HOTSEC

Integrated security and access system

User manual for HotSec management software

v.1.0

Table of contents

General

Management software description

What is HotSec?

Management software for security and automation systems.

What does HotSec do?

Monitors and manages object' or objects' video, surveillance, access, fire alarm and automatic systems (hereafter systems) on desk or on computer screen or on display. The number of positions is not limited. Furthermore, it's possible to create innumerable teleworking positions, which presumes only Internet connection anywhere in the world.

What's HotSec for?

Considerably reduces the expenses made to manned surveillance and to tehcnical staff.
Reduces the risks linked to human factor.
Centralises system management or in other words, receives information simultaneously from different systems, which enables to create more precise, operative and effective reaction to the events taking place.
HotSec creates links between different system detectors and devices, which enables to create a considerably fuller picture from the events taken or taking place.
While taking required reports from one system, we can simultaneously display information from other systems.

Desktop

The desktop consists of object's digital plan, which is possible to enlarge/reduce or move. All the signs linked to system detectors or techincal devices are marked on the digital plan according to their real positions on the object.
Move the cursor on the object plan and the information about the addresses of the detectors and statuses will be displayed.
Real time picture of the camera will appear in new window when moving to its sign.
Events log is placed at the bottom of the screen.
On the desktop, the number of objects belonging to a particular client is not limited.
Each and every object can be opened under its icon.

Working

For example, in the case of alarm, an object map will open on the desktop, showing the accuracy of the detector or an armed area – what system and which device had an alarm.

Worker in duty or manned alarm centre or the security control centre benefit from it – they can send the security service or the operative services straight to particual event, exluding the situations with big buildings where the security service drives around the building without knowing the exact location of attack or any other unwanted event.

HotSec is also capable of receiving information from other systems, such as in the case of incoming alarm from the motion detector – the system enables to display the real time picture of the nearest cameras either automatically or by clicking the camera icon. In the case of fire, we receive visual information from the movement in the rooms and the expansion of fire. For the alarms coming from automation systems, we can automatically or visually monitor the activity log and get an overview who is where in the building. HotSec enables to create a variety of possible relations between the systems and system parts or in other words, between the detectors and the devices.

HotSec also acts as central events log – it enables to display event logs from one desktop simultaneously or separately. It also enables to perform different reports from particular systems or from all systems simultaneously.

In order to visualize all the events precisely, HotSec acts as the synchronizer of all the timezones of different systems. The frequency of synchronization can be measured however you wish, although it is an automatic process.

HotSec enables to give different access levels to different system users. For example, the automatics engineer sees only the automatic icons, can display certain parametres and the linkedd events. Staff worker, who is allowed to wizard new cards, can only add users and access levels to all or certain areas. The security worker can see all the icons on the desktop and takes action depending on the nature of alarms and events, but cannot give privileges, change parametres, arm or disarm certain areas etc.

Of course, it all depends on the security conception of a particular company, which we can also help to construct.

Security

The system enables to display information such as who watched when and what in the system or which actions or reports were taken. Each user enters with personal password or identification card and depending on their position, has access to different, yet only work-linked functions – department feature.

All the system centres, detectors and devices work independently and will not stop working when problems with data communication or IT occur.

If the system management is held outside the building or via telework, HotSec will work over computer network (Internet), connection is via secure data channel (VPN, SSL).

HotSec works in the client's server and the vendor or the builder have absolutely any undesired access to HotSec management software.

Depending on the client's needs, wishes, the capacity of the objects and the agreements, can also provide the server service (so-called accommodation service).

Access control system

HotSec enables to get information such as who is where in the building, displaying the information which access controls where lately used.

HotSec enables to create a circuit for the security worker, by setting the order and timeline of passing the points –if infringed, the system will transmit an alarm depending on the event. If the circuit is held inside, the signals will be transmitted from the motion detectors and from the access control system. The card readers of the access control system can also be used as the controllers of circuit (so-called checkpoints). For example, if there's a burglary or an undesired person has stayed in the object, HotSec enables by detector visualization to identify the location and/or direction of the person in order to catch the intruder in the right time and right place.

In addition to opening door, HotSec enables to arm or disarm certain area. When the worker enters his cabinet, he opens the door with card and simultaneously disarms the room. HotSec is capable of managing multifunctional access systems, such as proximity readers with keypad, the functions of keypads and proximity readers taken as separate units, as well as different access points in order to guarantee larger access security.

In addition to the text above, it is possible to apply the means of common access system, such as giving access rights and forbidding who can go when into certain place, monitoring the user, using the worker's control etc. What matters the most, is the fact that all the log reports can be centrically supported with the information from other systems. All the functions can be applied from teleworking position, which has the rights.

Applying access card as a means of payment

HotSec enables to create an account for each user. The money on the account can be used to pay for some products or services. It is possible to use both the advance and afterwards payments in relation to the services used.

Such services can be:

- Using the coffee machine
- Using the vending machine
- Paying for the parking

- Paying in the eatery
- Copying and printing

Surveillance system

HotSec enables to arm and disarm all the areas from the desktop. For example, if a client has different objects in different cities, it is possible to arm and disarm an object, check the statuses of object systems or give/remove the arming privileges relating to all the objects as a whole or separately; the only condition is Internet connection.

It is possible to apply the automatic arming of object or different rooms of the object at certain time. It is a good instrument to reduce the risk of human factor, when arming is forgotten or other motifs cause the disarming.

We also receive information about staying in the rooms from the detectors set to disarmed mode. The system enables to switch off the lights, reduce the amount of ventilating air and heating if there have been any movement during certain time. It is also possible to switch electric devices on and off.

In case of evacuation, we can monitor and check whether all the people have evacuated and there's no movement in the rooms. For example, in case of fire, the motion detectors transmit the signal of people moving in the dangerzone.

Fire alarm systems

HotSec shows the alarms of fire systems with the accuracy of an area or room.

HotSec enables to display the picture of nearest camera or cameras automatically or switches certain cameras automatically to armed mode.

Cooperation with other systems gives us substantially bigger overview of the situation concerning the justice and nature of alarm, the expansion of fire, people moving in the dangerzone etc. Broader information of the event gives a significant advantage to the operative and security services to react precisely and effectively, for the protection of workers' life and health and for the maintenance of the enterprise' asset.

Video system

HotSec enables to display the real time picture of the camera by clicking on the icon. The videosystem can be used as a separate surveillance system, where the surveillance function of the cameras is to constantly monitor the control centre. Cameras can be set to arming mode on certain time. In any other time, only the motions are recorded. Once set to arming mode, the system will give an alarm on the marked area and when the camera is unplugged from electricity or from transmission network. In case of an alarm, real time picture of the camera will be displayed on the requested desktop, for example in the security centre or in the centre

of security service with alarm signal. The control centre worker or the security worker will rely on the information they received and decide the reaction to the event. The purpose of the system is to identify any possible attacks and/or react from the very beginning.

Automation system

HotSec enables to display information about different automatic systems on the desktop. For example: the temperature, pressure, air and humidity, CO_2 concentration in air, amperage, water quality (chlorine concentration) etc. HotSec enables to monitor the required indicators in real time on the desktop and display the linkedd logs. If required, it is possible to display the information about modifications in parametres to control centre or to special employee, in order to react before any undesired action takes place. Also, certain employees can change the parametres.

HotSec enables to read different indicators from the distance. For example, it is possible to display information from different counters (e.g water or other fluid indicators) during some period.

Transmitting alarms

HotSec enables to start transmissing alarms in case of prohibited action or the alarm situation in systems or deviations from set parametres.

A variety of communication equipment and broadcast channels can be used to transmit alarm signals (radio transmitters, telephone lines, GSM modem, Ethernet, Kõu, Wimax etc.) and messaging devices (SMS, e-email etc).

Basic functions

- visualizing systems
- controlling systems
- recording events
- compiling reports

User manual

While compiling the user manual for HotSec management software, it is taken into account that the user has the elementary skills for working with computer and with Windows programs.

The user manual describes the general guidelines for working with the software programs:

- managing the users of local security system
- managing the end users of local security system
- adding new users

- changing and deleting data
- adding and changing rights to access system
- monitoring the technical status of local security system
- managing the alarm events
- filing and compiling reports for the events of local security system
- printing reports

The present user manual does not contain actions linkedd to installing local security systems and for making drawings into graphical part.

Language options for HotSec

- Language options for software program:
- estonian
- english
- russian
- finnish
- sweden
- latvian

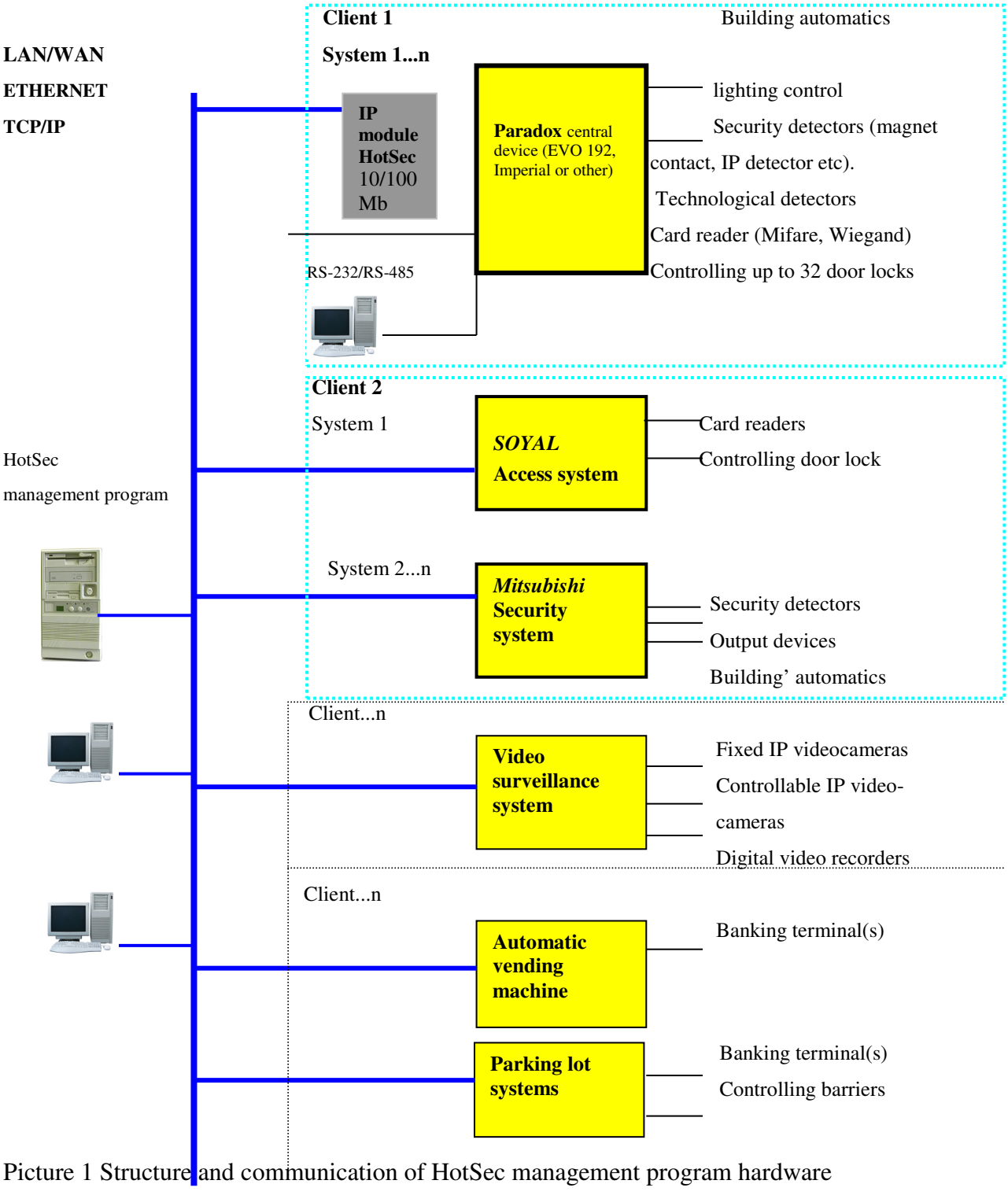
Licensing

Each client is given a system license according to the required amount. The license is on USB dongle and is located in the server of HotSec software.

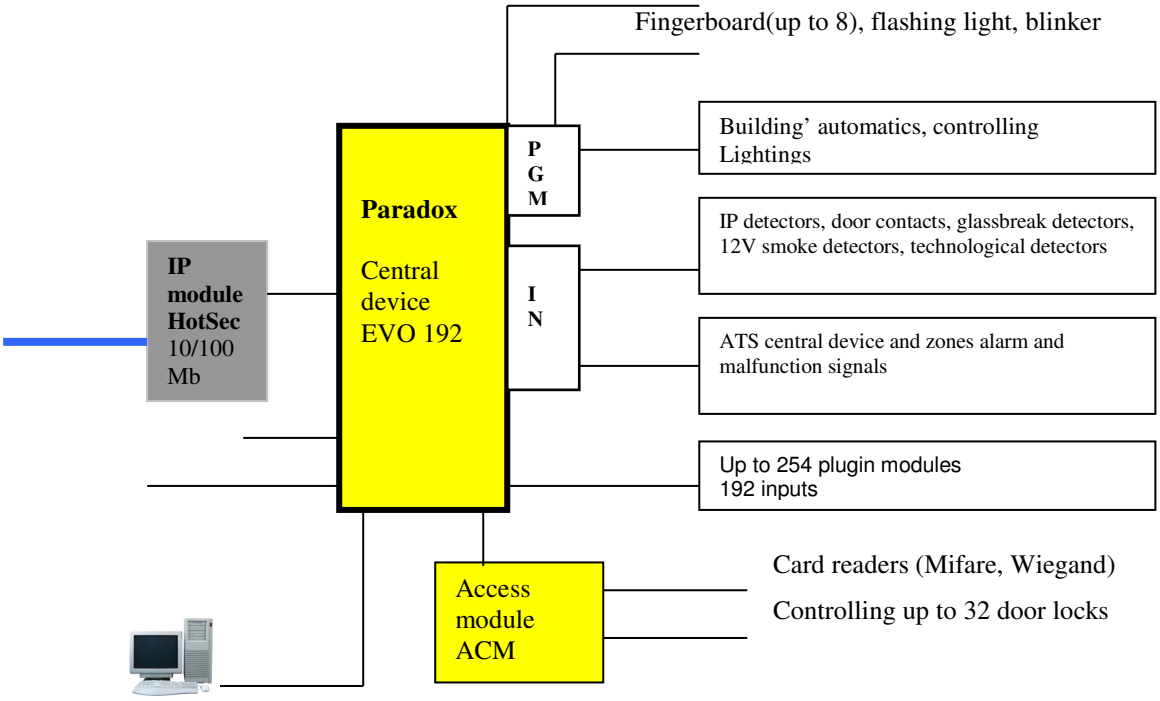
- the system license contains these required options for client:
- the number of Paradox security alarm panels
- the number of Soyal access system doors
- the number of Mitsubishi security system panels
- the number of users working simultaneously with the program
- existing video system
- existing synchronization

Management program structure and communication

Hardware and communication structure



Picture 1 Structure and communication of HotSec management program hardware



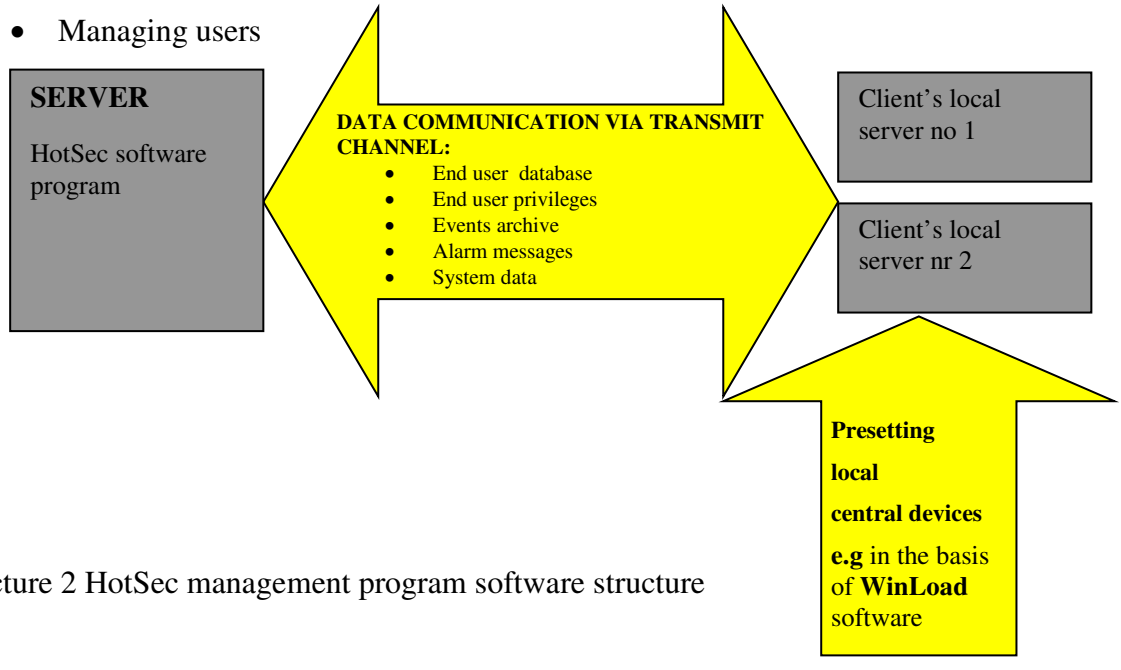
Pictures 1-2 Example of Paradox EVO-192 structure

Software structure

HotSec Modular management software is made to monitor and control the systems in buildings.

The basic functions of HotSec management software are:

- Visualizing systems
- Controlling systems
- Recording events
- Compiling reports
- Managing users



Picture 2 HotSec management program software structure

Terms

User	HotSec management program user according to certain class of rights (level),
End user	The user of local access system or security system according to the rights acquired
Local security system	Security, video or building' automatics installations placed on the client's object.
Security area or partition	Set of security alarms and its detectors, which form the area with logical and unified rights.
Installation	The devices or set of devices installed to the object.
Object	In HotSec system, object is the name for the installation
System	Set of technical objects linked to each other
Preset	Before giving to the client, the installer has set default settings or any data required for the system
HotSec client	Monitoring position, which is installed to the user's computer
Area	The mental part of object on the graphical plan as a whole

Installing, starting and closing the management program

Installing the management program

HotSec management program will be installed to the computer (e.g client's computer) either by the service provider or by licensed user, who installs the software program. The program works with Windows 98, Windows 200, XP or Vista.

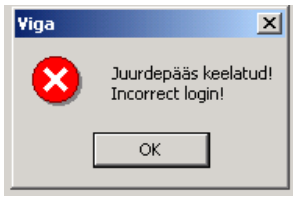
After the installation, HotSec client icon for the management program will appear on the desktop.

Opening the management program

1. On the desktop, click on the HotSec management program icon
2. Clicking the HotSec icon will open the identification window.

In the window, type the user name and password

3. On the System field: if several systems are managed, search the required system from the options. If the user manages only one system, type the default IP address.
4. Clicking the Options bar will open and hide the system bar.
5. After typing the data, click OK
6. Clicking the Close button will close the management program.
7. User is unidentified when access is denied or data error occurs.



8. Click OK and re-enter the correct data. If still not succeeded, contact the installer.
9. In order to guarantee the safe use of program, only the persons with certain rights (the default username and password for the first login are admin and parool 1) can work with it. Only the system administrator can change the password for using the software.

Classes (levels) in HotSec management program:

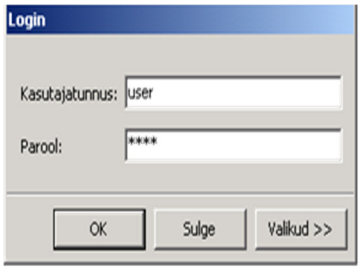
-User -can view and control his objects, and view alarms and system maps
-Operator -can control objects
-Supervisor -can add new users and give them rights
-Administrator -can change the system settings, monitor and control objects

Clicking the HotSec client icon will open the management software. In Program's User computer, HotSec icon will appear in the desktop, on the menubar. Clicking the icon will open the program and the log in window.It is possible to set the management program so, that every time user logs in, the program will automatically start. (check Program settings, tick in ''automatic log in'' window).

Authenticating the management program user

Clicking the HotSec icon will open the identification window. To log in, enter user name and password. Click the OK button.

The purchased license and user rights limit the use of operations available in HotSec management program. The program window on the desktop confirms the user authentication according to his class (level). Depending on the rights, the picture will differ –inaccessible fields will



be hided.

If logged in, management program window will appear on the desktop.

Typical program window is on Picture 3 and Picture 4.

When program opens, homepage with all the settings, quick launch menus, graphics and active log will appear on the desktop.

The apperance of graphics window and active log window depends –if the window views are preset or if it's the first login. The set window will be in memory and the next time it opens, the previous view will appear.

According to login rights, HotSec program window will appear on the desktop.

Program user window

According to HotSec program login rights, the next user window (preset, an example with admin rights) will appear on the desktop. Desktop layout is automatically saved and is the same every time the program opens.

Settings menu

Quick launch toolbar

Graphics window

Objects/areas bar

Client's homepage object/areas map (homepage is selected)

Activity log window

Activity log filters settings and options bar

Activity log in real time

System statuses in program –message bar

Program title bar, login name and class

Blue – object/area is armed

Green – object/area is disarmed

Grey – central device is poweroff

Blinking purple/green – arming/disarming delay is on

Blinking red – armed area/ alarm in memory

Window background is **Grey** –user has CommError with server

Picture 3 Program user window (example, depends on settings) view

Setting the program user window

Every user can design the window (screen picture) according to his rights and priorities while using the management program. Basic views are **graphics window** (client's object maps) and the **activity log** window.

To change the proportions of graphics window or activity log window, click in window. When window is active (turns blue),drag with left mouse button to the place you need.

To change the proportions (size) of the graphics window or activity log window, move the cursor to any window edge (arrow will appear) and move the edge to desired size by holding down left mouse button.

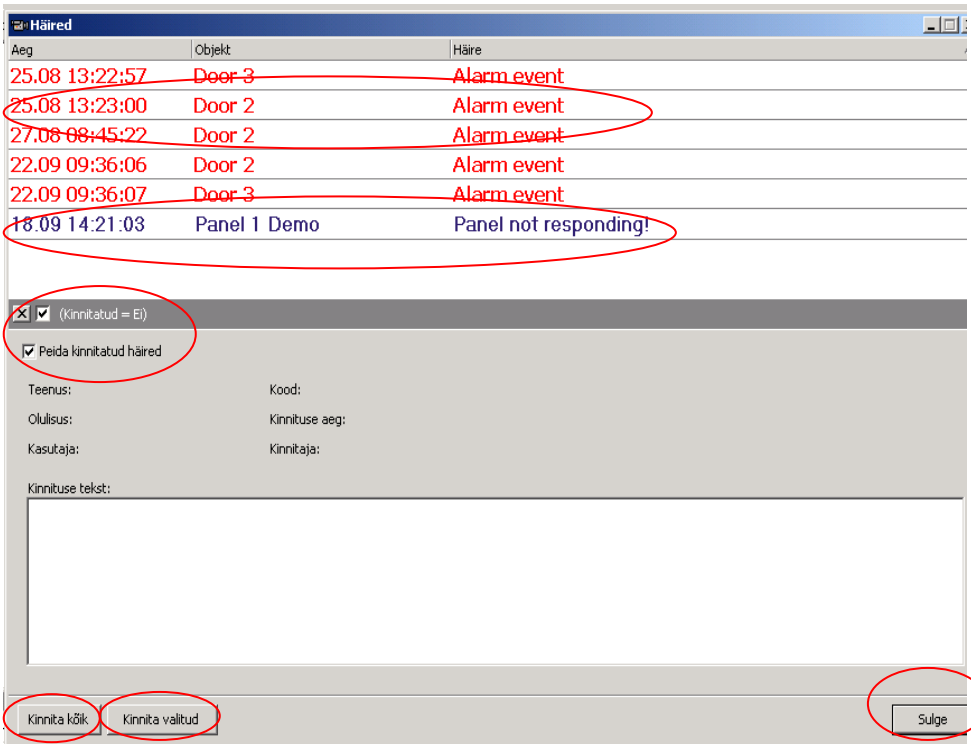
To move the image, move the cursor to graphics window and move the image by holding down left mouse button. To enlarge or reduce the image, use zooming or mouse wheel.

Management program user can use only one window out of two, if needed. Choose with quick launch buttons: setting system card or showing the activity log. If the user has extra monitor (display), one of the windows can be displayed there (in full view).

Picture 4 Setting the program user window (user screen)

Alarm window opening the program

When you open management program, active and unaccepted alarm window will appear on the desktop (see Picture 3) and in the bottom, under the system statuses there's the number of alarms.



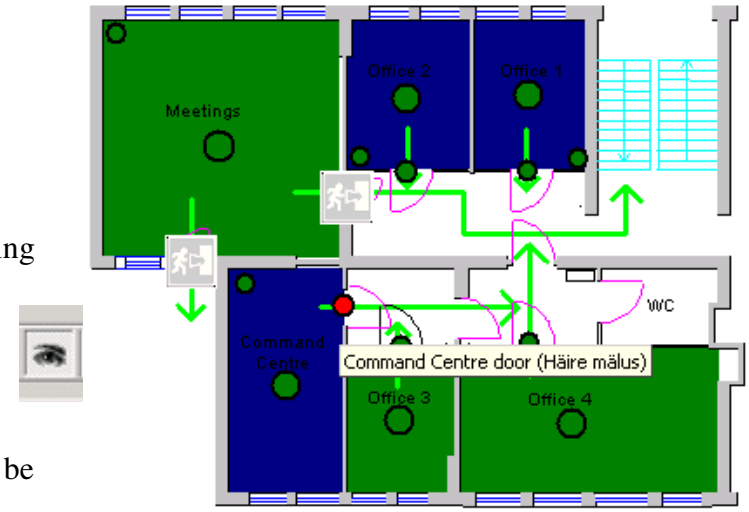
Picture 5 Alarm window opening the program

In the alarm window, the active and unaccepted alarms are red.

Checking alarms

In real time, the armed security area will signal the alarm when the security group blinks red on the graphics map.

On the object map (e.g floor map), the location of alarm detector will be displayed automatically, if the monitoring alarms icon is on.



In the activity log window, the alarm data will appear. The alarm will be lost from memory, if object is armed again.

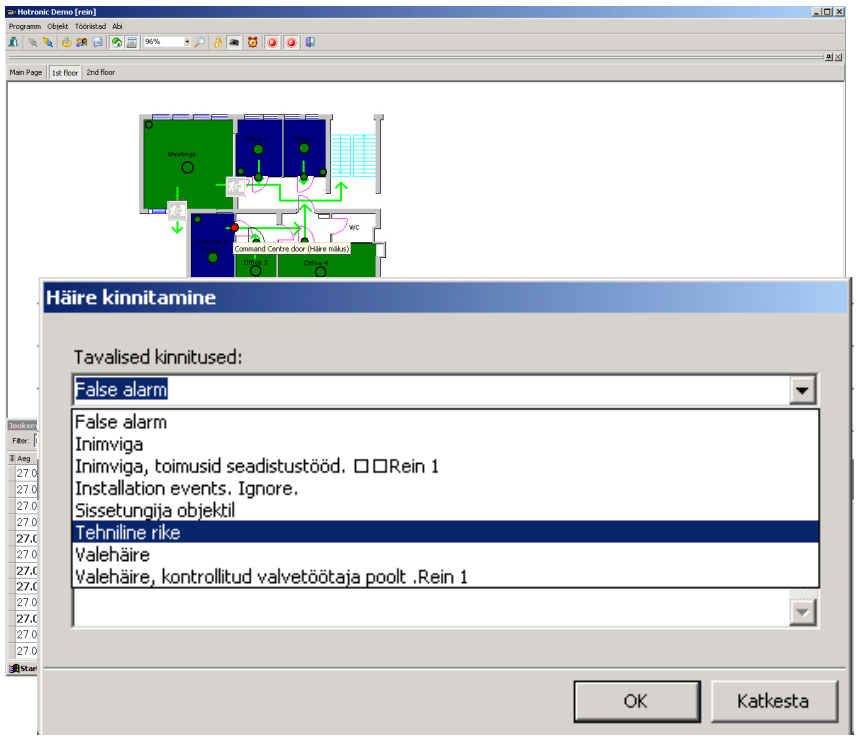
Picture 6 displaying the alarm message on the object map (example, alarm in memory)

Accepting alarms

On alarm event:

Accept the alarm by clicking the bell icon, in the opening window add explaining about the alarm or simply accept.

Picture 7 Window with alarm, alarm log window



Picture 8 Window accepting the alarm

Acting on alarm event, transmitting the alarm

Transmitting the alarm takes place according to the procedure agreed, to the terms in security contract and to the agreements.

Possible versions:

- the object's alarm is transmitted to patrol car
- the object's owner is informed, further actions to find reason for alarm is agreed

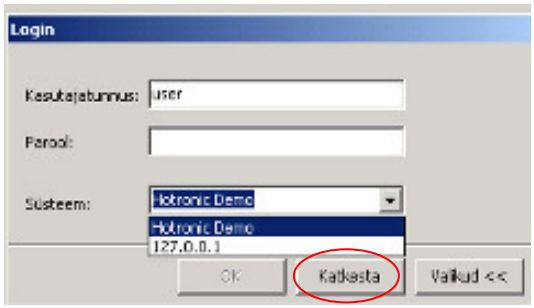
Closing the management program, possible login problems

1. Possible options to close the management program:

   - On the quick launch icon, click Close client

   - On the settings taskbar, choose Program Settings and Close

   - On the Quick launch menu, click Connect to Server, login window appears, click Cancel.



Picture 9

   It is also possible to change the class without disconnecting or, if several systems are managed, choose new system.

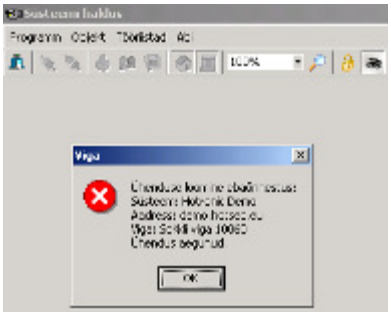
   - To choose new system, click the Options button and on the system bar, choose new system from the list.

   Enter user name and password.

   If the user has only one system, then there's no options - enter only the IP address of system.

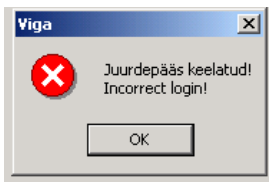
   Login window

2. If the connecting fails, an error with information on the system data and the cause will appear on the desktop.



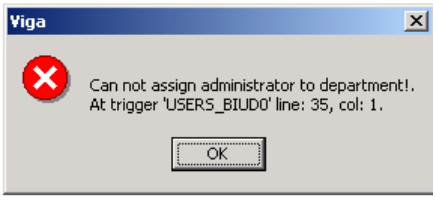
User's activity depend on the character of error:

- If login fails, enter the user name and password again
- Check the server data from settings menu
- Check the Internet connection
- If problem continues, contact the installer



for reasons.

- Give accurate information about the error to the installer.



Picture 10 Error windows

3. Transmitting the error by e-mail (to the installer)

To copy the error window, press Ctrl +C and place the information to mailbox by pressing Ctrl + V

4. When user with admin rights updates the program version, the updates will take place automatically.

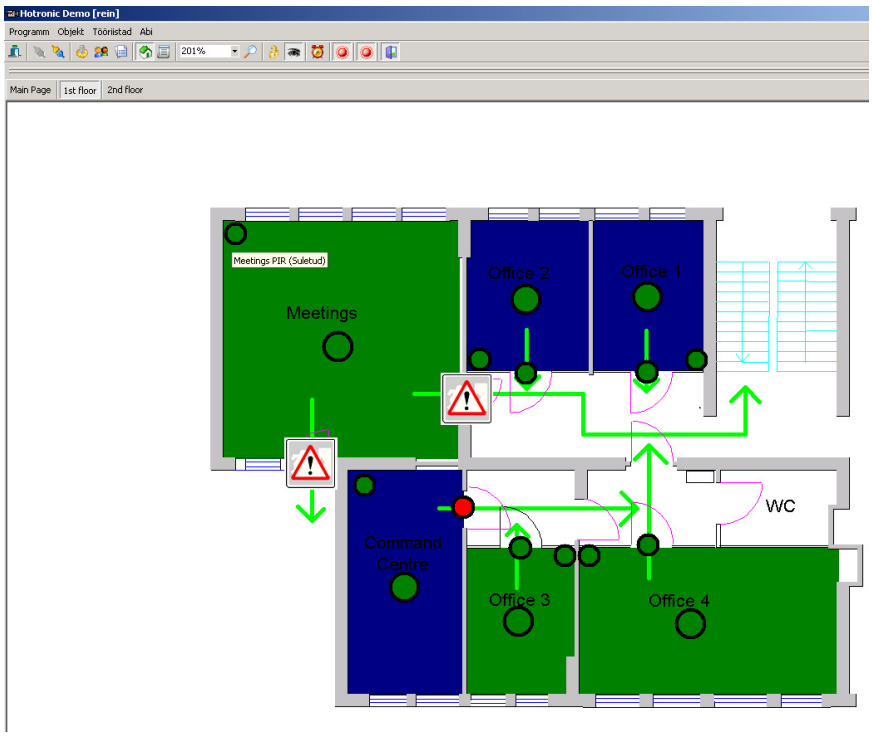
Graphical part description

It is possible to upload the ready-made object drawing from file (.jpg, bmp.,dwg, .dxf) or plot it in the management program. Detailed guideline for plotting the graphical part of management program is in separate user manual.

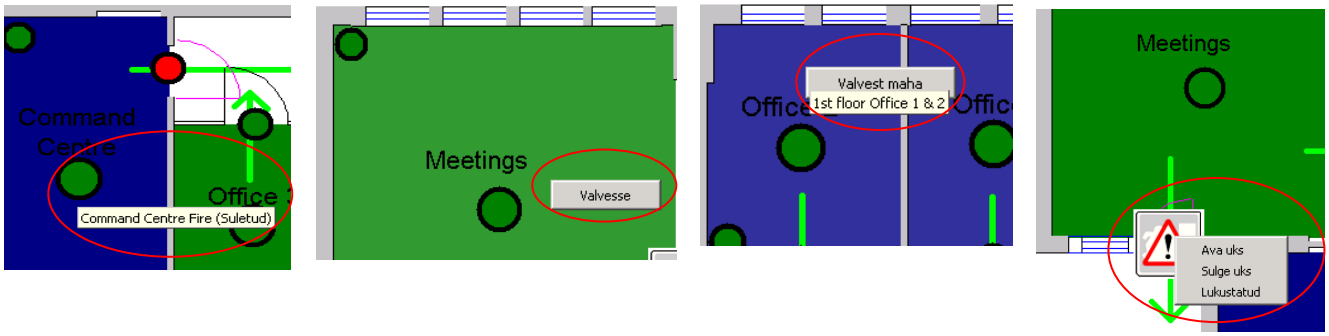
The object scheme can be decomposed and different parts of the building (floors or its parts) can be placed on different layers (according to client's wish; preset).

Actions on the object map

Moving the mouse over the scheme will activate the areas below the cursor. Clicking the active security group with right mouse button enables to arm certain group now or with delay. Similar actions apply for the access system, where clicking right mouse button opens or closes certain doors.



Picture 11 View of the security system and detectors on the graphics page (on the map, showing detectors is turned on with quick launch button)



Picture 12 Views of available actions on the object's graphical drawing (the object map).

Clicking the door icon on the object scheme with right mouse button enables to change the doors mode – open door, close door or lock door. All door statuses can be controlled from the menu Object -> All doors -> and commands „Open", „Close", „Lock", or „Unlock".

Signs on the object map and their meanings

The graphical part, which is used to visualize the management program, gives very good overview to the user. The signs used in the system and their definitions are below.

Access system signs

On the object scheme, the doors are marked with following signs (see Picture 11)

Clicking the door sign with right mouse button enables to change the door mode.
The door signs are preset, it is possible to change them if required.

Door not in use

According to timescale, door open

According to timescale, door closed/ with card
Door temporarily open

Door open/alarm

Door locked

Door offline

Picture 13 Signs of the access system

Surveillance system signs

The detector has three statuses:

Red – detector is interfered

Grey – detector is in normal status

Yellow – detector temporarily bypassed

Security groups have following statuses:

Green – area is in normal status, disarmed

Blue – area is in normal status, armed

Purple/Green – arming/disarming delay is requested

Blinking red – area in alarm

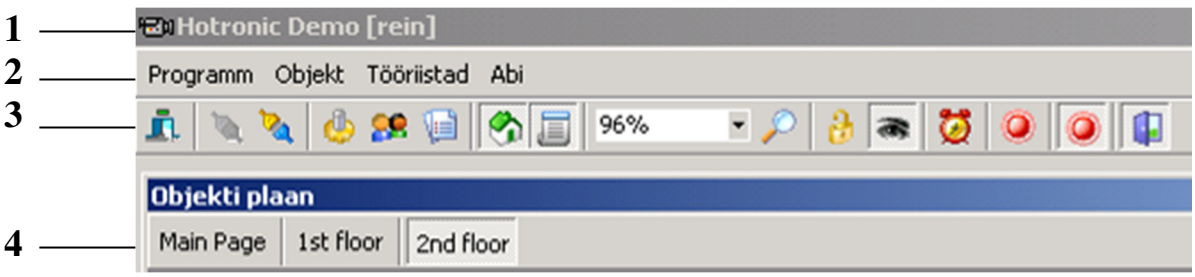
Videosystem signs

It is possible to display signs of different videocameras on the map. Clicking on icon will display the videocamera's picture in separate window. In case the videocamera is attached to certain detector or area, the picture of this detector or security area will automatically open in an alarm event.

When closing the program, software will remember the size of video window and the location on desktop. The location and size will be the same, when opening.

Menu bar icons and settings descriptions

Description of basic view



Picture 16 Settings and quick launch icons view

Description of the taskbars (on top of the window):

1 – title bar of management program's software –program logo with client name and program user name

2 – submenu with setting options

3 – list of objects on the object map (number of objects is not limited)

Description of the program taskbar (in the lower corner of window):

1 2 3 4 5 6

Picture 17 Message bar and service status indicators of the management program.

1-4 Objects connected to management program: local system status indicators and definitions.

- Roheline Systems connected to management program are working and in online mode
- Punane System(s) not connected (offline mode)
- Kollane Malfunction occurs in system(s) connected to management program
- Sinine Service is busy, data update progress

1 – Paradox central devices

2 – Surveillance system

3 – Access system

4 – Synchronization

5 – Active alarm messages in the log –unaccepted alarms

6 – Status indicators' information, moving the cursor to indicator will appear the record

Menu bar options description

From the settings menu bar, the following submenus can be chosen:

1 – Program

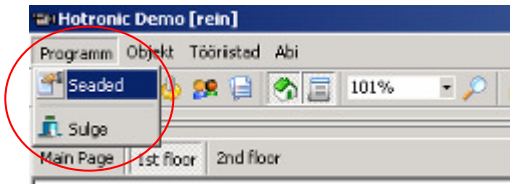
2 – Object

3 – Tools

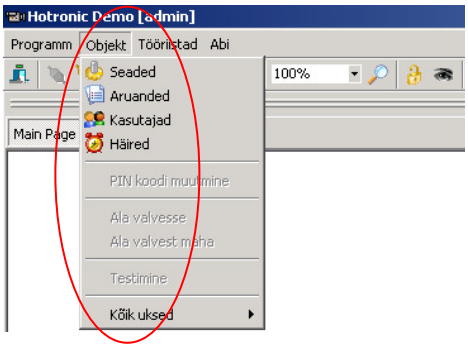
4 – Help

Picture 18 Settings menu bar

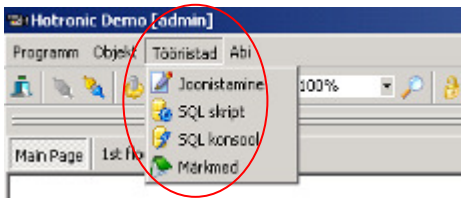
In the **„Settings“** submenu, all basic data, which is required to client's system, will be set (see also p.4.1)

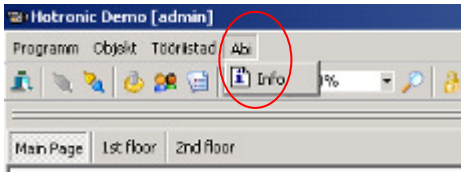


In the **„Object“** submenu, the dataset of client's main system and client's object (the installation) or the management of reports and users will be set.



In the **„Tools“** submenu, the graphics part of client's system will be set (drawings, floor maps etc).



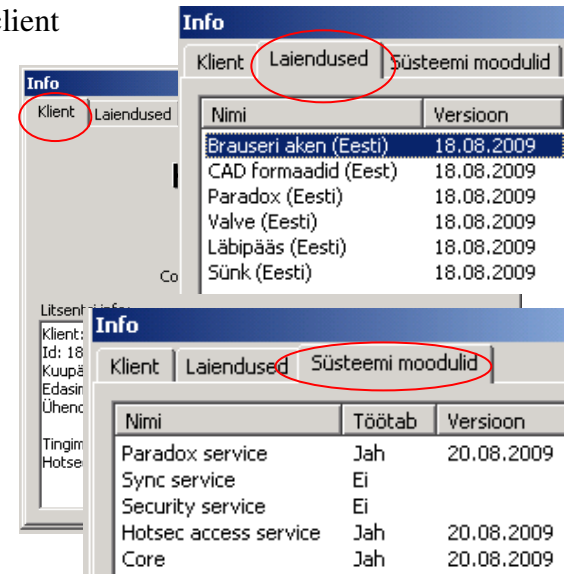


Picture 19 Settings submenus

In the **„Help“** submenu, there's information on client license and basic system data.

Required information to know which particular version we are dealing with.

Information about the plugins and system modules in client's system.



Picture 20 Client's info about management software license

The system modules or service packet connected to
management software contains:

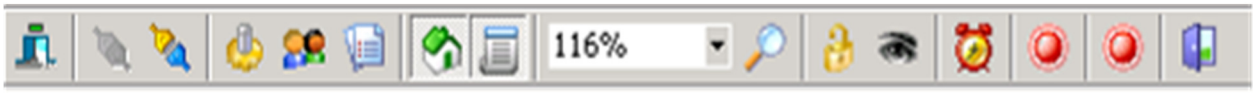
Paradox surveillance
Synchronization
Surveillance
HotSec access
Program core

Picture 21 Service packets of client's management software

The amount of service packet depends on
the client's needs and the amount of purchased license.

Menu bar Quick launch icons description

On the quick launch menu bar, it is possible to enter submenu by clicking the shortcut key.



Picture 22 Quick launch icon bar view

Descriptions for the Quick launch icons:
1 closing client (closing the program)
2 creating shortcut
3 disconnecting
4 system settings
quick option to system settings window (same as object->settings)
5 user management
quick option to manage users (same as object->users)
6 system reports
quick option to system reports (same as object->reports)
7 toggle system map, object map
8 toggle activity log
Using this quick launch button enables to open the events log. The log will open to its previous location, which is set by the user. As an alternative to docked log, it is possible to

drag it to another screen (in case there's more than 1 display to monitor the system) in order to get a better overview.

9 changing the zoom map, zoom in/out the drawing (mouse wheel does the same thing)

10 Zoom to fit all

11 Lock client, lock program/ change program user

12 Toggle monitoring alarms, activate to monitor possible alarms, if there's more than one security area and their drawings are located on different areas

13 Show alarms, accept alarms

14 Toggle zones visibility on map

15 Toggle sensor visibility on map, the icon can not be

16 Toggle door visibility on map, using this quick option button enables to hide or show the doors marked on the object scheme.

The detailed description of using quick launch option is in the settings of present manual.

Setting the client's program

Client – the user of HotSec integrated software for managing surveillance and access systems and client's systems, to which the technical security systems are installed.

The client's program settings are required when adding new user.

The settings are required and characterise client's individual data and settings.

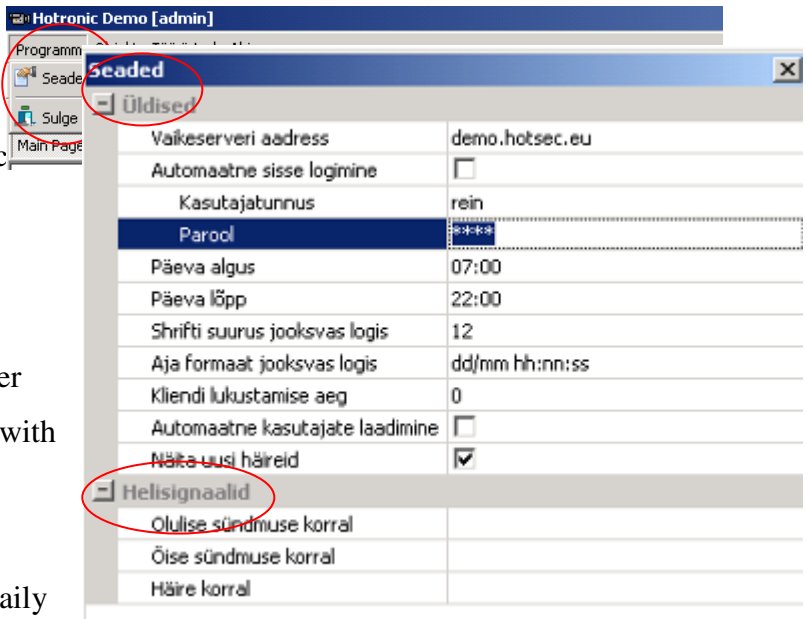
Picture 23 Program settings view

Selecting the settings in client's program

Choose from the Settings menu bar

Program->Settings

To enter new data or change data –in Settings window, click left row and double-c on the right row.



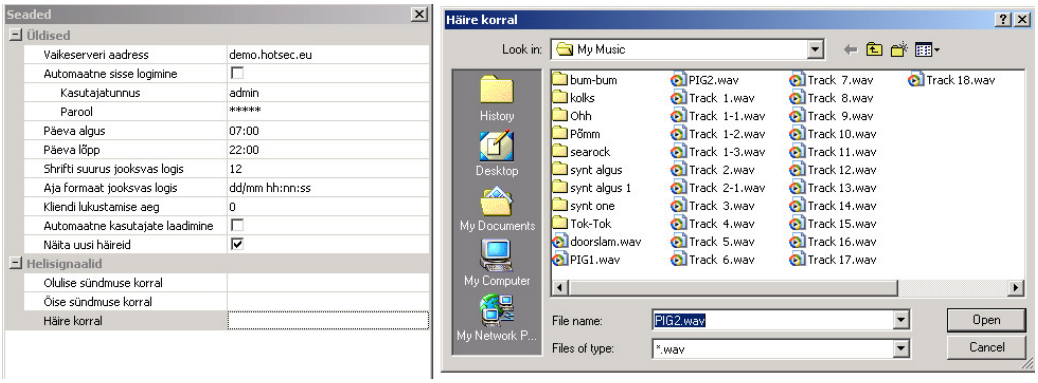
In the opening window, you can change:

- the default IP address of HotSec server
- login to the management program with user name and password
- the length of day (required to differ daily

events from night events)

- events log font size
- time and date formats
- keyboard lock delay in seconds.
  After delay, the system will ask for user name and password
- automatic upload of system settings
- event sounds
- standard .wav files can be used

Picture 24 Client system settings window



Picture 25 Importing wav files to set sounds

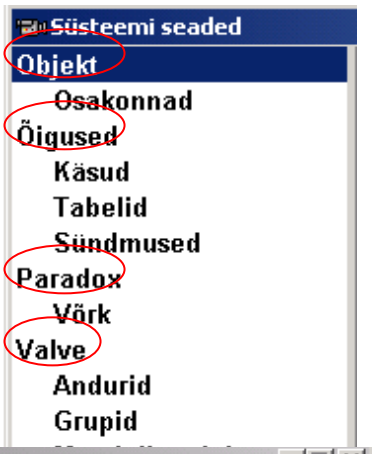
Selecting the system settings

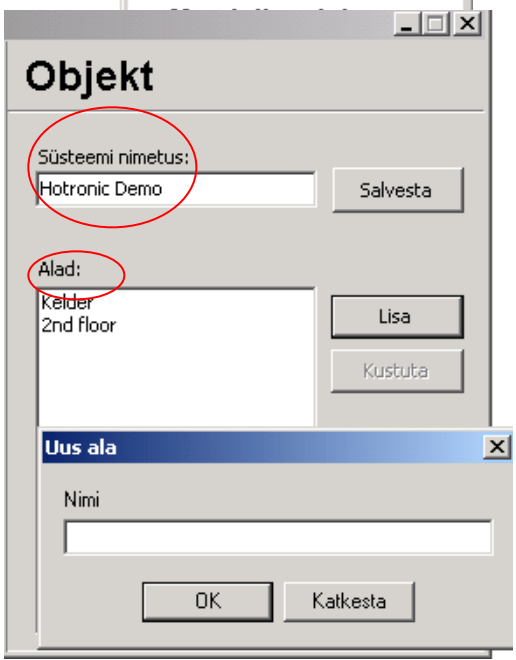
To enter the system submenus, choose System settings from the menu bar or the

icon from quick launch menu.

Submenus for system settings:

- **Object** -> system settings, department settings, binding privileges
- **Privileges** -> setting the first user levels (rights)
- **Paradox** -> settings for the central device in program
- **Security** -> security system settings
- **Synchronization** ->unified time synchronization for connected central devices





Picture 26 System settings submenus view

Object settings

System name –in HotSec system, it's the name of client installation. System name will be displayed automatically
on the system title bar.

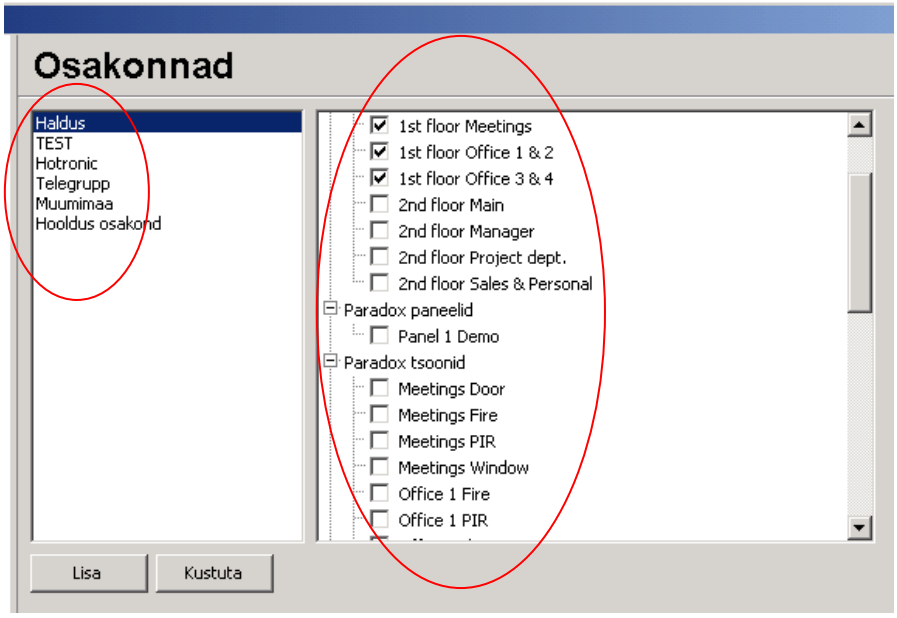
To add new object, click on the system name row.
Enter the name of new object (system), save data by clicking Save.
Area is the notional part of object. On the graphical map, it can be looked from both sides. Areas are linked to graphical part (see picture 3, areas bar).

Add ->write the name of new area ->OK
To delete an area, click on row and ->Delete. Picture 27 Object settings views
Number of areas is not limited.

Departments

Enables to add new departments, change the names of the departments and allowed actions or delete them. We need to add department to every user. Linking the user with department makes the further use of management program more effective, especially when it comes to big and decomposed systems and to clients with large numbers of end users. Every department can set its required rights by panels, arming areas and by zones.

The left-side field contains the list of existing departments.
Clicking on the department' name will appear the system table of rights on the right side.
In the right side of the window, the actions allowed (enabled rights) for department are set for using the security systems.



Picture 28 Department settings views

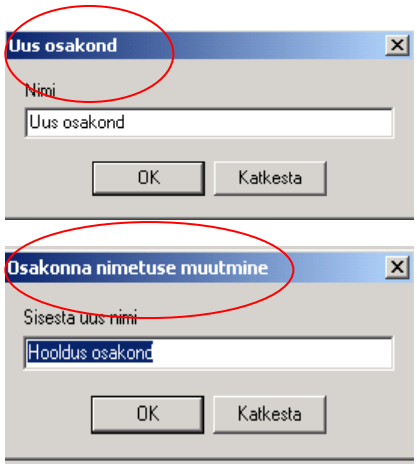
For example:

- Areas (see p. 4.2)
- Paradox partitions
- Paradox panels (central device)
- Paradox zones
- Paradox PGM-s

- Paradox doors
- Doors
- Security areas or other

To add new department, click Add, type new name and save OK
To change the name of department, double-click on the existing department field and type the new name of department, save OK

To give ceratin privileges to department, tick the field on the right (Security areas, zones, panels, PGM-s, Doors)



Picture 29Adding new department or changing name

Privileges

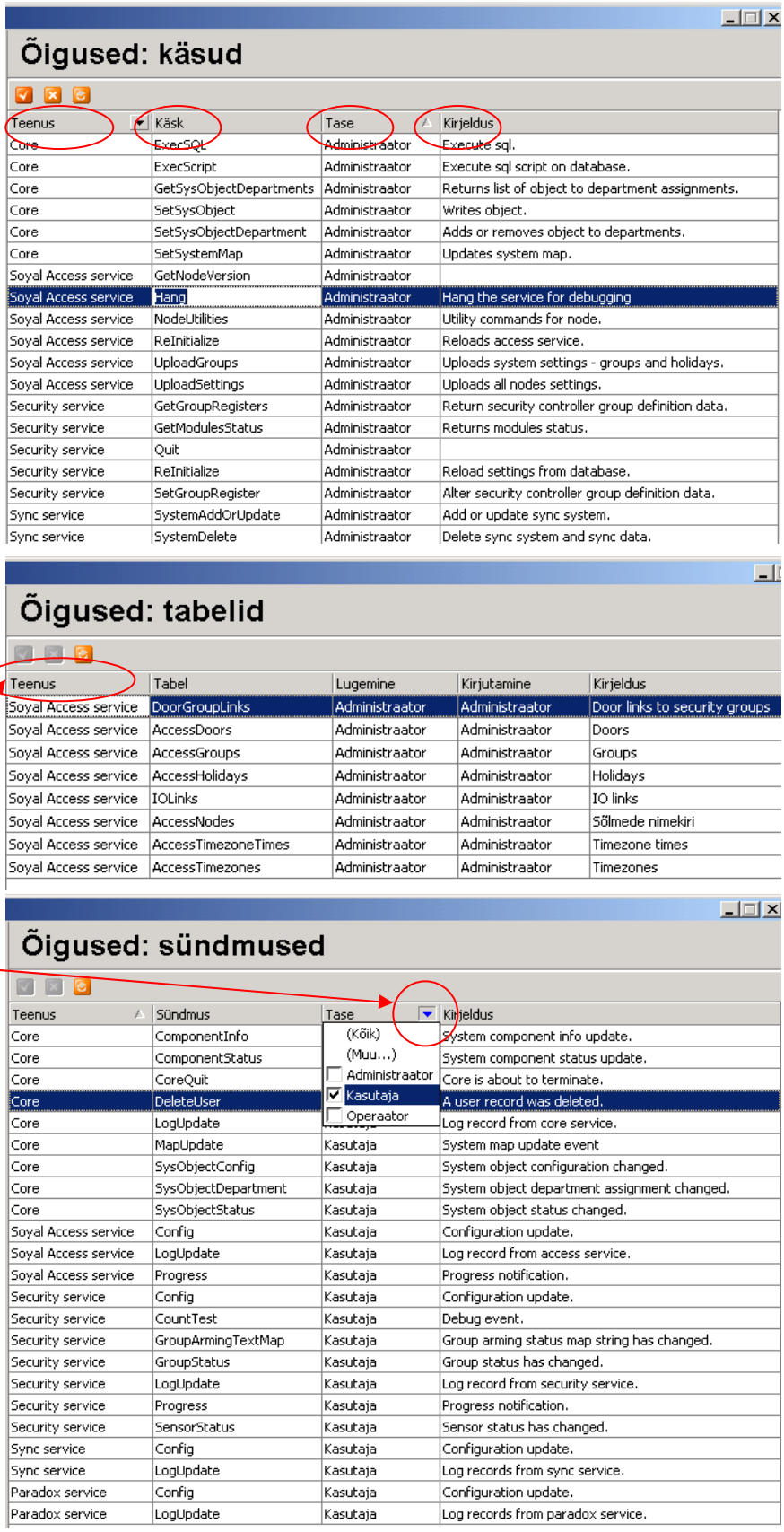
In order to manage the HotSec program,
required privileges will be given to program
users. Buttons description:

- posting changes,
- cancel
- reload data

1. HotSec system has five different

classes for users (see table 2):
User
Operator
Supervisor
Admin and
System account

Clicking the „Privileges“ table
submenu
will change the alphabetical
order of column’s list.
Double-click on the column key will open the window with the list of options.



Picture 30 „Privileges“ submenu views with partial list

Table 1 „Privileges“ (default settings) submenu

Coordinating table of setting the „Privileges“ submenu for HotSec management program. The table gives better overview of setting the „Privileges“ submenu and describes the interrelations between certain system and its needs. To set, choose an option and „tick“ in window.

COMMANDS

SERVICES	COMMAND	CLASS	DESCRIPTION
Core	Command describes certain action required to management program. To perform a command, user class must be selected in the column „Level“. **Admin class** – only admin has the privilege **User** – pirivilege applies to the rest of classes	Admin	Column list describes the commands in detail.
Paradox Service		Supervisor	
Security Service		User	
Soyal Access Service		Operator	
Sunc Service		System account	

TABLES

SERVICES	TABLE	WRITING	READING	DESCRIPTION
Core	User classes must be set in columns „Reading“ and „Writing“. **Admin class** –only admin has privilege. **User** – privilege applies to the rest of classes	Admin	Admin	Details in the column list.
Security Service		Operator	Supervisor	
Soyal Access Service		Supervisor	User	
		User		

EVENTS

SERVICES	EVENT	CLASS	DESCRIPTION
Core	Event reflects the management program software. To perform an event, user class must be set in „Class“ column. **Admin class** –only admin has privilege **User** – the privilege applies to the rest of classes.	Admin	Column list describes the events in detail.
Paradox Service		Supervisor	
Security Service		User	
Soyal Access Service		Operator	
Sunc Service			

Table 2 User classes of HotSec management program and the description of allowed actions

Table gives short overview of the actions allowed to users

No.	Description of action	User class (level)				
		Admin	Super-visor	Operator	User	System account
1	**Logging to the management program according to user class**	+	+	+	+	
2	Changing the login user name and password according to user class	+	+	+	+	

3	Management program settings	+	+	-	-	
4	Adding new users according to class	+	+	-	-	
5	Setting user privileges	+	+	-	-	
6	**Using management program graphics according to privileges**	+	+	+	+	
	- Arming objects	+	+	+	+	
	- Disarming objects	+	+	+	+	
	- Toggle monitoring alarms	+	+	+	+	
	- Accepting alarms according to privileges	+	+	+	+	
7	System reports	+	+	+	+	
8	Adding new reports, printing	+	+	+	+	
9	System settings	+	-	-	-	
	- adding objects, changing	+	-	-	-	
	- adding departments, changing	+	-	-	-	
	- setting system rights	+	-	-	-	
	- Paradox settings	+	-	-	-	
	- security settings	+	-	-	-	
	- access system settings	+	-	-	-	
	- drawing the graphics	+	-	-	-	

Paradox central device

Compared to other integrated security systems, HotSec has the advantage of integrating widely used Paradox security alarm central devices into the system hardware. Every bigger installation company has the experience to install and set the product.

Paradox local central device (panel) has to be installed and set according to requirements and the user manual.

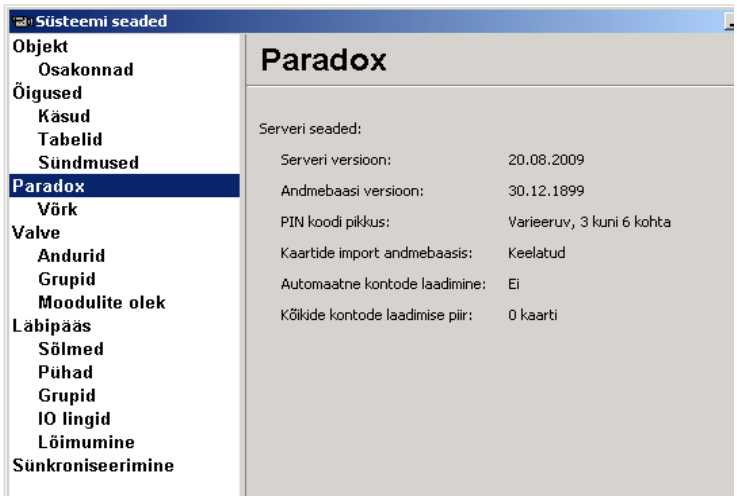
Possible options for programming the local central device (panel):

- From the central device keyboard (LED, LCD)
- With Paradox Memory Key
- With WinLoad software. The central device can be programmed right in the installation place or from telemanaging, that is using telephone line or Internet connection. To use telemanaging, the WinLoad program can be in client's computer with the software program. The required settings (4-digit panel number in identificator, 4 or 6-digit PIN code) must be previously entered in the sections of central device.

The previous parameters of local central device to connect with HotSec management system:

- Names of the zones,
- Zone parametres
- Zone settings in security areas (partitions)
- Names of security areas

- Access system settings



Picture 31 Paradox settings general data view

Paradox: network

The window displays all the client objects' Paradox central devices connected to the system.

1 **2** **3** **4**

1 – Panel – the name of client's object, the list of client's local objects in management system

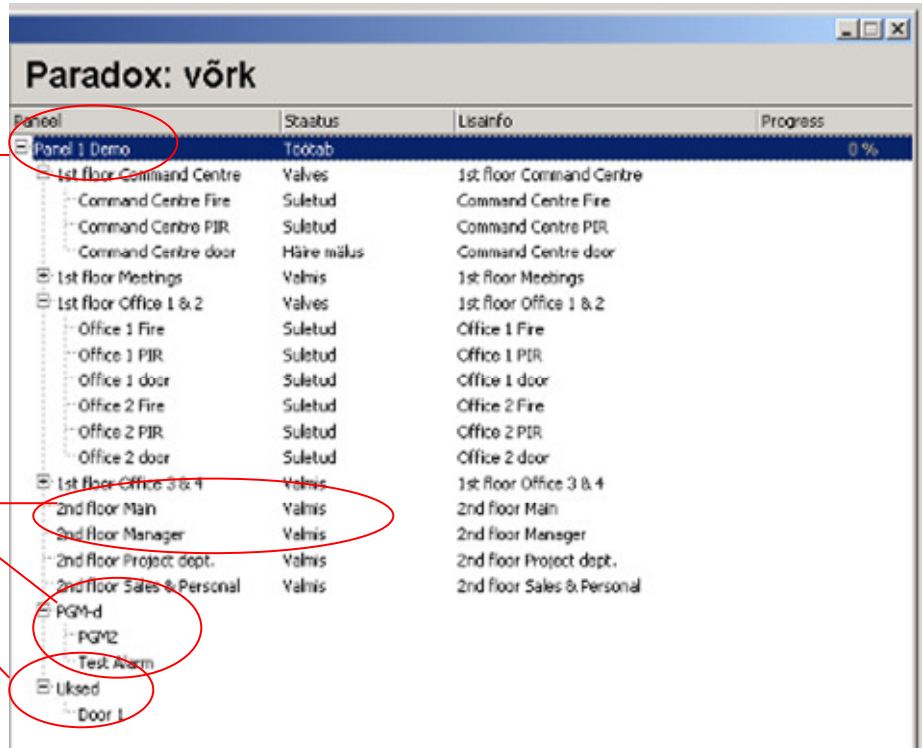
2 – Status – shows the panel status in real time (armed, disarmed, working, open)

3 – Extra information – can add extra information, if required

4 – Progress – shows the data upload/ refresh progress

Looking network configuration:

1. To open or close object (panel), click on **+/-** sign or click the required row with right mouse button. In the options, click **„Open".**
2. On the panel, the list of object's security areas,



PGM-s and access doors will open.

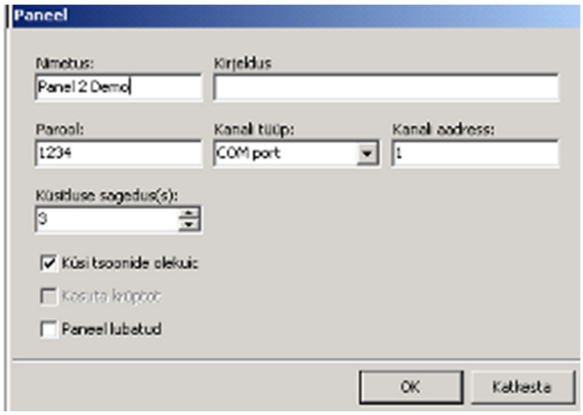
3. List of security zones alarm settings

Picture 32 Paradox network security

Adding new object (panel)

1. To add new object (panel), click the right mouse button on the objects row. In opening window, enter required data. Compulsory fields are:

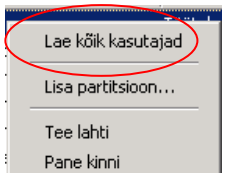
- **Name** – name of client's object/installation
- **Password** (4 or 6-digit PIN code, which is previously set in Paradox central device)
- **Channel type** – choose Com port or Ethernet
- **Channel address** – IP address of panel
- **Polling frequency** timespan between 1...60 sec



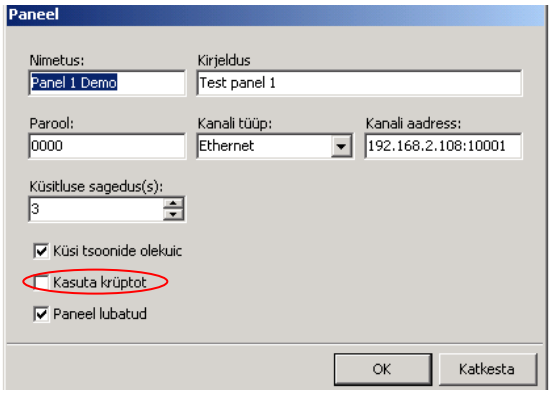
Click OK to save, to close without saving click Cancel

Uploading data into local device when adding new users or changing data:

On panel's field, click with right mouse button. In the opening window, click „Load all users" field. The data will upload into new panel device, it can be monitored in the „Progress" row.



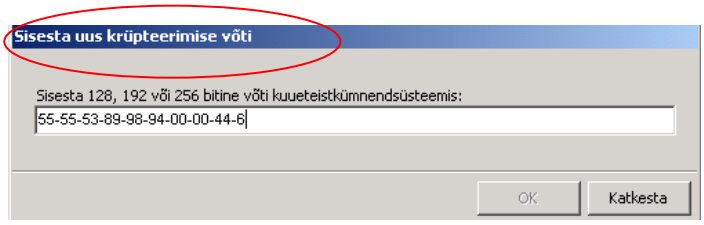
To change panel data, activate entry and enter the changes, OK to save.



The encrypted signals in the transmit channel between the server and object can be used to rise security level. Each channel can have its own encryption key.

Ticking in the „Use encryption" window will appear

another window to enter the encryption key.

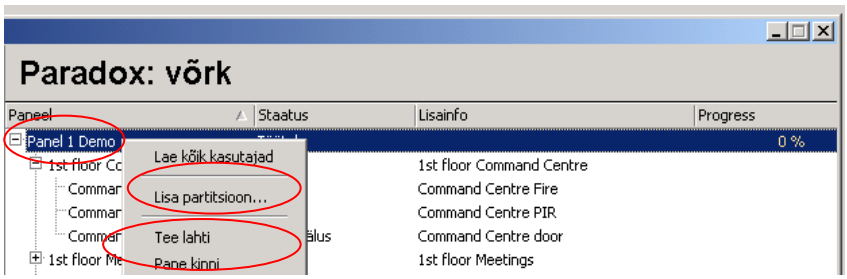


The same code of encryption key must be entered in the IP module of local object.

Picture 33 Adding new central device (panel) to the system

Adding new partition

Right-click to add new partition in panel.

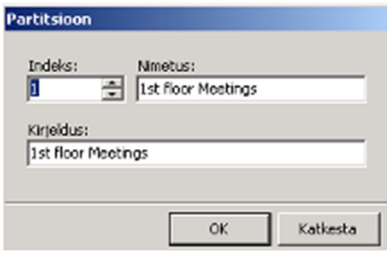


Index – the number of Paradox central device partition (security area).

Most central devices 1...8, Imperial 1...32. In relation to the partition number on central device, filling compulsory.

Name – name of the security area,

Description – additional description in free form



Picture 34 Adding new partition to Paradox network

To save data, click OK.

Adding new zone

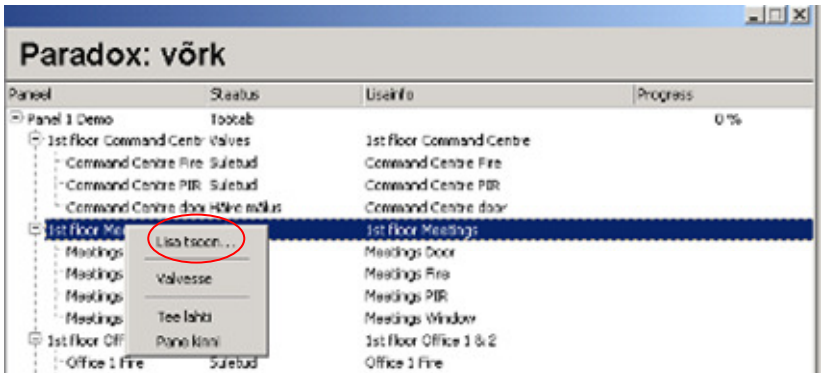
Enter data:

Index – the zone number of Paradox central device, in relation to the zone number on the central device, filling compulsory

Name – name of the zone

Type – choose required type of sensor from the list. Required option, it's related to graphics (the drawing)

Description – additional description in free form.



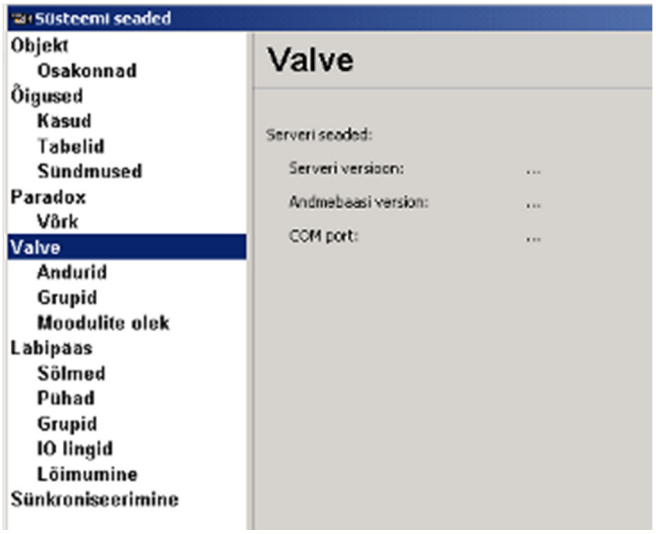
To save data, click OK

Picture 35 Adding new zone to Paradox network

Surveillance system settings

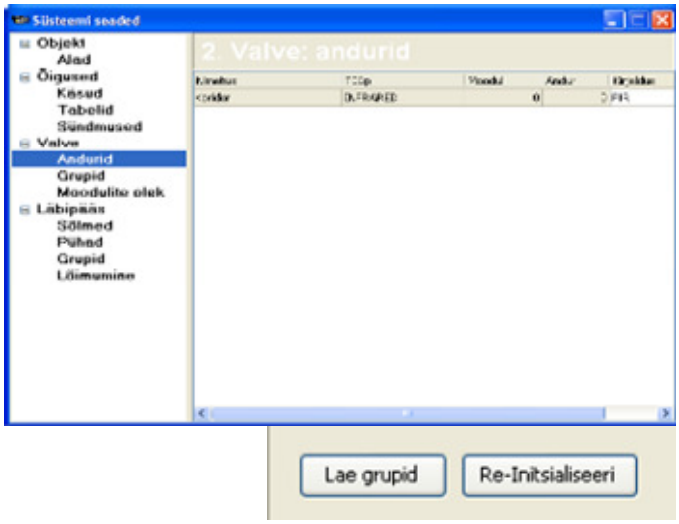
To load security sensors and groups into controller, click Load groups.

Re-initialize: required after adding or changing the modules/groups



Picture 36 General data of the surveillance system server

Detectors



Insert button on the keyboard ->enter the following on the field:

Name (compulsory) –name of detector

Type –choose the type from the list. Exact type is required to document the system.

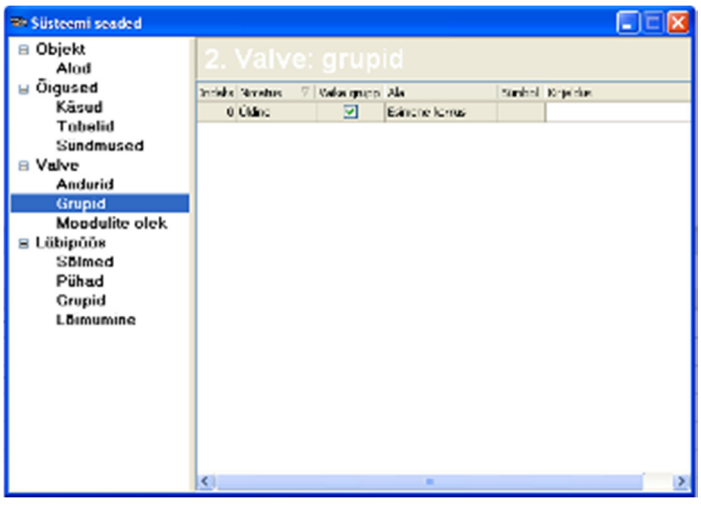
Module (compulsory) –enter the address of plugin module.

Detector (compulsory) –enter the address of detector (module input)

Description –additional description of detector, if the name is not enough.

Picture 37 Security groups table

Security groups



In HotSec system, the security group is called the logical amount of detectors. When it comes to different systems (e.g Paradox), different names for security area or partition are used.

Insert button from keyboard ->edit data in the appeared field

Index –leave empty, the system will

automatically generate it.

Name (compulsory) –name of the security group

Area –from the drop-down menu, choose the area related to security group. It is required to display the location of detector in an alarm event on the graphic drawing.

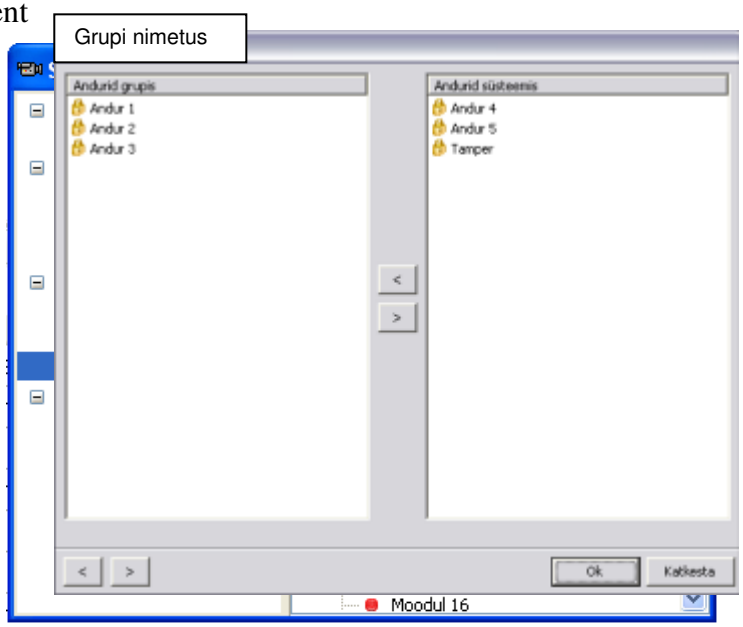
Symbol – one-letter symbol, if required

Description –the group description in free form

Clicking on the entered security group field will appear the security group setting window.

In the right corner, there's all the existing system detectors.

To add detector to group, activate the required detector(s) and press the arrow button.



Picture 37 Setting detectors into group

To remove detector from group, activate the required detector(s) and press the arrow button.

Modules state

Shows the modules state in the surveillance system. Green marks normal state, red a problem.

Picture 38 Modules table

Access system settings

SOYAL access system settings will be chosen by the installer.

To load the previously set access system settings into controller, click **Load settings**.

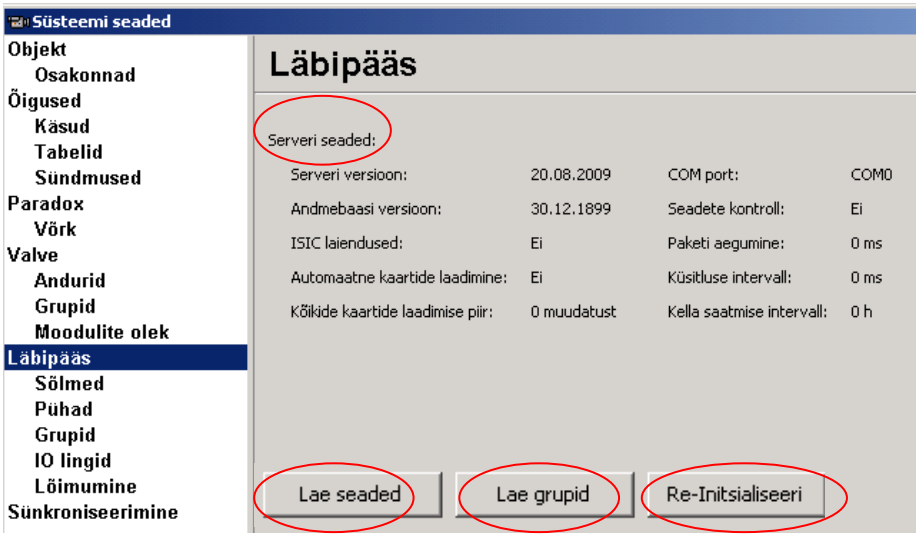
To load the previously set access groups settings into controller, click **Load groups**.

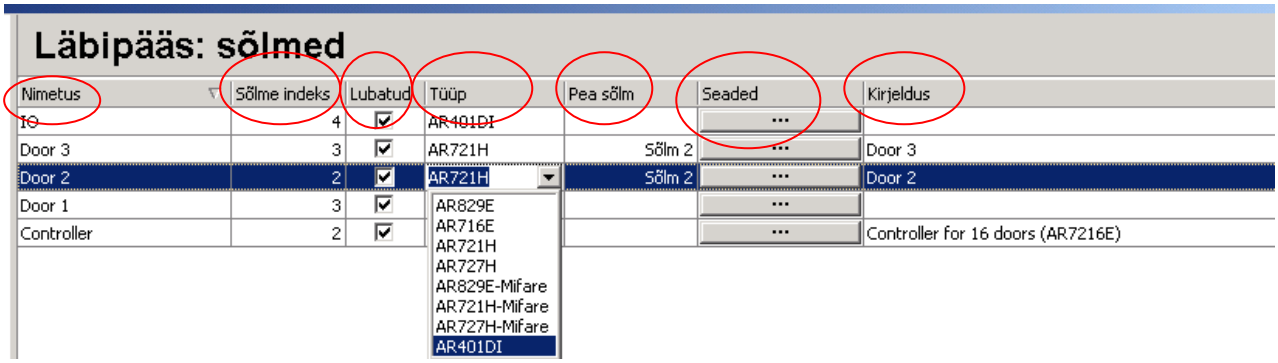
Re-initialize –required after adding or changing the modules/groups.

Picture 39 General settings for access system

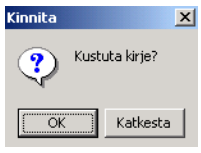
Nodes

The cardreaders, controllers and IO links (the input/output modules) existing in the system form the nodes of access system.





Picture 40 Table setting the nodes of access system



Insert button from keyboard – adds new row to make node

DEL button from keyboard – removes the selected row, asks before deleting.

Node index – the address of node

Enabled – node working or not

Type – choose type from options

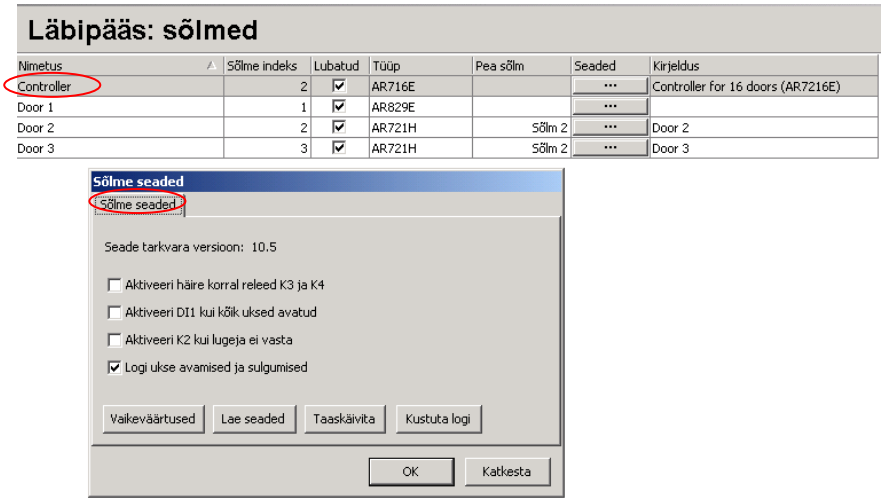
Master node – if there's subnode, it is possible to set its master node

Settings – the window for setting node opens. The options of settings are different, e.g controller, door or IO module

Description – node description in free form, default the same as the name

Node settings parametres

1. **Node settings window for the controller:**



Picture 41 Controller settings window

-Enable K3 and K4 relays on alarm,

-Enable DI1 when all doors open,

-Enable K2 when reader offline

-Log open and close events

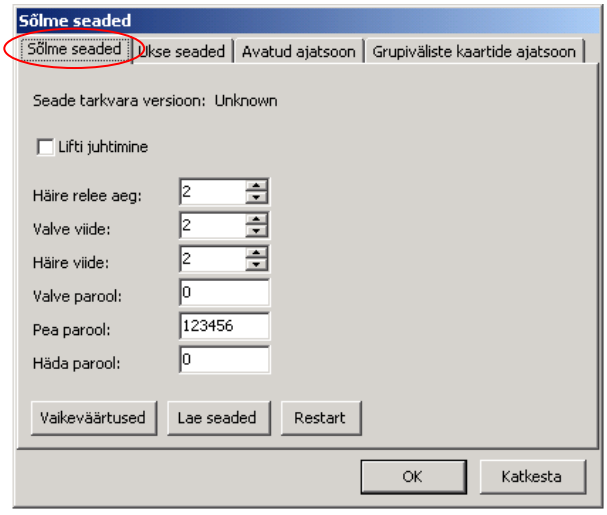
Default –default settings

Upload settings –load changes to controller(s)

Restart –restart after changing

Clear log – deletes log

2. **Node settings window for the door**



Picture 42 Door node settings window

Elevator control –the node is used to control elevator

Alarm relay time (in seconds) – the time the node output relay is active

Arming delay (in seconds) – the time after which alarm is transmitted

Arming password – if the password is needed to arm the device

Master password – the „installer code“ of node

Duress code –

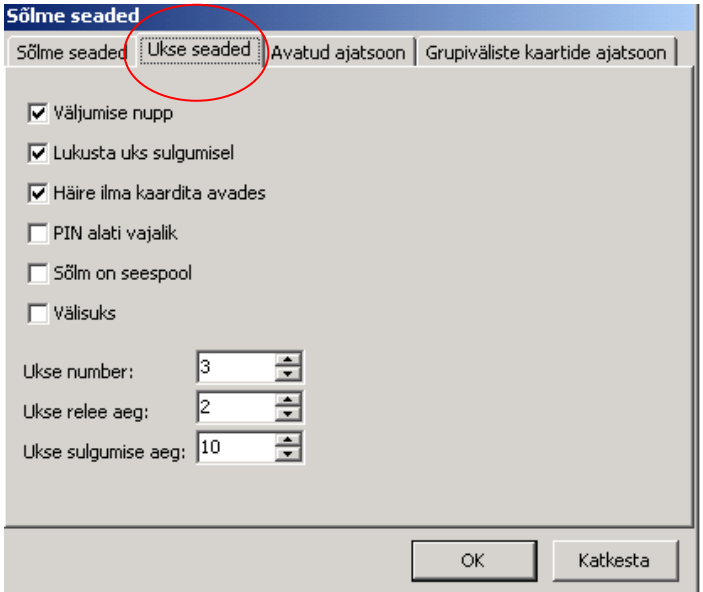
Default –

Upload settings –loading the changes

Restart – door controller restart

To save, click OK

The data and changes will not be saved, if you click Cancel



Picture 43 Door settings

Door settings

The following access system door parametres can be changed in the settings

Exit button – whether the button is used or not, when exiting

Lock door when closes – in this option, the system waits until the door magnet closes. If the option is not active, the door will be closed when the door relay time is up.

Alarm on force entry – if the option is active, then the system alarm is generated when the door was not opened using card (e.g evacuation „butterfly“ or key)

PIN code always required – in addition to card, PIN code is asked to allow access.

Door is inside – sets the direction for reader (in/out)

Exterior door – is used with reports. If it’s the exterior door, the entrys and exits on the object will be counted according to it.

Door number – door number in the system. When default, appears automatically.

Door relay time (in seconds) –after allowing access the door relay will be open

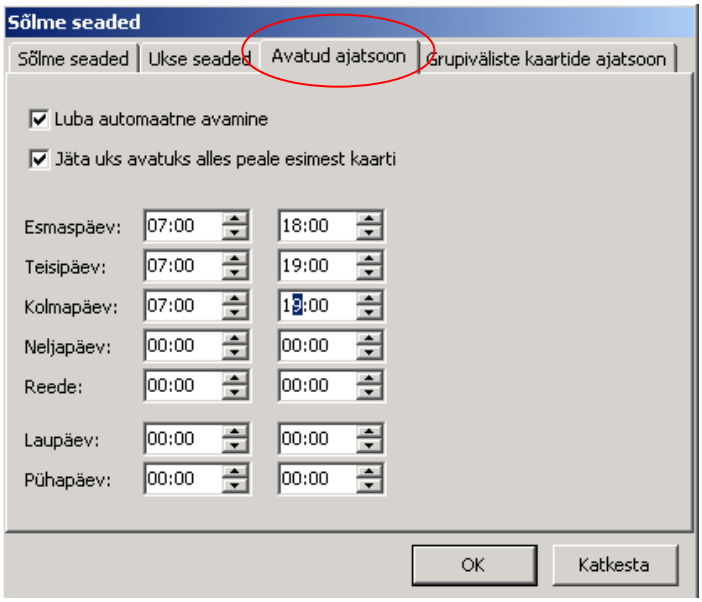
Door closing time (in seconds) –after this time, the „door unlocked“ alarm will be generated.

Open timezone settings

In the settings, you can set the time interval when the door is open. The time interval can be set in week days and by day and night time.

Enable auto open timezone – regardless of time intervals, this option must be active if we need to set the auto opening.

Keep closed until first valid card –in case the setting is active, the door stays open after the first accepted card. The setting considerably helps to reduce security risks.



Picture 44 Door timezone settings window

To save data, click OK. The data and changes will not be saved, if you click Cancel.

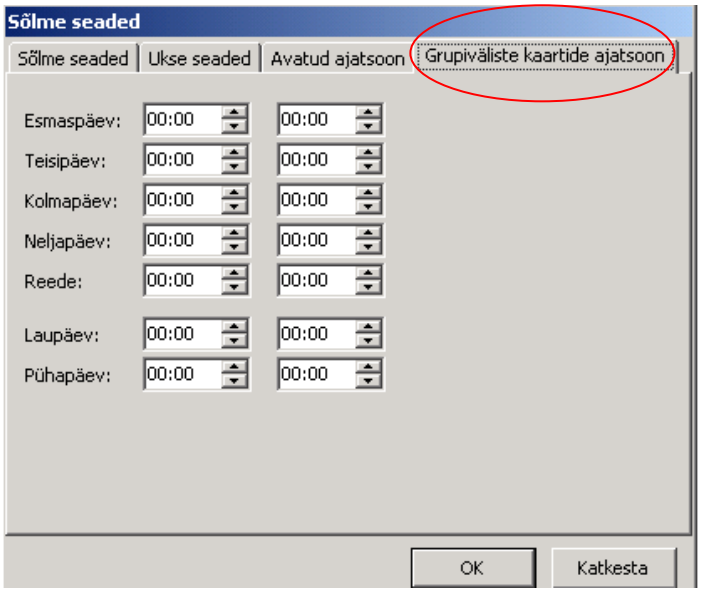
Group override card timezones

Applies to the cards added to single users.

Can set the time interval, when the door is opened. The time interval can be set in week days and by day and night time.

To save data, click OK

The data and changes will not be saved, if you click Cancel.



Picture 45 Group override card timezones

Holidays

The door auto open mode will not work on days in table (Holidays). Also, the group is inactive, if not set differently (delay – „is active on holidays too“). Holidays and shortened days can be set by time (when the doors open and close).

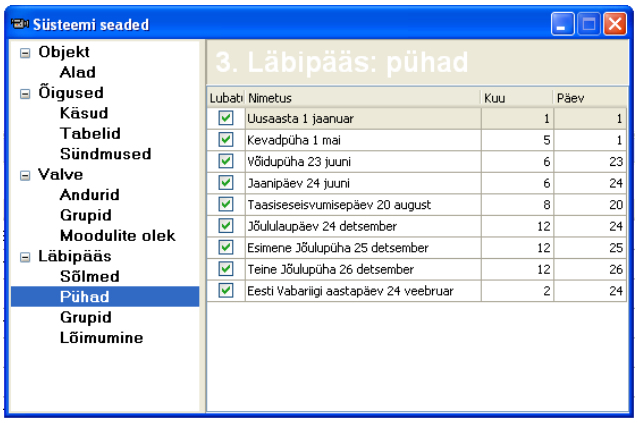
Insert button from keyboard -> new row is added, enter required data

Del button from keyboard-> delete the selected row

Name – name of holidays in free form

Month – month in numbers

Day – the date

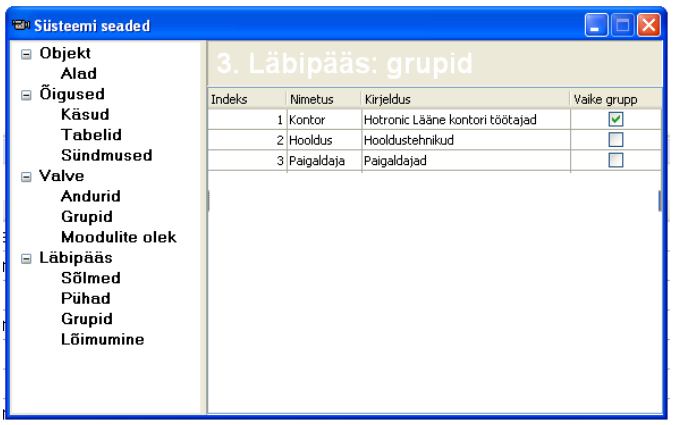


Picture 46 Holiday list table

Access groups

Picture 47 Access groups table

The system settings will be in the opening window. It’s possible to change the access groups (add, remove, group).



Insert button from keyboard ->add new row

Del – delete selected row

Index –appears automatically

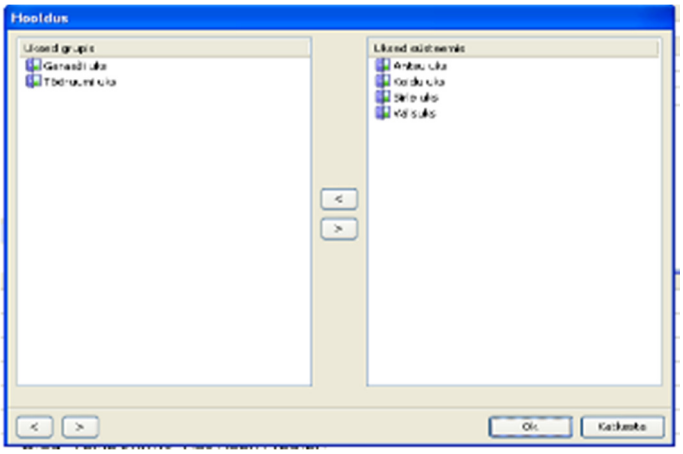
Name – name of the group

Description – group description in free form

To add doors in group, double-click on the name, will activate in the list (right box). Click -> necessary door.

(left arrow) <

(right arrow) >



Picture 48 Access groups settings table

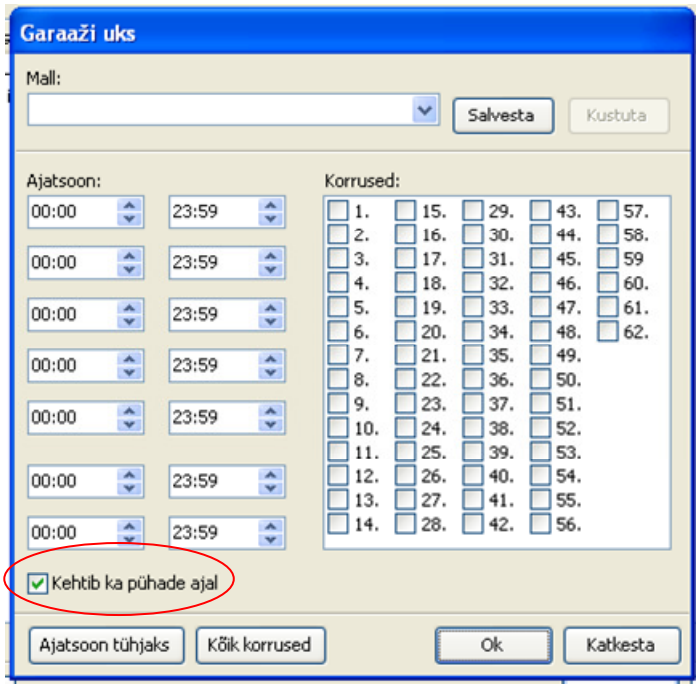
Picture 49 Time mode settings

You need to set timezone (time) to the doors in group, that is when door is accessible in certain group.

Double-click on the door in group->set door working time. Every day has its own start and end (7+7 time fields).

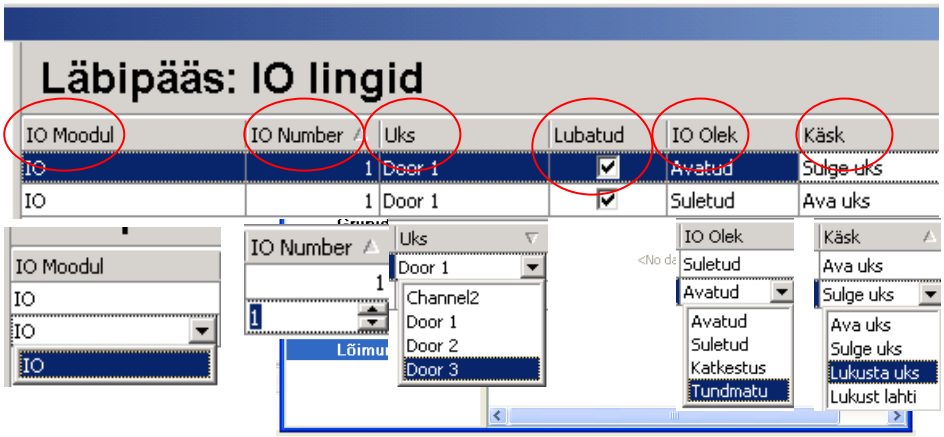
If the elevator has reader, then it's possible to set floor, where user can go.

To save, click OK.



IO links

Picture 50 IO input/output module settings



Integration

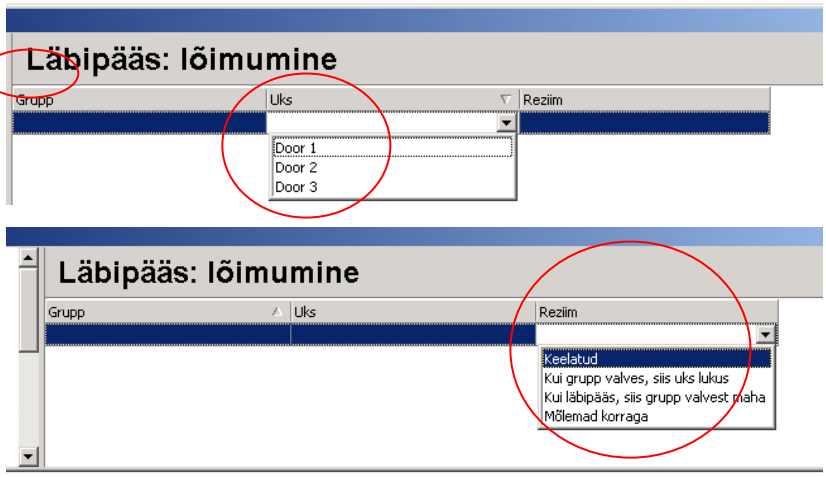
Enables to connect the security groups and access doors.

Insert from keyboard-> add a new row

Del –deletes selected row

In the options, doors in group and their modes are set:

-denied
-when group armed then door locked
-disarm group on door access
-both



Picture 51 Connecting access groups and security groups

Synchronization

HotSec management software enables to create time synchronization for the central devices connected to the system. It ensures the same time in system, while saving the events.

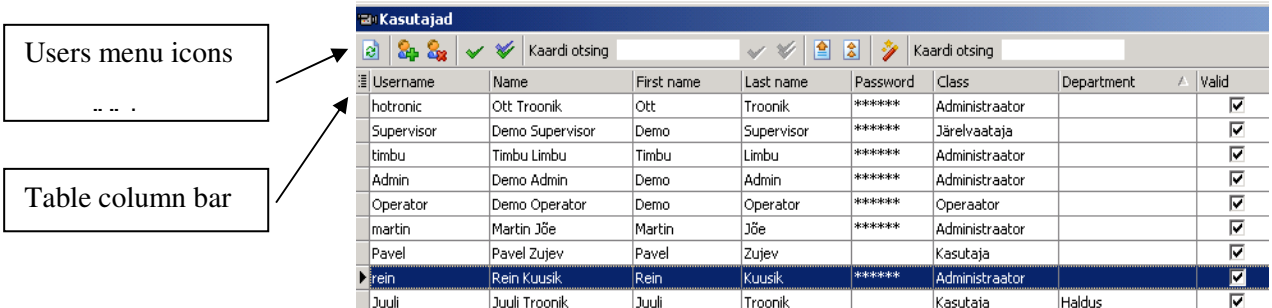
User management

All system user data (as well as program users and end users) can be looked, added and modified in the Users database.

General data of users table, checking and changing data

From the settings menubar, choose Object->Users or Quick launch icon

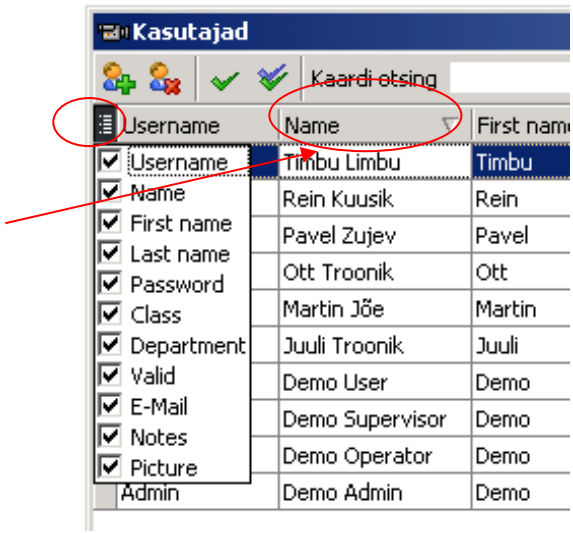
A window with all the users table in system will appear. General view of table or the number of columns displayed depends on the options in options window (see picture 52)



Picture 52View of users table

Each user can design the users table by ticking the necessary fields. To add and hide columns in the users table, choose by ticking. According to the tick, the columns will be added or hided.
On the column title field, it's possible to change the alphabetical order of counter's record with a double-click. To change column width, drag the separating line between the table with left mouse button.

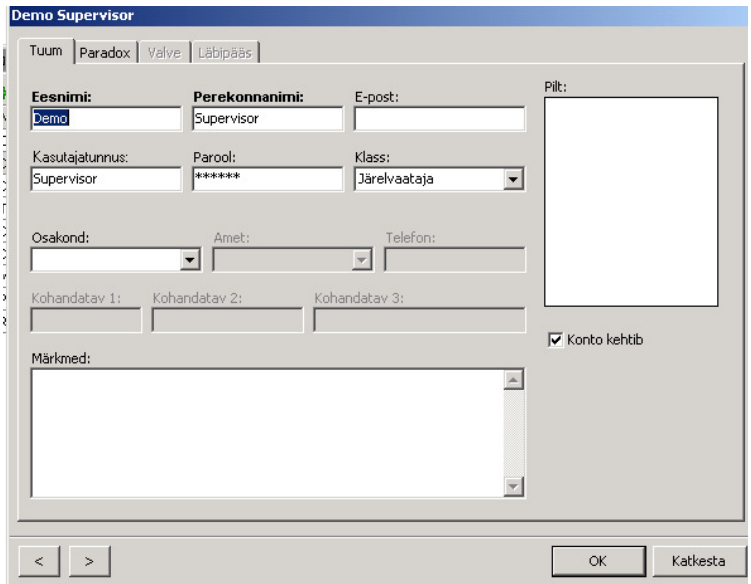
Use other sorters to find users and user data.



Picture 53 Designing the users table columns

1- add new user
2- delete selected user
3- delete the selected user account
4- upload all users to panels
5- find user by card number
6- upload selected user PIN code
7- upload all users PIN codes
8- upload selected user cards
9- upload all user cards
10- adding new cards
11- find users by card numbers

To check or change system users (selected option „CORE“) , double-click



on user data field and window with personal data opens. If necessary, the data can be fixed, modified or added.

After changing data, save by clicking OK.

Picture 54 User data card in „Core“ option

If it’s not necessary to save changes, click Cancel.

In the „Paradox“ option,

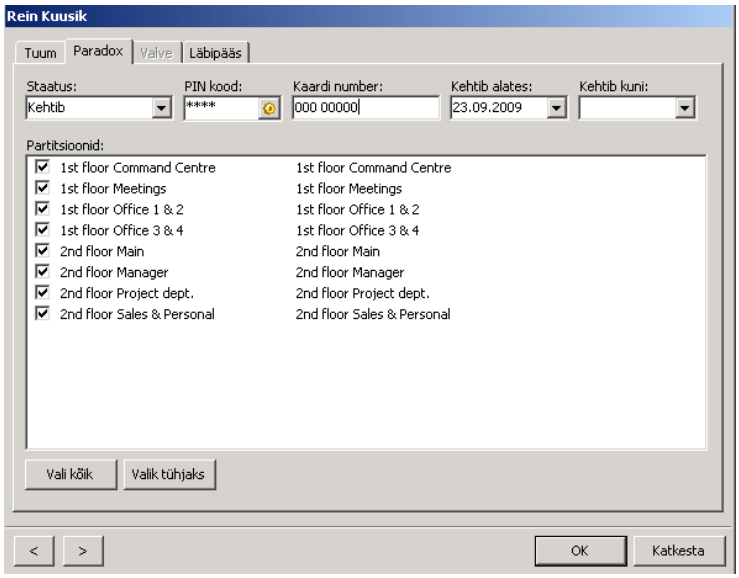
all user data is set:

card number, PIN code,

rights starting and expiring dates

and classes for using security system

(e.g allowed partitions).



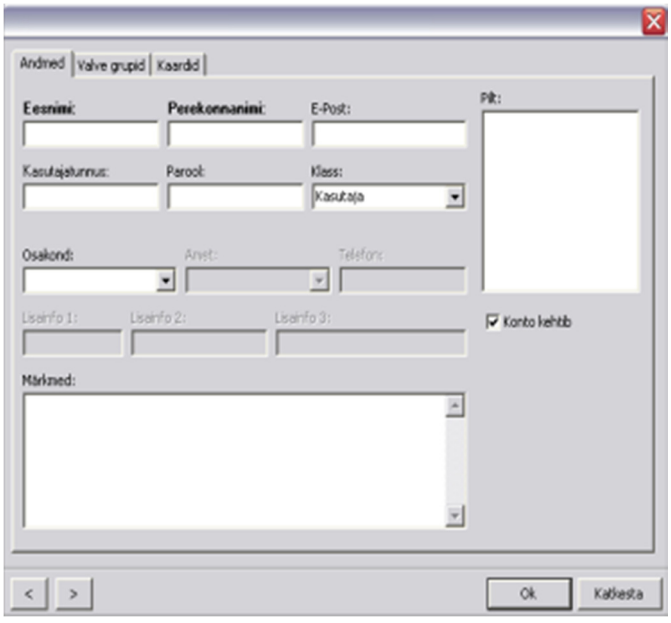
Picture 55 User data card in „Core“ option

Adding new user

Picture 56 User card

1. **Choose Add user**

In the opening window, enter the following data:

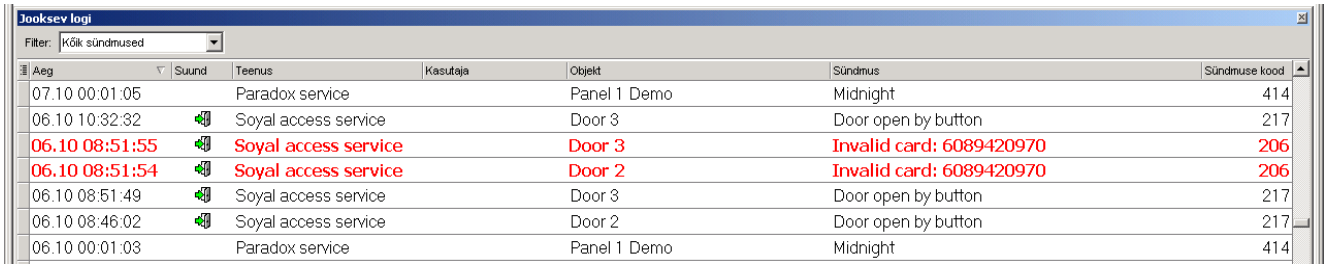


- first and last name (compulsory)
- user name and password. Are set for software users (not needed for end users).
- Class –choose from options, which privileges are allowed for software user
- Department (entering different departments will create a list. Later, when you set department for new
- workers, you don’t have to type it again,
- you can search with browser). Adding
- department is compulsory, it is necessary to give privileges and taking reports.
- photo (in the window, click with right mouse button,

upload picture e.g from staff database.

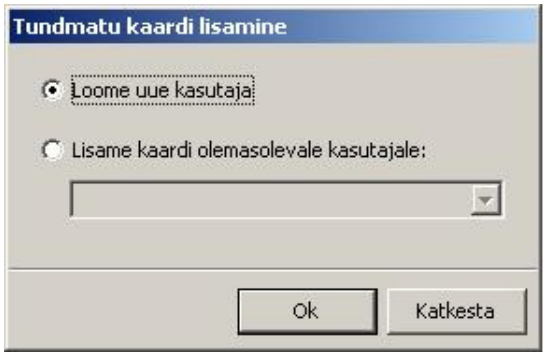
- set valid account (tick)

2. From activity log



Picture 57 New cards wizard from activity log

- Show new card to the reader
- Activity log will display a record „invalid card“ with number
- Click on the record, „new card from event“ window will appear
- The option „Create new user“ will open new
- users wizard, the card number is already defined.
- The option „Add card to an existing user“ enables to add new card to an existing user in system.



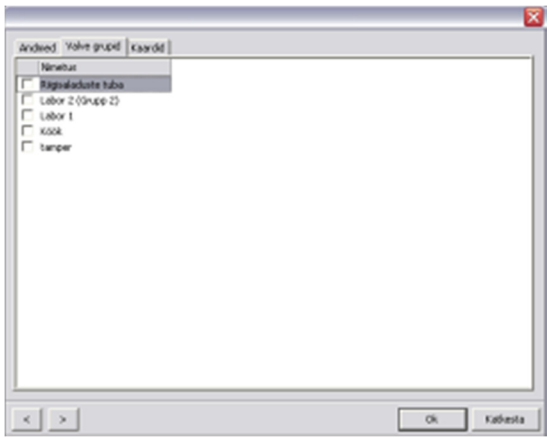
Picture 58 Adding new card to user

Security groups

Each user gets security group –user can arm and disarm the group (see also security groups)

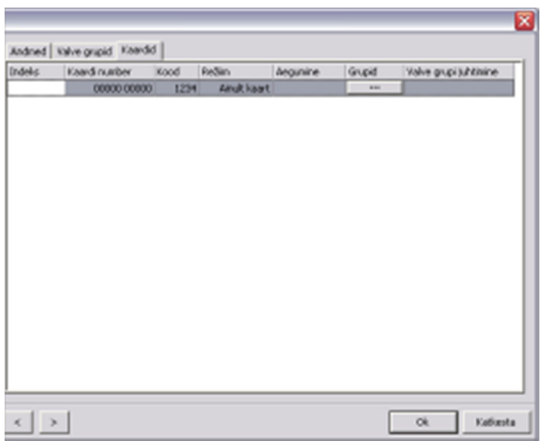
To add card data ->Insert from keyboard ->fields will activate

- index appears automatically
- card number



Picture 59 Security group settings

- code (according to selected mode). If new user has only card, the default code is 1234.
- User gets the code (or chooses it himself), if he uses card and PIN code to open doors.
- Under mode, set possible access variants (e.g card only, card and key)
- Expiration – set card expiration date by clicking on the expiration field; in the



calendar

- groups – set access zones by clicking the group field

(set what user can access)

security group control –if the system controls access

and security systems.

Use arrow keys to navigate between layers. Picture 60 Security group editor

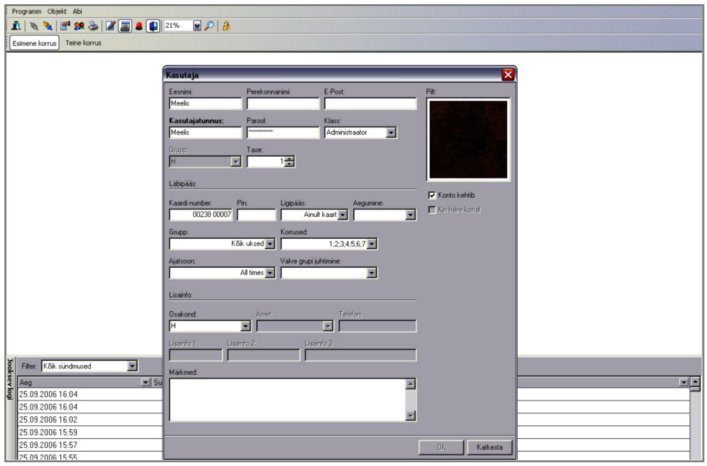
For precise identification in new user wizard, add user photo and e-mail address. If data saved, click

OK.

To delete user from list, activate user and

click 

Picture 61 User card view



Checking user info

It is possible to check user info in activity log, but not any changes.

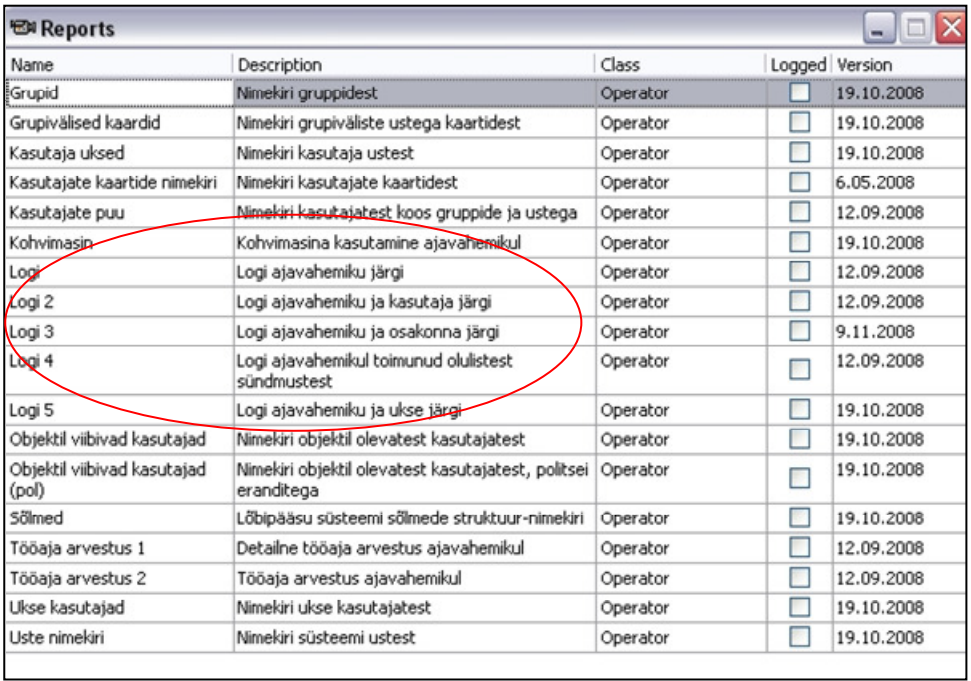
Double-click on the user name you want to check, „user window“ appears.

Reports

The „Reports“ submenu enables the user to get an overview of the system database configuration and the previous events.

Choose Object->Reports or Quick launch button

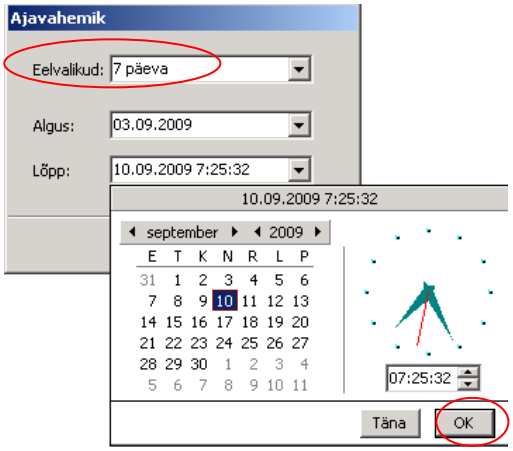
In the opening window (Picture 61), it’s possible to take reports from different actions, users, doors and events.



The forms of reports are previously defined and can be changed or added, if necesssary.

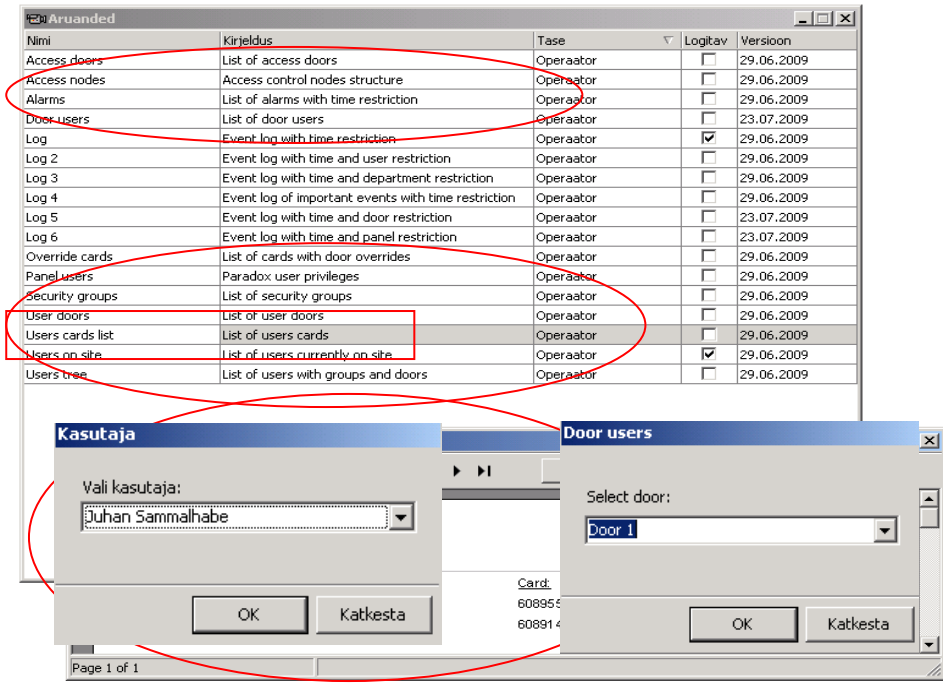
Double-click on field,
set timespan
according to window,
and choose door.
The actions report
will be displayed after
saving the data. It is
possible to print
the report or save as pdf.

To set timespan to events, double-click on field. Choose between existing options (e.g today, the day before, 7 days, 30 days etc) or set timespan with free option.



Picture 63 Setting timespan for creating report

To set the required option in system configuration and in user classes reports (e.g card users), double-click on field.



Picture 64 User card report and example of option

Report will be created according to user; next report after door option.

Picture 66 Setting options while creating reports

The Events window will show the events report in real time. The number of events (previously set) is displayed here.

It is recommended to remove all filters (filter settings are „All events“) when toggling events in activity log. It ensures that all events are transmitted to activity log (possibility that operative info is hided, will be excluded).

User manual extra

Quick manual for operator (operator class)

Integrated security and access system

User manual for HotSec operator

v.1.0

Operator who logs in to HotSec management program, can monitor and control the objects in system, according to his previously set user level (class).

User manual for operator contains short instructions to use management program.

Opening the management program

→ On the operator desktop, click the management program icon

Login
Authenticating the user
Changing password

→ 
In the window, enter:
User name: ……..
Password: …….
Click OK
Program opens

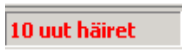
↓

Changing password -

Checking alarms

When program opens, the alarm window with unaccepted list of alarms will be displayed on desktop.

→ 1.Check alarm events in the window.
2. Checking alarm events
Variant. 1 Click on message row



Or

Var. 2 Click on the Quick launch icon 
To close window, click Close

Accepting alarms

→ From the list, choose unaccepted alarm event (red), click on event row,
Click Accept selected
Type the alarm cause on text field
Click OK
To hide accepted alarms, click √. The accepted alarms will be hided

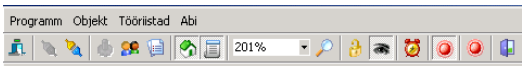
Transmitting alarms

Act according to job

→ 1.Give the car patrol object address and alarm data.
2. Inform the contacts

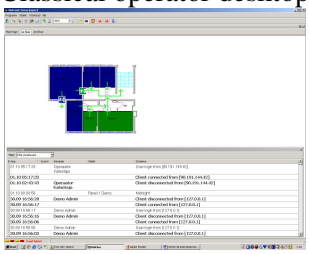
Actions allowed for operator class

Admin user sets operator rights to use th management program.
If action is allowed, Quick launch icons an settings menu bar are active.
If action is denied, the icons and menu bar are hided (with gray background, not active)



Working with management program

Classical operator desktop, actions



1. Monitoring object statuses on object maps.
2. Monitoring alarm events in real time.
3. Arming and disarming objects.
4. Checking end users

Reports

1.Click on Quick Launch icon to check reports 
2. Select the type of required report.
3. If necessary, enter time or events filters.
4.Print report.
5. Or save in computer.

Closing the program

To close programs, click shortcut keys