activeVIEW

Active View Online Platform Manual

English

Quick start

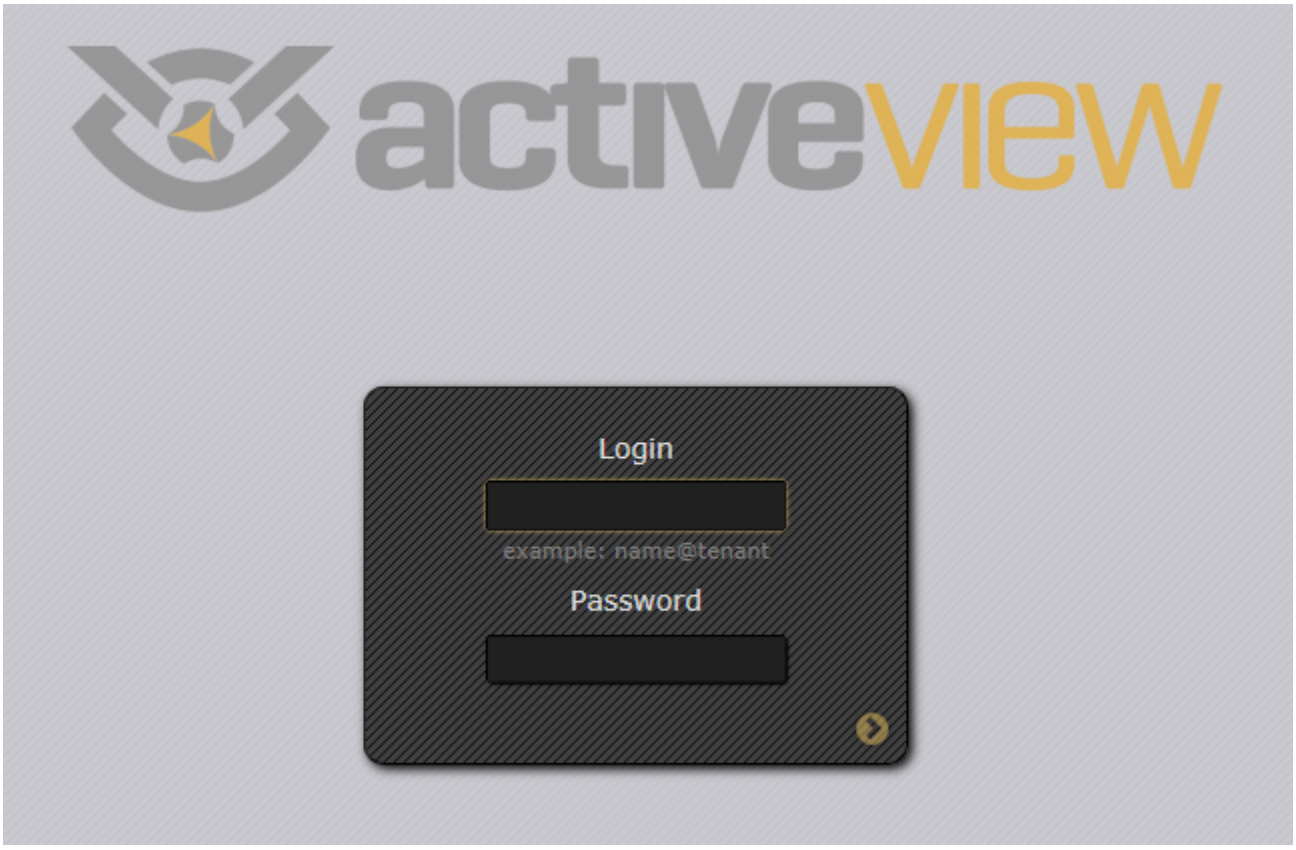
After receiving your first ActiveGuard device, you can start using ActiveView. This quick start section will walk you through some basic functionalities and give you some understanding of what the application looks like and how it works.

Connecting your ActiveGuard

Make sure your device is properly configured to connect to the ActiveView server through your mobile operator's network. If in doubt, contact your administrator. Next, place a SIM card inside your ActiveGuard (refer to the ActiveGuard user manual for details) and turn it on. Now you are ready to start using ActiveView.

Verifying connection

When you start ActiveView, you see a ***login screen***. Use your user name and password to log in to the application.



After successfully logging in, you are taken to the ***main screen***. On the upper edge, there is the main menu. You can use it to get to main application functionalities, such as *Alarms*, *Events*, *Reports*, *Management*, *Administration*. In the upper right corner you can see your name. Click it to change user settings, change your password or log out.

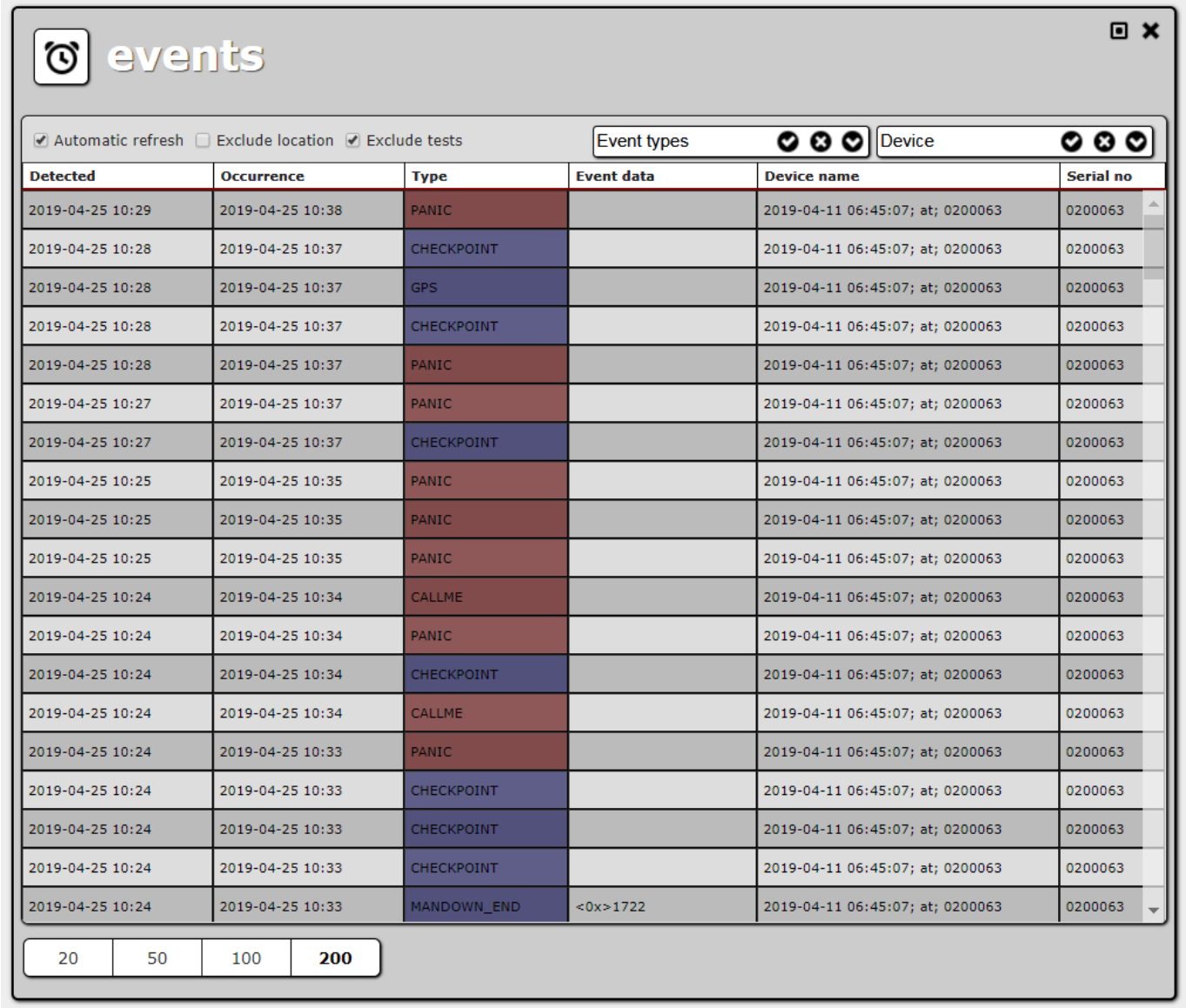
Your ActiveGuard should have connected to the server by now. To see a list of connected devices, choose the *Management* tab in the main menu and then select *Devices*. The ***Devices panel*** will open. Find your ActiveGuard and double-click it to open its ***detail view***.

Now you see two panels: the first one is the device list and next to it, on the right, there are details of the selected device. This pattern is used across the whole application. Details of an object chosen in one panel are presented in a new panel on the right. This way, you can open two, three or more panels, with more and more details. If not all panels fit the screen, you can scroll them left and right, by moving your mouse while holding the Ctrl key and the left mouse key. Alternatively you can click on buttons on the left and right edges of the browser window (with **<** and **>** icons).

The device's details panel shows the connection status, signal strength and battery level of your ActiveGuard.

When your device is connected to the server, it sends different kinds of events. Some of them are just for technical purposes (e.g. *TEST* event). Other mean that an alarm occurred (e.g. *PANIC* event).

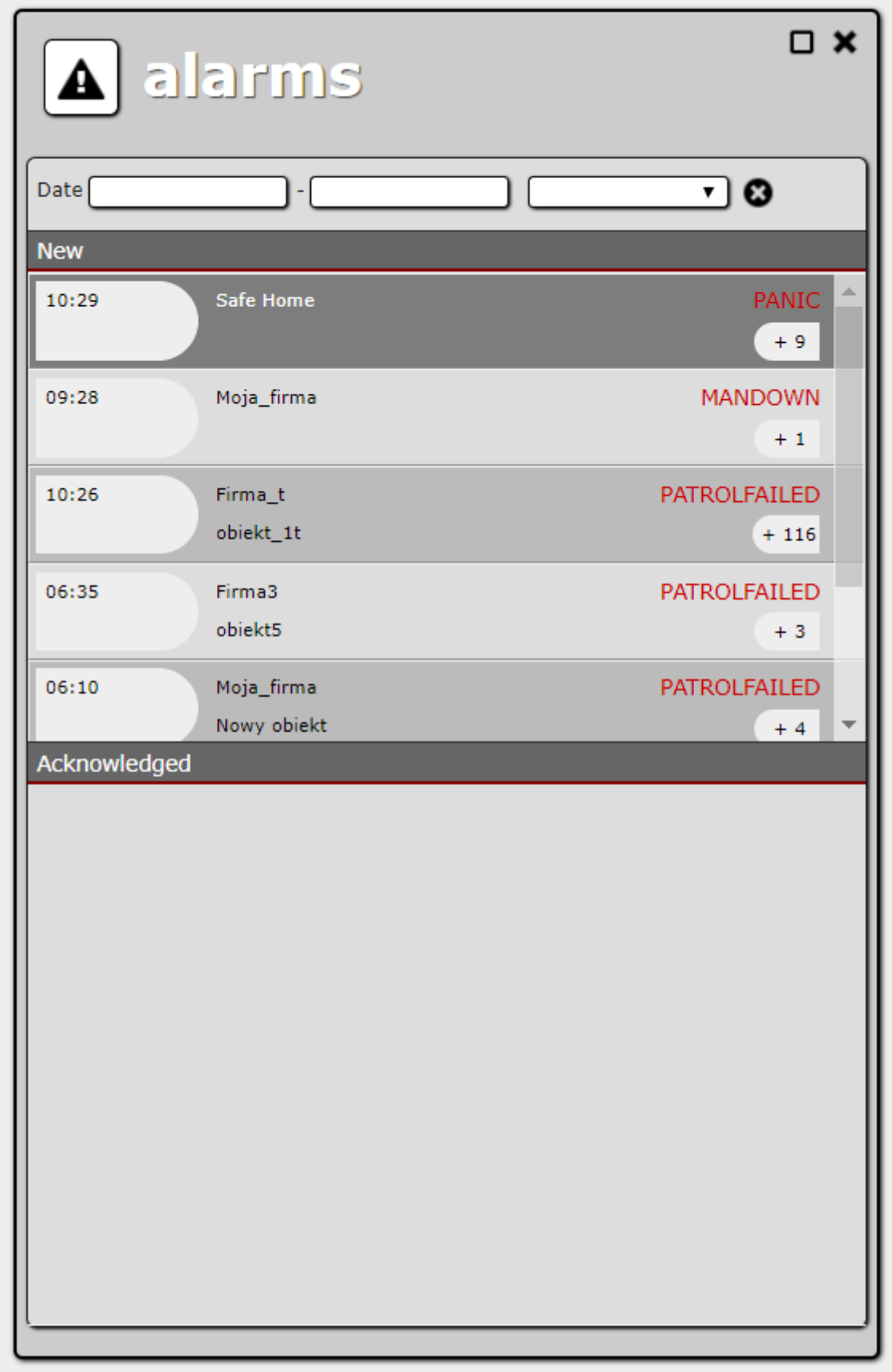
All events received by ActiveView are listed in the ***Events panel***. Choose *Events* in the main menu to open it.



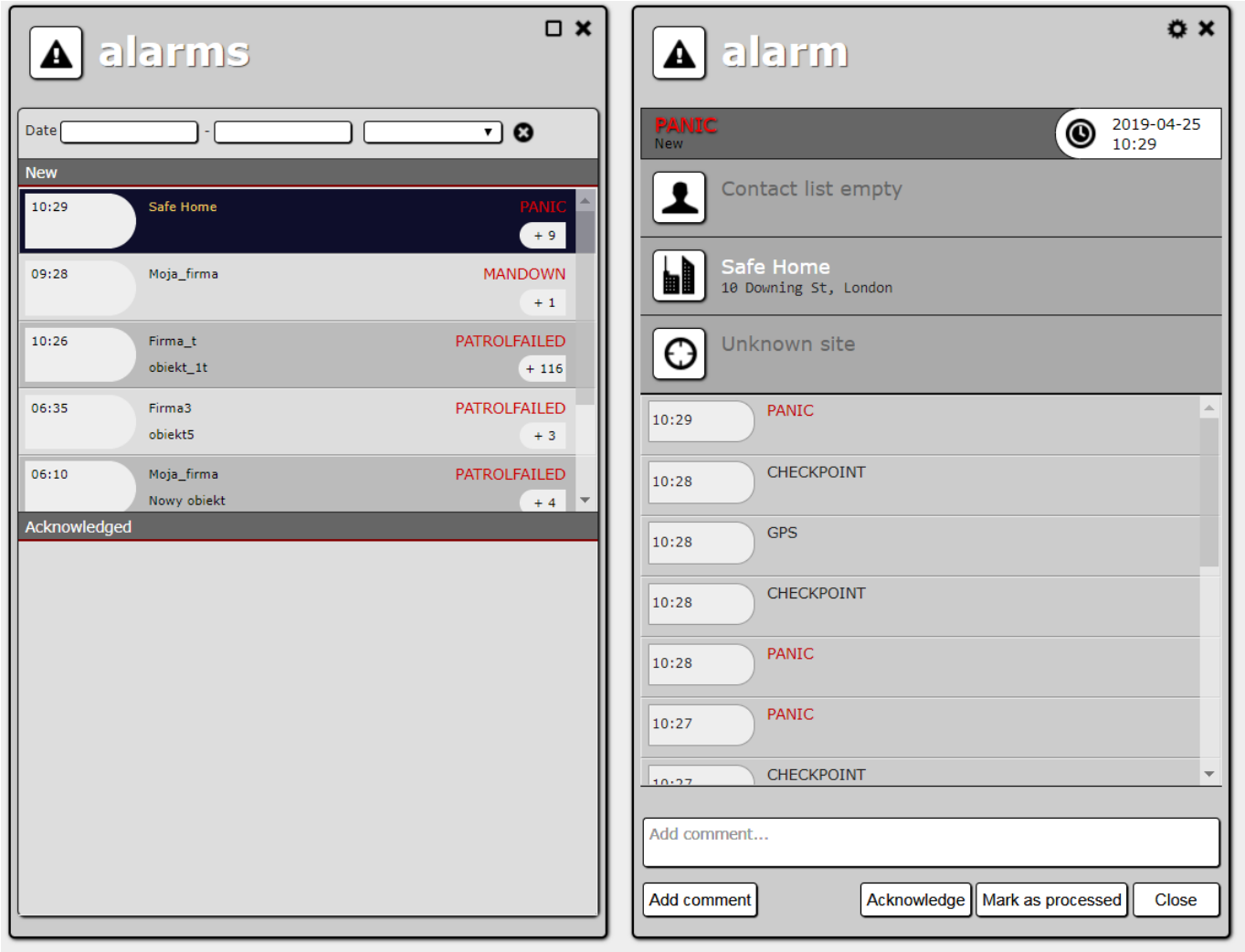
Now hit the Panic button on your ActiveGuard. You should see a *PANIC* event on top of the events list.

Use appropriate filters to display the events in detail: Skip *LOCATION*, Skip *TEST*, due to the type of event or device.

When ActiveView receives a *PANIC* event, it generates an alarm. The *Alarms* tab in the main menu should start blinking. Choosing it opens the ***Alarms panel***.



Find *PANIC* alarm in the *New* section and double-click it. You now see the **alarm's details**, including its type (*PANIC*), time of occurrence and list of other alarms and events which occurred on the same site.



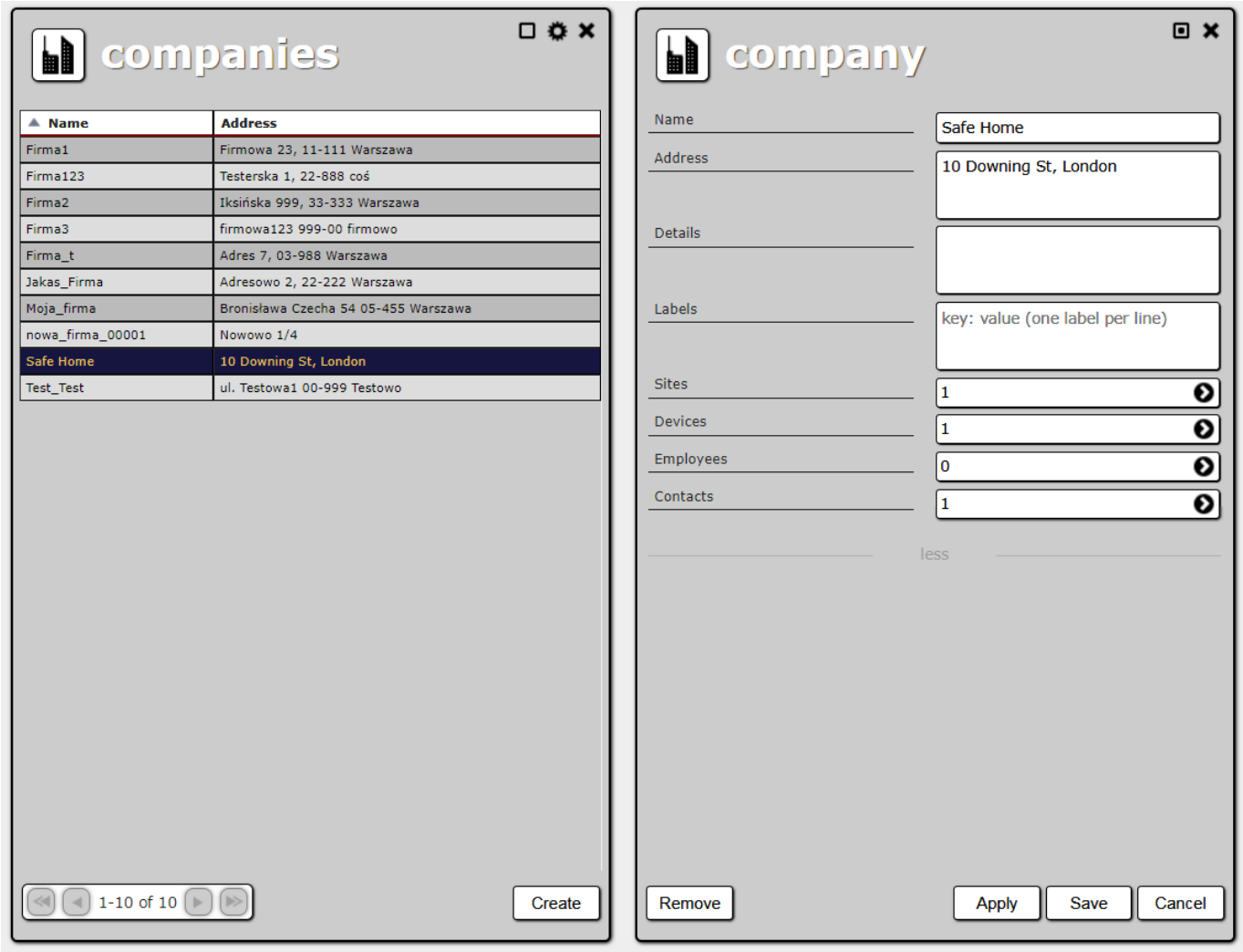
Adding a patrolled site

One of the main functions of ActiveView is the verification of guard patrols. To use it, you have to define a patrol route.

Adding a company

Patrol routes are associated with sites. So first you need to set up data like the company, site and so on.

Go to *Management → Companies* where you will be able to create a company representing your client. Choose *Create* and set the company name. You can also fill in its address and additional information (details). Now choose *Save*.

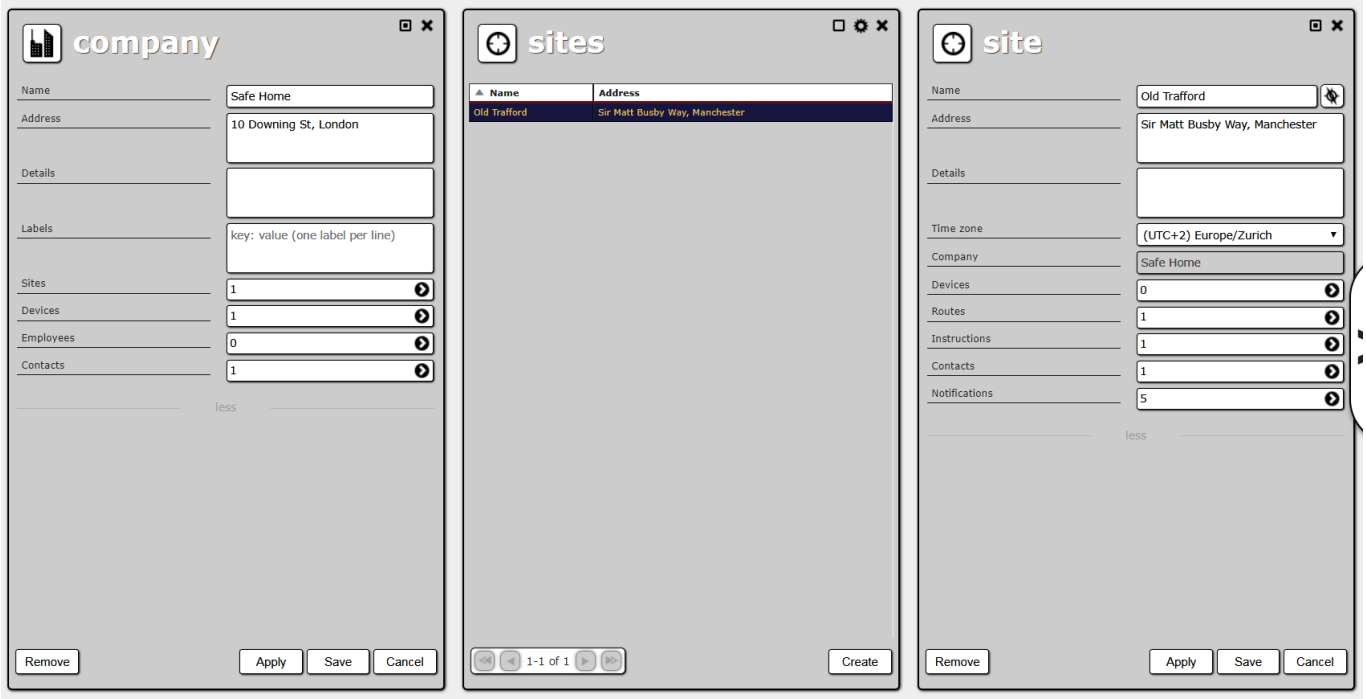


This is an example of creating an object in ActiveView. You open a **list** and choose *Create* in the bottom right corner. Then, in a ***new panel***, you fill in the details (some of them are mandatory, some optional) and choose *Save*. This creates a new object and closes the details panel. You could also choose *Cancel*, which would close the panel without creating a new object. And you could choose *Apply*, which would create new object, but leave the details panel open.

When you open details of an existing object (try it with the company you have just created), you get the *Apply*, *Save* and *Cancel* options too. You also get a *Remove* option, which lets you remove the object. All these options are always available in the same place, at the bottom of every details panel.

Adding a site

You have created a company, now you can create your client's site. On the **company details panel**, click *Sites* and then *Create* to create a new site. Fill in the name and address (optional) and save changes.



The next step is to link your device to the client's site. Open your **ActiveGuard's details** (*Management → Devices*) and choose the company and the site which you have created earlier.

You now have a company, a site and a device linked to them. The only thing left to define a route are

checkpoints (RFID tags).

Adding checkpoints

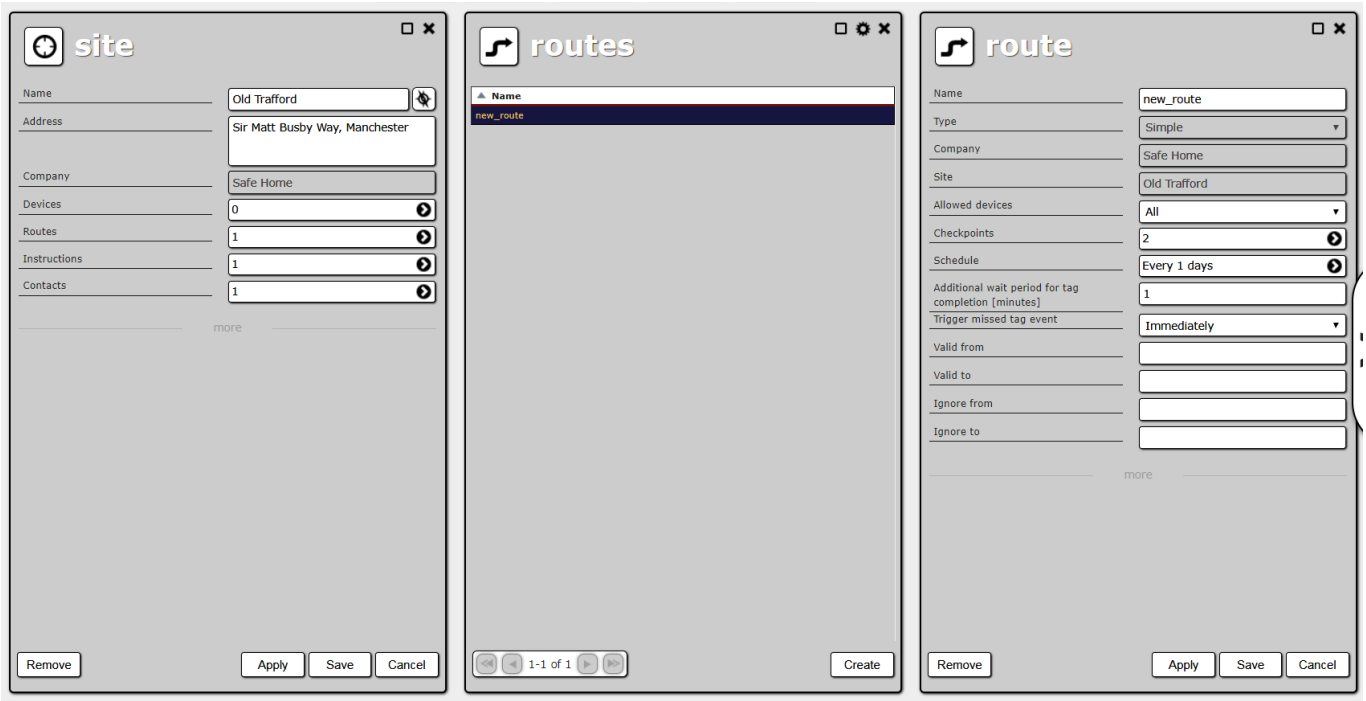
When you read a checkpoint with an ActiveGuard linked to a site, ActiveView automatically records it and connects it with the site. Try reading some checkpoints and then select *Management* → *Tags* in the main menu. Your new checkpoints should be on the list, connected with your client's site. You can open their details and change their names for convenience.

Verification of a patrol

To verify a guard patrol, you have to define a patrol route.

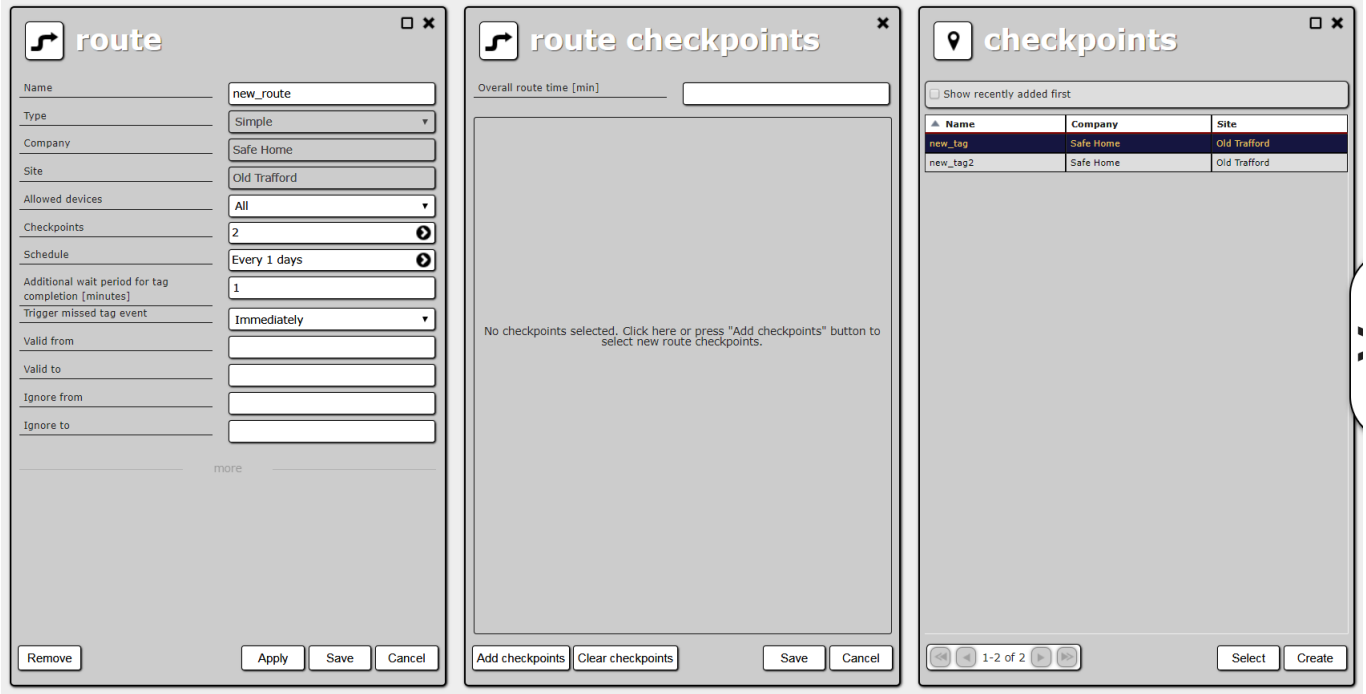
Defining a route

Open the details of your client's site. You can do it either by finding the right company (*Management* → *Companies* in the main menu), listing its sites and choosing the one you are looking for or by listing all sites (*Management* → *Sites*) and choosing it there. On the **site details panel**, click *Routes*, and then *Create*.

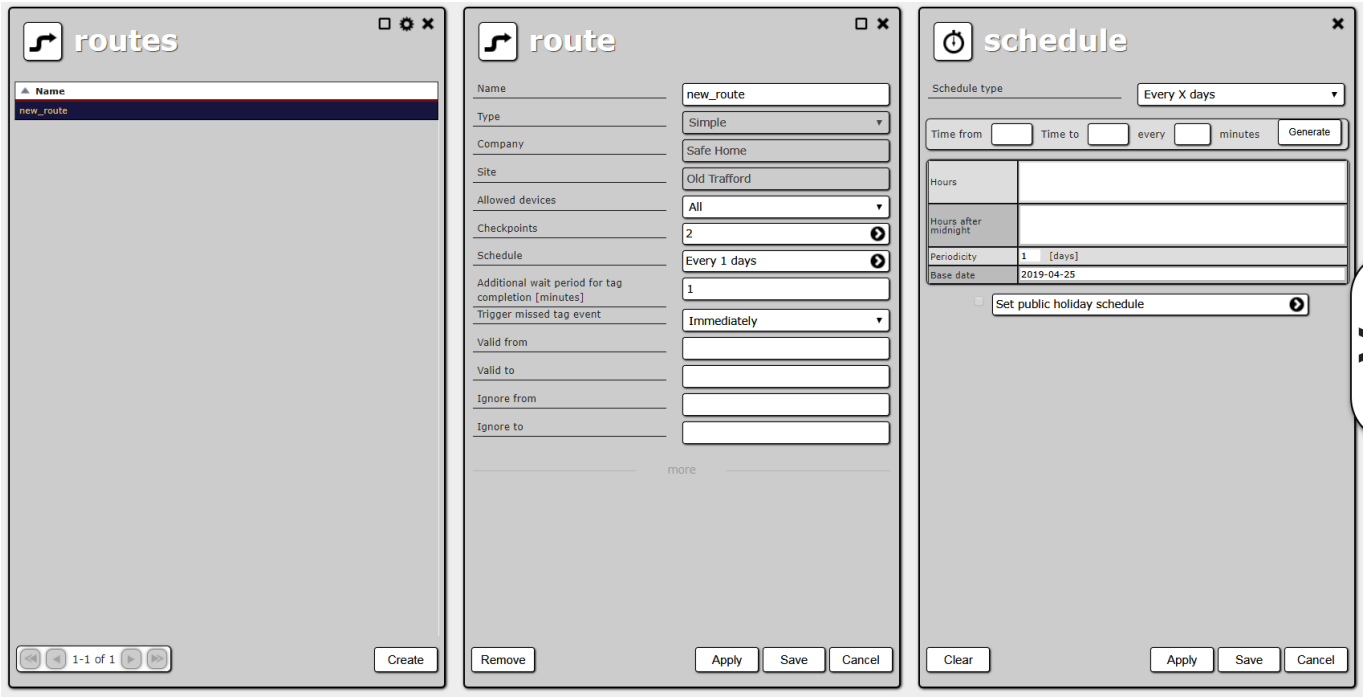


Enter a name for the route. Then click *Checkpoints* to open the **route's checkpoints list**. The default route type is a simple route (that's the one you are going to create). It means that a guard has a defined amount of time to pass all the checkpoints on the route without any particular order. First, enter the *overall route time* (route duration). Then click *Add checkpoints*, which opens a list of all

checkpoints connected to the site. You can choose more than one row by “ctrl clicking” it. After you have made the selection, choose *Select*.

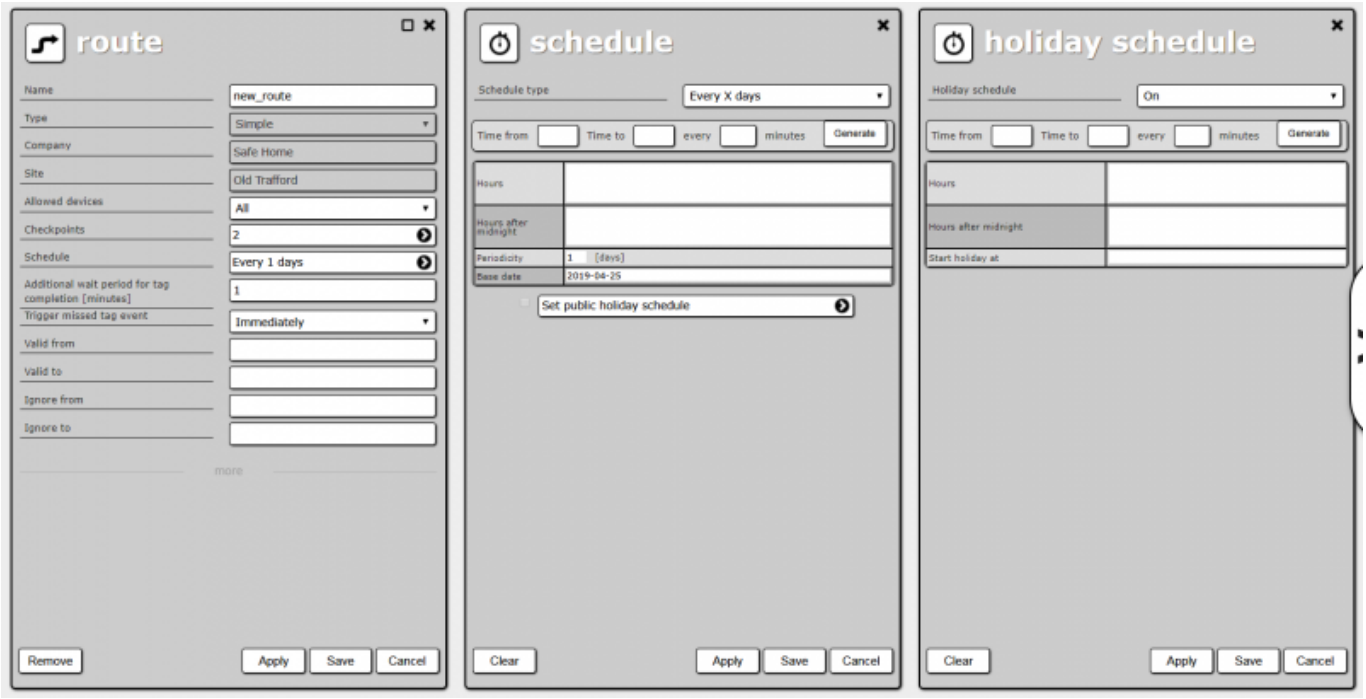


Now choose *Save* on the **route checkpoints panel**. You have defined what a single patrol looks like. The next step is to tell ActiveView when guards should perform patrols, i.e. define a schedule. To do this, click *Schedule* on the **route details panel**.



The default schedule type is “every X days”. It means that, depending on the periodicity, guards patrol a site every day, every second day and so on. On days when they do, patrols start at times you define (e.g. at 9 am, at 1 pm and at 5 pm). For your first route, you can leave the default *periodicity* and the *base date* of the schedule. You only need to fill in the *hours* list (it understands a 24-hour clock, times separated by semicolons, for example: 11:30; 13:30; 15:30). Next choose *Save* on the

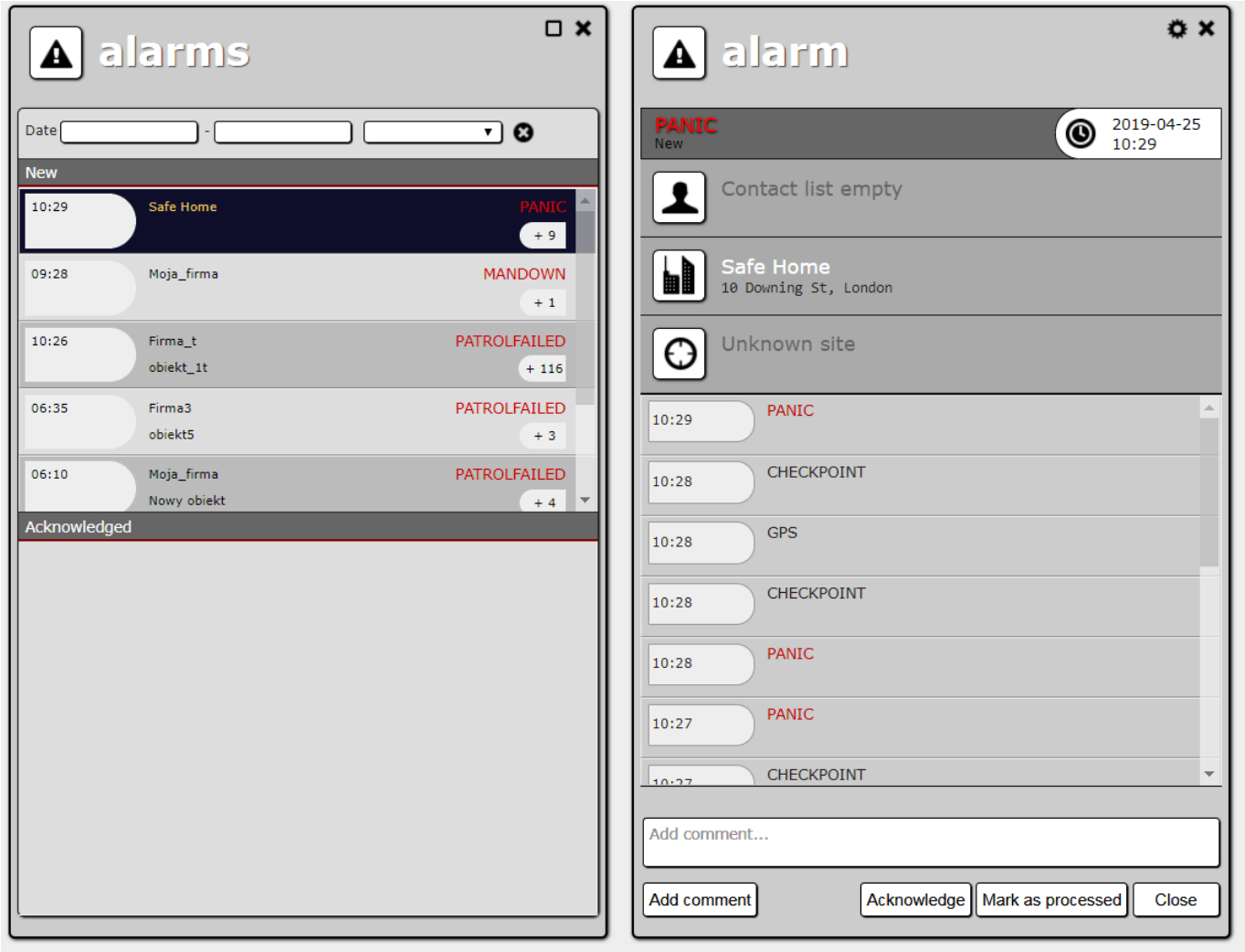
schedule panel. You have named your route, chosen checkpoints and schedule, and then select *Save* on the schedule panel.



Additionally, there is a *form for holidays* (both for weekdays and every X days). The user can define the start time of the *holiday* in the path (the holiday lasts 24 hours). The holiday form opens together with the main form, if holidays are active in this path, activation / deactivation of holidays is performed on the main form.

Looking for alarms

Open the **Alarms panel** (*Alarms* in the main menu). Wait until a patrol starts (it depends on the schedule you have defined). After the route's duration, if the guard has not passed all checkpoints on the route, an alarm pops up.



These were the basics of ActiveView. Read the rest of the documentation to learn about all functionalities, including alarm handling, e-mail and text message notifications, reports, administration and more.

Configuring the device

An Active Track device can be configured in two ways: by using a set of AGP3 cables or by sending text message to the device's card number.

You can watch the video presenting how to configure the Active Track device:

How to configure the Active Track device

Upload device setting by mobile phone

Insert SIM card without PIN CODE to charged device then send text to it.

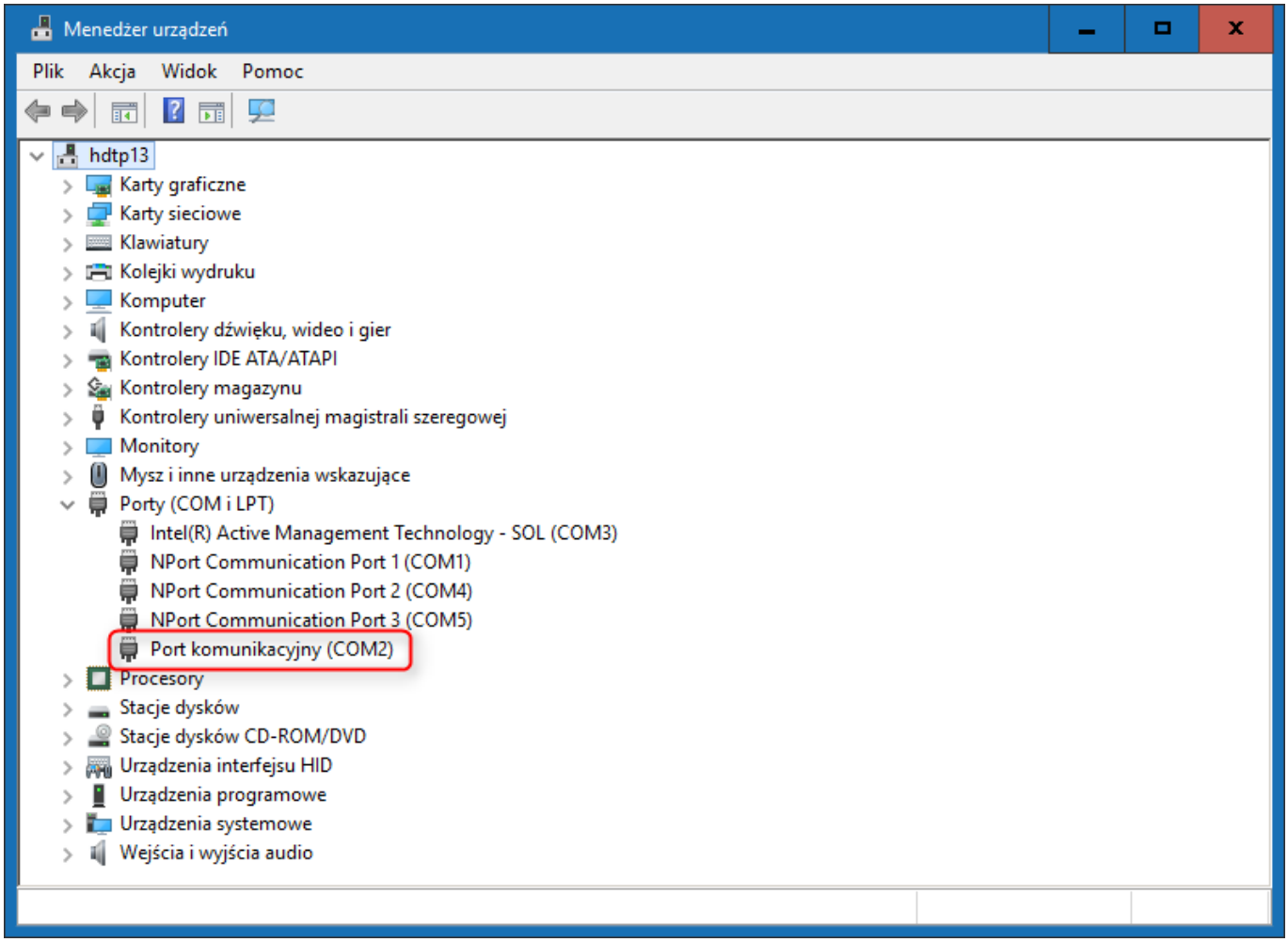
Example of message: **1111 SERVER=94.42.165.180 PORT=7407 APN=internet KILL**

NOTE: APN depends on GSM provider. SIM card must have credit to connect server by GPRS.

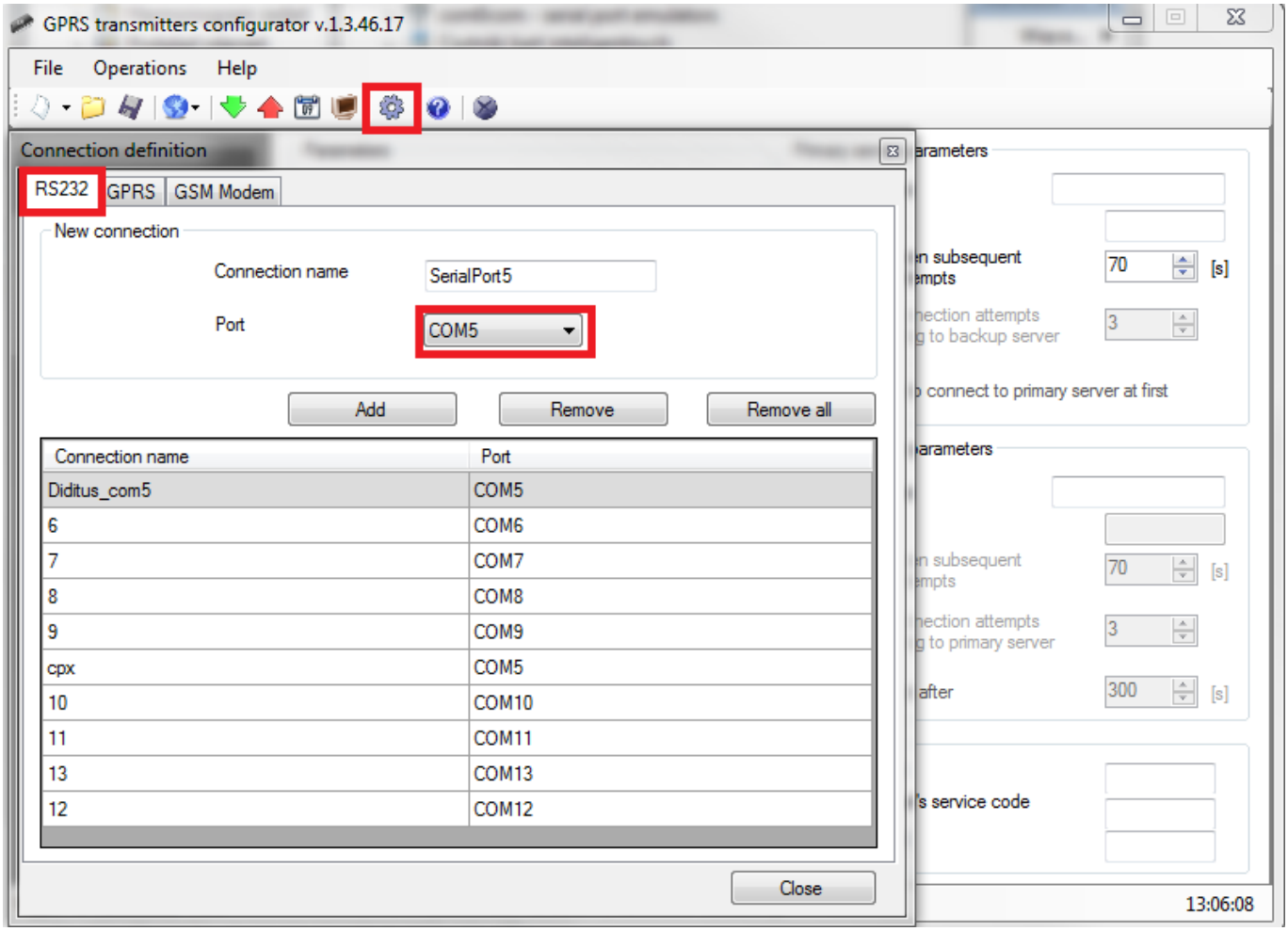
Upload setting by GPRS transmitter configurator

- In order to configure a transmitter using the GPRS Transmitter Configurator, please download the program from the website, after registering: http://www.ebssmart.com.
- Link device to PC like below. Panic button should flashing. Use AGP3 set plus RS232/USB adapter.

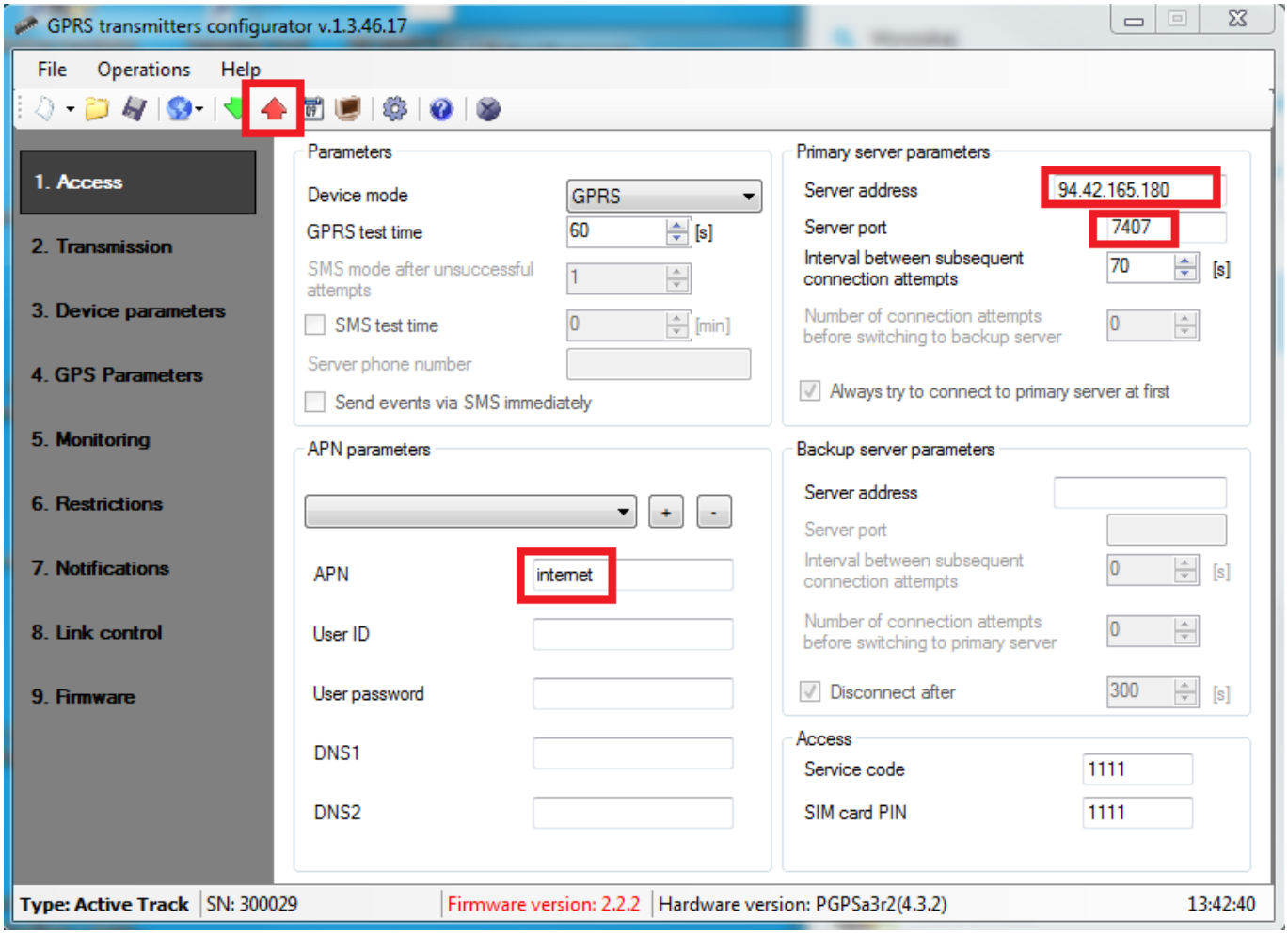
- Find the Serial Port number.



- Set up the Serial Port in GPRS transmitter configurator.



- File out the Server address, Port and APN then press red arrow.



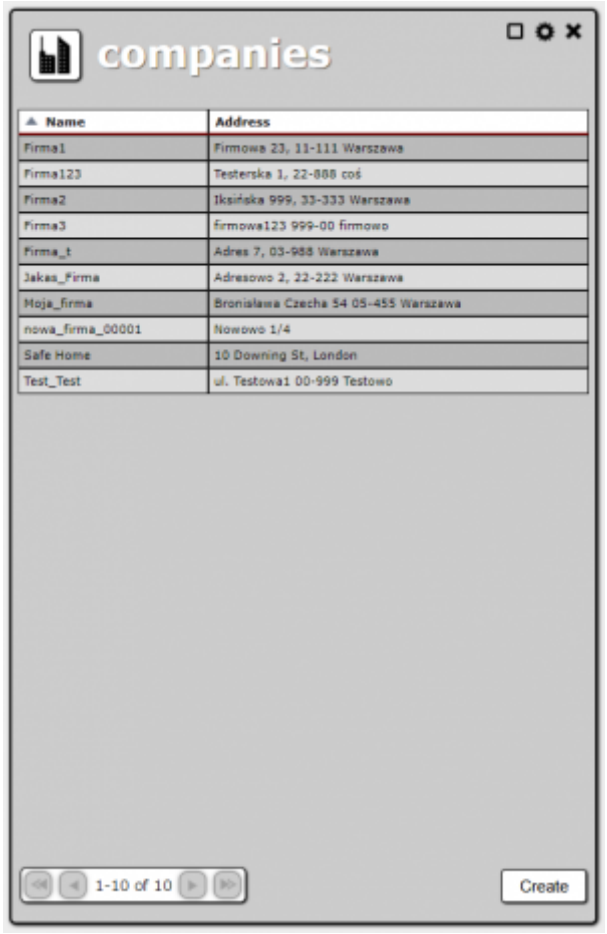
- Unplug adapter with cable. Insert SIM card. Remember to change PIN Code or remove it.

We configure Active Guard device in the same way, only we set different server port - *7409*.

Application interface

The ActiveView interface consists of panels. There are two main types of panels: lists and details.

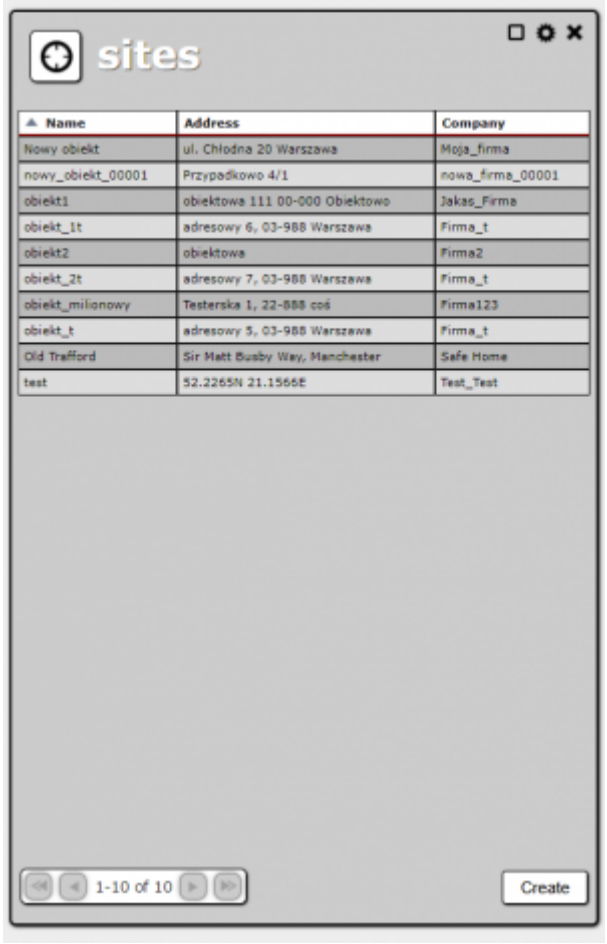
List panel



A ***list panel*** contains the following elements:

- **Rectangle icon** (top right corner): expands or compresses the panel (switches between normal and double size).
- **Cog icon** (top right corner): opens a menu with additional rarely used tools.
- **X icon** (top right corner): closes the panel.
- **List**: single click selects a row (you can use ctrl and shift keys to select more than one row); a single or double-click (depending on user settings) opens details; a click on a column heading sorts the table by that column (or switches between ascending and descending sort order).
- **"Pager"** (bottom left corner): shows the current page of the list and allows switching between pages.
- **Create button** (bottom right corner): allows creating a new item.

Details panel



A **details panel** contains the following elements:

- **Rectangle icon** (top right corner): switches between basic and full details view (i.e. shows or hides less important item details).
- **X icon** (top right corner): closes the panel without saving changes.
- **Fields with item details**: editable and read-only fields; clicking on fields with the “>” icon on the right opens the sub-details panel (e.g. a list of routes associated with a site).
- **More**/**Less**: the same as the rectangle icon.
- **Remove button**: removes the item.
- **Apply button**: saves changes without closing the details panel.
- **Save button**: saves changes and closes the details panel.
- **Cancel button**: closes the panel without saving changes (the same as the X icon).

Alarms

Alarms detected by ActiveView can be accessed through two lists:

- ***The alarms list***: consists of current (not processed) alarms and is updated automatically;
- ***The alarms browser***: allows searching for and browsing all alarms (current and processed) and is refreshed on demand.

Both lists allow selecting an alarm and opening its details.

Processing alarms is considered the most important task for the ActiveView user. Therefore, when a new alarm occurs, ActiveView notifies the user with sound and visual notifications.

Alarm life cycle

The alarms detected by ActiveView are grouped by sites which they come from. What this documentation calls an alarm is in fact a group of alarms, which occurred in succession.

An alarm is always in one of the following states:

- *new*,
- *acknowledged*,
- *processed*.

When an alarm occurs and is detected by the application, it is in the *New* state.

If another alarm from the same site occurs, it is added to the existing one. The state does not change. If, on the other hand, this new alarm is from another site, ActiveView treats it as a new alarm (it is listed as a separated item).

When a user Acknowledges an alarm (by selecting a corresponding option), its state changes to *Acknowledged*.

Now if another alarm from the same site occurs, it is again added to the existing one. This time however, the state changes back to New. These state changes (from *New* to *Acknowledged* and back) can occur any number of times.

When an alarm is in *New* or *Acknowledged* state, a user can mark it as processed (by selecting the corresponding option). The alarms state changes to Processed and cannot be changed back (this is the end of the alarm’s life cycle).

If one more alarm from the same site occurs, ActiveView treats it as a new alarm (it is listed as a separated item, in *New* state).

Alarms list

To open the **alarms panel**, select *Alarms* in the main menu.

The **alarms panel** contains the following elements:

- *Filters*: date and time of detection; alarm type. The X icon clears filters.
- *New alarms list*.
- *Acknowledged alarms list*.

Both lists are updated automatically, as soon as a new alarm is detected or alarms state changes.

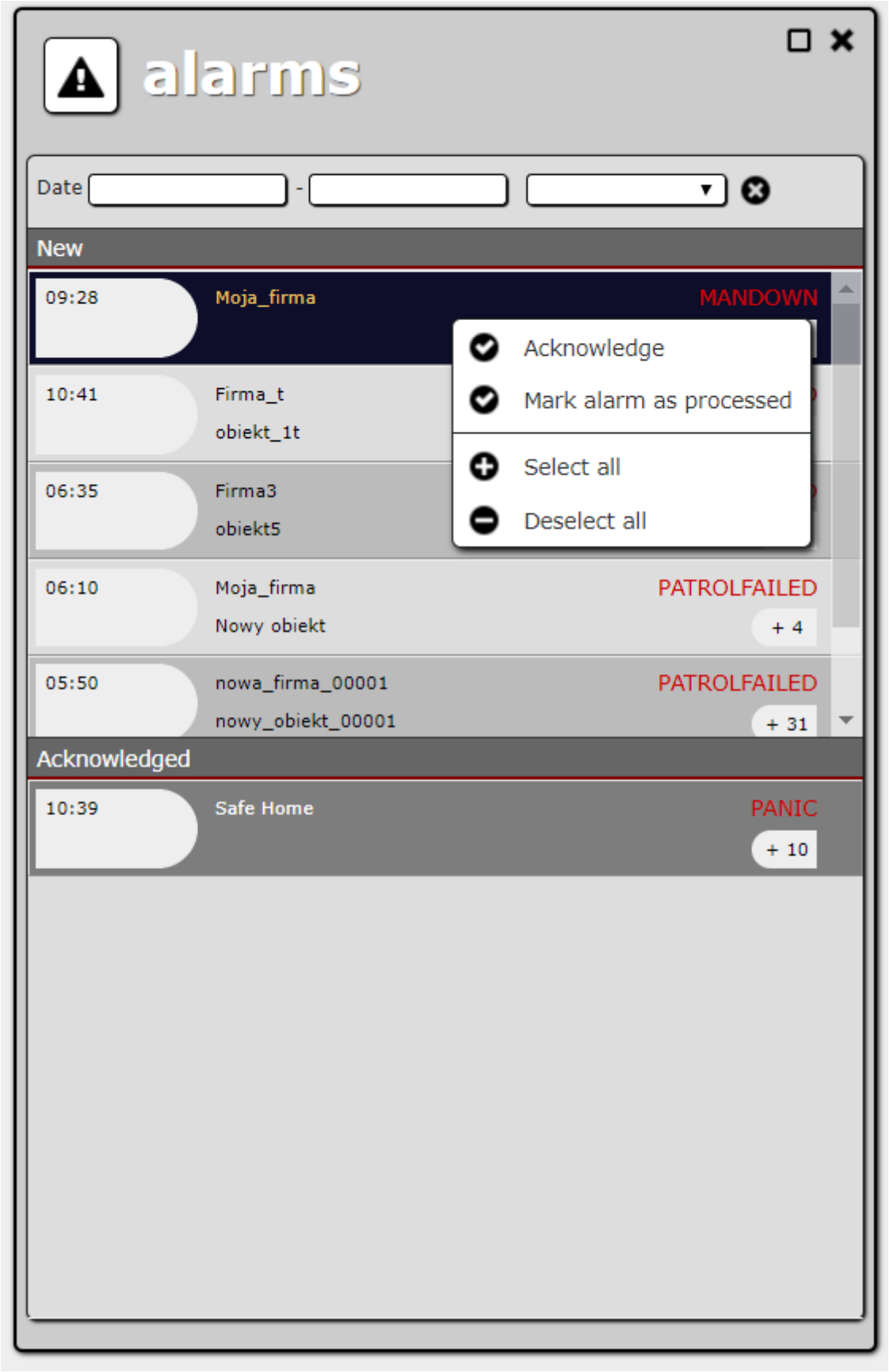
Alarms in both lists are sorted first by priority (the most important alarms at the top) and then by the time of detection by ActiveView (the oldest at the top of alarms with the same priority).

On both lists, there are the following data available for every alarm (from left to right):

- ***date and time of detection*** of the last alarm in the group (last alarm from the site);
- ***name of the company*** which the site belongs to;
- ***name of the site*** where alarms occurred;
- ***type*** of the most important alarm in the group (i.e. the most important not processed alarm from the site);
- ***number*** of other alarms grouped with it (i.e. other not processed alarms from the site).

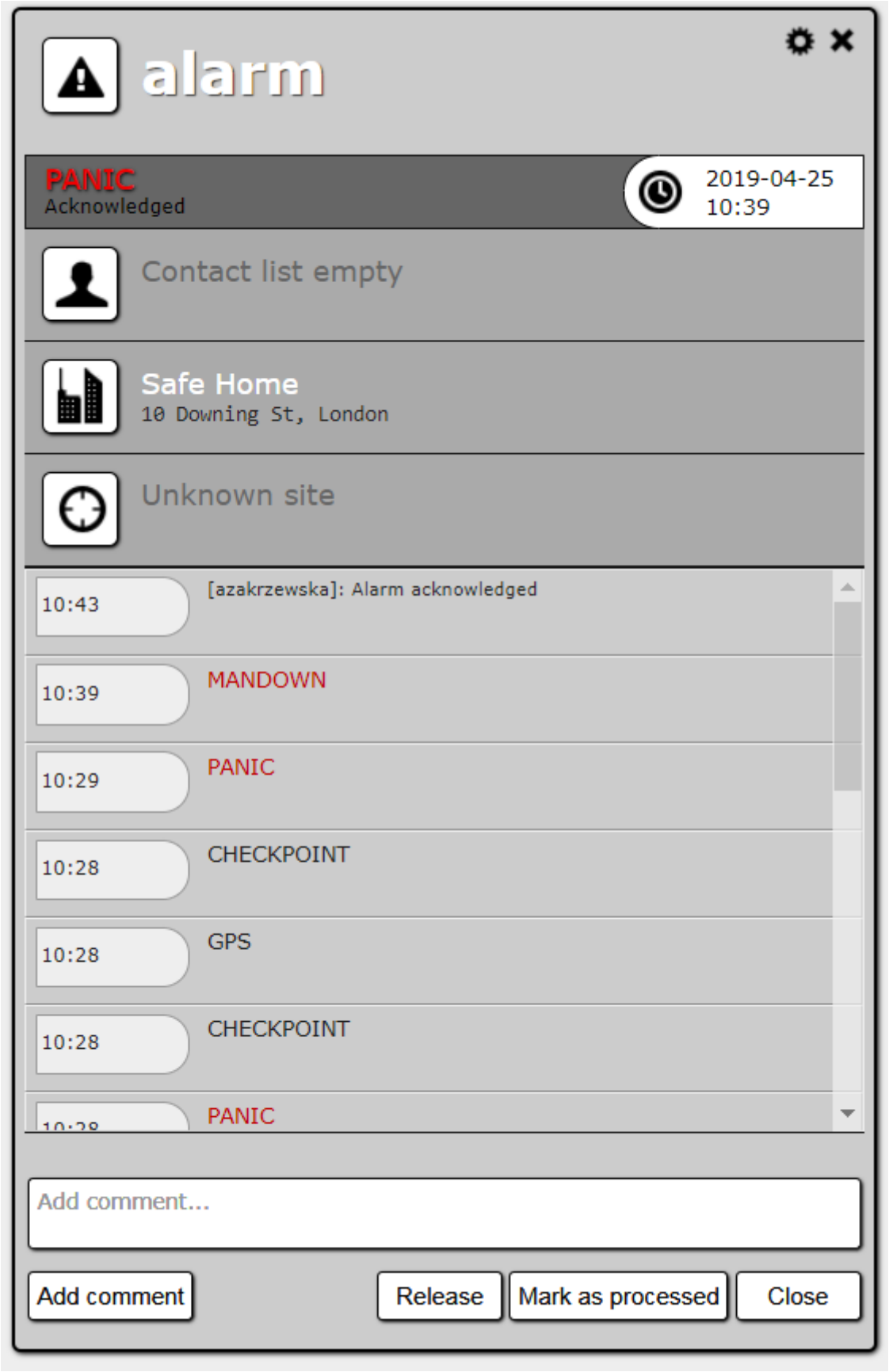
On the alarms lists, there is a context menu for an alarm available. It contains the following options:

- **Acknowledge**: the same as Acknowledge option in alarm details (see below); acts on all selected alarms (possibly more than one).
- **Mark alarm as processed**: the same as Mark as processed option in alarm details (see below); acts on all selected alarms (possibly more than one).
- **Select all**: selects all alarms in a list (new and acknowledged separately).
- **Deselect all**: deselects all alarms in a list (new and acknowledged separately).



Alarm details

The **alarm details view** contains detailed information about the alarm. It also allows performing the actions associated with it.



The **alarm details panel** contains the following elements:

- **Type** of the most important alarm in the group (i.e. the most important not processed alarm from the site). The tooltip for the alarm type contains the ID of the alarm.
- **State** of the alarm.
- **Date and time of detection** of the last alarm in the group (last alarm from the site).

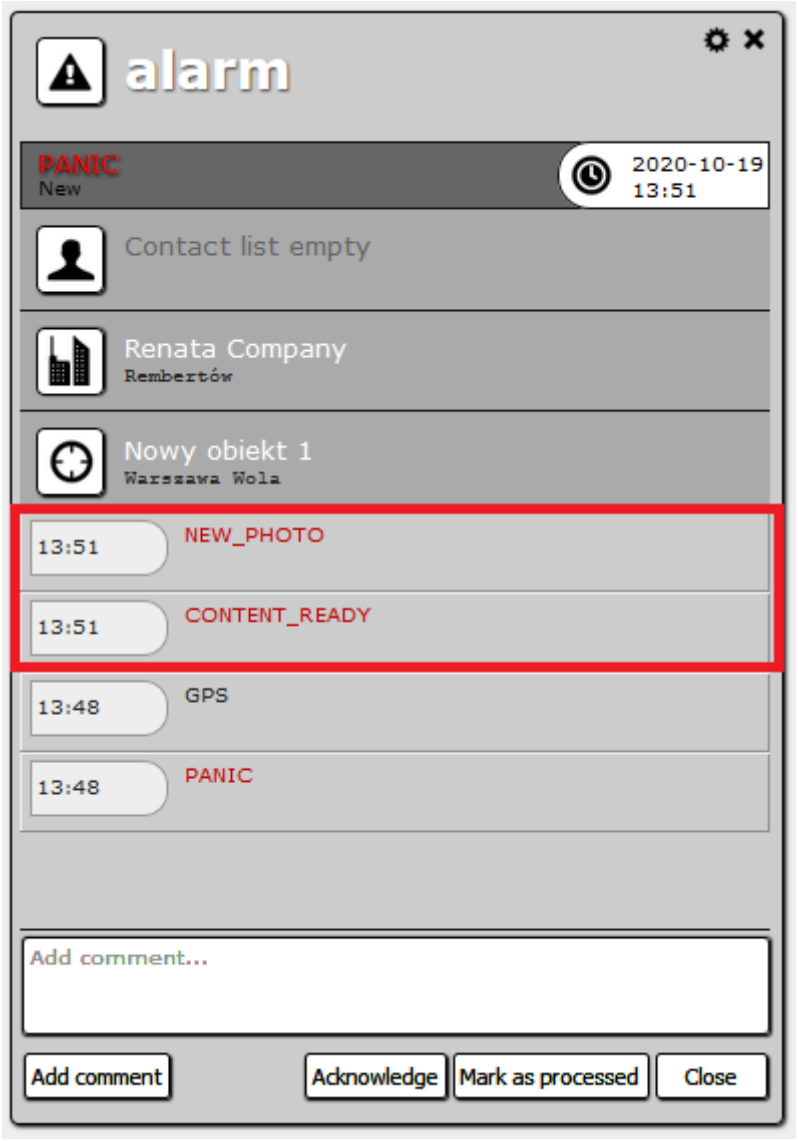
- **Site contacts**: the most important site contacts name and phone number are visible. There are two icons on the right:
  - **down arrow**: shows additional contact details;
  - **right arrow**: shows next contact linked to the site.
- **Company name and address**.
- **Site name and address**. Clicking on a site name displays its details panel in read-only mode. From this panel you can, for example, see instructions and people connected to this site.
- **List of not processed alarms** from the site and other events which occurred since the first visible alarm (sorted by detection date and time in descending order). Clicking on a row expands its details (e.g. the device from which the alarm signal came).
- **Comment** text field (only New and Acknowledged alarms).
- **Action buttons** at the bottom of the panel.

The following actions are available:

- ***Add comment*** (only *New* and *Acknowledged* alarms): adds the text from the comment text field as an alarm comment (user note). The comment is preceded by the name of the user who added it.
- ***Acknowledge*** (only *New* alarms): changes the state of the alarm to *Acknowledged*. A note "[user] Alarm acknowledged" is added to the alarm history.
- ***Mark as processed*** (only *New* and *Acknowledged* alarms): changes the state of the alarm to *Processed*. A note "[user] Alarm marked as processed" is added to the alarm history.
- ***Close***: closes the panel.
- ***Switch time zone***: to switch the time zone, click the date and time of alarm detection or choose a corresponding option from the additional options menu under the cog icon (in the upper right corner of the panel). This switches time presentation between local time zone (set in user settings) and site time zone.
- ***Send text message***: to send a text message, click the phone number of a contact person. The *"send text message"* dialog box appears. There is a predefined message the user can change. The character counter shows the number of messages to be sent (in brackets) and characters left until there will be one more message needed. After the message is sent, a note with its contents is added to the alarm history.
- ***Send e-mail***: to send an e-mail, click on an e-mail address of a contact person. It will create a new message in your default e-mail client, addressed to the contact person.

Displaying photographs from the AT Mobile application

If the user of the AT Mobile mobile application has sent a report with a photograph and a comment, covered with a selected type, then after entering the "Alarm details" view, two new events will appear on the list: ***NEW_PHOTO*** and ***CONTENT_READY***.

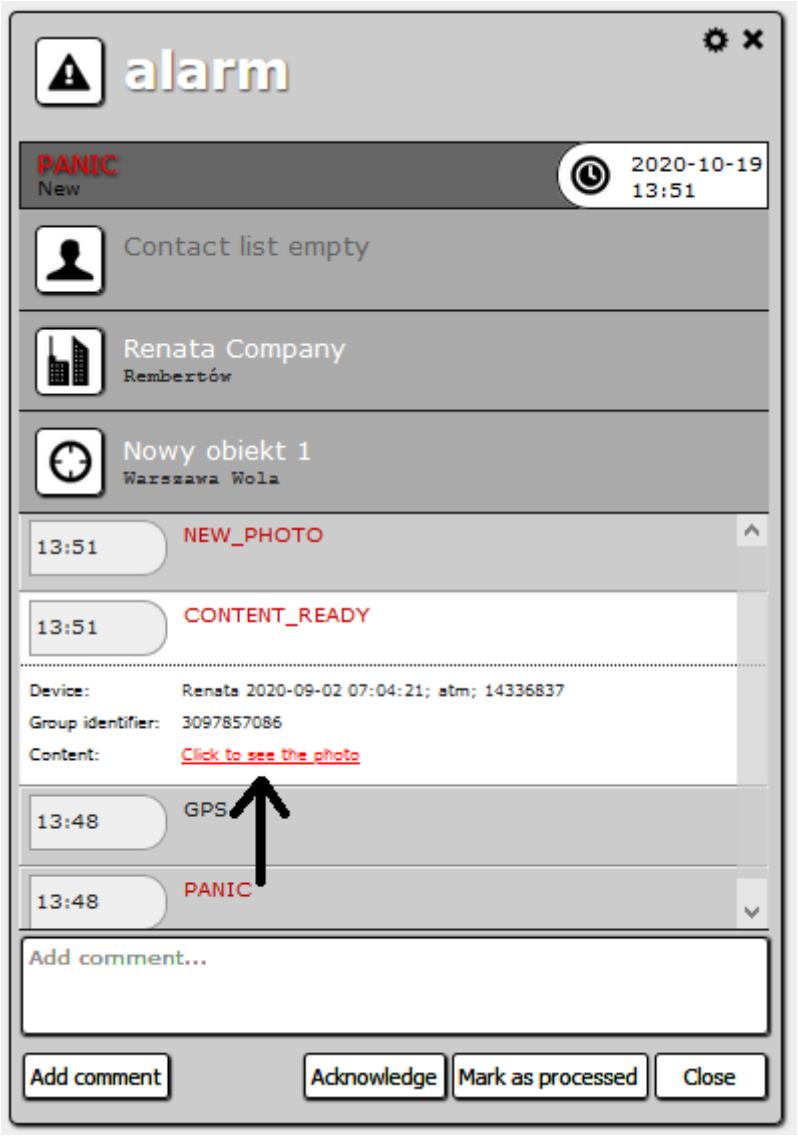


After clicking on NEW_PHOTO, the list with detailed information on the report from the mobile application will open.

- Device - device name and type;
- Reason - type of alarm indicating the reason for the sent report; available types: ALARM, ALARM COMMENT, OBJECT DAMAGE, EQUIPMENT DAMAGE, PATROL PROBLEM, PATROL NOTIFICATION, PATROL TASK, ADDITIONAL TASK, MANDATORY TASK, OTHER);
- Media type;

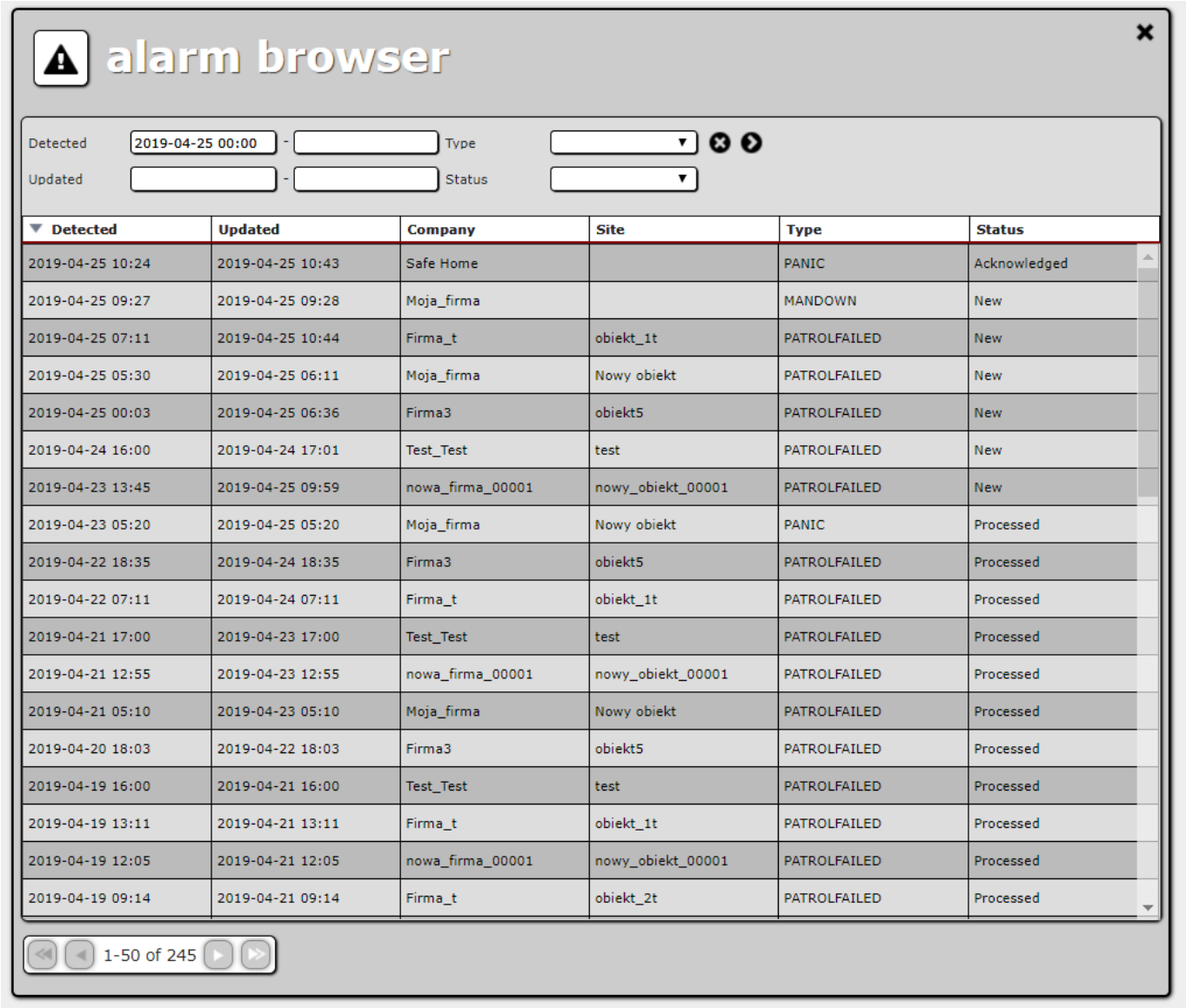
- Group identifier;
- Group size;
- Comment - the text of the comment added to the report in the AT Mobile application;

After clicking the *CONTENT_READY* button to open the list, where, apart from the device name and type and the identification number in the *Content* item, a link will be available to display the photograph. Clicking on *Click to see the photo* will display a photograph taken from the AT Mobile mobile app on the right.



Alarms browser

To open the **alarms browser panel**, select the *Alarms browser* under the *Alarms* tab in the main menu.



Detected	Updated	Company	Site	Type	Status
2019-04-25 10:24	2019-04-25 10:43	Safe Home		PANIC	Acknowledged
2019-04-25 09:27	2019-04-25 09:28	Moja_firma		MANDOWN	New
2019-04-25 07:11	2019-04-25 10:44	Firma_t	obiekt_1t	PATROLFAILED	New
2019-04-25 05:30	2019-04-25 06:11	Moja_firma	Nowy obiekt	PATROLFAILED	New
2019-04-25 00:03	2019-04-25 06:36	Firma3	obiekt5	PATROLFAILED	New
2019-04-24 16:00	2019-04-24 17:01	Test_Test	test	PATROLFAILED	New
2019-04-23 13:45	2019-04-25 09:59	nowa_firma_00001	nowy_obiekt_00001	PATROLFAILED	New
2019-04-23 05:20	2019-04-25 05:20	Moja_firma	Nowy obiekt	PANIC	Processed
2019-04-22 18:35	2019-04-24 18:35	Firma3	obiekt5	PATROLFAILED	Processed
2019-04-22 07:11	2019-04-24 07:11	Firma_t	obiekt_1t	PATROLFAILED	Processed
2019-04-21 17:00	2019-04-23 17:00	Test_Test	test	PATROLFAILED	Processed
2019-04-21 12:55	2019-04-23 12:55	nowa_firma_00001	nowy_obiekt_00001	PATROLFAILED	Processed
2019-04-21 05:10	2019-04-23 05:10	Moja_firma	Nowy obiekt	PATROLFAILED	Processed
2019-04-20 18:03	2019-04-22 18:03	Firma3	obiekt5	PATROLFAILED	Processed
2019-04-19 16:00	2019-04-21 16:00	Test_Test	test	PATROLFAILED	Processed
2019-04-19 13:11	2019-04-21 13:11	Firma_t	obiekt_1t	PATROLFAILED	Processed
2019-04-19 12:05	2019-04-21 12:05	nowa_firma_00001	nowy_obiekt_00001	PATROLFAILED	Processed
2019-04-19 09:14	2019-04-21 09:14	Firma_t	obiekt_2t	PATROLFAILED	Processed

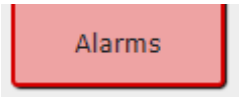
Alarms in the browser can be searched by the following criteria:

- *date and time of detection by ActiveView*;
- *date and time of the last update*;
- *alarm type*;
- *alarm status*.

The **>** button executes the search. The **X** button clears the search criteria.

Alarm notifications

ActiveView notifies the user about alarms in two ways. It changes the appearance of the *Alarm tab* in the main menu and it plays sounds.



Both notification types have two stages: subtle and full.

Subtle notification means that:

- *visual*: the Alarms tab has a red background.
- *sound*: an alarming sound is played once.

Full notification means that:

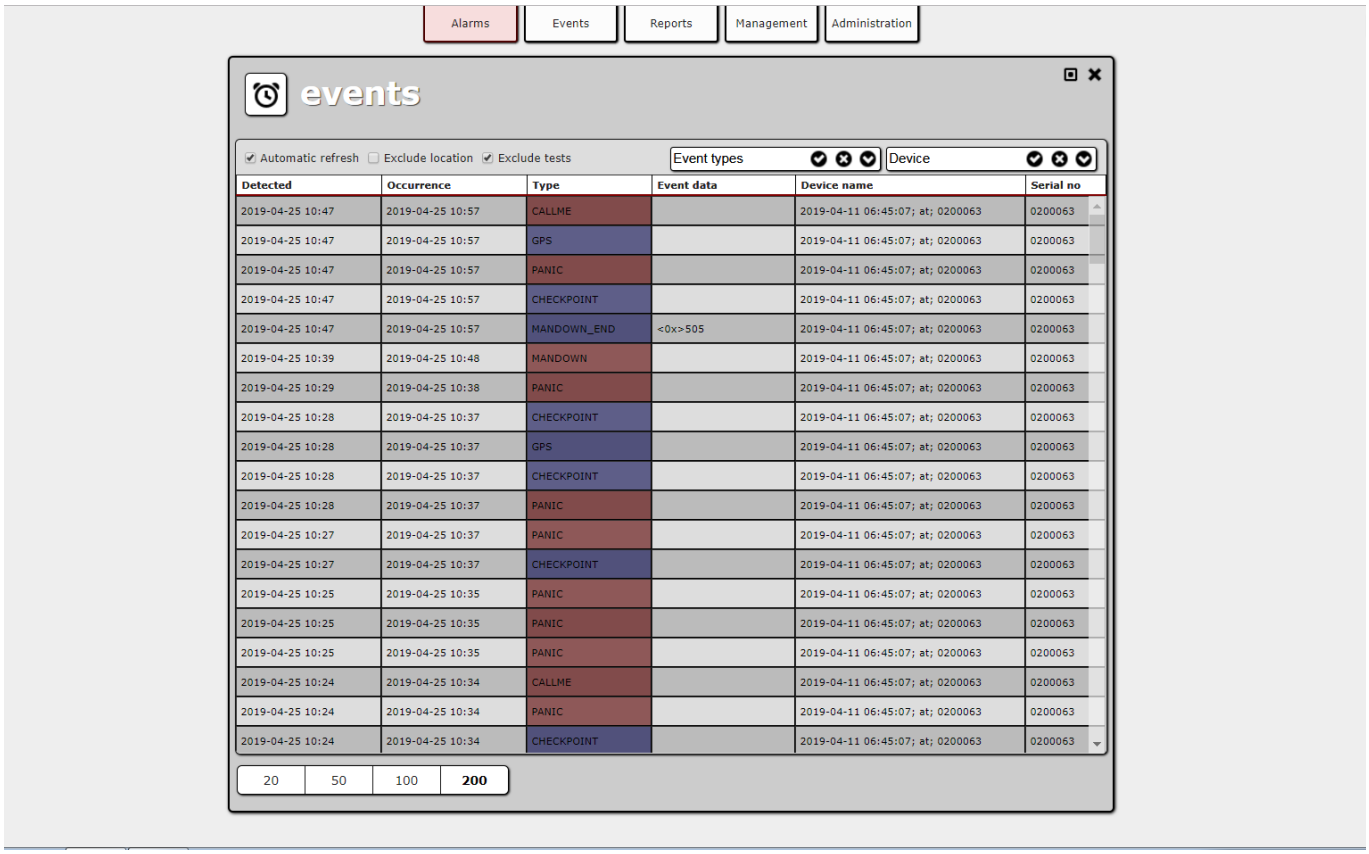
- *visual*: the Alarms tab has a red background and is blinking.
- *sound*: an alarming sound is played constantly.

Alarm notification follows the following rules:

- any *New* alarms exist – **full visual notification**;
- any *Acknowledged* alarms exist, but no *New* – **subtle visual notification**;
- any *New* or *Acknowledged* alarms exist; the alarms list or alarm details are open (visible) – **subtle sound notification**;
- any *New* or *Acknowledged alarms exist*; the alarms list or alarm details are not open (not visible) or there has been no activity in the application for some time – **full sound notification**.

Events

ActiveView receives different types of events from connected devices. If you need to verify that the application receives the events it is supposed to, you can use the **events list**. To open it, choose *Events* from the main menu.



Event types are distinguished with colours:

- ***grey*** – technical events (TEST, LOCATION, DISC);
- ***red*** – alarm events (events with ALARM role; see OSM events configuration for details);
- ***blue*** – other events.

For every event, two times are presented:

- ***Detected*** – date and time of the event detection by ActiveView;
- ***Occurrence*** – date and time of the event occurrence, recorded by the device.

The former can be later, if the communication between the device and ActiveView was interrupted.

Event data column contains information about additional data send by ActiveView. For *READ* events this column displays name of the read tag. For the remaining events, additional data is decoded from HEX to ASCII format. Only printable ASCII chars are presented. For example **48656c6c6f00776f726c6421** is displayed as **Hello<00>world!**, because **00** is not printable.

Above the list, there is the **Automatic refresh checkbox**. If checked, the list is updated

automatically, whenever a new event occurs. If not, it is not updated at all.

The list shows the last 20, 50, 100 or 200 events (depending on the user's choice).

There are the following filter options available:

- ***Exclude location*** – *LOCATION* events are not listed.
- ***Exclude tests*** – *TEST* events are not listed.
- ***Event types*** – if any event types are selected in the list, only these are listed. If there are no event types selected, all are listed.

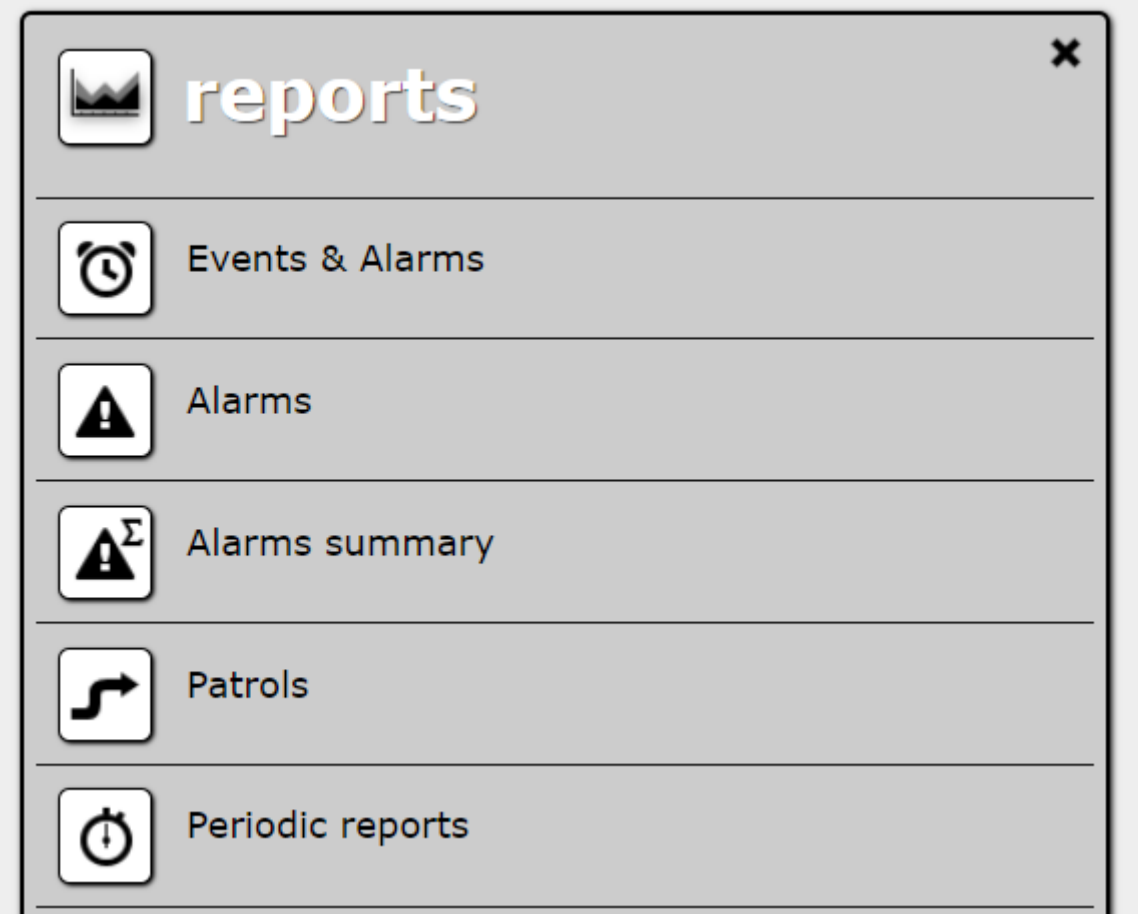
NOTE: If there have been only few events of the selected types recently, it is possible that the list is shorter than the selected 20, 50, 100 or 200 rows (it can even be empty).

There is a context menu for an event available, with two options:

- **Show device** – opens the details of the device which has sent the event.
- **Show tag** [only for *READ* events] – opens the details of the read *RFID* tag.

Reports

Historical information about alarms, patrols and other events is available in the form of reports. To open available reports list, choose *Reports* from the main menu.



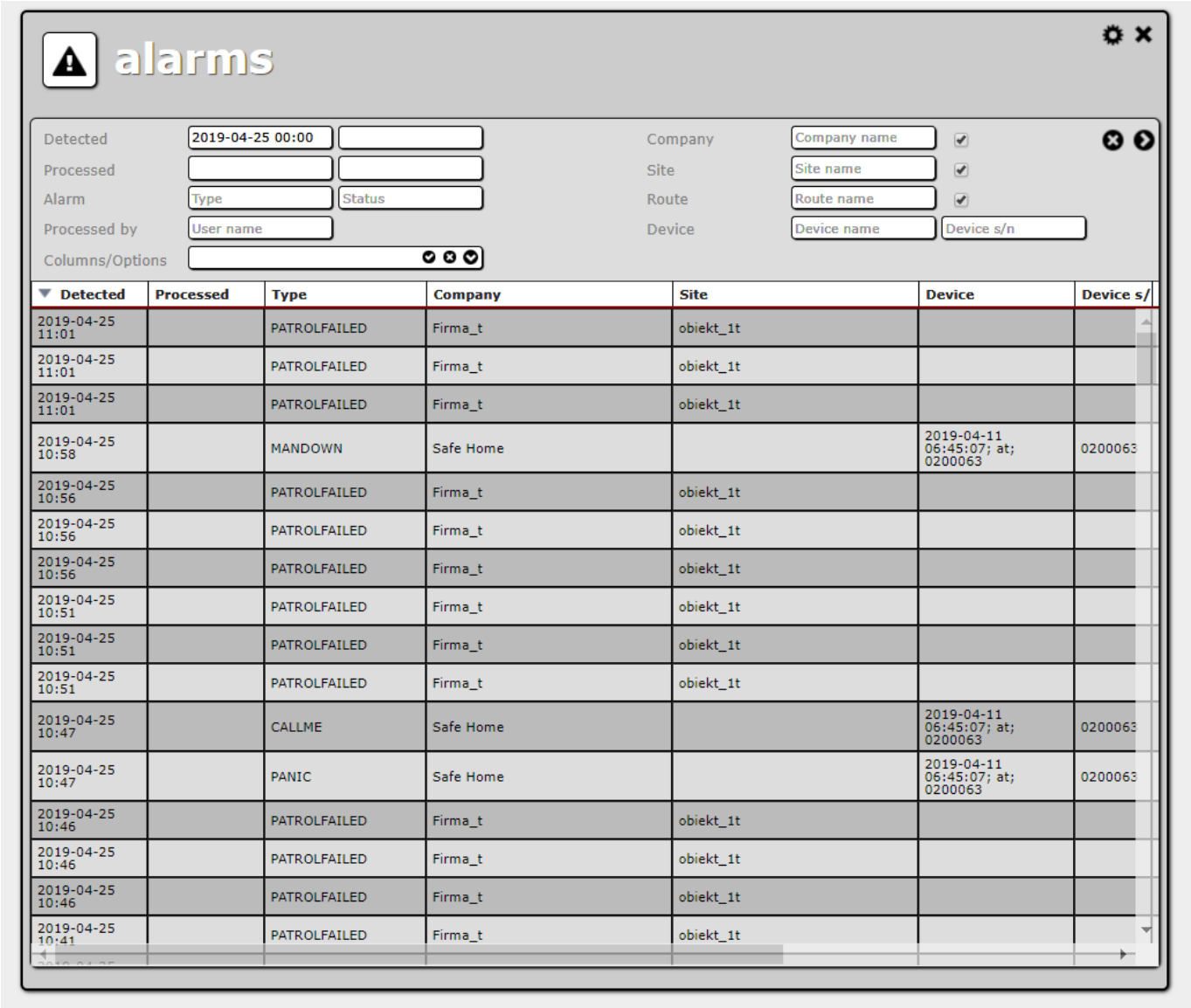
There are the following report types:

- *Events and Alarms*,
- *Alarms*,
- *Alarms summary*,
- *Patrols*.

Each report type can be generated on demand on the screen, in a printable format or to a *CSV* file. Reports can also be generated automatically and sent by e-mail periodically.

Basic report features

Choosing a report from the reports panel opens a new panel with this report.



Every **report panel** contains filters (search criteria) and a table with report results.

To generate a report with data meeting the pre-set criteria, click the **>** button. To clear criteria, click the **X** button.

Reports displayed on screen or generated in a printable format have a 1,000 record limit. It means only the first 1,000 records meeting the criteria are shown. The limit does not apply to *CSV* files, which always contain full results.

Like other lists, report results can be sorted by every column. Clicking a column heading sorts table by that column or switches between ascending and descending sort order.

To generate the report in a printable format or in a *CSV* file (i.e. export the report), choose the relevant option in the tools menu under the **cog icon** (in the upper right corner). There are two export options:

- ***Print***: contains the same data as the list on the screen, only the style is adjusted to printing.
- ***Export to CSV***: the generated *CSV* file includes all visible columns and id columns for entities such as companies, sites, routes, etc. and is not limited to 1,000 records.

Events and alarms report

This report contains all significant events which had happened in the system. They can be divided into the following categories:

- ***Informational events:***
  - events received from ActiveGuards, ActiveTracks and other connected devices (excluding *TEST* and *LOCATION* events);
  - patrol events such as *PATROL_FINISHED*, *TAG_COMPLETED*;
  - workplace entry and exit events.
- ***Alarm events:***
  - alarms such as *PANIC*, received from ActiveGuards, ActiveTracks and other connected devices;
  - Patrol failed alarm, generated by ActiveView based on user-defined routes;
  - alarms caused by reading an alarm TAG.
- ***Events from the AT Mobile application:***
  - Apart from having functionalities in close solutions such as Active Track or Active Guard, the AT Mobile application enables sending a report containing a photograph and a comment. The last column in the *NEW_PHOTO* item contains the comment text attached to the report, while the item *CONTENT_READY* contains the photograph. To display them, double-click left mouse button on the event or right-click and select Show photo. A photograph from the AT Mobile application will be displayed on the right.

The events and alarms report has the following columns:

- *Detected* – date and time when the event/alarm was received/detected by the system.
- *Occurrence* – date and time of the event/alarm occurrence.
- *Type* – type of the event/alarm.
- *Device, Device s/n* – device name and serial number. **NOTE**: Empty for patrol events/alarms which are not associated with any particular device (all but *TAG_COMPLETED*).
- *Company* – company name. **NOTE**: Empty if the event/alarm comes from a device not associated with any company.
- *Site* – site name. **NOTE**: Empty if the event/alarm comes from a device not associated with any site.
- *Route* – route name. **NOTE**: Filled only for events/alarms associated with patrols.
- *Tag* - tag name. **NOTE**: Filled in only for patrol events/alarms
- *Guard name* – guard name. **NOTE**: Filled only for events/alarms generated by a TAG read with a device linked to a guard.
- *Employee name* – employee name. **NOTE**: Filled only for workplace entry and exit events.
- *Alarm Group* – if the event is connected to a site (e.g. comes from a device linked to a site) and there was an alarm on the site, when the event was detected, Alarm group is the ID of that alarm.
- *Comment* – a comment to an alarm. **NOTE**: Filled only for *COMMENT_ADDED* events.

When a filter is defined (i.e. a search criterion for a column is set), records with a corresponding column empty will not be returned.

ActiveTrack devices add position information to some of the events they send. This information is available in the *CSV* format of the *Events and alarms report*. There is also an additional option in the tools menu (under the cog icon), to show the currently listed events on a map. It opens a new browser window with the trace of the device marked. All events form a single trace, so you should use the *Device filter* in order to get meaningful results.

NOTE: Devices connected to ActiveView regularly send technical events, such as *TEST*. The events

are not listed in the *Events and alarms report* by default. In the case of ActiveTrack devices, these events can contain position information. In particular, there is the *LOCATION* technical event, which only purpose is to inform ActiveView about the device's position. If you want these events in the *Events and alarms report* (i.e. to be able to see them on a map), ask your ActiveView administrator.

Alarms report

This report aggregates basic information about alarms.

The alarms report has the following columns:

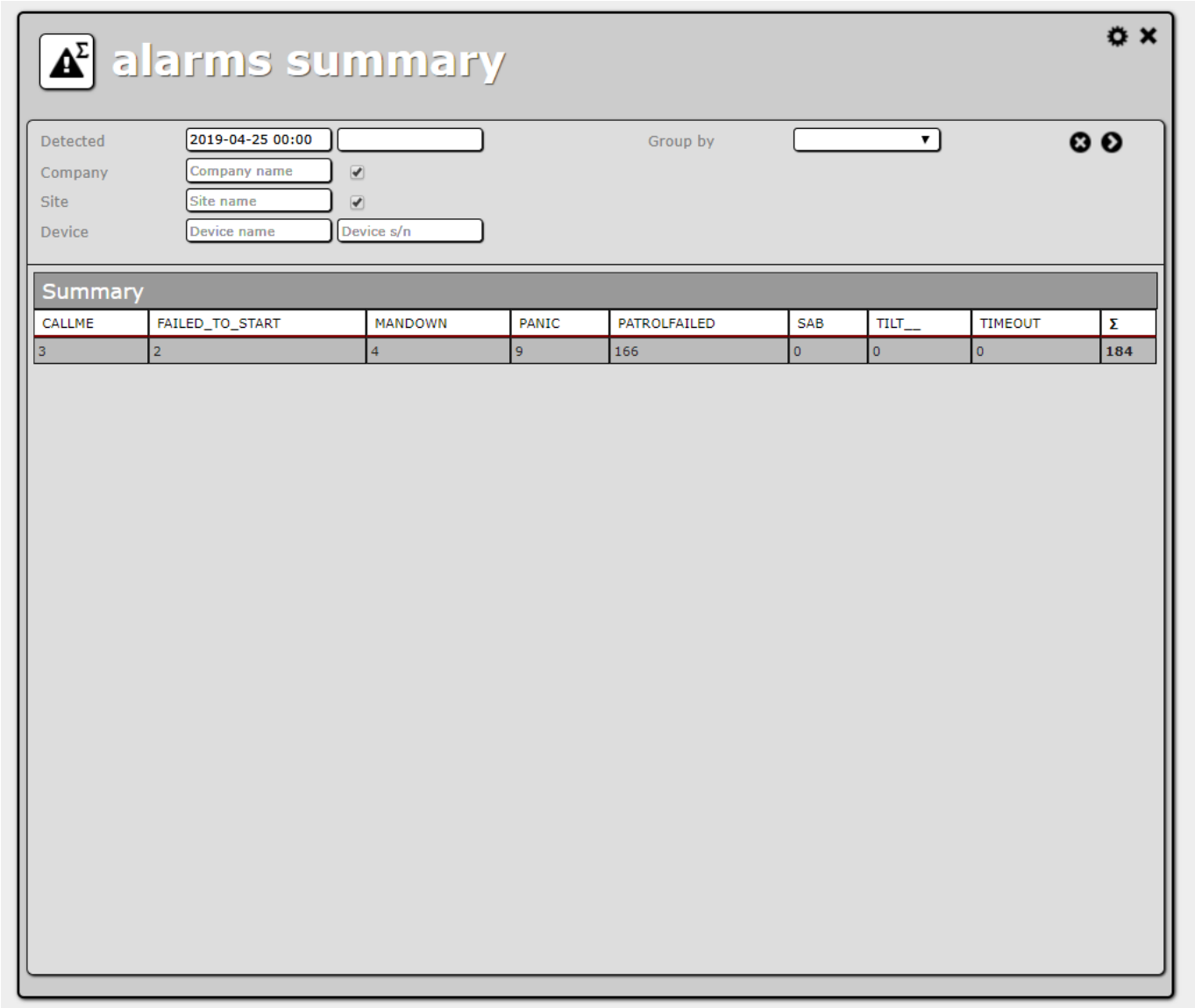
- *Detected* – date and time when the alarm was detected by the system.
- *Processed* – date and time when the alarm was processed. **NOTE**: Empty if it has not been processed yet.
- *Type* – type of the alarm.
- *Company* – company name. **NOTE**: Empty if the alarm comes from a device not associated with a company.
- *Site* – site name. **NOTE**: Empty if the alarm comes from a device not associated with a site.
- *Device, Device s/n* – device name and serial number. **NOTE**: Empty for Patrol failed alarms, because they are not associated with any particular device.
- *Route* – route name. **NOTE**: Filled only for alarms associated with patrols.
- *Status* – alarm status (state).
- *Processed by* – name of the ActiveView user who processed the alarm. **NOTE**: Empty if it has not been processed yet.

ActiveTrack devices can be configured to add position information to alarm events. This information is available in the *CSV* format of the *Alarms report*. There is also an additional option in the tools menu (under the cog icon), to show the currently listed alarms on a map. It opens a new browser window with the trace of the device marked. All alarms form a single trace, so you should use the *Device filter* in order to get meaningful results.

NOTE: This report does not group alarms by site, like the alarms list and alarms browser. Even if two or more alarms from a single site were detected in succession, they are listed separately.

Alarms summary report

This report is based on the same data as the *Alarms report*, but the data are aggregated. The report contains totals for every alarm type, for every company, site or device (depending on user choice).



In the Alarms summary report, columns correspond to different types of alarms. Rows correspond to companies, sites or devices, depending on the grouping chosen by the user in report parameters. There is also a final row with totals for every alarm type (summary).

The alarms included in sums can by filtered by the following criteria:

- *Detected* – date and time when the alarm was detected by the system.
- *Company* – company name. **NOTE**: Setting this filter will exclude all alarms not associated with a particular company (see *Alarms report* description for details).
- *Site* – site name. **NOTE**: Setting this filter will exclude all alarms not associated with a particular site (see *Alarms report* description for details).
- *Device* – device name or device serial number. **NOTE**: Setting this filter will exclude all alarms not associated with a particular device (see *Alarms report* description for details).
- *Group by* - possibility of grouping by company, site or device.

Patrols report

This report shows information about finished patrols (either successful or not).

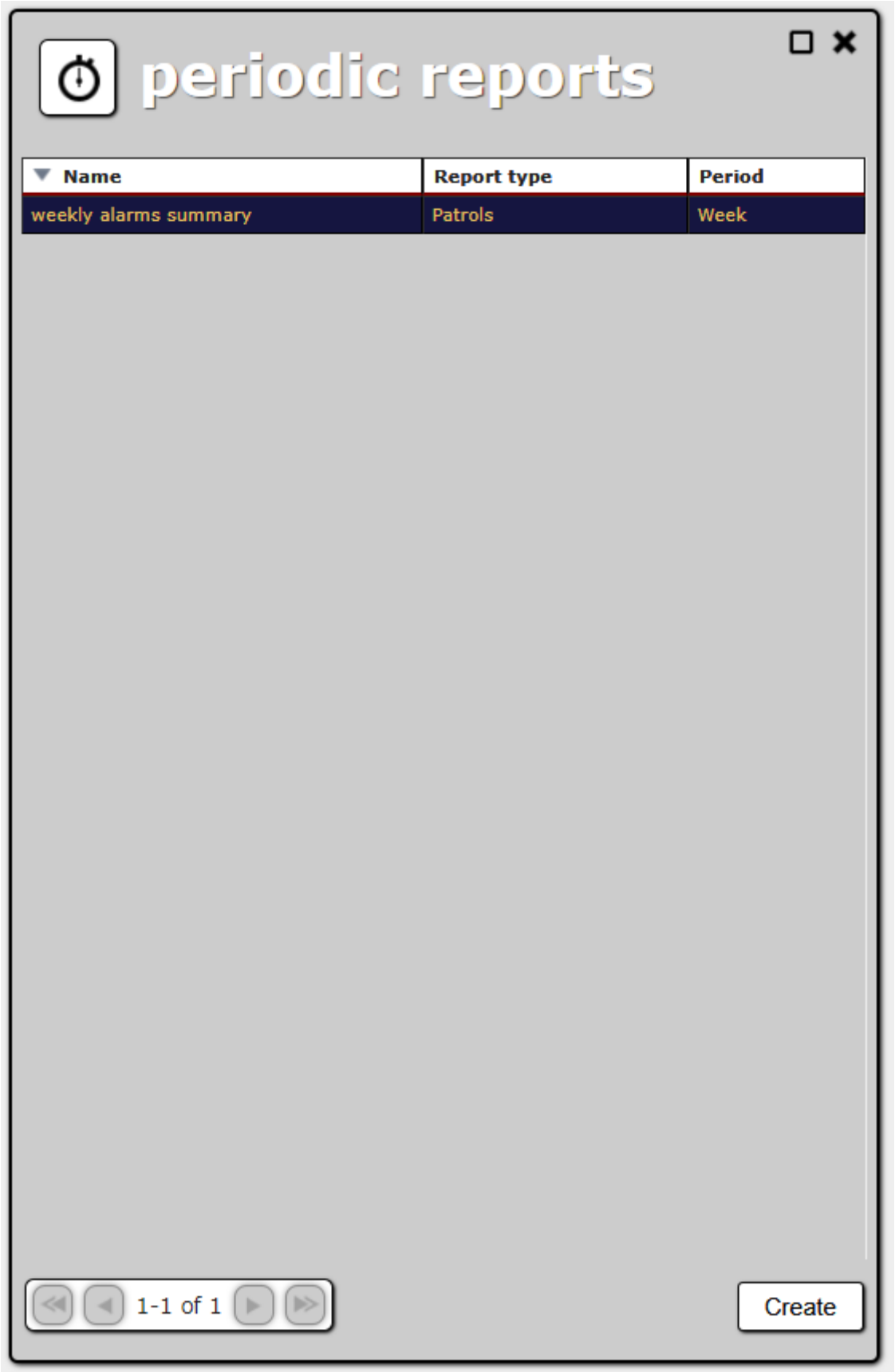
The Patrols report has the following columns:

- *Patrol start* – patrol start date and time.
- *Company* – the name of the company which the site where the patrol was conducted belongs to.
- *Site* – the name of the site where the patrol was conducted.
- *Route* – the name of the route which defined the patrol.
- *Checkpoints [+]* – the number of successful checkpoints (i.e. checkpoints passed on time).
- *Checkpoints [-]* – the number of unsuccessful checkpoints (i.e. checkpoints not passed on time).

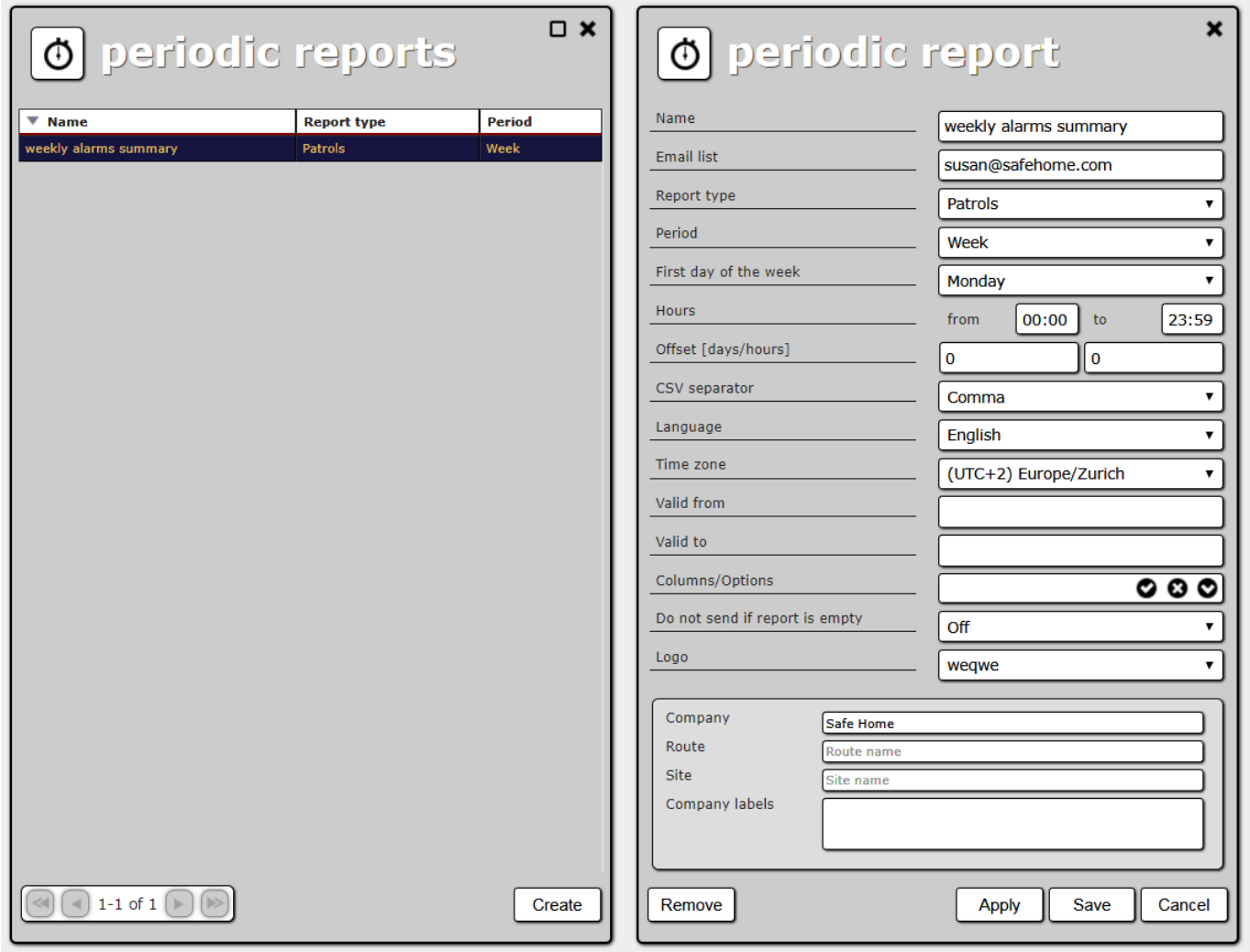
Unsuccessful patrols are highlighted in red (i.e. the patrols with at least one unsuccessful checkpoint).

Periodic reports

Each report can be configured to be sent by e-mail. To open **periodic reports list**, select *Reports* → *Periodic Reports* in the main menu.



You can create a new periodic report and edit or remove an existing one.



Every **periodic report** has the following properties:

- **Name** – unique periodic report name. It allows you to find the report on the periodic reports list.
- **E-mail list** – recipients' e-mail addresses, separated by commas.
- **Report type** – type of report to be generated.
- **Period** – time periods the report will cover. Choosing for example "Month" will result in a report generated every month, covering the previous month.
- **First day of the week** [*weekly reports only*] - reports will cover 7 days from the first day of the week. Choosing for example "Wednesday" will result in a report generated every Thursday, covering last Thursday, last Friday, Saturday and so on until Wednesday (i.e. the previous day).
- **Period first day** [*monthly, quarterly and yearly reports only*] - reports will cover a month, a quarter or an year from the "period first day" of every month/quarter/year (see examples below).
- **Hours** - the hours reports will cover every day (see examples below). Default values "from 00:00" and "to 23:59" mean that reports will cover whole days.
- **Offset [days/hours]** – offset in days and hours from the end of the chosen period when reports will be generated. For example: for a period of a week and offset 3 days and 8 hours, reports will be generated every Thursday, at 8 a.m., and will cover time span from previous Monday to last Sunday.
- **CSV separator** – a character used to separate columns in generated CSV files. The default is the separator character set in user settings.
- **Language** - language in which reports will be generated.
- **Time zone** – time zone in which periods will be calculated and times and dates in reports will be displayed. The default is the time zone set in user settings.
- **Valid from** - reports will start to be generated after this date and time (see examples below).
- **Valid to** - reports will not be generated after this date and time (see examples below).

- **Columns** – set of columns which will be included in report (default all columns).
- **Filters** – all filters applicable to the chosen report type, except filters by date and time (data for periodic reports are filtered by date based on the selected periodicity).

E-mails with periodic reports contain report results in a printable format and in a *CSV* file (attached). For periodic reports to work, a correct e-mail configuration is needed (see E-mail configuration for details).

Example 1

You want a daily report, covering time span from 9 a.m. (inclusive) to 5 p.m. (exclusive), generated after 3 a.m.:

- Period: Day
- Hours: from 9:00 to 16:59
- Offset: 0 days and 10 hours
- Valid from: empty (default)
- Valid to: empty (default)

Example 2

You want a weekly report, covering time span from Thursday to Wednesday every week and from 8 p.m. (inclusive) to 8 a.m. (exclusive) every day, generated every Friday, at 10 a.m.. You also want this report to be generated only from 1 July 2014 to 31 December 2014:

- Period: Week
- First day of the week: Thursday
- Hours: from 20:00 to 7:59
- Offset: 1 day 2 hours
- Valid from: 1/07/2014
- Valid to: 31/12/2014

With this definition, you will get the following reports:

- The first one will be generated on on 1 July, at 10 a.m. It will cover time span from 8 p.m. 19/06/2014 to 8 a.m. 20/06/2014, from 8 p.m. 20/06/2014 to 8 a.m. 21/06/2014 etc., the last time span will be from 8 p.m. 25/06/2014 to 8 a.m. 26/06/2014
- The second report will be generated on 4 July, at 10 a.m. It will cover time span from 8 p.m. 26/06/2014 to 8 a.m. 27/06/2014, from 8 p.m. 27/06/2014 to 8 a.m. 28/06/2014 etc., the last time span will be from 8 p.m. 2/07/2014 to 8 a.m. 3/07/2014
- The same goes for subsequent reports.
- The last report will be generated on 26 December, at 10 a.m.

Example 3

You want a quarterly report, but with quarters starting on 9 February, 10 May, 9 August and 9 November (in the 40th day of each quarter):

- Period: Quarter
- Period first day: 40
- Hours: from 00:00 to 23:59 (defaults)

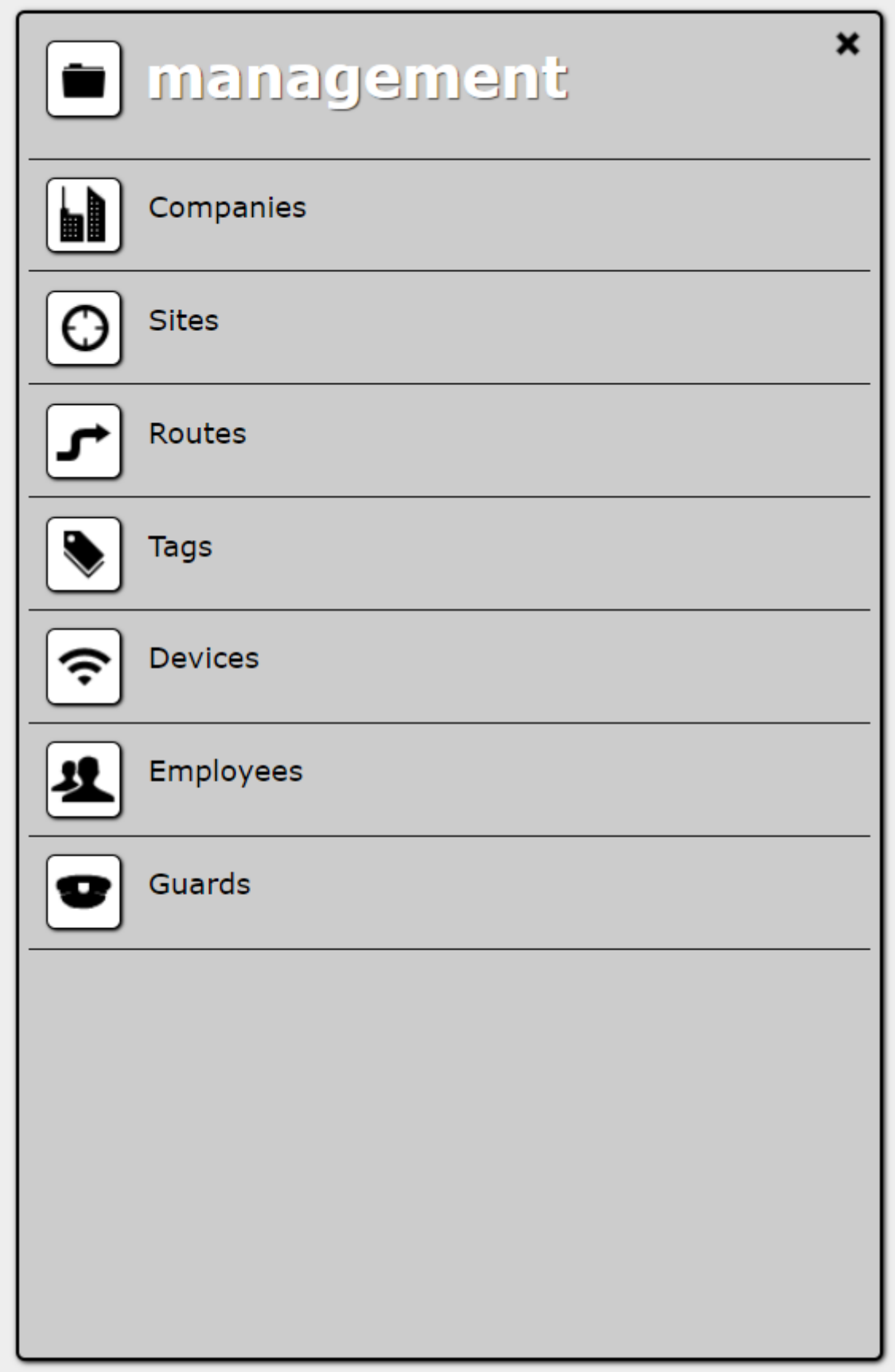
- Offset: 0 days and 0 hours (defaults)
- Valid from: empty (default)
- Valid to: empty (default)

With this definition the first report generation date depends on when you create the definition. For example:

- If the definition is created on 10 January, then:
  - the first report will be generated on 9 February (around midnight). It will cover time span from 9 Decemeber in the previous year to 8 February in the current year;
  - the second report will be generated on 10 May (around midnight). It will cover time span from 9 February to 9 May;
  - ... and so on.
- If the definition is created on 1 April, then:
  - the first report will be generated on 10 May (around midnight). It will cover time span from 9 February to 9 May;
  - the second report will be generated on 9 August (around midnight). It will cover time span from 10 May to 8 August;
  - ... and so on.

Management

Most ActiveView functionalities rely on configuration of sites, routes, devices and so on. All these entities can be managed in the Management section of the application. To open it, choose *Management* from the main menu.



There are several types of entities you can create and edit in ActiveView. You can read about managing them in the following sections:

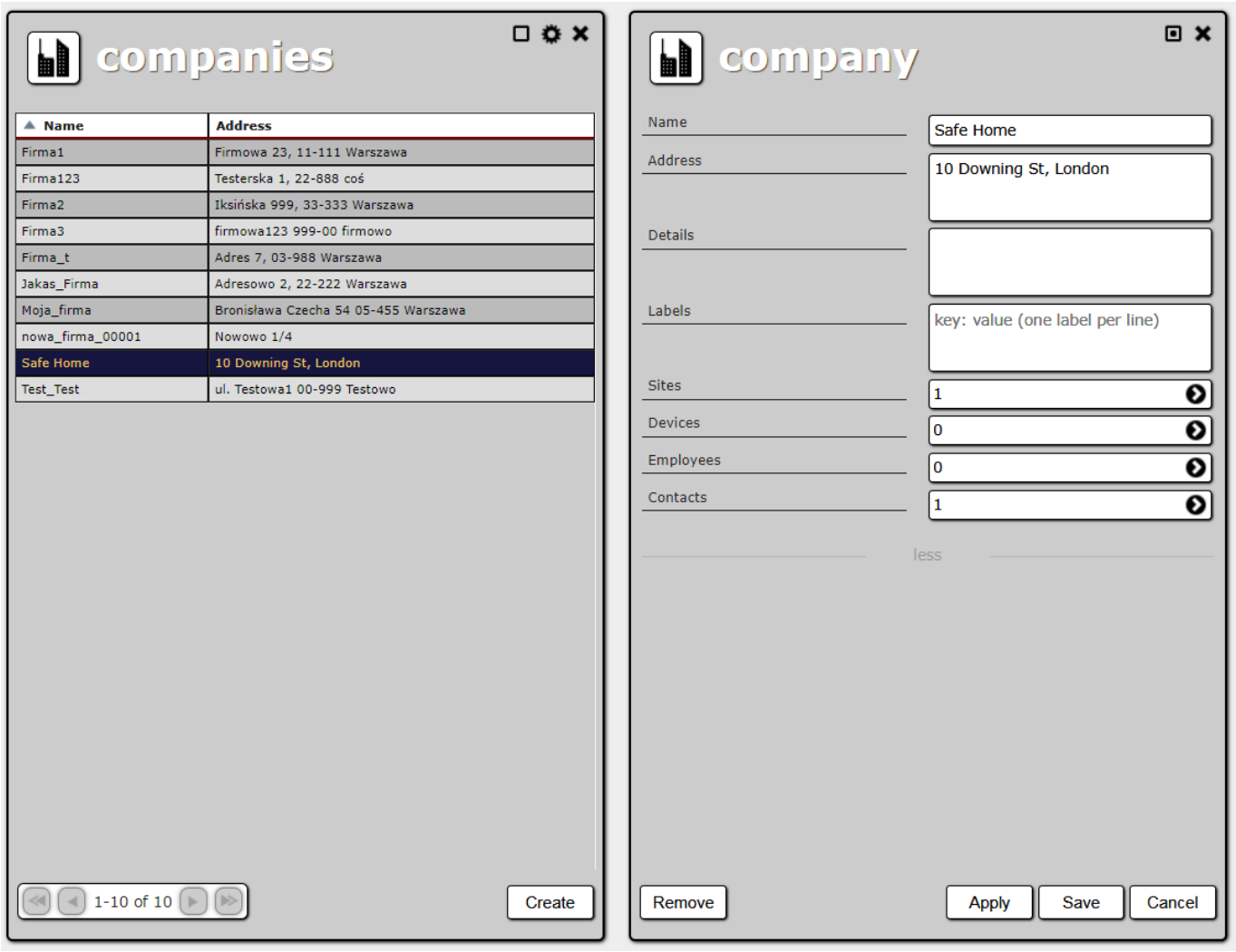
- Companies
- Sites
- Routes

- Tags
- Devices
- Employees
- Guards
- Instructions

Companies

Companies represent clients of the security agency which is the main user of the application. To open the companies list, select *Management → Companies* in the main menu.

You can create a new company and edit or remove an existing one.



Every company has the following properties:

- **Name** – unique company name.
- **Address**
- **Details**
- **Labels** - a new company parameter. Enter the key, i.e. the name and the corresponding specific value. Each label should be involved in the new line.
- **Sites** – displays the number of sites owned by the company. Clicking it opens a new panel with a list of these sites, where you can manage them.
- **Devices** – displays the number of devices associated with the company. Clicking it opens a new panel with a list of these devices, where you can manage them.
- **Employee** – displays the number of employees of the company. Clicking it opens a new panel with

a list of these employees, where you can manage them.
- **Contacts** – displays the number of contacts from that company. Clicking it opens a new panel with a contact manager, where you can browse, create, edit and remove contacts (see below).

Contact manager

The contact manager has two columns. On the left, there is a list of contacts. On the right, there are the details of a chosen contact. With + and X buttons you can create and remove contacts.

You can fill the following details about each contact:

- *name*;
- *first phone number*;
- *send text message notifications to the first phone number (checkbox labelled "!!!");*
- *second phone number;*
- *send text message notifications to the second phone number (checkbox labelled "!!!");*
- *first e-mail address;*
- *second e-mail address;*
- *password – used by the security agency to authenticate the person, e.g. over a phone;*
- *additional information.*

If a contact is associated with a site and an alarm from that site is detected:

- contact details are displayed in alarm details,
- if sending text message notifications is turned on for any of the contact's phone numbers, text message notifications are sent.

NOTE: Changes to contact details are not saved until you save the whole company details.

Removing a company

When a company is removed, all of its sites (and all of their routes; for consequences see Removing a route), employees and contacts are removed as well.

Links to devices are also deleted. The devices are not removed, but are not linked to any company or site.

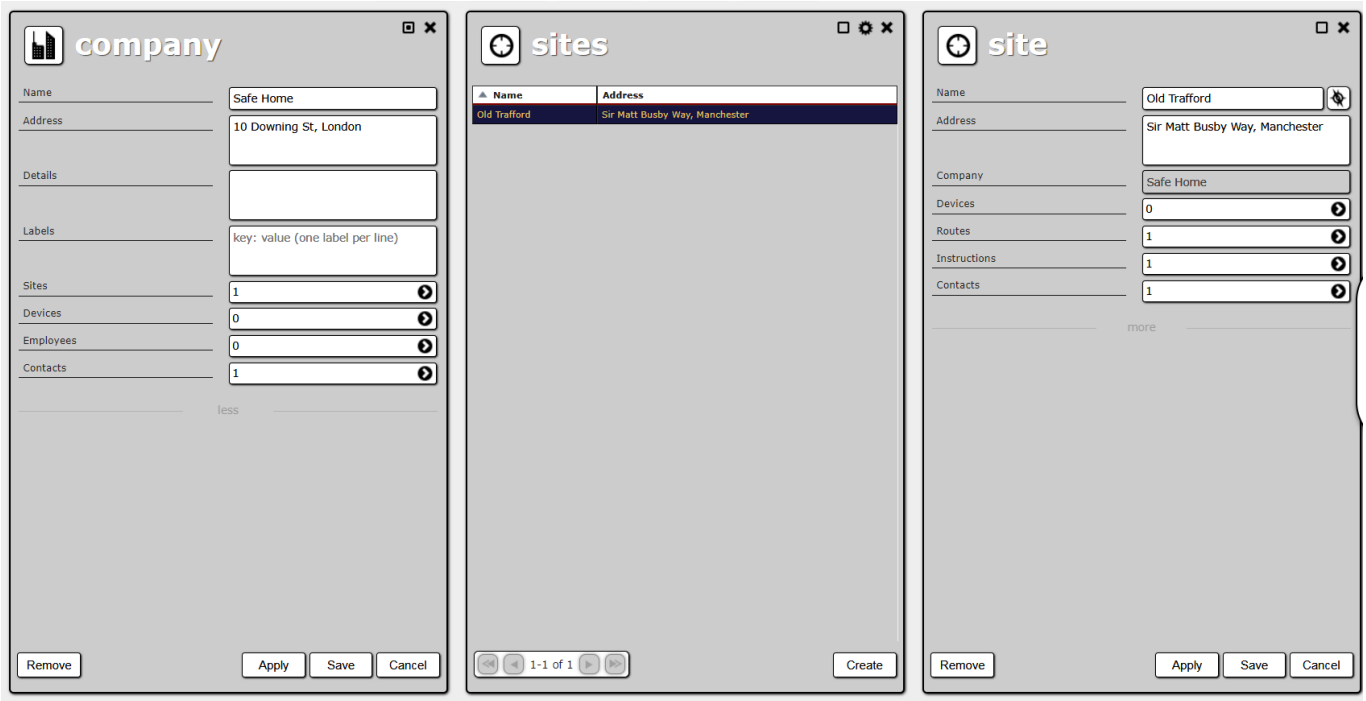
This does not affect past events or alarms. They are still available unchanged in the alarm browser and in the reports.

Sites

Sites represent buildings, areas and other places which the security agency supervises. Every site belongs to a company. There are two ways in which you can open a site list:

- select *Management* → *Sites* in the main menu to open a complete site list (i.e. a list of sites of all companies);
- click *Sites* on the company details panel to open this company's site list.

In both lists, you can create a new site and edit or remove an existing one.



Every site has the following properties:

- **Name** – site name. It has to be unique within the company to which the site belongs.
- **Address** – site address (it can be shown on a map; for details see below).
- **Details**
- **Time zone** - the time zone the site is located in (see below). The default is the time zone set in user settings.
- **Company** – the company to which the site belongs. It is set when the site is created and cannot be changed later.
- **Devices** – displays the number of devices linked to this site. Clicking it opens a new panel with a list of these devices, where you can manage them.
- **Routes** - displays the number of patrol routes defined for the site. Clicking it opens a new panel with a list of these routes, where you can manage them.
- **Instructions** - displays a list of instructions which can be used to provide operator with information on how to react in various situations (see Instructions for details).
- **Contacts** – displays the number of company contacts linked to this site. Clicking it opens a new panel, where you can choose which company contacts should be linked to this site (see below).

- **Notifications** – displays the number of types of alarms from this site which will generate text message notifications. Clicking it opens a new panel with a list of alarm types, where you can tick the ones you want notifications for.

Site time zone

Site time zone affects the following functionalities:

- route schedules are expressed in site time zone (see Schedule for more information on route schedules);
- on the alarm details panel you can switch between site and browser (user) time zone (see Alarm details for details);
- alarm detection time in an e-mail on alarm is expressed in site time zone (see E-mail on alarm for details).

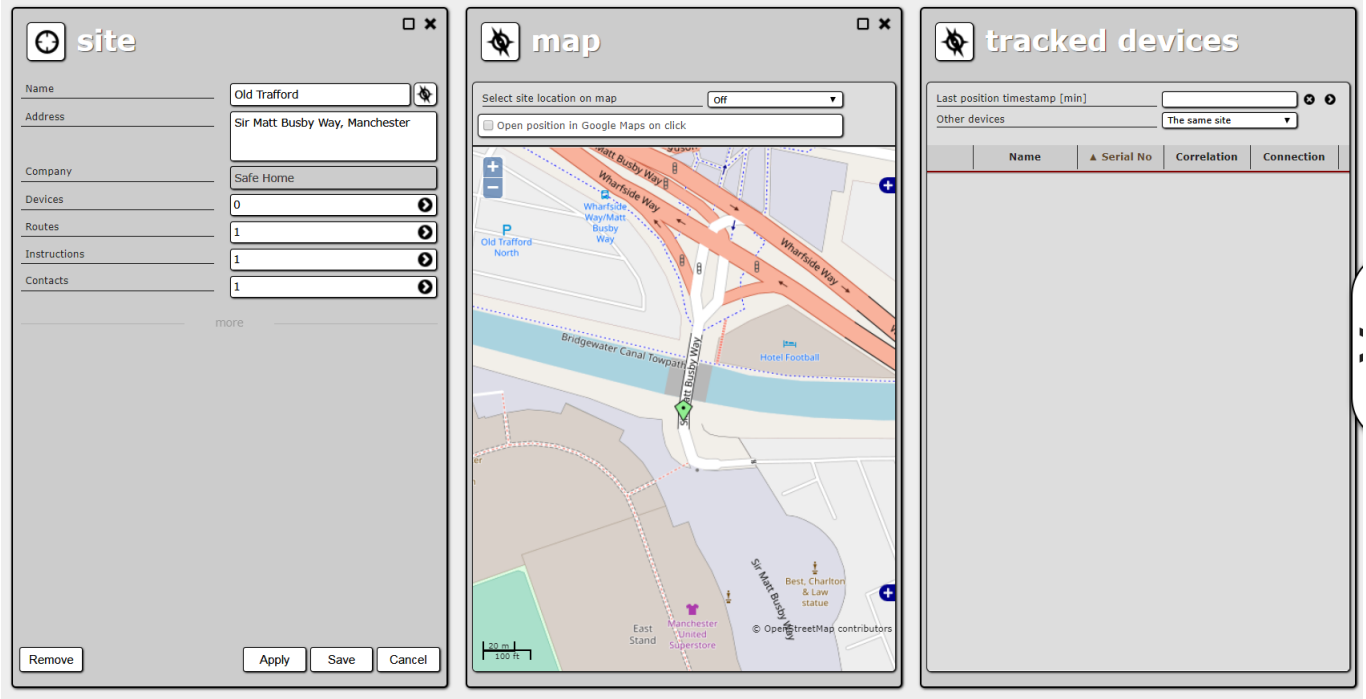
Site contacts

The contact linking panel has two columns. On the left, there are contacts of the company to which the site belongs. On the right, there are contacts linked to the site. You can link contacts to the site either by dragging them between columns or by using < and > buttons.

Site contacts are presented in alarm details. They are listed in the order set in the site contact list. You can reorder contacts either by dragging them up and down or by using up and down arrow buttons.

Site on a map

If the site address if filled, there is a map option available (a button with a compass rose icon to the right from the name field). Choosing it opens a new panel with a map showing the site location (if the map server is able to locate the address). Above the map, there is an option to select the site location on the map. If you turn it on and click anywhere on the map, the application will insert latitude and longitude of that place into the address field. **NOTE**: Selecting a location on the map is available only if *Google Maps* are set as the maps provider.



Removing a site

When a site is removed, all of its routes are removed too (for consequences, see Routes: Removing a route).

Links to devices, tags and contacts are also deleted. The devices, tags and contacts are not removed, but are now linked only to the parent company.

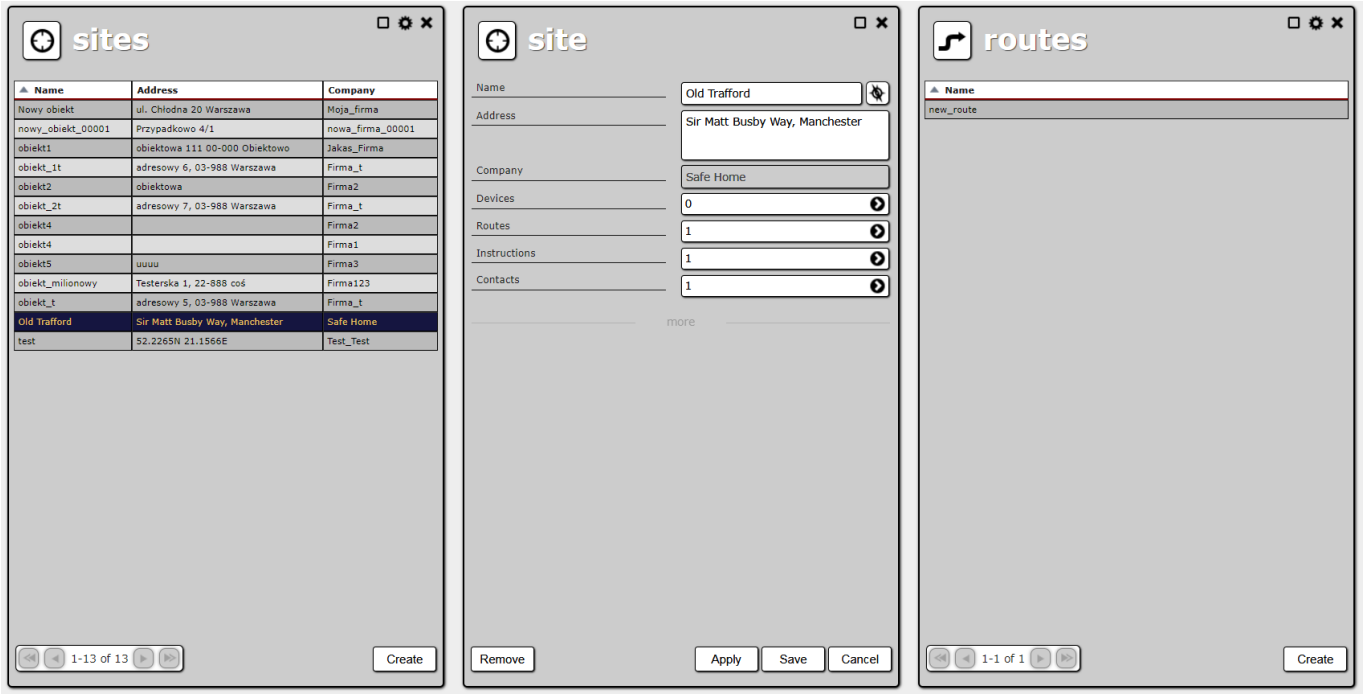
This does not affect past events or alarms. They are still available unchanged in the alarm browser and in the reports.

Routes

Routes are what guards follow when they patrol sites. Every route is defined for a single site (it cannot cover more than one site). There are two ways you can open a route list:

- select *Management → Routes* in the main menu to open a complete route list (i.e. a list of routes for all sites);
- click *Routes* on the site details panel to open this site's route list.

In both lists, you can create a new route and edit or remove an existing one.



Every route has the following properties:

- **Name** – route name. It has to be unique within the site the route is defined for.
- **Type** – route type: simple or advanced (see Route definition (checkpoints) below). It is set when the route is created and cannot be changed later.
- **Details**
- **Company** – the company to which the site for which the route is defined belongs. It is set when the route is created and cannot be changed later.
- **Site** – the site for which the route is defined. It is set when the route is created and cannot be changed later.
- **Checkpoints** – displays the number of checkpoints the route consists of. Clicking it opens a new panel with the route's definition (see below). You have to choose a company and a site first, because a route consists of checkpoints from a particular site.
- **Schedule** – displays the type of schedule defined for the route. Clicking it opens a new panel where you can change the route's schedule (see below).
- **Path validity framework dates** - the range of dates in which the path will be active. Possibility of setting the range when the path is inactive. By default, the fields are not filled in and the path is

valid from creation to infinity. The route can be defined earlier, but it will be valid only from “from” and “to” the entered date. You can also temporarily disable the path by defining dates in the “Ignore from” and “Ignore to” fields.

Route definition (checkpoints)

There are two types of routes:

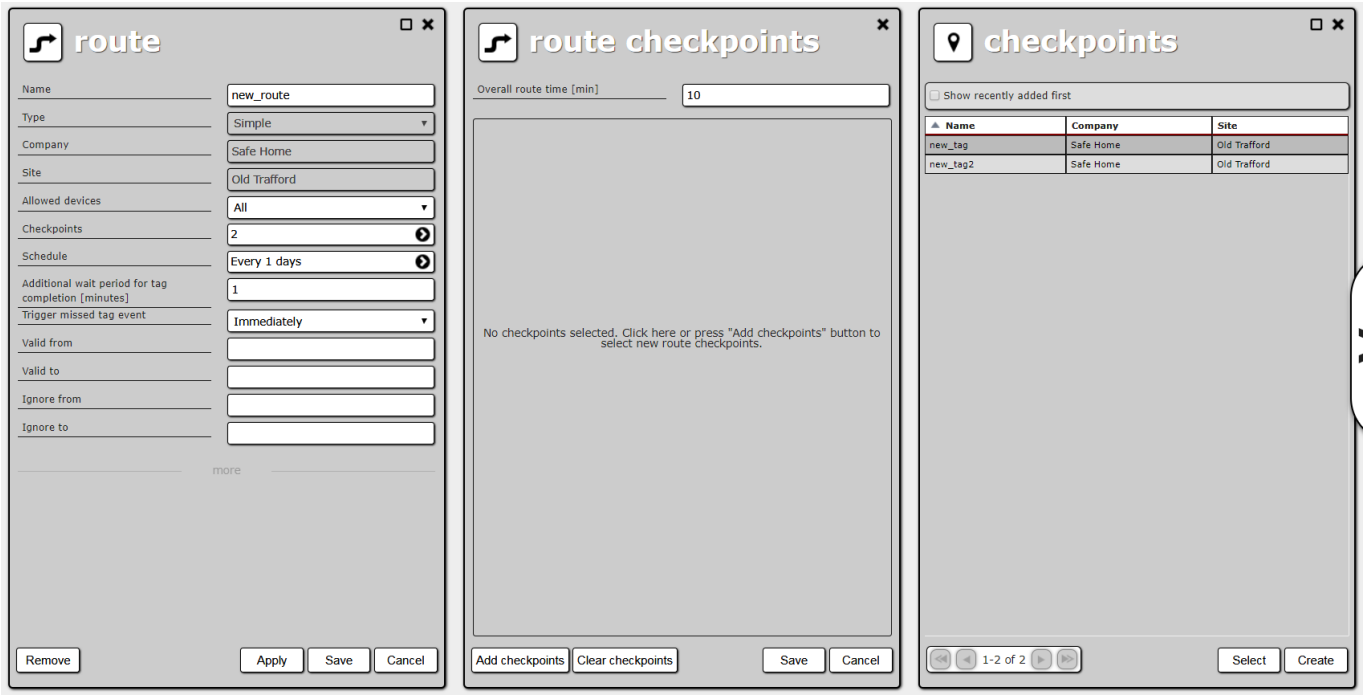
- ***Simple*** – a guard has a defined amount of time to pass all checkpoints of the route without any particular order.
- ***Advanced***– a guard has to pass checkpoints in a defined order, at defined moments in time and for each failed TAG there is a separate event (TAG MISSED, PATROL FAILED).

Simple route

Simple route is a set of checkpoints. A guard has a defined amount of time to pass all of them, without any particular order. See Patrol failed alarms below, for details on patrol completion and failure.

Simple route’s definition consists of:

- an overall route time (route duration),
- a list of checkpoints; for every checkpoint there are the following fields and options:
  - name (read only),
  - X button – removes the checkpoint from the list.



Below the checkpoints list, there are options to clear the list and to add new checkpoints. Choosing

the latter opens a list of all checkpoints connected with the site. You can select one or more (using ctrl and shift keys) and then choose *Select* to add them to the route.

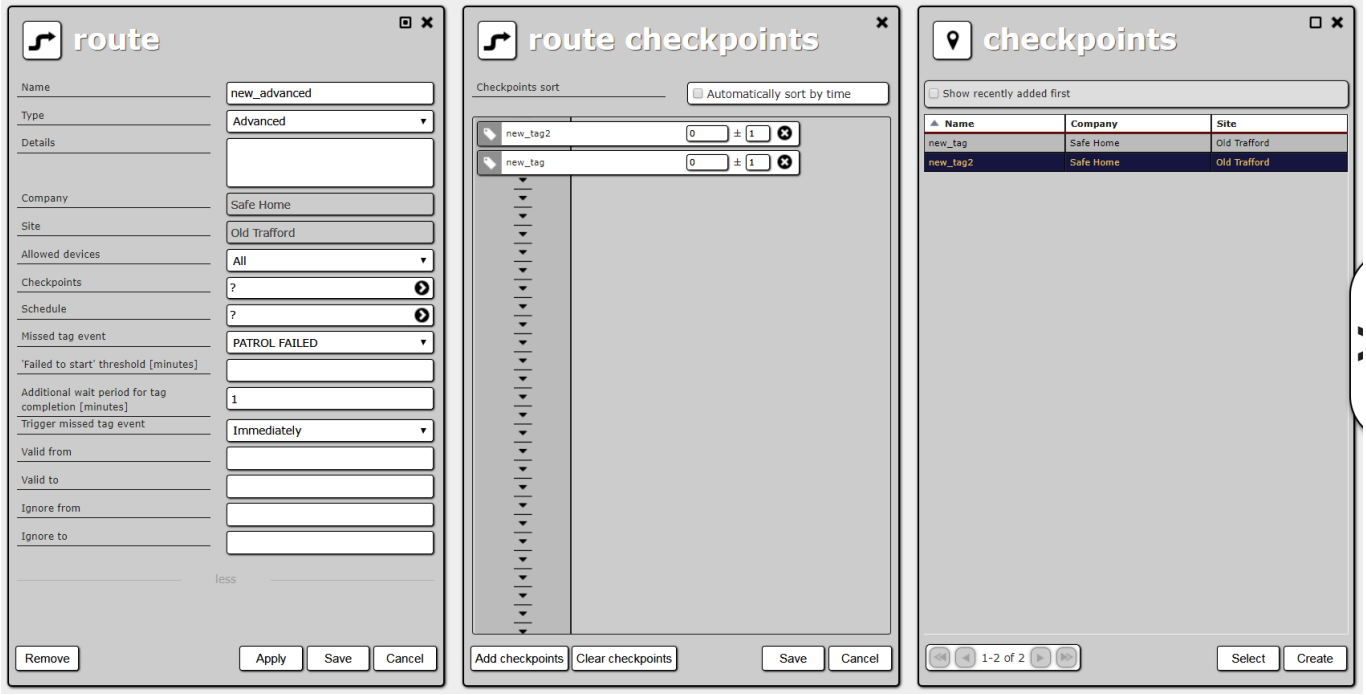
NOTE: Saving a route definition (checkpoints list) does not mean it is stored in the database. You have to save the whole route to make any changes permanent.

Advanced route

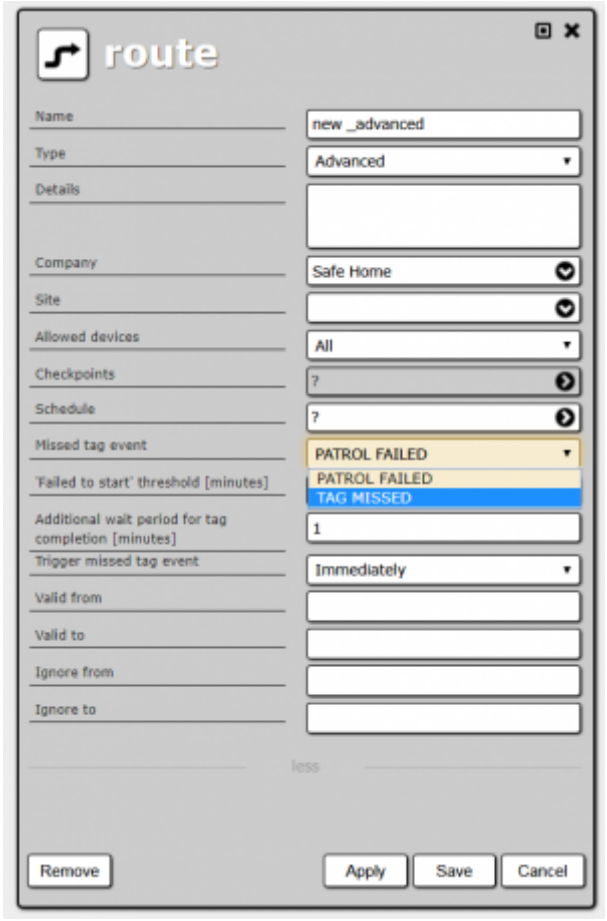
Advanced route is a list of checkpoints. A guard has to pass each of them at a defined point in time. See Patrol failed alarms below, for details on patrol completion and failure.

Advanced route's definition consists of a list of checkpoints. For every checkpoint there are the following fields and options:

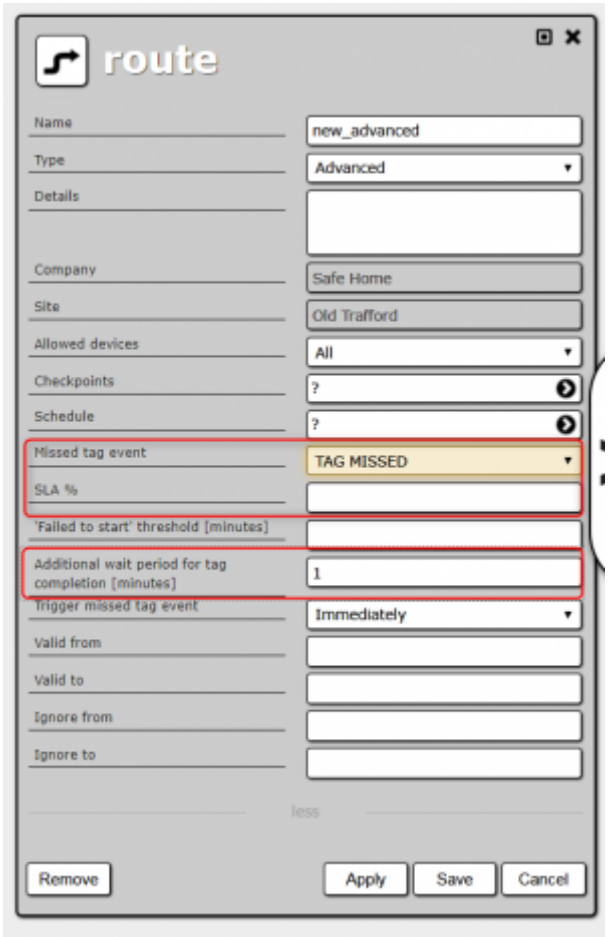
- **name** (read only);
- **checkpoint time** – the time from the beginning of a patrol, when the checkpoint should be passed (in minutes);
- **time tolerance** – number of minutes before and after the checkpoint time, when the checkpoint can be passed without causing an alarm. The minimum tolerance is 1 minute.
- **X** button – removes the checkpoint from the list.



Below the checkpoints list, there are the same *Clear* and *Add new* options as in the simple route definition panel (see above).



The *Tag Missed* event type applies to the unrepeated tag. It does not cause an alarm.



SLA is a percentage threshold of passed checkpoints. This feature allows you to specify how many percent of tags can be omitted from the path for the patrol to complete. It is valid only for advanced routes.

The Failed to Start alarm event determines how many minutes after the start of the route until the first tag is not reflected, the route will receive the *FAILED_TO_START* status.

Schedule

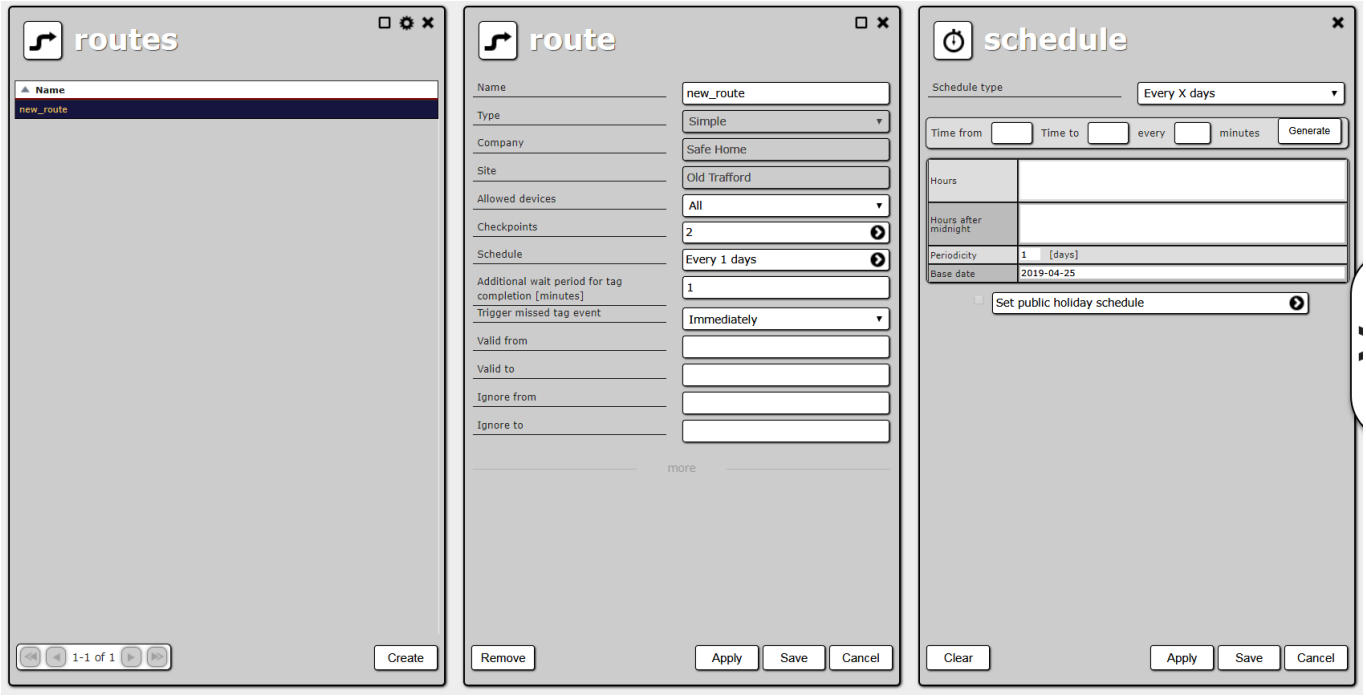
There are two types of route schedules:

- **Every X days** – patrols start at defined times (e.g. at 9 am, at 1 pm and at 5 pm) every day, every second day and so on (depending on the periodicity).
- **Days of the week** – patrol start times are defined for every day of the week. Every week, patrols start at the same time on particular days of the week.

All times in a schedule are expressed in the site time zone (see Sites for more information on site time zone).

The *Every X days* schedule has the following fields:

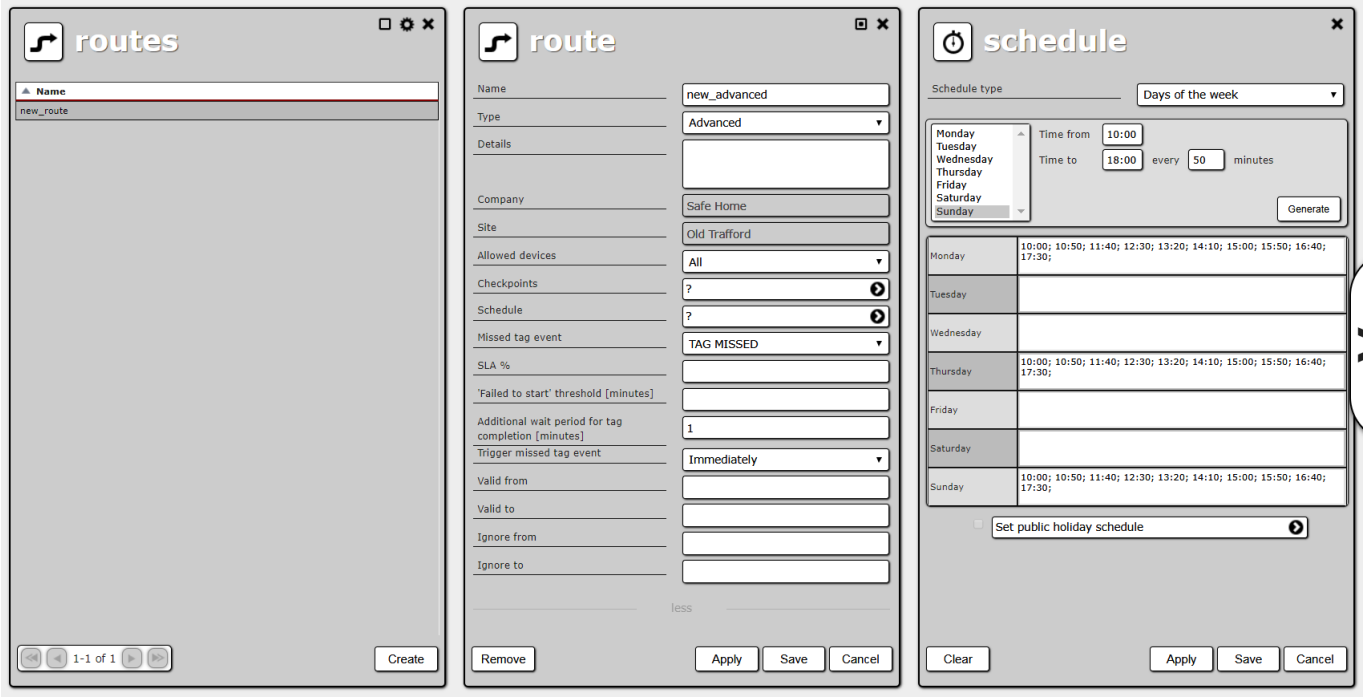
- **Hours** – semicolon-separated list of times when patrols start (expressed in a 24-hour clock, for example: 11:30; 13:30; 15:30). These times refer to the dates resulting from the chosen periodicity.
- **Hours after midnight** – semicolon-separated list of times when patrols start after midnight (expressed in a 24-hour clock, for example: 1:30; 3:30; 5:30). These times refer to the days after the dates resulting from the chosen periodicity.
- **Periodicity** – 1 means every day, 2 means every second day and so on.
- **Start date** – the basis to calculate the dates when patrols occur. For example periodicity 3 and start date 31.12.2012 result in patrols on the 31.12.2012, the 3.01.2013, the 6.01.2013 and so on.



In the bottom left corner of the panel, there is an option to clear *Hours* and *Hours after midnight* fields.

Above the schedule fields, there is an automatic times generator. You set time when you want patrols to start (**Time from**), time when you want them to end (**Time to**) and how often you want a patrol (**every … minutes**). After you choose **Generate**, generated times are appended to **Hours** and **Hours after midnight** fields. The latter is used when **Time from** is later then **Time to**.

The *Days of the week* schedule has a times list for every day of the week (semicolon-separated, expressed in a 24-hour clock, like Hours in the *Every X days* schedule).



The clear option at the bottom and the automatic times generator at the top are also available.

In the times generator, you can choose days of the week for which the generated times will be appended. If Time from is later then Time to, times after midnight are appended to the next day of the week.

Patrol failed alarms

ActiveView generates a patrol failed alarm if a guard does not pass a checkpoint he/she is supposed to. When exactly a guard should pass a checkpoint depends on the route type, definition (checkpoints list) and schedule.

For a *simple route*, every time a patrol starts according to schedule, a guard has the “overall route time” to pass all the checkpoints. If he/she passes them before that time, the patrol is considered completed. If he/she does not, a patrol failed alarm is generated after the “overall route time” from the patrol’s start.

For an *advanced route*, every time a patrol starts according to schedule, a guard has to pass all the checkpoints at defined times.

If he/she passes the first checkpoint after *checkpoint time* minus *time tolerance*, but before *checkpoint time* plus *time tolerance* from the patrol's start, nothing happens. If he/she does not, a patrol failed alarm is generated (after *checkpoint time* plus *time tolerance* from the patrol's start).

The same goes for all the checkpoints of the route. Every checkpoint not passed on time generates an alarm.

Right after a guard passes the last checkpoint on time (in *checkpoint time +/- time tolerance*), the patrol is considered completed.

Removing a route

When a route is removed, all future patrols resulting from its schedule are cancelled. However, patrols which have already started, continue (i.e. will result in alarms if checkpoints are not passed on time).

Tags

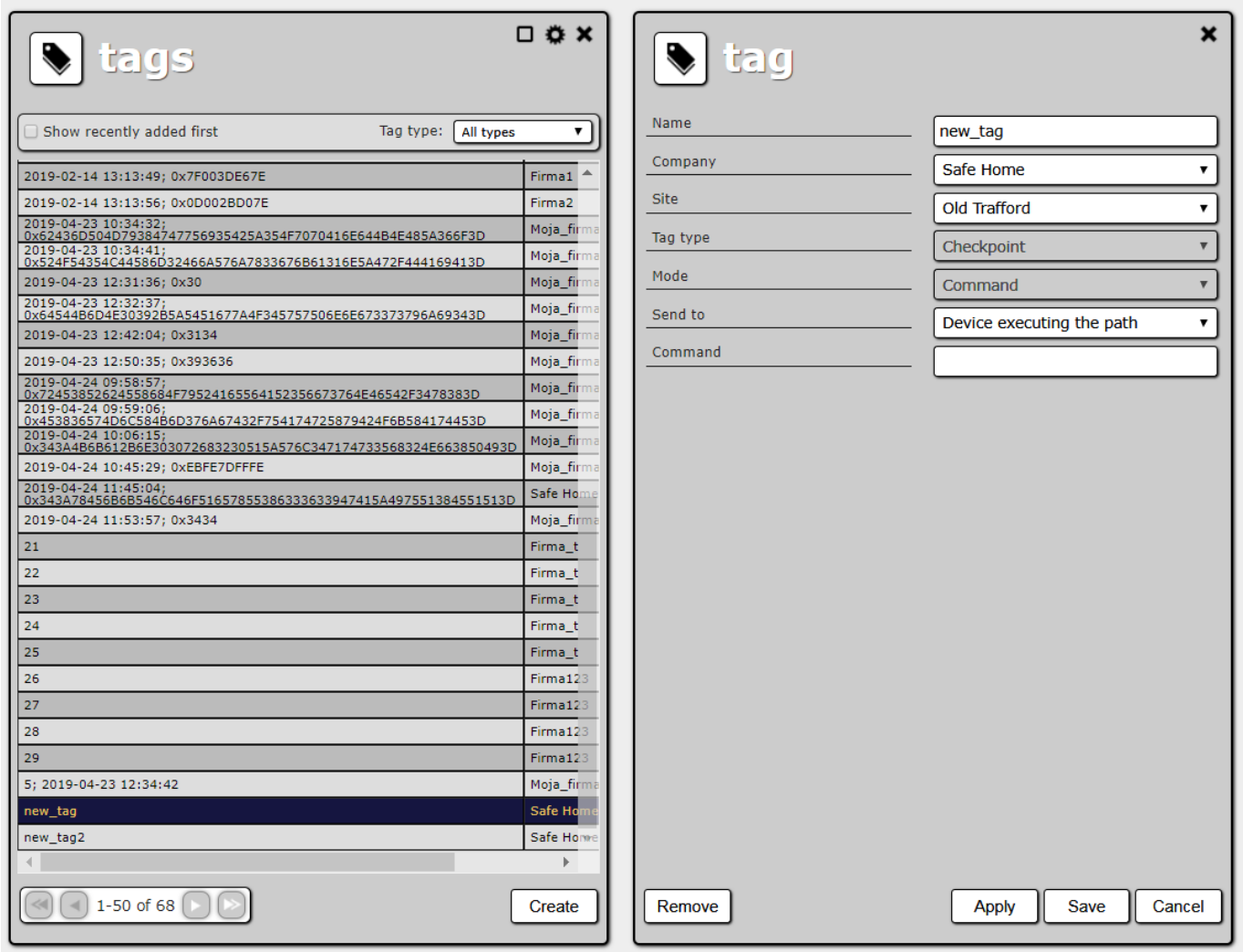
RFID Tags play an important role in ActiveView. They are used as checkpoints which make up routes. *RFID Tags* can also be treated as people identifiers and action triggers.

There are two types of tags: *normal tags* and *virtual tags*. *Normal tags* are just ActiveGuard devices. *Virtual tags* are checkpoint tags, which are not connected to any device – they represent area or action to be performed on path. While normal tags are checked by with an ActiveGuard, virtual tags are checked either by entering some area or automatically.

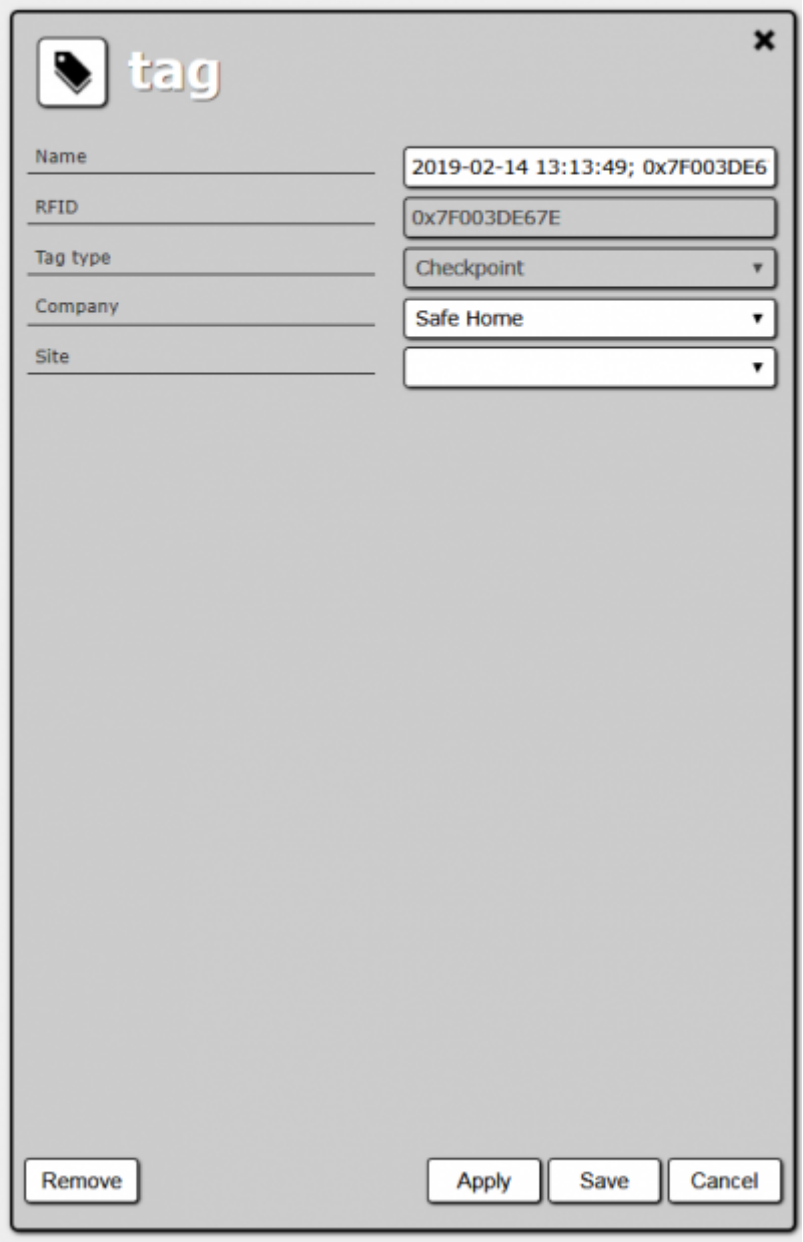
To open the tags list, select *Management* → *Tags* in the main menu. From there, you can edit or remove tags. The list is updated automatically, so you will see new tags without reloading it.

New tags are added to the system when you read them with an ActiveGuard for the first time. The default tag type is checkpoint. If the ActiveGuard you used is linked to a site, the read tag is automatically connected to the site.

New *virtual tags* can be added by simply using “Create” button.



You can filter the tag list by type. You can also tick the **Show recently added first** option. It will sort the tags by addition date and time in descending order. When you read new tags to add them to ActiveView, the option makes finding them easier.



Every *normal* tag has the following properties:

- **Name** – unique tag name. When the tag is first read, it is added to the system under a name in the following form: <date and time>; <RFID>
- **RFID** (read only)
- **Tag type** – determines the effects of reading the tag.

There are the following types:

- *Checkpoint* – it can be used in a route definition. You can choose a **company** and a **site** it will be connected with (only a checkpoint connected with a site can be a part of a route). If a checkpoint is indeed a part of a route, it cannot be deleted.
- *Alarm tag* – reading an alarm tag generates an alarm. You can choose the type of alarm that will be generated.

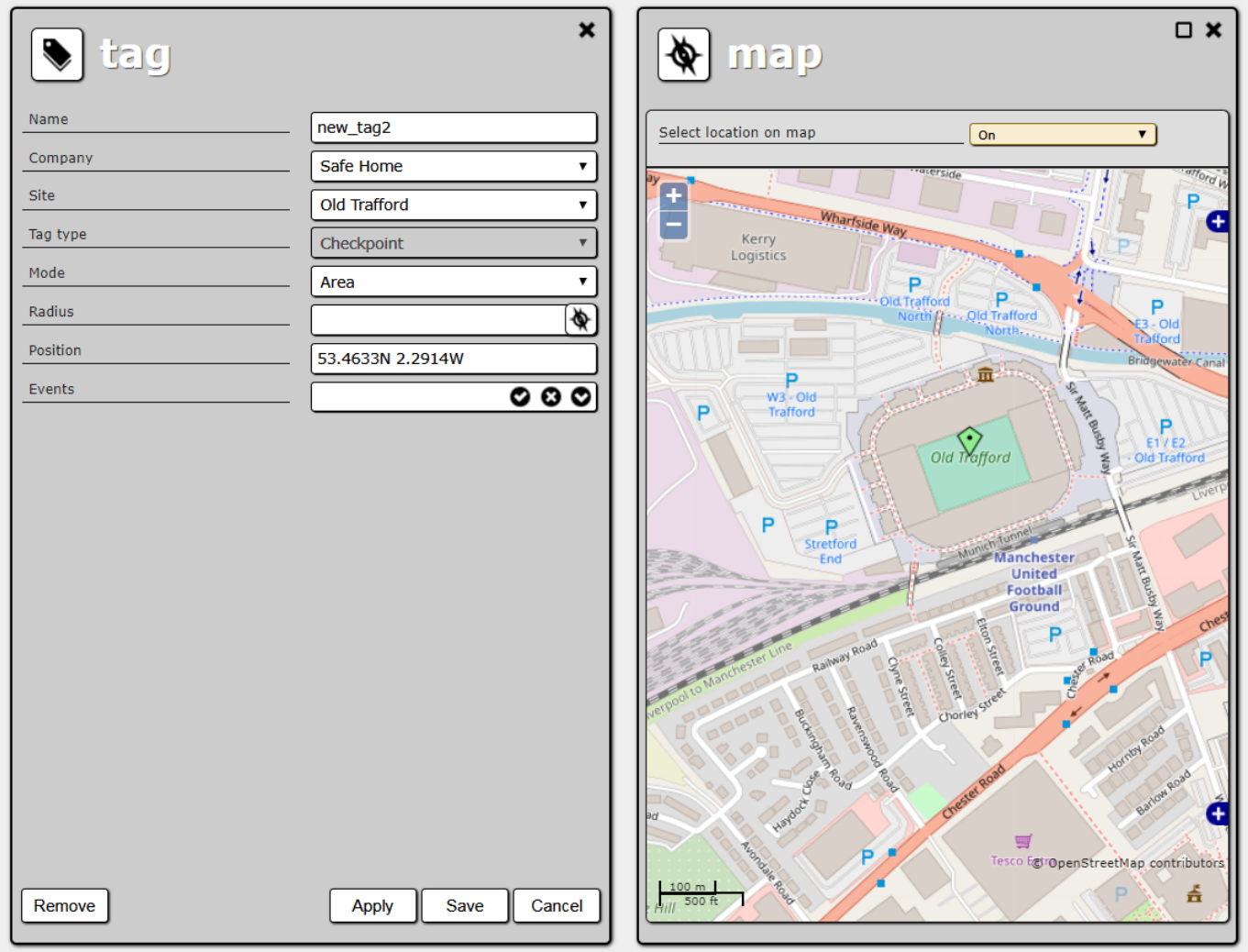
- *Guard identifier (e.g. guard badge)* – reading a guard identifier with an ActiveGuard will automatically link it to the guard (if this function is turned on in the device's settings). You can choose the guard the identifier is assigned to.
- *Employee identifier (e.g. employee badge or fingerprint template)* – when an employee identifier is read with an ActiveGuard in the "enter work mode", a workplace entry event is recorded. When it is read with an ActiveGuard in the "exit work mode", a workplace exit event is recorded. These events can be listed in the Events and alarms report. You can choose a company and the employee the identifier is assigned to.
- *Disconnecting from site* – reading a tag of this type with an ActiveGuard linked to a site will delete this link (if this function is turned on in the device settings).
- *Enter work mode* – reading a tag of this type with an ActiveGuard will switch it to the "enter work mode" (if this function is turned on in the device settings).
- *Exit work mode* – reading a tag of this type with an ActiveGuard will switch it to the "exit work mode" (if this function is turned on in the device settings).
- *Disable enter/exit work mode* – reading a tag of this type with an ActiveGuard will switch it to the normal mode, i.e. neither the "enter work mode" nor the "exit work mode" (if this function is turned on in the device settings).

All *virtual tags* are of checkpoint type. There are two types of *virtual tags*:

- **Area tag** – this tag is checked when ActiveTrack enters some specified area (circle defined by center and radius). The area tag only works when it is added to the path.
- **Command tag** – this tag is checked automatically. When it is checked, a command is send to devices (either the device executing the path, all devices in a site or all devices in a company).

Area tag

Area tag is a *virtual tag*, because it represents an area (only circle) rather then an real tag. It is also checkpoint tag, because it can be used in routes just like any normal checkpoint tag.



Area tags have the following properties:

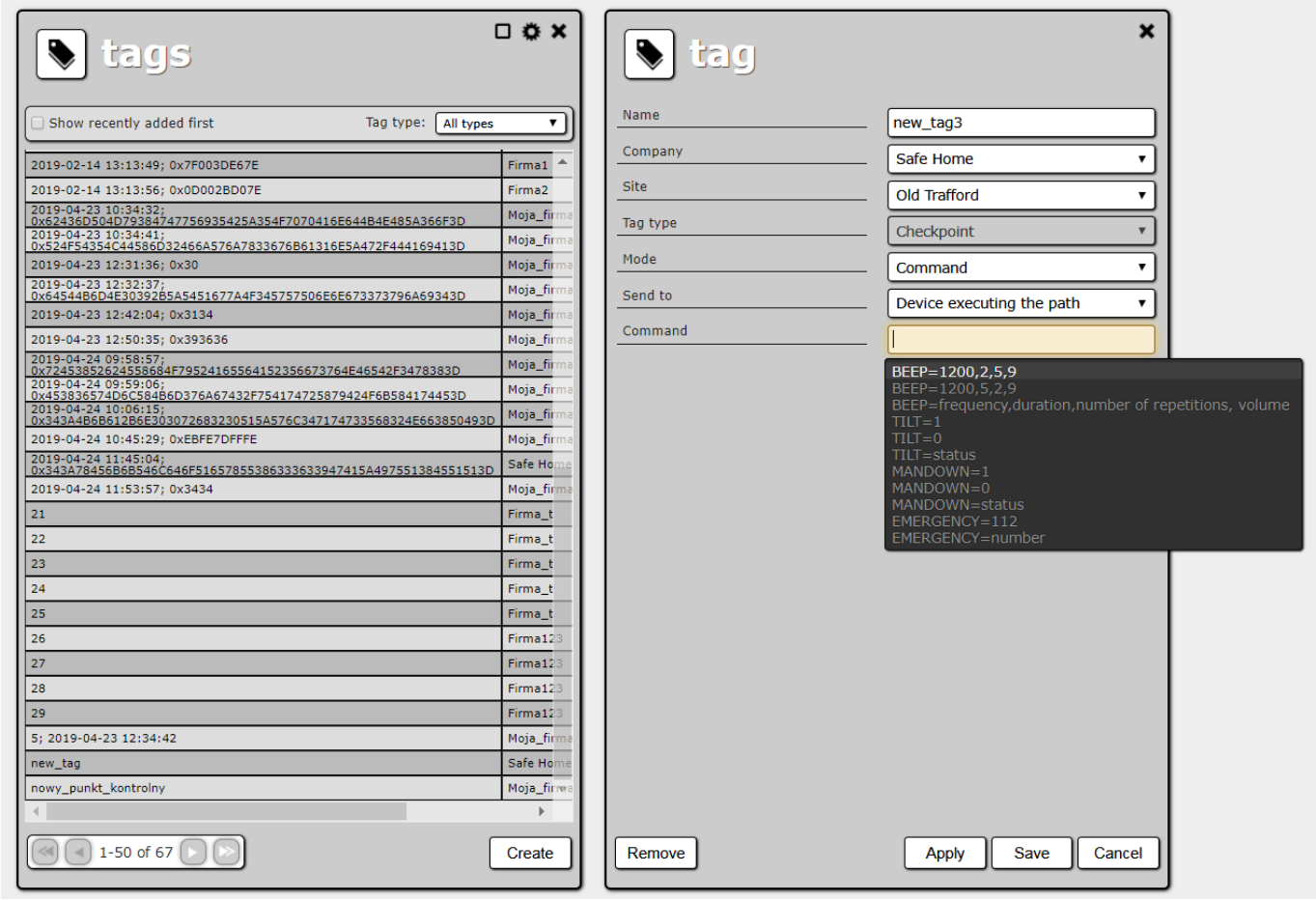
- **Name**,
- **Position** – defines center of the circle,
- **Radius** – defines size of circle,
- **Events** – list of events, which can be send from ActiveTrack

Area tag is checked when ActiveTrack, while being in the specified circle, sends the message, type of which belongs to the specified list. Position of ActiveTrack is determined using GPS coordinates.

Position of the are tag can be specified in one of two ways. You can enter GPS coordinates directly into *Position* text box. Alternatively, you can click on the button with Compass rose next to the radius text box. This will show you the map. Now you can specify the position by placing marker in the desired place.

Command tag

Command tag is a *virtual tag*, because it does no represent an real tag. It is also checkpoint tag, because it can be used in routes just like any normal checkpoint tag.



Command tags have the following properties:

- **Name**,
- **Send to** – specifies to which devices is the command send.
- **Command** - command which is send.

Command tag is checked automatically. For example, if definition of a route states that command tag should be checked between 10th and 12th minute after route is started, the command tag is automatically checked in 10th minute.

Once command tag is checked, the specified command is send to the chosen devices. Any command can be entered and sample commands are prompted below the *Command* text box. Command can be send to:

- device executing the path, which is the last device used on this path,
- all devices from the site, to which this command tag belongs,
- all devices from the company, to which this command tag belongs.

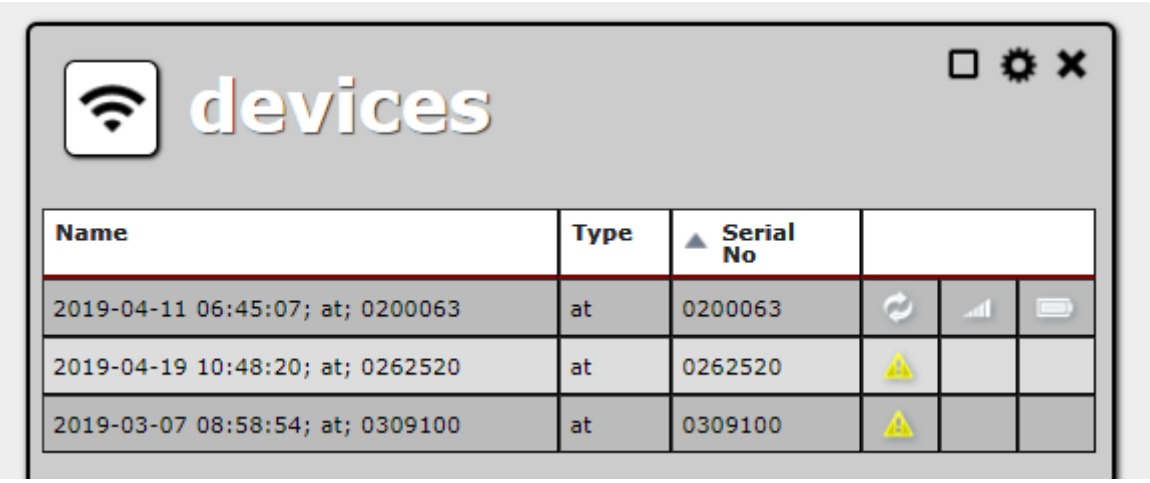
Additional actions

Furthermore there is a context menu for tags on the tags list. The following actions are available on tags:

- **Edit selected** – opens tag details. If more than one tag is selected, the name and the RFID fields are hidden and the other tag properties are changed in all the tags at once.
- **Remove selected** – removes all selected tags.
- **Select all** – selects all tags on the current page.
- **Deselect all** – deselects all tags.

Devices

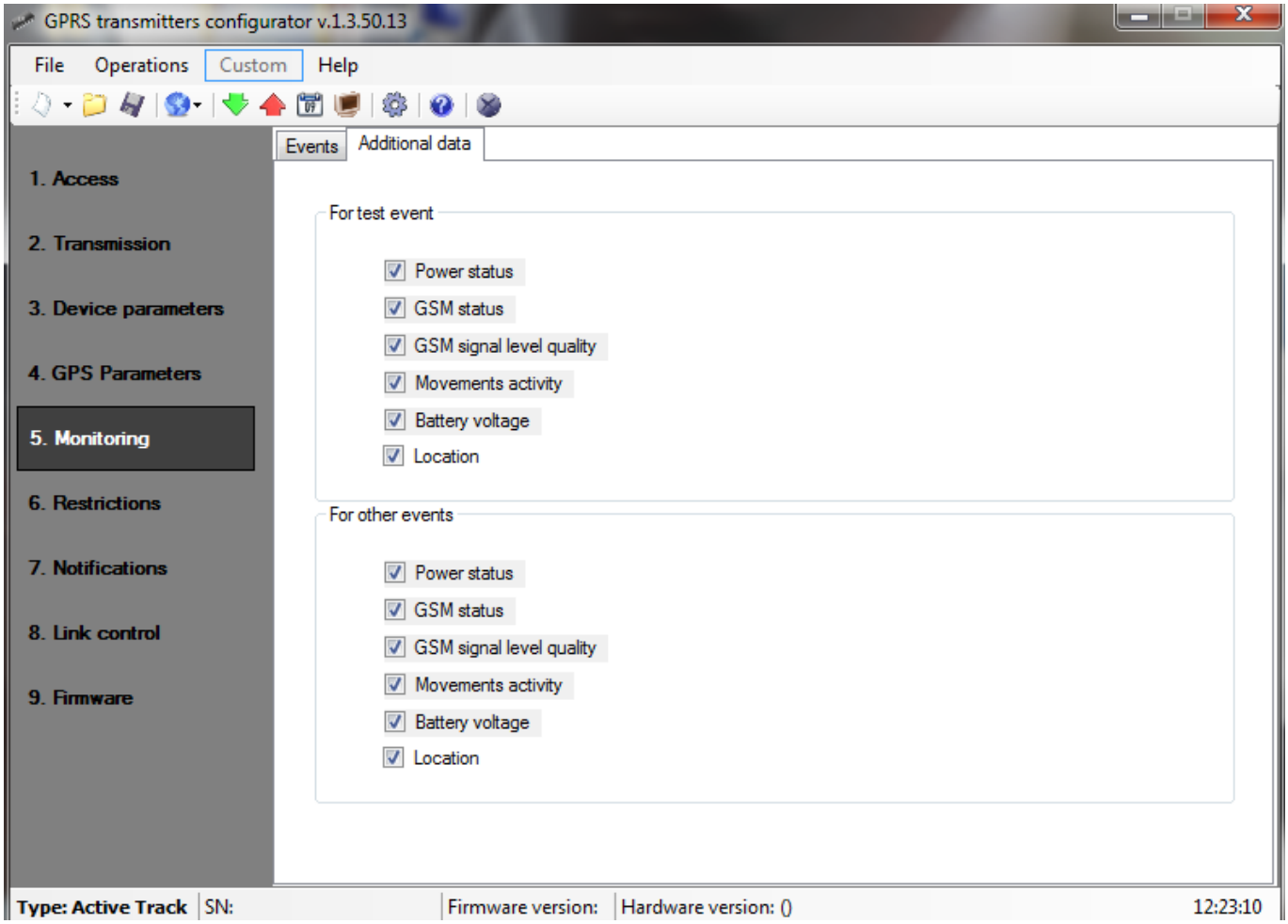
You can connect different devices to ActiveView, and the most important devices are: standard version of the Active Track device, the Active Track Mobile application in the mobile version and the Active Guard device. To open a list of all devices, select *Management* → *Devices* in the main menu.



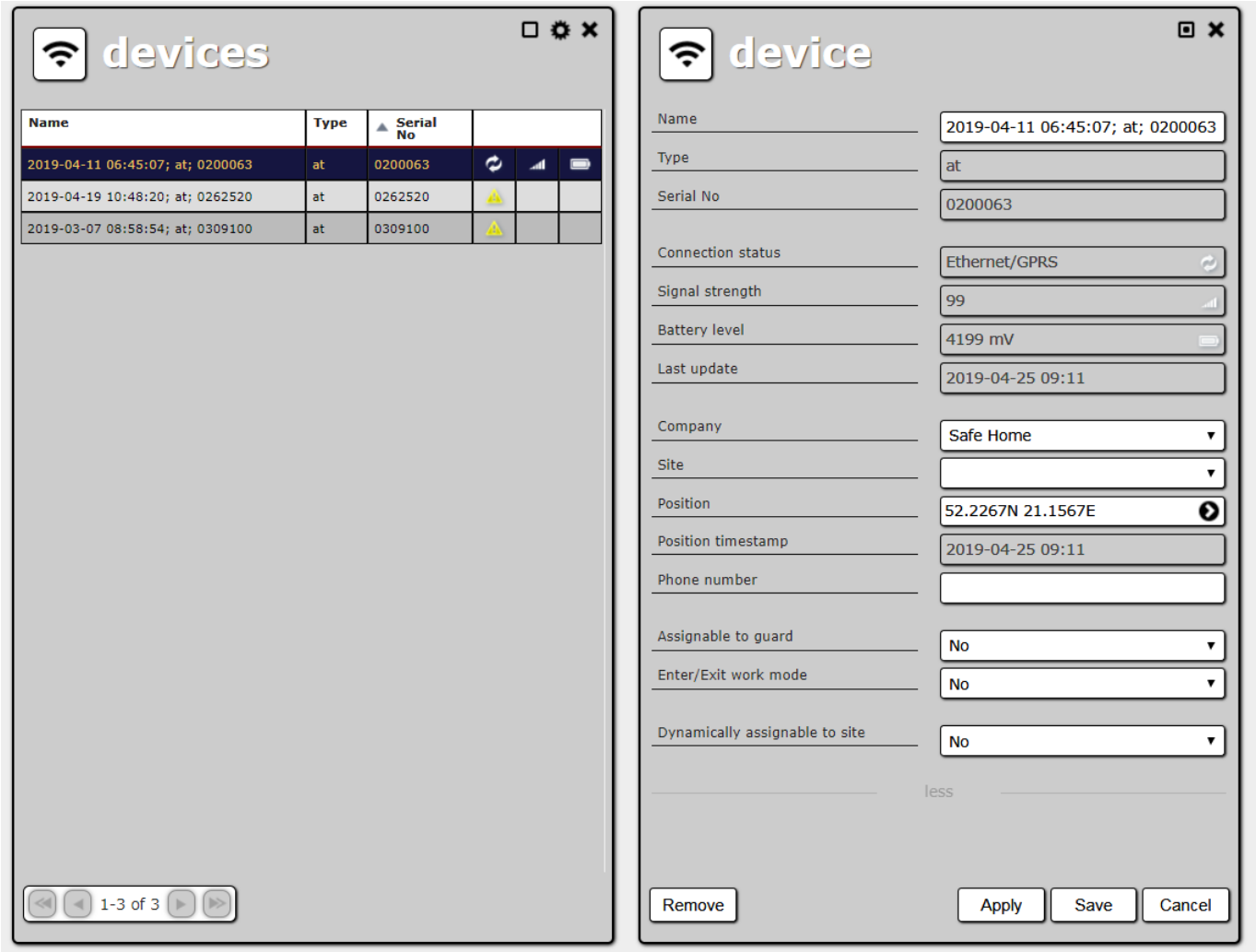
In this list, you can see the current state of all devices (updated automatically, without reloading the page by the user):

- connection status:
  - Ethernet/GPRS
  - SMS
  - Disconnected
- signal strength (no information when the device is disconnected, dimmed when the status is out of date);
- battery level (no information when the device is disconnected, dimmed when the status is out of date).

NOTE:Device configuration should have selected additional data.



You cannot create a new device yourself. It has to be assigned to you by an ActiveView administrator. Then you can edit or remove the device.



Every device has the following properties:

- **Name** – device name. When the device is assigned by the administrator to an organization (a tenant of the ActiveView), it gets a name in the following form: <type>; <serial number>; <date and time>
- **Type** – device type.
- **Serial No** – device serial number. The pair “type – serial number” is always unique.
- **Connection status** – the channel the device is using to connect to the ActiveView. One of the following:
  - Ethernet/ GPRS
  - SMS
  - Disconnected
- **Signal strength** – signal strength of the GSM network. The “?” stands for one of the following:
  - the device is disconnected;
  - the device does not send status information;
  - status information is out of date.
- **Battery level** – battery level of the device. The “?” has the same meaning as for signal strength.
- **Last update** – date and time when the device sent a status information for the last time. The “?” means one of the following:
  - the device is disconnected;
  - the device does not send status information.
- **Company** – the company the device is linked to.
- **Site** – the site this device is linked to.
- **Position** [ActiveTrack only] – shows the current position (latitude and longitude) of the device

(dimmed when the status is out of date). Clicking it opens a new panel with a map (see below).
- **Position timestamp** [ActiveTrack only] – date and time when the device sent its position for the last time.
- **Phone number** – phone number of the device, displayed in alarm details.
- **Assignable to a guard** – if set to “Yes”, the device can be linked to a guard. You can choose the guard manually or you can read a guard’s identifier with it (a special tag assigned to the guard) and it will be linked automatically.
- **Guard** [available if *Assignable to a guard* is set to *Yes*] – linked guard’s name.
- **Enter/Exit work mode** – if set to *Yes*, the device can operate in *Enter work mode* and *Exit work mode*. These modes are changed by reading appropriate tags (see Tags for details). If set to *No*, reading those special tags has no effect.
- **Work mode** [available if *Enter/Exit work mode* is set to *Yes*] – the current enter/exit work mode.
- **Dynamically assignable to site** – if set to *Yes*, reading a checkpoint will automatically link this device to the company and site the checkpoint is connected with.

Active Track Mobile

Active Track Mobile (AT Mobile) application is a universal and intuitive mobile application designed to work with smartphones with Android operating system, version at least 6.0. This product is perfect where no water resistance, shock or damage resistance is required from equipment. It is an alternative mobile solution for standard Active Track devices. As different smartphones offer various hardware functions/options, the AT Mobile app enables only those functions that are supported on the specific smartphone.

The AT Mobile application, together with the Active View platform and the OSM.Server receiver, is a tool for sending, receiving and real-time recording of events from the performed actions, such as:

- sending a PANIC alarm,
- sending a report with a comment and photograph,
- QR code reading,
- NFC tag reading,
- sending information with current GPS position,
- device standstill (Mandown function).

Using Active View, you can:

- register the device on which the AT Mobile application is located,
- configure AT Mobile application settings:
  - define phone numbers that will appear in the application after pressing the handset icon (“Manager's phone number” item),
  - set the frequency of sending GPS position (“GPS interval” item),
  - specify the frequency of checking the device's standstill (“Mandown interval” item
  - enable/disable the shock function (“Enable shock” item);

AT Mobile application status and modes

As previously mentioned, it is necessary to connect the device to Osm.Server for the application to work correctly. The status *“Online”/”Offline”* indicates that the device is connected correctly/incorrectly. *“Standby”/”On Patrol”* application modes are related to the operation/shutdown of functions recording the behaviour of a smartphone. *“On Patrol”* mode means the effective working time during which the device is monitored. In this mode, the option to periodically report GPS location, monitor the device's standstill and rapid movement/impact is active.

AT Mobile Features

- Triggering the *“Panic”* alarm – sends the “Panic” message to request support for a security guard. Available in *“Standby”/”On Patrol”* modes.
- Location sharing function sends the current position of the device. Available in *“Standby”/”On Patrol”* modes.
- QR code read – enables the user to scan a QR code tag. Available in *“Standby”/”On Patrol”* modes.
- NFC code read – enables the user to scan a NFC code tag. Available in *“Standby”/”On Patrol”* modes.
- Making an emergency call to the phone numbers previously defined in ActiveView. Available in *“Standby”/”On Patrol”* modes.
- Sending a text report with a photograph to ActiveView. Several report types are available for selection, indicating the reason for the report being sent. Moreover, it is possible to take a photograph directly from the app or add a photograph in the smartphone's memory. Available in both *“Standby”/“On Patrol”* modes.
- Temporary location sharing function allows to send the current device position in a regular manner. Available only in the *“On Patrol”* mode
- Non-activity monitoring (Mandown) – monitors the non-activity of the device. It the device remains motionless for longer than defined, the function sends a signal. Available only in the *“On Patrol”* mode.

Device enrolment

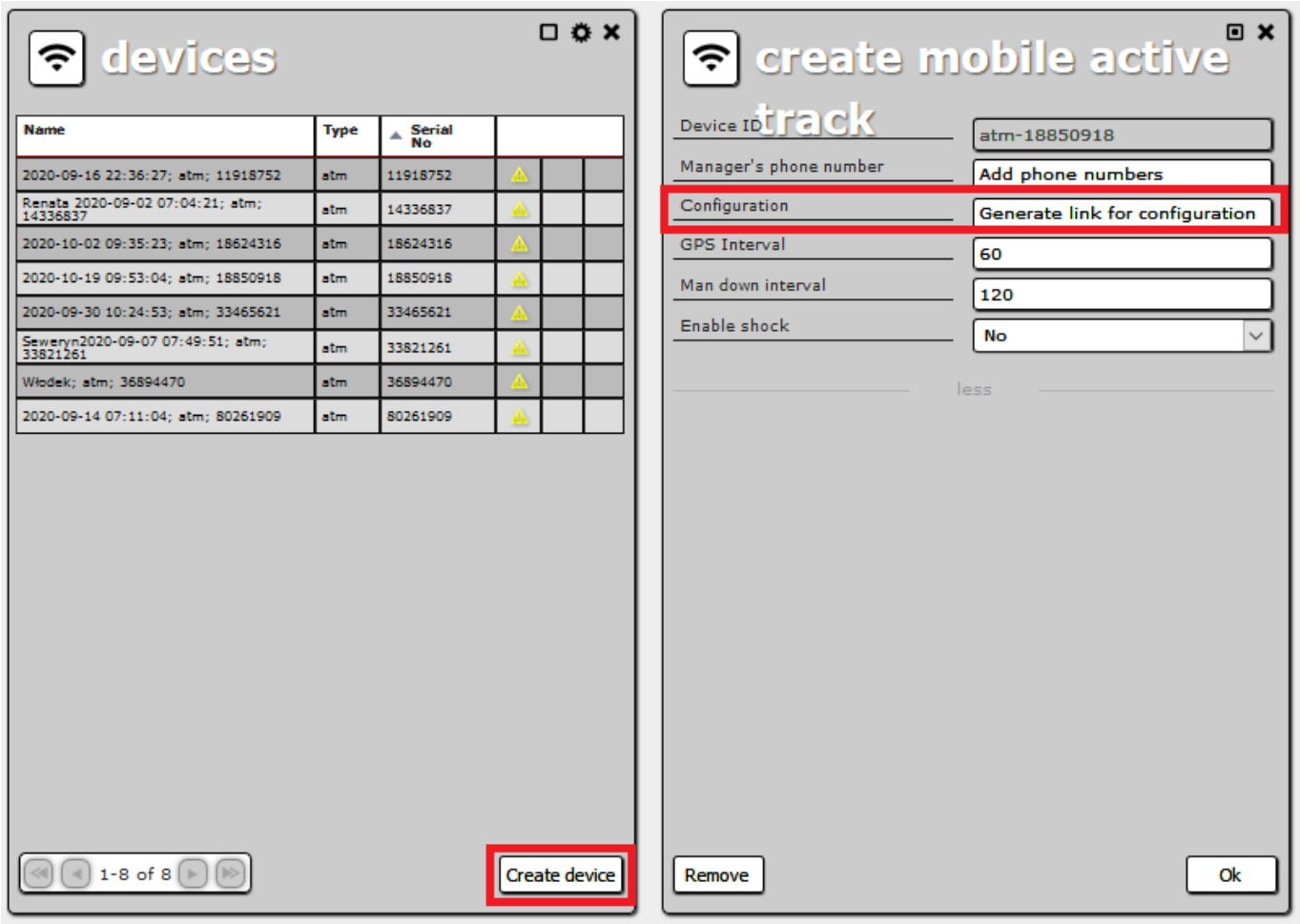
An AV user with adminstration rights can add a new device in the following tab: “Administration”→ “Devices” →“Create device”. A new device will appear in the list on the left, while a new window with an automatically created profile of a given device will appear on the right.

Set the available options as follows:

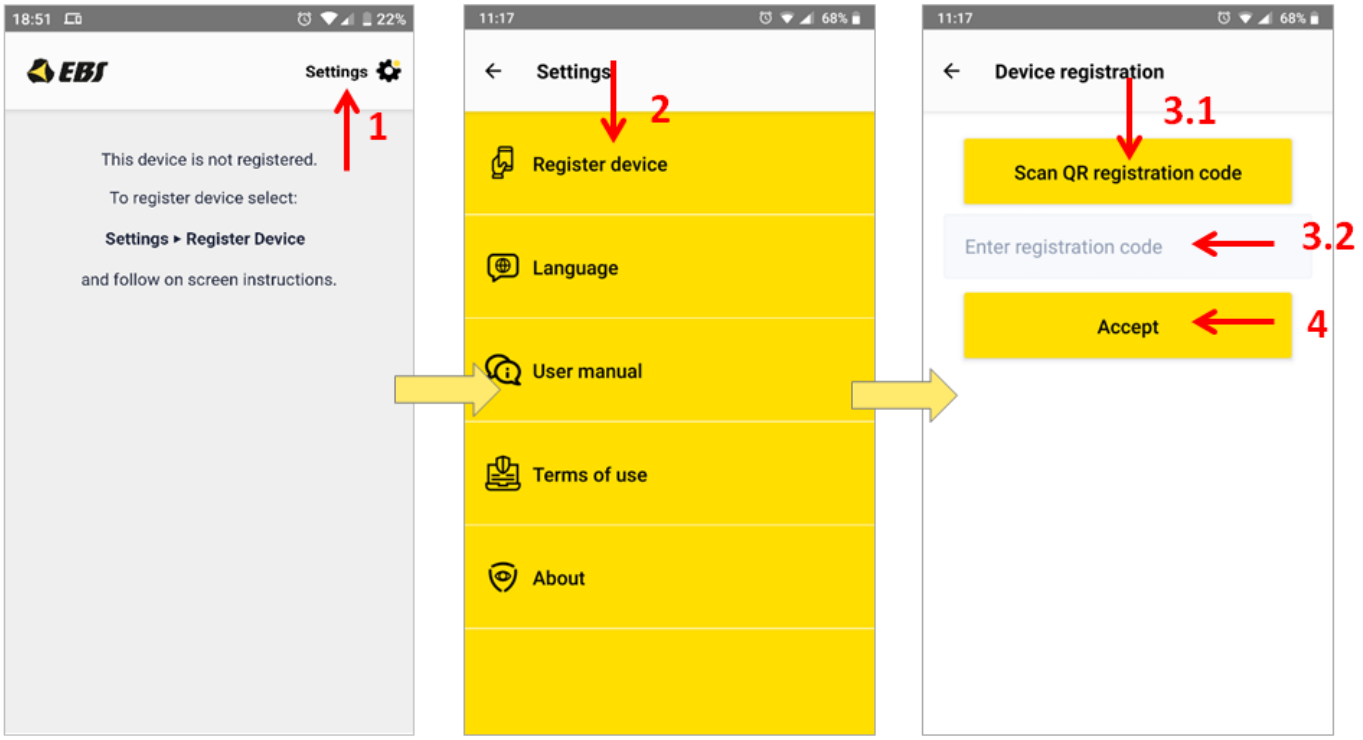
- *Add phone numbers* - define the list of phone numbers that will be available in the AT Mobile application when trying to make an emergency call;
- *Configuration* - Generating QR code for device registration (see description below);
- *GPS interval* – defines how often (in seconds) the position of the device in the “On Patrol” mode should be sent;
- *Mandown interval*; - setting the time after which the device is stopped to send such information to ActiveView;
- *Manager's phone number* - define the list of phone numbers that will be available in the AT Mobile application when trying to make an emergency call;
- *Enable shock* - Activates/disables the monitoring of sudden shocks and falls.

To register a device correctly (in this case a smartphone), click on *“Generate link for configuration”* in

the *Configuration* field. The QR code will appear on the screen and below the configuration code link.



In order to register a device in the AT Mobile application (after downloading from the Google Play Store and starting it), select *Settings* from the main screen (item 1) , then *Register device* (item 2), and then scan the QR number from Active View (item 3.1) or paste a link with the configuration code (item 3.2). When finished, click *Accept* button.



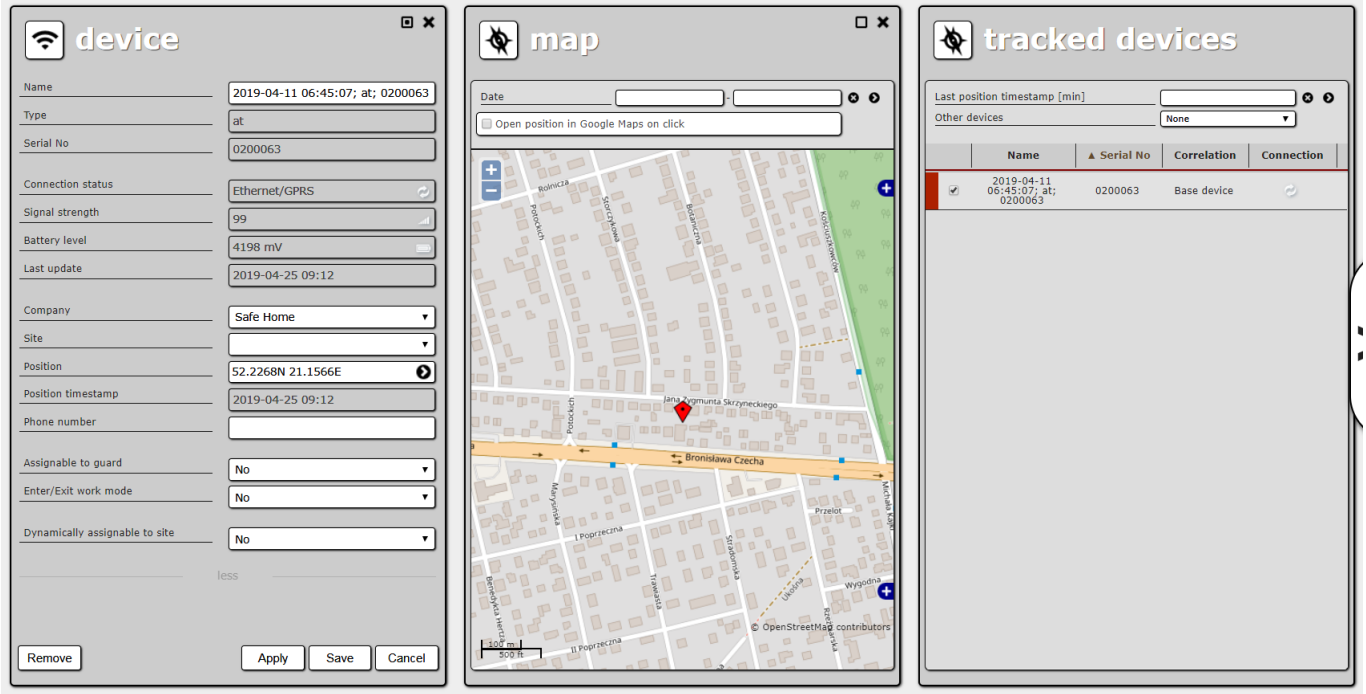
Connection status

The device connection status depends on the last event sent by the device. The rules are as follows:

- the device sent any event other than *SMS_RECEIVED*, *DISCONNECT*, *STILL_DISCONNECTED* and *TIMEOUT* – status changes to *GPRS*;
- the device sent an *SMS_RECEIVED* event – status changes to SMS (text messages);
- the device sent a *DISCONNECT*, *STILL_DISCONNECTED* or *TIMEOUT* event – status changes to *Disconnected*;
- the device has not sent any events over a period defined by the administrator (e.g. for five minutes) – status changes to *Disconnected*.

Device on a map

Clicking on the position option on an ActiveTrack details panel opens a new panel with a map showing the current location of the device.



Above the map there is a date range filter. Choose appropriate dates and click the **>** button to view the device's trace from the chosen date range.

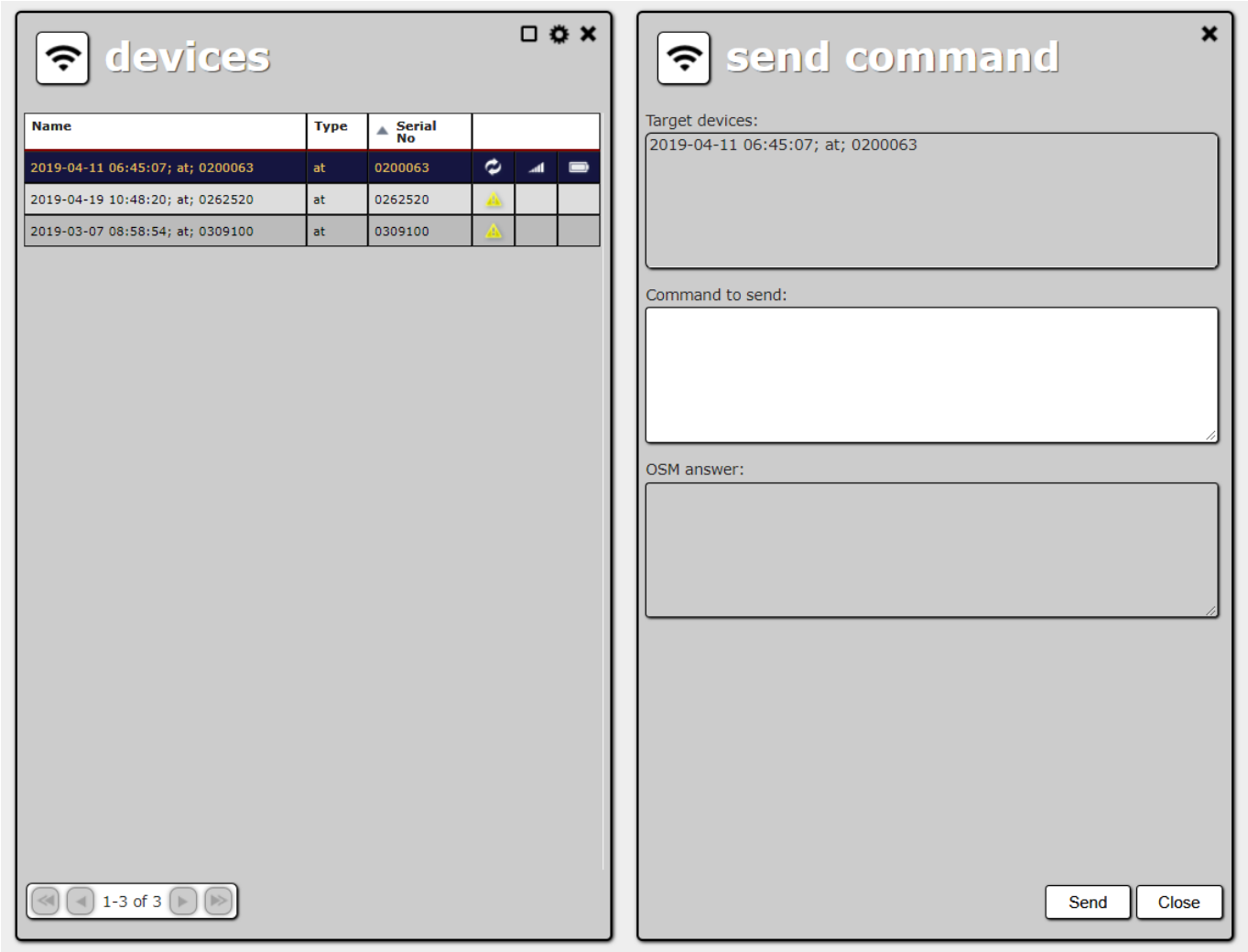
The trace is limited to number of nodes set in the user settings (the default is 100; see User settings for details). If there are more locations of the device recorded, they are filtered evenly. If you need more precision, try narrowing down the date range.

You can click on a node to see some details, like time and date, exact position, speed, etc.

Sending commands

You can select one or more devices and send a command to them. To do this, use *Send command via OSM* from the context menu or from the tools menu.

NOTE: *OSM* is a special software ActiveView uses to communicate with devices. List of commands find in device manual. The commands use without service code infront.



The **Send command panel** contains the following elements:

- **Target device list** – list of devices which the command will be sent to.
- **Command to send** – this text will be sent to the devices as a command when you choose the Send option.
- **OSM answer** – answers from devices which OSM sent to ActiveView. If you close the panel before these answers arrive, you will not be able to see them (the answers will be lost).

Removing a device

Removing a device does not affect past events or alarms. They are still available unchanged in the alarms browser and in the reports.

NOTE: You cannot open the details of a deleted device, so it is impossible to see its past trace from there. Events and alarms report, however, has an option to show events on a map. See Events and alarms report for details.

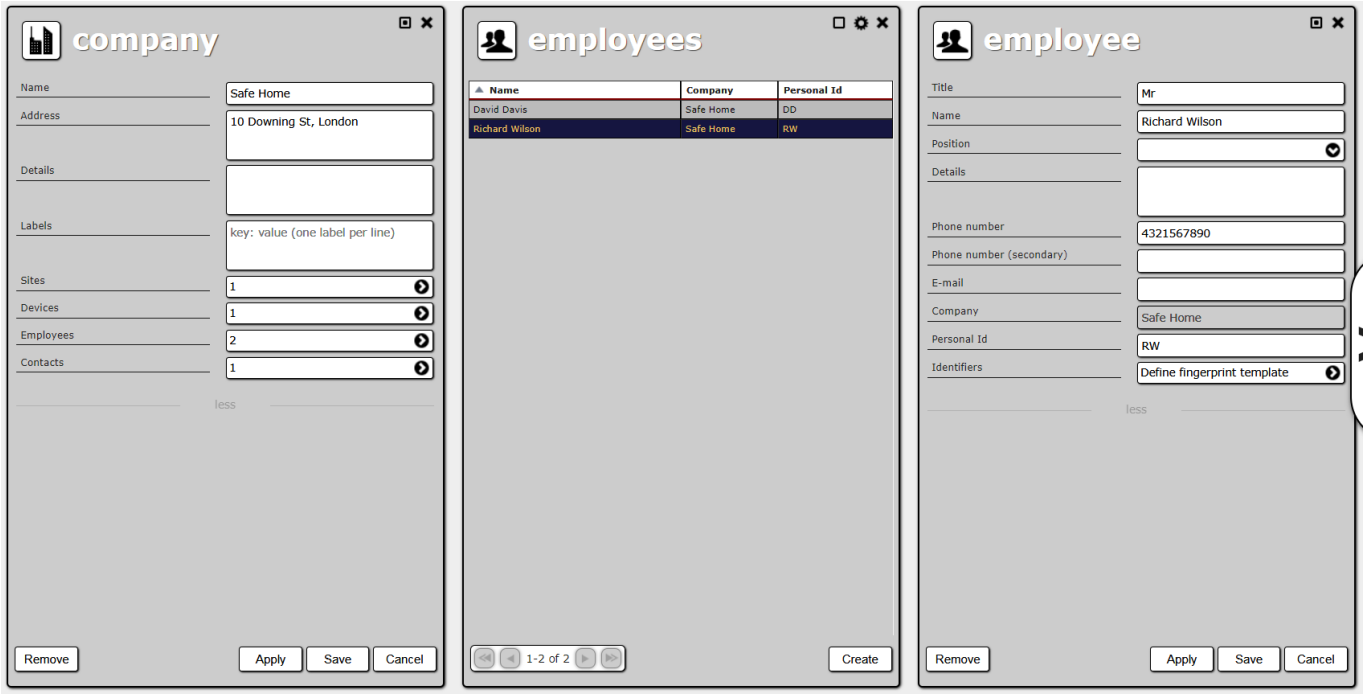
Employees

A company in ActiveView has a list of employees. Combined with employee identifiers and ActiveGuard devices, it can be used to keep track of employees' work time.

There are two ways in which you can open an employee list:

- select *Management* → *Employees* in the main menu to open a complete employee list (i.e. a list of employees of all companies);
- click *Employees* on the company details panel to open the company's employee list.

In both lists, you can create a new employee and edit or remove an existing one.



Every employee has the following properties:

- *Title*
- *Name* – employee name. It has to be unique within the employee's company.
- *Position*
- *Details*
- *Phone number*
- *Phone number (secondary)*
- *E-mail*
- *Company* – the employee's company. It is set when the employee is created and cannot be changed later.
- *Personal Id*
- *Identifiers* - employee's identifiers (e.g. employee badge or fingerprint template)

After you have created an employee, you can assign an employee identifier. See Tags or FPX-finger print for details.

Removing an employee

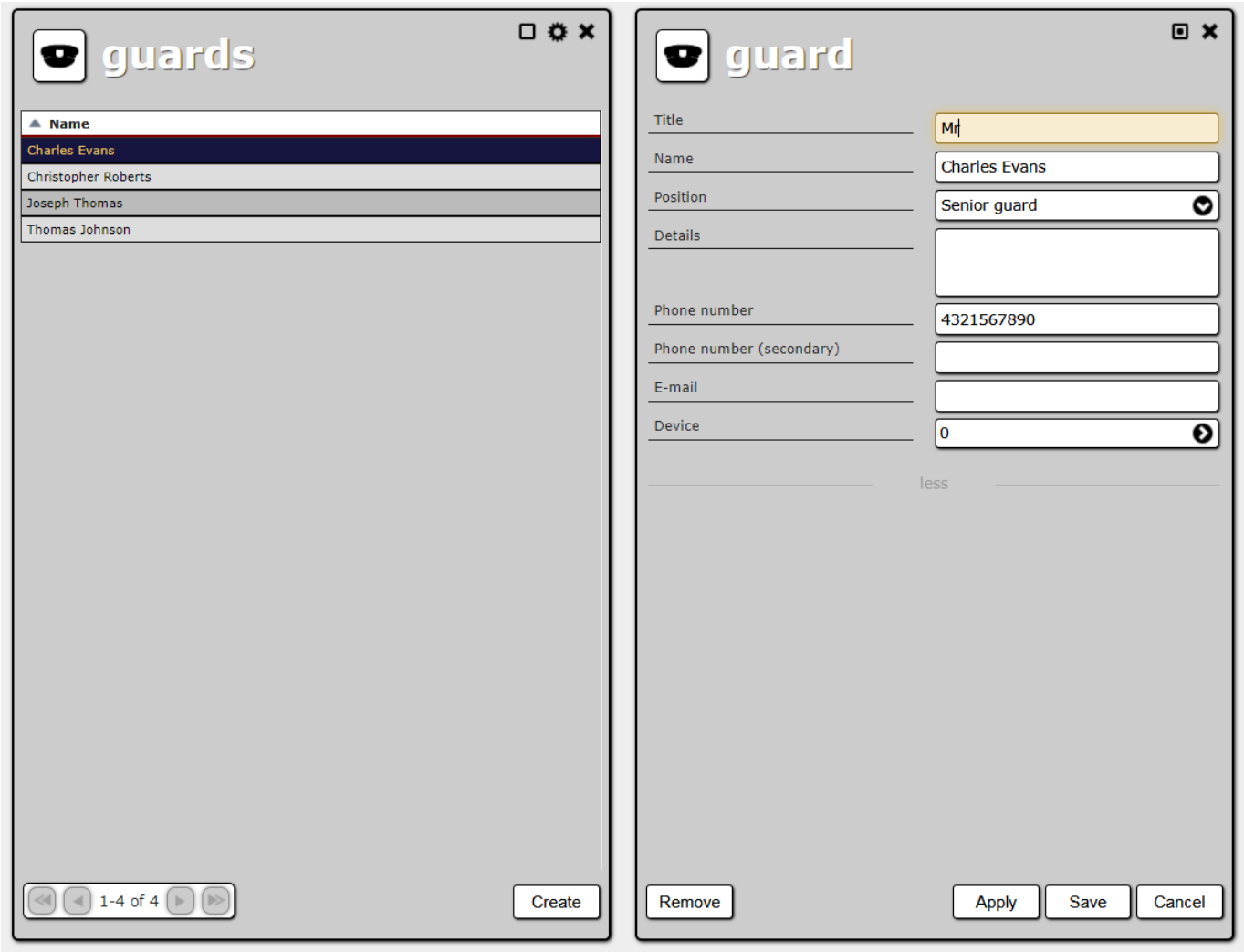
Removing an employee does not affect past events. They are still available unchanged in the alarm browser and in the reports.

Guards

In ActiveView, devices can be linked to guards. This allows keeping track of guard activity, especially patrols.

To open the guard list, select *Management* → *Guards* in the main menu.

You can create a new guard and edit or remove an existing one.



Every guard has the following properties:

- *Title*
- *Name* – a unique guard name.
- *Position*
- *Details*
- *Phone number*
- *Phone number (secondary)*
- *E-mail*
- *Devices* – displays the number of devices linked to this guard. Clicking it opens a new panel with a list of these devices.

You can link a device to a guard in the device details. See Devices for details.

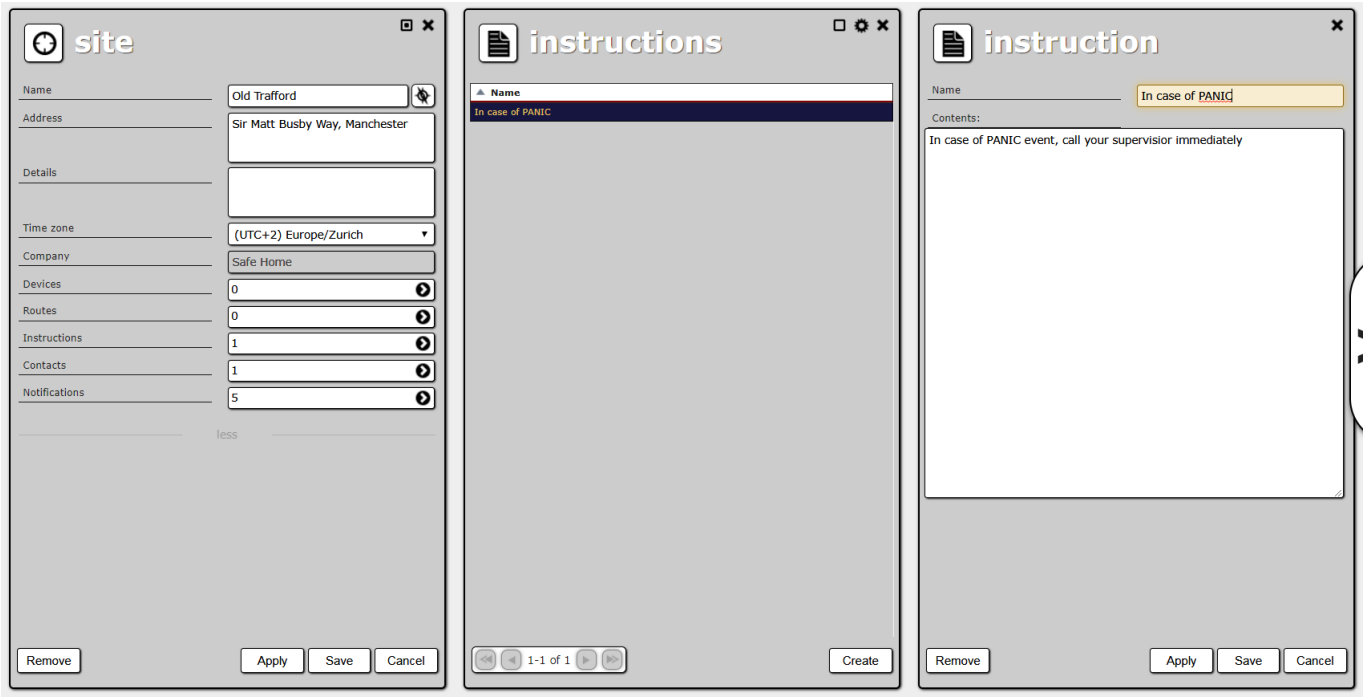
Removing a guard

Removing a guard does not affect past events or alarms. They are still available unchanged in the alarms browser and in the reports.

Instructions

A site in ActiveView has a list of instructions. Instructions can be used to provide operator with information on how to react in various situations (e.g. PANIC event or missed patrol).

You can access instructions list from site details panel - just click *Instructions* button.

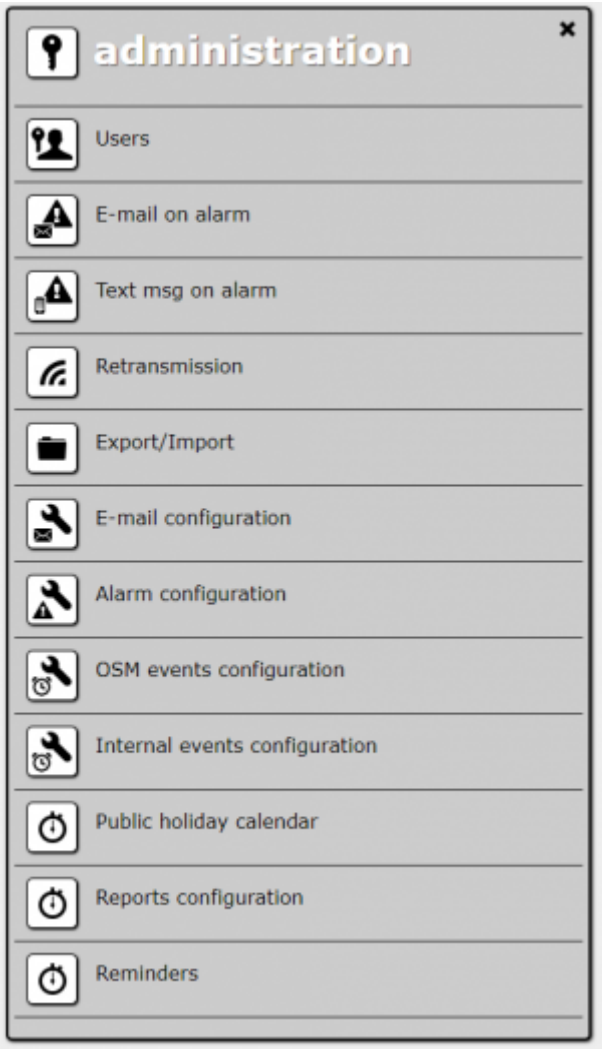


Every instruction has two properties:

- *Title*, which summarizes instruction contents,
- *Contents*, instruction itself.

Administration

ActiveView can be customized by the user to match the needs of his or her organization better. Customization options are grouped in the Administration section of the application. To open it, choose *Administration* from the main menu.



The administration options are divided into the following categories:

- Users
- E-mail on alarm
- Text message on alarm
- Retransmission
- Export/Import
- E-mail configuration
- Alarm configuration
- OSM events configuration
- Internal events configuration
- Public holiday calendar
- Raports configuration

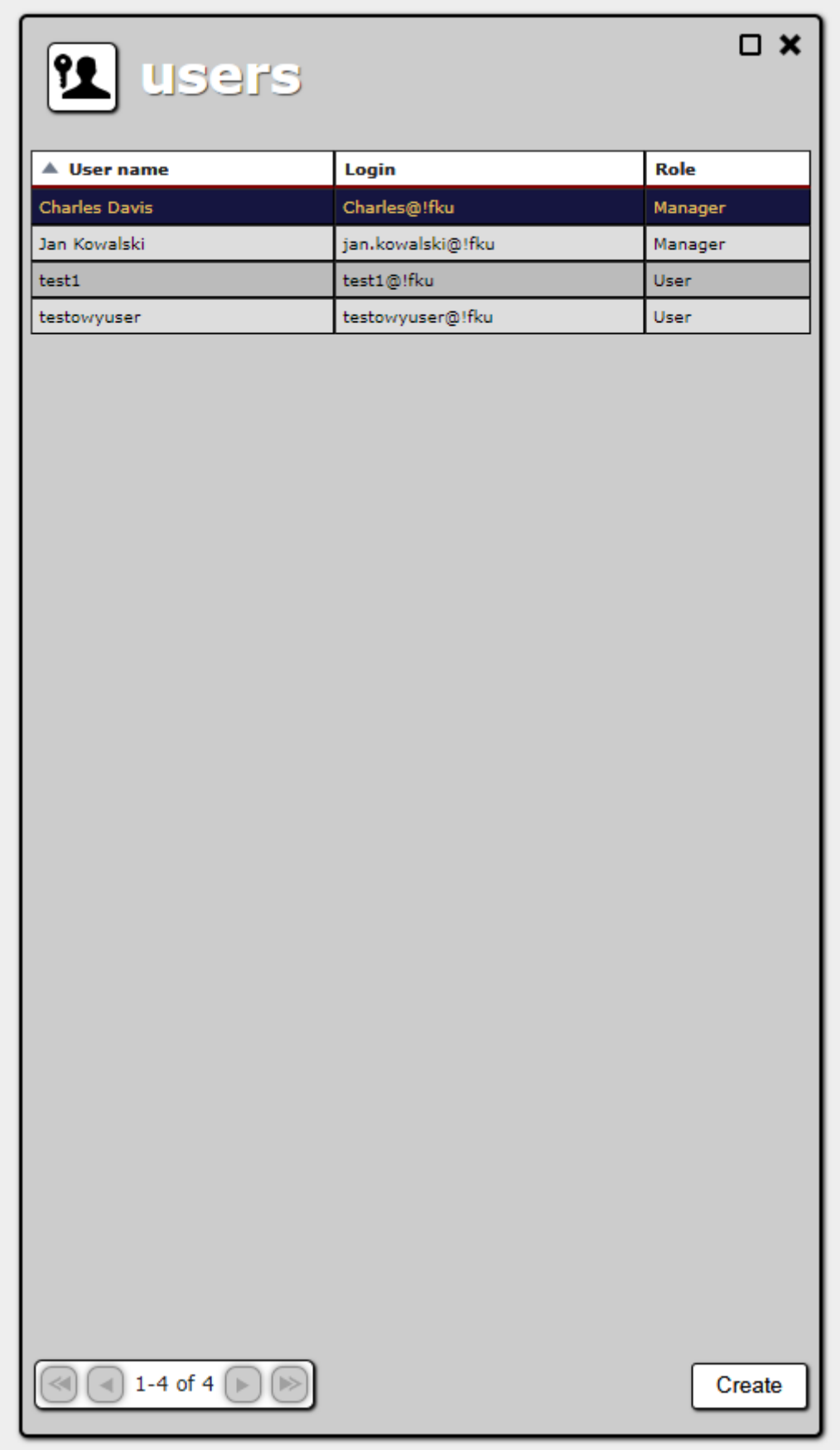
- Reminders

Users

Every person that uses Active View online platform needs to have an authorized account profile with login name and specified password. There is a different levels of access to that platform.

To open the application user list, select *Administration* → *Users* from the main menu.

You can create a new user and edit or remove an existing one.



Types of users

There are three types of users:

- *Manager*,
- *User*,
- *End User*.

Manager

A *Manager* has access to all ActiveView functionalities (except administration on the server side).

Example: Security company ARC manager or office manager.

User

A *User's* responsibility is to process alarms. This type of user has access to:

- *Alarms section,*
- *Reports section, without periodic alarms.*

Example: Security company operator working at ARC.

End user

An *End user* represents someone who has contracted the security agency to protect his/her company.

This type of user always has a company assigned. He/she can have access to all or some of the company's sites. He/she is allowed to view events and alarms only from these sites and from devices linked to them.

An *End User* can view (but not modify in any way):

- *alarms* – he/she can browse and search for alarms, but cannot open alarm details or perform any action on an alarm;
- *reports* – he/she can generate reports on demand, but cannot view or configure periodic reports;
- the company that is assigned to him/her (with additional details, like contacts);
- *employees of the company*;
- *sites he/she has access to (with additional details, like contacts);*
- *routes for these sites;*
- *devices linked to these sites.*

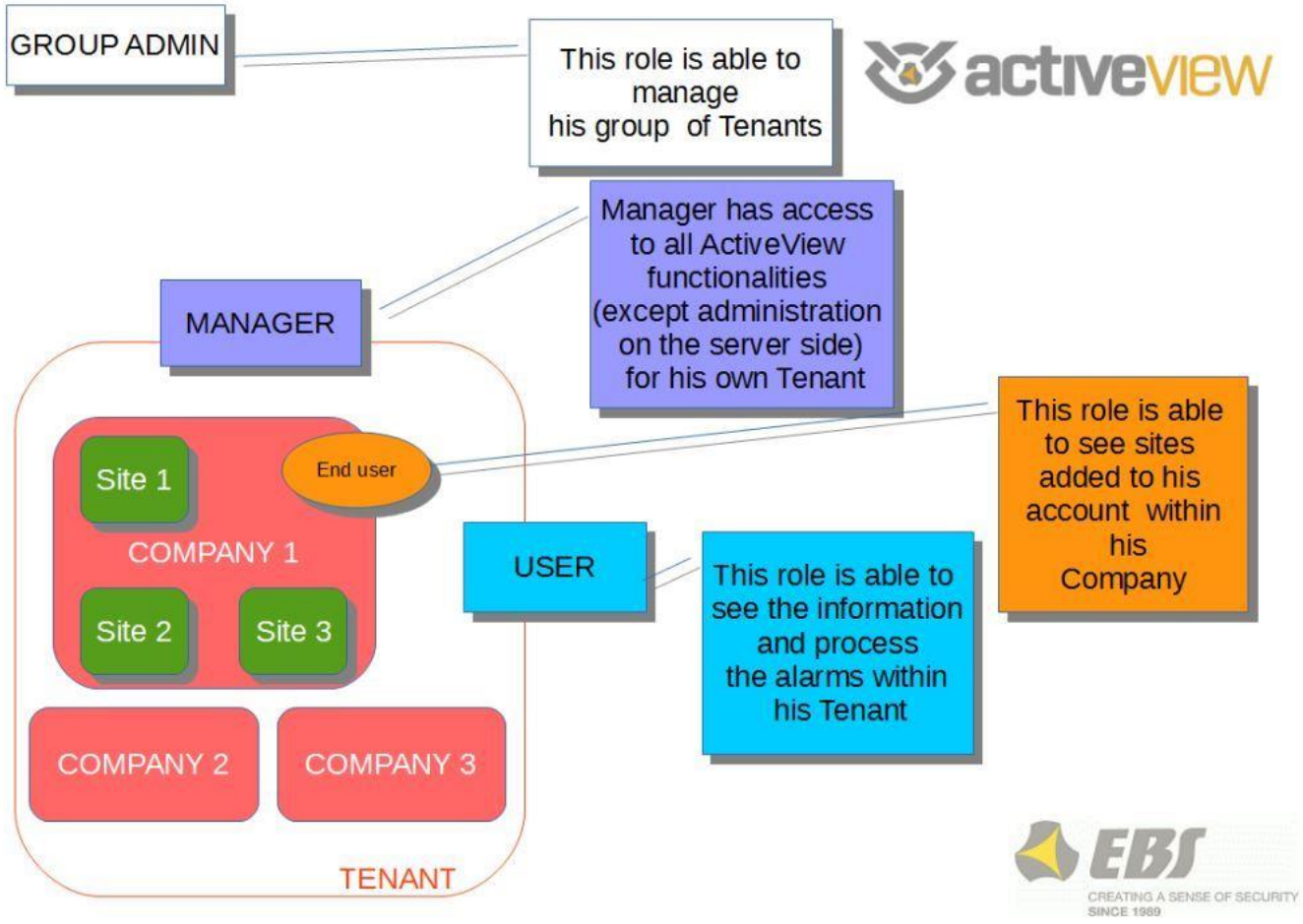
Example: Employee of the customer that is authorized to control security company and the services they provide with our equipment.

User details

Every user has the following properties:

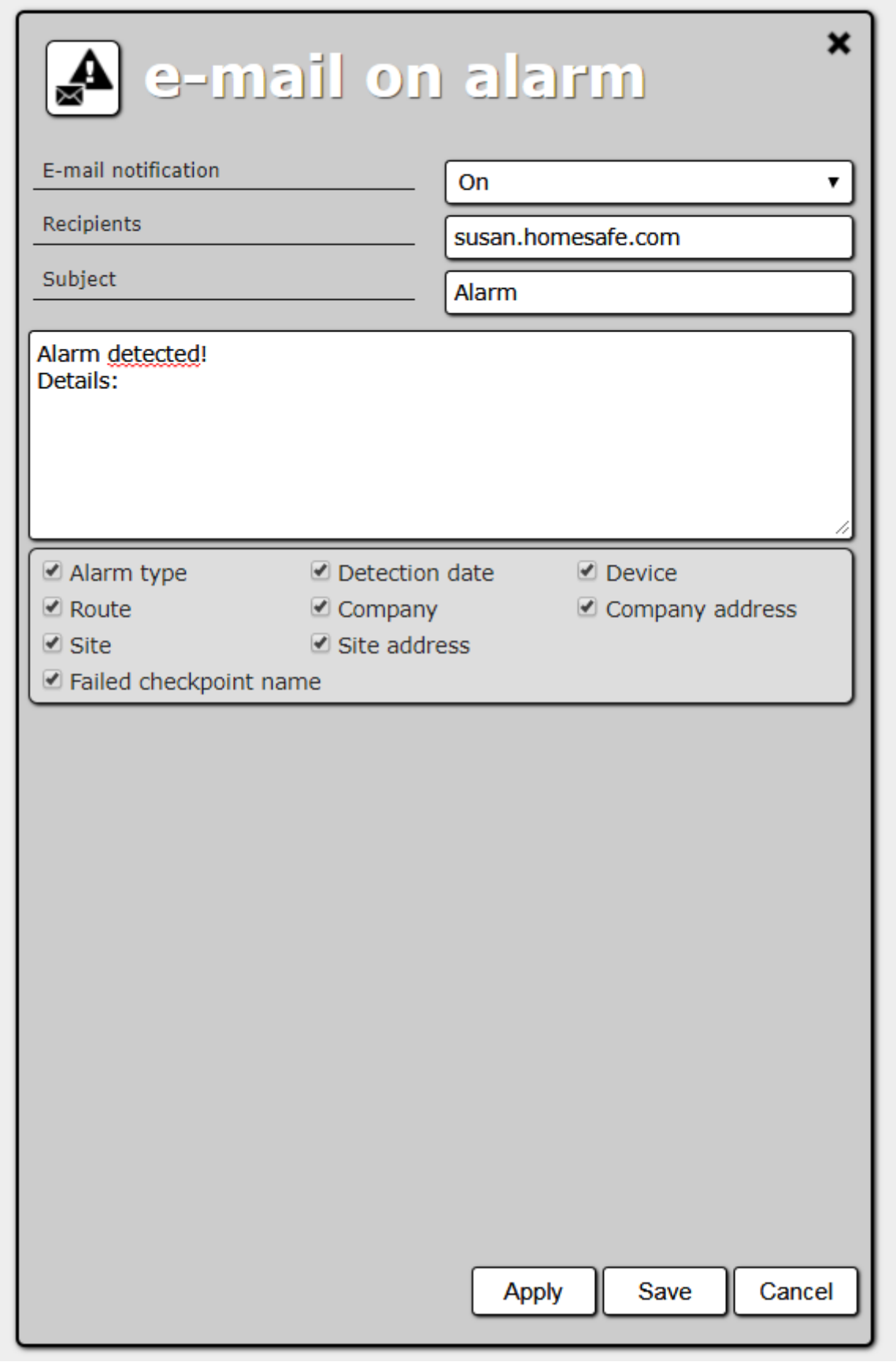
- **Login** – blank characters and the @ (at) character are not allowed.
- **Name**
- **Password** – to avoid errors, it has to be entered twice when a user is created.
- **Role** – type of user.
- **Company** [available if *Role* is set to *End user*] – a company assigned to the user.
- **Sites** [available if *Role* is set to *End user*] – a list of the company's sites (down arrow opens the list, "check" button selects all, X button clears selection); the end user has access to those which are selected.
- **Visible events** [available if *Role* is set to *End user*] – a list of all events and alarms (down arrow opens the list, "check" button selects all, X button clears selection); the end user sees only those which are selected.

NOTE: When a user logs in to the application, he/she must use his/her login and a code of the organization he/she works for, separated with the @ character. For example, a user called John who works for EBS should log in as *john@ebs*.



E-mail on alarm

ActiveView can send an e-mail whenever it detects an alarm. To configure this feature, select *Administration → E-mail* on alarm from the main menu.



In the **e-mail on alarm configuration**, you can change the following settings:

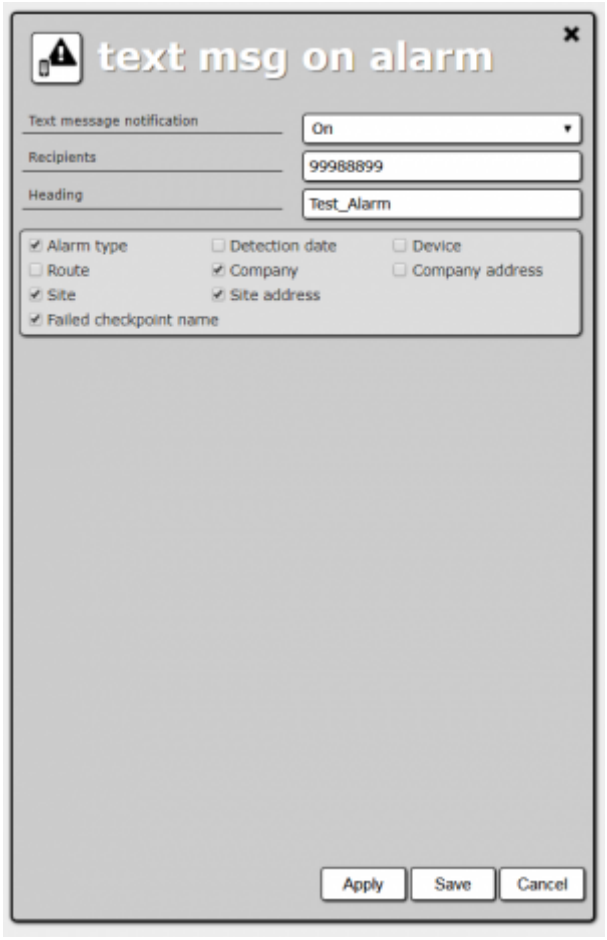
- *E-mail notification* – decides if e-mail notifications are sent (on) or not (off).
- *Recipients* – recipients' e-mail addresses, separated by commas.
- *Subject* – the subject of e-mails which will be sent.
- *Heading* (a text box without a label) – fixed text put at the beginning of e-mails which will be sent.

- *Contents* (a series of checkboxes) – you can choose which pieces of information about the alarm the e-mail will contain. Not all information types apply to every alarm, e.g. there is no route name for a Panic alarm. If you select *detection date*, then it will be expressed in site time zone, if the alarm comes from a particular site, or server time zone, if it doesn't (i.e. comes from a device not linked to a site).

NOTE: In the alarm list, alarms are combined (grouped) together (one group per site). This is not the case with e-mail notifications. An e-mail is sent for every new alarm irrespective of the site it comes from.

Text message on alarm

ActiveView can send a text message whenever it detects an alarm. To configure this feature, select *Administration → Text msg on alarm* in the main menu.



In the **Text msg on alarm configuration**, you can change the following settings:

- *Text message notification* – decides if text message notifications are sent (on) or not (off).
- *Recipients* – recipients' phone numbers, separated by commas.
- *Heading* – fixed text put at the beginning of text messages which will be sent.
- *Contents* (a series of checkboxes) – you can choose which pieces of information about the alarm the text message will contain. Not all information types apply to every alarm, e.g. there is no route name for a *Panic* alarm.

If the message that is generated exceeds 160 characters, it is divided and sent in as many text messages as needed.

Besides recipients set in the *Text msg on alarm configuration*, notification text messages are sent to site contacts (if text message notifications are turned on). More specifically, if:

- an alarm occurs from a site, and
- a contact person is linked to this site, and

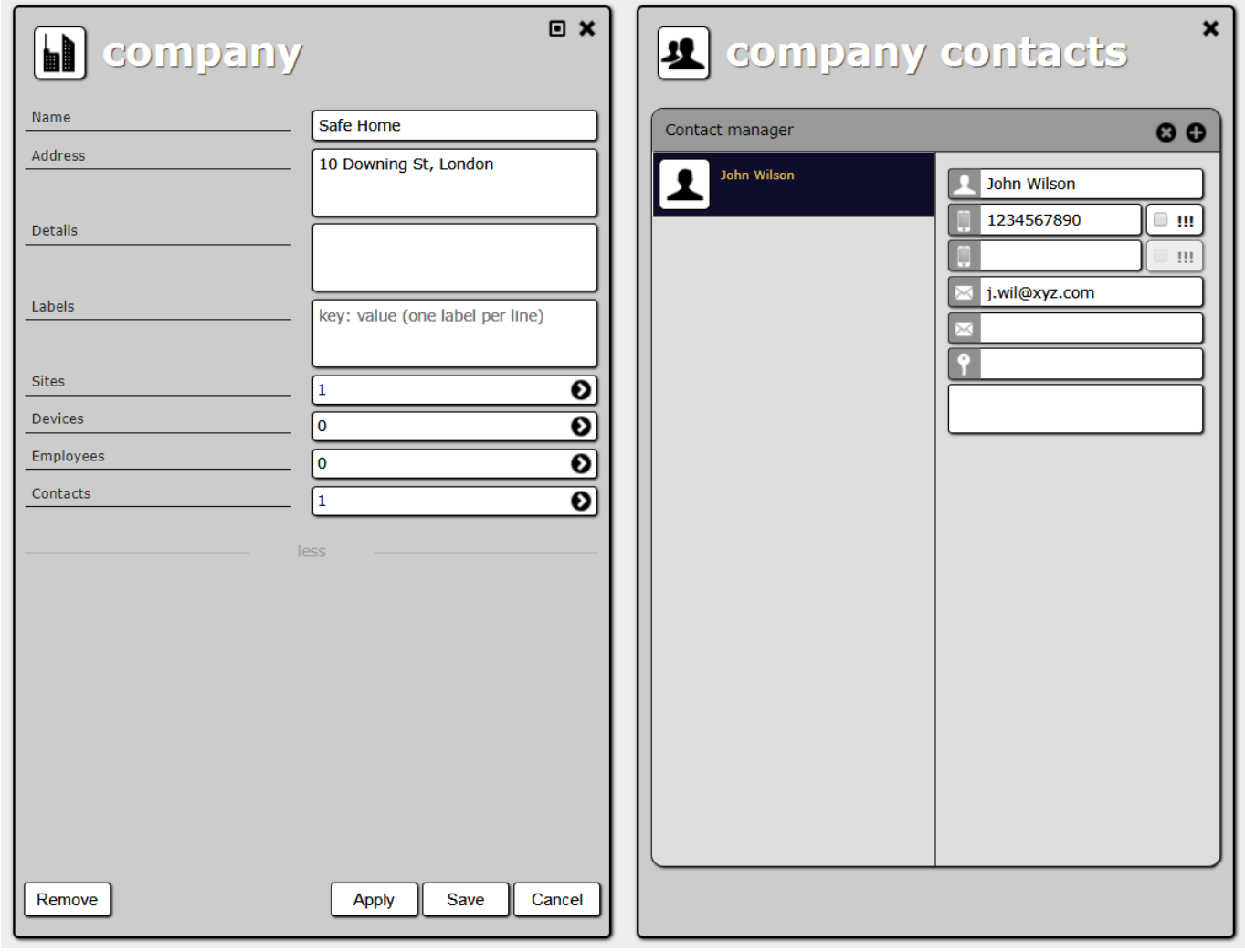
- the contact person has sending text message notifications turned on for any of his or her phone numbers,

then a text message notification is sent to that number (or numbers).

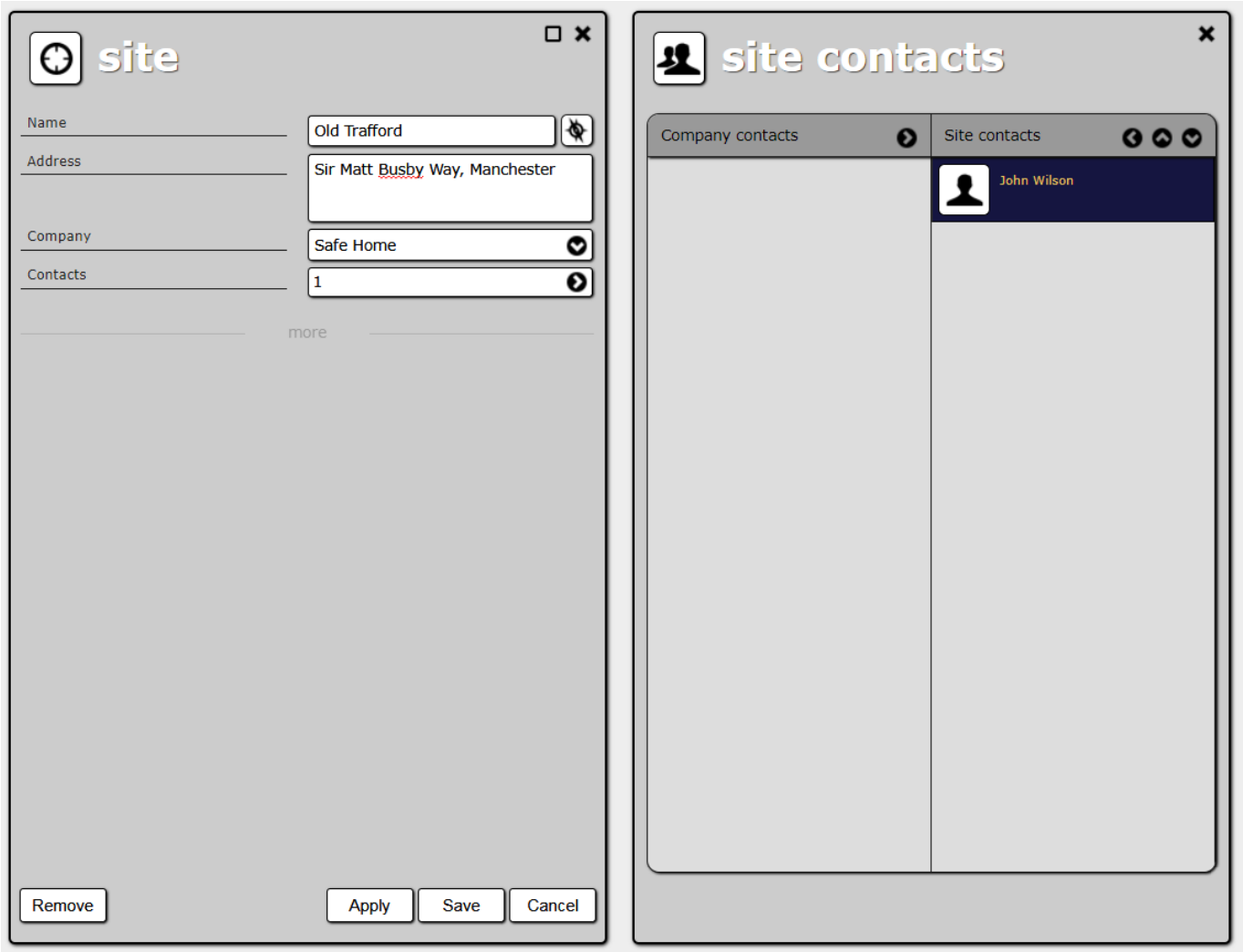
NOTE: In the alarm list, alarms are combined (grouped) together (one group per site). This is not the case with text message notifications. A text message is sent for every new alarm irrespective of the site it comes from.

SMS notification are for devices added to company and site.

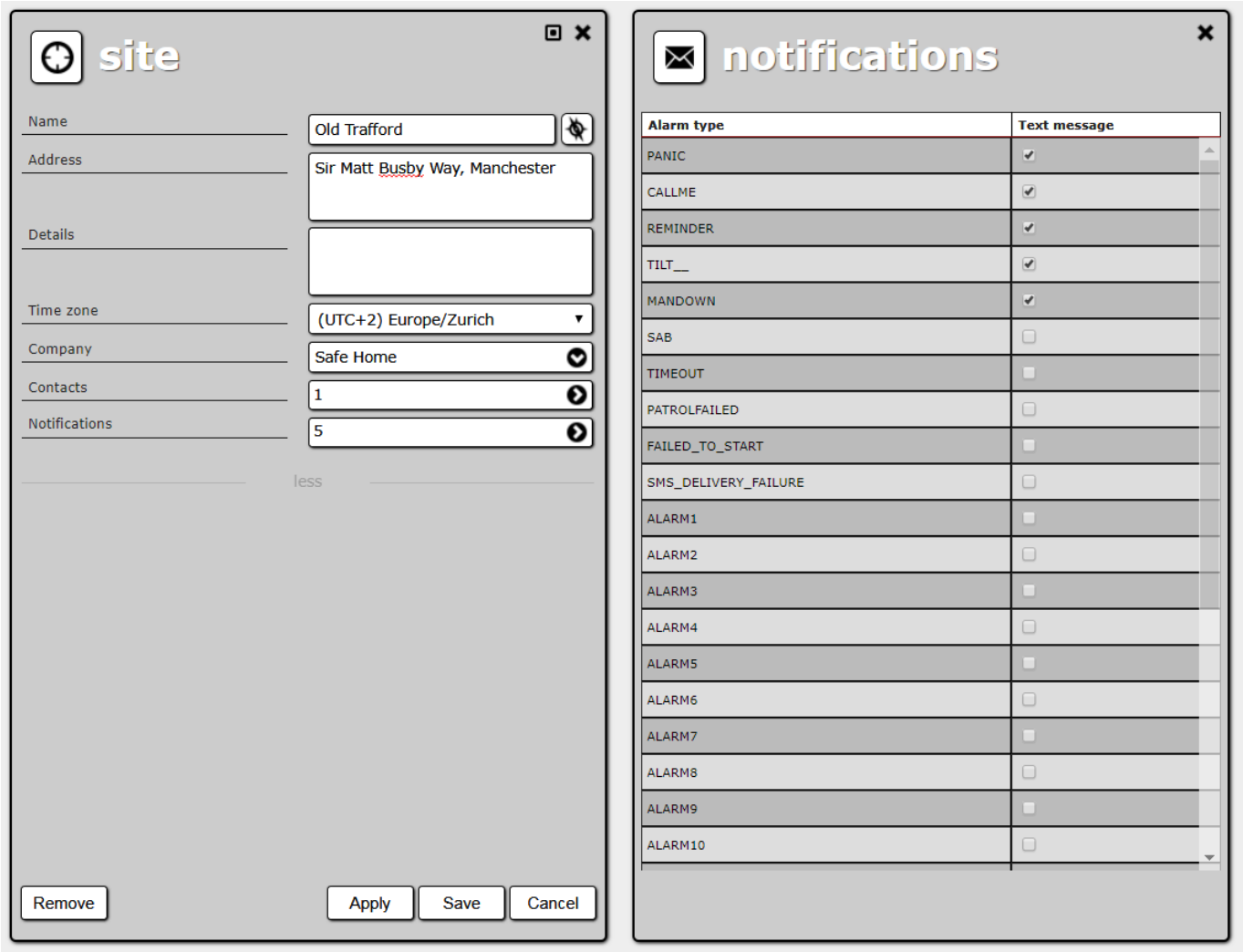
If you want recive SMS notification for choosen sites. Please add contact to company, set up a SMS notification (chceckbox).



Contact add to site.



Choose which notification you need for site.



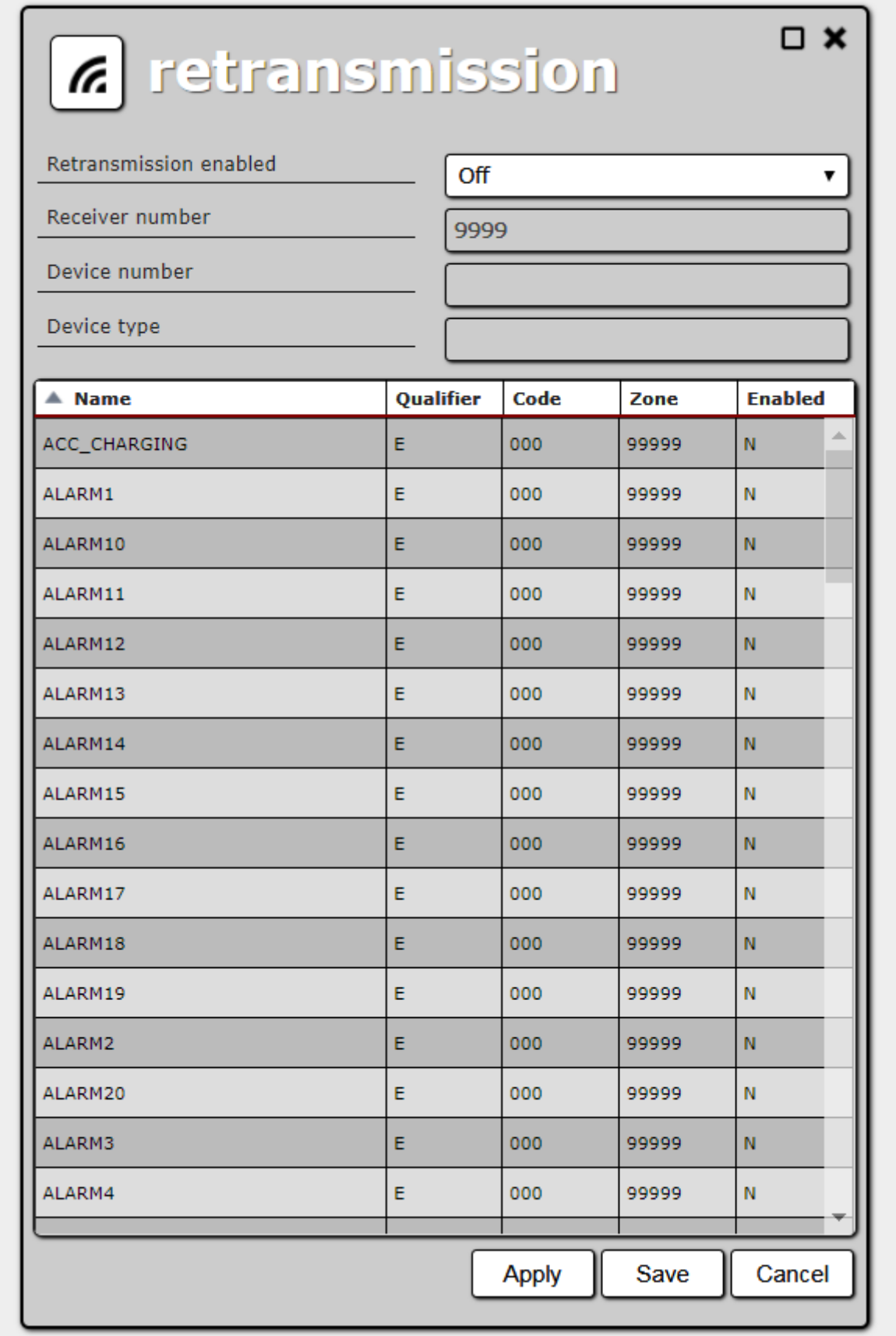
NOTE: SMS notification works only when account have dedicated device for sending notification (transponder). To activate it please contact system administrator and supply information about account name and serial number of device to be used as transponder.

Retransmission

Retransmission - retransmission of telecommunication packets that have been damaged or lost. This is the basic mechanism used by communication protocols to ensure reliable communication. Protocols that ensure reliable communication in such networks use retransmission of missing and/or damaged packets to ensure reliability.

ActiveView can retransmit events and alarms using the Surguard protocol. Surguard messages are sent through a dedicated device. Client software which understands the Surguard protocol should be connected to the device. If you want to start using this functionality, contact your ActiveView administrator. Retransmission can be enabled for devices ex20.

Retransmission configuration allows you to set parameters used in Surguard messages. To open it, select *Administration → Retransmission* from the main menu.



Retransmission configuration

Retransmission configuration panel contains the following elements:

- **Retransmission enabled** – decides if retransmission is on or off.
- **Receiver number** – a four-digit number. A constant part of every Surguard message (see below).
- **Device number** – serial number of the device used by ActiveView to send Surguard messages (read only, defined by the administrator).
- **Device type** – type of the device used by ActiveView to send Surguard messages (read only, defined by the administrator).
- **events/alarms list** – a list containing all possible events and alarms. It comprises the following columns:
  - **Name** – event/alarm name.
  - **Qualifier** - event/alarm retransmission qualifier (for usage see below).
  - **Code** – event/alarm retransmission code (for usage see below).
  - **Zone** – zone assigned to event/alarm (for usage see below).
  - **Enabled** – if ticked the event/alarm is retransmitted.

Surguard messages

Surguard (Contact ID) messages sent by ActiveView have the following form:

```
5RRLLs18AAAAQXXXYYZZZ
```

The RRLL part is event/alarm-independent. It is the receiver number set in the retransmission configuration.

The meanings of other parts depend on the type of the event/alarm:

- patrol start/end:
  - AAAA – retransmission code of the site
  - QXXX – qualifier and code of the event (see above)
  - YYZZZ – retransmission code of the route
- checkpoint passed:
  - AAAA – retransmission code of the site
  - QXXX – qualifier and code of the event (see above)
  - YYZZZ – retransmission code of the checkpoint
- patrol failed, simple route:
  - AAAA – retransmission code of the site
  - QXXX – qualifier and code of the alarm (see above)
  - YYZZZ – retransmission code of the route
- patrol failed, advanced route:
  - AAAA – retransmission code of the site
  - QXXX – qualifier and code of the alarm (see above)
  - YYZZZ – retransmission code of the route
- alarm/event from a device linked to a site:
  - AAAA – retransmission code of the site
  - QXXX – qualifier and code of the event/alarm (see above)
  - YYZZZ – retransmission code of the device
- alarm/event from a device not linked to a site:
  - AAAA – 4 last digits of retransmission code of the device
  - QXXX – qualifier and code of the event/alarm (see above)

- YYZZZ – retransmission code of the device

Export/Import

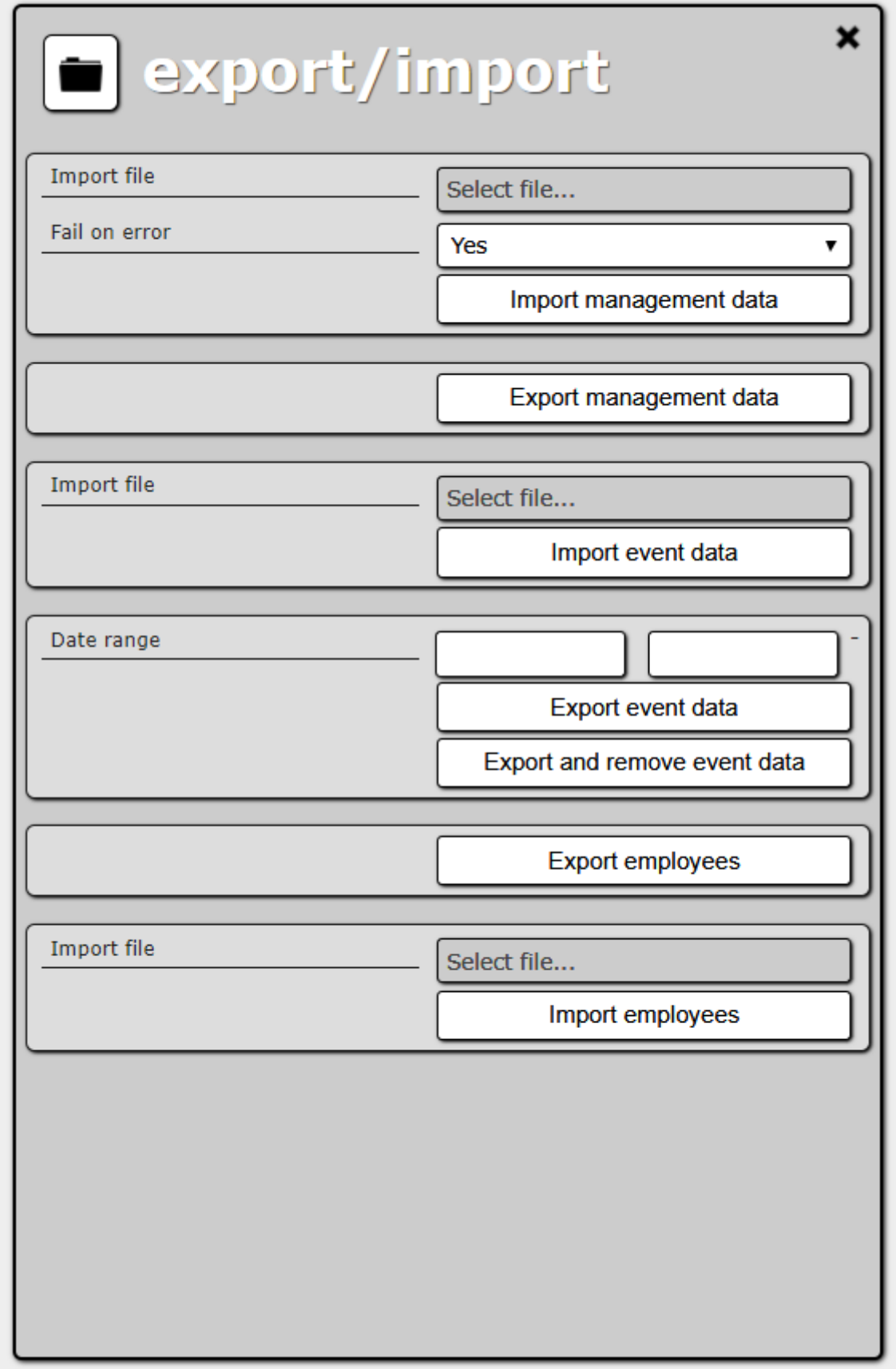
ActiveView can export and import data in an XML format.

Data stored by ActiveView can by divided into two categories:

- Management data, such as companies, sites, devices, etc. These data are relatively constant and of small volume. Imort of those data is idempotent. It means that import of existing that casue that no changes will happen.
- Events received from devices and generated by the application. These data, on the other hand, grow in time (the more devices are connected to the application, the faster they grow). Import of those data isn't idempotent. If you want to re-import event you need to remove the existing one or event will be duplicated.

You can export and import these two types of data separately.

To export/import data, select *Administration* → *Export/Import* in the main menu.



The **Export/import panel** contains the following elements:

- Import management data section:
  - **Import file** – opens a dialog box where the user can choose the file to be imported.
  - **Fail on error** – *No* means ActiveView will skip data with errors and continue importing the file. *Yes* means no data will be imported if there are any errors.

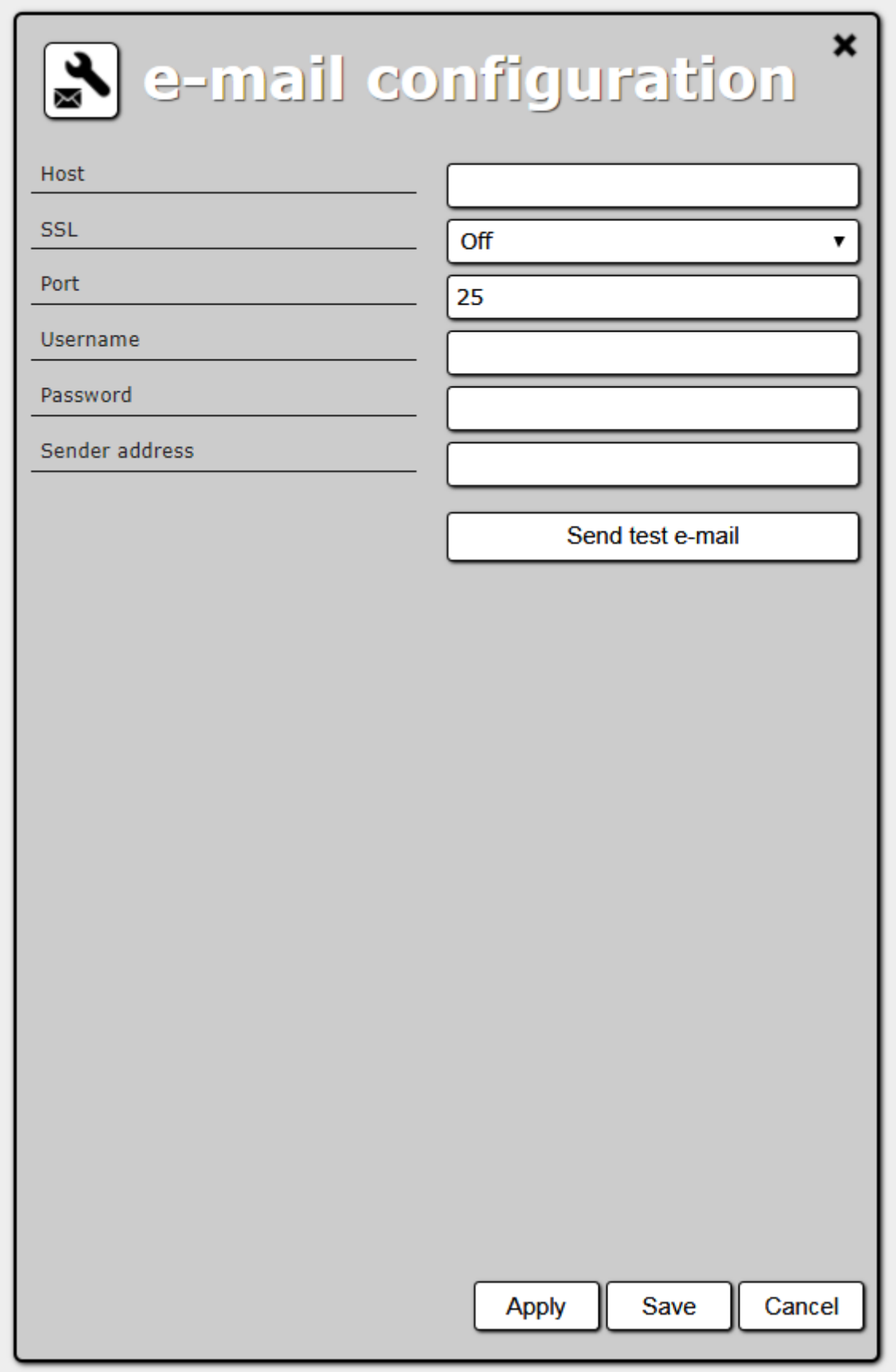
    - **Import management data** – starts the import process.
- Export management data section:
    - **Export management data** – starts the process of exporting the management data. After it is complete, the user can store the file.
- Import events data section:
    - **Import file** – opens a dialog box where the user can choose the file to be imported.
    - **Import event data** – starts the import process. After it is complete, imported events are available in reports (but not in the alarm list).
- Export events data section:
    - **Date range** – range of detection dates of events to be exported. Notice that the resulting file can be very large if you choose a long time span.
    - **Export event data** – starts the process of exporting the event data. After it is complete, the user can store the file.
    - **Export end remove event data** – starts the process of exporting the event data and removing them from all reports (the alarm list is not affected). After it is complete, the user can store the file.
- Export employees data section:
    - **Export employees** – starts the process of exporting the employee data. After it is complete, the user can store the file.
- Import employees data section:
    - **Import employees** – opens a dialog box where the user can choose the file to be imported. After it is complete, data are available in *Employee* tab (in *Management* section).

Management data import errors

The exported management data file contains companies, sites, routes and so on. Importing such a file is equivalent to creating all these entities using the user interface. This means that the same data validation rules are applied. If an entity complies with these rules, it is created. If it does not (an error occurs), it is skipped (with all its child entities) or the whole import process is cancelled (depending on the user’s choice).

E-mail configuration

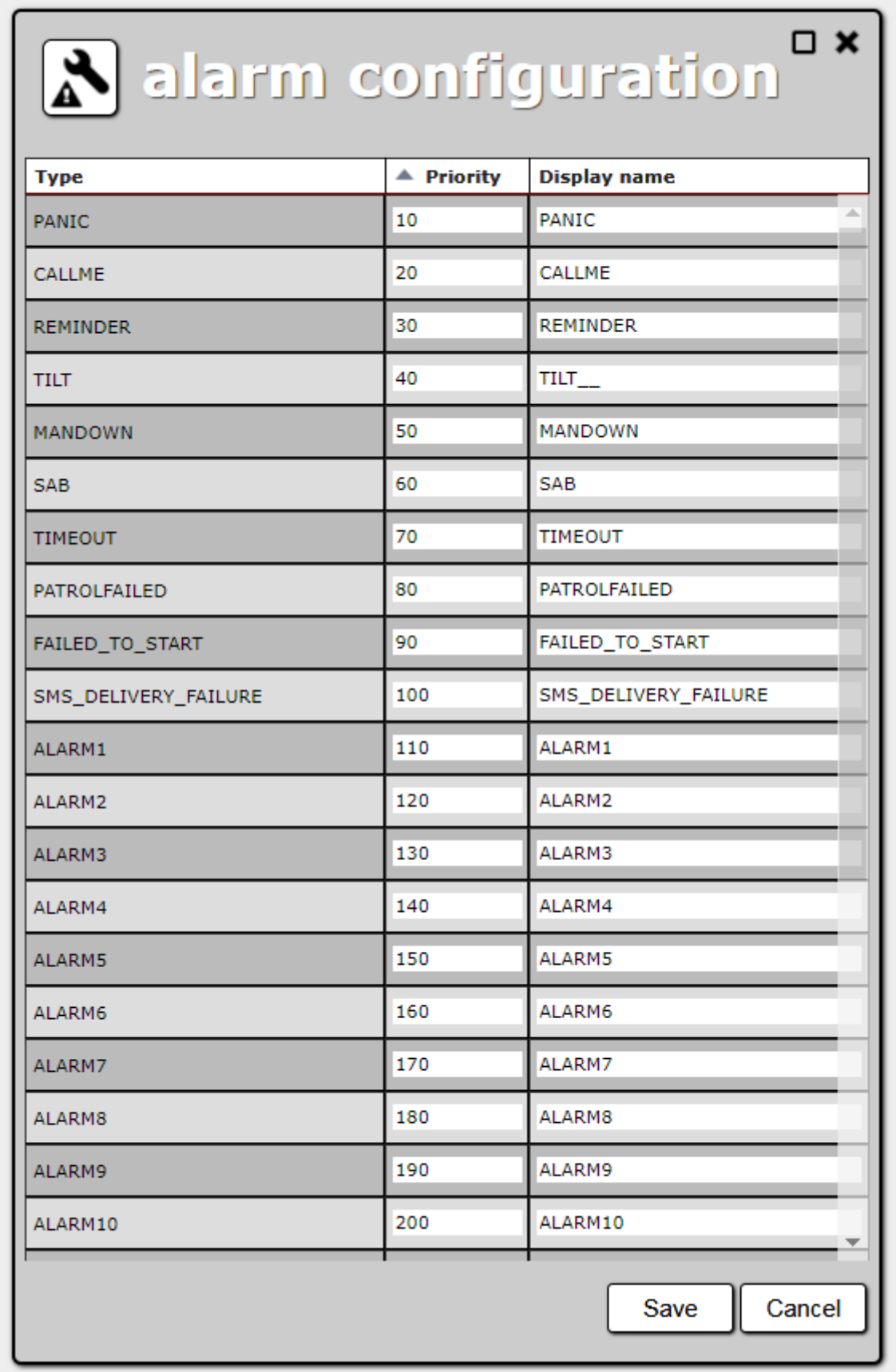
ActiveView uses an external e-mail server to send e-mails (periodic reports and e-mail alarm notifications). To change e-mail server configuration, select *Administration → E-mail configuration* in the main menu.



You can test your configuration by sending a test e-mail (**Send test e-mail** option).

Alarm configuration

You can change alarm priorities and display names in the alarm configuration. To open it, select *Administration → Alarm configuration* in the main menu.



On the alarm configuration panel, there is a list with all possible alarm types. For each alarm type, you can set a priority (lower means “more important”) and a name which is used in the rest of the application.

Alarm priority settings affect the order of alarms in the alarm list and the alarm displayed as the most important of a group (of alarms from one site). See Alarms for details.

Among other things, you can change display names to translate alarm names into your language.

OSM events configuration

ActiveView communicates with devices using special software called OSM. OSM uses its own names for event types. You can map those OSM event types to different reactions of the system and name them in a way easier for you to understand.

Event types

There are two main categories of events from devices:

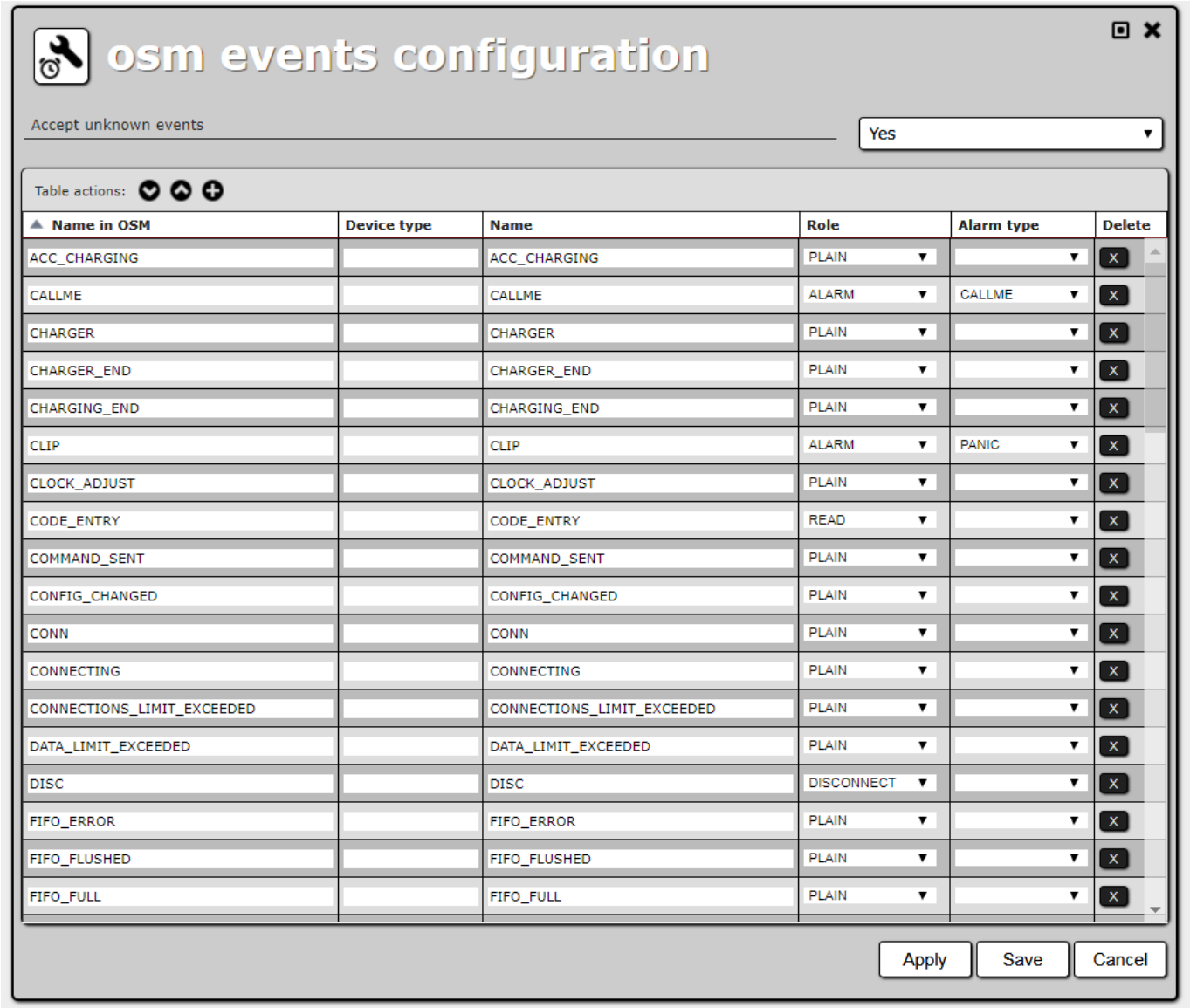
- *Plain* – ActiveView does not understand them. The events are listed in the application, but not processed in any way.
- *Other* – ActiveView performs different actions when it receives the events.

ActiveView performs the following types of actions in response to *Other* events, depending on the event role:

- *READ* – records, that a TAG has been read (see Tags and Routes for details on TAGs usage);
- *DISCONNECT* – changes device connection status to disconnected (see Devices for details);
- *SMS_RECEIVED* - changes device connection status to SMS (see Devices for details);
- *TEST, LOCATION* – records, that a test or location message has been received (these types of events differ from plain events in that they are not visible in reports);
- *ALARM* – informs users about the alarm (see Alarms for details).

Event configuration

To change events types and names, select *Administration* → *OSM events configuration* in the main menu.



On the **OSM events configuration panel** there is a list of mapped events. The list has the following columns:

- *Name in OSM* – name of the event sent by the OSM.
- *Device type* – type of the device which sent the event. The pair *name in OSM* – *device type* must be unique.
- *Name* – the name ActiveView will use for the event identified by *name in OSM* and *device type*. If *device type* is empty, the name is used for all events with the corresponding *name in OSM* (whatever the *device type*).
- *Role* – the event role ActiveView assigns to the event identified by *name in OSM* and *device type* (see Event types above).
- *Alarm type* [applicable if *Role* is set to ALARM] – the type of the alarm, that will be caused the event identified by *name in OSM* and *device type*.
- *Delete* – clicking it deletes the record.

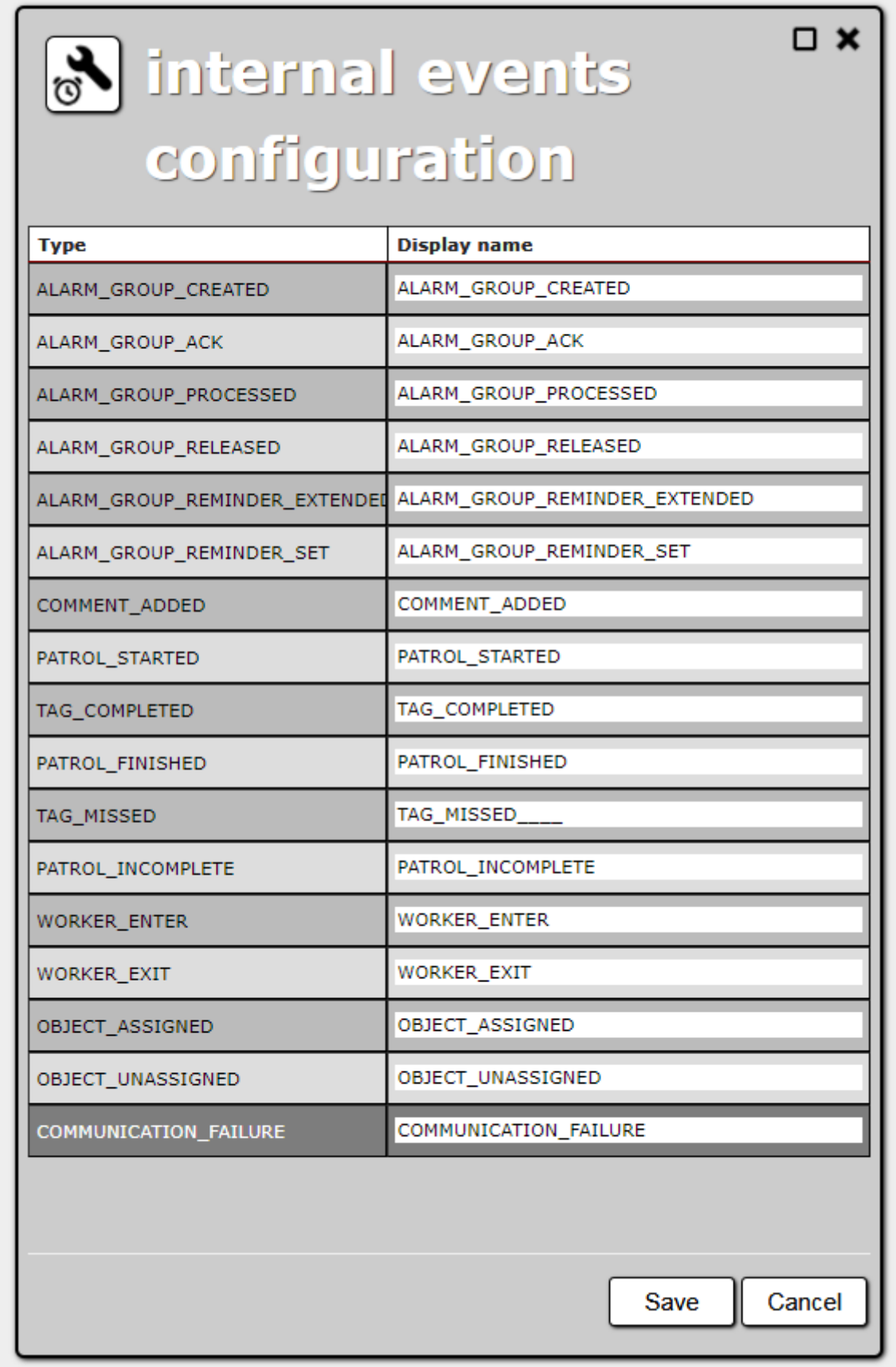
Above the list, there are the following table actions:

- **down arrow** – scrolls the list to the last record;
- **up arrow** – scrolls the list to the first record;
- **plus sign** – adds a new record.

Above the list and the table actions, there is the **Accept unknown events** option. If set to *No*, ActiveView will ignore events with *name in OSM* and *device type* not mapped in the event configuration. If set to *Yes*, ActiveView will treat unknown events the same as plain events.

Internal events configuration

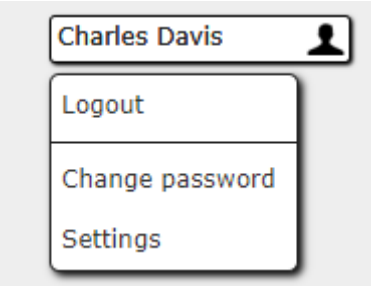
Besides events from devices, ActiveView processes events, which it generates itself, e.g. start of a patrol or addition of a comment to an alarm. Names of the events can be changed in the internal events configuration. To open it, select *Administration → Internal events configuration* in the main menu.



On the internal events configuration panel, there is a list with all possible internal events. For each event type, you can set a name which is used in the rest of the application.

User menu

In the top right corner, there is the user menu available (click on your user name to open it).

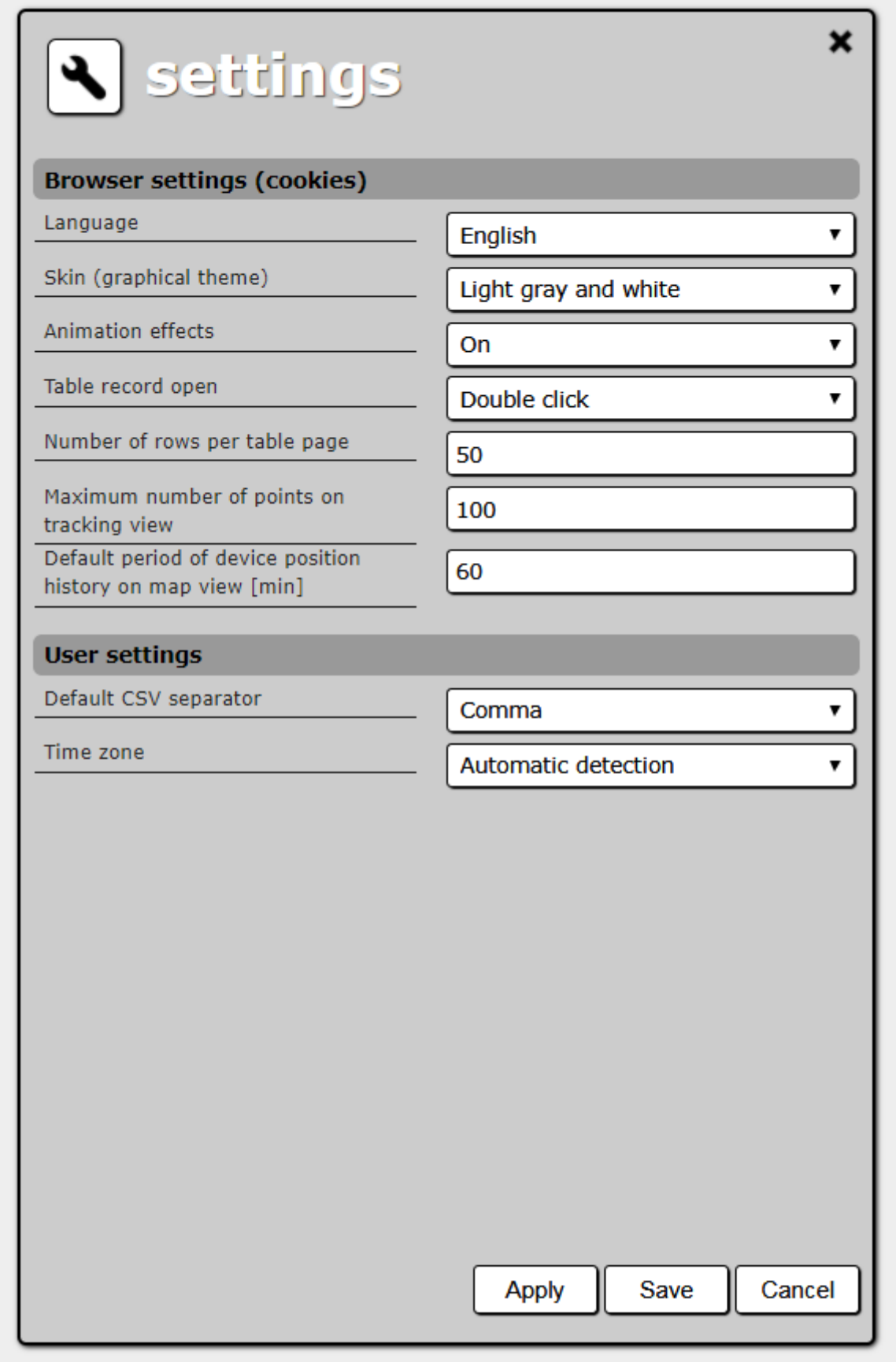


There are the following options in the **user menu**:

- **Logout** – logs the user out of the application.
- **Change password** – allows the current user to change his/her password.
- **Settings** – opens a panel with the current user's settings.

User settings

The **user settings** affect the look and feel of the application.



There are two types of those settings:

- Browser settings are stored in the browser (i.e. not on the server). This means they do not follow the user when he/she changes computers. You can, for example, have different settings on a laptop and on a tablet.
- User settings are stored on the server and follow the user. This means that the user has the same

settings on every device he/she uses to log in to the application.

There are the following user settings:

- *Language* [stored in the browser] – the language of the user interface.
- *Skin (graphical theme)* [stored in the browser] – set of colours, icons, etc. used by the user interface.
- *Animation effects* [stored in the browser] – if turned on, panels slide smoothly, fade in and out, etc.
- *Table record open* [stored in the browser] – affects the way the details of items in lists are opened: with a single or a double click on an item.
- *Number of rows per table page* [stored in the browser] – the number of rows displayed on a single page of a paged list (table). This setting allows the adjustment of list panels to screen height.
- *Maximum number of points on tracking view* [stored in the browser] – the maximum number of nodes of a device trace, shown on a map. See Devices for details. This setting allows the adjustment of trace accuracy to browser performance.
- *Default CSV separator* [stored on the server] – the default separator character used in CSV files generated by the application.
- *Time zone* [stored on the server] – the time zone used to present time in the application. It affects alarm list, event list, reports and route definitions.

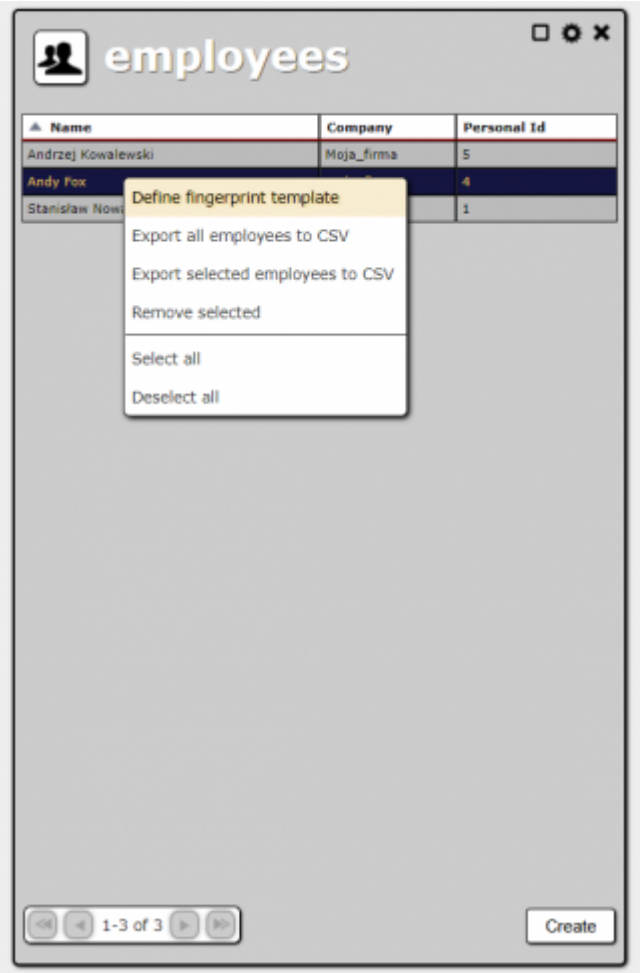
Working with FPX in ActiveView system

FPX device recognizes only fingerprint if its template is saved in the device. Active View application simplifies registration of fingerprint templates into the FPX device and manage linking up employee with his fingerprint templates and RFID cards. Fingerprint, after registration of its new template, will be automatically assigned to the employee if employee has set up “Personal ID” in the employee's record stored in AV.

Creating a fingerprint for the employee

In order to define employee's fingerprint template, designated FPX device must be online. The first step in defining a new fingerprint template is setup the device to be in recording mode (device will be initialized to record a new fingerprint template). This can be done in the AV application in two ways - from the list of employees or from the employee settings panel. Both ways are described below. For each employee many finger prints and RFID cards may be registered.

Sending the command to define fingerprint template from the list of employees



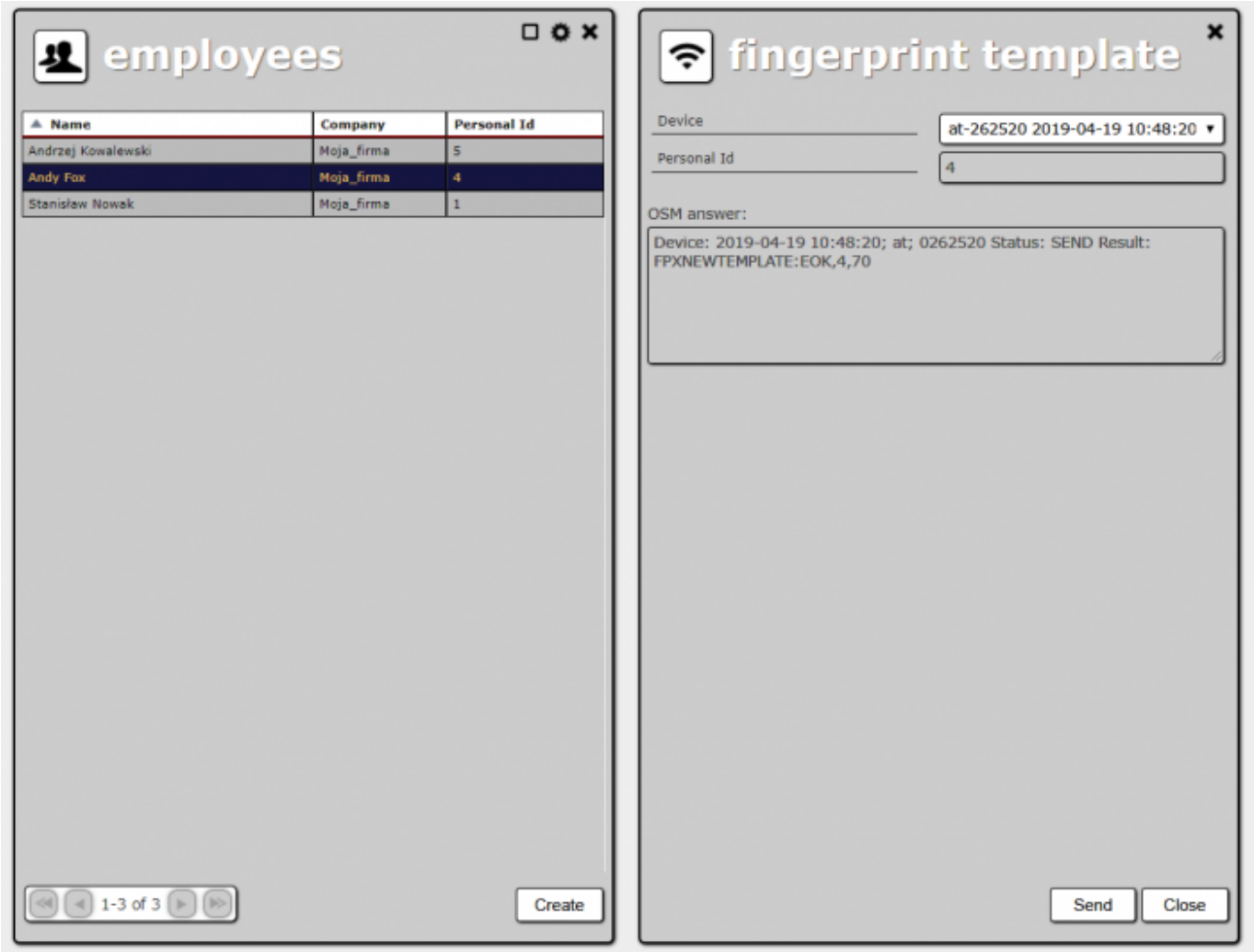
In order to create employee's fingerprint template select one of them and in the list and right click on the employee or click the cog in the right corner. A contextual menu will be displayed. Click *Define fingerprint template* item then fingerprint template form will be displayed. It contains the following fields:

- **Device** - with the list of company's devices. If employee is not assigned to any company or if none of devices is assigned to his company, the list will be empty.
- **Personal Id**
- **OSM answer** frame

The following buttons are available at the bottom of form: *Send* and *Close*. Clicking *Send* button, initializes the FPX device. After sending the message, the answer will be displayed in the *OSM answer* frame. Message example:

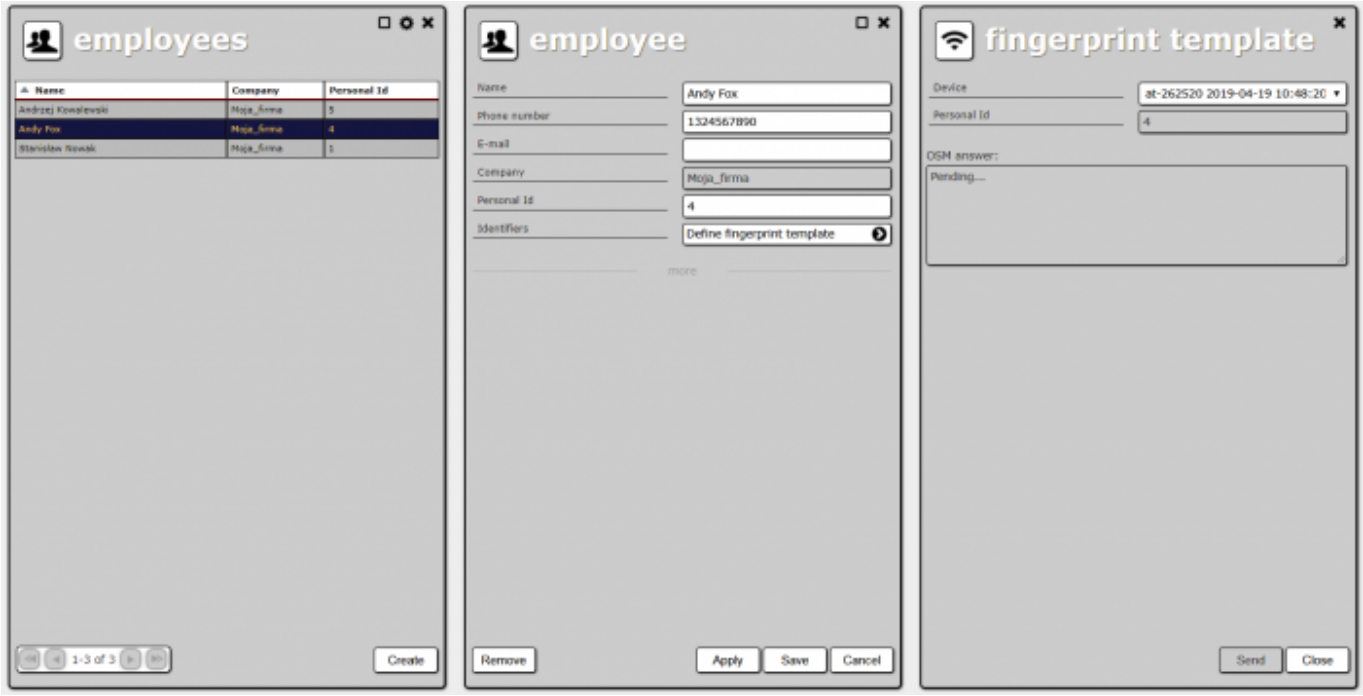
Device: FPX: 0262520 Status: SEND Result: FPXNEWTEMPLATE:EOK,id223,70

If during sending the message an error occurs, then appropriate error message will be displayed. Finally you can close form by clicking *Close* button or register another finger for the same employee.



Sending the command to define fingerprint template from the employee panel

You can also initialize the FPX device from the employee panel. Open the record of the particular employee. Click the field labeled *Identifiers* (it contains inscription *Define fingerprint template*). After that, *fingerprint template* form will be displayed. Further steps have been described above

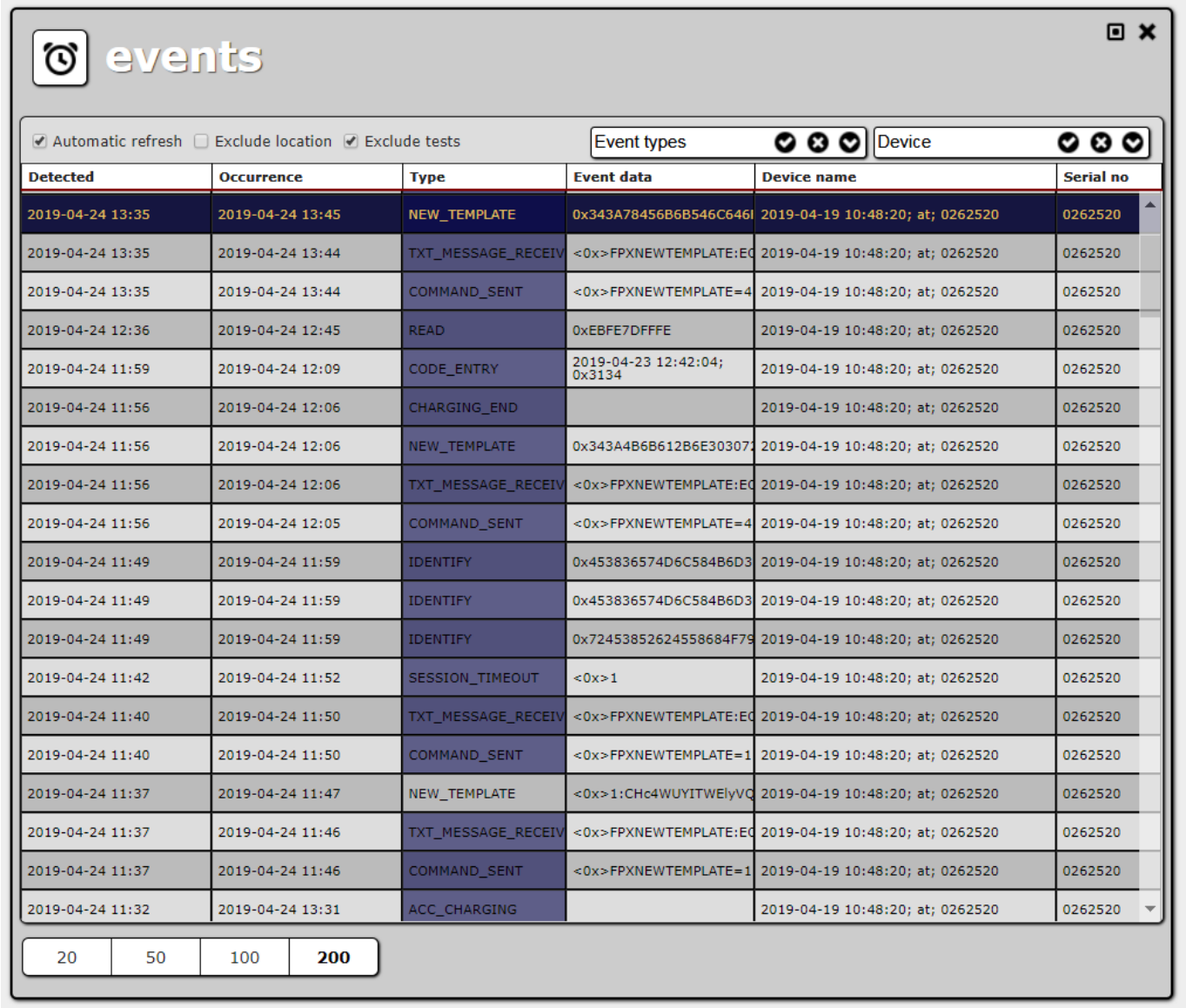


Add fingerprint template on FPX device

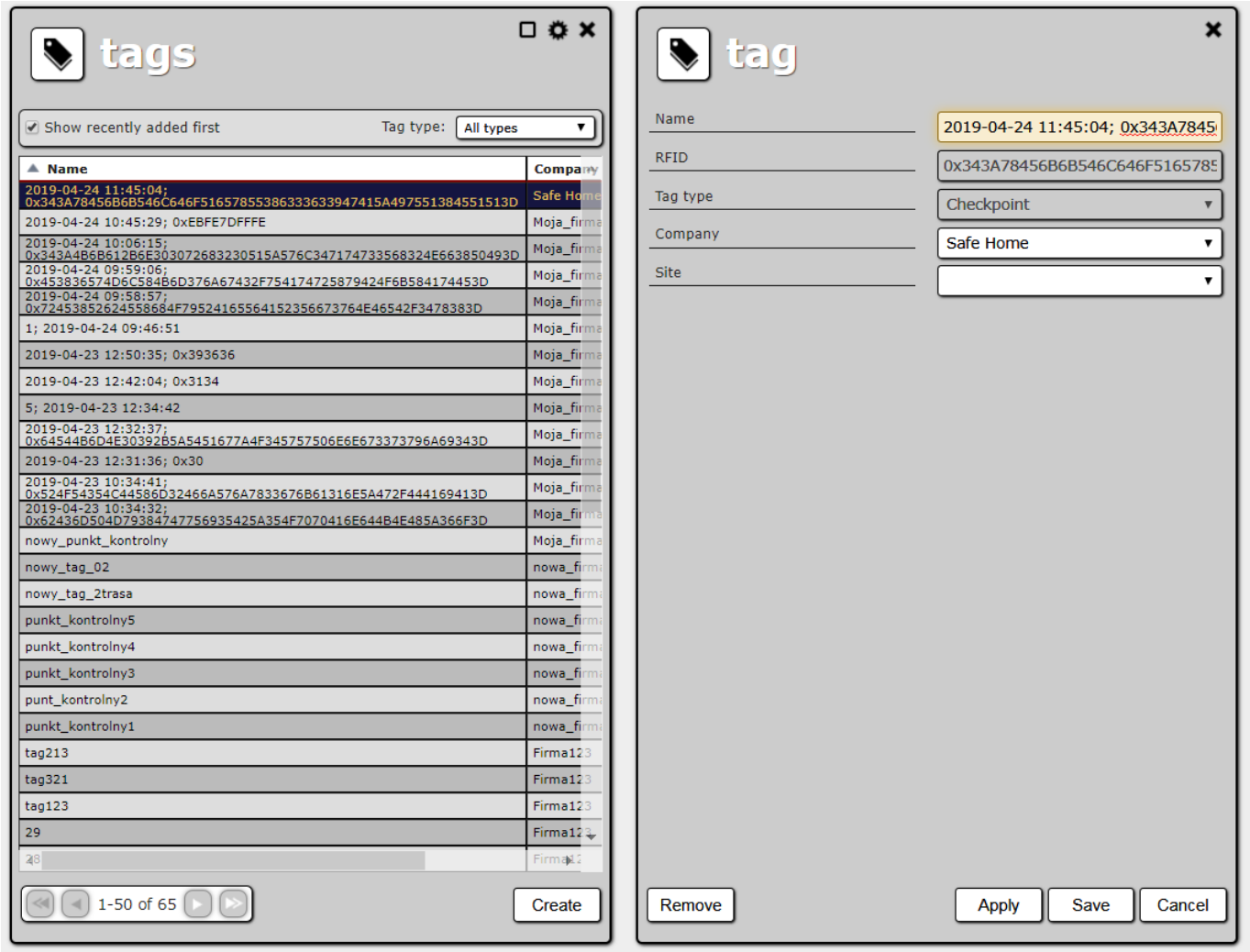
Initialized FPX device confirms its readiness by BEEP sound. The employee, for whom you want to define a fingerprint template, should put the finger to the scanner. In the given example, the employee has 70 seconds to scan his finger. After applying a finger to a scanner, two LEDs: the green one (OK) and the red one (READ), will start blinking rapidly. When the fingerprint has been read and approved, the device makes 3 short beeps, along with flashing green led (OK), to confirm that the fingerprint has been added correctly.

When fingerprint is not recognized correctly, the red led will light up and the device makes a single long BEEP. Then you should repeat the steps described above, starting with a initializing of FPX device.

To verify whether the fingerprint template has been registered in the FPX, open the Events panel and find an event named **NEW_TEMPLATE**.



After receiving the *NEW_TEMPLATE* event, the new *Employee identifier* tag is created in the system. The *Personal ID* and the *fingerprint template ID* are extracted from the event data. If there is a worker with the same *personal ID* in the system, then the new tag is assigned to him. The *fingerprint template ID* is inserted into the RFID field in the tag's properties.



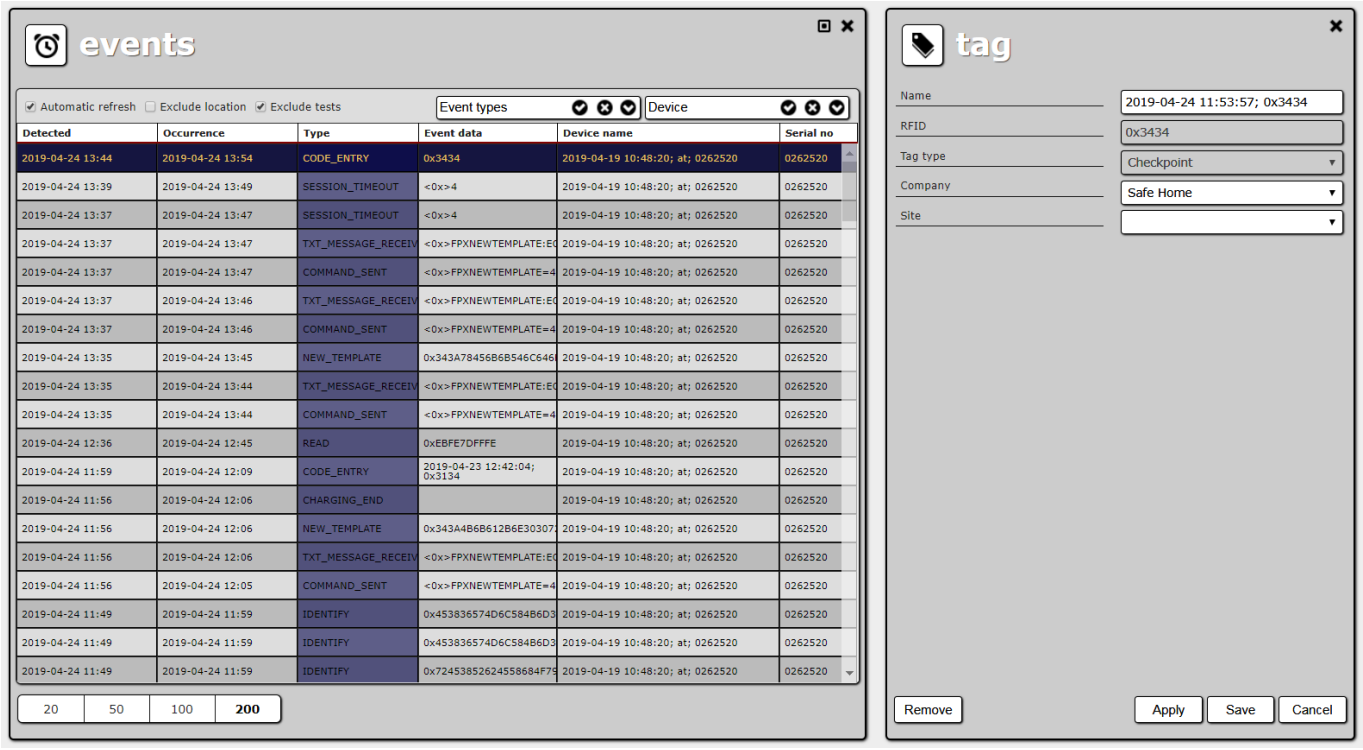
Code entered on the keypad as employee identifier

FPX device sends the code (typed on the keypad) to AV application. The code can be registered as an *employee identifier* or tag of other type. Application can treat received code (according to settings) the same way as READ event.

Example:

If you would like to send code 14 to application , please type on FPX: 1,4,#

Typing # sign triggers the device to send a code to the server.



Synchronization fingerprints between devices FPXs

Fingerprint templates of all employees registered in AV records will be collected by AV automatically. In AV employees should be assigned to any company. Synchronization of the FPX device is done by uploading to it all templates of employees who belong to the same company as FPX.

Single template can be synchronized up to two hours in case the system is not busy with the mass synchronization process.

When new device (without templates) is connected to the system, synchronization can take a few hours, depending on how many templates must be synchronized.

Removing fingerprints templates from devices

Please be aware that removal of particular employee from the employee list in application will reflect the removal of his fingerprint templates from FPX device.

If you would like to remove all fingerprint templates from particular device, send the command to device as shown below:

FPXDELETEALL

If the device is assigned to the company where there are employees with registered fingerprints then these templates will be sent to device again.

Guard Tour Systems

Many companies aim to provide protection of company facilities on twenty-four hour, seven day per week basis. They epmloy security officers, whose duty is to provide periodic patrols of the facility in order to detect suspicious and abnormal actions.

Patrols should be executed according to established procedures. The patrol route should include all important points of the facility. Depending on the size of the site, there can be several different routes and each of them can include different areas. Patrols are made at least several times per shift.

Often guards work alone with no supervision. The lack of control can cause that guards remain at their posts and don'□t go on patrol. On some occasions they can skip some points of the tour, especially if the access to this part is more difficult.

Guard Tour systems help to solve these problems. In general, guard tour systems allows to control security officers work and forces the performing patrols according to the planned schedule and route. If guards know that their activities are recorded they are motivated to follow the schedule and make patrols properly. The system provides a record of all patrol activities, therefore all the activities deviating from the procedures can be quickly identified. The written record can also be used for incident investigation and as proof of patrol activities for insurance companies or regulatory agencies.

Electronic Guard Tour Systems

ActiveView Software with cooperating devices is an example of electronic guard tour system.

Electronic guard tour systems are based on use electronic data gathering devices (Active Guard and Active Track) which are which are carried by the security officers during patrols. An electronic data gathering device is usually a small hand-held device in the shape of a wand or small PDA with a few buttons. The patrol route consists of the checkpoints. Those points contains tags that can be read by the device. During a patrol, the guard visits each checkpoint and scans tag using the device. The information about meeting checkpoint and time is automatically sent to the system. Therefore the employer knows that the guard was in the right place at the right time. The guard can also send notification about any abnormal conditions found during the patrol.

Advantages of Electronic Guard Tour Systems

- Large number of checkpoints possible
- Small size of checkpoint tags, possibility to place them almost anywhere
- Small devices, easy to carry
- Ability to control performing the patrol by the guard, information about visiting checkpoints at the right time
- Easy identification of missed stops and abnormal patrol activity

- Ability to send alarm message with information about incident or abnormal conditions found during patrol
- Automatically created reports, powerful management of reports
- Ability to store data many months or years in databases