Single-User Software with Verification

SL02

Operation Manual

PERCo®

SL02

SINGLE-USER SOFTWARE WITH VERIFICATION

OPERATION MANUAL

TABLE OF CONTENTS

GENERAL

This Operation Manual includes important information about the SL02 Single-user software with verification, its application and main features. The Manual provides straightforward instructions on how to use this software as detailed step-by-step procedures.

The Manual is designed for operators with working knowledge of Microsoft Windows software and operational experience with such common software packages as MS Office, etc.

Application of the SL02 Single-user software with verification

The software is designed as a single-operator programme appropriate to use for:

- administration of employee and visitor lists (full names);
- issue of access cards;
- access rights assignment under authorized/non-authorized principle;
- access authorization/denial or activation/deactivation of the Guard mode;
- employee and visitor identification and verification by means of photo and video frame images;
- real-time capture of dynamic video image;
- setting and change of access modes;
- hardware configuration;
- database event logging with data exportable e.g. to an Excel file.

STARTING OPERATION

In order to use the SL02 Single-user software with verification (hereinafter referred to as "the software"), it should be installed at a PC connected to the local area network, LAN.

Installation of the software

1. Insert the disc with the licensed software into the CD-ROM drive, wait for the installation program icon to appear.
2. If, by some reason, the installation icon does not appear automatically, use Windows Explorer or any other file manager application to access the disc contents, and run the **VisitorsSetup.exe** program.
3. Follow the Installation Wizard instructions that appear on your screen.
4. Click on the Ready button when the installation is complete.

Starting the software

To start the software:

1. Click on the **Start button.**
2. Select **All Programs→ PERCo → Single-user software with verification → Single-user software with verification**. The software work window will appear on the screen with the Employees section opening on default; subsequent runs

of the software will open the last Section where the software was exited. When the software window is reduced, its sign will appear in the System Tray icon as shown below:

Descriptions of corresponding work windows are given in the beginning of each Section.

LICENSING

With the installation complete, the SL02 Single-user software with verification will require additional entering of the activation key.

The controller included in your system package serves as the hardware feature to protect the software against unauthorized use. Functioning of the controller as the hardware license guard does not affect its other functional capabilities.

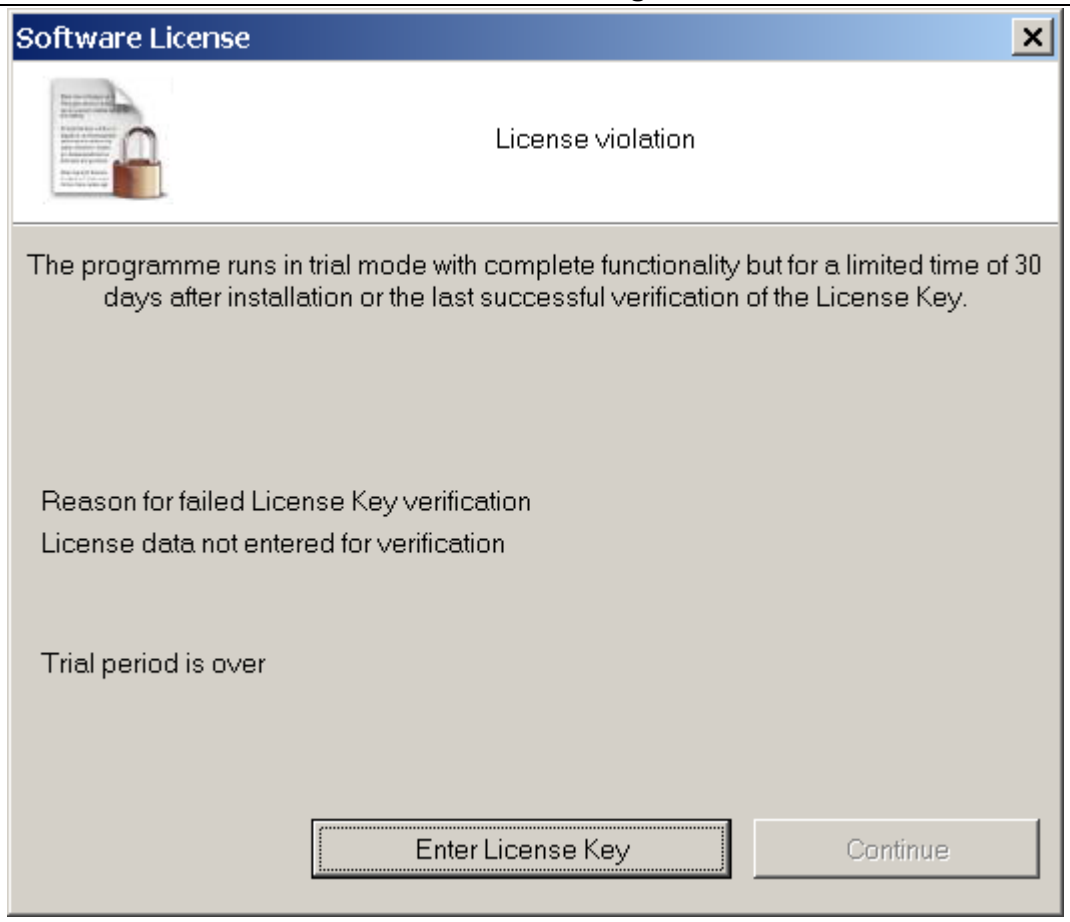
In order to make the software registration easier as well as for demonstration of the software performance capabilities, the software allows a trial period of 30 days since its first run.

During the trial period the software is fully functional but a warning note indicating the time up to the end of the trial period will appear. After 30 days the trial period expires and access to the software is cancelled.

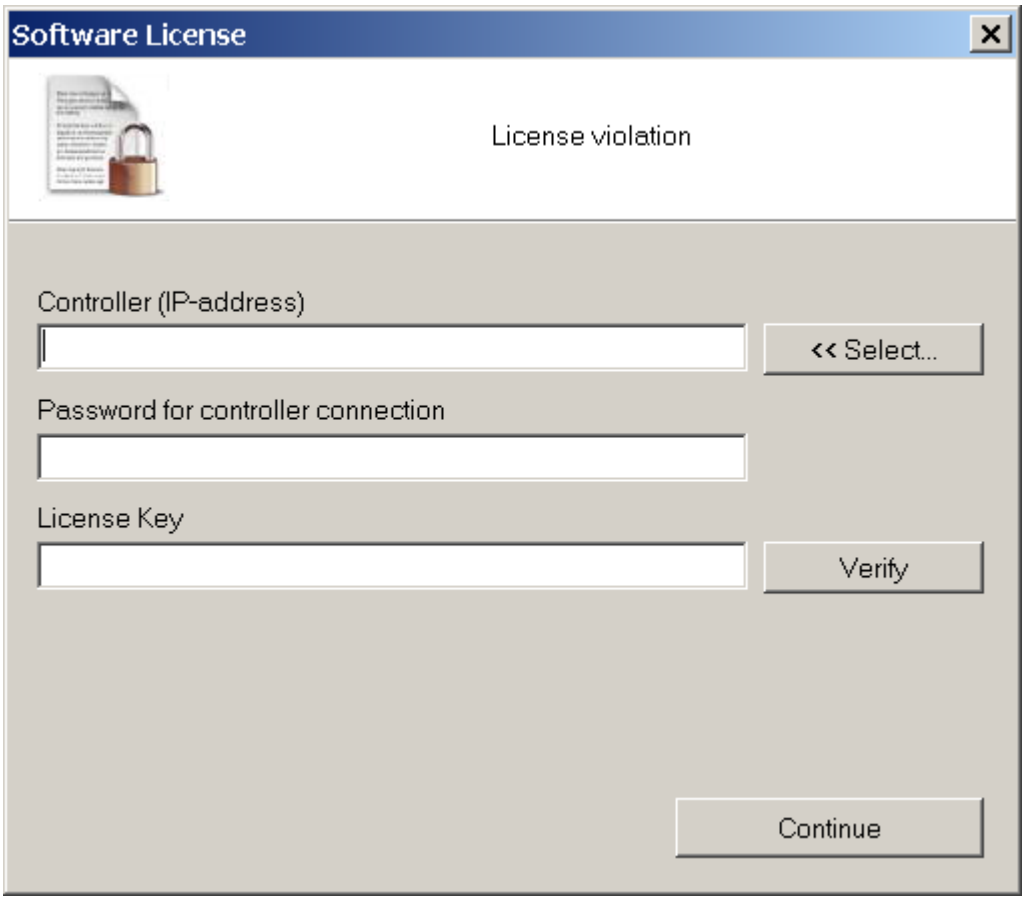
To receive the activation key for your software you should select a controller in the system that you want to provide the hardware license protection for the software; fill our standard license application form and send it to PERCo company.

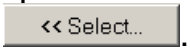
After receipt of the license agreement with the software License Key, the Key should be entered into the software.

Enter the License Key when starting the SL02 Single-user software with verification.



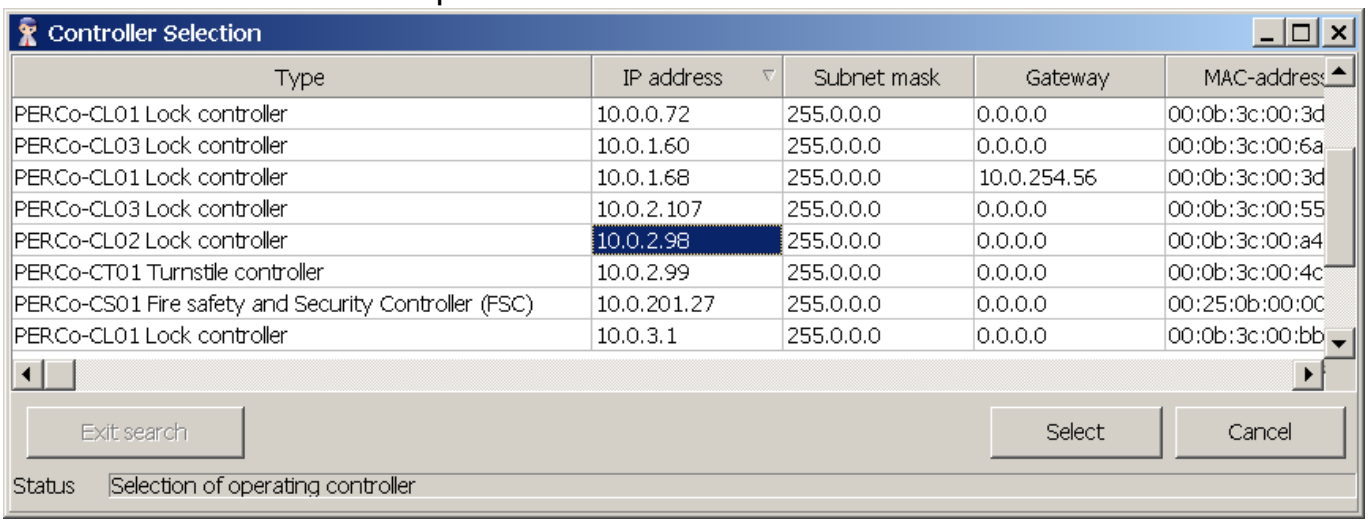
Click on the **Enter the License Key** button to enter the License Key. A window will appear:



Firstly, select a controller to provide the hardware license protection for the software using the **Select** button 

.

Select controller in the opened window:



After a click on the **Select** button, the controller address will appear in the window. Enter the password to access the controller, then enter the License Key and click on the Test button.

After the testing the software is ready for use.

If a wrong License Key is entered and the system cannot decode it as the key does not conform to the selected controller, the software informs about the License Key registration error. In the event of such an error check the communication between the selected controller and the software, as well as the correctness of the entered License Key and take another try.

NOTE

Checking of the License Key will always by carried out by means of your selected controller! In the event of the controller communication failure the system automatically switches to the 30-day trial mode.

EMPLOYEES

The Employees Section is designed for employees' and visitors' data entry, assignment of access cards with unique ID numbers, allowing and denying of access, authorizing or denying the right to activate/deactivate the Protection mode, inspection of a certain employee's event log over a specified period of time. Click on the Employees tab to open the section.

Employees work window

The work window of the Employees section looks as follows:

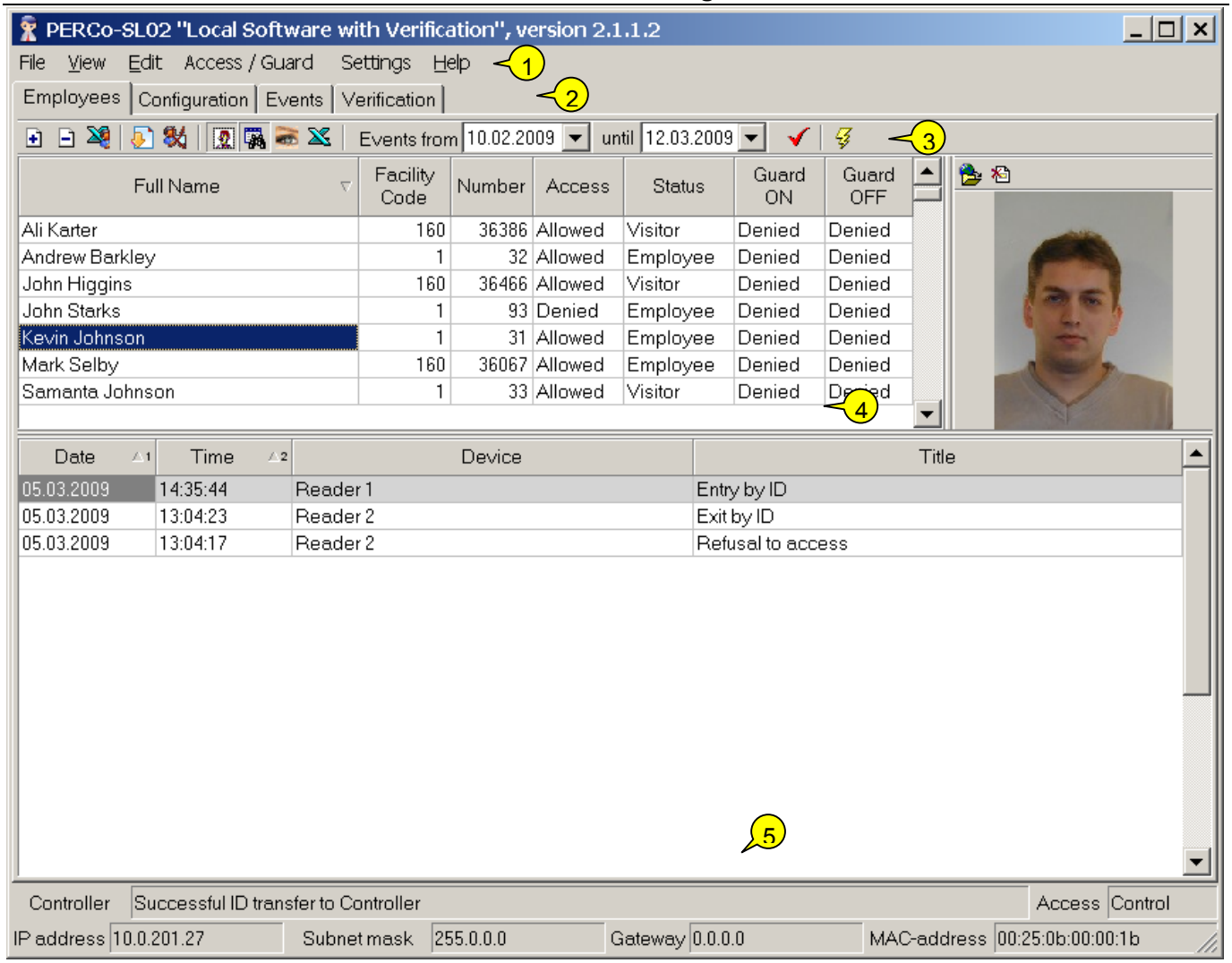


Fig.1. Employees section work window

NOTE

Lines with data that has not been exported to the controller, and therefore not saved into the system, are highlighted with yellow colour.

1. The window top contains the main menu.
2. There are following section tabs under the main menu: **Employees**, **Configuration**, **Events**, **Verification**.
3. Functional elements of the window are described in the Appendix 1.
4. The central part of the window contains a **desktop**. The data are given as a table made of several columns, each with a particular functionality. Such a tabular presentation conveniently allows sorting data by various attributes in descending or ascending order. The arrangement of the columns can be easily changed by dragging. The event list related to a selected employee/visitor is located below the desktop. A status line at the bottom of the desktop displays the service information (status of the controller, access mode, IP-address, etc.)

Adding an employee/a visitor data

After the software installation, the list of the employees and visitors is empty. To add an employee/ visitor:

1. Click on the **Add Employee button** — . A yellow highlighted line will appear in the list (refer to NOTE fig.1).
2. Enter the employee's forename (names) and surname, or surname and initials into the Full Name column.
3. Click on the **Employee** in the status column and select either **Employee** or **Visitor** in the dropdown list :

4. The Access column displays the default option **Allowed,** informing that this employee / visitor is authorized to pass through a certain operating device (OD) in the set access mode. For how to authorize/deny access refer to the Access Authorization/Denial section below.
5. On the next stage the employee should be issued an access card. Refer to the Entering an ID number section below for the access card issue procedure.

NOTE
You can also add an employee/a visitor by clicking on the **Down** (↓) or **Insert buttons**.

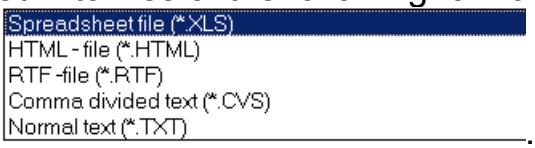
Deleting an employee/ a visitor

To delete an employee/a visitor from the list:
1. Choose any box in the line containing the data of the employee/ visitor to be deleted and click on the **Delete Employee button** — .
2. Click on the Yes button in the appearing confirmation dialog box. The employee/ visitor and their access card data will be deleted from the database.

NOTE
Nothing changes in the Event Log when an employee is deleted.

Export of employees

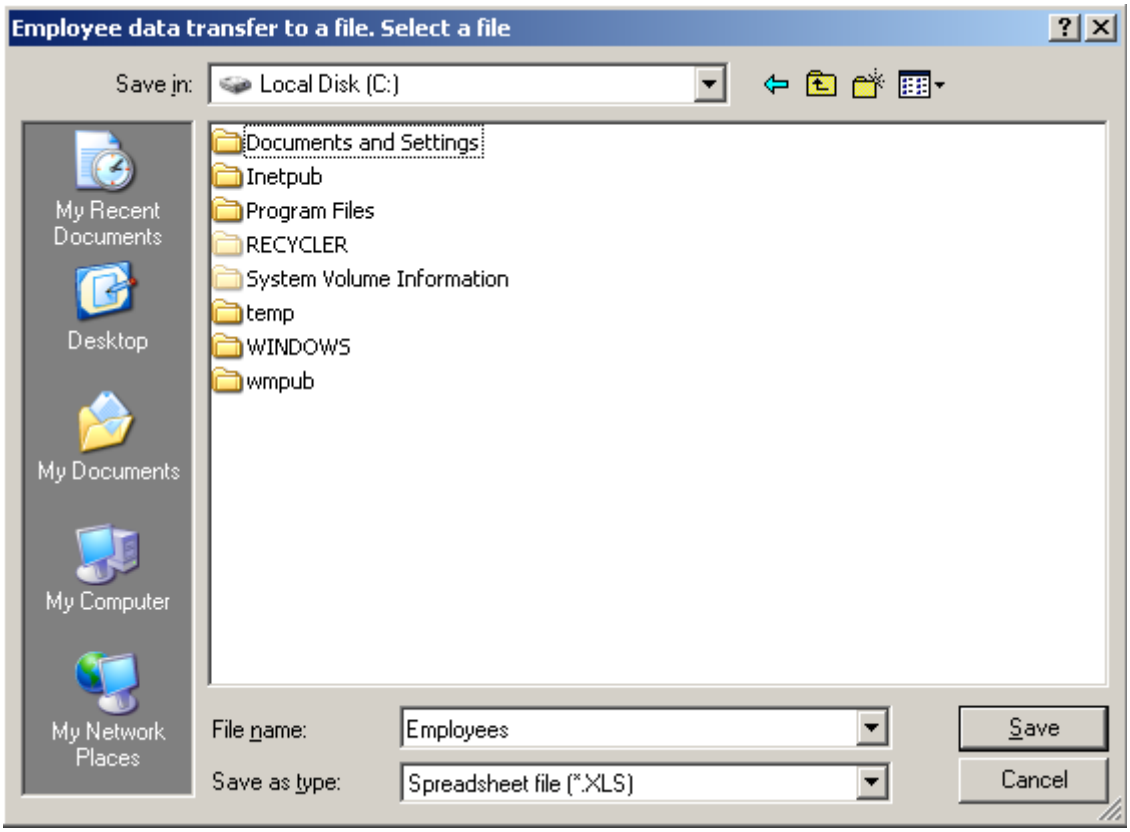
The employees can be exported into files of the following formats:



- ***.XLS** — Excel document format (default setting);
- ***.HTML** — WEB-page format;
- ***.RTF** — Word document format;
- ***.CVS** — Text document format;
- ***.TXT** — Text document format.

To export employees:

1. Click on the **Employee Export** button —  .
2. Select the disc and the folder in the opened Export window, specify the file name and extension and click on the Save button:



The employee data will be exported into the specified file.

Entering an ID number

Not all access cards are issued with their ID numbers visible on the front or rear of the card. In view of this, the software allows for two options of entering an ID number:

- receiving an ID number from a controller
- manual entering of an ID number.

Receiving an ID number from a controller

If just a number is shown on the card or no identifying information whatsoever is visible, the only way of receiving an ID number is via a controller.

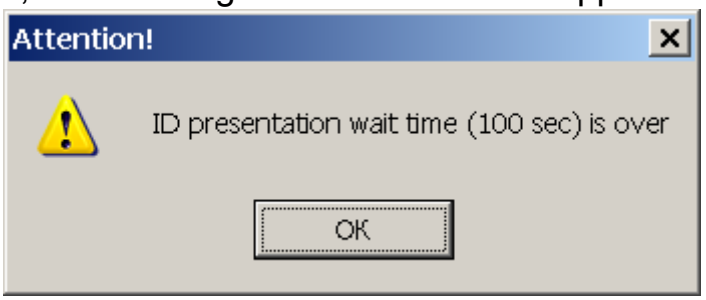
The controller should be configured before receiving an ID number (refer to the Configuration section, the Controller configuration subsection).

To receive an ID number from a controller:

1. Enter the employee/ visitor information into the Full Name column.
2. Click on the Receive ID from Controller button —  . The process of ID number receiving is displayed in the status line.
3. Present the card to the card reader of the controller selected in the Configuration section. The process of receiving an ID number is accompanied by

flashing light indication and an audio signal on the controller. To cancel receiving of an ID number, click on the Cancel in the status line:

4. If, during the pre-installed period of time of 100 seconds, the card is not presented to the reader, the following information window appears on the screen:



5.Click on the **OK button**.

6. If this operation is successful, the values the system received from the access card are shown in the **Facility Code** and **Number** columns:

Full Name	Facility Code	Number	Access	Status	Guard ON	Guard OFF
Kevin Johnson	1	31	Allowed	Employee	Denied	Denied

7. Click on the **Transfer to Controller** button for correct completion of the operation.

NOTE

ID numbers from the controller are received successively, card by card, with the row to enter a new ID number received from the controller chosen with the cursor. For the next ID number, choose the row with the employee name to enter the ID number and repeat the above procedure.

Manual entering of an ID number

If the card series and number are visible, they can be entered manually through the row with am employee/ visitor data:

Enter the card series into the Facility Code column. If the first digits are nulls, they will not be visible in the table and are not necessarily to be entered.

Enter the visible card number into the Number column. If the first digits are nulls, they will not be shown in the table and are also not necessarily to be entered.

Facility Code	Number	Access
1	31	Allowed
1	32	Allowed
1	33	Allowed
1	93	Denied

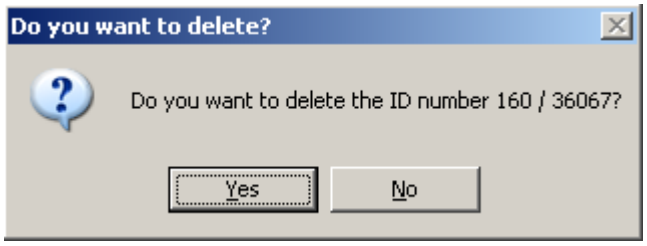
Click on the Transfer to Controller button.

The employee/visitor access card is ready for use.

Deleting an ID number

To delete an ID number from the controller:

1. Highlight any box in the row with the ID number to be deleted.
2. Click on the **Delete ID from Controller button** —  . The below confirmation window will appear:



Confirm the deletion by clicking on the Yes button. Data from the **Facility code** and **Number** columns will be deleted.

3. The ID number will be deleted from the controller.

Employee/visitor photo

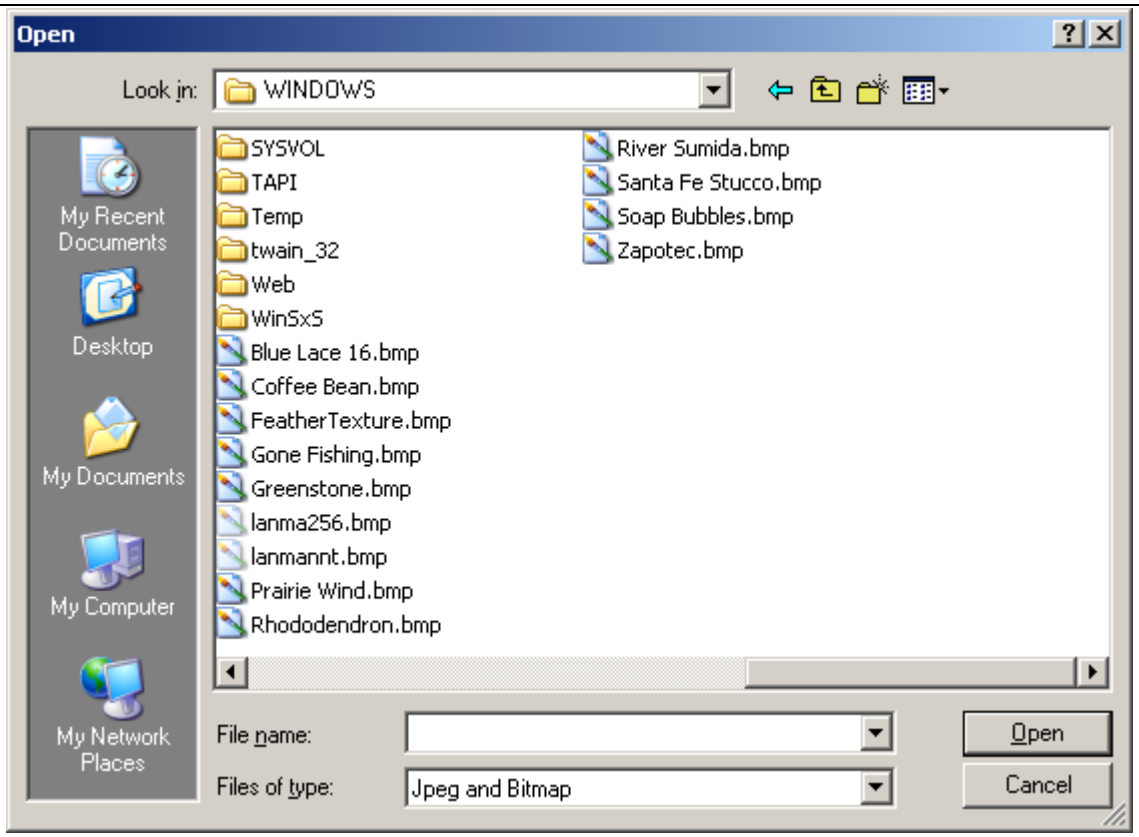
The software allows saving and deleting photos of employees /visitors. The software also provides the feature of displaying or hiding an employee/a visitor photo.

Uploading a photo

In order to be unloaded, the employee photo file should be in one of the following graphic formats: *.jpg or *.bmp. The photo uploading sequence is as follows:
Choose the row with the employee/visitor data you want a photo to be uploaded or changed for.

1. Click on the Photo displaying ON/OFF button —  . The photo upload bar will appear in the right part of list:

2.Click on the Upload Photo button —  . The standard file selector window will appear:



3.Select the folder and the appropriate photo file and click on the Open button.

4. The employee/visitor photo will be shown in the photo view area:

Full Name	Facility Code	Number	Access	Status	Guard ON	Guard OFF
Ali Karter	160	36386	Allowed	Visitor	Denied	Denied
Andrew Barkley	1	32	Allowed	Employee	Denied	Denied
John Higgins	160	36466	Allowed	Visitor	Denied	Denied
John Starks	1	93	Denied	Employee	Denied	Denied
Kevin Johnson	1	31	Allowed	Employee	Denied	Denied
Mark Selby	160	36067	Allowed	Employee	Denied	Denied
Samanta Johnson	1	33	Allowed	Visitor	Denied	Denied

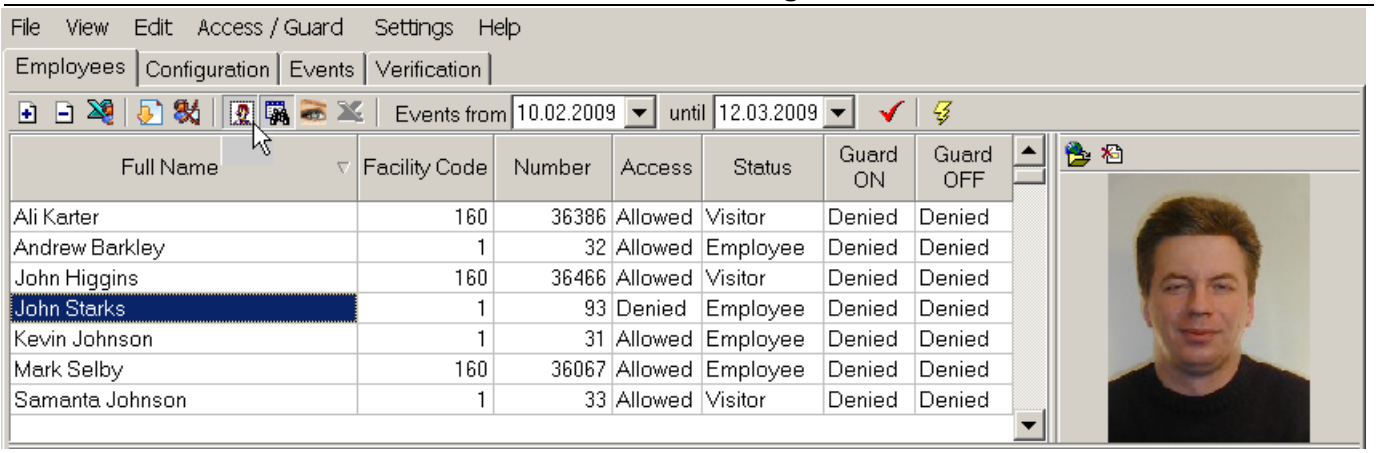
5. Click on the Transfer to Controller button to save the changes.
The employee/visitor photo will be saved into the database.

Deleting a photo

To delete an employee/ visitor photo:
Choose the row with data of the employee / visitor to be deleted. The photo displaying feature should be active (the Photo displaying ON/OFF button — is pressed). Click the Delete photo button on the photo view area. The photo is deleted from the photo view area.

Photo displaying activation/deactivation

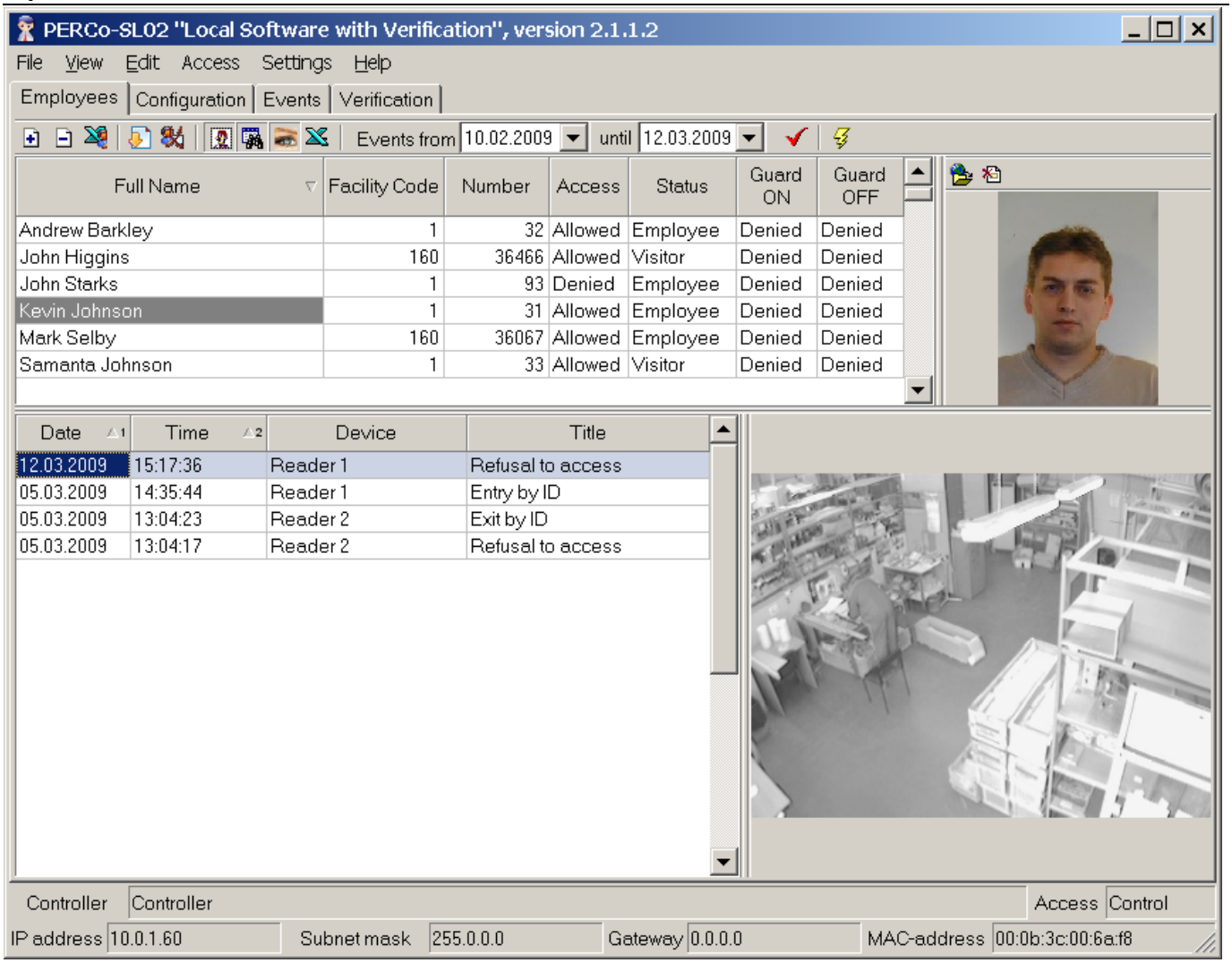
To enable using the Photo displaying activation/deactivation feature, the photo should be uploaded to the system (refer to the Uploading a photo subsection above). Use the Photo displaying ON/OFF button — to activate/ deactivate the Photo displaying activation/deactivation feature:



Video frame activation/deactivation

The software provides the feature of displaying video frames received from a video camera when the system is in the Indication/Verification mode (refer to the Selection of Indication/Verification mode subsection in the Verification section), for example when an employee is passing through an operating device (OD). Select a video camera in the Configuration section to display a video frame (refer to the Video camera selection/deactivation section below) and proceed as follows:

1. Choose the row with an employee/ visitor data and activate the Event viewing mode by clicking on the Show Events button - . An event list for the selected employee/visitor will appear at the bottom of the window.
2. Click on the Update Event List button — to get the most recent event list.
3. Click on the Video Frame ON/OFF button — in the functional toolbar. The video frame view area will appear on the right side of the event list.
4. Choose an event in the list. A video frame taken by the video camera at the moment of this event will appear:



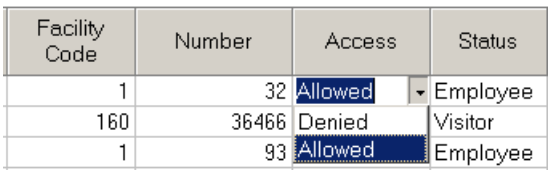
NOTE

If both the Photo Displaying and the Video Frame modes are active, both images are visible in the Employee section window.

Access authorization/denial

For all employees/visitors access is allowed by default in a set operating mode (refer to the Access Modes section). Proceed as follows to change this setting:

1. Choose the row with the employee/visitor data and the operating mode to be changed.
2. Choose the Access column and click on the Allowed option. The arrow of the dropdown list will appear on the right side of the column.
3. Click on the arrow and choose the **Denied** option in the list:



4. Click on the **Transfer to Controller** button to save the changes.

5. To authorize access, follow the same procedure but choose the **Allowed** option in the list.

NOTE
Denying of access makes activation of the Guard mode impossible.

Guard mode activation/deactivation

Employees can be authorized the rights to activate or deactivate guard of the premise. The rights to activate or deactivate the Guard mode are divided so that one employee can only activate the Guard while another employee can only deactivate it.

While the Guard mode is active, access to the premise will be denied for all access cards. To allow access, the Guard mode must be deactivated.

To activate or deactivate the Guard mode, an authorized access card should be presented twice to the reader while the door is closed. Alternating blinking of the yellow and red LED indicators confirm that the guard of the facility is active. While on default, features of activation or deactivation of the guard are not allowed:

Status	Guard ON	Guard OFF
Employee	Denied	Denied
Visitor	Denied	Denied
Employee	Denied	Denied
Employee	Denied	Denied

To authorize the right of activation or deactivation of the guard:

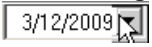
1. Choose the **Guard ON** or **Guard OFF** column in the row of the employee to be assigned the right to activate or deactivate the premise guard.
2. Click on the **Denied** option. Click on the arrow of the dropdown list on the right and chose the **Allowed** option:

Status	Guard ON	Guard OFF
Employee	Denied	Denied
Visitor	Denied	Denied
Employee	Allowed	Denied
Employee	Denied	Denied

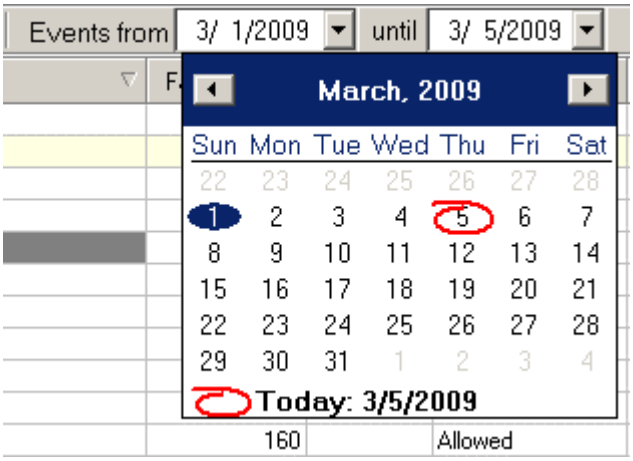
3. Click on the **Transfer to Controller** button  to save the changes.
4. Follow the same procedure to disable the right of activation or deactivation of the premise guard but choose the **Denied** option.

Event viewing

The software enables viewing of events related to activities of a selected employee over a specified period of time.

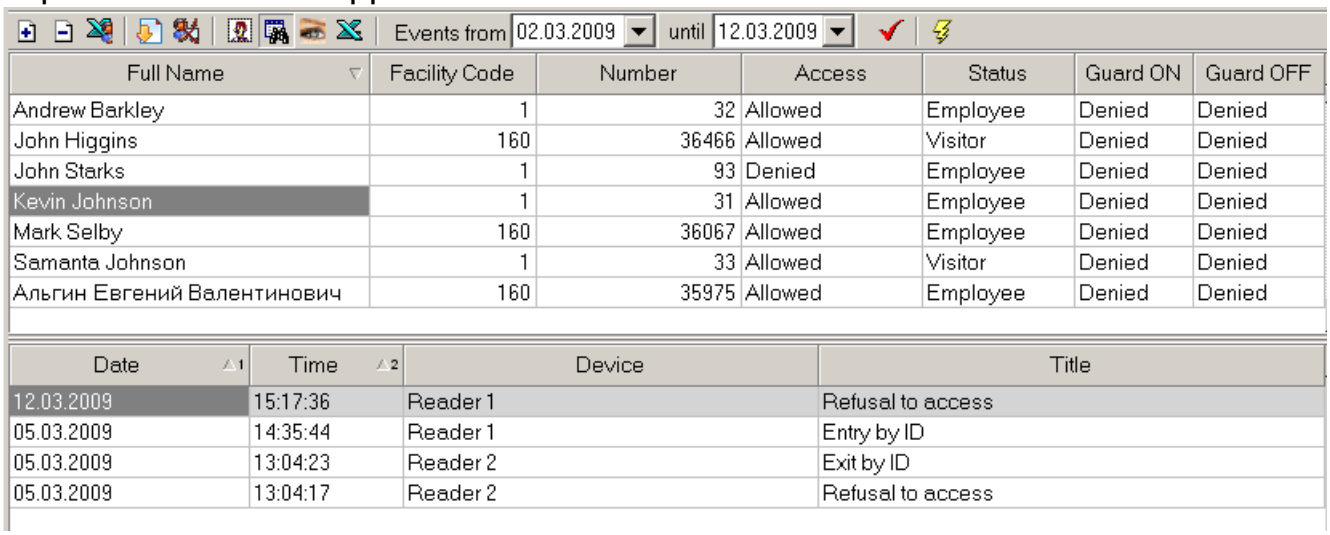
1. Enter the initial viewing date manually or by clicking on the left arrow of the date field in the event viewing time setting box **Events since … until…**, located above the list of the employees: 

2. Choose the initial viewing date by the below calendar:



3. Repeat the procedure to set the final viewing date in the right date field. While on default, this field automatically shows the current date.

4. Choose the row with the specified employee data and click on the Show Events button. An additional window with the event list over the specified period of time will appear:



Full Name	Facility Code	Number	Access	Status	Guard ON	Guard OFF
Andrew Barkley	1	32	Allowed	Employee	Denied	Denied
John Higgins	160	36466	Allowed	Visitor	Denied	Denied
John Starks	1	93	Denied	Employee	Denied	Denied
Kevin Johnson	1	31	Allowed	Employee	Denied	Denied
Mark Selby	160	36067	Allowed	Employee	Denied	Denied
Samanta Johnson	1	33	Allowed	Visitor	Denied	Denied
Альгин Евгений Валентинович	160	35975	Allowed	Employee	Denied	Denied

Date	Time	Device	Title
12.03.2009	15:17:36	Reader 1	Refusal to access
05.03.2009	14:35:44	Reader 1	Entry by ID
05.03.2009	13:04:23	Reader 2	Exit by ID
05.03.2009	13:04:17	Reader 2	Refusal to access

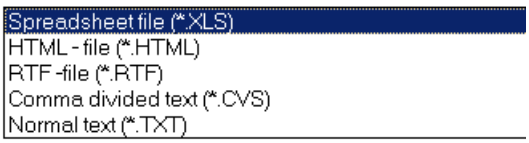
5. Use the Update Event List button for periodical updates of the list. This button is active only in the Event viewing mode.

6. Activate the Video Frame activation mode to display a video frame for a specific (refer to the Video Frame ON/OFF section).

7. Click again on the Show Events button to leave the viewing mode.

Event export

The event log of a selected employee / visitor over a specified period of time can be saved into a file of the following formats:



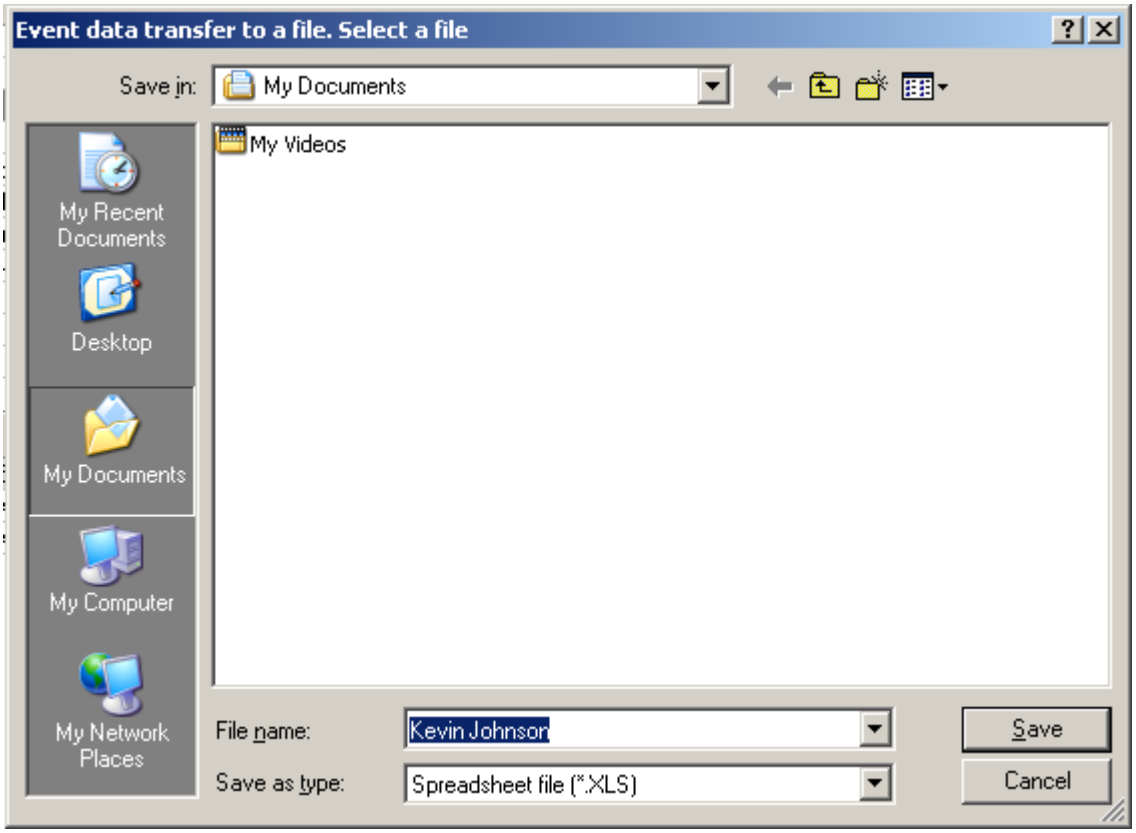
*.**XLS** — Excel document format (default setting);

*.**HTML** — WEB-page format;

*.RTF — Word document format;
*.CVS — Text document format;
*.TXT — Text document format.

To export events:

1. Choose the row with the employee/visitor data in the table.
2. Specify the event viewing period (refer to the Event Viewing section above).
3. Click on the Show Events button to display the event log. Click on the Event List Update — to refresh the event list.
4. Click on the Event **Export button** — in the File Menu. Select the disc and folder in the opened window, specify the file name and format, click on the Save button:



Event data will be exported into the specified file.

CONFIGURATION

The Configuration section refers to settings of the system hardware: controllers, readers, operating devices, video cameras. Click on the **Configuration** tab.

Configuration section work window

The Configuration section work window looks as follows:

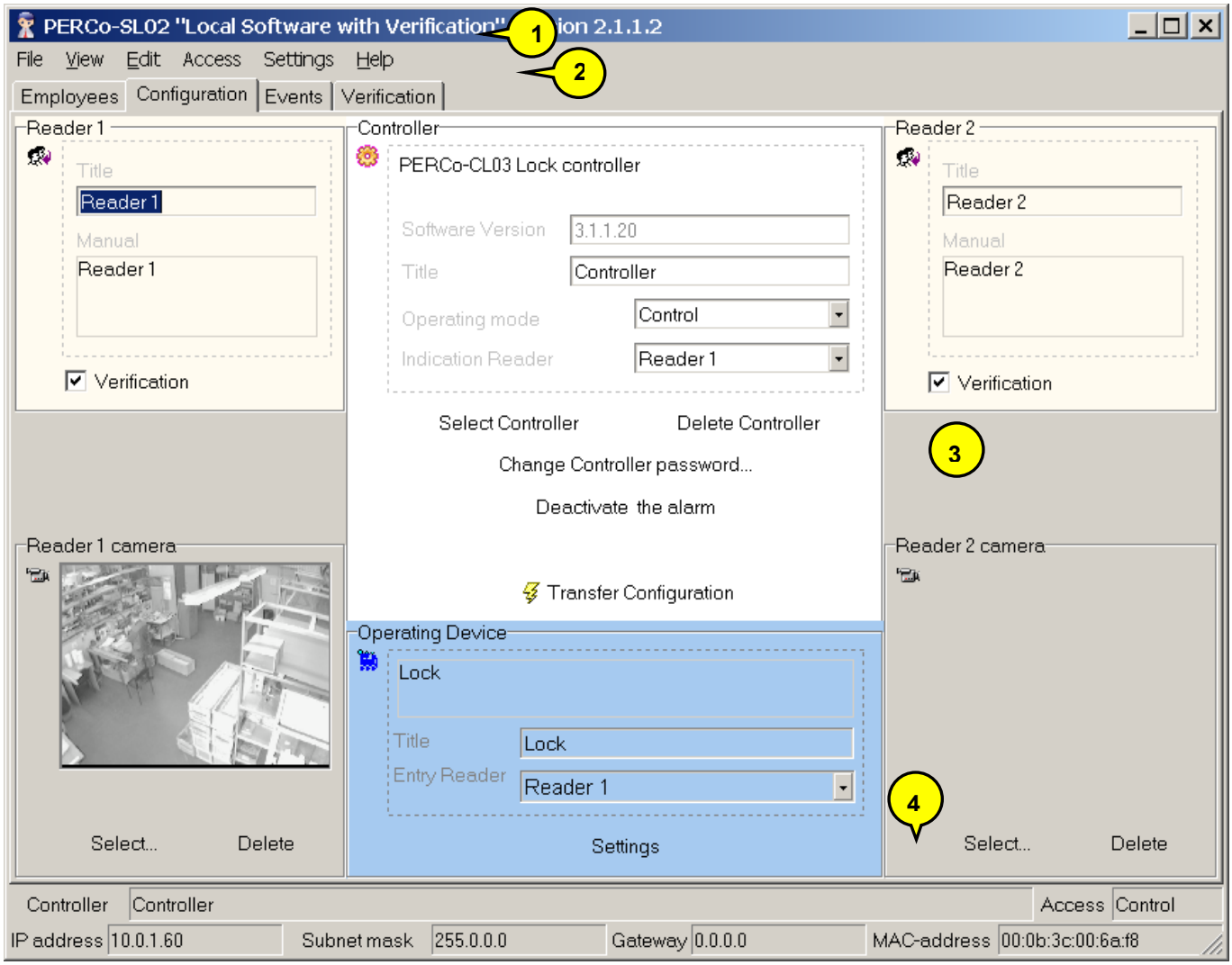


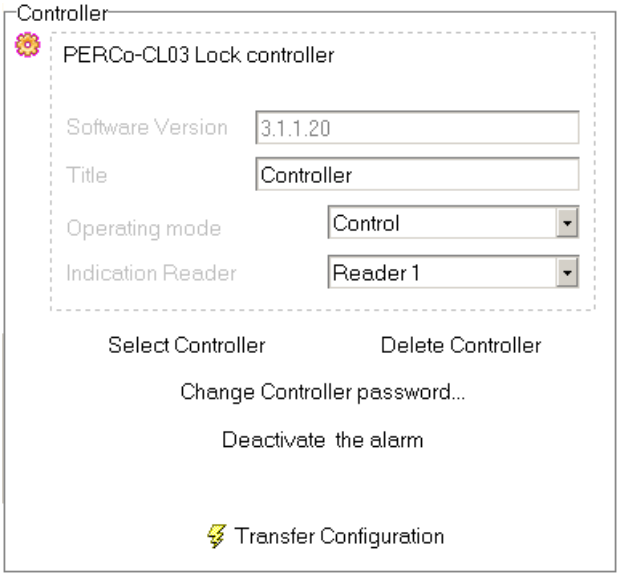
Fig.2. Configuration section work window

1. The top of the window contains the Main menu. Use the **Access** menu for configuration of the access cards' rights.
2. Section tabs of the following sections are located under the Main menu: **Employees**, **Configuration**, **Events**, **Verification**.
3. The central part of the window contains the desktop with the hardware settings windows for a controller, a reader (or, depending on the controller type, two readers), an operating device and video camera selection windows.

4. The bottom of the work window contains a status line to display the service information (status of the controller, access mode, IP-address, etc.)

Controller configuration

Regardless of the number of the controllers installed at the enterprise, the software enables real time operation with only one selected controller. In order to activate another controller, the current controller should be deactivated and another one chosen from the list. The settings are modified in the **Controller** window:



Window elements

The **Title** text field is meant for a descriptive name of a controller, for instance **the main entrance controller**. This provides the operator with information about the selected controller in a convenient form when there are several controllers in the system (refer to the NOTE to the Reader window section below).

The operator cannot enter any information via the **Title** text field of the controller window; this information is transferred from the hardware to identify a unique device, for instance the **CL03 lock controller**.

Use the **Operating mode** dropdown list for selection of the appropriate operating mode of the controller. This operating mode will determine access of employees through the operating device served by this controller. Click on the list arrow and select the required mode:

NOTE

Use the remote control panel or the **Access** option of the Main menu for a quick change of the operating mode (refer to the fig. 2 description). Refer to the Operating modes section for further details about the operating modes.

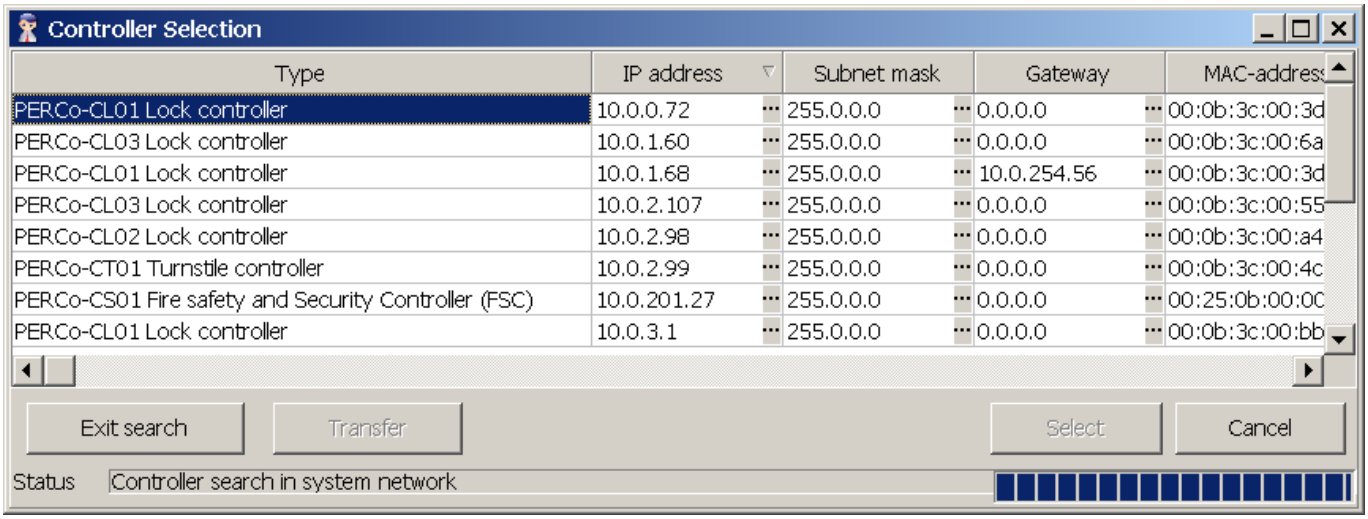
The name of the reader connected to the controller is selected in the **Reader ID** text field, e.g**. Reader 1** that can be used as an ID-number reader during an employee

access card issue (refer to the Receiving an ID number from a controller subsection) in the **Employees** section. The selected reader name will be employed during the current and successive sessions provided that the controller was not deleted or changed (refer to NOTE to the Reader window section below).

Controller selection

The software enables real time operation with only one selected controller. Select one controller if there are several controllers installed in the system. Each controller comes as a network device, with its own IP-address.

1. Click on the Select Controller button. The **Controller selection** window with the list of all devices installed in the system will appear on the screen:



2. When the window is open, an automatic search for all controllers in the network will start, the search flow being displayed in the status line at the bottom of the window. The list contains all the controllers found in the network.

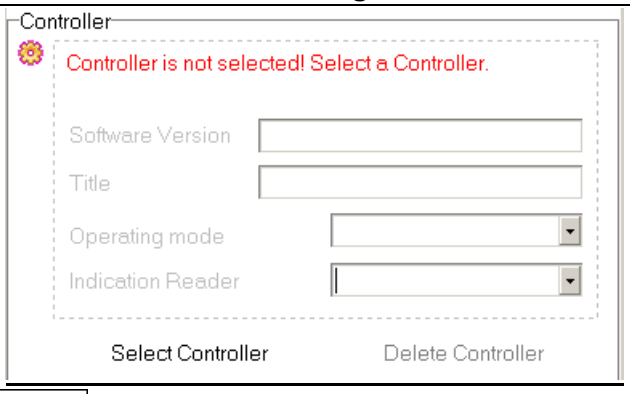
   This search may take a long time with a large number of controllers connected to the network. When a required controller is found, the search can be stopped by clicking on the Exit Search button. For selection, click on the row of the required controller and push the Select button.

3. Click on the Transfer Configuration button to save the settings into the system.

Controller change

The Delete Controller button is not meant for deleting a controller from the system configuration but for deactivating of the current controller and subsequent selection of another controller. To change a controller:

1. Click on the Delete Controller button. All data in the window fields will be deleted while a message that no controller is selected will appear in the **Declaration** field:



2. Click on the Select Controller button to select another controller and repeat the procedure given in the Controller selection subsection above.
3. Click on the Transfer Configuration button to save the settings into the system.

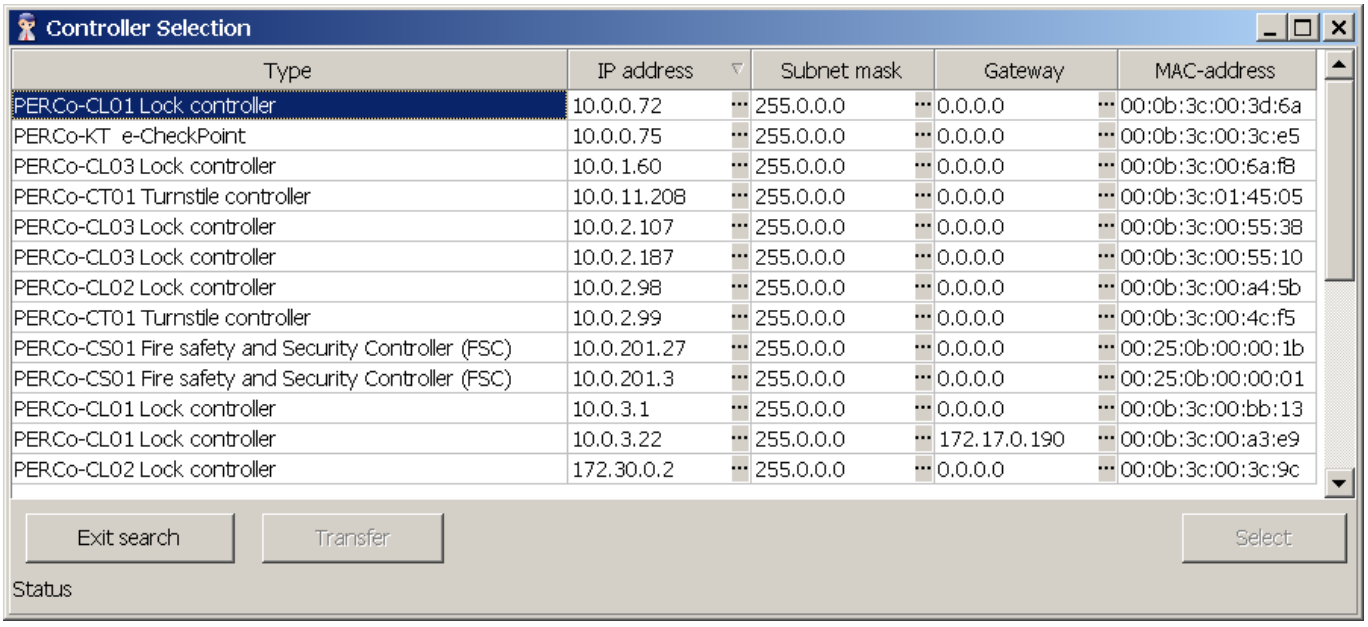
Change of controller settings

Settings of a controller that can be changed are as follows:

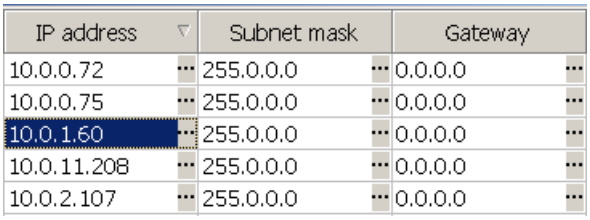
- IP-address;
- Subnetwork mask;
- Gateway.

To change any of the above settings:

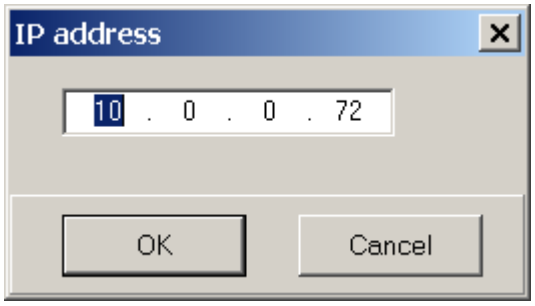
1. Open **Controller selection** window:



2. Choose the controller row in the column with changing settings and click on the ... button on the right side of the current value:



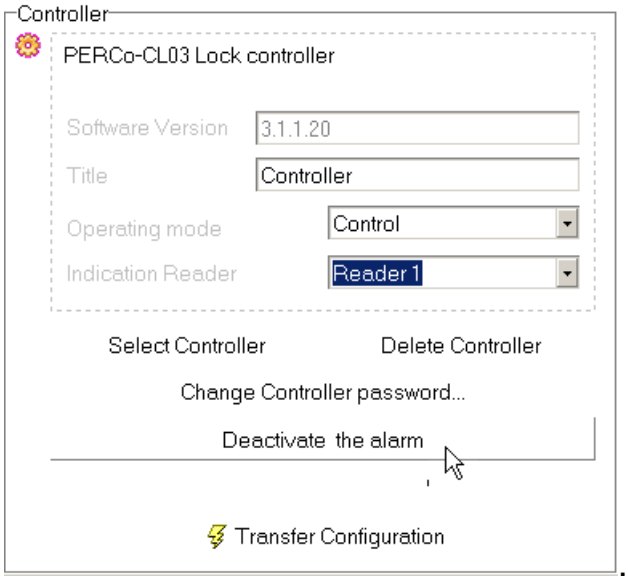
3. An **IP-address** window will appear:



4. Enter new values and click on the **OK** button.
5. Click on the Transfer button in the **Controller selection** window.
6. Click on the Transfer Configuration button to save the settings into the system.

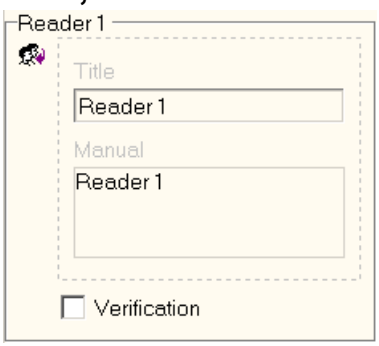
Alarm deactivation

The system can be in the alarm state. Click on the Deactivate Alarm button to deactivate the alarm:



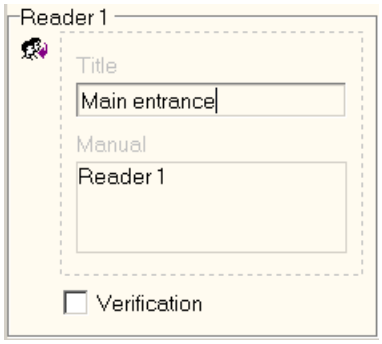
Reader window

Depending on the controller type, one or two readers can be connected to it. The **Reader** window provides the description of a specific reader connected to a specified controller. Two text fields**, Manual** and **Title** are used for this purpose:



A text in the **Manual** field cannot be changed as it is transferred from the hardware and serves for identification of a unique device.

The **Title** field is used for entering of specifying information about the reader location, e.g., Reader 1: at the **Main Entrance**:



This information will be reflected in the corresponding **Controller, Camera for [Reader 1]** and **Operating device** windows as well as in the **Verification** section window**.**

NOTE

Information, entered in the **Title** fields of every device windows, is saved during all current session as well as at the ending of the software operation and its successive run. When deleting (changing) a controller, information entered by the Operator in the **Title** field is replaced by default data (in this particular case—Reader 1).

The Reader window contains very important functional element – the **Verification** check box:

It is used for switching between the **Indication** and **Verification** modes in the Verification section. For further details, refer to the Selecting Indication/Verification mode subsection in the «*verification*» Section below.

Video camera selection/deactivation

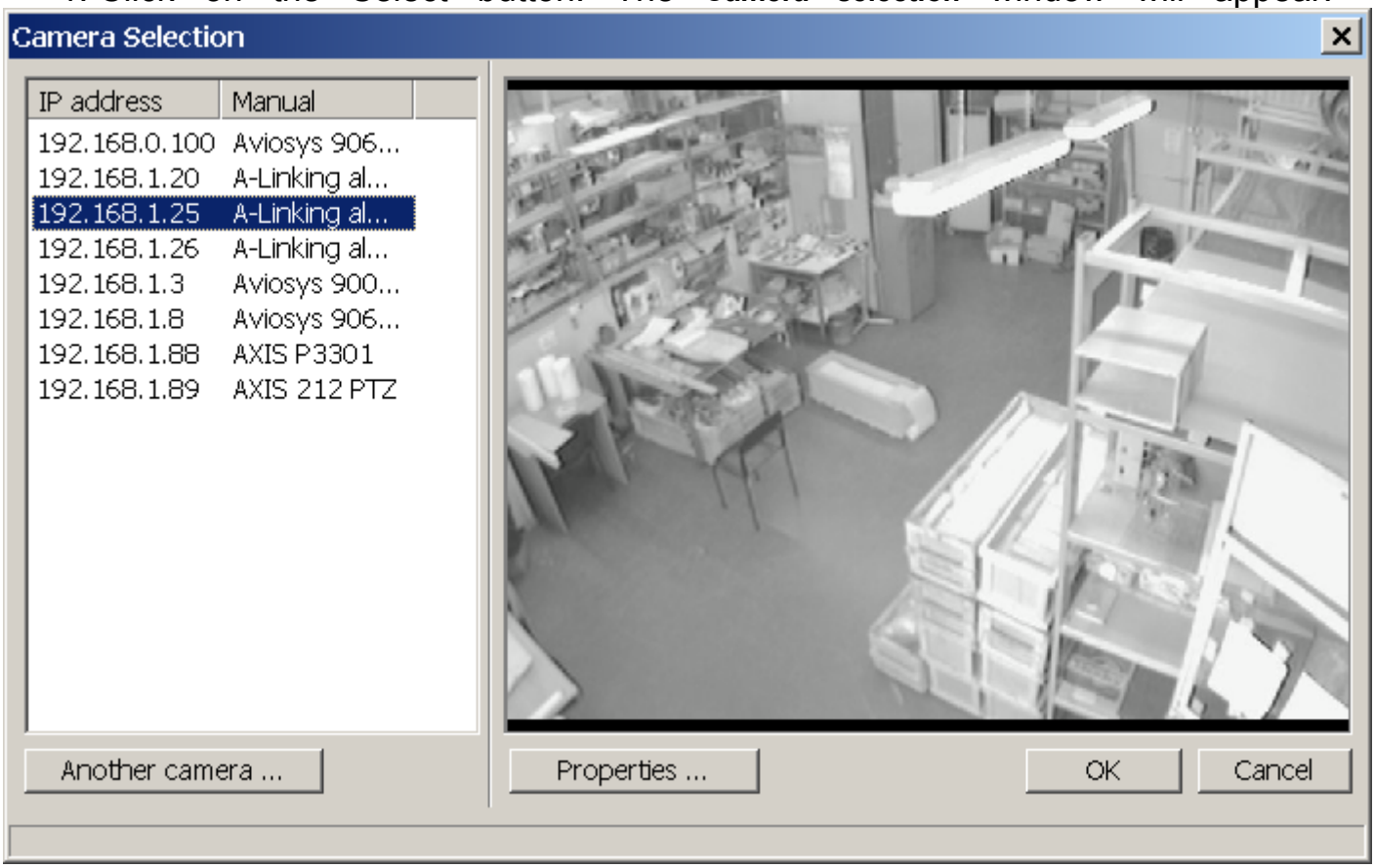
The system provides the feature of selecting a video camera to transmit information that will be displayed when an access card is presented to a specified reader in the Verification/Indication modes. As far as the system is concerned, each video camera is a network device with its own IP-address.

Selection of a video camera for a specified reader is made in the **Camera for [Reader1]** window:

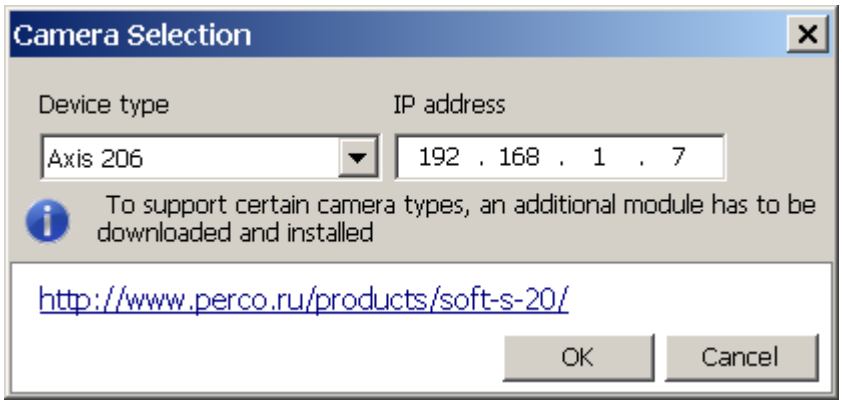
No video camera is selected at the software start.

To **select** a video camera:

1. Click on the Select button. The **Camera selection** window will appear:



In a few seconds the list of cameras will show the addresses for the found cameras. If by some reason the wanted camera is not found automatically, the User can add it manually by clicking the **Another camera…** button:



Select the camera type in the dialog box and enter its IP-address.

When the camera is selected, some of its settings can be determined by the **Settings**: User name, password, operating mode and port. Please refer to the camera documentation as these settings depend on the manufacturer and the camera model.

NOTE

Some types of cameras will require installation of a special support module. Ask the module from your dealer or download it from PERCo website where you can also get the list of supported hardware.

2.The right part of the window shows an image transmitted from the selected video camera. Click on the OK button to confirm the selection. A dynamically changing image from the video camera and some additional camera information (subject to camera type) will appear in the **Camera for [Reader1]** window. The received video frames will be displayed in the Verification section window.

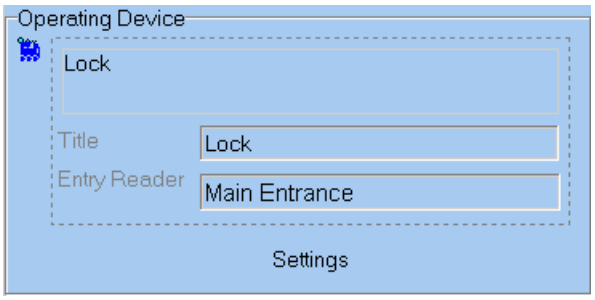
To **deactivate** image transmission from the video camera:

1. Click on **Delete** button:

2. The image and camera information will disappear and the **Camera for [Reader1]** window will return to its original appearance: (refer to the figure in the beginning of this section).

Operating Device configuration

Various operating devices can be connected to a controller: electromagnetic and electromechanical locks, turnstiles and other hardware. Such connected devices should be properly configured. For this purpose use the **Operating device** window in the Configuration section:



Operating device window elements

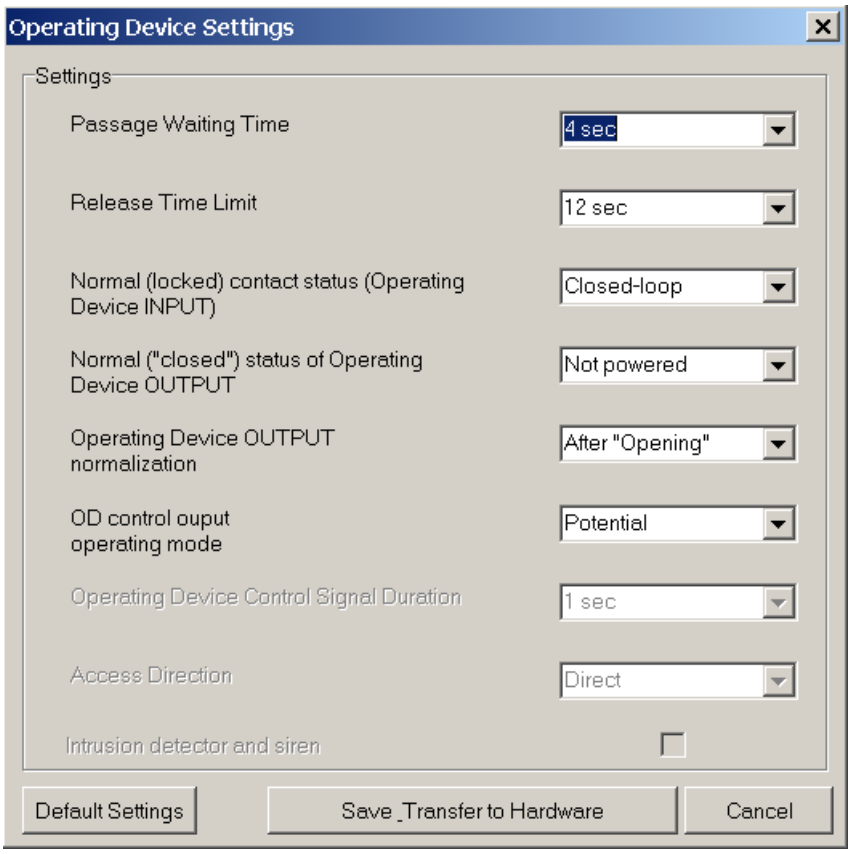
The **on** text field is used for entering of a descriptive name of an operating device (OD), e.g., **Lock** или **Main Entrance Turnstile**. When there are several OD's in the system, this enables fast determination which device exactly is connected to the selected controller. In this particular case, a generic name **Lock** is used as the Description.

The **Entry Reader** text field contains name of a reader that comes as the entry reader depending on the passage (access) direction selected in the **Operating Device Settings** dialog box, e.g., **Reader 1**. This name will be used during the

current and successive sessions provided that the controller is not deleted or changed (refer to NOTE to the «*Reader window*» section above).

The operator cannot enter any information via the **Title** text field of the controller window; this information is transferred from the hardware to identify a unique device, e.g. **Lock**.

The bottom part of the window contains the **Settings** button, that is used for opening of the **Operating device settings** dialog box:



Operating Device settings

The **Operating Device settings dialog box** contains several settings for installation of a specified OD realized as dropdown lists and the three buttons: On Default, Save & Transfer to Hardware and Cancel. Each operating device in the system (various locks types, turnstiles and other hardware) will have different settings. The system determines the settings automatically for all OD's, connected to the controller but the settings can be changed when necessary, in accordance with documentation for a specific operating device.

Some of the settings are interdependent. For example, if the **OD Control Output Operation mode** is **Potential,** the **OD Control pulse duration** will be unavailable.

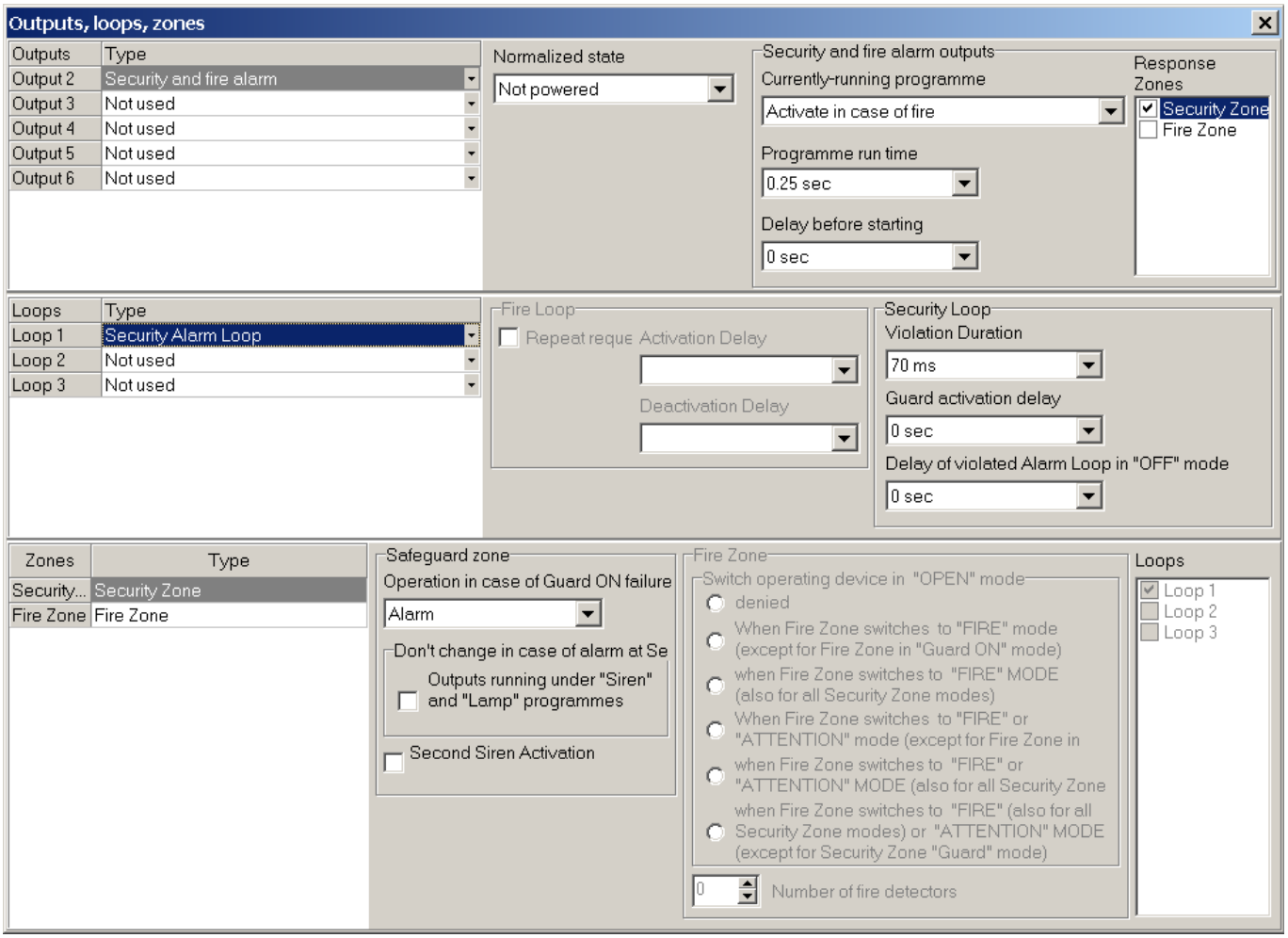
Some of the settings can be changed without referring to the documentation. For example, depending on the number of employees passing through a certain OD, the value of the **Passage waiting time** setting can be increased from **4 seconds** set on default to a higher value. The **Release time limit** setting can also be changed. This setting represents a time window after which a signal is given that the OD is not closed. In case of bidirectional access control, the **Access direction** dropdown list is used. The **Direct** option represents entrance registration by the reader selected as an entry reader in the **Operating Device Settings** dialog box and exit registration by

another reader. **The Reverse option** represents entrance and exit registration in the reverse direction. If only one reader is used, the **Access direction** setting is unavailable.

If in doubt about changing settings, use system default settings for each particular operating device.

Configuration of FACU and FSSC features

The following features are part of the FACU and the FSSC: zones, alarm loops, outputs. Their functional settings are determined by means of the **Outputs, Loops, Zones** dialog window, opened by the **FACU Features** button of the **Controller** window:



When a new the feature type is selected, its settings will appear on the right of the feature's list (Press the Enter key after selection of the feature type from the dropdown list).

The zones and loops can be related to either security or fire safety, with different settings combined under corresponding headings (**Fire** loop and **Security** loop, **Security** zone and **Fire** zone). Only settings of a selected component type can be changed.

For example, the Second Siren Activation setting is featured by both security and fire zones; therefore it is displayed in the zone list and can always be altered.

There are 2 fixed zones in the FSSC – one is always for security, another is always for fire safety. As a result, all the security loops are automatically placed into the security zone while all the fire loops are in the fire zone. For example, the Second

Siren Activation setting is featured by both security and fire zones, therefore it is displayed in the zone list and can always be altered.

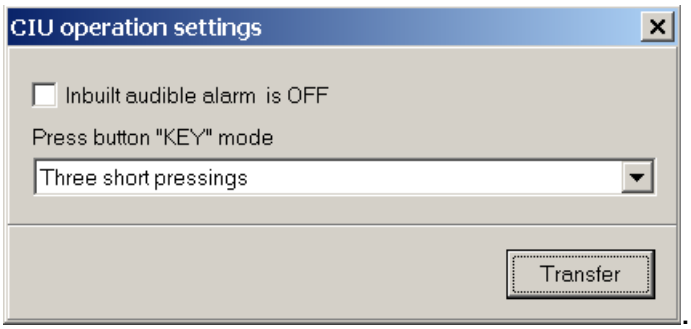
Thereby, for the FSSC the checkboxes to include the loops in the zones (the **Loops** list in the right part of the **Zones** toolbar) are disabled.

It is different for the FACU: any zone can be set as either security or fire zone. A certain loop can belong to only one zone. When the loop is included in one zone, it is automatically excluded from another zone.

The FACU has no operation device, so the “OD Switch to Open” setting makes no sense and the corresponding features are unavailable.

The operating device of the FSSC (a lock) is physically connected via the №1 Output, therefore it is absent from the list of outputs and the OD settings are determined in the same way as settings of lock and turnstile controllers (refer to the “Operating device settings” subsection).

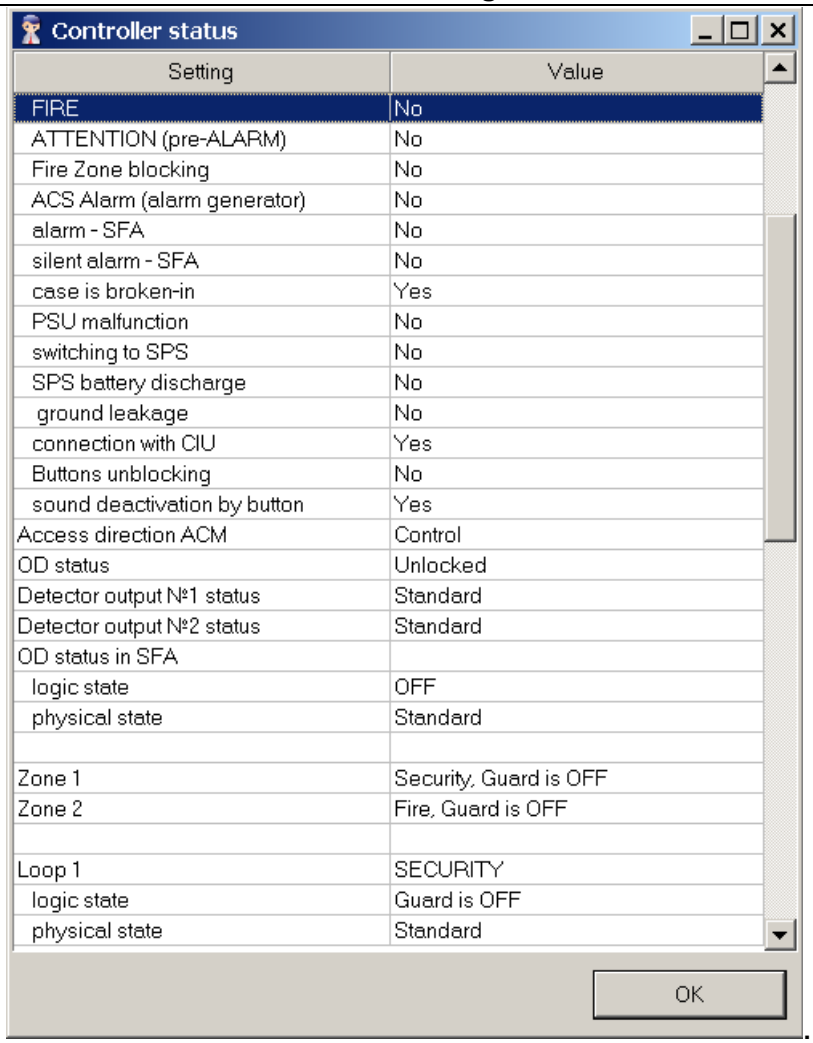
Options of the CIU (Control and Indication Unit) operation can be changed with the **Options** button:



NOTE

When the CIU inbuilt audio indicator is deactivated, it will switch on only by ACS command.

The **Status** button can help know the FACU (the FSSC) operation settings as well as the status of its features:



The Reset button is assigned a function similar to the **CIU Reset** button's: deactivation of the «Fire», «Attention», «Alarm», «Malfunction».

For more information about the FACU, the FSSC settings and the CIU functional capabilities refer to the **"S-20 Fire alarm and security control units. Operation Manual"**.

Operating modes

The system provides 5 operating modes.

Open. When this mode is activated, the operating device (OD) is unlocked and remains unlocked all time that the operating mode is active. Pressing of the remote control panel (RC) button is ignored. When an authorized card is presented, the corresponding access event is registered by the ID number. Depending on the type of the reader, the indication comes as an LED arrow or green light.

Control. This operating mode is the standard mode of the system functioning. When this mode is activated, the OD gets locked and access is possible by only those cards that conform to all the access authorization criteria.

When an authorized card is presented to the reader, the OD becomes unlocked for the passage waiting time that is set in the **Configuration** section (refer to the subsection Operating device settings above). Depending on the type of the reader, the indication comes as an LED hand-with-card icon or a green light indicator.

Closed. This mode is used for denial of access through an operating device. When this mode is active, the OD gets locked and remains locked all the time that this mode is active. Pressing of the remote control panel (RC) button is ignored. Whatever card is presented, the system registers an event of an authorized access attempt. Depending on the type of the reader, the indication comes as an LED **STOP** sign or a red light indicator.

Conference (only for lock controllers). This mode is similar to the Control mode but with different indication. The yellow and green indicators are used to inform employees that a conference is being held at the premise.

Guard. When the **Guard** mode is active, the OD gets locked and remains locked all the time that this mode is active. Pressing of the remote control panel (RC) button is ignored. Opening of the door is registered as an event of an unauthorized access through the OD.

Readers protocol

Use **Settings> Readers Protocol** of the Main menu for changing the hardware algorithm for ID processing (access controllers software):

By default the controllers use a full ID code (8 bytes maximum). It is possible to set Weigand 26 mode in which the controller works only with 3 lower bytes. This allows to define the ID in the "classic" way — breaking the number into the family code (a number less than 255) and the number (a number less than 65535). Such numbers are often seen on ID-cards.

When the universal protocol is used, the ID is presented by a single number and in all the tables (employees, event log) only one column is assigned for the ID. When the Weigand 26 protocol is used, two columns are assigned for the ID: facility code and number.

EVENTS

The Events section allows logging all events for all devices. Unlike the other sections of the software, the Events section is rather informative than functional.

Events work window

Click on the **Events** tab to open the section work window:

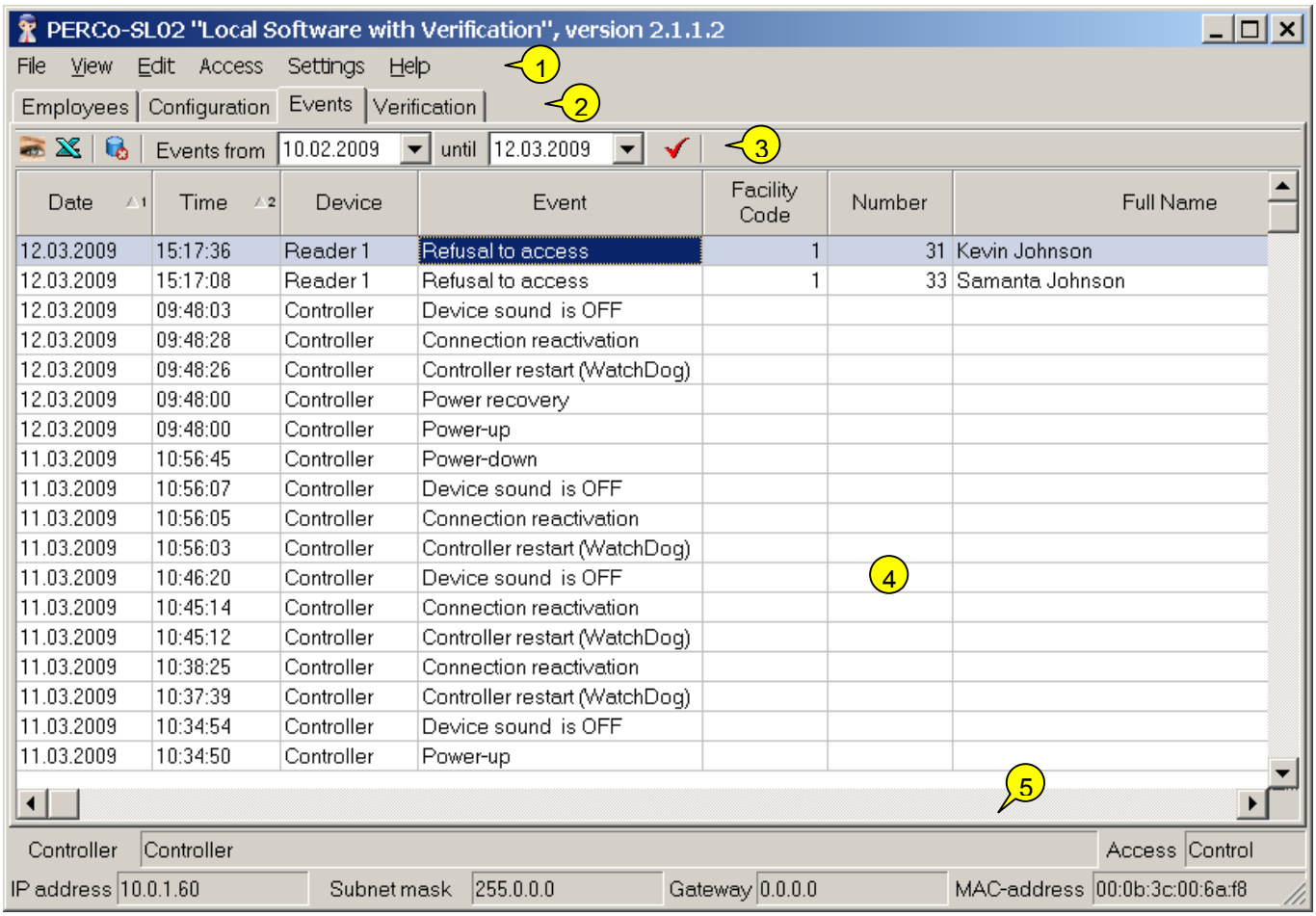


Fig.3. Events section work window

1. The top part of the window contains the Main menu. For the purpose of operating with the event log, the **File** menu is employed.
2. Tabs of the following sections are located under the Main menu:
   Employees, **Configuration**, **Events**, **Verification**.
3. Functional elements of the window are described in the Appendix 2.
4. The central part of the window contains a desktop. The data are given as a table made of several columns. Such a tabular presentation conveniently allows sorting data by various attributes in descending or ascending order. In the above figure the events are sorted in reverse chronological order i.e. the last event on top. The column order can be easily changed by dragging. Video frames will be displayed on the right.
5. The bottom of the work window contains a status line to display the service information (status of the controller, access mode, IP-address, etc.).

Video frame activation/deactivation

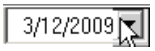
The software enables display of video frames transmitted from a video camera when the system is in the Verification / Indication mode (refer to the subsection Selection of Indication/Verification mode in the Verification section) for a specific event related to an employee access (**Access by ID number**, **Access failure, etc.**). When this mode is active, a video frame will appear in the right part of the window. To activate this mode:

1. Click on the **Video frame ON/OFF button** —  . The video frame display will appear on the right side of the list.
2. Choose the event related to the access (passage) control of a specified employee. The display will show a video frame received from the video camera at the moment of the event registration (refer to Fig. 3 of the Events work window subsection above).
3. To deactivate display of video frames, click again on the Video Frame ON/OFF button.

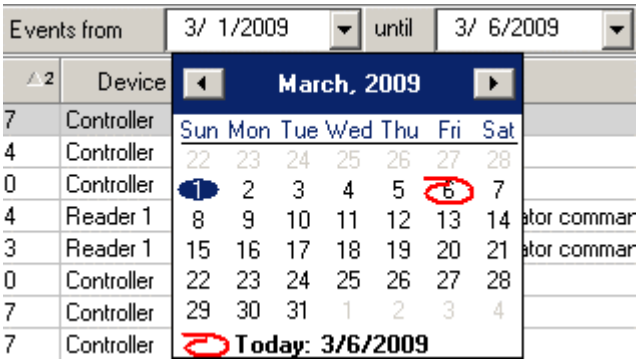
Event viewing time setting

The software enables viewing of events over a specified period of time. On default all events are automatically entered into the event log immediately after the software installation and until the present moment. To set an event viewing time value:

1. Enter the initial viewing date manually or by clicking on the left arrow of the date field in the event viewing time setting box **Events since … until…**, located above the list of the employees:



2. Choose the initial viewing date by the below calendar:



3. Repeat the procedure to set the final viewing date in the right date field. While on default, this field automatically shows the current date.
4. Use the Update Event List button for periodical updates of the list. This button is active only in the Event viewing mode.

The **Name** field is filled in with data from the database the moment of an event. Subsequent changes of the data (deletion, name or card number amendments) have no effect on past events. This enables maintaining the event history.

The types of events are displayed in the **Event** column and provide brief information on what happened at a certain moment. If the event is related to a concrete employee, the employee data is displayed in the **Facility code**, **ID number** and **Full Name** columns.

NOTE

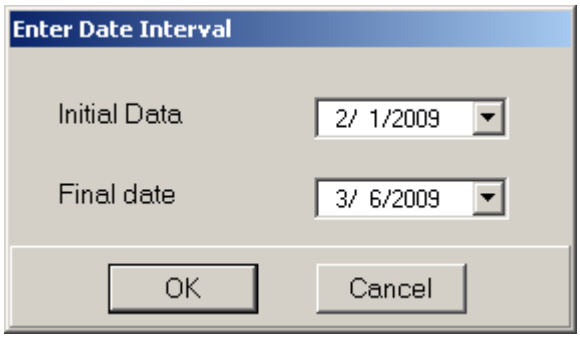
For detailed technical information on the event types refer to the technical specification of the controller you use, subsections 4.3.4.1 - 4.3.4.2.

Contact PERCo support service if you need assistance.

Event deletion

The event log size can be fast increasing. In order to delete outdated events:

1. Click on the **Delete Events button** — . The **Enter Date Interval** dialog box will appear on the screen:



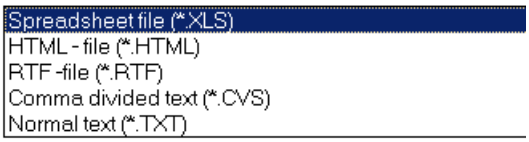
2. Set the initial and final dates of the interval manually or by means of the calendar that is opened by clicking on the arrow of the dropdown list:

3.Click on the **OK button for confirmation**.

Events over the specified time period will be deleted from the list.

Event export

An event log for a specified time period (the whole time period on default) can be saved into a file of the following formats:



*.**XLS** — Excel document format (default setting);

*.**HTML** — WEB-page format;

*.**RTF** —Word document format;

*.**CVS** — Text document format;

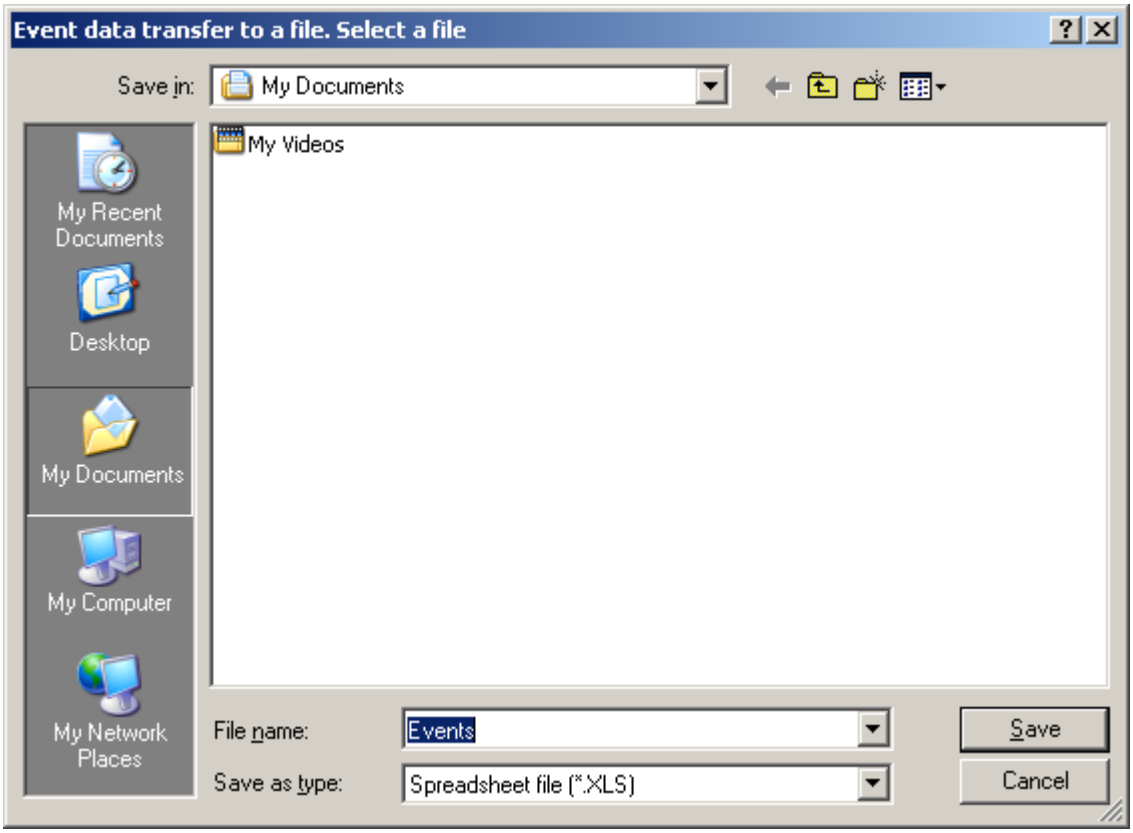
*.**TXT** — Text document format.

For event exporting:

1. Set the event viewing time if necessary (refer to the Event viewing time setting above).

2. Click on the Update Event List button to to refresh the event list.

3. Click on the Event **Export** button. In the opened export window select the disc and folder, specify the file name and extension and click on the Save button:



Events data will be exported into the specified file.

VERIFICATION

The Verification section is used for control of employee/visitor access through a specified operating device (OD), as well as for identification of employees /visitors who are authorized to activate or deactivate the premise guard. The software enables choosing either the Indication or the Verification mode described below. Click on the **Verification** tab to open the section.

Verification work window

The Verification work window will open after clicking on the Verification tab:

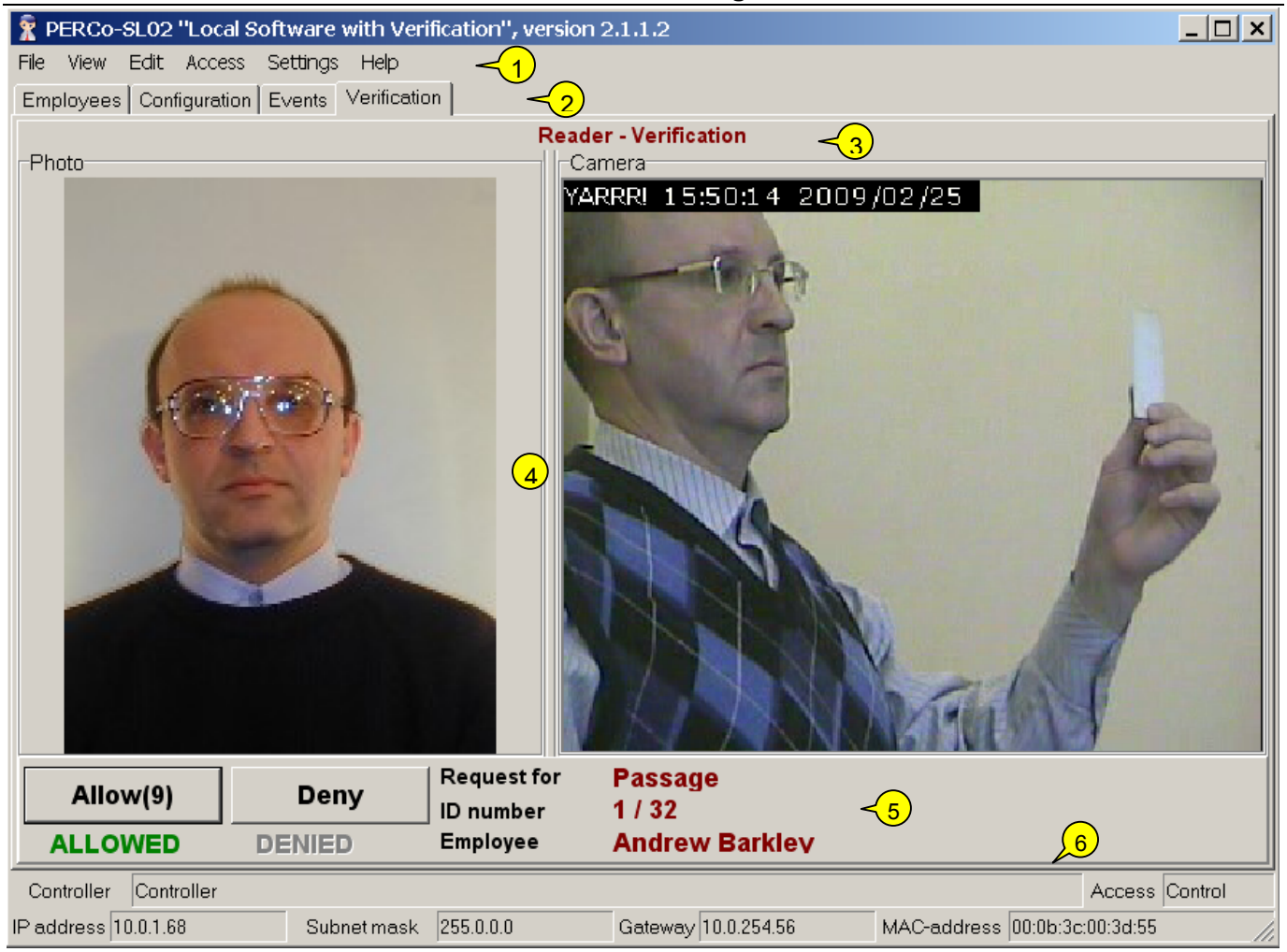


Fig.4. Verification work window

1. The top of the window contains the Main menu. The Verification mode employs the features of the **Settings** menu.
2. Tabs of the following sections are located under the Main menu: **Employees**, **Configuration**, **Events**, **Verification**.
3. Information on the connected device (**Reader 1**) and the access control mode (**Verification**). These settings are modified in the **Reader** window of the Configuration section.
4. The view area is located in the centre and consists of two windows: the employee/visitor photo display window and the video frame display.
5. The desktop is located below. Its right part displays **Event** (in the Indication mode) or **Request** (in the Verification), corresponding to the operating device connected to the selected controller, and the access card **ID number** and personal data of the employee / visitor (the **employee** field.) The left part displays access status for the employee/visitor access card: **Allowed** or **Denied**. Two buttons, Allow and Deny this employee/visitor access, are located above in the desktop (the buttons are used in the Verification mode).
6. The bottom of the work window contains a status line to display the service information (status of the controller, access mode, IP-address, etc.)

Indication and Verification modes

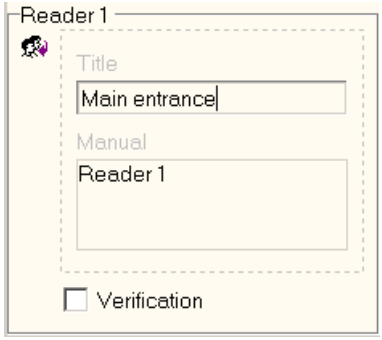
The system makes provision for two modes: Indication and Verification.

The **Indication** mode can be considered as *«an operator-unverified mode»*: decisions about either allowing or denying employee access are taken by the controller on the basis of parameters set in the **Employees** and the **Configuration** sections, with information about the presented card holder displayed in a software window together with an image transmitted from the video camera selected during the configuration.

The **Verification** mode allows decision-making by the operator on the basis of the data received by the system when an employee/visitor card is presented to a selected reader. Based on received visual (employee/visitor photo, video frame) and text information, the operator decides to either allow or deny access of this employee/visitor through the selected operating device, or activate/deactivate the premise guard (the Allow and Deny buttons). If, at the end of the time interval determined in the **Verification Settings** window (opened by the **Settings** menu command →**verification**), the operator does not take their own decision, the controller makes the decision on the basis of the parameters set in the same window. The countdown is displayed on the button corresponding to the access mode of the presented card:

Selection of Indication/Verification mode CVS Election between the modes is made in the Reader window of the Configuration section (refer to the Reader Window subsection above).

1. Click on the **Configuration** Section tab.
2. In the **Reader 1** window:



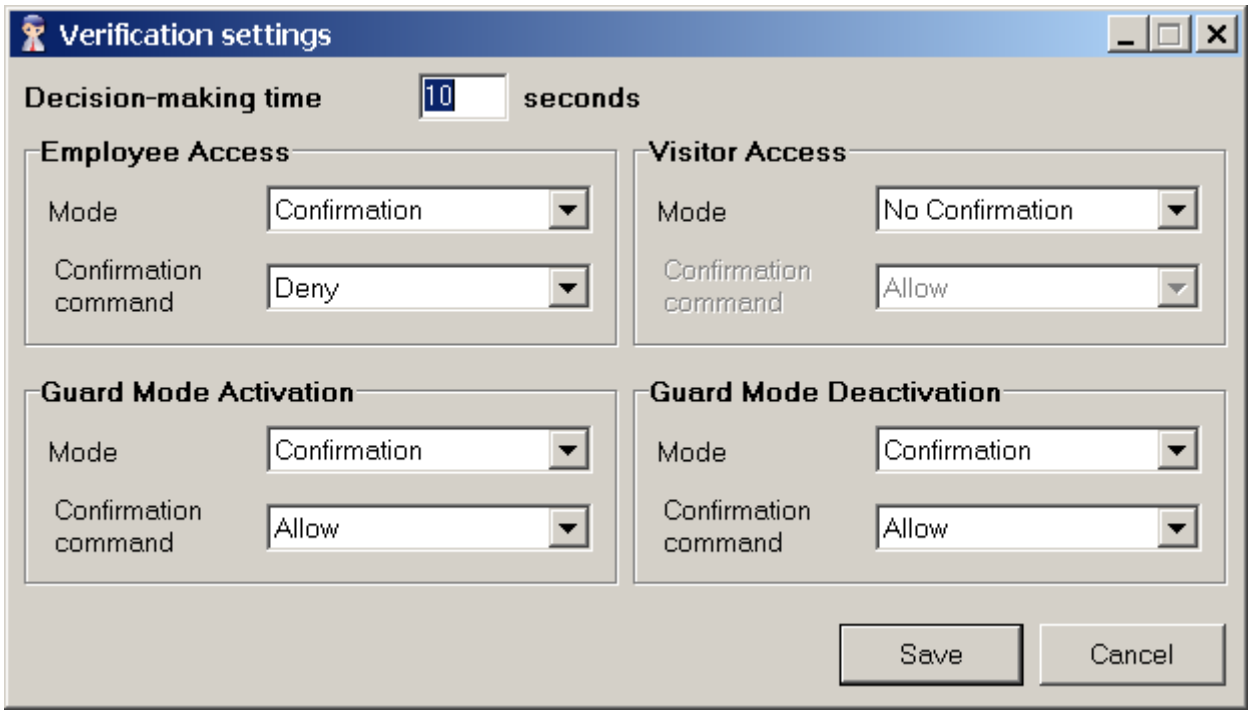
✓ tick on the **verification** check box to activate the Verification mode;
✓ tick off the **verification** check box to activate the Indication mode (this mode is active on default).

Verification settings

Verification settings are modified in the same name window.

1. Choose the **verification** option in the **Settings** menu (**Settings** → **verification**):

2. The **Verification Settings** dialog box will appear:

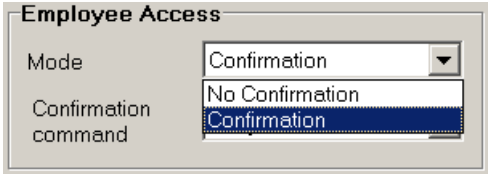


3. In the **Decision-making time** field set a time interval for the operator to enter the confirmation command (**10 sec. on default**). If no confirmation command is entered by the operator, the decision is taken by the controller on the basis of settings fixed in the Verification section windows or access rights of the employee/visitor card set in the Employees section (in the Indication mode).

NOTE

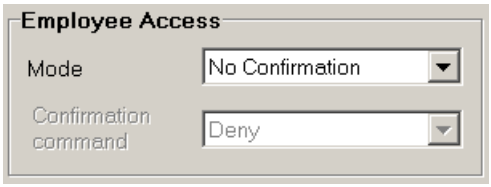
Contents of the **Employee access, Visitor access, Guard ON and Guard OFF** sections are identical. They contain 2 dropdown lists — **Mode** and **Confirmation command,** that also employ the same set of options.

4. Click on the arrow of the Mode dropdown list in the Employee access section and choose either option:



✓ The **No Confirmation** mode enables decision making by the controller on the basis of access rights of the employee/visitor card set in the Employees section. The Allow and Deny buttons are unavailable. The left part of the section desktop displays the access status of the card:

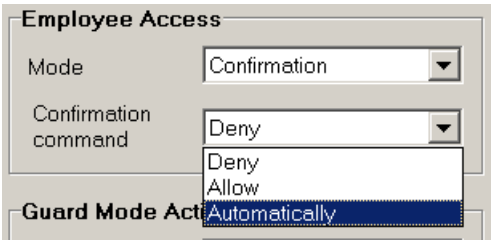
In the **No Confirmation** mode the **Confirmation Command** dropdown list is unavailable:



✓ The **Confirmation** mode enables entering the confirmation command by the operator during a preset time interval.

If, at the end of this interval, the operator does not press the **Allow(6)** or **Deny(8)** buttons, the controller employs the command set in the **Confirmation command** dropdown list. The digits in brackets right of the button name indicate the number of seconds left before the access decision should be taken.

5. In the **Confirmation CVS** mode click on the arrow of the **Confirmation Command** dropdown list to choose one of the options:



✓ The **Automatically** option is a default setting. If, during the preset time interval, the operator does not take the decision to allow / deny access or activate / deactivate the facility guard, the controller will make such a decision based on the access rights read from the employee/visitor card.

✓ **Deny** — if, during the preset time interval, the operator does not take the decision to allow / deny access or activate / deactivate the facility guard, the controller will take the **Deny** decision irrespective of the access rights of the employee/visitor card.

✓ **Allow** — if, during the preset time interval, the operator does not take the decision to allow / deny access or activate / deactivate the facility guard, the controller will take the **Allow** decision irrespective of the access rights of the employee/visitor card. Repeat the above steps for each window section or use the default software settings.

6. Click on the **Save** button to save the settings.

Photo displaying

The left side of the desktop contains the Photo window. When an access card is presented to a reader, this window displays the employee / visitor photo if this

photo is uploaded and saved in the database. For the photo uploading sequence refer to the subsection Uploading a photo in the **Employees section**.

Video frame displaying

The right part of the desktop contains the **Camera** window with dynamically changing video frames transferred from a camera selected in the **Configuration** section. The update rate depends on the video camera /server characteristics, transmission capacity and traffic load of the network, other characteristics. For the camera selection sequence refer to the Video selection/deactivation subsection in the **Configuration** section.

Access authorization/denial

In the **Indication** mode the decision about access authorization or denial is taken by the controller on basis of the access rights assigned to each concrete employee CVS / visitor in the Employees section window (refer to the subsection Access authorization/denial). In this case the software operator (the operator) will just be an observer.

In the **Verification** mode the decision is taken by the operator (the operator) during the time interval preset in the **Verification Settings** window (refer to the **Verification Settings** subsection above).

✓ Click on the 

button before the end of the preset time interval for access authorization.

✓ Click on the 

button before the end of the preset time interval for access denial.

NOTE

The operator can take a non-standard decision, e.g. authorizing access for a card with the **Denied** status (the access status is set in the Employees section (refer to the Access authorization/denial subsection).

The card status is displayed in the left part of the desktop:

If the operator (the operator) presses no button during the preset time interval, the controller takes the decision on basis of the settings fixed in the **Verification Settings** window (refer to the **Verification Settings** subsection above).

Guard activation/deactivation

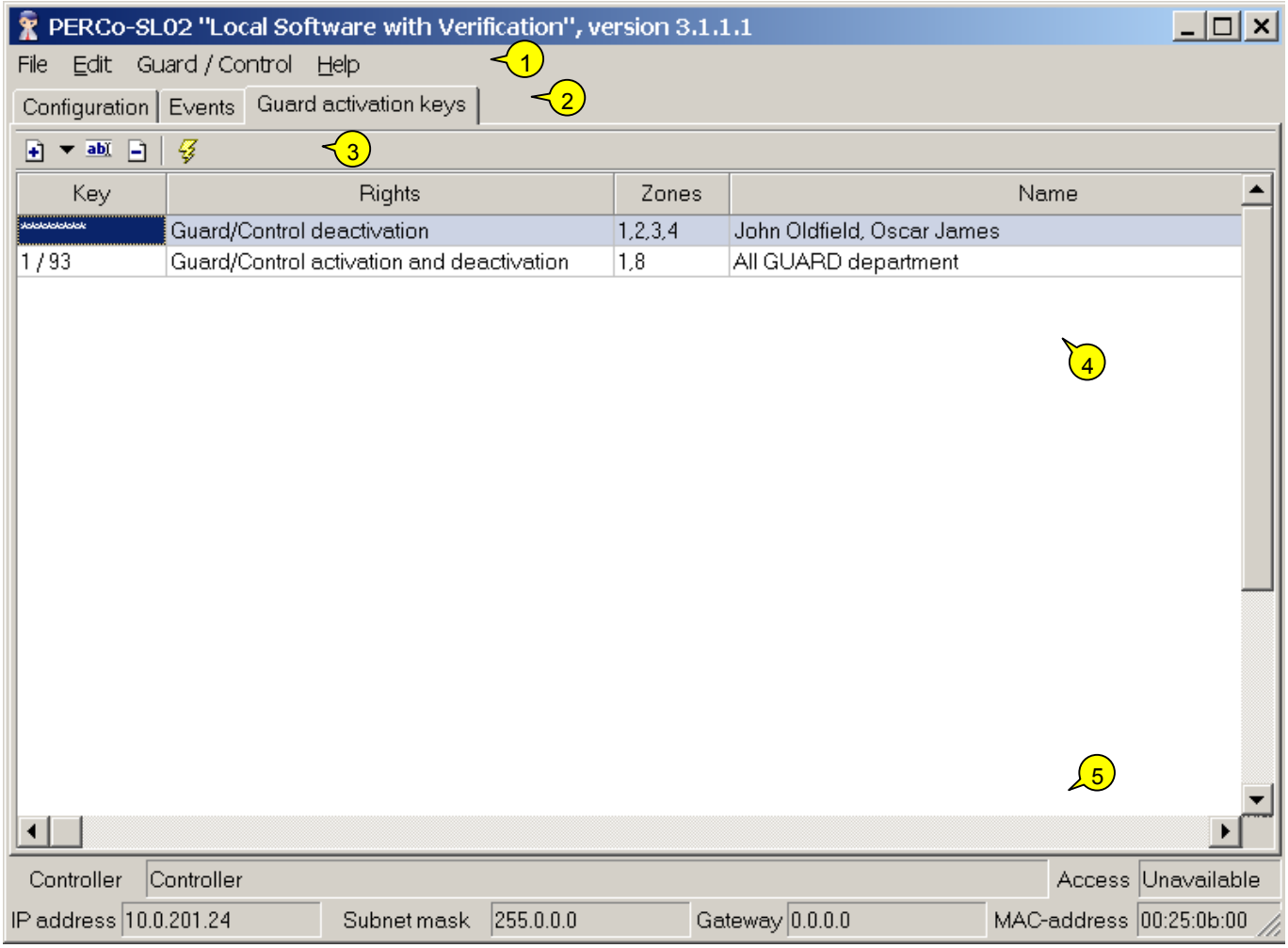
In the Verification mode the premise guard is activated as followsfirstly, the card should be presented to the reader, then after the operator's reply and change of the reader indication, the card should be presented to the reader one more time. The software operator can activate /deactivate guard of the facility by themselves. To do this, select the **Guard ON** or **Guard OFF** option in the **Access** menu:

GUARD ACTIOVATION KEYS (SFRCU ONLY)

This section is only for creating the list of Guard activation/deactivation keys for SFRCU zones.

The key can be an ID or a combination of digits from 1 to 8 (a PIN-code, from 4 to 8 digits in a key). Use of the keys eliminates unauthorized control over the zones status (before activation/deactivation of the zones guard with CIU, SFRCU awaits either ID presentation or PIN-code entering). The maximum allowed number of keys is 200. Each key has certain designated rights (only Guard activation, only Guard deactivation, only Guard activation/deactivation) and a selection of zones (and consequently, a selection of the related alarm loops) to operate by means of the key. The key can be tied with a random text, for example names of the employees authorized to use it. This text will be visible in the "Name" column (ref. section "EVENTS") for events connected to guard activation/deactivation by key.

To open the section click the **Guard activation keys** tab. The work window of the section will be as follows:



1. The top part of the work window contains the main menu.

2. Under the main menu the tab of the following sections are located: **Configuration, Events**, **Guard activation keys**.

3. Functional elements of the window are described in «**Appendix 3**».

4. The central part of the work window contains **the desktop** – the list of keys. The data is given as a table consisting of several columns with different functions. Such representation method allows sorting of the data by various criteria in descending or ascending order. When a key is added/ changed, a bar with the key's parameters will be visible at the bottom of the work window.

5. The lower part of the work window contains the status line, displaying the service information (the controller status, access mode, IP- address, etc.).

Adding a key

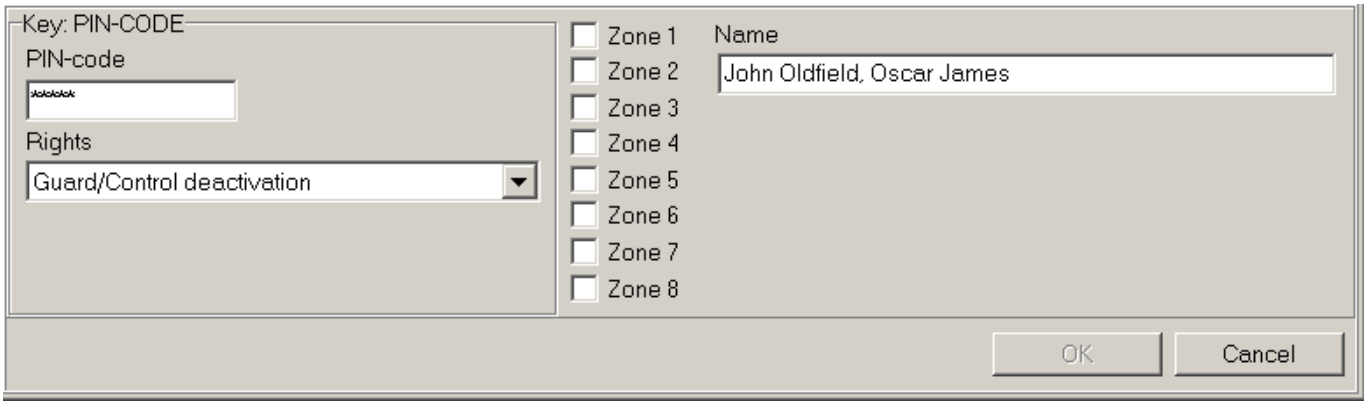
The key list is empty upon installation.

To add a key:

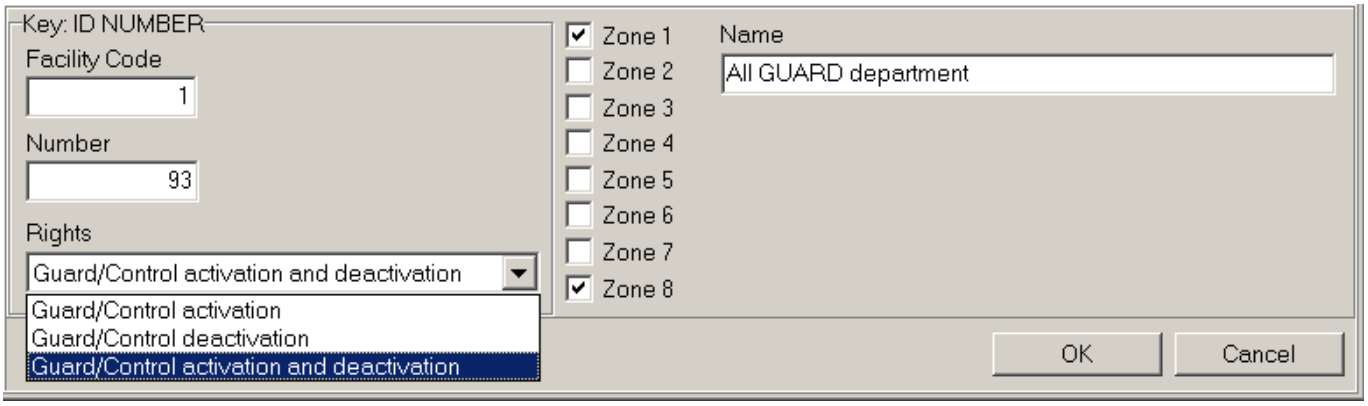
1. Click on the arrow on the right of the button (add a key). After that, a menu to select the key type will be highlighted:

2. Once the key type is selected, the bar to enter the key parameters will appear in the bottom part of the work window (the bar composition depends on the key type):

For a PIN-code key

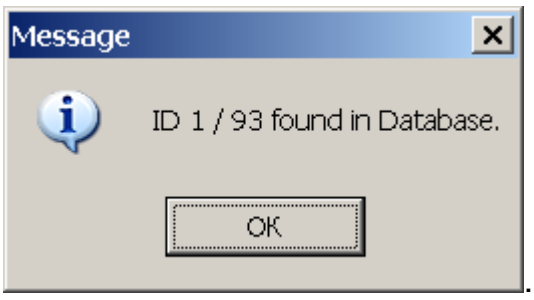


For an ID key



The obligatory parameters are PIN-code (the facility code and the number for the identifying key) and selection of at least one zone. Once the parameters are determined, the “OK” saving the key in the data base becomes available.

The software checks the uniqueness of the key (inside ID’s of the selected type), and shows the below window when a duplicate is being saved:



Changing a key

To change a key, click on the  **Change** button. The bar with the key parameters will be visible, same as when a key is being. The type of the key cannot be changed here.

Deletion of a key

To delete a key from the list (from the data base):

1. Select any cell in the line with data of the key to be deleted and click on the **Delete** button — .
2. Click the «**Yes**» button in the appearing dialog box.

Transfer of key into SFRCU

To transfer the keys list into SFRCU, click the button.

The result of the transfer (successful or faulty transfer) will be displayed in the status line.

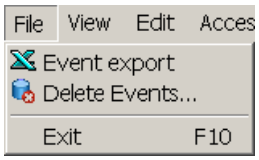
For detailed information on use of the key refer to the document **"S-20 Security and Fire safety Receiving and Control Units. Operation Manual".**

FINISHING OPERATION

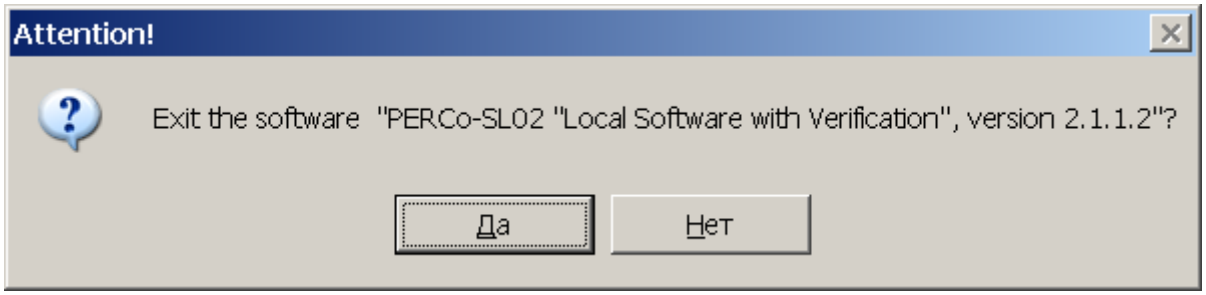
To finish the operation and exit the software:

1. Transfer all unsaved data to the controller by clicking on the Transfer to Controller button.
2. Click on the Close button in the row of the heading

or perform the following sequence of commands **File →Exit**:



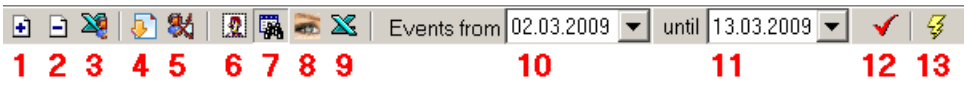
3. Click on the Yes button in the exit dialog box:



The software will be closed.

APPENDIX 1

The Employees section functional elements.



1 — **Add Employee**

2 — **Delete Employee**

3 — **Export employee**

4 — Receive **ID from Controller**

5 — **Delete ID from Controller**

6 — Photo Displaying ON/OFF

7 — Show **Events**

8 — Video Frame ON/OFF

9 — Event Export

10 — Initial Event Viewing Date

11 — Final Event Viewing Date (the current date on default)

12 — Update Event List

13 — Transfer to Controller

APPENDIX 2

The Events section functional elements.

1 — Video Frame ON/OFF

2 — Event **Export**

3 — **Delete Events over a period**

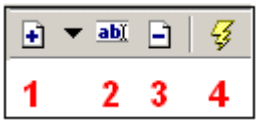
4 — Initial Event Viewing Date

5 — Final Event Viewing Date (the current date on default)

6 — Update the **Event List**

APPENDIX 3

The Guard activation keys (SFRCU only) section functional elements.



1 — **Add a key**

2 — **Change a key**

3 — **Change a key**

4 — Transfer of keys into SFRCU

PERCo Industrial

Tel.: +7 812 3216172, +7 812 3298924
Fax: +7 812 2923608

Legal address:
123-V ul. Leona Pozemskogo,
Pskov, 180600, Russia

e-mail: support@perco.ru

www.percoweb.com

PERCo®

www.perco.ru