

The list of available tabs can be different depending on the type of the controller. The following tabs are available:

- **External connections**– this tab contains information about external connections of the controller;
- **Alarm generator**;
- **Additional inputs**;
- **Additional outputs**;
- **Additional input-output**;
- **CL-05.1 lock** ;
- **OD** (Lock, Turnstile);
- **General**;
- **LICON properties and Lines**;
- **Status** – this tab informs about status of the controller;
- **Double-check access cards list**;
- **Reader**.

14.1 «General» tab

This tab contains two subtabs:

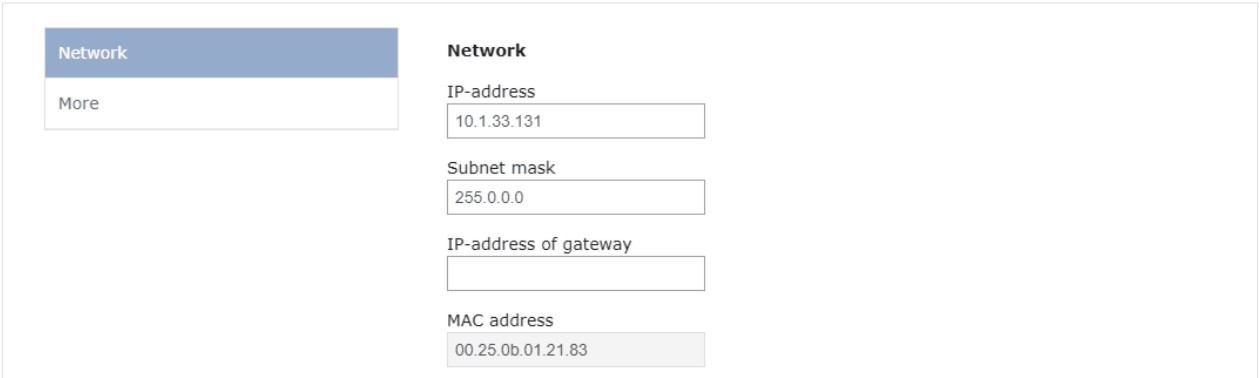
- **More;**
- **Network.**

14.1.1 «Network» subtab

This tab displays information about network parameters:

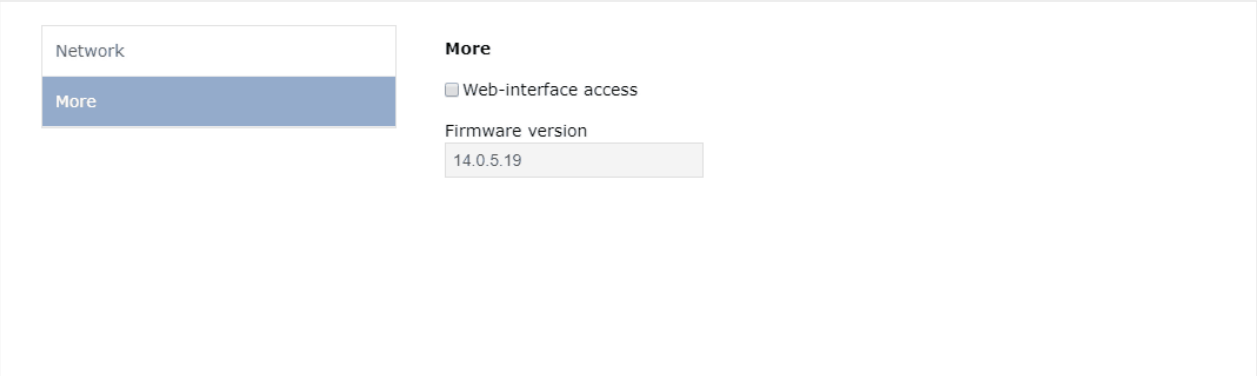
- **IP-address;**
- **Subnet mask;**
- **IP-address of gateway;**
- **MAC-address.**

Window overview:



14.1.2 «More» subtab

This subtab contains the following parameters:



Firmware version – the current version of the firmware is displayed in the field.

14.2 OD tab («Lock», «Turnstile»)

Forward passage direction . This parameter changes readers numeration towards the passage direction.

- By default, the numeration of readers corresponds to the position of the «reader number» (XP2) jumper which is placed on the board (in ***PERCo*** turnstiles: right reader - №1, left reader - №2).
- If this parameter is switched off: the reader that must have №1 (or odd number) according to the jumper position – will be detected in the controller as №2 (even number) and vice versa.

Normal (i.e blocked) contact state (OD input) (Normally opened / Normally closed). This parameter allows you to specify the state of the door sensor when the OD is in blocked state.

Normal "Closed" state of the OD output (Deenergized / Energized). This parameter indicates if the OD output is energized (control voltage is applied to relay or transistor) when the OD is blocked.

OD output normalization (After «Opening» / After «Closing»). This parameter defines the moment of the OD output normalization.

Unblocking time limit. This parameter allows to specify the time period at the end of which the controller will inform that *«OD is not closed after passage with identificator»* because OD is not blocked.

Unblocked state holding time (Identificator analysis time). OD unlocking period.

Double-checking waiting period. This parameter allows you to limit the time period between presenting of the access and double-checking cards if the card access permissions are set to access with double-checking / access with supervision / transit confirmation with the driver card.

Passage registration with identifier presentation. The passage will be considered as completed by the controller right after identificator presentation. This will be done regardless to the actual passage through OD.

Important!

It is impossible to carry out the following operations for **Readers** of both passage directions when you apply **Passage registration with identifier presentation** parameter:

- set values that differ from **No** for **Permissions confirmation** parameter (i.e. it is prohibited to carry out the verification procedure with the RC);
- carry out verification procedure with the software.

Non-compliance of the abovementioned might lead to malfunction of the (Antipass) zonality control function.

It is also not recommended to set **Protection from passage of identificator** parameter to **Hard** mode, when you apply this parameter.

Internal protection from passage of identificator (Local Antipass). The controller can trace incidents of card representment to the same reader.

OD output operational mode. This parameter allows you to select OD operational mode.

- **Potential.**
- **Pulse** – this mode is used only by locks that support it. It is recommended to use it with self-cocking electromechanical locks that are opened with fast pulse (for example «CISA» locks).

Fire Alarm in "Security" mode. When checked, the emergency unlocking (OD passage opening) will be done even when the security zone and its OD are in alarmed mode. Signals that have **type: Fire Alarm** will be ignored in «Armed» ACM when this parameter is unchecked (by default).

14.3 «Lock CL05.1» tab

Normal (i.e blocked) contact state (OD input) (Normally opened/ Normally closed). This parameter allows you to specify the state of the door sensor when the OD is in blocked state.

Normal "Closed" state of the OD output (Deenergized/ Energized). This parameter indicates if the OD output is energized (control voltage is applied to relay or transistor) when the OD is blocked.

OD output normalization (After «Opening»/ After «Closing»). This parameter defines the moment of the OD output normalization.

Unblocking time limit. This parameter allows to specify the time period at the end of which the controller will inform that *«OD is not closed after passage with identificator»* because OD is not blocked.

Unblocked state holding time(Identificator analysis time). OD unlocking period.

Double-checking waiting period. This parameter allows you to limit the time period between presenting of the access and double-checking cards if the card access permissions are set to access with double-checking / access with supervision / transit confirmation with the driver card.

Passage registration with identifier presentation. The passage will be considered as completed by the controller right after identificator presentation. This will be done regardless to the actual passage through OD.

Important!

It is impossible to carry out the following operations for **Readers** of both passage directions when you apply **Passage registration with identifier presentation** parameter:

- set values that differ from **No** for **Permissions confirmation** parameter (i.e. it is prohibited to carry out the verification procedure with the RC);
- carry out verification procedure with the software.

Non-compliance of the above mentioned might lead to malfunction of the (Antipass) zonality control function.

It is also not recommended to set **Protection from passage of identificator** parameter to **Hard** mode, when you apply this parameter.

Internal protection from the passage of identificator (Local Antipass). The controller can trace incidents of card representment to the same reader.

OD output operational mode. This parameter allows you to select OD operational mode.

- **Potential**
- **Pulse** – this mode is used only by locks that support it. It is recommended to use it with self-cocking electromechanical locks that are opened with fast pulse (for example «CISA» locks).

Zone change while passing. This parameter activates the feature of zone changing when passing through OD.

Fire Alarm in "Security" mode. When checked, the emergency unlocking (OD passage opening) will be done even when the security zone and its OD are in alarmed mode. Signals that have **type: Fire Alarm** will be ignored in «Armed» ACM when this parameter is unchecked (by default).

14.4 «LICON properties» and «Lines» tabs

LICON properties tab contains parameters of the ***CR01 LICON*** controller. **Lines** tab allows you to change the content of messages that are displayed on LCD-display.

Forward passage direction . This parameter allows you to specify the direction which will be considered as entrance. The right reader is considered as enter, left – as exit when the parameter is applied. Everything works vise versa when this parameter is not applied.

Important:

«Enter» and *«Exit»* LCD messages will not be changed even after change of the passage direction. The text can be edited in **Localization of the displayed data** drop down menu.

Working time balance indication. Balance of working time and violation information of the presented card will be displayed on LCD in addition to event registered time.

Server response waiting time (2 sec. by default). Entry field can be used for specifying time while controller is waiting for the server response. The response contains personal information (full name) of the presented access card. The card number will be displayed on LCD screen if it is impossible to obtain the personal information.

Employee personal information display time (2 sec. by default). Personal information of the presented access card will be displayed on LCD screen according to parameter that is set in this entry field.

14.5 «Additional inputs» tab

Additional inputs of controllers can be used for monitoring status of the external equipment that is connected to it. Inputs can be used for connection of the alarm reset button or FireAlarm input emergency unlocking command issuing device etc. The following parameters are available:

Type. A drop down list allows you to select from one of the following variants:

- **No**. There are no devices that are connected to this input.
- **Normal output**. This input will be used for connecting of the external device. Status of this device must be monitored by the controller. It is possible to configure the controller response protocol for commands that are sent by the external device.
- **Special**. It is used for autonomous alarm reset, switching off the siren.
- **FireAlarm input**. It is used for emergency unlocking command issuing device connection and opening of Fire Alarm OD.

Normal state of the contact (*Opened/Closed*). Selection of this parameter depends on the type of connected equipment. This parameter defines which controller input level is considered as normalized.

Important:
Normal state of the contact parameter is not available for input type: **FireAlarm input**. The constant **Closed** value is applied.

The other output parameters can differ depending on the selected type.

Normal output

Subnet mask/activation/normalization time criteria:

- **For the specified time**. Selected additional inputs will be masked/ activated/ normalized for the specified time.
- **During actuation time**. Selected additional inputs will be masked/ activated/ normalized for the whole period of time while this input receives control signals.
- **During actuation time and after**. This parameter is a combination of the two previous. Selected additional inputs will be masked/ activated/ normalized for the time while this input receives control signals and for the specified time.

Additional inputs, masked when activated. This parameter allows to specify controller additional inputs that must be masked (i.e. they will not react on control signals received from the external device) while receiving control signals from the connected external device. Select those additional inputs that should be masked. Specify the mask time criteria.

Additional outputs, masked when activated. This parameter allows you to specify controller additional outputs that must be activated while receiving control signals from the connected external device. Select those additional outputs that should be activated. Specify the activation time criteria. It should be noted, that activation of relay-controlled output that is connected with activation of additional input doesn't consider possible shunting of this input. It is important in cases when passage control sensor is used.

Additional outputs, normalized when activated. This parameter allows you to specify controller additional outputs that must be normalized receiving control signals from the connected external device. Select those additional outputs that should be normalized. Specify normalization time criteria.

Special

Alarm reset (Alarm generator). This parameter will reset the alarm after the output will receive the control signal.

14.6 «Additional outputs» tab

Additional outputs can be used for operating any external equipment. The following parameters are available for configuration:

Important:
Deenergizing will lead to normalization of all outputs.

Type. The drop down list offers the following types of outputs for selection:

- **No**. There is no external device that is connected to this output.
- **Normal output**. This input will be used for connecting to the external devices. Status of this device must be monitored by the controller. It is possible to configure the controller response protocol for commands that are sent by the external device. Additional equipment is connected to the output. Operation of this device is similar to the other system devices (except Alarm generator).
- **Alarm generator**. The decision on activation of the additional output is based on parameters that are applied to **Alarm generator**.

Normalized state (Deenergized/ Energized). This parameter defines if the control voltage is applied to output relay in normalized output state. For outputs №1 and №2 normalized state: Deenergized.

Activization time. During this period of time, the output will change its state from normalized to the opposite state if there is a command received.

14.7 «Additional input-output» tab

Type. A drop down list allows you to select from one of the following variants:

- **No**. There are no devices that are connected to this input.
- **Normal output**. This input will be used for connecting of the external device. Status of this device must be monitored by the controller. It is possible to configure the controller response protocol for commands that have been sent by the external device.
- **Alarm generator**. The decision on activation of the additional output is based on parameters that are applied to **Alarm generator**.

- **FireAlarm input**. This output is intended to be used for the connection of command issuing device that is responsible for emergency Fire Alarm passage unlocking.
- **Synchronizing input/output**. This output is used for synchronization of two controllers when arranging ACP for bidirectional passage. The controllers have to be connected to each other through outputs.

Normal state of the contact (*Opened/ Closed*). The selection of this parameter depends on the type of connected equipment. This parameter defines the signal level. This parameter defines which controller input level is considered as normalized.

14.8 «Alarm generator» tab

This resourse is connected to OD controller and allows to select events that have to generate alarm signals of the controller and relevant operation of the alarm output (one of the relay-controlled outputs that has **Type: Alarm generator**). The following parameters are available:

Alarm generation on identificator presentation. This parameter allows you to specify the types of events that are connected to access card presentation. The alarm signal will be generated after registration of such event. It is possible to select the type of alarm for every type of event:

- **No.**
- **Silent.** The alarm is generated but the outputs which have **Type: Alarm generator** will not be activated.
- **Loud.** The alarm will be generated.

Alarm generation on unauthorized OD unblocking. This parameter is used for configuring ACM *«Control»* and *«Closed».* It is possible to switch on the generation of alarm in case of OD mechanical unblocking with key (i.e. bypassing the controller command).

Alarm generation on unacceptably long OD opening. This parameter is used for configuring ACM *«Control».* It is possible to configure the alarm generation if OD has not been normalized after opening during the **Critical opening period** that is specified for this OD.

Alarm generation on controller housing opening. Select if the alarm signal will be generated in case of the controller housing opening.

14.9 «Reader» tab

This resourse is connected to OD controller and helps to configure parameters of verification, timed access, card pass protection (Antipass) parameter. The following parameters are available:

Protection against EMPLOYEES/VISITORS identifiers handover (Antipass). This parameter is used for configuring controller reaction on employee/visitor card presentation if he has violated zonality control function (Antipass). It is possible to select one type of control for every ACM of the controller:

- **No.** The controller doesn’t consider zonality of the card when granting access.

- **Soft**. The controller will grant access whilst it will register the monitored event *«ID Card presentation, zonality violation». «Passing by card with zonality violation»* event will be registererd after passing.
- **Hard**. The controller will deny access by card whilst it will register the monitored event *«ID Card presentation, zonality violation». «Passing by card with zonality violation»* event will be registererd after passing. Verification procedure will be launched afterwards if **RC verification (or Software verification)** parameter is applied to reader.

Time control for the EMPLOYEES/VISITORS identifiers. This parameter is used for specifying controller reaction on employee/visitor card presentation for the selected ACM when timed access criteria has been applied. It is possible to select one type of control for every controller ACM:

- **No**. The controller doesn't monitor timed access criteria of the card.
- **Soft**. The controller will grant access for the presented card whilst it will register the monitored event as *«ID Card presentation, time violation». «Passing by card with time violation»* event will be registererd after passing.
- **Hard**. The controller will deny access by card whilst it will register the monitored event *«ID Card presentation, Time violation». «Access denied, timed access violation»* event will be registered. Verification procedure will be launched afterwards if **RC verification (or Software verification)** parameter is applied to reader.

Additional inputs, masked on OD unblocking. This parameter allows to specify which additional inputs of the controller must be masked (i.e. they will not respond to command signals sent by external devices) during OD unblocking. Select additional inputs that must be masked. Configure mask time criteria.

Mask time criteria:

- **For the specified time**. Selected additional inputs will be masked for the specified time.
- **During actuation time**. Selected additional inputs will be masked till OD is unblocked.
- **During actuation time and after**. This parameter is a combination of two previous. Selected additional inputs will be masked till OD is unblocked, plus the specified time.

Additional outputs, activated during OD unblocking. This parameter allows you to select additional outputs of the controller that will be activated during OD unblocking. Select additional outputs that must be activated. Configure activation time criteria.

Additional outputs, normalized during OD unblocking. This parameter allows you to select additional outputs of the controller that will be normalized during OD unblocking. Select additional outputs that must be normalized. Configure normalization time criteria.

Normalization/activation time criteria:

- **For the specified time**. The output is activated/ normalized for the specified time. The countdown begins from the moment card presentation regardless of access permission/denial.

- **During actuation time**. The output is activated/ normalized for the specified time. The countdown begins from the moment of OD unblocking. The output will be switched to its original state after OD unblocking or upon the expiration of the unblocking state holding period.
- **During actuation time and after**. This parameter is a combination of two previous. The output is activated/ normalized for the specified time, from the moment of OD unblocking and till its blocking, plus the specified period, or upon the expiration of the unblocking state holding period if the passage has been omitted.

Additional outputs activated on EMPLOYEES valid identifiers presentation. This parameter is used for specifying outputs that will be activated on access card presentation that has access privileges to the controller (the card is not blocked and has not expired). This parameter can be used when additional indication is applied to additional outputs. This indication gives information to operator about card status. Select additional outputs that must be activated. Set the activation time criteria.

RC confirmation. This parameter allows you to specify whether the request will be formed and sent to verification device when ACM «Control» is used. The following devices can be used as verification devices: RC, card capture reader or other equipment.

- **No**. The confirmation of the verification device is not needed.

  Important:
  If **Passage permission confirmation** value differs from NO, then access can be confirmed by RC button.

- **Yes**. This parameter is used for card capture configuration and RC or software verification. It is possible to configure verification method indipendently for employees and visitors:
  - **during passage** – Verification is used for every passage;
  - **during passage with time violation** – Verification is used for passages with time violation (**Identificator time control parameter** must be set to Hard position).
  - **passage with zonality violation** – Verification is used in case of reentrancy without exiting (**Protection from the pass of identificator** parameter must be set to **Hard** mode).

Confirmation waiting period during verification. This parameter allows you to set confirmation waiting period.

RC confirmation. Check this parameter if you would like to use the RC in ACM *«Control»* with this reader.

Withdraw visitor identificator after passage. The presented card will be withdrawn after passage if the parameter is checked. The data will be sent to Archive. This option is available only when there is a connection between system server and the controller.

15 Parameters of the Suprema controller

The list of parameters can differ depending on the type of the controller. The following tabs are available:

- **General**;
- **Lock**;
- **Reader**.

The global configuration of light and aural indication for all **Suprema** controllers is set on **Suprema controllers** tab.

Important:

For integration biometric controllers should have inner software ("firmware") version not less than:
for controller BioEntry W2 – 1.1.1;
for controller BioEntry Plus (platform BioStar 2) – 2.3.1.

15.1 Tab «General»

Tab consists of two subtabs:

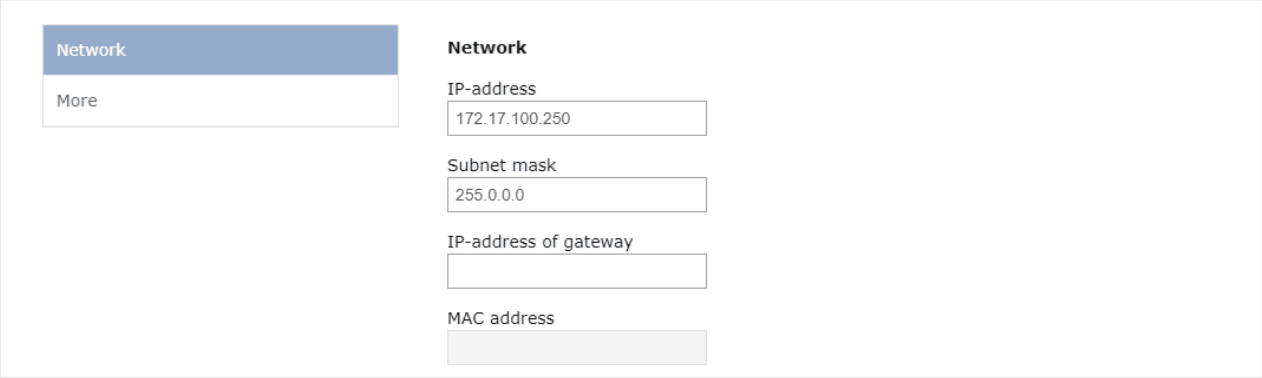
- «**Network**»;
- «**More**».

15.1.1 «Network» subtab

This subtab displays information about following network parameters:

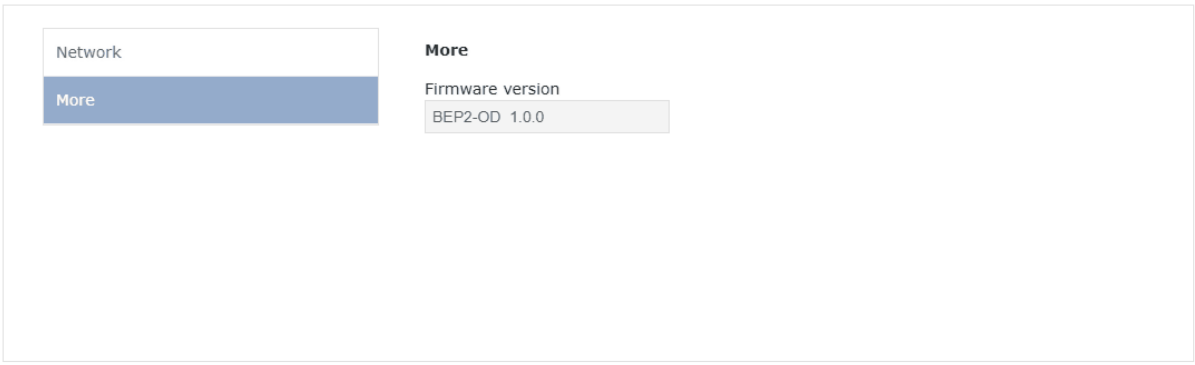
- **IP-address**;
- **Subnet mask**;
- **IP-address of gateway**;
- **MAC-address**.

Window overview:



15.1.2 «More» subtab

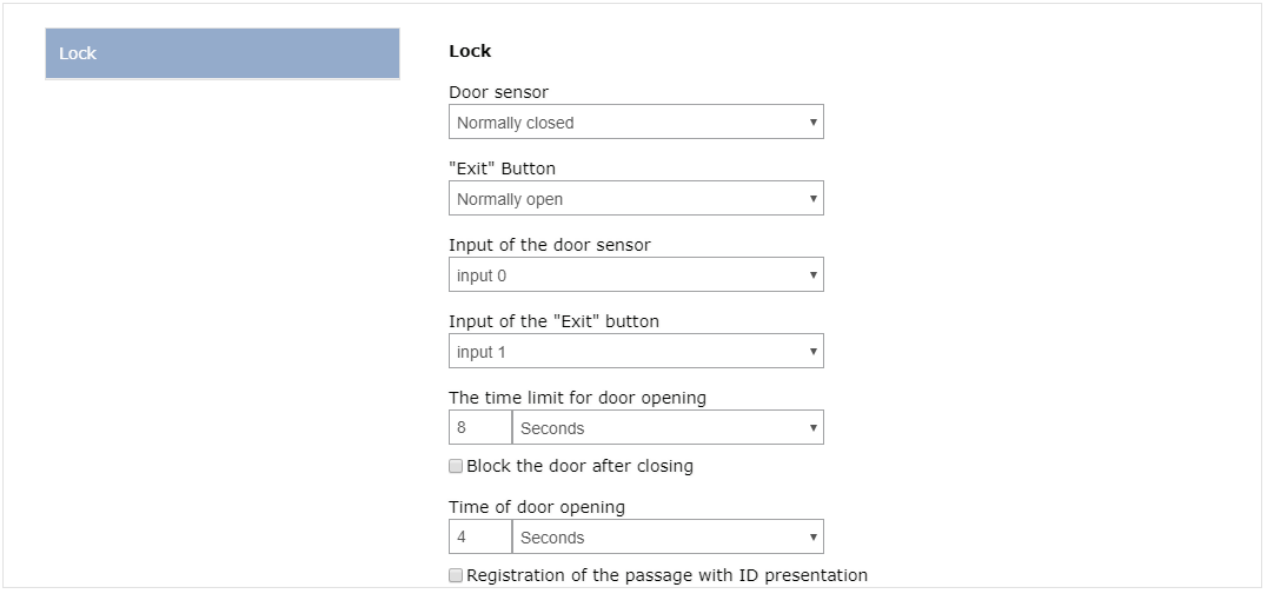
This subtab contains the following parameters:



Firmware version – software version of the controller is displayed in this field.

15.2 «Lock» tab

«Lock» tab contains the following parameters:



- **Door sensor.** This drop down list is used for specifying the normal state of the door sensor (sealed contact):
  - **Normally closed**;
  - **Normally opened**.

  Important:

  The state of the sensor is considered as normal when the door is locked. Consequently, if the door sensor is in the normally closed state when the door is locked, then it is necessary to select **Normally closed** pararameter**.**

- **'Exit' button**. Use the drop down list to select one of the following options of the **'Exit' button**:
  - **Normally closed**;
  - **Normally opened**.

Important:
The state of the **'Exit' button** is considered as normal when the door is blocked. Consequently, it is necessary to select **Normally closed** option if it is meant that the relay contact unlocks after the **'Exit'** button is held down (i.e. the relay changes its state).

- **Door sensor input**. Use the drop down list to select the controller input that will be used for connection of the **door sensor**:
  - **Input 0**;
  - **Input 1**.
- **'Exit' button input**. Use the drop down list to select the controller input that will be used for connection of the **'Exit' button**:
  - **Input 0**;
  - **Input 1**.

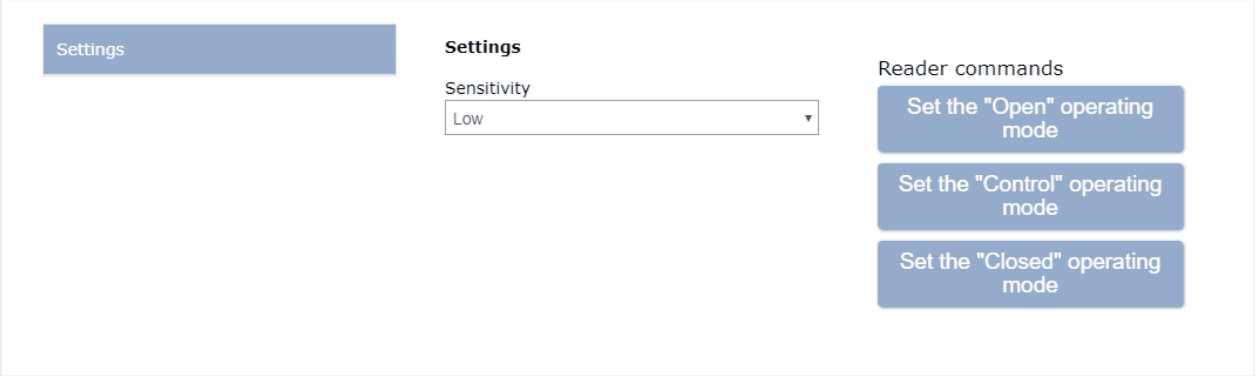
  Important:
  It is Hardly not recommended to connect the **door sensor** and **'Exit' button** to the same input of the controller.
- **Door opening waiting limit** – The controller will switch to alarm mode at the end this period because the door was not locked and blocked. A drop down list allows to set the value and to select units of measurement:
  - **Milliseconds**;
  - **Seconds**;
  - **Infinity**.
- **Door opening time** – a period while the door is switched to unblocked state for opening. A drop down list allows to set the value and to select units of measurement:
  - **Milliseconds**;
  - **Seconds**;
  - **Infinity**.

The door will be blocked after closing if **Block door after closing** option is checked.

If **Passage registration with identifier presentation** option is checked, then the passage will be registered right after presentation of identificator, i.e. – without signals from turnstiles, door sensor etc.

15.3 «Reader» tab

«Reader» tab contains the following parameters:



- **Sensitivity.** Use the drop down list to specify the reader sensitivity:
  - **Low;**
  - **Level 1;**
  - **Level 2;**
  - **Level 3;**
  - **Level 4;**
  - **Level 5;**
  - **Level 6;**
  - **High.**

  Important:
  Sensitivity parameter defines sensitivity of the fingerprint scanning sensor. High sensitivity level provides high quality and high speed of the scanning. Low sensitivity level reduces environmental factor – temperature, humidity, premises lighting conditions, surface condition of the scanning area (finger pads). The manufacturer recommends to use high sensitivity level by default. It is possible to lower sensitivity level when necessary.

The following reader commands are supported:

- **Set the "Open" operating mode** – this access control mode unblocks OD. The passage switches to free mode and the procedures of card presentation and fingerprint scanning are skipped;
- **Set the "Control" operating mode** – the passage is done in normal mode by card presentation and/or fingerprint scanning procedure;
- **Set the "Closed" operating mode** – this access control mode blocks OD, blocks passage, the reader will not respond to presentation of a card and/or fingerprint scanning.

16 Camera settings

Listed below tabs are designed for IP-cameras settings (incl. Cameras with ONVIF standard) and analog cameras, connected to IP-servers. The following tabs are available:

- **Camera;**
- **About camera;**
- **Video.**

16.1 Camera

In Camera tab it's necessary to insert data for authorization to control the camera.

Camera settings:

- **Login;**
- **Password**.

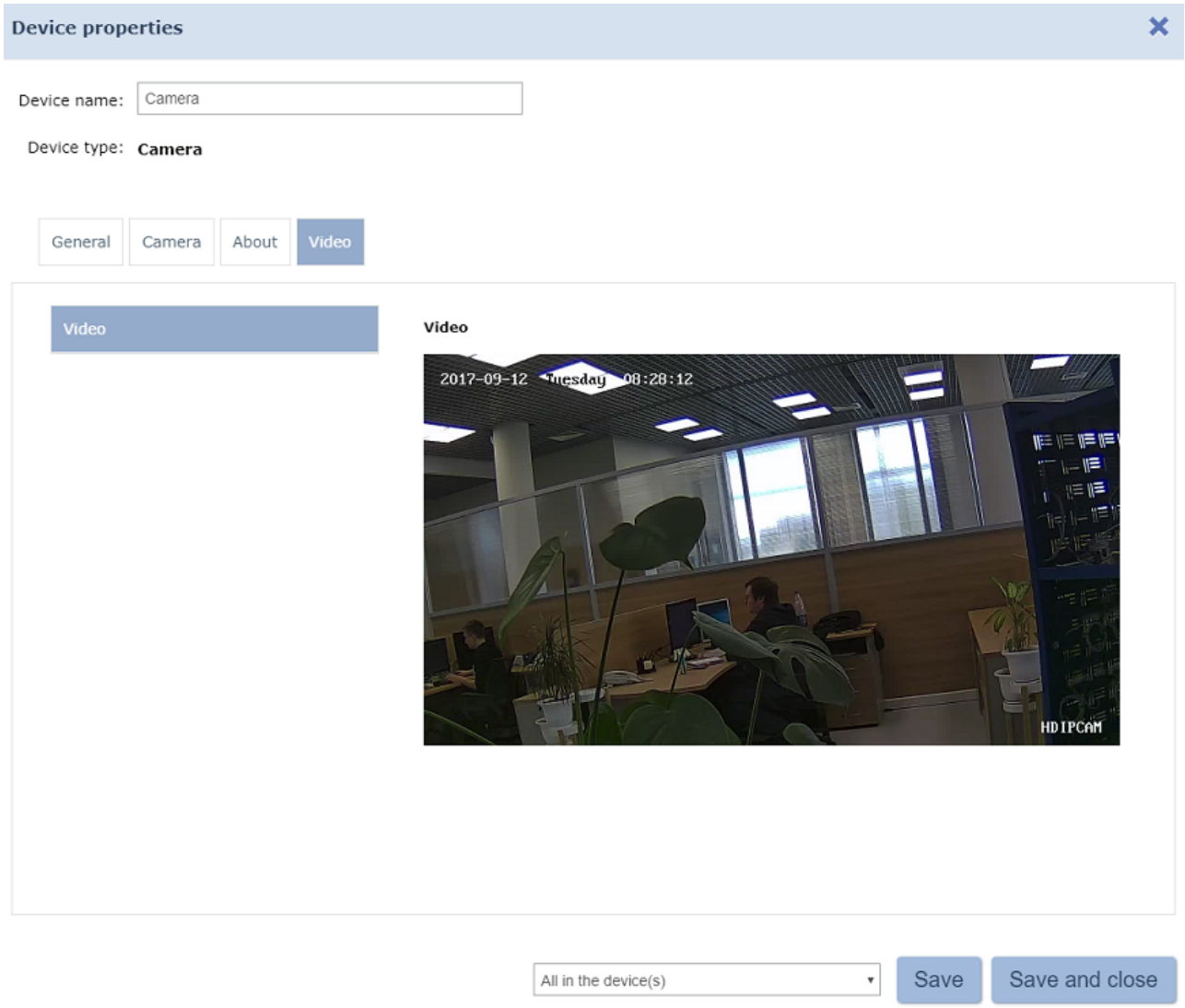
16.2 About camera

About camera:

- **Manufacturer**. Field shows camera manufacturer's name.
- **Model.** Field shows camera model name.
- **Firmware.** Field shows current camera firmware version.
- **Serial number.** Field shows camera serial number.
- **URI.** Field shows URI (Uniform Resource Identifier).

16.3 Video

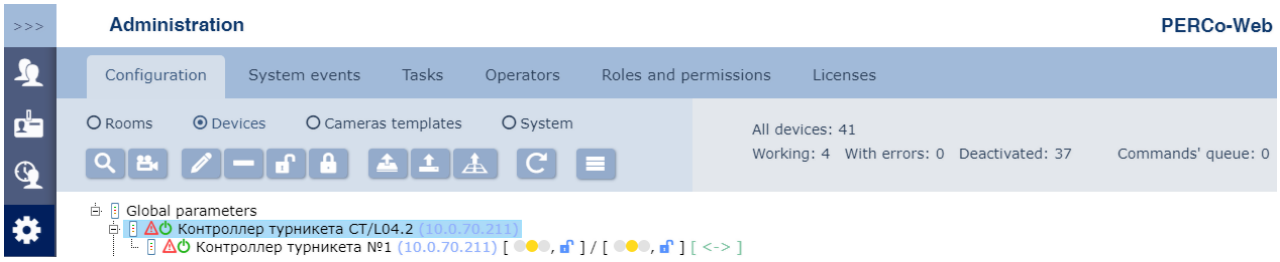
Video tab shows live video from a chosen camera. To open a full-screen mode click on camera image. To exit full-screen mode click on image again. Page overview:



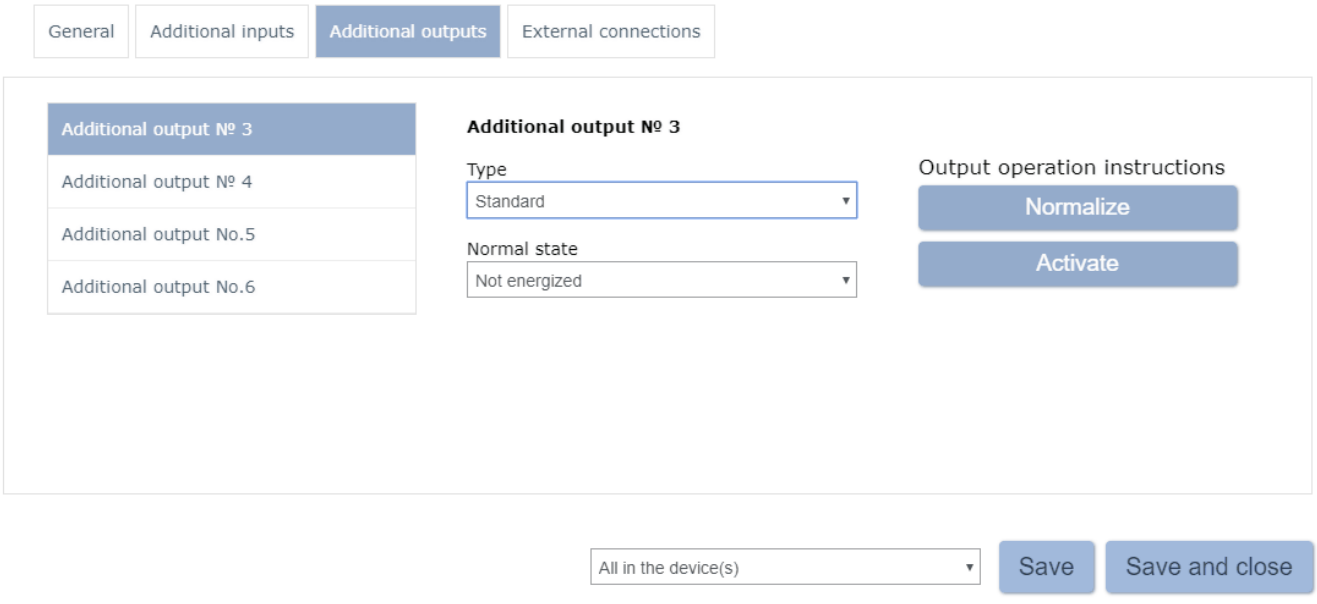
17 Setting up the ACS controller for operation with card capture reader

The system has option of withdrawing all temporary access cards by using the PERCo card capture reader. It is necessary to configure the card capture reader after installation:

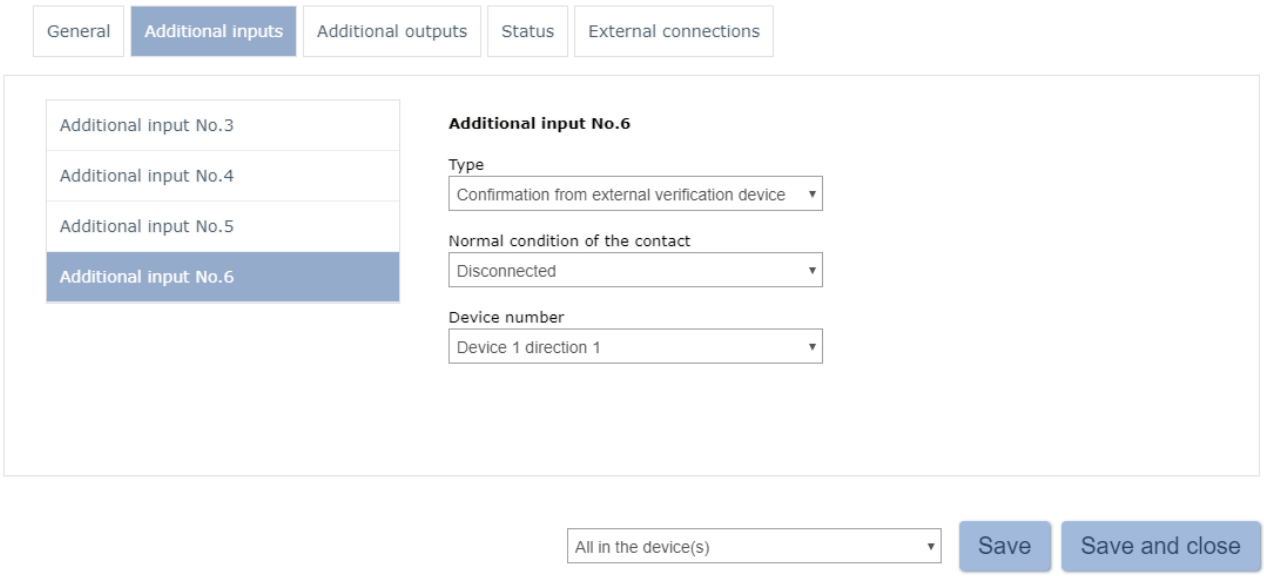
1. Log in the system by using Web-browser (see *PERCo-Web Administator's manual*).
2. Go to **«Administration»** section and open **«Configuration»** subsection.
3. On the page working area select the main controller that is physically connected to the card capture reader:



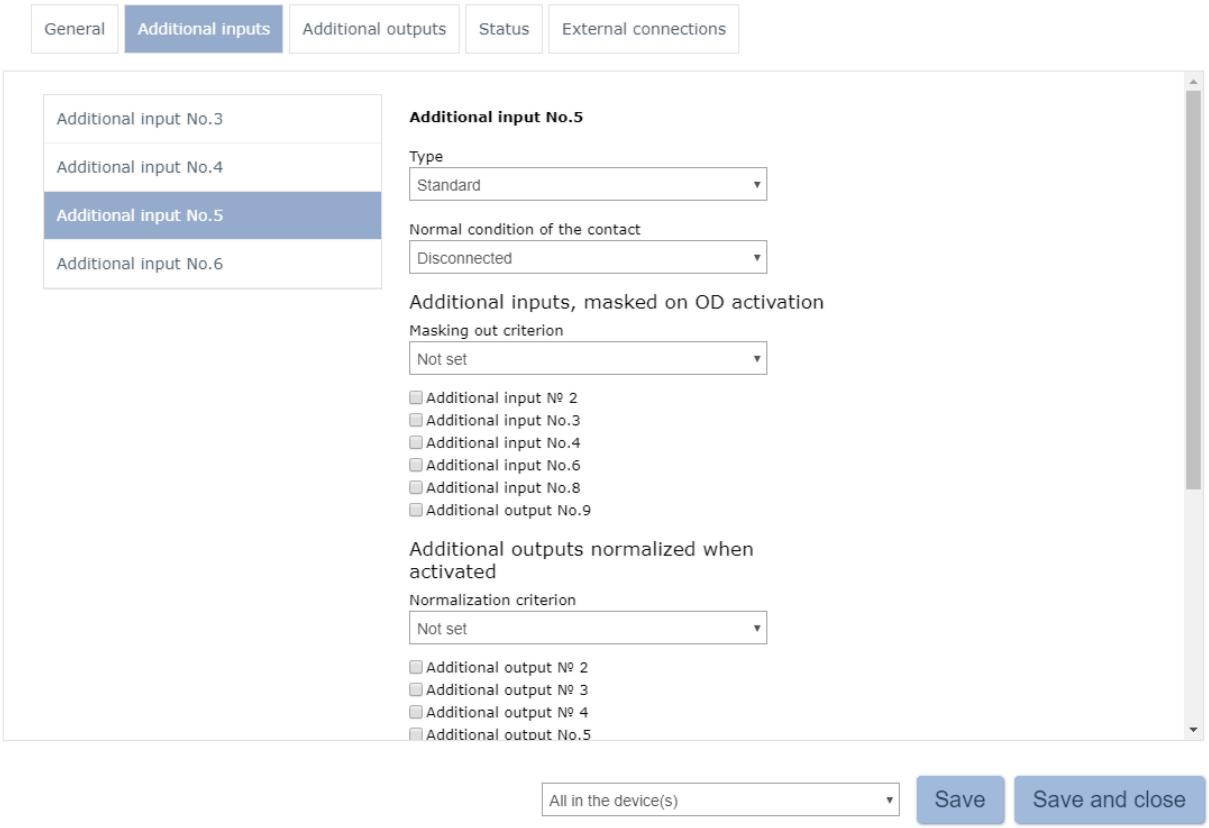
4. Click  **Edit** button on the page toolbar. **Device properties** window will appear.
5. In the appeared window switch to **Additional outputs** tab.
6. On the page working area select **Additional output №...** (the number of the output must correspond to the output of the controller that is physically connected to *«Withdraw card»* input of the card capture reader).
7. Use the drop down list for specifying:
   - **Standard** value for **Type** parameter;
   - **Not energized** value for **Normal state** parameter.



8. Switch to **Additional inputs** tab.
9. If the card capture reader is used as a controller's external verification device (signal *«Card withdrawn»* enters into the separate input of the controller), then select **Additional input №...** (number of the controller's input that is physically connected to the *«Card withdrawn»* output of the card capture reader) from the page working area and configure the following parameters by using the drop down menus:
   - Set **Confirmation from external verification device** value for the **Type** parameter;
   - Set **Disconnected** value for the **Normal condition of the contact** parameter;
   - Set **device... direction...** values (number of the OD and number of the direction must comply with numbers that are controlled by the card capture reader) for **device** parameter:

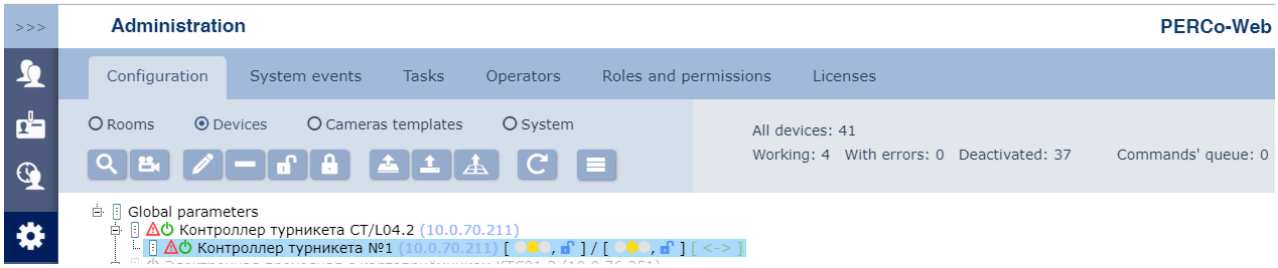


10. Set the type of system's response to the *«Alarm»* signal of the card capture reader. To do this: select **Additional input №...** value (number of the input must comply with the controller's input that is physically connected to the *«Alarm»* output of the card capture reader) and set the following parameters by using the drop down menus from the page working area:
    - Set **Standard** value for the **Type** parameter,
    - Set **Disconnected** value for the **Normal condition of the contact** parameter,



- Set the desired response of the controller by using output's activiation and normalization parameters.

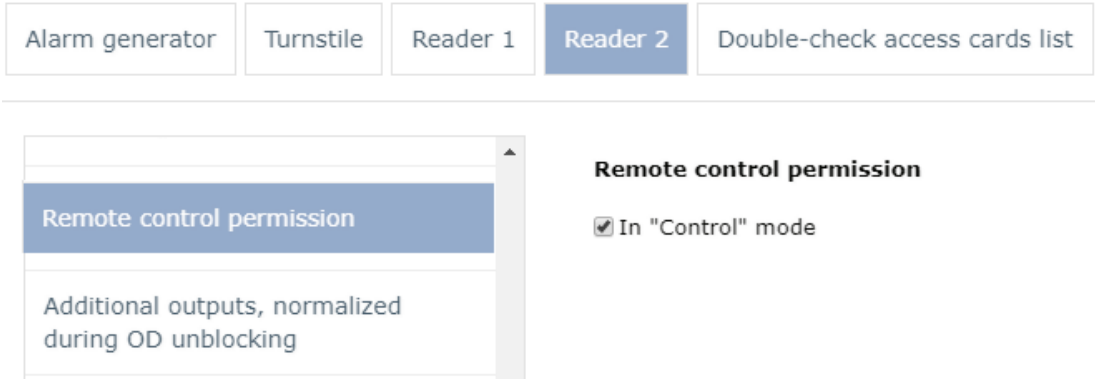
11. Click **Save and close** button. **Device properties window** will close.
12. Select OD controller that is controlled by the card capture reader:



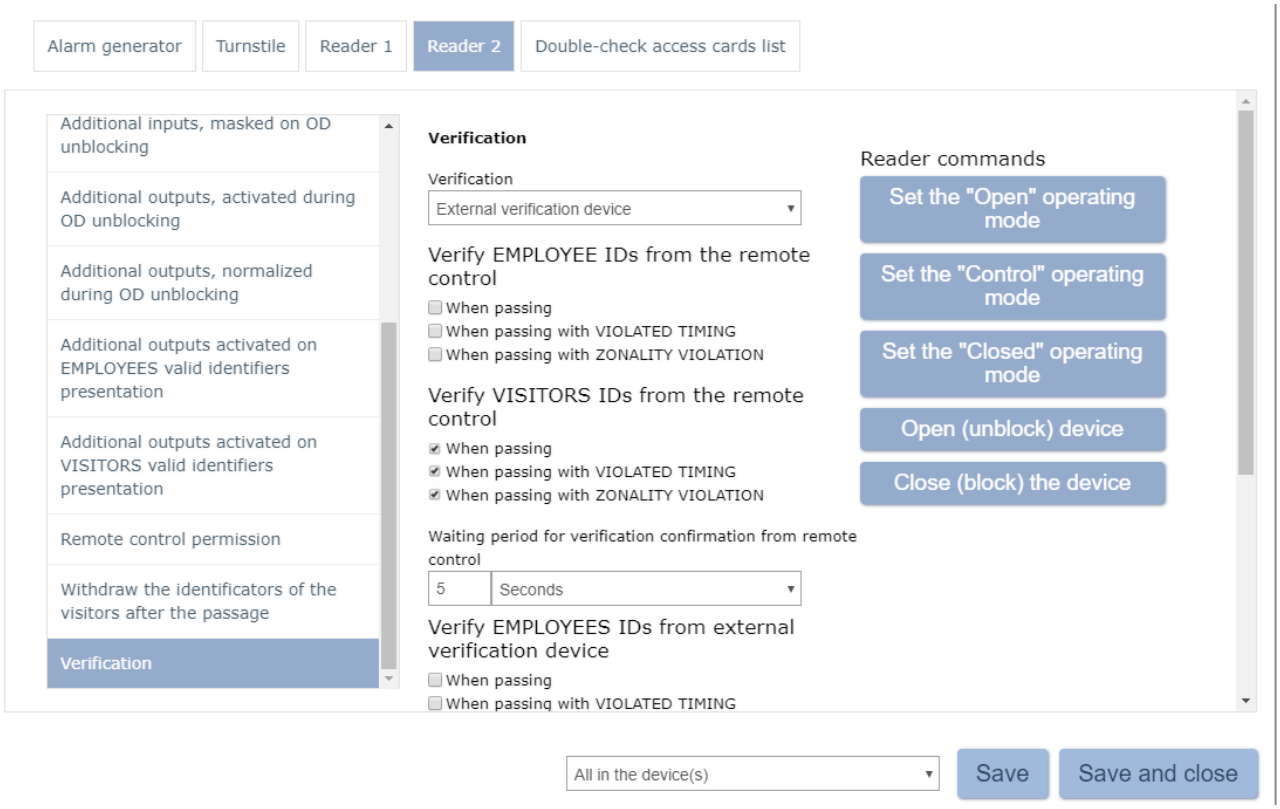
13. Click  **Edit** button located on the page toolbar. **Device properties** window will appear.
14. Switch to Reader №… tab (number of the reader must correspond to the reader that is controlled by the card capture reader).
15. Controller recognizes the *«Card withdrawn»* signal sent by the card capture reader as a confirmation that the card has been withdrawn. Set the following values in the left side of the Verification window in order to configure the confirmation parameters:

- **EVD,** if the card capture reader is used as a controller's external verification device (*«Card withdrawn»* signal enters the separate input of the controller),
- **RC**, if *«Card withdrawn»* output of the card capture reader is connected to the controller in parallel with **RC**. In this case it is also

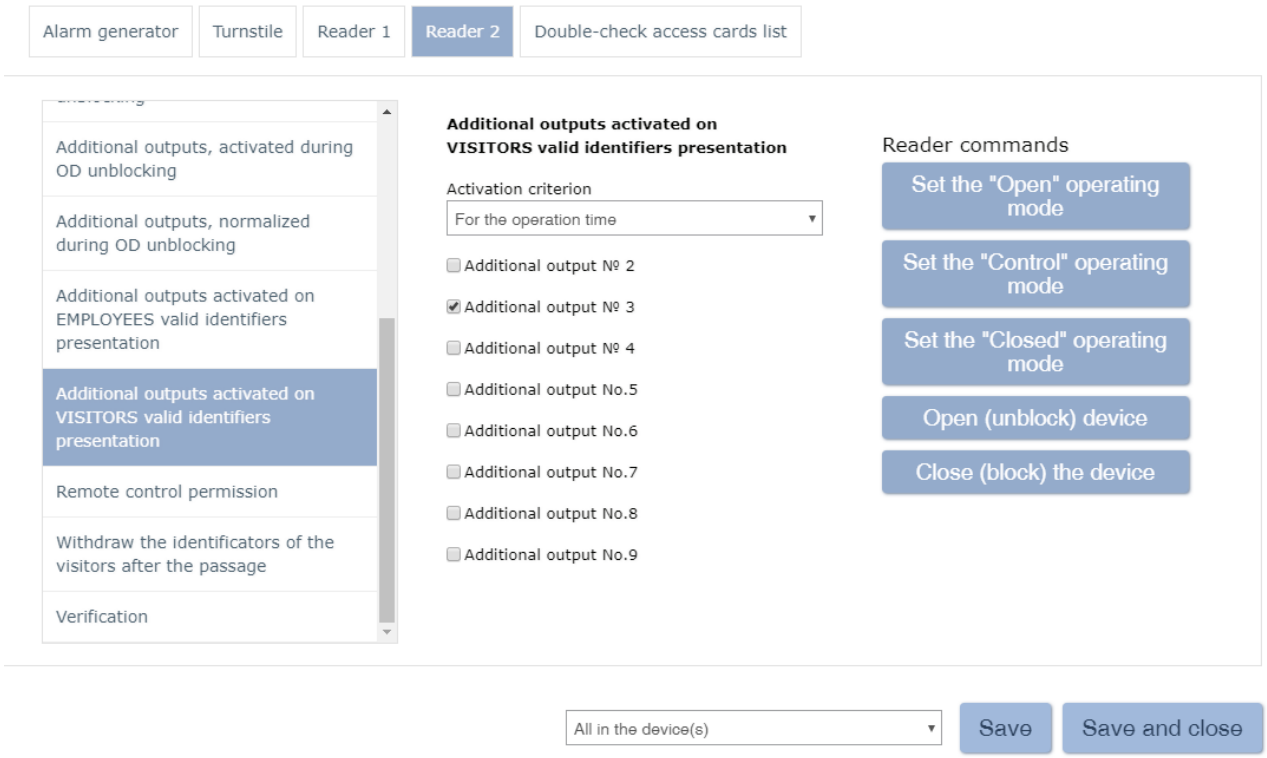
necessary to check **ACM «Control»** box located in the left side of the **RC permissions** window:



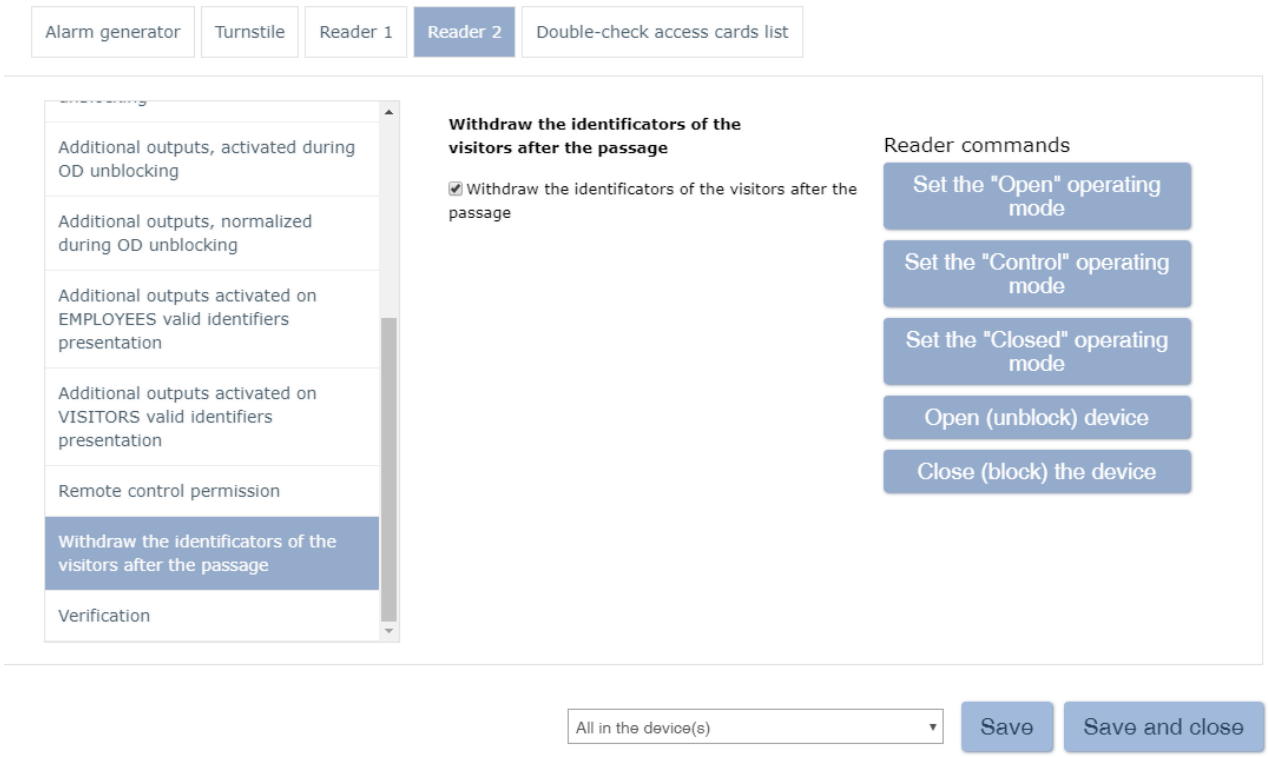
16. Check the following boxes for **Verify Visitor's Identifiers with EVD** (or **with RC** accordingly) parameter:
    - **When passing;**
    - **When passing with VIOLATED TIMING;**
    - **violation with ZONALITY VIOLATION.**
17. Specify the desired value for **Waiting period for verification confirmation from remote control** (or **from EVD**) parameter, which will be used by the controller.



18. Select **Additional outputs activated on VISITORS valid identifiers presentation** parameter from the left side of the window.
19. Set the **For the operation time** value for the **Activation criterion** parameter by using the drop down menu from the page working area.
20. Check the **Additional output №...** box (number of the output, that is connected to the *«Withdraw card»* input of the card capture reader).



21. Select **Withdraw the identificators of the visitors after the passage** parameter and activate it.



22. Click **Save and close button**. **Device properties** window will be closed and are parameters will be saved.

8 Control commands

Alarm generator

Reset alarm – *«Alarm»* mode will be switched off.

Raise the alarm – the controller will be switched to *«Alarm»* mode, all exits that have **Type: Alarm generator** will be activated.

Lock

Set to armed mode – OD will be switched to *«Armed»* ACM.

Set to disarmed mode – OD will be switched from *«Armed»* ACM to the previous ACM.

Reset alarm – *«Alarm»* mode will be switched off. OD will be switched to *«Armed»* ACM.

Block – OD will be blocked.

Unblock – OD will be unblocked.

Reset zonality – resets lock zonality.

Additional output

Activate – all outputs that have **T ype: Normal output**, will be activated. The activation period is defined by **Activization time** parameter.

Important:

Additional outputs that have **T ype: Alarm generator** can not be activated with **Activate** command.

Normalize – all outputs that have **T ype: Normal output** will be normalized.

Reader

Set to « Open» operational mode – OD will be switched to *«Open»* ACM.

Set to «Control» operational mode – OD will be switched in *«Control»* ACM.

Set to «Closed» operational mode – OD will be switched in *«Closed»* ACM.

Open (unblock) OD – OD will be unblocked for the period that is defined by **Unblock time** . This command is available when *«Control»* ACM is used. This parameter unblocks OD for a short period of time.

Close (block) OD – OD will be blocked. This command is available when *«Control»* ACM is used. This command blocks OD after executing **Open (unblock) OD** command.

19 Terms and definitions

Antipass – the security system function which controls the repeated passages (registration) through one ACP in the same direction by using the same identificator.

Global Antipass – the security system function which controls identificator zonality, i.e. – the function controls passage (registration) sequence violations through one ACP and conciders the passage direction. The consequence of passage through one ACP is defined by the mutual position of zones and their nesting (example, it is impossible to enter the premise not entering the building).

Workstation (WKS) – software and hardware package which is used for activity automation. This includes operator working place (remote PC), that has access privileges to sections and subsections of the software.

Data base (DB) – an assortment of data that is organized to be easily accessed by the system. The DB contains: access card numbers, users personal data, cards access permissions, registered events etc. DB is located on the system server. Database management is carried out by «PERCo-Web Manager».

Indicator unit – ensemble of LED or pictographic indicators that inform about OD status and / or applied ACM of the reader direction. The indicator unit can be built in reader, controller, turnstile post, IP-Stile or outside-mounted.

Verification – a procedure of card access confirmation by using the verification device. The confirmation can be done automatically (by the controller, card capture reader) or manually (by using WRC, RC buttons, software commands). Verification is done on the basis of visual comparison of the user appearance and the photo that is stored in the system DB.

Video window – a panel from the section working area that displays video from connected IP-videocameras in real time. The devices are pre-configured and associated with verification points.

Identificator – a device or attribute which is used for user verification. Each identificator has unique code. The system uses EM-Marine, HID and MIFARE cards as identificators.

Operating device (OD) – a device that is used for acces restrictio: turnstile, gate, lock etc.

ID Card – a proximity card (electronic key) that is used for user identification. The card has the same size as a credit card (can have other design: breloques and other). Access card has built-in chip with unique numeric code. It doesn't require internal power supply and this makes service life period almost unlimited. The system uses HID, EM-Marin, MIFARE cards.

Double-checking – a procedure of a card presentation confirmation by presentation of the other, double-checking card.

Controller (system) – a device that is used for operating the access control system or its elements. ACP is organized on the base of the controller.

Firmware upgrade – «Flash tool» program is used for upgrading the firmware and formatting controller memory. The program and firmwares are included in the «S-20 firmware upgrade software package». Recent version can be downloaded from Support> Software section of www.perco.com web-site.

Operator privileges – access permissions to the software subsections which are given to operator by administrator. The access permissions can be given to the following sections: Rooms, Departments, Positions, Work schedules, Access templates, ID cards templates, Controllers, Cameras, Video servers, Verification templates.

Zone – a part of the enterprise territory access to which is available only through ACP by presenting the acces card.

Access control mode (ACM) – mode of operation the system or its elements (controller, reader), for example ACM «Open», «Closed», «Control» etc.

Access control system (ACS) – ensemble of software and hardware which is used for restriction of access for people (transport).

Reader – a device that reads the access card number and sends this number to controller for user identification.

IP-Stile (IP STILE) – a production-line device, ensemble of software and hardware for organizing one bi-directional ACP. IP STILE includes: OD (Turnstile) with build in ACS controller, two readers and the software.

PERCo

Polytechnicheskaya str., 4, block 2
194021, Saint Petersburg
Russia

Tel: +7 812 247 04 64

E-mail: export@perco.com
support@perco.com

www.perco.com

www.perco.com