



Areashell

Administrator's guide

Deployment, Configuration, and Administration of Areashell Software

Version 1.7

Last updated: 2019-02-12

© 2019 Areashell Inc. All rights reserved.

Trademarks

Areashell, Areashell AM are trademarks or registered trademarks of Areashell Inc. in the U.S., Russia and other countries.

Other company and product names mentioned herein may be trademarks of their respective companies.

Limitation of liability

Every effort to ensure the reliability and accuracy of the information has been taken in compiling this guide. This manual is subject to change in accordance with the dynamics of development of the product and may not contain the most recent versions of screen shots, parameters, and other characteristics of the product. Company Areashell Inc. is not responsible for printing or clerical errors.

Under no circumstances will Areashell Inc. and its partners be responsible for errors and/or omissions in this document, and incurred in connection with the losses of the purchaser of the product (whether direct or indirect, including loss of profits).

Third-party products are mentioned for information purposes only or for Areashell AM dependency configuration. Company Areashell Inc. is not responsible for the performance or use of these products.

All agreements or warranties, if any, take place directly between the supplier and the user of the product.

Official Web-site: <http://www.areashell.com>

Contents

1	Work in the Management Console	5
1.1	Work with the list of objects in the system configuration	5
1.2	Creation of configuration objects	6
1.3	Viewing and editing the configuration parameters of objects	7
1.4	Deleting configuration objects	8
2	Configuring the system	9
2.1	License registration	9
2.2	Directory service integration	9
2.2.1	Connection settings to the Active Directory directory service	9
2.2.2	Connection Settings LDAP directory service	10
2.3	Email system integration	11
2.4	Configuring HID VertX / EDGE access control controllers	13
2.4.1	Configuring HID VertX / EDGE card formats	13
2.4.2	Configuring HID VertX / EDGE card sets	15
2.4.3	Configuring HID VertX / EDGE keypad translations	16
2.4.4	Configuring HID VertX / EDGE controllers	17
2.4.5	Configuring HID VertX / EDGE readers	20
2.4.6	Configuring HID VertX / EDGE inputs	23
2.4.7	Configuring HID VertX / EDGE outputs	24
2.4.8	Configuring HID VertX / EDGE output groups	24
2.4.9	Configuring reader groups	25
2.5	Configuring areas	26
2.6	Configuring graphics maps	30
2.7	Configuring the automation subsystem	31
2.7.1	Configuring macros	31
2.7.2	Configuring event triggers	32
2.7.3	Configuring macro execution schedules	34
3	Administering access policies	35
3.1	General principles of administrative access policies	35
3.2	Holidays	35

3.3	Time schedules	37
3.4	User Roles	38
3.4.1	Role permissions	38
3.4.2	Role permission inheritance	42
3.5	User groups	43
4	User Administration	46
4.1	User registration	47
4.1.1	Registering users manually.....	47
4.1.2	Registering users through importing data from directory services	50
4.1.3	Registering users by importing data from a file	50
4.2	User data editing.....	51
4.3	User Rights Management	51
4.1	Administration of user credentials.....	54
5	System monitoring and control.....	58
5.1	Alarm acknowledgment	59
5.2	Event monitoring in table mode	60
5.3	System monitoring in areas mode	62
5.4	System monitoring in graphic map mode.....	69
6	Reports.....	70
7	Technical support	75

1 Work in the Management Console

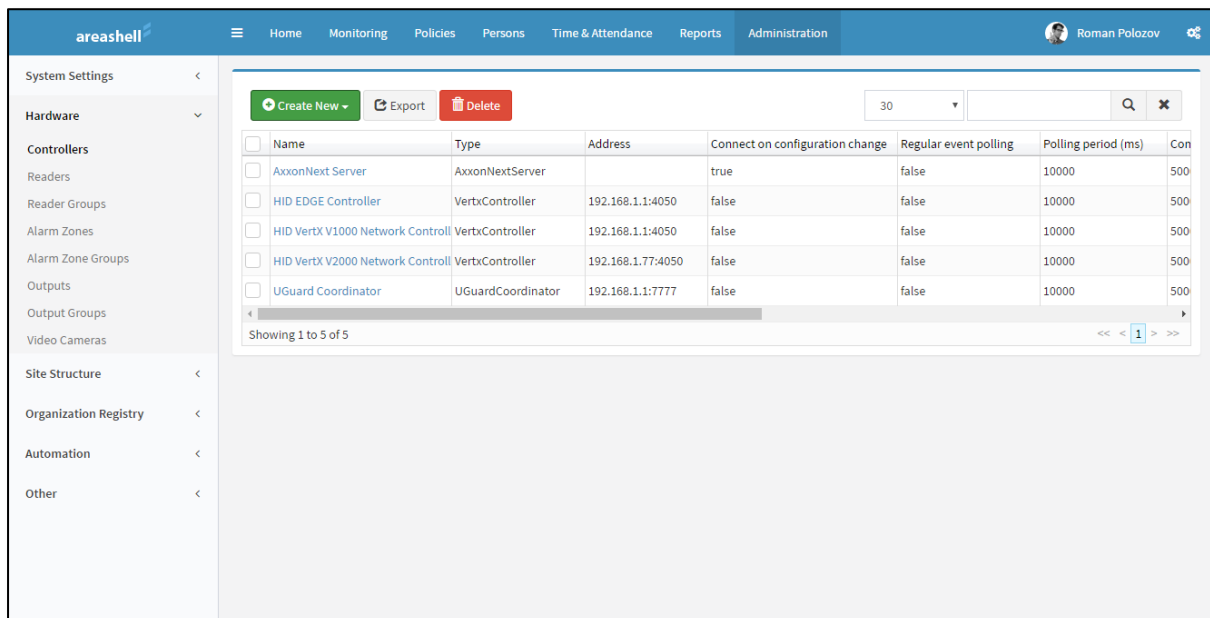
All system control elements in the management console are grouped in the sections:

- Monitoring – monitoring the current situation in the system, monitoring events occurring in the system, controlling the hardware;
- Policies – setting and administration of user access policies in areas, to areas controlled territory and the system functions;
- Persons – registration and user administration, accounts, cards and other identifiers;
- Reports – View and manage reports based on the information stored in the system;
- Administration - the administration of all aspects of the functioning of the system, including hardware, graphical plans, the internal parameters of the system, and others.

1.1 Work with the list of objects in the system configuration

The entire system configuration is stored in the form of configuration objects. All configuration objects in the management console to administer sections are grouped by type and destination in the Forums.

To view the list of existing objects in the system configuration, select the appropriate section in the main (upper) Management Console menu, and then – one of the subsections of the selected partition. A panel opens with a list of objects of the appropriate type.



The screenshot shows the Areashell Management Console interface. The top navigation bar includes 'Home', 'Monitoring', 'Policies', 'Persons', 'Time & Attendance', 'Reports', and 'Administration'. The left sidebar shows a tree view with 'System Settings' expanded, containing 'Hardware', 'Site Structure', 'Organization Registry', 'Automation', and 'Other'. The main content area displays a table of hardware objects under the 'Hardware' section. The table has columns for Name, Type, Address, Connect on configuration change, Regular event polling, Polling period (ms), and Con. There are 5 objects listed, with pagination showing 'Showing 1 to 5 of 5'.

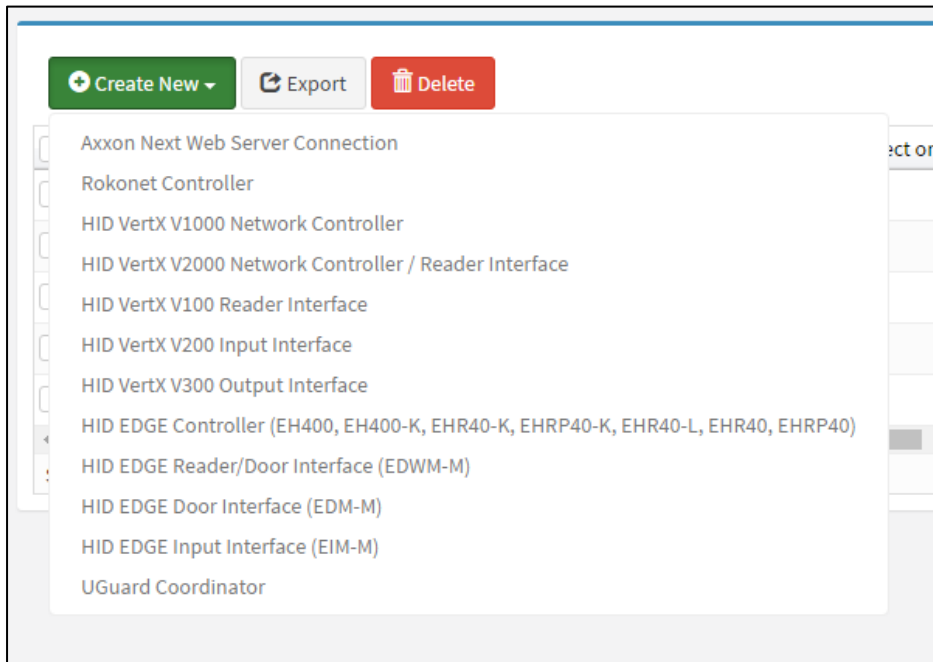
Name	Type	Address	Connect on configuration change	Regular event polling	Polling period (ms)	Con
AxonNext Server	AxonNextServer		true	false	10000	500
HID EDGE Controller	VertxController	192.168.1.1:4050	false	false	10000	500
HID VertX V1000 Network Controll	VertxController	192.168.1.1:4050	false	false	10000	500
HID VertX V2000 Network Controll	VertxController	192.168.1.77:4050	false	false	10000	500
UGuard Coordinator	UGuardCoordinator	192.168.1.1:7777	false	false	10000	500

To sort out the table with objects, click on the needed title. In the case of a large number of objects that do not fit on one page, you can navigate between pages by using the links

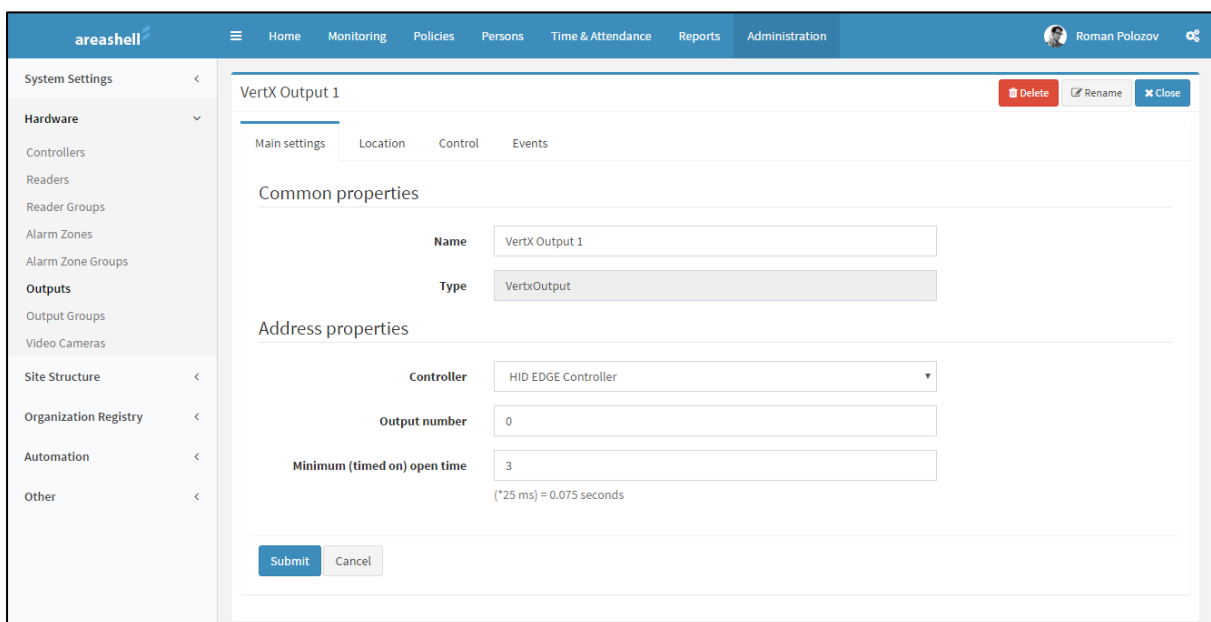
at the bottom of the panel. Use the controls in the toolbar to change the number of lines displayed on one page, filter objects by name, export a table in external file.

1.2 Creation of configuration objects

To create new configuration objects press the button *Create* and select the type of the object in the drop-down menu.



The properties window of the newly created object of a selected type with the default settings will open. Enter or change the necessary parameters for the created object and then click Save.



After saving or without saving the new object, a table of objects of the appropriate type displays.

1.3 Viewing and editing the configuration parameters of objects

To view and edit the configuration of a particular object select it in the table.

The table panel with a list of properties for the selected object opens instead of the table.

The screenshot displays the Areashell Administration web interface. The top navigation bar includes links for Home, Monitoring, Policies, Persons, Time & Attendance, Reports, and Administration. The left sidebar shows a tree view with categories like System Settings, Hardware, Site Structure, Organization Registry, Automation, and Other. The 'Notification Templates' section is expanded. The main content area is titled 'Common properties' and contains a form for editing a 'Notification Template 1'. The form fields are: Name (Notification Template 1), Type (NotificationTemplate), From (admin@areashell.com), To (users@areashell.com), Subject (Alarm Event!), and Text body (Alarm event from Areashell AM demo server). At the bottom of the form are 'Submit' and 'Cancel' buttons.

Typically, the object parameters window contains several tabs.

In case of object settings changes on any of the tabs, press the Save button to save the changes to the database or Cancel - to cancel the changes.

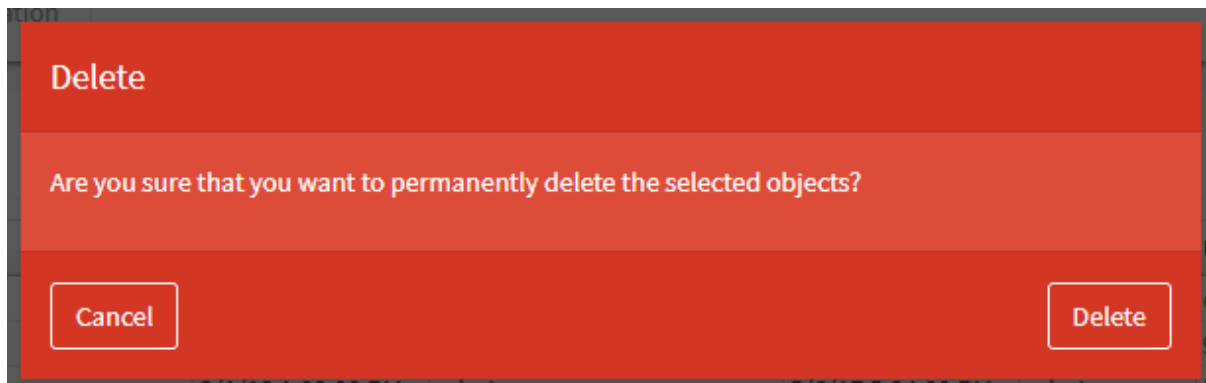
To change the name of an object, press RENAME. Usually in the list of object bookmarks there is a tab Properties with a field NAME. It is also possible to rename the object by changing the value of this field and pressing the Save button.

To go back to the table with objects, press the Close button in the toolbar.

To delete the selected object and return to the table with objects, click the Delete button in the toolbar and confirm the deletion in the pop-up window.

1.4 Deleting configuration objects

To delete any configuration system objects in the table, mark these objects in the left column, click Delete and confirm the deletion in the pop-up window.



When trying to delete some of the configuration objects, an error message on the console may appear. Usually this means that the object is used by other system objects and can not be deleted without first deleting references to it.

2 Configuring the system

2.1 License registration

Select Administration / Settings / System Information to view the information about the registered Areashell AM license, register or renew the license. In this section, information on the registered license, end user, distributor, the available and used at the current time memory on the server displays. To register a new license:

- Click Select file;
- Select the needed license file window and click Open;
- Click Upload a file;
- Information about a new license displays in the management console;
- Check the license parameters and click Save.

2.2 Directory service integration

Areashell AM supports integration with LDAP directory services and Microsoft Active Directory to implement two functions:

- Authenticate Areashell AM users using directory services;
- Import data from a directory service users in Areashell AM system.

Areashell AM User Authentication Setting using a directory service is described in the installation manual Areashell AM.

This section describes how to configure the user data import functions from a directory service in Areashell AM system.

To connect Areashell AM to directory service, create an LDAP entity type compound, and set the settings for a directory service in its settings.

2.2.1 Connection settings to the Active Directory directory service

To connect to the Active Directory server, the following set of parameters can be used:

- Server Type: Active Directory
- Server name: <network name or IP-address of the Active Directory server>
- Server Port: 389
- User name: administrator@domainname.com
- Root DN: CN = Users, DC = domainname, DC = com
- Filter: (& (objectClass = user) (objectCategory = person))
- Processing Boundaries: Subtree

To connect to a server on the Active Directory Global Catalog mode the following set of parameters can be used:

- Server Type: Active Directory
- Server name: <network name or IP-address of the Active Directory server>
- Server Port: 3268

- User name: administrator@domainname.com
- Root DN: <empty>
- Filter: (& (objectClass = user) (objectCategory = person))
- Processing Boundaries: Subtree

The screenshot displays the 'Administration' section of the Areashell web interface. On the left is a sidebar with a tree view containing 'System Settings' (expanded), 'Hardware', 'Site Structure', 'Organization Registry', 'Automation', and 'Other'. Under 'System Settings', 'LDAP Connections' is selected. The main content area is titled 'Common properties' and 'Server settings'. In 'Common properties', the 'Name' is 'AD Connection' and the 'Type' is 'LDAPConnection'. In 'Server settings', the 'Server type' is 'Active Directory'. There is an unchecked checkbox for 'Disabled users processing'. The 'Server name' is 'pdc.areashell.com' and the 'Server port' is '389'. There is an unchecked checkbox for 'SSL connection'. The 'User name' is 'administrator@demo.areashell.com' and the 'Set user password' checkbox is checked. The 'User password' field contains six asterisks. The 'Root DN' is 'CN=Users,DC=demo,DC=areashell,DC=com'. The 'Filter' is '(&(objectClass=user)(objectCategory=person))'. The 'Scope' is 'Subtree'. At the bottom of the form are buttons for 'Check connection', 'Import users', 'Generate HID VeriX/EDGE RFIDs', 'Generate UGuard RFIDs', 'Submit', and 'Cancel'.

2.2.2 Connection Settings LDAP directory service

To connect to the LDAP server, the following set of parameters may be used:

- Server Type: LDAP
- Server name: <network name or IP-address of the LDAP server>
- Server port: 389
- User name: administrator@domainname.com
- Root DN: DC = domainname, DC = com
- filter: (& (objectClass = user) (objectCategory = person))
- Processing Boundaries: Subtree

2.3 Email system integration

Areashell AM supports integration with e-mail systems, supporting SMTP to send e-mail notifications.

To configure sending e-mail notifications when certain events occur (for example, breaking doors and other alarms) follow the steps:

- Register your SMTP-server under Servers notifications;
- Create a template with text notification e-mail message;
- Create a macro with the command Send the notice, specifying the created notification server, the notification template and postal address of the recipient;
- Create a trigger message indicating the created macro command and setting the filter parameters for the events.

To connect Areashell AM to the e-mail server, create SMTP-server object or alike in Administration / Settings / Notification Servers and specify in its settings connection parameters to your email server.

The screenshot displays the 'SMTPConnection' configuration page within the Areashell Administration interface. The left sidebar shows the navigation menu with 'System Settings' expanded, leading to 'Notification Servers'. The main content area is titled 'SMTPConnection' and includes tabs for 'Properties' and 'Events'. The 'Properties' tab is active, showing various configuration sections:

- Common properties:** Name (SMTPConnection), Type (SMTPConnection).
- Server settings:** Server name (smtp.gmail.com), Server port (465), Secure channel protocol (None, SSL, TLS), User name (administrator), User password (Password).
- Message sending properties:** From name (Areashell), From email (donotreply@somedomain.com).
- Test configuration:** To (toaddress@domain.com), Subject (Test message), Message text (This is a test message from Areashell Security System.).

At the bottom of the form are 'Submit' and 'Cancel' buttons. A 'Test configuration' button is also present within the test configuration section. The top of the interface shows the Areashell logo, navigation tabs (Home, Monitoring, Policies, Persons, Time & Attendance, Reports, Administration), and a user profile for Roman Polozov.

To send e-mail notifications by using the registered server, create notification templates (emails). Templates are created in Administration / Settings / Notification templates.

When creating an e-mail notification template in the fields Subject and Message, use variables that will be replaced by the values of the event that initiated notification.

The variable name begins with '\$ {' and ends with '}' (without the quotes).

Currently supported variables are described in the table:

Variable	Comment
<code>\${event.alarmLevel}</code>	Event alarm level
<code>\${event.priority}</code>	Event priority
<code>\${event.eventCode}</code>	Event code
<code>\${event.timeLocal}</code>	Local time of occurrence of the event (in the case of an event message received from the hardware controller – its local time)
<code>\${event.timeGlobal}</code>	UTC time when the event occurred
<code>\${event.regTime}</code>	Time of event registration in system server (may differ from local time if an event occurs in offline mode, while the controller has no connection to a server)
<code>\${event.timeZone}</code>	Time zone in which the event occurred
<code>\${event.source.id}</code>	System object ID, on which the event occurred (reader, zone controller, etc.).

<code>\${event.source.name}</code>	Name of the object on which the event occurred (reader, zone controller, etc.).
<code>\${event.cardNumber}</code>	Card number if the event is an access event
<code>\${event.credential.id}</code>	System ID of the identifier (card), if the event is an access event, and the identifier (card) is registered in the system
<code>\${event.credential.name}</code>	Name of the identifier (card) in the system, if the event is an access event, and the identifier (card) is registered in the system
<code>\${event.subject.id}</code>	System ID card holder, if the event is associated with the presenting of ID (access event), and the owner is registered in the system
<code>\${event.subject.name}</code>	The full name of the card holder, if the event is associated with the provision of ID (access event), and the owner is registered in the system

2.4 Configuring HID VertX / EDGE access control controllers

To configure the hardware HID VertX / EDGE you need to configure the following configuration objects in the system:

1. Configure one or more objects Vertx Card Format
2. Configure one or more objects VertX Card Set
3. Configure VertX keypad translations
4. Configure HID VertX / EDGE hardware controllers
5. Configure HID VertX / EDGE readers
6. Configure HID VertX / EDGE reader groups for later use in user roles (optional)
7. Configure HID VertX / EDGE inputs
8. Configure HID VertX / EDGE outputs
9. Configure HID VertX / EDGE output groups

After configuring the hardware HID VertX / EDGE, you can place objects HID VertX / EDGE on graphical plans, assign them to the areas used in the automation device, configure access policies to assign permissions to users (cardholders).

The following sections show how to configure objects HID VertX / EDGE.

2.4.1 Configuring HID VertX / EDGE card formats

Configuration card formats for HID VertX / EDGE controllers is under Console Administration / System Settings / Shared Configuration Objects.

All registered HID VertX / EDGE card formats will be uploaded to all registered in the system HID VertX / EDGE controllers.

To configure the card format you need:

- Create an object of card format VertX type
- Create an object of set of cards VertX type

When creating an object of VertX card format, specify the following parameters:

- Card format ID (any number greater than 0, not used in other card formats)
- The path and file name in the controller, on which the card format of the file will be loaded
- File format (eff or vff)

In addition to these parameters a file that describes the card format should be uploaded. Card format files can be obtained from your system vendor.

The screenshot displays the 'Administration' section of the Areashell web interface. The left sidebar contains a navigation menu with categories like 'System Settings', 'Shared Configuration Objects', and 'Hardware'. The main content area is titled 'VertxCardFormat 99' and includes tabs for 'Main settings' and 'Events'. Under 'Main settings', there are three sections: 'Common properties' with fields for 'Name' (VertxCardFormat 99) and 'Type' (VertxCardFormat); 'Controller parameters' with fields for 'Card format ID' (1), 'File name in controller' (/mnt/flash/FmtsConfig/h10301_99.vff), and 'File type' (vff); and 'File uploading' which shows the 'Size of the stored file' (4896) and an 'Upload file' section with a 'Choose File' button and a 'Submit file' button. At the bottom of the form are 'Submit' and 'Cancel' buttons. The top of the interface shows the 'areashell' logo and a navigation bar with links to Home, Monitoring, Policies, Persons, Time & Attendance, Reports, and Administration. The user 'Roman Polozov' is logged in.

2.4.2 Configuring HID VertX / EDGE card sets

After configuring the card format, create one or more VertX Card Sets.

When creating VertX / EDGE card set, specify the following parameters:

- Card format – select a previously created card format
- Cards set ID – any number greater than 0, not used in other card formats
- The path and file name in the controller, on which the card format of the file will be loaded
- File format (eff or vff)
- In a case of eff file format, specify the format of the parameters in the fields 'Field A value' – 'Field H value' (ask the required settings from your system vendor).

The screenshot displays the 'Administration' section of the Areashell web interface. On the left, a sidebar menu lists various system settings categories: System Settings, Shared Configuration Objects, Hardware, Site Structure, Organization Registry, Automation, and Other. The main content area is titled 'Common properties' and 'Controller parameters'. Under 'Common properties', the 'Name' field is set to 'VertxCardSet' and the 'Type' is 'VertxCardSet'. Under 'Controller parameters', the 'Card format' is selected as 'VertxCardFormat 99'. The 'Card set ID' is set to '1' with a range indicator '(1-253)'. Below this, there are eight input fields for 'Field A value' through 'Field H value', all of which are currently set to '0'. At the bottom of the form, there are 'Submit' and 'Cancel' buttons.

2.4.3 Configuring HID VertX / EDGE keypad translations

To use the readers with a keyboard, you must first create at least one object VertX Keypad Translation, after which it can be used in reader preferences.

All registered HID VertX / EDGE keypad translations will be uploaded to all registered in the system HID VertX / EDGE controllers.

Configuring HID VertX / EDGE keypad translations can be done in the console section Administration / Settings / Shared Configuration Objects.

The screenshot displays the 'System Settings' page in the Areashell administration console. The top navigation bar includes links for Home, Monitoring, Policies, Persons, Time & Attendance, Reports, and Administration. The user 'Roman Polozov' is logged in. The left sidebar shows 'System Settings' expanded. The main content area is titled 'Common properties' and contains two fields: 'Name' (VertxKeypadTranslation) and 'Type' (VertxKeypadTranslation). Below this is the 'Keypad translation parameters' section, which lists 12 raw values for keys 0 through B. The values are: 0, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11. At the bottom of the form are 'Submit' and 'Cancel' buttons.

Property	Value
Name	VertxKeypadTranslation
Type	VertxKeypadTranslation
Keypad translation parameters	
Keypad type ID	0
Raw value for key 0	0
Raw value for key 1	1
Raw value for key 2	2
Raw value for key 3	3
Raw value for key 4	4
Raw value for key 5	5
Raw value for key 6	6
Raw value for key 7	7
Raw value for key 8	8
Raw value for key 9	9
Raw value for key A	10
Raw value for key B	11

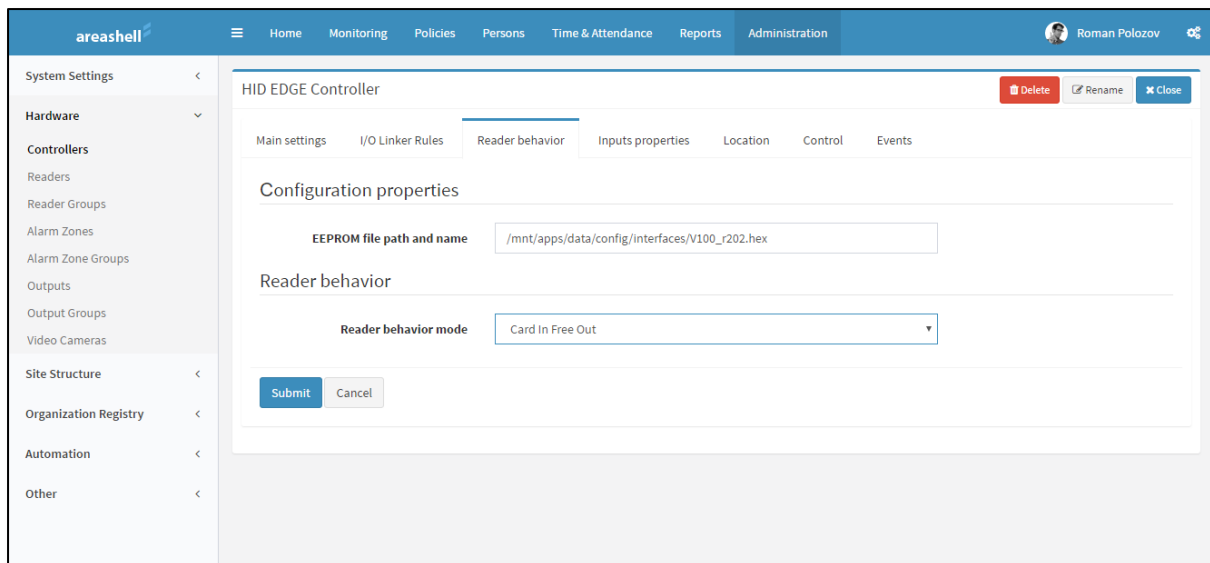
2.4.4 Configuring HID VertX / EDGE controllers

Configuring HID VertX / EDGE controllers is made in the console section Administration / Hardware / Controllers.

The screenshot displays the 'HID EDGE Controller' configuration page in the Areashell web interface. The left sidebar shows the navigation menu with 'Hardware' expanded and 'Controllers' selected. The main content area is titled 'HID EDGE Controller' and includes tabs for 'Main settings', 'I/O Linker Rules', 'Reader behavior', 'Inputs properties', 'Location', 'Control', and 'Events'. The 'Main settings' tab is active, showing the following configuration options:

- Common properties:**
 - Name: HID EDGE Controller
 - Type: VertxController
- Address properties:**
 - IP address: 192.168.1.77
 - TCP port: 4050
 - Internal ID: 1
 - Encrypted communication: ☐ Enabled
 - Shared seed: 2244668800
 - Get controller info button
- Controller information:**
 - Controller type: HID EDGE Controller (EH400, EH400-K, EHR40-K, EHRP40-K, EHR40-L, EHR40-K) (dropdown)
 - MAC address: (empty field)
 - VertX/EDGE version: (empty field)
 - VertX/EDGE version date: (empty field)
 - Host name of controller: (empty field)
- Time zone properties:**
 - Time zone: (UTC+4:0) Europe/Samara - Samara Time (dropdown)
 - VertX/EDGE time zone string: EST+5EDT,M3.2.0/2,M11.1.0/2
 - std offset dst [offset],start[/time],end[/time] (Example: EST+5EDT,M3.2.0/2,M11.1.0/2)
- Communication settings:**
 - Connect on configuration change: ☒ Enabled
 - Regular event polling: ☒ Enabled
 - Polling period (ms): 1000
 - Communication timeout (ms): 5000

At the bottom of the form are 'Submit' and 'Cancel' buttons.



areashell

HomeMonitoringPoliciesPersonsTime & AttendanceReportsAdministration

Roman Polozov

System Settings<

Hardware<

Controllers

Readers

Reader Groups

Alarm Zones

Alarm Zone Groups

Outputs

Output Groups

Video Cameras

Site Structure<

Organization Registry<

Automation<

Other<

HID EDGE Controller

DeleteRenameClose

Main settingsI/O Linker RulesReader behaviorInputs propertiesLocationControlEvents

Tamper Input

Enabled☒ Enabled

High range upper limit255

High range lower limit129

Low range upper limit128

Low range lower limit0

Debounce iterations4

(*8 ms) = 0.032 seconds

AC Fail Input

Enabled☒ Enabled

High range upper limit255

High range lower limit129

Low range upper limit128

Low range lower limit0

Debounce iterations4

(*8 ms) = 0.032 seconds

Battery Fail Input

Enabled☒ Enabled

High range upper limit255

High range lower limit129

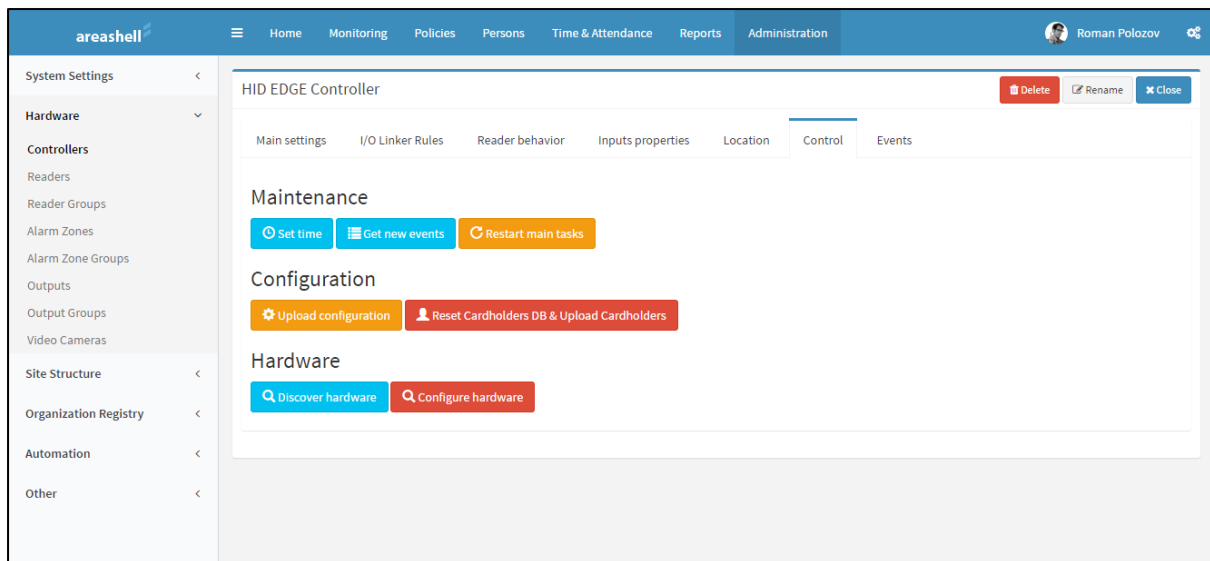
Low range upper limit128

Low range lower limit0

Debounce iterations4

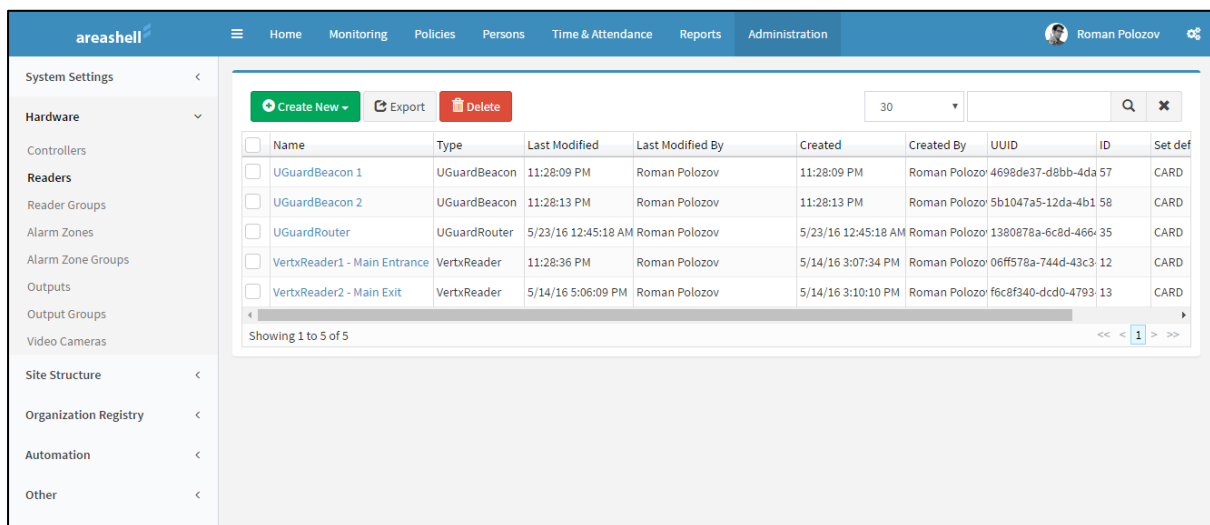
(*8 ms) = 0.032 seconds

SubmitCancel



2.4.5 Configuring HID VertX / EDGE readers

Configuring Reader HID VertX / EDGE is made in the console section Administration / Hardware / Readers.



areashell

Home
Monitoring
Policies
Persons
Time & Attendance
Reports
Administration

Roman Polozov

System Settings
Hardware
Site Structure
Areas
Maps
Checkpoint Settings
Organization Registry
Automation
Other

Delete
Rename
Close

Main settings
Inputs properties
Location
Control
Events

VertxReader1 - Main Entrance

Common properties

Name: VertxReader1 - Main Entrance

Type: VertxReader

Address properties

Controller: HID VertX V2000 Network Controller

Port: 0

Mode settings

Reader type: Wiegand

Set default mode: Card only

Host lookup type: No lookup

Time settings

Normal grant access time: 250
(*25 ms) = 6.2500000 seconds

Ext grant access time: 750
(*25 ms) = 18.7500000 seconds

Minimum open time: 0
(*25 ms) = 0.0000000 seconds

Direct relay minimum time: 250
(*25 ms) = 6.2500000 seconds

Door held time: 1500
(*25 ms) = 37.5000000 seconds

REX open time: 250
(*25 ms) = 6.2500000 seconds

Keypad settings

Keypad reader: ☐ Enabled

Keypad type:

PIN entering time limit: 60

Max PIN attempts: 10

PIN lockout time: 0

PIN suppress schedule:

Max PIN size: 15

End PIN code: 11

Clear PIN code: 10

PIN commands: ☐ Enabled

Anti-pass-back settings

APB Type: Real APB

Timed APB timeout: 60

APB violation action: Log violation only

Area out of which the door leads: HQ Security Room

Area into which the door leads: Headquarters

Elevator settings

Elevator reader: ☐ Enabled

Time the relay is on, in seconds: 10

Type of output: Relay output

The state of the elevator control: Relay output

Poll delay, in milliseconds: 10

Elevator relay controller:

Submit Cancel

areashell

Home Monitoring Policies Persons Time & Attendance Reports Administration

Roman Polozov

System Settings <

Hardware v

VertxReader1 - Main Entrance

Delete Rename Close

Main settings Inputs properties Location Control Events

Exit request input

Enabled ☒ Enabled

High range upper limit 255

High range lower limit 197

Low range upper limit 196

Low range lower limit 0

Debounce iterations 12

(*8 ms) = 0.0960000 seconds

Unlock door ☒ Enabled

Door monitor input

Enabled ☒ Enabled

High range upper limit 196

High range lower limit 0

Low range upper limit 255

Low range lower limit 197

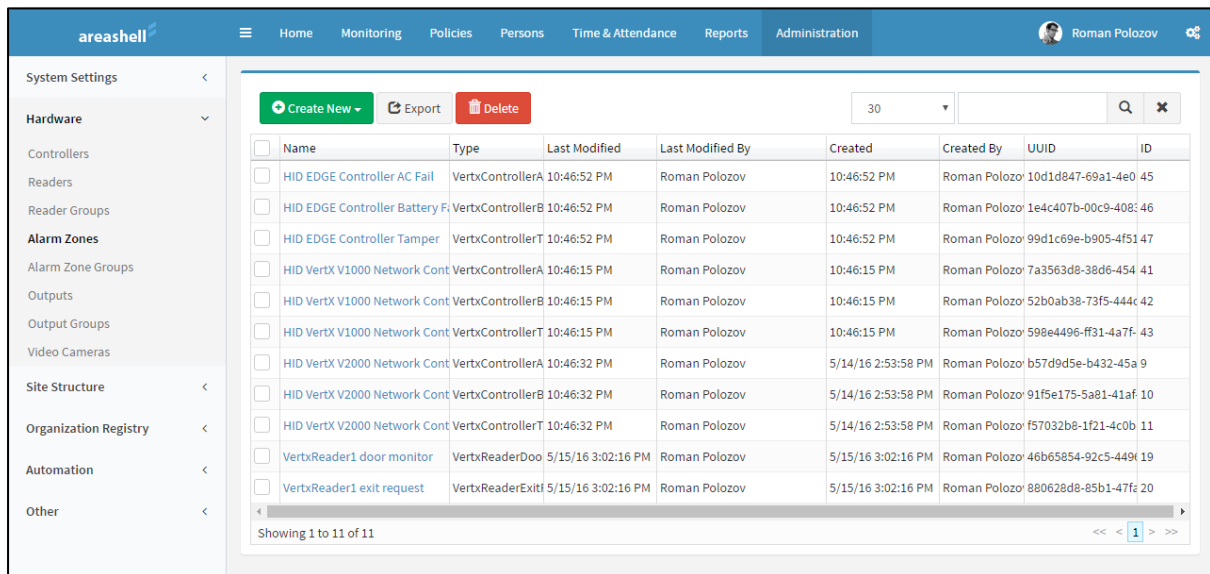
Debounce iterations 12

(*8 ms) = 0.0960000 seconds

Submit Cancel

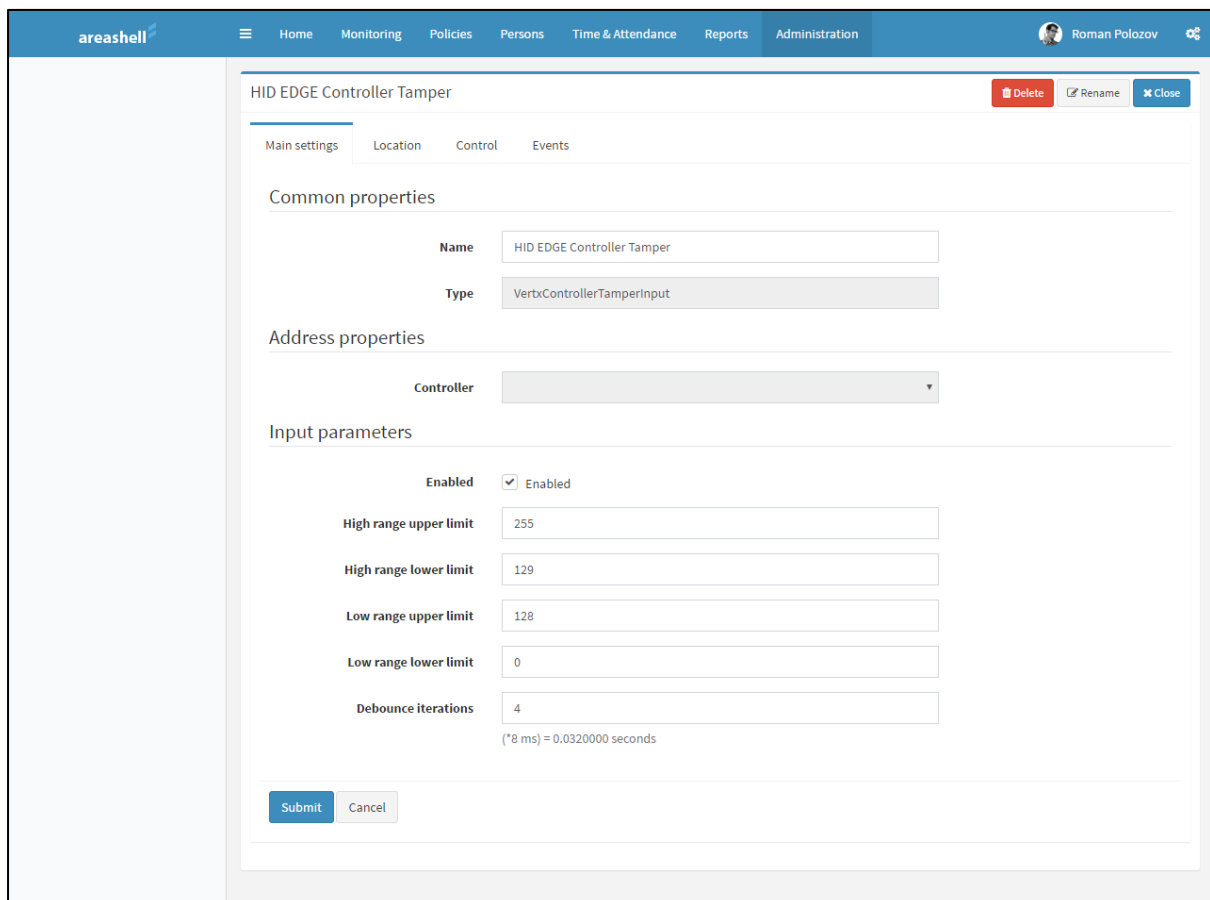
2.4.6 Configuring HID VertX / EDGE inputs

Configuring HID VertX / EDGE inputs is made in the console section Administration / Hardware / Alarm Zones.



The screenshot shows the Areashell Administration console with the 'Alarm Zones' section selected in the left sidebar. The main area displays a table of configured alarm zones. The table has columns for Name, Type, Last Modified, Last Modified By, Created, Created By, UUID, and ID. There are 11 entries in the table, including HID EDGE Controller AC Fail, HID EDGE Controller Battery Fail, HID EDGE Controller Tamper, and various HID VertX V1000 and V2000 Network Controller entries. At the bottom, it says 'Showing 1 to 11 of 11'.

Name	Type	Last Modified	Last Modified By	Created	Created By	UUID	ID
HID EDGE Controller AC Fail	VertxControllerA	10:46:52 PM	Roman Polozov	10:46:52 PM	Roman Polozov	10d1d847-69a1-4e0	45
HID EDGE Controller Battery Fail	VertxControllerB	10:46:52 PM	Roman Polozov	10:46:52 PM	Roman Polozov	1e4c407b-00c9-408	46
HID EDGE Controller Tamper	VertxControllerT	10:46:52 PM	Roman Polozov	10:46:52 PM	Roman Polozov	99d1c69e-b905-4f51	47
HID VertX V1000 Network Controller	VertxControllerA	10:46:15 PM	Roman Polozov	10:46:15 PM	Roman Polozov	7a3563d8-38d6-454	41
HID VertX V1000 Network Controller	VertxControllerB	10:46:15 PM	Roman Polozov	10:46:15 PM	Roman Polozov	52b0ab38-73f5-444c	42
HID VertX V1000 Network Controller	VertxControllerT	10:46:15 PM	Roman Polozov	10:46:15 PM	Roman Polozov	598e4496-ff31-4a7f	43
HID VertX V2000 Network Controller	VertxControllerA	10:46:32 PM	Roman Polozov	5/14/16 2:53:58 PM	Roman Polozov	b57d9d5e-b432-45a	9
HID VertX V2000 Network Controller	VertxControllerB	10:46:32 PM	Roman Polozov	5/14/16 2:53:58 PM	Roman Polozov	91f5e175-5a81-41af	10
HID VertX V2000 Network Controller	VertxControllerT	10:46:32 PM	Roman Polozov	5/14/16 2:53:58 PM	Roman Polozov	f57032b8-1f21-4c0b	11
VertxReader1 door monitor	VertxReaderDoo	5/15/16 3:02:16 PM	Roman Polozov	5/15/16 3:02:16 PM	Roman Polozov	46b65854-92c5-449	19
VertxReader1 exit request	VertxReaderExit	5/15/16 3:02:16 PM	Roman Polozov	5/15/16 3:02:16 PM	Roman Polozov	880628d8-85b1-47fe	20



The screenshot shows the configuration form for the 'HID EDGE Controller Tamper' alarm zone. The form has tabs for Main settings, Location, Control, and Events. The 'Main settings' tab is active. The form includes fields for Name, Type, Address properties (Controller), and Input parameters (Enabled, High range upper limit, High range lower limit, Low range upper limit, Low range lower limit, Debounce iterations). The 'Submit' button is at the bottom.

HID EDGE Controller Tamper

Buttons: Delete, Rename, Close

Tabs: Main settings, Location, Control, Events

Common properties

Name: HID EDGE Controller Tamper

Type: VertxControllerTamperInput

Address properties

Controller: [Dropdown]

Input parameters

Enabled: ☒ Enabled

High range upper limit: 255

High range lower limit: 129

Low range upper limit: 128

Low range lower limit: 0

Debounce iterations: 4

(*8 ms) = 0.0320000 seconds

Buttons: Submit, Cancel

2.4.7 Configuring HID VertX / EDGE outputs

Configuring HID VertX / EDGE outputs is made in the console section Administration / Hardware / Outputs.

The screenshot displays the Areashell web interface. The top navigation bar includes links for Home, Monitoring, Policies, Persons, Time & Attendance, Reports, and Administration. The left sidebar shows a tree view with categories like System Settings, Hardware, Site Structure, Organization Registry, Automation, and Other. The 'Hardware' category is expanded, showing sub-items like Controllers, Readers, Reader Groups, Alarm Zones, Alarm Zone Groups, Outputs, Output Groups, and Video Cameras. The 'Outputs' item is selected, leading to the 'VertX Output 1' configuration page. This page has tabs for Main settings, Location, Control, and Events. The 'Main settings' tab is active, showing 'Common properties' with fields for Name (VertX Output 1) and Type (VertxOutput). Below this, the 'Address properties' section includes a Controller dropdown (HID EDGE Controller), an Output number field (0), and a Minimum (timed on) open time field (120). A note indicates that 120 is equivalent to 3.00000000 seconds (*25 ms). At the bottom of the form are 'Submit' and 'Cancel' buttons. In the top right corner of the configuration window, there are buttons for Delete, Rename, and Close.

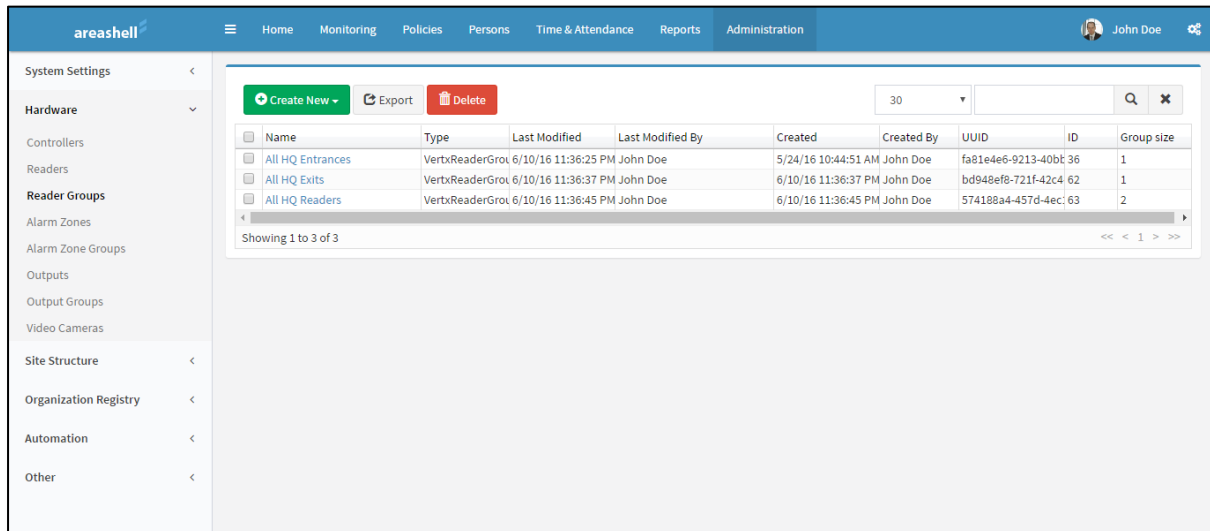
2.4.8 Configuring HID VertX / EDGE output groups

Configuring HID VertX / EDGE output groups is made in the console section Administration / Hardware / Output Groups.

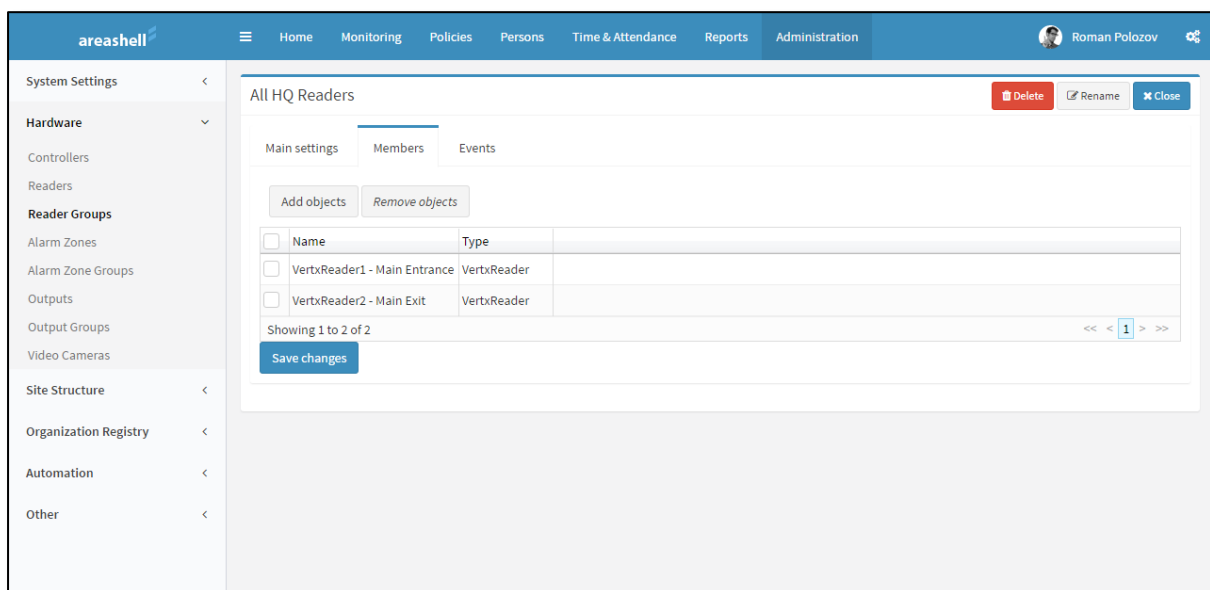
2.4.9 Configuring reader groups

Reader groups are used when assigning user access rights in the room and on the controlled areas of the territory. The groups include readers.

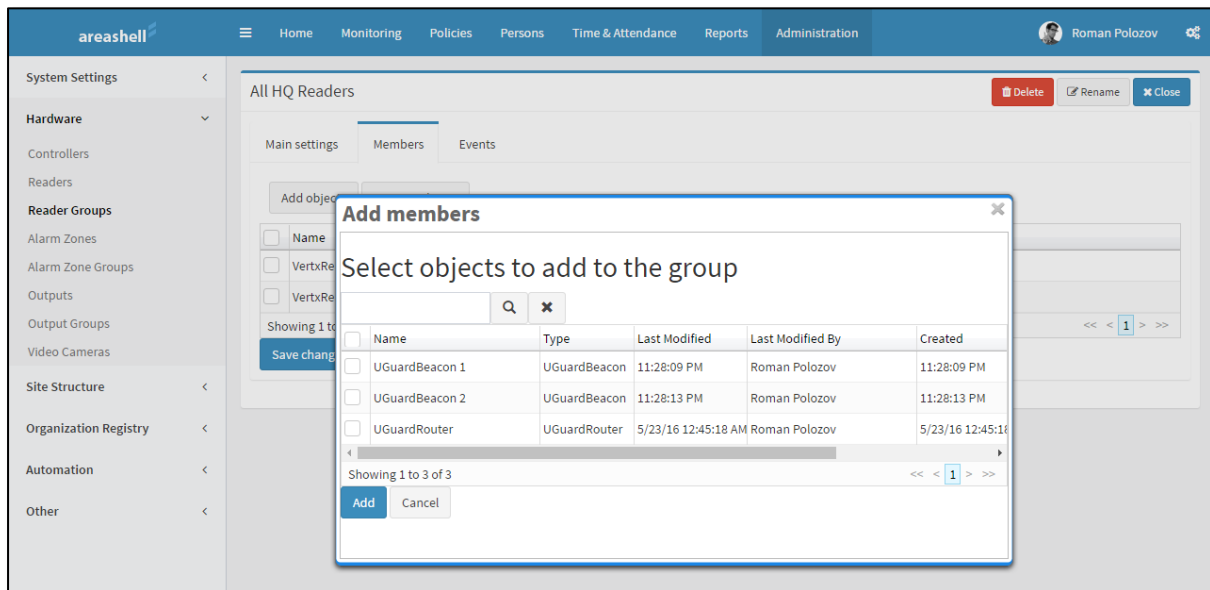
Administration of reader groups is made in the console section Administration / Hardware / Readers Group.



Adding and removing of reader to / from the group can be made on Members tab.



To add readers to the group click Add objects, select the readers in the dialog box and click Add.



Attention: The readers connected to different controllers can be added to one group.
The group will be uploaded into all controllers whose readers are included in it.

To remove the reader from the group select it in the box and click Remove objects.
Click Save Changes to save the new configuration in the database.

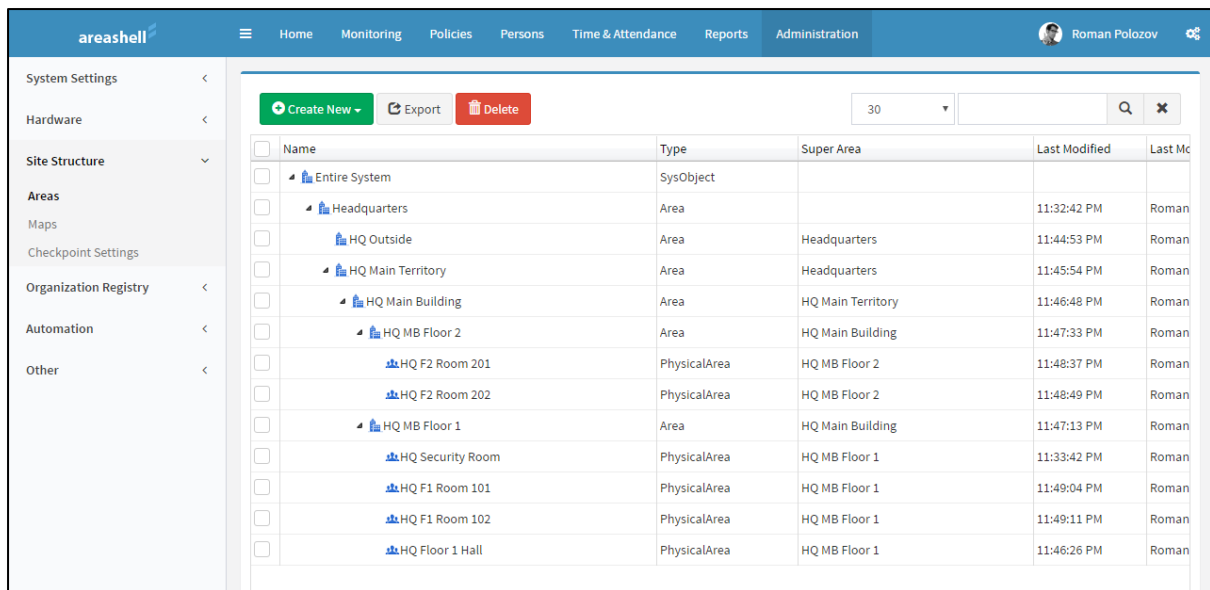
2.5 Configuring areas

Configuring of areas is made in the console section Administration / Site structure / Areas.

Areas can be of two types:

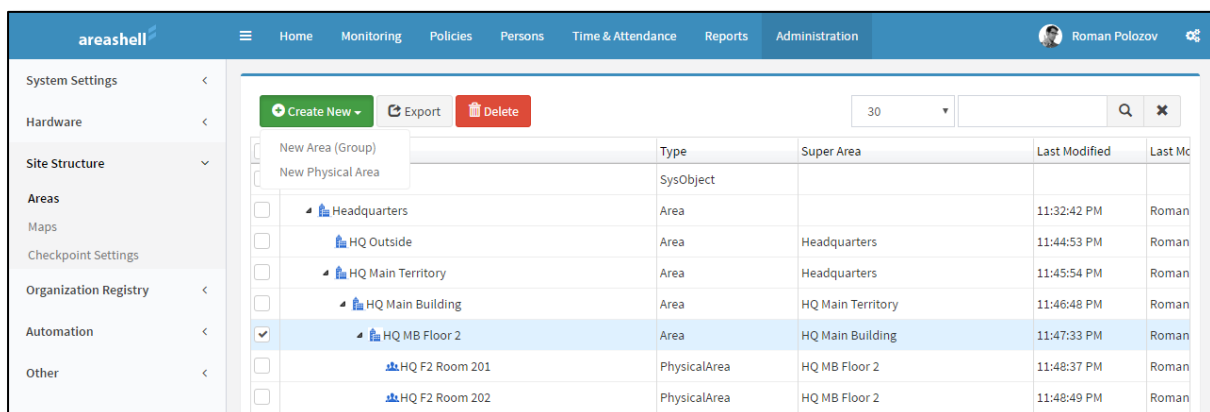
- Area;
- Physical area.

Areas may not contain physical objects, but may include other areas or physical areas. Physical region may contain physical objects (readers, controllers, zone and chamber etc.), but can not contain any other fields. Thus, the areas can be arranged in a hierarchy with Areas on the all levels except of the lower one and with Physical Areas on the lowest levels.



Name	Type	Super Area	Last Modified	Last Modified By
Entire System	SysObject			
Headquarters	Area		11:32:42 PM	Roman
HQ Outside	Area	Headquarters	11:44:53 PM	Roman
HQ Main Territory	Area	Headquarters	11:45:54 PM	Roman
HQ Main Building	Area	HQ Main Territory	11:46:48 PM	Roman
HQ MB Floor 2	Area	HQ Main Building	11:47:33 PM	Roman
HQ F2 Room 201	PhysicalArea	HQ MB Floor 2	11:48:37 PM	Roman
HQ F2 Room 202	PhysicalArea	HQ MB Floor 2	11:48:49 PM	Roman
HQ MB Floor 1	Area	HQ Main Building	11:47:13 PM	Roman
HQ Security Room	PhysicalArea	HQ MB Floor 1	11:33:42 PM	Roman
HQ F1 Room 101	PhysicalArea	HQ MB Floor 1	11:49:04 PM	Roman
HQ F1 Room 102	PhysicalArea	HQ MB Floor 1	11:49:11 PM	Roman
HQ Floor 1 Hall	PhysicalArea	HQ MB Floor 1	11:46:26 PM	Roman

To create a new internal group of areas or a physical area within the outer group of areas, first select the outer area by checking it in the left column in the table area, and then click Create New / New Area (Group) or Create New / New Physical Area.



Name	Type	Super Area	Last Modified	Last Modified By
Headquarters	Area		11:32:42 PM	Roman
HQ Outside	Area	Headquarters	11:44:53 PM	Roman
HQ Main Territory	Area	Headquarters	11:45:54 PM	Roman
HQ Main Building	Area	HQ Main Territory	11:46:48 PM	Roman
HQ MB Floor 2	Area	HQ Main Building	11:47:33 PM	Roman
HQ F2 Room 201	PhysicalArea	HQ MB Floor 2	11:48:37 PM	Roman
HQ F2 Room 202	PhysicalArea	HQ MB Floor 2	11:48:49 PM	Roman

The new area will be created as a child area of the selected area group, and selected area group will be set for the new area as a super area.

The area can be moved from one area group to another by changing the parameter Super Area on Location tab in settings of the area.

To configure an area on Location tab set the following parameters:

- Super area is a group of areas in which given area is located.
- Time zone is the time zone in which the given area is located. The parameter affects the processing of event messages from physical objects in this area. The physical area must always be in the same time zone. Group areas may include internal regions that are in different time zones. In this case, the outer band areas can be set to any of them.
- Latitude and longitude affect the display of the areas on geographical plans. The point with these coordinates of the marker area is displayed on the global map.

These parameters may be quickly changed by moving a marker on the map at the bottom of the panel.

- Default map zoom level affects the display of the area on geographical maps (1 – the whole world; 5 – a country; 10 – a big city; 13 – a small town, 17 – houses, 21 – the maximum zoom level).
- Local map is a local graphic plan in Areashell system configuration (see section “Configuring graphic maps”).

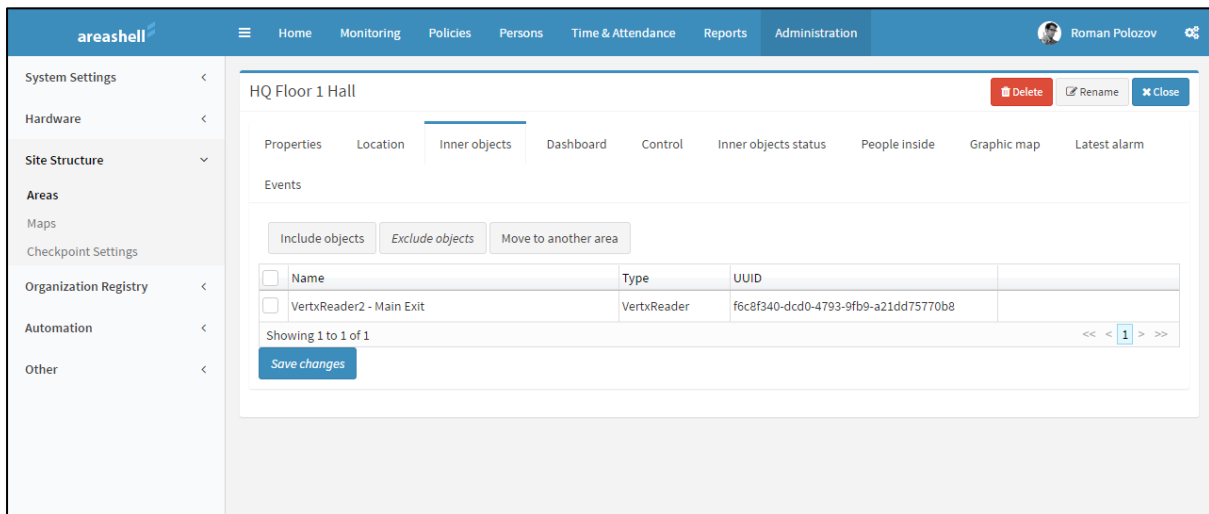
If a local map is set for the area, then two display modes *Global map* and *Local map* will be available for this area on the tab Graphical Map in monitoring mode.

The screenshot displays the 'areashell' Administration interface. The left sidebar contains navigation links: System Settings, Hardware, Site Structure, Areas, Maps, Checkpoint Settings, Organization Registry, and Automation. The main content area is titled 'HQ Main Building' and includes tabs for Properties, Location, Dashboard, Control, Inner objects status, People inside, Graphic map, Latest alarm, and Events. The 'Location' tab is active, showing 'Location properties' with the following fields:

- Super Area:** HQ Main Territory
- Time zone:** (UTC-8:0) US/Pacific - Pacific Daylight Time
- Latitude:** 34.0486770
- Longitude:** -118.2492828
- Altitude:** 0.0000000
- Default map zoom level:** 12

Below these fields is a button labeled 'Import geodetic location from super area'. Under the 'Location on local map' section, the 'Local map' dropdown is set to 'GraphicMap'. The 'Location on global map' section features a Google Map of Los Angeles with a red location pin in the downtown area. At the bottom of the map section are 'Submit' and 'Cancel' buttons.

The list of physical objects that are in the physical area can be configured on the tab Inner objects.



To include objects into the area:

- Click Include objects
- Select (check in the left column) the needed objects in the window that appears (sorting by different columns and searching can be used)
- Click Add in the window,
- Click Save Changes on the panel.

Attention: If the zone is controlled by any reader (by presenting a card at this reader this zone can be reached), then the reader is usually not in this area but in the adjacent one. That is, it should be included in the adjacent area as an internal object.

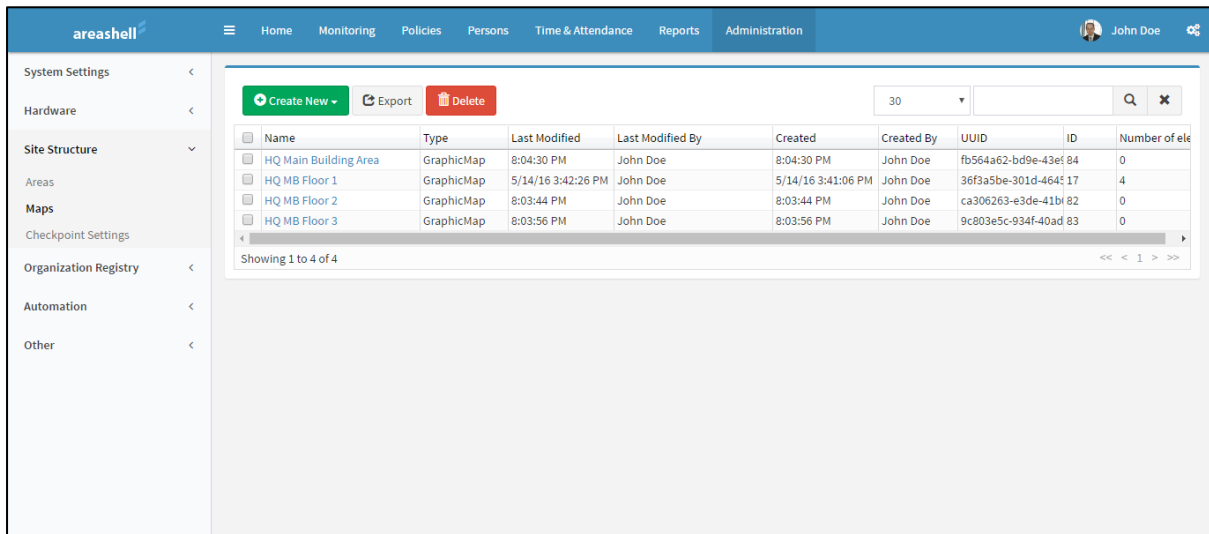
In the setting of the reader there is a separate option 'Area into which the door leads', where the physical area the reader leads to is set.

When the reader is included in the area, this area is seen in the parameter 'Area out of which the door leads' of the reader. When this setting is changed, the reader also appears in the list of internal objects of the new area.

The tabs Dashboard, Inner objects status, People inside, Graphics map, and Events are for monitoring and controlling the area. They do not allow to change the parameters of the area.

2.6 Configuring graphics maps

Configuring the graphics maps is made in the console section Administration / Site Structure / Maps



When creating a new plan on the tab New Graphic Map it is necessary to:

- set the name in Name field,
- click 'Choose File' in 'Upload the background image' and choose the image with the background image of the map,
- click Submit at the bottom of the panel to save your changes.

After selecting a plan the downloaded background image of the plan can be viewed on the tab Properties.

Placing the system objects on the map is made on Map editor tab.

To place a new object on the plan:

- Click on the background image of the plan at the point where you want to place the object system (a new element of the blue color will be seen at a given point on the plan);
- In the toolbar in the section 'System object' select the system object, which will be associated with this element of the map;
- Press Ok button in the toolbar (element of the map will turn darker and an icon will appear in it).

To change it, select the plan element by clicking it (the selected item will turn darker). The selected element can be moved, or the system object associated with it can be changed.

To change the position of the selected map element drag and drop it by mouse.

To change associated with the selected element of the site plan, choose a new object in the parameter 'System object' in the toolbar.

After changes to the object settings are made, click the Ok button in the toolbar (map element will turn lighter).

Attention: After adding, removing, or changing elements of the plan, click 'Save Plan' in the toolbar to save the changes to the database. Otherwise, after closing the map editor (for example, after switching to a different console page) the changes will be lost.

2.7 Configuring the automation subsystem

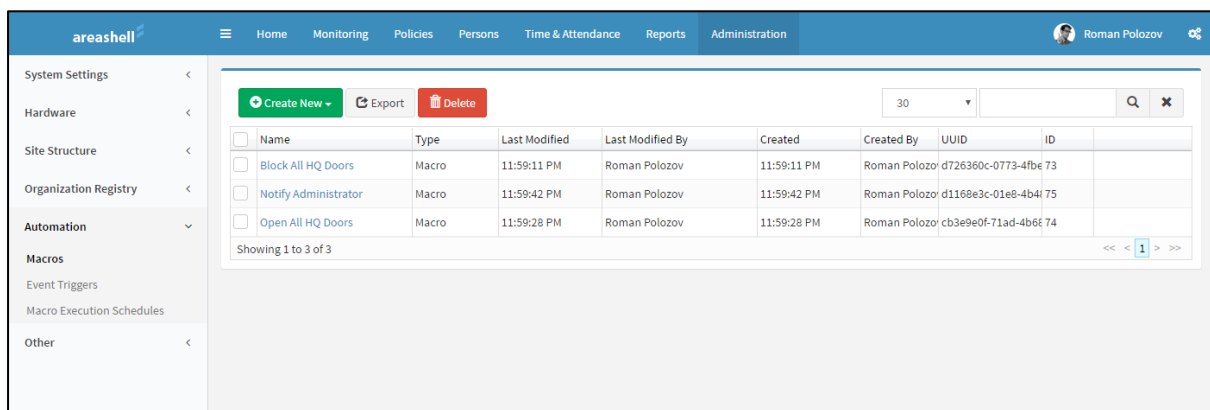
Areashell system automation subsystem uses the following configuration objects:

- Macro. It contains a sequence of instructions executed;
- Event trigger. It runs macro command specified in its settings when an event described in its settings occurs
- Macro execution schedule. It runs macro specified in its settings, in accordance with the specified schedule settings.

Physical system objects (for management), the notification server and notification templates (for sending event notification via e-mail) and other objects are used in the settings of the configuration objects of the automation subsystem.

2.7.1 Configuring macros

Configuring the macros is made in the console section Administration / Automation / Macros.

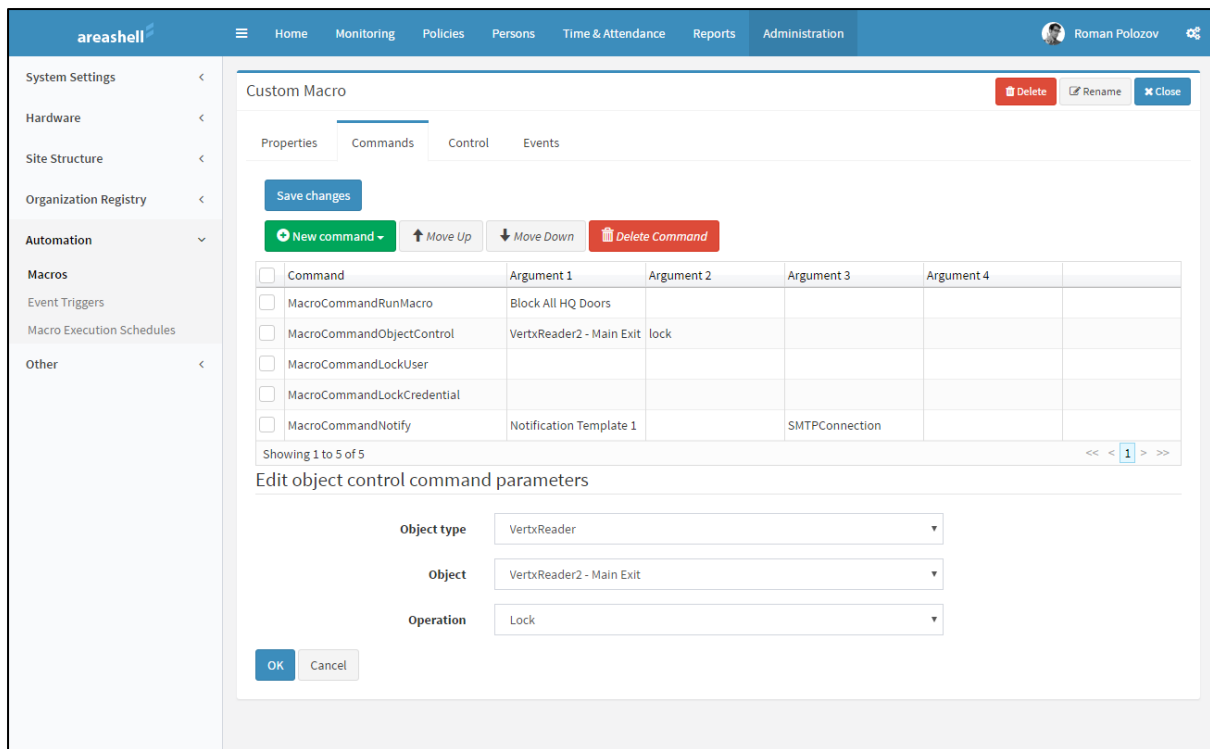


To create a new macro, click Create New / New Macro, specify a name and click Submit.

The sequence of instructions executed by a macro is set on the settings tab Commands.

To add a new command in the sequence, click New command and select the type of the command. The new command will appear in the list, and the form of the command parameters will appear under the list. The list of command parameters depends on its type. Set command parameters on the form and then click 'Apply' to apply the settings to the selected command.

The settings of any macro command can be changed by selecting it in the list.



To change the sequence of instruction execution, choose one or more commands in the list and click Move Up or Move Down in the toolbar.

Attention: After adding, deleting, modifying the parameters or the sequence of commands, click 'Save Changes' in the tool bar to save the changes to the database. Otherwise, when the edit panel of macro command is closed (for example, switching to a different console page), the changes will be lost.

2.7.2 Configuring event triggers

Event triggers can be configured in the console section Administration / Automation / Event Triggers.

To create a new trigger, click the toolbar Create New / New Event Trigger, set the trigger name, and then click Submit. A new trigger will appear in the table.

To adjust the trigger settings, select it in the table.

Set the following options when configuring the trigger:

The following parameters can be specified on the Schedule tab:

- Enabled – trigger starts the macro only if this option is checked.
- Activation date - trigger does not run the macro before the date in this parameter.
- Deactivation date – trigger does not run a macro after the date in this parameter.
- Time schedule – trigger starts the macro only in the time periods of the time schedule specified in this parameter.

- React on offline events – if the parameter is not checked , trigger launches the command only if the message about the event occurrence is delivered in the online mode. An event is considered online if the time period between the occurrence of the event (by internal controller clock) and the time of its registration in the system (by the server clock) is less than 10 seconds.
- Macro to run – a macro that will be started by this trigger when it receive a message about an event.

The following parameters can be specified on the tab 'Event filter':

- Minimum alarm level – the trigger starts the macro only if event alarm level is greater than the value set in this parameter.
- Maximum alarm level – the trigger starts the macro only if event alarm level is less than the value set in this parameter.
- Source objects – if the list is empty, the trigger starts the macro when receiving an event from any object; if the list is not empty, then the trigger launches the macro only when receiving an event from any object selected in this list.
- First name, Last name, Organization, Department, Credential number – if the values are not set (all these fields are empty), the trigger starts the macro when receiving an event about any user or in case of the absence of a user (for example, alarm in a zone). If any value is set (at least one of these fields is not empty), then the trigger launches the macro only when an event is received about the user, whose first, or last name, or other data field contains the specified string (events without a user do not initiate launch of the macro).

The screenshot displays the 'Alarm Trigger' configuration window in the Areashell administration tool. The 'Event filter' tab is selected. Under 'Event alarm level', the 'Minimum alarm level' is set to 20000 and the 'Maximum alarm level' is set to 2147483647. The 'Person' section contains input fields for 'First name', 'Last name', 'Organization', 'Department', and 'Credential number', all of which are currently empty. To the right, the 'Event codes' section lists several event types with checkboxes: 'Communication error', 'Online', 'Beeper off', 'Beeper on', 'Get events', 'Set time', 'Upload cardholders', 'Upload configuration', and 'Interface status'. All checkboxes are unchecked. Below this, the 'Source objects' section features 'Include objects' and 'Exclude objects' buttons, and a table with columns for 'Name', 'Type', and 'UUID'.

2.7.3 Configuring macro execution schedules

Configuring macro execution schedules is made in the console section Administration / Automation / Macro Execution Schedules.

To create a new macro execution schedule, click Create New / New Macro Execution Schedule, enter the name of the schedule and click Submit. The new schedule will appear in the table.

To configure the schedule settings, select it in the table.

When configuring the schedule, set the following parameters:

- Enabled – schedule launches a macro only if this option is checked.
- Activation date – the schedule does not start the macro before the date specified in the parameter.
- Deactivation date – the schedule does not run a macro after the date specified in the parameter.
- Time schedule – the schedule starts the macro at the beginning of the time periods of the time schedule are starting.
- Macro to run – a macro that will run by this schedule.

The screenshot displays the 'Macro Execution Schedules' configuration page in the Areashell Administration console. The left sidebar shows the navigation menu with 'Automation' expanded and 'Macro Execution Schedules' selected. The main content area is titled 'Open all public doors at start of the day' and includes tabs for 'Schedule properties' and 'Events'. The 'Schedule properties' tab is active, showing the following configuration:

- Common properties:**
 - Name: Open all public doors at start of the day
 - Type: MacroExecutionSchedule
- Activation properties:**
 - Enabled: ☒
 - Activation date: 06/01/2016
 - Deactivation date: 07/01/2017
 - Time schedule: TimeSchedule
- Run macro properties:**
 - Macro to run: Open all public doors

At the bottom of the configuration area are 'Submit' and 'Cancel' buttons. In the top right corner of the configuration area, there are 'Delete', 'Rename', and 'Close' buttons.

3 Administering access policies

3.1 General principles of administrative access policies

The main objects of administrative access policies are:

- Holidays
- Access Schedule
- User Roles
- Users' Groups

Holidays are used to change the user access mode (card holders and other identifiers) pass through the point. The system supports a single list of holidays, which is loaded into all hardware controllers registered in the system. Pass mode during the holiday is determined by the check specified in the settings of the temporary access scheduling intervals (see the section Time schedules).

3.2 Holidays

Configuring the holidays is performed in the console section Policies / Holidays.

<input type="checkbox"/>	Name	Type	Holiday Date	Holiday Type	Last Modified	Last Modified By	Created	Created By	UUID	ID
<input type="checkbox"/>	Halloween	Holiday	10/31/16	Holiday 1	6/10/16 11:01:18 PM	Roman Polozov	6/10/16 11:01:18 PM	Roman Polozov	a8187117-388d-449f-53	
<input type="checkbox"/>	Independence Day	Holiday	7/4/16	Holiday 1	6/10/16 10:59:42 PM	Roman Polozov	6/10/16 10:59:42 PM	Roman Polozov	15c11b3f-7615-482a-51	
<input type="checkbox"/>	Memorial Day	Holiday	5/30/16	Holiday 1	6/10/16 11:00:18 PM	Roman Polozov	6/10/16 11:00:18 PM	Roman Polozov	2e5fb4ba-9277-4bf0-52	
<input type="checkbox"/>	New Year's Day	Holiday	1/1/17	Holiday 1	6/10/16 10:59:03 PM	Roman Polozov	5/22/16 5:54:47 PM	Roman Polozov	44028ac7-6cd4-4aef-33	

Showing 1 to 4 of 4

When configuring a holiday, specify the following options:

- Holiday type – a parameter that allows to group holidays by type. Holidays types are equivalent, but the permissions settings in the access schedule can be set separately for different types of holidays.
- Holiday date – sets the date of the holiday in the particular year.
- Every year – should the date be automatically transferred to the next year.

The screenshot displays the 'areashell' web application interface. The top navigation bar includes links for Home, Monitoring, Policies, Persons, Time & Attendance, Reports, and Administration. The user 'Roman Polozov' is logged in. The left sidebar shows a menu with 'Holidays', 'Time Schedules', 'Person Roles', and 'Person Groups'. The main content area is titled 'New Year's Day' and contains a form with the following sections:

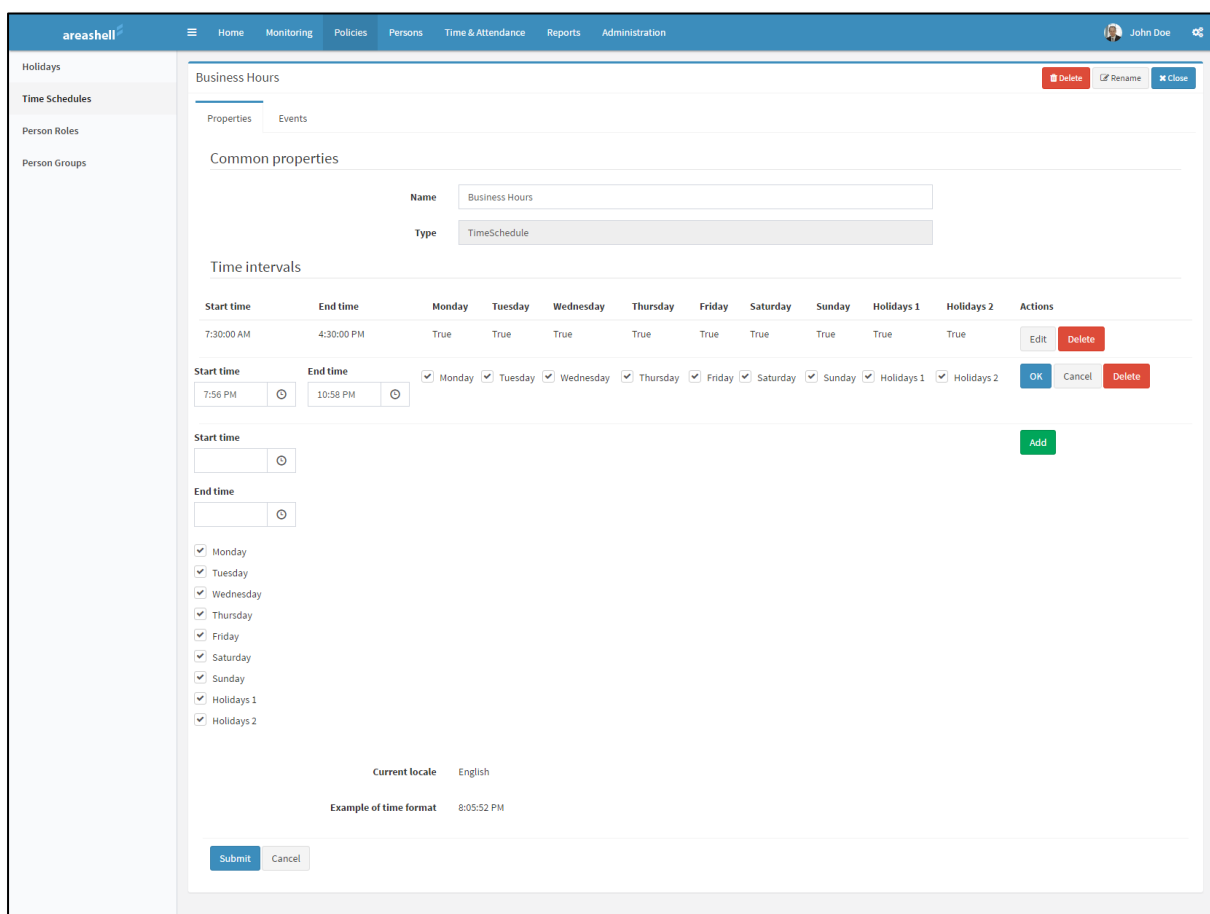
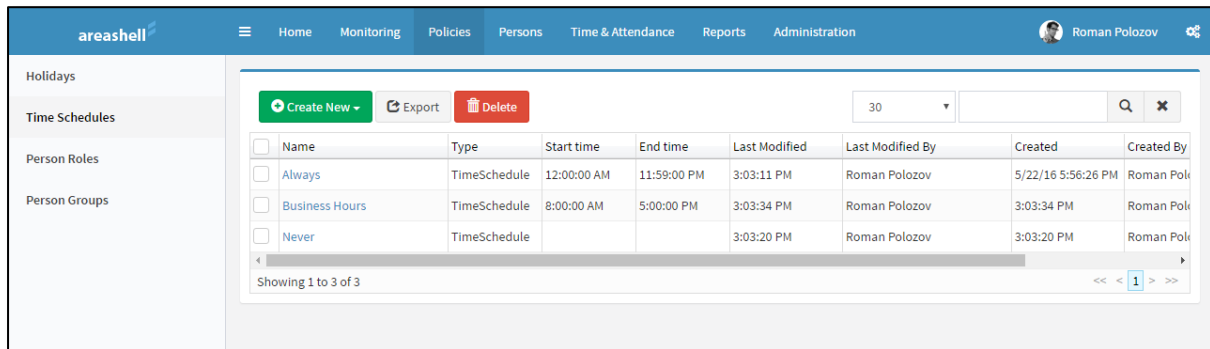
- Properties:** Includes tabs for 'Properties' and 'Events'.
- Common properties:**
 - Name:** Text input field containing 'New Year's Day'.
 - Type:** Dropdown menu set to 'Holiday'.
- Parameters:**
 - Holiday Type:** Dropdown menu set to 'Holiday 1'.
 - Holiday Date:** Text input field containing '1/1/17'.
 - Every year:** Checkbox labeled 'Enabled' which is checked.

At the bottom of the form are 'Submit' and 'Cancel' buttons. In the top right corner of the form area, there are 'Delete', 'Rename', and 'Close' buttons.

Comment: All holidays will be uploaded into all hardware controllers.

3.3 Time schedules

Configuring the time schedule is made in the console section Policies / Time Schedules.



Comment. All time schedules are loaded into all hardware controllers.

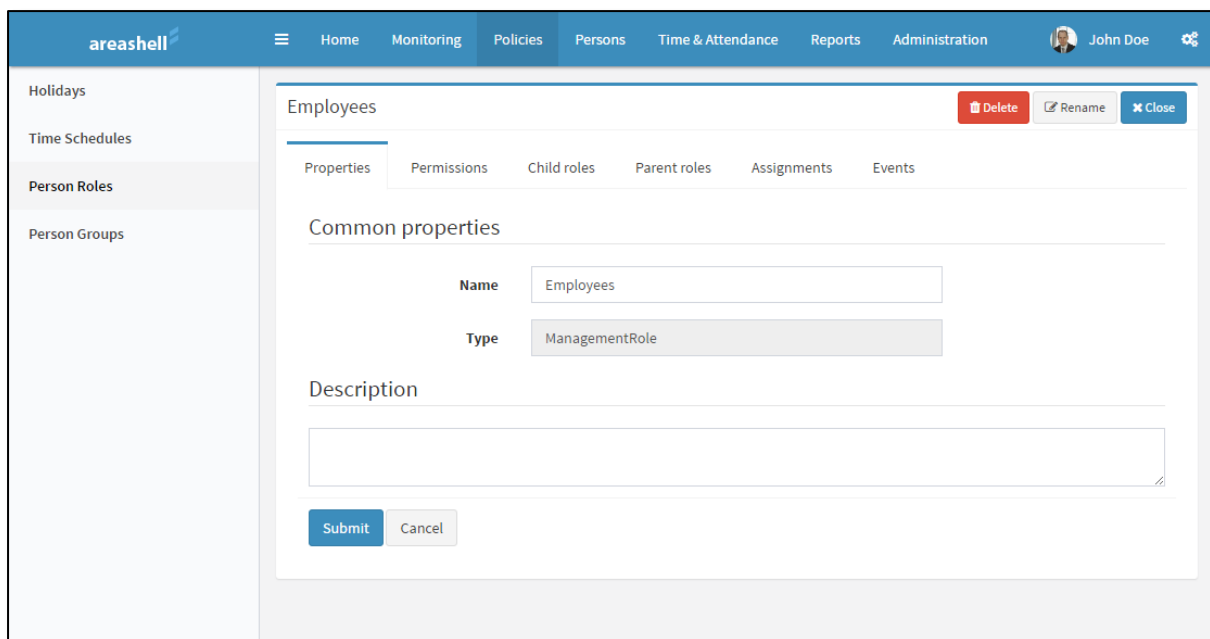
3.4 User Roles

A role is the basic mechanism of administrating user access to physical facilities and logical access to the system resources.

The role contains a list of resources to which access is permitted for users who are assigned this role.

Configuring user roles is performed in the console Policies / User Roles.

It is possible to specify the role name and enter a comment describing its purpose and its usage cases. The system only displays the comment and it does not affect the loading of configuration to the controllers or users' rights.



The screenshot shows the Areashell web application interface. The top navigation bar includes the 'areashell' logo, a menu icon, and tabs for Home, Monitoring, Policies, Persons, Time & Attendance, Reports, and Administration. The user 'John Doe' is logged in. On the left sidebar, 'Person Roles' is selected. The main content area displays the 'Employees' role configuration form. The form has tabs for Properties, Permissions, Child roles, Parent roles, Assignments, and Events. The 'Properties' tab is active, showing 'Common properties' with fields for 'Name' (Employees) and 'Type' (ManagementRole). There is a 'Description' text area and 'Submit' and 'Cancel' buttons at the bottom. Action buttons 'Delete', 'Rename', and 'Close' are in the top right corner of the form.

3.4.1 Role permissions

A list of objects and system resources, access to which is provided by this role, is on the tab "Rights"

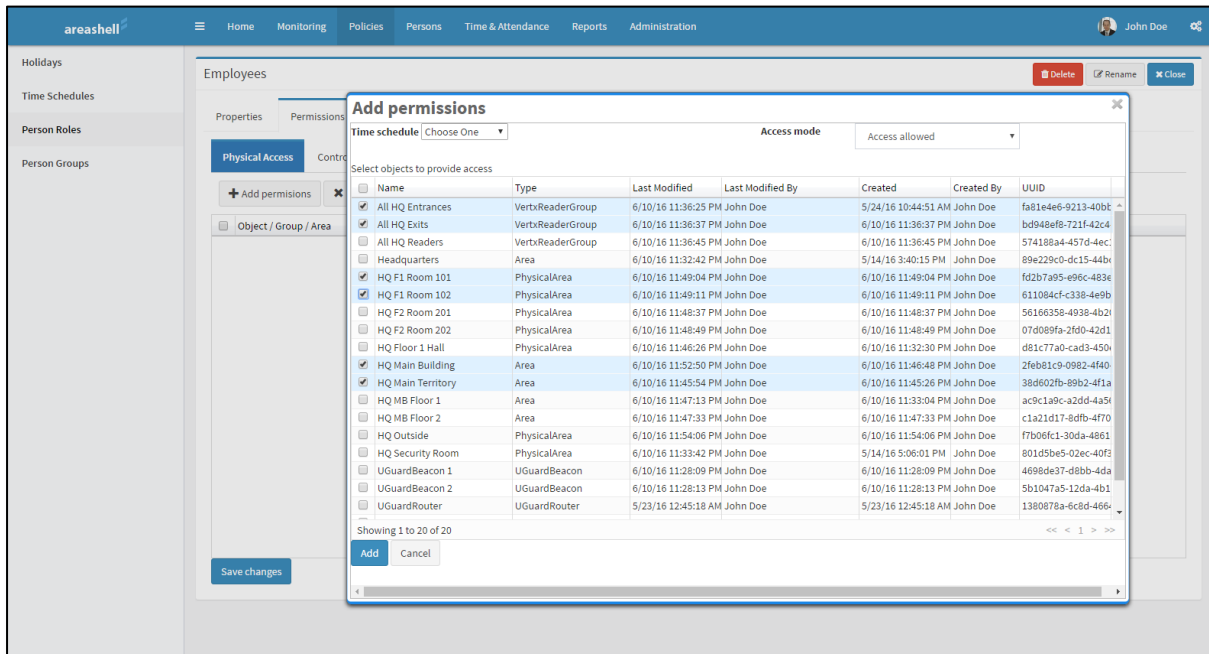
For easier administration, the resource list falls into groups:

- Physical access - the right to physical access to the area and premises
- Management - property management rights system through Areashell system web-based management interface
- Logical access - access rights to system functions (windows and panels Areashell web interface of the system)

The role can simultaneously contain access rights to all of these groups.

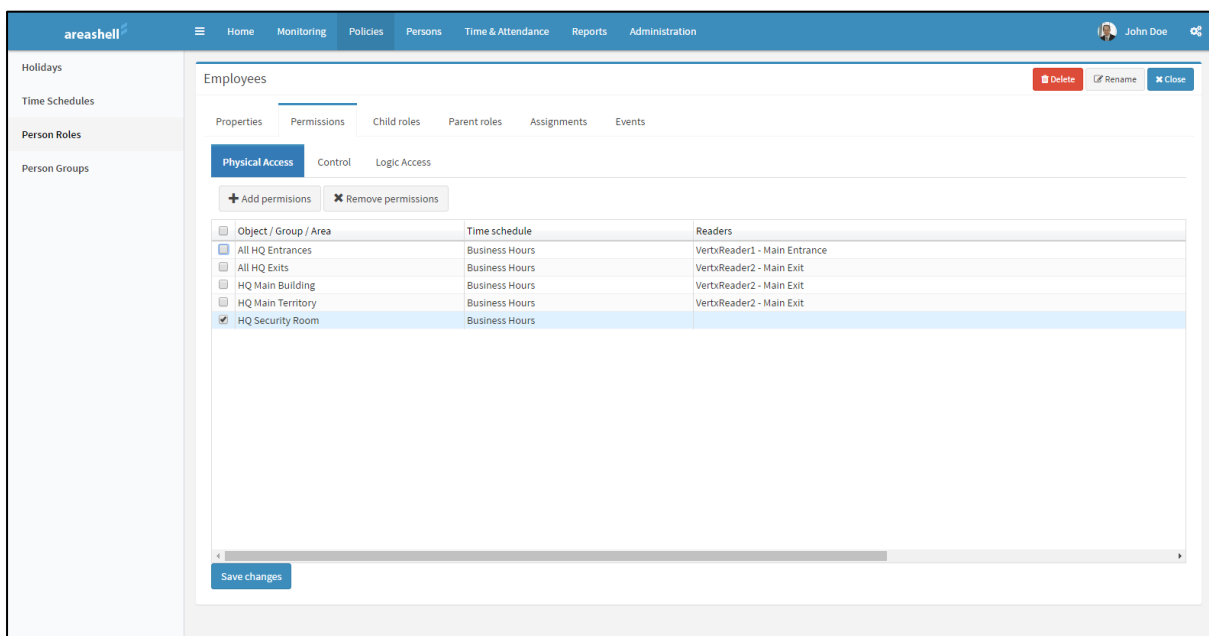
3.4.1.1 Administrating physical access rights

To add the role of physical access rights in the premises, click 'Add rights' on tab 'Physical Access', select needed readers, a group of readers or field, enter the access schedule in the 'Schedule', click 'Add', click 'Save Changes'.



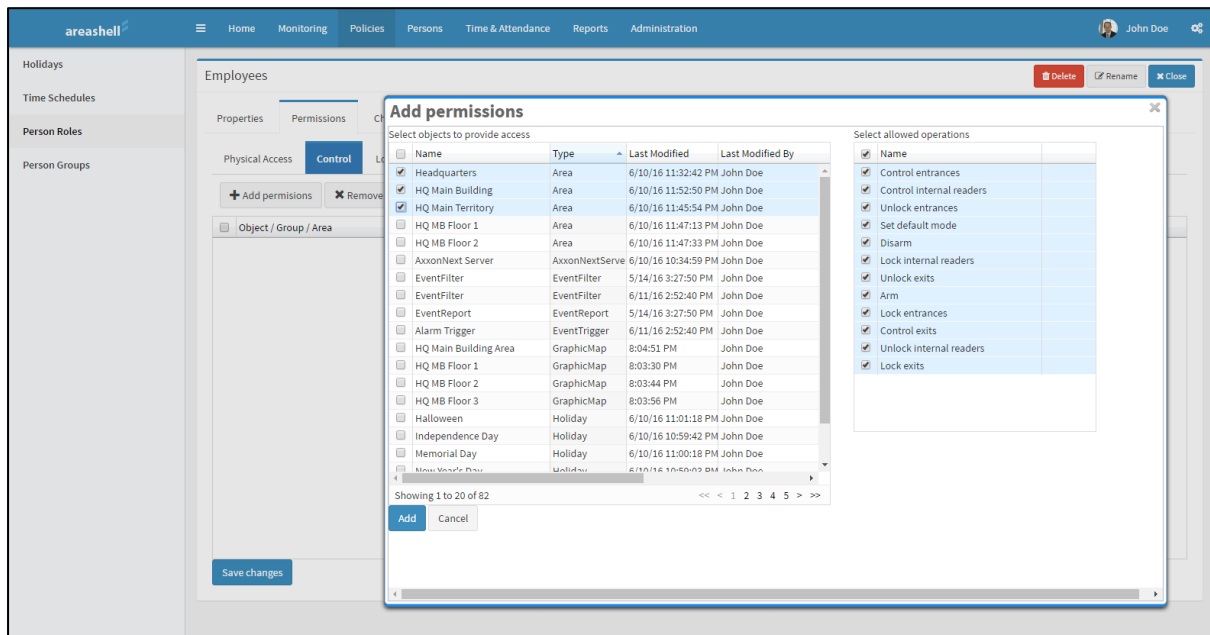
When setting the role of access rights to any area, the owners of this role (direct or indirect) have an access not only to this region, but also to all areas included in it (its daughter's domains).

To remove a previously assigned role of physical access rights, select it in the list, click 'Delete right', click 'Save Changes'.



3.4.1.2 Administrating object management rights

To add the role of object management rights through the system's web interface, click 'Add rights' on tab 'management', select the required system objects in the left side of the window, enter the allowed operations on selected objects in the list on the right side of the window, click 'Add', click 'Save changes'.



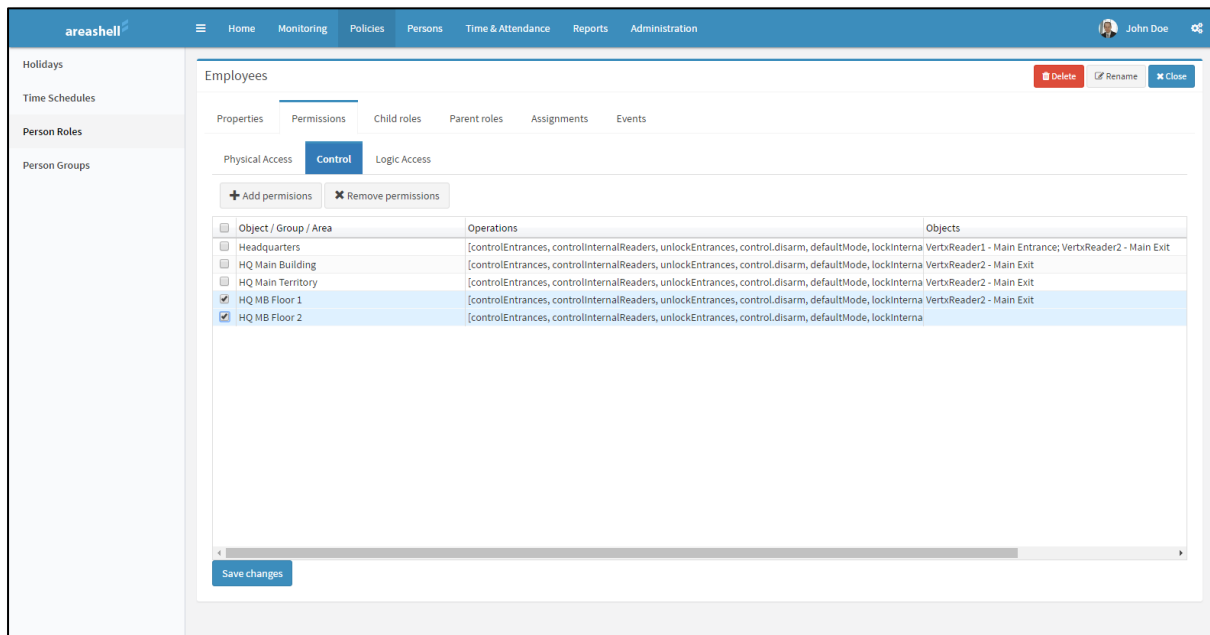
When setting the role of access to any area, the owners of this role have access to all the objects included in this area.

When setting the role of access rights to any area, the owners of this role (direct or indirect) have access not only to this area, but also to all areas included in it (its daughter's domains).

When setting the role of access rights to a group of security zones, owners of this role (direct or indirect) are allowed to manage all protection zones included in this group.

When setting the role of access rights to a group of outputs, the owners of this role (direct or indirect) are able to control all outputs included in this group.

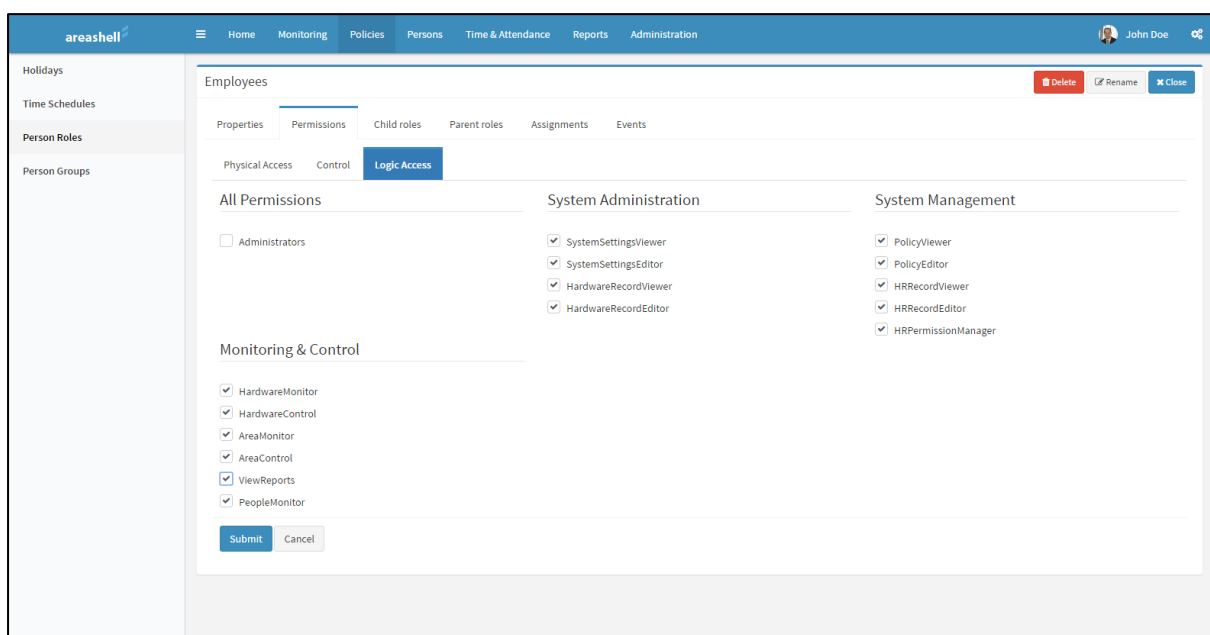
To remove previously assigned roles of facility management rights, select them in the list, click 'Delete rights', click 'Save Changes'.



3.4.1.3 Administrating system functions access rights

To set access rights to system functions through its web interface (Areashell web interface windows and panels) go to the tab 'logical access', specify operations permitted for this role in the operation system and click 'Apply'.

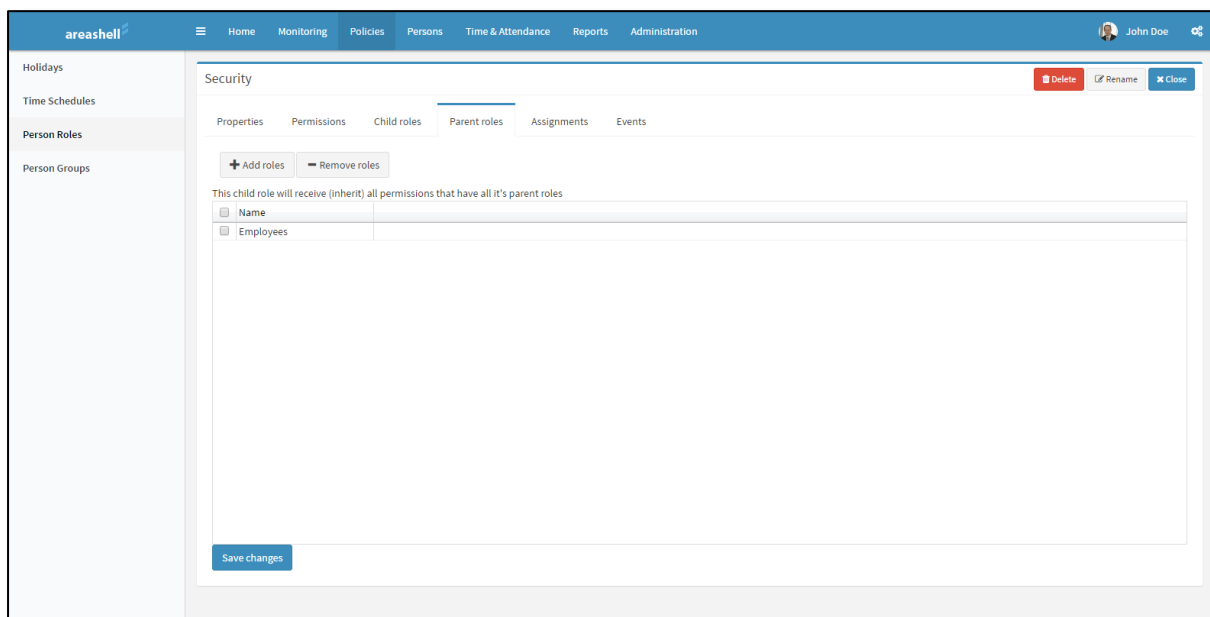
Comment. If "the Administrators" in the section 'All right' is checked, then all transactions in the system, regardless of the presence or absence of checks in other operations, are allowed for this role.



3.4.2 Role permission inheritance

Roles can be arranged in a hierarchy. One or more parent (basic) roles, as well as one or more daughter's roles, can be set for any role. Daughter's roles get all the permissions assigned to the parent (basic) roles.

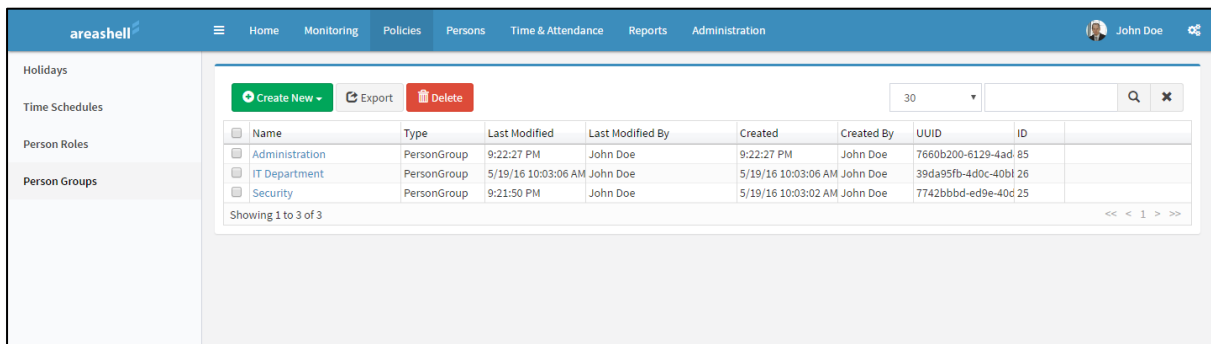
It is recommended first to configure the basic roles that contain common settings of access rights templates. Later they will become parental roles; for example, the role of the "Employee"). Then it is recommended to configure daughter's roles that inherit rights from the base, parental roles, and will be assigned to users and user groups (for example, the role of "Head of department" or "Security Officer").



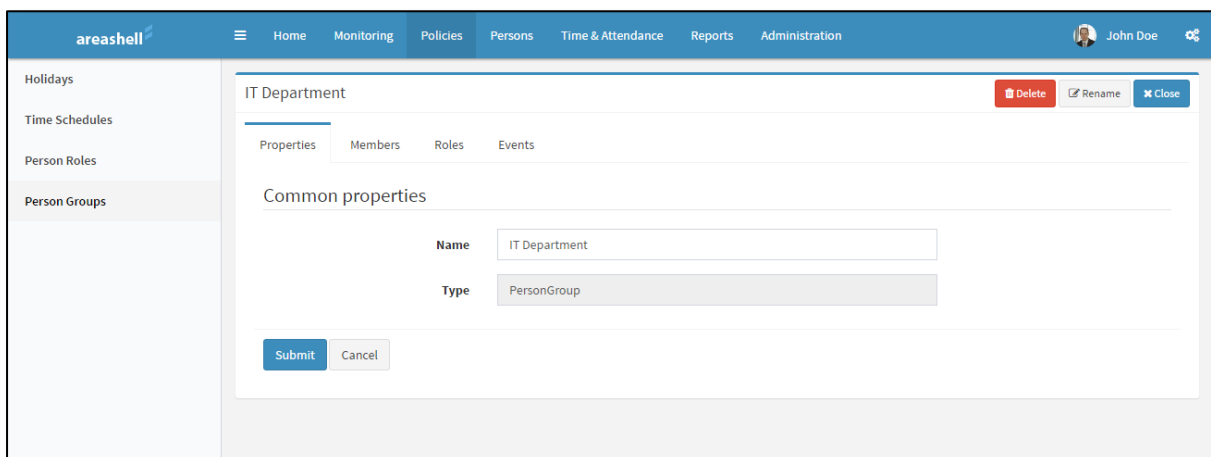
3.5 User groups

Users' groups can be used to simplify the user role administration. Roles can be assigned to users' groups as well as to individual users. All group users included in the group have the rights set for these roles.

Configuring users' groups is made in the console Policies / User Groups.



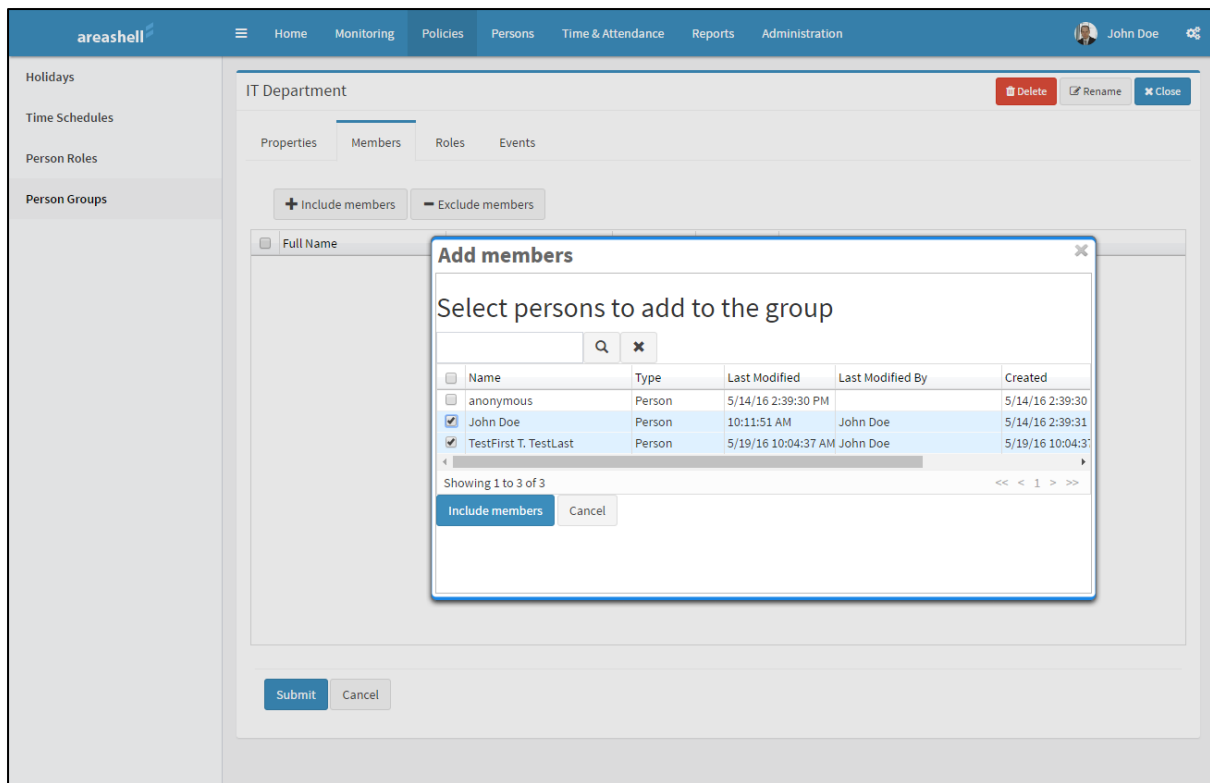
The group name that will be in the system list can be set on the tab "Properties"



To view a list of users who are included in the group, include and exclude users from the group is possible in the tab 'Included users'.

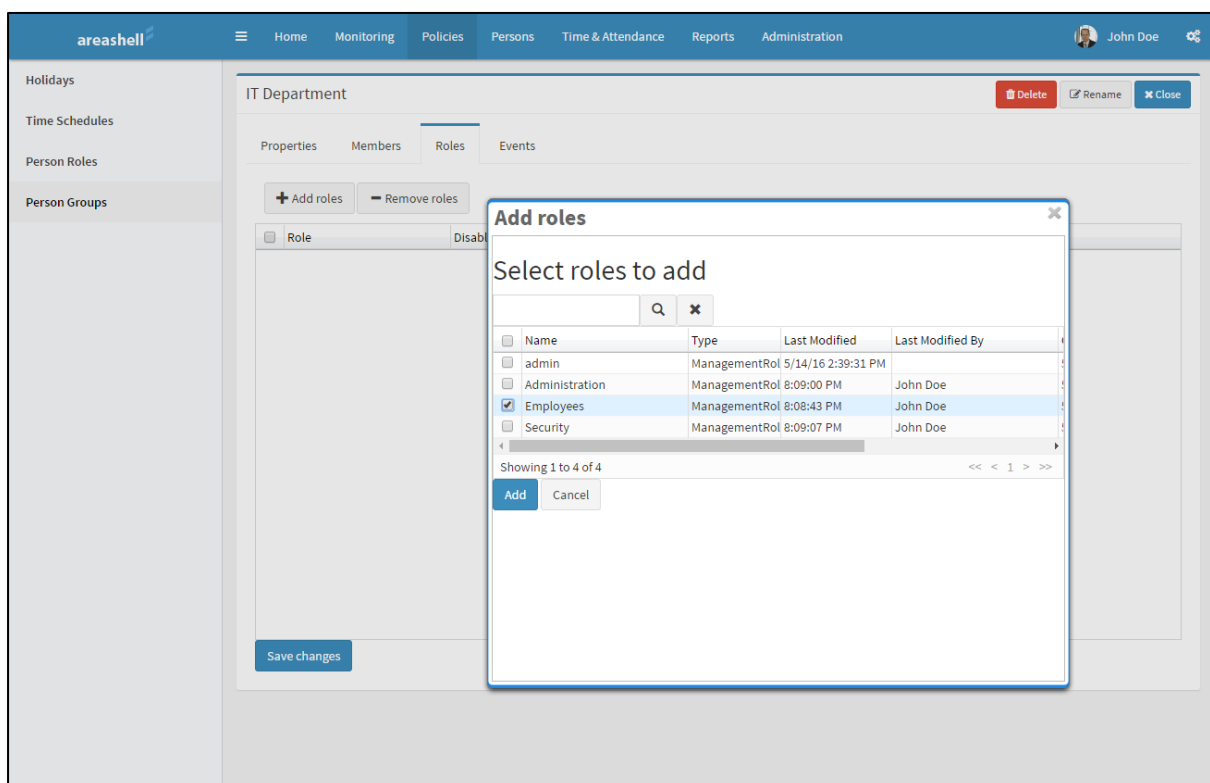
To include users to the group, click 'Switch User', select the user in the window, click 'Include members', then click 'Apply'.

Comment. To simplify the search for a particular user, use the search field at the top of the window. Type a few symbols of a last name or user name, press Enter or click the magnifying glass. To clear the search field and obtain a complete list of users, clear the search field, or click the cross.



View or edit the list of roles assigned to the users group in the tab "Roles"

To assign a user group a new role, click 'Add', select required roles in the pop-up window, click 'Add', click 'Save Changes'.



To remove previously assigned roles to group members, select them in the list, click 'Delete role', click 'Save Changes'.

The screenshot shows the 'areashell' administration interface. The top navigation bar includes 'Home', 'Monitoring', 'Policies', 'Persons', 'Time & Attendance', 'Reports', and 'Administration'. The left sidebar lists 'Holidays', 'Time Schedules', 'Person Roles', and 'Person Groups'. The main content area is titled 'IT Department' and has tabs for 'Properties', 'Members', 'Roles', and 'Events'. The 'Roles' tab is active, showing a table of assigned roles. Above the table are buttons for '+ Add roles' and '- Remove roles'. The table has columns for 'Role', 'Disabled', 'Activation time', and 'Expiration time'. Three roles are listed: 'Administration', 'Employees', and 'Security', all with 'Disabled' set to 'false'. A 'Save changes' button is at the bottom left of the table area. In the top right corner of the 'IT Department' section, there are buttons for 'Delete', 'Rename', and 'Close'.

<input type="checkbox"/>	Role	Disabled	Activation time	Expiration time
<input checked="" type="checkbox"/>	Administration	false		
<input type="checkbox"/>	Employees	false		
<input checked="" type="checkbox"/>	Security	false		

4 User Administration

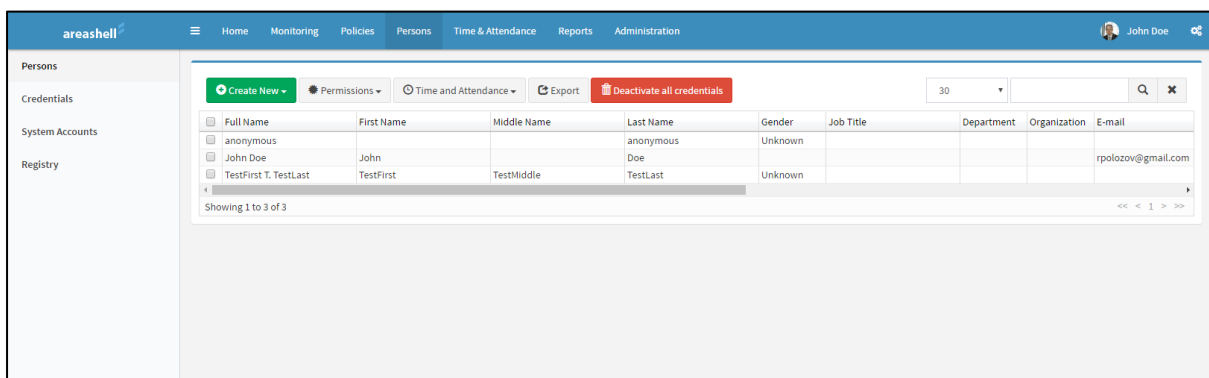
Data users, their access rights to premises and areas of the territory, their access rights to the system functions, user IDs are registered in Areashell database.

Different entities such as a remote card reader (proximity card), RFID-tags, personal identification numbers, a combination of user name and password, digital certificates, and others can be used as user IDs.

Each user can register multiple identities for different purposes. For example, to provide access to the system console, register the ID of the user name and password, and for physical access to the premises - a proximity card and PIN.

Comment. By default in the system there is one auto-generated system user: admin. The user admin has all the rights in the system and has a login account with the name 'admin' and the password 'admin'. For safety reasons, the admin user password must be changed after the installation of the system on the account settings panel of the user.

Working with the user registry is done in the Users section of the console.

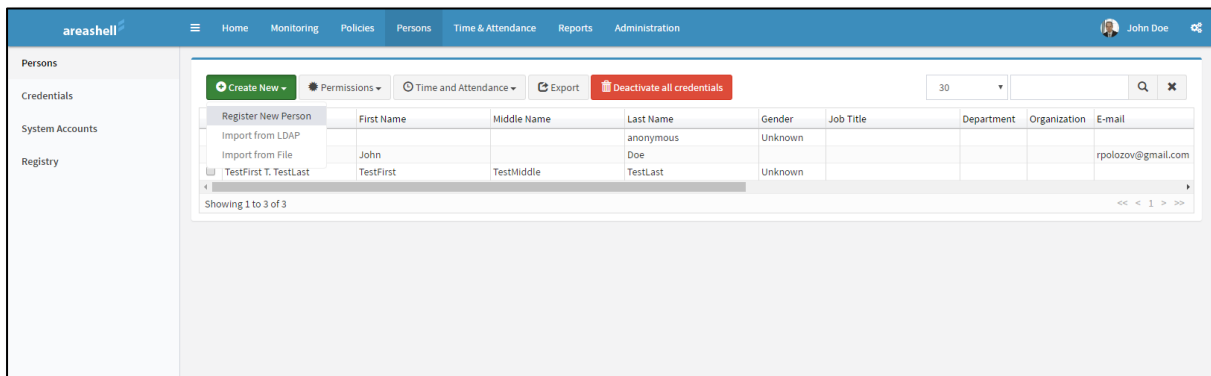


4.1 User registration

Users can be registered manually by entering user credentials in the form, or import the data from the corporate service LDAP / Active Directory directory or a file.

4.1.1 Registering users manually

To register a new user manually, select "Create / Register new user" from the toolbar.



On the opened panel 'Changing the user data' the following settings can be set:

- User credentials;
- Data of access control system ID (in the section 'To issue a new ID RFID') to create it automatically;
- Data of Areashell system account (in the 'Create an account') for its automatic creation;
- Upload a photo (you need to click 'Upload', select the file in the window that appears, click 'Upload image');
- Specify the comment text in any form (comment only is reflected in the system and does not affect the process of loading of configuration to the controllers or user rights).

areashell Home Monitoring Policies Persons Time & Attendance Reports Administration John Doe

Persons

Credentials
System Accounts
Registry

Personal

First Name: John
Middle Name:
Last Name: Doe
Gender: Male

Organization

Organization: Areashell
Department: IT Department
Job Title: IT Director

Contacts

E-mail: jdoe@areashell.com
Phone: 9876543210

Issue new RFID credential (optional)

Number: 12345
Card set: VertxCardSet
PIN: ****
☒ Enabled
Activation time: 06/01/2016
Expiration time: 06/01/2017
Access type: Card Or PIN

Create new system account (optional)

Name: jdoe
Password: *****
☒ Enabled
Activation time: 06/01/2016
Expiration time: 06/01/2017

Submit Cancel

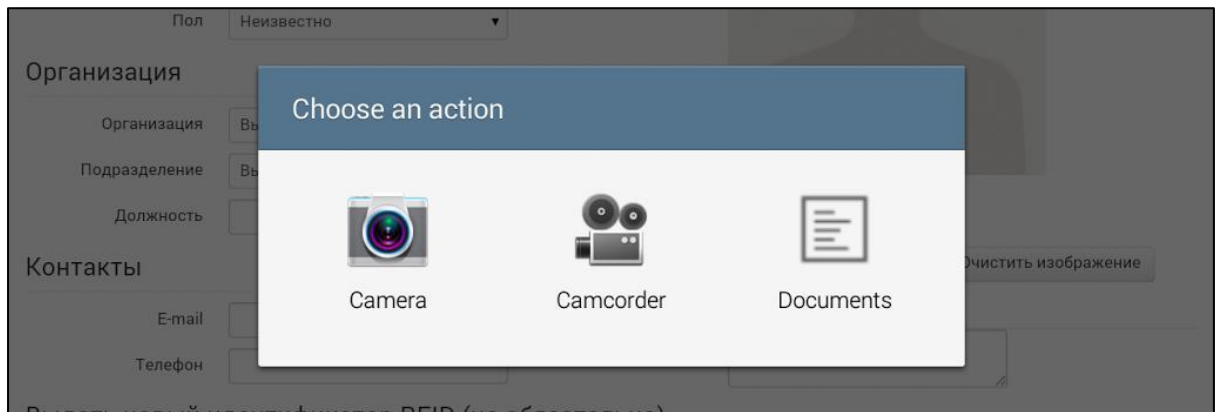
Picture

Upload new picture
Choose File No file chosen Upload Clear
uploaded file: photo.jpg

Notes

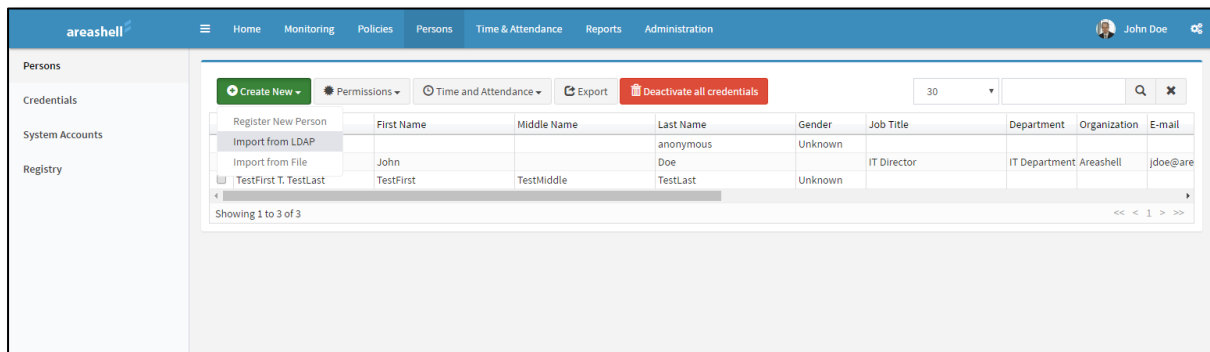
Comment. The picture loaded on the form, as well as other user data, is stored in the system database only after clicking 'Submit' at the bottom of the page.

Comment. When working on a mobile device in a mobile web browser that supports the proper function, there is an opportunity to upload a photo of the user directly photographing it by using the built-in camera device. In this case, after pressing the 'Upload' in the system window offering to select the device from which to import an image, select the built-in camera (Camera). After receiving the image in the camera, the saved file will automatically enter the field "Upload Image", where it is necessary to click 'Upload picture'. Save the properties by clicking the 'Submit' at the bottom of the page.



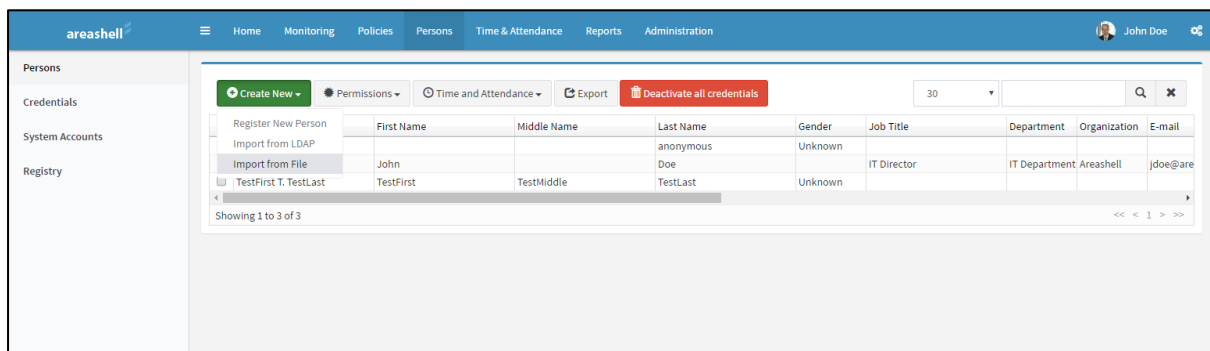
4.1.2 Registering users through importing data from directory services

To register new users by importing data from LDAP / Active Directory enterprise directory service, click on the toolbar "Create / Import from an LDAP directory."



4.1.3 Registering users by importing data from a file

To register new users by importing data from a file, click on the toolbar "Create / Import from file'.



4.2 User data editing

To change the user data, the management of its rights' issue or withdrawal, identifiers need to select the user in the user table.

Editing of personal data or uploading of a new photo can be made on the tab Properties.

The screenshot displays the 'areashell' user management interface. The top navigation bar includes links for Home, Monitoring, Policies, Persons, Time & Attendance, Reports, and Administration. The left sidebar lists 'Persons', 'Credentials', 'System Accounts', and 'Registry'. The main content area is titled 'John Doe' and features a 'Properties' tab. The 'Properties' tab is divided into several sections: 'Personal' (First Name: John, Middle Name, Last Name: Doe, Gender: Choose One), 'Organization' (Organization: Areashell, Department: IT Department, Job Title: IT Director), 'Contacts' (E-mail: jdoe@areashell.com, Phone: 9493316116), and 'Active credentials' (a table with columns: Type, Identity, Enabled, Activation time, Expiration time). The 'Active credentials' table shows one entry: Login, admin, true, and empty cells for activation and expiration times. To the right of the 'Personal' section is a 'Picture' section with a user photo and an 'Upload new picture' button. Below the 'Picture' section is a 'Notes' section with a text area. At the top right of the 'Properties' tab, there are buttons for 'Delete', 'Rename', and 'Close'.

4.3 User Rights Management

To assign user rights to access to the premises and to the system functions, the roles are assigned to the user.

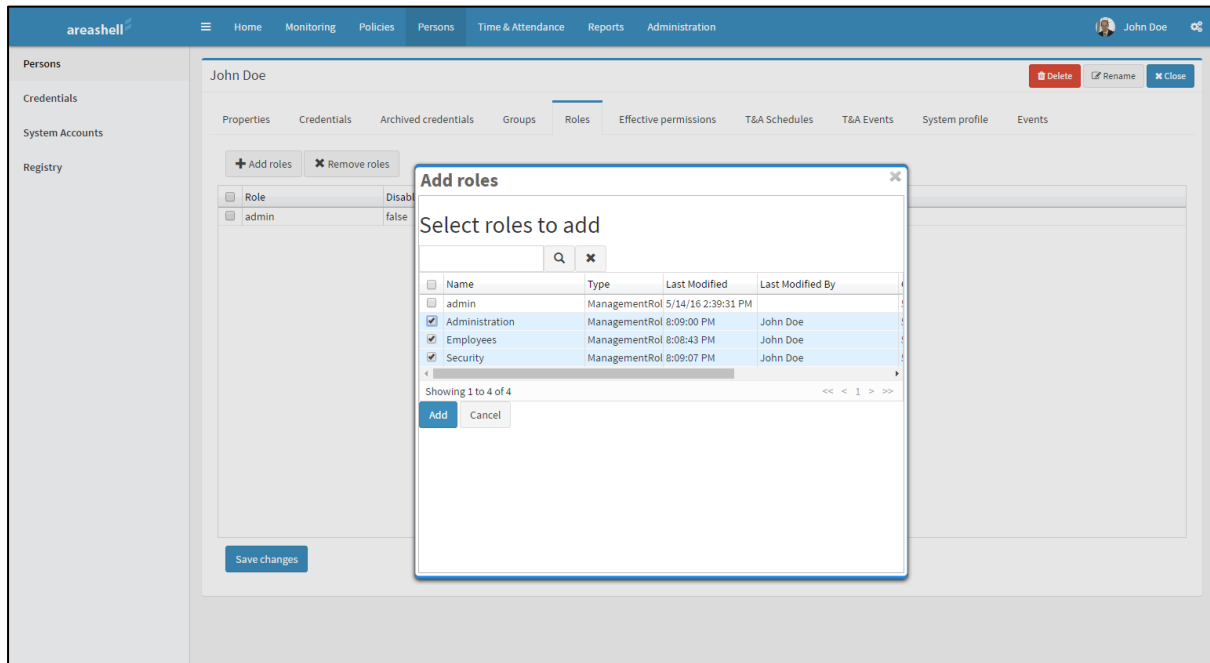
Roles can be assigned directly to users, by adding these roles in the control panel of user roles and indirectly through entering the user to the group.

A user can have several roles, and be included in multiple user groups. The user gets all the rights assigned to all his roles and all of its user groups.

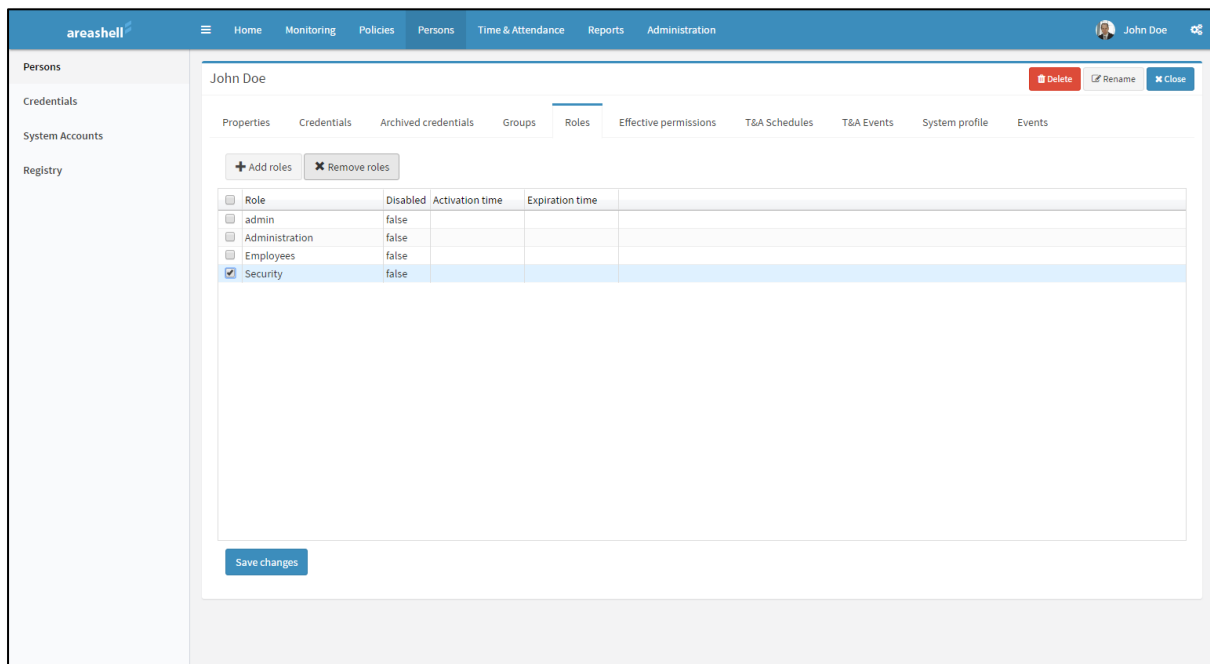
4.3.1.1.1 Direct role assigning to the user

Direct assigning of roles to the user is made on the 'Roles' tab.

To add a role, click "Add Roles", select the role in the window, click 'Add', click 'Save Changes'.



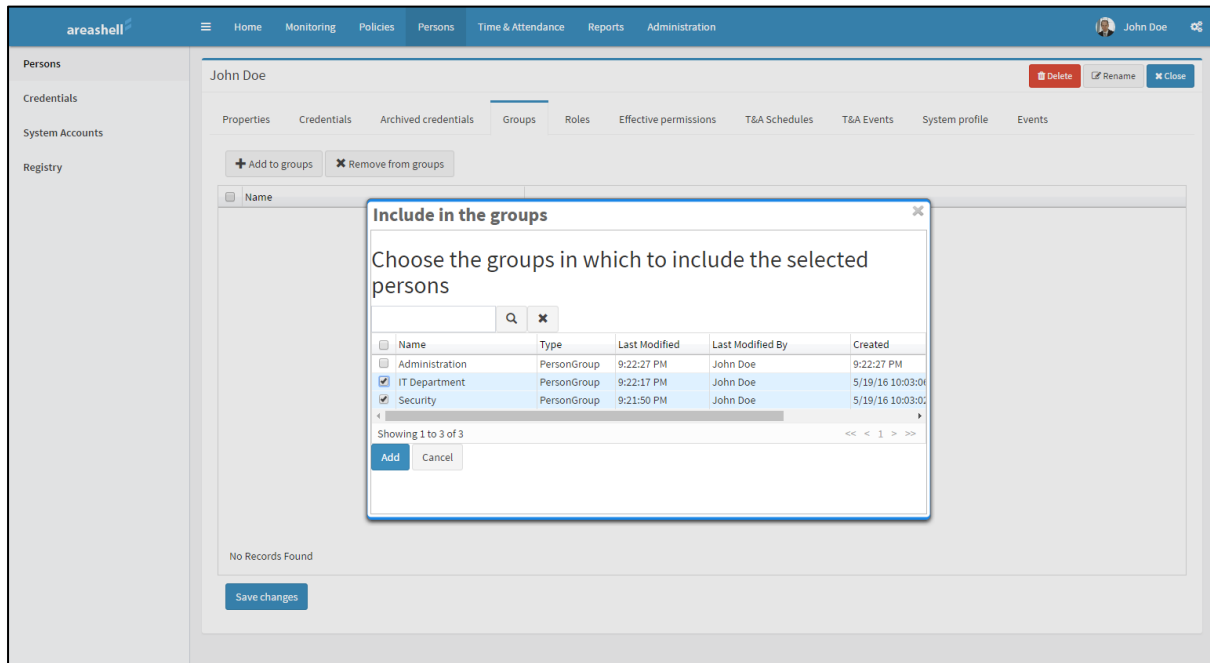
To remove previously assigned roles, select them in the list, click 'Delete role', click 'Save Changes'.



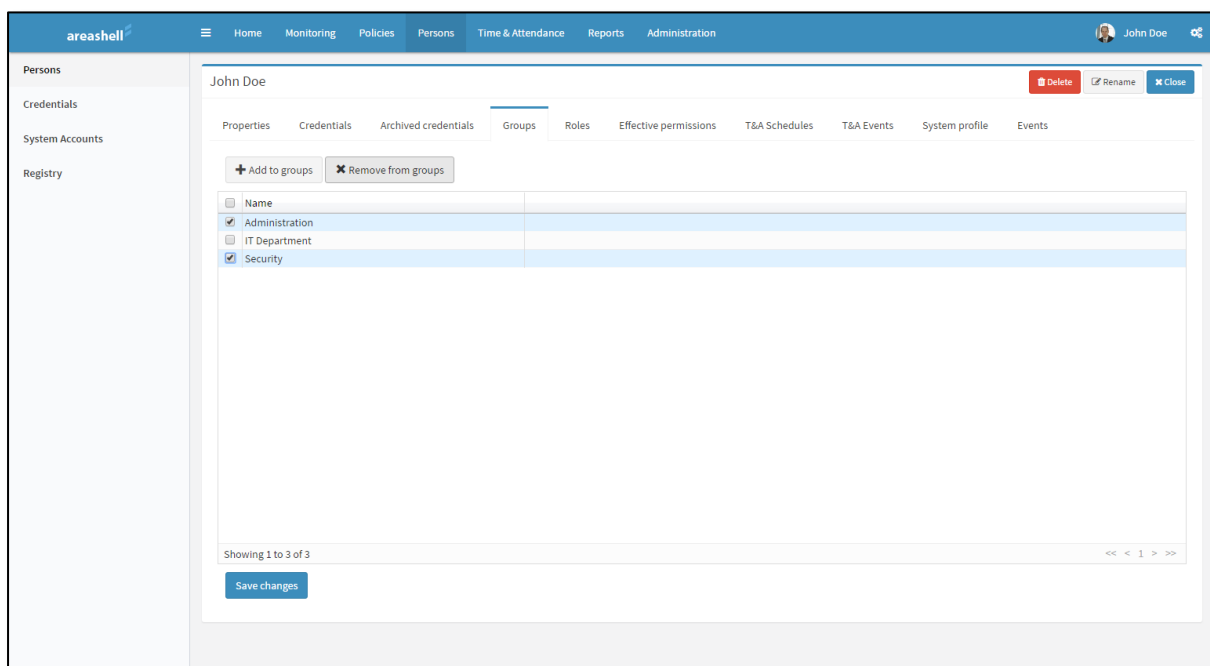
4.3.1.1.2 Including users to groups

Including users to groups is made on 'Groups' tab.

To add a user, click 'Add to Group' in the group, select the role in the window, click 'Add', click 'Save Changes'.



To exclude user from groups to which he/she was included previously, select it in the list, click 'Remove from group', click 'Save Changes'.



4.1 Administration of user credentials

Administering User IDs (cards, key fobs, RFID-tags, etc.) is made on the tab 'identifiers' of the user's card.

To register a new user ID in the access control system (physical access), click 'Create the RFID' tab 'identifiers', enter the ID parameters in the panel at the bottom of the page, click 'Apply'.

The screenshot displays the 'Identifiers' tab for user John Doe. The interface includes a sidebar with 'Persons', 'Credentials', 'System Accounts', and 'Registry'. The main panel shows a table of credentials for John Doe, with columns for Type, Identity, Enabled, Activation time, and Expiration time. Below the table is a form titled 'Edit HID VertX/EDGE RFID Properties' with fields for Number, Card set, PIN, Enabled, Activation time, Expiration time, and Access type. The form has 'Submit' and 'Cancel' buttons at the bottom.

Type	Identity	Enabled	Activation time	Expiration time
Login	admin	true		
VertxRFID	123456	true	6/21/16	6/21/17

Edit HID VertX/EDGE RFID Properties

Number: 123456

Card set: VertxCardSet

PIN: ****

Enabled: ☒ Enabled

Activation time: 6/21/16

Expiration time: 6/21/17

Access type: Choose One

Submit Cancel

When selecting an identifier at the bottom of the page, the panel with the ID parameter is displayed. After correcting the ID settings, click Apply to save changes to the database system.

Specify the following options when configuring a holiday:

- Number – the identifier recorded on the recording medium (card, key fob, the RFID-tag, etc.), and read by the reader.
- Card Set – the system configuration object that describes the card format and its parameters (usually contains the organization code).
- If the card set is not specified, the conversion of the identifier read from the controller is not made, and it is necessary to set the original, complete ID number in the field Identifier's number.

If the card set is specified, the controller converts the ID read from the media, and in the ID field it is necessary to set only a part of the individual identity without organization code, control bits and other identifier's fields.

- Activation time – the date and time from which the system allows the access to this identifier. Given a date has not yet arrived, then the access is denied and it will be denied till the date comes.
- Deactivation time – the date and time from which the system denies access to this identifier. If the date is set in the past, then the access will be denied to the ID.
- Access Type specifies the required for the presentation of the identifier (authentication factors). There are some options: Card Only, PIN Only, Card or PIN, Card and PIN.
- Enabled – this flag should be set for all identifiers that should have the access.

The screenshot shows the 'Persons' section for 'John Doe' in the Areashell administration interface. The interface includes a navigation bar with tabs like Home, Monitoring, Policies, Persons, Time & Attendance, Reports, and Administration. The 'Persons' tab is active, showing a table of credentials for 'John Doe'. The table has columns for Type, Identity, Enabled, Activation time, and Expiration time. Below the table is a form titled 'Edit HID VertX/EDGE RFID Properties' with fields for Number, Card set, PIN, Enabled, Activation time, Expiration time, and Access type. The 'Enabled' checkbox is currently unchecked.

Type	Identity	Enabled	Activation time	Expiration time
VertxRFID	123456	false	6/21/16	6/21/17

Edit HID VertX/EDGE RFID Properties

Number: 123456

Card set: VertxCardSet

PIN:

Enabled: ☐ Enabled

Activation time: 6/21/16

Expiration time: 6/21/17

Access type: Choose One

Submit Cancel

All active IDs immediately after the creation are loaded into all hardware controllers of the system, in the settings of which the 'Communicate with the configuration change' flag is set and to the readers of which the user has access.

Comment. Access permissions are not set for credentials. Access permissions are set for the user through assigning user's roles and including the user into user groups. These permissions are loaded into controllers for all active user credentials.

When unchecking the check box 'Activated' ID and saving the changes to the database a credential is removed from the control panels of the system, in settings of which the

check box 'communicate with a configuration change' is checked, a credential disappears from the list on the active IDs tab 'credentials' and appears on the inactive IDs tab 'Archive credentials'.

When checking an active credential in the list and pressing the button Delete, a credential is also deleted in the list of active credentials and moved to the list of inactive credentials.

In order to restore the activity of an inactive credential, select it from the list of inactive credentials (on the tab 'Archive IDs'), check 'Enabled', click 'Apply'. This ID will disappear from the list on the tab 'Archive credentials', appear on the tab 'credentials', and will be loaded into the control panels.

To control the list of rights obtained by the user through assigning roles and including in groups, use the tab 'Effective rights'.

Type	Access mode	Resource	Time schedule	Role
<input type="checkbox"/> Inherited logic access	Access allowed			Employees
<input type="checkbox"/> Inherited logic access	Access allowed			Security
<input type="checkbox"/> Inherited logic access	Access allowed			Employees
<input type="checkbox"/> Logic access	Access allowed			Employees
<input type="checkbox"/> Logic access	Access allowed			Employees
<input type="checkbox"/> Logic access	Access allowed			admin
<input type="checkbox"/> Inherited logic access	Access allowed			Employees
<input type="checkbox"/> Logic access	Access allowed			Security
<input type="checkbox"/> Logic access	Access allowed			Employees
<input type="checkbox"/> Physical access		All HQ Entrances	Business Hours	Employees
<input type="checkbox"/> Physical access		All HQ Entrances	Business Hours	Employees
<input type="checkbox"/> Physical access		All HQ Entrances	Business Hours	Employees
<input type="checkbox"/> Physical access		All HQ Exits	Business Hours	Employees
<input type="checkbox"/> Physical access		All HQ Exits	Business Hours	Employees
<input type="checkbox"/> Physical access		All HQ Exits	Business Hours	Employees
<input type="checkbox"/> Control	Access allowed	Headquarters		Employees
<input type="checkbox"/> Control	Access allowed	Headquarters		Employees
<input type="checkbox"/> Control	Access allowed	Headquarters		Employees

Showing 1 to 30 of 39

If such a credential as Account is created for the user in the list of credentials, then the user can log in to the web-based system management console.

The screenshot shows the 'John Doe' user profile in the 'Credentials' tab. The left sidebar contains links for 'Persons', 'Credentials', 'System Accounts', and 'Registry'. The top navigation bar includes 'Home', 'Monitoring', 'Policies', 'Persons', 'Time & Attendance', 'Reports', and 'Administration'. The user profile header shows 'John Doe' with 'Delete', 'Rename', and 'Close' buttons. Below the header are tabs for 'Properties', 'Credentials', 'Archived credentials', 'Groups', 'Roles', 'Effective permissions', 'T&A Schedules', 'T&A Events', 'System profile', and 'Events'. The 'Credentials' tab is active, displaying a table with columns: Type, Identity, Enabled, Activation time, and Expiration time. The table contains three rows: 'Login' (admin), 'VeriRFID' (123456), and an empty row. Below the table is the 'Edit Account Properties' section with fields for 'Login name' (admin), 'Password' (masked), 'Enabled' (checked), 'Activation time' (6/01/2016), and 'Expiration time'. 'Submit' and 'Cancel' buttons are at the bottom.

Type	Identity	Enabled	Activation time	Expiration time
Login	admin	true		
VeriRFID	123456	true	6/21/16	6/21/17

Attention. The user account can be created automatically by the system if, when installing the system, the user authentication with the use of corporate directory service was configured and enabled, and the user entered into the system management console.

Parameters of the system work can be set for users who have an account in the system on the tab 'System Profile'.

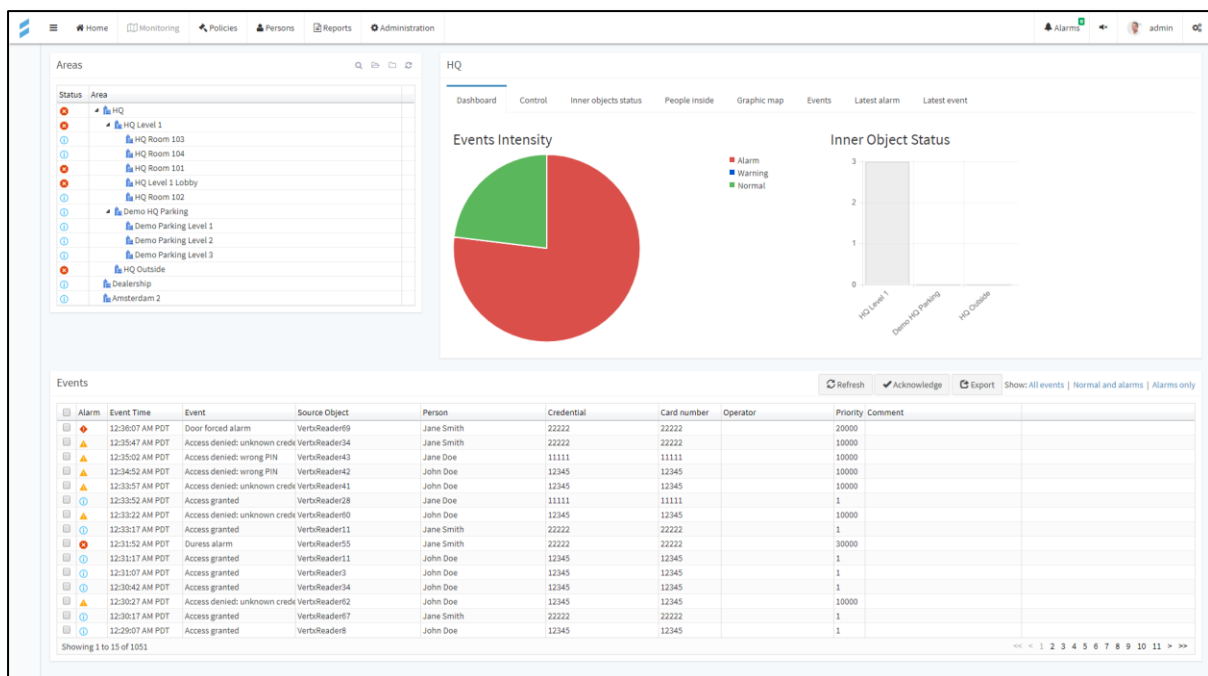
The screenshot shows the 'John Doe' user profile in the 'System profile' tab. The left sidebar and top navigation bar are the same as in the previous screenshot. The 'System profile' tab is active, displaying 'Personal user preferences' with fields for 'Control console locale' (English), 'Time zone' ((UTC-8:0) America/Los_Angeles - Pacific Daylight Time), 'Sound alarm notifications' (checked), and 'Monitoring mode refresh interval (sec)' (500). Below this is the 'Event tables properties' section with four checkboxes: 'Show global time column' (checked), 'Show registration time column' (checked), 'Show TimeZone column' (checked), and 'Show TimeZone offset column' (checked). The 'Monitoring properties' section has a 'Default checkpoint' dropdown menu set to 'Choose One'. 'Submit' and 'Cancel' buttons are at the bottom.

5 System monitoring and control

Tracking the current situation and the operational management of the system is carried out in the section Monitoring Console.

Several modes of operation are available in the section Monitoring.

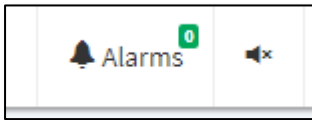
- Areas – monitoring the status of areas, tracking the user location in the areas, tracking and managing objects in the areas;
- Graphic Maps – monitoring system state objects status in the local graphic plans;
- Checkpoint – message monitoring on several specific readers in the form of cards;
- Object location – monitoring the current position of mobile objects in the global graphic plans;
- Only events – monitoring new events in the system in the form of a table.



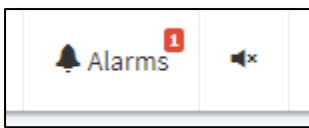
5.1 Alarm acknowledgment

The button Alarm in all modes of section Monitoring in the title bar shows the current number of recent unacknowledged alarms.

If there is no alarm, the button displays value 0.

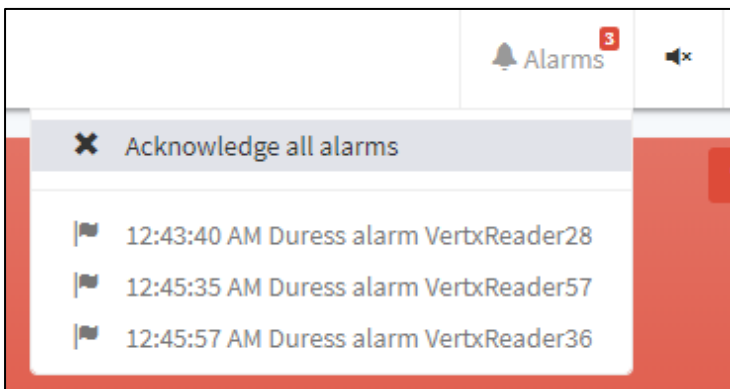


When the alarms happen, their numbers are displayed and there is an audio signal that attracts attention (the use of audio signals should be allowed in a web browser for this web site).



When pressing the alarm button the panel with a list of unacknowledged alarms opens. Any alarm can be acknowledged by selecting it in the list. All the alarms can be acknowledged by selecting 'Confirm all alarms'.

After confirmation, the alarm disappears from the list and, if there are no unacknowledged alarms, the alarm button displays 0 and the audio signal disappears.



5.2 Event monitoring in table mode

Monitoring new events appearing in the system in the form of a table is available in a special mode Only Messages in Monitoring section and in Areas, Graphic Maps, Location modes.

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
▲	12:47:11 AM PDT	Access denied: no door access	VerbiReader13	Jane Smith	22222	22222		10000	
▲	12:46:29 AM PDT	Access denied: door schedule	VerbiReader59	John Doe	12345	12345		10000	
○	12:46:18 AM PDT	Access granted	VerbiReader47	Jane Smith	22222	22222		1	
▲	12:46:08 AM PDT	Access denied: area violation	VerbiReader48	Jane Doe	11111	11111		10000	
▲	12:45:57 AM PDT	Duress alarm	VerbiReader36	Jane Doe	11111	11111		30000	
○	12:45:53 AM PDT	Access granted	VerbiReader24	John Doe	12345	12345		1	
▲	12:45:48 AM PDT	Access denied: unknown creds	VerbiReader43	John Doe	12345	12345		10000	
○	12:45:35 AM PDT	Duress alarm	VerbiReader57	Jane Doe	11111	11111		30000	
○	12:45:30 AM PDT	Access denied: unknown creds	VerbiReader5	Jane Smith	22222	22222		10000	
▲	12:45:19 AM PDT	Access denied: unknown creds	VerbiReader33	Jane Smith	22222	22222		10000	
○	12:45:09 AM PDT	Access granted	VerbiReader11	Jane Smith	22222	22222		1	
○	12:45:02 AM PDT	Access granted	VerbiReader69	Jane Smith	22222	22222		1	
○	12:44:55 AM PDT	Access granted	VerbiReader44	Jane Smith	22222	22222		1	
○	12:44:48 AM PDT	Access granted	VerbiReader42	John Doe	12345	12345		1	
○	12:44:46 AM PDT	Access granted	VerbiReader70	Jane Smith	22222	22222		1	
▲	12:44:37 AM PDT	Access denied: door schedule	VerbiReader29	John Doe	12345	12345		10000	
▲	12:44:32 AM PDT	Access denied: door schedule	VerbiReader26	John Doe	12345	12345		10000	
○	12:44:28 AM PDT	Access granted	VerbiReader34	John Doe	12345	12345		1	
○	12:44:24 AM PDT	Access granted	VerbiReader33	Jane Smith	22222	22222		1	
▲	12:44:14 AM PDT	Access denied: door schedule	VerbiReader24	John Doe	12345	12345		10000	
▲	12:44:03 AM PDT	Door forced alarm	VerbiReader11	Jane Smith	22222	22222		20000	
▲	12:43:57 AM PDT	Access denied: APB violation	VerbiReader54	Jane Smith	22222	22222		10000	
▲	12:43:40 AM PDT	Duress alarm	VerbiReader28	John Doe	12345	12345		30000	
▲	12:43:25 AM PDT	Access denied: APB violation	VerbiReader40	John Doe	12345	12345		10000	
▲	12:43:01 AM PDT	Door forced alarm	VerbiReader35	Jane Doe	11111	11111		20000	
▲	12:42:51 AM PDT	Access denied: no door access	VerbiReader5	John Doe	12345	12345		10000	
○	12:42:48 AM PDT	Access granted	VerbiReader47	Jane Doe	11111	11111		1	
○	12:42:47 AM PDT	Access granted	VerbiReader17	John Doe	12345	12345		1	
▲	12:42:40 AM PDT	Access denied: door schedule	VerbiReader5	Jane Doe	11111	11111		10000	
▲	12:42:38 AM PDT	Access denied: no door access	VerbiReader37	Jane Doe	11111	11111		10000	

The events in the table can be filtered according to their alarm level. To view all events in the table, select the title 'All events'. Select Only Alarms to view alarm events only.

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
○	12:47:35 AM PDT	Duress alarm	VerbiReader61	Jane Doe	11111	11111		30000	
○	12:45:57 AM PDT	Duress alarm	VerbiReader36	Jane Doe	11111	11111		30000	
○	12:45:35 AM PDT	Duress alarm	VerbiReader57	Jane Doe	11111	11111		30000	
○	12:44:01 AM PDT	Door forced alarm	VerbiReader11	Jane Smith	22222	22222		20000	
○	12:43:40 AM PDT	Duress alarm	VerbiReader28	John Doe	12345	12345		30000	
○	12:43:03 AM PDT	Door forced alarm	VerbiReader35	Jane Doe	11111	11111		20000	
○	12:36:07 AM PDT	Door forced alarm	VerbiReader69	Jane Smith	22222	22222		20000	
○	12:31:52 AM PDT	Duress alarm	VerbiReader55	Jane Smith	22222	22222		30000	
○	12:25:07 AM PDT	Door forced alarm	VerbiReader50	John Doe	12345	12345		20000	
○	12:16:07 AM PDT	Door forced alarm	VerbiReader39	John Doe	12345	12345		20000	
○	12:16:02 AM PDT	Door forced alarm	VerbiReader53	John Doe	12345	12345		20000	
○	12:10:12 AM PDT	Duress alarm	VerbiReader27	Jane Doe	11111	11111		30000	
○	12:09:02 AM PDT	Door forced alarm	VerbiReader55	Jane Smith	22222	22222		20000	
○	12:07:02 AM PDT	Door forced alarm	VerbiReader69	John Doe	12345	12345		20000	
○	12:02:12 AM PDT	Door forced alarm	VerbiReader46	John Doe	12345	12345		20000	
○	12:00:42 AM PDT	Door forced alarm	VerbiReader1	Jane Doe	11111	11111		20000	
○	12:00:27 AM PDT	Duress alarm	VerbiReader31	John Doe	12345	12345		30000	
○	9/9/18 11:56:47 PM	Door forced alarm	VerbiReader33	Jane Doe	11111	11111		20000	
○	9/9/18 11:54:37 PM	Door forced alarm	VerbiReader65	Jane Doe	11111	11111		20000	
○	9/9/18 11:53:32 PM	Door forced alarm	VerbiReader15	Jane Doe	11111	11111		20000	
○	9/9/18 11:52:37 PM	Duress alarm	VerbiReader48	Jane Smith	22222	22222		30000	
○	9/9/18 11:52:52 PM	Duress alarm	VerbiReader63	Jane Smith	22222	22222		30000	
○	9/9/18 11:50:07 PM	Duress alarm	VerbiReader21	John Doe	12345	12345		30000	
○	9/9/18 11:48:07 PM	Door forced alarm	VerbiReader72	Jane Smith	22222	22222		20000	
○	9/9/18 11:52:32 PM	Duress alarm	VerbiReader18	Jane Smith	22222	22222		30000	
○	9/9/18 11:17:27 PM	Door forced alarm	VerbiReader4	John Doe	12345	12345		20000	
○	9/9/18 11:15:27 PM	Duress alarm	VerbiReader31	John Doe	12345	12345		30000	
○	9/9/18 11:12:02 PM	Door forced alarm	VerbiReader28	Jane Smith	22222	22222		20000	
○	9/9/18 11:07:27 PM	Door forced alarm	VerbiReader50	Jane Smith	22222	22222		20000	
○	9/9/18 11:06:07 PM	Door forced alarm	VerbiReader33	John Doe	12345	12345		20000	

To view more detailed information about an event, click on it in the table.

Event Details

Access denied: APB violation

John Doe
12345

Local time: Monday, September 10, 2018 12:48:11 AM PDT
 UTC: Monday, September 10, 2018 7:48:11 AM UTC
 Reg. time: Monday, September 10, 2018 12:48:11 AM PDT
 Source Object: VertReader45
 Operator:
 Acknowledged by:

[Acknowledge](#) [Close](#)

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
<input type="checkbox"/>	12:48:36 AM PDT	Access granted						1	
<input type="checkbox"/>	12:48:34 AM PDT	Access granted						1	
<input type="checkbox"/>	12:48:33 AM PDT	Access granted						1	
<input type="checkbox"/>	12:48:12 AM PDT	Access denied						10000	
<input type="checkbox"/>	12:48:11 AM PDT	Access denied						10000	
<input type="checkbox"/>	12:48:09 AM PDT	Door forced alarm						20000	
<input type="checkbox"/>	12:48:04 AM PDT	Access denied						10000	
<input type="checkbox"/>	12:48:00 AM PDT	Door forced alarm						20000	
<input type="checkbox"/>	12:47:52 AM PDT	Access granted						1	
<input type="checkbox"/>	12:47:49 AM PDT	Configuration						1	
<input type="checkbox"/>	12:47:45 AM PDT	Access denied						10000	
<input type="checkbox"/>	12:47:37 AM PDT	Access denied						10000	
<input type="checkbox"/>	12:47:35 AM PDT	Duress alarm						30000	
<input type="checkbox"/>	12:47:29 AM PDT	Access granted						1	
<input type="checkbox"/>	12:47:25 AM PDT	Access denied						10000	
<input type="checkbox"/>	12:47:23 AM PDT	Access granted						1	
<input type="checkbox"/>	12:47:15 AM PDT	Access granted						10000	
<input type="checkbox"/>	12:47:11 AM PDT	Access denied						1	
<input type="checkbox"/>	12:46:47 AM PDT	Configuration						10000	
<input type="checkbox"/>	12:46:29 AM PDT	Access denied						1	
<input type="checkbox"/>	12:46:18 AM PDT	Access granted						10000	
<input type="checkbox"/>	12:46:08 AM PDT	Access denied						1	
<input type="checkbox"/>	12:45:57 AM PDT	Duress alarm						30000	
<input type="checkbox"/>	12:45:53 AM PDT	Access granted						1	
<input type="checkbox"/>	12:45:48 AM PDT	Access denied						10000	
<input type="checkbox"/>	12:45:47 AM PDT	Configuration synchronized	ParkingCloudConnection					1	
<input type="checkbox"/>	12:45:35 AM PDT	Duress alarm	VertReader57	Jane Doe	11111	11111		30000	
<input type="checkbox"/>	12:45:30 AM PDT	Access denied: unknown cred	VertReader9	Jane Smith	22222	22222		10000	
<input type="checkbox"/>	12:45:10 AM PDT	Access denied: unknown cred	VertReader33	Jane Smith	22222	22222		10000	
<input type="checkbox"/>	12:45:05 AM PDT	Access granted	VertReader51	Jane Smith	22222	22222		1	

Showing 1 to 30 of 1500

To save in the database the confirmation that the original message of the event has been viewed by the operator click Acknowledge. A separate acknowledging message with information about the operator who acknowledged it and the exact time of acknowledgement is saved in the database. If the event has already been acknowledged, the acknowledgements field displays the names of the operators who have acknowledged it.

Click Close to return to the event table.

To acknowledge several messages, select them in the table, checking the checkboxes in the first column of the table (check the checkbox in the title of the first column to select all the rows in the current page) and click the Acknowledge button

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
<input checked="" type="checkbox"/>	12:49:13 AM PDT	Access denied: door schedule	VertReader58	John Doe	12345	12345		10000	
<input checked="" type="checkbox"/>	12:49:10 AM PDT	Access granted	VertReader74	Jane Smith	22222	22222		1	
<input checked="" type="checkbox"/>	12:49:09 AM PDT	Access granted	VertReader58	Jane Doe	11111	11111		1	
<input checked="" type="checkbox"/>	12:49:07 AM PDT	Access denied: unknown cred	VertReader58	Jane Doe	11111	11111		10000	
<input checked="" type="checkbox"/>	12:48:47 AM PDT	Configuration synchronized	ParkingCloudConnection					1	
<input checked="" type="checkbox"/>	12:48:40 AM PDT	Access granted	VertReader45	Jane Smith	22222	22222		1	
<input checked="" type="checkbox"/>	12:48:36 AM PDT	Access granted	VertReader26	John Doe	12345	12345		1	
<input checked="" type="checkbox"/>	12:48:34 AM PDT	Access granted	VertReader39	Jane Doe	11111	11111		1	
<input checked="" type="checkbox"/>	12:48:33 AM PDT	Access granted	VertReader41	Jane Doe	11111	11111		1	
<input checked="" type="checkbox"/>	12:48:12 AM PDT	Access denied: wrong PIN	VertReader1	Jane Doe	11111	11111		10000	
<input checked="" type="checkbox"/>	12:48:11 AM PDT	Access denied: APB violation	VertReader45	John Doe	12345	12345		10000	
<input checked="" type="checkbox"/>	12:48:09 AM PDT	Door forced alarm	VertReader3	Jane Smith	22222	22222		20000	
<input checked="" type="checkbox"/>	12:48:04 AM PDT	Access denied: wrong PIN	VertReader31	Jane Doe	11111	11111		10000	
<input checked="" type="checkbox"/>	12:48:00 AM PDT	Door forced alarm	VertReader51	Jane Doe	11111	11111		20000	
<input checked="" type="checkbox"/>	12:47:52 AM PDT	Access granted	VertReader28	John Doe	12345	12345		1	
<input checked="" type="checkbox"/>	12:47:49 AM PDT	Configuration synchronized	ParkingCloudConnection					1	
<input checked="" type="checkbox"/>	12:47:45 AM PDT	Access denied: wrong PIN	VertReader28	John Doe	12345	12345		10000	
<input checked="" type="checkbox"/>	12:47:37 AM PDT	Access denied: APB violation	VertReader40	Jane Smith	22222	22222		10000	

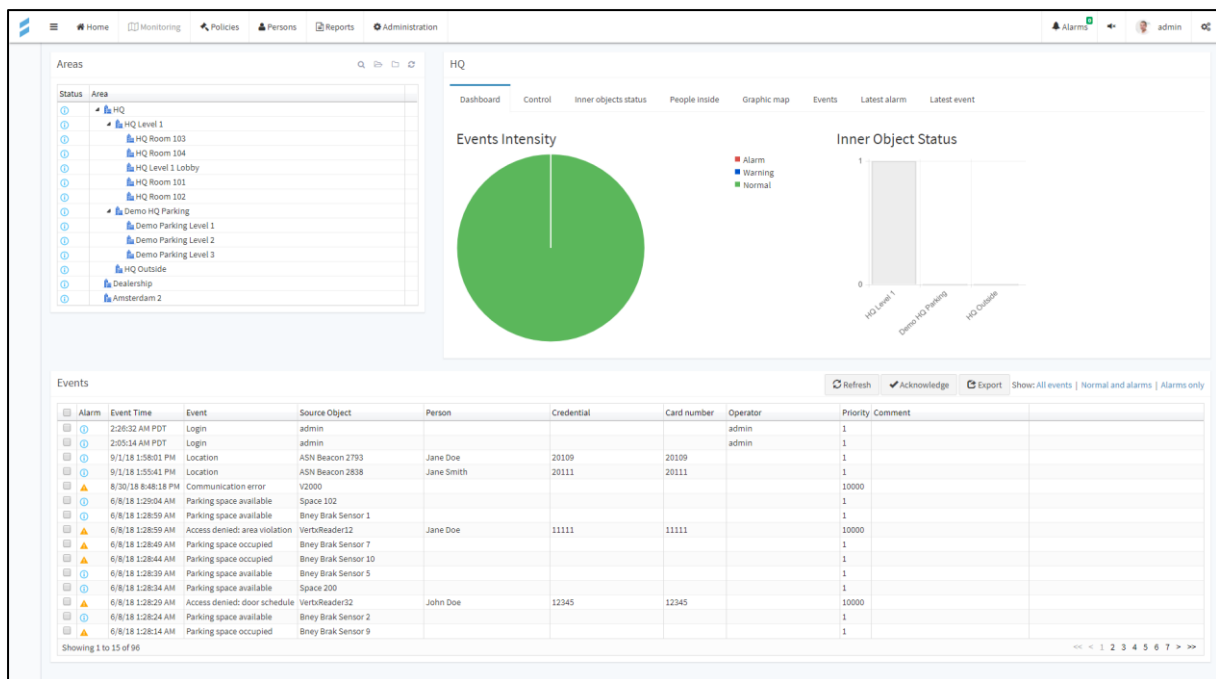
5.3 System monitoring in areas mode

The tree panel area (top left), the panel of the state and control of the selected area (top right), and the panel with the recent events table (below) are displayed in the page in the area mode.

The icon on the panel with an area tree in the column Status displays the status of each area. If any area has an alarming status, then all groups of areas in which it is included will have the alarm status too. For example, if the area Room is included in the group of areas Floor, which, in turn, is a part of the areas of Buildings, and if the alarm message comes from any object, located in the room, then the alarm status will be in all three areas: Building, Floor, Room.

When selecting any area in the area tree in the panel to the right, there appears the panel with a set of bookmarks, which display detailed information and zone status of objects in the area that are included, users, the domain control panel and the objects located therein.

The tab Panel displays general information about the status of the selected area: the ratio between the current number of alarm and non-alarm messages, a chart showing the number of messages from the sub-areas of the selected area.



An area control command can be executed on the Control Panel: to move all of the objects in the default mode, lock or unlock the inputs or outputs, supply or disarm zones located in the area, etc.

Attention: If the selected area contains enclosed areas, the command will be issued to all the objects in all enclosed areas. For example, if to issue the command 'Disarm' for the area Building, then all alarm zones in this building will be disarmed.

The screenshot displays the Areashell Administration interface. The top navigation bar includes Home, Monitoring, Policies, Persons, Reports, and Administration. The left sidebar shows a tree view of Areas, including HQ and Demo HQ Parking. The main content area is titled 'HQ' and contains several sections: 'Set default mode' with a 'Set default mode' button, 'Entrances' with 'Unlock entrances', 'Lock entrances', and 'Control entrances' buttons, 'Exits' with 'Unlock exits', 'Lock exits', and 'Control exits' buttons, 'Internal readers' with 'Unlock internal readers', 'Lock internal readers', and 'Control internal readers' buttons, and 'Alarm zones' with 'Arm' and 'Disarm' buttons. Below these sections is an 'Events' table with columns for Alarm, Event Time, Event, Source Object, Person, Credential, Card number, Operator, Priority, and Comment. The table shows a list of events, including access denied, login, location, communication error, and parking space availability. The bottom of the interface shows 'Showing 1 to 15 of 97' events.

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
Access denied: wrong PIN	2:27:22 AM PDT	Access denied: wrong PIN	VerbaReader36	Jane Doe	11111	11111		10000	
Login	2:28:32 AM PDT	Login		admin			admin	1	
Login	2:55:14 AM PDT	Login		admin			admin	1	
Location	9/1/18 1:58:01 PM	Location	ASN Beacon 2793	Jane Doe	20109	20109		1	
Location	9/1/18 1:55:41 PM	Location	ASN Beacon 2838	Jane Smith	20111	20111		1	
Communication error	8/30/18 8:48:18 PM	Communication error	V2000					10000	
Parking space available	6/8/18 1:29:04 AM	Parking space available	Space 102					1	
Parking space available	6/8/18 1:28:59 AM	Parking space available	Bney Brak Sensor 1					1	
Access denied: area violation	6/8/18 1:28:59 AM	Access denied: area violation	VerbaReader32	Jane Doe	11111	11111		10000	
Parking space occupied	6/8/18 1:28:49 AM	Parking space occupied	Bney Brak Sensor 7					1	
Parking space occupied	6/8/18 1:28:44 AM	Parking space occupied	Bney Brak Sensor 10					1	
Parking space available	6/8/18 1:28:39 AM	Parking space available	Bney Brak Sensor 5					1	
Parking space available	6/8/18 1:28:34 AM	Parking space available	Space 200					1	
Access denied: door schedule	6/8/18 1:28:29 AM	Access denied: door schedule	VerbaReader32	John Doe	12345	12345		10000	
Parking space available	6/8/18 1:28:24 AM	Parking space available	Bney Brak Sensor 2					1	

The tab Inner Object Status displays a list of all enclosed objects that are in the selected area. The column Status displays the alarm status of objects. The columns Latest Event, Event Time, Registration Time display the relevant information about the recent events on the mobile objects.

The screenshot displays the Areashell 1.7 Administration interface. The top navigation bar includes links for Home, Monitoring, Policies, Persons, Reports, and Administration. The left sidebar shows a tree view of areas, with 'HQ Level 1' selected. The main content area is titled 'HQ Level 1' and contains a table of object status. The table has columns for Status, Source Object, Type, Latest Event, Event Time (local), Event Time (UTC), Registration Time, and Registration Time (UTC). Below the table, there is a section for 'Events' with a table of event logs. The event log table has columns for Alarm, Event Time, Event, Source Object, Person, Credential, Card number, Operator, Priority, and Comment. The interface also includes a 'Refresh' button and a 'Show: All events | Normal and alarms | Alarms only' dropdown menu.

Status	Source Object	Type	Latest Event	Event Time (local)	Event Time (UTC)	Registration Time	Registration Time (UTC)
ADN Beacon 2838	Unknown						
VerbiReader	VerbiReader	Unknown					
VerbiReader10	VerbiReader	Access granted	2:35:27 AM PDT	9:35:27 AM UTC	2:35:27 AM PDT	9:35:27 AM UTC	
VerbiReader11	VerbiReader	Unknown					
VerbiReader12	VerbiReader	Unknown					
VerbiReader13	VerbiReader	Unknown					
VerbiReader14	VerbiReader	Access denied: wrong PIN	2:44:37 AM PDT	9:44:37 AM UTC	2:44:37 AM PDT	9:44:37 AM UTC	
VerbiReader15	VerbiReader	Access denied: wrong schedule	2:38:07 AM PDT	9:38:07 AM UTC	2:38:07 AM PDT	9:38:07 AM UTC	
VerbiReader16	VerbiReader	Access denied: wrong PIN	2:27:22 AM PDT	9:27:22 AM UTC	2:27:22 AM PDT	9:27:22 AM UTC	
VerbiReader17	VerbiReader	Unknown					
VerbiReader18	VerbiReader	Unknown					
VerbiReader19	VerbiReader	Unknown					
VerbiReader2	VerbiReader	Unknown					
VerbiReader3	VerbiReader	Unknown					
VerbiReader4	VerbiReader	Duress alarm	2:44:17 AM PDT	9:44:17 AM UTC	2:44:17 AM PDT	9:44:17 AM UTC	
VerbiReader5	VerbiReader	Access denied: no door access	9:40:07 AM UTC	2:40:07 AM PDT	9:40:07 AM UTC	2:40:07 AM PDT	
VerbiReader6	VerbiReader	Access denied: area violation	2:46:57 AM PDT	9:46:57 AM UTC	2:46:57 AM PDT	9:46:57 AM UTC	
VerbiReader7	VerbiReader	Access denied: no door access	2:30:22 AM PDT	9:30:22 AM UTC	2:30:22 AM PDT	9:30:22 AM UTC	
VerbiReader8	VerbiReader	Access granted	2:37:22 AM PDT	9:37:22 AM UTC	2:37:22 AM PDT	9:37:22 AM UTC	
VerbiReader9	VerbiReader	Unknown					

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
2:46:57 AM PDT	Access denied: area violation	VerbiReader6	Jane Doe	11111	11111		10000		
2:46:12 AM PDT	Access denied: wrong PIN	VerbiReader30	Jane Doe	11111	11111		10000		
2:46:42 AM PDT	Access denied: door schedule	VerbiReader44	Jane Smith	22222	22222		10000		
2:46:37 AM PDT	Access denied: wrong PIN	VerbiReader14	Jane Doe	11111	11111		10000		
2:44:27 AM PDT	Access granted	VerbiReader62	John Doe	12345	12345		1		
2:44:22 AM PDT	Access granted	VerbiReader62	Jane Doe	11111	11111		1		
2:44:17 AM PDT	Duress alarm	VerbiReader4	Jane Doe	11111	11111		10000		
2:43:37 AM PDT	Access denied: wrong PIN	VerbiReader29	Jane Smith	22222	22222		10000		
2:43:17 AM PDT	Access granted	VerbiReader44	John Doe	12345	12345		1		
2:42:17 AM PDT	Access granted	VerbiReader48	Jane Doe	11111	11111		1		
2:41:52 AM PDT	Access granted	VerbiReader69	Jane Smith	22222	22222		1		
2:40:32 AM PDT	Access denied: unknown cred	VerbiReader55	Jane Doe	11111	11111		10000		
2:40:07 AM PDT	Access denied: no door access	VerbiReader5	Jane Doe	11111	11111		10000		
2:39:52 AM PDT	Access denied: area violation	VerbiReader17	John Doe	12345	12345		10000		
2:39:27 AM PDT	Access denied: APB violation	VerbiReader38	John Doe	12345	12345		10000		

To open object control panel, select an object in the list (display panel depends on the type of object selected). After giving the control command of the chosen object, it is possible to return to the list of objects in the area, by clicking the Close button in the object control panel.

The screenshot displays the Areashell 1.7 Administration interface. On the left, a sidebar shows a tree view of areas under 'HQ', including 'HQ Level 1', 'HQ Room 101', 'HQ Room 104', 'HQ Room 101', 'HQ Level 1 Lobby', 'HQ Room 102', 'Demo HQ Parking', 'Demo Parking Level 1', 'Demo Parking Level 2', 'HQ Outside', 'Chelmsbury', and 'Amsterdam 2'. The main panel is titled 'VerbiReader4' and contains several sections: 'Control' (People nearby, Events, Latest alarm, Latest event), 'Access' (Access grant, Access deny, Reset cardholder status), 'Inputs' (Forced alarm, Held alarm, Local alarm feedback), 'Outputs' (Strike, Beeper, Aux output), and 'LEDs' (Green LED, Red LED, PIN request flash red/green). Each section has toggle buttons for 'On', 'Off', and 'Tuned On'. At the bottom, an 'Events' table lists recent events with columns for Alarm, Event Time, Event, Source Object, Person, Credential, Card number, Operator, Priority, and Comment. The table shows various access events for Jane Smith and John Doe. A 'Showing 1 to 15 of 130' indicator is at the bottom left of the table.

It is possible to view the list of people in the chosen area on the tab People Inside. When selecting a group of areas in the given list, a list of all users, who are in all the internal areas of the selected group, displays. That is, by choosing, for example, the area Floor, it is possible to get a list of all users who are on this floor, and by choosing area Building- all the people in the selected building.

The tab Graphic Map shows a local graphic map of the area with the objects located in this area (if the local graphic map is specified in the area settings) or a global map of the area with all the objects located there.

If the area has both the geographical location and the local graphic map, switching between displaying local and global map can be done by pressing either the Global map or the Local map in the header of the panel.

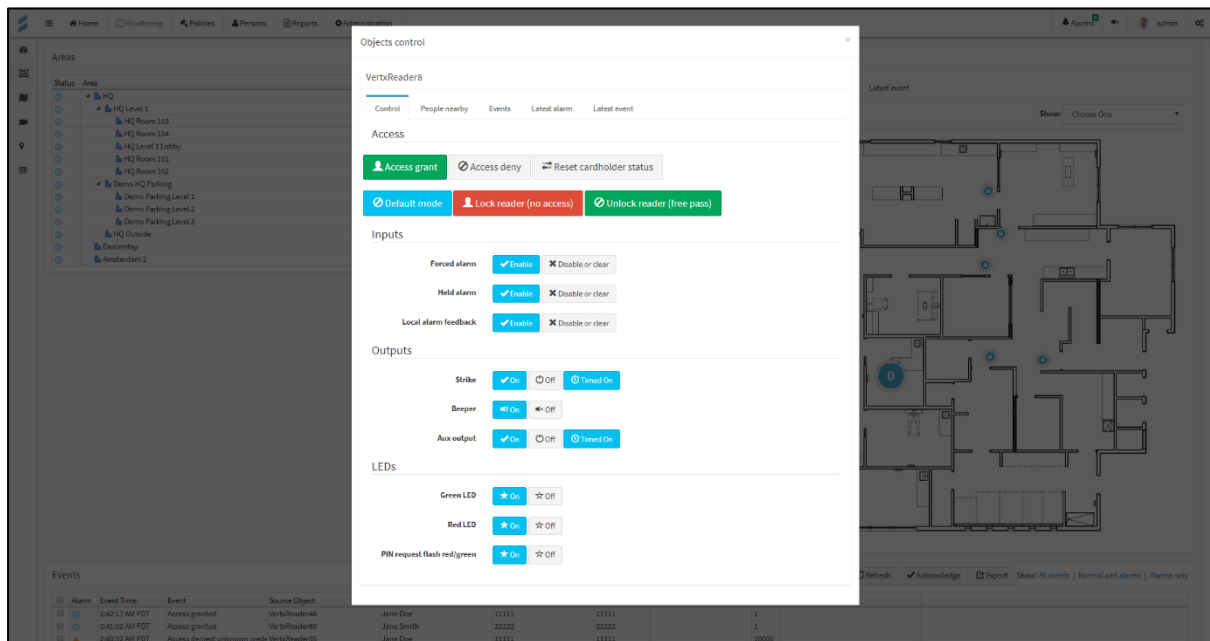
The state of the objects located inside the area (or internal areas of the selected area) can be seen on the local graphic map in the Local Map mode.

The screenshot displays the Areashell 1.7 interface. The top navigation bar includes links for Home, Monitoring, Policies, Persons, Reports, and Administration. The left sidebar shows a tree view of areas under 'Areas', including HQ Level 1 and Demo HQ Parking. The main area is titled 'HQ Level 1' and features a 'Graphic map' tab. Below the tab are buttons for 'Local map' and 'Global map'. The map itself shows a floor plan with various colored markers (blue, yellow, green) indicating object locations. At the bottom, there is an 'Events' table with columns for Alarm, Event Time, Event, Source Object, Person, Credential, Card number, Operator, Priority, and Comment. The table lists several access events, including denied and granted access, with associated timestamps and user information.

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
▲	2:40:32 AM PDT	Access denied: unknown cred	VerbaReader55	Jane Doe	11111	11111		10000	
▲	2:40:07 AM PDT	Access denied: no door access	VerbaReader5	Jane Doe	11111	11111		10000	
▲	2:39:52 AM PDT	Access denied: area violation	VerbaReader47	John Doe	12345	12345		10000	
▲	2:39:27 AM PDT	Access denied: APB violation	VerbaReader38	John Doe	12345	12345		10000	
○	2:39:17 AM PDT	Access granted	VerbaReader62	Jane Doe	11111	11111		1	
▲	2:39:02 AM PDT	Access denied: unknown cred	VerbaReader51	John Doe	12345	12345		10000	
▲	2:38:32 AM PDT	Access denied: wrong PIN	VerbaReader57	Jane Smith	22222	22222		10000	
▲	2:38:07 AM PDT	Access denied: door schedule	VerbaReader15	Jane Doe	11111	11111		10000	
▲	2:38:02 AM PDT	Access denied: door schedule	VerbaReader59	Jane Smith	22222	22222		10000	
○	2:37:22 AM PDT	Access granted	VerbaReader8	Jane Doe	11111	11111		1	
○	2:37:02 AM PDT	Access granted	VerbaReader59	Jane Doe	11111	11111		1	
○	2:36:02 AM PDT	Access granted	VerbaReader37	Jane Smith	22222	22222		1	
○	2:35:27 AM PDT	Access granted	VerbaReader20	John Doe	12345	12345		1	
○	2:35:12 AM PDT	Access granted	VerbaReader35	Jane Doe	11111	11111		1	
▲	2:34:07 AM PDT	Access denied: no door access	VerbaReader71	John Doe	12345	12345		10000	

Showing 1 to 15 of 118

When selecting any object on the local graphic plan, the object control window opens. This window displays the list of recent posts on the subject. There it is also possible to give a control command (similar to Internal Objects Status tab).



The facility control window can be closed by checking the cross in the upper right corner.

The location and status of the objects or subareas, located inside the selected area, can be seen in the global map in Global Map Mode.

When selecting an object or subarea marker on the map, the object control window opens.

Areas

Status	Area
📍	SaferPlace
📍	Bney Brak
📍	Kodak Building
📍	France House
📍	Wimazer Parking Lot

Bney Brak

Dashboard | Control | Inner objects status | People inside | **Graphic map** | Events | Latest alarm | Latest event

Local map | **Global map** | Show: Choose One

Events

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
📍	12:08:17 PM IDT	Login	7673				7673	1	
📍	12:02:56 PM IDT	Online	Bney Brak Coordinator					1	
📍	11:19:08 AM IDT	Online	Bney Brak Coordinator					1	
📍	11:05:02 AM IDT	Communication error	Bney Brak Router					10000	
📍	10:54:33 AM IDT	Parking space available	BB ASN ParkingSensor 03040002					1	
📍	10:40:40 AM IDT	Parking space available	BB ASN ParkingSensor 15040002					1	
📍	10:30:37 AM IDT	Parking space available	BB ASN ParkingSensor 13040002					1	
📍	10:29:07 AM IDT	Parking space available	BB ASN ParkingSensor 74150002					1	
📍	10:21:40 AM IDT	Parking space available	BB ASN ParkingSensor 17040002					1	
📍	10:00:58 AM IDT	Parking space available	BB ASN ParkingSensor 10040002					1	
📍	9/8/18 4:55:20 AM	Communication error	SaferPlaceCoordinator					10000	
📍	9/8/18 4:55:19 AM	Communication error	Kodak Coordinator					10000	
📍	9/8/18 4:55:18 AM	Communication error	Wimazer Coordinator					10000	
📍	8/26/18 8:31:27 PM	Parking space occupied	ASN ParkingSensor e6040002					1	
📍	7/29/18 1:05:01 PM	Parking space available	VIMC77m jcr-n 86040002					1	

Showing 1 to 15 of 37

The work with events in the table is performed similarly to dealing with events in the mode Events Only.

5.4 System monitoring in graphic map mode

The Maps page displays the list of graphic maps registered in the system (in the top left corner), the panel of the selected graphic map (in the top right corner) and the panel with the recent events table (at the bottom).

The column Status of the graphic maplist displays the status of each plan. If any object on the plan has an alarming status, then the map itself will have an alarming status too.

When choosing any map in the list, a panel appears in the right panel with this graphic map, where the icons displayed on the map are the objects of the system.

When selecting any object on the graphic map, the object control window opens. In this window, it is possible to view the list of recent events on the object or issue a control command (similar to the Inner Objects Status tab).

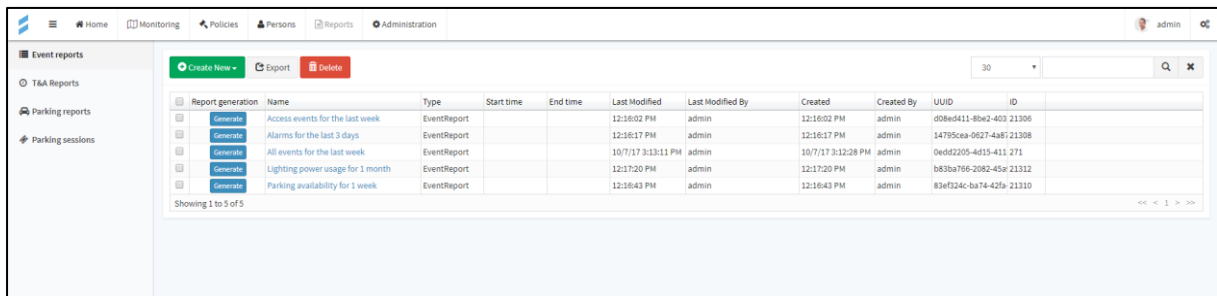
The screenshot shows the 'Maps' page in the Areashell 1.7 interface. On the left, a sidebar lists available maps: Graphic Map, Biometric Map, DoorMap, HQ Level1 Map, and Parking Map. The main area displays the 'HQ Level1 Map' with a floor plan and various colored icons representing system objects. Below the map, an 'Events' table is visible, showing a list of recent events with columns for Alarm, Event Time, Event, Source Object, Person, Credential, Card number, Operator, Priority, and Comment. The table is filtered to show 'Normal and alarms' and 'Alarms only'.

Alarm	Event Time	Event	Source Object	Person	Credential	Card number	Operator	Priority	Comment
Alarm	2:43:37 AM PDT	Access denied: wrong PIN	VerbiReader29	Jane Smith	22222	22222		10000	
Alarm	2:43:27 AM PDT	Access granted	VerbiReader44	John Doe	12345	12345		1	
Alarm	2:42:17 AM PDT	Access granted	VerbiReader48	Jane Doe	11111	11111		1	
Alarm	2:41:02 AM PDT	Access granted	VerbiReader49	Jane Smith	22222	22222		1	
Alarm	2:40:32 AM PDT	Access denied: unknown cred	VerbiReader55	Jane Doe	11111	11111		10000	
Alarm	2:40:07 AM PDT	Access denied: no door access	VerbiReader5	Jane Doe	11111	11111		10000	
Alarm	2:39:32 AM PDT	Access denied: area violation	VerbiReader47	John Doe	12345	12345		10000	
Alarm	2:39:27 AM PDT	Access denied: APD violation	VerbiReader38	John Doe	12345	12345		10000	
Alarm	2:39:17 AM PDT	Access granted	VerbiReader42	Jane Doe	11111	11111		1	
Alarm	2:39:02 AM PDT	Access denied: unknown cred	VerbiReader51	John Doe	12345	12345		10000	
Alarm	2:38:32 AM PDT	Access denied: wrong PIN	VerbiReader57	Jane Smith	22222	22222		10000	
Alarm	2:38:07 AM PDT	Access denied: door schedule	VerbiReader15	Jane Doe	11111	11111		10000	
Alarm	2:38:02 AM PDT	Access denied: door schedule	VerbiReader59	Jane Smith	22222	22222		10000	
Alarm	2:37:22 AM PDT	Access granted	VerbiReader8	Jane Doe	11111	11111		1	
Alarm	2:37:02 AM PDT	Access granted	VerbiReader9	Jane Doe	11111	11111		1	

Working with events in the table is similar to working with events in the Events Only mode.

6 Reports

Reporting is made in Reports section of the console.

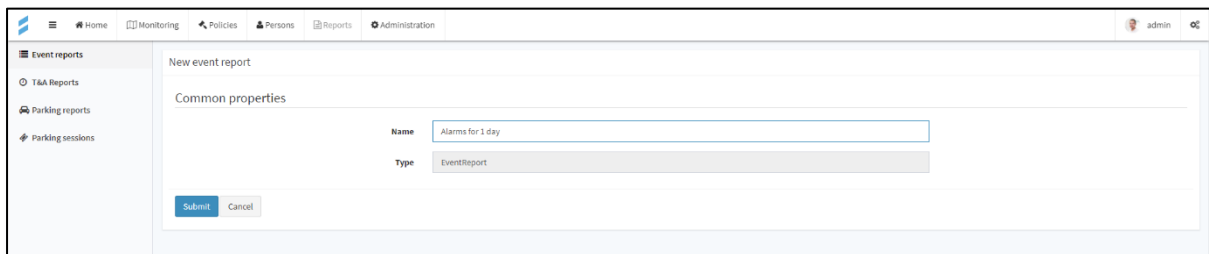


The screenshot shows the 'Reports' section of the Areashell console. The left sidebar contains a menu with 'Event reports', 'T&A Reports', 'Parking reports', and 'Parking sessions'. The main area displays a table of event reports with columns for Report generation, Name, Type, Start time, End time, Last Modified, Last Modified By, Created, Created By, UUID, and ID. There are 5 reports listed, each with a 'Generate' button. The table is paginated, showing 1 to 5 of 5 items.

Report generation	Name	Type	Start time	End time	Last Modified	Last Modified By	Created	Created By	UUID	ID
Generate	Access events for the last week	EventReport			12:16:02 PM	admin	12:16:02 PM	admin	d08e0411-8be2-403-21306	
Generate	Alarms for the last 3 days	EventReport			12:16:17 PM	admin	12:16:17 PM	admin	14795cea-0627-4a81-21308	
Generate	All events for the last week	EventReport			10/7/17 3:13:11 PM	admin	10/7/17 3:12:28 PM	admin	0e0d2205-4d15-411-271	
Generate	Lighting power usage for 1 month	EventReport			12:17:20 PM	admin	12:17:20 PM	admin	b63ba766-2082-45a-21312	
Generate	Parking availability for 1 week	EventReport			12:16:43 PM	admin	12:16:43 PM	admin	83ef224c-ba74-42fa-21310	

To create a report, first create its configuration by clicking Create / New event report.

In the panel 'Create a new event report' enter the name of the new report, and then click 'Submit'.



The screenshot shows the 'New event report' form in the Areashell console. The form has a 'Name' field with the value 'Alarms for 1 day' and a 'Type' dropdown menu with the value 'EventReport'. There are 'Submit' and 'Cancel' buttons at the bottom.

New event report

Common properties

Name:

Type:

Open the created report by selecting it in the table. The panel with the report configuration opens.

The screenshot shows the 'Alarms for 1 day' configuration panel in the Areashell Administration interface. The panel is divided into several sections:

- Date/Time:**
 - Time field for filter:** A dropdown menu set to 'Local time'.
 - Time mode:** Radio buttons for 'Relative time' (selected) and 'Absolute time'.
 - Maximum events age:** A text input field with '1' and a 'Days' dropdown.
 - Minimum time:** A text input field with a calendar icon.
 - Maximum time:** A text input field with a calendar icon.
 - Current locale:** English.
 - Example of time format:** 12:57:24 PM.
- Event alarm level:**
 - Minimum alarm level:** A text input field with '2000'.
 - Maximum alarm level:** A text input field with '2147483647'.
- Person:**
 - First name:** A text input field.
 - Last name:** A text input field.
 - Organization:** A text input field.
 - Department:** A text input field.
 - Credential number:** A text input field.
- Event codes:** A list of checkboxes for various event codes:
 - ☐ A to D limits changed
 - ☐ Credential updated
 - ☐ Host lookup
 - ☐ Access denied: APB violation
 - ☐ Access denied: APB Violation Exit
 - ☐ Access denied: Area Violation
 - ☐ Access denied: Area Violation Exit
 - ☐ Access denied: credential deleted
 - ☐ Access denied: door group or schedule not configured
- Source objects:**
 - Include objects:** A button.
 - Exclude objects:** A button.
 - Table:** A table with columns 'Name', 'Type', and 'UUID'.

At the bottom of the panel are 'Submit' and 'Cancel' buttons.

Specify the following settings when configuring the report:

- Time field for filter – parameter that allows selecting the time field in which the events will be filtered;
 - o Local time – time of event occurrence received from the controller (or the local time of the server for events generated by the system itself, and not derived from hardware controllers);
 - o UTC – the time of the event occurrence received from the controller, but reduced to the time zone UTC;
 - o Registratin time – the time of registration of events in the system database (may be different from the local time in the case the events took place in offline mode, ie when there is no communication between the controller and the server).
- Time selecting mode:
 - o Relative time – the time in the report filter is relative to the time of its generation;
 - o Absolute time – the time in the report filter clearly indicates the settings, regardless of the generation time of the report;
- Maximum age of the events – can be set only in the Relative time mode
- Minimum time and Maximum time – can be set only in Absolute time mode

- Minimum and maximum alarm levels allow filtering the events by the alarm levels
The following event alarm levels are used:
 - o Normal events – 1000;
 - o Events that need attention – 10000;
 - o Alarm events – 20000;
 - o Alarm events, critical for the system as a whole - 30000.
- The list of objects, the events of which should be included in the report, can be specified in the list of events sources.
If the list is empty, than the events are not filtered by this parameter, and the report will include the events from all system objects.
To include objects in the list, click Include Objects button, check the needed objects in the window, and click ' Include ' .
To exclude objects from the list, check them and click 'Exclude Objects'.
- User / First Name or Last Name – enter the part of a first name or last name of the system user, whose events are to be included in the report. Events of other users will be excluded from the report. If the field is empty, the report will contain the events of all users and events, where the user is not specified (alarm messages, etc.)

Click Submit to save the report configuration in the system database and Close to return to the reports table.

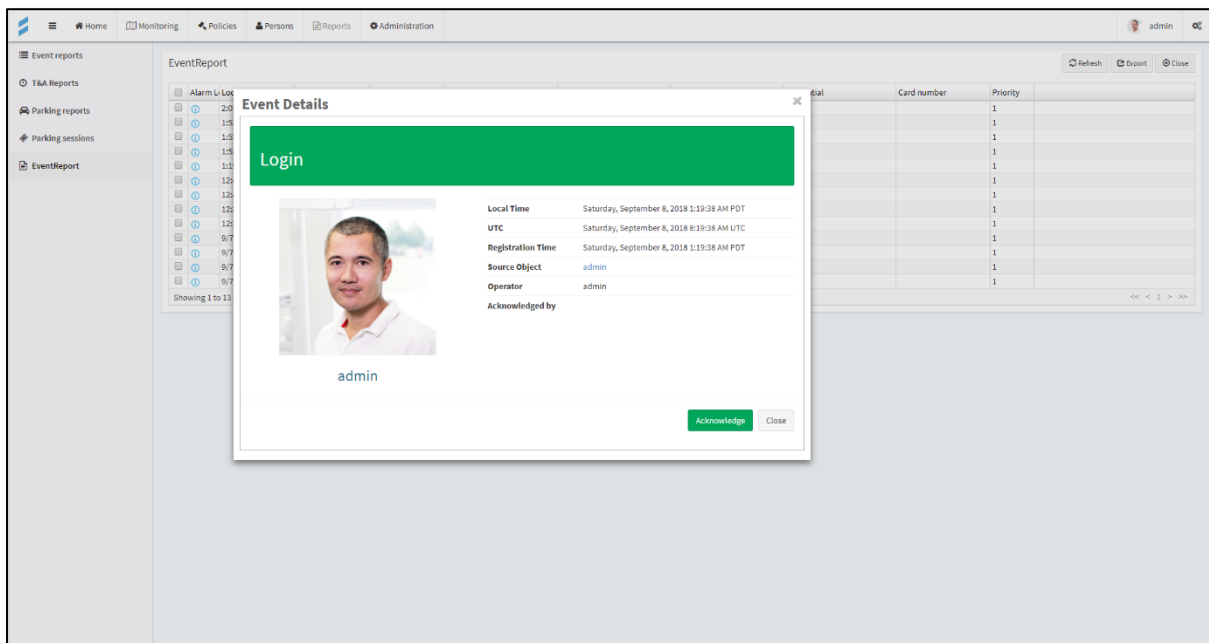
To generate the report, click **Generate** in the **Report Generation** column in the line of the required report in the report table. A new tab with the name of the generated report will be created in the side menu. This tab will be automatically selected, and the generated report will appear on the page.

The report is displayed on multiple pages, the navigation between them is carried out by using the links at the right bottom of the report table.

Alarm	Local Time	UTC	Registration Time	Event	Source Object	Person	Credential	Card number	Priority
Warning	12:58:38 PM PDT	12:58:38 PM PDT	12:58:38 PM PDT	Access denied: wrong PIN	VertReader15	Jane Doe	11111	11111	10000
Success	12:58:29 PM PDT	12:58:29 PM PDT	12:58:29 PM PDT	Access granted	VertReader59	Jane Doe	11111	11111	1
Success	12:58:24 PM PDT	12:58:24 PM PDT	12:58:24 PM PDT	Access granted	VertReader33	Jane Doe	11111	11111	1
Success	12:58:18 PM PDT	12:58:18 PM PDT	12:58:18 PM PDT	Access granted	VertReader15	Jane Smith	22222	22222	1
Warning	12:58:13 PM PDT	12:58:13 PM PDT	12:58:13 PM PDT	Access denied: APB violation	VertReader43	Jane Doe	11111	11111	10000
Error	12:58:09 PM PDT	12:58:09 PM PDT	12:58:09 PM PDT	Door forced alarm	VertReader42	Jane Doe	11111	11111	20000
Success	12:58:03 PM PDT	12:58:03 PM PDT	12:58:03 PM PDT	Access granted	VertReader58	John Doe	12345	12345	1
Warning	12:57:58 PM PDT	12:57:58 PM PDT	12:57:58 PM PDT	Access denied: area violation	VertReader23	John Doe	12345	12345	10000
Success	12:57:55 PM PDT	12:57:55 PM PDT	12:57:55 PM PDT	Access granted	VertReader59	John Doe	12345	12345	1
Warning	12:57:54 PM PDT	12:57:54 PM PDT	12:57:54 PM PDT	Access denied: APB violation	VertReader27	Jane Doe	11111	11111	10000
Warning	12:57:51 PM PDT	12:57:51 PM PDT	12:57:51 PM PDT	Access denied: unknown credential	VertReader50	John Doe	12345	12345	10000
Warning	12:57:31 PM PDT	12:57:31 PM PDT	12:57:31 PM PDT	Access denied: area violation	VertReader23	Jane Smith	22222	22222	10000
Warning	12:57:25 PM PDT	12:57:25 PM PDT	12:57:25 PM PDT	Access denied: APB violation	VertReader57	Jane Doe	11111	11111	10000
Success	12:57:21 PM PDT	12:57:21 PM PDT	12:57:21 PM PDT	Object created	Alarms for 1 day				1
Success	12:57:21 PM PDT	12:57:21 PM PDT	12:57:21 PM PDT	Event filter	EventFilter				1
Success	12:57:02 PM PDT	12:57:02 PM PDT	12:57:02 PM PDT	Access granted	VertReader5	Jane Doe	11111	11111	1
Success	12:56:59 PM PDT	12:56:59 PM PDT	12:56:59 PM PDT	Access granted	VertReader73	John Doe	12345	12345	1
Success	12:56:58 PM PDT	12:56:58 PM PDT	12:56:58 PM PDT	Access granted	VertReader8	Jane Doe	11111	11111	1
Success	12:56:57 PM PDT	12:56:57 PM PDT	12:56:57 PM PDT	Access granted	VertReader63	John Doe	12345	12345	1
Warning	12:56:51 PM PDT	12:56:51 PM PDT	12:56:51 PM PDT	Access denied: door schedule	VertReader31	Jane Smith	22222	22222	10000
Warning	12:56:45 PM PDT	12:56:45 PM PDT	12:56:45 PM PDT	Access denied: door schedule	VertReader73	Jane Doe	11111	11111	10000
Warning	12:56:38 PM PDT	12:56:38 PM PDT	12:56:38 PM PDT	Access denied: no door access	VertReader74	Jane Smith	22222	22222	10000
Success	12:56:27 PM PDT	12:56:27 PM PDT	12:56:27 PM PDT	Access granted	VertReader13	Jane Smith	22222	22222	1
Warning	12:55:55 PM PDT	12:55:55 PM PDT	12:55:55 PM PDT	Access denied: no door access	VertReader48	Jane Doe	11111	11111	10000
Warning	12:55:49 PM PDT	12:55:49 PM PDT	12:55:49 PM PDT	Door forced alarm	VertReader7	John Doe	12345	12345	20000
Warning	12:55:43 PM PDT	12:55:43 PM PDT	12:55:43 PM PDT	Access denied: no door access	VertReader47	Jane Smith	22222	22222	10000
Warning	12:55:41 PM PDT	12:55:41 PM PDT	12:55:41 PM PDT	Access denied: area violation	VertReader6	Jane Doe	11111	11111	10000
Warning	12:55:39 PM PDT	12:55:39 PM PDT	12:55:39 PM PDT	Access denied: unknown credential	VertReader22	Jane Doe	11111	11111	10000
Error	12:55:29 PM PDT	12:55:29 PM PDT	12:55:29 PM PDT	Door forced alarm	VertReader56	Jane Doe	11111	11111	20000
Success	12:55:25 PM PDT	12:55:25 PM PDT	12:55:25 PM PDT	Access granted	VertReader52	Jane Doe	11111	11111	1
Success	12:55:23 PM PDT	12:55:23 PM PDT	12:55:23 PM PDT	Access granted	VertReader12	John Doe	12345	12345	1
Warning	12:55:17 PM PDT	12:55:17 PM PDT	12:55:17 PM PDT	Access denied: wrong PIN	VertReader15	Jane Doe	11111	11111	10000
Warning	12:55:10 PM PDT	12:55:10 PM PDT	12:55:10 PM PDT	Access denied: area violation	VertReader19	Jane Doe	11111	11111	10000
Success	12:55:07 PM PDT	12:55:07 PM PDT	12:55:07 PM PDT	Access granted	VertReader48	Jane Doe	11111	11111	1
Success	12:54:48 PM PDT	12:54:48 PM PDT	12:54:48 PM PDT	Access granted	VertReader64	Jane Doe	11111	11111	1
Warning	12:54:45 PM PDT	12:54:45 PM PDT	12:54:45 PM PDT	Access denied: door schedule	VertReader59	John Doe	12345	12345	10000
Warning	12:54:42 PM PDT	12:54:42 PM PDT	12:54:42 PM PDT	Access denied: area violation	VertReader35	John Doe	12345	12345	10000
Warning	12:54:37 PM PDT	12:54:37 PM PDT	12:54:37 PM PDT	Access denied: wrong PIN	VertReader52	John Doe	12345	12345	10000
Warning	12:54:35 PM PDT	12:54:35 PM PDT	12:54:35 PM PDT	Door forced alarm	VertReader17	Jane Smith	22222	22222	20000
Warning	12:54:31 PM PDT	12:54:31 PM PDT	12:54:31 PM PDT	Access denied: unknown credential	VertReader62	Jane Smith	22222	22222	10000

The generated report can be exported to a CSV file (comma separated values file) by clicking on the **Export** button.

To view more information about an event, select it in the table.



Multiple reports can be generated at the same time. It can be done by generating new reports on the Reports tab in the top secondary menu. A new tab in the side menu will be created for each new report. These tabs can be used for navigation between the generated reports. To close a tab, click on it and then click 'Close' in the title of the report table, then the tab will disappear from the side menu.

7 Technical support

If you have questions or comments on the operation of the system, please contact your system provider.

If you have access to the system console, the coordinates of your provider is available from the section Administration / System Information, panel License Information, lines Distributor, Distributor email, and Distributor phone).

Alternatively, you can contact Areashell technical support department by the following Email: support@areashell.com