ATS8600
User Guide
ATS8600 2016 SP5

Contents

1 Initial system startup 5

1.1 Creating the system administrator's user account 5
1.2 License activation 6
1.3 Trial version 7

2 Operating procedures 8

2.1 Filtering 8
2.2 Working with the Tree 8
2.3 Saving changes 10
2.4 Event History 10
2.5 Information bar 11

3 System configuration 12

3.1 Connecting devices 12
3.1.1 Driver installation 12
3.1.2 Driver upgrade 12
3.1.3 Creating a device tree 13
3.1.3.1 Device tree auto detection 13
3.1.3.2 Creating a device tree manually 13
3.1.4 Starting communication 14
3.1.5 Device status information table 15
3.1.6 Remote device control 16
3.2 Visualization 16
3.2.1 Device visualization 17
3.2.2 Creating a map hierarchy 18
3.2.3 Assign action to button 18

4 Operating the system 20

4.1 Working at the dispatcher site 20
4.1.1 Monitor panel windows 20
4.1.2 Operating the Monitor panel 21
4.1.3 Dealing with alarms 21
4.2 Overview of the history of alarms 23
4.3 Video wall 23
4.3.1 Live video display 23
4.3.2 Playing back video footage 24

4.4 Persons management 25
4.4.1 Creating an application account 25
4.4.1.1 Creating a user account 25
4.4.1.2 Creating roles 26
4.4.1.3 Identifier history 27
4.4.2 Organizational structure creation 27
4.4.3 Deleting an organizational unit record 28
4.5 Granting access to secured areas 28
4.5.1 System settings for identifiers 29
4.5.1.1 Card formats in use 29
4.5.1.2 Validation rules for identifiers 29
4.5.2 Assigning identifiers 30
4.5.2.1 Card learning 31
4.5.3 Creating card decks 31
4.5.4 Definition of access permissions 32
4.5.4.1 Simple access permission 32
4.5.4.2 Advanced access permission 33
Creating an access level 33
Holidays 34
4.5.5 Sending identifiers to a device 35
4.5.6 Access reports 35
4.6 Creating a region 36
4.7 Permission setting and status 36
5 Advanced system properties 39
5.1 Sending emails 39
5.2 Connecting a GSM gateway 39
5.3 Automatic actions 40
5.3.1 Automatic action creation 40
5.3.2 Timed automatic action creation 42
5.3.3 Automatic action script 42
5.3.4 Running Powershell script 42
5.4 Visitors management 43
5.4.1 Creating a reception 44
5.4.2 Visitor evidence 44
5.4.3 Modifying Visitor Data 45
5.5 Access Guard 46
5.6 Displaying camera feed automatically 47
5.7 Linking a camera with a device 47
5.8 Counting persons 48
5.9 Event priorities 49

5.10 Alarm priority 49
5.11 Data import and export 49
5.11.1 Exporting data to a .csv file 49
5.11.2 Importing the device tree from a csv file 50
5.11.3 Importing persons and identifiers from a csv file 50
5.11.4 Importing manually created csv file 51
5.12 Reports 53
6 System maintenance 54
6.1 System diagnostics 54
6.2 Deleting older events 54
6.3 Database size monitoring 55
7 Appendices 56
7.1 Badge report data 56

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.

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.

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 recycled 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.
- **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 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. Udalosti môžu mat nasledovné priority:

-  - fire alarm

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

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).

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.

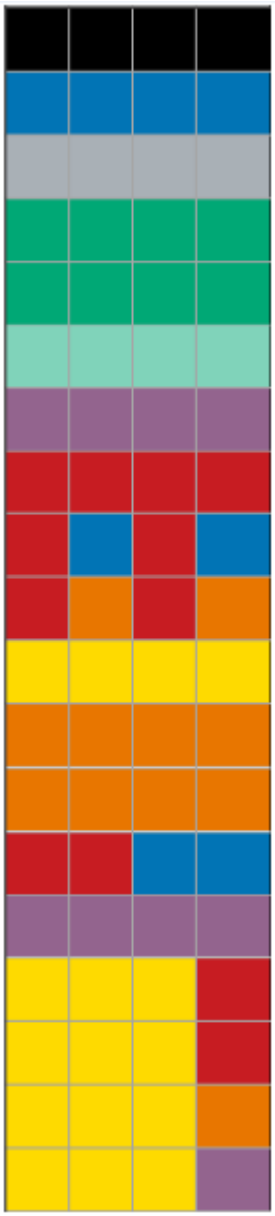
You can stop communication with the device by clicking the **Stop** command. If the circuit is activated and you repeatedly click the **Start command,** the circuit will restart.

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 - unknown/no status

Blue - normal status

Grey - bypassed

Green - locked

Green - armed

Cyan - partially armed

Violet - activated

Red - rearmed

Red/Blue - alarm

Red/Orange - tamper

Yellow - test

Orange- failure

Orange - disconnected

Red/blue - alarm precondition

Violet - not ready to arm

Yellow/Red - alarm during test

Yellow/Red - alarm precondition during test

Yellow/orange - tamper during test

Yellow/violet - activated during test

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 shape**
  - **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.
- **Add AutoCAD Map** - adding map vector graphics in the AutoCad format (supported format dwfx). 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

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
   - **Bring to front**, **Send to back** - displaying the visualized object with respect to other objects on the map

   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

   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.

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.

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 . Click again 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.
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.
   vi. **Responsible people for this alarm:** displays persons responsible for the region in which the alarm occurred.
   vii. **Persons count:** displays the number of persons present in the region in which the alarm occurred.
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. 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 and double-click or 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.

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 Live Video** 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 move a camera from a small window to the main window. Click ✕ to close the camera feed.

You can switch display mode by clicking **Full+3, 2x2, 3x3** tabs.

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:

- - 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.
- **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.

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 described 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 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 recycled 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**.

Warning:
The **Credential Types** tab is available only if at least two card types are enabled in the system. If only one card type is enabled in the system, this card type will be applied automatically to all connected devices supporting persons management. If another card type is only enabled after persons' access started to be managed by security technologies, it will be necessary to manually select the card type in use individually on all technologies once the other card type is enabled.

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.

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.

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. Swipe the card through the card reader. The card will be loaded into the system and the card code will be filled in automatically.
7. 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.

4.5.3 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 **Print** to generate the card imprint report which can be printed on a printer.

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.
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:

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.

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. **Map** - you can add map for the region.

4.7 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 permissions are available for commands:

- **Arm** - can arm the object.
- **Uninhibit** - can cancel the bypassing of the object.
- **Inhibit** - can bypass the object.
- **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.

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**.

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.
- 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.

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 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.

5.3.4 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 Visitee Required** - check to request whom a visitor visited when registering a visit.
   v. **Exit Reader** - an exit reader used at the end of the visit.
3. To delete a reception, select the reception in the list and click .

Use the Report tab to create a new report.

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. Click in the card list, select a card to be assigned to the visitor, see Creating card decks.
   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 Level** - 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 visitor privilege is enabled.

5.4.3 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 Access Guard

Access Guard provides a way for users to control persons who enter buildings, rooms etc. Every person, who goes trough access point using some credential is shown in panel Access Guard. 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 trough more detailed inspection.

The **Access Guard** functionality must first be enabled in ATS8600 system settings:

1. Click on **Navigation** and select **Extensions**.
2. Check **Access Guard**.

To use **Access Guard** follow these steps:

1. Click on **Navigation** and open panel **Access Guard**.
2. Add access point (door), which you want to monitor by clicking on the button  and from the device tree select door. You can monitor 2 access points at the same time.

- 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. 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 Access Guard. Value **Random Check Probability** represents probability percentage. Default value is 2.

Note:
Access photos in Access Guard 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. Check the **Client Camera Pop-up**option to allow the use of the automatic camera pop-up in the application.
3. Create a new automatic action and define the part with conditions for the action by following the procedure described in chapter Automatic action creation.
4. Choose the **Show Live Video 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.
5. 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.

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 **Smer** 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 just persons on premise** 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 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.

5.10 Alarm priority

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

5.11 Data import and export

5.11.1 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.

5.11.2 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.

5.11.3 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 2016, all fields will be mapped automatically.

5.11.4 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. 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).

Example of csv file of a person with card:

Id	Name	Card_CardCode	Card_Name

3456	PersonA	12398766	Card1

5.12 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 devvices** - 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 3. It is extended logging, which require 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. **Long** - 365 days

iii. **Medium** - 180 days

iv. **Short** - 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.

7 Appendices

7.1 Badge report data

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

Badges.Holder.Properties.MiddleName

Badges.Holder.Properties.FirstName

Badges.Holder.Properties.FirstTitle

Badges.Holder.Properties.LastTitle

Badges.Holder.Properties.IdentificationCard

Badges.Holder.Properties.InternalNumber

Badges.Holder.Properties.ExternalNumber

Badges.Holder.Properties.Address

Badges.Holder.Properties.CellPhone

Badges.Holder.Properties.City

Badges.Holder.Properties.Country

Badges.Holder.Properties.Disabled (Handicapped)

Badges.Holder.Properties.Email

Badges.Holder.Properties.Gender

Badges.Holder.Properties.Note

Badges.Holder.Properties.Phone

Badges.Holder.Properties.Position

Badges.Holder.Properties.ValidFrom

Badges.Holder.Properties.ValidTo

Badges.Holder.Properties.Zip

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.

Badges.Card.Properties.Name

Badges.Card.Properties.CardCode

Badges.Card.Properties.IssueCode

Badges.Card.Properties.FacilityCode

Badges.Card.Properties.Status