User Manual

Table of contents

Copyright notice

Liability waiver

Introduction

SimpleID in an innovative access control software that supports HID Edge IP readers/controllers and VertX IP controllers, Mercury IP readers/controllers and also Suprema's IP fingerprint readers.

SimpleID has been designed with the goal of providing a simple and at the same time highly effective interface to enable users of all level to have a complete control over the system.

SimpleID is made and supported by UAB Midpoint Security located in Kaunas, Lithuania (EU).

For more product information and support, please visit our web site www.midpoint-security.com.

Overview

SimpleID software consists of 3 components:

1.   SID Controller Communication Service
2.   SID Graphical User Interface
3.   Web Interface

SID Controller Communication Service is used to communicate with hardware devices such as HID VertX controllers and Edge readers. It sends configuration, cards and commands, and receives events from hardware devices. There are no user adjustable settings in this program. It will start automatically every time your PC boots up. If you wish to verify whether SID Controller communication Service is functioning, you may do so by viewing Windows Task Manager and checking if SIDController.exe process is running.

SID Controller Communication Service should be installed on only one computer. This computer should be always powered on.

SID GUI is a Graphical User Interface which is used to configure communication settings, users, cards, doors, access groups, time schedules etc. It also has Monitoring feature, which is used for live monitoring of system events. Below is the main menu of the SimpleID software:

The main menu consists of 16 default tabs and an information panel. The tabs switch the inner windows. Almost all inner windows consist of 2 different panels:

- **List panel:** displays a list of configuration objects, such as doors, time schedules, users, etc. You can search, select, add new or delete selected items.
- **Details panel:** displays and allows to modify settings of a selected item.

List panel   **Details panel**
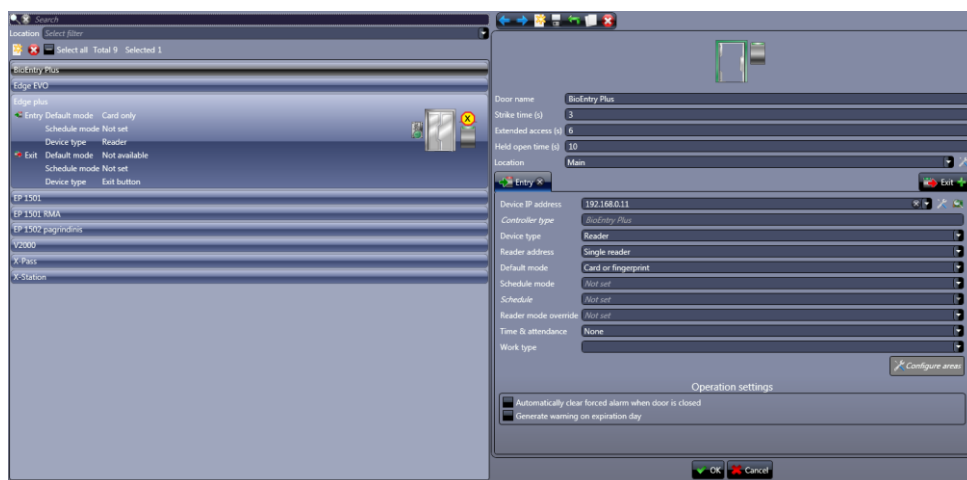
Web Interface is a Graphical User Interface which is still under development.

General information

General list controls
Mouse Click: you can select an individual item in the list by clicking on it with a mouse button. With simple mouse button click you can select only one item at a time.
Hold CTRL+Click: this combination allows you to add or remove a single item from the selection.
Hold SHIFT+Click: while holding the SHIFT key you can press on several items. The first item you clicked on will be the starting element of the selection and the last item you click on will be the ending element of the selection. If you release SHIFT button and then start holding it again the starting element of the selection will change to the next item you click on (each SHIFT key release will reset the starting element of the selection). This selection mode will deselect all other items, which will not belong to the range.
Hold CTRL&SHIFT+Click: this selection mode works the same as "**Hold SHIFT+Click**", but it will not deselect already selected items which do not belong in the range.
INSERT Key: when the list has focus clicking this button will insert a new item to the list.
DELETE Key: when there are selected items in the focused list, pressing this key will delete (or deactivate) all selected items at once (can be 1 or more items).

 Settings

Language group
Language: SID supports user interface localization. Translation is performed "on the fly", directly in the GUI. Some settings can not be translated while the system is running, so after changing the language it is recommended to restart SimpleID GUI.
Service language: language of Access Control system service.
Export: exports the data for translation to other languages. Supported formats include MS Excel and CSV (comma separated values).
Import: imports translation data from the specified file. Supported formats include MS Excel and CSV (comma separated values).
Select encoding: the text encoding to use for exported file.

Miscellaneous group

Ask for confirmation before exiting: select if you want to see a confirmation dialog when closing SimpleID GUI.
Offline event age: these events will not be shown on the map, only will be visible in the event list.
Modules: opens the Modules window.
Card reader settings: opens the Card reader settings window.
Regional settings: opens the Regional settings window.
Expand records on mouse-over delay (ms): indicates precise time interval (ms) after which list items expand.

Backup group

	Backup	
Database location	.\SQLEXPRESS\SIDDB	
Backup folder	C:\BackupGeraBaze	
Photo folder	Saved on machine: 172.16.0.123	C:\ProgramData\Access Control System\DBFileStreamData\Photos
Backup interval (days)	14	
Last backup time	2014-02-21 11:36:43	
Delete events older than (days)	365	
Last events purge	2013-09-26 13:44:31	
Delete inactive users older than (days)	365	
Date of the last purge of inactive users	2014-02-27 10:12:18	
Delete inactive cards older than (days)	365	
Date of the last purge of inactive cards	2014-02-27 09:22:36	
Disable users access levels with no access events after (days)	0	
Date of last action	1753-01-01 00:00:00	
Disable user after all access levels expiration (days)	0	
Date of last action	1753-01-01 00:00:00	
Disable user after it's expiration (days)	0	
Date of last action	1753-01-01 00:00:00	
Delete deactivated users after (days)	0	
Date of last action	1753-01-01 00:00:00	
Delete event photo after (days)	31	
Date of last action	2014-02-27 09:22:36	
Purge current events older than (days)	7	
Purge current events at	00 : 00	
Date of last action	1753-01-01 00:00:00	

Database version: 456   System ID: 17136

[Backup now] [Restore] [Create new] [Clean up DB now] [Delete all history]

Database location: the path to the database in the MS SQL Server. Press the "..." button to open database connection configuration window.

Backup folder: the folder on the server computer, in which the backup files are saved. Press the "..." button to browse for a backup folder. Make sure this folder exists on the server computer!

Photo folder: the folder on the computer, where service is running, in which photos are saved. Press the „..." button to browse for a photo folder. Make sure this folder exist on the computer, where service is running.

Backup interval (days): the interval in days between each backup procedure.

Last backup time: the date when the last backup was performed.

Delete events older than (days): during the backup procedure, events older than the specified number of days will be automatically deleted. Enter '0' to disable this feature.

Last events purge: the date when the last events purging was done.
Delete inactive users older than (days): Users which have not used their identifications for the specified amount of days, will be deactivated automatically. Enter '0' to disable this feature.
Date of the last purge of inactive users: the date when the last purging of inactive users was done.
Delete inactive cards older than (days): Identifications which were not used for the specified amount of days, will be deleted automatically. Enter '0' to disable this feature.
Date of the last purge of inactive cards: the date when the last purging of inactive cards was done.
Disable users access levels with no access events after (days): Disable user access levels with no access events after (days). Enter '0' to disable this feature.
Date of last action: the date when the last action was done (Disable users access levels with no access events after (days)).
Disable user after all access levels expiration (days): Disable user after (days) when his access levels expire. Enter '0' to disable this feature.
Date of last action: the date when the last action was done (Disable user after all access levels expiration (days)).
Disable user after it's expiration (days): disables user after it's expiration reach specified amount of days. Enter '0' to disable this feature.
Date of last action:
Delete deactivated users after (days): Delete inactive users from the database after a specified amount of days. Enter '0' to disable this feature.
Date of last action: the date when the last action was done (Delete deactivated users after (days)).
Delete event photo after (days): deletes event photo after specified amount of days. Enter '0' to disable this feature.
Date of last action: shows the date of last action taken (delete event photo after (days)).
Purge current events older than (days): This function is not used.
Purge current events at: the time the purging must begin.
Date of last action: the date when the last action was done (Purge current events older than (days)).
Database version: the number of the current database version used for technical support.
System ID: the unique number of this system.
Backup now: perform a backup of the database instantly.
Restore: perform a database restore from a selected backup file (can only be done from the workstation which is running the database server).
Create new: create a new database structure (wipe all user-created data from current database, a new System ID will be generated).
Clean up DB now: delete old event photos, events older than time established, controller comands, expired user cards, purge inactive users, inactive cards, disable expired user access levels, users with expired access levels, expired users, deletes deactivated users.
Delete all history: delete old event photos, events older than time established, controller comands, expired user cards, purge inactive users, inactive cards, disable expired user access levels, users with expired access levels, expired users, deletes deactivated users.

Data Import/Export group

Data Import/Export
Import data Export

Import data: imports user data from a CSV (comma separated value) or Excel files.
Export: exports user data to a CSV or Excel file.

TA schedule Import/Export group

TA schedule Import/Export
Import data Export

Import data: TA schedules automatic import.

Sounds group

Sounds	
Unacknowledged event	**Acknowledged**
Sound	Sound
Playback repeat 1 time only	Playback repeat 1 time only
Event repeat each	Event repeat each
Acknowledge automatically	Close automatically

Playback repeat: playback repeat specified time set.
Event repeat each: event repeat each time interval you choose.

Unacknowledged event	Acknowledged
Sound: the sound file to be played when there is a new event matching one of the user-defined event filters.	**Sound:** the sound file to be played when there are acknowledged but not closed events.
Acknowledge automatically: specify if the events should be acknowledged automatically.	**Close automatically:** specify if the events should be closed automatically.

System group

System

| Upload data to all controllers | ✓ Automatic upload | ☐ Wait for Door Open event when counting users |
| Submit logs | Show GUI logs | Show service logs | Cancel auto reports |

Upload data to all controllers: uploads all configuration data to all controllers.	
Automatic upload: once you change anything in the configuration, these changes will be uploaded to the controllers.	
Wait for Door Open event when counting users: users, whose scans their card, but does not open the door are not counted.	
Submit logs: Allows you to archive and save application log files to the local computer or submit them to your support representative via e-mail.	
Show GUI logs: opens the SimpleID GUI log file storage folder on the local computer.	
Show service logs: opens the SimpleID Controller Configuration Service log file storage folder if it is installed on the local computer.	
Cancel auto reports: cancel auto reports generation.	

Card reader settings window

Card reader settings

☐ Is active

Type	StrongLink
COM port	COM1
Baud rate	19200

✔ OK   ✖ Cancel

Is active: Enables the configuration of the card scanner.
Type: device type.
COM Port: The COM port number where the card scanner is connected (for USB connected devices the COM port number usually starts from 5).
Baud rate: The speed of the communication line (bits per second).

Regional settings window

Regional settings

Calendar type | Gregorian

Weekend days
- ☐ Monday
- ☐ Tuesday
- ☐ Wednesday
- ☐ Thursday
- ☐ Friday
- ☑ Saturday
- ☑ Sunday

✔ OK   ✖ Cancel
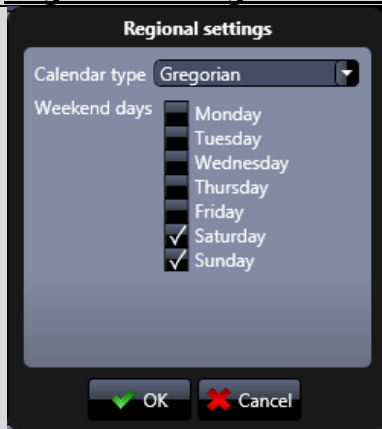
Calendar type: Option between two calendar's types Persian and Gregorian.

Weekend days: Marked checkboxes shows weekend days.

Modules window

Modules

🔍 ✖ Search

☐ Select all Total 7 Selected 1

Elevators
Intruder detection
Notifications
SimpleLogon
Weight control
Weight detection
Occupancy

☐ Enabled

✔ OK   ✖ Cancel

Modules window: Elevators

☑ Enabled

Enabled: if checked, enables the usage of this module.
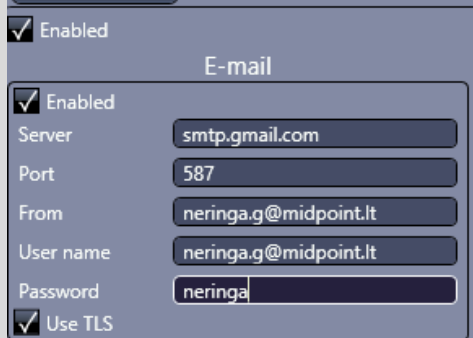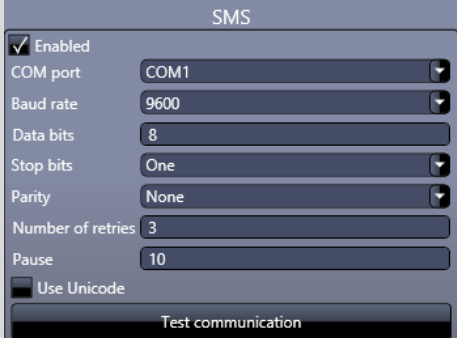
Modules window: Intruder detection
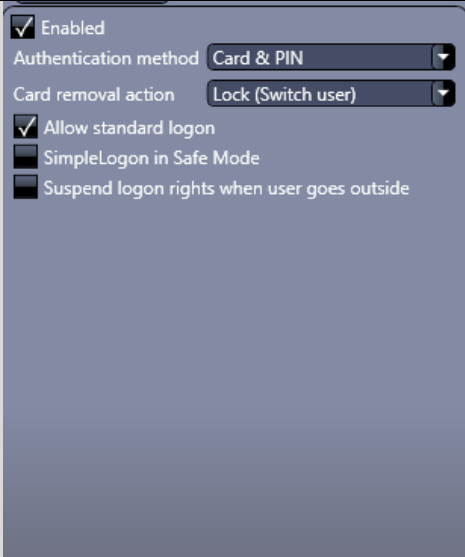
Enabled: if checked, enables the usage of this module.	
Hide logon dialog (stealth mode): hides logon dialog.	

Modules window: Notifications

E-mail	**SMS**
Enabled: Enables usage of e-mail sending function.	**Enabled:** Enables usage of SMS sending function.
Server: server address.	**COM port:** serial port number to be used.
Port: server port.	**Baud rate:** serial port communication speed in bits per second.
From: notification sender.	**Data bits:** serial port communication line data packet size.
User name: email address.	**Stop bits:** serial port communication line empty packet size.
Password: password of email written in username field.	**Parity:** serial port communication setting.
Use TLS: this checkbox enables use of TLS. TLS (Transport Layer Security) is cryptographic protocol, designed to provide communication security over the Internet.	**Number of retries:** serial port communication setting.
	Pause: serial port communication setting.
	Use Unicode: enables encoding of most languages, which hasn't symbols from Latin alphabet.
	Test communication: test if data entered provides communication.

Modules window: Simple Logon

| ☑ Enabled |
| Authentication method Card & PIN |
| Card removal action Lock (Switch user) |
| ☑ Allow standard logon |
| ☐ SimpleLogon in Safe Mode |
| ☐ Suspend logon rights when user goes outside |

Enabled: if checked, enables the usage of this module.

Authentication method: for example Card & PIN.

Card removal action: actions preferred after removing card from reader: none (no actions are taken), lock (Switch user), log off, shut down.

Allow standard logon: allows standard logon to computer.

Simple Logon in Safe Mode: runs Simple logon in Safe Mode.

Suspend logon rights when user goes outside: When user leaves his work place his PC is automatically locked and no one can log in until user comes back to his workplace.

Modules window: Weight control

| ☑ Enabled |
| ☐ Replace the following weight groups after first use |
| ➕ Add |

Enabled: if checked, enables the usage of this module.

Replace the following weight groups after first use: After first access replace weight groups with new ones.

Add: Select access levels
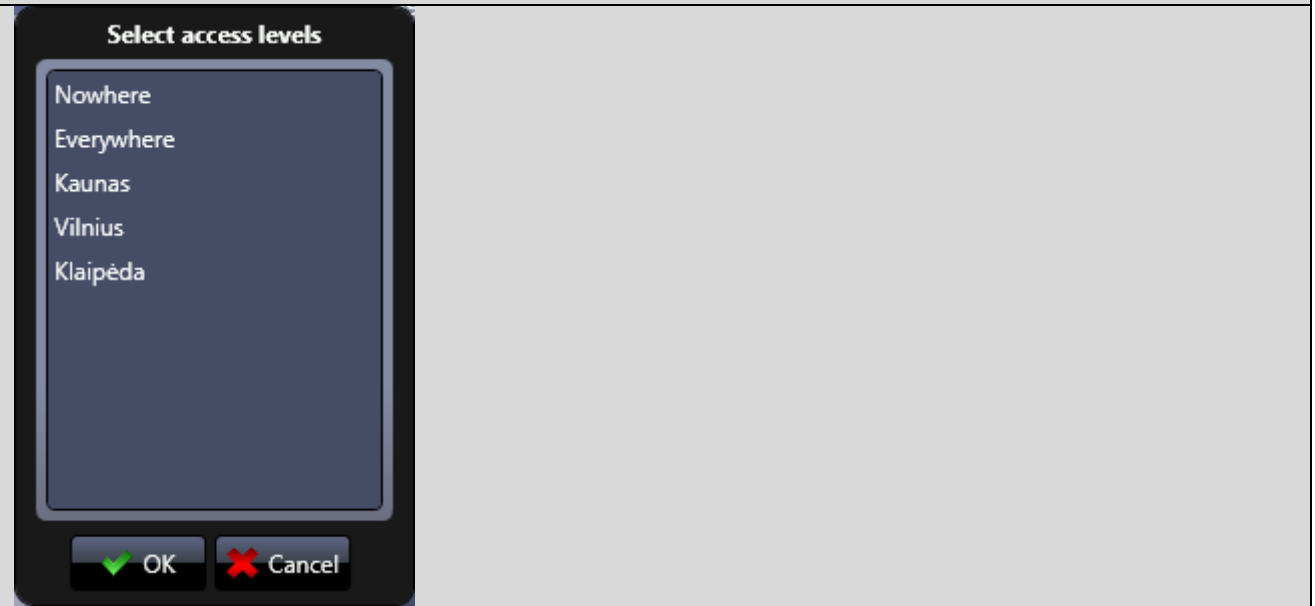
Modules window: Weight detection

☑ Enabled

Enabled: if checked, enables the usage of this module.

Modules window: Occupancy

☑ Enabled	
⊙ Serial port ◯ LAN	
Encoding	Baltic (Windows) ▾
Department display time (s)	10
Display user name (s)	2
COM port	COM1 ▾
Baud rate	9600 ▾
Data bits	8
Stop bits	One ▾
Parity	None ▾
Number of retries	3
Pause	10
Hours to analyze	24

Enabled: if checked, enables the usage of this module.

Serial port/LAN: Select the connection type of the occupancy device.

Encoding: Encoding of the messages transmitted to device.

Department display time (s): time limit in seconds for how long the department should be shown.

Display user name (s): time limit in seconds for how long the users name should be shown.

COM port: serial port number to be used.

Baud rate: serial port communication speed in bits per second.

Data bits: serial port communication line data packet size.

Stop bits: serial port communication line empty packet size.

Parity: serial port communication setting.

Number of retries: number of retries to restore communication with device.

Pause: serial port communication setting.

Hours to analyze: event history should only be checked for the time period (hours) entered here.

Real time connection to Access Control Service

Real time connection to Access Control Service
ACS host	172.16.0.123
Port	8523
Name	EventService
API Service Name	SID
API Service Port	8080
Test connection (green = OK, red = Error)

ACS host: the name or IP address of the computer which is running the Access Control System service.
Port: Event service port.
Name: Event service name.
API Service Name: the subdirectory name which will be used to form the address of the API Service.
API Service Port: TCP protocol port number to run the API Service (default 8080 or 58008).
Test connection: Test button to see if connection settings are correct.

Automatic reports

Automatic reports
☑ Leave last [3] history entries undeleted
☐ Delete asociated report files
Clear history

Leave last (number) history entries undeleted: leave last specified amount of automatic reports undeleted.
Delete associated report files: marked checkbox enables this feature.
Clear history: clears history of automatic reports.

TA schedule Import
Activate automatic imports: this checkbox activates automatic schedules import.
Directory name for import: the folder on the computer, in which imports are saved. Press the „...“ button to browse for a folder.
File mask: file extension.
Backup directory name: directory to which the schedules are copied after import.
Directory scan interval (seconds): import directory will be scanned every x seconds.
Import logs count: number of import logs to save.
Preview automatic import logs: preview of automatic import logs.
Delete logs: delete automatic import logs.

Users import from Directory Service

Data import

Source: Active Directory ▼

Connection

LDAP Connection string	LDAP://172.16.0.213/cn=users,dc=rebeladmin,dc=com
User name	Administrator
Password	***********
Reenter password	***********

TEST

Primary key

First and family name ▼

Duplicate record treatment		Automatic import @params	
User data:	Overwrite ▼	Activate automatic imports ☐	
Deactivate AD user	Deactivate ▼	Directory scan interval (seconds)	300
Deactivated access control user	Activate and updat ▼	Import logs count	10
		Preview automatic import logs	Delete logs

Data binding

Auto Reset

Preview

givenname	samaccountname	cn	pwdlastset	whencreated	badpwdcount	displayname	
Unbound ▼	Unbound ▼	Unbound ▼	Unbound ▼	Unbound ▼	Unbound ▼	Unbound ▼	
Jonas	Users\Jonas	Jonas Jonaitis	130397086210230000	2014-03-19 13:17:00	0	Jonas Jonaitis	0
Sima	Users\Sima	Sima Simaityte	0	2014-03-19 13:27:23	0	Sima Simaityte	0
Antanas	Users\Antanas	Antanas Antanaitis	130397092756167500	2014-03-19 13:27:55	0	Antanas Antanaitis	0
Ignas	Users\Ignas	Ignas Ignasijus	0	2014-03-19 13:28:34	0	Ignas Ignasijus	0

Import 💾 Save ✖ Close

DAP Connection string: LDAP is the provider, domain.com – server name specified as a DNS host name, CN=Users (CN – Common Name), DC (Domain Component), for example ("dc=domain" and "dc=com") full DNS name of the domain.

User name: connection to server user name, for example: "Administrator".

Password: enter password in this field (and repeat it in "Reenter password"), for example: "Midpoint1".

Test: Test connection.
Primary key: The primary key for characteristics that cannot be duplicated.
Duplicate record treatment: actions would be taken for duplicated users.
Preview: Preview for bound data.
Import: import data from AD (active directory).

Data import window

Character set: the encoding of selected file.
Has header row: this should be checked if the file has a row with captions of the fields and this row will not be imported.
Table/Sheet: if selected file is in Ms Excel and has several worksheets, here you can select which one to use.
Start from row: allows you to select the first row to start importing from (skip importing of preceding rows).
Duplicate record treatment: allows you to select what to do in each case of detected duplicate data.
Primary key: field values to be checked against the current database (for duplicate records).
Data binding: shows which field of SimpleID to use when inserting data of the selected column in „**Preview**" table.
Preview: this table shows a preview of the data in the file being imported and also allows you to select any data column (to be bound to a SimpleID field).

Data export window

Export

☑ Export header row

Field options

Character set	Unicode (UTF-8)
Field delimiter	; - Semicolon
Text delimiter	" - Double quote

Data options

Data to export: Users

Available fields	Exported fields
	First name
	Middle name
	Family name
	Employee number
	Phone
	Secondary phone
	E-mail
	Messenger
	User name
	Password
	User type
	Activation
	Expiration
	Additional field #1:
	Additional field #2:

✔ OK   ✖ Cancel

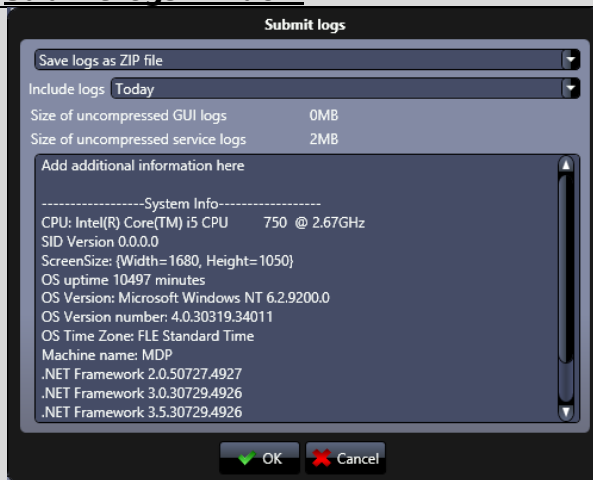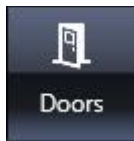|	
Export header row: the exported file will contain a header row with field captions.	
Character set: file encoding to be used.	
Field delimiter: different fields will be separated by this character.	
Text delimiter: text strings will be enclosed by this character.	
Data to export: type of data you would like to export.	
Available fields: fields which will not be exported.	
Exported fields: fields which will be exported.	

Submit logs window

```
                    Submit logs
Save logs as ZIP file                              ▼
Include logs  Today                                ▼
Size of uncompressed GUI logs        0MB
Size of uncompressed service logs    2MB

Add additional information here                    ▲

------------------System Info------------------
CPU: Intel(R) Core(TM) i5 CPU      750 @ 2.67GHz
SID Version 0.0.0.0
ScreenSize: {Width=1680, Height=1050}
OS uptime 10497 minutes
OS Version: Microsoft Windows NT 6.2.9200.0
OS Version number: 4.0.30319.34011
OS Time Zone: FLE Standard Time
Machine name: MDP
.NET Framework 2.0.50727.4927
.NET Framework 3.0.30729.4926
.NET Framework 3.5.30729.4926                      ▼

              ✔ OK    ✖ Cancel
```

In this window you can select whether you want to save the archived communication log files to your PC or send them to your support representative. You can also select the age of the log files to submit and enter some additional information.
Use this feature in case you encounter any problems with the software.

Doors tab

Door details panel	
Door name: specifies name of the door (can be associated with something to make it clear, when there are many doors).	
Strike time (s): indicates for how long the door lock must remain unlocked after the access granted decision.	
Extended access (s): indicates how much time (s) relay will be activated; will work for users, which in user configuration have "extended access" checkbox marked.	
Held open time (s): indicates the time given for closing the door. If the door is not closed within this time period, "Held open" alarm shall be generated.	
Location: Set door location, it can be building, city, company subdivision etc.	
Device IP address: indicates controller IP address.	
Controller type: indicates the type of the controller selected in the 'Device IP address' field.	
Device type: indicates the type of the reader (card reader, fingerprint reader or exit button).	

Reader address: indicates which reader to use if the controller has more than 1 reader attached to it (only available for VertX controllers: left reader or right reader).
Default mode: selects default reader mode (what type of credentials must be presented in order to unlock the door: card only, card or PIN, card & PIN, fingerprint only, card or fingerprint, card and fingerprint, PIN or fingerprint, PIN and fingerprint). Available options depend on which type of a controller is selected in Device IP/MAC address fields.

Keypad format: indicates which keypad format to use for the controller selected in the IP/MAC address fields. It is only visible for readers that are set to "Card & PIN", "Card or PIN" or "PIN only" mode.
Schedule mode: Select a mode you want this reader to switch to during the selected schedule.
Schedule: Select a schedule during which the reader will change its mode to the one specified in '**Schedule mode**' field.
Reader mode override: this is the mode set by the operator and will be valid until the operator clears it.
Time & Attendance: specifies if this door is used as clock in/clock out reader for Time & Attendance calculations.
Work type: Used in T&A report, when user can have different paid positions at different time.

<u>**Door details panel: Operation settings**</u>   Operation settings   ☐ Automatically clear forced alarm when door is closed   ☐ Turn on beeper and LED if exit button is pressed   ☐ Disable forced open alarm   ☐ Disable held open alarm   ☐ Generate warning on expiration day   ☐ Entry & exit controlled separately (i.e. turnstile)
Automatically clear forced alarm when door is closed: marked checkbox enables this feature.
Turn on beeper and LED if exit button is pressed: turns on beeper and LED if exit button is pressed. Marked checkbox enables this feature.
Disable forced open alarm: marked checkbox enables this feature.
Disable held open alarm: marked checkbox enables this feature.
Generate warning on expiration day: marked checkbox enables this feature.
Entry & exit controlled separately (i.e. turnstile): marked checkbox enables this feature.

Door details panel: Location
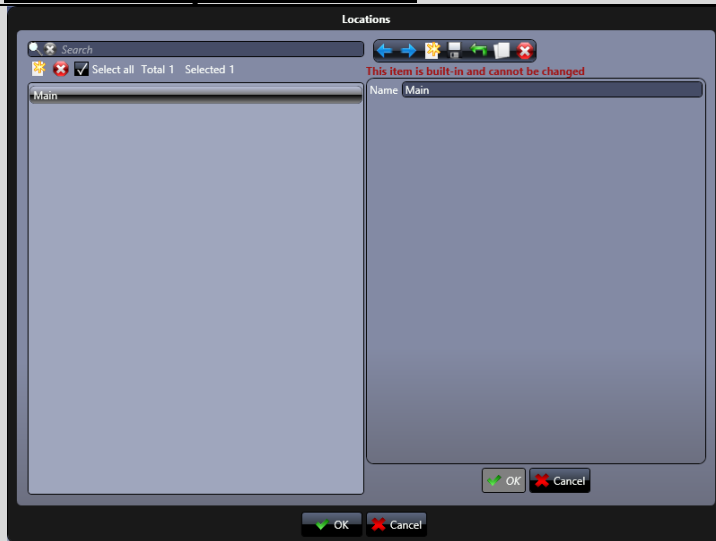
Name: specifies the name of the newly created location.

Door details panel: Device settings (Suprema devices)

	Controller type: the list of different manufacturer's controllers.
	Firmware version: device firmware version.
	Firmware date: device firmware date.
	Device MAC address: MAC address is most often assigned by the manufacturer and is stored in its hardware.
	Serial number: serial number can be found on device or box.
	Network addressing: DHCP With DHCP IP addresses and networking parameters are requested automatically from a DHCP server.
	Network addressing: Static IP IP address and networking parameters configured manually.
	Device IP address: numerical label assigned to each device.
	Ping Button: tests if particular device is reachable across an IP network.
	Subnet mask: determines what subnet an IP address belongs to.
	Default gateway: provides a default route for TCP/IP hosts to use when communicating with other hosts on remote networks.
	Port: TCP port of the device.
	Here I am interval (s): how often controller sends "Here I am" message.
	TCP connection timeout (s): Transmission Control Protocol specified connection timeout in seconds.

Initiate connection to server: initiates connection to server.

Host IP address: host IP address.

Connect through router: enables connection through the router.

Router IP address: router IP address.

Router port: router port.

Security level: there are 3 security levels normal, secure and more secure (you can choose it according to your needs).

Fast mode:

Matching timeout: shows how much time to wait response from controller after fingerprint is scanned.

Administrator PIN: administrator PIN.

Use SecureIO #0 for door controls: marked checkbox enables this feature.

Activate lock when door opens: activates lock when door opens. Marked checkbox enables this feature.

Anti-passback master: marked checkbox enables this feature.

Slave (secondary) devices: master (primary) controls one or more other devices known as slaves (secondary).

Enable tamper alarm: marked checkbox enables tamper alarm.

Upload all data to controller: uploads all changes made on users, access levels, APB areas etc.

Upload only network data to controller: upload network data to controller.

Door details panel: Device settings (HID devices)

Device settings Controller type [HID VertX EVO V1000 ▾] Firmware version [ ] Firmware date [ ] Device MAC address [ ] Network addressing ○ DHCP ● Static IP *Device IP address* [ ] [Ping] *Subnet mask* [ ] *Default gateway* [ ] Port [4070] Here I am interval (s) [20] ○ Connect to IP ● Connect to hostname *Host IP address* [ ] *Server host IP addess* [ ] ⬛ *Controller mode* [CardInCardOut] User name [ ] Password [ ] Reenter password [ ] [IO Linker rules] [Slave devices] [Open web config] ☐ Use FTP uploads (Faster but may not work under firewalls) ☑ Enable tamper alarm [Upload all data to controller] [Upload only network data to controller] ✔ OK ✖ Cancel	**Controller type:** the list of different manufacturer's controllers.
	Firmware version: device firmware version.
	Firmware date: device firmware date.
	Device MAC address: MAC address is most often assigned by the manufacturer and is stored in its hardware.
	Network addressing: DHCP With DHCP IP addresses and networking parameters are requested automatically from a DHCP server.
	Network addressing: Static IP IP address and networking parameters configured manually.
	Device IP address: numerical label assigned to each device.
	Subnet mask: determines what subnet an IP address belongs to.
	Default gateway: provides a default route for TCP/IP hosts to use when communicating with other hosts on remote networks.
	Port: TCP port of the display device.
	Here I am interval (s):
	Connect to IP: marked checkbox enables this feature.
	Connect to hostname: marked checkbox enables this feature.
	Host IP address: host IP address.
	Server host IP address: server host IP address.

Controller mode: controller mode set automatically.

User name: username.

Password: password.

Reenter password: ensures that passwords matches.

IO Linker rules: IQ linker rules can be entered manually.

Slave (secondary) devices: master (primary) controls one or more other devices known as slaves (secondary).

Open web config: opens device web configuration.

Use FTP uploads (Faster but may not work under firewalls): marked checkbox enables this feature.

Enable tamper alarm: marked checkbox enables tamper alarm.

Upload all data to controller: uploads all changes made on users, access levels, APB areas etc.

Upload only network data to controller: uploads only network data to controller.

Door details panel: Device settings (Mercury devices)

Device settings Controller type [EP1501 ▼] Firmware version [ ] Firmware date [ ] Device MAC address [ ] Network addressing ● DHCP ○ Static IP Device IP address [192.168.0.251] [Ping] Subnet mask [255.255.255.0] Default gateway [192.168.0.4] Port [3001] Here I am interval (s) [20] Server hostname [ ] [↪] User name [ ] Password [ ] Reenter password [ ] ☐ Use 1st reader port for slave devices [Slave devices] [Open web config] ☑ Enable tamper alarm [Upload all data to controller] [Upload only network data to controller] [✔ OK] [✖ Cancel]	**Controller type:** the list of different manufacturer's controllers.
	Firmware version: device firmware version.
	Firmware date: device firmware date.
	Device MAC address: MAC address is most often assigned by the manufacturer and is stored in its hardware.
	Network addressing: DHCP With DHCP IP addresses and networking parameters are requested automatically from a DHCP server.
	Network addressing: Static IP IP address and networking parameters configured manually.
	Device IP address: numerical label assigned to each device.
	Subnet mask: determines what subnet an IP address belongs to.
	Default gateway: provides a default route for TCP/IP hosts to use when communicating with other hosts on remote networks.
	Port: TCP port of the display device.
	Here I am interval (s): count of seconds controller will send "Here I am" message.
	Server hostname: server hostname.
	User name: user name.
	Password: password.
	Reenter password: ensures that passwords matches.

Use 1st reader port for slave devices: this feature is enabled when checkbox is checked.

Slave (secondary) devices: master (primary) controls one or more other devices known as slaves (secondary).

Open web config: opens device web configuration.

Enable tamper alarm: marked checkbox enables tamper alarm.

Upload all data to controller: uploads all changes made on users, access levels, APB areas etc.

Upload only network data to controller: uploads only network data to controller.

Door details panel: Device settings (MusDo CCS7000)

Device settings screenshot with fields: Controller type (MusDo CCS7000), Device MAC address, Device IP address (192.168.0.123) [Ping], EEi Web Service IP (192.168.0.213), EEi Web Service Port (0), Device Pin (1234), Password, Reenter password, checkboxes for Enable auto arming of security areas, Enable auto disarming of security areas, Check user profile permissions for auto arming/disarming, Upload all data to controller, OK / Cancel	**Controller type:** the list of different manufacturer's controllers.
	Device MAC address: MAC (Media Access Control) address is a number that identifies the network adapter(s) installed on your computer. The address is composed of up to 6 pairs of characters, separated by colons.
	Device IP address: is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.
	EEi Web Service IP: eei web service IP.
	EEi Web Service Port: eei web service port.
	Device Pin: device PIN.
	Password: password.
	Reenter password: ensures that passwords matches.

Enable auto arming of security areas: enables auto arming of security areas.

Enable auto disarming of security areas: enables auto disarming of security areas.

Check user profile permissions for auto arming/disarming: Checks user profile permissions for auto arming/disarming.

Upload all data to controller: uploads all changes made on users, access levels, APB areas etc.

Door details panel: Device settings (Mobile device)

Device settings screenshot with fields: Controller type (Mobile device), IMEI (123456789012345), User name (Test), Password, Reenter password, Timeout before photo (0), Auto close timeout (0), checkboxes Require photo, Get photo, Authentication type (Only PIN), Camera type (Camera facing back), Admin PIN, Reenter admin PIN, OK / Cancel	**IMEI:** mobile phone, GSM modem or device with a built-in phone / modem has a unique 15 digit IMEI (International Mobile Equipment Identity) number.
	User name: user name
	Password: password.
	Reenter password: ensures that passwords matches.
	Timeout before photo: timeout before photo.
	Auto close timeout: auto close timeout.
	Require photo: marked checkbox enables this function.
	Get photo: marked checkbox enables this function.
	Authentication type: two types of communication can be selected: PIN, NFC (near field communication).

Camera type: mobile device camera position.

Admin PIN: administrator PIN.
Reenter admin PIN: ensures that PIN matches.

Door details panel: Device settings: IO Linker rules
IO (input/output) linker rules can be created manually. And deleted by pressing 🗙 button.

Door details panel: Device settings: Slave devices	
	Baud rate: The speed of the communication line (bits per second).
	Panel number: panel ID.
	Device: slave (secondary) devices that can be added for master (primary) device, they are different it depends on different controllers manufacturers.
	Notes: can be added manually.
	Add: slave devices can be added manually.
	Detect slave devices: slave devices added automatically by detecting them.

Keypad formats window

Keypad format: the name of the keypad format.

PIN length: length of PIN codes.

PIN entry timeout: time interval which is given for a user to enter his PIN number from first to last digits.

Number of retries: number of times the PIN can be entered incorrectly. After reaching this limit the reader will not accept PIN code entries for the time period entered in "Lockout time" field.

Lockout time: Time to lock the reader after several failed attempts to enter a PIN.

Enter button: if a users PIN number is shorter than 'PIN length' he can press the specified button to send the PIN to the controller.
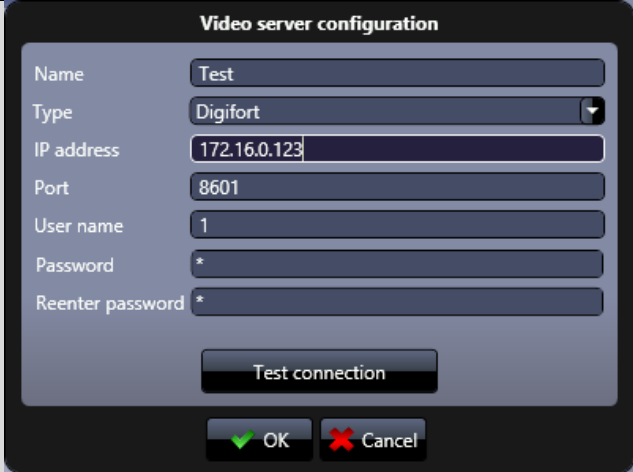
Cancel button: when pressed during the PIN entry this button will cancel the operation and nothing will be sent to the controller.
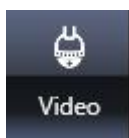
 Video tab

Video details panel

Camera name: specifies name of the camera (can be associated with something to make it clear, when there are many cameras).

Video server name: name of the video server, can be configured in video server configuration window.

Video camera on server: existing video cameras list on configured server.

Video server IP address: an Internet Protocol address (IP address) of video server.

Camera type: can be video server (one of video server cameras) or IP camera (connected directly).

Monitored doors: doors monitored by described video camera.

Location: describes video camera location.

Apply filter: the purpose is to filter related events of precisely camera by chosen criteria.

Camera description: specifics or other information related with camera.

Use event thumbnail photo older by (milliseconds): uses event photo older by milliseconds given.

Snapshot resolution: snapshot taken by camera resolution.

Thumbnail resolution: thumbnail resolution.

Live stream settings

Camera IP {1}: camera IP address.
Camera user name {2}: camera user name.
Camera password {3}: camera password.
Camera port {4}: camera port.
Camera link template (default „rtsp://{2}:{3}@{1}:{4}"): composed of the elements described above.
Show live stream: shows live stream.

Video server configuration window
Name: specifies name of the video server.
Type: video server type.
IP address: an Internet Protocol address (IP address) of video server
Port: video server port.
User name: user name.
Password: password.
Reenter password: ensures that password entered correctly.
Test connection: test if data entered provides communication.

Filter configuration window
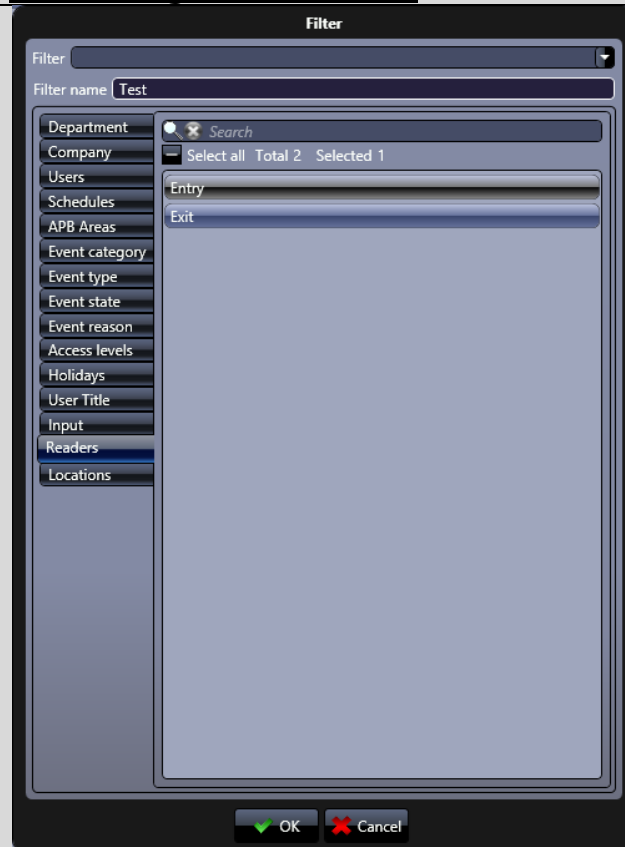
Filter name: specifies name of the filter.

Inputs tab

Inputs details panel: Glassbreak detector, Motion detector

Name	Test
Location	Main
Device IP address	172.16.0.203
Controller type	*HID VertX V2000*
Device type	Glassbreak detector
Input address	Left door open
Contact type	Alarm contact

Name: indicates the name of this Input device.

Location: indicates location of input device.

Device IP address: indicates the controllers IP address which will use input device.

Controller type: indicates controller which will use the input device.

Device type: indicates types of the input devices.

Input address: indicates the alarm input on the selected controller device.

Contact type: select the contact type used by the alarm input device (Normally open or normally closed).

Inputs details panel: Weight detector

Name	Test
Location	Main
Device IP address	172.16.0.203
Controller type	*HID VertX V2000*
Device type	Weight detector
Input address	Left door open
Contact type	Alarm contact
Doors	Project lead office door
Doors	Lobby door
Weight Ok output	
Weight not Ok output	
Allowed deviation (grams)	0
Connection	Com
COM port	COM1
Baud rate	9600
Data bits	8
Stop bits	One
Parity	None

Name: indicates the name of this Input device.

Location: indicates location of input device.

Device IP address: indicates the controllers IP address which will use the input device.

Controller type: indicates controller which will use the input device.
Device type: indicates types of the input devices.
Input address: indicates the weight detector input on the selected controller device.
Contact type:
Doors: indicates doors which will use this input.
Weight Ok output: can be selected output if weight is OK.
Weight not Ok output: can be selected output if weight is not OK.
Allowed deviation (grams): allows deviation from weight in grams.
Connection: where are two connection types: com and LAN (network in a limited area such as a home, school, computer laboratory, or office).
COM port: serial port number to be used.
Baud rate: the speed of the communication line (bits per second).
Data bits: serial port communication line data packet size.
Stop bits: serial port communication line empty packet size.
Parity: serial port communication setting.

Inputs details panel: License plate
Name — Test
Location — Main
Device type — License plate recognition server
Camera — DF Camera that always has video
Door — Lobby door
Name: indicates the name of this Input device.
Location: indicates location of input device.
Device type: indicates types of the input devices.
Camera: indicates camera capturing license plates.
Doors: indicates doors which will use this input.
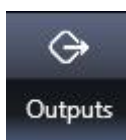
Outputs tab

Outputs details panel: Siren, Weight is OK, Weight is not OK

Name	Test
Location	Main
Device IP address	172.16.0.203
Output	Relay 1
Device type	Siren
Schedule mode	*Required field*
Schedule	*Required field*

Name: indicates the name of this Output device.

Location: indicates location of Output device.

Device IP address: indicates the controllers IP address which has the output device.

Output: listed outputs.

Device type: indicates types of the output devices.

Schedule mode: schedule mode has two values it can be activated or deactivated.

Schedule: schedule has as many values as are created schedules (schedules can be created in schedules tab).

Outputs details panel: Arm/disarm trigger

Name	Test		
Location	Main		
Device IP address	172.16.0.203		
Output	Relay 1		
Device type	Arm/disarm trigger		
Apply filter	Access granted vents		
Action	Pulse	Pulse time (s)	100
Wait for	2	identical events in (s)	100

Name: indicates the name of this Output device.

Location: indicates location of Output device.

Device IP address: indicates the controllers IP address which has the output device.

Output: listed outputs.

Device type: indicates types of the output devices.

Apply filter: filters output events by what criteria are chosen for filtering.

Action: can be pulse, turn on and turn off.	**Pulse time (s):**
Wait for: number of identical events.	**Identical events in (s):** waits specified amount of time.
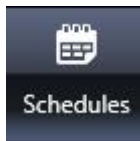
Schedules tab

Schedules details panel

Schedule name: Test
Location
Main
Selected interval begins at: 11:40   Ends at: 13:55

00:00   06:00   12:00   18:00   23:59

Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
National holidays
Other holidays

New workday starts at: 00:00:00 (Time & attendance setting)

Time schedule is a user-configured combination of time intervals for a duration of one week. It may be used to define at which times users will be able to access doors. Each schedule consists of 9 day-schedules: 7 weekday-schedules and 2 holiday-schedules. There are 2 time schedules that are built automatically.

Always works all the time with all controllers. **Never** is for specifying some built-in values and it works the same for a user as if he did not have any schedule assigned to him.

Blue circles represent workdays. Usually from Monday to Friday, as defined in regional settings of the PC. Red circles represent weekends. Usually Saturday and Sunday, as defined in the regional settings of the PC.
Green circles represent holidays, which you can be defined in "**Holidays**" tab of SimpleID.

Schedule name: indicates the name of this schedule.

Location: indicates location where schedule will be used.

Selected interval begins at: indicates the start time of the selected interval. You can change this to get precise time.

Selected interval ends at: indicates the end time of the selected interval. You can change this to get precise time.

Weekday-schedules: you can add up to 5 intervals in for each day-schedule in SimpleID. These intervals indicate when a user will get 'access granted' from the readers.

Holiday-schedules: SimpleID allows you to configure 2 types of holidays: national and other holidays. If a certain day of month is marked as one of these holidays, the system will use holiday-schedules instead of normal weekday-schedules.
New workday starts at: indicates when the day ends and a new day starts. This option is used for Time & attendance calculations.
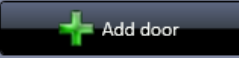
Access levels tab

Access level details panel

An access level is like a set of keys. It is a selection of doors that may be assigned to a user, which in turn defines his/her access permissions.
After including a door into an access level, you may leave the default time schedule "Always", which means that the user having this access level will be able to open the door at all times. Or you may change to another time schedule if you want the user to be able to open the door only at certain times.
Name: indicates the name of this access level.
Location: indicates location where this access level will be used.
"Add door" button: opens a dialog to add more doors to this AL (only unused doors will be shown).
Assign schedules: assigns a selected schedule to all the doors in this access level (for all readers).
Require operator confirmation (host mode): access must be confirmed by operator.
Default action if operator does not respond: default action can be chosen from Deny access or Grant access.
Time (s) for operator to respond: time in seconds for operator action.
Door entry reader schedule: This shows the schedule of the entry reader for this door (you can set an individual schedule for each door's entry reader using this).
Door exit reader schedule: This shows the schedule of the exit reader for this door (you

can set an individual schedule for each door's exit reader using this).
Remove door from AL: you can remove the door from this access level by pressing this button.
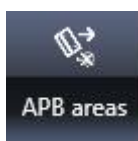
APB areas tab

APB areas details panel

Name	Inside
Location	Main
APB exempt	
Reset APB if door does not open (s)	0
☐ Daily APB reset for all users enabled	
Reset APB for all users daily at	23:59:59 ✖
Daily time limit	00:00:00 ✖
Single entry time limit	00:00:00 ✖

➕ Add door

PCB design office — Anti-passback type Soft ▾ ➡ Leads from Outside ▾ Leads to Inside ▾ ✖

Vehicle Entry Gate (North) — Anti-passback type Soft ▾ ➡ Leads from Inside ▾ Leads to Outside ▾ ✖

Name: indicates the name of APB area.
Location: indicates location where APB area will be used.
APB exempt:
Reset APB if door does not open (s): reset APB if doors don't open in specified amount of time (s).
Daily APB reset for all users enabled: marked checkbox enables this function.
Reset APB for all users daily at: resets APB for all users on specified time.
Daily time limit: can be set daily time limit for APB area.
Single entry time limit: time limit for single entry.
"Add door" button: adds doors to APB area.
Door entry reader anti-passback type: anti-passback type set to doors it can be hard (allows just one time), disabled and soft.
Door exit reader anti-passback type: anti-passback type set to doors it can be hard (allows just one time), disabled and soft.
Leads from: doors lead from APB area.
Leads to: doors lead to APB area.
Remove door from APB areas: deletes doors from APB area.
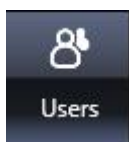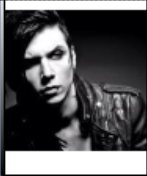
Users tab

General user details

	Employee	Identification
Family name	Admin	
First name	Admin	
Middle name		
Phone		
Secondary phone		
E-mail	D@ggg.com	
Messenger		
Department		
Company		
Title		
Employee number		
Location		

Main

Access level

Everywhere (Main) ,Validity: 3-12-2014 3:16 , Active

☐ Extended access

User type: Administrator

Time and Attendance

T&A type: Simple   Work schedule

Additional field #1:

Additional field #2:

Additional field #3:

Load photo from disk: load a picture from a local directory and use it as the users photo.

Capture photo from camera: capture an image from a connected camera and use it as users.

❌ **Delete photo:** remove photo of the user.
💾 **Save photo:** Save current photo as an image into a local directory.
🔄 **Reset APB status for this user:** clear any APB violations the user currently has.
Configuration of automatic notifications: setup automatic notifications (you must enable them in the "Settings → Modules" window).
Employee details information about user as his name, surname, email, company etc.
User type: user types with access rights.
🔧 **Configure user types:** user type configuration.
🔧 **Configure user login details:** user login details configuration.
Extended access: extended amount of time to go through the doors. Time in seconds can be set in doors information (doors tab).
T&A type: there is two options simple and advanced. When advanced option selected more advanced schedules can be created (T&A tab).
Work schedule: simple T&A type selection allows select work schedules, which can be created and edited in Schedules tab.
Additional field #1,#2,#3: additional fields is for optional information about user, for example user's characteristics.

Credential details

Card

Add new card: add a new card for this user.

Add new fingerprint: add a new fingerprint template group for this user.

Add new PIN: add a new PIN code for this user.

Card format: select a card format from the list.

Configure card format: open card formats configuration window.

Facility code: the facility code number of the card.

Number: the number of the card.

Get number from scanner: scan card number from a locally attached USB or serial card reader.

Select a number from the list of unused cards: if any cards have been shown to any of configured card readers in the system and are not assigned to users, they will be shown when you press this button.

Hex code: hexadecimal expression of this card.

Design: card design can be selected from already created designs.

Print card: prints the card.

License plate

License: license plate number.

Make: car make.

Model: car model.

Color: car color.

Fingerprint

Add new fingerprint template: scan fingerprints from any fingerprint reader in the system or locally attached USB reader. One fingerprint template holds 2 fingerprints, so one fingerprint template group can store up to 4 different fingerprints.

Remove fingerprint template: delete this fingerprint template from the reader.

Trigger duress alarm: if this is checked, then using any fingerprint from that template will start a duress alarm.

PIN

PIN: enter PIN code in this field (and repeat it in "Reenter PIN").

Activation: identification activation.

Expiration: identification expiration.

User tab filters

	Search
Access level	Select filter
Department	Select filter
Location	Select filter
Company	Select filter
T&A type	Both
User status	Active

Configuration of automatic notifications.

Configuration of automatic notifications

Search

Select all Total 1 Selected 1

Kazkas

☑ Is active

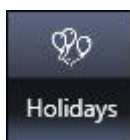Name Kazkas

Notification filter Kaz\kas

☑ Limit notifications to once per [1] minutes
if more than [1] messages are sent in [1] minutes.

Actions

E-mail E-mail From event's user

✔ OK   ✖ Cancel

Automatic notifications configuration window. Notifications must be enabled and configured in Settings->Modules->Notifications.

Holidays tab

General holidays details

Name	Christmas
Location	

Main

Holiday starts on

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
49	28	29	30	1	2	3	4
50	5	6	7	8	9	10	11
51	12	13	14	15	16	17	18
52	19	20	21	22	23	24	25
53	26	27	28	29	30	31	1
2	2	3	4	5	6	7	8

December 2011

Holiday ends on

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
49	28	29	30	1	2	3	4
50	5	6	7	8	9	10	11
51	12	13	14	15	16	17	18
52	19	20	21	22	23	24	25
53	26	27	28	29	30	31	1
2	2	3	4	5	6	7	8

December 2011

Holiday type National holidays

☐ Repeat each year

Name: indicates name of holiday.
Location: indicates holiday's location.
Holidays starts on: sets holidays beginning.
Holidays ends on: sets holiday ending.
Holiday type: can be two types of holiday: national holidays and other holidays.
Repeat each year: checked checkbox ensure that those holidays will repeat each year.

🗐
Reports
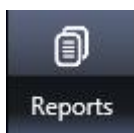
Reports tab

There are 7 different types of reports that may be generated by the software: Events, occupancy, users, devices, access levels, time & attendance and door access. Each of these report types have the same options groups for report customization.

Option groups of reports tab
Report options group: here you can setup the look of the report: enter header, subtitle, specify if pages should be numbered or if the date and time should be printed and also you can select a limit for the number of events.
Report interval group: here you must select the first and the last dates, which will define a time interval to be used to generate the report.
Report fields group: in here you can include to or exclude fields from the reports. You can also change the sequence of the f ields in the report. To include a field in the report select it in "Available fields" list and press a button with a single arrow pointing right.

Buttons with double arrows include/exclude all fields.	
Report filters group: here you can select which data filters should be applied for the report. Filters are grouped by type. Different report types can have more or less filter types available.	
Report items: here you can select individual items which should be included in the report. All other items will be excluded from this report.	

Automatic report details

	Name: Automatic report name.
	Active: activates automatic reports generation.
	Report type: consists of all existing reports.
	Report template: default or custom report template.
	Export to excel: marked checkbox enables this feature.
	Time: report generation time.
	Recurrence: recurrence of automatic report generation.
	Delivery: generated report is saved to file.
	Location: shows where report is saved.
	Date: shows when report was generated.
	Result: status of report generation.
	Comment: shows why failure appeared or where file is saved when generation is successful.

Monitoring tab

Monitoring tab overview	
Monitoring tab consists of 2 sections: map panel on the left side and events/maps/doors list panel on the right side.	
Map panel	**Events/maps/doors/inputs panel**
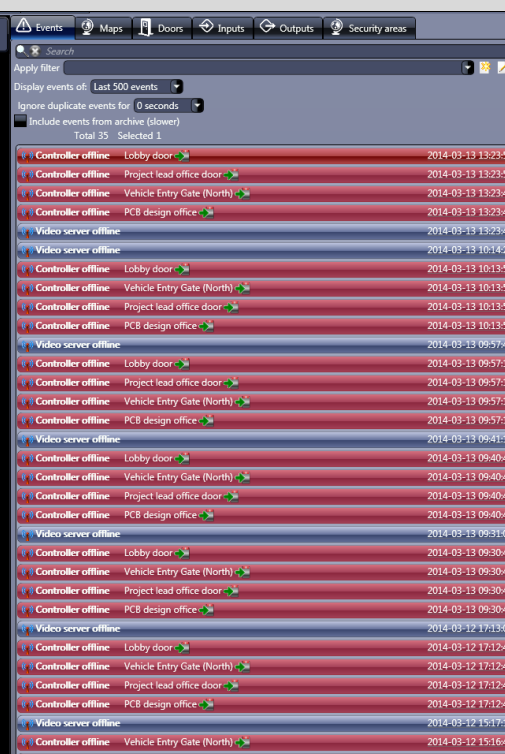
Quick navigation bar: in here you can switch through maps quickly, turn edit mode for a map on/off, revert changes and also zoom in/out the map.

, **Edit map/Save button:** turns on edit mode or saves a map if already in edit mode
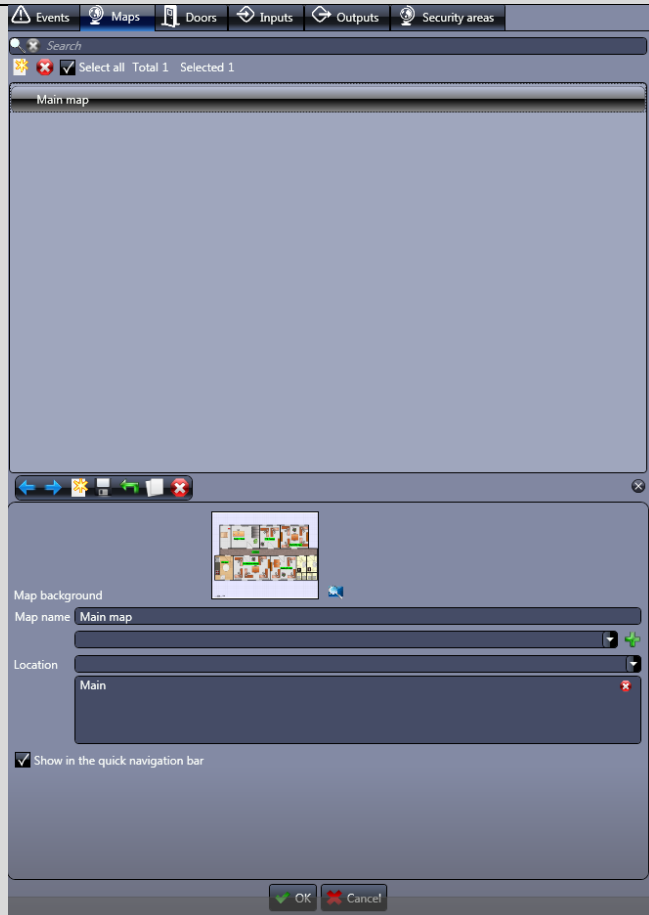
Zoom to fit: press this button to zoom the map so its height/width fits the window.
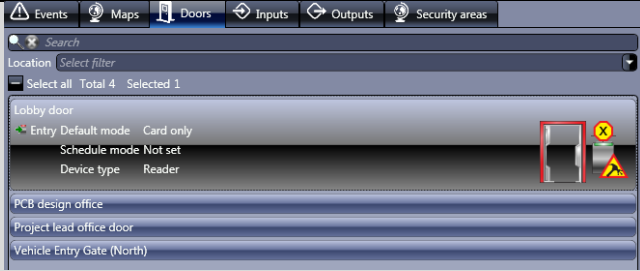
Revert changes: press this button to discard the changes made to this map.

Maps canvas: maps, events and doors are drawn in here; also you edit maps in this area.

List panels: Here you can switch between "Events", "Maps", "Doors" and "Inputs" list panels.

Events list

Search: enter text in here to filter the list by these keywords.

Apply filter: select a predefined filter by which all events would be sifted out.

New filter: press this button to create a new event filter (see "Filter window").

Edit filter: press this button to edit the selected filter.

Acknowledgment settings: opens the acknowledgment settings window.

Display events of: limit the number of events to be displayed either by date/time or by amount.

Events list: the events are shown in here.

| Maps list	
Search filter: filter the list by entered keywords.	
New map: press this button create a new map.	
Delete map: press this button to delete the selected map.	
Select all: toggle this check-box to select all, select none or restore previous selection of list items.	
Maps list: all of the configured maps are shown in this list.	
Map background: this is the image you will be seeing. The doors and events will be drawn on this image in the "Maps canvas". To add a new image click the button beside the image.	
Map name: the events are shown in here.	
Map icon: the icon is shown in the quick navigation bar and also in the maps list. Press the "+" sign to add a new icon from file.	
Show in the quick navigation bar: when this is checked the map will be shown in the quick navigation bar for fast access of this map.	

Doors list
Search filter: filter the list by entered keywords.
Location: filters the list by the location.
Select all: toggle this check-box to select all, select none or restore previous selection of list items.
Doors list: all of the configured doors are shown in this list. You can drag a door from this list onto a map in the "**Maps canvas**" when the map is in editing mode.

Inputs list
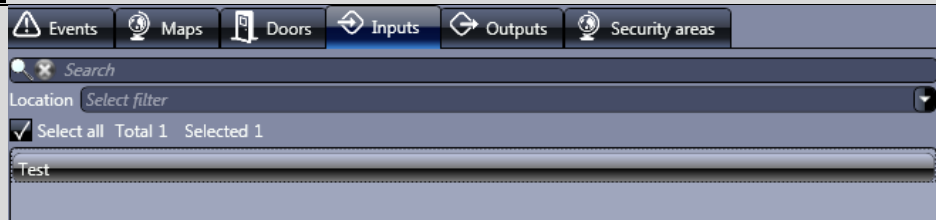
Search filter: filter the list by entered keywords.
Location: filters the list by the location.
Select all: toggle this check-box to select all, select none or restore previous selection of list items.

Outputs list
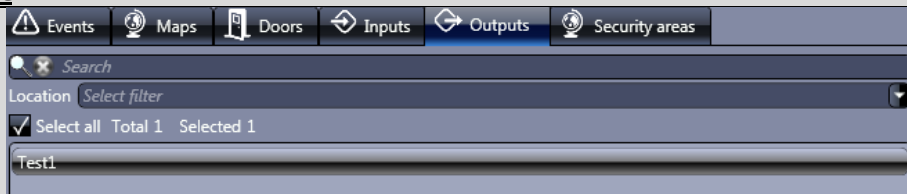
Search filter: filter the list by entered keywords.
Location: filters the list by the location.
Select all: toggle this check-box to select all, select none or restore previous selection of list items.

Security areas list
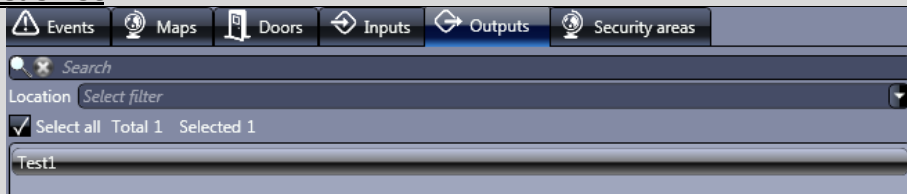
Search filter: filter the list by entered keywords.
Location: filters the list by the location.
Select all: toggle this check-box to select all, select none or restore previous selection of list items.

Occupancy tab

| |
|---|
| **Occupancy tab overview** |
| Monitoring tab consists of users/APB areas/doors list panels and events list. |
| |
| **Search:** filter the list by entered keywords. |
| **Display events of:** amount of events to be displayed. |
| **Apply filter:** filters events by created filter. |
| **Create new filter:** create new filter. |
| **Edit filter:** edit created filter. |
| **Configure display fields:** Displayed fields configuration. |
| **Remove this column:** removes column. |
| **Add new column:** add one more column. |
| **Select LPR door:** select doors for license plate recognition. |
| **Enter plate number:** field to enter license plate manually. |
| „Check „button: check if license plate exists in database. |
| **Events list:** the events are shown here. |

Occupancy: Users
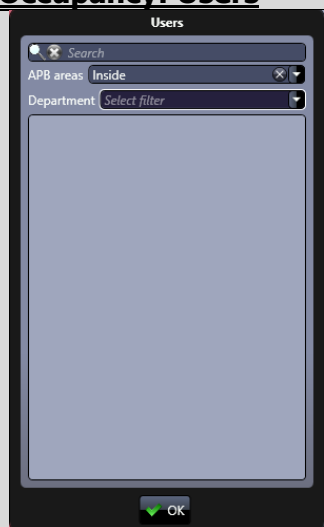
	Search: filter the list by entered keywords.
	APB areas: filters list by APB areas.
	Department: filters list by department.

Occupancy: APB areas
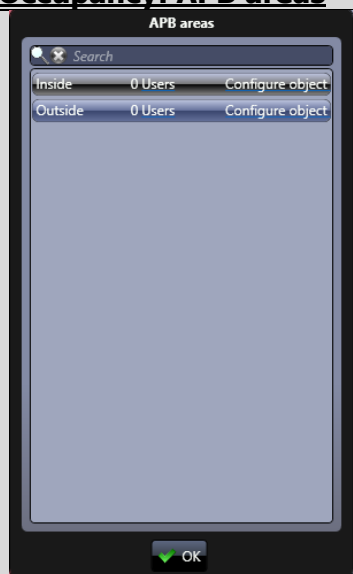
	Search: filter the list by entered keywords.

Occupancy: APB areas

	Search: filter the list by entered keywords.
	Location: filter list item by location.

Time & attendance tab

T&A tab overview

T&A tab consists of Individual schedules/Work schedule configuration/Settings tabs.

T&A: Individual schedules

Individual schedules window consist of user information, users with advanced schedule list and schedules list.

Individual schedules: User information

User information and work schedules in chosen month.

Individual schedules: Users with Advanced T&A list

Users with Advanced T&A list and those user's work schedule. Filter-filters users by those 4 fields (Family name, First name, Department, Employee number).

Individual schedules: Schedules list and detailed information
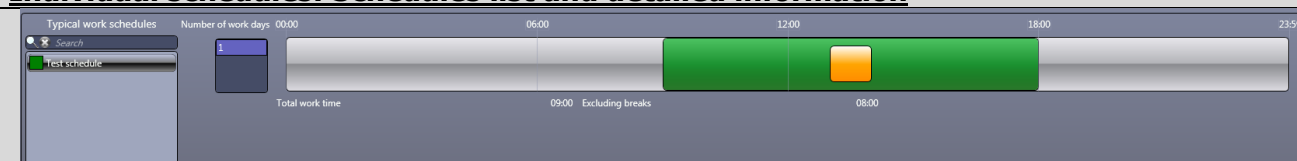
"Typical work schedules" (on the left) show all advanced schedules created. "Number of work days" shows how many days selected schedule consist of. Green bar on the right shows work time and breaks included in selected schedule.

T&A: Work schedule configuration

Name: name of work schedule.	
Color picker: different colors can be picked for work schedules.	
Report scheduled work time (ignores actual work time): sets work start and end time based on schedule, doesn't matter if user came earlier or left later.	
Unless user is absent: if user has absence reason not to come to work, then "Report scheduled work time (ignores actual work time)" is not applied.	
Use first and last events only (ignores all other events during the day): uses first and last day event, ignores all other entry and exit events during the day.	
Flexible: adds flexible work time to interval, user can come to work earlier or leave later.	
Get work type from reader: uses work type from controller, this work type can be set in doors tab-> door details->work type.	
Regular work time during weekends and holidays: when this feature is enabled, work hours are counted as regular work time, not as day off or holidays.	
Number of work days: available to add or delete work days.	
Add work day: Add one work day.	
Remove work day: remove one work day.	

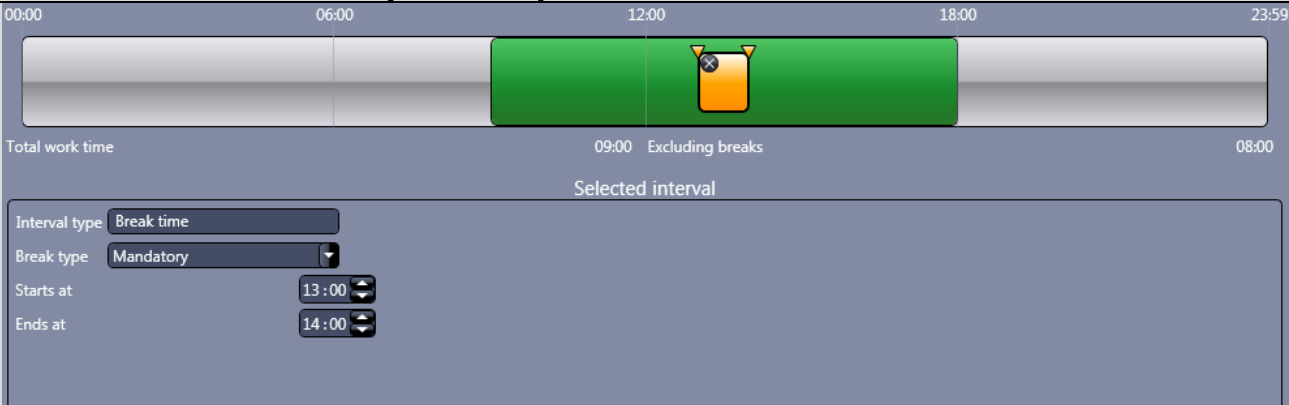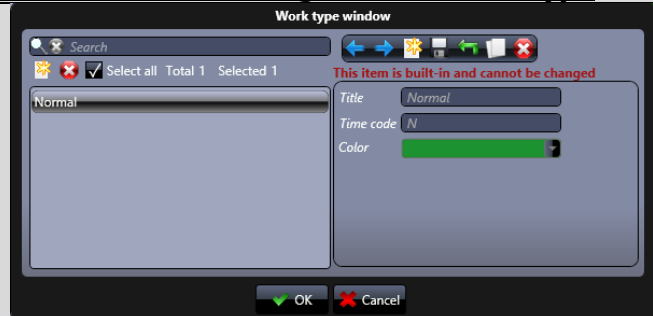| |
|---|
| **Interval type:** |
| **Overtime:** when user worked more hours when assign to user. |
| **Work type:** default normal work type selected. |
| ✏ **Work type:** new work time can be created. |
| **Starts at:** work hours start at. |
| **Ends at:** work hours ends at. |
| **Regular hourly break:** regular break can be optional and mandatory. |
| **Allow to accumulate hourly breaks up to:** |
| |
| **Interval type:** break. |
| **Break type:** can be mandatory or optional. |
| **Starts at**: break starts at. |
| **Ends at:** break ends at. |

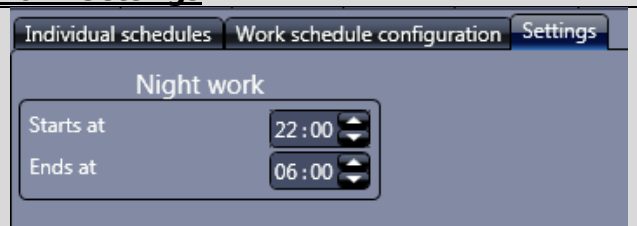| **Work schedule configuration: Work type**	
	Title: Name of work type.
	Time code: N-normal, can be something like that.
	Color: any of colors can be picked.

T&A: Settings	
	Start at: Night work starts.
	Ends at: Night work ends.
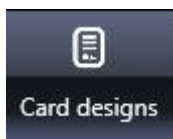
Card designs tab

Card designs tab overview

Name: Name of card design.	
Orientation: card orientation can be portrait or landscape.	
Type: object type can be text or image.	
Horizontal alignment: it can be align horizontally to left, right or center.	
Vertical alignment: object can be aligned vertically to top, bottom or center.	
Data source: data source listed, for example: first name, family name etc.	
Font: text font.	
Font size: text font size.	
Foreground: foreground color.	
Background: background color.	
Set background image: sets background image.	
Clear background: clears background	
Add object: adds object to card.	