

# CredolD v3 specification document v1.0 - 2017-11-17

## 1. Software requirements

Minimum requirements for the system, to be able to run CredolD software:

- CPU - Dual core processor, Intel Pentium IV 2 GHz, AMD Athion 3800+ or better;
- RAM - 4 GB;
- DirectX 10 compatible graphics card;
- MS Windows XP/Vista/7/8/8.1/10 and MS Windows Server 2008/2012/2016, 32 and 64 bit;
- MS SQL 2008/2012/2014/2016 Standard or Express Database;
- MS .Net Framework v3.5 SP1 and v4.6.2;

## 2. Supported hardware

CredolD supports different hardware systems from multiple manufactures. The table below displays the hardware CredolD supports.

Manufacturer	Device name	Module devices
HID	EDGE Plus E-400-K / ES400-K	VertX V100-E VertX V200-E VertX V300-E
	EDGE Plus ER40-K / ERP40-K / ESR40-K / ESRP40-K	
	EVO EDGE Plus EH-400-K / ESH400-K	
	EVO EDGE Plus EHR40-K / EHR40-L / EHRP40-K / ESHR40-K / ESHRP40-K	
	VertX V1000	
	VertX V2000	
	VertX EVO V1000	
	VertX EVO V2000	

<b>Mercury</b>	EP1501	MR50 MR52 MR16in MR16out
	EP1502	
<b>Suprema</b>	Xpass	Secure I/O 2
	Xpass S2	
	BioEntry Plus	
	BioEntry W/W2	
	BioLite Net	
	BioStation 2/A2/L2/T2	
	FaceStation 2	
<b>Axis</b>	A1001	
<b>ASB Security</b>	ccsMuSDO 7xxx	
<b>Otis</b>	Otis elevator	

<b>Additional hardware</b>	
<b>Android OS</b>	Mobile device
<b>USB devices</b>	USB card and fingerprint readers
<b>DigiFort</b>	Video camera and LPR support
<b>NumberOK</b>	Camera LPR support

### 3. GUI menu and main functions



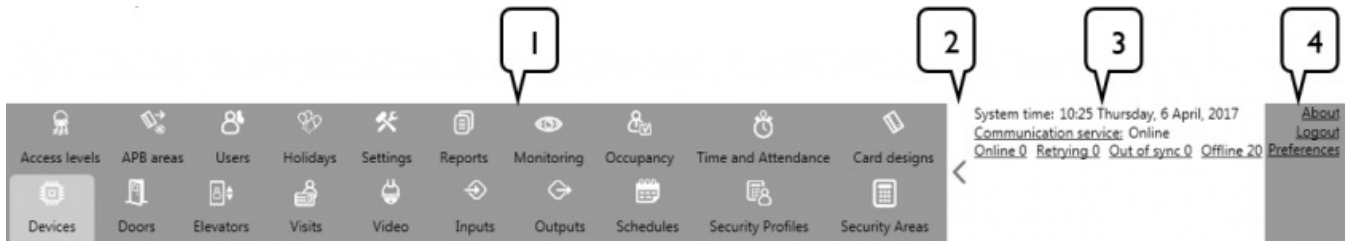
On the title screen, the information that is displayed is in this order:

- Software brand (CredolD, TerraID);
- Software version;
- The users name that is currently connected;

On the right side of the screen, it is possible to:

- Minimize;

- Full screen;
- Maximize;
- Close;



1. **Main menu tabs.** Main menu tabs are displayed here, where by clicking on them, opens up that tab. The number of tabs that are available depends on the license [3.3] and module settings [24.4].
2. **Second main menu tab (button).** Switches between main and secondary menu tabs where enabled main menu buttons are displayed. Which buttons are displayed are configured in the **Preferences** settings window.
3. **System status panel.** The System status panel displays the current systems time and statuses of the software's services and devices. As well, additional functions can be made for devices.
4. **Extra options.** Informational settings about the software and license can be viewed, as well configurations to the **Second main menu tab** can be made here. Logged in user can also configure its password and to logout from CredolD.

## 3.1 Menu Tabs

CredolD software contains 20 menu tabs, where different functions of the software can be made. These tabs are:

- Devices;
- Doors;
- Elevators;
- Visits;
- Video;
- Inputs;
- Outputs;
- Schedules;
- Security Profiles;
- Security Areas;
- Access levels;
- APB areas;
- Users;
- Holidays;
- Settings;
- Reports;
- Monitoring;
- Occupancy;
- Time and Attendance;
- Card Design.

It is possible to open menu tabs in a new window by right-click on the selected tab icon and by selecting "Open in new window". The new opened window won't have the GUI main menu section.

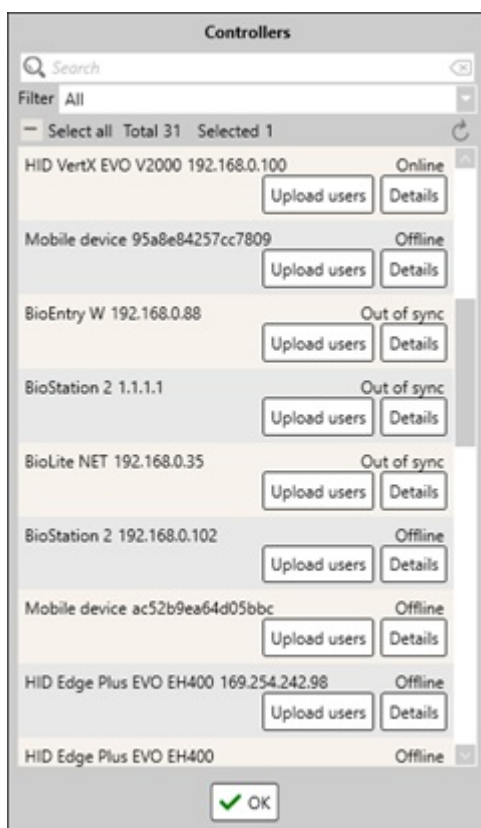
## 3.2 System status panel

The System status panel displays the current systems time and statuses of the software's services and devices. As well, additional functions can be made for devices.

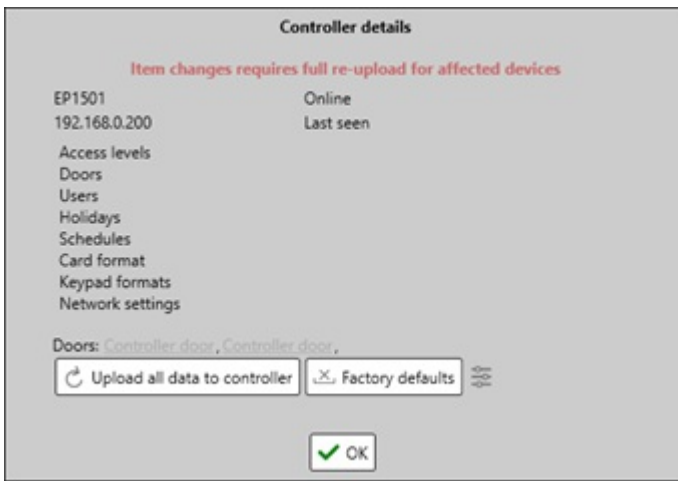
System time: 14:25 Wednesday, 12 April, 2017  
Communication service: Online  
Online 1 Retrying 0 Out of sync 0 Offline 19

- **System time.** Shows time depending on the OS systems time. Format is depended on OS system.
- **Communication service.** Displays if software service is online or offline (offline in red text). Clicking on “Communication service” will open a Service manager, where it is possible to start or stop the software’s service. Administration privileges is required.
- **Devices status.**
  - **Online.** Displays the number of devices that are currently online and synchronized with the software.
  - **Retrying.** Displays devices that are having issues with data transfer and that the data is being re-sent to them. If the data transfer is unsuccessful, then the device status changes to **Out of sync**.
  - **Out of sync.** Displays devices that are not synchronized with the software.
  - **Offline.** Displays devices that are unable to connect with the software or are offline.

By clicking one of the device status buttons (**Online, Retrying, Out of sync** or **Offline**), opens “Controllers” window. This window displays how many and which devices have the current statuses, depending on the selected filter.



- **Upload users.** Uploads all users to the controller;
- **Details.** Opens “Controller details” window for the selected controller.



- Displays the controllers type, IP address, its status and the data that is uploaded to the controller;
- **Doors.** Displays doors that are configured with the selected controller.
- **Upload all data to controller (button).** Uploads all needed data to the controller and reboots it. This is required for synchronizing the controller with the CredolD and a reboot is done to ensure that all settings save (some settings only save after a reboot).
- **Factory defaults (button).** Factory resets the controller. Note, all data will be removed from the controller, this also resets controllers network settings and due of that, the controller might not be able to communicate with the software.
  - **Erase and upload.** Factory resets the controller and then after reconnecting, uploads all data and synchronizes with CredolD. **This function is deprecated.**
  - **Erase.** Factory resets the controller.
- **Device settings (button).** Opens Devices tab and focuses on the selected controller.

## 3.3 Extras options

- **About.** Brings up an info window that where additional information about the software is displayed, as well as license information can be viewed.



- On the left-bottom corner, CredolD's version is displayed and additional information.
- **Manage licenses.** Here it is possible to view the current license information and activate license either by typing in a license key, activating it online or by loading up a license file [25.5].
- A link to Midpoint security web page is displayed, <https://www.midpoint-security.com>.
- **Logout.** Logout from CredolD as the current user. After login out, "Logout" button changes to "Login" button. This enables to login with a different user.
- **Preference.** The password for the current login user can be changed and main menu buttons can be enabled or disabled.
  - **User.** Displays users first and last name which is login at the moment.
  - **Login details.** Able to change the currently login user's password.
  - **Main menu buttons.** Enable/disable the main menu tabs that would be showed on the second Menu tab. To check the second menu tab, click on (<) on the menu tab to switch between primary and secondary menu tabs.

## 4. Panels main buttons



1. **Search.** Every tab that has a search function, has different searching properties. On what properties it has, follow each tab's sections for more information.
2. **Clear (button).** Clears the search field to be empty. If there is nothing written on the search field, Clear button will have a gray color and is disabled. After there are symbol on the search field, the button becomes activate and turns changes color to red.
3. **Location.** Filter the list by locations.
4. **Add new item to list & Create new item (button).** Creates a new item and adds it to the list.
5. **Remove selected item from the list & Remove this record (button).** Removes the selected item.
6. **Select all (checkbox).** Selects or de-selects all items. By its side, "Total" shows how many total items there are on the list, "Selected" shows the how many devices are being selected at the moment from the list.
7. **Refresh list (button).** Refreshes the list.
8. **Show previous/next list item (button).** By clicking "Show previous list item", will select an item above the one that was selected before, clicking "Show next list item" will select the below item.
9. **Save changes (button).** Saves settings for the selected item.
10. **Revert changes (button).** Reverts any changes that were made to the last saved settings.
11. **Create new record based on the current one (button).** Creates a new item based on the previously selected item. Does not create a perfect duplicate item, some key settings are not duplicated. More information on different item duplication is written on each tab specification.

## 5. Devices tab

On **Devices** tab, devices can be added, modified or removed from the software. Devices are added to the CredolD automatically as the software is capable to catch devices who are trying to connect to it or by using **Search for new devices** button, which then searches for any devices that can be added to the software. Also, the devices can be added manually.

There are 3 ways a device can be added to CredolD:

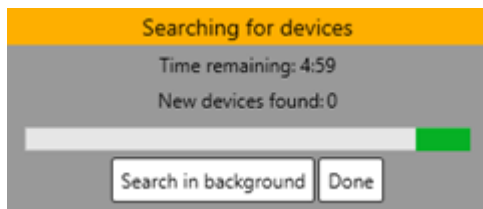
- CredolD picks the device automatically. Only works with Suprema and HID devices on a simple network.
- By searching the device, using **Search for new devices** button [\[5.1\]](#).
- Adding the device manually.

### 5.1 List panel

- Search is available by the following criteria: by name and IP.
- **Search for new devices (button).** Opens "Searching for devices" window, where it enables the device searching function. CredolD will then search for any devices that can be connected to the software for 5 minutes. The function works according to each manufacturers specification's and is only available in LAN. The function has guarantee finding all available hardware, if the devices network settings are configured correctly. While searching for devices, no further configurations can be made on CredolD.

While searching for devices, no further configurations can be made on CredolD. By clicking on **Search in background** button, the searching function will continue and configurations on CredolD can be made. By clicking on **Done** button, closes the "Searching for devices" window and ends the searching

process.



- **Search in the background (button)**. Hides the search “Searching for devices” window, but continues the searching procedure, allowing to continue work while the software is searching for devices.
- **Done (button)**. Closes the window and ends the searching function.

Need to know information while searching for specific manufactures devices.

- **HID** and **Suprema** devices work through UDP broadcast. Only available in LAN and NIC – the primary one.
  - To be able to search for **Mercury** devices and connect it through UDP, an Apple software called Bonjour (Bonjour Print Services) is required to be installed on the system.
  - **Axis** controllers are connected to CredID using HTTP protocols.
  - The search function is not supported for **MuSDO**, **Mobile** and **Otis elevators**
- Devices are sorted out by their ID. Filtering by **Devices type** is not supported. It is recommended to name the devices for easier searching capabilities.
  - Devices are displayed in this order:

	Devices name		ID		Device type		IP or IMEI	
--	--------------	--	----	--	-------------	--	------------	--

## 5.2 Details panel

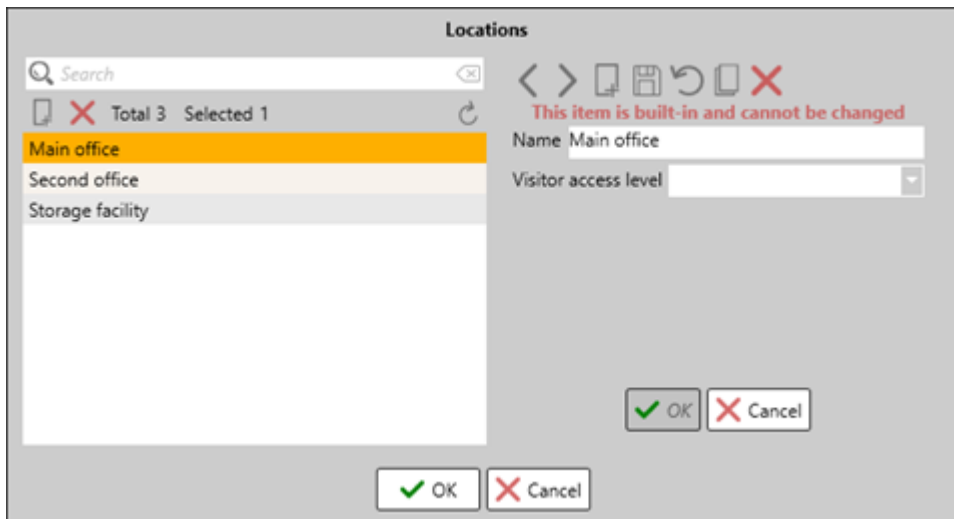
Details panel displays devices information, where it can be modified. This includes type, firmware information, network settings and additional information, depending on the device.

It is always recommended to review the settings carefully while adding a device using the search function or manually, as not all settings are received from the devices. Some fields have to be filled manually, such as login settings, additional network settings and similar settings.

## 5.3 Main device functions

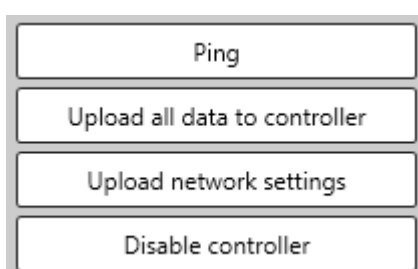
- **Controller type**. A device type is selected. This function is unchangeable if the device is added automatically. Each manufacturing brand has their appropriate settings to configure and these settings will be showed on details panel depending what controller type is selected. Addable devices:
  - Axis A1001.
  - BioEntry Plus.
  - BioEntry W.
  - BioEntry W2.
  - BioLite Net.
  - BioStation. **This device is no longer supported.**
  - BioStation T2.
  - BioStation A2.
  - BioStation L2.
  - MusDO CCS7000. Used to add ccsMusDO CCS7XXX controllers.
  - HID EDGE Plus E400. Used to add E400-K, ER40-K, ERP40-K.
  - HID EDGE Plus EVO EH400. Used to add EH400, EHR40, EHRP40.
  - EP1501.
  - EP1502.
  - FaceStation 2.
  - Mobile device.
  - Otis elevator.
  - HID VertX EVO V1000.

- HID VertX EVO V2000.
- HID VertX V1000.
- HID VertX V2000.
- Xpass.
- Xpass S2.
- X-Station. **This device is no longer supported.**
- **Name.** Devices name. If the device is added automatically or using the “Search for new devices” function, a name will be automatically given “Auto Discovery IP: [IP] MAC/Serial: [MAC/Serial address]”. It is recommended to change this name to a more appropriate name to make it user friendly and for easier searching capabilities.
- **Locations.** Indicates the location the device is assigned to. By its right side, there is a **Location** button which opens “Locations” window, where it is possible to configure custom locations and to add **Visitor access levels** to locations.  
There is a built-in location “Main office”, which is not editable nor it is possible to remove it. Note, if the device has doors configured to it, it is not possible to change its location.



- **Name.** Indicates the name of the location.
- **Visitor access level.** Access levels are selected here which will indicate which access levels visitors will be able to use on the specific location.
- **Device MAC address.** Indicates devices MAC address. MAC address is not displayed on **Otis elevator** and **Mobile device**.
- **Networking addressing.** Indicates the network type that is used for the device. There are 2 modes: **DHCP** and **Static IP**.
  - **DHCP.** It is not advisable to use DHCP mode as stable connection won't be guaranteed and some devices might not connect at all, depending on the manufacturers devices. HID and Suprema can work in DHCP mode as they identify with CredID not using IP, but by MAC and serial number. Other devices might have trouble connecting with DHCP mode.
  - **Static IP.** It is recommended to configure a static IP address for devices for a stable and secure connection.
- **Device IP address.** Indicates devices IP address. This field is not displayed for **Mobile devices**.
- **Subnet mask.** Indicates devices Subnet mask. This field is not displayed for **Otis elevator**, **MuSDO CSS7000** and **Mobile devices**.
- **Default gateway.** Indicates devices default gateway address. This field is not displayed for **Otis elevator**, **MuSDO CSS7000** and **Mobile devices**.

## 5.4 Main device buttons





- **Ping (button).** Opens cmd.exe and pings the IP address of the selected device by sending 1472 byte packets.
- **Upload all data to controller (button).** Uploads all needed data to the controller and reboots it. This is required for synchronizing the controller with CredolD and to ensure that all settings save. Some settings require a reboot of the device.
- **Upload network settings (button).** Uploads only network settings to the device.
- **Disable controller (button).** Disables the controller. Disconnects the device from the software and disables the details panel for that controller. “**Disable controller**” button is then change to “**Enable controller**”, which when pressed, will enable the controller and connect with the device.

**Note!** If a controller does not enable, check if the device module is enabled for that device. To do so, go to “Settings tab > Modules > [Manufacturers name] module” and check if the module is enabled. Another cause for the device to be disabled, is that there might not be enough reader counts in the license. Check license information [\[3.3\]](#) or contact your installer for license information.

## 5.5 Separate settings for devices

### 5.5.1 Axis A1001

To be able to add an Axis A1001 controller, Name, network settings (device IP, subnet mask, default gateway), TCP service port and login credentials have to be presented. Though these settings can be changed through CredolD as well. It is possible to connect a factory default Axis A1001 controller on CredolD and configure its network settings.

Controller type	Axis A1001
Name	
Location	Main office
Firmware version	
Device MAC address	
Network addressing	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
Device IP address	
Subnet mask	
Default gateway	
TCP service port	80
Here I am interval (s)	20
User name	root
Password	*****
Reenter password	*****

- **Firmware version.** Displays Axis devices current firmware version.
- **TCP service port.** Axis TCP service port. By default, Axis uses 80 port.
- **Here I am interval (s).** The time it checks connections with Axis device. By default, it is 20 second.
- **User name.** Login user name that is used to connect to Axis device.
- **Password & Reenter password.** Login password that is used to connect to Axis device.

### 5.5.2 Suprema

Every Suprema device mostly follows the same configuration process. Depending on the device, it has some extra configuration requirements or possibilities. **Note!** CredolD only supports Suprema devices that work with BioStar 2. Devices such as BioStation 1, X-Station, Face Station and the extension module Secure I/O are no longer supported since version 3.3.859.

The screenshot shows the configuration page for a BioEntry Plus device. The settings are as follows:

- Controller type: BioEntry Plus
- Name: [Redacted]
- Location: Main office
- Firmware version: [Redacted]
- Firmware date: [Redacted]
- Device MAC address: [Redacted]
- Serial number: [Redacted]
- Network addressing: DHCP (selected), Static IP
- Device IP address: 192.168.0.1
- Subnet mask: 255.255.255.0
- Default gateway: [Redacted]
- TCP service port: 51212
- Here I am interval (s): 20
- TCP connection timeout (s): 2
- Packet size: 1400
- Enable 100Base-T: [unchecked]
- Initiate connection to server: [checked]
- Security level: Normal
- Fast mode: Auto
- Matching timeout: 1 time only
- Use Wiegand input as a secondary device: [unchecked]
- Use Wiegand output: [unchecked]
- Use SecureIO 2 for door control: [unchecked]
- Anti-passback master: [unchecked]
- Enable tamper alarm: [unchecked]

- **Firmware version.** Displays Suprema devices current firmware version.
- **Firmware date.** Displays the firmware’s release date.
- **Serial number.** Indicates Suprema devices identification number.
- **TCP service port.** Indicates Suprema devices TCP service port. By default, Suprema devices that work with BioStar 2 use 51212 port. Older generation devices use 1471 port.
- **Here I am interval.** **This function is deprecated.** Suprema device no longer uses this function, it communicates with the software automatically all the time.
- **TCP connection timeout.** **This function is deprecated.**
- **Packet size.** Indicates the size of packets that are used to communicate with the Suprema devices.
- **Enable 100Base-T (checkbox).** Enable to use 100 Mbps ethernet connection.
- **Initiate connection to server (checkbox).** Connects to the device using Server mode. This option cannot be disabled as it is required to have a server mode activated for Suprema devices to connect with the software.
- **Use Wiegand input as a secondary device (checkbox).** Used while connecting Wiegand standard reader device as a secondary reader for the same door. It makes Suprema devices inputs active and accept card numbers from the reader. Typically, this reader only activates the same single relay available on the same device. If this checkbox is checked, **Use Wiegand output** function cannot be used as Suprema Wiegand connection can only operate in either INPUT or OUTPUT mode.
- **Use Wiegand output (checkbox).** Accepted card numbers are sent from one reader to another through Wiegand protocol. If this checkbox is checked, **Use Wiegand input as secondary device** function cannot be used as Suprema Wiegand connection can only operate in either INPUT or OUTPUT mode.
- **Use SecureIO 2 for door controls (checkbox).** Enabling this option, moves the door control (lock relay, exit button and door contact) to SecureIO 2 device. After enabling this checkbox, “Synchronize” button must be pressed on the SecureIO 2 device to synchronize its operation with the main device.
- **Anti-passback master (checkbox).** Indicates that this reader is the master reader at controlling APB functionality.
- **Enable tamper alarms (checkbox).** The system will report if a tamper switch is being activated.
- **Slave devices (Button).** Opens “Slave devices” configuration panel.
  - Possible to change connections **Baud rate** to: 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200;
  - Add or remove SecureIO 2 module. Only one SecureIO 2 can be added per device.

### 5.5.2.1 BioEntry Plus, BioEntry W, BioLite Net exclusive settings

These are settings are exclusive to biometric devices.

The screenshot shows the exclusive settings for biometric devices:

- Security level: Normal
- Fast mode: Auto
- Matching timeout: 1 time only

- **Security Level.** Set security level for fingerprint authentication. The higher the security level is set, the false rejection rate (FRR) gets higher, but the false acceptance rate (FAR) gets lower. Settings: Normal, Secure and More secure. By default, devices have “Normal” security level set.
- **Fast mode.** Set fingerprint authentication speed. Settings: Auto, Normal, Fast and Faster. “Auto” has the authentication speed configured according to the total amount of fingerprint templates registered within the device. By default, devices have “Auto” authentication speed set.
- **Matching timeout.** A matching timeout time interval. If the authentication is not completed within the

set time, the authentication fails.

## 5.5.2.2 BioLite Net and BioStation T2 exclusive settings

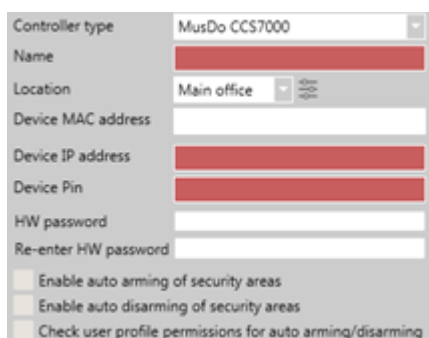
- **Administrator PIN.** Set Administrator PIN, which is used to login directly to the device through its interface. By default, the Administrator credentials are: ID: 99999999; PIN: 911911. **Note!** Please change the Administrator PIN on Suprema devices on the first use.

## 5.5.3 MuSDO CSS7000

MuSDO device manufacturer is ASB Security. Most configurations and preparations of the device is done through connected keypads which are connected with the MuSDO controller and through ASB Security's software WinCCS.

On CredolD, the device controller is called MuSDO CCS7000, but this includes most of the MusDO CSS7xxx devices that are compatible with CredolD.

Note, that sufficient input/output licenses are required when integrating MuSDO devices to CredolD.



Controller type	MusDo CCS7000
Name	
Location	Main office
Device MAC address	
Device IP address	
Device Pin	
HW password	
Re-enter HW password	
<input type="checkbox"/>	Enable auto arming of security areas
<input type="checkbox"/>	Enable auto disarming of security areas
<input type="checkbox"/>	Check user profile permissions for auto arming/disarming

- **Device Pin.** This is the installer code that is used on MuSDO devices. By default, if the installer code isn't changed, it is "9876".
- **HW password.** This is the flash password that is either configured through MuSDO keypad by the name "WUI mCCS key" or through WinCCS software, by the name "flash password". This setting has to be set on the MuSDO devices for it to be able to connect to CredolD.
- **Enable auto arming of security areas (checkbox).** This function is deprecated.
- **Enable auto disarming of security areas (checkbox).** This function is deprecated.
- **Check user profile permissions for auto arming/disarming (checkbox).** This function is deprecated.

## 5.5.4 HID

CredolD supports EDGE Plus E400 (E400, ER40, ERP40), EDGE Plus EVO EH400 (EH400, EHR40, EHRP40), VertX V1000, V2000 and VertX EVO V1000, V2000 controllers. Modules V100, V200, V300 can be added as slaves through V1000 controller.

For HID controllers to work with CredolD software, devices firmware has to be:

- EVO devices – 3.1.1.1168 or higher.
- Not EVO devices – 2.2.7.149 or higher.

Main HID settings on Device tab.

- **TCP service port.** HID TCP service port. By default, HID uses 4070 port.
- **Here I am interval.** The time interval in which a controller sends „Here I am“ message to CredID. By default, HID devices should have this setup for 120 seconds.
- **Connection type.** There are 2 ways a HID controller can connect to CredID:
  - **Connect to IP.**
    - **Host IP address.** Shows the IP of the host it is connecting to. This setting is not editable and only can be changed through the devices graphical user interface.
    - **Server host IP address.** Displays the servers IP address. On the right side, there is a button which will show all server IP addresses. This field is not required to be filled in as its purpose is to check server IP addresses.
  - **Connect to hostname.**
    - **Host name.** Network name of the server where CredID service is running. This setting is not editable and only can be changed through the HID’s device graphical user interface.
    - **Server hostname.** Displays the servers host name, the PCs name. On the right side, there is a button which will show all servers host names. This field is not required to be filled in as its purpose is to check server host names.
  - **Controller mode.** Identifies the mode that the controller is in. This field is only present for HID controllers. These modes are changed in Doors tab, while changing **Entry & exit controlled separately** There are two types of modes a controller can be in:
    - **CardInCardOut.** Identifies that both readers use the same door, as both ways require identification to pass through a door.
    - **CardInFreeout.** Identifies that both readers are separated from each other, having their own IO panel from the controller. In this mode, each reader can controller its own door, but with an exit button or unmonitored exit door.
  - **User name.** User name credential that is used to login to the HID graphical user interface. When a HID device is added automatically or while using search function, it will have „root“ user name assigned to it. This must be changed to „admin“, as user name „admin“ is used to login to HID graphical user interface.
  - **Password & Reenter password.** Password that is used to login to the HID graphical user interface. When a HID device is added automatically or while using search function, it will have password set as „pass“. This is the „root“ user name password. This must be changed to the password that is configured in the HID graphical user interface.
  - **Use FTP uploads (checkbox).** Used in the older systems (pre-2016) for establishing faster communication with HID controllers. Should not be enabled for modern systems and devices.
  - **IO Linker rules (button).** Opens „IO Linker rules“ panel where mini-scripting can be done. Allows specifying special commands to be executed on HID controllers when certain conditions are met. Does not work with all HID controllers. Please refer to HID product user manuals for more details.
  - **Open Web configuration (button).** Opens a browser and connects to the controller with the configured IP address.
  - **Enable tamper alarms (checkbox).** When enabled, the system will report if a tamper switch is being activated.

## 5.5.4.1 VertX V1000 and VertX EVO V1000 exclusive settings

- **Slave devices (button).** Opens „Slave devices“ configuration panel.



- VertX V1000 can downstream up to 32 devices, supporting 3 different modules that can be connected through 1/2 (left side) and 3/4 ports (right side):
  - V100-E – 2 reader interfaces.
  - V200-E – 16 input alarm panel.
  - V300-E – 12 relay output board.
- Slave devices are connected using Baud rate of 38400. This setting is not editable.
- Slave devices can be added by using „Detect slave devices“ function, which will search for any connected slave devices to VertX V1000. Or it can be added manually, by clicking „Add“ on 1/2 or 3/4 ports panel and then selecting the device in the „Device“ section.
- Slave panel is made out of 4 sectors:
  - **Panel number.** Shows the panel number.
  - **Device.** Select a device type (V100, V200, V300).
  - **Notes.** Editable field. Add notes to the slave device.
  - **Remove (X).** Removes the selected slave device.

## 5.5.5 Mercury

CredoID supports EP1501 and EP1502 Mercury controllers. Modules MR50, MR52, AssaAbloy and MR16IN/OUT can be added as slaves through EP1501 and EP1502 controllers.

Main Mercury controller functions on Device tab:

- **Firmware version.** Displays Mercury controller's current firmware version.
- **Firmware date.** Displays the firmware's release date.
- **TCP service port.** Mercury controller's TCP service port. By default, Mercury controller port is 3001.
- **Here I am interval.** The time interval in which a controller sends „Here I am“ message to CredID.
- **User name.** Login user name that is used to connect to Mercury device. The user name is configured in Mercury's controller graphical user interface. Default user name cannot be used.
- **Password & Reenter password.** Login password that is used to connect to Mercury controller. The password is configured in Mercury's controller graphical user interface. Default password cannot be used.
- **Use 1st reader port for slave devices (checkbox).** Uses the first internal reader ports as connections for slave devices. Only available for EP1501 controller.
- **Slave devices (button).** Opens „Slave devices“ configuration window.
  - EP1501 can have downstream up to 16 slave controllers and 8 inputs/outputs, while EP1502 can have downstream up to 32 slave controllers and 64 inputs/outputs, supporting up to 4 different types of slave devices:
    - MR50 – 1 reader interface module.
    - MR52 – 2 reader interface modules
    - AssaAbloy "Aperio" devices - up to 8 readers / monitored doors.
    - MR16IN – 16 zone input monitor modules.
    - MR16OUT - 16 zone output monitor module
  - Slave devices are connected using Baud rate of 2400, 9600, 19200 and 38400. By default, the Baud rate is set on 9600.
  - Slave devices can be added by using „Detect slave devices“ function, which will search for any connected slave devices. Or it can be added manually, by clicking „Add“ on and then selecting the device in the „Device“ section.
- **Open Web configuration (button).** Opens a web browser and connects to the Mercury controller with the configured IP address.
- **Enable tamper alarms (checkbox).** When enabled, the system will report if a tamper switch is being activated.

## 5.5.6 Otis elevator

Otis controllers are specifically used for elevator configuration, as the controller is designed for elevator control systems. DEC's are connected to Otis controller which act as a communication channel between the user and the elevator control system. As well, DEC's can be connected through different controllers, like HID VertX EVO V2000 controller.

Main Otis elevator controller functions on Device tab:

The screenshot shows a configuration window for an Otis elevator controller. It features several input fields and dropdown menus:

- Controller type:** A dropdown menu set to 'Otis elevator'.
- Name:** A text field with a red background, indicating it is required or has an error.
- Location:** A dropdown menu set to 'Main office'.
- Device IP address:** A text field containing '192.168.0.251'.
- Operation mode:** A dropdown menu set to 'Operation mode 3'.

At the bottom of the form is a button labeled 'Slave devices'.

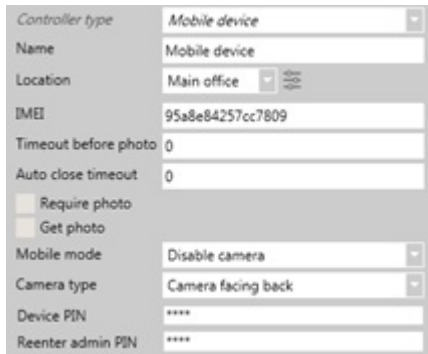
- **Device IP address.** The Otis service IP address.
- **Operation mode.** Identifies an operation the Otis controller will be working on:
  - **Operation mode 1.** Default floor. When a credential is presented, a default floor (lobby floor) and authorized floors will be sent to the DEC's. The user picks the desired floor after that.
  - **Operation mode 2.** Access to Authorized floor(s). When a credential is presented, only authorized floors will be sent to the DEC's. The user picks the desired floor after that.
  - **Operation mode 3.** User entry of destination floor. A user selects their desired floor. This may be performed with or without the presentation of a credential.
  - **Operation mode 4.** Default floor or user entry of destination floor. A user has to present a credentials. The user will be sent to the default floor (lobby floor) by default, unless a destination floor was chosen by the user before the timeout.
- **Slave devices (button).** Opens „Otis DEC's“ window, where it is possible to add or remove DEC's devices by adding their IP address.

For more information on Otis elevator controller and DEC's, please read Otis user guide which can be received from Otis contacts or from contacting [support@midpoint-security.com](mailto:support@midpoint-security.com).

## 5.5.7 Mobile device

CredoID has an application called Credo Mobile Access Platform (MAP) that allows to make a mobile device into access control reader or attendance terminal for access control and employee attendance, allowing to scan card identifications and take pictures of users. To be able to use this feature, a mobile device with Android OC system is required, as well as CredoID Mobile license with enough reader counts are needed too.

Main Mobile devices functions on Devices tab:



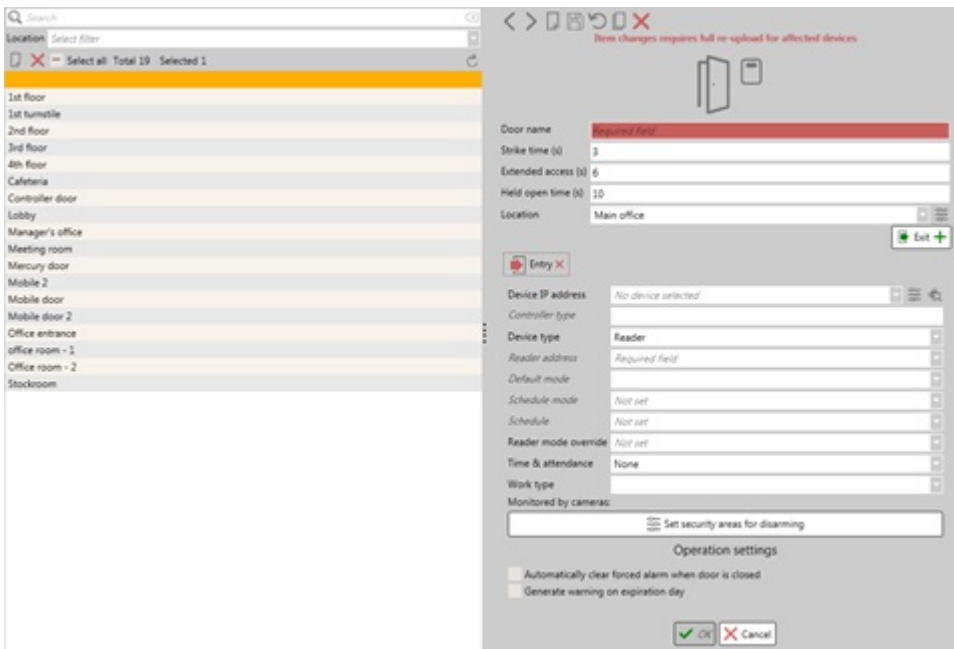
The screenshot shows a configuration form for a mobile device. The fields are as follows:

Controller type	Mobile device
Name	Mobile device
Location	Main office
IMEI	95a8e84257cc7809
Timeout before photo	0
Auto close timeout	0
Require photo	<input type="checkbox"/>
Get photo	<input type="checkbox"/>
Mobile mode	Disable camera
Camera type	Camera facing back
Device PIN	****
Reenter admin PIN	****

- **IMEI.** Mobile devices unique 15-digit IMEI number.
- **Timeout before photo.** Indicates the time before taking a photo.
- **Auto close timeout.** Indicates time before the event is sent automatically.
- **Require photo (checkbox).** Indicates that a photo is required to be taken and sent to CredoID after a credential is presented.
- **Get photo (checkbox).** After an identification is presented, will allow to take a picture to add to the event.
- **Mobile mode.** Indicates if the camera is enabled or disabled. By default, the camera is disabled.
  - **Disable camera.** Camera mode will be disabled and no photos will be able to be taken.
  - **Enable camera.** Camera mode will be enabled and photos will be able to be taken and added to events or users. This allows to take photos after a credential is presented.
- **Camera type.** Indicates which camera will be used for taking pictures. By default, **Camera facing back** is used.
  - **Camera facing back.** Uses the camera located on the back of the mobile device.
  - **Camera facing front.** Uses the camera located on the front of the mobile device.
- **Device PIN & Reenter admin PIN.** The admin PIN number that is used to access Credo MAP settings tab on the mobile device. The PIN number can only contain numbers and must be 4 digits long.

## 6. Doors tab

On Doors tab, controller readers are assigned as doors. Here doors are reviewed, created, modified and removed. On doors details panel, readers settings are changed.



## 6.1 List panel

On the list panel, configured doors are displayed. From here, doors can be created, modified or removed.

- Search is available only by name.
- Doors are sorted out by the English alphabet.
- By selecting one of the doors from the list, in the details panel its information is presented.
- On the list panel, only doors names are displayed. If a mouse is hovered over a door which is in the list, more detailed information is given about the door:
  - (Left side) Gives small information for both Entry and Exit readers (more information on Doors details panel section):
    - **Default mode.** Displays configured default mode.
    - **Schedule mode.** Displays configured schedule mode.
    - **Device type.** Displays devices reader type.
  - (Right side) Displays an illustration of a configured door. More information on Doors status section.

## 6.2 Details panel

Details panel displays selected doors, reader information settings. Here, they are configured and modified. Some reader settings require that controllers reboot to be able to save settings properly, a full upload is required for the device [\[3.2\]](#) or [\[5.4\]](#).

Doors illustration statuses are displayed on section [19.4](#).



Item changes requires full re-upload for affected devices

Door name Required field

Strike time (s)

Extended access (s)

Held open time (s)

Location

Device IP address

Controller type

Device type

Panel number

Reader address

Default mode

Keypad format

Schedule mode

Schedule

Reader mode override

High Security Mode

Time & attendance

Work type

Monitored by cameras:

**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)

- **Door name.** The name of the configured door.
- **Strike time.** Indicates for how long the lock must remain unlocked after granting access. Full upload to controllers is required [3.2 or 5.4].
- **Extended access (s).** Indicates for how long the lock must remain unlocked after granting access for a user with extended time enabled. Full upload to controllers is required [3.2 or 5.4].
- **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 event is generated. Full upload to controllers is required [3.2 or 5.4].
- **Locations.** Set up location for the door [5.3].
- **Entry & Exit directions (button).** There are 2 direction that can be configured for a door to be readers or an exit button.
- **Device IP address.** Assign a controller to a door. The controllers displayed on the list depends on selected **Locations** and if it has free reader ports open (not yet added to any door). The information that is displayed on the device list: IP/IMEC; MAC; Status; Device type; Device name.
- **Network configuration for this controller (button).** Located on the right side of the **Device IP address** By clicking on it, opens Device tab and focuses on the selected device.
- **Search for new devices (button).** Located on the right side of the **Network configuration for this controller** This opens the Searching for devices and enables the device search function [5.1].
- **Controller type.** Displays the type of the controller that is assigned to the door. This field is not editable.
- **Device type.** Indicates the type of role the device should take: **Reader** or **Exit**
- **Panel number.** Indicates the port of the device it should use. This function only shows up for Mercury controllers EP1501, EP1502 and HID controllers VertX V1000 and VertX EVO V1000. For Otis elevator, DEC's IP address acts as a panel number.
- **Reader address.** Indicates which reader to use. Depending on the controller, the displayed options are different. If a controller only has 1 reader address, "Single reader" will be displayed. If the controller has multiple reader addresses – "Reader 1" and "Reader 2" are displayed.
- **Default mode.** Select access credentials for the door. Depending on the device type, different selection options are presented:
  - For Axis, HID, Mercury, Mobile devices:
    - Card only.
    - PIN only.
    - Card or PIN.
    - Card & PIN.
  - For Suprema devices:
    - For BioEntry Plus, BioEntry W, BioEntry W2 devices:
      - Card only.
      - Fingerprint only.

- Card or fingerprint.
  - Card & fingerprint.
- For BioLite Net, BioStation 2/A2/L2 devices:
  - Card only.
  - Card or fingerprint.
  - Fingerprint & PIN.
  - Fingerprint only.
  - Card & fingerprint.
  - Card & PIN.
  - Fingerprint & card & PIN.
- For Xpass and Xpass S2 devices:
  - Card only.
- **Keypad format.** Select a keypad format for PIN identifications. This option appears when a **Default mode** is set for HID devices as "PIN only", "Card or PIN" or "Card & PIN". Only available for HID devices. By default, it is possible to choose built-in formats:
  - HID 00;
  - HID 11;
  - HID 20;
  - HID 09.
- **Keypad format configuration (button).** On the right side of **Keypad format** field, there is a **Settings** button, which opens Keypad format configuration window. In this window, it is possible to review built-in keypad formats and configure custom ones. Built-in keypad formats cannot be removed.



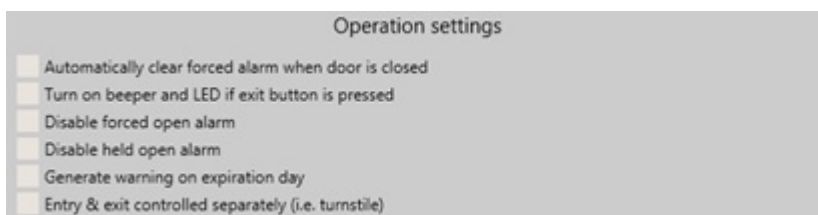
- **Keypad format.** Keypad format name.
- **Keypad structure.** Keypads button configuration.
- **PIN length.** The length of the PIN number.
- **PIN entry timeout.** Time interval which is given for a user to enter the PIN number from first to last digit.
- **Number of retries.** Number of times the PIN number can be entered incorrectly. After reaching this limit, the reader will not accept PIN number entries for a time period that is configured in **Lockout time**
- **Lockout time.** The locked time interval for the reader after the maximum number of **Number of retries** attempts have been reached.
- **Enter button.** Specify which button will have the "Enter" function. This button is used to confirm the PIN number or when a PIN number has to be entered that is shorter than PIN length.
- **Cancel button.** Specify which button will have the "Cancel" function. This button is used to cancel unfinished PIN number and reset it, that it would be entered from the start.
- **Schedule mode.** Indicates which mode is used during a specific schedule. Note, that this function only works after selecting a **Schedule** for the device. Schedule mode types:
  - **Unlock.** Unlocks the door, letting anyone through;
  - **Lock.** Locks the door, does not let anyone through;
  - **Card only.** Locks the door and only allows users with access credentials.
- **Schedule.** A schedule is selected during which period the **Schedule mode** will be active. The door stays locked during non-schedule time. By default, it is possible to choose built-in schedules: Always and Never.
- **Reader mode override.** Overrides the readers mode to either **Lock**, **Unlock** or default by leaving the field empty.
- **High Security Mode.** An option "Two card mode" can be selected to make a door more secure, by allowing access only when presenting two different cards. By default, High Security Mode is set on "Off"

option. This setting not available for Axis A1001 controller and BioStation 2/A2/L2 devices.

- **Time & attendance.** Specifies if the reader uses Time & attendance feature and its calculations. Readers with T&A feature, generate different types of events, that include either Clock-in or Clock-out types.
  - **None.** Generates normal events for the reader. This is set by default.
  - **Clock-in reader.** Generates events with clock-in events for the reader. It is advised to use on Entry directions.
  - **Clock-out reader.** Generates events with clock-out events for the reader. It is advised to use on Exit directions.
  - **Clock-in/Clock-out reader.** Generates events with either clock-in or clock-out events for the reader. This feature can only be used on readers with interactive screens, such as Suprema devices like BioLite Net, BioStation 2, where a user can select to either clock-in or clock-out.
- **Work type.** Assigns a configured work type, which is configured on Time & attendance schedule configuration tab.
- **Monitored by cameras.** Displays cameras that are configured on Video tab and are linked with the door. By clicking on the cameras name, it will go to the selected cameras configuration panel on Video tab.
- **Set default camera (button).** On the right side of the **Monitored by cameras** field, there is a button which brings "Set default camera" window. In this window, a default camera is selected from the cameras that are on the doors list.
- **Set security areas for disarming (button).** Sets security areas for disarming purposes for the reader.

## 6.3 Operations settings

Operations settings are located below the doors initial settings panel. Here, some exceptional settings can be configured for the readers. Each reader has a set amount of available operation settings.



- **Automatically clear forced alarm when door is closed (checkbox).** Clears "Forced open" alarm when the door is closed. If this function is enable, function **Disable forced open alarm** is then disabled. This function only works for HID and Axis controllers.
- **Turn on beepers and LED if exit button is pressed (checkbox).** Turns on connected beepers and LED's when an exit button is pressed for a short period of time. Only works if the **Device type** is set as Exit button. This function only works for HID controllers.
- **Disable forced open alarm (checkbox).** "Forced open" alarm events are not generated. If this function is enable, function **Automatically clear forced alarm when door is closed** is then disabled. This function only works for HID controllers.
- **Disable held open alarm (checkbox).** "Held open" alarm events are not generated. This function only works for HID controllers.
- **Generate warning on expiration day (checkbox).** **This function is deprecated.**
- **Entry & exit controlled separately (i.e. turnstile) (checkbox).** When enabled, each reader will use its own IO side panel of the controller. This enables the controller to be able to controller separate doors for each reader. This also changes the **Controllers mode** from **CardinCardout** to **CardinFreeout**.

## 6.4 Reader management window

By clicking on the selected illustrated doors reader, located on the Doors tab [6] or Monitoring tab [19.4], **Reader management** window appears. In this window, it is possible to change some of the doors settings. As well acts as a quick host confirmation window for a specific door, where access can be granted to users by the host.

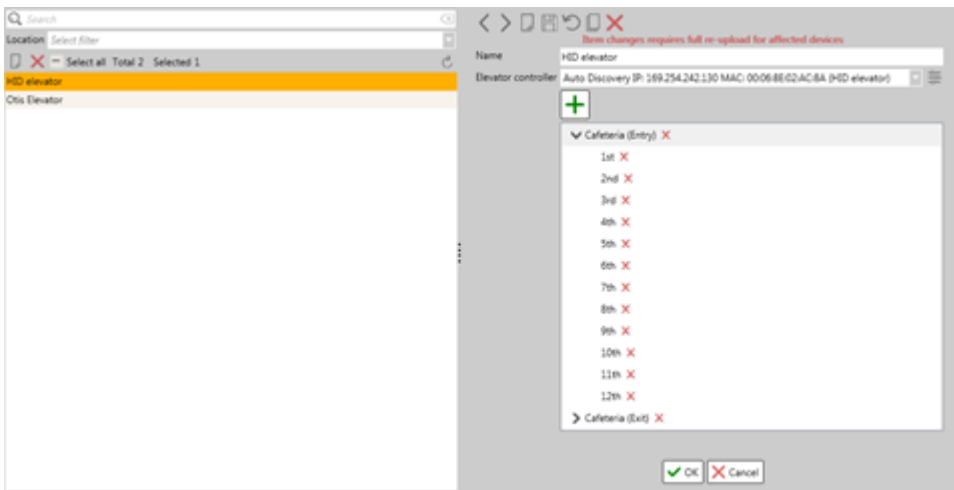


- **Reader mode override.** Overrides the readers mode to either **Lock**, **Unlock** or **Default mode**. Button **Apply** must be pressed for the settings to save.
- **User check.** Users information can be checked and then access can be granted for the user through the managing door. The field gives a list of users to choose from, depending on these criteria's:
  - Users are displayed depending on these filters: Family name, Employee number or License plate number;
  - For a user list to show up, at least 3 symbols must be typed.
- **Check (button).** This is a license plate number check function. After entering a license plate number in the **User check** field, click **Check** to generate an event for a user which will require a host confirmation. Does not work if a user is selected. It is recommended to use the **Check** function in Occupancy tab [20].
- **Camera & Live stream video.** Able to view live stream from the cameras that are monitoring the door.
- **Grant access.** An operators action that generates "Access granted. Operator action" events and opens the door for the managed reader. If a user is selected, it will be tagged into the event.
- **Clear forced open alarm.** Clears "Forced open" alarm for the managing reader.
- **Turn on/off auxiliary output.** Turn on or off auxiliary output for the reader. Only works with HID controllers.
- **Turn on/off beeper.** Turn on or off beeper output for the reader. Only works with HID controllers.
- **Turn on/off LED.** Turn on or off LED output for the reader. Only works with HID controllers.
- **Configure.** Opens the doors configuration panel in the Doors tab.

## 7. Elevators

In this panel, Otis and HID elevators are configured. Elevators are configured using HID VertX V1000 or VertX EVO V1000 and VertX V100, V200, V300 modules, as well, CredoID supports Otis elevators.

Note, that sufficient CredoID elevator licenses are required to be able to configure elevators on CredoID.



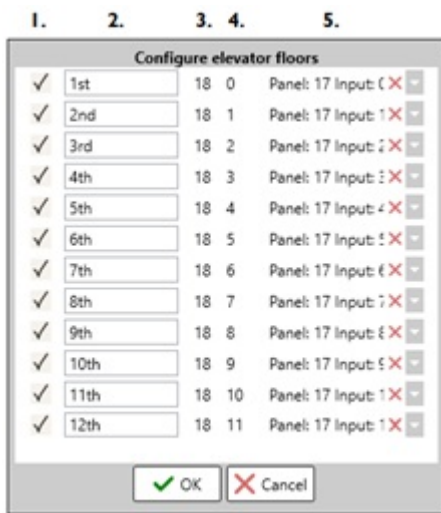
On List panel, elevators can be created, removed or by selecting them, to view their settings in the Details panel.

- Configured elevators are displayed.
- Configured elevators are sorted out by name.
- Search is available only by name.
- By selecting one of the elevators from the List panel, in the Details panel elevators information is presented.

On Details panel, elevator configuration process is configured.

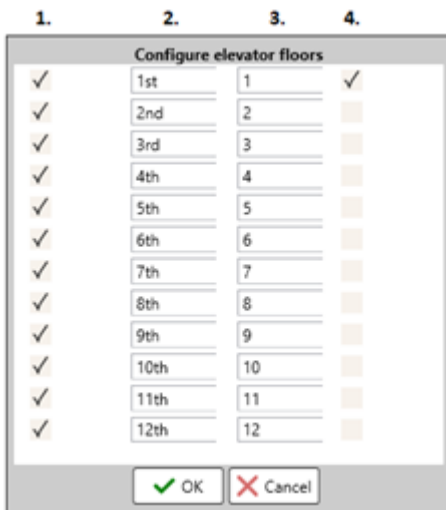


- **Name.** Elevators name.
- **Elevator controller.** Select the controller that is configured on Device tab. Only three types of controllers can be selected: VertX V1000, VertX EVO V1000 and Otis elevator controller. Configuration process for VertX V1000 [\[5.5.4.1\]](#) and Otis elevators [\[5.5.6\]](#) are different.
- **Configure elevator floors (button).** By right side of **Elevator controller** field, there is a settings button, which will bring Configure elevator floors window. Depending whatever HID or Otis elevators are being configured, different settings will be displayed.
  - HID elevator floor configuration:



1. **Enable (checkbox).** Enables the floor for use.
2. **Name.** Name the floor.
3. **Module number.** Indicates the ID of V300 module that is being used.
4. **VertX V200 inputs.** Indicates the inputs of the V200 module that will be used for the floors.
5. **Relays.** Choose a V300 relay which will have the configured settings.

o Otis elevator floor configuration:



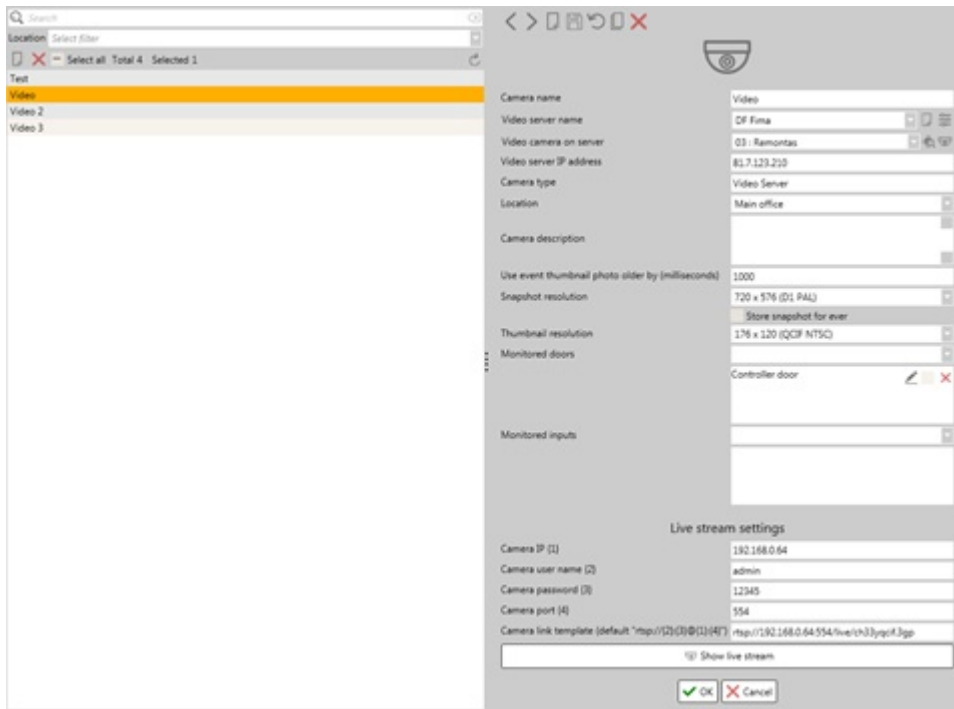
1. **Enable (checkbox).** Enables the floor for use.
2. **Name.** Name the floor.
3. **Module number.** Indicates the module that is being used.
4. **Relays.** Indicates the relay of the V300 module.

- **Add reader (button).** Opens „Add elevator reader“ window, where it is possible to select doors. Addable doors correspond with the selected **Elevator controller** (HID or Otis). If HID is selected, only doors of VertX V1000 with V100 module will be displayed, while with Otis, doors with DEC are displayed.
- **Elevator door list (field).** Displays added elevator doors. By right-clicking on the selected door, an option „Add Floors“ can be chosen. This opens „Add elevator reader floor“ window, where it is possible to add configured floors. To add multiple doors simultaneously, either ctrl(hold)+mouse1 or shift(hold)+mouse1, to select multiple doors. By the right side of the elevator door, remove button is present which will remove the elevator door from the list.

## 8. Video

In Video tab, camera illustrations are created which connect to a video server or a certain camera, and takes their settings information and video data (video captures, live stream).

Note, that sufficient CredolD camera licenses and Video server software, and licenses are required to be able to configure video and camera settings.



On List panel, videos can be created, removed or by selecting them, to view their settings in the Details panel.

- Configured cameras are displayed.
- Configured cameras are sorted out by name.
- Search is available only by name.
- By selecting one of the cameras from the list, in the details panel its information is presented.

## 8.1 Main functions



- **Camera name.** Indicate camera name.
- **Video server name.** A configured video server is chosen in this field. Video servers are created by clicking on „**Create new video server**“ button, located on the right side of the **Video server name**. To edit an already created video server, click „**Edit video server**“ button, located on the right side of the „**Create new video server**“ button.
- **Create new video server & Edit video server (button).** Opens **Video server configuration** window, where a new video server can be created or modify an already created video server.

- **Name.** The name of the video server.
  - **Type.** Indicates the type of video server that will be used. There are 3 types:
    - DigiFort.
    - IPCameraRTSP.
    - NumberOK.
  - **IP address or hostname.** The IP address or hostname of the video server.
  - **Port.** Port number of the video server.
  - **User name.** The user name that is used to connect to the video server.
  - **Password & Reenter password.** The password that is used to connect to the video server.
  - **Test connection (button).** Test the connection to the video server. This button is disabled while creating a new video server and is enabled when configuring an already created video server, by clicking on **Edit video server**.
- **Video camera on server.** Video server cameras are displayed and selected from this field.
  - **Search video cameras on video servers (button).** Searches for cameras on the video server. Located on the right side of the **Video camera on server**
  - **Show camera view (button).** Opens a "Camera view" window, where it displays the last known saved camera on **Video camera on server**. Located on the right side of the **Search video cameras on video server** button.



- **Image.** In the middle, a snapshot of the camera is showed. If an "X" image is displayed, an image was not received from the camera. The image resolution depends on the **Snapshot resolution** selected resolution.
  - **Live view (button).** Shows live view of the camera. **Live stream settings** have to be configured to be able to see live view of the camera and the computer system must support .vlc video format to work [8.2].
  - **Export image (button).** Takes a snapshot of the picture and saves in the selected location.
  - **Show in browser (button).** Opens the snapshot image on a default web browser.
  - **Refresh (button).** Requests a new snapshot from the camera and displays a new image. By its right side, a date and time of the image displayed.
- **Video server IP address.** Displays video servers IP address that is selected in the **Video server name**. This field is not editable.
  - **Locations.** Indicates the location that the camera is assigned to.
  - **Camera description.** Description for the camera. This is an informational field.
  - **Snapshot resolution.** The resolution of the snapshot that will be taken from the camera. Snapshots are displayed in Camera View window. The list displays available resolutions by CredolD, custom resolutions are not available. Please choose a resolution accordingly to the cameras settings.
  - **Store snapshot for ever (checkbox).** Store every snapshot taken in a location that is setup on Setting tab > Photo folder. By default, the snapshots are store in "C:\ProgramData\Access Control System\DBFileStreamData\Photos".
  - **Thumbnail resolution.** The resolution of the thumbnail that will be taken from the camera. Thumbnails



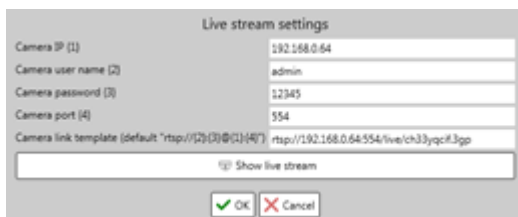
are Snapshot images with a different resolution and are displayed on events in the Monitoring and Occupancy tabs. The list displays available resolutions by CredolD, custom resolutions are not available. Thumbnails are not store anywhere.

- **Monitored doors.** Indicates doors which will have cameras snapshots taken, depending on the filter that is being used, which is defined by created filter in **Monitored doors filter**.
- **Monitored door filter (button).** By right side of added monitored door, there is a button "Edit filter", which will open a filter window [25.1]. Here, a filter has to be created and assigned that will define, when a snapshot is taken and added to the event. Note, that filters that are defined for monitored doors, can be used for monitored inputs too. By the right side of "Edit filter" button, there is a checkbox, which enables or disables the filter.
- **Monitored inputs.** Indicates inputs which will have cameras snapshots taken, depending on the filter that is being used, which is defined by created filter in **Monitored doors filter**.
- **Monitored input filter (button).** By right side of added monitored input, there is a button "Edit filter", which will open a filter window [25.1]. Here, a filter has to be created and assigned that will define, when a snapshot is taken and added to the event. Note, that filters that are defined for monitored inputs, can be used for monitored doors too. By the right side of "Edit filter" button, there is a checkbox, which enables or disables the filter.

## 8.2 Live stream settings

Live stream video can be seen through the software if Live stream settings are configured correctly, depending on the video server and even more depending on the camera itself. A live stream can be checked through Video tab by pressing "Show live stream" button and through Cameras view window, by "Live view" button. There are 2 ways a live stream can be configured for a camera:

- Typing in the cameras settings;
- Typing in the link template that will connect to the camera locally.



4 main settings have to be configured to be able to view live stream:

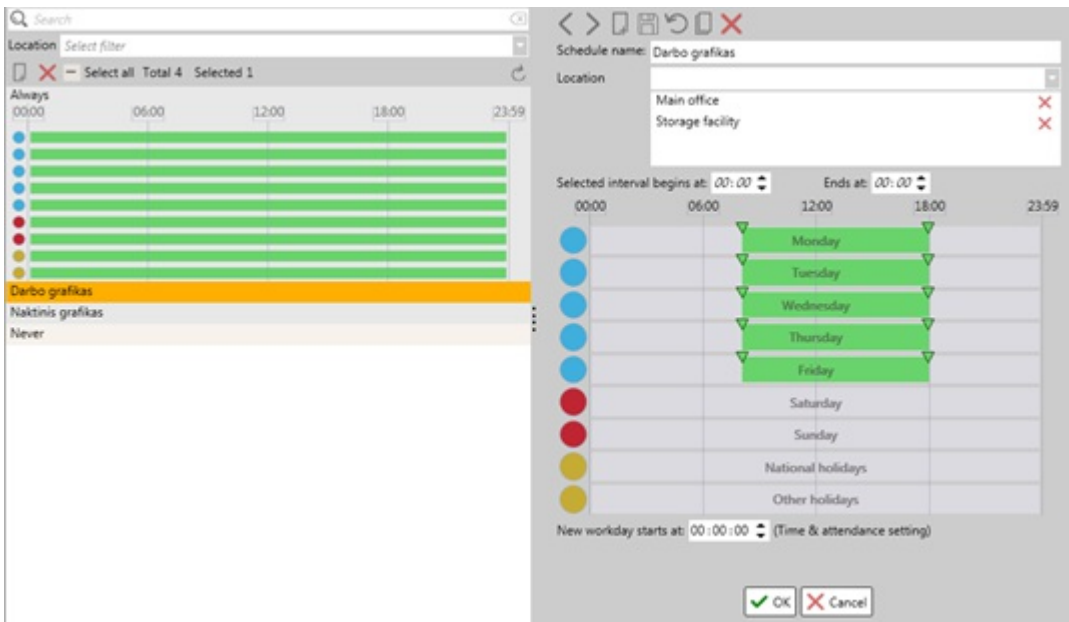
- **Camera IP {1}.** The IP address of the camera.
- **Camera user name {2}.** The user name login that is used to connect to the camera.
- **Camera password {3}.** The password login that is used to connect to the camera.
- **Camera port {4}.** The port that the camera uses.

This function won't work all the time as usually cameras requires a more specific string to be able to get a live stream from it. It is recommended to use the second option and type in the link that will call into the cameras live stream video.

- **Camera link template (default "rtsp://{2}:{3}@{1}:{4}")**. A link to the live stream footage has to be typed in. Note, that the given example only displays the login sequence, additional information has to be given. Example: "rtsp://admin:admin@192.168.0.70:557/Interface/Cameras/Media?Camera=Demo1".

## 9. Schedules

**Schedules** (also known as **Time zones**) are universal and are used through all Access Control System: in Access levels, Door locking, Time and attendance. They are configured in **Schedules** tab.



Time schedule is a user-configured combination of time intervals for a duration of one week and holidays. It may be used to define at which times devices should be active or when users will be able to access doors. Each schedule consists of 9 day-schedules: 7 weekday-schedules and 2 holiday-schedules.

There are two built in Schedules named **Always** and **Never** which are used internally in the system and cannot be changed. New schedules can be entered, edited and removed.

- **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 does not have any schedule assigned to him.

Note, that if schedules from Schedule tab is used for Time and attendance calculations, be sure that the schedules have only 1 work interval block per schedule day, as multiple schedule blocks per day will generate wrong Time and attendance calculations. To be able to use multiple schedule blocks per day and have correct work day calculations, schedules from Time and attendance tab has to be used.

## 9.1 List panel

On the list panel, configured and built-in schedules are displayed. From here, schedule can be created and added to the list or removed.

- Search is available only by name.
- Schedules are sorted out by the English alphabet.
- By hovering over a schedule, it displays the configured schedule time intervals.
- By selecting one of the schedules from the list, in the details panel its information is presented.

## 9.2 Details panel

On details panel, a selected schedules details are displayed and can be configured.

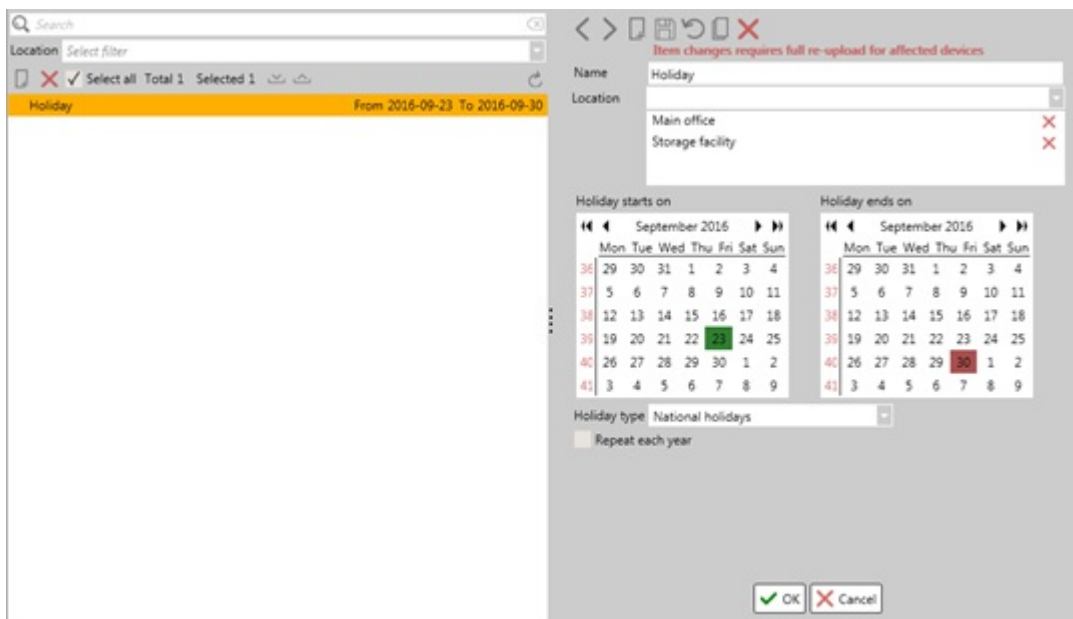
- **Schedule name.** The name of the schedule.
- **Location.** Locations are assigned to the schedule. Multiple locations can be assigned.
- **Selected interval begins at.** Indicates the start time (hh:mm) of the selected schedule block interval. The start of the schedule block can be changed.
- **Selected interval ends at.** Indicates the end time (hh:mm) of the selected schedule block interval. The end of the schedule block can be changed.
- **Schedule configuration fields.** Schedule intervals are configured in these fields. There is in total 9 day-schedules: 5 work-schedules (blue), 2 weekday-schedules (red) and 2 holiday-schedules (yellow). To create a schedule block, click and hold left-mouse button on one of the schedule fields and then drag in any given direction. Possible functions of schedule fields:

- To identify selected schedule blocks, a remove button will be next to the selected schedule blocks.
- Multiple schedule blocks can be created for the schedule, the limit of the blocks depends on the devices.
- Schedules interval can be change by editing „**Selected interval begins at**“ to edit the starting point and „**Selected interval ends at**“ to edit the end of the interval. Or by moving start and end arrow points, that are located above the schedule interval.
- It is possible to multi select (ctrl + left-mouse button) schedule blocks from different schedule fields. This allows to edit all of the selected schedule blocks start and end points to have the same parameters. Only one schedule block can be selected per schedule field.
- If a schedule that is being edited overlaps over other schedule blocks, it will remove the overlapped schedule block from the schedule field.
- **New workday starts at.** Indicates when the day ends and a new one starts. This option is used for Time & attendance calculations.

# 10. Holidays

Holidays can be configured in the Holidays tab. Holidays can be applied to any work or weekend days. Holiday schedules are configured in the Schedule tab, named as „National holidays“ and „Other holidays“.

Note, that configured holidays on Holidays tab, are not calculated when creating a Time and attendance report. Holiday intervals have to be configured on Time and attendance tab to be included in the reports.



## 10.1 List panel

On the list panel, configured holidays are displayed. From here, holidays can be created and added to the list or removed.

- Search is available only by name.
- Holidays are sorted out by date (the first holiday on the list is the oldest).
- The holiday interval (from, to) is displayed by the right side of the configured holidays.
- It is possible to export and import holidays, by clicking on **Export** or **Import**. The exported holiday file is in .xml format. To import holidays, in .xml file, the holidays have to be in rows and should be configured like this (note, that the .xml should not contain headers, only holiday data):

Holiday name	Start date and time	End date and time	Repeat each year (TRUE or FALSE)	Holiday type (NationalHolidays or OtherHolidays)
--------------	---------------------	-------------------	----------------------------------	--

Holiday	2017-09-23	2017-09-24	TRUE	NationalHolidays
---------	------------	------------	------	------------------

## 10.2 Details panel

On details panel, a selected holidays details are displayed and can be configured.

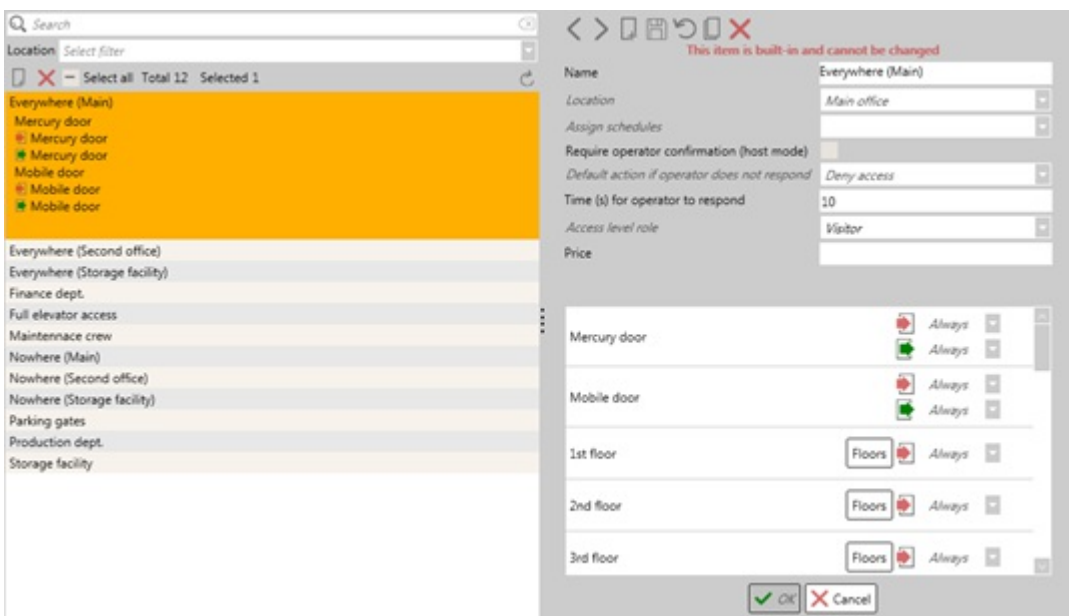
- **Name.** The name of the holiday.
- **Location.** Locations are assigned to the holiday. Multiple locations can be assigned.
- **Holiday starts/ends on.** The holiday interval. The start of the holiday is chosen on **Holiday starts on** calendar and is indicated by green color and the end of the holiday interval – **Holiday ends on** calendar, indicated as red.
- **Holiday type.** Indicates what kind of holiday it is. Possible types: National holidays and Other holidays.
- **Repeat each year (checkbox).** If this box is checked, the holiday will be repeated each year.

## 11. Access levels

An Access level is like a set of keys. It is a selection of doors that may be assigned to a user or visitor, which in turn defines the users access permissions. Access level can only use doors from the same location it is assigned to.

There are built in access levels for every location, that cannot be removed or edited.

- **Everywhere (location name).** Access levels are set for every door on the specified location with schedules set as Always. This will allow to go through every door on the specified location.
- **Nowhere (location name).** Access levels are set for every door on the specified location with schedules set as Never. This won't allow to go through every door on the specified location.



### 11.1 List panel

On the list panel, configured and built-in access levels are displayed. From here, access levels can be created and added to the list or removed.

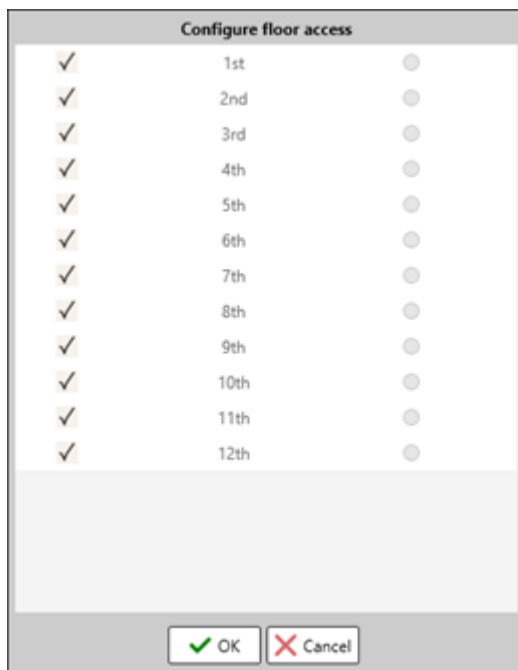
- Search is available only by name.
- Access levels are sorted out by the English alphabet.
- By hovering over an access level, it displays doors and readers with directions. Only 6 rows are displayed and if there are more doors and directions, it won't display all information.

- By selecting one of the access levels from the list, in the details panel, its information is presented.

## 11.2 Details panel

On details panel, selected access levels details are displayed and can be configured.

- **Name.** The name of the access level.
- **Location.** Location is assigned to the access level.
- **Assign schedules.** Sets schedules for all added doors to the one selected from the list. This field is hidden if there are no doors added to the access level.
- **Require operator confirmation (host mode) (checkbox).** To be able to pass through the door with an access level with this function enabled, a host confirmation is required for a user to pass. This function only works with License plate recognition module enabled and configured.
- **Default action if operator does not respond.** A timeout of the confirmation event, generated when a host confirmation is required. After **Time for operator to respond** time has passed, user will be either **Denied access** or **Granted access**. This function only works when **Host mode** is enabled.
- **Time (s) for operator to respond.** A time interval for an operator to respond to after an event is generated that requires a host confirmation.
- **Access level role.** **This function is deprecated.**
- **Price.** This function is used for Billing purposes. When a unit is written down, each time a user passes through the access level, the configured unit is added to the sum. Billing report then can be made in the Reports tab [23.8].
- **Add door (button).** Adds doors to the access level. Opens an „Add door“ window, where door(s) can be selected and added to the access level. Only doors from the selected location will be displayed on the list.
- **Doors list (field).** Displays added doors with reader directions and assigned schedules. Possible functions:
  - On the left, a door name is displayed.
  - On the right, reader directions are displayed (Entry and Exit), with their assigned schedules.
  - Schedules can be manually assigned for reader directions by clicking on the drop-down list near them and selecting a schedule. This as well can be done with **Assign schedules** function, to assign the same schedules to all readers.
  - On the far right, there is a remove button, which will remove the added door.
  - If an elevator door is added with configured floors, after saving the access levels, **Floors** button is displayed on that door. Pressing this button, opens „Configure floor access“ window.

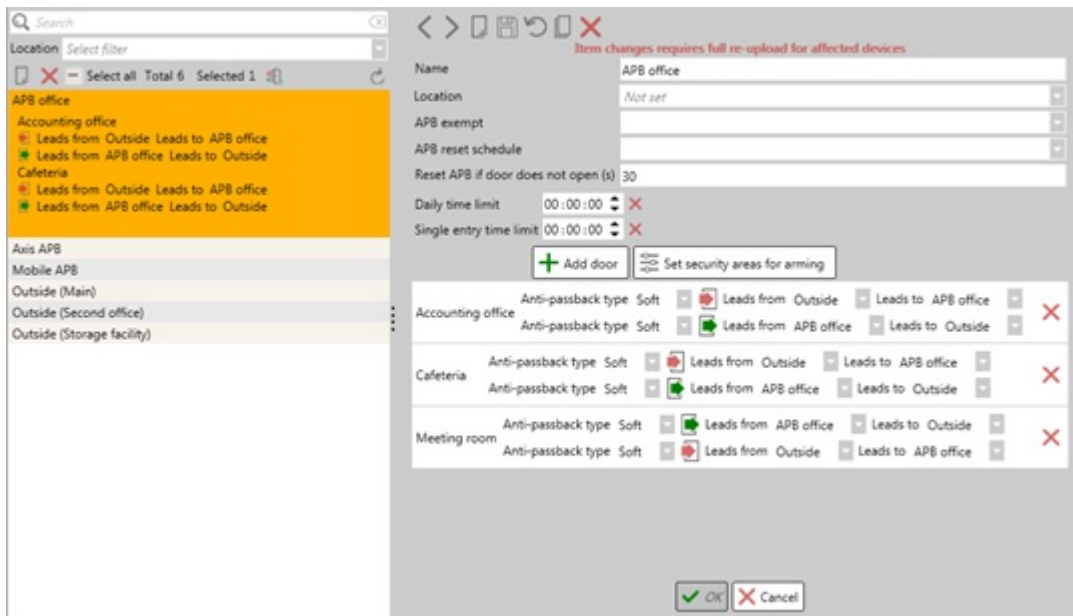


- **Enable (checkbox).** Selects which floors will be allowed to get to with the configured access level.
- **Floor name.** Displays floor name.
- **Lobby floor (select).** Select which floor will act as a lobby floor for the configured access level. This function is only available for Otis elevator configuration.

# 12. APB (Anti-Pass-Back) areas

APB (Anti-Pass-Back) areas are used for identifying how many users are in certain areas and to prevent users from entering or leaving the APB areas several times. As well can be used for generating an alarm or to prevent a user to enter through a door if the user is already registered in the APB area already.

There are built in Outside APB areas for every location. These APB areas cannot be removed or edited. An Outside area is where a user ends up after they have exited an APB area. Though, if a user is inactive for over 48 hours, he will be moved out from Outside area to Unknown.



There are few important rules that have to be known while configuring APB areas:

- Different manufacturer controllers cannot be added to the same APB area. Only one type of manufacturer devices can be in the same APB area.
- Doors which have an exit button, cannot be used for APB areas due that the system can't track if a user has left the area or not.
- About devices and need to know information. Not mentioned manufacturers or device, either does not support APB functionality or is not implemented.
  - **HID.** APB is supported up to 5 HID controllers (per 64 entry readers) through RS-485 cable. Does not allow to have different anti-passback types for one controller, only one type should be used per controller.
  - **Mercury.** APB is supported for EP1501 and EP1502 controllers (16 entry readers). APB only work per controller, as Mercury controllers do not communicate with each other.
  - **Suprema.** Currently not support with Credoid.
  - **Axis.** APB is supported on A1001 Axis controller. APB only works per controller, as Axis controllers don't communicate with each other. Axis controllers do not require a full data upload when APB settings are set, only when removing APB areas, a full upload is required.

## 12.1 List panel

On the list panel, configured and built-in APB areas are displayed. From here, APB can be created and added to the list or removed.

- Search is available only by name.
- APB areas are sorted out by the English alphabet.
- **Reset APB status for all users (button).** Resets all user's APB status, putting them in Unknown area.
- By hovering over an APB area, it displays added doors and directions, which have additional info displayed near them, indicating which reader will lead to a specific APB area. Only 6 rows are displayed and if there are more doors and directions, it won't display all information.

- By selecting one of the APB areas from the list, its information and configuration window is presented on the details panel.

## 12.2 Details panel

On details panel, selected APB areas details are displayed and can be configured.

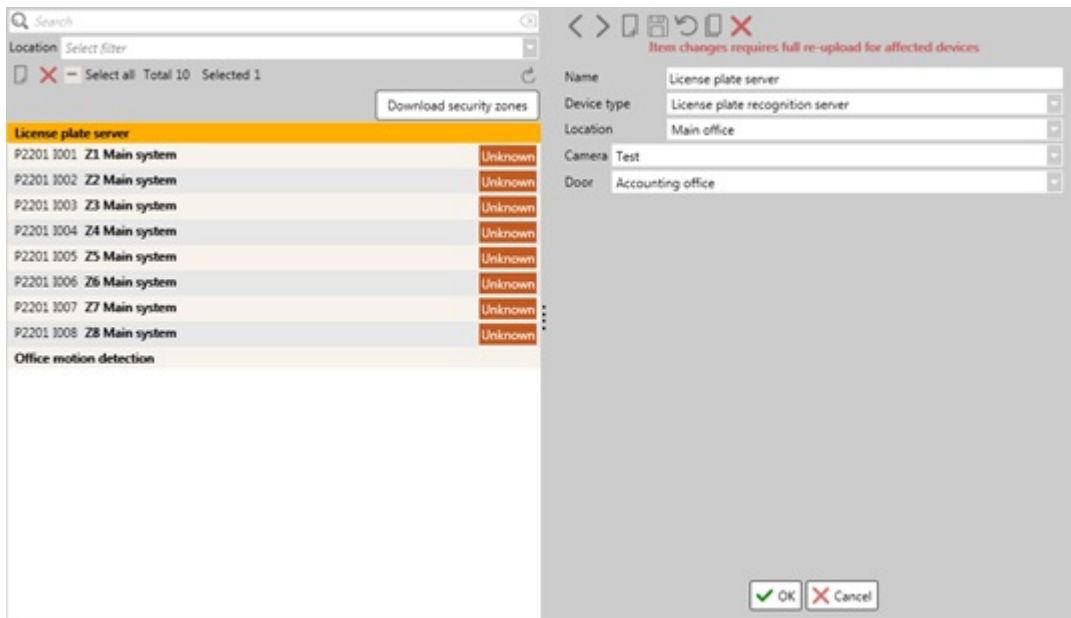
- **Name.** The name of the APB area.
- **Location.** Location is assigned to the APB area.
- **APB exempt.** With a selected access level, users which have the selected access level, will be excluded from this APB areas rules and restrictions. Due of this, a user will be able to enter or leave the APB area for unlimited number of times. Only one exempt access level can be chosen per APB area. Only works with HID and Axis controllers.
- **APB reset schedule.** If a schedule is selected, APB area user count will be reset after a start of a schedule block. Note that for each schedule block, there will be a APB reset. This feature does not work with Axis controllers.
- **Reset APB if door does not open.** If the door is not opened during the specified time interval after a user has presented a credential, the APB is reset for that user. This function only works for HID controllers. Axis has this feature built in and enabled, as APB registered only after a door contact has changed.
- **Daily time limit.** The amount of time a user is allowed to be in the APB area daily. If the daily time is reached, it will generate an alarm event for that user. By the right side, there is a button „Clear“, which sets the time back to 00:00:00.
- **Single entry time limit.** The amount of time a user is allowed to be in the APB area. If the time limit is reached, alarm event is generated for that user. By the right side, there is a button „Clear“, which sets the time back to 00:00:00.
- **Add door (button).** Adds doors to the APB area. Opens an „Add door“ window, where door(s) can be selected and added to the APB area. Only doors from the selected location will be displayed on the list.
- **Set security areas for disarming (button).** Sets security areas for disarming purposes for the APB area. **This function is deprecated.**
- **Door list (field).** Displays doors that are added to the APB area.
  - **Door name.** On the left, displays the added doors name.
  - **Anti-passback type.** Indicates an anti-passback mode for the reader. Full upload to controller, except Axis controllers, is required after changing this setting [\[3.2\]](#) or [\[5.4\]](#). There 3 possible modes.
    - **Soft.** After violation is done by the user, it grants access for the user and generates an alarm event of anti-passback violation.
    - **Hard.** After violation is done by the user, it denies access for the user and generates an alarm event of anti-passback violation.
    - **Disable.** After violation is done by the user, it grants access for the user and does not generate an alarm event of anti-passback violation. This setting does not work for Axis controllers, it will act as **Soft**
  - **Leads from/to.** Indicates from which APB area each reader leads to.
  - **Remove (button).** On the right side of the added door, there is a button which will remove the door from the list.

## 13. Inputs

On Inputs tab, Motion detectors, license plate recognition servers, security zones are reviewed, created, modified or removed. An input sends a signal or data from a device to the CredolD, such as motion detection alarms, security zones statuses, license plate recognition information.

As well, on Inputs tab, security zones are also added, but they cannot be created nor modified by usual means, as they are downloaded from a configured MuSDO devices. Actions, such as Acknowledge, Bypass or Un-bypass can be made on security zones.

Note, that **Weight detector input type is deprecated.**



## 13.1 List panel

On the list panel, downloaded security zones and configured inputs are displayed. From here, inputs can be created and added to the list or removed. As well, it is possible to operate security zones.

- Search is available only by name.
- **Download security zones (button)**. Downloads security zones from MuSDO devices and then refreshes the inputs list.
- Inputs are sorted out by the English alphabet. Note, that security zones are sorted by their device ID.
- Security zones have additional information displays on the list panel:
  - Device ID.
  - Input ID.
  - Input name.
  - Security zone state.
- By selecting one of the inputs from the list, in the details panel its information is presented.

## 13.2 Details panel

On details panel, selected inputs or security zones details are displayed and can be reviewed, configured or actions can be done. Different inputs have different configurable settings, as well depends on the selected controller type.

Note, that security zones settings are not changeable, only certain actions can be made. To configure security zones, it has to be done by connecting to MuSDO device through ASB Securities software WinCSS and from there, configurations can be made [\[5.5.3\]](#).



- **Name**. The name of the input.
- **Device type**. Device type is selected, which determines what kind of input it is.



- **Motion detector & Glass break detector.**
  - Indicates the location that is assigned to the input.
  - **Device IP address.** Indicates the device which will be used for the input. The device is selected from the list. After selecting a device, its IP address will be displayed on this field.
  - **Controller settings (button).** Located on the right side of the **Device IP address** This will redirect to the Device tab and focus on the selected device.
  - **Controller type.** Displays the type of the selected device.
  - **Input address.** Input address has to be selected from the device. The amount of inputs address and their types, depends on the selected controller.
  - **Panel number.** Select a panel from which the inputs will be used. This field is only available for HID devices: VertX V1000 and VertX EVO V1000.
  - **Contact type.** Indicates a resistor type. There are built-in resistor types, that are represented from HID specifications. The built-in resistor types work with HID controllers and some may work with other manufacturer devices. For more information, follow the manufacturers devices brochures.
  - **Contact settings (button).** Located on the right side of the **Contact type** Opens „Input configuration“ window, where built in contact types can be reviewed and custom ones can be created. Built-in contact types are not editable nor cannot be removed.



- **Name.** The name of the contact type.
- **Normal resistance range from & to (Ohm).** Description of the resistance range that the resistor operates while in normal state.
- **Alarm resistance range from & to (Ohm).** Description of the resistance range that the resistor operates while in alarm state.
- **Switch type.** Defines the state the resistor is at the start. This field is not editable, as it displays the state it will have depending the **Normal resistance range from & to (Ohm)** and **Alarm resistance range from & to (Ohm)**
  - **Normally closed.** If there is no current, no alarm is generated. Only after a current is applied, alarm is generated.
  - **Normally opened.** If there is current going through the resistor, no alarm is generated. Only after there is no current, alarm is generated.
- **Supervision type.** Defines inputs supervision type. This field is not editable, as it displays the state it will have depending the **Normal resistance range from & to (Ohm)** and **Alarm resistance range from & to (Ohm)**
- **Weight detector.** This function is deprecated.
- **License plate recognition (LPR) server.**

- **Location.** Location is assigned to the input.
- **Camera.** Select a camera that has LPR functionality.
- **Door.** Select a door that will be operating with the LPR functions.
- **Security Zone.** Security zone inputs can only be configured through WinCCS software. In CredolD, these inputs are added through MuSDO devices, which should have inputs configured on it and connected to CredolD. By clicking on „Download security zones“ button on the List panel, it will

download all security zones from the connect MuSDO devices.

Name: Z2 Main system  
Device type: Security Zone  
Location: Main office  
Device IP address:  
Controller type: MuSDo CCS7000  
Unknown

**Security**

Recall Acknowledge Bypass Un-bypass

**Events**

2017-05-15 17:03:04 Input anti-mask  
2017-05-12 12:20:25 Input anti-mask

**Assigned security areas**

Area 2 Unknown

- **Location.** Location is assigned to the security zone.
- **Device IP address.** Displays MuSDO devices IP address.
- **Controller type.** Displays MuSDO device type.
- **Recall (button).** Recalls / refreshes the security input/zone.
- **Acknowledge (button).** Acknowledges the temper if it is triggered.
- **Bypass (button).** Bypasses the security input/zone.
- **Unbypass (button).** Unbypasses a bypassed security input/zone.
- **Events.** Displays events related to the input/zone.
- **Assigned security areas.** Displays security areas that are assigned to the input/zone.

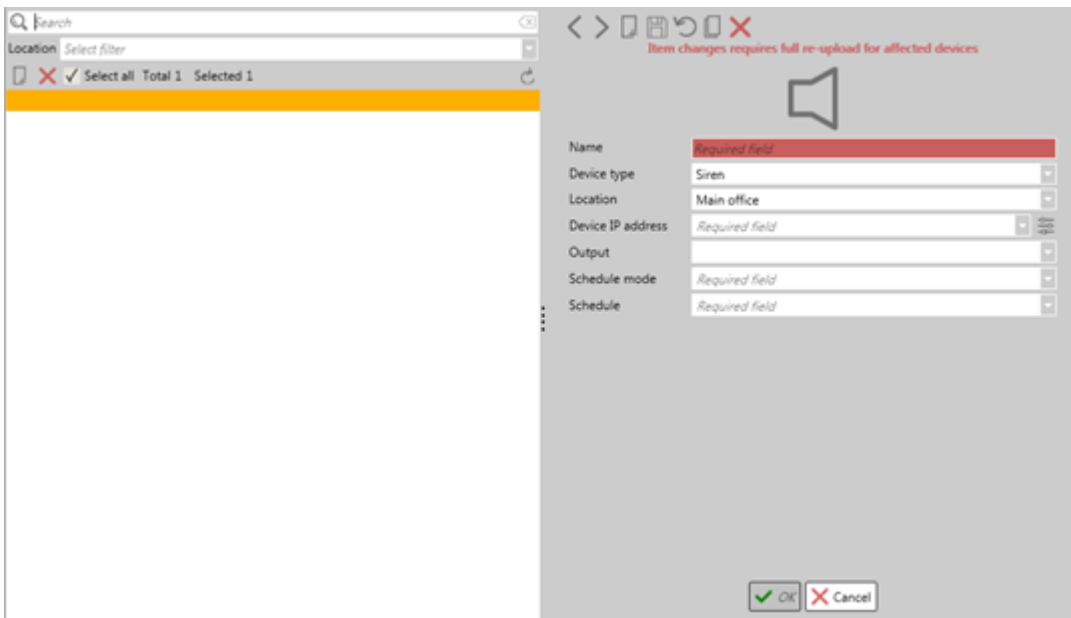
## 14.Outputs

Many devices require a slave module to be able to configure an output. Most built-in outputs in the devices are used for door specific functions (door monitoring, exit button) and due of this, an extension is needed to be able to configured outputs for the devices.

- **HID.** Controllers, such as VertX EVO V2000 or EH400-K, do not need slave devices to be able to configure outputs, with an exception for VertX V1000 and VertX EVO V1000 which require VertX V100 modules.
- **Mercury.** EP1501 controller requires MR16out module to be able to add outputs, while EP1502 has additional built-in outputs (6 outputs in total), that can be used for output configuration without the need for MR16out module, although it can be still be added.
- **Suprema.** All Suprema devices require Secure I/O 2 module to be able to configure outputs.
- **Axis.** Axis can use Auxiliary outputs for output configuration.

Configurable outputs:

- **Output.** A simple output that is used for security alarms, fire alarms or custom output configuration.
- **Weight is OK.** This function is deprecated.
- **Weight is not OK.** This function is deprecated.
- **Trigger.** A trigger output that after a controller receives a specific event(s), it will either open the output for a short time, turns it on or turns it off.



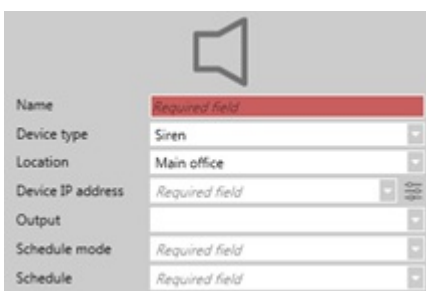
## 14.1 List panel

On the list panel, configured outputs are displayed. From here, outputs can be created and added to the list or removed.

- Search is available only by name.
- Outputs are sorted out by the English alphabet.
- By selecting one of the outputs from the list, in the details panel its information is presented.

## 14.2 Details panel

On details panel, selected outputs details are displayed and can be configured. Different outputs have different configurable settings, as well, it depends on the selected controller type.



- **Name.** The name of the output.
- **Device type.** Device type is selected, which determines what kind of output it is.
  - **Output.**
  - **Trigger.**
- **Location.** Indicates the location that is assigned to the output.
- **Device IP address.** The device that will be used for output configurations. A device is selected from the list. After selecting a device, its IP address will be displayed on this field.
- **Controller settings (button).** Located on the right side of the **Device IP address** This will redirect to the **Device** tab and focus on the selected device.
- **Panel number.** Select a slave device that has output compatibility (HID – VertX V100 module; Mercury – MR16out module; Suprema – Secure I/O 2 module). The slave device has to be connected to the controller and added as a slave device through **Device**
- **Output.** Select relay or auxiliary output that will be used.
- **Schedule mode.** Indicates the state (Activated or Deactivated) of the output during the **Schedule** Only available for Output device type.
- **Schedule.** Select a schedule for the output. During the schedule time, the output will be in state that is

selected on Schedule mode field. During non-schedule time, it will have the opposite state. Only available for Output device type.



Name	Required field
Device type	Arm/disarm trigger
Location	Main office
Device IP address	Required field
Output	
Apply filter	
Action	Pulse
Pulse time (s)	
Wait for	identical events in (s)

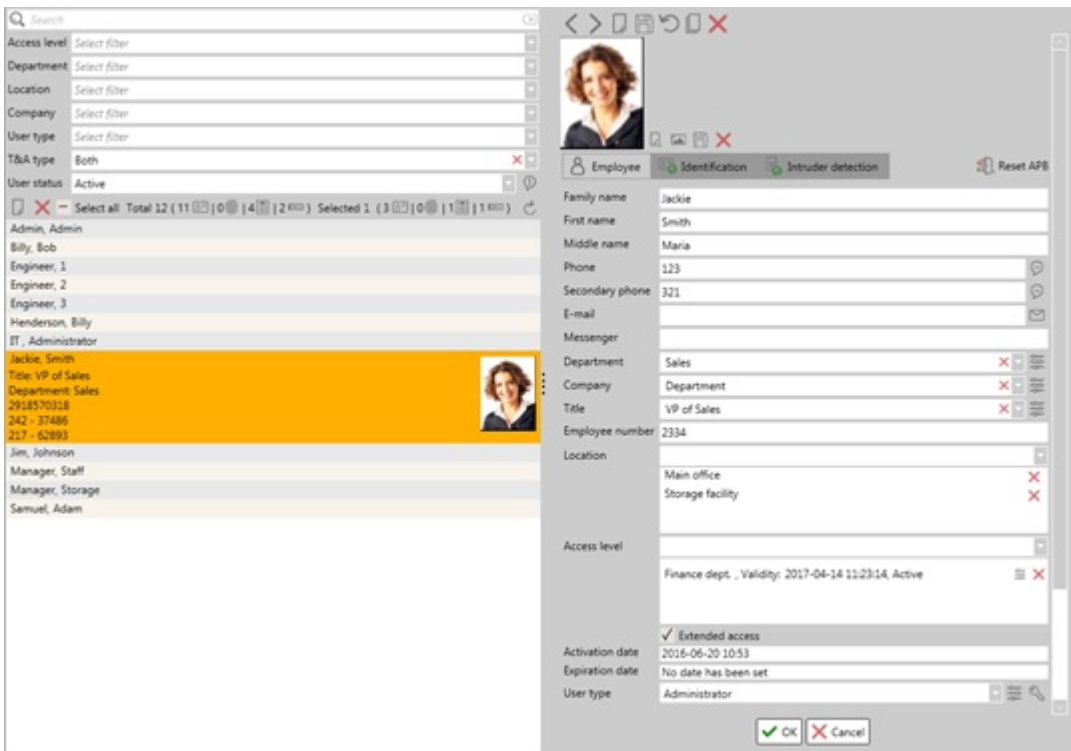
- **Apply filter.** Applies a filter, that after specified events, an action will be taken for the trigger.
- **Create new filter (button).** Opens a „Filter“ window, where a trigger filter can be viewed, created, modified or removed.
- **Edit filter (button).** Opens a „Filter“ window and focuses on the created filter, that was selected on **Apply filter**
- What action should be taken after the output is triggered.
  - **Pulse.** Turns on the output for a duration **Pulse time**.
  - **TurnOn.** Turns on the output.
  - **TurnOff.** Turns off the output.
- **Pulse time.** The time interval the output should be turned if **Pulse** action is done.
- **Wait for.** Indicates how many events it will take for the output to trigger. If the field is left empty, only 1 event will be needed to trigger. Possible to set that after 2 or 3 identical events, the output will trigger.
- **Identical events in.** The duration of time that requires 2 or 3 identical events for the output to trigger. This field is configurable if **Wait for** is set on 2 or 3 events.

## 15. Users

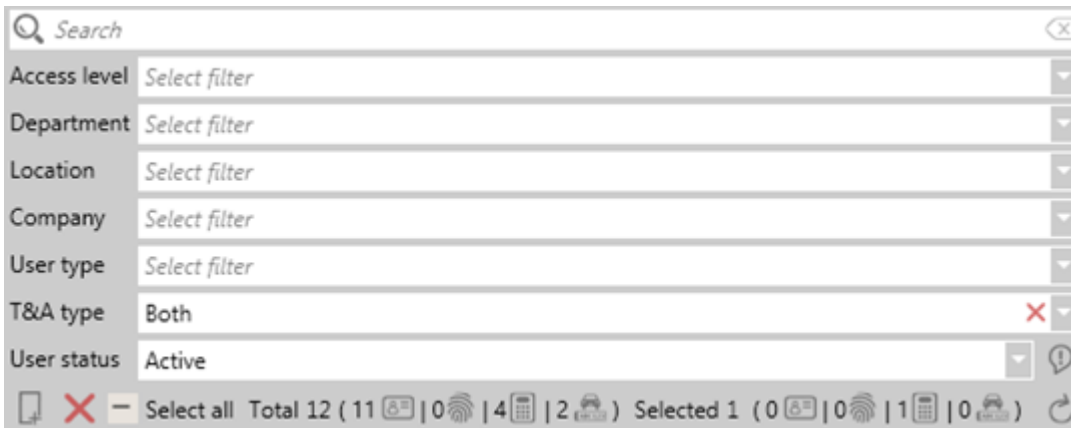
There are many functions that can be done here, concerning user configuration. Created users can be viewed, modified, deactivated or re-activated. Identifications, such as cards, fingerprints, PIN or license plate numbers, can be assigned or removed from the user.

Automatic notifications can also be configured on this tab, which will send a notification (SMS, e-mail, HTTP) after certain events are generated. Automatic notification license is required for this function to work.

By default, an Admin user (Admin Admin) is created in CredoID, with whom first logins to the software can be made. This user cannot be disabled nor removed, will always have **User type** set as **Administrator** and its **User name** for login purposes set as „admin“.



## 15.1 List panel



On the list panel, configured users are displayed, as well displays how many identifications are selected and how many there are in total. Also, it is possible to review information of the selected users, by hovering over a user.

From this panel, users can be created and added to the list, as well can be deactivated or re-activated. Also, automatic notifications can be configured from this panel.

- Search work by:
  - First name.
  - Family name.
  - Middle name.
  - Employee number.
- Users tab contains filter fields, which makes it easier to filter and find users. Users can be filtered by:
  - **Access levels.**
  - **Departments.**
  - **Locations.**
  - **Companies.**
  - **User types.**
  - **T&A types.** There are 3 types of selections for this filter: **Simple**, **Advanced** or **Both**. By default, this filter is set on **Both**.
  - **User status.** There are 3 types of selections for this filter: **Active**, **Deactivated** or **Both**. By default, this filter is set on **Active**.

- **Automatic configuration (button).** Located on the right side of the **User status** Opens „Configuration of automatic notifications“ window, where automatic configurations can be made. For more information, follow Automatic configuration section [15.3].
- **Identification information.** The total and selected identifications types are displayed below the filter fields. The types of identifications that are displayed [15.2.3].
  - Card.
  - Fingerprint.
  - Face recognition.
  - PIN.
  - License plate.
- Users are sorted out by the English alphabet.
- By hovering over a user, small amount of information is displayed:
  - Family and First name.
  - Title.
  - Department.
  - Added cards facility and card number.
  - On the right side, users photo is displayed.
- By selecting one of the users from the list, in the details panel its information is presented.

## 15.2 Details panel


After selecting a user from the List panel or by creating a new one, user’s information is showed on this panel. Here, user configurations can be made, such as details about the user, its location or what access levels it has, expiration date and much more.

In Details panel, user information is divided to 4 sub-panels:



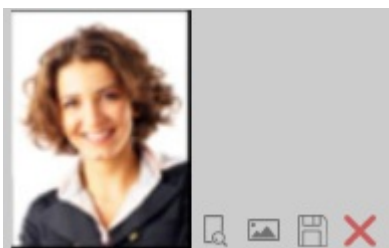
- **Employee.** User configuration settings.
- **Identification.** For adding or removing assigned credentials for the user.
- **Intruder detection.** For specifying security profiles for the user.
- **Billing.** For billing information.

By default, „Employee“ sub-panel is always displayed first until selecting a different sub-panel.




	<p>Reset APB status for this user</p>	<p>Located on the right side of sub-panels. By pressing this button, it will reset APB status for the selected user (it will be in unknown area).</p>
---	---------------------------------------	---

### 15.2.1 User photo configuration

A user photo is not mandatory while creating a user. A user photo aspect has to be 3:4. If the added photo has a different aspect than 3:4, it will fit the photo with the default aspect.



Icon	Name	Description
		<p>Opens a window, where a photo file</p>

	Load photo from disk	can be selected from a folder and assigned to a user. This window also opens up when pressed on the Users photo. Supported formats: PNG, JPG, JPEG, GIF and RMP.
	Capture photo from camera	Opens a window, where a photo can be captured from a device with a camera. More details below.
	Save photo	Saves the photo of the user to a folder with a selected format. If no photo is added to the user, this button is disabled.
	Delete photo	Deletes the photo of the user.

- **Capture photo from camera.** Opens up a window where a photo can be taken from a device that has a camera. If a device is present, it will automatically show a live stream from the camera, unless the camera is already in use. To capture a photo of a user, click **Capture** button.



- **Select video capture device.** A list of connected devices with installed camera. By selecting the camera, it will show live stream on the window and photo then can be taken. By default, the first camera in English alphabetic order is selected first.
- **Live face detection (checkbox).** Enabling this checkbox, CredoID will try to detect faces which helps cropping user pictures. The detection function tries to detect the user's eyes, which will be in displayed in a red box, while a white box surrounds the detected face.



After taking a picture from a camera, the next phase is cropping the picture. Since in most cases,

cameras will take different aspect photos rather than 3:4, it is advised to crop the photo to 3:4 aspect for best results. Especially when not using Live face detection, as then the cropping value would be the size of the photo. If the picture is taken with **Live face detection** function, it will create a crop box around the detected face with 3:4 aspect.

- **Cropping tool.** After taking a photo, a cropping box appears (white box), which indicates the part of the photo that will be used. To adjust the cropping lines, bellow **Select video capture device**, there are settings which moves and sizes the cropping box in pixel format. The crop box can be also moved by clicking and then holding left-mouse button on the crop box and then moving it around.
  - **Left.** How many pixels from the left side of the photo the cropping box should be stationed.
  - **Top.** How many pixels from the top of the photo the cropping box should be stationed.
  - **Width.** The width of the cropping box.
  - **Height.** The height of the cropping box.
- **Crop (button).** Crops the photo, using the crop box.
- **Retry (button).** Goes back to the picture capture section, where a different photo can be taken. The settings in the cropping section are not saved.

After a photo is added, User settings have to be saved.

## 15.2.2 Employee sub-panel

To create a user, 3 main fields has to be filled in: **Family name**, **First name** and **Location**. Other fields aren't mandatory.

### 15.2.2.1 User information fields

Family name	Jackie	
First name	Smith	
Middle name	Maria	
Phone	123456789	📞
Secondary phone	987654321	📞
E-mail	YoutEmail1@domen.com	✉️
Messenger		
Department	Sales	✖️ 📄
Company	Department	✖️ 📄
Title	VP of Sales	✖️ 📄
Employee number	2334	

- **Family name.** Users family name. This field is required to be filled in.
- **First name.** Users first name. This field is required to be filled in.
- **Middle name.** Users middle name.
- **Phone & Secondary phone.** Users phone numbers.
- **Send SMS (button).** Located at the right side of **Phone & Secondary phone** Opens up a window, where it is possible to send a SMS message to a phone number. Note, that Automatic notifications license is required. As well, the equipment is needed that could send a SMS message (modem). Further configurations have to be made in the *Settings* tab, under Notifications module [\[24.4\]](#).

**Send SMS**

Phone

Message

- **Phone.** The phone number to which the SMS message will be sent to. This field is automatically filled in if **Phone** or **Secondary phone** fields are configured (depending on which **Send SMS** button is pressed).
- **Message.** The message that will be sent to the phone number. Note, that the maximum length of



characters in the SMS message is 160. If Unicode is used, maximum characters for a SMS message is about 70.

- **E-mail.** Users e-mail address. An email address must be: [symbols]@[symbols].[symbols≤6] (example: YourEmail1@domen.com). Multiple e-mail address can be assigned to a user, by separating them with a comma.
- **Send E-mail (button).** Located at the right side of **Send E-mails** Opens up a window, where it is possible to send an e-mail message manually. Note, that Automatic notifications license is required and e-mail notification settings have to be configured in the Settings tab, under Notifications module [\[24.4\]](#).

- **E-mail.** The e-mail address to which an e-mail will be sent to. This field is automatically filled in if **E-mail** field is configured.
  - **Subject.** The subject of the e-mail. This field is not mandatory to fill.
  - **Message.** The message that will be sent to the e-mail address.
  - **Signature.** Indicates the signature that will be added to the e-mail.
- **Messenger.** Additional field, which is used to indicate different ways of communicating with the user.
  - **Department.** Select a configured department. Departments are created, modified or removed in the Department configuration window, which is reachable by clicking on **Department configuration** button, located on the right side of the **Department** field.
  - Select a configured company. Companies are created, modified or removed in the Company configuration window, which is reachable by clicking on **Company configuration** button, located on the right side of the **Company** field.
  - Select a configured title. Titles are created, modified or removed in the Title configuration window, which is reachable by clicking on **Title configuration** button, located on the right side of the **Title** field.
  - **Employee number.** Users unique employee number. It is not possible to enter an employee number that is already entered on another user.

## 15.2.2.2 User access levels and dates

Location	Main office	X
	Storage facility	X
Access level	Finance dept. , Validity: 2017-04-14 11:23:14, Active	X
	Production dept. , Validity: 2017-05-10 15:14:02, Active	X
	✓ Extended access	
Activation date	2016-06-20 10:53	
Expiration date	No date has been set	

- **Locations.** Assign location(s) to a user. At least 1 location has to be assigned to a user to be able to save settings.
- **Access level.** Assign access levels to a user. Assignable access levels depend on assigned location(s) to the user. By default, it is allowed to select Everywhere or Nowhere access levels per location. By assigning any of the default access levels (Everywhere or Nowhere), it will remove all of the access levels (from that location) in the process that are assigned to the user. **Validity** of the access level is displayed near the assigned access levels, displaying:
  - Date and time when the access level starts to be active. By default, displays the date and time when the access level is assigned.
  - Expiration of access level date and time.

- Remaining use limit of access level.
- Status of access level: Active, Inactive, Expired.
- **Access level configuration (button).** This button is located on the right side of assigned access levels in the **Access level** field, which opens **Access level configuration** window.

- **Status.** Displays access levels current status: Active, Inactive, Expired, Waiting for approval. As well, it can force the access level to be in either Active or Inactive state. This also updates its status in the **Access level** field.
- **Activation & Expiration time.** Indicates the time (hh:mm) when the access level starts to be active and when it expires.
- **Calendar.** Indicates the dates when the access level starts to be active and when it expires. If expiration date is not set, access level won't expire. If the expiration date is already expired, it will present a warning underneath the expiration calendar.
- **Clear (button).** Clears expiration date and time.
- **Use limit.** Indicates how many times a user can go through an access level. After a limit has been reached, the access level for that user becomes inactive. Note, that this is a dynamic field, meaning that the limit number decreases each time a user passes with the access level. There are 3 states **Use limit** can have:
  - **Not set.** If nothing is written in the **Use limit** field, there won't be any limit.
  - **Enabled.** If a limit is set.
  - **Reached.** When the limit has reached zero.
- **Reset at midnight.** Resets the limit number, that is written on the field next to it, at midnight. If no number is written, it does not reset the limit at midnight.
- **Supervisor approval.** Configured access level for the user will be disabled until a host has approved of it. An e-mail is sent to the selected host, which have **Administrator** user type, where a host receives a detailed information of the user and links to either approve or deny the request. Until that, the access level state will be **Waiting for approval**.
- **Extended access (checkbox).** When a credential is presented by the user on the reader who has **Extended access** enabled, the door will operate using the **Extended time**, rather than the **Strike time**. The time interval depends on the configured door.
- **Activation date.** Indicates the date and time when the user starts to be active. By default, when a user is created, **Activation date** is set the moment it was created
- **Expiration date.** Indicates the date and time when the user expires. By default, a user does not have an expiration date when created, it is set as "No date has been set". When clicked on the field, it will generate an expiration date and time the moment when it was done. Note, that expired users are moved to deactivated state.

### 15.2.2.3 User type and login configuration

User type identifies user's permissions when it is logged in to CredoID, such as: what menu tabs are enabled, if a user can read or edit fields. By default, when a user is created, it is given a built-in User type "**User**", which have very limited permissions. Only built-in admin user (Admin Admin) has a default User type "**Administrator**" and it is unchangeable.

When a user is created, it does not have login credentials. User login credentials are created in Login details configuration window. Only built-in admin user (Admin Admin) has a built-in login credentials (**User name**: admin; **Password**: admin). Its **User name** is unchangeable, but **Password** is configurable. It is recommended to change the password for the Admin Admin user when CredoID is installed for security

reasons.

- **User type.** Indicates a User type that is assigned to user. By default, User type “**User**” is assigned to a user when it is created. There are already built-in User types that can be assigned to users: Administrator, System operator, User, User administrator and Visitor. User types can be created in **User types configuration**
- **Configure user types (button).** Located on the right side of the **User type** Opens User type configuration window, where user types can be viewed, created, modified or removed. There are built-in user types which are used on every location and can be viewed, but cannot be modified nor removed:



- **Administrator.** Can read & write everything.
- **System operator.** Can read & write everything, except Doors and APB areas.
- **User.** Do not have any permission (everything is set on None).
- **User administrator.** Have permissions to read & write Access levels, Users, Time & attendance, Card design and Locations.
- **Visitor.** Do not have any permission (everything is set on None). This type is assigned to visitors by default.
- **Configure user login details (button).** Located on the right side of the **Configure user types** Opens Login details window, where **User name** and **Password** can be configured for a user. By default, only admin user (Admin Admin) has a built-in login credentials. Every user has to have a unique user name if multiple logins are created.

## 15.2.2.4 Time & attendance type and additional information









On this section, Time & attendance type can be selected for a user, as well additional information can be written down, which will be displayed on the events.

- **T&A type.** Indicates what type of time & attendance type a user uses. The type indicates which schedules it will use for T&A calculations. There are two types:
  - **Simple.** Uses schedules from **Schedule** tab [9]. A schedule is selected from **Work schedule** field.
  - **Advanced.** Uses schedules from **Time and Attendance** tab [22]. When this type is assigned to a user, the user can be seen in the Time and attendance tab, where schedules can be assigned to him.

- **Work schedule.** Assign a schedule, that are from **Schedules** tab, to a user. This field only appears if **T&A type** is selected as **Simple**.
- **Additional field #1 & #2.** Information fields, that can be displayed on events. Only 60 symbols can be entered in the field.
- **Additional field #3.** Information field, that is only displayed on **User** tab.

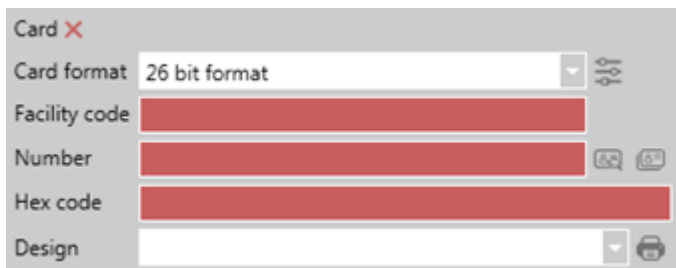
### 15.2.3 Identification sub-panel

Identifications, such as cards, fingerprints, PIN numbers and license plate numbers can be created and added to a user in **Identification** sub-panel. When creating identifications, they are placed in sets, containing one of each identification and called "ID set [number]". Identification or a full set can be removed by clicking on "Remove" button.

Icon	Name	Description
	Card	An icon, symbolizing a card identification. By clicking on "Add new card" button (  ) , it will create a new card identification.
	Fingerprint	An icon, symbolizing a fingerprint identification. By clicking on "Add new fingerprint" button (  ) , it will create a new fingerprint identification.
	PIN	An icon, symbolizing a PIN identification. By clicking on "Add new PIN" button (  ) , it will create a new PIN identification.
	License plate	An icon, symbolizing a License plate identification. By clicking on "Add new license plate" button (  ) , it will create a new license plate identification.

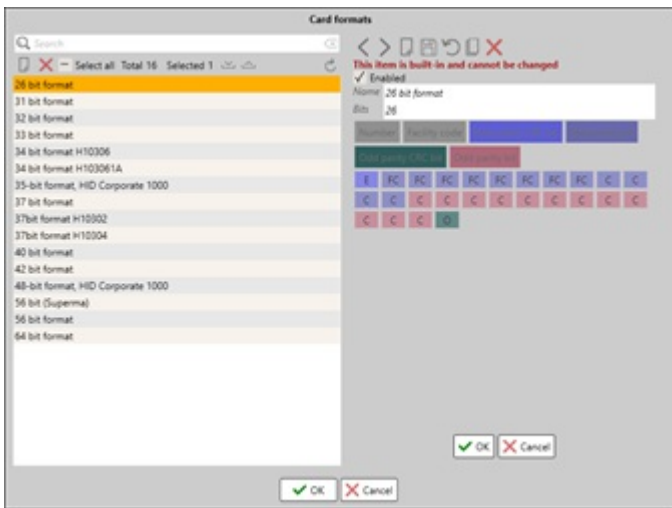
If there are fields that are not filled in, but they required to be, additional identifications cannot be added until those fields are filled in or the identification is removed.

#### 15.2.3.1 Card identification and card formats



Card can either be added manually or by scanning it from a device. Configured cards cannot be modified, only can be printed out or removed.

- **Card format.** Indicates the card format, which is either assigned automatically when a card is added by scanning from a device or is manually set adding a card manually. By default, there are many built-in card formats, but only 4 are enabled by default: 26, 32, 47 and 56-bit formats. Additional formats can be enabled in **Card formats**
- **Configure card format (button).** Opens **Card formats** window, where card formats can be viewed, created, modified or removed. By default, there are many built in card formats that can be used, but they are not editable nor they can't be removed, only enabled or disabled.



On the list panel (left side), it displays created card formats and simple functions can be made, such as creating new formats or removing selected ones. As well, it is possible to import (📄) and export (📤) card formats in .xml file.

On the details panel (right side), card formats are configured and modified.

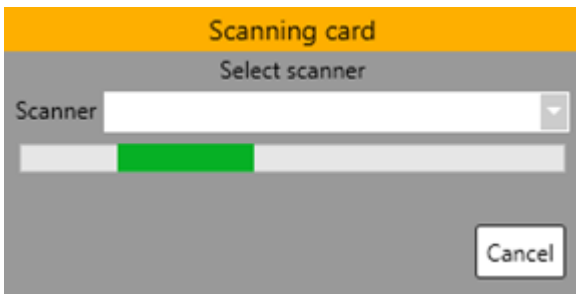
- **Enabled.** Enable or disable the card format. By enabling a card format, it will show upon **Card format** list and cards with such formats will be allowed to be assigned to users. Disabled card formats are not allowed to be assigned to users. If a card format is being disabled while assigned cards are using the formats, it will present a warning message, indicating how many cards will be effected after the card format is disabled. The effected cards will be removed from the users.
- **Name.** Name of the card format.
- **Bits.** How many bits the card format will use. The amount of entered bits will be represented as Bit blocks down below.
- **Number.** The bits that indicates which will be used as a card number.
- **Facility code.** The bits that indicates which will be used as a facility code numbers.
- **Convert to decimal (checkbox).** Received bits are converted to decimal format.

A parity bit, such as **Even parity bit** and **Odd parity bit**, are used as a very simple quality check for the accuracy of the transmitted binary data. The designer of the format decides if each parity bit should be even or odd. A selected group of data bits will be united with one parity bit, which are leading **Even parity CRC bit** and **Odd parity CRC bit**, and the total number of bits should result in either an even or odd number.

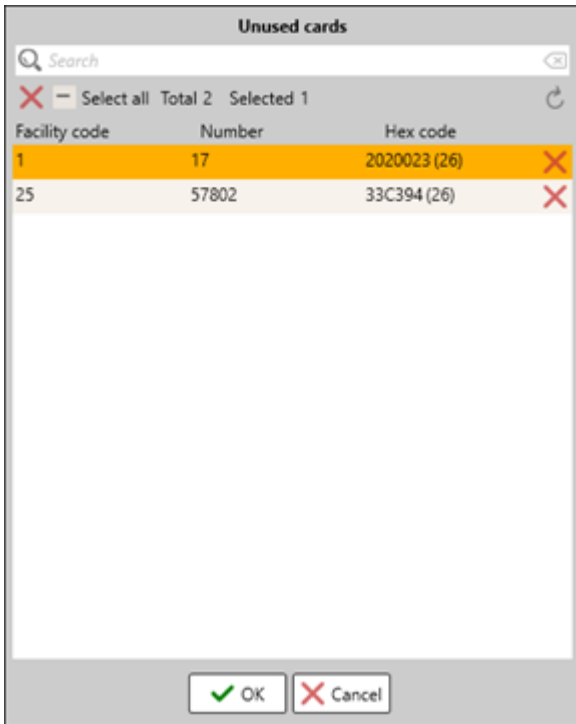
For more information on card formats and how they are created, please follow HID's "Understanding Card Data Formats" manual (link below):

[https://www.hidglobal.com/sites/default/files/hid-understanding\\_card\\_data\\_formats-wp-en.pdf](https://www.hidglobal.com/sites/default/files/hid-understanding_card_data_formats-wp-en.pdf)

- **Facility code.** Indicates the cards facility code number. This field is not displayed if a card format does not have facility codes configured. After entering facility code, hex code is generated/updated. The maximum facility code number that can be entered is the  $2^x$ , where x stands for the number of bits that are assigned to it (8 bits assigned, in total 255 numbers starting from 0).
- **Number.** Indicates the cards number. After entering a card number, a hex code is generated/updated. The maximum card number that can be entered is the  $2^y$ , where y stands for the number of bits that are assigned to it (8 bits assigned, in total 255 numbers starting from 0).
- **Get number from scanner (button).** Button located on the right side of **Number** By clicking on this button, it will open **Scanning card** window. In the **Scanner** field, a device is selected that can scan cards and scanning process starts. After a successful scan, the window closes and the card information will be saved automatically. If there is an error or a timeout, a warning message is displayed and the window is closed.



- **Select a number from the list of unused cards (button).** Button located on the right side of **Number**. By clicking on this button, it will open **Unused cards** window. Here, unused cards can be added to the user. Unused cards are generated after an unregistered card is scanned by a device and it is registered in the **Monitoring** tab. By adding a card from the list, the window closes and the card information will be saved automatically.






- **Hex code.** Cards hex number, which is sum of a facility code and card number. While writing a Hex code, it will constantly update Facility code and Card numbers. It is not recommended to fill in Hex code first while a card format has a facility code as it might generate incorrect numbers.
- **Design.** Select a card design for a card, that are configured on Card design tab [21].
- **Print card (button).** Located on the right side of the **Design** field. After selecting a card design from **Design** field, a configured design can be printed on the card. After clicking on the button, it will open a review image (as .xps file) of the card with the implemented information (First name, Family name, Card number...), depending on the configured design. After that, printing can be done.

### 15.2.3.2 Fingerprint identification



To add a fingerprint, a fingerprint scanner is required to be connected to CredolD or if it is a USB fingerprint scanner, it only has to be connected to the system. It is possible to add 2 fingerprint templates per fingerprint identification.

Icon	Name	Description

	Fingerprint status	Identifies if a fingerprint is assigned or not.
	Scan fingerprint	Opens Scanning fingerprint, where a device can be selected from a list and a fingerprint can be scanned and assigned. After presenting a fingerprint with a successful scan, another scan must be done to confirm the save.
	Remove	Removes an assigned fingerprint from the template.

**Trigger duress alarm (checkbox).** By checking this box for a fingerprint template, when that fingerprint is registered in the system, it will generate an alarm. This should be placed only on 1 fingerprint template per fingerprint identification.

If an error appears during a fingerprint scan, the scan will be canceled and the Scanning fingerprint window will close. Scanning might instantly fail either when opening Scanning fingerprint window or by selecting a device. This can happen due of these reasons:

- Unstable connection with the device.
- The device is disabled.
- Hardware issues.

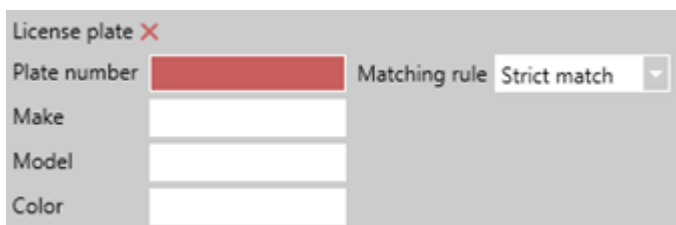
### 15.2.3.3 PIN identification



A PIN identification is entered for a user. The PIN numbers are written in the **PIN** and **Reenter PIN** fields. The maximum length of a PIN number can only be 6 digits.

Settings are not allowed to be saved if PIN numbers in the **PIN** and **Reenter PIN** fields are entered incorrectly or the entered PIN number is already registered in the database.

### 15.2.3.4 License plate identification



While configuring license plate identification, **Plate number** and **Matching rule** are the main fields that has to be configured, while other fields are informational.

- **Plate number.** The license plate number of a vehicle. If a license plate number is entered that is already registered in the database, it will open a window, displaying to which user the license plate number is assigned to and if an override should be made. Maximum length of a Plate number is 10 symbols.
- **Matching rule.** Indicates a matching rule for the license plate.
  - **Strict match.** The license plate has to match 100%.
  - **Letters and numbers only.** Orthodox symbols are removed from the plate number on events and during checking.
  - **Accept wildcards.** Accepts part of a license plate number (example: license plate number – UPS 865321. UPS is the wildcard).
- **Make.** Car manufacturer name.
- **Model.** Car model name.

- **Colors.** Cars color.

## 15.2.4 Intruder detection sub-panel



User security profiles are used with MuSDO devices. A security profile is created in the **Security profile** tab with specific rules to access a security area. **This function is deprecated.**

- **User security profile.** Select a security profile that a user will be using. Only 1 security profile can be assigned per user. Security profiles are created in the **Security profiles**
- **Security areas.** Assign security areas to which a user can operate with the security profile.

## 15.2.5 Billing sub-panel




Billing information for the user is described here. This information is presented in the Billing reports [\[23.8\]](#).

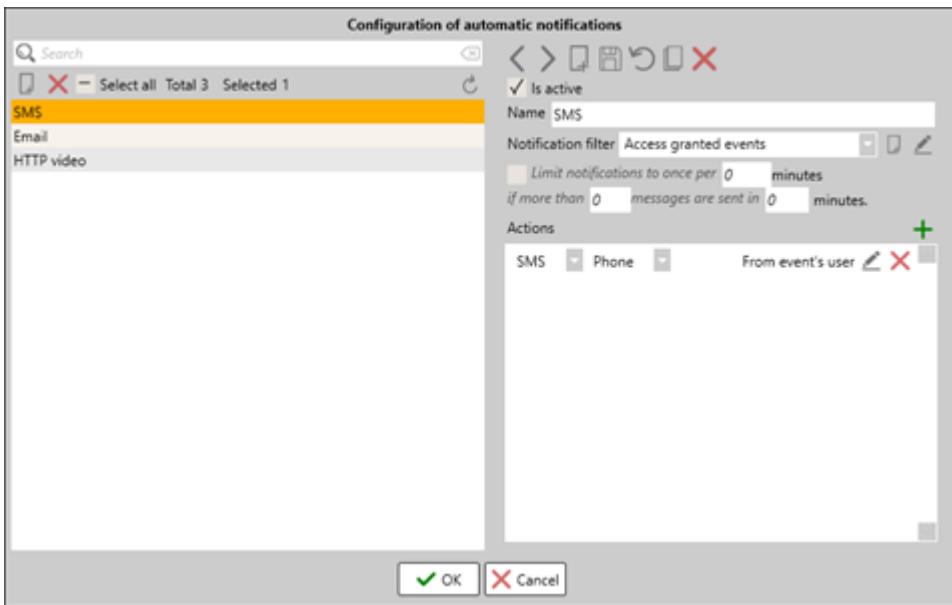
- **Contact number.** Indicates users contact number.
- **Contract date.** Indicates the date when the users had signed the contract. This opens a calendar where a date is selected.
- **Payment condition.** Payment conditions can be described here.

# 15.3 Automatic notifications

Automatic notifications are configured through **User** and **Settings** tabs [\[24.4\]](#), as well it is necessary to have Notifications license. After notifications have been configured on Notifications module, further configurations can be made in **Users** tab.

To access Configuration of automatic notifications window, click on automatic notifications button  located on the List panel [\[15.1\]](#).





On the list panel, notifications can be created, modified or removed. By selecting a created notification, its details are presented on the details panel. To configure a notification, **Name**, **Notification filter** and **Actions** have to be configured correctly.

- **Is active (checkbox).** If the box is checked, the notification will be enabled.
- **Name.** The name of the notification.
- **Notification filter.** Select a filter from a list which indicates when the notification will trigger. Notification filters are created by clicking on “**Create new filter**” button, which opens a filter window [25.1].
- **Create new filter (button).** Located on the right side of the **Notification filter** Opens a notification filter window, where filters for notifications can be created, modified or removed.
- **Edit filter (button).** Located on the right side of the **Create new filter** Opens a notification filter window with the selected filter from the **Notification filter** field.
- **(1- enable checkbox) Limit notification to once per (2 – field) minutes if more the (3 – field) messages are sent in (4 – field) minutes.** Limits the number of notifications that are received.
- **Add new item to list (button).** Located above the **Action** Adds a new action to the Action list. By default, when an action is added, it is set as an SMS notification by default.
- **Action field.** Displays created action notifications. It is possible to modify and remove the added action notifications. An action notification consists of three parts:
  - **Notification type.** Select a notification type that will be used for this action (SMS, E-mail, Video server, HTTP://).
  - **Receiver information.** Select a receiver information, to whom the notification will be sent to (Phone, secondary phone, E-mail, configured video servers or custom). This field is not present when HTTP:// notification type is selected. If a custom type is selected, a new field appears near the **Notification action message** button, where a custom receiver’s information has to be written down.
  - **Notification action message (button).** Opens “Edit notification action message” window, where the message that will be sent can be configured.



- **Message.** The message that will be sent to the receiver. A custom message can be written down, as well it is possible to send information about the received events, user details and reader information.
- **Event fields.** Select event information that will be send to the receiver. By selecting an information type, it will be added to the Message field (example, %EventTime%).
- **User fields.** Select user information that will be send to the receiver. By selecting an information type, it will be added to the Message field.
- **Reader fields.** Select reader information that will be send to the receiver. By selecting an information type, it will be added to the Message field.

## 16. Visits

On Visits tab, created visitors can be viewed, created, modified or removed. Unlike users, visitors have limited permission, requires host user and has to be approved by the administrators or monitoring users to become active and receive certain permission. Visitors configuration process is similar to user's configuration.

Name	ID number	Activation date
3 Engineer ( 879879 564456 )	2017-04-19 11:16:35	Registered
Name Name ( Admin Admin )	2017-05-12 14:34:44	Registered

### 16.1 List panel

On the list panel, configured visitors are displayed. From here, visitors can be reviewed, created and added to the list or removed. By selecting one of the visitors from the list, in the details panel, its information is presented.

- Search is available by visitors First name, Family name, Host name and ID number.
- Visitors are sorted out by the English alphabet.

On the list field, created visitors are presented with an additional information:

- Visitors First and Family name.
- The assigned hosts First and Family name.
- The date and time the visitor is activated.
- The visitors state.
  - **Registered.** A visitor that has been recently created. In this state, the visitor is inactive until it has been approved.
  - **Approved.** A visitor that is approved, will be active until **Duration** time.
  - **Canceled.** The visitor becomes inactive after the visitor has been canceled.
  - **CheckIn.** Indicates that the visitor has checked in. This is done through CredolD GUI after a visitor has been approved. Does not change any credentials.
  - **CheckOut.** Indicates that the visitor has checked out and becomes inactive.
  - **TimeExceeded.** Indicates that the visitors time has been expired. This does not make the visitor

inactive.

- **NoShow.** Indicates that the visitor did not checked in nor checked out during after the **Duration** time has been expired.

## 16.2 Details panel

After selecting a visitor from the List panel or by creating a new visitor, visitor's information is presented on this panel. Here, visitor's configurations can be made, similar to user configuration, such as details about the visitor, access levels it has, activation and expiration dates.

Visitor information is divided to 2 sub-panels:



- **Visitor.** Visitor configuration settings can be made here.
- **Identification.** For adding or removing assigned credentials to the visitor.

A photo can be assigned to a visitor, though, it is not mandatory while creating a visitor [\[15.2.1\]](#).

Identification sub-panel works the same as in the User tab [\[15.2.3\]](#).

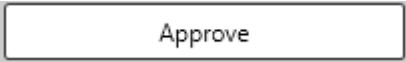
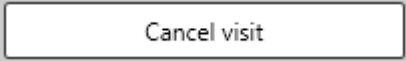

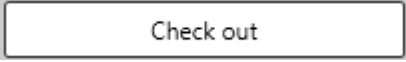
### 16.2.1 Visitor sub-panel

To create a user, 7 main fields has to be filled in: **Host**, **Document type**, **ID number**, **Family name**, **First name**, **Location** and **Access level**. Other fields are not mandatory to be filled in to be able to save visitor settings.

The screenshot shows a form with the following fields: Host (dropdown, Required field), Document type (dropdown, Required field), ID number (text input, Required field), Family name (text input, Required field), First name (text input, Required field), Phone (text input), Secondary phone (text input), E-mail (text input), Location (dropdown, No locations are assigned), Access level (dropdown, No access levels are assigned for this user), Activation date (text input, 2017-06-05 16:27), Duration (text input, 2017-06-05 17:27), and Remarks (text area).

- **Host.** Select a host (user), to whom the visitor is assigned to visit. This field is mandatory.
- **Document type.** Select a configured document type for a user, describing the ID number. This is an information field, which describes the visitors ID number type (example: pass number, vehicles license plate, custom ID). Document types are configured by clicking on the "**Configure document type**" button, located on the right side of the **Document type**. This field is mandatory.
- **ID number.** The assigned visitors ID number. It represents an ID number depending on the **Document type**. This field is mandatory.
- **Family name.** Visitors family name. This field is mandatory.
- **First name.** Visitors first name. This field is mandatory.
- **Phone & Secondary phone.** Visitors phone numbers.
- **Send SMS (button).** Located at the right side of **Phone** & **Secondary phone**. Opens up a window, where it is possible to send a SMS message to a phone number [\[15.2.2.1\]](#). Note, that Automatic notifications license is required. As well, the equipment is needed that cab send a SMS message (modem). Further configurations have to be made in the *Settings* tab, under Notifications module [\[24.4\]](#).

- **E-mail.** Visitors e-mail address. An email address must be: [symbols]@[symbols].[symbols≤6] (example: YourEmail1@domen.com). Multiple e-mail address can be assigned to a visitor, by separating them with a comma.
- **Send E-mail (button).** Located at the right side of **Send E-mails** Opens up a window, where it is possible to send an e-mail message manually [15.2.2.1]. Note, that Automatic notifications license is required and e-mail notification settings have to be configured in the Settings tab, under Notifications module [24.4].
- **Locations.** Assign a location(s) to a visitor. At least 1 location has to be assigned to a visitor to be able to save settings. This field is mandatory.
- **Access level.** Assign access levels to a visitor. Assignable access levels depend on assigned location(s) to the visitor. By default, it is allowed to select Everywhere or Nowhere access levels per location. By assigning any of the default access levels (Everywhere or Nowhere), it will remove all of the access levels (from that location) in the process that are assigned to the visitor. **Validity** of the access level is displayed near the assigned access levels, displaying:
  - Date and time when the access level starts to be active. By default, displays the date and time of the **Activation date**.
  - Expiration of access level date and time, which by default is **Duration**
  - Status of access level: Active, Inactive, Expired.
- **Activation date.** Indicates the date and time when the visitor starts to be active. By default, the activation date is set when a visitor is created.
- **Duration.** Indicates the date and time when the visitor access levels expire. After Duration time has expired, access levels and identifications become inactive.
- **Remarks.** An informational field.

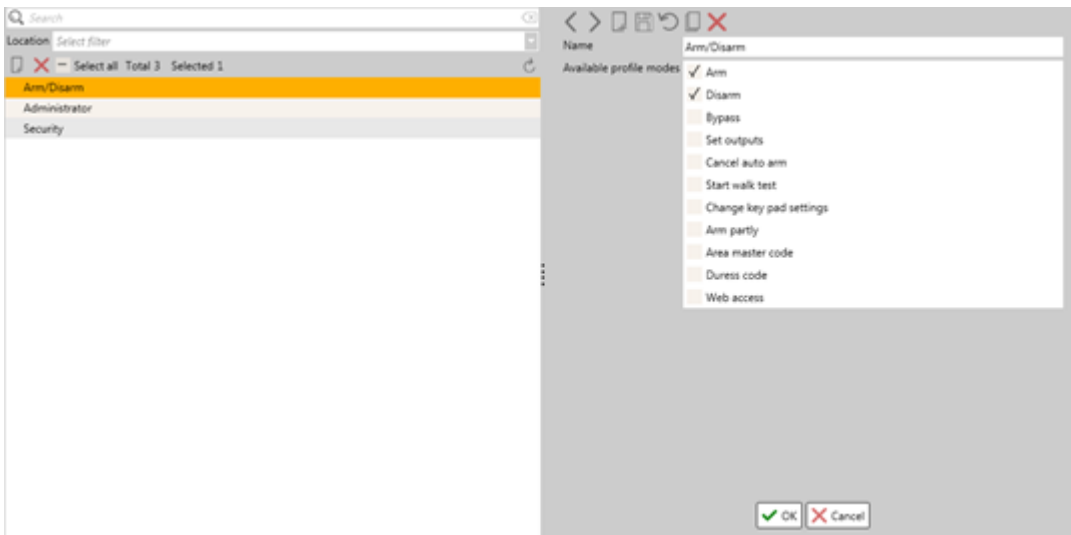
Moderator buttons	Description
	Activates the visitor, moving it from "Registered" status to "Approved", enabling visitors access levels and identifications. After the visitor has been approved, this button is disabled and "Check in" button becomes enabled.
	Cancels the visit, disabling visitors access levels and identifications. This function can be done at any time.
	Indicates that the visitor has checked in to the moderator. This button is only available after the user has been approved.
	Indicates that the visitor has checked out to the moderator. This button is only available after the user has been checked in.

Note, that if visitor mandatory settings are modified (Host, Document type, ID number, Family name, First name, Location and Access level) while the visitor is in **Approved** state, the visitor will be moved to **Registered** state, which makes the visitor inactive. This also applies to other visitor settings, but only when those fields have information typed in them. While modifying empty fields or applying a photo for a user, which wasn't added before, won't change visitors state.

## 17. Security profiles

**This function is deprecated.**

On Security profiles tab, certain profiles are created with selected modes. Created profiles can be added to users in User tab, under Intruder detection sub-panel [15.2.4]. Depending on security profiles configurations, users are able to configure security areas with the profile they are given. This tab is only used with MuSDO device.



### List panel:

- Security profiles can be viewed, created or removed.
- Search is available only by name.
- Security profiles are sorted out by the English alphabet.

### Details panel:

Security profile configurations are done on details panel.

- **Name.** The name of the security profile.
- **Available profile mode.** Indicates modes the profile can have, which indicates which modes user will be allowed to have.
  - Arm;
  - Disarm;
  - Bypass;
  - Set outputs;
  - Cancel auto arm;
  - Start walk test;
  - Change key pad settings;
  - Arm partly
  - Area mater code;
  - Duress code;
  - Web access.

## 18. Security areas

Configured security areas can be viewed and changes to the areas can be made. On this tab, it is possible to arm and disarm security areas and view event history.

Security areas are configured through ASB Security software WinCCS. After security areas have been configured on MuSDO device, security areas can then be downloaded from MuSDO devices and further configurations can be made on CredolD.

### 18.1 List panel

On the list panel, downloaded security areas are displayed. From here, security areas can be reviewed and actions can be made, such as to arm or disarm a security area.

- Search is available only by name.
- Security areas are sorted out by the devices ID number.

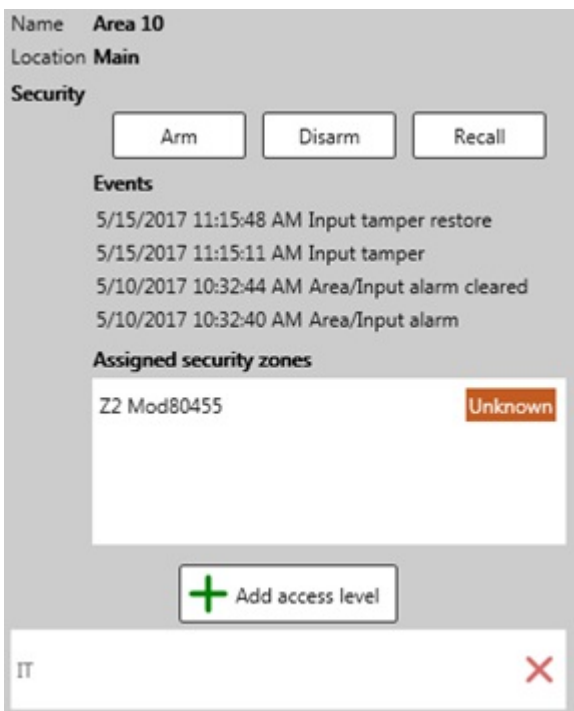
- Additional security area information is displayed on the list: Device IP, Security area number, Security area name and the state of the security area.
- By selecting one of the security areas from the list, its information is presented on the Details panel.



- **Download security areas (button).** Downloads security areas from connected MuSDO devices and adds them to the security area list. As well refreshes the current list.
- **Arm (button).** Arms the selected security area. It is possible to arm multiple security areas by selecting multiple security areas from the list and clicking on this button.
- **Disarm (button).** Disarms the selected security area. It is possible to disarm multiple security areas by selecting multiple security areas from the list and clicking on this button.

## 18.2. Details panel

On details panel, selected security areas details are displayed and further configurations can be made.



- **Name.** Displays the name of the security area. The name of the security area is configured on MuSDO device itself, through WinCCS software.
- **Location.** Displays the location it is assigned to.
- **Arm (button).** Arms the selected security area.
- **Disarm (button).** Disarms the selected security area.
- **Recall (button).** Refreshes the status of the security area.
- **Events.** Displays events related to the security area.
- **Assigned security zones.** Displays security inputs/zones that are assigned to the security area.
- **Add access level (button).** Add an access level to the security area. The selected access level will be linked with the security area, meaning that when the security area is armed, the access level is disabled. Disarming the security area, will re-enable the access level. Only 1 access level can be assigned per security area. The assigned access level is displayed below the button. **This function is deprecated.**

Every security areas status has their own color representing then, which are presented on the List panel and on Monitoring tab.

- **Armed** state is displayed in a **green** background.
- **Disarmed** state is displayed in a **blue** background.
- **Alarmed** state is displayed in a **red** background.
- **Temper** state is displayed in an **orange** background.

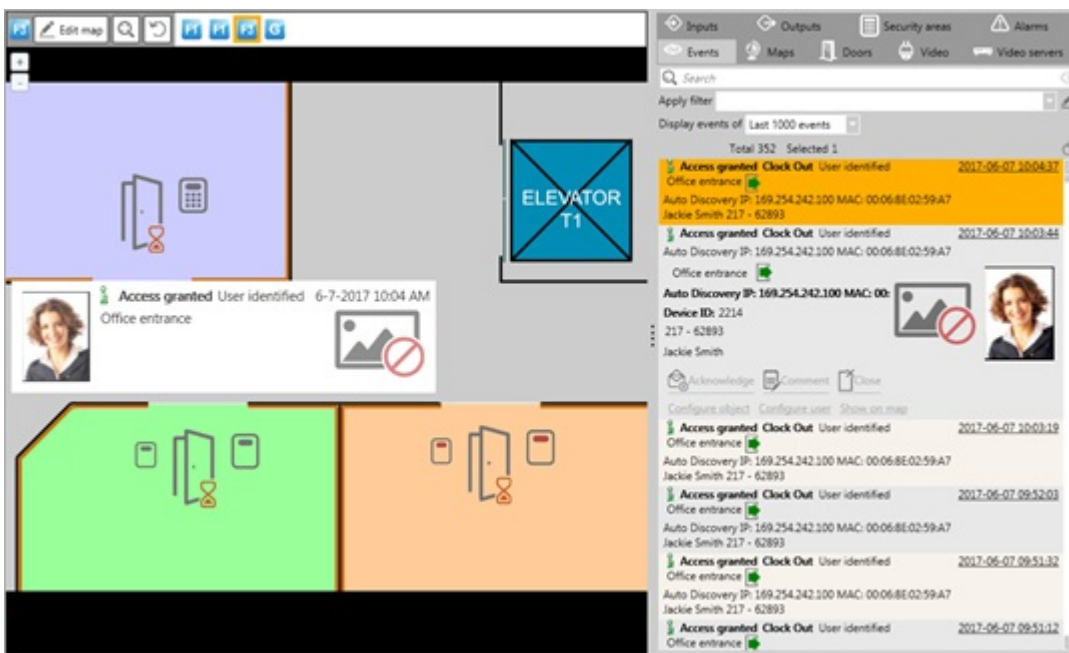
- **Unknown** state is displayed in a **brown** background.

# 19. Monitoring

Monitoring tab displays configured maps, event history, status of doors and security areas, and alarm events. As well it is possible to do multiple actions for doors, outputs, inputs, security areas, video cameras and much more.

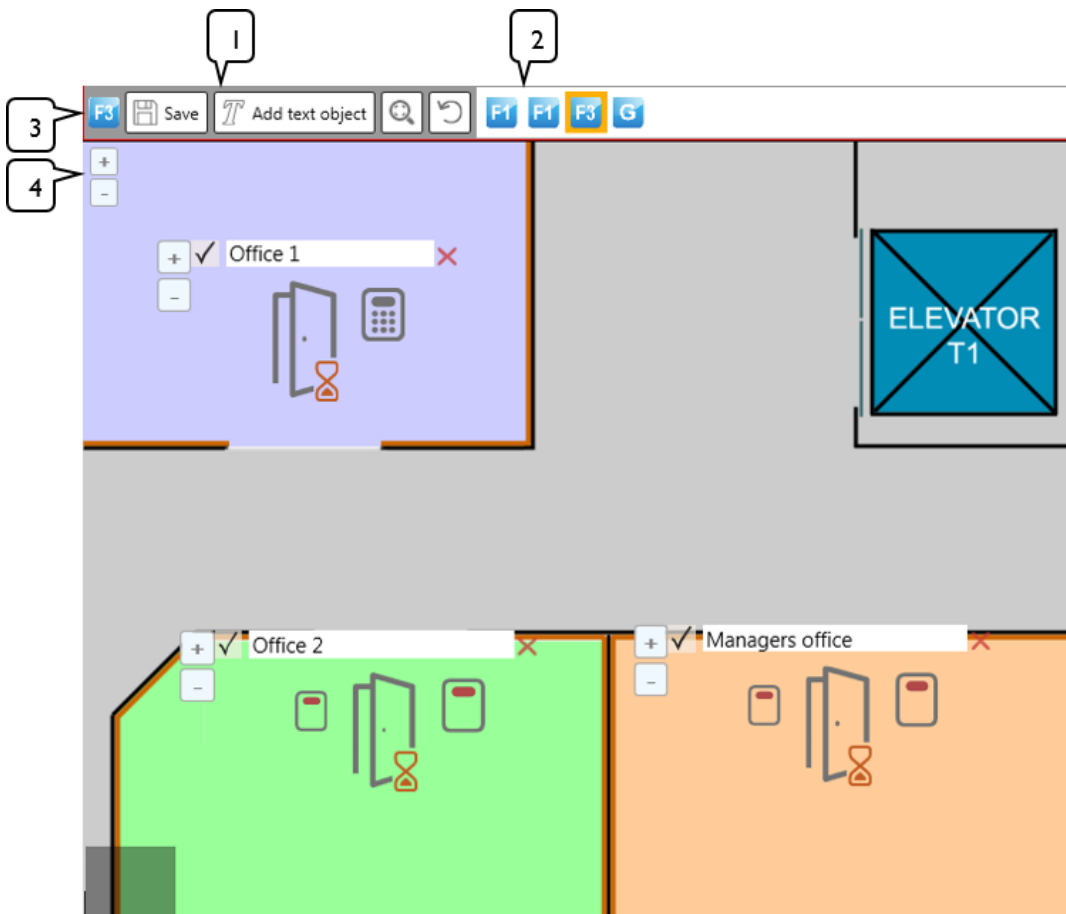
Monitoring tab consists of 2 sections:

- Map panel (left side).
- Sub-panels (right side).



## 19.1 Map layout panel

The map panel consists of a navigation panel and a map layout. On this panel, maps can be edited, by changing the layout of items, actions on the doors, inputs, outputs and security areas can be made. To edit the map layout, click on **Edit map** button and changes to the selected map can be done. While in edit mode, it is not possible to switch between maps.



### 1. Map edit buttons.

Icon	Name	Description
	Edit map	The selected map goes in edit mode and the layout of the map changed, items can be added, modified or removed. After the map goes into edit mode, the "Edit map" button is change to "Save changes" button.
	Save changes	Saves the map changes. This button is only available in edit mode. After changes are saved, this button is replaced with "Edit map" button.
	Add text object	Adds a text box on which a text can be written down and it can be moved around, it can be enabled or disabled. This button is only available in edit mode.
	Zoom to fit	Zooms the map to the top-left corner.
	Revert changes	Reverts to the last saved settings and the zooms on the maps coordinates where the last save was done.

- Map navigation panel.** This panel displays created maps, which are created in the **Maps** sub-panel. By selecting a map icon, the map layout will be represented on the map.
- Displays the selected map layout.
- Zoom in and out function. It is possible to zoom in and out using a mouse wheel as well.

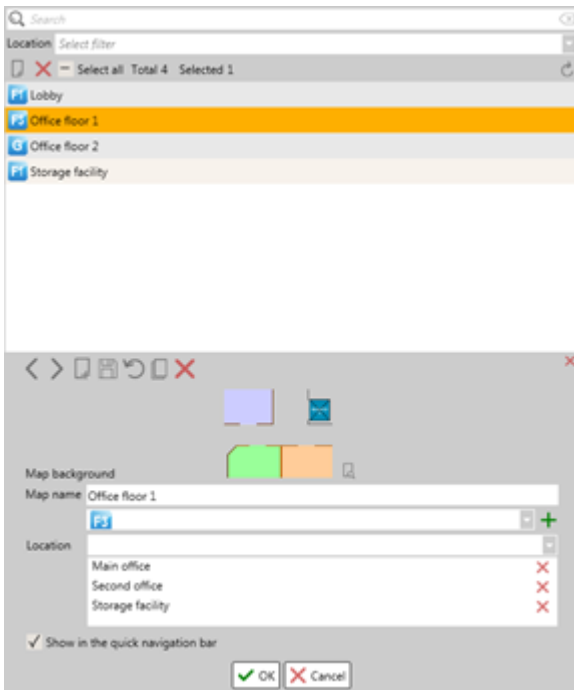
## 19.2 Maps sub-panel

On this panel, maps are reviewed, created, modified or removed. On the list, the created maps with



their representative icons are displayed. By selecting a map from the list, its details are presented below the list. Search is only available by name.

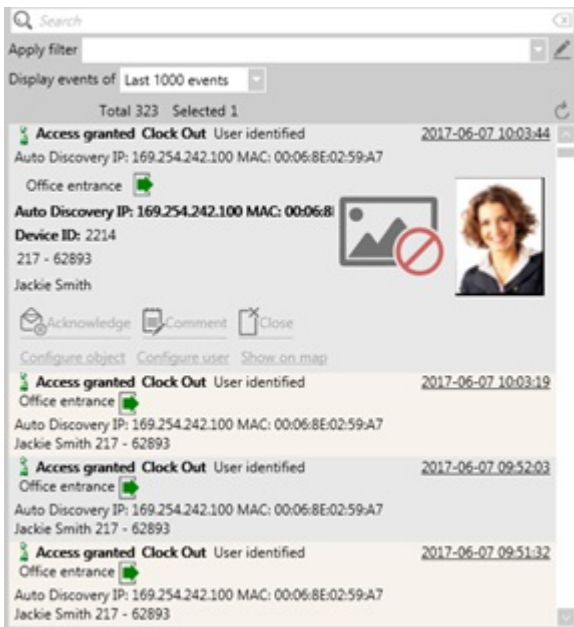
It is possible to add the map icon on the map layout, for easy access to the specific map.



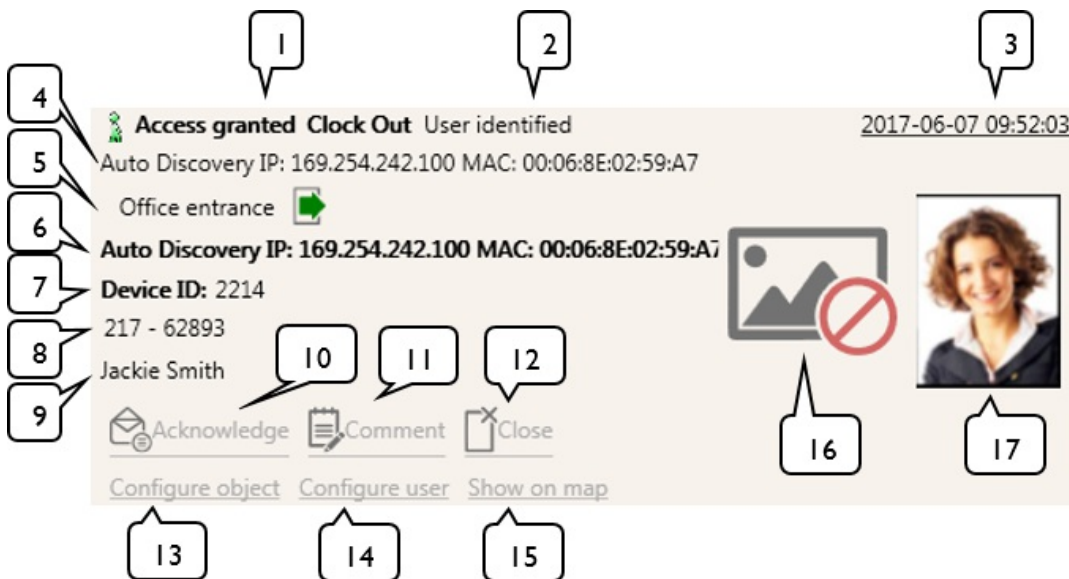
- **Map background.** Displays the selected map background. By default, there is a CredoID white background. To add a custom background, click on **Load photo from disk** button, located on the right side of the background icon.
- **Map name.** The name of the map.
- **Map icon.** Select an icon from the list for the map, which will be displayed on the Map navigation panel. To add a custom icon, click on **Add new icon** button, located on the right side of the **Map icon** second field.
- **Location.** Assign locations to the map.
- **Show in the quick navigation bar (checkbox).** Enabling this check box, will place the map icon on the **Map navigation panel**, for quick access to the maps layout.

## 19.3 Events sub-panel

On this tab, live system event feed is displayed. Any events, related to devices or notifications are displayed here. There are a lot of different kinds of events that can be registered by the system, due of this, only the needed information is presented. The event list updates automatically.



- **Search function.** It is possible to search events by:
  - Users (First name, Family name, card identification number).
  - Device name.
  - Door name.
- **Apply filter.** Select a created filter to filter out events. Filters are created, by clicking on “Edit filter” button, located at the right side of the **Apply filter** field [25.1].
- **Display events of.** Select how many events should be displayed on the event list.
- **Events.** Events are displayed on the events list. By hover over the event, it should expand and display additional information about the event. As well, additional actions on the events can be made.



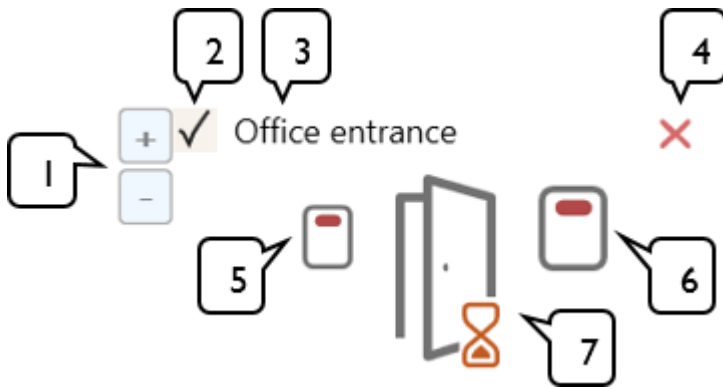
Displayed event information:

1. **Event type.** Displays the events type (example: Access granted, Access denied, Door forced open and etc.).
2. **User identification status.** Displays information if the user is identified in the system.
3. **Event time.** Displays the date and time of the event.
4. **Device name.** Displays the name of the device the event was received.
5. **Door name and direction.** Displays the name of the door that the device is assigned to and the direction of the reader.
6. **Device name in bold.** Displays the name in bold of the device the event was received.
7. **Device ID.** Displays the ID number of the device.
8. **Identification.** Displays the identification of the user that was presented on the reader (card number, PIN, license plate number).
9. **User.** Displays the First and Family name of the user that generated the event.

10. **Acknowledge (button).** Acknowledges the event. The event will be moved from Unacknowledged state to Acknowledge. This is an Alarms sub-panel function.
11. **Comment (button).** Opens "Event comment" window where a comment can be written down for the event.
12. **Close (button).** Closes an acknowledged event and it will be moved to the close state. This button is only available when the event has been acknowledged. This is an Alarms sub-panel function.
13. **Configure object (button).** Open Door tab and focuses on the door from which the event was received.
14. **Configure user (button).** Opens User tab and display the user who generated the event.
15. **Show on map (button).** Zooms in on the item from which the event was generated.
16. **Camera photo.** Displays a photo received from a camera. If no camera is connected to the object from which the event is generated, no image will be displayed.
17. **User photo.** Displays users photo. If a user does not have a photo, no photo will be displayed.

## 19.4 Doors sub-panel




On the door sub-panel, all configured doors are displayed. By hovering over a door, it will display additional information [6.1]. These doors can be added on a map, while it is in map edit mode, by dragging it on the map.






While in map edit mode, doors icon size can be adjusted and a name can be enabled:

1. **Increase or decrease the size on the object (buttons).** By clicking on the plus (+) button, it will increase the size of the object while minus (-) – decreases.
2. **Enable name (checkbox).** By enabling this check box, the name will be displayed on top of the door.
3. **Door name.** The name of the door. This field has to be written manually.
4. **Remove.** Removes the door from the map.
5. **Exit reader.** Displays the status of the exit reader. By clicking on it, will open up a reader management window [6.4].
6. **Entry reader.** Displays the status of the entry reader. By clicking on it, will open up a reader management window [6.4].
7. **Door status.** Displays the status of the entry reader.

Possible reader and door statuses are displayed below. If the line in the middle of the reader picture is green, that means that the reader is online, while the red significance that it is offline.

Icon	Name	Description
	Card reader	Card reader image, which only scans cards.
	PIN or fingerprint reader	Indicates PIN or a fingerprint reader with or without card reading mode.
	Open door	Indicates that the door is open.

	Held open door	Indicates that the door is held open. This icon is also displayed when there is no known state about the door.
	Closed door	Indicates that the door is closed.
	Forced open door	Indicates that the door is forced open and alarm is generated.

## 19.5 Video sub-panel

On the Video sub-panel, all created cameras are displayed. These cameras can be added on a map by dragging it on the map (an icon is displayed below which re-presents a camera on the map), while the map is in edit mode. By double left-click on camera from the list, it will open Camera view window [\[8.1\]](#). This can also be opened while the camera is placed on the map by right-click on it while the map is not in edit mode.



## 19.6 Input and Output sub-panels

On the Inputs sub-panel, created inputs and downloaded security zones are displayed. They can be added on a map by dragging it on the map, while it is in edit mode. Also, there is a “Download security zones” button which downloads data from MuSDO devices concerning security zones.

On the Outputs sub-panel, created outputs are displayed. They can be added on a map by dragging it on the map, while it is in edit mode.

## 19.7 Security areas sub-panel

On the Security areas sub-panel, downloaded security areas are displayed. They can be added on a map by dragging it on the map, while it is in edit mode. The sub-panel contains same buttons and features as the List panel in Security areas tab [\[18.1\]](#).

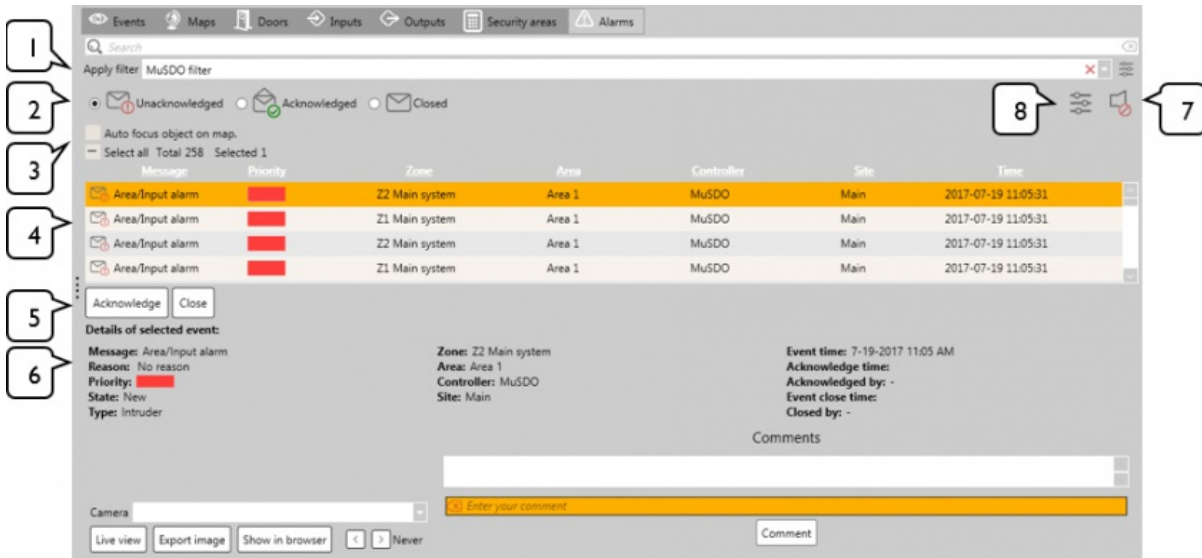


A security area is firstly displayed on the map in square shape. The blue corners are moveable and this way, the shape of the security area can be changed. It is also possible to make a custom geometry shape by right-click on the security area and selecting “Edit area”. This will remove the current security area and using a mouse, it is possible to draw a custom security area. Note, that to complete a custom geometry security area, the first and the last points have to be connected.

Security areas color changes, depending on its status [\[18.2\]](#).

## 19.8 Alarms sub-panel

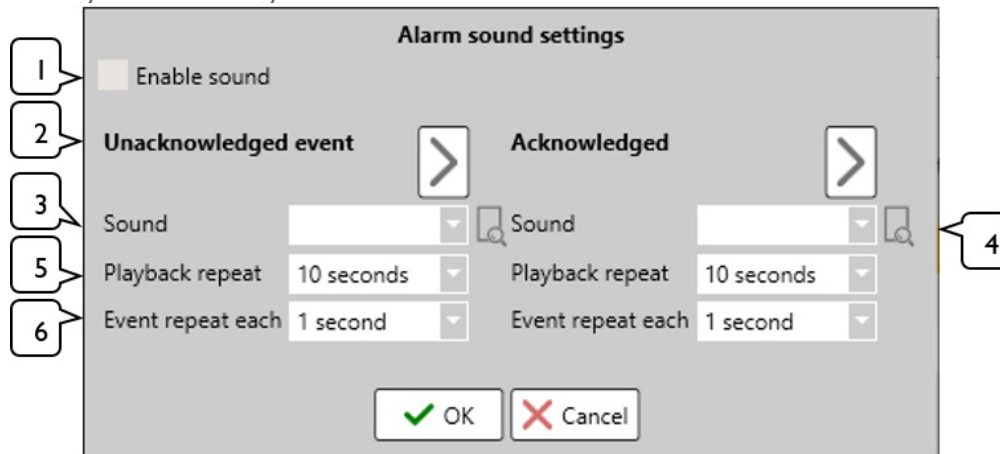
On Alarm sub-panel, generated alarm events are presented. Alarms are events which are determined by the filter that is used. By that filter, any event that matches the filters requirements, will be placed in the alarms sub-panel. When an alarm is received, it is Unacknowledged event, from where it can either be Acknowledged or Closed.



1. **Apply filter.** Alarm filters are created and selected here. A filter has to be created and assigned, to be able to receive alarm events [\[25.1\]](#).
2. **Sub-tabs.** Here, alarms are categories into 3 groups:
  - **Unacknowledged.** Received unacknowledged alarms are placed in this sub-tab. From here, alarms have to be either acknowledged or closed.
  - **Acknowledged.** After unacknowledged alarms have been acknowledged, they are placed in this sub-tab. From here, alarms can be reviewed or closed.
  - **Closed.** Closed alarms are placed in this sub-tab. Here, they can be reviewed.
3. **Auto focus object on map (checkbox).** When this checkbox is enabled, when a new alarm is received, it will automatically focus on that item on the map from which it was received. As well, clicking on any received alarm from the list, it will focus on that item on the map from which it was received from. Note, when an alarm is received from MuSDO devices, it will focus only on a security area. Focus configurations are done in GUI config files. For more information, contact your supplier.
4. **Alarm list.** Here, received alarms are presented. Alarms information is presented in this order:
  - **Message.** The type of an alarm.
  - **Priority.** Displays the priority of the alarm.
  - **Zone.** Displays from which input/security zone the alarm is received.
  - **Area.** Displayed from which security area the alarm is received.
  - **Controller.** Displays from which controller the alarm is received.
  - **Site.** Displays the location.
  - **Time.** Displays the time the alarm was received.
5. **Acknowledge & Closed (buttons).** Acknowledges or closes the alarm event. Both of these buttons are present on Unacknowledged sub-tab, while on Acknowledged sub-tab only Closed button is available. On Closed sub-tab, no further actions can be taken on the alarms.
6. **Details of the selected alarm.** Information about the received alarm is presented here. Information is divided into 3 parts:
  - **Details about the alarm.** Displays information from the Alarm list, as well additional information, such as Acknowledged time, Acknowledged by, Event close time and Closed by.
  - **Camera information.** Camera view configuration buttons and displays the photo taken for the event [\[8.1\]](#).

- **Comments.** Able to leave a comment for the alarm. Comments cannot be removed once a comment is made.

7. **Stop sound notifications.** Mutes any alarms sounds that are currently playing.
8. **Configure sound settings.** Opens Alarm sound settings configuration window, where alarm sound settings can be configured.



1. **Enable sound.** Enables alarm sound feature. By default, this feature is disabled until enabled.
2. **Unacknowledged & Acknowledged sound test.** By clicking on the arrow buttons, it will play the selected sound from **Sound**
3. **Sound.** Select a sound file for the unacknowledged or acknowledged alarm sounds. By default, there are 2 sound samples that are possible to select.
4. **Sound file import.** Import a custom audio file. The audio file has to be a .wav file.
5. **Playback repeat.** How long the alarm sound will be played in total. By default, this setting is set for 10 seconds.
6. **Event repeat each.** Determine the time the alarm audio starts to repeat. By default, the setting is set so that the alarm audio starts to repeat each second.

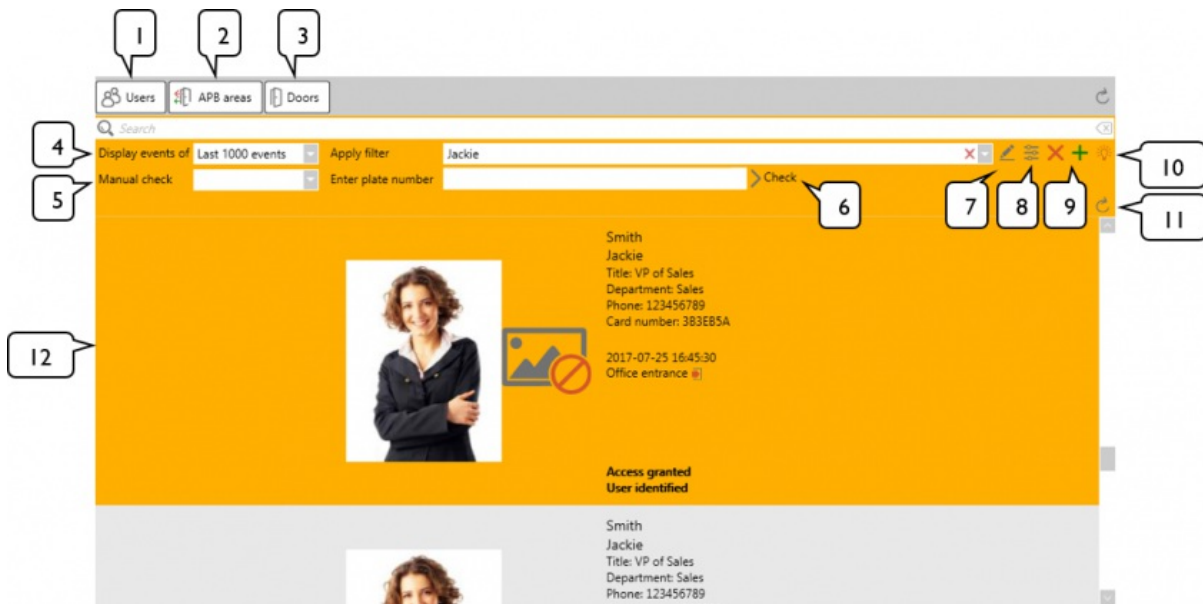
**Known issue.** If an error appears while playing an audio file, it might not be possible to play any sounds on GUI at all until the GUI is restarted. This issue might happen due of a corrupted audio file

## 20. Occupancy

Occupancy tab is used for event management as well as for APB area review, LPR license number checking and much more. This tab gives much more control over received events, providing more details about the events, multiple occupancy windows can be opened which can use different kinds of filters and actions can be taken on events which require host interaction.

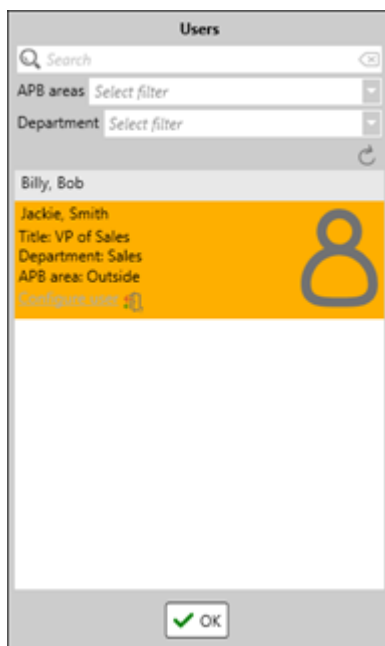
It is possible to search events in Occupancy tab by:

- Users (First name, Family name, card identification number).
- Device name.
- Door name.



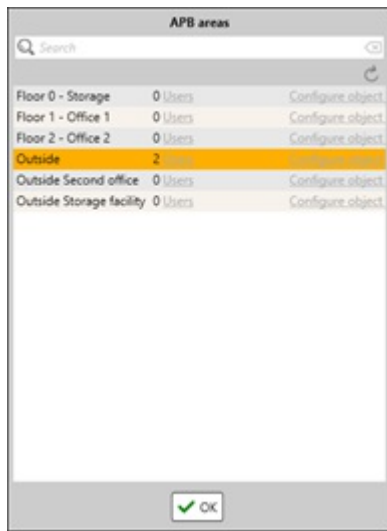
1. **Users (button).** Displays recently active users that were registered in the events, as well shows how many users are on a selected APB area. If a user is idle for over 48 hours, it will be removed from this list and APB areas. Search works by First name and Family name. Users can also be filtered by APB areas and departments.

By hovering over a user, it displays some key information about the users, such as: First name, Family name, Title, Department, APB area it is currently in and the users photo. By clicking on "Configure user" button, it will direct you to Users tab and focus on the selected user.

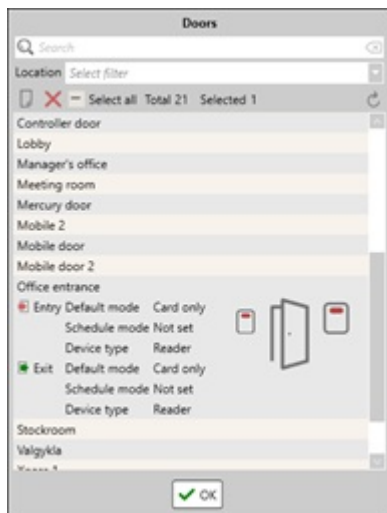


2. **APB areas (button).** Displays all configured APB areas and the number of users that are currently in the APB areas. If a user is idle for over 48 hours, it will be removed from the APB area. Search works only by APB area name.

Highlighted "Users" button, opens the User window from the Occupancy tab. Highlighted "Configure object" button, opens the APB areas tab and focuses on the selected APB area.



3. **Doors (button).** Displays all configured doors. From here, information about the doors can be reviewed [6.1] and door reader management window can be opened [6.4]. Search functions works by door name. Doors can be filtered by Locations.



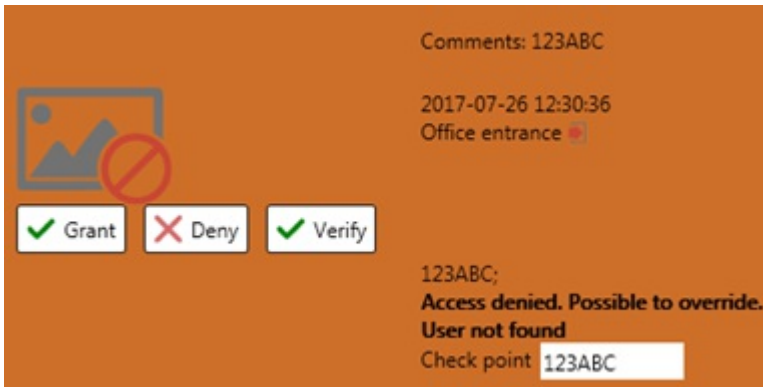
4. **Displays events of.** Select how many events should be displayed on the event list.
5. **Manual check.** Here, a door is selected which has a LPR input connected to it. A door with a LPR function has to be selected to be able to check license plate numbers.
6. **Enter plate number.** A license plate number is entered here and by clicking on the **Check** button located on the right side of the **Enter plate number** field, it will generate an event that requires a host interaction. There can be two types of events that can be generated: unknown user event and known user event.

If the license plate number matches the users license plate number, then in the event, that user's information will be presented with options to either grant access or deny it.





If the license plate number does not match with any user, it will generate an event type “User not found” and give the host three options: **Grant** access, **Deny** access or **Verify** the data, which checks the database again to see if it matches any users license plate number and if it has access. If the data is verified and the user has access, it grants access, in other cases, the event does not change.



Additional information about license plate number checking:

- By typing at least three symbols, **Enter plate number** will display a user list (First name; Family name; License plate number) which fit the license plate number symbols.
- License plate number checking events have a timeout interval until the event is closed. The timeout interval is configured on Access level tab [\[11.2\]](#). By default, the timeout interval is 10 seconds.
- If a checking event is created with an event type “User not found”, the timeout interval is not applied to this event.
- If a new event is generated on the same reader while there is a license plate number checking event, the last event will be closed (override).

7. **Edit filter (button)**. Brings up a filter window, where filters can be reviewed, created, modified or removed [\[25.1\]](#).

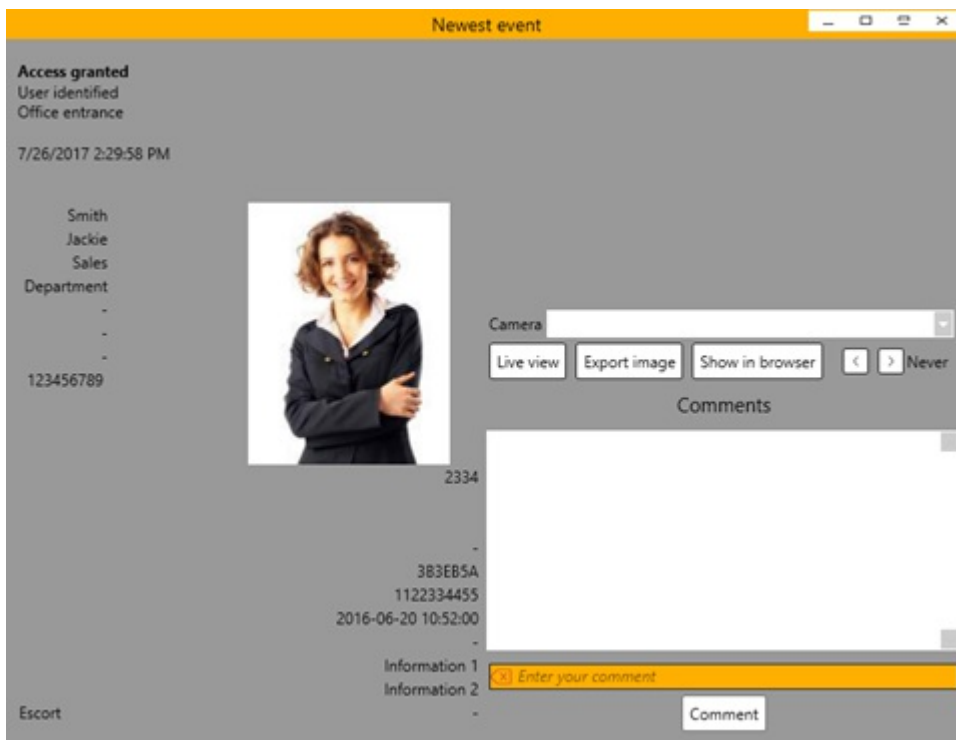
8. **Configure display fields (button)**. Brings up a Display fields configuration window, where it is possible to configure what will be displayed on the received events, such as user, identification, event and door information.

As well, there is an additional function to ignore duplicate events for a duration of time. If this field is configured, duplicate events won't be displayed in the Occupancy tab, depending the time interval configured. The maximum time interval is 5 minutes. By default, this function is disabled (set 0 seconds).

9. **Add new or Remove this column (button)**. By clicking **Add new column**, will add an additional occupancy column to the right, acting as a separate tab for event monitoring. **Remove this column** removes the selected column. This button is disabled if there is only 1 column.

10. **Newest event (button)**. Opens Newest event window where newest event from the specific occupancy column is displayed. This window automatically updates when an event is received. The information that is displayed on this window:

- Information about the event, user and doors. What information is displayed, depends on what fields are enabled in the **Configure display fields**
- Received camera photos [\[8.1\]](#).
- Comment section, where a comment can be leaved on the event.



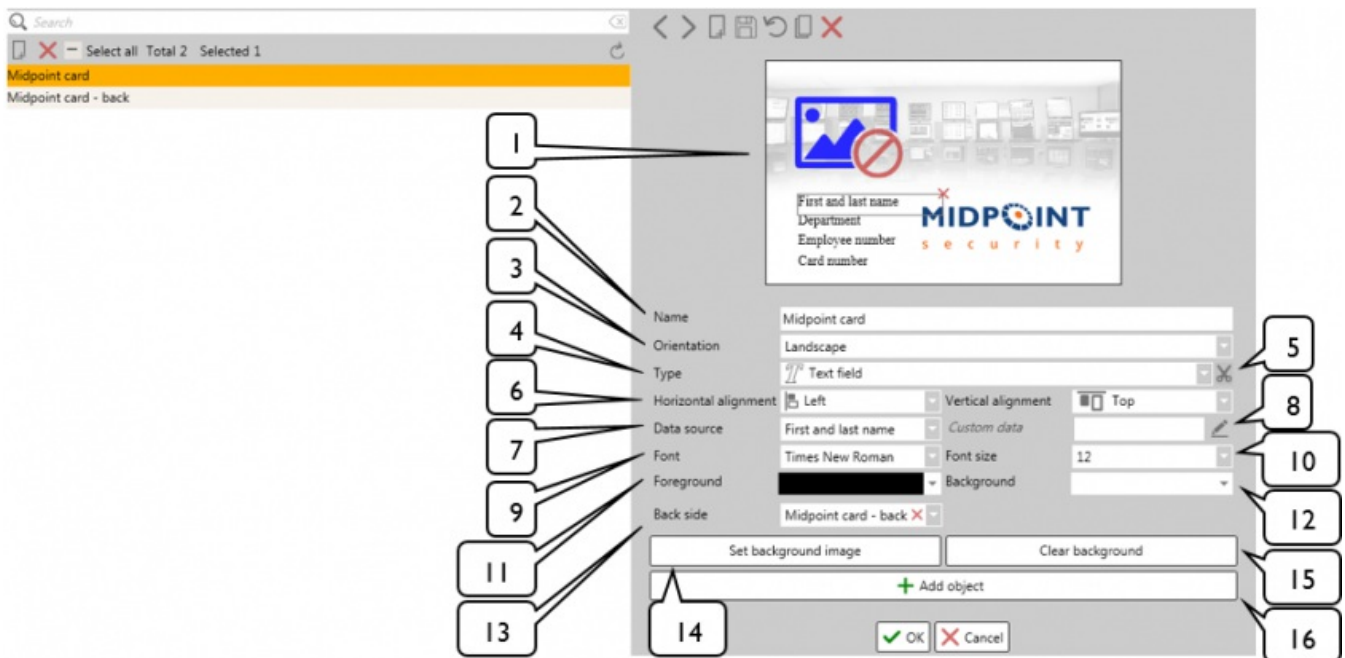
11. **Refresh list (button)**. Refreshes the current column.
12. **Event list (button)**. Displays incoming events. What information is displayed on the event, depends on the **Configure display fields** settings.

## 21. Card design

On this tab, card designs can be made which then can be assigned to identification cards and be printed out with a connected card printer.

On the list panel, created card designs are displayed. By selecting a card design, its information is displayed on the details panel. Search function works by name.

On the card design configuration window, object placement and their sizes can be changed. To place an object, may it be a user or custom images or text, click **Add object** button (16) and select the type of object it is on **Type** field. Further configurations are done to the objects and the full design, are done below the configuration window.



1. **Card design configuration window.** Here, the changes to the card design is made. To place an object on the map, click **Add object** (the type of the object is change in the **Type** field). Objects are moved around the configuration window with a mouse and by hold-drag the sides (bottom and right) of the object borders, changes its size.
2. **Name.** The name of the card design.
3. **Orientation.** The orientation of the card design. Possible choices: Landscape or Portrait.
4. **Type.** The type of added object type. Possible object types: Image or Text. This field is only available when an object is selected.
5. **Image size to borders.** Makes the image into the size of the vertical or horizontal borders length. This could increase, decrease or distort the image. This function is only available for image **Types**.
6. **Horizontal & vertical alignment.** Change the texts or images horizontal and vertical alignments.
7. **Data source.** The source of the data that will be presented on the card design. Depending on the selected Type, the data sources differ (for text type, user or identification, while for image – users photo). Custom information can also be presented.
8. **Custom data (button & field).** If Custom data source is selected, a custom text or an image has to be presented. For text types, a field is presented, where custom information can be written, while for image types, an image file has to be imported.
9. **Font.** Select the font for the text. This function is only for text types.
10. **Font size.** Select the size of the font. This function is only for text types.
11. **Foreground.** Changes the color of the font. This function is only for text types.
12. **Background.** Changes the background color for the selected type.
13. **Back side.** Select already created card design to be the back side of the card design.
14. **Set background image (button).** Import a background image for the card design.
15. **Clear background (button).** Removes the imported background image.
16. **Add object (button).** Adds an object on the Card design configuration window. By default, it adds a text object.

## 22. Time and attendance (T&A)

On Time and attendance tab it is possible to configure and review work days for individual users. Custom schedules can be created and many additional features that helps to calculate work days more efficiently and with better results.

Time and attendance tab is separated into 3 sub-panel:

- **Individual schedules.** For reviewing and making changes to the user's calendar / schedules. Assign or modifying created schedules to users, manage absences, review user information.
- **Work schedule configuration.** Work schedules are created, modified or removed on this panel.
- **Settings.** Night work time can be configured here, which determines when the night shift starts and ends.

To fully configure a schedule for a user, a schedule has to be created on the **Work schedule configuration** sub-panel and then that schedule has to be assigned to the user on **the Individual schedules** sub-panel.

T&A reports are created in on Reports tab, under Time and attendance reports sub-tab [23.6]. Note, that schedules have to be configured first to be able to create correct reports.

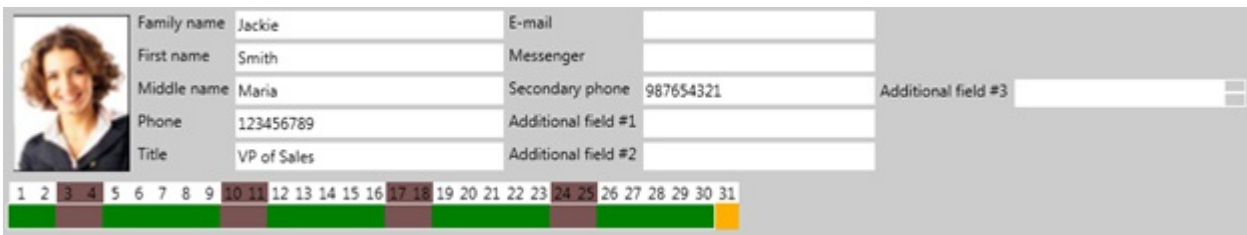
## 22.1 Individual schedules

On Individual schedules sub-panel, user’s information can be reviewed and schedules are assigned, modified or removed from the users.



Individual schedules sub-panel is divided to 3 sections:

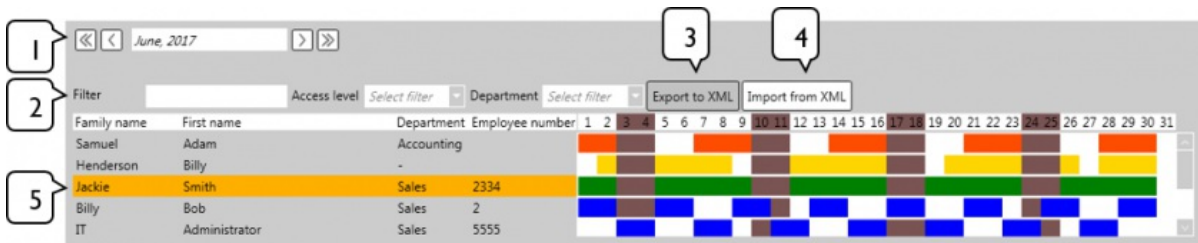
- **User information field.** Here, selected user’s information [15.2.2] as well as selected months schedules are presented. The user information fields are not editable, only the schedule field is editable.



1. User information, which are configured on Users tab, are displayed here. These fields are not editable.
2. The selected months schedules are displayed below. This field is editable and schedules can be assigned, modified or removed. If the month is shorter than 31 days, those days are colored yellow and are not editable.

- **Calendar.** Displays all users who has **T&A type** set on Users tab as “Advanced” and their calendar field. Work schedules can be assigned, modified or removed, as well it is possible to manage absences on the calendar field.

1. **Selected year and month.** Displays which year and month is currently displayed on the calendar.



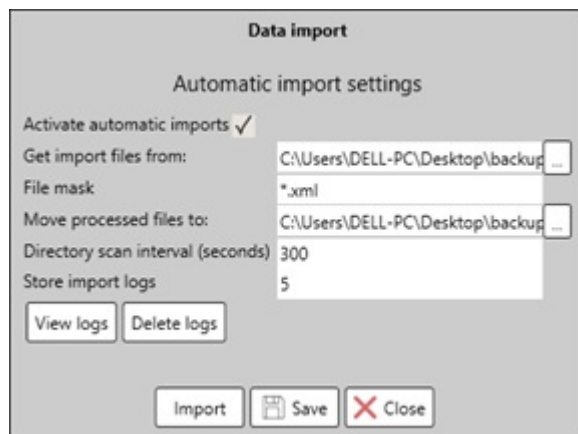
Icon	Description
	Moves the calendar back by 1 year.
	Moves the calendar back by 1 month.
	Moves the calendar forward by 1 year.
	Moves the calendar forward by 1 month.

2. **Filter.** These fields filter the user list.

- Filter fields works by: First name, Family name.
- Possible to filter users by the **Access level** they are assigned to.
- Possible to filter users by the **Department** they are assigned to.

3. **Export to XML (button).** This function is deprecated.

4. **Import from XML (button).** Import schedules on the calendar. After clicking on it, "Data import" window shows up, where data can be selected and imported [25.2]. As well it is possible to configure automatic imports.



- **Activate automatic imports (checkbox).** Enable or disable the schedule automatic imports function. If this checkbox is disabled, configurable fields are disabled (except **Store import logs** field).
- **Get import files from.** Select the folder from which the schedule import files will be taken from.
- **File mask.** Type in the file mask. By default, it is "\*.xml".
- **Move processed files to.** Imported files are moved into a designated folder.
- **Directory scan interval (seconds).** The interval in which the folder, where the schedule import files should be stationed, will be scanned for import. The minimum interval is 300 seconds (5 minutes) while the maximum – 86400 seconds (24 hours). By default, the interval is set for 3600 seconds (1 hour).
- **Store import logs.** The maximum possible import logs that will be stored. The oldest logs will be removed. By default, the maximum import logs are set for 10 logs.
- **View logs (button).** Opens up "Import logs" window, where it is possible to review import logs and what information was imported.
- **Delete logs (button).** Deletes all import logs.
- **Import (button).** Import a schedule file.
- **Save (button).** Saves the configured settings.

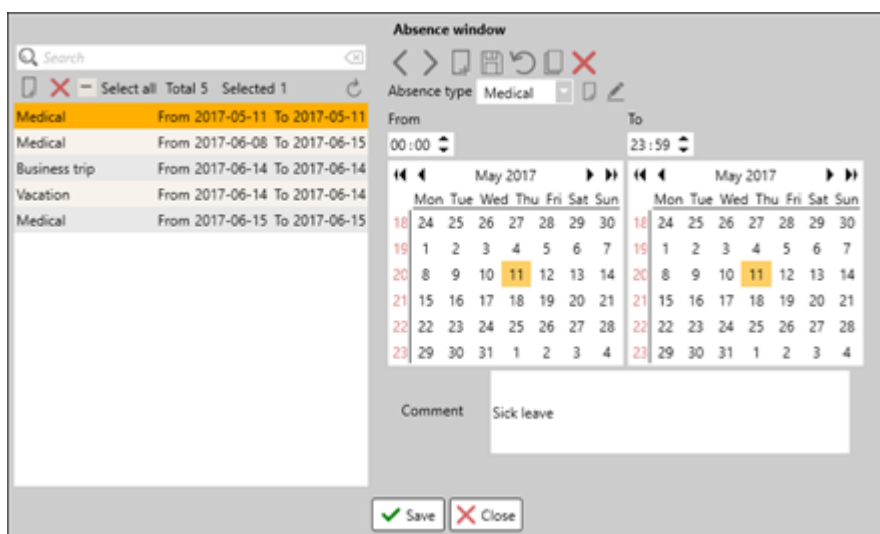
- **Close (button).** Closes the window. Note, this does not save configured settings.

5. **Calendar.** Displays users list and their calendar. Here, for the selected user, schedules and absences are added, modified or removed.

- Users list contains this information about the user: Family name, First name, Department and Employee number.
- Calendar displays 31 days of the selected month. Weekends are colored in a different color (brown).
- Schedules are assigned to user from **Typical work schedules** list, from where it has to be selected and dragged on the calendar. Or by using the **Import from XML**
- By right-clicking on the calendar, an option menu is presented with additional functions.

Copy selection
Copy month
Paste
Clear selection
Clear month
Fill month
Manage absences
Clear absence
<input type="checkbox"/> Automatic schedule
Custom schedule

- **Copy selection.** Copy the selected schedule block on which it was selected.
- **Copy month.** Copy the selected user's whole month.
- **Paste.** Pastes the settings that were copied before.
- **Clear selection.** Removes the selected schedule from the user.
- **Clear month.** Removes the entire months schedules.
- **Fill month.** Fills the whole month with the selected schedule from the **Typical work schedules** list.
- **Manage absences.** Opens "Absence window" where an absence can be reviewed, created, modified or removed.

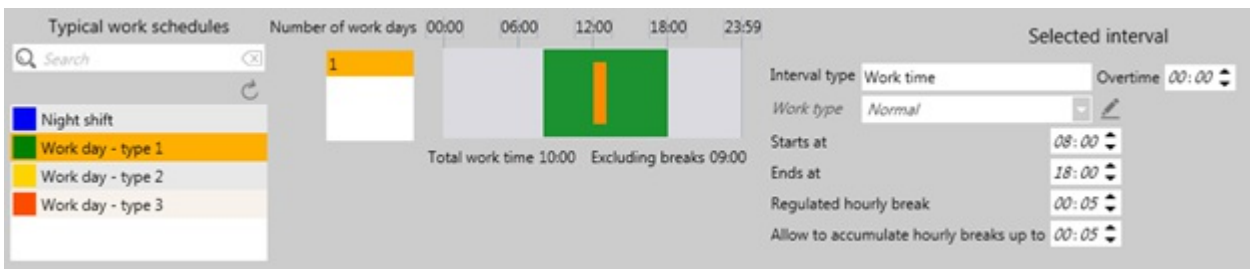


Created absences can be reviewed on the list panel. Absences are sorted out by date, oldest being the top. On the details panel, selected absences information is displayed.

- **Absence type.** This describes what kind of absences it is. There are built in absences types, which cannot be removed nor edited (Medical, Vacation, Business trip, Suspension, Personal, Training, Customer visit, Jury duty). New absences can be created by clicking on the **"New absence reason"** button which is located on the right side of the **Absence type** field.
- **Calendar.** Select the date and time interval for the absence.
- **Comment.** An information field for describing the absence.
- **Clear absence.** Clears an absence on the selected location.
- **Automatic schedule (checkbox).** The selected work schedules will be transferred to the next month.
- **Custom schedule.** Opens "Custom schedule window" where the selected schedule can be

configured to have a custom schedule. This will only apply to the selected schedule block, not the whole schedule.

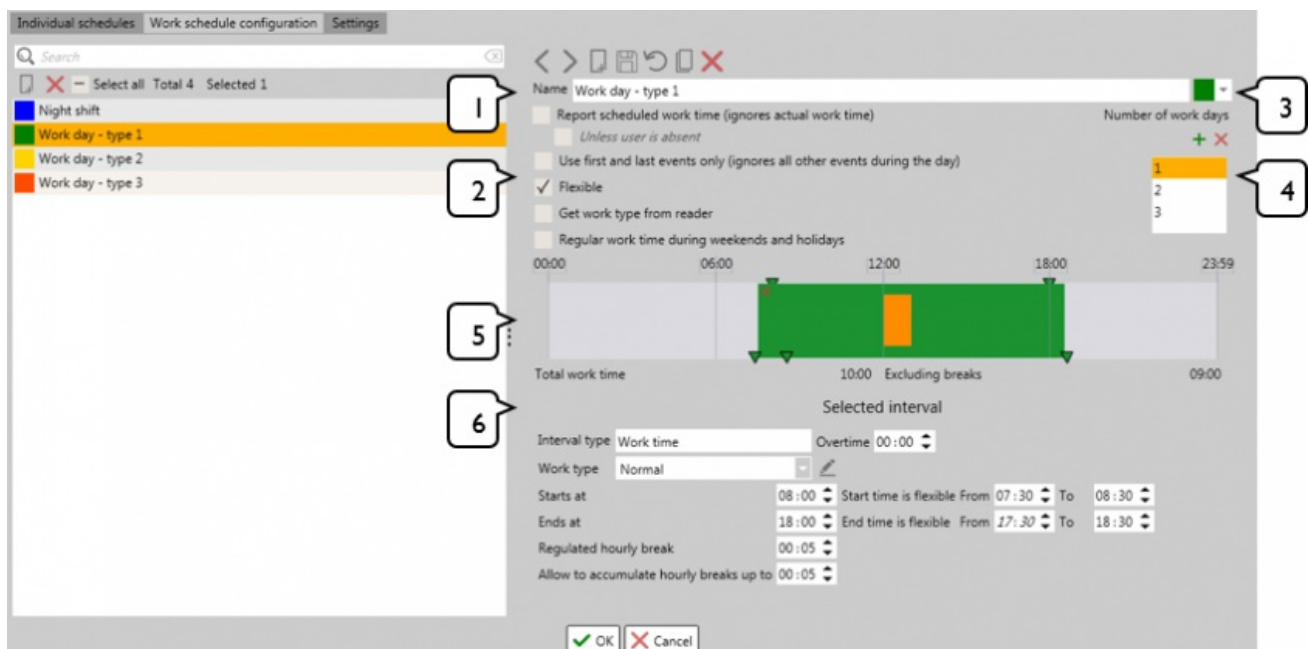
- **Work schedules.** Displays created work schedules and their time interval with additional information. From here, schedules are assigned to users by dragging the selected schedule on the calendar.



- **Typical work schedule.** Created work schedules are displayed here.
  - Schedules are sorted out by name.
  - Search function only works by name.
  - From here, schedules are added to users by dragging the selected schedule and adding it on the calendar.
  - Selecting a work schedule, will display the **Number of work days** it has and the **Work interval** on the right side.
- **Selected interval.** After selecting an interval from the selected schedules Work interval, on the far right it will display additional information [22.2]. These fields are not editable.

## 22.2 Work schedule configuration

Work schedules can be reviewed, created, modified or removed on this sub-panel. On the list panel, created schedules are displayed with their representative colors, while on details panel – schedule configurations are made.



1. **Name.** The name of the schedule.
2. **Schedule settings.** Schedule settings which describes the behavior of the schedule. These settings effect the way Time and Attendance reports are calculated.
  - **Report scheduled work time (ignores actual work time).** Ignores the actual work time and applies full work schedule time. **This function is deprecated.**
    - **Unless user is absent.** Applies an absent day to the user unless a clock-in or a clock-out was done during any time of the work schedule. This function is only available if **Report scheduled work time** is checked. **This function is deprecated.**

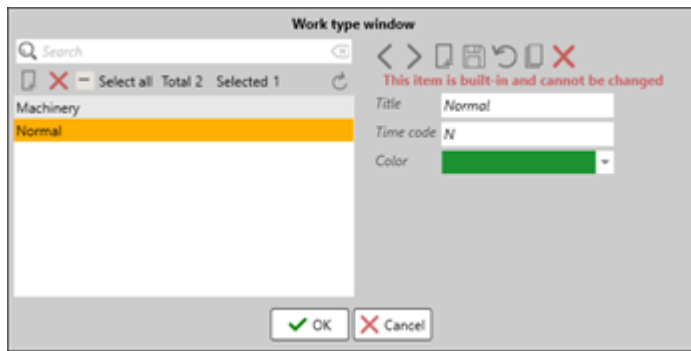
- **Use first and last events only.** Only uses the first and last events during the day while creating a report.
  - **Flexible.** Grants flexibility for the work schedule. This will add extra configuration for the work schedule on the **Work interval** (represented as green arrows on the bottom of the interval) and **Selected interval** settings. **This function is deprecated.**
  - **Get work type from reader.** Receives work type from readers. Work types are configured on **Selected intervals** sections, by clicking on **Edit work type** button, located on the right side of the **Work type**. After a work type has been configured, it can be assigned to a door on Doors tab. **This function is deprecated.**
  - **Regular work time during weekends and holidays.** The schedule will act as a normal work day during weekend and holiday days.
3. **Work schedule color.** Opens up a color pallet, from which a color can be picked to represent the configured work schedule. This color is represented on the calendar on Individual schedule sub-tab.
  4. **Number of work days.** Add or remove the amount of days that the work schedule will have. Each day has to be configured separately. When a work schedule is added on the calendar, it will add all configured days in a row.
  5. **Work schedule interface.** Work schedules are added, modified or removed on work schedule interval. To create a work time interval, hold left-click and drag on **Work schedule interface**. On the bottom of the Work schedule interface, Total work time is displayed, as well as a time interval **Excluding breaks**.
    - **Normal work time.** To create a normal work time interval, hold left-click and drag on **Work schedule interface** and a green bar will be created, which indicates **Normal work time**. To change the start and the end of the interval, drag the sliders (▼) which is located on the top of the **Work schedule interface** or by configuring **Starts at** and **Ends at** in the **Selected interval** Only 6 **Normal work time** intervals can be created per schedule.
    - **Flexible work time.** Flexible work time can only be configured when the **Flexible** checkbox is enabled. To configure flexible work time, either drag the sliders (▼) which are located on the bottom of the **Work schedule interface**. There are 3 sliders in total:
      - First indicates the start time of flexible work time.
      - Second indicates the end of the start time of flexible work time.
      - Third indicates the end of the end time of flexible work time.

Flexible work time can also be configured through **Selected interval** section, by changing **Start time is flexible From & To** and **End time is flexible From & To**.

- **Break time.** To create a break time interval, hold left-click and drag inside a work time interval and this will create an orange bar, which indicates **Break time**. To change the start and the end of the break time interval, drag the sliders (▼) which is located on the top **Break time** interval itself or by configuring **Starts at** and **Ends at** in the **Selected interval** section after selecting the break time interval. Only 3 **Break time** intervals can be created per schedule.
6. **Selected interval settings.** Displays configurable options that are available for the selected work or break interval.
    - **Interval type.** Indicates the type of interval is selected. There are only 2 types of intervals: **Work time** and **Break time**. This field is not editable.
    - **Overtime.** Indicates work schedules overtime interval.
    - **Work type.** Brands the work time for indicating the type of schedule it is, also a work type can be assigned to a reader. By default, there is a built in Work type "**Normal**", which is used when creating a Normal work interval. Break time interval have built in **Break types** and no other types can be created:
      - **Mandatory.** Break time which no matter what, the break time interval will be included in the T&A report even if the users did not leave during the break time or did not use the full time.
      - **Optional.** Break time during which is not necessary for users to use the full break time or have a break time at all. The amount of time the user spend during the break time, will conclude in the T&A reports. The time spent not being on the break during the optional break time, will be included in the total work time.

To create, review, modify or remove work types, click on the **Configure work type** button, which opens "Work type window", located on the right side of the **Work type** field. By default, **Normal** work type is not editable nor it is possible to remove.





- By default, **Normal** work type has **Time code** "N" and representative **Color**
  - **Title**. The name of the work type.
  - **Time code**. A short name of the work type, which is used on T&A reports.
  - **Color**. Representative color of the work type, which colors the work the interval.
- **Starts at**. Indicates the starts of the work/break time.
  - **Ends at**. Indicates the end of the work/break time.
  - **Start time is flexible From & To**. Indicates the time interval for flexible start work time. **From** cannot be higher than **Start at** while **To** cannot be lower than **Start at**. This function is only available if **Flexible** checkbox is enabled.
  - **End time is flexible From & To**. Indicates the time interval for flexible end work time. **From** is not editable and will always indicate the same time as **Ends at** while **To** cannot be lower than **Ends at**.
  - **Regulated hourly break**.
  - **Allow to accumulate hourly breaks up to**.

## 23. Reports

On this tab, different kinds of reports can be generated. All reports are generated in .xlsx format. Possible reports:

- Event report.
- Occupancy report.
- User report.
- Device report.
- Access level report.
- Time & attendance report.
- Door access report.
- Billing report.
- Access reports.

All report sub-panel have a very similar layout, which consists of a details and filter panels. Only Automatic reports sub-panel has a different layout as it is used for creating templates for automatic report generation.

**Details panel.** Report configuration options are chosen here, such as the name of the report title, the limit of rows on the report, time interval, what fields will be displayed on the report and much more, depending on the type of the report.

Report template:

Template name

Title

Subtitle

Page numbering

Report date and time

Show report header on each page

eco-Friendly

Limit

Time interval

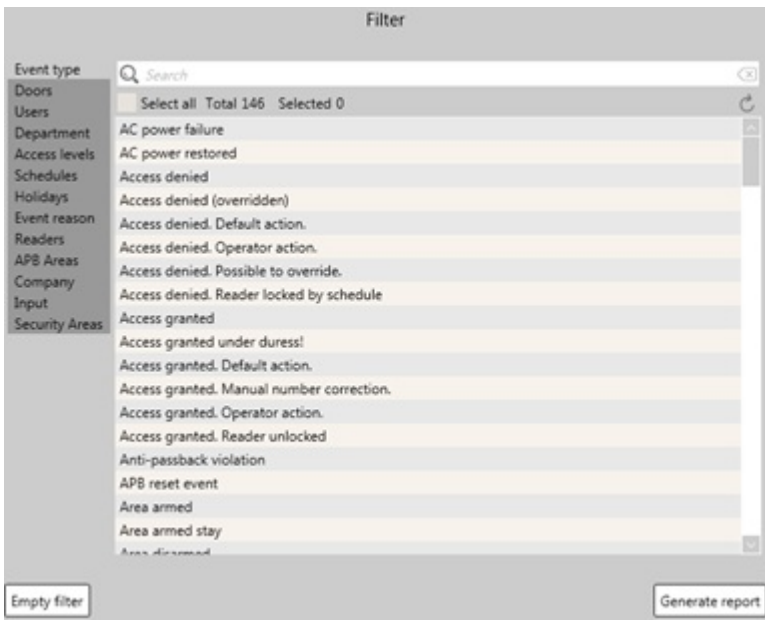
From

To

June 2017							June 2017								
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun		
23	29	30	31	1	2	3	4	23	29	30	31	1	2	3	4
24	5	6	7	8	9	10	11	24	5	6	7	8	9	10	11
25	12	13	14	15	16	17	18	25	12	13	14	15	16	17	18
26	19	20	21	22	23	24	25	26	19	20	21	22	23	24	25
27	26	27	28	29	30	1	2	27	26	27	28	29	30	1	2
28	3	4	5	6	7	8	9	28	3	4	5	6	7	8	9

- **Report template.** Select created report template from the list. By default, there is a built-in template "Default report template" which has no settings selected. This template cannot be removed.
- **Create new template (button).** Located on the right side of **Report template** Creates a new report template with default settings and enables **Template name** field.
- **Save template (button).** Located on the right side of **Create new template** Saves the templates settings.
- **Template name.** The name of the report template. This field is only available when a non-default template is selected.
- **Title.** The title of the report, which will be presented in the report file.
- **Subtitle.** The subtitle of the report, which will be presented in the report file.
- **Page numbering (checkbox).** **This function is deprecated.**
- **Report date and time (checkbox).** **This function is deprecated.**
- **Show report header on each page (checkbox).** **This function is deprecated.**
- **Eco-Friendly (checkbox).** Report files won't have any colorful tables.
- **Limit.** Indicates how many rows will be used in the report file. If more rows are used in the report then the requested limit, a warning will be presented that not all information will be presented in the report file.
- **Time interval.** Indicates the time interval that will be included in the report. By selecting a time interval, it will change the calendars settings according to the selected interval. If the calendar is manually changed, the Time interval type is then changed to Custom. This field is only available for Event and Time and Attendance report types. Types of Time intervals:
  - **Custom.** The time interval is manually set on the calendar.
  - **Today.** Today's time interval from 00:00:00 to 23:59:59.
  - **Last 24 hours.** From the moment selected, it will select the last 24 hours on the calendar.
  - **Yesterday.** Selects yesterday's time interval from 00:00:00 to 23:59:59.
  - **This week.** Selects this weeks' time interval from the first working day 00:00:00 to the current time.
  - **Last week.** Selects last weeks' time interval from the first working day 00:00:00 to the last day of the week 23:59:59.
  - **This month.** Selects this months' time interval from first day of the month 00:00:00 to the current time.
  - **Last month.** Selects last months' time interval from the first working day 00:00:00 to the last day of the month 23:59:59.
  - **This year.** Selects this years' time interval from first day of the year 00:00:00 to the current time.
- **Calendar.** Custom time interval can be selected here. The left calendar indicates the start of the report while the right calendar – the end of the report time. On the top of each calendar, specific time can be selected (hh:mm:ss). These calendars are only available for Event, Time and Attendance, Door access, Billing, Access statistics and Automatic reports.

**Filter panel.** Filter panel is present on every report sub-tab, except Automatic report sub-tab. On the filter panel, filters for the reports are selected, which information should be included into the report file. Each report sub-tab may have a different set of filters [\[25.1\]](#).



- **Empty filter (button).** Clears all filters for the selected report template. If any filter is selected, a message near the button is displayed, noting that there are filters selected (Note: additional filter turned on!).
- **Generate report (button).** Generates a report file with the selected settings in a specified location.

Possible filter types that can be used in different reports:









Filter type	Report type
Event type	Event report
Doors	Event report, Device report, Door access report, Access statistics
Users	Event report, User report, T&A report, Door access report, Billing report, Access statistics
User Title	User report
Department	Event report, Occupancy report, User report, T&A report, Billing report, Access statistics
Access levels	Event report, User report, Access level report, Billing report
Schedules	Event report
Holidays	Event report
Event reason	Event report
Readers	Event report
APB Areas	Event report, Occupancy report, Access statistics
Company	Event report, Occupancy report, User report, T&A report, Door access report, Billing report, Access statistics
Input	Event report
Security Areas	Event report

**Fields section.** Fields section is where detail fields are selected that will be included in the report file. Detail fields consists of two sections:

- **Available fields.** Indicates available fields that can still be added to the **Report fields**. Fields that are left in the **Available fields** section are not included in the report file.
- **Report fields.** Indicates fields which will be included in the report file. Fields are added from **Available fields** section.

To move fields around in the Fields section, firstly, click a field with a mouse button and then using

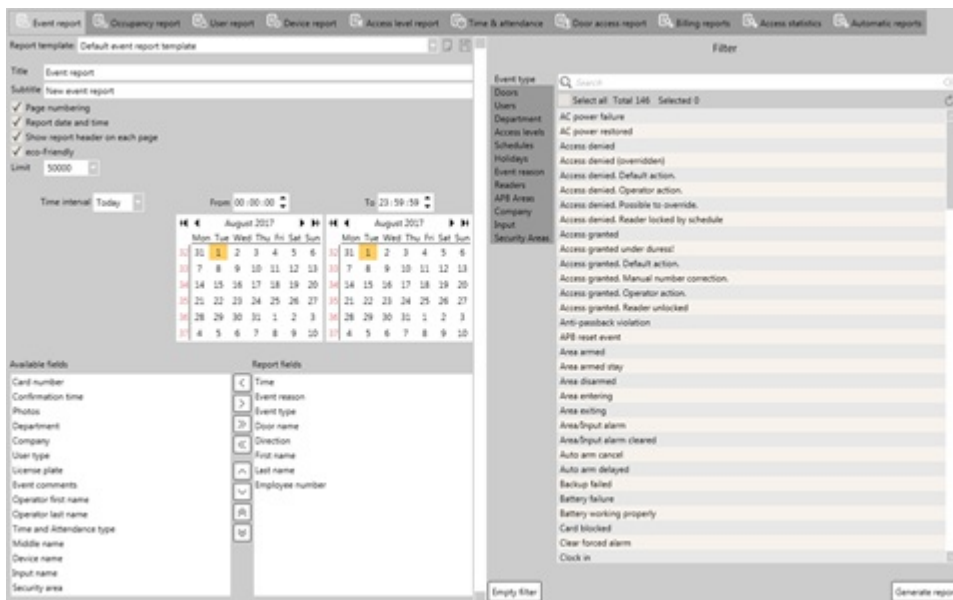
the sections buttons, add, remove, go up or down the list. Depending on the Report fields order, from top to bottom, this will be represented in the report file in that order (from first to last).

Icon	Description
	Moves the selected field from Report fields section to Available fields
	Moves the selected field from Available fields section to Report fields
	Moves all fields from Available fields section to Report fields
	Moves all fields from Report fields section to Available fields
	Moves the selected field up in the Report fields list
	Moves the selected field down in the Report fields list
	Moves the selected field to the top of the Report fields list
	Moves the selected field to the bottom of the Report fields list

## 23.1 Event report

On this sub-tab, event reports are created, which can give a detailed report about the events. Event reports have a variety of report fields and filter types.

Event reports can have event, user, identification, host, device, input and security area detail fields.



An example of the event report can be seen below which consists of one sheet.

Time	Event reason	Event type	Door name	Direction	First name	Last name	Employee number	Company	Department
2017-07-26 14:29:58	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-26 14:18:49	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-26 13:41:15	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-26 13:41:02	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-25 16:46:55	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-25 16:45:33	User identified	Access granted	Office entrance	Entry	Smith	Jackie	2334	Department	Sales
2017-07-25 16:45:30	User identified	Access granted	Office entrance	Entry	Smith	Jackie	2334	Department	Sales
2017-07-25 16:45:24	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-25 16:45:07	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-25 16:44:58	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-25 16:44:51	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales
2017-07-25 16:44:39	User identified	Access granted	Office entrance	Exit	Smith	Jackie	2334	Department	Sales

## 23.2 Occupancy report

On this sub-tab, occupancy reports are created, which give a detailed report about the APB areas and users that go through them. Occupancy report sub-tab does not contain a calendar, but instead periods of time are selected for the report. As well, there are only three filter types: APB areas, Department and Company.

- **Report type.** Indicates the type of occupancy report will be created. There are two report types:
  - **Detailed.** The occupancy report will include Summary and Detail sheets. The Detail sheet includes Report fields information and displays users in their current APB area.
  - **Summary.** The occupancy report will only include Summary field. In Summary field, it displays the user amounts that are currently in active APB areas.
- **Event type.** Indicates what type of events will be used while generating an Occupancy report. By default, the setting is set on Access control events.
  - **TA clock in/clock out events.** Uses clock-in and clock-out events. These events are generated when readers door setting Time & attendance is set on **Clock-in, Clock-out or Clock-in/Clock-out**.
  - **Access control events.** Uses "Access granted" events. When a report is generated, only the first and the last "Access granted" events are used for every single day.
  - **PC logon events.** Uses events generated by logon programs.
  - **Access control and PC logon events.** Uses the first and last "Access granted" of the day and logon programs generated events.
- **Group by.** Indicates by what group the occupancy report will be created. By default, the setting is set on APB area.
  - **-.** Groups users by their activities during certain time period, **Analyze events of last**.
  - **Department.** Groups user's activities by created departments. If in certain departments there are no activities, they won't be included in the report file.
  - **APB area.** Groups user's activities by APB areas. If in certain APB areas there are no activities, they won't be included in the report file.
- **Analyze events of last.** Indicates the time period that will be analyzed on the report from the current time the report is created. By default, this setting is set on 48 hours.
- **Highlight event if older than.** Highlights Time of last use fields time intervals in bold, which exceeds the selected time interval. By default, this setting is set on 24 hours.

Possible report fields for Occupancy reports:

- Middle name.
- Title.
- Phone.
- E-mail.
- Messenger.
- Additional field 1, 2 & 3.

An example of the occupancy report can be seen below which consists of a Summary and Detail sheets, grouped by APB area.

Area	Users
Office 1 area	1
Users with no activity during the last 48 hours	12
<b>Total users:</b>	<b>13</b>

Area	Office 1 area									
First name	Middle name	Last name	Department	Time of last use	Place of last use	Title	Phone	Messenger	Email	
Smith	Maria	Jackie	Sales	2017-08-02 10:06:03	Office entrance	VP of Sales	123456789	1233334455	example@email.com	
<b>Total users:</b>	<b>13</b>									

## 23.3 User report

On this sub-tab, user reports are created, which give a detailed report about the users, depending on the selected report fields. User report has User, Access level, Department, Company and User title filters.

The interface shows a 'Filter' section with the following options:

- Access level: Select Filter
- Department: Select Filter
- Company: Select Filter
- User Title: Select Filter
- Location: Select Filter
- User type: Select Filter
- TBA type: Both
- User status: Active

The 'Report fields' section includes:

- Middle name
- Phone
- Email
- Company
- Messenger
- Additional field 1
- Additional field 2
- Additional field 3
- Access levels
- Activation date
- Expiration date
- Work schedule
- Employee number
- Active card numbers
- Deleted card numbers
- User type
- License plates
- Contract number
- Contract date
- Payment condition
- Payment balance

At the bottom, there is a 'Generate report' button and a note: 'Note: additional filters turned on'.

- **One user per page (checkbox).** Rather than adding users to one sheet page, users are separated by sheet pages if this function is enabled.
- **Group by.** Indicates how users will be grouped in the report file. By default, the users aren't grouped.
  - -. Does not group users by any criteria.
  - **Department.** Groups users by their departments.

An example of the user report can be seen below which displays detailed user information.

Photo	Last name	First name	Department	Title	Middle name	Phone	Email	Company	Messenger	Employee number	Activation date	Expiration date	User type	Access level
	Admin	Admin									2017-07-31 12:46:30		Admin	
	Bobby	Bob	Sales			0888888	123456@gmail.c	Department	123456	123456	2018-06-20 00:00:00	2018-06-29 23:59:00	User	
	Jackie	Smith	Sales	VP of Sales	Maria	1123456789	example@email.com	Department	1122334455	2334	2017-08-02 00:00:00		User	

## 23.4 Door report

On this sub-tab, door reports are created, which give a detailed report about the doors. Door report sub-tab only contains one filter type, Doors, and only has a handful of report fields.

Report template: Default device report template

Title: Device report  
 Subtitle: New device report  
 Page numbering  
 Report date and time  
 Show report header on each page  
 eco-friendly  
 Limit: 50000

Available fields: Door name, Direction, Type, Reader mode, IP, MAC

Filter: Doors  
 Location: Select filter  
 Select all Total 21 Selected 0  
 1st floor  
 1st turnstile  
 2nd floor  
 2nd floor  
 3rd floor  
 4th floor  
 Büro patalajok - 1  
 Büro patalajok - 2  
 Cafeteria  
 Controller door  
 Lobby  
 Manager's office  
 Meeting room  
 Mercury door  
 Mobile 2  
 Mobile door  
 Mobile door 2  
 Office entrance

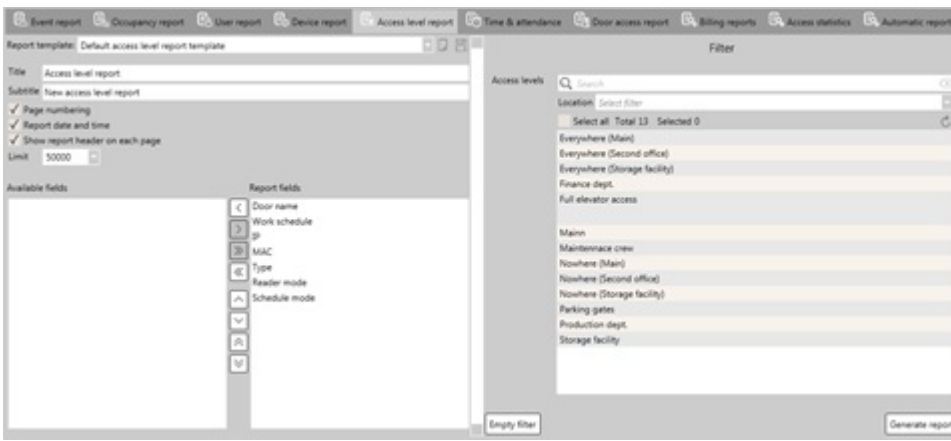
Buttons: Empty filter, Generate report

An example of the door report can be seen below which displays information about the doors.

Door name	Direction	Type	Reader mode	IP	MAC
1st turnstile	Entry	Reader	CardOnly	169.254.242.129	00:06:8E:40:F9:18
2nd floor	Entry	Reader	CardOnly	192.168.0.249	
3rd floor	Entry	Reader	CardOnly	192.168.0.249	
4th floor	Entry	Reader	CardOnly	192.168.0.249	
Cafeteria	Entry	Reader	CardOnly	169.254.242.130	00:06:8E:02:AC:8A
Cafeteria	Exit	Reader	CardOnly	169.254.242.130	00:06:8E:02:AC:8A
Manager's office	Entry	Reader	CardOnly	192.168.0.251	
Meeting room	Entry	Reader	CardOnly	169.254.242.98	00:06:8E:40:72:82
Office entrance	Entry	Reader	CardOnly	192.168.0.100	00:06:8E:02:59:A7
Office entrance	Exit	Reader	CardOnly	192.168.0.100	00:06:8E:02:59:A7

## 23.5 Access level report

On this sub-tab, access level reports are created, which give a detailed report about the access levels. Access report sub-tab only contains one filter type, Access levels, and only has a handful of report fields.

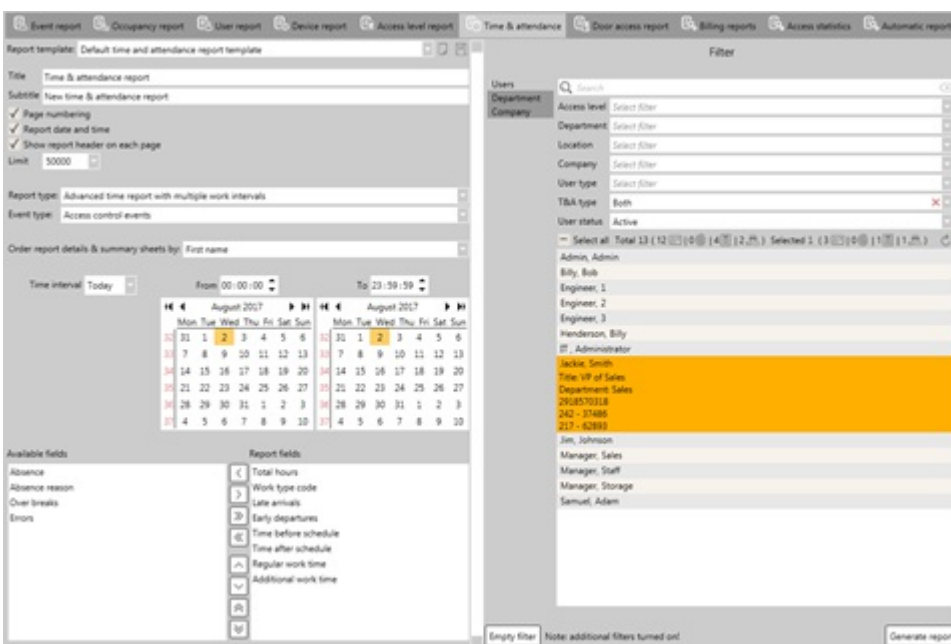


An example of the access level report can be seen below which displays information about the access levels.

Access level: Finance dept.						
Door name	Work schedule	IP	MAC	Type	Reader mode	Schedule mode
Controller door	Exit : Always	192.168.0.200	000FE50231E5	Reader	Card only	Not set
Controller door	Entry : Always	192.168.0.200	000FE50231E5	Reader	Card only	Not set
Access level: Full elevator access						
Door name	Work schedule	IP	MAC	Type	Reader mode	Schedule mode
1st floor	Entry : Always			Reader	Card & fingerprint	Not set
2nd floor	Entry : Always	192.168.0.249		Reader	Card only	Not set
3rd floor	Entry : Always	192.168.0.249		Reader	Card only	Not set
4th floor	Entry : Always	192.168.0.249		Reader	Card only	Not set
1st turnstile	Entry : Always	169.254.242.129	00:06:BE:40:F9:1B	Reader	Card only	Not set

## 23.6 Time & attendance report

On this sub-panel, time and attendance reports are generated for users with Simple and Advanced **T&A type**. The main important thing while creating a T&A report, is to be sure that schedules are configured correctly, users T&A type status and if clock-in and clock-out function is used, check door configuration.



- **Report type.** This function is deprecated.
- **Event type.** Indicates what type of events will be used while generating a T&A report.



- **TA clock in/clock out events.** Uses clock-in and clock-out events. These events are generated when readers door setting Time & attendance is set on **Clock-in, Clock-out** or **Clock-in/Clock-out**.
- **Access control events.** Uses "Access granted" events. When a report is generated, only the first and the last "Access granted" events are used for every single day.
- **PC logon events.** Uses events generated by logon programs.
- **Access control and PC logon events.** Uses the first and last "Access granted" of the day and logon programs generated events.
- **Use first and last events only (checkbox).** While generating a T&A report, only the first and the last events will be used of the day. This function is only available for **TA clock in/clock out events** and **PC logon events**
- **Order report details & summary sheets by.** Orders the users by the selected order, on reports Summary and Details tabs. Possible orders:
  - **First name.**
  - **Last (Family) name.**
  - **Title.**
  - **Employee number.**
  - **Department.**

T&A report has different fields for generating a report than other report types. Possible report fields for T&A report are displayed in the table below.

Field	Description	Calculation
Total hours	The total work time	Sums up all of the time that the user has spent during the day. Mandatory break times are not included.
Regular work time	The work time during the schedule	Displays the amount of time a user has spent during the schedule time. This time cannot exceed the total work time of the schedule. If the schedule time is exceeded, the maximum schedule time is presented and the remaining time is classified as additional work time.
Late arrivals	Displays the time of a late arrival	If a user checks in after the schedule has started, the amount of time has been passed since the schedule has started, will be classified as late time.
Early departure	Displays the time of early leave	If a user checks out before the schedule ends, the time that was left until the schedule end will count as early departure.
Time before schedule	Displays the time the user worked before schedule started	If a user comes early, the time from when the user arrived to the start of the schedule will count as time before schedule.
Time after schedule	Displays the time the user worked after schedule started	If a user leave's after the schedule already have ended, the time from the schedules end to when the user finally leave, will count as time after schedule.
Additional work time	Displays all of the additional time the user has worked	Any time the user works that is not included in the schedule or working while on optional break time, it will count as additional work time.
Over break	Displays the overtime of break times	If a user exceeds the break time, the time after the break time and the next time a user clocks-in, will count as over break time.
Absence	Displays the amount of time the user was absent	The absences time is generated when a user is absent the whole day, then the work schedule time becomes the absences time. Also, absences time can be generated by the monitoring personal, who create an absent day for the user.

Absence reason	Displays the reason of absences	The absences type is depended on the monitoring admin.
Work type code	Displays the schedules work type	Work types are assign to schedules or to readers.
Errors	Displays an error message of bad calculations	If a bad calculation is made, an error message is displayed (Start or End time missing), describing the reasons of it. Usually the errors display when a segment of work interval is incomplete.

Time and Attendance report file consists of 5 sheet pages:

- **Summary.** Displays a summary of worked days and report fields for selected users.

Employee number	Line No.	First name	Last name	Department	Title	Type	Days worked	Total hours	Regular work	Late arrivals	Early departure	Over breaks	Time after	Time before	Addition of work	Absence
2334	0	Smith	Jackie	Sales	VP of Sales		3	28.86	23.85	6.47	2.33	2.15	12.45	6.56	6.89	18.89
Manual adjustment							0	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Total:							3	28.86	23.85	6.47	2.33	2.15	12.45	6.56	6.89	18.89

Information fields that are used in the Summary sheet page:

- **Employee number.** Users employee number.
  - **Line No.** The number of the user in the T&A Summary page list.
  - **First name.** Users First name.
  - **Last name.** Users Last name.
  - **Department.** The department user is assigned to.
  - **Title.** Users title.
  - **Type.** Type field consists of three rows:
    - The initial report calculation.
    - Manual adjustments are made here.
    - The total report calculations, that sums up the initial report calculations with the manual adjustments.
  - **Days worked.** Displays how many days a user has worked.
  - **Report fields.** Fields from the Report fields are presented, such as Total hours, Regular work, Late arrivals, Early departure, Over breaks, Time after schedule, Time before schedule, Additional work time and Absence fields.
- **Details.** More detailed page, where selected users T&A work schedules are presented in detail, depending on the selected T&A report settings and report fields.

Date	Work schedule	Work type code	Clock in	Clock out	Errors	Total hours	Time before schedule	Time after schedule	Late arrivals	Early departures	Regular work time	Addition of work time	Over breaks
2017-06-13	Work day - type 1	Ni	2017-06-13 07:37	2017-06-13 12:10	-	04:32:37	00:22:03	00:00:00	00:00:00	00:00:00	04:00:00	00:32:37	00:00:00
2017-06-13	Work day - type 1	Ni	2017-06-13 13:33	2017-06-13 17:30	-	04:29:32	00:00:00	04:30:40	00:00:00	00:00:00	04:00:00	00:39:32	00:00:00
2017-06-14	Work day - type 1	Ni	2017-06-14 07:46	2017-06-14 17:27	-	09:38:35	00:11:33	04:26:59	00:00:00	00:00:00	08:00:00	01:38:35	00:00:00
2017-06-15	Work day - type 1	Ni	2017-06-15 08:28	2017-06-15 16:29	-	08:00:49	00:00:00	00:29:05	00:28:33	00:00:00	07:00:49	01:00:00	00:00:00

Information fields that are used in the Details sheet page:

- **Date.** Indicates the date of specific T&A work time interval (YYYY-MM-DD).
  - **Work schedules.** Indicates users work schedule during the specific time period.
  - **Work type code.** Indicates work schedules code.
  - **Clock in.** Indicates when a user generated a clock-in event (YYYY-MM-DD hh:mm).
  - **Clock out.** Indicates when a user generated a clock-out event (YYYY-MM-DD hh:mm).
  - **Report fields.** Selected report fields are then presented.
- **Schedules.** Displays all created T&A work schedules, presenting them in detail. Simple schedules from



Information fields that are used in the Time card sheet page:

- **Line No.** The number of the user in the T&A Time card page list.
- **Time sheet number.** This function is deprecated.
- **Employee number.** Users employee number.
- **Department.** The department user is assigned to.
- **First name and family name.** Users First name and Family name.
- **Title & qualifications.** Users title.
- **Number of work hours per month.** Displays the total work hours in the months interval. T&A advanced schedules have to be configured.
- **Days.** Displays all days of the month. Green fields represent weekends while red fields represent absence or errors. The numbers on the months days represent the total work time of those specific days.
- **Actual number of work hours per month.** More detailed information about work hours per month is presented here, separated into segments:
  - **Days.** Indicates how many days of the month a user has attended.
  - **Total.** Indicates the total work hours that a user has worked per month.
  - **Night time.** Indicates the total night work hours that a user has worked per month.
  - **Deviations.** Deviation per month calculations should be made here. This is an editable field, which should be filled by the administrator.
  - **On duty at home.** Indicates how many hours a user has worked per month from home environment. This is an editable field, which should be filled by the administrator.
  - **On duty at work.** Indicates how many hours a user has worked per month from a work place. This is an editable field, which should be filled by the administrator.
  - **Days off.** How many day-offs a user had per month. This is an editable field, which should be filled by the administrator.
  - **Holidays.** How many holiday days a user had per month. This is an editable field, which should be filled by the administrator.
- **Absences.** Absences calculation and information are displayed here.
  - **Legend.** A legend is given by an administrator. This is an editable field, which should be filled by the administrator.
  - **Number of days.** How many days a user has been absent per month.
  - **Number of hours.** How many hours a user has been absent per month.

## 23.7 Door access report

On this sub-tab, Door access reports are created, which give a detailed report about users who has access through specific doors. Door access report configuration only has one calendar field, which means that the report can be created for a specific date and time. Door access report sub-tab contains three filter types: Users, Doors and Company. In the field section, fields from User tab are present.

While creating a door access report, it is recommended to select manually which doors and users should be included in the report for better results.

An example of the door access report can be seen below which displays information about the door access for a specific door.

Photo	Last name	First name	Department	Title	Middle name	Phone	Email	Messenger	Employee number	Access level	Activation date	Expiration date	Additional field 1
	Jackie	Smith	Sales	VP of Sales	Maria	329456789			2334	Everywhere	Jun 20 2018 10:52AM		

## 23.8 Billing report

On this sub-tab, Billing reports are created, which give a detailed report about users billing calculations during a time period. Billing report sub-tab contains these filter types: Users, Department, Company and Access levels.

- **Sum report rows.** Indicates by what order the report the data will be presented.
  - **By user.** Orders the rows by users First name.
  - **By company.** Orders the rows by companies alphabetically.
  - **By Department.** Orders the rows by departments alphabetically.
- **Currency.** Indicates currency that is being used. The currency type has to be written manually.
- **Unit.** Indicates units.
- **Exclude users without activity (checkbox).** User who were inactive during the selected time period, won't be included in the billing report.

In the field section, fields from User tab are present, as well additional fields are included, specifically used for billing calculations.

- **Row number.** The reports tables row list.
- **Total transaction count.** Indicates how many times a transaction was made.
- **Total for all transactions.** Displays the total price number of all transactions.
- **Contract number.** Displays the users billing contact number.
- **Contact date.** Displays the users billing contact date.
- **Payment conditions.** Displays the users billing payment conditions.
- **Average transaction price.** Indicates the average transaction price for the user.
- **Currency.** Displays the currency.
- **Unit.** Displays the unit.
- **Document date.** Indicates the date of the transaction calculation date.

Billing report file consists of 3 sheet pages:

- **Summary.** Displays a summary of billing calculations and report fields for selected users.

Row number	First name	Last name	Employee number	Department	Title	Total transaction count	Total for all transactions	Currency	Contract number	Payment condition
1	Administrator	IT	223311	IT	IT administrator	10	22.00 Euro	Euro	321546	Detract from monthly salary
2	Smith	Jackie	2334	Sales	VP of Sales	6	13.20 Euro	Euro	321654	Detract from monthly salary
3	Johnson	Jim	123456	Sales	Manager	0	0.00 Euro	Euro	321654	Transfer payment through bank

- **Details.** More detailed page, where all transactions are displayed in detail, depending on the selected billing report settings and report fields.

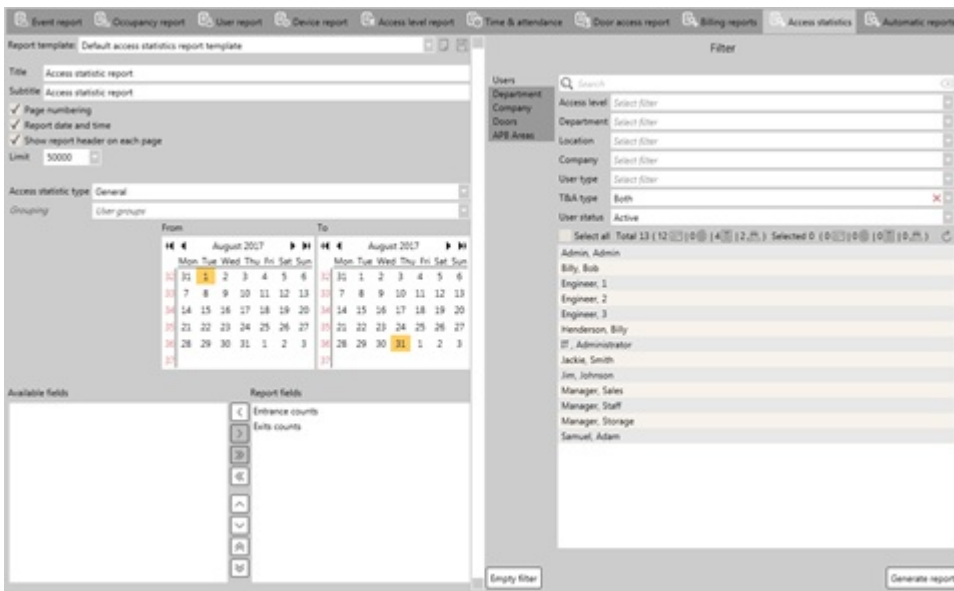
Date	Schedule	Time	Amount of transactions	Reader	Employee number	Contract number	Contract date	Payment condition	Payment balance
2017-08-04		09:55:35	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		09:55:39	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		09:55:39	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		09:55:45	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		09:55:47	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		09:55:53	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		10:01:41	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		10:01:41	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		10:01:44	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro
2017-08-04		10:01:44	-2.20 Euro	Cafeteria - reader	223311	321546	2017-08-01	Detract from monthly sal	-22.00 Euro

- **Chart.** A chart is displayed of selected months for selected users, displaying how many transactions are made by users on every day of the month, the total amount of transactions in a month and card numbers that were used.

Employee number	Days	Total count	Card numbers
1	1		
2	2		
3	3		
4	4		
5	5		
6	6		
7	7		
8	8		
9	9		
10	10		
11	11		
12	12		
13	13		
14	14		
15	15		
16	16		
17	17		
18	18		
19	19		
20	20		
21	21		
22	22		
23	23		
24	24		
25	25		
26	26		
27	27		
28	28		
29	29		
30	30		
31	31		
Monthly totals		19	

## 23.9 Access statistics

On this sub-tab, Access statics reports are created, which display the amount of entrance and exits that has happened in all departments in the specific time period. Access statistics report sub-tab contains these filter types: Users, Department, Company, Doors and Access levels.



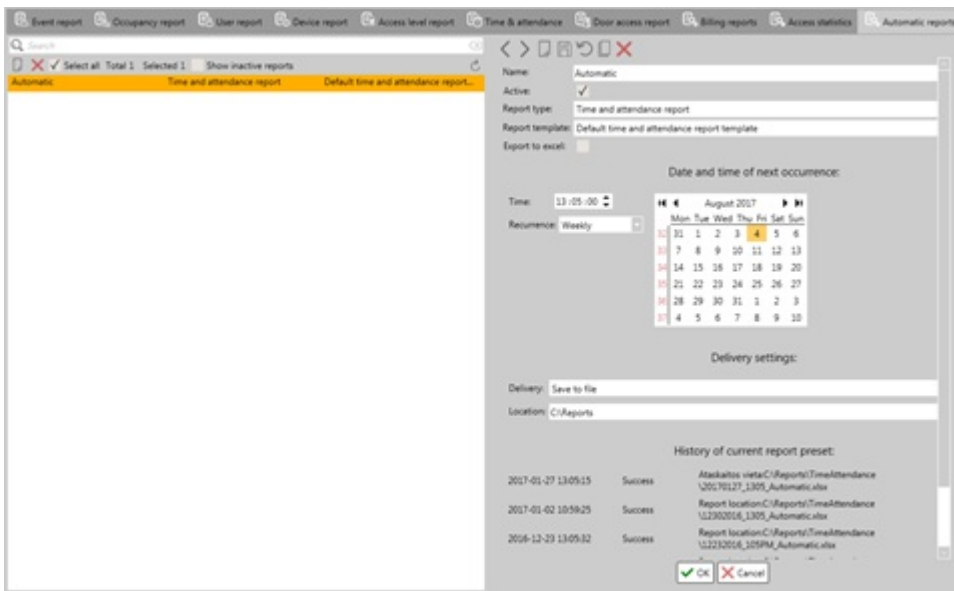
- **Access statistic type.** Indicates how much detailed the access statistics should be.
  - **General.** Creates a report which displays a general amount of access made by each user in the selected time period.
  - **Detailed by month.** Creates a report which displays access made in monthly periods.
  - **Detailed by week.** Creates a report which displays access made in weekly periods.
  - **Detailed by hours.** Creates a report which displays access made in hourly periods.
- **Grouping.** Indicates how the report should be grouped by. This function is only available for **Detailed by month** access statistics type, which has two grouping types: User groups and Months. Other access statistics types use User group.

An example of the access statistics report can be seen below which displays information about the entrances and exits counts for each user, using **Detailed by month** access statistics type.

Group	Month	Entrance count (IN)	Exit count (OUT)
Without department (1)	2017-08	0	0
	Total	0	0
IT (1)	2017-08	10	0
	Total	10	0
Sales (2)	2017-08	9	0
	Total	9	0
All groups	2017-08	19	0
	Total	19	0

## 23.10 Automatic reports

On this sub-tab, automatic reports are created, which create selected reports automatically over time periods. This sub-tab is different from other report tabs, as it contains a list and details panel, where individual automatic reports are created.



Automatic report details panel is divided into 4 parts:

- **Report details.** Details about the automatic reports are chosen here.
  - **Name.** The name of the automatic report.
  - **Active (checkbox).** Indicates if the automatic report is enabled or not.
  - **Report type.** Indicates the report type of created automatic report.
  - **Report template.** Indicates the report template from the **Report type** which will be used for the created automatic report.
  - **Export to excel (checkbox).** Exports the report in excel format. By default, this function is disabled.
- **Date and time of next occurrence.** Indicates when the automatic reports start and the time interval between these reports.
  - **Time.** Indicates the time of day the report is generated.
  - **Recurrence.** Indicates the occurrence rate.
    - **One time.** Generates an automatic report once.
    - **Daily.** Generates an automatic report daily.
    - **Weekly.** Generates an automatic report weekly.
    - **Monthly.** Generates an automatic report monthly.
  - **Calendar.** Indicates from which date automatic reports should start.
- **Delivery settings.** Indicates where the file automatic reports will be saved.
  - **Delivery.** Indicates how the report file will be delivered. By default, there is only one option **Save to file**.
  - **Location.** Indicates the location where the report files will be saved. The location is either typed in or selected by clicking on the **Select location** button, located on the right side of the **Location** field.
- **History of current report preset.** Displays automatic report logs, where it displays the time when the report was generated, the success or failure status, the location where the event is generated and a button which leads to the location where the report is generated.

## 24. Settings

All manner of changes can be done to CredoID through Settings tab. To have an optimized CredoID, it is advised to check and setup available settings, such as backup, language, module and much more can be done. Settings tab is categorized into groups:

- Backup;
- Automatic reports;
- Data exchange;
- Miscellaneous;
- System;
- Language;
- Real time connection to Access Control Service.

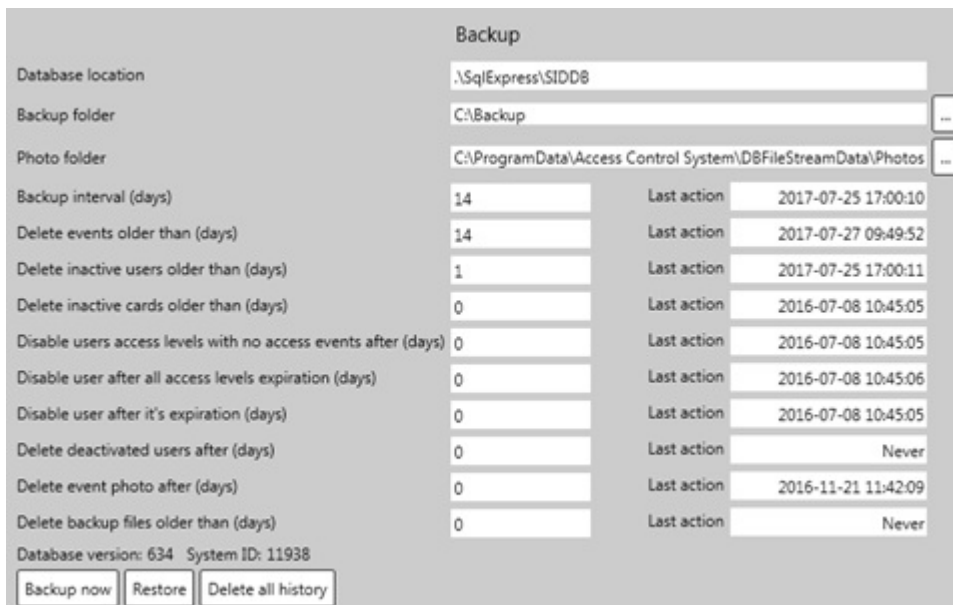




## 24.1 Backup settings

On this section, database settings, location of backups and photos folder can be configured, as well backups and restores can be made. As well, it is possible to setup to remove older events, photos, backups, inactivate user and much more, depending on how old they are.

If a setting is set as „0“, contents won't be removed. **Last action** indicates when was the last time content was removed.

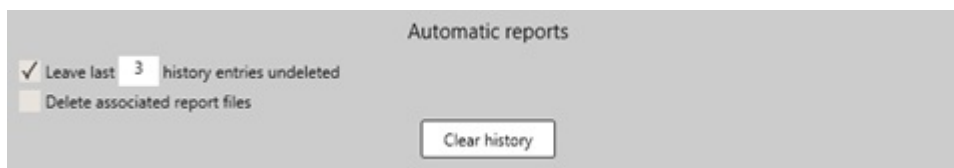


- **Database location.** Displays the database that is currently being used from SQL server. This field is not editable.
- **Backup folder.** The location where the backup files will be stored. Either edit the location in the field or by selecting the directory, using the button on the right side of the field. Note, that database backups are stored on the hard drive of the database server.
- **Photo folder.** The location where the camera photos will be stored. Either edit the location in the field or by selecting the directory, using the button on the right side of the field.
- **Backup interval.** Automatic backup file feature. Indicates the time interval when an automatic backup file made.
- **Delete events older than.** Indicates how long events stay in the database until they are removed.
- **Delete inactivate users older than.** Indicates how long inactivate users stay in the database until they are removed.
- **Delete inactivate cards older than.** Indicates how long inactivate cards stay in the database until they are removed.
- **Disable users access levels with no access events after.** Indicates how long until user access level becomes inactive.

- **Disable user after all access levels expiration.** Indicates how long a user stays active in the database after all access levels have been expired or inactive.
- **Delete user after its expiration.** Indicates how long a user stays active after its expiration and then deactivating the user.
- **Delete deactivated users after.** Indicates how long deactivated users stay in the database until they are removed.
- **Delete event photo after.** Indicates how long event photos stay in the database until they are removed.
- **Delete backup files older than.** Indicates how long backup files stay in the **backup folder** until they are removed.
- **Database version.** Indicates the database version, which is scripted by SQL from the database.
- **System ID.** Indicates the systems ID number, which is randomly generated in the database. This ID is sent to the controllers to identify with which database it is currently working with. If the ID's don't match, the controller becomes un-synced with the database.
- **Backup now (button).** Creates a backup file in the **Backup folder**
- **Restore (button).** Brings up a Backup window, which shows backup files from the **Backup folder**. By selecting a backup file and clicking „OK“, backup restore process starts. After backup restore is complete, CredolD service and GUI has to be restarted to complete the process.
- **Delete all history (button).** Deletes all old card (inactive, unused), users (deactivated) and events from the database. When using this feature, it is recommended to backup your database first in case sensible data is lost.

## 24.2 Automatic reports settings

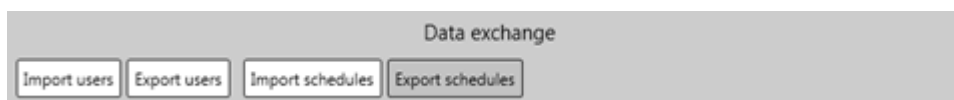
Additional settings for automatic reports. For more information on automatic reports, follow section [23.10](#).



- **Leave last [insert number] history entries undeleted.** How many automatic report history entries will be left while older ones are removed. By default, this feature is enabled and set for 3 entries.
- **Delete associated report files.** **This function is deprecated.**
- **Clear history (button).** Removes all automatic report history entries from the database.

## 24.3 Data exchange settings

User and Time & attendance imports and exports are made on this section. Note that user and **T&A export functions are deprecated** and their functionalities are limited.



### 24.3.1 Import users

Opens Data import window, where user imports can be done. Upon clicking on the button, a warning message is displayed, which warns the user of possible data corruptions if data imports are done incorrectly. It is recommended to create a backup file before importing users to the current database in case sensible data is lost or due of data corruption.

Data import configuration window consists of Data import section, Import configuration settings which differ with different **Source** types, Duplicate record treatment, Automatic import settings, Data binding, Additional settings and Preview sections.

- **Data import settings.** On this section, first import configuration processes are made, such as identifying the import file source and primary keys.
  - **Source.** Select the method for data import. There are 3 methods to import user data, which each have their own configuration window:
    - **Spreadsheet.** Imports user data from a file located in the local folders. Only 2 formats can be imported: .csv and .xls types.
    - **Active Directory.** Users are imported from server "Active Directory User and Computer" list.
    - **Other database.** Users are imported from Orucul or SQL database libraries.
  - **Character set.** Indicates character set that will be used while importing. By default, "Unicode (UFT-8)" character is selected.
  - **Has header now (checkbox).** If the import file or list has implemented headers, this checkbox should be enabled to not import the first row as user data (which is usually the headers). When enabled, the first row will be indicated as the header field. This helps to bound headers more easily on the **Preview** section.
  - **Primary key.** Indicates the primary key by which CredoID treats the users by while importing data. If a duplicate user is found, it adds to the imported user the additional data it has to already imported user (such as card identifications). By default, "First and family name" is set as a primary key.
  - **Table/Sheet.** Select which sheet should be imported. This is only available for Spreadsheet source type and when the file sample is imported while it has multiple sheets.
  - **Starts from row.** Indicates the starting row of the import sample.
- **Spreadsheet – Separator options.** On this section, separator settings are done, which indicates how words are separated on the import file. This section is only available for Spreadsheet source type and when an .csv import sample is imported. .xls file format does not have separator options.

It is advised to first open the sample file which will present the files data in the **Preview** section. By reviewing the files lines, separator changes can be made and in the Preview section changes will be made. An example of a correct spreadsheet import configuration settings can be seen above. Possible separator settings:

- **Tab.**
  - **Semicolon.**
  - **Comma.**
  - **Space.**
  - **Trim whitespace.**
  - **Other.** Type in a separator character.
  - **Text delimiter.** If words have a delimiter, they can be removed by selecting the correct delimiter.
- **Active Directory – Connection.** Connection to the Active Directories server is made here, from where it will import user data.

- **LDAP Connection string.** The connection string to the Active Directories user library.
  - **User name.** User name which is used to connect to the Active Directory.
  - **Password.** Password which is used to connect to the Active Directory.
  - **TEST.** Test the connection to the Active Directories user library. If connection is made, the user data can be seen on the **Preview** section.
- **Other database – Connection.** Connection to the database server and libraries are made here. As well, results can be reviewed and data can be saved. This section is only available for Other database source type.

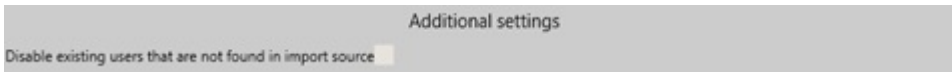
- **Database type.** ODBC or MS SQL database type is selected here.
  - **Connection string.** Indicates the string to the database.
  - **Table/View.** Indicate the table which will be imported.
  - **Preview data (button).** After clicking, the sample data is imported on the **Preview** section.
  - **Dump data.** Save the import data from the database to a file.
- **Duplicate record treatment.** Settings which indicates what actions are taken when duplicate data is imported.

- **User data.** Possible actions: Overwrite, Modify or Do not modify.
  - **Access levels.** Possible actions: Overwrite, Modify or Do not modify. This function is not available for Active Directory source type.
  - **Cards.** Possible actions: Overwrite, Modify or Do not modify. This function is not available for Active Directory source type.
  - **PINs.** Possible actions: Overwrite, Modify or Do not modify. This function is not available for Active Directory source type.
  - **Fingerprints.** Possible actions: Overwrite, Modify or Do not modify. This function is not available for Active Directory source type.
  - **Locations.** Possible actions: Overwrite, Modify or Do not modify. This function is not available for Active Directory and Other database source types.
  - **License plates.** Possible actions: Overwrite, Modify or Do not modify. This function is not available for Active Directory and Other database source types.
  - **Deactivated users.** Possible actions: Activate and update or Skip and log.
  - **Same card/PIN issued to multiple users.** Possible actions: Activate latest or Skip and log.
- **Automatic import settings.** On this section, automatic imports can be configured, so that from a specific folder, imports are made after a duration of time. Note, that after automatic import settings are configured. The Credoid service and GUI should be restarted.

- **Active automatic imports (checkbox).** Activates automatic imports function. By default, this function is disabled.
  - **Get import files from.** Location from where the import files will be taken from. By clicking on the button located on the right side of the field, a destination can be chosen. This field is only available for Spreadsheet source type.
  - **File mask.** Indicates the file mask, by which determines what kind of file will be taken from the folder, would it be by name (users\*) or file format (\*.csv or \*.xls). This field is only available for Spreadsheet source type.
  - **Move processed files to.** Location where processed files will be transferred to. By clicking on the button located on the right side of the field, a destination can be chosen. This field is only available for Spreadsheet source type.
  - **Directory scan interval.** Time interval which indicates when the import folder will be scanned. Minimum time is 300 seconds (5 min.) and the maximum is 86400 seconds (24 hours).
  - **Store import logs.** Indicates the maximum number of import log files that can be stored, older import logs will be removed. If this field is left empty or "0", the import logs won't be removed.
  - **View logs (button).** Opens Import logs window, where it displays history of automatic imports.
  - **Delete logs (button).** Removes the history of automatic imports.
- **Data binding.** Binding process buttons which are used to either help the binding process or reset it.



- **Open sample file (button).** A Spreadsheet file is added from here. Only .csv or .xls file formats can be imported. This button is only available with Spreadsheet source type.
- **Auto (button).** Auto binds the imported fields to the correct ones. The results can be reviewed in the Preview section. If the Spreadsheet file has a header row, it is easier to bind the columns by enabling **Has header row**.
- **Reset (button).** Removes all bound headers from the Preview section and makes them unbound.
- **Additional settings.** An additional settings section, where **Disable existing users that are not found in import source (checkbox)** can be enabled or disabled. By enabling this function, while importing users, the existing users are deactivated. By default, this function is disabled.



- **Preview.** Here, a review of the import sample is displayed. This section updates automatically if changes are made, such as changing **Separator options**.

FirstName	MiddleName	LastName	EmployeeNumber	Phone	SecondaryPhone	Email	IMessenger	UserName
First name ▾	Middle name ▾	Family name ▾	Employee number ▾	Phone ▾	Secondary phone ▾	E-mail ▾	Messenger ▾	User name
Bob		Bobby	123456	8888888	9999999	123456@gmail.c	123456	pk

All fields are bound

On the first row, there are built in columns which indicate what information should be where. The second row is the import samples header row, where each column has to be bound to a specific field. After that, other rows indicate import sample data that will be imported.

On the bottom-right corner there is a message which indicates if all fields are bound. If the fields are not bound, the users cannot be imported. There are two types of messages:

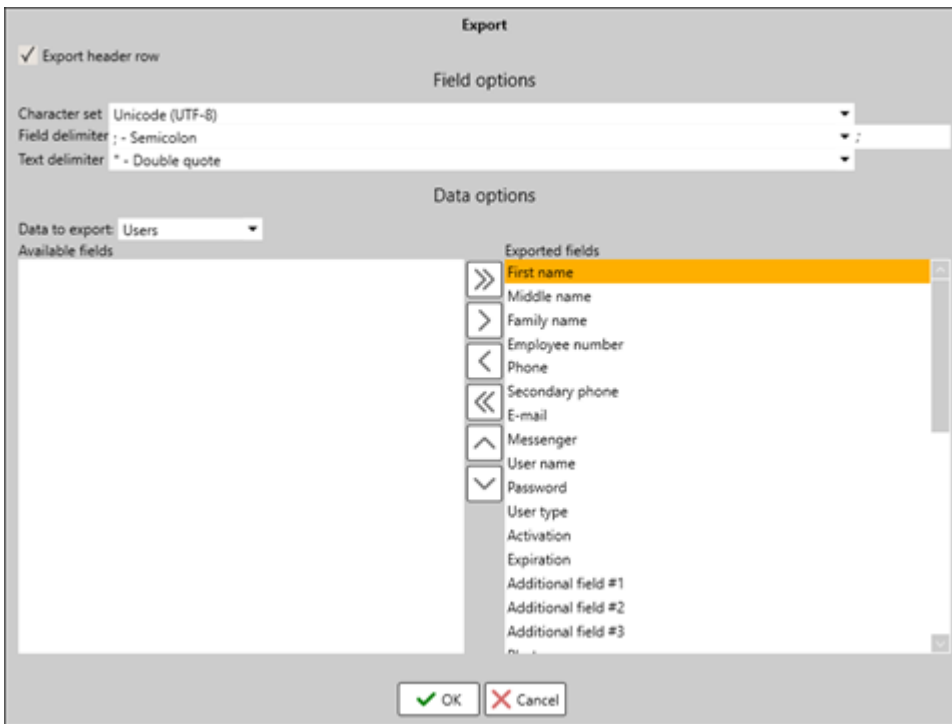
- There are unbound fields remaining (displayed in yellow colors).
- All fields are bound.
- **Data import main buttons.** Buttons, which starts the import process or closes the Data import window.



- **Import (button).** Starts the import process. If the import procedure is done correctly and all columns are bound, the import should be successful. After an import process is done, a log window will be displayed, showing a successful import procedure, warnings and errors.
- **Save (button).** Saves the import settings. The next time Data import window is opened, the settings that were left behind, should remain.
- **Close (button).** Closes the Data import window.

## 24.3.2 Export users

Opens Export window, where user exports can be done. **This function is deprecated** and only limited user exports can be made with .xml file format.

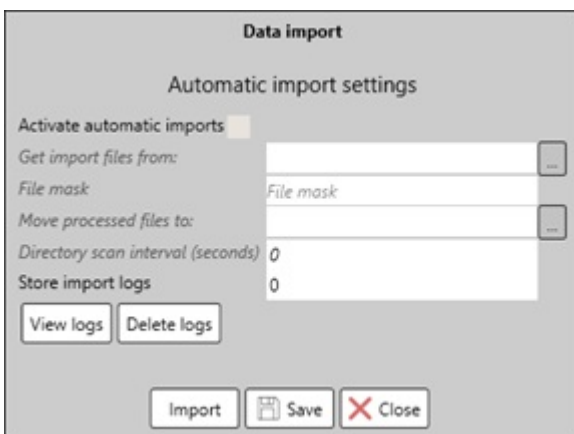


- **Export header row (checkbox).** By enabling this function, header rows will be imported into the export file.
- **Field options.** Separator options and other field options are done here.
  - **Character set.** Indicates character set that will be used while importing. By default, “Unicode (UFT-8)” character is selected.
  - **Field delimiter.** This setting indicates how words are separated on the export file. On the right side of the field, the separator delimiter is displayed.
  - **Text delimiter.** Set a text delimiter.
- **Data options.** Fields are selected here which data will be exported to the file.
  - **Data to export.** **This function is deprecated.**
  - **Available fields.** Displays all available fields that can be exported. The fields that are left here, won't be exported to the file.
  - **Exported fields.** Displays fields which will be exported to the file.

### 24.3.3 Import schedules

Opens Data import window, where automatic Time and attendance work schedules can be imported. Upon clicking on the button, a warning message is displayed, which warns the user of possible data corruptions if data imports are done incorrectly. It is recommended to create a backup file before importing T&A work schedules to the current database incase sensible data is lost or due of data corruption.

Automatic import settings and procedure is similar to user import, which is described in the [24.3.1](#) section. The import file sample of .xml file format is described in the [25.2](#) section.



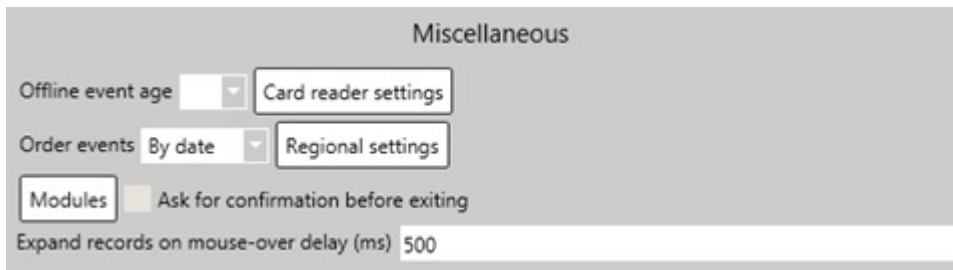
- **Active automatic imports (checkbox).** Activates automatic imports function. By default, this function is

disabled.

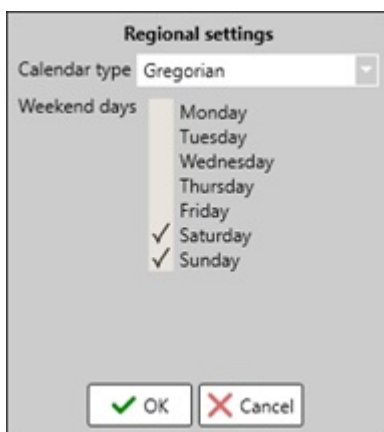
- **Get import files from.** Location from where the import files will be taken from. By clicking on the button located on the right side of the field, a destination can be chosen.
- **File mask.** Indicates the file mask, by which determines what kind of file will be taken from the folder, would it be by name (schedule\*) or file format (\*.xml). This field is only available for Spreadsheet source type.
- **Move processed files to.** Location where processed files will be transferred to. By clicking on the button located on the right side of the field, a destination can be chosen.
- **Directory scan interval.** Time interval which indicates when the import folder will be scanned. Minimum time is 300 seconds (5 min.) and the maximum is 86400 seconds (24 hours).
- **Store import logs.** Indicates the maximum number of import log files that can be stored, older import logs will be removed. If this field is left empty or "0", the import logs won't be removed.
- **View logs (button).** Opens Import logs window, where it displays history of automatic imports.
- **Delete logs (button).** Removes the history of automatic imports.
- **Import (button).** Imports .xml file format import file.
- **Save (button).** Saves the import settings. The next time Data import window is opened, the settings that were left behind, should remain.
- **Close (button).** Closes the Data import window.

## 24.4 Miscellaneous settings

A variety of different settings can be configured on this section.



- **Offline event age.** If set, the system checks time stamps of each event received from controllers. If the difference between the time stamp of an event and current system time is significant (user-configurable), the event will be recorded to the database without processing. Pop-up messages will not be displayed on maps and linked actions (video, email, SMS) will not be executed. Recommended setting if controllers disconnect and accumulate offline events.
- **Card reader settings (button).** **This function is deprecated.**
- **Order events.** Orders received events by data or by database ID number. This is useful when received events have incorrect time. By default, Order events is set by data.
- **Regional settings (button).** Opens Regional settings window, where regional options can be set. After changes have been made, restart of CredoID service and GUI is required.

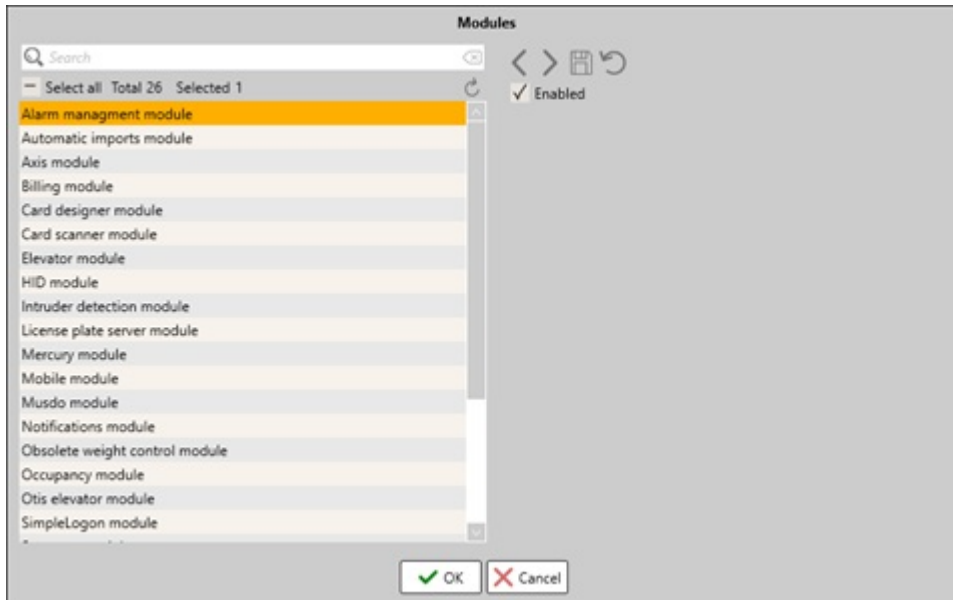


- **Calendar type.** Select the type of calendar that will be used in CredoID. Possible options: Gregorian or Persian.
- **Weekend days.** Select weekend days that will be used in CredoID.



- **Ask for confirmation before exiting (checkbox).** When enabled, when exiting the software, it will be required to present a user name and password of a user with the rights to do so.
- **Expand record on mouse-over delay.** The time it takes for additional information to expand for a selected item (door, user, events and etc.) while hover a mouse over it.
- **Modules.** Opens Modules window, where every single module status can be reviewed and their settings changed. It is important to enable some modules that are disabled by default, such as main tab modules or device modules. Note, that some modules require license for them to work.

The modules window consists of a List panel, where modules are displayed and Details panel, where modules settings are displayed. One of the main modules settings is **Enable** checkbox.



CredolD consists of these modules and their settings:

- **Alarm management module.** Alarm management module which enables Alarm functions in the Monitoring tab [19.8].
- **Automatic imports module.** Enables automatic user and schedule imports [24.3].
- **Axis module.** Enables Axis device compatibility with the software.
  - **Enable automatic discovery (checkbox).** By enabling this feature, CredolD will be able to automatically add Axis controllers to its device list. By default, this function is enabled.
- **Billing module.** Enables billing features in the Access levels [11.2], Reports [23.8], Users [15.2.5] tabs.
- **Card designer module.** Enables Card design tab and its functions [21].
- **Card scanner module.** Enables the feature to use USB devices.
- **Elevator module.** Enables Elevator tab and its functions [7].
- **HID module.** Enables HID device compatibility with the software.
  - **Enable automatic discovery (checkbox).** By enabling this feature, CredolD will be able to automatically add HID controllers to its device list. By default, this function is enabled.
- **Intruder detection module.** Enables all alarming functions for security areas, zones and similar options. This module is used with **MuSDO module**.
  - **Hide logon dialog (checkbox).** **This function is deprecated.**
- **License plate server module.** Enables license plate server (LPR) functions in the Inputs [13] and Occupancy [20] tabs.
- **Mercury module.** Enables Mercury device compatibility with the software.
  - **Enable automatic discovery (checkbox).** By enabling this feature, CredolD will be able to automatically add Mercury controllers to its device list. By default, this function is enabled.
- **Mobile module.** Enables Mobile device compatibility with the software.
- **Musdo module.** Enables MuSDO device compatibility with the software.
  - **Data polling rate.** The refresh time of the communication between the MuSDO device and CredolD, in milliseconds.
- **Notification module.** Notification function settings can be configured here, such as E-mail, SMS, HTTP or Video server notifications, which are used on Users tab [15.3].

For e-mail notification to work, a connection to the mail server and the account is required.

- **Enabled (checkbox).** Enables E-mail notification function, which also makes E-mail fields configurable.
- **Server.** E-mail outgoing mail server. Example, Gmail SMTP server: smtp.gmail.com and for IMAP: imap.gmail.com.
- **TCP service port.** The mails servers TCP port (example, Gmail: 587).
- **From.** E-mail address from which the notifications will be sent from.
- **User name.** E-mail user name, usually is the e-mail address.
- **Password.** E-mails login password.
- **Use TLS (checkbox).** Enables TLS security protocol.

For SMS notifications to work, a mobile modem or a device that can substitute an SMS modem is required. Note, that SMS notifications have a limited symbol amount (160 symbols) and has even less symbols if Unicode is being used (70 symbols). As well, there is a pause interval after each SMS notification and if the notifications are working on a very active system, SMS notifications might not keep up with the system and end up sending messages late.

- **Enabled (checkbox).** Enables SMS notification function, which also makes SMS fields configurable.
- **COM port.** Indicates the COM port which has a modem or a device that can send a SMS message.
- **Baud rate.** Indicates the Baud rate that will be used. This setting should be the same as the modems Baud rate.
- **Data bits.** Indicates the data bits that will be used. This setting should be the same as the modems data bits setting.
- **Stop bits.** Indicates the stop bits that will be used. This setting should be the same as the modems stop bits setting.
- **Parity.** Indicates the parity setting that will be used. This setting should be the same as the modems parity setting.
- **Number of retries.** Indicates the number of tries Credoid will try to send an SMS message if an error occurs, until it timeout.
- **Pause.** The pause interval after an SMS notification is send.
- **Use Unicode (checkbox).** Enables Unicode. Note, that this decreases the SMS length from 160 symbols to 70 symbols.
- **Test communication (button).** Tests the communication between Credoid and modem.

HTTP and Video server notifications are enabled here. Further configurations are done on Users tab, under automatic configurations [\[15.3\]](#).

- **Obsolete weight control module.** This function is deprecated.
- **Occupancy module.** Enables Occupancy tab and its functions [\[20\]](#).

- **Otis elevator module.** Enables Otis device configurations in Device tab and Elevator tab. As well, on the Details panel, further Otis configurations can be done, where DEC's can be assigned to doors readers of other type devices than Otis.
- **SimpleLogon module.** **This function is deprecated.**
- **Suprema module.** Enables Suprema device compatibility with the software.
  - **Enable automatic discovery (checkbox).** By enabling this feature, CredolD will be able to automatically add Suprema controllers to its device list. By default, this function is enabled.
  - **Bit order.** Indicates the bit order that will be used while communicating with Suprema devices.
  - **Byte order.** Indicates the byte order that will be used while communicating with Suprema devices.
  - **Host port.** The host port of Suprema service on CredolD. This is used to communicate with Suprema devices on the same ports. By default, this setting is set on 51212 port.
  - **Fingerprint format.** Indicates the fingerprint format that will be used on the database and on Suprema devices. There are three types of fingerprint formats: Suprema (Suprema own fingerprint format), ISO (Europe standard) and ANSI (American standard). Note, that if there are multiple format fingerprints on the database, a stable connection with Suprema devices will be lost as they might go corrupt as they only except one type of fingerprint format.
- **Tamo module.** **This function is deprecated.**
- **Time and Attendance module.** Enables Time and Attendance tab and its functions [22].
- **Video server module.** Enables Video tab and its functions [8].
- **Visitor.** Enables Visits tab and its functions [16].
- **Web interface module.** Enables Web UI and its functions. **This function is deprecated.**
- **Weight detection module.** **This function is deprecated.**
- **Who is in display module.** **This function is deprecated.**

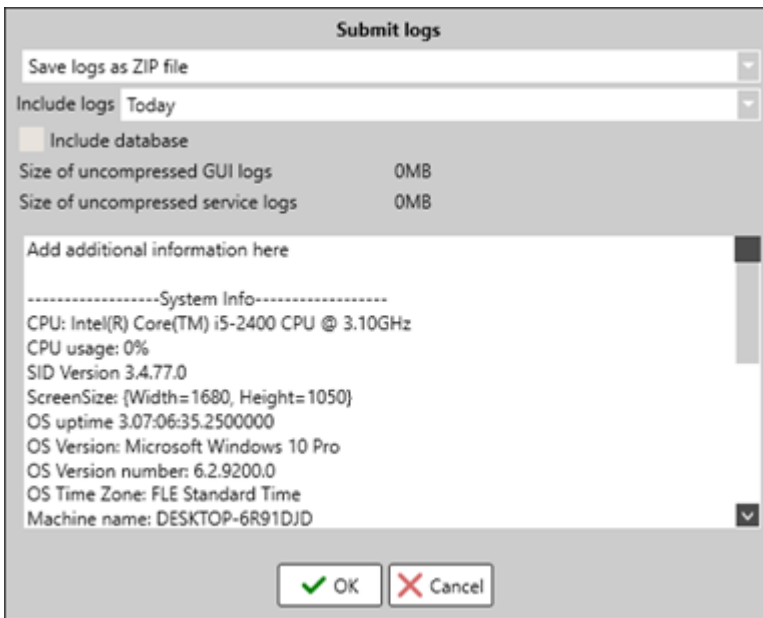
## 24.5 System settings

Additional system process configuration can be done here.

- **Upload data to all controllers (button).** Makes a full data upload to all devices that are currently online.
- **Automatic upload (checkbox).** By enabling this function, any data changes, such as user, access levels, door changes will be automatically send to the online devices whenever a change is made. This way, the devices are kept up to date with the database data. By default, this function is enabled.

Note, that it might be recommended to disable this function in big systems as devices and CredolD might not be able to handle the updating processes of all devices at the same time if multiple changes are made frequently. It would be better to disable this function, make changes and then use **Upload data to all controllers** button to upload all data to the controllers at the same time.

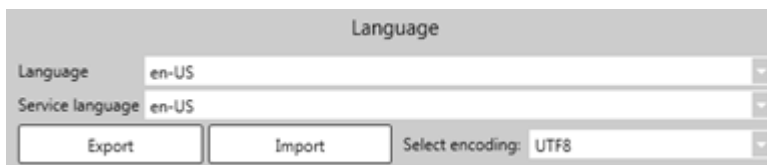
- **Wait for Door Open event when counting users (checkbox).** This function is used for APB areas while counting users. When enabled, users will only be entering an APB area when the Door Open event is registered.
- **Submit logs (button).** Opens Submit logs window where a .zip file or send directly to can be created which will contain log files, database backup file and additional information. As well, displays the size of the submit form and information about the computer system and CredolD.



- **Format submit type.** Indicates the what action is taken with the log and database files. There are 2 possible actions:
  - **Save logs as ZIP file.** Saves all files in a .zip file at the designated location.
  - **Send logs by e-mail.** Sends the data to [support@midpoint.it](mailto:support@midpoint.it) e-mail address. Notification settings must be configured to be able to send an email. **This function is deprecated.**
- **Include logs.** Indicates from which time the logs should be included.
- **Include database (checkbox).** Includes a database backup file into the submit form.
- **Size of uncompressed GUI logs.** Displays the size in MB of GUI log files.
- **Size of uncompressed service logs.** Displays the size in MB of service log files.
- **Show GUI logs.** Opens the folder where GUI log files are stored. By default, GUI log files are stored in C:\ProgramData\Access Control System\GUI\Logs.
- **Show service logs.** Opens the folder where service log files are stored. By default, service log files are stored in C:\ProgramData\Access Control System\Service\Logs.
- **Cancel auto reports.** Cancels every automatic report that will be generated in that day.

## 24.6 Language settings

Language settings are configured in this section, such as choosing the language for CredolD GUI and service. As well, it is possible to import or export language files.



- **Language.** Indicates the language that will be used for CredolD GUI. After changing a language, it is recommended to restart GUI to complete the full changes.
- **Service language.** Indicates the language that will be used for CredolD service. This changes the Service, notifications, reports and logs language. After changing a language, it is recommended to restart GUI and service to complete the full changes.
- **Export (button).** Export the selected GUI language file. In this file, translations can be made.
- **Import (button).** Import a language file to CredolD. It is important that the language file should fit the language currently selected and the name of the file unchanged. Importing a language file incorrectly, might result in errors.
- **Select encoding.** Indicates encoding type that will be used while exporting a language file. By default, the type is UTF8.

Languages that are possible in CredolD:

- **ar-KW.** Arabic.
- **az-AZ.** Azeri.

- **en-US.** English.
- **fa-IR.** Farsi.
- **fi-FI.** Finish.
- **fr-FR.** French.
- **he-IL.** Hebrew.
- **ja-JP.** Japanese.
- **lt-LT.** Lithuanian.
- **lv-LV.** Latvian.
- **nb-NO.** Norwegian.
- **nl-NL.** Dutch.
- **pl-PL.** Polish.
- **ru-RU.** Russian.
- **tr-TR.** Turkish.

## 24.7 Real time connection to Access Control Service settings

Here, communications settings that are used to connect CredoID GUI with the service are configured. Note, it is recommended to leave the default settings, even if connecting to a service located on a different system, as these settings are changed in config files.

Real time connection to Access Control Service	
ACS host	Localhost
TCP service port	8523
Http service Port	58008
Test connection (green = OK, red = Error)	

- **ACS host.** The IP address where the CredoID service is running. If the service is running on the local system, leave it as "localhost". It is recommended to not change this field, even when connecting to a service located on a different system. Connections to the service is done through config files or during GUI lost connection time [\[25.3\]](#).

Note, by changing ACS host, this also changes backup and photo folder locations.

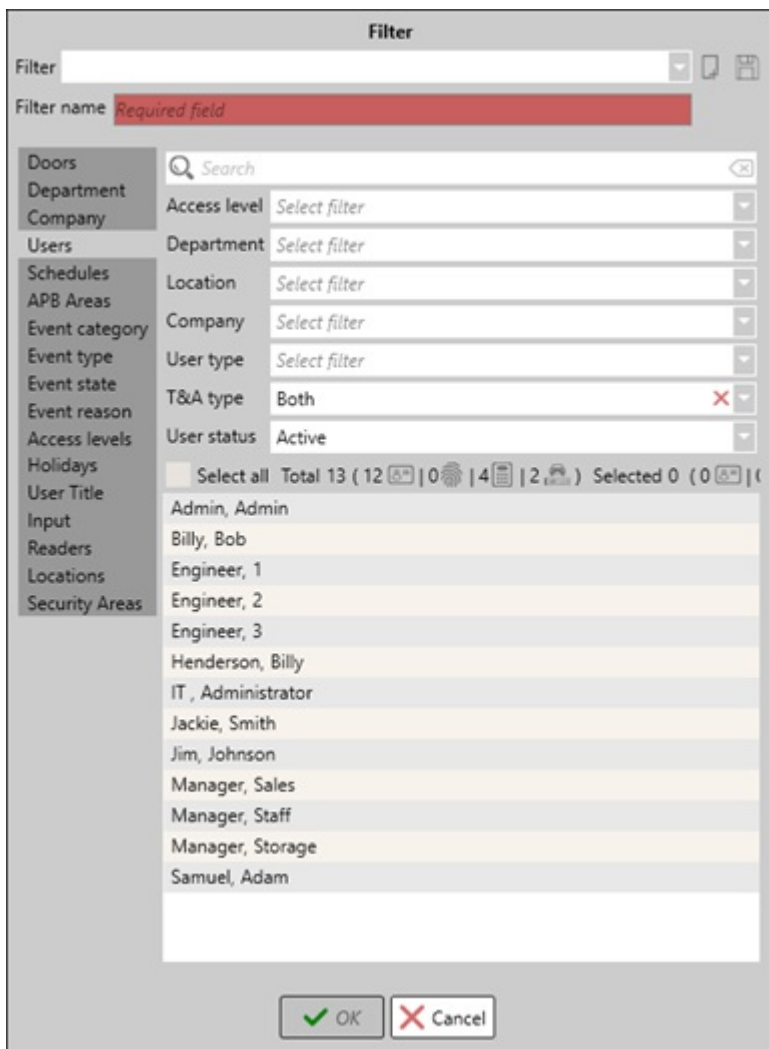
- **TCP service port.** The TCP port that is used to connect with the CredoID service. CredoID TCP service is 8523. It is not recommended to change this setting as connection to the service might be lost. The CredoID TCP service port is hard coded into config files.
- **HTTP service port.** The HTTP port that is used to connect with the CredoID web service. CredoID HTTP service is 58008. It is not recommended to change this setting as connection to the web service might be lost. The CredoID HTTP service port is hard coded into config files.
- **Test connection (button).** Tests connection with the CredoID service. If the connection is stable, the buttons background color will change to green, if not – red.

## 25. Additional information

### 25.1 Filters

Filters are used to filter out certain items from a group, such as events, alarms, or categorize what items will trigger a certain action. Depending on the setting that a filter is being created, their purpose and settings may vary. A good example where filters are used, are in Monitoring, Occupancy, Video, Reports, Users tabs.

Usually filters will contain groups from Devices (Locations), Users (Department, Company, User title), Doors (Doors, Readers), Input, Security Areas, Schedules, Holidays, APB areas, Access levels tabs, as well as event categorization. From these groups, created items or categories can be selected for the filter.



Most filter groups are self-explaining, such as Doors, Schedules or Locations, which take information from the menu tabs. Though there are several groups which take information from MS SQL database, such as event groups.

- **Event category.** Indicates the category the event belongs to.
  - **Access.** Indicates access alarms, such as granted or denied events.
  - **Alarm.** Indicates events which causes alarms.
  - **Communication.** Indicates events about communication with devices.
  - **Control.** Indicates control based events, which are made manually through GUI.
  - **Intruder.** Indicates events which are caused by intruder events, such as Force door open.
  - **Trouble.** Indicates trouble events which are received from devices, such as Battery fail, Auxiliary fail.
- **Event type.** Displays a list of all possible events that can be generated.
- **Event state.** Indicates events which are categorized as alarm events.
  - **Acknowledged.** Acknowledged alarm events.
  - **Closed automatically.** Alarm events that were closed automatically.
  - **Closed.** Alarm events that are closed.
  - **New.** Unacknowledged alarm events.
  - **None.** No alarm event categorization.
- **Event reason.** Displays all possible reasons for the event generation.

## 25.2 Schedule import file structure

At the moment, there is no simple solution to import schedules fast and efficient, as to import them correctly, each schedule block has to be defined individually. Schedule import file has to be in .xml format.

Here is an example of a schedule import file.

```

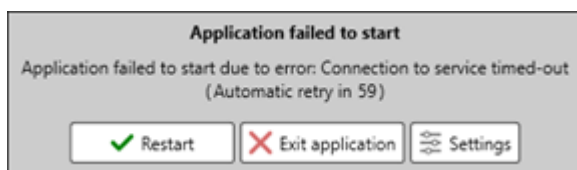
<SlidingSchedulesList xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SlidingSchedules>
    <SlidingSchedule>
      <EmployeeNumber> 123456 </EmployeeNumber> % The start of a schedule block
      <DateTime> 2017-06-14T00:00:00 </DateTime> % Employee number
      <AbsenceType> None </AbsenceType> % Date of the schedule
      % Type in the name of the absence. If no
      absence should be applied, type "None"
      <AbsenceFrom xsi:nil="true" />
      <AbsenceTo xsi:nil="true" />
      <WorkSchedule xsi:type="WorkScheduleDetails">
        <Name>Work_schedule</Name> % Note, that it is advised that the schedules
      names should not contain spaces
      <WorkScheduleDays>
        <WorkScheduleDay>
          <Intervals>
            <WorkScheduleInterval> % The schedules full time has to be written
              <Begin> 2017-06-14T07:00:00 </Begin>
              <End> 2017-06-14T15:45:00 </End>
              <Type> Work </Type>
            </WorkScheduleInterval>
            <WorkScheduleInterval>
              <Begin> 2017-06-14T11:00:00 </Begin>
              <End> 2017-06-14T11:30:00 </End>
              <Type> Break </Type>
            </WorkScheduleInterval>
          </Intervals>
        </WorkScheduleDay>
      </WorkScheduleDays>
    </WorkSchedule>
  </SlidingSchedule> % End of a schedule block
% -----
  <SlidingSchedule> % Start of another schedule block
    .
    .
    .
  </SlidingSchedule> % End of another schedule block
% -----
</SlidingSchedules>
</SlidingSchedulesList>

```

## 25.3 GUI connection to service

If there is a communication issue between Credoid GUI and service, "Application failed to start" window will be presented. This issue indicates a connection issue and presents options to try again, review or change communication settings or close the application.

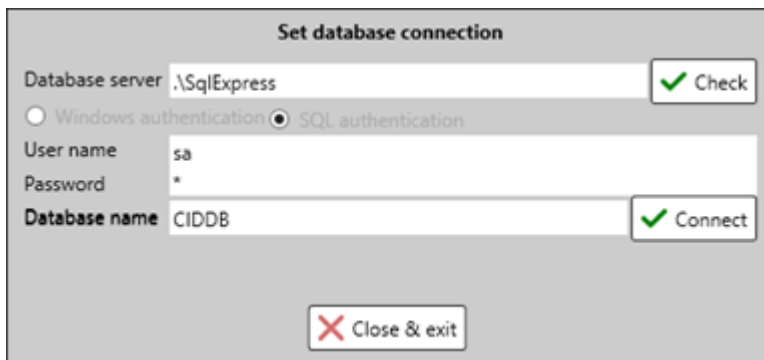
Note, to be able to change to which MS SQL database Credoid should connect, Credoid GUI should be run in Administrator.



- **Restart.** Restarts the application.
- **Exit application.** Closes the "Application failed to start" window and GUI.
- **Settings.** Opens "Connection to service" window, where Real time connection to Access Control Service settings can be changed.



- **ACS host.** The IP address where the CredolD service is running. If the service is running on the local system, leave it as "localhost". Note, by changing ACS host, this also changes backup and photo folder locations.
- **TCP service port.** The TCP port that is used to connect with the CredolD service. CredolD TCP service is 8523. It is not recommended to change this setting as connection to the service might be lost. The CredolD TCP service port is hard coded into config files.
- **Test connection (button).** Tests connection with the CredolD service. If the connection is stable, the buttons background color will change to green, if not – red.
- **Database connection (button).** Opens "Set database connection" window, where the connection to a certain MS SQL database can be changed. To open this window, CredolD GUI has to be run in Administrator.
- **Submit logs (button).** Opens Submit logs window where a .zip file or send directly to can be created which will contain log files, database backup file and additional information. As well, displays the size of the submit form and information about the computer system and CredolD [24.5].
- **Show GUI logs.** Opens the folder where GUI log files are stored. By default, GUI log files are stored in C:\ProgramData\Access Control System\GUI\Logos [24.5].



- **Database server.** The location of the MS SQL server and where database files are stored.
- **Check.** Checks connection to the MS SQL location. If connection is stable, **Database name** field and **Connect** button should be enabled. If the connection is unstable, it will present an error describing the issue.
- **Authentication type.** Select the type of authentication that is used to connect to MS SQL server. It is possible to choose **Windows authentication** or **SQL authentication**. When selecting **SQL authentication**, a user name and a password has to be presented.
- **Database name.** The name of the database.
- **Connect.** Connects to the database and upon CredolD service restart, CredolD will connect to the designated database.

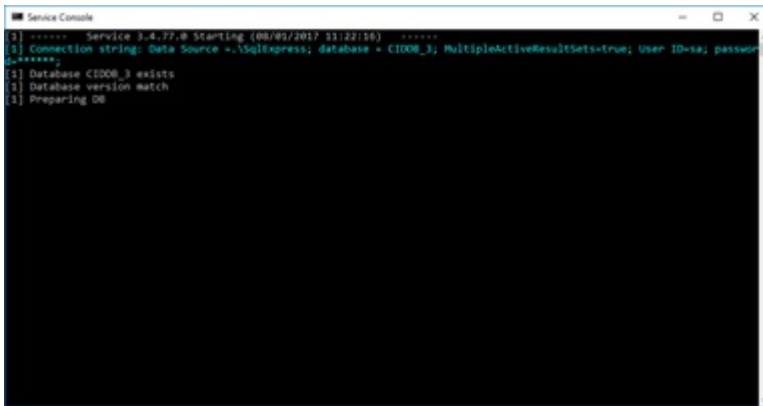
Possible causes of connection issue with CredolD service:

- CredolD service (SIDController.exe or Service Console) is not running.
- CredolD service is not running in Administrator rights.
- CredolD GUI is connecting to a location where service is not running (configuration issue).
- Issue with MS SQL database connection.
- MS SQL server packages are not installed.
- Due of other issues (System, hardware, Windows, etc.).



## 25.4 Service console

To be able to run CredolD GUI, either CredolD service (SIDController.exe) or Service Console must be running. Service console is used for advanced users, where service actions and logs are displayed. In here, services actions, errors and additional information can be reviewed. This also generates more detailed service logs.



```
Service Console
[1] ***** Service 3-4-77-0 Starting (08/02/2017 11:22:16) *****
[2] Connection string: Data Source = .\sql\express; database = C1008_3; MultipleActiveResultSets=true; User ID=sa; password
[3] *****
[4] Database C1008_3 exists
[5] Database version match
[6] Preparing DB
```

To open Service Console, launch Service Console in Administrator, located in the start menu, under CredolD folder (C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CredolD). Note, SIDController.exe should not be running, as only one service can be running at the same time.

## 25.5 Licensing

License has to be activated to be able to launch CredolD GUI and to use specific features. Depending on the licenses contents, it will activate specific features and unlock tabs for the used database.

License is directly connected with the generated hardware key, which can be seen during the CredolD installation procedure or on License information window. Hardware key structure is generated depending on the systems hardware:

- CPU.
- Disk drive (hard drive).
- Network adapter.

**Note #1.** Several hardware keys might be generated on the same system if there are more of the same hardware. This might cause for the system to select a different hardware key and thus a new license has to be made.

**Note #2.** IF hardware changes are made, different hardware keys might be generated and thus requiring for a new license. To avoid this, it is recommended to install CredolD on a system where minimum hardware changes are required.

License can be activated on a License information window, which can be opened:

- When a new database is created and CredolD GUI is launched.
- Through CredolD GUI extra options [\[3.3\]](#).
- When a license is either expired or over-extended and then launching CredolD GUI.



## License information

**License key** BA57-6DCF-5326-7149

This copy of CredolD is not licensed.

If you intend to use the software for longer than the 30-day evaluation period please contact one of our dealers to obtain a valid license.

<http://www.midpoint-security.com/>

You can contact us by email or phone

[sales@midpoint-security.com](mailto:sales@midpoint-security.com)

We appreciate your business!

Midpoint Security

- Activate using license file or activate online
- Activate online using license key

License key:

Activate Online

Load license file

Quit

There are 3 ways to activate a license:

1. **Activate Online.** When activated, it will connect to the licensing server and check if there is a valid license for the generated hardware key. If there is a valid license for it, the license information will be downloaded and license will be activated. If no valid license is found, a demo license is created for the hardware key and it is activated. This requires internet connection.
2. **Activate Online using license key.** If you have in possession of a license key from your supplier, but it is not yet activated due of a missing hardware key or have an incorrect hardware key, you can activate your license by using the license key given by the supplier. This will connect to the licensing server and add the hardware key to the created license key and active the license fully. This requires internet connection.
3. **Load license file.** Load a license file that you have received from your distributor/supplier.

**Note #1.** Only one type of license can be created for each individual hardware key.

Revision #18

Created 1 week ago by [Povilas R.](#)

Updated 2 minutes ago by [Aivaras](#)