

<b>6. DATABASE ADMINISTRATOR .....</b>	<b>3</b>
6.1 DATABASE ADMINISTRATOR INTERFACE .....	6
6.1.1 Program Menu .....	7
6.1.2 Toggling Buttons.....	11
6.1.3 Action Buttons.....	11
6.1.4 Inspector.....	12
6.1.5 Event Log.....	13
6.2 DEVICE ADDRESSES. THE PHYSICAL STRUCTURE OF THE SYSTEM.....	14
6.2.1 The System Entity .....	15
6.2.2 The Workstation Entity (Computer) .....	16
6.2.4 The COM Port Entity .....	25
6.2.5 The Ethernet Adapter Entity.....	27
6.2.6 The List of Connected Devices. Orion and Orion Pro Protocols .....	29
6.2.7 The List of Connected Biometric Readers .....	56
6.2.8. The List of Connected UOPs .....	59
6.2.11 Connecting Devices Using Printer Protocol .....	63
6.2.12 Entity Events .....	63
6.3 MAPS TAB. CREATING LOGICAL ENTITIES AND STRUCTURE OF INTRUSION AND FIRE ALARM SYSTEM.....	65
6.3.1 Partitions and Partition Groups .....	66
6.3.2 The Maps Tab. Adding Entities to Maps .....	75
6.4 THE SYSTEM STRUCTURE TAB. INTRUSION AND FIRE CENTRALIZED CONTROL.....	101
6.4.1 Configuring Centralized Control of Relay Outputs .....	102
6.4.2 Setting Transmission of Events and System Entity States .....	108
6.4.3 Associating Control Elements to System Readers .....	109
6.4.4 Configuring System Responses to the Events of System Entities .....	112
6.4.5 Renaming System Events .....	117
6.4.6 Configuring Display of User Photo by the System Monitors .....	120
6.4.7 Associating Cameras to Device Zones .....	121
6.5 THE ACCESS TAB. CREATING LOGICAL EVENTS AND STRUCTURE OF ACCESS CONTROL SYSTEM .....	123
6.5.1 The Access Zone Entity.....	128
6.5.2 The Access Point Entity.....	129
6.6 THE MANAGEMENT SCENARIOS TAB.....	140
6.6.1 Creating Management Template-Based Scenarios .....	142
6.6.2 Creating Scenarios Using Built-In Script Language .....	146
6.6.3 Examples of Tasks of Management Scenarios.....	150
6.8 THE SCHEDULE TAB. SCHEDULE OF MANAGEMENT SCENARIOS .....	157
6.9 THE TIME ZONES TAB. CONFIGURING TIME ZONES.....	159
6.9.1 Time Zone for Intrusion and Fire System (IFS).....	162
6.9.2 Time Zone for Access Control System (ACS).....	173
6.9.3 Time Zones for Time and Attendance (T&A).....	175
6.9.4 Time Zones for Scenarios .....	177
6.10 THE ACCESS LEVELS TAB. CREATING ACCESS LEVELS AND WORKING SCHEDULES .....	178
6.10.2 Configuring Access Levels for Access Control System.....	187
6.10.3 Combined Access Levels.....	197
6.10.4 Configuring Working Schedules.....	201
6.10.5 Configuring Access Levels for System Monitor Operators .....	203
6.11 THE EMPLOYEES TAB. CREATING THE LIST OF EMPLOYEES.....	207
6.11.1 The Employee Entity.....	209
6.11.2 Employee Card. Printing a Badge .....	222
6.11.3 Saving an Employee Photo as a File .....	228
6.11.4 Exporting Employee Details and Credentials to CSV File .....	228
6.12 THE CREDENTIALS TAB. CREATING THE LIST OF SYSTEM CREDENTIALS .....	230
6.12.1 Creating Passwords for Software Modules .....	233
6.12.2 Creating PIN Codes.....	237
6.12.3 Creating the List of Touch Memory Buttons, Proximity Cards and Fingerprints .....	240
6.12.4 Synchronizing the Credentials of the Orion Pro Database and Access Controllers.....	247
6.13 SYNCHRONIZING THE ORION PRO DATABASE WITH S2000M PANEL .....	269

6.13.1 Importing Configuration from the S2000M .....	269
6.13.2 Exporting Database to S2000M .....	273
6.14 SETTINGS .....	277
6.14.1 Settings of Database Administrator .....	277
6.14.2 Setting User Events .....	281
6.14.3 Setting Event Groups .....	283
6.14.4 Configuring Network Ports .....	285
APPENDIX 6.A CENTRALIZED CONTROL RELAY PROGRAMS.....	286
APPENDIX 6.B. SCENARIOS OF RELAY OUTPUT CENTRALIZED CONTROL.....	291
APPENDIX 6.B. STANDARD SCENARIO STEPS .....	297


## 6. Database Administrator

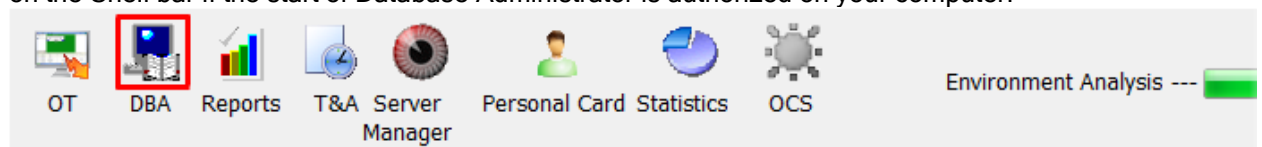
*It is recommended to get acquainted with the terms and definitions of Orion Integrated Security System before getting started Database Administrator (See Chapter 1. About the System)*

The **Database Administrator** network client of the Orion Pro system is used to configure the systems and controllers.

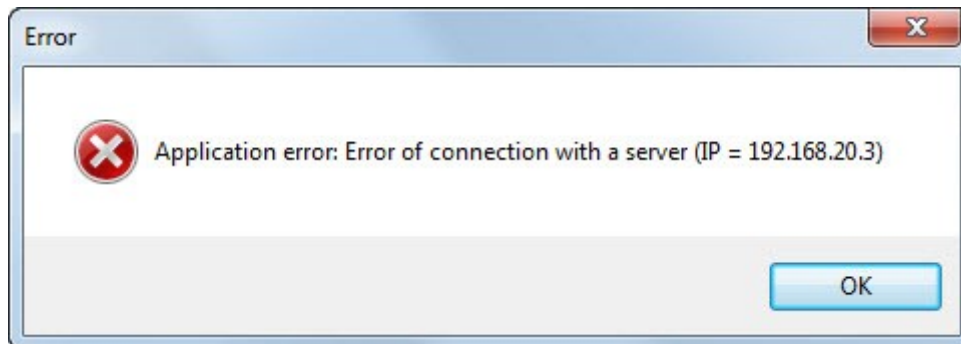
The Database Administrator allows a system user to:

- Describe the physical structure of the system: workstations and workstation-connected devices and cameras
- Define logical system elements: partitions, partition groups, access points, and access zones
- Add system entities to site maps
- Create management scenarios
- Configure system automated responses to any events;
- Enter employee details
- Define employee privileges
- Enter credentials : software passwords, PIN-codes, and Touch Memory and Proximity tokens
- Program Time Zones and Access Levels, PIN-codes, tokens to system devices using Scanning Cores.

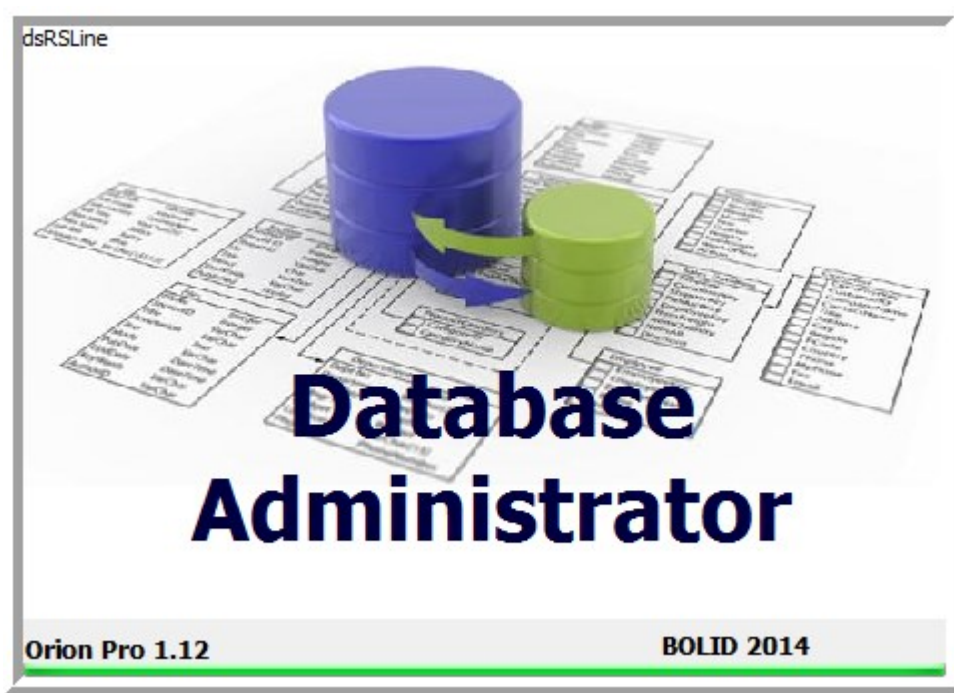
The Database Administrator ( Abd.exe located in directory where Orion Pro is installed) is started from the System Shell. Please start the System Shell of the Orion Pro system, left click the corresponding icon on the Shell bar if the start of Database Administrator is authorized on your computer:



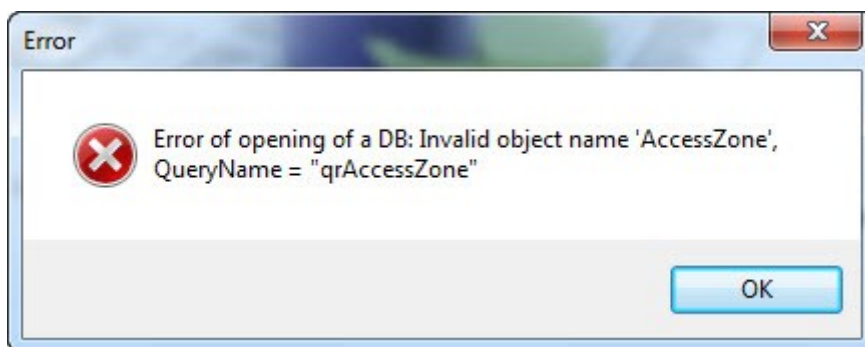
If there is no connection to the Central Server, the Database Administrator cannot be started and the error box will appear with the following message:



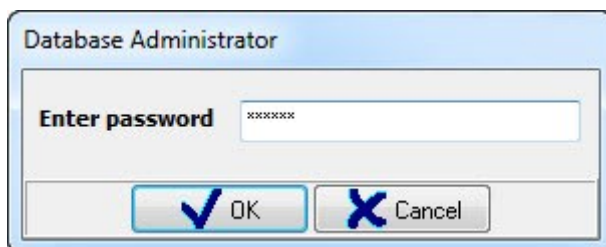
If the Central Server connection is successful, the splash window will appear and the Database Administrator will start loading the Database:



If a database version is not compatible with the revision of the Orion Pro system currently used, the loading process will be terminated at the very first table where the table structure mismatched the structure of this table in the database of the used Orion Pro, and a warning box will appear to this respect. For example:



If the version of the Database is as required, its loading will result in a dialog box where you should enter your password to log in to the Database Administrator:



The password entered should belong to an employee who has a user status such as **Owner**, **Administrator**, or **Badge Office Operator**; this password must give rights to run Database Administrator. The accessibility of the Database Administrator tabs and menus depends on a user status and password-associated rights and privileges.

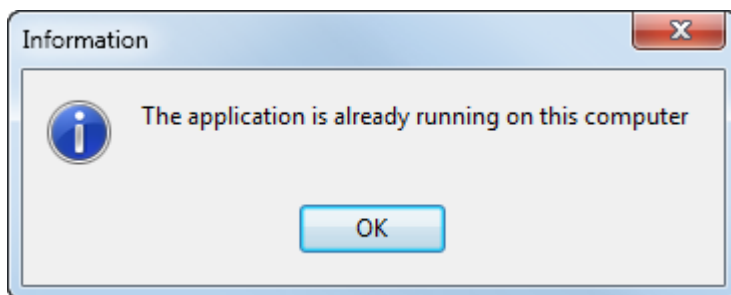
For the explanation of user status and password rights, see Chapter 6.11.1.1 *Employee Status* and Chapter 6.12.1 *Creating Software Passwords*). Let's discuss examples of an employee status and password rights as applicable to Database Administrator module:



- Access to the tabs of the Database Administrator depending on the status of an account:
  - Owner and Administrator have access to any windows of the software (depending on password rights)
  - Duty Officer, Duty Operator, Credentials Holder and User have no rights to run the Database Administrator module
  - Database Operator have rights to access to the Employees and Credentials tabs only (depending on password rights)
- Access to the tabs of the Database Administrator module depending on password rights:
  - **Database Administrator Off** disables rights to work with Database Administrator
  - **Database Administrator On** give rights to work with Database Administrator in accordance with the following:
    - **Access to Intrusion and Fire Alarm Systems** give rights to access the Device Addresses, Floor Plans, and System Structure windows
    - Access to **Access Control, Management Scenarios, Management Tree, Schedules, Access Levels, Personnel, and Credentials** give rights to run the corresponding windows.

The default employee in new and demo databases of Orion Pro's is "John Smith" who has maximum privileges and password "1".

Attention! You can run one instance of a Database Administration a single workstation. If Database Administrator is already running on a workstation, your attempt to start it once more (for example in a folder with installed Orion Pro) will not result in starting one more instance of the Database Administrator. And the following message will appear.



It is worth mentioning that more than one Database Administrator modules can be run on different workstations at a time. A logical question arises about how the coordination of such modules is provided, namely, how information updates are provided in Database Administrator modules, when database changes are made on one of them.

The Database Administrator has the following logic implemented to support updates of database information in case of its remote changes:

- If the database is changed remotely, a message about changing a table (or several ones) will appear in the Event Log (Chapter 6.1.5 Event Log) of the **Remotely Changed Table** in Database Administrator (Bottom of the Database Administrator screen).

For example:

Date	Time	Description
3/10/2015	4:26:31 PM	Changed data in the Employees table

- A current user of Database Administrator sees these messages and can perform required actions to update information in Database Administrator, if required:

If data are changed in any Database Administrator, all other Database Administrators will receive messages about such changes. This message will be displayed in the event log, and updates related to **Scenarios, Management Tree, Schedules, Time Zones, Access Levels, and Credentials** will take effect automatically in **Database Administrators**. In addition, the data update message will be displayed in the event log of the **Network Exchange** tab:

Date	Time	Description
05.09.2014	16:40:51	: RefreshTablesData

Switching to any of the above tabs will refresh displayed information.

Thereafter, if database changes occurred in relation to one of these tabs of Database Administrator while you are working in this tab, you should toggle another tab and then come back to the required tab where the displayed information will be refreshed.

**Device Addresses, Maps, System Structure, and Access Control** tabs do not support the automated updates. To update information on these windows please right click the event log field of Remotely Changed Tables to choose on the following actions:

- Update tables for the current window:

Refresh tables for the current tab	F5
Refresh all tables	Ctrl+F5

(or press <F5> on the keyboard).

The update will take effect for the information from database tables related to the current (opened) maintenance window of Database Administrator.

- Update all tables:

Refresh tables for the current tab	F5
Refresh all tables	Ctrl+F5

(or press <Ctrl+F5> on the keyboard).

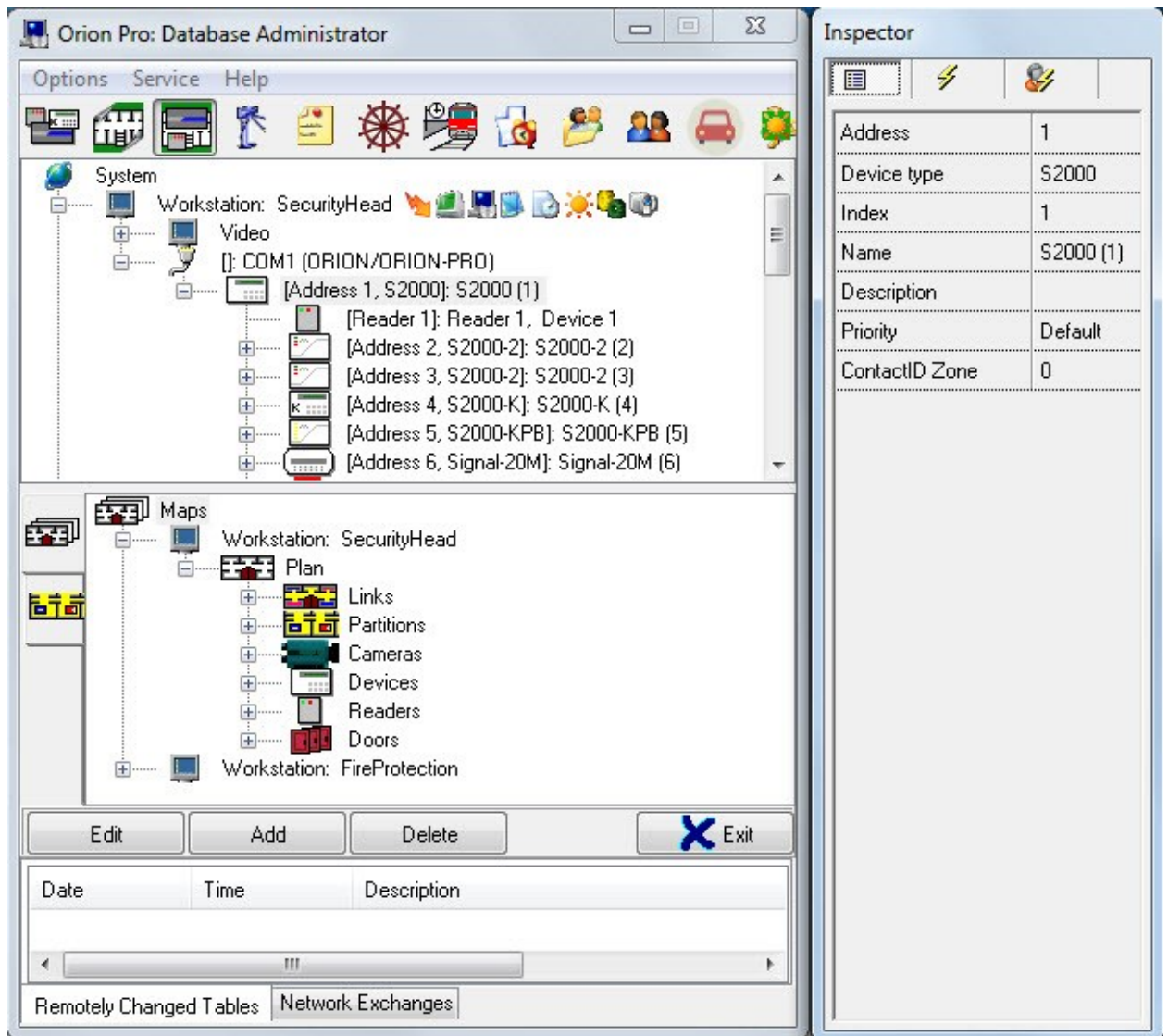
Information from all database tables will be updated.

Performing any of two actions above will result in:

- Refreshing displayed information on the current (active) tab of Database Administrator
- Cleaning the event log from outdated messages related to tables containing information that has been updated.

## 6.1 Database Administrator Interface

Database Administrator graphic interface is shown in the figure below:



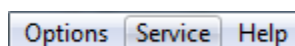
The figure above shows, the elements of the Database Administrator module:

1. Menu bar
2. Buttons to toggle between the Database Administrator tabs
3. Current window area
4. Event Log
5. Action buttons
6. Inspector dialog box.

The Current Window Area displays the maintenance window selected using toggle buttons or menu commands. Options of each tab are described in the corresponding Chapters (see chapters *6.2 Device Addresses* - *6.12 Credentials*)

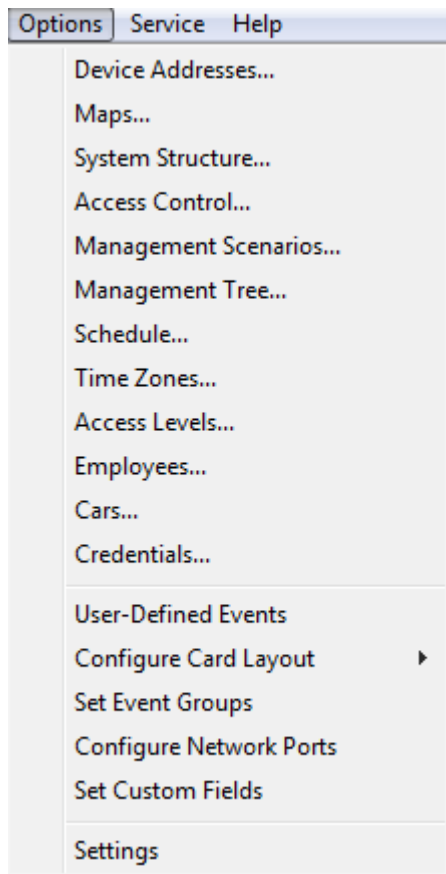
Other elements are described in chapters *6.1.1 Program Menu* - *6.1.5 Event Log*

### 6.1.1 Program Menu



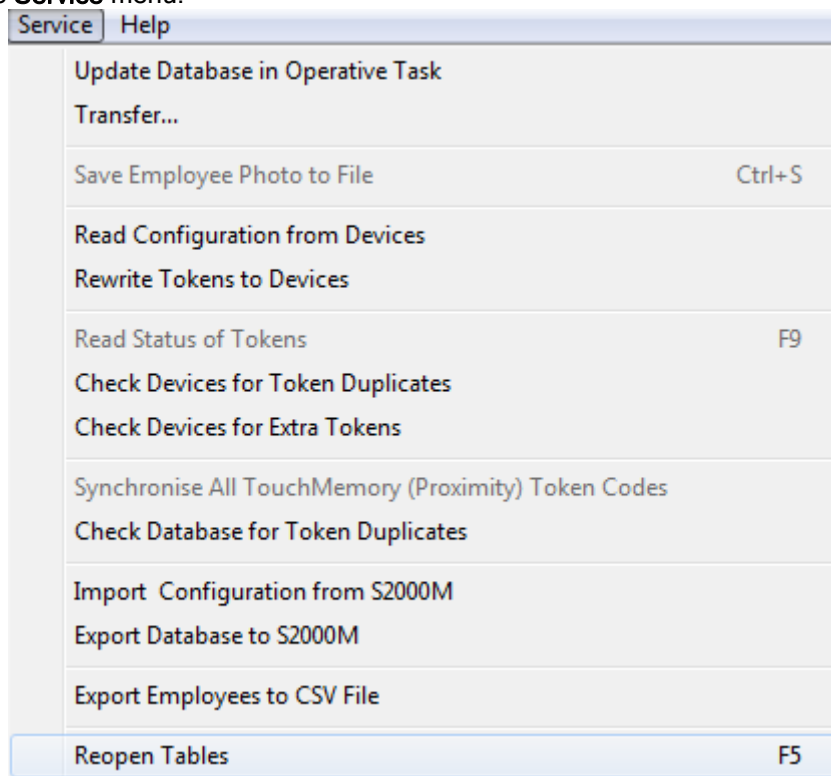
The Menu bar includes the following elements:

1. The **Options** menu:



- 1.1. **Device Addresses...** opens the Device Addresses window.
- 1.2. **Maps...** opens the Maps window
- 1.3. **System Structure...** opens the System Structure window.
- 1.4. **Access Control...** opens the Access Control window.
- 1.5. **Management Scenarios...** opens the Management Scenarios window.
- 1.6. **Management Tree...** opens the Management Tree window.
- 1.7. **Schedule...** opens the Schedule window
- 1.8. **Time Zones...** opens the Time Zones window.
- 1.9. **Access Levels...** opens the Access Level window.
- 1.10. **Employees...** opens the Employees window.
- 1.11. **Credentials...** opens the Credentials window
- 1.12. **User-Defined Events** opens the Setting User Events dialog box to add, edit and delete user events.  
(These actions are described in Chapter 6.14.2 *Defining User Events*)
- 1.13. **Configure Card Layout** opens the **Badge Layout Editor** window to create and edit badge layouts for further printing (usually proximity card printers are used for this purpose)  
(These actions are described in Chapter 6.11.2.1 *Creating Badge Layout*)
- 1.14. **Set Event Groups** opens Set Event Groups where you can customize groups of system object evens (See Chapter 6.14.3 Setting Event Groups).
- 1.15. **Configure Network Ports** is used to configure network ports for the software modules. (See Chapter 6.14.4 *Configuring Network Ports*.)
- 1.16. The **Settings** item opens the Settings window to set the performance parameters of the Database Administrator module (These actions are described in Chapter 6.14.1 *Settings of Database Administrator*).

The **Service** menu:



- 1.17. **Update Database in Operative Task** instructs all System Shells (as well as their Scanning Cores, Monitors, and Video Serves) to update the database information. When database update is completed in any Scanning Core, the corresponding message will be displayed in the Event Log in **Network Exchanges**:

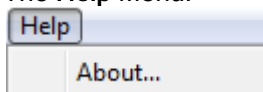
Date	Time	Description
14.08.2014	12:23:16	: Database restart in Scanning Core completed, computer SUPPORT-11-57 (192.168.11.57)
14.08.2014	12:23:16	: Database restart in Scanning Core completed, computer SUPPORT-11-57 (192.168.11.57)

Information in the System Shell, Scanning Core, and Monitors modules is updated automatically when database changes are occurred in relation to time zones, access levels, and the lists of employees and credentials.

This menu action is used to instruct all System Shells (Scanning Cores, Monitors, and Video Server) to complete entire update of database information.

- 1.18. **Transfer...** is used to transfer Devices of COM-port or S2000 (S2000M) panel to another COM port or panel.  
(The description of this action is provided in Chapter 6.2.6.1.3 *Device Transfer*).  
*This menu item is accessible only on the Device Addresses and System Structure windows (tabs).*
- 1.19. **Save Employee Photo to File** is used to save an employee photo to a file. (See Chapter 6.11.3 *Saving an Employee Photo to a File*).  
*This menu item is accessible on the Employee tab only.*
- 1.20. **Read Configuration from Devices** is used for reading configurations and tokens codes from devices by Scanning Cores. (See Chapter 6.12.4.1 Reading Configurations and Token Codes by Scanning Cores. Receiving of Credential States).
- 1.21. **Rewrite Tokens to Devices** is used to rewrite tokens to devices.  
(The related actions are described in Chapter 6.12.4.3.3 *Rewriting Credentials to Devices*).
- 1.22. **Read Status of Tokens** is used to obtain status of tokens (credentials), stored in devices, via Scanning Core. (See Chapter 6.12.4.1 Reading Configurations and Token Codes by Scanning Cores. Receiving of Credential States).  
*This menu item is accessible only when the Credentials window (tab) is open.*
- 1.23. **Check Devices for Token Duplicates** instructs Scanning Cores to search duplicates of tokens in devices.  
(For the description of these actions, see Chapter 6.12.4.5 *Searching Token Duplicates in Devices*.)

- 1.24. **Check Devices for Extra Tokens** instructs Scanning Cores to search token codes that is not stored in the Database of the Orion Pro system.  
(For the description of these actions, see Chapter 6.12.4.6 *Searching Extra Tokens in Devices*).
  - 1.25. **Synchronize All Touch Memory (Proximity) Token Codes** instructs Scanning Cores to check and change, if needed, token codes and their assigned rights in devices in accordance with the settings of the Orion Pro database.  
(For the description of these actions, see Chapter 6.12.4.3.2 *Synchronizing All Tokens with Devices*)  
*This menu item can be accessed only when the Credentials window is opened.*
  - 1.26. **Check Database for Token Duplicates** is used to search token duplicates in the Orion Pro Database.  
(For the description of these actions, see Chapter 6.12.4.4 *Searching Token Duplicates in Database*)
  - 1.27. **Import Configuration from S200M** instructs a corresponding Scanning Core to import a configuration from the S2000M panel to the Orion Pro database. (For the descriptions of these actions see Chapter 6.13.1 *Importing Configuration from S2000M Panel*)  
*This menu item is available only when on the Device Addresses and System Structures windows.*
  - 1.28. **Export Database to S2000M** instructs a corresponding Scanning Core to export the Orion Pro database to the S2000M panel. (For the description of these action see Chapter 6.13.2 *Exporting Database to S2000M*)  
*This menu item is available only when on the Device Addresses and System Structures windows.*
  - 1.29. **Export Employees to CSV File** exports list of employees and tokens to CSV file.  
(For the description of these actions see chapter 6.11.4 *Exporting Employees and Credentials to CSV File*.)
  - 1.30. **Reopen Tables** is used to update information from all database tables in the Database Administrator module. (For the descriptions of these actions see the foreword in chapter 6. Database Administrator.)
2. The **Help** Menu.



- 2.1. **About ...** is to open the About... window:














This window shows the versions of Orion Pro and Database Administrator, as well as information about the Bolid Company.

### 6.1.2 Toggling Buttons



To facilitate entering and viewing the system information, Database Administrator is subdivided into 11 tabs, with each of them been used to edit relevant system data. You can toggle between windows using Database Administrator's toolbar buttons, the items of Options menu or <Ctrl+Tab> keyboard shortcut.

Buttons toggling between the Database Administrators tabs:

	Toggles <b>Device Addresses</b>
	Toggles <b>Maps</b>
	Toggles <b>System Structure</b>
	Toggles <b>Access Control</b>
	Toggles <b>Managements Scenarios</b>
	Toggles <b>Management Tree</b>
	Toggles <b>Schedule</b>
	Toggles <b>Time Zones</b>
	Toggles <b>Access Levels</b>
	Toggles <b>Employees</b>
	Toggles <b>Credentials</b>

The toolbar also includes an icon indicating a status of connection to the Central Sever:



- You are connected to the Central Server,




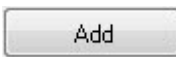
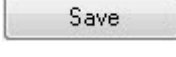
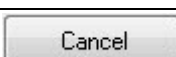

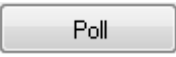

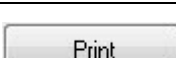
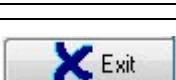
- You are disconnected from the Central Server.

### 6.1.3 Action Buttons

This area includes action buttons affecting the entities of the Orion Pro system; it also includes the **Exit** button of the Database Administrator module.

Buttons may be not the same for each table of Database Administrator.






	To edit properties of selected system objects. (The accessibility of this button depends on a selected system objects and selected Database Administrator's tab)
	To add a system object. (The accessibility of this button depends on a selected system object and selected window of Database Administrator)
	To save when a new object is added or properties of existing are edited . (This button is active only when editing or adding actions are performed)
	To cancel actions related to adding a new object or editing properties of existing one. (This button is active only when editing or adding actions are performed)
	To delete a system entity. (The accessibility of this button depends on a selected system object and selected window of Database Administrator)
	To obtain the list of connected devices from Scanning Core. (This button is active only when the Device Addresses window is opened)
	To check for errors in the text of a management scenario (script). (This button is active only when a scenarios edited in Management Scenarios)
	To print an employee badge using a printer (usually, special Proximity-card printers are used for this purpose). (This button is active on the Employees tab only)
	To quit Database Administrator

#### 6.1.4 Inspector

Each system Entity had its own individual properties. The properties for each system entity configured in Device Addresses, Map, and System Structure and Access Control are displayed in the Inspector box.



The Inspector window includes three tabs:

	Object properties
	Associate scenario to object events
	Rename Object Event

The Entity events tab is used to modify the properties of a selected object. (There are rare cases when some properties cannot be changed. The properties of each entity are described in relevant chapters of this Guide)

The **Associate management scenario to entity events** tab is used to associate management scenarios to the events of selected system entities. (See chapter 6.4.4 Configuring System Response to Entity Events. Associating Management Scenarios to Entity Events)

The Rename entity events tab is used to rename events of a selected entity.

It is worth mentioning that each type of entities has its own set of properties and events. This set of events can be modified. (See chapter 6.14.3 Setting Event Groups)



### 6.1.5 Event Log

Date	Time	Description
3/10/2015	4:26:31 PM	Changed data in the Employees table

Event Log displays the following:

- Messages about remote changes of database tables (using the Database Administrator instance running on other workstation)
- Networks exchanges between Database Administrator and Scanning Cores.

Event log includes to tabs:

- **Remotely Changed Tables:**

Date	Time	Description
3/10/2015	4:26:31 PM	Changed data in the Employees table

You can access the following context menu by right-click in the tab's field:

Refresh tables for the current tab	F5
Refresh all tables	Ctrl+F5

See the foreword to Chapter 6. *Database Administrator* for description of Database Administrator's work when database remote changes occurred.

- **Network Exchanges:**

Date	Time	Description
14.08.2014	12:23:16	: Database restart in Scanning Core completed
14.08.2014	12:23:16	: Database restart in Scanning Core completed

This tab displays information on the following operations:

- Reading configuration and token codes in devices,
- Receiving information on tokens (credentials)
- Synchronizing one token
- Synchronizing all tokens
- Rebooting the database in Scanning Core
- Obtaining the list of time zones stored in a device
- Writing a time zone to a device
- Receiving the list of level accesses from a device
- Writing an access level to a device.

Network interaction errors are also displayed here.

You can access the following context menu by right-clicking in the tab's field:

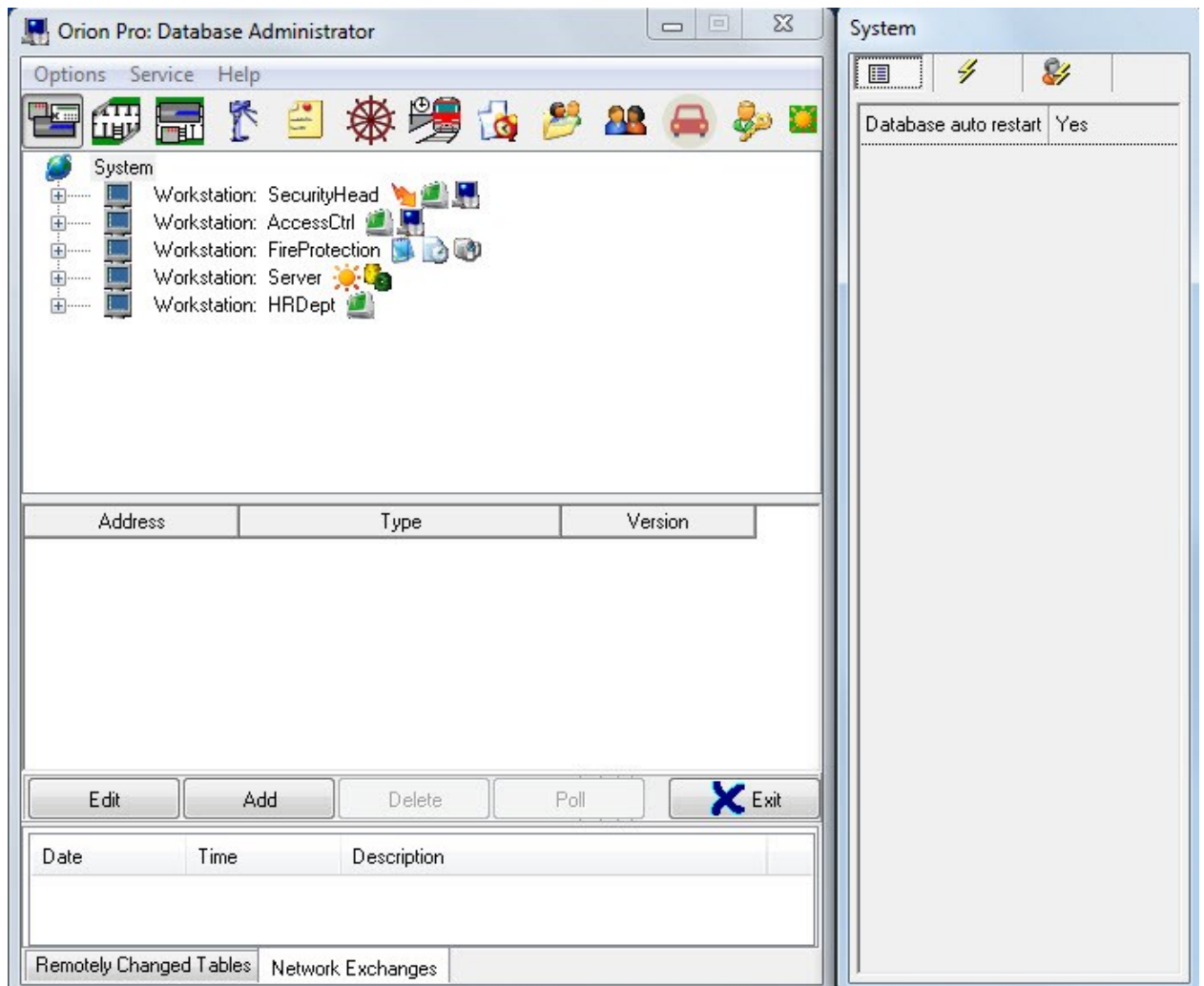
Delete all messages
Save to file

You can delete all messages from the Event Log or save events as a text file (\*.txt).

Attention! The Event Log can be hidden. Log viewing can be changed by the **Show Software Log Event** option in the Database Administrator settings (See chapter 6.14.1 Settings of Database Administrator).

## 6.2 Device Addresses. The Physical Structure of the System

When started, the Database Administrator shows its first tab - Device Addresses



The Device Addresses tab shows the following information:

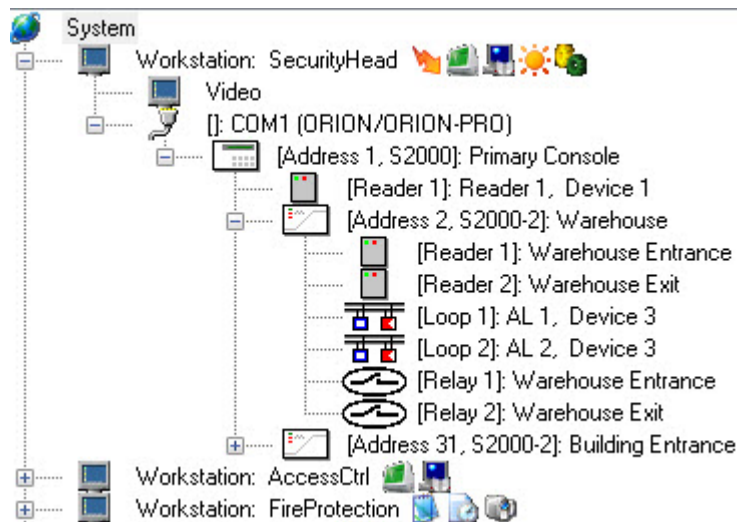
1. System tree
2. List of found devices.

The Physical structure of the system is defined in the Device Addresses tab:

- Types and properties of workstations and their network interactions;
- Quantity, ID numbers and properties of COM ports and Ethernet boards connected to a workstation;
- Quantity, types, addresses and properties of devices connected to a workstation;
- Types and properties of loops, addressable zones, supervised circuits, relay and supervised outputs of devices;
- Types and properties of workstation- connected video systems as well as cameras connected to these video systems.

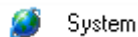
Entities and devices of the Orion system form a tree-like structure of interaction in the system. The main node is **System**, with workstations being added (connected) to this node. The **Workstation** is a node, to which COM ports, Ethernet adapters, and video systems are added, which in turn, becomes nodes for Devices and Cameras. The added Device includes as many readers, loops, and relay outputs as relevant for the type of Device.

Example:

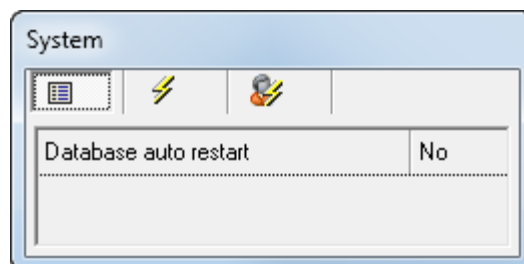


### 6.2.1 The System Entity

Initially, a clear database has only one entity, this is System. The System entity cannot be added or removed:



The System entity has only one property and no events:



Property	Selectable values	Descriptions
<b>Data base auto restart</b>	Yes/No	<p>When the connection to the Central Server fails and then recovers, and if the <b>Data base auto restart</b> property has:</p> <ul style="list-style-type: none"> <li>- <b>Yes</b>, the database information will be updated in System Shells, System Monitors and Scanning Cores on workstations where a connection failure occurred;</li> <li>- <b>No</b>, no actions will be performed.</li> </ul> <p><b>Yes</b> is default.</p>

## 6.2.2 The Workstation Entity (Computer)

One of the main system entities is Workstation (Computer).



Workstation:

In the tree of system entities, workstations are connected to the System entity.



As said above, COM Ports and Ethernet Adapters and Video Systems are connected to Workstations in the tree of entities:



In the tree of entities, the following is displayed for the Workstation entity:

- Name
  - Workstation: SecurityHead
- The list of Orion modules authorized to run on this workstation:
  - Scanning Core
  - System Monitor
  - Database Administrator (DBA)
  - Report Generator
  - Time and Attendance (T&A)
  - Central Server
  - Server Manager
  - Video System

To add a new Workstation (Computer) entity, select **System** in the tree and click the **Add** button. Further, set all properties of a new Workstation (except for **Options** that is to be edited after adding the entity) and press the **Save** button.

*Please keep in mind that **Options** of the Workstation entity can be set (edited) only after adding the entity to the system.*

To remove the Workstation entity, please select a required entity in the .Entities Tree and press the **Delete** button, and then confirm this action by pressing the **Yes** button in the appeared System Request dialog box.

*When you remove the Workstation entity all other entities associated to this entity will be also deleted: Video Systems, COM Ports, and Devices.*

The properties of the **Workstation** entity:

Workstation

Number	1
Name	SecurityHead
TCP\IP	192.168.20.3
Options	
Standby server IP	
Subscriber No:	SecurityHead
Alarm Handling	Yes
Temporary License Key	No
Screen Saver Timeout	60
Voice Notification	Yes
Sound Signal	3
Voice Notification Replays	6
Comments in Notification	Yes
Photo Display Time (s)	7
Remote Alarm Handling	No
Failover Support	Yes
Failover Delay	10
Failback Delay	10
Accumulate Statistics	No
Statistics Polling Interval	1000
Delta	5
Local Cache	Yes
Photo	Show always
Workstation Off-Line Notification	No
Automatically generate passage event	Yes
Automatically connect to keybox server	Yes

Properties	Possible Field Values	Description
Number (No)	1..2147483647	The unique index of a workstation in the system... <i>Attention! There cannot be two workstations with the same index in the system.</i>
Name	A string length of 1 to 15	Network name of a computer serving as a workstation in the system. Default value: blank (must be entered)
TCP\IP	A string length of 1 to 15to characters	IP address of a computer serving as a workstation in the system. Default value is 127.0.0.1

Options	<p><i>Refer to Chapter 6.2.2.1 The Options Property of Workstation. Defining Types of Workstations and Network Interaction Principles</i></p>	<p>The list of Orion Pro modules to run on this workstation.</p> <p>The list of workstations with their data displayed and their entities controllable on the current workstation.</p> <p><i>Attention! The <b>Options</b> property are not accessible immediately during adding an entity and can be accessible only when you further proceed with editing the entity (using the <b>Edit</b> button)</i></p> <p>Default settings: No software modules and workstation are selected in the checkbox.</p>
Failover Support	Yes / No	<p>This is used to define whether the Failover is supported by this workstation (redirecting of the Orion Pro software modules to the standby Central Server of the Orion Pro system if the connection to the primary Central Server fails.</p> <p><i>The failover support is further described in the 1. About the System and 4. Central Server Manager, and in 5. System Shell chapters.</i></p> <p>Default value: <b>No</b></p>
Standby Server IP	A length of 0 to 20 characters	<p>The IPaddress of a workstation with the installed standby Central Server where Orion Pro's modules running on the current workstation will be redirected in case of disconnection from the primary Central Server.</p> <p><i>Attention! If the <b>Failover support</b> is set as "<b>NO</b>", the <b>Standby server IP</b> option will be ignored and can have any value.</i></p> <p>Default value: blank</p>
Failover Delay	10..10000	<p>This is used to define the delay time (in seconds), during which an operator can cancel the redirection of the Orion Pro modules to the standby Central Server when the connection to the primary Central Server fails.</p> <p><i>Attention! If <b>Failover support</b> is set as "<b>NO</b>", the <b>Failover delay</b> option is ignored and can have any value</i></p> <p>Default value: 10</p>
Failback Delay	10..10000	<p>This is used to define the delay time (in seconds) during which an operator can cancel the automatic redirection (failback) of the Orion Pro modules back to the Primary Central Server when the connection is restored recovered.</p> <p><i>Attention! If <b>Failover support</b> is set as "<b>NO</b>", the <b>Failback delay</b> option is ignored and can have any value</i></p> <p>Default value: 10</p>

Local Cache	Yes/No	<p>This parameter enables the local (off-line) operation of the System Monitor and/or Scanning Core modules on the current workstation in case of disconnection from the Central Server, and further transmission of the offline operation changes to the database when the connection is restored.</p> <p><i>Attention! If the System entity has <b>No</b> for the <b>Database Auto Restart</b> parameter, events (occurred during disconnection period) will not be uploaded to the database when connection is restored.</i></p> <p><i>Attention. If neither Scanning Core nor System Monitor is selected to run on the workstation, the <b>Local cache option</b> is ignored and can have any value in this field.</i></p> <p><i>The use of Local cache is described in Parts 1. About the System and 5. System Shell.</i></p> <p>Default value: <b>No</b></p>
Workstation Off-Line Message	Yes/No	<p>This option defines where the System Monitor will display a connection failure message in a pop up window, when communications with a Scanning Core module of other workstation fails.</p> <p><i>Attention! If the System Monitor is not selected to run on the current workstation, this option is ignored and can have any value this field.</i></p> <p>Default value: <b>No</b></p>
Temporary License Key	Yes/No	<p>This option defines which license key will be used to start the Scanning Core module - permanent (No) or temporal (Yes)</p> <p><i>Attention! If the Scanning Core is not selected to run on the current workstation, this option will be ignored.</i></p> <p>Default value: <b>No</b></p>
Alarm Handling	Yes/No	<p>This is used to define whether to toggle the Alarms tab of the System Monitor module automatically when an alarm occurs.</p> <p><i>Attention! If the System Monitor is not selected to run on the current workstation, this property will be ignored regardless of its value</i></p> <p>Default value: <b>Yes</b></p>
Remote Alarm Handling	Yes/No	<p>This is used to define whether to toggle the <b>Alarms</b> tab of the System Monitor module automatically on the current workstation if an alarm occurs on other (remote) workstation.</p> <p><i>Attention! If the System Monitor is not selected to run on the current workstation, this property will be ignored regardless of its value</i></p> <p>Default value: <b>Yes</b></p>

ScreenSaver timeout	0..2000000000	<p>This defines the waiting time (in minutes) for a screen saver to start (If 0, a screen saver will not start) in the System Monitor,</p> <p><i>Attention! A screen saver in the System Monitor will be the same as selected in the Windows options. If <b>None</b> is selected for the screen saver in Windows, a screen saver will not start.</i></p> <p><i>Attention! If the System Monitor is not selected to run on the current workstation, this property will be ignored regardless of its setting.</i></p> <p>Default value: 60</p>
Photo	<p>Not show</p> <p>Show for a set time</p> <p>Show always</p>	<p>This is used to define how an employee's photo will be displayed in the System Monitor module.</p> <p><i>Attention! If the System Monitor is not selected to run on the current workstation, this property will be ignored regardless of its setting.</i></p> <p><i>For the details, see chapter 6.4.6. Configuring Display of a User Photo in System Monitors.</i></p> <p>Default value: <b>Show for a set time</b></p>
Photo Display Time (s)	0..4000000	<p>This is used to define (in seconds) how long the System Monitor module displays employee photos as driven by access events.</p> <p><i>Attention! If the System Monitor is not selected to run on the current workstation, or this property is not set as <b>Show for a set time</b>, the <b>Photo display time (s)</b> property will be ignored regardless of its setting.</i></p> <p>Default value: 7</p>
Voice Notification		<p>This is used to define whether to enable <b>Voice Notification</b> in the System Shell when alarms occur.</p> <p>Default value: No</p>
Sound Signal	1..6	<p>This is used to select the type of sound signal that precedes an alarm voice notification in the System Shell when an alarm occurs</p> <p><i>Attention! If <b>Voice Notification</b> is set as <b>No</b>, the <b>Sound signal</b> option is ignored regardless of its setting.</i></p> <p>Default value: 3</p>
Voice Notification Replays	0..2	<p>This is used to set how many times a voice notification will be replayed in the System Shell when an alarm occurs:</p> <p>1: 1 replay, 2: 2 replays, 0: a notification will be replayed continuously till the <b>Sound Off</b> button is pressed or new notification is received.</p> <p><i>Attention! If <b>Voice Notification</b> is set as <b>No</b>, the <b>Voice notification replays</b> option is ignored, regardless of its settings.</i></p> <p>Default value: 1</p>




Gather Statistics	Yes / No	<p>This is used to instruct Scanning Core to collect (and save in the database) statistics of ADC values of addressable sensors and loops connected to the current workstation.</p> <p><i>Attention! If the Scanning Core module is not selected to run on the current workstation, the <b>Gather Statistics</b> property is ignored regardless of its settings.</i></p> <p><i>You should keep it in mind that it has to be specified individually for each loop whether to gather statistics for it or not. (See Chapter 6.2.6.4 The Loop Entity)</i></p> <p><i>Default value: <b>No</b></i></p>
Statistics Polling Interval	100..2000000	<p>This is used to define polling interval for gathering ADC values (ms).</p> <p><i>For example, ADC values are collected for 4 addressable sensors where statistic pooling interval is set as 1000 ms (1sec), each of this sensor will be polled every 4<sup>th</sup> second.</i></p> <p><i>Attention! If the Scanning Core module is not selected to run on this workstation, or the <b>Gather statistics</b> parameter is set as <b>No</b>, the <b>Statistics polling interval</b> is ignored regardless of its settings</i></p> <p><i>Default value: <b>1000</b></i></p>
Delta	0..20	<p>This function defines the difference between the last database-recorded ADC value and the last received ADC value of an addressable sensor, and when this difference value is reached, it triggers recording the last received ADC value to the database.</p> <p><i>For example, If the Delta parameter has value 3 and the last database-recorded ADC values of some addressable sensor is 10, the next record of ADC value for this sensor will be made when its value is 7 (or lower) or 13 (or higher).</i></p> <p><i>If the <b>Delta</b> parameter is set as <b>0</b>, an ADC value will be always recoded after polling regardless whether it is changed or not.</i></p> <p><i>If the Delta is set as 1, the ACS values will be recorded each time when an ADC value is changed. E.g. If the ADC value of an addressable smoke sensor is 10, the next ADC value will be recorded to the database when it is different from 10.</i></p> <p><i>Attention! The <b>Delta</b> parameter is used for smoke addressable sensors <u>only</u>.</i></p> <p><i>Attention! If the Scanning Core module is not selected to run on this workstation, or the <b>Gather statistics</b> function is set as <b>No</b>, this parameter is ignored regardless of its settings.</i></p> <p><i>Default value: <b>5</b></i></p>

Automatically generate a passage event	Yes / No	<p>This parameter is used to instruct Scanning Core to generate passage event automatically, when an <b>Access Granted</b> event is received from a panel.</p> <p><i>Attention! This function is supported only by old panels: S20004 ver. 1.12 and older and S2000-2 ver. 1.02.</i></p> <p><i>Default values: <b>No</b></i></p>
Automatically connect to a keybox server	Yes / No	<p>This parameter defines whether to provided automatic connection to a keybox server.</p> <p>Default value: <b>Yes</b></p>

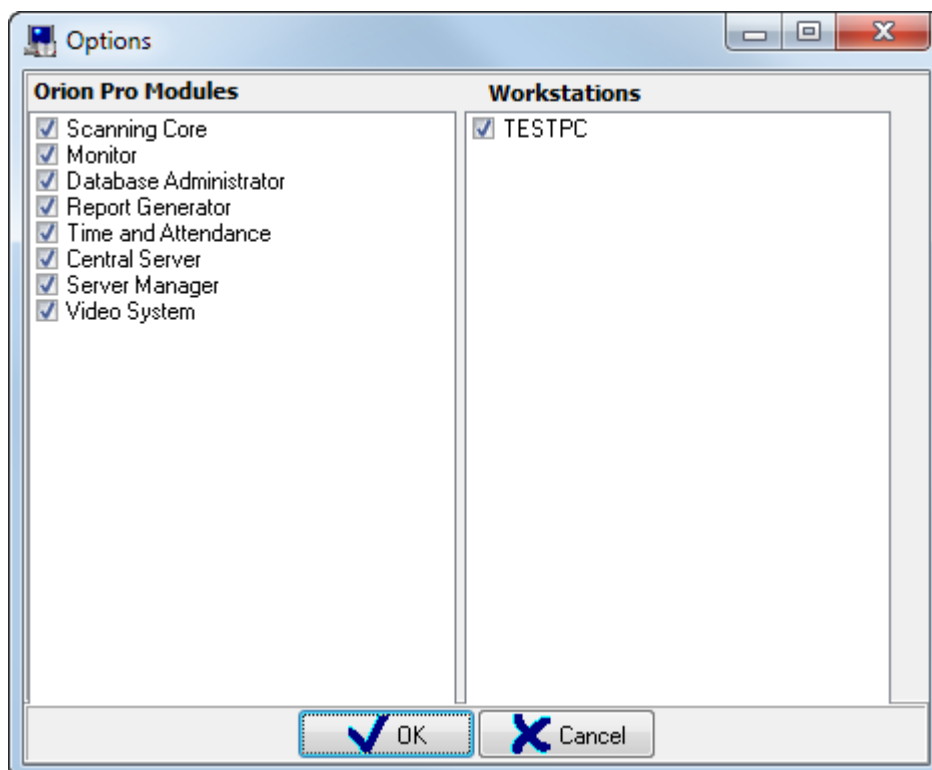
#### 6.2.2.1 The Options Parameter of Workstation. Defining the Interaction of Workstations in the Network

The Options parameter enables you to define the following settings of the Workstation:

1. The list of Orion Pro modules that will be run on the current workstation.
2. The list of Workstation that will transmit status data of devices and cameras connected to those Workstations: In other words, the action related to the selected workstation are as follows:
  - a. Transmission of events and entity states from the selected workstation to be displayed in the System Monitor of the current workstation.
  - b. Voice notification on alarms from a selected workstation will be played on the current workstation using a speech engine.
  - c. Management and control of entities of a selected workstation using the System Monitor on the current workstation.

Please keep in mind, that the Options parameter in not accessible right after the workstation is added to the system. It becomes accessible further when you proceed with editing. That is, you cannot edit the **Options** parameter till you first save the added Workstation entity; then you should press the **Edit** button to start editing parameters of the Workstation, and select **Options** in the **Inspector** dialog box and press button  to open the **Options** window.

The **Options** editing window is shown in the figure below:



The left pane of the window includes the Orion Pro software modules selectable for running on this workstation

The right pane of the window includes the list of workstations the information of those is to be transmitted to the current workstation.

*The **Workstations** list depends on a number of workstations in the system.*

*Important! The Video System (Video Server) module is actually is the driver of **Scanning Core** to provide the operation with video systems. Therefore, for those workstations where video integration is used, both the Scanning Core and Video System checkboxes have to be selected.*

Please, keep in mind that the transmission of events can be provided only for the workstations with System Monitor selected to run and only from those with Scanning Core modules selected. That is, in the **Options** of workstations (where System Monitors selected to run), you should select those workstations from the list of workstations (with Scanning Cores selected to run) that will transmit (share) information to the current workstation.

Transmission (Sharing) is not provided:

- For Workstations where the System Monitor Module is not selected to run, and
- From Workstations where Scanning Core is not selected to run

For Example:

Let's assume that we have a site that has the following security elements:



- FireProtection workstation to control a fire alarm and extinguishing system; the Scanning Core and System Monitor modules are selected to run on this workstation.
- AccessCtrl workstation to control intrusion detection and video surveillance systems
- SecurityHead workstation to control all system segments including capability of generating reports on all events. The scanning Core and System Monitor are selected to run on this workstation
- Server workstation to manage the Central Server and administer the database. The System Central Server, Database Administrator, and Central Server Manager are selected to run on this computer.
- HRDepartment workstation to maintain records of employees' time and attendance. The Time and Attendance module is selected to run on this workstation.



In our example, an operator working on the FireProtection workstation is responsible for controlling fire protection system. An operator working with AccessCtrl workstation is responsible for access control, intrusion detection, and video surveillance systems. The SecurityHead are responsible for control and supervision of the two above.

Therefore, the data from FireProtection and AccessCtrl workstations will be sent to the System Monitor running on the SecurityHead workstation. Thus, the Fire Protection and AccessCtrl workstations should be selected in the checkboxes in the **Options** parameter of the SecurityHead workstation:

Orion Pro Modules	Workstations
<input type="checkbox"/> Scanning Core	<input checked="" type="checkbox"/> SecurityHead
<input checked="" type="checkbox"/> Monitor	<input checked="" type="checkbox"/> AccessCtrl
<input type="checkbox"/> Database Administrator	<input type="checkbox"/> Server
<input checked="" type="checkbox"/> Report Generator	<input type="checkbox"/> HRDept
<input type="checkbox"/> Time and Attendance	
<input type="checkbox"/> Central Server	
<input type="checkbox"/> Server Manager	
<input type="checkbox"/> Video System	

As no events are transmitted to the FireProtection workstation from other workstation, the Options of this workstation will have the following selection:

Orion Pro Modules	Workstations
<input checked="" type="checkbox"/> Scanning Core	<input type="checkbox"/> AccessCtrl
<input checked="" type="checkbox"/> Monitor	<input type="checkbox"/> FireProtection
<input type="checkbox"/> Database Administrator	<input type="checkbox"/> Server
<input type="checkbox"/> Report Generator	<input type="checkbox"/> HRDept
<input type="checkbox"/> Time and Attendance	
<input type="checkbox"/> Central Server	
<input type="checkbox"/> Server Manager	
<input type="checkbox"/> Video System	

The same holds true for the AccessCtrl workstation, where no data are transmitted to:

Orion Pro Modules	Workstations
<input checked="" type="checkbox"/> Scanning Core	<input type="checkbox"/> SecurityHead
<input checked="" type="checkbox"/> Monitor	<input type="checkbox"/> FireProtection
<input type="checkbox"/> Database Administrator	<input type="checkbox"/> Server
<input type="checkbox"/> Report Generator	<input type="checkbox"/> HRDept
<input type="checkbox"/> Time and Attendance	
<input type="checkbox"/> Central Server	
<input type="checkbox"/> Server Manager	
<input checked="" type="checkbox"/> Video System	

Due to the same reason, no workstation is selected on the Server and HRDept workstation, but only software modules are selected.

Attention! As the above example explains, in addition to the transmission of status and events of entities from X workstation to Y workstation, it enables controlling entities of X workstation while working on Y workstation.

To manage operator rights to control the system entities, it is necessary to use software passwords with specific operators' access levels (see Chapter 6.10.5 Creating Access Levels for the System Monitor Operators. 6.12.1 Creating Passwords for the Software Modules).

In addition, you can limit the display of information in the System Monitor to make it individually available for each specific operator.

## 6.2.4 The COM Port Entity

When you have defined workstations for the system you should include devices connected to Scanning Cores.

The first step is to define which COM ports and Ethernet adapters will be used on workstations with the Scanning Core.

Let's discuss the COM Port entity of the system

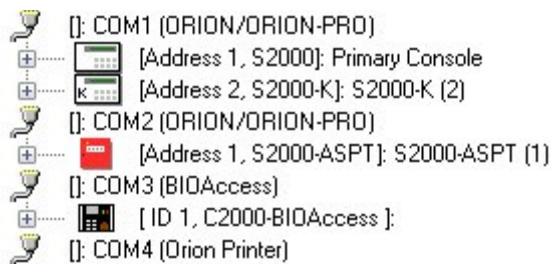


COM Ports are associated to the workstations in the system tree.



It is worth mentioning that if the COM Port (as well as devices) is added to the workstation, it is necessary to select Scanning Core in the **Orion Pro Modules** window to run the Scanning Core on this workstation.

As said above, the COM Port entity serves as a node accommodating devices:

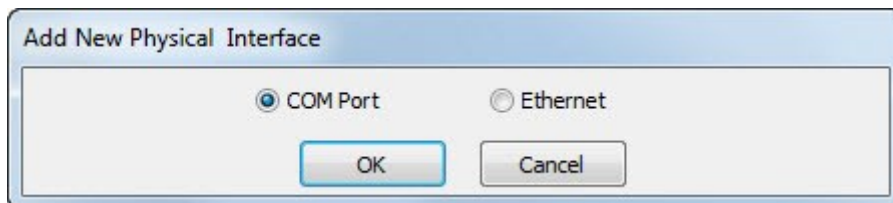


The COM Port entity shows the following information in the Tree:

- Number (Index).



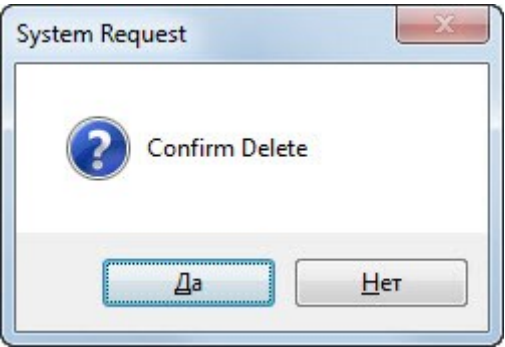
To add a new COM port, please select a required workstation in the Tree and press the **Add** button. Then, select **COM Port** in the appeared box and press **OK**:



Further, make necessary settings for all parameters of the new COM Port entity and click the **Save** button.

To edit the parameters of the **COM Port** entity, choose the required entity in the Tree and click the **Edit** button. Then, make necessary changes and press **Save**.

To delete a COM Port, select a required entity in the Entities Tree and press the **Delete** button. Then, confirm the delete action by pressing the **Yes** button in the appeared window.



When **COM Port** is deleted, all devices associated to this entity will be deleted as well.

COM Port:

Inspector

Port	1
Converter	Standard
Polling priority	Normal
Protocol	ORION/ORION-PRO


TCP\IP	192.168.20.3
--------	--------------

Parameters	Possible Values	Description
Port	1..256	<p>It must match a COM Port Number (to which devices are connected) in Windows OS.</p> <p>Default value: Minimum COM port number for available range (1...256) not used on the current workstation</p>
(Interface) Converter	Standard i7520 S2000	<p>This is a type of Interface converter used for converting RS-485 interface (than one that is Orion System based on) to RS-232 of the COM Port.</p> <p>If <b>Standard</b> is selected, the Scanning Core sends additional TX/RX (Transmit / Receive). This type should be selected if PI-GR Interface Converter is used.</p> <p>In case of S2000 Panel (or i7520), additional instructions will not be generated (improving data exchange rate and channel sustainability). These types are selected when converters with automatic TX/RX switch-over are used, e.g. S2000-PI interface Converter, S2000 or S2000M panels.</p> <p><i>Attention! This parameter is used for COM ports that operate under Orion/Orion Pro protocol.</i></p> <p>Default Value: No default value</p>

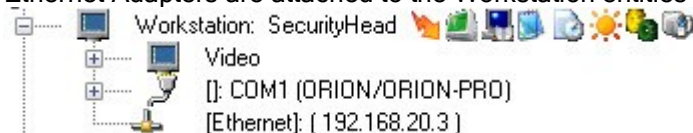
<b>Polling Priority</b>	Highest Very High High Normal Low Very Low Almost Stopped	Priority level for polling the COM Port by Scanning Core  Default: <b>Normal</b>
<b>Protocol</b>	Orion/Orion Pro BIOAccess Keybox UOP Dot-Matrix Display Orion Printer	Protocol of devices connected to the COM-Port  Default: No default values
<b>IP Address of Keybox Driver</b>	string in the following format: <b>XXX.XXX.XXX.XXX</b>	IP address of the computer where Keybox Driver is installed. It is recommended to run Keybox Driver on the same computer with Scanning Core. In this case, Keybox Driver will be started automatically. In case of remote operation the Keybox driver has to be started manually  Attention! This item is available only for COM ports using a Keybox protocol.  <i>Default value: 127.0.0.1</i>

## 6.2.5 The Ethernet Adapter Entity

Let's consider the Ethernet Adapter entity.



 [Адаптер LAN]

Ethernet Adapters are attached to the Workstation entities in the Entities Tree.




It is worth mentioning that if the E Port (as well as devices) is added to the workstation, it necessary to select the Scanning Core in **Orion Pro Modules** to run it on this workstation.

As said above, the COM Port entity is a node to which devices are connected:

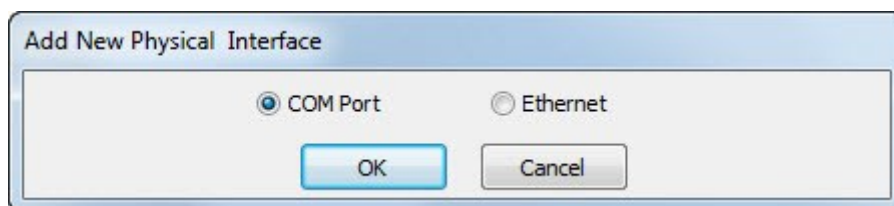
 [Ethernet]: ( 192.168.20.103 )  
 [ ID 1, C2000-BIOAccess ]:

Entities Tree shows the following information for the Ethernet Adapter entity:

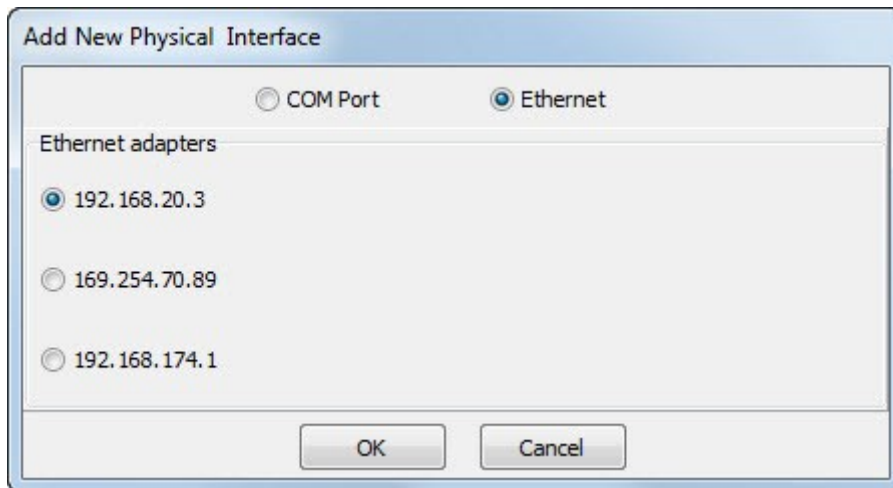
- IP Address.

 [Ethernet]: ( 192.168.20.103 )

To add a new Ethernet adapter, please select a required workstation and click **Add**. Then select **Ethernet** in the appeared box:



Then select a required Ethernet adapter from the list and press **OK**:



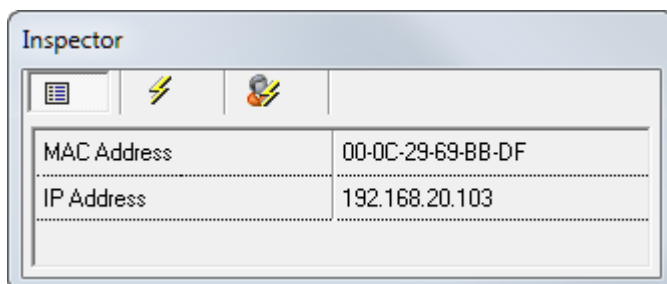
Then click **Save**.

To edit the parameters of the Ethernet Adapter, please select the Ethernet entity you need to configure and press the **Edit** button. Then make necessary changes and press the **Save** button.


To delete an **Ethernet** entity, select a required Ethernet entity in the Entities Tree and press the Delete button. Then confirm the delete action in the appeared dialog box by pressing the **Yes** button.

*When the Ethernet entity is deleted, all its associated devices will be deleted as well.*

Ethernet Adapter Properties:



Attributes	Possible Values	Description
<b>MACAddress</b>	Notation in the following format: XX-XX-XX-XX-XX-XX	MAC address of Ethernet adapter. Values are set automatically (*)
<b>IP Address</b>	Notation in the following format: XXX.XXX.XXX.XXX	IP address of Ethernet address Default: Values are set automatically

(\*) If you want to change the MAC Address, select the parameters and click the  button.




## 6.2.6 The List of Connected Devices. Orion and Orion Pro Protocols




When you have defined all system workstations, you should proceed with Devices connected to Scanning Cores. The first step is to decide what COM Ports will be used on workstations with installed Scanning Cores.

The second step is to add attach devices to COM Ports.


Let's consider the Devices entity.

 [address 1, S2000]: Panel

In the Entities Tree, the devices are added to the COM Port operating ORION/ORION PRO protocols.

 [COM1 (ORION/ORION-PRO)]  
 [address 1, S2000]: Panel  
 [address 2, S2000]: Panel 2

As said above, the Device entity includes the number of readers, loops, and relay outputs as relevant to the type of device:

 [Address 31, S2000-2]: Building Entrance  
[Reader 1]: Main Exit  
[Reader 2]: Main Entrance  
[Loop 1]: AL 1, Device 31 (1)  
[Loop 2]: AL 2, Device 31 (1)  
[Relay 1]: Main Exit (1)  
[Relay 2]: Main Entrance (1)

*Zones of a device are presented in the following order: **readers>loops>relay outputs***







*Association of devices, as well as properties of such entities as devices, readers, loops, and relay outputs will be considered further.*

The text below describes the process of setting the protocol in the Administrator Database for devices connected to any of the COM ports with ORION/ORION PRO Protocols.









*(See Chapters 1.2.2.1 Orion Protocol and 1.2.2.2 Orion Pro Protocol)*

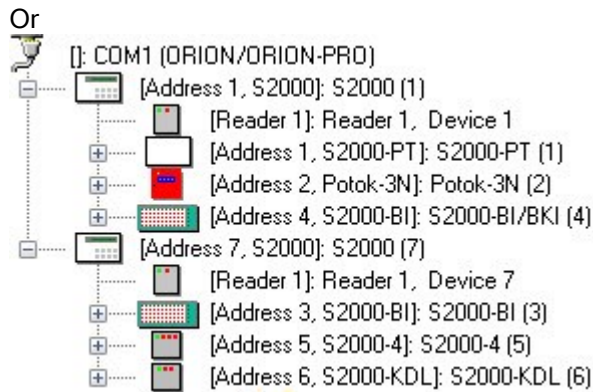
A protocol ensuring interoperability of the Scanning Core with COM-Port devices is set through the Entities Tree. That is

- If devices are added directly to COM Port, the protocol will be Orion:

 [COM1 (ORION/ORION-PRO)]  
 [Address 1, S2000-K]: S2000-K (1)  
 [Address 2, S2000-KS): S2000-KS (2)  
 [Address 3, S2000-BI): S2000-BI (3)  
 [Address 4, S2000-BI): S2000-BI/BKI (4)  
 [Address 5, S2000-4): S2000-4 (5)

- If devices are connected to S2000 and S2000M panels, the protocol will be Orion Pro:

 [COM1 (ORION/ORION-PRO)]  
 [Address 1, S2000): S2000 (1)  
[Reader 1]: Reader 1, Device 1  
 [Address 1, S2000-PT): S2000-PT (1)  
 [Address 2, Potok-3N): Potok-3N (2)  
 [Address 3, S2000-BI): S2000-BI (3)  
 [Address 4, S2000-BI): S2000-BI/BKI (4)  
 [Address 5, S2000-4): S2000-4 (5)  
 [Address 6, S2000-KDL): S2000-KDL (6)



### 6.2.6.1 Adding a Device to the List of Devices (Device Branch)

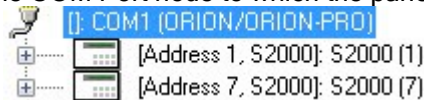
The Database Administrator enables you to create the list of workstation-connected devices manually (using the Add button), or to poll devices connected to the workstations with Scanning Cores, as well as generate the list of connected devices based on the data received directly from the PC COM Ports

#### 6.2.6.1.1 Adding Devices Manually

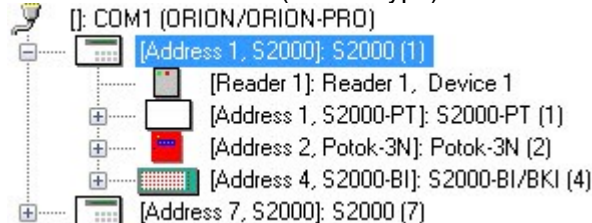
To add a new Device entity, please select a required nod in the Entities Tree and click the **Add** button. Then enter all necessary values for the new Device entity and click the **Save** button.

The selection of a node to add a device depends on a device type and protocols to be used

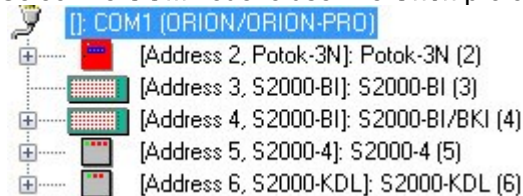
To add a S2000-type device (this type is selected for the S2000 and S2000M panels), please always select the COM Port node to which the panel will be added:



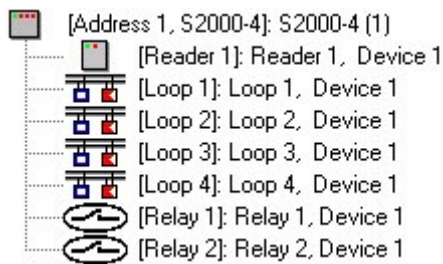
- To add all other types of devices:
  - Select the **Device** node ( S2000 type) to use the **Orion Pro** protocol:



- Select the **COM** node to use the **Orion** protocol:



As said above, the Device entity includes the number of readers, loops (input points) and relay outputs as relevant to the type of device:



The attributes and parameters of readers, loops, and relay outputs should be adjusted as required. It is worth mentioning, in most cases, types of loops and output relays have required values by default. However, there are some exemptions, if it is impossible to define proper values:

1. For devices such as S2000-4, Signal-20, Signal-20/ 02, Signal-20P, Signal-20M, and UO-4C, all **Loops** are set as an **Intrusion** type by default. In this, case you select the type of loop as defined in the settings of the physical device.
2. For devices such as S2000KDL, S2000-KDL-2I and S2000KDLS, the Element Type and Type parameters of any Zone (Loop) is defined as **Zone/Loop** and **Intrusion** respectively by default. In this case, you should select the type of loop as defined in the device's settings. In addition, for zones with addresses used for the S2000SP2 addressable relay modules, please select Relay for the **Element type** parameter and Addressable relay module for the **Type** parameter
3. By default, no S2000-KPB (Actuator Control Module) is specified for the devices such as the S2000-ASPT, therefore the inputs (loops ) and outputs of S2000-KPB' are not accessible. In this case, if one or more S2000-KPB devices are connected op S2000 ASPT, you should define their quantity and addresses in the **Connected S2000-KPB** field.
4. Ten (10) Intrusion loops are available for the Signal-10 device by default. To make threshold-addressable zones available, please select **Fire Threshold Addressable** type for the required loops (the first ten loops).

*The attributes and parameters of the Device, Reader, Loop and Relay Output entities are addressed in Chapters 6.2.6.2. The Device Entity, 6.2.6.3 The Reader Entity, 6.2.6.4 The Loop Entity, and 6.2.6.4 The Relay Output Entity.*

To change attributes of Device, Reader, Loop, and Relay Output, please select a required entity in the Entities Tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete the Device entity, please select the entity in the Tree and click **Delete**. Then confirm the delete actin by clicking the **Yes** button.

You cannot delete the Reader, Loop, and Relay Output. This will be done automatically when you delete the device.

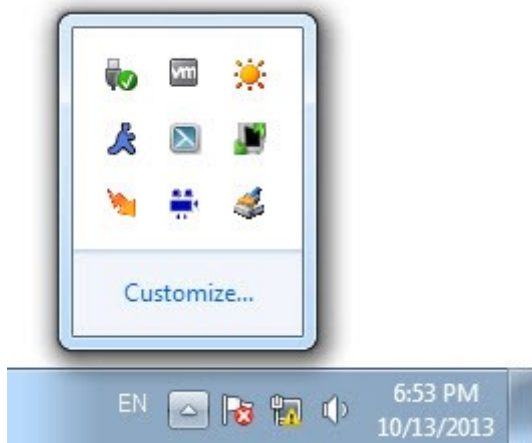
### 6.2.6.1.2 Polling Workstation-Connected Devices

The Database Administrator cannot work directly with COM ports of your PC.

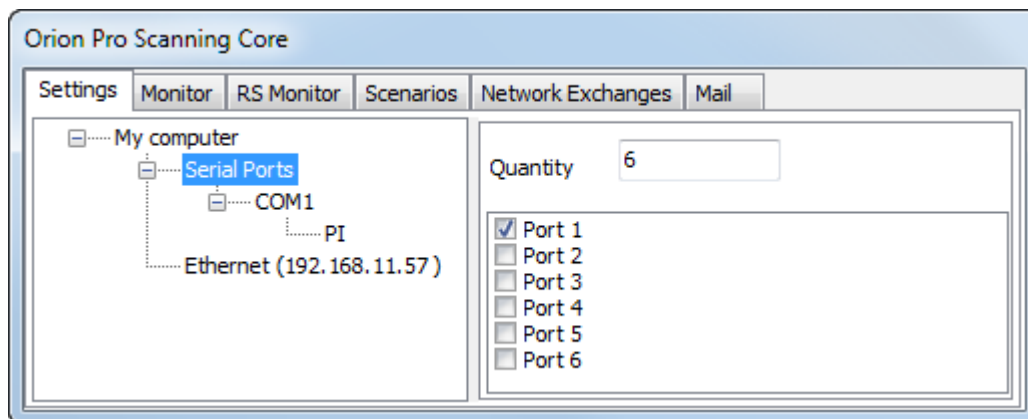
All actions related to configuring and searching devices are completed by Scanning Cores as instructed by the Database Administrator. Thus, to obtain the list of connected devices, you need to start the Scanning Core on the workstation; with the workstation's details have been already included in the database as described in *Chapter 6.2.2 The Workstation Entity* and in *Chapter 6.2.2.1 The Options Parameter. Defining the Interaction of Workstations in the Network*.

The Scanning Core is launched by the System Shell automatically. Start the Shell on the workstation with connected devices. The System Shell sets the connection to the System Central Server and receives the workstation parameters from the database. If the Scanning Core is selected to run on the current workstation the Scanning Core will be started automatically.

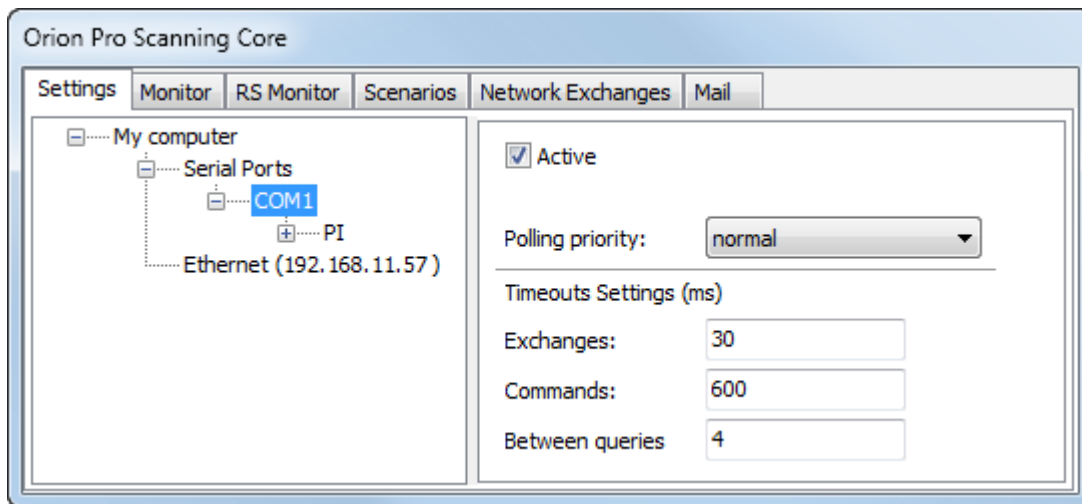
Find the icon of the Scanning Core Go in the system tray (right bottom of the screen) and open the application window by double click



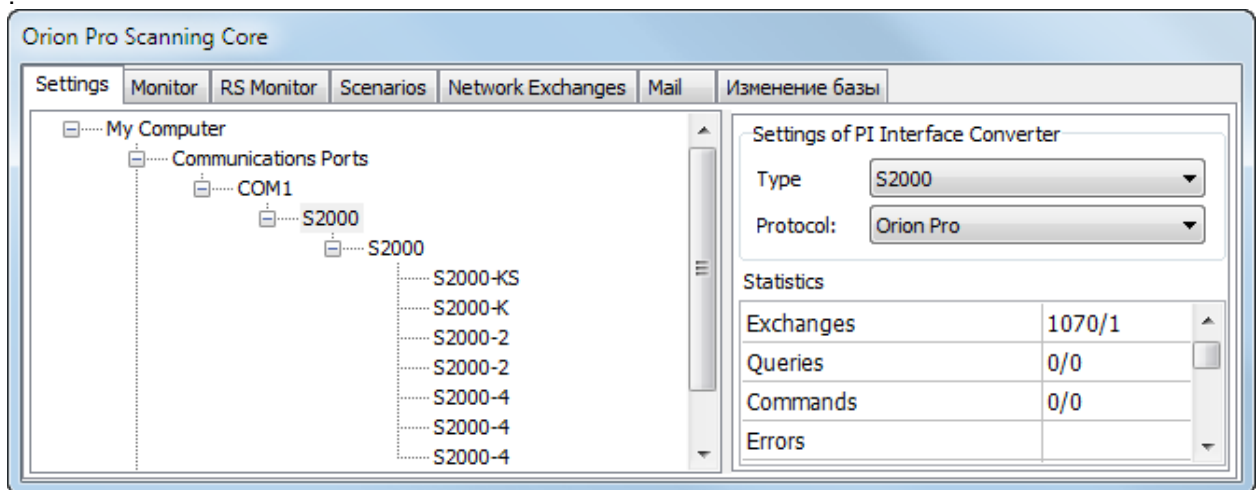
In the appeared window, go to the Settings tab and enable polling those ports where devices are connected.



Then, activate the COM ports and the Scanning Core will find devices connected to these ports



P.S. If the Orion Pro protocol is used and the Scanning Core is launched for the first time, please select the Orion Pro protocol rather than Orion protocol for the PI ( **PI Interface Converter** )



Let's come back to the Database Administrator. To obtain the list of found devices in the Database Administrator, please select the required workstation with running Scanning Core in the Entities Tree and click the **Poll** button

The bottom part of the main window will display the list of found devices with their network addresses. The arrangement structure of found devices is the same as in the Entities Tree (in respect to COM Port and Device entities and depends on the protocol used:

- Orion Pro

Address	Type	Version
Computer "VMVASILIEV", COM2		
1	S2000	2,05
7	S2000-KS	1,05
10	S2000-K	1,03
12	S2000-2	1,06
18	S2000-2	1,02
19	S2000-4	2,04
22	S2000-4	2,04

Orion:

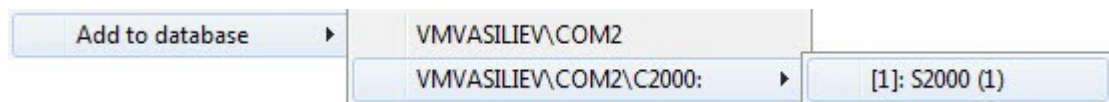
Address	Type	Version
Computer "VMVASILIEV", COM2		
7	Potok-3N	1.03
10	Signal-10	1.03
12	S2000-ASPT	3.00
18	S2000-BI	2.20
19	S2000-BI	2.20
22	S2000-4	2.04
24	S2000-BI rev. 01	1.01
31	S2000-2	1.15

To add a found device to the database, please select a device from the found devices and write click it to the **Add to database** item in the context menu, then select an entity in the submenu to add the device:

- **COM Port** - for S2000 panels with any protocol, as well as for all types of devices, if the Orion protocol is used:



- **S2000 panel** - for all types of devices but for the S2000 panels, if the Orion Pro protocol is used:



In this case, the S2000 panel must be assigned to the COM Port in advance.

You can select a few devices using the <Shift> key (Range Selection) and <Ctrl> (Combined Selection).

As said above, the Device entity includes the number of readers, loops, and relay outputs as relevant to the type of device by default:



The attributes and parameters of readers, loops, and relay outputs should be adjusted if required.

It is worth mentioning, in most cases, types of loops and output readers have required values by default, automatically. However, there are some exemptions, if it is impossible to define proper values:

1. For devices such as S2000-4, Signal-20, Signal-20/ 02, Signal-20P, Signal-20M, and UO-4C, all **Loops** are set as an **Intrusion** type by default. In this case, you select the type of loop as defined in the settings of the physical device.
2. For devices such as S2000KDL, S2000-KDL-2I and S2000KDLS, the **Element Type** and **Type** parameters of any Zone (Loop) is defined as **Zone/Loop** and **Intrusion** respectively by default. In this case, you should select the type of loop as defined in the device's settings. In addition, for zones with addresses used for the S2000SP2 addressable relay modules, please select Relay for the **Element Type** parameter and **Addressable** relay module for the **Type** parameter.
3. By default S2000-ASPT ver 2.xx and S2000-ASPT 3.xx do include connected S2000-KPB modules, therefore no relays and loops of these S2000-KPB modules are accessible. In this

case, if one or more the S2000-KPB devices are connected to S2000 ASPT ver 2xx or S2000 ASPTver 3.xx, they and their address must be defined in the **Connected S2000-KPB** field.

4. The Signal-10 device includes ten loops of Intrusion type by default. To make threshold-addressable zones available, please set a required loop(s) (first ten loops) as the **Fire Threshold Addressable** type (the first ten loops).

*The attributes and parameters of the Device, Reader, Loop and Relay Output entities are addressed in Chapters 6.2.6.2. The Device Entity, 6.2.6.3 The Reader Entity, 6.2.6.4 The Loop Entity, and 6.2.6.4 The Relay Output Entity.*

To change attributes of **Device**, **Reader**, **Loop**, and **Relay Output**, please select a required entity in the Entities Tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete the Device entity, please select the entity in the Tree and click **Delete**. Then confirm the delete action by clicking **Yes**.

You cannot delete the Reader, Loop, and Relay Output entities. They will be deleted automatically when you delete the device.



### 6.2.6.1.3 Transferring Devices

The Database Administrator offer capabilities of moving a device from one node (S2000 Panel or COM Port) to another (including nodes on another workstation).

For example, you can change the protocol with help of this action:

- Moving devices from S2000 Panel to COM Port will replace the Orion Pro protocol with the Orion protocol
- Moving devices form COM Port to S2000 Panel will replace the Orion protocol with the Orion Pro protocol

*It is highly **NOT** recommended moving a device from one workstation to another, if the device's entities (readers, loops, and relay outputs) are associated to system logical entities (partitions and partition groups) or management scenarios*

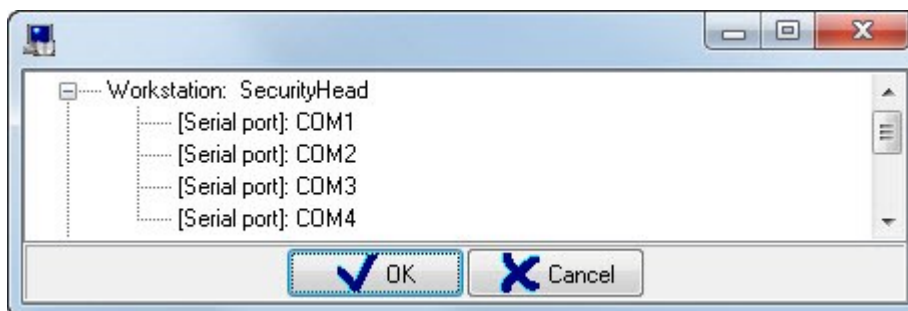
To transfer a device, please select a device in the Entities Tree, then choose **Service>Transfer..** in the menu. Then in the appeared box, select an entity to which you want associate the device in the following manner:

- COM Port: for S2000 panel with any protocol, as well as for all types of devices, if the Orion protocol is going to be used:
- S2000 panel - for all devices but for the S2000 panels, if the Orion Pro protocol is going to be used:

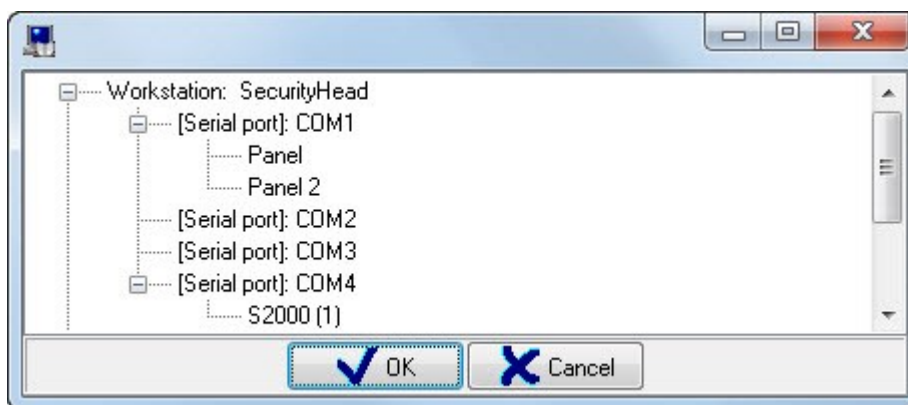
You can select a few devices at a time using the <Shift> key (Range Selection) and <Ctrl> (Combined Selection).

The selection of available devices depends on a type of device transferred:

- If the S2000 devices is transferred, it can be done to COM Port only:



- If any other device but for S2000 is transferred, it can be done to COM Port or S2000 either:



*Please keep in mind that the S2000 panel is transferred from one COM Port to another, all panel-associated devices will transfer together with the panel as well.*




6.2.6.2 The Device Entity

Above Chapter 6.2.6The List of Connected Devices. Orion and Orion Pro Protocols explains the location of the Device entity in the Entities Tree, as wells as how they can be added, edited and deleted. This chapter explains the information the Entities Tree shows for the Device entity and the properties of the this entity:

The Entities Tree shows the following information:

- Address
- Type
- Name

 [address 3, S2000-K]: S2000-K (3)

The Device's properties:

Inspector

Address	4
Device type	S2000-KDL
Index	4
Name	S2000-KDL (4)
Description	
Priority	Default
ContactID Zone	0


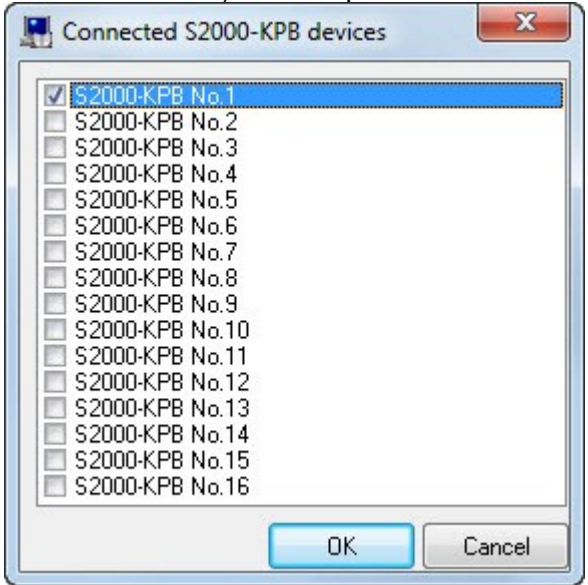
Transmission	
--------------	--

Time Zones	
Access Levels	

Connected S2000-KPB	
---------------------	--

Properties	Possible Values	Description
Address	1..127	<p>The address of the device.</p> <p>It must match the device's address for the RS 485 interface.</p> <p>The S2000's address depends on the protocol used: If the Orion Pro is used it must be RS-232 address; and if the Orion protocol is used, it must be an address for RS-485 interface.</p> <p><i>In highly recommended to set the same address for RS-232 and RS-485 interfaces in the S2000 Panel</i></p> <p>Default values:</p> <ul style="list-style-type: none"> <li>- a minimum address from the available range (1...127) not used for the current COM Port, when a device is added manually,</li> </ul> <p>The physical address of a device, if the device is added from the list of found devices</p>
Device Type	S2000, S2000-K, S2000-KS, S2000-BI, S2000-BI(2.23) S2000-BKI (2.20) S2000-BKI S2000-2 S2000-4 Signal-20 Signal-20 mod. 02 Signal-20P Signal-20P ver.2.04 Signal-20I Signal-10 S2000-KDL S2000-KDL-2I S2000-KDLS S2000-SP1 S2000-KPB S2000-ASPO S2000-ASPO ver.2.00 S2000-ASPO ver.3.00 S2000-PO Potok-3N Potok-3N ver.1.03 S2000-BI mod. 01 Rupor Rupor ver. 2.00 Rupor mod. 01 Rupor-200 S2000-IT UO-4S S2000-PGE BBPS-12 RS BBPS-12-2A RS BBPS-24-2A RS S2000-Adem S2000-PP	<p>Device Type.</p> <p><i>Value <b>S2000</b> is set for S2000 Panels and for S2000-M Panels as well.</i></p> <p><i>This parameter is accessible when a device is being added manually to the database</i></p> <p>Default values:</p> <p>Nothing, if a device is added manually</p> <p>An actual physical type, if a device is added from the list of found devices.</p>

<b>Index</b>	1..2147483647	<p>The unique number of a device in the system.</p> <p><i>Attention! The device is may be a biometric reader, subscriber, or dot-matrix display</i></p> <p><i>Default value: a minimum number from the available range (1..2147483647) of addresses not used in the system.</i></p>
<b>Name</b>	A length of 1 to 25 characters	<p>Device Name.</p> <p><i>Please keep in mind that the name length for the S2000 (S2000M) Panel cannot exceeds 16 characters. Thus, the longer name will be reduced to 16 characters if it is exported to the database.</i></p> <p>Default value: the name of a device with address in parentheses, e.g. S2000-K(1)</p>
<b>Description</b>	A length of 0 to 200 characters	<p>Comments.</p> <p><i>This field is optional.</i></p> <p>Default value: blank</p>
<b>Priority</b>	By default High Medium high Medium Medium low Low No polling	<p>Priority of polling by the Scanning Core module</p> <p>Default value: By default</p>
<b>Contact ID Zone</b>	0..2147483647	<p>Number of a device's Contact ID used for the event transmission to devices such as S2000-IT, UO-4S and S2000-PGE.</p> <p>Default value: 0</p>
<b>Transmission</b>	<p><i>(See 6.4.2. Configuring Transmission of Events and States of System Logical Entities)</i></p>	<p>Event Groups for transmission</p> <p>Partitions for transmission</p> <p><i>Attention! This property is available for devices such as S2000K, S2000-IT, UO-4S, or S2000-PGE exclusively, and only after a relevant device has been added to the database.</i></p> <p>Default value: No Event Group or Partition is selected</p>

<p><b>Connected S2000-KPB</b></p>	<p>(see the description of this parameter)</p>	<p>The list of device-connected S2000-KPB modules</p> <p>The connected S2000-KPB is edited in a dialog box opened by clicking the  button (visible if the this parameter is selected) in the Inspector:</p>  <p>Numbers of connected S2000-KPB devices have to match numbers of S2000-KPB devices specified in the configuration of the S2000-ASPT</p> <p><i>Attention! This property is available for devices such as S2000-ASPT exclusively, and only after a relevant device has been added to the database.</i></p> <p>Default value: No S2000-KPB module is selected</p>
<p><b>Time Zones</b></p>	<p>(See 6.12.4.2 Entering Time Zones and Access Levels to Controllers )</p>	<p>The list of time zones of the database and the list of time zones of a device.</p> <p><i>Attention! This property is available for devices such as S2000-2 and S2000-4 exclusively, and only after a relevant configuration has been read (from the cache or a device).</i></p>
<p><b>Access Levels</b></p>	<p>(See 6.12.4.2 Entering Time Zones and Access Levels to Controllers)</p>	<p>The list of access levels from the database and the list of access levels form a device.</p> <p><i>Attention! Attention! This property is available for devices such as S2000-2 and exclusively, and only after a relevant configuration has been read (from the cache or a device).</i></p>

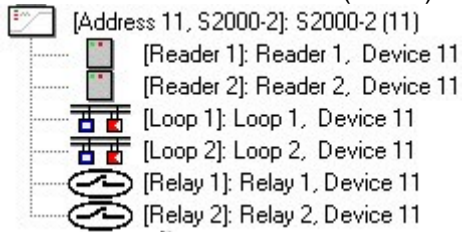
P.S. It is worth mentioning that when the Orion protocol is used, the S2000 panel is added to the database only for purpose of exporting a database configuration to the panel. But in such case, if the panel is always in the database, it will slow down the polling function of the Scanning Core as the Scanning Core is constantly attempting to found the missing device but the panel itself is operating in the PI-Backup Mode and does not respond to any commands (queries). Thus, it is strongly recommended setting the **Priority** property as **No polling** for S2000 panel in the database.

### 6.2.6.3 The Reader Entity

Let us discuss the Reader entity.

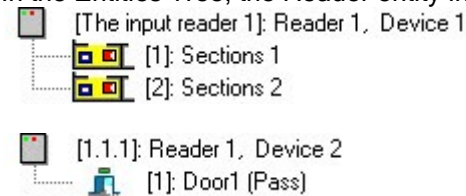


The Readers are associated (added) to the Devices in the Entities Tree.



*A Device's zones are displayed in the following order: readers>loops>relay outputs*

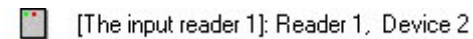
In the Entities Tree, the Reader entity includes partitions, partition group, and access points:



*See Chapter 6.4.3 Associating Control Elements to Readers of the System and Chapter 6.5.2.1. Associating Access Points to Readers and Device Relay Outputs*

The Entities Tree shows the following information for the Reader entity:

- Number
- Name.

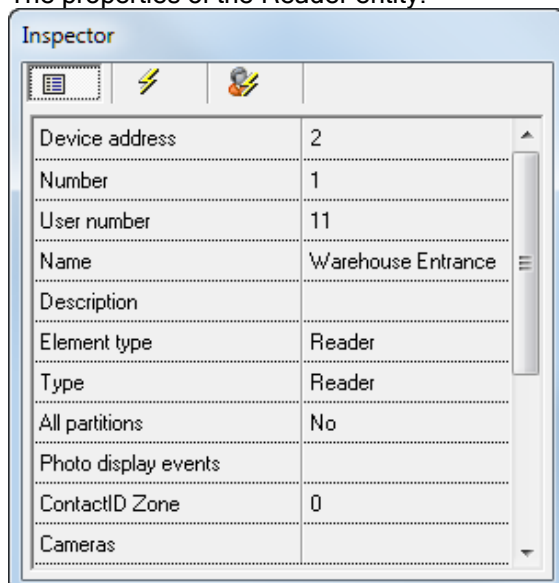


Please, be mindful that the Reader entity is added to the system by default when a relevant Device is added to the system.

The Reader is deleted by default when an associated Device entity is deleted from the system. Therefore, the Reader is subject to editing only.

To edit the Reader's properties, select a required entity in the tree and click the **Edit** button. Then make necessary changes in the properties as required and click the **Save** button.

The properties of the Reader entity:




Device address	2
Number	1
User number	11
Name	Warehouse Entrance
Description	
Element type	Reader
Type	Reader
All partitions	No
Photo display events	
ContactID Zone	0
Cameras	

Property	Possible values	Description
Device address	1..127	The address of a device to connect readers to. <i>This is not accessible for editing.</i> Value: a device address
Number (No)Homep	1..2	The number of a reader. <i>This is not accessible for editing.</i> Value: The Number (No) of a reader
User number	1..2147483647	The unique number of the device's entity in the system.  <i>Here, the Device's entity is understood as a reader, loop, relay output, and a subscriber zone. Thus, the User number must be unique for all of these specified entities: a reader, loop, and relay output and subscriber zone.</i>  <i>Default value: the minimum value from the available range (1..2147483647) not used in the system.</i>
Name	A length of 1 to 30 characters	The name of a reader.  Default value: a string including a reader name and device number. Example: Reader 1, Device 5
Description	A length of 1 to 200 characters	Comments  <i>Unnecessary to be filled</i>  Default value: no default values
Element type	Reader	Type of device entity.  <i>This is not subject for editing.</i>  Value: <b>Reader</b>
Type	Reader	Type of reader  Default value: <b>Reader</b>
ContactID Zone	0..2147483647	Reader's ContactID number used transmitting events to devices such as S2000-IT, UO-4S, and S2000-PGE.  Default value: 0
All partitions	Yes/No	Defines that all partitions are associated to this reader.  <i>(see Chapter 6.4.3 Associating Control Elements to Readers)</i>  Default value: <b>No</b>
Photo display events	<i>(see. 6.4.6 Configuring Display of Credential Holder's Photo in the System Monitors)</i>	Events that triggers display of employee's details (including a photo) related to an employee initiating such an event  This affects all the System Monitor modules running on various workstations in the system as a function of the Photo property for this workstations  <i>Default value: no events is selected.</i>
Cameras	<i>(See 6.4.7. Associating Cameras to Device Zones)</i>	The list of cameras with their video recorded as driven by the reader's alarm (external alarm recording mode must enable in cameras' settings).  This cameras can be displayed also if one selects the

		<b>Show video recording</b> item of the contextual menu of an reader alarm on the Alarms Tab  Default value: an blank list
--	--	--

#### 6.2.6.4 The Loop Entity

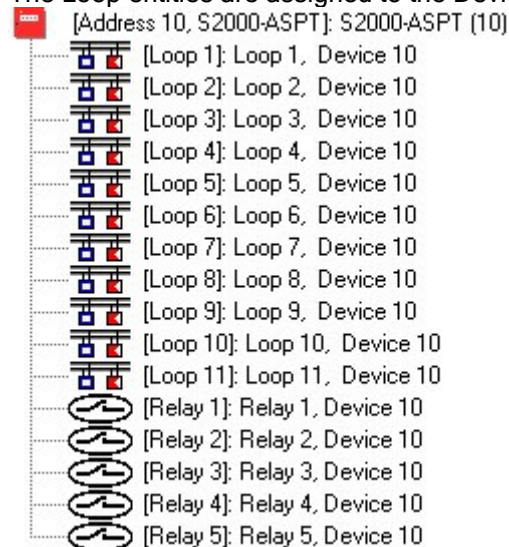
Let us consider the Loop entity:

 [Loop 1]: Loop 1, Device 10

The term Loop includes the following meanings:

- Loop (signaling input circuit),
- Addressable zone,
- Supervised circuit.


The Loop entities are assigned to the Device entities in the Entities Tree.



*The Device Zones are displayed in the following order: readers ->loops ->relay outputs.*

The Entities Tree shows the following information for the Loop entity:

- number,
- name,
- the number (ID) of a partition (ID) ( if a loop is added to any partition).

 [Loop 1]: Loop 1, Device 10

It is worth recalling that the Loop entity is added to the system by default when a relevant Device supporting loops is added to the system.

The Loop is deleted by default when an associated Device entity is deleted from the system. Therefore, the Loop is subject to editing only/

To edit the Loop's properties, select a required entity in the tree and click the **Edit** button. Then make necessary changes in the properties as required and click the **Save** button.

The properties of the Loop entity:

The Inspector window displays the following properties and values:

Device address	2
Number	1
User number	13
Name	AL 1, Device 3
Description	
Element type	Zone/Loop
Type	Entrance
24-hour zone	No
Accumulate statistics	No
Entrance zone timeout	1
ContactID Zone	0
Cameras	

Property	Possible values	Description
Device address	1..127	<p>The address of a device where a loop belongs</p> <p><i>This property is not editable.</i></p> <p>Value: Device address</p>
Number	1..127	<p>The number of a loop.</p> <p><i>This property is not editable.</i></p> <p>Value: Loop number</p>
User number	1..2147483647	<p>The unique number of the device's entity in the system.</p> <p><i>Here, the Device's entity is understood as a reader, loop, relay output, and a subscriber zone. Thus, the User number must be unique for all these specified entities: a reader, loop, and relay output and subscriber zone.</i></p> <p><i>Default value: the minimum value from the available range (1..2147483647) not used in the system.</i></p>
Name	A length of 1 to 30 characters	<p>The name of loop.</p> <p><i>Please keep in mind that the Loop's name cannot exceeds 16 characters in the S2000M panel. Thus, when the database is exported to the Panel a longer loop name will be shortened to 16 characters</i></p> <p>Default value: the name of a loop with a loop number and device address  <i>E.g: Loop 3, Device 12</i></p>
Description	A length of 1 to 200 characters	<p>Comments</p> <p><i>Unnecessary to be filled</i></p> <p>Default value: no default values</p>
Element type	Zone/Loop	Type of a device's entity



		<p><i>The can be edited only for the zones of S2000-KDL device</i>  <i>(See note 1 to this table)</i></p> <p>Value: Zone/Loop</p>
<p><b>Type</b>  <i>(see the description of this property)</i></p>		<p>The type of loop.</p> <p>This property defines conformity between logical (as in settings in the Orion Pro database) and actual (as in devices' settings). The properly selected type allows users to manage and accumulate addressable ADC values of addressable detectors, make management scenarios triggered by zone events, and to control extinguishing, etc.</p> <p>Possible values (Types of loops):</p> <ul style="list-style-type: none"> <li>Intrusion</li> <li>Entrance</li> <li>Panic button</li> <li>Fire</li> <li>Manual Release</li> <li>Smoke analog addressable</li> <li>Heat analog addressable</li> <li>Auxiliary</li> <li>Manual call point (Rupor)</li> <li>Door sensor circuit</li> <li>Manual call (ASPT)</li> <li>Pressure detector</li> <li>Auto Mode (Extinguishing)</li> <li>Main power supply</li> <li>Backup power supply</li> <li>Device mode</li> <li>Remote command</li> <li>Fire equipment fault monitoring</li> <li>Device status</li> <li>Mass</li> <li>Pressure</li> <li>First operating pump start</li> <li>First operating pump power</li> <li>Automatic control of the first operating pump</li> <li>Second operating pump start</li> <li>Second operating pump power</li> <li>Automatic control of the second operating pump</li> <li>Backup pump start</li> <li>Backup pump power</li> <li>Automatic control of the backup pump</li> <li>Jockey pump start</li> <li>Jockey pump power</li> <li>Automatic control of the jockey pump</li> <li>Closing electric valve</li> <li>Opening electric valve</li> <li>Electric valve power</li> <li>Main input of Automatic Transfer Switch</li> <li>Backup input of Automatic Transfer Switch</li> <li>Drencher curtain</li> <li>Main storage tank</li> <li>Backup tank</li> <li>Drain pit</li> <li>Start mode</li> <li>Start pressure sensor</li> <li>Manual start (Potok)</li> <li>Pressure in the system</li> <li>26 V power supply</li> <li>Status of the supervised circuit 1</li> <li>Status of the supervised circuit 2</li> </ul>

		<p> Status of the supervised circuit 3  Status of the supervised circuit 4  Status of the supervised circuit 5  Status of the supervised circuit 6  Status of the supervised circuit 7  Status of the supervised circuit 8  Status of the supervised circuit 9  Status of the supervised circuit 10  Status of the supervised circuit 11  Status of the supervised circuit 12  Status of the supervised circuit 13  Status of the supervised circuit 14  Status of the supervised circuit 15  Status of the supervised circuit 16  Status of the supervised circuit 17  Status of the supervised circuit 18  Output voltage  Output current  Battery test  Charger test  Mains power test  Programmable auxiliary  Ademco (Receiver)  Ademco (Radio repeater)  Fire Threshold Addressable  Humidity measurement  Output R1  Output R2  Output R3  Output R4  27 V power supply  Aggregate 1  Aggregate 2  Aggregate 3  Aggregate 4  Potok remote start  Alarm loop monitoring  Mains power supply (220V) monitoring  Charger monitoring  Battery monitoring  Remote Voice Announcement start monitoring  Device status monitoring  Limit switch </p> <p><i>(See Note 2 to this table)</i></p> <p>The default value depends on the type of parent device of this loop:</p> <p>Loops are set as <b>Intrusion</b> for devices such as S2000-4, Signal-20, Signal 20(02), Signal-20P, Signal-20M, UO-4S, S2000-KDL, S2000-KDLS, S2000-KDL-2I, and Signal-10.</p> <p>Loops for all other devices are set as in a physical device itself</p>
<b>24-hour zone</b>	Yes/No	<p>This option defines whether a loop will be disarmed when its partition is disarmed:</p> <ul style="list-style-type: none"> <li>- If <b>YES</b>, the loop will not be disarmed</li> <li>- If <b>NO</b>, the loop will be disarmed</li> </ul> <p>Default value: <b>No</b></p>
<b>Accumulate statistics</b>	Yes /No	This is used to instruct the Scanning Core module to

		<p>collect (and save in the database) statistics of ADC values of this loop.</p> <p>You should keep it in mind that it has to be specified individually for each workstation whether to gather statistics from the workstation-connected loops or not. (See Chapter 6.2.2 The Workstation Entity)</p> <p>Default value: <b>No</b></p>
<b>ContactID Zone</b>	0..2147483647	<p>The Number of ContactID Loop used to transmit events to devices such as S2000-IT, UO-4S, and S2000-PGE.</p> <p>Default value: 0</p>
<b>Entrance zone timeout</b>	1..2147483647	<p>Entrance timeout is the Entrance loop's delay of going from Entrance Zone Alarm status into Intrusion Alarm status.</p> <p><i>Attention. Attention this property is available only for the Entrance loop</i></p> <p>Default value: 0</p>
<b>Cameras</b>	(See 6.4.7. Associating Cameras to Device Zones)	<p>The list of cameras with their video recorded as driven by the loop's alarm (external alarm recording mode must enable in cameras' settings).</p> <p>This cameras can be displayed also if one selects the <b>Show video recording</b> item of the contextual menu of an alarmed loop on the Alarms Tab</p> <p>Default value: No cameras are listed</p>

#### Note 1:

It is worth mentioning that when S2000-KDL, S2000-KDLS and S2000-KDL-2I are added to the database, it was impossible to identify what two-wire addresses belongs to addressable detectors belongs and what belongs to addressable relay modules. By default, the **Element type** and **Type properties** are set as **Zone/Loop** and **Intrusion**, respectively for devices such as S2000-KDL, S2000-KDLS and S2000-KDL-2I.

In this case, you should select a type that corresponds the type of these loops in the devices settings. And in respect to a zone with addresses used for S2000-SP2, select **Relay** for **Element type** and **Addressable relay module** for the **Type** field.

You can edit Element type for the Loop and Relay Output entities only for the zones of devices such as S2000-KDL, S2000-KDLS and S2000-KDL-2I.

Please, keep in mind that a device's zones are shown in the Entities Tree as follows: readers>loops>relay outputs.

#### Note 2:

Configuration conformity between a logical loop (as set in the Orion Pro database) and an actual (as in devices' settings) loop is required on the following basis:

- The type of loop determines what commands can sent to this loop (individually or as part of a partition): **Arming**, **Disarming**, **Auto Mode ON**, **Auto Mode Off**, **Release**(extinguishant), **Abort Release**.  
This is very important, for example, for the **Panic button** loop; for the loops of devices as S2000-ASPT and Potok-3N responsible for fire extinguishing.  
Such command limitation is also effective for the control of a loop by the Operator of System Monitor and for the automated control of a loop (individually or as in part of partition) by the Scanning Core module

- The **Type** of loop defines loop events that can be renamed or used as triggers for automated system responses to zone events.
- If proper selection of the type of loop allows the Scanning Core module to provide a correct export of the Orion Pro database to the S2000 and S2000M panels. This very important for the Manual release loops that affect the ASPT and ASPT-A relay actions; for the loops of S200-SPT and Potok-3N responsible for fire extinguishing

In addition to the above, it is important to note the following:

There is an exception for the Entrance loop. In addition to the above, this type of loop offers event processing logic.

The Entrance Zone is an intrusion loop with an alarm delay - the delay of going to the **Intrusion Alarm** state from **Entrance zone alarm** state (the Entrance zone alarm is a status the loop goes to after it is opened in Armed Status). The alarm delay allows entering through the entrance zone (door) to disarm the protected area before a sound alarm (siren) is generated. A delay length may be 1 to 2, 147, 483, 647 seconds. When an entrance loop reports an alarm, Scanning Core generates the **Entrance Zone Alarm** event. If delay time goes out and the zone is still in an alarm state (in other words, it was not armed or disarmed), the Scanning Core module will generate Intrusion Alarm.

There are various relay action (or programs) to respond the **Intrusion Alarm** status and **Entrance Zone** status (see 6.A Centralized Relay Outputs Control Program). For example, relay output with a Siren relay action (program) will be not activated when a partition goes into the Entrance Zone Alarm status, and relay output with the **Alarm Output** program will not be opened.

Entrance zones assigned in the Orion Pro database affect only Tactics of relay outputs controlled with Scanning Core and do not affect relay outputs controlled locally by alarm control panels.

Attention! It is highly recommended to configure input loops locally in devices themselves (all devices of the latest revision support that). But for the legacy devices that do not allow setting the input loops local, the outputs can be configured at the level of the Orion Pro software.

If a loop is configured as Entrance in the devices, it should be set as Intrusion in the Orion Pro database.

Please review what commands are allowed for various types of loops (\*):

Type of Loop	Actions						
	Arming	Disarming	Alarm Reset	Enable Auto Mode	Disable Auto Mode	Activate Extinguishing	Abort Extinguishing
Intrusion	✓	✓	✓	✗	✗	✗	✗
Entrance	✓	✓	✓	✗	✗	✗	✗
Panic button	✓	✗	✓	✗	✗	✗	✗
Fire	✓	✓	✓	✗	✗	✗	✗
Manual Call Point	✓	✓	✓	✗	✗	✗	✗
Smoke Analog Addressable	✓	✓	✓	✗	✗	✗	✗
Heat Analog Addressable	✓	✓	✓	✗	✗	✗	✗
Hydrometrical	✓	✓	✗	✗	✗	✗	✗
Fire Threshold Addressable	✓	✓	✓	✗	✗	✗	✗
Loop Supervision	✓	✓	✗	✗	✗	✗	✗
Manual Activation (Rupor)	✓	✓	✗	✗	✗	✗	✗
Manual Release (ASPT)	✓	✓	✗	✗	✗	✗	✗

Pressure Detector	✓	✓	✗	✗	✗	✗	✗
Auto Mode (fire extinguishing)	✗	✗	✗	✓	✓	✗	✗
Device Mode	✗	✗	✗	✗	✗	✓	✓
Remote Release Command	✓	✓	✗	✗	✗	✓	✓
Remote Release (Potok)	✗	✗	✗	✗	✗	✓	✓
Remote Voice Alarm Control	✓	✓	✗	✗	✗	✗	✗

(\*) No commands are sent for other loops (including Auxiliary and Manual release (Potok))

It is recommended using the following types of loops for zones defined in the settings of system controllers:

- For loops of devices such as S2000-2, S2000-4, Signal-20, Signal-20 ver02, Signal-20P, Signal-20 ver.2.04, Signal 20M, Signal-10, S2000-KDL, S2000-KDLS, S2000-KDL-2I, and UO-4S:

Type of Zone in Device	Type of Loop in Orion Pro Software Suite
1 - Smoke	Fire
2 -Combined Loop	Fire Manual Release
3 - Heat Loop	Fire Manual Call Point
4 - Intrusion Loop	Intrusion
5 - Intrusion with tamper control	Intrusion
6 - Auxiliary	Auxiliary
7 -Entrance	Intrusion
8 -Smoke threshold addressable	Smoke analog addressable
9 -Heat smoke threshold addressable	Heat analog addressable
10 - Heat thermostatic	Heat analog addressable
11 - Panic	Panic button
12 - Programmable auxiliary	Programmable auxiliary
14 - Fire threshold addressable	Fire threshold addressable
15 - Hydrometrical	Hydrometrical

The types of loops for S2000-KPB, S2000-ASPT, and S2000-ASPT ver. 2.00, Potok-3, Rupor, and Rupor-200 are defined by default when there are added to the database. It is not recommended changing the types of these loops, unless a specific situation is required.

#### 6.2.6.5 The Relay Output Entity

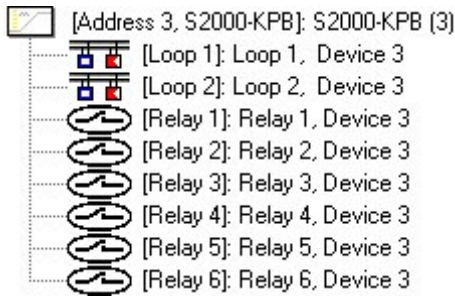
Let's consider the Relay Output entity.



The term *relay output* means the following:

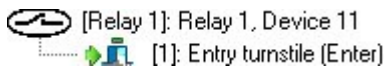
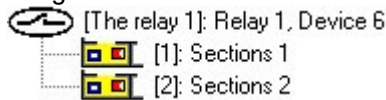
- Relay output,
- Supervised (monitored) output
- Addressable relay module.

Relay outputs are associated to the Device entities.



*The device's zones are displayed in the following manner: readers ->loops>relay outputs.*

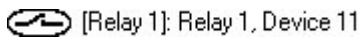
In the Entities Tree, Relay Output is the entity to which partition, partition groups, and access points are assigned:



*See Chapter 6.4.1 Setting Centralized Control of Relay Outputs and Chapter 6.5.2.1 Associating Access Points to Relay Outputs of Devices.*

The Entities Tree shows the following information for the Relay Outputs:

- Number,
- Name
- Partition number (if a relay output is added in any partition).






It is worth mentioning again that the **Relay Output** entity is added to the system by default when a relevant Device supporting relay outputs is added to the system.

The Relay output is deleted by default when an associated Device entity is deleted from the system. Therefore, the Loop is subject to editing only/

To edit the Relay properties, select a required entity in the tree and click the **Edit** button. Then make necessary changes in the properties as required and click the **Save** button.

The properties of the Loop entity:

**Inspector**

Device address	31
Number	1
User number	6
Name	Main Exit
Description	
Element type	Relay
Type	Relay
Centralized control	No
Tactics	Not manage
Relay action delay	0,000
Relay action time	0,000
ContactID Zone	0
Cameras	

Property	Possible values	Description
Device Address	1..127	<p>The address of a device where a relay output belongs</p> <p><i>This property is not editable</i></p> <p>Value: Device Значение: адрес прибора</p>
Number	1..127	<p>Number of relay output.</p> <p><i>This property is not editable</i></p> <p>Value: number of relay output</p>
User number	1..2147483647	<p>The unique number of the entity of a device in the system</p> <p><i>In this case the entity of devices may be a reader, loop, relay output and a subscriber zone. The user number must be unique for each of the device's entities: a reader, loop, relay output and subscriber's zone.</i></p> <p>Default value: the minimum number from the available range(1..2147483647) of number used in the system</p>
Name	A length of 1 to 30 characters	<p>The name of relay output.</p> <p><i>One should keep in mind, that a name's length cannot be longer than 16 characters. The longer names will be shortened to 16 characters when the database is exported to the panel (Console)</i></p> <p>Default value: a string including relay number and a device's address</p>

<b>Description</b>	A length of 0 to 200 characters	Comments. <i>Optional field</i> Default value: a blank field
<b>Element type</b>	Relay	Type of device's entity.  <i>This field is allowed to be edited only for zone (inputs) of S2000-KDL, S2000-KDLS, S2000-KDL-2I</i>  <i>(See Note 1 to the table)</i>  Value: Relay
<b>Type</b>	(see description)	Type of relay output  This defines conformity between logical (as set in the Orion Pro database) and actual (as a function of the device itself) type of relay output.  Available outputs:  Relay Addressable Relay Module Supervised Output KPB Output (ASPT) Visual Alarm1 (ESCAPE) Visual Alarm 2 (KEEP OUT)» Visual Alarm 3 (Auto OFF)» Audible Alarm (Siren) Release Circuit Start 1 Start2 Start 3 Start 4 Voice Alarm/Notification Valve , Addressable Valve Control Output  <i>Attention! It is not recommended changing the type of relay output defined by default when devices are added to the tree. The exemptions are zone (inputs) of S2000-KDL, S2000-KDLS, and S2000-KDL-2I</i> <i>(See Note 2)</i>  Default value depends on the type of device where a relay output belongs
<b>Contact ID Zone</b>	0..2147483647	The Number of ContactID Relay Output used to transmit events to devices such as S2000-IT, UO-4S, and S2000-PGE.  Default value: 0
<b>Centralized Control</b>	Yes / No	This property defines whether a relay is controlled by S2000/S2000M Panel (local control) or by the Scanning Core of the Orion Pro Suite (central control) <ul style="list-style-type: none"> <li>• If <b>Yes</b>: the relay output is controlled by the Scanning Core module; the centralized control settings for this output is not exported to the S2000/S2000M panel</li> <li>• If <b>No</b>: the Scanning Core module does not control the relay output but the thesentrized control settings for the output are expotered to the S2000/S2000M panel (that is actually</li> </ul>



		<p>control the output )</p> <p><i>Attention! this property are available only for the types of relay that supports the Centralized control (the Notes 2 to the table)</i></p> <p>This property is relevant for the <b>Orion Pro</b> protocol only.</p> <p>If the Orion protocol is used, a relay output will be controlled centrally (regardless of this field settings) by the Scanning Core module. Bu this centralized control settings will exported only when this property is set as <b>No</b>  <i>Please keep it in mind, that centralized control only can be provide only if the output is not controlled locally</i></p> <p>See Chapter 6.4.1 Setting Relay Output Centralized Control</p> <p>Default value: <b>No</b></p>
<b>Tactics</b>	<i>(see the Description of property)</i>	<p>This is to define a relay action (program) of centralized control for a system output.</p> <p><i>Attention! This property is available only for the types of relay outputs that support the centralized control (see Appendix 2 to the table)</i></p> <p>Available relay programs/actions:</p> <ul style="list-style-type: none"> <li>No control</li> <li>Switch On</li> <li>Switch Off</li> <li>Switch On for a Time</li> <li>Switch Off for a Time</li> <li>Blink (Off is Initial Position)</li> <li>Blink (On is Initial Position)</li> <li>Blink for a Time (Off is Initial Position)</li> <li>Blink for a Time (On is Initial Position)</li> <li>Lamp</li> <li>Alarm Output 1</li> <li>ASPT</li> <li>Siren</li> <li>Fire Output</li> <li>Fault Output</li> <li>Fire Lamp</li> <li>Alarm Output 2</li> <li>Switch On for a Time before Arming</li> <li>Switch Off for a Time before Arming</li> <li>Switch On for a Time upon Arming</li> <li>Switch Off for a Time upon Arming</li> <li>Switch On for a Time upon Disarming</li> <li>Switch Off for a Time upon Disarming</li> <li>Switch On for a Time if Arming Failed</li> <li>Switch Off for a Time if Arming Failed</li> <li>Switch On for a Time upon Auxiliary Alarm</li> <li>Switch Off for a Time upon Auxiliary Alarm</li> <li>Switch On upon Disarming</li> <li>Switch Off upon Disarming</li> <li>Switch On upon Arming</li> <li>Switch Off upon Arming</li> <li>Switch On upon Auxiliary Alarm</li> <li>Switch Off upon Auxiliary Alarm</li> </ul>

		ASPT-1 ASPT-A ASPT-A1 Switch On if Temperature Increased Switch On if Temperature Decreased Switch On if Extinguishing Initiation Delayed Switch On if Extinguishing Initiated Switch On if Extinguishing Confirmed Switch On if Extinguishing Failed Switch On if Auto Mode Enabled Switch Off if Auto Mode Enabled Switch On if Auto Mode Disabled Switch Off if Auto Mode Disabled  <i>The detail description of all relay actions (programs) are provided in Appendix 6.A see Centralized Control of Relay Outputs</i>  Default value: No Control
Relay action delay	0..8191,875	Pause before the initiation the a relay's action (programs) in seconds (the increment step is 1/8 second).  <i>Attention! This is available only for those type of relay outputs that support the centralizes control option (See Note 2 thereafter)</i>  Default value: 0
Relay action time	0..8191,875	The time in seconds during which relay action program completes (increment step is 1/8 of second)  <i>Attention! This is available only for those type of relay outputs that support the centralizes control option (See Note 2 thereafter)</i>  Default value: 0
Cameras	(см. главу «6.4.7 Привязка камер к зонам приборов»)	The list of cameras with recording as triggered by relay output alarms ( external alarm triggering mode must be activated for the cameras) These camera will be also displayed o if one selects the <b>Show video recording</b> item of the contextual menu of an alarmed loop on the <b>Alarms</b> tab  Default value: No cameras on the list

#### Note 1

When S2000-KDL, S2000-KDLS and S2000-KDL-2I are added to the database, it is impossible to identify what addresses of a two-wire circuit belongs to addressable detectors and what belongs to addressable relay modules. By default, the **Element type** and **Type properties** are set as **Zone/Loop** and **Intrusion**, respectively for devices such as S2000-KDL, S2000-KDLS and S2000-KDL-2I.

In this case, the zones of S2000-SP2 addressable module must have a **Relay** option selected for the **Element type** field and **Addressable relay module** selected for the **Type** field.

*Based on the above, the reverse conversion of an output to a loop are allowed for the devices such as S2000-KDL, S2000-KDLS, and S2000KDL-2I*

*relay* You can edit *Element type* for the *Loop* and *Relay Output* entities only for the zones of devices such as *S2000-KDL*, *S2000-KDLS* and *S2000-KDL-2I*. outputs.

Please, note that a device's zones are shown in the **Entities Tree** as follows: readers>loops>relay output















### **Note 2**

The need for proper **conformity** between logic(as set in the Orion Pro database) and actual (physical device's relay output)types of relay output isrequired to provide for the following:

- A type of relay output defines whether the output is the subject to the centralized control.
- The type of output defines the output events than can be renamed or used to associate management scenarios as system response to zone events.

Attention! It is not recommended changing the default type of relay output but for the zones of the S2000-KDL.

*Relay outputs that support centralized control are as follows:*

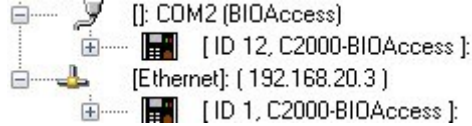
Type of Relay Output	Centralized Control
Relay	
Addressable Relay Module	
Supervised Output	
KPB Output (ASPT)	
Visual Alarm1 (ESCAPE)	
Visual Alarm 2 (KEEP OUT)	
Visual Alarm 3 (Auto OFF)	
Audible Alarm (Siren)	
Release Circuit	
Start 1	
Start 2	
Start 3	
Start 4	
Voice Alarm	

### 6.2.7 The List of Connected Biometric Readers

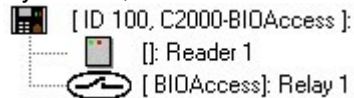
Let's discuss the Biometric Reader entity:

 [ ID 1, C2000-BIOAccess ]:

Biometricreader is associated to the COM Ports with the BIOAccess protocols or to Ethernet Adapters.



By default, the Biometric Reader entity has an assigned reader and relay output:



The list of workstation-connected biometric readers is made manually

To add the Biometric Reader, please select a required node (COM Port and Ethernet Adapter) and click the **Add** button. Then enter values in for all property of the new Biometric Reader and click the **Save** button.

You can edit the properties of readers, loops and relay outputs of the added biometric readers

The properties of The Biometric Reader, Relay Outputs and described in Chapter 6.2.7.1 *The Biometric Reader*, Chapter 6.2.6.3 *The Reader Entity*, and Chapter 6.2.6.5 *The Relay Output*

To edit the properties of a Biometric Reader, Reader or Relay Output, please select a required entity in the Entities Tree and click the **Edit** button. Then make necessary changed and click the **Save** button.

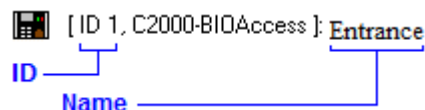
To delete the Biometric Reader entity, please select a required entity in the Entities Tree and click the **Detete** button. Then click **Yes** to confirm a delete action in the appeared dialog box.

#### 6.2.7.1 The Biometric Reader Entity

The above chapter discusses the location of Biometric Reader in the Entities Tree as well as actions related to adding, editing, and deleting of the entity. Hence this chapter focuses on the Biometric Reader' properties and information displayed for thi entity in the tree.

The Entities Tree displays the following information for the Biometric Reader entity:

- ID,
- Name.



The properties of the Biometric Reader:

**Inspector**

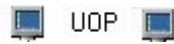
Device type	S2000-BIOAccess
Device ID	1
Name	
Description	
Fingerprint Enrolment	No
Device Polling	No
IPAddress	
IPPort	1
ContactID Zone	1

Property	Possible Values	Description
<b>Device Type</b>	S2000-BIOAccess»	Type of biometric reader <i>This parameter is not editable.</i> Default value: S2000-BIOAccess
<b>Device ID</b>	1..255	Device ID for a com-port connected biometric reader must comply with ID set in the physical device. It should be noted that maximum value for ID in a device is 255, and one COM Port can accommodated up to 31 biometric readers  Device ID for an Ethernet-connected reader is used only to facilitate configuring a device in the Database Administrator module. It may not match the physical device's ID.  Default value: - When added to a com port, the default value will be the minimum ID from the available range (1...255) not used on the current COM-port.  -When added to an Ethernet port, the default value for ID of biometric reader will be the minimum ID from the available range(1..255) of IDs not used on the current Ethernet adapter.
<b>IP Address</b>	Notation in format XXX.XXX.XXX.XXX	The IP Address of Biometric reader.  <i>Attention! This property is displayed and used only for a biometric reader connected to an Ethernet adapter.</i>  Default value: 0.0.0.0
<b>IP Port</b>	1..65534	The IP port of a biometric reader.  <i>Attention! This property is displayed and used only for a biometric reader connected to an Ethernet adapter.</i>  Default value: 4370
<b>Index</b>	1..2147483647	The unique number of a device in the system.

		<p><i>Attention! The device means: device, biometric reader, subscriber, dot-matrix display</i></p> <p>Default value: the minimum value from the available range (1..2147483647) not used in the system.</p>
<b>Name</b>	A length of 1 to 25 characters	<p>The name of a biometric reader.</p> <p>Default value: empty field</p>
<b>Description</b>	A length of 0 to 200 characters	<p>Comments</p> <p><i>Optional field</i></p> <p>Default value: empty field</p>
<b>Fingerprint Scanner</b>	<b>Yes/No</b>	<p>This property defines whether to use this biometric reader to record new fingerprints.</p> <p><i>This property is used only in the DBA module when a biometric reader is selected to scan new fingerprint.</i></p> <p>Default value: <b>No</b></p>
<b>Contact ID Zone</b>	0..2147483647	<p>The Number of ContactID biometric reader used to transmit events to devices such as S2000-IT, UO-4S, and S2000-PGE.</p> <p>Default value: 0</p>

### 6.2.8. The List of Connected UOPs

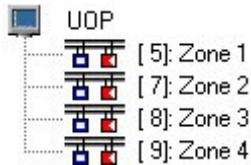
Let's discuss the Subscriber (UOP) entity.



The Subscriber entities are associated to COM ports with UOP protocols.



A Subscriber's zones are associated to the Subscriber entity in the tree:



The subscribers are added to workstations only manually.

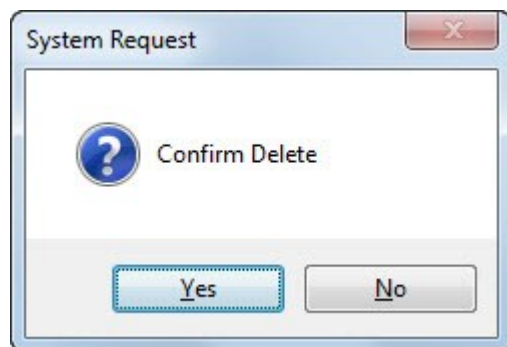
To add the Subscriber, please select a required node (COM Port and Ethernet Adapter) and click the **Add** button. Then enter values in for all property of the new Biometric Reader and click the **Save** button.

You can edit the properties of the Subscriber entity as required.

The properties of the Subscriber entity are described in Chapter 6.2.8.1 *The Subscriber Entity*. The Subscriber Zone Entity, Chapter 6.2.8.2 *The Subscriber Zone Entity*.

To edit the properties of a Subscriber, please select a required entity in the tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete the Subscriber entity, please select a required entity in the Entities Tree and click the **Delete** button. Then click **Yes** to confirm a delete action in the appeared dialog box.



#### 6.2.8.1 The Subscriber Entity

The above Chapter 6.2.8 *The List of Connected UOPs* discusses the place of the Subscriber entity in the system tree as well as actions related to adding, editing, and deleting of the entity. This chapter focuses on the Subscriber properties and information displayed for the entity in the system tree.




The Entities Tree shows the following information for the Subscriber entity:

- Name.



The properties of the **Subscriber** entity:

**Inspector**






Index	4
Name	UOP
Description	
Priority	Default
Subscriber ID	4
Phone numbers	

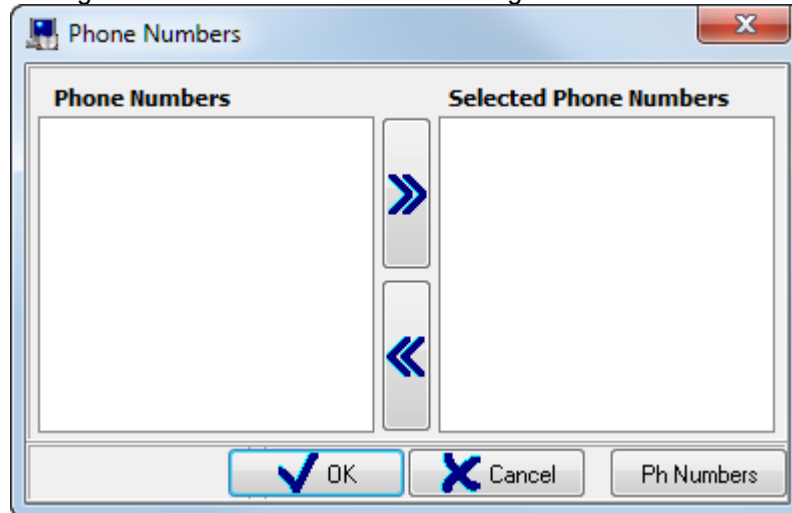
Property	Possible Values	Description
<b>Index</b>	1..2147483647	<p>The unique number of a device in the system.</p> <p><i>Attention! The device is may be a biometric reader, subscriber, or dot-matrix display</i></p> <p><i>Default value: a minimum number from the available range (1...2147483647) of addresses not used in the system.</i></p>
<b>Name</b>	A length of 1 to 25 chapters	<p>The name of a subscriber.</p> <p>The default value: the name of a device type. For example: UOP</p>
<b>Description</b>	A length of 0 to 200 characters	<p>A length of 0 to 200 characters Comments.</p> <p>This field is optional.</p> <p>Default value: blank field</p>
<b>Priority</b>	By default High Medium high Medium Medium low Low No polling	<p>Priority of polling by the Scanning Core module</p> <p>Default value: By default»</p>
<b>Subscriber Number</b>	A length of 1 to 15 characters	<p>A subscriber number that is specified in the settings of a communicator (OU-4S, S2000-PGE, and S2000-IT) and defines the unique number of a protected site or entity.</p> <p><i>Attention! There cannot be two subscribers with identical numbers in the system.</i></p> <p>Default value: empty field</p>
<b>Phone Numbers</b>	<i>See Chapter 6.2.8.1.1. Phone Numbers of Subscriber. The Phone Number Entity</i>	<p>The list of phone numbers of protected site.</p> <p><i>Attention! This field must be filled.</i></p> <p><i>Attention! This property is not accessible when an entity is being added, it can be accessed only when you proceed with editing</i></p> <p><i>Default value: empty field</i></p>




#### 6.2.8.1.1 Phone Numbers of Subscriber. The Phone Number Entity


It is worth mentioning again that when the entity is being added, the property is not accessible and can be accessed only when you proceed with editing. In other words, first you must add (**Add**) and save (**Save**) the Subscriber entity. Then click the **Edit** button and select the **Phone Numbers** property and click the  button to open the Phone Numbers dialog box.


The figure show the Phone Numbers dialog box:



The right pane lists the phone numbers associated to a Subscriber. The left pane list all other phone numbers.

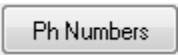
To associate a phone number to the Subscriber, please select a phone number to double-click it or use the  button in the center.

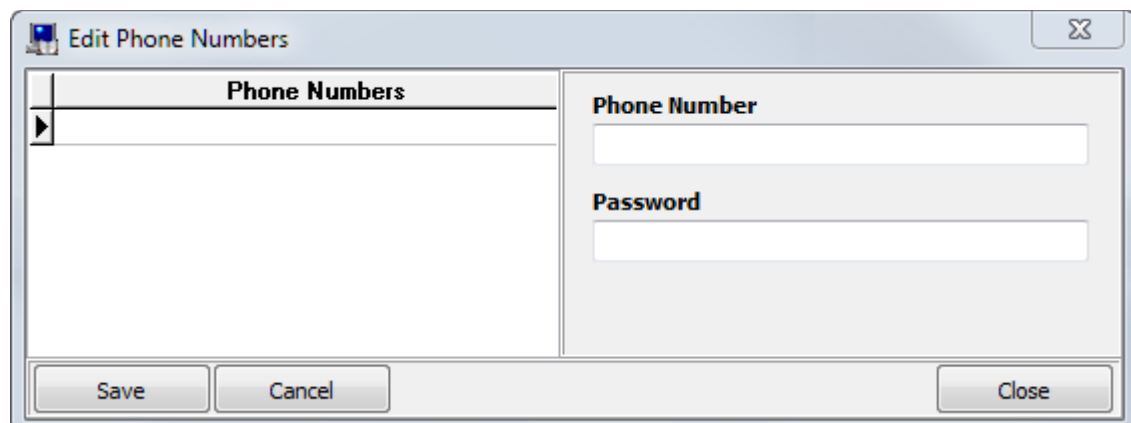
You can select multiple phone numbers using <Shift> (Range Selection) or <Ctrl> (Combined Selection) and associated them all together to the Subscriber using the  button.

To delete any association of a phone number to the Subscriber, please select a required phone number from number associated to the Subscriber and use double-click or the  button in the center.

Click the **OK** button to accept your changes.

To edit the list of phone numbers, please click






To add a new phone, please click the Add button. Then enter a phone number and click the **Save** button.

To change the phone number, select a required phone in the list of phone numbers and click the **Edit** button. Then change the phone number as required and click the **Save** button.

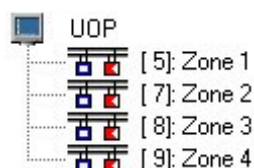
To delete a phone number, please select a required phone in the list of phone numbers and click the **Delete** button. Then confirm the action the appeared dialog box by clicking the **Yes** button.

### 6.2.8.2 The Subscriber Zone

Let's consider the Subscriber Zone entity.

 [ 5]: Zone 1

Subscriber zones are associated (added) to the Subscribers in the tree view.



The subscriber zones are added only manually.


To add the Subscriber Zone, please select a required node in the tree and click the **Add** button. Then enter values in for all property of the new Subscriber Zone click the **Save** button.

To edit the properties of a Subscriber Zone, please select a required entity in the tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

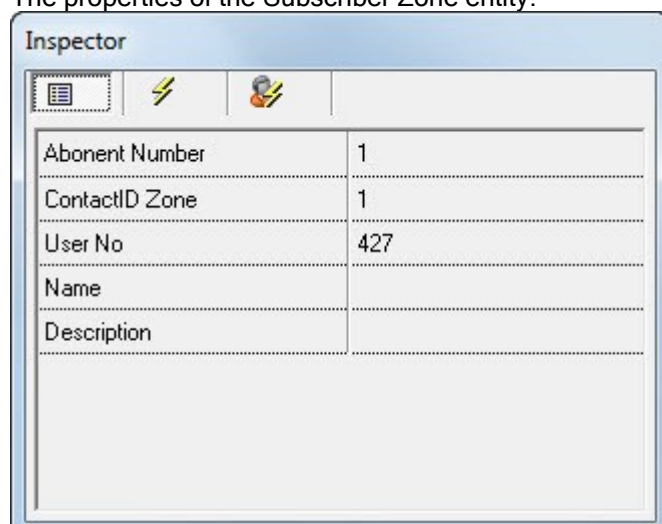
To delete the Subscriber Zone entity, please select a required entity in the tree and click the **Delete** button. Then click **Yes** to confirm a delete action in the appeared dialog box

The Subscriber Zone entity shows the following in the tree view:

- Contact ID Zone
- Name
- The number of partition (if a zone is added to any department).

 [ 10]: Zone 1, Canteen (10)

The properties of the Subscriber Zone entity:




An 'Inspector' window with a title bar and a toolbar containing icons for a list, a lightning bolt, and a person. Below the toolbar is a table with five rows and two columns. The first column contains property names, and the second column contains their values.

Abonent Number	1
ContactID Zone	1
User No	427
Name	
Description	

Property	Possible Values	Description
Subscriber ID	1..127	The Number of a Subscriber where the zone belongs <i>This property is not editable.</i> Value: Subscriber ID
Contact ID Zone	1.. 2147483647	The number of Subscriber's Contact ID Zone. <i>It must match the number of ContactID zone at a protected site</i> Default value: a minimum number from the available range (1...2147483647) not used for the currently subscriber
User No	1..2147483647	The unique number of a device's entity in the system. <i>Attention! In this case, the devices is understood as a reader, loop, relay output, and subscriber zone. Hence, a User No must be unique for all entities of the following: reader, loop, relay output, subscriber zone!</i> Default value: a minimum number from the available range (1...2147483647) not used in the system.
Name	A length of 1 to 30 characters	The name of a subscriber zone. Default value: no value
Description	A length of 0 to 200 characters	Comments. <i>This field is optional</i> Default value: no value
Element type	Zone/Loop	Type of device's entity. <i>This attribute is not editable.</i> Value: Zone/Loop
Type	UOP Zone	Type of subscriber zone. <i>This attribute is not editable.</i> Default value: UOP Zone

### 6.2.11 Connecting Devices Using Printer Protocol





To connect devices using printer protocol, please select the Orion Printer protocol for the COM Port entity.

















 [ ]: COM3 (Orion Printer)

No other actions are required. The device itself is not added to the database.

### 6.2.12 Entity Events

Events are generated for the most of system entities. The Scanning Cores modules receive these events from devices, or the modules generate the events themselves based on the events received from devices. In addition, the Scanning Core modules can generate virtual events.

Entity	Events	
	Own (Physical)	Virtual
Workstation		
Video System		

Camera		
Device/ Biometric Reader / Subscriber / Keybox		
Reader		
Loop/Subscriber Zone /KeyboxCylinder		
Relay Output		
Partition		
Partition Group		
Access Zone		

It is worth mentioning the following:

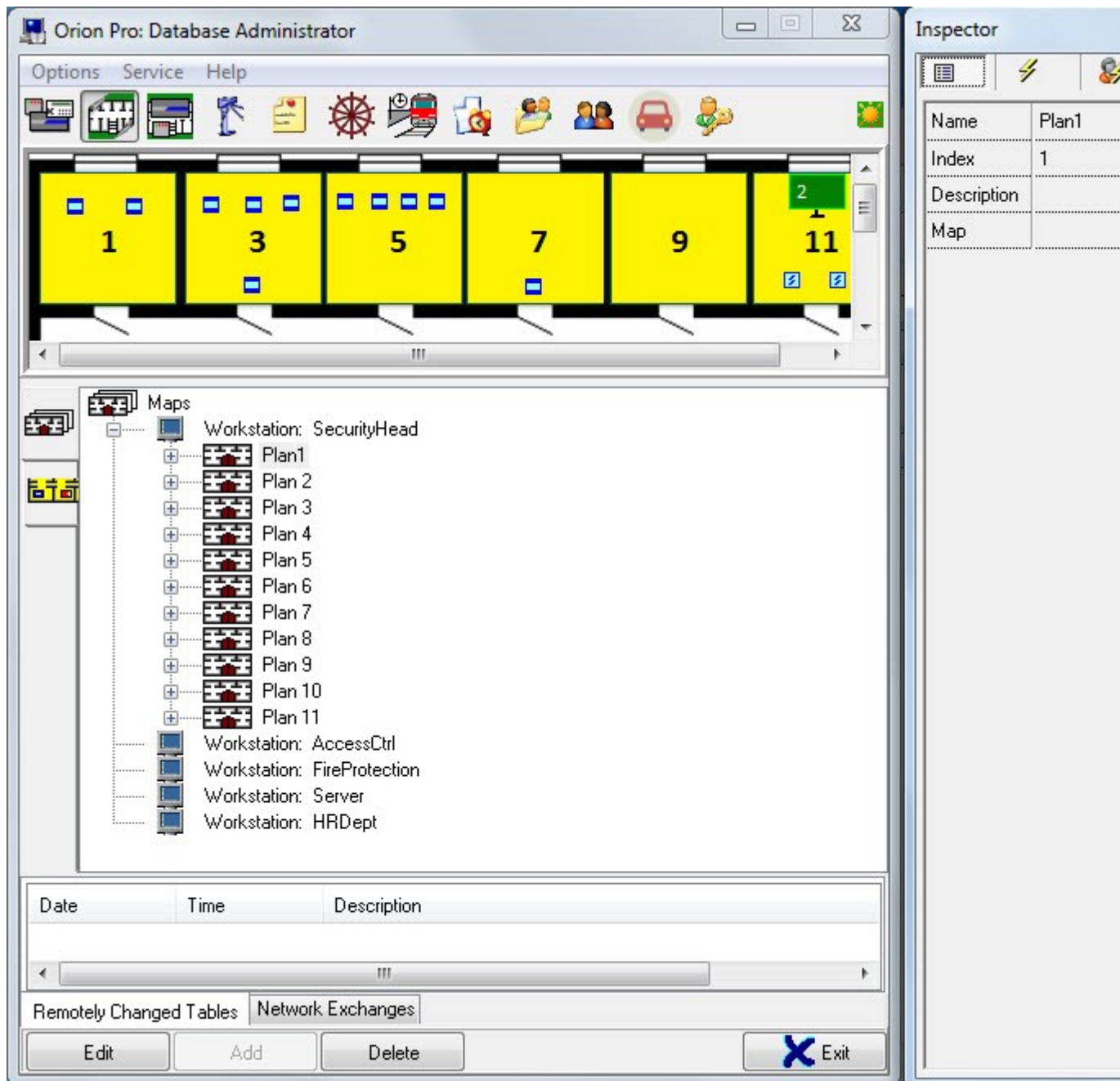
- The Partition entity has its own events. But virtual events (neither displayed anywhere nor logged in the Event Log) are generated for the Partition entity as well. These virtual events duplicate the events of loops, relay outputs, and cameras included in this Partition. In other words, for example, if any event occurs on the loop, additionally, virtual event will be generated for the partition that includes the loop. This is provided to facilitate configuring system responses to entity events.
- The Video System entity has its own events. But virtual events (neither displayed anywhere nor logged in the Event Log) are generated for the Video System entity as well. These virtual events duplicate camera events for this system.
- The Workstation entity has its own events. But virtual events (neither displayed anywhere nor logged in the Event Log) are generated for the Workstation entity as well. These virtual events duplicate workstation events for this Workstation.
- The Access Zone entity does not have its own events. But virtual events (neither displayed anywhere nor logged in the Event Log) are generated as well. These virtual events duplicate the events of readers that control doors providing entry to this access zone.

Each type of entity has its own Event Group. The composition of any Event Group can be changed. But it is not required in most cases, since event groups are created automatically for each specific type of entity and include all necessary events. However, changes can be made in included events in certain situations to facilitate task related to system configuring (such as filtering of events transmitted to S2000-K and S2000-IT devices). The description of Event Groups is provided in Chapter 6.14.3 *Setting Event Groups*.

During the process of configuring the system, entity events are used to complete the following tasks:

1. The events of entities can be associated with management scenarios to provide scheduled system responses to entity events.  
Virtual events are implemented to facilitate this task. For example, if it is required to run the scenario (that is to open free access through access points) when a FIRE event occurs on any loop of a certain partition, you will not have to associate the scenario to a FIRE event of each loop of the partition as you can associate the scenario to the virtual FIRE event of this partition. Procedures related to associating scenarios to system events are described in Chapter 6.4.4. *Configuring Scheduled System Responses to Entity Events. Associating Management Scenarios to System Events*.
2. Entity Events can be renamed.  
This can be useful for renaming events of an auxiliary loop monitoring the status of fire equipment (e.g. Vent damper position)  
*Attention! The virtual events are neither displayed anywhere nor logged in the Event Log. Thus a virtual event cannot be renamed.*  
*The descriptions of procedures related to event renaming are provided in Chapter 6.14.2 Defining User Events. 6.4.5 Renaming the System Events.*
3. The Event Group is used to ensure the transmission of events to S2000-K and S2000-IT devices. Procedures related to configuring the transmission of events are described in Chapter 6.4.2 *Configuring Transmission of Events and Status of System Logical Entities*.

### 6.3 Maps Tab. Creating Logical Entities and Structure of Intrusion and Fire Alarm System



The Maps Tab displays the following:

1. Toggling buttons



–Toggles Map view,



–Toggles Partition and Partition Group.

The selected view area

The selected map

The **Maps** Tab is used to define the system logical structure:

- Logical entities of Intrusion and Fire Alarm System: partitions and partition groups

- To be displayed in System Monitor, Maps are added to the system to accommodate graphical representation of system entities: reverences, partitions, loops, relay outputs, cameras, devices, readers and doors (access points)

### 6.3.1 Partitions and Partition Groups

In the ORION Integrated Security System, the management and control of the system elements can be provided on *local* or *centralized basis*.

If local control is engaged, the device itself is responsible for initiating relay actions and programs in response to zone states (input status, granting access, arming and disarming zones (inputs), and control of fire extinguishing.

In case of Centralized Control, *all decisions* are taken by a network controller (S2000/S2000mM Panel or Orion Pro Suite).

In this case, a relay output is controlled in accordance to the states of logical entities (partitions and partition groups) rather than to the states of zones.

Arming and disarming is provided in accordance to the states of logical entities (partition and partition groups) rather than individual zones.

The advantages of operation with partitions (partition groups) over the operation with zones are as follows:

- Arming and disarming partitions (or partition groups) takeless a user's efforts and time, and reduces an operator's error probability. Particularly, when it is needed to arm or disarm a great number of zones, one will benefit a lot from grouping them into a partition, especially when the zones belong to different devices.
- The user can arm and disarm only those partitions (partition groups) he is authorized to
- A user can control fire extinguishing on those partitions (partition groups) only he is authorized to
- Arming, disarming and extinguishing control of the on the partitions can be provided not only using a device or a network controller but also using device controlled by the network controller: such devices include S2000-K, S2000-KS, S2000-4, S2000-2, Signal 20P SMD, S2000-KDL, S2000-BI, S2000-PT and S2000-BKI
- System outputs (relay) can be configured
- Possibility of using S2000-BI, S2000-BKI, S2000-BI rev. 01, S2000-PT, and S2000-KS.

The **Partition** is a group of zones (loops, addressable zones, supervised (controlled) circuits and outputs), characterized by any shared attribute. One specific zone can be added to one partition only.

Usually one partition includes all zones of a certain area wherein intrusion and fire zones are added to two different zones where an intrusion partition included intrusion zones only and fire partition includes fire zones only. Exception can be made, though, e.g. in case of perimeter protection, etc.

*It is worth mentioning, that in Orion Pro Suite, the partitions can include cameras. This is implemented for centralized arming/disarming cameras with credential (TouchMemory button/iButton, Proximity card, or PIN code) via a reader or keypad as well as for the management of System Monitor operators' rights to access cameras.*

The Partition Group is the group of partitions characterized by any attribute. One partition can be added to multiples partition groups.

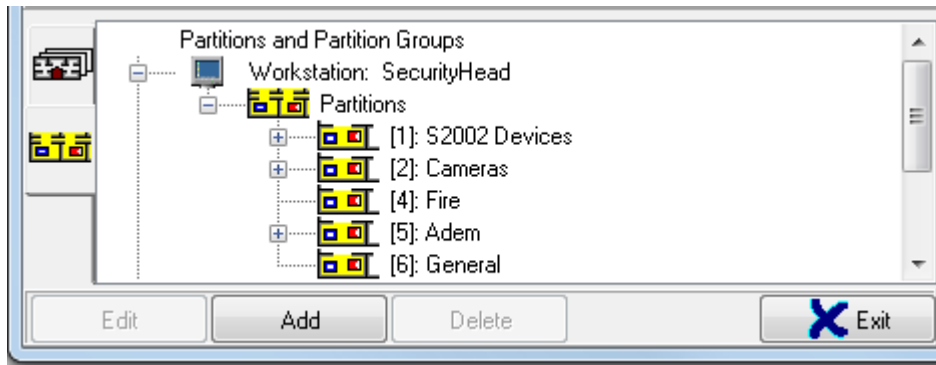
Usually partition groups are created to facilitate and management.

Important! The numbers (No) of partitions and partition groups must be unique within a single workstation. In other words, any two *Partitions* or/and any two *Partition Groups* may not share the same number on one workstation.

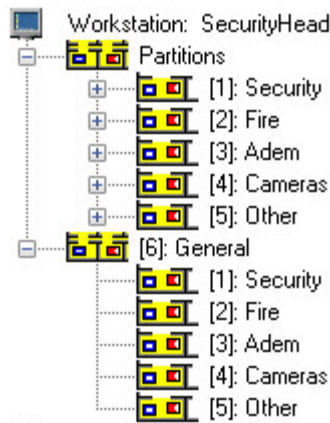
Let's discuss the structure of Maps tab.

The main window is divided into two parts. The bottom part display **Partition and Partition Groups** or **Maps** (Floor Plans)

Partitions and Partition Groups screen displays the partition and partition groups in tree view:

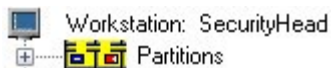


The main tree node is Partitions and Partition Groups. All workstation of the system are associated to this node. The Workstation node serves to add partitions and partition groups of the current workstation. By default, the Workstation node includes the Partitions node where partitions are added:



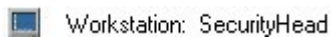
*Partition and Partition Groups are displayed in the following manner: partition groups> the Partitions node where partitions are associated.*

As the figure shows, when you add a workstation to the system, the corresponding Workstation node is automatically added to the tree of partitions and partition groups; the Workstation node includes Partitions node being associated to it



The tree shows the following information for the Workstation entity:

- Name



*The Workstation entity' attributes cannot be edited in the tree of partitions.*

### 6.3.1.1 The Partition Entity

In the Orion Pro Suite, partitions can belong to workstations where the Scanning Core modules are installed. Partitions will include device zones controlled by a relevant Scanning Core and the cameras of this workstation.

A partition can include zones (loops, addressable zone, supervised circuits, and outputs) of the following devices <sup>(\*)</sup>:


Device	Type of device zone
S2000-2	Loop
S2000-4	Loop

	Supervised output
Signal-20	Loop
Signal-20/02	Loop
Signal-20P	Loop
Signal-20P ver 2.04	Loop
	Supervised output
Signal-20-M	Loop
	Supervised output
Signal-10»	Loop
	Addressable point (detector)
	Supervised output
S2000-KDL	Addressable detector
	Addressable relay output
S2000-KDL-2I	Addressable detector
	Addressable relay output
S2000-KDLS»	Addressable detector
	Addressable relay output
S2000-KPB	Loop
	Supervised circuit
S2000-ASPT	Loop
	Supervised circuit
S2000-ASPTver. 2.00	Loop
	Supervised circuit
	Supervised circuit
S2000-ASPT ver. 3.00	Loop
	Supervised circuit
	Supervised output
Potok-3N	Supervised circuit
	Supervised output
Potok-3Nver. 1.03	Supervised circuit
	Supervised output
Rupor	Loop
Rupor ver. 2.00»	Loop
	Supervised circuit
	Supervised output
Rupor-200»	Supervised circuit
	Supervised output
RIP-12 RS	Supervised circuit
RIP-12-2A RS	Supervised circuit
RIP-24-2A RS	Supervised circuit
S2000-Adem	Addressable wireless detector
	Supervised circuit

(\*)Relay outputs of S2000-2 devices, S2000-4, Signal-20P ver 2.04, Signal-20M, Signal-10 and S2000-SP1, that do not controlled connected circuit but can have the states of the relay (ON, OFF, X Pattern Blinking) are also can be connected to a partition.

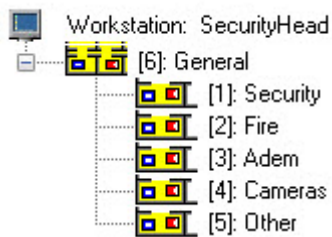
(\*\*)A partition can also include Subscriber (UOP) zones that cannot be controlled, and the status of each subscriber zone will be received only after the first event of a specific zone.

Let us discuss the Partition entity.

 [4]: Cameras

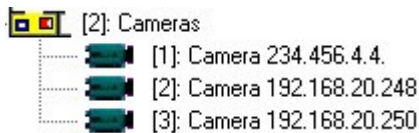
Partitions are associated to the Partitions nodes of Workstations:





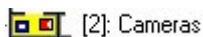
*Partitions and Partition Groups of one Workstation are displayed as follows: partition groups> the Partitions node where partitions are associated to.*

Loopsof relay outputs and cameras are associated to the Partitionentity in the tree of partitions and partition groups:



The tree of partitions and partition groups shows the following information for the Partition entity:

- Number
- Name



To add a new Partition entity, please select the Partitions node for a required Workstation and click the **Add** button. Then enter required values for all properties of the entity and click the **Save** button.

To edit the properties of the Partition entity, please select a required entity in the tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete the Partition entity, please select a required entity associated to the **Partitions** node in the tree of partitions and partition groups and click the **Delete** button. Then, confirm the action by clicking the **Yes** button in the appeared System Request dialog box.

The properties of the Partition entity:

Partition number	2
Name	Cameras
Description	No
High security area	No

Property	Possible Values	Description
Partition Number	1..9999	The unique number of a partition.

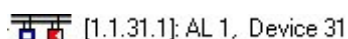
		<p><i>The number must be unique for the Partition and Partition Group entities within one workstation.</i></p> <p><i>Default value: minimum number from available range (1...9999) not used on the workstation where the partition belongs</i></p>
<b>Name</b>	A length of <b>1 to 30</b> characters	<p>The name of a partition.</p> <p><i>Please keep it in mind that a name length of the partition cannot be more than 16 characters in the S2000 and the S200M Panels. When a database is exported to a panel, partition names will be shortened to 16 characters</i></p> <p><i>Default value: the number of a partition</i> <i>E.g: 29</i></p>
<b>Description</b>	A length of <b>0 to 200</b> characters	<p>Comments.</p> <p><i>Optional field.</i></p> <p>Default value: Empty field</p>
High security area	<b>Yes/No</b>	<p>Defines authorities to manage this partition:</p> <ul style="list-style-type: none"> <li>- If <b>Yes</b>, an operator cannot disarm this partition unless he has special authorities defined as settings of software passwords.</li> <li>- If <b>No</b>, an operator requires no special authorities to disarm the partition</li> </ul> <p><i>(See Chapter 6.12.1 Creating Passwords for Software Modules)</i></p> <p>Default value: <b>'No'</b></p>

It is worth mentioning again, that partition-added loops, relay outputs, and cameras are associated to the Partition entity in the tree of partition and partition groups:



The tree of partitions and groups show the following information for loops and outputs:

- Address
- Name.



The tree of partition and partition groups show the following information for the Camera entity:

- Number
- Name
- The name of map where the camera is added



To edit the property of a loop, relay output, and camera, please select a required entity in the tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

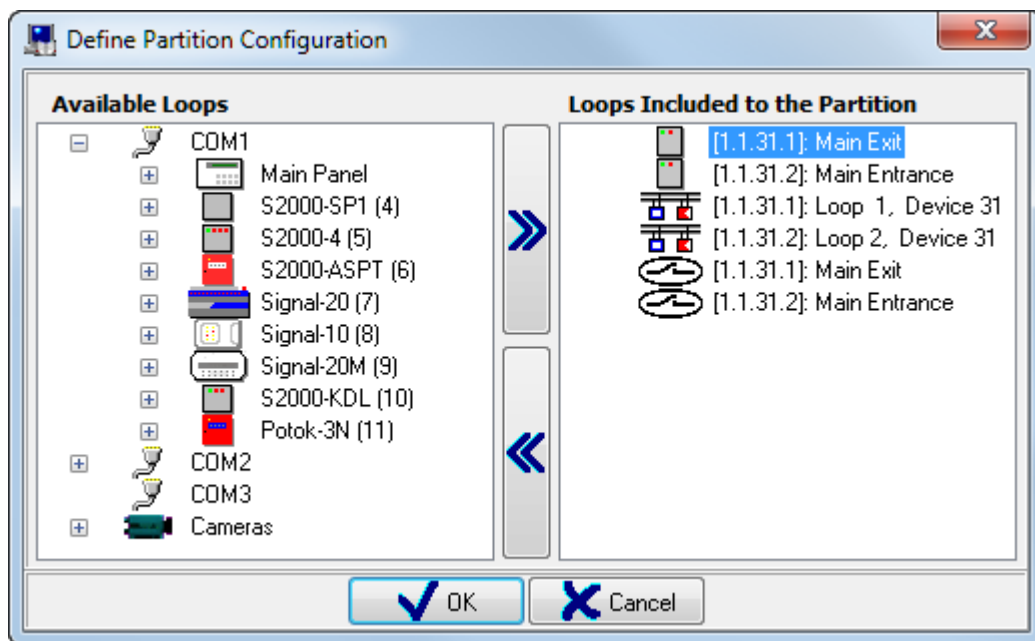
To add new loops, relay outputs, or cameras, please select a required partition in the tree view and click the **Add** button. Then, , define loops, relay output, and cameras that you want to include in the partition and click the **OK** button in the appeared **Define Partition Configuration** window.

To change loops, relay outputs and cameras included in a partition, please select a required partition in the tree of partitions and click the **Add** button. Then, in the appeared **Define Partition Configuration** window, select new loops, relay output, and cameras that you want to include in the partition and click the **OK** button

To remove a loop, relay outputs, and camera from a partition, you can also use the Define Partition Configuration window. To open this window, select a required partition and click the Add button.

You can also delete one loop, relay output, or camera from a partition by selecting a required loop, relay output, or camera in the tree view and clicking the **Delete** button. Then confirm the delete action by clicking the **Yes** button.

Let's consider the Define Partition Configuration dialog box:

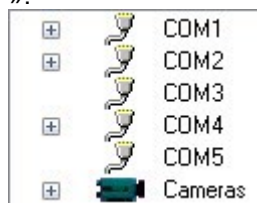


The left pane shows loops, relay outputs, and cameras of the current workstation, which are not included to any partition.

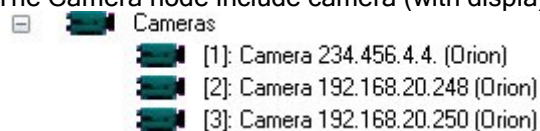
The left pane shows also shows the list of cameras of the current workstation, which are not included to any department.

All these entities are represented in the tree view. The root nodes of this tree are COM Port nodes (COM) with displayed number and Camera nodes:

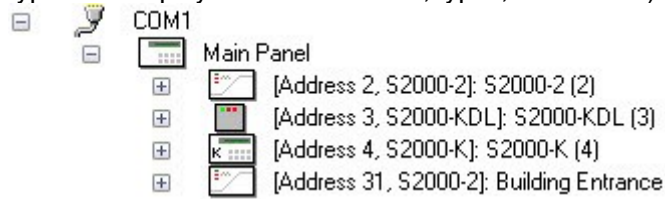
»:



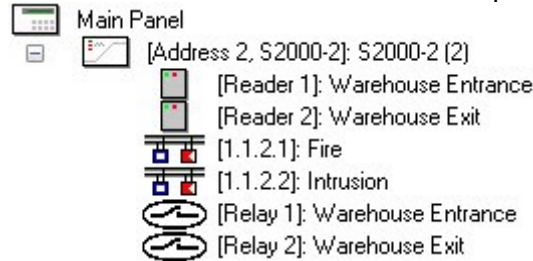
The Camera node include camera (with displayed number and name):




The COM Port node includes associated devices (the S2000 panels are displayed with names; all other types are displayed with addresses, types, and names):





The Device node includes associated loops and relay outputs (with their displayed number and names):



The right pane displays the list of partition included loops, relay outputs, and cameras.

To add a loop, relay output, or camera to a partition, please select the required entity in the tree and click it twice, or click the  button in the center.

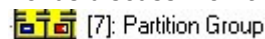
You can select multiple items using the <Shift> (Range Selection) or <Ctrl> (Combined Selection) and click the  button to add the selected items to the partition.

You can select multiple items using the <Shift> (Range Selection) or <Ctrl> (Combined Selection) and click the  button to remove them from the partition.

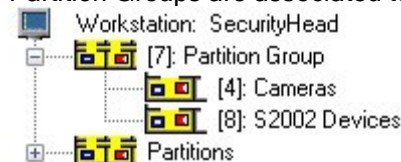
### 6.3.1.2 The Partition Group Entity

In the Orion Pro Suite, the Partition Groups (as well as Partitions) can belong to workstations where the Scanning Core modules are installed. The Partition Groups will include partitions previously created for the relevant Scanning Core module.

Let us discuss the Partition Group entity.

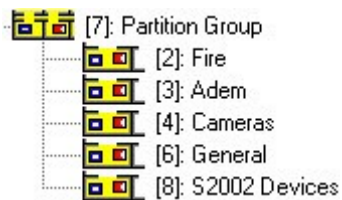


Partition Groups are associated to the Workstation nodes:



*Partitions and Partition Groups of one Workstation are displayed as follows: partition groups> the Partitions node where partitions are associated to.*

Partitions are associated to the Partition entity in the tree of partitions and partition groups:



The tree of partitions and partition groups shows the following information for the Partition Group entity:

- Number
- Name



To add a new Partition Group entity, please select a required Workstation in the tree view and click the **Add** button. Then enter required values for all properties of the new Partition Group entity and click the **Save** button.

To edit the properties of the Partition Group entity, please select a required entity in the tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

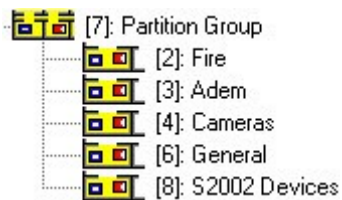
To delete the Partition entity, please select a required entity associated to the **Partitions** node in the tree of partitions and partition groups and click the **Delete** button. Then, confirm the action by clicking **Yes** in the appeared the System Request dialog box.

The properties of the Partition Group entity:

Property	Value
Group number	7
Name	Partition Group
Comment	

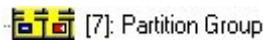
Property	Possible Values	Description
(Partition) Group Number	1..9999	<p>The unique number of a partition.</p> <p><i>The number must be unique for the Partition and Partition Group entities within one workstation.</i></p> <p><i>Default value: minimum number from available range (1...9999) not used on the workstation where the partition belongs</i></p>
Name	A length of 1 to 30 characters	<p>The name of a partition.</p> <p><i>Please keep it in mind that a name length of the partition group cannot be more than 16 characters in the S2000 and the S200M Panels. When a database is exported to a panel, partition names will be shortened to 16 characters</i></p> <p><i>Default value: the number of a partition</i>  <i>E.g.: 100</i></p>
Description	A length of 0 to 200 characters	<p>Comments.</p> <p><i>Optional field.</i></p> <p>Default value: Empty field</p>

It is worth mentioning again, that Partition Group provided association of partitions that was added to this partition group:



The tree of partitions and groups show the following information for the Partition Group:

- Number
- Name.



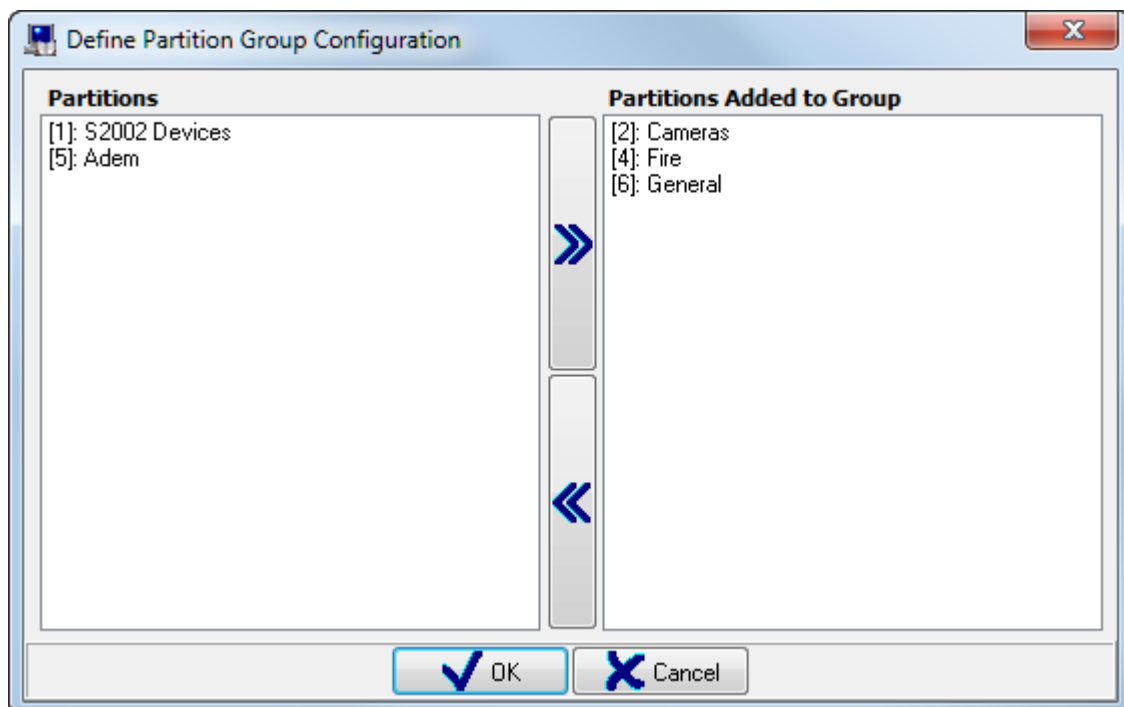
To add new partitions to a partition group, please select a required partition group in the tree view and click the **Add** button. Then define in the appeared dialog box what new partitions will be included in the partition group and click the OK button.

To change the configuration of a partition group, please select a required partition group in the tree of partitions and partition group and click the **Add** button. Then, in the appeared **Define Partition Configuration** window, define what partitions will be included in the partition group and click OK,

You can also use the **Define Partition Group Configuration** window to remove a partition from a partition group. Select a required partition and click the Add button to open the Define Partition Configuration window.

In addition, you can delete one partition by selecting a required partition associated to the partition group and click the Deleted button. Then confirm the delete action by clicking the **Yes** button in the appeared dialog box.


The **Define Partition Group Configuration** window:





The right pane contains partitions added to a partition group


The left pane shows all other partitions available on the current workstation.

To add a partition to a group of partitions, please double click a required partition in the list of partitions or

click the  button to add it to a partition group.

Using the <Shift> key (Range Selection) or <Ctrl> (Combine Selection) you can select multiple partitions to add them to a partition group using the  button.

To delete a partition from a partition group, please double click a partition from the list of grouped partitions or click the  button in the center of the window.

Using the <Shift> key (Range Selection) or <Ctrl> (Combine Selection) you can select multiple partitions to delete them to from the group using the  button.

### 6.3.2 The Maps Tab. Adding Entities to Maps

As said before, site maps and floor plans can be added on System Monitor modules. These maps can contain icons of entities of logical and physical structures of Intrusion detection, fire protection, and access control systems. These entities include the following: Link, Partition, Loop, Relay Output, Camera, Device, Reader, and Door.

Map is graphical representation (plan) of a certain area at a protected site.




















In addition to displaying the status of each entity (Link, Partition, Loop, Relay Output, Camera, Device, Reader, and Door), maps allow performing some actions for these entities (arming, disarming, granting access, releasing (extinguishing), etc.)

It is important to understand that it not obligatory to add entities to maps. Status display and control options for the most of entities are available on data display and control tabs, even if these entities are not added to the maps.

*System Monitor's Data and Control Tabs offer few capabilities to manage the Partition, Loop, and Relay Output and Camera entities as compared the managing capabilities of the **Map** entities.*

*The Data and Control Tabs also offer capabilities to control system entities such as Access Group, Access Zone, and Employees that cannot be added to area maps.*

*See tables for system entities that are displayed in the System Monitor modules on area maps and Control Tabs:*

Entity	Displayed on		View on area map
	Area maps	Control Tabs	
Link			Area of arbitrary form
Partition Group			–
Partition			Area of arbitrary form
Loop			One or more sensor icons
Relay Output			One or more icons of relay-controlled units
Camera			Camera icon
Door			Door icon
Reader			Reader icon
Device			Device icon
Access zone			–
Employee			–

*Important! Accessibility of entities to view their states and events as well as to control them in the System Monitor module depends on an Operator's password privileges and access level (See Chapter 6.10.5.*

It is clear that you cannot place the icons of an entity on the map if this entity hasn't been created in the system. Therefore, one must create an entity before adding it to a map.

This holds true for the Link entity, which is a link to an area map. So before placing another-map link on a map, first this another map must be added to the system.

Usually actions of creating maps and placing entities are as follows:

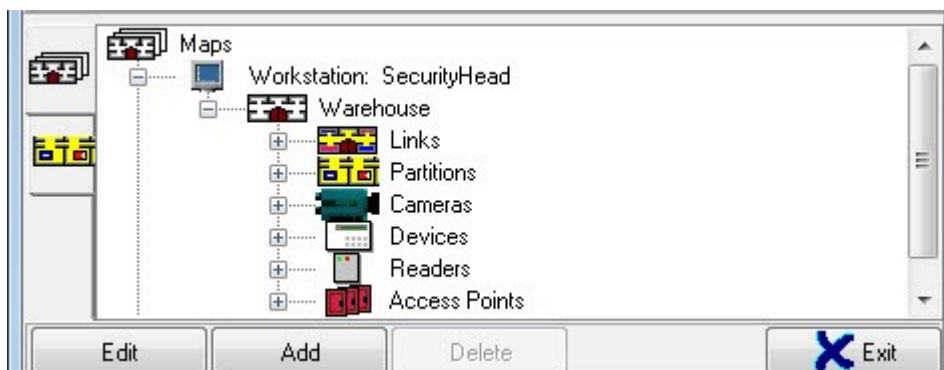
- 1) Adding system entities such as partitions, loops, relay outputs, cameras, devices, readers, and doors.
- 2) Adding area maps
- 3) Adding links that follow to another maps
- 4) Adding partitions with included loops and relay outputs to maps
- 5) Adding doors (access points) and readers to maps
- 6) Adding devices to maps
- 7) Adding cameras to area maps.

The above procedures are not always must be followed in the order as specified. Each system administrator can develop its own order to be followed. Also, it is not necessary to complete all of the specified procedures.

Let's discuss the structure of the Maps tab.

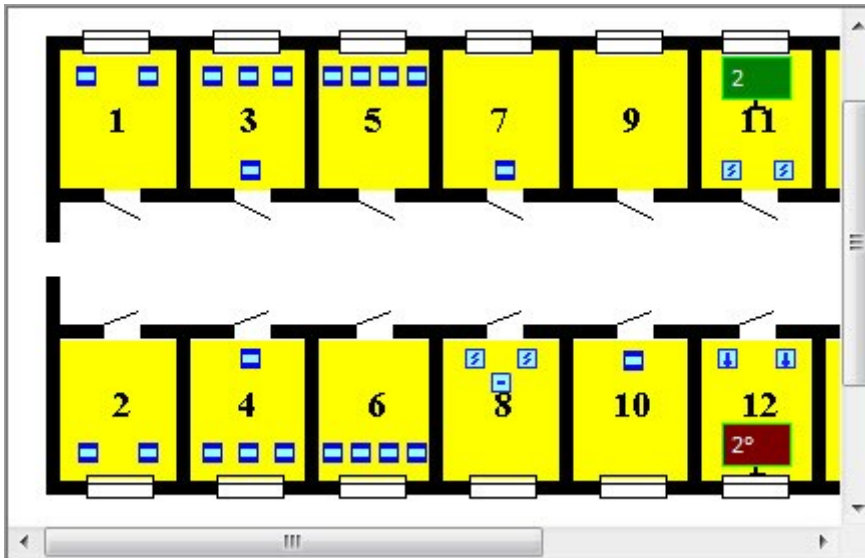
The Maps window is divided into two parts. The bottom part contains the **Partition and Partition Groups** view or **Maps** view.

The Maps tab displays the Area Maps tree:



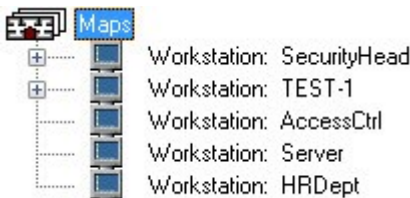
The upper part of the window provides the view of a selected map:





Let's discuss the structure of the Maps tree. The main node of the Area Maps tree is **Maps**

When workstation is added to the system, the Workstation node is automatically added to the Area Maps tree and associated to the Maps node:



The Workstation entity displays the following information in the tree:

- Name.



Area maps are associated to the Workstation entity:



### 6.3.2.1 The Map Entity

In the Orion Pro Suite, an area map can belong to workstation with installed the Scanning Core module. The area map will show the structure of the subsystem (or part of it) controlled by the relevant Scanning Core.

Let's discuss the Area Map entity.



The area maps are associated to the Workstations in the tree of area maps:



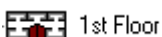
The Map entity includes Links, Partitions, Cameras, Devices and Readers, and Access Points (or Doors):



Links, Partitions, Cameras, Devices, Readers, and Assess Points are associated to the nodes with corresponding names.

The Map shows the following information in the tree of area maps:

- Map name



To add a new map, please select a required **Workstation** in the tree of area maps and click the **Add** button. Then enter all necessary changes for the new Map entity and click the **Save** button.


To edit properties of any Map entity, please select a required entity in the tree of area maps and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete the Map entity, please select a required entity in the tree of area maps and click the **Delete** button. Then confirm the delete action and click **Yes**:

When you delete an area map, all links from other maps to this map will be also deleted.

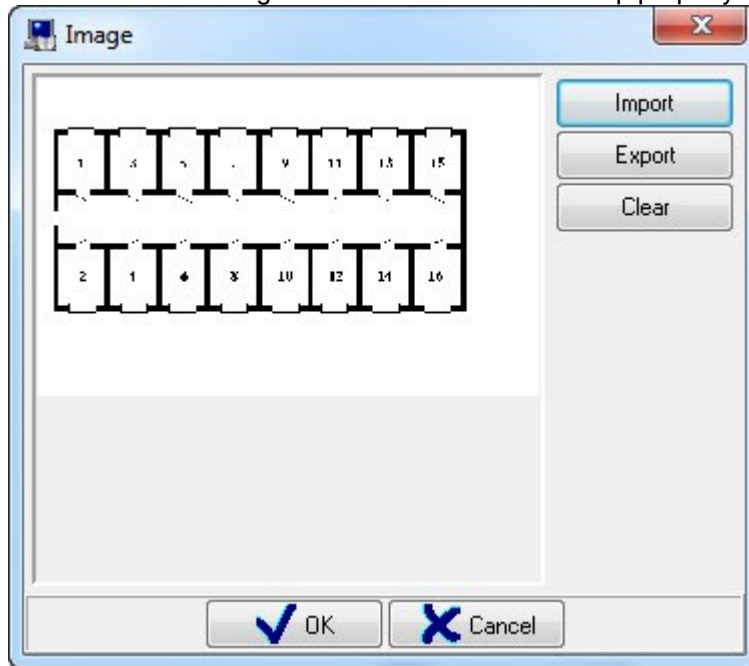
Properties of the Map entity:

Property	Possible Values	Description
<b>Name</b>	A length of 1 to 25 characters	The name of a map. Default value: empty field (must be filled)
<b>Index</b>	1..2147483647	The index of a map. This index defines the order of displaying maps on the screen in the System Monitor module. Default value: 0
<b>Description</b>	A length of 0 to 200 characters	Comments <i>An optional field.</i>



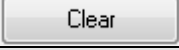


		Default values: empty field
<b>Map</b>	Graphical representation of an area map in the *.bmp format	<p>The graphical representation of an area layout</p> <p>The <b>Map</b> property can be edited in the Image window that can be edited by clicking the  icon (it is visible when the Map property is selected) in the Inspector window (See Note 1 to this table)</p> <p>Default values: empty ( a map image must be loaded)</p>

Note 1:

Let's discuss the Image window used to edit the Map property:



This window offers the following functions (clicking the related buttons):

Map Image Action Buttons to Work with a Map Image	
	Opens the Open dialog box of Windows to load a .bmp image to the Map property
	Opens the <b>Save as</b> standard window to save the current map image into *.bmp file
	Removes a map image from the Map property.
Buttons to confirm or cancel the actions related to a map image.	
	Confirms changes that were completed using the action buttons.
	Overrides changes that were completed using the action buttons.

Note 2

As said before, you can use a bitmap (\*.bmp) image as a map image. It is recommended to use a 24-bit image.

When database parameter is defined in the Server Manager module, the default value for BLOP field (where an image is saved) is 2048 Kb. Hence, by default, the bmp-image file you want to download to the database cannot be more than 2 MB. Larger images will be cropped.

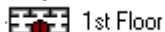
If you need to use a larger-sized image file, you should make some settings in the register of Windows OS on a workstation where the Central System Server is installed. To do that, go to the [HKEY\_LOCAL\_MACHINE\SOFTWARE\BOLID\ORION\CSO\DBPARAMS] directory of the register and set 4096, 8192 or 16384 value for the «BLOB SIZE» parameter, which will enable loading image files of 4 MB, 8 MB, and 16 MB.

Changes will be effective after restarting the Central Server module. In other words, all the software modules of the Orion Pro suite must be restarted.

*Important! Increased size of BLOP fields will slow down the interaction of any applications with the MSSQL database including the Orion Pro software. If you use images of 8 or 16 MB in the database, your database can be loaded 5-10% longer*

### 6.3.2.2 The Link Entity on a Map

The Link Entity is provided to facilitate toggling between area maps in the System Monitor modules:



One of the examples of using links to facilitate toggling between area maps is use of links from the entire site general layout (e.g. multi-floor building) to each floor of the building, or even a room plan in larger scale

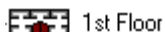
Graphically, the Link is arbitrary area clickable to switch over to a linked area map in the System Monitor module.

The Links are associated to the Links node in the tree of area maps:

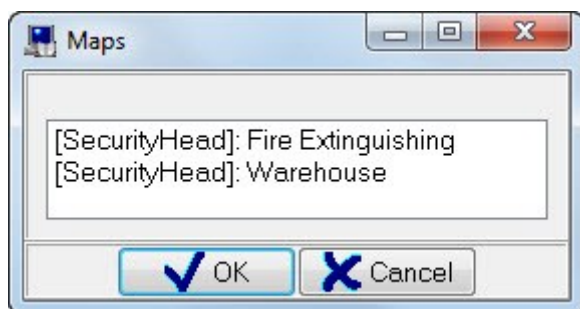


The map tree shows the following information for Link entity:

- Name.



To add a new Link entity to an area map, please select a required Links entity in the tree and click the **Add** button. In the appeared Maps dialog box, select an area map which you want to link and click the **Ok** button.



The Maps dialog box displays all maps but for the following:

- The current map and
- Other maps linked on the current map.

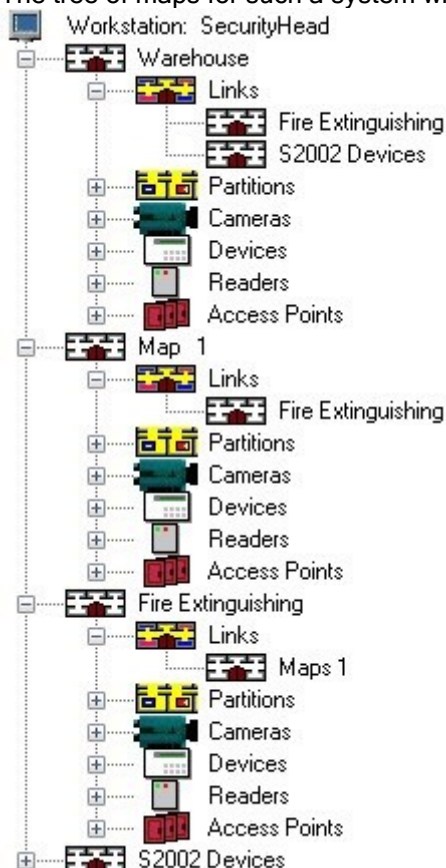
This dialog box also displays the name of a workstation and the name of a map.

You can use <Shift> (Range Selection) and <Ctrl> keys to select multiple maps in the Maps box. When you press the OK button the links will be added to the maps you have selected.

To delete the Link entity, please select a required entity in the tree of maps and click the **Add** button. Then click the **Yes** button in the appeared dialog box to confirm the delete action

Let's discuss example of a map tree of the system with three area maps. The first area map is a general layout of two-floor building with added links to the two floor layouts. The second and the third map are layouts of the first and second floors. Each of these floors has a link added to the layout of another floor.

The tree of maps for such a system will have the following view:




When added to a map, the Link entity id a link to another map (i.e. it is a virtual entity) and has the Link Area property only. All other properties of the Link entity belong to the map the Link entity links to

To edit the attributes of the Link entity (as well as the map it links to), please select a required entity and click the **Edit** button. Then make required changes for the attributes and click the **Save** button.

The properties of the Maps entity are described in Chapter 6.3.2.1 The Maps Entity. This chapter focuses on the Link Area property belonging to the Link entity.

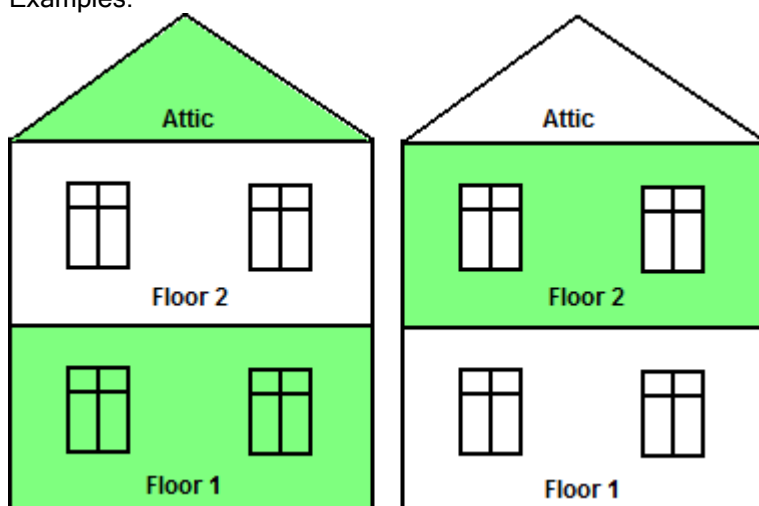
Inspector	
Name	Fire Extinguishing
Index	3
Description	
Link area	

The **Link area** property is edited in the Image Editor window that can be opened by clicking the  button (displayed when selected).

The functions of the Image Editor are described in Chapter 6.3.2.8 Image Editor. This chapter explains only what type of image is added to area map for the Link entity.

An arbitrary shaped area is set on a map for the Link entity. This area is saved in the Link area property.

Examples:



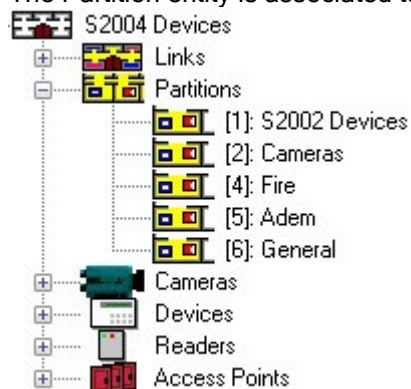
### 6.3.2.3 The Partition Entity on the Map

The Partition entity can be added to area maps to represent graphically the partitions states on the map.

Unlike other entities (such as Loop, Relay Output, Camera, Device, Reader, and Access Points) one specific partition can be added to several area maps that belong to the same workstation the partition belongs to.

Graphically, the partition is an arbitrary mapped area clickable to display a partition control menu in System Monitor.

The Partition entity is associated to the Partitions nodes in the tree of maps



The tree of maps shows the following information for the Partition entity:

- Number
- Name

[1]: partition 1

To add the Partition entity to a map, please select the Partitions node of a required map in the tree and click the **Add** button. The Partitions window will appear. Please, select a partition you want to add and click OK.



The Partitions dialog box shows the workstation-added partitions but for the partitions that is already associated to this workstation.

The Partitions dialog box shows the number and name of each partition. You can use <Shift> (Range Selection) and <Ctrl> keys to select multiple partitions in the dialog box. When you press the OK button the partitions will be added to the map you have selected.

*If you add a partition to a map you will also have to add manually loops and relay outputs of this partition to the map.*

To delete the Partition entity from the map, please select a required entity in the tree and click the **Delete** button. Then confirm the delete action by clicking **Yes** in the appeared dialog box.

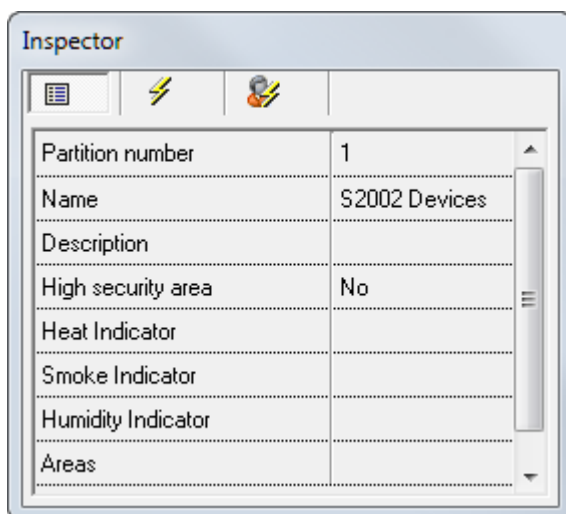
*When you delete a partition from a map, the partition will not be deleted from the Database.*


*When you delete a partition from a map, the partition loops and relay outputs added to this map will be deleted as well.*

Adding a Partition to a map makes more properties accessible, namely **Areas**, **Smoke Indicator**, **Heat Indicator**, and **Humidity Indicator**. All other properties of the Partition entity are also available.

If a partition had been added to more than one map, the values of the **Areas**, **Smoke Indicator**, **Heat Indicator**, and **Humidity Indicator** properties may be not the same for different maps.

The properties of the Partition entity are described in Chapter 6.3.1.1 *The Partition Entity*. This chapter explains only the **Areas**, **Smoke Indicator**, **Heat Indicator**, and **Humidity Indicator** properties which can be accessible as the partition properties in the tree of maps only, if added to the map.

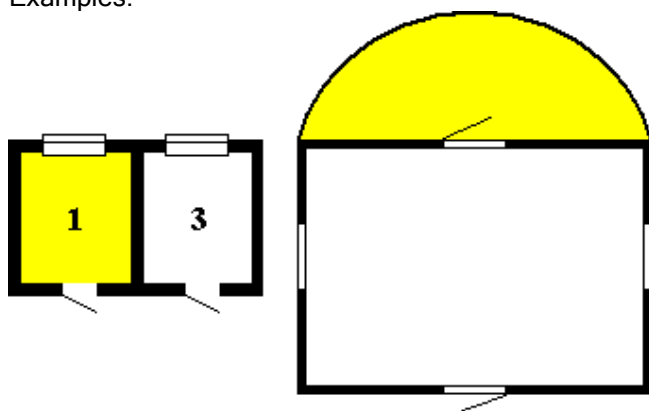


The **Areas** property is edited in the Map Design Editor you can open by clicking the  button (displayed if this property is selected)

Guide for using Map Design Editor is described in Chapter 6.3.2.8 Entity Representation Editor. This chapter focuses on what types of images can be used for the Partition entity.

An area of a required shape is set on a map for the Partition entity. This area is saved in the Areas property.

Examples:



Let's consider the Smoke Indicator, Heat indicator, and Humidity Indicator properties. Using this data you can add indicators of smoke, heat, and humidity measurements to on area map.


A partition's smoke indicator will display average ADC values from all addressable smoke detectors of the partition. An ADC value for an addressable smoke detector is equal to the value of this detector's smoke level.

A partition's heat indicator will display average ADC values from all addressable heat detector of the partition. An ADC value for an addressable heat detector is equal to the temperature value measured by this heat detector.

A partition's humidity indicator will display average ADC values from all addressable humidity detectors of the partition. An ADC value for an addressable humidity detector is equal to the temperature value measured by this heat detector.

Now, the display of ADC readings is supported only by smoke addressable loops, heat addressable loops, and humidity addressable loops and only for corresponding analog addressable detectors of S2000-KDL, S2000-KDL-2I, and S2000-KDLS devices. Adding such indicators for other devices' loops is useless.

*Please keep in mind, that it has to be specified for each workstation whether to gather data (statistics) from the workstation-connected loops (see Chapter 6.2.2 The Workstation Entity (Computer); the same has to be specified for each loop (see Chapter 6.2.6.4 The Loop Entity).*

The **Smoke Indicator**, **Heat Indicator**, **Humidity Indicator** properties can be defined in the Map Design Editor which can be accessed by clicking the  button (appears when a discussed property is selected) in the Inspector box.

The work with the Map Design Editor is described in Chapter 6.3.2.8. This chapter explains what icons are used for indicators of smoke, and heat and humidity sensors readings.

Icons used for indicators are as follows:

Smoke Indicator: 

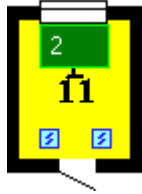
Heat Indicator: , and



Humidity Indicator: 

Only one of each indicator (smoke, heat, and humidity) can be added to one partition added to any one map.

Example of Smoke Indicator on a map:



#### 6.3.2.3.1 The Loop and Relay Output Entities on the Map

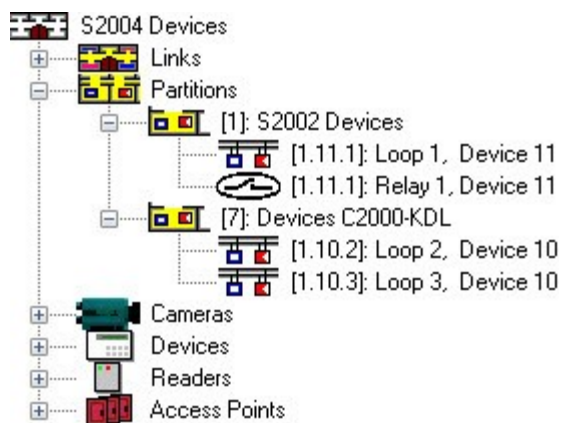
The Loop and Relay Output entities can be added to maps to represent graphically the states of individual loops and relay outputs on the map and provide advanced loop controls.

One specific Loop or Relay Output can be added only to one map that includes the partition with this Loop or Relay Output

*Loops and relay outputs not included into any partition cannot be added to a map.*

Graphically, a loop and relay output is one or more on-map icons clickable to display a loop control menu in the System Monitor module.


In the tree of maps, the Loop and Relay Output entities are associated to partitions:



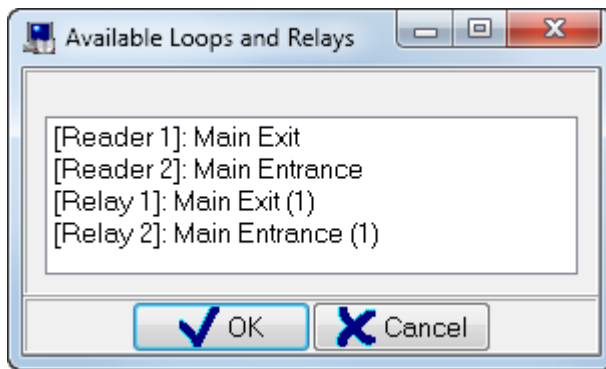
The tree of maps shows the following information for the Loop and Relay Output entities:

- Address
- Name

 [1.11.1]: Loop 1,

 [1.11.1]: Relay 1,

To add the Loop or Relay Output entity to a map, please select a required node in the tree and click the **Add** button. Then highlight a required loop in the appeared dialog box and click the OK button.



The Loops/Relay Outputs dialog box shows all loops and relay outputs of the current partition but for loops and relay outputs that already placed on to any map.

The Loops and Relay Outputs dialog box shows a loop name and address as well as the number (No) of a partition.

Using the <Shift> (Range Selection) and <Ctrl> keys (Combined Selection), you can select multiple loops or relay outputs. When you click **OK**, the selected loops and relay outputs will be added to the map.

To delete the Loop or Relay Output entity from a map, select a required entity from the map and click the **Delete** button. Then confirm the delete action by clicking **Yes** in the appeared window.

When the Loop entity is added to a map, the **Detectors** property becomes available in addition to all other properties.

When the Relay Output entity is added to a map, the **Location** property becomes available in addition to all other properties.

To modify the properties of the Loop or Relay Output entity, please select a required entity in the tree and click the **Edit** button, then change properties as required and click the **Save** button.


The properties of the Loop entity are described in Chapter 6.2.6.4. *The Loop Entity*; the properties of the Relay Output entity are described in Chapter 6.2.6.5 *The Relay Output Entity*. This chapter discusses only the **Detectors** and **Location** property items, which are available only in the tree of maps when an entity is added to the map.


#### Loop properties

Device address	11
Number	1
User number	482
Name	Loop 1, Device 11
Description	
Element type	Zone/Loop
Type	Intrusion
24-hour zone	No
Accumulate statistics	No
ContactID Zone	0
Detectors	
Cameras	

Relay Output properties:]

Inspector	
Device address	11
Number	1
User number	484
Name	Relay 1, Device 11
Description	
Element type	Relay
Type	Relay
Centralized control	No
Tactics	Not manage
Relay action delay	0,000
Relay activation time	0,000
ContactID Zone	0
Location	
Cameras	

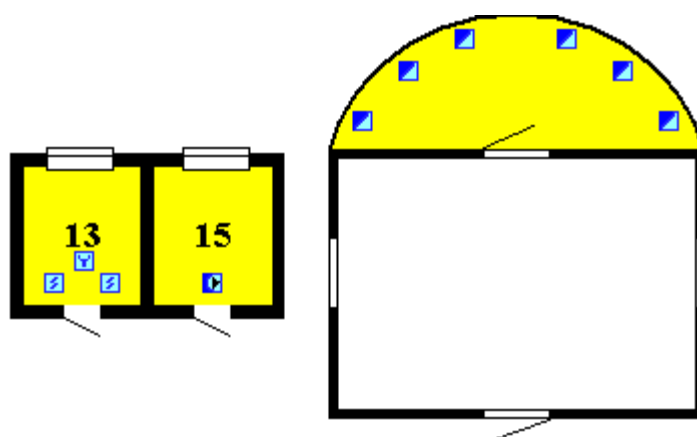
The **Detectors** property is edited in the Map DesignEditor window be opened by clicking the  button (appeared when the property is selected).

The **Location** property is edited in the Map DesignEditor window which can be opened by clicking the  button (visible when the property is selected) in the Inspector box.

The Map (Design) Editor functions are described in *Chapter 6.3.2.8.Map Design Editor*. This chapter discusses map-added icons for Loops and Relay Outputs.

For Loops and Relay outputs you can set one or more type of icons on a map. These settings will be saved in the **Detectors** and **Location** properties.

Examples:

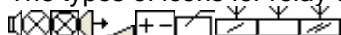


The types of icons for loops:



Ten custom icons can be used.

The types of icons for relay outputs:



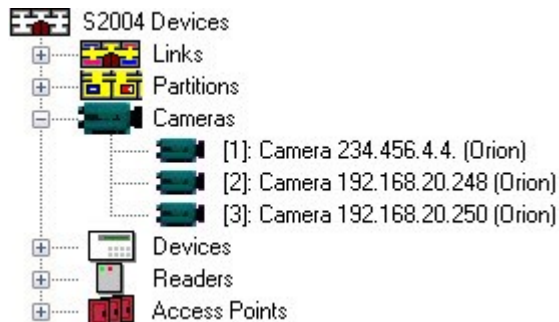
#### 6.3.2.4 The Camera Entity on the Map

The Camera entity can be added to maps to represent graphically the status of the camera on the map and provide advanced camera control capabilities.

One specific Camera entity can be added only to one map that belongs to the workstation where a camera associated to.


Graphically, the camera is an on-map icon clickable to display a camera control menu in the System Monitor module.

In the tree of maps, the Camera entities are associated to the Cameras node:

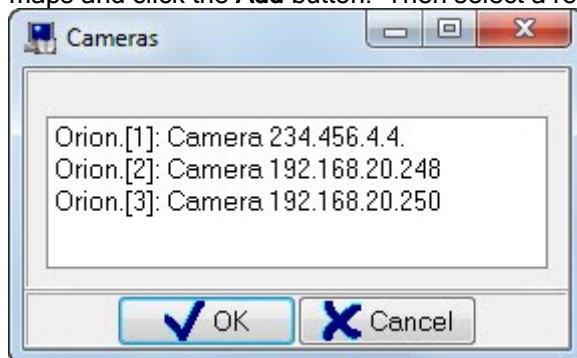


The tree of maps shows the following information for the Camera entity:

- Number
- Name
- Name of video system

 [1]: Axis M1031W (Orion Video)

To add the Camera entity to a map, please select the **Cameras** node of a required map in the tree of maps and click the **Add** button. Then select a required camera in the appeared dialog box and click **OK**:



The **Cameras** dialog box shows all cameras of the current workstation but for the cameras that already placed on any map.

The **Cameras** dialog box shows the video system name and the number and number of a camera.

Using the <Shit> (Range Selection) and <Ctrl> keys (Combined Selection), you can select multiple cameras. When you click **OK**, the selected camera will be added to the map.

To delete the Camera entity from a map, select a required entity from the map and click the **Delete** button. Then confirm the delete action by clicking **Yes** in the appeared window.

*When a camera is deleted from a map, it is not deleted from the database.*

When the Camera entity is added to a map, the **Location** property becomes available in addition to all other properties.


To modify the properties of the **Camera** entity, please select a required entity in the tree and click the **Edit** button, then change properties as required and click the **Save** button.

The properties of the **Camera** entity are described in Chapter 6.2.3.1 *The Camera Entity*. This chapter discusses only the **Location** property items, which are available only in the tree of maps when the camera is added to the map.


Camera properties:

Camera

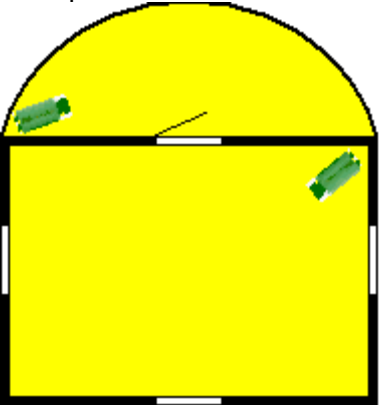
Name	Camera 192.168.20.248
Type	Orion
Camera No	2
Index	2
Location	
Configuration	
Auto rearming	Disabled

The **Location** property item of the Camera is edited in the **Map Design Editor** window which can be opened by clicking the  button (visible when the property is selected) in the Inspector box.

The Map Design Editor functions are described in Chapter 6.3.2.8 *The Map Design Editor*. This chapter discusses types of icons added to a map for the Camera entity.

You can set the location of a camera icon () on a map, which will be saved in the Location property.

Examples:



Types of camera icons:



### 6.3.2.5 The Device Entity on the Map

The Device entity can be added to maps to represent graphically a device state on the map.

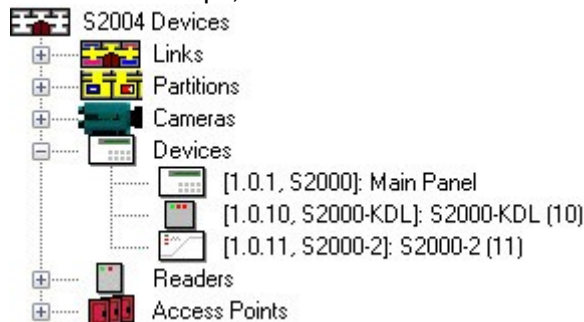
For the S2000-K device, the **Submit a Message** menu is available on a map to send a message to this device.

For the RIP-12 RS device, information about of the device's power will be accessible in the device's card on the map.

One specific Device entity can be added only to one map that belongs to the workstation where the device is associated to.

Graphically, a mapped (on-map) device is an icon of a device

In the tree of maps, the Device entities are associated to the Devices node:

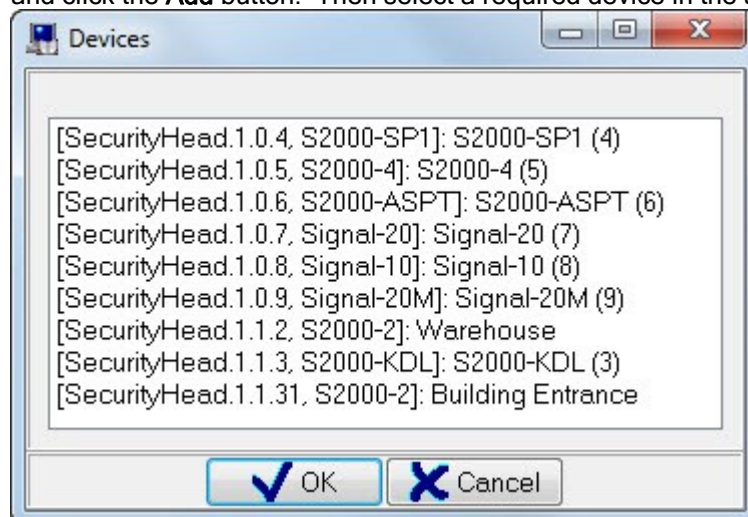


The Tree of maps shows the following information for the Device entity:

- Address
- Type
- Name.



To add the Device entity to a map, please select the **Devices** node of a required map in the tree of maps and click the **Add** button. Then select a required device in the appeared **Devices** dialog box and click **OK**:



The **Device** dialog box shows all devices of the current workstation but for the devices that already placed on any map. The **Devices** dialog box shows a device's name, type, and address.

Using the <Shit> (Range Selection) and <Ctrl> keys (Combined Selection), you can select multiple devices. When you click **OK**, the selected device will be added to the map.

To delete the Device entity from a map, select a required entity from the map and click the **Delete** button. Then confirm the delete action by clicking **Yes** in the appeared window.

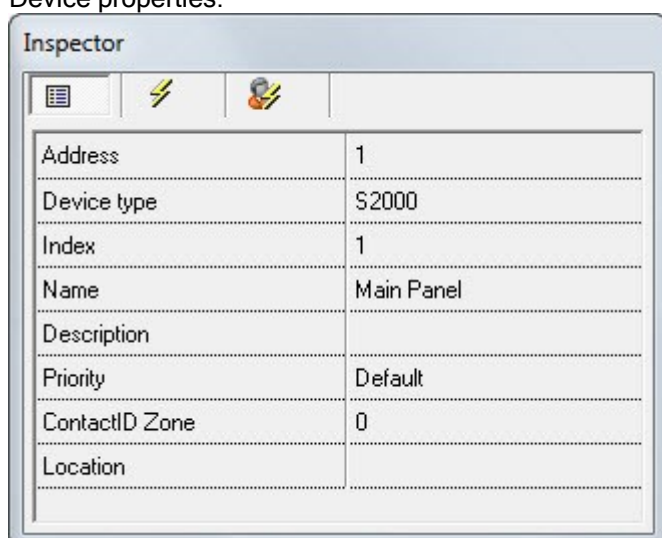
*When a device is deleted from a map, it is not deleted from the database.*

When the Device entity is added to a map, the **Location** property becomes available in addition to all other properties.

To modify the properties of the **Device** entity, please select a required entity in the tree and click the **Edit** button, then change properties as required and click the **Save** button.


The properties of the **Device** entity are described in Chapter 6.2.5.2 *The DeviceEntity*. This chapter discusses only the **Location** property item, which are available only in the tree of maps when the Device is added to a map.

Device properties:



The Inspector window displays the following properties for a device:

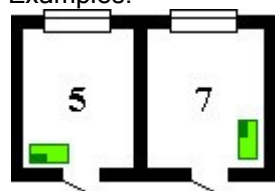
Address	1
Device type	S2000
Index	1
Name	Main Panel
Description	
Priority	Default
ContactID Zone	0
Location	

The **Location** property of the Device entity is edited in the **Map Design Editor** window which can be opened by clicking the  button (visible when the property is selected) in the Inspector box.

The Map Design Editor functions are described in Chapter 6.3.2.8 *Map Design Editor*. This chapter discusses types of icons added to a map for the Device entity.

You can set the location of a Device icon on a map, which will be saved in the Location property.

Examples:



Types of icons for the Device entity:



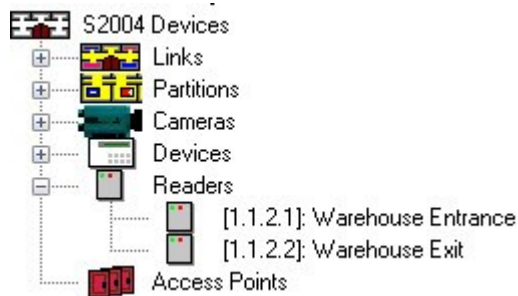
### 6.3.2.6 The Reader Entity on the Map

The Reader entity can be added to the map to represent graphically a reader state.

One specific Reader entity can be added only to a single map that belongs to the workstation where the Reader is associated to.


Graphically, a mapped reader is an icon clickable in the System Monitor to display a menu with access point control options available for the reader, or a menu to send a text message to the (controller).

In the tree of maps, the **Reader** entities are associated to the **Readers** nodes:

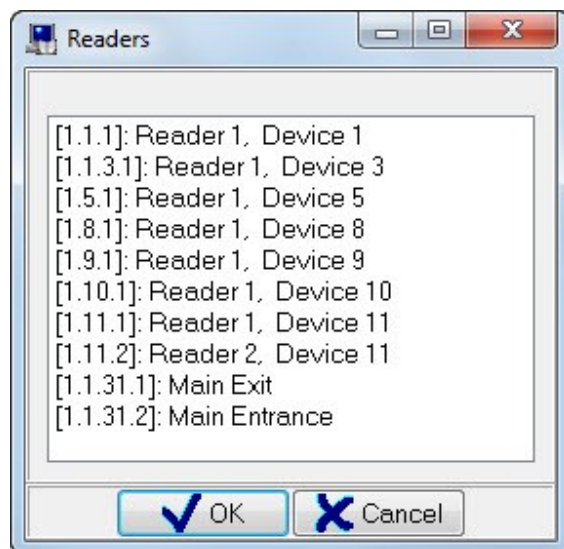


The Tree of maps shows the following information for the Reader entity:

- Address
- Name

 [1.1.2.1]: Warehouse Entrance

To add the Reader entity to a map, please select the **Readers** node of a required map in the tree of maps and click the **Add** button. Then select a required Reader in the appeared **Readers** dialog box and click **OK**:



The **Reader** dialog box shows all Readers of the current workstation but for the Readers that already placed on any map. The **Readers** dialog box shows a Reader's name and address.

Using the <Shift> (Range Selection) and <Ctrl> keys (Combined Selection), you can select multiple Readers. When you click **OK**, the selected Readers will be added to the map.

To delete the Reader entity from a map, select a required entity from the map and click the **Delete** button. Then confirm the delete action by clicking **Yes** in the appeared window.



When the Reader entity is added to a map, the **Location** property becomes available in addition to all other properties.


To modify the properties of the **Reader** entity, please select a required entity in the tree and click the **Edit** button, then change properties as required and click the **Save** button.

The properties of the **Reader** entity are described in Chapter 6.2.5.3 *The ReaderEntity*. This chapter discusses only the **Location** property item, which are available only in the tree of maps when the Reader is added to a map.

Reader properties:

Inspector

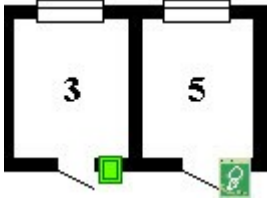
Device address	2
Number	1
User number	11
Name	Warehouse Entrance
Description	
Element type	Reader
Type	Reader
All partitions	No
Photo display events	
ContactID Zone	0
Location	
Cameras	


The **Location** property of the Reader entity is edited in the **Map Design Editor** window which can be opened by clicking the  button (visible when the property is selected) in the Inspector box.

The Map Design Editor functions are described in Chapter 6.3.2.8 *Map Design Editor*. This chapter discusses types of icons added to a map for the Reader entity.

You can set the location of a Reader icon on a map, which will be saved in the **Location** property.

Examples:



Types of icons for the readers: 

### 6.3.2.7 The Access Point Entity on the Map

The Access Point entity can be added to the map to represent graphically an Access Point state.

One specific Access Point entity can be added only to a single map that belongs to the workstation where the access point controller is associated to.

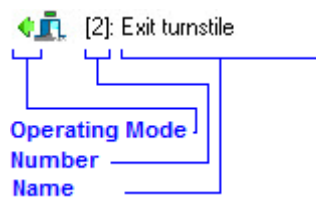
Graphically, a mapped reader is an icon clickable in the System Monitor to display a menu with access control options available for the Access Point.

In the tree of maps, the Access Point entities are associated to the Access Points nodes:

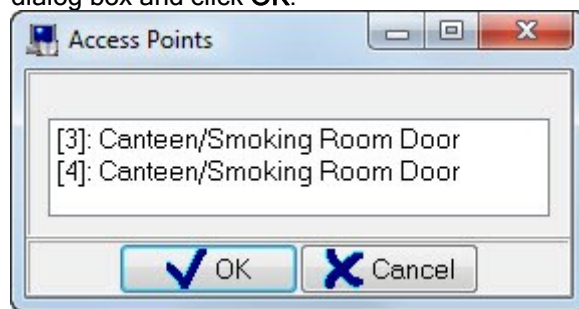


The tree of maps shows the following details for the Access Point entity:

- Operating mode
- Number
- Name



To add the Access Point entity to a map, please select the **Access Point** node of a required map in the tree of maps and click the **Add** button. Then select a required Reader in the appeared **Access Points** dialog box and click **OK**:



The **Access Points** dialog box shows all Access Points of the current workstation but for the access points that already placed on any map. The **Access Points** dialog box shows Access **Points'** names and addresses.

Using the <Shit> (Range Selection) and <Ctrl> keys (Combined Selection), you can select multiple Readers. When you click **OK**, the selected Access Points will be added to the map.




To delete the Access Point entity from a map, select a required entity from the map and click the **Delete** button. Then confirm the delete action by clicking **Yes** in the appeared window.

When the Access Point entity is added to a map, the **Location** property becomes available in addition to all other properties.

To modify the properties of the **Access Points** entity, please select a required entity in the tree and click the **Edit** button, then change properties as required and click the **Save** button.

The properties of the **Access Point** entity are described in Chapter 6.2.5.2 *The Access Point Entity*. This chapter discusses only the **Location** property item, which are available only in the tree of maps when the Access Point is added to the premise map.

Door



Number	2
Name	Exit turnstile
Description	
Type	Turnstile
Operating mode	Exit
Access zone to exit	[0]: Outside World
Exit relay	[SecurityHead.1.1.31.2]: Main Entrance
Exit relay action	Switch on
Exit relay activation time	5
Location	

The **Location** property is edited in the **Map Design Editor** window which can be opened by clicking the  button (visible when the property is selected) in the Inspector box.

The Map Design Editor functions are described in Chapter 6.3.2.8 *Map Design Editor*. This chapter discusses types of icons added to a map for the Access Point entity.

You can set the location of a Reader icon on a map, which will be saved in the **Location** property.

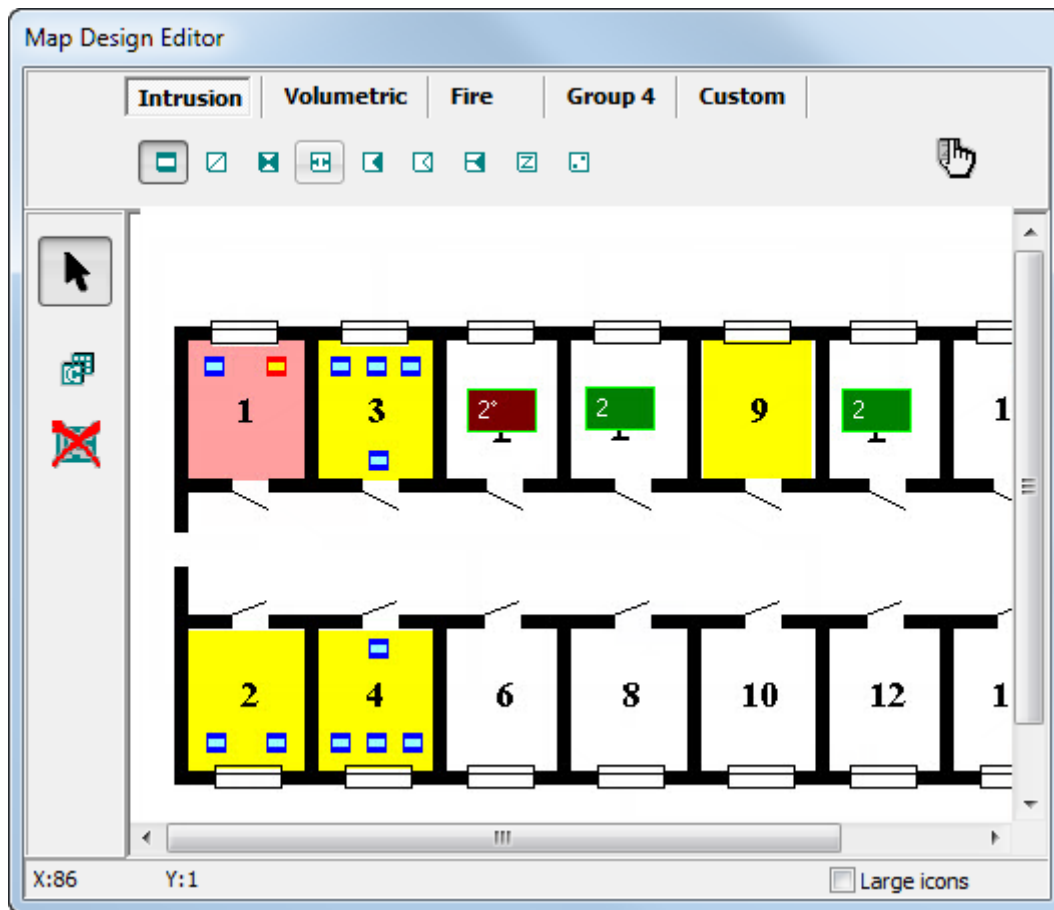
Example:



Types of icons for access points:












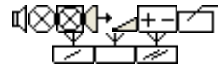

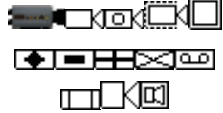


### 6.3.2.8 Map Design Editor




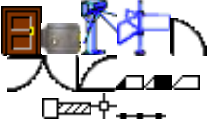


The figure shows that the editor window consist of five areas:

1. Premise map view area
2. Action buttons.
3. Icon selection buttons
4. The Large icons check box.
5. Coordinates of the current mouse pointer.

Icons to represent systems entities when placed on a map

Entity	Type	Maximum icons	Default Icons	All Icons	Rotation capabilities
Link	Area on any shape	-	-	-	-
Partition	Area on any shape	-	-	-	-
Smoke Indicator	Icon	1			No
Heat Indicator	Icon	1			No
Humidity Indicator	Icon	1			No
Loop	One or more icons	2147483647		 + custom icons	No
Relay Output	One or more icons	2147483647			No
Camera	Icon	1			Yes
Device	Icon	1			Yes

Reader	Icon	1			Yes
Door (Access Point)	Icon	1			Yes









Two types of entity representation are available: shaped areas and icons. Let's discuss creating, editing and deleting these two types of representation.

## 1. Area

The Area shape is used for the **Link** and **Partition** entities.


The icon selection toolbar is not available for this type of representation.

Available action buttons are as follows:



Buttons	Description
	Enables mode to select editable polygon area and change the size of a rectangle
	Enables a user to create new rectangular area
	Deletes a selected polygon area
	Enables creating anchor points of a polygon area
	Enables moving anchor points of a polygon area
	Enables deleting anchor points of a polygon area
	Saves changes and closes Map Design Editor
	Overrides changes and closes Map Design Editor


*Please keep in mind, that the area for one Link or Partition entity can include several polygon areas*


To create entity areas on the map you must complete the following:

- Left-click the  function button to go into the mode of creating new rectangular areas.
- Define a new area on the map. To do that, please press and hold down a left mouse button to draw a rectangular area
- Draw more rectangular areas, if needed



A new polygon area is added by drawing a rectangular area. If needed, you can edit the shape of the area:



- You can edit the shape of a polygon area by moving its anchor points. The anchor points are red ones (if you edit the rectangular area, its angular points will be anchor points).
- To modify a shape you should go into the command mode (the  button) and select a required area by clicking one of its anchor points. Then click the  button (move anchor points), left click an anchor point and hold down the left mouse button while dragging the selected anchor points.

To add a polygon area, please click the  button (Add a Polygon Area), and then left click one of the existing anchor points. A new point will be placed on the middle of the line between the selected point and the next clockwise point.

To delete a polygon area, please click the  button (Delete Anchor Points), then left click a point you want to delete.

To delete a polygon area you should complete the following:

- Go into the **Command mode** (the  button) and left click any anchor point of the area you want to delete.
- Left click the  button (**Delete a Polygon Area**)

To quit **Map Design Editor** and save all changes on a map, please click the  button. To quit without saving changes please, click the  button, or press the <Esc>key.

## 2. Icons

Icons are used for entities such as Smoke Indicator, Heat Indicator, Loop, Relay Output, Camera, Device, Reader, Door (Access Point).

There is a toolbar with buttons to select required icons:

- It displays available icons that can be added for the Loop entity:



Using the **Intrusion**,


**Motion**,


**Fire**,

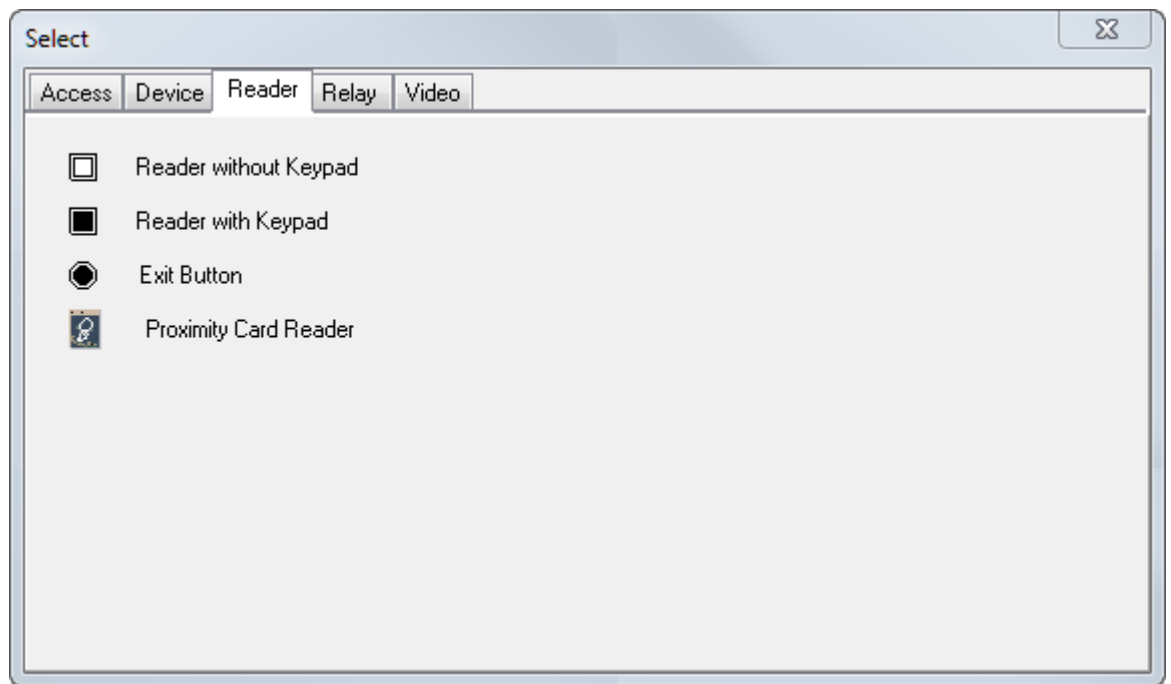
**Group 4**,

and **Custom**

You can toggle between icon groups

You can use the  to open the Select Input Point dialog box.

- The button  is available for Relay Out, Camera, Device, Reader and Access Point entities to select an icon to be placed on a premise map:




(The figure shows the **Select** dialog box for the Reader Entity).

Toolbar action buttons:


Button	Description
	Toggles the command mode to select and move an icon
 or	Enables you to add a new icon.
 or	Deletes a selected icon
	To enter icon inclination angle This field is available only for the Camera, Device, and Reader, Door (Access Point).
	Saves changes and quits the Map Design Editor.
	Cancel changes and quits the Map Design Editor.

To place an icon on a map, please do the following:



- Left click the related function buttons ( or )
- Select a required icon on the icon selection bar.
- Left click the map where you want to place the icon.
- Select the Large icons check box (bottom right)) if you want to use large icons (not available for Smoke Indicator, Heat Indicator)

- When you add icons for Camera, Device, Reader, or Door entities, you can define the icon angle in the  field, as needed.
- When you add icons for Loops and Relay Output, in addition, you can add more icons of related types, if needed.

When necessary, you can move an icon within a map

To move an icon, please click the  button to go in a corresponding mode, Click a required icon and drag the icon while holding down the button.

To delete an icon, please do the following:

- Click the  button to go in the command mode select a required icon by a left click.
- Click the delete button (  or  ), to delete the selected icon.

To quit and save all changes on **Map Design Editor**, please click the  button. To quit without saving changes please, click the  button, or press the <Esc>key.

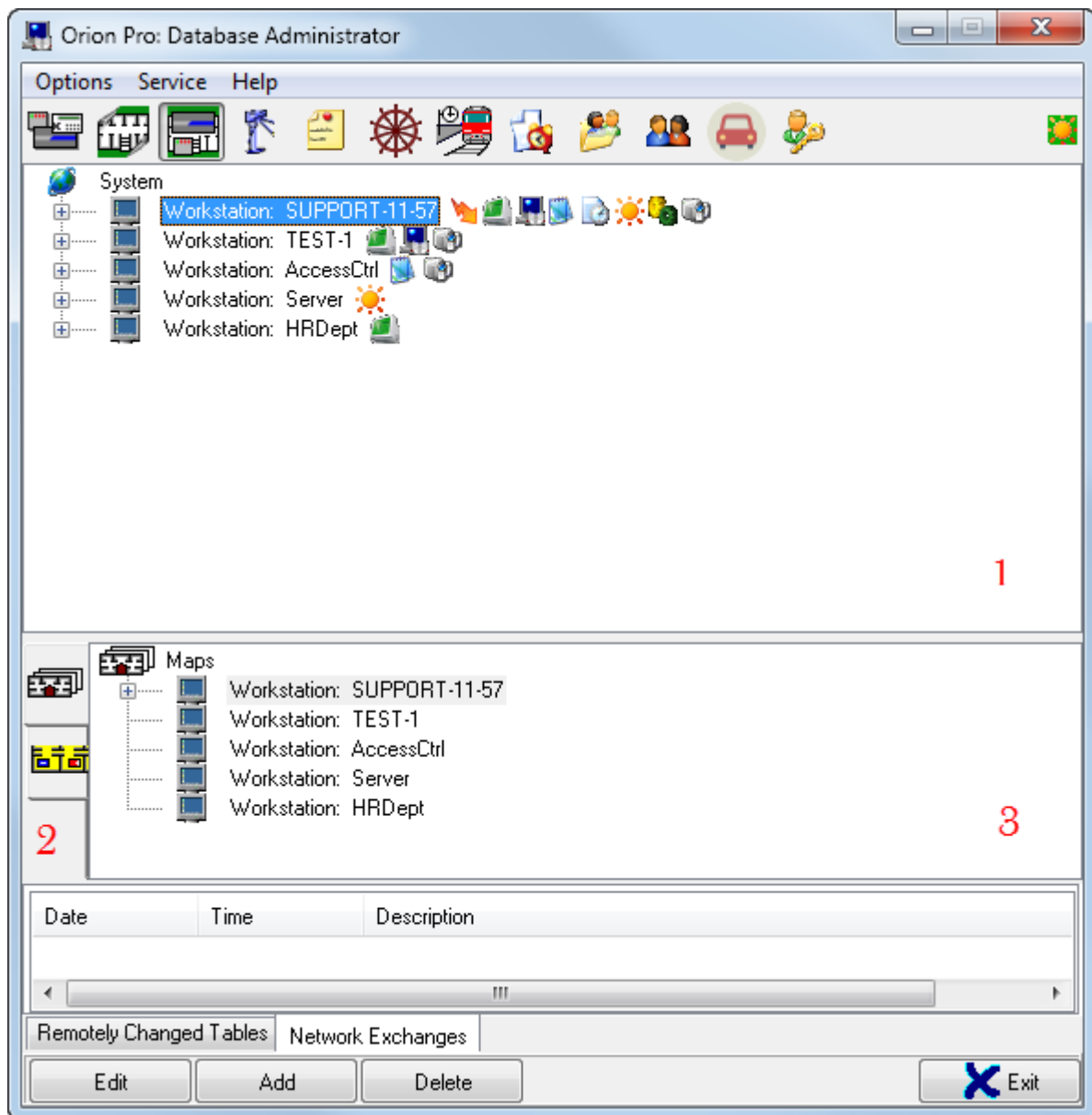
*It is worth mentioning that the Orion Pro software allows editing all icons. To edit the icons, you can use the Orion Pro GUI Editor module (see Chapter 15 Orion Pro Graphical User Interface), or other graphics editor to edit icon image files located in the Data subfolder of the folder with installed Orion Pro (a sensor.bmp contains default icon images; sens15.bmp contains larger icon images).*

**IMPORTANT!** *When the sensor.bmp and sense 15.bmp files are edited, these files must be copied to all workstations where the Data Administrator and System Monitor modules run.*

*It should be noted, that Orion Pro allows associating images related to other entities (not recommended). To do that, you have to select Extended List of Map Elements in the settings of Database Administrator (See chapter Database Administrator Settings). In this case, all images will be available for any type of entities.*



## 6.4 The System Structure Tab. Intrusion and Fire Centralized Control



The System Structure Tab shows the following:

1. Tree of System Entities.
2. View Toggle Buttons



- Toggles the **AreaMaps** view



- Toggles the **Partition and Partition Groups** view.

3. The area of selected view.

The tree of system entities are described in the chapter dealing with the Device Addresses tab  
The tree of maps and tree of partition and partitions are described in the chapter dealing with the Maps tab.

The System Structure tab enables the users to do the following:

- Configure centralized control for relay outputs

- Set the transmission of events and states related to the logical entities of the system
- Associate control elements to the system readers
- Configure system responses to the events of entities
- Set display of a card holder photo in the System Monitor modules
- Associate cameras to device zones
- Associate partitions to keybox cylinders

#### 6.4.1 Configuring Centralized Control of Relay Outputs

The Orion Pro Scanning Core can control the relay outputs of S2000-2, S2000-4, Signal -20/02, Signal -20P, Signal-20P ver. 2.04, Signal-20M, Signal-10, S2000-KDL, S2000-KDL-2I, S2000-KDLS, S2000-SP1, S2000-KPB, S2000-ASPT ver 3.00. The relay outputs controlled by Scanning Core or S2000/S2000M panel are hereinafter called **system relay outputs** (unlike **local relay outputs** of alarm control devices where these devices themselves control the relay outputs).

System relay outputs can be used to control annunciators (audible and visual) and actuators (locks, etc.), and to communicate alarms and alerts to a central alarm station.

The system relay outputs' responses depends on the status of a partition, partition group or predetermined relay action (relay program).

*The properties of Relay Output are described in Chapter 6.2.6.5 The Relay Output Entities, and the centralized (relay) control programs are described in Appendix 6A. Centralized Relay Control Programs and in Appendix 6B. Centralized Relay Control Action Scenarios.*

To configure the centralized control of relay outputs by directly assigning relay action to a relay output, please do the following:

- 1) Select relay outputs to be used for system control
- 2) Determine whether the S2000M or Orion Pro Scanning Core is to be used to control the relay outputs
- 3) Define the partition and partition groups to affect the states of the selected relay outputs:
- 4) Determine how the states of relay outputs responses to the states of the associated partition and partition groups, in other words, you should select relay actions (or a relay control program)

The next two chapters described two versions of configuring relay outputs :

- Old scheme assumes direct assignment of a relay action (relay control program)
- New control scheme assumes usage of management scenarios.

The difference between these two schemes is as follows:

In the process of the new scheme implementation, a partition state is monitored but states of partition groups are not analyzed.

The new control scheme has more tactics. Furthermore, some tactics (relay actions) have been revised: (more monitored states have been added. A Manual Release loop has been implemented to affect extinguishing tactics, etc.)

*Note that the old scheme and the new one assume that output and the output-associated partitions belong to the same Scanning Core.*

##### 6.4.1.1 The Old Control Scheme. Direct Tactic Association

First, select a relay output to be used for the system-based control. Please be sure that the selected output is not locally controlled by the device itself.

It should be remembered that the relay output is not locally controlled when the relay output has no associated loop but has the **Not manage** tactic set in the settings of a physical device (using the Uprog configuration utility).

It also should be kept in mind that:

For the S2000-ASPT/03 device, only relay output **6 Auxiliary Equipment Control** can be used as a system output.

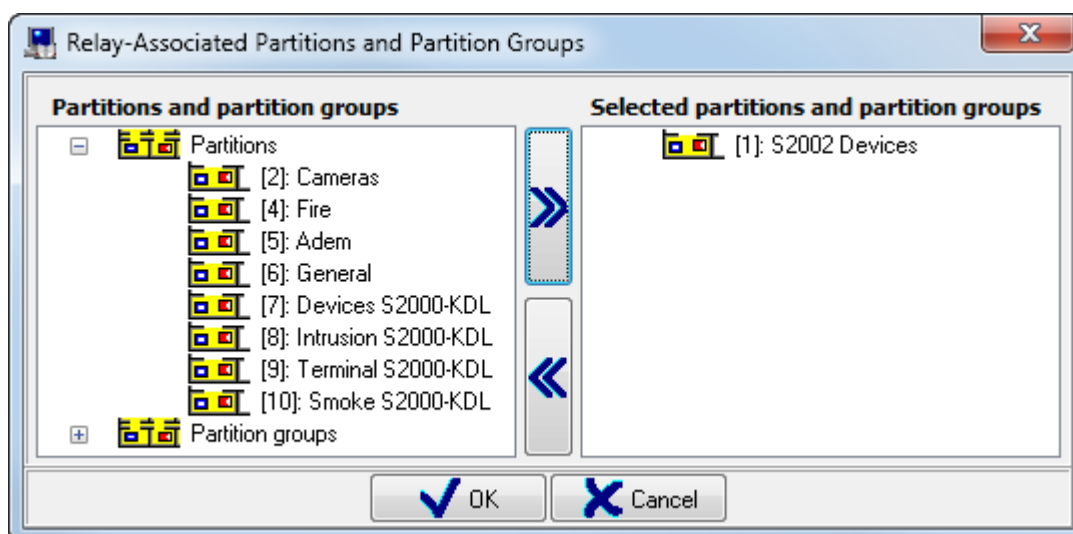
For the S2000-2 device, only relay output **2** can be used as a system output when the S2000-2 device operates in the One-way access door mode (as configured with the Uprog utility).

For the S2000-4 device, any relay output can be used as a system output, but relay output 1 can be used as a system output only when the device is not used for access control.  
Since a relay output will be controlled according to the selected tactic (program), please select a required relay output and set a proper value for the Centralized Control attribute:

Centralized Control = No		Centralized Control = Yes	
Orion Pro Protocol	Orion Protocol	Orion Pro Protocol	Orion Protocol
The Scanning Core controls an output	The Scanning Core controls an output	The Scanning Core controls an output	The Scanning Core controls an output
Centralized control settings for this output are exported to the S2000/S2000M Panel that will be responsible for the relay output control.	Centralized control settings for this output are exported to the S2000/S2000M Panel that will be responsible for the relay output control.	Centralized control settings for this output are not exported to the S2000/S2000M Panel and it will not be control the relay output.	Centralized control settings for this output are exported to the S2000/S2000M Panel and it will not control the relay output.
Used when in the Orion Pro protocol, the control is provided using the S2000/S2000M Panel.	Used when the Scanning Core is backed up by the S2000/S2000M Panel as a standby	Used, when the Scanning Core is responsible the control in the Orion protocol	Used when the Scanning Core is <b>not</b> backed up by the S2000/S2000M Panel as a standby.


Then, you should define what partitions and partition group will affect the status of the selected relay output.


Please select a required relay output in the tree of entities and click the **Add** button to open the Relay-Associated Partitions and Partition Groups (Related):



The right pane displays the list of partitions and partition groups related to the relay output.


The left pane displays the list of all others partitions and partitions group of the current workstation.

To associate a partition or a partition group to the relay output, please select a required partition (or partition group) from the Partition and partition groups list and double click it or use the  button in the middle of the window

You can select multiple partitions or partition group using <Shift> (Range Selection) or <Ctrl> (Combined Selection) and click the  button to associate all of them to the relay output.

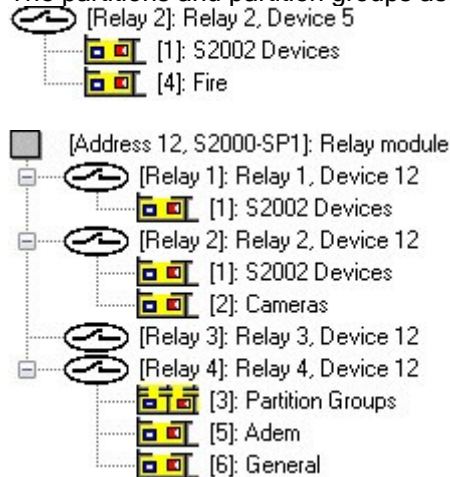
To remove an association a partition or partition group to the relay output, please select and double click a partition or a partition group associated to the relay output, or you can use the button in the middle of the window.

Using <Shift> (Range Selection) or <Ctrl> (Combinend Selection) you can select multiple associations to

remove them using the  button.


Then click the **OK** button to accept your changes

The partitions and partition groups associated to the relay output will be displayed in the system tree:




The tree of system entities shows the following information for the Partition entity:

- Number (ID)
- Name

 [5]: Adem

The tree of system entities shows the following information for the Partition Group entity:

- Number (ID)
- Name

 [3]: Floor 1

As said before, you can delete the association of partition or partition group to a relay output using the **Relay-Associated Partition and Partition Groups** window.

In addition, in order to delete the association of partition (or partition group) to a relay output, you can select the partition or partition group associated to a required relay output in the tree of system entities, then click the **Delete** button. Then confirm the delete action by clicking **OK** in the appeared dialog box.

The last step of configuring the relay centralized control is to define how the status of relay output depends on the states of this relay associated partitions.

This will require proper settings to be made for the **Tactics**, **Relayaction delay**, and **Relay action time** properties.

*All centralized control programs (relay programs) are described in Appendix 6.A Relay centralized control programs*

For example, we have a fire partition. When a Fire loop alarm (Fire) event occurs, the first system relay output, responsible for sound alarm, is to be activated (ON), then after 30 seconds the second relay output responsible for fire extinguishing is to be activated (ON) for 5 seconds.

So, the partition is associated to both relay outputs with the following settings:

- For the 1st relay output:

Tactics	ON
Relay action delay	0,000
Relay action time	0,000

- and for the 2-nd:

Tactics	ON
Relay action delay	30,000
Relay action time	5,000

*It should be kept in mind that the Signal-20P ver2.02 and earlier, and Signal-20P require that timing parameters have to be set in the settings of the device itself. Furthermore, the Signal-20P ver.2.03 requires any value rather than 0 is to be set for the **Relay action time** parameter (for example: 0, 125)*

#### 6.4.1.2 The New Control Scheme. Using Control Scenarios

First, select a relay output to be used for the system-based control. Please be sure that the selected output is not locally controlled by the device itself.

**Again**, it should be remembered that the relay output is not locally controlled when the relay output has no loop associated but has the **Not manage** tactic set in the settings of a physical device (using the Uprog configuration utility).

It also should be kept in mind that:

- For the S2000-ASPT/03 device, only relay output 6 **Auxiliary Equipment Control** can be used as a system output.
- For the S2000-2 device, only relay output 2 can be used as a system output when the S2000-2 device operates in the One-way access door mode (**as configured with the Uprog utility**).
- For the S2000-4 device, any relay output can be used as a system output, but relay output 1 can be used as a system output only when the device is not used for access control functions.

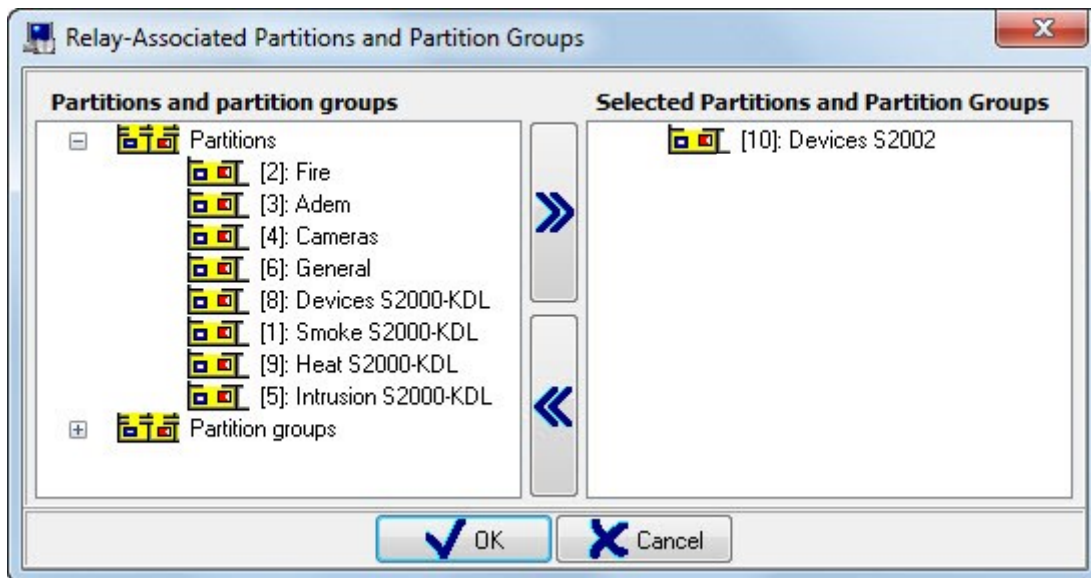
Since a relay output will be controlled according to a management scenario, please select a required relay output and set a proper value for the Centralized Control property:

Centralized Control = No		Centralized Control = Yes	
Orion Pro Protocol	Orion Protocol	Orion Pro Protocol	Orion Protocol
Scanning Core controls an output			
The settings for centralized control of this output this output will be exported to the S2000/S2000M Panel that will be responsible for the relay output control.	The settings for centralized control of this output will be exported to the S2000/S2000M Panel.	The settings for centralized control of this output this output will not be <b>not</b> exported to the S2000/S2000M Panel that will not be responsible for the relay output control	The settings for centralized control of this output this output will not be exported to the S2000/S2000M Panel
<b>These settings are wrong</b>	Applicable when the S2000/S2000M Panel is used as a standby for Scanning Core	Used in the Orion Protocol, when the Scanning Core is responsible for the control	Applicable when the S2000/S2000M Panel is used as a standby for Scanning Core
	The parameters for the output control must be specified.		

Then, you should define what partitions must affect the status of a selected relay output.


*Important! The status of partition groups is not analyzed by the Scanning Core.*

To define relay-affecting partitions, please select a required relay output in the tree of entities and click the **Add** button to open the Relay-Associated Partitions and Partition Groups:




The right pane shows the partitions associated to the relay output.  
The left pane shows all the other partitions and partition group of the current workstation.


To associate a partition to the relay output, please double click a required partition from the list or use the

 button in the middle of the window


You can select multiple partitions using <Shift> (Range Selection) or <Ctrl> (Combined Selection) and

click the  button to associate all of them to a relay output.

To remove the association of a partition to the relay output, please select and double click a partition

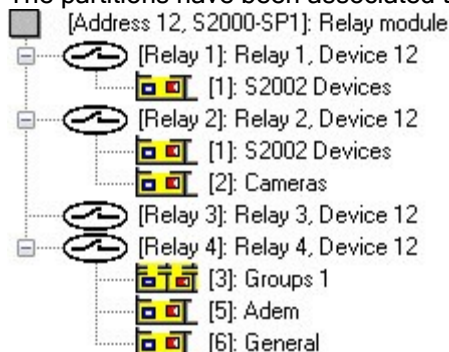
associated to the relay output, or you use the  button in the middle of the window.

Using <Shift> (Range Selection) or <Ctrl> (Combined Selection) you can select multiple associations to

remove them using the  button.

Then click the **OK** button to accept your changes.

The partitions have been associated to the relay output will be displayed to the tree of system entities:



The tree of entities displays the following for the Partition entity:

- Number
- Name.

 [1]: S2002 Devices

As said before, you can delete the association of a partition to the relay output using the **Relay-Associated Partition and Partition Groups** window.

In addition, in order to delete the association of a partition to the relay output, select the partition associated to a required relay output in the tree of system entities, then click the **Delete** button. Then confirm the delete action by clicking **Yes** in the appeared dialog box.

The last step of configuring the relay centralized control is to define how the status of relay output depends on the states of this relay associated partitions.

This requires a scenario to be created for each partition (associated with the relay output). A scenario is a list of relay outputs (related to the partition) in the form of tactics (relay programs)

Then this scenario should be associated to the **Status Changed** event of the partition.

It is clear that:

- When the list of relays is the same for two or more partition, only one scenario may be created but it is associated to all partitions
- Tactic (relay program) for one individual relay **must be the same** in all management scenarios

*All relay-related scenarios are described in Appendix 6.B Relay Centralized Control Scenarios. Chapter 6.6.1 Creating Centralized Control Scenarios describes the process of creating a scenario. Associations of scenarios to the system entities are described in Chapter 6.4.4 Configuring System Response to System Events.*

Let's consider the following example:

Let's assume that the following outputs have to be controlled

- Output 1 by **Activate** relay program as a response to the states of Partition1, Partition2, and Partition3
- Output2 by the Siren relay program as a response to the status of Partition1, Partition2, and Partition3
- Output 3 by the **Deactivate** tactic as a response to the status of Partition1 and Partition2

Let's create two scenarios:

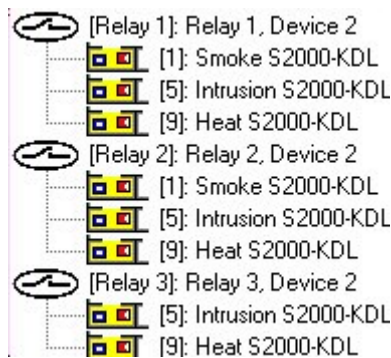
- Scenario1

Scenario steps	
[Out] Tactic 1- Switch On	
[Out] Tactic 12-siren	
[Out] Tactic 2 - Switch off	
Relay	[SecurityHead.1.12.1]: Relay 1, Device 12
Relay	[SecurityHead.1.12.3]: Relay 3, Device 12
Relay	[SecurityHead.1.12.2]: Relay 2, Device 12

- Scenario2

Scenario steps	
[Out] Tactic 1- Switch On	
[Out] Tactic 12-siren	
Relay	[SecurityHead.1.12.1]: Relay 1, Device 12
Relay	[SecurityHead.1.12.2]: Relay 2, Device 12

Then we will associate the partitions to the relay:



Please associate the scenarios to the partitions as follows:

- Scenario1 to the Status Changed event of Partition1 and Partition2,
- Scenario 2 to the Status Changed event of Partition 3.

**Note! Important!** Since relay actions are based on the control scenarios, the settings must be provided for the **Tactic**, **Relay action delay**, and **Relayactiontime** properties when the control settings have to be written to the S2000/S2000M panel in case of database exporting (used for the Orion protocol, see the table above).

For example, we have a fire partition. When a Fire loop alarm (Fire) event occurs, the first system relay output, responsible for sound alarm, is to be activated (ON), then after 30 seconds the second relay output responsible for fire extinguishing is to be activated (ON) for 5 seconds.

So, we have the partition associated to both relay outputs with the following settings:

- For the first relay:

Tactics	ON
Relay action delay	0,000
Relay action time	0,000

and

For the second relay:

Tactics	ON FOR A TIME
Relay action delay	30,000
Relay action time	5,000


*It should be kept in mind that the Signal-20P ver2.02 and earlier, and the Signal-20P require timing parameters have to be set in the settings of the physical device itself. Furthermore, the Signal-20P ver.2.03 requires any value rather than 0 is to be set for the **Relay action time** parameter (for example: 0,125).*

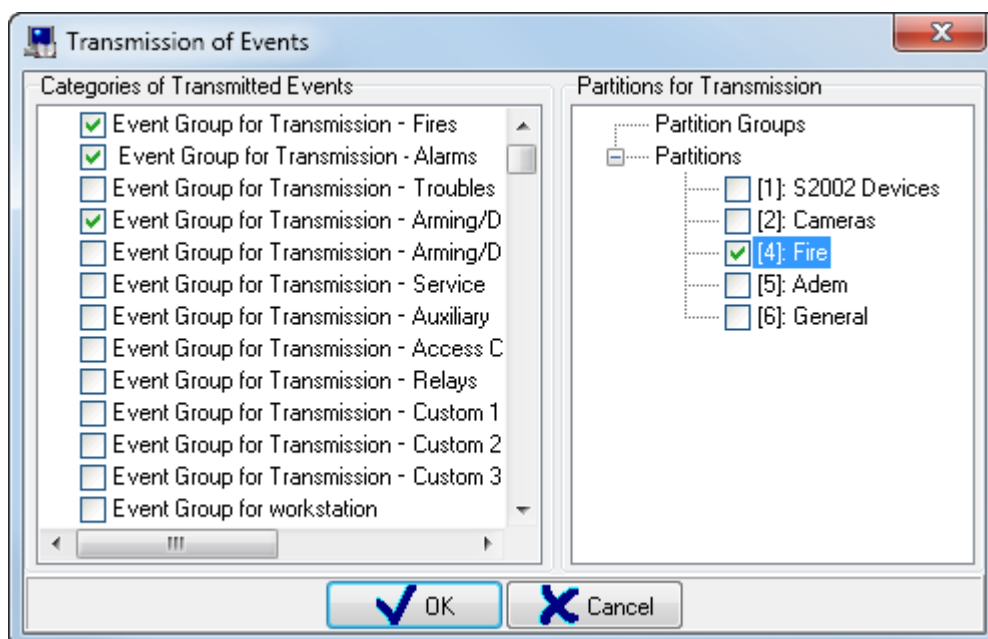
## 6.4.2 Setting Transmission of Events and System Entity States

Events can be transmitted to the S2000-K keypad (ver 1.04 and higher) to show them on the LCD display and generate sound when an alarm event is received, this device also has nonvolatile storage for the system events. The events can be also transmitted to the S2000-IT Phone Communicators, OU-4S GSM-Based **Annunciator**, and S2000-PGE GSM& Ethernet-Based System.

**Partitions (partition groups) triggering events transmitted to the device can be configured individually for each device.** Using this feature one can define what events (e.g alarm or fire events) are allowed for transmission and what events are not (e.g arming and disarming). Using the list of partitions/partition groups, you can allow transmission only those events that are triggered in the partition or partition groups selected from the available list.



To set the transmission of events to a certain device, please select any of the S2000-K, S2000-IT, UO-4S or S2000-PGE device from the tree as required and click the **Edit** button, then select the **Transmission** property and click the  button to open the **Transmission of Events** dialog box.



Groups of events to be transmitted to the device are selected in the left part of the window, and partitions and partition groups of the transmitted events are selected in right part of the window

It is recommended to use the first **twelve** event groups:

The first **nine** groups are corresponds to group of events contained in the S2000/S2000M panel.

The next three groups do not include events by default. Thus, you can create **three** groups of events to meet your needs as required

*Event groups can be edited in the Settings/Setting EventGroups menu (See Chapter 6. 14.3).*

You can also use the Partition Event Group for a partition group.

Please consider the following specifics of event transmission in the Orion Pro Integrated Security System

- In order S2000-K keypads can display events transmitted by the panel, the **Event Indication** and **Alarm Indication** parameters must be set in the device itself.
- The S2000-K keypad may not support some messages from the S2000/S2000M panel and the Scanning Core of the Orion Pro software. Such messages will not be displayed.

The transmission rate of the S2000-II, OU-4S or S2000-PGE hardware is not high. It is recommended to transmit only important and critical events (alarm and fire) to a communicator. Considering this, you should select (permit) only event groups that are required and to ban the transmissions of other groups.

### 6.4.3 Associating Control Elements to System Readers

Users can get access to partition and partition groups when the present the following:

- Enter password into S2000 and S2000M panels or using S2000K or S2000-KS keypads
- Present the TouchMemory or Proximity card to readers connected to the S2000-2, S2000-4, Signal-20P, Signal -10, and S2000-KDL, S2000-KDL-2I, S2000-KDLS, S2000-PT, S2000-BKI, S2000-BI, and UO-4S;

**Important!** Note that the User cannot control (operate) more than one partition or partition group via one specific reader using a TouchMemory button or Proximity card.

The User will have an access to control (operate) partitions and partition groups, if the User have rights to control (operate) these partitions and partitions groups, and the permission is assigned to the reader to be used for that purpose.

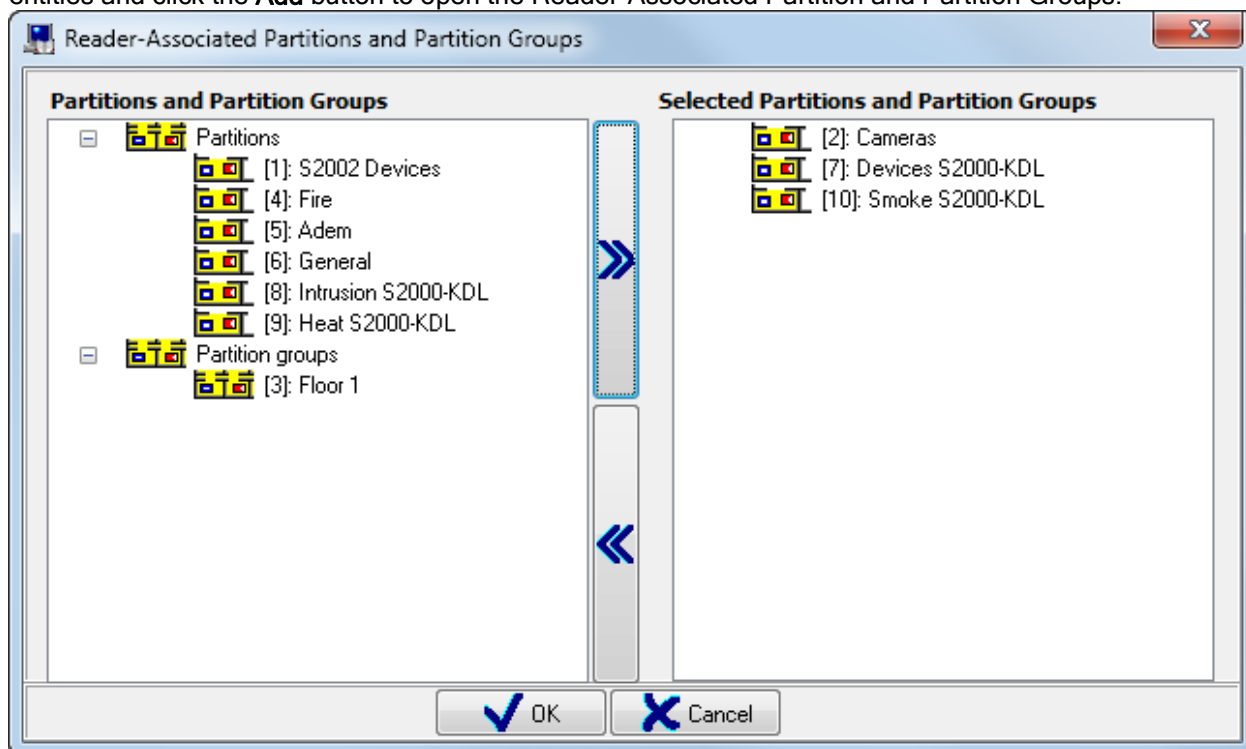
The User's rights are defined by the access level of his/her password. An access level defines the list of allowed partitions and control rights for each partition  
The relevant information is provided in Chapter 6.10.1 Creating Access Levels to Control Intrusion and Fire Entities, and in Chapter 6.12.3 Creating Credentials: TouchMemory buttons, Proximity cards and fingerprints.

Permissions of a reader are defined by the list of partitions and partition groups allowed to be control via this reader.

To allow a partition (or a partition group) to be controlled with a reader, please associate the partition or partition group to this reader.


In other words, when we associate a partition or a partition group to a reader, we inform the system that the reader is allowed to control (operate) this partition or partition group.


To associate a partition (or a partition) group to a reader, please select a required reader in the tree of entities and click the **Add** button to open the Reader-Associated Partition and Partition Groups:




The right part of the window includes the partitions and partition groups associated to the reader.  
The left part of the window includes all the other partitions and partitions groups of the current workstation.


To associate a partition (or a partition group) to the reader, please select a required partition or partition group from the list of partitions and partitions groups, then double click the selected item with left mouse

button or use the  button located in the middle of the window

Using <Shift> (Range Selection) <Ctrl> (Combined Selection) you can select multiple partitions or partition groups, then use the  button to associate all of them to the reader

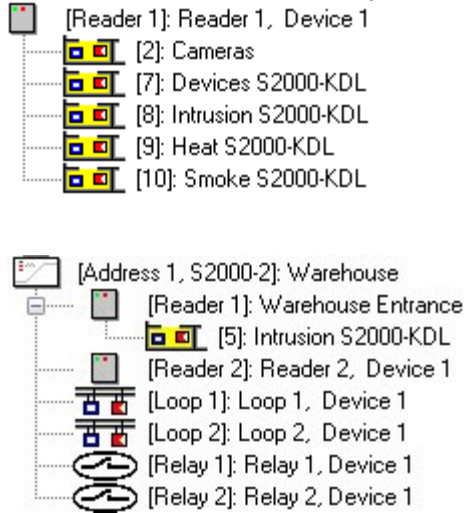
To delete the association of a partition (or a partition group) to a reader, please select a required partition (or a partition group) from the list of partitions or partition groups associated the reader, then double click

it or use the  button in the middle of the window.

You can use <Shift> (Selection Range) or <Ctrl> (Combined Selection) to select multiple partitions or partition groups and delete the associations of all selected partition and partition groups using the  button.

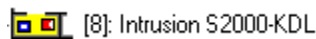
Then click the OK button to accept all changes.

Associated to the reader , the partition and partition groups have appeared in the tree of system entities:



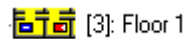
The tree of the system entities shows the following information for the Partition entity:

- Number
- Name



The tree of the system entities shows the following for the Partition Group entity:

- Number
- Name

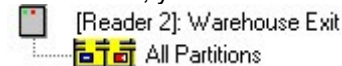


As said above, you can delete the association of partitions or partition group to a reader using the **Reader-AssociatedPartitionsand Partition Groups** dialog box.

In addition, in order to delete the association of a partition (or a partition group), please select a required partition (or partition group) associated to a required reader, then click the **Delete** button. Next, click the **Yes** button to confirm the delete action.

It is also possible to define that a reader can to be used to control operate all partition of the workstation. To do that, you should select **Yes** for the **All partitions** property of the reader.

In this case, you will see **All Partitions** virtual entity associated to this reader in the tree of system entities:



*The properties of the Reader entity are described in the Chapter 6.2.6.3 The Reader Entity.*

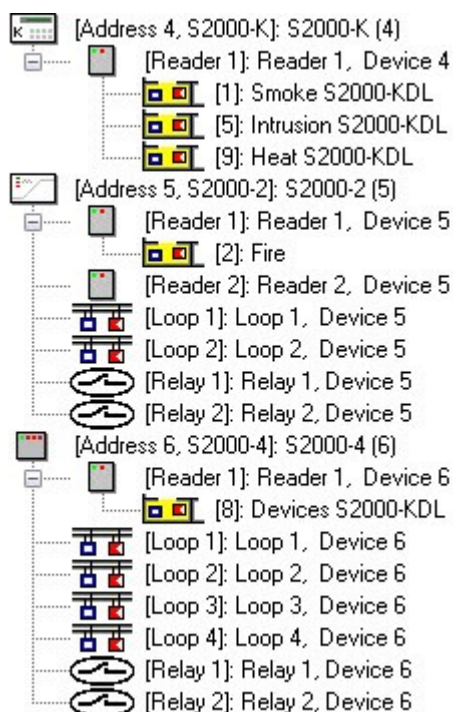
*It should be noted that unlike Orion Pro Suite, the S2000/S2000M panel support association to a device rather than to a reader. Thus, in the Orion Pro Suite, you can provide settings for the use of TouchMemory button or Proximity card to control (operate) two partitions (or two partition groups) with two readers of one S2000-2 device - one reader for each partition (or partition group). But when exported to the panel, both readers of the S2000-2 device are allowed to control (operate) one **and the same partition (or partition group) only.***

*Further, we will consider the example of assigning permissions to control partitions, including associating of partition to a reader*

- There are five partitions. The first three partitions will be controlled with a S2000-K keypad using a PIN code, the fourth partition will be controlled with a S2000-2 device using a TouchMemory

button or Proximity card, and the fifth partition will be controlled with a S2000-4 using the same token.

- First, an access level must be created, which describes operating permissions for all five partitions.
- Next, we will associate the first three partitions to a S2000-K device, the fourth partition will associate to S2000-2, and the fifth partition will be associated to the S2000-4 device



- Last, PIN code and TouchMemory button are added to the system with access level created being assigned.

#### 6.4.4 Configuring System Responses to the Events of System Entities

System responses to the events are provided on the basis of scenarios. Scenarios are micro programs responsible for specific actions (mainly, they send commands to the system entities). To make it simple, a management scenario is a sequence of actions with each responsible for a specific action.

The scenarios can be initiated automatically as a response to system events.

Management scenarios are described in Chapter 6.6 Management Scenarios. Examples of using scenario are provided in Chapter 6.6.3. Examples of Tasks Completed Using Management Scenarios. This chapter focuses on setting of scenarios as responses to events occurred in the system

In the Orion Pro system, the management scenarios are completed by the Scanning Core


The events of system entities are described in Chapter 6.2.12 The Events of Entities. Here, we only recall what system entities have events:

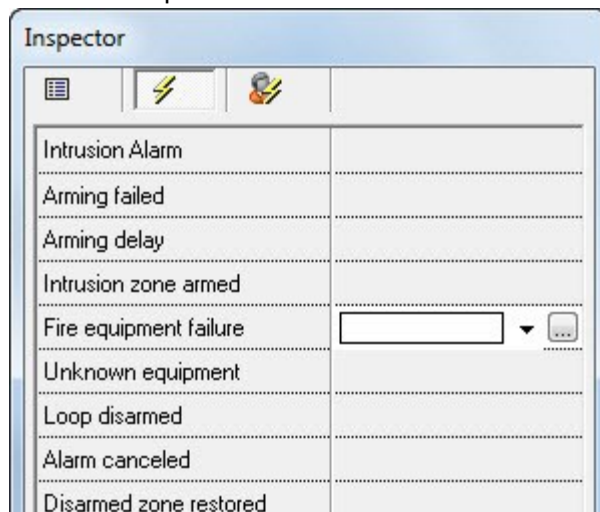
Entity	Events	
	Own	Virtual
Workstation	✓	✓
Video System	✓	✓
Camera	✓	✗
Device/Biometric Reader/Subscriber/Keybox	✓	✗
Reader	✓	✗
Loop/Subscriber Zone/Keybox cylinder	✓	✗
Relay Output	✓	✗
Partition	✓	✓

Partition Group	✓	✗
Access Zone	✗	✓

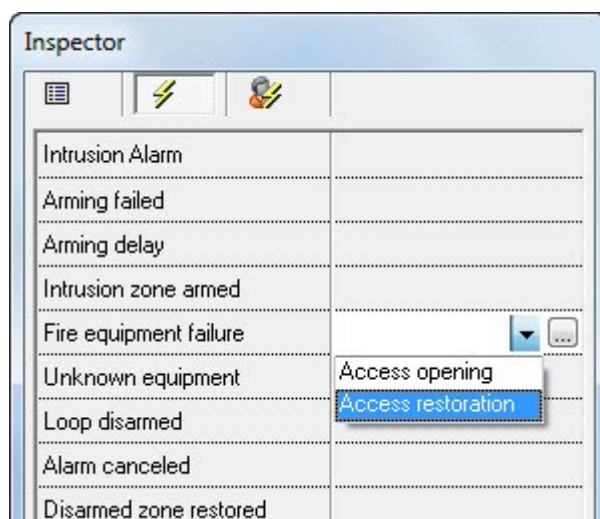
To make a scenario triggered by an event occurred in respect to a specific entity, it should be associated to that event.

To associate scenario to an entity event, please do as follows:

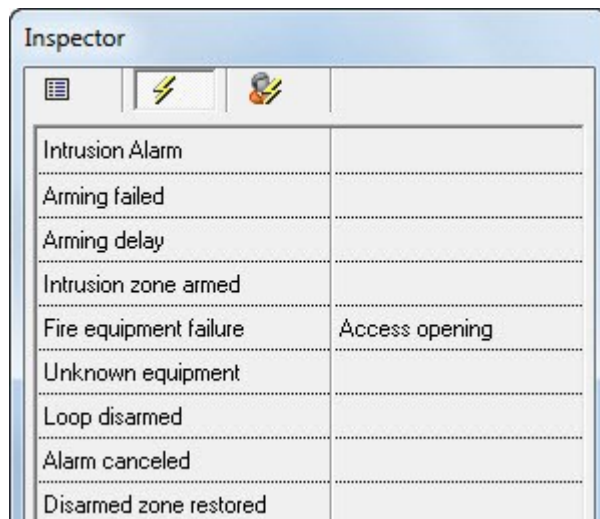
- Go to the System Structure tab (or the Access tab, if a scenario will be associated to the events of the Access Zone entity):
- Select the system entity, to the events of which the scenario will be associated, in the tree of system entities, or in the tree of partitions and partition groups, or in the tree of maps
- Click the Edit button to start the editing mode
- Click the button  in the Inspector toolbox to toggle the Associating Management Scenarios to Entity Events.
- Choose a required event:



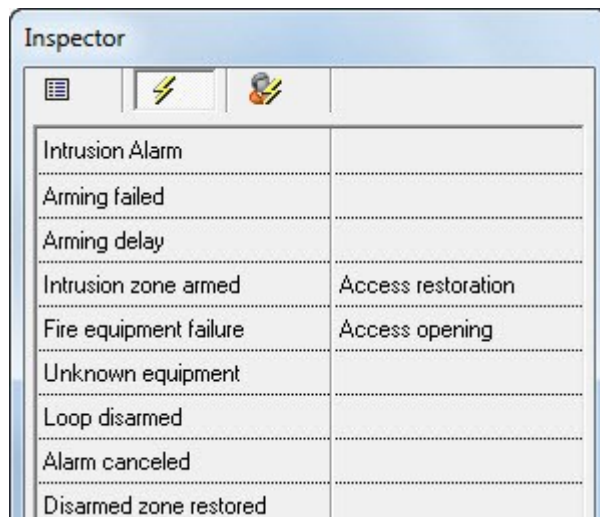
- Then select a scenario (action):



- The selected scenario will be displayed in the Inspector of entities:




- The scenarios can be associated to other entity events as required:

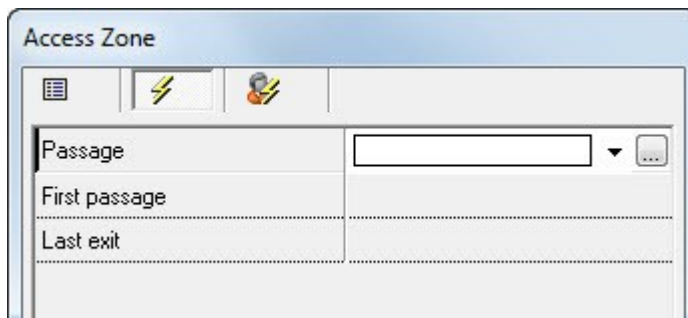


- If you need to delete an association of scenario to an event, please select this event and press the <Del> key on the keyboard.
- To save all changes, click the **Save** button

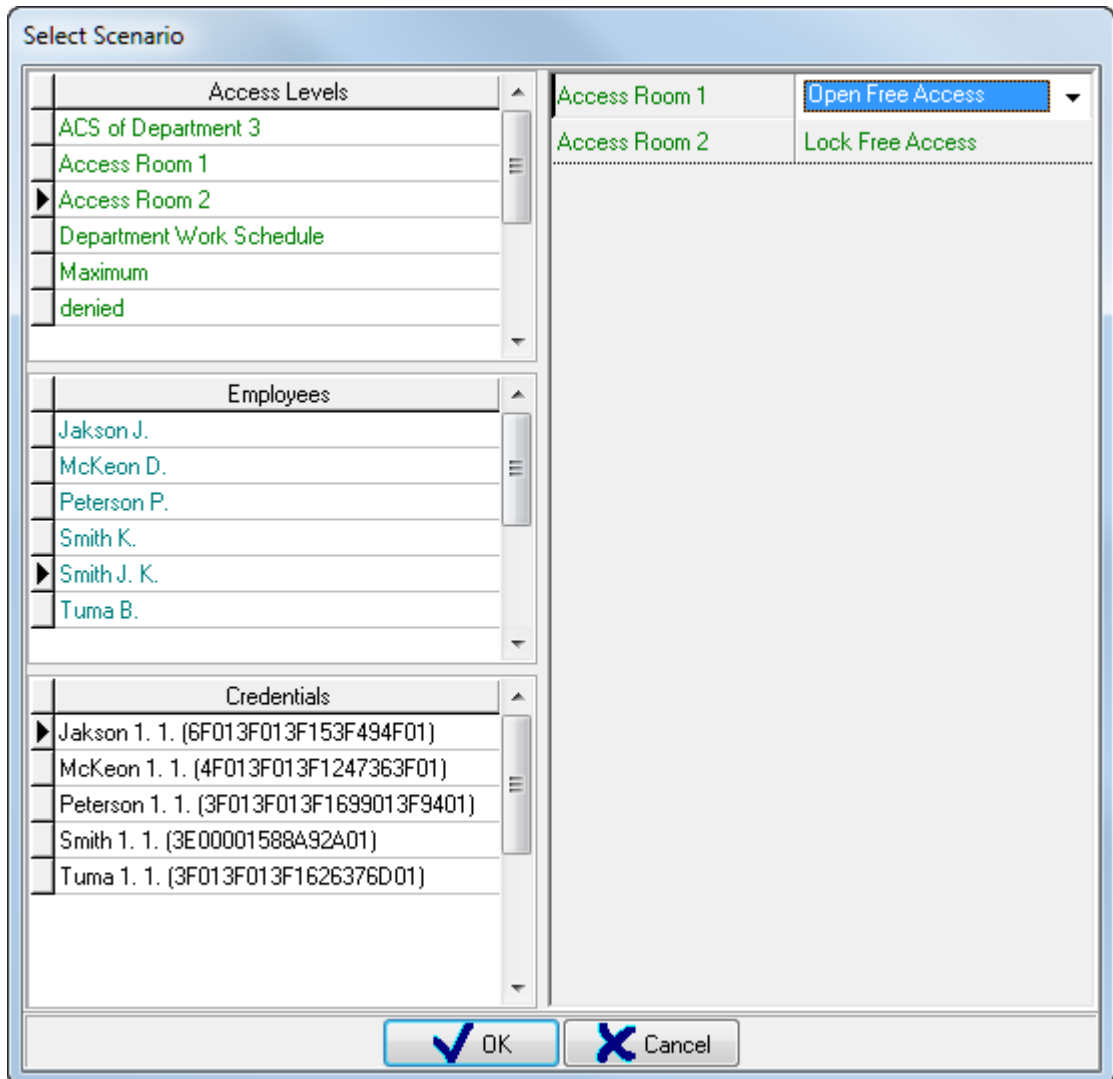
Scenarios can be launched as responses to the events initiated by a specific person or by a person with specific access level or specific credentials (PIN code, touch memory button, or Proximity card).

This required the following to be done:

- Go to the System Structure tab (or the Access tab, if a scenario will be associated to the events of the Access Zone entity):
- Select the system entity, to the events of which the scenario will be associated, in the tree of system entities, or in the tree of partitions and partition groups, or in the tree of maps
- Click the Edit button to start the editing mode
- Click the button  in the Inspector toolbox to toggle the Associating Management Scenarios to Entity Events.
- Choose a required event:



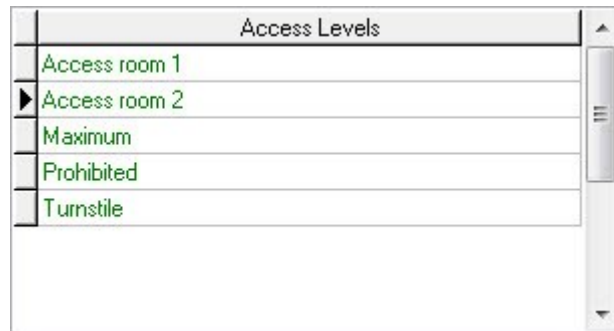
- Open the Select Scenario dialog box by clicking the  button:



This window displays the following information:

- The list of all access levels,
- The list of all employees,
- The list of all PIN codes, TouchMemory buttons, Proximity cards.  
*It is worth mentioning that TouchMemory buttons and Proximity are shown with the codes, but codes are not shown for PIN codes.*
- The elements of the above list where management scenarios are associated to.
- Set the association of scenarios to required elements in the Select Scenarios dialog box:
  - To associate scenario to a required element, please:

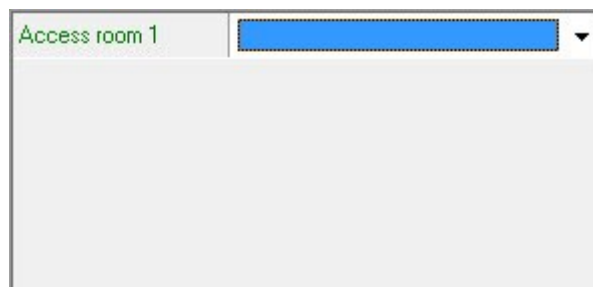
- ✓ Select an element from the list of access levels, employees, or credentials:



Then double click it to add the element on the right part of the box:



- ✓ Then select an element in the right part of the window



to select a required scenario from the dropdown list:



- ✓ The selected scenario will be displayed to the right of the element:



- ✓ If required, multiple elements can be added to associate scenarios to them:



Access room 1	Access opening
Access room 2	Access restoration

- If you need to delete the association of scenario to an certain element, please select the required element and choose an empty line on the top of the dropdown list:

Access room 1	Access opening
Access room 2	Access restoration
Turnstile	<div> <div></div> <div>Access opening</div> <div>Access restoration</div> </div>

The empty field will appeared on the right from the element:

Access room 1	Access opening
Access room 2	Access restoration
Access room 1	
Turnstile	Access restoration

This means that no scenarios are associated to this element. When this window (**SelectScenario**) is closed, this element will be deleted from the list of elements with associated scenarios.

- To quit the **SelectScenario** dialog box and save all changed, please click the **OK** button.
- The scenarios can be selected to other entity events as required.
- Click the **Save** button to accept changes.
- The Inspector of the entity will show three dots in the field of an event, meaning this event has a scenario associated:

Access Zone	
Passage	...
First passage	
Last exit	

#### 6.4.5 Renaming System Events

Events are generated for the most of system entities in the processing of system operations. The Scanning Core receives events devices or generates it itself based on events received from devices. In addition, Scanning Cores generates virtual events.

Entity events are described in the Chapter 6.2.12 Entity Events. Here, we only recall what system entities have events:

Entity	Events	
	Own	Virtual

Workstation	✓	✓
Video System	✓	✓
Camera	✓	✗
Device/Biometric Reader/Subscriber/Keybox	✓	✗
Reader	✓	✗
Loop/Subscriber Zone/Keybox Cylinder	✓	✗
Relay Output	✓	✗
Partition	✓	✓
Partition Group	✓	✗
Access Zone	✗	✓

*Attention! Virtual events are not displayed and recorded anywhere. Therefore they cannot be renamed.*

*If necessary, you can rename system events for individual entities of Intrusion, Fire, and Access Control systems*



This used for the following cases:

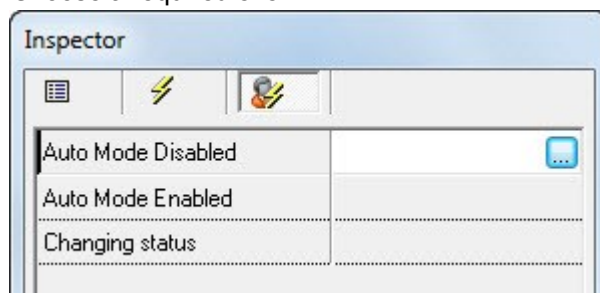
- To rename events of Potok-3N. For example, for loop events and supervised outputs that control electric valve.
- To rename events for loops such as Auxiliary Loop and ProgrammableAuxiliary Loop monitoring the states of devices.


Chapter 6.14.2 *Defining User Events* describes actions required for adding custom events to the systems. The chapter focuses on their actions for renaming entity events.

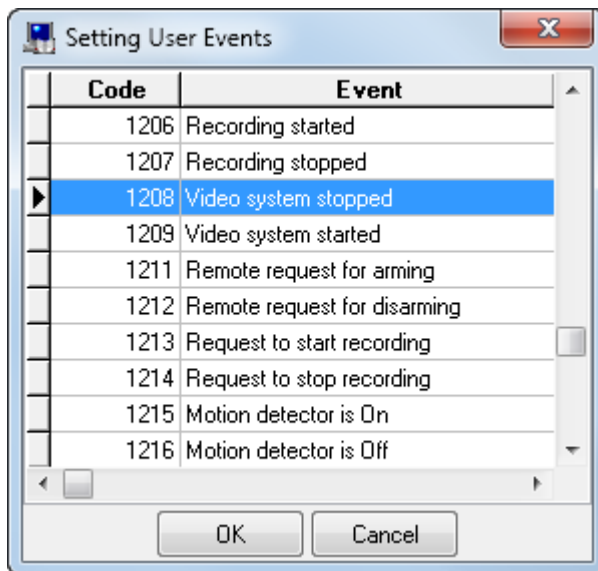
To rename an entity event, please do the following:

Go to the System Structure tab.

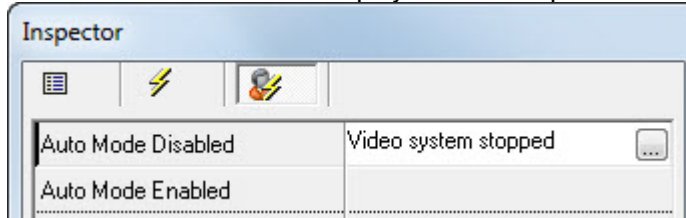
- Go to the System Structure tab.
- Select the system entity, to the events of which the scenario will be associated, in the tree of system entities, or in the tree of partitions and partition groups, or in the tree of maps
- Click the Edit button to start the editing mode
- Click the button   in the Inspector toolbox to toggle the Renaming Entity Events.
- Choose a required event:



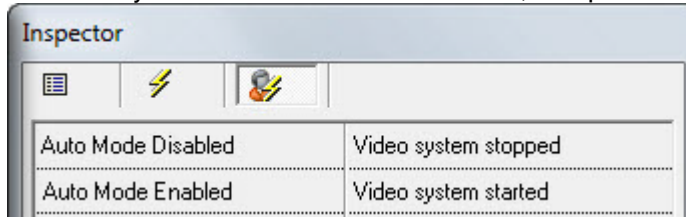
- Click the  button to open the Setting User-Define System Events and select required event in the appeared box, then click the OK button:



- The selected event will be displayed in the Inspector box:



- Other entity events can be renamed as well, if required:



- If it is required to delete any renamed events, select this event and press<Del> key.
- To accept all changes, click the **Save** button.

*Attention!When the database is exported to the S2000M Panel, only renamed events of loops and supervised outputs can be exported. The S2000M of version 2.05 and newer versions support exports of renamed events of devices and readers.*

#### 6.4.6 Configuring Display of Employee Photo in System Monitor

The System Monitor of the Orion Pro Suite supports the display of an employee photo when events initiated by this employee.

The list of events triggering the photo display is configured individually for each reader of the system.

To display employee photos as responses to the events of a reader of Access Control, Intrusion, and Fire Alarm Systems, one should define the events for the reader that will trigger the system to display the photos.

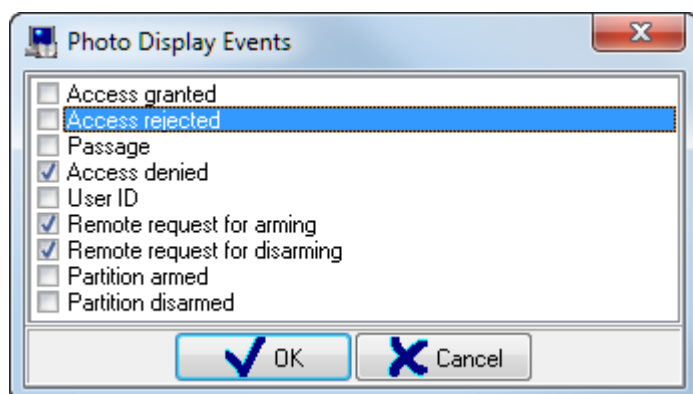
- Go to the System Structure tab.
- Choose a required reader in the tree of system entity, or in the tree of maps
- Click **Edit** the button to start editing
- Select the **Photo display events** property:



The Inspector window displays the following properties for a reader:



Device address	1
Number	1
User number	1
Name	Reader 1, Device 1
Description	
Element type	Reader
Type	Reader
All partitions	No
Photo display events	
ContactID Zone	0
Cameras	

- Click the  button to open the **Photo Display Events** dialog box, select the events that will trigger displaying photos of employees in the System Monitor, and then press the OK button.



The Photo Display Events dialog box contains the following list of events with checkboxes:

- ☐ Access granted
- ☐ Access rejected
- ☐ Passage
- ☒ Access denied
- ☐ User ID
- ☒ Remote request for arming
- ☒ Remote request for disarming
- ☐ Partition armed
- ☐ Partition disarmed

Buttons:  OK  Cancel

- To accept all changes, please click the **Save** button.

It should be noted, that display of employees photos has to be set in properties at each workstation with a System Monitor selected to run.

*The relevant information is provided in Chapter 6.2.2 the Workstation Entity.*

It also should be noted the list of readers initiating photo-triggering events must be specified in each System Monitor.

*The relevant information can be found in Chapter 8 System Monitor.*

#### 6.4.7 Associating Cameras to Device Zones

In the Database Administrator, cameras can be associated to any loop, relay output, reader or access point, so that they start recording automatically as a response to alarm event at a specified entity.

This is achieved by defining the list of cameras for a loop (relay output, reader or access point) that would start recording if that loop (relay output, reader or access point) goes into alarm ( External alarm recording must enabled for such cameras).

Also, only these cameras would be displayed in the **Video Archive** window if **Show video** menu command is selected for a loop, relay output, reader, or access point in the **Alarms** tab of the System Monitor module.

Workstation	Num...	Time	Event	Description	Partition	Zone	Action 1	Time 1	Operate
SECURITYHEAD	97	3/16/2015 6:44:12 PM	Device disconnected	Signal-20 ser. 02 (41)	-	2/0/41	-	-	-
SECURITYHEAD	98	3/16/2015 6:44:14 PM	Device disconnected	Signal-20 ser. 02 (41)	-	2/0/41	-	-	-
SECURITYHEAD	99	3/16/2015 6:44:15 PM	Device disconnected	S2000-BI/BKI (46)	-	2/0/41	-	-	-
SECURITYHEAD	100	3/16/2015 6:44:16 PM	Device disconnected	S2000-4 (46)	-	2/0/41	-	-	-
SECURITYHEAD	101	3/16/2015 6:44:17 PM	Device disconnected	S2000-2 (45)	-	2/0/41	-	-	-


Record of Response Team Dispatch  
Record of Police Call  
Show Video  
Move to Handled Alarms  
Move All to Handled Alarms

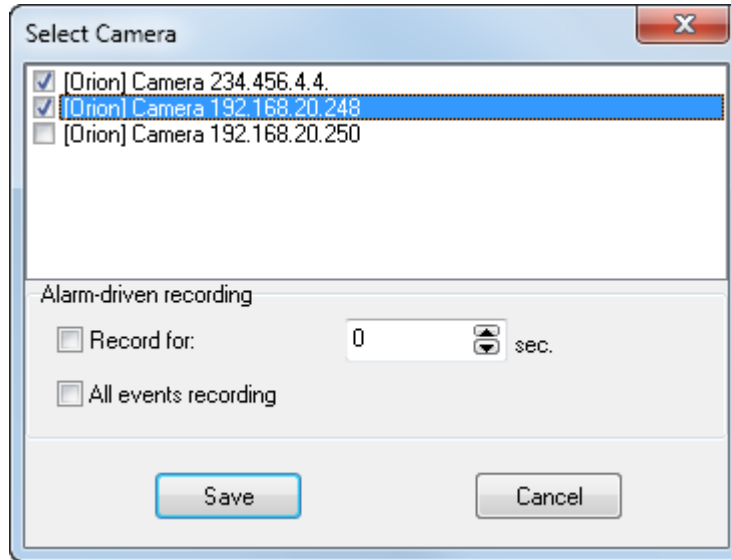
To define the list of cameras, the following should be done:

- Go the System Structure tab or to the Access tab
- Select a required entity (loop, relay output, reader or access point) in the tree of system entities (for loop, relay output, or reader), or in the tree of access control entities (for access point) or the tree of maps (for all entities)
- Click the **Edit** button to start editing of entity properties
- Select the **Camera** property:

**Inspector**

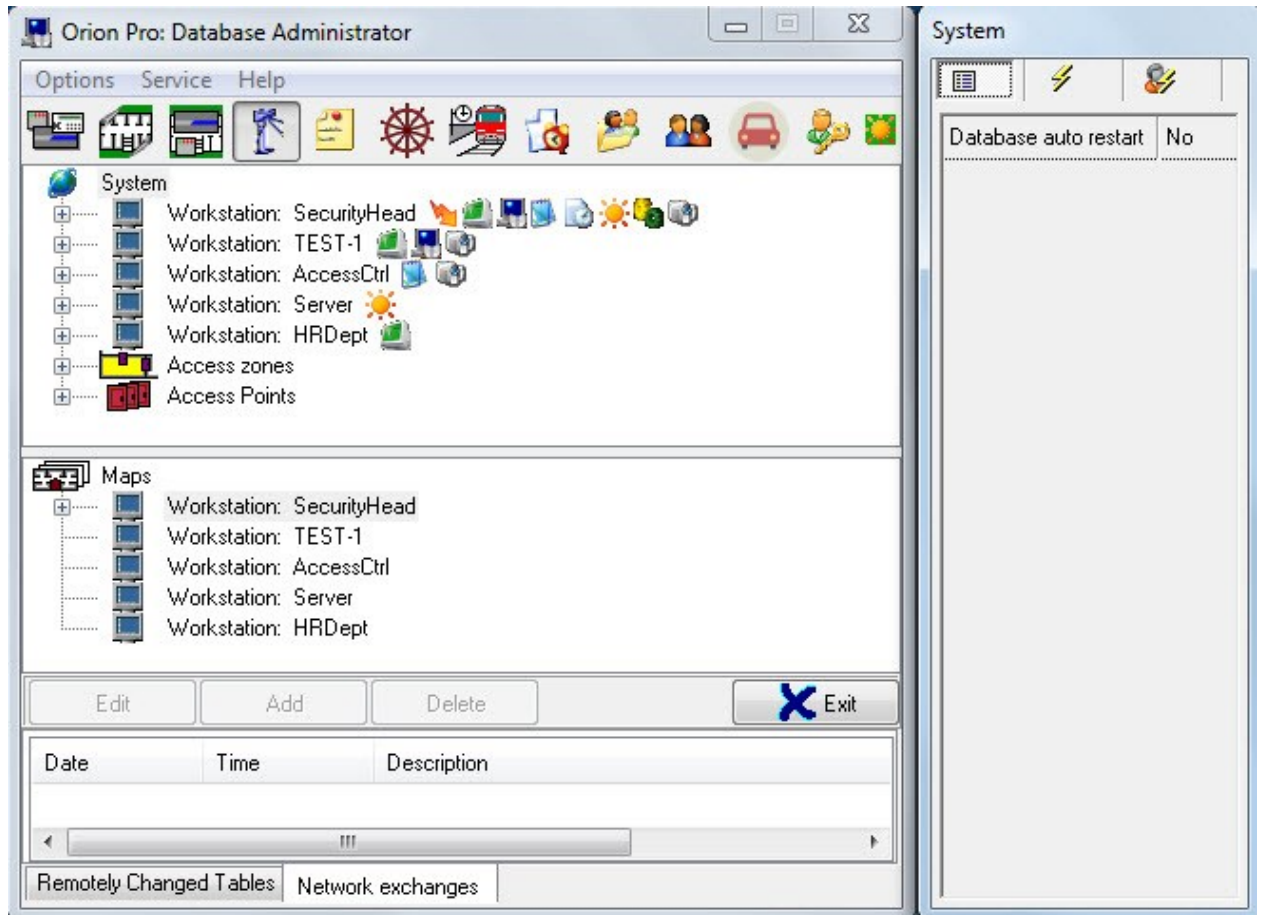
Device address	2
Number	1
User number	13
Name	Loop 1, Device 13
Description	
Element type	Zone/Loop
Type	Entrance
24-hour zone	No
Accumulate statistics	No
Entrance zone timeout	1
ContactID Zone	0
Cameras	

- Click the  button to open the **Select Camera** dialog box, than select cameras for the recording and specify the time the recoding will continue (**Record for**), then click the **Ok** button



- Click **Save** to accept the changes.

## 6.5 The Access Tab. Creating Logical Events and Structure of Access Control System



The Access tab shows the following:

1. The tree of access control entities.
2. The tree of maps.

The Access tab is used to define the structure of an access control system, specifically:

- To create logical entities of an access control system: access zones and access points.

The system offers various access control approaches:

- *Local Access (Control):* When all credentials (tokens' pass codes) are stored in a controller responsible for an access point and that controller grants or bans an access.
- *Centralized Access (Control):* When all credentials (tokens' pass codes) are stored in Orion Pro' Database Administrator module, and it is the Scanning Core is responsible for granting or banning an access

Access Points can be as follows:

- Two-way access points ( One door for entry and exit, Turnstiles, Vehicle Barriers, Mantraps)
- One-way access points (One-way door, i.e one door for exit or entry only)

*Each **two-way** access point is recommended to be based on one S2000-2 controller.*

Different access modes can be set for access points (individually for each direction (entry or exit) for two-way access points such as Turnstiles, Barriers, and Mantraps):

- **Normal:** An access is granted when a credential(s) is presented;
- **Access Locked (Lockdown):** No access of any type is allowed ;

- **Open Access (Free):** An access is allowed with no credentials being required.

System-controlled Access Points can function in two main modes:

- When an access direction is monitored (route tracing), that is when access zones are used
- When an access direction is not monitored, that is when the concept of access zones is not used.

The entire system-controlled area can be subdivided into access zones. Maximum access zones in the system are 65,535 (0 to 65534).

The area that is not under control of the system (beyond your facility or building) is regarded as **Outside World** and has index (ID) '0'. This zone is added in the system by default when the database is created, and it cannot be deleted.

An access point with a controlled direction is always located between of access zones. If an access point is located inside an access zone, it must work with no direction control.

*A one-way access point with an exit button cannot be used in a mode where a passage (access) direction is controlled.*

The tasks implemented on the level of access zones are as follows:

- Tracking the location of employees
- Antipassback
- Time and Attendance.

Let's consider the anti-passback rule.

If local access control is used, antipassback applies to access points controlled by a S2000-2 controller. With centralized access control, *anti-passback* is implemented for access points controlled by S2000-2 and S2000-4 controllers.

An anti-passback rule is regarded violated if no entry to any other access zone is registered after zone X is accessed, but an attempt is made to re-enter the same access zone X again.

*Anti-passback* can be as follows:

- None (*anti-passback* rule is ignored)
- *Hard Anti-Passback*
- *Soft Anti-Passback*
- *Timed Anti-Passback*.

**Hard anti-passback** prevents a re-entry to the same access zone until an exit from this zone is recorded. When an antipassback rule is breached, no access is granted, and the **Access Denied** message is generated

**Soft anti-passback** allows re-entry but generates the **Access Granted** and **Passage** messages accompanied by the **anti-passback breach** tag.

**Timed anti-passback** uses an additional parameter - **Anti-Passback Lockout Period**. During this period after an entry to an access zone, a timed anti-passback rule applies in the same manner as the hard anti-passback does (if a re-entry is attempted, a controller denies access and generates the **Access Denied** message accompanied by the **Anti-passback Breach** tag). When this period expires, timed anti-passback is identical to soft antipassback (a re-entry is allowed but the **Access Granted** and **Passage** messages are generated with the **anti-passback breach** tag).

If anti-passback applies to a locally-controlled device, the anti-passback is *called local anti-passback*.

In the system, network anti-passback is implemented. If controlling unit is available (S2000/S2000M or Scanning Core) access messages will be re-transmitted to all access controllers in the system. Thus, the anti-passback rule is verified taking into account entries to the access zone, as registered by all controllers of the system (within one workstation).

Therefore, if an access zones has several access points (for example, several checkpoints, or several parallel turnstiles), after the entry to this access zone via one access point, the re-entry to this zone will be banned (locked) at this access point and all other access points as well, but the exit will be allowed; and wise versa, if a person exits from this area via one access point, the attempts to exit from this area will be



banned (locked) at all other access points as well, but the entry will be allowed (if an anti-passback rule applies to the access credentials).

The use of anti-passback between two access zones will be correct, if the following requirements are observed:

- ✓ The normal access between zones is provided via access points only.
- ✓ The access points on the boundary between these zones must have entry and exit readers (identification on the entry and on exit) and entry/exit detector or the like (a one-way access point with an exit button cannot be used on the boundary between two access zones).

The number (ID) of an access zone must be set the same for all readers of access points controlling access to the same zone in order to ensure the proper functioning of network anti-passback mode.

The anti-passback rule will be tighter, if the **zonal anti-passback** parameter is applied (Route Tracking). In this case, the system considers entries to any access zone, and if access is attempted via one of the readers of an access point, anti-passback requires that the last registered access will be to the access zone where the reader is located, that is to the zone controlled by a second reader of this access point.

For example, we have a two-reader access point located on boundary between Access Zone 1 and Access Zone 2, first, the access to Zone 2 is registered, and then access to Access Zone 3 (controlled by a different access point) is recorded, the further attempt to go through the access point between Access Zone 1 and Access Zone 2 will result in the following:

- If zonal anti-passback mode is in place, the anti-passback rule would be breached regardless of an access (passage) direction, as the last-recorded access (passage) was made to a different zone from Access Zone 1 and Access Zone 2, and the person's actual location in one of these zones is regarded as inappropriate;
- If no zonal anti-passback is used, the anti-passback rule would not be breached if an access is attempted to Access Zone 1, but it would be breached if an access is attempted to Access Zone 2, since, with respect to this access point, the user is still in Access Zone 2 (the user's entry to Access Zone 3 is ignored by the access point).

The Zonal anti-passback parameter is effective, only if any one of the Hard, Soft, or Timed anti-passback modes is enabled. If the anti-passback is disabled, the Zonal anti-passback parameter is not applicable. Zonal anti-passback applies to two-way access points only.

With local access control, to support zonal anti-passback, each two-way access point must be controlled by one S2000-2 (version 1.05 or later)

With centralized access control, the zonal anti-passback parameter always applies to two-way access points if anti-passback is used.

To prevent sequential entries of several persons presenting the same credential (e.g. a card) to several closely located readers (e.g. at several turnstiles), from the moment of granting an access (a card read by one reader) till the moment of entry (passage) registration, this credential (e.g. a card) will be banned for a read in other readers of the system for a short time as per anti-passback. Specifically, when a gained access via one reader is not followed by entering the zone but the same credential is further presented to another reader (of another controller), it will be considered as the anti-passback breach at this reader. If hard or timed anti-passback applies for that credential at that reader the access for this credential will be banned. The ban is lifted only after an entry (**Passage**) is registered for this credential. If no entry (passage) occurs (a granted access has been not completed, or an entry (Passage) detection capability is not used), ban will be lifted in a minute. While the ban is in effect, the access by this credential is possible only via the reader that was the last one to grant the access to this credential; or via any other reader where no anti-passback rule applies to this credential (a person can re-access with this credential only via the reader that was the last one to grant this access).

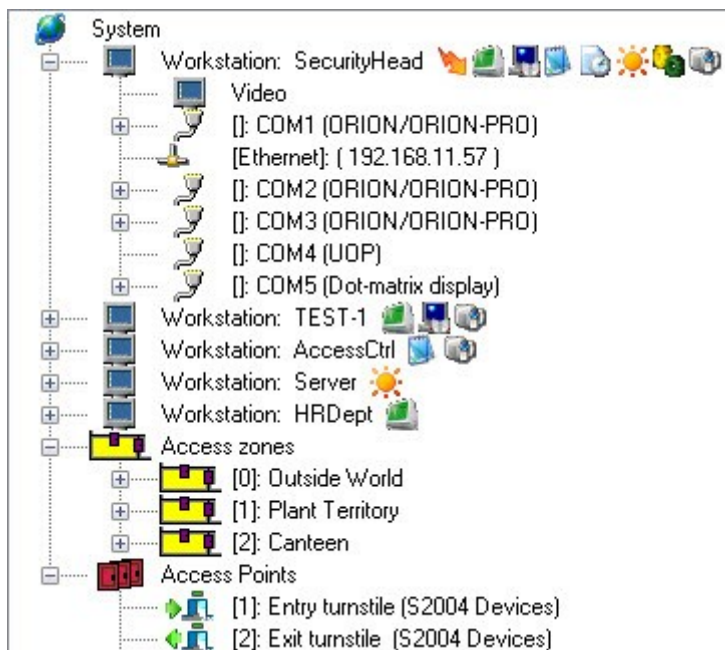
Anti-passback as a response to the **Access Granted** event can be implemented only in the local access control mode based on S2000-2 (1.05 or later versions).

The Orion Pro System also offers the following:

- Setting various access control approaches for access points:
  - ✓ Simple Access: When only one credential item is presented

- ✓ With supplementary code (Multiple-factor authentication): Access requires supplementary code to main credential.
- ✓ Two- or three-man rule: Access requires two (three) different credentials with coordinated access levels.
- Using the readers of the system for remote arming and disarming
- Providing each user with the access level-based rights for individual access points or access zones, as well as partitions or partition groups for remote arming and disarming. At this level, a user account is set whether to be a subject to the anti-passback rules.
- Assigning time-correlated access rights (time zones) to a user for each access point/zone, as well partitions and partition groups. With this respect, the system supports the following capabilities:
  - Defines holidays (days when time intervals are enabled as different from those applicable to the week days)
  - Transfers working days
  - Create complicated floating work schedules
  - Create complicated work schedules with irregularly recurring periods.
- Create a central security control station. An operator of System Monitor can grant an access at access points (within his access level authorities) on behalf of his name, or using the Forced access command. The Forced access command can be used only if an employee has left his/her credential at home, and the employee has to be granted an access as if on one's own account (important for Time and Attendance). Furthermore, an Operator can lock/unlock system readers.

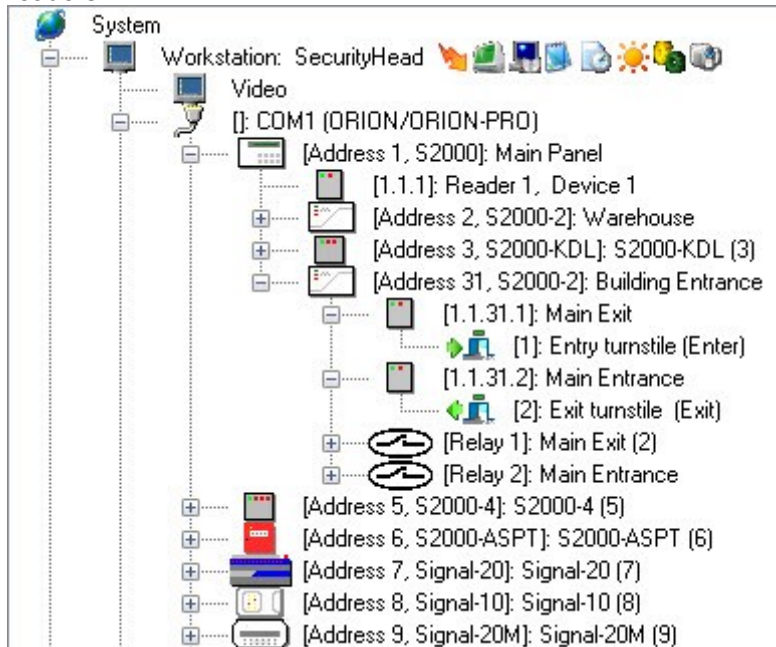
Let's consider the structure of the tree of access control system:



**System** is the main tree node. This node automatically accommodates all system workstations, as well as two virtual nodes: **Access Zones** and **Access Points**:



The **Workstation** is a node, to which **COM ports** are added, which in turn, becomes nodes for **Devices**. **Readers** and **Relay Outputs** are added to the **Devices** nodes. Access points are associated to relays and readers:



The Workstation entity cannot be deleted from the tree of the access control system. Workstation-connected entities cannot be added, deleted, or edited. Only associations of access points to devices can be modified.

The tree of access control system shows the following information for the Workstation entity:

- Name
- The list of Orion Pro's modules authorized to run on this workstation.



The tree of access control system shows the following information for the COM Port entity:

- Number (ID)




The tree of the access control system shows the following information for the Device entity:

- Address
- Type
- Name




The tree of the access control system shows the following information for the Reader entity:

- Number
- Name

 [1.1.31.1]: Main Exit


The tree of the access control system shows the following information for the Relay Output entity:



- Number
- Name
- Partition ID ( if relay output is added to a partition)

 [Relay 1]: Main Exit (2)

Two virtual nodes (Access Zones and Access Points) are displayed underneath all workstations in the tree of the access control system. These nodes are always available in the system, and they cannot be deleted.


The **Access Zones** node includes all access zones defined in the system:



 Access Zones

-  [0]: Outside World
-  [1]: Plant Territory


*It should be noted again, that the Outside World node is automatically added to the system when a database is created. This node cannot be deleted.*


Access Points are associated to their controlled Access Zones:

 Access Zones

-  [0]: Outside World
-  [2]: Exit turnstile (exit)

Access points (doors, turnstiles and the like) are associated to the Access Points node:


 Access Points

-  [1]: Entry turnstile (S2004 Devices)


### 6.5.1 The Access Zone Entity



In the Orion Pro Suite, access zones belongs to no workstation.

Let's consider the Access Zone entity.


 [0]: Outside World



The Access Zone entities are associated to the Access Zones node in the tree of access control system.

 Access Zones

-  [0]: Outside World
-  [1]: Plant Territory

The tree of an access control system associates Access Zone entity with the access point leading to the relevant access area, the access direction being defined.

 [1]: Plant Territory

-  [1]: Entry turnstile(entry)
-  [4]: Canteen/Smoking Room Door(exit)

The tree of access control system displays the following information for the Access Zone entity:

- Number
- Name.

 [1]: Plant Territory

To add a new Access Zone entity, please select the Access Zones node in the tree of the access control system and click the **Add** button. Then enter required values for all properties of the new Access Zone entity and click the **Save** button.

To edit the properties of the Access Zone entity, please select a required entity in the tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete the Access Zone entity, please select a required access zone in the tree of the access control system and click the **Delete** button. Then, confirm the delete action by clicking the **Yes** button in the appeared System Request dialog box

To delete all the Access Zone entities but for the **Outside World** access zone, please select the **Access Zones** node in the tree and click the **Delete** button. Then, confirm the delete action by clicking the **Yes** button in the appeared System Request dialog box:

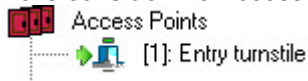
The properties of the Access Zone entity:

Access Zone	
Number	0
Name	Outside World
Description	

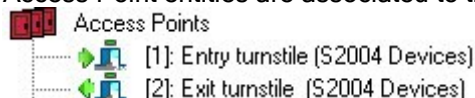
Property	Possible Values	Description
<b>Number (ID)</b>	1..65534	The unique number of an access zone. Defaults value: minimum number from an available range (1..65534) not used in the system
<b>Name</b>	A length of 1 to 25 characters	The name of an access zone. Default value: “ <b>Access Zone</b> ” and number of access zone Example: Access Zone 7
<b>Description</b>	A length of 10 to 200 characters	Comments: <i>Optional field</i> Default value: empty field

## 6.5.2 The Access Point Entity

Let's consider the Access Point entity.






Access Point entities are associated to the **Access Points** node:



The tree of the access control system shows the following information for the Access Point entity:





- Operating mode:
  - Passage – no icon
  - Entry –

- Exit - ,
  - Entry /Exit - ,
  - Number
  - Name
-  [5]: Turnstile

To add a new Access Point entity, please select the **Access Points** node in the tree of the access control system and click the **Add** button. Then enter required values for all properties of the new Access Zone entity and click the **Save** button.

Notethat when a new door is added to the system, this door is automatically associated to relay outputs (as specified in door properties) and relevant readers of a device (or devices) with required access direction defined.

*The access control tree shows the following information for an access point associated to a relay output or readers :*

- Direction (by arrows ) :
    - Passage (with no direction specified no specified direction) – no icons
    - Entry → 
    - Exit ← 
    - Entry/Exit -  \* (only access point associated to a relay output )
  - Number
  - Name
  - Direction (textually).
-  [6]: Door6

To edit the properties of the Access Point entity, please select a required entity in the tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete the Access Point entity, please select a required access point in the access control tree and click the **Delete** button. Then, confirm the delete action by clicking the **Yes** button in the appeared System Request dialog box

Properties of the Access Point entity:

Access Point	
Number	6
Name	Canteen Door
Description	
Type	Two-way access door
Operating mode	Entry/Exit
Access zone to enter	[2]: Canteen
Entry relay	[SUPPORT-11-57.1.14.1]: Relay 1,
Entry relay action	ON
Entry relay action time	5
Accessed zone to exit	[1]: Plant Territory
Exit relay	[SUPPORT-11-57.1.14.2]: Relay 2,
Exit relay action	ON
Exit relay action time	5

Property	Possible Values	Description
Number (ID)	1..2147483647	The unique number of an access zone.  Defaults value: minimum number from an available range (1.. 2147483647)not used in the system
Name	A length of 1 to 25 characters	The name of an access point.  Default value: “Access Point” and number of access point Example: Access Point 12
Description	A length of 10 to 250 characters	Comments:  <i>Optional field</i>  Default value: empty field
Type	One-way access door Two-way access door (One door for Entry/Exit) Turnstile Vehicle Barrier Mantrap	Type of access point  <i>(See Appendix 1 to this table).</i>  Default value: One-way access door
Operating mode	Passage Entry Exit Entry/Exit	Access point operating mode  <i>(See Appendix 2 to this table).</i> Default value: Entry
Access zone to enter	«[NO] or one of the access zones	Access area where an employee will find oneself entering through this access point.  <i>(See Appendix 3 to the table).</i>  <i>This property is accessible if the Operating mode property is defined as Entry or Entry/Exit.</i>  Default value: NO
Entry relay	<i>Relay output of S2000-2 or S2000-4 device</i>	Relay output actuating mechanism to provide entry.  <i>(See appendix 1 to this table).</i>  <i>This property is accessible the Operating mode property is defined as Passage, Entry or Entry/Exit.</i>  Default value: No relay output is selected
Entry relay action	(Switch)ON, (Switch) OFF	A relay action (program) of a device controlling this access point.  <i>This property is accessible the Operating mode property is defined as Passage, Entry or Entry/Exit.</i>  <i>No this parameter is not used in the Orion Pro Suite.</i>  Default value: ON
Entry relay action time	1..8191	Period (in seconds) of relay action to provide entry.  <i>This property is accessible, if the Operating mode property is defined as Passage, Entry or Entry/Exit.</i>  <i>Now, this parameter in not used in the Orion Pro Suite.</i>  Default value: 5 (sec)
Accessed zone to exit	«[NO]», one of the access zones of the	An access zone where an person will find oneself exiting through this access point.

	system	<p>(See Appendix 3 to this table).</p> <p>This property is accessible the Operating mode property is defined as Entry or Entry/Exit.</p> <p>Default output: NO</p>
Exit relay	Relay output of S2000-2 or S2000-4 device	<p>Relay output controlling actuating mechanism to provide exit.</p> <p>(See appendix 1 to this table).</p> <p>This property is accessible the Operating mode property is defined as Passage, Entry or Entry/Exit.</p> <p>Default value: No relay output is selected</p>
Exit relay action	(Switch)ON, (Switch) OFF	<p>A relay action (program) of a device controlling this access point to provide exit.</p> <p>This property is accessible the Operating mode property is defined as Passage, Entry or Entry/Exit.</p> <p>No this parameter is not used in the Orion Pro Suite.</p> <p>Default value: OFF</p>
Exit relay action time	1..8191	<p>Period (in seconds) of relay action to provide exit.</p> <p>This property is accessible the Operating mode property is defined as Passage, Entry or Entry/Exit.</p> <p>Now, this parameter is not used in the Orion Pro Suite.</p> <p>Default value: 5 (sec)</p>
Cameras	(See Chapter 6.4.7 Associating Cameras to Devices)	<p>The list of cameras that start recording if an alarm occur at an access point (external alarm recording must be enable for a camera to this effect)</p> <p>These cameras are displayed if <b>Show video</b> menu command is selected for an access point in the <b>Alarms</b> tab of the System Monitor module.</p> <p>Default video: Empty list</p>

#### Appendix1

Let us consider what devices can be used to provide access points of various types:

Access Point Type	Relay Outputs
One-way access door	Relay output 1 of one S2000-4 device
	Relay output 1 of S2000-2 device
	Relay output 2 of S2000-2 device
Two-way access door (One door for Entry and Exit)	Relay output 1 of one S2000-2 device
	Relay output 1 of one S2000-4 device and Relay output 1 of another S2000-4 device (not recommended)
Turnstile	Relay output 1 and relay output 2 of one S2000-2 device
	Relay output 1 of one S2000-4 device and Relay output 1 of another S2000-4 device (not recommended))
Vehicle Barrier	Relay outputs 1 and 2 of one S2000-2 device
Mantrap	Relay outputs 1 and 2 of one S2000-2 device



*P.S. When a two-way access point (Turnstile, Barrier, and Mantrap) is based on a S2000-2 device, relay output 1 must be used for Entry Access and relay output 2 must be used for Exit access.*

*P.S. When a two-way access door (One door for Entry/Exit) is based on a S2000-2 device, only relay output 1 must be used to control Entry and Exit transactions.*









## Appendix 2

Let's consider the operating modes of access point types:

Access Point Type	Operating Mode
One-way access door	Passage
	Entry
	Exit
Two-way access point (One door for Entry/Exit)	Entry/Exit
Turnstile	Entry/Exit
Vehicle Barrier	Entry/Exit
Mantrap	Entry/Exit

## Appendix 3

Let's consider the use of access zones in respect to the access point operating modes:

Access Point Operating Mode	Access Zones	
	Accessed Zone to Enter	Accessed Zone to Exit
Passage		
Entry		
Exit		
Entry/Exit		

Attention! If a two-way access point is to be used with undefined direction (without an access zone concept), the Entry/Exit mode must be set for this point, and no access zone must be specified ( [No] must be set for **Access to Enter** and **Accessed Zone to Exit**):

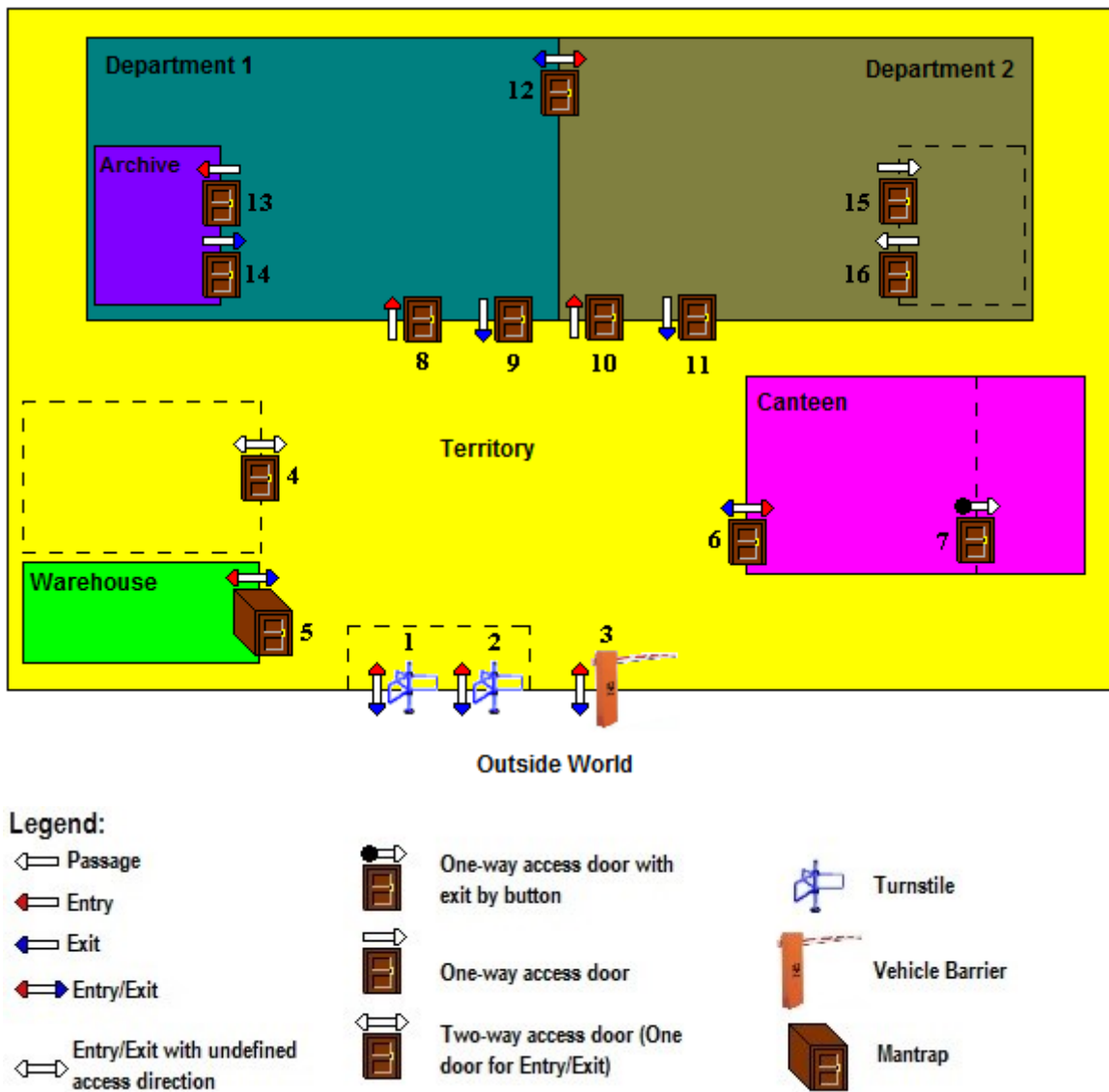
Entry/Exit	[NO]	[NO]
------------	------	------

**Note** that the access zones specified in the properties of access points in the database must match the access zones as specified in the settings of devices controlling these access points.

If access zones are not used for some access points, value 65535 must be set in the settings of devices (controllers) controlling these access points.

If necessary, the Uprog utility can be used to reconfigure required devices

Let's consider the example of access control system:



The figure shows the system uses the following access zones;

0. Outside World : an area beyond the controlled site
1. Territory: All areas but for the departments, canteen, and warehouse
2. Warehouse :High security area
3. Canteen
4. Department 1
5. Department 2
6. Archive – premises inside Department 1

The figure also shows that:

- The **Territory** includes a building (dashed line) which is not defined as an individual access zone but the access to this zone is controlled with two-way access door (4) using credentials (for entering and exiting);

- **Department 2** also includes premises (dashed line) which is not defined as an individual access zone with but it is controlled by two one-way access doors (one for entering and one for exiting) using credentials
- The **Canteen** includes a separate facility (dashed line), which is not defined as individual access zone but its access is controlled by one-way access door: entry by credential, exit by button;

The logic of the access points is as follows:

- Turnstile (1), Turnstile (2) and Barrier (3) two-way access points allow entering the site area ([1] Territory access zone) and exiting the site area ([0] Outside World)

Operating mode: Entry/Exit

- Door (4) two-way access door allows in and out of the building. Since the access point is inside the building it operates without control of access direction, i.e. the access zone approach is not used

- Mantrap (5) two-way access point allows in the warehouse area ([2] Warehouse access zone) and out of the warehouse to enter the site area ([1] Territory access zone)

Operating mode: Entry/Exit

- Door (6) two-way access door allows in the canteen ([3] Canteen access zone) and out of the canteen area to the site area ([1] Territory)

Operating mode: Entry/Exit

- Door (7) one-way access door allows in to the canteen, but with exit by button only. Since the access point is inside the access area and uses an exit button, it does not control a passerby access direction (In and Out).

Operating mode: Passage

- Door (8) and Door (10) one-way access doors allow in to Department 1 ([4] Department 1) and Department ([5] Department 2), respectively.

Operating mode: Entry

- Door (9) and Door (11) one-way access doors allow out of Department 1 and Department 2, respectively to get in the site area ([1] Territory).

Operating mode: Exit

Door (12) two-way access door allows in Department 2 ([5] Department 2), and out of it to get in Department 1 ([4] Department 1)

- Door (13) one-way access door allows in the Archive access zone [6]

Operating mode: Entry









- Door (14) one-way access door allows out of Archive to get in Department 1 ([4] Department 1 access zone)

Operating mode: Exit

- Door (15) and Door (16) allow in to the interior room and out of it to get in Department 2. Since the doors are inside of the access zones they do not control access direction (Entry or Exit)

Operating mode: Passage.

Example of the settings for the above access points

Access Point Setting	As displayed in the access control tree																
<div> Access Points</div> <div> [7]: Door 7</div> <div>One way access door/ Passage</div> <div>Controlled by an S2000-4 panel with address 4 (COM Port 5, panel address is 2).</div> <table><tr><td>Number</td><td>7</td></tr><tr><td>Name</td><td>Door 7</td></tr><tr><td>Description</td><td></td></tr><tr><td>Type</td><td>One-way access door</td></tr><tr><td>Operating mode</td><td>Passage</td></tr><tr><td>Relay</td><td>[SecurityHead.1.6.1]: Relay 1, Device 6</td></tr><tr><td>Relay action</td><td>ON</td></tr><tr><td>Relay activation time</td><td>5</td></tr></table>	Number	7	Name	Door 7	Description		Type	One-way access door	Operating mode	Passage	Relay	[SecurityHead.1.6.1]: Relay 1, Device 6	Relay action	ON	Relay activation time	5	<div> [Address 6, S2000-4]: S2000-4 (6)</div> <div> [1.6.1]: Reader 1, Device 6</div> <div> [7]: Door 7 (Pass)</div> <div> [Relay 1]: Relay 1, Device 6</div> <div> [7]: Door 7 (Pass)</div> <div> [Relay 2]: Relay 2, Device 6</div>
Number	7																
Name	Door 7																
Description																	
Type	One-way access door																
Operating mode	Passage																
Relay	[SecurityHead.1.6.1]: Relay 1, Device 6																
Relay action	ON																
Relay activation time	5																



#### Access Points

- [8]: Door 8
- [9]: Door 9

[8] One way-access door / Entry

[9] One way-access door / Exit

Controlled by an S2000-2 device with address 2 (COM Port 5, panel address 2)

Number	8
Name	Door 8
Description	
Type	One-way access door
Operating mode	Entry
Access zone to enter	[1]: Hall
Entry relay	[SecurityHead.1.1.4.1]: Relay 1, Device
Entry relay action	ON
Entry relay action time	5
Number	9
Name	Door 9
Description	
Type	One-way access door
Operating mode	Exit
Accessed zone to exit	[0]: Outside World
Exit relay	[SecurityHead.1.1.4.2]: Relay 2, Device
Exit relay action	ON
Exit relay action time	5



#### Access Zones

- [0]: Outside World
- [9]: Door 9 (exit)
- [1]: Hall
- [8]: Door 8 (Entry)



#### [Address 4, S2000-2]: S2000-2 (4)

- [1.1.4.1]: Reader 1, Device 4
- [8]: Door 8 (Entry)
- [1.1.4.2]: Reader 2, Device 4
- [9]: Door 9 (Exit)
- [Relay 1]: Relay 1, Device 4
- [8]: Door 8 (Entry)
- [Relay 2]: Relay 2, Device 4
- [9]: Door 9 (exit)



#### Access Points

- [2]: Turnstile 2

Turnstile, Entry/Exit

Controlled by SC2000-2, address: 1 (COM Port 5, panel address 2)

Number	2
Name	Turnstile 2
Description	
Type	Turnstile
Operating mode	Entry/Exit
Access zone to enter	[0]: Outside World
Entry relay	[SecurityHead.1.1.3.1]: Relay 1, Device
Entry relay action	ON
Entry relay action time	5
Accessed zone to exit	[1]: Hall
Exit relay	[SecurityHead.1.1.3.2]: Relay 2, Device
Exit relay action	ON
Exit relay action time	5



#### Access Zones

- [0]: Outside World
- [2]: Turnstile 2 (Entry)
- [1]: Hall
- [2]: Turnstile 2 (exit)



#### [Address 3, S2000-2]: S2000-2 (3)

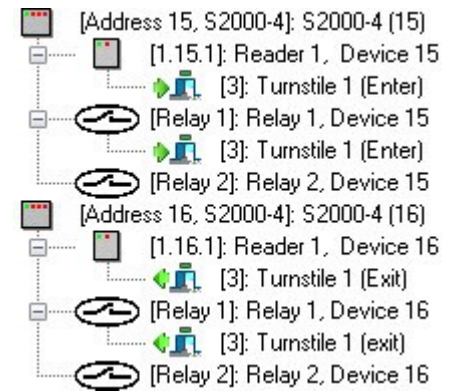
- [1.1.3.1]: Reader 1, Device 3
- [2]: Turnstile 2 (Enter)
- [1.1.3.2]: Reader 2, Device 3
- [2]: Turnstile 2 (Exit)
- [Relay 1]: Relay 1, Device 3
- [2]: Turnstile 2 (Enter)
- [Relay 2]: Relay 2, Device 3
- [2]: Turnstile 2 (exit)



### Turnstile, Entry/Exit

Control by S2000-4 devices with address 5 and 6 (COM Port 5, panel address 2).

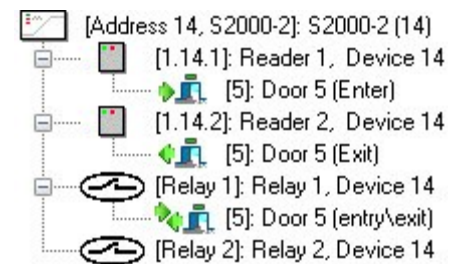
Number	3
Name	Turnstile 1
Description	
Type	Turnstile
Operating mode	Entry/Exit
Access zone to enter	[0]: Outside World
Entry relay	[SecurityHead.1.15.1]: Relay 1, Device 15
Entry relay action	ON
Entry relay action time	5
Accessed zone to exit	[1]: Hall
Exit relay	[SecurityHead.1.16.1]: Relay 1, Device 16
Exit relay action	ON
Exit relay action time	5



### Two-way access door, Entry/Exit (Entrance Area)

Controlled by an S2000-2 device (address: 10) (COM Port - 5, panel address: 2).

Number	5
Name	Door 5
Description	
Type	Two-way access door
Operating mode	Entry/Exit
Access zone to enter	[No]
Entry relay	[SecurityHead.1.14.1]: Relay 1, Device 14
Entry relay action	ON
Entry relay action time	5
Accessed zone to exit	[No]
Exit relay	[SecurityHead.1.14.1]: Relay 1, Device 14
Exit relay action	ON
Exit relay action time	5

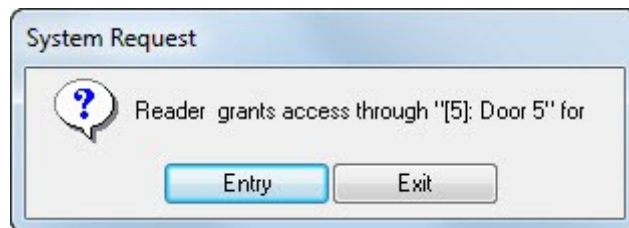


### 6.5.2.1 Associating Access Point to Readers and Relay Outputs

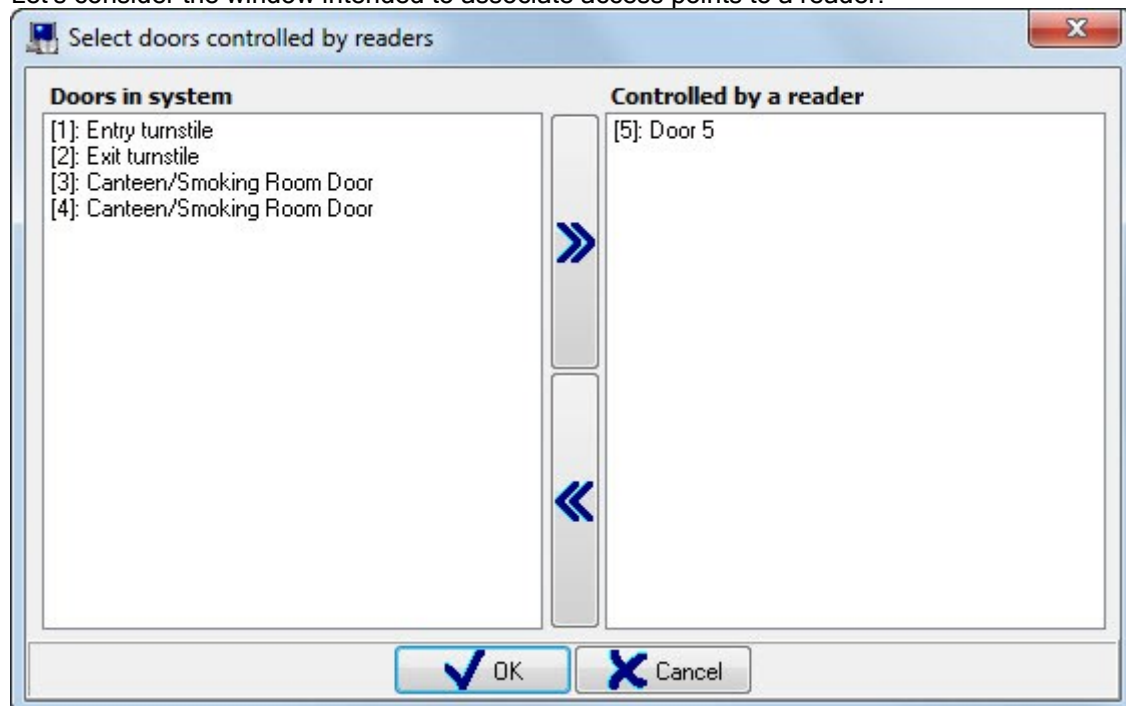
Sometimes, you may have to re-associate access points to readers.

To delete an association between an access point and a reader, please select a required access point in the access control tree and click the **Delete** button. Further, confirm the delete action in the **System Request** dialog box by clicking the **Yes** button.


To associate an access point to a reader, please select a required reader in the access control system tree, and then click the **Add** button. Then, select an access point in the appeared dialog box and click **OK**. If a two-way access door is the subject of association, the System Request dialog will appear where should define and an access direction by clicking **Entry** or **Exit**:



Let's consider the window intended to associate access points to a reader:

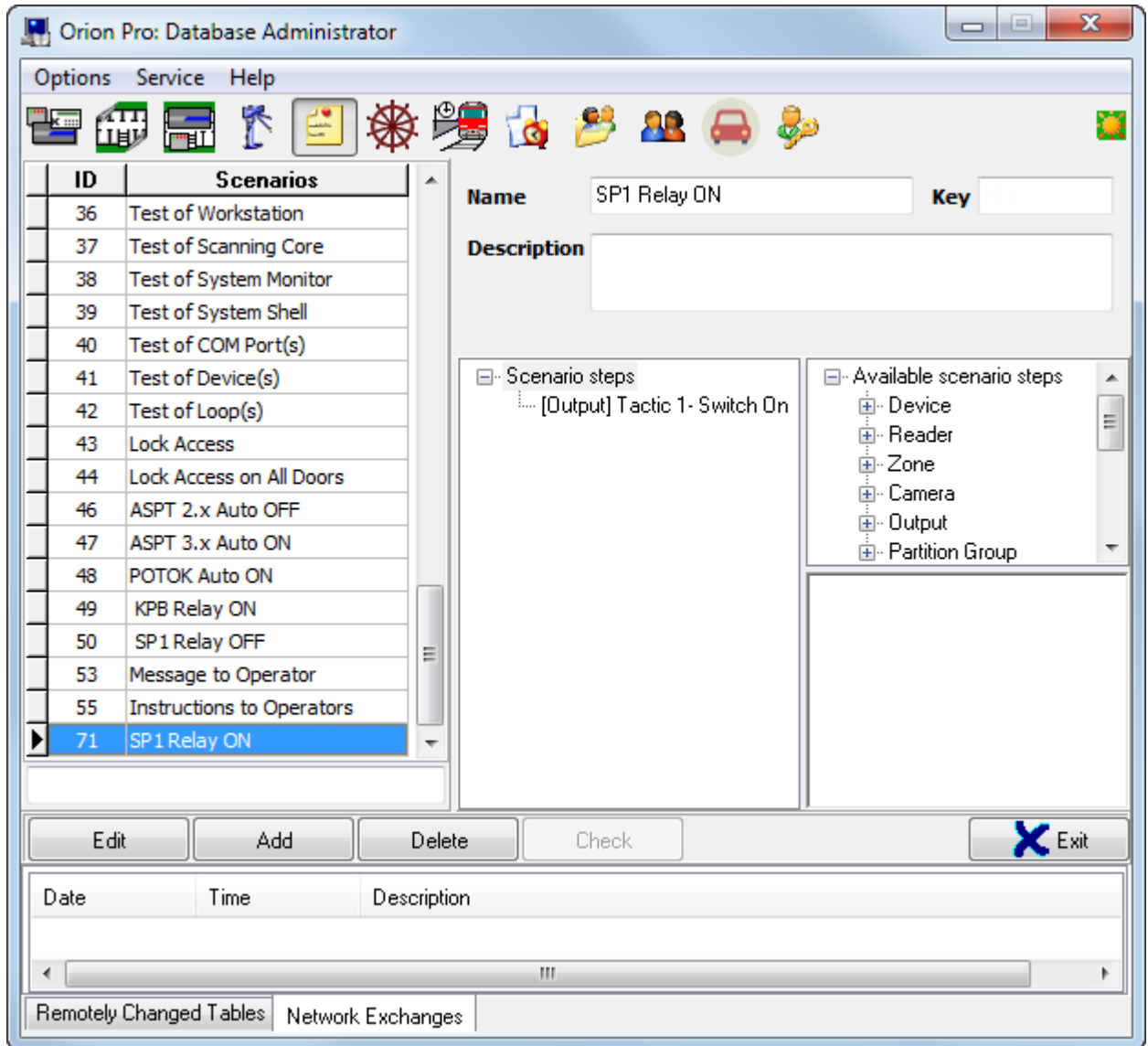


The right pane of the window shows the access points associated to the reader.  
The left pane of the window shows all the other access points of the current workstation.

To associate an access point to the reader, please select a require access point in the access control tree and double click it or the  button in the middle of the window.



## 6.6 The Management Scenarios Tab



The Management Scenarios tab includes the following:

1. List of management scenarios.
2. The attributes of a selected management scenario.
3. The display area of an action sequence of (scenario steps) or currently selected scenario script depending on whether it is based on a template or macrolanguage.

The Management Scenario tab is used to create management scenarios.

Scenarios are scripts or micro programs performing certain actions (mainly they send commands to the system entities).

The scenarios can be of the following types:

- Based on a template (in this case, it is the set of sequential steps with each responsible for a certain action);
- Based on a proprietary macrolanguage specially developed for this purpose (in this case, the scenario is a program based on a macro language).

Scenario can be initiated by:



- An operator of the System Monitor module:
  - ✓ Using hot keys,
  - ✓ Using the management tree,
- Automatically on schedule,
- Automatically as a response to system events.

This chapter focuses on the process of creating scenarios.

*The Description of creating a management tree is provided in Chapter 6.7 Management Tree Tab. The description of creating a schedule is provided in Chapter 6.8 The Schedule Tab. The Schedule of Management Scenarios Settings of automated scenario launched on schedules are described in Chapter 6.4.5 Configuring System Responses to Entity Events. Associating Scenarios to System Events.*

Let us consider the management scenarios:

ID	Scenarios
40	Test of COM Port(s)
41	Test of Device(s)
42	Test of Loop(s)
43	Lock Access
44	Lock Access on All Doors

The List of Scenarios displays the following information:

- Unique ID for each scenarios in the database
- Name.

Name:	43	Lock Access
-------	----	-------------

The bottom part of the list includes a field to search a scenario by name:

When you begin entering the first characters of the searched scenario's name, it will move to the scenario with a name starting with these characters:

ID	Scenarios
1	Access restoration
2	Access opening
4	To turn on the relay

It is worth mentioning that the list of scenarios is arranged in the order as they added to the database of the Orion Pro Suite (in other words, in accordance with their IDs).

In addition, the list can be sorted by two identifications:

- By ID
- By name

To change the order, please click the name of any column of the Scenarios list

( **ID**

or **Scenarios** ).

Each further click will change the type of sort order:

ID	Scenarios	ID	Scenarios
5	Disarming Room 1	49	KPB Relay ON
6	Disarming Room 2	50	SP1 Relay OFF
7	Disarming Room 3	28	ABORT RELEASE ASPT 2.x
8	Disarming Room 4	26	ABORT RELEASE Potok (Loop
9	Arming Room 1	21	Activate Rupor
10	Arming Room 2	23	Activate Rupor 01
11	Arming Room 3	9	Arming Room 1
12	Arming Room 4	10	Arming Room 2
14	SP1 Relay OFF	11	Arming Room 3
15	Blinking 20 SP1 Relay	12	Arming Room 4
16	Blinking 40 SP2 Relay	46	ASPT 2.x Auto OFF
17	KPB Relay ON	47	ASPT 3.x Auto ON
18	KPB Relay OFF	19	Blinking 20 KPB relay
19	Blinking 20 KPB relay	15	Blinking 20 SP1 Relay
20	Blinking 40 KPB relay	20	Blinking 40 KPB relay

In the Orion Pro system, the Scanning Core is responsible for management scenarios.

*Management scenarios and their schedules are not associated to Scanning Cores in the Orion Pro 1.12 system. Thus, it results in the following logic of starting management scenarios:*

- *Scenario runs as a response to system events:*

*The scenarios based on templates and launched as response to a specified event will be launched in the Scanning Core where a related event occurs*

- *An operator starts scenario using hot keys or the management tree.*

*A command to execute a scenario is sent to all Scanning Cores and System Monitors in the system. Therefore the scenario will be executed in all Scanning Cores.*

- *A scenario runs by schedule.*

*Schedules are loaded to each Scanning Core module. Therefore, a scenario will run in each Scanning Core modules.*

Considering the above, it is recommended to use the following approach for the macrolanguage-based scenarios, where they run on schedule, hot keys or from the management tree:

The management scenarios that is run on schedule, by hot key or from the management tree must be checked - some actions are required for the local Scanning Core (run the sequence of actions) or for a remote Scanning Core (but void running for the sequence of actions).

(The example of such a scenario is provided in Chapter 6.6.3 Task Resolved by Using Management Scenarios)

P.S. Scanning Cores also runs the scenarios that use commands for the System Monitor, System Shell entities, and the like. Such scenarios must be created using the macro language and run by any one of the Scanning Cores (i.e. to use the within-scenario test to check whether required actions are performed by one specific Scanning Core.)

### 6.6.1 Creating Management Template-Based Scenarios

To add a new template-base scenario:

- Click the **Add** button
1. In the appeared box, confirm whether a scenario will be based on a template by clicking the **Yes** button:
- Create a management scenario in the scenario window:

**Name** Script **Key** None

**Description**

**Scenario steps**

- [Core] Send a text message to

**Core**

- Display a message in the pop-up window
- Send a text message to Scanning Core
- Pause
- Pause (delay)
- Pause with the countdown window
- Request to Operator
- Play sound file
- Show camera
- Hide camera
- Run External Program
- Sending e-mail with a text to enter
- Sending e-mail
- Sending e-mail on event
- Connect to the mailbox
- Receive mail
- Allow receiving mail from the address ..
- Ban mail from the address ..

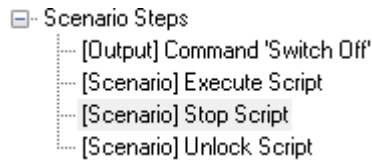
**Text** entrance opening

Scenario properties are displayed on the top:

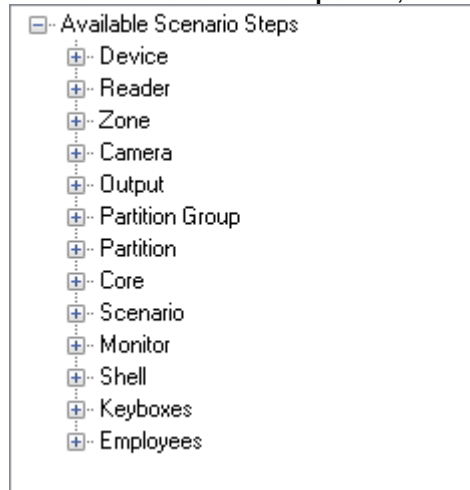
**Name** Request to Operator **Key** Ctrl + Shift + S

**Description**

The left part of the widow includes the **Scenario Steps** tree:



The right part of the window includes:  
the **Available Scenario Steps** tree,



the parameters of a scenario step selected in the Scenario Steps tree:

Text	entrance opening
------	------------------

To create a template-base management scenario, you should create the sequence of scenario steps and define their parameters:

The list of scenario steps is created in a way as follows:

- To add a new step in a scenario, please select it in the **Available Scenario Steps** tree and hold down the left button to drag it to the **Scenario Steps** tree. Alternatively, you can double click a required scenario step in the **Available Scenario Steps** to add it to the **Scenario Steps** tree.
- To move a scenario step in the **Scenario Step** tree, click it in the **Available Scenario Steps** and to drag it to required place in the tree holding down the left mouse button.
- To remove a scenario step from the **Scenario steps** tree, please select a required scenario step and press the <Del> key on the keyboard, then click **OK** to confirm the delete :

To configure the parameters of a scenario step, please select a required scenario step in the **Scenario Steps** tree, and then enter values in the parameter fields:

Computer	SecurityHead
Camera	[SecurityHead.2]: Camera 192.168.20.248

Parameters and possible values are not the same for different management scenarios.

*Description of each scenario steps can be found in Appendix 6 B. Standard Scenario Steps.*

- When the scenario is completed, click the **Save** button.

Properties of the Management Scenario Entity:

**Name**  **Key**

**Description**

Property	Possible values	Description
<b>Name</b>	A length of 1 to 25 characters	Management scenario's name. Default value: NewScenario1
<b>Description</b>	A length of 0 to 200 characters	Comments. <i>Optional field</i> Default value: empty field
<b>Key</b>	'None' or a hot key	Hot key is used as a quick start by a System Monitor operator. <i>This field is optional.</i> To set a hot key, left click this box and press a required key or key combination on your keyboard: <b>Key</b> <input type="text" value="Ctrl + Alt + F5"/>  To remove a hot key, click the box and press <Backspace> on a keyboard: <b>Key</b> <input type="text" value="None"/>  Default key: ' <b>None</b> ' (no key is set)

To edit a management scenario, please select a required management scenario from the list of scenarios and click the **Edit** button. Then make changes as required and click the **Save** button.

To delete a management scenario, please select a required scenario from the list of scenarios and click the **Delete** button. Then, click the **Yes** button in the appeared dialog box to confirm the delete action

It is worth mentioning that there is an option to display a macrolanguage programming code of a template-based management scenario.

To enable that, please select the **Show scenario text in template entering mode** check box in the settings of Database Administrator. (Options>Settings)

*The description of all parameters of Database Administrator is provided in Chapter 6.14.1 Database Administrator Settings*

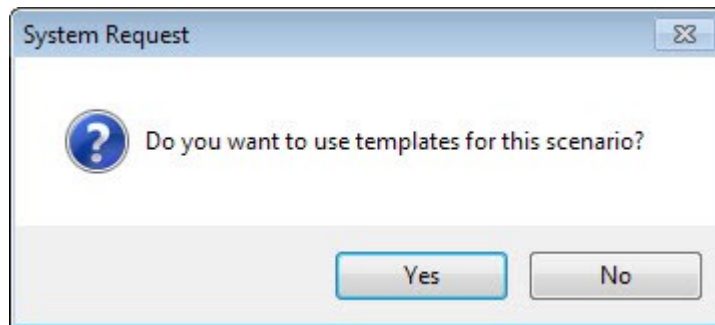
Note that if you have a template-base management scenario added (and saved) with no scenario steps included, that management scenario cannot be further edited (it can be deleted only).

All scenarios steps are described in *Appendix 6.B Standard Scenario Steps*

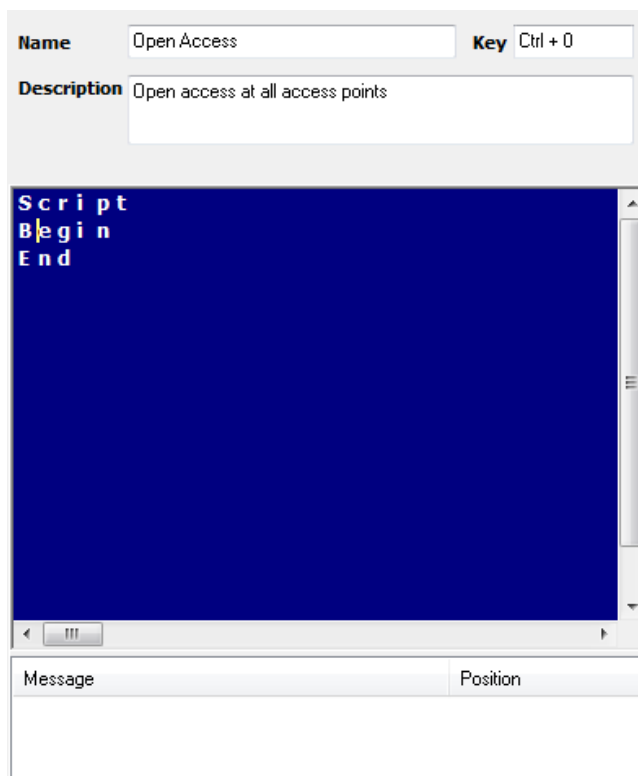
## 6.6.2 Creating Scenarios Using Built-In Script Language

To add a new macrolanguage-based management scenario,

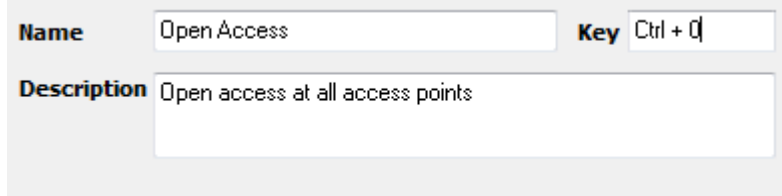
- please click the **Add** button, and then click **No** to define that the scenario will be based on the macrolanguage:



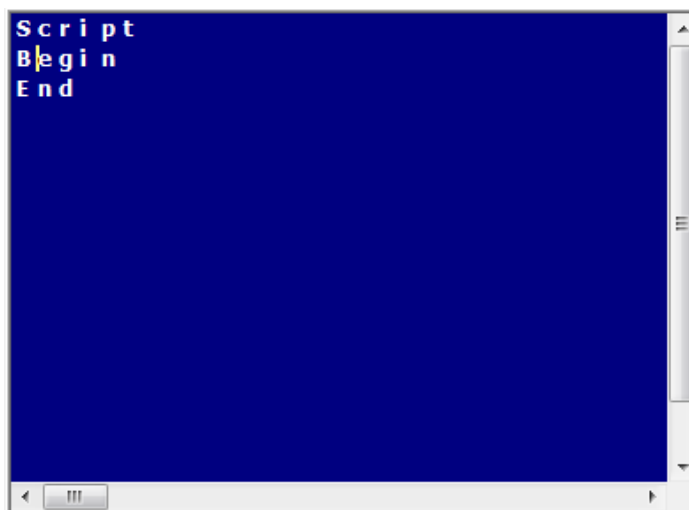
- Then enter a script for the management scenario in the area for entering script:

A window for configuring a management scenario. It has three main sections. The top section has a "Name" field with "Open Access" and a "Key" field with "Ctrl + O". The middle section has a "Description" field with "Open access at all access points". The bottom section is a large blue area for entering script, with the text "Script", "Begin", and "End" visible. Below the script area are two tabs: "Message" and "Position".



The bottom part shows the properties of the management scenario:

A window showing the properties of a management scenario. It has a "Name" field with "Open Access" and a "Key" field with "Ctrl + O". Below these is a "Description" field with "Open access at all access points".

The script entering area is in the middle of the window:



Underneath, you can see the area for error messages if found during the check:

Message	Position
 [Script] Expected "End"	
 [Script] Errors: 1. Warnings: 0	

To generate a macrolanguage-based scenario, please enter a script in the script enter area.

See *Description of OPIOH\_Scripts macrolanguage* document for the syntax and operating principles of embedded macrolanguage of Orion Pro's management scenarios.

To check spelling of the entered script, please click the **Check** button. Check results are displayed in the error box. If no results are visible after you have checked a script that means your entered script is correct. Otherwise, you will see errors in the error box.

- To complete your scenario, click the **Save** button.

Properties of the Management Scenario entity:

<b>Name</b>	<input type="text" value="Open Access"/>	<b>Key</b>	<input type="text" value="Ctrl + Q"/>
<b>Description</b>	<input type="text" value="Open access at all access points"/>		

Property	Possible values	Description
<b>Name</b>	A length of 1 to 25 characters	Management scenario's name. Default scenario: NewScenario1
<b>Description</b>	A length of 0 to 200 characters	Comments. <i>This field is optional.</i> Default value: empty field
<b>Key</b>	'None' or a hot key	A hot key is used as a quick start by a System Monitor operator. <i>This field is optional.</i> To set a hot key, left click this box and press a required key or key combination on your keyboard:

		<p><b>Key</b> Ctrl + Alt + F5</p> <p>To remove a hot key, click the box and press &lt;Backspace&gt; on a keyboard:</p> <p><b>Key</b> None</p> <p>Default key: None (no key is set)</p>
--	--	--

To edit a management scenario, please select a required management scenario from the list of scenarios and click the **Edit** button. Then make changes as required and click the **Save** button.

To delete a management scenario, please select a required management scenario from the list of scenarios and click the **Delete** button. Then, click **Yes** in the appeared dialog box to confirm the delete action

The management scenarios based on the embedded language can be saved and imported from a text file.

To save or import a management scenario, click the **Edit** button to enter an editing mode, then right click the scenario script area, and select the **Load from file** or **Save to file** item in the popup menu as required.

Load from file
Save to file
Settings...

Then specify a file path to import or save a management scenario in a standard system dialog window.

The Database Administrator offers capability of setting colors for script of a management scenario. Click the **Edit** button to enter an editing mode, then right click the scenario script area, and select the **Settings** menu command to open the **Scenario Editor** window.

In this window, you can:

Set a type, size, and color of script fonts for management scenarios in the Highlight Syntax:

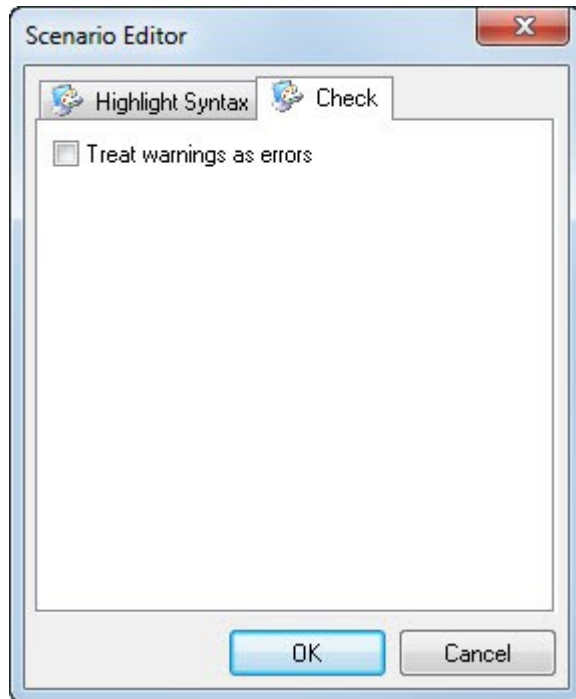
The image shows a 'Scenario Editor' dialog box with a title bar and a close button (X). It contains two tabs: 'Highlight Syntax' and 'Check'. The 'Highlight Syntax' tab is active. It features several settings:

- Text font:** A dropdown menu.
- Background:** A color selection box showing 'clNavy'.
- Font size:** A numeric input field set to '10'.
- Descriptors:** A color selection box showing 'clLime'.
- Keywords:** A color selection box showing 'clWhite'.
- Lines:** A color selection box showing 'clAqua'.
- Numbers:** A color selection box showing 'clRed'.
- Symbols:** A color selection box showing 'clYellow'.
- Comments:** A color selection box showing 'clSilver'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.



- Select the check box of the **Treat warnings as errors** option in the Check tab:



## 6.6.3 Examples of Tasks of Management Scenarios

Let us consider the examples of two tasks resolved using management scenarios.

### Task 1:

If the intrusion detection, fire protection, and access control systems are controlled by the Scanning Core only, the interaction between these systems can be implemented using management scenarios.

Specifically, fire evacuation tasks can be resolved (automatically open free access) at the site exit for employees to escape when a fire alarm occurs).

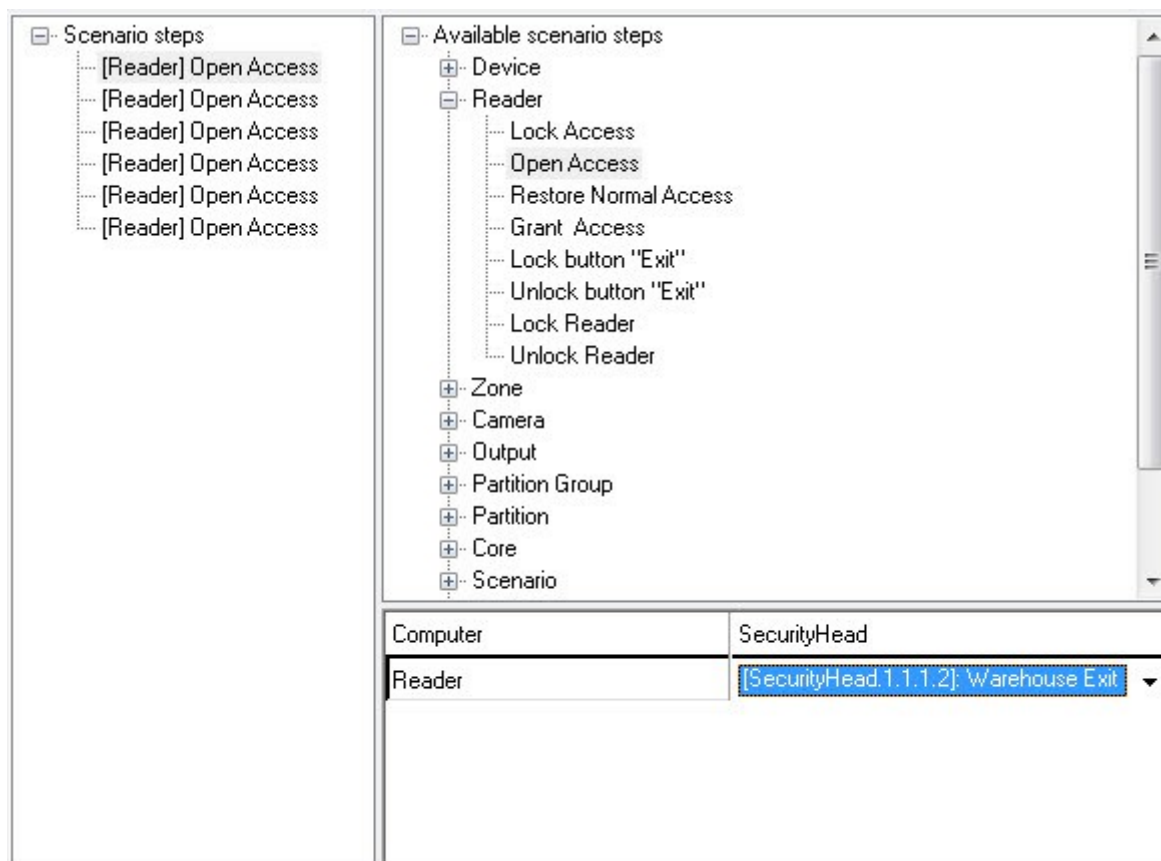
In other words, the task is to use a scenario to provide a free access (for exit) through access points in case of fire alarm in any fire partition.

A template-based scenario will be used for this purpose. It will include several steps to the Open Access scenario.

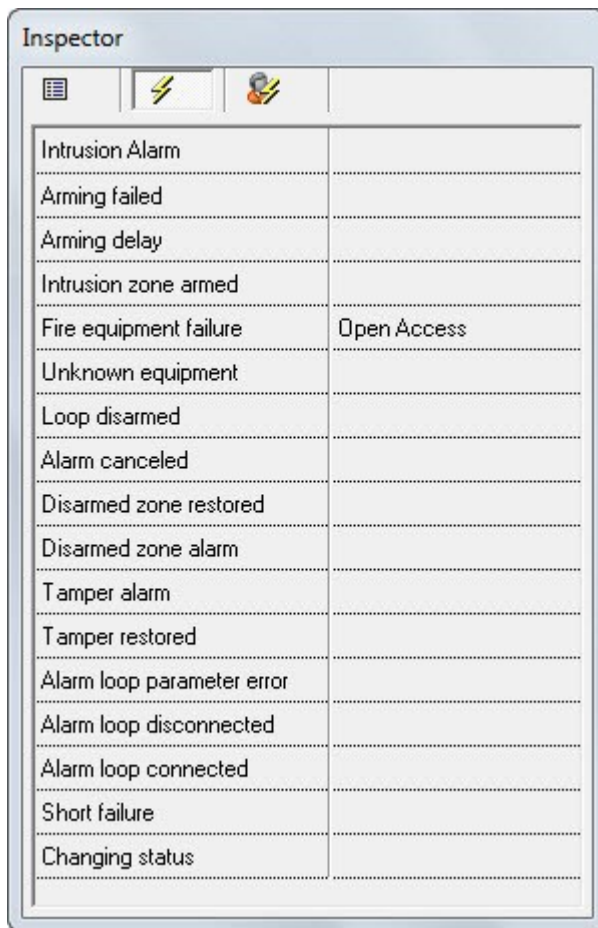
The S2000-2 and S2000-4 controllers block (filter out) direct commands to their relay outputs (ON, OFF, etc.) used for access control purpose. To unlock an access point (open free access), the **Open Access** command should be used.

Let us create the Evacuation template-based scenario with the Open Access scenario steps. The number of scenario steps equals to access points where a free access to exit must be given.

Define an exit reader of a relevant access point for each scenario in the **Reader** field.



To ensure the access point unlocking in case of fire, please associate the Evacuation scenario (newly developed) to the Fire alarm event.



Thus, when any fire partition goes into alarm, a free access will be given at each access point controlled by the readers specified in the Evacuation management scenario.

### **Task 2:**

Some facilities or enterprises require to have an access lockdown for the entire night time.

Scheduled scenarios can resolve the above task.

The task will be subdivided into two subtasks:

1<sup>st</sup> subtask will lock the access every night as scheduled

2<sup>nd</sup> subtask will return normal access mode (using credentials) at the access point every morning as scheduled.

Let's consider the implementation of the first task.

Let's create a management scenario that will lock down the access points.

Since this scenario runs on schedule it will be executed in each Scanning Core. To prevent Scanning Cores from sending their commands to each access controlling device but for their own devices only, the macrolanguage-based scenario must be used with the check of the scenario's script.

Let's create the Lock Access scenario. Textually, the scenario will be as follows:

```
//-----
Script
Vars
Var Computers 1;
Var Workstation =2;
Var Door1;
Var Reader2;
Var X;
Var Y;
```

```

BeginScenario
Computers1 = CreateEntity( "Computers" );
If not EmptyValue( Computers1 ) then
For X = 0 ПоComputers1.Quantity() - 1 Cycles
  If not EmptyValue( Computers1.Element( X ) ) Тогда
    Eh not EmptyValue( Computers1.Element( X ).Workstations'() ) Than
      Workstation2 =
Computers1.Element( X ).Workstations().Receive as a NetworkPlaceType
( "ScanningCore" );
    If not EmptyValue( Workstation2 ) Then
      IF Workstation2.Local() == Then true // Required check
        Doors = Workstation2.Doors();
        If not EmptyValue( Doors ) Then
          For Y = 0 ПоDoors1.Quantity() - 1 Cycle
            If not EmptyValue( Doors1.Element( Y ) ) Then
              Reader2 = Doors1.Element( Y ).ReaderforExit();
              If not EmptyValue( Reader2 ) Than
Reader.LockAccess();
EndIf;
                Reader2 = Doors1.Элемент( Y ).ReadertoExit();
                If not EmptyValue( Reader2 ) Тогда
Reader2.LockAcces();
EndIf;
EndIf;
EndIf;
EndIf;
EndIf;
EndIf;
EndIf;
EndIf;
EndCycle;
EndIf;
EndScript

```

//-----

Then the Lock Access time zone is created with a start time: specified

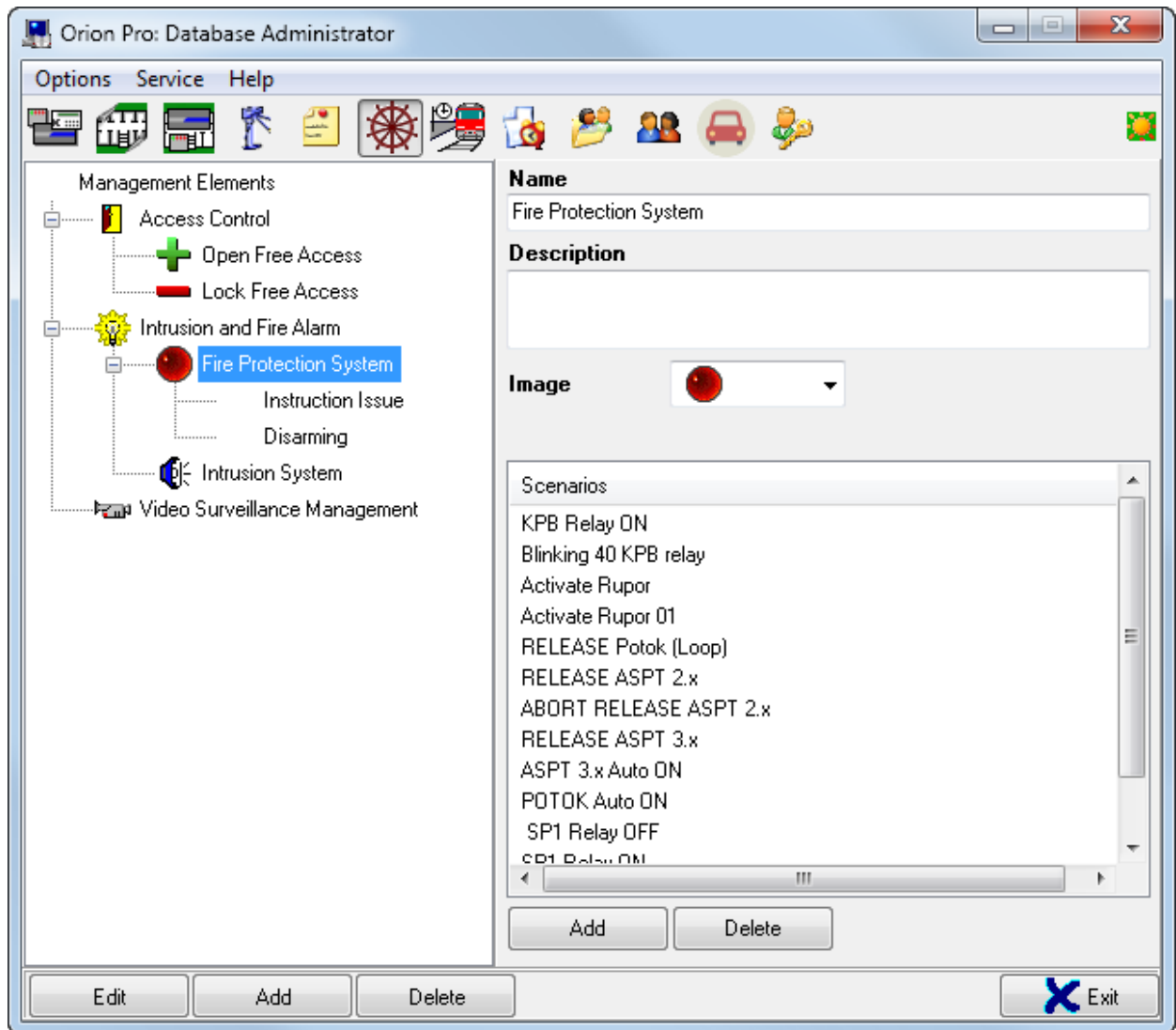
End	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
21:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start time	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
21:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Finely, scheduled run is generated.

Management Scenario	Time Zone
Lock Access on All Doors	Lock Access

The second task is resolved in the same way as the first one.

## 6.7 Management Tree Tab



The Management Tree tab shows the following information:

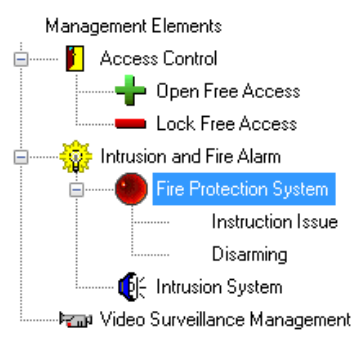
1. Management Tree.
2. The properties of a selected management node.
3. The management scenarios of a selected management tree.

The Management Tree tab is intended to maintain a system management tree.

An operator of the System Monitor can manually start scenarios using the management tree.

*The process of creating management scenarios is described in Chapter 6.6 The Management Scenarios Tab.*

The management tree includes the following nodes:



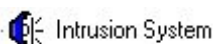
**Management Elements** is a main node of the system. It does not include any scenarios, and actually it is the name of the management tree that cannot be edited or deleted.

Each management node (except for Management Elements) can have scenarios assigned:



The Management Tree displays the following information for each node:


- Icon (if defined in the properties of the node)
- Name




Please, do the following actions to add a new management node to the management tree:

- Select a management node where a new node will be associated:
- In the right pane of the window, enter properties and make up the list of scenarios for a new node:

The upper part of the pane includes definable attributes (Name and description) of the management tree:

<b>Name</b>	Fire Protection System
<b>Description</b>	
<b>Image</b>	 ▼

<b>Name</b>	Management of fire system
<b>Description</b>	
<b>Image</b>	 ▼

The lowest box contains the list of management scenarios of the management tree:

Scenarios
KPB Relay ON
Blinking 40 KPB relay
<input type="button" value="Add"/> <input type="button" value="Delete"/>

The list of scenarios of a management tree is made up in a following manner:


- To add a new management scenario, please click the **Add** button, then select a required scenario in the **Select Scenario** dialog window and click the **OK** button.


Select Scenario																		
<table border="1"> <thead> <tr> <th>Scenario</th> </tr> </thead> <tbody> <tr><td>Activate Ruror 01</td></tr> <tr><td>Deactivate Ruror 02</td></tr> <tr><td>RELEASE Potok (Loop)</td></tr> <tr><td>ABORT RELEASE Potok (Loop)</td></tr> <tr><td>RELEASE ASPT 2.x</td></tr> <tr><td>ABORT RELEASE ASPT 2.x</td></tr> <tr><td>RELEASE ASPT 3.x</td></tr> <tr><td>▶ Open Access</td></tr> <tr><td>Close Access</td></tr> <tr><td>Message to Operator</td></tr> <tr><td>Test of Computers</td></tr> <tr><td>Test of Computer</td></tr> <tr><td>Test of Workstations</td></tr> <tr><td>Test of Workstation</td></tr> </tbody> </table>	Scenario	Activate Ruror 01	Deactivate Ruror 02	RELEASE Potok (Loop)	ABORT RELEASE Potok (Loop)	RELEASE ASPT 2.x	ABORT RELEASE ASPT 2.x	RELEASE ASPT 3.x	▶ Open Access	Close Access	Message to Operator	Test of Computers	Test of Computer	Test of Workstations	Test of Workstation	<table border="1"> <thead> <tr> <th>Description</th> </tr> </thead> <tbody> <tr> <td>door</td> </tr> </tbody> </table>	Description	door
Scenario																		
Activate Ruror 01																		
Deactivate Ruror 02																		
RELEASE Potok (Loop)																		
ABORT RELEASE Potok (Loop)																		
RELEASE ASPT 2.x																		
ABORT RELEASE ASPT 2.x																		
RELEASE ASPT 3.x																		
▶ Open Access																		
Close Access																		
Message to Operator																		
Test of Computers																		
Test of Computer																		
Test of Workstations																		
Test of Workstation																		
Description																		
door																		
<input type="button" value="✓ OK"/> <input type="button" value="✗ Cancel"/>																		

The left part of the Select Scenario window includes all management scenarios of the system except for those already added to the current management node.  
The right part of the window displays comments to a selected management scenario (textual information entered in the Description property field of this management scenario).

- To remove a management scenario from the list, select a required scenario and click the **Delete** button, then confirm the deletion action by clicking the **Yes** button:
- To complete the management node, click the **Save** button.

The properties of a management node:

<b>Name</b>	Fire Protection System
<b>Description</b>	
<b>Image</b>	 ▼

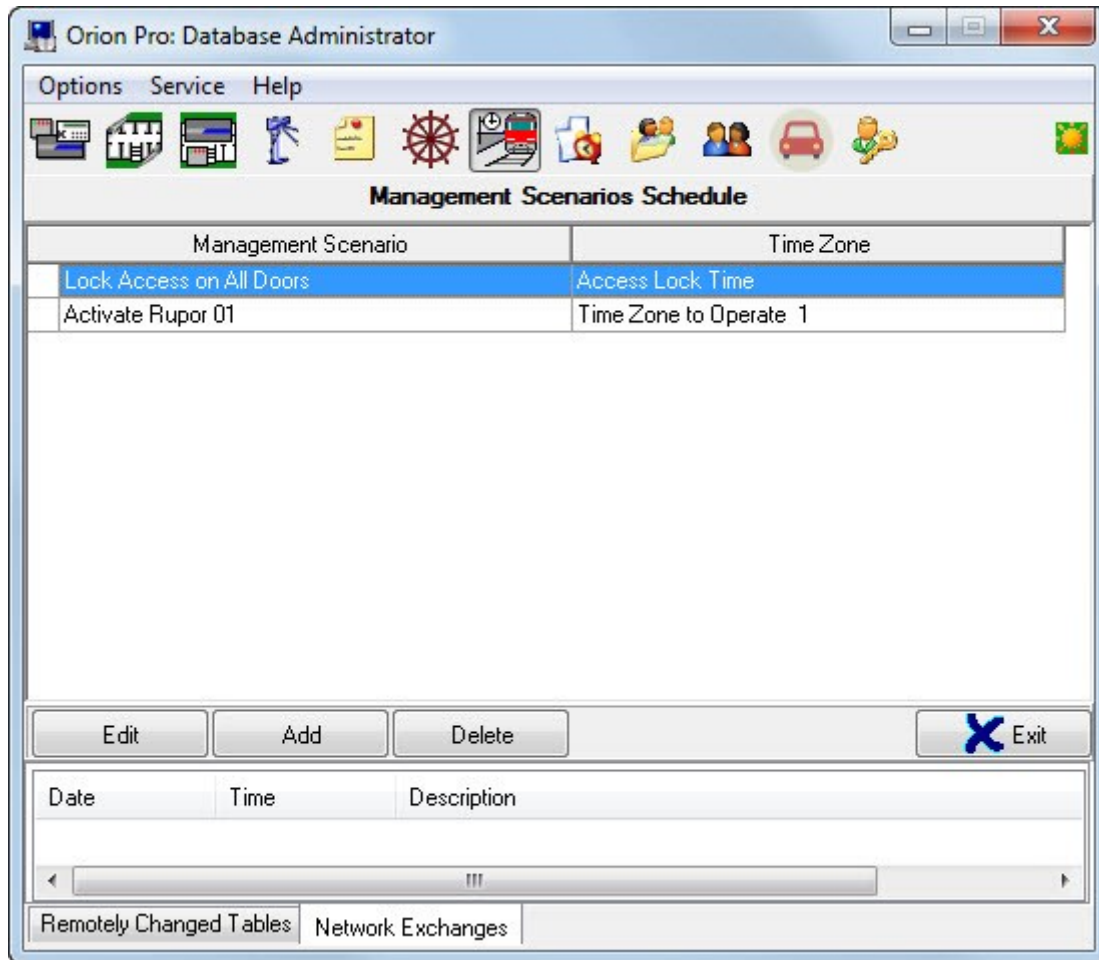
Properties	Possible Values	Description
Name	A length of 0 to 200 characters	The name of a management tree. <i>This field is optional.</i> Default value: Empty field
Description	A length of 1 to 200 characters	Comments. <i>This field is optional.</i> Default value: Empty field
Image		The icon of a management tree. <i>This field is optional.</i> Default value: empty field

To change parameters of a management tree node, please select a required node in the management tree and click the **Edit** button. Then make necessary changes and click the **Save** button.

*Attention. When you delete a node from the management tree, all other nodes associated to this node will be deleted.*



## 6.8 The Schedule Tab. Schedule of Management Scenarios



The Management Scenario Tab shows the following information:

1. The Schedule of Management Scenario.

The scenario may be executed automatically on defined time (on schedule).

The **Schedule** tab is used to create schedules for management scenarios.

The Management Scenario Schedule is a two-column list. The Scenarios column (left) lists management scenarios, the Time Zone column (right) includes time zones governing the runs of management scenarios.

Each line item in the Schedule is a schedule for running one specific scenario. In other words, a time zone is associated to each scenario to start it automatically as this time zone defines.

To add a new line item to the schedules, please

- Click the Add button to add a new line to the list:

Management Scenario	Time Zone
Lock Access on All Doors	Access Lock Time
Activate Rupor 01	Time Zone to Operate 1

- Then select the required scenario in the dropdown list of the Management Scenario column:

Management Scenario	Time Zone
Lock Access on All Doors	Access Lock Time
Test of System Monitor	Time Zone to Operate 1
Test of System Shell	
Test of COM Port(s)	
Test of Device(s)	
Test of Loop(s)	
Lock Access	
Lock Access on All Doors	

- Then select a time zone in the dropdown list of the Time Zone column:

Management Scenario	Time Zone
Lock Access on All Doors	Access Lock Time
Activate Ruper 01	Time Zone to Operate 1
	Time Zone to Operate 2
	Access Lock Time

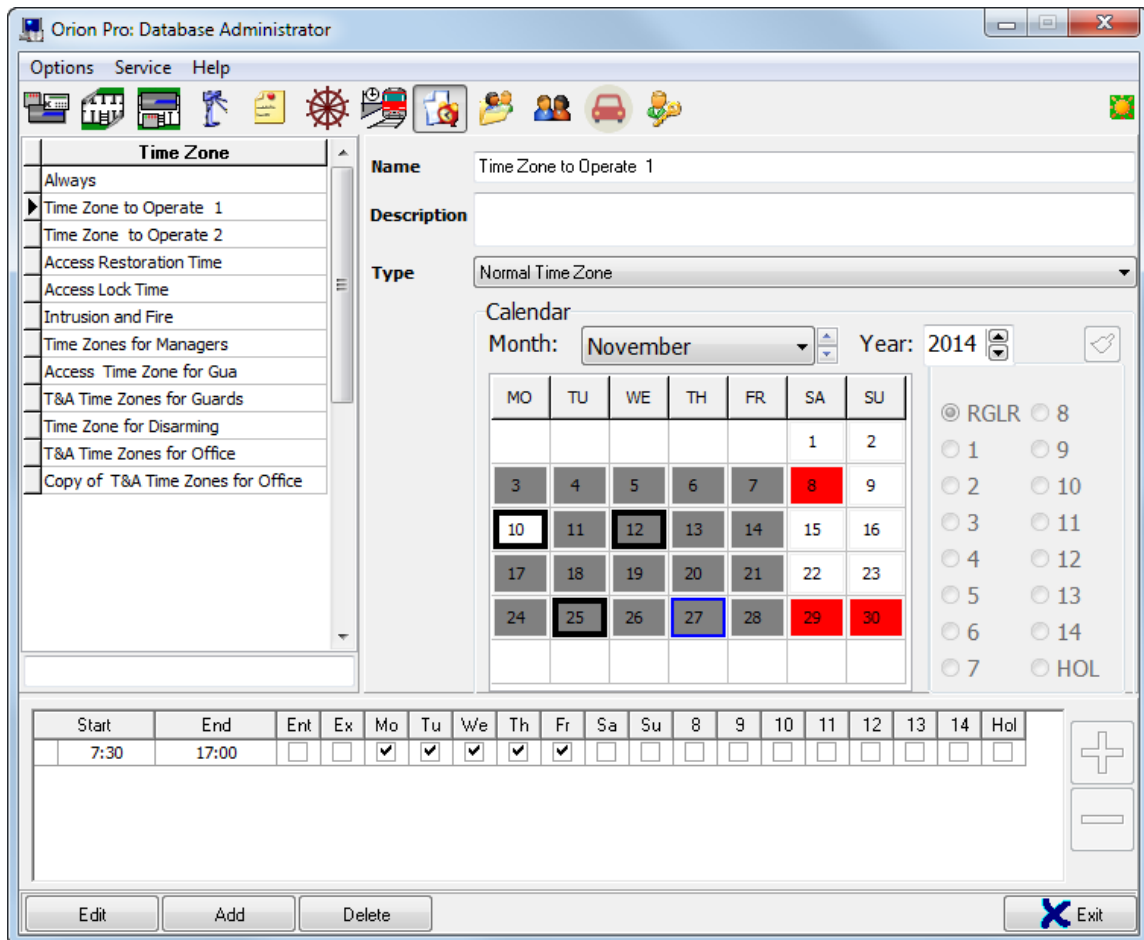
*It is worth mentioning, the Management Scenarios Schedules displays only those time zone that that is set as **Time Zone for Management Scenarios**.*

- Click the **Save** button.

To make changes in scenario schedules, please click the **Edit** button. Then make necessary changes and click the **Save** button.



To delete a line item from the schedules of management scenarios, select a required line and click the **Delete** button. Then click **Yes** to confirm the delete action in the appeared dialog box.

## 6.9 The Time Zones Tab. Configuring Time Zones



The Time Zones tab shows the following information:

1. List of Time Zones
2. Selected time zone attributes
3. Selected time zone calendar display
4. Calendar tools area
5. Display of time intervals of a selected time zone

*It is worth mentioning that the calendar handling area is hidden by default. In order to display this area, please click the  button under the calendar. To hide the area click the same button that has the following appearance  when this area is open.*

The Time Zones tab is used to create time zones for Intrusion (Detection) and Fire (Alarm) System, Access Control System, Time and Attendance, and Management Scenarios

- A time zone for Intrusion and Fire System (IFS Time Zone) includes a group of time intervals defining the period when users are allowed to operate IFS entities at a protected site.
- A time zone for Access Control System (ACS Time Zone) includes a group of intervals defining the time when employees may access a protected area through access control points.
- A time zone for Time and Attendance includes a group of time intervals defining employees' work schedules
- A time zone for management scenarios includes time points to launch management scenarios.

Each time zone's calendar can be changed:

- Define any day as a holiday (i.e., a day with active time intervals different from other days of a week)
- Carry over working days
- Create flexible and rotating shift work schedules

Let's consider the list of time zones:

Time Zone
Always
Time Zone to Operate 1
Time Zone to Operate 2
Access Restoration Time
Access Lock Time
Intrusion and Fire Time
Time Zones for Managers
Access Time Zone for Gua
T&A Time Zones for Guards
Time Zone for Disarming
T&A Time Zones for Office

The Time Zone box displays the names of times zones:

- Name.

Time Zone to Operate 1

The bottom part contains the search field:

tim

When you start typing in this field (case sensitive), it moves you to a name beginning with the characters you type:

Time Zone
Always
Time Zone to Operate 1
Time Zone to Operate 2
Access Restoration Time
Access Lock Time
Intrusion and Fire Time
Time Zones for Managers
Access Time Zone for Gua
T&A Time Zones for Guards
Time Zone for Disarming
T&A Time Zones for Office

Acc

Please keep in mind that time zones are listed in the same order as they were added to the database (in accordance with their unique IDs)

Time zone list can be sorted by:

- IDs, or
- Name

To change the arrangement principle, click the column heading (Time Zone).

The type of sorting will be changed with every new click:

Time Zone	Time Zone
Access Lock Time	Always
Access Restoration Time	Time Zone to Operate 1
Always	Time Zone to Operate 2
Intrusion and Fire Time	Access Restoration Time
T&A Time Zones for Guards	Access Lock Time
T&A Time Zones for Office	Intrusion and Fire Time
Time Zone to Operate 2	Time Zones for Managers
Time Zone for Disarming	T&A Time Zones for Guards
Time Zone to Operate 1	Time Zone for Disarming
Time Zones for Managers	T&A Time Zones for Office

Further, the Guide describes how to configure time zones, to create management scenarios through definition of time periods and development of calendars.

The major part of such information is provided in *Chapter 6.9.1 The Time Zone for Intrusion and Fire Detection System (IFS)*, *Chapter 6.9.2 The Time Zone for Access Control Systems (ACS)*, *Chapter 6.9.3 The Time Zone for Working Time and Attendance Control*, and *Chapter 6.9.4 The Time Zone for Management Scenario Schedules*

This chapter focuses on Time Zone attributes

Time Zone Attributes:

<b>Name</b>	Access Lock Time
<b>Description</b>	
<b>Type</b>	Normal Time Zone

Attributes	Possible Values	Description
<b>Name</b>	Line is 1 to 25 characters long	The name of a time zone. Default value: empty field
<b>Description</b>	Line is 0 to 200 characters long	Comments. <i>This field is optional.</i> Default value:
<b>Type</b>	Normal Time Zone Scenario Time Zone	A type of time zone. <b>Normal Time Zone</b> is set for Intrusion and Fire Detection System, Access Control System and Time and Attendance Control <b>Scenario Time Zone</b> is assigned to time zones intended to launch the schedule of management scenarios. Default value: <b>Normal Time Zone</b>

Attention! You can make a copy of a time zone. Right click the time zone you want to copy and select the Create a copy of this time zone item in the pop-up menu:

Create a copy of this time zone
---------------------------------

A copy of time zone will be created with 'Copy of' added before the name of a copied time zone:

Time Zone	
	Always
	Copy of Always

Attention! The Orion Pro software supports the unlimited number of time zones and time periods within each time zone. Thus, there are no limits for centralized control operation. But if you want to save a time zone to a device for the local control of intrusion, fire, and access, beware of the limited number of time zones to be handled by each device.

Device	Version	Time Zones	Periods within time zone
S2000-2	1.02-1.11	15	10
	1.15	16	10
S2000-4	1.10-1.12	8	8
	2.00-3.00	15	10

By default, Orion Pro includes an **Always** time zone that cannot be edited or deleted. This time zone may apply to any time or day of the week, and it can be used with intrusion, fire and access control systems.

### 6.9.1 Time Zone for Intrusion and Fire System (IFS)

This chapter focuses on creation of time zones for intrusion and fire system (IFS time zone)

To add a new Time Zone entity, please:

- Click the **Add** button.
- Enter necessary values for the properties of the new Time Zone entity - **Name** and **Description**. Please, make sure that the default **Normal Access Zone** is selected in the Type field.
- Configure time periods (*See Chapter 6.9.1.1 Time Periods for more details on how to create IFS time periods*)
- Change calendar settings, if needed (*Chapter 6.9.1.2 Using Calendar describes the calendar development process*).
- Finally, click the **Save** button.

To edit the Time Zone properties, please, select a required time zone from the list and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete a Time Zone item, please select a required zone and click the **Delete** button, then click **Yes** to confirm the delete action:

#### 6.9.1.1 Time Periods

By default, there are no time periods in a new time zone. To add a time period, please click the **Edit**



button to enable the editing mode, then click the button and enter required values in the fields of the new time period.

To modify field values of a time period, please click Edit button, then select a required time period from the list of time values and set values you want.

To delete a time period from a time zone, please click Edit to go into the editing of time zone, and then



select a time period from the list of time periods and click the button.

Then, confirm the delete action by clicking the **Yes** button:

A time period has the following fields:

Field	Possible Values	Description
<b>Start</b>	'0:00'...'23:59'	Launch of a time period Default value: '0:00'
<b>End</b>		End of a time interval Default value '23:59'
<b>Ent</b>	<input checked="" type="checkbox"/> (checked), <input type="checkbox"/> (unchecked)	<i>Not used for intrusion and fire detection time zones</i> (*)
<b>Ex</b>		<i>Not used for intrusion and fire time zones.</i> (*)
<b>Mo</b>	<input checked="" type="checkbox"/> (checked), <input type="checkbox"/> (unchecked)	Time period activity attribute:
<b>Tu</b>		Monday (the 1 <sup>st</sup> day of schedule) Tuesday (the 2 <sup>nd</sup> day of schedule) Wednesday (the 3 <sup>rd</sup> day of schedule) Thursday (the 4 <sup>th</sup> day of schedule) Friday (the 5 <sup>th</sup> day of schedule)
<b>We</b>		
<b>Th</b>		
<b>Fr</b>		Default value: : <input checked="" type="checkbox"/>
<b>Sa</b>		Time period activity attribute: Saturday (the 6 <sup>th</sup> day of a schedule), Sunday (the 7 <sup>th</sup> day of the schedule).
<b>Su</b>		Default value: <input type="checkbox"/>
<b>8</b>		Time period activity attribute: From the 8 <sup>th</sup> day to the 14 <sup>th</sup> day of the schedule.  Default value: <input type="checkbox"/>
<b>9</b>		
<b>10</b>		
<b>11</b>		
<b>12</b>		
<b>13</b>		
<b>14</b>		
<b>Hol</b>		Attribute of time period activity on holiday (**)  Default value: <input type="checkbox"/>

(\*) If a time zone is used for local control of the S2000-2 controller's loops, the parameters **Ent** and **Ex** define whether the loops can be controlled using Reader 1 (Ent) and Reader 2 (Ex) of the controller.

(\*\*) The Holiday (**Hol**) is used only to facilitate the perception of a schedule, and actually is the same as the other schedule days (1-14), so it can be defined as the 15<sup>th</sup> day of the schedule.

A schedule can include up to 14 days (plus **Holiday**).

A 7-day schedule is the most common type of schedules, but other types can be used in case of shift-based or flexible schedules.

The most typical schedules are as follows:

If a schedule is based on a calendar week (e.g., Monday through Friday are working days with Saturday and Sunday being days-off), only seven days of the schedule will be used (and the 8<sup>th</sup> day as a Holiday) and others will not be used.

Complex and flexible schedules are not associated with a calendar week. The number of used schedule days depends on the schedule logic. For example, the **3 working days, 3 days-off** schedule uses six schedule days (plus the 7<sup>th</sup> day (Holiday))

Below are three examples of time zones:

#### **Example 1**

The task is to configure a time zone for arming/disarming an IFS (Intrusion and Fire System) entity. The operations are allowed from 7:30 till 17:30 from Monday through Thursday, and from 7:30 till 16:30 on Friday.

The schedule will use 7 calendar days (Mo - Su), plus **Hol** (Holiday)

Therefore, the time periods of this schedule will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:30	17:30	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:30	16:30	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The above task allows another way of time zone configuration as shown below, though it seems less user-friendly than the previous one:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:30	17:30	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:30	16:30	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

It is recommended to use the first version.

### Example 2

The task is to configure a time zone for arming/disarming an IFS entity. Operations shall follow the '**3 over 3 days**' schedule, where operations may happen from 8:00 till 17:00 for 3 days running with no operations for the next 3 days. The schedule will use 6 days of the schedules plus **Holiday**.

Therefore, the time periods of this schedule will look as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
08:00	17:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Example 3

The task is to configure a time zone for arming/disarming an IFS entity.

The arming/disarming operations shall follow the '**3 working days, 3 days-off, 3 working nights, 3 days-off**' schedule where arming/disarming can be provided from 8:00 till 20:00 three days running with no arming/disarming allowed for the next three days, then three more days when arming/disarming are allowed from 20:00 till 8:00, and then no operation is allowed for the next three days; holidays are not foreseen.

The schedule uses 12 schedule days.

The time periods will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
8:00	17:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20:00	23:59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0:00	08:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 6.9.1.2 Using the Calendar

When time periods are set, the list of calendar days needs to be defined for a time zone.



Calendar

Month: October Year: 2014

MO	TU	WE	TH	FR	SA	SU
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

☒ RGLR ☐ 8  
☐ 1 ☐ 9  
☐ 2 ☐ 10  
☐ 3 ☐ 11  
☐ 4 ☐ 12  
☐ 5 ☐ 13  
☐ 6 ☐ 14  
☐ 7 ☐ HOL

*Attention! The Orion Pro software allows a user to define calendar days for a one-year period*

By default each calendar day is set as **Regular (RGLR)**.


But other values can be assigned to any day of a calendar.

The following values are available: Regular, "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12", "13", "14", Holiday.

If the day is set as Normal, the day corresponds to a week day in the calendar (i.e. 1 is Monday, 2 is Tuesday, 3 is Wednesday, 4 is Thursday, 5 is Friday, 6 is Saturday, and 7 is Sunday in accordance with the calendar).

The most common two types of calendar configurations are as follows:

- If the schedule is associated with a calendar week (e.g. Days from Monday through Friday are deemed working days but Saturday and Sunday are days-off), then most days of the list cannot be redefined (Regular day for the week corresponds to the calendar day). Several days only are set as Holidays or can be redefined (in case of working days rescheduled because of the national holidays).
- If rotating or flex-time schedules (not based on a calendar week) are used, all days from the list are redefined directly with no days left for the Regular days.

You can clear the list of calendar days in the Database Administrator (define all days of the list as Regular). To do that, please click the  button in the editing mode.



The calendar color coding scheme has the following logic:

- Day definitions:
  - If a day is set as a specific day (different from Holiday), it will be framed:

Example: 1

Or 2

- If a day is not redefined and has a default definition as Regular, it will not be framed.

Example: 

or 

- If a calendar day is set as Holiday (**Hol**), it will not be framed.



Example: 

- Active time periods:

- If any one of time periods is active for a defined calendar day, this day will be highlighted grey.

Examples:  or .






- If no time period is active for a calendar day, this day will not be highlighted:

Example:  or .

- If a calendar day is set as **Holiday**, this day will be always highlighted red whether the time period is active or not.

Example: .

Hence, there are five graphic representations in the Calendar:

-  – Regular day with one active time period at least
-  – Regular day with no active time periods (a day-off),
-  – Redefined day of the schedule with one active time period at least,
-  – Redefined schedule day with no active time periods (a day-off),
-  – Holiday

Makeup of calendar days is illustrated with the examples from *Chapter 6.9.1.1 Time Periods* above

*Example 1:*

Arming/Disarming shall be allowed from 7:30 till 17:30 from Monday through Thursday and from 7:30 till 16:30 on Friday.

The schedule uses seven calendar days (Mo - Su) plus Holiday.

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:30	17:30	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:30	16:30	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Since the schedule uses a standard week, most days are not redefined (all are set as Regular days)

Calendar

Month: January Year: 2014

MO	TU	WE	TH	FR	SA	SU
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

☒ RGLR ☐ 8  
☐ 1 ☐ 9  
☐ 2 ☐ 10  
☐ 3 ☐ 11  
☐ 4 ☐ 12  
☐ 5 ☐ 13  
☐ 6 ☐ 14  
☐ 7 ☐ HOL

Only some days are defined as holidays, and some will be moved.

The time period in the above example with January 2009 has the following configuration: The **Holiday** value is assigned for days within January 1-10, and the 1<sup>st</sup> day (corresponds to Monday) is set for January 11 (since this is the first working day of the year nationwide). The remaining days of January are not redefined.

Calendar

Month: January Year: 2009

MO	TU	WE	TH	FR	SA	SU
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

☐ RGLR ☐ 8  
☒ 1 ☐ 9  
☐ 2 ☐ 10  
☐ 3 ☐ 11  
☐ 4 ☐ 12  
☐ 5 ☐ 13  
☐ 6 ☐ 14  
☐ 7 ☐ HOL

Example 2:

Arming/Disarming shall follow the **3 over 3 days** schedule, when operations may happen from 8:00 till 17:00 for 3 days running with no operations for the next 3 days.

The schedule will use 6 days of the schedule plus **Holiday**.

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
08:00	17:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

A specific value is set for each day. If it is deemed that in 2009, the working days, after the New Year holidays, start from the 11<sup>th</sup> of the January (that corresponds to the 1<sup>st</sup> day of the schedule), the schedule for January, 2009 has the following configuration:

- Holiday is set for the dates from the 1<sup>st</sup> through the 10<sup>th</sup> of January

- The 1<sup>st</sup> day is set for 11<sup>th</sup> of January, the 2<sup>nd</sup> day for the 12<sup>th</sup> of January, the 3<sup>rd</sup> day for the 13<sup>th</sup> of January, the 4<sup>th</sup> of 14<sup>th</sup> of January, and the 5<sup>th</sup> day for 15<sup>th</sup> of January, and the 6<sup>th</sup> day for 16<sup>th</sup> of January

And further, in accordance with the 3 days over 3 days schedule:

- the 1<sup>st</sup> day for the 17<sup>th</sup> of January, the 2<sup>nd</sup> day for the 18<sup>th</sup> of January, the 3<sup>rd</sup> day for the 19<sup>th</sup> of January, the 4<sup>th</sup> day for the 20<sup>th</sup> of January, and the 5<sup>th</sup> day for the 21<sup>st</sup> of January, and the 6<sup>th</sup> day for the 22<sup>nd</sup> of January;
- etc.

Example 3:

The operations shall follow the **3 working days, 3 days-off, 3 working nights, 3 nights-off** schedule where operations may happen from 8:00 till 20:00 three days running with no operations next three days, then the operations are allowed from 20:00 till 8:00 next three days running with no operation the next three days: no holidays.

The schedule uses 12 schedule days.

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
8:00	20:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20:00	23:59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0:00	08:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

A specific value is set for each day. If it is deemed that in 2009, the working days after the New Year national holidays start from the 3<sup>rd</sup> of the January (that corresponds to the 1<sup>st</sup> day of the schedule), the schedule for January, 2009 has the following configuration:

- The 11<sup>th</sup> and 12<sup>th</sup> days are set for the 1<sup>st</sup> and the 2<sup>nd</sup> of January, respectively
- The 1<sup>st</sup> day is set for 3<sup>rd</sup> of January, the 2<sup>nd</sup> day for the 4<sup>th</sup> of January, the 3<sup>rd</sup> day for the 5<sup>th</sup> of January, the 4<sup>th</sup> of 6<sup>th</sup> of January, and the 5<sup>th</sup> day for 7<sup>th</sup> of January, the 6<sup>th</sup> day for 8<sup>th</sup> of January, the 7<sup>th</sup> day for 9<sup>th</sup> of January, and the 8<sup>th</sup> day for 10<sup>th</sup> of January, and the 9<sup>th</sup> day for 11<sup>th</sup> of January, and the 10<sup>th</sup> day for 12<sup>th</sup> of January, the 10<sup>th</sup> day for 12<sup>th</sup> of January, the 11<sup>th</sup> day for 13<sup>th</sup> of January, the 12<sup>th</sup> day for 14<sup>th</sup> of January

And further, in accordance with the **3 working days, 3 days-off, 3 working nights, 3 nights-off** schedule

- The 1<sup>st</sup> day for the 15<sup>th</sup> of January, the 2<sup>nd</sup> day for the 16<sup>th</sup> of January, the 3<sup>rd</sup> day for the 17<sup>th</sup> of January, the 4<sup>th</sup> day for the 18<sup>th</sup> of January, the 5<sup>th</sup> day for the 19<sup>th</sup> of January, and the 6<sup>th</sup> day for the 20<sup>th</sup> of January, the 7<sup>th</sup> day for the 21<sup>th</sup> of January, the 8<sup>th</sup> day for the 22<sup>nd</sup> of January, the 9<sup>th</sup> day for the 23<sup>rd</sup> of January; the 10<sup>th</sup> day for the 24<sup>th</sup> of January, the 11<sup>th</sup> day for the 25<sup>th</sup> of January, the 12<sup>th</sup> day for the 26<sup>th</sup> of January, etc.

Calendar

Month: January Year: 2009

MO	TU	WE	TH	FR	SA	SU
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

☐ RGLR ☐ 8  
☒ 1 ☐ 9  
☐ 2 ☐ 10  
☐ 3 ☐ 11  
☐ 4 ☐ 12  
☐ 5 ☐ 13  
☐ 6 ☐ 14  
☐ 7 ☐ HOL

It is clear that it will take long to redefine all 365 calendar days. To facilitate and expedite this, you can use the calendar tools:

**from:** // 15 **till:** // 15  
**Period:** 1 **Time Zone:**   
← →  
Fill Copy

Action Buttons:

Button	Action
<span>Copy</span>	Copies all calendar days from a time zone specified in the Time Zone field to a currently edited time zone: <b>Time Zone:</b> <span>Always</span>
<span>→</span>	Provides one day shift of the schedule to the right for the period between the points specified in the <b>from</b> and <b>till</b> fields: <sup>(*)</sup> <b>from:</b> <span>01/07/15</span> <span>15</span> <b>till:</b> <span>12/31/15</span> <span>15</span>
<span>←</span>	Provides one-day shift of the schedule to the left for the period between the points specified in the <b>from</b> and <b>till</b> fields: <b>from:</b> <span>01/07/15</span> <span>15</span> <b>till:</b> <span>12/31/15</span> <span>15</span>
<span>Fill</span>	Copies the values set for <b>X</b> days starting from Day <b>Y</b> , to all days of the period from <b>Y+X</b> date to <b>Z</b> date, where <b>X</b> is the number of days specified in the <b>Period</b> field, <b>Y</b> is the date specified in the <b>from</b> Field and <b>Z</b> is the date specified in the <b>till</b> field (usually it is the end of the year) <b>Period:</b> <span>4</span> <b>from:</b> <span>01/07/15</span> <span>15</span> <b>till:</b> <span>12/31/15</span> <span>15</span>

<sup>(\*)</sup>When the list of calendar days shifts to the right for the period of **X** days, it results in the following:

- Each day of the period (from the **second** to the last day) will have a value assigned to the preceding day
- The first day of the period will be set as **Regular Day**
- The values for the remaining days outside the period will stay unchanged.

For example, there is a list of calendar days with the first seven days set as '1', '2', '3', '4', '5', '6', '7'; if the period is defined from the 2<sup>nd</sup> to the 6<sup>th</sup> day and the shift of the period to the right is applied, the first seven days will have the following values: '1', Regular day, '2', '3', '4', '5', '7'.

(\*\*) For example, the list of calendar days has the following values for the days: 'Nrm', '1', '2', '3', '4', 'Nrm', 'Nrm', 'Nrm', 'Nrm', 'Nrm', and if the period is set from the 2<sup>nd</sup> day of the schedule till the end of the year, and after the **Fill** button is applied, the list of the days will have the following values assigned: 'Nrm', '1', '2', '3', '4', '1', '2', '3', '4', '1', '2', '3', '4', and so on till the end of the year.

Let's consider how to fill the list based on the above examples (Example 2 and Example 3)

Example 2:

The arming/disarming operations shall follow the **3 days over 3 days** schedule where the operations are allowed from 8:00 till 17:00 three days running with no arming/disarming operation for the next three days.

The schedule uses 6 days, plus Holiday.

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
8:00	17:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

A specific value is set for each day. If it is deemed that in 2009, the working days, after the New Year holiday season, start on January 11 (that corresponds to the 1<sup>st</sup> day of the schedule), the schedule for January, 2014 has the following configuration:



- Holiday is set for the dates of the 1<sup>st</sup> to the 10<sup>th</sup> of January
- The 1<sup>st</sup> day is set for 11<sup>th</sup> of January, the 2<sup>nd</sup> day for the 12<sup>th</sup> of January, the 3<sup>rd</sup> day for the 13<sup>th</sup> of January, the 4<sup>th</sup> of 14<sup>th</sup> of January, and the 5<sup>th</sup> day for 15<sup>th</sup> of January, and the 6<sup>th</sup> day for 16<sup>th</sup> of January



In other words, we set values for the first cycle of the **3 days over 3 days** schedule (6 days total) starting from the first day of the schedule.



Then, define the following values using calendar tools:

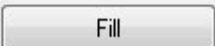
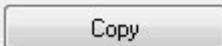
**from:** – '11.01.2009', (The first day of the schedule)  
**till:** – '31.12.2009', (The end of the year)  
**Period:** '6'. (The length of one schedule cycle)



from: 01/07/09  till: 12/31/09 




Period: 4  Time Zone: 

Days to be copied are highlighted in green.

Calendar




Month: January  Year: 2009  

MO	TU	WE	TH	FR	SA	SU
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

☒ RGLR ☐ 8  
☐ 1 ☐ 9  
☐ 2 ☐ 10  
☐ 3 ☐ 11  
☐ 4 ☐ 12  
☐ 5 ☐ 13  
☐ 6 ☐ 14  
☐ 7 ☐ HOL

Finally, click the **Fill in** button.

Calendar

Month: January  Year: 2009  

MO	TU	WE	TH	FR	SA	SU
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

☐ RGLR ☐ 8  
☒ 1 ☐ 9  
☐ 2 ☐ 10  
☐ 3 ☐ 11  
☐ 4 ☐ 12  
☐ 5 ☐ 13  
☐ 6 ☐ 14  
☐ 7 ☐ HOL

*The list of calendar days is adjustable for changes in the working schedules caused by holidays or other reasons.*

Example 3:

The arming/disarming operations shall follow the **3 working days, 3 days-off, 3 working nights, 3 days-off** schedule where operations may happen from 8:00 till 20:00 three days running with no operations for the next three days, then next three days, the operations are allowed from 20:00 till 8:00, and then no operation is allowed for the next three days: with no provisions for holidays.

The schedule uses 12 schedule days





Calendar

Month: January Year: 2009

MO	TU	WE	TH	FR	SA	SU
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

☒ RGLR ☐ 8  
☐ 1 ☐ 9  
☐ 2 ☐ 10  
☐ 3 ☐ 11  
☒ 4 ☐ 12  
☐ 5 ☐ 13  
☐ 6 ☐ 14  
☐ 7 ☐ HOL

Finally, click the **Fill in** button.

Calendar

Month: January Year: 2009

MO	TU	WE	TH	FR	SA	SU
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

☒ RGLR ☐ 8  
☐ 1 ☐ 9  
☐ 2 ☐ 10  
☐ 3 ☐ 11  
☒ 4 ☐ 12  
☐ 5 ☐ 13  
☐ 6 ☐ 14  
☐ 7 ☐ HOL

The list of calendar days is adjustable for changes in the working schedules caused by holidays or other reasons.

### 6.9.2 Time Zone for Access Control System (ACS)

This chapter focuses on differences between ACS time zones and IFS time zones. The major information on configuring a time zone is provided in chapter 6.9.1 Time Zone for Intrusion and Fire Systems (IFS).

ACS time zones are configured following the same way as for IFS time zones. But for the two fields of time period: Ent and Ex

Unlike IFS time zone, these fields are usable in ACS time zone:

Field	Possible Values	Description
<div>Ent</div>	<input checked="" type="checkbox"/> (checked), <input type="checkbox"/> (unchecked)	Attribute of time period activity for entry.  Default value: <input type="checkbox"/>
<div>Ex</div>		Attribute of time period activity for exit.  Default value: <input type="checkbox"/>

It is worth clarifying some points of ACS time zone logic:

- Centralized access control (networked):

- If centralized access control is used with one-way access point, it is necessary to define the attributes of entry or exit activity in accordance with the operating mode of that access point.

In other words, if one-way access door is used in the Entry mode, you should use a time zone with the **Entry** attribute of time zone activity. And vice versa, if one-way access door is used in the Exit mode, you should use a time zone with the **Exit** attribute of time zone activity.

(See, example 1 to this chapter.)

- Local access control (standalone):

- When local access control is provided using the S2000-2 controller, you cannot configure individual time zones for entry and exit. One access zone should be configured in accordance with a required logic.

(See examples 3 and 4 to this chapter.)

- When local access control is provided using the S2000-4 controller, you should keep in mind that no **Ent** and **Ex** fields are available for this device. Therefore, if local access control is provided using two S2000-4 controllers, and time for exit and entry are not the same, you must create two time zones: one for entry and another for exit.

(See example 5 to this chapter)

Please keep in mind, that if you use a time zone to lock down access or open free access via an S2000-2 controller in the local access control mode (i.e. at access level for Open or Lockdown codes (credentials), the **Ent** and **Ex** parameters define whether it is possible to open or lock down the access using Reader 1 (**Ent**) or Reader 2 (**Ex**).

The four examples below are helpful for the better understanding of the process of configuring access control time zones

### Example 1

The task is to configure a time zone for the centralized access control at a one-way access point with the **Exit** operating mode. Access is allowed from 7:30 till 17:30 from Monday till Thursday, and from 7:30 till 16:30 on Friday.

The time zones will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:30	17:30	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:30	16:30	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Example 2

The task is to configure a time zone for the centralized access control mode at a two-way access point. Access is allowed from 7:30 till 17:30 from Monday till Thursday, and from 7:30 till 16:30 on Friday.

The time zones will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:30	17:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:30	16:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Example 3

The task is to configure a time zone for the S2000-2-based local access control at a two-way access point. An entry is allowed from 7:30 till 8:00 with an exit from 17:00 till 17:30 from Monday till Friday.

The time periods will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:30	17:30	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:30	16:30	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Example 4

The task is to configure a time zone for a S2000-2-based local access control at two (2) one-way access points. The first access point allows an entry from 7:00 till 17:00 on Monday, Wednesday, and Friday but the second access point allows an entry from 7:00 till 17:00 on Tuesday, Thursday, and Saturday.

The S2000-2 controls the first one-way door with Reader1 (and Relay Output 1), i.e. as the **Entry** direction, and the second one-way door with Reader 2 (and Relay Output 2), i.e. as the **Exit** direction. Since it is impossible to have one time zone for Entry and another for Exit, a single time zone is created.

The time periods of such a time zone will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:00	17:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:00	17:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

These two time periods cannot be merged into a single period, for an access would be gained via both one-way access doors from Monday till Saturday.

#### Example 5

The task is to configure a time zone for a local access door at one two-way access point controlled by two S2000-4 devices. The entry access is allowed from 7:30 till 8:00 and the exit access is allowed from 17:00 till 17:00 from Monday through Friday.

Since that access control is based on two S2000-4 controllers, two time zones have to be configured.

The time slots of the first time zone will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:00	17:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The time slots of the second time zone will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:00	17:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### 6.9.3 Time Zones for Time and Attendance (T&A)

*This chapter focuses on differences between T&A and IFS time zones. The key information on configuring time zones is provided in Chapter 6.9.1 Time Zone for Intrusion and Fire Systems (IFS).*

*T&A time zones are configured in the same way as IFS time zones, but a user has to apply a different logic with T&A time zones.*

T&A time zone defines strict timelines of employees' working schedule.

The following two examples helpful for the better understanding of the process of T&A time zone configuration.

#### Example 1

An employee's working schedule is from 8:00 to 17:00 (with lunch from 12:00 -13:00) from Monday till Friday. The T&A time zone will have the following time periods:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
08:00	12:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13:00	17:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The employee may come to work earlier and leave it later, as well as he/she may have some breaks during the day. Therefore, the ACS time zone will allow entry and exits in a wider range than a standard working schedule.

For example, an employee is allowed to access from 7:30 till 17:30 from Monday till Friday. The ACS time zone will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
7:30	17:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Or, in case of a strict access rule where an employee is allowed an entry access from 7:30 till 8:00 and an exit access from 17:00 till 17:30 from Monday till Friday:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
7:30	08:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17:00	17:30	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Example 2

A guard has the following working schedule: two days from 8:00 till 20:00 (no lunch), two days-off, two days from 20:00 till 8:00 (no lunch), and two days-off. The T&A time zone will have strict timelines:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
7:30	20:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20:00	23:59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0:00	08:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The employee may come to work earlier and leave it later than the scheduled time, as well as he/she may have some breaks during the day. Therefore, the ACS time zone will allow entry and exits in a wider range than a working schedule.

For example, guard is allowed to access from 7:30 till 20:30 for two days running, then two days-off, then two working days from 19:00 to 8:00, and then two days-off.

The ACS time zone will be as follows:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
7:30	20:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19:30	23:59	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0:00	08:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

An employee can control (arm/disarm) IFS entities during the working time only. Therefore, the IFS time zone will have the following time slots:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
08:00	20:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20:00	23:59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0:00	08:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Thus, the T&A time zone is identical to the IFS time zone in this case.

## 6.9.4 Time Zones for Scenarios

*This chapter focuses on differences between time zones for scenarios and IFS time zones. The key information on configuring time zones is provided in Chapter 6.9.1 Time Zone for Intrusion and Fire Systems (IFS).*

*Configuration of a time zone to launch management scenarios follows the same logic as IFS time zones, but there are some differences in configuring a time zone for scenarios:*

1. The Type property has to be set as **Time Zone for Scenarios**
2. Time periods do not include the following fields: , ,  and .
3. There is the  field instead of those

Field	Possible Values	Description
<input type="text" value="Start at:"/>	'0:00'...'23:59'	Scenario start time. Default Value: '0:00'

Thus, time zone includes launch times of management scenarios instead of time periods.

The following two examples describe the process of time zone setting to launch management scenarios.

### Example 1

If an access lockdown scenario has to be launched every weekday (from Monday till Friday) at 18:00, the time zone for scenario launch would be as follows:

End	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
18:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Example 2

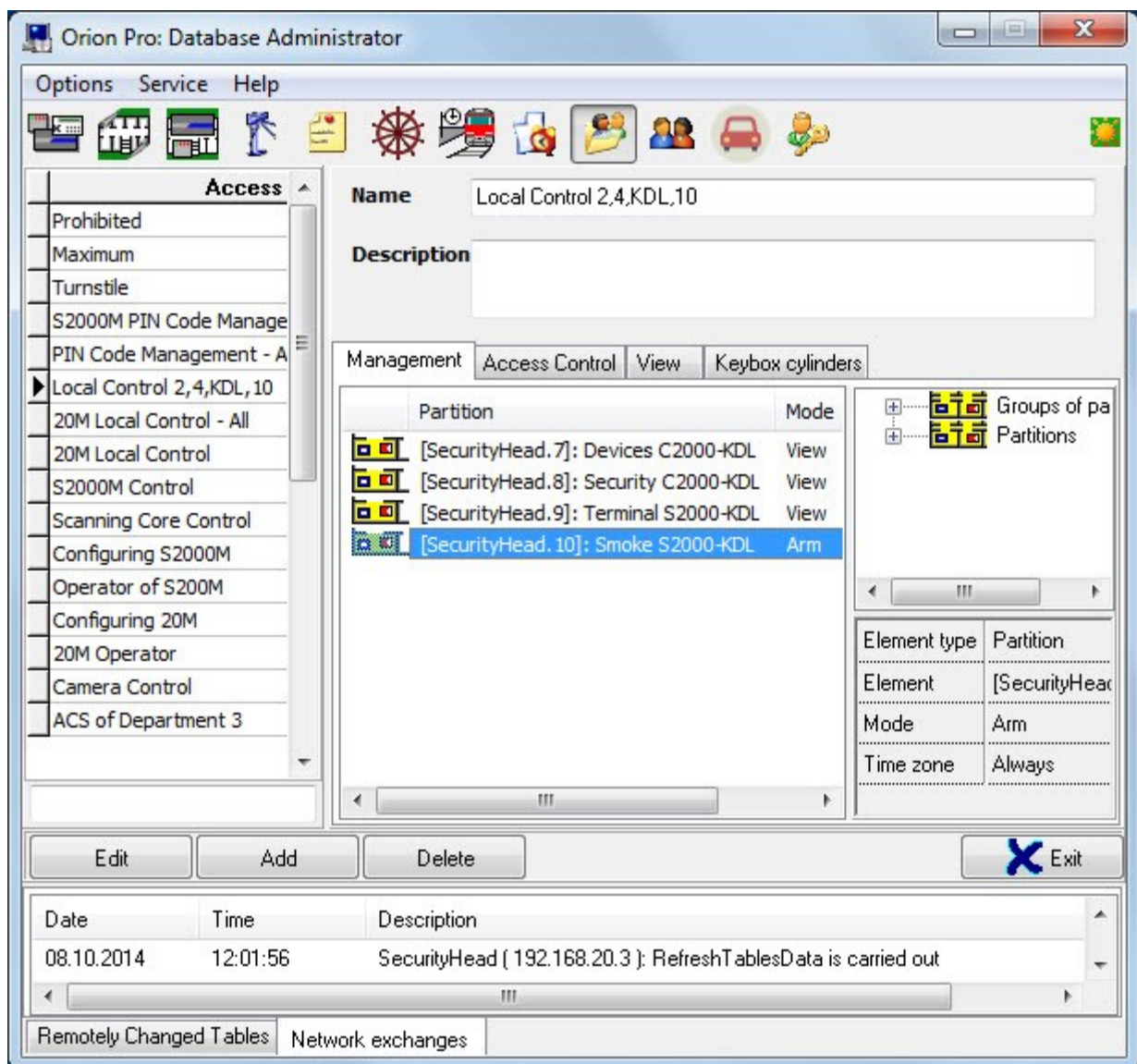
The requirement is to launch a room ventilation scenario every weekday (from Monday till Friday) at 7:00 and on weekends (Saturday and Sunday) at 12:30 (PM).

The launch times of time zone will be as follows:

End	Mo	Tu	We	Th	Fr	Sa	Su	8	9	10	11	12	13	14	Hol
07:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## 6.10 The Access Levels Tab. Creating Access Levels and Working Schedules



The Access Level tab displays the following:

1. The list of access levels
2. The properties of a selected access level.
3. The buttons to toggle between tabs:

Management — Toggles the **Management** tab (operation)

Access Control — Toggles the **Access Control** tab

View — Toggles the **View** tab,

Keybox cylinders — Toggles the Keybox cylinders.

4. The view area of the current tab of a selected access level.

The Access Levels tab is used to configure access levels to control IFS and ACS entities, as well as working schedules, and access levels (privileges) of System Monitor operators (SM operators):

- The IFS Access Level define when and what component of intrusion and fire system entities can be operated (armed/disarmed or activated) by an employee and what IFS entity's details an employee is eligible to receive
- The ACS Access Level defines when and what access zones (an access point) can be accessed by an employee.
- The Work Schedule defines when and what access zones can be attended by an employee
- SM Operator Access Level defines an operator's privileges - when and what IFS or ACS component is permitted to be controlled by an operator, and what system entity can be accessible for an operator in the System Monitor (SM Operator).

**Attention!**

- An IFS access level can be assigned (in the Credentials tab) to a PIN code, Touch Memory token, and Proximity card.
- An ACS access level is assigned (in the Credentials tab) to Touch Memory button, or Proximity card.
- A working schedule is assigned (in the Employees tab) to an individual or a team
- An SM Operator access level is assigned (in the Credentials) to software passwords

An employee can have two access levels, as a rule:

- A combined access level to operate with Intrusion & Fire Detection and Access Control system (or an access level to operate with ACS system)
- A work schedule

It is not efficient to create an individual access level for each employee. Access levels are generated for groups of employees with common features (e.g., originating from the same department)

Access Levels	
Prohibited	
Maximum	
Turnstile	
S2000M PIN Code Managemen	
PIN Code Management - All	
▶ Local Control 2,4,KDL,10	
20M Local Control - All	
20M Local Control	
S2000M Control	
Scanning Core Control	
Configuring S2000M	
Operator of S2000M	
Configuring 20M	
20M Operator	
Camera Control	
ACS of Department 3	

The list of access levels shows the following information:

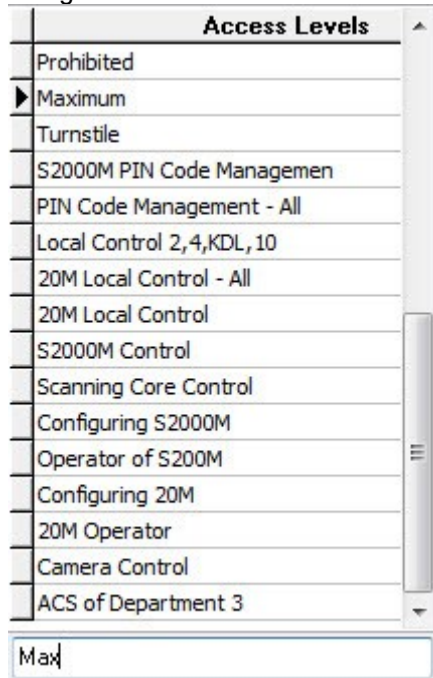
- The name of an access level

Prohibited

The bottom part of the list contains a search field to find an access level by a name:

Mar

When you start entering the name (case sensitive), it will move to the first item containing the characters being entered:

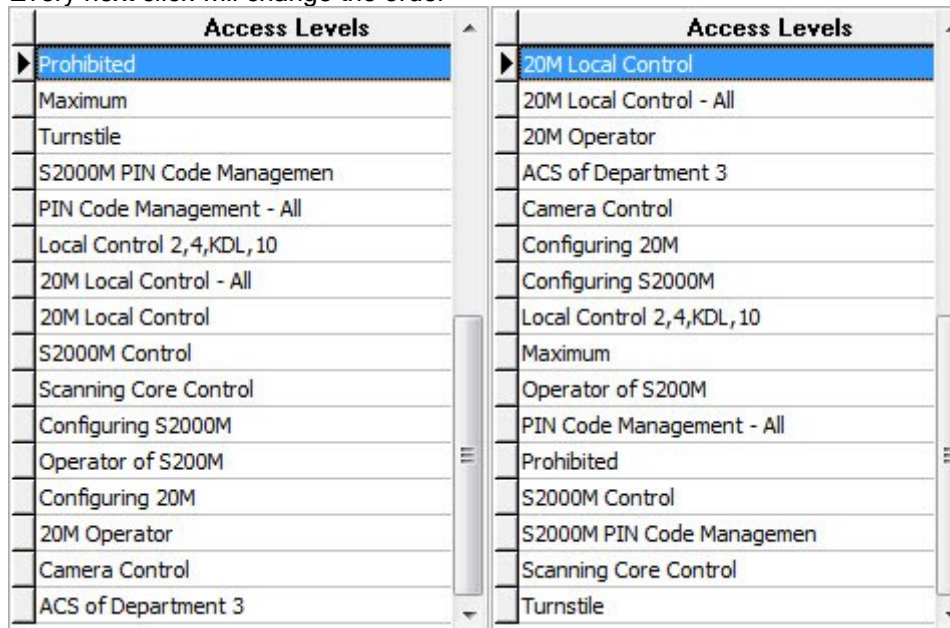


The access levels are arranged following the order they were added to the database of the Orion Pro software (i.e. in accordance with the ID identifier)

You can arrange the access levels by ID or by name

To change the order, please click the **Access Levels** column heading

Every next click will change the order





Further, the Guide will discuss how to configure IFS and ACE access levels, combined access levels, working schedules, and privileges for System Monitor operators, as well as access levels for handling partitions when keyboxes cylinders are removed / inserted.

This chapter focuses on the properties of access levels.

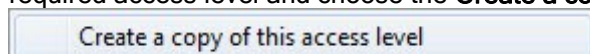
Properties of the Access Level entity:

**Name** Prohibited

**Description** Passage through doors and partition control are prohibited

Property	Possible Values	Description
<b>Name</b>	A length of 1 to 25 characters	Access level name Default value: empty field
<b>Description</b>	A length of 0 to 200 characters	Comments <i>This field is optional.</i> Default value: empty field

Attention! If necessary, you can create a copy of an access level. To do that, please right-click on a required access level and choose the **Create a copy of this access level** item in the contextual menu:



The copy of the access level will be created with '**Copy of**' added to the name of the copied access level:

Operator

Copy of Operator

By default, there are two access levels in the Orion Pro Suite: Prohibited (Banned) and Maximum. These default levels cannot be modified and deleted.

The Prohibited (Banned) level prevents any operations with IFS and ACS entities.

The Maximum level gives rights to control and operate all IFS entities and access all access points at any time. (\*)

*(\*) The Maximum level cannot be used for local combined tokens/cards stored in the S2000-2 and S2000-4 controllers. To achieve this purpose, you have to create a new access level.*

To add a new access level, please:

- Click the **Add** button.
- Enter values in the **Name** and **Description** fields of the new Access Level entity.
- Configure an access level to perform one of the following tasks:
  - Operate the Intrusion and Fire System
  - Manage the Access Control System
  - Monitor the Intrusion and Fire System, and the Access Control Systems
  - Use Working Schedules
  - Manage and use Operator Privileges
- Click the **Save** button

To modify the Access Level entity, please select a required access level in the list of access levels and click the **Edit** button. Then, make necessary changes and click the **Save** button.

To delete the Access Level entity, please select a required access level in the list of access levels, and click the **Delete** button. Then, click **Yes** to confirm the action.

## 6.10.1 Configuring Access Levels of Intrusion and Fire System

This chapter describes how to configure access levels related to the entities of intrusion and fire protection system: partitions and partition groups.

Please be advised, that access levels include permission and rules to control (arm, disarm or activate) IFS entities. But you also have to define a reader and IFS entities to be controlled by this reader (in other words, link IFS entities to the readers of system controllers)

*How to link partitions and partition groups is described in Chapter 6.4.3. Associating Control Elements to System Readers.*

Other points to consider are as follows:

- A PIN code may be used to control multiple IFS entities
- Only one IFS entity - one partition or partition group - can be controlled using a Touch Memory token or Proximity card as applied to one reader of S2000-2, S2000-4, Signal-20P, Signal 10, S2000 KDL, S2000-KDL-2I, S2000-KDLS, S2000-BI, or UO-4S
- If you have to operate multiple IFS entities using a Touch Memory token or Proximity card you can control such entities using multiple different readers - one reader is for each entity (partition or partition group).

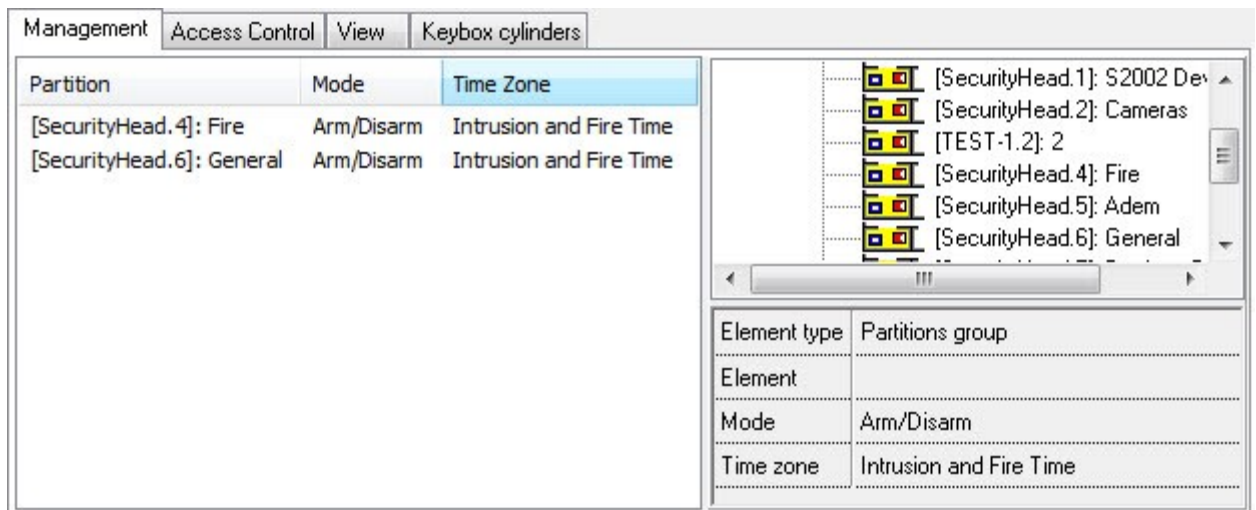
The following logic is used to control IFS entities in the Orion Security System:

- When the Orion Pro software is used as a network controller to provide the centralized control of IFS entities, each entity can have an associated time zone during which the operations with the entity will be allowed. In Orion Pro, this logic is used for the Orion protocol.
- When the S2000M device is used as a network controller to provide the centralized control of IFS entities, it is impossible to make that each entity has an associated time zone during which the operations with this entity will be allowed. In the Orion Pro software, this logic is used for the Orion Pro protocol.
- When system devices are controlled locally (Stand-alone mode):
- The S2000-2 and S2000-4 controllers can have associated time zones to allow a user to operate entities (arming/disarming, activating, gaining access) within this time zone.
- The Signal-10, Signal-20M, S2000-KDL, S2000-KDL-2I, S2000-KDLS and UO-4S cannot have associated time zones to permit user actions with entities.

*The Orion Pro system supports the storing credentials in the S2000-2, S2000-4, and Signal-10. If you need a local control for Signal-20M, S2000-KDL, S2000-KDL-2I, S2000-KDLS, and UO-4S, you have to use the Uprog utility.*

*Attention! To add the zone operation rights to the S2000-2, S2000-4, or Signal-10, please create a partition with device zones only and add this partition to the access level.*

*All permissions to operate (access) IFS entities are set in Management tab of the Access Tab.*

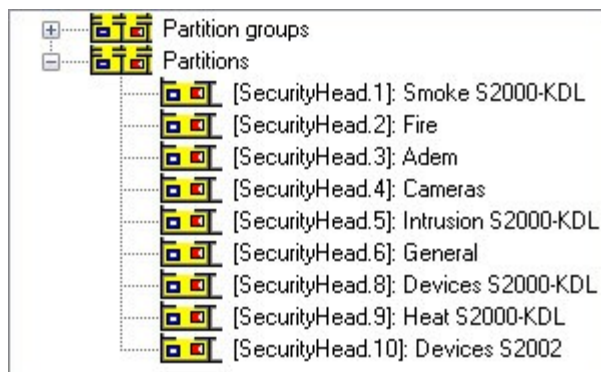


This tab shows the following information:

- The list of IFS entities added to the access level:

	Partition	Mode	Time Zone
	[SecurityHead.2]: Fire	Arm/Disarm	IFS Time Zone
	[SecurityHead.6]: General	Arm/Disarm	IFS Time Zone

- The tree of partitions and partition groups:




- Permissions to operate an entity selected on the list of IFS entities:

Element type	Partition
Element	[SecurityHead.6]: General
Mode	Arm/Disarm
Time zone	Intrusion and Fire Time

The list of IFS entities of the access level shows the following information:

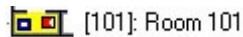
- Element type:
  - – Partition

-  Partition group (Groups of partitions),
- 
- Number
- Name
- Mode
- Time Zone



The tree of partitions and partition groups shows the following information:

- Number
- Name



To add a new entity to an IFS access level, please do the following:

- click the **Edit** button and select an entity you want to add
- double click or drag it to the list of the access level's IFS entities
- define privileges to handle and the entity

You can add all partitions or all partition groups to the IFS access level. To do that, please double click the Partitions node or Partition Group node, or drag a required node to the list of the access level's IFS entities.

To change the entity handling privileges, please enter the editing mode (**Edit**):

- Select a required entity on the list of the access level's IFS entities
- Make necessary changes into the privileges to operate the entity

To delete entity from the list, please go into the Editing mode (**Edit**), then:

Select a required entity from the access level's list of entities

Press the **Del** key on the keyboard, and then confirm the action in the dialog box:

See below the attributes of an entity privileges:

Element type	Partition
Element	[SecurityHead.6]: General
Mode	Arm/Disarm
Time zone	Intrusion and Fire Time

Property	Possible Values	Description
Element type	Partition Partition group	Element type. <i>It is not recommended modifying this attribute.</i>
Element	All partitions, <i>One of the system partitions</i> All partition groups <i>One of the partition groups</i>	One of the IFS entities: partition, partition group, all partitions or all partition groups <i>It is not recommended modifying this property</i>
Mode	View Arming Disarming Arming/Disarming	Permissions and rules applicable to an entity <ul style="list-style-type: none"> <li>• View (one can only view an entity )</li> <li>• Arming (one can only arm an entity with no permission to disarm)</li> <li>• Disarming (one can only disarm an entity with no permissions to arm)</li> </ul>

		<ul style="list-style-type: none"> <li>Arming/Disarming (one can arm and disarm an entity)</li> </ul>
Time zone	<i>One of the time zones</i>	A time zone within the selected entity that can be subjected to the above control operations (or accessed by a user)

**Attention!** Since an access level can include control rights (permissions and rules) applicable both to partitions and partition groups, the following rule takes place: the **Partition** entity added to an access level has priority over the **All partitions** entity added to the same access level. But the **Partition group** entity added to an access level has priority over the **All partition groups** entity of the same access level.

Let's consider some examples.

### Example 1

The task is to establish configurations to control five partitions using a PIN-code for S2000-K keypad within the Orion Pro protocol.

All five partitions are added to an access level:

Partition	Mode	Time Zone
[SecurityHead.7]: Devices C2000-KDL	Arm/Disarm	Always
[SecurityHead.8]: Security C2000-KDL	Arm/Disarm	Always
[SecurityHead.9]: Terminal S2000-KDL	Arm/Disarm	Always
[SecurityHead.10]: Smoke S2000-KDL	Arm/Disarm	Always
[SecurityHead.6]: General	Arm/Disarm	Always

These five partitions are associated with the reader of an S2000-K device:



### Example 2:

The task is to configure control of two partitions using a touch memory button (i-button) and a S2000-BKI device under the Orion protocol with arming operations allowed at one time and disarming at another time.

Each partition can be added twice to an access level with proper settings of permissions and time zones:

Management	Access Control	View	Keybox cylinders
	Partition	Mode	Time Zone
	[SecurityHead.1]: S2002 Devices	Arm	Time Zone to Operate 1
	[SecurityHead.1]: S2002 Devices	Disarm	Time Zone to Operate 2
	[SecurityHead.2]: Cameras	Arm	Time Zone to Operate 1
	[SecurityHead.2]: Cameras	Disarm	Time Zone to Operate 2

Partitions will be associated to the reader of a S2000-BKI device:



It is quite clear that such logic cannot be implemented under the Orion Pro protocol, when control function belongs to S2000M panel that does not support time zones.

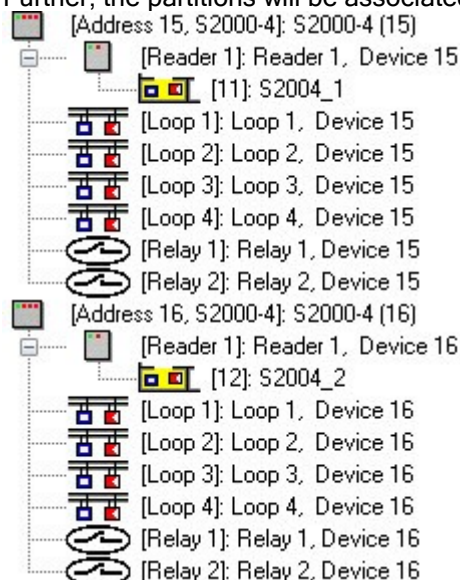
### Example 3

The task is to configure control of two partitions using a Touch Memory button and two S2000-4 devices where each partition is controlled (armed/disarmed) with its dedicated device

Two partitions will be added to the access level:

Management	Access Control	View	Keybox cylinders
Partition	Mode	Time Zone	
[SecurityHead.11]: S2004_1	Arm/Disarm	Always	
[SecurityHead.12]: S2004_2	Arm/Disarm	Always	

Further, the partitions will be associated with the readers of the S2000-4 devices:



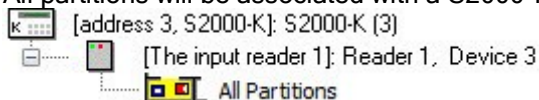
### Example 4

The task is to make a configuration where a Pin-code will be used for an S2000-K keypad to control all partitions except one that can be viewed only.

The access level will include the **All partitions** entity and a required partition:

Management	Access Control	View	Keybox cylinders
Partition	Mode	Time Zone	
All Partitions	Arm/Disarm	Always	
[SecurityHead.5]: Adem	Arm/Disarm	Always	

All partitions will be associated with a S2000-K keypad, where the keypad is configured as a reader:



Finally, if you have to export database data to the S2000M panel, please be advised that:

- This panel does not support time zone - operations with an entity can be always banned or allowed.
- The panel limits the number of access levels as well as the number of access levels that can be included in one specific partition:

Panel	The maximum of access levels	The maximum access levels in one partition
S2000 ver 1.20-1.24	252	8
S2000M ver 2.01-2.05	252	8



## 6.10.2 Configuring Access Levels for Access Control System

This para discusses how to configure an access level for an access control system (ACS).

The access level is used to set permissions and rules to control access entities (Access Points). In addition, one also has to define an access point to control and what readers to be use for that (i.e. to associate an access point with the readers of the system devices).

When an access point is created, it is automatically associated to appropriate readers.

The Orion Integrated Security System uses the following logic for access control system:  
The access control can be local (credentials data are stored in devices), or centralized (credentials data are stored in the database)

*Attention! Biometric readers support local control only.*

The centralized control can be organized only if the Orion Pro Suite is used as a network. The S2000/S2000M panel cannot be used as a network controller.

The centralized control may be enabled in the Orion and Orion Pro protocols.

*Attention! The S2000M ( ver 2.04 or higher) has to be used to ensure the centralized access control under the Orion Pro protocol.*

*The S2000 panel (all versions), and the S2000M panel (versions of 2.01 to 2.03) cannot be used for centralized access control under the Orion Pro protocol.*

Permissions for the access control systems are set in the Access Control tab.

Rules and permissions for access control implementation are defined in the Access Control tab:




Access Point/Zone	Mode	Time Zone
[0]: Outside World	Passage	Always
[2]: Canteen	Passage	Always
[5]: Door5	Passage	Always

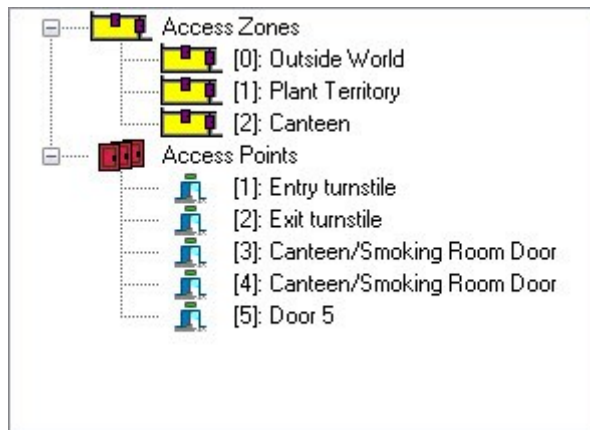
Element type	Access zone
Element	[0]: Outside World
Mode	Passage
Time zone	Always
Antipassback	None
Two-person rule confirmation	None
Three-person rule confirmation	None
Confirming	None
Confirm by button	None

This tab shows the following information:

- The list of ACS entities added to the access level:

	Access Point/Zone	Mode	Time Zone
	[0]: Outside World	Passage	Always
	[2]: Canteen	Passage	Always
	[5]: Door5	Passage	Always






- The tree of access zones and access points:



- Permissions and rules for the ACS entity selected in the access level:

Element type	Access zone
Element	[0]: Outside World
Mode	Passage
Time zone	Always
Antipassback	None
Two-person rule confirmation	None
Three-person rule confirmation	None
Confirming	None
Confirm by button	None

The list of ACS entities added to the access level includes the following information:

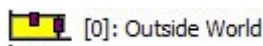
- Operating mode as graphically represented (only for access points):
  - Passage –no icons
  - Entry – 
  - Exit – 
  - Entry/Exit – 
- Type:
  -  –Access Zone
  -  –Access Point
- Number (ID)
- Name
- Mode
- Time Zone

 [1]: Entry turnstile      Enter/Exit      Always



The tree of access zones and access points shows the following information for each entity:


- Number
- Name



[0]: Outside World

To add a new entity to the access level, please go into the editing mode, then:

- Select a required entity in the tree of access zones and access points
- Double click the entity or drag it to the list of ACS entities of the access level
- Define permissions and rules for the entity functioning.

You can add all access zones (  All Access Zones ) or all access points to the access level's list of ACS entities. To do that, please double click the Access Zones node or Access Points node or drag it to a required entity in the list of ACS entities.

To change permissions and rules of access control entity, please enter the editing mode and:

- Select a required element in the list of ACS entities of the access level, and
- Make changes you want.

To delete an entity from the access level, please enter the editing mode, then:

- Select a required entity in the tree of access zones and access points
- Press the <Del> key on the keyboard, and confirm the deletion by clicking **Yes** in the emerging dialog box:

Let's discuss the permissions and rules for the entity operations;

Element type	Access zone
Element	[0]: Outside World
Mode	Passage
Time zone	Always
Antipassback	None
Two-person rule confirmation	None
Three-person rule confirmation	None
Confirming	None
Confirm by button	None

Properties	Possible Values	Description
<b>Element type</b>	<b>Access Zone</b> <b>Access Points</b>	Element type It is not recommended modifying this property
<b>Element</b>	<b>All Access Zones</b> <i>One of the access zones</i> <b>All Access Points</b> <i>One of the access points</i>	One of the ACS entities: an access point, access zone, all access points and all access zones It is not recommend modifying this property.
<b>Mode</b>	<b>Passage</b> <b>Entry</b> <b>Exit</b> <b>Entry/Exit</b>	Rules applicable to the operation of an access control entity including Access Point: <ul style="list-style-type: none"> <li>• <b>Passage</b> (allows access through the following: <ul style="list-style-type: none"> <li>○ One-way access point</li> <li>○ Two way access point (in both direction)</li> </ul> </li> </ul>

		<ul style="list-style-type: none"> <li>• <b>Entry</b> (allows access through the following access points): <ul style="list-style-type: none"> <li>○ One-way access points working in the <b>Entry</b> operating mode</li> <li>○ Two-way access points working in the <b>Entry</b> operating mode),</li> </ul> </li> <li>• <b>Exit</b> (allows access through the following access points): <ul style="list-style-type: none"> <li>○ One-way access points working in the <b>Exit</b> operating mode</li> <li>○ Two-way access points working in the <b>Exit</b> operating mode),</li> </ul> </li> <li>• <b>Entry/Exit</b> (allows access through two way access points in both directions). The Access Zone entity may have the following value only: <ul style="list-style-type: none"> <li>• <b>Passage</b> (used to allow access through all access points in both directions).</li> </ul> </li> </ul>
<b>Time Zone</b>	<i>One of the time zone of the system</i>	Time zone allowing access through an access point in accordance with a defined mode.
<b>Anti-passback</b>	<b>None</b> <b>Hard</b> <b>Timed</b> <b>Soft</b>	Define whether the anti-passback will be used to control access to an access zone <i>(See comments 2 to the table )</i>  <i>This attribute is not accessible for the access points operating in the <b>Passage</b> mode</i>
<b>Anti-Passback Lockout Period</b>	'0:00'...'23:59'	Timed anti-passback lockout time <i>(See comments 2 to the table)</i>  <i>This parameter is accessible only for those access points and zones where the <b>Anti-pass-back</b> property is set as <b>Timed</b>.</i>
<b>Two-person rule confirmation</b>	<b>None</b> One of the access levels used your system	Access level to gain access in accordance with a <i>Two-person rule confirmation</i> (in other words, access is granted as response to two different credentials with appropriate access levels)  <i>(See Note 4 to this table)</i>
<b>Three-person rule confirmation</b>	<b>None</b> , <i>One of the access levels used in your system</i>	Access level to gain access in accordance with <b>Three-person rule confirmation</b> (in other words, the access is granted as response to two different credentials with appropriate access levels)  <i>(See Note 4 to this table)</i>
<b>Confirming</b>	<b>Yes /No</b>	Defines whether the access level is confirming for access in accordance with Two (three)-person rule <i>( See Note 4 to this table)</i>
<b>Zonal anti-passback</b>	<b>Yes/No</b>	Defines whether the zonal anti-passback parameter is to be used to control access to this access zone or not.  <i>(See Note 3 to this table)</i>  <i>This parameter is accessible for an access zone and access points that have any value expect for <b>None</b> for the Anti-passback parameter</i>

Note 1

**Attention!** Since an access level can include permissions and rules applicable both to access zones and access points, the following rule shall apply: the **Access Point** entity added to an access level has the priority over the **All Access Points** entity added to the same access level. The **Access Zones** entity added to an access level has priority over the **All Access Zones** entity of the same access level. The **Access Point** of the access level has priority over the **Access Zone** added to the same access level.

The prioritized list of entities as per their access level is as follows:

- Access Point (the highest priority)
- All Access Points
- Access Zone
- All Access Zones (the lowest priority)

## Note 2

Let's consider the anti-passback rule.

If access is controlled locally, antipassback applies to access points controlled by a S2000-2 controller. If access control is centralized, *anti-passback* is implemented for access points controlled by S2000-2 and S2000-4 controllers.

An antipassback rule is regarded as violated if an entry to access zone **X** was not followed by an entry to another access zone while a re-entry to zone **X** is attempted

Anti-passback can be implemented as follows:

- None (anti-passback rule is ignored)
- Hard Anti-Passback
- Soft Anti-Passback
- Timed Anti-Passback.

**Hard anti-passback** prevents a re-entry to the same access zone until an exit from this zone is recorded. When an antipassback rule is breached, no access is granted, and the **Access Denied** message is generated.

**Soft anti-passback** allows re-entry but generates the **Access Granted** and **Passage** messages accompanied by the **anti-passback breach** tag.

**Timed anti-passback** uses an additional parameter - **Anti-Passback Lockout Period**. During this period after an entry to an access zone, a timed anti-passback rule applies in the same manner as hard anti-passback does (if a re-entry is attempted, a controller denies access and generates the **Access Denied** message accompanied by the **anti-passback breach** tag). When this period expires, timed anti-passback is identical to soft antipassback (a re-entry is allowed but the **Access Granted** and **Passage** messages are generated with the **anti-passback breach** tag).

If anti-passback applies to a locally controlled device, the anti-passback is *called local anti-passback*.

In the system, network anti-passback is implemented. If a controlling unit is available (S2000/S2000M or Scanning Core), access messages will be re-transmitted to all access controllers in the system. Thus, the anti-passback rule is verified taking into account entries to the access zone, as registered by all controllers of the system (within one workstation)

Therefore, if an access zone has several access points (for example, several checkpoints, or lanes of turnstiles), after one enters this access zone via one access point, the re-entry to this zone will be banned (locked) at this access point and all other access points as well, but the exit will be allowed; and vice versa, if a person exits from this area via one access point, the attempts to exit from this area will be banned (locked) at all other access points as well, but the entry will be allowed (if an anti-passback rule applies to the access credentials).

## Note 3

The anti-passback rule will be tighter, if the **zonal anti-passback** parameter is applied (Tracking). In this case, the system analyzes entries to any access zone, and if access is attempted via one of the readers of an access point, anti-passback requires that the last registered access will be associated with the access zone where the reader is located, i.e. with the zone controlled by a second reader of this access point.

For example, we have a two-reader access point located on the boundary between Access Zone 1 and Access Zone 2. First, access to Zone 2 is registered, and then access to Access Zone 3 (controlled by a different access point) is registered, the further attempt to go through the access point between Access Zone 1 and Access Zone 2 will result in the following:

- If zonal anti-passback mode is enabled, the anti-passback rule would be breached regardless of an access (passage) direction, as the last-recorded access (passage) happened at another zone rather than at Access Zone 1 and Access Zone 2, and the user's actual stay in one of these zones is regarded as a breach;
- If no zonal anti-passback is used, the anti-passback rule would not be breached if an access is attempted to Access Zone 1, but it would be breached if an access is attempted to Access Zone 2, since, with respect to this access point, the user is still in Access Zone 2 (the user's entry to Access Zone 3 is ignored by the access point).

The Zonal anti-passback parameter is effective, only if any one of the **Hard**, **Soft**, or **Timed** anti-passback modes is enabled. If the anti-passback is disabled, the Zonal anti-passback parameter does not apply. Zonal anti-passback applies to two-way access points only.

Zonal antipassback applies to two-way access points.

*If a centralized access control mode is used along with anti-passback, two-way access points always use the zonal anti-passback features.*

#### **Note 4**

Let's consider two (three)-person rule confirmation.

In this mode, the system functions in the following manner:

If the access level of a presented credential includes an access mode based on a two/three-person rule, the **User Authentication** event (**USER'S CODE ENTRY**) is generated, a green LED starts 5-Hz flashing and a controller waits for 30 sec till another credential(s) is authenticated with an access level confirming the first produced credential. If a second credential has an appropriate access level but access granting requirements have not been met yet (a three-person rule access), the **User Authentication** event is generated again and the controller waits for a third credential to be submitted within 30 seconds.

If the second and third credentials meet granting access requirements for one of the submitted credentials at least, the access will be granted.

#### *Attention!*

*The two/three person rule is applicable to the main credentials only. The two/three person rule does not work with credentials used to enable **Free Access** or **Locked Access** modes.*

*Two/three person rule for local access control is supported by S2000-2 devices*

*Please see some examples below*

#### **Note 5**

In this mode the system works in the following way:

If the access level of a presented credential includes **Confirm by button** mode, the User Authentication event will be generated, a green LED starts 5-Hz flashing and a controller waits for 20 sec till access button is pressed confirming access of the presented credential to a requested zone

Let us discuss some examples

#### **Example 1**

The task is to provide access through two passage-type access points at any time.



See some properties of the two access points:

Number	3	Number	5
Name	Canteen/Smoking Room Door	Name	Door5
Description		Description	
Type	Turnstile	Type	Two-way access door
Operating mode	Entry	Operating mode	Entry/Exit
Access zone to enter	[2]: Canteen	Access zone to enter	[No]
Entry relay		Entry relay	[SecurityHead.1.6.1]: Relay 1, Device 6
Entry relay action	ON		
Entry relay action time	5		

The access points will run without route tracking features (**Passage** mode) and have the following access control settings:

- First, add the access points to the list of ACS entities of the access level.
- Next, please define the following for the properties of the access points:
  - Set the **Passage** value for the **Mode** property
  - Define a time zone (**Time Zone**'s field) allowing access via the selected access points

The access level for the considered example will be as follows:

	Access Point/Zone	Mode	Time Zone
	[3]: Canteen/Smoking Room Door	Passage	Always
	[5]: Door5	Passage	Always

Element type	Access Point	Element type	Access Point
Element	[3]: Canteen/Smoking Room Door	Element	[5]: Door5
Mode	Passage	Mode	Passage
Time zone	Time Zone for Managers	Time zone	Time Zone for Managers
Antipassback	None	Antipassback	None
Two-person rule confirmation	None	Two-person rule confirmation	None
Three-person rule confirmation	None	Three-person rule confirmation	None
Confirming	None	Confirming	None
Confirm by button	None	Confirm by button	None

## Example 2

The task is to provide access through two access points within the period defined in **Time Zone for Managers** and an anti-passback rule applied.

See some properties of the above access points:



Number	1	Number	2
Name	Turnstile 1	Name	Turnstile2
Type	Turnstile	Type	Turnstile
Operating mode	Entry/Exit	Operating mode	Entry/Exit
Access zone to enter	[1]: Plant Territory	Access zone to enter	[1]: Plant Territory
Accessed zone to exit	[0]: Outside World	Accessed zone to exit	[0]: Outside World

When configuring an access level for access points with route direction tracking, it makes sense to include access zones (instead of access points) into access level description where access is provided through assigned access points

In other words, the access level for such access points will have the following configuration:





- Existing access zones ( where access points provide access) will be added to the access level
- The properties of the added access zones will have the following settings:
  - Mode** is set as **Passage** by default and cannot be modified
  - Time Zone** includes the time zone that allows access through the selected access points.

The access level for the considered example will be as follows:

Management	Access Control	View	Keybox cylinders
Access Point/Zone		Mode	Time Zone
	[0]: Outside World	Passage	Time Zone for Managers
	[1]: Plant Territory	Passage	Time Zone for Managers

Element type	Access Zone	Element type	Access Zone
Element	[0]: Outside World	Element	[1]: Plant Territory
Mode	Passage	Mode	Passage
Time Zone	Time Zone for Managers	Time Zone	Time Zone for Managers
Antipassback	Hard	Antipassback	Hard
Two-Person Rule Confirm	None	Two-Person Rule Confirm	None
Three-Person Rule Confir	None	Three-Person Rule Confir	None
Confirming	None	Confirming	None
Zonal Anti-Passback	None	Zonal Anti-Passback	None
Confirm by button	None	Confirm by button	None

If you want to allow access through the points described in Example 1 and within the **Time Zone for Managers** time zone, the access level will be as follows:

Access Point/Zone	Mode	Time Zone
 [0]: Outside World	Passage	Time Zone for Managers
 [1]: Plant Territory	Passage	Time Zone for Managers
 [3]: Canteen/Smoking Room Door	Passage	Time Zone for Managers
 [5]: Door5	Passage	Time Zone for Managers

### Example 3

It is worth mentioning that sometimes it is a specific access point with tracking mode that you have to add to an access level, rather than access zones.

For example:

- When you want to provide and access through a two-way access point operating in a route direction tracking mode and controlled by two S2000-4 controllers with different time settings for entry and exit.
- When you need to provide access to the same zone but through different access points at a different time.

Let's consider an example. The access is required through access points controlled by S2000-2 devices:

- Through two access points (Turnstile 1 and Turnstile 2) at a time specified in the **Time Zone for Managers** with a hard anti-passback option

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su
07:30	17:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:30	16:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Through the Turnstile 3 access point at the time defined in **Time Zone Hard** a hard anti-passback

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su
7:30	17:30	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7:30	16:30	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16:00	16:30	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>




See some properties of the above access points providing entry to access zones:

Number	1	Number	2
Name	Turnstile 1	Name	Turnstile2
Type	Turnstile	Type	Turnstile
Operating mode	Entry/Exit	Operating mode	Entry/Exit
Access zone to enter	[1]: Plant Territory	Access zone to enter	[1]: Plant Territory
Accessed zone to exit	[0]: Outside World	Accessed zone to exit	[0]: Outside World

Number	3
Name	Turnstile 3
Type	Turnstile
Operating mode	Entry/Exit
Access zone to enter	[1]: Plant Territory
Accessed zone to exit	[0]: Outside World

The access level for this example will be as follows:

No access level for this example will be as follows:

Management	Access Control	View	Keybox Cylinders
	Access Point/Zone	Mode	Time Zone
	[0]: Outside World	Passage	Time Zone for Managers
	[1]: Plant Territory	Passage	Time Zone for Managers
	[3]: Turnstile 3	Entry/Exit	Time Zone Hard

Element type	Access Zone	Element type	Access Zone
Element	[0]: Outside World	Element	[1]: Plant Territory
Mode	Passage	Mode	Passage
Time Zone	Time Zone for Managers	Time Zone	Time Zone for Managers
Antipassback	Hard	Antipassback	Hard
Two-Person Rule Confirmation	None	Two-Person Rule Confirmation	None
Three-Person Rule Confirmation	None	Three-Person Rule Confirmation	None
Confirming	None	Confirming	None
Zonal Anti-Passback	None	Zonal Anti-Passback	None
Confirm by button	None	Confirm by button	None

Element type	Access Point
Element	[3]: Turnstile 3
Mode	Enter/Exit
Time Zone	Time Zone Hard
Antipassback	Hard
Two-Person Rule Confirmation	None
Three-Person Rule Confirmation	None
Confirming	None
Zonal Anti-Passback	None
Confirm by button	None


#### Example 4

The task is to configure access at the time described in the Time Zone for **Accounts Department**. **Entry** is to be acknowledged by an entrance post guard (two-person rule) and **Exit** is a conventional access mode.


See some properties of the above access point:

Number	5
Name	Paying Office Door
Type	Two-way access door
Operating mode	Entry/Exit
Access zone to enter	[5]: Paying Office
Accessed zone to exit	[4]: Accounts Departments



The guard's access level (ACS for Guards) will include the following entity:


Management	Access Control	View	Keybox Cylinders
	Access Point/Zone	Mode	Time Zone
	[5]: Paying Office Door	Entry	Accounts Department



Element type	Access Point
Element	[5]: Paying Office Door
Mode	Entry
Time Zone	Accounts Department
Antipassback	None
Two-Person Rule Confirmation	None
Three-Person Rule Confirmation	None
Confirming	Yes 
Confirm by button	None

The access level of a Paying Office employee will have the following entities:

Management	Access Control	View	Keybox Cylinders
	Access Point/Zone	Mode	Time Zone
	[5]: Paying Office Door	Entry	Accounts Department
	[5]: Paying Office Door	Exit	Accounts Department

Element type	Access Point	Element type	Access Point
Element	[5]: Paying Office Door	Element	[5]: Paying Office Door
Mode	Entry	Mode	Exit
Time Zone	Accounts Department	Time Zone	Accounts Department
Antipassback	None	Antipassback	None
Two-Person Rule Confirmation	ACS for Guards 	Two-Person Rule Confirmation	None
Three-Person Rule Confirmation	None	Three-Person Rule Confirmation	None
Confirming	None	Confirming	None
Confirm by button	None	Confirm by button	None

The access levels of a guard and paying office employee described above may include access zones rather than access points, depending on a system configuration.

### 6.10.3 Combined Access Levels

The above chapters discuss how to configure access levels of IFS and ACS systems. It is clear that individual access levels for IFS or ACS are used rarely (usually if either IFS or ACS system is used at a site)

With IFS and ACS applications, an individual may be provided with the following:

Deferent access levels for IFS and ACS, if

- operations with ACS and IFS entities are performed using multiple tokens or/and pin-codes
- One access level for both ACS and IFS entities is used:
  - If operations with IFS entities are performed using PIN-codes, and tokens are used to work with ACS entities.
  - If operations with IFS and ACS are performed using one token (ibutton or card)

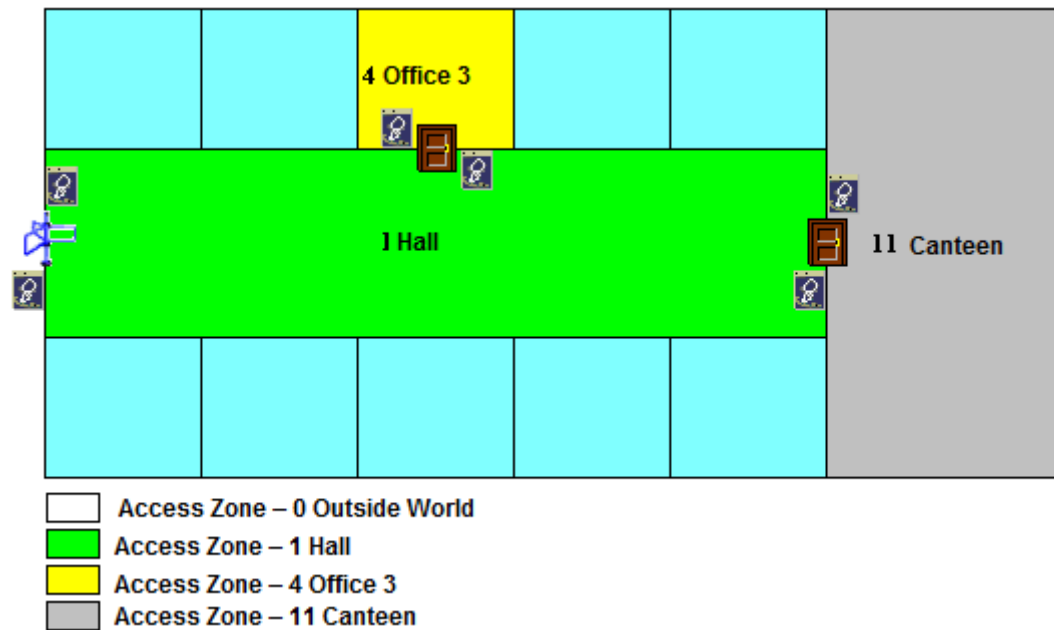
Since, an employee most likely has one token (Touch Memory button or Proximity card), and one PIN code, if necessary, only one access level is created for such an employee to perform actions with IFS and ACS entities.

An access level that includes permissions and rules to operate both IFS entities and ACS entities are called **Combined**.

Let's discuss the following case as an example of a combined access level.

Example of an access level:

There is a protected site with the following structure:



The protected area includes:

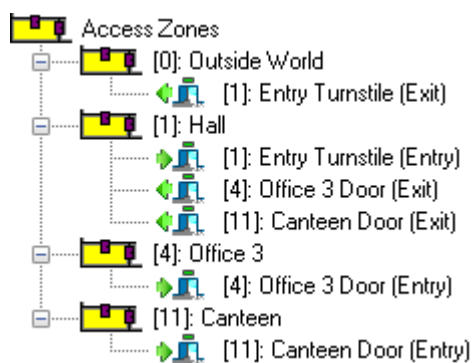
- Partitions:

- (1) Hall
- (4) Office 3,
- (11) Canteen



- Access Zones:

- [0] Outside World
- [1] Hall
- [4] Office 3
- [11] Canteen



- Access Points:

- (1) Entry Turnstile

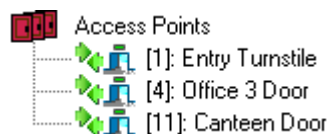
Number	1
Name	Entry Turnstile
Type	Turnstile
Operating mode	Entry/Exit
Access zone to enter	[1]: Hall
Entry relay	[SUPPORT-11-57.9.45.1]: Relay 1, Device 1
Accessed zone to exit	[0]: Outside World
Exit relay	[SUPPORT-11-57.9.45.2]: Relay 2, Device 1

- (4) Office 3 Door ,

Number	4
Name	Office 3 Door
Type	Two-way access door
Operating mode	Entry/Exit
Access zone to enter	[4]: Office 3
Entry relay	[SUPPORT-11-57.9.44.1]: Relay 1, Device 4
Accessed zone to exit	[1]: Hall
Exit relay	[SUPPORT-11-57.9.44.1]: Relay 1, Device 4

- (11) Canteen Door

Number	11
Name	Canteen Door
Type	Two-way access door
Operating mode	Entry/Exit
Access zone to enter	[11]: Canteen
Entry relay	[SUPPORT-11-57.9.45.1]: Relay 1, Device 1
Accessed zone to exit	[1]: Hall
Exit relay	[SUPPORT-11-57.9.45.1]: Relay 1, Device 1

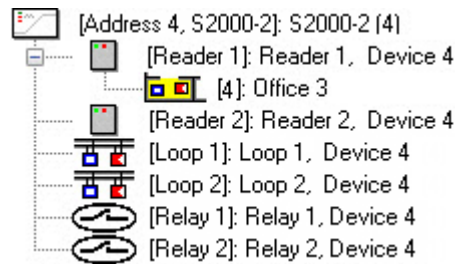


Let's create an access level for an employee of Office 3 who works weekdays from 8:00 till 17:00 (lunch from 12:00 till 13:00). The employee is allowed to do the following:

- Enter and exit through the entry turnstile (from 7:30 till 17:30) with antipassback enabled.
- Enter and exit through the Office 3 door (from 7:30 till 17:30) with antipassback enabled.
- Entry and exit through the Canteen door (from 12:00 till 13:00) with antipassback enabled.
- Arm and disarm the partition [4]: Office 3 from 7:30 till 17:30 using Reader 1 of S2000-2 with address (44) which controls the Office 3 Door access point

The centralized control is enabled here.

Then, associate Office 3 partition to the 1<sup>st</sup> reader of the S2000-2 (address 4)



Let us create the **Office3 Time Zone** times zone for access through Entry Turnstile and Office 3 Door and for arming/disarming Office 3 partition

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su
07:30	17:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

A time zone for access through the Canteen door will be **Office3 Time Zone (lunch)**:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su
12:00	13:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The access level for an employee from the Office 3 will be as follows:

Management	Access Control	View	Keybox Cylinders
	Partition	Mode	Time Zone
[4]: Office 3	Arm/Disarm	Office3 Time Zone	
Element type	Partition		
Element	[4]: Office 3		
Mode	Arm/Disarm		
Time Zone	Office3 Time Zone		
Management	Access Control	View	Keybox Cylinders
	Access Point/Zone	Mode	Time Zone
[0]: Outside World	Passage	Office3 Time Zone	
[1]: Hall	Passage	Office3 Time Zone	
[4]: Office 3	Passage	Office3 Time Zone	
[11]: Canteen Door	Entry/Exit	Office3 Time Zone (lunch)	
Element type	Access Zone		
Element	[0]: Outside World		
Mode	Passage		
Time Zone	Office3 Time Zone		
Antipassback	Hard		
Two-Person Rule Confirmation	None		
Three-Person Rule Confirmation	None		
Confirming	None		
Zonal Anti-Passback	None		
Confirm by button	None		

Element type	Access Zone
Element	[1]: Hall
Mode	Passage
Time Zone	Office3 Time Zone
Antipassback	Hard
Two-Person Rule Confirmation	None
Three-Person Rule Confirmation	None
Confirming	None
Zonal Anti-Passback	None
Confirm by button	None

Element type	Access Zone
Element	[4]: Office 3
Mode	Passage
Time Zone	Office3 Time Zone
Antipassback	Hard
Two-Person Rule Confirmation	None
Three-Person Rule Confirmation	None
Confirming	None
Zonal Anti-Passback	None
Confirm by button	None

Element type	Access Point
Element	[11]: Canteen Door
Mode	Entry/Exit
Time Zone	Office3 Time Zone (lunch)
Antipassback	Hard
Two-Person Rule Confirmation	None
Three-Person Rule Confirmation	None
Confirming	None
Zonal Anti-Passback	None
Confirm by button	None

#### 6.10.4 Configuring Working Schedules

In Orion Pro 1.12, working schedules also serve as access levels. In other words, a working schedule is defined by an access level specifically created to maintain time and attendance using access control capabilities.

For time and attendance purposes, two access levels are usually created for each employee:

- The first one is an access level used for an access control (as well as for IFS system, if necessary) with a time zone created for access control (IFS system, if necessary)
- The second one is a working schedule that defines access zones covering an employee's working place, and a time zone for time and attendance.

In some cases, there may be more than one access levels for ACS and IFS, but time and attendance can have only one access level.

An access level for ACS entities (or combined access level for ACS and IFS) is assigned (on Credentials tab) to a card (a combined access level can be assigned to PIN code, if necessary).

A working schedule is assigned (on Employees tab) to an individual employee or entire department.

The system utilizes working schedules to obtain information on when and what access zone an employee has to attend.

A working schedule (i.e. an access level for T&A) is created in the same manner as an access level for the access control system. They differ in the added entities and the logic of their utilization.

The Access level for Time and Attendance (T&A access level) includes an additional access zone which if attended by employees, it will report the attendance at work.

It is clear, that it is not needed to add an access zone identified as '**0 - Outside World**' to an access level.

*Please be advised of the following in respect to the T&A access levels:*

*Only access zones are analyzed*

*The Access Point entity (as well as Partition, and Partition Groups, etc.) is not analyzed*

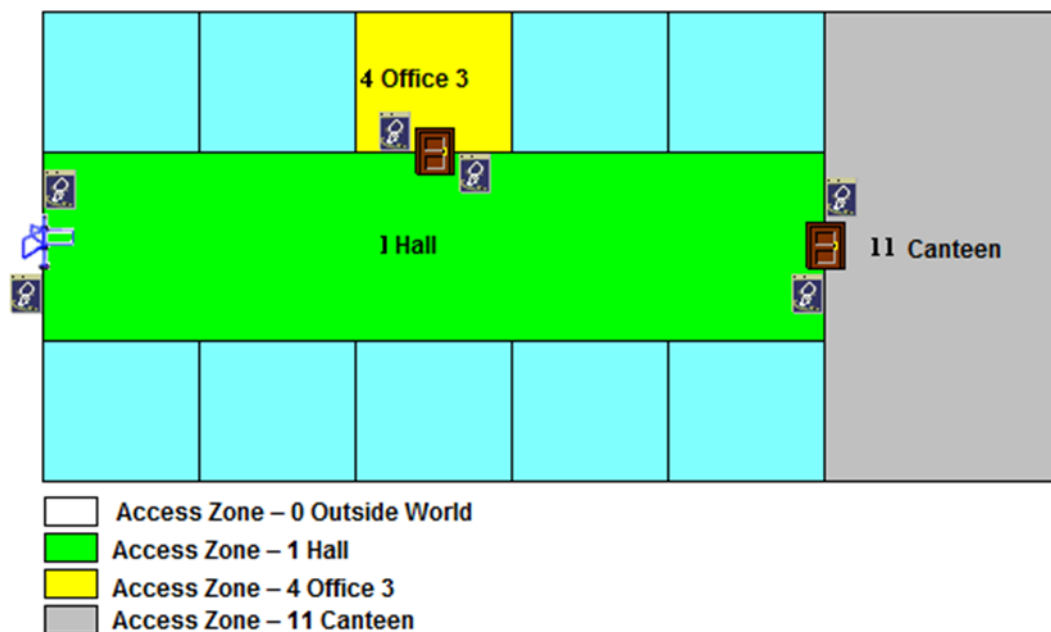
*The Access Zone entity is analyzed by a time zone only*

*All other permissions and rules for the Access Zone entity are not analyzed.*

Procedures of how to configure ACS access levels are described in Chapter in 6.10.2 Configuring Access Levels. This chapter describes how to create and configure an access level (working schedule) for Time and Attendance (working schedule)

Example!

A protected site has the following structure:





Let's create a working schedule (T&A access level) for an employee from Office 3, who works weekdays from 8:00 till 17:00 (lunch 12:00 - 13:00). The employee is regarded as attending work when he/she is in access zone 1-Hall and 4-Office 3.

The previous chapter discusses how to configure an employee's combined access levels applicable for access control and intrusion detection and fire protection systems. The employee's access to the site (permissions to operate partitions) is allowed in a wider time range than his/her work schedule, specifically at any time from 7:30 to 17:00.

An access level for time and attendance requires specific times for the employee's working schedule. The time zone for a working schedule (T&A access level) of an employee from Office 3 will be called **T&A of Office 3**:

Start	End	Ent	Ex	Mo	Tu	We	Th	Fr	Sa	Su
08:00	12:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13:00	17:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The T&A access level for the employee from Office 3 will be as follows:

Management	Access Control	View	Keybox Cylinders
	Access Point/Zone	Mode	Time Zone
	[1]: Hall	Passage	T&A of Office 3
	[4]: Office 3	Passage	T&A of Office 3

The **1-Hall** and **4-Office 3** access zones have been added to the T&A access level, and the employee's attendance in the zones is regarded as his/her working time.

However, the 0 - Outside World and 11 - Canteen are not added to the access level, thus his/her attendance at this zone is not regarded as his/her working time.

The configured T&A access level can be associated with an employee (or the entire department of the employee) in the Employee tab.

The combined access level described in the above chapter will be associated with a token (ibutton or card) in the Credentials tab.

### 6.10.5 Configuring Access Levels for System Monitor Operators

In Orion Pro 1.12, the rights of the System Monitor operator are defined by a special access level created to include the following:

- Entities of the system that the operator can control (partitions, partition groups, device zones (inputs), access points, and readers)
- Events of entities that the operator can view (partitions, partition groups, device zones (inputs), access points, and readers)

As mentioned above, the access level for an SM operator is assigned (on the Credentials tab) to a software password of an employee or several software passwords.

If an operator is allowed to control (operate) a system entity (partition group, partition, device's zones (inputs), access point, or reader), the operator can view events of this entity by default.

If an operator is not allowed to control (operate) a system entity, he/she cannot see status or events unless specially authorized to do so.

#### *Attention!*

*An SM operator can see entities on maps and tab of the System Monitor, if the rules to operate the entities and to view the entity status and events are included in the access level associated with the operator's software password.*

Please, keep in mind the following:

- If an access level includes permission to operate any of the partition groups, the partitions from that partition group and the loops of the partition are accessible as well.
- If an access level includes permissions and rules to perform actions in respect of a certain partition, the partition's loops and cameras can be controlled too.
- If an access level includes permissions and rules to perform actions to control a certain access point, the reader or readers associated with that access point are also accessible.

#### Note:

- You can disable zone(loop) and camera control using the Management of Individual Zone option in the software password menu
  - You can disable management of fire extinguishing using the Fire Extinguishing option in the software password menu.
- (The description of how to create software passwords are provided in Chapter 6.12.1 Creating Software Passwords (Software Logon Rights))

The Access Level for the System Monitor operator includes the following:

- Intrusion and Fire System Operation Rights (the Management tab in the Access Levels tab)
- Access Control System Management Rights (the Access Control tab in the Access Levels tab)
- Status and Events View Rights (the View tab)
- Keybox Management Rights (Keybox Cylinders tab)

Operations rights for the Intrusion and Fire System are defined in the same manner as for creating IFS access levels. The differences between them are the priority of entities and the number of analyzed entities.

1. **Attention!** Since an access level can include management rights permissions and rules applicable both to partitions and partition groups, SM operator rights for entities are prioritized as follows:

- Partition <sup>(the highest priority)</sup>
- Partition Group
- All groups
- All partitions <sup>(the lowest priority)</sup>

1. The IFS entities added to the SM Operator's access level will have the following properties to be analyzed:

Property	Possible Values	Description
Element type	Partition Partition group	Element type. <i>It is not recommended modifying this attribute.</i>
Element	All partitions , <i>One of the system partitions</i> All partition groups <i>One of the partition groups</i>	One of the IFS entities: partition, partition group, all partitions or all partition groups <i>It is not recommended modifying this property</i>
Mode	View Arming Disarming Arming/Disarming	Operations and actions performable with an entity: <ul style="list-style-type: none"> <li>• View (The Operator can only view an entity )</li> <li>• Arm (The Operator can only arm an entity with no permission to disarm)</li> <li>• Disarm (The Operator can disarm an entity with no permissions to arm)</li> <li>• Arm/Disarm (The Operator can arm and disarm an entity)</li> </ul>

The rights and rules for the access control systems are defined following the same method as for creating access level for an access control system. The difference is the number of entity's analyzed properties.

2. The ACS entities added to the SM Operator's access level will have the following properties to be analyzed:

Properties	Possible Values	Description
Element type	Access Zone Access Points	Element type  We do not recommend modifying this property.
Element	All access zones <i>One of the access zones</i> All access points <i>One of the access points</i>	One of the ACS entities: an access point, access zone, all access points and all access zones We do not recommend modifying this property.
Mode	Passage Entry Exit Entry/Exit	Rules applicable to the operation of an access control entity including Access Point: <ul style="list-style-type: none"> <li>• <b>Passage</b> (allows access through the following: <ul style="list-style-type: none"> <li>○ One-way access point</li> <li>○ Two way access point (in both direction)</li> </ul> </li> </ul>

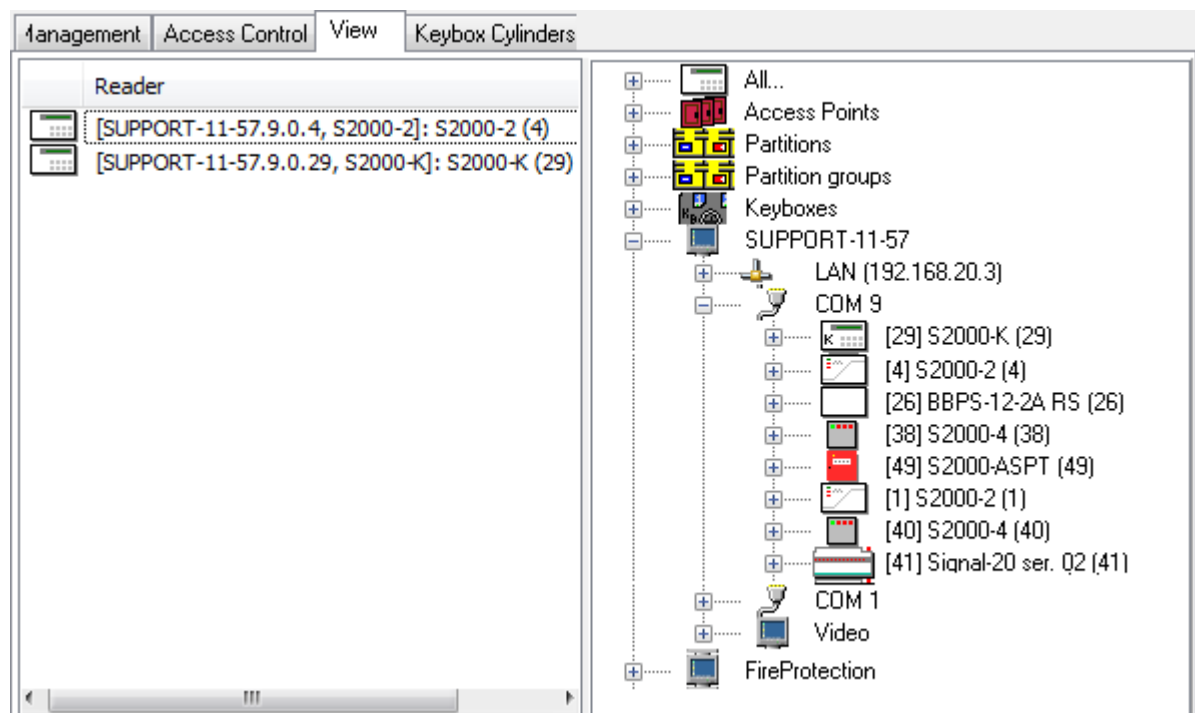


		<ul style="list-style-type: none"> <li>• <b>Entry</b> (allows access through the following access points: <ul style="list-style-type: none"> <li>○ One-way access points working in the <b>Entry</b> operating mode</li> <li>○ Two-way access points working in the <b>Entry</b> operating mode),</li> </ul> </li> <li>• <b>Exit</b> (allows access through the following access points: <ul style="list-style-type: none"> <li>○ One-way access points working in the <b>Exit</b> operating mode</li> <li>○ Two-way access points working in the <b>Exit</b> operating mode),</li> </ul> </li> <li>• <b>Entry/Exit</b> (allows access through two way access points in both directions).</li> </ul> <p>The Access Zone entity may have the following value only:</p> <ul style="list-style-type: none"> <li>• <b>Passage</b> (used to allow access through all access points in both direction).</li> </ul>
--	--	--

If an operator has rights to operate a certain entity, he/she can view the status and events of this entity as well.

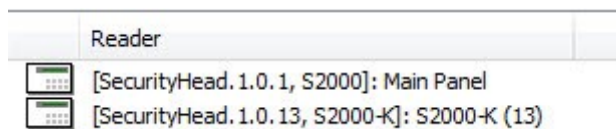
If an operator may not operate an entity, but has to view it only, he must have view rights assigned in order to do that.

The rights are assigned in the Management tab.

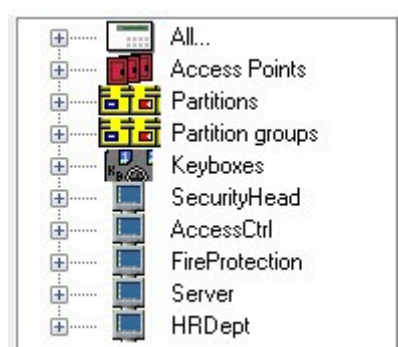


This tab page shows the following:




- The list of system entities added to the access level:









- The view tree of the system:




The view list of the system entities and the access level list of system entities display the following information:

1. For entities such as Access Point () , Partition () and Camera () :
  - a. Number
  - b. Name

 [1]: Entry turnstile
2. For entities such as Device () , Reader () , Loop () and Relay Output () :
  - a. Address
  - b. Name








 [SecurityHead.1.0.5, S2000-4]: S2000-4 (5)


P.S. The list of system entities added to the access level shows a full address of the entities:

 [SecurityHead.1.6.1]: Loop 1, Device 6 . And the Device entity includes the type

To add a new entity to the list of entities, please enter the editing mode, then:

- Select an entity you want to be viewed.
- Double click the entity

You can add all access points (  All Access Points ), all partitions (  All Partitions ), all devices (  All Devices ), all readers (  All Readers ),  All Loops , all relay outputs  All Relays and all cameras  All Cameras to an access level.

To do that, please double click a node you need. All entities as the above are included in the  All... node

To delete an entity from the view of an access level, please enter the editing mode:

- Select an entity you want to delete
- Press the <Del> key, and click **Yes** button in the dialogue box to confirm the delete action:

Finally, note that:

- If any partition is added to a view access level, the status and events of the partition's loops and outputs can be viewed as well.
- If any access point is added to a view access level, the status of events of a reader(s) controlling the access point can be viewed as well.

## 6.11 The Employees Tab. Creating the List of Employees

Orion Pro: Database Administrator

Options Service Help

[All departments]

Employees (8)

- Ivanov P.
- Jakson J.
- McKeon D.
- Peterson P.
- Smith J. K.
- Smith K.
- Tuma B.
- eee e.

Employee ID: 5

Last Name: Ivanov

First Name: Peter

Middle Name:

Status: User

Work Phone:

Home Phone:

Contact-id number:

Company: BOLID Company

Department: Executive Management

Job Title: Manager

Schedule: Department Work Schedule

☐ Flexible Schedule ☒ Day Carryover Ban

Car:

Home Address:

Date of Birth: 15

Date	Time	Description
25.03.2015	16:30:09	: Database restart in Scanning Core completed, computer SUPPORT-11-57 (192.168.11.57)

Remotely Changed Tables Network exchanges

Edit Add Delete Print Exit

The Employees tab displays the following information:

1. The list of employees
2. The attributes of a selected employee.

The Employees tab allows:

1. Editing a list of employees
2. Editing lists of companies, departments, and job titles.
3. Printing badges (cards) of employees.

List of Employees:

The list of employees includes Names of each employee:

The lower part of the list contains a search field to find an employee in the list by his/her ID, name, car, or company:

The method of search is selectable in the dropdown list:

When entering (case sensitive) an employee ID, name, vehicle, or company in the search field, it moves to the item of the list starting with the characters being entered:

The upper part contains fields for arranging the list of employees:

To arrange employees in the list, please click the corresponding button:

- By name ,

- By status,
- By Employee ID (EMPLID).



This list can be filtered to display employees from a required department. To do that, please select a required department:



### 6.11.1 The Employee Entity

To add a new Employee entity, please:

- Click the Add button.
- Enter values for the properties of the new Employee entity.
- Click the **Save** button.

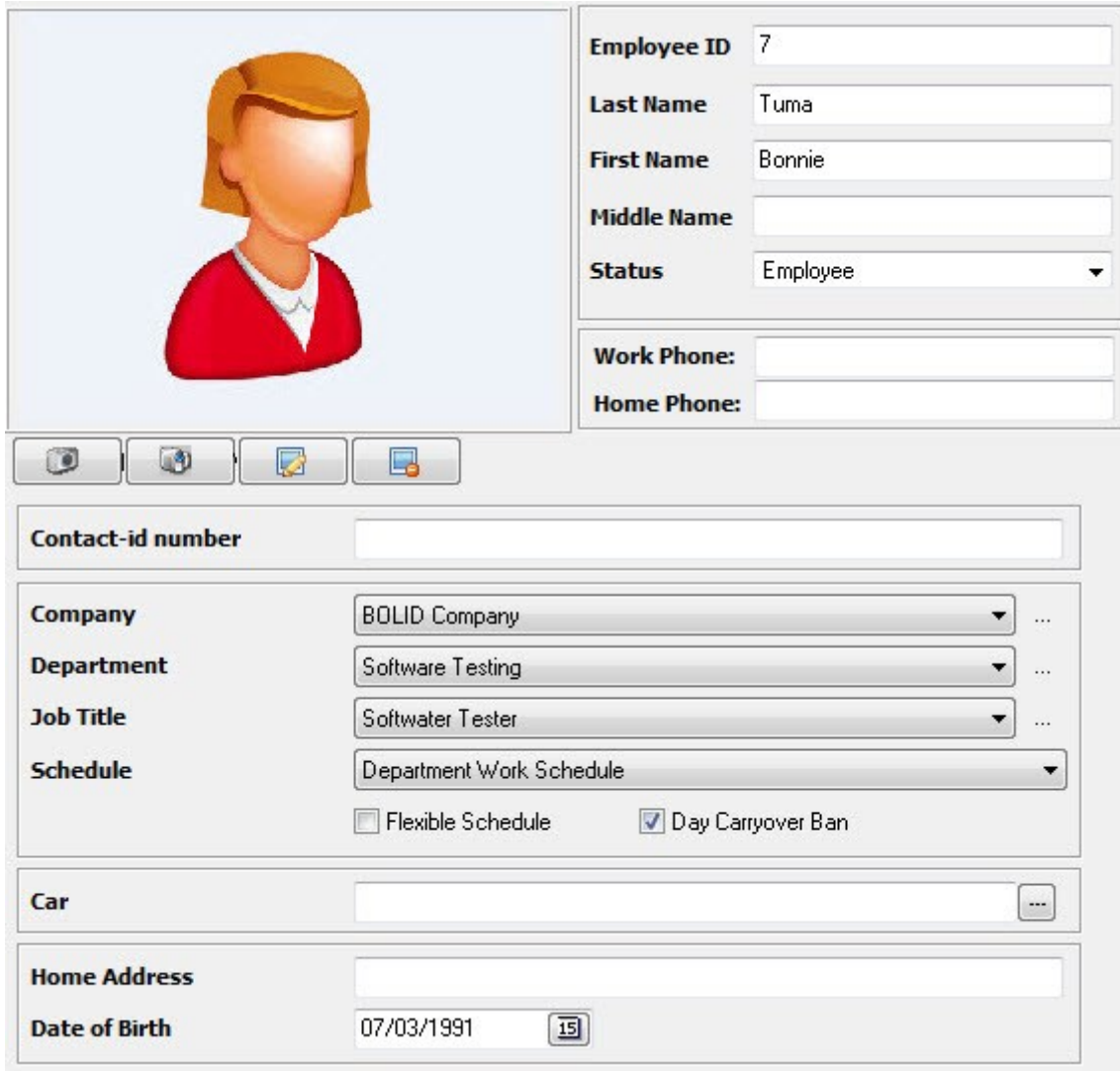
To modify the attributes of the Employee entity, please select a required employee in the list and click the **Edit** button. Then enter necessary changes and click the **Save** button.

To delete the Employee entity, please select an employee you want to delete from the list of employees and click the **Delete** button. Then click **Yes** in the appeared dialog box to confirm the deletion.

*Orion Pro Suite supports import of employees list from the \*.csv file using the Employee Import Wizard utility included in the Orion Pro Suite (Refer to Chapter 16 Employee Import Wizard)*

*(Continued Next Page)*

The attributes of the Employee entity:



Employee ID: 7

Last Name: Tuma

First Name: Bonnie

Middle Name:

Status: Employee

Work Phone:

Home Phone:

Contact-id number:

Company: BOLID Company

Department: Software Testing

Job Title: Softwater Tester

Schedule: Department Work Schedule

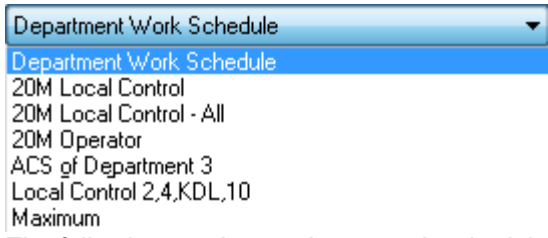
☐ Flexible Schedule ☒ Day Carryover Ban

Car:

Home Address:

Date of Birth: 07/03/1991

Attribute	Possible Values	Description
Employee ID	A length of 0 to 50 characters	Employee ID (EMPLID) is the employee ID in a company sheets. <i>This field may be empty (not recommended).</i> Default value: empty field
Last Name	A length of 0 to 25 characters	The last name of an employee Default value: empty field
First Name	A length of 1 to 25 characters	The first name of an employee Default value: empty field
Middle Name	A length of 0 to 25 characters	An employee's middle name <i>This field may be empty.</i> Default value: empty field
Status	Owner Administrator Duty Officer Duty Operator User ( or Credential Holder)	An employee's authority level. <i>(Refer to Chapter 6.11.1.1 the Status of an Employee )</i> Default value: User

	Employee Badge Office Operator (BO Operator)	
Work Phone	A string length of 0 to 25 characters	An employee's work phone. <i>This field is optional;</i> Default : empty field
Home Phone	A string length of 0 to 25 characters	An employee's home phone number. <i>This property is optional.</i> Default value: Empty field
Contact-id number	0..2147483647	An employee's contact-id number used to transmit events to S2000-IT, YO-4S, and S2000-PGE devices. Default value: 0
Company	One of the in-system- companies or empty field	A company where an employee works <i>This property may have no values in its field (Not recommended).</i> <i>If the <b>Company</b> field of an employee has no values entered, the employee will not be visible in the Time and Attendance software module.</i> <i>(Refer to Chapter 6.11.1.2. The Company Property</i> Default value: Empty field
Departments	One of the in-system departments or empty field	The department of an employee. <i>This property may have no values in its field (Not recommended).</i> <i>If this property of an employee is not set, this employee will not be visible in the Time and Attendance module.</i> <i>(Refer to Chapter 6.11.1.3. The Department Property.</i> Default value: Empty field
Job Title	One of the system job tittle or empty field	An employee's job title <i>This property's field may be empty.</i> <i>(Refer to Chapter 6.11.1.4 Job Title )</i> Default value: empty field
Work Schedule	Department Work Schedule or one of the access levels	Employee's working schedule Work schedule are selectable items in the dropdown list:  The following can be used as a work schedule: <ul style="list-style-type: none"> <li>A specific employee work schedule (T&amp;A access level). In this case, an employee's time attendance will be accounted in accordance</li> </ul>

		<p>with a defined work schedule.</p> <ul style="list-style-type: none"> <li>Department Work Schedule, an employee's time and attendance will be accounted in accordance with the schedule of a department where an employee works.</li> </ul> <p><i>(Refer Chapter 6.11.1.3 The Department Property)</i></p> <p>Default value: Department Work Schedule</p>
Flexible Schedule	<input checked="" type="checkbox"/> (Yes), <input type="checkbox"/> (No)	<p>This property enables or disables a flexible schedule:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> (Yes) – A flexible schedule is enabled - the time and attendance accounts only hours worked regardless of late punch-ins, absences, and early punch-outs of an employee.</li> <li><input type="checkbox"/> (No) – A flexible schedule is disabled. All employee schedule breaches are accounted).</li> </ul> <p><i>For the most part, a flexible schedule does not apply.</i></p> <p>Default value: <input type="checkbox"/> (No)</p>
Day Carryover Ban	<input checked="" type="checkbox"/> (Yes) <input type="checkbox"/> (No)	<p>This property defines whether to allow the day carryover option on not :</p> <ul style="list-style-type: none"> <li>(Yes)– The day carryover is not allowed. The employee is not allowed to work night shifts</li> <li>(No)– The day carryover is allowed. The employee may work night shifts:</li> </ul> <p>If you select the 'Day Carryover Ban' option, hours worked will be counted as it set in the Time and Attendance client: through the end of a day, through the end of a working day or till an employee's last recorded 'Passage' event in the system. The option is used against access control procedure violations when the system has not registered the exit from a site.</p> <p><i>The Day Carryover Ban option is selected for employees in most cases.</i></p> <p>Default value: <input type="checkbox"/> (No)</p>
Car	A string length of 0 to 200 characters	<p>An employee's car</p> <p><i>This property is optional.</i></p> <p>Default value: empty field</p>
Home Address	A string length of 0 to 200 characters	<p>An employee's home address</p> <p><i>This property is optional</i></p> <p>Default value: empty field</p>
Date of Birth	'01.01.1900'...'31.12.2099' or empty field	<p>The birth date of an employee.</p> <p><i>This property field is optional</i></p> <p>Default value: empty field</p>
Photo	Photo or empty field	<p>The photo of an employee.</p> <p><i>This property field is filled in optionally</i></p> <p>Default value: empty field</p>

#### 6.11.1.1 Status

The status of an employee is selected from the dropdown list:





The status of the user (employee) defines his rights in the system:

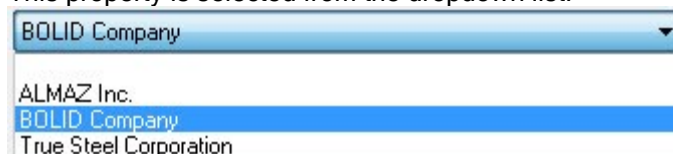
Status	User rights to run software modules	Rights in Database Administrator
<b>Owner</b>	The highest status. The Owner has rights to run all modules and perform all functions.	The Owner has rights to perform any functions including the assignment owners and administrator accounts
<b>Administrator</b>	The Administrator has rights to run all software modules  The Administrator has rights to generate and edit report in the Report Generator Module.	The Administrator has rights to perform any functions except for the assignment of owners and administrators.
<b>Duty Officer Duty Operator</b>	This user have rights to run the Operative Task, Report Generator, and Time and Attendance modules  The user may close System Shell	-
<b>User Employee</b>	This user have rights to start Report Generator and Time and Attendance  Most employees have this status ( User/Employee).	-
<b>Badge Office Operator</b>	An employee with this status has rights to run the Database Administrator, Report Generator and Time and Attendance  Also, such an employee has rights to close System Shell.	The user have rights to use Employees and Credentials tab of Database Administrator tabs related to the issue of badges (ibuttons and cards)  This status gives no rights to assign Owners and Administrators  A user with this status has no rights to define PIN codes and software passwords


**Attention!** There must be at least one user with the **Owner** status in the system.

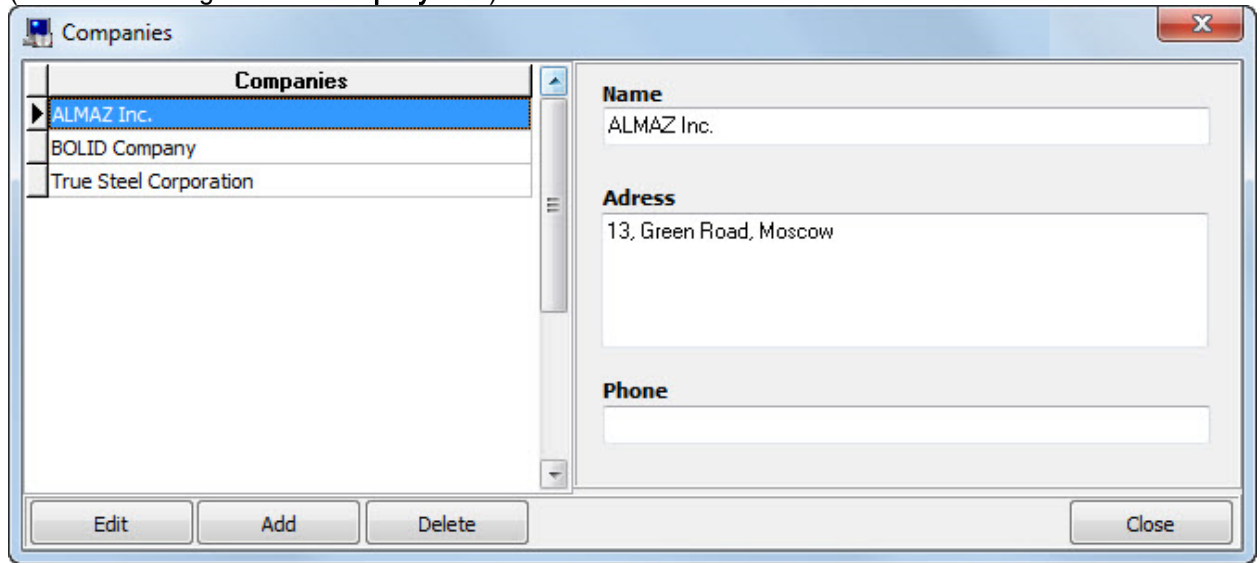
In addition to Status, an employee rights depends on the properties of software passwords assigned to such an employee (Refer to Chapter 6.12.1 Creating Software Passwords).

#### 6.11.1.2 The Company Item

This property is selected from the dropdown list:



The list of companies is edited in the Companies dialog box. To open this dialog box, click the  button (located to the right of the **Company** item):



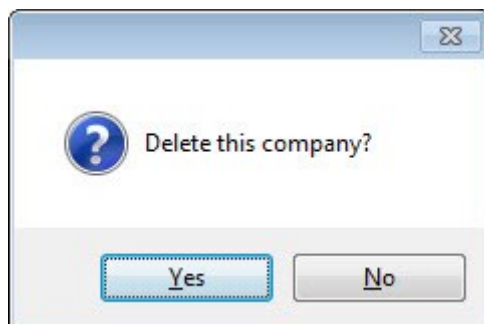
The left pane of the window contains the list of companies.  
The right pane shows the details of a selected company

To add a new company:

- Click the **Add** button.
- Enter details for the new company.
- Click the **Save** button.

To modify company details, please select a required company in the list and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete a company, please select a required company from the list of companies and click the **Delete** button. Then click **Yes** in the appeared dialog box to confirm the deletion:



*The details of the Company:*

**Name**

**Address**

**Phone**

Attribute	Possible Values	Description
Name	A string length of 1 to 100 characters	The name of a company. Default value: empty field
Address	A string length of 0 to 150 characters	The address of a company <i>This attribute may have no values.</i> Default value: empty field
Phone	A string length of 0 to 30 characters	The phone of a company <i>This attribute may have no values.</i> Default value: empty field

#### 6.11.1.3 The Department Item

This department is selected from the dropdown list:

Executive Management


Sales Department

Software Developments

Software Testing

Technical Support

Warehouse

The list of departments is edited in the **Departments** dialog box. To open this dialog box, click the  button (located to the right of the **Department** interface item:

The left pane of the window contains the list of departments.  
The right pane shows the details of the department you selected

To add a new department, please:

- Click the **Add** button.
- Enter details for the new department.
- Click the **Save** button.

To modify the attributes of a department entity, please select a required company in the list and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete a department, please select a required department from the list of departments and click the **Delete** button. The click **Yes** in the appeared dialog box to confirm the deletion:

The Department item has the following attributes:

Attribute	Possible Values	Description
<b>Name</b>	A string length of 1 to 80 characters	The name of a department Default value: Empty field
<b>Description</b>	A string length of 1 to 100 characters	Comments <i>This attribute may have no values</i> Default value: Empty field
<b>Work Schedule</b>	<b>Not Specified</b> or one of the access levels	The work schedule of a department. The schedule is selected from the dropdown list

		Department Work Schedule Department Work Schedule 20M Local Control 20M Local Control - All 20M Operator ACS of Department 3 Local Control 2,4,KDL,10 Maximum Default value: Not specified
--	--	--

#### 6.11.1.4 The Job Title Item

A job title is selected from the dropdown list:

The list of job titles is edited in the **Job Titles** dialog box opened by clicking the button (located to the right of the **Job Title** item):

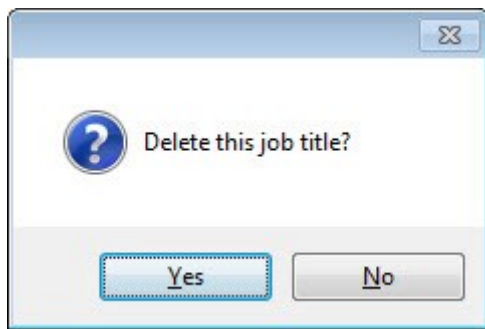
The left pane of the window contains the list of job titles.  
The right pane shows the details of a selected job title

To add a new job title, please:

- Click the **Add** button.
- Enter values for the properties of the new job title.
- Click the **Save** button.

To modify the attributes of the job title, please select a required job title from the list and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete a job title, please select a required job title from the list.



The attributes of the job title item:


**Name**  
Deputy chief

Attributes	Possible Values	Description
<b>Name</b>	A string length of 1 to 80 characters Default Value: empty field	The name of a job title

#### 6.11.1.5 The Photo Item

The Photo contains a photographic image of an employee.

An employee's photo can be loaded from the bmp or jpg file or captured from a USB camera connected to the workstation.

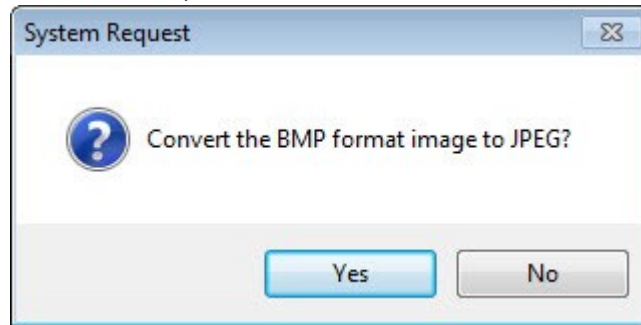
To load an employee's photo, please go to the editing mode, then click the  button, and select an employee image file in the standard dialog box.

To take an employee photo using a USB camera, please go to the editing mode, then:

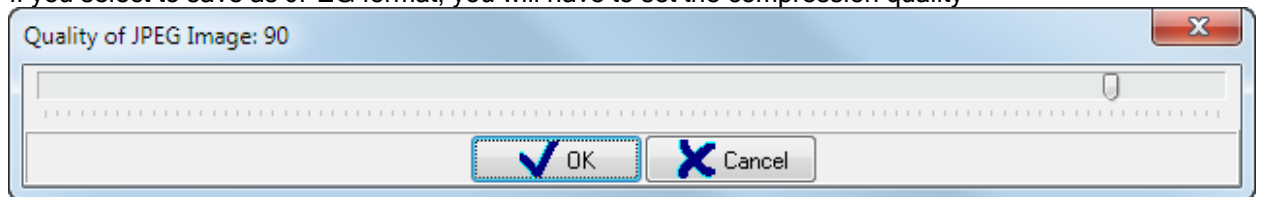
- Click .
- The **Video Frame** window will appear:



- Click the **Freeze** button to take a picture.
- Click the **Save** button. Select a format to save an employee's picture (a jpg format is recommended):





If you select to save as JPEG format, you will have to set the compression quality

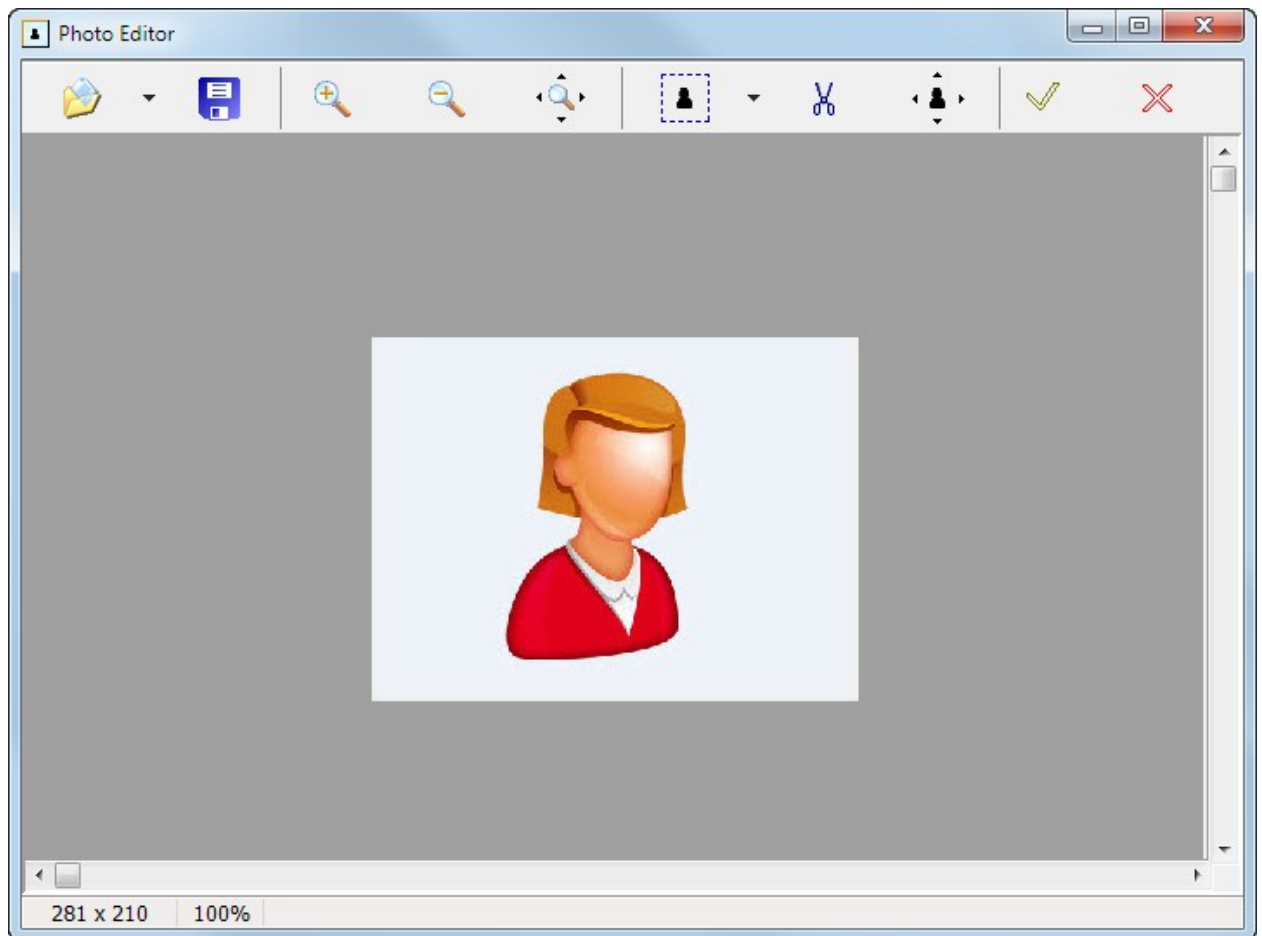








*Note, that maximum size of employee photo stored in the database is defined by the Maximum size of Employee Photo parameter of the Database Administrator module (Refer to Chapter 6.14.1 Database Administrator Settings)*

*Please connect only one USB camera to a computer to ensure proper image capturing.  
To edit an employee's photo, go to the editing mode of the Employee entity:*

- Click the  button
- Edit a photo in the appeared Photo Editor window.
- Click the  button to accept changes


The Editor Photo window offers the following functions:

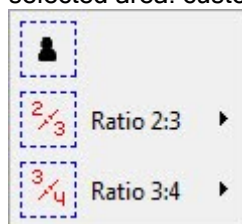


- 
- – Load an image form a file.
- 
- – Save photo as a file
- 
- – Zoom in.
- 
- – Zoom out
- 
- – As original
- 




- – Select an area in the photo.


If you click the  button, the menu will appear where you can choose proportion of a selected area: custom, 2/3, 3/4.

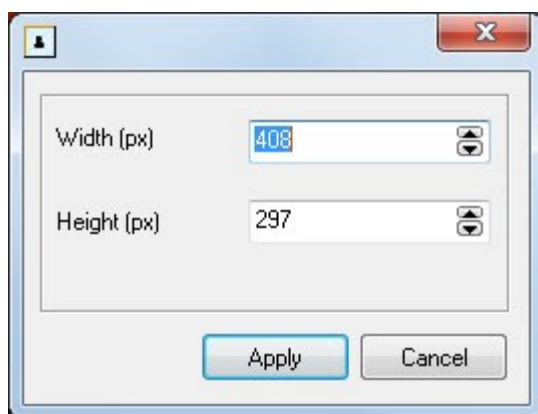


If you select 2/3 or 3/4 ratio, please specify what side you want to lock as original and what side is to be resized to match required ratio.






- 
- – Crop a picture in accordance with boundaries of a selected area.

- 
- – Change resolution of photo in the pop-up dialog box.



You cannot change the ratio of a photo

-  – Accept all changes and close the Photo Editor dialog box.
-  – Close the Phot Editor dialog box with no changes accepted.

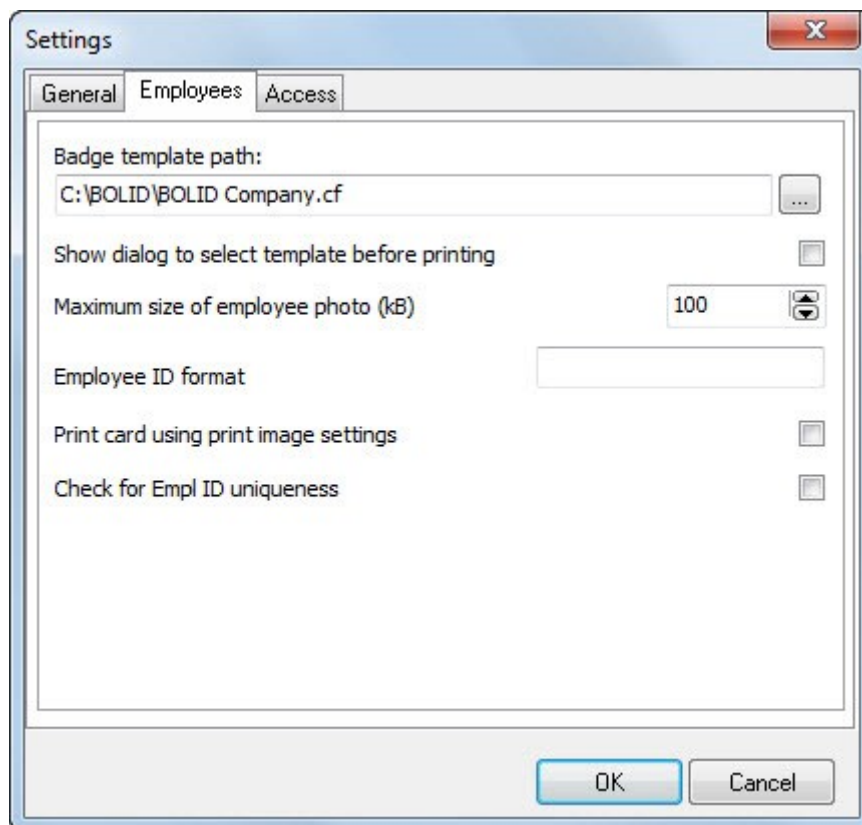
To delete an employee photo, please go to the editing mode and click the  button

### 6.11.2 Employee Card. Printing a Badge

The Database Administrator module supports printing badges on Proximity cards using special printers.

To print an employee badge, please do the following:

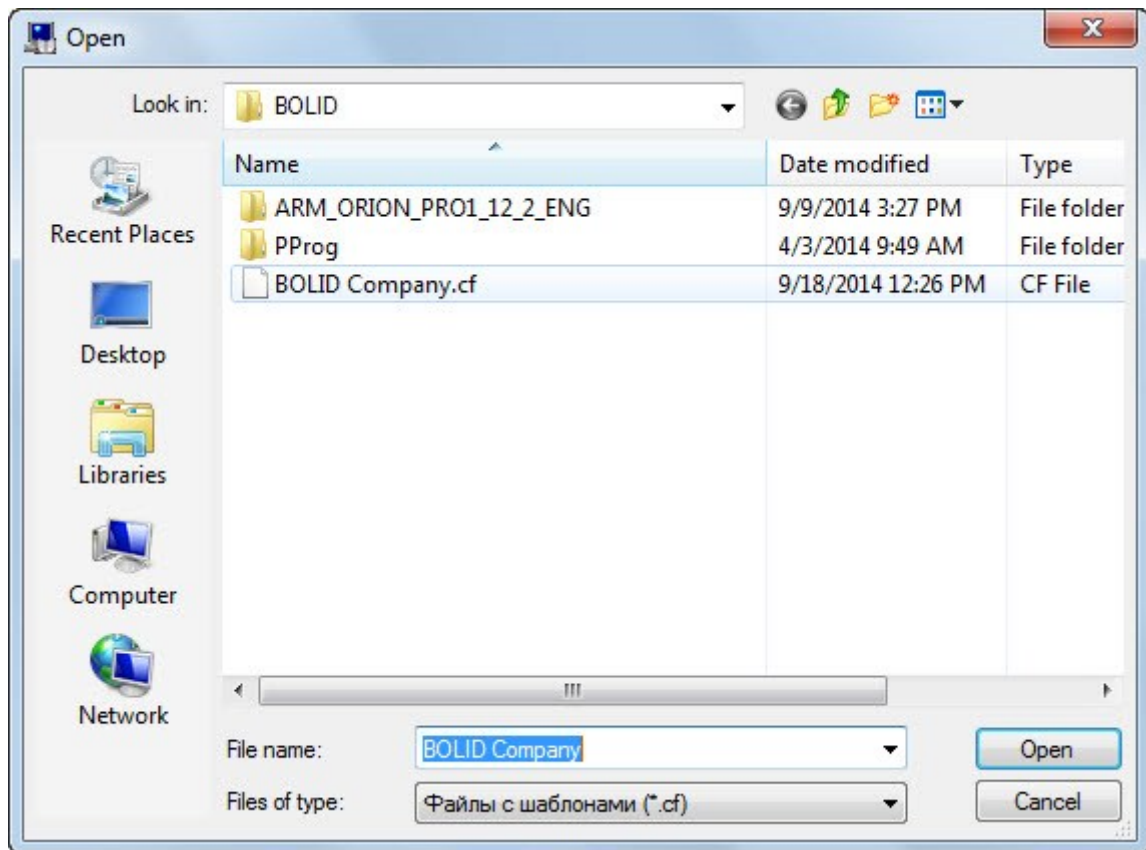
1. Create a badge template using the **Options/Configure Card Layout** menu. (Refer to 6.11.2.1 Configuring a Card Layout)
2. Navigate to **Options/Settings** menu to open the **Settings** tabbed window. Then go to the **Employees** tab and specify a file path in the **Badge template path** field.



*If you use a printer based on a magnetic unit, please select the **Print card via print image settings** parameter in the checkbox.*

1. Please, select a required employee from the list of employees and click the **Print** button.

If the **Show dialog to select template before printing** parameter is selected in the Database Administrator settings, you will have to choose a template every time you print a badge.

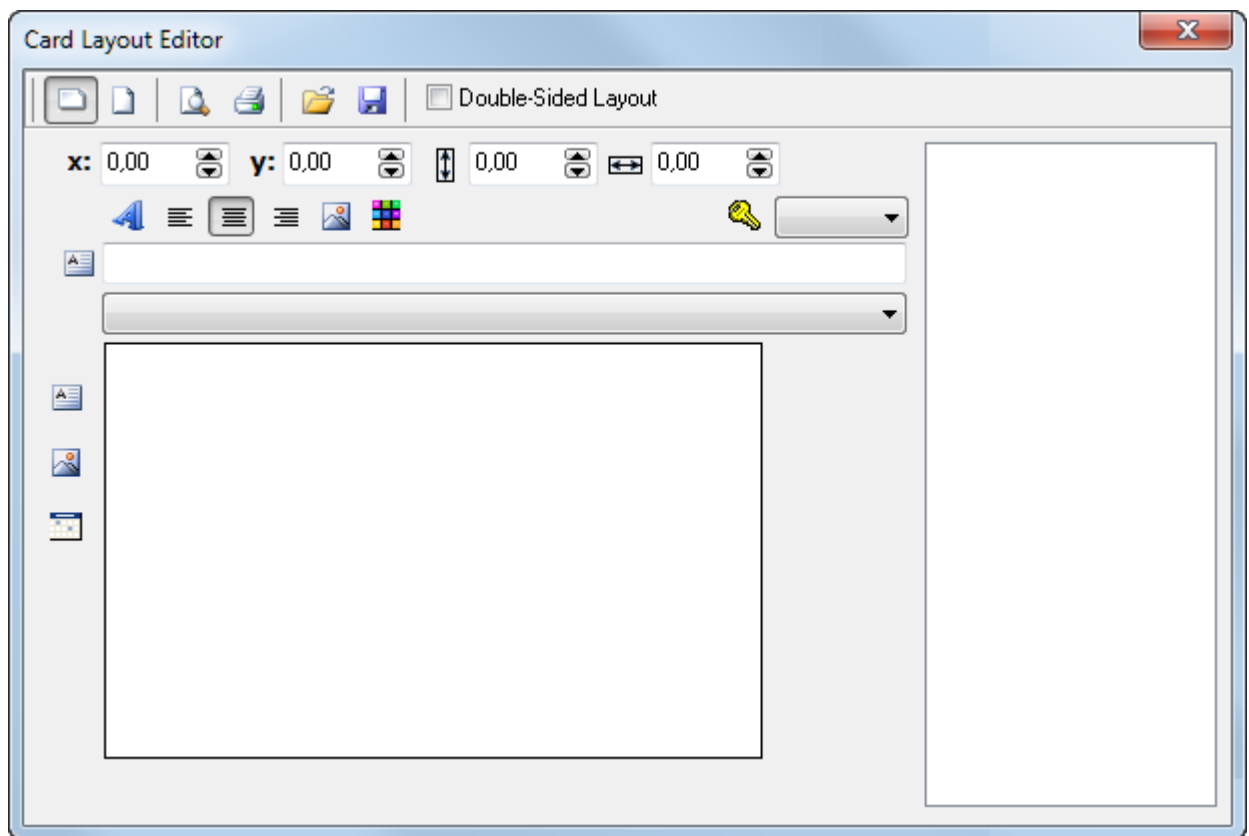


1

*In this case, there no sense of specifying a path to a specific template, and the **Badge template path** field may be left empty.*

#### 6.11.2.1 Creating Badge Layout



The **Card Layout Editor** dialog box is used to create and edit an employee badge template. To do that please choose **Options/Configure Badge Layout/Standard Badge**.



You can perform the following functions using this window:


- Save to and load a template from a file.

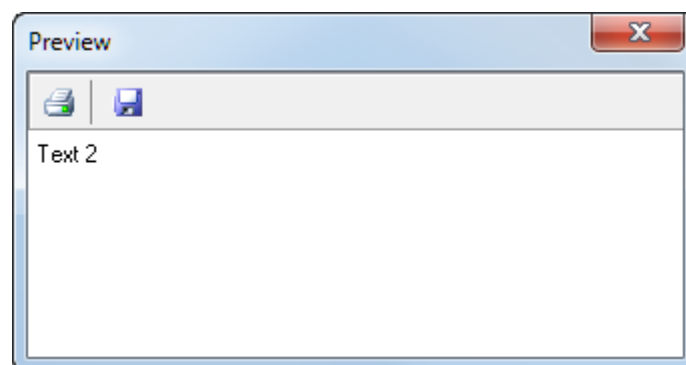
Use the following buttons to perform that:


-  – Save as a file
-  – Load from a file

- Preview and preprint a new.

Use the following buttons to do that:




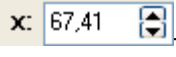

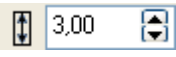
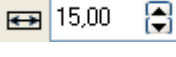

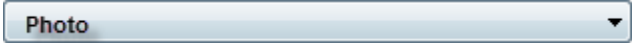
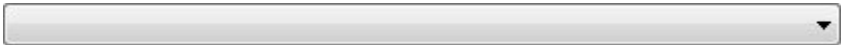


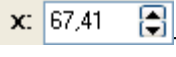
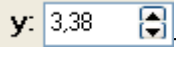
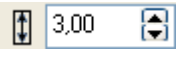
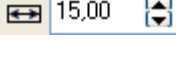

-  – Preview a created template

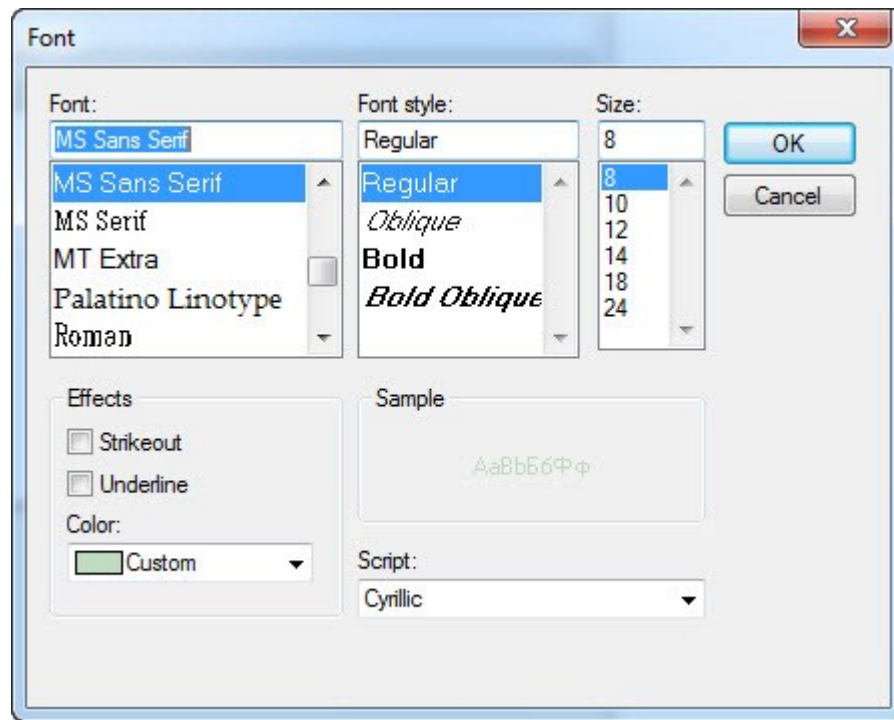


-  – Print a test template.




- Set a photo's orientation.

Please, use the following buttons:

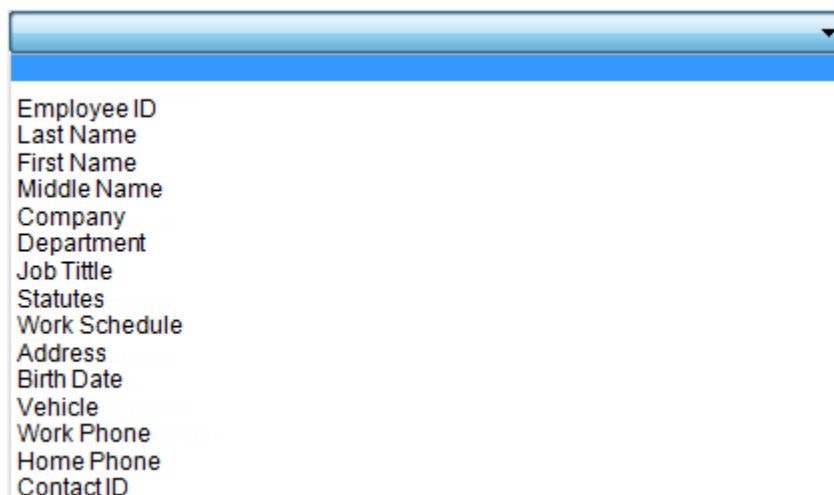
-  – Toggle landscape
-  – Toggle portrait
- Add a photo or any other graphics to an employee template:
  - Click the  button.
  - Position the image by dragging it to a required place or using field alignment:
    1.  – align the upper left corner of the image against the left side of a layout.
    2.  – align the upper left corner of the image against the upper side of a layout.
  - Set an image size using field adjustments
    1.  – height
    2.  – width
  - Type an image name  
  
*Additional details may be needed only to facilitate template configuration.*
  - Define whether it will display an employee photo or other picture.
    1. To display an employee photo, please select the Photo item in this field dropdown list.   
*An employee's photo will be printed to a badge.*
    2. To display a photo in this area, please leave this field empty  

- And click the  button to load an image
- Add any text or an employee's details from the database.
  - Click the  button.
  - Position the text place on a layout by clicking and dragging it to the place you need or using the field alignment:
    1.  – Align the upper left corner of your text against the left side of layout.
    2.  – Align upper left corner of the text relative to the upper side of the layout.
  - Set a text's field size:
    1.  – Field height.
    2.  – Field width.
  - Provide text font settings in the **Font** window. To open this window, please click the  button



- Align a text using the following buttons:

1.  – Align to the left
2.  – Center text
3.  – Align to the right

- Entry a text name



*When database details are to be displayed, the text is entered only to facilitate the process of configuring a layout*

*When entered information is to be displayed on a badge, it is the text entered in this field will be displayed.*

- Define what text or an employee's details are to be displayed in a badge,
  1. To display employee details on a badge, please select one of the items from the dropdown list:

The available items are as follows:

1. Employee ID
2. Last Name
3. First Name
4. Middle Name
5. Last and first names
6. Company
7. Department
8. Job Title
9. Statutes
10. Work Schedule
11. Address
12. Birth Date
13. Vehicle
14. Work Phone
15. Home Phone
16. Contact ID


*In this case, when an employee badge is printed, the corresponding information will be taken from the database.*

In addition, you can select from the

dropdown list the **Card**

**Code** item.

*In this case, when an employee badge is printed, the card code information of the badge will be taken from the database.*

Using this field   one can select how a card code will be displayed:


- Full
- Wiegand16
- Wiegand24



2. If you want the text to be printed on a card, please leave the following field empty:

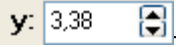
*In this case, the printed badge will contain text entered in the field*

- Add a print date to a card layout.

To do that, please proceed with the following actions:

- Press the  Button
- Position the date position on a layout by clicking and dragging it where you want or using the field adjustment:


1.    – Align the upper left corner of the data text against the left side of the template.

2.  3,38 – Align the upper left corner of the data text against the upper side of the template.




- Set a text's field size:

1.  3,00 – Field height.

2.  15,00 – Field width

- Provide select font settings in the **Font** window. To open this window, please click the  button

- Align a text using the following buttons:

1.  – Align to the left
2.  – Center text
3.  – Align to the right

- Entry the name of date in the field



*The text entered in this field is used only to facilitate layout configuration processes. When printed, the badge will contain a print date*

### 6.11.3 Saving an Employee Photo as a File

The Database Administrator module offers a capability of saving an employee's database-stored photo as a file.

To save an employee photo as a file, please select a required employee from the list of employees, then go **Service/Save Employee Photo as File**, the standard Windows' dialog box will appear, then locate and name a file you want to save, and click the **Save** button.

You can save an employee photo using the **Edit Photo** dialog box as well. (Refer to Chapter 6.11.1.5 Attributes of Photo Item

### 6.11.4 Exporting Employee Details and Credentials to CSV File

The Database Administrator module provides capability of exporting a list of employees and credentials from the database to a CSV file using the Employee Import Wizard utility.

To launch the **Employee Import Wizard** follow Service/Export Employees to CSV File

When launching this way, the wizard will skip the following windows:

- Welcome to Import and Export Wizard.
- Database Parameters.
- Select Operational Mode

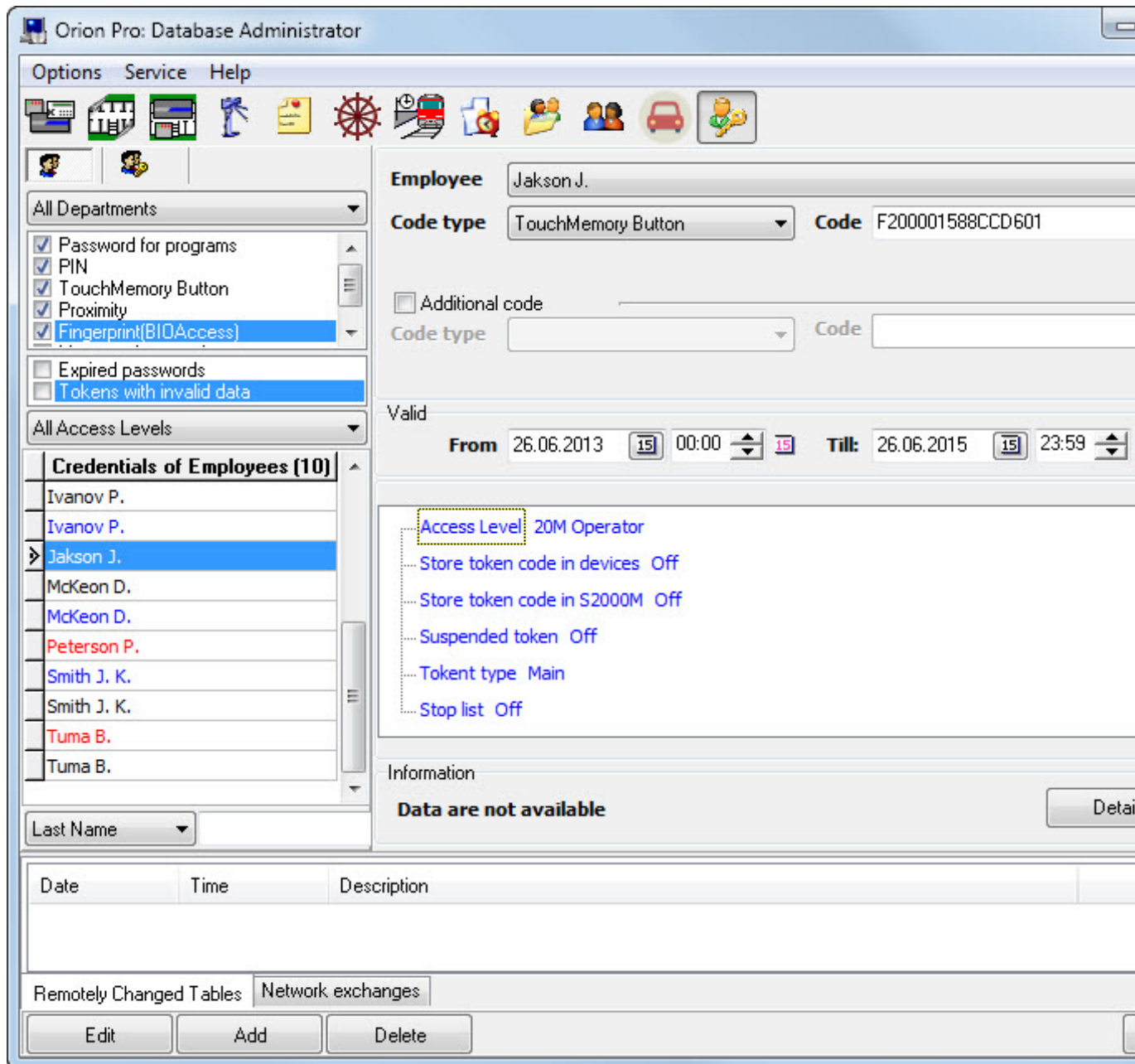


The Data Files dialog box will be displayed immediately, where you have to enter name of files for the list of employees and the list of credentials.

Logic of Import and Export Wizard and the structure of files containing lists of employees and credentials are described in Section 16 Employee Import Wizard of this Guide.

P.S. Note that in addition to the Database Administrator, the above functions require the Employee Import Wizard utility.

## 6.12 The Credentials Tab. Creating the List of System Credentials



The Credentials tab shows the following:

1. List of credentials
2. Properties of a selected credential
3. Information showing compliance between database settings and device configurations for selected credentials (tokens or fingerprints)

The Credentials tab allows user to:

1. Modify the list of credentials for the Orion Pro software modules, as well as IFS and ACS systems:
  - Software passwords (used to run software modules)
  - PIN codes
  - Touch Memory buttons
  - Proximity cards
  - Fingerprints.

## 2. Synchronize the list of database-stored credentials with the system device configurations

Let's consider the list of credentials (**Credentials of Employees**):

Software Password  
PIN  
Touch Memory Button  
Proximity Card  
Fingerprint (BIOAccess)  
Expired passwords  
Tokens with invalid data  
All Access Levels  
**Credentials of Employees [6]**  
▶ Jackson J.  
McKeon D.  
Peterson P.  
Smith J. K.  
Smith J. K.  
Tuma B.  
Last Name

In the list of Employee credentials, credentials are represented as the names of credential holders:

Smith J. K.

PIN codes, Touch Memory buttons, Proximity cards, and fingerprints are shown in black color, Passwords are shown in blue color. Expired passwords (credentials) of any type are shown in red font color.

The lower part of the list contains the search field to search credentials by a code, short code, or employee last name (credential holder).

Last Name

The method of search is selected in the dropdown list:

Last Name  
Last Name  
Code  
Short code

When you start entering a code, short code, or an employee's name (case sensitive), it moves to the first item that begins with the characters being entered:

**Credentials of Employees [10]**  
▶ Jackson J.  
McKeon D.  
McKeon D.  
Peterson P.  
Smith J. K.  
Smith J. K.  
Tuma B.  
Tuma B.  
Last Name ja

The upper part contains fields to search and filter credentials:

All Departments ▼

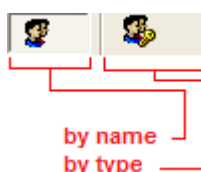
☒ Software Password  
☒ PIN  
☒ Touch Memory Button  
☒ Proximity Card  
☒ Fingerprint (BIOAccess)

☐ Expired passwords  
☐ Tokens with invalid data

All Access Levels ▼

Pressing buttons toggles the corresponding search methods:

- By a credential holder's last name
- By a credential type



You can filter the list of credentials to display credentials related to one specific department only. To do that, please select a required department in the dropdown list:

All Departments ▼  
 All Departments  
 Executive Management  
 Sales Department  
 Software Developments  
 Software Testing  
 Technical Support  
 Warehouse

The list of credentials can be also filtered to display only credentials with an assigned access levels. To do that, please select a required access level from the dropdown list:

All Access Levels ▼  
 All Access Levels  
 Simple input  
 20M Local Control  
 20M Local Control - All  
 20M Operator  
 ACS of Department 3  
 Camera Control  
 Configuring 20M  
 Configuring S2000M  
 Local Control 2,4,KDL,10  
 Maximum

Credentials can be filtered by:

- type:

☒ Software Password  
☒ PIN  
☒ Touch Memory Button  
☒ Proximity Card  
☒ Fingerprint (BIOAccess)

- by additional parameters:

☐ Expired passwords  
☐ Tokens with invalid data

### 6.12.1 Creating Passwords for Software Modules

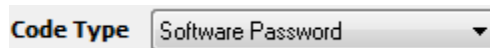
The passwords authorize users to launch software modules of the system.

To add a new Password for Programs, please:

- Click the **Add** button
- Select an employee from the dropdown list to whom you want to assign a password.

A screenshot of a web interface showing a dropdown menu labeled 'Employee'. The selected option is 'Jakson J.'.

- Select the **Software Password** item in the **Code Type** dropdown list:

A screenshot of a web interface showing a dropdown menu labeled 'Code Type'. The selected option is 'Software Password'.

- Enter a code to be used as a software password ( for Orion Pro software modules).

A screenshot of a web interface showing an input field labeled 'Code'. The field contains the text 'xxxxxx'.

- Define a validity period for the password using the **From** and **Till** fields.

A screenshot of a web interface showing two date and time selection fields. The 'From' field is set to '26.06.2013 14:47' and the 'Till' field is set to '31.08.2015 14:47'. Both fields have a '15' icon next to them.

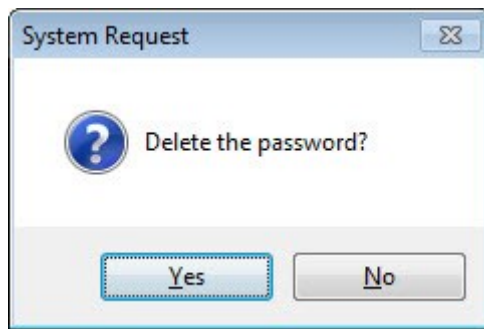
- Set rights to access software modules.

A screenshot of a web interface showing a list of software modules and their access rights. The list includes: Central Server Manager (On), Database Administrator (On), Access to Intrusion and Fire Alarm (On), Access Control (Off), Scenarios (Off), Management Tree (Off), Schedule (Off), Time Zones (Off), Access Levels (Off), Employees (On), Vehicles (On), Credentials (Off), and Operative Task (On). Each item has a small icon to its left and a status indicator to its right.

- Click the **Save** button.

To modify a **software password**, please select a required password in the list of passwords and click the **Edit** button. Then make required changes and click the **Save** button.

To delete a password, please select a required password in the list of passwords and click the **Delete** button. Then click **Yes** to confirm the delete action in the appeared dialog box. Complete changes you want and click the **Save** button.



Settings of the **Software Password** item:

**Employee**

**Code Type**  **Code**

☐ Additional code

**Code Type**  **Code**

**Contact ID**

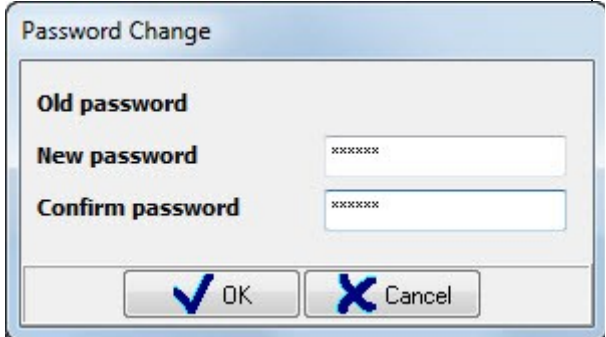
Valid

**From** 26.06.2013 14:47 **Till:** 31.10.2016 14:47

Rights to start programs

- Central Server Manager On
- Database Administrator On
  - Access to Intrusion and Fire Alarm On
  - Access Control On
  - Scenarios On
  - Management Tree On
  - Schedule On
  - Time Zones On
  - Access Levels On
  - Employees On
  - Vehicles On
  - Credentials On
- Operative Task On

Properties	Possible values	Description
Employee	<i>One of the employees in the system</i>	An employee that holds this password. Default value: an employee selected in the list of employees on the Employees tab
Code type	Software Password PIN Codes Touch Memory Button Proximity Card Fingerprint	Code type. <i>The <b>Software Password</b> item must be selected</i> Default value: The same type code as for the credential selected from the list of credentials

		Code	A string length of 6 to 19 characters	<p>A password code</p> <p><i>This code can include alphanumeric Cyrillic and Latin characters.</i></p> <p>To enter a password code, click the <b>Code</b> fields to open the <b>Password Change</b> dialog box:</p>  <p>Default Value: Empty Field</p>
Valid	From		'01.01.1900'...'31.12.2099'	<p>The date when a password validity period begins.</p> <p>Default value: the same date as for the credential entry selected from the list of credential entries</p>
	Till		'01.01.1900'...'31.12.2099'	<p>The date when password expires.</p> <p>Default value: the same date as for the credential entry selected from the list of credential entries</p>
Authorities to Launch Software Modules (*)	Server Manager		On/Off	<p>Authorization to run the Server Manager module.</p> <p>Default value: <b>Off</b></p>
	Database Administrator	Database Administrator	On/Off	<p>Authorization to run the Database Administrator module.</p> <p>Default value: <b>Off</b></p>
		Access to Intrusion and Fire System	On/Off	<p>Authorization to access the following tabs of the Database Administrator module:</p> <ul style="list-style-type: none"> <li>• Device Addresses</li> <li>• Maps</li> <li>• System Structure</li> </ul> <p>Default value: <b>Off</b></p>
		Access Control	On/Off	<p>Authorization to access the Access Control tab of the Database Administrator module</p> <p>Default value: <b>Off</b></p>
		Management Scenarios	On/Off	<p>Authorization to access the Management Scenarios tab of the Database Administrator module</p> <p>Default value: <b>Off</b></p>
		Management Tree	On/Off	<p>Authorization to access the Management Tree tab of the Database Administrator module</p> <p>Default value: <b>Off</b></p>
		Schedule	On/Off	<p>Authorization to access the Schedule tab of the Database Administrator module</p> <p>Default value: <b>Off</b></p>

		Time Zones	On/Off	<p>Authorization to access the Time Zones tab of the Database Administrator module</p> <p>Default value: <b>Off</b></p>
		Access Levels	On/Off	<p>Authorization to access the Access Levels tab of the Database Administrator module</p> <p>Default value: <b>Off</b></p>
		Employees	On/Off	<p>Authorization to access the Employees tab of the Database Administrator module</p> <p>Default value: <b>Off</b></p>
		Credentials	On/Off	<p>Authorization to access the Credentials tab of the Database Administrator module</p> <p>Default value: <b>Off</b></p>
	Operative Task	Operative Task	On/Off	<p>Authorization to run the System Monitor module</p> <p>Default value: <b>Off</b></p>
		Management of Individual Zones	On/Off	<p>Authorization to control individuals zones using maps and relevant tabs/panes in the System Monitor module.</p> <p>Default value: <b>Off</b></p>
		Management of High Security Partitions	On/Off	<p>Authorization to disarm High Security Partitions using the System Monitor module (maps and relevant tabs/panes).</p> <p>Default value: <b>Off</b></p>
		Management of Fire Extinguishing System	On/Off	<p>Authorization to enable/disable AUTO (extinguishing) mode and to activate/abort fire extinguishing for S2000-ASPT and Potok-3N devices.</p> <p>Default value: <b>Off</b></p>
		Operator Privileges	<i>One of the access levels</i>	<p>Privileges defined by an access level to control system entities, and view states and events of the entities in the System Monitor.</p> <p><i>The Process of creating access levels for the System Monitor operator is described in Chapter 6.10.5 Creating Access Levels for System Monitor Operator</i></p> <p>Default value: no access levels selected</p>
		Handle Alarms	On, Off	<p>Authorization to handle alarms in the System Monitor module (mark alarms as Handled, move alarms to archive, and modify alarm attributes).</p> <p>Default value: <b>Off</b></p>
		Time and Attendance	On, Off	<p>Authorization to run the <b>Time and Attendance</b> module</p> <p>If it's toggled, the user will have all authorities to run <b>Time and Attendance</b>: generate reports on all employees of the company, provide advance settings of the client, mark an absence as <b>Authorized</b></p> <p>If this toggle is off, the user can still launch <b>Time and Attendance</b> but generate only his own reports with no access to the client settings; the user can add absence reasons but cannot mark them as Authorized ones</p>



			Default value: Off
	<b>Report Generator</b>	<b>On, Off</b>	Authorization to run the Report Generator module. Default value: Off
	<b>Personal Card</b>	<b>On, Off</b>	Authorization to run the Personal Card module Default value: Off

(\*) **Attention!** An employee's system status also affects the privileges to launch programs (Refer to *Chapter 6.11.1.1 Status*)

Attention! By default, the database includes software password for Smith J. K. with the **Maximum** access level and full set of privileges to run the software modules.

### 6.12.2 Creating PIN Codes

PIN Codes are used by user to get authorized access to perform the following:

- Arm and disarm partitions and partition groups via S200M panel, S2000-K and S2000-KS keyboards, and S2000-BKI indication and control panel
- Enable/disable Auto Mode, and initiate/cancel fire extinguishing process via S2000/S2000M panels and S2000-PT indication and control panel

To add a new PIN code, please:

- Click the **Add** button.
- In the **Employee** dropdown list, select an employee to whom you want to assign a PIN code:

**Employee** Jakson J. ▼

- Select the **PIN code** item in the Code type dropdown list:

**Code type** PIN ▼

- Enter PIN code you want in the **Code** field.

**Code** \*\*\*\*\*

- Define a pin code validity period in the **From** and **Till** fields.

Valid **From** 26.06.2013 15 00:00 15 **Till** 26.06.2015 15 23:59 15

- In the Access Level field, set an access level defining PIN code rights to operate partitions and partition groups, and control fire extinguishing

**Access Level** Maximum

- Specify the location where a pin code will be stored.

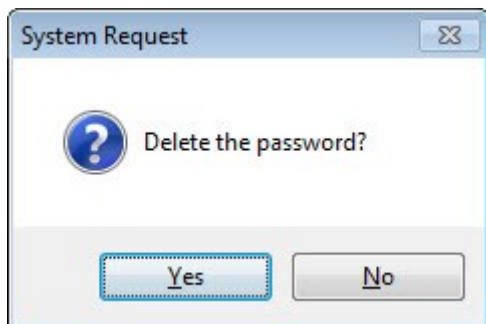
Store token code in S2000M On

Store token code in devices Off

- Click the **Save** button.

To modify a PIN code, please select a required PIN Code from the list of credentials and click the **Add** button. Then make necessary changes and click the **Save** button.

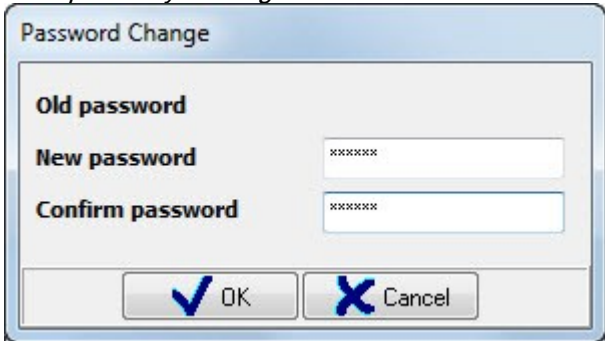
To delete a PIN code, please select a PIN code you want to delete and click the **Delete** button. Then confirm the delete action by clicking **Yes** in the appeared window.



The attributes of PIN Code as a system entity:

A screenshot of a web form for configuring a PIN code. The form has several sections. The top section is for the 'Employee' (Jakson J.) and 'Code Type' (PIN). Below this is a section for 'Additional code' with a 'Code' field. The 'Contact ID' is set to 0. The 'Valid' section shows 'From' and 'Till' dates and times. Below the form, there are links for 'Access Level Maximum', 'Store token code in S2000M On', and 'Store token code in devices Off'. At the bottom, there is an 'Information' section with the text 'Not Available' and a 'Details...' button.

Properties	Possible values	Description
Employee	<i>One of the employees in the system</i>	An employee that holds this credential. Default value: an employee selected in the list of employees on the Employees tab
Code Type	Software Password PIN Code Touch Memory Button Proximity Card Fingerprint	Code type. <i>The PIN Code item must be selected</i> Default value: The same code type as of a credential selected from the list of credentials.

			<p>The Number of PIN Code. <sup>(*)</sup></p> <p><i>A PIN code contains from 4 to 8 digits</i></p> <p><i>Four digits is the most commonly used length for a PIN code.</i></p> <p><i>A PIN code is entered in the Password Change dialog box opened by clicking the Code field:</i></p>  <p>Default value: empty field</p>
Validity Period	From	'01.01.1900'...'31.12.2099'	<p>The date when the PIN code validity begins.</p> <p><i>The validity dates are effective only when system devices are controlled by the Scanning Core module. When the devices are controlled by the S2000M, validity dates are not used. <sup>(**)</sup></i></p> <p>Default value: the same date as for the credential entry highlighted in the list of credentials</p>
	Till	'01.01.1900'...'31.12.2099'	<p>The date when the PIN code validity expires.</p> <p><i>The Period of validity is used only when system devices are controlled by the Scanning Core module. When the devices are controlled by S2000 and S2000M validity dates are not effective. <sup>(**)</sup></i></p> <p>Default value: the same date as for the credential entry highlighted in the list of credentials</p>
Access Level		<i>One of the access levels in the system</i>	<p>The access level defining rights of the PIN code to operate partitions and fire extinguishing control systems.</p> <p>Default value:</p> <ul style="list-style-type: none"> <li>The access level of the PIN code selected from the list of credential entries (credentials of employees), If a selected credential is a PIN code</li> <li>If any other type of credential is selected (highlighted), an access level is not defined.</li> </ul>
Store token code in S2000M		On, Off	<p>This parameter defines whether the PIN code is exported when the database is exported to the S2000M</p> <p>Default value: <b>Off</b></p>
Store token code in devices		On, Off	<p>This parameter defines whether to store a PIN code in devices.</p> <p>Attention! Now, one can use PIN codes for local control in the Signal-20M device only. The Orion Pro Software does not support the synchronization of its credentials with this device. Thus, this parameter is not used so far.</p> <p>Default value: <b>Off</b></p>

(\*) The acceptability of PIN code values depends on the **Disable duress code check** parameter. By default, this option is not enabled, thus, the PIN codes different by one digit only cannot be entered to the database (for example 1111 and 1112).

*(Description of the database parameters is provided in Chapter 6.14.1 Settings of Database Administrator.)*

### 6.12.3 Creating the List of Touch Memory Buttons, Proximity Cards and Fingerprints

Touch Memory buttons and Proximity cards are used for Access Control, Intrusion and Fire systems. Fingerprints are used for Access Control only.

To add new credentials such as Touch Memory button, Proximity card or Fingerprint, please:

- Click the **Add** button.
- In the Employee dropdown list, select a person with whom you want to assign a credential.

**Employee**  ▼

- Select Touch Memory button, Proximity card, or Fingerprint in the **Code type** dropdown list.

**Code type**  ▼

- Enter the code of Touch Memory button, Proximity card or Fingerprint in the **Code** field:


**Code**  

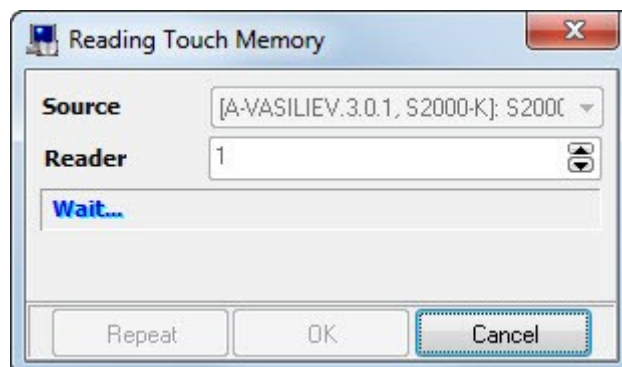
The codes of Touch Memory buttons and Proximity cards can be entered manually or taken from a reader of a relevant device.

Please note that:

- The Database Administrator verifies checksum of the entered code (credential). If the code is invalid it won't be saved.
- The Database Administrator does not interact with devices directly. All code reads are performed by Scanning Cores as instructed from the Database Administrator. Therefore, to obtain a credential code, the Scanning Core has to be launched on a workstation where the device is connected to.
- Type and model of readers (connected to the devices to be scanned (read) by the Scanning Core, and those connected to devices that will be used to control ACS and IFS components) must match (or the readers must send the same token code).

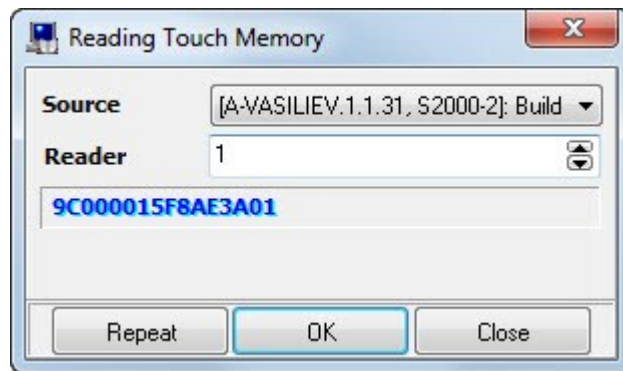
To read a token code with a reader, please:

Click the  button to open the Reading Touch Memory dialog box. Select a device in the Source field, and a reader in the Reader field which will be used to read the code of a Touch Memory button or Proximity card.



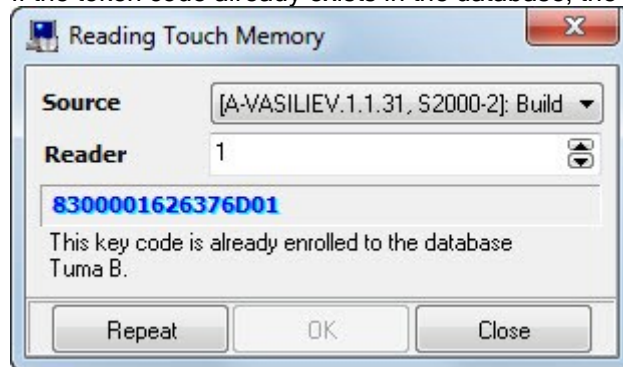
The dialog box titled "Reading Touch Memory" has a close button (X) in the top right corner. It contains two dropdown menus: "Source" with the value "[A-VASILIEV.3.0.1, S2000-K]: S2000" and "Reader" with the value "1". Below these is a text field containing "Wait...". At the bottom are three buttons: "Repeat", "OK", and "Cancel".

- Present a button/card to a reader



- Click the **OK** button.

If the token code already exists in the database, the following will appear.



In this case, you can initiate a token read again by clicking the Repeat button.

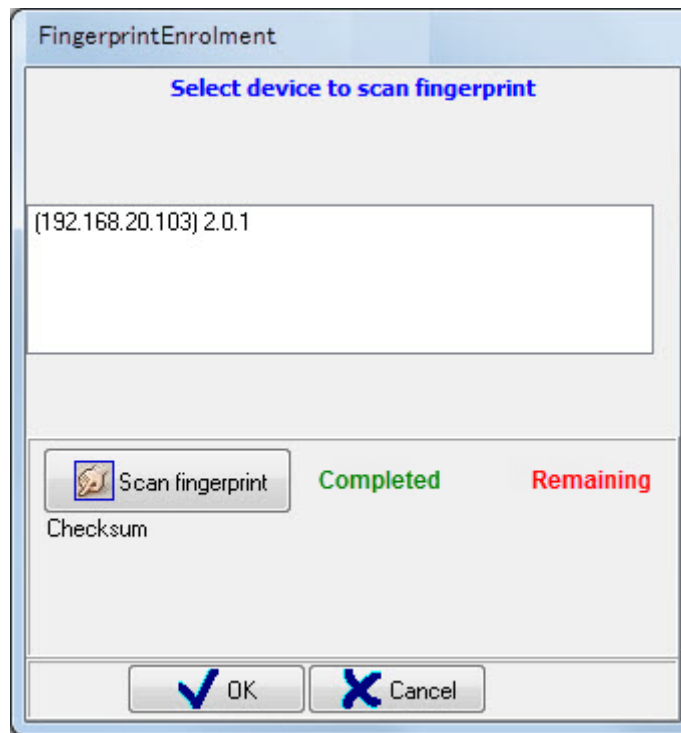


Fingerprints are enrolled to the database using a biometrics reader. Please be mindful of the following:

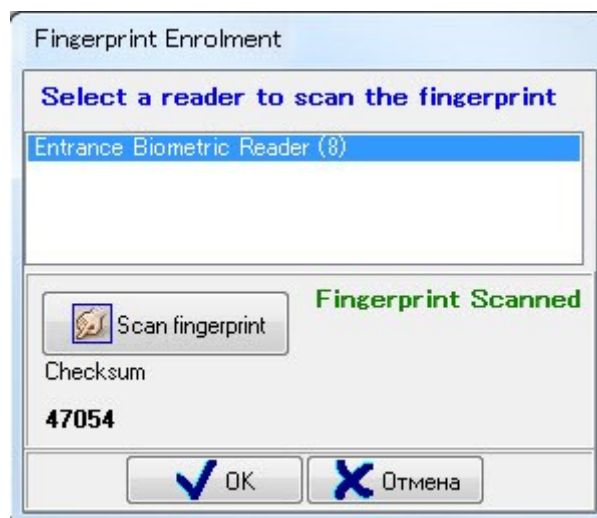
- The Database Administrator module does not work with devices directly. All code reads are performed by Scanning Cores as instructed by the Database Administrator. Therefore, to obtain a credential code, Scanning Core has to be launched on a workstation where the device is connected.

To scan a fingerprint, please:

- Click the  button
- Click the  button in the appeared dialog box.



- Place a finger on a reader three times



*Attention! When presenting a fingerprint to a reader please consult the information displayed in the Database Administrator module rather the messages on the device display. That is, when you present a finger to a reader the second/third time, please wait till relevant information appears in the Scanning Fingerprint dialog box.*

- Click the OK button.

If a Scanning Core responsible for a token/fingerprint read device is not launched, the Database Administrator log will show a relevant message:

Date	Time	Description
30.03.2009	13:20:03	Socket Error # 10061   Connection refused

- If readers function as two-factor authentication facilities where the user shall present two types of credentials, additional verification code shall be provided. To do that, please select the

**Additional code** checkbox, and choose TM/Proximity and PIN code (for keypad readers) in the **Code type** field, then enter PIN code or token/code in the **Code** field.

☒ Additional code

**Code Type** PIN **Code**

- Select the validity period for tokens in the fields **From** and **Till**.

Valid

**From** 26.06.2013 00:00 **Till** 11.10.2014 23:59

- Set parameters for the credential you create.

Access Level Arming Room 1

Store token code in devices On

Store token code in console Off

Suspended token Off

Token type Main

Stop list Off

- Click the **Save** button.

To edit a Touch Memory button, Proximity card or Fingerprint, please select a required credential and click the **Edit** button. Make necessary changes and click the **Save** button.

To delete a Touch Memory button, Proximity card, or Fingerprint, please select a required Touch Memory button, Proximity card, or Fingerprint and click **Delete**, and then click **Yes** in the appeared dialog box to confirm the action.

Let's consider parameters of tokens (Touch Memory button, Proximity card) and Fingerprint:

**Employee** Jakson J.

**Code Type** Touch Memory Button **Code** 2B00000BCE3CB301

45884 Wiegand16

☐ Additional code

**Code Type** **Code**

**Contact ID** 0

Valid

**From** 26.06.2013 00:00 **Till** 27.06.2016 23:59

Access Level Department Work Schedule

Store token code in devices Off

Store token code in S2000M Off

Suspended token Off

Token type Main

Stop List Off

Information

**Not Available** Details...

Parameter		Possible values	Description
Employee		<i>One of the employees in the system</i>	An employee that holds this credential.  Default value: an employee selected in the list of employees on the Employees tab
Code Type		Software Password PIN Code Touch Memory Button Proximity Card Fingerprint	Code Type.  <i>One of the <b>PIN Code, Touch Memory Button, Proximity Card, or Fingerprint</b> credentials must be selected</i>  Default value: The same type code as for a credential entry selected from the list of credential entry.
Code		<i>A number of code or checksum</i>	A token code or fingerprint checksum.  Default value: empty field
Additional Code	Additional Code	<input type="checkbox"/> (no), <input checked="" type="checkbox"/> (yes)	This defines whether an additional code is to be used.  Default value: <input type="checkbox"/> (no)
	Code Type	TM/Proximity PIN Code	Type of additional code.  Default value: empty
	Code	<i>Code of a token or finger print</i>	A PIN code, token, or finger print used as additional credential.  <i>A PIN code contains from 1 to 8 digits</i> Default value: empty field
Validity Period	From	'01.01.1900'...'31.12.2099'	Date when the token/fingerprint, PIN code validity period begins  <i>Validity period is used in the following cases:</i> <ul style="list-style-type: none"> <li>➤ When access control, arming/ disarming partitions and partitions groups, extinguishing control are performed using the Scanning Core module (centralized control)</li> <li>➤ When access control functions and arming and disarming of loops are provided locally using standalone devices (local control).</li> </ul> <i>When arming/disarming and control of fire extinguishing system are performed using S2000 or S2000M Panels, the dates of validity is not used.</i>  Default value: The same date as for credential selected in the list of credential entries
	Till	'01.01.1900'...'31.12.2099'	Date when the validity period of a token/fingerprint expires:  <i>Validity period is used in the following cases:</i> <ul style="list-style-type: none"> <li>➤ When access control, arming/ disarming partitions and partitions groups, extinguishing control are performed using the Scanning Core module (centralized control)</li> <li>➤ When access control functions and arming and disarming are provided locally using standalone devices (local control).</li> </ul> <i>When arming/disarming and control of fire extinguishing system are performed using S2000 or S2000M Panels, the dates of validity is not used.</i>  Default value: The same date as for credential selected in the list of credential entries.
Access Level		<i>One of the access levels in the system</i>	The access level defines rights of a token holder to



		<p>operate the components of access control, intrusion detection and fire protection systems.</p> <p><i>Attention! If <b>Simple input</b> is selected as an access level, a token or fingerprint is considered an operative credential (and rights for such a token shall be defined in the field appeared underneath (Refer to Chapter 6.12.3.1 Use of Touch Memory Button, Proximity Card or Finger Print as an Operative Credential))</i></p> <p>Default value:</p> <ul style="list-style-type: none"> <li>When a pin code credential is selected from the list of credentials, an access level will be the same as for the PIN code selected from the list of credentials entries;</li> <li>Otherwise, an access code is not defined</li> </ul>
Store token code in device	On, Off	<p>This option defines whether to store a token code in devices or not.</p> <p>If a token's access level includes access control rights, this option defines whether this token code will be written to a device (S2000-2 or S2000-4) in case of synchronization. In other words, this parameter defines the type of access control: local or centralized.</p> <p>If a token's access level includes IFS control rights:</p> <ul style="list-style-type: none"> <li>➤ When they include privileges to arm and disarm loops of a specific device only (S2000-2 (version 1.05) or S2004), this options defines where the code token will be written to a device in case of synchronization.</li> <li>➤ When the rights include privileges to arm/disarm partitions that include loops of other devices (S2000-KDL and Signal, etc) or loops of several devices, this option is ignored, tokens are not written to devices; and if databases is to be exported to the S2000M panel, token export depends on the <b>Store token code in the S2000M</b> option.</li> </ul> <p><i><u>Attention!</u> This feature is not accessible for fingerprints. A fingerprint is always stored in devices.</i></p> <p>If a token's access level include rights to operate both ACS and IPS elements, the combination of the above rules determines how a token code is stored in devices, including the situations, when a token code with access control rights is stored in ACS devices, but will not be stored in IFS devices.</p> <p>Default value: <b>Off</b></p>
Store token code in S2000M/Console	On,Off	<p>This parameter defines whether a token code is to be exported while the database is exported to the S2000M panel.</p> <p><i>Attention! This feature is not available for fingerprint credentials.</i></p> <p>Default value: <b>Off</b></p>
Suspended token	On,Off	<p>This parameter defines whether to suspend a token /fingerprint or not.</p>

		<i>Suspension of a token is quite a rare situation.</i> Default value: <b>Off</b>
Token type	<b>Basic Master, Free Access Lockdown</b>	Type of token.  The Basic type is the most common type of tokens  Free Access token is used to switch a controller (S2000-2 or S2000-4 version 2 or higher) to the <b>Open Access</b> mode (free access through an operated access point). Lockdown token locks down the readers of a controller.  The MASTER token is used to configure tokens locally in a device itself  <i>Attention! This feature is not available for the fingerprint credentials.</i>  Default value: <b>Basic</b>
Stop-List	<b>On, Off</b>	This parameter defines whether a token is enrolled a stop-list or not  A user with a token enrolled in a stop list will be granted an access in accordance with an access level but an alert message will be generated to this effect. <i>Attention! This feature is not available for fingerprints.</i>  Default value: <b>Off</b>

*Synchronization of credentials (Touch Memory buttons, Proximity cards and fingerprints) and device configurations are described in Chapter 6.12.4 Synchronizing Credentials of the Database and Access Controllers)*

#### 6.12.3.1 Use of Touch Memory Buttons, Proximity Cards, and Fingerprints as an Operative Credentials

The Orion Pro software supports creation of operative tokens and fingerprints by selecting **Simple Input** as an access level.

In this case, the rights are defined in the credential itself (in the appeared field) rather than by an access level:

The screenshot displays the Orion Pro software interface for configuring credentials. The top section shows a list of configuration options for a credential:

- Access Level: Simple Input
- Store token code in devices: Off
- Store token code in S2000M: Off
- Suspended token: Off
- Token type: Main
- Stop list: Off

Below this, there is a section for Access Points and Time Zone. The Access Points section shows a list of points with their corresponding icons and names:

- [1]: Entry turnstile
- [2]: Exit turnstile
- [3]: Canteen/Smoking Room Door
- [4]: Canteen/Smoking Room Door
- [5]: Door 5

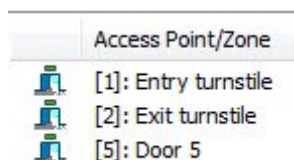
The Time zone section shows a dropdown menu for selecting the time zone.

Please, note the rights assigned to operative credentials are not shown in the list of access levels. These rights will be deleted when a credential entry is deleted (or when any access level is associated to the credential). The credential-related rights can be edited in the same mode as of credentials).

Please keep in mind, that the list of rights is defined by the list of access points accessible for an employee as well as by the period of validity.

The relevant area (displayed when the **Simple Input** option is selected as an access level) will include the following:

- The list of access points added to the list of credential-assigned rights:

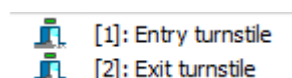


- The tree of a system's access points:



The list of access points added to the credential rights will show the following information for each system entity:

- Number
- Name



To add a new entity to the list of credential rights, please do the following:

- Select a required entity in the tree of access points.
- Double click or drag it to the list of credential-assigned rights.

You can add all access points to the list of credential-assigned rights ( Access Points) by dragging , the **Access Points** node to the list.

To delete an entity from the list of credential rights, please do the following:

- Select a required entity in the list of credential rights.
- Click the <Del> key on the keyboard, then confirm the deletion by clicking **Yes** in the appeared dialog box:

#### 6.12.4 Synchronizing the Credentials of the Orion Pro Database and Access Controllers

To synchronize credentials (Touch Memory buttons, Proximity cards, and fingerprints) of the database and devices configurations, the following should be completed:

- Make sure that you have launched the Scanning Cores that control devices you want to synchronize with;
- Configurations have to be read from devices you want to synchronize;
- The status has to be obtained for database credentials you want to synchronize.

All these actions, as well as the processes of synchronization, search of token duplicates in the database and devices, and search of extra tokens in devices are described in Chapter 6.12.4.1- 6.12.4.6.

#### **6.12.4.1 Reading Configurations from Devices. Obtaining the Status of Credentials**

As said above, to synchronize the list of credentials, the device configuration has to be read from devices and the status of database credentials has to be obtained.

This chapter focuses on these actions.

To read configuration from devices, first you have to launch Scanning Cores that control the devices.

**Attention!** The Database Administrator does not interact with devices directly. The Scanning Cores are responsible for work with devices following the instructions of the Database Administrator. Configuration read results are stored in relevant Scanning Cores.

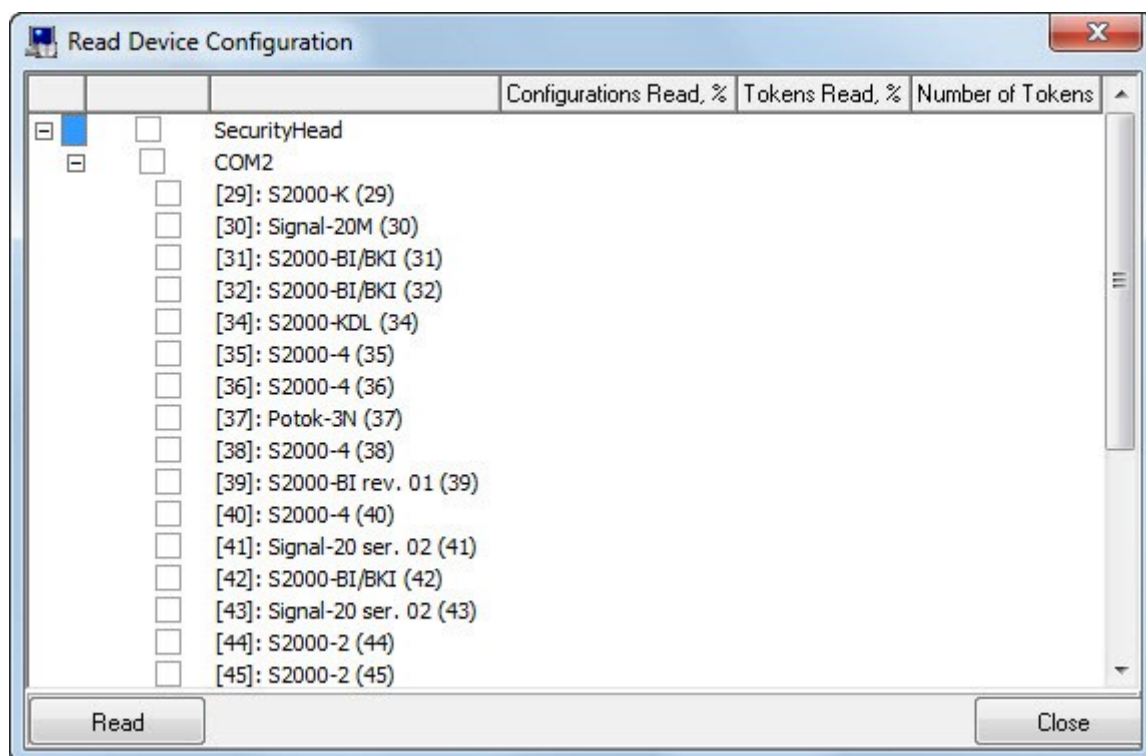
## IMPORTANT!

To expedite the process of configuration reading, all read configuration data and credentials are saved as files in **Defconf** folder located in the root folder with installed Orion Pro on a corresponding workstation.

When Scanning Core is launched, configurations (and the list of credentials) are loaded automatically from the files. When the Database Administrator initiates a command to read configurations, configurations will be read from a device followed by the immediate replacement of configuration files. Thus, in most cases to read configuration is necessary for the first system startup as well as for device reconfiguration using Uprog.

Please proceed with the following actions to read device configurations:

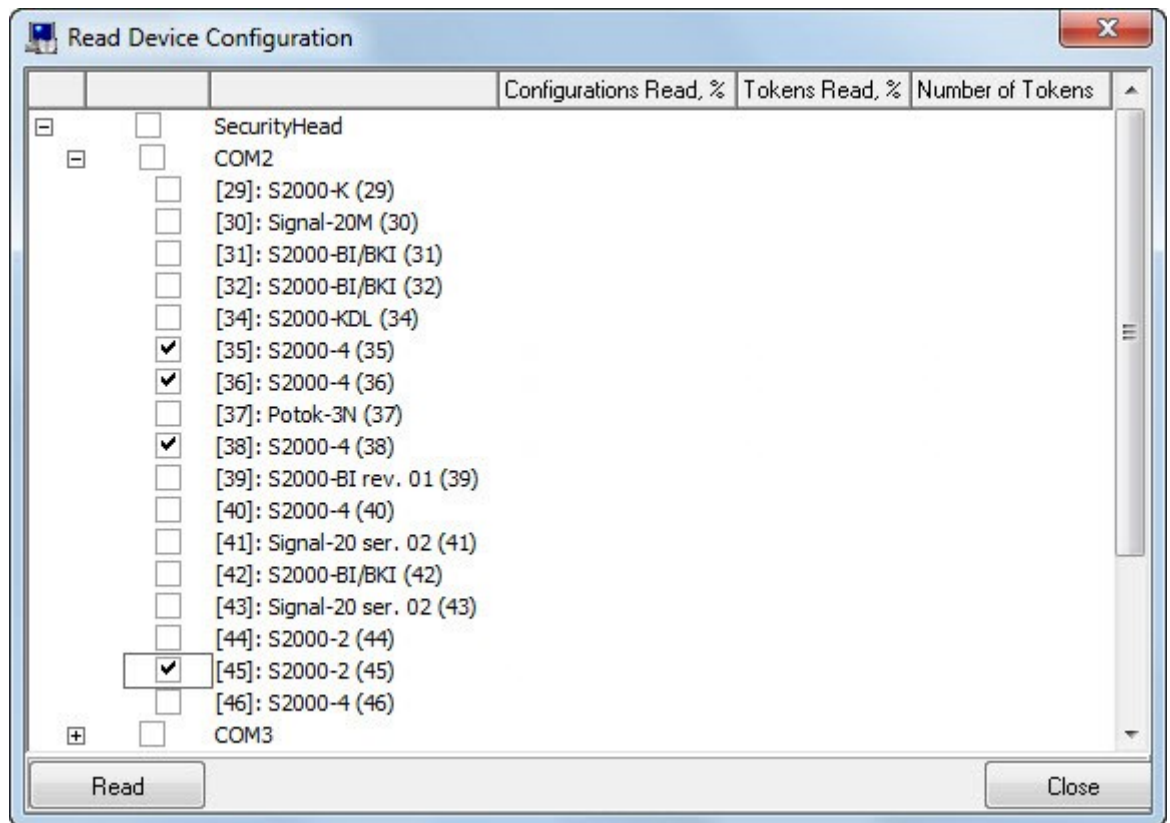
- Go to Service / Read Device Configuration to open the **Read Device Configuration** window



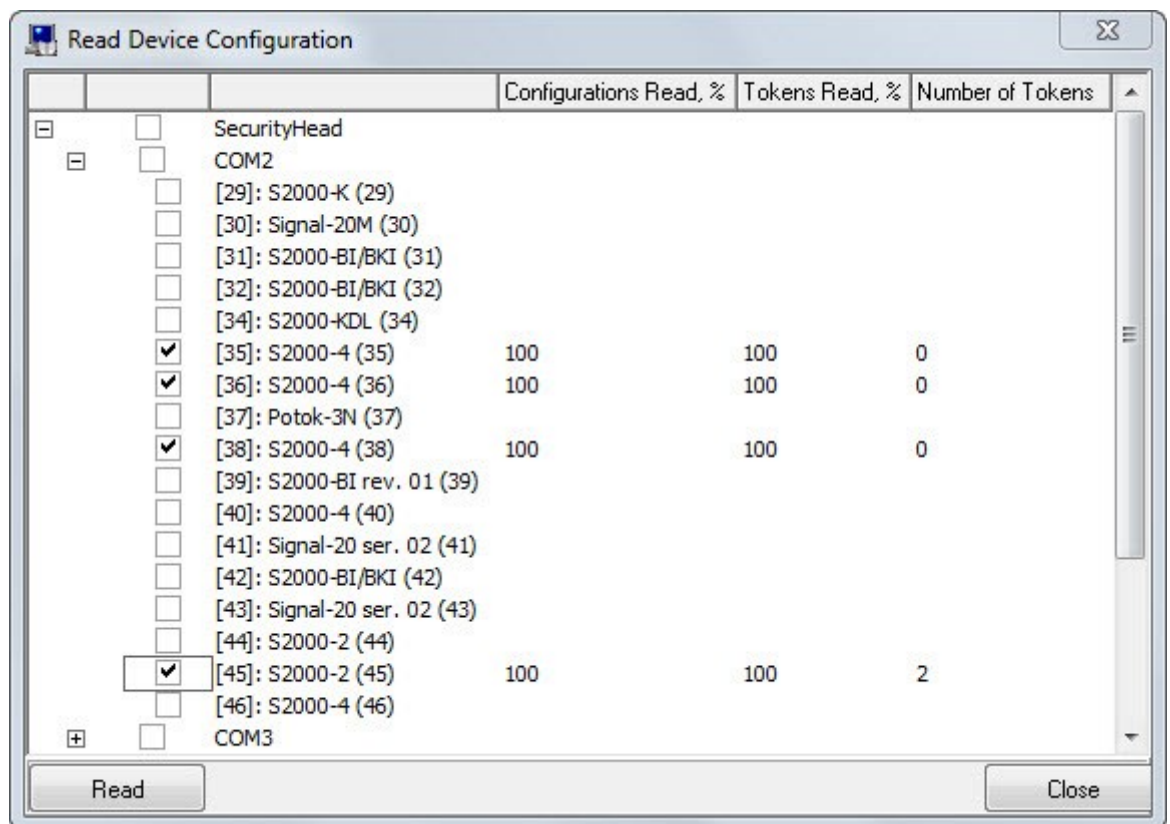
Before opening this window, the Database Administrator will attempt to connect to all Scanning Cores. If any of Scanning Core is not running or failed to start, the Database Administrator Log will show a relevant message:

Date	Time	Description
10.02.2015	16:10:08	Method GetDeviceConfigurationStatus computer Support-11-57 (192.168.11.57): ...
10.02.2015	16:10:17	Method GetDeviceConfigurationStatus computer Support-11-57 (192.168.11.57): ...

- Select required devices in the following list:



- Click the **Save** button.
- Wait until configurations and credentials have been read:



- Click the Close button.

*Attention!*

*Since the configuration read results (and list of credentials) is stored in Scanning Core, the procedures to read configuration shall be performed after Scanning Core has been launched.*

*In other words, if Scanning Core is running permanently and a configuration (and the credentials list) has been read, there is no need to read the configuration once more when the Database Administrator starts.*

*Please be mindful that the Credentials can be synchronized only with the following devices: S2000-2, S2000-4, Signal-10, S2000-BIOAccess, and keyboxes. Therefore, there is no sense of reading configurations from other devices.*

Please, be advised for proper analysis display of the compliance between credentials stored in the database and credentials stored in devices, the status of credentials must be obtained from Scanning Core.

To do that, please toggle the Credentials tab, and then select **Service/ Read Status of Tokens** (press the <F9>key)

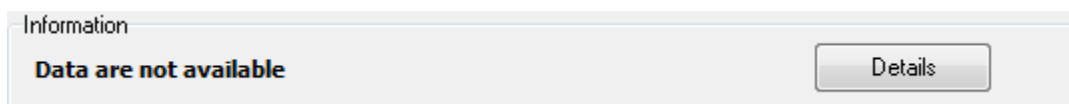
The relevant information on actions taken will be displayed in the Database Administrator Log:

Date	Time	Description
19.09.2014	15:53:30	SecurityHead ( 192.168.20.3 ): Compare data in database and devices is carried out
19.09.2014	15:53:30	SecurityHead ( 192.168.20.3 ): Compare data in database and devices completed

The Database Administrator can be configured to request the status of credentials automatically when one toggles the Credentials tab. To achieve that, please select the **Check the status of credentials when switching to the Credentials tab** item of the Database Administrator settings (Refer to 6.14.1 Settings of the Database Administrator)

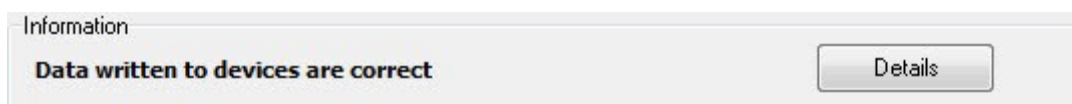
All expired Touch Memory and Proximity tokens and fingerprints are displayed red in the list of credentials.

Until the status of credentials is obtained, all other tokens are displayed black along with related information for each token or fingerprint:



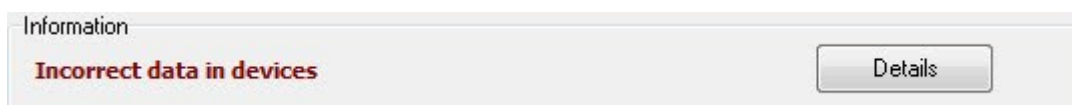
To read a token or fingerprint status, please do the following:

- If the credential data stored in the database match those stored in devices the following message will be displayed:



and the relevant credentials will be displayed in black font color in the list of credentials entries;

- If the information of credentials stored in the database does not comply with data of those stored in devices, the following will be displayed:



and the credentials entries will be displayed in brown font color in the list of credentials entries.

#### 6.12.4.2 Configuring Time Zones and Access Levels in Controllers

Matching of data base settings with the info stored on devices requires controllers to store up-to-date info on appropriate access levels in addition to user credentials (for S2000-2, S2000-BIOAccess devices and keyboxes) and on time zones( for S2000-2, S2000-4, S2000-BIOAccess devices and keyboxes). Access levels and time zones are saved to devices automatically. Also, access levels and time zones can be saved manually in S2000-2 and S2000-4 devices.

This chapter focuses how to save/write access levels and time zone in devices manually in the Database Administrator module.

**Attention!**

In order to add access levels and time zone to devices properly, please make sure that your Scanning Cores have the latest database changes loaded.

If access levels and times zones have been edited, no preparatory actions are needed to start configuring time zone and access levels in devices.


If the changes have been made for access points or association of access points with readers, the data in Scanning Cores have to be updated.

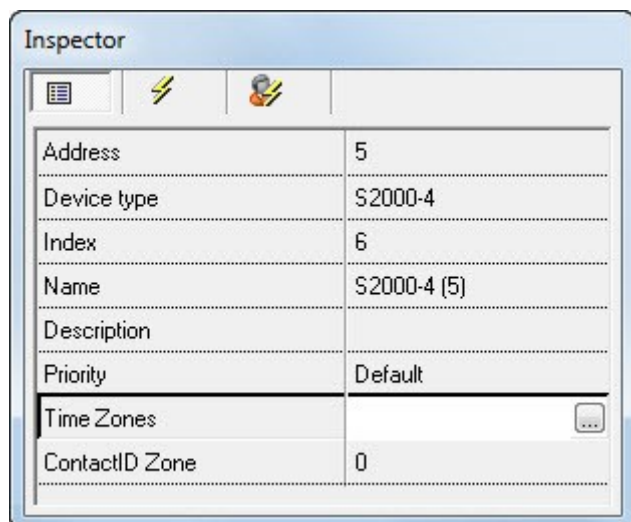
**Attention!**

*First, time zones have to be added to a device before you proceed with adding access levels.*


To write times zone to a device, please

Select a required S2000-2 or S2000-4 device

Click the **Edit** button to enable the editing mode, then select the **Time Zones** item, and click the  button.

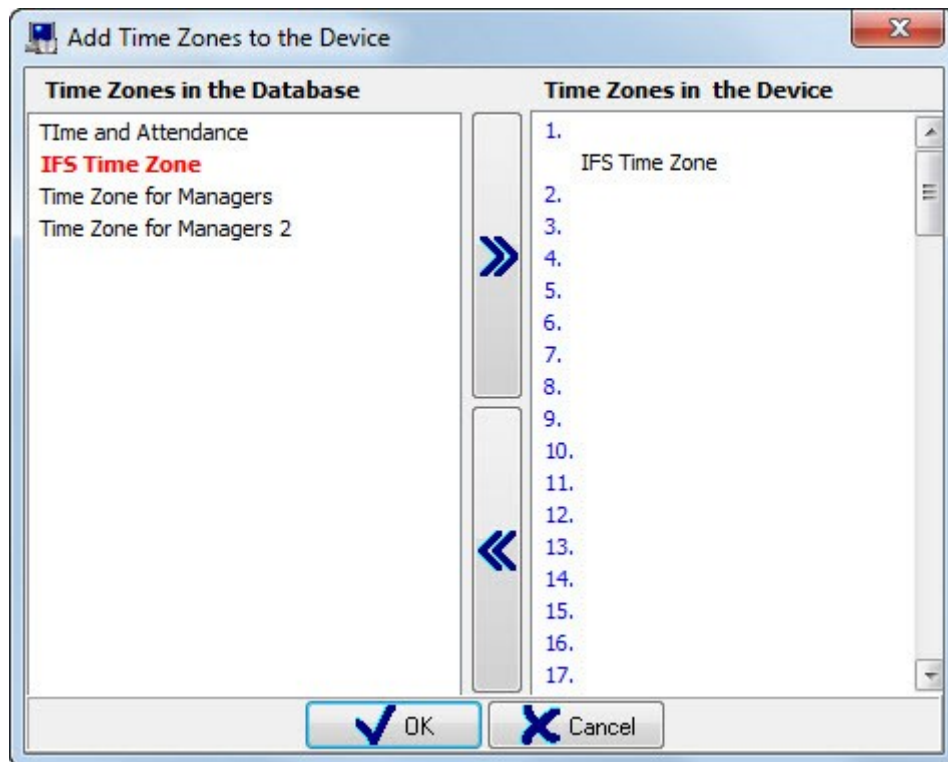


The image shows a software window titled "Inspector". It contains a table with the following fields and values:


Address	5
Device type	S2000-4
Index	6
Name	S2000-4 (5)
Description	
Priority	Default
Time Zones	
ContactID Zone	0

- The **Add Device Time Zones** dialog box will appear:






The left pane of the dialog box includes the time zones stored in the database, and the right pane included the time zones stored in the device.

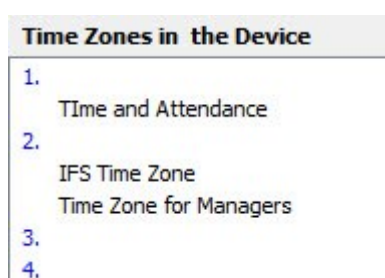
- To add a time zone, please select a required time zone in the list of time zones stored in the database, and click the  button, or
- Double click a required time zone in the list of time zones
- Click a required time zone and hold the mouse button to drag the time zone to the list of time zones stored in a device.

To remove a time zone from a device, please select a required time zone in the list of time zones

stored in the device and click the  button.


- Select a required time zone in the list of time zones stored in the device, and then press the <Del> key on the keyboard.
- Click the OK button.
- Then click the **Save** button to save all changes and quit the editing mode.

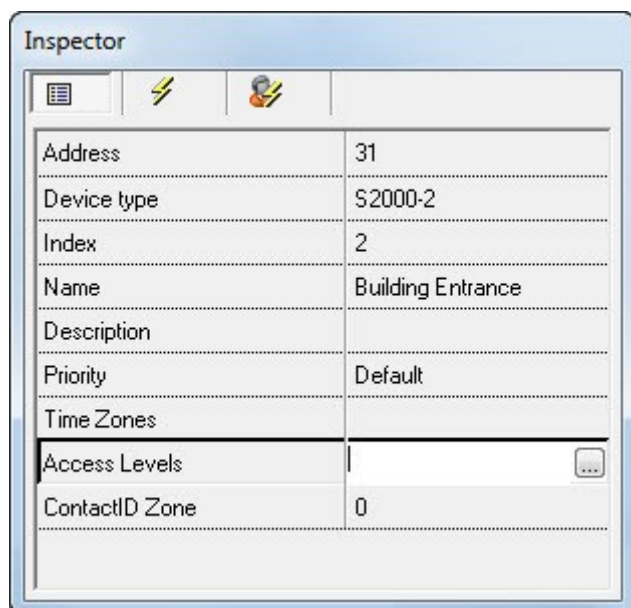
If there are two or more identical time zones, but a device includes one of these time zones, the list of time zones will show all these identical time zones if it includes one of them.




To add an access level to a device, please:

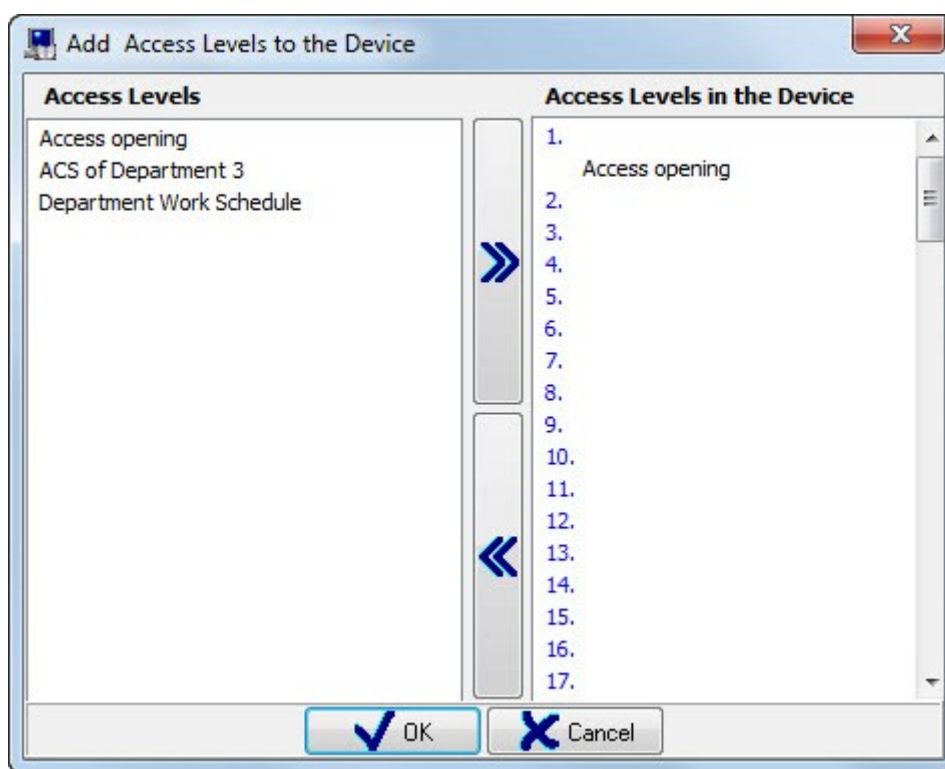
Select a required S2000-2 device in the tree of devices in the Device Addresses tab (or System Structure) If necessary, add time zone first.

- Click the **Edit** button to enable the editing mode; select the Access Levels item and click the  button.



Inspector	
Address	31
Device type	S2000-2
Index	2
Name	Building Entrance
Description	
Priority	Default
Time Zones	
Access Levels	
ContactID Zone	0

- add an access level to the device in the appeared dialog box.



**Add Access Levels to the Device**

**Access Levels**

Access opening  
ACS of Department 3  
Department Work Schedule

**Access Levels in the Device**

1. Access opening  
2.  
3.  
4.  
5.  
6.  
7.  
8.  
9.  
10.  
11.  
12.  
13.  
14.  
15.  
16.  
17.


OK

Cancel


The left part of the appeared dialog box shows the list of access levels stored in the database (to be added to the device as required in accordance with the database settings), the right part contains the access levels stored in the device.

*If the list of access levels does not show any of the access levels, this access level is not the subject of inclusion to a device in accordance with the database settings related to the access levels and access points*

To add an access level to a device, please do the following:

- Select a required access level in the list of access levels stored in the database and click the  button.
- or
- Double click a required access level in the list of access levels stored the database settings
- Click a required access level and hold the mouse button to drag the access level to the list of access levels stored in devices.

To delete an access levels from a device, please select a required access level in the list of

access levels stored in the device and click the  button.

- Select a required access levels in the list of access levels in the device, then press the <Del> key on the keyboard.
- Click the OK button.
- Then click the **Save** button to save all changes and close the window.

*Attention!*

*Please be mindful that the deletion of an access level or time zone may lead to the need of synchronizing tokens.*

It also must be understood, that two or more access levels (different on their appearance) may be identical with respect to one specific device.

For example, the database includes the following entries:

- Two two-way access point AP1 and AP2, where each is controlled by S2000-2 device.
- Two access levels:
  - The first access levels allows entry and exit through both access points in time defined by time zone TZ1
  - The second access level allows entry and exit through AP1 in time periods defined by time zone TZ 1

Both access levels are identical for the S2000-2 device controlling the AP1 access point, as they include the same access rights for the AP1 access point.

When two or more access levels are treated by the same S2000-2 device as identical, and this device includes one of these access levels, the list of device-added access levels will show those identical access levels (as apply to the device) along with the name of this level.

#### Access Levels in the Device

1. Department Work Schedule
2. Access opening  
ACS of Department 3
- 3.
- 4.

#### 6.12.4.3 Synchronizing the List of Credentials in the Database and Devices

To synchronize the credentials of the database and the device configurations

To synchronize credentials (Touch Memory buttons, Proximity cards, and fingerprints) of the database and devices configurations, the following prerequisites should be completed:

- Make sure that you have launch Scanning Cores controlling the devices you want to synchronize with;
- Device configurations have to be read from the devices you want to synchronize (from the devices itself or from the catch);
- The status of the database-stored credentials has to be obtained.

*Attention!*

*The synchronization of the database-stored credentials can be done only with connected devices provided their configurations have been read.*

Attention!

In order to have configurations saved to devices properly, all Scanning Cores have to get all recent databased changes loaded.

If any changes have been made with access levels, times zones, credentials or employees before synchronization, no preparatory actions are needed to start synchronization of credentials.

If the changes have been made with other items (access points or association of access points to readers), the data in Scanning Cores have to be updated.

Next, we will discuss the possible options of synchronization of credentials, employees, time zones, or access levels:

Option 1:

- Device configuration has been read.

In this case, no additional efforts are required to add/edit/delete tokens and fingerprints or add/edit/delete employees, time zone and access levels. Synchronization will be done automatically.

Option 2:

- Device configuration has not been read.

When keys/cards/fingerprints/employees/time zones/access levels are added/edited/deleted, such configuration device reads must be followed by individual synchronization of specific keys/cards/fingerprints or system-wide synchronization of credentials.

Attention! In this case, the deletion of a token/fingerprint is not recommended.

More details for both options:

The database is updated automatically in the Scanning Core, if changes were applied to the following:

- The list of credentials
- The list of employees
- The list of time zones
- The contents of access levels

When changes are made for any other database entities, the total update of database information in Scanning Cores is required before any actions with the above lists.

Attention!!! The information of this chapter is applicable only to the local control. In case of centralized control, synchronization is not required. The database update is provided following the same logic (as describe in the previous para).

#### 6.12.4.3.1 Synchronization of One Credential with Devices

*This chapter discusses the synchronization of a single credential. Actions preceding synchronization are described in Chapter 6.12.4.3 Synchronization of the List of Credentials in the Database and Devices.*

To synchronize codes and rights of a credential, the following prerequisites have to be completed:

- Make sure that you have launched Scanning Cores controlling devices you want to synchronize with;
- Configurations have to be read from the devices you want to synchronize (from the devices itself or from the cache) ;
- The status of the database credentials has to be obtained.

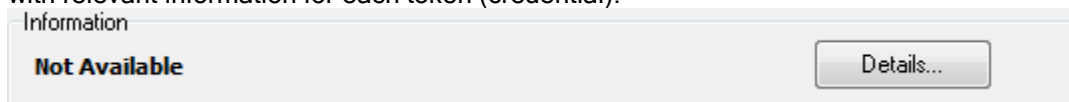
**Attention!**

*The synchronization of the database-stored credentials can be done only with connected devices provided their configurations have been read.*

*This chapter assumes that at least one device's configuration has been read beforehand.*

The Database Administrator can be configured to request status of credentials automatically when one toggles the Credentials tab. To achieve that, please select the **Check the status of credentials when switching to the Credentials tab** item of the Database Administrator settings (Refer to 6.14.1 Settings of the Database Administrator)

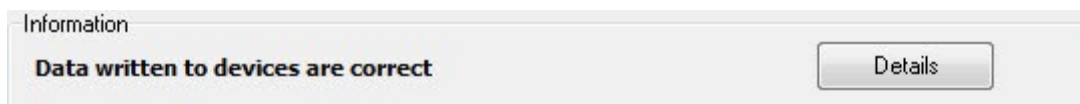
Till status obtained, all credential entries (except of expired ones) are displayed in black font color along with relevant information for each token (credential):



In this case, the synchronization is impossible.

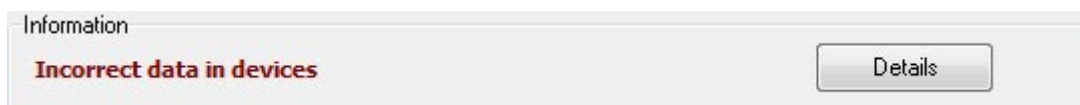
To read the status of a credential, please do the following:

- If the information of credentials stored in the database complies with that stored in devices, the following will be displayed for such credentials:



And the credentials entries will be displayed black in the list of credentials entries;

- If the information of credentials stored in the database does not comply with data of those stored in devices, the following information will be displayed:

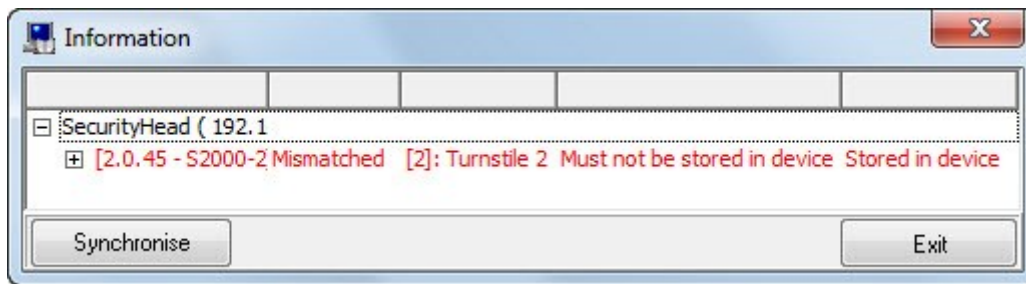


and the credentials entries will be displayed brown in the list of credentials entries.

In this case, the synchronization is required.

**Attention!** The synchronization of one token or fingerprint is performed in the **Information** dialog box opened by clicking the **Details** button.

To synchronize a token/fingerprint, please select a required token/finger print from the list of credential entries and click the **Details** button to open the Information dialog box. (The **Details** button is not active when the mode of editing is enabled)



When opened, the Information dialog will display information of the following activity

Date	Time	Description
3/20/2015	5:05:31 PM	SecurityHead ( 192.168.20.103 ): Obtaining list of time zones from device is in progress
3/20/2015	5:05:31 PM	SecurityHead ( 192.168.20.103 ): Obtaining list of time zones from device completed

#### Attention!

The information window contains only those devices that must store tokens or fingerprints in accordance with the database settings.

*Exceptions are devices that store code of tokens or fingerprints, but in accordance with the database settings shouldn't do that.*

If no device of a workstation has to store credentials, this workstation will not be displayed.

Hence, if the Information window displays no device after a device configuration read, this is because of the settings of the database. If this is not as expected, one should check the database settings for the following:

- Access points
- Associations of access points to the readers of system devices
- Access levels
- The **Store token codes in devices** parameter

The Information window displays the following information on the **Workstation** component:

SecurityHead ( 192.168.20.103 ): I

- Name,
- IP Address.

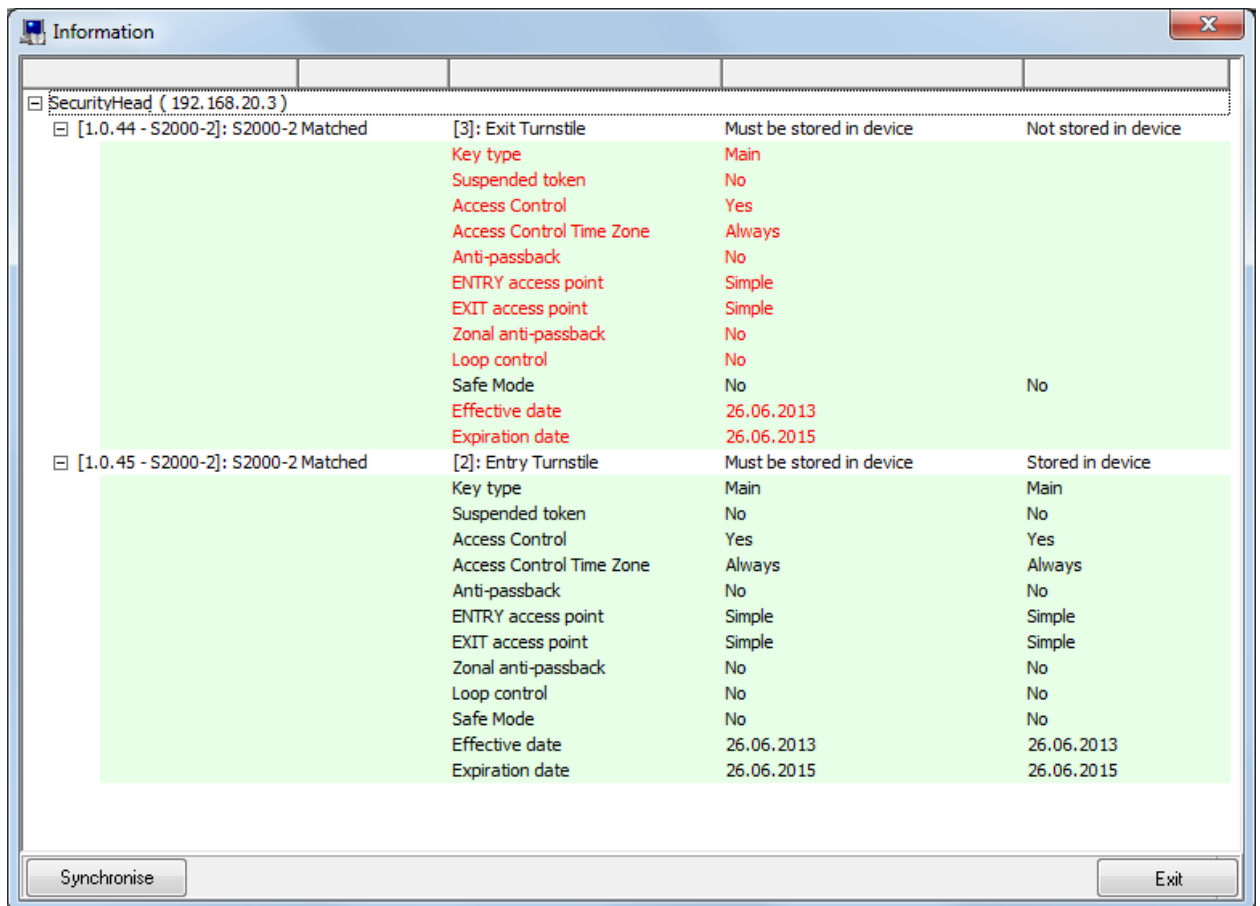
The Information window displays the following information for the Device entity:

[2.0.45 - S2000-2]: S2000-2 (45) Matched [2]: Turnstile 2

- Address
- Type
- Name
- Conformity of between database settings and the credential details stored in devices
- The name of access point(s) controlled by the device

Also for each device:

- The list of configuration parameters store in the devise is displayed underneath the name of an access point
- The **Must be stored in device** column displays parameters that must be stored in the device in accordance with the database settings
- The **Stored in device** column display parameters actually stored in the device



There are several versions of conformity between the credential settings stored in the Database and those in a specific device.

#### Version 1:

If a device configuration have been read and the credential settings in the database match those stored in the device, all parameters will be shown black:

Key type	Main
Suspended token	No
Access Control Time Zone	Always
Anti-passback	No
ENTRY access point	Simple
EXIT access point	Simple
Effective date	26.06.2013
Expiration date	26.06.2015

No actions are required in this case.

#### Version 2:

If a device configuration has been read, but the database settings the token/fingerprint mismatch those stored in the device, the mismatched items will be shown red:

❑ [1.0.45 - S2000-2]: S2000-2 Mismatched	[2]: Entry Turnstile	Must be stored in device	Not stored in device
	Key type	Open	Open
	Suspended token	No	No
	Access Control	Yes	Yes
	Access Control Time Zone	Time Zone to Operate 1	Always
	Anti-passback	No	No
	ENTRY access point	Simple	Simple
	EXIT access point	Simple	Simple
	Zonal anti-passback	No	No
	Loop control	No	No
	Safe Mode	No	No
	Effective date	26.06.2014	26.06.2014
	Expiration date	18.06.2015	18.06.2015

In this case the synchronization is required.

Version 3:

If the configuration has been read, but the token/credential must not be stored in the device in accordance with the database settings, the device will be shown red, the relevant column will be called **Must not be stored in device**:

❑ [1.0.45 - S2000-2]: S2000-2 Mismatched	[2]: Entry Turnstile	Must be stored in device	Not stored in device
	Key type	Open	Open
	Suspended token	No	No
	Access Control	Yes	Yes
	Access Control Time Zone	Time Zone to Operate 1	Time Zone to Operate 1
	Anti-passback	No	No
	ENTRY access point	Simple	Simple
	EXIT access point	Simple	Simple
	Zonal anti-passback	No	No
	Loop control	No	No
	Safe Mode	No	No
	Effective date	26.06.2014	26.06.2014
	Expiration date	18.06.2015	18.06.2015

In the case, the synchronization is required.

Version 4:

If device configuration has not been read, the device will be shown black with no data in a relevant column having the Configuration is not read heading:

[1.0.45 - S2000-2 Matched	[2]: Entry Turnstile	Must be stored in device	Keys codes list is not read
	Key type	Open	
	Suspended token	No	
	Access Control	Yes	
	Access Control Time Zone	Time Zone to Operate 1	
	Anti-passback	No	
	ENTRY access point	Simple	
	EXIT access point	Simple	
	Zonal anti-passback	No	
	Loop control	No	

It is clear that each type and version of device requires their own set of parameters for token and fingerprint.

For example:

- S2000-2, version 1.02 :

Key type	Main
Suspended token	No
Access Control Time Zone	Always
Anti-passback	No
ENTRY access point	Simple
EXIT access point	Simple
Effective date	26.06.2013
Expiration date	26.06.2015



- S2000-2», version of higher1.05 or higher

S2000-2» version 1.10 or higher

S2000-2» version 1.15 or higher

Key type	Main
Suspended token	No
Access Control	Yes
Access Control Time Zone	Always
Anti-passback	No
ENTRY access point	Simple
EXIT access point	Simple
Zonal anti-passback	No
Loop control	No
Safe Mode	No
Effective date	26.06.2013
Expiration date	26.06.2015

- S2000-4 versions 1.10-1.12:

Suspended token	No
Access Control	Yes
Access Control Time Zone	Always
Loop control	Yes
Loop 1	Arm, Disarm
Loop 2	Arm, Disarm
Loop 3	Arm, Disarm
	Arm, Disarm

- S2000-4 version 2.00 or higher

S2000-4 version 2.10 or higher

S2000-4 version 3.00 or higher

Key type	Main
Suspended token	No
Access Control	Yes
Access Control Time Zone	Always
Loop control	Yes
Time Zone to Operate	Time Zone to Operate 1
Loop 1	Arm, Disarm
Loop 2	Arm, Disarm
Loop 3	Arm, Disarm
	Arm, Disarm
Safe Mode	No
Effective date	26.06.2013
Expiration date	26.06.2015

- S2000-BIOAccess:

Suspended token	No
Access Control Time Zone	Always
Access Control	Yes
Effective date	26.06.2013
Expiration date	26.06.2015

- Signal -10 version 1.00 or higher:

Key type	Main
Suspended token	No
Loop 1	Arm, Disarm

*Please note that parameters responsible for arming/activation specific loops are shown only when this actions are allowed for this credential.*

*To synchronize the settings of the database of the current credential, please click the Synchronize button in the Information window. The synchronization process details will be displayed in the log of the Database Administrator module*

If the log shows a message notifying that a credential synchronization error occurred because of missing a relevant access level or time zone in the device, first, time zone and access levels will be added automatically, then the credential will be added.

Please note that the **Socket Error...** occurring while reading a credential code, device configuration or polling devices means that Administrator cannot connect to a relevant Scanning Core. This may happen because of the following:

- The Scanning Core is not running
- The Scanning Core is running but there is no connection between the workstation with the Database Administrator and workstation with the Scanning Core
- The connectivity between the workstations is good, but a workstation with the Scanning Core has a wrong IP address set in the Database Administrator
- The connectivity between the workstations is good; but the workstation with the Scanning Core has two network adapters, and the second adapter's IP address is specified for this workstation in the Database Administrator.

#### 6.12.4.3.2 Synchronizing All Credentials with Devices

*This chapter discusses the synchronization of the entire list of tokens and fingerprints. The actions preceding synchronization are discussed in Chapter 6.12.4.3 Synchronizing the List of Credentials in the Database and Devices.*

To synchronize codes and rights of all credentials (Touch Memory, Proximity cards, and fingerprints) of the database with device configurations, the following prerequisites should be completed:

- Make sure that you have launched Scanning Cores controlling devices you want to synchronize with;
- Device configurations have to be read from devices you want to synchronize (from the devices itself or from the catch) ;
- The status of the database credentials has to be obtained.

**Attention!**

*The synchronization of the database-stored credentials can be done only with connected devices provided their configurations have been read.*

To synchronize all database-stored tokens and fingerprints will all devices, please select **Service/Synchronize All Touch Memory (Proximity)**.

The process of synchronization will be reported in the Database Administrator Log.

If the log displays a credential synchronization error due to a missing access level or time zone, required access levels and time zones will be added automatically, then a credential will be added.

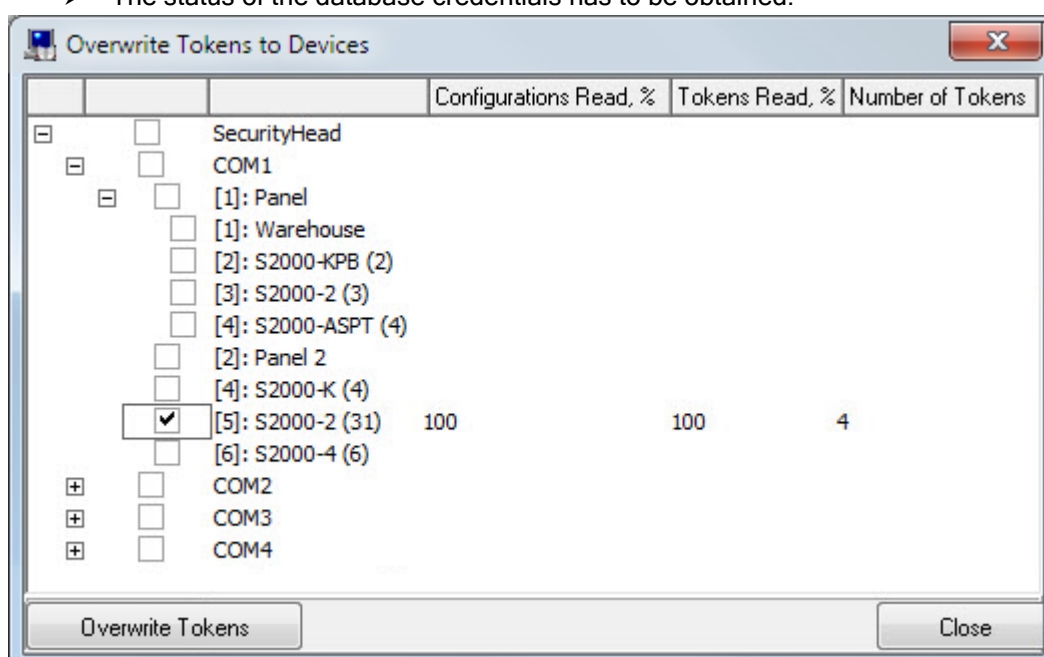
If after synchronization, any credential does not function as intended, please check the credential parameters of devices in the Information window (refer to *Chapter 6.12.4.3.1 Synchronization of Individual Credential with Devices*)

### 6.12.4.3.3 Overwriting Credentials in Devices

The list of tokens/fingerprints can be synchronized with selected devices overwriting all prior tokens/fingerprints in these devices.

To synchronize credentials (Touch Memory buttons, Proximity cards, and fingerprints) of the database and devices configurations, the following prerequisites should be completed:

- Make sure that you have launched Scanning Cores controlling devices you want to synchronize with;
- Configurations have to be read from the devices you want to synchronize (from the devices itself or from the catch) ;
- The status of the database credentials has to be obtained.

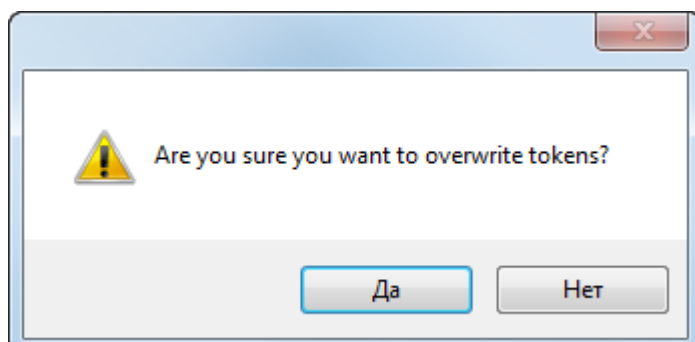


**Attention!**

*The synchronization of the database-stored credentials can be done only with connected devices provided their configurations have been read.*

All necessary actions are performed in the Overwriting Tokens in Devices window; you can open by selecting Service/Overwrite Tokens to Devices:

To synchronize all Touch Memory buttons and Proximity cards with some devices, please select required devices in the **Overwrite Tokens to Devices** dialog box and click the **Overwrite Tokens** button, then click **Yes** to confirm synchronization in the appeared window.

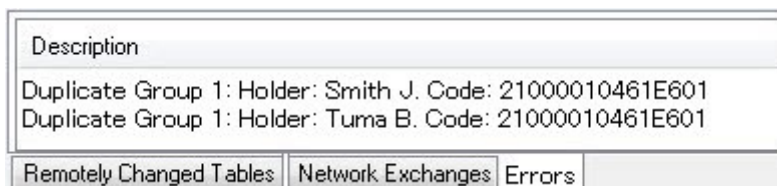


*Attention!!! Performing this type of synchronization you will delete all stored credentials in the devices before adding the credentials to devices.*

#### 6.12.4.4 Searching Credential Duplicates in the Database

The Orion Pro Database Administrator module allows searching the duplicates of Touch Memory and Proximity tokens added to the database.

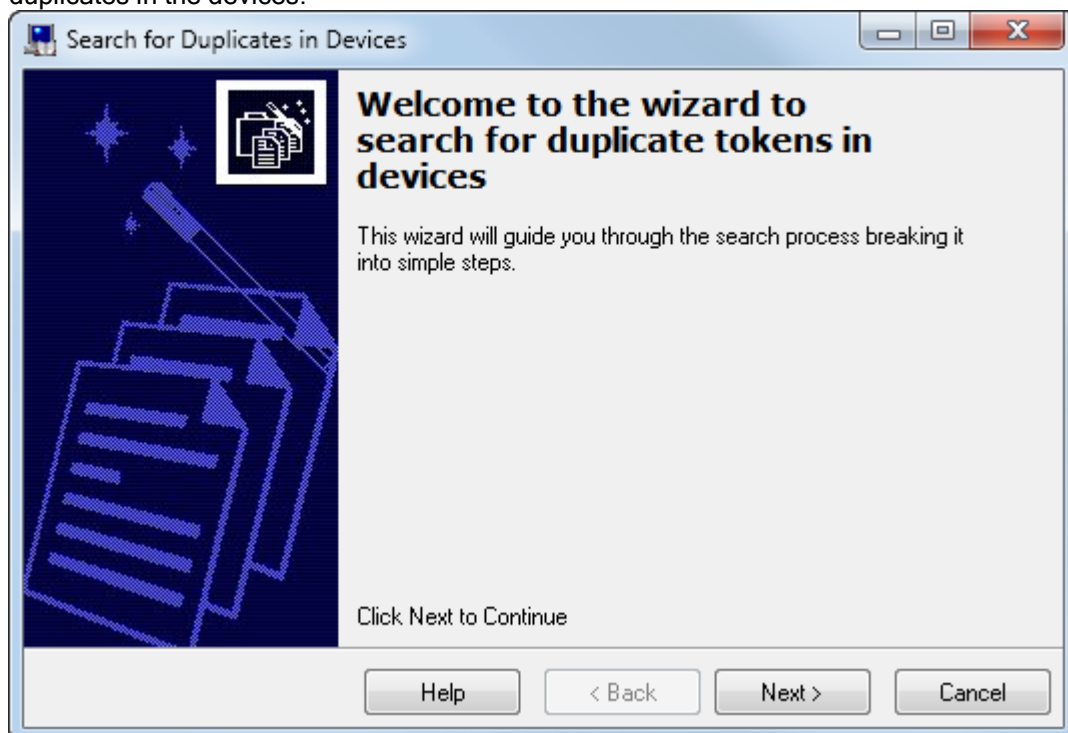
To search the duplicates of tokens in the database, please select **Service/Check Database for Token Duplicates**. It will search token duplicates in the database, and if any duplicates found, the Error tab will appear in the Database Administrator Log.



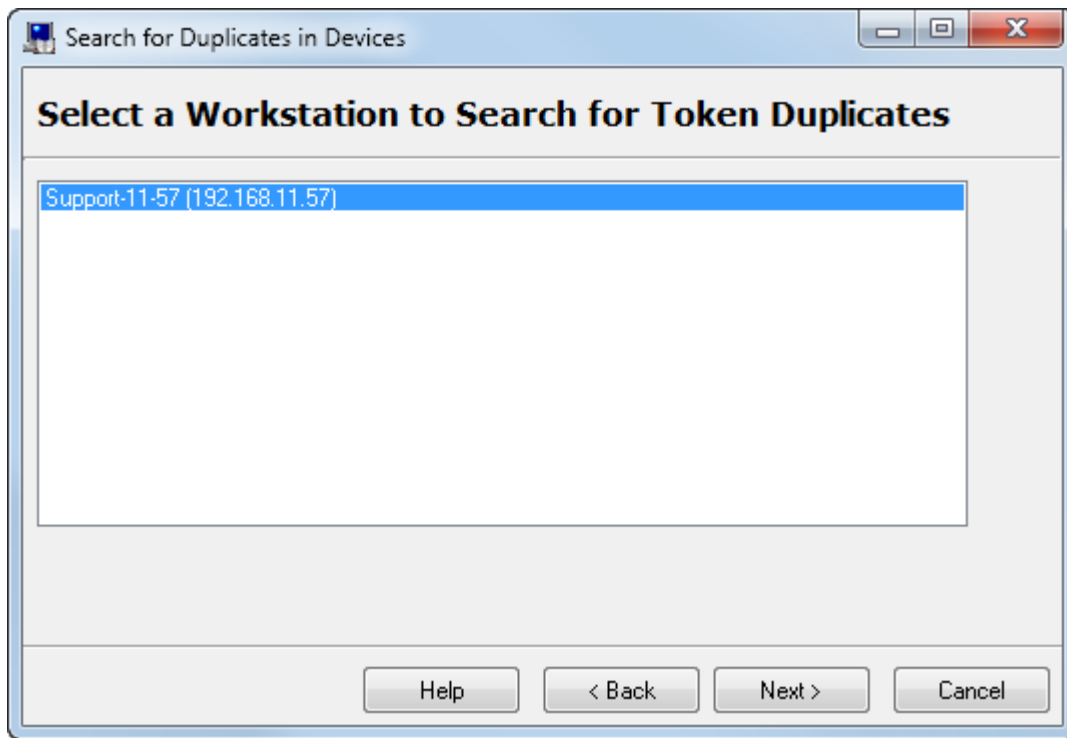
This tab will show all duplicates of tokens existing in the database. When needed, any token can be deleted selecting a required token in the list of credentials and click the **Delete** button. Then click **Yes** to confirm the deletion.

#### 6.12.4.5 Searching for Token Duplicates in Devices

The Database Administrator module offer functions to search for token duplicates in devices. Attention!!! Please read device configuration first (from devices or from catch) before searching token duplicates in the devices:

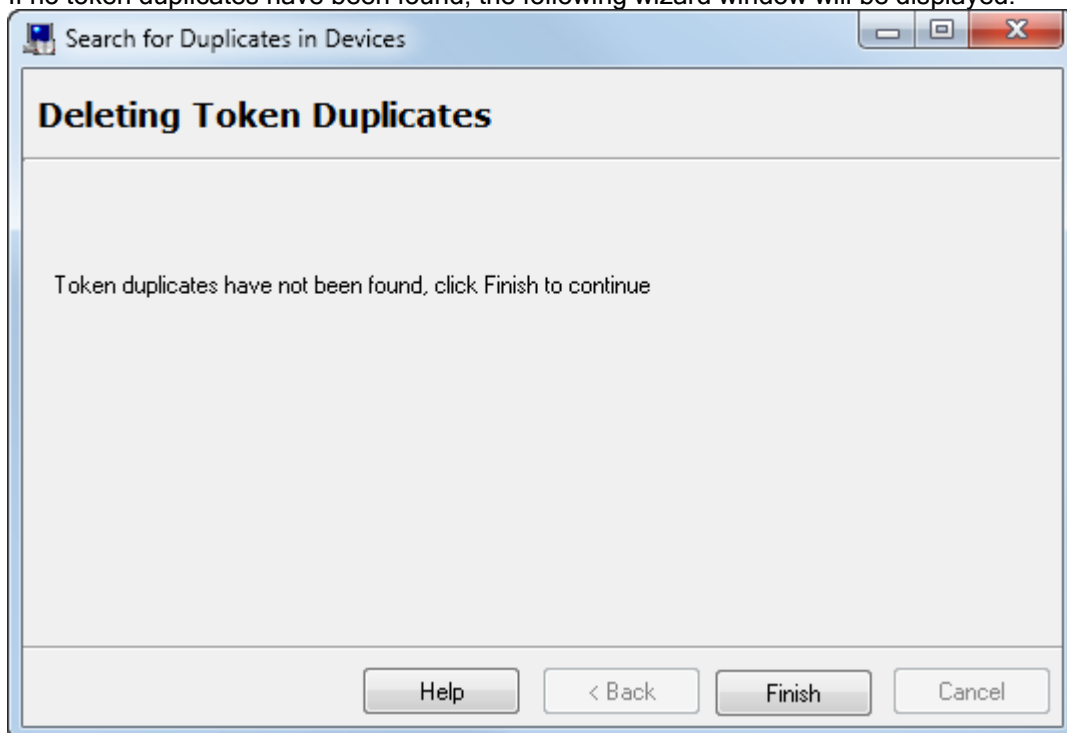


Clicking the Next button will display the further wizard window, where a workstation is to be selected to search them for token duplicates:

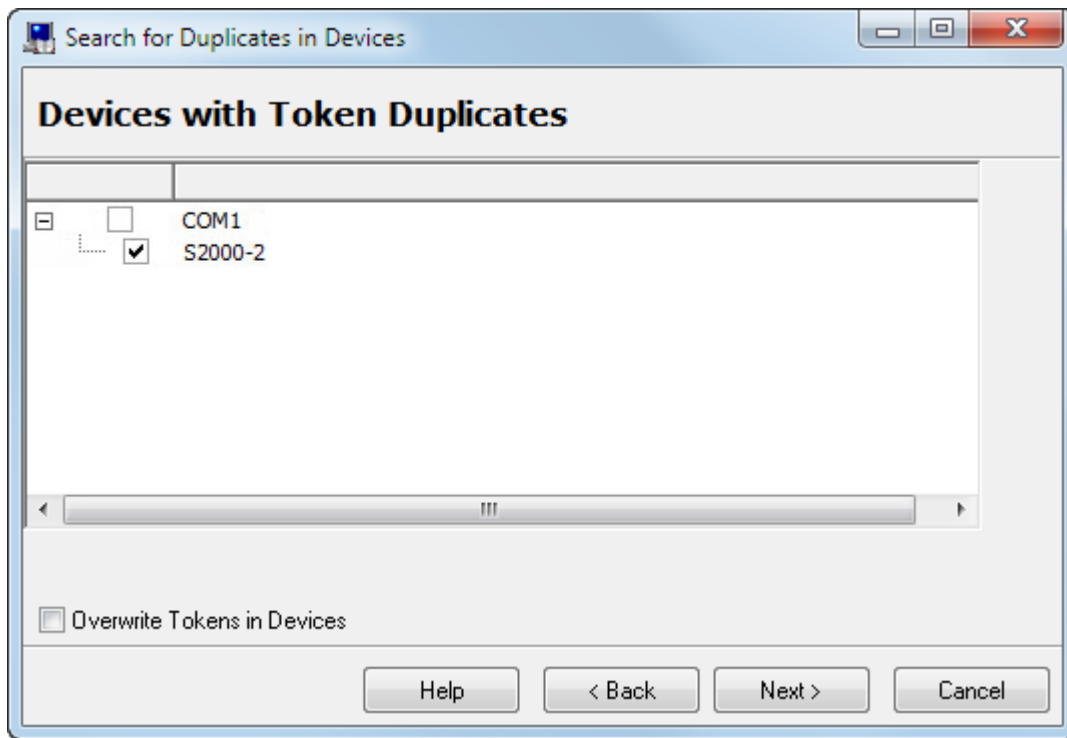


Click the Next button to start searching for duplicates in the workstation-connected devices whose configurations have been read.

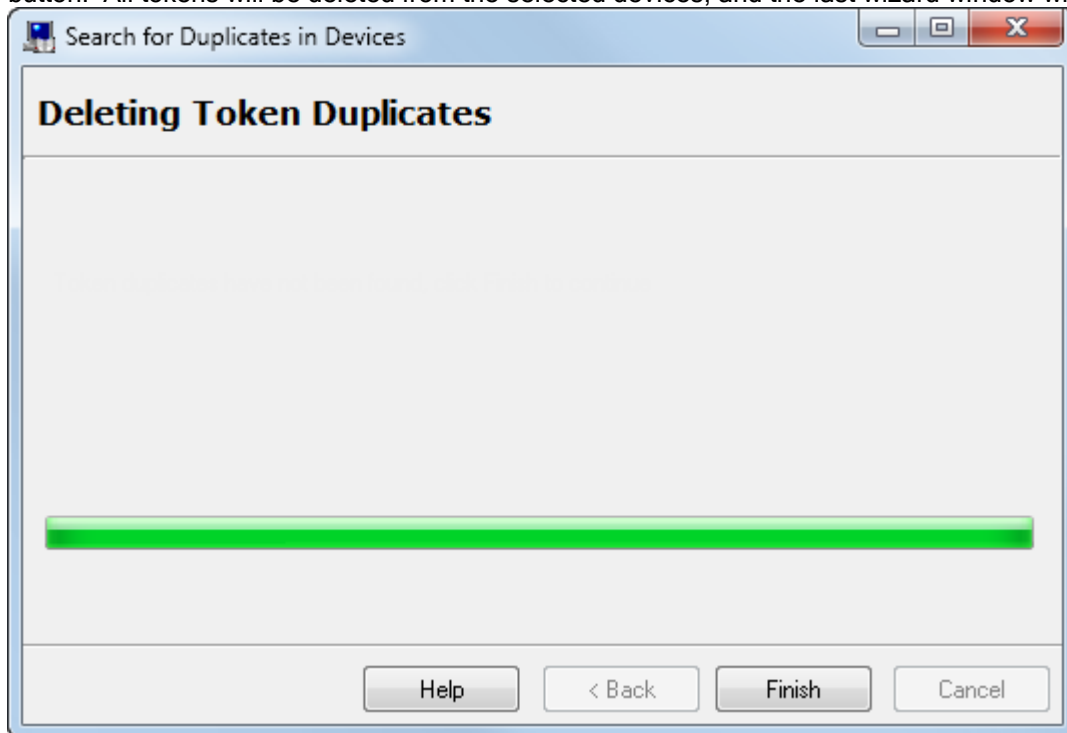
If no token duplicates have been found, the following wizard window will be displayed:



If any token duplicates have been found, the third wizard window will appear to display the devices that have token duplicates:



To delete tokens from the devices, please select checkboxes near required devices and click the **Next** button. All tokens will be deleted from the selected devices, and the last wizard window will be displayed:



To complete the wizard work, please click the **Finish** button. If **Overwrite Tokens** function in the preceding window has been checked, after deleting duplicates, new credentials will be written (added) to the devices in accordance with the database settings.

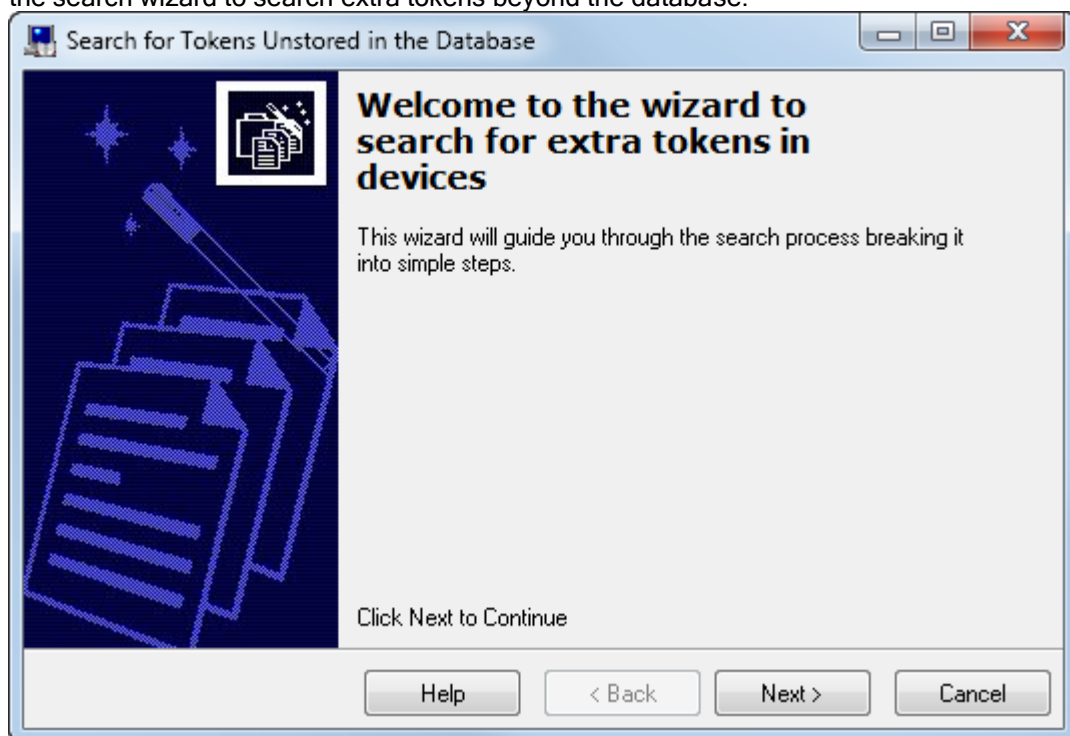
#### 6.12.4.6 Searching for Extra Tokens in Devices

The Database Administrator module offer functions to search for extra token in devices.

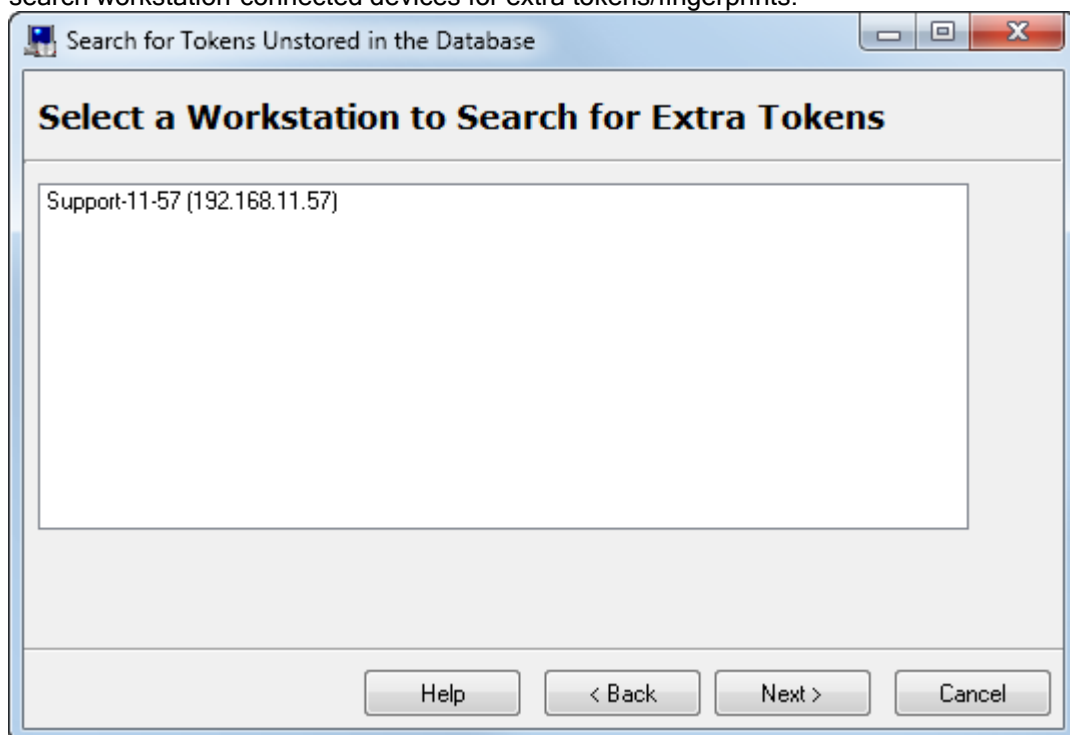
This method is recommended if the tokens are stored in a device while being missing in the database.

Attention!!! Please first read device configuration (from devices or from cache) before searching extra tokens in the devices:

To search extra tokens in the devices, please select **Service/Check Devices for Extra Tokens**. It will start the search wizard to search extra tokens beyond the database:

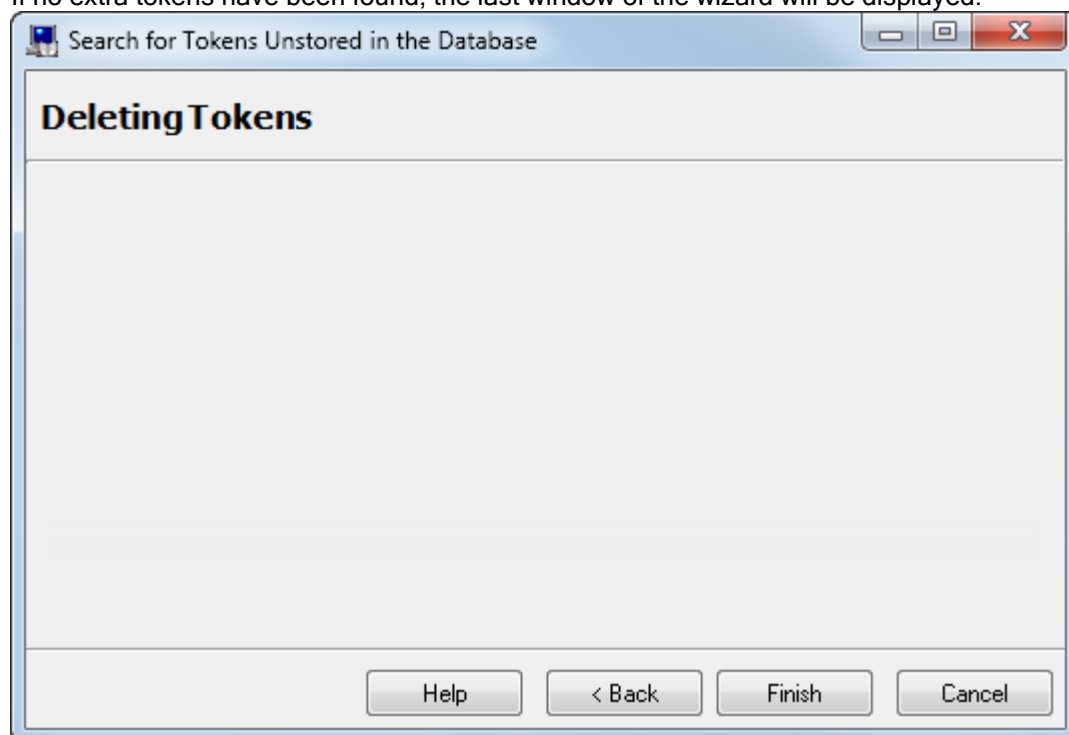


Clicking the Next button will display the further wizard window, where workstation is to be selected to search workstation-connected devices for extra tokens/fingerprints:

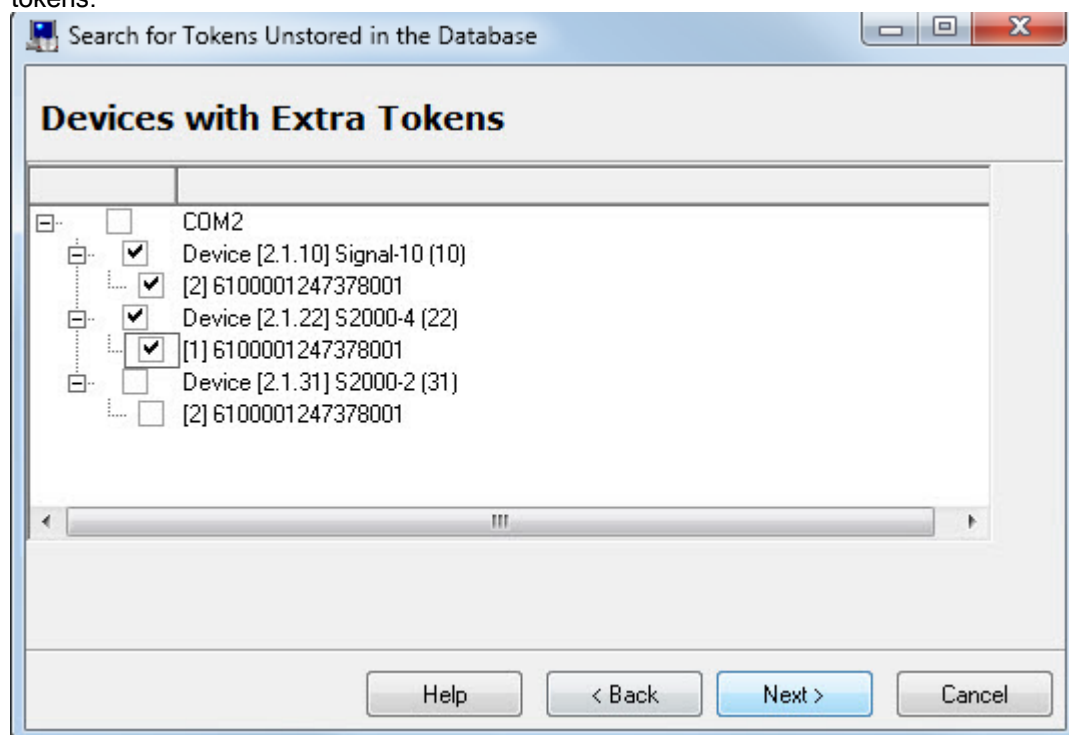


Click the **Next** button to start searching for extra tokens in the workstation-connected devices whose configurations have been read.

If no extra tokens have been found, the last window of the wizard will be displayed:

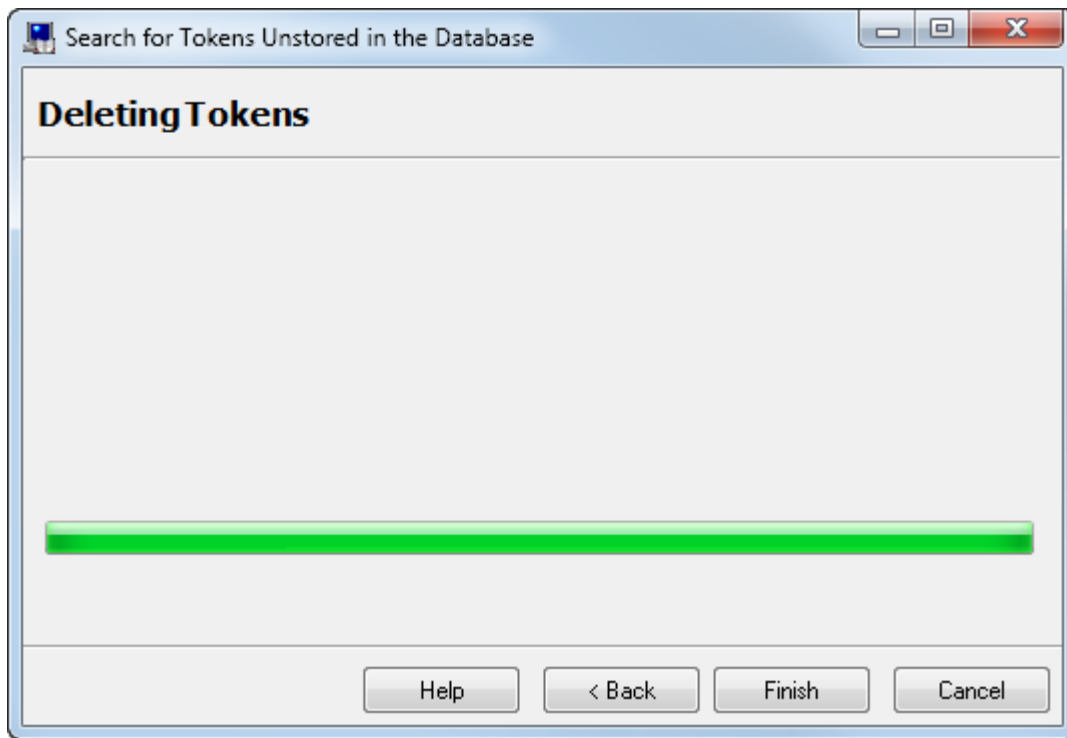


If any extra tokens have been found, the third wizard window will appear to display the devices with extra tokens:



To delete tokens from the devices, please select checkboxes near required devices and click the **Next** button. All tokens will be deleted from the selected devices, and the last wizard window will be displayed:





To complete the wizard work, please click the **Finish** button.

## 6.13 Synchronizing the Orion Pro Database with S2000M Panel

The Database Administrator of the Orion Pro suite allows exporting structure of intrusion detection and fire protection system (IFS) to the S2000M Panel

Importing IFS configuration from the S2000M to the database is also supported.

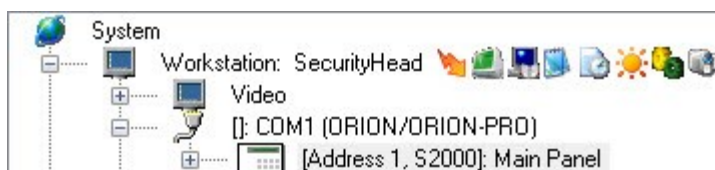
### 6.13.1 Importing Configuration from the S2000M

Database Administrator allows (using Scanning Cores) importing created configurations from the S2000M Panel

*Usually, this is used at sites where Orion System' devices (hardware platform) had been used before the decision to use the software platform (the Orion Pro Suite) - in other words, at the initial stage of database development.*

*To import the configuration from the S2000M to the database of the Orion Pro Suite, please go to the Device Address tab (System Structure) to do the following:*

- Add and configure a workstation with Scanning Core where a S2000M panel is connected. Add COM Port to the workstation, and then associate the S2000M to the COM Port via RS-485 interface.



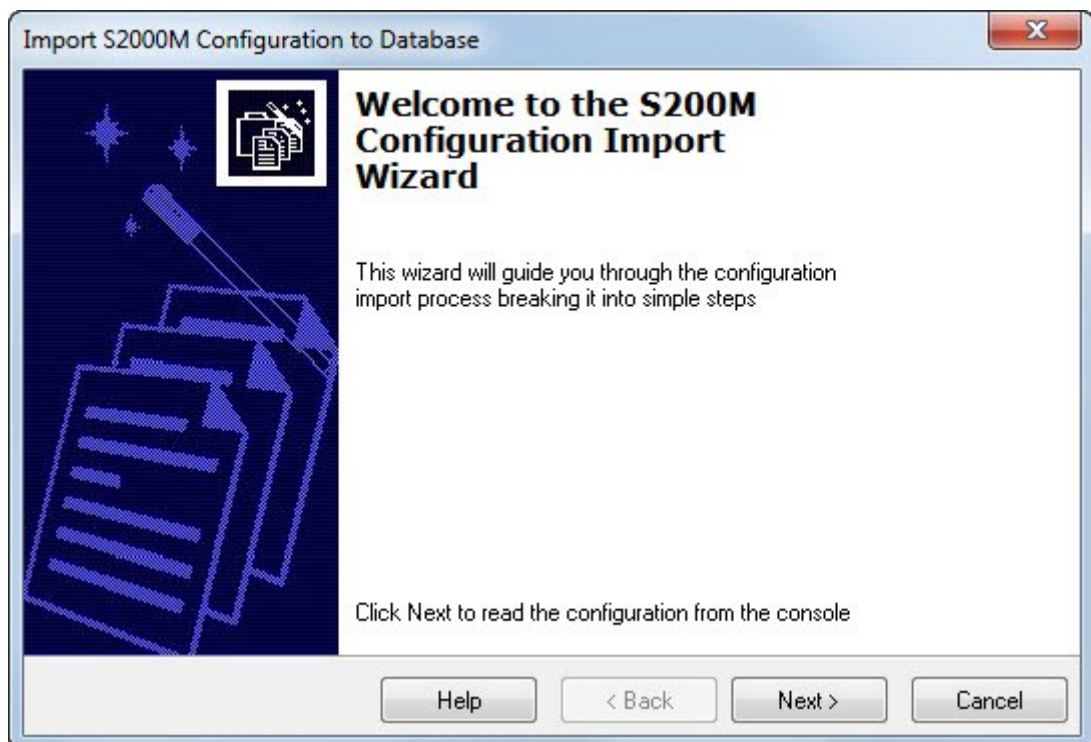
**Attention!** *If the devices connected to this COM Port are functioning in the Orion Pro protocol (and S2000M in the Computer mode) the address of the S2000M in the database settings must*

*be set as its address for RS-232 interface when the process of importing the configuration has been completed.*

*Therefore, it is strongly recommended using the same address for RS-232 and RS-485 interfaces. In this case, this address will not require attention.*

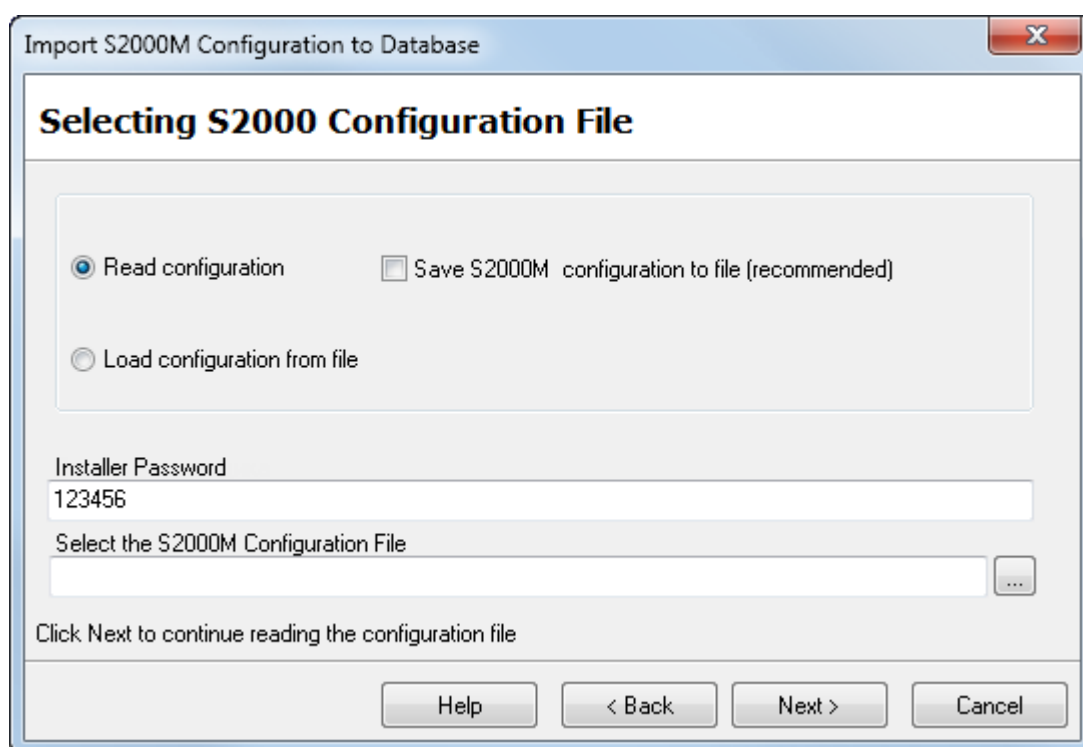
If you plan to use the Orion protocol, the S2000M panel has to be switched over to the **PI\Reserve** mode. If the Orion Pro protocol is to be used, the S2000M has to be set as **Computer** and it will be switched in the **Programming Mode**.

- If the Scanning Core with connected panel has been already running, it is recommended that you should update the database of the Scanning Core (**Service/Update Database in Operative Task**). Otherwise the Scanning Core has to be started (from Shell)
- Further, open the Import S2000M Configuration to Database wizard. (Choose **Service/Import S2000M Configuration**).



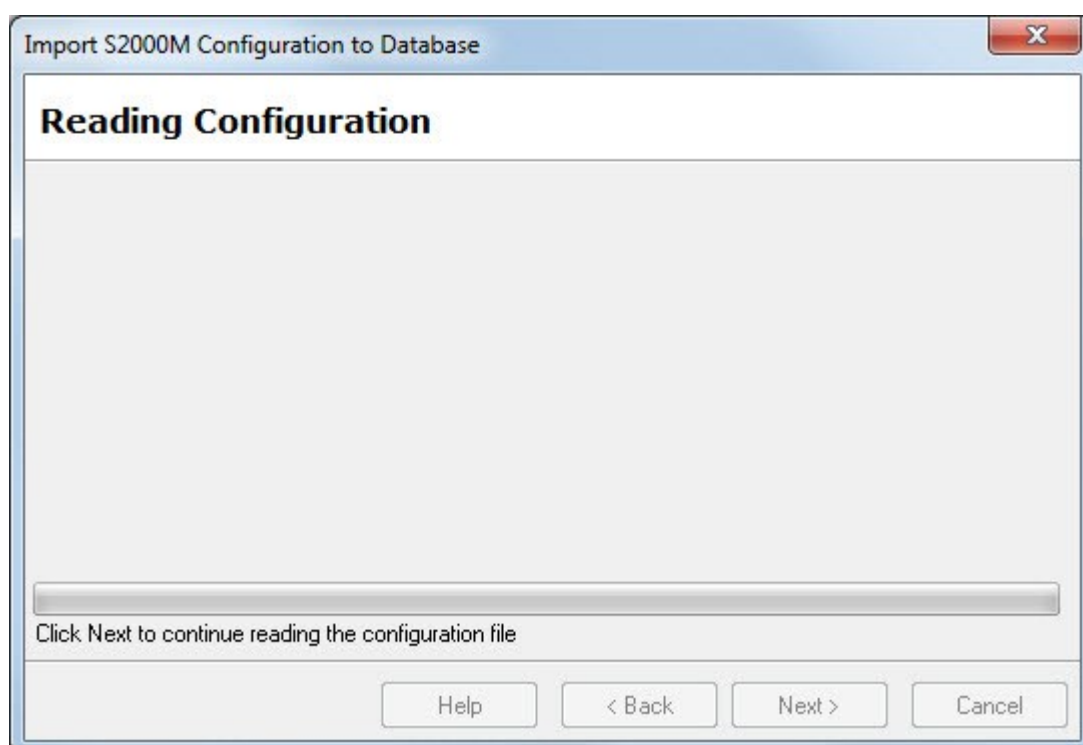
To proceed further, click the **Next** button.

- In the appeared (second) window, please define the way of configuration reading:
  - If it is the first time you start the system, you should choose reading a configuration from S2000M.  
If the Save **S2000M** configuration to file item is checked and the file location path is specified, the read configuration will be saved as a file.
  - Subsequently, one can choose to load a configuration from a file (if its location is specified in advance)



After choosing how configuration will be read, please click the Next button to proceed further.

- The next window will show the process of reading the configuration from the S2000M device or from a configuration file.

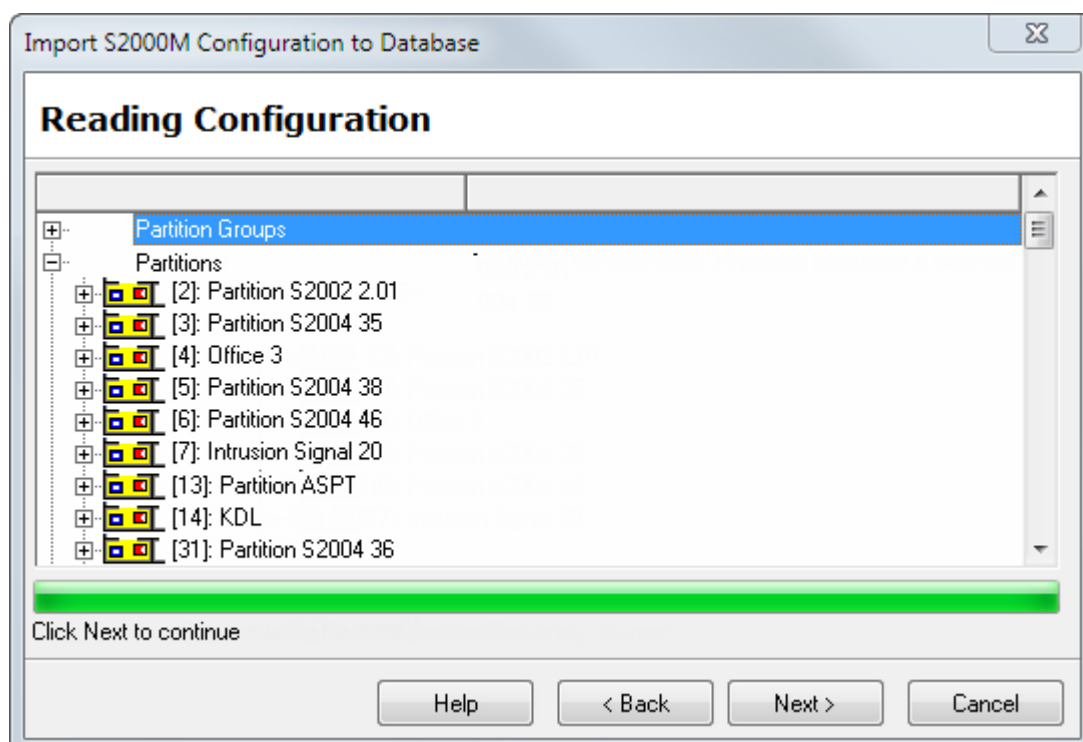


*The configuration read process will not start immediately, please wait for 1 or 2 minutes.*

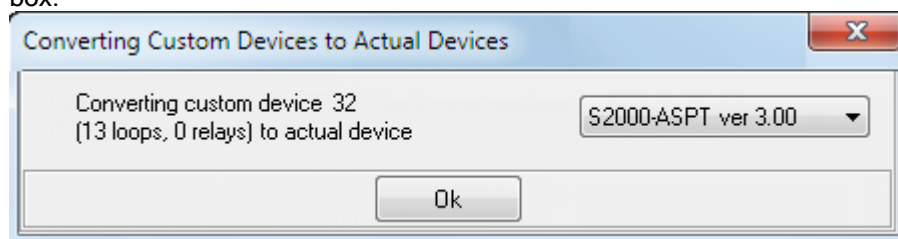
*When process has completed, please click the **Next** button to proceed further*

- The next window will show the recognized IFS system taken from the S2000M panel. It will also include conversion errors (for example, if a S2000M's configuration includes a partition

with the same index as used in the database of the current workstation. These data will not be imported.

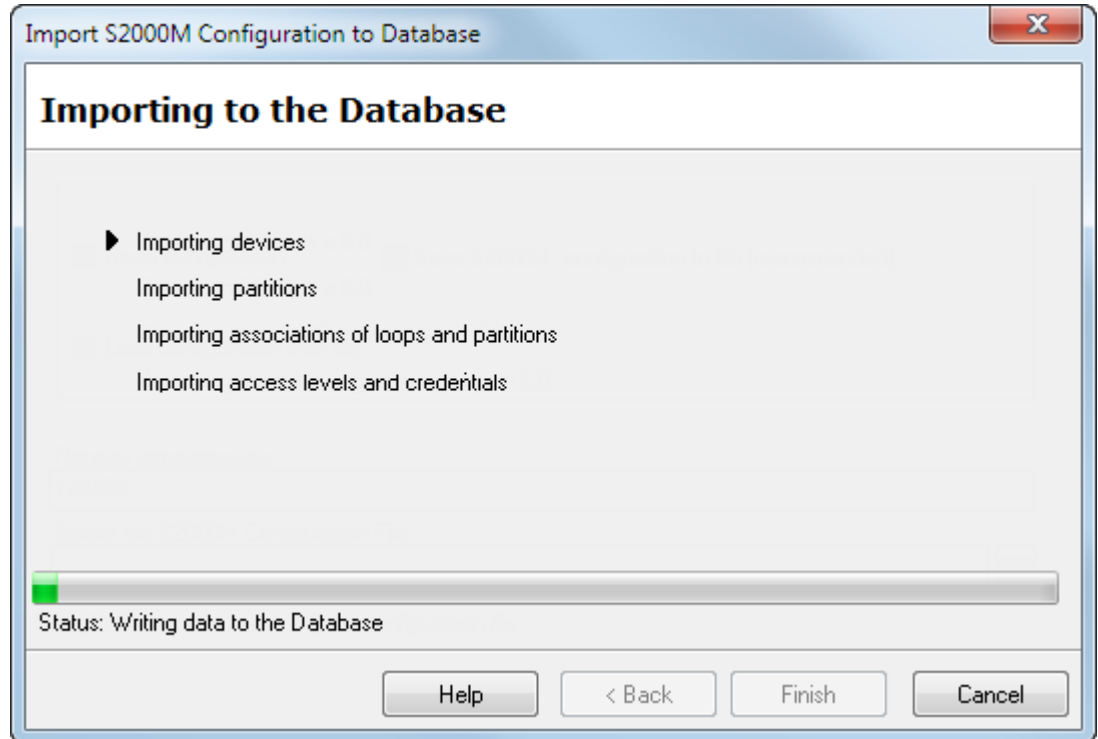


In S2000M configuration includes the custom types of devices, each custom type (assigned to one device at least) will be reported in the **Converting Custom Devices into Actual Devices** dialog box:



In the dialog box, you will have to select an actual device type for the device that is specified as a custom one, and click the Ok button. Please click the **Next** button to proceed further.

- The next (fifth) windows will show the process of writing S2000M configuration-read data to the Orion Pro database



- 
- Wait till the writing process is completed and click the **Finish** button to close the wizard.
- If you plan to use the Orion Pro protocol, please switch the S2000M panel from the programming mode to the standby mode.
- *If COM Port-connected devices will function in Orion Pro protocol (when S2000M functions as a **Computer**), and RS-323 and RS-485 addresses of the S2000M are different, please set the RS-232 address for the S2000M in the database*
- Update the database-related information in the Scanning Core (**Service/Update Database in Operative Task**). Alternatively (as recommended), you can restart the System Shell (therefore, Scanning Core) on your workstation.

### 6.13.2 Exporting Database to S2000M

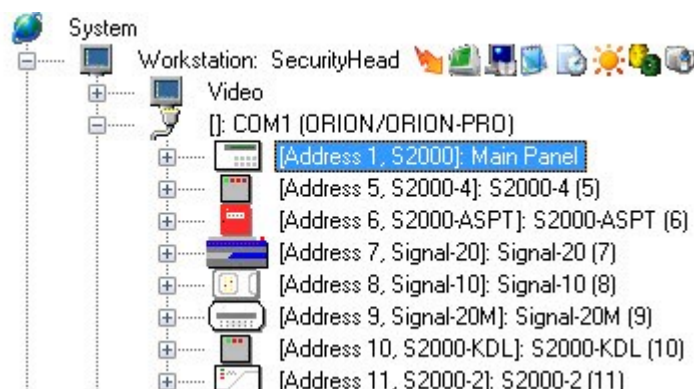
*Attention! This chapter assumes that a database-receiving S2000M panel will have the same addresses for RS-232 and RS-485 interfaces.*

*Attention! The PProg utility has to be installed and launched at least once on the relevant computer.*

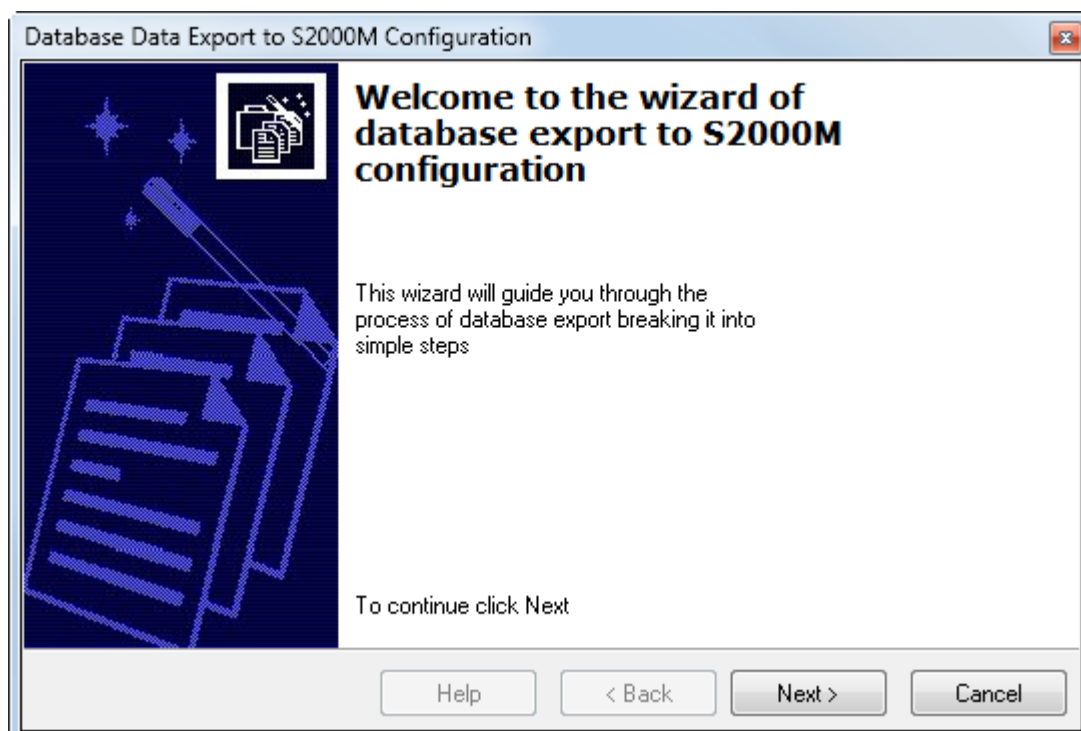
To export settings of the IFS system please follow instruction as described further:

- If the Orion protocol is used, please transfer devices from a COM port to the S2000M panel in the database before exporting the database to the panel (refer to Chapter 6.2.6.1.3 Transferring Devices). Completing export, please transfer devices to a COM port.)
- If any database changes have been made after starting a relevant Scanning Core, please update the database data in the Scanning Core (Service/Update Database in Operative Task)
- If the Scanning Core has not been started yet, please launch the Scanning Core (from the System Shell)

- Switch the S2000M panel to the programming mode.
- Go to the Device Address tab
- Select the S2000M in the tree of system entities, where the configuration is to be exported.



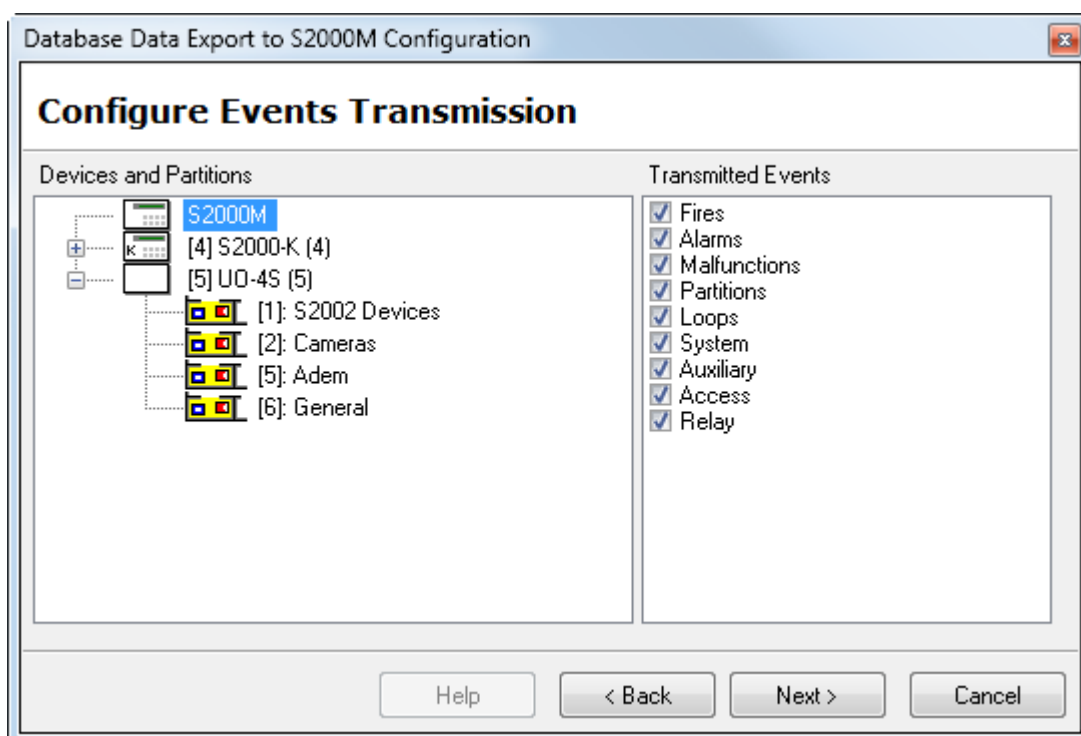
- Start the database export wizard by choosing the Service/Export Database to S2000M



To proceed further, click the **Next** button.

- The next (second) window of the wizard will show the list of S2000M-associated devices included in the settings of event transmission (sharing).

*Also, it will show the list of partitions or partition groups the events of which will be transmitted to this device.*



In the right pane of the wizard window, please select the event categories to be transmitted to this device by the S2000M.

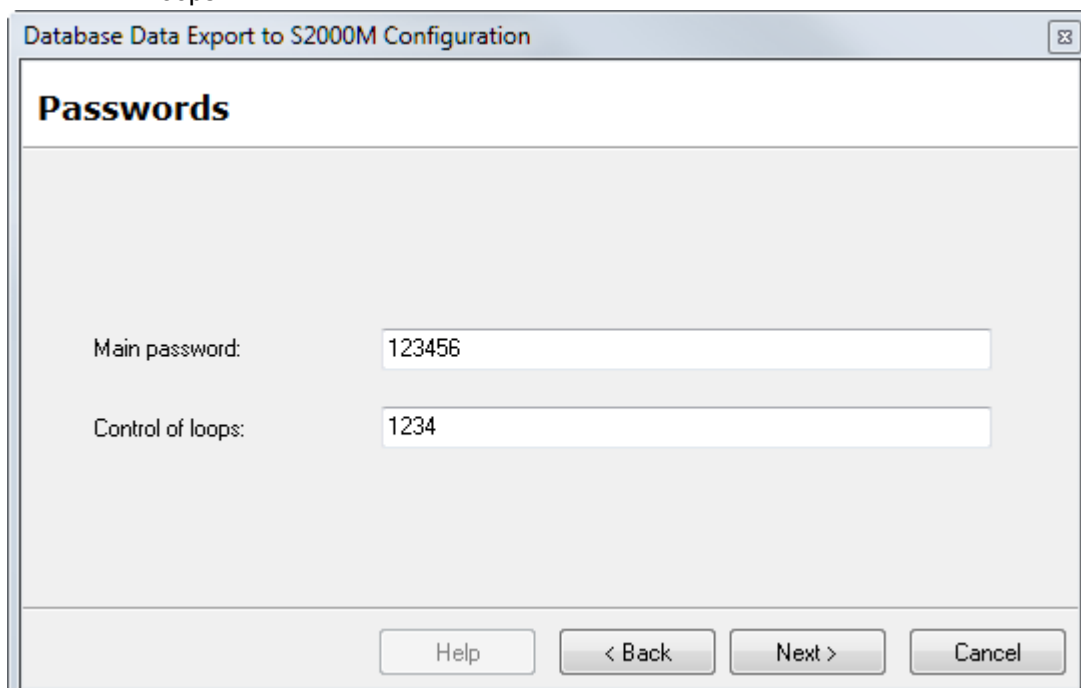
For the S2000M, please select event categories to be displayed on the S2000M's screen (as well as transmitted to the Orion Pro Scanning Core, if the Orion Pro protocol is used)

*Attention! If the Orion Pro protocol is used, only categories selected to display on S2000M panel will be transmitted to the Orion Pro Scanning Core.*

To proceed further, click the **Next** button

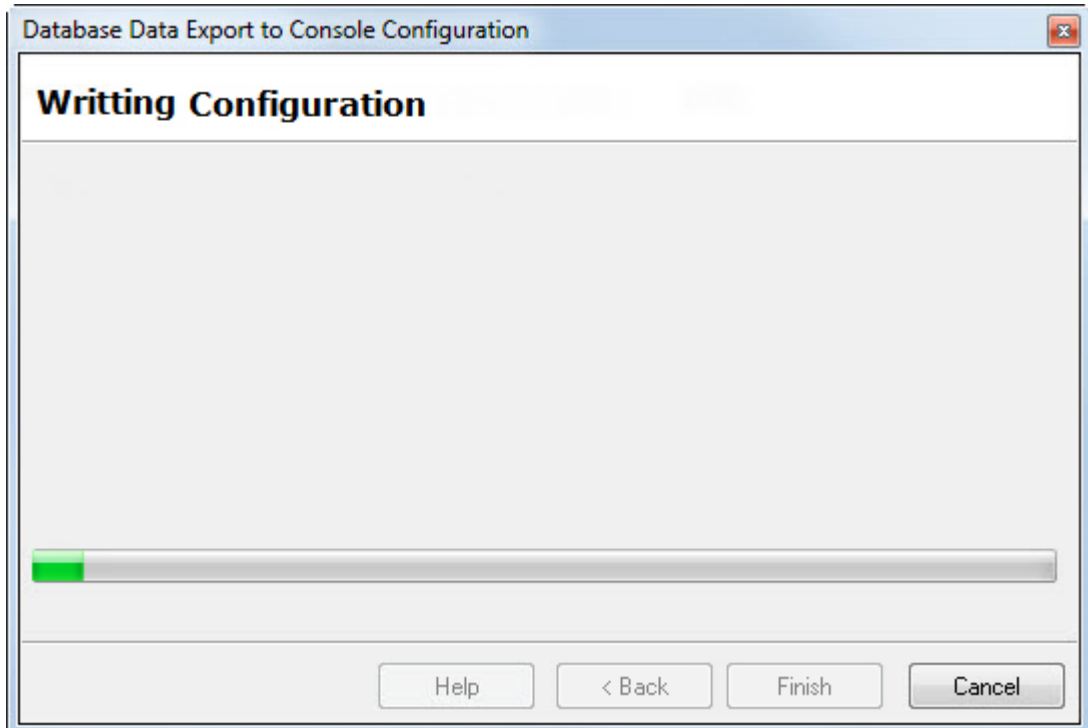
On the next (third) window, please specify the following for the S2000M:

- Installer password – Main password
- Password with maximum operation privileges (panel access level "255") - Control of loops.



To proceed further, please click the **Next** button.

- The last window displays the process of writing data to the S2000M.



Wait till the process is completed, then click the **Finish** button to close the wizard

- If the Orion protocol is used, please move the devices back to the COM Port from the S2000M. Update the database data in the Scanning Core (**Service/Update Database in Operative Task**)
- *Switch the S2000M from the programming mode to the standby mode.*

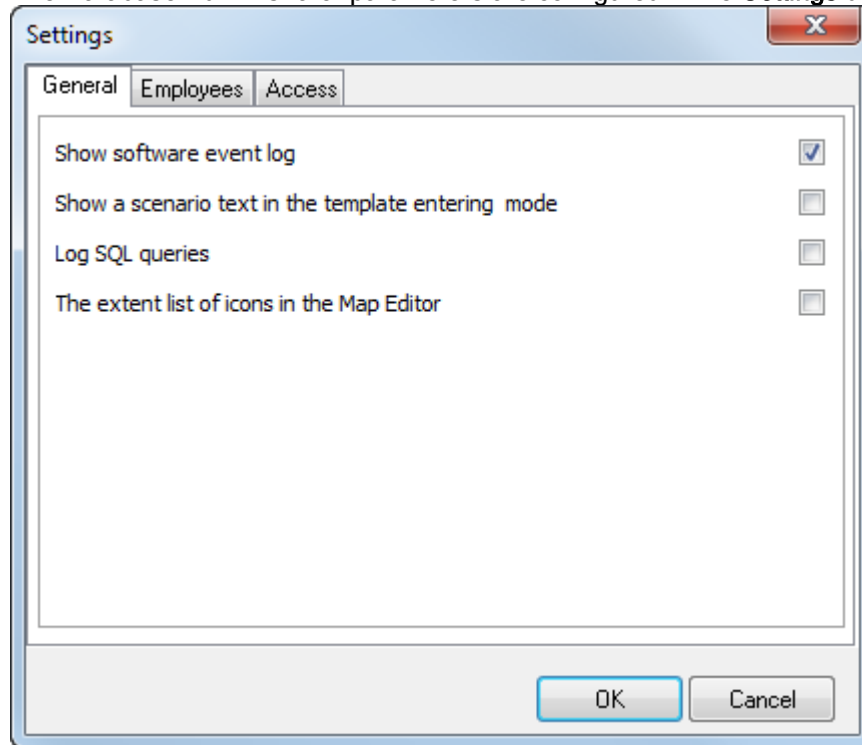
*After completing the database export to the S2000M panel, you can review the panel configuration by saving it to a computer using the PProg utility.*



## 6.14 Settings

### 6.14.1 Settings of Database Administrator

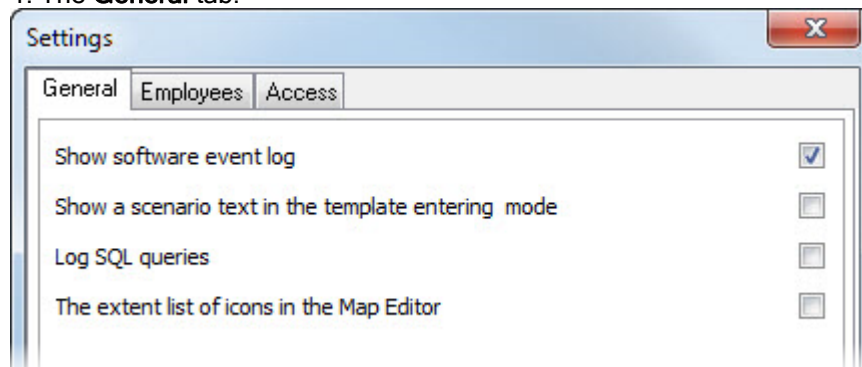
The Database Administrator parameters are configured in the **Settings** dialog box (**Options/Settings**):



The **Settings** dialog box includes three tabs:

1. General
2. Employees
3. Access

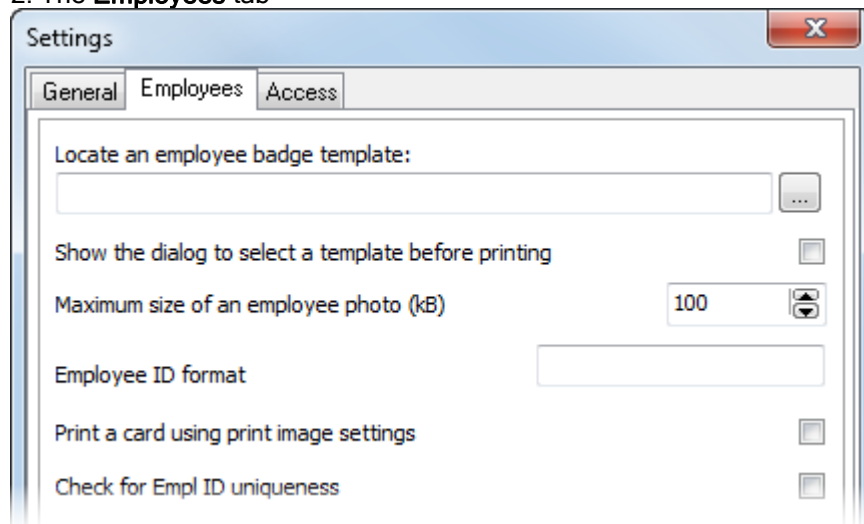
#### 1. The **General** tab:




Parameters	Possible Values	Description
Show software event log	<input type="checkbox"/> (No), <input checked="" type="checkbox"/> (Yes)	This parameter is responsible for the display of the Database Administrator Events: <ul style="list-style-type: none"><li>• <input type="checkbox"/> (No): The log will not be shown</li><li>• <input checked="" type="checkbox"/> (Yes): The log will be shown.</li></ul> Default value: <input checked="" type="checkbox"/> (Yes)
Show a scenario text in the template entering mode	<input type="checkbox"/> (No), <input checked="" type="checkbox"/> (Yes)	This parameter defines whether to display a scenario text based on the <b>Orion_Scripts</b> macrolanguage in the template entering mode:

		<ul style="list-style-type: none"> <li><input type="checkbox"/> (No): A text will not be shown</li> <li><input checked="" type="checkbox"/> (Yes): A text will be shown.</li> </ul> <p>Default value: <input type="checkbox"/> (No)</p>
Log SQL queries	<input type="checkbox"/> (No) <input checked="" type="checkbox"/> (Yes)	<p>This parameter defines whether to log actions made in the Database Administrator:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> (No): The log is enabled</li> <li><input checked="" type="checkbox"/> (Yes): The log is disabled.</li> </ul> <p>When this parameter is enabled, an operator's database changes are reported in the <b>Query Log</b> table.</p> <p>The information saved for each action are as follows:</p> <ul style="list-style-type: none"> <li>Time of a database changes</li> <li>The Database Administrator's computer IP address where a database change has been initiated.</li> <li>The ID or name of an operator who made changes in the database</li> <li>Detailed description of actions related to the changes in the database.</li> </ul> <p>Default value: <input type="checkbox"/> (No)</p>
The extent list of icons on a map	<input type="checkbox"/> (No) <input checked="" type="checkbox"/> (Yes)	<p>This parameter is responsible for the set of possible icons to represent system entities on a map</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> (No): Only relevant icons can be selected for a specific entity on a map,</li> <li><input checked="" type="checkbox"/> (Yes): All icons can be selected (i.e. all icons for all types <i>(not recommended)</i>)</li> </ul> <p>Default value: <input type="checkbox"/> (No)</p>

## 2. The **Employees** tab



Parameter	Possible Values	Description
Locate an employee badge template:	<i>A full path to a file or an empty field</i>	<p>This locates a file containing the template of an employee card to be used for printing a badge.</p> <p><i>If this field is empty, no badge will be printed.</i></p> <p>Default value: empty field</p>
Show a dialog to select a template before printing	<input type="checkbox"/> (No), <input checked="" type="checkbox"/> (Yes)	<p>This parameter defines whether to request the selection of a template before printing:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> (Yes): A dialog will be shown to select a template for printing.</li> <li><input type="checkbox"/> (No) – The selection dialog will not be requested. But the template defined by</li> </ul>

		<p><b>Locate an employee badge template</b> parameter will be used for printing</p> <p>Default value: <input type="checkbox"/> (No)</p>
Maximum size of an employee photo (kB)	1..2147483647	<p>This parameter defines the maximum size of an employee photo to store in the database.</p> <p><i>If an image being loaded for an employee badge photo exceeds the size defined by the <b>Maximum size of an employee photo</b> parameter, the photo loading will fail and the following message box will appear:</i></p>  <p>Default value: <b>100kB</b></p>
Employee ID format	<i>A string describing an ID format or empty field</i>	<p>This parameter defines a format of Employee ID (EMPL ID)</p> <p>Formatting is used for printing badges with an Employee ID containing alphanumeric numbers.</p> <p>The formatting rules are described in <b>Note 1</b> to this table.</p> <p>In most cases, the formatting is not required; therefore this parameter field is left empty.</p> <p>Default format: <b>empty field</b></p>
Print card using print image settings (supplementary image)	<input type="checkbox"/> (No), <input checked="" type="checkbox"/> (Yes)	<p>This parameter defines whether to use a supplementary image for card printing:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> (Yes) – Uses a supplementary image for printing. This feature is useful for using printers with magnetic functions.</li> <li><input type="checkbox"/> (No) – A supplementary image is not used. (Applicable for other most common printers)</li> </ul> <p>Default value: <input type="checkbox"/> (No)</p>
Check for Empl ID uniqueness	<input type="checkbox"/> (No), <input checked="" type="checkbox"/> (Yes)	<p>This parameter defines whether to add employees with the same Empl ID to the database:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> (Yes) – Employees with the same ID cannot be added to the database.</li> <li><input type="checkbox"/> (No) – Employees with the same ID can be added to the database</li> </ul> <p>Default value: <input type="checkbox"/> (No)</p>

**Note 1:**

A format string (mask) consists of three fields separated by a semicolon (;). The first part is the mask itself. The second is a character defining whether mask characters must be compared with the characters of a masked string or replace the characters of a masked string. The third part is a character used to replace characters missing in a masked string.

The characters used in the first mask field are as follows:

Characters	Value in Mask
!	If character '!' is used, the optional characters of a masked string are replaced with leading blanks. If this character is not used, optional characters will be replaced with trailing blanks
>	If the '>' character is used in the mask, all further characters (till the end of the mask or till the '<' character) must be upper-case characters
<	If the '<' character is used in a mask, all further characters (till the end of the mask or till the '>' character) must be lower-case characters
<>	If booth characters '<>' are used, the case is not checked.
\	The character following the '\ ' character is a literal. Please use this character for using special mask characters as literals
L	The 'L' character requires an alphabetic character in the specified position.
l	The 'l' character allows (but not require) an alphabet character in the specified position.
A	The 'A' character requires an alphabet or numeric character in specified position.
a	The 'a' character allows (but not require) an alphabet or numeric character in the specified position.
C	The 'C' character requires any character in the specified position.
c	The 'c' character allows (but not require) any character in the specified position.
0	The '0' character requires a numeric character in the specified position.
9	The '9' character allows (but not require) a numeric character in the specified position.
#	The '#' character allows (but not require) a numeric character, the '+' sign or '-' sign
:	The ':' character is used to separate hours, minutes, and seconds the sting indicating time.
/	The '/' character is used to separate a month, day, and year in the string representing a date.
;	The ';' character is used to separate three fields in a mask.

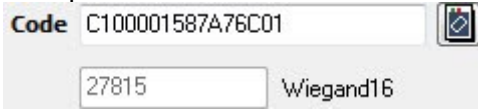
Any other symbol or character not specified in the above list can be used as a literal in the first part of the mask. Literals are placed automatically in a mask text if the '!' character is used in the second part of the mask; or they are compared with the characters of a masked string, if the '0' character is used as the second part of a mask.

Let us consider the following mask of phone number as an example: (000) 000-0000;1;\* '1' of the second field means that if the mask line does not include 10 digits, it will look like "(\*\*\* ) \*\*\*-\*\*\*\*" (if '0' is used, the '\*' character replaces only missing characters of a masked string).

The third field of this mask includes the character which replaces missing characters of a masked string

### 3. The Access tab:

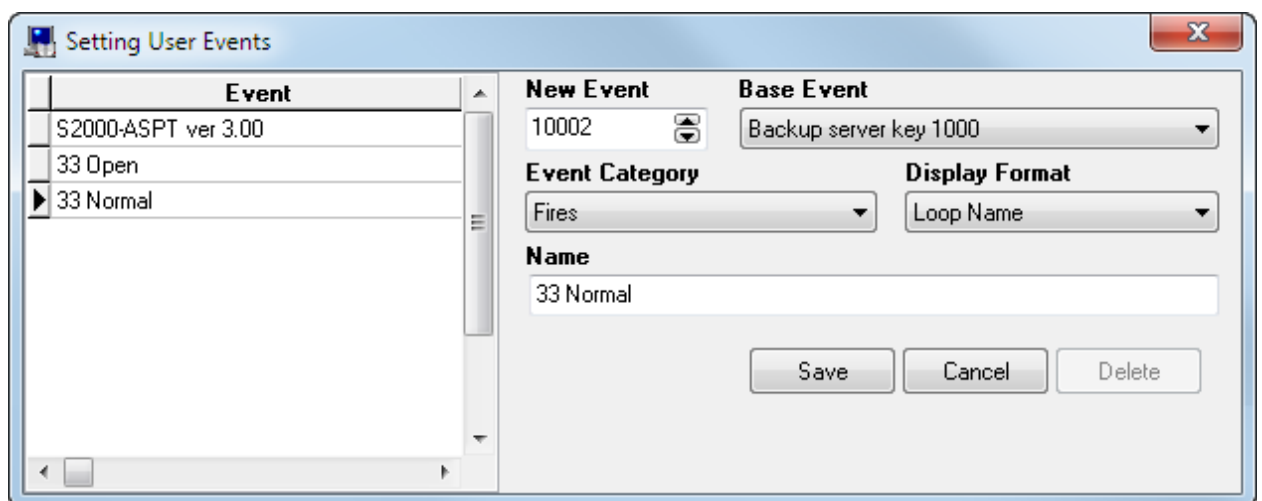
Parameter	Possible values	Description
Requests the status of credentials when switching to the Credentials tab	<input type="checkbox"/> (No) <input checked="" type="checkbox"/> (Yes)	<p>This parameter defines whether to request status of credentials each time when a user toggles the Credentials tab :</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> (Yes) – the status of credentials will be requested automatically when one toggles the Credentials tab,</li> <li><input type="checkbox"/> (No) – The status of credentials will not be requested when one toggles the Credentials tab.</li> </ul> <p><i>Please be mindful that a credential status will not</i></p>

		<i>be obtained automatically until one device configuration has been read at least. In other words this function will not work until a configuration from one device at least is available.</i> Default value: <input type="checkbox"/> (No)
Use the current date for the credential validity period	<input type="checkbox"/> (No) <input checked="" type="checkbox"/> (Yes)	This parameter defines whether to fill in the <b>From</b> field (a validity period start point) with the current date when adding any credentials: <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> (Yes) – Enable filling in the <b>Form</b> field with the current date</li> <li><input type="checkbox"/> (No) – Disable filling in the <b>Form</b> field with the current date</li> </ul> Default value: <input type="checkbox"/> (No)
Type of Short Code	Full Wiegand16 Wiegand24	This parameter defines how to display additional information on the code of the Proximity card. The Code field displays a card code converted to the Touch Memory format.  The additional field displays a card code in the Wiegand format as defined by the <b>Type of short code</b> parameter.  Default value: Wiegand16

### 6.14.2 Setting User Events

User events are used to rename the system events of some system entities (Refer 6.4.5.Renaming System Events).

This chapter focuses on the editing of custom events list in the Setting User Events dialog box (Options/User-Defined Events):



The left pane of the Setting User Events dialog box shows the list of user events (arranged by index number); the right pane shows the properties of a selected user event.

To add a new user-defined (custom) event, please click the Add button. Then enter values for all properties of new user events and click the Save button.

To edit any user-defined events, please select a required event in the list of user events and click the **Edit** button. Then make necessary changes and click the **Save** button.

To delete a user-defined event, please select and a user event you want to delete, ant click the Delete button. Then confirm the deletion by clicking **Yes** in the appeared dialog box

The user event properties:

**New Event**  
10001

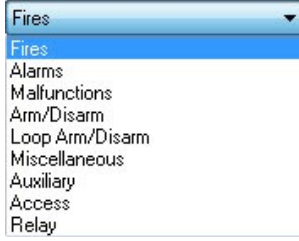
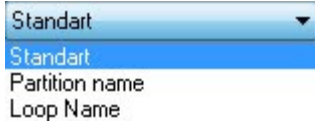
**Base Event**  
Pump On

**Event Category**  
Auxiliary

**Display Format**  
Standart

**Name**  
33 Open

Properties	Possible Values	Description
New Event	10000...10999	<p>The unique index of a user-defined event.</p> <p>Default value: minimum value from the range (10000...10999) available in the system</p>
Base Event	One of the system events	<p>A standard event will be represented by the user-defined event.</p> <p>This parameter defines the manner and color of event display in the System Monitor module</p> <p><i>In addition, this parameter is used when the database is exported to the S2000M (corresponds to the settings of renaming panel scenarios)</i></p> <p><i>The parameter value is selected from the dropdown list:</i></p> <div><div>Motion detector is Off</div><div><div>Main server connecting</div><div>Main workstation missed</div><div>Mains failure</div><div>Mains restored</div><div>Management scenario is run</div><div>Manual on valve</div><div>Manual on valve</div><div>Manual test</div><div>Message transmitted</div><div>Missed channel</div><div>Monitor is closing</div><div>Motion Detection Alarm</div><div>Motion detector is Off</div><div>Motion detector is On</div><div>Multiplex addressable loop is broken</div><div>Multiplex addressable loop is repaired</div><div>New vehicle detected</div></div></div> <p><i>Attention! When the database is exported to the S2000M panel, only the changed names of loops will be exported.</i></p> <p>Default value: empty field</p>

<b>Event Category</b>	Fires Alarms Malfunctions Arm/Disarm Loop Arm/Loop Disarm Miscellaneous Auxiliary Access Control Relay	<p>The category of event.</p> <p><i>This parameter is used when the database is exported to the S2000M (it corresponds to the settings of renaming panel scenarios) and defines whether an event will be stored in the S2000M buffer, displayed on an LCD, sent to a print , S21000 keypads and S2000-IN information panels</i></p> <p>A value is selected from the dropdown list:</p>  <p>Default value: empty field</p>
<b>Display Format</b>	Standard Partition Name Loop Name	<p>The event display format</p> <p><i>This parameter is used when the database is exported to the S2000M (it corresponds to renaming scenarios settings for the S2000M) and impact the view of event on LCD.</i></p> <p><i>The value is selected from the dropdown list:</i></p>  <p>Default value: No display format is selected</p>
<b>Text (Name)</b>	A string length of 1 to 100 characters	<p>Name of event</p> <p>A name typed in this field will be entered to the log of Database Administrator and buffer of the S2000M's event buffer.</p> <p><i>Please, note that if the database is exported to the S2000M, a name will be reduced to 16 characters!</i></p> <p>Default value: empty field</p>

### 6.14.3 Setting Event Groups

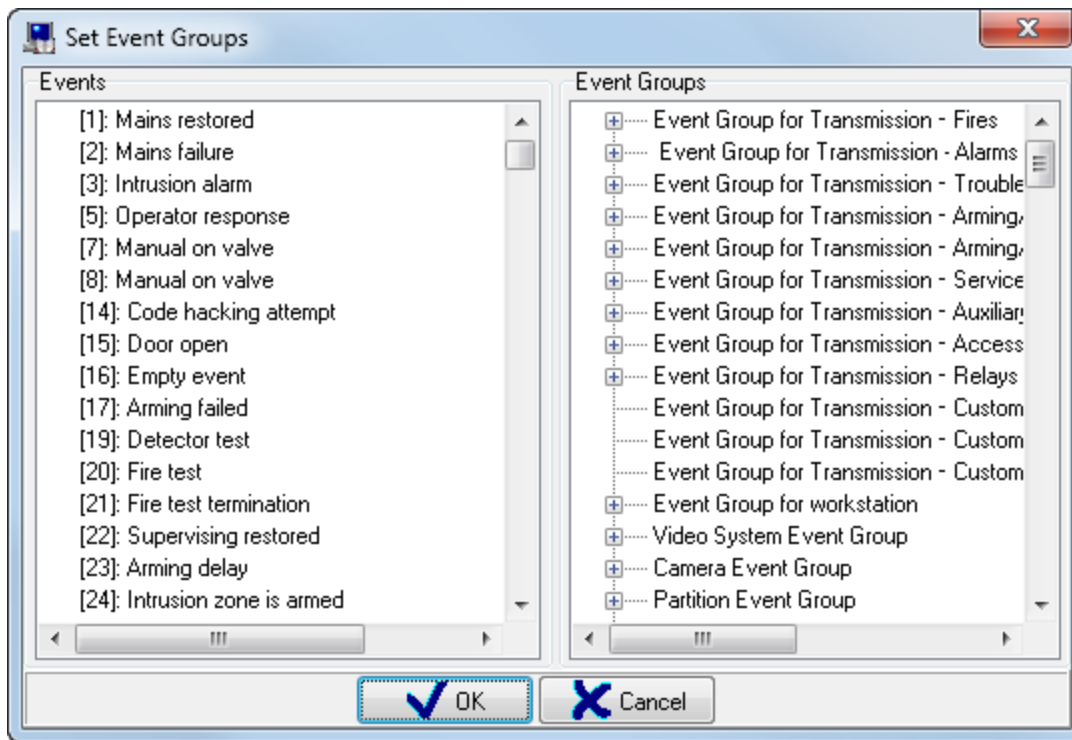
Most system entities have their own events that form event groups

For example, the event group for the Partition Group entity includes Arming Partition Group and Disarming Partition Group. There is no other event for the Partition Group entity.

The nature of entity events affects what entity events can trigger a management scenario and what entity events can be renamed (refer to Chapter 6.4.4 *Configuring System Responses to the Entity Events. Assigning Management Scenarios* and to Chapter 6.4.5 *Renaming System Events*). The event groups affect how events are filtered for transmission purposes. (Refer Chapter 6.4.2. *Configuring Transmission of Events and States of Logical Entities.*)

By default, there are partition groups created for all types of system entities in the Orion Pro Software, and these partition groups already include all necessary events. In some specific cases (the release of a device version requiring new events), the configuration of event groups can be modified.

To edit the event groups, go to **Options/Set Event Groups** to open the **Set Event Groups** dialog box:



The left pane of the **Set Event Groups** dialog box displays the list of all system events (arranged by event index, the right pane includes the list of event groups.

To add a new event to any event group, please select a required event in the list of events, and drag it to the event group you want.

To delete an event from an event group, please select a required event of the event group you want to edit, and press the <Del> button on the keyboard.

#### 6.14.3.1 Configuring Event Groups for Voice Alarms

Three are event groups related to Voice Alarm Module:

- **Voiced Events**
- **Events Voiced till Operator Response**
- **Prioritized Voiced Events**

The events, intended to trigger voice alarms, have to be included in the Voiced Events group. **If the event is NOT included into the Voiced Events group, this event will not be accompanied by a voice alarm regardless of other settings and event groups.** If an event is included to the **Voiced Events** group only, a voice notification will replay as many times as set for the **Voice notification replays** parameter in the workstation settings.

If an event is included in the Voiced till Operator Response group, voice notification will replays as much as 999 times. This is a practically equivalent to an infinite loop. The voice alarm (notification) for such an event can be interrupted by an operator only. Or this notification can be stopped in the voice alarm module, or in case of alarm (i.e. the voice notification (alarm) play can be stopped (interfered) by a more prioritized voice alarm.

If the event is included in Prioritized Voiced Events, the event voice notification will replayed, if occurs, between replays of a notification beyond the Prioritized Voiced Events. If a voiced event occurs at a time when prioritized voiced event is playing, this event will be put in the prioritized waiting list to be played right after the current voice notification. All other events beyond the Prioritized Events group will not be played until any prioritized events are active in the system.

The effects of each group are summed up. If an event is included in all groups, this event may be canceled only by an operator.



#### 6.14.4 Configuring Network Ports

The Orion Pro Suite can run more than 10 software modules with each of them taking its own TCP port address. When many software module run on the same workstation, it may be often necessary to change ports for the applications launched. This may be caused by the conflicts when two applications use the same “popular” address of three ports.

In addition, the setting selected ports can be useful when the TCP/IP ports are controlled by a fire wall and the narrow range of free ports (controlled or uncontrolled) have to be distributed among the applications (software modules).

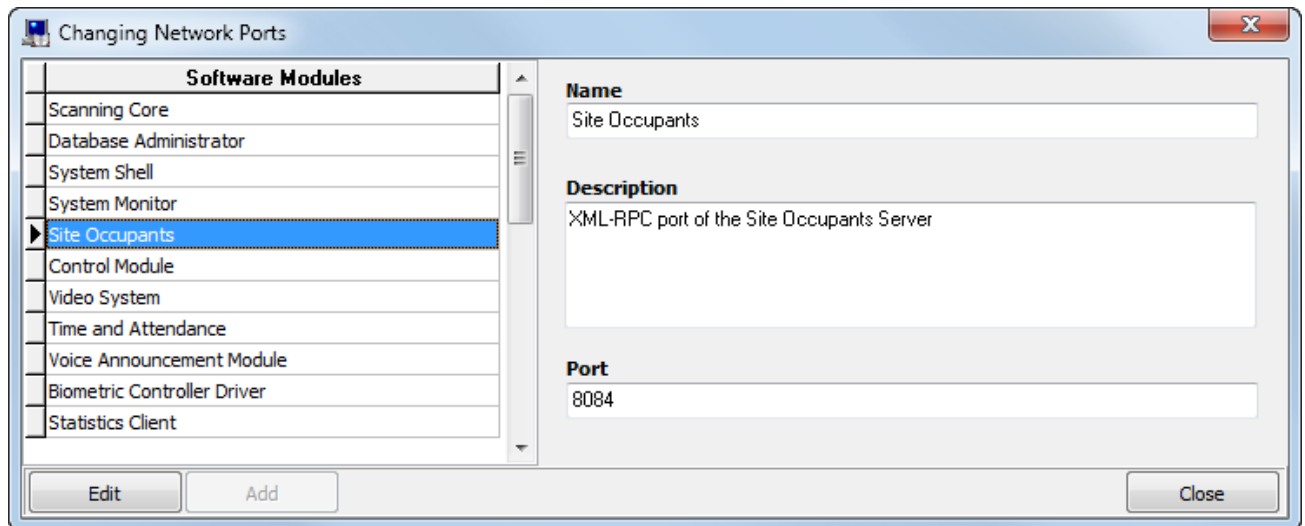
The Orion Pro Software supports changing ports for individual software modules:

Software module	Settings in the Change Network Ports menu in DBA	Manual configuration in the orion.ini file	Default port index
Database Server (CSO.exe)		Manually; an application restart is required (*)	2001
Database Administrator (Abd.exe)	Yes, effective after updating the database in the Operative Task		8081
Scanning Core (CoreOrion.exe)	Yes, effective after updating the database in the Operative Task		8080
System Shell (Shell.exe)	Yes, effective after updating the database in the Operative Task		8082
System Monitor (omonitor.exe)	Yes, effective after updating the database in the Operative Task		8083
Site Occupants (LockDown.exe)	Yes, effective after manual reconnection to the database		8084
Control Module (CoreOrion.exe)	Yes, effective after updating the database in the Operative Task		8085
Video System (Videodriver.exe)	Yes, effective after updating the database in the Operative Task		8086
Time and Attendance (NWTimePro.exe)	Yes, effective after manual reconnection to the database		8094
Voice Announcement Module (SoundServer.exe)	Yes, effective after updating the database in the Operative Task		8095
Biometric Controller Driver (badriver.exe)	Yes, effective after updating the database in the Operative Task		8096
Statistics Client (Stat.exe)	Yes, effective after updating the database in the Operative Task		8099
Personal Card (PersonCard.exe)	Yes, effective after updating the database in the Operative Task		8882
OPC Server	Yes, effective after updating the database in the Operative Task		7070
Dot-Matrix Display Driver (HelioRGM_Service.exe)	Yes, effective after updating the database in the Operative Task		7071
OrionPro 2 Protocol Driver	Yes, effective after updating		8100

	the database in the Operative Task		
Keybox Driver (KeyBoxServer.exe)	Yes, effective after updating the database in the Operative Task		8181
Port for Scanning Core to be linked with the Keybox driver (CoreOrion.exe)	Yes, effective after updating the database in the Operative Task		8183

(\*)Port for the Central Server is configured in the Orion.ini file on all workstations. Please use **Notepad** to open the Orion.ini file and change the SrvPort parameter in the SrvLog section. Then save changes and restart the system.

To configure the allocation of ports for other Orion Pro modules, please select Options/Configure Network



The appeared window will show available software modules and a default port used for launching the applications. To change port a port number, please click the **Edit** button, then make necessary changes and click the **Save** button. To apply settings, please close the window, update the database in the Scanning Core using the corresponding item in the DBA menu or reconnect software modules (applications) to the database (Time and Attendance, Site Occupants) (see the table above)

## Appendix 6.A Centralized Control Relay Programs

Number	Action Name	Description
1	Switch On	Switch On in case of Intrusion Alarm or Fire Alarm; otherwise switch Off
2	Switch Off	Switch Off in case of Intrusion Alarm or Fire Alarm; otherwise switch On
3	Switch On for a Time	If 'Intrusion alarm' or 'Fire alarm' - ON for a time; else OFF output.
4	Switch Off for a Time	If 'Intrusion alarm' or 'Fire alarm' - OFF for a time; else ON output.
5	Blink (Off is Initial Position)	If 'Intrusion alarm' or 'Fire alarm' - blink (0,5 s ON, 0,5 s OFF); Else OFF output.
6	Blink (On is Initial Position)	If 'Intrusion alarm' or 'Fire alarm' - blink (0,5 s ON, 0,5 s OFF); Else ON output.
7	Blink for a Time (Off is Initial Position)	If 'Intrusion alarm' or 'Fire alarm' - blink (0, 5 s ON, 0, 5 s OFF) during given time; else OFF output.

8	Blink for a Time (On is Initial Position)	If 'Intrusion alarm' or 'Fire alarm' - blink (0,5 s ON, 0,5 s OFF) during given time; else ON output
9	Lamp	If 'Fire alarm', 'Fire pre-alarm', 'Intrusion alarm', 'Entry alarm' or 'Arm failed', then blink (0,5 s ON, 0,5 s OFF); if 'Disconnected alarm loop', "Relay disconnected", "Fire trouble", "Loop open circuit", "Configuration error", "Open relay output", "Relay output short circuit", "Battery failed", "AC power failed", "Power failed", "2-wire line short circuit" or "2-wire line trouble", then blink (0,25 s ON, 1,75 s OFF); If there is at least one armed zone, then ON output; if all zones are disarmed, then OFF output.
10	Alarm Output 1	If all partitions are armed, then ON (close) outputs; else OFF (open) output.
11	ASPT	ON for a given time, if at least two zones in partition have 'Fire alarm' status and there are no zones having states "Auxiliary alarm", "Relay disconnected", "Open relay output", "Relay output short circuit". When the failure removed the relay output will be ON
12	Siren	If 'Fire alarm' then blink given time (1,5 s ON, 0,5 s OFF); if 'Attention', then blink given time (0,5 s ON, 1,5 s OFF); if 'Intrusion alarm', then ON for a given time; else OFF output.
13	Fire Output	If 'Fire alarm' or 'Fire pre-alarm', then ON (close) outputs; else OFF (open) output.
14	Fault Output	If there are zones in the states 'Disconnected alarm loop', "Relay disconnected", "Fire trouble", "Loop open circuit", "Configuration error", "Open relay output", "Relay output short circuit", "Battery failed", "AC power failed", "Power failed", "2-wire line short circuit" or "2-wire line trouble" or "Disarmed", "Disarmed and ready" "Disarmed and not ready", or "Arming has failed", then OFF (open) output.; else ON (close) output.
15	Fire Lamp	If 'Fire alarm', 'Fire pre-alarm', 'Intrusion alarm', 'Entry alarm' or "Arming has failed", then blink (0,5 s ON, 0,5 s OFF); if 'Disconnected alarm loop' or 'Fire alarm', then blink (0,25 s ON, 1,75 s OFF); if state of all relay associated zones is 'Zone armed', then ON; else OFF output.
16	Alarm Output 2	If all zones are armed or disarmed, then ON; else OFF output.
17	Switch On for a Time before Arming	If at least one zone is in "Arming delay" state, then ON for a given time; else OFF output.
18	Switch Off for a Time before Arming	If at least one zone is in "Arming delay" state, then OFF for a given time; else ON output.
19	Switch On for a Time upon Arming	If at least one zone is armed, then ON for a given time; else OFF output.
20	Switch Off for a Time upon Arming	If at least one zone is armed, then OFF for a given time; else ON output.
21	Switch On for a Time upon Disarming	If at least one zone is disarmed, then ON for a given time; else OFF output.

22	Switch Off for a Time upon Disarming	If at least one zone is disarmed, then OFF for a given time; else ON output.
23	Switch On for a Time if Arming Failed	If at least one zone is in the state 'Arm has failed', then ON for a given time; else OFF output.
24	Switch Off for a Time if Arming Failed	If at least one zone is in the state 'Arm has failed', then OFF for a given time; else ON output.
25	Switch On for a Time upon Auxiliary Alarm	If at least one zone is in the state 'Auxiliary alarm', then ON for a given time; else OFF output.
26	Switch Off for a Time upon Auxiliary Alarm	If at least one zone is in the state 'Auxiliary alarm', then OFF for a given time; else ON output.
27	Switch On upon Disarming	If at least one zone is disarmed, then ON; else OFF output.
28	Switch Off upon Disarming	If at least one zone is disarmed, then OFF; else ON output.
29	Switch On upon Arming	If at least one zone is armed, then ON; else OFF output.
30	Switch Off upon Arming	If at least one zone is armed, then OFF; else ON output.
31	Switch On upon Auxiliary Alarm	If at least one zone is in the state 'Auxiliary alarm', then ON; else OFF output.
32	Switch Off upon Auxiliary Alarm	If at least one zone is in the state 'Auxiliary alarm', then OFF; else ON output.
33	ASPT-1	ON for a given time, if at least one zone in partition have 'Fire alarm' status and there are no zones having states "Auxiliary alarm", "Relay disconnected", "Open relay output", "Relay output short circuit". When the failure removed the relay output will be ON
34	ASPT-A	ON for a given time, if at least two zones in partition have 'Fire alarm' status and there are no zones having states "Auxiliary alarm", "Relay disconnected", "Open relay output", "Relay output short circuit". When the failure removed the relay output will not be on
35	ASPT-A1	ON for a given time, if at least one zone in partition has 'Fire alarm' status and there are no zones having states "Auxiliary alarm", "Relay disconnected", "Open relay output", "Relay output short circuit". When the failure removed the relay output will not be on
36	Switch On if Temperature Increased	ON for a given time when the temperature has exceeded "temperature high" threshold (in "High temperature" status); else OFF output.
37	Switch On if Temperature Decreased	ON for a given time when the temperature has being below "temperature low" threshold (in "Low temperature" status); else OFF output.
38	Switch On if Extinguishing Initiation Delayed	ON for a given time during launching delay counting before automatic fire extinguishing system starting (in "Launching delay" state); else OFF.
39	Switch On if Extinguishing Initiated	ON for a given time if launching pulse for automatic fire extinguishing system has been given ("Launching" state); else OFF.
40	Switch On if Extinguishing Confirmed	ON if launching has been confirmed (in "Extinguishing" state); else OFF.
41	Switch On if Extinguishing Failed	ON if launching has been failed (in "Launch fault" state); else OFF.

42	Switch On if Auto Mode Enabled	ON in "Auto extinguishing" state; else OFF.
43	Switch Off if Auto Mode Enabled	OFF in "Auto extinguishing" state; else ON.
44	Switch On if Auto Mode Disabled	ON in "Manual extinguishing" state; else OFF.
45	Switch Off if Auto Mode Disabled	OFF in "Manual extinguishing" state; else ON.

#### Comments for the executive programs:

1) Devices of the latest versions support controlling their relay outputs with a delay. The delay time and the activation time can be selected in the range of 0 to 8,191.875 sec in increments of 1/8-sec. In addition, these devices support various types of 'blinking' patterns (sequence) differing in their periods and pulse ratio. Some devices of earlier versions don't support delay activation of the outputs with and support blinking only with frequency 1 Hz and pulse ratio 2, while the activation time can be given in the range of 0 to 255 seconds in increments of 1 second. The possibilities to control outputs of addressable executive modules S2000-SP2 are defined by the possibilities of the S2000-KDL described in the controller's Manual.

2) Outputs with assigned programs 9, 10, 13, 14, 15, 16 are controlled without delay.

3) Outputs with executive programs with constant action (e.g. Switch On or Alarm Output 1) are turned on (both for opening and closing) when the relevant activation condition has been met and retain in such state until the condition avoids. As soon as the condition has been false the relay outputs return to their initial state. On the contrary, the outputs with time limited programs (that is, with limited activation time) return to initial state not only when the activation conditions have disappeared but also if the time has elapsed. All the time limited programs will operate similarly to programs with constant action if the activation time is set to the maximum value being equal to 8,191.875 seconds. When the console has been powered on and has found a relay module, it switches the relays to the states which correspond to the current state of the partitions assigned with this relays. If a relay is operated by a time limited program, the console switches it to its initial state as if it has completed to work after a given time.

4) The programs 11, 33, 34, and 35 are designed to control fire-fighting equipment including fixed fire extinguishing installations. According to the requirements for fixed fire extinguishing systems, a fire extinguishing equipment can be activated only after receiving fire alarm messages from two independent alarm loops which monitor premises. To avoid leakage of an extinguishing agent (gas, dry chemical), the system can be discharged only when all the doors from the premises are closed. In addition, the circuits of light and sound alarms must be monitored for failures (open/short circuit failures), and the system must not be discharged in case a failure of a light or sound alarm. To monitor door positions, alarm loops of so called *Auxiliary* type are used. If a door open sensor has been activated (the relevant door has been open), the Auxiliary alarm loop enters Auxiliary Zone Alarm state. When the door has been closed, the Auxiliary alarm loop recovers its state within so called Recovery Time. To control light and sound alarms, one can use outputs of S2000-KPB devices which monitor their load circuits for open and short circuit failures. Output executive programs are implemented in such a way so that starting them is blocked up if a linked auxiliary alarm loop has been activated or an output circuit has found to be failed. As mentioned above, to create automatic fire extinguishing control in the premises there should be two or more fire alarm loops for these premises, the doors are to be monitored using auxiliary alarm loops, and alarms should be controlled by means of S2000-KPB outputs. These loops and outputs form a single *fire partition* associated with one or more outputs designated to give the start pulse and assigned with the ASPT executive program. If two or more fire alarm loops in the partition have been in alarm, the relay output turns on with given time and delay provided all the doors are closed and all sound and light alarms are operative. If at least one door is open or at least one alarm circuit is failed, the relay does not

start. If two latter conditions disappear with fire alarm being retain then outputs with the program 11 (ASPT) and the program 33 (ASPT-1) will be turned on with given delay while outputs with the program 34 (ASPT-A) and the program 35 (ASPT-A1) will not be turned on (but they will be turns on if there are no time limitations for control). There are other distinctions between the programs. Activation of relay outputs with the program 34 or the program 35 is blocked up if there are blocking conditions in any associated partition. On the contrary, an output with the program 11 or the program 33 will be turned on if there is at least one partition met the discharge conditions (there are fire alarms and there are no broken auxiliary alarm loop and failed outputs) without regard to another concerning partition states.

5) The executive programs 11 (ASPT) and 34 (ASPT-A) provide switching the output on both in case of activation of two smoke or heat detectors within a partition and in case of a signal from a manual call point if the zone of the manual call point is programmed with the type 'Manual Release' in the console configuration.

6) A Fault Output is used to monitor operative conditions of fire partitions. The output is opened when one of the following failures has been occurred:

- A fault of a fire alarm loop (short circuit, open circuit, or fault of the fire detector),
- A fault of a monitored circuit of an output (a short circuit failure or an open circuit failure of the relay output),
- A loss of connection between monitored alarm loops or outputs (loss of communication between the console and the control and indicating equipment or executive module connected via the RS-485 interface or disconnection of an addressable device or addressable executive module from the polling loop of an S2000-KDL controller),
- A fault of a device (a short circuit or an open circuit of the polling loop),
- A power failure of a device (power failure, battery failure, 220 V power failure),

Also, this output is to be open if the partition status is Disarmed and Arming Failed because these states are considered as inoperable conditions for fire partitions.

As this output is normally closed and opens to operate, powering off the relay modules and an open circuit failure of the wires conducting signals from relay outputs to a monitoring station are considered to be fault signals.

7) An output operated by the Fire Lamp program differs from an output operated by the Lamp program by being switched on only when all the partitions assigned with this output are armed.

8) The program 17 (Switch On for a Time before Arming) can be used to automatically reset responded four-wire detectors for arming. To do this, the detectors are powered through the normally closed contact of the relay output of an S2000-SP1 device. This output is to be assigned with the executive program 17, and the activation time should be selected to be sufficient to reset detectors. For the alarm loops which four-wire detectors are brought to an arming delay should be given. The arming delay must be more than the sum of the resetting time and the maximum restore time of detectors after power reset. As a result, when an arming command is given the relay will turn on for the given time switching off the power of the four-wire detectors and thus resetting the activated ones.

9) The programs 38 to 45 can be used when the S2000M console operates a fixed fire-fighting system (gas, dry chemical, or aerosol fire-fighting system) based on S2000-ASPT devices. These programs allow switching device outputs on or off either for a given time or without limitation, until the relevant condition is in effect. In order to operate outputs without time limitations, the activation time should be set to the maximum possible value (8,191.875 seconds).

The program 38, Switch On if Extinguishing Initiation Delayed can be used for activating audible alarms and light boxes "ESCAPE" and "KEEP OUT" when the discharge delay is being counted.

The Program 39 also can be used in a gas extinguishing system for several discharge areas with the common extinguishing installation, with each discharge area being protected by a separate S2000-ASPT. Each S2000-ASPT monitors states of fire detectors in its discharge area, and in case of a fire it generates a message about a discharge pulse and issues the control pulse which opens the gaseous discharge valve from the gas pipe to the area it protects. If extinguishing has been initiated in any discharge area, the console can issue a pulse to supply the gas into the shared pipe. The program 39, Switch On if

Extinguishing Initiated can be used for this purpose. The program 41, Switch On if Extinguishing Failed can be used for initiating a standby fire extinguishing installation.

1.2.23 The console provides organizing up to 32 Entrance Zones. An Entrance Zone is an intrusion alarm loop with alarm delay ability. The alarm delay (the entrance delay) permits entering to the protected area via the Entrance Zone without an immediate alarm and provides disarming the premises. The delay can be given as 0 to 254 s. When the entrance alarm loop has been activated, the console generates an ENTRY ALARM message.

If the delay has been elapsed but the Entrance Zone has been retaining in alarm, that is it has not yet been armed or disarmed, the console generates an INTRUSION ALARM message. The states Intrusion Alarm and Entry Alarm are differently processed by the relay executive programs (see Table 7). For example, if an output is assigned to the Siren executive program, then this output will not be switched in case of an Entry Alarm, but an output with the assigned Alarm Output 1 program will be opened.

The Entrance Zones given for the console are effective only for the device outputs which are controlled by the console and does not effect on outputs controlled by their intrusion and fire alarm panels.

## Appendix 6.5.Scenarios of Relay Output Centralized Control

Program No	Program Name	Program Description	Parameters
1	Switch On	Switch on in case of Intrusion Alarm or Fire Alarm; otherwise switch off	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
2	Switch Off	Switch off in case of Intrusion Alarm or Fire Alarm; otherwise switch on	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
3	Switch On for a Time	Switch on for a set time in case of Intrusion Alarm or Fire Alarm, otherwise switch off.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
4	Switch Off for a Time'	Switch off for a set time in case of Intrusion Alarm or Fire Alarm, otherwise switch on	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
5	Blink (Off is Initial Position)	If 'Intrusion alarm' or 'Fire alarm' - blink (0,5 s ON, 0,5 s OFF);	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Blinking Pattern Number</div>
6	Blink (On is Initial Position)	If 'Intrusion alarm' or 'Fire alarm' - blink (0,5 s ON, 0,5 s OFF);  otherwise ON output.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Blinking Pattern Number</div>

7	Blink for a Time (Off is Initial Position)	Blinks In case of 'Intrusion Alarm' or 'Fire Alarm' - blink (0.5 s ON, 0.5 s OFF) for a set time; otherwise OFF.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Blinking Pattern Number</div>
8	Blink for a Time (On is Initial Position)	Blinks (0,5 s ON, 0,5 c OFF) in case of 'Intrusion Alarm' or 'Fire Alarm' for a set time, otherwise ON	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div> <div>Blinking Pattern Number</div>
9	Lamp	Blinks (0,5 s ON, 0,5 s OFF in case of 'Fire alarm', 'Fire Pre-alarm', 'Intrusion alarm', 'Entry alarm' or 'Arm failed'; Blinks (0,25 s ON, 1,75 s OFF) in case of 'Disconnected alarm loop', "Relay disconnected", "Fire trouble", "Loop open circuit", "Configuration error", "Open relay output", "Relay output short circuit", "Battery failed", "AC power failed", "Power failed", "2-wire line short circuit" or "2-wire line trouble"; switch On in case of one zone armed at lease; switches Off is On if one zone is armed at least; the output if Off if all zones are disarmed	<div>Computer</div> <div>Relay</div>
10	Alarm Output 1	If all partitions are armed, then ON (close) outputs; otherwise OFF (open) output.	<div>Computer</div> <div>Relay</div>
11	ASPT	ON for a given time, if at least two zones in a partition have Fire Alarm status and there are no zones having states "Auxiliary alarm", "Relay disconnected", "Open relay output", "Relay output short circuit". When the failure removed the relay output will be ON	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
12	Siren	Pulsing for a set time (1.5s ON, 0,5s OFF) , in case of 'Fire Alarm' if 'Attention', then blink given time (0,5 s ON, 1,5 s OFF); if 'Intrusion alarm', then ON for a given time; otherwise OFF output.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
13	Fire Output	If 'Fire alarm' or 'Fire pre-alarm', then ON (close) outputs; otherwise OFF (open) output.	<div>Computer</div> <div>Relay</div>
14	Fault Output	If there are zones in the states 'Disconnected alarm loop', "Relay disconnected", "Fire trouble", "Loop open circuit", "Configuration error",	<div>Computer</div> <div>Relay</div>



		<p>“Open relay output”, “Relay output short circuit”, “Battery failed”, “AC power failed”, “Power failed”, “2-wire line short circuit” or “2-wire line trouble” or “Disarmed”, “Disarmed and ready” “Disarmed and not ready”, or “Arming has failed”, then OFF (open) output.; otherwise ON (close) output.</p>	
15	Fire Lamp	<p>In case of Fire, blink (0.25 s On, 0.25 Off)  In case of Fire Pre-alarm, blink (0.25 s On, 0,75 s Off);  In case of Intrusion Alarm, Entrance Zone Alarm or Failed Arming, blink (0.5 s On, 0.5 s Off);  In case of the followings (Zone Disconnected, Relay Disconnected, Failure", Zone Failure, Zone Short Circuit, Zone Parameter Error, Output Circuit Opened, Output Short Circuit, Battery Failure, Mains Failure, Power Supply Failure, Enclosure Tampering, Two-wire line short circuit, Two-wire line failure, Addressable Device Unstable Response, Addressable Device Wrong Response or Attention is Required, blink (0.25 s On, 1.75 s Off);  If case of all relay-associated Zones armed, On;  IN case of All loops disarmed, Off.</p>	<div>Computer</div> <div>Relay</div>
16	Alarm Output 2	If all zones of output-repeated partitions functions normally (armed or disarmed), On, otherwise Off	<div>Computer</div> <div>Relay</div>
17	Switch On for a Time before Arming	If at least one zone is in “Arming delay” state, then ON for a given time; otherwise OFF.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
18	Switch Off for a Time before Arming	If at least one zone is in “Arming delay” state, then OFF for a given time; otherwise ON output.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
19	Switch On for a Time upon Arming	If at least one zone is armed, then ON for a given time; otherwise OFF output.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
20	Switch Off for a Time upon Arming	If at least one zone is armed, then OFF for a given time; otherwise ON output.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>

21	Switch On for a Time upon Disarming	If at least one zone is disarmed, then ON for a given time; otherwise OFF output.	Computer Relay Action Delay Action Time
22	Switch Off for a Time upon Disarming	If at least one zone is disarmed, then OFF for a given time; otherwise ON.	Computer Relay Action Delay Action Time
23	Switch On for a Time if Arming Failed	If at least one zone is in the state 'Arm has failed', then ON for a given time; otherwise OFF.	Computer Relay Action Delay Action Time
24	Switch Off for a Time if Arming Failed	If at least one zone is in the state 'Arm has failed', then OFF for a given time; otherwise ON.	Computer Relay Action Delay Action Time
25	Switch On for a Time upon Auxiliary Alarm	If any auxiliary zones is alarmed, switched On for a set of time; otherwise Off	Computer Relay Action Delay Action Time
26	Switch Off for a Time upon Auxiliary Alarm	If any auxiliary zones is alarmed, switched On for a set of time; otherwise Off	Computer Relay Action Delay Action Time
27	Switch On upon Disarming	If at least one zone is disarmed, then ON; otherwise OFF.	Computer Relay Action Delay
28	Switch Off upon Disarming	If at least one zone is disarmed, then OFF; otherwise ON.	Computer Relay Action Delay
29	Switch On upon Arming	If at least one zone is armed, then ON; otherwise OFF output.	Computer Relay Action Delay
30	Switch Off upon Arming	If at least one zone is armed, then OFF; otherwise ON output.	Computer Relay Action Delay
31	Switch On upon Auxiliary Alarm	If at least one zone is in the state 'Auxiliary alarm', then ON;	Computer Relay Action Delay

32	Switch Off upon Auxiliary Alarm	If at least one zone is in the state 'Auxiliary alarm', then OFF;	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
33	ASPT-1	ON for a given time, if at least one zone in partition have 'Fire alarm' status and there are no zones having states "Auxiliary alarm", "Relay disconnected", "Open relay output", "Relay output short circuit". When the failure removed the relay output will be ON	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
34	'ASPT-A'	ON for a given time, if at least two zones in partition have 'Fire alarm' status and there are no zones having states "Auxiliary alarm", "Relay disconnected", "Open relay output", "Relay output short circuit". When the failure removed the relay output will not be on	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
35	'ASPT1-A'	ON for a given time, if at least two zones in partition have 'Fire alarm' status and there are no zones having states "Auxiliary alarm", "Relay disconnected", "Open relay output", "Relay output short circuit". When the failure removed the relay output will not be on	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
36	Switch On if Temperature Increased	ON for a given time when the temperature has exceeded "temperature high" threshold (in "High temperature" status);	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
37	Switch On if Temperature Decreased	ON for a given time when the temperature has exceeded "temperature high" threshold (in "High temperature" status);	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
38	Switch On if Extinguishing Initiation Delayed	ON for a given time during launching delay counting before automatic fire extinguishing system starting (in "Launching delay" state); otherwise OFF.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
39	Switch On if Extinguishing Initiated	ON for a given time if launching pulse for automatic fire extinguishing system has been given ("Launching" state); otherwise OFF.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
40	Switch On if Extinguishing Confirmed	ON if launching has been confirmed (in "Extinguishing"	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
41	Switch On if Extinguishing Failed	ON if Discharge failed (in "Discharge Failed" state); otherwise OFF.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>

42	Switch On if Auto Mode Enabled	ON in "Auto Mode" state; otherwise OFF.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
43	Switch Off if Auto Mode Enabled	OFF in "Auto Mode" state; otherwise ON.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
44	Switch On if Auto Mode Disabled	ON in Auto Mode Disabled status; otherwise OFF.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
45	Switch Off if Auto Mode Disabled	OFF in Auto Mode Disabled status; otherwise ON.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
46	ASPT with Release Hold <sup>(*)</sup>	<p>Switch On for a set time, if two zones at least go into the Fire Alarm with no hold conditions in place such as: Auxiliary Alarm, Output Disconnected, Output Circuit Open, and Relay Output Short Circuit). This condition prevents the activation, but the output will be activated as soon as the condition is terminated.</p> <p><i>Unlike the <b>ASPT</b> relay program, this action, the zone/loop status is analyzed in any relay-associated partition</i></p>	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
47	ASPT-1 with Hold <sup>(*)</sup>	<p>Switch on for a set time, if a partition's fire zone goes into the fire alarm with no hold conditions in place such as: Auxiliary Alarm, Relay Disconnected, Open Relay Output, Relay Output Short Circuit.</p> <p>This condition holds activation, but if a holding condition is terminated, the output will be activated.</p> <p><i>Unlike the ASPT relay program, for this action, the loop status is analyzed in any relay-associated partition.</i></p>	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
48	ASPT-A with Hold (Activation Hold) <sup>(*)</sup>	<p>Switches On for a set time, if two or more fire zones of a partition go into Fire Alarm with no holding condition in place such as: Auxiliary Alarm, Relay Disconnected, Open Relay Output, and Relay Output Short Circuit.</p> <p><b>If is a holding condition is terminated, the output still stays Off.</b></p> <p><b><i>Unlike the ASPT relay program, for this tactic, the loop status is analyzed in any relay-associated partition.</i></b></p>	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>

49	ASPT-A1 with Emergency Hold (Activation Hold) <sup>(*)</sup>	<p>Switch On for a set time, when a partition's fire zone go into Fire Alarm with no release hold conditions in place such as :</p> <p>Auxiliary Alarm, Relay Disconnected, Open Relay Output, Relay Output Short Circuit.</p> <p>If the hold condition is terminated, the output will remain Switched Off</p> <p><i>Unlike the ASPT relay (action) program, for this tactic, the loop status is analyzed in any relay-associated partition</i></p>	<table><tr><td>Computer</td></tr><tr><td>Relay</td></tr><tr><td>Action Delay</td></tr><tr><td>Action Time</td></tr></table>	Computer	Relay	Action Delay	Action Time
Computer							
Relay							
Action Delay							
Action Time							

<sup>(\*)</sup> Please note the S2000M does not include tactics (relay programs) from 46 to 49.

## Appendix 6.B. Standard Scenario Steps

Group of Scenario Steps	Scenario Step	Description	Parameters				
Device	Send Text Message	Send a text message to a device (only for S2000-K)	<table><tr><td>Computer</td></tr><tr><td>Device</td></tr><tr><td>Text</td></tr></table>	Computer	Device	Text	
	Computer						
	Device						
	Text						
Activate Playback	Playback a voice alarm/notification.  It provides voice alarm device with a playback scenario number, the time and delay for the playback that is initiated by an individual command for (Start/Stop Voice Alarm/Notification) for all devices shared one COM Port.	<table><tr><td>Computer</td></tr><tr><td>Device</td></tr><tr><td>Action Delay</td></tr><tr><td>Playing Time</td></tr><tr><td>Playback Number</td></tr></table>	Computer	Device	Action Delay	Playing Time	Playback Number
Computer							
Device							
Action Delay							
Playing Time							
Playback Number							
Deactivate Playback	Deactivates voice alarm/announcement This commands instructs a device that the Start/Stop voice alarm command means canceling voice alarm	<table><tr><td>Computer</td></tr><tr><td>Device</td></tr></table>	Computer	Device			
Computer							
Device							
Start/Stop Voice Alarm	A command that starts or stops a voice alarm function.  The actual action imitated by this command depends on preceding commands - 'Activate Playback' or 'Deactivate Playback' This instruction is sent to all devices sharing the COM port where this scenario step 'Device' is connected.	<table><tr><td>Computer</td></tr><tr><td>Device</td></tr></table>	Computer	Device			
Computer							
Device							

	Generate Audible Indication	<p>Generates an audible indication (signal) on a device.</p> <p>Types of audible indications:  Sound off  Single Beep  Double beep  Triple beep  Long beep  Intermittent beep</p> <p>This function is supported by the following devices: S2000M, S2000-K, S2000-KS, S2000-2, and S2000-4.</p>	<div>Computer</div> <div>Device</div> <div>Sound Type</div>
	Transmission Mode Control	<p>Control a transmitting mode of S2000-IT device</p> <p>Transmission Control Types:  <i>Suspend transmission over specified routes</i>  <i>Resume transmission over specified routes</i>  <i>Clear specified routes</i></p>	<div>Computer</div> <div>Device</div> <div>Transmission Mode</div>
Reader	Lock Access	<p>Locks access requested via a selected reader</p> <p>(In case of the S2000-2 device operating in the <b>One Door for Entry/Exit, Vehicle Barrier, or Mantrap</b> modes the lock down will be effective for both readers</p>	<div>Computer</div> <div>Reader</div>
	Open Access	<p>Opens free access for entry or exit via a access point controlled by a defined reader</p> <p>(In case of the S2000-2 device operating in the One Door for Entry/Exit, Vehicle Barrier, or Mantrap modes, it opens free access via both readers</p>	<div>Computer</div> <div>Reader</div>
	Restore Normal Access Control	<p>Restore normal credential-based access control procedures for a selected reader.</p> <p>In case of the S2000-2 device operating in the One Door for Entry/Exit, Vehicle Barrier, or Mantrap modes, it restores normal access control procedures for both readers).</p>	<div>Computer</div> <div>Reader</div>
	Grant Access	<p>Grants access via an access point to direction controlled by a defined reader</p>	<div>Computer</div> <div>Reader</div>

	Lock Exit Button	Locks access requested with an Exit button.  (In case of the S2000-2 device, it locks an Exit button controlling access in the same direction as the defined reader does In case of the S2000-4 device, its single Exit button will be locked	Computer Reader
	Unlock Exit Button	Restore an access granting function of an Exit button.  In case of the S2000-2 device, it unlocks an exit button controlling an access in the same direction as a defined reader.  In case of the S2000-4 device, its single Exit button will be unlocked.	Computer Reader
<b>Zone/Loop</b>	Arm Zone	Arms a selected loop	Computer Zone
	Disarm Zone	Disarms a selected loop / zone	Computer Zone
	Arm Zone with Delay	Delayed loop/zone arming	Computer Zone Delay Time
	Enable Auto Mode	Enables the automatic of fire extinguishing A corresponding device loop has to be selected.	Computer Zone
	Disable Auto Mode	Disable the automatic mode of fire extinguishing  The corresponding device zone has to be selected.	Computer Zone
	Reset Alarm	Silence a zone/loop alarm.	Computer Zone
	Arm Camera	Arm a selected camera	Computer Camera
	Disarm Camera	Disarm a selected camera	Computer Camera
	Start Recording	Starts recording from a selected camera	Computer Camera
	Stop Recording	Stops recording from a selected camera	Computer Camera
	Motion Detection On	Turns on video motion detection	Computer Camera
	Motion detection On	Turns off video motion detection	Computer Camera

	Display Image	Display a camera image	<div>Computer</div> <div>Camera</div>
	Hide Image	Hides a camera image	<div>Computer</div> <div>Camera</div>
	Rotate	Rotates camera to a preset position	<div>Computer</div> <div>Camera</div> <div>Position</div>
	Restore to original position	Restores a relay output to original status	<div>Computer</div> <div>Relay</div>
	Switch On	Initiates the <b>Switch On</b> relay action (program) for the selected output with a delay in sec as set in the <b>Action Delay</b> parameter.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
	Switch Off	Initiates the <b>Switch Off</b> relay action (program) for a selected output with a delay in sec as set in the <b>Action Delay</b> parameter.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div>
	Switch On for a Time	Initiates the <b>Switch On for a Time</b> relay action (program) for a selected output with a delay in seconds as set in <b>Action Delay</b> and <b>Action Time</b> parameters.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
	Switch Off for a Time	Initiates the <b>Switch Off for a Time</b> relay action (program) for a selected output with a delay in sec as set in <b>Action Delay</b> and <b>Action Time</b> parameters.	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div>
	Blink (OFF is Initial Position )	Initiates the <b>Blink (OFF is Initial Position)</b> relay action with a delay in seconds as set for the <b>Action delay</b> parameter	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Blinking Pattern Number</div>
	Blink (ON is Initial Position )	Initiates the <b>Blink (ON is Initial Position )</b> relay action for a selected relay with delay initiation as set in the <b>Action delay</b> parameters, as well as with a selected Blinking Pattern	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Blinking Pattern Number</div>
	<b>Blink for a Time (OFF is Initial Position )</b>	Initiates the <b>Blink for a Time (OFF is Initial Position)</b> relay action with initiation delay and time (in seconds) as set in the <b>Action Delay</b> and <b>Action Time</b> parameters, as well as with selected Blinking Pattern	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div> <div>Blinking Pattern Number</div>



Blink for a time (ON is Initial Position )	Initiates the <b>Blink for a Time (ON is Initial Position )</b> relay action with initiation delay and time (in seconds) as set in the <b>Action delay</b> and <b>Action time</b> parameters, as well as with a selected Blinking Pattern	<div>Computer</div> <div>Relay</div> <div>Action Delay</div> <div>Action Time</div> <div>Blinking Pattern Number</div>
Arm Partition Group	Arms a selected partition group.	<div>Computer</div> <div>Partition Group</div>
Disarm Partition Group	Disarms a partition group.	<div>Computer</div> <div>Partition Group</div>
Arm a partition group if the last person leaves a selected zone	Arms a partition group if the last person leaves a selected zone.	<div>Computer</div> <div>Partition Group</div> <div>Access Zone</div>
Disarm a partition group when a first person enters a selected zone	Disarms a partition group when a first person comes in a selected zone	<div>Computer</div> <div>Partition Group</div> <div>Access Zone</div>
Arm a partition group after a last person with an access level leaves a selected zone	Arming a partition group after a last person with a defined access level leaves a selected access zone	<div>Computer</div> <div>Partition Group</div> <div>Access Zone</div> <div>Access Level</div>
Disarm a partition group after a first person with an access level enters selected access zone	Disarming a partition group of a first person with a defined access level enters a selected access zone	<div>Computer</div> <div>Partition Group</div> <div>Access Zone</div> <div>Access Level</div>
Arm a partition group when the last person of a department leaves an access zone	Arms a selected partition group if the last person of the selected department has left the selected access zone.	<div>Computer</div> <div>Partition Group</div> <div>Access Zone</div> <div>Department</div>
Disarm a partition group when the first person from a department enters a access zone	Disarms a partition group when the first person from a selected department enters a selected access zone	<div>Computer</div> <div>Partition Group</div> <div>Access Zone</div> <div>Department</div>
Activate ASPT	Activated fire extinguishing system  A partition group containing all loops of a required S2000-ASPT or Potok-3N is set in the <b>Partition</b> parameter	<div>Computer</div> <div>Partition</div>

	Enable Auto Mode	Enables automatic fire extinguishing mode of the S2000-ASPT or Potok-3H devices. A partition containing all loops of a required device is to be select in the Partition parameter	<div>Computer</div> <div>Partition</div>
	Disable Auto Mode	Disables the automatic fire extinguishing mode of the S2000-ASPT or Potok-3H devices.  A partition containing all loops of a required device is to be select in the Partition parameter	<div>Computer</div> <div>Partition</div>
	Reset Alarm	Silences an alarm in a selected partition, and then rearms it again	<div>Computer</div> <div>Partition</div>
	Arm partition	Arms a selected partition.	<div>Computer</div> <div>Partition</div>
	Disarm partition	Disarms a selected partition	<div>Computer</div> <div>Partition</div>
	Arm workstation-associated partitions	Arms all partitions associated to a selected workstation/computer.	<div>Computer</div>
	Disarm workstation-associated partitions	Disarms all partitions associated to a selected workstation.	<div>Computer</div>
	Arm a partition when the last person leaves a selected zone.	Arms a selected partition if the last employee leaves a selected access zone.	<div>Computer</div> <div>Partition</div> <div>Access Zone</div>
	Disarm a partition when the first person enters a selected zone	Disarms a selected partition, when the first employee enters in a selected access zone.	<div>Computer</div> <div>Partition</div> <div>Access Zone</div>
	Disarm workstation-associated partitions when the first person enters a selected zone	Disarms all partitions of a selected workstation, if the first person enters a selected access zone.	<div>Computer</div> <div>Supervised Zone</div>
	Arm all workstation-associated partitions when the last person leaves a selected zone	Arms all partitions of a selected workstation, if the last employee left a selected access zone.	<div>Computer</div> <div>Supervised Zone</div>
	Arm a partition when the last person with an access level leaves an access zone	Arms a partition if the last person with a selected access level leaves a selected access zone.	<div>Computer</div> <div>Partition</div> <div>Access Zone</div> <div>Access Level</div>
	Disarm a partition when the first person with an access level enters an access zone	Disarms a partition if the first person with an access level enters an access zone	<div>Computer</div> <div>Partition</div> <div>Access Zone</div> <div>Access Level</div>

	Arm a partition when the last person of a department leaves a zone	Arms a selected partition when the last person of a selected department leaves a selected zone.	<div>Computer</div> <div>Partition</div> <div>Access Zone</div> <div>Department</div>
	Disarm a partition when the first person of a department enter a zone	Disarms a selected partition when the first person of a selected department enter a selected access zone	<div>Computer</div> <div>Partition</div> <div>Access Zone</div> <div>Department</div>
<b>Core</b>	Display Message in a Pop-Up Window	Displays a text message in a pop-up window.	<div>Computer</div> <div>Text</div>
	Send Text Message to the Scanning Core	<p>Sends a text message to a core (the Scenarios tab).</p> <p><i>This scenario step will run in all Scanning Cores if the scenario is not launched by an event.</i></p>	<div>Text</div>
	Delay	<p>Delays the initiation of a scenario as set in seconds</p> <p><i>This scenario step will run in all Scanning Cores if the scenario is not launched by an event.</i></p>	<div>Pause</div>
	Delay with Countdown Window	Suspend the initiation of a scenario as set in seconds, with a countdown window popped up.	<div>Delay</div>
	Request to Operator	Displays a window with a request to Operator. It shows message and action time-out. It also shows a scenario to be started if an operator chose Yes, and another scenario, if he chose No, otherwise it times out	<div>Computer</div> <div>Text</div> <div>Query Time</div> <div>Execute Script, if 'YES'</div> <div>Execute Script, if 'NO'</div>
	Play sound	Plays a .wav file.	<div>Computer</div> <div>File</div>
	Start External Program	Starts an external program (.exe file).	<div>Computer</div> <div>Program</div>
	Compose and Send Email	Sends e-mail but first requests Operator for the details: email recipient address, email subject and body.	<div>Computer</div> <div>Server Port</div> <div>SMTP Host</div> <div>Login</div> <div>Password of Sender's Mailbox</div> <div>Sender Address</div>

	Send Email	Send e-mail using presets	<div>Computer</div> <div>Server Port</div> <div>SMTP Host</div> <div>Login</div> <div>Password of Sender's Mailbox</div> <div>Sender Address</div> <div>Recipient Address</div> <div>Subject</div>
	Send Email on Event	Sends an e-mail with detailed description of event triggered the scenario.	<div>Computer</div> <div>Server Port</div> <div>SMTP Host</div> <div>Login</div> <div>Password of Sender's Mailbox</div> <div>Sender Address</div> <div>Recipient Address</div> <div>Subject</div>
	Play a Custom Voice Message	Plays a voice message on a selected workstation  A played message is entered as a written text	<div>Computer</div> <div>Message</div> <div>Repeat</div> <div>Pause</div>
	Play Interface Event Message	Plays a voice message, on a selected computer, about event triggered the scenario.	<div>Computer</div> <div>Repeat</div> <div>Pause</div>
	Save Event to Log	Saves a user event to the Event Log	<div>Computer</div>
	Disable Voice Announcement	Disables voice announcement in the message synthesizer (the Sound-Off mode of message synthesizer).  The voice announcement enabled can be by the Enable voice announcement scenario or by instruction from the System Monitor, in the synthesizer or by restarting the synthesizer	<div>Computer</div>
	Enable Voice Announcement	Enable voice announcement in the message synthesizer on a selected computer.	<div>Computer</div>

	Execute Script	Execute a selected scenario (script) with a delay as set in seconds  <i>This scenario step will run in all Scanning Cores, if the scenario is not triggered by an event.</i>	<table><tr><td>Scenario</td><td></td></tr><tr><td>Delay</td><td>0</td></tr></table>	Scenario		Delay	0																
Scenario																							
Delay	0																						
Monitor	Request to Operator	Displays a window with a request to Operator. It shows message and action time-out. It also shows a scenario to be started if an operator chose Yes, and another scenario, if he chose No, otherwise it times out.	<table><tr><td>Computer</td><td><input type="text"/></td></tr><tr><td>Text</td><td></td></tr><tr><td>Query Time</td><td>10</td></tr><tr><td>Execute script, if Yes</td><td></td></tr><tr><td>Execute script, if No</td><td></td></tr></table>	Computer	<input type="text"/>	Text		Query Time	10	Execute script, if Yes		Execute script, if No											
	Computer	<input type="text"/>																					
	Text																						
	Query Time	10																					
Execute script, if Yes																							
Execute script, if No																							
	Send Text Message to Monitor	Display a text message in a pop-up window.	<table><tr><td>Computer</td><td></td></tr><tr><td>Message</td><td></td></tr></table>	Computer		Message																	
Computer																							
Message																							
	Compose and Send Email	Sends e-mail preliminary requesting Operator for the details: email recipient address, subject, and text of an email message.	<table><tr><td>Computer</td><td></td></tr><tr><td>Server Port</td><td></td></tr><tr><td>SMTP Host</td><td></td></tr><tr><td>Login</td><td></td></tr><tr><td>Password of Sender's Mailbox</td><td></td></tr><tr><td>Sender Address</td><td></td></tr><tr><td>Recipient Address</td><td></td></tr><tr><td>Subject</td><td></td></tr><tr><td>Email Body</td><td></td></tr><tr><td>Sound Type</td><td></td></tr></table>	Computer		Server Port		SMTP Host		Login		Password of Sender's Mailbox		Sender Address		Recipient Address		Subject		Email Body		Sound Type	
Computer																							
Server Port																							
SMTP Host																							
Login																							
Password of Sender's Mailbox																							
Sender Address																							
Recipient Address																							
Subject																							
Email Body																							
Sound Type																							
	Send Email	Send e-mail using presets	<table><tr><td>Computer</td><td></td></tr><tr><td>Server Port</td><td></td></tr><tr><td>SMTP Host</td><td></td></tr><tr><td>Login</td><td></td></tr><tr><td>Password of Sender's Mailbox</td><td></td></tr><tr><td>Sender Address</td><td></td></tr><tr><td>Recipient Address</td><td></td></tr><tr><td>Subject</td><td></td></tr><tr><td>Email Body</td><td></td></tr><tr><td>Sound Type</td><td></td></tr></table>	Computer		Server Port		SMTP Host		Login		Password of Sender's Mailbox		Sender Address		Recipient Address		Subject		Email Body		Sound Type	
Computer																							
Server Port																							
SMTP Host																							
Login																							
Password of Sender's Mailbox																							
Sender Address																							
Recipient Address																							
Subject																							
Email Body																							
Sound Type																							
	Play Custom Voice Message	Play a custom voice message on a selected computer  A voice message is entered as a text	<table><tr><td>Computer</td><td></td></tr><tr><td>Message</td><td></td></tr><tr><td>Repeat</td><td></td></tr><tr><td>Pause</td><td></td></tr></table>	Computer		Message		Repeat		Pause													
Computer																							
Message																							
Repeat																							
Pause																							

	Play Interface Event Message	Plays a voice message, on a selected computer, about event triggered the scenario.	<div>Computer</div> <div>Message</div> <div>Repeat</div> <div>Pause</div>
	Start Screen Saver	Starts the screensaver on a selected workstation	<div>Computer</div>
	Open the <b>Switch Operator</b> window	Opens the <b>Switch Operator</b> window	<div>Computer</div>
	Generate a shift report	Generates the shift reports on a selected workstation	<div>Computer</div>