8. System Monitor

System Monitor provides the following functionality:

- Displaying real time information coming from one or multiple workstations online;
- Displaying the status of each system entity on interactive maps and management tabs in real time mode;
- Displaying video images from cameras, servers and DVRs as well as playing video recordings
- Tracking employees online with resolving power up to an access zone,
- Managing and controlling loops/zones, partitions, partition groups, access points and other entities of the system using interactive premises maps and management tabs,
- Online operator's control of fire extinguishing using interactive maps,
- Launching Response Scenarios by security system operators,
- Allocation of system control privileges to an Operator,
- Online handling and saving history of system alarm events

The System Monitor (\ omonitor.exe\ in the Orion Pro system folder) starts automatically on a workstation when the System Shell is started on the same workstation (If System Monitor module is selected in the DBA to run on this specific workstation)
If you quit the System Monitor you can start it again by clicking a corresponding button on the System Shell bar (highlighted red on the below figure):

8.1 Starting System Monitor

Attention! Chapters 8.1, 8.1.3, 8.1.4, 8.1.5, and 8.2.8 describe the operation logic of the System Monitor and Scanning Core as well.

Before the System Monitor started:

- The Scanning Core is started on a specific workstation, If it is selected to run on this specific workstation in the Database Administrator.

When started, the Scanning Core performs the following:

- Device employee locations using the Site Occupants module
- Sets contacts with all devices connected to the workstation
- Synchronizes current dates and times between devices and the computer (workstation)
- Polls(requests) the status of devices;
- Obtains occurred events from devices
- Provides automatic control of the system

When the above completed, the System Monitor starts and the database is loaded. When database loading completed, an Operator's password for the System Monitor is requested.

8.1.1 Entering Passwords

Each System Monitor operator (an SM operator) must have his/her own personal password to run the System Monitor module.

When software passwords are assigned to an SM operator in the Database Administrator, allocated privileges of each password can be as follows:

- Rights to operate the System Monitor module
- Rights to operate individual zones (in addition to partitions, it allows an operator to control partition-included individual zones using premises maps and list of zones)
- Rights to operate high security partitions (access to operate **High Security** partitions
- Rights to operate Intrusion Detection and Fire Protection System (enable/disable Auto Mode, Activation of Extinguishing, and Extinguishing (Release) Abort
- Rights to handle alarms (operator's rights to handle the list of alarms – maintaining records regarding alarm response measures, and moving alarms to the archive.
- Rights to operate system entities: zones, partitions, partition groups, access points and cameras; as well as rights to obtain information on events and states of system entities: zones (loops (inputs) and relay outputs), partitions, partition groups, access points, readers, devices and cameras (assigned by an access level defining rights to operate entities and access information).

*Please refer to Chapter 6 Database Administrator for detailed description of how to create a password to access Orion Pro's applications (**software password**).*

When starting the System Monitor, each operator has to enter his/her own password.

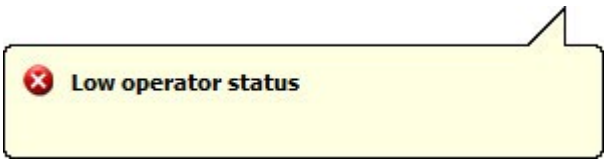
A password is entered in the **Login** dialog box when System Monitors starts upon loading the database

The further actions depend on data entered:

- If one clicks the **Cancel** button, the System Monitor will be closed;
- If one enters the wrong password and clicks the **OK** button, the System Monitor will respond as follows:
  - It will not accept a password,
  - and generate the following messages:
    - In case of unknown password:

(*The **Password rejected** event and the **Password not found** description will be added to the Event Log*).

- If the employee status does not allow working with System Monitor:

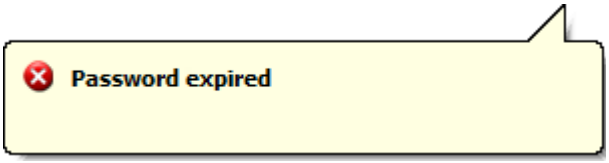


(The **Password rejected** event with the **Low Operator** status description, and the name of a password holder be added to the Event Log)

- If the password does not provide any rights to run the System Monitor (Operative Task):

(The **Password rejected** event with the **Insufficient rights** description and the name of the password holder will be added to the Event Log)

- In case of an expired password :



(The **Password rejected** event with the **Password has expired** description and the name of the password holder will be added to the Event Log.

  - And will wait for a correct password;

- If the password is correct, the System Monitor will perform as follows:
  - Accepts entered password and displays **Operator Switched** event in the **Event Log**, as well the name of entered password holder
  - Allows an operator to access the system.

The Operator's ability to control various system entities and obtain information on their system events and states depends on the password parameters:

- If an operator has rights to operate some system entities (zones (loops and relay outputs), partitions, partition groups, access points (including readers), these entities will be accessible on corresponding tabs (Zones, Partitions, Partition Groups, Access Control and Employees tabs) and on premises maps.

  The Alarm Log and Event Log will include and show events related to the above entities.
  - The operations and actions allowed by assigned rights in respect with the above entities will be as follows:
  - Arming and disarming
  - Operations and actions with individual zones
  - Operations and actions with high security partitions
  - Management of fire extinguishing system

- If an operator has rights to view events and states of system entities (zones (loops and relay outputs), partitions, partition groups, access points (including readers), these entities will be accessible on corresponding tabs (Zones, Partitions, Partition Groups, Access Control and Employees tabs) and on premises maps

  The Alarm Log and Event Log will display events related to the above entities.
  In addition, the states of these entities will be available for viewing.
  Operations and control actions will not be available for these entities

The entities that are not covered by operation or viewing rights will not be displayed in tabs or on premises maps.

- The maps that display at least one of the entities will be accessible.

  The maps that display no entity will not be accessible.
- If an operator has rights to handle alarms he/she will have rights to handle alarm on the Alarms tab. Otherwise, the operator is not allowed to perform any actions in the Alarms tab page.

8.1.2 Polling the System Entities .Color Scheme of Displayed Entities. Entity Multistate

When the System Monitor loads the database, it will read all system entities' states from Scanning Cores of all requested workstations.

In accordance with obtained status of system entities (zones, cameras, partitions, partition groups, access points, readers and devices), the System Monitor shows their states on premises maps on the Zones, Partitions, Partition Groups, and Cameras tab pages.

By default, the System Monitor uses the color scheme for entities states as described in the chapter *Appendix 8.B Color Scheme for System Entity States*
The table of Appendix 8B includes main pictures (icons) to represent entities. There are also more icons to represent entities such as Loop, Relay Output, Access Point, Reader, Device, and Camera.

Please keep in mind that you can change colors and icons representing states using the Orion Pro GUI Editor (Refer to Chapter 15 Orion Pro GUI Editor)

Important! The status of the system entity may include more than one states, the most prioritized status is regarded as the main one. That main status affects the color of icon represented entity in the tabs and premises maps

Let's discuss the multistate on the example of S2000-IK addressable detector. This entity has several none-overlapping groups of states:
1 - (Armed, Disarmed, Arming Failed, Intrusion Alarm.),
2 - (Tamper Restore, Tamper Alarm),
3 - (PL Restore, PL Short Circuit, PL Failure),
4 - (Connected, Disconnected,),
5 – (Contact Restore, No Contact).

Accordingly, the multistate of the S2000-IK addressable detector is formed by five states (one from each group of states

Each state has its own priority. The status with a maximum priority is the main status of an entity.
E.g. an S2000-IK addressable detector with a multistate including (Armed, Tamper Restored, PL1 Restore, Connected, Contact Restore) has the Armed status as the main one.

The *Appendix D Prioritized States of Zones (Partition, Partition Group)* lists the states in higher-to-lower priority order

Attention! If the entity includes other entities, the entity' status is determined by the aggregate of multi-states of entities included in this entity with the highest priority status regarded as the main one:

- The multistate of a partition is the aggregate of states of all loops, relay outputs, and cameras included into this partition, as well as the states of devices where the partition-associated loops and outputs are connected

- The multistate of a partition group is the aggregate of states of all partitions included in the partition group

- The multistate of a map is the aggregate of states of all loops and partitions added to the map (a map state is indicated by the color of a map name and links referring to this map)

The multistate of a partition, partition group and premises map includes the states belonging to one state group.

For example, a partition includes two loops of the Signal-20P: a fire loop with multistate (Disarmed, Contact Restored) and auxiliary loop with a multistate (Auxiliary Restore, Contact Restore). Considering that, the multistate of the partition will have the following states: Disarmed, Auxiliary Restored, Tamper Restored, and Power Supply Restored, and Contact Restored.
As example shows, in addition to the loop states, there is a multistate of the Signal-20P appeared, which hosts loops: Tamper Restored, Power Supply Restored, and Contact Restored.
The main state will be the **Disarmed** status that has the highest priority.

The examples of the multistate representations are provided in the following chapters: *Chapter 8.3.3.2.1 Obtaining Information on Loops, Relays and Cameras, Chapter 8.3.3.2.2 Obtaining Information on Partitions; Chapter 8.3.3.3.2 Obtaining Information on Partition Group; Chapter 8.3.3.6.1 Obtaining Information on Access Zone; 8.3.3.6.3 Obtaining Information on Access Point; 8.3.3.7.1 Obtaining Information on Camera; 8.3.4.2.1 Obtaining Information on Camera; 8.3.4.2.1 Obtaining Information on Reader; and 8.3.4.2.2 Obtaining Information on Device.*

8.1.3 Employee Tracing

When the System Monitor loads the database, in addition to obtaining the states of all system entities, it also determine the location all database-enrolled employees by the recent events. The System Monitor indicates an access zone of each employee's current location.

If a Scanning Core is launched on a workstation directly before starting the System Monitor, it will locate employees by requesting the Site Occupants module, and then it will start fetching device events. It is worth mentioning that process of fetching events will be started only when employees' location have been determined.

In accordance with obtained events, the Scanning Core and System Monitor will move employees in required access zones.

The necessity of locating employees is that the System Monitor shows the location of employees and the Scanning Core supports antipassback mode immediately rather than after the first entry of each employee.

8.1.4 Fetching Last Events

When started, the Scanning Core collects events from devices and polls entities for their status at the same time.

The events of devices connected to a dedicated COM Port or Ethernet will be fetched as follows:

- From the event buffer of the S2000M, if the S2000M is connected to a dedicated COM Port and works in the Computer mode (i.e. if the Orion Pro protocol is used)

- From the event buffer of each device connected to a dedicated COM Port via S2000-PI and PI-GR interface converter (i.e. if the Orion protocol is used) or connected via Ethernet

If devices are connected to a COM Port with the Orion protocol using the S2000M in the PI-Reserve mode, the events fetching will not be performed because all events are stored in the event buffer of the S2000M panel serving as an interface converter during operation of the Scanning Core.

Connection of Devices to a workstation is described in more detail in *Chapter 1.2.2 System Devices, Orion and Orion Pro Protocols, Connection Charts*.

The process of event fetching varies by a protocol used in the Orion Pro system to interact with devices, namely:

- The Orion Pro protocol :

All events are read from the S2000M, and received with an event occurrence timestamp:

In case of the **Orion Pro** protocol, the following actions will be provided:

- If more than two minutes elapsed after event:
  - No centralized control tactics (relay actions) will be initiated as well as no scenarios will be executed in response to this event
  - The entity will keep its status unchanged
  - The status of entity will not be changed
  - Representation of employee location will be moved to a corresponding access zone.
- If less than two minutes elapsed after event:
  - Centralized control relay tactics (relay action) will be initiated and scenarios will be launched in response to the event
  - The entity status will be changed
  - The employee will be moved to a corresponding access zone

If the **Orion** protocol is used, the following will be performed:

- If more than two minutes elapsed after event:
  - The events will be marked as an old one (it will be highlighted yellow in the event log of the System Monitor)
  - No centralized control tactics (relay actions/programs) will be initiated as well as no scenarios will be run in response to this event
  - The status of entity will not be changed
  - Representation of employee location will be moved to a corresponding access zone.
  - If less than two minutes elapsed after event:
- If less than two minutes elapsed after event:
  - Centralized control relay tactics (relay action) will be initiated and scenarios will be launched in response to event
  - The entity status will be changed
  - The employee will be moved to a corresponding access zone.

Each event read by the Scanning Core is the subject to the following:

- Recording to the Events Log,
- Transmitting to the System Monitor of a current workstation,
- Sharing with other workstation in accordance with transmission (sharing) settings of a current workstation.

If an event causes a status change; this changed status will be transmitted to the System Monitor the current workstation. As well as shared with other workstations of the system as configured.

An alarm is logged in the Event Log as well as in the Alarm Log.

When System Monitor receives and event, the event appears in the Event Log as well.

The Alarm Handling attribute is set as Yes, an Alarm event will switch to the alarm handling tab page.

In case of an access event, a corresponding employee will be moved to a corresponding access zone.

When the System Monitor receives an entity status, it will replace current status with new received status. The new status will be shown in all management tabs and premises maps.

8.1.5 Automatic System Control

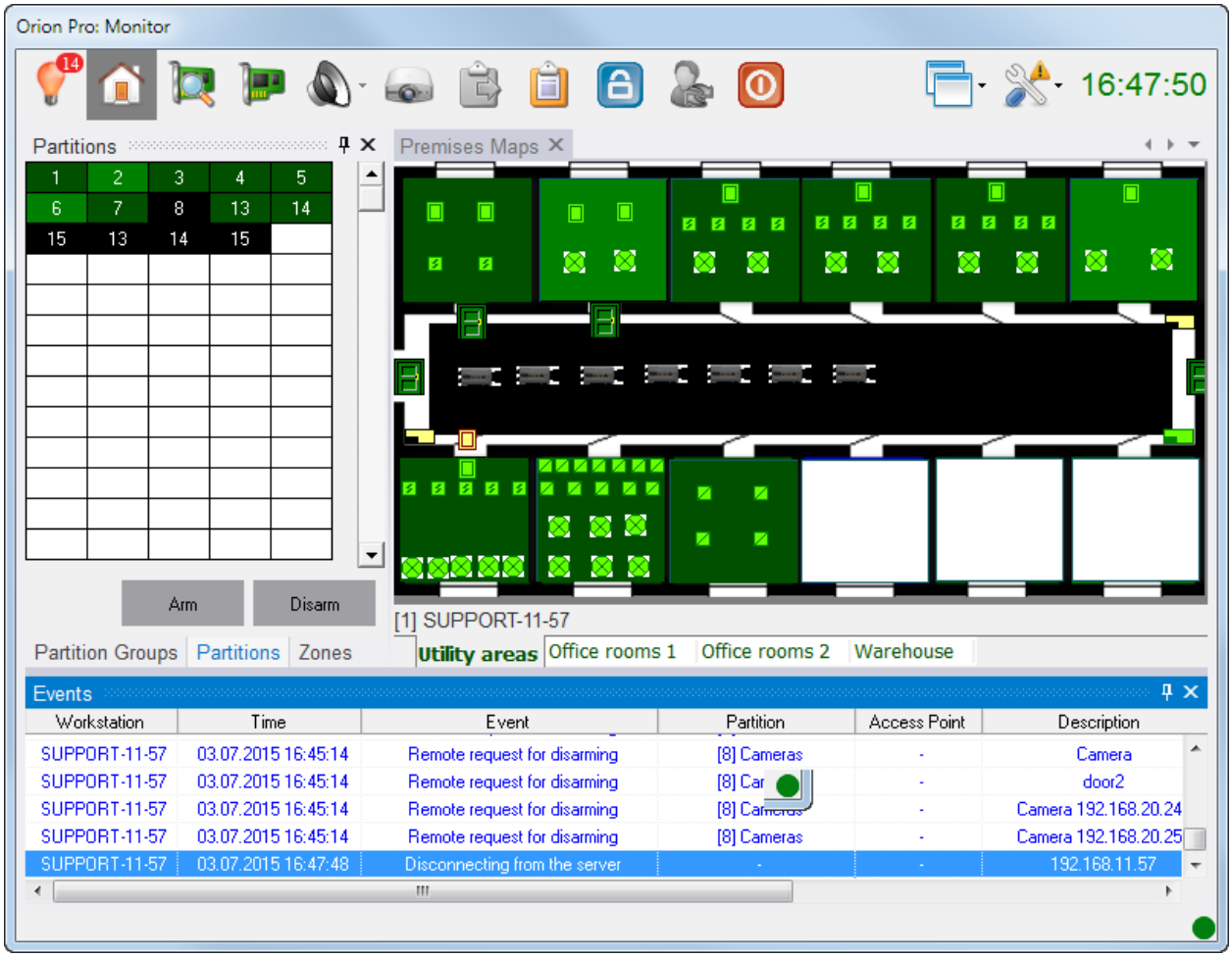
If started before the System Monitor on the same workstation, the Scanning Core will be responsible for the following automatic control activities after it starting and completing the above actions:

- Monitors communications with devices
- Receives events from devices
- Transmits events to devices
- Transmits system entities' to devices
- Provides centralized control of relay outputs
- Provides centralized arming and disarming
- Provides centralized fire extinguishing control
- Provides centralized access control functions ensuring online anti-passback: hard, timed, and soft
- Runs management scenarios as response to system events
- Runs scenarios on schedules

If started alone, the Scanning Core will be responsible for automatic system control as well.

8.2 User Interface

The following figure shows the main window:



Note! The actual size and proportions of the application window have been changed to fit the figure to this document format.

The figure shows that the windows consist of three areas (each is highlighted red):

1. The Toolbar with tab toggling buttons, action buttons and clocks.

 – toggles the **Alarms** tab (hot key is <Alt+F1>);

 –toggles the **Management** tab (hot keys is <Alt+F2>);

 – the **Status Request** button (hot key is <Alt+F3>);

 – the **Connected Devices** button (hot key is <Alt+F5>);

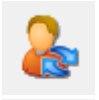
 – the **Voice Announcement** button (hot key to disable a current voice alarm is <Alt+F6>);

 – this button toggles the **IP Cameras** window (hot key <Alt+F7>);

 – the **Shift Report** (Session Report) (a hot key is <Alt+F8>);

 – the **Event Log** button (a hot key is <Alt+F9>);

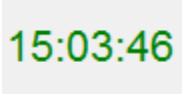
 – the **Screen Saver** button (a hot key is «горячая клавиша» – <Alt+F10>);

 – the **Switch Operator** button (hot key is <Alt+F11>);

 – the **Quit** button (the hot key is <Alt+F12>);

 – allows arranging window floating panes of the application;

 – the **Settings** button;



–current system time

(Chapters *8.3 and 8.4 describe the tab pages of the System Monitor module; Chapters 8.2.1-8.2.11 describe actions of the above actions buttons* .)

2. Tab Page Area.

This is an area where Alarms or Management tab pages are displayed.

(Chapters *8.3 and 8.4 of this guide describes the tab pages of the System Monitor*)

It should be noted, the Video Cameras window is opened outside the main application window (Refer to Chapter 8.5.1).

8.2.1 Status Request

During the operation of System Monitor, one may need to update the status of each entity: loops, relay outputs, cameras, partitions, partition groups, readers, access points, and devices.

To request a current status of a system entity, please click the Status Request button  or the <**Alt+F3**> hot key.

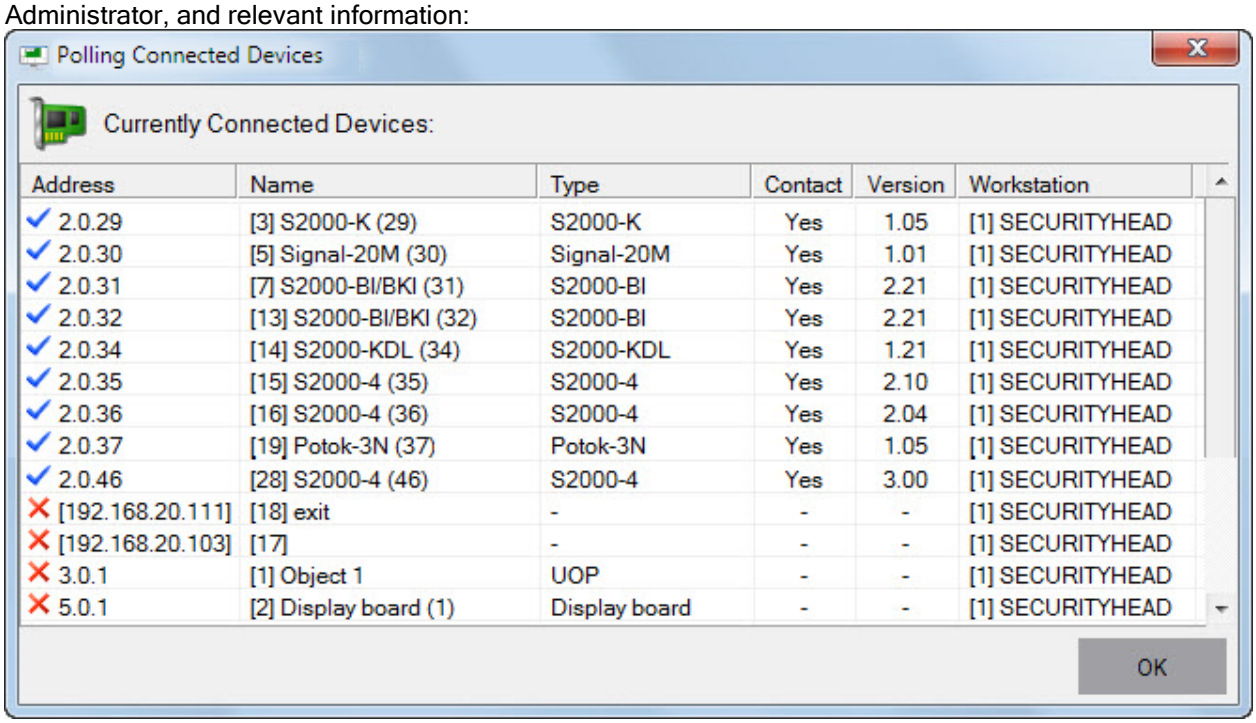
When this button has been clicked, the System Monitor requests relevant Scanning Cores for the current states of the system entities. The current status of each device will be updated in the System Monitor if required.

8.2.2 Connected Devices

If needed, a SM Operator can view what devices and cameras are connected

To view the list of connected devices and cameras, please click the Connected Devices button () the <**Alt+F5**> hot keys.

The window will appear to show the list of connected devices and cameras assigned in the Database Administrator, and relevant information:



It shows the following information about a device:

1. **Address** is a device's address (shown as ComportNumber.PanelAddress.DeviceAddress with a connection-status icon:

   ✓ –Device Connected
   ✗ –Device Disconnected (o the Scanning Core in not running)
   ? – Device is connected, but the database-specified type of device mismatches the actual physical type of connected device;

(In case of Ethernet biometric readers, the address will be shown as *IPAddress*).

2. **Name** – a devices' name in the database ;
3. **Type** – a type of devices in the database;
4. **Contact** - specifies whether the device is connected:
   - **Yes**: Device is connected,
   - **-**: Device is disconneted (or the Scanning Core is not running);
5. **Version** – Device version, (*in case of disconnection this field will be blank*)
6. **Workstation** – Index and name of workstation where this devices is connected.

In case of cameras, the following will be displayed:

1. Address - is a camera's address as shown in the following order [*Camera Number*] Name of video subsystem:

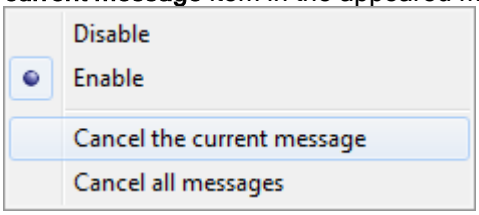
   ✓ –Camera Connected,
   ✗ – Camera Disconnected (or the Scanning Core is not running);
2. **Name** - the name of a camera in the Database;
3. **Type** - this field always shows "*Camera*";
4. **Contact** - shows a connection status of a camera:

   Yes : Camera connected,
   - (dash): Camera disconnected (or the Scanning Core is not running);
5. **Version** – *no information*;
6. **Workstation** - index and name of a workstation where a related camera is connected.

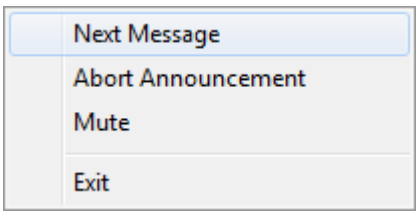
8.2.3 Disabling Audio

If a specific workstation has the **Voice notification** option set as **Yes** in the Database Administrator, the Voice Alarm Module will play alert notifications on this workstation when a system alarm event occur.

To cancel the current message, please click  in the System Monitor and select the **Cancel the current message** item in the appeared menu:

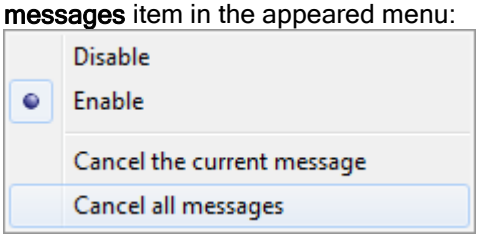


Or press <**Alt+F6**>, or right click the Voice Announcement module in the system tray, then select next message item in the appeared context menu:

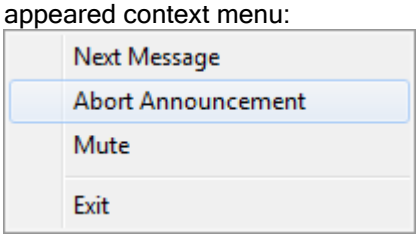


A next alarm event will trigger this voice alarm function again

To cancel all alarm messages, please click  in the System Monitor and select the **Cancel all messages** item in the appeared menu:

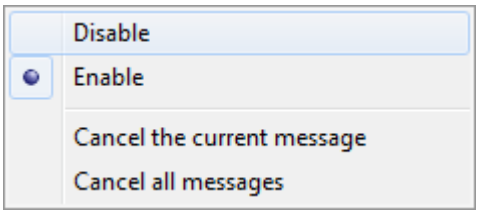


or right click the **Voice Alarm** icon () in the system tray, then select the **Cancel message** item in the appeared context menu:

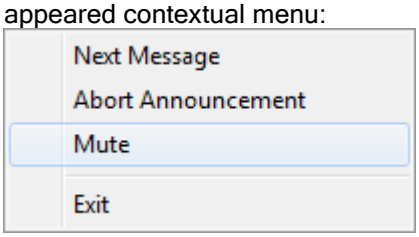


A further alarm event will trigger this voice alarm function again

To disable the voice announcement, please click the  Voice Announcement button and select the **Disable function** in the appeared menu box:

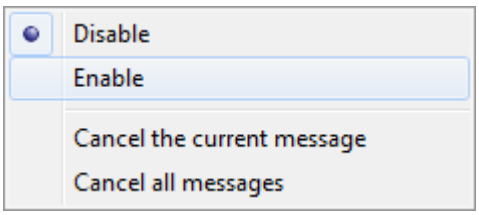


or right click the Voice Announcement icon () in the System Tray and select the **Mute** item in the appeared contextual menu:

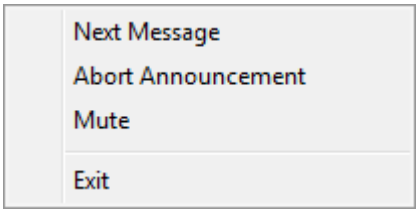


The Voice Announcement button will change to  , and the system tray icon will change to  .

To enable the voice announcement, please click the  button in the System Monitor and select the **Disable** item in the appeared menu:



or right click the Voice Announcement icon ( ) in the System Tray to unselect the **Mute** item in the appeared contextual menu:



The Voice Announcement button will change to the  the system tray icon will change to .

8.2.4 Shift Report

If needed, an SM Operator can generate a report on all alarm events occurred and response action taken during the operator session.
Usually, such a report is generated before switching to a new operator session (shift)

To generate a report, please click the Shift Report button () or press the **<Alt+F8>** hot key.

When this button clicked (pressed), the report will be generated on alarms (occurred during the current operator session till the moment of report generation) and displayed in the Preview window

*Please note that the **Preview** window is a component of the Report Generation module and has the same functional features as the display area of a generated report in the Report Generator (see Chapter 10.1.5 Generated Report Display Area)*

Attention! If the Preview window is already opened, the Shift Report button is not accessible. In such a case, to generate a new report, the view window of generated report has to be closed.

8.2.5 Viewing Event Log

Viewing Event Log on the Management tab page may not be friendly for an SM Operator since the Event Log automatically moves to the last event received.

To make it friendlier, the System Monitors offers a special feature. To use this feature, please click the Logviewer button or press the <Alt+F9> hot keys to open the Event Log dialog box displaying events occurred before opening this box.

The chapter 8.3.2.4 Viewing Event Log discusses the structure of the Logviewer window.

Please keep in mind that the System Monitor loads events occurred over the last 7 days by default. If needed, this period settings can be changed.

The period for loading events (including alarm events) can be configured in the *dShell.ini (Refer to chapter 5.2.2 Loading Events).*

8.2.6 Activating Screen Saver

If the Screen Saver launch is selected to be launched on a current workstation and a specified amount of time passes without the keyboard being touched or the mouse being moved, the Screen Saver will be activated.
The Screen Saver can be started manually in the System Monitor either. To do it, please click the  button or press the<Alt+F10> hot keys.

Note that the System Monitor uses the same screen saver as selected in the options of the Windows Desktop. Therefore you will have to select one of the screen savers installed on a workstation. If no screen saver is selected, the Screen Saver utility will not be activated (but an operator' password will be requested in any case).

When the Screen Saver is started, a relevant event and the name of current operator will be added to the Event Log.

When the Screen Saver is closed, the password of a current operator will be requested to enter in the appeared Logout dialog box:

In this case,

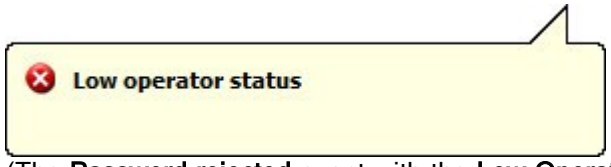
- The Cancel button is locked and unfunctional.

The further actions depend on what data are entered:

- If one clicks OK after entering the wrong password, the System Monitor:
  - will not accept the password,
  - and generate the following messages
    - in case of an unknown password:

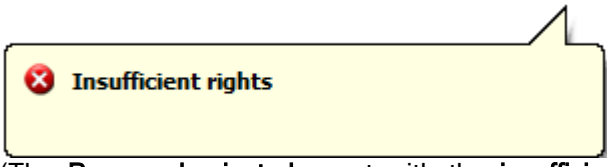
(*The **Password rejected** event and the **Password not found** description will be added to the Event Log*).

- If an employee status does not allow working with the System Monitor:



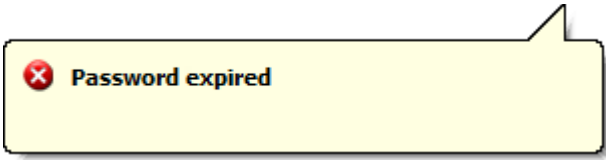
(The **Password rejected** event with the **Low Operator status** description, and the name of a password holder will be added to the Event Log)

- If the password does not provide any rights to run the System Monitor (Operative Task):



(The **Password rejected** event with the **insufficient rights** description and the name of the password holder will be added to the Event Log)

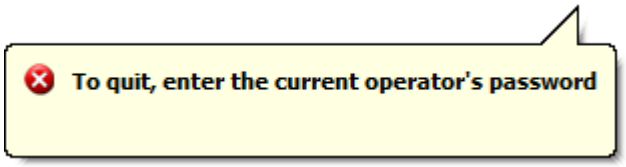
- In case of an expired password :



(The **Password rejected** event with the **Password expired** description and a password holder's name of will be added to the Event Log.

  - And will wait for the right password;

- If one enters a correct password of another operator and click **OK**, the System Monitor:
  - will not accept the password,
  - generate the following message:



The **Password rejected** event will be added to the event log. The **To quite, enter the current operator's password** record and the name of the passport holder will be added to the log as well. If the password is unknown, the name will not be added.

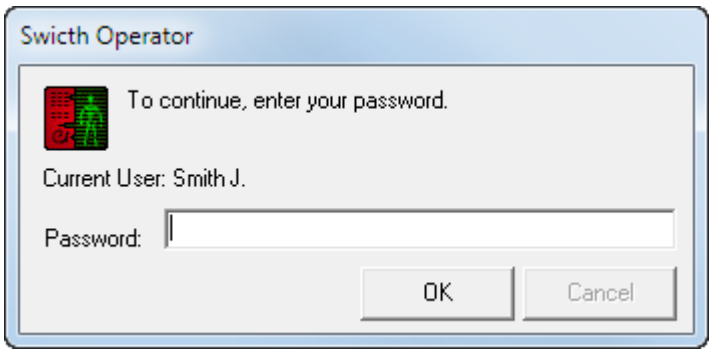
  - And will wait for the right password to be entered;

- If one enters the password of the currently logged operator and click the **OK** button, the System Monitor will respond as follows:
- It will accept the operator credential
- and allow that operator to continue working with the system

8.2.7 Switching Operator Session

During the process of work, an SM operator may need to be replaced with another one. In order to transfer the system management from one operator to another operator of the System Monitor, an operator intending to start a new session has to enter his/her personal password.

To enter a password, please click the  **Switch Operator** button or the **<Alt+F11>** hot keys to open the **Switch Operator** dialog box where a new operator starting his/her session must enter a personal password:

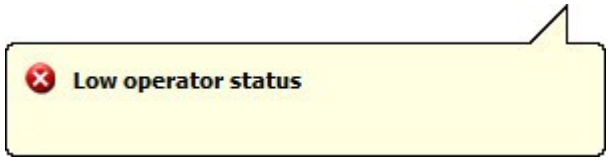


The further actions will depend on data entered
If one clicks the **Cancel** button, the switching process will be canceled:
If one enters the wrong password and clicks the **OK** button, the System Monitor will respond as follows:

- a current operator will not be switched to a new one
- and the following messages will be generate
  - in case of an unknown password:

(*The **Password rejected** event and the **Password not found** description will be added to the Event Log*).

  - If the assigned status does not allow an employee to work the System Monitor:

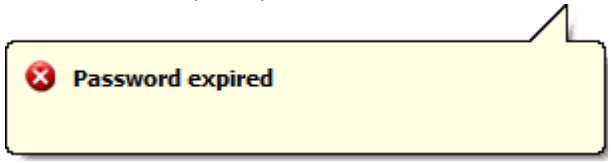


(The **Password rejected** event with the **Low Operator status** description, and the name of a password holder will be added to the Event Log)

  - If the password does not provide any rights to run the System Monitor (Operative Task):

(The **Password rejected** event with the **Insufficient rights** description and the name of the password holder will be added to the Event Log)

  - In case of an expired password:



(The **Password rejected** event with the **Password expired** description and the name of a password holder will be added to the Event Log.

- And will wait for the right password.

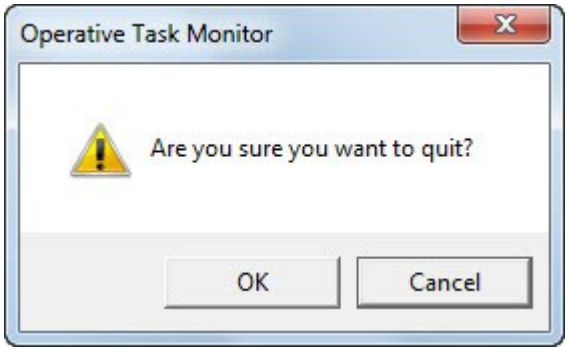
- If one enters the password of a currently logged operator and clicks the **OK** button, the System Monitor will respond as follows:
  - It will not switch to another operator session
  - But the current operator can continue working with the system
- If a correct password of another operator is entered, the System Monitor will respond as follows:
  - It will accept the entered password

- And will start a new operator session, and the **Operator Switched** event as well as the name of operator holding this password will be added to the event log.
- And the new operator will be able to manage and control the system in accordance with his/her assigned rights.

In the process of system functioning, the Database Administrator module may be instructed to restart the database. In this situation, the database will be restarted, and the status of each system entity will be obtained. In this case, a currently logged operator will continue his/her work with the System Monitor without having to enter his/her password.

8.2.8 Quitting the Application

To close the System Monitor application click the  button or press the <**Alt+F12**> button, then click **OK** in the appeared box to confirm your intention of quitting the System Monitor:



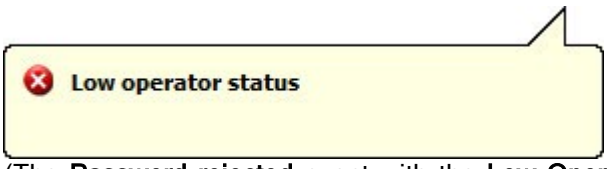
Then enter an SM operator's password currently logged on the system:

In this case:

- If an operator click the **Cancel** button, the System Monitor will not be closed:
- If one clicks  after entering the wrong password, the System Monitor:
  - will not accept the password,
  - and generate the following messages
    - in case of unknown password:

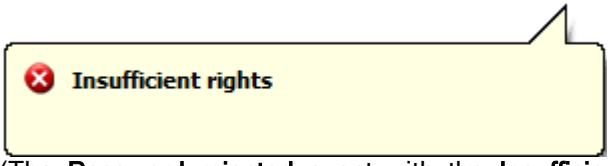
(*The **Password rejected** event and the **Password not found** description will be added to the Event Log*).

- If a person's system status does not allow working with System Monitor:



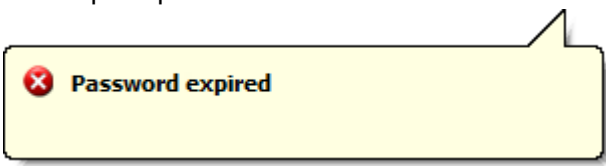
(The **Password rejected** event with the **Low Operator status** description, and a password holder name will be added to the Event Log)

- If the password does not provide any rights to run the System Monitor (Operative Task):



(The **Password rejected** event with the **Insufficient rights** description and the name of the password holder will be added to the Event Log)

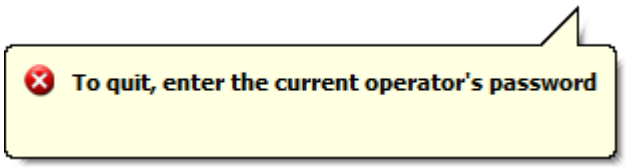
- If an expired password:



(The **Password rejected** event with the **Password expired** description and the name of a password holder will be added to the Event Log.

  - And will wait for a correct password;

- If one enters the correct password of another operator and click **OK**, the System Monitor will respond with the following:
  - It will not accept the password, and
  - generate the following message:



The **Password rejected** event will be added to the event log. **To quite, enter the current operator's password** record and the name of the passport holder will be added to the log as well. If the password is unknown, the name will not be added.

  - And will wait for the right password to be entered

- If one enters the currently logged operator's password and click the **OK** button, the System Monitor will respond as follows:
  - It will accept the operator's password,
  - and the application will be closed

    (*The **Monitor closing** message and the name of an operator will be added to the Event Log)*

Attention! If the System Monitor and Scanning Core both are running on a current workstation, the following will happen when the System Monitor is shut down:

- *If the current workstation shares events and states with any other workstations in the system, the Scanning Core of the current workstation will continue running*

- *If there is only one workstation in the system or that workstation does not share any events to any other workstation in the system, the Scanning Core of this workstation is shut down.*

8.2.9 Floating Panes

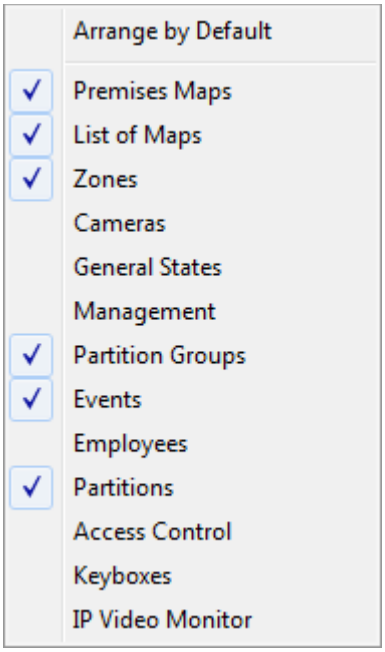
The Graphic User interface of the System Monitor includes the floating panes:

- When the Management tab is opened the following window panes can be accessed:
    - Premises Maps
    - List of Maps
    - Zones
    - Cameras
    - General States
    - Management
    - Partition Groups
    - Events
    - Employees
    - Partitions
    - Access Control
    - Keyboxes
    - IP Video Monitor
    - Events
- Alarm Handling Tab:
    - Event Log
    - Premises Maps,
    - Alarm Handling bar,
    - Video Cameras (IP Video Monitor).

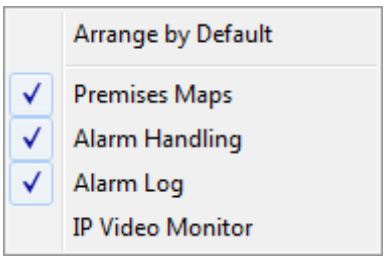
Note that, IP Video Monitor is displayed on the Management and Alarm Handling tabs at the same time.

Each of the above windows can be closed and reopened. To do that, please click the  button and select a required item in the appeared menu:

- On the Management tab:



- On the Alarms Handling Tab page:



With a window pane item is checked item, a related pane will be shown on the screen, if an item is unchecked, it will be closed.

The application remembers the positions of each pane and box, and if any is reopened it will appear in the recent location on the screen.

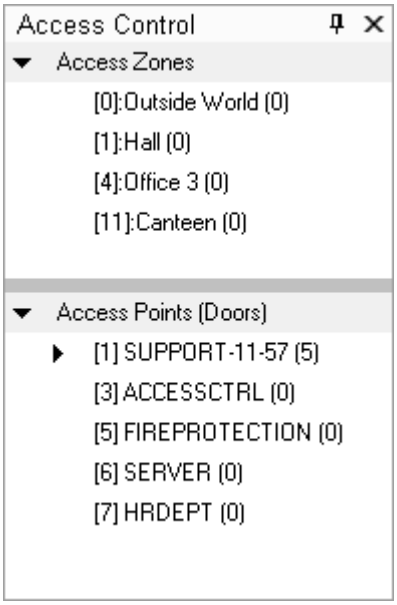
A floating pane can be located within the System Monitor area, or it can be attached to a right, upper, or bottom inner side of the System Monitor. Floating panes can be placed outside the System Monitor main window.

A floating pane can be displayed entirely, or it can be represented by an icon (in case of attachment to the System Monitor's side) but it appears for a time while being pointed by a mouse cursor.

Further example explains how to move and dock the Access Control pane:

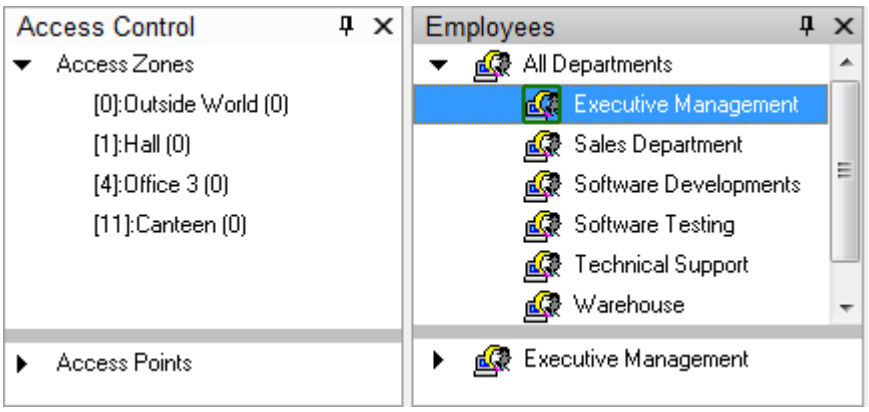
By default the window pane is closed. To show it, please click the  button and select the **Access Control** item in the dropdown menu.

The window pane will be shown within the main window of the System Monitor.
Dragging the pane by the title bar you can place it within the main window of the System Monitor on top of all other windows. In this case it should be resized as needed.

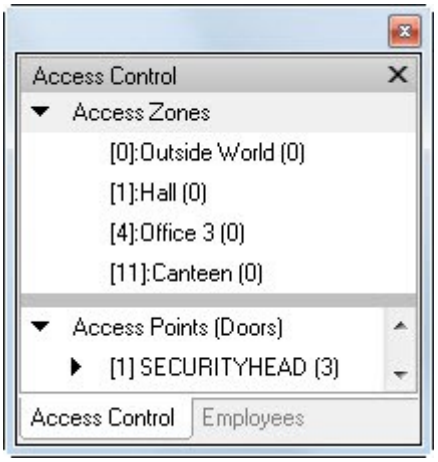


A user can move the pane to dock it to any side of the Management tab page. If another floating pane is already attached to this side, the following can be done:

The Access Control pane can be placed next to other pane:



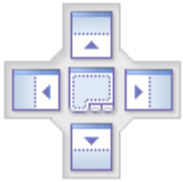
- Or tabbed with another window.



(in this case, to toggle between panes you must click a title tab of a related window pane).

To attach a pane to any side of the main window, please proceed with the following:

- When one starts moving a pane to one of the System Monitor side, one of the following icon will appear:
-  , , , or .
  If the floating pane is dragged to this icon, the pane will be attached to a chosen side of the main window
- When a window is moved towards any already attached window pane, the following icon will appear:



- If one drags a pane to the right, left, upper or bottom part of this icon, the pane will be attached to the right, left, upper, or bottom inner side of the attached window.
- If a user positions a floating pane to the center of the icon, the pane will be grouped (tabbed) with already attached pane.

If you want close a window pane, please click the upper right  button.

To hide a window pane, please click the  button (in the upper right corner). In this case the pane will be transformed into a tab-like icon and when a mouse is pointed to the icon, the pane will appear:

To lock the pane on the screen, please click the button (the right upper corner) when the window pane is displayed.

Please note that all windows can be arranged by default to look as if the System Monitor is launched first time. To do that, click the  button and select the **Arrange by Default** item.

8.2.10 Application Parameters

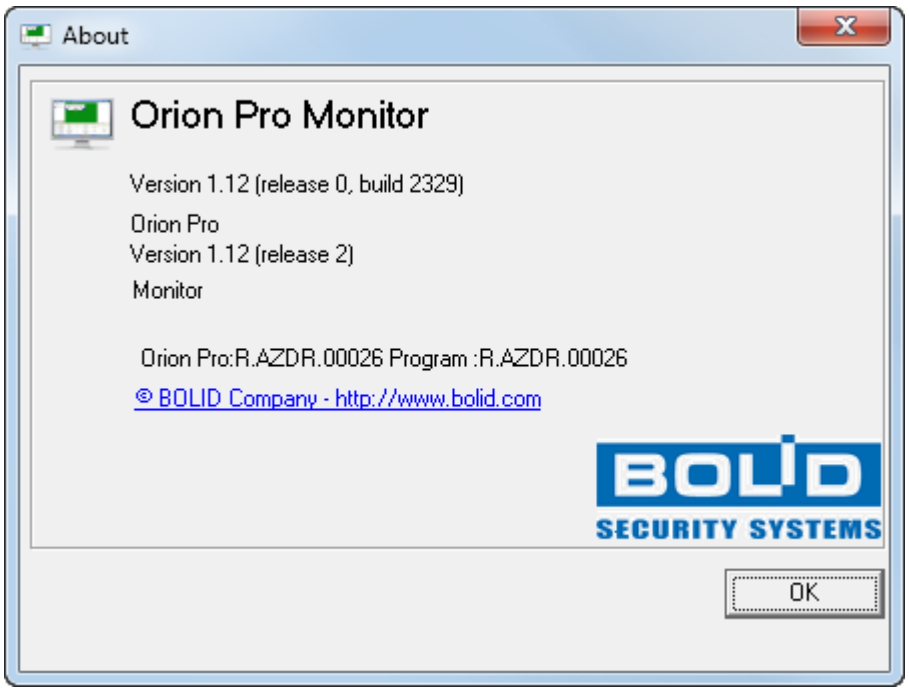
To access the application parameter, please click  :

Parameter	Description
Error Log	Opens the Error Log of the System Monitor.
Allow Resizing	When checked, it allows resizing the main window, otherwise it's not allowed.
Allow Moving	When checked, it allows moving the main window, otherwise it's not allowed
Allow Minimizing	When checked, it allows minimizing the main window, otherwise it's not allowed.
On Top	When unchecked, it allows any other window to be displayed on top of the window of the System Monitor; otherwise it is not allowed.
Sticky Window	When this item checked, the window of the System Monitor will be automatically docked to a screen side, if it is dragged closely to this side edge.
About	Displays a window with information about the application (see the next chapter).

8.2.11 The About Window

To open the About window showing the information on the Bolid Company and the Orion Pro Suite, please click the  button and select the About menu.

The About window will appear:



8.3 Management Tab Page

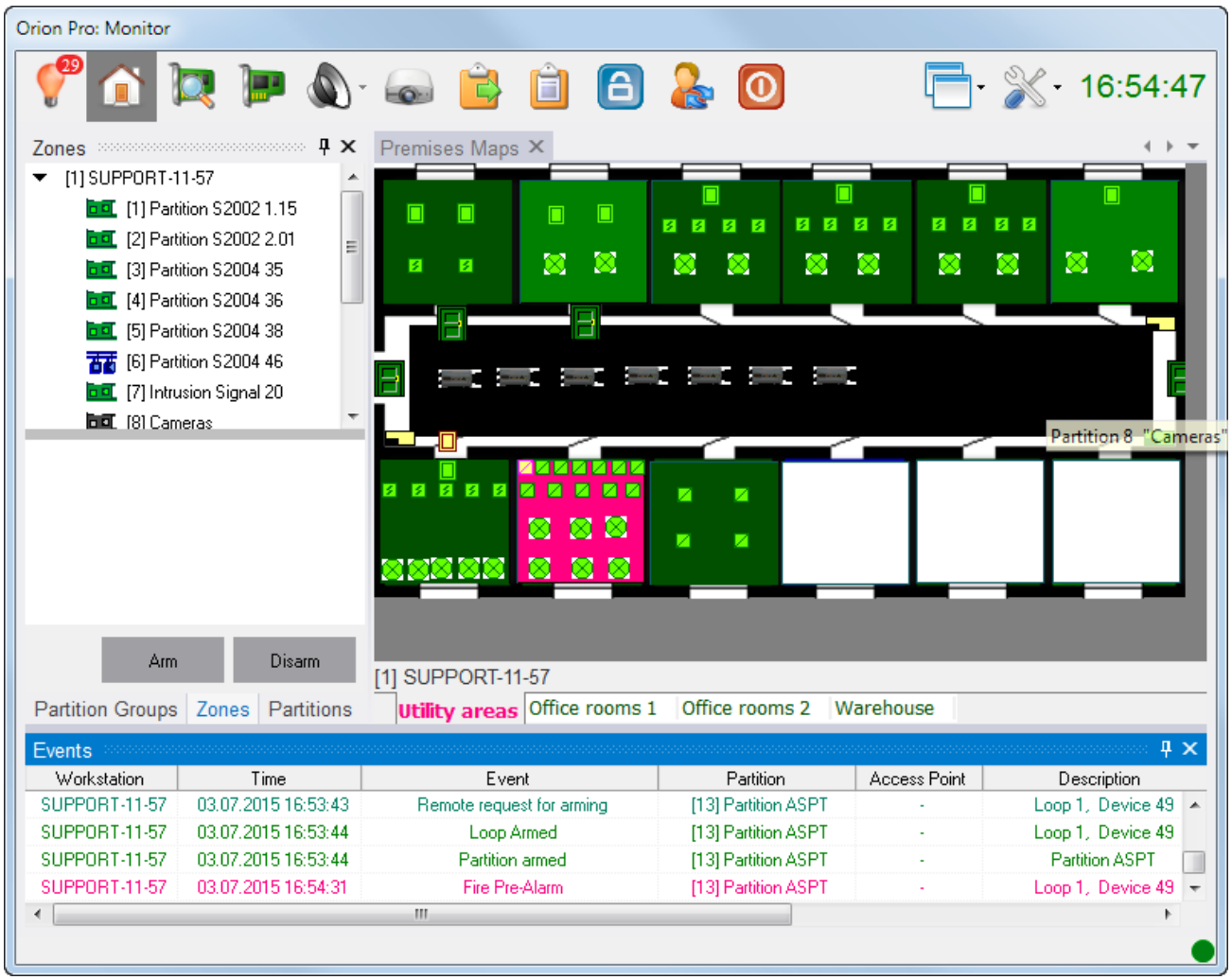
To switch to the Management tab, please click the  button or press the <**Alt+F2**> hot keys.

The management tab offers the following functions:

- Interactive display of system entities status on maps and management tabs;
- Display of system events in real time;
- Tracking employees online with resolving power up to an access zone;
- Operator's online control of the following:
  - Zones
  - Partitions
  - Partition Groups
  - Cameras
  - Access Points
  - Keyboxes
  - Fire Extinguishing
- Launch of Management Scenarios by an operator.

8.3.1 Management Tab User Interface

The figure shows the management tab page:



As the System Monitor main tabs include arrangeable floating panes, the following should be noted for the Management tab page:

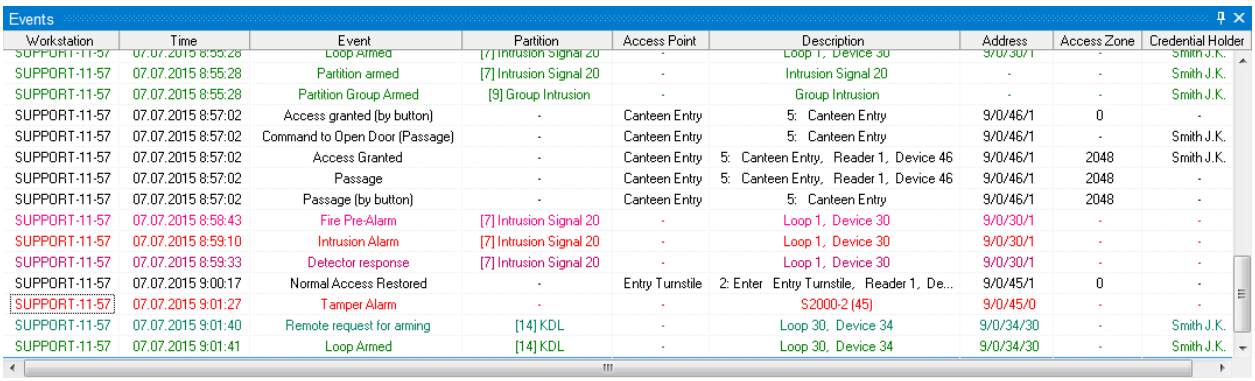
1. The Event Log is recommended on the bottom of the page

2. The following panes can be located in any order and place on the tab page:
   - Premises Maps
   - List of Maps
   - Partition Groups
   - Partitions
   - Zones
   - Cameras
   - Management
   - Employees
   - Access Control

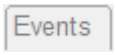
8.3.2 Event Log

When an event occur in the system it is recorded in the Event Log

It is recommended placing the Event Log pane at the bottom of the Management tab page. The Event Log will look like the following:



If the Event Log is not locked on the tab page and minimized down, please put the mouse cursor over the Events icon:



The following elements of the pane can be adjusted:

- The width of the Event Log' columns
  Move the mouse cursor to the edge of the column head, click the mouse, and adjust the column width as required.

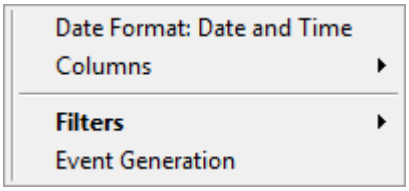
- Columns orders.
  Hover the mouse cursor the column head and drag it to a required place.

- The number and types and displayed columns.
  (discussed further in this chapter)

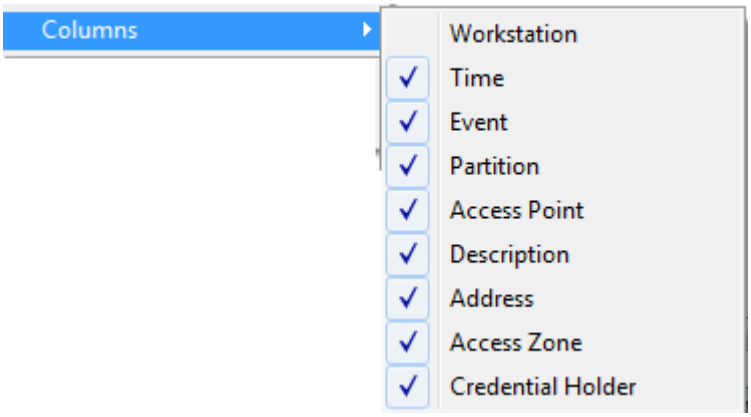
- Date and time format.
  (discussed further in this chapter)

- System events to be displayed (using filters for events)
  (Refer to chapter 8.3.2.3 Event Log Filter. The Filters Menu.

If you right click the Event Log area, the following contextual menu will be displayed:



- Using the **Data Format:** a user can define the format of the date and time:
  - Time Only
  - Date and Time.
- Using the **Columns** button: This items allows selecting columns to be displayed in the Event Log:



By default, all columns are selected to be displayed in the log

- The **Filters** item allows configuring filters for the event log.

  (*See chapter Refer to chapter 8.3.2.3 Event Log Filter. The Filters Menu)*

- Using Event Generation menu item, an operator can add an event to the event log.

  (see chapter 8.3.2.5 Adding Event to the Event Log)

8.3.2.1 The Structure of the Event Log

The Event Log shows the following information:

Column	*Description*	*Example*
Workstation	Workstation of event occurrence.	SUPPORT-11-57 SUPPORT-11-57 SUPPORT-11-57
Time	Date and time of event occurrence. *(In can be set to show an event time only)*	07.07.2015 8:59:33 07.07.2015 9:00:17 07.07.2015 9:01:27
Event	Event Name	Normal Access Restored Tamper Alarm Remote request for arming
Partition	If an event occurred in a partition or partition group, this field would show the ID of partition or partition group In all other cases, this field is empty	[7] Intrusion Signal 20 [7] Intrusion Signal 20 [7] Intrusion Signal 20 - - [14] KDL
Access Point	If an event occurred relates to an access point, this field would show the ID of partition or partition group In all other cases, this field is empty	Canteen Entry - Entry Turnstile
Description	The name of entity related to the event, or the auxiliary information.	5: Canteen Entry, Reader 1, Device 46 5: Canteen Entry Loop 1, Device 30

Address	If an event is related to a device, input loop, reader, or relay output, this field displays the address of a system entity. *(In case of an access point, it will show the address of a reader controlling this access point in a corresponding direction*) The format of displayed address: *HCOMPort/PanelAddress/Device Address/EntityAddress* Attention: • If a device connected to any COM Port with Orion protocol, *Panel Address is 0*; • In case of S2000 (S2000M), *Device Address* is 0; • In case of devices, Entity Address is 0. • In case of biometric reader, it will display the IP address in square brackets In all other cases, the field shows '-' (dash).	9/0/30/1 9/0/30/1 9/0/30/1 - - 9/0/46/1 9/0/30/1 9/0/30/1 9/0/30/1 9/0/45/1
Access Zone	In case of access control events, this field will show a zone as reported a device related to the event (event device) (*it can be empty for some access points)* In all other cases, the field will show '-'(dash).	2048 - - 0
Credential Holder	If the events related to any employee actions, this field shows the name of this employee In all other cases, the field shows '-'(dash).	- Smith J.K. Peterson P. Tuma B.

Some events (mainly related to access control) may have additional data such as: No rights, Time Zone Breached, etc.

Such events is labeled with (*) asterisk. To view additional data, please double click an asterisked event to open small box with additional data:

Event	Partition
(*)Access Denied	-
(*)Access Denied	-
Authentication	

Antipassback

8.3.2.2 Displayed Color Scheme

The main events have certain font colors such as:

Time	Event	Partition	Access Point	Address
07.07.2015 8:55:	Partition armed	[7] Intrusion Signal 20	-	-
07.07.2015 8:55:	Partition Group Armed	[9] Group Intrusion	-	-
07.07.2015 8:57:	Access Granted	-	Canteen Entry	9/0/46/1
07.07.2015 8:57:	Passage	-	Canteen Entry	9/0/46/1
07.07.2015 8:58:	Fire Pre-Alarm	[7] Intrusion Signal 20	-	9/0/30/1
07.07.2015 8:59:	Intrusion Alarm	[7] Intrusion Signal 20	-	9/0/30/1
07.07.2015 9:01:	Tamper Alarm	-	-	9/0/45/0
07.07.2015 9:01:	Remote request for arming	[14] KDL	-	9/0/34/3(
07.07.2015 9:01:	Loop Armed	[14] KDL	-	9/0/34/3(

The Appendix 8 B System Events provides color scheme for all event within the system.

Note that when events are read from devices, old events will be highlighted yellow:

A-VASILIEV	10.12.2013 16:22:58	Camera connected	Camera	[1] IP
A-VASILIEV	09.12.2013 16:35:27	Local programming	Reader 1, Device 1	1/1/0/1
A-VASILIEV	09.12.2013 17:21:28	S2000 console has been turned on	S2000 (1)	1/1/0/0
A-VASILIEV	09.12.2013 18:11:51	Mains failure	AL 23, Device 7	1/1/7/23

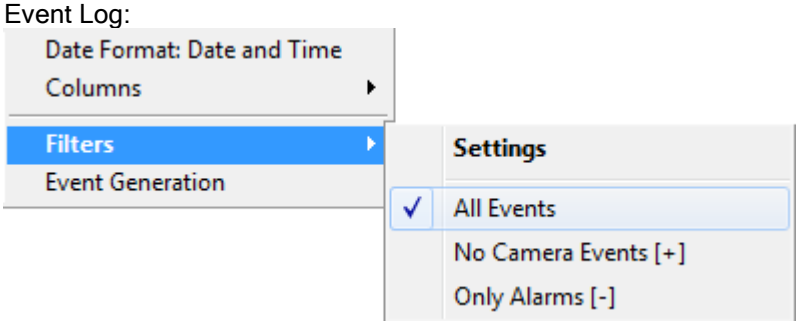
8.3.2.3 Event Log Filter. The Filters Menu

The System Monitor has functionality to exclude required events from displaying in the event log.
The Event Log logs ALL events, but if filters are used in the System Monitor, some events are not displayed.

By defaults, all system events are displayed.

The set of event filters can be defined using the **Filters** contextual menu of the Event Log
(Appendix 8.A *Creating Custom Event Filters* describes how to create custom filters)

To select a required event filter, please click the title of a corresponding filter in the contextual menu of the Event Log:



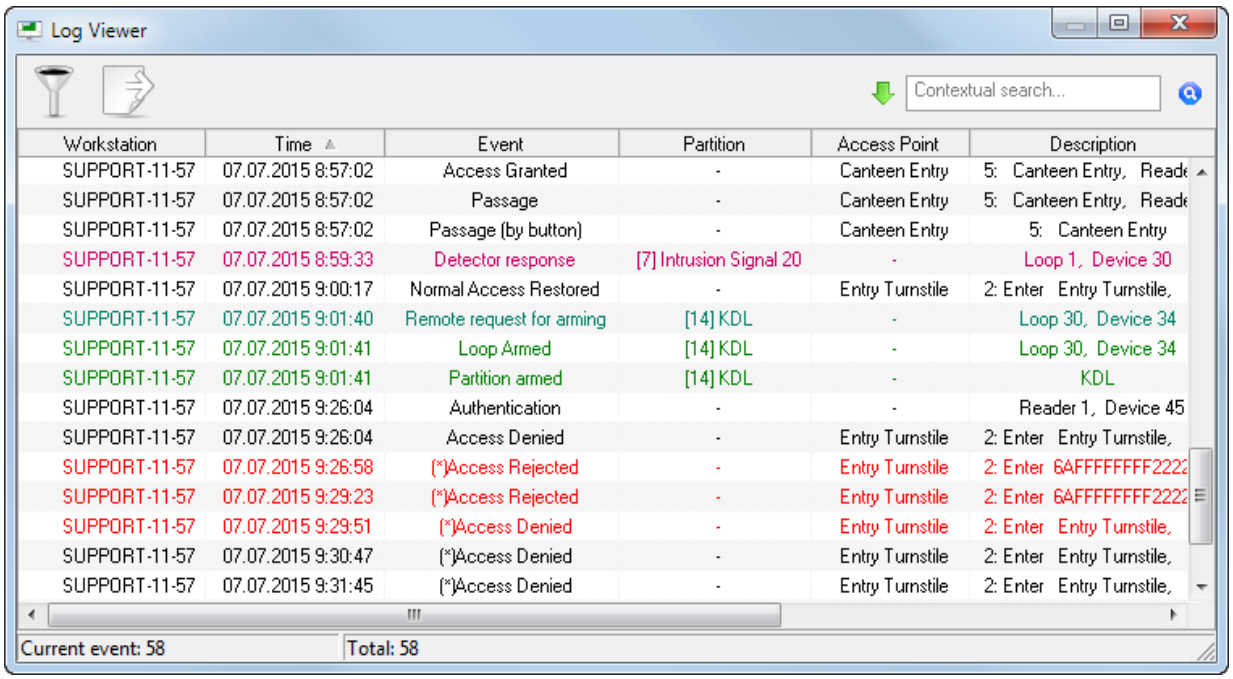
Symbols in brackets **[+]** (Inclusive or **[-]** Exclusive after the filter name shows the type of filter

Type	*Description*
Inclusive	The Event Log shows only events included in the filter
Exclusive	The Event Log does not show events included in the filter

8.3.2.4 Viewing Event Log

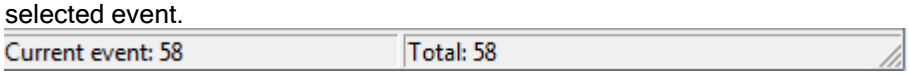
As said above, when an event occurred in the system, it is recorded to the Event Log. Since this is a real time process, all events are constantly being added to the Event Log, and when there are too much events, it may be difficult to view the Event Log for it always moves to the last added event.

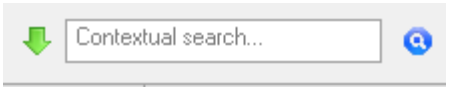
To make viewing the Event Log friendlier, the Log Viewer is provided. To open the Log Viewer, please click the  button or press **<Alt+F9>:**



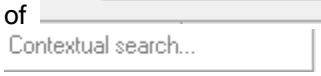
The Log Viewer shows all events displayed in the Event Log of the Management tab (in accordance with applied filter) till the moment of clicking the  button.

The status line at the bottom of the window shows number of loaded events and the ID number of a selected event.



With the help of 

box, one can search an event in the event log:

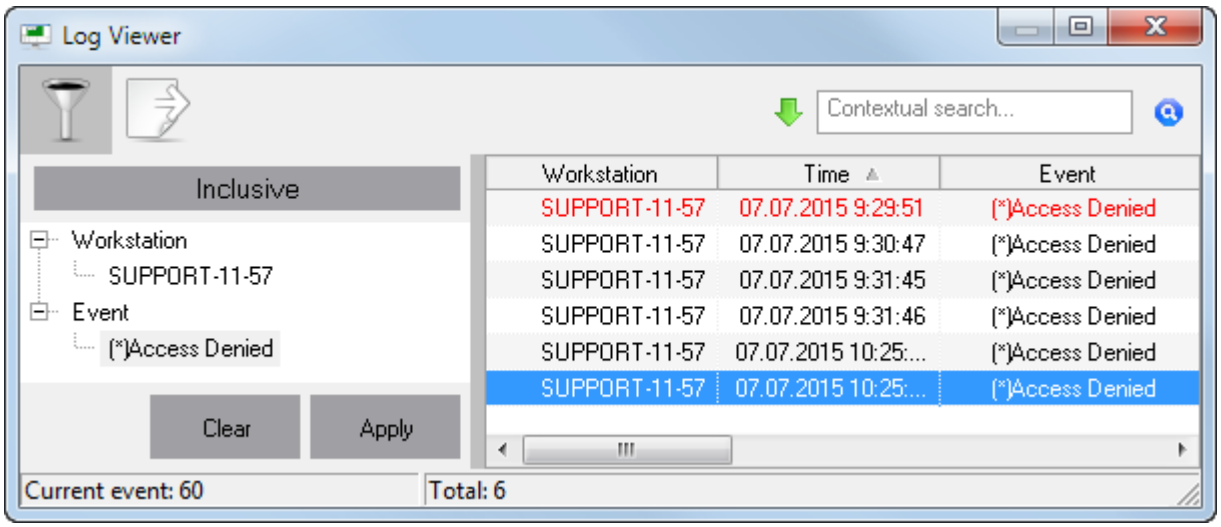
- The 

field serves to type a text to search through all columns of the event log. When a text is entered, it immediacy moves to the first events contains this text.

- Clicking the  button moves to the next event that contains the text in one of the columns the same as entered in the search field.

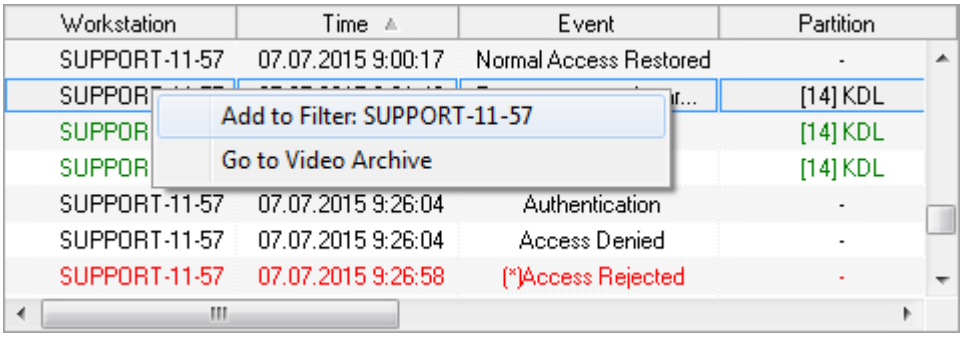
- The  buttons selects a search direction.

The  button opens a side pane to apply an additional filter for events displayed in the Log Viewer:

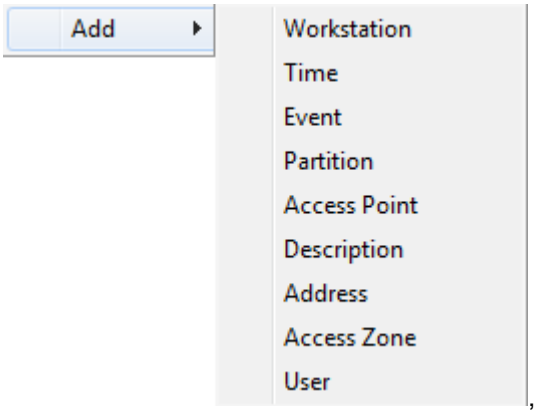


In order to add some element to, please do the following:

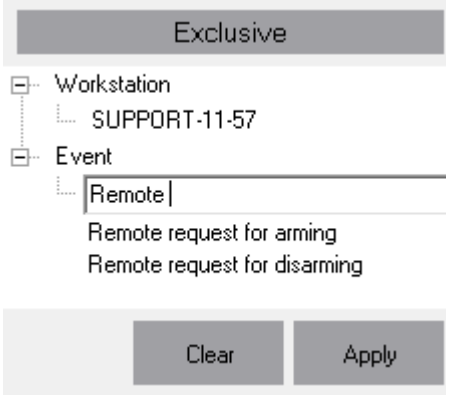
- Right click a required element in the list of events and select a required item in the appeared menu:



- Or right click on the filter area and select a type of filter in the contextual menu:



Then type a desired name of the element:



*Under the value being entered, you can see the name of event that includes the entered text.. You can select this text using the mouse or the **Down** cursor key.*

Clicking Inclusive and Exclusive, one can toggle between types of filters:

- **Inclusive**: If this type of filter is applied, the event list will contain only events that includes all applied elements of the filter
- **Exculsive**: If this type of filter is applied, those events that include all elements of this filter will be removed from the list of displayed filter.

To apply filter to the list of events, use the **Apply** (Apply) button.

The **Clear** Clear button disables filter and clear it from all elements.

Using the  button one can export the list of events (in accordance with an applied filter) to a tab-delimited text file (* txt).

When a user click the  button, the **Save As** dialog box will appear. Then enter a file name, select a file location, and click **Save** to export the list of events.

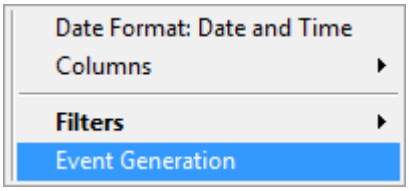
8.3.2.5 Adding Events to the Event Log

It may happen that an employee (as a database entity) has to be moved from one access zone to another.

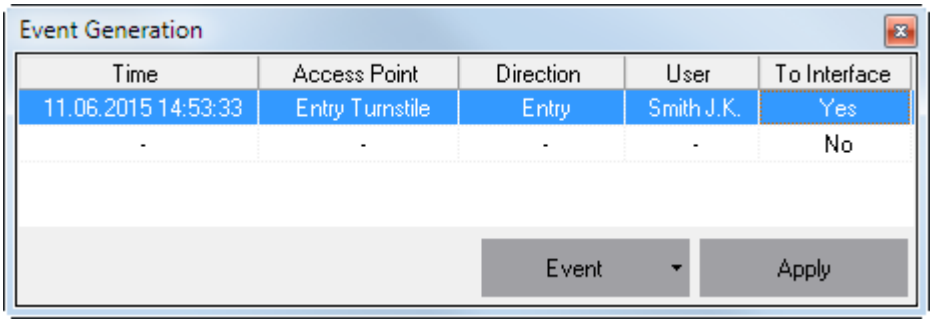
For example, it is known that an employee has left for home by jumping over the fence, but his/her working time is still counting.

As a countermeasure, the System Monitor offers the generation of the **Passage** event via a required access point in an appropriate direction for a selected employee.

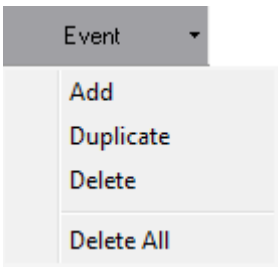
To do that, please click the **Event Generation** item in the contextual menu of the Event Log to open the Event Generation box:



The Event Generation box:



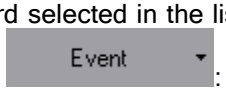
Click the **Event** button, and then click the **Add** item in the appeared contextual menu to add a new record for event generation.



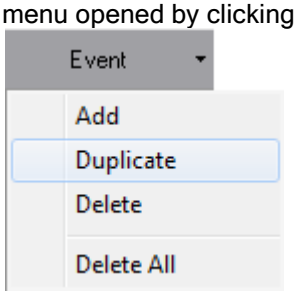
The following has to be selected for each record:

- Time of event generation,
- Access point
- Access direction through access point
- An employee for whom the event is generated
- Whether the event of committed access is to be shared (**To Interface**) with other devices (required for antipassback)

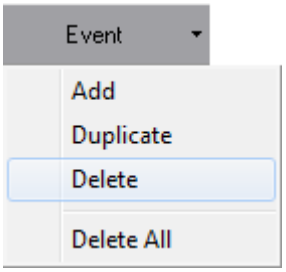
An access point, direction, and employee are selected from the dropdown menus. When the **Time** field is clicked the first time, the current data and time will be added to the column.

To add a copy of a record selected in the list of events, please click the **Duplicate** item of the contextual menu opened by clicking 

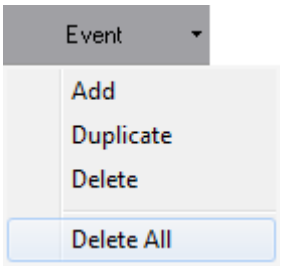
:



To delete a selected record from the list of events, please click the **Delete** item in the contextual menu:



To delete all records from the list of events, please click **Delete All** in the dropdown menu:



The **Apply** button is used to generate the **Passage** event for each record in the list. When generation of all events is completed, the list of event will be cleared.

The event generation process is the following

- If an event is set to be shared with other devices (to interface), the **Passage** event will be generated by a relevant Scanning Core (with a connected device controlling an access point selected in the event generation record).

  Once the event has been generated
  - This event will be shared to devices and other workstations
  - The employee will be moved to a relevant Access Zone in the Scanning Core as well as in all System Monitors of the system,
- If the event sharing option (To Interface) is not selected, the **Passage** event will be generated by the current System Shell.

  When generated, the event will be recorded into the Database with no other actions.

Further, such a generated event will be used by the Time and Attendance application.

8.3.3 Management and Information Panes

Premises maps, management, and info panes are used to control entities and obtain information on their status. The Premises Maps will be discussed further in *Chapter 8.3.4 Premises Maps.* This chapter discusses management and info panes.

The System Monitor can display the following management and info panes:

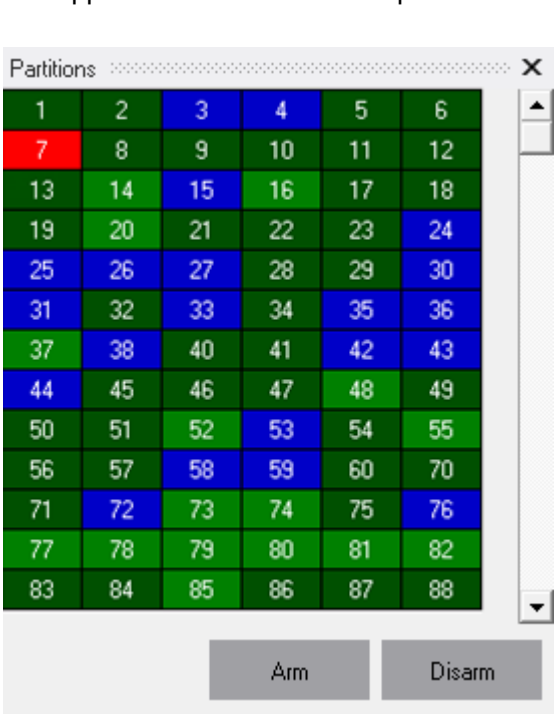
- The **Partition** pane:
  - Arming and disarming partitions
  - Obtaining info on a selected partition status
- The **Zones** pane
  - Arming and disarming zones
  - Obtaining info about zones and their status
- The **Partition Groups** pane
  - Arming and disarming partition groups
  - Obtaining info about partition groups and their status
- The **Management** pane
  - Launching management scenarios (scripts) using a management tree
- The **Employees** pane
  - Obtaining information on department personnel
  - Obtaining information on employees
  - Granting an access permit to each employee
- The **Access Control** pane
  - Obtaining info on names and quantity of employees attending each access zone
  - Obtaining info on employees and access zones
  - Granting access via access points
- The **Cameras** pane
  - Camera control functions
  - Obtaining info on cameras and their status
- The **Keybox** pane
  - Controlling keybox cylinders

8.3.3.1 The Partitions Pane

The Partition pane has the following functions:

- Arming and disarming partitions
- Obtaining info on partition status

The appearance of the Partitions pane:



The pane includes the following elements:

1. The table of Partitions
2. The **Arm** and **Disarm** buttons

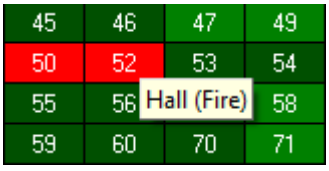
The partition table includes numbers of partition in the following order:

- The first partitions are those of the workstation where the System Monitor is running, in ascending order by a partition number
- They are followed by other workstations' partitions in ascending order by a partition number

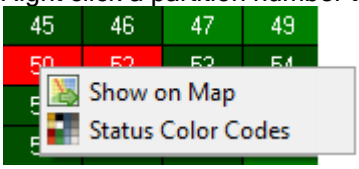
Each partition cell is highlighted in accordance with the status of that partition.

The color codes for partition states are provided in the Appendix 8 C

When a mouse cursor hovering on a partition number, the partition name will appear

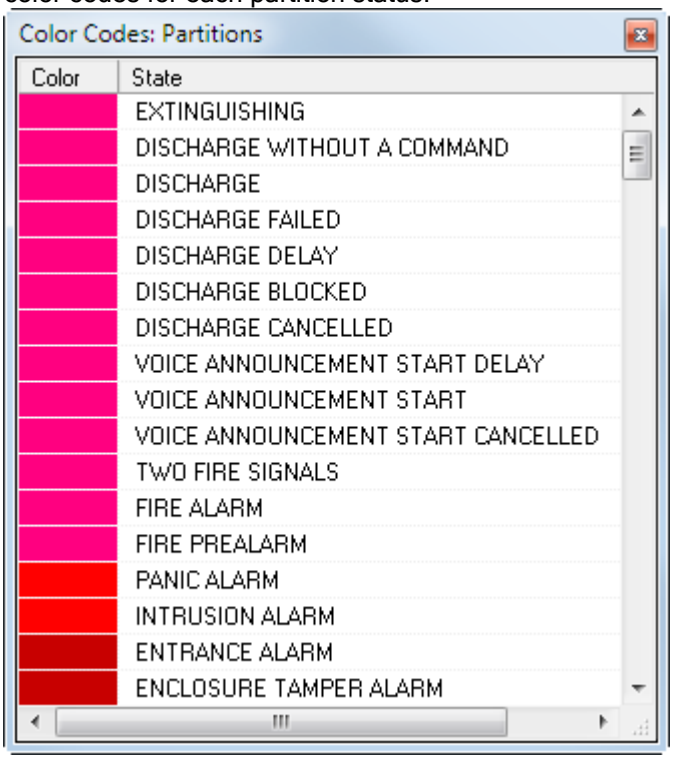


Right click a partition number to open a contextual menu:



If you select the **Show on Map** item, it will toggle a map with this partition and this partition flashes one time with another color (for finding it quickly on the map)

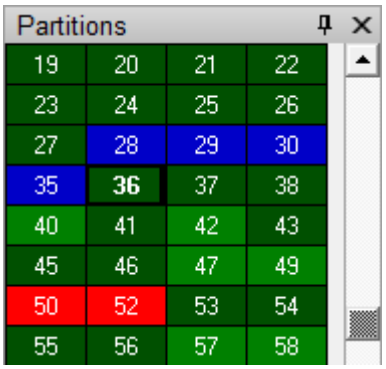
If you select, Status Color Codes item, the **Color Codes: partitions** window will be displayed. It shows color codes for each partition status:



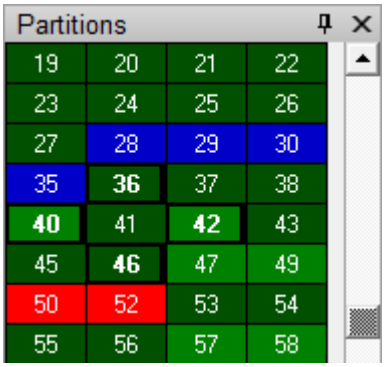
8.3.3.1.1 Operating the Partition Entity

8.3.3.1.1.1 Selecting Partitions to Control

To select a partition, click a partition number, the selected partition will be highlighted:



To make a multiple selection, hold down <**Ctrl**> key and click a required partition numbers. The selected partition will be highlighted.



Or click a partition number then select required partitions without releasing a mouse button.

8.3.3.1.1.2 Arming Partitions

To arm one or multiple partition(s), please:

1. Select one or more partitions

2. Click the **Arm** button:

After clicking the **Arm** button, the following will be done for each partition:

- If an operator has rights to operate a partition, arming a partition will be attempted:

  - The **Remote request for arming** event, partition's number and name, and operator's name will be added to the even log.

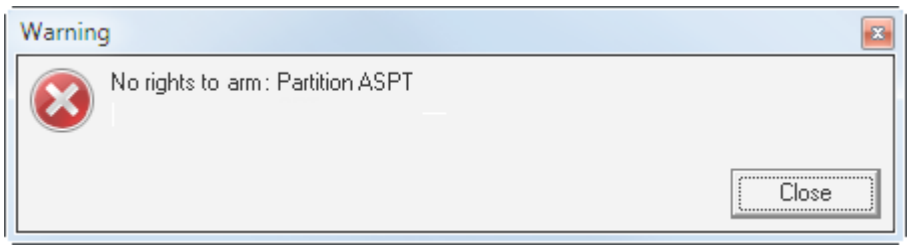
  - A command will be sent to a relevant device (camera) to arm each loop (camera) of the partition, if that loop type allows arming

  - When all arming requests are responded (received events on arming loops (cameras) or failed arming, the partition status will be finalized.

    Thus, the partition will go to the **Armed** status only when all loops (cameras) of relevant types will be armed. In this case, the **Partition Armed** event will be generated.

- If an operator:

  - Has not rights to operate a partition but has rights only to disarm a partition, there will be no attempts to arm a partition and the following message box will appear:

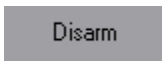


8.3.3.1.1.3 Disarming Partitions

To disarm one or multiple partitions, please follow the instruction below:

1. Select one or more partitions ;

2. Click the **Disarm** button:



After clicking the **Disarm** button, the following will be done for each partition:

- If an operator has rights to operate a partition, disarming a partition will be attempted:

  - The **Remote request for disarming** event, partition's number and name, and operator's name will be added to the even log.

  - Instruction will be sent to a relevant device (camera) to disarm each loop (camera) of the partition, if that loop type allows disarming

  - When all disarming requests are responded (received events on disarming loops (cameras) or failed disarming, the partition status will be finalized.

    Thus the partition will go the Disarmed status and the Partition Disarmed event will be generated.

(If a partition was in the Armed status, the **Partition Disarmed** event would be generated right after any first loop (camera) of the partition is disarmed .

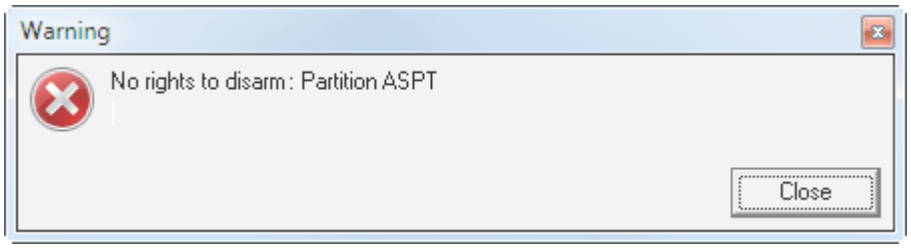
- If an operator:

  - has no rights to operate a partition but

  - has rights only to arm a partition and

  - has no rights to operate a High Security partition, but the partition is defined as one of High Security,

  the partition will not be disarmed and the following message box will appear:



Please note that when an operator deals with a partition, requests to disarm are never sent to loops such as Auxiliary loop, Panic button loop, and 24-hour loop.

Therefore, if a partition includes only Panic alarm zones and/or 24-hour zones, this partition will be disarmed.

The Appendix C Commands for loop described possible commands for all types of loops.

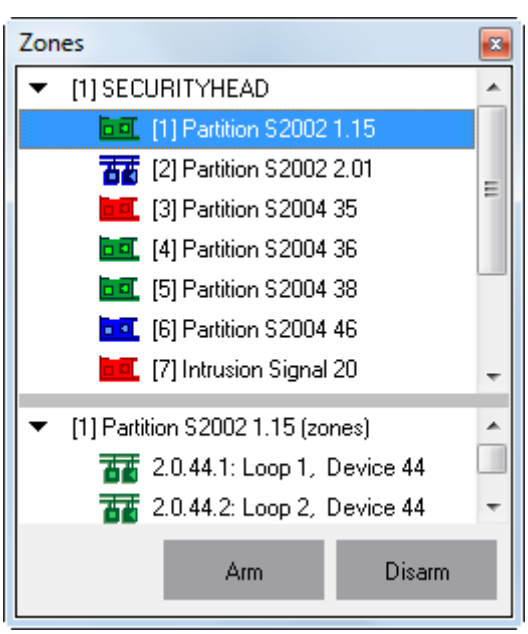
8.3.3.2 The Zones Pane

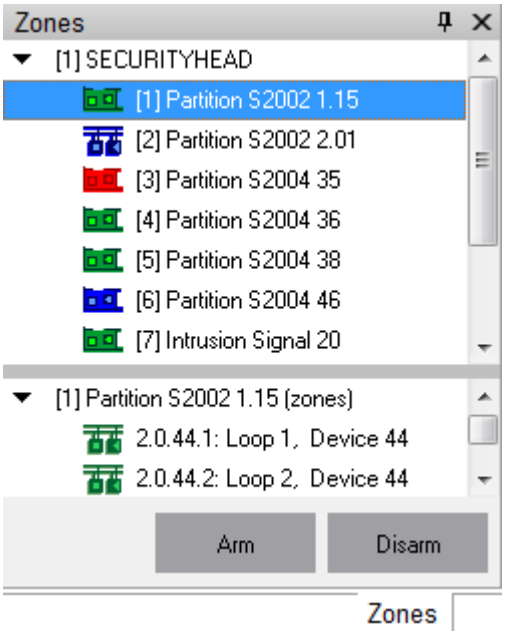
The Zones pane has the following functions:

- Arming and disarming zones and partitions

- Obtaining info about zones, partitions, and their status

The appearance of the Zones pane:



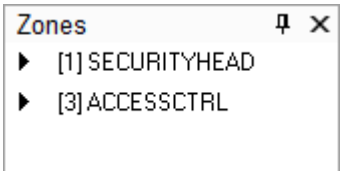


The figure shows the following elements of the pane:

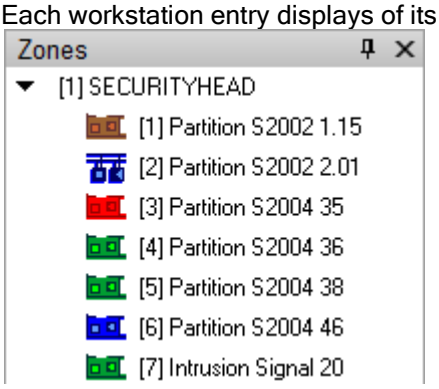
1. The list of partitions for each workstation
2. Zones of a selected partition
3. The Arm and Disarm button to operate zones or partitions.

The upper part of the pane includes workstation in the following order:

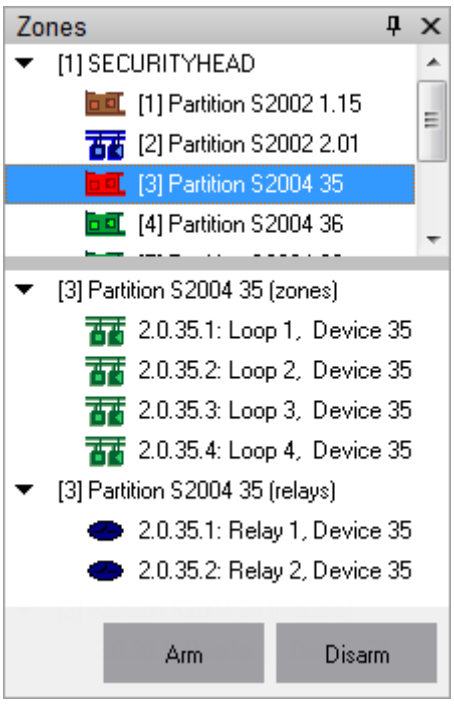
- The first one is a workstation where the System Monitor is running.
- Then other system workstation in the ascending order by their ID in the database.



Each workstation entry displays of its assigned partitions:

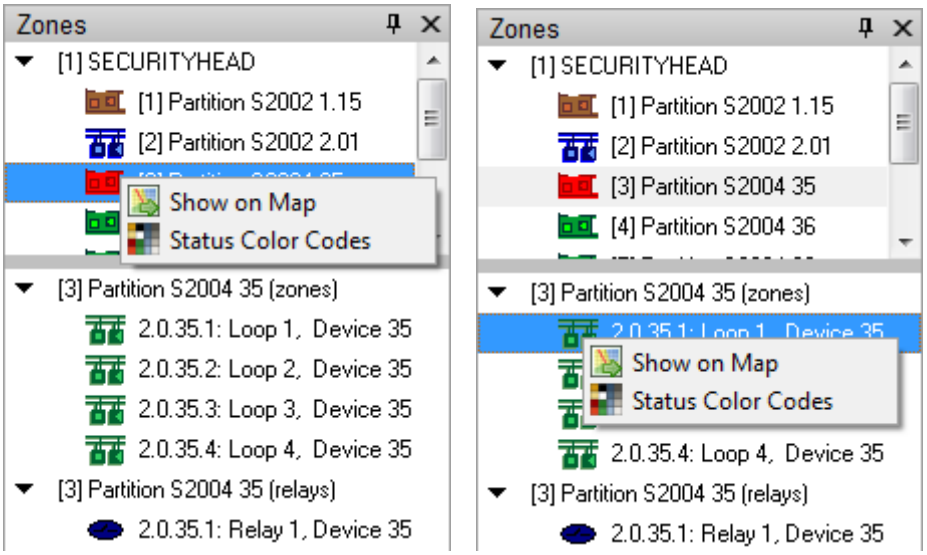


When any partition of the upper part is selected, the lower part will display zones (loops, relay outputs, and cameras) associated to the partition:



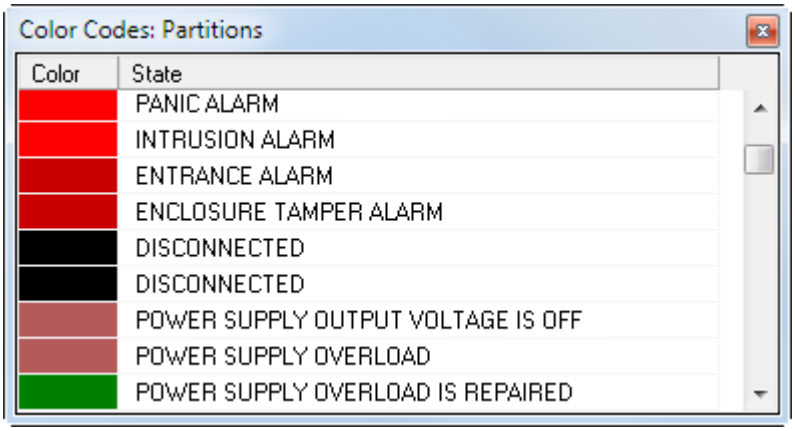
Each partition and zone (loop, relay output, and camera) is highlighted in accordance with their states. (*the color codes representing each status of partitions, loops, and cameras are provided in the Chapter 8.C Color Coders of System Entity States)*

Right click on the partition or zone number (ID) to open the contextual menu:



If you select the **Show on Map** item, it will toggle a map with this zone, and this zone flashes one time with another color (for find quickly on a map)

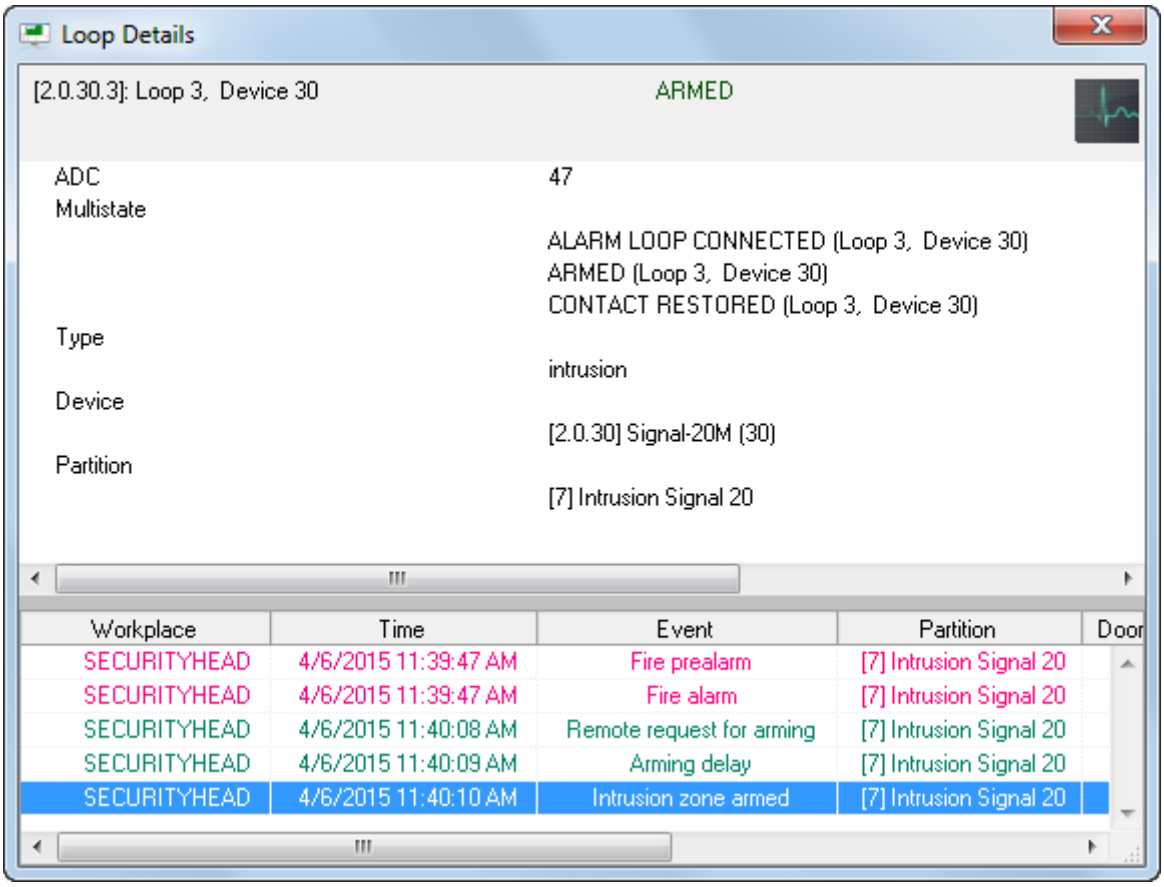
If you select, Status Color Codes item, the **Color Codes: Partitions** window will be displayed. It will include color codes for each entity status:



8.3.3.2.1 Obtaining Information about Loops, Relays or Cameras

The partition can include loops, relay outputs, and cameras. The information on each of these entities can be obtained using the Zones pane.

To get information about a loop, please double click the name of a loop to open the **Loop Details** window:



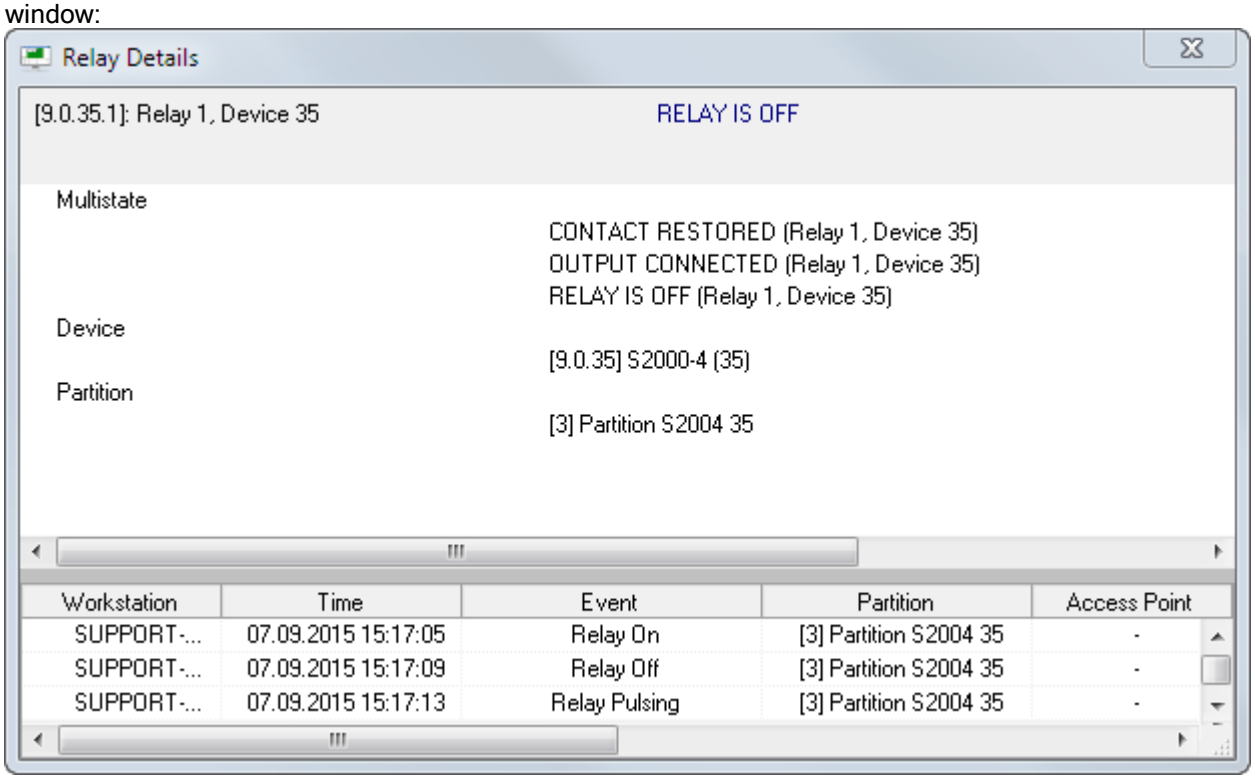
The **Loop Details** window shows the following information about the loop:

- The address and name of a loop
- The main status of a loop
- ADC data of devices' loops if those devices are able to provide it (send it back)
- Multistate (*)
- Type of loop
- The address and name of a device where this loop belongs to
- Loop events

(*) See chapter 8.1.2 for the description of the multistate of entities

The  button is used to update (request again) ADC values.

To get information about a relay output, please double click a relay output to open the **Relay Details** window:

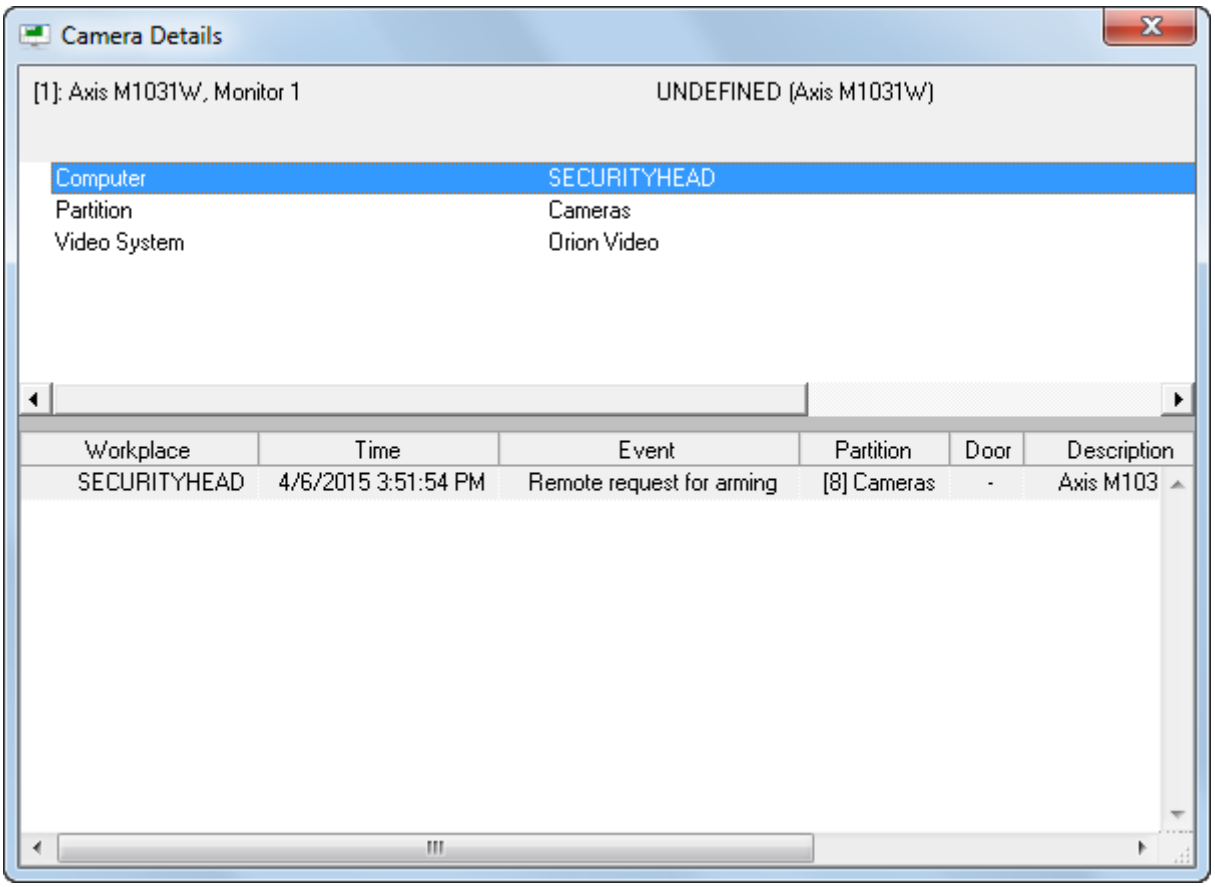


The **Relay Details** window shows the following information about the relay output:

- The address and name of the relay output
- The relay main status
- The multistate of the relay output (*)
- The address and name of a device where this loop belongs to
- The number and name of a partition where this relay output is associated to
- Loop events

(*) The description of multistate is provided in chapter *8.1.2.*

To get information about a camera, please double click a relay output to open the **Camera Details** window:



The **Relay Details** window shows the following information about the relay output:

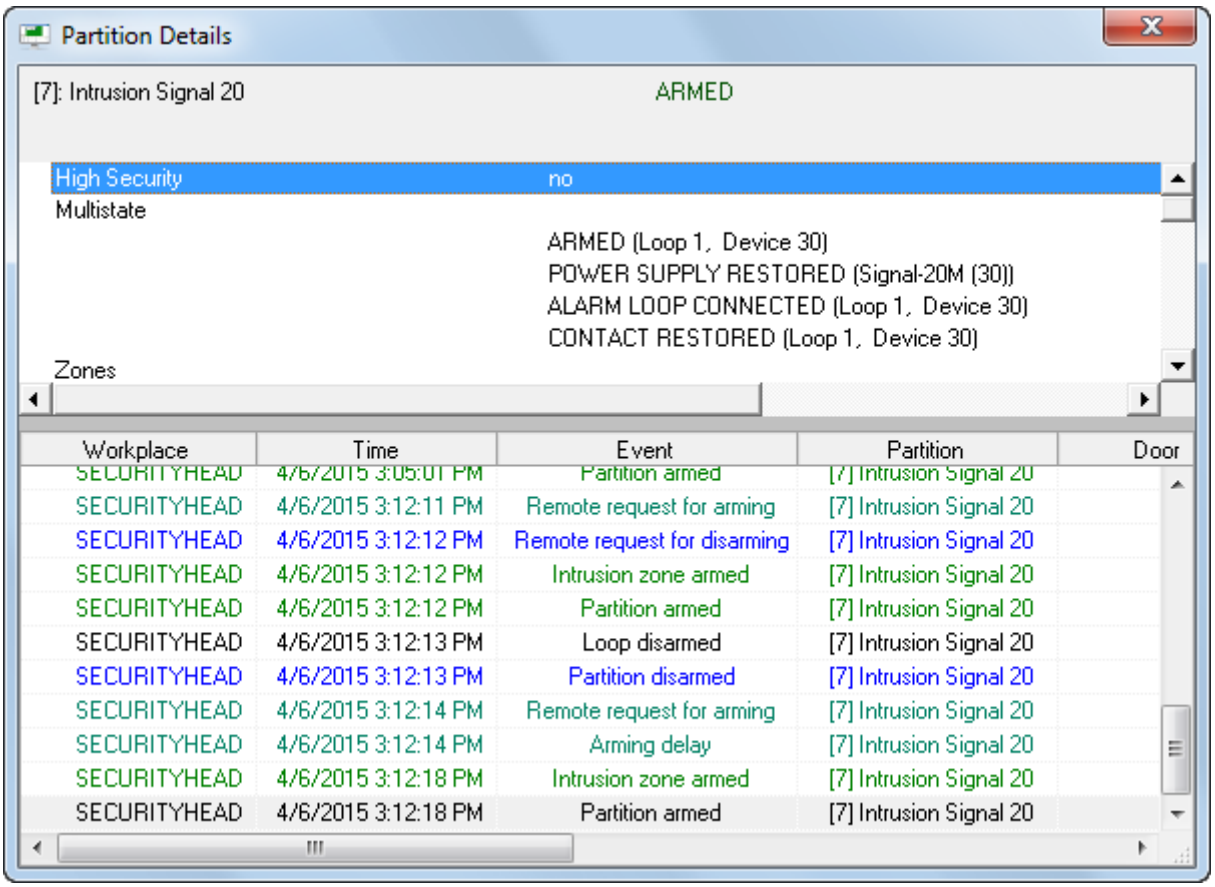
- The address and name of the camera as well as the number of a monitor
- The main status of camera
- Multistate of the camera (*)
- The name of a workstation where the camera is connected
- The number and name of a partition where this camera is associated to
- Name of a video system where this camera belongs
- The list of events related to this camera

(*) The description of multistate is provided in chapter *8.1.2.*

8.3.3.2.2 Obtaining Information about the Partition Entity

The Zone pane can provide the information about system partitions.

To get information about a partition, please double click a partition to open the **Partition Details** window:



The **Partition Details** window shows the following information about the partition:

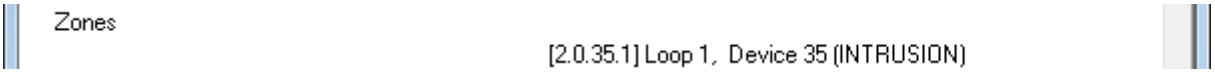
- The address and name of the partition r
- The partition main status
- Multistate of the partition (*)
- Loops associated to this partition(**)
- Relay outputs associated to this partition(***)
- Cameras associated to this partition(****)
- The list of events related to this partition

(*) The description of multistate is provided in chapter *8.1.2.*

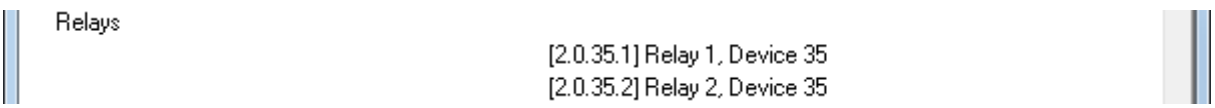
The multistate of a partition is the aggregate of states of all loops, relay outputs, and cameras included in this partition, as well as of states of devices where the partition-associated loops and relay outputs are connected
The multistate of a partition,

Please note, that if a partition has several entities with the same status, the multistate entry of the information window will show only one system entity for this status.

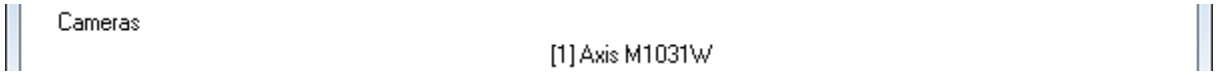
(**) the list of loops shows an address, name and type for each loop.



(***) The list of relay outputs shows an address and name for each relay output.



(****) The list of cameras shows the name and number for each camera.



8.3.3.2.3 Operating Loops and Cameras

8.3.3.2.3.1 Arming Zones

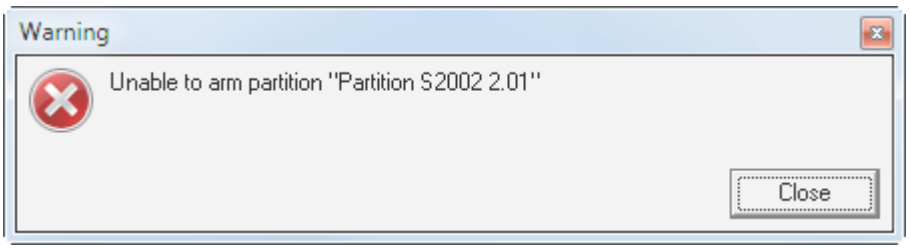
To arm loop or camera, please:

1. Select a loop or camera
2. Click the **Arm** button:

After clicking the **Arm** button, the following will occur:

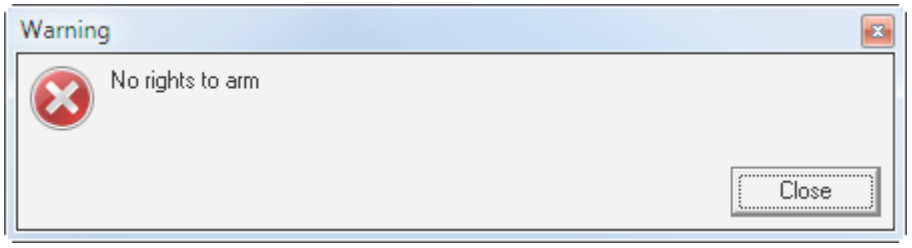
- If an operator has rights to operate a partition that includes this loop or camera, and the type of loop allows arming, the arming of the loop will be attempted:
    - The **Remote request for arming** event, loop (camera)'s number and name, as well as an operator's name will be added to the even log.
    - An command will be sent to a relevant device (video system) to arm the loop (camera)
    - When a request to arm is responded (received event on arming the loop (camera) or failed arming, the loop will go the Armed status.

- If an operator has rights to operate a partition that includes the loop but the type of this loop does not allow arming, no action will be attempted and the following message box will appear:



If an operator:

- has no rights to operate a partition that includes the loop (camera) but
- has rights only to disarm partition
- and has no rights to operate an individual zone, no action to arm the loop (camera) will be attempted and the following message window will be displayed:



8.3.3.2.3.2 Disarming Zones

To disarm a loop (camera) the following should be done:

1. Click a loop you want to disarm;
2. Click the **Disarm** button:

After clicking the Disa**rm** button, the following will occur:

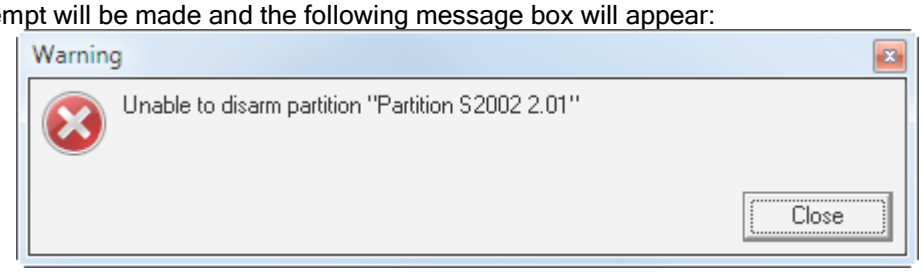
- If an operator has rights to operate a partition that includes the loop or camera, and the type of loop allows arming, it will attempt disarming a loop:

    - The **Remote request for disarming** event, loop (camera)'s number and name, as well as an operator's name will be added to the even log.

    - An command will be sent to a relevant device (video system) to disarm loop (camera)

    - When a disarming request is responded (event received on arming the loop (camera), the loop (camera) will go the **Disarmed** status

If an operator has rights to operate a partition that includes a loop, but the loop does not allow disarming, no attempt will be made and the following message box will appear:



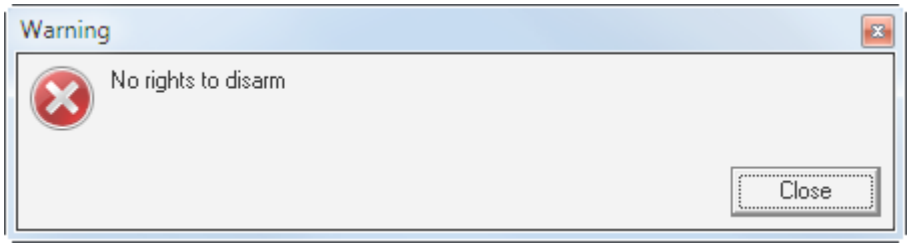
- If an operator:

    - has no rights to operate a partition where the loop (camera) is associated to

    - has rights only to disarm this partition and

    - has no rights to operate a High Security partition, but the partition with a required loop (camera) is defined as one of High Security,

    the loop will not be disarmed and the following message box will appear:



Please note that the requests to disarm are never sent to loops such as Auxiliary loop, Panic button loop, and 24-hour loop.

The *Appendix E Commands for Loops* describe possible commands for all types of loops.

8.3.3.2.4 Operating the Partition Entity

8.3.3.2.4.1 Arming a Partition

To arm a partition, please:

1. Click a partition name to select this partition

2. Click the **Arm** button:

After clicking the **Arm** button, the following will be done for each partition:

- If an operator has rights to operate a partition, arming a partition will be attempted:

    - The **Remote request for arming** event, partition's number and name, and operator's name will be added to the even log.

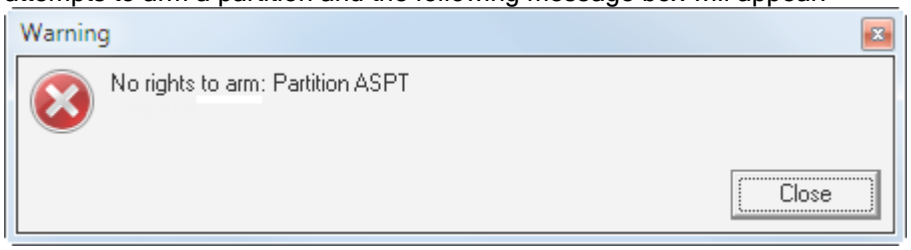
    - A command will be sent to a relevant device (camera) to arm each loop (camera) of the partition, if that loop type allows arming

    - When all arming requests are responded (received events on arming loops (cameras) or failed arming, the partition status will be finalized.

    Thus, the partition will go to the **Armed** status only when all loops (cameras) of relevant types will be armed. In this case, the **Partition Armed** event will be generated.

- If an operator:

    has no full rights to operate a partition but has rights only to disarm a partition, there will be no attempts to arm a partition and the following message box will appear:

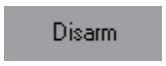


8.3.3.2.4.2 Disarming a partition

To disarm a partition, please follow the instructions:

1. Select a partition by a left mouse click

2. Click the **Disarm** button:



After clicking the **Disarm** button, the following will be done for each partition:

- If an operator has rights to operate a partition, the partition will be disarmed:

    - The **Remote request for disarming** event, partition's number and name, and operator's name will be added to the even log.

    - Instruction will be sent to a relevant device (camera) to disarm each loop (camera) of the partition, if a loop type allows disarming

    When all disarming requests are responded (received events on disarming loops (cameras), the partition will go to the **Disarmed** status and **Partition Disarmed** event will be generated.

If a partition was in the **Armed** status, the **Partition Disarmed** event would be generated immediately after a first loop (camera) of the partition is disarmed.

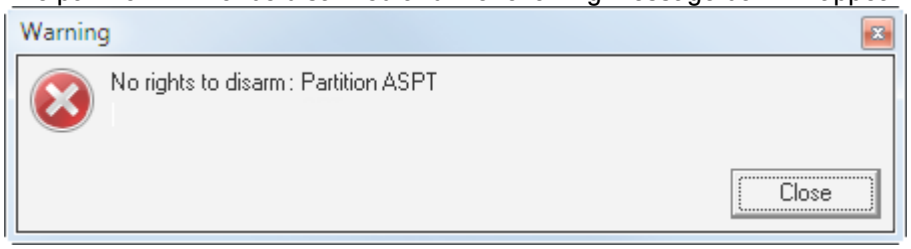
- If an operator:

    - has no rights to operate a partition but

    - has rights only to arm a partition and

    - has no rights to operate a High Security partition, but the partition is defined as one of High Security,

the partition will not be disarmed and the following message box will appear



Please note that when an operator deals with a partition, requests to disarm are never sent to loops such as Auxiliary loop, Panic button loop, and 24-hour loop.

Therefore, if a partition includes only Panic alarm zones and/or 24-hour zones, this partition will not be disarmed.

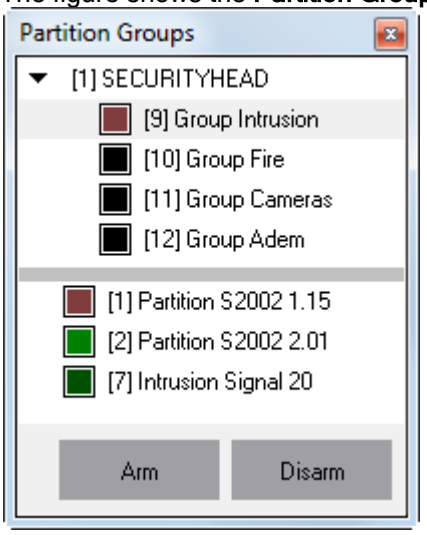
The Appendix E Commands for Loop describes possible commands for all types of loops.

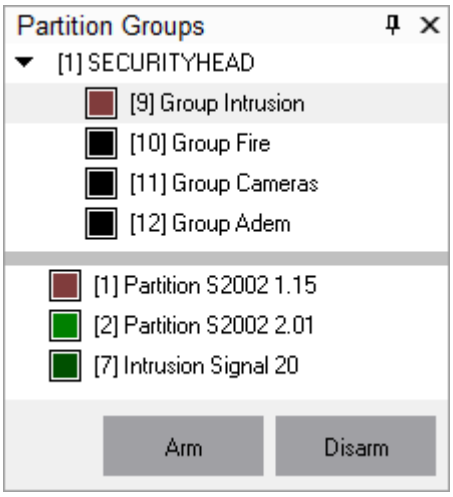
8.3.3.3 The Partition Group Pane

The Partition Group provides access to the following functions:

- Arming and disarming partitions, and partition groups
- Obtaining info about partition, partition groups and their status

The figure shows the **Partition Group** pane:



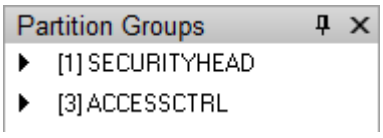


The figure shows the following elements of the pane:

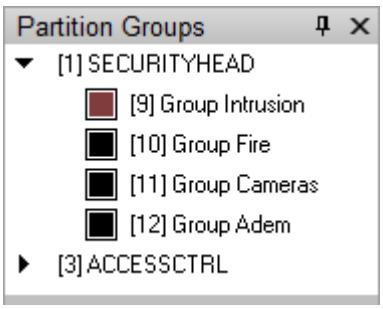
1. The list of partition groups,
2. Partitions included in a selected partition group
3. The **Arm** and **Disarm** button to arm and disarm partition groups.

The upper part of the pane includes workstations in the following order:

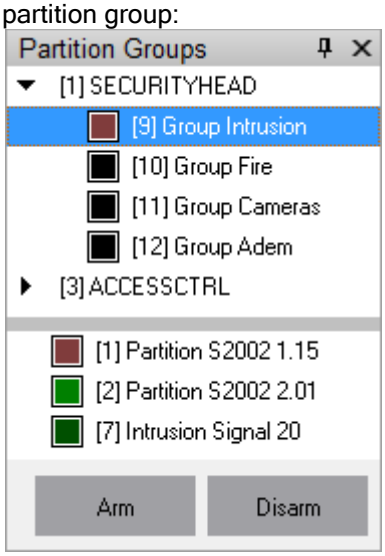
- The first one is a workstation where the System Monitor is running.
- Then other system workstations in the ascending order by their ID in the database..



Each workstation entry displays their assigned partition groups:

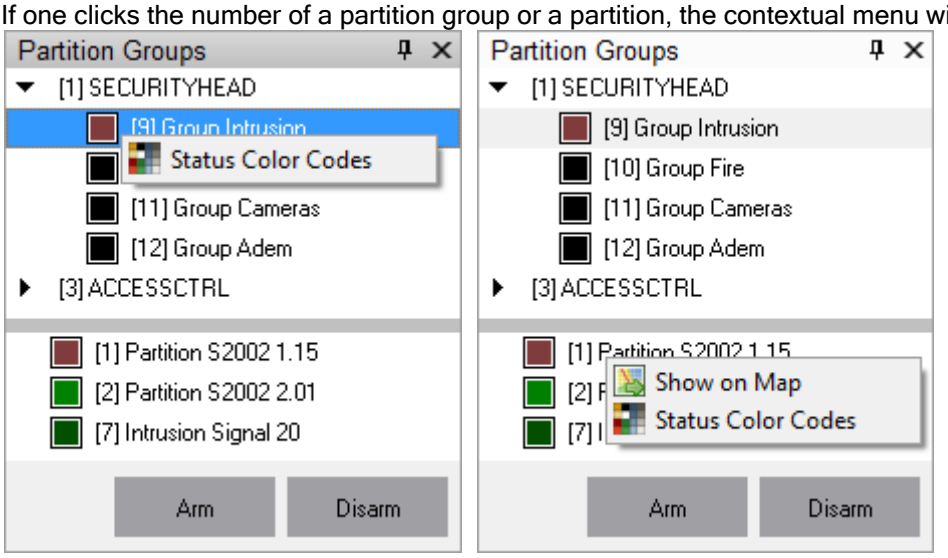


When any partition group is selected in the upper part, the lower part will display partitions included in this partition group:



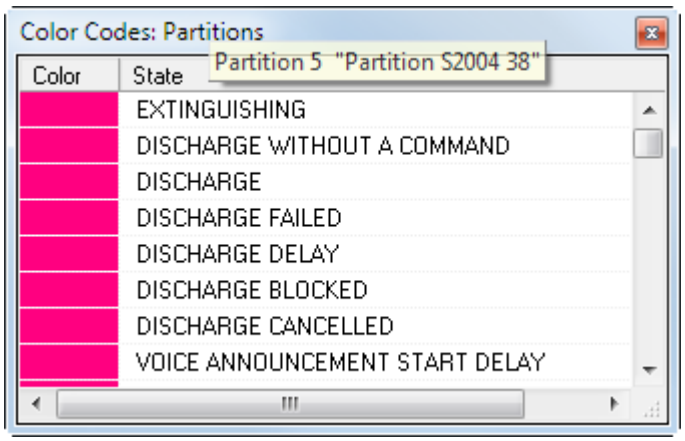
Each partition and partition group are highlighted in accordance with the status of that partition or partition group. *The color codes for partition states are provided in the Appendix 8 C.*

If one clicks the number of a partition group or a partition, the contextual menu will be displayed:



If you select the **Show on Map** item, it will toggles a map with this partition and flashes one time with another color (for finding it quickly on a map)

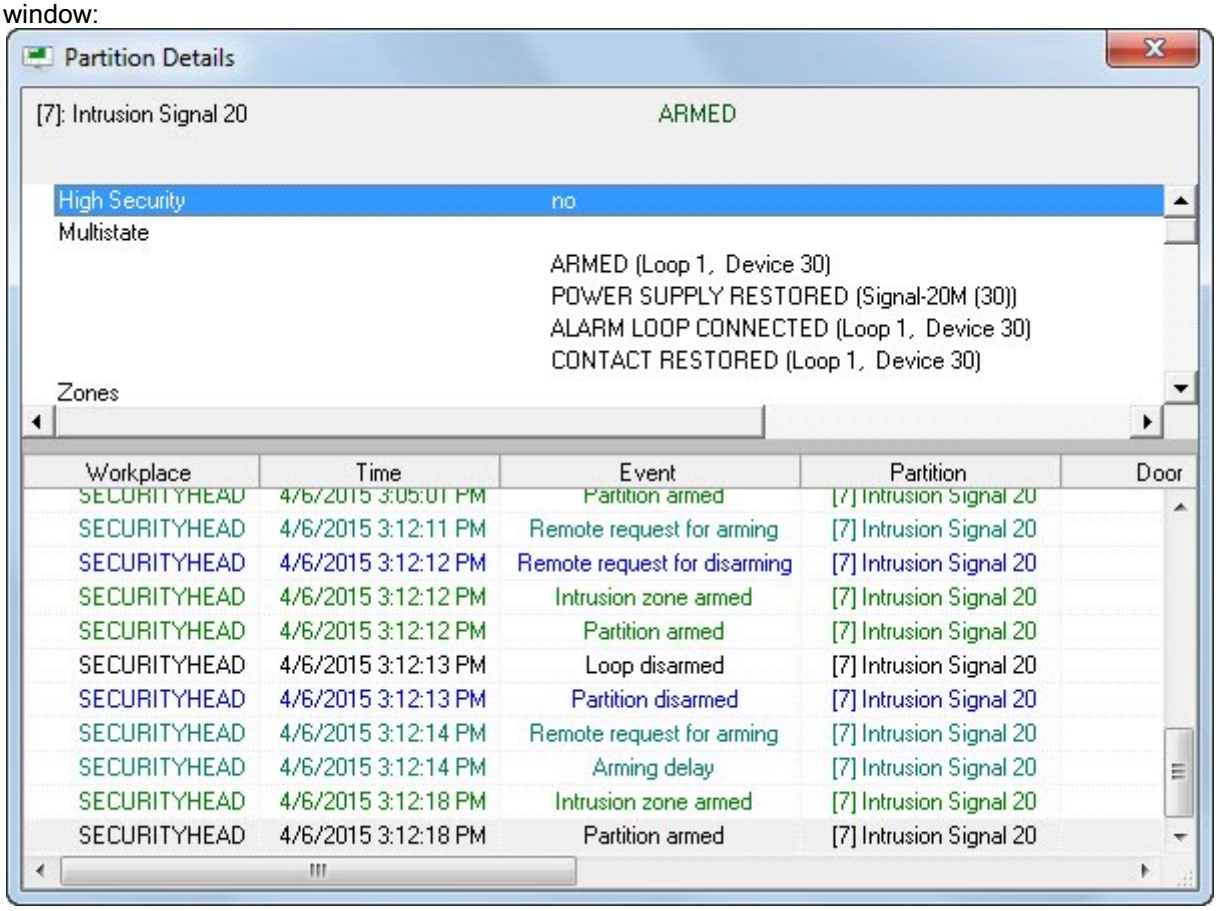
If you select, **Status Color Codes** item, the **Color Codes: Partitions** window will be displayed. It will include color codes for each entity status:



8.3.3.3.1 Obtaining Information about the Partition Entity

The Partition pane can be used to obtain information about system partitions.

To get information about a partition, please double click the name of a loop to open the **Partition Details** window:



The **Partition Details** window shows the following information about the partition:

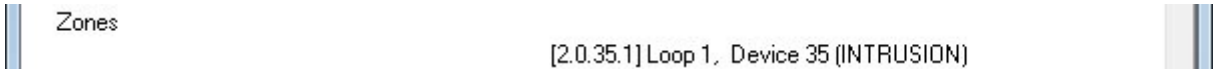
- The address and name of the partition
- The main status of the partition
- Where the partition is a High Security one
- Multistate of the partition (*)
- Loops associated to this partition(**)
- Relay outputs associated to this partition(***)
- Cameras associated to this partition(****)
- The list of events related to this partition

(*) The description of multistate is provided in chapter *8.1.2.*

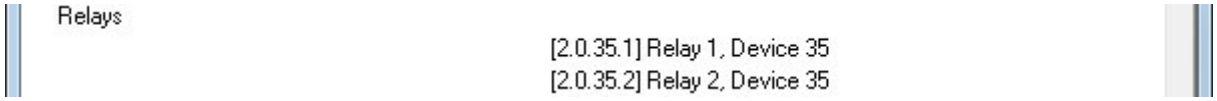
The multistate of a partition is the aggregate of states of all loops, relay outputs, and cameras included in this partition, as well as of states of devices where the partition-associated loops and relay outputs are connected

Please note, that if a partition has several entities with the same status, the multistate entry of the information window will show only one system entity for this status.

(**) The list of loops shows an address, name and type for each loop.



(***) The list of relay outputs shows an address and name for each relay output.

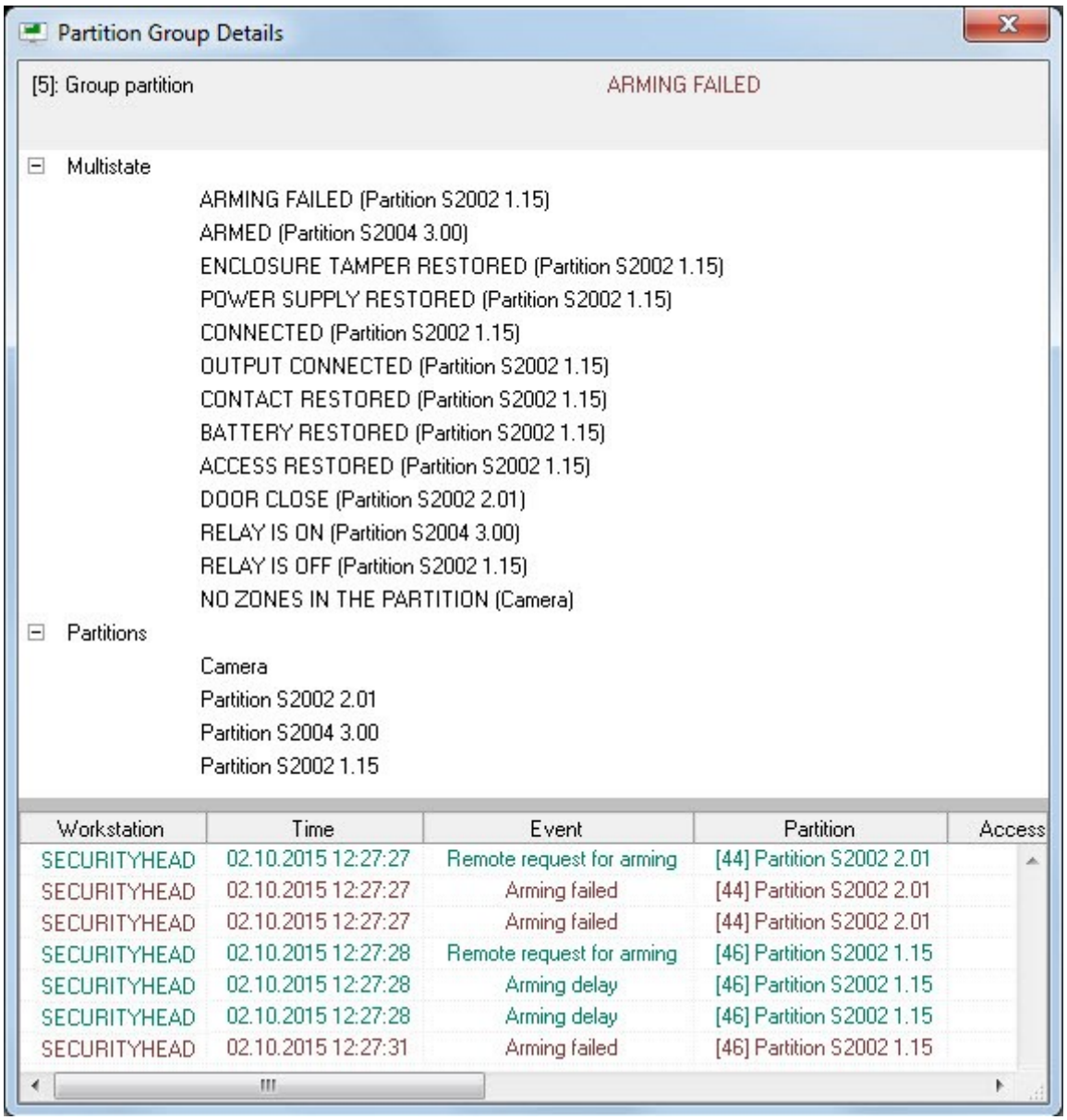


(****) The list of cameras shows the name and number for each camera.

8.3.3.3.2 Obtaining Information about the Partition Group Entity

The Partition Group pane can be used to obtain information about partition groups.

To get information about a partition, please double click the name of a desired group to open the **Partition Group Details** window:



The **Partition Group Details** window shows the following information about the partition:

- The address and name of the partition group
- The partition group main status
- The multistate of the partition group (*)
- Partitions included into to this partition group (**)
- The list of events related to this partition group and partitions included into this group

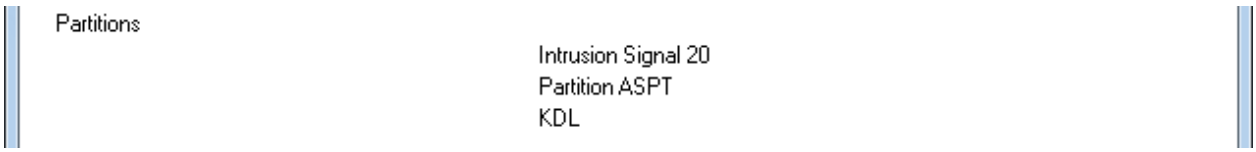
(*) The description of multistate is provided in chapter *8.1.2.*

The multistate of a partition group is the aggregate of the states of the partitions included into this partition group.

The information window shows each status with the name of partition that has this status.

Please note, that if a partition group has several partitions with the same status, the multistate entry of the information window will show only one partition that has such a status.

(**) The status is shown for each partition in the list of partitions.



8.3.3.3.3 Operating a Partition

8.3.3.3.3.1 Arming a Partition

To arm a partition, please:

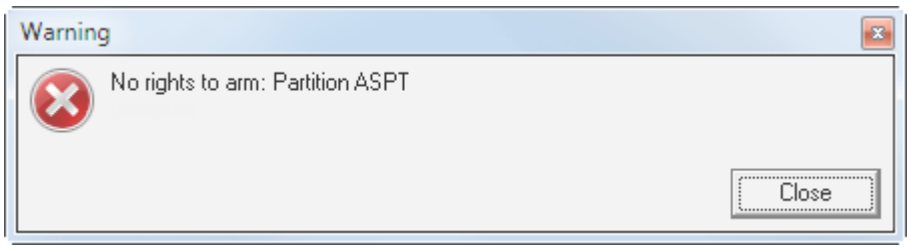
1. Click a partition name to select this partition
2. Click the **Arm** button:

After clicking the **Arm** button, the following will be done for each partition:

- If an operator has rights to operate a partition, arming a partition will be attempted:
    - The **Remote request for arming** event, partition's number and name, and operator's name will be added to the even log.
    - An command will be sent to a relevant device (camera) to arm each loop (camera) of the partition, if the type of loop allows arming
    - When all arming requests are responded (received events on arming loops (cameras) or failed arming, the partition status will be finalized.

  Thus, the partition will go to the **Armed** status only when all loops (cameras) of relevant types will be armed. In this case, the **Partition Armed** event will be generated.
- If an operator:

Has no rights to operate a partition but has rights only to disarm a partition, there will be no attempts to arm a partition and the following message box will appear:



8.3.3.3.3.2 Disarming a Partition

To disarm a partition, please follow the instructions:

1. Select a partition by a left mouse click
2. Click the **Disarm** button:

After clicking the **Disarm** button, the following will be done for each partition:

- If an operator has rights to operate a partition, the partition will be disarmed:
    - The **Remote request for disarming** event, partition's number and name, and operator's name will be added to the even log.

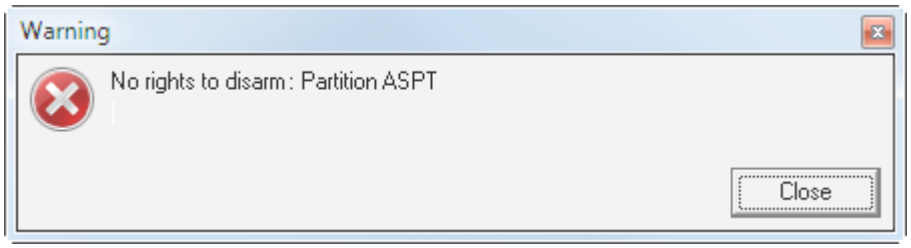
- Instruction will be sent to a relevant device (camera) to disarm each loop (camera) of the partition, if a loop type allows disarming

When all disarming requests are responded (received events on disarming loops (cameras), the partition will go to the **Disarmed** status and **Partition Disarmed** event will be generated.

If a partition was in the **Armed** status, the **Partition Disarmed** event would be generated immediately after a first loop (camera) of the partition is disarmed.

- If an operator:
  - has no rights to operate a partition but
  - has rights only to arm a partition and
  - has no rights to operate a High Security partition, but the partition is defined as one of High Security,

the partition will not be disarmed and the following message box will appear:



Please note that when an operator deals with a partition, requests to disarm are never sent to loops such as Auxiliary loop, Panic button loop, and 24-hour loop.

Therefore, if a partition includes only Panic alarm zones and/or 24-hour zones, this partition will not be disarmed.

The Appendix E Commands for Loop describes possible commands for all types of loops.

8.3.3.3.4 Operating a Partition Group

8.3.3.3.4.1 Arming a Partition Group

To arm a partition group, please:

1. Click a partition group
2. Click the **Arm** button:

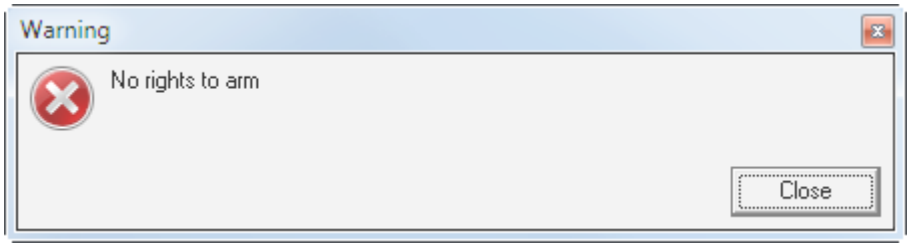
After clicking the **Arm** button, the following will be done:

- If an operator has rights to operate a partition group, the partition group will be armed:
  - The **Remote request for arming** event, partition group's number and name, and operator's name will be added to the even log.
  - A command will be sent to a relevant device (camera) to arm each partition of the partition group, and each loop (camera) of the partition, if that loop type allows arming
  - When all arming requests are responded (received events on arming loops (cameras) or failed arming, the partition group status will be finalized.

Thus, the partition group will go to the **Armed** status only when all loops (cameras) of relevant types will be armed. In this case, the Partition Armed event will be generated.

- If an operator has no rights to arm any partition of a partition group, any attempt to arm a partition group will fail

- If an operator has no rights to operate a partition but has rights only to disarm a partition, there will be no attempts to arm a partition and the following message box will appear:



8.3.3.3.4.2 Disarming a Partition Group

To disarm a partition group, please follow the instructions:

3. Select a partition by a left mouse click

4. Click the **Disarm** button:

After clicking the **Disarm** button:

- If an operator has rights to operate a partition group, the partition will be disarmed:

  - The **Remote request for disarming** event, partition group's number and name, and operator's name will be added to the even log.

  - A command will be sent to a relevant device (camera) to disarm each loop (camera) of the partition included in the partition group , if a type of such loop support disarming

  When all disarming requests are acknowledged (received events on disarming loops or/and cameras), the status of each partition will be formed, and then the status of this partition group will be formed.

  Therefore, this partition will go to the **Disarmed** status and the **Partition Group Disarmed** event will be generated.

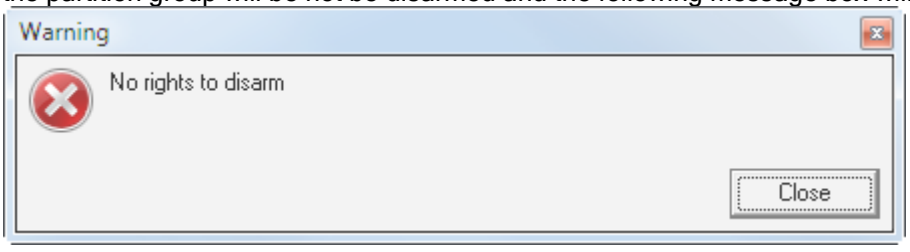
- If an operator:
  - has no rights to disarm a specific partition of a partition group
  - has no rights to operate a High Security partition, but the partition group includes a High Security partition

  this partition of the partition group will not be disarmed

  If a partition group includes a partition that has Panic alarm zones and 24-hour zones, such zones will not be disarmed.

- If an operator:
  - has no rights to operate a partition but
  - has rights only to arm a partition,

  the partition group will be not be disarmed and the following message box will appear:



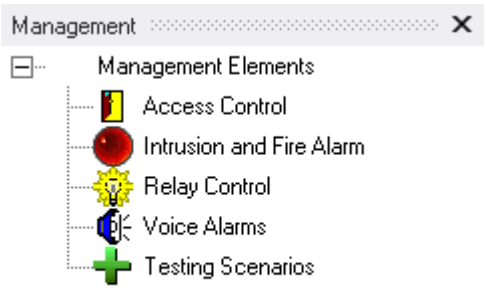
Appendix 8 *E Commands for Loops* describes commands for all types of loops.

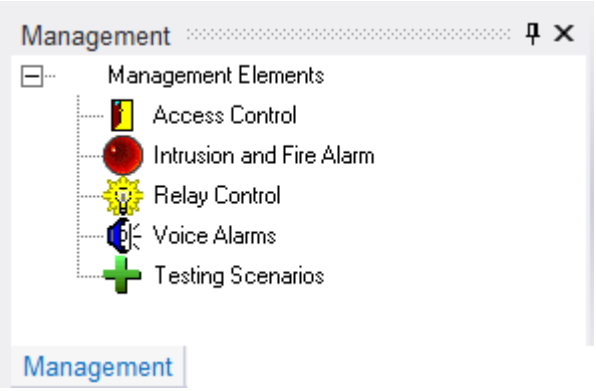
8.3.3.4 The Management Pane

The Management tab ensures the following functions:

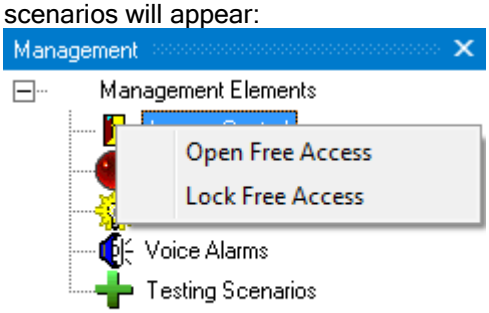
- Launch of management scenarios with using the management tree.

The appearance of the Management pane:





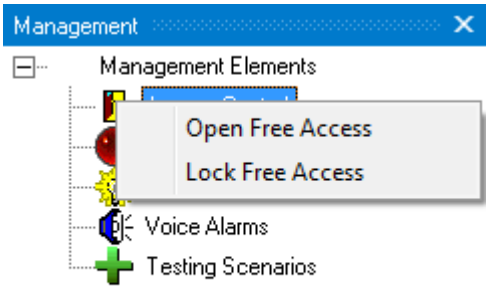
To view available scenarios for a tree element, please right click this node. The menu with available scenarios will appear:



8.3.3.4.1 Launching Scenarios Using the Management Tree

To launch one of the management scenarios at any of the management tree nodes, follow the instructions:

- Right click a node
- Chose a required scenario in the appeared menu



In this case, the management scenario will be executed, and **Management Scenario Launch** event and the operator name will be added to the event log.

8.3.3.4.2 Launching Scenarios by a Hot Key

Scenarios with an assigned hot key can be launched by using the specified keys.

This action can be performed, when the System Monitor window is active and no info box contextual menu is open.

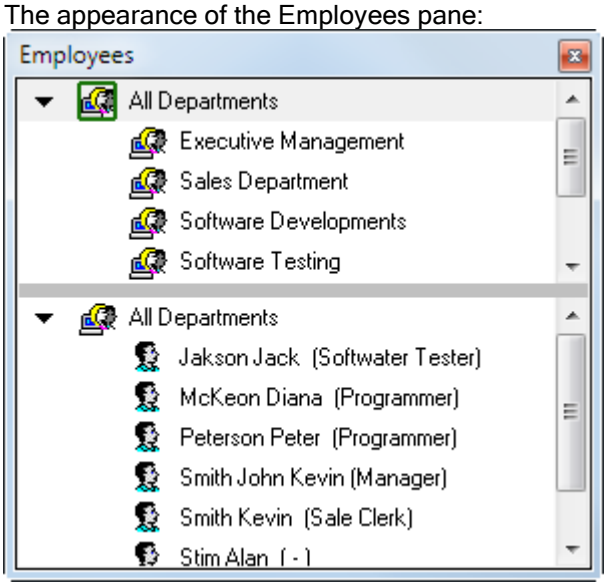
If an operator launches a management scenario by a hot key, the **Management Scenario Launched** event, and the current operator's name will be added to the Event Log.

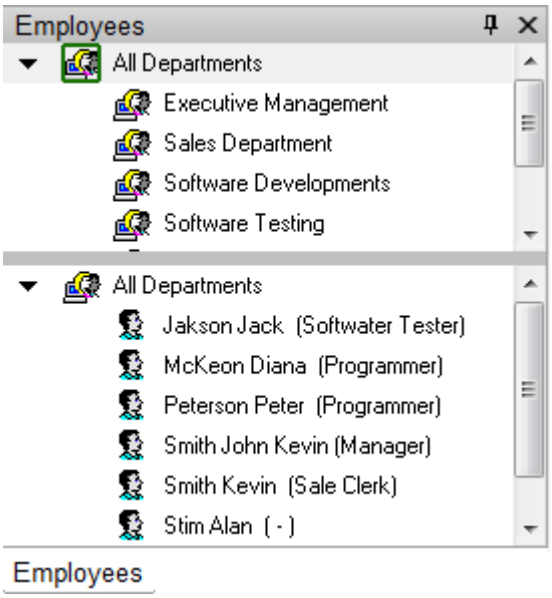
8.3.3.5 The Employees Pane

The Employees pane provided the following functionality:

- Obtaining information about department personnel
- Obtaining information of individual employees
- Granting access to employees

The appearance of the Employees pane:



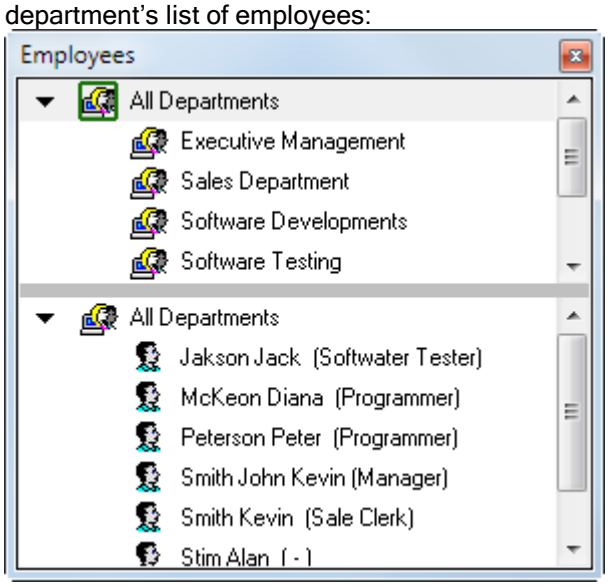


The figure of pane shows:

1. The list of departments

2. The list of employees of a selected department

If one clicks a specific department in the upper part of the pane, the lower part of the pane will display this department's list of employees:

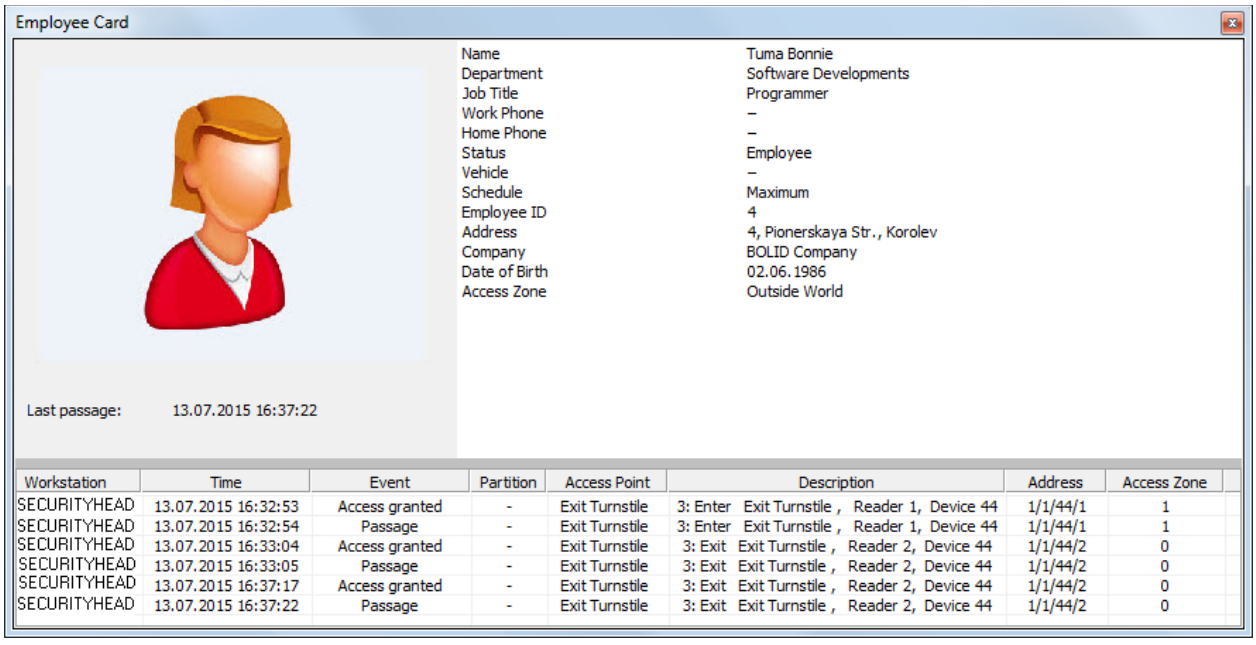


The list displays the following for each employee:

- Name
- Job Title

8.3.3.5.1 Obtaining Information about the Employee Entity

To get information about an employee, please double click his/her name in the personnel list of a selected department. The Employee Card info window will appear providing information about this employee:



The **Employee Card** window provides the following information:

- Photo
- Last passage (transaction)
- Employee's Name
- Department
- Job Title
- Work Home

- Home Phone
- Status
- Vehicle
- Working Schedule
- Employee ID
- Address
- Company
- Date of Birth
- Access Zone the employee attends at the moment
- The list of events.

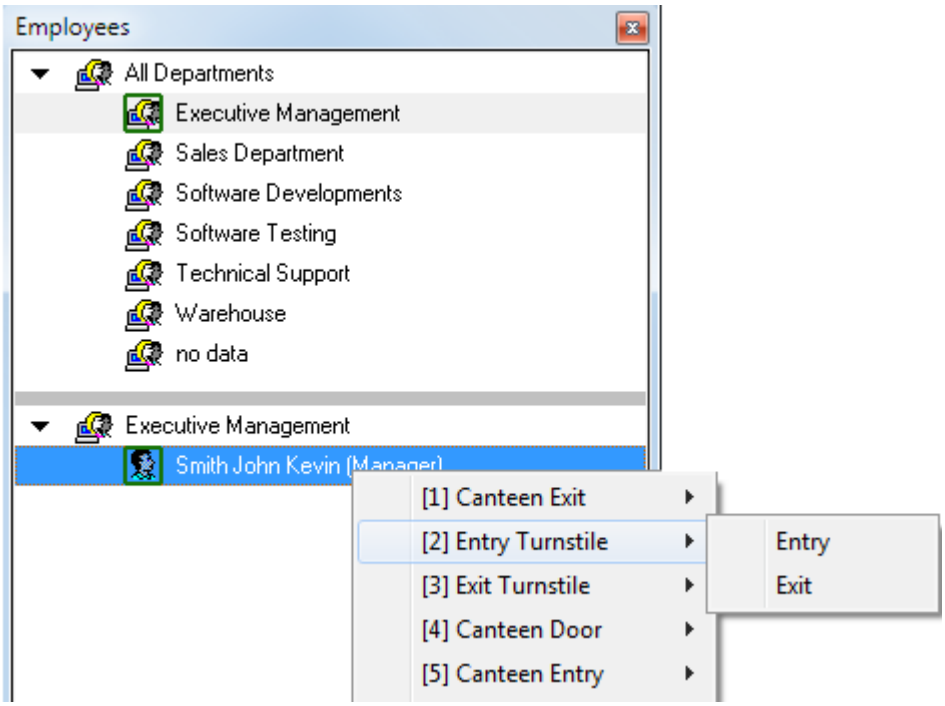
8.3.3.5.2 Granting an Access Permit

Some time, there may me needs for granting **an access permit.**

For example, an access permit can be granted, if an employee does not carry an access badge (token), but he/she can confirm his/her identity by a recognized identity document (passport, driver's license and some other photo ID). In this case, in addition to granting access to the employee t, the time and attendance as well as antipassback options will be activated.

To grant an employee an access permit, please do the following:

- Right click an employee's name in the list of employees of a selected department:
- Select an access point in the appeared menu
- Click a required access direction (Entry or Exit)



In this case:

- The **Open Door (Entry) command** , **Open Door (Exit) command** or **Open Door (Passage) command** event with the current SM Operator's name will be added to the event log,
- A command to grant the employee access will be initiated. The Access Granted and Passage commands will be generated with the name of an employee who gained access (important for Time and Attendance, and antipassback rules).
    1. After receiving the **Passage** event the employee will be assigned to the relevant access zone and antipassback rules will be applied to him.

Note that the possibility to give a command for granting access depends on the operator's rights.

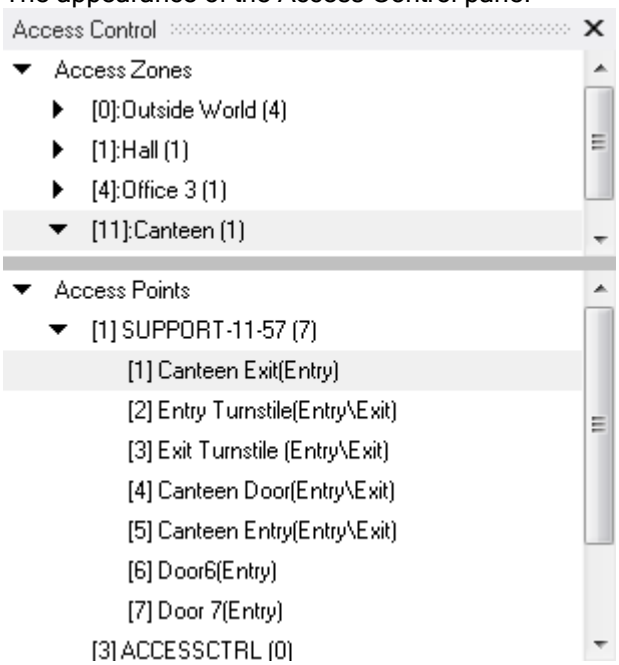
If an operator has rights to control an access point in the relevant direction then he/she will be able to give commands to grant access for this direction (i.e. the menu item for controlling an access point in this direction will be available for this operator). Otherwise, it will be impossible.

8.3.3.6 The Access Control Pane

The functions available on the pane are as follows:

- Obtaining information such as whom and how many of employees attending each access zone.
- Obtaining details of employees and access points.
- Granting access via access points

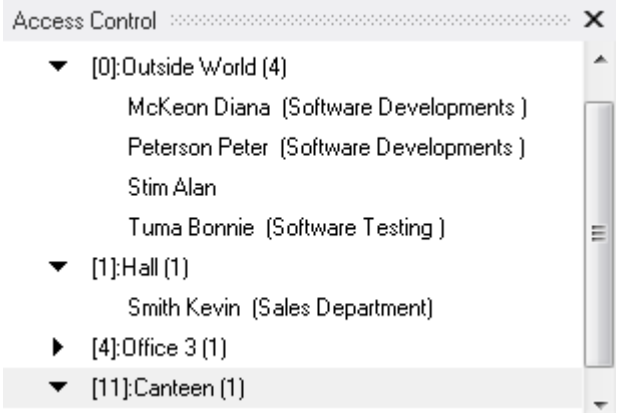
The appearance of the Access Control pane:



The pane of the figure shows the following:

1. The list of access zones with specified number of employees in each
2. The list of employees in each access zone at the moment
3. The list of access points for each workstation with specified operating mode

The upper part of the pane displays the list of access zones. The number of employees are indicated for each access zone. Each access zone has a collapsible list of employees attending this access zone at the moment. An employee line also includes a department of this employee.

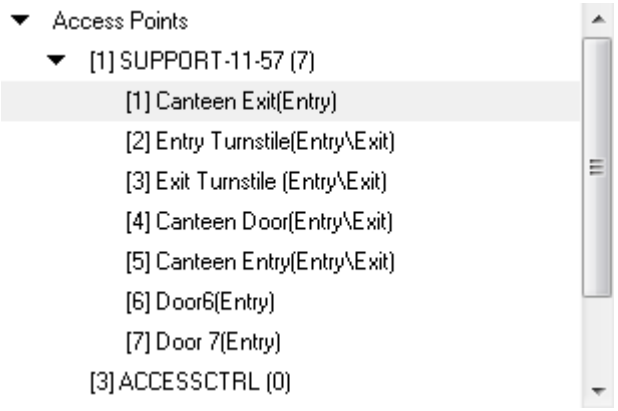


The list of employees in each zone is monitored in real time. In other words, when the event on a certain employee entering an access zone is received, the employee will be immediately reassigned to this access zone.

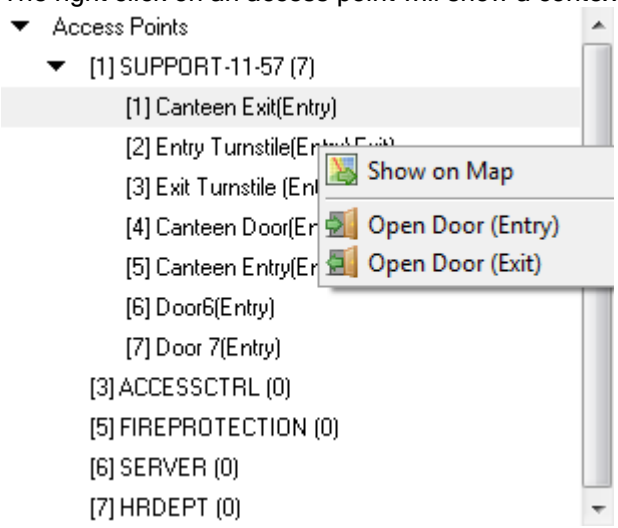
The bottom part includes the list of access zones for each workstation with their operating mode specified

The workstations are displayed in the following order:

- The first workstation is one where the System Monitor is running
- Then other workstation in ascending order by their ID in the database



The right click on an access point will show a contextual menu:

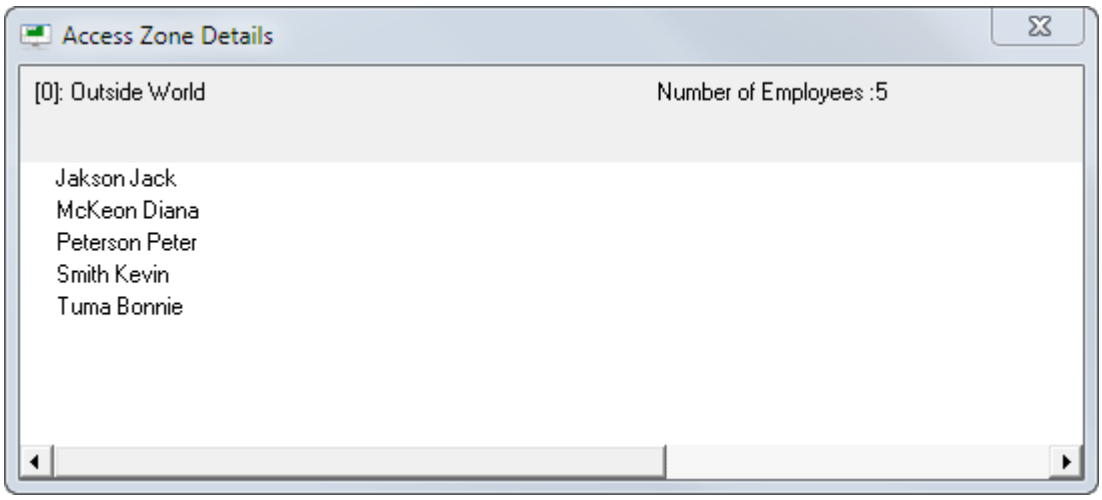


If one selects **Show on Map** item, it will toggle the map that includes this access point that will flash immediately once with different color to make it found easily on the map.

Also, the contextual menu includes action items to grant access via a relevant access point.
(*See chapter 8.3.3.6.4 Granting Access*)

8.3.3.6.1 Obtaining Access Zone Information

To get access zone details, please double click a required access zone. The Access Zone Details window will appear:

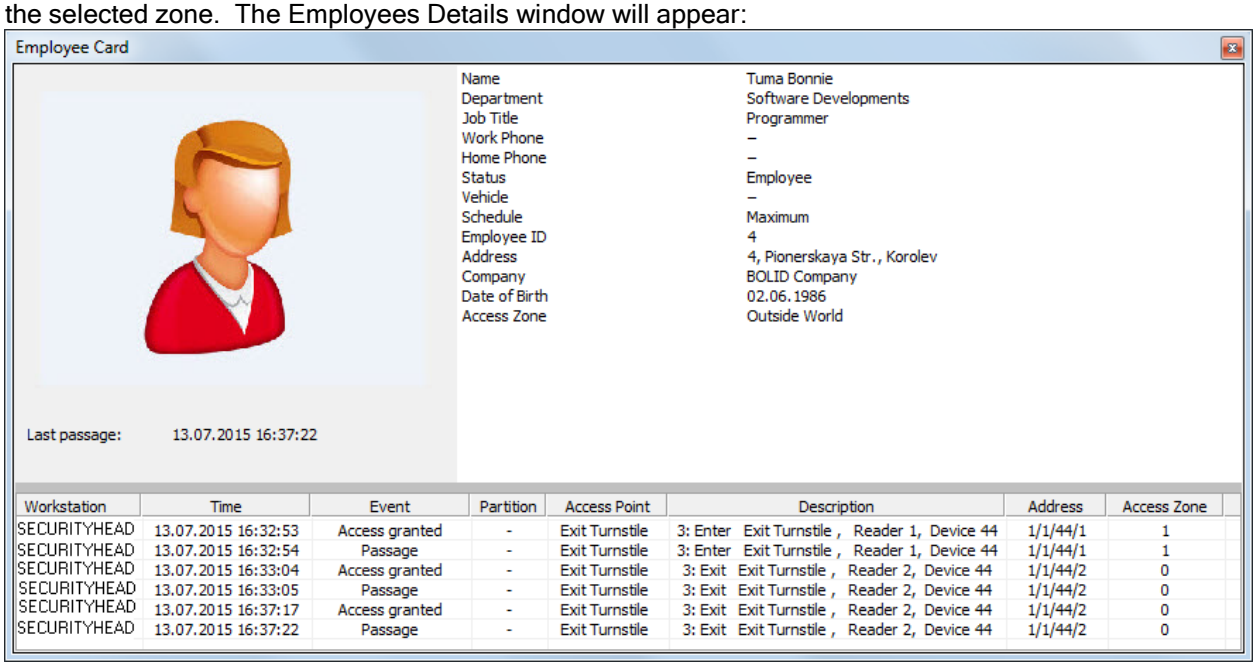


The Access Zone shoes the following information:

- Number (ID) and the name of the access zone,
- Number of employees in the access zone,
- List of employees attending the access zone

8.3.3.6.2 Obtaining Information about Employee

To get information employee details, please double click an employee's name in the list of employees in the selected zone. The Employees Details window will appear:

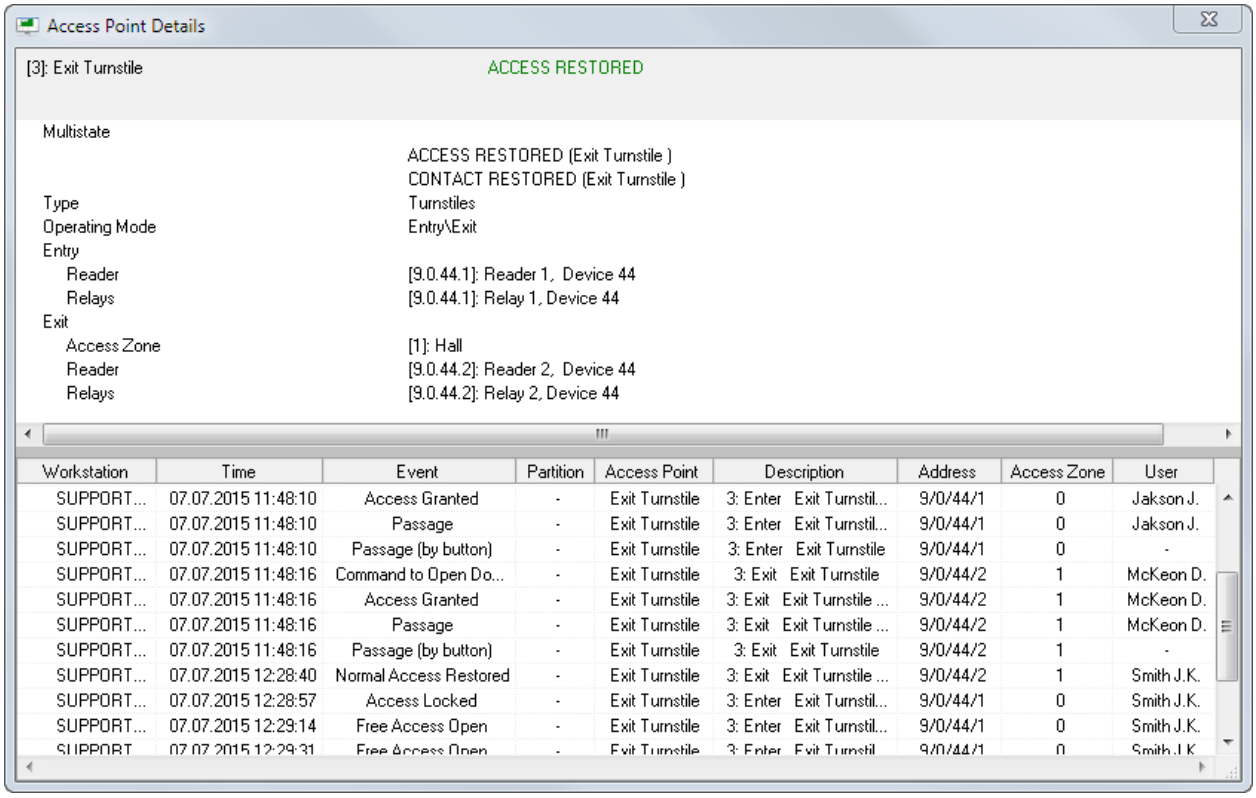


The Employee Details contains the following information for an employee:

- Phot
- Last passage (transaction)
- Name
- Department
- Job Tittle
- Work Phone
- Home
- System Status
- Vehicle Details
- Working schedule
- Employee ID
- Address
- Company
- Date of Birth
- Access zone occupied by the employee at the moment
- The list of events

8.3.3.6.3 Obtaining Information about the Access Point Entity

To get information on an access point, please double click a required access point in the pan. The **Access Point Details** window will appear:



The **Access Point Details** contains the following information:

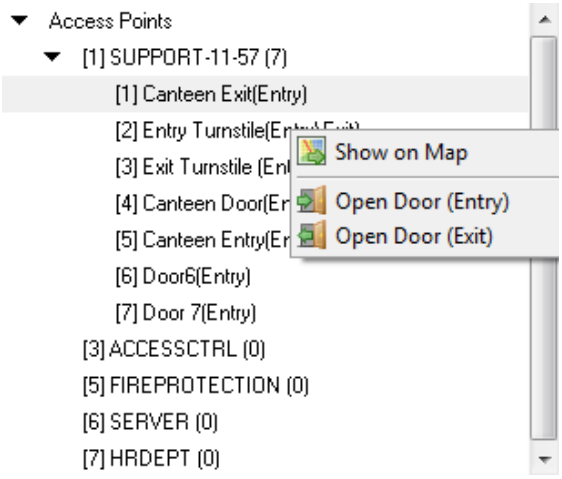
- The number and name of an access point:
- The status of an access point
- The multistate of an access point (*)
- Type of access point
- The operating mode of an access point
- Information for each direction (entry, exit) includes the following:
    - The number and name of an access zone (if used) where an access is provided in accordance with the defined access direction
    - The address and name of a reader providing access in this direction
    - The name and address of relay output controlling access in the direction
- The list of events related to this access points

(*) The description of multistate is provided in *Chapter 8.1.2.*

8.3.3.6.4 Granting Access

An SM operator can grant access via a certain access point:
To do so, please:

- Chose a required access point
- Right click it to open the contextual menu
- In the menu, please select an access direction that will be provided by the selected access point:



In this case:

- The **Open door (Entry) command** or **Open door (Exit) command,** or **Open door (Passage) command** event with the current SM Operator's name will be added to the event log,
- A command to grant access will be sent to a device. The **Access Granted** and **Passage** events will be generated with the current SM Operator's name.

Note that the possibility to initiate a command for granting access depends on the operator's rights.

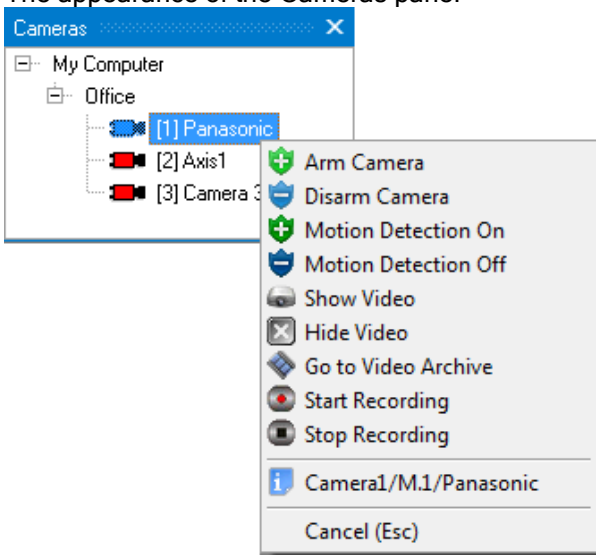
If the operator has rights to control the access point in a relevant direction the operator will be able to give commands to grant access for this direction (i.e. the menu item for controlling an access point in this direction will be available for this operator). Otherwise, it will be impossible.

8.3.3.7 The Cameras Pane

The following functions are available on the Cameras pane:

- Obtaining information about cameras and their states
- Controlling Cameras

The appearance of the Cameras pane:



The figure shows that the Cameras pane includes the list of cameras for each workstation.

Workstations are arranged in the following manner:

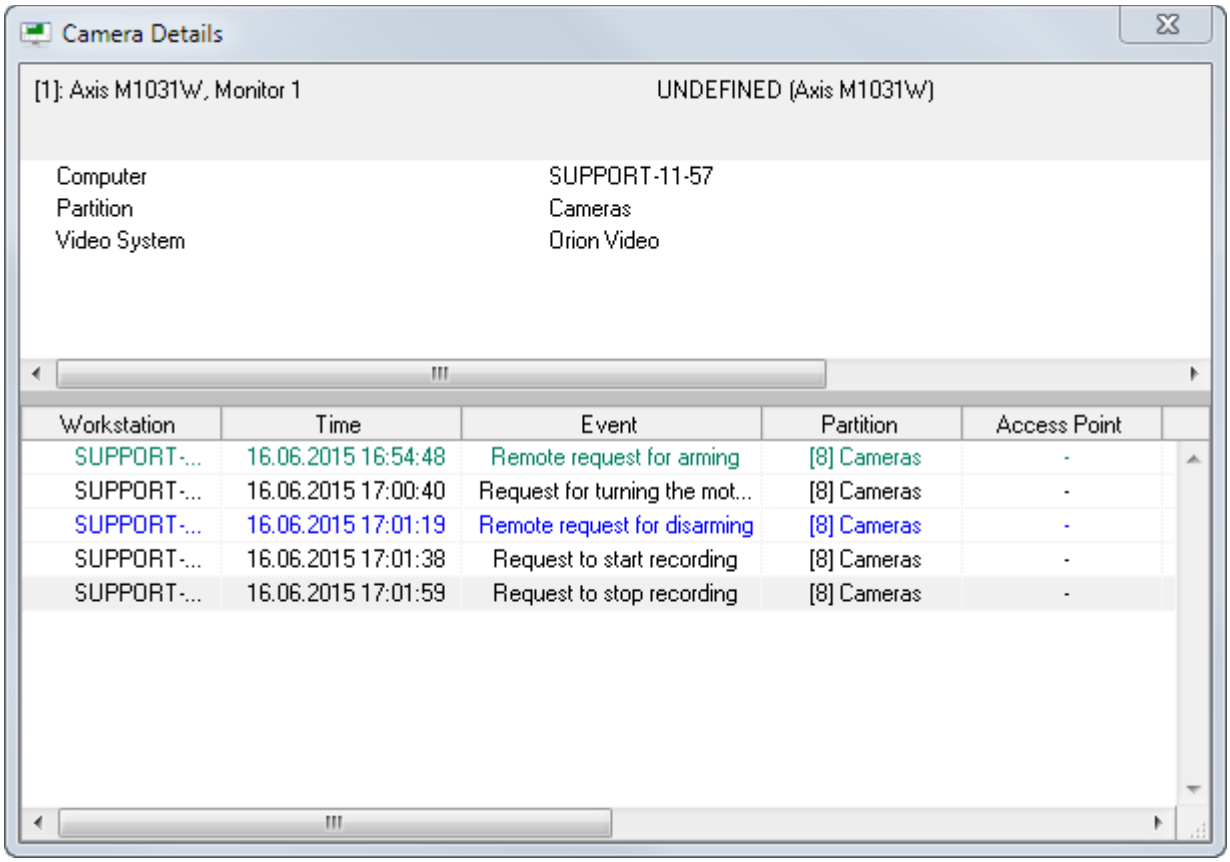
- The first workstation is that where the System Monitor is running
- Then other workstations follow in the ascending order by their IDs as per the database

Each camera icon has the color in accordance with its current status.

If one choses and right clicks a required camera, the map with this camera will be toggled and the camera icon will changed its color for a moment to help an operator to find it quickly on the map. At the same time, camera control menu will be displayed

8.3.3.7.1 Obtaining Information about the Camera Entity

To get information about a camera, please double click a required camera's name. The **Camera Details** window will appear:



The **Camera Details** window shows the following information:

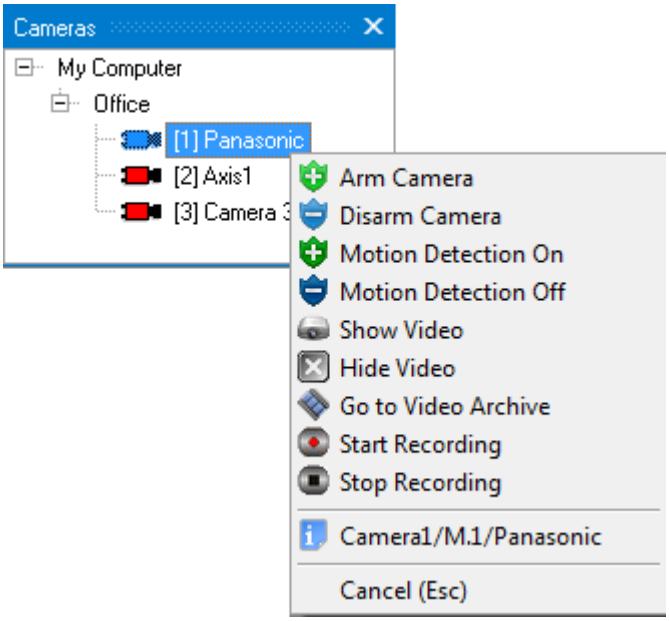
- The number and name of a camera, as well as the number of Monitor
- The main status of a camera (*)
- The name of a workstation where a camera is assigned to
- The name of video system where a camera belongs
- The list of cameras

8.3.3.7.2 Controlling a Camera

To control camera, please:

- Select a required camera
- Right click it, and

- Select a required action in the appeared menu



Please note that the accessibility of menu items depends on an operator's rights:

a. If the **Management of Individual Zone** property of an operator's password is set **Off** , the control of camera is not allowed

b. If the **Management of Individual Zones** property is set **Off**, then:

   i. If an operator has the right to arm a camera-included partition, the following action will be allowed:
      1. To arm a camera (**Arm Camera**)
      2. To turn on video motion detection (**Motion Detection ON**)
      3. To start recording (**Start Recording**)

   ii. If an operator has the right to disarm a camera-included partition, the following actions will be allowed:
      1. To disarm a camera (**Disarm Camera**)
      2. To turn off the video motion detection (**Motion Detection OFF**)
      3. To stop recording (**Stop Recording**)

   iii. If an operator has any rights (either arming or disarming rights), the following actions are allowed:
      1. To **Show Video**
      2. To **Hide Video**

   iv. If a camera-included partition is a High-Security one, the **Management of High Security Partitions** (Control High Security Partitions) option is set as '**Off'**, the following actions are not allowed:
      1. To disarm camera (**Disarm**)
      2. To turn off video motion detection (**Motion Detection OFF**)
      3. To stop recording (**Stop Recording**)

8.3.3.7.2.1 Arming Camera

To arm a camera, please follow the instructions:

1. Right click a required camera
2. Select the **Arm Camera** in the appeared menu.

In this case:

- The **Remote Request for Arming** event and an SM current operator's name will be added to the Event Log

- If the camera is in a normal mode (do not respond to motion), the camera will be armed (the **Armed** event and an operator's name will be added to the Event Log)

8.3.3.7.2.2 Disarming a Camera

To disarm a camera, please follow the instructions:
1. Right click a required camera
2. Select the **Disarm Camera** action in the appeared menu.

In this case:
- The **Remote Request for Disarming** event and a current SM Operator's name will be added to the Event Log
- The camera will be disarmed (the **Disarmed** event and an operator's name will be added to the Event Log)

8.3.3.7.2.3 Arming/Disarming a Video System (Group of Cameras)

To arm a video system, please:
1. Right click a required video system in the list;
2. Select the **Arm** item in the appeared contextual menu.

To disarm a video system, please:
1. Right click a required video system in the list;
2. Select the **Disarm** item in the appeared contextual menu.

In this case:
- The **Remote Request for Arming** or **Remote Request for Disarming** event (as per selection) and an SM current operator's name will be added to the Event Log

- The camera will be armed or disarmed in accordance with a selected action. The **Armed** or **Disarmed** event and an operator's name will be added to the Event Log. Such an event will be displayed for each camera associated to the video system.

8.3.3.7.2.4 Enabling Video Motion Detection

To turn the motion detection on, please:
1. Right click the name of a required camera

2. Select the **Motion Detection On** item in the appeared menu.

In this case:
- The **Request to enable motion detection** event and a current operator's name will be added to the Event Log.

- The video motion detection will be enabled (the **Motion Detection On** event and a current's operator name will be added the Event Log)

Attention!
1. *Enabling/Disabling **video motion detection function (Motion Detection ON/OFF)** has nothing to do with the Arming/Disarming notion in the Orion Pro Suite. Both these notions are differentiated. In other words, when a camera is **armed/disarmed**, it is one kind of motion analysis in the camera, but when the motion detection is enabled/disabled, it is another (parallel) motion analysis. The video motion detection is used to start/stop video recording with the help of management scenarios, etc.*

2. *Since the logic of differentiating between alarms and usual motion is not implemented in the video systems, enabling a motion detection function in the Orion Pro Suite will arm the camera in the video system itself.*

3. *Please note that if a camera is armed or disarmed in the video system itself, the following will happen in the Orion Pro Suite:*

When disarming a camera is initiated in the video system, the camera will be disarmed (if it was armed or an alarm occurred), but the motion detection will be disabled as well (if it was enabled or was in the motion detected status)

8.3.3.7.2.5 Disabling Video Motion Detection

To turn the motion detection off, please:

1. Right click the name of a required camera
2. Select the **Motion Detection Off** item in the appeared menu.

In this case:

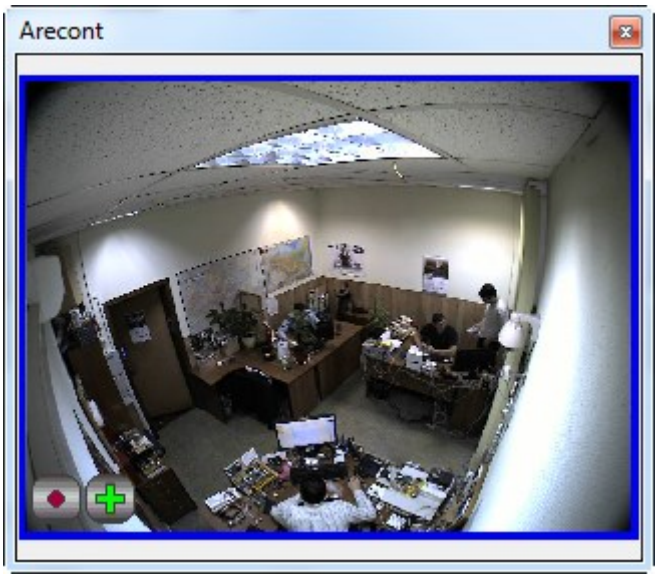
- The **Request to disable motion detection** event and a current SM Operator's name will be added to the Event Log.
- The video motion detection will be disabled (the **Motion Detection Off** event and a current SM Operator's name will be added to the Event Log)

8.3.3.7.2.6 Displaying Video Image

To display video image on the workstation monitor screen, please:
1. Right click a required camera
2. Select the **Show Video** item in the appeared menu

In this case:

v. If a selected camera is one of the Orion Video integrated cameras, a video image window will be opened



- If it is a third party camera, a command to display video image will be sent to a relevant video system. The **Show Video** event and a current SM operator's name will be added to the event log.

8.3.3.7.2.7 Hiding Video Image

To hide video image on the workstation monitor screen, please:
1. Right click a required camera
2. Select the **Hide Video** action in the appeared menu

In this case:

- If this camera is one of the Orion Video integrated cameras, a video image window will be closed
- If it is a third party camera, a command to hide video image will be sent to a relevant video system.

The **Hide Video** event and a current SM operator will be added to the event log.

8.3.3.7.2.8 Recoding Video Image

To start recording, please:

1. Right click a required camera
2. Select the **Start Recording** item in the appeared menu.

In this case:

- The **Start Recording** event and a current SM Operator will be added to the event log.
- The recording of video from the camera will start (the **Recording Started** event will be added to the event log)

8.3.3.7.2.9 Stop Video Recording

To stop video recording, please:

1. Right click a required camera on the pane
2. Select the **Stop Recording** action item in the appeared menu

In this case:

- The **Stop Recording** event and a current SM Operator' name will be added to the event log.
- The recording of video from the camera will stop (the **Recording Stopped** event will added to the event log)

8.3.3.7.2.10 Opening Video Archive to Play Video Records

To play back a video recording:

1. Right click a required camera
2. Select the **Go to Video Archive** in the appeared menu.

The Video Archive window will appear where a selected camera will be added to the list of cameras with available video recordings.

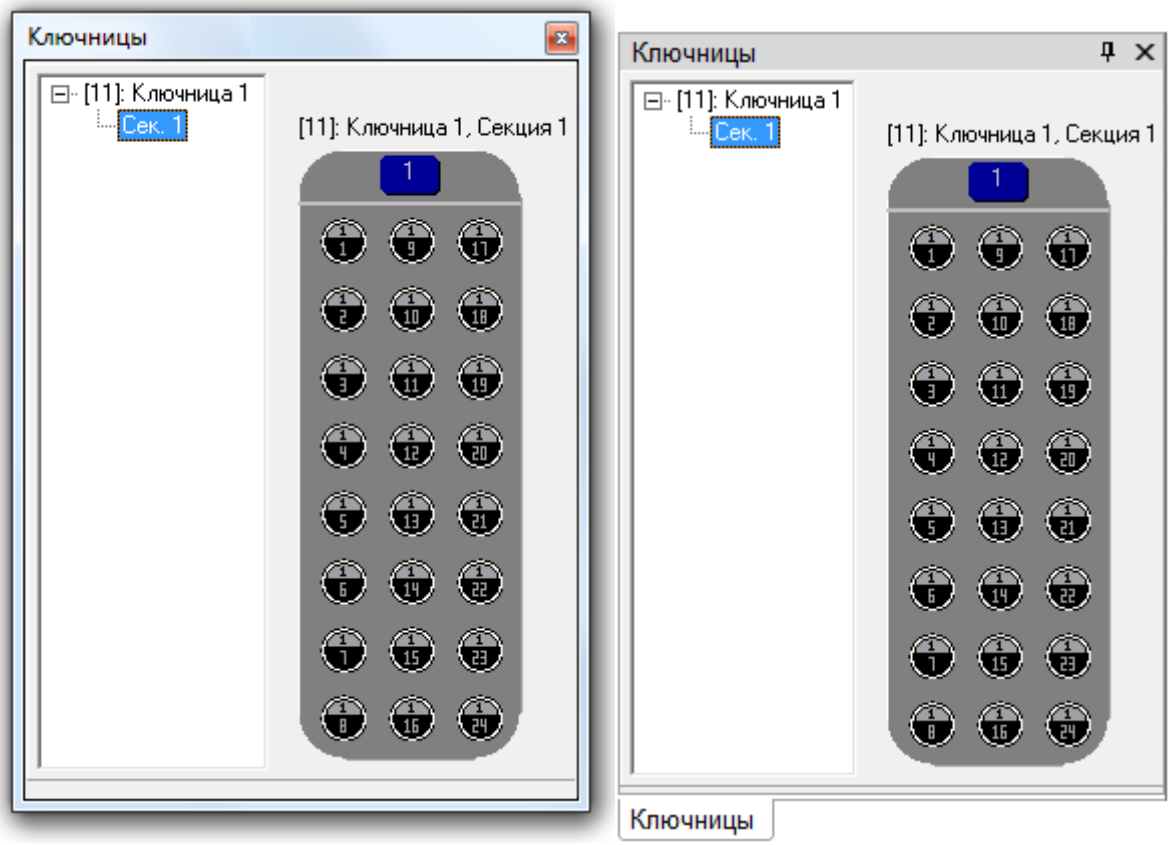
(See *Chapter 8.5.2 Video Archive*)

8.3.3.8 The Keyboxes Pane (This feature is reserved for the future functionality)

The Keybox pane offers the following functions: (all keybox functionality is in process of development):

- Access to key box cylinder.

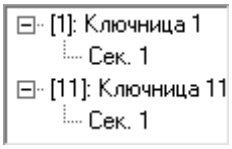
The appearance of the Keyboxes pane:



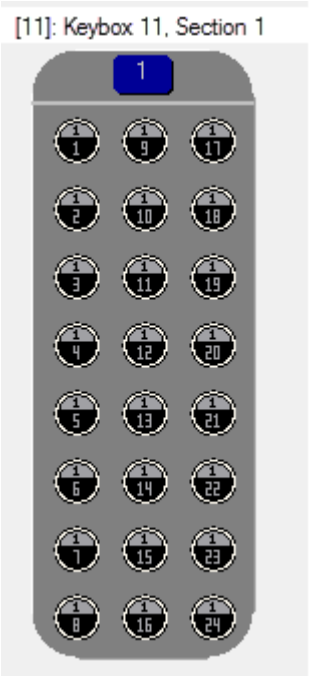
The pane provides the following information:

1. The list of keyboxes.
2. The list of sections for each keybox.
3. Representations of cylinders of the selected section.

The left part of the pane shows the list of keyboxes. It shows an address and name of each keybox. It also shows the sections of each keybox:

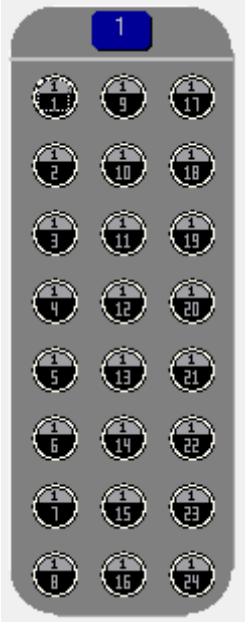


The right part shows keyboxes of a selected section.



8.3.3.8.1 Controlling the Cylinder Entity

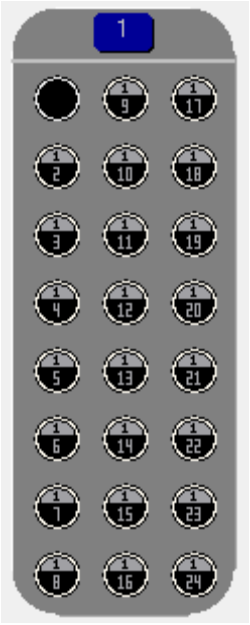
To get an access to a cylinder, please click on it with any mouse button



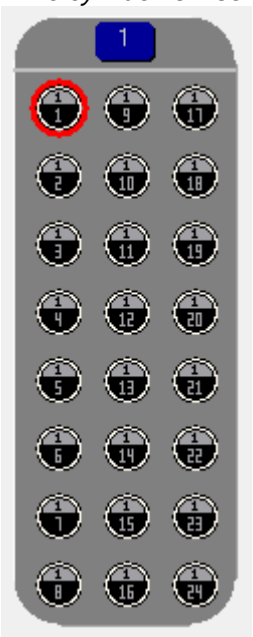
In this case:

- Access granted to Cylinder event and the name of the current operator will added to the Event Log.
- Access to the Keybox Cylinder will be granted.

P.S. When the cylinder is removed, the missing cylinder will be indicated:



If the cylinder is inserted or removed without permission, this keybox cylinder will be highlighted red:

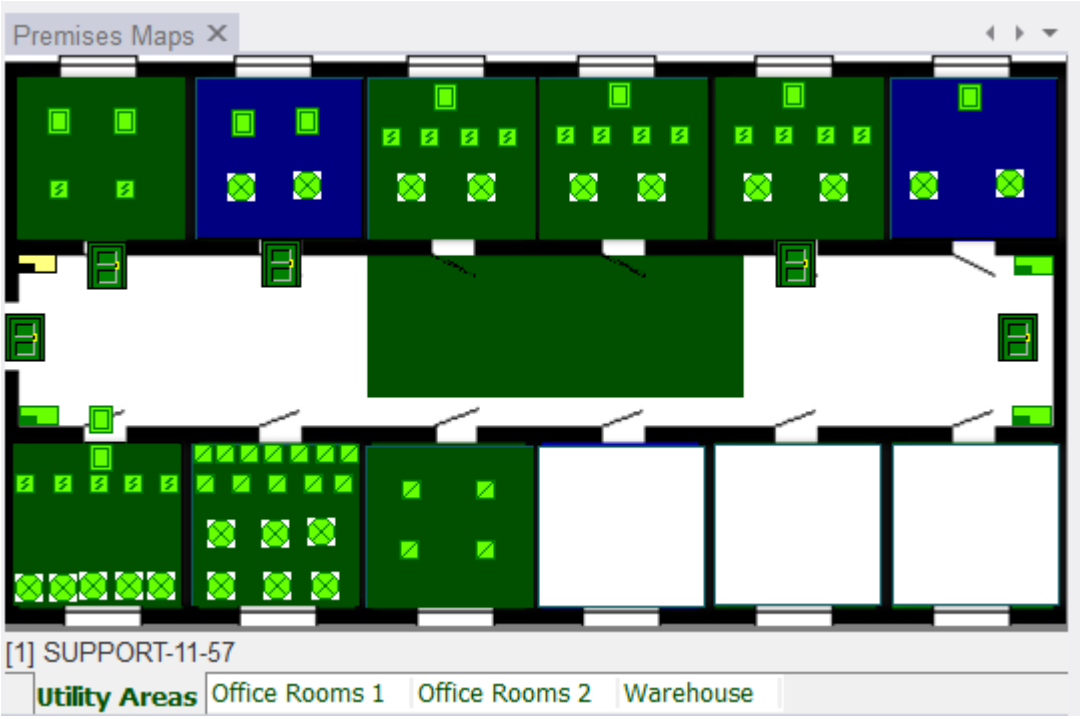


8.3.4 Premises Maps

As said before, premises maps are displayed on the Management tab page.

The Map Display pane can be hidden in the same manner as management, information, and event log panes. But we recommend you to keep it open.

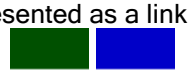
The appearance of the Map Display pane:



The following functions are available on the Map Display pane:

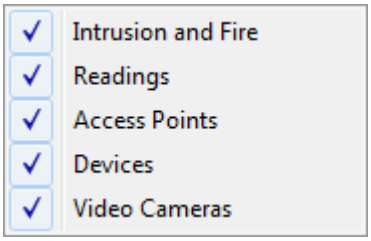
- Viewing status of each system entity in real time
- Operator's interactive control of:
  - loops
  - partitions
  - access points
  - readers
  - cameras,
  - fire extinguishing
- Providing the S2000-K with text messages

The premises maps show the following:

Entities	Examples of entity representation on a map
Loops (inputs)	
Relay outputs	
Partitions	Represented as the area of a partition: 
Readings (Indicators of smoke, temperature, and humidity of partitions)	
Access Point	
Readers	
Devices	
Cameras	
Links to premises maps	Represented as a link area: 

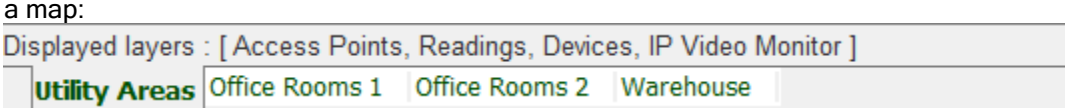
Each entity is represented by color representing its current status. (*Status color codes are provided in the Chapter 8.C Color Codes of System Entity Status*)

Clicking the blank area (free from any entities) will open a contextual menu that can be used to hide or show entities on premises maps:



Menu Item	Entities
Intrusion and Fire	Responsible for representing partitions, loops and relay outputs on premises maps.
Readings	This item is responsible for displaying smoke and temperature indicators on a map
Access Points	This item is responsible for displaying access points and readers
Devices	This menu item is responsible for displaying devices on a premises map
Video Cameras	This menu item is responsible for displaying cameras on premises maps

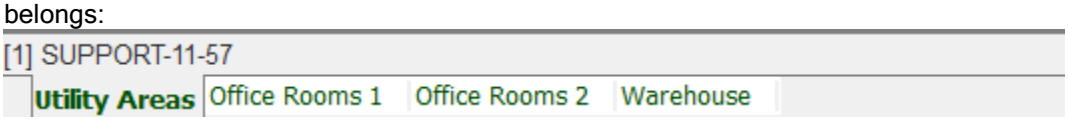
In case of changing displayed layers, the information of displayed elements will be shown at the bottom of a map:



The information disappears, when another map is selected.

8.3.4.1 Toggling between Maps

The bottom part of the map display area shows (above map tabs) the workstation where this map belongs:



This information includes:

1. The number (index) of a workstation as per the database,
2. The name of a workstation as per the database.

The Map selection bar includes tab buttons to toggle between maps:

Attention!

- Maps are arranged by their indexes.
- If a map belongs to another workstation rather than one where the current System Monitor is running, the number (Index) of this workstation will be displayed before the name of this map
- The name of a premises map has color that corresponds to the map's current status.

  Please keep in mind that the status of a premises map is the aggregate of states of loops and partitions related to this map.

Toggling between maps:

- To toggle a required map, please:
  - Click the tab of a required map, or
  - Right click the tabs area and select a required map in the appeared menu:

- To navigate between maps, please use the following keys:

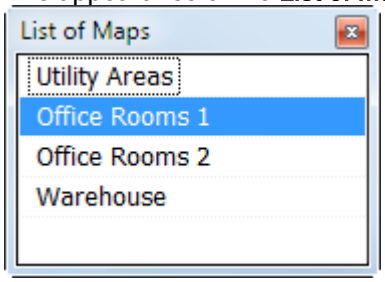
  < [> – to go to the previous map
  <] > – to go to the next map.
- If a map has a link to another map, clicking the link will switch over to this map.

8.3.4.1.1 The List of Maps

The List of Maps area offers the following functions:

- Toggling between premises maps.

The appearance of the **List of Maps** pane:



The pane shows the following information:

1. The list of maps

The name of map is displayed in a color corresponding to the current status of the map.

To toggle a required map, please click a name of this map in the list

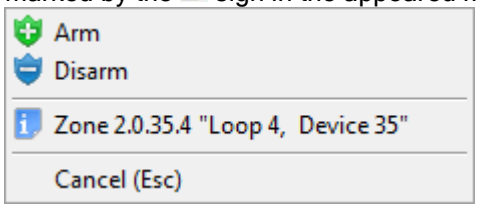
8.3.4.2 Obtaining Information on the System Entity

Using premises maps, one can obtain information about the following:

1. Loops
2. Relay Outputs
3. Cameras
4. Partitions
5. Access Points
6. Readers
7. Devices
8. Average temperatures, smoke concentration, and humidity of partition, as well as power supply information

8.3.4.2.A Obtaining Information about Loops

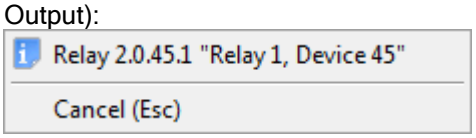
To get information about the Loop entity, Please right click its icon on a map, and then select an item marked by the sign in the appeared menu (this item shows the address and name of the loop):



The **Loop Details** window will appear
(The description of this window is provided in the Chapter *8.3.3.2.1 Obtaining Information about Loops, Relays, and Cameras.)*

8.3.4.2.B Obtaining Information about Relay Outputs

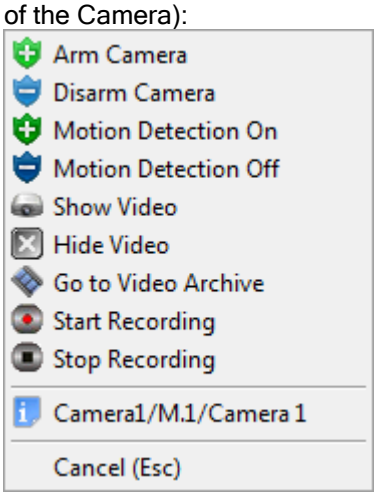
To get information about the Relay Output entity, please right click its icon on a map, and then select an item marked by the sign in the appeared menu (this item shows the address and name of the Relay Output):



The **Relay Output Details** window will appear
(The description of this window is provided in the Chapter *8.3.3.2.1 Obtaining Information about Loops, Relays, and Cameras.)*

8.3.4.2.C Obtaining Camera Details

To get information about the Camera entity, Please right click its icon on a map, and select an item(camera name) marked by the sign in the appeared menu (this item shows the address and name of the Camera):

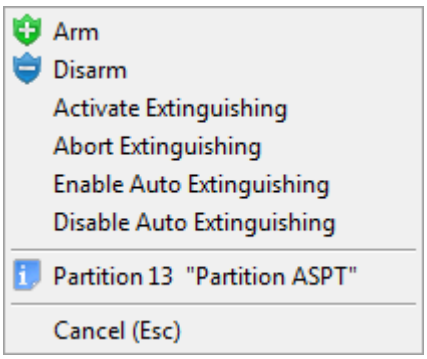


The **Camera Details** window will be displayed.

(*The description of this window is provided in the Chapter 8.3.3.7.1 Obtaining Information about Cameras*)

8.3.4.2.D Obtaining Partition Details

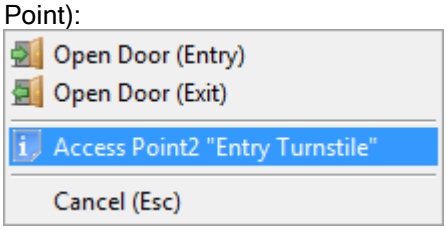
To get information about the Partition entity, please right or left click its icon on a map, and then select an item marked by the sign in the appeared menu (this item shows the address and name of the Partition):



The **Partition Details** window will be displayed.
(The description of this window is provided in the Chapter *8.3.3.2.2 Obtaining Information about the Partition Entity.)*

8.3.4.2. Obtaining Access Point Details

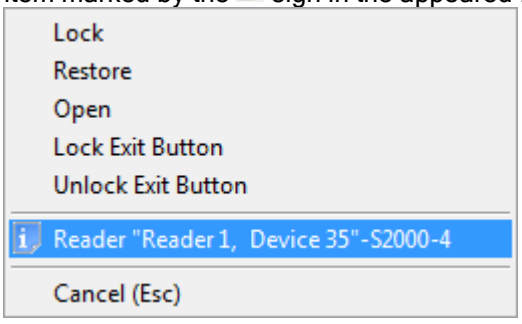
To get information about the Access Point entity, please right click its icon on a map, and then select an item marked by the sign in the appeared menu (this item shows the address and name of the Access Point):



The **Access Point Details** window will be displayed.
(The description of this window is provided in the Chapter *8.3.3.6.3 Obtaining Information about the Access Point Entity.)*

8.3.4.2.F Obtaining Reader Details

To get information about the Reader entity, please left or right click its icon on a map, and then select an item marked by the sign in the appeared menu (this item shows the address and name of the Reader):

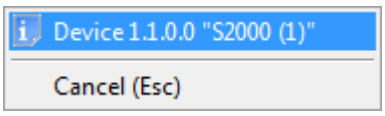


The **Reader Details** window will be displayed.

(The description of this window is provided in the Chapter 8.3.4.2.1 Obtaining Information about the Reader Entity.)

8.3.4.2.G Obtaining Device Details

To get information about the Device entity, please right or left click its icon on a map, and then select an item marked by the sign in the appeared menu (this item shows the address and name of the Device):



The **Device Details** window will be displayed.

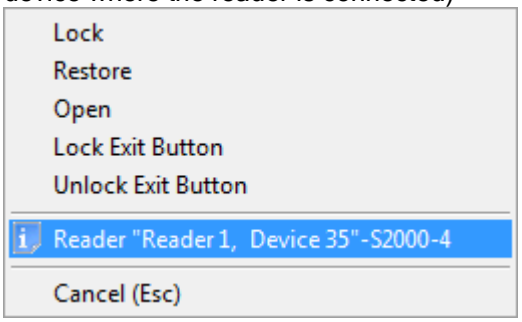
(The description of this window is provided in the Chapter 8.3.4.2.2 Obtaining Information about the Device Entity.)

Obtaining Information about Average Temperature, Smoke Concentration and Power Supply of a Partition

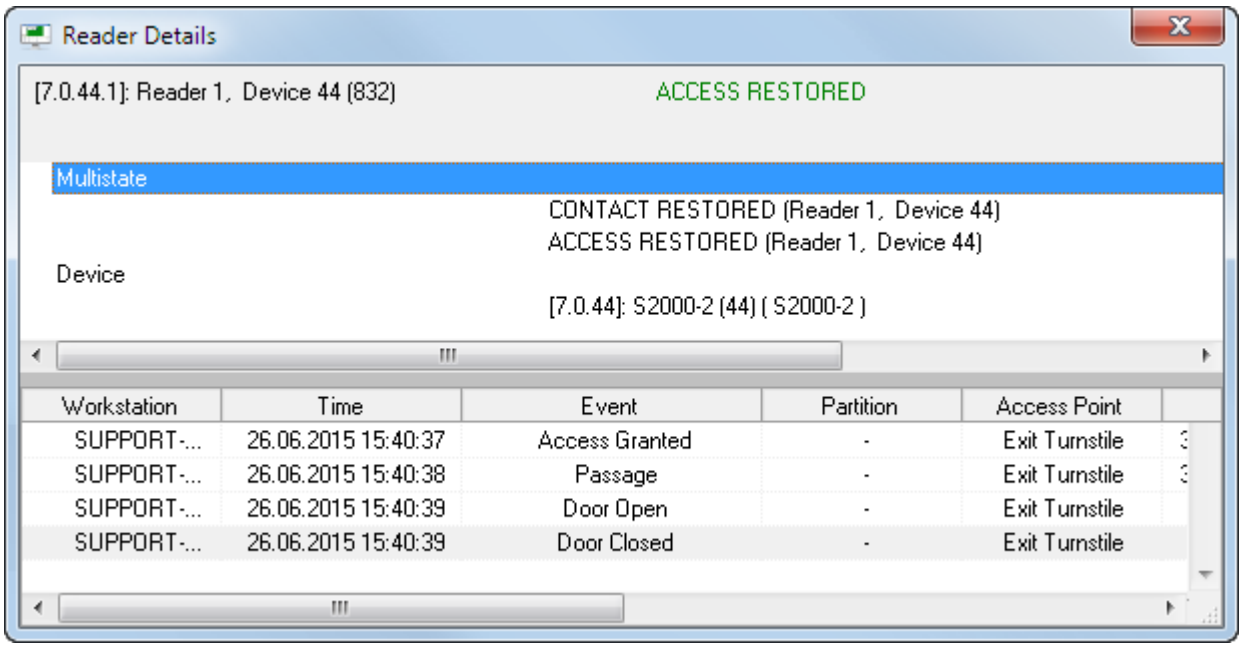
This functionality is described in Chapter 8.3.4.2.3 Indicators of Smoke, Temperature, and Power Supply

8.3.4.2.1 Obtaining Reader Entity Details

To get information about the Reader entity, please right or left click its icon on a map, and then select an item marked by the sign in the appeared menu (this item shows the name of the reader and type of a device where the reader is connected)



The **Reader Details** window will be displayed:



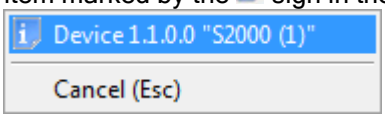
The **Reader Details** window displays the following information:

- The address and custom ID of a selected reader
- The main status of a reader
- The multistate of a reader (*)
- The address, name and type of device where the reader is connected
- Reader-related events

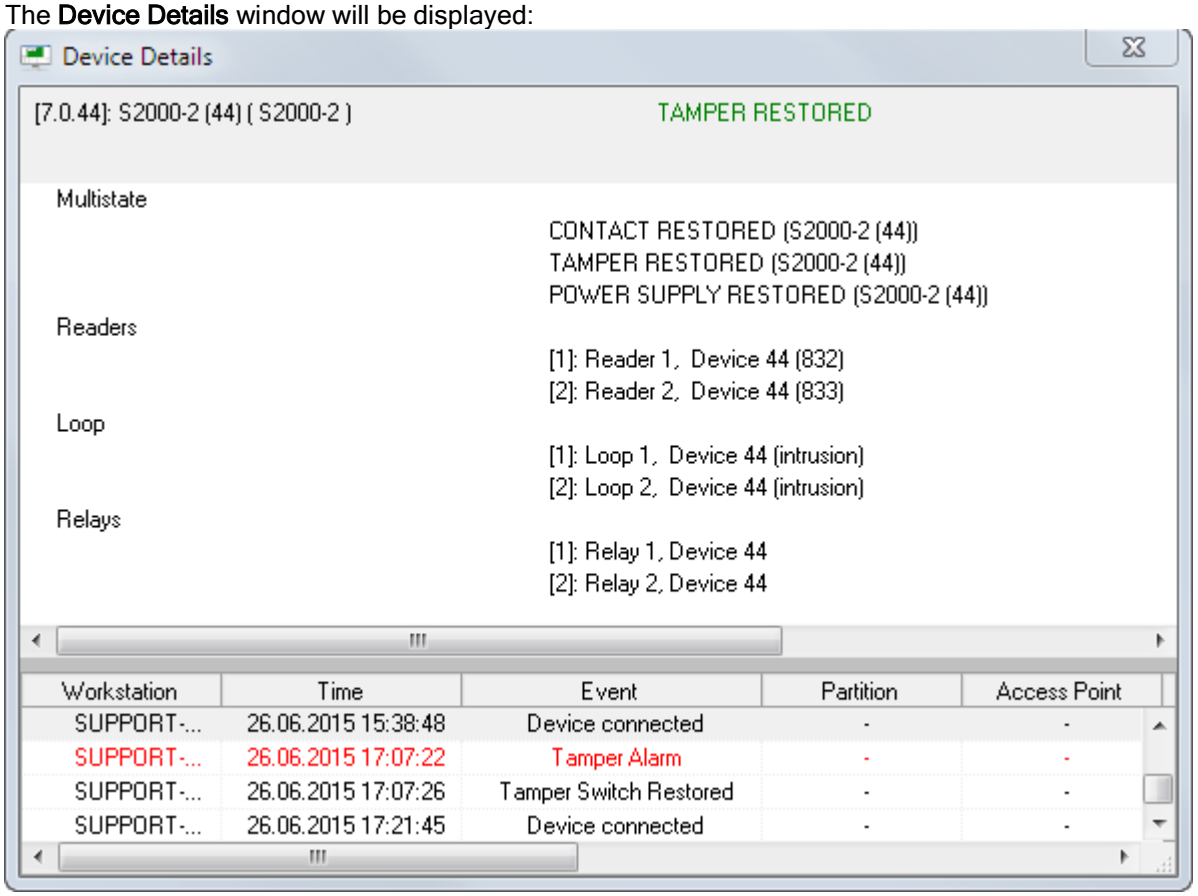
(*) Multistate of entities is described in Chapter *8.1.2.*

8.3.4.2.2 Obtaining Device Details

To get information about the Device entity, please right or left click its icon on a map, and then select an item marked by the sign in the appeared menu (this item shows the name and address of the Device):



The **Device Details** window will be displayed:



The **Device Details** window displays the following information:

- The address and type of device
- The device main status
- The device multistate (*)
- Information on the readers connected to the device – the number, name and custom ID of each reader
- Information on the device's loops – the number and name of each
- Information on the device's relay outputs
- Device-related events

(*) The Multistate of entities is described in Chapter *8.1.2.*

8.3.4.2.3 Indicators of Smoke Concentration, Temperature, Humidity and Power Supply

8.3.4.2.3.1 Obtaining Information on temperature, smoke and power supply situation

If statistics is gathered for some analog-addressable zones of a partition, and a map has a temperature indicator, this indicator displays the average temperature of these zones: 

.

The indicator color varies with the current average temperature of the partition:

- When temperature is 0° the indicator is dark red,
- When temperature increases, the indicator becomes brighter (it becomes ruby red when the indicator shows 50° or higher)
- When temperature decreases, the indicator becomes darker (it becomes bright blue when the temperature drops till -30 °C and lower.

If statistics is gathered for some analog-addressable zones of a partition and a smoke concentration indicator is used on a map, this indicator displays average smoke concentrations of these zones: 

.

The color of indicator varies in accordance with average smoke concentration of a partition:

- When smoke concentration is zero level, the indicator is dark green
- When concentration increased, the indicator color turns gradually greyer (it becomes grey when the smoke indicator show 120)

If statistics is gathered for some analog-addressable zones of a partition and a humidity indicator is used on a map, this indicator displays average humidity level of these zones: 

.

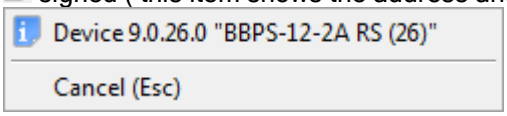
The indicator color will be dark green.

8.3.4.2.3.2 Obtaining Power Supply Details

The System Monitor offers capability to view output voltage of the BBPS-12 RS, BBPS-12-2A RS, and BBPS-24-2A RS power supplies

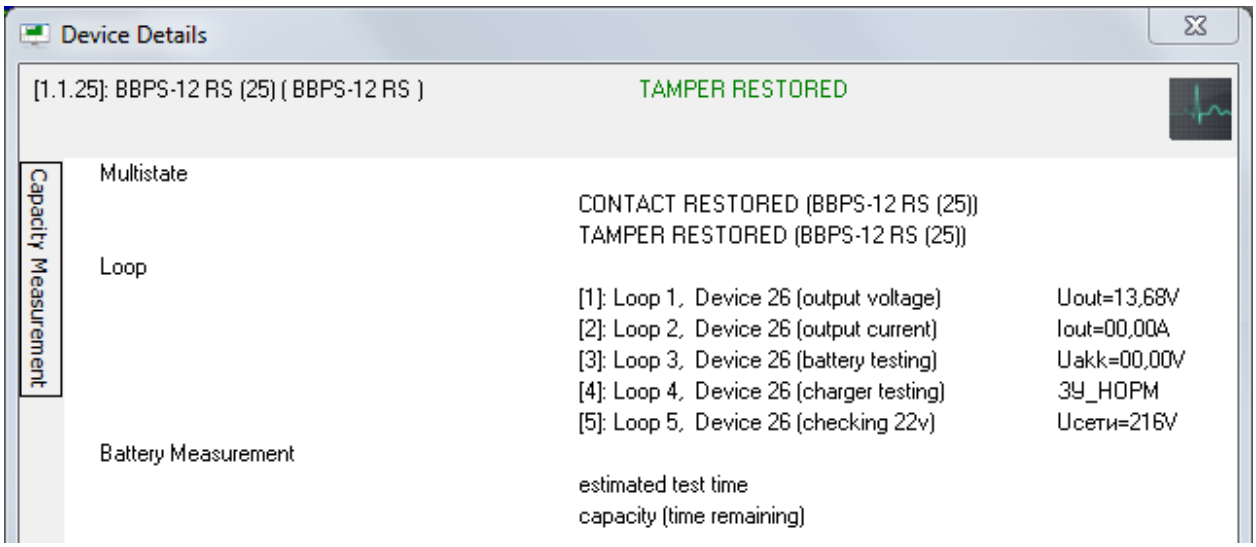
This functionality is available, when the RIP -12 RS icon is added to a map

To view output voltage, please left or right click the RIP-12 RS icon, then select an info item marked with  signed (this item shows the address and name of the device:

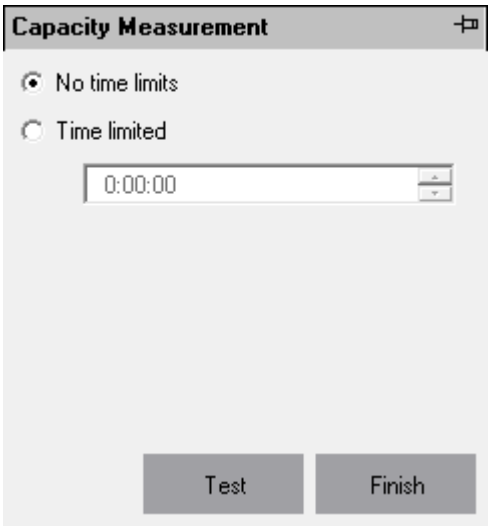


The information window will display information about the device. In case of the RIP-12 RS, unlike other devices, the window shows the following information for loops:
1st loop - Output voltage
2nd loop – Output current (load current)
3rd loop – battery output (battery age)
4th loop – Charger condition
5th loop – Mains voltage

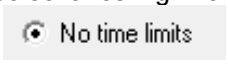
It will also show battery capacity, battery remaining time, and estimated testing time



The **Device Details** window offers a buttery testing function. If one clicks **Capacity Testing**, a battery testing toolbar will appear:



Please select a testing interval:

1.  – (No time limits) Full time testing. The calculated testing time is displayed in the Device Details window.

2.  – (Time limited) testing period is limited by time specified in the field:  .

Click the **Test** button to start testing.
Click the **Stop** button to stop testing.

Attention!

- There is no limitation to start testing the RIP-12RS in any time.
- The test of the RIP-24-2/7P1-R-RS RIP-24-2/7P1-P-RS can be started when its charged level is more than 80%.
- The test of the RIP-12-3/17M1-R-RS can be started if its charged level is more than 80% and the consumption current is at least 0.2A but not more than 3A.

8.3.4.3 Controlling Intrusion and Fire System

The premises maps provide access to control (arm/disarm) the following entities of the intrusion and fire alarm and protection systems:

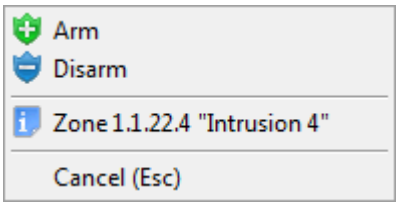
1. Loops
2. Partitions.

8.3.4.3.1 Arming/Disarming Loops

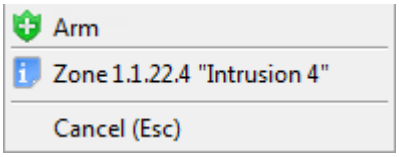
To arm or disarm a loop, please right click a loop icon to open a contextual menu.

The availability of contextual menu action items depends on a type of loop and operator rights defined by an access level assigned to the current operator's software password (See Appendix 8 E Loop Commands):

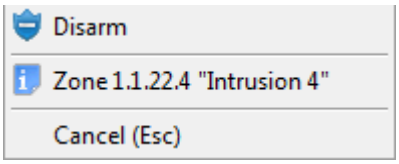
- Arming and disarming loops (full rights) :



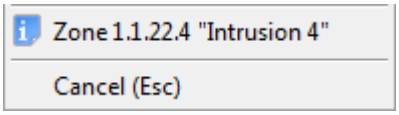
- Arming loops only:



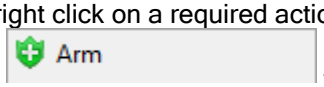
- Disarming loops only:

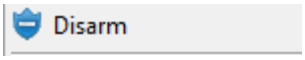


- Only viewing loop details



Left or right click on a required action item will initiate the following actions:

- 

– an attempt of arming a loop,
- 

– disarming a loop
-  – displaying an info window with loop details.

Details for manual arming and disarming actions in the system are described in the Chapter 8.3.3.2.3 Controlling Alarms and Cameras

Accessibility of arming and disarming action items of the menu depends on operator rights:

Please note that the accessibility of menu items depends on an operator's rights:

c. If the **Management of Individual Zones** property of an operator's password is set as **''Off''**, the operator is not allowed to arm a loop

d. If the **Management of Individual Zones** property is "**On**", then:

i. If an operator has rights to arm a partition, an operator is allowed to arm loops included in this partition.

ii. If an operator has right to disarm a camera-including partition, disarming a loop is allowed

iii. If a loop-including partition is a High-Security one, and the Management **of High Security Partitions** (Control High Security Partitions) option is set as '**Off',** a disarming action is not allowed.

Note the accessibility of arming/disarming actions also depends on the type of loop (Refer to Appendix E Commands for Loops. If the type of loop does not allow arming or disarming the corresponding menu items is not accessible

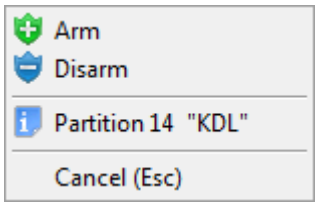
Obtaining loop details is always available.

8.3.4.3.2 Arming Partitions

To arm or disarm a loop, please right click a loop icon to open a contextual menu.

The available action items of the contextual menu depend on operator rights defined by an access level assigned to the current operator's software password

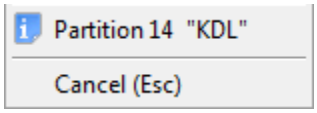
- Arming and disarming a partition (full rights)



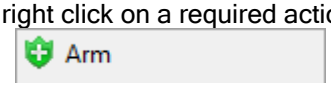
- Only arming a partition:

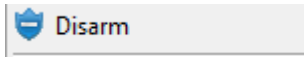
- Only disarming a partition:

- Only viewing partition details and status:



Left or right click on a required action item will initiate the following actions:

- 

– an attempt of arming a partition,
- 

– disarming a partition
-  – displaying an info window with partition details.

Details for system performance related to arming and disarming by the operator are described in Chapter 8.3.3.2.3 Controlling the Partition Entity

Accessibility of arm and disarm items in the menu depends on the operator rights:

Please note that the accessibility of menu items depends on an operator's rights:

e. If the **Management of Individual Zones** property of an operator's password is set as "Off", the operator is not allowed to arm the partition

f. If the **Management of Individual Zones** property is "On", then:

i. If an operator has rights to arm a partition, the operator is allowed to arm the partition

ii. If an operator has right to disarm a camera-included partition, arming the partition is allowed

iii. If a partition is a High-Security one, and the Management **of High Security Partitions** property of the operator's software password option is set as '**Off',** a disarming action is not allowed.

Note the accessibility of arming/disarming actions also depends on the types of loops included in the partition (Refer to Appendix E Commands for Loops. If a loop type do not support arming or disarming, the corresponding menu items are not accessible

Obtaining loop details is always available.

8.3.4.4 Fire Extinguishing Control

The SM Operator can control fire extinguishing system based on SC2000-ASPT and Potok-3N devices.

ATTENTION! When discussing fire extinguishing control, this chapter assumes that an individual partition is created for each S2000-ASPT and Potok-3N device, which includes all loops and supervised outputs of the S2000-ASPT device or corresponding loops of the Potok-3N device

Maps offer functions to control fire extinguishing using the following system entities:

1. Loops
2. Partitions

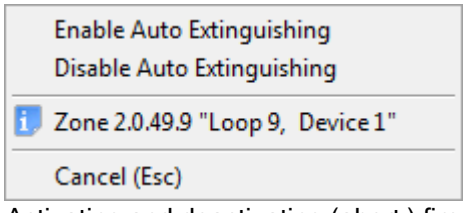
8.3.4.4.1 Controlling Fire Extinguishing Using Loops

To control extinguishing system using loops, please right click a loop icon to open the contextual menu.

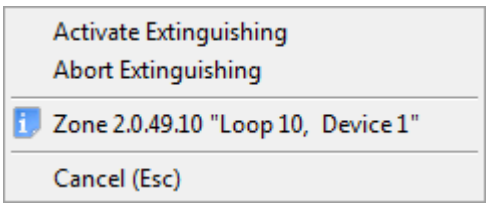
The available action items of the contextual menu depend on the following:

- operator rights defined by an access level assigned to the current operator's software password and
- the type of a loop (Refer to Appendix 8 E Commands for Loops

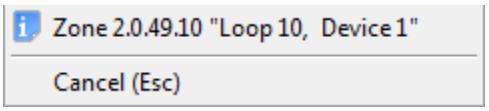
- Enabling/Disabling the automatic mode of fire extinguishing:



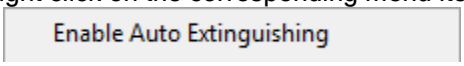
- Activating and deactivating (abort) fire extinguishing:

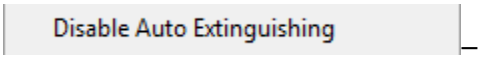


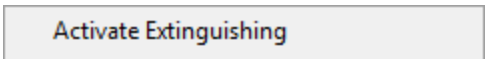
- Only viewing loop details and status:

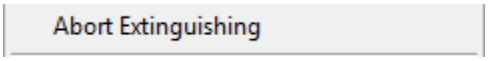


Left or right click on the corresponding menu item will initiate the following actions:

- 

– Enables the auto mode of fire extinguishing in the appropriate device,
- 

– Disables the auto mode of fire extinguishing in the appropriate device,
- 

– Activates fire extinguishing in the appropriate device (with a pre-run request of the SM operator's password)
- 

– Deactivate (abort) fire extinguishing in the appropriate device
-  – Displays the Loop Details window.

Please note that the accessibility of menu items to control fire extinguishing depends on an operator's rights:

g. If the **Management of Fire Extinguishing System** property of an operator's password is set as **Off**, the operator may not use loops to control fire extinguishing

h. If the **Management of Fire Extinguishing** property is "**On**", the operator is not allowed to use loops to control fire extinguishing, and all menu items are accessible

Note the accessibility of menu action items to control fire extinguishing actions also depends on the type of loop (Refer to Appendix E Commands for Loops. If a loop type does not support fire extinguishing control functions, the corresponding menu items are not accessible

The information item is always available

If an operator request to activate or cancel fire extinguishing:
Activation of Extinguishing or Cancel of Extinguishing event and the current SM Operator' name will be added to the Event Log
A corresponding command will be sent to the device.

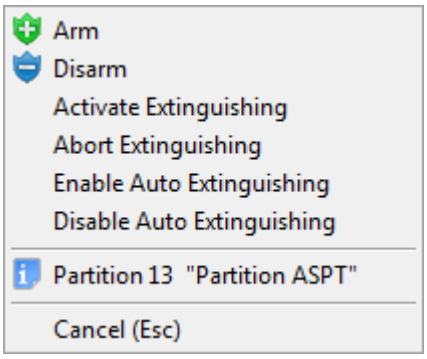
If an operator requests enabling or disabling Auto Mode, a corresponding command will be sent to the device.

8.3.4.4.2 Fire Extinguishing Control

To control fire extinguishing system using via partitions on the map, please right click a partition area to open the contextual menu.

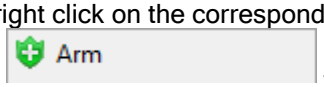
The accessibility of menu action items depends on operator rights defined by the current operator's software password:

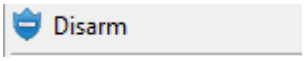
- Full control (enabling/disabling the automatic mode of fire extinguishing, and activation or deactivation (abort) of fire extinguishing:

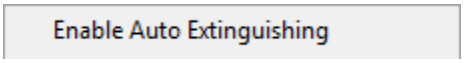


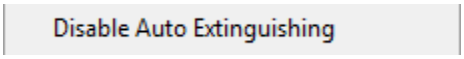
- Only viewing partition details and status:

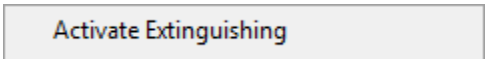
Left or right click on the corresponding menu item will initiate the following actions:

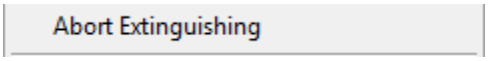
- 

–Attempts to arm a partition
- 

– Arms a partition
- 

– Enables the auto mode of fire extinguishing in the appropriate device
- 

– Disables the auto mode of fire extinguishing in the appropriate device
- 

- Activates fire extinguishing in the appropriate device (with a pre-run request of the SM operator's password)
- 

– Deactivate (abort) fire extinguishing in the appropriate device
-  – Displays the Partition Details info window.

The Arm and Disarm items can be used for a partition with loops (and supervised outputs of S2000-ASPT device. But they are have sense only in case of using S2000-ASPT devices of 3.00 version or higher

Accessibility of menu items and actions of the system in case of arming and disarming by an operator's request are described in Chapter 8.3.4.3 Fire Extinguishing Control. This chapter discusses the menu items accessible for SM Operator to control fire extinguishing using partitions.

Please note that the accessibility of menu items to control fire extinguishing depends on an operator's rights:

i. If the **Management of Fire Extinguishing System** property of an operator's password is unchecked, the operator is not allowed to use partitions to control fire extinguishing

j. If the **Management of Fire Extinguishing** property is checked, the operator is not allowed to use partitions to control fire extinguishing, and all menu items are accessible

Note the accessibility of menu items to control fire extinguishing also depends on a loop type (Refer to Appendix E Commands for Loops. If a loop type does not support fire extinguishing control functions, the corresponding menu items are not accessible

Obtaining information is always available

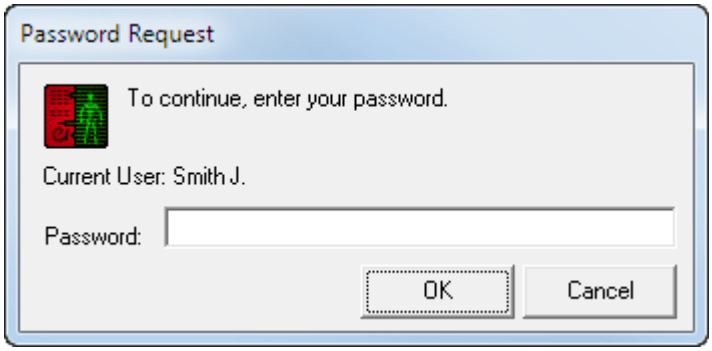
If an operator request to activate or abort fire extinguishing:

- **Activation of Extinguishing** or **Abort of Extinguishing** event and an SM Operator's name will be added to the Event Log
- A command to activate or abort fire extinguishing will be sent to the device.

If an operator request enabling or disabling Auto Mode, a corresponding command will be sent to the device.

8.3.4.4.3 Pre-Activation Request of an Operators Password

As said above (8.3.4.4.1 and 8.3.4.4.2), when an SM operator attempts to activate fire extinguishing using a partition or loop, the operator's password will be requested in the **Extinguishing Activation** dialog box:



The further system actions depend on what data are entered:

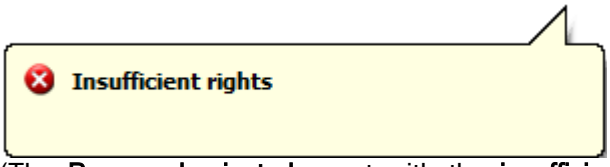
- If one clicks the **Cancel** button, fire extinguishing will not be initiated
- If one clicks **OK** after entering a wrong password, the System Monitor:
  - will not accept the password,
  - and generate the following messages
    - in case of unknown password:

(*The **Password rejected** event and the **Password not found** description will be added to the Event Log*).

- If the employee status does not allow working with the System Monitor:

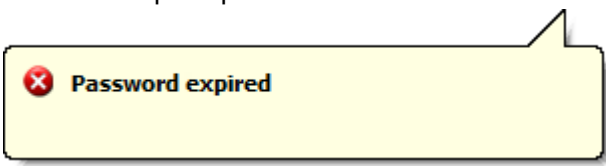
(The **Password rejected** event with the **Low Operator status** description, and a password holder name will be added to the Event Log)

- If the password does not provide any rights to run the System Monitor (Operative Task):



(The **Password rejected** event with the **insufficient rights** description and the name of the password holder will be added to the Event Log)

- In case of expired password :



(The **Password rejected** event with the **Password has expired** description and a password holder's name of will be added to the Event Log.

- If an operator has no rights to control fire extinguishing entities, no message box will be displayed.
  (The **Password rejected** event with the **No extinguishing control rights** description and a password holder's name of will be added to the Event Log.

  - The System Monitor will wait for a correct password.

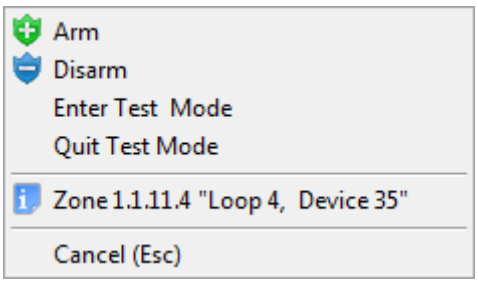
- If the password of currently logged operator or that of another operator is entered:
  - The system monitor will accept the password
  - The **Discharge** event and the name of a password holding operator will be added to the Event Log,
  - A command to activate extinguishing will be sent to a device.

8.3.4.4.3 Testing Detectors

The testing of S2000-KDL, S2000-KDL-2I, and S2000-KDLS devices can be controlled in accordance with the following algorithm:

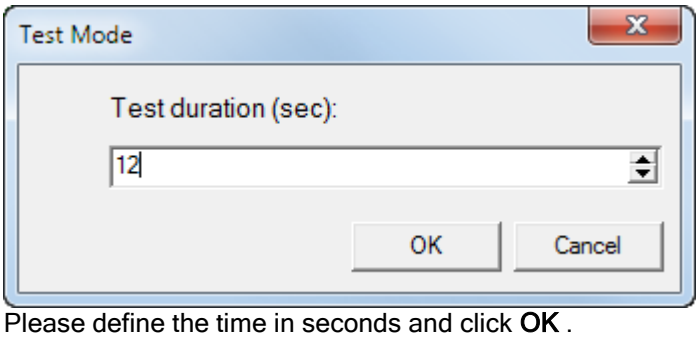
- For DIP-34A and S2000-IP. Any testing actions (presenting magnet, pressing button or applying laser) are resulted in forming the **Detector Test** event for the zone. To test the system response to the **Fire** event, please apply smoke or aerosol to a detector, or switch the zone to testing mode
- For intrusion detectors. As a rule, the indication of intrusion sensors are disabled by removing a required jumper or selecting the **AD indication is not allowed** for the **AD Indication Settings** parameter in the device settings. But in the process of configuring and testing, it is required to see the sensor response to stimulus (e.g. movement). In this case, please disarm the zone and switch it to the testing mode, then the indication will be as described in the manual and initiation of alarm will result in generating the **Detector Test** event.
- The test mode can continue as long as specified (in seconds) by a user when entering the test mode. The maximum test duration is 2.2 hours

To enter or exit the test mode, please right click a loop icon or partition area on the map to open contextual menu. The menu will show actions available for the current operator. But if you operate the S2000-KDL, S2000-KDL-2I and S2000-KDLS devices, and partition with these zones, the menu will also include items to enter or exit the detector test mode:



Right or left click on a corresponding menu items will result in the following:

- Enter Test Mode – Displays the window to define testing time:



Please define the time in seconds and click **OK** .

- Quit Test Mode – the test mode will be disabled.

If control actions are applied to a partition, the corresponding commands will be sent to all partition zones assigned to the S2000-KDL, S2000-KDL-2I, and S2000-KDLS.

8.3.4.5 Access Control System

Premises maps can be used to control the following entities of access control system:

1. Access Point
2. Reader

8.3.4.5.1 Access Points

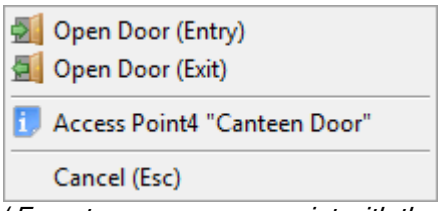
To grant access via an access point, please right click the icon of required access point to open the contextual menu.

The availability of contextual menu action items depends on the following:

- operator rights defined by an access level assigned to the current operator's software password and
- an access point type and operating mode

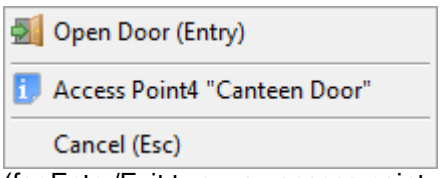
The contextual mode displays action items accessible for the current operator:

- Granting access in both direction (Exit and Entry)



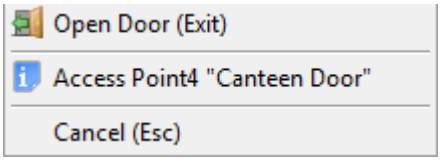
(*For* a *two-way access point with the Entry/Exit operating mode*

- Granting entry access:



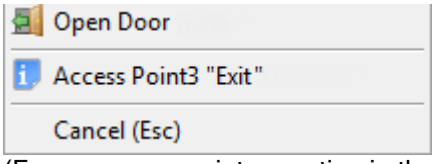
(for Entry/Exit two-way access point *or Entry one-way access point* .)

- Granting the Exit access:



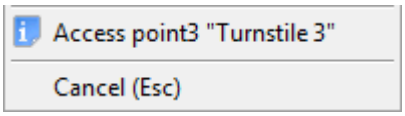
(*For an Entry/Exit two-way access point or Exit one-way access point)*

- Granting an access with no tracing an access direction mode:

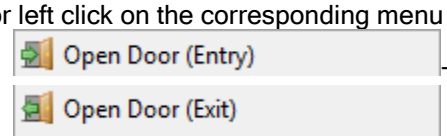


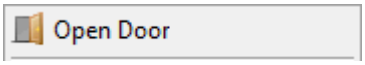
(For an access point operating in the **Passage** mode)

- No rights for granting access:



Right or left click on the corresponding menu item results in the following actions:

- 

– Granting **Entry** access via an access point
– Granting **Exit** access via an access point,
- 

– Granting access (with no tracing an access direction) via an access point
- – Displays the Access Point Details window.

If an operator initiates a command to grant access, the following will occur:

- The corresponding **Open Door (Entry)/Open Door (Exit)** event, and a current operator's name will be added to the Event Log
- An access granting command will be sent to a device. The **Access Granted** and **Passage** events will be generated with the current operator's name being added.

Note that possibility of granting access depends on an operator's rights.

If an operator has rights to grant access via an access point in a certain direction, i.e. an item to grant access in this direction will be available for this operator in the menu. Otherwise, it is not available.
The access point information item ( ) is always available.

8.3.4.5.2 Controlling a Reader

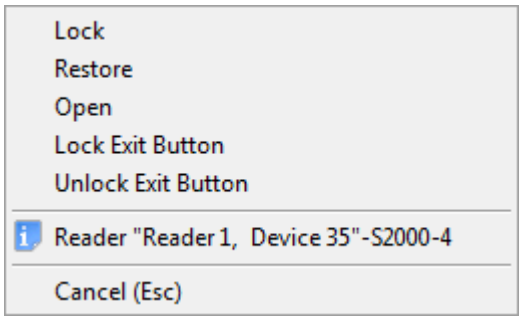
In order to perform the following:

- To lock access via an access point in a direction control by a reader
- To open (free)access via an access point in a direction control by a reader
- To Restore access (return to normal access control)
- To lock a push-to-open button
- To unlock a push-to-open button

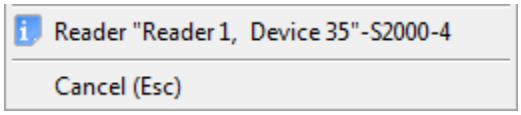
Please right click a required reader icon to open the contextual menu.

The available action items of the contextual menu depend on operator rights assigned to the current operator's software password:

- If an operator has rights to control an access mode via an access point in a direction controlled by this reader



- No rights to control access on the access point via a direction controlled by this reader:



The Left or right click on a relevant menu item will result in the following:

- Lock – Locks access via an access point in the direction controlled by a selected reader.

  (*In case of the S2000-2 functioning in the **One Door for Entry/Exit**, **Barrier**, and **Mantrap** modes, it will lock access controlled via both readers*)
- Restore – Restores access control by credentials in the direction controlled by this reader

  (*In case of the S2000-2 functioning in the **One Door for Entry/Exit**, **Barrier**, and **Mantrap** modes, it will restore a normal access control mode via both readers*)
- Open – Opens free access via a an access point controlled by a selected reader.

  (*In case of the S2000-2 functioning in the **One Door for Entry/Exit**, **Barrier**, and **Mantrap** modes, it will provide free access mode via both readers*)
- Lock Exit Button – Locks access provided via an access point by a button in the direction controlled by the selected reader.
- Unlock Exit Button – Restores access provided via an access point by a button in the direction controlled by the selected reader.

If an operator sends a command to change a mode:

- The **Access Locked**, or **Access Restored**, or **Free Access Open** event with the current operator name will be added to the Event Log
- One of these commands will be sent to a device

When an access is requested by button, no a command-related event will be generated. The event on locking/unlocking a button will be generated by a device itself as designed.

Please note that the possibility of sending a command to change an access mode depends on the operator rights.

If an operator has rights to control access in a relevant direction, the operator will be able to send a command to change access mode to this direction (in other words, there will be available menu items for the reader controlling access in this direction). Otherwise, these items will not be available

The reader information item is always available.

8.3.4.5.1 An Employee Card , Displaying and Employee Cards

In the process of System Monitor functioning, employee cards (profiles) can be displayed as triggered by the defined system events.

In accordance with the options selected in the Database Administrator, an employee card can be displayed in following manner:

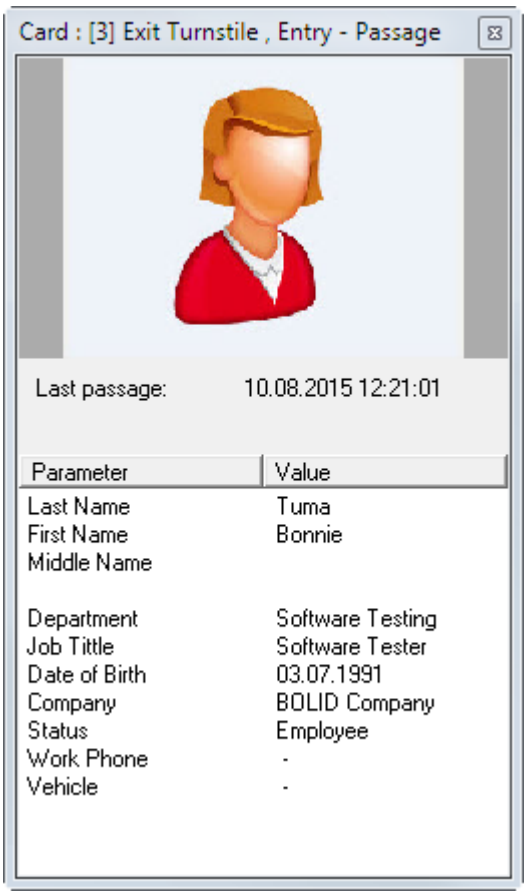
- Not displayed (**No show**)
- Displayed for a time (**Show for a Set Time**)
- Always displayed (**Show Always**).

A list of events triggering the display of an employee card can be configured for each system reader.

The list of events that can trigger displaying an employee card:

- Access Granted
- Access Rejected
- Passage (transaction)
- Access Denied
- Credentials
- Remote Request for Arming
- Remote Request for Disarming
- Partition Armed
- Partition Disarmed

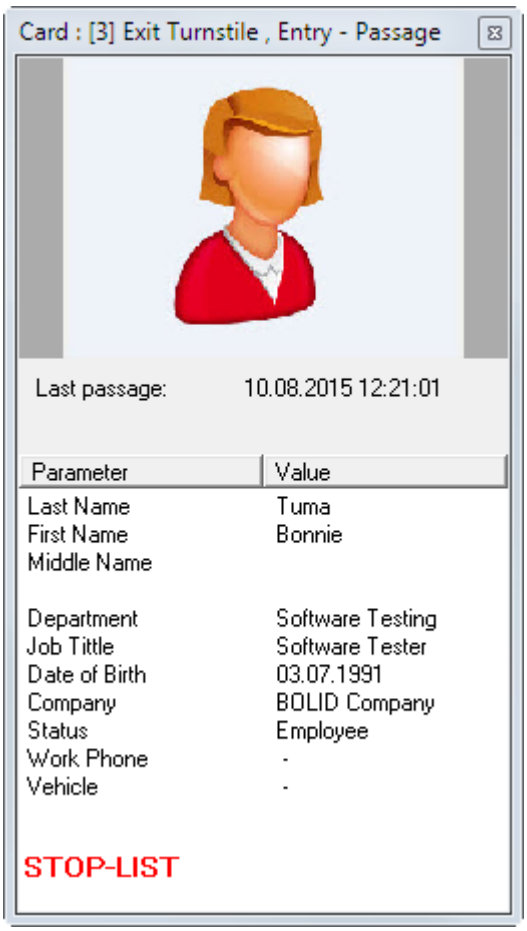
The following figure shows the example of an employee card:



As the figure shows, an employee card includes the following information:

1. Employee photo
2. The last transaction (entry or exit) by an employee
3. Last Name
4. First Name
5. Middle Name
6. Department
7. Job Title
8. Birth Date
9. Company
10. Status
11. Work Phone
12. Vehicle info

If the Stop List attribute is assigned to an employee card, it will be displayed on the bottom of the card:

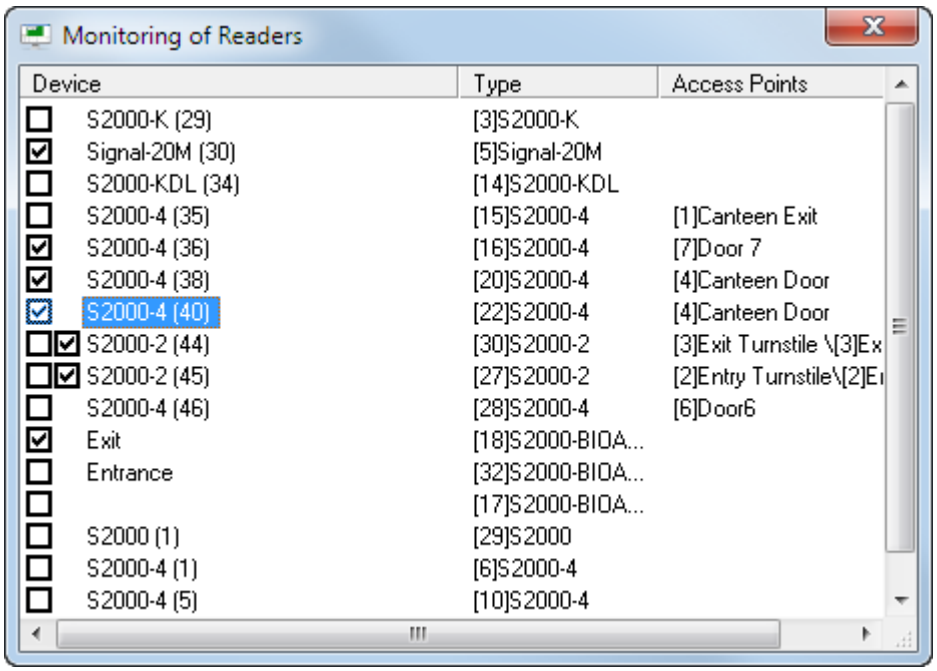


An employee card is displayed in the following manner:

- If it is set to be displayed for a set time:
  - During the period as defined in the database
  - Or till the event triggering another employee card to be displayed during the time specified in the database
- If it is set to be always displayed:
  - Always till a new event triggering the display of another employee as specified in the Database Administrator

Attention! By default the System Monitor does not show employee cards

To configure how employee cards will be displayed by the System Monitor, please press the <F7> key to open the **Monitoring of Readers window**, and select those readers where occurred events will have to trigger displaying employee cards:



As the figure shows, the Readers Monitoring window displays the following information:

1. A check box for each reader to select a device where a reader events will trigger displaying employee cards
2. The name of each reader
3. Index and type of each reader
4. Access point(s) controlled by a device

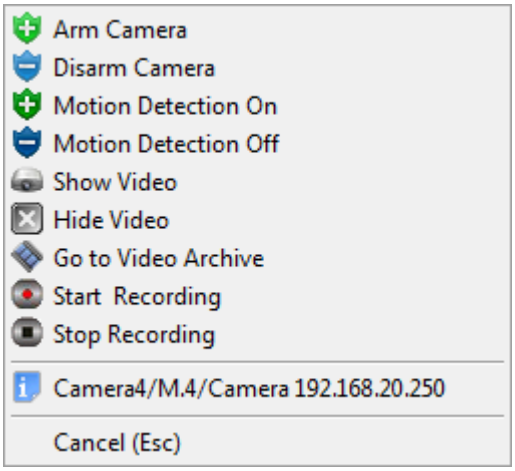
8.3.4.6 Controlling Cameras

The maps can be used to control video cameras of the security system

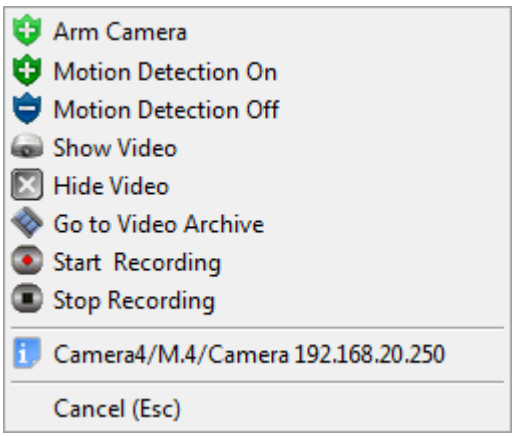
To control a camera, please right click a camera icon to open the contextual menu.

The available action items of the contextual menu depend on operator rights assigned to the current operator's software password:

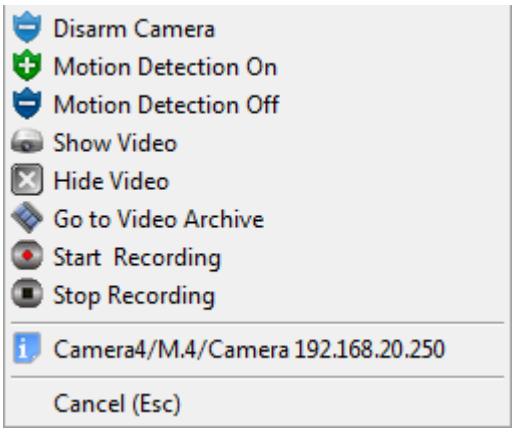
- Full control rights (arming and disarming a camera, enabling and disabling motion detection and recording video image):



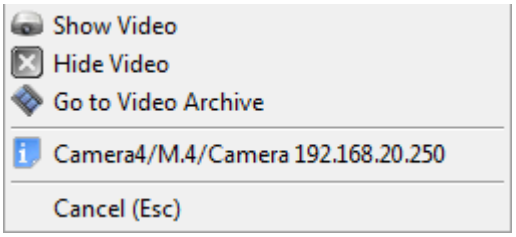
- Only arming a camera (as well as enabling motion detection, and recording):



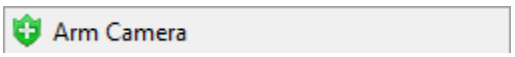
- Disarming a camera (as well as disabling motion detection and stopping video recording):



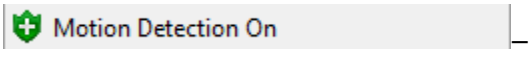
- Only viewing camera info:

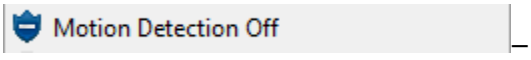


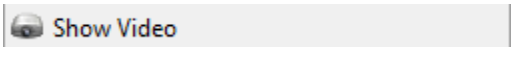
The left or right click on a relevant menu item will result in the following:

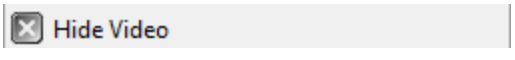
- 

– Arms the camera
- 

– Disarms the camera
- 

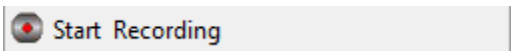
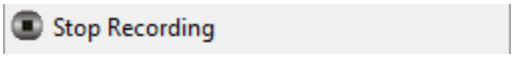
– Enables video motion detection
- 

– Disables video motion detection
- 

– Displays a camera video image on the screen,
- 

– Hides a camera video image on the screen
- 

–Opens video storage window where this camera will be added to the list of cameras for playing (*See Chapter 8.5.2 Video Archive*)

-  – Starts recording a video image from the camera
-  – Stops recording a video image from the camera
-  – Displays the Camera Details window

Detailed information on system actions in response to an operator's camera control commands are described in Chapter 8.3.3.7.2 Controlling the Camera Entity. This chapter focuses on what action items of the menu are available for the SM operator depending on the assigned rights

The accessibility of menu items depends on an operator's rights:

k. If the **Management of Individual Zones** property of an operator's password is set **Off**, the camera may not be controlled

l. If the **Management of Individual Zones** property is set as **On**, then:

i. If an operator has rights to arm a camera-including partition, the following action will be allowed:

4. To arm a camera (**Arm Camera**)
5. To turn on video motion detection (**Motion Detection On**)
6. To start recording (**Start Recording**)

ii. If an operator has rights to disarm a camera-including partition, the following actions will be allowed:

4. To disarm a camera (**Disarm Camera**)
5. To turn off the video motion detection (**Motion Detection Off**)
6. To stop recording (**Stop Recording**)

iii. If an operator has any rights (either arming or disarming rights), the following actions are allowed:

3. To **Show Video**
4. To **Hide Video**

iv. If a camera-including partition is a High-Security one, and the **Management of High Security Partitions** option is set as '**Off**', the following actions are not allowed:

1. To disarm camera (**Disarm**)
2. To turn off video motion detection (**Motion Detection Off**)
3. To stop recording (**Stop Recording**)

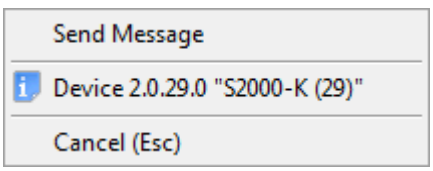
The camera information item is always accessible in the menu.

8.3.4.7 Sending a Text Message to the S2000-K Keypad

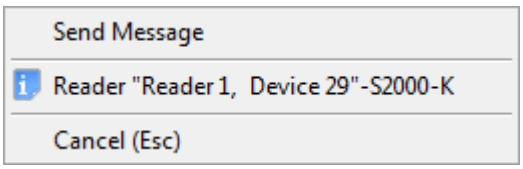
In the System Monitor, an operator can send a text message to the S2000-K device

To make this option available, add the icon of the S2000-K device or icon of a reader connected to the S2000-K device to the map.

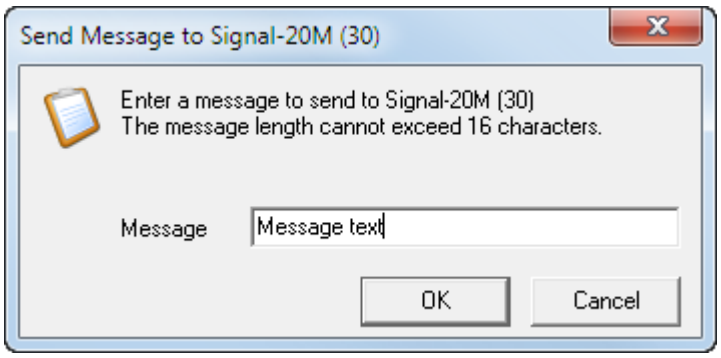
To send a text message to a S2000-K please right click the icon of the S2000-K on the map and select the **Send Message** item in the appeared menu:



Or right click the icon of a reader assigned to the S2000K keypad and select the **Send Message** item in the contextual menu:



The dialog box will appear. Please enter a text message and click the **OK** button:



Please note that the maximum message length cannot exceed 16 characters as it is the maximum number of characters of the LCD of a S2000-K keypad.

When sent, the message will be displayed on the S2000-K screen during 30 seconds

8.4 The Alarms Tab

To toggle the Alarms tab, please click the Alarm Handing button  or the <Alt+F1> short keys.

The Alarm Handling tab page offers the following functions:

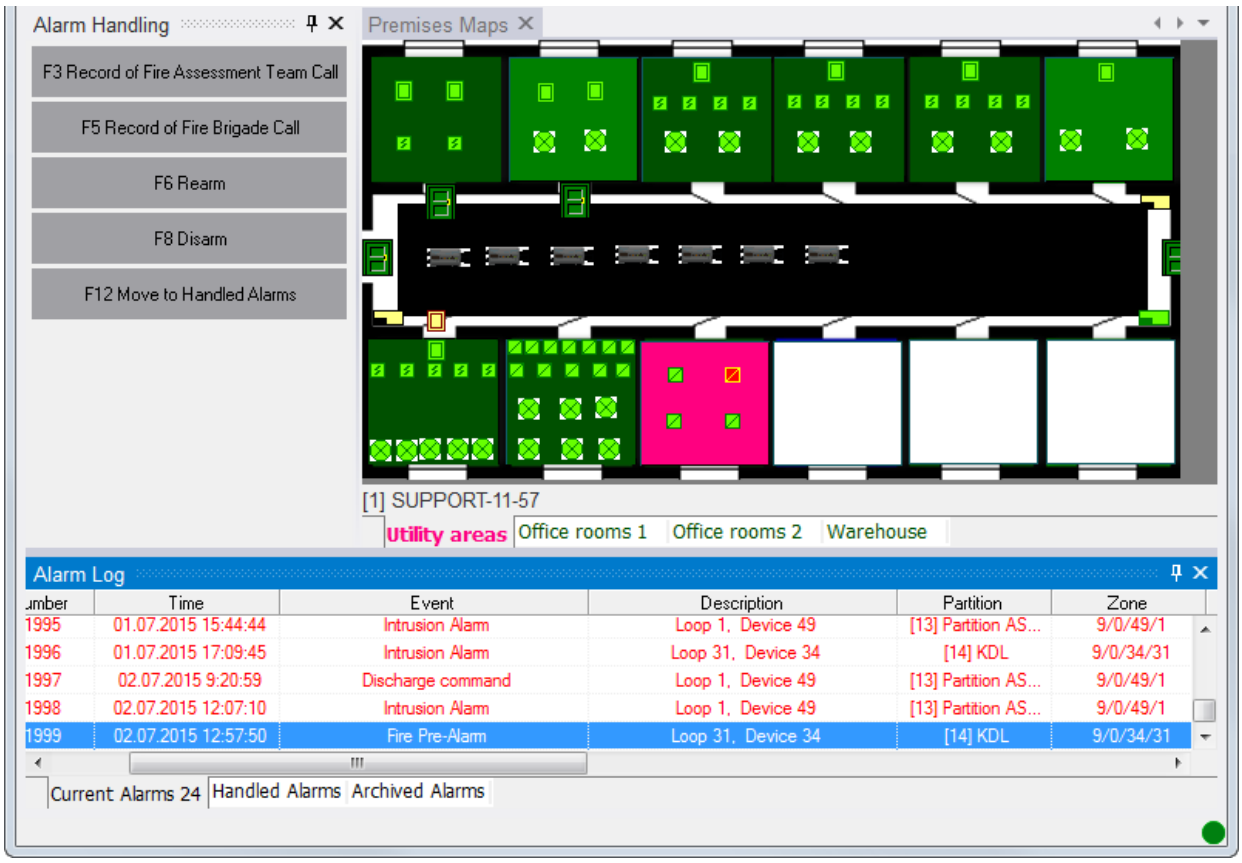
- Live display of alarms;
- Response to alarm events in real time
- Maintaining records of alarm causes and response actions;
- Viewing the archive of alarm events.

Also:

- Interactive graphics of system entity states on premises maps;
- Operator's interactive control of
  - zone
  - partitions
  - cameras
  - access points,
  - readers
- fire extinguishing
- Hot key launch of management scenarios
- Displaying a video archive window with cameras associated to an alarm event.

8.4.1 The Appearance of the Alarm Handling Tab

The figure shows the Alarm Handling tab page:



The System Monitor has a changeable view so the following should be recommended:

1. The recommended place of the Alarm Log pane is at the bottom of the tab page,
2. The following panes can be shown in any order and place:
    - Premises Maps
    - Alarm Handling

Interface, structure, and available functions of the premises maps on the Alarms tab page is the same as those of the premises maps displayed on the Management page (Refer to chapter 8.3.4 Premises Maps and Chapters 8.3.4.1-8.3.4.7.)

The Alarm Log pane shows the following tabs:

- Current Alarms
- Handled Alarms
- Archived Alarms

Where each of them includes:

- The Alarm Log
- Its own set of actions for the Alarm handling pane

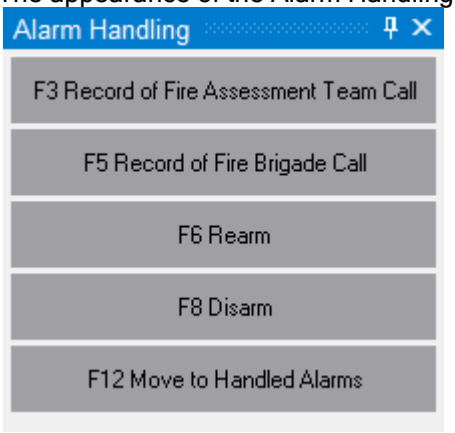
To toggle between tabs of the Alarm Log pane, please click the related tab buttons

: Current Alarms 19 | Handled Alarms 5 | Archived Alarms 2

- Current Alarms 19 – toggles the Current tab (to the right of the tab name (the actual number of current alarms is shown)
- Handled Alarms 5 –toggles the Alarm Handling
- Archived Alarms 2 – toggles the Archive Alarms

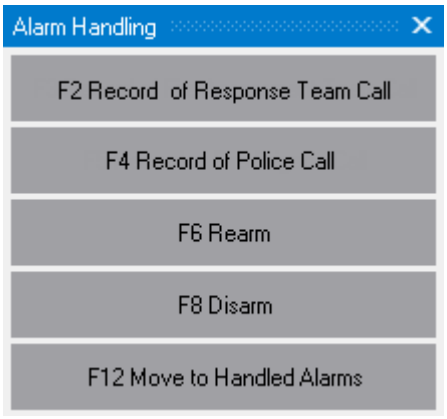
8.4.2 the Alarm Handling pane

The appearance of the Alarm Handling pane:



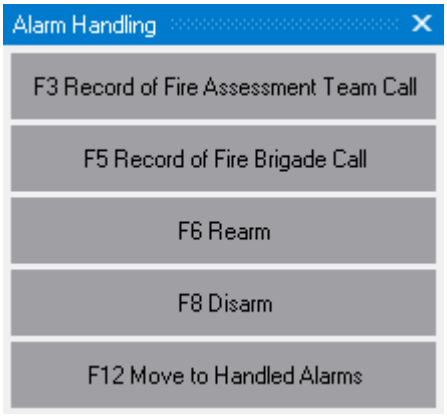
The available actions depend on what tab of the Alarm Log is selected:

- If the **Current Alarms** tab is active:
  - For the alarm event related to the intrusion part of the system:



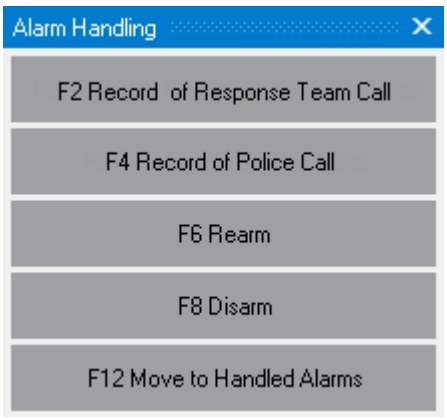
(*See Chapter 8.4.3.1 Handling Intrusion Alarms*)

  - For the alarms of the fire protection part of the system:



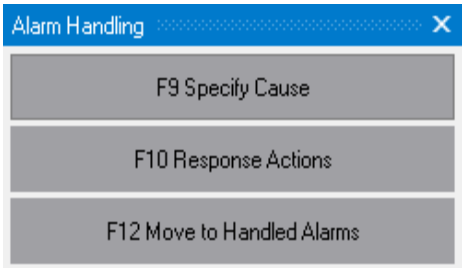
(See Chapter *8.4.3.2 Handling Fire Alarms*)

  - For the alarm event of a system entity and other events :



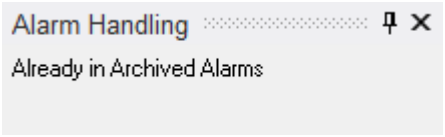
(See Chapter 8.4.3.3 Handling Access Alarms and Other Alarms)

In the **Handled Alarms** tab is active:



(See Chapter *8.4.4 The **Handled Alarm** Tab)*

- In the **Archived Alarms** Tab:



8.4.3 The Current Alarms Tab

If the **Handle Alarms** and **Handle Remote Alarms** options are selected in the DBA for the workstation where the System Monitor is running, an alarm event in the system will result in the following:

1. Switching the Current Alarms tabs of the Alarm Log pane on the Alarms tab page
2. Playing voice notification (if the Voice notification option is select in the DBA for the workstation where the System Monitor is running (Refer to Chapter 6.2.2 The Workstation Entity))
3. Toggling the map of premises where alarmed entity is located; the alarmed entity will start flashing
4. Adding the occurred alarm events

The alarm event is deemed as a current event till it is moved to the handled alarm events.

Attention! *Appendix 8. B System Events* explains what system events is regarded like alarms

The Alarm Log of the Current Alarms tab has the following structure:

Filed	Description
Workstation	The name of a workstation where occurred.
Number (ID)	The sequence number of an alarm event at workstation where the events occurred

Time	The data and time of an event
Event	The name of an alarm event
Partition	if occurred alarm relates to (i) a zone or camera; (ii) access control, this field displays: - (i) the number of a partition where these zones belongs - (ii) This field includes a number of an access point.
Description	Description of an entity where the event occurred
Zone	If an alarm comes from: - a zone, the zone name will be added to this field, - a camera, the camera name will be added to this field - a device, a device address will added to this field
Action 1	This field is used to add : Record of Fire Assessment Team (in case of fire alarms), or : Record of Response Team Dispatch (in case of intrusion alarms)
Time 1	Time of adding a record to the **Action 1** field
Operator 1	The name of an SM operator who has added a record in the **Action 1** field
Action 2	This field is used to add: Record of a fire brigade call (in case of fire alarms), or Record of a Police Call (in case of intrusion alarms)
Time 2	Time of adding a record to the **Action 2** field
Operator 2	The name of an SM operator who added a record in the **Action 2** field
Disarming/Rearming Action	If after a zone alarm, the zone is disarmed or rearmed on the Alarm Handling pane, the Disarming or Rearming action event will be added to this field.
Disarming/Rearming Time	Time of Disarming/Rearming Action
Operator	the operator name who has taken a disarming/arming action

No records are added to the other fields (Cause, Cause Logged Time, Operator, Response Action, Alarm Clear, Clear Time and Operator), and they are not displayed).

8.4.3.1 Handling Intrusion Alarms

The actions taken in response to intrusion alarms can be as follows:

1. Record of Response Team Dispatch
2. Record of Police Call
3. Rearming
4. Disarming
5. Moving an alarm events to the Handled Alarms
6. Moving all alarm events to the Handled Alarms.
7. Opening the video archive with assigned cameras

8.4.3.1.1 Record of Response Team Dispatch

To add a record of Response Team Dispatch, please select a required alarm in the Alarm Log by clicking an alarm event row, and then do one of the following actions:

- Press the <**F2**> key
- Click the 

on the Alarm Handling pane
- Right click an alarm event row to open the contextual menu. Select the **Record of Response Team Dispatch** item:

When one of the above actions is performed, the **Response Team Call** event will be added to the **Action 1 field**, the timestamp of this action will be added to the **Time 1** field, and the name of an operator responsible for this record will be added to the **Operator** 1 field in the current alarm row:

Action 1	Time 1	Operator 1
Response Team Call	02.07.2015 16:3...	Smith J.K.

8.4.3.1.2 Record of Police Call

To add the Record of Police Call, please select a required alarm in the Alarm Log by clicking an alarm event row, and then do one of the following actions:

- Press the <F4> key
- Click the 

button (Record of Police Call) on the Alarm Handling toolbox
- Right click an alarm event row to open the contextual menu. Select the **Record of Police Call** item:

After performing one of the above actions, the following will be added to an alarm row of the Alarm Log: the **Police Call** event will be added to the **Action 2** field, the date and time of logging this record will be added to the **Time 2** field, the name of an operator responsible for this record will be added to the **Operator 2**:

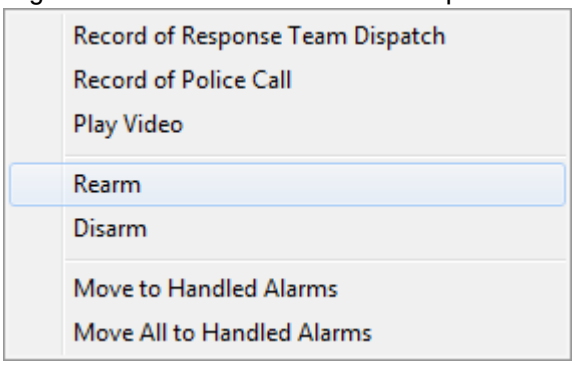
Action 2	Time 2	Operator 2
Police Call	02.07.2015 16:4...	Smith J.K.

8.4.3.1.3 Rearming an Entity

To rearm an entity where an alarm occurred, please select a required alarm in the Alarm Log to do one of the following actions:

- Press the <F6> key,
- Click the 

button on the Alarm Handling toolbox,
- Right click an alarm event line to open the contextual menu. Select the **Rearm** action item:



After performing one of the above actions, the following will be added to an alarm row of the Alarm Log, the **Rearming** event will be added to the **Disarming/Rearming Action** field, the date and time of logging this record will be added to the **Disarming/Rearming Time** field, the name of an operator responsible for rearming will be added to the **Operator** field:

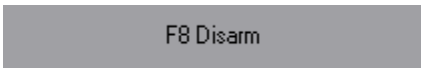
Arming/Disarming Action	Arming/Disarming Time	Operator
Rearm	02.07.2015 15:00:30	Smith J.K.

Rearming will be attempted.

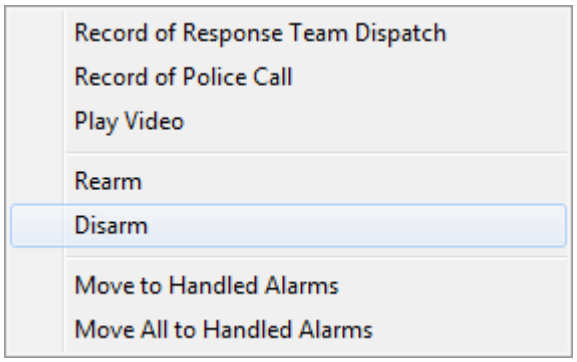
*Attention! We highly recommend that you should not use premises maps to rearm an alarmed entity as in this case the **Disarming/Rearming Action**, **Disarming/Rearming Time**, and **Operator** fields will remain empty. We recommend that you should use the above mentioned hot keys, action buttons, and contextual menu for arming purposes.*

8.4.3.1.4 Disarming an Entity

To disarm an entity where an alarm occurred, please select a required alarm event in the Alarm Log by clicking a required alarm row, and then do one of the following actions:

- Press the <F8> key
- Click the 

button on the Alarm Handling pane
- Right click an alarm event line to open the contextual menu. Select the **Disarm** action item:



After performing one of the above actions, the following will be added to the alarm event row: the **Disarming** event will be added to the **Disarming/Rearming Action field**, the date and time of this record will

be added to the Disarming/**Rearming Time** field, and the name of an operator responsible for rearming will be added to the **Operator** field:

Arming/Disarming Action	Arming/Disarming Time	Operator
Disarming	03.07.2015 11:59:31	Smith J.K.

The entity will be disarmed.

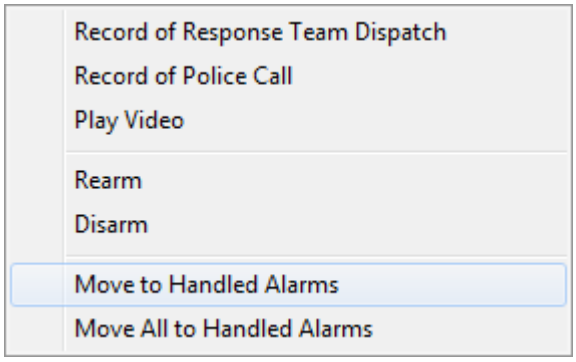
*Attention! We highly recommend you not to use premises maps to disarm an alarmed entity, as in this case the **Disarming/Rearming Action**, **Disarming/Rearming Time**, and **Operator** fields will remain empty. We recommend that you should use the above mentioned hot keys, action buttons, and contextual menu for disarming purposes.*

8.4.3.1.5 Moving an Alarm Event to the Handled Alarms

To move an alarm event to the Handled Alarms category, please select an alarm event by clicking an alarm event row in the Alarm Log, and then do one of the following actions:

- Press the <F2> key
- Click the 

button on the Alarm Handling toolbox,
- Right click an alarm event row to open the contextual menu. Select the **Move to Handled Alarms** action:



After performing one of the above actions, the **alarm** event will be moved to the **Handled Alarms** tab, and the following will be added to the alarm row of the Alarm Log, the **Clear** event will be added to the **Alarm Clear** field, and the date and time of moving this alarm will be added to the **Alarm Clear Time** field, the name of an operator responsible for moving (clearing) the alarm to the Handled Alarms category will be added to the **Operator** field:

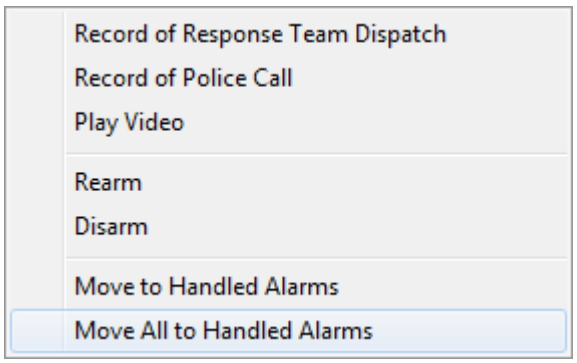
Alarm Clear	Alarm Clear Time	Operator
Clear	03.07.2015 12:0...	Smith J.K.

See Chapter 8.4.4 The Handled Alarm Tab.

Attention! After moving an alarm event to the Handled Alarms tab, the following action items are not available: Record of Response Team Dispatch, Record of Police Call, Rearm, and Disarm

8.4.3.1.6 Moving All Current Alarms to the Handled Alarms Tab

To move all alarm events to the Handled Alarms tab, please right click any alarm event in the Alarm Log and select the **Move All to Handled Alarms** action item in the appeared menu:



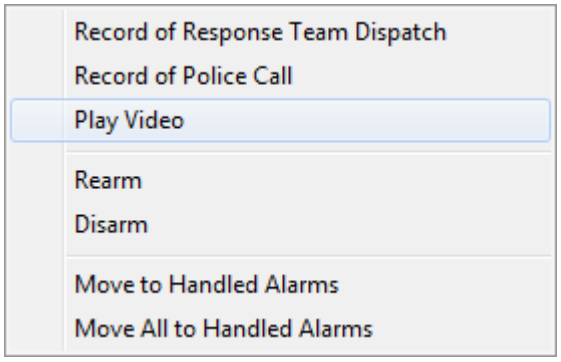
After doing that, all alarm events will be moved from the Current Alarms tab to the Handled Alarms tab, and the following will be added to each alarm row, the **Clear** events will be added to the **Alarm Clear** field for each alarm event, and the date and time of moving this alarm will be added to the **Alarm Clear Time** field of each alarm event, as well as the name of an operator responsible for moving (clearing) all current alarms to the Handled Alarms tab will be added to the **Operator** field for each alarm event:

(See Chapter 8.4.4 The Handled Alarm Tab).

Attention! After moving an alarm event to the Handled Alarm tab, the following actions are not available: Record of Response Team Dispatch, Record of Police Call, Rearm, and Disarm

8.4.3.1.7 Opening Video Archive with Entity-Associated Cameras

To open the video archive with entity-associate cameras, please select and right click an alarm event in the Alarm Log to open the contextual menu, and then select and **Play Video**:



The above actions will open the video archive with the list of cameras, where entity-associated cameras will be added (if there is space) to play back recordings (See Chapter 8.5.2 Video Archive).

8.4.3.2 Handling Fire Alarms

The actions taken for fire alarms can be as follows:

1. Record of Fire Assessment Initiation
2. Record of Fire Brigade Call
3. Rearming
4. Disarming
5. Moving an alarm events to the Handled Alarms
6. Moving all alarm events to the Handled Alarms.
7. Opening the video archive with assigned cameras

8.4.3.2.1 Record of Fire Assessment Team Dispatched

To add a record of a fire assessment team dispatch, please select a required alarm in the Alarm Log by clicking the alarm event line, and then do one of the following:

- Press <F3> key
- Click the 

button on the Alarm Handling toolbox
- Right click an alarm event line to open the contextual menu. Select **Record of Fire Assessment Initiation** :

After performing one of the above actions, the following will be added for the fire alarm event, the **Fire Assessment** event will be added to the **Action 1**, and the timestamp of logging this record will be added to the **Time 1** field, and the name of an operator responsible for this record will be added to the **Operator**1 field:

Action 1	Time 1	Operator 1
Fire Assessment	03.07.2015 12:5...	Smith J.K.

8.4.3.2.2 Record of Fire Brigade Call

To add the Record of Fire Brigade Call, please select a required alarm in the Alarm Log by clicking the alarm event line, and then do one of the following actions:

- Press the <F5> key
- Click the 

button on the Alarm Handling pane
- Right click an alarm event line to open the contextual menu. Select the **Record of Fire Brigade Call** item:

After performing one of the above actions, the following will be added to the alarm event row: the **Fire Brigade Call** event will be added to the **Action 2** field, the date and time of logging this record will be added to the **Time 2** field, and the name of an operator responsible for this record will be added to the **Operator 2** field:

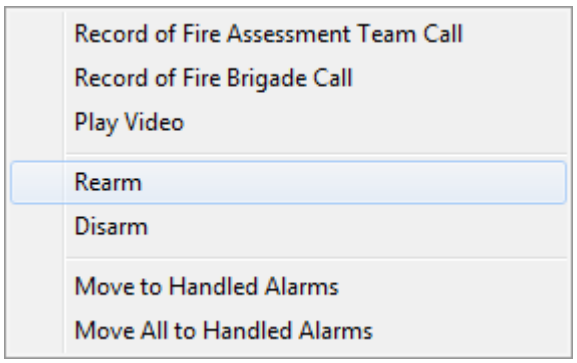
Action 2	Time 2	Operator 2
Fire Brigade Call	03.07.2015 14:1...	Smith J.K.

8.4.3.2.3 Rearming an Entity

To rearm an entity where an alarm occurred, please select a required alarm in the Alarm Log by clicking a required alarm row, and then do one of the following actions:

- Press the <F6> ley,
- Click the 

button on the Alarm Handling toolbox,
- Right click an alarm event row to open the contextual menu. Select **Rearm:**



After performing one of the above actions, the **Rearming** event will be added to the **Disarming/Rearming Action** field, the date and time of logging this record will be added to the **Disarming/Rearming Time** field, the name of an operator responsible for rearming will be added to the **Operator** field:

Arming/Disarming Action	Arming/Disarming Time	Operator
Rearming	03.07.2015 14:19:50	Smith J.K.

Rearming an entity will be attempted.

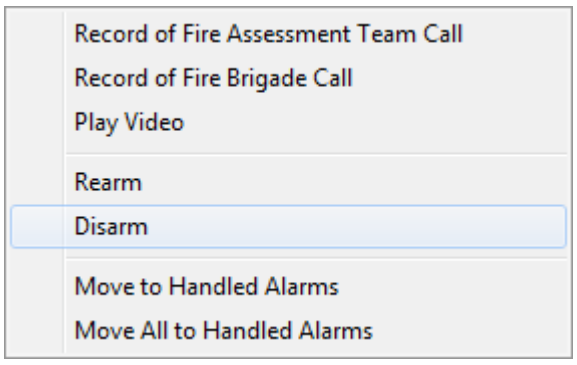
*Attention! We highly recommend that you should not use premises maps to rearm an alarmed entity as in this case the **Disarming/Rearming Action**, **Disarming/Rearming Time**, and **Operator** fields will remain empty. We recommend that you should use the above mentioned hot keys, action buttons, and contextual menu for arming purposes.*

8.4.3.2.4 Disarming an Entity

To disarm an entity where an alarm occurred, please select a required alarm event in the Alarm Log by clicking the row of a required alarm, and then do one of the following actions:

- Press the <F8> key
- Click the 

button on the Alarm Handling toolbox
- Right click an alarm event row to open the contextual menu. Select the **Disarm** action item:



After performing one of the above actions, the following will be added to the alarm row: the **Disarming** event will be added to the **Disarming/Rearming Action field**; the date and time of logging will be added to the **Disarming/Rearming Time** field, and the name of an operator responsible for rearming will be added to the **Operator** field:

Arming/Disarming Action	Arming/Disarming Time	Operator
Disarming	03.07.2015 14:22:08	Smith J.K.

The entity will be disarmed.

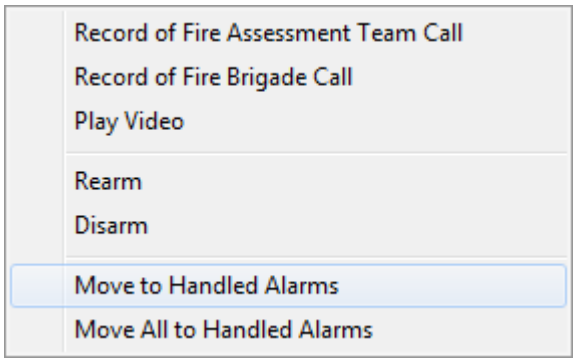
*Attention! We highly recommend you not to use premises maps to disarm an alarmed entity, as in this case the **Disarming/Rearming Action**, **Disarming/Rearming Time**, and **Operator** fields will remain empty. We recommend that you should use the above mentioned hot keys, action buttons, and contextual menu for disarming purposes.*

8.4.3.2.5 Moving an Alarm Events to the Handled Alarms Tab

To move an alarm event to the Handled Alarms category, please select an alarm event by clicking an alarm event row in the Alarm Log, and then perform one of the following:

- Press the <**F12**> key
- Click 

on the Alarm Handling toolbox
- Right click an alarm event row to open the contextual menu. Select the **Move to Handled Alarms** action:



After performing one of the above actions, the **alarm** event will be moved to the **Handled Alarm** toolbox, the **Clear** event will be added to the **Alarm Clear** field, the date and time of moving this alarm will be added to the **Alarm Clear Time** field, and the name of an operator responsible for moving (clearing) the alarm to the Handled Alarms category will be added to the **Operator** field:

Alarm Clear	Alarm Clear Time	Operator
Clear	03.07.2015 12:5...	Smith J.K.

See Chapter 8.4.4 The Handled Alarm Tab.

Attention! After moving an alarm event to the Handle Alarm tab, the following actions are not available: Record of Fire Assessment Team Dispatch, Record of Fire Brigade Call, Rearm, and Disarm

8.4.3.2.6 Moving All Current Alarms to the Handled Alarms Tab

To move all alarm events to the Handled Alarms pane, please right click any alarm event in the Alarm Log and select the **Move All to Handled Alarms** action item in the appeared menu:

After doing that, all alarm events will be moved from the Current Alarms tab to the Handled Alarms tab, the following will be added for each alarm event: **Clear** events will be added to the **Alarm Clear** field, the date and time of alarm moving will be added to the **Alarm Clear Time** field, as well as the name of an operator responsible for moving (clearing) all current alarms to the Handled Alarms tab will be added to the **Operator** field:

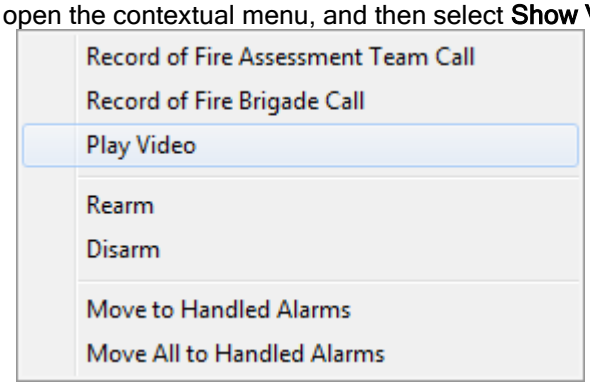
Alarm Clear	Alarm Clear Time	Operator
Clear	03.07.2015 12:5...	Smith J.K.

(Chapter 8.4.4 The Handled Alarms.

Attention! After moving an alarm event to the Handled Alarm tab, the following actions are not available: Record of Fire Assessment Team Dispatch, Record of Fire Brigade Call, Rearm, and Disarm

8.4.3.2.7 Opening Video Archive with Entity-Associated Cameras

To open the video archive with entity-associate cameras, please right click an alarm event in the Alarm Log to open the contextual menu, and then select **Show Video**:



The above actions will open video archive with the list of cameras, where entity-associated cameras will be added (if there is room enough) to play back this camera records (See Chapter 8.5.2 Video Archive).

8.4.3.3 Handling Access -Related and Other Alarms

The actions available for an operator to respond to the access control and intrusion alarms are as follows:

1. Record of Response Team Dispatch
2. Record of Police Call
3. Moving an alarm events to the Handled Alarms
4. Moving all alarm events to the Handled Alarms.
5. Opening the video archive with assigned cameras

8.4.3.3.1 Record of Response Team Dispatch

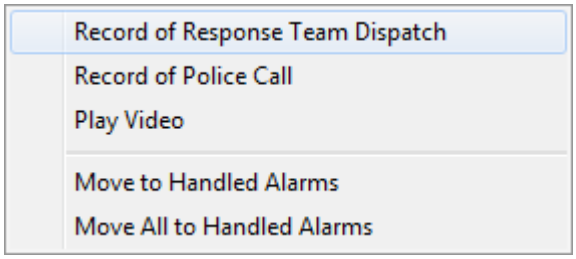
To add a record of Response Team Dispatch, please select a required alarm in the Alarm Log, and then do one of the following:

- Press the <**F2**> key

- Click 

on the Alarm Handling toolbox

- Right click the alarm event to open the contextual menu. Select the **Record of Response Team Dispatch** item:



After performing one of the above actions, the **Response Team Call** event will be added to the **Action 1 field**, the date and time of his record will be added to the **Time 1** field, the name of an operator responsible for this record will be added to the **Operator** 1 field:

Action 1	Time 1	Operator 1
Response Team Call	02.07.2015 16:3...	Smith J.K.

8.4.3.3.2 Record of Police Call

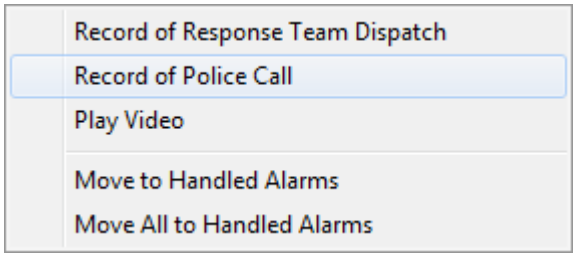
To add the Record of Police Call, please select a required alarm in the Alarm Log, and then do one of the following:

- Press the <F4> key

- Click 

(Record of Police Call) on the Alarm Handling toolbox

- Right click an alarm event row to open the contextual menu. Select the **Record of Police Call** item:



After performing one of the above, the following will be added for the alarm event: the **Police Call** event will be added to the **Action 2** field, the date and time this record will be added to the **Time 2** field, and the name of a responsible operator will be added to the **Operator 2** field:

Action 2	Time 2	Operator 2
Police Call	03.07.2015 15:0...	Smith J.K.

8.4.3.3.3 Moving an Alarm Event to the Handled Alarms

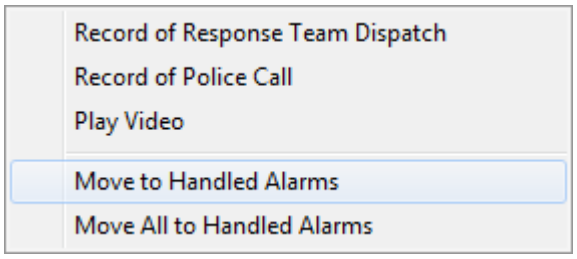
To move an alarm event to the Handled Alarms category, please select an alarm event by clicking an alarm event in the Alarm Log, and then do one of the following actions:

- Press the <F2> key

- Click 

on the Alarm Handling toolbox,

- Right click an alarm event to open the contextual menu. Select the **Move to Handled Alarms** action:



After performing one of the above, the **alarm** event will be moved to the **Handled Alarm** tab, and the following will be added for the alarm in the Alarm Log: the **Clear** event will be added to the **Alarm Clear** field, the date and time of alarm moving will be added to the **Alarm Clear Time** field, and the name of an operator responsible for moving (clearing) the alarm to the Handled Alarms category will be added to the **Operator** field:

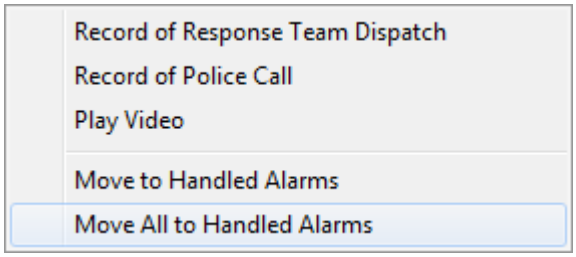
Alarm Clear	Alarm Clear Time	Operator
Clear	03.07.2015 12:5...	Smith J.K.

See Chapter 8.4.4 The Handled Alarm Tab.

Attention! After moving an alarm event to the Handle Alarm tab, the following action items are not available: Record of Response Team Dispatch, Record of Police Call, Rearm, and Disarm

8.4.3.3.4 Moving All Current Alarms to the Handled Alarms Tab

To move all alarm events to the Handled Alarms tab, please right click any alarm event in the Alarm Log and select **Move All to Handled Alarms** in the appeared menu:



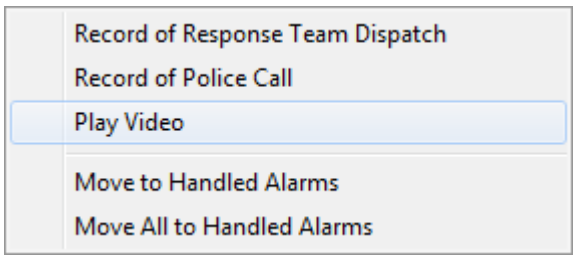
After doing that, all alarm events will be moved from the Current Alarms tab to Handled Alarms, and the following will be added for each event: the **Clear** event will be added to the Alarm Clear field and the date and time of alarm moving will be added to the **Alarm Clear Time** field, as well as the name of an operator responsible for moving (clearing) all current alarms to the Handled Alarms tab will be added to the Operator field for each alarm event:

Alarm Clear	Alarm Clear Time	Operator
Clear	03.07.2015 12:5...	Smith J.K.

Attention! After moving an alarm event to the Handled Alarm tab, the following actions are not available: Record of Response Team Dispatch and Record of Police Call

8.4.3.3.5 Opening Video Archive with Entity-Associated Cameras

To open the video archive with entity-associate cameras, please select and right click an alarm event in the Alarm Log to open the contextual menu, and then select and **Play Video**:



The above actions will open video archive with the list of cameras, where entity-associated cameras will be added (if there is space) to play back records (See Chapter 8.5.2 Video Archive).

8.4.4 The Handled Alarms

Movement of an alarm event to the Handled Alarms results in the followings:

1. The alarm event is moved to the Handled Alarms, and the following will be added to the alarm event row of the Alarm Log: the **Clear** event will be added to the **Alarm Clear** field, and the date and time of moving this alarm will be added to the **Alarm Clear Time** field, the name of an operator responsible for moving the alarm to the Handled Alarms category will be added to the **Operator** field:

Alarm Clear	Alarm Clear Time	Operator
Clear	03.07.2015 12:5...	Smith J.K.

2. Now, the alarm event is considered as the handled one.

It will be considered as a handled alarm till it is moved to the Archived Alarms category (tab)

The Alarm Log of the Handled Alarm tab has the following structures (the fields remaining empty on the Current Alarms tab have bold texts:

Field	Purpose
Workstation	The name of a workstation where an alarm occurred.
Number	A record number of an alarm received by a workstation
Time	Data and time of an event
Event	The name of an alarm event
Partition	if occurred alarm relates to (i) a zone or (ii) camera : -(i) Number of the partition where this zones belongs to will be specified - (ii) Number of an access point associated with a camera.
Description	Description of an entity where the event occurred
Cause	This field is used to specify the cause of an alarm occurred.
Cause Logging Time	This field is used to specify the time of logging the cause of an alarm occurred
Operator	The name of an SM operator specified the cause of an alarm occurred.
Response Action	This field is used to specify a response action to an alarm occurred.
Action Logging Time	This field is used to specify a time of logging the response action to an alarm
Operator	The name of an SM operator who specified a response action to an alarm occurred.
Zone	If an alarm comes from: - a zone, the zone name will be added to this field, - a camera, the camera name will be added to this field

	- a device, a device address will be added to this field
Action 1	This field is used to add : Record of Fire Assessment Team (in case of fire alarms), or : Record of Response Team Dispatch (in case of intrusion alarms)
Time 1	Time of adding a record to the **Action 1** field
Operator 1	The name of an SM operator who has added a record in the **Action 1** field
Action 2	This field is used to add: Record of a fire brigade call (in case of fire alarms), or Record of a police team call (in case of intrusion alarms)
Time 2	Time of adding a record to the **Action 2** field
Operator 2	The name of an SM operator who added a record in the **Action 2** field
Disarming/Rearming Action	If after a alarm, a zone is disarmed/rearmed on the Alarm Handling pane of the Alarms tab page, the Disarming or Rearming action event will be added to this field.
Disarming/Rearming Time	Time when the zone was disarmed or rearmed.
Operator	The name of an operator responsible for disarming/rearming.
Alarm Clear	This field is used to add the **Clear** event
Alarm Clear Time	This field is used to specify the time of alarm clearing, i.e. movement of an alarm from the Current Alarms tab to the Handled Alarms tab
Operator	The name of an operator who cleared an alarm (moved an alarm to the **Handled Alarms** category.

The actions available for the handled alarms are as follows:

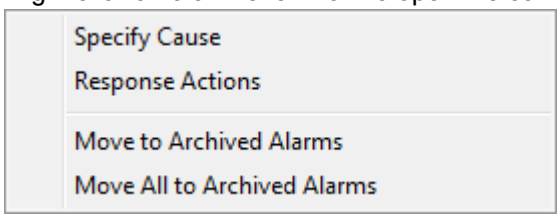
1. Specifying the cause of an occurred alarm event,
2. Specifying the action taken as a response to an alarm event
3. Moving an alarm event to the Archived Alarms category
4. Moving all alarm events to the Archived Alarms category

8.4.4.1 Specifying a Cause of Alarm Event

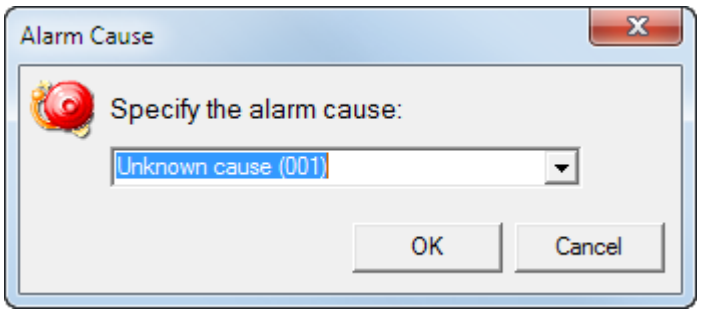
To specify the cause of an alarm event, please select a required alarm in the Alarm Log by clicking an alarm event row, and then do one of the following actions:

- Press the <F9> Key
- Click the Specify Cause 

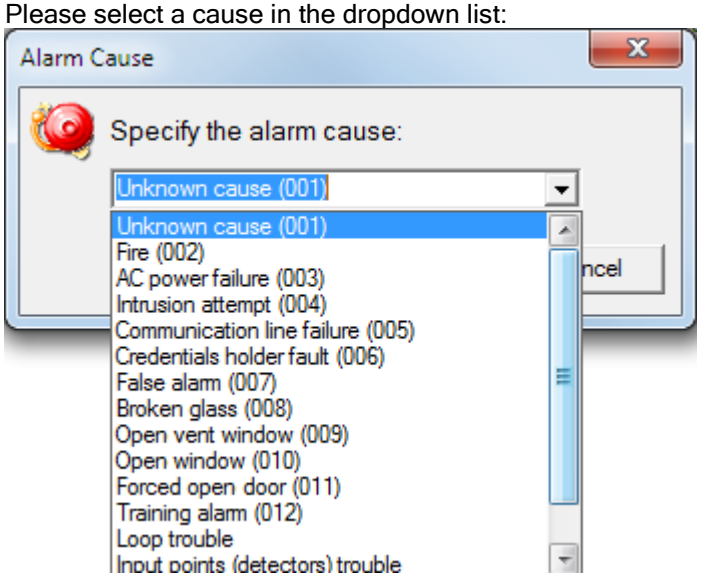
- Right click an alarm event row to open the contextual menu. Select the **Specify Cause**:



After one of the above actions, the Alarm Cause dialog box will appear:



Please select a cause in the dropdown list:



Or type a new custom cause:

Click the **Ok** button.

Note that the maximum length of an alarm cause description is 25 characters

*In this case, a selected or typed cause will be added in the **Cause** field of an alarm row, the data and time of logging the cause will be added to the Cause Logging Time field of this alarm event; the name of operator responsible for specifying this cause will be added to Operator field of the log:*

Cause	Cause Logging Time	Operator
Example of custom cause	06.07.2015 11:46:17	Smith J.K.

Please keep in mind that the new entered cause will be available in the default list of alarm causes

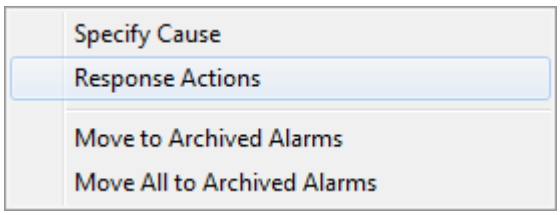
All causes (default and new) are stored in the reasons.ls file located in the Data folder located in the folder with installed Orion Pro Suite

8.4.4.2 Specifying Response Actions

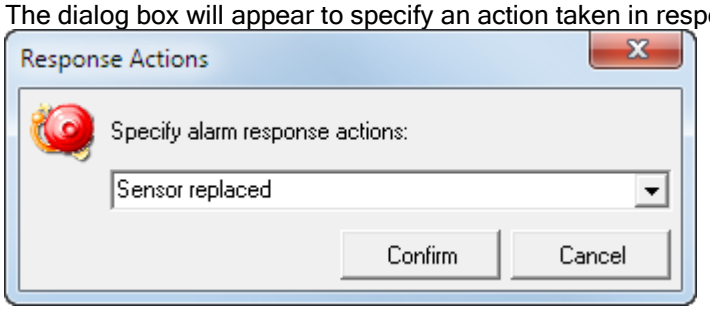
To specify an alarm response action, please select a required alarm in the Alarm Log by clicking an alarm event row, and then do one of the following actions:

- Press the <F10> key
- Click 

- Right click an alarm event row to open the contextual menu. Select the **Response Actions** item

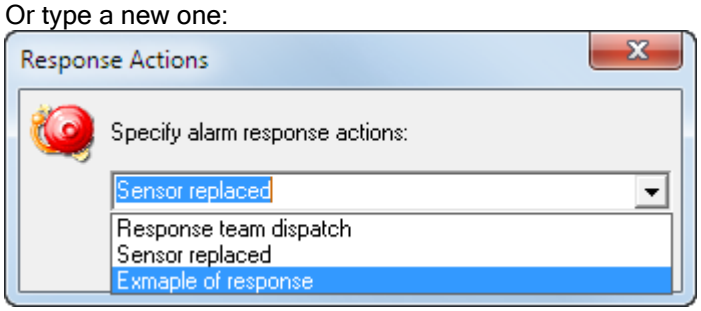


The dialog box will appear to specify an action taken in response to an occurred alarm event:



Please select a response action taken from the dropdown list:

Or type a new one:



And click the OK button.

Note that the maximum length of an alarm cause description is 25 characters

*In this case, a selected or typed cause will be added in the **Response Action** field of an alarm row, the data and time of logging a response action will be added to the **Action Logging Time** field of this alarm event; the name of operator responsible for specifying this action taken will be added to **Operator** field of the log:*

Response Action	Action Logging ...	Operator
Response team dispatch	06.07.2015 12:0...	Smith J.K.

Please keep in mind that if a new action is entered, it will be available in the default list of alarm response actions

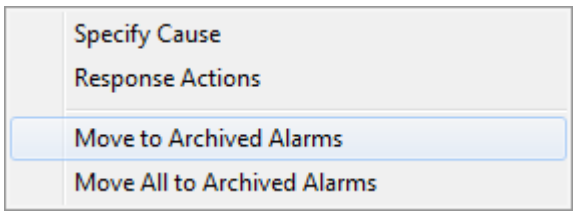
*All causes (default and new) are stored in the mesures.ls file located in the **Data** folder located in the folder with installed Orion Pro Suite. To edit actions, please open this file with a text editor.*

8.4.4.3 Moving an Alarm Event to the Archived Alarms Category

To move an alarm event to the Archived Alarms category, please select an alarm event by clicking an alarm event row in the Alarm Log, and then do one of the following:

- Press the <**F11**> key
- Click 

- Right click an alarm event row to open the contextual menu. Select the **Move to Archived Alarms** action:

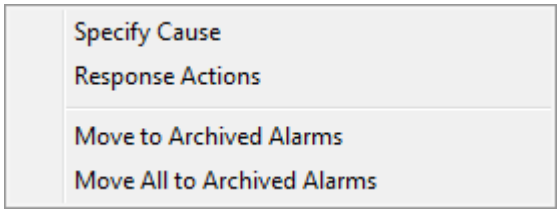


After performing one of the above actions, the **alarm** event will be moved to the **Archived Alarms** tab

Attention! After moving an alarm event to the Archived Alarms tab, the following action items are not available: Specify Alarm Cause, and Response Actions

8.4.4.4 Moving All Alarm to the Archived Alarms tab

To move all alarm events to the Handled Alarms tab, please right click any alarm event in the Alarm Log and select the **Move All to Archived Alarms** action item in the appeared menu:



After completing this, all alarm events will be moved from the Handled Alarms tab to the Archived Alarms tabs

Attention! After moving all alarm events to the Archived Alarms tab, the following actions are not available: Specify Alarm Cause, and Response Actions

8.4.5 The Archived Alarms Tab

When an operator moves an alarm event to the Archived Alarms it will result in the following:

1. An alarm event will be moved to the Archived Alarms tab

2. Now, this alarm event is considered as an archived one.

The Alarm Log of the Archived Alarms has the same structure as that of the Handled Alarm tab.
(See chapter *8.4.4 The Handled Alarms tab*)

The archived alarms can be viewed only; no other actions are available.

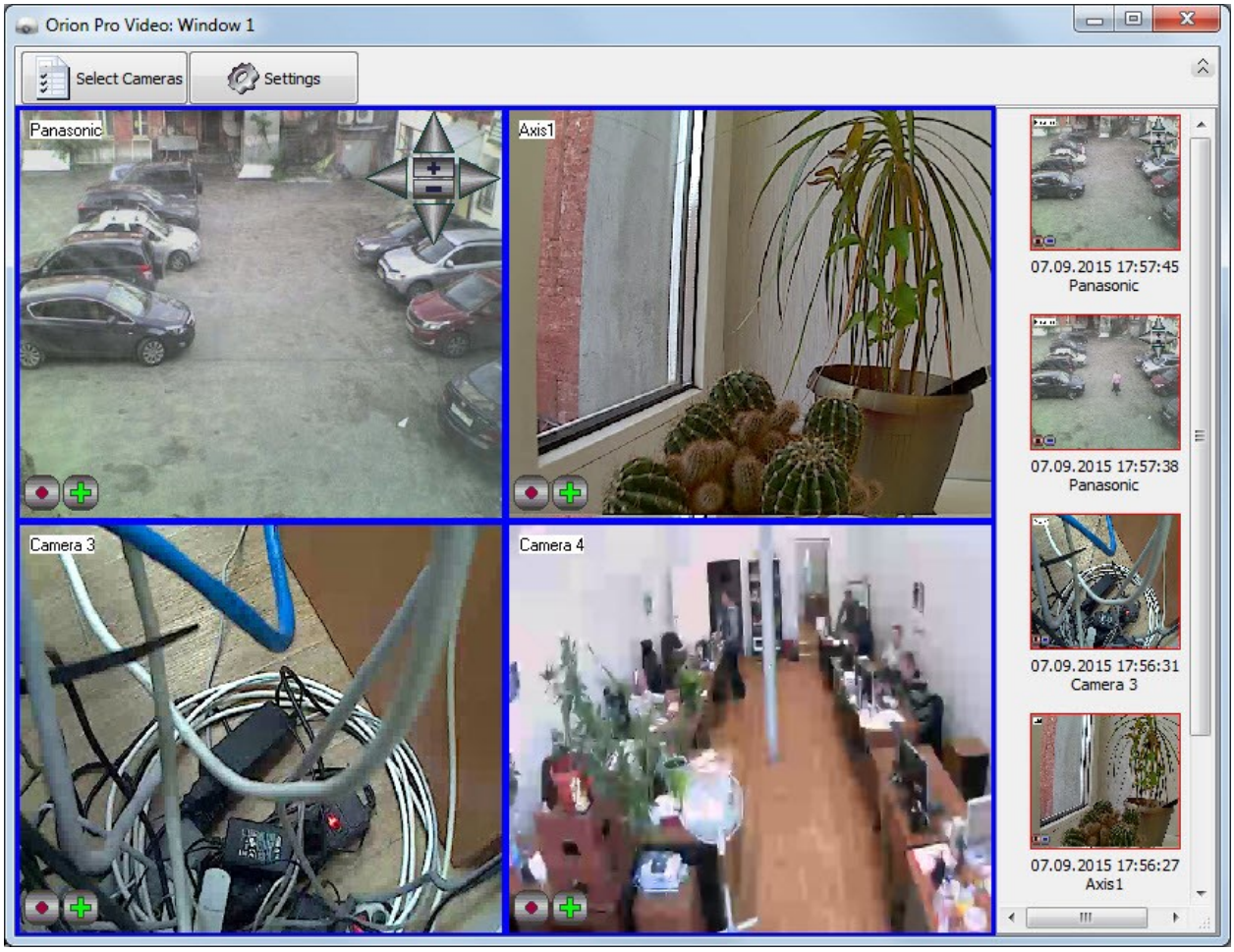
8.5 Orion Video

8.5.1 IP Video Monitor

If one clicks the  button or the <Alt+F7> key, the Video (IP Video Monitor) window will be displayed.

Please note that multiple IP Video Monitor windows can be opened to arrange their cameras in any odder as required

Visually, the IP Video Monitor is a segmented window with individual video image boxes that makes video viewing more friendly and provides control of multiple IP Cameras



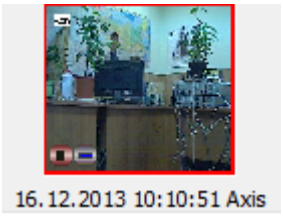
The number and arrangement of video image boxes are predefined and can be selected using preset buttons at the upper of the IP Video Monitor window:

It is an operator who assigned a camera video image to desirable video image box. Further, this chapter will discuss how to move cameras

Note that double click on one of the boxes, maximize this box over entire window area (on top of all other boxes). Usually it is required for a detailed review of a video recording.

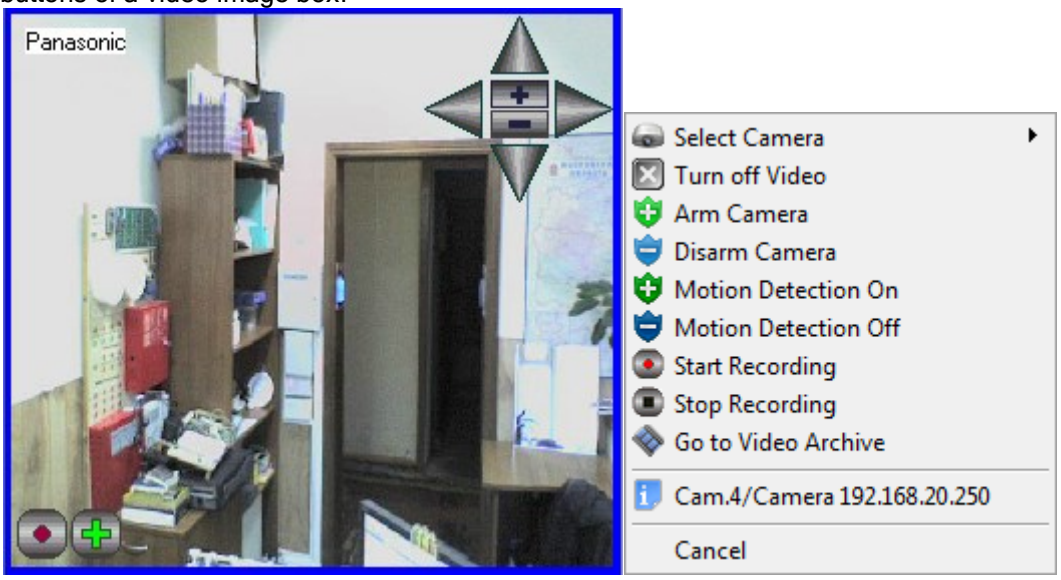
To return the original box size and show all boxes again, please double click the maximized box.

To the right of video boxes, one can see video frames captured from armed cameras at the moments of detection zone violations. The name of a camera as well as capture time and date are underneath each video frame.



The list of video images includes video images form all cameras of the IP Camera Monitor with the last event on top of the list.

Further, chapter discusses camera control actions accessible through the contextual menu or action buttons of a video image box.



Menu Item	Button	Actions
Select Camera		Selects a camera from the dropdown list of available cameras to show its video image in this box. In addition to video image, control items and action buttons will be available in the menu. The available actions depend on a camera model.
Turn off video (Отключить видео)		Turns off video image in this box. When a video box disconnected, all menu items and camera control buttons will not be available either, except for the Select Camera item
Arm Camera		Arms Camera. (The Arm Camera button is available only if a camera is disarmed)
Disarm Camera		Disarms Camera (The **Disarm Camera** button is available only if a camera is armed)
Motion Detection On		Enables Video Motion Detection
Motion Detection Off		Disables Video Motion Detection
Audio On		Mutes the audio (The **Audio On** button is accessible only when camera audio is turn off) (This menu item is displayed only for cameras that support audio)
Audio Off		Unmutes the audio of the camera (The **Audio Off** button is accessible only when camera audio is turn on) (This menu item is displayed only for cameras that support audio).
Start Recording		Starts recording (The **Start Recording** button is accessible only when the camera is not recording at the moment)
Stop Recording		Stops recording (The **Stop Recording** button is accessible only when the recording function is activated)

Pan/Tilt	-	Controls a camera in accordance with presets. The list of presents will be displayed in the dropdown list. (This menu item is available only for PTZ cameras *with presets in the Database)*
-		Tilt up (This button is available only for PTZ cameras)
-		Tilt down. (This button is available only for PTZ cameras)
-		Pan left (This button is available only for PTZ cameras)
-		Pan right (This button is available only for PTZ cameras)
-		Zoom In (This button is available only for PTZ cameras)
-		Zoom Out (This button is available only for PTZ cameras)
Go to Video Archive		Opens a video archive window where in the list of cameras only this camera will be available.

Note:
*If one selects **Play Video** in the contextual menu of Orion Video camera (on the Camera tab or premises map) it will open the window with video from the camera.*

All actions available in this box are the same as those available in the IP Cameras Monitor window .

8.5.2 Video Archive

Video Archive is individual application that is included in the Orion Pro Suite (VideoArchive.exe in the folder with installed Orion Pro)

The System Monitor provides multiple options to launch the Video Archive:

- The contextual menu of a camera on a premises map

- The contextual menu of cameras in the Cameras pane
- The contextual menu in a video image box of the Video Monitor window
- The contextual menu in the Alarm Log

In the first three cases, the list of cameras for record review, will include the camera used to go to the video archive (if the space allows)

In the last case, the list of cameras for record review will include the camera associated to the entity where an alarm triggered opening the video archive.

When the Video Archive window is closed, the list of cameras is cleared.

The appearance of the Video Archive window:

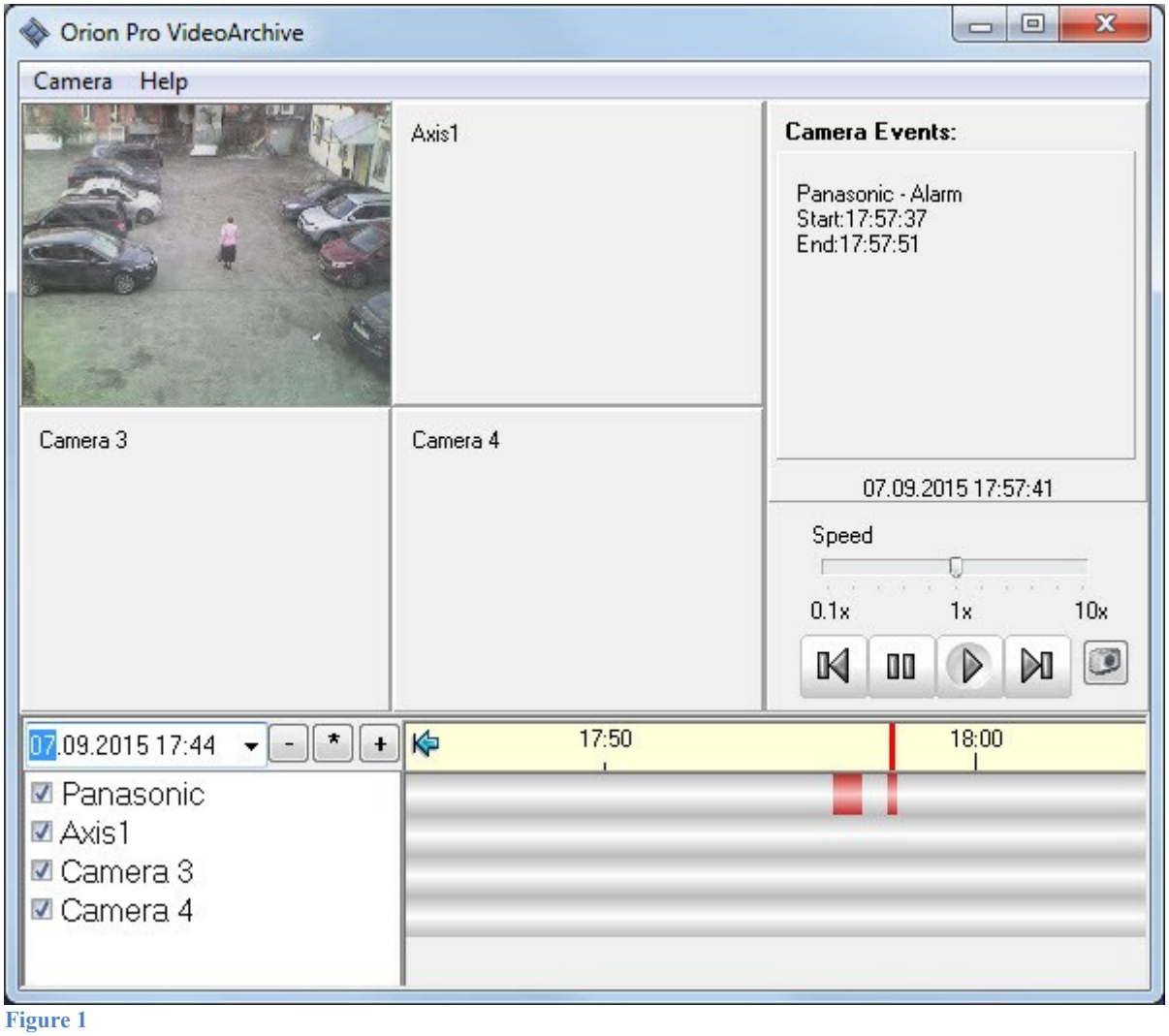
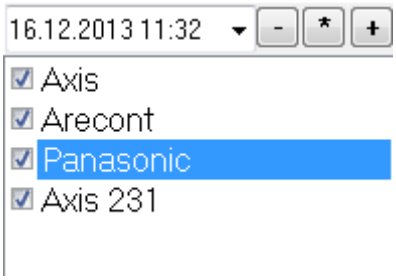


Figure 1

The layout of the Video Archive window may be divided into the functional areas:

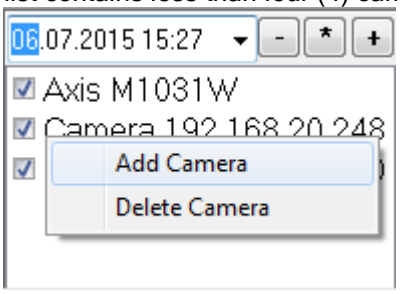
1. The list of cameras and selection field of data and time to assess video events:



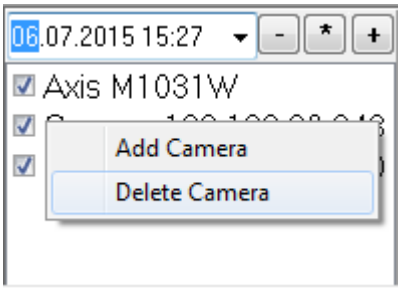
This area displays the list of camera recordings selectable for review. It can include up to four cameras.

If one unchecks a camera, the record timeline for this camera will disappear and no video recordings of this camera will be shown.

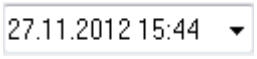
A camera can be added to the list of cameras with the help of the **Add Camera** menu item, if the list contains less than four (4) cameras.



The **Delete Camera** menu item is used to delete a camera from the list of cameras



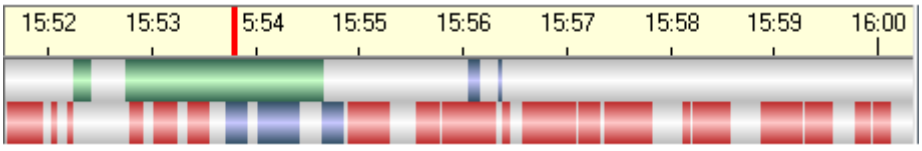
Also the area shows the starting date and time of video recordings



Using this button  you can select time range to load video recordings covering the selected period.

Timeline scale buttons:  and  .

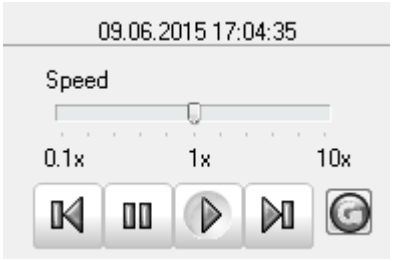
2. The timeline of video recordings. Video recordings are placed on the track of the timeline with each recording separated by time intervals.



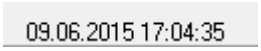
Video recordings can be of various colors:

- Alarm recording is red
- Detector-triggered recording is blue
- Operator-initiated recording – green
- Scenario –triggered recording is green
- External alarm recording is green

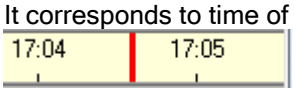
3. The Playback control buttons



The date and time of a current video recording (at the upper of the box):



It corresponds to time of the pointer on the timeline



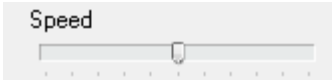
The  button is used to start playback

The  button is used to stop playback.

The  and  buttons are used to go the next and previous video images.

The right-most button  is used to refresh video archive window to display new added recordings without restarting the Video Archive module. If there are new records, they will be added to the timeline after clicking this button.

The speed slider is located above the control buttons

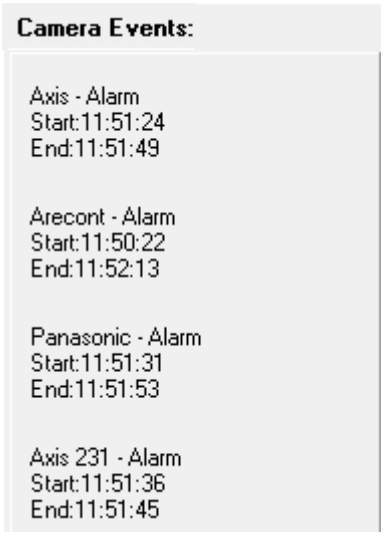


If needed, one can speed up playing a record for a convenient and brief review or to slow it down for a detailed review of events.

4. The Video recording box is a part of the Video Archive window where recorded video is displayed.

When moving within the timeline (manually or playing), the frames (if manually) or played video will be displayed in the relevant video image box if there are recordings related to the assessed time period (shown on the timeline and above the playback buttons)

5. Events arranged by cameras.

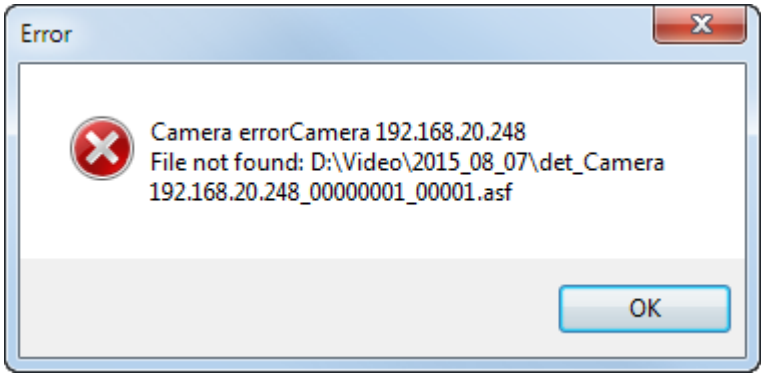


The list of camera events includes details of the recordings of cameras for the currently assessed period of time
It shows the following information for each event

- The name of a camera
- The trigger of recording video
- The data and time of capture start

- The data and time of capture end

Additional! When working with very old archived recordings, if free disk space is limited and the Video Cleaner service is running, the Video Archive may fail to find the desired file, as it might have been deleted by an appropriate service. In this case, the application will generate the following message:



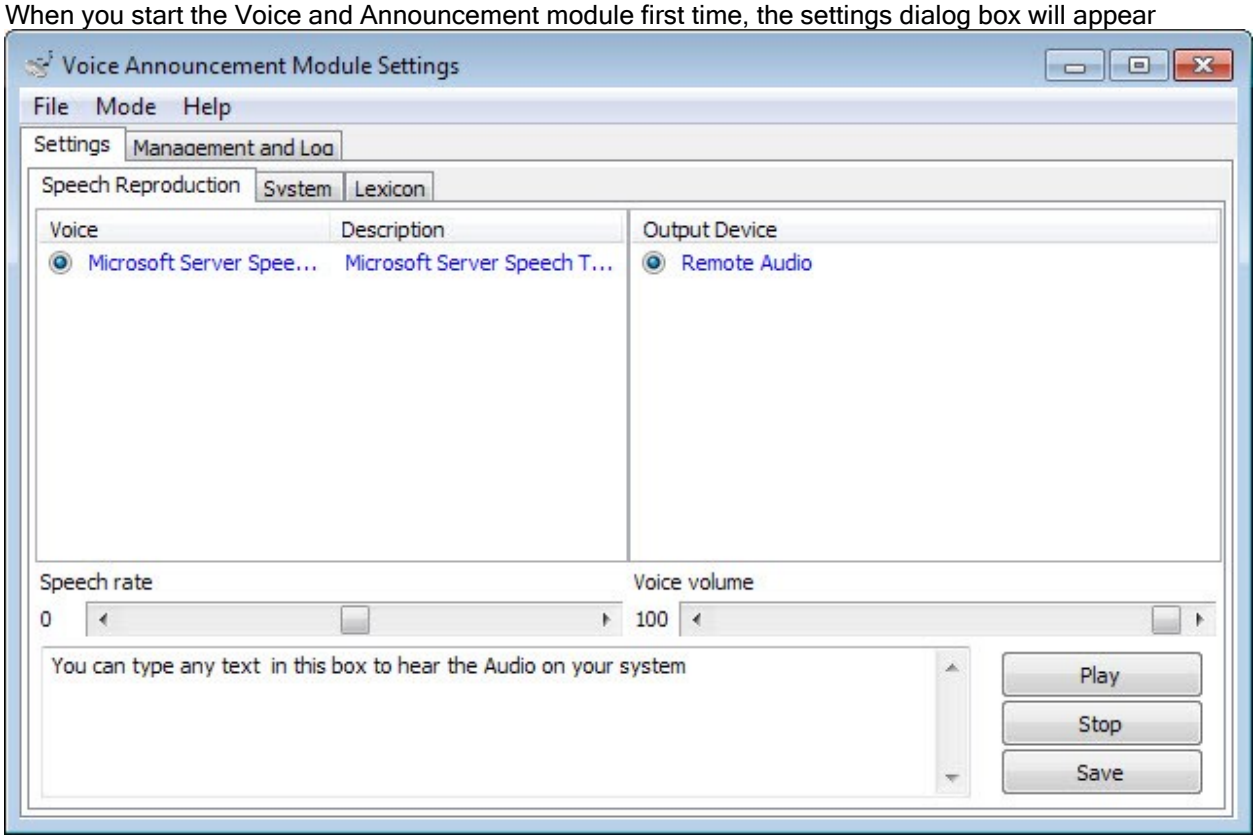
8.6 Voice Announcement Module

As said before, the Voice Announcement Module (the SoundServer.exe file in the folder where the Orion Pro is installed) is launched atomically by the System Shell, if the application is selected in the Database Administrator to run on the current workstation.

Chapter 8.2.3 Disabling Audio discusses how to manage voice announcements, this chapter mainly focuses on settings of the Voice and Announcement module.

8.6.1. First Start of the Voice Announcement Module

When you start the Voice and Announcement module first time, the settings dialog box will appear



Please make sure of the text is playing correctly (if you cannot hear any sound, please check to see that loudspeakers or headphones are connected to an appropriate audio output device in the right panel). Then click Start button. The system will go to normal operating mode and starts receiving system events

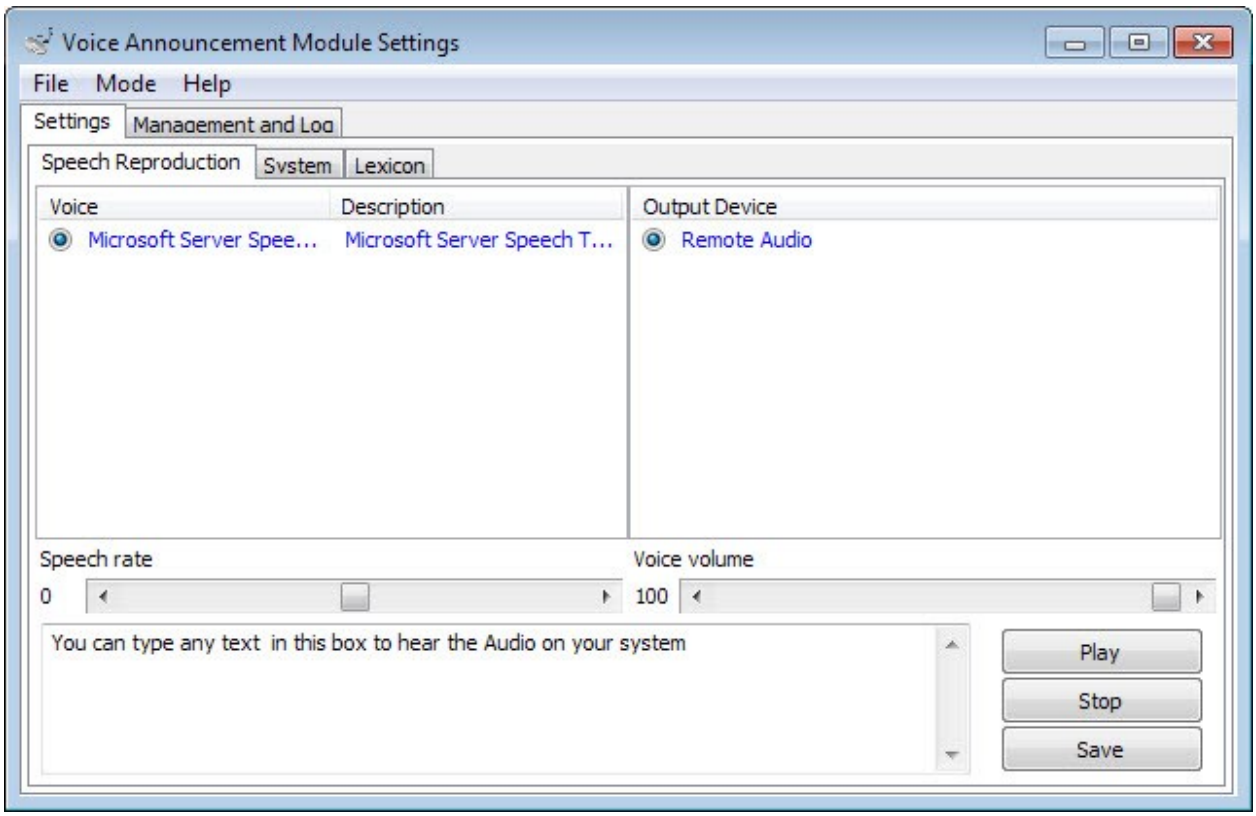
When deploying the system on multiple workstations with the same configuration, the system can be configured on one workstation, and then SoundConf.ini configuration file can be copied to other workstations. If the configuration is applied successfully, the Voice Announcement module starts in the normal operating mode. In case of error (unavailable output device) the settings dialog box will appear the same way as if it start first time.

8.6.2. Configuring the Voice Announcement Module

Settings can be made in three tabs: Voice, System, and Lexicon Settings.

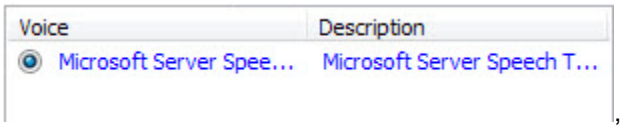
8.6.2.1. Voice Settings

The Speech Reproduction tab is used to set parameters of voiced alarms.



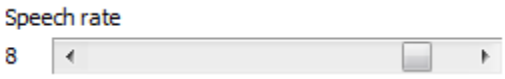
One can select:

- Voice (it must corresponds to the language of announcements) :



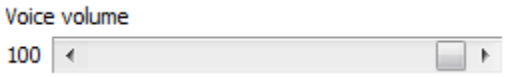
,

- Speech rate:



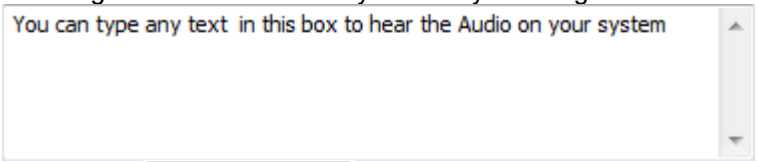
,

- Voice volume:



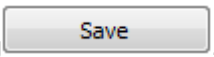
.

All changes can be immediately tested by entering an announcement text in the box on the bottom:



Please click 

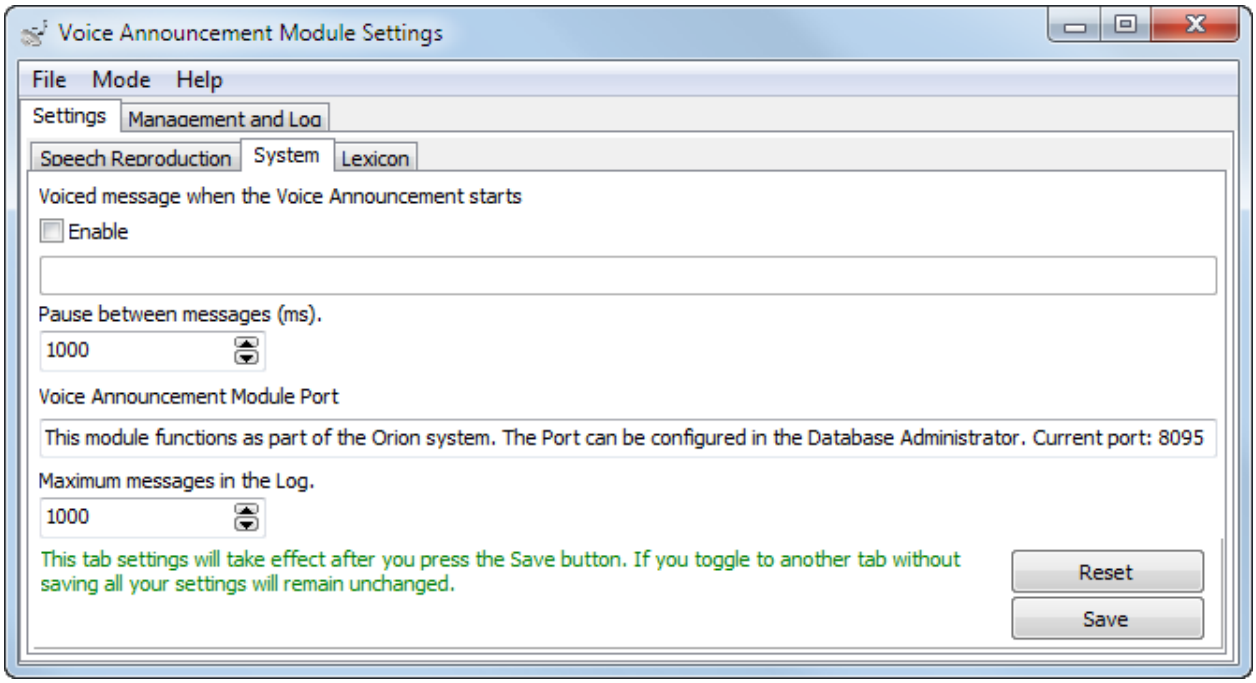
. The text will be voiced in accordance with applied settings.

The settings will be effective for voice incoming messages only after clicking 

. If one goes to another tab and them comes back, new changes will be still displayed on the tab, however without saving them they will be effective only for the test text.

8.6.2.2. System Parameters

The System tab is used to set additional system parameters.



To enable audio message playing when the Voice Announcement starts: please select the Enable checkbox and enter text you want to be voiced immediately after the Voice and Announcement going to the normal operating mode:

The Voice Announcemt has been started .

By default, the announcement text field is empty.

The **Pause between messages** is an interval between various voiced messages:

Pause between messages (ms).

1000

Pauses between repeats of the same audio message are in accordance with this parameter settings, but can be redefined by a calling side.

The port of the voice announcement module can be configured individually if the Voice Announcement runs in the offline mode. But we do not consider this case. In case of failed connection with the Central Server, the parameter will be accessible for configuring, but if the connection is recovered during restart, this parameter will be requested from the database.

Voice Announcement Module Port

This module functions as part of the Orion system. The Port can be configured in the Database Administrator. Current port: 8095

Maximum messaged in the log – the amount of messages displayed in the Management and Log tab.

Maximum messages in the Log

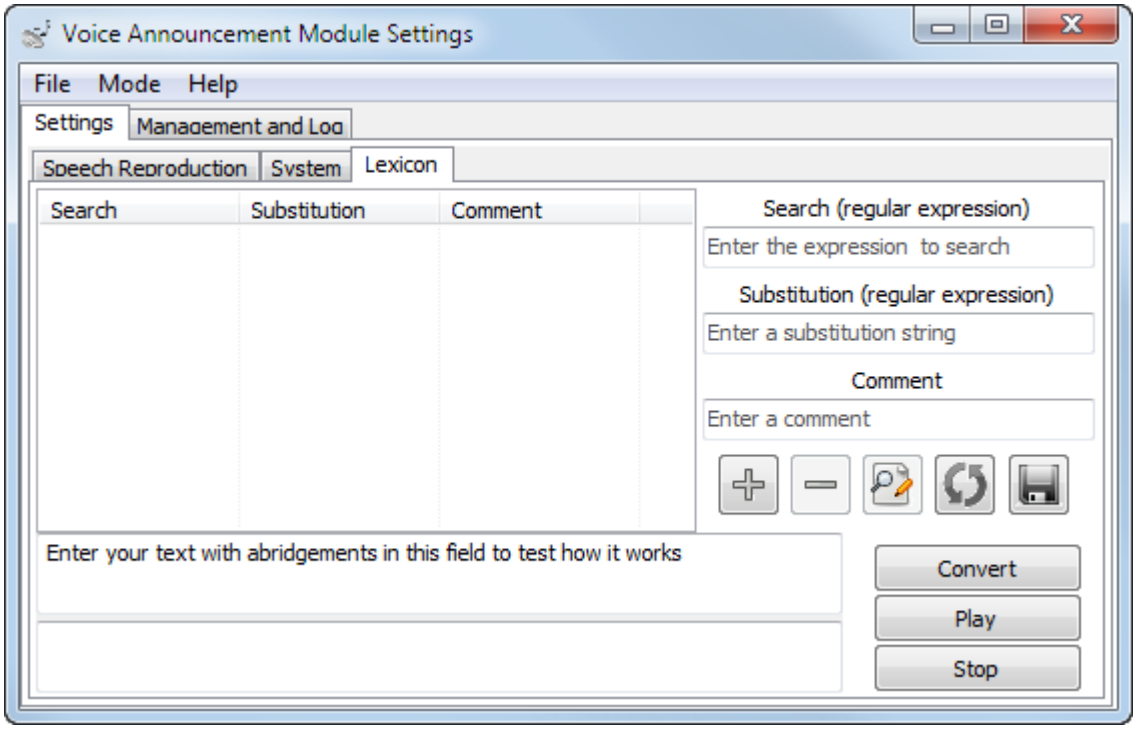
1000

If does not affect the server operation, the values more than 5000 are not recommended.

The Save Save button saves this tab parameters to the configuration, but they will applied only after the restarting Voice Announcement module; the Reset button resets all values to the current configuration (the last effective configuration). If one quits the tab in the configuration process, it will reset to the default values.

8.6.2.3.Tuning Lexicon Rules

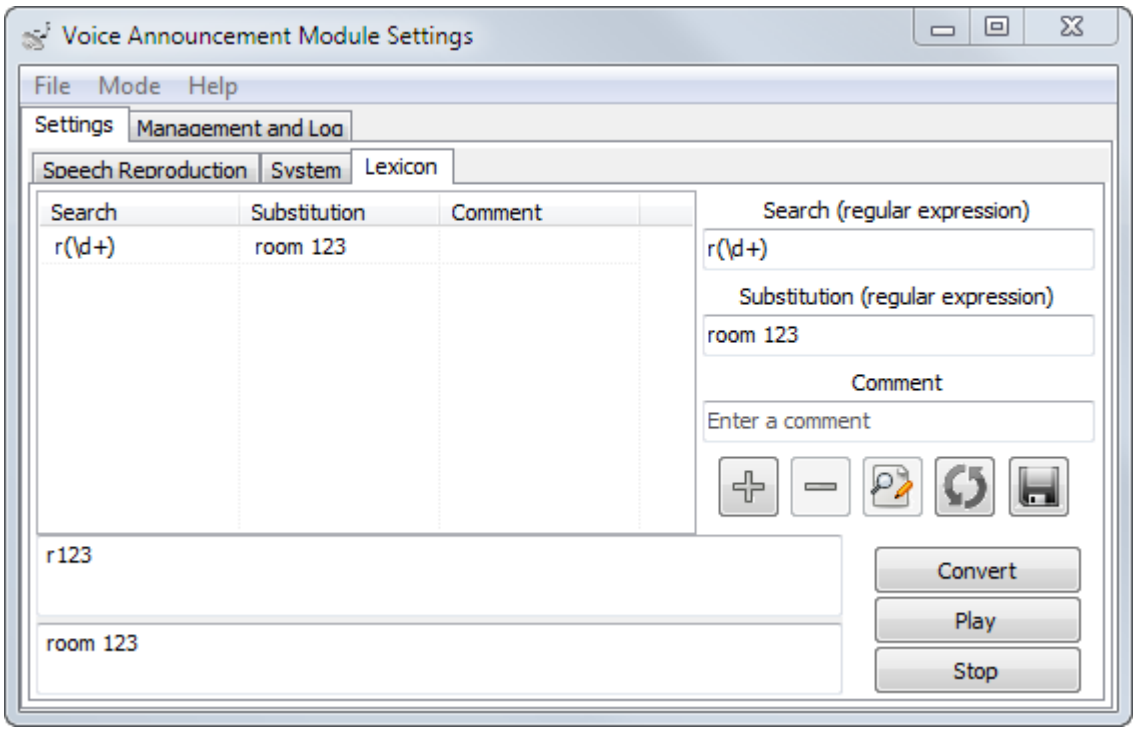
The Lexicon rule is used to set up rules to substitute abridgments for voice announcements.

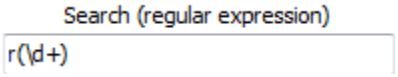


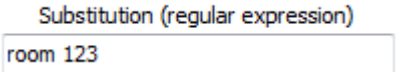
The tuning of substitution rules is a standard procedure. The information about such rules (also known as "regular expression" can be found following this link: https://en.wikipedia.org/wiki/Regular_expression

The following example explains how to substitute abridgments will full expressions:

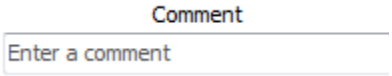
For example, we need to produce "room 123" from abridgments "r123" .
For the Search string we can use the following regular expression: **r(\d+).** The **room \1** expression will be used for the Substitution string:
Where:
\d: numeral;
\d+: a numerical group;
(\d+): A numerical group to be inserted in the Substitution string to replace the "**\1"** expression;
\1: the place where numerical groups (parenthesized) will be inserted.



The expression to be substituted is entered to this field: 

The substitution expression is entered in this field: 

.

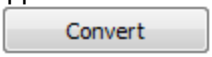
Enter comments in this field 

to help for editing.

This button  is used to add the rule described in the above fields to the list of lexicon rules.

The  button deletes the rule selected in the list of rules.

The  button is used to apply changes made for the existing rules.

There are two fields under the list of rules. The upper one is used to test how an expression will be converted on the basis of available rules. Click the 

to see message converted into the speech in the lower field. Click 

to hear the audio of converted message.

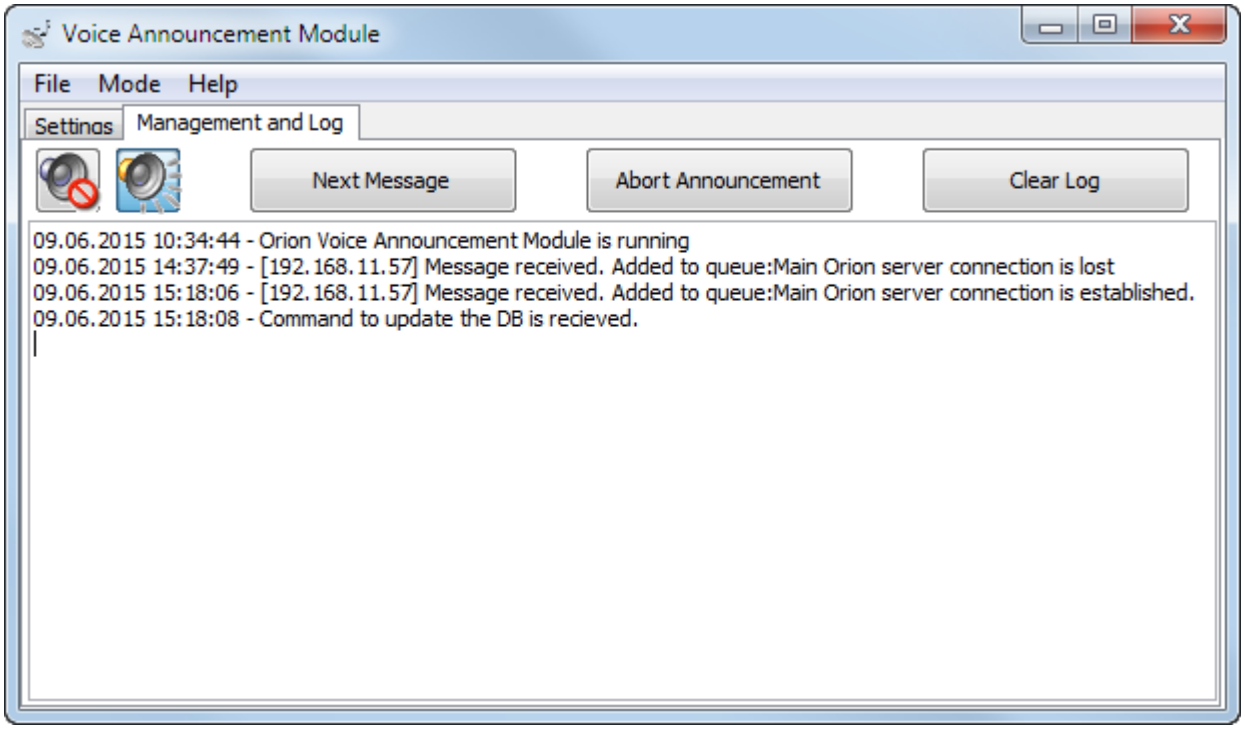
Click the  button to load rules used by the Announcement module on the current workstation (soundserver.red field in the folder with the installed Orion Pro).

Click this button  when you want to save changes in the list of rules for voice announcement on the current workstation.

8.6.3. Management and Log

Chapter 8.2.3 Disabling Audio (Mute Mode) discusses how to control announcement in the System Monitor or using the  icon in the system tray.

The Voice Announcement module also offers control functions in the Management and Log tab.



To cancel the current voiced message, click the 

Next Message button.

To abort all messages, please click the Abort Announcement button 

.

To disable the Announcement module (Mute), please click  .

To enable the Announcement module (Unmute), please click  .

The Management and Log tab also includes the Log of the Voice Announcement module:

09.06.2015 10:34:44 - Orion Voice Announcement Module is running
09.06.2015 14:37:49 - [192.168.11.57] Message received. Added to queue:Main Orion server connection is lost
09.06.2015 15:18:06 - [192.168.11.57] Message received. Added to queue:Main Orion server connection is established.
09.06.2015 15:18:08 - Command to update the DB is recieved.

This 

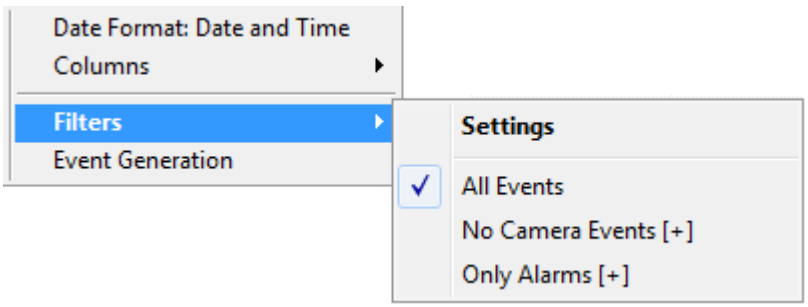
button is used to clear the log.

Appendix 8.A Setting Custom Event Filters

The System Monitor offers two types of custom filters for the Event Log:

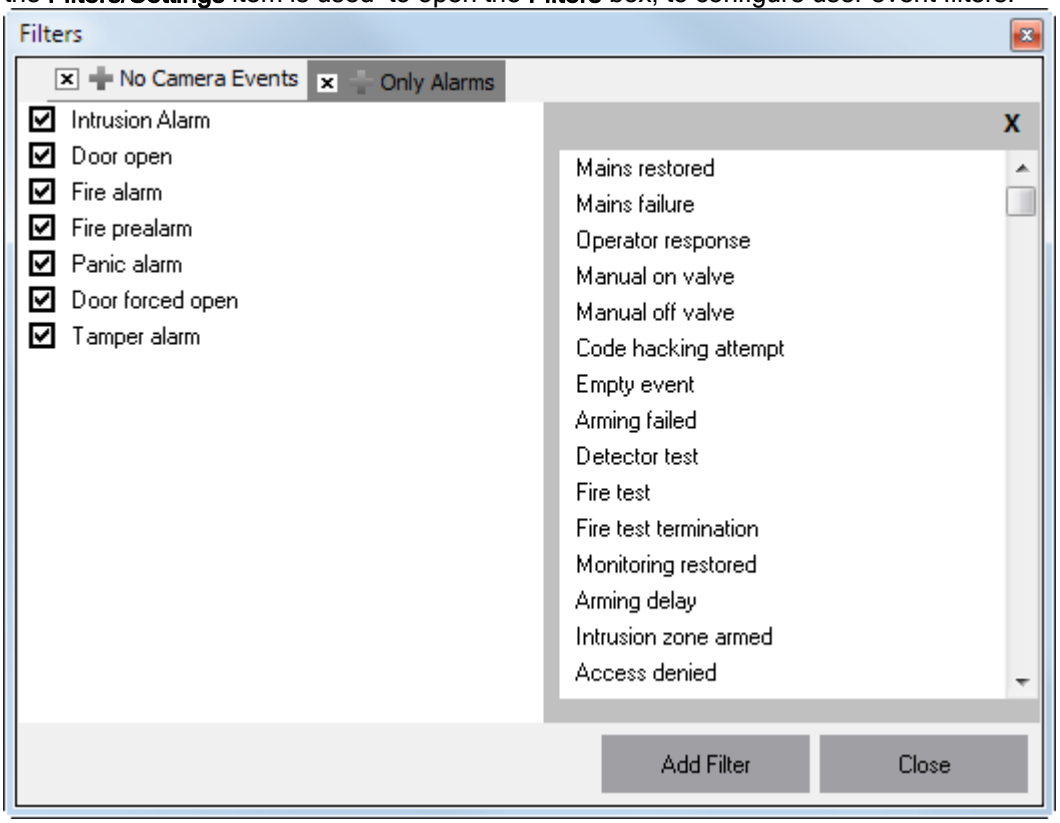
Type	*Description*
Inclusive	The Event Log displays only event contained in the filter.
Exclusive	The Event Log avoids displaying events contained in the filter.

A required filter can be selected using the dropdown list of the contextual menu of the Event Log:

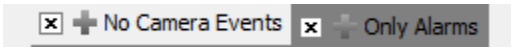


The list includes the All events filter (default) as well as user-added filters. The type of filter is specified in the brackets: Inclusive [+], or Exclusive [-]:

the **Filters/Settings** item is used to open the **Filters** box, to configure user event filters:



The user ffilter tabs are used to toggle between filters:



The contextual menu with custom filter items offers the following actions:

- Renaming a selected filter
- Changing the type of filter:

This и 

button is used to a new custom filter. The ☒ button is used to delete a custom filter

The central part of the Filters window shows the events contained in the selected filter

- ☑ Intrusion Alarm
- ☑ Door Open
- ☑ Fire Alarm
- ☑ Fire Pre-Alarm
- ☑ Panic Alarm
- ☑ Door Forced Open
- ☑ Tamper Alarm

The checkboxes are used to define whether to use ☑these events or not (☐).

This 

button is used to open the list of Orion Pro events available (no added) for this filter.

One can add any available event by dragging it from the list to the filter.

Multiple events can be selected to drag them to the active filter tab page:

- <Ctrl> + <A> – Select all events from the list.
- <Ctrl> + mouse click on an event – Adds an event to the group of selected events.
- <Shift> + mouse click – Select the range of events.

The following contextual menu:

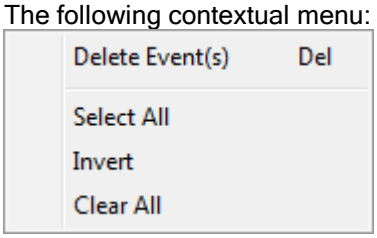


Figure 2

Offer the following actions:

- Deleting selected events,
- Selection all events,
- Inverting all selections
- Clearing all selections.

Appendix 8.B System Events

The table below includes all system events.

Для каждого события будет приведена следующая информация:

- Event # (Event Number).
- Event Name.

  (*Event name has the same color as it is displayed in the Event Log)*
- Whether an event is an alarm.

  (*In addition to Event Log, an alarm event is added to the Alarm Log*)

Event No	Event	Alarm
1	Mains restored	
2	Mains Failed	
3	Intrusion alarm	T
5	Operator Response	
17	Arming Failed	
19	Alarm Test	
20	Fire Test	
21	Fire test termination	
23	Arming Delay	
24	Arming Delay	
25	Access Denied	
26	Access Rejected	
27	Door Forced Open	T
28	Access Granted	
29	Access Prohibited	
30	Access unlocked	
31	Door Restored	
32	Passage	
33	The door is held open (Door Held Open)	T
34	User ID	

35	Auxiliary zone restored	
36	Auxiliary zone alarm	
37	Fire Alarm	T
38	Second auxiliary zone alarm	
39	Equipment restored	
40	Fire alarm 2	T
41	Equipment failure	
42	Unknown equipment	
44	Fire prealarm	T
45	The loop is open	T
47	Multiplex addressable loop is restored	
58	Panic alarm	T
67	The date is changed	
69	The log is full	
70	The log is overflowed	
71	Low level	
72	Normal level	
73	The time is changed	
74	High level	
75	Too high level	
76	High temperature	
77	Too low level	
78	Normal temperature	
82	Heat sensor failure	
83	Heat sensor restored	
84	Local programming	

90	Phone line failure	
91	Phone line restored	
94	Radiator heating	
95	Cooling danger	
96	Freezing danger	
97	Overheating of return water	
98	Pollution of the air filter	
99	Fan failure	
100	100 Summer-Day	
101	101 Summer-Night	
102	102 Winter-Day	
103	103 Winter-Night	
109	109 Loop disarmed	
110	110 Alarm cancelled	
117	117 Disarmed zone restored	
118	118 Entrance alarm	
119	119 Disarmed zone alarm	
121	121 Relay open failure	
122	122 Short failure of the output circuit (relay)	
123	123 Output circuit (relay) is restored	
126	126 The output (relay) is disabled	
127	127 Connecting the output (relay)	
128	128 Relay status changed (relay On/Off)	
130	130 Pump On	
131	131 Pump Off	
135	135 Automatic test error	

136	136 Power restored	
137	137 Release circuit activated	T
138	Release circuit failure	T
139	139 No discharge after the discharge command	T
140	140 Manual test	
141	141 Discharge delay	T
142	142 Automatics off	
143	143 Automatic discharge cancelled	
144	144 Extinguishing	T
145	145 Discharge without a discharge command	T
146	146 Discharge command	T
147	147 Discharge blocked	
148	148 Automatic mode is on	
149	149 Tamper alarm	T
150	150 Start of Voice Notification	
151	151 Voice Notification start cancelled	
152	152 Tamper restored	
153	Actuator Active	
154	Actuator Initial	
158	158 Internal zone repaired	
159	159 Voice Notification start delay	
165	165 Alarm loop parameter error	
172	172 Printer on	
173	173 Printer off	
187	187 The alarm loop is disabled	
188	188 The alarm loop is connected	

189	189 PL1 communication loss	
190	190 PL2 communication loss	
191	191 PL1 communication restored	
192	192 Output voltage is disabled	
193	193 Output voltage is enabled	
194	194 Power supply overload	
195	195 Power supply overload is repaired	
196	196 Charger failure	
197	197 Charger restored	
198	198 Power failed	
199	199 Power restored	
200	200 Battery restored	
201	201 PL2 communication restored	
202	202 Battery failed	
203	203 Watchdog timer reset	
204	204 Service required	
205	205 Battery test error	
206	206 Low temperature	
211	211 Battery discharged	
212	212 Backup battery discharged	
213	213 Backup battery restored	
214	214 Short failure	T
215	215 PL short failure	
216	216 Detector response	
217	217 RS-485 interface branch communication loss	
218	218 RS-485 interface branch communication restored	

219	219 Access unlocked	
220	220 Pressure detector is activated	
221	221 Pressure detector failed	
222	222 Polling loop trouble	
223	223 Patrol check	
224	224 Illegal response of the device in the polling loop	
225	225 Unstable response of the device in the polling loop	
238	238 Change of duty	
239	239 Operative task stopping	
240	240 Operative task starting	
241	241 Partition armed	
242	242 Partition disarmed	
243	243 Remote request for arming	
244	244 Remote request for disarming	
245	245 Remote request for access	
246	246 Wrong password	
247	247 Wrong partition	
248	248 Excess of power	
249	249 Programming (Configuration parameters changed)	
250	250 Device disconnected	
251	251 Device connected	
253	253 S2000 console has been turned on	
254	254 Date stamp	
255	255 Time stamp	
265	265 Two fire alarms	
270	270 Access granted (by button)	

271	271 Passage (by button)	
272	272 Access prohibited (by button)	
273	273 Access locked (by button)	
274	274 Access controled (by button)	
280	280 Partition group arming	
281	281 Partition group disarming	
310	310 Shell closing	
311	311 Switch On	
312	312 Switch Off	
313	313 Switch On for a Time	
314	314 Switch Off for a Time	
315	315 Blink from Off Condition	
316	316 Blink from On Condition	
317	317 Blink for a Time from Off Condition	
318	318 Blink for a Time from On Condition	
319	319 Lamp	
320	320 Alarm Output 1	
321	321 ASPT	
322	322 Siren	
323	323 Fire Output	
324	324 Trouble Output	
325	325 Fire Lamp	
326	326 Alarm Output 2	
327	327 Switch On for a Time Before Arming	
328	328 Switch Off for a Time Before Arming	
329	329 Switch On for a Time Upon Arming	

330	330 Switch Off for a Time Upon Arming	
331	331 Switch On for a Time Upon Disarming	
332	332 Switch Off for a Time Upon Disarming	
333	333 Switch On for a Time When Arming Failed	
334	334 Switch Off for a Time When Arming Failed	
335	335 Switch On for a Time Upon Auxiliary Loop Breaking	
336	336 Switch Off for a Time Upon Auxiliary Loop Breaking	
337	337 Switch On Upon Disarming	
338	338 Switch Off Upon Disarming	
339	339 Switch On Upon Arming	
340	340 Switch Off Upon Arming	
341	341 Switch On Upon Auxiliary Loop Breaking	
342	342 Switch Off Upon Auxiliary Loop Breaking	
343	343 ASPT-1	
344	344 ASPT-A	
345	345 ASPT-A1	
360	360 Management scenario is run	
370	370 Remote control command	
380	380 Message transmitted	
390	390 Request for switching automatic mode on	
391	391 Request for switching automatic mode off	
392	392 Request for discharge	
393	393 Request for cancelling the discharge command	
401	401 The relay is On	
402	402 The relay is Off	
403-439	403-439 The relay is On/Off	

525	525 Forced access	
527	527 The key is blocked centrally	
528	528 The key is unblocked centrally	
600	600 Channel monitoring mark	
601	601 Missed channel	
602	602 Channel restored	
997	997 Channel monitoring mark	
999	999 The protocol has been edited	
1034	1034 The password has been rejected	
1035	1035 Change of duty	
1036	1036 Screensaver is starting	
1101	1101 Monitor Closing	
1102	1102 System Shell Closing	
1103	1103 Discharge	
1133	1133 First passage	
1136	1136 Last exit	
1200	1200 Camera connected	
1201	1201 Camera disconnected	
1202	1202 Motion detector alarm	
1203	1203 Alarm end	
1204	1204 Armed	
1205	1205 Disarmed	
1206	1206 Recording started	
1207	1207 Recording stopped	
1208	1208 Video system stopped	
1209	1209 Video system started	

1211	1211 Remote request for arming	
1212	Remote request for disarming	
1213	Request to start recording	
1214	Request to stop recording	
1215	Motion detector is On	
1216	Motion detector is Off	
1218	Request for turning the motion detector on	
1219	Request for turning the motion detector off	
1220	Camera rotation	
1224	Motion detector response	
1225	Motion detector response has terminated	
1230	Display the camera on the screen	
1231	Stop displaying camera on the screen	
1400	Database reloading command	
1401	Database reloading command	
1402	Database is updated	
1403	Database is updated	
1450	Operative Task demo mode	
1451	Backup key 1000	
1452	Backup key is over	
1453	Backup server key 1000	
1454	Backup server key is over	
1531	Open Door command (Entrance)	
1532	Open Door command (Exit)	
1533	Open Door command (Passage)	
1541	Lock access command	

1542	1542 Restore access control command	
1543	1543 Set free pass mode command	
1544	1544 The command to control access	
1604	1604 Connecting to the backup server	
1605	1605 Main server connecting	
1650	1650 Custom event	
1651	1651 External event	
1652	1652 Connecting to the server	
1653	1653 Disconnecting from the server	
3000	3000 A Keybox has been found	
3001	Keybox off-line	
3002	Keybox power is off	
3003	Keybox power is on	
3004	Keybox low battery	
3005	Correct pen case is got by the card	
3006	Correct pen case is put in by card	
3007	Pen cas is put in without card	
3008	Cylinder removed without card	
3009	Wrong cylinder inserted	
3010	Wrong pen case is got	
3011	Disarmed pen case is got	
3012	Reject mode activated	
3013	Key storage server disconnected	
3014	Key storage server stopped	
3015	Granting access to keybox cylinder	
3016	Key box server connected	

4000	Scanning Core Started	
4001	Database Reloading Started	
4002	Database Reloading Completed	
4003	Scanning Core Closed	

Appendix 8.C Commands for Loops

The Appendix provides the list of commands used for different types of loops (*):

Loop Type	Commands						
	Arming	Disarming	Reset Alarm	Enable Auto Mode	Disable Auto Mode	Activate Extinguishing	About Extinguishing
Intrusion	✓	✓	✓	✗	✗	✗	✗
Entrance	✓	✓	✓	✗	✗	✗	✗
Panic Button	✓	✗	✓	✗	✗	✗	✗
Fire	✓	✓	✓	✗	✗	✗	✗
Manual Call Point	✓	✓	✓	✗	✗	✗	✗
Smoke Addressable and Analogue	✓	✓	✓	✗	✗	✗	✗
Heat Addressable and Analogue	✓	✓	✓	✗	✗	✗	✗
Humidity	✓	✓	✗	✗	✗	✗	✗
Fire Addressable and Analogue	✓	✓	✓	✗	✗	✗	✗
Loop Supervision	✓	✓	✗	✗	✗	✗	✗
Manual Activation (Rupor)	✓	✓	✗	✗	✗	✗	✗
Manual Release (ASPT)	✓	✓	✗	✗	✗	✗	✗
Manual Release (Potok)	✓	✓	✗	✗	✗	✗	✗
Pressure Detecter	✓	✓	✗	✗	✗	✗	✗
Auto Mode	✗	✗	✗	✓	✓	✗	✗
Device Mode	✗	✗	✗	✗	✗	✓	✓
Remote Activation	✓	✓	✗	✗	✗	✓	✓
Potok Remote Activation	✗	✗	✗	✗	✗	✓	✓
Programmable Auxiliary	✓	✓	✗	✗	✗	✗	✗

(*) No commands are provided for the loops of other types