

**ATS8600**  
**User Guide**  
**ATS8600 2018**

# Contents

<b>1</b>	<b>Initial system startup</b>	<b>6</b>
1.1	Creating the system administrator's user account .....	7
1.2	License activation .....	7
1.3	Trial version .....	9
<b>2</b>	<b>Operating procedures</b>	<b>10</b>
2.1	Filtering .....	10
2.2	Working with the Tree.....	10
2.3	Saving changes .....	12
2.4	Event History .....	12
2.4.1	Defining custom event filter .....	13
2.5	Information bar .....	14
2.6	Time format .....	15
<b>3</b>	<b>System configuration</b>	<b>16</b>
3.1	Connecting devices.....	16
3.1.1	Driver installation .....	16
3.1.2	Driver upgrade .....	16
3.1.3	Creating a device tree .....	17
3.1.3.1	Device tree auto detection.....	17
3.1.3.2	Creating a device tree manually .....	17
3.1.4	Starting communication .....	18
3.1.5	Device status information table .....	19
3.1.6	Remote device control .....	20
3.2	Visualization .....	21
3.2.1	Device visualization .....	21
3.2.2	Creating a map hierarchy .....	23
3.2.3	Assign action to button .....	23
3.2.3.1	Executing external process .....	24
<b>4</b>	<b>Operating the system</b>	<b>25</b>
4.1	Working at the dispatcher site.....	25
4.1.1	Monitor panel windows .....	25
4.1.2	Operating the Monitor panel .....	26
4.1.3	Dealing with alarms .....	26
4.2	Overview of the history of alarms .....	28

4.3	Video wall .....	29
4.3.1	Live video display .....	29
4.3.2	Playing back video footage .....	30
4.4	Persons management .....	30
4.4.1	Creating an application account .....	30
4.4.1.1	Creating a user account.....	31
4.4.1.2	Creating roles .....	31
4.4.1.3	Identifier history.....	32
4.4.2	Organizational structure creation .....	32
4.4.3	Automatic person import .....	33
4.4.3.1	Photo replication .....	33
4.4.4	Deleting an organizational unit record .....	34
4.5	Granting access to secured areas.....	35
4.5.1	System settings for identifiers .....	35
4.5.1.1	Card formats in use.....	35
4.5.1.1.1	Credential conversion patterns.....	35
4.5.1.2	Validation rules for identifiers.....	37
4.5.2	Assigning identifiers .....	37
4.5.2.1	Card learning.....	38
4.5.2.2	Merging identifiers.....	39
4.5.2.3	Card programming.....	39
4.5.3	Creating card decks .....	40
4.5.4	Definition of access permissions .....	40
4.5.4.1	Simple access permission .....	41
4.5.4.2	Advanced access permission.....	41
4.5.4.2.1	Creating an access level.....	41
4.5.4.2.2	Holidays.....	43
4.5.5	Sending identifiers to a device .....	43
4.5.5.1	Prioritized identifier sending.....	44
4.5.6	Access reports .....	44
4.6	Creating a region .....	45
4.6.1	Region report .....	45
4.6.2	Region report - variables .....	46
4.7	Creating muster region.....	46
4.8	Permission setting and status.....	47

## **5 Advanced system properties 50**

5.1	Sending emails .....	50
5.1.1	Creating email with event variables .....	50
5.2	Connecting a GSM gateway.....	51
5.3	Automatic actions .....	51

5.3.1	Automatic action creation .....	52
5.3.2	Timed automatic action creation .....	53
5.3.3	Automatic action script .....	53
5.3.3.1	Writing automatic action script.....	54
5.3.4	Running Powershell script .....	56
5.4	Visitors management.....	57
5.4.1	Creating a reception .....	57
5.4.2	Visitor evidence .....	58
5.4.3	Exit reader .....	59
5.4.4	Modifying Visitor Data .....	59
5.5	Image Monitor .....	59
5.6	Displaying camera feed automatically .....	60
5.7	Linking a camera with a device.....	61
5.8	Counting persons .....	61
5.9	Maximum number of persons in region.....	62
5.10	Region presence .....	63
5.11	Event priorities .....	64
5.12	Alarm priority .....	64
5.13	Data import and export.....	64
5.13.1	Exporting data to a .csv file .....	64
5.13.2	Importing the device tree from a csv file .....	65
5.13.3	Importing persons and identifiers from a csv file .....	65
5.13.4	Importing manually created csv file .....	66
5.14	Reports .....	68
<b>6</b>	<b>System maintenance</b>	<b>69</b>
6.1	System diagnostics .....	69
6.2	Deleting older events .....	69
6.3	Database size monitoring.....	70
6.4	Automatic database backup .....	70
6.5	Database restore .....	70
6.6	Visitor retention period and visit closing.....	71
6.7	Person retention period.....	71
<b>7</b>	<b>Modules</b>	<b>72</b>
7.1	GDPR .....	72
7.1.1	GDPR Panel .....	76
<b>8</b>	<b>Appendices</b>	<b>79</b>
8.1	Badge report data.....	79
8.2	Reception report data .....	80

8.3 Events - variables ..... 82

# 1 Initial system startup

After successful installation, start the application by selecting the respective launch command (e.g., select the application from the Start menu via Programs -> Gamanet a. s. -> ATS8600 Client).

At initial login, the language of the login screen is determined based on the regional settings of the operating system. At repeated login, the language of the login screen is the same as the language of the user who was last logged in.

In the login window, enter the appropriate information:

- **Sign in** - the user's login name for the application
- **Password** - the user's password for the application

In this login window you can also choose other properties for logging in to the application by checking the relevant boxes:

- **Remember** - check this box for the system to remember your login data, which will be filled in automatically in the login window the next time you run the application.

In case of a new installation, a predefined user is created in the system, with the user name **support** and the predefined password **support**. After logging in as the 'support' user, it is necessary to change the password immediately.

As the ATS8600 system is designed as a multi-user system with responsibilities divided among individual users, at the very beginning it is recommended to create a personal user profile for the main administrator of the system. This ensures that all other operations will be traceable in the history under the name of a specific user. It is recommended to leave the 'support' user in the system and to safely store its changed password. If the account of the main system administrator is disabled, it will be possible to revert to the 'support' user account and to change the administrator's password or to create a new system administrator.

Each user has the option to change his personal setting of ATS8600 client. Either by clicking on the name of signed in user in the top right corner or in Settings tab on selected person.

Personal settings contain these options, they are activated after restart of ATS8600 client:

- **Startup Panel** - sets panel which is shown after user signs in.
- **Enforce Fullscreen Mode** - enforces full screen view of ATS8600 client.
- **Card Numbers Format** - sets how identifier numbers are used in ATS8600 client. Identifier numbers can be used in decimal or hexadecimal format.
- **Language** - sets language of ATS8600 client for this user.
- **Time Zone** - sets timezone of ATS8600 client for this user.
- **Home Map** - sets a map, which is shown when user enters Monitor panel.

## 1.1 Creating the system administrator's user account

To quickly create one's own user account, follow these steps:

1. Use the **Navigation** control to open the Persons tree and right-click the Root node. Select **Add - Person** and select the required person type.
2. Enter the person's contact details.
3. On the **Roles** tab, check the **Administrator** role.
4. On the **Credentials** tab, add the identifier type of **Forms Authentication** and enter the user name/password. Upon entering the password, the system checks its strength based on built-in security algorithms. The password is considered strong enough when the green symbol appears after the password. Click **Change** to confirm the new password.
5. When the **User must change password at next logon** box is checked, the system will request the password to be changed when the person logs in for the first time.
6. Select the person's required personal setting on the **Settings** tab.
7. Restart the application and log in using the new login details.

## 1.2 License activation

Without the activation of a valid licence, the system can only work in the trial mode for a limited time, see Trial version. The valid license must be activated to ensure the correct and permanent operation of the system. The valid license allows the user to use the ATS8600 system legally.

To activate the license or to show the status of the existing license, click Navigation - Licenses. The window with the current license information appears.

If you own a trial version of the ATS8600 system and you do not have a license, the attributes in this window are empty.

If you already own a license, the attributes contain the current license information. If you want to connect further devices to the system or gain access to new functions, you need to update the licence.

The license is received in the form of an activation key from the supplier of your ATS8600 system upon fulfilling the licensing conditions.

The License panel contains the following information:

- **License status** - the status of the currently active license
- **Version** - the software product version for which the license is issued
- **MAC address** - the hardware identifier of the device with the activation key assigned to it
- **Devices:** - the list of devices allowed to be connected based on the license. There are limitations in terms of the numbers for each device and possibly also the license expiry date.
- **Modules** - contains the list of application modules that the user can access in the application. There may be a separate limitation for each application module in terms of the license expiry

date

Note:

See the product web page to view the ATS8600 licensing information.

Warning:

The device list contains only the devices that are included in the activated license and have their drivers installed. If you have an activated licence for a device that is not included in the list, you must install a driver for this device.



## 1.3 Trial version


Trial version is active for 2 months after first installation. This version is only for getting to know new ATS8600 version.

- During trial mode all functions and panels are enabled and functional.
- All devices and server extensions work without restriction.
- 2 weeks before license (trial or full) ending date, users will be warned with info panel, see Information bar.
- When full license ends, trial version **will not** be activated. Trial version is only for trying ATS8600.

## 2 Operating procedures

After a successful user login to the system, the main screen of the ATS8600 application is displayed. The main instrument to operate the application is the **Navigation** button, which you can use to switch between the individual sections of the application.

The personal settings of the user currently logged in can be found in the upper right corner of the application.

To the right of the personal setting there is the  button with the options to restart or exit the application or the display information about the ATS8600 program. You can also click **Reset settings** to reset user settings such as the layout of windows and restore their default values.

The application is divided into logical sections, so even complex data structures can be presented to the user in a simple manner. The basic information entered into the system is recorded in a tree structure (persons, devices, regions), other objects are represented by lists.

### Note:

If you want to create object with the name that is used as resource key and is automatically translated (e.g, automatic action with the name "General" is saved as "General settings") you need to add character "~" to the beginning of the name (e.g. "~General" will be saved as "General").

## 2.1 Filtering

A filter is a readily available search tool in all parts of the application. When the filtering condition is entered, the displayed data will be filtered and the user will only see the results meeting the condition. Also, the search string will be highlighted in colour. When you click the triangle next to the filtering magnifying glass, you can display further filtering criteria depending on where you are in the application. The Filter is ON icon indicates that filtering is enabled.

At the same time, it is possible to filter by a specific property value when you enter the name of the property in the language of the client application and the required value.

### Example:

Searching for devices with the address value of 200. Enter Address:200 in the filter

Searching for devices of type input. Enter category:input in the filter

### Warning:

If the searched property or value consists of several parts separated by a space, such a criterion must be enclosed in quotation marks (such as "IP Address":localhost).

## 2.2 Working with the Tree

The tree with its nodes is an effective element of graphic program-user communication, as it allows even complex data structures to be presented to the user in a relatively simple way. It is used to quickly browse data in the hierarchical system structure. Clicking the tree node (object) displays its details on the right side of the screen.

A node can be expanded or collapsed using the following controls:

- "+" to expand

- "-" to collapse

The following keyboard shortcuts can be used when working with a tree structure:

- expanding the selected node without subordinated nodes: NUM+
- expanding the selected node, including subordinated nodes: NUM\*
- collapsing the selected node: NUM-

If the tree window is not wide enough for all the data to fit in, the user can change the tree window width smoothly by moving its edge using the mouse.

The CTRL+X keyboard shortcut can be used to cut the currently selected object and to put it to the Clipboard. The Clipboard content can be pasted to another part of the same tree. Select the node in the tree, under which the object from the Clipboard should be pasted, and press CTRL+V. The object will be moved including its child nodes. Moving objects using keyboard shortcuts is supported in the Persons, Devices and Regions trees. The object can be pasted only under a node under which it is also possible to create the type of the object being moved using the Add function. The Clipboard is emptied after the object was successfully moved. In case of an attempt to insert the object at an unsupported location, the Clipboard will be emptied and the operation will be terminated without any change in the tree structure.

Similarly, the copy function can also be used by pressing CTRL+C and then CTRL+V with the difference that the object being copied remains in the Clipboard, so it can be inserted multiple times.

The system supports the selection of multiple objects at once. Only the objects placed at the same hierarchical level can be selected at the same time.

To change an element category (such as a ramp to access door), right-click the required object, select the **Change category** command and choose the required element type. If multiple elements have been selected at once, the category can only be changed if all selected elements belong to the same category.

Click **Archive** to archive the object including its child elements.

Archived objects in the tree are only visible if the **Show archived persons** filter is enabled. When an object is archived, the following applies to it:

- The archived object is read-only, its modification is prohibited.
- The structure of the deleted part of the tree is preserved, but changes to the structure are prohibited.
- At the next access data synchronization, archived persons are not sent to devices. At the same time, their accounts to access the ATS8600 application will be blocked.
- You can search the event history of archived objects.
- Export/import operations ignore archived objects.

In order to preserve the tree structure, it is only possible to restore an item if its parent has not been archived (its original parent element exists in the tree). Right-click the node to be restored and select the **Restore** command. The restored object is inserted at its original place in the organizational structure. You can restore the archived object including its child elements by clicking **Restore with children**.

To permanently remove the archived object from the system, right-click the object and select the **Delete** command. This operation has to be confirmed in the next dialog box. If you

permanently delete the archived object, its history is also deleted irreversibly.

## 2.3 Saving changes

The ATS8600 system is designed to immediately save changes made in the client application. This requires permanent online connection with the ATS8600 server. If communication with the server is lost, a connection lost warning appears and the operation of the application is disabled until the connection is automatically restored to prevent loss of data.

Changes made by the user are saved to the database the moment the user leaves the field in which a value was entered. Changes are only saved if the application successfully validates the entered data. Otherwise, a colored frame appears around the field with the entered value indicating invalid data. The user must correct the data or the invalid data will not be saved. This prevents the entry of invalid data to fields (for example, if the system expects a numeric value, it is not possible to enter a text string). Unless an object is saved in the database, the exclamation mark is shown next to the name of the object.

The ATS8600 system is a multi-user network application, so changes made to one client application are continuously sent to other client applications, where other users can work with the data.

If it is necessary to return to the previous change, press CTRL+Z to undo the last operation.

## 2.4 Event History

You can find the event history by clicking the **Events** tab, which is available in all standard sections of the application. The following tools are available to search the event history:

- Click the triangle next to the event finder to show the menu in which you can select the event types to be displayed. It is also possible to define custom filters, see Defining custom event filter.
- **Refresh (F5)** - It refreshes the listing of events one time.
- **Show events including events from children nodes** - If the node the events of which you are viewing has child nodes in the hierarchical structure, clicking this button also shows events from the child nodes.
- **Print** - The list of events can be printed or exported to a file by means of this function. Printing of various lists can be helpful when creating reports. You can print the printing report or save it to Excel and use the collected data in a different way.
- **Time** - By clicking the time filter it is possible to set the time from which events should be displayed. To display events within another time period, enter the required value and execute the **Refresh (F5)** command.

If an event is associated with a person, device or region, you can display a window with detailed information about the person (or the device/region) by clicking the object name in the event.

Right-click an event to copy it or turn it into an automatic action.

If an event is associated with device that has linked camera, you can right-click on this event and show recording on linked camera from the time when event occurred. More in chapter Linking a

camera with a device.

If there are no events matching the specified criteria, the message appears and it is necessary to modify the searched time frame or required event types.





Each event contains icon, which marks event type and priority. Events can have the following priorities:

-  - fire alarm
-  - alarm
-  - error
-  - warning
-  - information




### 2.4.1 Defining custom event filter

In addition to predefined event filters ATS8600 system allows to define custom event filters.




Custom filters can be defined in two places, right in Events tab:

1. Click on triangle icon in event filter.
2. Available filters are shown.
3. Click on  button.
4. List of events that can be added is shown.
5. Click on  next to the event, which you want to add. You can also add event with multiselect.
6. By clicking on "Click here to add another condition ..." list of available persons, devices, regions, event types is shown. You can add these into the filter condition.
7. Click on Next and enter filter name, then click on Finish.
8. Now you can enable this filter, after event refresh, only filtered events are shown.
9. Existing filters can be edited by clicking on  or deleted by clicking on  button. Filters can be also edited in Event Filters panel.

Second option to create event filter is in Event Filters panel:

1. Click on button **Navigation** and select **Event Filters**.
2. Click on button  and enter filter name.
3. Click on  button and select required events, event types, persons, devices or regions.
4. By clicking on "Click here to add another condition ..." you can add another condition.
5. By clicking on  you can delete the filter.

Note:


By clicking on  you can show the script of conditions for this filter. By clicking on  another variable can be added. Click on  to return to wizard editor.

To be able to create new filter, user has to have enabled privilege Create new Event Filter.

## 2.5 Information bar

While working with the application, information may appear at the bottom of the application intended to guide the user to the next operation or to indicate failures in the security system. You can click **Resolve** to continue to resolve the situation. Click **Postpone** to postpone the message by a certain time and return to it later to resolve it. Click the cross in the message to postpone it by 30 minutes (or to permanently close it if the message does not have the option to postpone).

Postponed messages are stored in the list in bottom right corner. These messages can be shown

by clicking on the button . Afterward, list of postponed messages is shown. Icon on this button corresponds to message type with highest priority.

Information bar can contain following information:

- **Start with creating new company and rest of your company structure** - appears when organizational structure does not contain company. By clicking on Resolve, company is created, after entering company name, information bar disappears.
- **Server Is Running Low On Memory** - appears when RAM usage in percentages on ATS8600 server goes over defined value set in Monitor Server Resources extension.
- **Client is updating...** - appears when a change in ATS8600 client is detected. For example after CCTV driver installation. Information bar is showing update progress.
- **Client successfully updated. Restart required.** - appears after successful update of ATS8600 client. By clicking on Resolve, you restart the ATS8600 client. If you do not restart the client, changes will not be applied.
- **Client update failed.** - appears when update of ATS8600 client fails.
- **No Database Backup for Several Days** - appears when automatic database backup fails at least 3 times. It is active when using Automatic Database Backup extension.
- **Database Size Threshold Reached** - appears when ATS8600 database size is bigger than limit set in Monitor Database Size extension.
- **License is not installed** - appears when trial version is going to expire soon or already expired. By clicking on Resolve, activation license window is open.
- **License is not activated yet.** - appears in panel Licenses if no license is activated. By clicking on Resolve, activation license window is open.
- **Invalid person configuration** - appears when ATS8600 contains person with invalid configuration. For example when check primary key option is enabled and two persons have the same internal number. By clicking Resolve you will be redirected to panel Persons, also persons with invalid configuration will be filtered.
- **To be able to add card into card deck you have to enable some card types at Installation settings panel.** - appears in panel Cards when no credential types are enabled. By clicking on Resolve, you will be redirected to panel Credential Types.
- **Enable card type which is used on installation or create your own card type.** - appears in panel Credential Types when no credential types are enabled. After enabling at least one

credential type, information bar disappears.

- **Credential synchronization needed** - appears when access rights are changed for some device, by clicking on Resolve, you execute credential synchronization to all relevant devices. If you select Postpone, changes to access rights will not be sent to devices.
- **Credentials synchronization is in progress** - appears when credential synchronization was executed, shows progress of credential synchronization.
- **Credentials Synchronization Failure** - appears when credential synchronization failed. By clicking on Resolve, credential synchronization will be executed again. If you select Postpone, credential synchronization will not be executed.
- **Active alarms in system** - appears when there is active alarm in the system. After clicking on Resolve, you will be redirected to panel Monitor and alarm window will be open.

## 2.6 Time format

Time format used in ATS8600 client is dependent on language set in ATS8600 client and Windows system settings. Time format respects region format settings of currently signed in user in Windows system and his time format settings.

Note:

For changes to take effect, you have to restart ATS8600 client.

## 3 System configuration

The ATS8600 system is intended to integrate security technologies; therefore, the connection of security technologies is the main part of system configuration. After devices are connected to the system, you can perform further operations with them: using remote device control, visualizing devices on maps depending on their geographic location or monitoring the security system status and dealing with alarms.

### 3.1 Connecting devices

Connecting a device to the ATS8600 system consists of the following consecutive steps:

1. Installing a driver for the device
2. Creating a device tree (either by adding manually or by using a wizard)
3. Starting communication and checking its proper function

#### 3.1.1 Driver installation

1. Click **Navigation** and choose **Drivers**.
2. A window with the list of installed drivers appears. New driver can be installed from a file or online storage.
3. To install a new driver from a file, click **Install driver from file** and locate the installation package.
4. To install a new driver from online storage go to **Online** tab and install required driver.

Note:

In some cases, you may also be requested to sign the license agreement for a specific driver, which can be done by clicking **I Accept**.

Warning:

After the installation of the driver the update of the client application may be required, which will be performed automatically in the background. After the update the restart of the client application may be required as indicated on the information bar. This notification must be dealt with by following the instructions given in chapter Information bar.

#### 3.1.2 Driver upgrade

1. Click **Navigation** and choose **Drivers**.
2. A window with the list of installed drivers appears. Driver update can be installed from a file or online storage.
3. To install new version of a driver from a file, click **Install driver from file** and locate the installation package.
4. To upgrade driver from online storage go to **Updates** tab and install required driver upgrade.



### 3.1.3 Creating a device tree

The following subchapters describe the possibilities for creating a device tree in the ATS8600 system using the import feature or by entering elements manually.

#### 3.1.3.1 Device tree auto detection

Some devices allow the ATS8600 system to detect elements configured on the device and to load such elements into the device tree. To add the device tree by auto detection, follow these steps:

1. Click **Navigation** and choose **Devices**.
2. Right-click the **Installation** node to choose **Add - Add using wizard** and select the name of the required wizard.
3. In the next window, enter properties required to establish communication with the device (based on an integration manual) and click **Next**.
4. After successful connection to the device, the wizard will display a list of elements to be imported. Confirm the changes that will subsequently be recorded in the database and the import is completed.

#### Tip:

Auto detection can also be used in the device tree already existing in the system to achieve the synchronized status of the tree. Right-click the bus controller of the tree and select the **Load configuration from device** command. Communication with the device will be terminated and the device import wizard appears with the connection data already populated. You can use the wizard to detect changes in the device configuration and to synchronize the ATS8600 tree with the actual device configuration. After the import is completed successfully, standard communication with the device will be automatically established.

#### 3.1.3.2 Creating a device tree manually

The manual creation of a device tree is only recommended if an existing tree is being extended or if the respective device driver does not support device tree auto detection. Otherwise, a more efficient method to create the tree is recommended, which is described in chapter Device tree auto detection.

After the driver is successfully installed, click **Navigation** and select **Devices**. The device tree opens, which is intended to manage all connected devices in the ATS8600 system.

1. Right-click the **Installation** node to choose the **Add** command and select the required device.
2. Then enter element properties based on the integration manual for the device and continue adding more elements until the tree is complete. The method of adding a device to the tree depends on the menu displayed upon right-clicking the object under which you wish to add the new element. The system contains controlled hierarchy support; that is, it verifies what type of objects can be created at the given node.

The tree structure should reflect the actual connection of devices including all connected

elements.

Warning:

Only devices that have their drivers installed in the ATS8600 system can be added to the device tree (see chapter Driver installation).

Tip:

A responsible person may forget to add some elements configured on the device to the device tree. The moment there is any activity on this missing element and the communication protocol sends the information to the ATS8600 system, a missing device event appears. You can easily add the device to the tree by right-clicking the device missing event. After the circuit is restarted, communication with this device will be established.








### 3.1.4 Starting communication

After creating the device tree, the system ATS8600 shows devices statuses in real time. To establish communication between the device and the ATS8600 system, it is necessary to start the communication circuit of the given device. Right-click the device bus controller and choose **Commands - Start**.

After the circuit has been initialized, you can notice the changing statuses of the individual elements in the device tree, which indicate the real statuses of the connected device from now on.

You can stop communication with the device by clicking the **Stop** command. If the circuit is activated and you repeatedly click the **Start command**, the circuit will restart.

While working with the device tree, you can encounter the following additional device statuses:

-  - disabled device. The respective circuit in the ATS8600 system has been disabled, which means that the device does not communicate.
-  - device configuration error. Some of the device properties in ATS8600 are incorrectly specified.
-  - circuit restart is required. It occurs after a change in the device tree (elements added/ removed or properties modified).
-  - processing a command. It is displayed after the command is issued for the circuit until the processing of the command is finished. It occurs for commands taking longer to complete, such as circuit restart or synchronization of identifiers.
-  - connecting, reconnecting. It occurs while initiating connection to the device.
-  - network trouble. It occurs when there is problem with network connection between device and ATS8600.
-  - synchronizing identifiers. Sending access information and identifiers to the device is under way.








### 3.1.5 Device status information table

In ATS8600, tree elements may have the following statuses visualised by the colour of the element. In the picture, each status is indicated by 4 colours in succession. It means, for example, that an unknown status is indicated by solid black and an alarm status is indicated by alternating red and blue.








Black	Black	Black	Black	Black - unknown/no status
Blue	Blue	Blue	Blue	Blue - normal status
Grey	Grey	Grey	Grey	Grey - bypassed
Green	Green	Green	Green	Green - locked
Green	Green	Green	Green	Green - armed
Cyan	Cyan	Cyan	Cyan	Cyan - partially armed
Lime green	Lime green	Lime green	Lime green	Lime green - activated
Red	Red	Red	Red	Red - rearmed
Red	Blue	Red	Blue	Red/Blue - alarm
Red	Orange	Red	Orange	Red/Orange - tamper
Yellow	Yellow	Yellow	Yellow	Yellow - test
Orange	Orange	Orange	Orange	Orange- failure
Orange	Orange	Orange	Orange	Orange - disconnected
Red	Red	Blue	Blue	Red/blue - alarm precondition
Violet	Violet	Violet	Violet	Violet - not ready to arm
Yellow	Yellow	Yellow	Red	Yellow/Red - alarm during test
Yellow	Yellow	Yellow	Red	Yellow/Red - alarm precondition during test
Yellow	Yellow	Yellow	Orange	Yellow/orange - tamper during test
Yellow	Yellow	Yellow	Violet	Yellow/violet - activated during test

Some device statuses in ATS8600 can also be represented, by changing device element icon.

Door statuses:

-  Door is in normal/closed state and blocked.
-  Door is unblocked. Door can be opened.
-  Door is opened.
-  Door is opened permanently.
-  Door is opened too long. After the door was normally opened, it was not closed before time interval expired.
-  Door was forcibly open. Door was opened, when not unblocked.
-  Door is locked.

Lift statuses:

-  Lift is in normal/closed state and blocked.
-  Lift is unblocked. Lift can be opened.
-  Lift is opened.
-  Lift is opened permanently.
-  Lift is opened too long. After the lift was normally opened, it was not closed before time interval expired.
-  Lift was forcibly open. Lift was opened, when not unblocked.
-  Lift is locked.

### 3.1.6 Remote device control

After communication with devices has been successfully established, device statuses can be monitored and the devices can also be controlled remotely. The ATS8600 system verifies which commands can be executed at a particular device node. Right-click the required device to select **Commands** and confirm the required command from the menu. After the command is executed, the device's feedback is visible through changing the status of the corresponding node in the device tree.

If supported by the device, some commands may be greyed out depending on the current context and status of the device to prevent an invalid command from executing repeatedly. (For example, it is not possible to arm a subsystem that has already been armed.) This behaviour can be overridden by pressing the SHIFT key, which enables all commands.

Note:

It is possible to disable individual device commands for ATS8600 users. See chapter Permission setting and status.

## 3.2 Visualization

Visualization graphically represents devices in the ATS8600 system in terms of their physical layout. The main visualization element is a map representing individual parts of the installation (such as a country, city, area, building, floor, or office ground plan). Devices visualized on maps can subsequently be controlled by dispatchers.

Click **Navigation - Visualization** and select **Designer**. The visualization edit panel opens.

There is one predefined map in the system, which can be used for visualization. When you right-click the colored background of the map, the pop-up menu appears:

- **Add AutoCAD Map** - adding map vector graphics in the AutoCad format (supported format dwfx). This feature is obsolete. To see how to export a valid file, refer to 'AutoCad Background' manual.
- **Add Image Map** - adding map raster graphics in standard formats (jpg, jpeg, png, gif).
- **Select All** - selecting all objects on the map.
- **Delete map** - removing map graphics.

In addition to the map editor, the **Designer** panel contains the following assist windows:






- **Maps** - the tree with the hierarchy of maps created in the system.
- **Devices** - contains the tree with the devices entered into the system that can be visualized.
- **Regions** - the list of trees of regions entered into the system. After adding region to the map, icon with the number of persons present in that region is shown.
- **Other** - contains other elements:
  - **Label** - adding a label to the map. A label is designed for adding a text description to objects on the map. Press Ctrl + Enter to finish text editing.
  - **Button** - adding a button to the map. You can use the button to start defined actions directly from the map. How to assign action is described in chapter Assign action to button.
  - **Counter** - adding the value of certain counter to the map. Enter name of the counter in ATS8600 into Counter name field.

Under the assist windows, there is the editor of properties of the currently highlighted object on the map. If no object is highlighted, the properties of the current map are shown.

### 3.2.1 Device visualization

The following procedure describes the example of simple device visualization:

1. In the **Designer** panel, select the **Maps** tab.
2. Right-click the map area to select the Add AutoCAD Map or Add Map Image command and choose the required graphics file representing the room in which the device is located.
3. Open the **Devices** tab and highlight the device to be visualized on the map.
4. Drag & drop the element to the required position on the map.
5. This creates the device icon on the map and you can perform more actions with it:

- You can change the object size by moving spheres in the corners of the object
-  - changing the rotation of the object
-  - displaying the visualized object with respect to other objects on the map
-  - when more objects are selected, you can align them by clicking on one of the options
-  - mirror flip icon, vertically or horizontally
-  - when three or more objects are selected you can split the space horizontally.


You can display a pop-up menu with more functions by right-clicking the object:

- **Lock** - locking the object on the map to prevent further changes to the object
- **Delete** - removing the object from the map (this command does not remove the object itself from the ATS8600 system)
- **Change shape** - changing the shape of the visualization object
- **Select All** - selecting all objects on the map
- **Unselect All** - unselecting all objects on the map
- **Navigate to** - navigate to object in tools tab on the right side of the window

The following properties can be set for the map:

- **Contrast Shapes** - specifies if visualization shapes on the map should have emphasized edges. The **Color of Contrast Shapes** property specifies the highlight colour.
- **Map Ratio** - specifies the map aspect ratio. If the Unspecified value is set, a magnifying glass will appear over the map, which you can use to move around the map.

More properties can be set for visualized objects on the map, such as:

- **Alarm Propagation** - an alarm from the device will be propagated on the map
- **Failure Propagation** - a fault from the device will be propagated on the map
- **Commands** - the assignation of a command to be executed when you left-click the visualized element shape in the **Monitor** panel. Click  to display the wizard in which you enter the command to be executed when you left-click the device symbol on the ground plan in the **Monitor** panel. You can add more commands including only those commands that can be performed on the device. When you click the symbol in the **Monitor** panel, only those commands are performed which can be performed depending on the status of the element. More in chapter Assign action to button.

6. Similarly, continue to visualize other devices. Next to the search function above the list of devices, you can turn on various filters for more efficient visualization:

- **Show only not visualized** - only shows those devices that are not visualized on any map in the system ATS8600
- **Show only not visualized on current map** - only shows those devices that are not visualized on the current map

Note:

The system remembers the shape of the visualized object. For example, if you have visualized a subsystem and changed its shape to a rectangle, all other visualized subsystems will be created

using the rectangle shape until you change it again. These settings are preserved individually for each object type.

### 3.2.2 Creating a map hierarchy

The previous chapter described the basic visualization of a device within a single map. However, we assume that the user's visualization will be divided across a higher number of maps, with individual maps representing different geographical units (such as a country, cities, areas, buildings, floors, rooms).


In this chapter, you will find how to create new maps and links between them.

1. Under the **Maps** tab, create the required hierarchy of maps and name them. Unnecessary maps may be deleted.
2. Add graphics showing the main view of the installation (such as a photo of the area) to one of the maps.
3. Add graphics representing the side view of the building to another map.
4. As the third map, use the map from the previous chapter containing visualized devices and the ground plan of the room.
5. Open the first map (Area) and drag & drop another map that you want to make a link to from the **Maps** tab. This will create a navigation button allowing the user to quickly switch maps in the **Monitor** panel.

#### Note:

One map can contain any number of added links to other maps, which makes it possible to create any hierarchy of maps according to the actual layout of the installation and devices. Also, you can insert a map link several times. The system does not allow the insertion of a map link pointing to itself.

#### Tip:

Click  to start the export of all graphical map background data from the database to a selected folder.

### 3.2.3 Assign action to button

It is possible to define action for each button. After clicking on this button defined action will be executed.

Steps describing how to assign action to button:

1. Add button to the map in panel **Designer**.
2. In properties of this button click on **\*\*\*** in **Commands** field.
3. New window opens. Click on **Add new command**.
4. Select desired action and enter additional information.
5. If you click again on **Add new command**, you can add another action.
6. If the button has more actions defined, they will be all executed.
7. These actions will execute if you click on the button in panel **Monitor**.

Note:

You can define actions the same way on other items on map.

### 3.2.3.1 Executing external process

For buttons in visualization you can also define action to run external process on the computer, where the ATS8600 client is running.

Steps to define this action are following:

1. Add button to the map in panel **Designer**, see Assign action to button.
2. As action select **Execute Process On Client**.
3. Into **Process** field enter process, which you want to execute. For example Notepad.exe, or enter the whole path to the process file.
4. Into **Process** field you can also enter web address. For example <https://www.c4portal.com>, in this case, the web page will be open in the default internet browser.
5. Into **Arguments** field you can enter additional process arguments. For example path to the file you want to open with Notepad. This field is optional.
6. Now when user clicks on this button in Monitor panel, given process will be executed.



## 4 Operating the system

### 4.1 Working at the dispatcher site

The dispatcher site is a primary part of the physical security of the installation. In the ATS8600 system, the **Monitor** panel is used for this purpose, providing dispatchers with constant surveillance over the security of the system, the real-time overview of the status of all connected devices, their remote control and the ability to deal with alarms. The **Monitor** panel shows visualized devices on maps, which you created in the **Visualization** panel.

Assuming that the device to be monitored is already connected to the system, the creation of the dispatcher site consists of the following steps:

1. Create a new person to be assigned corresponding permissions or the Dispatcher role.
2. Assign a sign-in account to this person.
3. In the person's personal settings, enter the value of the **Home Map** property, which specifies the map that the dispatcher will be shown by default when the application is started.
4. After the person (the Dispatcher) signs in, that person can start monitoring the security system and dealing with incidents based on directives in force.

The following chapters describe the individual tools that dispatchers can use while working with the **Monitor** panel.

#### 4.1.1 Monitor panel windows

The main part of the Monitor window shows the map that displays visualized devices and other objects and allows them to be controlled remotely.

On the toolbar of the panel, there is a tool for searching the maps and elements visualized on them.



Click **Print** to print an electronic fire signalization daily inspection report or the list of bypassed devices. To print an electronic fire signalization daily inspection report, there must be a fire alarm device in ATS8600.

There are several ways to navigate among maps:


- On the navigation bar, point to the **Monitor** menu. The list of available maps appears and you can select the required map to open it.
- To the left of the currently opened map, recently opened maps are listed, which you can access by clicking the respective map image.
- You can use links to other maps created during the visualization (see chapter Creating a map hierarchy). If a link to another map has been defined for a map object, upon hovering the mouse over the object a hand-shaped icon is shown to indicate the option to switch to the other map.

The **Live** window displays online events that have recently been received by the system. When


viewing the events, the photograph of the person linked to the event is displayed in this window. The photograph appears only if the event is related to a specific person who has a photograph in the personal profile.


Online events are recorded as they occur. To temporarily suspend the receiving of online events, click . You can then analyse a particular incident. After it is resolved, the receiving of events needs to be restarted by clicking . After refreshing, all events that have occurred during the suspended period will be loaded.

In the **History** window, you can search past events that occurred on one of the objects located on the current map.

If an event associated with a visualised element is selected, click  to highlight the element on the map.

The **Alarms** window is displayed if the system records an alarm that is either new or at the stage of being dealt with by operators. After all alarms are resolved, the window closes automatically. For a detailed description of alarm management, see chapter Dealing with alarms.

The **Inhibited devices** window displays inhibited devices in the system. It also shows name of the person who inhibited this device and when. When device is selected you can click on  highlight the element on the map. Right click on device you can issue commands on given device. Highlighting the element on the map is also possible by double clicking on the device.

If the window header contains the  icon, you can click the icon to unlock the window and to open it as a separate movable window. Subsequently, the window can be placed wherever on the screen or moved to a secondary screen. To lock the window in the original position, click the cross in the upper-right corner of the window.

## 4.1.2 Operating the Monitor panel

The purpose of the Monitor panel is to control devices remotely. Control is similar to using the device tree. Right-click a device and select the required command from the pop-up menu. Left-clicking will execute the user-defined command for each visualized element (see chapter Device visualization).







Upon performing the command, the device icon changes as well, directly indicating the change of the status. For example, in case of the command to open a door, the closed door icon changes to the open door icon.

Panel **Monitor** can be controlled by gestures. Touching the visualized objects shows possible actions. Alarm details can be opened by swiping from right to left with 1 finger on alarm in alarms window. You can close alarm by swiping with 2 fingers from left to right on alarm details header.

## 4.1.3 Dealing with alarms

The operators of the ATS8600 security system are typically not required to deal with all events; only those with so-called "critical events", such as alarms and errors reported by devices. An optimal workflow for dealing with such events is provided by the Alarm Management function, which is available in the **Monitor** panel. The Alarm Management combines the recording of critical events with the recording of actions required for their resolution.

The following process describes how the personnel deals with alarms:

1. A critical event occurs in the system. The **Alarms** window is automatically displayed and a new entry describing the critical event appears in the list. An audible alert also sounds to draw attention to the occurrence of the alarm.
2. Click the event in the **Alarms** window to open the alarm details. To mute the audible alert of the ATS8600 application, click . Active state of muted signalization is displayed with  icon, if this state is active, then all new alarms will be muted. Click again on this icon to resume the audible alert.
3. Click **Accept alarm** to register that you acknowledge the event and will deal with it. After the alarm is confirmed, the entry in the **Alarms** window is greyed out to show other users that the alarm is already being dealt with in the system. A note about the time of alarm acknowledgement with the name of the user responsible for it is automatically recorded. Every alarm can be acknowledged only once.
4. You can open a map showing the device from which the alarm event originated by clicking **Go to map**.
5. You can click **Print** to print the report for the alarm. Report also contains list of present persons in relevant regions.
6. If the alarm occurred on an element linked with a camera, you can click the camera icon to watch the video feed from the camera. For the procedure to link a camera with a device, see chapter Linking a camera with a device.
7. The alarm window displays the following alarm information:
  - i. **Duration:** the duration of the alarm starting from the first occurrence of the alarm event
  - ii. **Count:** the alarm count. If the same alarm event occurs at the same device while dealing with the previous alarm event, these alarm events are grouped into one alarm and the alarm count increases. If the user turned off the alarm's audible alert after the alarm occurred, another occurrence of the alarm is only signalled by a short beep instead of the standard alarm audible signal.
  - iii. **Note:** If necessary, notes can be entered for the alarm, such as the method of resolving the alarm and the result of reviewing the critical situation. To add a note, click . It may be required to enter a note before the alarm can be resolved. This can be set for each region on the **Assets** tab on the **Regions** panel by checking **Enforce Alarm Note**, see Creating a region.
  - iv. **Accepted by:** the time and the name of the person that acknowledged the alarm.
  - v. **In:** displays the region in which the alarm occurred. By clicking on  you can view assigned muster regions and number of persons in these regions. You can also see list of present persons in associated regions. You can move persons manually to muster regions by clicking on  icon next to the person. How to create muster region can be found here Creating muster region.
  - vi. **Responsible people for this alarm:** displays persons responsible for the region in which the alarm occurred. By clicking on the person name you can show telephone number for this person.
  - vii. **Persons count:** displays the number of persons present in the region in which the alarm occurred. By clicking on the person name you can show telephone number for this person.
8. To star the alarm, click  in the alarm window. The starred alarms can be seen on the

**Alarms** panel in the **Starred alarms** section (see chapter Alarm history overview).

9. By clicking on **evacuate**, event requesting evacuation is sent in the client. Event is only shown in the application, you can add additional functionality by using automatic action reacting to this event.
10. After the critical situation is resolved, click **Resolve alarm** in the alarm window. A note will be added to the alarm about the time of alarm resolution and the name of the user responsible for it and the alarm will be removed from the **Alarms** window. If it is the last alarm in the window, the **Alarms** window closes automatically. If the alarm has been resolved by another user in the meantime, the **Resolve alarm** button disappears to prevent the alarm from being resolved again.

Default priorities for each event are set in the ATS8600 system. If necessary, these priorities can be modified to match customer needs (see chapter Event priorities).

If the filter is active and a new alarm occurs, a warning appears indicating a new alarm occurred during filtering. Although new alarms are not visible, the user is notified of their occurrence.

Note:




If supported by both the device and the driver, the receipt of the alarm also mutes the alarm on the device. When the alarm is resolved, it will also be resolved on the device.



If a note is required before the resolution of the alarm, the Resolve alarm button is greyed out unless a note has been added.


Individual alarms are sorted on the Monitor panel by their priority (see chapter Alarm priority).

## 4.2 Overview of the history of alarms

Dispatchers deal with current critical situations in the Monitor panel within the Alarms window. However, it is sometimes necessary to backtrace a record of resolving a critical problem. The **Alarms** panel serves for this purpose.

1. Click **Navigation - Security - Alarms** to show the list of all alarm events recorded in the system.
2. The **Alarms Overview** section contains an overview of resolved and active alarms for the recent period. Click  to cancel all active alarms.
3. In the **Custom History** section, you can view the list of alarms being currently dealt with or the details of a selected alarm event.
4. Select the required alarm click the **\*\*\*** icon to display a detailed overview of the alarm with the following additional information:
  - i. **Notes** - notes added by the personnel while dealing with the alarm. To add more notes to the alarm, click .
  - ii. **Events** - events from objects related to the alarm are shown. Events from the occurrence of the alarm up to its resolution are shown.
  - iii. Click  to print a complex alarm report.

- iv. Click  to star the alarm.
  - v. Click  to return to the basic view of the list of alarms.
5. In the **Starred alarms** section you can view the list of starred alarms.


By clicking on  icon for given alarm you can view recording from linked camera from the time of alarm occurrence. Camera has to be linked to the node where alarm occurred. See Linking a camera with a device. The button is disabled if no camera is associated to the alarm.

## 4.3 Video wall

A video wall is a display window designed to display images from camera systems. It can be used to display live camera feed, to play recorded footage from connected recorders or to control rotary cameras.

### 4.3.1 Live video display








You can open live camera feed by clicking the **Show** command on any camera in the device tree. The ATS8600 system allows the opening of live feed from several cameras at the same time (only from cameras of the same type in the tree).

Camera feed is opened in the **CCTV Wall** panel. When more than one camera is opened, various panel display modes are available. By default, the **Full+3** mode is selected, when the recently opened camera is displayed in a large window and other possible cameras in three small windows. Click  to close the camera feed.

You can switch display mode by clicking on  button and by selecting desired layout. This icon will be changed based on current layout.

You can use the F11 key to display the **CCTV Wall** panel in full screen. You can exit the full-screen view by pressing F11 again.




The following controls may also be available depending on the connected device's options. These controls are associated with currently selected camera, which is marked by red border. To change camera which you want to control, click on the header with the name of that camera:

-  - Show PTZ camera controls. This button is disabled when non PTZ camera is selected.
-  - Activate the client's computer microphone and transmit sound to the camera. Click again to disable the transmission of sound.
-  - Adjust the volume of the sound signal from the camera.
-  - Mute and restore the playback of sound from the camera.
-  - Save the current video frame to a file.
-  - Show selected camera in fullscreen.
-  - Exit fullscreen camera view.

- **Stream name** - Use this option to select the camera stream to play, which can decrease the data rate transmitted over the network or improve the quality of the displayed video.

### 4.3.2 Playing back video footage

On the required camera, select the **Show Recorded Video** command and enter the date and time from which the playback of video footage should start. The **CCTV Wall** panel is displayed where you can control video footage playback by the following controls (their function can be limited by the communication protocol of the camera system):

- use the slider bar to move the video footage in time
- use the arrows to control playback direction, stopping or frame-by-frame playback
- use the **Playrate** menu to set playback speed
- use the slider to set the volume of the sound being played back
- click  to mute or to turn on the playback of the sound track of the footage
- click  to save the recording from the recorder to the client computer
- click  to save the current video frame to a file

The operation of the recorded video footage window is identical to the live video feed window described in chapter Live video display.

## 4.4 Persons management

The ATS8600 system allows the management of the records of people in the organizational structure, the assignment of individual identifiers to the people (cards, PINs) and the definition of permissions for these people to access security technologies as well as the ATS8600 application. The Persons tree serves for complex management of the company's organizational structure.

### 4.4.1 Creating an application account

A person that already exists in the system can be assigned a sign-in account to also become a user of the ATS8600 application. Using complex permission management, the person can be given permissions for those parts of the application that he/she needs to use based on his/her work responsibilities. The person's access to the other parts of the application can be denied to prevent possible misuse of ATS8600 security system data.


Granting access to the ATS8600 application consists of the following general steps:

1. Creating a user account
2. Assigning permissions to the user account
3. Installing the client application on the user's computer and logging in to the personal account

The following chapters contain a detailed description of how to grant access for an application user.

### 4.4.1.1 Creating a user account

To create a user account, follow these steps:


1. Highlight the person to whom you want to assign the sign-in account.
2. On the **Credentials** tab, click  to add one of the following identifier types
  - i. **Forms Authentication** - it is a regular login when the user password is stored in the ATS8600 database. Enter the required username and password. Upon entering the password, the system checks its strength based on built-in security algorithms. The password is considered strong enough when the green symbol appears after the password.
  - ii. **Windows Authentication** - this login method uses the password defined for logging in to Windows as the user password. For a local Windows account, enter the account the user will use to log in. For a domain account, also enter the name of the domain to which the user belongs.
3. Select the person's required personal setting on the **Settings** tab.

This procedure has created the application login account for the person. However, once logged in, the person will not be able to perform any operation due to missing permissions. Therefore, proceed with defining permissions based on the user's responsibilities.

### 4.4.1.2 Creating roles

Roles can be used to define the status of users according to their access rights in the ATS8600 system. A role is a set of permissions assigned to persons. Access rights for application functions are defined for each role.

After the user is granted access to the ATS8600 application, it is recommended to create a role with specified permissions to access the individual sections of the application based on the user's responsibilities. This role can then be assigned to other users with the same responsibilities. This will ensure a transparent structure of defined permissions and the possibility to easily change them at one place if it is necessary in the future.

1. Click **Navigation** and select the **Roles** item.
2. Click  to add a new role and enter its name and, optionally, its description.
3. On the **Permissions** tab, you can find all application objects for which a permission can be defined.
4. Use the dropdown menu to go through the object types that require permission for a role to be set.

For individual object types in the system you can set the following permission types (depending on the object type for which the permission is set):

- **View** - can read the object
- **Modify** - can modify object information
- **Delete** - can delete the object
- **CreateInContainer** - can create child elements under the object
- **ChangeParent** - can change the object parent
- **ModifyPermissions** - can set permissions for the object

- **ModifyPhysicalAccess** - can set an access permission for the object
  - **Modify State** - can set the object status (e.g. identifier status)
5. To set individual permissions, follow the instructions described in chapter Permission setting and status.
  6. When all required permissions are assigned, click the **Persons** tab and check the organizational structure elements to which the role should be applied.

From now on, the user will be able to access the application based on the permissions resulting from the assigned role. More than one role can be assigned to the user. In such a case, the assigned permissions are added; that is, applied positively.

Note:

In addition to persons, a role can also be set on other organizational structure elements, where the assigned role is subsequently inherited by persons under the node. In this way, one role can be assigned to an entire department (for example, a reception) and all persons placed under this department will inherit the role and its permissions.

In the ATS8600 system, permissions can be defined directly for organizational structure elements, without the need to use roles. In the long run, however, this approach is less efficient as the organisational structure elements become the owners of permission definitions. After an element with explicitly defined permissions has been removed from the organizational structure, the permission definition for the object is also deleted. Therefore, the preferred application permission definition method is to use roles and to assign them to organizational structure elements.

System ATS8600 already has some predefined roles (Administrator, HR Manager, Dispatcher, Reception, Service Technician).

Tip:

To duplicate a role created by the user, right-click the name of the role and select **Duplicate**.

Note:

A role can also be assigned to organisational structure elements in the Persons tree on the **Roles** tab by checking the required role.

### 4.4.1.3 Identifier history

Click **History** on the **Credentials** tab to show the history of the highlighted identifier, so you can browse when the identifier was used in the system.

## 4.4.2 Organizational structure creation




Organizational structure (OS) of the company is created by adding individual objects and records to the Persons tree. The initial point of the navigation tree within the OS creation is the Root node. Using the **Add** function, new objects can be created from this node.

The following procedure describes an optimal example for creating a basic organizational structure:

1. Use the **Navigation** button to select the **Persons** panel.
2. Right-click the Root node to select the **Add** command and create the new **Company** item.




Enter the company's contact details.

3. Right-click the company to create the required divisions, departments, and centres. These elements symbolize smaller organizational structure units for more transparent placement of employees according to their work responsibilities or locations.
4. Then, in the tree, right-click the object under which you want to create a new person. Select the command **Add - Person** and select the person type to be created.
5. Enter the created person's contact details. Click  to assign a photograph or click  to delete the person's existing photograph. Supported photograph formats are: \*.png, \*.jpg, \*.jpeg, \*.gif. It is also possible to capture the photograph by means of the web camera if available when you click .

The system contains controlled hierarchy support, which means it verifies what type of objects can be created at the given tree node. From the user's perspective, it is reflected in the function pop-up menu when creating a new object.

The system allows the creation of several companies in the tree. When adding persons into individual companies, one person cannot be assigned to two or more companies. However, the added person can be transferred between companies or OS elements.

The organizational structure can also be created by importing from a file (see chapter Data import and export).

The system allows the verification of persons' unique primary key to be turned on in Company. It means that persons in Company cannot have the same internal number. To turn on this function, first select Company for which you want to turn on this function and check **Check primary key**. If some persons have the same internal numbers and this function is turned on, the persons will be flagged with . The information bar also appears to indicate an invalid configuration. The conflicting internal number is also indicated by the red frame while entering the number.

### 4.4.3 Automatic person import

Similar to device tree autodetection, ATS8600 contains autoimport of persons into organizational structure.

The following procedure describes how autoimport to organizational structure can be used:

1. Click on **Navigation** button and select **Persons** panel.
2. Create new **Company**.
3. Right click on this company, select **Add - Add using wizard** - and then select desired type of autoimport.

#### 4.4.3.1 Photo replication


Photo replication represents automatic import of profile photos for persons. After running this autoimport, profile photos from defined folder will be assigned to respective persons.

Running photo replication consists of the following steps:

1. Create/Select organizational unit where you want to import photos.
2. All nodes have to have filled internal number. This number has to be unique.
3. Persons have to have internal number that matches photo names. For example if person has internal number 123, photo file has to be 123.\*

4. Save all photos into folder, this folder has to be accessible by ATS8600 client.
5. Right click on the company and select **Add - Add using wizard - ServerPhoto**.
6. Enter required information:
  - i. **Directory** - path to photos folder.
  - ii. **Search Pattern** - pattern by which photos will be searched.
  - iii. **Include Subdirectories** - include sub-directories when searching.

You can setup automatic photo synchronization:

1. After filling up the information above check **Enabled** under **AutoImport** in autoimport configuration window.
2. Set value **Sync At** to time, when this synchronization should be run.
3. **Timeout** represents timeout of photo synchronization.
4. After setting up automatic photo synchronization, icon  will be shown next to the organizational unit, where automatic photo synchronization is set.

#### 4.4.4 Deleting an organizational unit record

The system supports the two-step deletion of an organizational structure record with the aim of preventing accidental deletion of important data.

Clicking **Archive** will archive the required object (including its child elements if a part of the tree is being deleted)

The following applies to the archived objects:

- The structure of the deleted part of the tree is preserved.
- Upon next upload, persons will not be uploaded to the devices. At the same time, their accounts to access the ATS8600 application will be blocked.
- You can search the event history of archived objects.
- The modification of archived objects and their structure is not allowed.
- The export/import operations ignore the archived content.

To show the archived objects in the tree, display the assist switches by clicking the triangle next to the search box and turn on the **Show archived persons** filter. After the archived objects are shown, they can be restored by right-clicking and selecting the **Restore** command. When a part of the tree is to be restored, either a full branch of the tree (using multiple selection) or the hierarchically highest archived level can be restored. For example, it means that the system does not allow a person to be restored as long as the person's parent department remains archived. The restored elements are placed back to their original position in the hierarchy. It is also possible to restore an element with all of its child elements by selecting the **Restore with children** command.

To permanently remove objects from the system, right-click the archived object and select the **Delete** command. The object will be permanently removed from the system including all child nodes and complete history.

##### Warning:

Permanent deletion is irreversible and the data about the deleted object is lost, so this action should only be carried out with the approval of the authorized person.

## 4.5 Granting access to secured areas

Access means permission to enter a secured areas of the installation using personal identifiers such as a PIN code or smart card.


Providing the person with access to such areas includes the following steps:

1. Setting identifier types to be used in the system.
2. Registering the identifiers in the system.
3. Assigning the identifier to the person for verification at the access point.
4. Assigning access permissions to the person.
5. Sending access information to devices.

### 4.5.1 System settings for identifiers

The ATS8600 system allows the use of various types of identifiers. We recommend enabling only those types of identifiers that will actually be used in the installation. It will provide the better transparency of the security system and prevent the issuance of an unsupported identifier type to the person by mistake.

#### 4.5.1.1 Card formats in use

1. Click **Navigation** to open the **Credential Types** panel.
2. Check the card formats you plan to use for the installation. If necessary, you can create a new card type by clicking .
3. The card number can be made up of several code sequences according to the card technology specification. Set individual code lengths as necessary. Changes to the card type can only be made as long as there is no card of such type in the system.
4. Click **Navigation** to open the **Devices** panel and locate the central unit to which identifiers are sent.
5. Highlight the required central unit and click the **Credential Types** tab.
6. Check the card formats you wish to send to the device.

Note:





As different security technologies can interpret the same card in various ways, it may be necessary to create conversion formulas for specific security technologies. These formulas will convert the card number to a format that the device can accept. Formulas can be created manually or loaded from a file in **Show conversion patterns**.

##### 4.5.1.1.1 Credential conversion patterns

Conversion patterns provide conversion of credential numbers into required format, which is accepted by the device. Patterns can be created manually or imported from the file in section **Show conversion patterns** in the **Credential Types** panel.

Creating new conversion pattern consists of the following steps:

1. Select credential type for which you want to create conversion pattern.
2. Click on **Show conversion patterns**.

3. By clicking on  you create new conversion pattern.
4. Enter name and then click on  to edit this pattern.
5. In section **Source** graphical representation of the source credential format is shown. Each bit is marked by color, depending on which part of the credential code they represent.
6. In section **Target** you can set bit length for each part of the target credential format.
7. In section **Parities** you can create parity, which can be then used in target credential format. Click on **Add new parity**, then enter name and type.
8. Bits of the target credential which are used for parity calculation are set by entering Mask, mask has to be entered in decimal form. Example of parity mask:
  - We have credential code in binary: **1010 1100**. If we want to use bold bits for parity calculation, then mask in binary will be: 1001 0000, and we will enter this value into **Mask** field in decimal form: 144.
9. Parity guarantees that number of 1-bits will be even or odd, depending on the parity type:
  - **Even** - Number of 1-bits together with parity bit will be even. For example if we have credential number in binary: **1010 1100**, and bold bits are used for parity calculation. Parity bit will be 1. Because number of 1-bits is 3 and to get even number we need 1 more, so the number of 1-bits will be 4.
  - **Odd** - Works the opposite way as even parity. Number of 1-bits together with parity bit will be odd. If we use the same credential number, number of 1-bits is 3. That means, parity will be 0, because number of 1-bits is already odd.
10. Conversion patterns can also contain more parities. When calculating target credential, parities are used from the top to bottom. Order of parities can be changed by clicking on  or . For example, we have credential number in bit format 1010 0101. Parity1 is 1001 0010 and Parity2 is 1011 1011. Target pattern will be CCCC CCP**1P2**. First parity is used Parity1, result is 1010 0010, then Parity2 is used on this result. Target credential number is 1010 0111.
11. In section **Target** we see target credential format representation. For each bit you can select from the following options:
  - i. **C** - copy - given bit is copied from the source credential number.
  - ii. **N** - negate and copy - given bit is copied and negated from the source credential number.
  - iii. **1** - given bit will be always 1.
  - iv. **0** - given bit will be always 0.
  - v. **Parity** - option to select from created parities.
  - vi. **Number** - number in front of each target bit represents bit from the source credential number. For example. 5 means that 5th bit from the source credential number will be used and you can use it on any position in the target credential format, even multiple times.
12. In section **Calculator** you can test this conversion pattern. Enter number of the source credential into the left side in decimal and calculated target credential will be shown on the right side.

Note:

Hovering the mouse over the fields with credential number or parity mask will show conversion into other numeral systems(binary, octal, decimal, hexadecimal).

### 4.5.1.2 Validation rules for identifiers

The ATS8600 system allows the use of rules to validate the identifiers entered into the system. You can use this functionality to ensure that, for example, only PIN codes of a certain length meeting the security criteria are entered into the system.


1. Click **Navigation** to open the **Credential Rules** panel.
2. Check the validation rule to be applied when new identifiers are entered.

#### Warning:

If the system already contains identifiers violating the validation rule you want to enable, these conflicts must first be removed manually. The validation rule can only be enabled after all the conflicts with the rule are resolved.

### 4.5.2 Assigning identifiers

An identifier used to access secured areas is assigned as follows:

1. Click **Navigation** to open the **Persons** panel.
2. On the **Credentials** tab, click  and select the required identifier type
  - i. **Pin** - enter a unique personal code in compliance with validation criteria (see chapter Validation rules for identifiers)
  - ii. **Fingerprint** - a fingerprint can be added to the person. Fingerprints can only be added if there is a fingerprint reader device present in ATS8600 and fingerprint is enabled in **Credential Types**. After creation, **Card Number** is filled in automatically. Displayed squares represent individual fingerprints. Click one of them, select a fingerprint reader and read the fingerprint.
  - iii. **Card** - the list of cards available in the system appears. Select a required card and click **Assign** to assign the card to a person.
3. If the required card is not yet present in the system, you can create it by clicking **Create new card**. Select a card deck to which the new card is to be stored and specify the format of the new card (these settings are not shown if there is only one card deck in the system or only one card format is in use).
4. Enter required card parameters (based on card format).
5. By checking **Pin** you can add extension PIN, which will have to be used when combined authentication is set on the reader.

Click **History** to show the history of the highlighted card. For example, you can browse here to see when and at which access points the identifier was used.


Turning on the **Include assigned cards** switch next to the search box also shows cards currently assigned to persons. As each card in the system can only be assigned to one person, the selection of a card already assigned to a person will reassign the card to the new person.


You must assign a status to each card in the system, reflecting how the person is going to use it.

- **Enabled** - set this status when the identifier is assigned to a person for granting access to objects. This identifier allows the person to use his/her permissions on devices. Each usage of the enabled identifier is recorded as an event in the report together with the information about who used the identifier, and when and at which device it was used.
- **Disabled** - select this status to terminate (block) the person's permission to enter. The

identifier with this status prevents the person from accessing the device. If the person with the disabled identifier attempts to use this identifier when entering the object, the system will record this event in the list of events.

- **Lost** - set this status when the owner of the identifier reports the loss of the identifier. When attempting to use the identifier with the Lost status, the system does not allow the person to enter the object, and this activity will be recorded as an event in the report together with the information about when and on which device the use of the lost identifier was attempted.

Click  to generate a labelled card imprint report. You can do this even for card that does not have card number entered yet.

Click  to remove the card from the person. Such a card will be treated as available in the card deck by the system and can be assigned to another person.

Person can also have merged credentials, see Merging identifiers.

The person becomes a card owner when he/she is assigned the card. This way, the person is able to use specific permissions for defined devices in the building. Granting access to the building is one of such permissions. You can define the devices (e.g. entrance door) through which the person is allowed to pass with the assigned identifier as described in chapter Definition of access permissions.




#### Warning:

PIN codes will remain assigned to persons even after the person is archived. Therefore, the ATS8600 system does not allow the same PIN code to be assigned to another person as long as the original PIN holder is present in the database. The PIN code will be released when the original holder is permanently removed from the ATS8600 system. An alternative method is to cancel the PIN code for the original holder before the person is archived.

### 4.5.2.1 Card learning

To speed up the implementation of new cards to the ATS8600 system, it is possible to load cards directly from a device - card reader. It is possible to implement more cards into the system quickly by simply swiping cards through the reader.

Follow these steps:

1. In the **Persons** panel, select a person for whom you want to load a new card into the system.
2. On the **Credentials** tab, click .
3. The list of card readers appears, select the card reader to swipe the card.
4. A new line appears in the list of identifiers, indicating that the system is waiting to swipe the new card.
5. If there are more card decks in the system, you must specify the name of the deck in which the new card will be stored.
6. You can enter card name. At this moment it is possible to print card label, by clicking on .
7. Swipe the card through the card reader. The card will be loaded into the system and the card code will be filled in automatically.
8. When finished, click  again to exit the card learning mode.

Warning:

If you load a card that is already present in ATS8600 and not assigned to anybody, it will be assigned to that person. If the card has been assigned to somebody, it will be removed from the person and assigned to the new person.

Warning:

The card auto-loading functionality is supported only if the corresponding device sends the card code to the ATS8600 system.

### 4.5.2.2 Merging identifiers


Merging of identifiers provides option to merge card and PIN or fingerprint and PIN. Difference compared to extended PIN on card is that extended PIN does not have to be unique. But PIN used in merged identifier has to be unique in ATS8600 system. Persons can have more merged identifiers assigned. This functionality has to be supported by device driver.

Merge credential by following these steps:


1. In the **Persons** panel select a person for which you want to merge identifiers.
2. Assign card to person, see Assigning identifiers.
3. Add PIN to this person.
4. Hold CTRL key, click on card and then on PIN, which you want to merge.
5. Required card and PIN are selected.

6. Click on button  and identifiers will be merged. Merged card is marked with    icon.

Steps to unmerge credentials:

1. In the **Persons** panel select a person for which you want to unmerge credentials.
2. Select one identifier from the merged identifiers.
3. Click on button  and identifiers will be unmerged.

Note:

You can also unmerge merged identifiers by removing one identifier from merged identifiers by clicking . For example if you delete PIN from merged identifier, person will still have the card assigned as regular card.

Warning:

Device driver has to support this functionality, otherwise no merged identifier will be sent to the device.


### 4.5.2.3 Card programming

Some devices support programming of cards. Which means that it is possible to program card with some data. This feature has to be supported by device driver and device.

To use this feature with supported driver follow these steps, and steps in integration manual of the device:



1. Go to panel Credential Types and enable desired credential type.
2. If you have supported driver installed, Card programmer section will be visible. Select card

programmer and fill required informations according to device integration manual.

3. Then assign some card of this credential type to some person.
4. When card is in edit mode, you can click  icon, to program the card.
5. For more detailed steps follow integration manual for given device.

### 4.5.3 Creating card decks


The purpose of card decks is to keep track of cards in the system in a more transparent way. Under one deck we normally understand a group of cards managed by a certain part of the organisational structure. The system allows to divide responsibilities among users in terms of who will use which deck to assign cards to persons.


1. Click **Navigation** and open the **Cards** panel.
2. One predefined card deck is created in the system. If necessary, you can create more decks by clicking  above the list of card decks.
3. Click  on the **Cards** tab to add a new card to the deck.
4. Enter the required card parameters (based on the card format settings performed as per chapter Card formats in use).


When you check the **Pin** option, you can enter the extension PIN code for the card, which will have to be used in the case of combined authentication using the card reader. This option only becomes available when the card has been assigned to a person.

Click **History** to show the history of the highlighted card. For example, you can browse here to see when and at which access points the identifier was used.

If a higher number of cards needs to be entered in the system, we recommend using the bulk card batch generating function:

1. Click  and select the card format you want to add.
2. In the next window, enter a general textual description, which will be used automatically as the name for generated cards (with numbering).
3. Enter the initial card code and the number of cards and click **Generate {0:Count} cards**.
4. The requested number of new cards will be generated automatically by the system.

Click  to generate the card imprint report which can be printed on a printer. You can do this even for card that does not have card number entered yet.

A card deck can be deleted by clicking , but only if no cards in the card deck are assigned. The predefined card deck cannot be deleted.

### 4.5.4 Definition of access permissions

In the ATS8600 system, there are two ways to define access permissions:

- A simple permission to access a device without the need to define specific properties for a person (time restrictions, advanced settings)
- An advanced permission to access a device based on access levels where time restrictions and other specific access settings can be defined for a person



### 4.5.4.1 Simple access permission

1. To allow access in a simple way, click Navigation and select the Persons panel.
2. Click the Access tab where you can find all available devices present in the ATS8600 system.
3. Change the permission status to modify access for the currently highlighted node of the organizational structure.

For the description of how to work with permissions, refer to chapter Permission setting and status.

#### Warning:

To ensure that access information changes are also transferred to the device, it is necessary to synchronize identifiers (see chapter Sending identifiers to a device)

#### Note:

When you open the **Access** tab in the device tree, you can use the opposite approach to granting access when you allow access to the device highlighted in the tree on the left and select the organizational structure in the tree on the right.

#### Tip:

If the ATS8600 system receives an event of denied access for a person known in the ATS8600 system, you can easily grant access for this person to the access point by right-clicking this event.

### 4.5.4.2 Advanced access permission

The advanced access setting includes several steps required to allow access for a person:

1. Creating an access level.
2. Assigning access points to the access level.
3. Setting the extended properties of the access level and assigning time frames.
4. Assigning the access level to organizational structure elements.

Although the initial configuration using this method is more complex, it makes it possible to easily assign access permissions to persons at several access points at the same time.


#### 4.5.4.2.1 Creating an access level

An access level is a group of access permissions defined for a certain group of persons. The creation of an access level clarifies the definition of the organisational structure's access permissions, making it possible to efficiently find what access rights have been assigned to each person.

Access levels contain access information such as doors, subsystems, time restriction definitions, and advanced properties.


Persons with the same access permissions can be assigned the same access level. This allows a possible batch change of these persons' access to be carried out at one place and, subsequently, the persons assigned to this access level inherit the change.

To create an access level, follow these steps:


1. Click **Navigation** and choose the **Access Levels** panel.
2. Click  to create a new access level and then enter its name.

3. On the **General** tab, set the extended access level properties as necessary (the properties shown here depend on which devices are connected to the system ATS8600). Extended properties describe a more complex security framework of a particular person for devices in the ATS8600 system. In other words, they specify the settings and the rights that the person has for a device. Extended properties will be assigned to a person even if access level does not have any access point.
4. For example: the option to enter a PIN on the device is defined on the Access tab, but other specific rights for this device are defined on the Extended Properties tab.
5. Click the **Access points** tab and check the access points that persons assigned to this access level are allowed to access.
6. Click the **Persons** tab and check the organizational structure elements to which the access level will apply.

If necessary, time frames can be added to specify which days and time periods the access level is in effect. This option is only enabled, when access level has assigned access points.

1. Click the **Calendar** tab.
2. Click  to add a new time frame. Check the days for the time frame to be active and enter the start and end time of its validity.

The **HO** column represents non-working days, which are defined separately for each country (see chapter Holidays).

Several time frames can be added to the access level. To remove the time frame, click  at the end of the line for the respective time frame.

Warning:

To ensure that access information changes are also transferred to the device, it is necessary to synchronize identifiers (see chapter Sending identifiers to a device)

To remove the access level, click  above the list of access levels.

Note:

Organizational structures elements can also be assigned to an access level in the Persons tree by clicking the **Access Levels** tab and checking the required access level.

Tip:

To duplicate an access level created by the user, right-click the name of the access level and select **Duplicate**.

You can search for individual elements in access levels. For example, if you want to find all access levels with the Support person, enter "persons:Support" or just "Support" in the filter. All access levels containing the person are displayed.

Warning:

If a person is assigned to several access levels with different time frames defined for each level, the person's access will reflect the sum of all calendars from all access levels assigned to the person. For example, if Access Level 1 grants the person's access on working days from 8 a.m. to 5 p.m. and Access Level 2 grants the person's access every day of the week from 9 a.m. to 6 p.m., as a result the person will be granted access from 8 a.m. to 6 p.m. on working days and from 9





a.m. to 6 p.m. on weekends.

#### 4.5.4.2.2 Holidays

Holidays and non-working days are important for access management so they must be defined correctly. On each device supporting access management, holidays are taken into consideration according to the country set in properties of this device in the device tree. The easiest way to define holidays is to load them from a file. If such a file is not available, the system allows the editing of holiday definitions manually.

The holidays definition can be loaded from a \*.hol file, which is part of the Microsoft Outlook installation, or can be downloaded from the internet as a separate file.

To create a holiday definition, follow these steps:

1. Click **Navigation** and choose the **Holidays** panel.
2. Click  to add a new set of holidays. The set means a common group of holidays valid for a specific area; for example, a country.
3. When defining holidays, there are two ways to enter information:
  - i. adding manually: on the **General** tab, click . Enter the name and date of the holiday. To remove the holiday, click  after the date of the holiday.
  - ii. importing: on the **General** tab, click . When the import wizard appears, enter the path to the file to be imported. Then select countries for which holidays are to be imported. After successfully importing the definition from the file, all holidays of the respective country for the upcoming period will be shown in the list.

#### Warning:


Changes made in the holiday definition will take effect on the device only after the next successful synchronization of identifiers.

To delete a set of holidays, click  above the list of sets of holidays.

#### 4.5.5 Sending identifiers to a device

The identifier assigned to a person serves as a tool for the person to use the devices for which the person has a permission. The ATS8600 system is designed to detect in the background all user changes made to access permissions. If an access-related change occurs (such as adding a new person, changing an identifier or access permissions), the system will display a notification that the synchronization of persons is required within approximately one minute.

The user can confirm the synchronization to start immediately or postpone it if more access-related changes are anticipated.

The ongoing synchronization of identifiers is shown by the  status in the device tree next to the central unit currently being synced.

You can check the result of the last synchronization by highlighting the respective central unit in the device tree and selecting the **General** tab. The bottom part of the tab shows the date and status of the last synchronization of identifiers, as well as the overview of the occupied access memory of the device.

Identifiers can be sent to the device also by issuing commands manually:

- **Send Credential Changes** - only changes detected in the system are sent to the device.
- **Clear Memory and Send All Credentials** - clears device identifier memory and sends all identifiers again.
- **Send All Credentials** - send all identifiers without clearing the device identifier memory. Identifiers are sent with the same positions as in previous upload. Can be used when replacing faulty device panel. Not meant to be used in everyday operation.

#### 4.5.5.1 Prioritized identifier sending

When big number of identifiers are sent to the device, some person may need to be sent prioritized. For example if some person that is being sent to the device needs to have their access rights updated sooner and cannot wait until the sending of identifiers finishes.

Usage of prioritized identifier sending is following:

1. Start sending of identifiers into the device. (All identifiers or just changes).
2. Let's assume that person, we want to prioritize and grant access, is not in the device memory yet, and does not have access.
3. While identifiers are sending into the device, this person badges the card on required card reader.
4. At this moment person has access denied. Now this person will be prioritized and sent into the device.
5. Person badges the card again.
6. At this moment person has access granted. Even though sending of identifiers into the device can still be running.

Prioritized identifier sending works with full identifier sending and also when sending just changes. Works when adding or revoking access.

##### Warning:


Prioritized identifier sending works only with cards.

The device has to send information about the person, card or position. Prioritization works base on access events.

Prioritized sending works only for running sending of identifiers. Any changes made while these identifiers are being sent, will be send in next identifier synchronization.

#### 4.5.6 Access reports


For individual devices, the system allows the creation of a printable report based on the overview of access permissions. The generated report contains access permissions related to a currently selected device and its child nodes.

1. Click **Navigation** and choose the **Persons** or **Devices** panel.
2. On the **Access** tab, click  and select the required report type:
  - i. **Print** - print all access permissions for access points
  - ii. **Print only allowed** - print only allowed access permissions for access points

## 4.6 Creating a region

Regions can be created in the ATS8600 system. The Regions tree provides an overview of the structure of devices in the ATS8600 system in terms of their physical location in the environment. A region is an area/space that contains devices managed by the ATS8600 system. A region is virtually one installation of the ATS8600 system that disregards the number and location of the covered buildings and the number of devices included within the system.





To create a region, follow these steps:


1. Click **Navigation** and choose the **Regions** panel.
2. In the Regions tree, create the hierarchy of regions representing the areas of your installation (such as an area, buildings, floors, rooms).
3. Above the Regions tree, click  to display the device tree.
4. Locate the required device in the Device tree and drag & drop the device to respective regions. Each device can be placed in each region only once.
5. More settings can be made for each region under the Assets tab:
  - i. **Responsible Person** - you can add a person responsible for the region.
  - ii. **Deputy** - you can add a deputy person responsible for the region.
  - iii. **Intrusion Alarm Priority** - you can change the alarm priority, see Alarm priority.
  - iv. **Fire Alarm Priority** - you can change the fire alarm priority, see Alarm priority.
  - v. **Enforce Alarm Note** - check this option to require that a note is added after the alarm is resolved in this region.
  - vi. **Maps** - you can add map for the region.

### 4.6.1 Region report

Custom reports can be created for regions in ATS8600 system.

To create a report follow these steps:

1. Select desired region for which you want to create report and select tab **Assets**.
2. Select **Report** and enter name of this report into field Report.
3. For each report you can enable some options:
  - i. **Monitor**  - report can be printed in panel Monitor.
  - ii. **Alarm**  - report can be printed in panel Monitor in alarm window.
  - iii. **Fire Alarm**  - report can be printed in panel Monitor in fire alarm window.
  - iv. **Auto Print**  - report will be automatically printed after accepting alarm. It will be printed on default printer in the system. This button is enabled only when Alarm or Fire Alarm is enabled on this report.
  - v. **Shortcut** - option to select key F2-F9, after pressing this key given report is shown.

By clicking on  you can delete report. By clicking on  you can edit report.

## 4.6.2 Region report - variables

It is possible to add various variables and counters into report.

To add **Variable** follow these steps:

1. Create new report following the steps above. Click edit and after that click edit again.
2. Report editor is open. On the right side click Dictionary, right click on Variables and select **New Variable**.
3. Enter desired name of this variable and click OK.
4. Drag and Drop this variable into report and save.
5. Value of this variable can be edited in given region in tab General. After entering new value, this new value is shown in given report.

To add **Counter** follow these steps:

1. Create new report following the steps above. Click edit and after that click edit again.
2. Report editor is open. On the right side click Dictionary and drag and drop Counters (Business Objects>Common) into report.
3. In report field with 2 parts is shown. First part represents name of counter which is visible in report. Doubleclick on this part and edit the name. Confirm by clicking OK.
4. Doubleclick on second part of this field. Enter name of counter in ATS8600. Name has to be in upper case. For example `{Common.Counters.Values.TESTCOUNTER}` confirm by clicking OK.
5. If you want to have counter value editable in ATS8600 report select counter field and in Properties check Editable. Save this report.

Values in report in ATS8600 client can be edited by following these steps:

1. Open report.
2. Check **Edit Fields**. All editable items are marked.
3. Edit desired value and uncheck **Edit Fields**.
4. It is possible to edit all values that are set to Editable in report editor.

## 4.7 Creating muster region

Muster regions can be created in the ATS8600 system. These regions provide muster reports with a list of persons present in this region. Mainly in a case of emergency, when persons are moved into these muster regions, then application user can see if all persons evacuated into muster regions.


A Muster region can be created by these steps:

1. Click **Navigation** and choose the **Regions** panel.
2. In the region tree, add Muster region, in the same way as if adding standard region.
3. Each standard region can belong to a muster region based on the following rules:

- i. Each region on the same level as muster region.
  - ii. Each region with the same parent region as muster region.
  - iii. All regions belong to muster region, which is directly below root region.
  - iv. If muster region is under region, muster region does not contain this region.
4. Add reader under muster region, see Counting persons. Extension **Counting Persons In Regions** has to be enabled.

If person enters muster region, this person is automatically removed from other regions.

Persons can also be moved to muster regions manually;

1. Go to present persons in given region, see Counting persons.
2. If you want to move some person into muster region click on the  button next to the person.
3. If region belongs to multiple muster regions, a list of these muster regions is shown. Select muster region, where person should be moved.
4. Person will be moved into this muster region and removed from the original region.

A resent person report can be printed by clicking on  in Persons Present tab in given region.

Usage of muster region in alarms can be found here Alarm management.

## 4.8 Permission setting and status

The object permission can have the following basic statuses:

- **Allow** - a person has a permission for the chosen object and permission type. This permission is only related to the object on which it is set and is not transferred to its child elements. This permission was created by a direct setting, which is indicated by a dark blue icon.
- **Allow with inheritance** - a person has a permission with inheritance for the chosen object and permission type. This permission was created by a direct setting, which is indicated by a dark green icon.
- Inherited permission **Allow with inheritance** - a person has a permission for the chosen object and permission type. This permission was created by inheriting the permission from a parent, which is indicated by a pale green icon.
- **Deny** - a person does not have a permission for the chosen object and permission type. This restriction was created by a direct setting, which is indicated by a dark red icon.
- Inherited permission **Deny** - a person does not have a permission for the chosen object and permission type. This restriction was created by inheriting the restriction from a parent, which is indicated by a pale red icon.

When hovering the mouse over the corresponding permission, the details of the set permission are shown:

- **Trustee** - the set permission holder, from whom the permission is inherited to the currently highlighted object in the tree.
- **Object** - the name of the object for which permissions are monitored.

Individual objects are added into the system in a particular hierarchical structure (organizational structure). So it is also easy to recognise the object parent-child hierarchy in the graphical presentation.

To simplify permission granting, the system has a permission inheritance function. This means that when you set permissions for a parent object, these permissions are inherited by its children, which is often used in practice.

If any inherited permission is not suitable, it can be changed individually. A permission can be set at any hierarchic level.

It is also possible to use the principle of uninherited permissions when the permission/restriction is not transferred hierarchically to the children of the object on which the permission is set.

You can use the following ways to change the permission status on a selected object:

- Right-click the object to display the menu with permission statuses you can use for the selected object
- The permission status can also be changed by simply clicking the permission icon (cyclically switching among **Allow**, **Allow with inheritance**, **Deny**, **Revoke**).

If the object for which you are changing the permission also has other hierarchically subordinate objects, they may inherit the permission setting.

For **Devices** permissions, it is possible to deny the execution of commands on individual devices. To disable a command, you must first enable all commands on the device and then disable the specific command. To do it, click **•••** to display individual commands. Then set the permission status of the command to be disabled for the person to **Deny**.

The following example permissions are available for commands:

- **Arm** - can arm the object.
- **Uninhibit** - can cancel the bypassing of the object.
- **Inhibit** - can bypass the object.
- **Clear Memory and Send All Credentials** - can send all identifiers to the object.
- **Close** - can close the object.
- **Off** - can turn off the object.
- **On** - can turn on the object.
- **Disarm** - can disarm the object.
- **Open** - can open the object.
- **Open Permanently** - can permanently open the object.
- **Reset** - can reset the object.
- **Start** - can start the object.
- **Stop** - can stop the object.

You can also change permissions for PTZ commands, PTZ presets, video export, snapshot and others.

Note:

Thus, the final permissions are a result of inheriting and setting permissions. When changing



permissions (also inherited), the setting at the lowest level in the hierarchy always has the highest priority: Organizational structure -> Role -> Person. Thus, the permission setting for a person has the highest priority; that is, it overrides permission settings for the OS or a role.

# 5 Advanced system properties

## 5.1 Sending emails

The ATS8600 system allows the security system to be connected to an email server so that users can set the sending of notifications about various events in the system.

To configure the email client, follow these steps:

1. Click **Navigation** and choose the **Devices** panel.
2. Right-click the **Installation** node to select **Add - External Notification - Mail Sender**.
3. Enters parameters for the email server. For setting these parameters consult the email server administrator.
4. To start communication with the email server, right-click the bus controller and select the **Start** command.

When the connection to the email server is established, the ATS8600 system is capable of sending email messages to persons with their email addresses registered in the ATS8600 system. Email sending is available in automatic actions (see chapter Automatic actions) or directly in the Persons tree when you click **Send E-Mail**.

Every event contains various variables, which can be used. List of these can be found here Events - variables. How to use them can be found in chapter Creating email with event variables.

### 5.1.1 Creating email with event variables

Emails in ATS8600 system can be send automatically with automatic action. See Automatic actions. In the email it is possible to send variables from the event, that evoked the automatic action.

An example of creating such an email:

1. Create automatic action, see Automatic actions. As condition, for example select event **Person property changed**.
2. As action select **Send email**. Select recipient and enter subject.
3. Into Text part enter text, which you want to send.
4. In the text you can use variables from event, which invoked the automatic action. Available variables for given event can be found in chapter Events - variables.
5. For this example we find the event **Person property changed** in the table.
6. According to the table event variables Id, Name, Value, OldValue are available.
7. In the text variables can be used as **'{0:VariableName}'**, with quotation marks.
8. The resulting text can look like this for example: "Event occurred with data: **'{0:Id}' '{0:Name}' '{0:Value}' '{0:OldValue}'**".
9. When we change internal number on person Support, received email will look like this: "Event occurred with data: 'Support' 'Internal number' '123' '551'".

## 5.2 Connecting a GSM gateway

The ATS8600 system allows the connection of a GSM gateway to the security system. Users can use the GSM gateway to set notifications about various events in the system.

To configure the GSM gateway, follow these steps:

1. Click **Navigation** and choose the **Devices** panel.
2. Right-click the **Installation** node to select **Add - External Notification - SMS Gateway**.
3. Follow the device's installation manual to enter the GSM gateway's parameters.
4. To start communication with the GSM gateway, right-click the bus controller and select the **Start** command.

When the connection is established, the ATS8600 system is capable of sending SMS message to persons with mobile phone number registered in the ATS8600 system. SMS sending is available in automatic actions (see chapter Automatic actions) or directly in the Persons tree when you click **Send SMS**.

### Note:

It is recommended that no PIN code is set for the SIM card because the ATS8600 system might use all permitted attempts to enter the PIN code and the SIM card will be blocked.

### Warning:

The communication port must be specified as COM + number. (for example: COM1)

The ATS8600 system supports this functionality via GSM gateways and mobile phones represented in the operating system by assigned serial ports and capable of processing standard AT commands.

## 5.3 Automatic actions

Automatic actions allow the definition of logical relations between individual devices managed in the ATS8600 system. At the same time, they help to automatize processes.

An example of an automatic action is when a holder swipes his or her card to disarm the area that he or she has entered. The purpose of that automatic action is that the system immediately recognises the card-holder and does not require him or her to enter any disarm code.

Automatic actions also have various advanced purposes; e.g. automatic activation of air-conditioning if there are more than 10 people in the room.

Administrating automatic actions means:

1. selecting the event types to initiate automatic actions;
2. selecting the devices to monitor these events;
3. setting a person to whom a notification is to be sent or setting the execution of any command.

An automatic action consists of two main parts:




1. a set of conditions on the basis of which the automatic action is subsequently performed
  - i. these conditions can be defined by the set of events originating in the ATS8600 system
  - ii. they can be defined from the individual statuses of devices
  - iii. they can be created on the basis of the fact that a user issued a command in ATS8600
2. the form in which the automatic action is performed:
  - i. email, SMS or executing a command that can be performed by a person on the devices in ATS8600

### 5.3.1 Automatic action creation

Click **Navigation** and choose the **Automatic actions** panel. The automatic actions panel will display where the administration of automatic actions is performed. This panel consists of two main parts:

- the left part of the window displays the list of created automatic actions
- the right part of the window contains the definition of the highlighted automatic action and its history can also be searched there.

To create a new automatic action, follow these steps:

1. Click  and enter the name of the automatic action.
2. Click  to create a condition based on an event received in the ATS8600 system.
3. Click the **Click here to add another condition ...** field and in the next step choose an event to which the automatic action responds. Click the **Click here to add another condition ...** field repeatedly to add more events to the condition or restrict the condition to apply to a specific device, region or person. Unnecessary conditions can be removed by clicking .
4. Click the **Click here to add another action ...** field and choose a command to be performed when the condition is fulfilled. An entity where the command is to be performed (such as a device) also needs to be defined for the command. To do this, click the **Click here to add another entity ...** field. Select a required object from the menu.
5. If the definition of the automatic action is valid and has been successfully interpreted, the red validation frame shown while editing the condition and the action will disappear.

The following object types can be automatic action output entities:

- Devices - automatic device remote control is possible.
- Counters - the counter value can be increased or decreased based on the occurrence of certain events and its threshold values can be evaluated.
- Timers - an event in the system can start the timer and the system can notify if another specified event does not occur before the specified time elapses.
- Sending an email or SMS - a person can be notified of an event. More in chapter Sending emails. Text can contain variables from event, see Creating email with event variables.
- Running a Powershell script - an external Powershell script can be run to execute further commands.

The automatic action is now in effect and will be performed whenever the input conditions are fulfilled. If there are more entities (such as events), the input conditions are evaluated using the OR logical operator among these entities. When another entity type (such as a device) is added between the original and new entity, the AND logical operator is used.

Example:

If you define a condition responding to three events and specify two devices, the condition is fulfilled if at least one of the three events occurs and it occurs on one of the two devices.

Warning:

The email address of the person selected as an automatic action email recipient must be entered in ATS8600.


The phone number of the person selected as an automatic action SMS recipient must be entered in ATS8600.

If the automatic action needs to be temporarily suspended, on the **General** tab uncheck the **Enabled** option. You can browse the events of the highlighted automatic action on the **Events** tab.

You can use the **Calendar** tab to assign time frames to the automatic action, which defines time periods for the automatic action to apply. The principle of creating time frames is identical to the access level time frames described in chapter Creating an access level. To be able to use Holidays in time periods, in General Settings tab select Holiday Set, which should be used for given automatic action. How to create holiday set can be found here [Holidays](#).



### 5.3.2 Timed automatic action creation


The ATS8600 system allows the creation of timed automatic actions when an event-based input condition is not taken into consideration, but a fixed time is specified when the action is to be performed.

1. Click  and specify the time to run the automatic action.
2. Define the output part of the automatic action, which is identical to what is described in the previous chapter.

### 5.3.3 Automatic action script

Each automatic action can be additionally modified by directly editing its script. Editing the script can only be done by a skilled and trained person, so you should submit such a request to the supplier of your system.

1. Click .
2. The automatic action script appears and can be edited manually.
3. If necessary, you can add a new variable to the script by clicking .

The system continuously verifies script syntax and changes are saved only if script syntax is correct. If the script remains simple, you can click  to restore the wizard form of the script. If the script is too complex, this option is greyed out and further changes to the automatic action can only be made by editing the script itself.

### 5.3.3.1 Writing automatic action script

This chapter describes statements that can be used to write automatic action script.

Syntax:

```
WHEN ([ EVENT | PERSON | REGION | EVENTTYPE | DEVICE ] [ IS | == | != ]
[ name_of_event | 'guid' ])
  [[ AND | OR ]...n]
  [ AND (it.VariableName [ IS | == | != | > | >= | < | <=] "value")]
  [[ AND | OR ]...n]
ACTION action_name
{
    [action_property = "value"]
    [,...n]
}
```

Example:

```
WHEN ( EVENT IS PersonPropertyChanged )
AND ( PERSON IS '8361eb78-d08e-435f-9065-bf2aeac85816' )
AND ( it.Name == "City" )
AND ( it.OldValue == "London" )
AND ( it.Value == "Bratislava" )
OR ( EVENT IS Alarm )
ACTION SendMail
{
    Recipients = { '8361eb78-d08e-435f-9065-bf2aeac85816' },
    Subject = "Subject of email",
    Text = "Text of the email."
}
```

In this example, automatic action executes, when event Person property changed occurs and Person in the event has guid '8361eb78-d08e-435f-9065-bf2aeac85816' and property City changes from London to Bratislava. Or if Alarm event occurs. Action that will be executed is Send email to person with guid '8361eb78-d08e-435f-9065-bf2aeac85816' and given subject and text.

For example this events would trigger the action: "'Support' changed property 'City' of 'PersonPeter' from 'London' to 'Bratislava'." or "Alarm on 'Input 0'."

Guids and names can be entered by clicking \*\*\* button and selecting required item.

Description of automatic action script parts:

- **WHEN (condition\_statement)** - describes when condition, meaning what needs to occur for the automatic action to execute.
- **condition\_statement** - represent statements which have to be true for the automatic action to execute.

Conditions can contain Event, Person, Region, Device or Event Type:

- **EVENT IS name\_of\_event** - is true when occurred event matches defined event in name\_of\_event.

- **PERSON IS guid\_of\_person** - is true when occurred event contains the person defined in guid\_of\_person.
- **REGION IS guid\_of\_region** - is true when occurred event contains the region defined in guid\_of\_region.
- **EVENTTYPE IS guid\_of\_eventtype** - is true when occurred event is type of defined in guid\_of\_eventtype.
- **DEVICE IS guid\_of\_device** - is true when occurred even contains the device defined in guid\_of device.
- **INVOKE AT aa\_time** - is true when current time equals defined time in aa\_time.

Conditions can also be negative for example PERSON != guid\_of\_person.

More conditions can also be combined into one WHEN condition, using logical operators:

- **OR** - is true when one of the conditions is true.

Example: (PERSON IS guidA **OR** PERSON IS guidB) - will execute when event contains one of the persons.

- **AND** - is true when all the conditions are true.

Example: (PERSON IS guidA **AND** PERSON IS guidB) - will execute when event contains both persons.

You can combine multiple conditions:

For example:

(PERSON IS guidA **AND** EVENT IS event\_name **OR** PERSON IS guidB) - will execute when occurred even is event\_name and person in the event is guidA. Or when person in any event is guidB.

As part of the condition you can also use event variables as **it.VariableName**. Available variables for given event can be found in chapter Events - variables.

For example:

(EVENT IS PersonPropertyChanged) AND (**it.Name** == "City" AND **it.Value** == "Bratislava" AND **it.OldValue** == "London") - will execute when Person property changed event occurs, but only if changed property was city and it changed from London to Bratislava.

- **ACTION action\_name {action\_properties}**
- **action\_name** - describes action that should be executed when condition is true.
- **action\_properties** - additional properties for the action.

### 5.3.4 Running Powershell script

Automatic actions can be used to run any Powershell script, which ensures an interaction between ATS8600 and other system.

The script must be saved in the Scripts folder, which must be created in the installation folder on the ATS8600 server.

When a Powershell script is called in the Automatic actions wizard, the entire file name including the extension must be entered.

In addition to standard commands, Powershell scripts can include the following syntax of the ATS8600 system.

Parameter	Description
\$eventId	unique event type identifier
\$devices	the enumeration of all devices related to the event that initiated the given automatic action
\$persons	the enumeration of all persons related to the event that initiated the given automatic action
\$properties	the enumeration of all properties of the event

Method	Description
\$c4.CounterIncrement( "counterName", [int] STEP )	Increase the counter "counterName" by the STEP value
\$c4.CounterDecrement( "counterName", [int] STEP )	Decrease the counter "counterName" by the value STEP
\$c4.SendCommand( [GUID]commandType, [IHandle]destination, [string]parameter )	Send the "commandType" command to the "destination" device with the "parameter" parameter
\$c4.StartTimer( [string]name, [TimeSpan] after )	Start the "name" timer from the "after" value  The example of starting a timer that expires in 1 hour and 25 minutes:  \$timespan = new-timespan -hour 1 -minute 25  \$c4.StartTimer( "timer1", \$timespan )
\$c4.StopTimer( [string]name )	Stop the "name" timer
\$c4.SendSms( [IHandle] recipient, [string] text )	Send an SMS to the "recipient" recipient with the "text" content
\$c4.SendEmail( [IHandle] recipient, [string] text )	Send an e-mail message to the "recipient" recipient with the "text" content



\$c4.GetDeviceId([Guid]"someguid")	Get the "deviceId" value from the unique device identifier
------------------------------------	--

## 5.4 Visitors management

ATS8600 provides the Visitors Management functionality to also enable visitors to move around in the building. This functionality is intended to provide the complex registration of visits as well as the management of visitors.

The Visitors Management functionality must first be enabled in the ATS8600 system settings:

1. Click **Navigation** and choose **Extensions**.
2. Check **Visitors Management**.



The management of visitors is based on the following steps:

1. Creating a reception.
2. Registering a new visit.
3. Finishing the visit.

### 5.4.1 Creating a reception

Receptions are created in order to centralise the company visitor management within ATS8600, since individual receptions are not authorized to see each another's visits.

To create a reception, follow these steps:

1. Click **Navigation** and open the **Receptions** panel.
2. One predefined reception is created in the system. If necessary, you can create more receptions by clicking  above the list of receptions.
  - i. **Apis7000 File Location** - a file containing data about visitors from an ID card reader. This option is available only if Apis driver is installed.
  - ii. **Client MAC Address** - it is possible to set the default reception. Enter the MAC address of a client computer; this reception is chosen when registering visits on the computer.
  - iii. **Fingerprint Reader** - select a fingerprint reader.
  - iv. **Is PIN Required** - check to require extended PIN for card on a visitor. It will be not possible to create visitors with only card on this reception.
  - v. **Is Visitee Required** - check to request whom a visitor visited when registering a visit.
3. To delete a reception, select the reception in the list and click .

Use the Report tab to create a new report. Available variables are described here Reception report data.












Note:

Users in ATS8600 can only create a new reception if the Create new reception privilege is enabled.

## 5.4.2 Visitor evidence


Visitors are registered at the company reception. To register visitors, a receptionist records every visitor event and assigns an identifier and access level to the visitor.

To register a new visitor, follow these steps:

1. Click **Navigation** and open the **Visits** panel. If more receptions are available, select the required reception from the list.
2. Enter the visitor's name in the search bar. The names of visitors matching the search string appear in the list. If the visitor being searched does not exist yet, the visitor with the name matching the search string will be added to the list.
3. Click  before the name of the required visitor to create a new visit.
4. Enter the visitor's contact details.
  - i. Click  to assign a photograph or click  to delete the visitor's existing photograph. Supported photograph formats are: \*.png, \*.jpg, \*.jpeg, \*.gif. It is also possible to capture the photograph by means of the web camera if available when you click .
  - ii. **Credentials** - click  to read the visitor's fingerprint. Fingerprints can only be added if there is a fingerprint reader device present in ATS8600 and it is assigned to reception, otherwise this button is not visible. Click  in the card list, select a card to be assigned to the visitor, see Creating card decks. If the option Is PIN Required on reception is enabled, you have to add extended PIN to the card.
  - iii. **Visited** - click  to select the person the visitor is going to visit. This field may be mandatory depending on the reception settings.
  - iv. **Access Levels** - click  to select an access level to be assigned to the visitor from the list. This will determine where the visitor can enter. To create an access level, follow the procedure in chapter Creating an access level.
  - v. Click  to print the report.
5. If the visitor is an unwanted person, a red bar appears at the bottom and it is up to the receptionist to decide whether the visitor will be allowed entry.
6. Click  to confirm the visitor's data and register the new visitor.
7. Click  to cancel the registration of the new visitor.

Individual visits are shown in the list of visits in the left part of the panel. To view finished visits, check **Show closed visits** in the visits filter.

Each visit in the list contains the name, the visitor's company, the visitee, and the Check In and Check Out data.

To finish a visit, click  before the name of the visit to be finished. If an exit reader is set for the reception, the visit is finished automatically when the card is read on this exit card reader. After the visit is finished, the access card will become available again.

#### Tip:

It is not recommended to allow visitors to have access to private company premises, but only to public premises (passages, dayrooms etc.).

#### Note:

The created visitor is remembered in the system and his/her contact details do not need to be filled in again at his/her next visit.

The visit event history can be viewed in the Receptions panel on the Events tab of the selected reception.

Users in ATS8600 can only create a new visitor if the Create new visitors privilege is enabled.

### 5.4.3 Exit reader


Exit reader automatically closes visit that goes through this reader. You can set more exit reader in the system and they are not linked with receptions.

How to assign exit reader:

1. Click on button **Navigation** and open panel **Regions**.
2. Create region structure as needed. How to create region can be found here Region creation.
3. Add reader, which you want to use as exit reader, under region.
4. Select this reader in region tree and in **General** tab check **CheckOut Visit**.

### 5.4.4 Modifying Visitor Data

Visitor data can be modified directly in the data about each visit or in the **Visitors** panel, all visitors are registered in this panel.

To delete a visitor, select the visitor in the list of visitors and click  above the list.

To flag a visitor as an unwanted person, check **Person Unacceptable**. You can also fill the Reason field as to why the person is unwanted.

In the list of visitors, unwanted persons are indicated by .

This indication is only for information and does not deny the visitor's entry to the building. When creating a new visit, the receptionist is warned of such a visitor by the red bar and it is up to him/her to decide whether the visitor will be allowed to enter the building.


## 5.5 Image Monitor

Image Monitor provides a way for users to control persons who enter buildings, rooms etc. Every person, who goes through access point using some credential is shown in panel Image Monitor. This function provides sufficient information about the person, with verification, if the credential was used by authorized person and it was not misused. This function also provides random person check, this marked person should go through more detailed inspection.

The **Image Monitor** functionality must first be enabled in ATS8600 system settings:

1. Click on **Navigation** and select **Extensions**.
2. Check **Image Monitor**.

To use **Image Monitor** follow these steps:

1. Click on **Navigation** and open panel **Image Monitor**.
  2. Add access point (door), which you want to monitor by clicking on the button  and from the device tree select door.
- When person uses credential on monitored door, photo of a person, to whom this card belongs to is shown. Under the photo is the description, showing if the person has access granted or not, it also shows time, that the credential was used.
  - Details about this person can be shown by clicking on the photo.
  - When new person uses credential on the door, previous photo is moved to the left part of the door window. Here photos from 4 latest accesses are shown, also time and color signaling if access was granted or not and internal number. You can also click on these photos and view more details about the person.
  - At the bottom part of the window for each door, you can open this door by clicking on button **Open**.

Person can be randomly select for more detailed inspection. This person is marked with text **Access granted. Check this person** and orange color.

1. By clicking on the photo of this person you open window with inspection results form. You can enter alcohol level, alcohol tester ID, witnesses and notes.
2. You have to enter alcohol level and alcohol tester ID to be able to confirm the form.
3. If the inception passed check **Verification Result** and confirm by clicking on OK.
4. After confirming the text under photo show result. Results can be also found in events in panels **Persons, Devices a Monitor**.
5. Probability of this random check can be configured in panel **Extensions** in settings **Image Monitor**. Value **Random Check Probability** represents probability percentage. Default value is 2.

Note:

Access photos in Image Monitor are actualized only when you are in this panel. After going to other panel images are cleared.

## 5.6 Displaying camera feed automatically

In certain situations, a live video camera feed must automatically be displayed to the ATS8600 application user. This can be particularly useful when dealing with emergency situations at the dispatcher site when the immediately available view of the area can speed up an assessment of how serious the issue is.

The automatic camera feed display function can be set as follows:

1. Click **Navigation** and choose the **Extensions** panel.
2. Create a new automatic action and define the part with conditions for the action by following the procedure described in chapter **Creating and automatic action**.
3. Choose the **Show On Client Computer** command as a response, enter the name of the required camera and the name of the user for whom the camera is to be displayed.

4. If the condition is fulfilled, the live feed from the camera is automatically displayed on all client sites where the user is logged in (regardless of which part of the application the user is currently working with).

Note:

The user for whom the camera is to be displayed must have the **View** permission for this camera.

## 5.7 Linking a camera with a device

Sounding the alarm on the device has always the same result: The operational staff has to investigate and resolve the event immediately. In such cases, it is useful to logically pair signalization devices, such as detectors, with cameras that have them in their field of vision. Based on the pairing it is then possible to open the live camera feed directly from the pop-up menu of a signalization device. The video feed from the camera monitoring the element in question can be displayed immediately based on a received critical event, without the need to look for the camera that "could have seen" the element in a hurry.

Follow these steps to logically pair signalization devices and cameras:

1. In the device tree, select a device to which you want to assign associated cameras.
2. Select the **Cameras** tab and check the cameras with the field of vision covering the signalization device. The system is able to assign multiple cameras.

Based on the setting, it is possible to open the live camera feed directly from the pop-up menu of the device to which the camera was assigned.

If the signalization device registers any event in the system, right-click the event and click **Show recorded video on** to play back the video recording from associated cameras. You can view recordings like this only from cameras that are linked to this device.

In the camera settings in the device tree, you can set the **Record Playback Delay** value determining the time before the event that the playback of the recording should start. This means that when the event recording is selected, its playback will start from the set time before the event.


## 5.8 Counting persons

The ATS8600 system allows the counting of persons presents in the individual sections of the installation. The ATS8600 application's user can immediately see where a specific person is currently located or how many people there are in a specific area. The Regions tree is used for this functionality. The counting is performed on the basis of personal identifier usage when entering and leaving an area. To see the people present in the region, the entrance and departure readers must be assigned.

The Persons Present functionality must first be enabled in the ATS8600 system settings:

1. Click **Navigation** and choose **Extensions**.
2. Check the **Counting Persons In Regions** option. When you expand the details, you can enable the additional **Soft Antipassback Enabled** functionality, which records a warning in the case of repeated entry of the person to the same area.

To set the counting of persons, follow these steps:

1. Click **Navigation** and choose the **Regions** panel.
2. In the Regions tree, create the hierarchy of regions representing the areas of your installation (such as an area, buildings, floors, rooms).
3. Above the Regions tree, click  to display the device tree.
4. Find access devices in the device tree and drag & drop readers to corresponding regions depending on which reader is for entry or departure. Each device can be placed in each region only once.
5. The reader pass direction must be set for individual readers depending on whether they are used for entry to the region or departure from it. Highlight the reader in the Regions tree and on the **General** tab set the **Direction** property to the required value.


Note:

It is a software functionality that may or may not reflect the device settings for antipassback or other properties.

When the **Counting Persons In Regions** application behaviour is enabled, the list of present persons is displayed on the tab called **Persons Present** in the Persons tree and the Regions tree. The list contains the information about the location of persons belonging to the currently highlighted element of the organizational structure or about the present persons in the highlighted region.

Each person can normally be present only once in each region. The exception is the situation when a reader provides entry to several regions at the same time. The moment the person exists one of these regions, his/her presence will be automatically terminated in the other regions, too.

Enabling the **Show only persons on premises** filter in the Persons tree will only display the persons currently present in one of the regions of the ATS8600 system.

To remove a person from a region, click . This operation will also reset the person's antipassback flag on the device (if the operation is supported by the device's communication protocol) and the person can enter the region again.

## 5.9 Maximum number of persons in region

The ATS8600 system allows to set maximum number of persons limit for individual sections of the installation, regions. After reaching this limit of number of persons in region, event is created informing about reached or exceeded limit. After reaching the limit, no action is taken, and you have to create automatic action reacting to this event.

Maximum number of persons in region limit can be set by following these steps:

1. Enable counting of persons in region see Counting persons.
2. Click **Navigation** and choose the **Regions** panel.
3. Select region, where you want to set the limit.
4. In **General Settings** tab, set **Maximum Persons In Region** to value, which represents maximum number of persons in region.
5. From this moment, if number of persons reaches or exceeds the limit, event will be created.

Usage in automatic actions:

1. Create automatic action, see Automatic action.

2. As condition set Persons in region exceeded threshold
3. If you want to define region, for which this automatic action should be executed add region to "When" condition. Otherwise it will be executed for every region.
4. If automatic action should only be executed after exceeding number of persons by certain number, add Rules.txtPropertyCurrentCount into When condition, this value represents current number of persons in region.
5. Rules.txtPropertyLimit represents the value of limitu set on region. If used, this value has to be equal to limit set on region, otherwise automatic action will not be executed.



## 5.10 Region presence

The ATS8600 system provides reporting of the time spent in region for each person. It is simply a report of first entry and last exit from selected regions per day and per person.

The Regions Presence functionality must first be enabled in the ATS8600 system settings:

1. Click **Navigation** and choose **Extensions**.
2. Check the **Regions Presence** option. You also have to enable **Counting Persons In Regions**.

To set the Regions Presence functionality follow these steps:

1. Click **Navigation** and choose the **Regions** panel.
2. In the Regions tree, create the hierarchy of regions representing the areas of your installation (such as an area, buildings, floors, rooms).
3. Above the Regions tree, click  to display the device tree.
4. Find access devices in the device tree and drag & drop readers to corresponding regions depending on which reader is for entry or departure. Each device can be placed in each region only once.
5. The reader pass direction must be set for individual readers depending on whether they are used for entry to the region or departure from it. Highlight the reader in the Regions tree and on the **General** tab set the **Direction** property to the required value.
6. In region tree select the region where you want to check region presence.
7. In **Presence** tab you can see history of entries into the region based on selected time period. Default value is month.
8. When person enters into the region for the first time that day, it will be shown in this table.
9. **Check In** represents first entry into this region for given person that day.
10. When person leaves the region through the exit reader, **Check Out** is set to the time of the exit for this person.
11. **Duration** represents the time spent in the region for given person per day.
12. By clicking on  button you can print history of check ins and check outs for selected time period.

### Note:

On region in General tab set Shift Start Time and Shift End Time.

When person enters into the region for the first time Check Out is automatically set to Shift End

Time set in General.

If person does not have entry time or exit time into the region, Shift Start Time respectively Shift End Time from General tab for given region is used.

If person leaves the region more times, the last exit time is used.

This feature is simple reporting of time spent in the region, not full attendance feature.

## 5.11 Event priorities

The ATS8600 system allows users to define event priorities. Based on these priorities, the system evaluates which events are to be displayed as alarms in the **Monitor** panel.

1. Click **Navigation** and choose **Events**.
2. You can set the required priority level for each event by expanding the menu and selecting one of values **Info, Warning, Error, Alarm, Fire Alarm**. The system supports the selection of multiple events at once. In such a case, a value set for any selected event is also propagated to the other selected events. Alarm priority is shown as icon in front of the event message. See Event History.

The Alarm Management only displays events with the **Alarm** and **Fire Alarm** priority.

## 5.12 Alarm priority

In ATS8600, the alarm priority for each region can be defined. It means that alarms from one region have a higher priority than from another.

1. Click **Navigation** and choose **Regions**.
2. Create a hierarchy of regions with devices in the same way as in chapter Creating a region.
3. Select a region in the Regions tree and on the **Assets** tab set **Fire Alarm Priority** and **Intrusion Alarm Priority** to the required values.
4. The following priorities are available from highest to lowest: **High, Normal, Low, None**.

## 5.13 Data import and export

### 5.13.1 Exporting data to a .csv file

The ATS8600 system allows the export of data from the Persons, Devices and Regions trees to the csv format.

1. Open the required tree and highlight the node you want to export to a csv file.
2. Right-click to choose **External data - Export**.
3. In the wizard, enter the name of the target file to the **File** field and click **Next**.
4. After the export is successfully completed, click **Finish**.

Note:

If an element is archived, it cannot be exported. If several elements are selected, only those that



are not archived will be exported.

### 5.13.2 Importing the device tree from a csv file

The device tree can be imported from the csv file exported from ATS8600 (for example on a different server) or created through a third-party application. (If you want to import manually created csv file follow steps in chapter Importing manually created csv file.)

Such a file must be in the required format specific for the given monitoring device type. To import, follow these steps:

1. Click **Navigation** and choose **Devices**.
2. Right-click the **Installation** node to select **External data - Import**.
3. In the next window, enter the path to the import file and click **Next** to continue.
4. Confirm the changes that will subsequently be recorded in the database and the import is completed.

#### Note:

The device tree can also be imported from a file in the c4b format created in an earlier ATS8600 version. C4b file made in ATS8600 2015 with latest service pack is supported.

### 5.13.3 Importing persons and identifiers from a csv file

The ATS8600 system supports the import of the organisation structure from a csv file. During import, the user can choose the fields that need to be imported. If the import file also contains identifiers, these can be assigned to individual persons during import.

1. In the Persons tree, highlight the organizational structure node under which the data from the csv file will be imported.
2. Right-click to select **External data - Import**.
3. Enter the name of the import file to the **File** field and click **Next**.
4. The wizard will show the names of columns from the loaded file. Column names from csv file are on the left side and ATS8600 fields are on the right side.
5. Check to select the data to be imported. Use the dropdown menu to select the type of data in the respective column.
6. With this menu you can map columns from csv file to ATS8600 fields.
7. If the column name matches a type in ATS8600, the type will be selected automatically. Mandatory fields are Id and Name.
8. By deselecting the checkbox in front of the field you disable importing of this field.
9. If the data is selected correctly, you can click **Next**.
10. After you click **Next**, the file will be analyzed. The wizard will display a summary of changes to be made in the application.
11. Click **Next** to confirm the changes. After the import is successfully completed, click **Finish**.

When persons are imported, the import file must contain a column with the Name heading and for each person there must be a value entered in this column, which the ATS8600 system will map into the **Name** field. There also has to be Id field with unique number or string. More about csv file format can be found in chapter Importing manually created csv file.

#### Note:

When importing csv file that was exported from ATS8600 2018, all fields will be mapped automatically.

### 5.13.4 Importing manually created csv file

The ATS8600 system supports the import of the organization structure also from csv file that was created manually.

When creating your own csv file, follow these rules:

- File has to have 2 mandatory columns Id and Name.
- Id has to be unique number or string in the whole imported set.
- When importing file, first column is marked as Primary Key by default.
- Values in column marked as Primary Key have to be unique and not duplicated.
- For hierarchy to work, file has to contain column Parent, which contains values from Primary Key column.
- Items without category will be imported as person.
- Column names are automatically mapped even in other languages.
- File has to be saved as csv (comma delimited).

Simple csv file with persons without hierarchy;

1. Create columns Id and Name, where Name is Surname of Person.
2. Into Id column enter unique Id number/string.
3. Into Name column enter name of the organization structure.
4. Save this file as \*.csv and close the program where you created this file.
5. In ATS8600 client import this csv file.
6. After clicking **Next**, import configuration is shown.
7. Columns from the file are on the left side and ATS8600 fields are on the right side.
8. Fields Id and Name are mapped automatically.
9. If some field is not mapped, use the dropdown menu to assign ATS8600 field to file column. Checkbox is checked automatically.
10. If you do not want to import some field, uncheck its row.
11. You can change the Primary Key by clicking on the key icon and then clicking again on the field where you want to put it.
12. After clicking **Finish** items are imported as Persons.

CSV file example:

Id	Name
1234	PersonA
65345	PersonB

Creation of csv file with hierarchy and object type. This example describes steps for creation of company under Root element with person under this company.

1. Create column Id, Name, Parent, Category.

2. First we create company. Into column Id enter unique ID number/string. For simplicity we will refer to it as Id1.
3. Column Parent leave empty.
4. Into column Name enter name of the organisation structure.
5. Into column Category enter Company.
6. Next will be person in this company. Create new row with unique Id. For simplicity we will refer to it as Id2.
7. Into column Parent enter Id of parent element. In our case Id1.
8. Enter surname into Name column and into Category column enter Person.
9. Save as \*.csv and continue the same way as in previous example.

Example of this csv file:

Id	Parent	Name	Category
2453		Company1	Company
8543	2453	PersonA	Person

Column Category can have the following values:

- Company - company
- Division - division
- Center - center
- Department - department
- ExternalEmployee - external employee
- Person - person
- ManagerEmployee - manager

To import personal PIN codes, the Pins column must be present in the import file. When the Pin value is specified, it ensures that the personal PIN code is assigned to the person. One person can have more PIN codes. Enter these PIN codes into Pins column delimited by "|".

If you want to assign access level to imported person add column AccessLevels and enter name of the existing access level. Access level has to exist in ATS8600.






If you want to assign role to imported person add column Roles and enter name of the role in English if it is default role in ATS8600, list of default roles can be found here Role creation. If you want to assign role that you created manually, enter the same name that you entered in ATS8600. This role has to exist in ATS8600.

When cards are imported, there must be the Card\_CardCode column in the import file. When the Card\_CardCode value is specified, it ensures that the card with this code is assigned to the person. If the Card\_CardCode value is specified for the person, it can also specify the Card\_Name value, which is mapped into the card name. If several card formats or card decks are allowed in the system, during import you can select in which card deck the imported card should be created and what format it will have. The Card\_CardCode value in the file must comply with the format set for the import card type (see chapter Card formats in use). If the file contains more card formats, these have to be mentioned in Card\_CardType column, value has to be guid of card type.

Example of csv file of a person with card:

Id	Name	Card_CardCode	Card_Name
3456	PersonA	12398766	Card1

## 5.14 Reports

You can view report by clicking on button , afterward report preview is shown. By clicking on button  again report can be printed. With button  **Export** you can export this report into required file format. (xps, pdf, rtf, txt, png, html, PowerPoint, Excel, Word 2007). By clicking on  you can edit this report and clicking on  will delete this report. How to use report editor can be found on the following addresses Report Editor documentation, Report Editor videos.

ATS8600 contains following reports:

- **Events** - event list.
- **Roles** - list with assigned roles to selected person.
- **Badge** - visualization of selected card. When editing you can use following data, see Badge report data.
- **Access** in persons - list of device nodes, where selected person has access. You can view all device nodes or just nodes with allowed access.
- **Access** in devices - list of persons, who have allowed access to selected device node in device tree. You can view all persons or just persons with allowed access.
- **Persons** - list of persons, who have assigned selected access level.
- **Alarms** - alarm list.
- **Alarm details** - alarm details.
- **Persons** - list of persons, who have assigned selected role.
- **Inhibited devices** - list of inhibited devices.
- **Electronic fire signalization daily inspection report** - report is visible only when fire alarm device exists.



## 6 System maintenance

### 6.1 System diagnostics

The core of the ATS8600 system is the **ATS8600 Application Server** service, which is installed on the ATS8600 server and runs permanently. This service is responsible for communication between the server and client stations and devices.

Click **Navigation - Diagnostic** to open a panel with diagnostic information about the ATS8600 system:

- **Client logs** - log files for the client application running on your computer.
- **Server logs** - log files for the server application running on the ATS8600 server.
- **Reports** - statistical data about the installation and the number of registered objects.

Log files serve the purpose of troubleshooting application issues, the cause of which would otherwise require a time-consuming diagnostic process. Under normal operation of the security system, Trace logs can be disabled, in which case only unexpected exceptions and application errors are logged. If the further diagnosis of the system is necessary, Trace logging can be enabled by clicking . It is extended logging, which requires more disk space. After the issue analysis is completed, it is recommended to disable Trace logging by clicking .

In some cases, it is useful to clear existing logs by clicking **Delete all logs** before the simulation of a recurrent error. Log files can be downloaded to a file on the local computer by clicking **Download all logs**.

### 6.2 Deleting older events

The ATS8600 system is designed to keep all information created in the security information system for an unlimited time. It may sometimes be necessary for the information to be stored only for a specified time, with older information being regularly deleted from the system.

The event deletion functionality is provided by the **Clean audit logs** application module, which you can set as follows:

1. Click **Navigation** and choose the **Extensions** panel.
2. Check the **Clean audit logs** item to enable the deletion of older events.
3. Click **Navigation** again and choose the **Events** panel.
4. You can individually set a retention period for each event in the system. After its expiry, events older than the defined period will be deleted automatically. This process is irreversible and results in the loss of data, so this functionality should only be used after careful analysis and approval by authorized persons.
5. The system has predefined event retention periods (**Retention period**) set as follows:
  - i. **Forever** - the event is retained indefinitely
  - ii. **365 days** - 365 days

- iii. **180 days** - 180 days
- iv. **30 days** - 30 days
- v. **Never** - the event is not recorded in the database at all; the system only works with it while online. It means that it is recorded among online events in the **Monitor** panel and used by other application modules, such as Automatic actions.

The system supports the selection of multiple events at once. In such a case, a value set for any selected event is also propagated to the other selected events.

## 6.3 Database size monitoring

The ATS8600 system allows the monitoring of database size and it can notify the user if the specified size is exceeded so that appropriate changes to the system can be made to ensure the trouble-free operation of the ATS8600 security system.

1. Click **Navigation** and choose the **Extensions** panel.
2. Check the **Monitor Database Size** application behaviour. You can then expand the advanced settings and enter the database size value in GB. The predefined value is 8 GB.
3. Upon exceeding this value, the system will display the system warning, to which an authorized user of the ATS8600 application can respond.

## 6.4 Automatic database backup

The ATS8600 system allows automatic database backup in set time. This function can be enabled by following these steps:

1. Click on button **Navigation** and select panel **Extensions**.
2. Check the **Automatic Database Backup** application behaviour. In extended settings of this extension you can set time and destination of this database backup.

- **Backup Time** - time when backup should be executed.
- **Directory** - directory where the backup file will be saved. ATS8600 client has to have access to this directory.

## 6.5 Database restore

**Database Restore** application can be used to restore database. This application is installed with ATS8600 installation. Application can be found in Start > Gamanet a. s. > Database Restore.

Database restore process:

1. Run Database Restore application.
2. Select file with database backup \*.bak and click Next.
3. Confirm steps and click Next.
4. After finishing you will be informed if the database restore was successful.

## 6.6 Visitor retention period and visit closing

It is possible to automatically remove visitors, that are older than given time period and automatically close visits. You can enable this function by following these steps:

1. Click on button **Navigation** and select panel **Extensions**.
2. Expand extended settings of **Visitors Management** extension. Here you can set following values:

- **Visitor Retention** - Permanently delete visitors that are inactive for longer than defined time. Default value is 90 days.
- **Automatic CheckOut** - Automatically ends and closes visit. You can select from the following options:
  - i. **Disabled** - Automatic visit closing is disabled.
  - ii. **Retention** - Each visit will be automatically closed after it is active defined time, maximum delay is 1 minute. Default value is 12 hours and can be set in the field **Automatic CheckOut After**.
  - iii. **Timed** - All visits will be automatically closed at defined time. Default value is midnight and can be set in the field **Automatic CheckOut At**.

## 6.7 Person retention period

It is possible to automatically remove archived persons, that are older than given time period. You can enable this function by following these steps:

1. Click on button **Navigation** and select panel **Extensions**.
  2. Check the **Person Retention Period** application behaviour. In extended settings of this extension you can set time period after which archived persons are permanently deleted.
- **Person Retention Period** - Permanently delete archived persons that are archived for longer than defined time. Default value is 365 days.

# 7 Modules

## 7.1 GDPR

The ATS8600 provides interface for an effective implementation of data protection principles and the adoption of necessary safeguards into processing to comply with the GDPR requirements and protect the rights of individuals concerned. It is an effective tool for implementing the GDPR into the client environment, with an emphasis on the duty of anyone who processes personal data as a controller or a processor to implement appropriate security measures, taking into consideration the conditions under which personal data are processed, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The key element is the management of natural persons' access that complies with the GDPR requirement for a data protection by default (ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons) and also the flexibility of access setups and control to allow for the client to adopt data protection by design compliant with the GDPR requirements.

By regulating the navigation of persons in a defined space, it provides protection against any security, integrity and availability breaches, while allowing for evaluation and assessment of the effectiveness of security measures in place within the client's environment. The ATS8600 complies with strict GDPR requirements and provides the necessary mechanisms for a successful GDPR implementation.

Baseline GDPR requirements for measures:

- The ability to ensure the ongoing confidentiality, integrity, availability of personal data  
It enables the system to control both the access and movements of persons connected to the company (employees) as well as of visitors navigating in a defined space.  
It allows for a clear authentication of persons upon entering a protected environment, for instance by using biometric data administration.
- Regular testing, evaluation, assessment processes of the effectiveness of measures to ensure security  
An analysis and evaluation of recorded data, its comparison, evaluation aimed at assessing the appropriateness of proposed measures.
- Adoption of measures based on risks that are presented by personal data processing as a result of unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the data.  
The system's flexibility allows for designing individual specific measures (such as the introduction of access to an environment using biometric authentication, notification of the system activities, definition of access measures for employees based on the principle 'I only know what I need to know', registration of visitors and regulation of their movement, database encryption, etc.)
- Reporting security incidents that constitute a violation of personal data protection within 72 hours from their identification to the Office for Personal Data Protection and adopting measures to prevent them



Notifications of any system activities together with an analysis of data related to the control of movement of persons are to enable to identify and assess faster whether the recorded security incident was a violation of personal data protection (the reporting duty applies also to non-cyber security incidents that are primarily related to a human factor failure while being compliant with the security measures in place).

## Data minimization

Surname field is the only mandatory field to enter when creating the person in ATS8600. The other fields are optional. In case of strict regulation at the customer, we recommend to fill in some unique person ID instead of real surname.

## Right to erasure

How can I easily remove all data from a person that wants to be forgotten?

ATS8600 stores all data in a central MS SQL database. There are typically three types of data stored about persons:

1. Contact data (Name, Address, ID numbers, Photo, etc.)
2. Credentials (PIN codes, passwords, accounts, proximity cards, biometric credentials)
3. Events
  - Access events of the person in the building
  - Application events related to the person in ATS8600 environment

**To delete contact data** from the application, first it is necessary to archive the person in the Persons tree. If the person is in an archived state, his information is accessible as read-only and he can be restored later. By deleting the archived person permanently, the person's data, including all contact information, are irreversibly removed from the C4 database.

### Deleting credentials:

- Non-transferable credentials (PIN, biometrics, account/password) can be separately deleted in the Credentials panel of Persons tree if the person is still active (not archived). Once the person is permanently deleted, all his previous non-transferable credentials are automatically deleted too.
- Transferable credentials (Proximity cards) can be unassigned from the person in the Credentials panel of the Persons tree if the person is still active (not archived). Once the person is permanently deleted, all his previous transferable credentials are automatically unassigned and can be assigned to other persons again.

**To delete event history**, go to the Events panel and set up the required retention interval for the events which might be related to the person. ATS8600 allows the customization of event retention for each event, individually based on the needs of the customer.

A core feature of the ATS8600 application is credential sending to the connected devices (mainly intrusion and access panels). During the credential sending, some personal information might also be transmitted to the device, depending on the technical possibilities of the device's memory. When deleting a person from ATS8600, it is necessary to consider that the previously sent personal data might partially remain in the device's memory and it might be required to delete them manually using some additional software for device configuration.

The ATS8600 software generates application logs for diagnostic purposes. The logs might contain personal information if they were entered or processed when the logging was enabled. **To**

**remove logs**, go to the Diagnostics panel in ATS8600 client and click **Delete all logs**. It is necessary to perform this operation on all ATS8600 workstations where personal data were processed in the past (Client diagnostic logs are stored on individual workstations locally).

In the ATS8600 client application installation folder, the last used password might be stored if “Remember” on the login screen is checked. In the same folder, the application also caches the photographs of persons for optimal performance. The client application installation folder is located in the operation system’s logged in user folder. To remove all personal data from the client application installation folder, please uninstall the ATS8600 client application on all workstations where the personal data was processed in the past.

ATS8600 application allows interconnection with external information systems via the public API. The API allows the processing and transfer of personal information into an external database for further processing. When deleting personal data from ATS8600 it is necessary to consider the deletion of the previously transferred data based on the technical possibilities of the external system.

## **Right of access by the data subject**

How can I provide an overview to a user of what information we have stored with his private data (contact details, logs, pictures, etc.)?

**To find the personal data of the subject**, go to the ATS8600 Persons tree and using the filter, find the corresponding person. By clicking on the person name in the tree, you can see their contact information on the right side of the application.

**To find the events related to the subject**, keep the previous selection from above and go to the Events tab. Click the calendar icon, select the required time interval and then click the Refresh button to show the events. By clicking the Print button, you can export the report into the selected formats.

## **Verification**

How can I confirm that a person is who he says he is (e.g. authentication)?

The person has to identify himself using the credential or combination of credentials which are stored in the ATS8600 application, subsequently the operator of the ATS8600 client is able to verify them.

## **Access to personal data**

How can I create a report providing details who has access where?

By opening the Persons tree – Permissions tab – Persons submenu you can see the overview of permission settings related to persons. Particular column represents the level of permission.

## **Secure communication**

What functionality is present to assure that private data cannot be retrieved or manipulated? With this I mean not only the fact that we have permissions, but beyond that? Like access to the DB, data stored in the DB, encryption used between components (like between device and driver, driver and application, application and SQL, application and client)?

The ATS8600 client application can only be accessed using an account/password. There is a

security entropy applied for the password to ensure that the password is unpredictable. ATS8600 application users access the data entities in ATS8600 based on their assigned permission levels.

SQL database access and file access on the disk has to be properly configured in the permissions of operation system/Database instance user's settings, to allow access for only the responsible persons.

### **Security between device and driver**

Depends especially on the technical possibilities of the connected device and its communication protocol. Please refer to the integration manual of the corresponding device at [www.c4portal.com](http://www.c4portal.com) to find out, whether Encrypted communication is listed as supported. If encrypted communication is an optional setting, ensure that it is also enabled in C4 Device tree.

If the secure communication is not available for the device, it is recommended to achieve secured connection on the network level (VPN, VLAN, etc.)

### **Security between driver and application server**

Ensured by Named Pipes technology used for this communication.

### **Security between application server and SQL database**

Ensured by ADO.NET technology used for this communication.

### **Security between client and application server**

Communication between ATS8600 client and application server is always encrypted (HTTPS).

## 7.1.1 GDPR Panel

**GDPR** settings and reports can be found in **GDPR** panel.

To use **GDPR** follow these steps:

1. Click on **Navigation** and open panel **GDPR**.

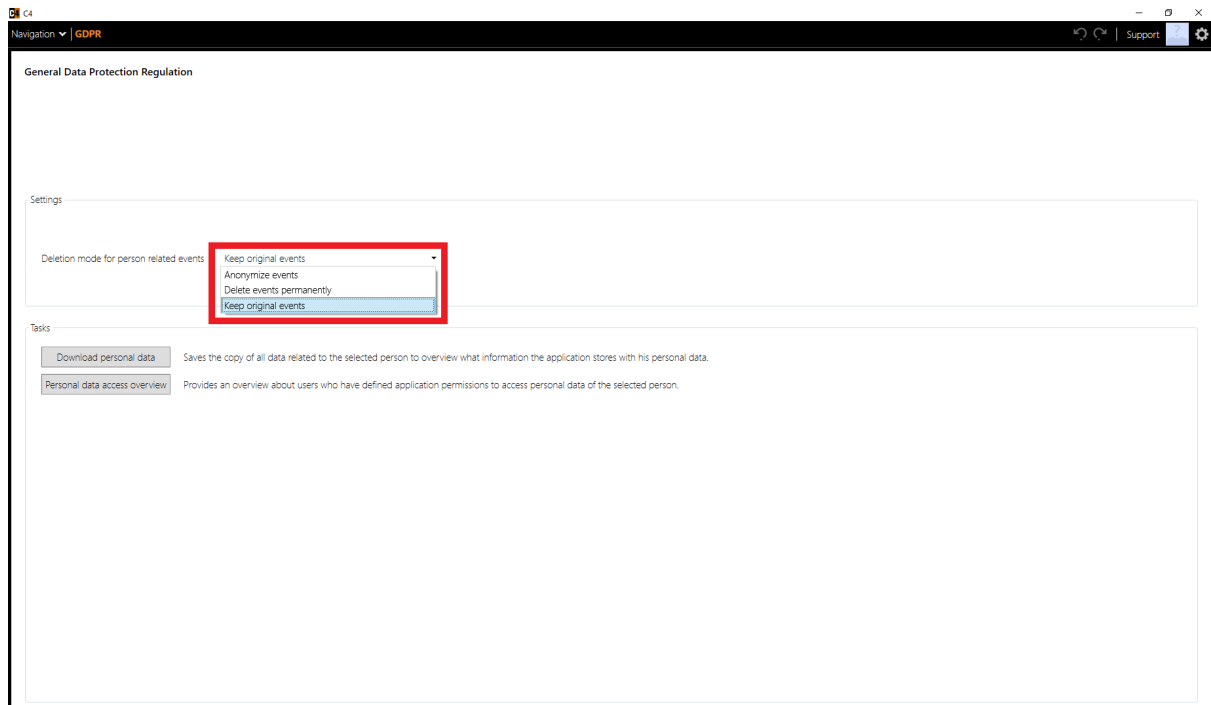
### Settings

The **GDPR** panel will open. The first part of the **GDPR** panel is dedicated to Settings. Currently the only setting option is for: Deletion mode for person related events. This is for managing events that are related to a deleted person in the system. There are three options:

- **Anonymize events** – The events associated to the deleted person will be anonymized. Instead of the original person name, the “Anonym” text will be shown in the events. Warning: This is an irreversible operation. Accepting this option will cause the related data to be lost!
- **Delete events permanently** – The events associated to the deleted person will be permanently deleted. Warning: This is an irreversible operation. Accepting this option will cause the related data to be lost!
- **Keep original events** – Associated events of the deleted person will contain the original data stored at the time of logging.

Once one of the options is chosen, ATS8600 will ask the user to **confirm** their decision or **cancel**.

When option anonymize or delete events is selected, 10 000 events are processed in each batch, when the batch is finished next one starts in 5 seconds. Time to process all events is dependent on ATS8600 server machine performance.



### Tasks

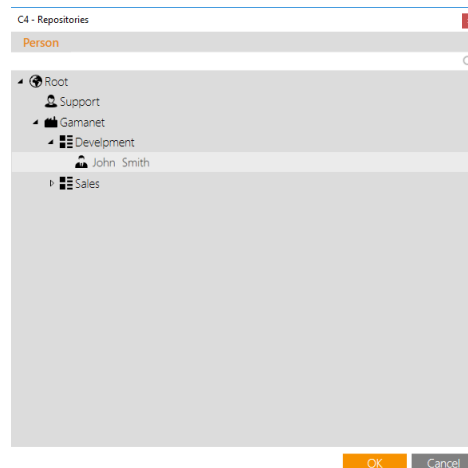
The **GDPR** panel allows the user to carry out 2 tasks:

- **Download personal data:** Save the copy of all data related to the selected person to overview what information the application stores with his personal data.
- **Personal data access overview:** Provides an overview about users who have defined application permissions to access personal data of the selected person.

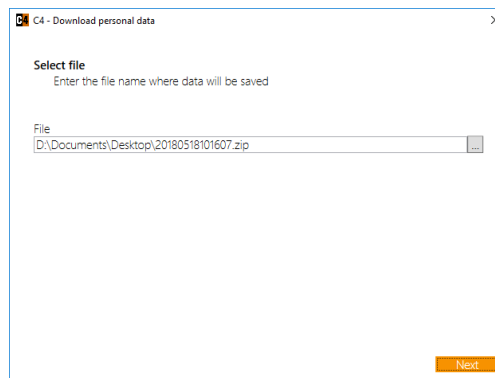
### Download Personal data / Personal data access overview



The two downloads are carried out in the same way:

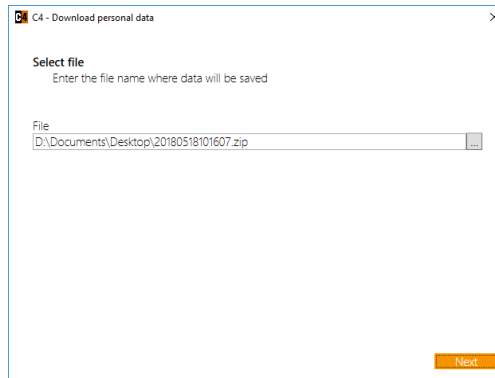
1. Start by clicking the **Download personal data/Personal data access overview** button.
2. A window will pop-up, allowing you to select the person, who's personal data should be downloaded. Once you choose the given person, click **OK**.



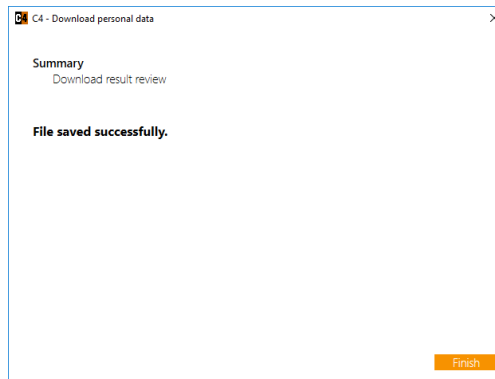
3. The next window will allow you to choose the file name and location to where the data will be saved. Once you have chosen a file path and have a name for the file, click **Next**.



4. The next step is for password encrypting the downloaded data. Write down a safe password. The pop-up will only allow you to click **Next** once the password is deemed safe enough. The buttons next to the password box are for:  - viewing the password,  - saving password to clipboard.



5. Once you click **Next**, the personal data will start downloading.
6. Once the download is finished, you will get a download result review – stating whether the file was saved successfully. Clicking on **Finish** will close the window.



## 8 Appendices

### 8.1 Badge report data

{{(dynamic)Badges.Holder.Properties}.Name} - for getting formatted name of holder use following expression: {GetFormattedName(Badges.Holder.Properties)}

{{(dynamic)Badges.Holder.Properties}.MiddleName}

{{(dynamic)Badges.Holder.Properties}.FirstName}

{{(dynamic)Badges.Holder.Properties}.FirstTitle}

{{(dynamic)Badges.Holder.Properties}.LastTitle}

{{(dynamic)Badges.Holder.Properties}.IdentificationCard}

{{(dynamic)Badges.Holder.Properties}.InternalNumber}

{{(dynamic)Badges.Holder.Properties}.ExternalNumber}

{{(dynamic)Badges.Holder.Properties}.Address}

{{(dynamic)Badges.Holder.Properties}.CellPhone}

{{(dynamic)Badges.Holder.Properties}.City}

{{(dynamic)Badges.Holder.Properties}.Country}

{{(dynamic)Badges.Holder.Properties}.Disabled} (Handicapped)

{{(dynamic)Badges.Holder.Properties}.Email}

{{(dynamic)Badges.Holder.Properties}.Gender}

{{(dynamic)Badges.Holder.Properties}.Note}

{{(dynamic)Badges.Holder.Properties}.Phone}

{{(dynamic)Badges.Holder.Properties}.Position}

{{(dynamic)Badges.Holder.Properties}.ValidFrom}

{{(dynamic)Badges.Holder.Properties}.ValidTo}

{{(dynamic)Badges.Holder.Properties}.Zip}

{{(dynamic)Badges.Holder.Properties}.Photo} - for displaying holder photo write following expression to Image component imageUrl: {ToUrl(Badges.Holder.Properties.Photo)}

Badges.Holder.Parents - all holder ancestors can be indexed with [i] and each has same set of properties as holder

Badges.Holder.Parent - direct parent of card holder (department or division where holder belongs if defined). Has same set of properties as holder

Badges.Holder.Company - company of person (if defined). Has same set of properties as holder.

{{(dynamic)Badges.Card.Properties}.Name}

{{(dynamic)Badges.Card.Properties}.CardCode}

{{(dynamic)Badges.Card.Properties}.IssueCode}

{{(dynamic)Badges.Card.Properties}.FacilityCode}

{{(dynamic)Badges.Card.Properties}.Status}

## 8.2 Reception report data

Visitor (VisitorModel)

{Visitor.Name} - for getting formatted name of holder use following expression:  
{GetFormattedName({Visitor.Name})}  
{{{(dynamic)Visitor.Properties}.FirstName}  
{{{(dynamic)Visitor.Properties}.DateOfBirth}  
{{{(dynamic)Visitor.Properties}.Car}  
{{{(dynamic)Visitor.Properties}.Company}  
{{{(dynamic)Visitor.Properties}.Note}  
{{{(dynamic)Visitor.Properties}.LastCheckIn}  
{{{(dynamic)Visitor.Properties}.Photo} - for displaying visitor photo write following expression to Image component imageUrl: {ToUrl({{(dynamic)Visitor.Properties}.Photo})}  
{{{(dynamic)Visitor.Properties}.IdentificationCard}

Visitee (PersonModel)

{Visitee.Name} - for getting formatted name of holder use following expression:  
{GetFormattedName(Visitee.Name)}  
{{{(dynamic)Visitee.Properties}.MiddleName}  
{{{(dynamic)Visitee.Properties}.FirstName}  
{{{(dynamic)Visitee.Properties}.FirstTitle}  
{{{(dynamic)Visitee.Properties}.LastTitle}  
{{{(dynamic)Visitee.Properties}.IdentificationCard}  
{{{(dynamic)Visitee.Properties}.InternalNumber}  
{{{(dynamic)Visitee.Properties}.ExternalNumber}  
{{{(dynamic)Visitee.Properties}.Address}  
{{{(dynamic)Visitee.Properties}.CellPhone}  
{{{(dynamic)Visitee.Properties}.City}  
{{{(dynamic)Visitee.Properties}.Country}  
{{{(dynamic)Visitee.Properties}.Disabled}  
{{{(dynamic)Visitee.Properties}.Email}  
{{{(dynamic)Visitee.Properties}.Gender}  
{{{(dynamic)Visitee.Properties}.Note}  
{{{(dynamic)Visitee.Properties}.Phone}  
{{{(dynamic)Visitee.Properties}.Position}  
{{{(dynamic)Visitee.Properties}.ValidFrom}  
{{{(dynamic)Visitee.Properties}.ValidTo}  
{{{(dynamic)Visitee.Properties}.Zip}  
{{{(dynamic)Visitee.Properties}.Photo} - for displaying visitee photo write following expression to Image component imageUrl: {ToUrl({{(dynamic)Visitee.Properties}.Photo})}  
{{{(dynamic)Visitee.Properties}.Parents} - all visitee ancestors can be indexed with [i] and each has same set of properties as holder



{{(dynamic)Visitee.Properties}.Parent} - direct parent of visitee (department or division where visitee belongs if defined). Has same set of properties as visitee  
{{(dynamic)Visitee.Properties}.Company} company of person (if defined). Has same set of properties as visitee.

#### Credential (CredentialModel)

{Credential.Name}  
{{(dynamic)Credential.Properties}.CardCode}  
{{(dynamic)Credential.Properties}.IssueCode}  
{{(dynamic)Credential.Properties}.FacilityCode}  
{{(dynamic)Credential.Properties}.Status}

#### Reception (ReceptionModel)

{Reception.Name}  
{Reception.Description}  
{Reception.IsVisiteeRequired}

#### AccessLevel (AccessLevelModel)

{AccessLevel.Name}  
{AccessLevel.Description}

#### Note:

If Properties field is not available, go to Dictionary section in Report Editor. Expand Business Objects, right click on required object (e.g. Visitor), Click Edit, then click Retrieve Columns, and check Properties. Confirm by clicking OK.

### 8.3 Events - variables

Variables	Device Id	Person Id	Name	Properties	Value	Old Value	Parent Id	Entity Id	Region Id	Holder	Device Desk	Level Id	Credentia Id	Category Id	Others
Access denied	•	•													DeviceReader, CredentialId, Reason
Access granted	•	•													DeviceReader, CredentialId
Access Granted To Lift	•	•													DeviceReader
Access granted for an unknown credential	•														IdentifierCode
Access during exit time	•														
Assigned to access level		•											•		
Access level created			•										•		TimeFrames
Access level deleted permanently													•		
Access level property changed				•	•	•							•		
Unassigned from access level		•											•		
Access point assigned													•		PointId
Access point unassigned													•		PointId
Sounder delay disabled	•														
Sounder delay enabled	•														
Active Call Redirected	•								•						
Alarm Acknowledged		•	•												
Antimasking alarm	•														
Alarm cancelled by keyswitch	•														
Alarm cancelled by user	•	•													
Alarm	•														Subaddress
Alarm Resolved		•	•												
Flow alarm	•														
Alarm during the exit time	•														
Inundation alarm	•														
Alarm invoked manually															Text
Alarm Marked As Starred															AlarmId

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentiaId	CategoryId	Others
Alarm Multibreak	•														
Panic alarm	•														
Panic alarm finished	•														
Alarm cancelled automatically	•														
Alarm restored	•														
Alarm during exit time restored	•														
Alarm Restored Multibreak	•														
Alarm occurred shortly after arming	•														
Alarm Unmarked As Starred															AlarmId
Alert Action Finished	•														
Alert Action Started	•														
All Active Alarms Deleted															
Extension disabled															AppBehaviorId
Extension enabled															AppBehaviorId
Extension property changed		•			•	•	•								
Area Failure Search Restored	•														
Area Search Failure	•														
Area Search Incomplete	•														
Armed automatically	•														
Armed by a key switch	•														
Armed	•		•												
Arming failed	•														
Armed too early	•														
Armed too late	•														
Armed during the exit time	•														
Armed partially	•		•												
Partially armed remotely	•		•												
Rearming after alarm	•														

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentialId	CategoryId	Others
Armed remotely	•	•													
Access granted Attendance mode	•	•													AttendanceMode, Direction, IdentifierCode
Audio Signal Lost	•														
Audio Signal Recovered	•														
Audio Transmission Started															CameraId
Audio Transmission Stopped															CameraId
Authentication failed		•													
Authentication failure	•														
Automatic arming postponed by user	•	•													
Automation Zone Off	•														
Automation Zone On	•														
Automation Zone On Level	•														Percentage
Backup amplifier activated	•														
Backup amplifier deactivated	•														
Backup Connection Activated	•														
Backup Connection Deactivated	•														
Low battery	•														
Low battery restored	•														
Detected usage of blocked credential	•														DeviceR, CredentialId, CredStatus
Buzzer turned off	•														
Buzzer turned on	•														
Buzzer failure	•														
Buzzer failure restored	•														
Buzzer Muted	•														
Uninhibit	•	•													

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentialId	CategoryId	Others
Inhibit	.	.													
Call Ended	.														
Fire brigade signalization failure	.														
Device Calling	.								.						Priority
Call Redirected	.								.						
Cancel Code Request Sent	.														
Capture Picture Requested	.														VideoTime
Card assigned to deck															CardId, DeckId, OldDeckId
Low battery on card	.	.													CredentialId
Changed content of the card		.								.					CodeParts
Card deck created			.												DeckId
Card deck deleted		.													
Card deck property changed		.		.	.	.									
Card format for card type created		.	.												CardTypeId
Card format deleted															FormatId
Card format property changed		.		.	.	.									
Card Programming Failed		.													Reason
Card Programmed Successful		.													
Credential Type Assigned To Device	.														CardTypeId, FormatId
Card type created		.	.											.	
Card Type Deleted															TypeId
Card type property changed		.		.	.	.									
Credential Type Unassigned From Device	.														CardTypeId
Card removed from deck															CardId, DeckId
Closed	.														

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentialId	CategoryId	Others
Close Timed	•		•												
Valid code entered	•		•												
Comms Failure	•														
Comms Failure Restored	•														
Communication Timeout	•														
Communication lost	•														
Communication Timeout Recovered	•														
Communication test	•														
Configuration changed	•														
Change of time	•														
Technician logged into system	•														
Duplicated address detected	•														DeviceD1, DeviceD2, Address
Configuration error Empty virtual parent	•														
Invalid property value	•														PropertyName
Incorrect devices configuration	•														
Technician logged out of system	•														
Connected	•														
Connection ended	•														DeviceOut
Connection established	•														DeviceOut
Connection established partially	•														DeviceOut
Communication cannot be established due to invalid authentication	•														
Connection interrupted	•														DeviceOut
Continual recording finished	•														
Continual recording started	•														
Control desk Notification	•											•			

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentiaId	CategoryId	Others
acknowledged															
Control desk Notification deleted	.											.			
Control desk notification Active 1	.											.			
Control desk notification Active 2	.											.			
Control desk notification Emergency call	.											.			
Control desk notification Error	.											.			
Control desk notification Line fault	.											.			
Control desk notification Normal call	.											.			
Conversation ended	.								.						
Conversation started	.								.						
Counter Value Changed				.	.										
Courier In	.														
Credential created		.	.											.	HolderId, DeckId, Status
Credential deleted		.													HolderId
Credential disabled		.								.					Reason
Credential enabled		.								.					
Credential holder removed		.													HolderId
Card activated		.													HolderId
Credential property changed		.		.	.	.				.					
Credentials Merged										.					Credential1, Credential2, CombinationId
Credentials Unmerged										.					Credential1, Credential2
Credential validation rule disabled															RuleId
Credential validation rule enabled															RuleId

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentialId	CategoryId	Others
Credential Validation Rule Property Changed		•			•	•	•								
Database Backup Failed	•														Retries
Database Size Reached Configured Threshold															DatabaseSize, Threshold
Binary data sent	•														SentData
Defocus Detected	•														
Delayed Reset Pressed	•														
Device Access Memory Cleared	•														
Device Access Memory Forced Upload	•														
Device Added To Call	•								•						DeviceFrom
Device archived		•						•							
Device Camera Created	•														CameraId
Device Camera Deleted	•														CameraId
Device category changed		•													PreviousCategory, NewCategory, TypeId
Command sent	•														Command
Device created		•		•				•							•
Configuration fault	•														FaultCode
Device link created	•														LinkId
Device link deleted	•														LinkId
Device mode activated	•														DeviceMode
Device parent changed		•		•											OldParent, NewParent
Device permanently deleted		•						•							
Device property changed		•			•	•	•								
Device restored		•						•							
Device Upload Resolved	•		•												
Dial In Answer	•														
Dialler retry attempt	•														
Dial Remote	•														



Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CategoryId	CategoryId	Others
Dirty	•														
Disabled	•														
Disarmed automatically	•														
Disarmed by keyswitch	•														
Access to area during alarm	•		•												
Remotely disarmed during alarm	•		•												
Disarmed	•		•												
Disarm Failure Too Early	•														
Disarm Failure Too Late	•														
Partially disarmed	•		•												
Partially disarmed remotely	•		•												
Remotely disarmed	•		•												
Disconnect Early	•														
Disconnected	•														
Document associated											•				DocumentId, DocName, Metadata
Document association removed											•				DocumentId, DocName
Door closed	•		•												
Door opened	•		•												
Door forced open	•														
Door opened permanently	•														
Door open too long	•														
Device driver aborted its activity due to its own request.	•														
Insufficient license to start	•														
Driver installed		•		•											Version
Network connection interrupted	•														
Network connection restored	•														Retries

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredateId	CategoryId	Others
Driver in a test version	•														
Driver started	•														
Failed to start	•														
Driver stopped	•														
Driver stopped License expired	•														
Duress signal from keypad	•		•												
Reset emergency in area by a key	•														
Reset emergency in area by user	•		•												
Enabled	•														
Engineer reset performed	•														
Engineer reset required	•														
Evacuation Finished	•														
Evacuation Started	•														
Event Filter Created		•		•											ScriptBody
Event Filter Deleted		•													
Event Filter Failed To Compile		•													
Event Filter Property Changed		•			•	•	•								
Event Filter Script Changed		•													ScriptBody
Event Type Property Changed		•			•	•	•								
Event Retention Period Changed		•				•									NewValue
Event Type Severity Changed		•													NewType, OldType
Missing Framework Or DLL	•														
Unhandled exception	•														ExceptionDescription
Execute Process On Client Requested															Process, Args
Exit button pushed	•														
Exit Failure	•														

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentiaId	CategoryId	Others
Extension Pin Disabled										•					CardId
Extension Pin Enabled										•					CardId
Message sent	•	•													Address, Text
Message sending failed	•	•													Address, Text, FailureReason
Face Detected	•														
Failure	•														FailureDescription
Restoring after an encryption error	•														
Failure restored	•														FailureDescription
Failure signalization activated	•														
Failure signalization deactivated	•														
Failure signalization delay disabled	•														
Failure signalization blocked	•														
Failure signalization delay enabled	•														
Failure signalization enabled	•														
Failure signalization fault	•														
Jamming fault	•														
Restore after a jamming fault	•														
Film Low	•														
Film Low Restored	•														
Film Out	•														
Film Out Restored	•														
Finger Deleted										•					CredentialId, Finger
Finger Enrolled										•					CredentialId, Finger, Quality
Alarm counter status	•														CNT
Fire alarm	•														

Variables	Device Id	Person Id	Name	Properties	Value	Old Value	Parent Id	Entity Id	Region Id	Holder	Device Desk	Level Id	Crede ntial Id	Category Id	Others
Fire alarm activated by operator	.														
Fire pre-alarm	.														
Fire pre-alarm ended	.														
Fire alarm was restored	.														
Fire brigade signalization	.														
Fire brigade signalization delay disabled	.														
Fire brigade signalization disabled on	.														
Fire brigade signalization delay enabled	.														
Fire brigade signalization enabled	.														
Turning off fire brigade signalization	.														
Fire fighting signalization delay disabled	.														
Fire fighting signalization delay enabled	.														
Fire fighting disabled	.														
Fire fighting enabled	.														
Fire fighting failure	.														
Fire protection enabled	.														
Fire fighting turned off	.														
Fire warning	.														
Fire warning restored	.														
Firmware Upgraded	.														
Firmware is incompatible with the driver	.														Firmware
User first opened door	.		.												
Floor Accessed On Device	.														DeviceFloor
Floor Secured On Device	.														DeviceFloor
Fuse failed	.														
Restore after a fuse failure	.														
General Call Started	.														Priority

Variables	Device Id	Person Id	Name	Properties	Value	Old Value	Parent Id	Entity Id	Region Id	Holder	Device Desk	Level Id	Credential Id	Category Id	Others
Grounding Fault	•														
Grounding Fault Recovered	•														
Group Call Started	•														Priority
Guard Dead	•														
Hardware Failure	•														
Hardware Failure Restored	•														
Holiday created		•	•												SetId
Holiday deleted		•													SetId
Holiday property changed		•		•	•	•									SetId
Holiday set created		•	•												Holidays
Holiday set deleted		•													
Holiday set property changed		•		•	•	•									
Invalid code attempted too often	•														
Image Stored	•														
Import Changes Confirmed		•													Type
Import Failed		•													RootId, Type, ChangesTime
Import Finished		•													RootId, Type, ChangesTime
Import Started		•													Type
Installation Issue Resolved Audit Log															Type, Installation
Internal communication error	•														Detail
Restore after an internal communication error	•														Detail
Interval Added To Call	•														Interval
Log deleted	•														
Key Retrieved	•		•												
Key Returned	•		•												
Unknown Key Returned	•		•												
Key turned to Off position	•														

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredeatialId	CategoryId	Others
Key turned to On position	•														
Key turned	•														
Lift Landed	•														DeviceFloor
Line Crossing Detected	•														
Line Down	•														
Line Fault Monitor Restored	•														
Line Up	•														
Live video stream requested															VideoSourceId
Local Alarm	•														
Local Alarm Recovered	•														
Locked	•		•												
Mains failed	•														
Restore after a mains failure	•														
Map Archived		•					•								
Map created		•	•				•							•	
Map deleted		•					•								
Map Parent Changed		•	•												OldParent, NewParent
Map Property Added To Region								•							MapId
Map property changed		•			•	•	•								
Map Property Removed From Region								•							MapId
Map Restored		•					•								
Maximal level overrun	•														
Memory failure	•														
Memory failure restored	•														
Memory locked	•														
Memory unlocked	•														
Memory is full	•														FullnessPercentage
User entered menu	•		•												
User exited device menu	•		•												

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentialId	CategoryId	Others
Minimal level underrun	•														
Configuration failure Missing device	•														Address, Description, DeviceCategory, DeviceTypeId, DeviceName
Missing Privilege Operation Attempted											•				PrivilegeId
Day mode activated	•														
Night mode activated	•														
Presence mode activated	•														
Presence mode deactivated	•														
Monitoring Company Command	•														
Monitoring Company Command Restored	•														
Motion detected	•														
Multiple Call Started	•														Priority
Muster Region Roll Called								•							
Network Down	•														
No dial tone	•														
Non Transferable Credential Created		•		•										•	HolderId
Not enough High Securer Users	•														
Not enough High Securer Users, warning outputs activated	•														
Not enough High Securer Users, warning outputs restored	•														
Not enough High Securer Users restored	•														
Object Removal Detected	•														
Opened	•														
Open Timed	•		•												

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CategoryId	Others
Overheated	•													
Overheat restored	•													
Overloaded	•													
Overload restored	•													
Panel Access Allowed														PanelId, TrusteeId
Panel Access Denied														PanelId, TrusteeId
Password changed			•											PasswordId
Permission denied														ObjectId, TrusteeId, ChangedPermissions
Permission Denied Non Inherited														ObjectId, TrusteeId, ChangedPermissions
Permission granted														ObjectId, TrusteeId, ChangedPermissions
Permission without inheritance granted														ObjectId, TrusteeId, ChangedPermissions
Permission revoked														ObjectId, TrusteeId, ChangedPermissions
Person Manually Added the Region			•					•						
Person archived		•					•							
Person category changed		•												PreviousCategory, NewCategory
Person created		•	•				•						•	
Person parent changed		•	•											OldParent, NewParent



Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentialId	CategoryId	Others
Person permanently deleted		•					•								
Person property changed		•		•	•	•									IsAttached
Person forcibly removed from region		•	•												
Person restored		•					•								
Phone communicator failure	•														
Restoring of phone communicator after a technical problem	•														
Pin Received	•														Pin
Popup Disabled	•														
Popup Enabled	•														
Power save mode finished	•														
Power save mode started	•														
Preset activated by user	•		•												Preset
Preset stored by user	•		•												Preset
Printer failure	•														
Restored after a printer failure	•														
Privilege granted			•												PrivilegeId
Privilege revoked			•												PrivilegeId
PTZ Command Sent	•														Command, Move, Count
Random Check Report Failed			•												DoorId, AlcoholLevel, AlcoholTestId, CheckWitness, Observation
Random Check Report Passed			•												DoorId, AlcoholLevel, AlcoholTestId, CheckWitness, Observation
Random Check Started			•												DoorId
Reception Created				•											ReceptionId

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CreationalId	CategoryId	Others
Reception Deleted															ReceptionId
Reception Property Changed					.	.	.								ReceptionId
Requested recorded video															VideoSourceId, RequestedUtc Time
Recording bookmark created	.														BookmarkName
Redial	.														
Redirect Calls To Device Activated	.								.						
Redirect Calls To Device Deactivated	.								.						
Redirect Calls From Device Activated	.								.						
Redirect Calls From Device Deactivated	.								.						
Region archived		.					.								
Region category changed		.													PreviousCategory, NewCategory
Region created	.	.	.				.							.	
Device link added to region	.							.							
Device link deleted from region	.							.							
Person Left the Region		.	.												Door
Region Entrance Detected	.														
Region is evacuated								.							
Region Exiting Detected	.														
Person Entered the Region		.	.												Door
Region Is Empty								.							
Region Is Not Empty								.							
Persons in region exceeded threshold								.							Limit, CurrentCount
Persons in region reached threshold								.							Limit

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredeNtiaId	CategoryId	Others
Persons in region restored threshold								.							Limit, CurrentCount
Region parent changed		.	.												OldParent, NewParent
Region permanently deleted		.					.								
Region property changed		.		.	.	.									
Detected region re-entry															Person, Region, Door
Region Report Created			.					.							ReportId
Region Report Deleted								.							DocumentId
Region Report Property Changed				.	.	.		.							DocumentId, ReportName
Region restored		.					.								
Remote Callback Triggered	.														
Remote Disconnect Activated	.														
Remotely Redirect All Calls	.								.						DeviceFrom
Report Printed				.											ReportId
Report shown				.											ReportId
Reversed settings	.														
Cold restart	.														
Restart	.														
Restored	.														
Ring shunt restored after short circuit	.														Ring
Ring shunt failure	.														Ring
Device Ringing	.														
Ring interrupted	.														Ring
Ring shunt restored after termination	.														Ring
Role assigned			.												RoleId
Role created			.												RoleId
Role deleted															RoleId
Role property changed				.	.	.									RoleId

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentialId	CategoryId	Others
Role unassigned			•												RoleId
Automatic Action Executed		•													
Automatic action created		•	•												ScriptBody, TimeFrames
Automatic action deleted		•													
Automatic action disabled		•													
Automatic action enabled		•													
Automatic action failed to compile		•													
Automatic action property changed		•		•	•	•									
Automatic action script changed		•													ScriptBody
Requested recorded video stream															VideoSourceId, From, To
Sudden Scene Change	•														
Security Action Finished	•														
Security Action Started	•														
Service Connector Direct Connect	•														
Service mode activated	•														
Service mode deactivated	•														
Service On	•														
Service Out	•														
Service Requested	•														
Short Circuit	•														
Short Circuit Recovered	•														
Short Supervision	•														
Short Supervision Restored	•														
Automatic security monitoring station (SMS) test call	•														
Security monitoring station (SMS) test call failed	•														

Variables	Device Id	Person Id	Name	Properties	Value	Old Value	Parent Id	Entity Id	Region Id	Holder	Device Desk	Level Id	Crede ntial Id	Category Id	Others
Security monitoring station (SMS) test finished	•														
Manual security monitoring station (SMS) test call	•														
Dialing control communication panel	•														
Message received	•		•												Address, Text
Soft Anti-Passback	•		•												
Sounder activated	•														
Sounder deactivated	•														
Sounder disabled	•														
Sounder enabled	•														
Sounder failure	•														
Sounder restored after failure	•														
Sounder Muted	•														
Sudden Change of Sound Intensity	•														
Storage failure	•														AI
Storage device is full	•														AI
Recording restored after failure	•														AI
Recording restored after storage device freed	•														AI
Successful Event Reporting To Central Station	•														
Supervision	•														
Supervision Failed	•														
Supervision Restored	•														
Suspicious Button Active	•														
Synchronisation Ended	•														
Synchronisation Failed	•														Reason
Synchronisation Started	•														
Tamper	•														

Variables	Device Id	Person Id	Name	Properties	Value	Old Value	Parent Id	Entity Id	Region Id	Holder	Device Desk	Level Id	Credential Id	Category Id	Others
Tamper restored by user	•	•													
Tamper completed	•														
Alarm During Soak Test Finished	•														
Alarm in test mode	•														
Alarm During Soak Test	•														
Automatic test	•														
Battery test failed	•														
Failure in test mode	•														
Battery test restored after a failure	•														
Battery test finished	•														
Test Finished	•														
Soak Test Finished	•														
Recovery of normal state in test mode	•														
Test Secure Failed	•														
Test Secure Finished	•														
Test Secure Started	•														
Test Secure Succeeded	•														
Battery test started	•														
Test Started	•														
Soak Test Started	•														
Test Successful	•														
Timed Anti-Passback	•	•													
Timed Antipassback Full	•														
Time set. Offset with real time was ? minutes	•														TimeOffset
Added new time restriction entry											•				FrameId, Days, From, To
Time Frame Day Added											•				FrameId, Day, AllDay
Time Frame Day Removed											•				FrameId, Day, AllDay
Time restriction modified		•			•	•	•				•				
Removed time restriction											•				FrameId

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredentiaId	CategoryId	Others
entry															
Egress timeout	•														
Ingress timeout	•														
Timer Aborted	•														TimerName
Timer Elapsed	•														TimerName
Timer started	•														
Timer stopped	•														
Switch to T2	•														
Too Many Retries	•														
Unattended Baggage Detected	•														
Attempted unauthorized operation											•				MissingPermissions
Unknown Card Detected															DeviceReader, CardType, CardCode, FacilityCode, IssueCode, DisplayName
Technical event on device	•														EventDescription
Unlocked	•		•												
Credentials Synchronization Failure	•		•												Reason
Changed PIN	•		•												
User signed in				•											UserId, Credential, SessionId, MatchingId
User signed off															UserId, SessionId, FormerConnectionId
Value below the tolerance limit	•														
Value over the tolerance limit	•														
Recorded vehicle	•														VehicleRegistr

Variables	DeviceId	PersonId	Name	Properties	Value	OldValue	ParentId	EntityId	RegionId	Holder	DeviceDesk	LevelId	CredateId	CategoryId	Others
registration plate:															ationPlate
Video Content Analysis Event	•														
Videosignal Displayed On Monitor	•														DeviceMonitor
Video signal lost	•														
Video signal restored	•														
Video Stored	•														
Visit Closed															VisitId, VisitorId, ReceptionId
Visit Created				•											VisitId, Start, ReceptionId, VisitorId, Visiteeld, Reason
Visitor Category Changed		•													PreviousCategory, NewCategory
Visitor Created				•											VisitorId
Visitor Deleted															VisitorId
Visitor Property Changed					•	•	•								VisitorId
Passage test failed	•														
Passage test finished	•														
Passage test started	•														
Passage test succeeded	•														
Warning before automatic arm	•														
Warning	•														
Warning ended	•														
Zone activated	•														
Normal state restored	•														