ACS ASSISTANT v1.7.1

User Manual

Content

"Guard plus" software runs on a base of a server platform. Program launches on a server computer. An internet browser is used (browser acts as client) for working with the program. To get access to the program, input a server address in format: **server_address:port**, in address line of browser, where

- port – port, on which program works. It can be changed in config.json. configuration file. Default port value: 5870.
- server_address – localhost, server ip-address or domain name.
  - localhost – used in case a browser launches on a local computer (server computer);
  - server ip-adress – used in case a browser and the server run on different computers. For example, 192.168.1.125;
  - domain name – used in case there is a domain name for ip-address, on which server runs.

1 User control panel

User control panel includesthe following(*Fig.1*):

1. Fire mode activation/deactivation button;
2. Change interface language button (English, Russian,…);
3. Information area about the current user in the system.

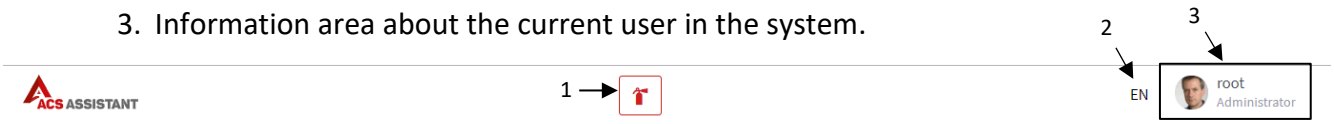


Fig.1User control panel

2 Fire mode

In case of fire you need to activate the fire mode by pressing the button to open all the doors. States of the button are:

- – fire mode is not active;
- – fire mode is active.

In fire mode all the doors are in the "open" position.

3 Main menu

Main menu is a navigation bar with the following sections (*Fig.2*):

- Monitoring
- Device management
- Management
- Settings
- Export/Import

- System log
- Documentation

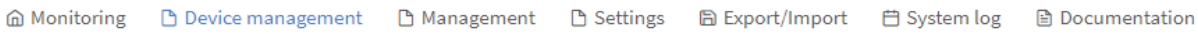


Fig.2Main menu

3.1 Monitoring

"Monitoring" section includes "System monitoring", "Photo verification" and "Events log".

3.1.1 System monitoring

The monitoring page displays the current system parameters in numerical form, as well as charts. Frequency of monitoring data updating is determined by the user. *(1 atFig.3)*.

Monitoring parameters**:**

- the percentage of CPU usage by the program;
- amount of memory used by the program in megabytes;
- average load in one minute;
- response time in milliseconds;
- number of requests per second;
- status codes that were received in the report on the request for the specified period (1 in *Fig.3*).

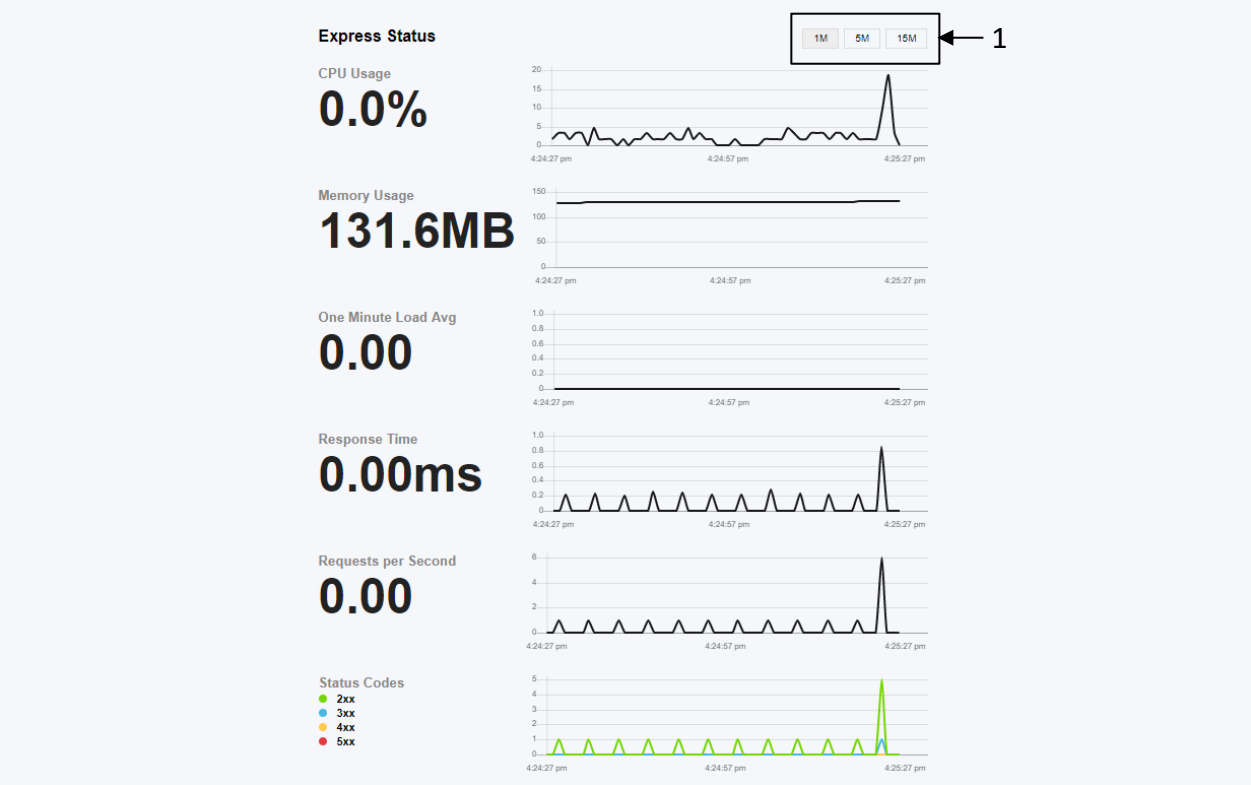


Fig.3 Page "Monitoring"

3.1.2 Photo Verification

The photo verification page is a log of events that shows all movements of persons/guests through pass points with detailed information about them.

Events from controllers that work via RS-485 can be displayed with a delay (2-6 seconds). Events from controllers that are connected to the IP series converter are displayed on the photo verification page in 1-3 seconds. In case where the speed of events on the photo verification page is important, it is recommended to use IP series converters.

"Photo verification" page structure *(Fig.4):*

1 - the form on the left displays the last event that goes to the event log as soon as it is updated to the next last event *(Fig.4,Fig.5)*;

2 - the event log displays all events that correspond to the applied filters, in order from the last event to the first. The photo verification event log is presented in the form of a table with fields:

- **PHOTO** (of the person who performs this event)
- **FULL NAME** – displays, if the short name of a person is not given; if a short name is given, then a short name displays;
- **WORKING AREA** – the location where an event occurred;
- **PASS KEY** (number locked at the event)
- **TIME** – the time of the recorded event;
- **DIRECTION** – entrance or exit with a description of the event;

3 – button that opens "Filter" window;

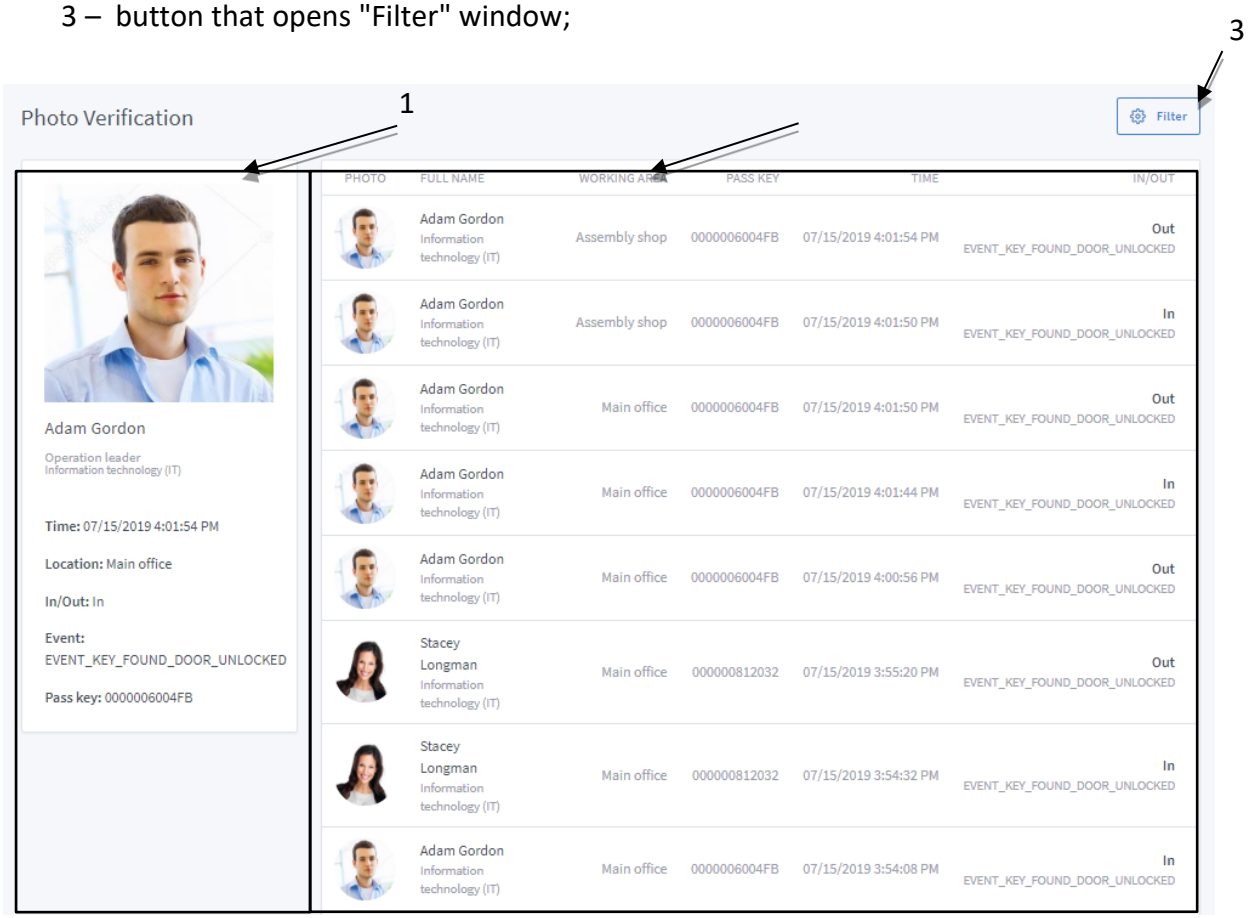


Fig.4 Page "Photo Verification"

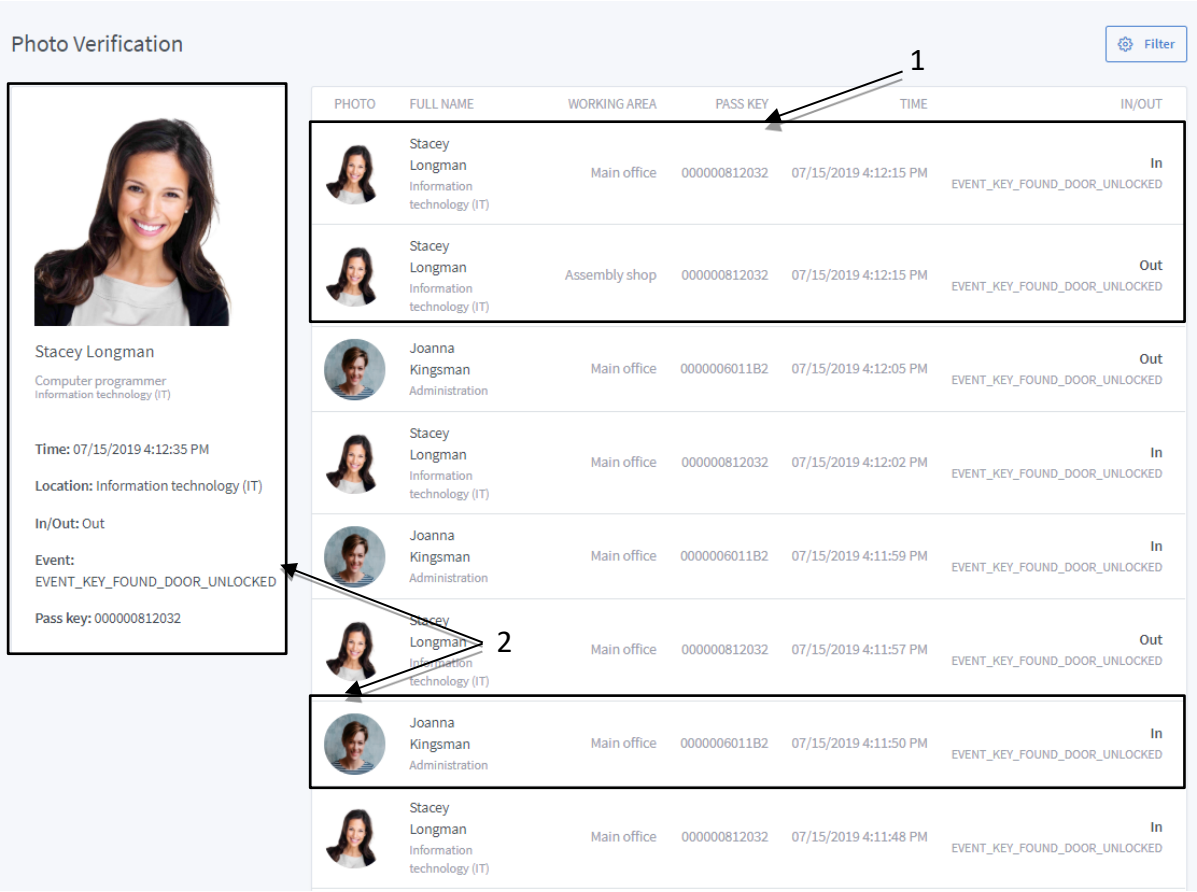


Fig.5 Page "Photo Verification", updating the latest event

Depending on a pass point *(see section 3.3.2 "Set pass points")* two events “in/out” appear in the log *(see 1 -Fig.5).*

The concept of **zero pass point** is introduced to specify the main entrance to the territory (exit from the territory)*(see section 3.3.2 "Set pass points").*

Entrance/exit, recorded at a zero pass point, is shown as one event *(2 at Fig.5).*

Photo verification event filter

“Filter” functionality allows to sort events by certain parameters. To open a window, press the “Filter” button*(3 at Fig.4).*

Structure of the “Filter” window*(Fig.6)*:

There are drop-down lists to choose the following parameters:

1 – person (persons) *(Fig. 7)*;

2 – working area(s) *(Fig. 9)*;

3– organizational units*(Fig. 8)*;

4– pass point(s)*(Fig.10)*;

5– direction (requires to select an option);

6 – “reset all settings” button;

7 – “close window” button with auto save.

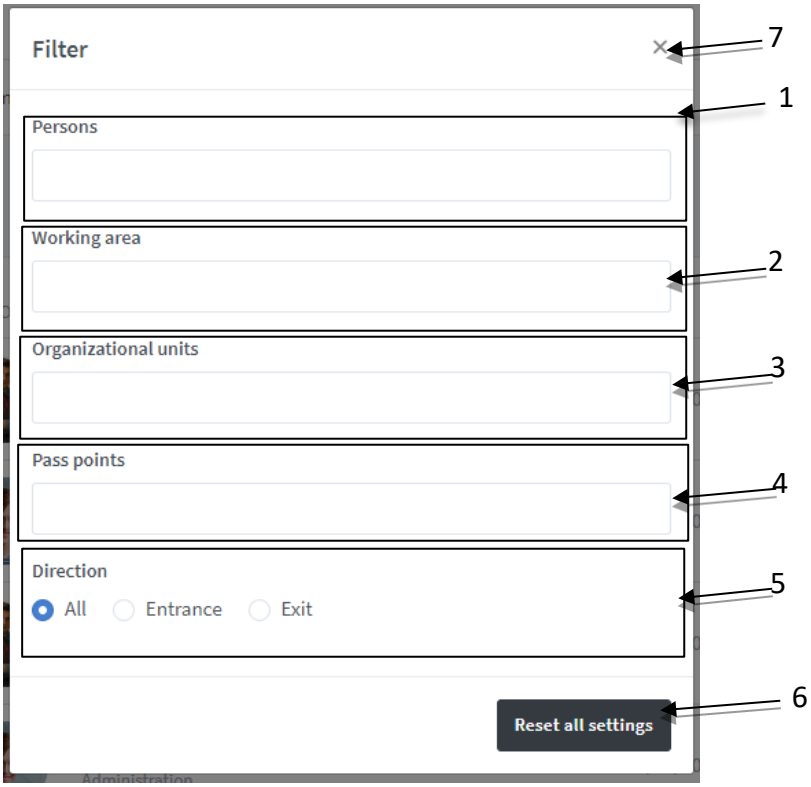


Fig.6 "Filter" window

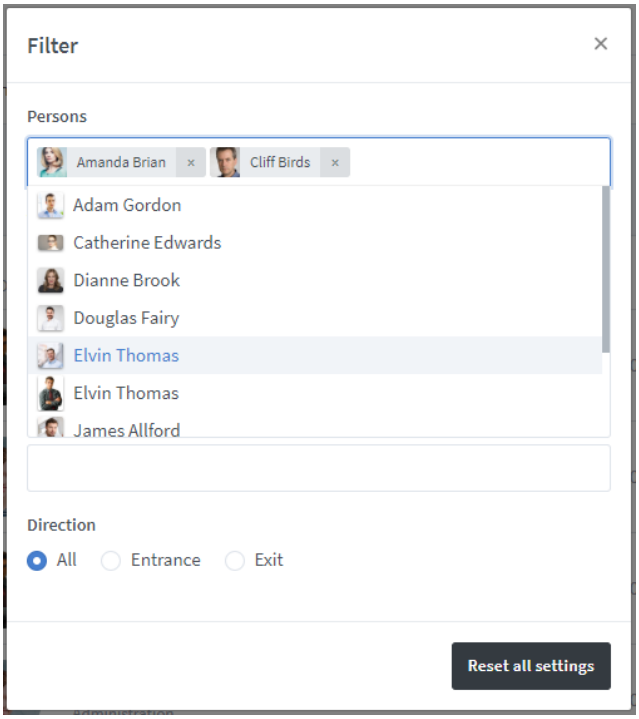


Fig. 7 Select person(s)

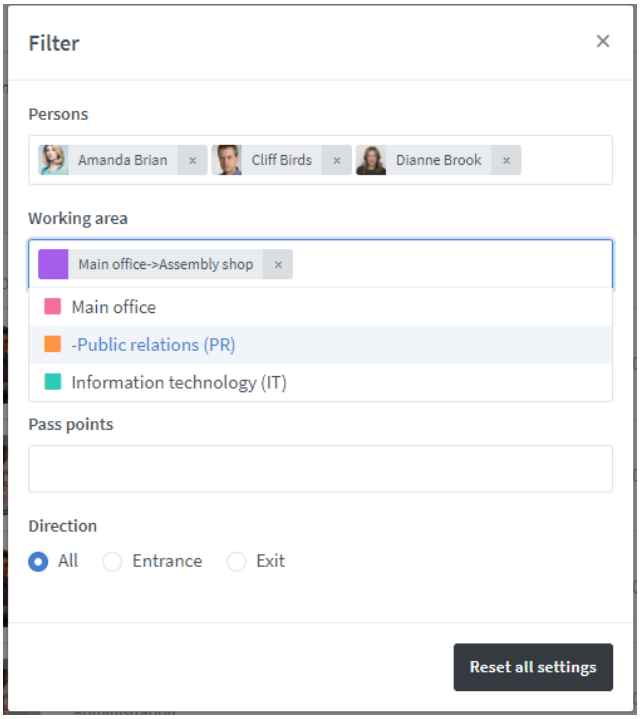


Fig. 8 Select organizational unit

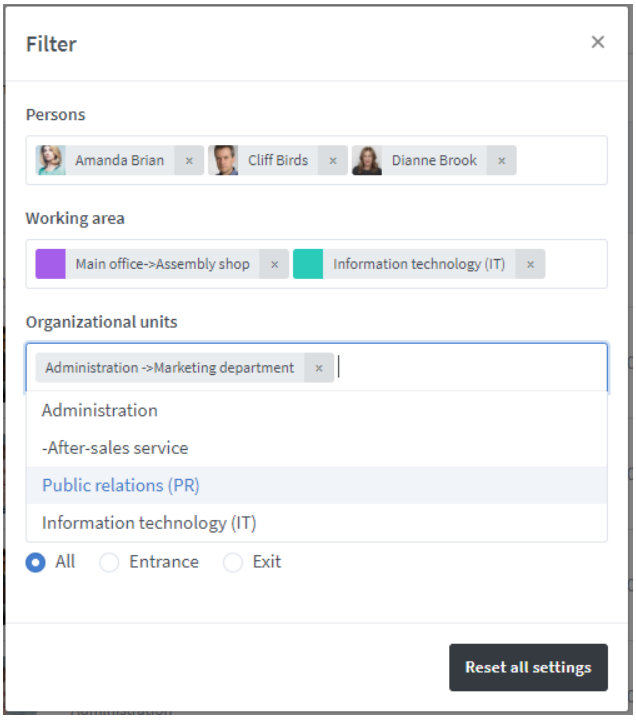


Fig. 9 Select working area

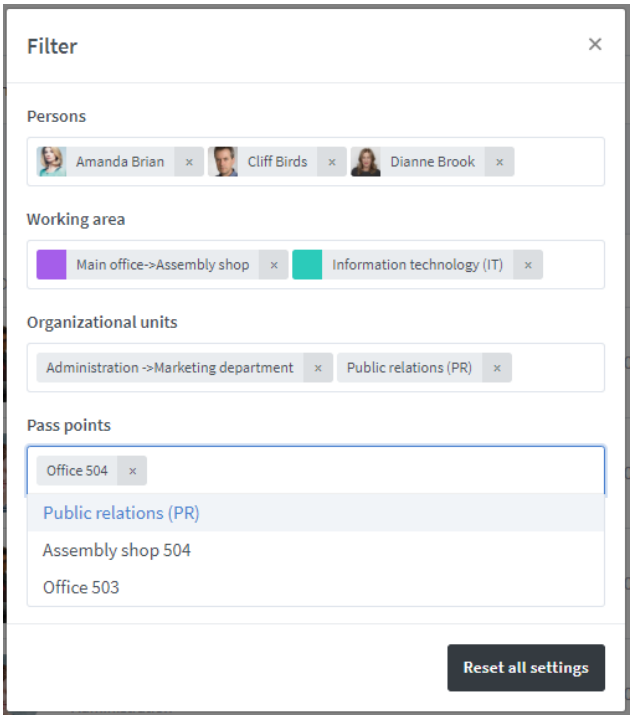


Fig.10 Select pass point

After selecting all the necessary parameters close the window by clicking a cross in the upper right corner. *(see. 7 at Fig.6)*, the parameters entered will be automatically saved and the event log will be updated with the relevant sorting.

To reset all filter settings, click the button **Reset all settings**.

3.1.3 Events log

The subsection is a log which shows all Events log with detailed information about them.

"Events log" page structure *(Fig.12*, *Fig.12)*:

Filter:

1 - button to minimize/expand the event log;
2 - button on / off events display in the journal in real-time;
3 - start time of the event display period (this field is hidden if real-time monitoring is enabled);
4 - end time of the event display period (this field is hidden if real-time monitoring is enabled);
5 - events filter by persons;
6 - event filter by event type;
7 - save filter settings;

The selected filter settings are applied to the event log after clicking the "Save Settings" button.

8 - filter reset button to default values;

Event Log Filter Defaults:
- real-time monitoring enabled;
- display of all employees;
- display of events of any type.

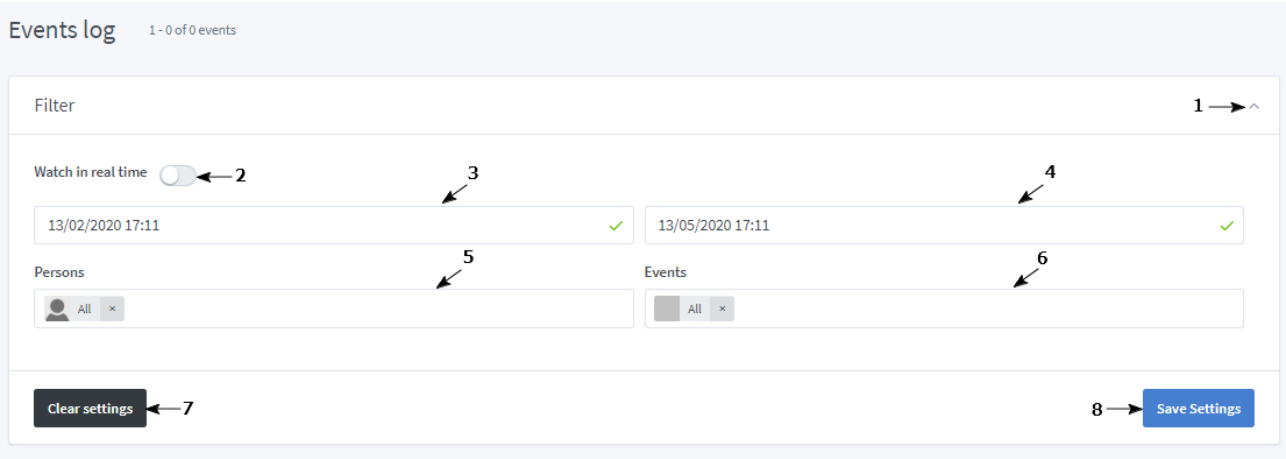


Fig.11 Events log filter

Event log:

9 - "Reset log events" button;

10 - the number of Events log displayed on one page in the log (can be changed);

11 - the list of events is presented in a log with the following fields:

- **TIME** – date and time of an event;
- **CONTROLLER –** controller that recorded an event;
- **DIRECTION** – shows if a person is inside or outside, also indicates a working area in which an event occurred (if pass points are not set);
- **PASS POINT** – indicates a pass point and corresponds to its name (if set) *(Fig.13)*;
- **TO AREA/ FROM AREA** – show between which areas a person moved depending on the pass points settings *(Fig.13)*;
- **PASS KEY** – identification number recorded by a controller;

For the event "Successful entrance":
- when opened with RS-485 command, the identifier with the number 00001E is indicated (the Dallas card number format is indicated as an example).
- when opened with the button identifies the identifier with the number FFFFFF (the Dallas card number format is indicated as an example).

- **ORGANIZATIONAL UNIT**– person's organizational unit with an assigned pass key;
- **PERSON** – person with an assigned pass key;
- **EVENT** – information about an event;

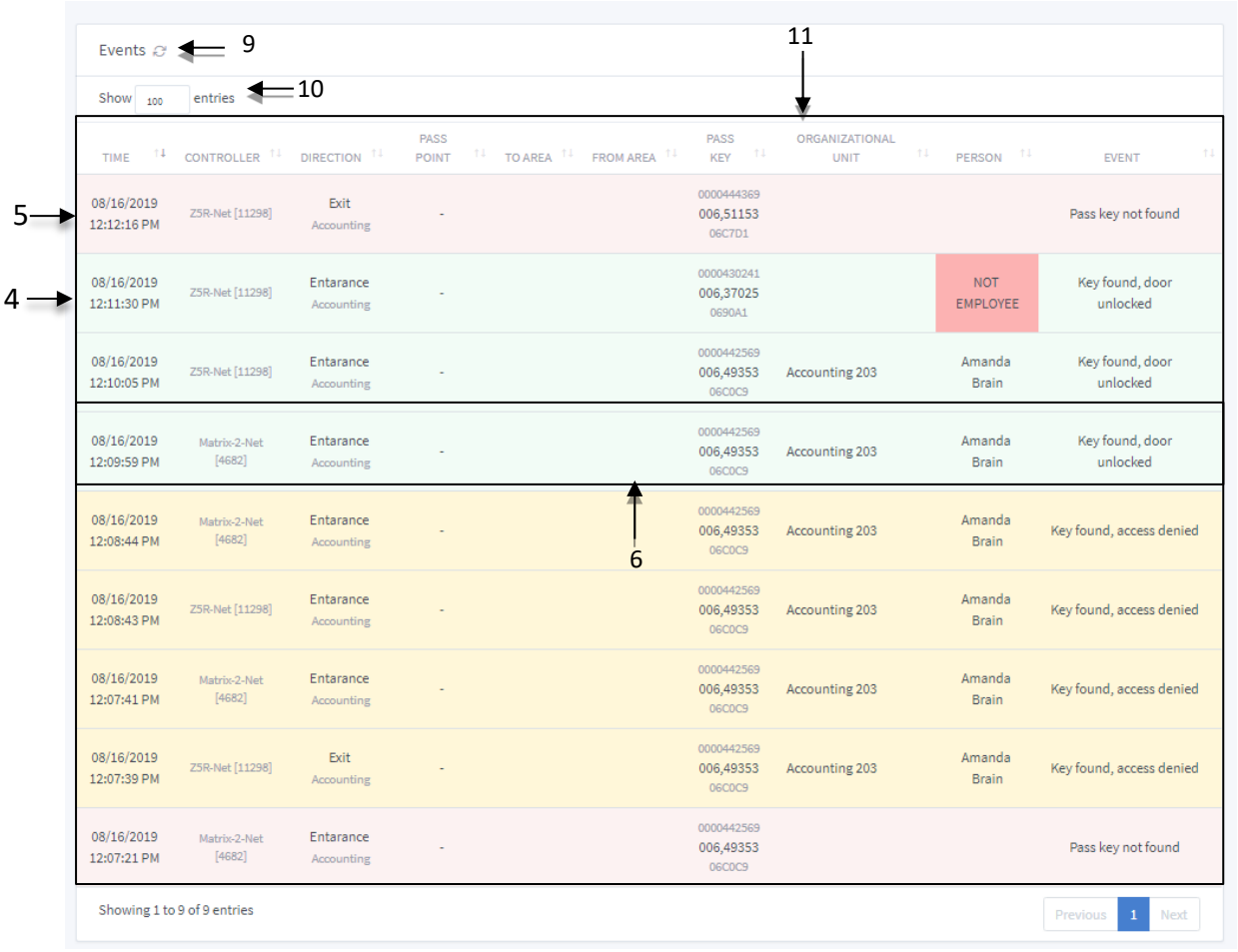
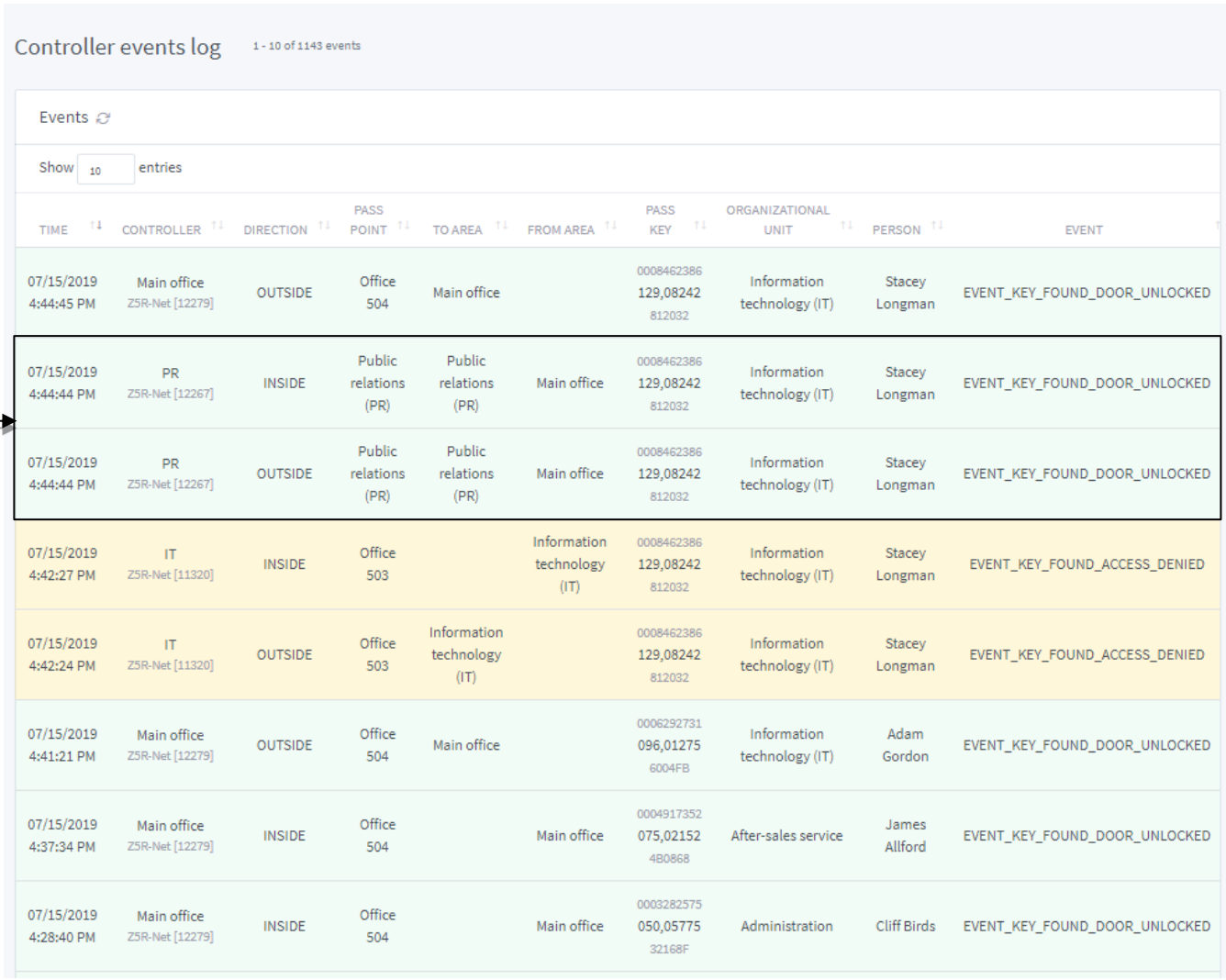


Fig.12 Page "Events log": «Pass points» are not set»

If event log row is highlighted in green - access was allowed, in yellow - access was denied, in red - identifier is not found in the controller's memory *(5 atFig.12)*.

Also, if passage happens using a pass key that is not in the system, but is in the controller's memory, event in log will be displayed with a note ***Pass key without user****(4 at Fig.12).*

- If "Pass points" are not set *(see section3.3.2Set pass points)* the log shows entry/exit as one event *(6 at Fig.12)* with working area in the column "Direction", where an event was recorded.
- If "Pass points" are set two events are shown: entry and exit,displaying between which areas it happened in columns "From area"/"To area" (1 at *Fig.13*).



1

Fig.13 Page "Events log": "Pass points" are set

3.2 Device management

In this section a user can see all devices connected to the system; add devices to the system to manage and configure.

The “Device Management” page contains two tabs: converters (*Fig.14*) and controllers (*Fig.27*). The corresponding buttons are responsible for switching between the tabs *(1, 2 at Fig.14)*.

3.2.1 Converter and “Guard Plus” software operating modes

A converter can operate in three modes: *server*, *client* and *proxy.*

- **Proxy mode**

In proxy mode, the connection between Guard Plus and the converter is established through the proxy server (the converter and Guard Plus act as clients). The connection is made using the authentication key (AUTH_KEY), which must be entered the first time the converter is connected. This method is used for connection when the converter and the program work on different networks and it is impossible to establish a direct TCP connection.

The authentication key (AUTH_KEY) added to the system is cached and constantly used for searching.

If the converter is added to the system, after restarting the program, it is not required to enter the authentication key (AUTH_KEY) again.

If the converter is configured to zproxy.con.ru, but it is on the same subnet as Guard Plus, then, before entering the authentication key (AUTH_KEY), this converter will be displayed on the interface with the TCP connection type.

- **Server mode**

The converter waits passively for a connection from the Guard Plus (Guard Plus acts as a client). A request is broadcast to discover the converter and Guard Plus connects to it. This method is used in the networks where broadcast UDP requests from the program can reach the converter, and its response reaches the program.

- **Client mode**

The converter is actively trying to connect to Guard Plus, acting as a client, and Guard Plus as a server. By default, TCP port 25000 is used for a connection. This mode allows you to work on networks where the distribution of broadcast packets is impossible or prohibited, but it is possible to connect directly to the program from the converter’s location.

In any mode, the connection for the information exchange is established through the TCP protocol.

After changing the operating mode of the converter, the program automatically changes the type of connection and updates the data on the converter.

An exception is the change of the converter operation mode to a proxy: if, until the mode was changed, the authentication key had not been entered into the program, then the connection will not be restored automatically until the authentication key is entered.

Detailed instructions for configuring the converter are provided in the user manual for the corresponding converter model.

3.2.2 Device management: Converters

The page is to manage and configure converters. Also from this page, there is an access to the appropriate controllers through converters.

"Controllers list" page structure*(Fig.14)*:

1 - open converters list button;
2 - open controllers list button;
3 - converters list updating button;
4 - the number of entries displayed on one page (can be changed);
5 - "Add converter" button;
6 - search field;
7 - converters list is presented in the form of a table with fields:

- **#** – sequence number of the converter in the list;
- **NAME**– name of the converter and the number of controllers connected to the device;
- **SERIAL**– device serial number, this field also displays converter firmware version;
- **LINE**–line number and address, this field also displays license information;

Changing the IP address of a converter added to the system that operates in CLIENT mode is done automatically by the system.

Changing the IP address of a converter added to the system that works in SERVER mode is done manually by the user using the window for changing converter settings.

- **MODE**– displays the mode of the converter:
  - **NORMAL** – automatic speed detection and transmission direction;
  - **TEST** – checking and configuration the network of controllers;
  - **ACCEPT** – start the network without installing software on a computer;
  - **ADVANCED** – operation of the converter under control of special software;

  The device connection type is also displayed.:

  - **CONNECTION: TCP** – work with a converter, which is configured for SERVER mode;
  - **CONNECTION: SERVER** – work with a converter, which is configured for CLIENT mode;
  - **CONNECTION: PROXY** – work with a converter through a proxy server.

- **STATE** – displays the address of the client that is connected to the converter, as well as the status of the converter:
  - **CONNECTED** – converter is connected;
  - **DISACTIVE** – converter is off and not being used;
  - **FORBIDDEN** – converter is busy with another client;
  - **DISCONNECTED** – no connection to the converter;
  - **CONNECTING** – connecting to the converter;
  - **BUSY** – converter is not responding;
  - **WAITING FOR CONNECTION -** waiting for a connection from a converter (Guard Plus in SERVER mode).
- **ON/OFF**– enable/disable converter;
- **OPTIONS:**

– view controllers list;

– attach license file;

– change converter info;

– delete converter.

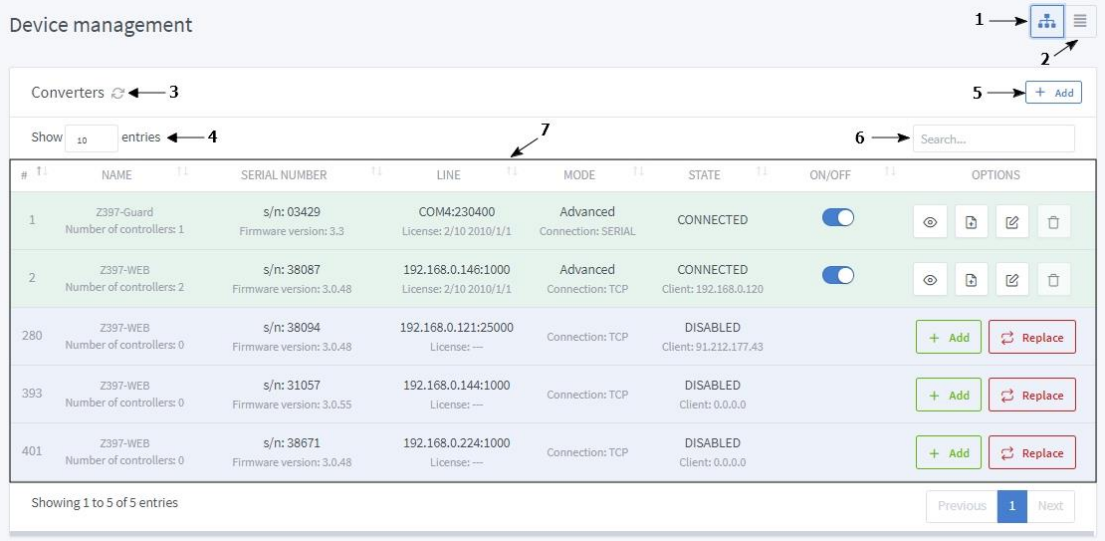


Fig.14 Page "Device management: Converters"

Add converter to the system

In ACS ASSISTANT, there are two ways to add a converter to the system - manual and automatic.

IP series converters can be added in two ways, and converters that work using RS 485 are added to the system only in an automatic way.

To add converter manually you need to do the following:

1. Click the “Add” button at “Device management” page *(1 at Fig.14)*, as a result, “Converter adding” window will open *(Fig.15*).
2. Fill the fields in “Converter adding” window:

- **Name**— converter name (optional);
- **Address** — converter IP-address;
- **Port** — port number in range from 0 to 65535;
- **Connection type** — predefined (by default TCP/IP);
- **Description** — short description of the converter (optional);
- **Do not close the modal window** — if this checkbox is unchecked “Converter adding” window remains open after adding a device.

3. Click *button* Add *(1 at Fig.15).*

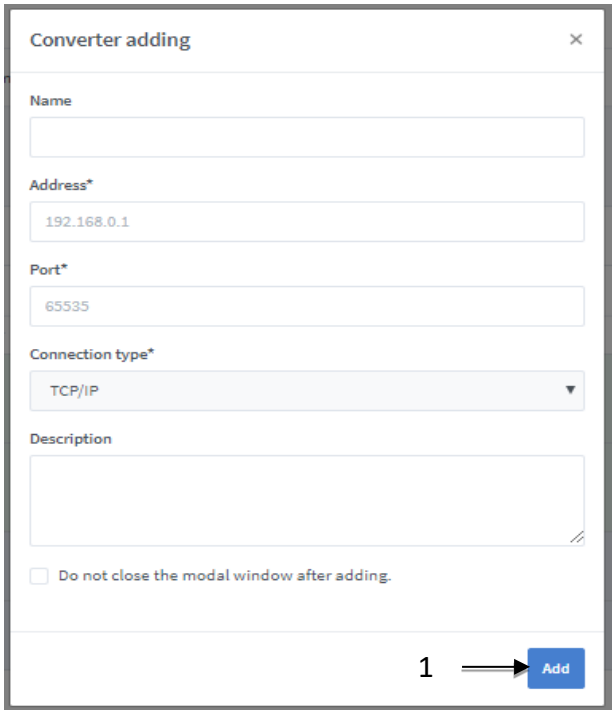


Fig.15 Converter adding window

Add the authentication key (AUTH_KEY) to the system:

1. Click the “Add” button at “Device management” page (1 at*Fig.14*), as a result, the “Add Converter” window will open (*Fig.15*).
2. Select “PROXY” from the drop-down list in the “Connection Type” field (*Fig.15*).
3. In the window that opens, enter the authentication key (*Fig.16*) and click the "Add" button.

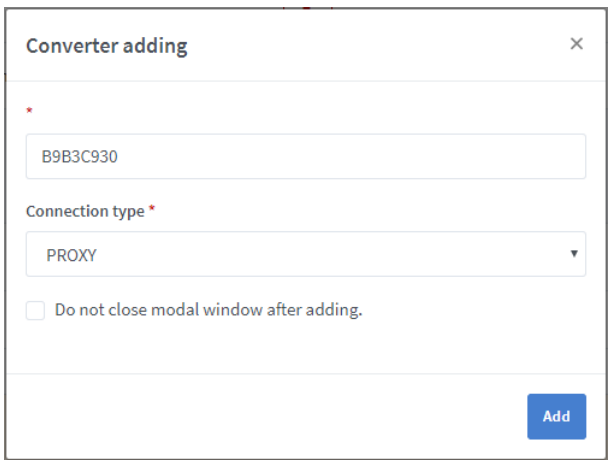


***Fig.16* Entering the key to access the converter**

4. If the converter is found on the proxy server, then it will be displayed in the list of devices. After that, you need to add the converter to the system (see the paragraph “Add the converter automatically” below).

If a converter is added to the system in PROXY mode, the LINE column displays the domain address of the proxy server and its port (*Fig.18*), which corresponds to the proxy server settings (see the System Settings section).

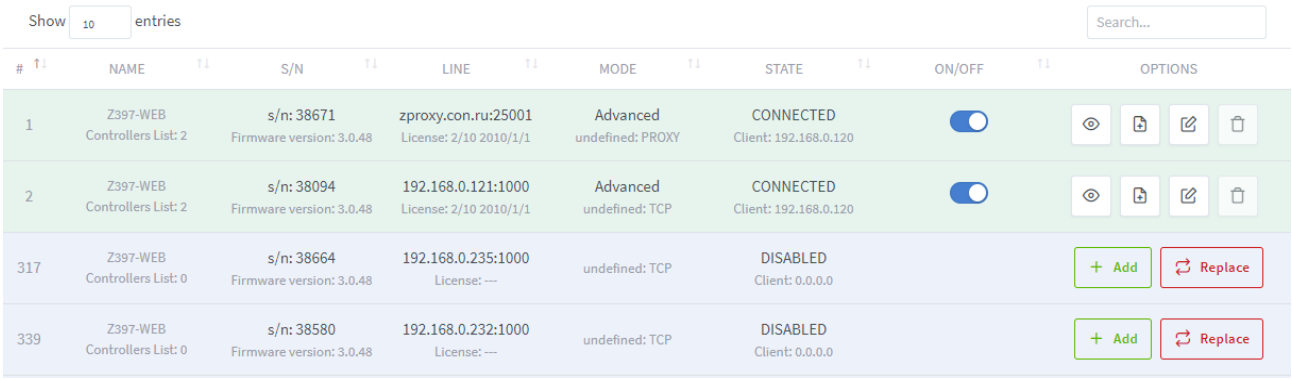


Fig. 16 Displaying a converter added to the system in PROXY mode

To add converter automatically do as follows:

1. Find the required converter in the list.
2. Click “Add” button*(1 at Fig.16).*
3. Wait for the connection with the converter *(Fig.18).*

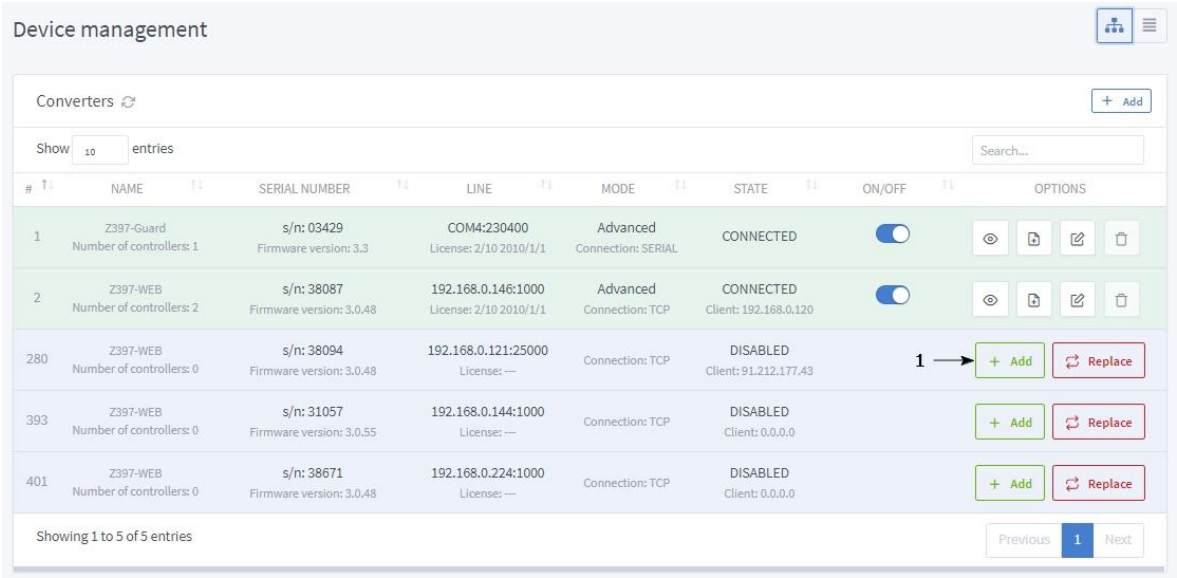


Fig.17 Automatic converter adding to the system

Wrong serial number displays for converters that connect using RS 485 and are not added to the system. Correct serial number displays after adding.

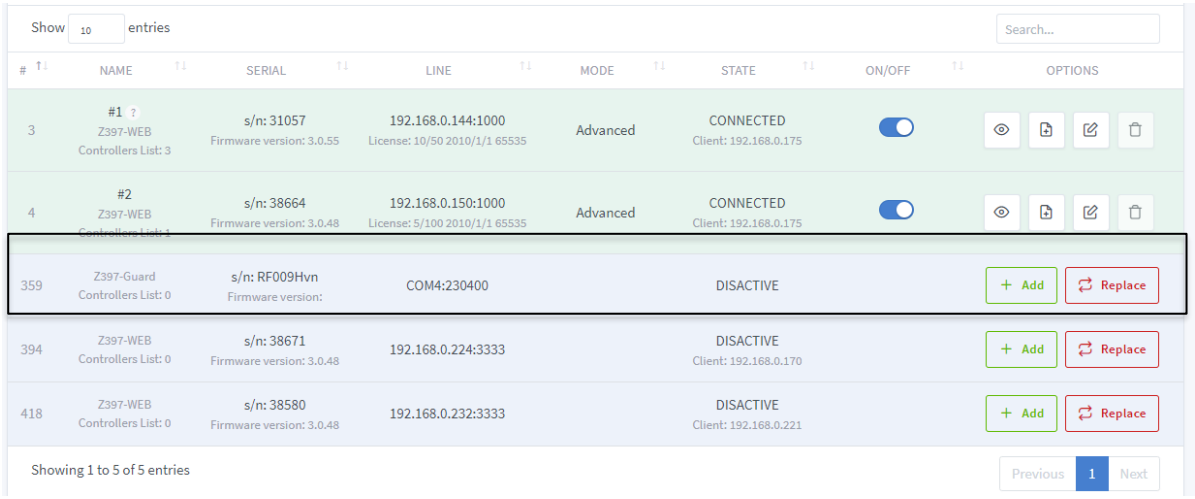


Fig.18 Converter is connected

Change converter info:

To change converter info do as follows:

1. Click button at "Device management" page, as the result "Edit converter" window will open*(Fig.19).*
2. Edit corresponding fields.
3. Click button Edit *(1 at Fig.19).*

If converter is connected you can edit only name and description. If there is a necessity to edit address and port (IP converters only) you need to disconnect converter and then edit it, after that connect it again.

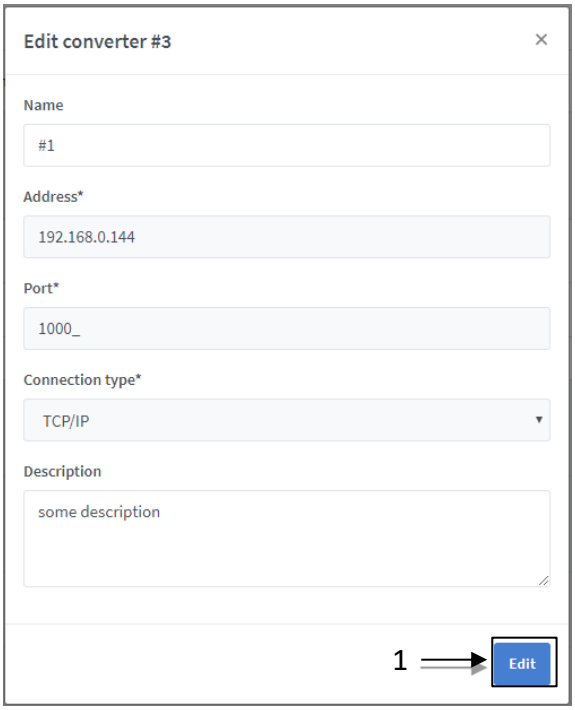


Fig.19 "Edit converter" window

Replace converter

To replace converter, you need to do as follows:

1. Select a converter (from those that are not added to the system) which should replace another one.
2. Click “Replace” button.
3. In this window*(Fig.20)*,find a converter that needs to be changed and click “Select” button*(1 at Fig.20).*
4. Wait for the converter to be replaced.

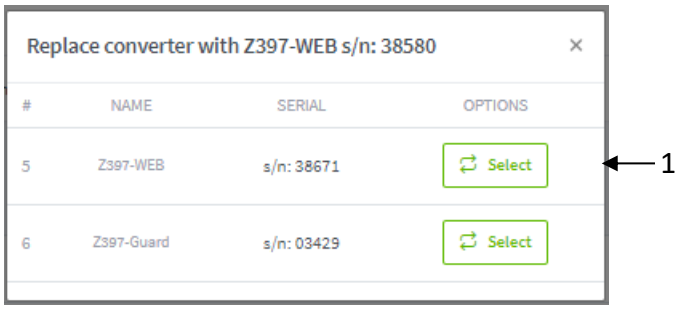


Fig.20 Converter selection window to be replaced

Delete converter

Converter can be deleted after it is disconnected.

To delete a converter do as follows:

1. Click button near a converter that needs to be deleted in “Options” column at “Device management” page.
2. As a result, the confirmation window will appear *(see Fig.21)*.

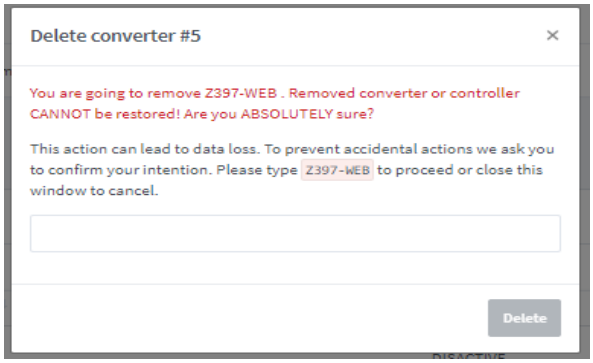


Fig.21 Confirmation window of deleting converter

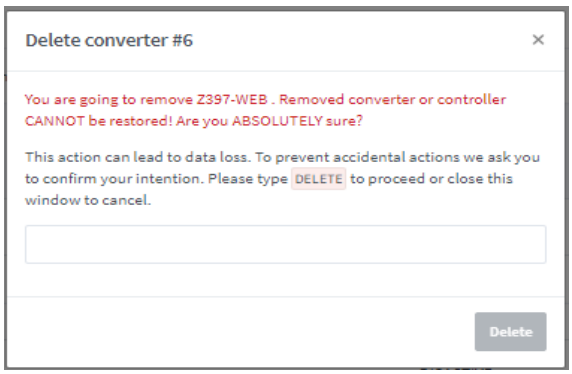


Fig.22 Confirmation window of deleting converter that does not exist

3. After following all the instructions and confirming intentions to delete converter, button “Delete” will be active*(Fig.21*). If the converter is with incorrect settings or it does not exist at all (error when adding), then the window will match *(Fig.22)*.

To prevent accidental actions, “Delete” button is blocked until the user confirms their intentions.

4. Click button Delete .

View controllers list

This option is used to view the list of controllers connected to the selected converter. Clicking button will open controllers list page*(seeFig.23).*

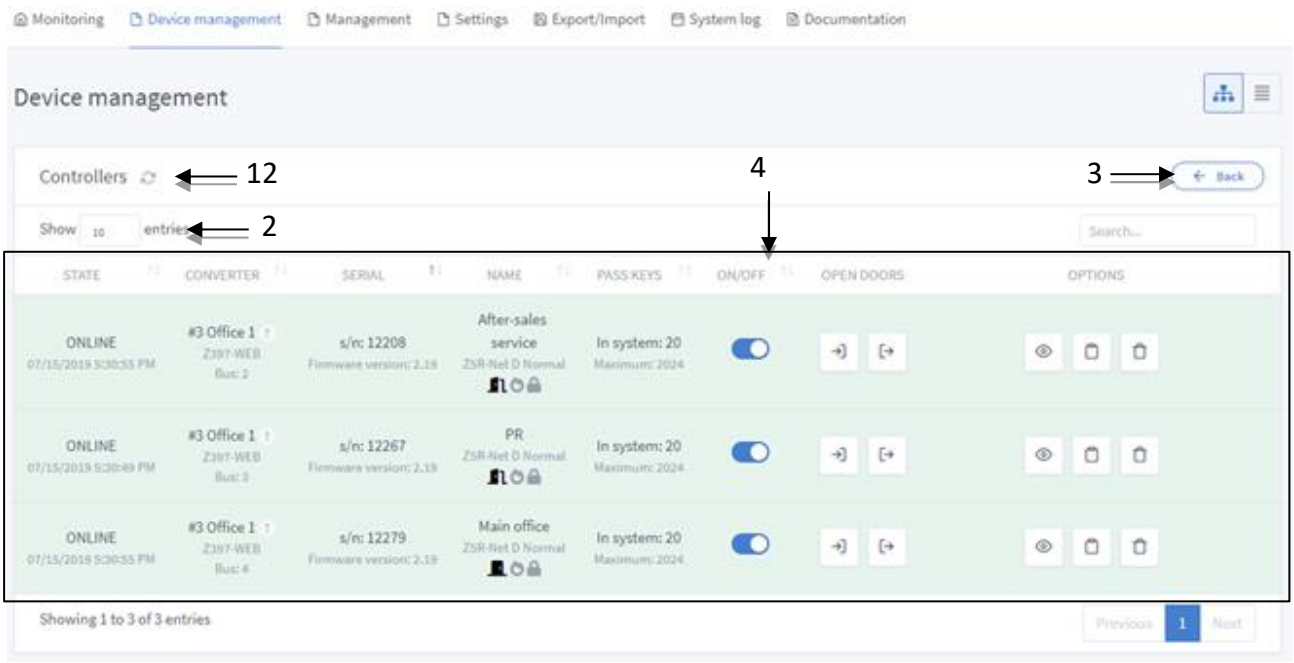


Fig.23 Page for viewing the list of controllers connected to the converter

“Controller list” page structure*(Fig.23)*:

1 - **“**Update controllers list" button;
2 - Controller list search field;
3 - “Back to converters list” button;
4 - the list of controllers is presented in the form of a table with fields:

- **STATE** – the state of the controller; depending on the state the line in the list is highlighted in color:
  - **ONLINE** – controller is online, no errors;
  - **OFFLINE** – controller is offline;
  - **DISACTIVE** – controller is disabled;
  - **ERROR** – error is found.
  - **CONNECTING** – connecting to the converter;

In case of error, informational button will appear near controller state. If you click this button, error information will be displayed.

- **CONVERTER**– name and number of a converter, this field also displays a bus number;
- **SERIAL**– the serial number of a controller; this field also displays a firmware number of a controller;
- **NAME**– name of a controller;
- **PASS KEYS**– number of cards in the system; and the maximum number of cards for this controller;
- **ON/OFF** – enable and disable controller;

- **OPEN DOORS**– door control buttons:

  – open doors for entry;

  – open doors for exit.

- **Options**:

  – view controller info;

  – view events history;

  – delete controller.

Options description are in the section "Device management: controller list".

Attach a license

Attaching a license file is available only for connected converters

License — there are certain limits on the number of serviced controllers and the number of cards in each of the controllers. The initial (free) license serves 2 controllers and 10 cards. To increase the maximum number of controllers and cards, you need to apply for the purchase of a license.

When a converter added to the system and it has no license, the system will automatically install the basic one - 2 controllers and 10 cards.

When switching from Guard Light software to Guard Plus software, you must request the appropriate license for the converter from the manufacturer. When adding a converter to the Guard Plus system, which the license is not compatible with this software, a basic license will be automatically installed.

To attach a license file do as follows:

1. Click button in “Options” column for converters in «Device management» section *(1 at Fig.24)*.
2. Select a license file *(1 at Fig.25)*. License files have the extension: .lic or .dat**.**

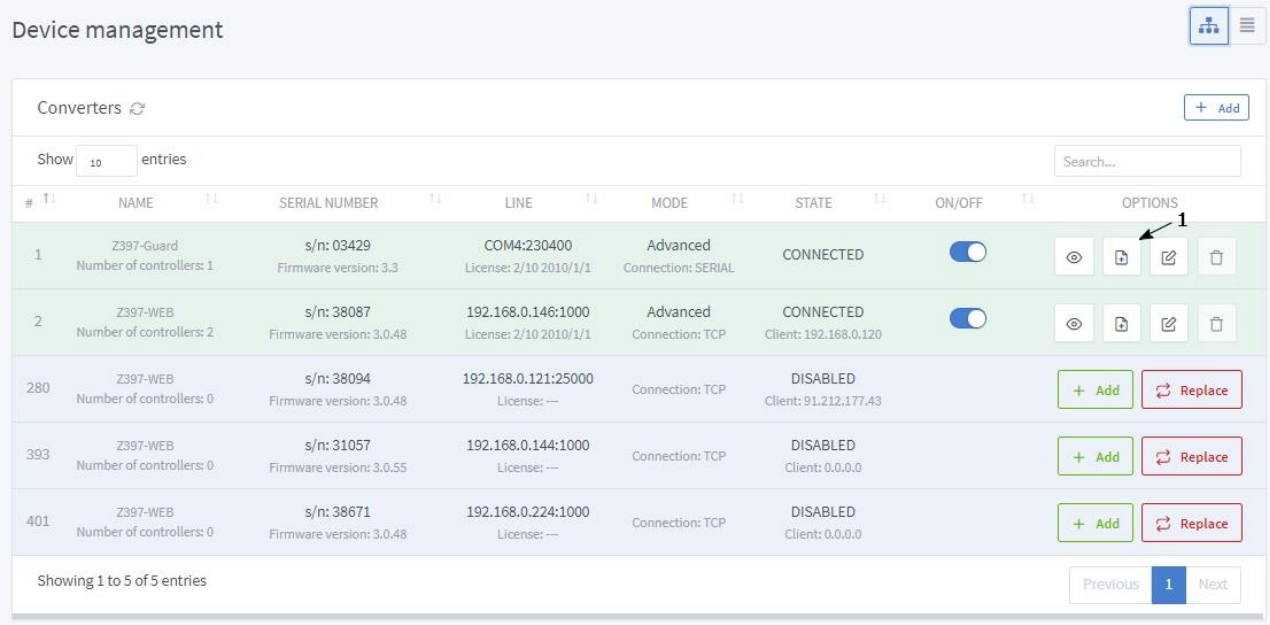


Fig.24 Attaching converter license

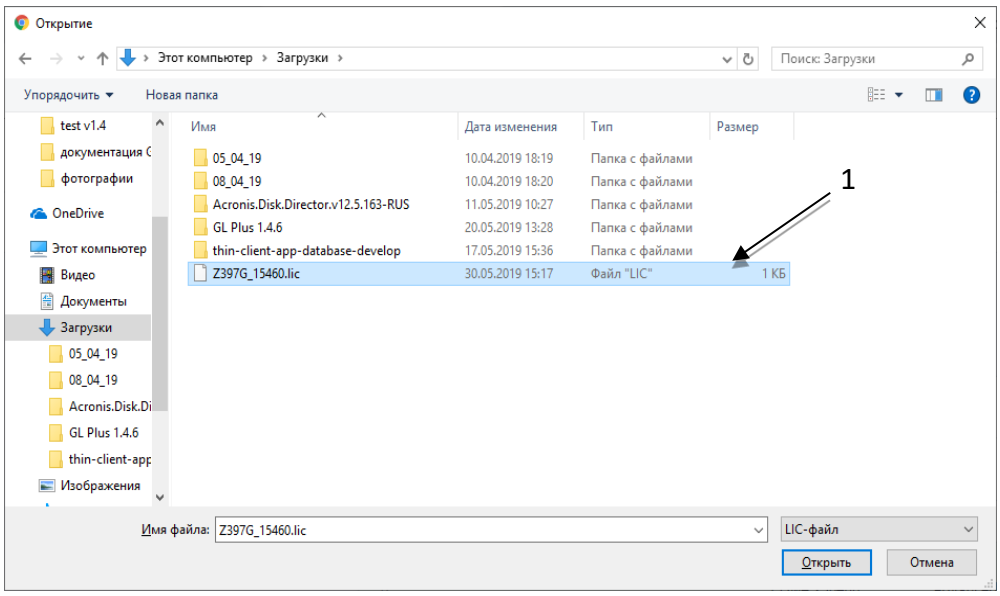


Fig.25 Selecting a license file

3. As a result, the installed license will be displayed in the corresponding field of the “Line” column on the page for viewing the list of converters (1 in *Fig.26*).

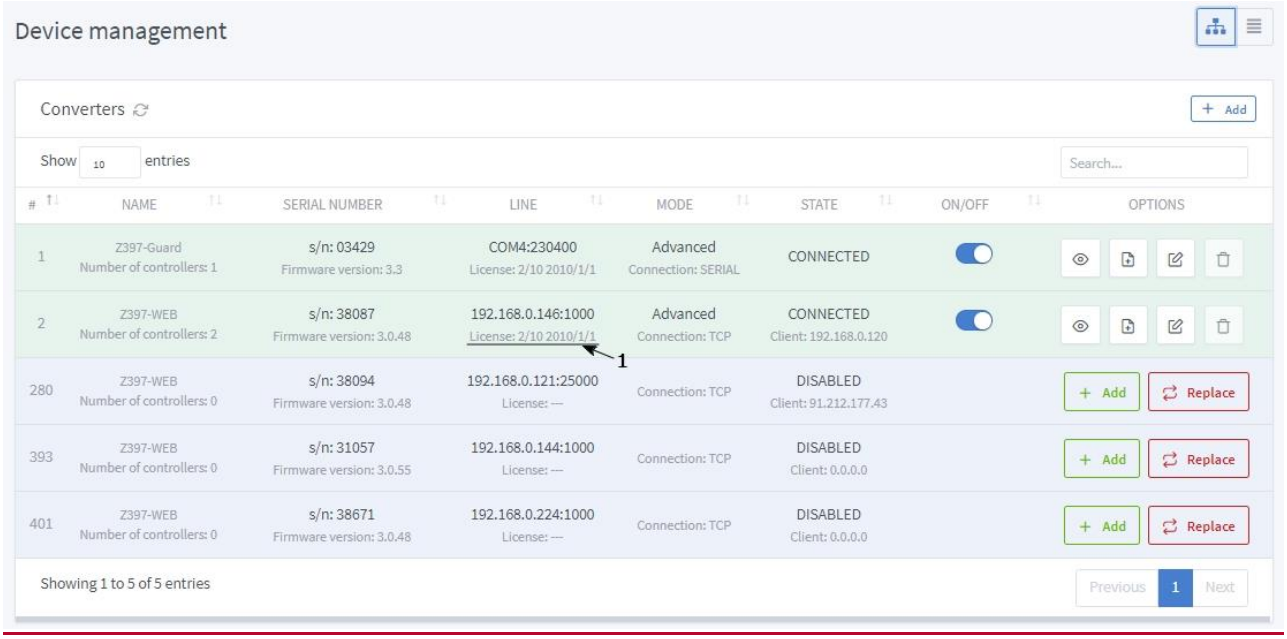


Fig.26 Current license display

3.2.3 Access modes switching

Access mode – a type of access control to the controller working area. The access mode is for situations when different requirements for access control are presented at different times of the day. For example, when considering the office or store work schedule, it can be divided into several periods. The first is morning: sellers or managers come to work, access for outsiders should be blocked. Working day: customers come, they need to enter the premises freely. Evening: similar to the morning - workers get ready and go home, visitors have nothing to do in the office, they can exit using the exit button. Night: only security workers can have access, access to other people is not granted.

There are two ways to switch access modes in the Guard Plus system: by time zone and by network command.

By time zone. The controller has two additional time zones, which allow you to set the time period with the current access mode, in which the controller should be in the active time zone. This access mode activation method has the highest priority.

By network command. Using Guard Plus, the operator can remotely switch access modes. Access mode switching is performed on the controller settings page (Fig. 29).

3.2.4 Device management: Controllers

This page allows to work with controllers, where you can see information about controllers, that are added to the system, and perform all the available manipulations with them.

“Controllers list” page structure *(Fig.27)*:

1 - **“**Update controllers list" button;
2 - number of controllers displayed at a page;
3 - search field;
4 - the list of controllers is presented in the form of a table with fields:

- **STATE** – the state of the controller and the time of the latest synchronization (depending on the state the line in the list is highlighted in color):
  - **ONLINE** – controller is online, no errors;
  - **OFFLINE** – controller is offline;
  - **DISACTIVE** – controller is disabled;
  - **ERROR** – error is found.
  - **CONNECTING** – connecting to the controller;

In case of error informational button will appear next to the controller state label, on click the error, information will be displayed.

- CONVERTER – name and number of a converter, this field also displays a bus number;
- SERIAL – the serial number of a controller; this field also displays a firmware number of a controller;
- NAME – name of a controller;
- PASS KEYS – the number of pass keys in the controller’s memory (displays only pass keys synchronized through the system), and the maximum number of cards for this controller (under license);
- ON/OFF – enable and disable controller;
- OPEN DOORS – door control buttons:
- **Options**:

  – view controller info;

  – view event history;

  – delete controller.

5 - “Add controller to the system” button
6 - “Replace controller” button
7 - page navigation buttons

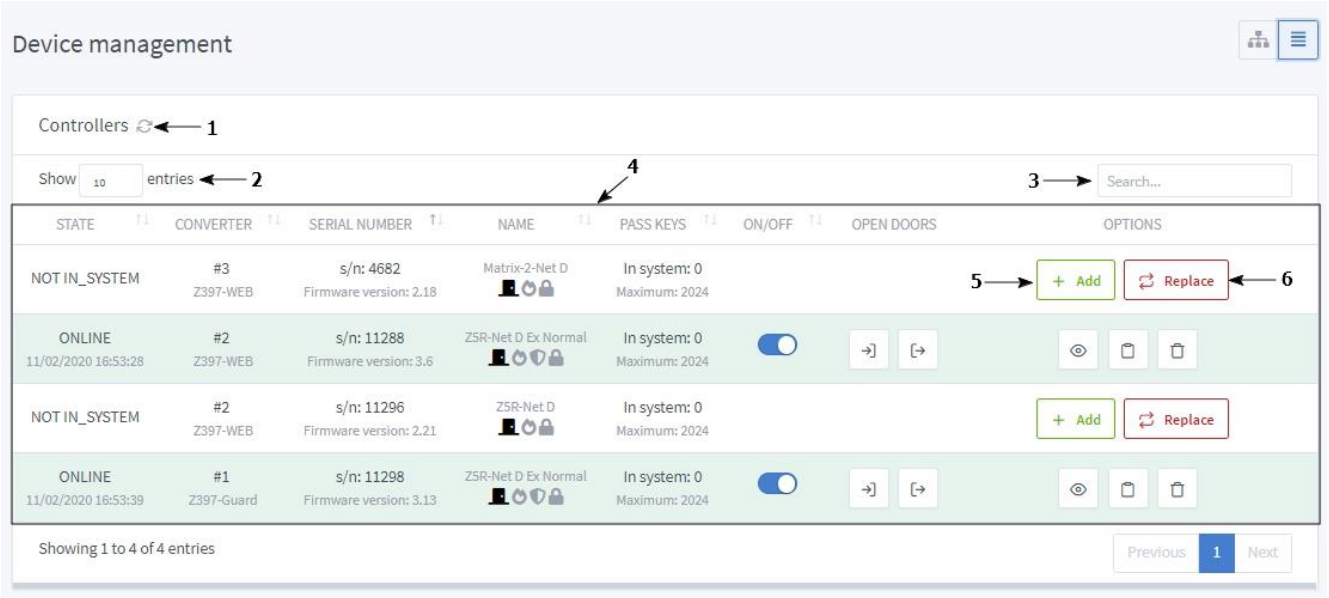


Fig.27 Page "Device management: Controllers"

Adding controller to the system

When adding a controller to the system, all its previously set parameters are reset.

1. Find the required controller in the list.
2. Click the "Add" button *(5 in Fig.27)*
3. Wait for connection to the controller. When successfully connected to the controller, "ONLINE" is displayed in the STATE field.

Replace controller

To replace a controller, you need to do as follows:

1. Select a controller (of those that are not added to the system), which should replace another one.
2. Click "Replace" button.
3. In this window*(Fig.28)*find a controller that needs to be changed and click "Select" button*(1 atFig.28).*
4. Wait for the controller to be replaced.

Fig.28 Controller selection window to be replaced

You can replace a controller from the controller page through converter *(see Fig.20),* as well as from the page "Controller management" *(see Fig.29).*

View controller information

This option is for viewing and also for editing some information about the controller. This option is for viewing, as well as for editing some information about the controller and setting the mode switching time zones. After pushing the  button, two windows appear: information window *(Fig.29)* and time zone settings window (*Fig.30*).

Controller information view:

- **Type**— controller type;
- **Name**— name of a controller (can be edited);
- **Serial number**— serial number of a controller;
- **Status** — status of a controller: ONLINE, OFFLINE, ERROR, DISACTIVE;
- **State**—ACTIVE/DISACTIVE;
- **Pass key capacity**— the maximum number of pass keys that can be stored in the controller's memory (pass keys capacity valueis presented in a format: max_q/curr_q, where max_q – the maximum number of pass keys that can be stored in the controller's memory, curr_q – current number of pass keys in the memory);
- **Event capacity**— maximum number of events that can be stored in the controller's memory (event capacity value is presentedin a format: max_q/curr_q, where max_q – maximum number of events, curr_q – current number of events in the controller's memory);

Events are recorded to controller's memory only in case if there is no connection to a controller. When maximum number exceeded, earlier events are deleted.

- **Controller software version** — the version number of the controller software;
- **Device time** — the current date and time of a controller;
- **To use system time:**
  - On – it uses system time based on the specified time zone in the system settings.
  - Off – it uses the time zone specified in the field "Timezone" on the page "View controller information window" (*Fig.29*).
- **Timezone —** controller time zone (if a user uses system time, then the time zone indicated in the system settings is displayed, this field also becomes unavailable for editing);

To display time of events (entries, exits) correctly, it is necessary to set up the correct time zone on all controllers used.

- **Door opening time, s** — time of the voltage supplying or tapping it off from the controller to the lock;

Waiting time parameters for opening and closing a door are applied only when a door opening /closing sensor is installed.

- **Waiting time for opening door, s**— if this parameter is not zero, then the event about the enter/exit will not be formed immediately when the card is presented, but at the moment of a door opening. After the expiration of the indicated number of seconds, events “Door unlocked”, "Pass point is passed" or "Pass point is not passed” appear;
- **Waiting time for closing door, sec**— indicates to the controller the time during which the door should be closed. If this time is exceeded, the controller will generate an event that the door is left open.

Door opening time, waiting time for opening door, waiting time for closing door can be changed in the range from 0 to 25 seconds.

If the number is bigger than 25 seconds, information will be saved **incorrectly**.

Also, when **door opening time** is 0 seconds, door will be blocked, because the impulse does not have time to trigger to process an event. The best time is 3 seconds.

- **Inversion of readers**— logical exchange of entry and exit points, used for readers installed in adjacent rooms or in case of installation errors (can be edited);
- **Modes** (optional) – access mode:
  - NORMAL - provides a passage for simple and blocking pass keys;
  - BLOCK – a passage for blocking pass keys is open, for simple pass keys - closed;
  - WAIT - after presenting a valid pass key, the controller switches to the Free Pass mode;
  - OPEN – the lock is always off.

This setting is available only for controllers that support mode switch.

If the time zone of mode switching is active, the controller switches to the time zone mode. After time zone deactivation, it switches to the mode from controller’s settings.

- **Converter**— number and name of the converter which the controller is connected to;
- **The latest connection**— time and date of the latest connection of the program to the converter;
- **Description**— short description of a controller (can be edited);

Edit controller information

You can change controller's name, time zone, open time, opening time, and controller description, as well as activate / deactivate inversion of readers in the controller information window. To confirm changes, click button Save *(1 atFig.29).*

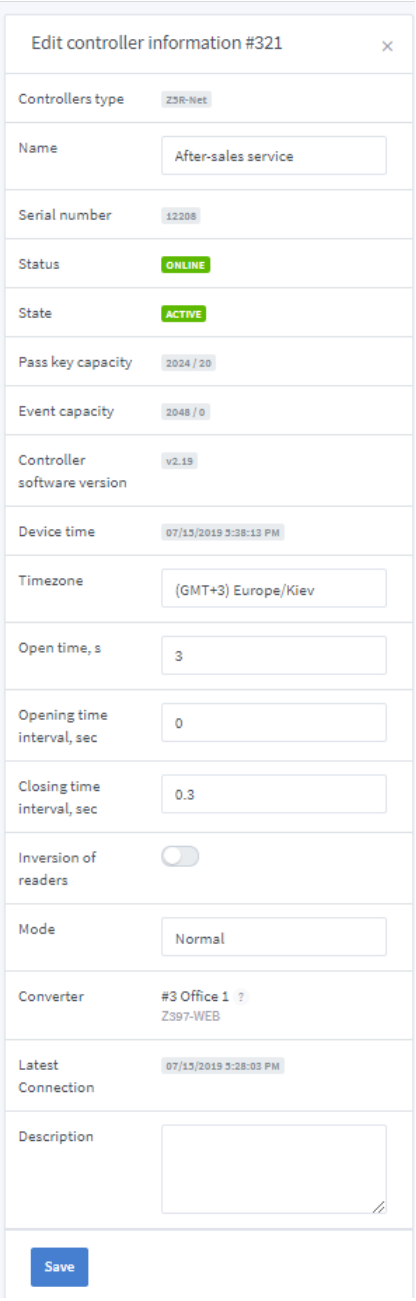


Fig.29 View controller information window

Setting time zones for mode switching

One can switch access mode by time zone clicking the button (button for viewing information about the controller) on the page "Device Management: number of controllers". 2 configurable time zones are available for each controller.

Structure of the time zone settings window:

ON/OFF – time zone on/off;

MON-SUN – day (days) of the week, when the controller is in the specified operating mode;

FROM/TILL – period in which the controller switches to the specified mode.

If the time zone is active, the controller switches to the specified mode, regardless of the controller settings (see the Modes field in *Fig.29*).

MODE - controller operation mode (NORMAL, BLOCK, WAIT, OPEN).

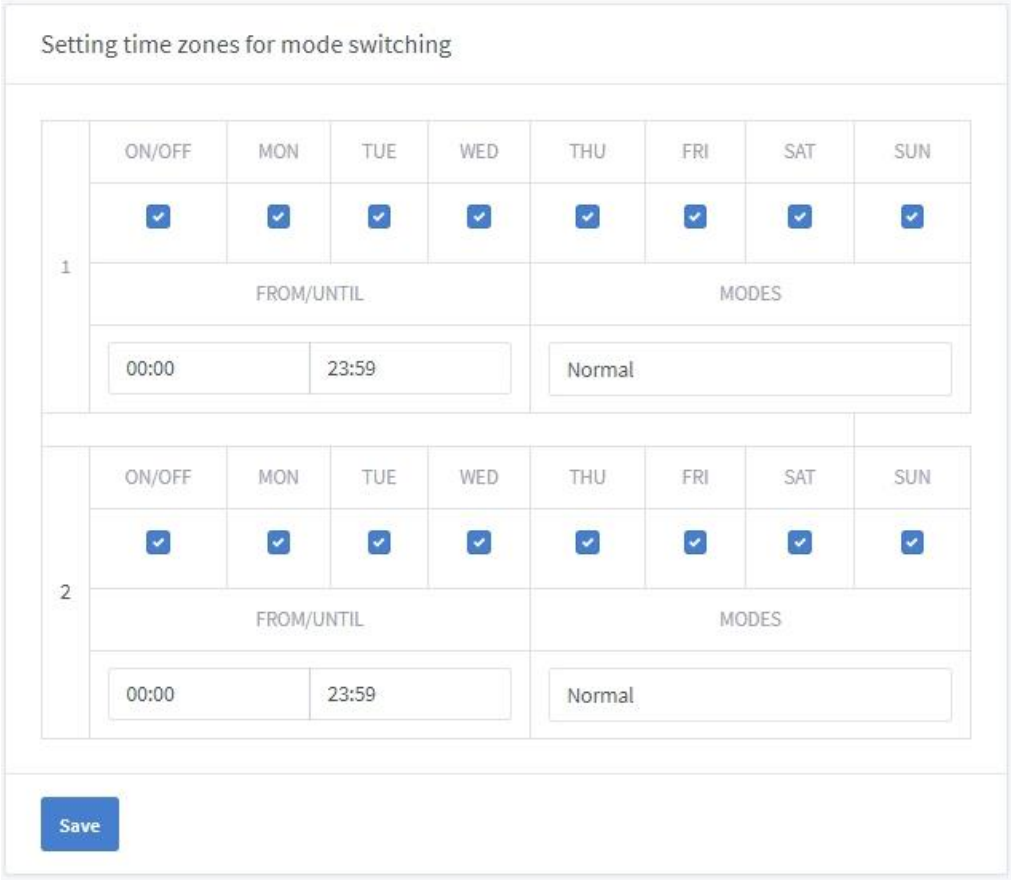


Fig.30 Window «Setting time zones for mode switching»

After adding the controller to the system, the time zone settings are set to the default values (*Fig.30* shows the default settings).

To set a time zone, do the following:

1. Activate the zone in the ON / OFF field.
2. Select the day (s) of the week where the access mode will be switched.
3. Specify the period of time in the FROM/TILL field.
4. Set the time zone mode.
5. Save time zone settings by clicking the “Save” button.

View event history

This option is used to view the event history of the controller. When you click the button in the options field, you go to “Controller event history” page *(Fig.31*).

“Controller event history” page structure *(Fig.31):*

1 - “Update event history” button;
2 - the number of entries displayed on one page (can be changed);
3 - “Back to controllers list” button;
4 - “Clear the history” button;
5 - search field;
6 - event log is presented in the form of a table with fields:

- **TIME**— date and time of recording an event;
- **TYPE**— description of an event;
- **SOURCE** — source of an event (0 – open a door using a button from the web interface, 1 – open a door using a pass key);
- **CODE** — a pass key code that triggered an event.

For the event «EVENT_ENTER_SUCCESS»:

- when opened with RS-485 command, the identifier with the 00000000001E is indicated in the «Code» field.
- when opened with the button, in the field “CODE” identifier is indicated with the number 000000FFFFFF.

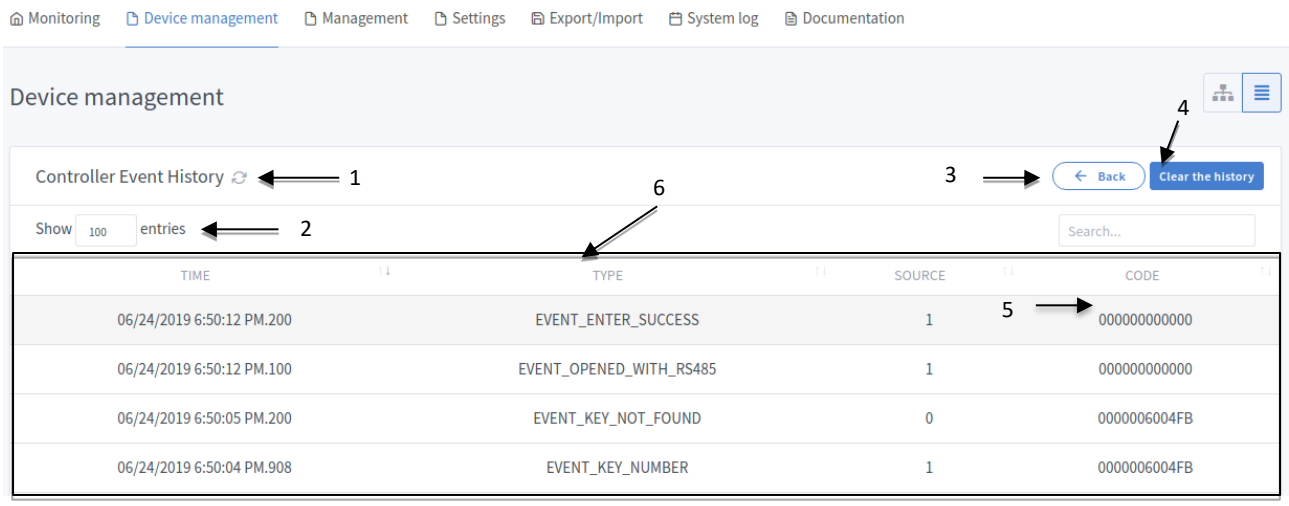


Fig.31 “Controller event history”

Delete controller

To delete controller do as follows:

1. Click  button near a controller that needs to be deleted in “Options” column at “Device management” page.
2. As a result, a confirmation window will appear*(see Fig.32)*.

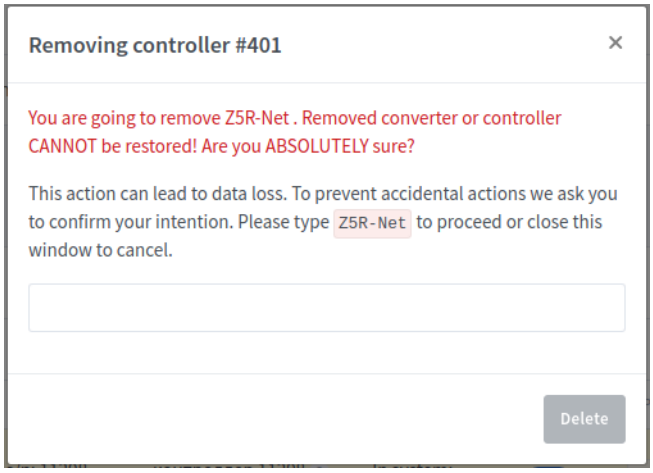


Fig.32 Confirmation window of deleting controller

3. After following all the instructions and confirming intentions to delete controller, button "Delete" will be active.

To prevent accidental actions, "Delete" button is blocked until the user confirms their intentions.

4. Click button Delete

3.3 Management

"Management" menu includes the following sections:

"Working areas" - working areas management (viewing and editing existing areas, adding new areas);

"Set pass points" - setting and editing pass points;

"Organizational units" – organizational unit management (viewing the list of existing organizational units, adding new organizational units, editing organizational unit information and editing access settings for organizational units);

"Persons" – persons management (viewing the list of persons, adding persons, editing information about persons and editing access settings for each person);

"Manage pass keys" - pass keys management(viewing all pass keys in the system, editing pass keys, manually adding pass keys);

"Manage guests pass keys" - guests pass keys management(viewing the list of guests pass keys added to the system, issuing pass keys to guests, editing information and adding new pass keys);

"Reports" - viewing reports of different types (time sheet, movement, traffic);

"Access map" - viewing access maps for each person;

"Synchronization" - synchronization of schedules and pass keys for each group of controllers.

3.3.1 Working areas

In order to simplify access settings, the concept "Working area" has been introduced. "Working area" concept is to simplify the configuration of access.

The working area is an independent space (territory) to which access is regulated. There are controllers for each working area to control access to the specified territory. This subsection is responsible for creating and editing working areas.

"Working areas" page structure *(Fig.33)*:

1 - add new working area;

2 - "Show/hide detailed info about working area" button;

3 - "Detailed info about working area full screen view" button;

4 - "Edit working area" button;

5 - "Add sub working area" button;

6 - "Delete working area" button;

7 - "Remove controller from working area" button.

After deleting a parent working area, all its children areas remain; first child area in a list becomes a parent area instead of deleted one.

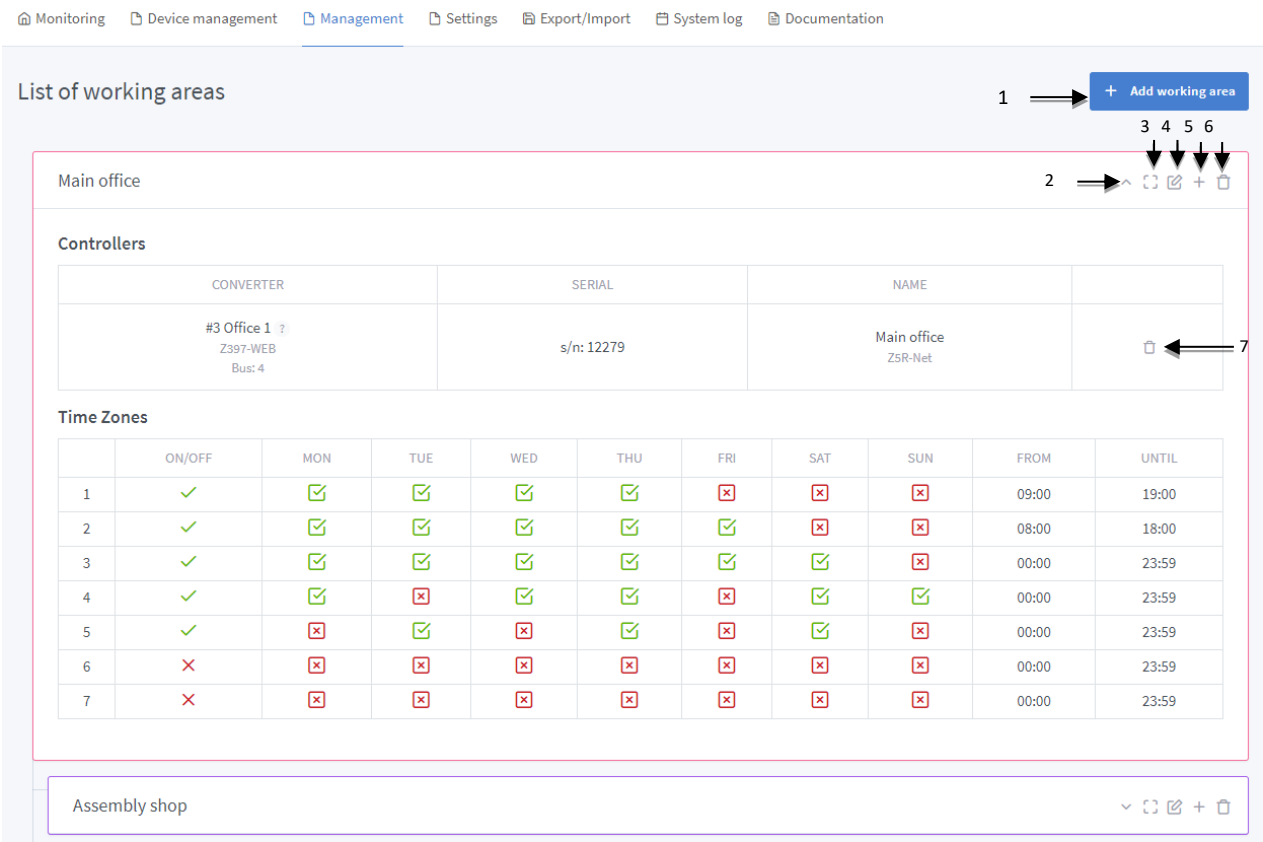


Fig.33 Page "Working areas"

Add working area

When adding a working area with a controller attachment or when attaching a controller to an existing area, it is necessary to perform synchronization with the controller manually.

To add a working area do as follows:

1. Click button + Add working area at the page "Working areas", as a result, "Detailed Information" tab opens. *(Fig.34*).
2. "Detailed Information" tab has:
   - **Parent working area** — area that can include one or more child areas;
   - **Working area name** — name of an area that is clear for everyone (for example, "Accounting" or "Administration");
   - **Comment** — comment to a zone (optional);
   - **Working area color** — a color of an area in the RGB system, it is also possible to select a color from the set.
3. To go to the tab of attaching controllers to the working area *(Fig.35),*click button *(Fig.34)* → Next

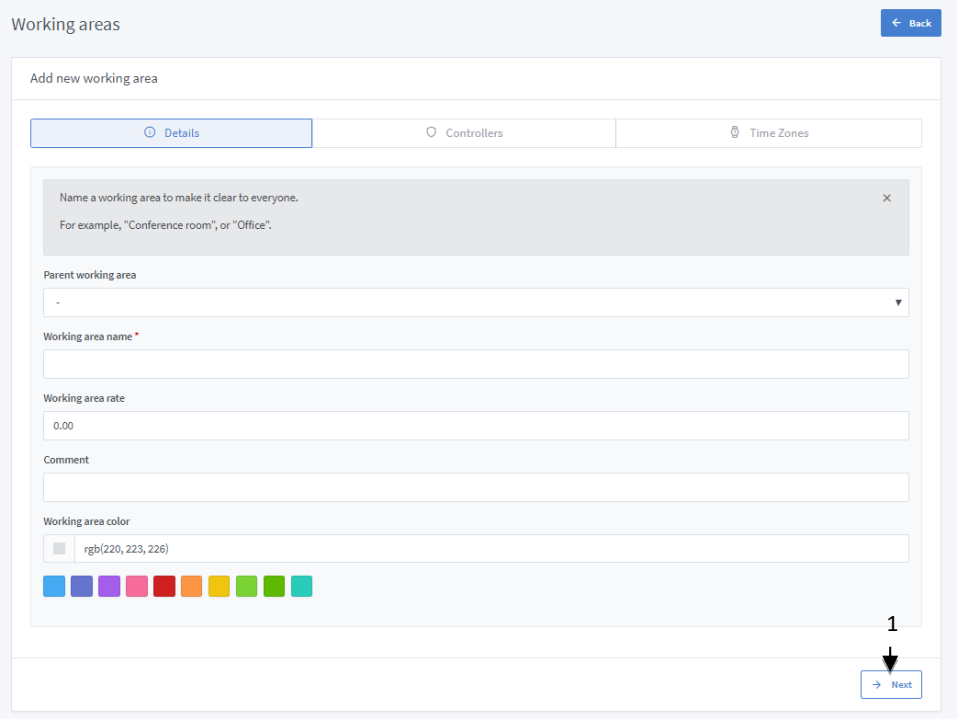


Fig.34 Add working area: detailed info

4. On “Controllers” tab*(Fig.35)*select controller (or controllers)which is installed in this room and controls access to it.

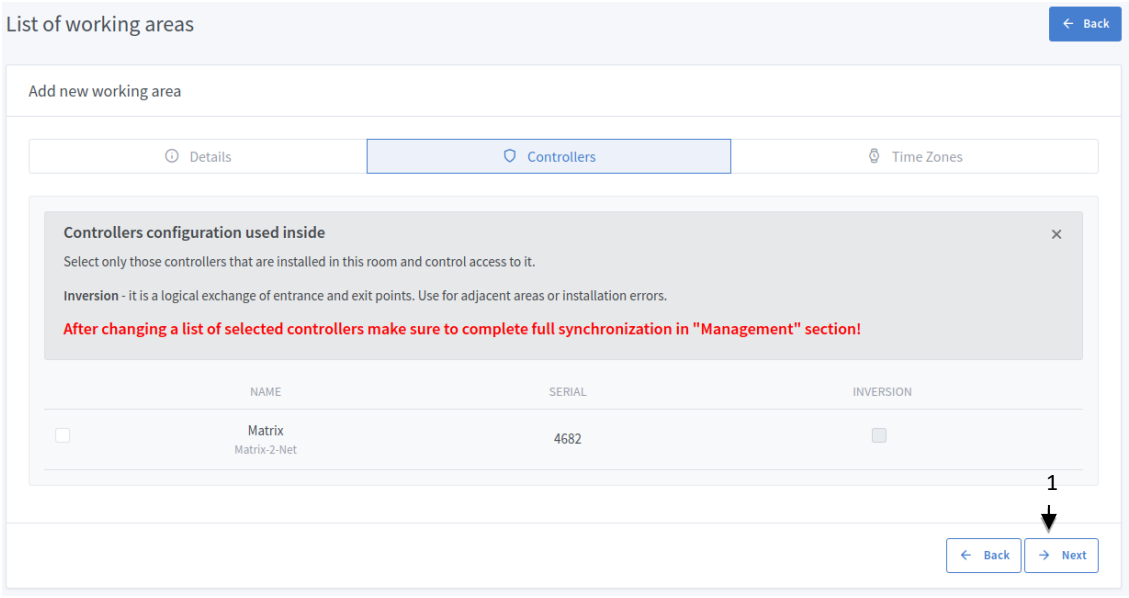


Fig.35 Add working area: controllers

5. Go to “Time zones” tab*(Fig.36)*clicking Next ton*(1 at Fig.35).*
6. Set time zones for working areas on “Time zones” tab *(Fig.36),*to use it further in access rules settings or directly for an employee.
   There are 7 time zones available for setting. If a zone has a parent zone (that is, this zone is a successor zone), then you can select "Inherit from the parent" option *(Fig.37)* and for this working zone the time zones will completely correspond to the parent.

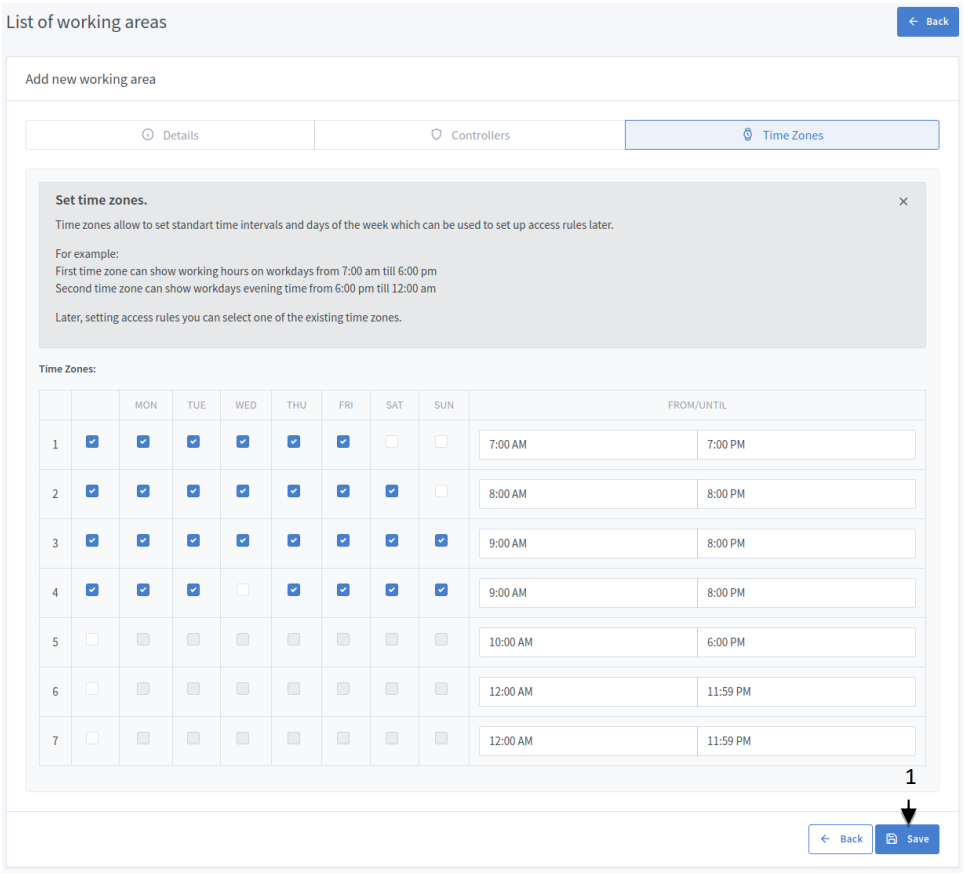


Fig.36 Add working area: time zones

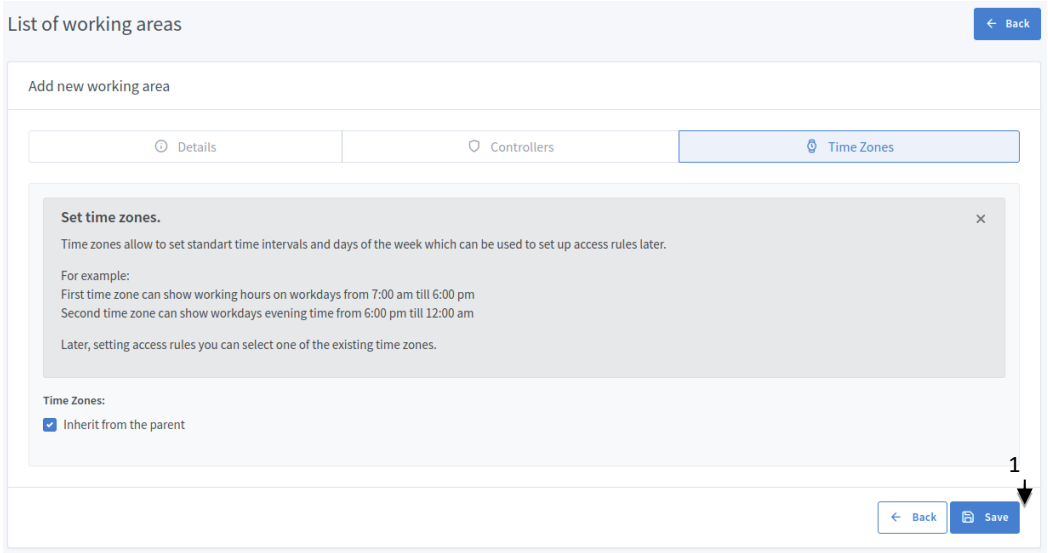
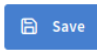


Fig.37 Inherit time zones from the parent

7. To save working area settings click button 

(1 at Fig.36, Fig.37).

3.3.2 Set pass points

This subsection provides functionality for setting up each controller as a pass point (entrance/exit) between the areas, that determine the direction of movement of a person.

“Set pass points” page structure *(Fig.38)*:

1 - “Update pass points” button;
2 - field showing maximum number entries on one page;
3 - search field;
4 - working area with a controller assigned (pass point);
5 - pass point name (custom);
6 - pass point corresponding controller;
7 - controller serial number;
8 - pass point state (on/off; determines whether or not to take into account the settings of each pass point);
9 - select entrance point;
10 - select exit point;
11 - navigation buttons.

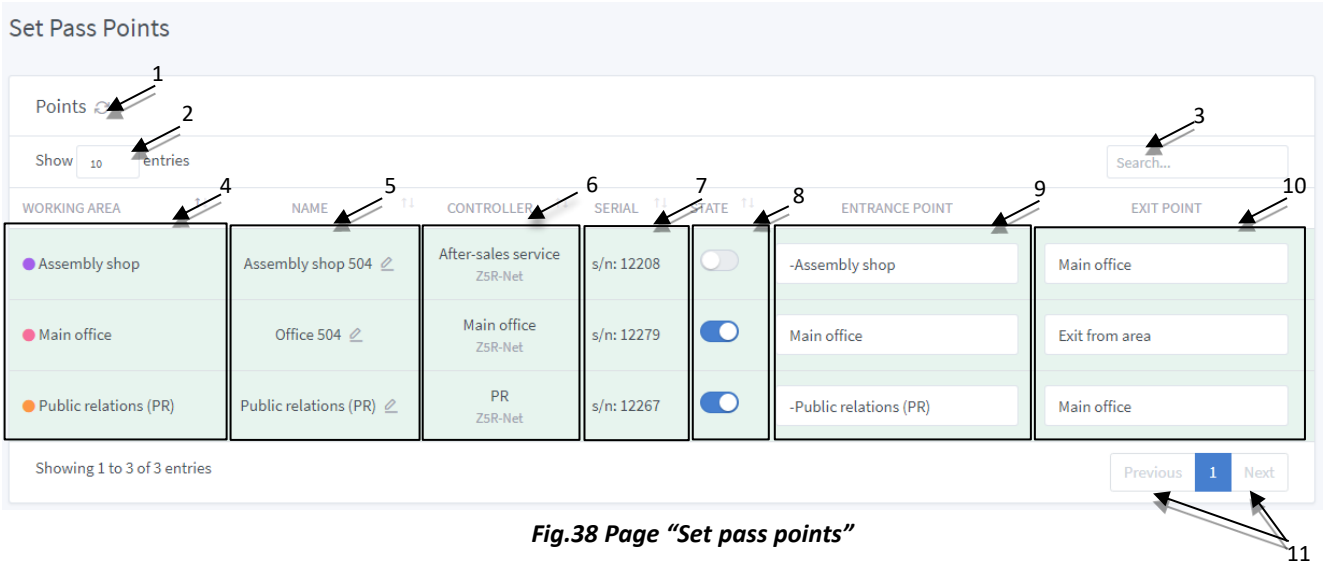


Fig.38 Page “Set pass points”

Select entrance and exit points

Pass point means a controller after passing which, the system obtains “entrance/exit” event. At “Set pass points” page each controller, in accordance with working area to which it is assigned, has its entrance point (where to) *(Fig.39)*and exit point (where from) set *(Fig.40)*.

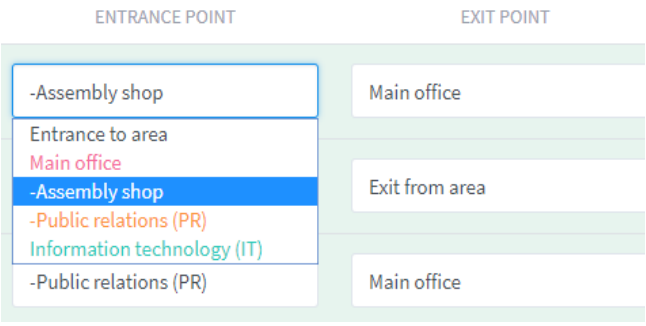


Fig.39 Select entrance point

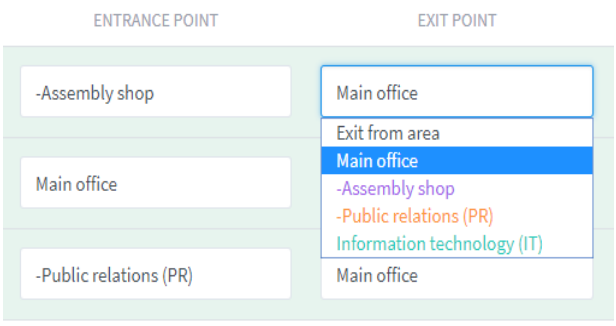


Fig.40 Select exit point

Zero pass point

This concept is introduced as the definition of the entrance/exit points to/from the territory of a building, where Physical Access Control System (PACS) is installed (main entrance to a building, office, factory etc.).

When setting a zero pass point, entrance point is set*(9 at Fig.38),* and exit point remains by default as “exit from the area”.

The results of these settings are necessary to display correctly events at the pages “Photoverification”, “Events log”, “Reports” etc.

There can be several zero pass points, you just need to set them appropriately. Zero pass points that are not set are not added to the system (it is the points that have enter and exit points as “To area” or “From area”).

A pass point means a strict fixation of the first entrance and the last exit of a person from a territory where Physical Access Control System (PACS) is installed, **for correct information in the reports**.

Add pass point name

After selecting the entry point and the exit point for the pass point (controller), you can add a name for convenience*(Fig.41)*. By this name this pass point can be selected in the Photoverification filter. *(see Fig.10),* and it will be displayed at “Events log” page in a column “Pass point”*(see Fig.13).*

To add or edit a name of a pass point, click on the corresponding button *(1 at Fig.41).* This action will open the input window *(Fig.42).*

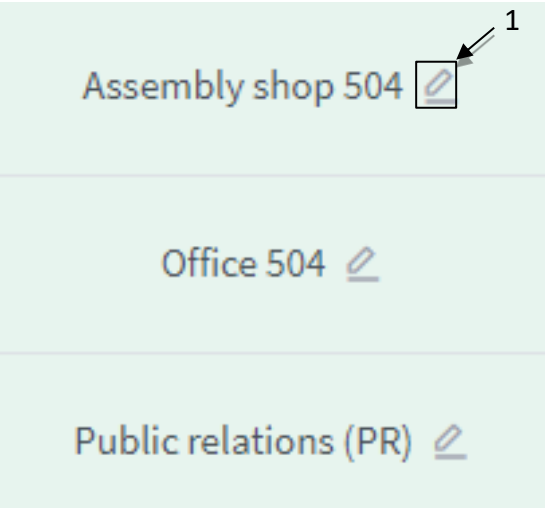


Fig.41 Add pass point name

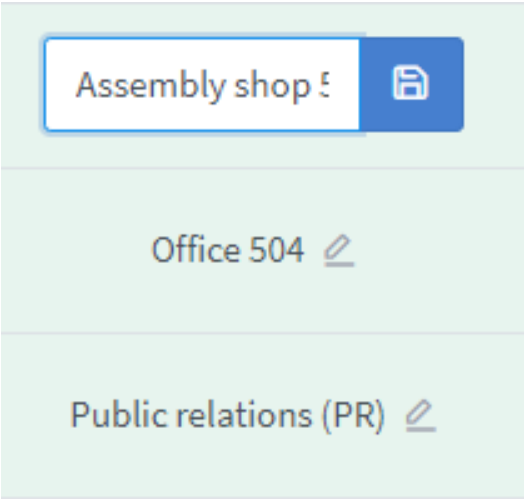


Fig.42 Input field for pass point name

 - save name.

3.3.3 Organizational units

This subsection allows to create organizational units for persons positioning. When creating organizational units, the work schedule of each organizational unit is indicated, so you can get reports on the actual presence of persons in the workplace. Also, individual access rights can be set for each organizational unit, which will apply only to persons who belong to this organizational unit.

"Manage organizational units" page structure *(Fig.43)*:

1 - "Add new organizational unit" button;

2, 3 – "Show/hide detailed information about organizational unit" button;

4 - "Detailed information about organizational unit full screen view" button;

5 - "Edit organizational unit" button;

6 - "Add child organizational unit" button;

7 - "Delete organizational unit" button.

After deleting a parent organizational unit, all its children remain; first child organizational unit in a list becomes a parent organizational unit instead of deleted one.

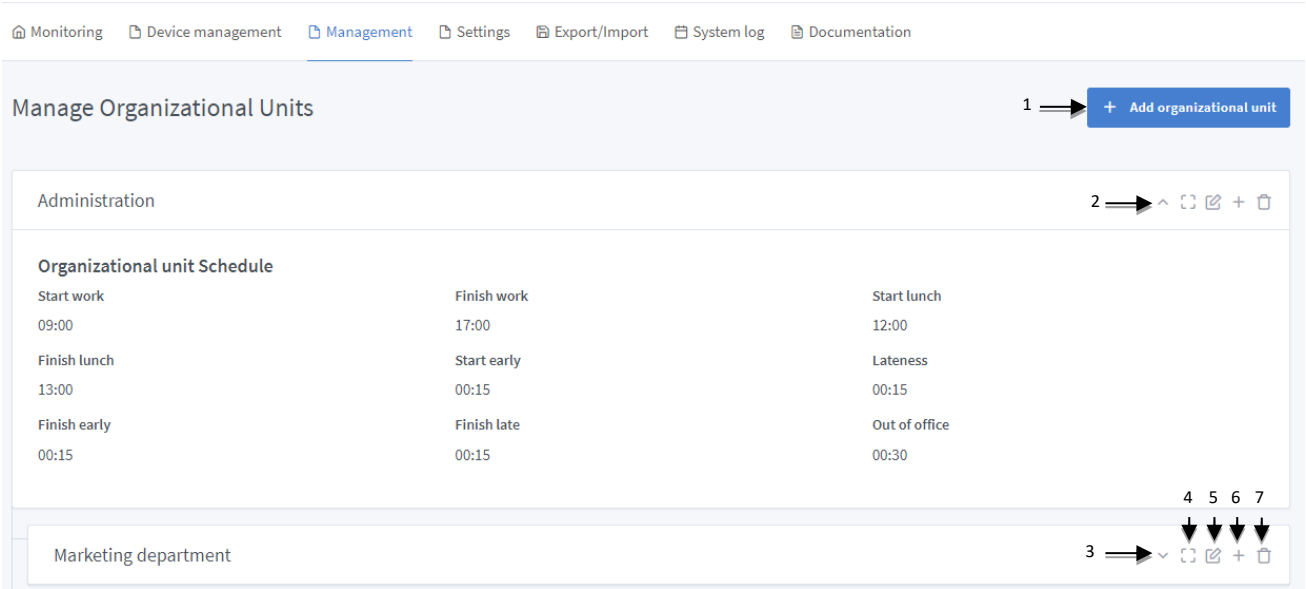
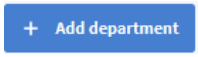


Fig.43 Page "Manage organizational units"

Add new organizational unit

To add a new organizational unit do as follows:

1. Click 

button at "Manage organizational units" page, as a result, the "Organizational unit details" tab will open. *(Fig.44).*
2. Tab "Organizational unit details" has:

- **Parent organizational unit**—an organizational unit that can include one or more other organizational units;
- **Organizational unit name** — a name of an organizational unit which is clear for all users (for example, "Accounting" or “Administration");
- **Comment**— comment to an organizational unit (optional);

3. Click [Next] button *(1 at Fig.44) i*n order to open “Organizational unit schedule” tab (*Fig.46*)

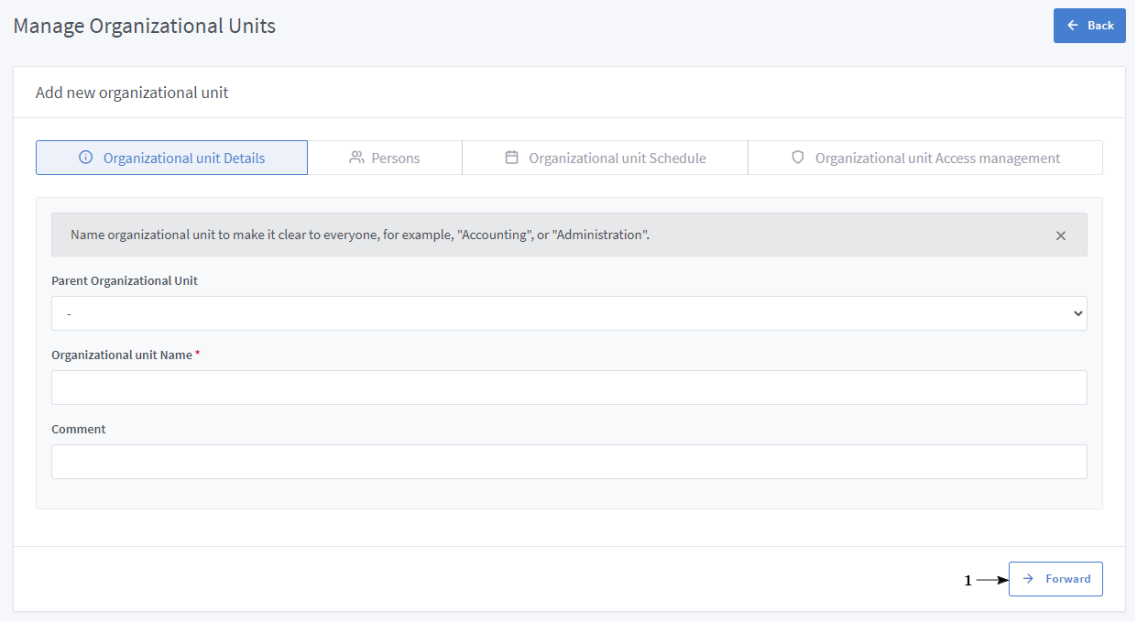


Fig.44 Add new organizational unit: detailed info

4. You can assign persons to a newly created organizational unit in the “Persons” tab if necessary.

“Persons” tab structure:

1 - output area for persons without an assigned organizational unit;

2 - output area for the list of persons assigned to a newly created organizational unit;

3 - search field for searching persons on both lists;

4 - the button for moving all persons from the "Persons in the organizational unit" list to the "Persons" list;

5 - the button for moving all persons from the "Persons" list to the “Persons in the organizational unit" list;

6 - the button to go to the “Organizational unit schedule” tab.

Assigning persons to the organizational unit can be performed only after the organizational unit is saved. If the creation/editing of the organizational unit. is not completed and the “Back” button is clicked, the selected persons will not be assigned to the organizational unit.

After the organizational unit is saved, the personal access settings of the persons assigned to the organizational unit will be inherited by organizational unit.

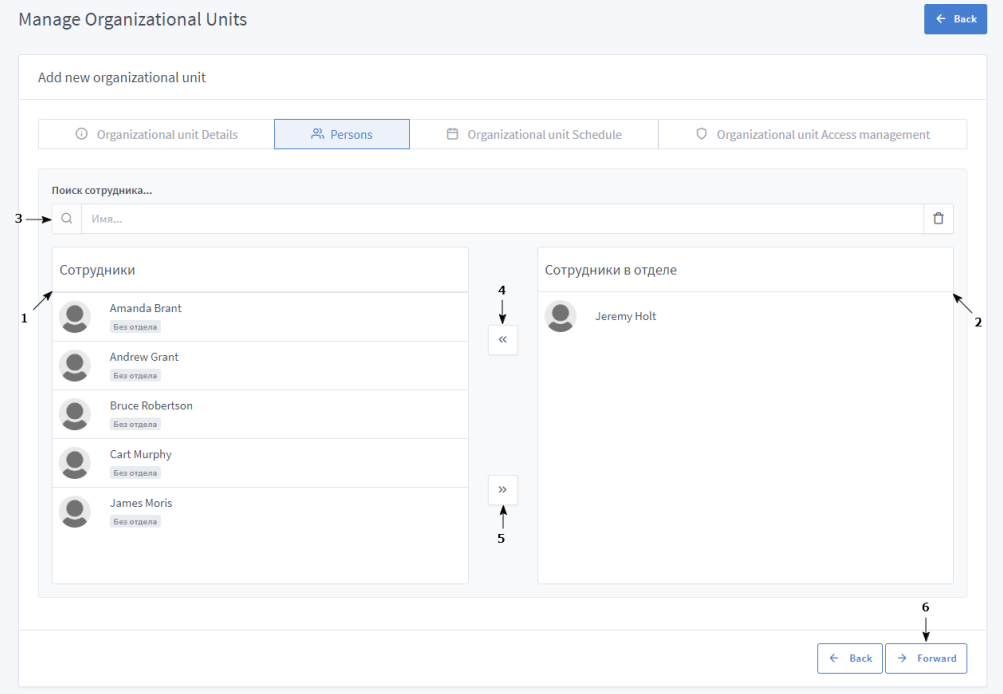


***Fig.45* Add new organizational unit: persons**

5. On “Organizational unit schedule” tab (*Fig.46),*set work schedule for an organizational unit in order to control labor discipline (this information is used for reports on the work of persons)*(see section 3.3.8 Reports)*.

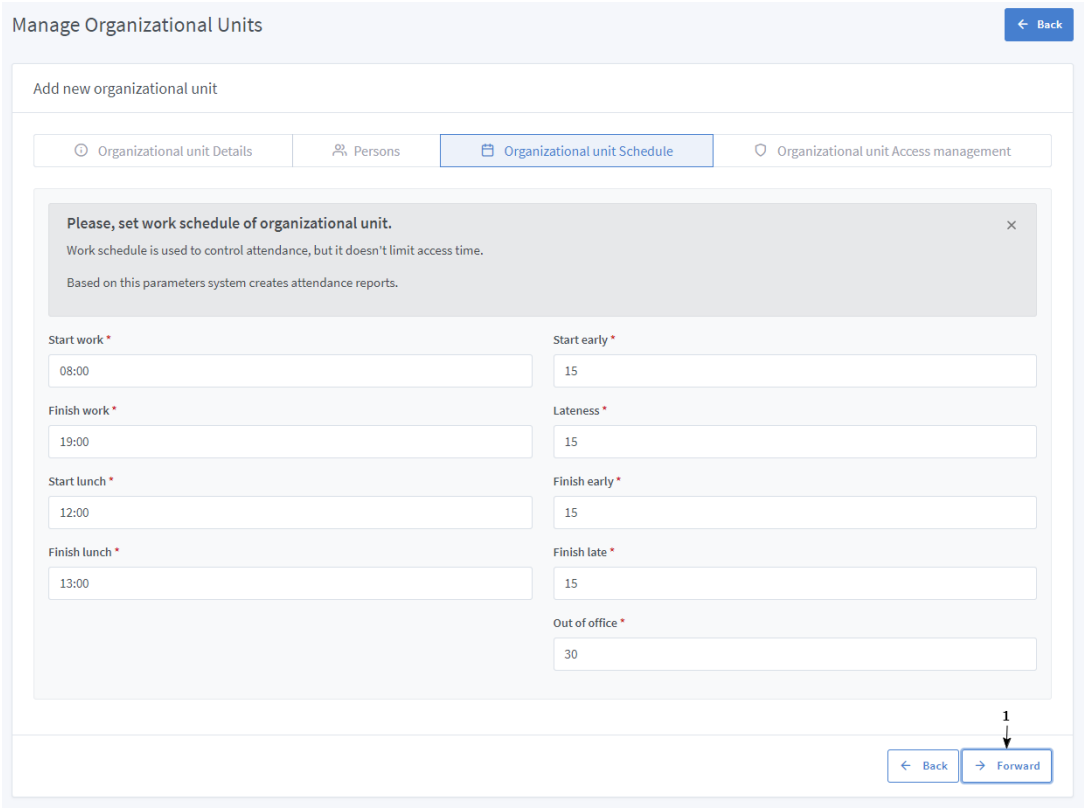


Fig.46 Add new organizational unit: Organizational unit schedule

The start time for lunch should be no earlier than the start time of work, and the end time for lunch no later than the end time of work. If the lunchtime is not within the range of working hours, the calculations for the report, which count the lunch time, will be performed incorrectly.

6. Click “Next” button*(1 at Fig.46) in order to open “Organizational Unit Time Zones” tab (Fig.46, Fig.47)*
7. Set access rules for an organizational unit. Access rules can be set on tabs “Everywhere"*(Fig.47)*and “Working areas”*(Fig.48).*

Set access rules tab “Everywhere” (*Fig.47*) - selected if all of this is a working area; there are also two access options: “Always” (access is allowed always and everywhere), “Never” (access is allowed never and nowhere).

Set access rules tab “Working areas” (*Fig.48*) - specify if this area is working area or not, access rules are set in the selected working area(s).

The following access rules are available: “Never” (this organizational unit never has an access to place(s) that are controlled by selected working area), “Always” (this organizational unit always has an access to place(s) that are controlled by selected working area), “On schedule” (access rules of an organizational unit are set according to time zones which can be selected from available time zones in this working area.

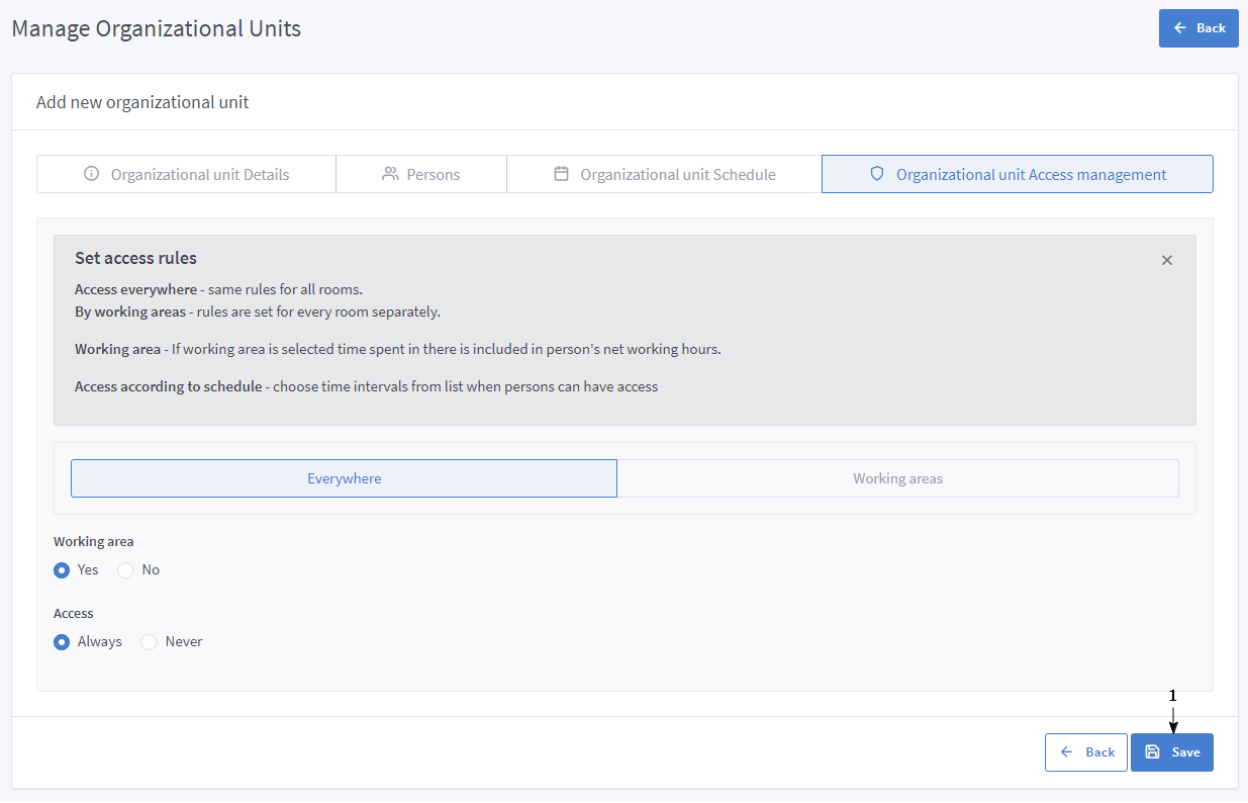


Fig.47 Add new organizational unit: set access rules (tab “Everywhere”)

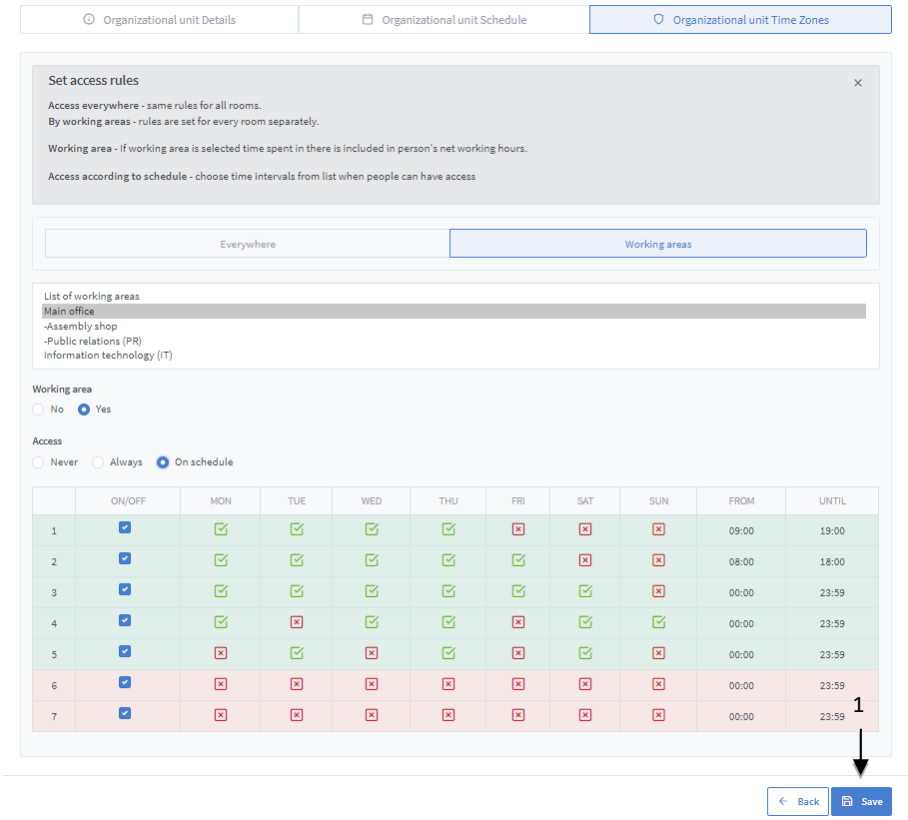


Fig.48 Add Organizational unit: set access rules (tab "Working areas")

1. To save organizational unit click button Save (*1 at Fig.47, Fig.48*).

Edit organizational unit

To edit an organizational unit, click "Edit" button *(5 at Fig 39)*. Rules that are applied here are the same as for adding.

3.3.4 Persons

This subsection allows to manage persons, including guests. The user can add persons to the system, set access rights for them and also assign them to the organizational units.

"Persons" page structure *(Fig.44)*:

1 - button that shows "Everyone";
2 - button that shows "Persons" (persons only);
3 - button that shows "Deleted" (persons/guests);
4 - button that shows "Guests" (guests only);
5 - "Add new person" button;
6 - "Update persons list" button;
7 - search field;
8 - the number of entries on one page;
9 - navigation buttons (if there are several pages of persons);
10 - persons list is presented in the form of a table with fields:

- **PERSON** – full name of an employee, it also displays whether a person is a guest;

- **STATE** – persons' state in the system (active, deleted);
- **Person's location** – the current location of the employee indicating the direction relative to a working area (the last event in the displayed area is the entrance or exit), as well as the date and time of entry into the area;

The color of the text to display the location of the employee corresponds to the color that was specified when creating the working area.

In case if an employee moved outside the working areas, then in the "Person's location" column the name of the area, from which the exit was made, is displayed, with a marker "Away", as well as the date / time of leaving the area and the direction .

- **NUMBER**– person's personal number;
- **Organizational units** – organizational units assigned to a person;
- **POSITION**– person's position;
- **PASS KEYS** – number of available pass keys;
- **ACTIONS**:

  - edit person's info - "Edit" button;
  - delete person - "Delete" button;
  - restore person –«Restore person» button;
  - person movement history
  - person changes history

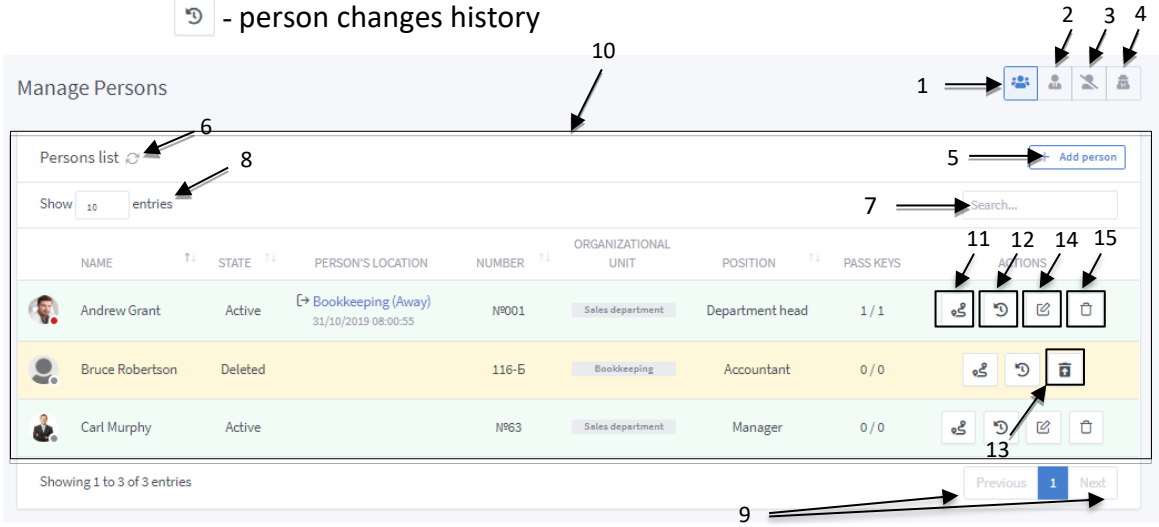


Fig.49 Page "Persons"

If person is active - the row is highlighted in green, if person is deleted - in yellow.

Add person

Click button + Add person and the page "Adding person" will appear*(Fig.45).*

"Adding person" page structure *(Fig.50)*:

1 - "Back to persons list" button;

2 - Form "Adding person" – adding person's information to the database;

The person gender field is disabled by default and is not displayed on the person adding page. To activate the ability to choose the gender of a person, you need to go to the system settings and activate person gender selection.

3 - Form “Available Pass Keys” – managing person’s pass keys (assigning available pass keys to a person, adding pass keys);

4 - Form “Organizational units” – assigning a person to an organizational unit;

5 - Form “Personal Access Settings” – setting person’s personal access to areas at the territory;

6 - “Guest” option - shows if a person is a guest or not;

7 - “Save” button;

8 - form for setting blocking periods for person’s pass keys (see *3.3.5 Pass keys blocking mode*).

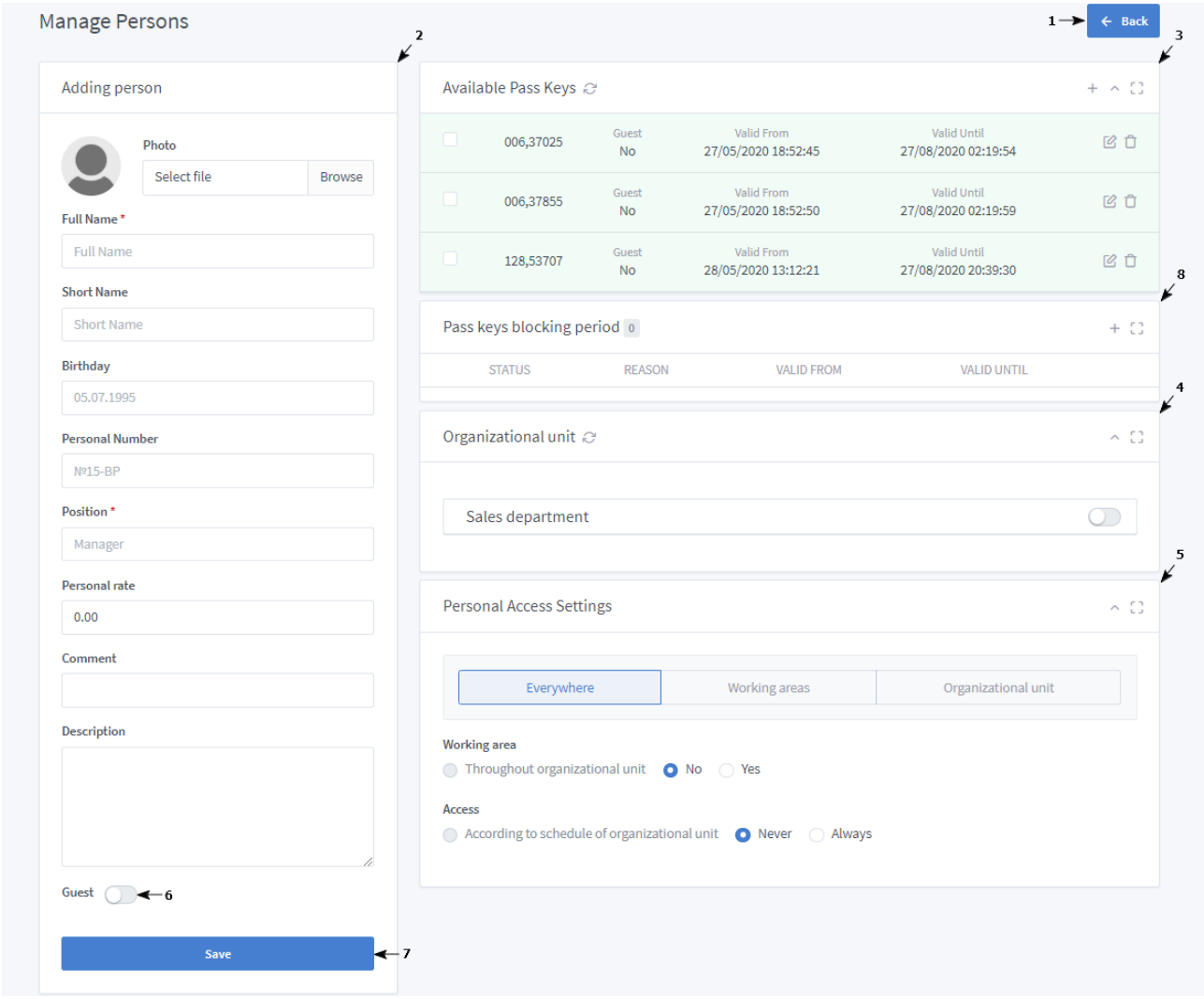


Fig.50 Page “Adding person”

Form “Adding person”

To add a person, you must fill in full name and position; other input fields are optional.

If “Guest” radio button is selected as “Yes” (6 at *Fig.50*), then “Position” field is optional.

Form “Available Pass Keys”

Form structure “Available Pass Keys”*(Fig.51)*:

1 - “Form update” button;
2 - “Add new pass key” button (manually);
3 - “Show/hide form” button;
4 - “Open form in full screen” button;
5 - “Edit a pass key” button;
6 - “Delete a pass key” button;
7 - the list of person’s available pass keys is presented in the form of a table with fields:

ASSIGN– assign a pass key to an employee*(8 at Fig.51)*;

PASS KEY– pass key number*(9 at Fig.51)*;

VALID FROM– date and time when a pass key became valid (access to areas using this pass key is open) *(10 in Fig. 46)*;

VALID UNTIL– pass key expiration date and time *(11 at Fig.51)*.

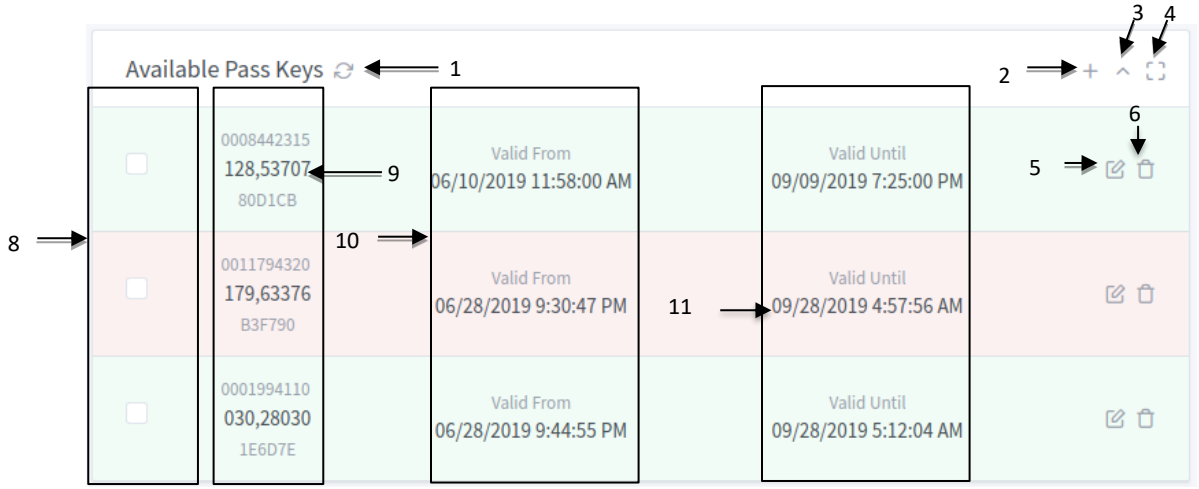


Fig.51 Adding person: Available pass keys

If pass key row is highlighted in green - pass key is active, in red - disabled. Deleted cards are not displayed in this form.

You can read how to add a pass key in “Manage Pass Keys” section.

Form “Pass keys blocking periods”

Form “Pass keys blocking periods” structure (Fig.51):

1 - indicator that shows number of person’s blocking periods;
2 - button that adds a blocking period;

3 - button that collapses the list of blocking periods (the list collapses to one of the closest periods);
4 - button that expands the form to full-screen;
5 - button that goes to editing a blocking period;
6 - button that deletes a blocking period.

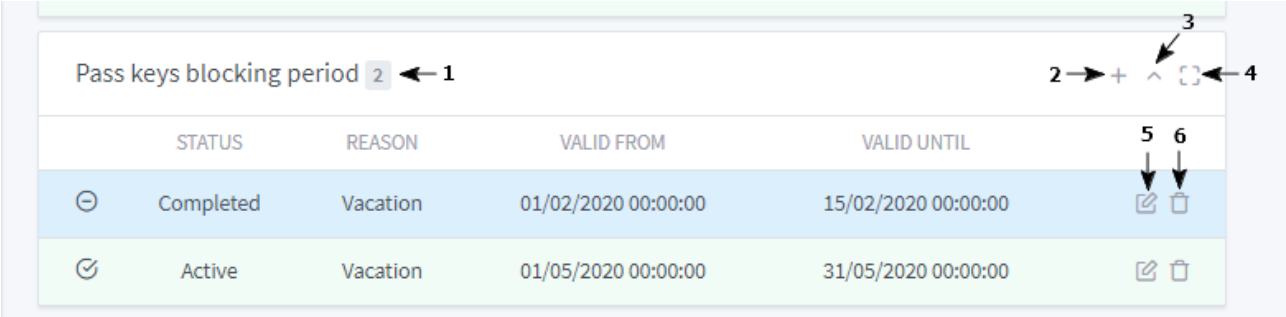


Fig.52 Form "Pass keys blocking periods"

Blocking period statuses

- **Pending** - the period is activated, the time of the beginning of the period has not come yet.
- **Completed** - the action of the blocking period is completed.
- **Blocked -** the period is added, but not activated in the settings (when the time comes for the period to start, person's pass key will not be blocked).
- **Active** - the time for blocking has come, person's pass keys are blocked.

Form "Organizational units"

Form structure "Organizational units" (*Fig.53*):

1 - "Update form" button;
2 - "Show/hide form" button;
3 - "Open form in full screen" button;
4 - "Assign persons to organizational units" buttons.

Fig.53 Adding person: Organizational units

A person can be assigned to one organizational unit only.

If a person is unassigned from the department, it is necessary to perform synchronization *(see section 3.3.10 Synchronization)* to reset access rights. After that, if necessary, new access rights can be set. After making changes to the access rights of a person, it is necessary to synchronize.

Form "Personal Access Settings"

"Personal Access Settings" from allows to set access rights to working are as for a particular user. There are three personal access settings available:

Everywhere (*Fig.54*) – specify what will be considered as a working area - not a single area or all the areas. Also, specify access rights - according to the schedule of the organizational unit (access settings are taken from the organizational unit access settings), never (no access to any working area), everywhere (there is access to any work area at any time);

Working areas*(Fig.56*) - specify what will be considered as a working area - not a single area or all the areas. Also, specify access rights - according to the schedule of the organizational unit (access settings are taken from the organizational unit access settings), on schedule (you can select necessary working areas and specify time zones for access), never (there is no access to any working area at any time), everywhere (there is access to any work area at any time);

Organizational unit *(Fig.55*) – all settings will be taken from the organizational unit settings (working area and access rights);

Form structure "Personal Access Settings"*(Fig.54*):

1. "Show/hide form" button;
2. "Open form in full screen" button.

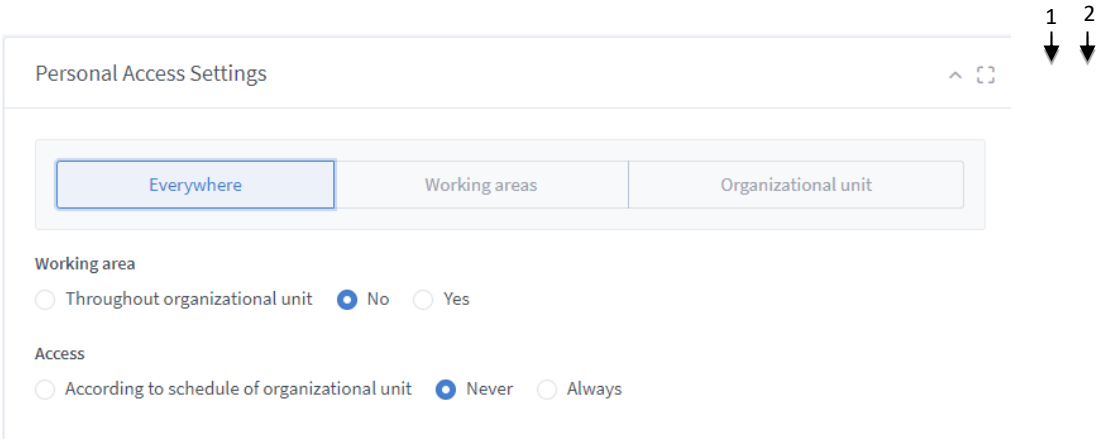


Fig.54 "Personal Access Settings": Everywhere

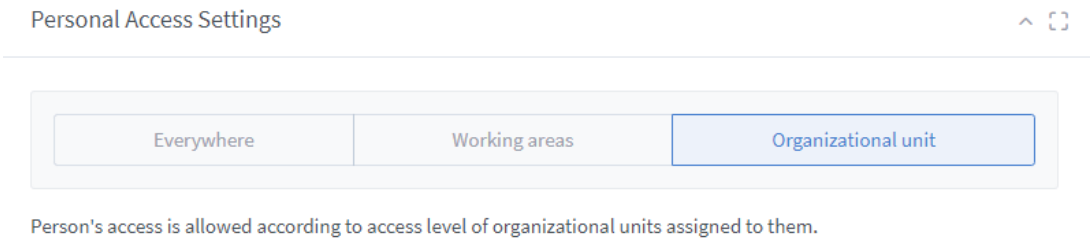


Fig.55 "Personal Access Settings": Organizational unit

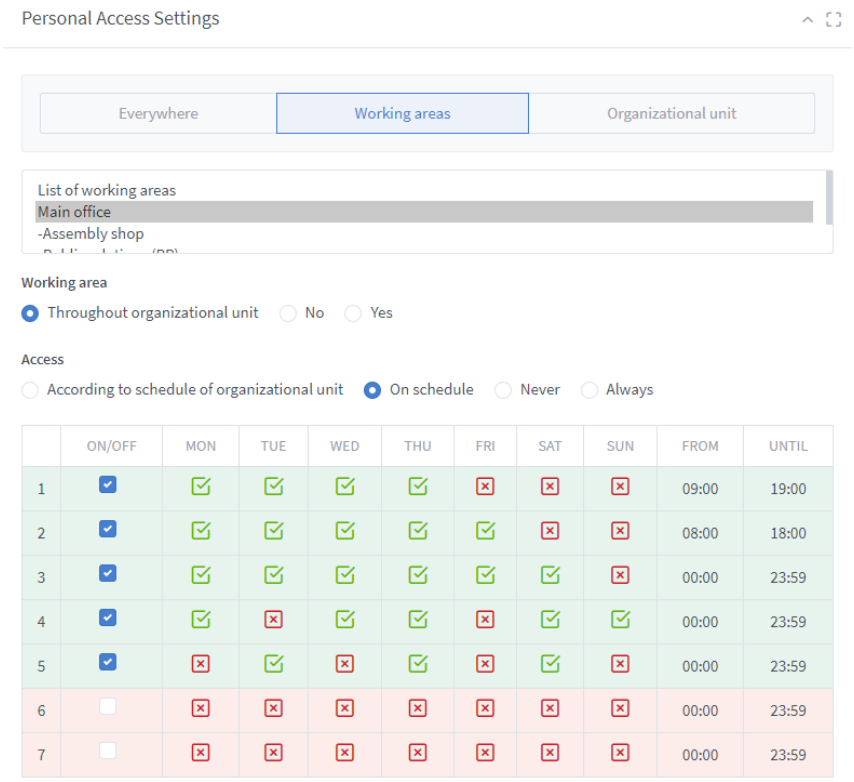


Fig.56 "Personal Access Settings": Working areas

Adding a person and saving information occurs after clicking "Save" button *(7 at Fig.50)*.

Edit person

Making changes to a person's profile (changing personal information, assigning pass key(s), assigning to an organizational unit, setting access rights) fully corresponds to the adding, but in order to edit, click "Edit" button (*Fig.49*) in the row of selected person.

Restore person

To restore a person, click the button "Restore person" *(13 in Fig.49),* and specify the reason for the restoring in the opened window, to confirm the action.

Person Changes History

To view the history of person changes, click the corresponding button *(12 in Fig.49)*. The "Person Changes History" window displays all person changes since creation *(Fig.57).*

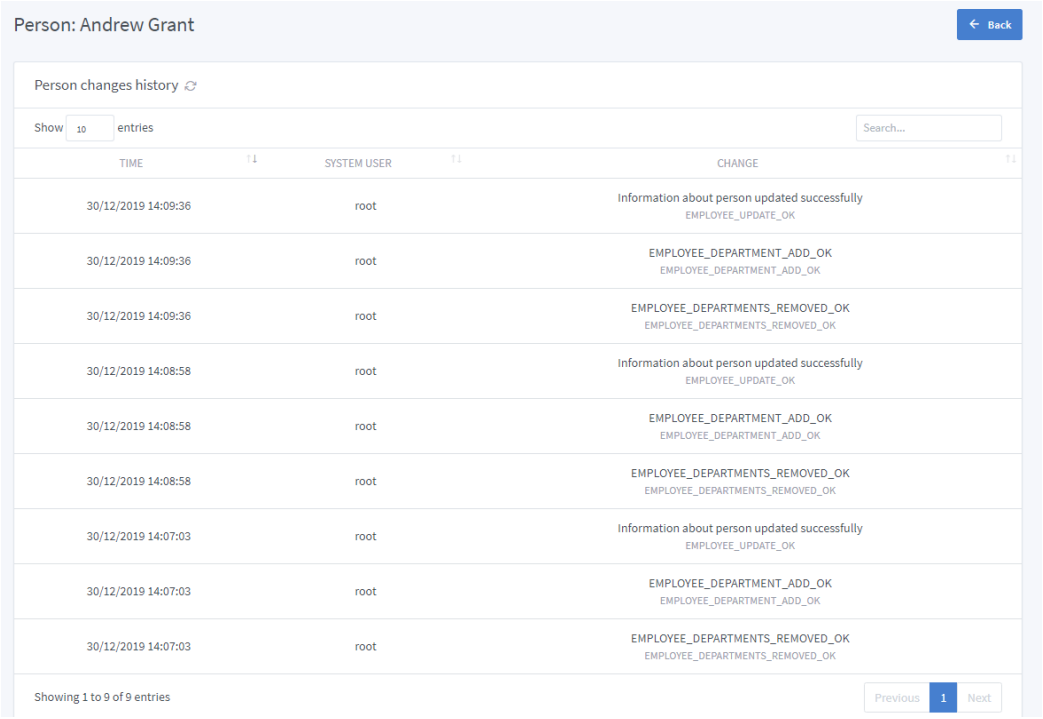


Fig.57 "Person Changes History" window

"Person Changes History" window structure *(Fig.57)*:

- events are displayed in a table with the following fields:
  - **TIME** – the time of a change;
  - **SYSTEM USER** – a user who was "in the system" at the time of the change;
  - **CHANGE** – a brief description of the result of the change;
- button to return to the list of employees.

Person Movement History

To view the person movement history, click the corresponding button *(11 in Fig.49)*. The "Person Movement History" window displays all recorded employee movements.

The display of events in this window corresponds to the display in the "Event log" *(see. Events log)*, but with the filter for a particular person.

3.3.5 Pass keys blocking mode

This mode provides the possibility to block pass keys for the period specified in the persons settings. A pass key can be blocked, for example, for the period of vacation or sick leave.

For the specified period, the person, whose pass keys are blocked, won't have access to the territory using their cards. In the report, all days of the blocking period are specified with the abbreviation of the reason for blocking. The reasons for blocking cards can be added by the user in the system settings.

To create a pass key blocking period, do the following:

1. Go to the person edit page.
2. On the “Pass keys blocking period” form, click the “add blocking period” button.

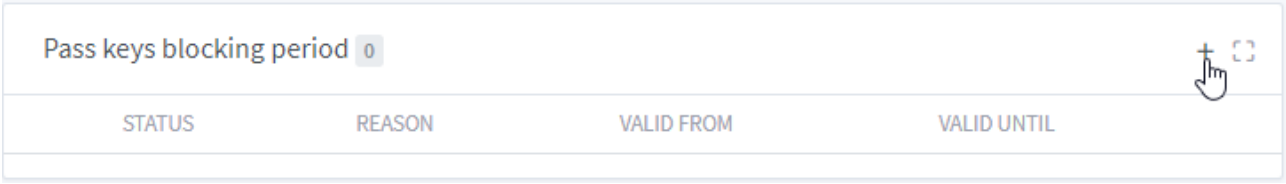


Fig.58 “Add blocking period” button

3. In the window “Add absence time” that opens, fill in the fields:
   - Reason (required) – choose the reason for blocking person’s pass keys from the list;
   - Valid from (required) – date and time when the blocking period starts;
   - Valid until (required) – date and time when the blocking period ends;
   - Activate – activation/deactivation of the period (If the period is not activated the pass key will not be blocked, when the period begins).
   - Display in the report - if the display of the blocking period in the report is on, all days of the period in the report will be marked with an abbreviation for the reason for the blocking.
4. Click the “Add” button in the “Add absence time” window.

To delete a pass key blocking period, do the following

- Click the “Delete” button in the period row.
- In the “Delete Period” window that opens, fill in the reason for deleting the period and click the “Delete” button.

3.3.6 Manage Pass Keys

This subsection allows to set and manage pass keys added to the system and also, add new ones.

“Manage Pass Keys” page structure *(Fig.59)*:

1 - “Add pass key” button (manually);
2 - “Update pass keys list” button;
3 - the number of entries displayed on one page;
4 - search field;
5 - pass keys list in the system is presented in the form of a table with fields:
   - **OWNER** – person’s full name who this pass key is assigned to, (if nothing is specified - a pass key is not assigned to anyone);
   - **NUMBER** – pass key number (a pass key number can be displayed in three formats at once: DALLAS, EM_MARINE, DECIMAL; the choice of pass key number formats for display is available in the system settings);
   - **TYPE**– pass key type;
   - **STATE** – pass key state (active / disabled/ deleted);

- **VALID FROM** – date and time when a pass key became valid;
- **VALID UNTIL** – pass key expiration date and time;
- **ACTIONS -**
  - – “Edit pass key” button;
  - – “View pass key event history” button;
  - – “Delete pass key” button;
  - – “Restore pass key” button.

On the top of page in the right corner situated buttons for extra sort:

a. all pass keys;
b. guest pass keys;
c. assigned pass keys;
d. unassigned pass keys;
e. inactive pass keys;
f. active pass keys;
g. deleted pass keys;

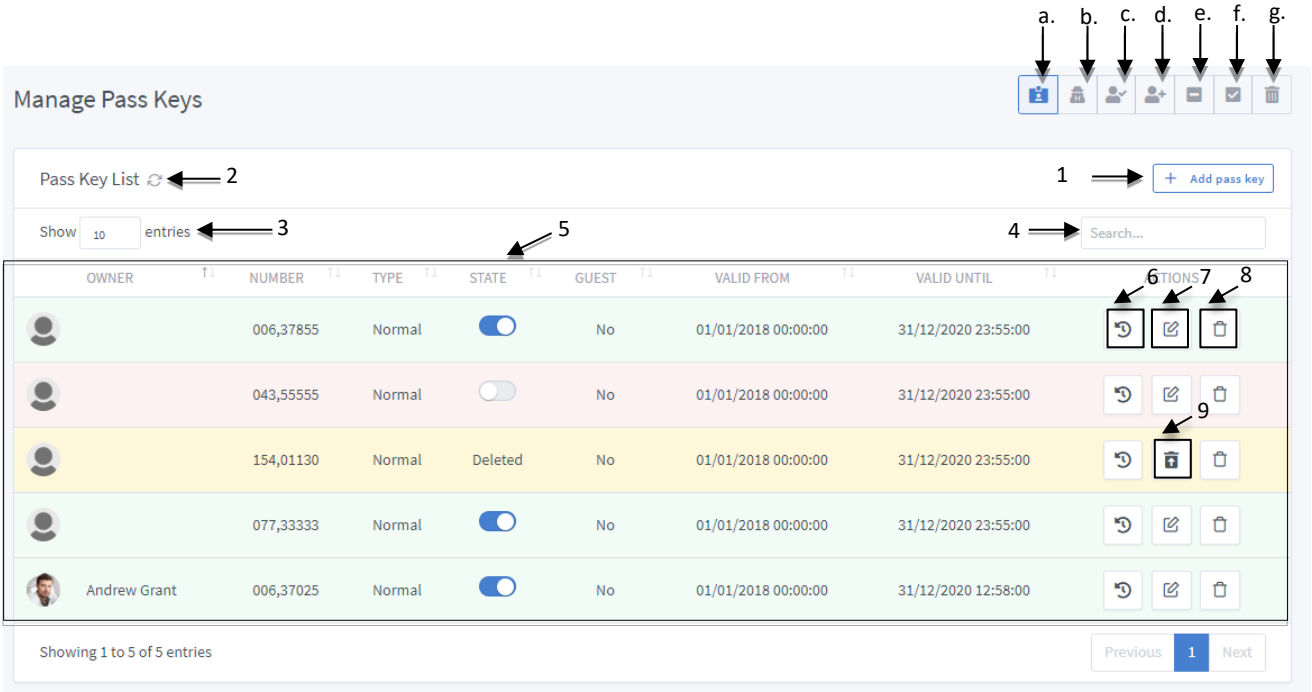


Fig.59 Page “Manage Pass Keys”

If pass key row is highlighted in green - pass key is active, in red - disabled, in yellow - deleted.

Automatic pass key adding

Automatic pass key adding is possible only if automatic pass key adding is enabled in the system settings. Default value: Enabled.

Automatic pass key adding to the system is via a controller. To add a pass key, you need to bring it to the reader of the controller, which is added to the system. After that, the pass key will be added to the system and displayed at the interface.

By default, the state of a pass key, which is added automatically, is active. (see section *3.4.1 System settings*). Also, it is possible to specify the validity period of a pass key, which is added automatically, in the system settings.

When adding a pass key automatically, the pass key will be added to the system with the DALLAS number format.

Add pass key (manually)

You can add a pass key manually from three pages - "Manage pass keys", "Add/edit person" and "Manage guest pass keys".

To add a pass key from “Manage pass keys” page do as follows:

1. Click “Add pass key” button *(1 at Fig.59)*, after that a window for adding a pass key will appear *(Fig.60)*.
2. Fill in required fields.
3. Check “Enabled” checkbox to activate a pass key.

Pass key number is a required field to fill in.
Pass key is considered invalid (you won’t be able to go through pass point using this card, even if access is granted) if validity period has not started or already expired, or if a pass key is disabled.

4. Check “Guest Pass Key” checkbox (if necessary).

If “Guest Pass Key” checkbox is checked, this pass key will be displayed at “Manage guest pass keys” page.

5. Click “Add” button to add a pass key *(1 at Fig.60)*.

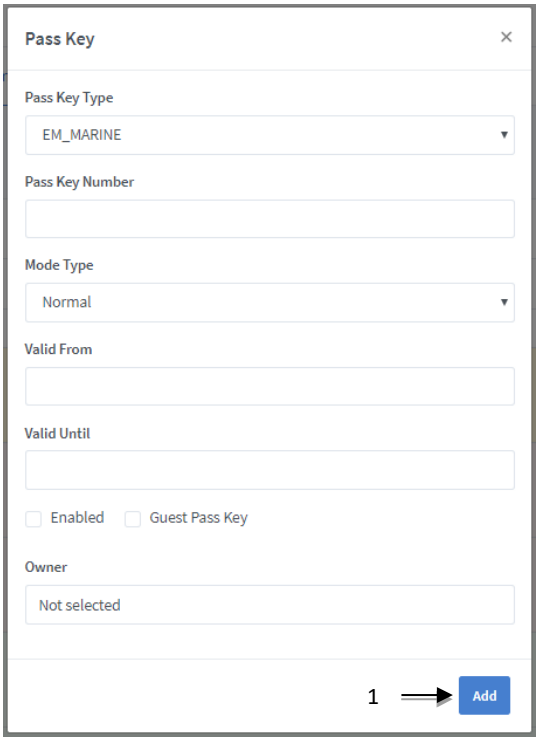


Fig.60 Page "Manage Pass Keys": Window "Adding pass key"

Adding a card from "Add/Edit Person" page requires all the above actions, the only difference is that there is no "Owner" field in the window *(Fig.61)*, because a pass key can be assigned directly in the profile of the person.

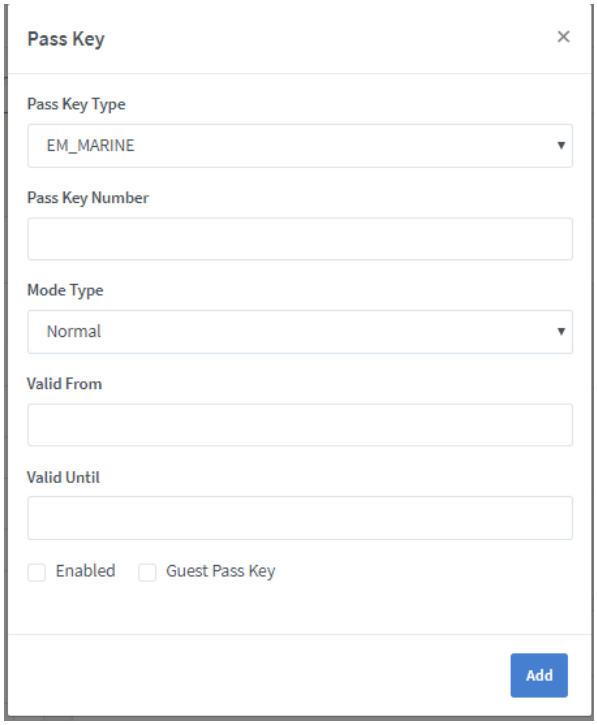


Fig.61Page "Add/Edit Person": Window "Adding pass key"

Edit pass key

Pass keys can be edited on two pages - "Manage Pass Keys" and "Add/Edit Person". On the "Manage Guest Pass Keys" page, you can only change pass key validity period, change the owner and set a pass key blocking when leaving the area *(see section 3.3.7Manage Guests Pass Keys).*

Editing a pass key requires the same actions as adding, but you need to click “Edit pass key” buttonat the corresponding page*(7 at Fig.59)*.

View events history

If necessary, you can view the history of events on each map. To do this, click the button in the column of the desired map *(6 at Fig.59).*

"Identifier`s event history” page structure *(Fig. 62):*

1 - identifier’s events history refresh button;

2 - button that returns to the “Manage Pass Keys" page;

3 - search field;

4 - event log is presented by the following columns:

- **TIME** - time of an event;
- **USER -** a user who is logged in during the event;
- **OWNER** - owner of an identifier (if an owner was assigned during the event);
- **ACTION -** description of an action.

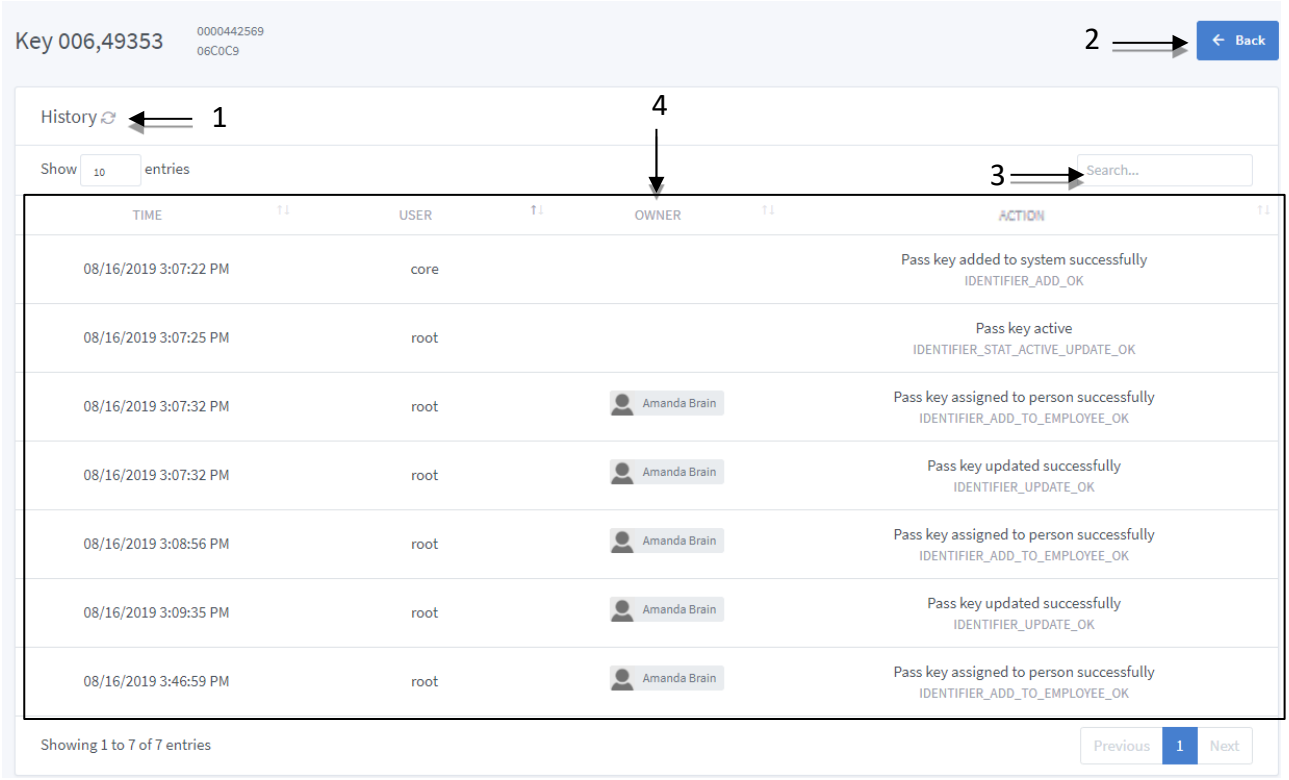


Fig. 62 Identifier`sevent history

Restore pass key

To restore a pass key, click the correspondent button (*9 at Fig.59)* and input a reason for restoring in the opened window *(Fig.63).*

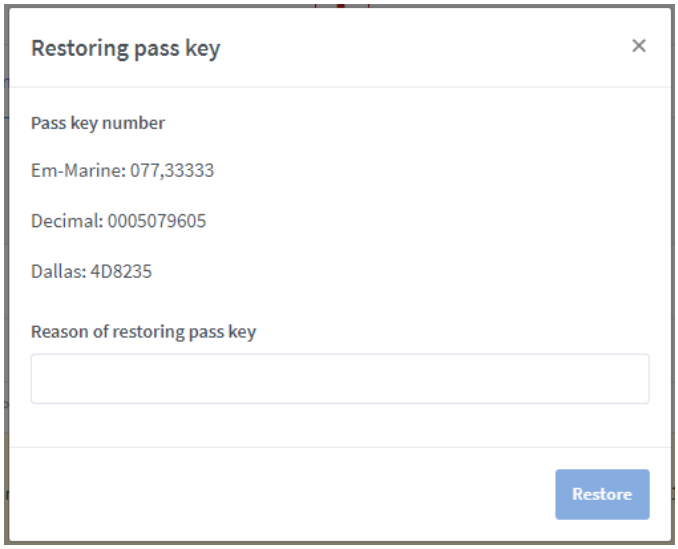


Fig.63Window: "Restore pass key"

Move pass key to "Deleted pass keys" list

To move a pass key to the deleted list, click the corresponding button *(8 in Fig.59).* The deleted pass key will be displayed in the list of pass keys with the status "Deleted". Later, it can be restored by clicking the "Restore" button *(9 in Fig.59).*

Delete pass key

To delete a pass key completely, do the following:

1. Move a pass key to the deleted list (see section above).
2. Click the "Delete" button *(8 in Fig.59),* as a result, a confirmation window appears.

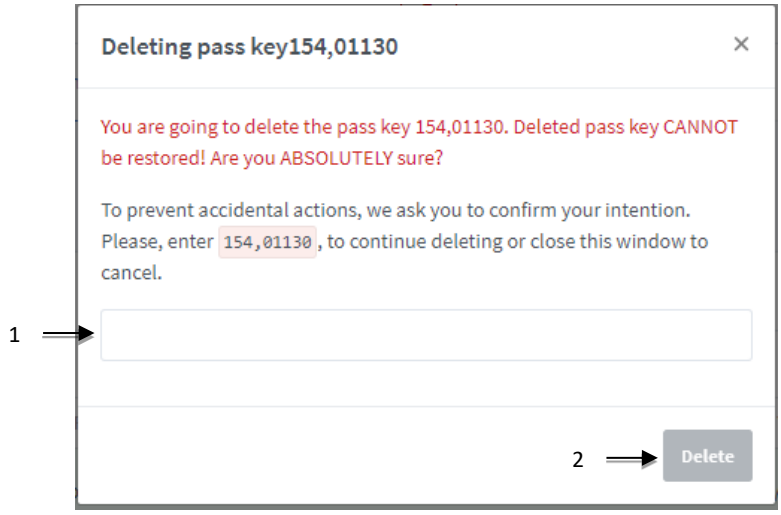


Fig. 64 Deleting pass key confirmation window

3. In the corresponding field *(1 in Fig. 64)* indicate the number of the card to be deleted in EM-Marine format. As a result, the delete button is activated *(2 in Fig. 64)*.

The identifier number is displayed only in EM-Marine format in the modal confirmation window for deleting a pass key, regardless of the formats selected for display in the system settings.

4. Confirm intentions clicking the button “Delete” *(2 in Fig. 64)*.

3.3.7 Manage Guests Pass Keys

This subsection allows to set and manage pass keys attached to guests (pass keys with checked “Guest Pass Key” checkbox).

“Manage Guest Pass Keys” page structure *(Fig.65):*

1 - “Update guest pass keys list” button;
2 - guest pass key list;
3 - “Add guest pass key” button;
4 - search field;
5 - “Edit pass key” button;
6 - “Take pass key away from guest” button;
7 - “Issue a guest pass key to a person” button;
8 - “Issue a guest pass key to a guest” button;
9 - filter for guest pass keys:

 – display all guest pass keys;

 – display assigned guest pass keys;

 – display unassigned guest pass keys.

10 - pages navigation buttons:

- Previous – navigate to previous page;
- Next – navigate to next page.

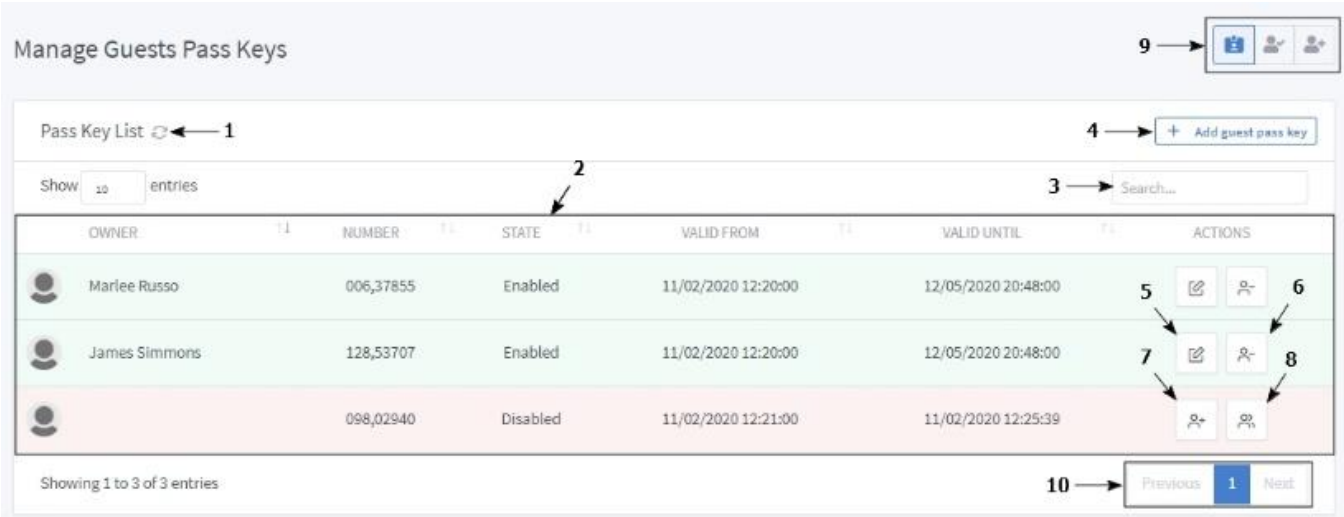


Fig.65 Page “Manage Guest Pass Keys”

Add guest pass key

To add a guest pass key click“ Add guest pass key” button*(3 at Fig.65)*. After that a window for adding will open*(Fig.66)*:

1 - pass key type
2 - pass key number
3 - “Add pass key” button

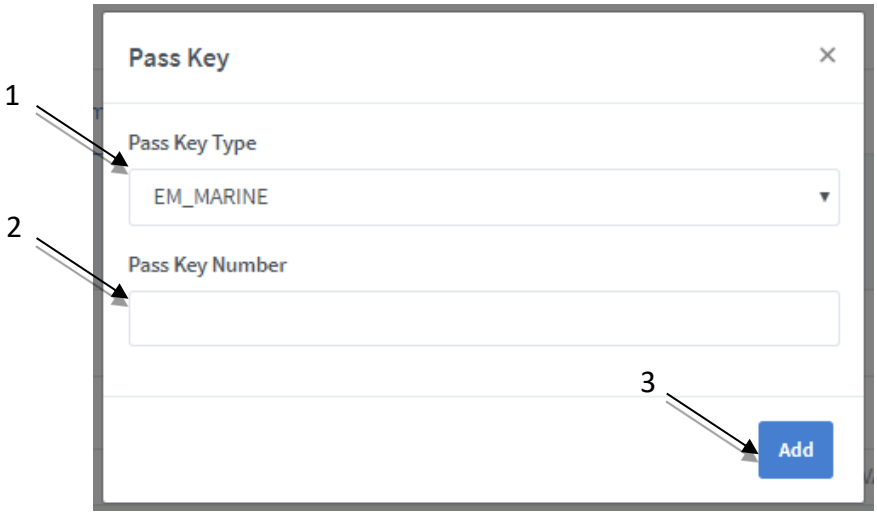


Fig.66 Window for adding a pass key

After a pass key adding, its state is disabled *(1 at Fig.67).* On the "Manage guest pass keys" page, pass key is activated only when it is issued to an owner and deactivated when a pass key is detached from an owner.

If necessary, a pass key can be activated/deactivated on "Manage Pass Keys" page *(see section "Manage pass keys" Fig.59).*

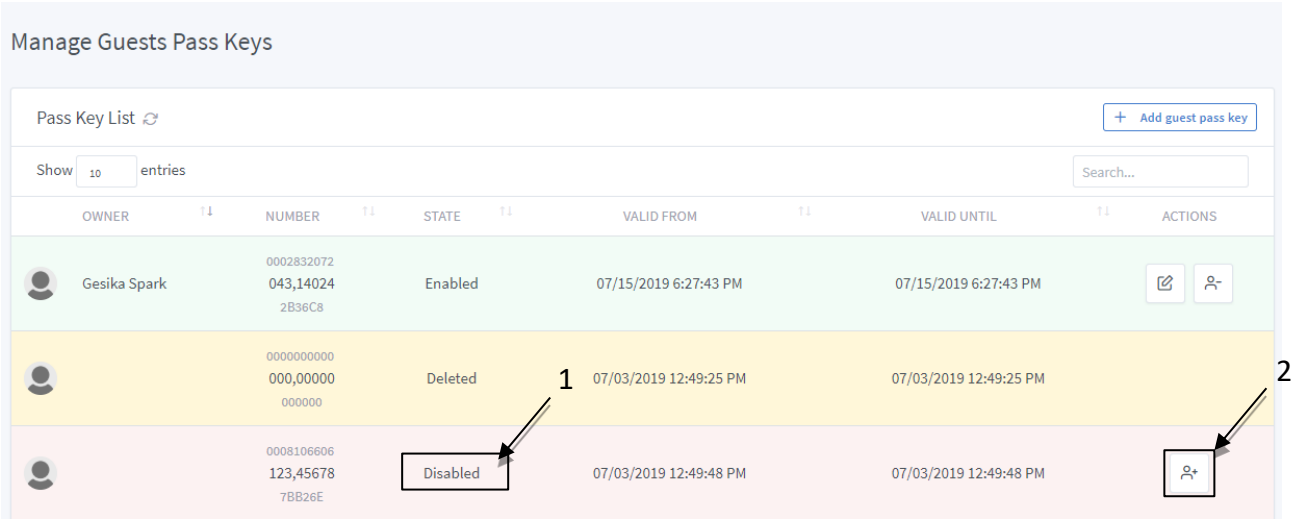


Fig.67 Added pass key state "Disabled"

By default, the "Issue pass key" button is not active. Activation occurs only after selecting the owner from the guest list or the list of persons *(1 at Fig.69)* or filling in the required name field, when adding manually (adding the owner manually is only available when issuing a card to a guest) *(1 at Fig.70).*

If pass key row is highlighted in green - pass key is active, in red - disabled, in yellow - deleted.

Issuing a guest pass key to a person

To issue a pass key, do the following:

1. Click the “Issue a guest pass key to a person” button (7 in *Fig.65*).
2. In the window "Card Issuance”, choose the cardholder from the list of persons (1 in *Fig.68*).
3. Set the validity period of the guest pass key from/till (2, 3 in *Fig.68*).
4. If necessary, set the flag “Block when leaving the zone” (4 in *Fig.68*), which activates the pass key blocking in case of passing through the zero pass point (see section *3.3.2 Set pass points*).
5. Click the “Issue pass key” button.

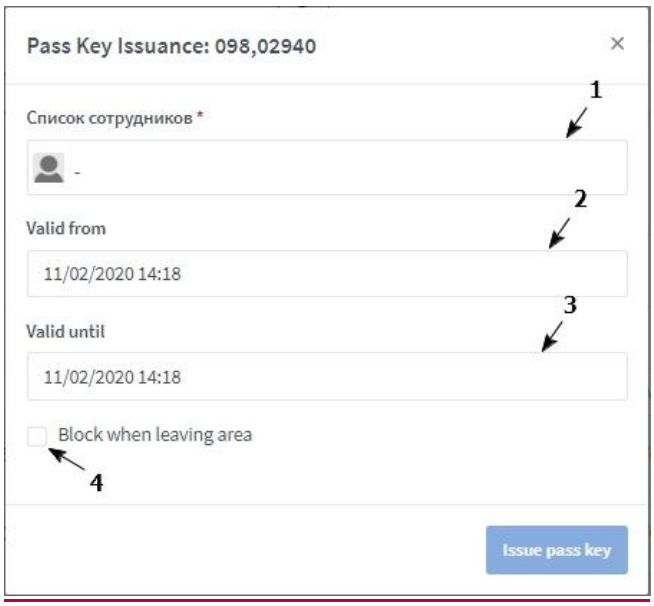


Fig.68 **Window "Pass Key Issuance”**

Issuing a pass key to a guest

To issue a pass key to a guest click “Issue a pass key to a guest” button*(2 at Fig.67)*. There two ways to issue a pass key to a guest:

Select a guest from a drop-down list, which displays all the guests already added to the system:

- In **“Pass Key Issuance”** window that will open, select a guest from the list *(1 at Fig.69)*
- Set a pass key validity period: from/until *(2,3 at Fig.70)*
- If necessary, check “Block when leaving the area” checkbox (this checked checkbox activates pass key blocking immediately after the guest leaves the working area where the access has been granted)
- Click “Issue pass key” button

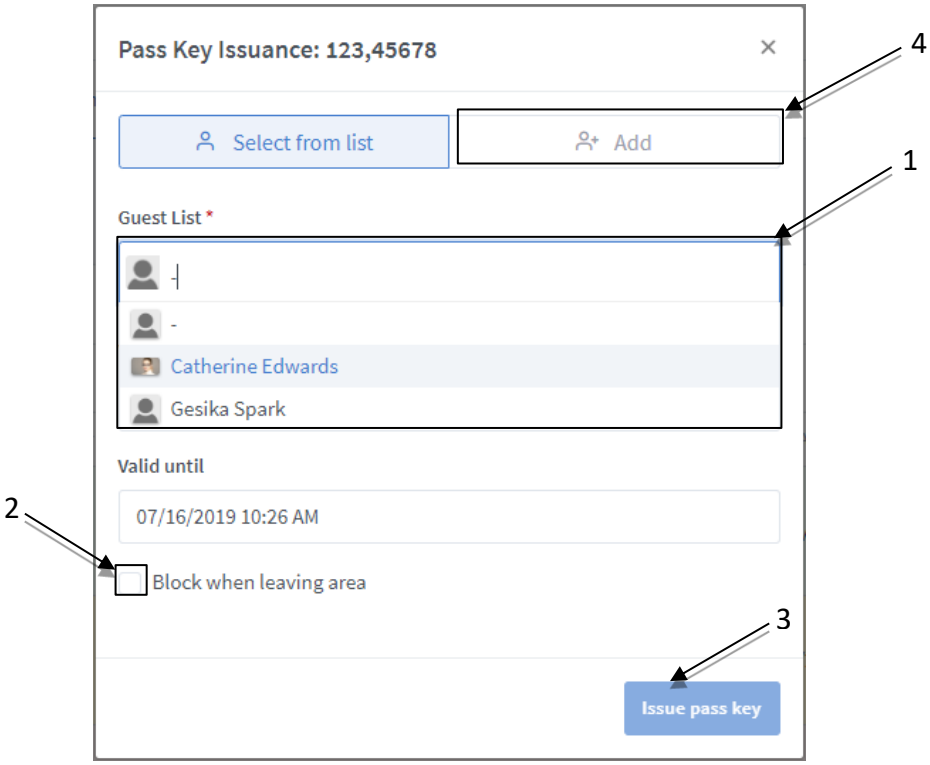


Fig.69 Issuing a pass key to a guest

Add a guest manually if the guest is not in the system*(4 at the Fig.69)*

requires the same actions as when selecting a guest from the drop-down list, only in this option you need to specify the name of a guest who is issued a pass key*(1 at Fig.70)*

Fig.70 Add guest manually

Edit and return a guest pass key

To edit pass key information, click “Edit information”*(see 5 at Fig.65)*. Window for editing information will open*(Fig.71)*.

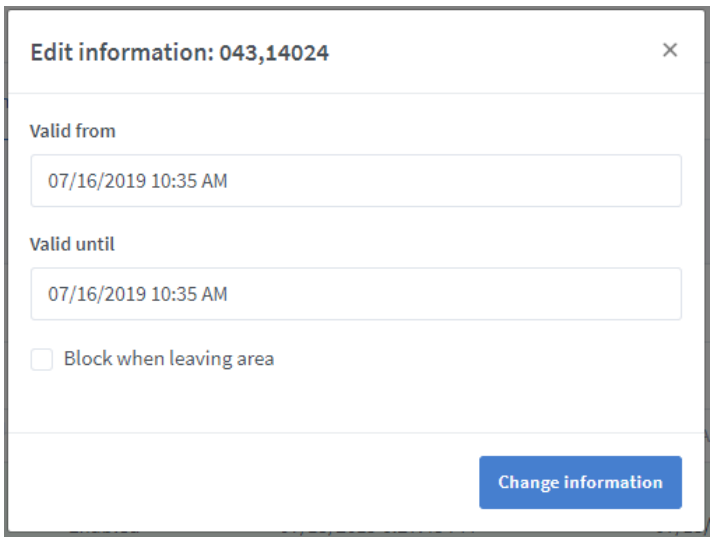


Fig.71 Window “Edit information”

In order to confirm that the pass key has been returned, click “Return pass key” button*(see 6 at Fig.65)*. To confirm the action, click “Confirm pass key return” button*(1 at Fig.72)*.

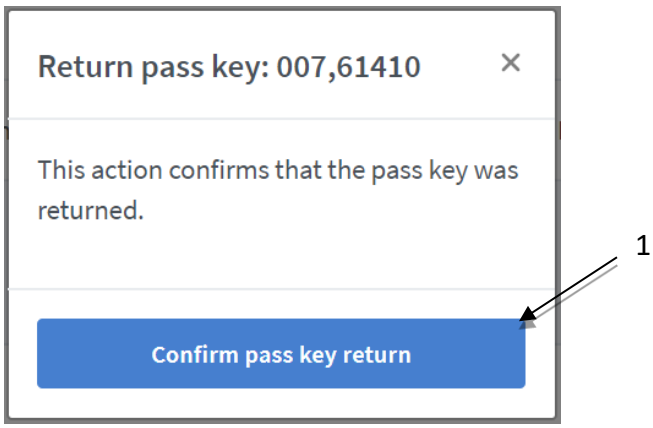


Fig.72 Confirm pass key return

3.3.8 Reports

This subsection allows to obtain and download reports on the actual presence of persons at their workplaces, the movement of persons and guests etc. Settings for reports are set at the discretion of the system user.

Receiving a report is not possible if persons are not in the database. If there are no persons in the database, then the system will ignore the request for the report and will give an error.

Reports can be represented in three ways:

- **Timesheet** – displays information about the time spent in the territory where the Physical Access Control System (PACS) is installed for the specified period (*Fig.73*). A timesheet report may contain the following information:
  - coming and leaving;
  - reporting time (time spent on the territory);
  - lateness;
  - early coming/leaving;
  - working fewer/extra hours;
  - money to pay according to a rate.

Timesheet can be presented in the form of a table "Timesheet" and in the form of charts.

- **Movements**– it contains information about the movements of all employees during the reporting period. (*Fig.77*).
- **Traffic** – allows you to track the number of events (entrances/exits) for each working area (*Fig.78*).

"Reports: Timesheet" page structure *(Fig.73)*:

1 - "View page in full screen" button;
2 - report period selection area;
3 - report type selection: timesheet, movement or traffic;
4 - Organizational units on which reports are formed;
5 - The "Persons" filter exists to generate reports for one or more employees (by default, the filter value is "Everybody").
6 - Select the type of rate calculation (by default, without rate calculation):

- **Without rate calculation** – a report is without rate calculation.
- **General rate calculation** – the general rate is specified by the user on the "Reports" page, right before the report is generated. After selecting the "General rate calculation" the input field on the "Reports" page appears.

The general rate applies to all persons for whom a report is generated, regardless of their personal settings, as well as the settings of work areas.

- **Personal rate calculation** – personal rate is specified in the persons settings.

- **Working area rate calculation** – working area rate is indicated in its settings. When generating a working area rate report, the rate of the working area and time spent by the person in this area are calculated.

Working area rate calculation is carried out only with the following settings:

- option “Apply working areas” is active;
- option “Apply lunchtime” is not active.

To do working area rate calculation, time spent in an area is calculated strictly (applied the time range between the nearest enter and exit throughout one area).

7 - enable/disable the option “Apply working areas” (yes/no):

- Applying working areas – only the time spent in the areas which indicated in access settings for the exact person as working areas is calculated;
- Not applying working areas – time spent in all areas is calculated.

8 - enable/disable the option “Apply remote persons”:

- no (by default) – remote persons are not displayed in reports, as well as in the filter list “Persons” (5 in *Fig.73*);
- yes – remote persons are displayed in reports, as well as in the filter list “Persons”.

9 - enable/disable the option “Apply lunchtime”:

- no (by default) – when generating a report, the calculation is made without applying lunchtime specified in the Organizational unit settings.
- yes – the calculation is made applying lunchtime.

The option “Apply lunchtime” cannot be applied to reports in the following cases:

- Option “Apply working areas” is active;
- Working area rate calculation is selected.

10 - buttons for controlling the visibility of report fields in “Timesheet”. The number of available fields to display in the report depends on the value of the “Organizational units" filter:

- All organizational units – coming, leaving, strict, flexible;
- One exact organizational unit – coming, leaving, strict, flexible, working fewer hours, working extra hours, lateness, early leaving, event filter for reports on working areas;

11 - report display area;
12 - “Generate report” button;
13 - “Download report” button (reports are downloaded in * .xlsx);
14 - event filter for report by work zones;
15 - event filter for report by controllers;
16 - show/hide filters button;
17 - “Generate chart” button;

18 - «Report by entities» button.

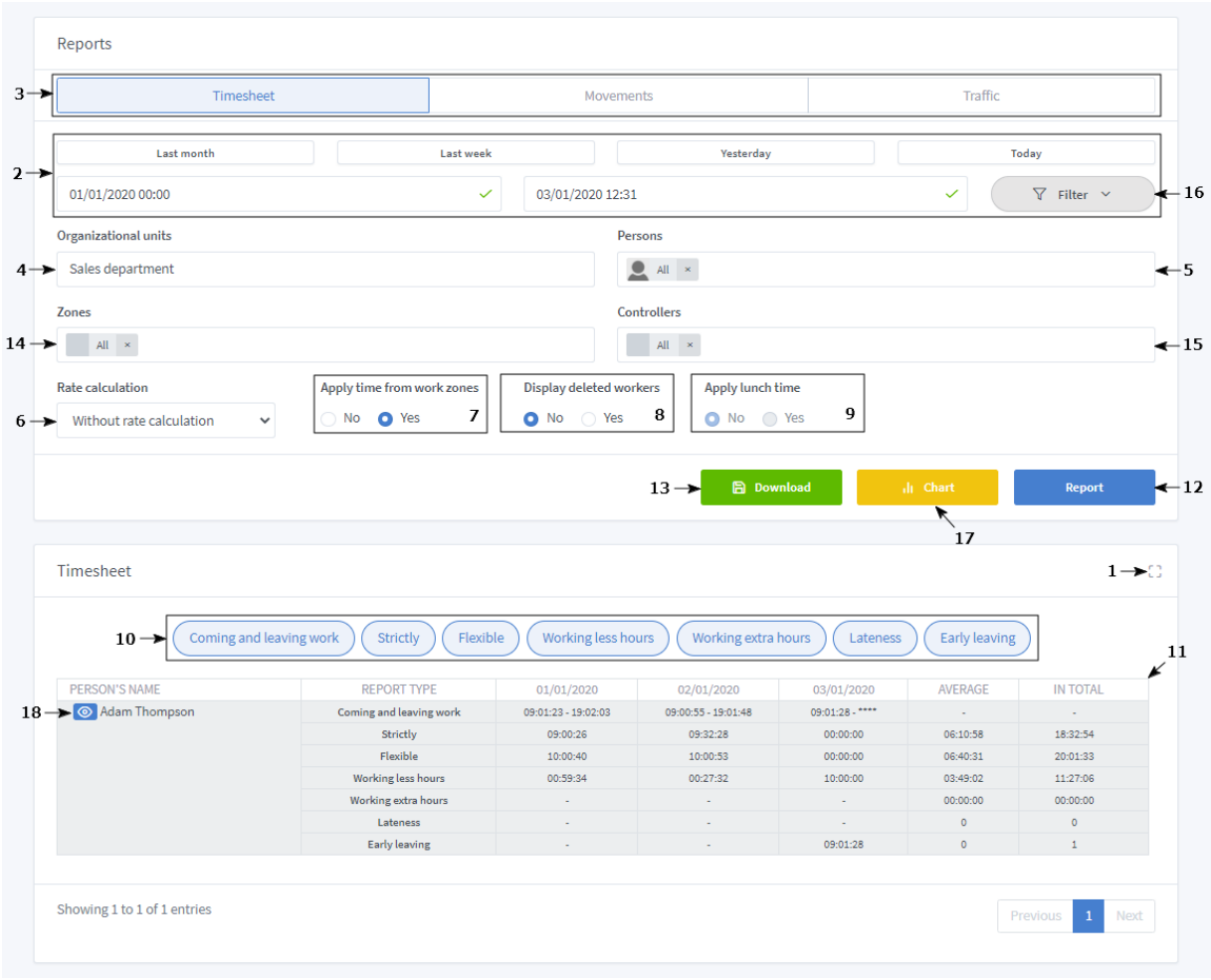


Fig.73 Page "Reports: Timesheet "

The format for displaying a report of the "Timesheet" type is configured using the buttons on the control panel for the visibility of report fields (7 in Fig. 70). A report of this type may contain the following fields:

- **Coming and leaving** – person coming and leaving are displayed (determined by the last events);
- **Strict** – hours worked per day (determined by the range of events from the first entry to the last person exit, for each day);
- **Flexible** - time worked per day (determined by the range of events from the first and last detection of a person pass key for each day, regardless of the type of event).
- **Working less hours** – negative difference between the specified and the actual work time;
- **Working extra hours** – positive difference between the specified and the actual work time;
- **Lateness** – person's arrival time (indicated when the arrival is recorded after the beginning of a work day);
- **Early leaving** – person's departure time (indicated when the departure is recorded before the end of a work day);

When calculating the time strictly, with the setting “Considering working areas”, the time range between the nearest enter and exit recorded in the same zone is counted.

When calculating “Time Sheet” report, “Key found, door unlocked” are the only events about persons that are taken into account *(see section3.1.3 “Events log”)*.

In case of “All Organizational Units” setting *(see 4 at Fig.73)* - all persons who are in the system will be displayed in reports.

If there are no events connected with a person during current period of time recorded, this will be displayed in a report with empty fields.

To display information in the report correctly, when changing a time zone on a device where the program is open, you should reload the page in a browser.

The correct calculation of values for reports on night shifts is made only for a period multiple of days (day/two/three). When choosing a period that is not a multiple of days, the calculation may not correspond to the real values.

Timesheet: report by working areas

A report by working areas (*Fig.74*) contains information on the time spent by a person in each area separately by day. The time in the report by working areas is calculated according to the “strict” type (only comings and leavings are calculated). The window for viewing the report by working areas is opened by clicking the button (18 in *Fig.73*).

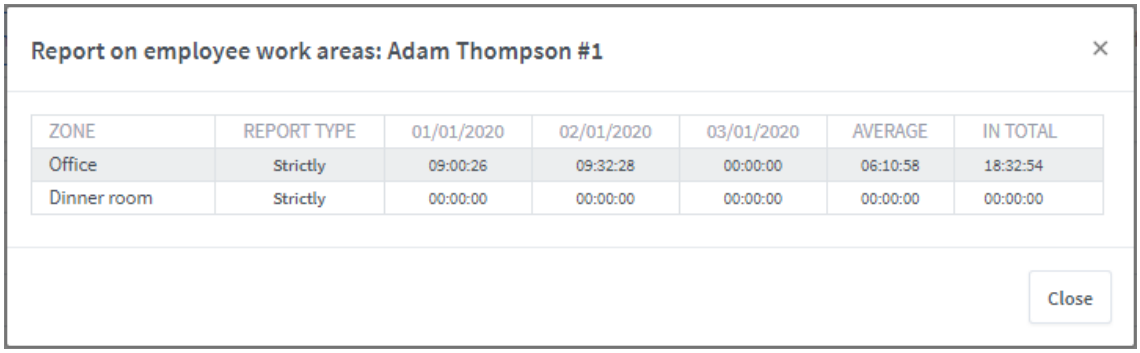


Fig.74 **Report by working areas**

Charts

A chart in the Guard Plus system is a graphical representation of a report of the "Timesheet" type. There are two chart types: by entities and coming/leaving chart.

Report filter options that affect chart generation:

- Period - for charts, only the date calculated. For example, if you specify the period from 01.02.2020 12:10 until 10.02.2020 00:01, all events from 01.02.2020 00:00 until 11.02.2020 00:00 will be calculated for the chart.

- “Apply working areas” option – if the option “Apply working areas” is enabled, then the time, which is displayed on charts, is taken from the working areas which are working places for the person. Otherwise, the time is displayed by all areas.
- Organizational units – when choosing a specific organizational unit, the schedule is generated only for persons of the selected organizational unit.
- Persons – a schedule is generated only for selected persons.
- Working areas – only the areas indicated in the filter will be displayed on the chart.
- Controllers – to build a chart, only events on the controllers specified in the filter will be calculated.

The chart by entities shows the time spent in each area separately for one day for one person. The “All zones” column displays the gap between the first and last events. Organizational unit schedule, to which the employee is assigned, is displayed on the chart in the form of vertical lines indicating the time above the schedule, which allows you to visually track lateness and early leavings.

The chart page contains the following elements (*Fig.75*)**:**

1 - field to select a person;

2 - area to select a day;

3 - chart display area;

4 - chart view button in full screen mode.

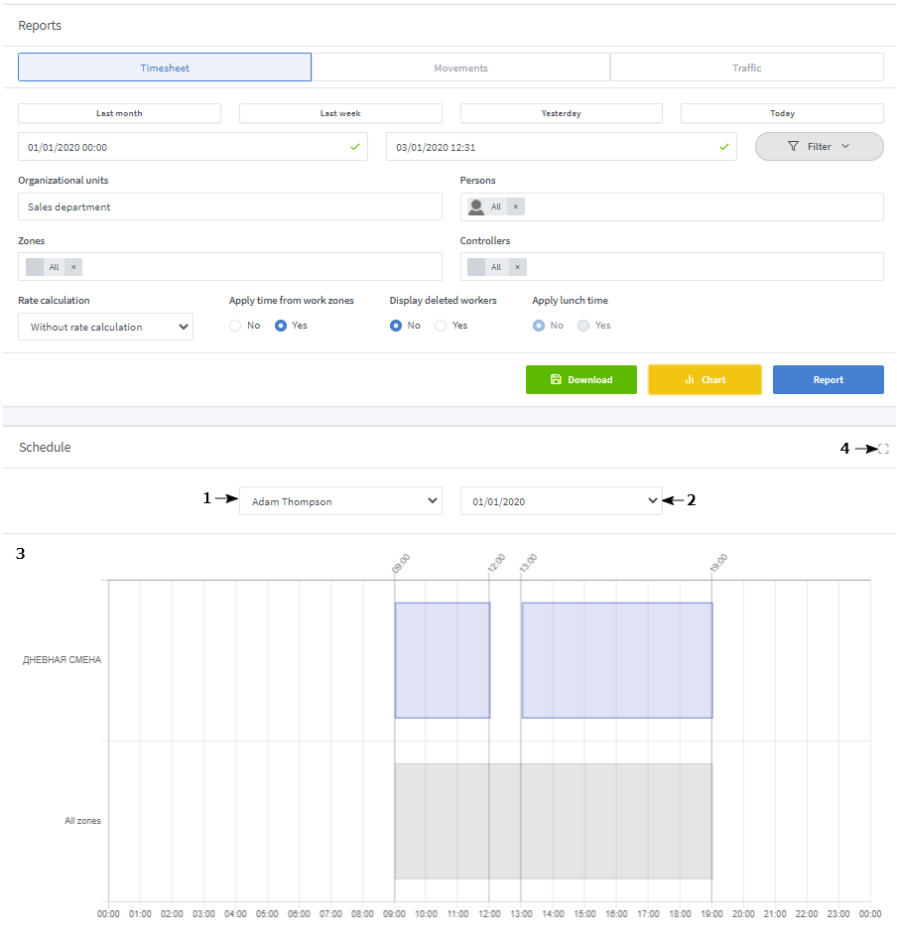


Fig.75 Reports: chart

Coming and leaving chart displays the arrival and departure range for the selected period, the range from the latest arrival to the earliest departure is considered to be the working range.

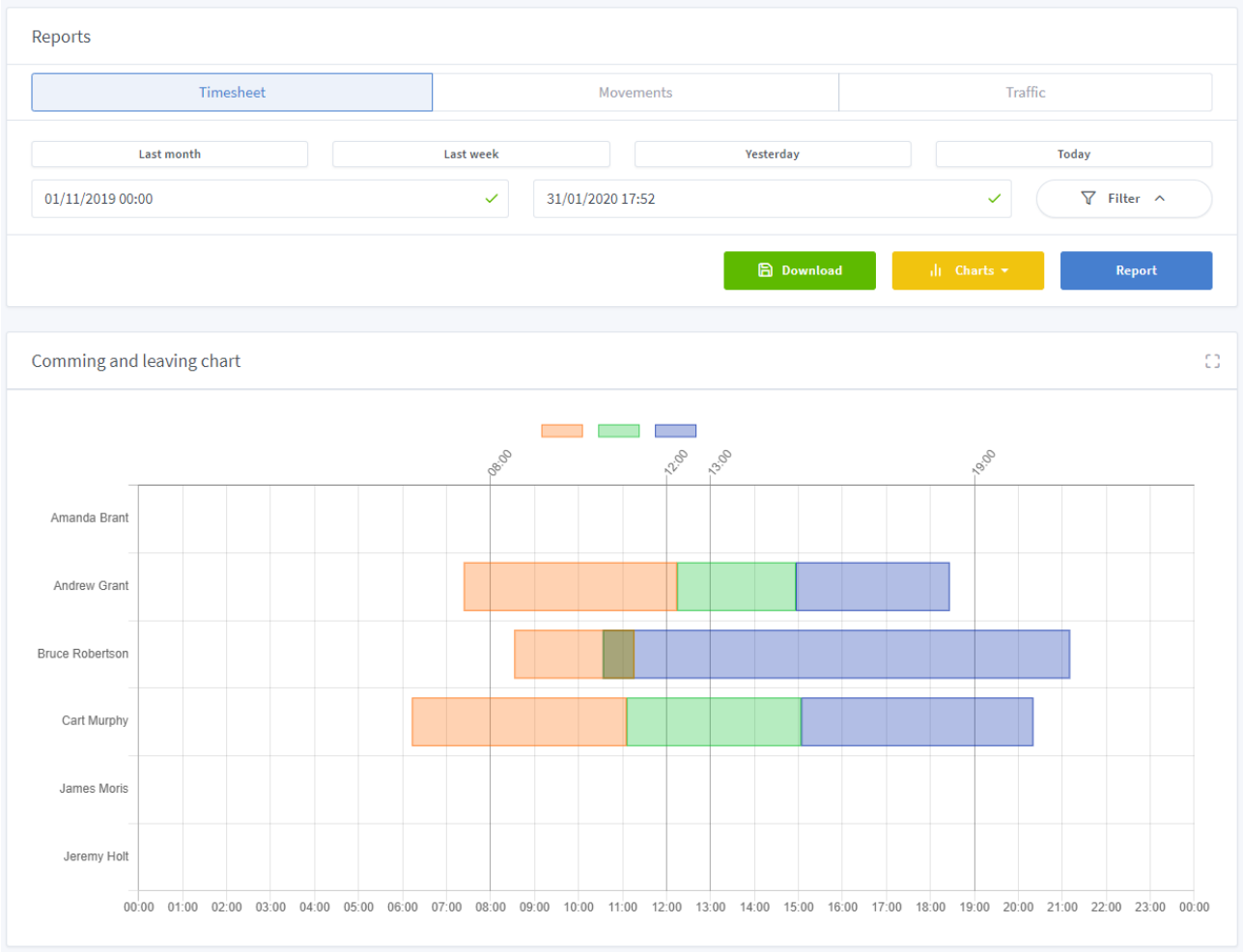


***Fig.76 Reports*: Coming and leaving chart**

If there is an overlap of ranges, it is recommended to enable/disable the legend: click on the name of the range that you want to disable (the legend is placed above the chart).

Tab structure "Reports: Movements" *(Fig.77):*

Person's movements are presented in a list with the following parameters:

- **TIME** – date and time of an event;
- **CONTROLLER** – controller ID-number, which recorded an event;
- **ENTRANCE/EXIT** - to/from where an event is recorded;
- **PASS KEY** - identification number recorded by a controller;
- **STATUS**- description of an event;
- **FULL NAME** – full name of a person;
- **SHORT NAME** - short name of a person.

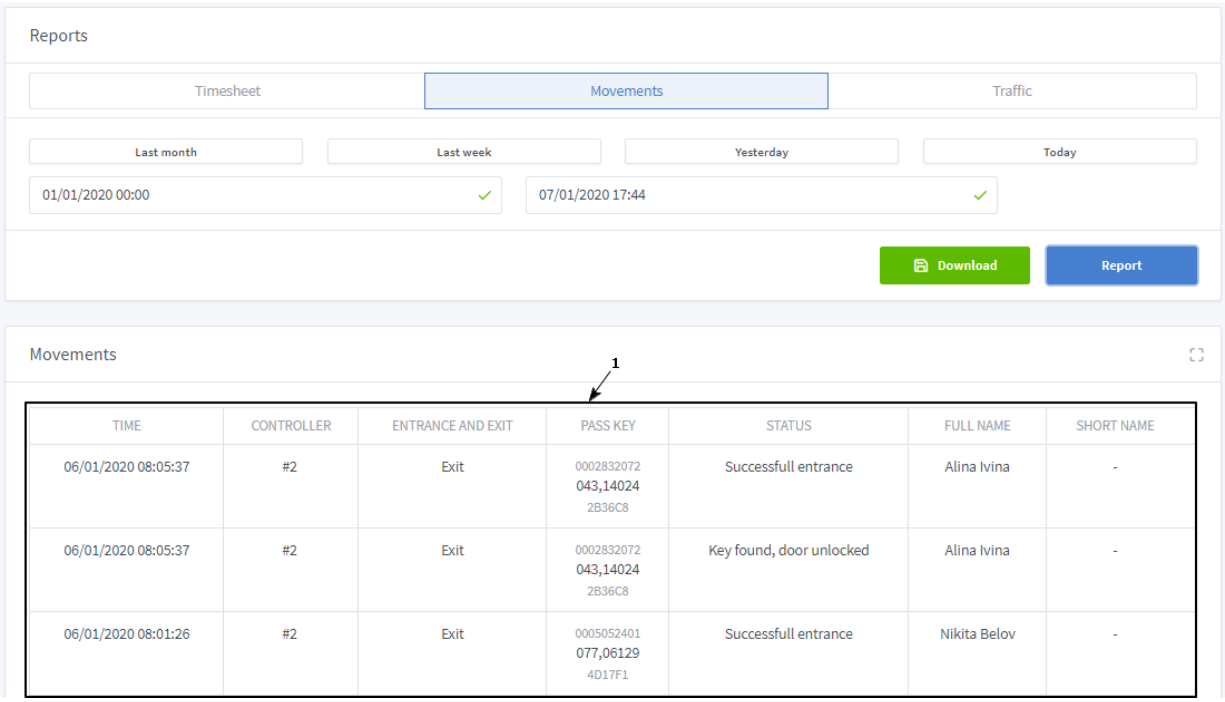


Fig.77Reports: Movements

Tab structure "Reports: Traffic" *(Fig.78):*

1 - traffic is presented in a list with the following parameters:

- **WORKING AREA** – working area on which events are displayed;
- **ENTRANCE** – events with the direction entrance;
- **EXIT** – events with the direction of exit;
- **BUTTON** – events that are displayed after pressing the button.

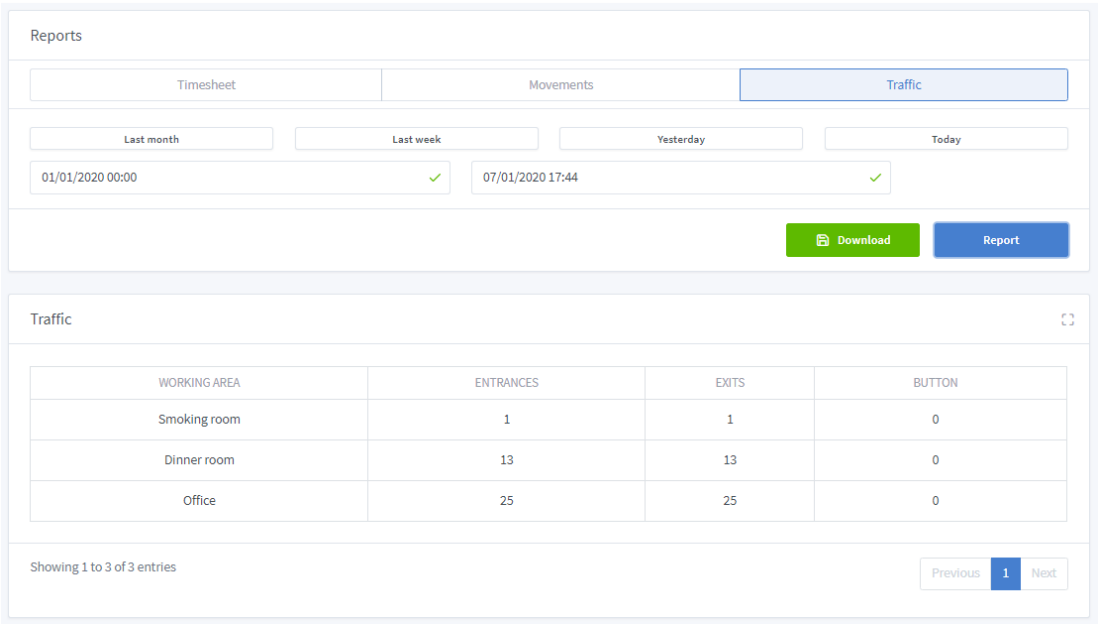


Fig.78 Reports: Traffic

To display the report, first, you should specify the period and type of report. After selecting the report options, click the "Report" button. *(7 in Fig.63).*

3.3.9 Access map

This subsection displays access information of all persons and guests, including those who added in the system in working areas.

“Users access map” page structure *(Fig.79):*

1 - user information display area:

- Full and short name;
- Position;
- Pass keys number assigned to the user;
- Access type (displays if tab “Everywhere” is set);

2 - display area access settings to all groups of controllers for the user with an indication of the time zone;

3 - “Generate access map” button.

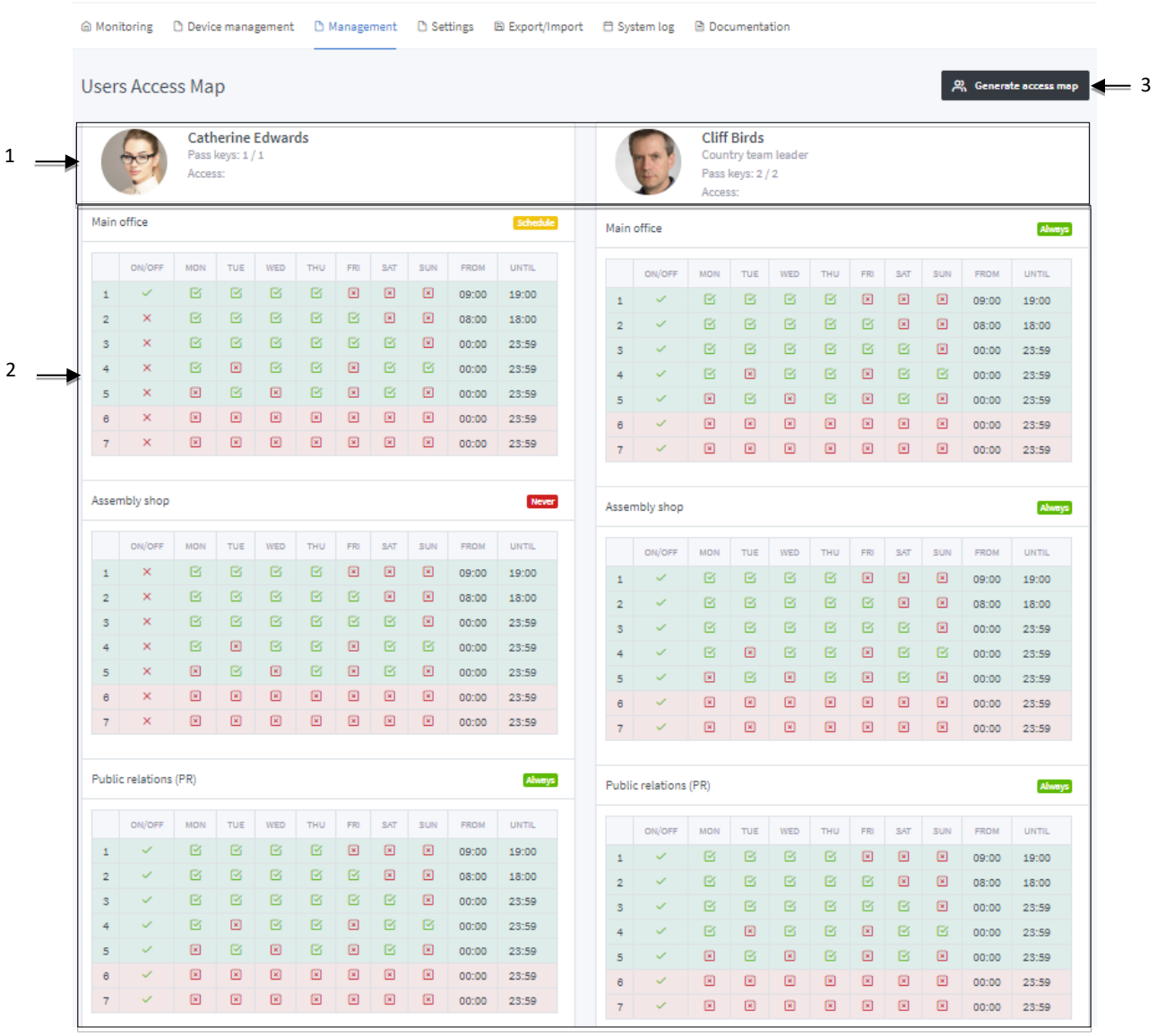


Fig.79 Page “Users Access Map"

3.3.10 Synchronization

This page allows to synchronize schedules, pass keys and access rights throughout all controllers (which are located in working areas). Synchronization is an update and saving of the changes made in the settings of the controllers, regarding persons' access.

With a large number of persons, the status of the synchronization process is displayed with a slight delay. It is necessary to press the synchronization button once (see 1 in Fig. 71) and wait for the process to complete.

"Synchronization" page structure *(Fig.80)*:

1 - "Start Synchronization" button;

2 - Synchronization progress status bar;

3 - Working area name (in which controllers are combined).

4 - Information about the controllers that are included in the working area:

- Controller name;
- Controller serial number;
- Controller state;
- Synchronization stages and their progress status.

5 - the button opens the "Event List" window, for viewing the list of tasks (by identifiers) for writing to a controller (displayed only when the "Automatic synchronization pass keys to controller" option is enabled *(see section 3.4.1 "System Settings")*).

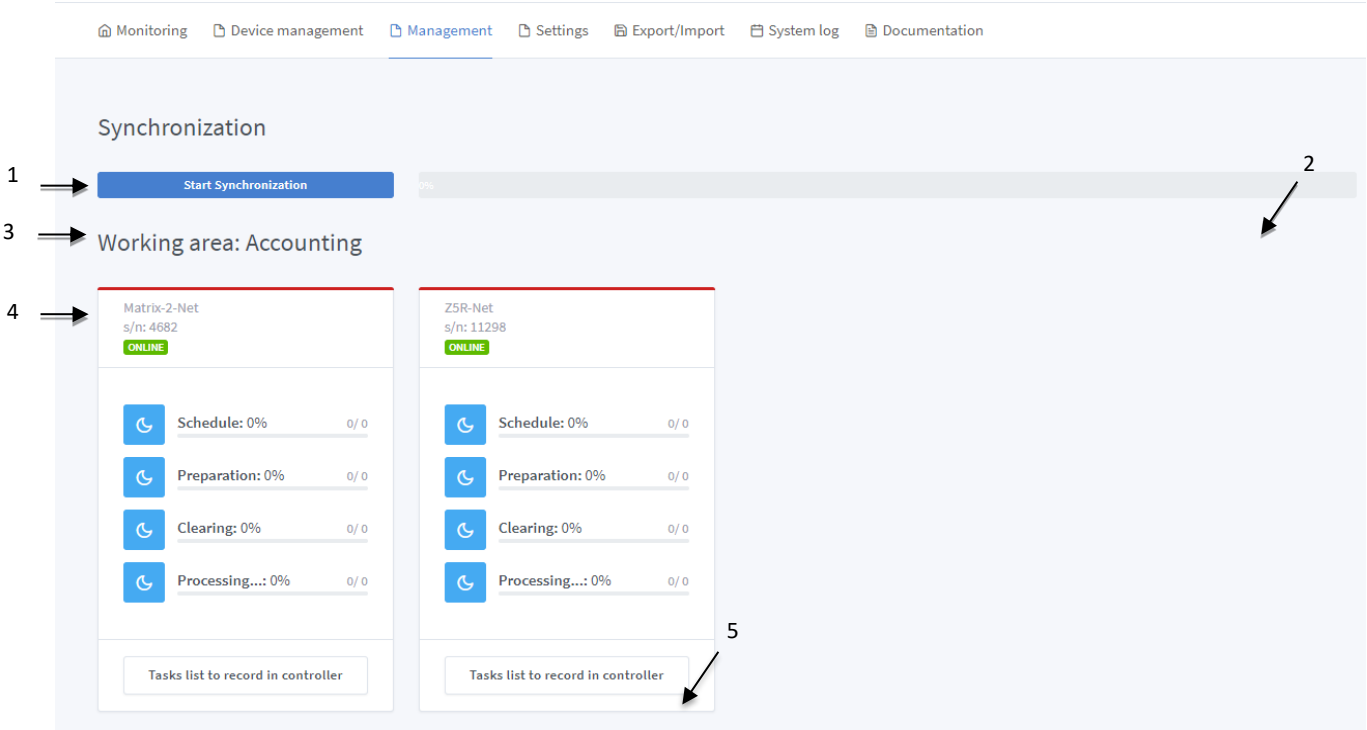


Fig.80Page "Synchronization"

Page structure "Event list" *(Fig. 81):*

1 – the number of displayed events at one page**;**

2,5 – button that closes the window;

3 – event list presented with the following fields:

- **ADDING TIME** - time when according to an identifier an event occurred;
- **ACCESS TYPE** - shows pass key type;
- **STATE –** displays two parameters:
    - **block -** yes: in case of un assigning a pass key from an owner, pass key deactivation (disablement or expiration)/no;
    - **delete -** yes: in case of deleting a pass key from a controller)/no;
- **PASS KEY** - identifier by which an event occurred;
- **ACTIONS** - button that deletes events from a list (in case of deleting this event will not be written to controller's memory) *(4 at Fig. 81)*.

Fig. 81Window: Event list

This window displays a list of events that should be written to controller's memory.

If there is no connection with the controller, but the controller is assigned to the working area, a list of tasks for writing to memory is collected on it, and when the connection is restored, all identifiers data will be updated.

For each identifier (by which an event occurred), the last event is added to the list for writing.

3.4 Settings

Settings menu includes two sections: "System settings" and "Backup".

3.4.1 System settings

This page is for general system settings.

“System settings” page structure *(Fig.82)*:

1 - “System settings default” button;

2 - setting area.

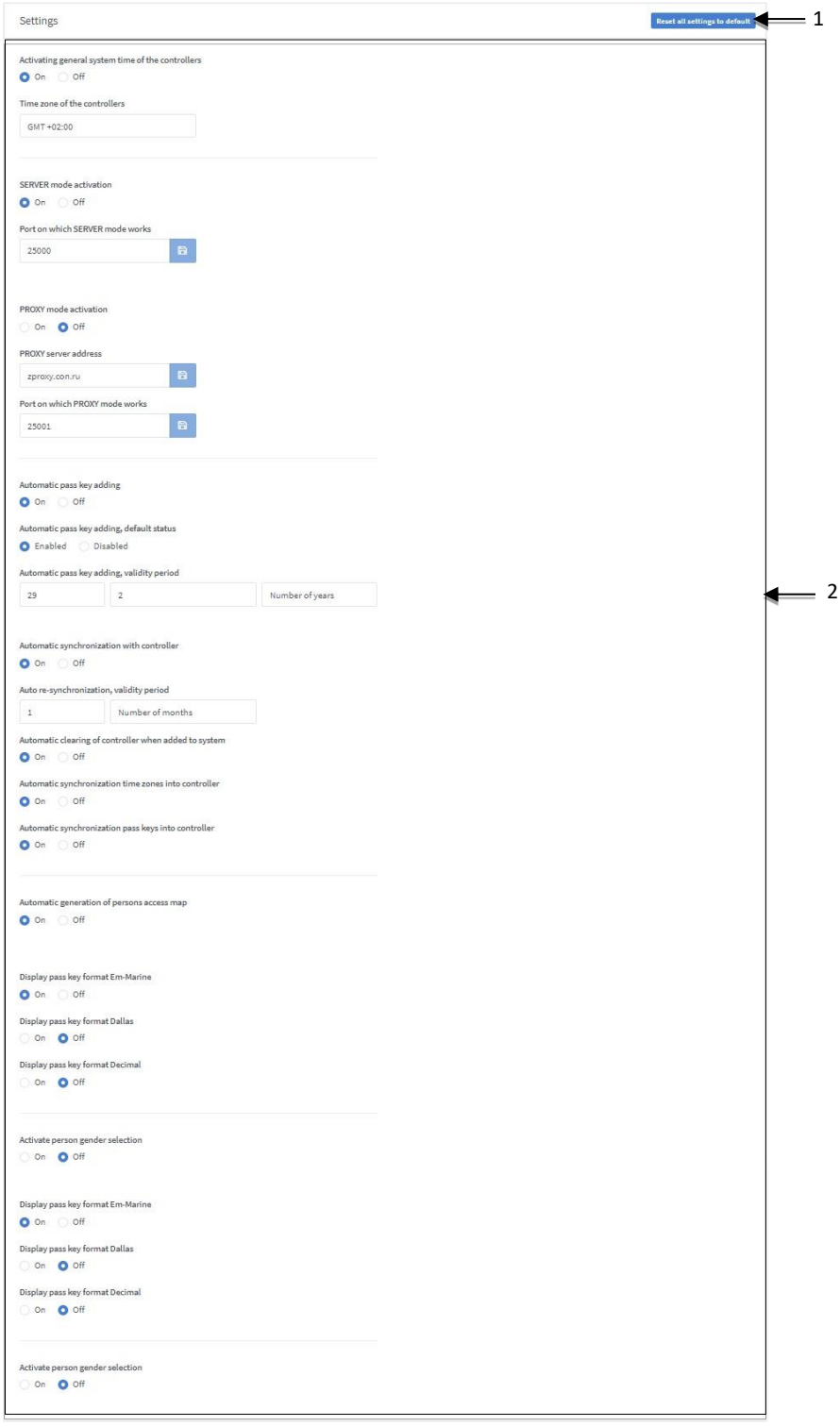


Fig.82 Page "Settings"

Settings description:

1. **Enabling general system time for controllers:**
   a. Activating general system time for controllers (enabled by default) – selected time zone activation for all the controllers, for which the use of system time is enabled. Enabled by default.

   b. Time zone of the controllers - select the desired time zone from the list.

2. **Configure SERVER mode**
   a. Activation of SERVER mode (enabled by default) - the setup starts / stops the server to work with the converter in CLIENT mode (see section *3.2.1*Converter and "Guard Plus" software operating modes).
   b. TCP server port (by default - 25000) - select the port on which the connection is established (the converter must be configured on the appropriate port).

To change the TCP server port, you must turn off this mode, enter a new port and save it, and then turn on the mode.

3. **Configure PROXY mode**

a. Activation of the PROXY mode (by default is off) - when the mode is activated, the proxy server will be constantly polled for the corresponding authentication keys (which are added to the system).
b. PROXY server address (by default - zproxy.con.ru) - indicates the IP address or domain name of the proxy server with which you want to connect.
c. Proxy server port (by default - 25001) - specifies the port of the proxy server that is available for connection.

4. **Automatic pass key adding** (by default - enabled) - if there is an attempt to pass through a controller which is added to the system, using an identifier that is not in the system, it will be added and displayed at page "Manage Pass Keys".
5. **Pass key status by default while adding a pass key** (by default- disabled):
   - Active – pass key that is added automatically will be active.
   - Disabled - pass key that is added automatically will be disabled.
6. **Pass key validity period when automatically added** – date when a pass key was automatically added is a date when it became valid. And an expiration date is calculated by adding days / months / years, which the user will specify in this setting (by default 29 days and 2 months)
7. **Automatic synchronization with the controller** – automatic synchronization with all the controllers, that are added in the system and assigned to a group (actions will be automatically performed as if you click "Synchronization" button *(1 at the page. 64)*) (by default - disabled).
8. **Automatic synchronization repeats** - is the period over which automatic synchronization will occur, par.4 (by default – 1 day).
9. **Automatic clearing of a controller when added to the system** - when a controller is added to the system, its memory will be completely cleared.
10. **Automatic synchronization of time zones to a controller** - when a controller is assigned to a working area, time zones will be automatically synchronized in accordance with the

settings of the working area. In the case of editing the time zones of the working area, data will be overwritten to a controller's memory.

Automatic synchronization of time zones to the controller occurs only if the controller is online.

11. **Automatic synchronization of pass keys to a controller** - only those identifiers that are assigned to the owners (with access settings and time zones of the controller) are automatically written to a controller's memory. For any actions with the identifier (adding/removing an owner, editing, deleting, etc.) - the data is updated in the memory of the corresponding controller.

The maximum number of pass keys that can be written to a controller's memory is determined by **License***(see section3.2.2Device management: Converters(Add License).*

12. **Persons access map automatic generation** - if this setting is enabled, then with any changes to persons settings, a new access map will be generated automatically (by default - enabled).
13. **Activate person gender selection** – if this setting is enabled, then the field for selecting a person gender is displayed. If this setting is disabled, then the person gender selection field will be hidden.
14. **The number of logs in the "System log"** - the maximum number of logs that can be stored in the system log (by default - 5000). After exceeding the specified number of logs, rotation is on: each newly added log deletes the very first log in the log.
15. **Reasons for blocking pass keys** (*Fig.83*) – choosing pass keys blocking reasons that will be available when creating/editing person's blocking periods. By default, when you first start, the list of reasons for blocking is empty.

Form "Reasons for blocking pass keys" structure:

- Field ABBREVIATION - the abbreviation for the reason for blocking.

The abbreviation is used when displaying the period of blocking in the report (reasons for the rightful absence of a person at the workplace).

- REASONS field - description of the reason for blocking the pass key.
- Options:

1. button to go to the "edit blocking reasons" form (*Fig.84*).
2. button to delete the reason for blocking.

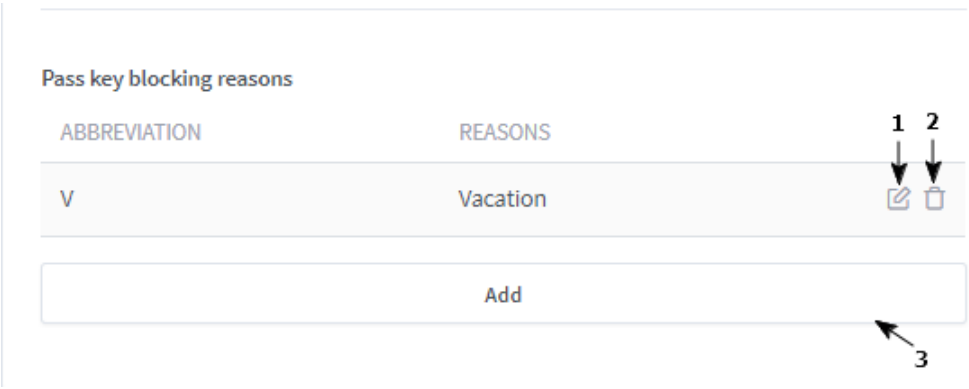


Fig.83 System settings: Reasons for blocking pass keys

To add reasons for blocking, do the following:

1. Click the “Add” button (3 на *Fig.83*). As a result, the form for adding a reason for blocking the pass key opens.
2. Fill in the “reason” and “abbreviation” fields (both fields are required).
3. Click the “Add” button.

To edit reasons for blocking pass keys, do the following:

1. Click the “Edit” button (1 на *Fig.83*). As a result, the form for editing the reason for blocking the pass key opens.
2. Make the necessary changes.
3. Click the “Edit” button.

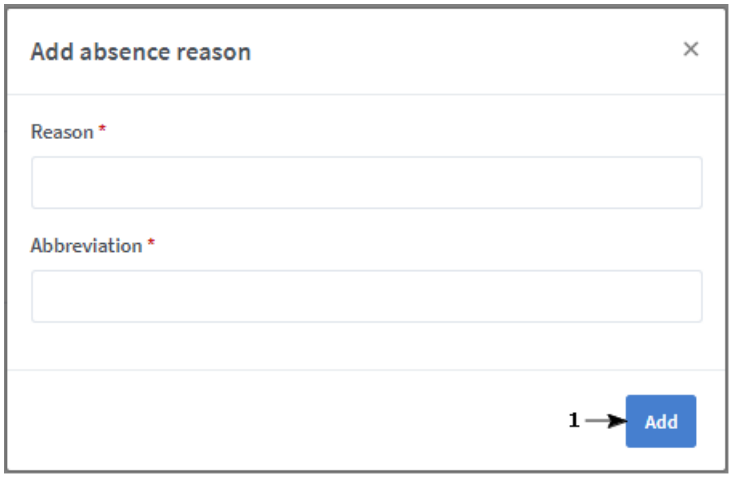


Fig.84 Edit reasons for blocking pass keys form

3.4.2 Backup

This page allows to create a backup schedule and download completed backups.

“Backup” page structure *(Fig.85)*:

1 – settings panel for running an automatic backup with ready-made period options and with the ability to customize the period yourself;
2 - personal period setting panel for running backup;
3 – “Run backup” button (manually); after clicking this button backup is made at once;
4 – “Update list of backup files” button;
5 – the number of backups on the one page;
6 – “Download backup on your computer” button;
7 – navigation buttons.

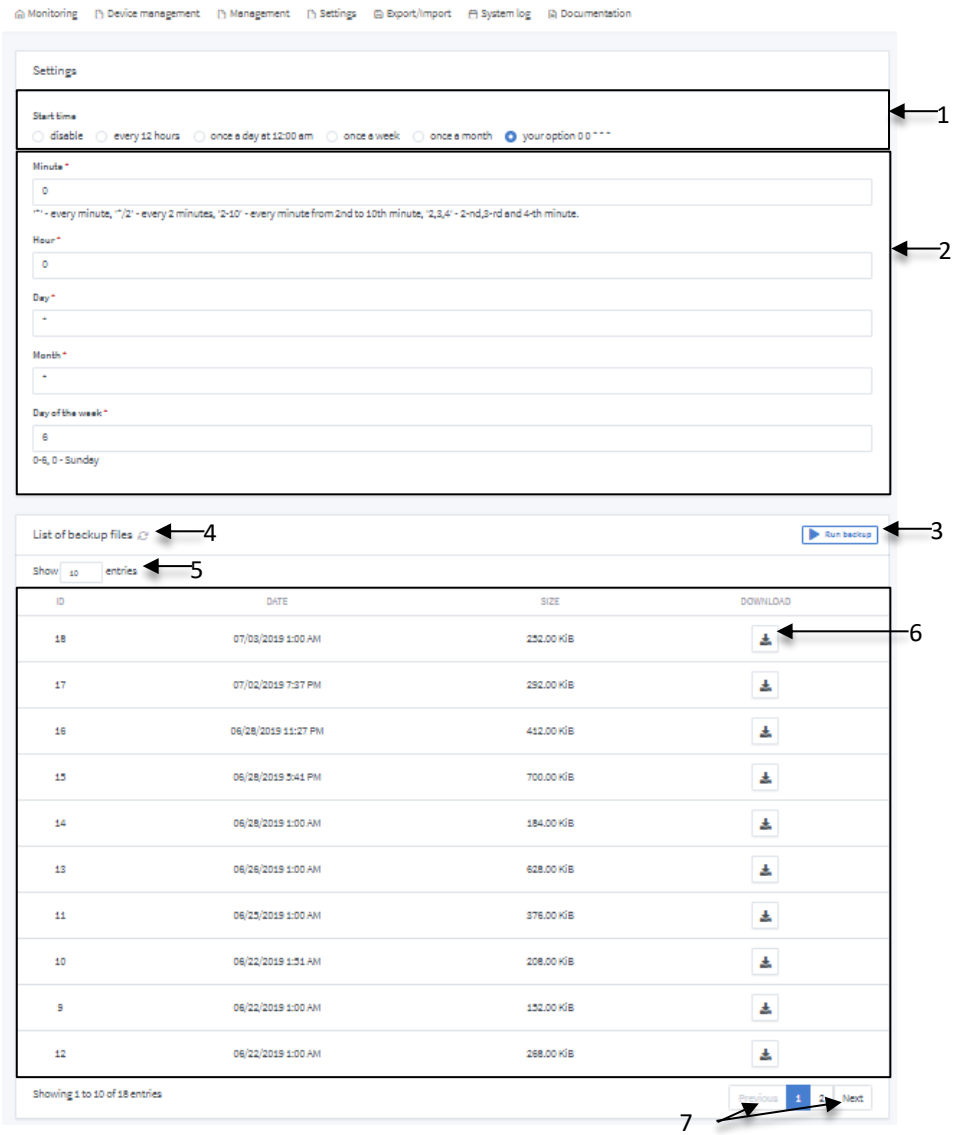


Fig.85 Page “Backup”

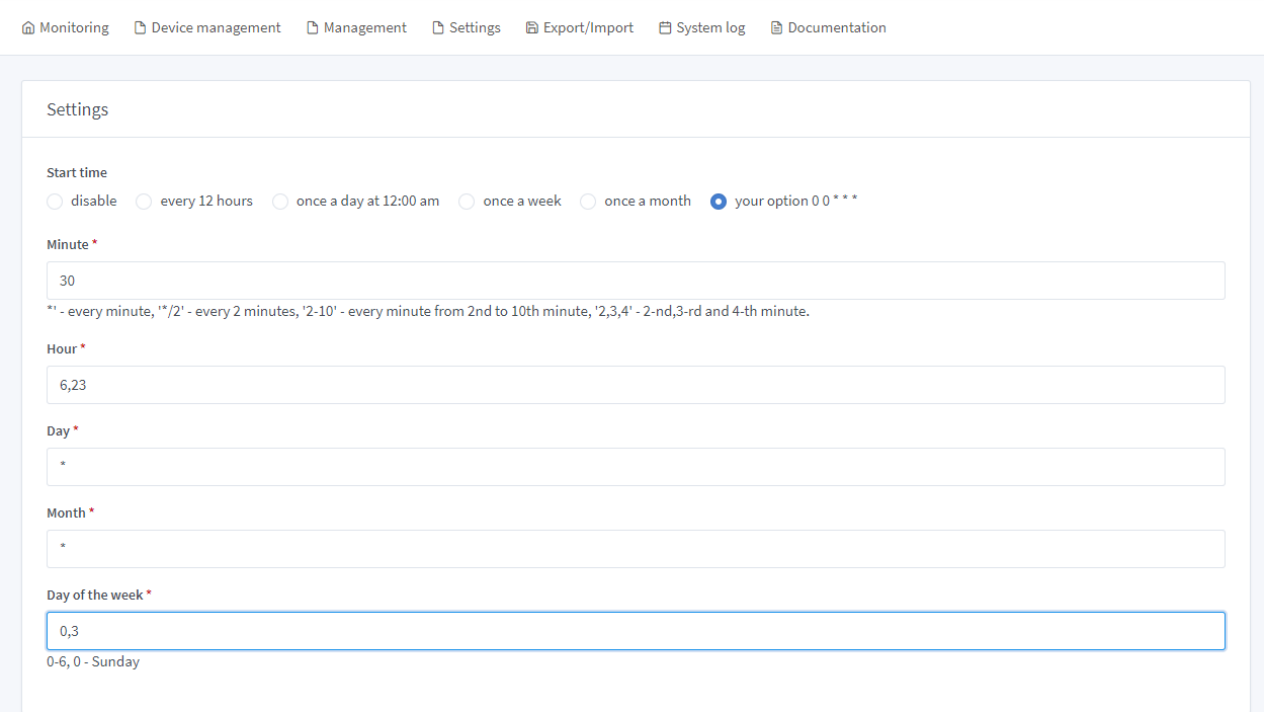


Fig.86Backup settings: Your option

Backup settings: Your option

Backup launching settings are based on “Cron” system. In this example*(Fig.86)*, backup runs every Sunday and Wednesday at 6:30 and 23:30.

Backup system changes launching settings as soon as you input required parameters.

«System backup period:

•once a week - creates backup every week on Sunday at 12 a.m.;

• once a month - the first day of every month.”

Restore system from backup

To restore system data from backup, you need to do as follows:

1. Copy backup file from backups folder;
2. Open db folder, delete the database file there and insert backup file;
3. Change the name and extension of backup file to **database.sqlite**;
4. Launch the program.

3.5 Export/Import

The “Export/Import” page imports/exports the system data files.

“Export/Import” page structure *(Fig.88)*:

1 - System data: import/export files in JSON format;

After importing system data, restart the system.

2 - System data, only the employees (employees and pass keys): import/export files in JSON, XML, CSV format;

When importing data in Guard Light format, persons, pass keys, organizational units are

3 - Data in Guard Light format: import/export files in XLSX format, import files in XML format;

4 - Data in Guard Commander format: import files in CSV format.

When importing data in Guard Commander format, photos are not added.

Exporting data from Guard Commander system, select “Dallas” format *(1 at Fig.87),* since the system supports 3bytes format for a pass key number.

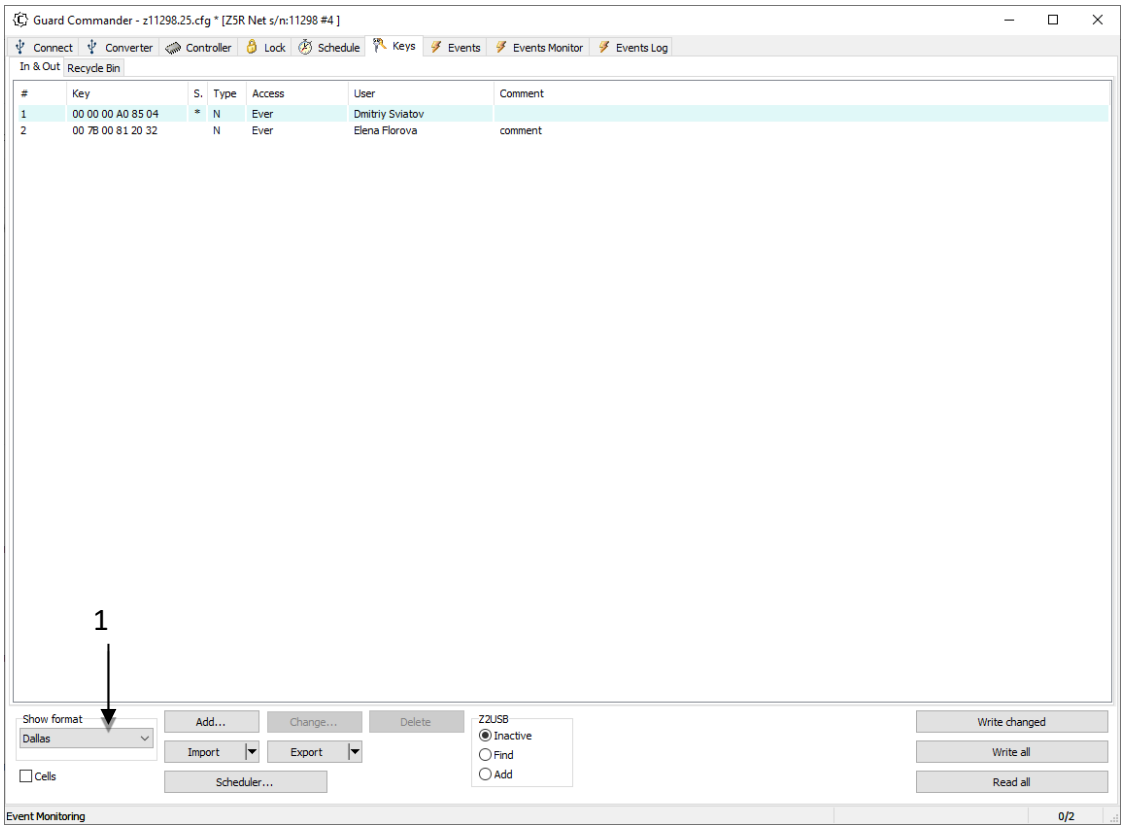


Fig.87 Guard Commander: data export

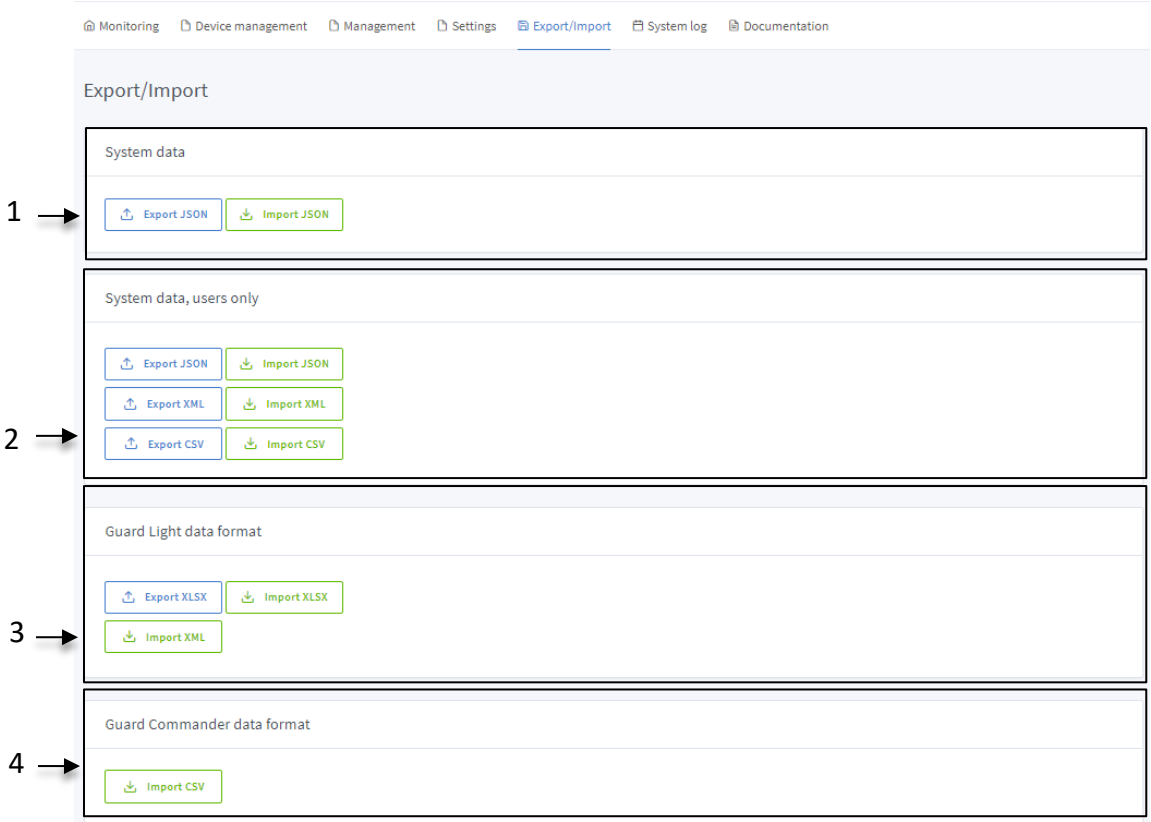


Fig.88 Page "Export/Import"

If you add pass keys after import, they expire in **24h** since import by default.

All the exporting files will appear in both "export" and "download" folders by default.

3.6 System log

In "System Log" menu, you can open the event log page.

"System Log" page structure *(Fig.89)*:

1 - "Clear event history" button;
2 - "Update system events list" button;
3 - The number of events displayed on one page;
4 - Search field;
5 - System log is presented in the form of a table with fields:

- **TIME**– time and date of event registration in the system;
- **MODULE**– the module in which the event occurred;
- **LEVEL** – event message type (INFO – information, WARN– warning, ERROR – error);
- **USER** – the user who initiated the event;
- **IP** – the IP address from which the event was recorded;
- **MESSAGE** – description of the event.

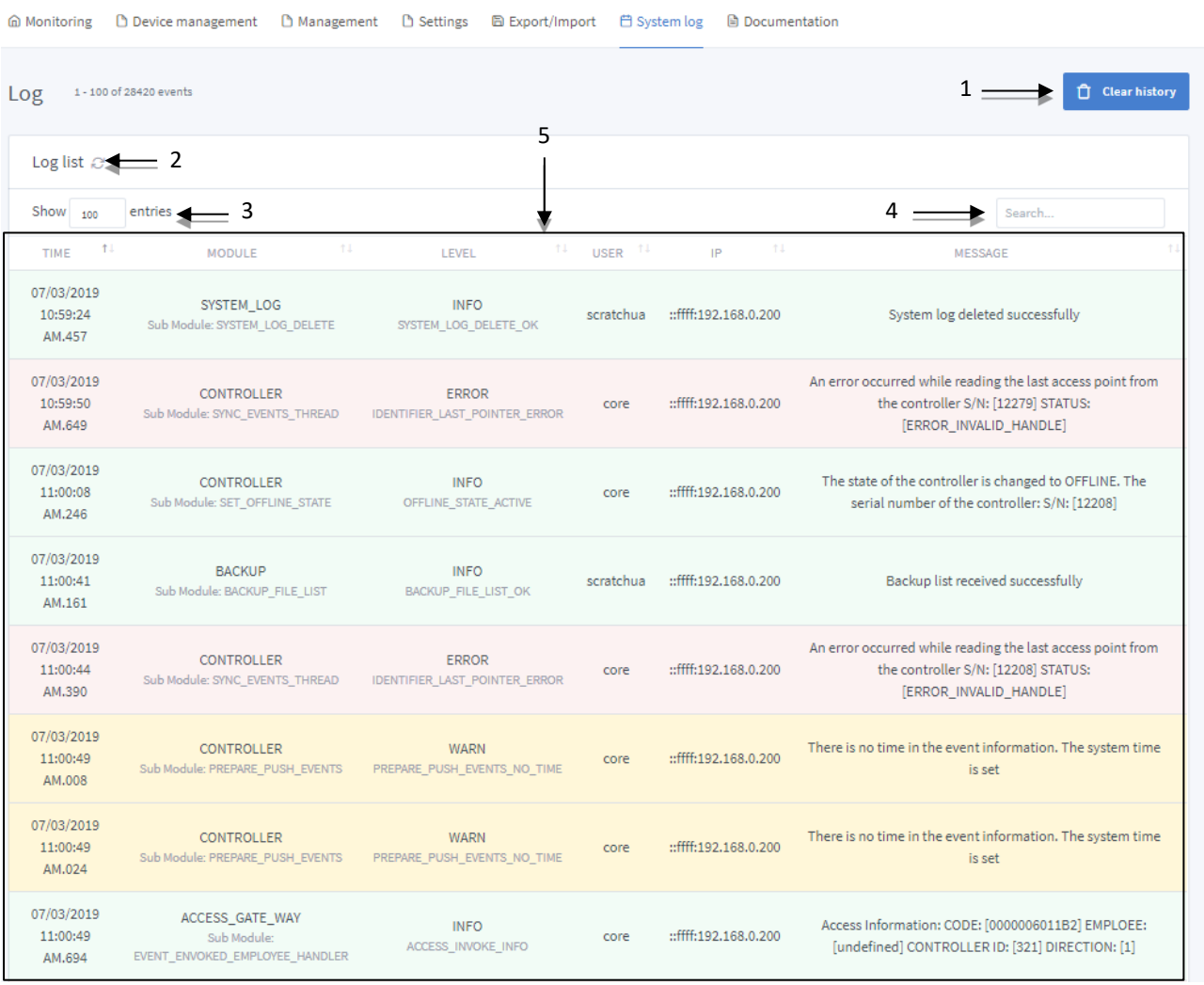


Fig.89 Page "System log"

System event row is highlighted, depending on the level of the event:

- in green - INFO (information)
- in yellow - WARN (warning)
- in red – ERROR (error).

3.7 Documentation

"Documentation" section opens this user manual.

4 User profile. User logout

To open a profile control panel, click current user information display area on the user panel *(Fig.90)*.

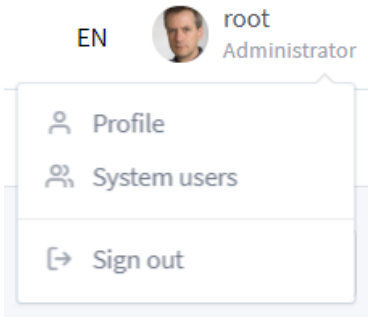


Fig.90 Manage user profile

Parameters for default signing in: **user** - root, **password** - root. User **root** cannot be deleted, you can only edit (except “Administrator”).

To open profile settings, click “Profile” button. To sign out click “Sign out” button.

4.1 Profile

You can edit user information in “Profile” form:

Profile photo: to upload a photo, click“ Browse"*(1 atFig.91);*

User’s full name;

User’s short name;

Email address.

To save changes, click “Save” button*(2 at Fig.91)*.

“Change password” form allows to change user’s password. To change password, fill in all required fields and click “Save” button*(3 at Fig.91).*

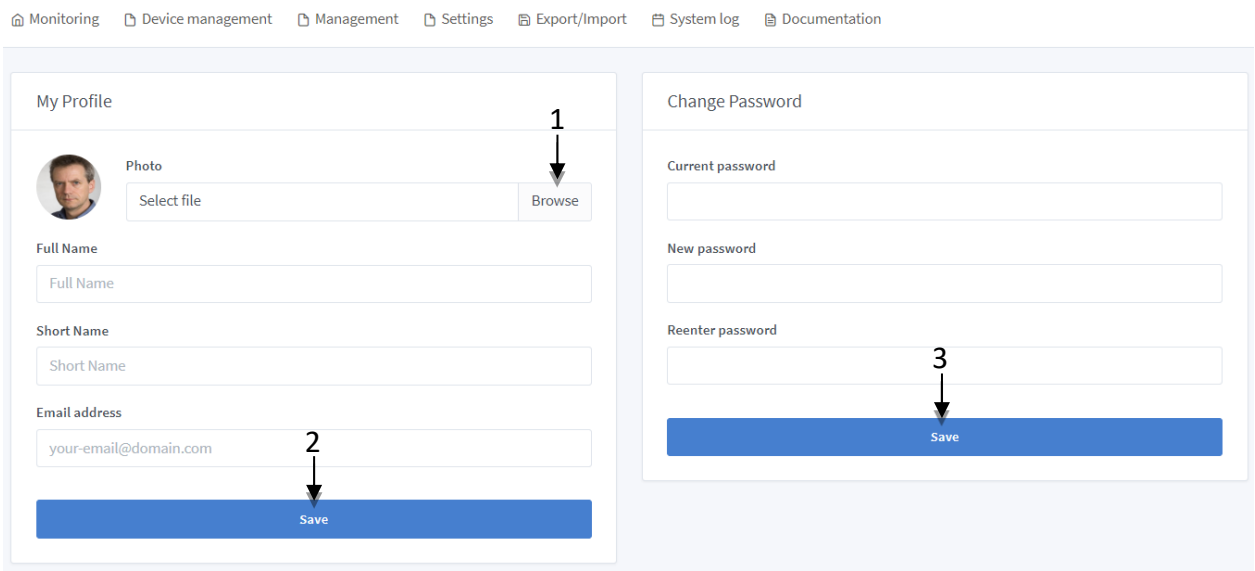


Fig.91 Form “Profile”

4.2 System users

If you want several persons to work with the system, then add each one as a User.

"System users" page structure *(Fig.92)*:

1 - "Add new system user" button;
2 - "Update users list" button;
3 - the number of users on one page;
4 - search field;
5 - users list is presented in the form of a table with fields:

- **LOGIN** - user's login and name in the system;
- **STATE** – recipient state (active/deleted);
- **E-MAIL** – user's e-mail;
- **ROLE** – specified user role that affects access rights;
- **SYSTEM LANGUAGE** – language that will be used when this user is authorized;
- **LAST AUTHORIZATION** – time of the last authorization of this user;
- **ACTIONS** – actions that can be performed with the user profile (edit/delete);

6 - "Edit system user" button;
7 - "Delete system user" button;
8 - navigation buttons.

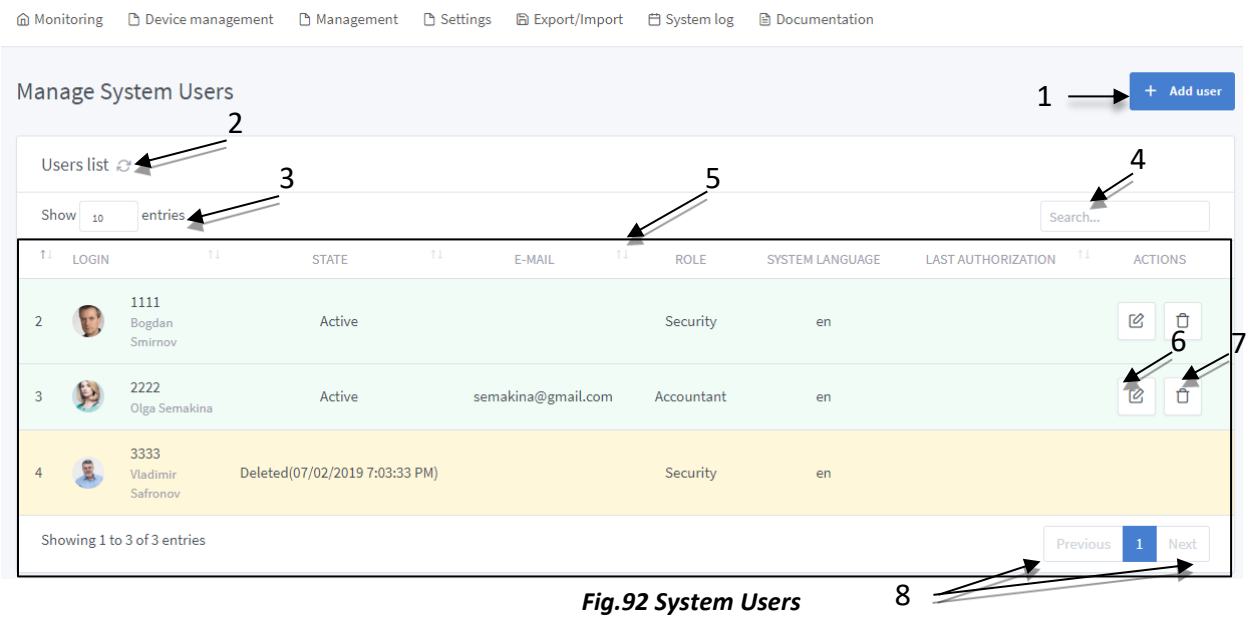


Fig.92 System Users

If the system user row is highlighted in green color - the user is active, in yellow - deleted.

If the user is deleted, the date and time of this action is displayed in "State" column.

Add system user

To add a system user, fill in the required fields (marked with an asterisk), other fields are filled in at the discretion of the user *(Fig.93)*.

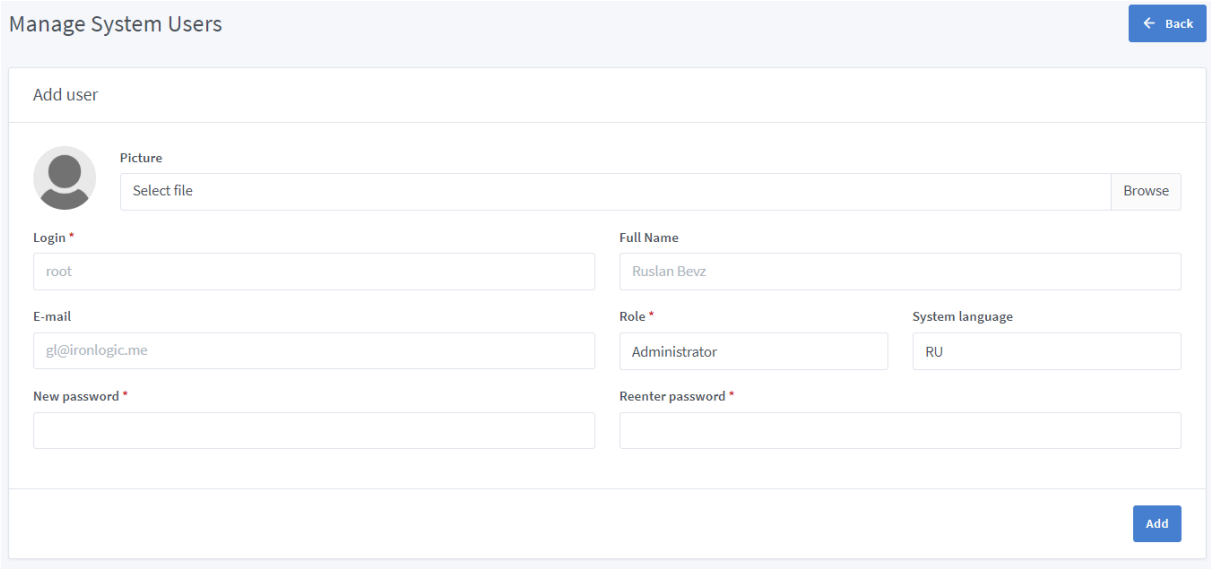


Fig.93 Add system user

To control access rights, concept of **Role** has been introduced. System user role regulates access rights to the system functionality. There are three user roles with personal access settings:

1. Administrator (full system functionality);
2. Security (Photo verification, Events log, Manage guests pass keys, Documentation) (*Fig.94*)
3. Accountant (Reports, Management: Organizational units, Persons, Pass keys, Guest pass keys, Access maps; Export/Import, Documentation *(Fig.95).*
4. Accountant(Reports) – (Reports, Documentation).

When adding a system user, role “Administrator” is set by default.

The **login** field after saving the user information is not available for editing.

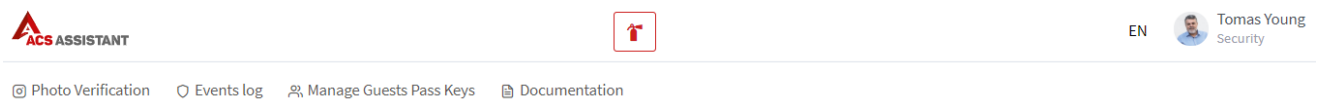


Fig.94 System main menu: role "Security"

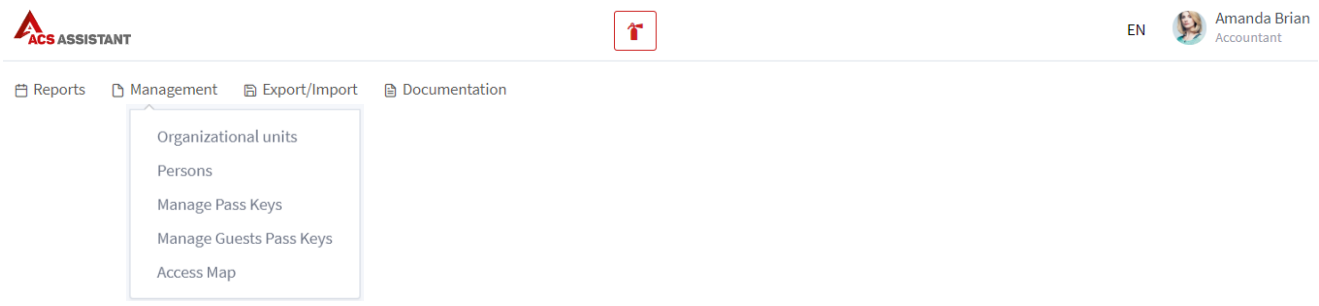


Fig.95 System main menu: role "Accountant"

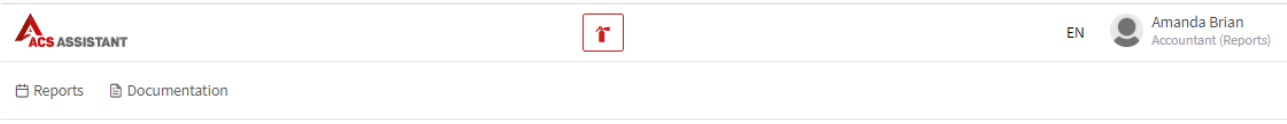


Fig.96 System main menu: role "Accountant(Reports)"

Change User Information

To change, click “Change” in the selected user field.

Grey fields cannot be changed or edited*(Fig.97)*.

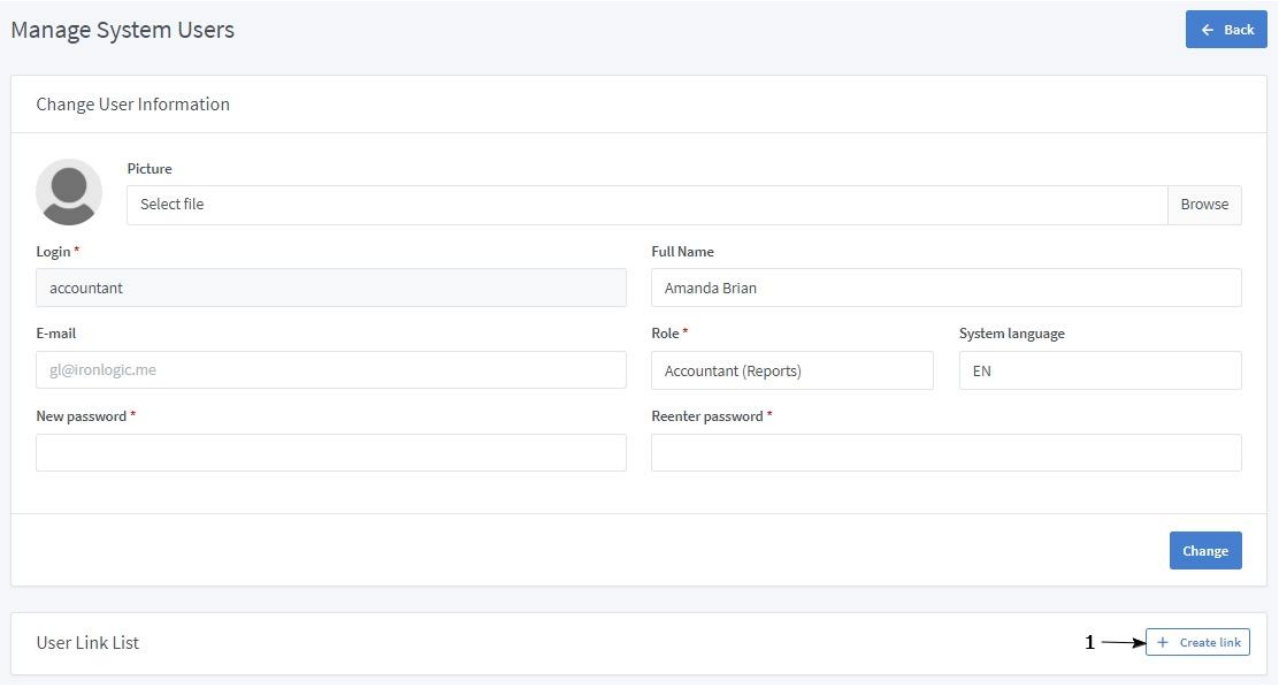


Fig.97 Manage System User

For a user with the Administrator role when editing all system users (except for users with the Administrator role), the function of adding redirection links to the system page is available, without authentication (without entering a login and password).

Adding a link

This functionality is to add users the ability to log in without authentication.

Adding a link should be done through a browser, which in the future will be used to enter the system using the link.

To add a link to the user, do the following:

1. Press the edit button for the corresponding user (6 in Fig. 84). As a result, the user editing page will open.
2. Click the “Add link” button (1 in Fig. 89 Fig. 85). This will open a window for creating links (Fig. 90).

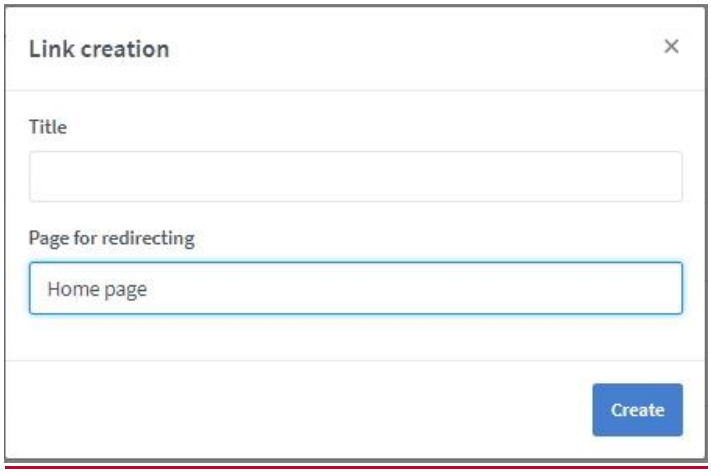


Fig.98 Window "Create link"

3. Select a page for redirecting in the appropriate field from the list of available ones and enter a link name (optional).

The list of available pages for redirection depends on the role of the system user:

Security: Photo verification, Event log, Guest pass keys management, Documentation;

Accountant: Reports, Management: Organizational units, Persons, Pass keys Management, Guest pass keys management, Access maps; Export / Import, Documentation.

Accountant (Reports): Reports, Documentation.

It is not possible to create a link for a user with the Administrator role.

4. Confirm the creation of the link by clicking the "Create" button (1 in *Fig.98*).

For each user, you can create a maximum of 10 links. For each browser, the last link created is active. Only one last link will always be valid in one browser. Only one user from one browser using one link can log in without entering a username and password.

The created link is active until the browser cookies are cleared. After deleting cookies, you must re-create the login link without having to authenticate.

5 Configuration system file

The configuration file contains the following settings:

1. PORT – port, which the system starts using at startup.
2. PROTOCOL – HTTP, or HTTPS.
3. PATH_HTTPS_KEY – directory where the HTTPS key is stored.
4. PATH_HTTPS_CERTIFICATE – directory where the HTTPS certificate is stored.

Directories where the HTTPS key and certificate are stored should be set only if an appropriate data transfer protocol is selected. If the HTTP is set, the key and certificate fields are ignored.

5. DB_DIR – directory where the system database is stored.

All paths to the key, certificate and DB folders must start from root (full path) and use "****" as path delimiter.

For example:

D:\\office-work-place\\dev-place\\programms_files\\private-keys\\localhost-privateKey.key

If DB folder is system, the system should be launched with administrator privileges.

Path to a database folder, that stores on a remote computer has the following format: ***ip-address remote******path***, where

- ***ip-address remote*** – ip-address of a remote computer;
- ***path*** – full path to a database folder (access to the folder must be open).

Example: \\\\192.168.0.221\\office-work-place\\dev-place\\db

6. LOG_LANGUAGE – language for system messages that will also be displayed in system log.

The language of system messages is English, by default, it can be changed only in this row.

7. *_LOG_LEVEL – logging levels for different system modules.

Configuration file should have the name - *config.json* and be in JSON format.

8. SYS_LOG_TO_FILE – automatic saving of system messages to "logs" folder, it is the folder from which system launches (true - messages are saved, false - are not saved).
9. WS_PORT_START - initial value of the range of ports for connecting photo verification.
10. WS_PORT_END – port range end value.

If you need to connect to a specific port, start and end values of the range must match.

For example:

- WS_PORT_START: 3001
- WS_PORT_END: 3001

11. FOTOVERIFICATION_RECONECT_FRONT_TIME – time, in milliseconds, after which photo verification interface should reconnect to the port in case of disconnection.
12. CLOSE_TERMINATE_OFF – closing program's terminal if a port is busy.
13. DEF_RTU_TIMER_MS – Idle time on a line on which a decision that data transfer is completed is made.
14. MIGRATION_DIRECTION – database migration direction.
15. MIGRATION_VERSION – the version of the database that the user needs;
16. TCP_CLIENT_WRITE_TIME_OUT – timeout time for recording to the controller, for devices in CLIENT mode;
17. TCP_SERVER_WRITE_TIME_OUT – timeout time for recording to the controller, for devices in SERVER mode.

If the configuration file is not found, the system creates it with the default settings:

- port – 5870;
- protocol – http;
- path_https_key – «-»;
- path_https_certificate – «-»;
- db_dir – *db folder will be created in the directory from where the system launches*;
- *_log_level – 2;
- sys_log_to_file – true;
- ws_port_start – 3000;
- ws_port_end – 3010;
- fotoverification_reconect_front_time – 2;
- close_terminate_off – true;
- def_rtu_timer_ms –150;
- migration deriction – up;
- migration version – last.

When configuration file is created, logging levels "2" are set by default, but in case if the user sets logging level or module name incorrectly, then "5".

Example of the configuration file:

{
PORT: 5870,
PROTOCOL: "http",
PATH_HTTPS_KEY:"-",
PATH_HTTPS_CERTIFICATE: "-",

```
    DB_DIR:"",
    DEVICE_MNG_LOG_LEVEL: 2,
    CONVERTER_LOG_LEVEL: 2,
    CONTROLLER_LOG_LEVEL: 2,
    CONTROLLER_ROUTE_LOG_LEVEL: 2,
    CONTROLLER_MANAGER_LOG_LEVEL: 2,
    GUARD_PROTOCOL_LOG_LEVEL: 2,
    EMPLOYEE_MANGEMENT_HANDLER_LOG_LEVEL: 2,
    ROUTES_LOG_LEVEL: 2,
    MODELS_LOG_LEVEL: 2,
    SYSTEM_SETTINGS_LOG_LEVEL: 2,
    ACCESS_GATE_WAY_LOG_LEVEL: 2,
    SYSTEM_LOG_CLASS_LOG_LEVEL: 2,
    UDP_CLINET_LOG_LEVEL: 2,
    SYS_LOG_TO_FILE: true,
    LOG_CLASS_LOG_LEVEL:2
    WS_PORT_START: 3000,
      WS_PORT_END:3010,
      FOTOVERIFICATION_RECONECT_FRONT_TIME: 2,
      CLOSE_TERMINATE_OFF: true,
      DEF_RTU_TIMER_MS: 150,
      MIGRATION_DIRECTION: "up",
      MIGRATION_VERSION: "last"
}
```

Logging levels values:

1. Only critical events.
2. All errors.
3. Warnings.
4. Informational messages.
5. Debugging messages.
6. All types of messages.

Logging levels are nested, e.g. on 3-rd level of logging 1-st, 2-nd and 3-rd level messages will be shown.

Startingform version v1.3.0.3 added new configuration parameters (**MIGRATION_DIRECTION** and **MIGRATION_VERSION**), it isnecessary for a smooth transition from one version to another. Information about migration seein section 6*Migration.*

6 Migration

The migration mechanism is for a smooth transition from one version to another. The migration process starts when Guard Plus launches, provided that the appropriate parameters are specified in the configuration file: **MIGRATION_DIRECTION and MIGRATION_VERSION.**

"MIGRATION_DIRECTION" – database migration direction. It can have the meanings of “up” and “down”. If “up” is specified, then the database will be updated to newer versions, respectively, if “down” is specified, it will return to earlier versions. “Up” is used by default.

"MIGRATION_VERSION" – the version of the database that the user needs. For the version of the database with the corresponding version of the program, see Appendix A. The format for specifying the version is “v_x_x”, where “x”are the numbers from 0 to 9. The default value is “last”. If "last" is specified, then the migration will be performed to the very first version or the very latest, depending on "MIGRATION_DIRECTION".

If the migration direction "MIGRATION_DIRECTION" is specified incorrectly, the system will determine the direction depending on "MIGRATION_VERSION".

For example, the current version of the database is v_1_3, and the version v_1_0 is specified in the configuration file. In this case, the system will determine the direction "MIGRATION_DIRECTION" as "down" and will be migrated to the version v_1_0.

If the desired version of the MIGRATION_VERSION database is specified incorrectly, then, depending on MIGRATION_DIRECTION, the migration will be performed either to the earliest version (for the direction of migration "down") or to the latest (for the direction of migration "up").

If "MIGRATION_DIRECTION" and "MIGRATION_VERSION" are incorrect, then the system checks the current version of the system database and if it does not correspond to the latest, the system automatically determines the migration direction and version:

- "MIGRATION_DIRECTION" - "up",
- "MIGRATION_VERSION" - "last".

As a result, the database will be updated to the latest version.

Appendix A

Migration to version v_1_0 is only possible for a program version lower than v1.3.0.3. For the program version v1.3.0.3 to work properly, the database version must be at least v_1_1.

#	Program version	Database version
1.	< V1.3.0.3	V_1_0
2.	V1.3.0.3	V_1_1
3.	V1.3.1.3	V_1_2
4.	V1.3.2.3	V_1_3
5.	V1.3.3.3	V_1_4
6.	V1.3.3.3	V_1_5

Appendix B. List of supported hardware

Guard Plus software supports the following Iron Logic hardware:

Converters:

1. Z-397 Guard USB/RS-485;
2. Z-397 Guard USB/RS-485/RS-422;
3. Z-397 Web
4. built-in converters in Z-5R Web controllers;

Controllers:

1. Matrix II Net;
2. Z-5R Net, Z-5R Net 8000;
3. Z-5R Web;
4. Eurolock EHT Net padlock controller.

Appendix C. Minimum Server Hardware Requirements

CPU	Dual Core 2 x 1,60 ГГц		
RAM	2 ГБ		
HDD	HDD 250 ГБ		
OS	Windows 7 Windows 8 Windows 8.1 Windows 10 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Linux	macOS
Architecture	32-bit, 64-bit	64-bit	64-bit

Guard Plus Software Supports Linux x64-Compatible OS. Tested on:

1. Ubuntu Server 19.10;
2. Debian 10.0;
3. CentOS 8;
4. Linux Mint 19.x (Ubuntu Bionic package base);
5. Linux Mint 3 (Debian Stretch package base);
6. Fedora 30;
7. Orange Pi PC + Armbian 5.90 (Ubuntu Bionic server 4.19.57 kernel);
8. macOS 10.14 Mojave;
9. macOS 10.15 Catalina.

Appendix D. Minimum workplace requirements

OS	Windows	Linux	macOS
Architecture	32-bit, 64-bit	64-bit	64-bit

The minimum requirement when choosing an operating system for the user's workplace is the ability to install and run Web browsers that support JavaScript in the operating system, in accordance with the ECMA-262 standard (ISO / IEC 16262), version ECMAScript 6 and higher.

The following Web browsers are recommended **for a client workplace without using desktop pass key readers**:

Name	Version
Google Chrome	68 and higher
Microsoft Edge	14 and higher
Mozilla Firefox	60 and higher
Opera	38 and higher
Safari (only macOS)	10 and higher

The minimum requirement when choosing an operating system for the user's workplace is the ability to install and run Web browsers that support JavaScript in the operating system, in accordance with the ECMA-262 standard (ISO / IEC 16262), version ECMAScript 6 and higher.