# GuardLight

## WORKING TIME RECORDING SYSTEM

## USER'S GUIDE

ironLogic

2022

# Table of Contents


**APLICATION** ..... **4**
**SYSTEM REQUIREMENTS** ..... **4**
**OPERATION** ..... **4**
**SYSTEM COMPOSITION** ..... **5**
**SOFTWARE INSTALLATION** ..... **5**
**HARDWARE INSTALLATION AND CONFIGURATION** ..... **7**
Installing drivers for Z-397 Guard converter and reader Z-2 USB ..... 7
Configuring converter Z-397 WEB ..... 9
Configuring controller Z-5R WEB ..... 9
Configuring controller Matrix II Wi-Fi ..... 12
**LICENSE** ..... **14**
License Options ..... 14
Purchase and ordering procedure ..... 14
License installation ..... 15
**SOFTWARE DESCRIPTION** ..... **17**
Main menu ..... 17
*Database* ..... *17*
*Department* ..... *17*
*Employee* ..... *17*
*Converters* ..... *17*
*Controllers* ..... *18*
*Reports* ..... *18*
*Help* ..... *18*
Software logo ..... 19
«Database» panel ..... 19
«Enable fire safety mode» button ..... 19
«Report» panel ..... 20
Tab bar ..... 20
*«Database tools» tab* ..... *20*
*«Events» tab* ..... *20*
*«Converters» tab* ..... *21*
*«Controllers» tab* ..... *21*
**HOW TO START THE SOFTWARE** ..... **22**
Startup parameters ..... 22
«Master» mode ..... 23
«Monitor» mode ..... 23
«Guard» mode ..... 23
«Object» mode ..... 25
Automatic startup ..... 27
**POPULATING THE DATABASE** ..... **28**
Main terms ..... 28
Database population sequence ..... 28
«Converters» tab ..... 28
*Server mode* ..... *29*
*Client mode* ..... *29*
*Converter firmware updates* ..... *30*
«Controllers» tab ..... 30
*Main parameters* ..... *31*
*Extended Mode and software configuration of controllers* ..... *31*
*Software configuration sensor and devices* ..... *32*
*Controller Z-5R Net in the Extended Mode* ..... *33*
*Firmware update* ..... *33*
*Terminal description* ..... *33*

*Controller Z-5R WEB* ..... *34*
*Terminal description* ..... *34*
*Configuration* ..... *35*
*Types of Extended Mode pass points* ..... *36*
*Advanced Extended Mode features* ..... *39*
*Controller firmware updates* ..... *41*
«Database tools» tab ..... 42
*List of departments* ..... *42*
*List of employees* ..... *43*
*Search for an employee in the database* ..... *46*
*«Information» panel* ..... *47*
«Database» main menu ..... 50
*Overwrite everything in controllers* ..... *50*
*Backup copy* ..... *50*
*Delete unknown cards* ..... *51*
*Search for lost cards* ..... *51*
*Exporting the list of employees* ..... *51*
*Importing the list of employees* ..... *52*
*Administrators* ..... *53*
**ACCESS MODES ..... 56**
Reasons for introducing access modes ..... 56
Overview of Access Modes ..... 56
Switching Access Modes ..... 56
«Normal» Access Mode ..... 57
«Blocked» Access Mode ..... 57
«Open» Access Mode ..... 58
«Waiting» Access Mode ..... 58
**REPORTS ..... 59**
Mark employees for the report ..... 59
Time interval for the report ..... 59
Information columns ..... 59
Work zones ..... 59
Report parameters ..... 59
Timesheet ..... 60
*By department* ..... *60*
*Rigorous* ..... *60*
*Free* ..... *61*
*Underwork* ..... *61*
*Overwork* ..... *61*
*Late arrivals* ..... *61*
*Early arrival* ..... *62*
*Coefficient* ..... *62*
*Tariff* ..... *63*
*Absences* ..... *63*
Net time ..... 63
Statistics ..... 64
Diagrams ..... 64
Labour discipline ..... 65
Arrivals and departures ..... 65
Movements ..... 66
Traffic ..... 66
**AUTOMATIC EVENT EXPORTING ..... 66**

# APPLICATION

The working time recording system is designed to record the time of arrival, departure and movement of employees during the working day. In addition, the system provides control of the passage through the doors fitted with lock controllers.
This is ensured as follows: each employee is given an identification card or a key fob (identifier). When entering or leaving the room, each employee must bring the identifier to the reader. Having received the card code from the reader, the controller gives the command to unlock the door lock, if such lock is installed. Thus, the time and direction of the employee's passage are recorded.
The Guard Light system allows you to:

– prepare monthly, weekly and daily reports on the duration of the actual stay of employees at work;
– identify violations of labour discipline;
– determine the current position of an employee;
– graphically display the movement of an employee throughout the day.
– promptly display changes in the employee's location;
– block the employee's cards for a specified period, for example, when the employee goes on vacation;
– use the pop-up system to inform about the movement of employees.

# SYSTEM REQUIREMENTS

The "**Guard Light**" software (hereinafter referred to as the Software) allows you to control the operation of the controllers and process the information received from them.
PC requirements:

– Windows (x32/x64) XP/Vista/7/8/8.1/10/11/Server operating system;
– disk space – 30 Mb;
– RAM – at least 2 GB;
– processor – at least 1 Ghz.

**A PC with the Windows operating system (XP – 11, Server) and software installed** allows you to upload identifier codes into the controller, as well as receive and process information about the passages of employees from it. Your PC must have one free USB port to connect the **Z-397 Guard** converter**, or the Z-397 WEB converter,** or **Z-5R WEB** and **Matrix II Wi-Fi controllers should be available via TCP/IP protocol**.

# OPERATION

The system operates as follows:
**Entry/exit using a card (or a keyboard code)** - when entering/leaving a work area, an identification card is brought to the reader (keyboard code is entered) and its code is transmitted to the controller by the reader (keyboard panel). The controller checks the existence of the card number (code) in its database, as well as the permissibility of passing according to the time zones assigned to the card, and if the access is granted, it unlocks the lock while the readers indicate the state "passage is granted" with a flashing green indicator and an intermittent sound signal.
**Exit using a button** – when the exit button is pressed, the controller unlocks the lock.

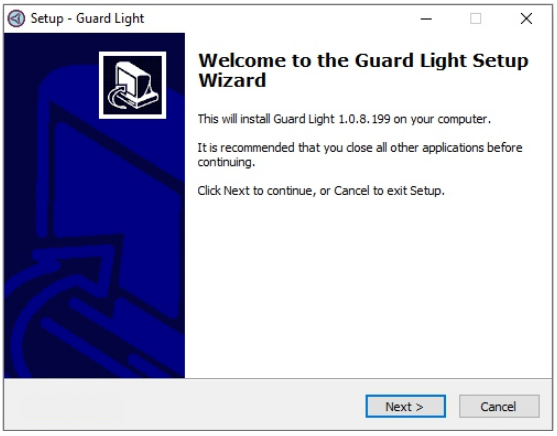
# SYSTEM COMPOSITION

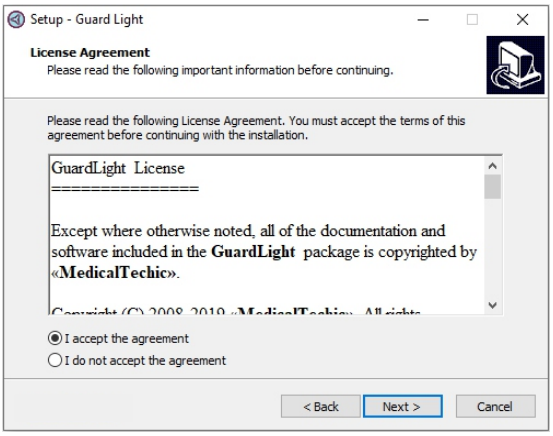
The system is based on network controllers Iron Logic **Matrix II Net, Matrix II Wi-Fi, Matrix III Net, Z-5R Net, Z-5R Net 8000, Z-5R WEB, Guard Net, Eurolock EHT, Z-5R WEB mini**. New models of network controllers are also supported as they are released by the manufacturer.
In addition to controllers, the system may include:
**RFID readers** – one or two per controller. One reader is installed at the entrance to the room and the other is installed at the exit. They read the identification code from the presented card and transmit it to the controller that controls the lock of this door. Instead of a second reader, a button can be connected to exit without control, but in this case, the passage monitoring function will not work correctly.
**Identification cards** – each employee can be assigned several cards, so their numbers allow for determining the time of his movement.
**Lock** – installed on the door and controlled by a controller. The system allows you to connect electromagnetic and electromechanical locks and electrical latches.
**Door position sensor** – installed on the door and allows the controller to record the fact of opening the door. The sensor's circuit should be closed when the door is closed and unclosed when it is opened. It is recommended to use reed sensors (balanced magnetic switches).
**Exit button** – used to open the door without a card. It is installed inside the room and also can be installed at the security post.
**Power supply unit** - provides the functioning of the controller, lock and readers. When using an uninterruptible power supply (UPS), the system will be able to perform its functions even when the room is de-energized. Battery life can be determined assuming that the consumption of the entire system **in standby mode** does not exceed one ampere when using an electromagnetic lock and less than 200 milliamperes when using an electromechanical lock. ***Important! At the time of activation, electromechanical locks consume a current that can exceed 3 amperes, so please take this into account when choosing a power supply unit.***
**Converter Z-397 Guard** - provides the conversion of the communication interface of controllers (RS-485) into a computer interface (USB) and then (using a driver) into a virtual COM port. RS-485 interface – allows you to connect devices at distances up to one kilometre. The converter is powered via a USB cable from the computer. To work with this Software, the converter must be switched to the "**Advanced**" mode.
**Converter Z-397 WEB** - provides a connection of the communication interface for controllers (RS-485) to a PC via TCP/IP (Ethernet) without creating a virtual COM port. The Software automatically detects the available converters and displays them on the "**Converters**" tab.
IP Controllers **Z-5R WEB, Matrix II Wi-Fi, Z-5R WEB mini** - connect to a PC via TCP/IP (Ethernet or Wi-Fi) without creating a virtual COM port. Logic controllers are represented by two devices: a converter (a communication module) and a controller. The Software automatically detects the available converters (communication modules) and displays them on the "**Converters**" tab.
**Reader Z-2 USB** - a desktop card reader that allows you to register new cards with the system without presenting them to an RFID reader connected to the controller.

# SOFTWARE INSTALLATION

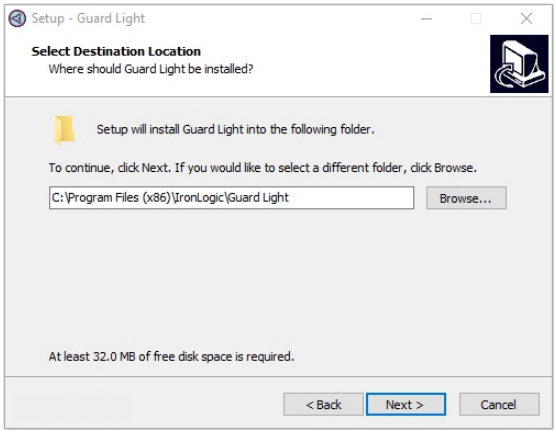
Download the archive with the Software at www.ironlogic.ru, link: Guard Light Software. Unpack the archive into a separate folder and run the installation file GuardLight_XXX_XXX_setup.exe.

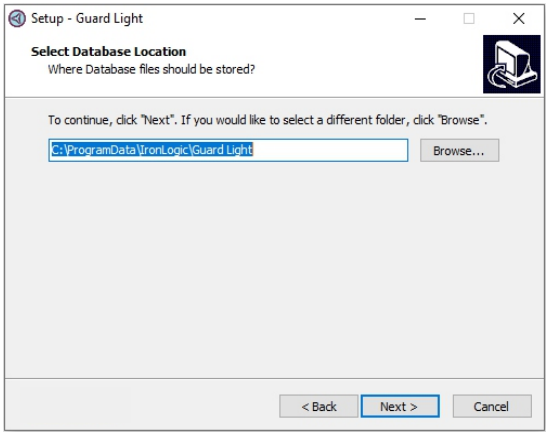
In the Software installer menu that appears, click on the "Next>" button.



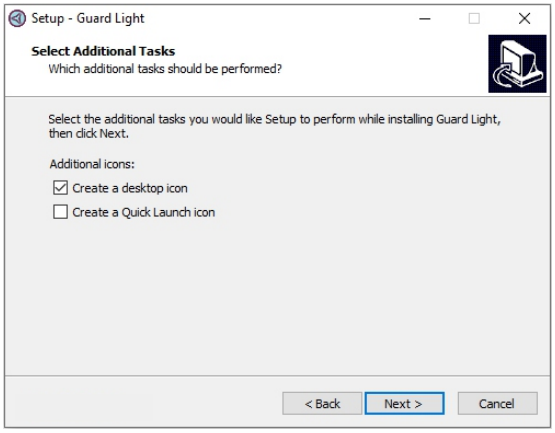

Check the box next to "I accept the agreement terms" and click on the "Next>" button.
Select the folder to install the Software by clicking on the "Browse" button. By default, the Software will be installed in the folder C:\Program Files(x86)\IronLogic\Guard Light\. We recommend that you install the Software not in the Windows system folder but in the root of drive C or D (For example: C:\IronLogic\ or D:\IronLogic\). When you reinstall the latest version of the Software, you will be prompted for a folder with the previously installed Software. Complete the selection of the installation folder by clicking on the "Next>" button.

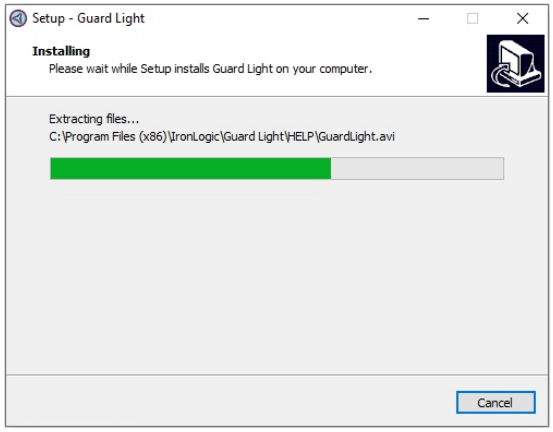


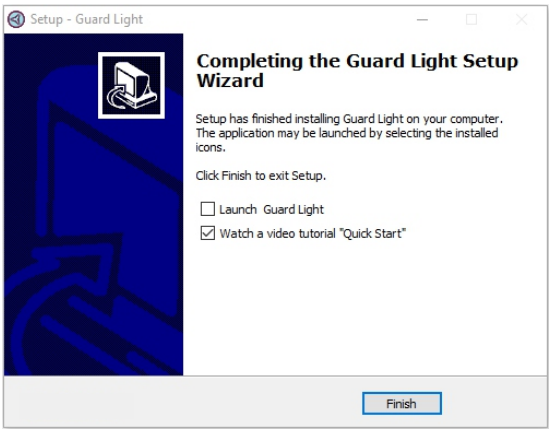

Select the folder to install the working directory of the Software by clicking on the "Browse" button. By default, the Software will be installed in the folder C:\ProgramData\IronLogic\Guard Light\. We recommend that you install the working directory not in the Windows system folder but in the root of drive C or D (For example: C:\IronLogic\ or D:\IronLogic\). When you reinstall the latest version of the Software, you will be prompted for a working directory with the previously installed Software. Complete the selection of the installation folder by clicking on the "Next>" button.

f necessary, check the "Additional icons" box and click on the "Next>" button. The Software installation bar will appear. Please wait for the installation to finish.




If necessary, after the installation is completed you can check the boxes on "Start Guard Light" or "View "Quick Start" video tutorial" and close the installer by clicking on the "Finish" button.




If you later need to update the Software version, you should close the running Software and install the latest version of the Software in the same folders.

# HARDWARE INSTALLATION AND CONFIGURATION

## *Installing drivers for Z-397 Guard converter and Z-2 USB reader*

For **Windows 8 (10)**, you need to (temporarily) disable unsigned driver blocking. How to do this - a description inside the archive with drivers. (Files: "Installing unsigned drivers in Windows 8.pdf", "Installing unsigned drivers in Windows 10_v.1.pdf", "Installing unsigned drivers in Windows 10_v.2.pdf", "Installing unsigned drivers in Windows 10_v.3.pdf").
When connecting a reader (converter) to a PC, Windows detects a new device but won't be able to install drivers.

Open the Add Hardware Wizard by clicking the message above the installation wizard icon on the taskbar or the icon itself. Prevent it from searching for a driver in Windows Updates by clicking on "Skip obtaining driver software from Windows Update."

In the menu that appears, click on the "Yes" button. A message will appear stating that the driver could not be installed. On the taskbar, the installation wizard icon will appear with a crossed red circle.
Next, you need to open Device Manager.
Select uninstalled drivers from the "*Other devices*" section (USB IronLogic RFID Reader, Z397 GUARD Converter) by double-clicking on the desired device. This will open the menu "Properties: USB IronLogic RFID Adapter". In this menu, click on the "*Update driver...*" button. In the menu that appears, select "*Browse my computer for driver software"* to find and install the driver manually.
In the menu "*Search for driver software in this location:*", click on the "*Browse...*" button and select the folder with the downloaded drivers (DRV_Win_All). Be sure to check the box "*Include subfolders*". Click on the "*Next*" button.

When installing drivers in **Windows 7 (8, 10)**, the following message will be displayed: "*Windows can't verify the publisher of this driver software.*" In this case, you must select "*Install this driver software anyway*" and continue the installation.

When the installation is complete, you will see the message "*The software update for this device completed successfully*" and "*The installation of driver software for this device is complete: USB IronLogic RFID Reader (Z397-Guard USB<->485)*". Click on the "*Close*" button.

Next, close the menu "Properties: USB IronLogic RFID Adapter" by clicking on the "*Close*" button.

The installed drivers will appear in the Device Manager under the "Universal Serial Bus (USB) Controllers" section.

After installing the USB device, "*USB Serial Port*" will appear in the "*Other Devices*" section.

You need to select it by double-clicking on the desired device. This will open the menu "Properties: USB Serial Port." In this menu, click on the "*Update driver...*" button. In the menu that appears, select "*Browse my computer for driver software"* to find and install the driver manually.

In the menu "*Search for driver software in this location:*", click on the "*Browse...*" button and select the folder with the downloaded drivers (DRV_Win_All). Be sure to check the box "*Include subfolders*". Click on the "*Next*" button.

When installing drivers in Windows 7 (8, 10), the following message will be displayed: "*Windows can't verify the publisher of this driver software.*" In this case, you must select "*Install this driver software anyway*" and continue the installation.

When the installation is complete, you will see the message "*The software update for this device completed successfully*" and "*The installation of driver software for this device is complete: USB IronLogic RFID Reader (Z397-Guard USB<->485)*". Click on the "*Close*" button.

Next, close the menu "Properties: USB Serial Port" by clicking on the "*Close*" button.

After the operations are performed, the reader (converter) will be installed in the system. In the "*Universal Serial Bus (USB) Controllers*" section, you should see the entry "*USB IronLogic RFID Reader (Z397-Guard USB<->485)*". In the "COM and LPT ports" section, you should see the entry "*USB IronLogic RFID Reader [Serial port] (COM...) (Z397-Guard USB<->485 [Serial port] (COM...))*".

If the drivers are installed incorrectly (like FTDI, or the COM port is not installed), then they must be removed via the software removing incorrectly installed drivers (the "remove" folder in the Software archive). Before running the remove.bat file (from the "var1" and "var2" folders in turn) as administrator, it is advisable to disable all USB devices (except for the mouse and keyboard). After you uninstall the FTDI drivers, reinstall them.

## *Configuring converter Z-397 Web*

For converter **Z-397 Web**, no driver installation is required but you may need to configure the converter itself. You can do this in the converter configuration file. There are two ways to access the converter configuration.
- Connect the converter via USB cord to your computer and in the USB drive that appears edit the configuration file in Notepad.
- Download and install the FindWeb utility. Log in to the Settings Wizard and select the desired modes and settings.

Examples of configuration files for **Z-397 Web converter** in "SERVER" or "CLIENT" mode.

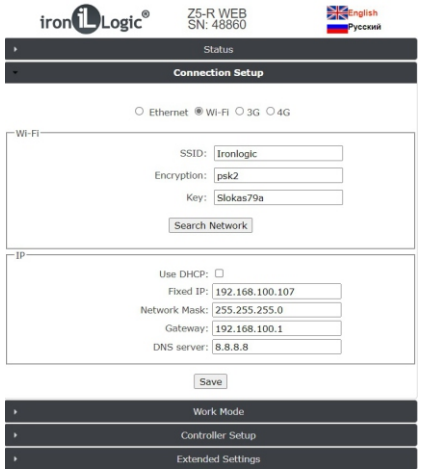
| Server | Client |
|---|---|
| [INFO]<br>SERIAL_NUMBER=33690<br>FW_VERSION=3.0.55(Aug 7 2017 11:13:16) | [INFO]<br>SERIAL_NUMBER=33690<br>FW_VERSION=3.0.55(Aug 7 2017 11:13:16) |
| [COMMON]<br>MODE=SERVER<br>AUTH_KEY=AEB5FA65 | [COMMON]<br>MODE=CLIENT<br>AUTH_KEY=AEB5FA65 |
| [NETWORK]<br>USE_DHCP=0<br>LOCAL_IP=192.168.100.102<br>NETMASK=255.255.255.0<br>GATEWAY=192.168.100.1<br>DNS=192.168.100.1<br>NODATA_TIMEOUT=0 | [NETWORK]<br>USE_DHCP=0<br>LOCAL_IP=192.168.100.102<br>NETMASK=255.255.255.0<br>GATEWAY=192.168.100.1<br>DNS=192.168.100.1<br>NODATA_TIMEOUT=0 |
| [TCP_SERVER]<br>LINE1_PORT=1000<br>LINE1_ALLOWED_IP=255.255.255.255<br>LINE2_PORT=1001<br>LINE2_ALLOWED_IP=255.255.255.255 | [TCP_CLIENT]<br>LINE1_REMOTE_ADDR=192.168.100.107<br>LINE1_REMOTE_PORT=25000<br>LINE2_REMOTE_ADDR=<br>LINE2_REMOTE_PORT=0 |
| [RS485]<br>LINE1_BAUD=19200<br>LINE1_PARITY=NONE<br>LINE2_BAUD=19200<br>LINE2_PARITY=NONE<br>RING_MODE=0 | [RS485]<br>LINE1_BAUD=19200<br>LINE1_PARITY=NONE<br>LINE2_BAUD=19200<br>LINE2_PARITY=NONE<br>RING_MODE=0 |

## *Configuring controller Z-5R Web*

For controller **Z-5R Web**, no driver installation is required but you may need to configure the controller itself. This can be done in the **WEB interface** of the controller.
On the "**Connection Settings**" tab, the method and parameters for connecting the communication module to the local network can be set.

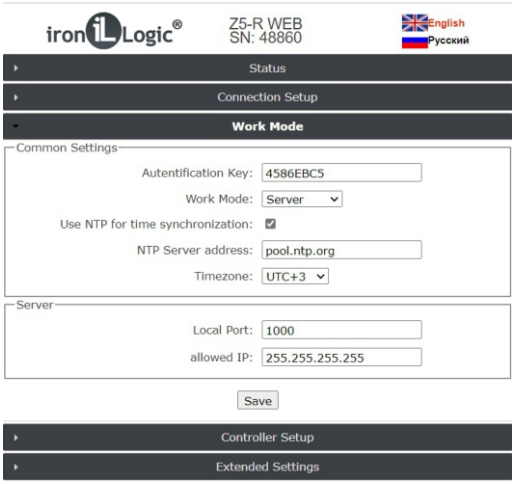
If you select the "**Ethernet**" connection method, the interface takes the following form:

If you use a DHCP server on your local network, the network settings are automatically obtained by the controller.
**Use DHCP**: Allows calling a DHCP server to automatically obtain the IP address and other network parameters necessary to operate on this local network.
**Without DHCP**: you must independently enter all the parameters corresponding to the configuration of the local network to which the device will be connected:
**Static IP:** A unique IP address that provides the device's address on the local network.
**Subnet mask:** A subnet mask used on this local network.
**Gateway:** An IP address of the gateway to communicate with other networks (including the Internet).
**DNS server:** An IP address of the DNS server.
For correct operation, all the parameters must be set. If you do not know some of the parameters, please contact your system administrator.
When all the parameters are configured, you must press the **"Save"** button.
If you select the **"Wi-Fi"** connection method, the interface will look like this:

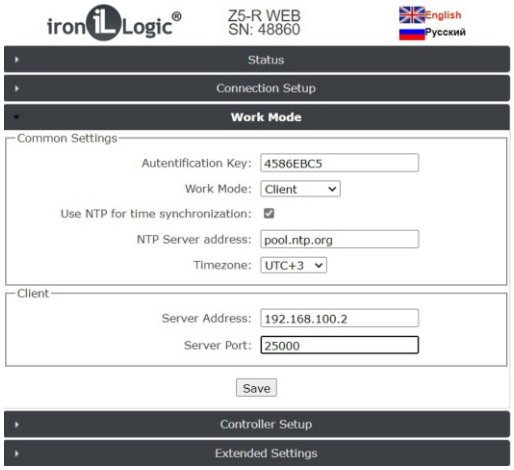



SSID: A name of the Wi-Fi network to which the device should be connected.
**Encryption:** The type of encryption in the Wi-Fi network to which the controller is connected (possible values - WPA, WPA2, none, etc.).
**Key:** An encryption key (password) used on this Wi-Fi network.
**Search for networks:** Activation of the search for currently available Wi-Fi networks.
**IP:** Network settings configuration (similar to setting up an Ethernet connection).
After the search for available Wi-Fi networks is finished, a dialogue box appears with a list of found networks to select the desired network. The level is displayed next to the network name.
To select a network, highlight the desired network and then press the **"Select"**. In this case, the name of the Wi-Fi network and the type of encryption will automatically appear in the settings. When using encryption, you must manually enter the encryption key:
Next, if there is no DHCP server, you must correctly configure the network settings.
To save the settings of all the parameters, you must click the **"Save"** button.
After configuring the connection to the local network, it is necessary to configure the mode of establishing communication between the controlling software and the communication module.
On the **"Operating Mode"** tab, the desired method of connection of the communication module to the software when operating in the network mode can be selected.

**Authentication key:** The authentication key is required to access the Web interface of the Z-5R controller (mod. Web). Initially, the factory value indicated on the label on the device casing is displayed here (see AUTH_KEY). At this configuration stage, it can be changed, if necessary (numbers and Latin letters are allowed).
**Operation mode:** The selection of the network mode of operation - **Server, Client.**
In the **"Server"** mode, the communication module listens for connections to its open local port of the control software.



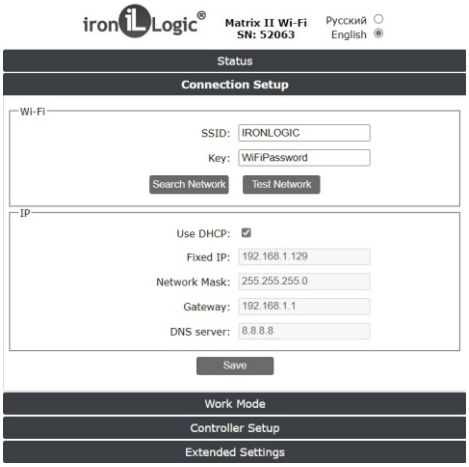

If the **"Server"** operation mode is selected, the following should be set:
**Local port:** A TCP port to which the control software will be trying to connect.
**Allowed IP:** An IP address of the computer from which the control software is allowed to connect to the controller (255.255.255.255 to allow all IP addresses). When all the parameters are configured, you must press the **"Save"** button.
If the **"Client"** operation mode is selected, the communication module will regularly try to establish a connection with the control software.



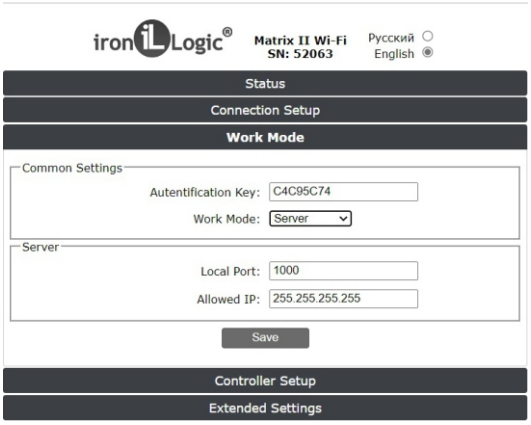

The following parameters should be set:
**Server address:** The IP address of the computer to which the controller must establish a connection to communicate with the control software.
**Server port:** An IP port to which the connection must be made.
When all the parameters are configured, you must press the **"Save"** button.
To finish working with the Web interface, you need to set the jumper from the CONFIG to NORMAL position and reboot the controller.

## *Configuring controller Matrix II Wi-Fi*

For controller **Matrix II Wi-Fi**, no driver installation is required but you may need to configure the controller itself. This can be done in the **WEB interface** of the controller.
On the **"Connection Settings"** tab, the method and parameters for connecting the communication module to the local network can be set.




**Network (SSID):** A name of the Wi-Fi network to which the device should be connected.
**Password:** An encryption key (password) used on this Wi-Fi network.
**Search for networks:** Activation of the search for currently available Wi-Fi networks.
After the search for available Wi-Fi networks is finished, a dialogue box appears with a list of found networks to select the desired network. The level is displayed next to the network name.
To select a network, highlight the desired network and then press the **"Select"**. In this case, the name of the Wi-Fi network will automatically appear in the settings.
Next, if there is no DHCP server, you must correctly configure the network settings.
**Without DHCP**: you must independently enter all the parameters corresponding to the configuration of the local network to which the device will be connected:
**Static IP:** A unique IP address that provides the device's address on the local network.
**Subnet mask:** A subnet mask used on this local network.
**Gateway:** An IP address of the gateway to communicate with other networks (including the Internet).
**DNS server:** An IP address of the DNS server.
When all the parameters are configured, you must press the **"Save"** button.
If **Matrix II Wi-Fi** is intended to operate in the network mode, i.e. under the control of external software, then after configuring the connection to the local network, it is necessary to configure the mode of establishing communication between the controlling software and the communication module.
On the **"Operating Mode"** tab, the desired method of connection of the communication module to the software when operating in the network mode can be selected.
**Authentication key:** The authentication key is required to access the Web interface of the controller. Initially, the factory value indicated on the label on the device casing is displayed here (see AUTH_KEY). At this configuration stage, it can be changed, if necessary (numbers and Latin letters are allowed).
**Operation mode**: The selection of the network mode of operation - **Server**, **Client**.
In the **"Server"** mode, the communication module listens for connections to its open local port of the control software.

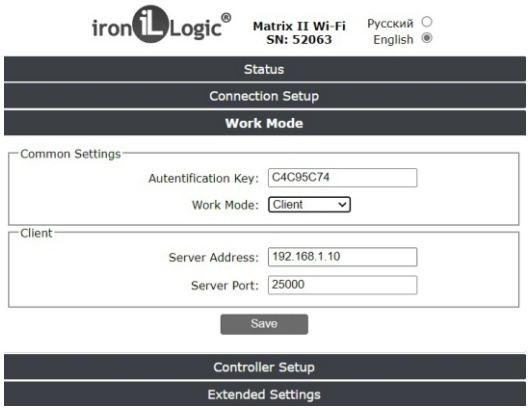



If the **"Server"** operation mode is selected, the following should be set:

**Local port:** A TCP port to which the control software will be trying to connect.

**Allowed IP:** An IP address of the computer from which the control software is allowed to connect to the controller (255.255.255.255 to allow all IP addresses). When all the parameters are configured, you must press the **"Save"** button.

If the **"Client"** operation mode is selected, the communication module will regularly try to establish a connection with the control software.




The following parameters should be set:

**Server address:** The IP address of the computer to which the controller must establish a connection to communicate with the control software.

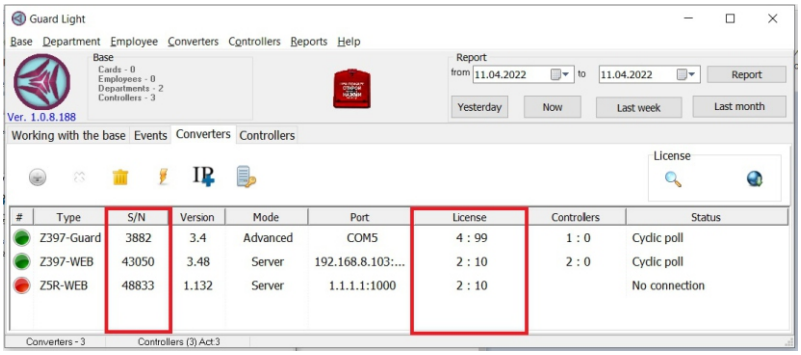
**Server port:** An IP port to which the connection must be made.

When all the parameters are configured, you must press the **"Save"** button.

To finish working with the Web interface, you need to set the jumper from the CONFIG to NORMAL position and reboot the controller.

# LICENSE

**A license** is a certain limit on the number of serviced controllers and cards in each of the controllers. The license is installed in the converter (**Z-397 Guard, Z-397 Web)** or IP controllers (**Z-5R Web, Matrix II Wi-Fi**). The initial (free) license covers 2 controllers and 10 cards. To increase this number, you need to apply for the purchase of the appropriate license. The license is purchased for each specific converter (**Z-397 Guard, Z-397 Web)** or a specific communication module for the IP controller (**Z-5R Web, Matrix II Wi-Fi**).
To order a license, you must specify the serial number of the converter (**Z-397 Guard, Z-397 Web)** or a communication module for the IP controller (**Z-5R Web, Matrix II Wi-Fi**). Its value is indicated in the Guard Light Software on the "Converters" tab in the "S/N" column. In the same place, the currently active values of the license parameters in the "License" column are indicated.




## *License Options*

1. For controller **Z-5R Web** or **Matrix II Wi-Fi**:
   - Guard Light-1/50L -- for the simultaneous operation of up to 1 controller and 50 cards
   - Guard Light-1/100L -- for the simultaneous operation of up to 1 controller and 100 cards
   - Guard Light-1/250L -- for the simultaneous operation of up to 1 controller and 250 cards
   - Guard Light-1/1000L -- for the simultaneous operation of up to 1 controller and 1000 card
   - Guard Light-1/2000L -- for the simultaneous operation of up to 1 controller and 2000 cards
2. For converter **Z-397 Guard** or **Z-397 Web**:
   - Guard Light-1/50L -- for the simultaneous operation of up to 1 controller and 50 cards
   - Guard Light-1/100L -- for the simultaneous operation of up to 1 controller and 100 cards
   - Guard Light-1/250L -- for the simultaneous operation of up to 1 controller and 250 cards
   - Guard Light-1/1000L -- for the simultaneous operation of up to 1 controller and 1000 cards
   - Guard Light-1/2000L -- for the simultaneous operation of up to 1 controller and 2000 cards
   - Guard Light-5/100L -- for the simultaneous operation of up to 5 controllers and 100 cards
   - Guard Light-5/500L -- for the simultaneous operation of up to 5 controllers and 500 cards
   - Guard Light-5/1000L -- for the simultaneous operation of up to 5 controllers and 1000 cards
   - Guard Light-5/2000L -- for the simultaneous operation of up to 5 controllers and 2000 cards
   - Guard Light-10/250L -- for the simultaneous operation of up to 10 controllers and 250 cards
   - Guard Light-10/500L -- for the simultaneous operation of up to 10 controllers and 500 cards
   - Guard Light-10/1000L -- for the simultaneous operation of up to 10 controllers and 1000 cards
   - Guard Light-10/2000L -- for the simultaneous operation of up to 10 controllers and 2000 cards

## *Purchase and ordering procedure*

There are two options for purchasing Guard Light:
1) Purchase one of the licenses.
In this case, you should first buy (from us or one of the suppliers of our products) a converter (**Z-397 Guard, Z-397 Web)** or a controller (**Z-5R Web, Matrix II Wi-Fi**). and the equipment necessary for them (controllers, readers) and install the Guard Light Software.

Next, you test it in the free 2L Guard Light license mode and determine which license do you need and for how many points of passage and number of people per passing point. You tell us the serial number of a converter (**Z-397 Guard, Z-397 Web)** or a controller (**Z-5R Web, Matrix II Wi-Fi**) and the license you have chosen. After paying the invoice, the license is activated.

2) Purchase a package.

The package includes:

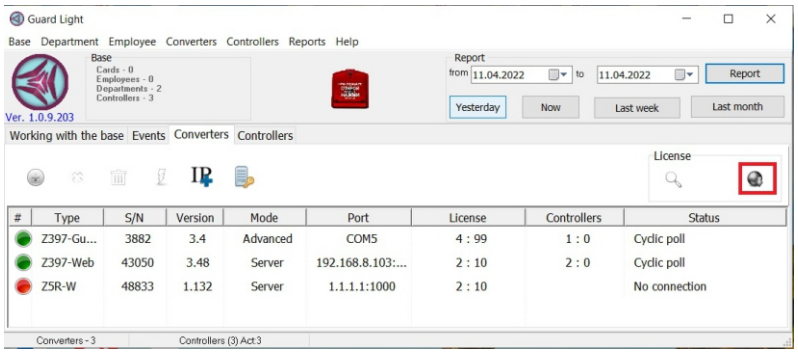
- a converter **Z-397 Guard** or **Z-397 Web** with a license activated in it.

To order a license, you need to select the converter and follow the link obtained via **Converters / License / Order a License on the Site**.

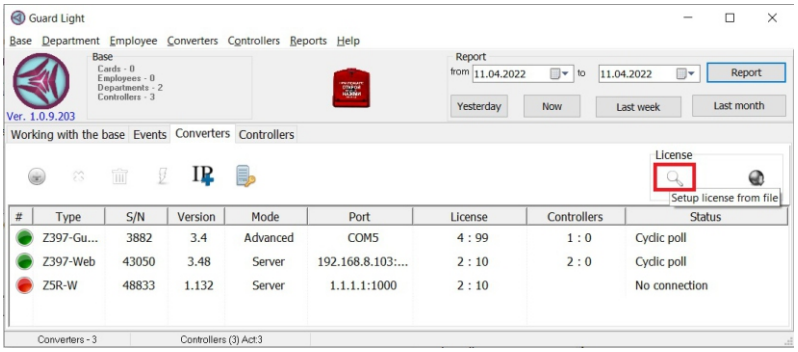
## *License installation*

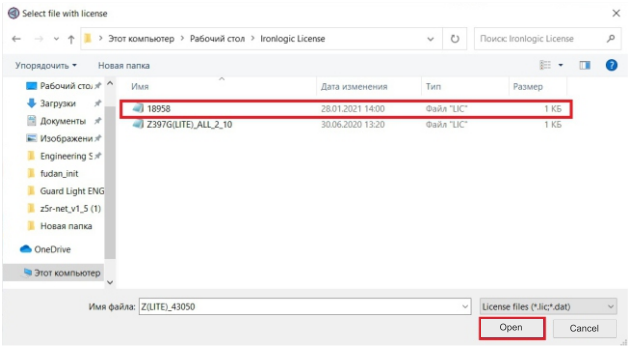
After purchasing a license, it can be applied in two ways.

The first option is when the Software independently downloads and installs the license from the manufacturer's website. This can be done by highlighting the converter and selecting the appropriate menu item **Converters / License / Download the available license from the site**. Of course, your computer must have an Internet connection.

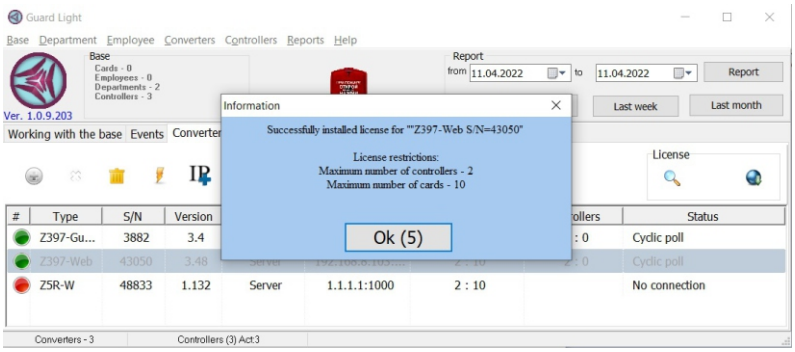



The second method must be used when obtaining a license in the form of a file. To do this, highlight the converter and select the menu item **Converters / License / Install license from a file**.




Select the license file location in the explorer window and click on the "Open" button. After selecting the license file, the license information menu appears.




Click on the "OK" button. The license will be recorded in the converter (communication module).

**Important!** The license is recorded in the converter, so all actions regarding the request or installation of the license are possible only when the converter is connected. Updating the Software version does not change the license settings.

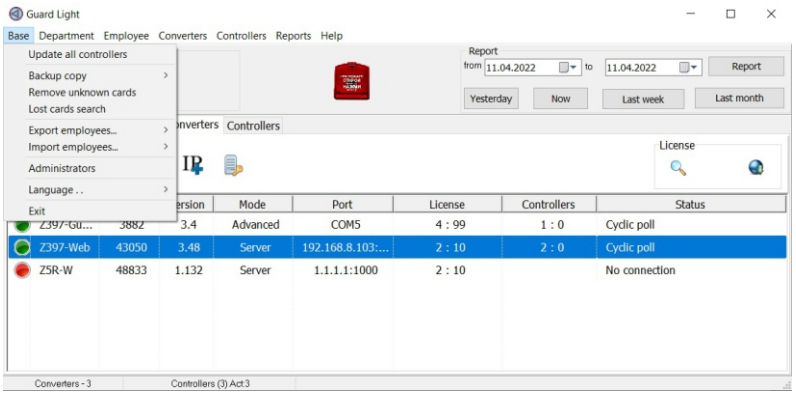
# SOFTWARE DESCRIPTION

## *Main menu*

The main menu has the following tabs: "Database", "Department", "Employee", "Converters", "Controllers", "Reports", "Help".

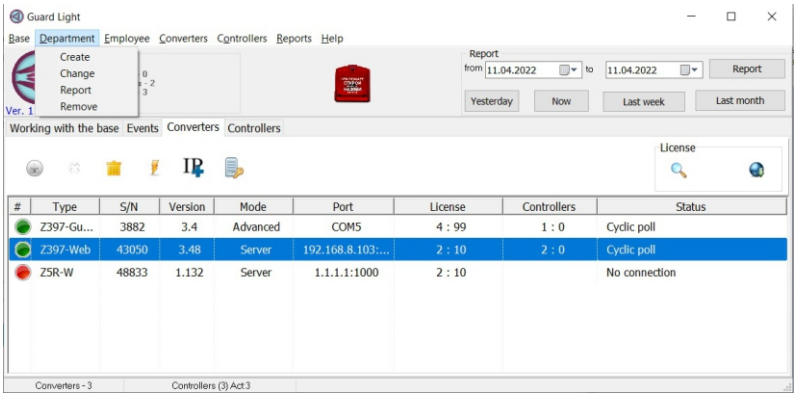
### Database

The "Database" tab has the following items: "Overwrite everything to controllers", "Backup copy...", "Delete unknown cards", "Search for lost cards", "Export the list of employees...", "Import the list of employees...", "Administrators", "Language...", "Object mode", "Close the programme".



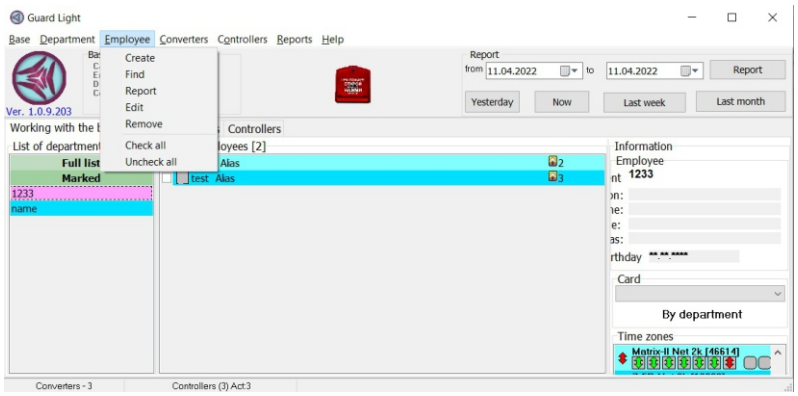

### Department

The "Department" tab has the following items: "Create", "Edit", "Report", "Delete".



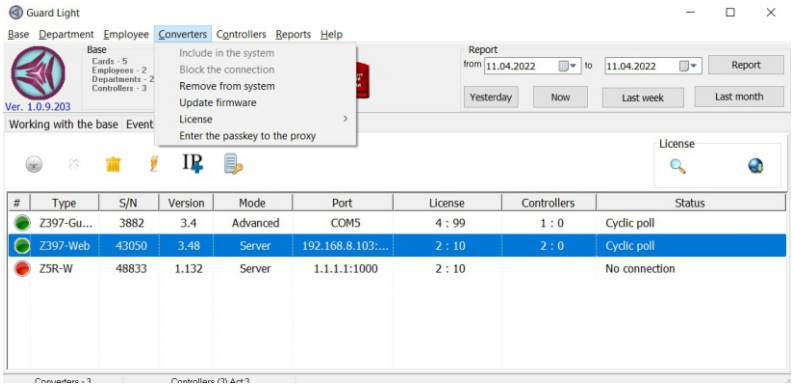

### Employee

The "Employee" tab has the following items: "Create", "Find", "Report", "Edit", "Delete", "Mark all", "Unmark all".



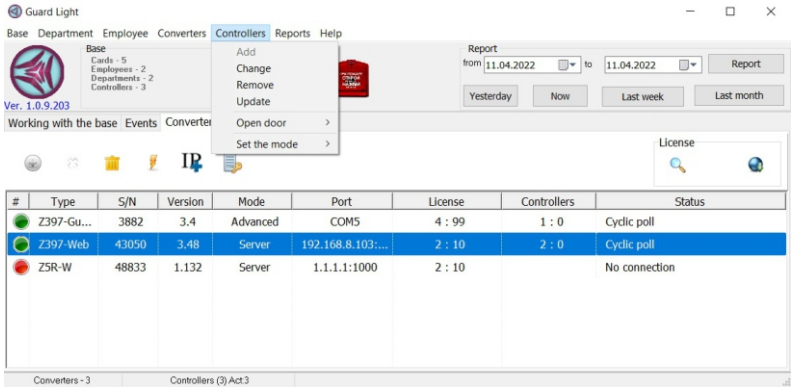

### Converters

The "Converters" tab has the following items: "Include in the system", "Block connection", "Remove from the system", "Update firmware", "License", and "Enter the proxy access key".



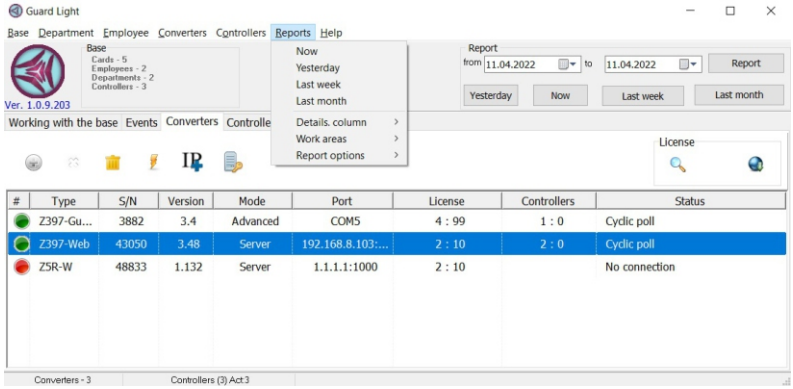

## Controllers

The "Controllers" tab has the following items: "Add", "Change", "Uninstall", "Update firmware", "Open door", "Set mode".



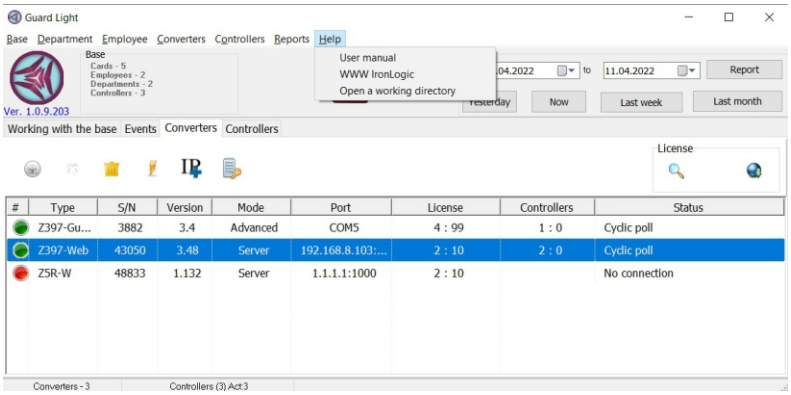

## Reports

The "Reports" tab has the following items: "Today", "Yesterday", "Last week", "Last month", "Info columns", "Work zones", "Report parameters".



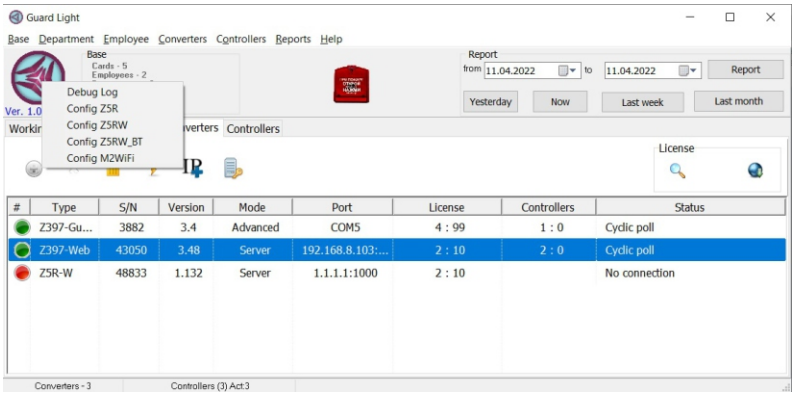

## Help

The "Help" tab has the following items: "Instruction manual", "Z-5R Extended" and "Open working folder".



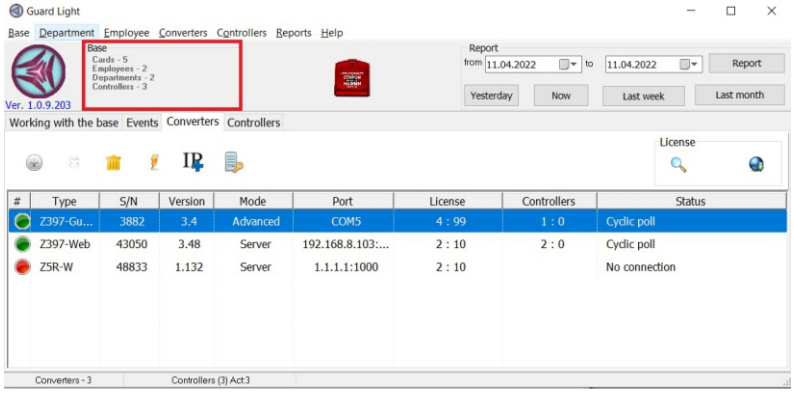
### *Software logo*

The upper-left corner of the programme. Right-click on the Software logo to bring up the context menu: "Debug Log" (to enable software log recording), "Config Z5R" (to review the configuration of the Z-5R Net Extended controller), "Config Z5RW" (to review the configuration of the Z-5R WEB controller), "Config M2WiFi" (to review the configuration of the Matrix II Wi-Fi controller). All controller configurations can be saved after editing and subsequently used.



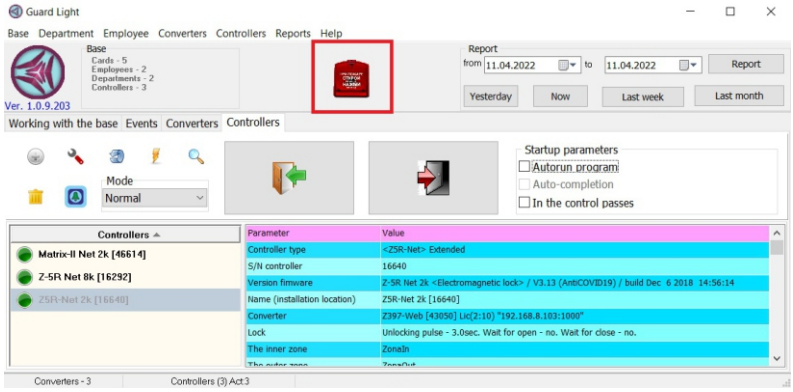

### *"Database" panel*

The "Database" information panel. The database information panel displays the number of cards, employees, departments and controllers in the populated database.



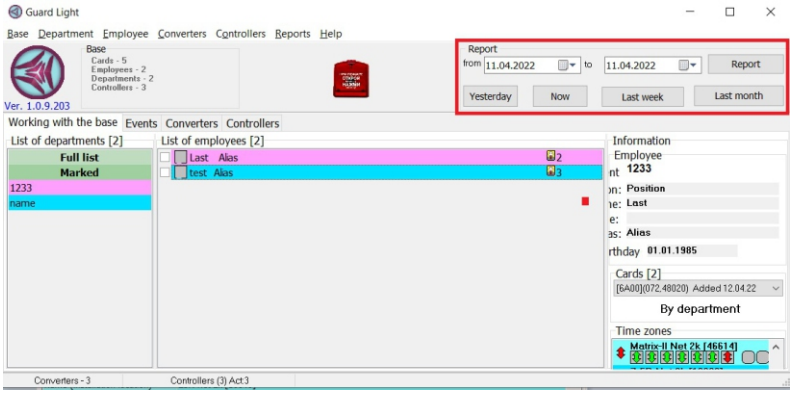

### *"Enable fire safety mode" button*

The fire safety mode activation button "Enable fire safety mode" turns on the evacuation mode on all connected controllers.



## *"Report" panel*

On the panel, the time for generating the report is selected.

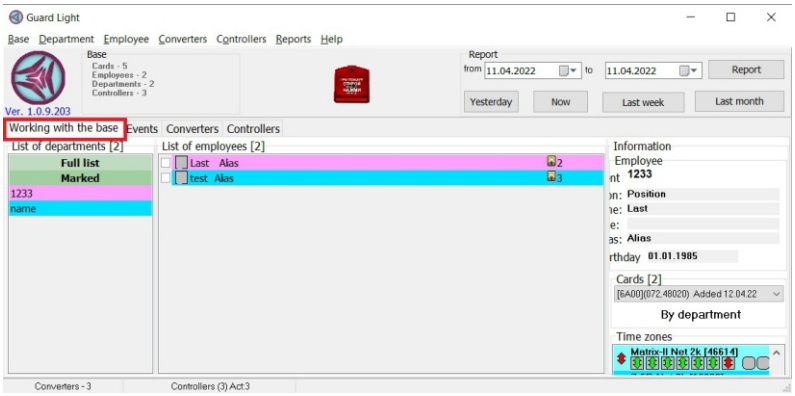



## *Tab bar*

The tab bar consists of 4 tabs: "Database tools", "Events", "Converters", "Controllers".

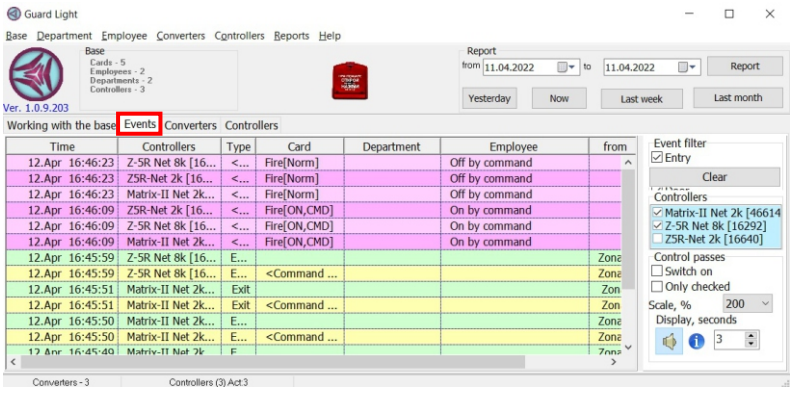
### "Database Tools" tab

The "Database tools" tab contains the following panels: "Department list", "Employee list", "Information" (includes "Employee", "Card" and "Time Zones" panels).



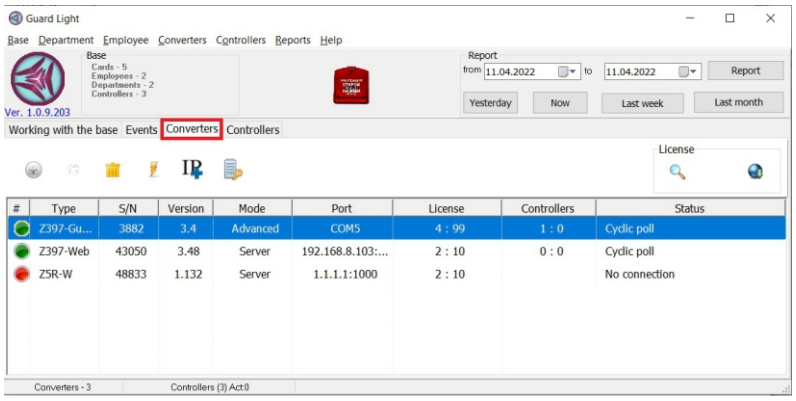

### "Events" tab

The "Events" tab has an event display menu and the "Controllers" panel, "Event filter" panel and "Passing control" panel.



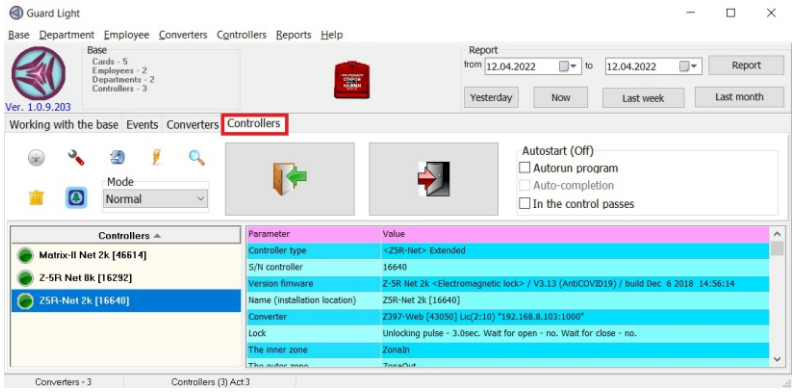
## "Converters" tab

The "Converters" tab has a toolbar for managing converters, the "License" panel and a menu for displaying connected or found converters with their parameters.




## "Controllers" tab

The "Controllers" tab has a toolbar for managing controllers, buttons for remote control of doors, an "Autostart" panel for enabling automatic Software startup and a menu for displaying connected or found controllers with their parameters.



# HOW TO START THE SOFTWARE

## *Startup parameters*

Typically, you can run the Software with settings to access its database from multiple computers on the network. To do this, you should define a computer from which the database can be edited while the other computers operate in the browse mode. At the same time, the network address where the shared database is stored must be set for all computers.
When launched, the Software searches for the file "**GuardLight.ini**" in the folder from which it is launched. If the file does not exist, you must create it manually in a text editor, such as Notepad. The first line is mandatory and the remaining lines can be added as needed, for example:

```
[ADVANCED]
Mode=Monitor
Dir=C:\Iron logic\Guardlight
COM_Delay=300
Port=25000
```

| Parameter | Value | Description |
|---|---|---|
| **Mode** | **Master** | The value of the "Master" field means that either the main or the first copy of the Software is launched. It is used when running the Software at the first or main workplace. |
| | **Monitor** | The value of the "Monitor" field means that the Software is running in the browse mode and editing is prohibited. It is used when you run a second copy on another computer to build reports. |
| **Dir** | **C:\Iron logic\Guardlight** | Database directory. It is used to transfer the database to a network drive and to run other copies of the Software. |
| **COM_Delay** | **300** | The additional delay in waiting for a response in milliseconds. It is used when there is high latency in the communication channel. |
| **Port** | **25000** | Server port for receiving connections from Z-5R Web, Matrix II WiFi and Z-397 Web in the "Client" mode. |

Using the "**Mode**" parameter, it becomes possible to run the Software on several computers in one local network, and in order to do this, the "**Mode**" parameter is set to "**Master**" for one application, while the rest of them should be set to "**Monitor**".
The "**Dir**" parameter must point to the same network directory in all cases (at all workplaces). Also, the "**Dir**" parameter should be configured if you are using a network with domains. Since Windows likes to update the local profile without warning and when it pleases, we recommend you to move the folder containing the database to a more secure location on the disk, for example, "**C:\Iron logic\Guardlight**".
The delay in waiting for the "**COM_Delay**" response should be changed only when there are really high latencies in the transmission channels, for example, when using virtual machines or in the case of communication via GSM modems.
It makes sense to configure the server port value "**Port**" only if there are conflicts with other programmes installed on the computer.

## *"Master" mode*

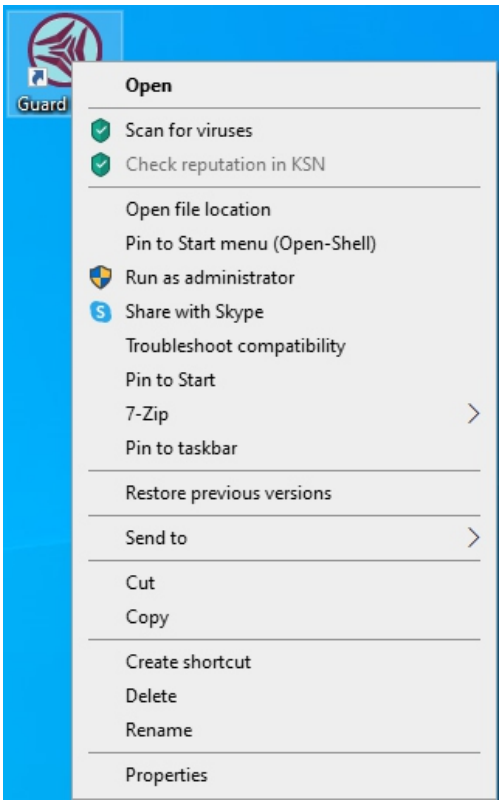
In the "Master" mode, the Software is installed and runs on the main computer.
In this mode, all the functionality of the Software is available (equipment management, database editing, handling reports, etc.). Starting with Guard Light Software version 1.0.6.153, you can run Guard Light in "Master" mode one at a time. Whoever runs the Software first will be the "Master" and other users will be asked to work in the browse mode and it will be indicated who exactly took over the database. The Software was updated with control over the database being busy when accessing it from different computers and saving the settings of the Software menu individually for each user.

## *"Monitor" mode*

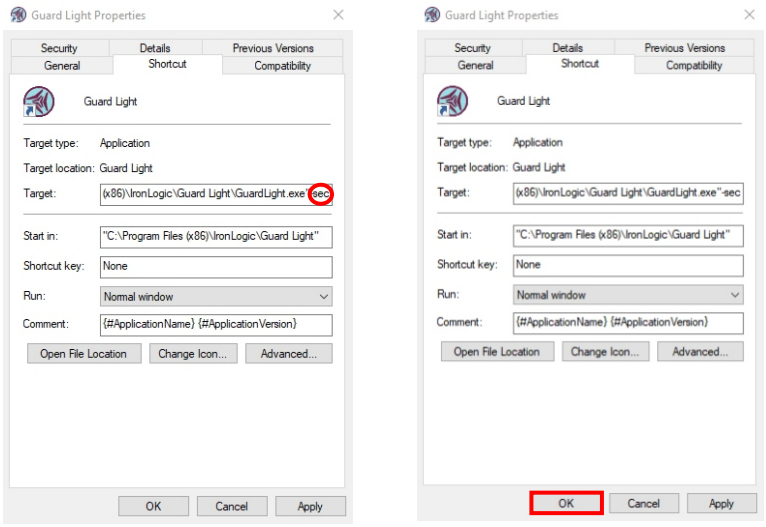
The "Monitor" mode means that the Software is running in the browse mode only and editing is prohibited. It is used when you run a second copy (or multiple copies) on another computer(s) to build reports. In this mode, you can work only with reports and cannot change anything in the database or review current events. In the first copy of the Software, in the GuardLight file.ini leave the "Master" mode (Mode=Master) and in the other copy write the "Monitor" mode (Mode=Monitor) and set the path to the general database on the network (for example: dir=\\comp2\IronLogic\Guard Light).

## *"Guard" mode*

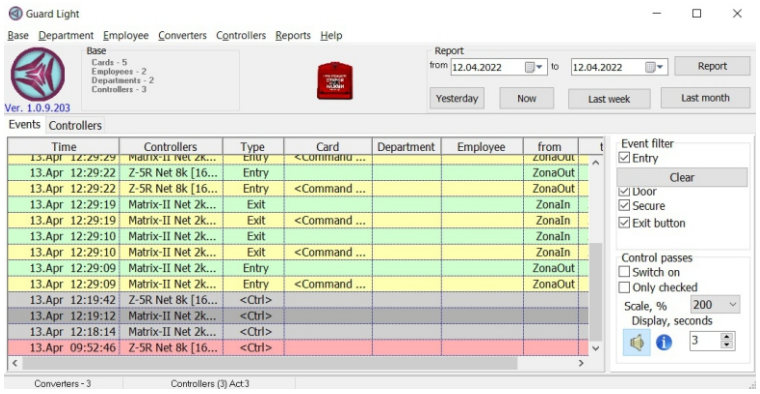
Starting with Guard Light Software version 1.0.8.173, the "**Guard**" mode has been added to the Software. In this mode, only passing control is enabled.
The "Guard" mode can be enabled by launching the main Software (in the "**Master**" mode) with the key "**-sec**" or "**-security**".
To do this, right-click on the Software shortcut and select "**Properties**".



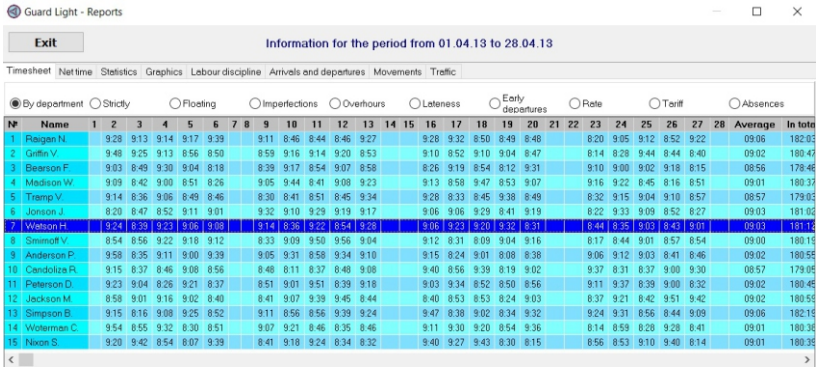

In the Software properties menu on the "**Shortcut**" tab in the "**Target**:" field after the quotation marks add "**-sec**" or "**-security**" separated by space.
For example: **“D:\IronLogic\Guard Light\GuardLight.exe” -sec**
Or: **“D:\IronLogic\Guard Light\GuardLight.exe” –security**



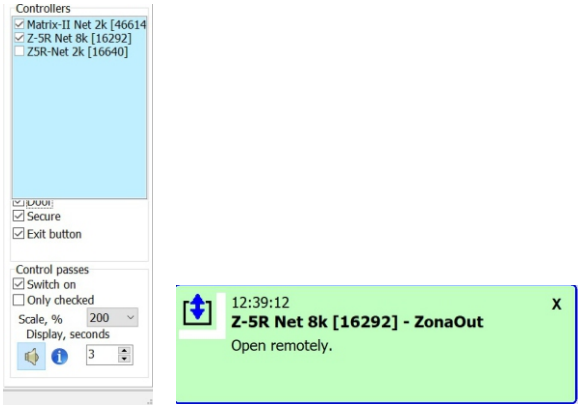

Save changes by clicking on the "OK" button.
Launch the Software shortcut by double-clicking the left mouse button. The Software will run in the browse mode. Editing data will be prohibited. Only two tabs of the Software will be available: "Events" and "Controllers".




Also in the "Guard" mode, you can work with reports.



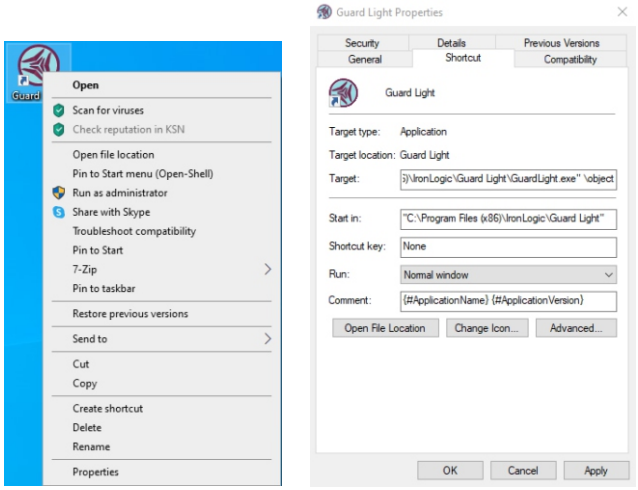

Event filters and passing control are available on the "Events" tab.




Pop-up messages about each passage are displayed.

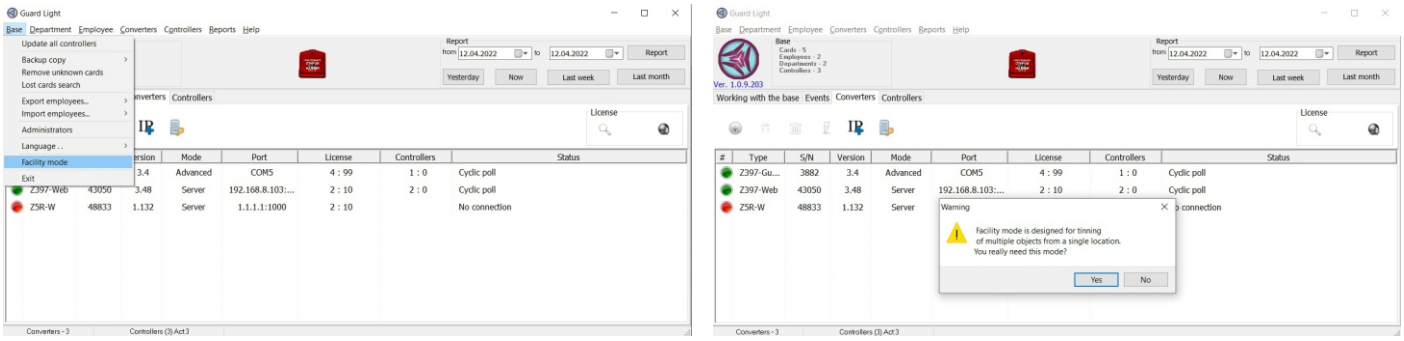
## *Object mode*

In this mode, an object selection menu appears where you can add, open or delete objects. You can check the ability to communicate with the converter without opening the object.
The **Object** is a separate database associated with its converters. The Software allows you to quickly switch between such objects establishing a connection with the object converters.
**Important! Before enabling the object mode, please make sure you really need it. Returning to normal mode is possible only by completely reinstalling the Software.**
The object mode can be enabled by running the Software with the "/**object**" key.
To do this, right-click on the Software shortcut and select "Properties".



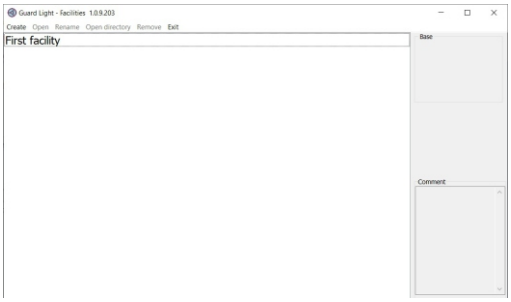

In the Software properties menu on the "**Shortcut**" tab in the "**Target**:" field after the quotation marks add "\object" separated by space.
For example: "D:\IronLogic\Guard Light_object\GuardLight.exe" \object
Save changes by clicking on the "OK" button.

Launch the Software shortcut by double-clicking the left mouse button and select the **Database/Object mode** menu item.

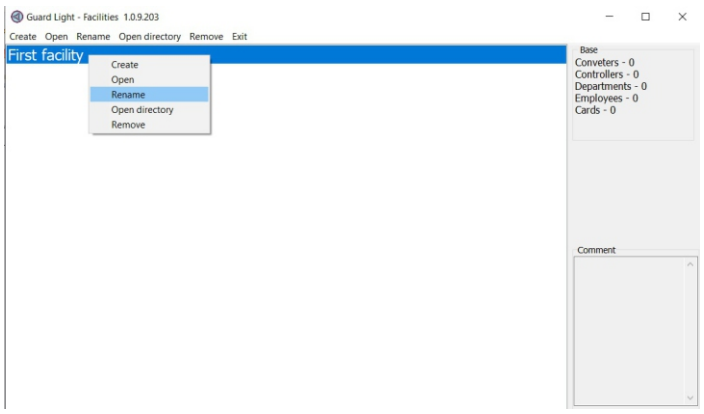


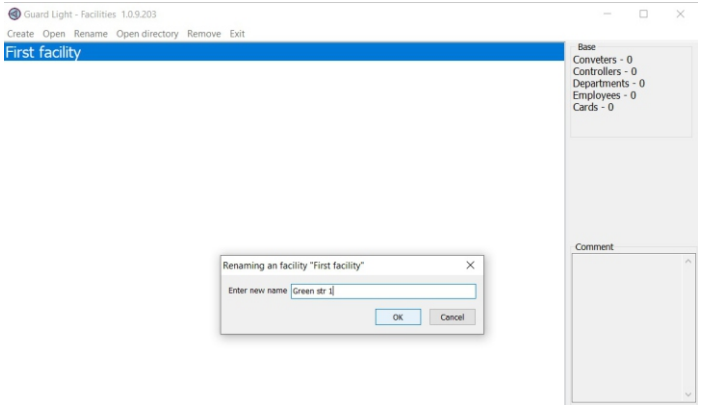

After checking the "Object mode" box, a warning window will appear. If you need the object mode, click on the "Yes" button.

When you start the Software, an object mode menu will appear.

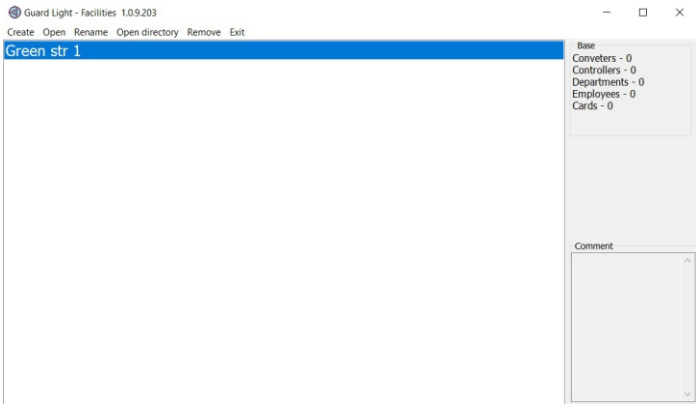


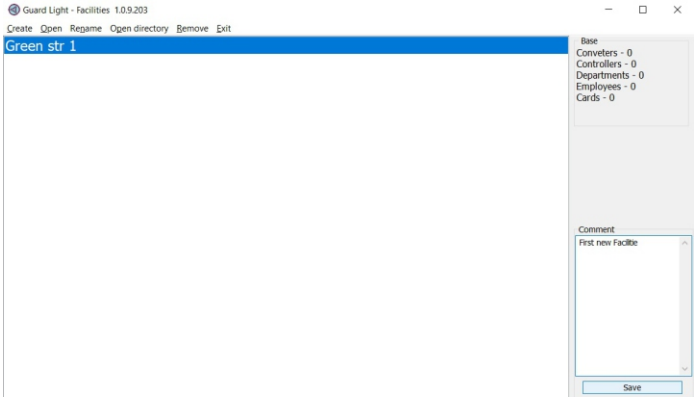

Rename the first main object from “First facility” to the object name you want. To do this, right-click on the object and select "Rename".



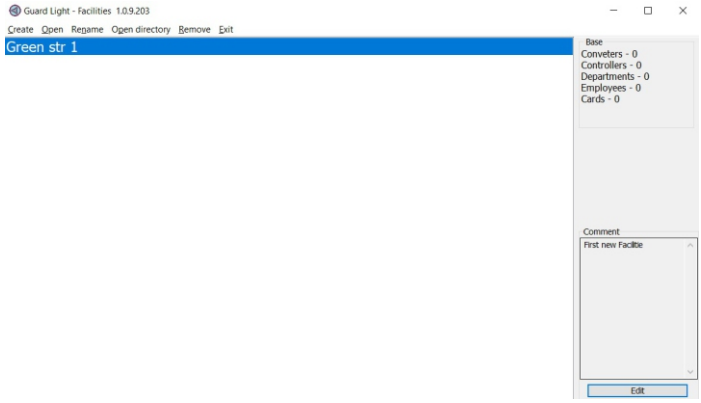



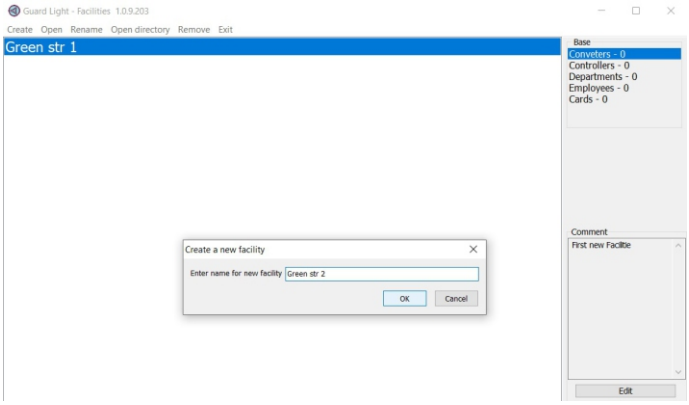

In the object renaming menu, enter the desired name and click on the "OK" button.
To add a comment, click on the "Edit" button.



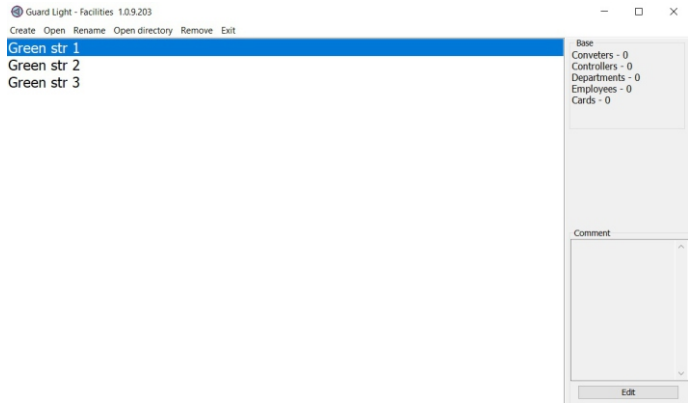




The "Comment" menu is activated. Add the necessary comments to the object and click on the "Save" button.
To create the next object, select "Create" from the main menu.




After creating all the objects, you can open them, connect the necessary converters with controllers and fill in the employee database.




***After activating the object mode, the opening of the desired database and the Software shutting down can be carried out only via the object selection menu.***

## *Automatic startup*

The controllers used have a memory for at least two thousand events. This means that you do not have to keep the controlling computer always on. In addition, on the "Controllers" tab, you can activate the **Automatic startup** function. When this function is activated, the Software will automatically start when the computer is turned on and read all accumulated events from the controllers.

If the **Automatic shutdown** is checked, the Software will automatically shut down its operation when all accumulated events are read.

If the **Passing control mode** is checked, the Software will continue operating in the background notifying you with pop-up messages about the employee movements.

# POPULATING THE DATABASE

## *Main terms*

**Employee** - a subject of accounting and control having an identification card;
**Department** - a group of employees who have common rules for working time recording;
**Schedule** – the work schedule of the department.
**Time zone** - periods when access to the premises is allowed;
**Database** – a list of employees, departments and time zones;
**Event** – any change in the state of sensors and readers;
**Card (identifier)** – a contactless mark with the code that can be read using radio waves. Usually, the card has a number, which is also displayed in the Software.

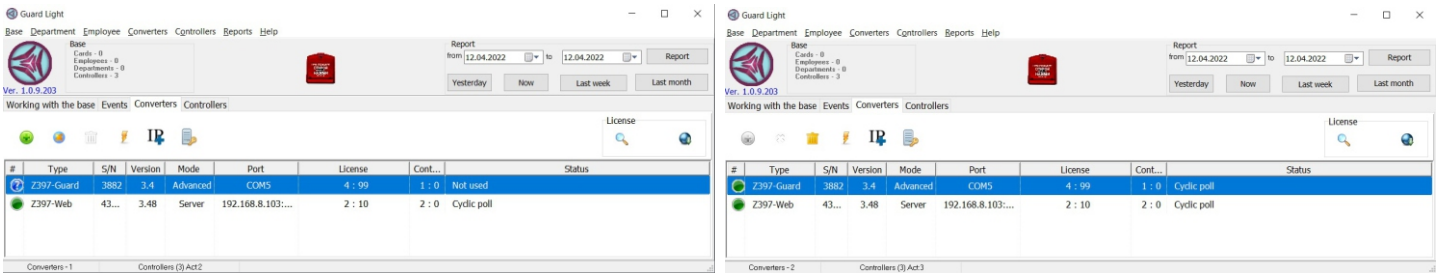
## *Database population sequence*

Before using the Software, you should populate the database. The following procedure is proposed:

1) turn on all the equipment and run the Software;
2) on the "Converters" tab, connect converters to the Software;
3) on the "Controllers" tab, connect controllers to the Software;
4) on the "Database tools" tab in the "Time zones" panel, configure the time zones of the controllers;
5) on the "Database tools" tab in the "Department list" panel, create departments;
6) on the "Database tools" tab in the "Employee list" panel, create employee records in specific departments.
7) on the "Database tools" tab in the "Employee list" panel, register employee passing cards.

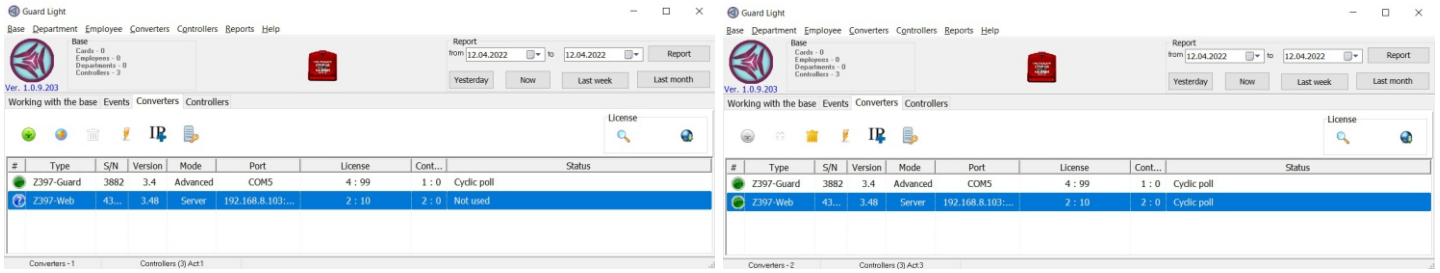
## *"Converters" tab*

To manage converters, go to the "Converters" tab. The Software independently scans all COM-ports in order to detect USB converters **Z-397 Guard**.



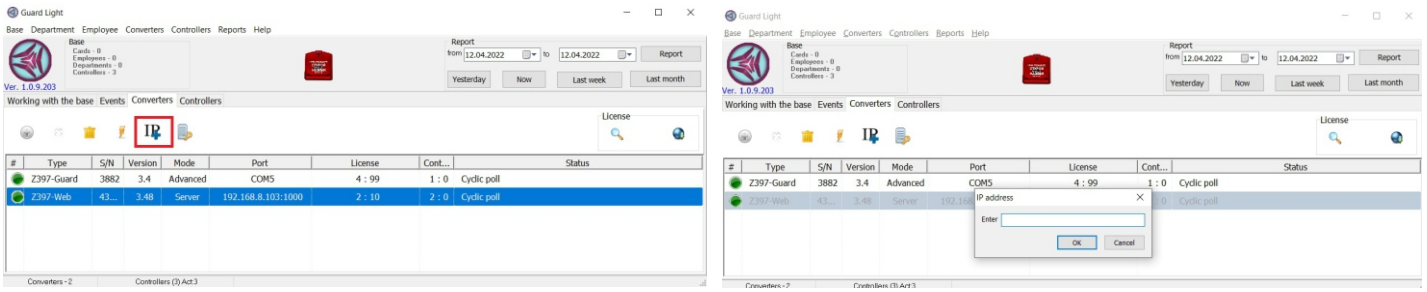

**Z-397 Guard** Converter should be switched to "**Advanced**" mode.

The Software sends requests to detect **Z-397 Web converters** or **Z-5R Web** and **Matrix II Wi-Fi controllers** to the local network.




The search results are displayed in the list of converters on the "Converters" tab.

If the requests can not reach the converter for any reason, you can try to enter its IP address manually by clicking the "Enter the converter IP address" button. In the "IP address" menu that appears, enter the IP address of the converter and click on the "OK" button.



In this case, attempts will be made to communicate directly with the converter running in the "SERVER" mode.

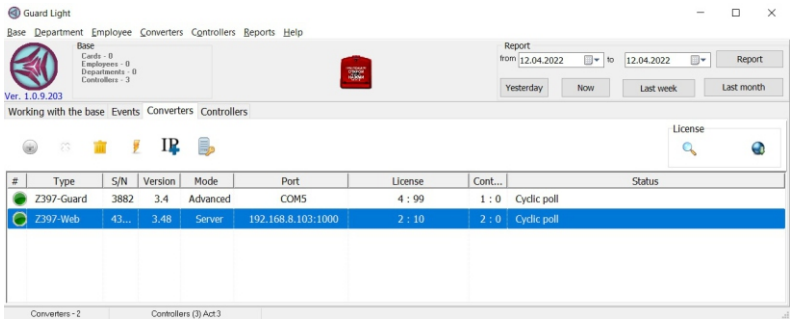
A coloured circle next to the converter type represents its status:

| | |
|---|---|
| | *a new converter available for connection to the system* |
| | *a converter connected to the system but not detected by the software (no signal)* |
| | *a converter in the software update mode* |
| | *a converter connected to the system and working properly* |
| | *a converter connected to the system but with license violations* |
| | *Z-397 Guard converter with incorrectly set mode* |

Converter **Z-397 WEB** and IP-controllers **Z-5R Web, Z-5R Web mini** and **Matrix II Wi-Fi** can work with the Software in two modes: ***server*** or ***client***.

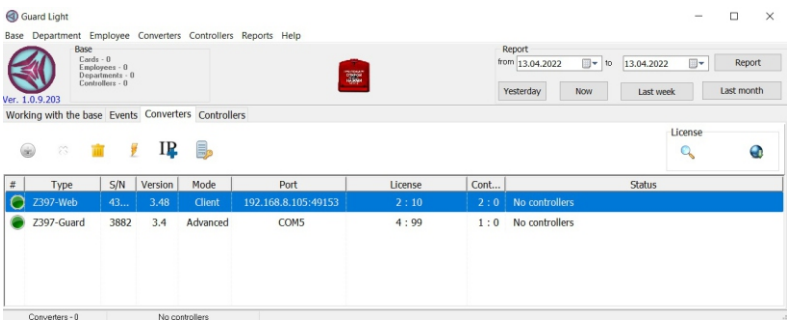
## Server mode

The converter passively waits for the Software to connect. By default, TCP port **1000** is used for communication. The Software detects the converter by broadcast requests and connects to it. This method is used in those networks where UDP broadcast requests from the Software are able to reach the converter and its response is able to reach the Software.



## Client mode

The converter actively tries to connect to the Software acting as a client while the Software acts as a server. By default, TCP port **25000** is used for communication. This mode allows operating in networks where the distribution of broadcast packets is impossible or prohibited, but it is possible to connect to the Software directly from the place where the converter is connected.



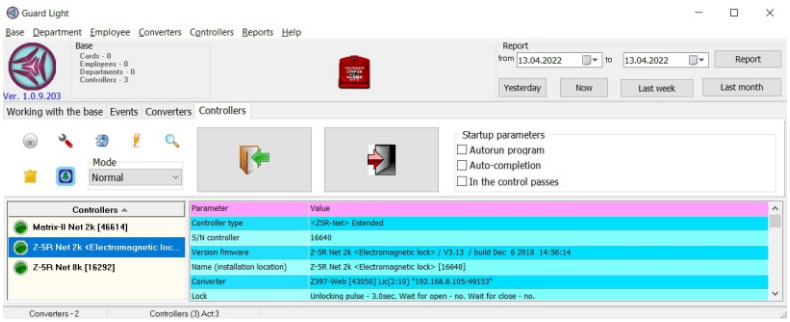
In any mode, the connection for the exchange of information is established via the TCP protocol.

### Converter firmware updates

The converter comes with factory firmware. For the converter to work properly in new versions of the Software, the firmware must be updated. The firmware is updated via the RS-485 communication line, and to do this the converter must be connected to the communication line and detected by the Software. To update the firmware, you need to select the necessary converter and click the button ("Update Firmware"). Next, select the firmware for the desired converter model (for example: Z397G_V3_5.rom or Z397WEB_v3.0.69.rom) and activate the update process by confirming your intentions.

## *"Controllers" tab*

To manage controllers, go to the "Controllers" tab. As with converters, there will be a list of controllers connected to the system.



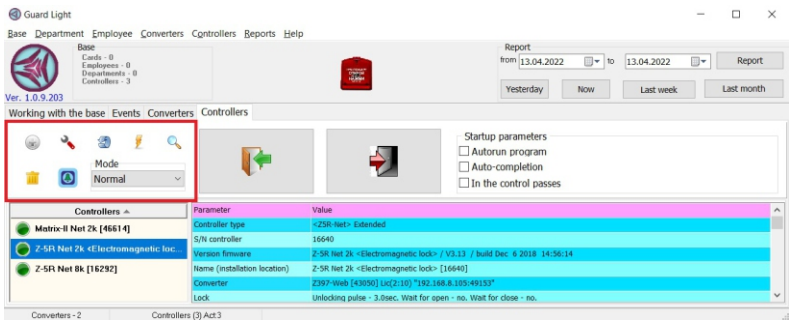

A coloured circle next to the controller name displays its status:

| | |
|---|---|
| | *a controller can be added to the system* |
| | *the controller is in the system, but communication with it has been lost* |
| | *the controller is busy updating the memory or program* |
| | *converter included in the system and working normally* |
| | *converter included in the system, but there are license violations* |
| | *Converter Z-397 Guard with incorrectly set mode* |

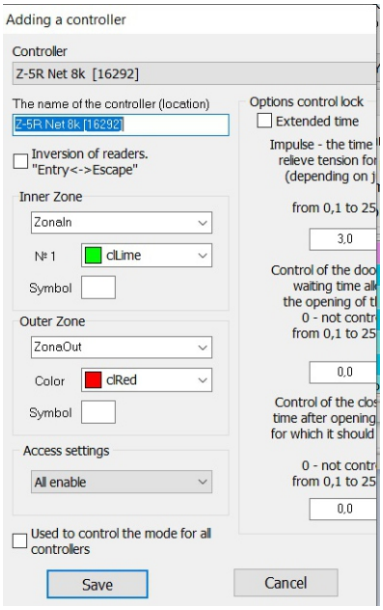
| | |
|---|---|
| | *controller in "Evacuation" state* |
| | *controller in «Locked" state* |
| | *Security on*<br>*All is okay* |
| | *Security on*<br>*Alarm* |

Also, next to the circle, the status of the enabled functions can be displayed:

The tab has a toolbar that allows you to manage the list of controllers. You can add and remove controllers, update their firmware and configure them.




It is also possible to remotely open the passage and switch the access mode.
To add the controller to the system, select the controller marked with a blue circle and click the "Add" button.
After the configuration form appears, it should be filled.

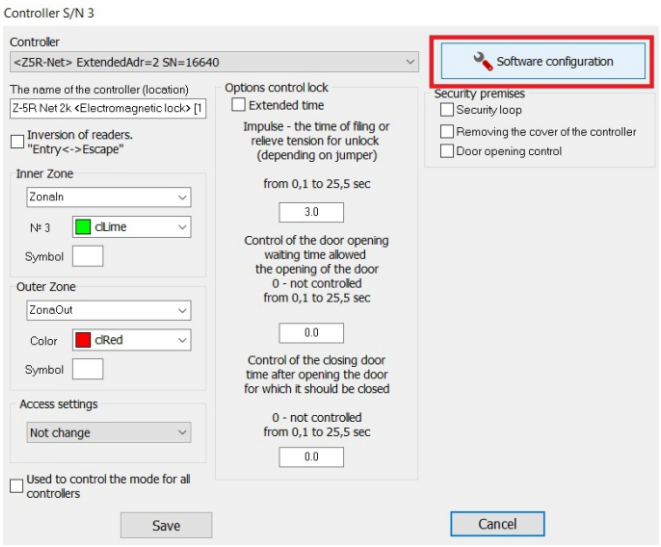



## Main parameters

1) **Controller** – a description of the selected controller.
2) **Controller name** – the name used to represent this controller in the time zone lists and events (no more than 6 characters are recommended).
3) **Inverse connection** – when the readers are connected backwards, opposite to the main logic. This is relevant for **Matrix-II Net** controllers installed in such a way that you need to bring the card to the controller for entry and not for exit (for example, at a turnstile).
4) **Inner zone – the name of the territory** closed by the controller (will be displayed on the diagrams in the reports). **Zone colour** – the colour of the icon in the list of employees when entering this zone, as well as the colour of the line on the diagram in the report. **Symbol** – a number or a letter that appears inside the icon in the list of employees.
5) **Outer zone** – similar to the inner zone.
6) **Access parameters** – choose which access parameters to assign to the cards for a given controller at the time of their creation. Allows you to speed up the configuration of access rights by simply copying the rights for any controller already included in the system.
7) **Lock control parameters** – for electromagnetic lock, it is the duration of the de-energized state of the lock, and for the electromechanical lock or electric latch, it is the duration of the voltage supply to open the lock. Also, to clarify the moment of passage, you can set the **door opening waiting time**. If this parameter is not zero, then the passage event will be formed not immediately when the card is presented but at the time the door is opened. **Door closing waiting time** informs the controller about the time to wait for the door to close, and if this time is exceeded, the controller will generate an event about leaving the door open. It makes sense to set the parameters for opening or closing waiting time only when the door sensor is installed.

## Extended Mode and software configuration of controllers

In the Extended Mode, the controllers can be configured for the desired mode of operation. To do this, right-click on the selected controller and select "Configure" in the context menu. In the controller settings menu, click the "Software Configuration" button and enter the controller configuration menu.




## Software configuration sensors and devices

The Extended Mode allows you to implement various functions, most of which are activated simply by placing the icon of the function element on the controller connection diagram. First, we will describe them, and then we will indicate their application.

| No. | Icon | Name | Description |
|---|---|---|---|
| 1 | | *Passage permission button* | *A sensor that signals the controller to start a passage unlocking cycle for an entering or exiting employee* |
| 2 | | *Turnstile exit button* | *A sensor that signals the controller to start a passage unlocking cycle for an employee exiting via the turnstile* |
| 3 | | *Turnstile entry button* | *A sensor that signals the controller to start a passage unlocking cycle for an employee entering via the turnstile* |
| 4 | | *Bell button* | *A sensor, which sends an active signal to the bell upon activation* |
| 5 | | *Door position sensor* | *A sensor, which state is used by the controller to determine the position of the door* |
| 6 | | *Security sensor* | *A circuit, which breaking or closing signals unauthorised actions* |
| 7 | | *Tamper* | *A sensor, which activation or deactivation signals the casing's unauthorised opening to the controller* |
| 8 | | *Passage blocking sensor* | *A sensor that prevents the controller from unlocking the passage* |
| 9 | | *Evacuation sensor* | *A sensor that switches the controller to "evacuation" mode to ensure unimpeded exit from the room* |
| 10 | | *Window position sensor* | *A sensor that disables the "electrical control" signal that controls the air conditioner when the window is opened* |
| 11 | | *Presence sensor* | *A sensor that prevents entry into the airlock if there is someone inside* |
| 12 | | *Lock closed position sensor* | *A sensor, which activation removes the active level from the electric motor lock in the locking mode* |
| 13 | | *Lock opened position sensor* | *A sensor, which activation removes the active level from the electric motor lock in the unlocking mode* |

| No. | Icon | Name | Description |
|---|---|---|---|
| 14 | | *Airlock signal* | *A signal, which low level indicates that a door is open in the airlock so the opening of other doors is blocked.* |
| 15 | | *Electromagnetic lock* | *A locking device requiring an active signal to lock the passage* |
| 16 | | *Electromechanical lock* | *A locking device requiring an active signal to unlock the passage* |
| 17 | | *Bell* | *An alarm device activated by the "bell" button* |
| 18 | | *Emergency alarm siren* | *A security alert device informing on the unauthorised opening of the door or activation of the security sensor* |
| 19 | | *Red LED* | *A red LED control signal on readers* |
| 20 | | *Green LED* | *A green LED control signal on readers* |
| 21 | | *Audio alarm* | *A buzzer control signal on readers* |
| 22 | | *Electrical control signal* | *A signal that controls the voltage supply to the power sources of the controlled consumers* |
| 23 | | *Mode control sensor* | *An external signal that puts the controller in "Blocked" mode and has the highest priority* |
| 24 | | *Security control sensor* | *An external signal that activates security functions* |
| 25 | | *"Sensor 1"* | *External contact sensor No. 1. Similar to No. 2,3,4* |

## Controller Z-5R Net in the Extended Mode

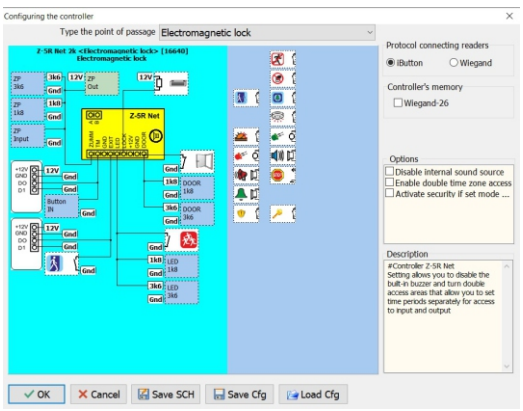
### Firmware update

The controller comes with factory firmware. To use the Extended Mode, the firmware must be updated. The firmware is updated via the RS-485 communication line, and to do this the controller must be connected to the communication line and detected by the Software. To update the firmware, you need to select the necessary controller and click the button . Next, select the firmware z5r_v3.14_ext.rom and activate the update process by confirming your intentions. After a successful firmware update, the "Software Configuration" button will be available in the controller parameter settings menu, by clicking on which you can open the "Controller Configuration" menu.

### Terminal description

The controller has only nine terminals for connection. This is a quite small number for a network controller, so the possibility of implementing the declared number of functions is not entirely obvious. However, the capabilities of modern microcontrollers make it possible to make some terminals multifunctional. **An increase in the number of connected sensors is performed using resistors connected in series with resistances of 1.8 kΩ and 3.6 kΩ, an accuracy of at least 5% and a capacity of at least 200 mW.**

Let us review the connection diagram in the menu of the programme used to configure the controller.



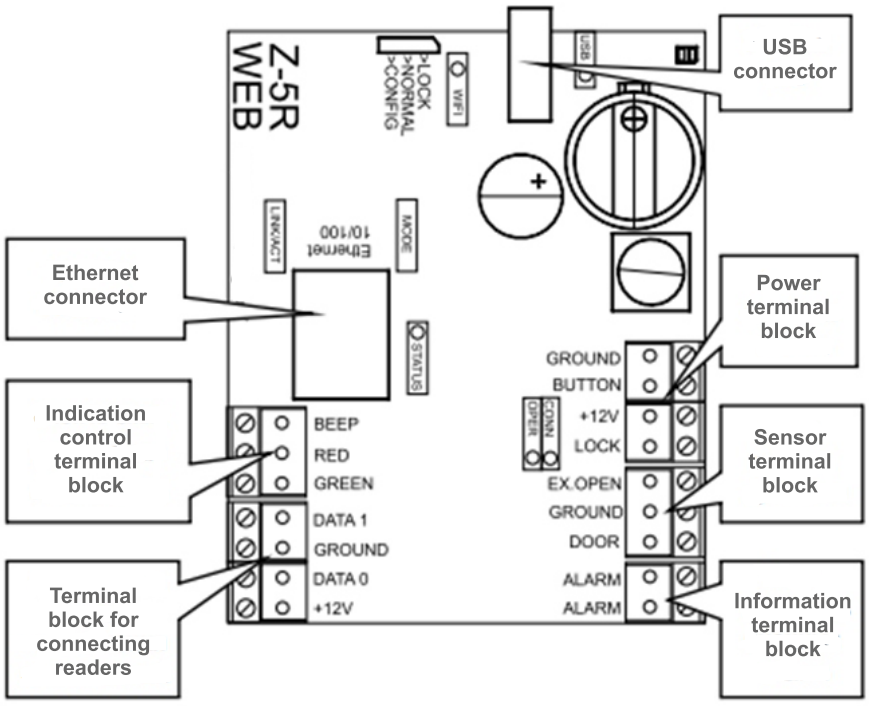
As can be seen from the diagram, the three terminals are multifunctional, namely LED, ZUMM and DOOR. Using 1.8 kΩ and 3.6 kΩ resistances, up to three sensors can be connected to each of them. Two of them – LED and ZUMM – can control external devices. It is necessary to note some limitations if the terminal is used as an output, then the input functions will not be available to it. The second limitation concerns a sensor that is connected directly without a resistor because when it is closed, it will be possible to determine the change in the state of the sensors connected via resistors only after it is opened. Therefore, we advise against connecting normally-closed sensors (for example, a reed switch) without resistors, unless you are planning to connect only these sensors and nothing else. It is necessary to indicate the peculiarity of the operation of LED and ZUMM terminals as outputs. The ZUMM output is a transistor collector pulled up to the supply voltage via a 2 kΩ resistor. In the absence of a load, the voltage at this terminal is respectively equal to the supply voltage. By producing an active signal, the controller turns on the transistor and connects this output to the ground. The transistor is equipped with overcurrent protection of up to 70 mA. You can't supply a serious load to it but it will be enough for most relays so it will undoubtedly manage to operate as a logical signal for the turnstile. When connecting a relay, you should connect one pin to +12V and the second pin to the ZUMM terminal itself and do not forget to install a bypass diode parallel to the relay coil. The capabilities of the LED are even more modest - at rest, it is pulled up to the internal +5 V via a 360 Ω resistor. When controlled, the pull-up can turn off. It was designed for the direct connection of an LED with a current of up to 20 mA. Controllable elements are connected between the output and the ground so the connection of anything between the LED and +12V terminals is unacceptable. The direct connection of any power element to this terminal hardly makes practical sense, but it can manage to control the base of the power transistor, which turns on the alarm, and also you can do without an economy resistor in the transistor base. In general, for a creative wireman, the controller turns into a construction kit and opens a huge field for the most unusual ideas.

## Controller Z-5R WEB

### Terminal description

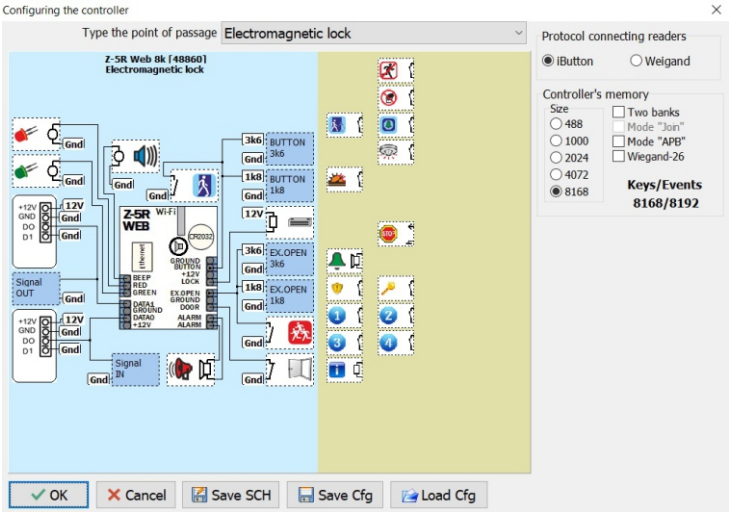
The controller has five terminal blocks for connection.

Location of terminals on the controller board




This is a quite small number for a network controller, so the possibility of implementing the declared number of functions is not entirely obvious. However, the capabilities of modern microcontrollers make it possible to make some terminals multifunctional. **An increase in the number of connected sensors is performed using resistors connected in series with resistances of 1.8 kΩ and 3.6 kΩ, an accuracy of at least 5% and a capacity of at least 200 mW.**

Let us review the connection diagram in the menu of the Guard Light Software used to configure the controller.




As can be seen from the diagram, most terminals are multifunctional, namely BEEP, RED, GREEN, BUTTON, LOCK, EX.OPEN and DOOR. Using 1.8 kΩ and 3.6 kΩ resistances, up to three sensors can be connected to the terminals BUTTON, LOCK and EX.OPEN. It is necessary to note some limitations if the terminal is used as an output, then the input functions will not be available to it. The second limitation concerns a sensor that is connected directly without a resistor because when it is closed, it will be possible to determine the change in the state of the sensors connected via resistors only after it is opened. Therefore, we advise against connecting normally-closed sensors (for example, a reed switch) without resistors, unless you are planning to connect only these sensors and nothing else. It is necessary to indicate the peculiarity of the operation of certain terminals as outputs. The terminal output is a transistor collector pulled up to the supply voltage via a 2 kΩ resistor. In the absence of a load, the voltage at this terminal is respectively equal to the supply voltage. By producing an active signal, the controller turns on the transistor and connects this output to the ground. The transistor is equipped with overcurrent protection of up to 70 mA. You can't supply a serious load to it but it will be enough for most relays so it will undoubtedly manage to operate as a logical signal for the turnstile. The direct connection of any power element to this terminal hardly makes practical sense, but it can manage to control the base of the power transistor, which turns on the alarm, and also you can do without an economy resistor in the transistor base. In general, for a creative wireman, the controller turns into a construction kit and opens a huge field for the most unusual ideas.

## Configuration

Let's go back to the configuration menu. At the top, there is a bar for selecting the type of pass point. From there, you should start configuring the controller. When you change its value, the diagram is updated - elements that are not used in this type of pass point are hidden and frequently used ones are automatically placed. Below the bar, there is a diagram with a list of available elements on the right. In the top rightmost part of the menu, there are switches common for the entire diagram, and when you select any element of the diagram, a description of the element and switches for the operating mode of this element, if any, are displayed in the lower right part of the menu. Configuration is performed by moving element icons to connection points. The icon can be captured by hovering the mouse cursor over it and pressing and holding the left mouse button. The process is similar to dragging and dropping icons on the desktop. At the same time, the available places for connecting this element in the diagram are highlighted in green and a description of this element is displayed on the right. If other terminal functions become unavailable due to using element functions, connection points for unavailable functions are automatically hidden.
The resulting diagram can be saved as a picture by clicking the "Save SCH" button for subsequent printing. You can also save the configuration to a file using the "Save Cfg" button, so that next time you can simply load it for another controller by clicking the "Load Cfg" button. This is useful when you configure multiple controllers in the same way.
Press the "Ok" button to apply the generated diagram, otherwise press the "Cancel" button.
After the configuration is complete and you return to the controller configuration menu, additional parameters are available depending on the selected functions.
"Security loop" – activate the security sensor control.
"Removing the controller cover" – made for other controllers and future modifications. "Door opening control" - activates an alarm when the door is tampered with, as well as when it is left open with the active door closing time control function.

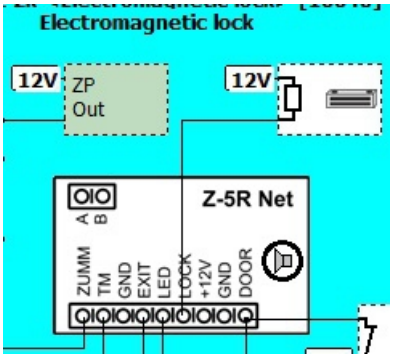
"External signal" – allows the transition to the "Evacuation" state activated by an external signal. "Temperature sensor" – allows the activation of the "Evacuation" mode when the specified threshold temperature is exceeded for models equipped with a temperature sensor. For information on setting the electrical control parameters, see below. The configuration will be loaded into the controller as soon as you exit the controller settings menu if a connection is established to it.

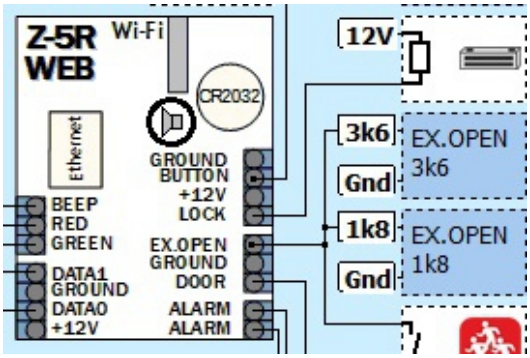
## Types of Extended Mode pass points

To simplify the configuration, there are several main types of pass points to choose from. When selecting the desired type, as mentioned above, sensors and locking devices are automatically placed and elements that are not used in this mode are hidden. You can change the purpose of some automatic connections, as well as add additional features.

### Electromagnetic lock

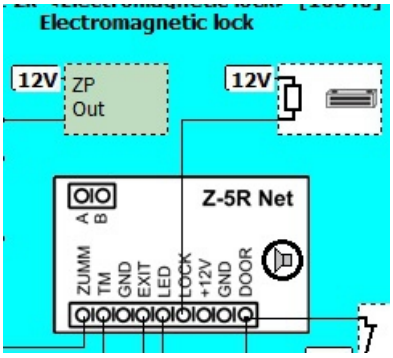
A mode of operation with an electromagnetic lock installed on the door. If a reed switch integrated into the lock is used, this must be indicated. Such sensor integration can be distinguished by the arrival of a door opening signal immediately when the lock is de-energized. On the other hand, it is possible to detect the door closure only with a powered lock.

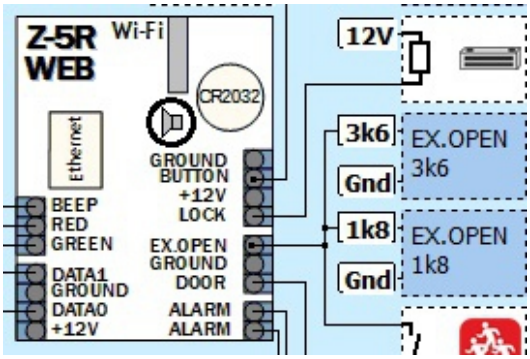



### Electromechanical lock

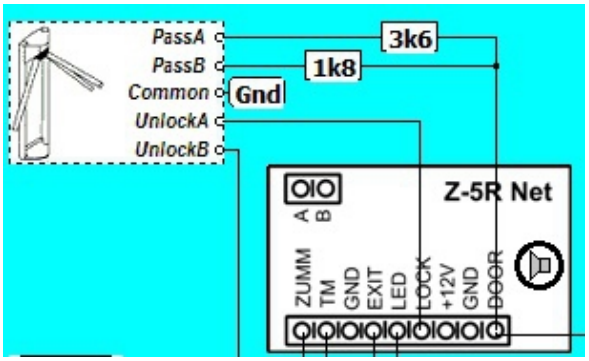
A mode of operation with an electromechanical lock installed on the door. In the emergency unlock mode, pulses will be applied to the lock. If the lock uses a low-power coil and allows a long-lasting supply of voltage, then the voltage will be supplied constantly for the duration of unlocking.




### Turnstile in Z-5R Net extended

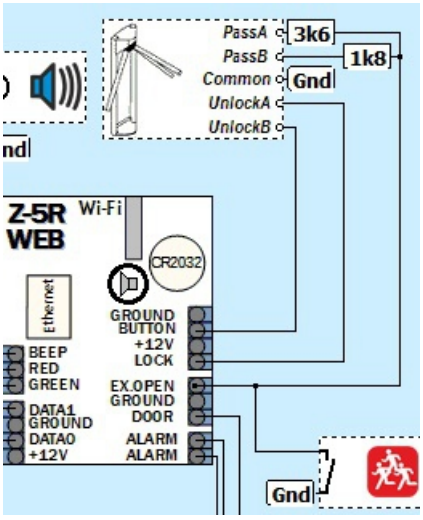
A mode of connection of the turnstile or any other device, when entry and exit require the transmission of control signals to different terminals. There are also two pass sensors - one for entry and the other for exit. In the "Evacuation" mode, an active level is transmitted to both control signals. Turnstile control should operate in potential mode, i.e. the turnstile should be unlocked only for the duration of the control signal. It should be noted that due to the presence of a resistor that pulls up the ZUMM pin to +12V, some models of turnstiles will work correctly only if the supply voltage of the controller is equal to the supply voltage of the turnstile control unit.



The controller itself can operate at a supply voltage of up to 20 V. Buttons for manual control of the turnstile are connected in parallel with the readers, so with normally open buttons there are no problems, and when using normally closed buttons you should connect them in any other place. If the buttons are connected in parallel to the output signals, the controller will perceive the passage using a button as a break-in attempt and form an emergency event. If you do not intend to use buttons, we recommend that you simply remove them from the diagram.

*** Resistances of 1.8 kΩ and 3.6 kΩ - accuracy of at least 5% and power of not less than 200 mW.**

## Turnstile in Z-5R WEB

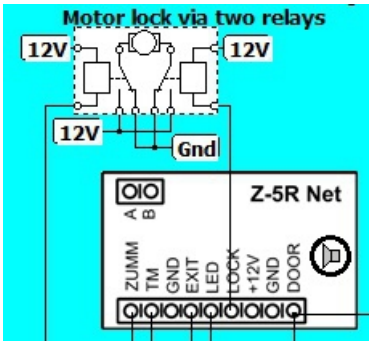


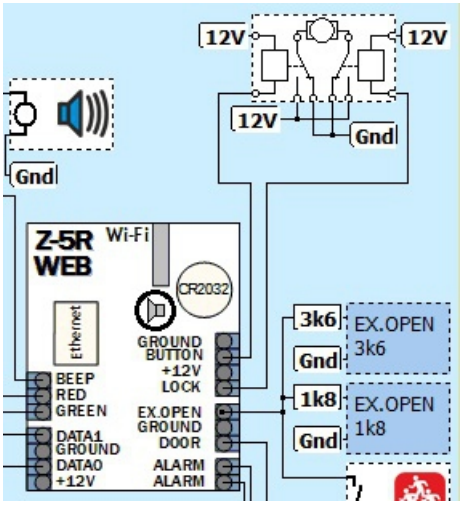

A mode of connection of the turnstile or any other device, when entry and exit require the transmission of control signals to different terminals. There are also two pass sensors - one for entry and the other for exit. In the "Evacuation" mode, an active level is transmitted to both control signals. Turnstile control should operate in potential mode, i.e. the turnstile should be unlocked only for the duration of the control signal. It should be noted that due to the presence of a resistor that pulls up BUTTON and LOCK pins to +12V, some models of turnstiles will work correctly only if the supply voltage of the controller is equal to the supply voltage of the turnstile control unit. Buttons for manual control of the turnstile are connected in parallel with the readers, so with normally open buttons there are no problems, and when using normally closed buttons you should connect them in any other place. If the buttons are connected in parallel to the output signals, the controller will perceive the passage using a button as a break-in attempt and form an emergency event. If you do not intend to use buttons, we recommend that you simply remove them from the diagram.

*** Resistances of 1.8 kΩ and 3.6 kΩ - accuracy of at least 5% and power of not less than 200 mW.**

## Motor lock via two relays

A connection mode for the motor lock (activator) or any other device, in which in order to switch the locking device to the "closed" or "open" state it is necessary to transmit control signals to different terminals or supply a voltage of different polarity, for example, a gate-lifting control device.



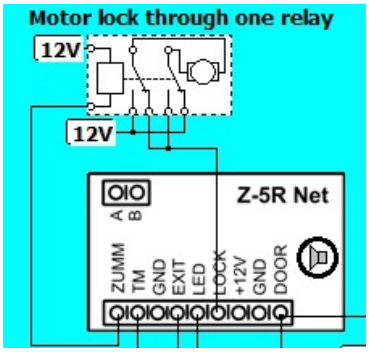



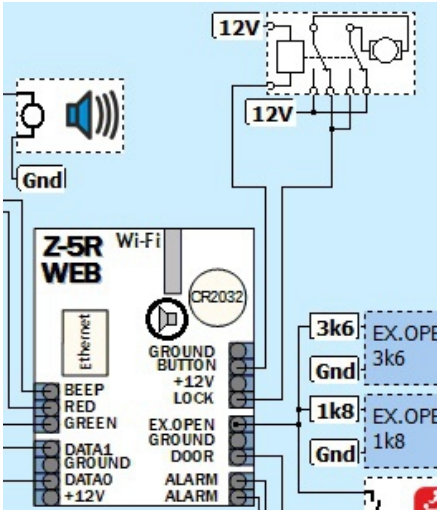

In the Z-5R Net controller, the active pulse for opening is transmitted to the LOCK terminal, and for closing - to the ZUMM terminal. In the Z-5R WEB controller, the active pulse for opening is transmitted to the LOCK terminal, and for closing - to the BUTTON terminal. It is also possible to connect end sensors to remove the control signal when the locking device reaches the end position. The current and voltage supplied to the locking device are switched by external relays or a circuit of the locking device itself. When "trigger" mode is enabled for this type of pass, the controller will be turning on each relay in turn. When the "Stop Command" mode is activated, both signals are turned on simultaneously before each activation for opening or closing, which means the "stop" command for some control units. The duration for which the active level is issued is the time of the open state of the lock and it can be limited by means of an end position sensor. When the sensor is triggered without a controller command, messages are generated that can be used to verify if the sensors are connected correctly.

**Due to the fact that locking the motor lock when the door is open can lead to its breakage, there is no automatic locking after any time - it can be done only by the door sensor or after a certain time if the door is not opened.**

**Motor lock via one relay**

A connection mode for the motor lock (activator) or any other device, in which in order to switch the locking device to the "closed" or "open" state it is necessary to supply a voltage of different polarity, for example, a car activator.



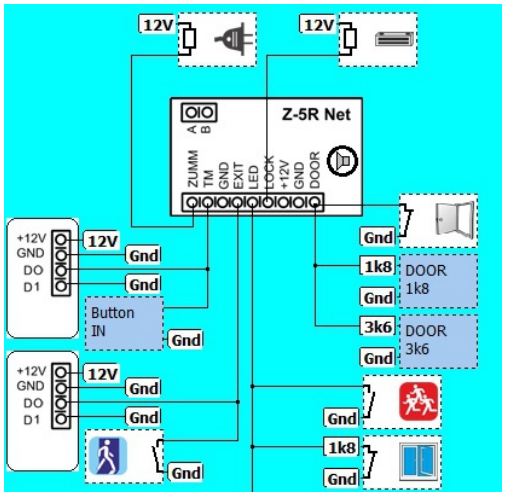



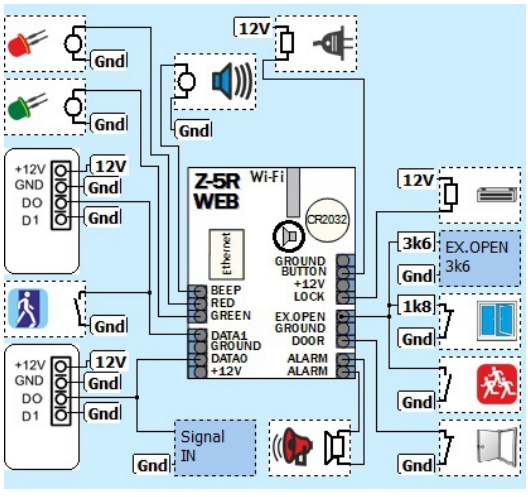

It is also possible to connect end sensors to remove the control signal when the locking device reaches the end position. The current and voltage supplied to the shut-off device are switched by an integrated current-controlled switch and the relay determines only the polarity of the supplied voltage. The current-controlled switch is activated with a delay after the relay is switched, which ensures the switching of terminals at zero current resulting in longer service life of the relay. The duration for which the active level is issued is the time of the open state of the lock and it can be limited by means of an end position sensor. When the sensor is triggered without a controller command, messages are generated that can be used to verify if the sensors are connected correctly.

**Due to the fact that locking the motor lock when the door is open can lead to its breakage, there is no automatic locking after any time - it can be done only by the door sensor or after a certain time if the door is not opened.**

**Electrical control**

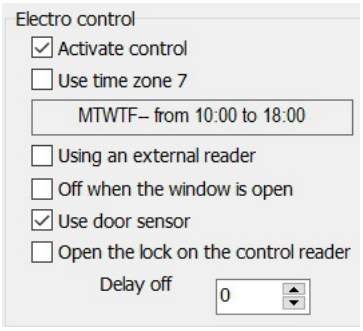
A mode in which power supply is additionally controlled, in addition to standard access control.



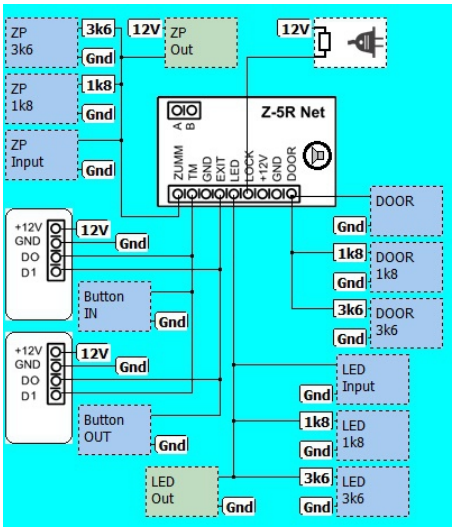

It is designed to provide de-energizing of power sockets or air conditioning in hotel rooms if there are no customers in them. An external power relay is used for power management. Readers must be connected via the iButton protocol, which allows you to determine whether the card is in the reader's zone or not. For the continuous power supply, the client must fix the card in the reader inside the room.

Configurable parameters, "activate" - activate the "Electrical Control" mode, otherwise it will not work. "By time zone 7" - automatically turn on the power relay during the activity of time zone 7, even if there is no client in the room. "By the external reader" - changes the operation logic. The card should be fixed not near the internal reader but the external one used for entry. "Turn off by the window sensor" - turns off the power relay when the window opening sensor is triggered. "Use the door sensor" – turn off the power relay without delay immediately after closing the door when the client leaves the room. "Open by the control" - perform a cycle of unlocking the door when the card is brought to the internal reader. "Shutdown delay" - time in seconds during which the power relay must remain on after the card is removed from the control reader.




**Auto control**

A mode for the car, in which the power supply to the signal device is managed when the state of the car sensors changes.

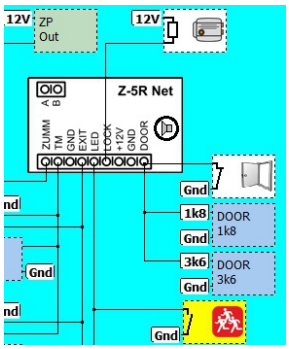


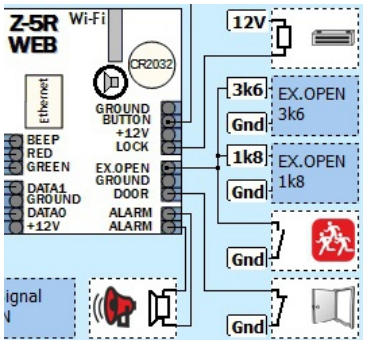

## Advanced Extended Mode features

In this section, the additional features introduced in the new firmware will be described. Most of them work autonomously and do not require any special actions by the control programme, except for configuration.

**Evacuation**

A function to ensure unhindered evacuation of people from the premises in case of emergency.



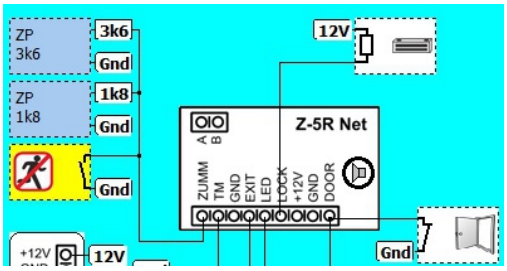



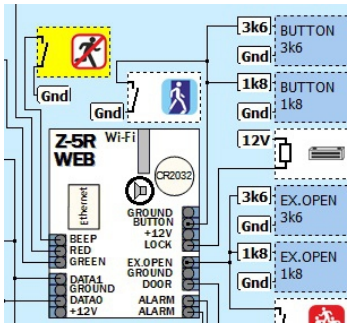

It has the highest priority and unlocks the lock or other locking device regardless of any active blocking. For reliable operation, it is recommended to connect it directly without a resistor, so that the state of other sensors does not affect the signal detection. The signal source can be the fire protection system controller, as it has several relays to inform external systems about the emergency, but you can also use a simple toggle switch at the guard post, since not only a fire can be the cause of the evacuation. In order for the controller to process this signal, do not forget to check the "External signal" box in the controller parameter settings menu. When a signal is detected, the controller independently unlocks the passage and generates an event. For the entire network to respond to the event, it is not necessary to transmit the signal to all controllers.

It is enough to connect the line to one controller and use the Z-397 Web converter with the firmware z397web_v3.0.66_fire.rom for communication. If the Software is running, then when a signal is detected, it will switch all controllers to evacuation mode. If the Software is shut down, the converter will do this. The only limitation is that unlike the Software, the converter unlocks only the controllers connected to it, so when using several converters, the evacuation signal must be transmitted to at least one controller for each converter.

**Blocking**

A function that has a reverse effect. Not to be confused with "Blocked" mode! Any attempt to pass will be blocked.



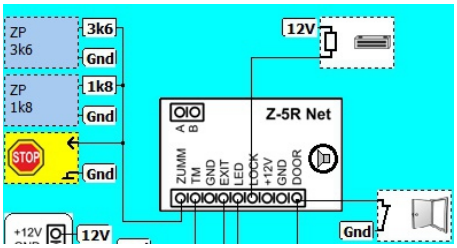

Neither the card nor the button or the Software command via the network can unlock the passage. Only the "evacuation" signal can overpower this mode. The meaning of this function is to help the security service in blocking the passage in the event of emergency situations. It is possible to control it via the security alarm system or simply from the toggle switch near the security guard's workplace. The mode is not broadcast to all controllers, so if several controllers need to be blocked, you need to transmit this signal to all of them.

**Airlock**

A function ensuring passage through a corridor with two or more doors provided that only one door can be opened at a time. Additionally, it is possible to use the presence sensor in this mode, that is any device that detects someone's presence inside the airlock. It can be either a weight sensor or an optical sensor. With an active signal level from such a device, the controllers block entry, so only exiting is allowed. It works as follows: initially, the potential on the ZUMM line (for Z-5R web - BEEP or other terminals) is high, so when its door opened, the controller sets zero potential while another (other) controller(s) blocks the passage after detecting a low level on the ZUMM (for Z-5R web - BEEP or other terminals). After closing the door, the controller restores the high level on the line allowing passage through other doors.

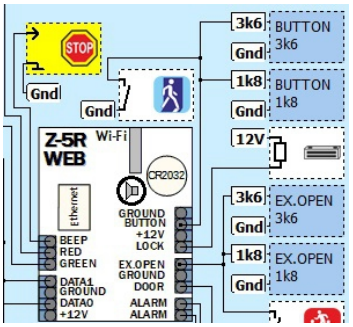
**Z-5R Net Airlock**

For this mode, the ZUMM terminal is used. All controllers operating in the airlock must be combined via ZUMM. Again, the twisted pair should connect all the controllers uniting them with one wire to ZUMM and the other to the grounding.



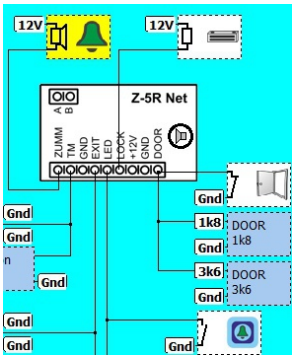

**Z-5R Web Airlock**

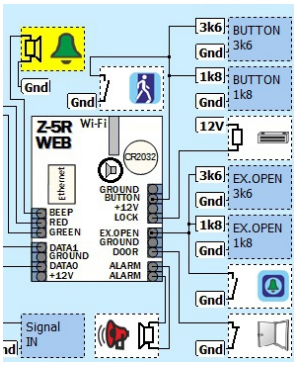
For this mode, BEEP (or RED, GREEN, or BUTTON) terminals are used. All controllers operating in the airlock must be combined. Again, the twisted pair should connect all the controllers uniting them with one wire to BEEP (or RED, GREEN or BUTTON) and the other to the grounding.




**Bell**

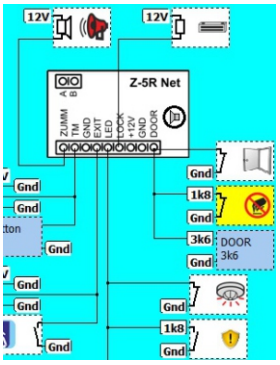
A simple service function. When you press the "bell button", the output signal "Bell" is put into an active state and lasts for three seconds from the last press of the button. In addition, a notification to the Software is generated. It allows you to connect calling devices and log their use.

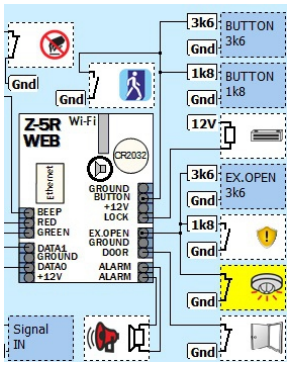



## Security

A function that allows integration into security systems.

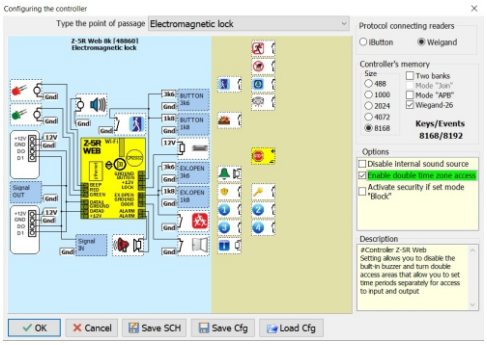



For its operation, the following elements are used: "security", "security circuit", "tamper", "door sensor" and "alarm". When the function is active, the controller checks the status of the security loop and tamper signalling when their state changes. The door sensor activates an alarm when the door is broken in or left open for a time longer than the time specified in the closing control parameter. A motion sensor or a reed switch on a window or safe can act as a security sensor. The siren output signal has a logic level or will be able to power the real sound system when assigning this function to the LOCK terminal. One solution is to connect a relay and use its terminals to supply power to the siren or to give a signal to the security console receiver, if any. You can turn the function on or off either by an external signal, for example, from a control panel, or by a command from a computer. It is also possible to set the "Security" function to turn on automatically when the "Blocked" mode is turned on. To visually monitor the mode when the feature is enabled, a security status icon will appear next to the controller status icon.

## Dual time zones

An additional set consisting of seven access time zones. Previously, each time zone set a time for entry and exit. Now, by selecting access by time zones, you can separately assign time ranges for entry and exit. Zones are assigned only in pairs - entry and exit. You cannot separately set the entry time from one zone and the exit time from another.




This feature is enabled by setting additional parameters on the controller.

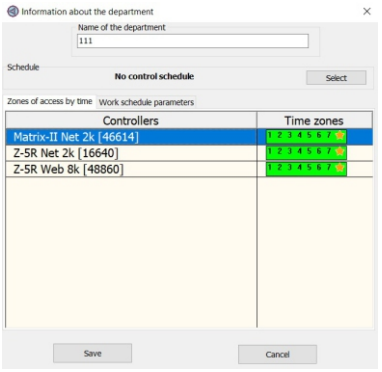
## Controller firmware updates

The controller comes with factory firmware. The firmware is updated via the RS-485 communication line, and to do this the controller must be connected to the communication line and detected by the Software. To update the firmware, you need to select the necessary controller and click the button ("Update Firmware"). Next, select the appropriate firmware (for example: m2n_v2.23_blk.rom; z5r8_v2.25_blk.rom; z5r_v2.21_blk.rom) and activate the update process by confirming your intentions.

*"Database tools" tab*

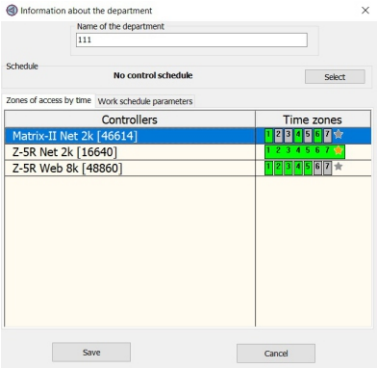
## List of departments

To create a department, open the context menu with the right mouse button by placing the mouse pointer on the list of departments or select the main menu item "**Department**". Next, select the **Create Department** item to open the department form that should be filled in, specifying: The name of the department and the **allowed access time zones** for the department being created. Their configuration and purpose will be discussed below. If you need to manage labour discipline when calculating working time, you should choose a **work schedule**.




## Access time zones

On the "Access time zones" tab, the department's access to certain controllers in the database by the selected time zone (or by several zones) of the controller or full access to the controller can be configured. Access zone configuration begins by removing the active "Full Access" mode by clicking on the orange star with the left mouse button. When the "Full Access" mode is inactive (grey star), you can enable or disable the controller's seven time zones.




## Work schedule

To control labour discipline, you need to create a work schedule, in which you should specify:
Daily routine.

1) Beginning of the working day in the department;
2) End of the working day;
3) Beginning of lunch;
4) End of lunch;
5) Short day;
6) End of the short day;
7) The type of work schedule is flextime or with a night shift.

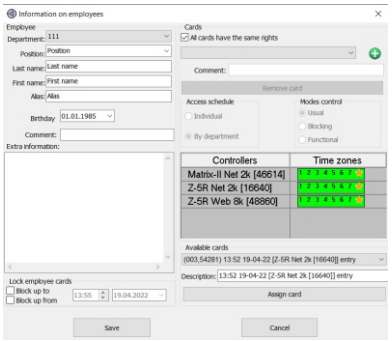
Check the boxes "Flextime/Night Shift" if the schedule is round-the-clock or shift.
To transfer the time calculation to the next day, you need to check the "Nighttime each day" box.
Monitoring labour discipline.

1) Permissible early arrival, time in minutes, how much earlier than the beginning of the working day can employee show up;
2) Late arrival, time in minutes, how much later than the beginning of the working day can employee show up;
3) Leaving early, time in minutes, how much earlier than the end of the working day can employee leave;
4) Leaving late, time in minutes, how much later than the end of the working day can employee leave;
5) Absence, time in minutes, how much in total can the employee be absent from the workplace during working hours per day.

You can view the work schedule settings on the "**Work schedule parameters**" tab.

The "**Create**" button allows you to create a new schedule with fields filled with default values, and the "**Copy**" button also creates a new schedule but with fields filled in in the same way as the selected schedule. Assign a new work schedule to a department by clicking the "**Use the selected schedule**" button.

## List of employees

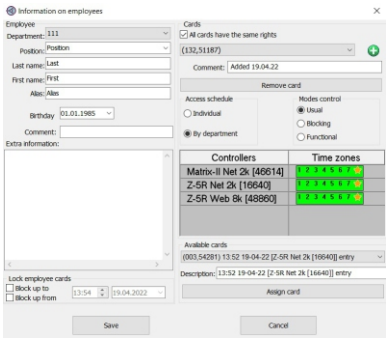


After you have created a department, you can create employee records.
Similar to creating a department, right-click on the list of employees to open the context menu and select the **Create** item. The appeared form must be filled in with the employee information.
The form has the following fields:

1) Position;
2) Employee last name;
3) Name;
4) Middle name;
5) Date of birth;
6) Comment – it will be displayed in the list of employees (for example, local phone number);
7) Additional information – several lines of text related to this employee (for example, passport number, home address and phone numbers);

Blocking allows you to cancel the employee's access to all controllers in case of the employee's business trip or vacation. This will prevent the use of employee cards in their absence.

## Employee cards



Multiple cards can be assigned to a single employee. Thus, for example, the employee arrives at work using one card to open the barrier in his/her garage, and then uses a handy and convenient bracelet to move inside the office. By assigning different levels of access for each card, it is possible to ensure the inability to leave the office using the bracelet.

1) Card functionality – each uses its own configuration or configuration is the same for every card;
2) List of cards;
3) Manual card registration button – allows you to record cards and codes manually and create records for access by using two cards or a code and a card;
4) A comment to the card will be displayed next to the number, for example, "bracelet" or "own card";
5) A button used to remove the card from the employee. After clicking it, the card goes to the list of available cards;
6) Access schedule – the allowed time zones are either taken from the department parameters or configured individually for this employee;
7) Mode control – whether the card has the right to change the access mode of the controllers;
8) Available cards – a list of unknown cards detected by readers and cards removed from employees;
9) Blocking – allows you to block all the cards of the employee either up to a specified moment (until returning from the vacation) or from a set time (for temporary employees).

### Adding a new card

Reader connected to the controller.

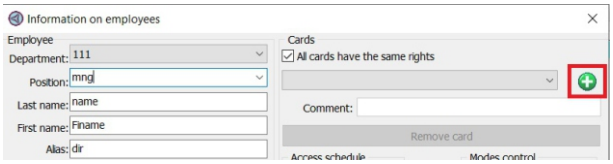
To add a new card, bring it to the reader and the controller will mark it as an unknown card and place it in the list of available cards. To assign an available card to an employee, you need to click on the "Assign Card" button. When you are finished entering the information, you should click the "Save" button.
The card must be brought to the reader before opening the "Employee information" menu.

Desktop reader.

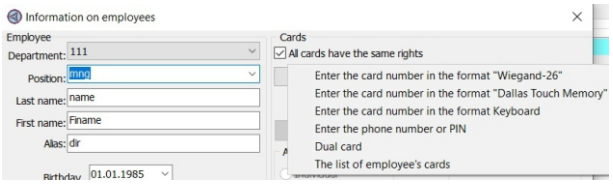
It is possible to add cards using readers **Z-2 EHR USB, Z-2 USB** and **Z-2 USB MF**. To do this, the reader must be connected to the computer with drivers installed. When you open the employee properties menu, devices are scanned and if a reader is detected, it will be connected to the Software. "**Z-2 USB**" will be added to the name of the "Available Cards" menu, and in this case, when you bring a new card to the desktop reader, its code will be added to the list of available cards. To assign an available card to an employee, you need to click on the "Assign Card" button. When you are finished entering the information, you should click the "Save" button.

Manual input.

It is possible to add cards manually. After opening the Employee Information menu, click on the button in the form of a green circle with a white cross in the "Card" panel.



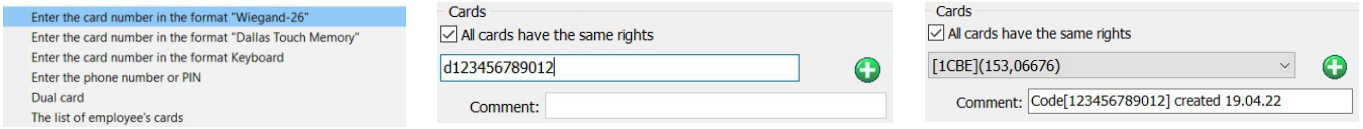

A list of possible ways and formats for the card registration will unfold.



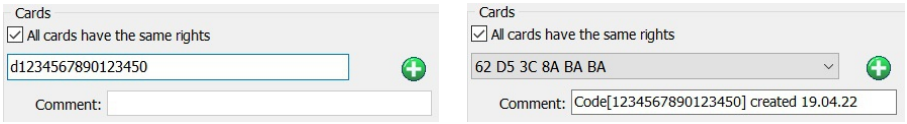

**"Enter the card number in the Wiegand standard"** – the number is entered in text form (123,45678).

Entering the number should be finalised by pressing the "Enter" key on the computer keyboard. When you're done inputting the number, you'll see a comment about the number you entered and the creation date.

**"Enter the card number in Wiegand standard" in decimal format** – the number is entered as decimal digits (d123456789012). The letter "d" should be written before the digits. The digits are converted to a text standard ([1CBE] (153,06676)).



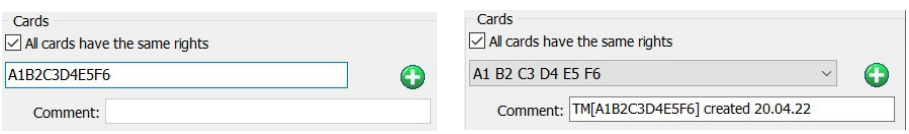

If you enter a long number (d1234567890123450), it will be written in hexadecimal form (HEX) (62 D5 3C 8A BA BA).



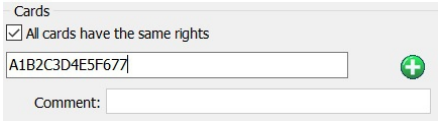

Entering the number should be finalised by pressing the "Enter" key on the computer keyboard. When you're done inputting the number, you'll see a comment about the number you entered and the creation date.

**"Enter the card number in the Dallas TM standard"** – the number is entered in hexadecimal form (HEX) (A1B2C3D4).

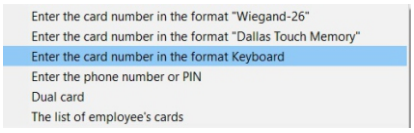
Entering the number should be finalised by pressing the "Enter" key on the computer keyboard. When you're done inputting the number, you'll see a comment about the number you entered and the creation date.
The length of the card number should not exceed 6 bytes (A1B2C3D4E5F6).

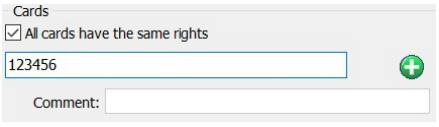


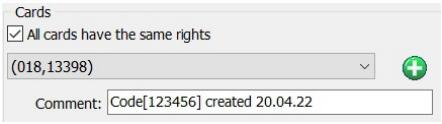
If the number length is greater than 6 bytes (A1B2C3D4E5F677), the top bytes are cut off (B2C3D4E5F677).



"**Enter a code for key input**" – the code is entered in decimal digits (123456).

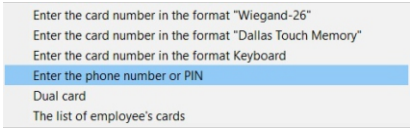


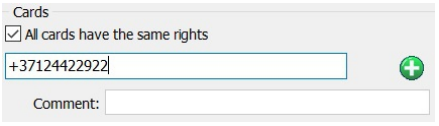




Entering the number should be finalised by pressing the "Enter" key on the computer keyboard. The number is converted to a text format (Wiegand). When you're done inputting the number, you'll see a comment about the number you entered and the creation date.

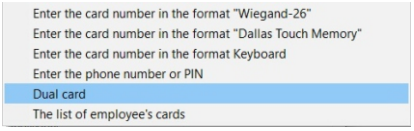
"**Enter phone number or pin code**" – the phone number is entered in full (+37124422922).

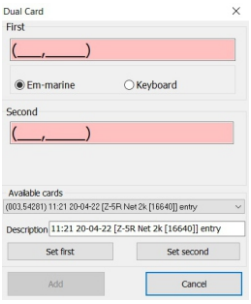


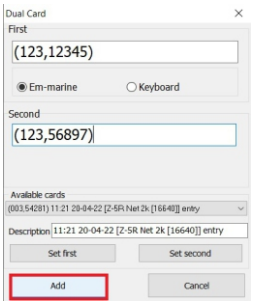
Entering the number should be finalised by pressing the "Enter" key on the computer keyboard. The number is converted to hexadecimal format (HEX) (07 93 12 8A 38 23). When you're done inputting the number, you'll see a comment about the number you entered and the creation date.

"**Dual card**" – numbers are entered in several ways.

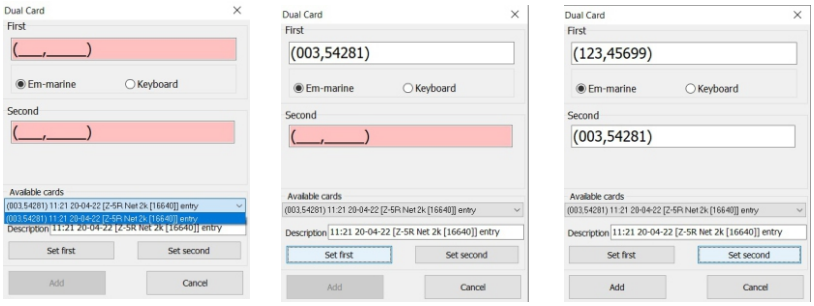



***Manual entry of card numbers in Wiegand format*** (text view). The card input is confirmed by clicking on the "Add" button. In the same way, you can also assign one card to the employee and the second shared (confirming) card to the guard. The shared card must be entered manually.

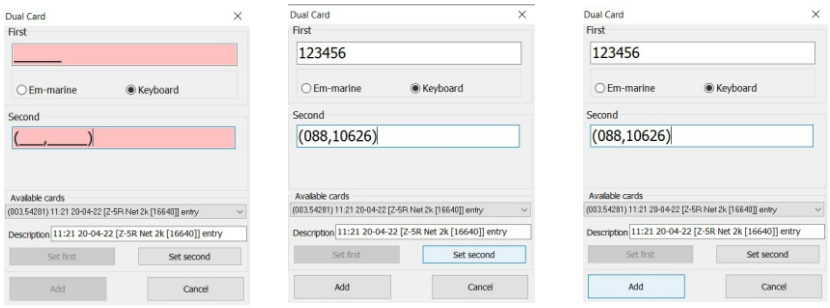



A dual card is entered from the expandable "Available cards" menu.

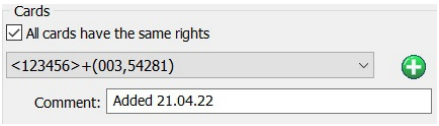



First, the first card is selected and assigned by clicking on the "Assign First" button. Then the second card is selected and assigned by clicking on the "Assign Second" button. The card input is confirmed by clicking on the "Add" button.

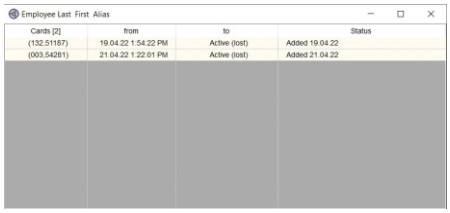
***Entering a code and a card.*** A keyboard code is entered as the first card, then the second card is entered manually or from the "Available cards" list. In the same way, you can also assign the first code to the employee and the second shared (confirming) card to the guard. The shared card must be entered manually.




The card input is confirmed by clicking on the "Add" button. Entering the number should be finalised by pressing the "Enter" key on the computer keyboard. After that, a dual card ((088,10626)+(079,08365)) and a comment to it will appear in the menu.



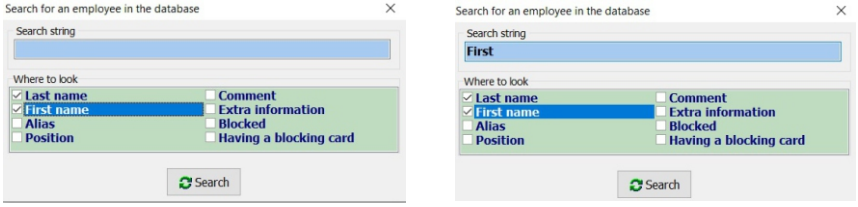

"**List of all employee's cards**" – a menu opens with a list of all employee's cards and information about their duration and status.



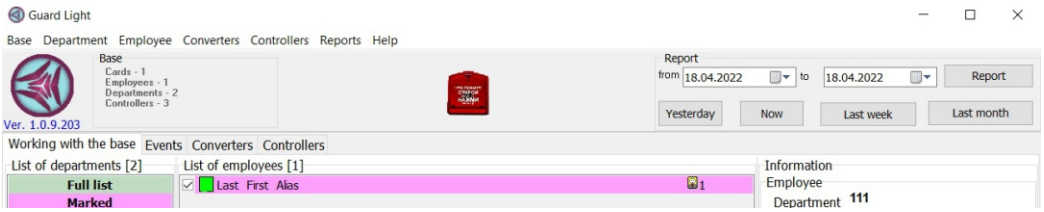
When you are finished entering the information about the employee, you should click the "Save" button.

## Search for an employee in the database

To speed up the search for an employee with any filters, the search bar is used.




Using the panel, you need to set the search string and specify which fields should be searched. After clicking the **Search** button, the Software will search the database and all employees matching the search string will be highlighted and displayed in the list of marked employees.




Special search characters such as asterisks, etc. are not supported.

## "Information" panel

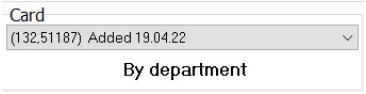
The "Information" panel in the "Database Tools" tab displays information about the selected employee and the status of the controllers' time zones.

**Employee**

All information about the selected employee is displayed here (Last name, First name, Middle name; Position; Date of birth).

**Card**

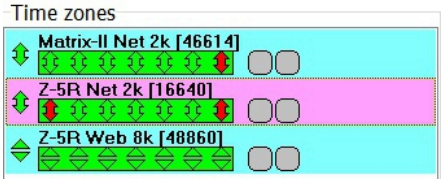
The "Card" panel displays information about the cards assigned to this employee.



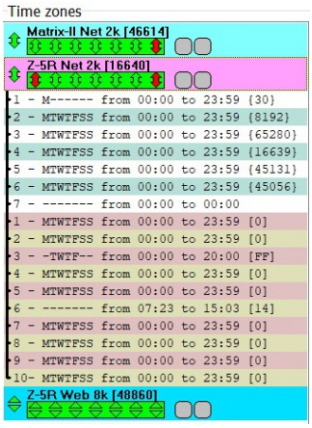

Below is the designated "Work Schedule" for the assigned cards (Individual, By Department).

**Time zones**

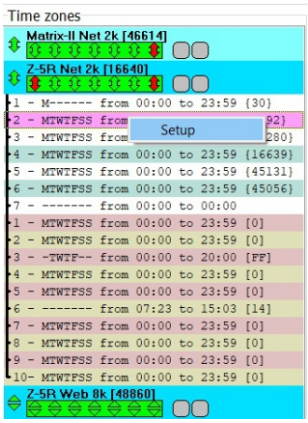
The "Time Zones" panel shows the time zones of all controllers and their status.




As mentioned above, time zones are periods of time when access to the premises is allowed. In the window under the name of the controller, 8 green or red arrows are shown. Arrows have two directions - "up" is the entrance and "down" is the exit. Green means that at the current time this zone is active and the passage through it is allowed and red means that the passage is prohibited. The left (first) arrow shows in which direction the passage is allowed at the moment through this pass point using the said card. This is the final result of the effect of all time zones. The current state for each time zone is shown by a group of seven arrows on the right. The leftmost arrow in the group displays the first time zone and so on - 2...7. If all arrows are contained in one common rectangle, this means that access without a time limit is assigned for this card, and if each arrow is in its own rectangle, this means that time zones are selected for the card. Double-clicking on the controller name (or its description) expands (collapses) the time zone description.

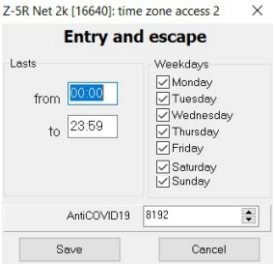


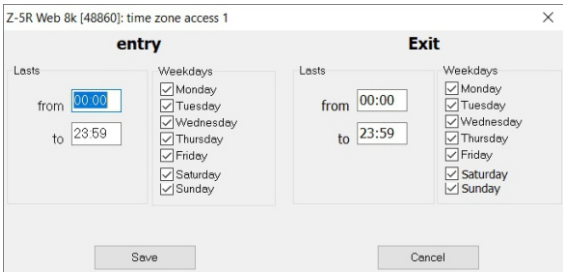
To change the time zone settings, select it and open the context menu with the right mouse button.




The configuration form contains the following fields:

1) "Duration" - the beginning and end of the zone's effect;
2) "Weekdays" are the days of the week when the zone is active.



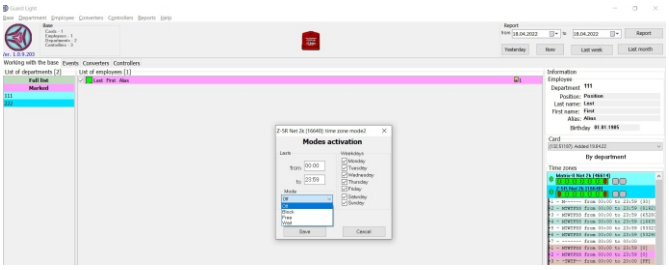

**Attention!** For the night shift, the days of the week set the beginning of the zone's effect, i.e. if it is set that the zone begins to operate from 10 p.m. to 7 a.m. and access is allowed only on Monday, then it will begin its operation on Monday at 10 p.m. and end on Tuesday at 7 a.m.

**Attention!** The zone is not related to the department work schedules, i.e. it is configured separately and should be obviously wider. For example, if the start of the working day is at 8 a.m. and the allowable early arrival is 30 minutes, then the zone should be activated not at 7:30 a.m. but earlier because before the beginning of the zone activation, the employee will not be able to get into the room. Therefore, the beginning of the zone's effect should be set at 7 a.m. or maybe even earlier. If the access of employees to the premises is regulated in another way (guards, mechanical locks, round-the-clock mode of operation), then it is recommended to leave the zones active round-the-clock in order to avoid misunderstandings.

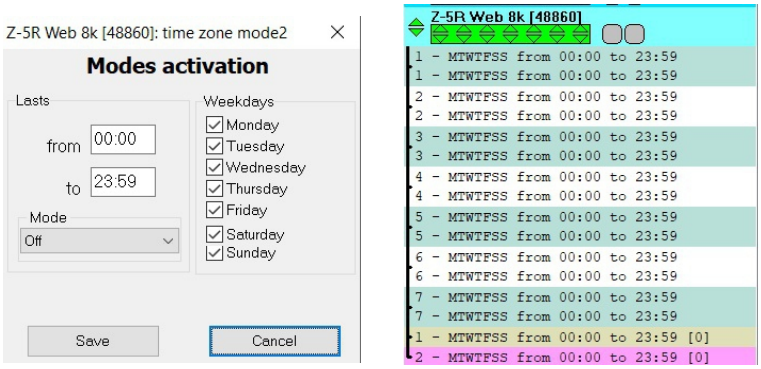
Also, when the dual time zone mode is activated in the controllers, each zone allows you to separately set the activation time and the days of the week for entry and exit.

**Time zones for enabling modes**

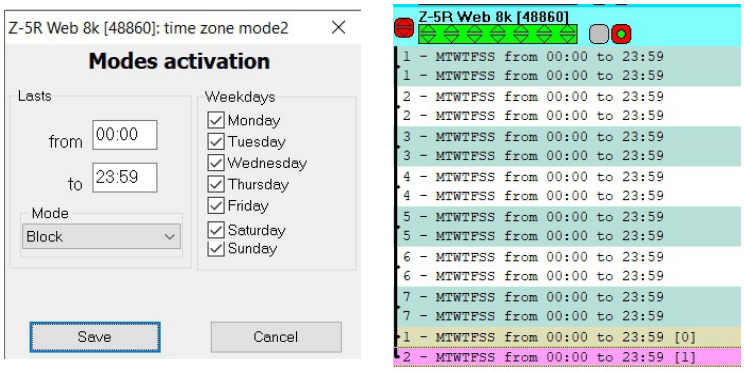
When using controllers with firmware that supports switching access modes using time zones, two more zones are added in which the access mode is additionally configured.



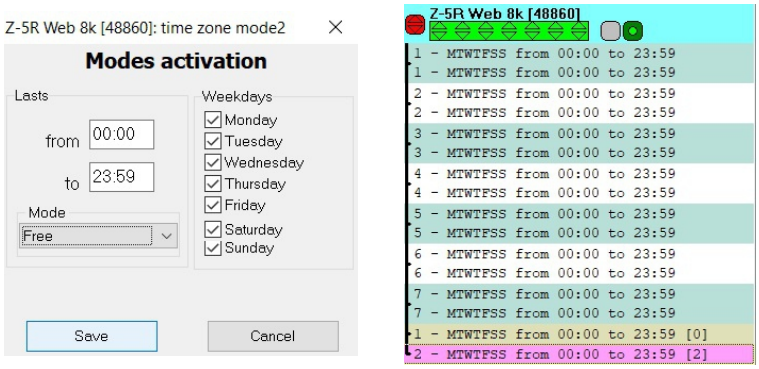
After double-clicking with the left mouse button on the 1st or 2nd zone for enabling the modes of the selected controller, the "Enable Modes" menu opens. By default, the "Inactive" mode is set.



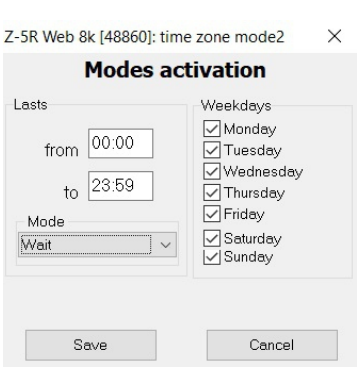

When you select the "Blocked" mode, the mode's duration and the days of the week when the mode will be active are set. To save the mode, you need to click on the "Save" button. The mode will automatically turn on in the controller at the specified time. The passage via the cards and the exit button will be blocked. You will be switched to the "Inactive" mode after the "Blocked" mode expires.

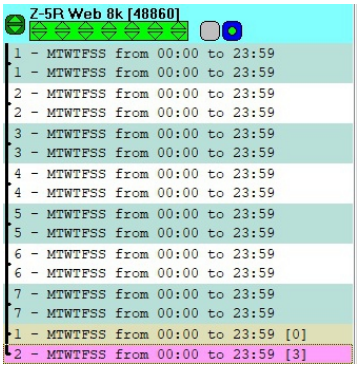



When you select the "Free" mode, the mode's duration and the days of the week when the mode will be active are set. To save the mode, you need to click on the "Save" button. The mode will automatically turn on in the controller at the specified time. The controller will switch into a free passage state and the lock will be de-energized. It will be switched to the "Inactive" mode after the "Free" mode expires.




When you select the "Standby" mode, the mode's duration and the days of the week when the mode will be active are set. To save the mode, you need to click on the "Save" button. The mode will automatically turn on in the controller at the specified time. The controller will enter the "Standby" state until the first pass card is presented. After reading the card, the controller will switch into the "Free" mode and the lock will be de-energized. It will be switched to the "Inactive" mode after the "Standby" mode expires.

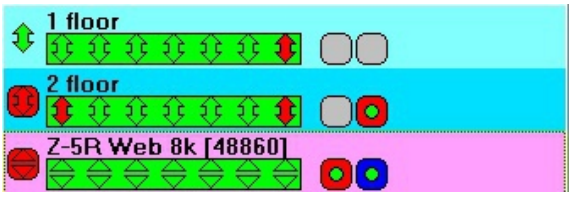



Mode activation indication.

| | |
|---|---|
| | "Inactive" mode |
| | "Blocked" mode is enabled |
| | "Blocked" mode is active |
| | "Free" mode is enabled |
| | "Free" mode is active |
| | "Standby" mode is enabled |
| | "Standby" mode is active |

Examples of indications for enabled and active modes.




## "Database" main menu

### Overwrite everything in the controllers

After you have recorded or changed the database of employees, the Software **automatically** updates the information in the controllers.

In cases of controller failure or malfunction, it is recommended to perform a complete update of the information in all controllers, and to do this you should select the **Overwrite everything in the controllers** menu item.

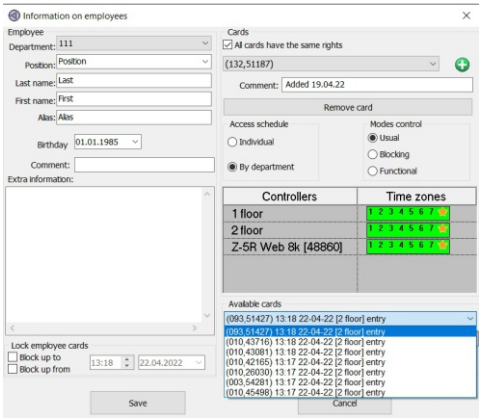
### Backup copy...

The next menu item **Backup copy/Load** is intended for the database restoration from the copy saved using the next menu item - **Backup copy/Save**. In addition, the Software automatically saves the last 10 configurations. They can be used to restore the database immediately after the problems are detected before making changes in other ways.

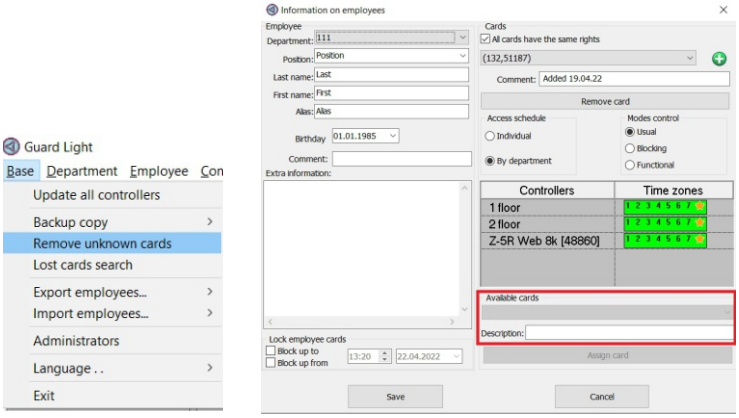
Please note that uploading the backup copy will completely replace the database and it will be impossible to restore it, therefore, before uploading the backup copy, save the current database in another backup copy. Updating the information in the controllers should be carried out by selecting the **Overwrite everything in the controllers** menu item.

## Delete unknown cards

If there are many card numbers in the "Available Cards" panel attached to the controller's reader, you can delete them.

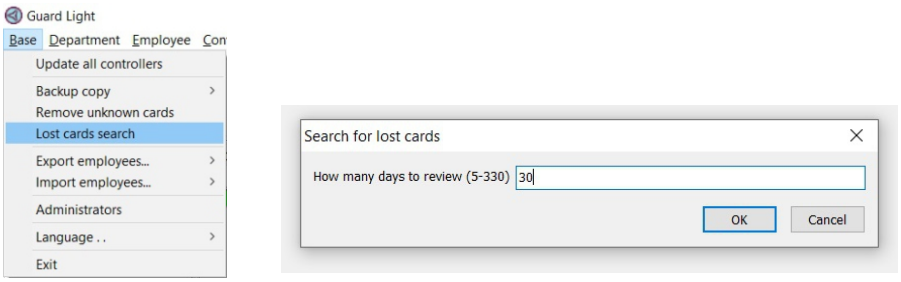



To do this, go to the "Database" main menu and left-click on "Delete unknown cards". The card numbers in the "Available Cards" panel will be deleted.




## Search for lost cards

To search for lost cards or cards that have not been read by the reader in a long time, you need to click on "Search for lost cards" in the "Database" main menu. In the "Lost cards" menu that appears, specify the time for searching for the cards and click on the "OK" button.

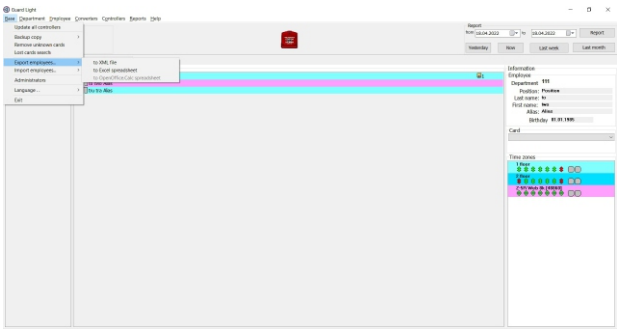



On the "Database Tools" tab, select the desired department.

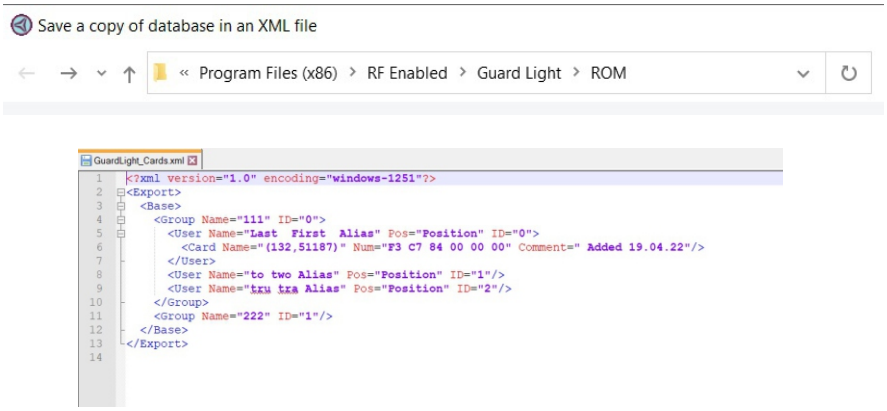
In the list of employees, the lost cards will be displayed with an icon in the form of a red clock.

## Exporting the list of employees

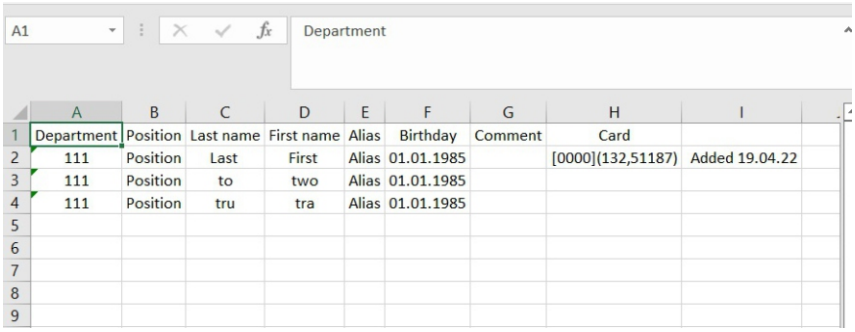
It is possible to export lists of employees for separate processing. Export is supported to XML formats and MS Excel or OpenOfficeCalc (LibreOfficeCalc) table. MS Excel or OpenOfficeCalc (LibreOfficeCalc) must be installed on the computer.



Export to an XML file. You can open the file with a browser.




If you have Microsoft Excel installed, you can export to an Excel spreadsheet.



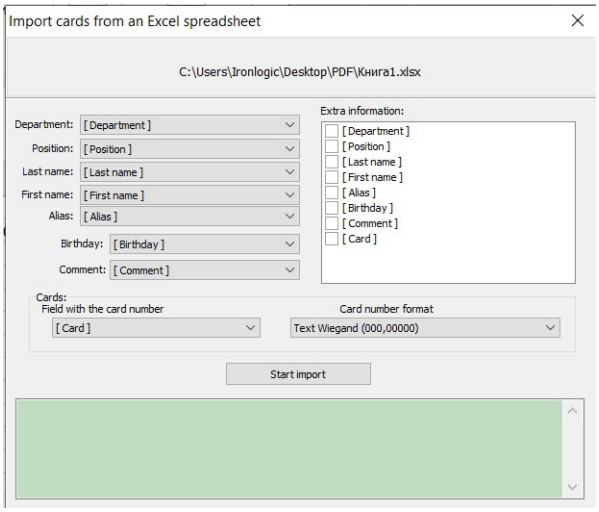
| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Department | Position | Last name | First name | Alias | Birthday | Comment | Card | |
| 2 | 111 | Position | Last | First | Alias | 01.01.1985 | | [0000](132,51187) | Added 19.04.22 |
| 3 | 111 | Position | to | two | Alias | 01.01.1985 | | | |
| 4 | 111 | Position | tru | tra | Alias | 01.01.1985 | | | |
| 5 | | | | | | | | | |
| 6 | | | | | | | | | |
| 7 | | | | | | | | | |
| 8 | | | | | | | | | |
| 9 | | | | | | | | | |

If openOfficeOrg or LibreOffice is installed, you can export to an OpenOfficeCalc or LibreOfficeCalc table.

## Importing the list of employees

Data can be imported both from export files and databases created in **Guard Commander**. **GuardLight** independently searches for data files for existing controllers. It is also possible to specify the location of these files manually.

When importing data from an Excel file, be aware that the Software looks for a certain data formatting in tables: The first row must contain the name of the fields and the first column must have no blank space. The first column - "Department" - must be filled in, otherwise the data will not be imported. Next, in the import form, you need to choose from which fields and what information should be taken. Click the **IMPORT** button. Some fields may be left blank (just not in the first column). If when importing cards, the same cards are found in the database, the **Additional information** field will indicate who has such a card.

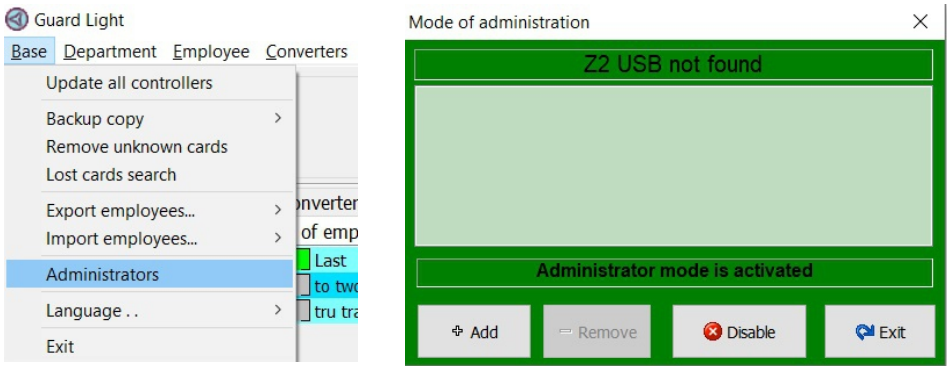


## Administrators

When you run the Software, if no administrator cards are set, it will run in the administrator mode. If at least one card is set, then in order to gain access to data changing, you need to activate the administrator mode by bringing the administrator card to the desktop reader with the administration mode menu open.

To prevent unauthorised changes to the database in case of shared access to the computer, it is possible to limit the rights by creating the administrator card. The background colour of the menu indicates the current state: green – administrator mode is active, red – access to changing is blocked. In this case, it is necessary to use a desktop reader **Z-2 USB**.

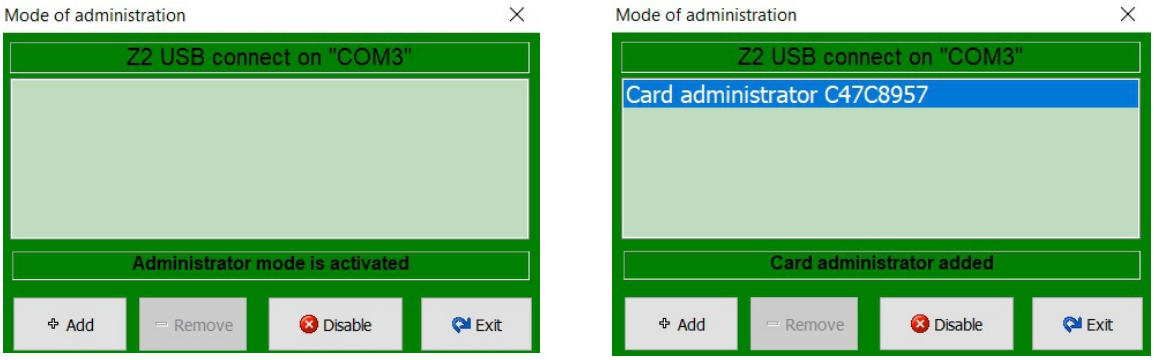
The administrator mode control menu can be opened through the main menu item **Database->Administrators.**




If the desktop reader is not detected, the Software will display the message "Z2 USB not detected".

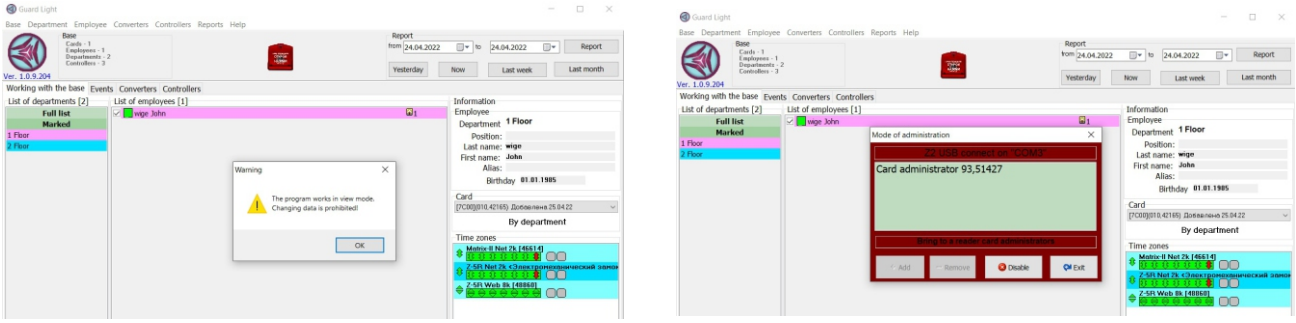
The first line of the "Administration Mode" menu displays information about the connected reader. Next, there is a list of administrator cards. Below it is the status bar and finally, the control buttons. "Add" and "Delete" respectively allow you to add and delete administrator cards. The "deny" button blocks the administrator mode. The "Exit" button closes the administration mode menu.

To add an administrator card, click on the "Add" button. The Software will offer you to "Bring a new card close to the reader."



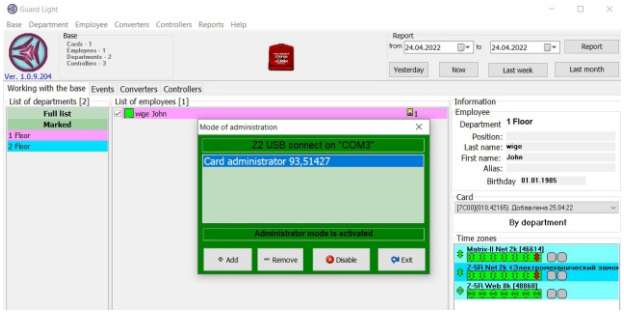

After being presented to the desktop reader, the card will appear in the administration mode menu and "Administrator card added" will be displayed in the status bar.

After restarting the Software and when you try to edit the database, the Software will display the message "The Software is running in the browse mode. Editing is not allowed."

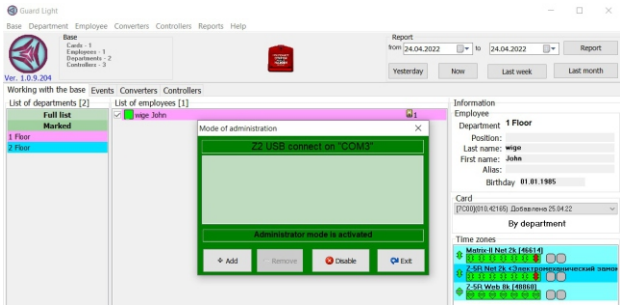


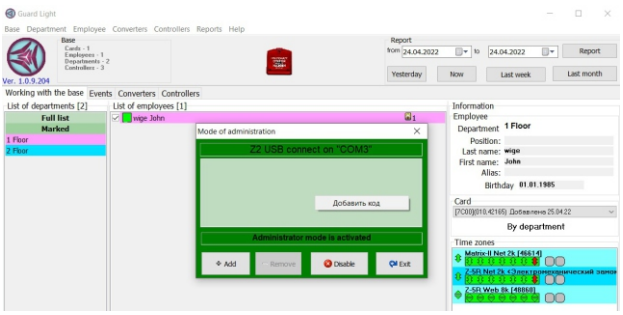
You need to open the main menu item **Database->Administrators**. The "Administration Mode" menu will appear in red and the status bar will contain the message "Bring up the administrator card."

Bring up the previously added administrator card. In the status bar, the message "Administrator mode is activated" will appear and the window colour will change to green.

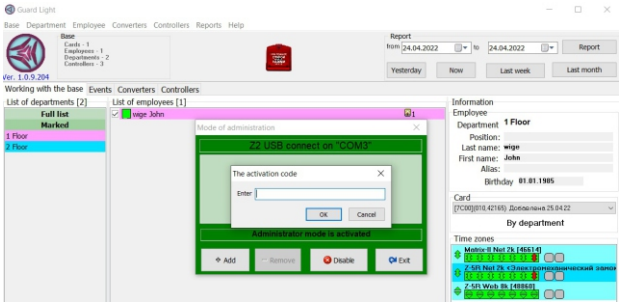


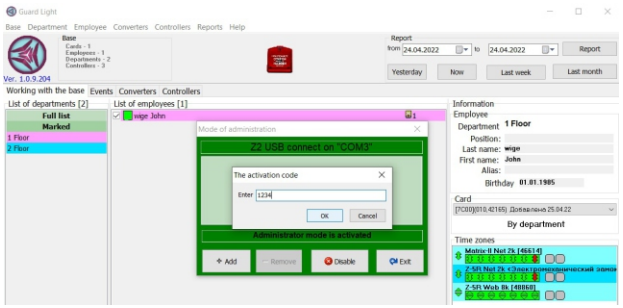

If necessary, you can enter a code instead of an administrator card. To enter the code, you need to open the main menu item **Database->Administrators** and click on the "Add" button in the "Administration Mode" menu. The Software will offer you to "Bring a new card close to the reader."



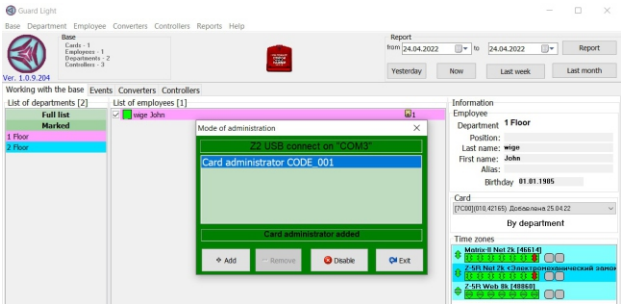




Next, right-click in the administrator card list menu. Left-click on the "Add code" message that appears.
In the "Activation code" menu, enter the necessary code and click the "OK" button.

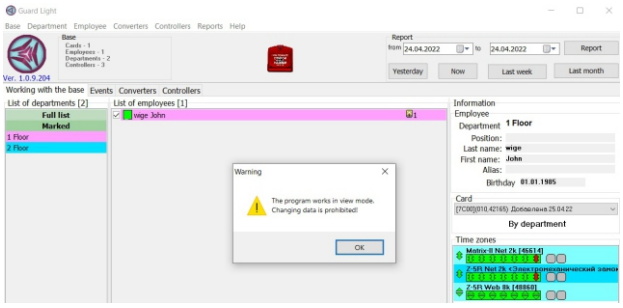


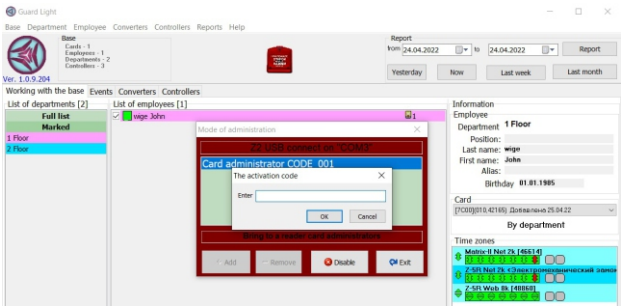




The card (code) will appear in the administration mode menu "Administrator Card CODE_001" and "Administrator card added" will be displayed in the status bar.

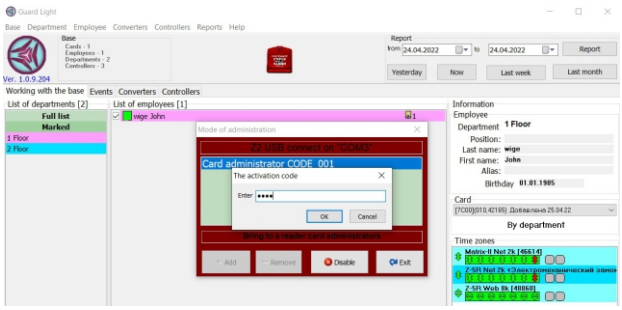


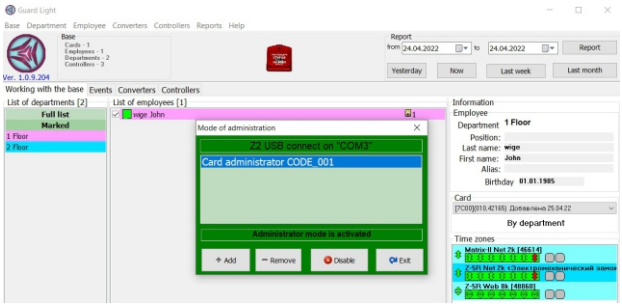

After restarting the Software and when you try to edit the database, the Software will display the message "The Software is running in the browse mode. Editing is not allowed."





You need to open the main menu item **Database->Administrators**. The "Administration Mode" menu will appear in red and the status bar will contain the message "Bring up the administrator card."





Next, double-left-click the administrator card in the administrator card list menu. In the "Activation code" menu that appears, input the previously entered code and click on the "OK" button.
In the status bar, the message "Administrator mode is activated" will appear and the window colour will change to green.
Administrator card codes are stored separately, so the administrator card can be either a special card stored separately or one of the cards for passage and passing via this card does not affect the administrator mode in any way.

# ACCESS MODES

## *Reasons for introducing Access Modes*

The expansion of ACS implementation has led to increased requirements for flexibility in access control. For example, different access control requirements are issued at different times of the day. So when considering the work schedule of an office or a store, you can highlight several periods. The first period is morning: Sellers or managers come to work and the passage should be blocked for outsiders. Business hours: Buyers/Customers come and they should freely get into the room. Evening: Similar to the morning - employees gather and go home and visitors have nothing to do in the office but they can go out using a button. Night: Only the guards can have access, which is denied to everyone else. Further variations of the following nature are possible: automatic switching of modes or manual using a card. Employees can be allowed to block the door if they are alone in the office but have to urgently go out. Access modes have been developed to meet all these needs. To activate the modes, you need to update the firmware in the controller to one of the firmware **XXX_vA.B_blk.rom** included in the distribution package. The update is available for the **Z-5R Net**, **Z-5R Net 8000** and **Matrix II Net controllers**.

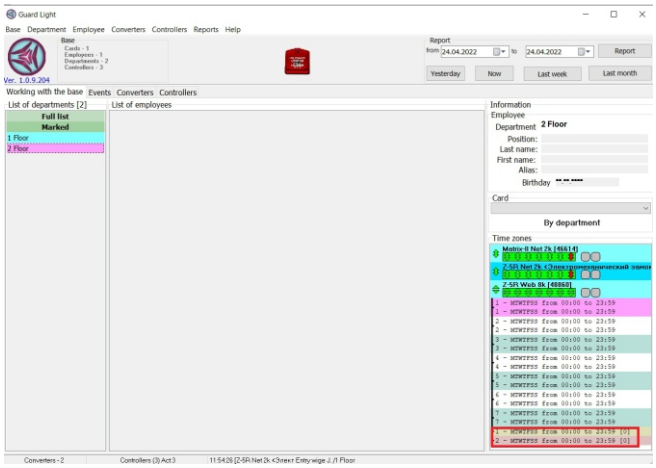
## *Overview of Access Modes*

In total, two access modes are essentially added: **"blocked"** and **"open" (free)**. The **"blocked"** mode is not a completely new mode, as it already existed in the standalone **Z-5R** and **Matrix II K** controllers. It is also available in the network controllers **Z-5R Net**, **Z-5R Net 8000** and **Matrix II Net**. The essence of the "**blocked**" mode is a ban on passing via the so-called "***basic***" cards. Only passage using "***blocking***" cards is allowed, which is also used to switch into this mode. The "**open**" mode involves a long-term unlocking of the lock to ensure unimpeded passage. It can be turned on using the same "***blocking***" card. To ensure a safe transition between modes in terms of access, a "**waiting**" mode has been added, in which the passage is blocked, but the first correct card that has the right of passage turns on the "**open**" mode. For easy reference to the operation, the standard access mode is called a "**normal**" mode.

## *Switching Access Modes*

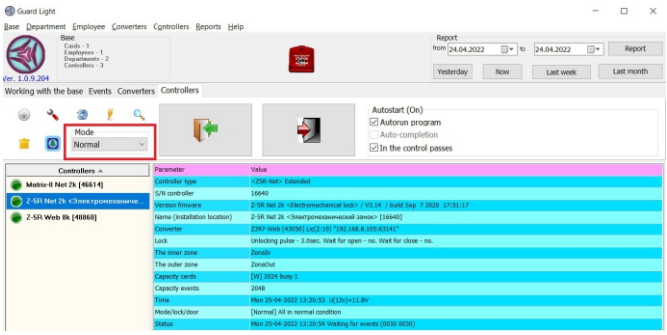
Switching modes is possible in several ways:

- **By the time zone**. The controller has two additional time zones that allow you to set the time with the current access mode in which the controller should be for the duration of the active time zone.




This method of activating the access mode has the highest priority.

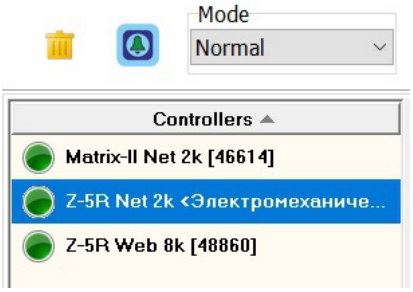
- **Using a command over the network**. Using "Guard Light", the operator can remotely switch access modes.

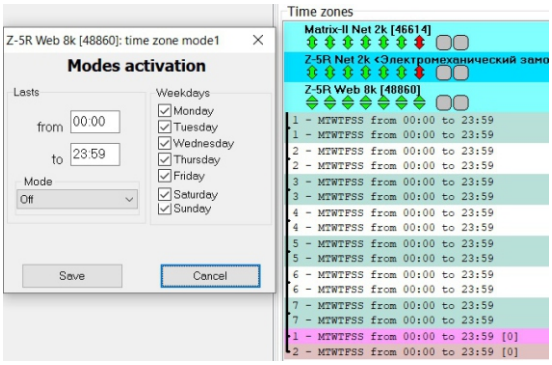


**- Using a "blocking" card.** To switch the controller from the "Normal" to "Blocked" mode, close the door and hold the card on the reader for more than 3 seconds. A similar operation with the door open leads to switching from the "Normal" to "Free Passage" mode. The controller can be returned to the "Normal" mode by holding the card at any position of the door. With the access mode "Free Passage" active enabled by the access time zone, switching the card is possible only to the "Waiting" mode. You should remember that due to the fact that the mode can be switched by holding the "blocking" card, it opens the passage upon removing it from the reader, unlike a regular card that opens the passage when brought to the reader. It should also be noted that switching by holding the card is not available when connecting readers via the Wiegand protocol. In this case, you should use "functional" cards.
**- Using a "Functional" card**. Switching is completely the same as with a "blocking" card, only without the need to hold it. It will not be possible to use a functional card for the passage, since its reading will cause a switching of modes but the passage will not open.

## *"Normal" access mode*

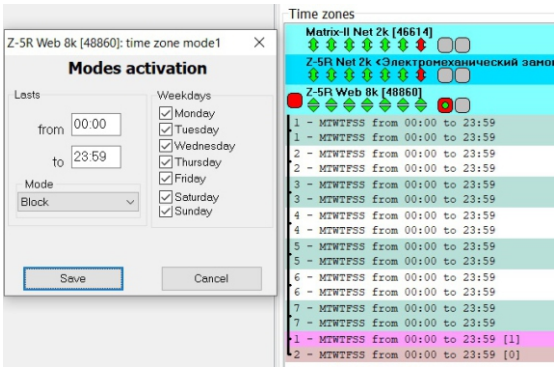
In the "Inactive" or "Normal" mode, the controllers operate in the standard mode. Access is carried out by cards according to the established time zones and access rules.

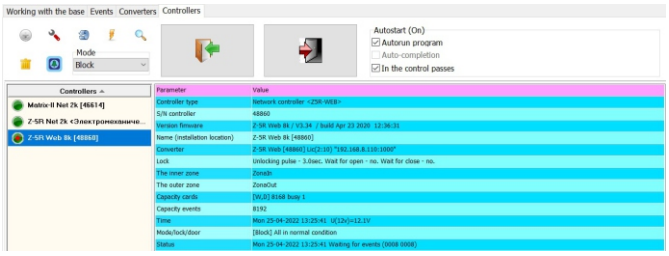



## *"Blocked" access mode*

As mentioned earlier, in this mode, access is possible only for "blocking" cards. You can enable the "Blocking" mode in the "Mode" menu and the "Blocked" mode is enabled by the mode activation time zone.



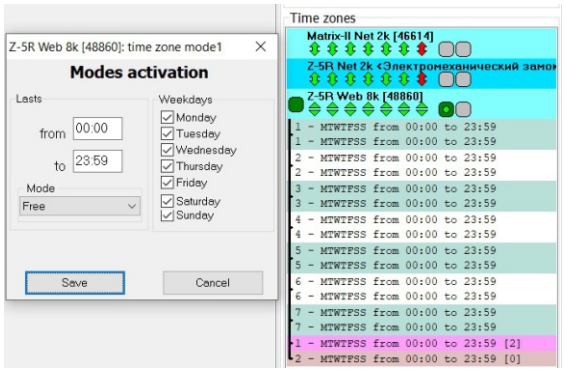



When activating the mode using the time zone, it is impossible to turn it off either with a card or a command. Exit using a button is possible.

It is also possible to unlock the passage using the operator's command "Open for entry".
The pass point can be blocked by using the Software to set the lock open state duration to zero. You can remove such a block only by using the Software and re-entering the normal time value.

## *"Open" access mode*

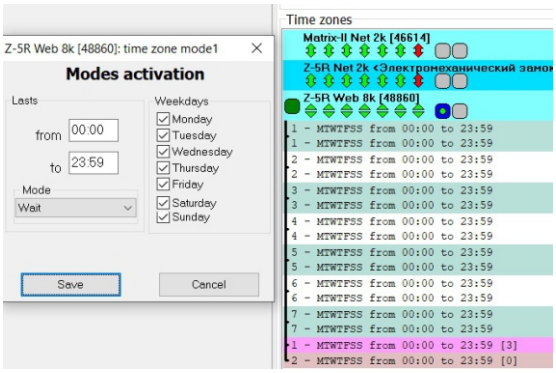
You can enable the "Open" mode in the "Mode" menu and the "Free" mode is enabled by the mode activation time zone. The controller switches into free passage mode and the lock is unlocked.



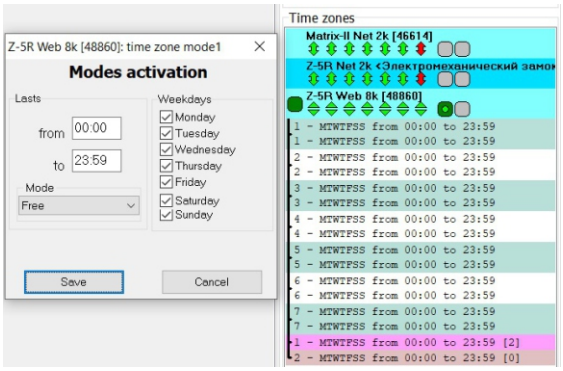
At the same time, despite the unlocked passage, card numbers from readers are accepted and employees can bring cards to the readers in order to ensure a full accounting of working time and movements.

## *"Waiting" access mode*

In a nutshell, the "Waiting" mode is a preparation for the "Open" mode and allows you to ensure that the door is blocked if no one entered the room.



This can be very useful when employees are late or on holidays in the middle of the week. Also, this mode allows you to temporarily block entry during the operation of the access time zone activating the "Open" mode. Moreover, the passage using a button or a command of the operator does not switch the mode back to "Open". It can only be done using a card, including the "basic" card.



At the same time, despite the unlocked passage, card numbers from readers are accepted and employees can bring cards to the readers in order to ensure a full accounting of working time and movements.

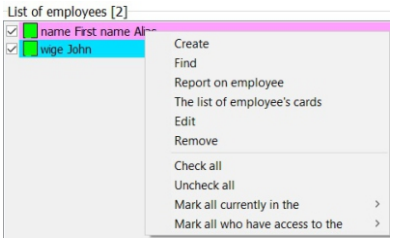
# REPORTS

The reports consist of five parts: **"Timesheet", "Net Time", "Statistics", "Schedule", "Labour Discipline", "Arrivals and Departures"** and **"Traffic"**.

***Depending on whether one or more persons are marked and whether one or more days are set in the period, the information of some parts may vary.***

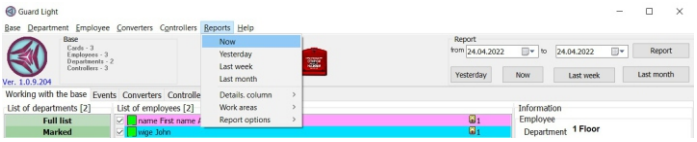
## *Mark employees for the report*

The general report is based on the marked employees, i.e. only those employees whose name box is "checked". To speed up the marking, we recommend you to use the context menu by right-clicking the mouse button. The menu allows you to immediately uncheck or check the entire displayed group.



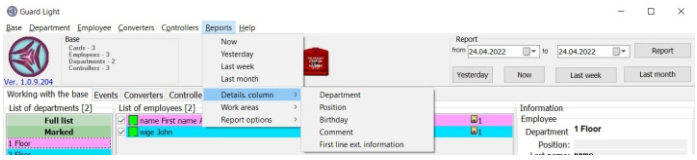

## *Time interval for the report*

To create a report, after marking employees, you need to specify the reporting period - from one day to three months. For the most frequent options, you can select such items as "Yesterday", "Today", "Last Week" or "Last Month" in the **Reports** menu, or select the buttons "Yesterday", "Today", "Last Week" or "Last Month" on the "Report" panel.



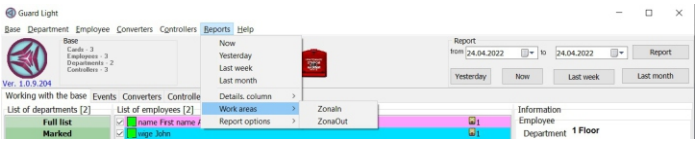
## *Information columns*

You can add additional fields to the timesheet to facilitate further processing and increase information content. The following columns are added from the "Employee Information" menu: "Department", "Position", "Date of birth", "Comment", "First line of additional information".



## *Work zones*

The table "Net Time" shows the duration of the employee's presence at the workplace. A workplace is any area accessed by an employee (the so-called inner zone of the controller) by moving through a pass point inside. If the zone structure is complex, i.e. by exiting, the employee still remains at the workplace (in the work area), then for the correct calculation of the net time when building the timesheet, it is necessary to mark those zones that should be considered work zones in the menu item **Reports/Work Zones**. By default, the controller's inner zone is called "ZonaIn" and the outer zone is called "ZonaOut". For the correct display and accounting of the controller zone, you need to rename it in accordance with the actual name of the room. (For example: Office, Accounting Department, Hallway, etc.)

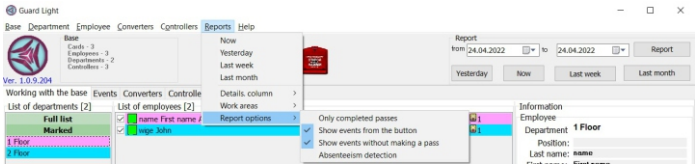


## *Report parameters*

The report parameters represent the events that act as the base for the report to be created and displayed.

- Only completed passages - the report is built on the actually performed passages confirmed by the activation of the door position sensor. In the absence of a door sensor, this report cannot be created since there is no registration of completed passages;

- Show events for the button – events are shown only for the exit button;
- Show events without passing – all events for the passages are shown without the confirmation of the completed passage. Such a report is generated if no door position sensor is installed;
- Unauthorised absence detection – the report shows the absence of an employee from the workplace in excess of the time specified in the work schedule.



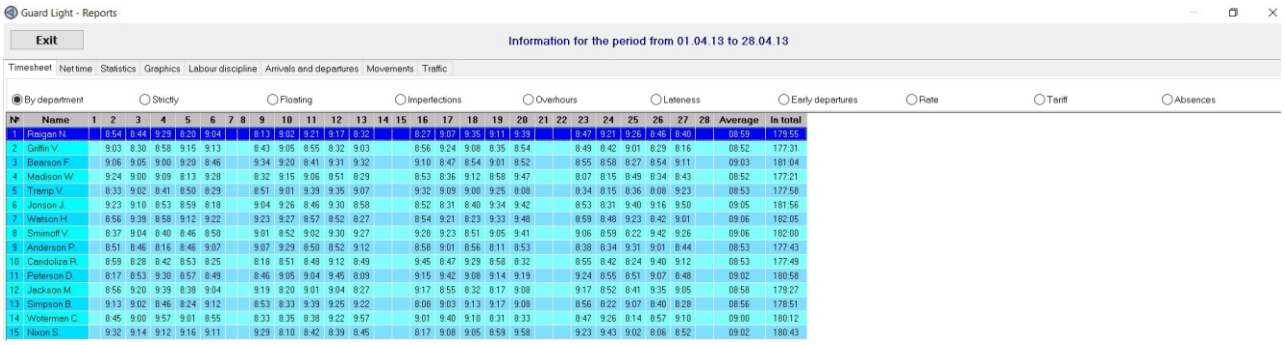
## *Timesheet*

The timesheet shows time spent at work for each of the finished days and the average duration of the working day for the reporting period. The length of the working day is calculated as the difference between the first card reading and the last minus the time for lunch. At the same time, it does not matter at all whether the entry or exit events were recorded and the following principle applies "if the employee passed through the pass point it means that he/she was at work."

For further processing, the timesheet can be exported to MS Excel or LibreOffice Calc (OpenOffice) by right-clicking and causing the context menu to appear. The timesheet has a number of settings for displaying reports: "By department", "Rigorous", "Free", "Underwork", "Overwork", "Late arrivals", "Early arrivals", "Coefficient", "Tariff", "Absences".

### By department

The full timesheet for the time worked is displayed according to the department settings. The number of hours worked each day, the average time spent at the workplace for the specified period and the total time of work for the period are indicated.



Guard Light - Reports

Exit

Information for the period from 01.04.13 to 28.04.13

Timesheet | Net time | Statistics | Graphics | Labour discipline | Arrivals and departures | Movements | Traffic

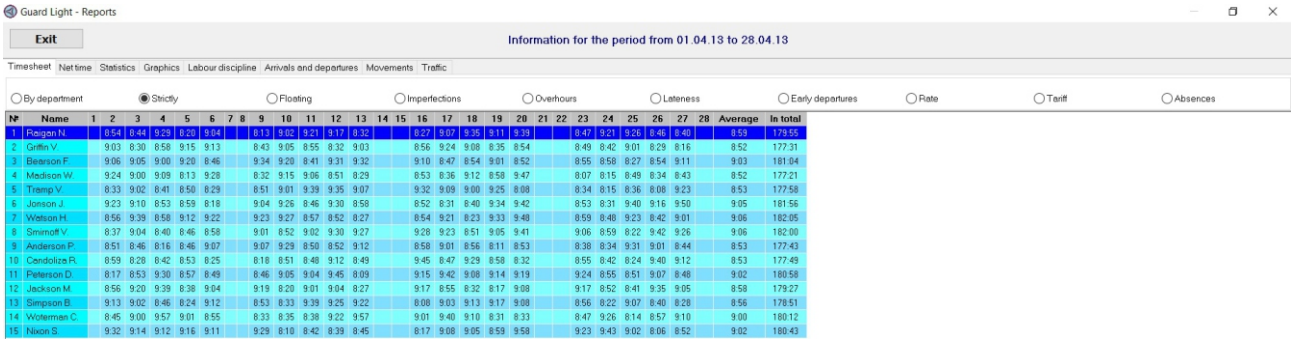
(•) By department ( ) Strictly ( ) Floating ( ) Imperfections ( ) Overhours ( ) Lateness ( ) Early departures ( ) Rate ( ) Tariff ( ) Absences

| № | Name | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | Average | In total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Raigan N. | 8:54 | 8:44 | 9:29 | 8:20 | 9:04 | | | | 8:13 | 9:02 | 9:21 | 9:17 | 8:32 | | | 8:27 | 9:07 | 9:35 | 9:11 | 9:39 | | | 8:47 | 9:21 | 9:26 | 8:46 | 8:40 | | | 8:59 | 179:55 |
| 2 | Griffin V. | 9:03 | 8:30 | 8:58 | 9:15 | 9:13 | | | | 8:43 | 9:05 | 8:55 | 8:32 | 9:03 | | | 8:56 | 9:24 | 9:08 | 8:35 | 8:54 | | | 8:49 | 8:42 | 9:01 | 8:29 | 8:16 | | | 8:52 | 177:31 |
| 3 | Bearson F. | 9:06 | 9:05 | 9:00 | 9:20 | 8:46 | | | | 9:34 | 9:20 | 8:41 | 9:31 | 9:32 | | | 9:10 | 8:47 | 8:54 | 9:01 | 8:52 | | | 8:55 | 8:58 | 8:27 | 8:54 | 9:11 | | | 9:03 | 181:04 |
| 4 | Madison W. | 9:24 | 9:00 | 9:09 | 8:13 | 9:28 | | | | 8:32 | 9:15 | 9:06 | 8:51 | 8:29 | | | 8:53 | 8:36 | 9:12 | 8:58 | 9:47 | | | 8:07 | 8:15 | 8:49 | 8:34 | 8:43 | | | 8:52 | 177:21 |
| 5 | Tramp V. | 8:33 | 9:02 | 8:41 | 8:50 | 8:29 | | | | 8:51 | 9:01 | 9:39 | 9:35 | 9:07 | | | 9:32 | 9:09 | 9:00 | 9:25 | 8:08 | | | 8:34 | 8:15 | 8:36 | 8:08 | 9:23 | | | 8:53 | 177:58 |
| 6 | Jonson J. | 9:23 | 9:10 | 8:53 | 8:59 | 8:18 | | | | 9:04 | 9:26 | 8:46 | 9:30 | 8:58 | | | 8:52 | 8:31 | 8:40 | 9:34 | 9:42 | | | 8:53 | 8:31 | 9:40 | 9:16 | 9:50 | | | 9:05 | 181:56 |
| 7 | Watson H. | 8:56 | 9:39 | 8:58 | 9:12 | 9:22 | | | | 9:23 | 9:27 | 8:57 | 8:52 | 8:27 | | | 8:54 | 9:21 | 8:23 | 9:33 | 9:48 | | | 8:59 | 8:48 | 9:23 | 8:42 | 9:01 | | | 9:06 | 182:05 |
| 8 | Smirnoff V. | 8:37 | 9:04 | 8:40 | 8:46 | 8:58 | | | | 9:01 | 8:52 | 9:02 | 9:30 | 9:27 | | | 9:28 | 9:23 | 8:51 | 9:05 | 9:41 | | | 9:06 | 8:59 | 8:22 | 9:42 | 9:26 | | | 9:06 | 182:00 |
| 9 | Anderson P. | 8:51 | 8:46 | 8:16 | 8:46 | 9:07 | | | | 9:07 | 9:29 | 8:50 | 8:52 | 9:12 | | | 8:58 | 9:01 | 8:56 | 8:11 | 8:53 | | | 8:38 | 8:34 | 9:31 | 9:01 | 8:44 | | | 8:53 | 177:43 |
| 10 | Candoliza R. | 8:59 | 8:28 | 8:42 | 8:53 | 8:25 | | | | 8:18 | 8:51 | 8:48 | 9:12 | 8:49 | | | 9:45 | 8:47 | 9:29 | 8:58 | 8:32 | | | 8:55 | 8:42 | 8:24 | 9:40 | 9:12 | | | 8:53 | 177:49 |
| 11 | Peterson D. | 8:17 | 8:53 | 9:30 | 8:57 | 8:49 | | | | 8:46 | 9:05 | 9:04 | 9:45 | 8:09 | | | 9:15 | 9:42 | 9:08 | 9:14 | 9:19 | | | 9:24 | 8:55 | 8:51 | 9:07 | 8:48 | | | 9:02 | 180:58 |
| 12 | Jackson M. | 8:56 | 9:20 | 9:39 | 8:38 | 9:04 | | | | 9:19 | 8:20 | 9:01 | 9:04 | 8:27 | | | 9:17 | 8:55 | 8:32 | 8:17 | 9:08 | | | 9:17 | 8:52 | 8:41 | 9:35 | 9:05 | | | 8:58 | 179:27 |
| 13 | Simpson B. | 9:13 | 9:02 | 8:46 | 8:24 | 9:12 | | | | 8:53 | 8:33 | 9:39 | 9:25 | 9:22 | | | 8:08 | 9:03 | 9:13 | 9:17 | 9:08 | | | 8:56 | 8:22 | 9:07 | 8:40 | 8:28 | | | 8:56 | 178:51 |
| 14 | Waterman C. | 8:45 | 9:00 | 9:57 | 9:01 | 8:55 | | | | 8:33 | 8:35 | 8:38 | 9:22 | 9:57 | | | 9:01 | 9:40 | 9:10 | 8:31 | 8:33 | | | 8:47 | 9:26 | 8:14 | 8:57 | 9:10 | | | 9:00 | 180:12 |
| 15 | Nixon S. | 9:32 | 9:14 | 9:12 | 9:16 | 9:11 | | | | 9:29 | 8:10 | 8:42 | 8:39 | 8:45 | | | 8:17 | 9:08 | 9:05 | 8:59 | 9:58 | | | 9:23 | 9:43 | 9:02 | 8:06 | 8:52 | | | 9:02 | 180:43 |

For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

### Rigorous

The time before and after the working hours of the department is cut off. The full timesheet for the time worked is displayed according to the department settings but only from the beginning to the end of the department's work schedule. Early arrivals and late departures are not taken into account.



Guard Light - Reports

Exit

Information for the period from 01.04.13 to 28.04.13

Timesheet | Net time | Statistics | Graphics | Labour discipline | Arrivals and departures | Movements | Traffic

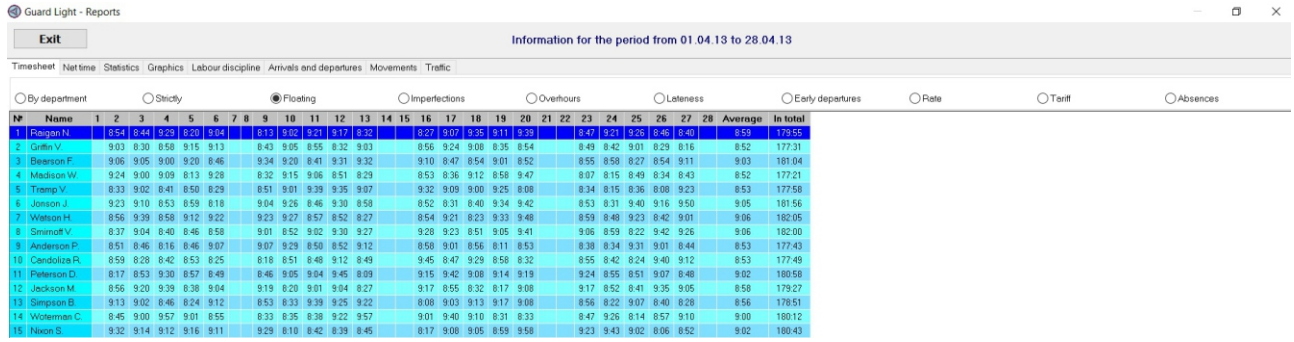
( ) By department (•) Strictly ( ) Floating ( ) Imperfections ( ) Overhours ( ) Lateness ( ) Early departures ( ) Rate ( ) Tariff ( ) Absences

| № | Name | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | Average | In total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Raigan N. | 8:54 | 8:44 | 9:29 | 8:20 | 9:04 | | | | 8:13 | 9:02 | 9:21 | 9:17 | 8:32 | | | 8:27 | 9:07 | 9:35 | 9:11 | 9:39 | | | 8:47 | 9:21 | 9:26 | 8:46 | 8:40 | | | 8:59 | 179:55 |
| 2 | Griffin V. | 9:03 | 8:30 | 8:58 | 9:15 | 9:13 | | | | 8:43 | 9:05 | 8:55 | 8:32 | 9:03 | | | 8:56 | 9:24 | 9:08 | 8:35 | 8:54 | | | 8:49 | 8:42 | 9:01 | 8:29 | 8:16 | | | 8:52 | 177:31 |
| 3 | Bearson F. | 9:06 | 9:05 | 9:00 | 9:20 | 8:46 | | | | 9:34 | 9:20 | 8:41 | 9:31 | 9:32 | | | 9:10 | 8:47 | 8:54 | 9:01 | 8:52 | | | 8:55 | 8:58 | 8:27 | 8:54 | 9:11 | | | 9:03 | 181:04 |
| 4 | Madison W. | 9:24 | 9:00 | 9:09 | 8:13 | 9:28 | | | | 8:32 | 9:15 | 9:06 | 8:51 | 8:29 | | | 8:53 | 8:36 | 9:12 | 8:58 | 9:47 | | | 8:07 | 8:15 | 8:49 | 8:34 | 8:43 | | | 8:52 | 177:21 |
| 5 | Tramp V. | 8:33 | 9:02 | 8:41 | 8:50 | 8:29 | | | | 8:51 | 9:01 | 9:39 | 9:35 | 9:07 | | | 9:32 | 9:09 | 9:00 | 9:25 | 8:08 | | | 8:34 | 8:15 | 8:36 | 8:08 | 9:23 | | | 8:53 | 177:58 |
| 6 | Jonson J. | 9:23 | 9:10 | 8:53 | 8:59 | 8:18 | | | | 9:04 | 9:26 | 8:46 | 9:30 | 8:58 | | | 8:52 | 8:31 | 8:40 | 9:34 | 9:42 | | | 8:53 | 8:31 | 9:40 | 9:16 | 9:50 | | | 9:05 | 181:56 |
| 7 | Watson H. | 8:56 | 9:39 | 8:58 | 9:12 | 9:22 | | | | 9:23 | 9:27 | 8:57 | 8:52 | 8:27 | | | 8:54 | 9:21 | 8:23 | 9:33 | 9:48 | | | 8:59 | 8:48 | 9:23 | 8:42 | 9:01 | | | 9:06 | 182:05 |
| 8 | Smirnoff V. | 8:37 | 9:04 | 8:40 | 8:46 | 8:58 | | | | 9:01 | 8:52 | 9:02 | 9:30 | 9:27 | | | 9:28 | 9:23 | 8:51 | 9:05 | 9:41 | | | 9:06 | 8:59 | 8:22 | 9:42 | 9:26 | | | 9:06 | 182:00 |
| 9 | Anderson P. | 8:51 | 8:46 | 8:16 | 8:46 | 9:07 | | | | 9:07 | 9:29 | 8:50 | 8:52 | 9:12 | | | 8:58 | 9:01 | 8:56 | 8:11 | 8:53 | | | 8:38 | 8:34 | 9:31 | 9:01 | 8:44 | | | 8:53 | 177:43 |
| 10 | Candoliza R. | 8:59 | 8:28 | 8:42 | 8:53 | 8:25 | | | | 8:18 | 8:51 | 8:48 | 9:12 | 8:49 | | | 9:45 | 8:47 | 9:29 | 8:58 | 8:32 | | | 8:55 | 8:42 | 8:24 | 9:40 | 9:12 | | | 8:53 | 177:49 |
| 11 | Peterson D. | 8:17 | 8:53 | 9:30 | 8:57 | 8:49 | | | | 8:46 | 9:05 | 9:04 | 9:45 | 8:09 | | | 9:15 | 9:42 | 9:08 | 9:14 | 9:19 | | | 9:24 | 8:55 | 8:51 | 9:07 | 8:48 | | | 9:02 | 180:58 |
| 12 | Jackson M. | 8:56 | 9:20 | 9:39 | 8:38 | 9:04 | | | | 9:19 | 8:20 | 9:01 | 9:04 | 8:27 | | | 9:17 | 8:55 | 8:32 | 8:17 | 9:08 | | | 9:17 | 8:52 | 8:41 | 9:35 | 9:05 | | | 8:58 | 179:27 |
| 13 | Simpson B. | 9:13 | 9:02 | 8:46 | 8:24 | 9:12 | | | | 8:53 | 8:33 | 9:39 | 9:25 | 9:22 | | | 8:08 | 9:03 | 9:13 | 9:17 | 9:08 | | | 8:56 | 8:22 | 9:07 | 8:40 | 8:28 | | | 8:56 | 178:51 |
| 14 | Waterman C. | 8:45 | 9:00 | 9:57 | 9:01 | 8:55 | | | | 8:33 | 8:35 | 8:38 | 9:22 | 9:57 | | | 9:01 | 9:40 | 9:10 | 8:31 | 8:33 | | | 8:47 | 9:26 | 8:14 | 8:57 | 9:10 | | | 9:00 | 180:12 |
| 15 | Nixon S. | 9:32 | 9:14 | 9:12 | 9:16 | 9:11 | | | | 9:29 | 8:10 | 8:42 | 8:39 | 8:45 | | | 8:17 | 9:08 | 9:05 | 8:59 | 9:58 | | | 9:23 | 9:43 | 9:02 | 8:06 | 8:52 | | | 9:02 | 180:43 |

For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## Free

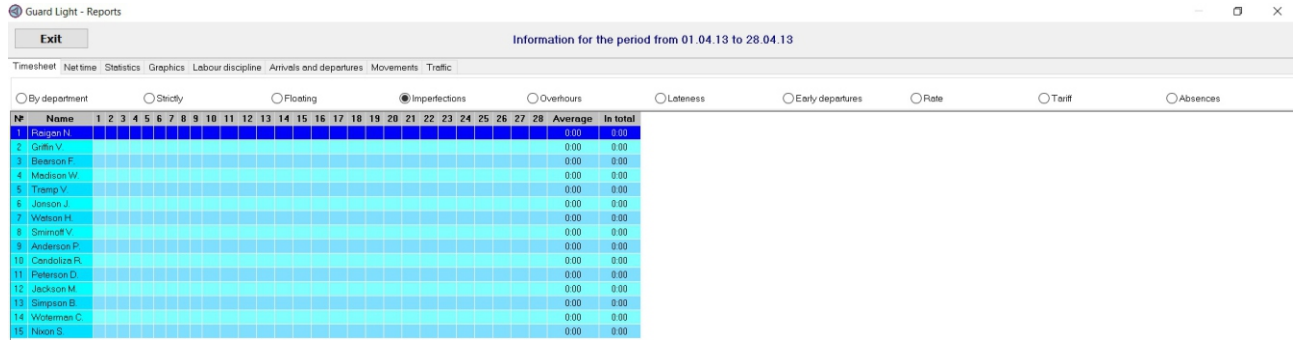
The net time spent by the employee at the workplace is displayed. All departures from the workplace are not taken into account.




For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## Underwork

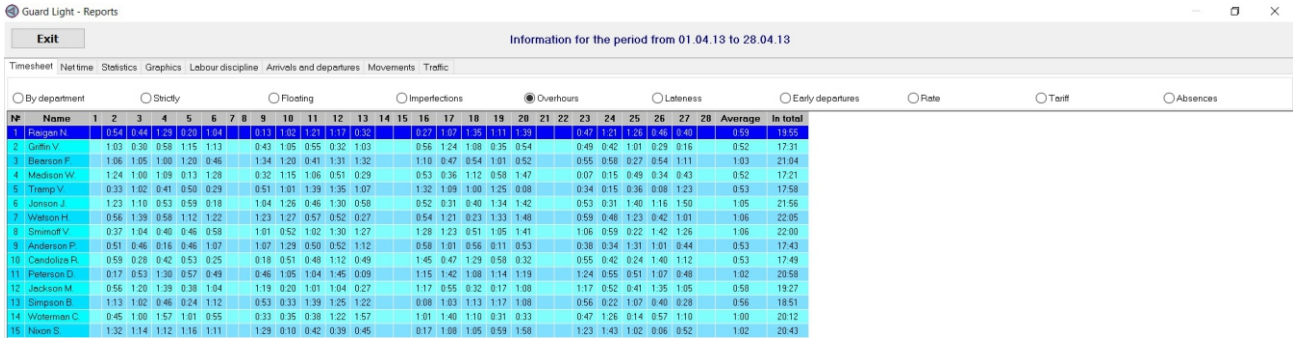
The time underworked by the employee according to the working schedule of the department is shown.




For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## Overwork

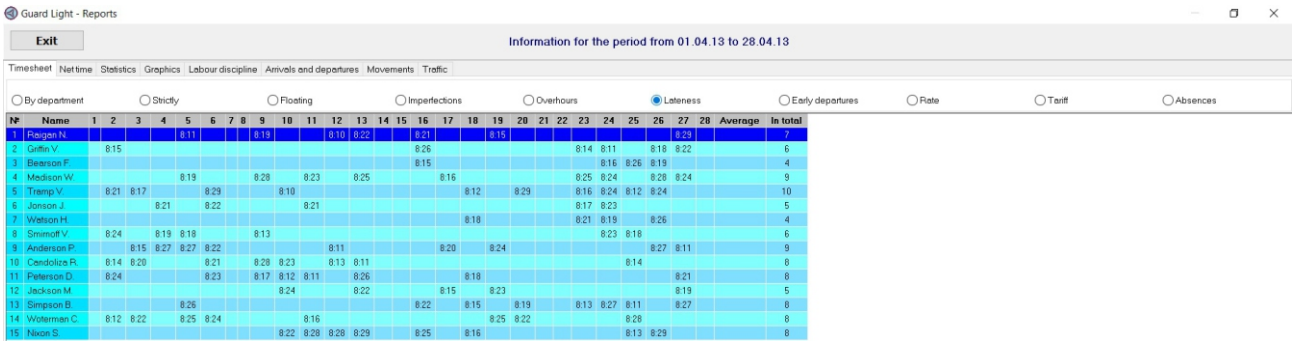
The time overworked by the employee in excess of the established time according to the working schedule of the department is shown.




For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## Late arrivals

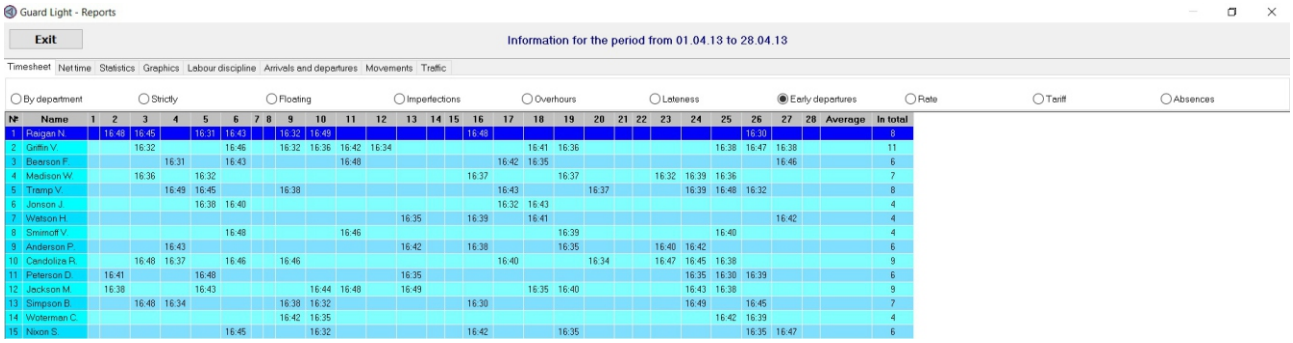
The time of late arrivals to work for each day during the accounting period is indicated.




For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## Early arrivals

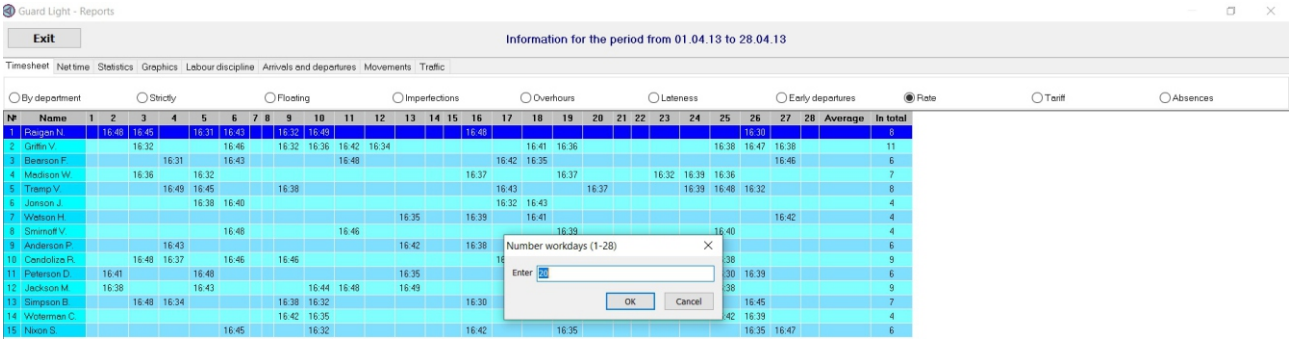
Early arrivals of the employee to the workplace before the start of the department work schedule are indicated.



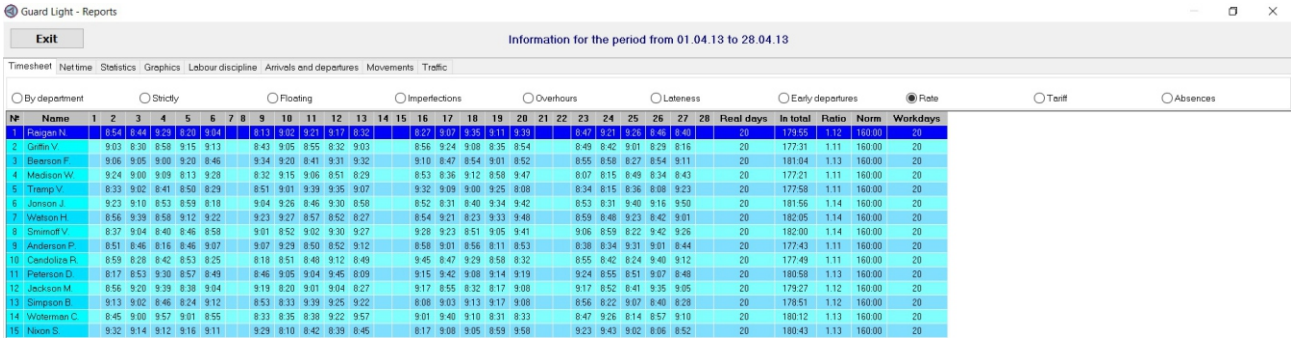

For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## Coefficient

Shows how many days should the employee have worked according to the standard of working time. The coefficient is entered in the "Number of working days (1-28)" menu.



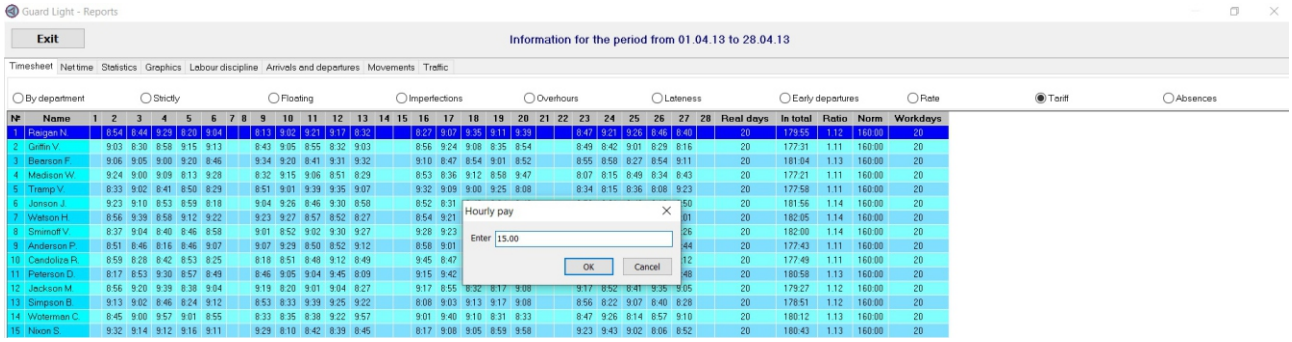

After clicking on the "OK" button, a timesheet is displayed indicating the time worked for each day, number of days actually finished, coefficient, the standard of working time and number of working days according to the standard.



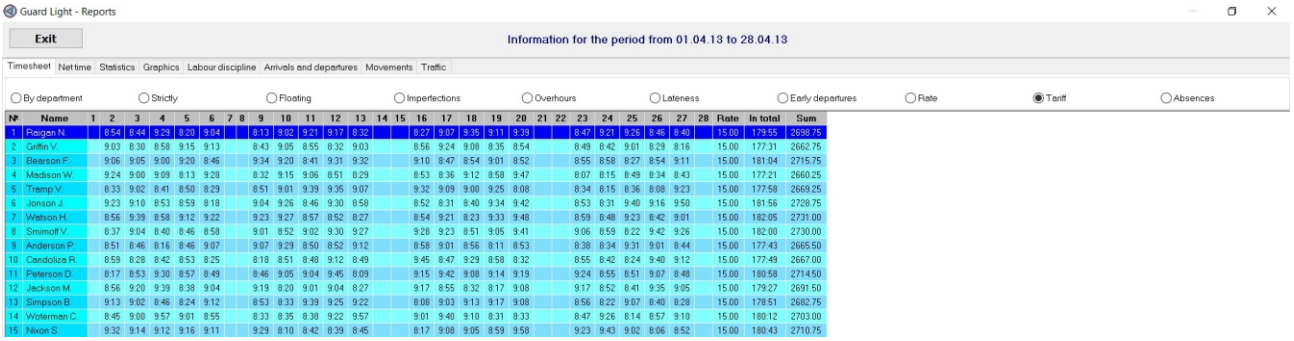
If the coefficient is less than one then the employee underworks and if it is greater than one then the employee overworks. The coefficient is used to reward or punish an employee.
For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## Tariff

This report shows the rate per work hour.

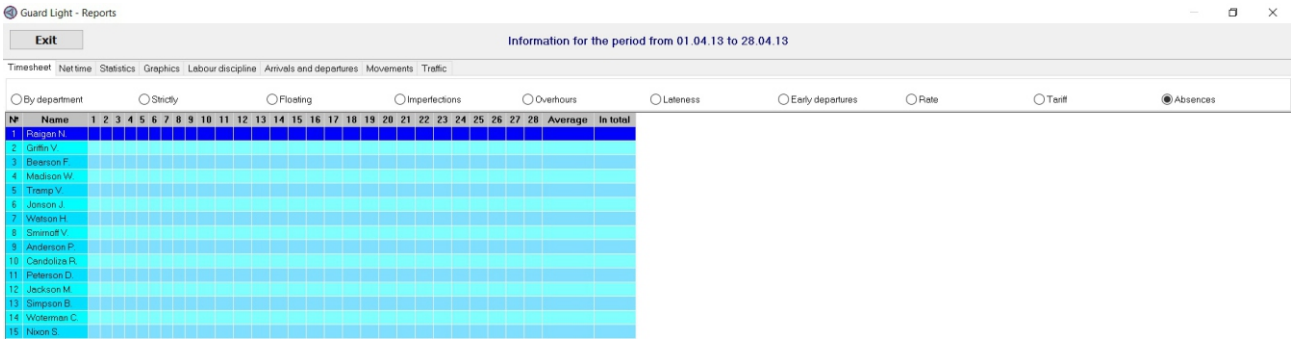



After entering the payment tariff in the "Amount of payment per hour" menu, click on the "OK" button. In addition to the timesheet, the columns "Tariff" and "Amount" will be shown.
For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.




## Absences

This report shows the time of absence of employees from work.




For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## *Net time*

This table shows the net time spent at the workplace, i.e. the time intervals between the entry and exit events are summed up and the remaining intervals are ignored. For correct calculation, the controller must be equipped with two readers - one for entry and the other for exit. Lunch is not deducted.

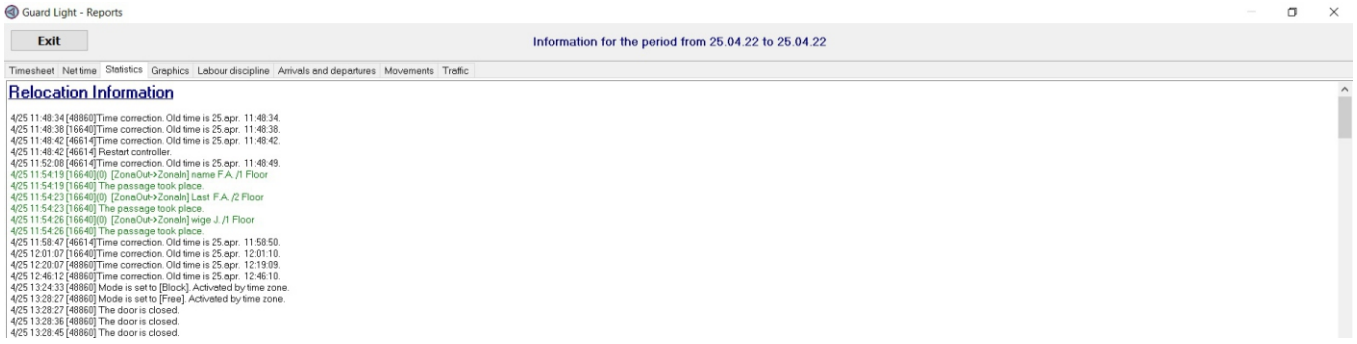
| № | Name | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | In total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Reigan N. | 8:54 | 8:44 | 9:29 | 8:26 | 9:04 | | | | 8:13 | 9:02 | 9:21 | 9:17 | 8:32 | | | 8:27 | 9:07 | 9:35 | 9:11 | 9:39 | | | 8:47 | 9:21 | 9:26 | 8:46 | 8:40 | | 179:55 |
| 2 | Griffin V. | 9:03 | 8:38 | 8:58 | 9:15 | 9:13 | | | | 8:43 | 9:05 | 8:55 | 8:32 | 9:03 | | | 8:56 | 9:24 | 9:08 | 8:35 | 8:54 | | | 8:49 | 8:42 | 9:01 | 8:29 | 8:16 | | 177:31 |
| 3 | Bearson F. | 9:06 | 9:05 | 9:00 | 9:20 | 8:46 | | | | 9:34 | 9:20 | 8:41 | 9:31 | 9:32 | | | 9:10 | 8:47 | 8:54 | 9:01 | 8:52 | | | 8:55 | 8:58 | 8:27 | 8:54 | 9:11 | | 181:04 |
| 4 | Madison W. | 9:24 | 9:00 | 9:09 | 8:13 | 9:28 | | | | 8:32 | 9:15 | 9:06 | 8:51 | 8:29 | | | 8:53 | 8:36 | 9:12 | 8:58 | 9:47 | | | 8:07 | 8:15 | 8:49 | 8:34 | 8:43 | | 177:21 |
| 5 | Tramp V. | 8:33 | 9:02 | 8:41 | 8:58 | 8:29 | | | | 8:51 | 9:01 | 9:39 | 9:35 | 9:07 | | | 9:32 | 9:09 | 9:00 | 9:25 | 8:08 | | | 8:34 | 8:15 | 8:36 | 9:08 | 9:23 | | 177:58 |
| 6 | Jonson J. | 9:23 | 9:10 | 8:53 | 8:59 | 8:18 | | | | 9:04 | 9:26 | 8:46 | 9:30 | 8:58 | | | 8:52 | 8:31 | 8:40 | 9:34 | 9:42 | | | 8:53 | 8:31 | 9:40 | 9:16 | 9:50 | | 181:56 |
| 7 | Watson H. | 8:56 | 9:39 | 8:58 | 9:12 | 9:22 | | | | 9:23 | 9:27 | 8:57 | 8:52 | 8:27 | | | 8:54 | 9:21 | 8:23 | 9:33 | 9:48 | | | 8:59 | 8:48 | 9:23 | 8:42 | 9:01 | | 182:05 |
| 8 | Smirnoff V. | 8:37 | 9:04 | 8:40 | 8:46 | 8:58 | | | | 9:01 | 8:52 | 9:02 | 9:30 | 9:27 | | | 9:28 | 9:23 | 8:51 | 9:05 | 9:41 | | | 9:06 | 8:59 | 8:22 | 9:42 | 9:26 | | 182:00 |
| 9 | Anderson P. | 8:51 | 8:46 | 8:16 | 8:46 | 9:07 | | | | 9:07 | 9:29 | 8:50 | 8:52 | 9:12 | | | 8:58 | 9:01 | 8:56 | 8:11 | 8:53 | | | 8:38 | 8:34 | 9:31 | 9:01 | 8:44 | | 177:43 |
| 10 | Candoliza R. | 8:59 | 8:28 | 8:42 | 8:53 | 8:25 | | | | 8:18 | 8:51 | 8:48 | 9:12 | 8:49 | | | 9:45 | 8:47 | 9:29 | 8:58 | 8:32 | | | 8:55 | 8:42 | 8:24 | 9:40 | 9:12 | | 177:49 |
| 11 | Peterson D. | 8:17 | 8:53 | 9:30 | 8:57 | 8:49 | | | | 8:46 | 9:05 | 9:04 | 9:45 | 8:09 | | | 9:15 | 9:42 | 9:08 | 9:14 | 9:19 | | | 9:24 | 8:55 | 8:51 | 9:07 | 8:48 | | 180:58 |
| 12 | Jackson M. | 8:56 | 9:20 | 9:39 | 8:38 | 9:04 | | | | 9:19 | 8:20 | 9:01 | 9:04 | 8:27 | | | 9:17 | 8:55 | 8:32 | 8:17 | 9:08 | | | 9:17 | 8:52 | 8:41 | 9:35 | 9:05 | | 179:27 |
| 13 | Simpson B. | 9:13 | 9:02 | 8:46 | 8:24 | 9:12 | | | | 8:53 | 8:33 | 9:39 | 9:25 | 9:22 | | | 8:08 | 9:03 | 9:13 | 9:17 | 9:08 | | | 8:56 | 8:22 | 9:07 | 8:40 | 8:28 | | 178:51 |
| 14 | Waterman C. | 8:45 | 9:00 | 9:57 | 9:01 | 8:55 | | | | 8:33 | 8:35 | 8:38 | 9:22 | 9:57 | | | 9:01 | 9:40 | 9:10 | 8:31 | 8:33 | | | 8:47 | 9:26 | 8:14 | 8:57 | 9:10 | | 180:12 |
| 15 | Nixon S. | 9:32 | 9:14 | 9:12 | 9:16 | 9:11 | | | | 9:29 | 8:10 | 8:42 | 8:39 | 8:45 | | | 8:17 | 9:08 | 9:05 | 8:59 | 9:58 | | | 9:23 | 9:43 | 9:02 | 8:06 | 8:52 | | 180:43 |

For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

## *Statistics*

The **statistics** provide statistical information about each employee for a specified period of time.

If you create a report **for one day**, the menu displays information about all events registered by the system for that day.




For further work, the information in the menu can be highlighted with the mouse and copied to any text editor using standard Windows tools.

## *Diagrams*

The **diagram** graphically displays a range of arrival and departure times for all employees if **multiple employees** and several days are selected.
In the case of processing **a single day**, all movements of employees are displayed while the colour shows the presence of the employee in a certain zone. The colour is adjusted when you configure the controller and set indoor and outdoor zones.
In the case of processing **a single employee**, his/her movements for each day are displayed separately.

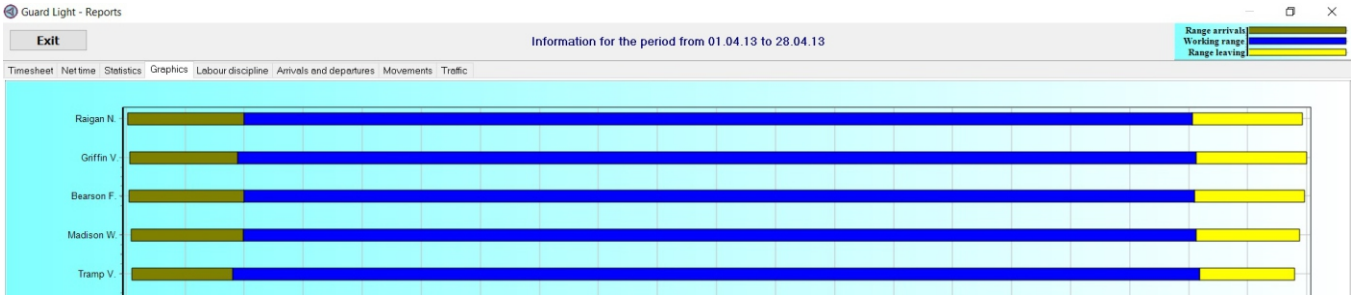
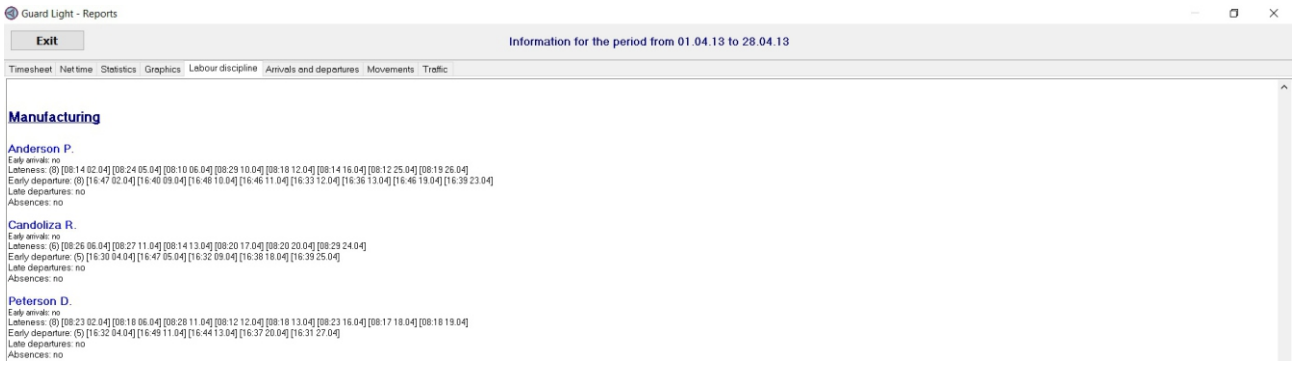



**Image zooming** is possible. To do this, point to the upper-left corner of the required area, hold the **left** button and move the mouse pointer to the lower-right corner. After releasing the mouse button, the selected area will be stretched over the entire diagram screen. By moving the mouse pointer while holding the **right** button, you can move the image in any direction. To undo zoom, you need to make a "**reverse**" highlighting, i.e. you need to move the mouse pointer from the lower right corner to the upper left corner while holding the **left** button. Regardless of the size of this selection, the image will take the original scale.
Exporting a diagram image is possible only to a graphic file of the BMP format and can be carried out using the context menu.

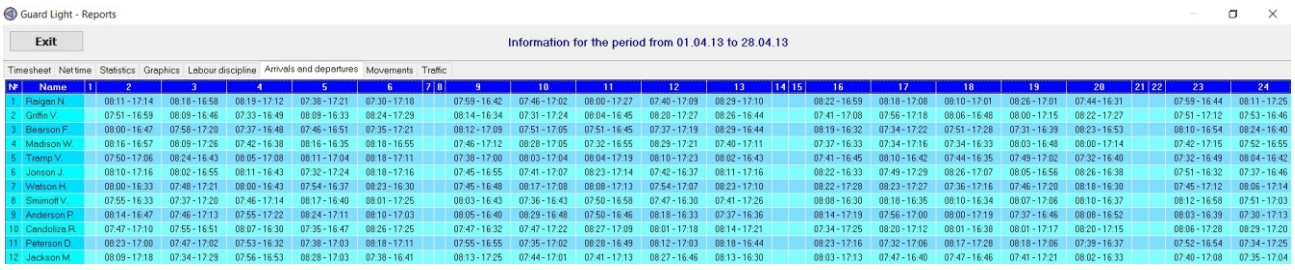
## *Labour discipline*

The menu displays the facts of violations of the work schedule specified when configuring the department parameters. For further work, the information in the menu can be highlighted with the mouse and copied to any text editor using standard Windows tools.

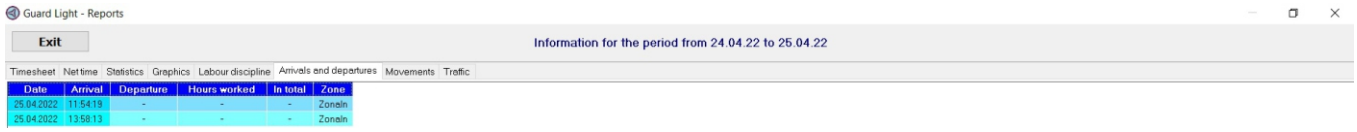



## *Arrivals and departures*

The table shows the ranges of the first and last detection of the employee's card for each day. The table format **depends on whether the number** of employees displayed is one or more.



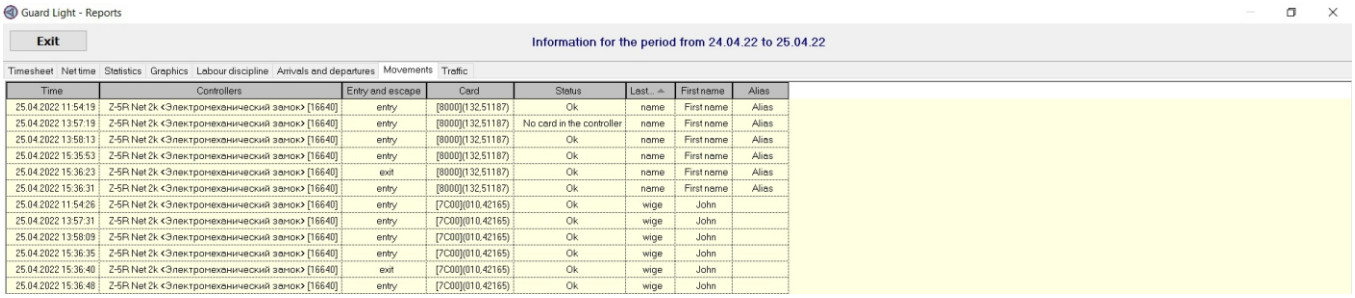

When generating a report for one employee per day or month, all arrivals and departures during each day are indicated. The number of hours worked per day and total working hours are also calculated.




For further processing, the table can be exported to MS Excel or OpenOffice by right-clicking and causing the context menu to appear.

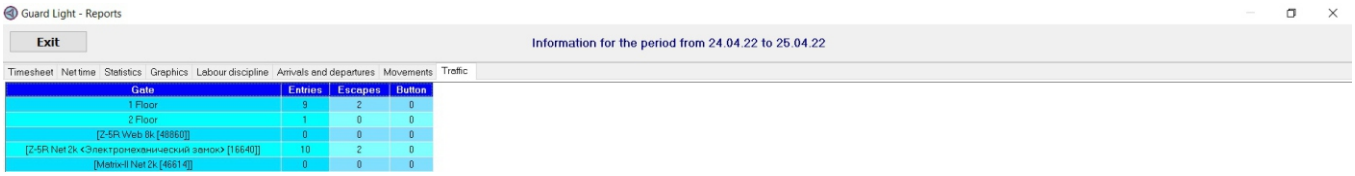
### *Movements*

All movements of the department and employees for the card and events for the exit button during the specified period are indicated.




### *Traffic*

This table allows you to estimate the number of passes (entries and exits) through each access point for the card and exit button.




## AUTOMATIC EVENT EXPORTING

GuardLight v.1.0.7.156 adds the option of periodical event exporting to a text file.
The archive with the Software feature a brief manual. To export events from the Software (where the Base and Logs folders are located), you need to place the GuardLight.upl file in the working folder, which should contain the controller numbers and the export period. A sample file is attached to the archive.
[PARAM]
Controllers=40000,40283
Duration=5
FileSob=C:\aaa.sob
LastSave=30.10.2017 12:36:15
Controllers – controller numbers separated by commas without spaces.
Duration – the export period in minutes.
FileSob=C:\aaa.sob – the GuardLight.sob file in CSV format will be created or further populated in the same working folder. You can also specify a random file (FileSob=C:aaa.sob).
LastSave – defines the time used as a starting point for the event export. Subsequently, the time is updated automatically.